DAG2000-24/32S FXS VoIP Gateway

User Manual V1.0

Dinstar Technologies Co., Ltd.

Address: 9th Floor, Guoxing Building, Changxing Road, Nanshan District, Shenzhen, China

Postal Code: 518052

Telephone: +86 755 61919966

Fax: +86 755 2645 6659

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

Website: www.dinstar.com

Preface

Welcome

Thanks for choosing the **DAG2000-24/32S Analog Gateway for VoIP**! We hope you will make full use of this rich-feature FXS VoIP Gateway. Contact us if you need any technical support: +86-755-61919966.

About This Manual

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

Intended Audience

This manual is aimed primarily at the following people:

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

Revision Record

Document Name	Document Version	Firmware Version
DAG2000-24/32S FXS VoIP Gateway User Manual V1.0	V1.0 (2020/92/12)	2.81.10.09

Contents

1 Product Introduction

1.1 Overview

DAG2000-24/32S VoIP gateway provides voice services based on IP network. It's a cost-effective and flexible solution for SOHO (Small Office-Home office), remote office, medium-sized enterprise and enterprise with multiple branches.

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

The gateway, based on standard SIP protocol is compatible with leading IP PBX, soft-switch and SIP-based platform.

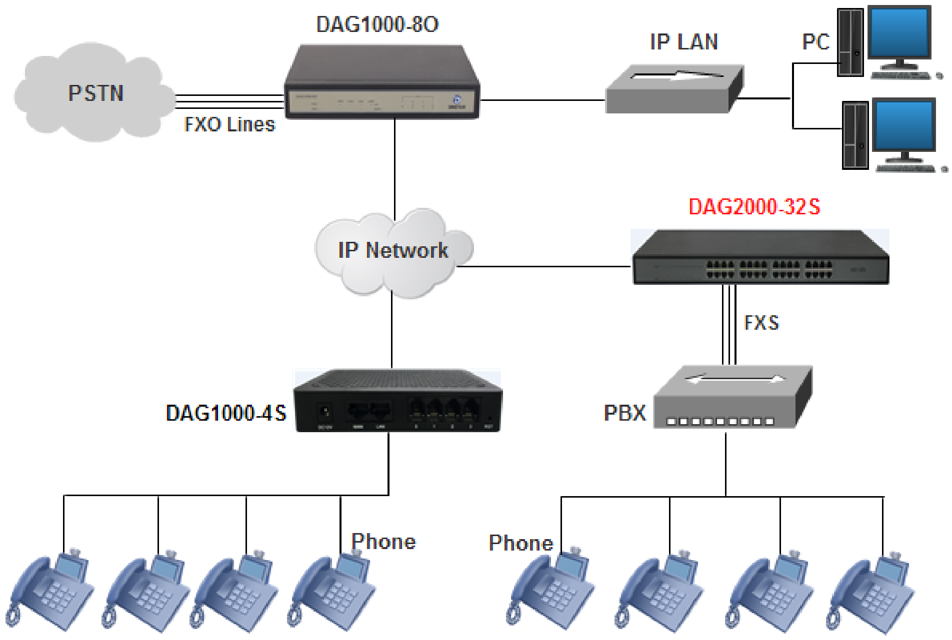
The FXS analog gateway available in the following configurations:

- ✓ DAG2000-24S, 24 port FXS VoIP gateway
- ✓ DAG2000-32S, 32 port FXS VoIP gateway

1.2 Application Scenario

The application scenario of DAG2000-24/32S is shown as follows:

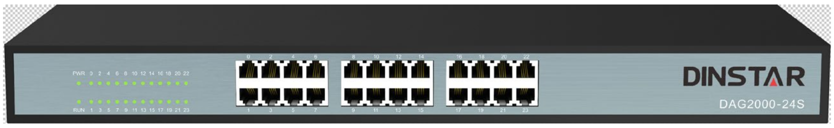
Figure 1-1 Application Scenario of DAG2000-24/32S



1.3 Product Appearance

1.3.1 Appearance of DAG2000-24S

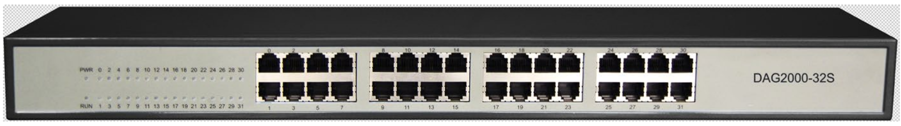
Front View:



Back View:

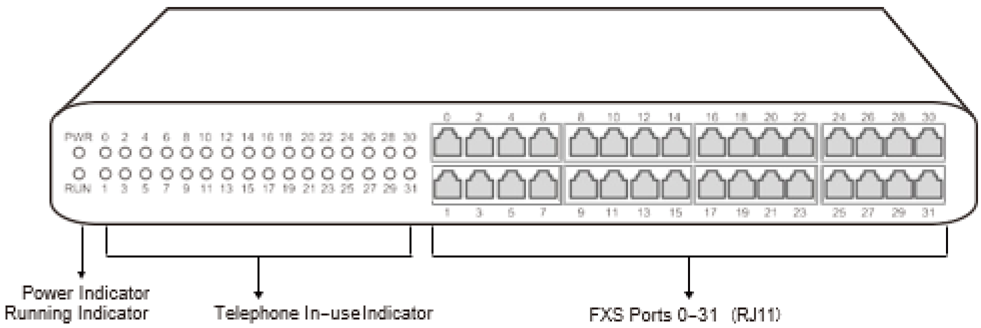
1.3.2 Appearance of DAG2000-32S

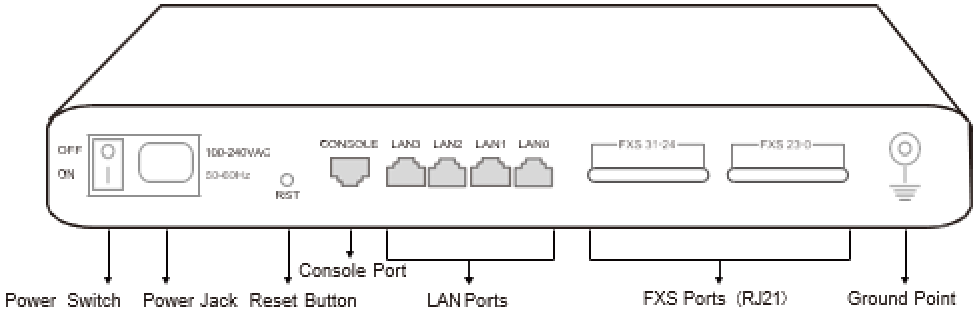
Front View:



Back View:

1.3.3 Ports and Connector





The description of interfaces of DAG2000-24/32S

Port Name	**Connector**	**Description**
Power Jack	Power Jack	To connect 100-240V AC 50-60HZ power supply
LAN Port	RJ45	to connect to the IP network over a DSL modem or Router or a LAN switch
FXS Ports 0-31	RJ11	FXS ports to connect standard analog phone or FAX machine or a PBX
Console Port	RJ48	Console port is used to carry out maintenance-related configurations

The description of indicators of DAG2000-24/32S

Indicator	**Definition**	**Status**	**Description**
PWR	Power Indicator	On	The gateway is powered on
		Off	The gateway has no power input or power supply is abnormal
RUN	Running Indicator	Slow Flashing	The gateway is running properly
		Fast Flashing	SIP account is registered successfully
		Off	The gateway is running improperly

FXS	Telephone In-use Indicator	On	FXS port is currently occupied by a call
		Off	FXS port is idle or faulty
WAN/ LAN	Link (Green)	Flashing	The gateway is properly connected to network
		Off	The gateway is not connected to network or network connection is improper

1.4 Features & Functions

1.4.1 Key Features

- Cost effective gateway with 24/32 FXS ports
- Fax over IP (T.38 and Pass-Through)
- Support IPv4 and IPv6
- TR069 and SNMP
- Multiple codecs: G.711A/U,G.723.1,G.729A/B,AMR,G.726 etc.
- Fully compatible with leading IMS/NGN, SIP based IP telephony system

1.4.2 Physical Interfaces

- Telephone Port

  DAG2000-24S: 24 FXS port (RJ11 and RJ21)

  DAG2000-32S: 32 FXS ports (RJ11 and RJ21)
- Ethernet Interfaces

  DAG2000-24/32S:

  4* LAN, 10/100Mbps, RJ-45
- Console:

  1*RS232, 115200bps

1.4.3 Voice Capabilities & Fax

- Codecs: G.711a/μ law, G.723.1, G.729A/B, G.726
- Silence Suppression
- Comfort Noise Generator(CNG)
- Voice Activity Detection(VAD)

 Copyright©2011-2020 Dinstar

- Echo Cancellation: G.168 with up to 128ms
- Adaptive (Dynamic) Jitter Buffer
- Hook Flash
- Adjustable Gain Control
- Programmable Gain Control
- FAX: T.38 and Pass-through
- High speed fax up to 14.4kbps
- Modem/POS
- DTMF: SIP Info/RFC2833/Inband
- VLAN 802.1P/802.1Q (Voice/Data/Management VLANs)
- Layer 3 QoS and DiffServ

1.4.4 FXS

- FXS Connector: RJ11
- Dial Mode: DTMF and Pulse
- Pulse: 10 and 20 PPS
- Caller ID: DTMF/FSK CLI Presentation
- Max Cable Length: 5km
- Reversed Polarity
- Programmable Call Progress Tone

1.4.5 VoIP

- Protocols: SIP v2.0 (UDP/TCP), RFC3261, SDP, RTP(RFC2833), RFC3262, RFC3263, RFC3264, RFC3265, RFC3515, RFC2976, RFC3311
- RTP/RTCP, RFC2198, RFC1889
- SIP over TLS
- RFC4028 Session Timer
- RFC3266 IPv6 in SDP URI
- RFC 3581 NAT.rport
- Primary/Backup SIP Server
- Outbound Proxy
- DNS SRV/A Query/NATPR Query
- SIP Trunk
- Early Media/Early Answer\
- NAT: STUN, Static/Dynamic NAT

1.4.6 Software Features

- Hunting Group
- Web ACL
- Telnet ACL
- Action URL
- PPPoE/IPv4/IPv6
- Digitmap
- Bandwidth Optimization
- Routing Rules based on Prefixes
- Caller/Called Number Manipulation

1.4.7 Supplementary Services

- Call Waiting and Call Holding
- Call Forwarding（Unconditional/Busy/No Reply）
- Call Transfer (Blind & Attended)
- Warm/Immediately Hotline
- Do-not-disturb
- Three Parties Conversation (3-way Conference)
- Message Waiting Indicator

1.4.8 Environmental

- Power Supply: 100-240VAC, 50-60 Hz
- Power Consumption:40W(Typical)
- Operating Temperature:0 ℃ ～45 ℃
- Storage Temperature: -20 ℃ ~80 ℃
- Humidity:10%-90% Non-Condensing
- Dimensions(W/D/H): 440*250*44mm
- Unit Weight: 3.2kg
- Compliance: CE, FCC

1.4.9 Maintenance

- SNMP V1/V2/V3
- TR069
- Auto Provisioning (HTTP/FTP/TFTP)
- Web/Telnet

Copyright©2011-2020 Dinstar

- Configuration Backup/Restore
- Firmware Upgrade via Web
- CDR
- Syslog(Emerg,alert, critical,error warning,notice,info, debug)
- Ping, Tracert Test
- Network Capture
- Outward Test (GR909 Standard)
- NTP/Daylight Saving Time
- IVR Local Maintenance
- Cloud-based Management

2 Quick Installation

2.1 Installation Attentions

To avoid unexpected accident or device damage, please read the following instructions before installing the DAG2000 device:

- DAG2000-24/32S is equipped with both RJ11 and RJ21 ports;
- For the wire sequence of RJ21, please refer to Section 6 Wire Sequence of this manual.
- Anti-jamming: to reduce the interference with telephone calls, it's highly recommended that telephone lines connected to the gateway should be placed away from power cables;
- Power supply: the gateway accepts AC input voltage of 100-240V. Please ensure safe and stable power supply;
- Network bandwidth: please ensure there is enough network bandwidth so as to guarantee stabilized running of the gateway;
- Ventilation: to avoid overheating, please do not pile up the gateway with other devices and make sure the gateway has good ventilation around.
- Temperature and humidity: to avoid any accident that might cause malfunction, it's advised to install the gateway in an equipment room where temperature and humidity are appropriate;
- Mechanical load: please make sure the gateway is placed steadily to avoid damage. It' s highly advised to horizontally place the gateway on a flat surface or a cabinet.

2.2 Installation Steps

- Connect the power adapter to the power jack of the DAG2000 device;
- Connect telephone line to the FXS port(s);
- Connect network cable to the LAN port;

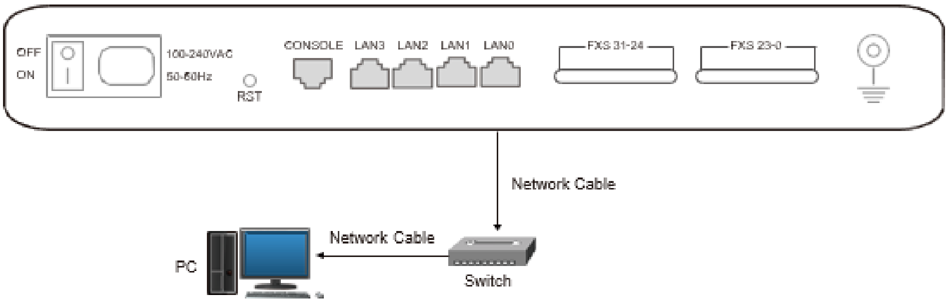
2.3 Network Connection

DAG2000-24/32Sworks in network mode: bridge mode. When it works without VLAN , network cable can connect to any of LAN port while VLAN enabled, network cable must be connected to LAN3.

2.3.1 Network Connection Diagram under Bridge Mode

Under the Bridge mode, the IP address of WAN port is the same with that of LAN port. Generally, when the device works under the bridge mode, the IP address of the device has been modified. In the following diagram, it is assumed that the IP address has been modified into 172.19.211.103.

Figure Network Connection Diagram under Bridge Mode



Note: The IP address of PC and that of WAN port of the DAG2000-24/32Sdevice are at the same network segment.

2.4 Preparations for Login

Firstly, connect the device to network according to the above network diagrams, and connect a telephone to the FXS port. Then dial *158# to query the IP address of the LAN port (default IP is 192.168.11.1).

Secondly, modify the IP address of the PC to make it at the same network segment with the LAN port of the device.

Thirdly, check the connectivity between the PC and the device. Click **Start → Run** of PC and enter **cmd** to execute 'ping 192.168.11.1' to check whether the IP address of LAN port runs normally.

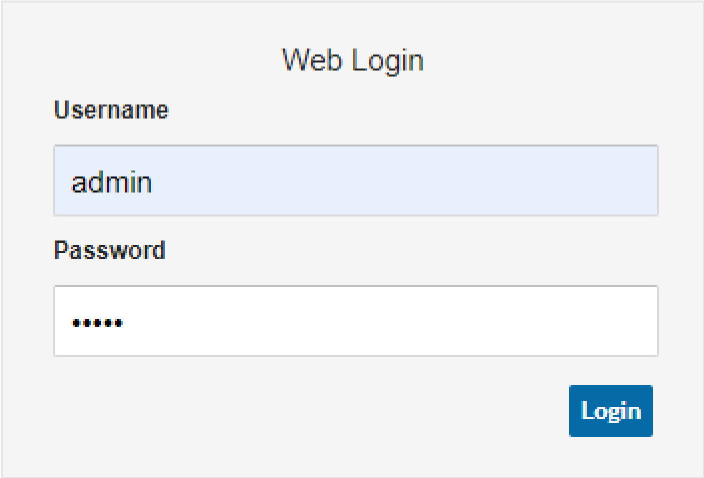
2.4.1 Log In Web Interface

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

You also can enter the IP address of WAN port, but it's required to modify the IP address of PC to make it at the same network segment with WAN port and 'Access Web by WAN' is enabled on the **Advanced →System Parameter** page.

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

Figure 2-1 Login GUI



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

3 Basic Operation

3.1 Methods to Number Dialing

There are two methods to dial telephone number or extension number:

- Dial the called number and wait for 4 seconds for dialing timeout, or dial the called number directly (the system will judge whether the dialing is completed according to Digitmap and Regular Expression dialplans).
- Dial the called number and press #.

3.2 Call Holding

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call holding feature enabled, the called party is able to switch to the new incoming call while keeping the current call holding on by dialing *# or pressing the flash button/flash hook.

When the called party dials *# once again or presses the flash button/ flash hook once again, he or she will switch back to the first call.

3.3 Call Waiting

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear a IVR voice 'Please hold on, the subscriber you dialed is busy' and the called party will hear three beeps if waiting tone is enabled.

By pressing the flash button or the flash hook, the called party is able to switch between the new incoming call and the current call.

3.4 Call Transfer

3.4.1 Blind Transfer

Blind transfer is a call transfer in which the transferring party connects the call to a third party without notifying the third party.

Copyright©2011-2020 Dinstar

Example: A gives a call to B and B wants to blindly transfer the call to C. Operation instructions are as follows:

1. A dials the extension number of B;
2. The extension of B rings, and B picks up the phone. Then A and B go into conversation;
3. B presses the flash button (or flash hook), and dial *87* after hearing a dialing tone to trigger blind transfer. Then B dials the extension number of C (end up with #).
4. The extension of C rings, B hangs up the phone and C picks up the phone. Then C and A goes into conversation.

Note:

- On the 'Advanced →Feature Code' page, blind transfer should be enabled.
- If B hears continuous busy tones after he dials the extension number of C, it means the call has timed out.

3.4.2 Attended Transfer

Attended transfer is a call transfer in which the transferring party connects the call to a third party after he confirms that the third party agrees to answer the call.

Example: A gives a call to B and B wants to attended transfer the call to C. Operation instructions are as follows:

1. A dials the extension number of B;
2. The extension of B rings, and B picks up the phone. Then A and B go into conversation;
3. B presses the flash button (or flash hook), and then dials the extension number of C (end up with #).

; Then one of the following situations will happen:

a. If C answers the call and accepts the transfer, B will hand up the phone, and then C and A go into conversation.

b. If the extension of C cannot be reached or if C rejects the call, B needs to press the flash button to resume the call with A.

3.5 Function of Flash-hook

Assume A and B are in a call conversation:

If B presses the flash hook, and then dial the number of C, B and C go into conversation and meanwhile the call between B and A is kept holding.

Then, if B presses the flash hook and dials 1, the conversation will switch back to A and B; if B presses the flash hook and dials 2 , the conversation will switch to B and C; if A presses the flash hook and dials 3, the conversation will switch to A , B and C (which is named ‘**three-way calling**’).

3.6 Description of Feature Code

DAG2000-24/32Sprovides convenient telephone functions. Connect a telephone to the FXS port and dial a specific feature code, and you can query corresponding information.

Code	Corresponding Function
***159#**	Dial *159# to query WAN IP
***158#**	Dial *158# to query LAN IP
***114#**	Dial *114# to query the phone number of a FXS port
***115#**	Dial *115# to query the phone number of a FXS port group
***168#**	Dial *168# to query the register status of a FXS port
157	Dial *157*0 to set route mode; dial *157*1 to set bride mode
150	Dial *150*1 to set IP address as static IP address; dial *150*2 to set IP address as DHCP IP address
152	Dial *152* to set IPv4 address, for example: Dial *152*192*168*1*10# to set IPv4 address as 192.168.1.10
156	Dial *156* to set IPv4 gateway, for example: Dial *156*192*168*1*1# to set IPv4 gateway as 192.168.1.1
153	Dial *153* to set IPv4 netmask, for example: Dial *153*255*255*0*0*# to set IPv4 netmask as 255.255.0.0
***170#**	Dial *170# to increase the sound volume of a FXS port
***171#**	Dial *171# to decrease the sound volume of a FXS port
160	Dial *160*1# to allow HTTP WAN access, Dial *160*0# to deny HTTP WAN access
165	Dial *165*000000# to restore username/password and network configuration to factory defaults
***111#**	Dial *111# to restart the device
47	Dial *47* to allow call through IP address, for example: Dial *47*192*168*1*1# to allow to call through the IP address of 192.168.1.1
***51#**	Dial *51# to enable the call waiting service
***50#**	Dial *50# to disable the call waiting service
87	Dial *87* to trigger blind transfer, for example:

	Dial *87*8000#, and you can blind transfer to the extension number 8000
72	Enable unconditional call forwarding service. Example: Dial *72*8000, and calls will be unconditionally forwarded to extension number 8000
***73#**	Disable unconditional call forwarding service
90	Enable the 'call forwarding on busy' service. Example: Dial *90*8000, and calls will be forwarded to extension number 8000 when the called number is busy
***91#**	Disable the 'call forwarding on busy' service
92	Enable the 'call forwarding on no reply' service. Example: Dial *92*8000, and calls will be forwarded to extension number 8000 when there is no reply from the called number
***93#**	Disable the 'call forwarding on no reply' service
***78#**	Enable the 'No Disturbing' service
***79#**	Disable the 'No Disturbing' service
***200#**	Dial *200# to access voicemail

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

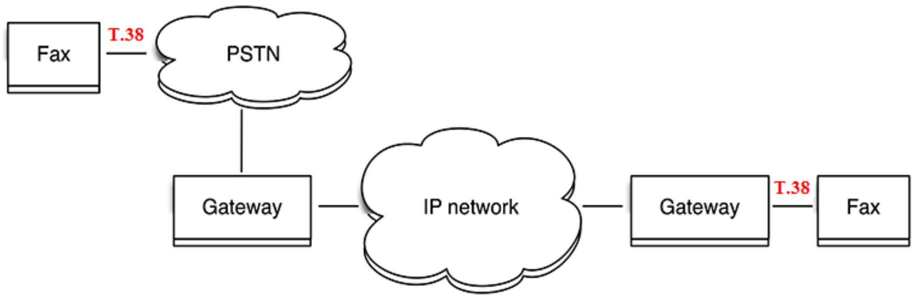
3.7 Send or Receive Fax

3.7.1 Fax Mode Supported

- T.38（IP-based）
- T.30（Pass-Through）
- Adaptive Fax Mode (automatically match with the peer fax mode)

3.7.2 Explanation of T.38 and Pass-through

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



T 3.0 (Pass-through): Under the pass-through mode, fax signal is not converted and fax traffic is carried in RTP packets. It uses the G.711 A or G711U codec in order to reduce the damage to fax signal.

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

3.8 Function of RST Button

Press the RST button of DAG2000-24/32Sfor a moment, the running indicator will turn from "slow flashing" into "no flashing", and then turn into "slow flashing" again. That means the device has been restored to factory defaults.

3.9 Query IP Address and Restore Default Setting

Query IP Address:

After connecting a telephone to the FXS port, you can dial *158# to query the IP address of LAN port and dial *159# to query the IP address of WAN port.

Reset Password:

1. On the "Security → Passwords" page of the Web interface, you can reset username and password.
2. You can also reset password through the Cloud platform.
3. Connect a telephone with the DAG2000 device, and then dial *165*000000# to restore username/password and network configuration to factory defaults.

Restore Device to Default Settings:

1. Connect a telephone with the DAG2000 device, and then dial *166*000000# to restore all configurations to factory defaults.
2. Press the RST button for a moment, the running indicator will turn from "slow flashing" into "no flashing", and then become "slow flashing" again. That means all configurations of the device has been restored to factory defaults.
3. On the "Tools → Factory Reset" page of Web interface, click **Apply** to restore the configurations of the device to factory defaults.

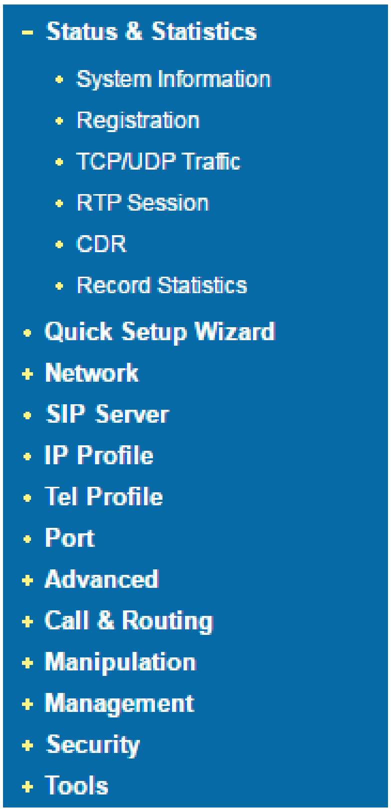
4 Configurations on Web Interface

4.1 Navigation Tree

The web management system of the DAG2000-24/32S VoIP device consists of the navigation tree and detailed configuration interfaces.

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

Figure 4-1 Navigation Tree of Web Interface



4.2 Status & Statistics

The 'Status & Statistics' menu mainly displays all kinds of information. It includes the following sub-menus: System Information, Registration, TCP/UDP Traffic, RTP Session, CDR and Record Statistics.

 Copyright©2011-2020 Dinstar

4.2.1 System Information

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

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

Figure 4-2 System Information

Table 4-1 Explanation of Items on System Information Interface:

Device ID	A unique ID of each device. This ID is used for warranty and cloud server authentication.
MAC address	Hardware address of the WAN port
IP Address	There are three kinds of IP address for the WAN port and LAN port: **DHCP: Obtain IP address automatically**. DAG2000 is regarded as a DHCP client, which sends a broadcast request and looks for a DHCP server from the LAN to answer. Then the first discovered DHCP server automatically assigns an IP address to the DAG2000 from a defined

	range of numbers. **Static IP Address:** Static IP address is a semi-permanent IP address and remains associated with a single computer over an extended period of time. This differs from a **dynamic IP address,** which is assigned *ad hoc* at the start of each session, normally changing from one session to the next. If you choose static IP address, you need to fill in the following information: ● IP Address: the IP address of the WAN port of the DAG2000; ● Subnet Mask: the netmask of the router connected the DAG2000; ● Default Gateway: the IP address of the router connected the DAG2000; **PPPoE:** PPPoE is an acronym for point-to-point protocol over Ethernet, which relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. PPPOE IP address refers to IP address assigned through the PPPoE mode. If you choose PPPoE, you need to fill in to fill in the following information: ● Username: the account name of PPPoE ● Password: the password of PPPoE ● Server Name: the name of the server where PPPoE is placed
DNS Server	IP addresses of primary DNS server and standby DNS server are displayed.
Cloud Register Status	Whether the DAG2000 device is registered to cloud or not.
System Uptime	The running time of the DAG2000 device since it is powered on.
NTP Status	Succeed: the DAG2000 device is sync to NTP server successfully; Failed: the DAG2000 device fails to be sync to NTP server. Then you should check network connection and the NTP server.
WAN Traffic Statistics	Total bytes of message received and sent by WAN 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	The software version that runs on the DAG2000 device. Model name, version number and the software development date are displayed.
Backup Software Version	Backup software is for the purpose of backup. When the current software fails, the backup software version will work.
U-boot Version	U-boot version
Kennel version	Linux Kennel version
FS Version	File system version
Hint Language	The current language of the DAG device

4.2.2 Registration

On the **Status & Statistics → Registration** page, you can view the registration status of each FXS port or port group.

Figure 4-3 Registration Status of Each FXS Port or Port Group

Port Registration Information

Port No.	Type	SIP User ID	SIP User Status
0	FXS	056000...	Registered
1	FXS	056001...	Registered

Port Group Registration Information

Port Group	Port	SIP User ID	SIP User Status
1 <10001>	0,1,...	10001...	Registered

Refresh

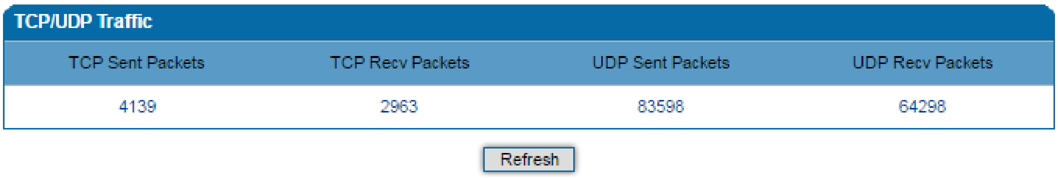
SIP User status:

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

4.2.3 TCP/UDP Statistics

On the **Status & Statistics → TCP/UDP Statistics** page, you can view the statistical number of sending or receiving packets over TCP, and the number of sending or receiving packets over UDP since the DAG2000 device is booted up.

Figure 4-4 TCP/UDP Statistics



TCP/UDP Traffic

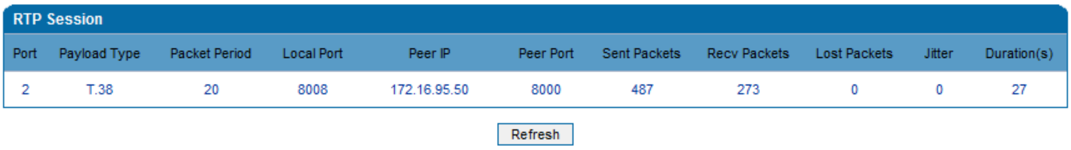
TCP Sent Packets	TCP Recv Packets	UDP Sent Packets	UDP Recv Packets
4139	2963	83598	64298

Refresh

4.2.4 RTP Session

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

Figure 4-5 Real-time RTP Session Information



RTP Session

Port	Payload Type	Packet Period	Local Port	Peer IP	Peer Port	Sent Packets	Recv Packets	Lost Packets	Jitter	Duration(s)
2	T.38	20	8008	172.16.95.50	8000	487	273	0	0	27

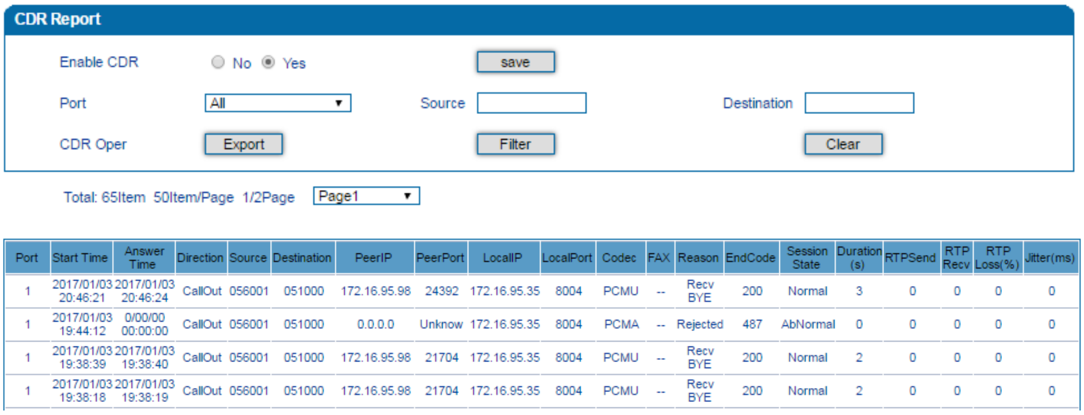
Refresh

4.2.5 CDR

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

On the **Status & Statistic → CDR** page, you can enable the CDR function and view the details of all calls through the FXS ports of the DAG2000 device. You can also export, filter or clear the CDRs. 5000 pieces of CDRs can be saved at most.

Figure 4-6 CDRs of FXS Ports



CDR Report

Enable CDR	No Yes	save			
Port	All	Source		Destination	
CDR Oper	Export	Filter		Clear	

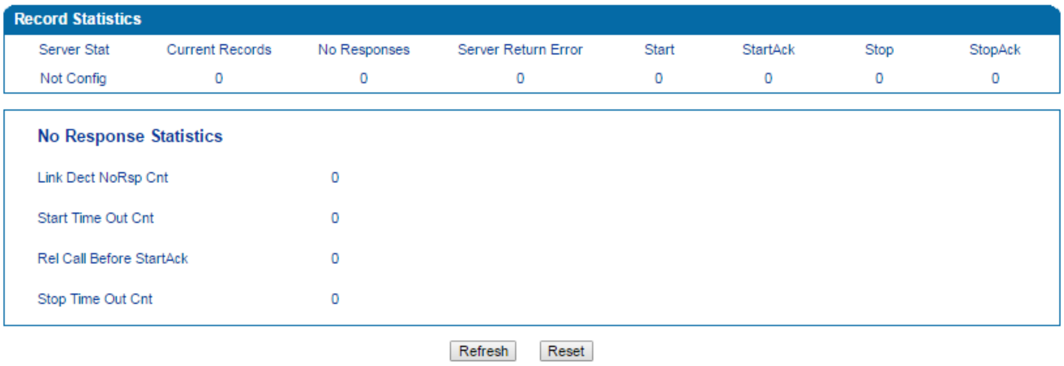
Total: 65Item 50Item/Page 1/2Page Page1

Port	Start Time	Answer Time	Direction	Source	Destination	PeerIP	PeerPort	LocalIP	LocalPort	Codec	FAX	Reason	EndCode	Session State	Duration (s)	RTPSend	RTP Recv	RTP Loss(%)	Jitter(ms)
1	2017/01/03 20:46:21	2017/01/03 20:46:24	CallOut	056001	051000	172.16.95.98	24392	172.16.95.35	8004	PCMU	--	Recv BYE	200	Normal	3	0	0	0	0
1	2017/01/03 19:44:12	0/00/00 00:00:00	CallOut	056001	051000	0.0.0.0	Unknow	172.16.95.35	8004	PCMA	--	Rejected	487	AbNormal	0	0	0	0	0
1	2017/01/03 19:38:39	2017/01/03 19:38:40	CallOut	056001	051000	172.16.95.98	21704	172.16.95.35	8004	PCMU	--	Recv BYE	200	Normal	2	0	0	0	0
1	2017/01/03 19:38:18	2017/01/03 19:38:19	CallOut	056001	051000	172.16.95.98	21704	172.16.95.35	8004	PCMU	--	Recv BYE	200	Normal	2	0	0	0	0

4.2.6 Record Statistics

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

Figure 4-7 Record Statistics



Record Statistics

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

No Response Statistics

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

Refresh Reset

4.3 Quick Setup Wizard

Quick setup wizard guides user to configure the device step by step. User only needs to configure network, SIP server and SIP port in the Quick Setup Wizard interface. Basically, after these three steps, user is able to make voice call via the DAG2000 device.

For the configurations of network, SIP server and SIP port, please refer to 4.4 , 4.5 and 4.6 .

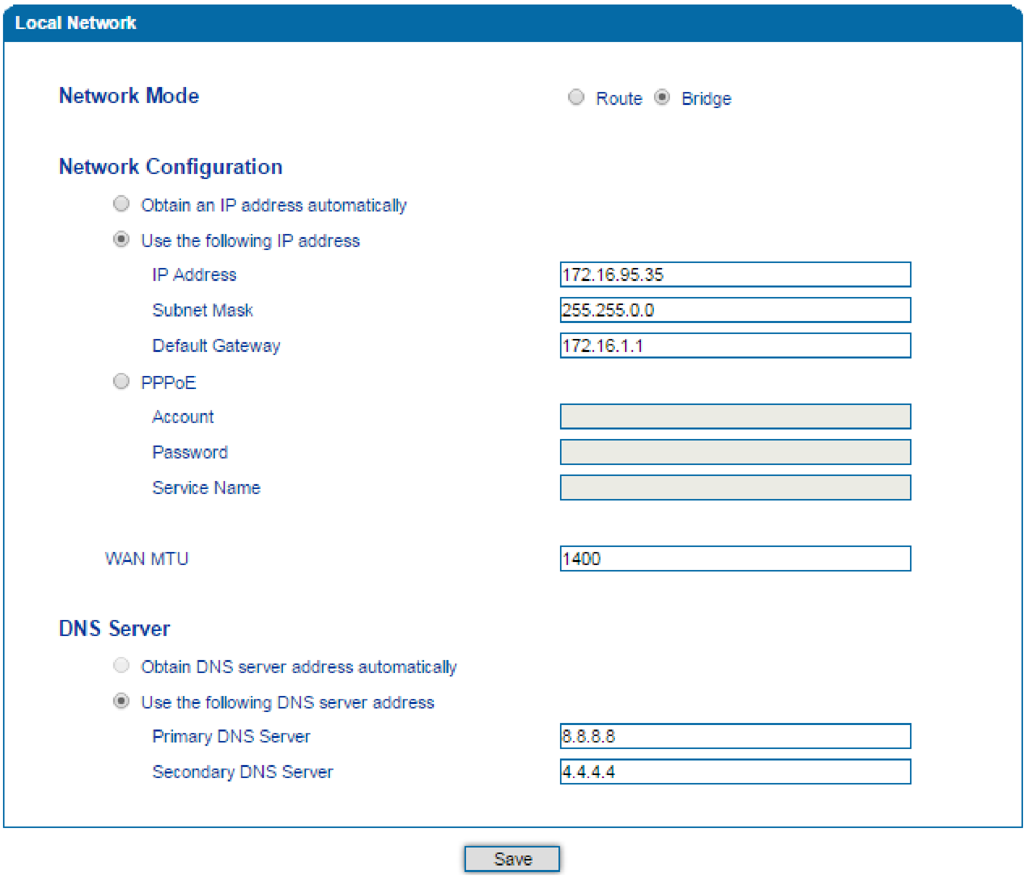
4.4 Network

4.4.1 Local Network

The device works under the bridge mode, WAN port and LAN port are the same. The device serves as a four-port Ethernet switch. Under this network mode, user only needs to configure the IP address of LAN port and DNS.

Under the route mode, the default IP address of LAN port is a DHCP IP address, while the default IP address of the LAN port is 192.168.11.1.

Figure 4-8 Network Setting under Bridge Mode



4.4.2 VLAN（Virtual Local Area Network）

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

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

Figure 4-9 Configure VLAN

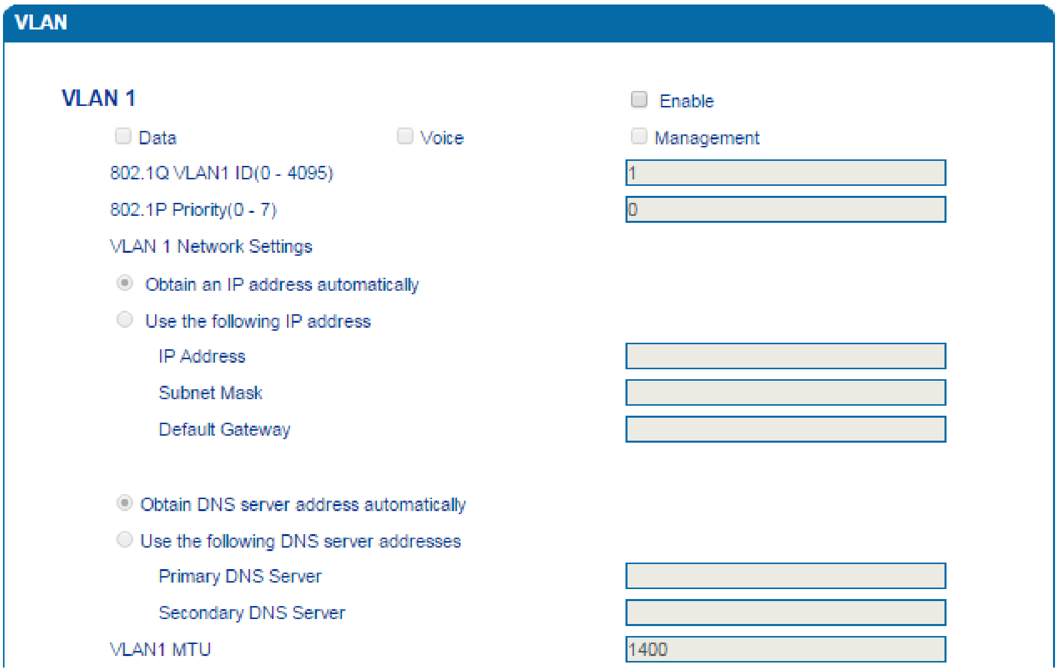


Table 4-2 Explanation of VLAN Parameters

VLAN1/VLAN2/VLAN3	The device supports three VLANs at most. Please enable VLAN according to actual needs.
Data/Voice/Management	Select what kind of messages are allowed to go through this VLAN. For example, if the checkbox on the left of data is selected, it means data messages are subject to the following network setting of this VLAN.
802.1Q VLAN ID(0-4095)	Set an ID to identify a VLAN based on 802.1Q protocol. Range is from 0 to 4095.
802.1p Priority（0-7）	Set the priority of a VLAN based on 802.1P protocol. 0 is the highest priority.
Network Setting	Set a DHCP IP address or static IP address for a VLAN, and set the IP address of the DNS server used by the VLAN.

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

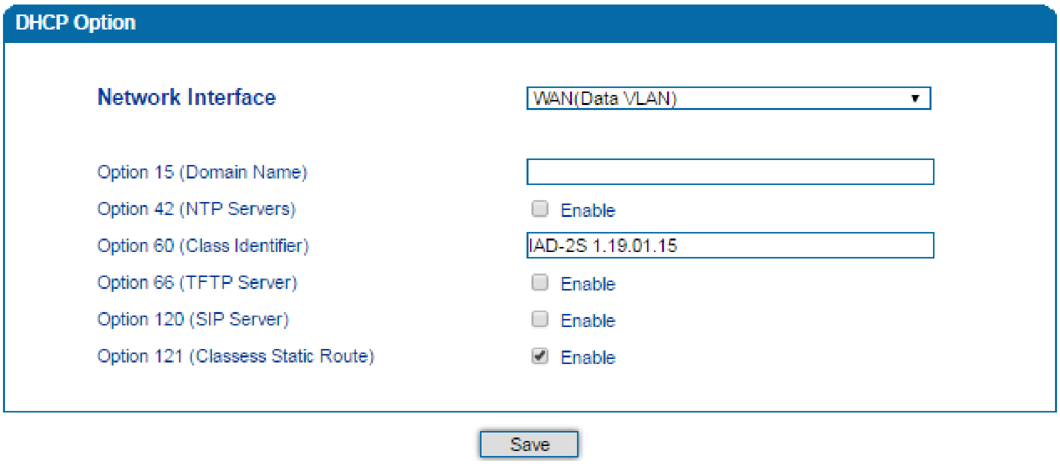
4.4.3 DHCP Option

When the DAG2000 device works as a DHCP client and applies for an IP address, DHCP server will return packets which include an IP address as well as configuration information of enabled option fields.

The following is the meaning of the option fields involved in DAG2000 (that means the following option fields are enabled, DHCP server will return information of corresponding option fields:

- Option 15: to set a DNS suffix;
- Option 42: to specify NTP server;
- Option 60: to define VCI (vendor class identifier) of DAG2000 on the DHCP server;
- Option 66: to specify TFTP server which will assign software version to DAG2000;
- Option 120: to fetch SIP server address;
- Option 121: to obtain classless static route. DAG2000 will add these static routes to the static route table after it fetches them from DHCP server.

Figure 4-10 Configure DHCP Option

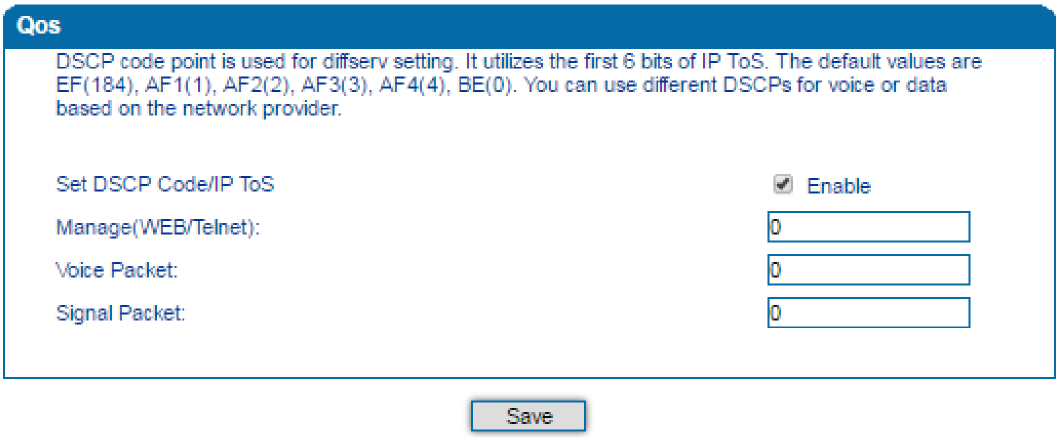


Network Interface: choose which VLAN to send request to DHCP server (or to receive information from DHCP server).

4.4.4 QoS

The DAG2000 device can label QoS priority on the IP messages it sends out, so as to resolve network delay or network congestion. Meanwhile, the device can give different QoS tags for management-related packets of Web/Telnet, voice packets and signal packets.

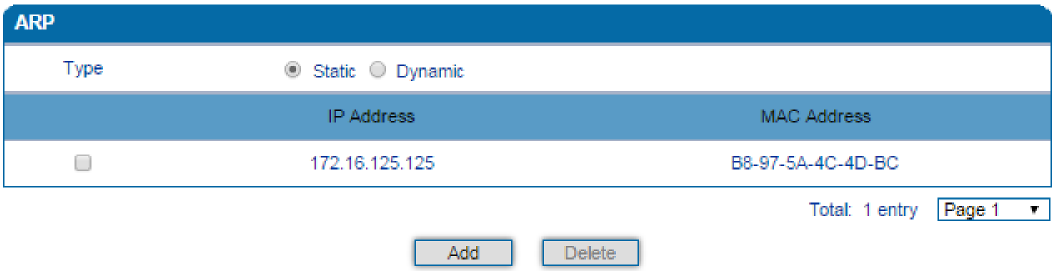
Figure 4-11 Qos



4.4.5 ARP

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

Figure 4-12 ARP



4.5 SIP Server

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

 Copyright©2011-2020 Dinstar

Figure 4-13 Configure SIP Server Information

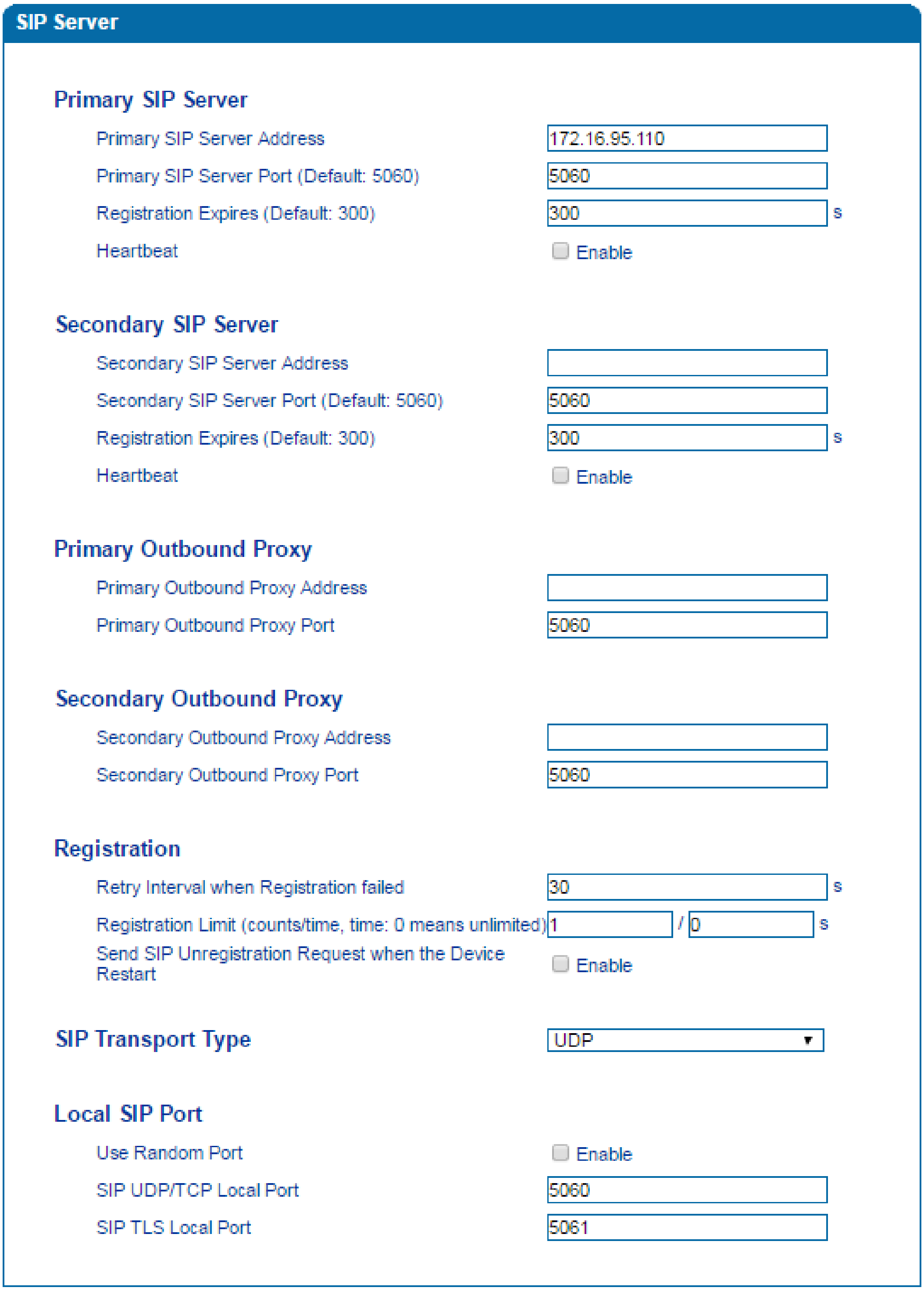


Table 4-3 Parameter Explanation of SIP Server

Primary SIP Server Address	The IP address or domain name of the primary SIP server. It is provided by VoIP service provider.
Primary SIP Server port	The service port of the primary SIP server. It is 5060 by default.

Copyright©2011-2020 Dinstar

Registration Expires	It is used to avoid excessively frequent registrations. When the time that is set expires, the DAG2000 device will send register request to the primary SIP server. The time is 300s by default.
Heartbeat	Heartbeat is used to check the connection between the DAG2000 device and SIP server.
Secondary SIP Server address	The IP address or domain name of the backup SIP server. It is provided by VoIP service provider.
Secondary SIP Server port	Service port of the backup SIP server. It is 5060 by default.
Registration Expires	It is used to avoid excessively frequent registrations. When the time that is set expires, the DAG2000 device will send register request to the backup SIP server. The time is 300s by default.
Secondary SIP heartbeat	Heartbeat is used to check the connection between the DAG2000 device and SIP server.
Outbound Proxy Address	The IP address or domain name of outbound proxy server, which is provided by VoIP service provider.
Outbound Proxy Port	Service port of outbound proxy server. It is 5060 by default.
Retry Interval when Registration failed	The retry interval after a registration fails. Default: 30s
Registration times per second	The maximum number of registrations in a second. 0 means no limitation for registrations.
SIP Transport Type	The way of SIP-based transmission. It can be UDP, TCP, TLS or Automatic. Default: UDP.
Use Random Port	If this parameter is selected, the local port of the DAG2000 device for using SIP services is chosen by random.
SIP UDP/TCP Local Port	The UDP/TCP port of DAG2000 device for using SIP services. Default SIP UDP/TCP local is 5060.
SIP TLS Local Port	The TLS port of DAG2000 device for using SIP services. Default SIP TLS local port is 5061.

Usually, SIP server does not participate in media processing. Under SIP network, media always use end-to-end negotiating. Simple SIP server is only responsible for the establishment, maintenance and cleaning of sessions, while relatively-complex SIP server (SIP PBX) not only provides basic calling and conversational support, but also offers rich services such as Presence, Find-me and Music On Hold.

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

SIP server based on windows platform, such as :mini SipServer、Brekeke，VoIPswitch etc.

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

4.6 IP Profile

IP Profile

Index	Description	SIP Server	SIP Server Port	Registration Expires	Heartbeat	Primary Outbound Proxy Address	Primary Outbound Proxy Port	Secondary Outbound Proxy Address	Secondary Outbound Proxy Port	DTMF Method	Preferred Vocoder
0	default	172.19.1.24	5060	300	Disable	---	5060	---	5060	RFC2833	G.711U

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

4.7 Tel Profile

Tel Profile

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

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

4.8 Port

A unique SIP account used for registration can be configured for each FXS port of DAG2000 device. Parameters of the SIP account include port number, whether to register, primary display name, primary SIP user ID, primary Authenticate ID, primary Authenticate password, off-hook auto-dial number, caller ID and so on.

Figure 4-14 Configure SIP Account for Port Registration

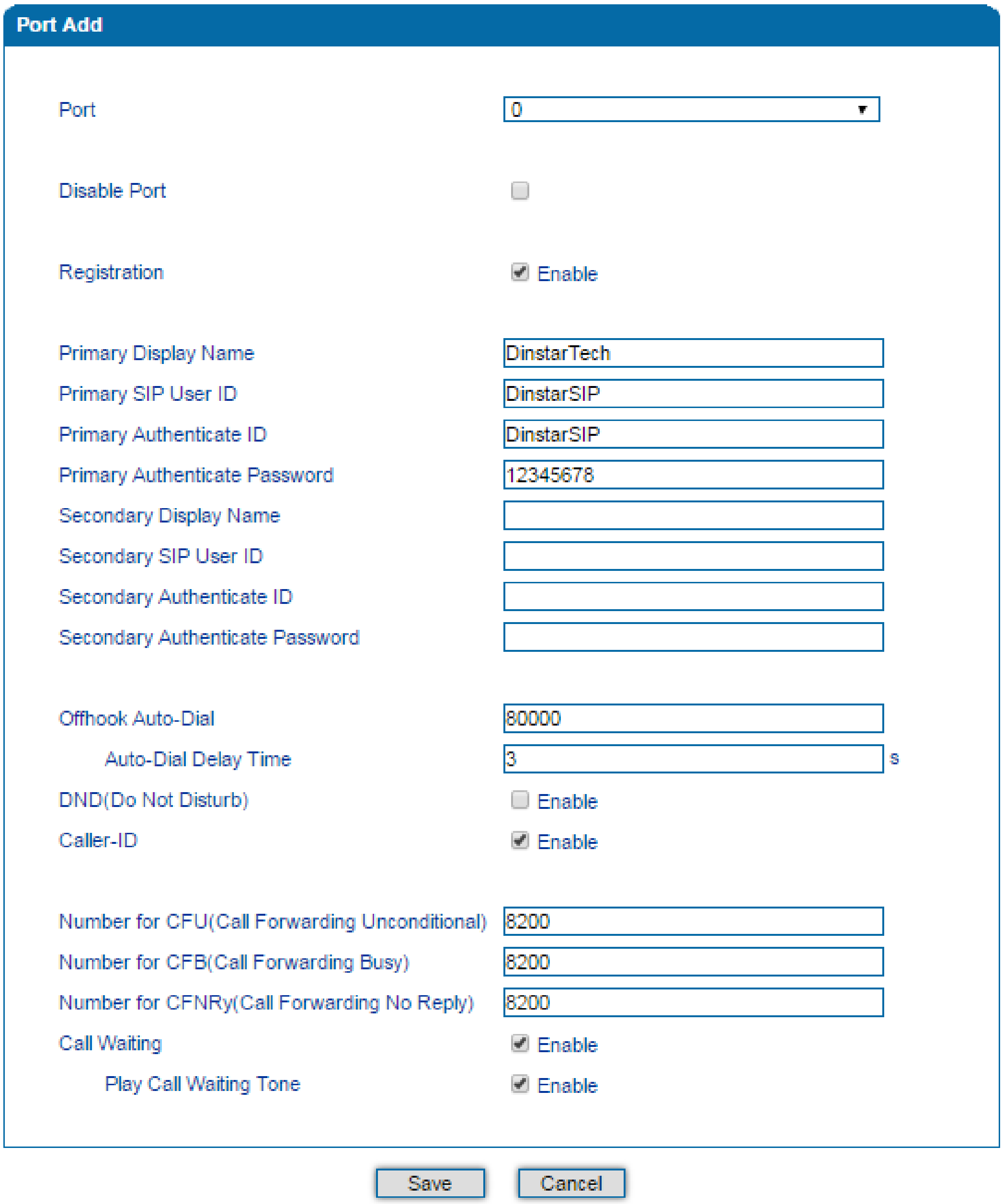


Table 4-4 Explanation of Parameters Related to SIP Registration

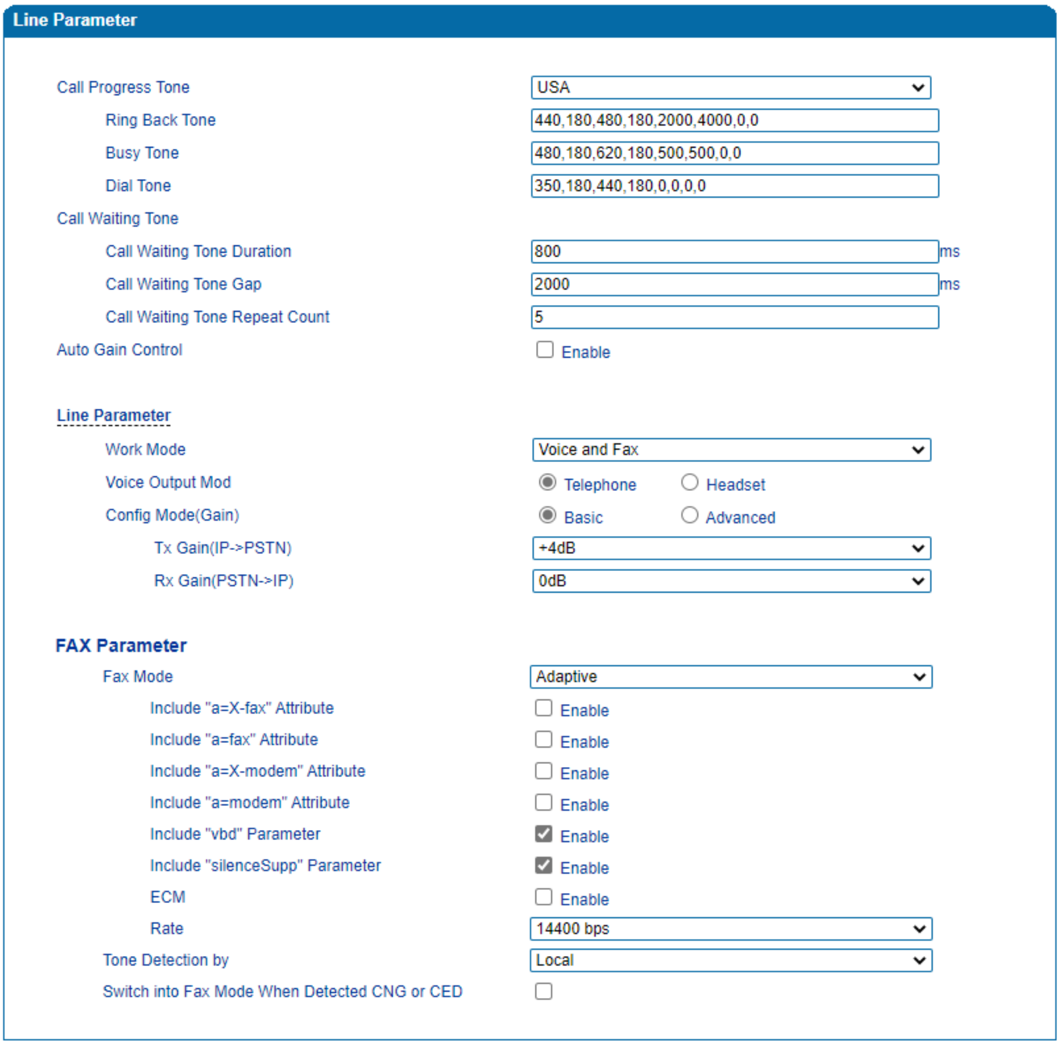
Port	The FXS port corresponding to this account
Disable port	Whether to disable port temporally
Registration	Whether to enable registration for the port
Primary /Secondary SIP Display Name	Description of primary /secondary SIP account. It is used to identify the SIP account.
Primary /Secondary SIP User ID	User ID of the SIP account, which is provided by VoIP service provider (ITSP) for registration. Usually it is in the form of digits

	similar to phone number or an actual phone number.
Primary/Secondary SIP Authenticate ID	SIP service subscriber's authenticate ID used for authentication of registration. It can be identical to or different from SIP User ID.
Primary/Secondary Authenticate password	SIP service subscriber's authenticate ID used for authentication of registration
Offhook Auto-dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-dial Delay Time	How long the auto-dial number is prolonged. If it is set as 3s, the auto-dial number is dialed after 3 seconds pass.
DND (Do Not Disturb)	the phone won't receive any calls if this feature is enabled
Caller ID	Enable or disable caller ID for corresponding port. If it is disabled, the caller ID for the calls through the port won't be displayed.
Number for CFU	Call forward unconditional. All incoming calls will be forwarded to pre-assigned number automatically
Number for CFB	Call forward on busy. If the line is busy, the call will be forwarded to pre-assigned number automatically
Number for CFNRy	Call forward no reply. If the call is not answered, the call will be forwarded to pre-assigned number automatically
Call Waiting	If call waiting is enabled, a special tone is sent if another caller tries to reach you
Play Call Waiting Tone	If call waiting tone is enabled, caller will hear special tone.

4.9 Advanced

4.9.1 Line Parameter

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



Call Process Tone	The signal tone standard after a phone is picked up. Choose national standards from the drop-down box. Default value is USA.
Auto Gain Control	Whether to enable automatic gain control
Work Mode	To set the FXS ports work in both Voice and Fax mode. There are several configure options: • Voice and FAX: to be able to make call and use FAX service • Voice Only: allows to make call only, Fax doesn't work if you connect a fax machine • Fax Only: allows to make Fax call only. • POS only: allows to connect POS terminal only
Gain mode	IP to PSTN(RX): adjust gain value to analog phone PSTN to IP(TX): adjust gain value from analog phone
FAX Parameter	The DAG2000-24/32Sdevice supports the three fax modes: T.38

	(IP-based), T.30 (Pass-Through) and Adaptive Fax Mode (automatically match with the peer fax mode).
Fax Mode	There are three fax modes: T.38, T.30(Pass-through), and Adaptive.
Include “a=X-fax” Attribute	If this parameter is enabled, “a=X-fax” attribute will be carried in SDP
Include “a=fax” Attribute	If this parameter is enabled, “a=fax” attribute will be carried in SDP
Include “a=X-modem” Attribute	If this parameter is enabled, “a=X-modem” attribute will be carried in SDP
Include “a=modem” Attribute	If this parameter is enabled, “a=modem” attribute will be carried in SDP
ECM	Whether to enable ‘Error Correction Mode’（ECM）.
Rate	The rate of sending or receiving fax, default value is 14400bps.
Tone Detection by	Fax sound is detected by caller, callee or automatically.
Switch into Fax Mode When Detect CNG or CED	If this parameter is enabled, the system will switch into fax mode when CNG or CED is detected.

4.9.2 FXS Parameter

On the **Advanced→ FXS/FXO** page, you can configure FXS parameters which include send polarity reversal, detect hook flash, CID type and so on.

Figure 4-15 Configure FXS Parameters

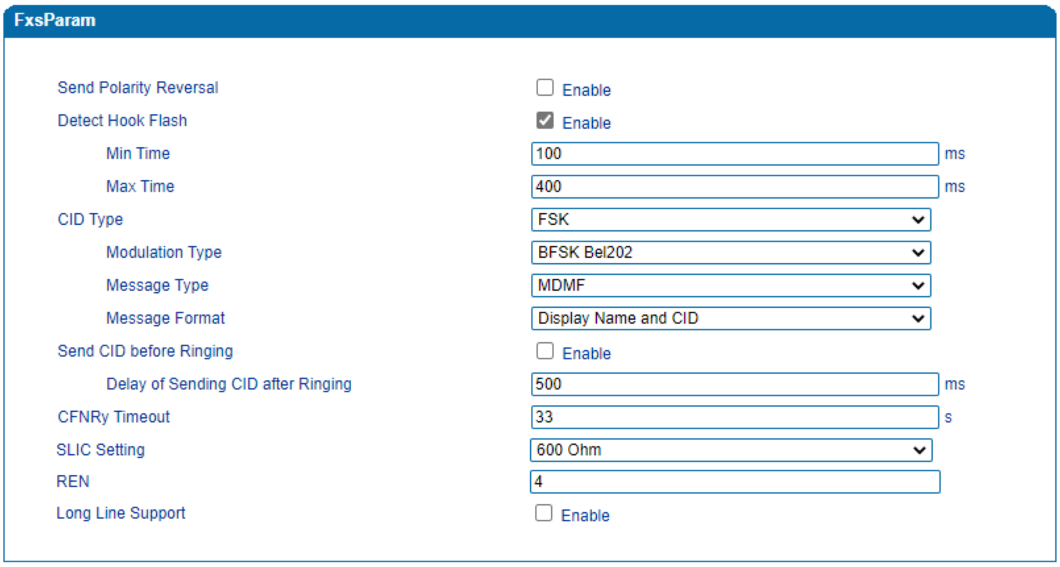


Table 4-5 Explanation of FXS Parameters

Send Polarity Reversal	If polarity reversal is enabled, call tolls will be calculated based on the changes in voltage. If polarity reverse is disabled, you need to set the time for offhook detection and call tolls will be calculated starting from the set time.
Detect Hook flash	If 'Detect Hook Flash' is enabled, you need to set a minimum time and a maximum time. If a phone's hook flash is pressed for a time period greater than the set minimum time but less than the maximum time, the action is considered as a 'hook flash' operation. If a phone's hook flash is pressed for more the set maximum time, the action is considered as 'hang up the phone'.
CID Type	There are two CID types, namely DTMF and FSK.
Message Type	There are two call display types including SDMF and MDMF
Message Format	The call display format in analog phone. It can be "Display Name and CID", "CID only", or "Display Name only"; default value is "Display Name and CID"
Send CID before Ringing	If this parameter is enabled, the device send Caller ID to phone before ringing, otherwise the caller ID will be displayed after ringing.
Delay of sending CID after Ringing	The time how long the caller ID will be delayed when the caller ID is set to be displayed after ringing. Default value is 500ms.
CFNRy Timeout	Timeout for 'call forwarding on no answer' service
SLIC Setting	Impedance matched with analog phone.

REN	The maximum number of extensions that can be connected to a single FXS port. If this parameter is configured, you need to restart the device for the configuration to take effect.
Long Line Support	Whether to enable 'Long Analog Extension Line'.

4.9.3 Media Parameter

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

Figure 4-16 Configure Media Parameters

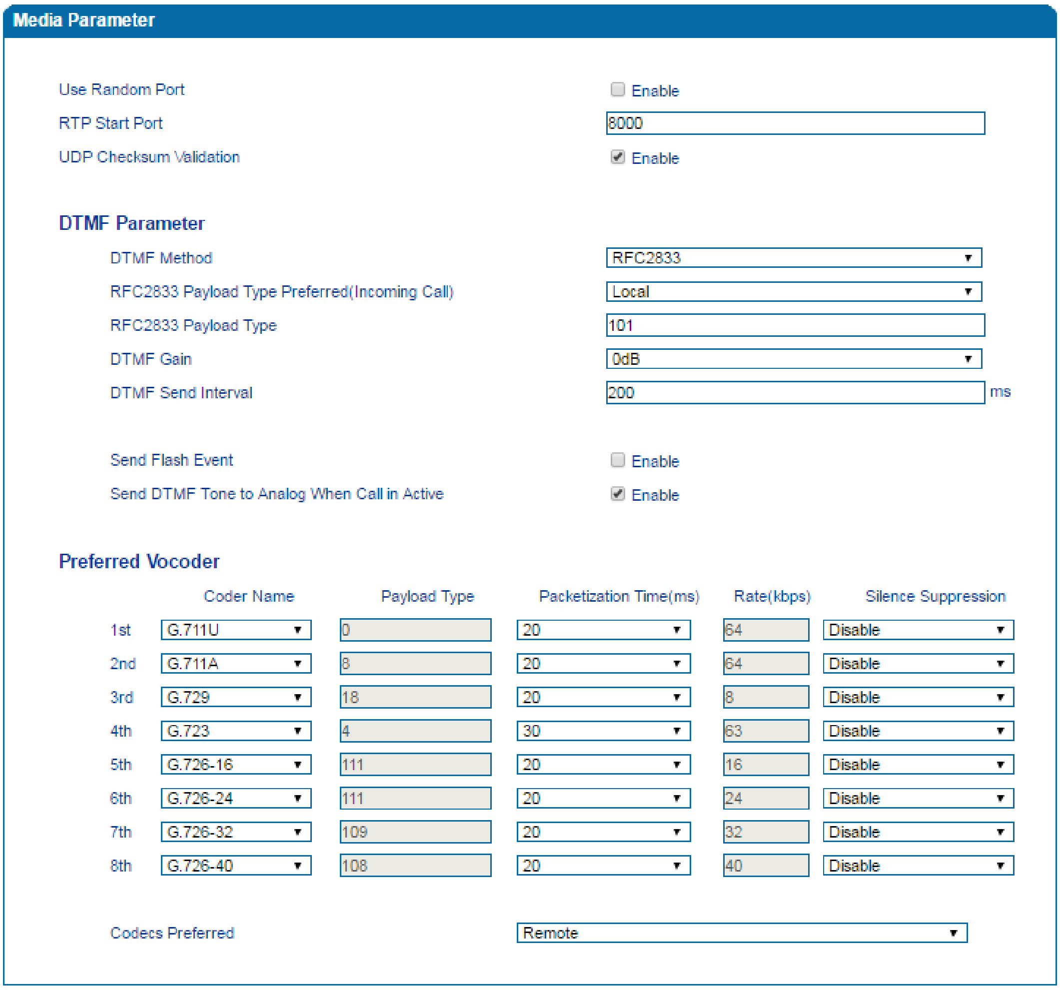


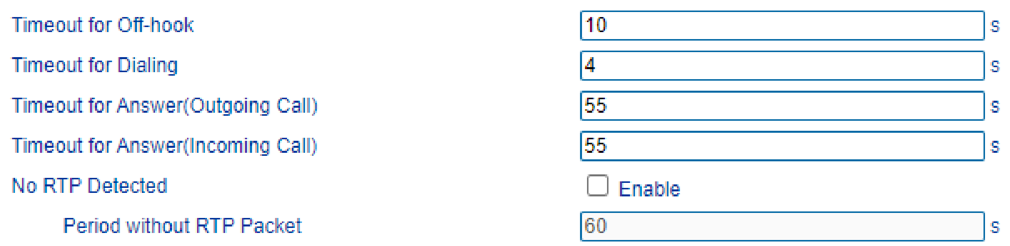
Table 4-6 Explanation of Media Parameters

Use Random Port	If this parameter is enabled, the DAG2000 device will choose a port by random as the start port for RTP.
RTP Start Port	When 'Use Random Port' is not selected, you need to configure a start port for RTP. Default RTP start port is 8000

UDP Checksum Validation	Choose whether to enable header checksum of UDP
DTMF Method	Include SINGAL, INBAND and RFC2833
RFC2833 Payload Type Preferred (Incoming Call)	For an incoming call, choose local or remote RFC2833 payload type as the preferred payload type
RFC2833 Payload Type	Local payload value, default value is 101
DTMF Gain	Default value is 0 DB
DTMF Send Interval	The interval for sending DTMF signal. The default value is 200ms.
Send Flash Event	If this parameter is enabled, the DAG2000 device will send flash-hook event to remote terminal, and thus user does not need to handle it locally
Send DTMF Tone to Analog When Call in Active	If this parameter is enabled, DTMF tone will be sent to analog phone when there is a call
Coder Name	The device supports G.729, G.711U, G.711A, G.723, G.726-16/24/32/40. When outgoing calls are made, G.729 will be used.
Payload Type	Each kind of coding has a unique load value, refer to RFC3551.
Packetization Time	The time for voice packaging
Rate	Voice data flow rate; It is defaulted by system.
Silence Suppression	Default value is 'disabled'. If this parameter is enabled, VoIP transmission bandwidth can be saved, and meanwhile network congestion can be avoided.
Codecs Preferred	Choose local or remote codec as the preferred codec

4.9.4 Service Parameter

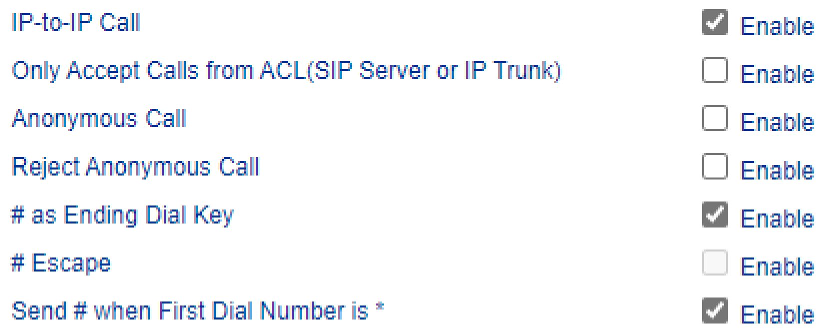
Service parameters include tiemout for dialing, digitmap,MWI message and so on.



Copyright©2011-2020 Dinstar

Timeout for off-hook	Mainly used to define a timer that when the user is off hook an analog phone without dial any digits
Timeout for dialing	With the help of dialing timeout, you can limit the time between two digits while users are typing the digits of a number through an extension. If the timeout expires, the gateway will consider the dialing has finished and will try to send message to SIP server. Default value is 4 seconds.
Timeout for answer(Outgoing call)	This parameter determines how long the caller party will wait for answer when making outgoing calls through a phone.
Timeout for answer(Incoming call)	This parameter determines how long the phone rings when there are incoming calls
No RTP Detected	If this parameter is enabled, the situation will be detected when there is no RTP packets received during the set time period.
Period without RTP Packet	The time period when there is no RTP packets received.

SUBSCRIBE for MWI (Message Waiting Indicator)	MWI is aimed to notify user that there is new voicemail. It is realized in the way of NOTIFY.
MWI Subscription Expires	The expiry time of MWI subscription; Default value is 3600s.
Voicemail User ID	The user ID used to access to voicemail
Visual MWI Type	There are two visual MWI Type, namely NEON and FSK

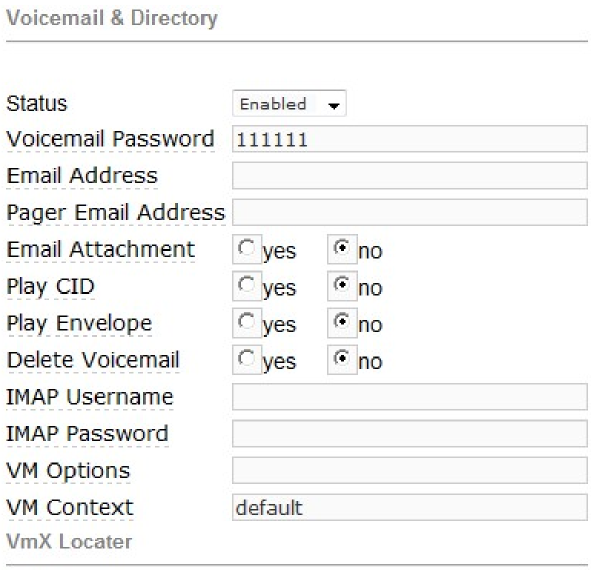


IP-to-IP Call	If this parameter is enabled, user can dial IP address through a phone to call destination gateway.
Only Accept Call from ACL (SIP server or IP Trunk)	If this parameter is enabled, the device only accepts incoming call from SIP server only. Default value is 'not enable'.
Anonymous Call	If this parameter is enabled, 'anonymous' will be included in SIP message.
Reject Anonymous Call	If this parameter is enabled, all anonymous calls will be rejected. Default value is 'not disable'.
# as ending Dial Key	If this parameter is enabled, '#' is used as the end mark for dialing.
# Escape	If this parameter is enabled, '#' is considered as a digit of the number that is dialed.
Send '#' when First Dial Number is '*'	If this parameter is enabled, '#' will be sent when first dialed digit is '*'.

Voicemail instructions:

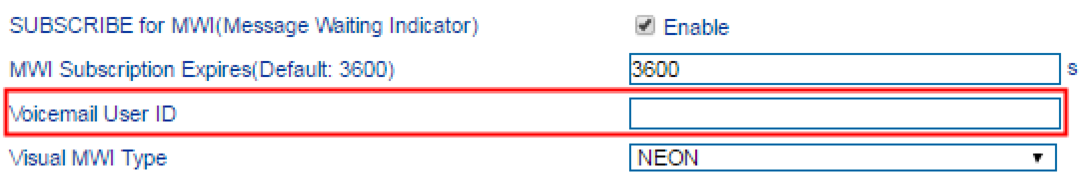
Here takes the DAG2000-32S device together with Elastix as the example to introduce how voicemail works in the device.

(1) After the device registers to Elastix server, enable the voicemail function in Elastix for the corresponding extension number and then set password. As below:

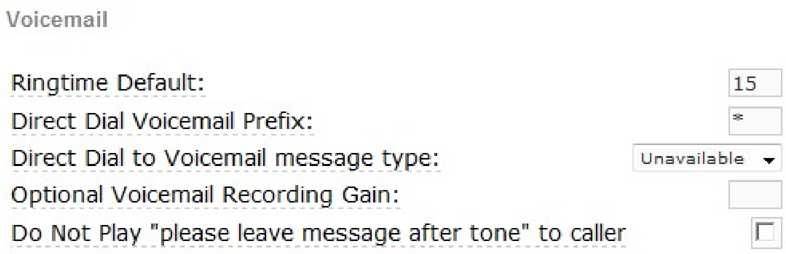


(2) Check feature code in Elastix and change it if necessary. Its default feature code setting is as follows:

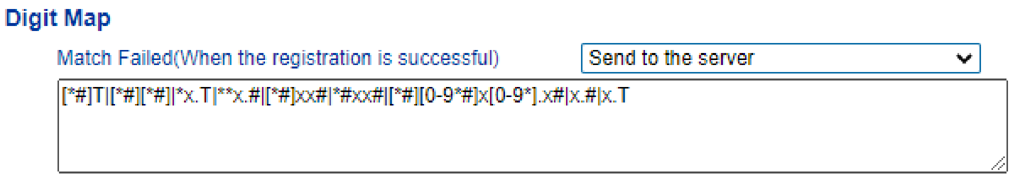
(3) On the Web interface of DAG2000-32S, click **Advanced → SIP Parameter** in the navigation tree and then enter voicemail User ID.



(4) Set ringing time in Elastix. Elastix will prompt user to leave a message after the corresponding extension rings 15 seconds (by default). Then the Elastix sever will record the message. Related setting is shown as follows:



(5) Dial *200# on the extension which is connected to DAG2000-32S, and then dial voicemail user ID and password for authentication. After that user will hear voice message.



Digitmap is used for number dialing of calls through FXS ports of the DAG2000 device.

Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *
Range	[ ]	One or more DTMF symbols enclosed in the [], but only one DTMF symbol can be selected
Range	()	One or more expressions enclosed the (), but only one can be selected
Separator	|	Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by hyphen (-) which matches any digit between and including the two digits.
Wildcard	x	Matches any digit of 0 to 9
Modifiers	.	Matches 0 or more times of the preceding element
Modifiers	?	Matches 0 or 1 times of the preceding element

4.9.5 SIP Parameter

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

Figure 4-17 Configure SIP Parameters

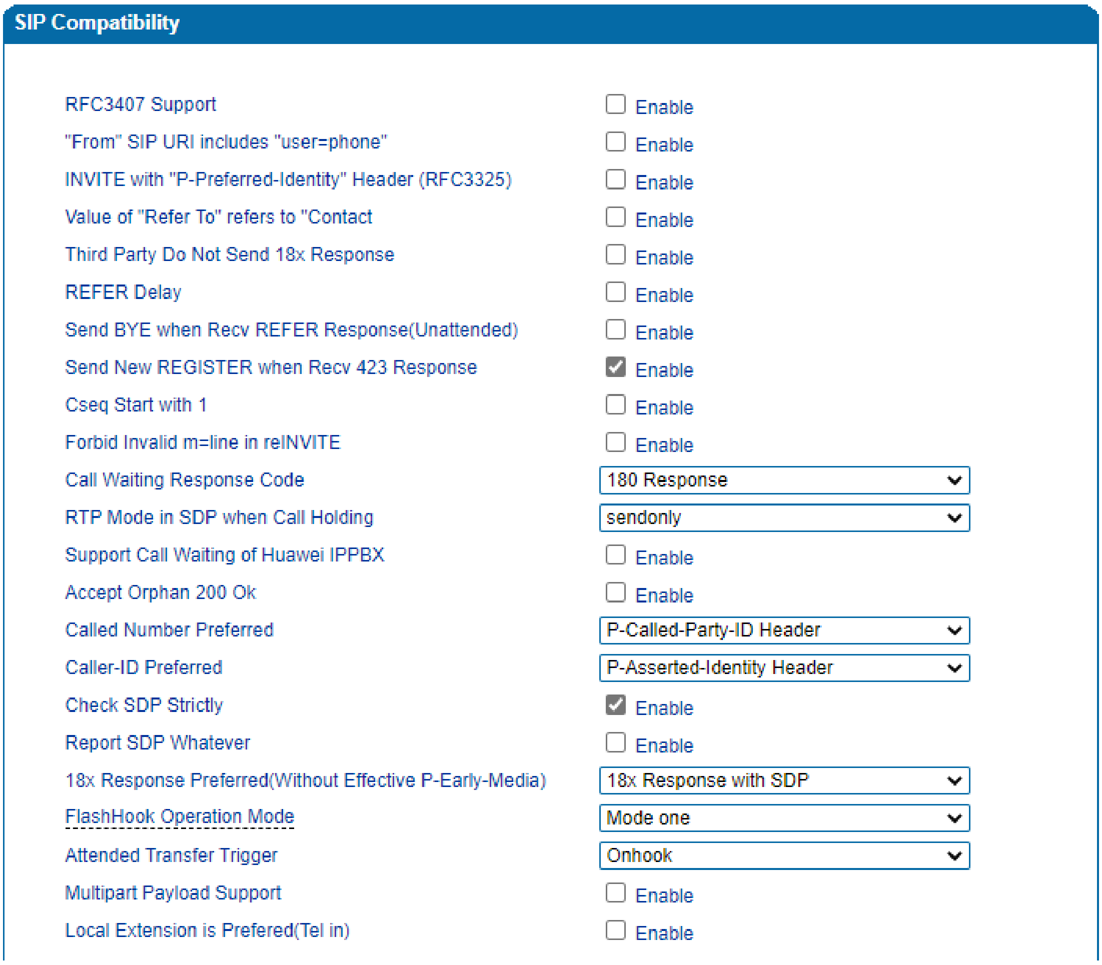


Table 4-7 Explanation of SIP Parameters

RFC3407 Support	Whether to enable RFC3407 support. If this parameter is enabled, the device will support RFC3407 which defines the SDP capability of backward compatibility.
URI Includes "user=phone"	If this parameter is enabled, 'user=phone' will be contained in URI. When calls are routed to PSTN network, the called number will be got from user name. Default value is 'not enable'.
INVITE with "P-Preferred-Identity" Header (RFC3325)	If this parameter is enabled, "P-Preferred-Identity" header will be added in INVITE message for anonymous call (Support RFC3325).
Only Accept Call from ACL (SIP server or IP Trunk)	If this parameter is enabled, the device only accepts incoming call from SIP server only. Default value is 'not enable'.
Value of "Refer To" refers to	If this parameter is enabled, 'contract header' needs to be

"Contact"	filled in in the 'refer to' field of a SIP message.
Third Party Do Not Send 18x Response	If this parameter is enabled, the third party will not send 18x response during an attended transfer.
Send BYE when Recv REFER Response (Unattended)	If this parameter is enabled, the third party will send BYE to release session after receiving REFER during a blind transfer.
Send New REGISTER when Recv 423 Response	If this parameter is enabled, the value of 'expires' header will be automatically updated and REGISTER will be re-sent after receiving of 423 response.
CSeq Start with 1	If this parameter is enabled, the value of CSeq starts with '1'.
Forbid Invalid m=line in reINVITE	If this parameter is enabled, the device will prevent 'invalid m=line' from being carried in the SDP of re-INVITE.
Call Confirm Tone	If this parameter is enabled, ring-back tone will be played when a call does not receive 180x response.
Call Waiting Response Code	User can choose 180 or 182 as call waiting response code
RTP Mode in SDP when Call Holding	Use 'send only' or 'inactive' as RTP mode during call holding.
Support Call Waiting of Huawei IPPBX	If this parameter is enabled, the device will support call waiting of Huawei IPPBX.
Accept Orphan 200 OK	If this parameter is enabled, the DAG2000 device will support different 'to-tag 200 OK' in an INVITE session.
Called Number Preferred	Choose P-Called-Party-ID header or Request-Line
Caller-ID Preferred	Choose P-Asserted-Identity header or From Header
Report SDP Whatever	If this parameter is enabled, SDP will be reported anytime
18x Response Preferred	Choose '18x Response with SDP', 'Last 18x Response' or 'Local Ring Tone Only'
Flashhook Operation Mode	Choose Mode one, Mode two or Mode three
Attended Transfer Trigger	Choose 'Onhook' or 'Flashhook +4'

Figure 4-18 Configure Default SIP Parameters & Early Media

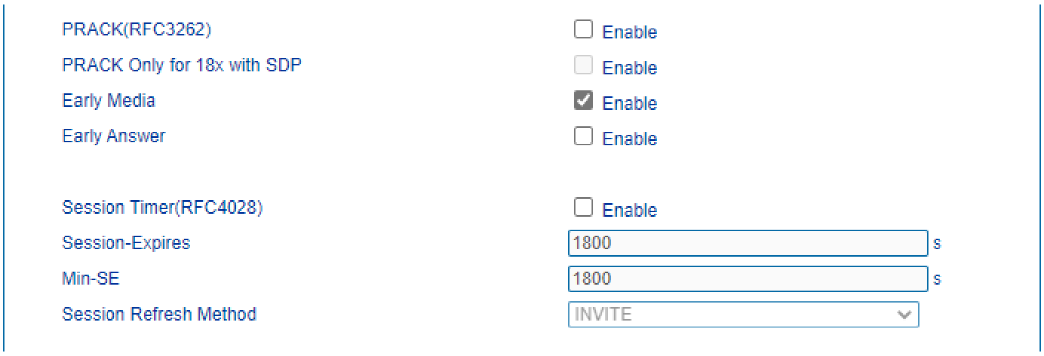


Table 4-8 Explanation of Default SIP Parameters & Early Media Parameters

Domain Query Type	There are two modes: A QUERY and SRV QUERY. Default is 'A QUERY'.
Domain Re-resolution Interval	The interval for re-parsing domain name. Range is from 0 to 3600s. Default value is 0, which means no re-parsing.
DNS cache	If this parameter is enabled, the DAG2000 device will cache the DNS query results.
PRACK(RFC3262)	If this parameter is enabled, the DAG2000 device supports reliable transmission of provisional response
PRACK Only for 18x with SDP	If this parameter is enabled, only PRACK will be sent when there's SDP in 18x response
Early Media	If this parameter is enabled, the DAG2000 device supports the receiving of Early Media.
Early Answer	If this parameter is enabled, the DAG2000 device supports early answer
Answer Update without Offer (for Port Group)	If this parameter is enabled, the system will update answer proactively although no offer is received.
Session Timer (RFC4028)	Whether to enable 'session timer', default value is 'not enable'.
Session-Expires	The interval for refreshing session; default value is 1800s. The Session-Expires header field conveys the session interval for a SIP session.
Min-SE	The minimum interval for refreshing session; default value is 1800s. The Min-SE header field indicates the minimum value for the session interval.
Session Refresh Method	The method to refresh session; default value is INVITE.

Figure 4-19 Configure Timer in SIP Protocol

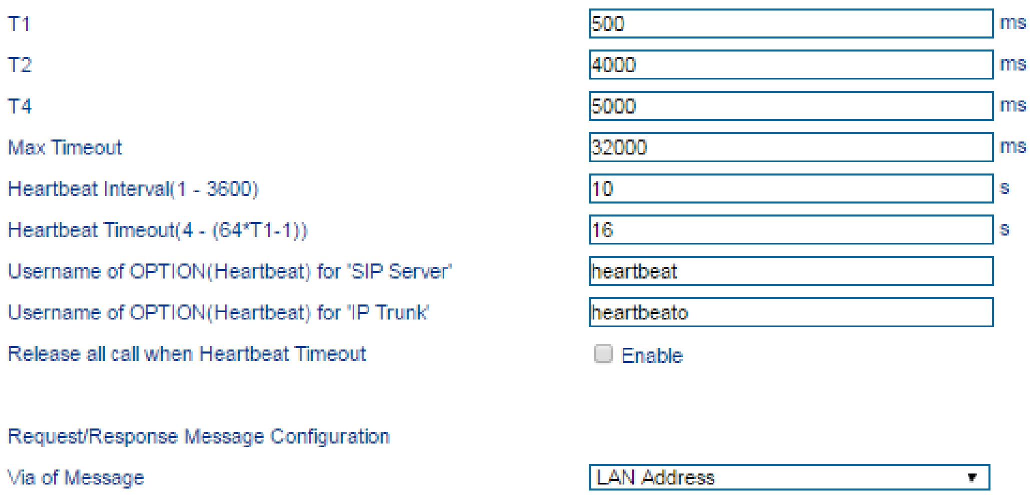
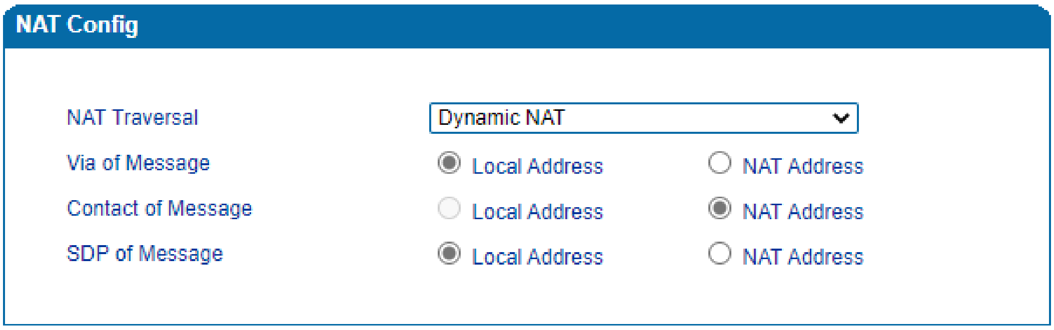


Table 4-9 Explanation of Timer Parameters in SIP Protocol

T1	Value of T1 timer in SIP protocol, default is 500ms
T2	Value of T2 timer in SIP protocol, default is 4000ms
T4	Value of T4 timer in SIP protocol, default is 5000ms
Max Timeout	The max timeout of sending or receiving SIP messages, default is 32000ms
Heartbeat Interval	The interval for sending heartbeat message, Default is 10s.
Heartbeat Timeout	The timeout for heartbeat message to be sent, default to 16s
Username of OPTION(Heartbeat) for “SIP Server”	The user ID part of OPTION SIP message in the heartbeat request for SIP server
Username of OPTION(Heartbeat) for “IP TRUNK”	The user ID part of OPTION SIP message in the heartbeat request for IP trunk
Via of Request/Response Message	Choose ‘LAN address’ or ‘WAN address’ to be carried in the ‘Via’ header of request/response message

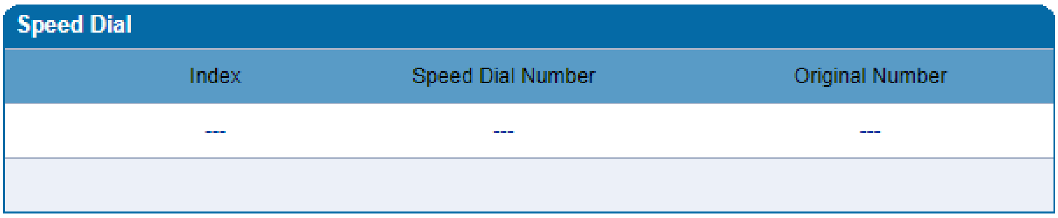
4.9.6 NAT Parameter



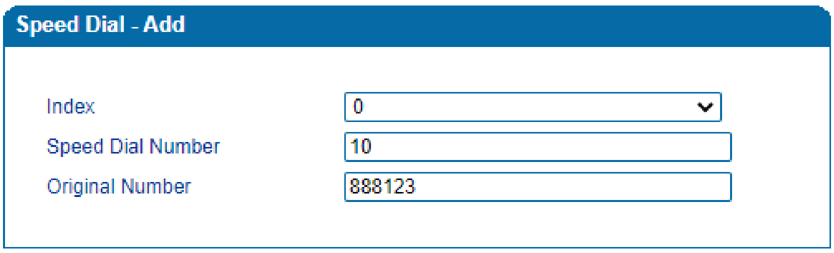
NAT Traversal (Network Address Translator Traversal) is a computer networking technique of establishing and maintaining Internet protocol connections across gateways that implement network address translation (NAT). NAT breaks the principle of end-to-end connectivity originally envisioned in the design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

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

4.9.7 Speed dial



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



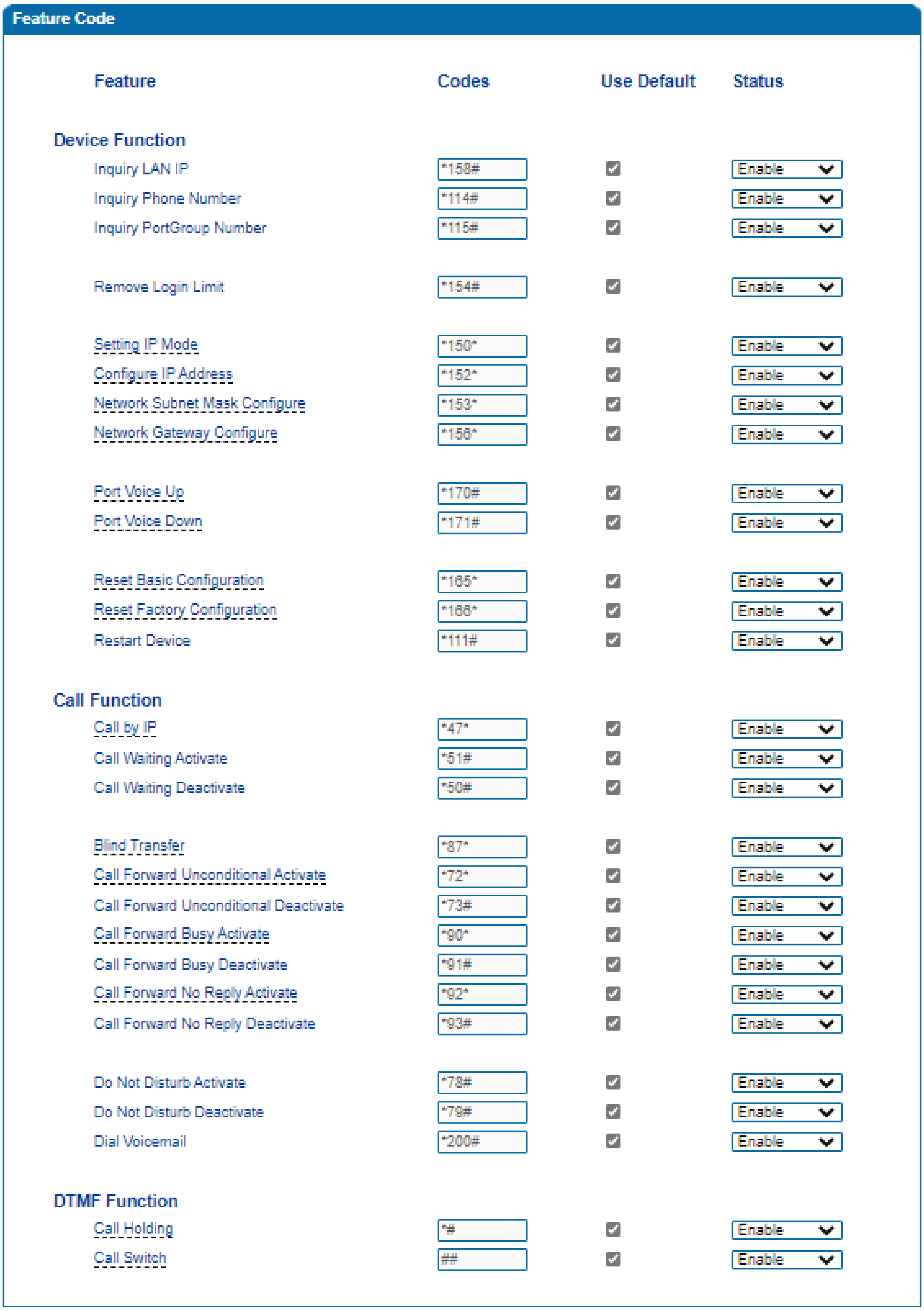
Copyright©2011-2020 Dinstar

Speed Dial

	Index	Speed Dial Number	Original Number
☐	0	10	888123

Total: 1 Entry

4.9.8 Feature Code



Feature Code

Feature	Codes	Use Default	Status
Device Function			
Inquiry LAN IP	*158#	☑	Enable
Inquiry Phone Number	*114#	☑	Enable
Inquiry PortGroup Number	*115#	☑	Enable
Remove Login Limit	*154#	☑	Enable
Setting IP Mode	*150*	☑	Enable
Configure IP Address	*152*	☑	Enable
Network Subnet Mask Configure	*153*	☑	Enable
Network Gateway Configure	*156*	☑	Enable
Port Voice Up	*170#	☑	Enable
Port Voice Down	*171#	☑	Enable
Reset Basic Configuration	*165*	☑	Enable
Reset Factory Configuration	*166*	☑	Enable
Restart Device	*111#	☑	Enable
Call Function			
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
DTMF Function			
Call Holding	*#	☑	Enable
Call Switch	##	☑	Enable

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

4.9.9 System Parameter

System parameters include NTP, daylight saving time, daily reboot time, web parameter, telnet parameter and remote management.

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

Figure 4-20 Configure System Parameters

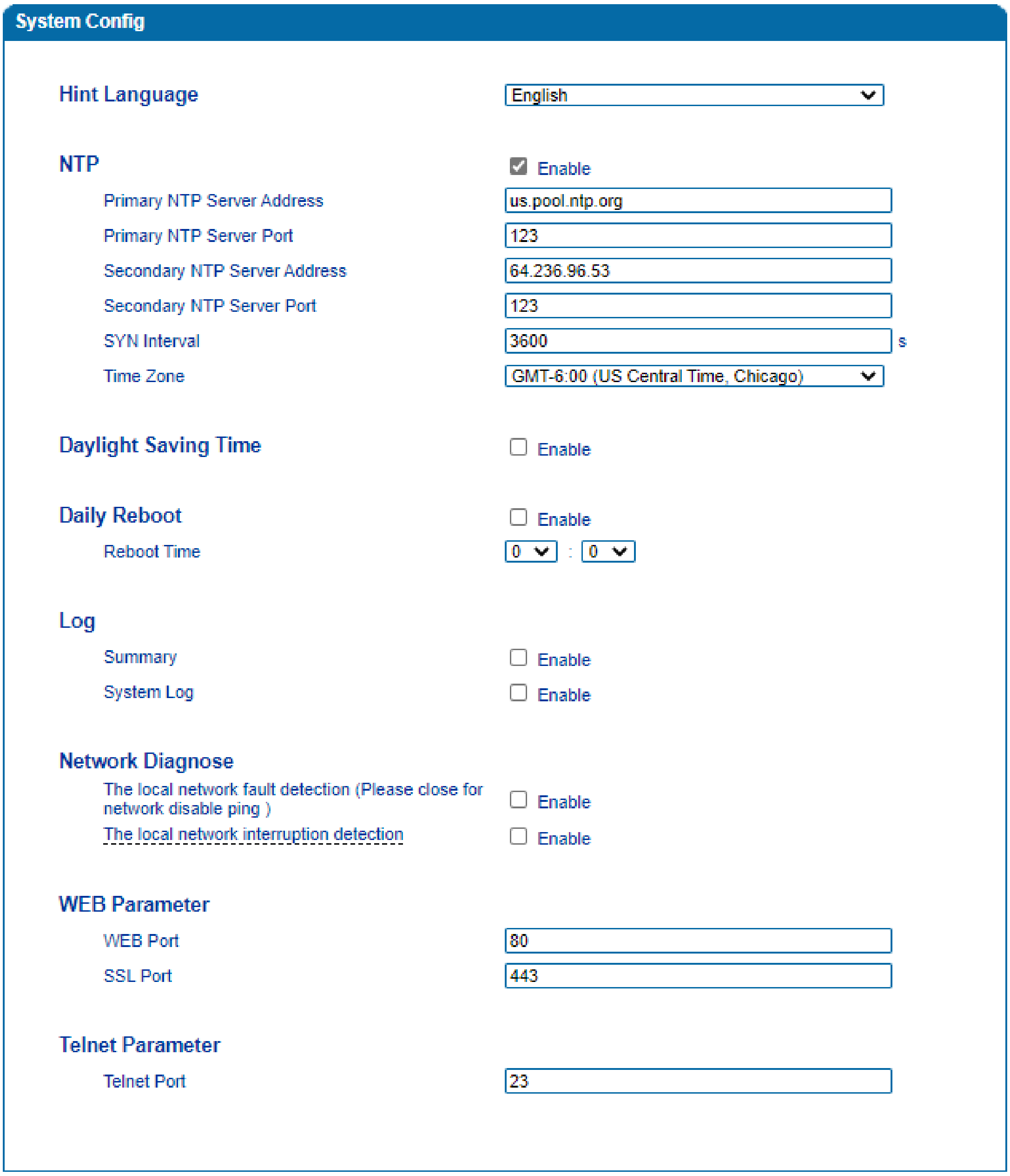


Table 4-10 Explanation of System Parameters

NTP	To enable or disable NTP
Primary NTP server address	The IP address of primary NTP server; default IP address is us.pool.ntp.org.
Primary NTP server port	The service port of primary NTP server; default port is 123.
Secondary NTP server address	The IP address of secondary NTP server ; Default IP address is 64.236.96.53

Secondary NTP server port	The service port of secondary NTP server; Default port is 123
SYN Interval	The interval to synchronize the time of the DAG2000-4S/8S. Default value is 3600s.
Time Zone	The time zone of the device; Default configuration is United States central time, Chicago.
Daylight Saving Time	Enable or disable daylight saving time
Daily Reboot	Whether to enable daily reboot
Reboot time	The time to reboot the device daily
WEB Port	The web port of the device; Default port is 80
SSL Port	The SSL port; Default is 443
Telnet port	Listening port of telnet service; Default port is 23

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

4.10 Call & Routing

4.10.1 Port Group

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

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

Figure 4-21 Add Port Group

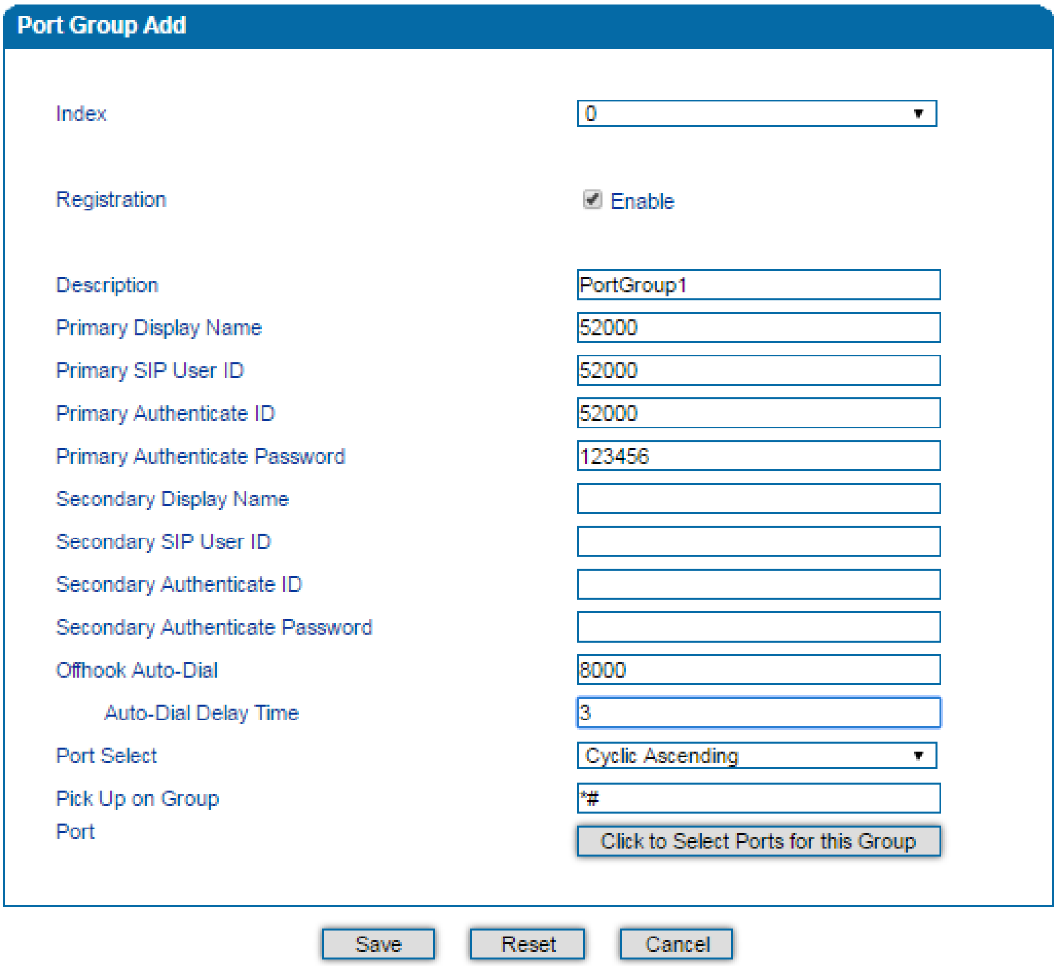


Table 4-11 Parameter Explanation of Port Group

Index	The NO. of the port group; It uniquely identifies a route.
Description	The description of the port group; it is used to identify the port group.
Primary/Secondary Display Name	Display name of the port group, which will be used in SIP message, for example: INVITE sip:bob@biloxi.com SIP/2.0 Via: SIP/2.0/UDPpc33.atlanta.com;branch=z9hG4bK776asdhds Max-Forwards: 70 To: Bob <sip:bob@biloxi.com> From: Alice <sip:alice@atlanta.com>;tag=1928301774 Here Bob and Alice is the display name
Primary/Secondary SIP User ID	User ID of this SIP account, which is provided by VoIP service provider (ITSP). It is usually in the form of digit similar to phone number or an actual phone number.

Primary/Secondary Authenticate ID	SIP service subscriber's ID for authentication; it can be identical to or different from SIP User ID.
Primary/Secondary Authenticate Password	SIP service subscriber's password for authentication
Offhook Auto-Dial	An extension or phone number is pre-assigned here so that the number is automatically dialed as soon as user picks up the phone
Auto-dial Delay time	How long auto-dialing will be delayed
Port Select	It specifies the policy for selecting a port for ringing in the port group • Ascending: the device always selects a port from the minimum number. • Cyclic ascending: the device always selects a port from a number next to the number selected last time. If the maximum number was selected last time, the next selected number is the minimum number. The sequence moves in cycles like this. • Descending: the device always selects a port from the maximum number. • Cyclic descending: the device always selects a port from a number next to the number selected last time. If the minimum number was selected last time, the next selected number is the maximum number. The sequence moves in cycles like this. • Group ring: all ports ring at the same time
Pickup UP on group	When one port rings, user can dial '*#' to pick up the call from other ports under the same port group.
Port	Select ports for this port group

4.10.2 IP Trunk

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

Figure 4-22 Configure IP Trunk

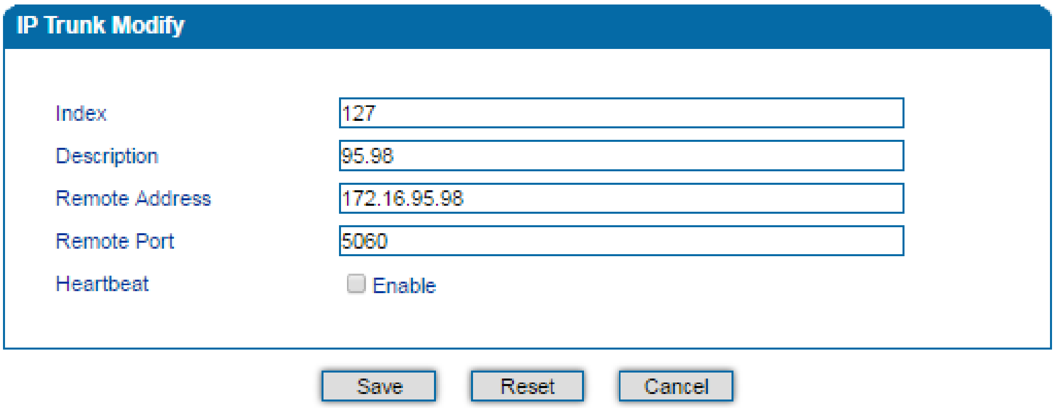


Table 4-12 Explanation of IP Trunk Parameters

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

4.10.3 Routing Parameter

Routing parameter determines a call is routed before or after manipulation.

Figure 4-23 Configure Routing Parameter

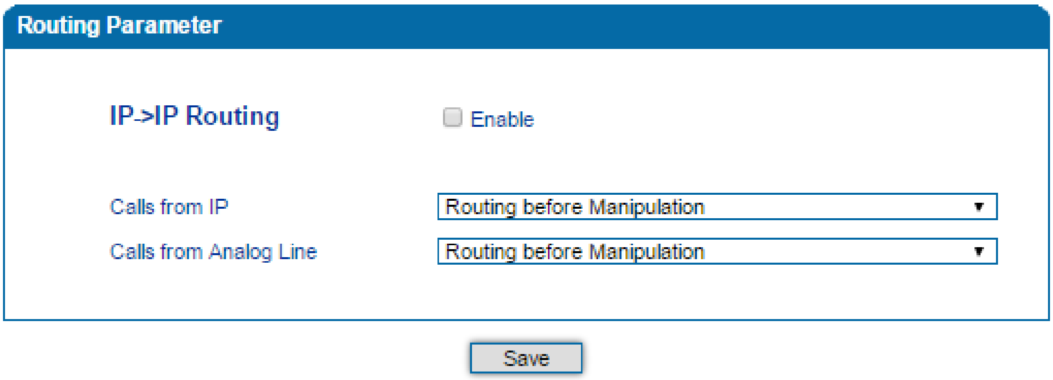


Table 4-13 Explanation of Routing Parameters

IP →IP Routing	Choose whether to enable IP → IP routing. If this parameter is enabled, calls from IP network will be routed to IP phones.

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

4.10.4 IP → Tel Routing

Calls from IP network can be routed to FXS port or port group of the DAG2000 device through IP →Tel routing.

Figure 4-24 Add IP →Tel Route

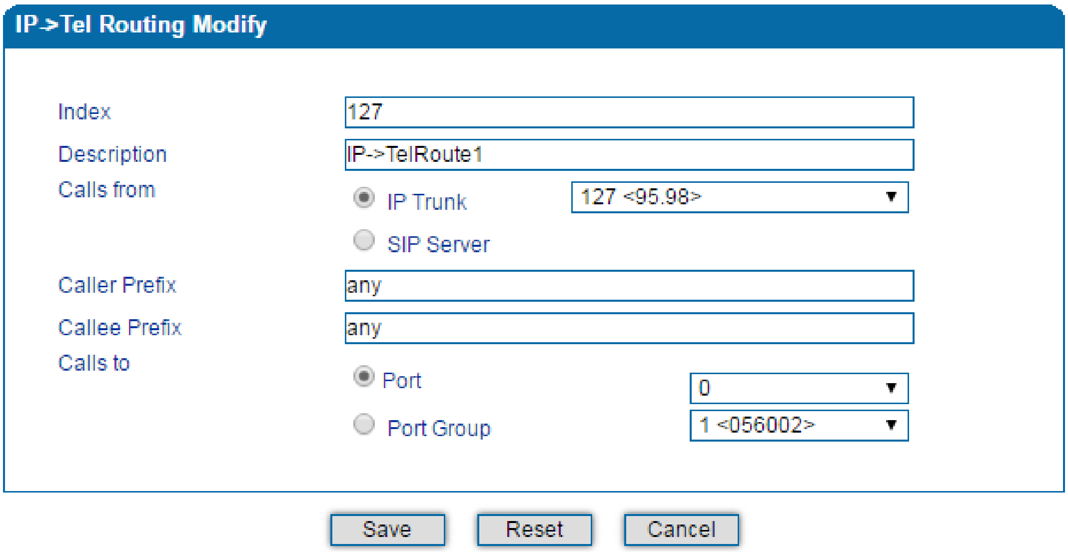


Table 4-14 Parameter Explanation of IP →Tel Routes

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

4.10.5 Tel → IP/Tel Routing

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

Figure 4-25 Add Tel →IP/Tel Route

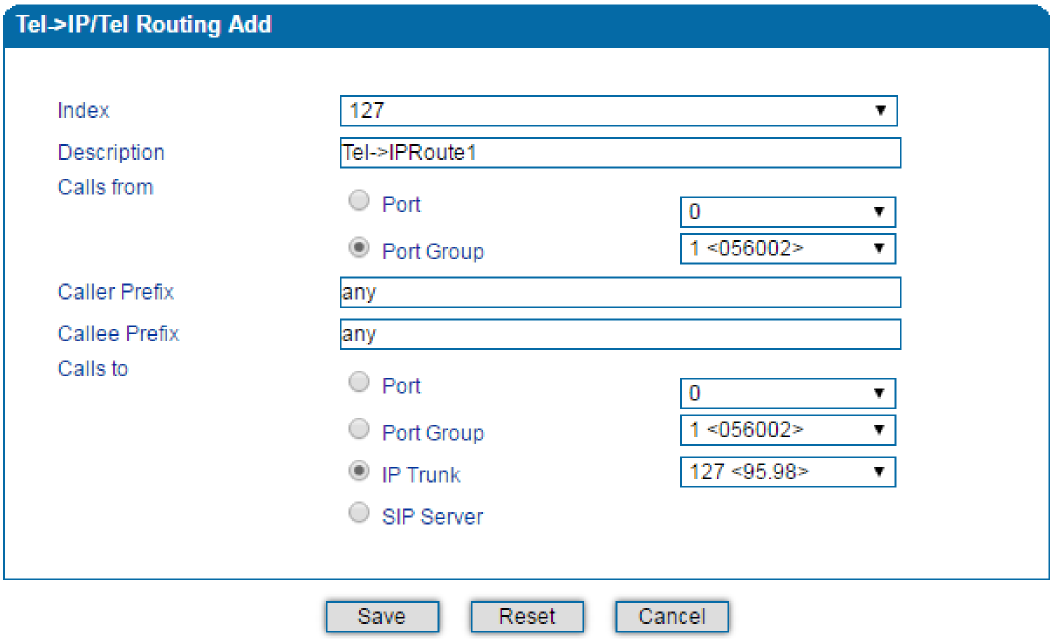


Table 4-15 Explanation of Tel →IP/Tel Route

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

4.10.6 IP → IP Routing

Calls from IP trunk can be routed to a different IP trunk through IP →IP routing. Configurations on this page won't take effect unless IP →IP routing has been enabled on the **Call & Routing →Routing Parameter** page.

Figure 4-26 Add IP →IP Route

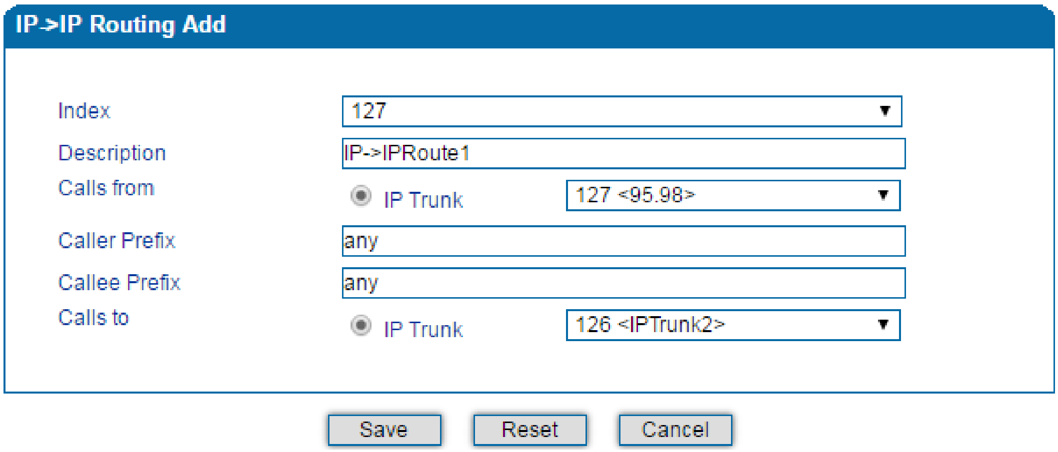


Table 4-16 Parameter Explanation of IP →IP Route

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

4.11 Manipulation

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

4.11.1 IP → Tel Callee

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

Figure 4-27 Add IP →Tel Called Number Manipulation

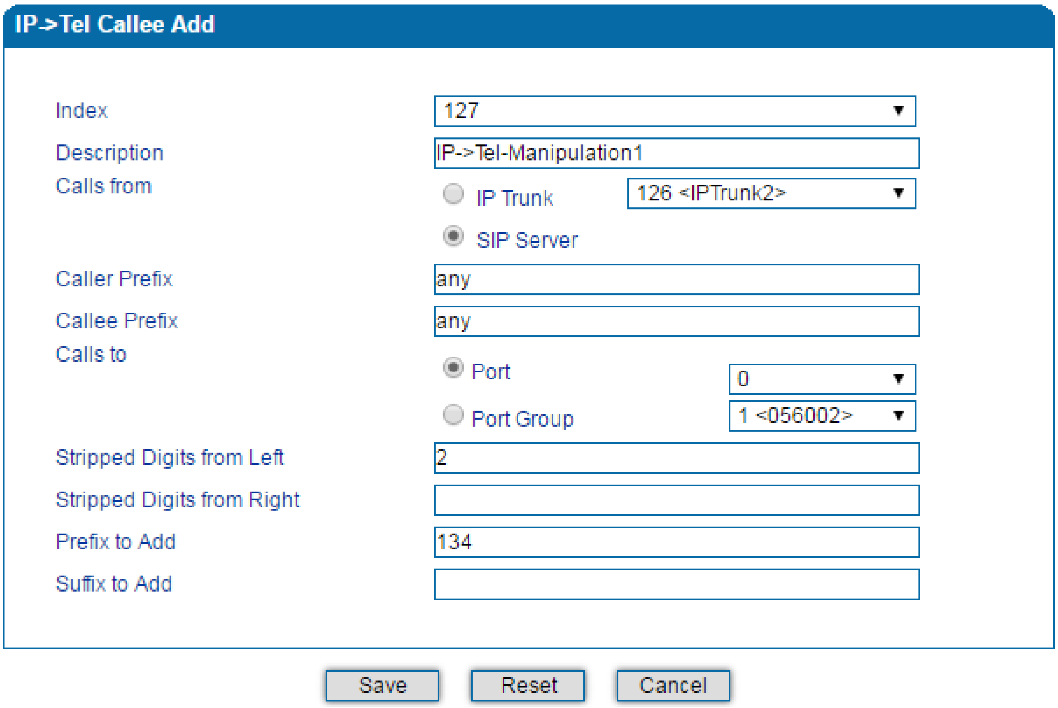


Table 4-17 Explanation of Parameters for IP →Tel Called Number Manipulation

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

Stripped Digits from Right	The number of digits which are lessened from the right of the called number
Prefix to Add	The prefix added to the called number after its digits are lessened.
Suffix to Add	The suffix added to the called number after its digits are lessened.

4.11.2 Tel → IP/Tel Caller

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

Figure 4-28 Add Tel → IP/Tel Caller Number Manipulation

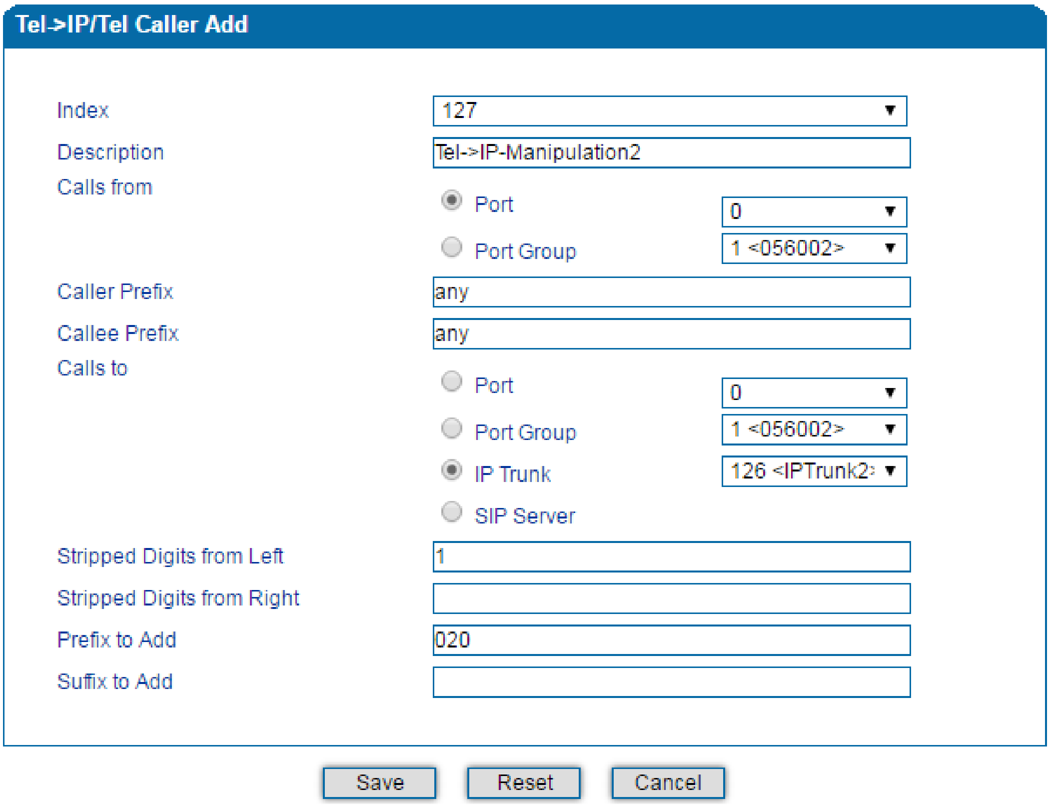


Table 4-18 Explanation of Parameters for IP →Tel Called Number Manipulation

Index	The index of this manipulation; range is from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Description of this manipulation; it is used to identify this manipulation.
Calls From	Determine the calls come from a port or a port group.
Caller Prefix	Set a prefix for caller number. The prefix's length is less than or equal to that of the caller number, which helps to match the caller number of this

	call. If caller number is 2001, the caller prefix can be 200 or 2. ‘any’ means match any caller number.
Callee Prefix	Set a prefix for called number. The prefix’s length is less than or equal to called number, which helps to match the called number. If called number is 008675526456659, the called prefix can be 0086755 or 00. ‘any’ means match any called number.
Calls to	Determine the call is routed to a port, a port group, an IP trunk or a SIP server.
Stripped Digits from Left	The number of digits which are lessened from the left of the caller number
Stripped Digits from Right	The number of digits which are lessened from the right of the caller number
Prefix to Add	The prefix added to the caller number after its digits are lessened.
Suffix to Add	The suffix added to the caller number after its digits are lessened.

4.11.3 Tel → IP/Tel Callee

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

Figure 4-29 Add Tel → IP/Tel Callee Number Manipulation

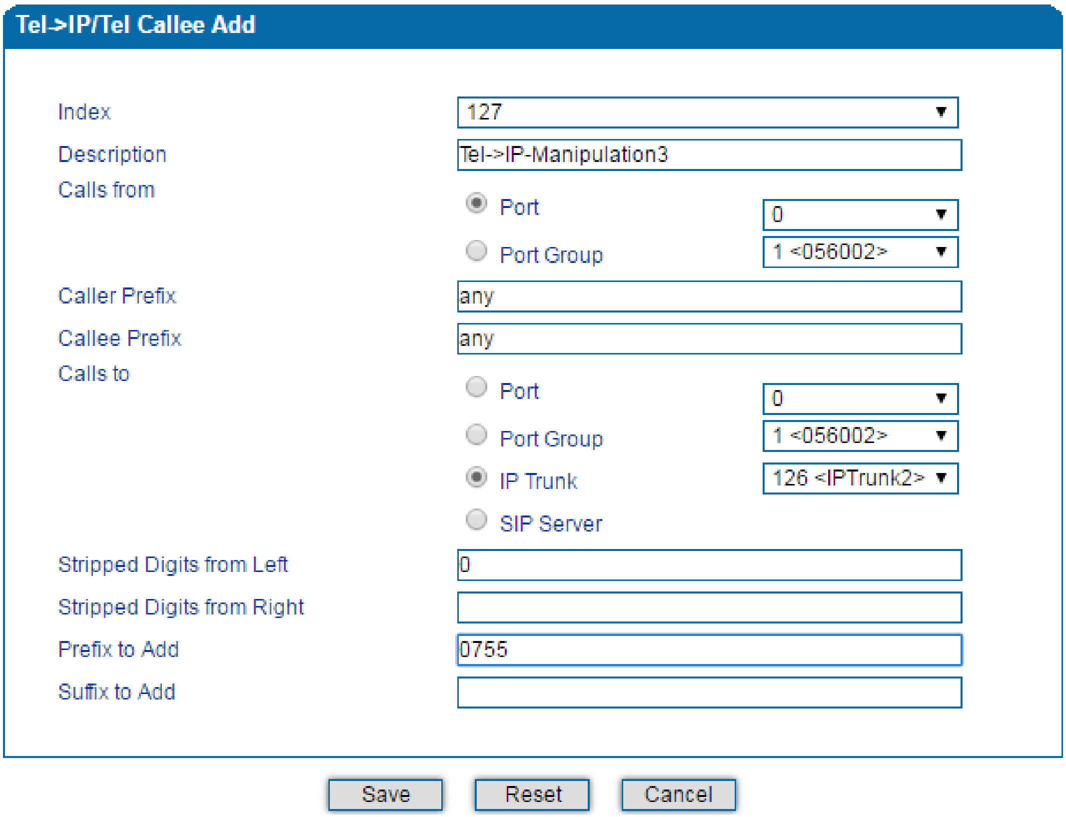


Table 4-19 Explanation of Parameters for Tel → IP/Tel Callee Number Manipulation

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

from Right	number
Prefix to Add	The prefix added to the called number after its digits are lessened.
Suffix to Add	The suffix added to the called number after its digits are lessened.

4.12 Management

4.12.1 TR069

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

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

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

Username and password are used for ACS authentication.

Figure 4-30 Configure TR069 Parameter

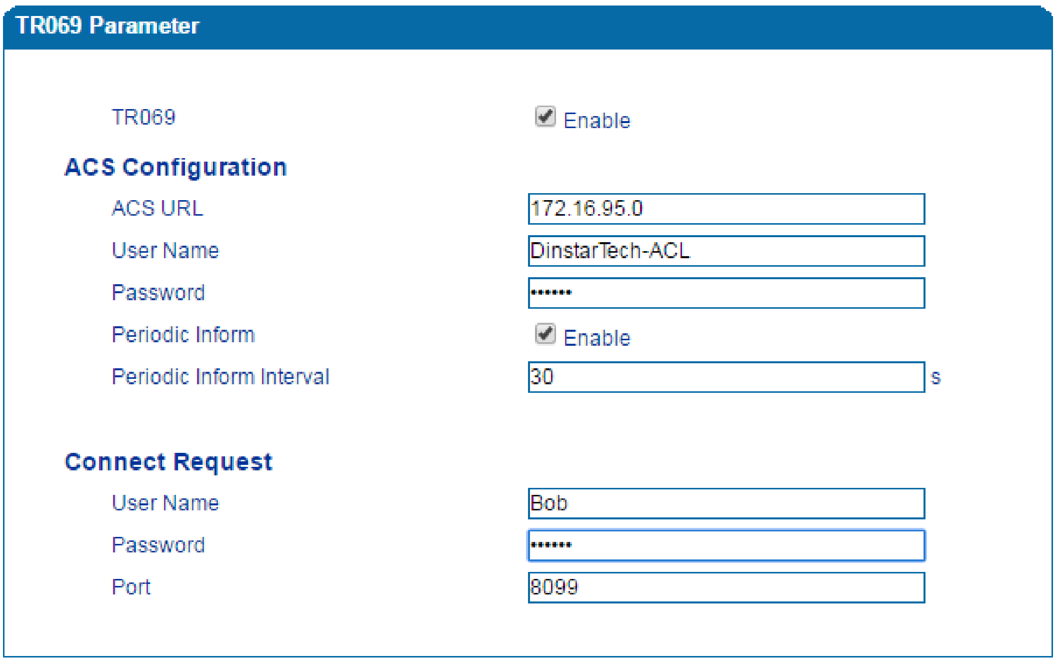


Table 4-20 Explanation of TR069 Parameters

TR069	Choose whether to enable TR069; it is ‘not enable’ by default.
ACS URL	The IP address or domain name of ACS, which is provided by service provider.

Username(ACS)	Username of ACS, which is provided by service provider.
Password(ACS)	Password of ACS, which is provided by service provider.
Periodic Inform	Choose whether to enable 'Periodic Inform'; if it is enabled, ACS will connect to CPE every 30 seconds (if the interval is set as 30 seconds).
Periodic Inform Interval	The interval set for periodic connection between ACS and CPE.
Username (CPE)	Username of CPE
Password (CPE)	Password of CPE
Port	The port to connect CPE and ACS

4.12.2 SNMP

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

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

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

Figure 4-31 Configure SNMP Parameters

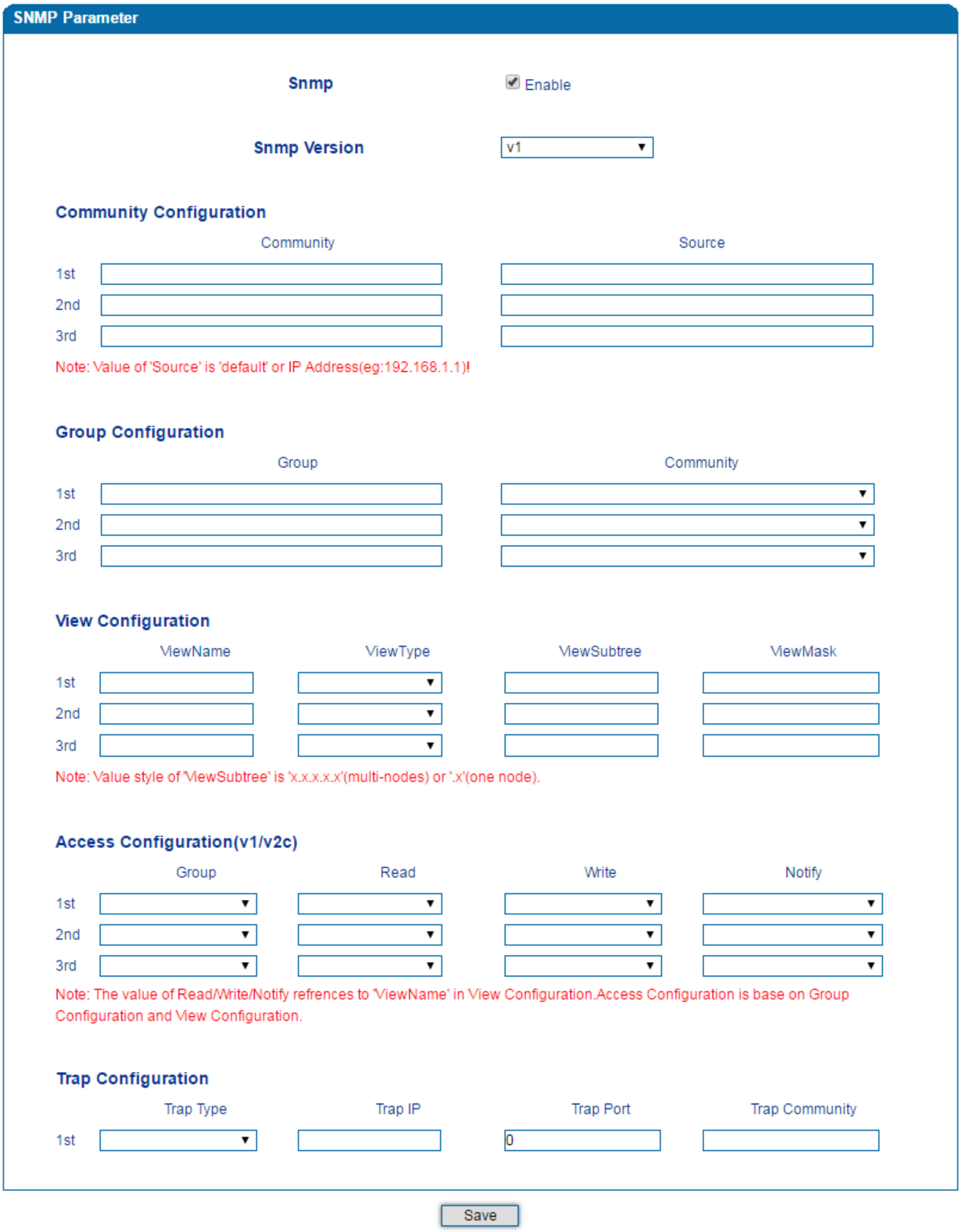


Table 4-21 Explanation of SNMP Parameters

SNMP	The DAG2000 device supports three versions of SNMP, namelyV1、V2C and V3.

Community Configuration	Community configuration exists in V1 and V2C. **Community:** fill in a community name used to read through SNMP protocol; it is a character string. **Source:** The IP address of SNMP server. SNMP server cannot identify the packets sent from DAG2000 unless the community configured in DAG2000 matches with the community configured in SNMP server.
Group Configuration	Group configuration exists in V1 and V2C and V3. **Group:** fill in a group name which is used to identify the group; it's a character string. **Community:** fill in a community which means this community has joined in the group. In the following, access permission of read, write and notify is configured for each group.
View Configuration	View configuration exists in V1, V2C and V3. **ViewName:** fill in a view name which is used to identify this view. **ViewType:** choose 'Included' or 'Excluded'. 'Included' means the view includes the OID of the corresponding ViewSubtree, while 'Excluded' means the OID of the corresponding ViewSubtree is excluded from this view. **ViewSubtree:** fill in the OID of the view subtree. **ViewMask:** it is used to withdraw a row of a table, such as an Ethernet port.
Access Configuration	Access configuration exists in V1, V2C and V3, under which permission of read, write or notify is configured for a community group. **Group:** choose a group name that has been configured. **Read:** Choose a 'read' view for the group. **Write:** Choose a 'write' view for the group. **Notify:** Choose a 'notify' view for the group.
Trap Configuration	Trap configuration exists in V1, V2C and V3, which is aimed to send trap alarm. **Trap Type:** Choose V1, V2C and Inform. **Trap IP:** the IP address of the destination SNMP server where trap alarm is sent. **Trap Port:** the port of the destination SNMP server, which will receive trap alarm. **Trap Community:** the community configured in the destination SNMP server.
User Configuration	User configuration exists in V3. When V3 transmits SNMP packets in an encryption way, this item needs to be configured. **User:** fill in a user name used to authenticate. **AuthType:** choose MD5 or SHA as authentication type.

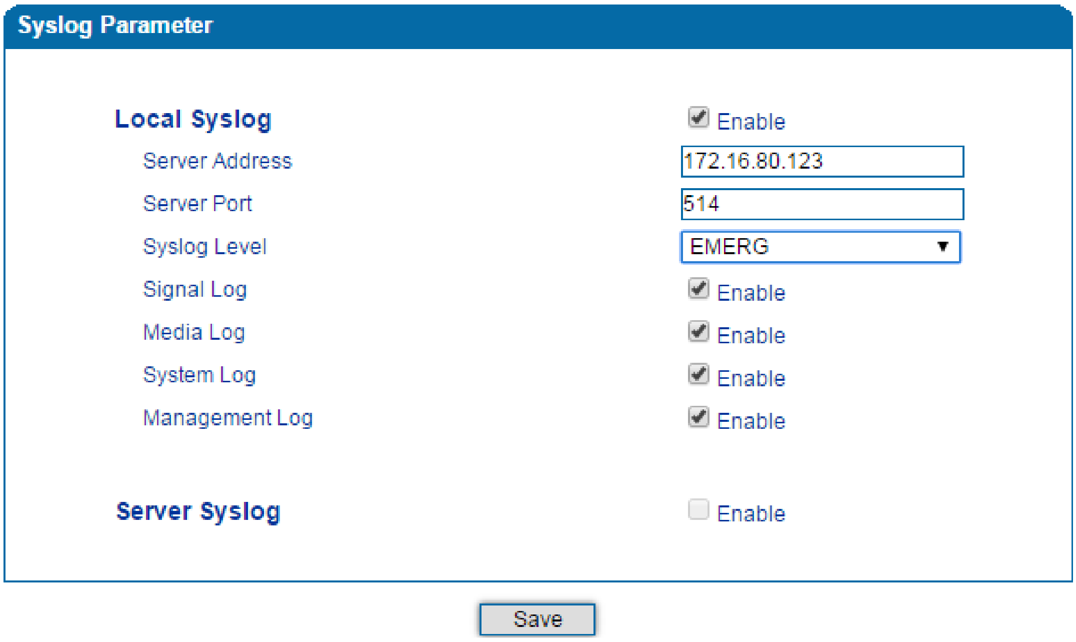
	AuthPassword: the password used to authenticate. **Privacy Type:** Choose DES, AES or AES 128 as encryption type. **Privacy Password:** the encryption password.

4.12.3 Syslog

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

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

Figure 4-32 Configure Syslog Parameters



When the DAG2000 device registers to SIM Cloud server, local syslog will be changed to non-configurable and all logs will be stored on the Cloud server.

4.12.4 Provision

Provision is used to make the DAG2000 device automatically upgrade with the latest firmware stored on an http server, an ftp server or a tftp server. Please refer to the Instruction for Using Provision.

Figure 4-33 Provision

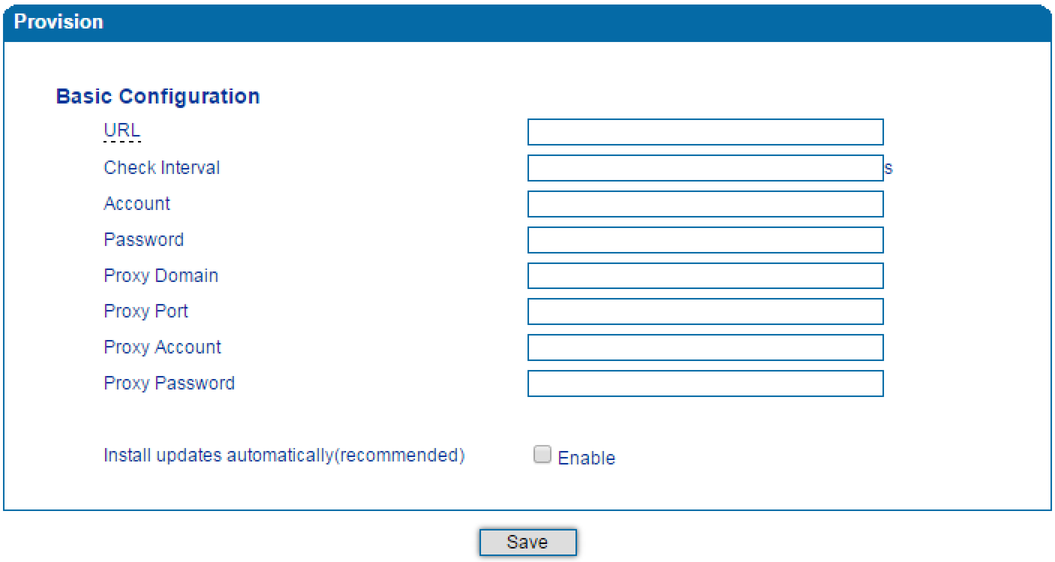


Table 4-22 Explanation of Provision Parameters

URL	URL of provisioning server, support HTTP, TFTP, FTP
Check Interval	The interval to check whether there is new firmware version on the provisioning server
Account	Account for logging in provisioning server
Password	Password for logging in provisioning server

4.12.5 Cloud server

You can register the DAG2000 device to cloud server, and then the device can be managed by the cloud server.

Figure 4-34 Configure Cloud Server

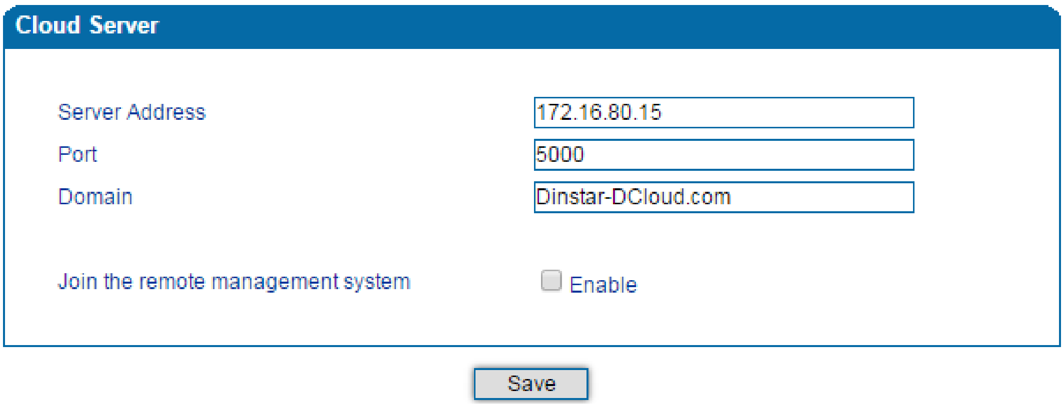


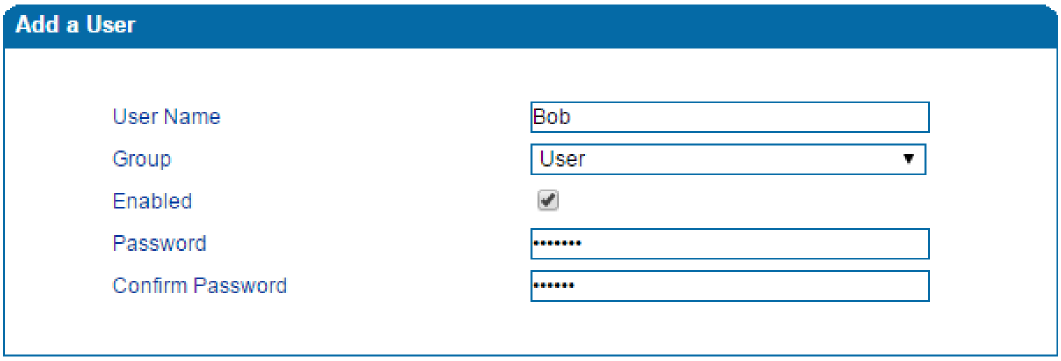
Table 4-23 Explanation of Parameters for Cloud Server

Server Address	The IP address of the cloud server
Port	The listening port of the cloud server
Domain	The domain name of the cloud server
Join the remote management system	Choose whether to join the remote management system of the cloud server.

4.12.6 User Manage

On the **Management → User Manage** page, the administrator of the DAG2000 device can classify users in different groups, and set login username and password for each user.

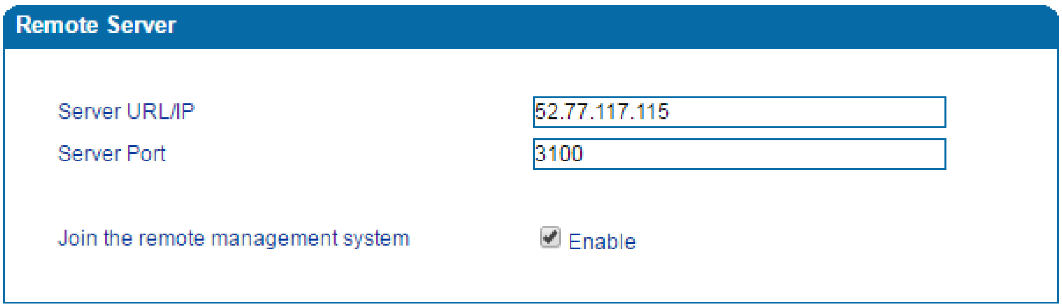
Figure 4-35 Modify Username and Password



4.12.7 Remote Server

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

Figure 4-36 Configure Remote Server

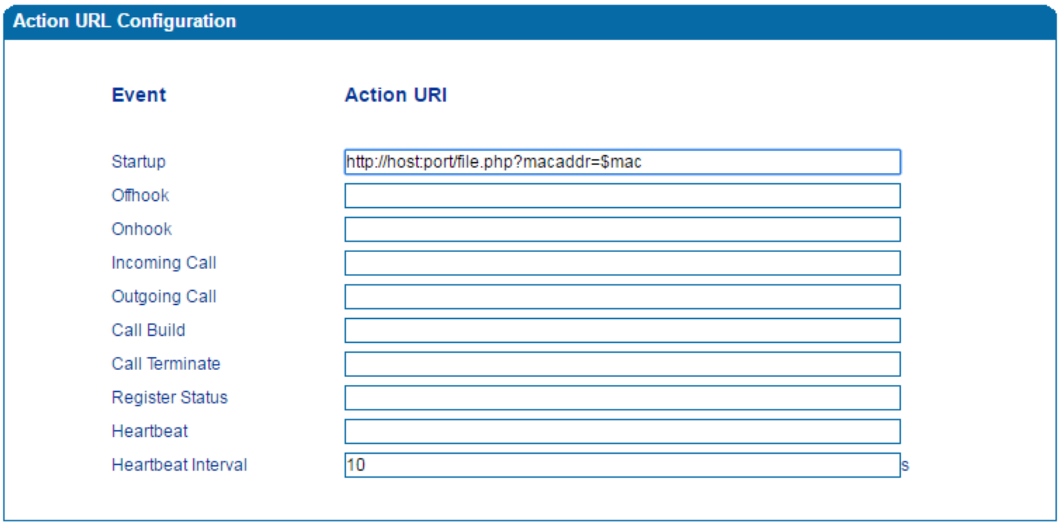


4.12.8 Action URL

Action URL is a means of allowing VoIP platform/VoIP server to learn about the statuses of the DAG2000 device. This is realized by GET request over the HTTP protocol. During the transmission of status, some data (such as device ID, mac address, called/caller number, IP address) carried in GET request can also be reported to VoIP platform/VoIP server.

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

Figure 4-37 Configure Action URL



Event: Statuses of DAG2000 device, which will be reported to VoIP platform/VoIP server.

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

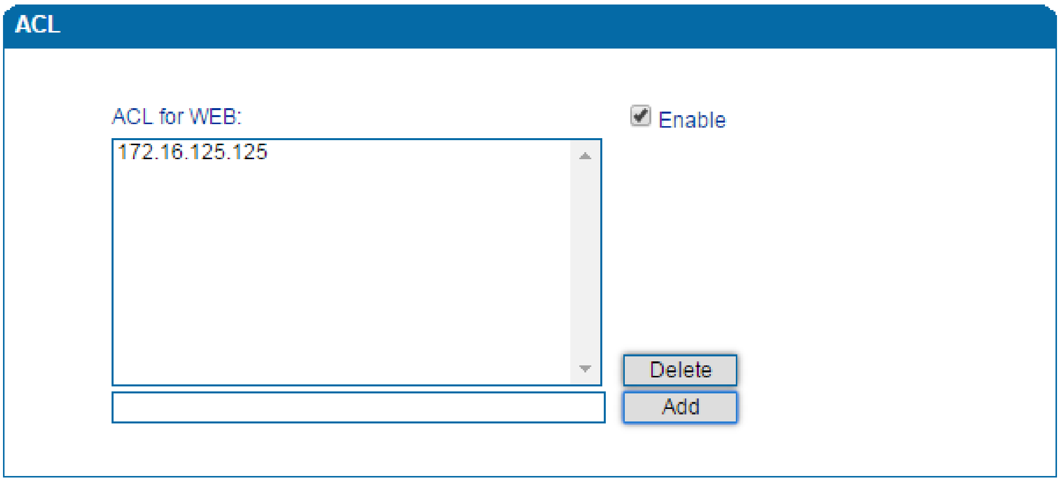
Heartbeat: heartbeat packets are sent to URL by the DAG2000 device, used to examine the connection between the DAG2000 device and HTTP/HTTP server.

4.13 Security

4.13.1 WEB ACL

ACL (Access Control List) for Web is used to configure IP addresses that are allowed to access the Web Interface of the DAG2000 device. The IP address list can't be null once ACL is enabled.

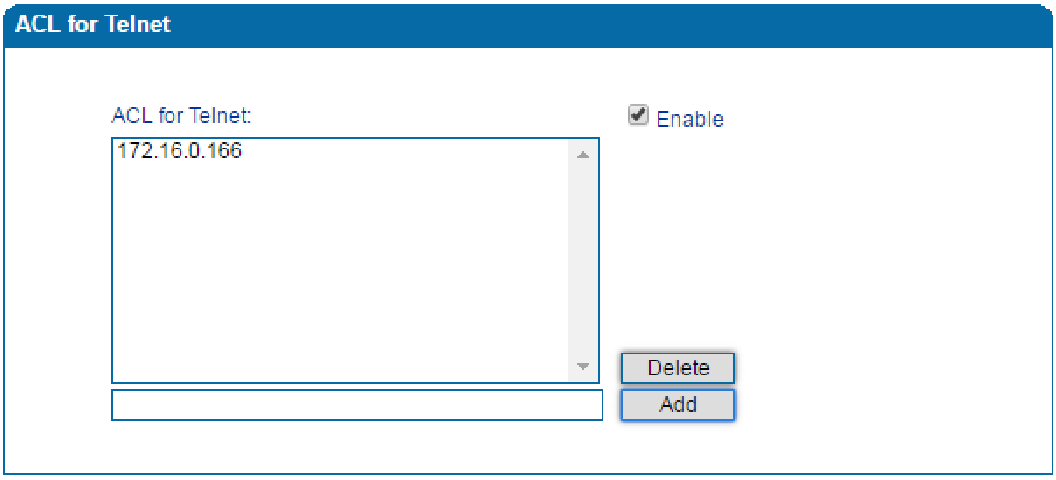
Figure 4-38 Add IP Address to Web ACL



4.13.2 Telnet ACL

ACL (Access Control List) for Telnet is used to configure IP addresses that are allowed to access the Telnet Interface of the DAG2000 device. The IP address list can't be null once ACL is enabled.

Figure 4-39 Add IP Address to Telnet ACL

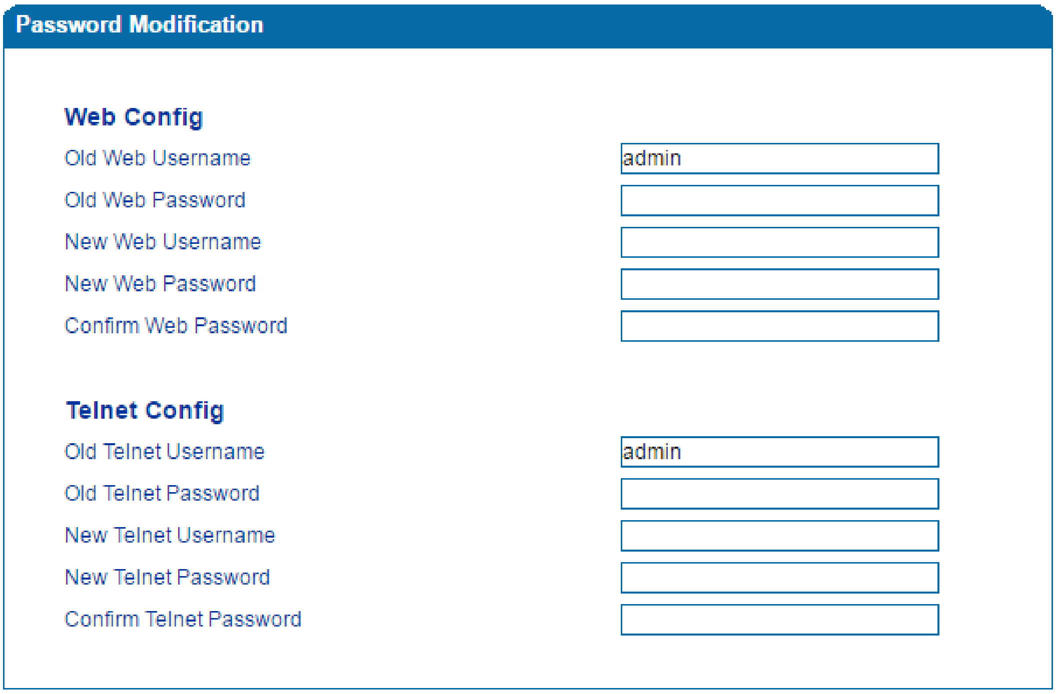


4.13.3 Passwords

You can configure or modify the username and password for logging in the Web interface and the Telnet interface of the DAG2000 device on this page.

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

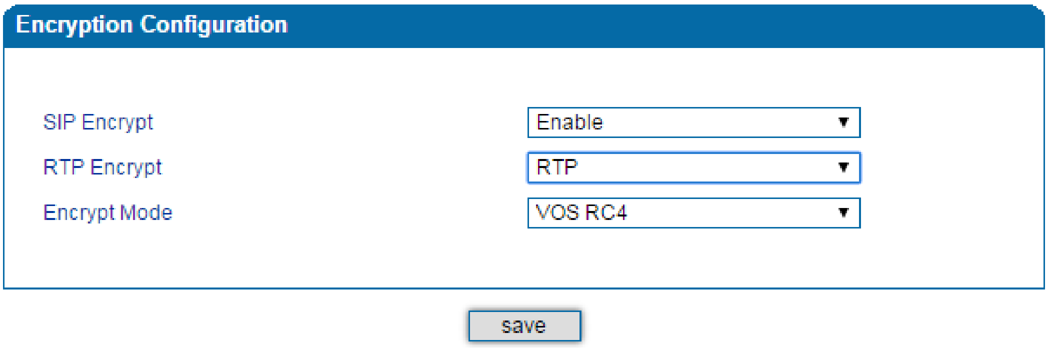
Figure 4-40 Modify Username and Password



4.13.4 Encrypt

When the DAG2000 device is registered to a VOS softswitch, you can encrypt SIP and RTP for the VOS softswitch.

Figure 4-41 Encrypt SIP and RTP



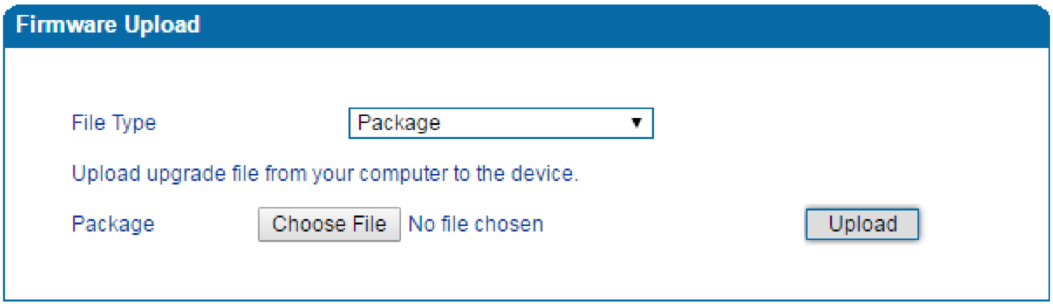
Note: If SIP encrption is enabled, heartbeat and anonymous calls should be disabled.

4.14 Tools

4.14.1 Firmware Upload

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

Figure 4-42 Upload Firmware



Steps of Firmware Uploading:

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

Step 2. Prepare firmware package.

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

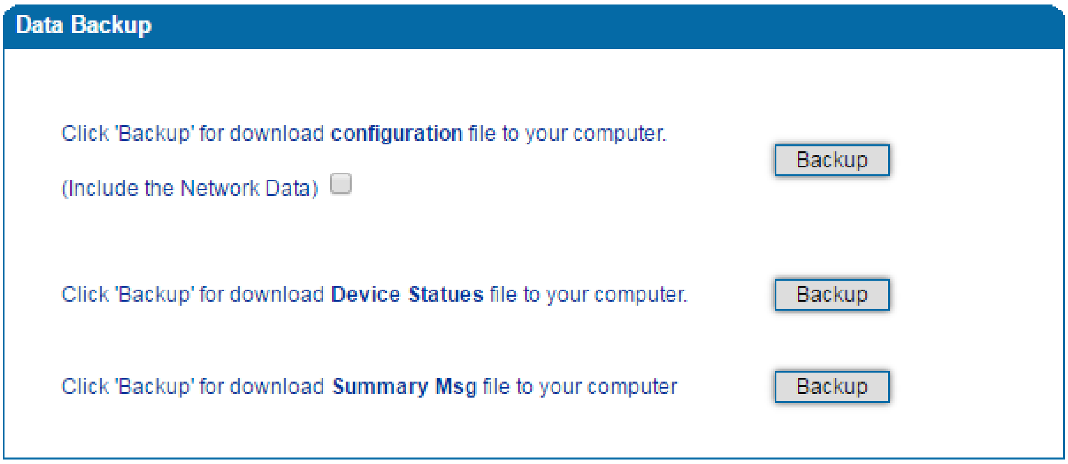
Step 4. Keep waiting until it prompts 'Software loaded successfully!'

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

4.14.2 Data Backup

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

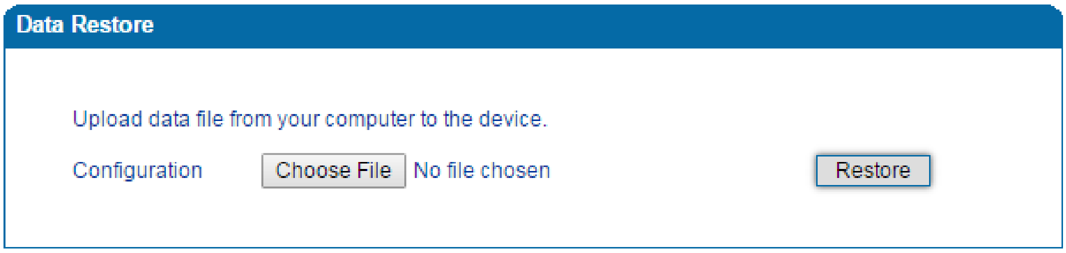
Figure 4-43 Backup Data



4.14.3 Data Restore

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

Figure 4-44 Restore Data



4.14.4 Ping Test

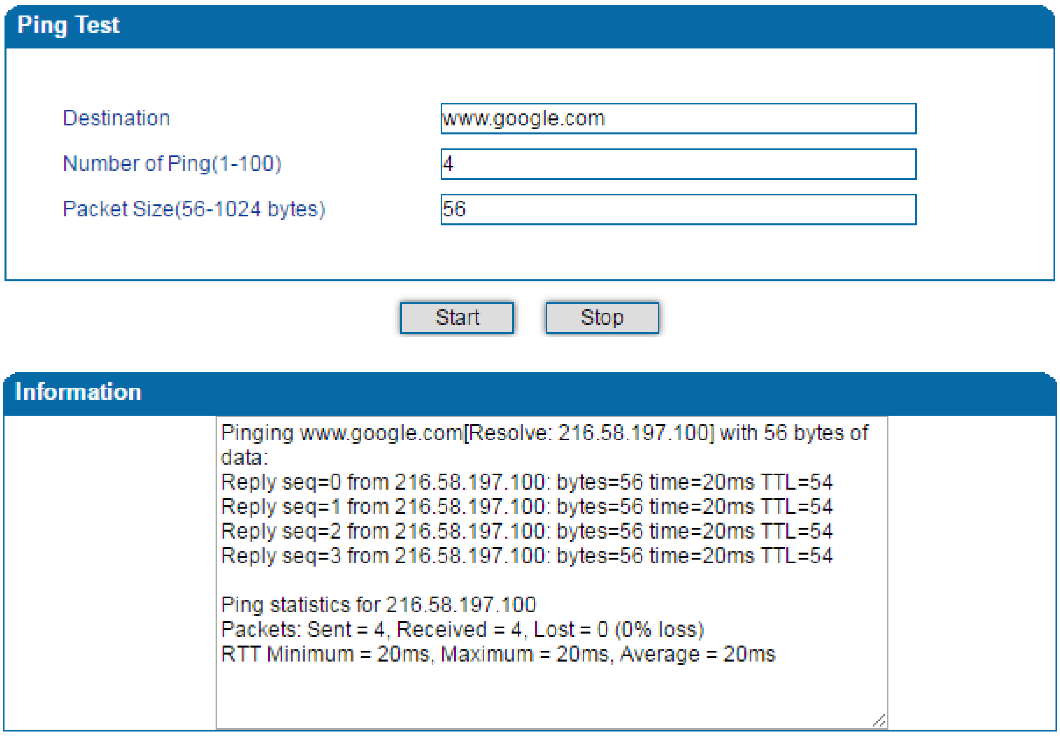
Ping is used to examine whether a network works normally through sending test packets and calculating response time.

Instructions for using Ping:

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

2. If related messages are received, it means the network works normally; otherwise, the network is not connected or is connected faultily.

Figure 4-45 Execute Ping Test



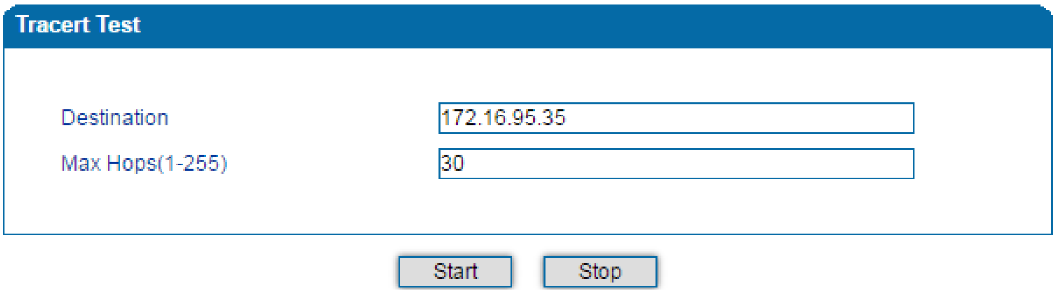
4.14.5 Tracert Test

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

Instruction for using Traceroute:

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

Figure 4-46 Execute Tracert Test



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

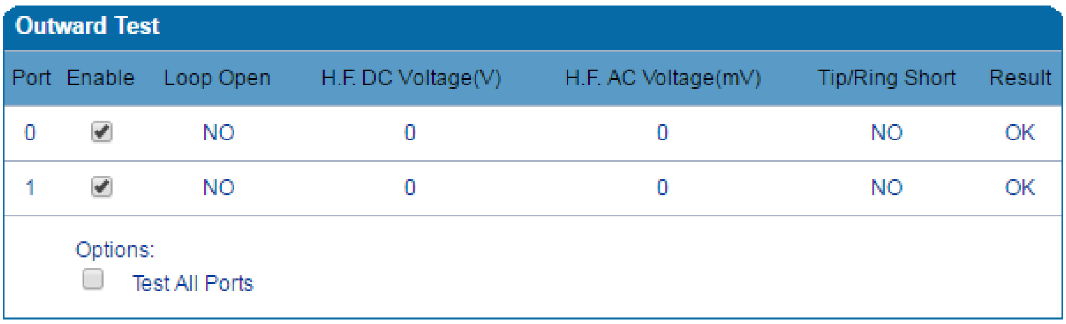
Max Hops: the maximum hops for searching the above IP address or domain name. For example, if 'max hops' is set as 30, and the configured IP address or domain name cannot be reached within 30 hops, it's thought that the IP address or domain name cannot be searched.

2. View the route information from the returned message.

4.14.6 Outward Test

Outward test enables you to diagnose the physical function of FXS port which follow the GR909 standard. To start outward test, select the FXS ports to be tested and click 'Start'. The testing may cost a few minutes.

Figure 4-47 Execute Outward Test



Test Results:

OK: the physical function of the tested FXS ports is working well;

FAIL: There's something wrong with the physical function of the tested FXS ports.

Copyright©2011-2020 Dinstar

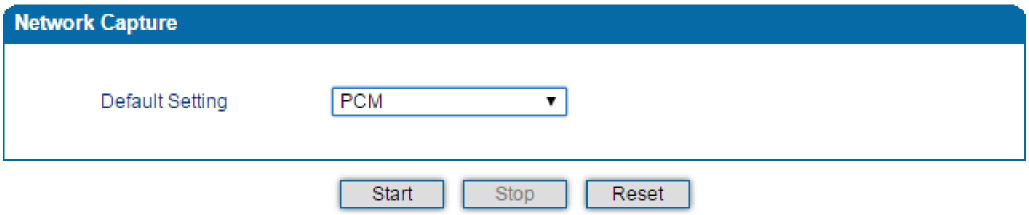
4.14.7 Network Capture

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

PCM Capture:

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

Figure 4-48 Capture PCM Packages



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

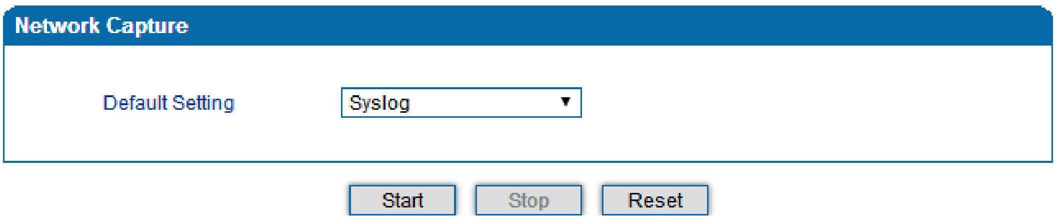
The captured package is named 'capture(x).pcap', among which x is the serial number of the capturing and will be added 1 in next time. The sample of PCM capture as below:

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)

Syslog Capture:

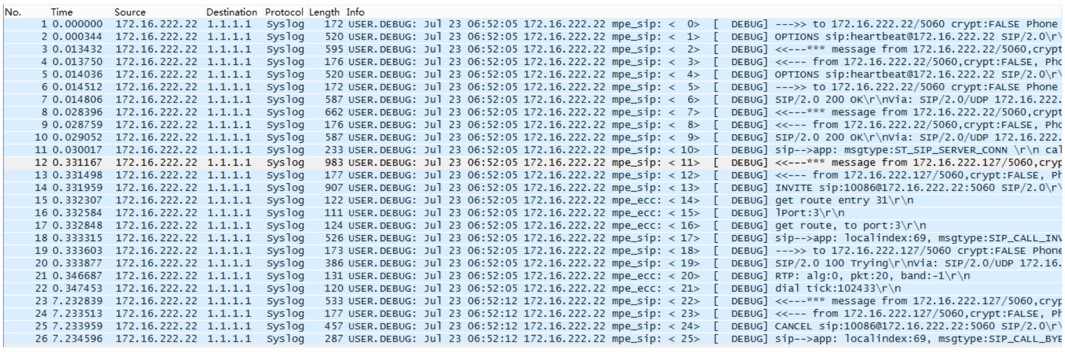
Syslog capture is another way to obtain syslog which is the same as remote syslog server and filelog. The captured file is save as pcap format so that it can be opened in some of capturing software like Wireshark, Ethereal software etc.

Figure 4-49 Capture Syslog Packages



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

The capture package is named 'capture(x).pcap', amont which x is the serial number of capturing and will be added 1 in next time. The sample of syslog capture as below:

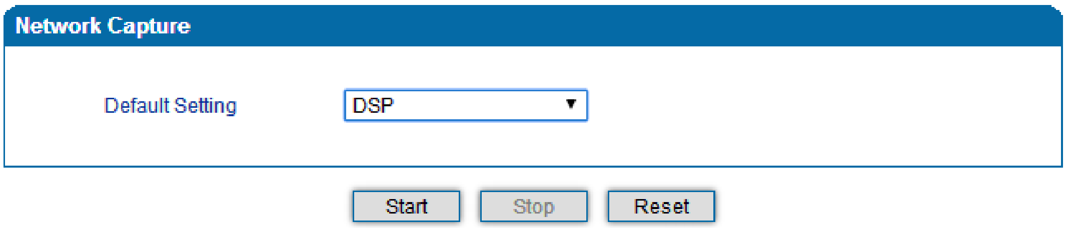


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 0> [DEBUG] --->> to 172.16.222.22/5060 crypt:FALSE Phone
2	0.000344	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 1> [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, Pho
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, Pho
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

DSP Capture:

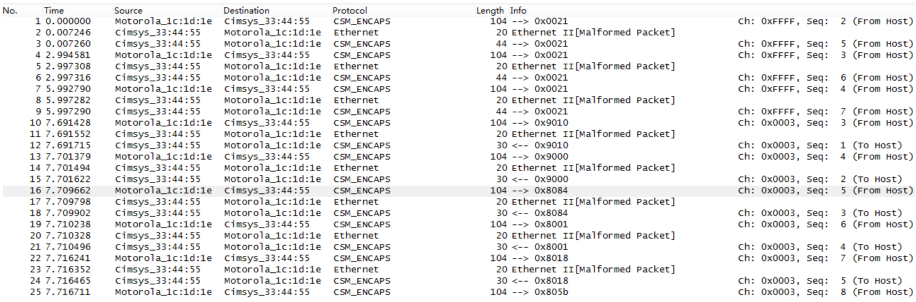
DSP capture helps to analyze voice stream inside DSP chipset. The DSP chipset will handle RTP from IP network as well as voice stream from analog phone.

Figure 4-50 Capture DSP Packages



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

The captured package is named 'capture(x).pcap', amont which x is the serial number of the capturing and will be added 1 in next time. The sample of RTP capture as below:

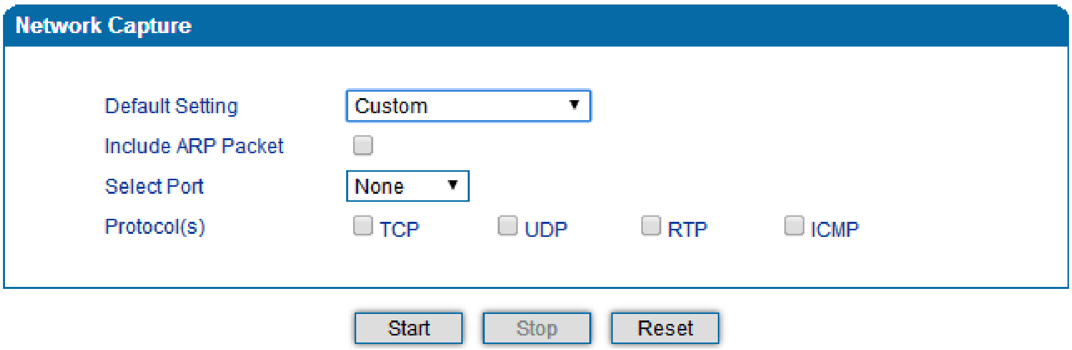


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCAPS	104	--> 0x0021 Ch: 0xFFFF, Seq: 2 (From Host)
2	0.007246	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]
3	0.007260	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCAPS	44	--> 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)

Customized Capture:

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

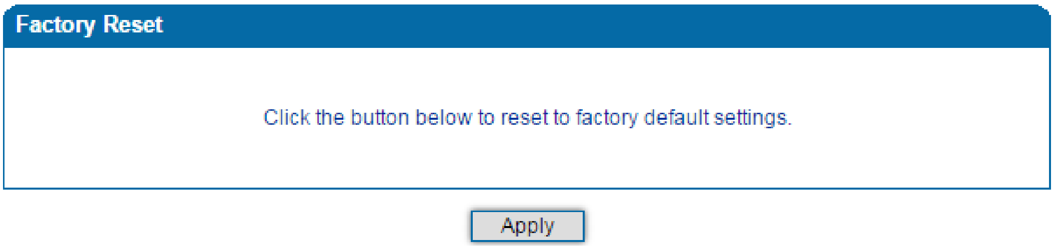
Figure 4-51 Customized Capturing



4.14.8 Factory Reset

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

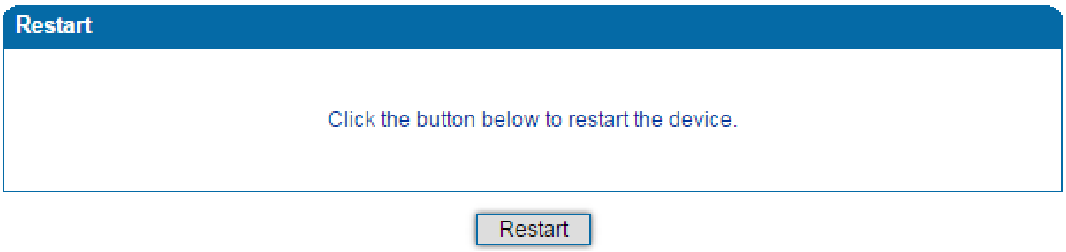
Figure 4-52 Reset Device to Factory Default Setting



4.14.9 Device Restart

For some configurations or changes to the DAG2000 device, you are required to restart the device for the configurations or changes to take effect.

Figure 4-53 Restart Device



5 Glossary

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