



Dinstar DAG-FXO VoIP Gateway

User Manual V2.0



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 **Dinstar DAG-FXO VoIP Gateway**! We hope you will make optimum use of this flexible, rich-feature VoIP gateway. Please read this document carefully before install the gateway.

About This Manual

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

This manual is written with reference to the default configurations of the **DAG-FXO VoIP Gateway**.

Intended Audience

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

- System Maintenance Engineer
- Network Engineer

Revision Records

Document Version 2.1 (2019/10/09)

- Document Name: Dinstar DAG-FXO VoIP Gateway User Manual V2.1
- Firmware Version: 1.81.10.06
- Revised Items: document layout, all contents, application scenario and network diagrams

Document Version 2.1 (2014/03/16)

- Document Name: DAG Series FXO Voice Gateway User Manual V2.0

Contents

1 Product Description	7
1.1 Overview	7
1.2 Application Scenario	7
1.3 Product Appearance	8
1.4 Ports, Connectors and Indicators.....	9
1.4.1 DAG1000-4O	9
1.4.2 DAG1000-8O	10
1.4.3 DAG2000-16O	11
1.5 Description of Indicators.....	12
1.6 Functions and Features.....	12
1.6.1 Protocol standard supported	12
1.6.2 Voice and Fax Parameters	13
1.6.3 Supplementary Services.....	13
2 Basic Operation	15
2.1 Callout and Callin via FXO Port.....	15
2.1.1 Call Out	15
2.1.2 Call In	15
2.1.3 Direct IP Calls	15
2.2 Call Features.....	16
2.3 Sending and Receiving Fax.....	17
2.3.1 T. 38 and Pass-Through	18
2.4 Local IVR Operation	18
2.4.1 Inquire IP address	18
2.4.2 Factory Reset.....	18
2.4.3 Set IP Address	18
3 Web Configuration.....	20
3.1 WEB Login	20
3.1.1 Login.....	20
3.1.2 Login WEB	21

3.2 Navigation Tree	22
3.2.1 System Information.....	22
3.2.2 Port Status.....	25
3.2.3 Current Call	26
3.2.4 RTP Session	26
3.2.1 CDR	27
3.2.1 Record Statistics.....	27
3.3 Quick Setup Wizard	28
3.4 Network Configuration	28
3.4.1 Local Network	28
3.4.2 VLAN Parameter.....	31
3.4.3 DHCP Option (Routing mode)	33
3.4.4 QoS.....	33
3.4.5 LAN QoS	33
3.4.6 ARP.....	34
3.5 SIP Server	34
3.6 IP Profile.....	36
3.7 TEL Profile	38
3.8 Port	39
3.9 Advanced	41
3.9.1 Line Parameter	41
3.9.2 FXO Parameters.....	42
3.9.3 Media Parameter	42
3.9.4 Service Parameter.....	44
3.9.5 SIP Compatibility.....	45
3.9.6 NAT Parameter	48
3.9.7 Speed Dial	48
3.9.8 Feature Code.....	49
3.9.9 System Parameter	50
3.10 Call & Routing	52
3.10.1 Wildcard Group	52
3.10.2 Port Group	53
3.10.3 IP Trunk	54
3.10.4 Routing Parameter	55

3.10.5 IP -> Tel Routing	56
3.10.6 Tel-IP/Tel Routing	56
3.11 Manipulation	57
3.11.1 IP -> Tel Callee	58
3.11.2 Tel -> IP/Tel Caller	59
3.11.3 Tel-IP/Tel Callee	60
3.12 Routing rule examples	60
3.12.1 Route any calls from any IP to specific port	60
3.12.2 Route any calls from any IP to specified port group	61
3.12.3 Route any calls from any port to specific SIP IP trunk	63
3.13 Management	64
3.13.1 TR069	64
3.13.2 SNMP (Simple Network Management Protocol)	65
3.13.3 Syslog	67
3.13.4 Provision	69
3.13.5 Cloud server	70
3.13.6 User manage	70
3.13.7 Remote server	71
3.13.8 Record Parameter	71
3.13.9 Radius Parameter	72
3.13.10 Action URL	72
3.14 Security	73
3.14.1 WEB ACL	73
3.14.2 Telnet ACL	74
3.14.3 Passwords	74
3.14.4 Encrypt	75
3.15 Tools	75
3.15.1 Firmware upload	75
3.15.2 Data Backup	76
3.15.3 Data Restore	77
3.15.4 FXO Test	78
3.15.5 Ping Test	79
3.15.6 Tracert Test	79
3.15.7 Network Capture	80

3.15.8 Factory Reset.....	84
3.15.9 Device Restart	85
4 Glossary	85

1 Product Description

1.1 Overview

Dinstar's DAG-FXO VoIP gateway is an access gateway based on IP network. It can provide low-cost, easy-to-use VoIP solutions and high-quality voice services for SOHO (Small Office-Home office), remote office, small enterprise and enterprise with multiple branches.

Based on standard SIP protocol, the gateway is compatible with IP PBX, soft-switch and SIP-based platforms.

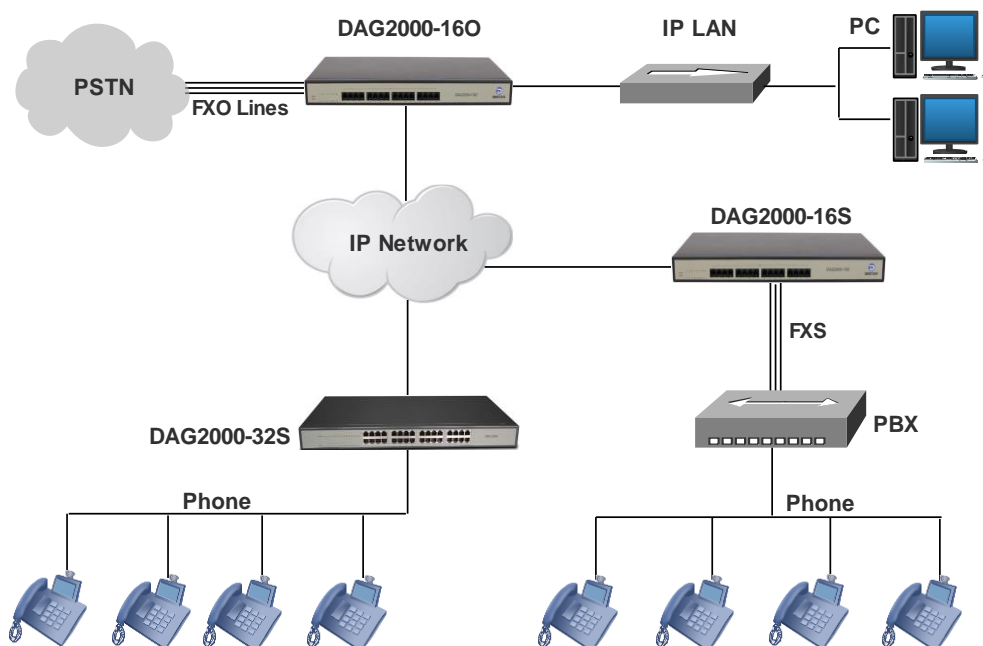
Dinstar provides FXO VoIP gateways with following models:

- DAG1000-40
- DAG1000-80
- DAG2000-160

This manual takes DAG2000-160 as the example to introduce the functions and configurations of Dinstar's FXO VoIP gateway, since the functions and configurations of all models are almost the same.

1.2 Application Scenario

Figure 1-1 Application Scenario of DAG2000-160 VoIP Gateway:



1.3 Product Appearance

Figure 1-2 Image of DAG1000-40



Figure 1-3 Image of DAG1000-80



Figure 1-4 Images of DAG2000-160



1.4 Ports, Connectors and Indicators

1.4.1 DAG1000-40

Figure 1-5 Indicators of DAG1000-40

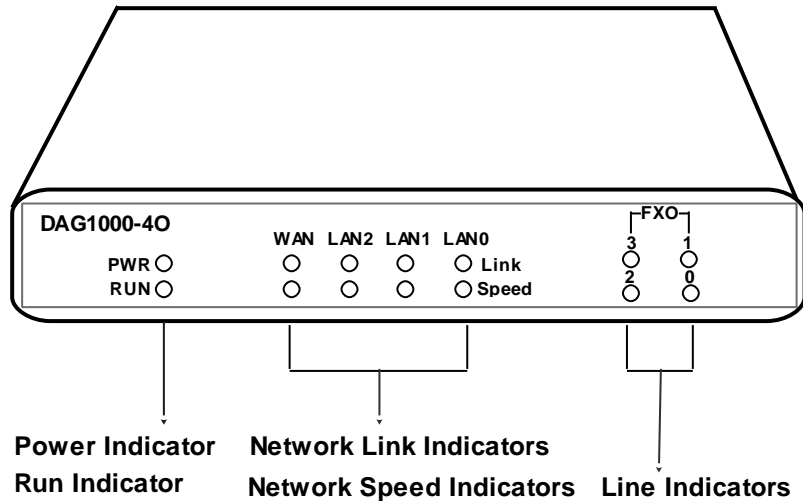


Figure 1-6 Ports of DAG1000-40

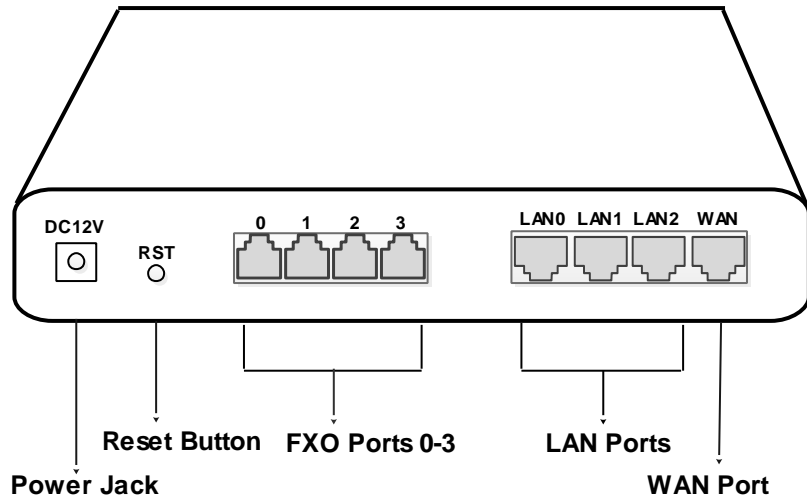


Table 1-1 Description of Ports

Port Name	Description
Power Jack	To connect DC 12V power supply
WAN/LAN Port	To connect to IP network over a DSL modem, router or LAN switch
FXO Ports 0-3	To connect to PSTN

Reset Button	Used to reset the gateway to factory default setting
--------------	--

1.4.2 DAG1000-80

Figure 1-7 Indicators of DAG1000-80

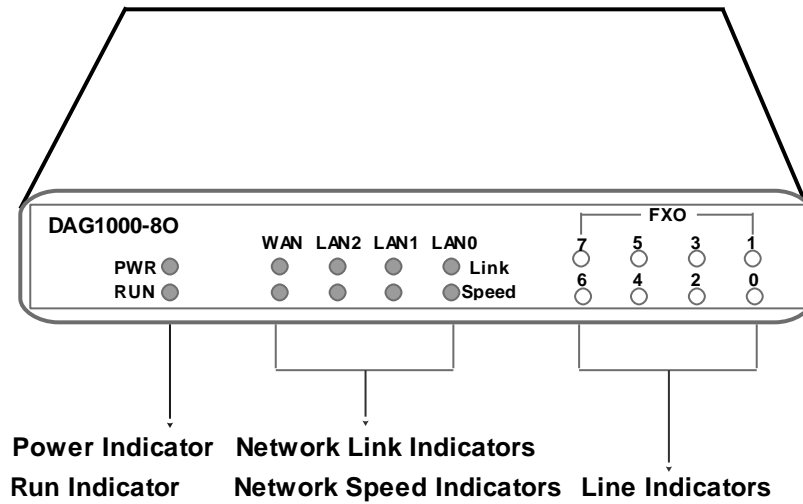


Figure 1-8 Ports of DAG1000-80

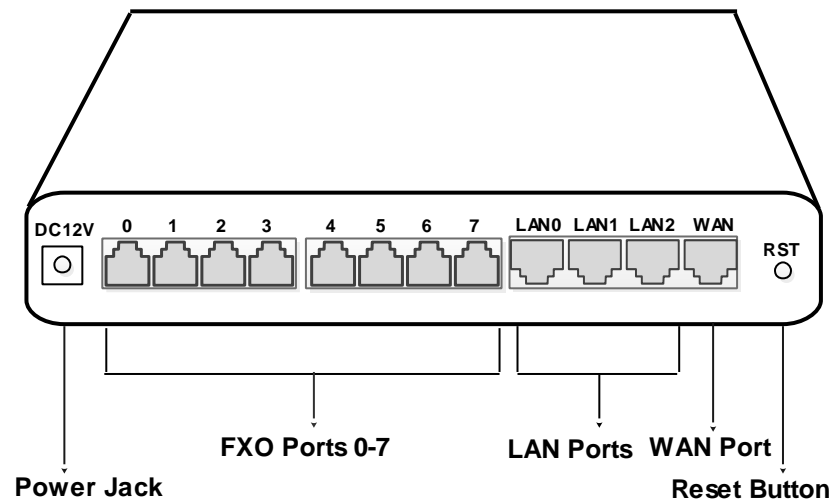


Table 1-2 Description of Ports

Port Name	Description
Power Jack	To connect DC 12V power supply
WAN/LAN Port	To connect to IP network over a DSL modem, router or LAN switch
FXO Ports 0-7	To connect to PSTN

Reset Button	Used to reset the gateway to factory default setting
--------------	--

1.4.3 DAG2000-160

Figure 1-9 Indicators of DAG2000-160

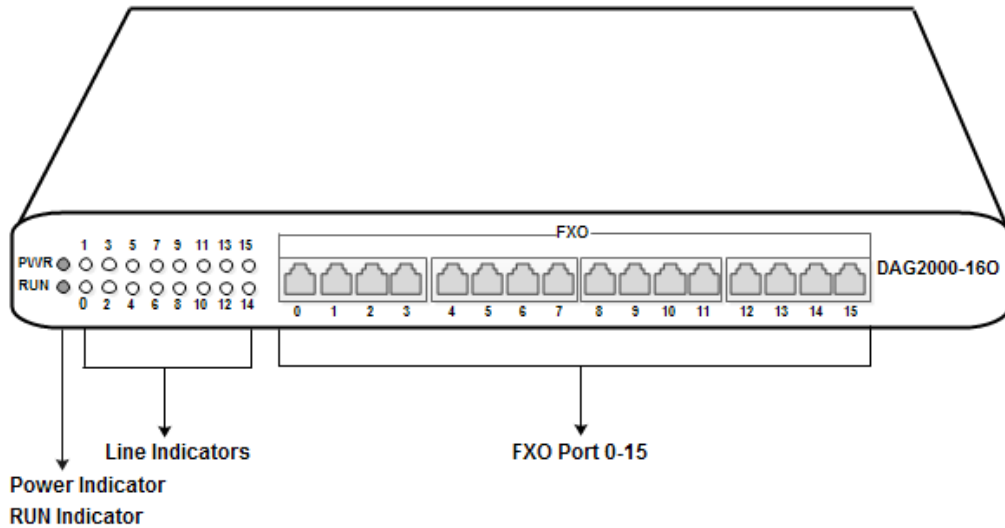


Figure 1-10 Ports of DAG2000-160

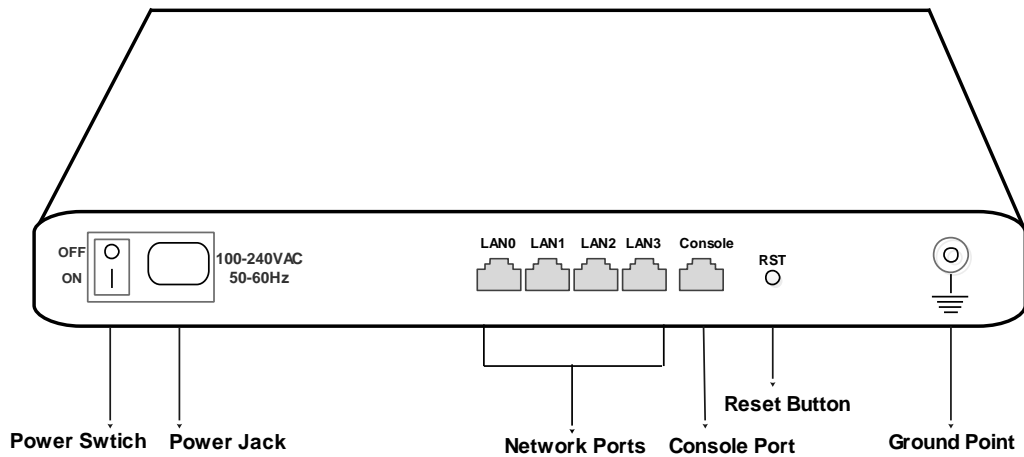


Table 1-3 Description of Ports

Port/Connector	Description
Power Switch	Turn on or turn off power supply
Power Jack	To connect 100-240V AC power supply
Reset Button	Used to reset the gateway to factory default setting

Console Port	Used to connect to serial line for the purpose of carrying out maintenance-related configurations
LAN Ports	To connect to IP network over a DSL modem, router or LAN switch
FXO Ports 0-15	To connect to PSTN
Ground Point	Used to connect to a ground wire

1.5 Description of Indicators

Indicator	Status	Description
PWR	On green	The DAG-FXO gateway is powered on.
	On dull	There is no power supply or power supply is abnormal.
RUN	Slow flash	The gateway is running properly.
	Quick flash	SIP account is registered successfully.
	No flash/ On dull	The gateway is running improperly.
FXO	On green	The corresponding FXO port is currently occupied by a call.
	On dull	No call occupies the corresponding FXO port currently.
WAN/LAN (Link)	On green	The gateway is properly connected to network.
	On dull	The gateway is not connected to network or the connection is improper.
WAN/LAN(Speed)	On green	The network speed is 100Mbps.
	On dull	The network speed is 10Mbps.

1.6 Functions and Features

1.6.1 Protocol standard supported

- SIP V2.0 (RFC 3261,3262,3264)
- SDP (RFC 2327)
- REFER (RFC 3515)
- RTP/RTCP (RFC 1889,1890)
- STUN (RFC 3489)

- ARP/RARP (RFC 826/903)
- SNTP (RFC 2030)
- DHCP/PPPoE
- TFTP/HTTP/HTTPS
- DNS/DNS SRV (RFC 1706/RFC 2782)
- VLAN 802.1P/802.1Q
- Differentiated Server

1.6.2 Voice and Fax Parameters

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

1.6.3 Supplementary Services

- Busy Tone Detection
- Detection for No Current in FXO Line
- Detection for Voice Interruption
- One-stage Dialing
- Two-stage Dialing
- Polling on FXO ports under PSTN
- Polarity Reversal
- Fake Billing Correction (FAS)
- DC/AC Impedance Configuration
- Calls Detection (Bellcore Type 1&2, ETSI, DTMF)
- Port Group
- IP Trunk
- Voice Mail

- Direct IP Call
- Redundant Registration Server
- 32 Inbound Routes
- 32 Outbound Routes
- Manipulation of Inbound and Outbound numbers

2 Basic Operation

2.1 Callout and Callin via FXO Port

2.1.1 Call Out

One-stage Dialing: After the DAG-FXO gateway receives a call number sent from softswitch or IPPBX, if the number matches one of the dialing rules set on **Advanced → Digit Map** interface, the call will directly choose a FXO port to go out based on port selection rule.

Two-stage Dialing: dial a FXO port's SIP account number from an extension of IPPBX, and then you will hear a PSTN's dialing tone. After that, you will be able to dial any number of PSTN lines.

2.1.2 Call In

Dial the number of a PSTN line connected to a FXO port of DAG-FXO gateway, and then you will hear a secondary dialing tone or a voice prompt of "please dial the extension number". Then dial the called number (extension number or telephone number), after the dialing is completed, the called number will be sent to IP server such softswitch or IPPBX.

Hotline auto-dialing: Dial the number of a PSTN line connected to a FXO port of DAG-FXO gateway, then the gateway will automatically route the call to designated extension number or telephone number according to preset hotline number.

2.1.3 Direct IP Calls

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

Elements necessary to completing a direct IP call:

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

Operation Process:

- 1) Pick up the analog phone then dial “*47”
- 2) Enter the target IP address.

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

Examples:

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

【Note】: You cannot make direct IP calls between FX00 to FX01 since they are using same IP. It only supports the default destination port 5060.

2.2 Call Features

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

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

Table 2.2-1 Feature Codec

Feature Codec	Operation Instructions
*158#	View the LAN port IP address
*159#	View the WAN port IP address
*114#	Inquire port account
150	Set the way of obtain IP address
157	Set network method
152	Set IP address
153	Set Subnet mask
156	Set default gateway IP address
*193#	Obtain IP address through DHCP again
*160*1#	Open WAN port to access web

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

2.3 Sending and Receiving Fax

The DAG-FXO gateway supports four fax modes:

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

2.3.1 T. 38 and Pass-Through

T.38 is the preferred fax mode because it is more reliable and works well in most network conditions. If the service provider supports T.38, please use this method by selecting T.38 as fax mode (default). If the service provider does not support T.38, pass-through mode may be used.

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.

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.

2.4 Local IVR Operation

2.4.1 Inquire IP address

Connect a PSTN line to one of the FXO ports of the DAG-FXO gateway, and then use a mobile phone or a fixed telephone to dial the number of the PSTN line. After you hear a dialing tone or a voice prompt, dial *158# to inquire the IP address of LAN port and dial *159# to inquire the IP address of WAN port.

2.4.2 Factory Reset

Connect a PSTN line to one of the FXO ports of the DAG-FXO gateway, and then use a mobile phone or a fixed telephone to dial the number of the PSTN line. After hearing a dialing tone or a voice prompt, dial *166*000000#, and you will hear “successful setting”, then hang up the phone and the gateway is reset to factory defaults.

2.4.3 Set IP Address

Before configuration, please ensure:

- ▶ The gateway is power on;
- ▶ Device has been connected to network;
- ▶ Telephone is connected to FXO port of the DAG1000-4S/8S gateway.

Configure dynamic IP address by DHCP:

Pick up the phone, dial *150*2# and then hang up the phone.

If the voice prompt indicates ‘setting successfully’, please restart the gateway after 10 seconds.

Configure Static IP address:

Take the configuration of IP address ‘172.16.0.100’ as example.

Pick up the phone, dial *150*1# and then hang up the phone.

Then configure IP address and subnet mask as follow:

- Configure IP address

Pick up the phone, dial *152*172*16*0*100# and then hang up the phone.

- Configure subnet mask

Pick up the phone, dial *153*255*255*0*0# and then hang up the phone.

- Configure gateway IP address

Pick up the phone, dial *156*172*16*0*1# and then hang up the phone.

- Query the IP address of the DAG1000-4S/8S gateway:

Pick up the phone, dial *158#.

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

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

3 Web Configuration

3.1 WEB Login

The default IP addresses of LAN port of the device is 192.168.11.1. Connect the DAG FXO gateway to the network according to the following network topology, and dial *158 to query the IP address of the gateway.

3.1.1 Login

Modify the IP address of the PC to make it at the same network segment with the DAG FXO device, since the default IP address of the gateway is 192.168.11.1.

Take Windows 7 as an example, the IP address of PC is changed into 192.168.11.10:

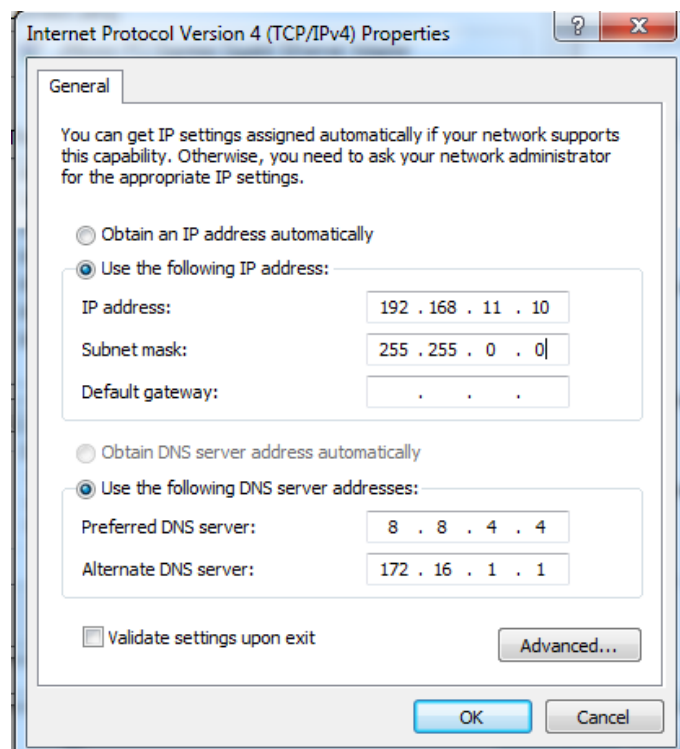


Figure 3.1-1 Modify IP address

Check the connectivity between the PC and the gateway. Click **Start** → **Run** of PC and enter cmd to execute 'ping 192.168.11.1' to check whether the IP address of the DAG FXO gateway runs normally.

3.1.2 Login WEB

Open a web browser and enter the IP address of LAN port of the DAG FXO gateway (the default IP of LAN port is 192.168.11.1; if this IP address has been changed, please enter the new IP address). Then the login GUI will be displayed. Both the default username and password are admin.

It is advised to modify the username and password for security consideration.

Figure 3.1-1 DAG FXO Login Interface

Enter default username and password: admin/admin, then click “Log in” to enter into the Web interface. And then you can see the following web interface.

System Information			
Device ID	da27-8170-2070-0021		
MAC Address	F8-A0-3D-28-78-A1		
IP Address	192.168.218.29	255.255.255.0	Static
	192.168.218.1		
DNS Server	213.42.20.20	195.229.241.222	
Cloud Register Status	Not Registered		
System Uptime	6511h: 05m: 30s		
NTP Status	Succeed		
NTP Time	2019-10-09 14:32:22		
Network Traffic Statistics	Received 2495906655 bytes	Sent 3633809630 bytes	
Usage of Flash	92 % (10190848 / 11010048) bytes		
Usage of RAM in Linux	34 % (77242368 / 222306304) bytes		
Usage of RAM in AOS	9 % (6639616 / 67100672) bytes		
Current Software Version	IAD-16O 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40		
Backup Software Version	IAD-16O 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40		
DSP Version	ARM_32_9 Mar 9 2018 10:46:34		
U-BOOT Version	3		
Kernel Version	8		
FS Version	6		
Hint Language	English		

Figure 3.1-2 DAG Configure Interface

3.2 Navigation Tree

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



Figure 3.2-1 Navigation Tree

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

3.2.1 System Information

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

System Information			
Device ID	da27-8170-2070-0021		
MAC Address	F8-A0-3D-28-78-A1		
IP Address	192.168.218.29	255.255.255.0	Static
	192.168.218.1		
DNS Server	213.42.20.20	195.229.241.222	
Cloud Register Status	Not Registered		
System Uptime	6511h: 30m: 40s		
NTP Status	Succeed		
NTP Time	2019-10-09 14:55:42		
Network Traffic Statistics	Received 2498039985 bytes	Sent 3634284083 bytes	
Usage of Flash	92 %(10190848 / 11010048) bytes		
Usage of RAM in Linux	34 %(77488128 / 222306304) bytes		
Usage of RAM in AOS	10 %(6713344 / 67100672) bytes		
Current Software Version	IAD-16O 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40		
Backup Software Version	IAD-16O 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40		
DSP Version	ARM_32_9 Mar 9 2018 10:46:34		
U-BOOT Version	3		
Kernel Version	8		
FS Version	6		
Hint Language	English		

Figure 3.3-1 System Information

System information as follow:

Table 4.3-1 System Information Description

Device ID	A unique ID of each device. This ID is used for warranty and cloud server authentication.
MAC address	Hardware address of the DAG FXO gateway
IP Address	The IP address of LAN port of the gateway DHCP: Obtain IP address automatically. DAG FXO gateway is regarded as a DHCP client, which sends a broadcast request and looks for a DHCP server to answer. Then the first discovered DHCP server automatically assigns an IP address to the DAG FXO gateway from a defined range of numbers.

	<p>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 <i>ad hoc</i> at the start of each session, normally changing from one session to the next.</p> <p>If you choose static IP address, you need to fill in the following information:</p> <ul style="list-style-type: none"> ● IP Address: the IP address of LAN port of the DAG FXO gateway; ● Subnet Mask: the netmask of the router connected the DAG FXO gateway; ● Default Gateway: the IP address of the router connected the DAG FXO gateway; <p>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.</p> <p>If you choose PPPoE, you need to fill in to fill in the following information:</p> <ul style="list-style-type: none"> ● 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 address of DNS server and default gateway information is displayed.
Cloud Register Status	Whether the DAG FXO gateway is registered to cloud or not.
System Uptime	The running time of the DAG FXO gateway since it is powered on.
NTP Status	<p>Succeed: the DAG FXO gateway is sync to NTP server successfully;</p> <p>Failed: the DAG FXO gateway fails to be sync to NTP server. Then you should check network connection and the NTP server.</p>
Network Traffic Statics	Total bytes of message received and sent by network port.
Usage of Flash	Detailed usage of Flash memory
Usage of RAM in Linux	Detailed RAM usage of Linux core
Usage of RAM in AOS	Detailed RAM usage of AOS

Current Software Version	The software version that runs on the gateway. 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 FXO gateway

3.2.2 Port Status

Port						
Port No.	Type	SIP User ID	User Status	Port Status	Call Status	
0	FXO	---	---	OnHook	Idle	
1	FXO	---	---	OnHook	Idle	
2	FXO	---	---	OnHook	Idle	
3	FXO	---	---	OnHook	Idle	
4	FXO	---	---	OnHook	Idle	
5	FXO	---	---	OnHook	Idle	
6	FXO	---	---	OnHook	Idle	
7	FXO	---	---	OnHook	Idle	
8	FXO	---	---	OnHook	Idle	
9	FXO	---	---	OnHook	Idle	
10	FXO	---	---	Offline	Idle	
11	FXO	---	---	Offline	Idle	
12	FXO	---	---	Offline	Idle	
13	FXO	---	---	Offline	Idle	
14	FXO	---	---	Offline	Idle	
15	FXO	---	---	Offline	Idle	

Port Group			
Port Group	Port	SIP User ID	User Status
12 <For_FAX_Line>	10,...	10012...	Registered
13 <For_Ext_134>	9,...	10010...	Registered
14 <For_Ext_222>	8,...	10000...	Registered
15 <10013>	0,1,2,3,4,...	10013...	Registered

Figure 3.3-2 Port and Port group registration information

3.2.3 Current Call

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

Figure 3.3-3 Current Call Statistics

The above interface shows the the current call information. If there are no calls currently, no information will be displayed.

3.2.4 RTP Session

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

Figure 3.3-4 RTP Session Statistics

The above interface shows real-time RTP conversation flow data information, includes:

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

3.2.1 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.

CDR Report

Enable CDR No Yes

Port Call State Source Destination

CDR Oper

Enable Advanced Option No Yes

Total: 1000Item 50Item/Page 1/20Page

Port	Start Time	Answer Time	Direction	Source	Destination	PeerIP	Codec	Reason	Duration (s)
9	2019/10/09 14:59:06	2019/10/09 14:59:09	TEL->IP	10010	10010	192.168.218.200	PCMU	Recv BYE	22
4	2019/10/09 14:20:27	2019/10/09 14:20:29	IP->TEL	10013	092283861#	192.168.218.200	PCMU	Recv BYE	196
3	2019/10/09 13:01:52	--	TEL->IP	0933499754000	10013	NOT GETED	PCMU	Rejected	0
3	2019/10/09 12:46:10	2019/10/09 12:46:12	IP->TEL	10013	2071140#	192.168.218.200	PCMU	Recv BYE	64
2	2019/10/09 12:28:31	2019/10/09 12:28:35	TEL->IP	092233344	10013	192.168.218.200	PCMU	Recv BYE	47

On the **Status & Statistic → CDR** interface, details of all calls through the DAG FXO gateway are displayed. The CDR function can be enabled on this interface.

3.2.1 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

3.3 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 DAG FXO device.

Setup Wizard - Local Network

Network Configuration

Obtain an IP address automatically

Use the following IP address

IP Address

Subnet Mask

Default Gateway

PPPoE

Account

Password

Service Name

WAN MTU

Manage Address

IP Address

Subnet Mask

DNS Server

Obtain DNS server address automatically

Use the following DNS server address

Primary DNS Server

Secondary DNS Server

3.4 Network Configuration

3.4.1 Local Network

DAG has two kinds of work mode: route and bridge. When DAG is set route mode, the DAG will work as small router and NAT function has enabled. In this situation, WAN port is normally connect to uplink router/switch or

ADSL MODEM, LAN port used to connect local computer or other network device(such as Ethernet switches, Hubs etc); When DAG is set bridge mode, WAN and LAN port are the same. The DAG just work as two ports or four ports Ethernet switch.

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

Note: DAG2000-160 just supports bridge mode. DAG1000-4/80 supports bridge and route mode.

► Bridge mode

Network configuration of bridge mode:

Local Network

Network Configuration

Obtain an IP address automatically
 Use the following IP address

IP Address
 Subnet Mask
 Default Gateway

PPPoE

Account
 Password
 Service Name

WAN MTU

Manage Address

IP Address
 Subnet Mask

DNS Server

Obtain DNS server address automatically
 Use the following DNS server address

Primary DNS Server
 Secondary DNS Server

Figure 3.5-1 Local network

- When “Obtain IP address automatically” is selected, the gateway will obtain IP address by DHCP.
- When “Use the following IP address” is selected, user needs to configure a static IP address.

- When “PPPoE” is selected, user needs to fill in the account and password offered by ISP.

【Notes】 :

- 1) If DHCP is selected to obtain IP address, please ensure DHCP server in the network works normally.
- 2) After the configurations are finished, please restart the gateway for the configurations to take effect.

► Route Mode

Network configuration of route mode:

Network Mode	<input checked="" type="radio"/> Route <input type="radio"/> Bridge
WAN Port	
Link Speed & Duplex	Auto Detect <input type="button" value="v"/>
<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Use the following IP address	
IP Address	172.16.22.222
Subnet Mask	255.255.0.0
Default Gateway	172.16.1.1
<input type="radio"/> PPPoE	
Account	
Password	
Service Name	
WAN MTU	1500
LAN Port	
Link Speed & Duplex	Auto Detect <input type="button" value="v"/>
IP Address	192.168.11.1
Subnet Mask	255.255.255.0
LAN MTU	1500
DNS Server	
<input type="radio"/> Obtain DNS server address automatically	
<input checked="" type="radio"/> Use the following DNS server address	
Primary DNS Server	202.96.128.68
Secondary DNS Server	202.96.134.133

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

3.4.2 VLAN Parameter

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

▶ 802.1Q

The IEEE 802.1Q standard defines the architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs and the protocols and algorithms involved in the provision of those services.

No Quality of Service mechanisms are defined in this standard, but an important requirement for providing QoS is included in this standard, e.g. the ability to regenerate user priority of received frames using priority information contained in the frame and the User Priority Regeneration Table for the reception Port.

▶ 802.1P

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

VLAN

VLAN NO.

Data
 Voice
 Management

802.1Q VLAN ID(1 - 4095)

802.1P Priority(0 - 7)

Network Configuration

Obtain an IP address automatically
 Use the following IP address

IP Address

Subnet Mask

Default Gateway

DNS Server

Obtain DNS server address automatically
 Use the following DNS server address

Primary DNS Server

Secondary DNS Server

MTU

Figure 3.7-3 VLAN parameter configuration

Explanations of the parameters in VLAN interface:

VLAN1/VLAN2/VLAN3	The gateway supports three VLANs at most. Please enable VLAN according to actual needs.
Data/Voice/Management,	If the checkboxes on the right of data, voice and management of VLAN1 are selected, it means data messages, voice messages and management messages are subject to the network setting, 802.1Q VLAN1 ID and 802.1P Priority of VLAN1.
802.1Q VLAN ID(0-4095)	Set an ID to identify a VLAN based on 802.1Q protocol.
802.1p Priority (0-7)	Set the priority of a VLAN based on 802.1P protocol.
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】: User needs to restart the gateway for the configurations to take effect.

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

3.4.3 DHCP Option (Routing mode)

On the following interface, you can choose the source of DHCP. Network interfaces include Data VLAN, Manage VLAN and Voice VLAN, while DHCP sources include TFTP Server, SIP Server and Static Route.

DHCP Option

Option 15 (Domain Name)	<input style="width: 80%;" type="text"/>
Option 42 (NTP Servers)	<input type="checkbox"/> Enable
Option 60 (Class Identifier)	<input style="width: 80%;" type="text" value="IAD-160 1.81.01.08"/>
Option 66 (TFTP Server)	<input type="checkbox"/> Enable
Option 120 (SIP Server)	<input type="checkbox"/> Enable
Option 121 (Classless Static Route)	<input type="checkbox"/> Enable

Figure 3.5-4 DHCP Option Interface

3.4.4 QoS

Qos

DSCP code point is used for diffserv setting. It utilizes the first 6 bits of IP ToS. The default values are EF(184), AF1(1), AF2(2), AF3(3), AF4(4), BE(0). You can use different DSCPs for voice or data based on the network provider.

Set DSCP Code/IP ToS Enable

3.4.5 LAN QoS

On the **LAN Qos** interface, user can set the priority of each LAN port and limit the incoming rate or outgoing rate of each LAN port.

LAN Qos

LAN Qos Enable

Port	Priority	Flow Control	Incoming Rate Limit	Outgoing Rate Limit
LAN 0	Low	<input type="checkbox"/>	64 kbps	64 kbps
LAN 1	Low	<input type="checkbox"/>	64 kbps	64 kbps
LAN 2	Low	<input type="checkbox"/>	64 kbps	64 kbps
LAN 3	Low	<input type="checkbox"/>	64 kbps	64 kbps

3.4.6 ARP

ARP is address resolution protocol. ARP helps user get the MAC address of a device through its IP address. Under TCP/IP network environment, each host is assigned with a 32-bit IP address, but MAC address needs to be known for message transmission in the physical network. ARP is a tool that converts IP address into MAC address.

The screenshot shows the ARP configuration page. At the top, there is a blue header with the text 'ARP'. Below the header, there is a 'Type' section with two radio buttons: 'Static' (which is selected) and 'Dynamic'. Below this is a table with two columns: 'IP Address' and 'MAC Address'. The table is currently empty, with dashes in both columns. At the bottom right of the table, there is a label 'Total: 0 entry' followed by a small dropdown menu.

Figure 3.7-9 ARP Parameters

3.5 SIP Server

Introduction of SIP Server:

- 1) SIP server is the main component of VoIP network and is responsible for establishing all the SIP calls. SIP server is also called SIP proxy server or register server. Both IPPBX and softswitch can act as the role of SIP server.
- 2) Usually, SIP server does not participate in media processing. Under SIP network, media always use end-to-end negotiating. Simple SIP server is only responsible for the establishment, maintenance and cleaning of sessions, while relatively-complex SIP server (SIP PBX) not only provides basic calling and conversational support, but also offers rich services such as Presence, Find-me and Music On Hold.
- 3) SIP server based on Linux platform, such as: OpenSER、 sipXecx, VoS, Mera etc.
- 4) SIP server based on windows platform, such as :mini SipServer、 Brekeke, VoIPswitch etc.
- 5) Carrier-grade soft switch platform, such as Cisco, Huawei, ZTE etc.

SIP Server	
SIP Server Address	<input type="text" value="192.168.218.200"/>
SIP Server Port (Default: 5060)	<input type="text" value="5060"/>
Registration Expires (Default: 300)	<input type="text" value="300"/> s
Heartbeat	<input type="checkbox"/> Enable
Primary Outbound Proxy	
Primary Outbound Proxy Address	<input type="text"/>
Primary Outbound Proxy Port	<input type="text" value="5060"/>
Secondary Outbound Proxy	
Secondary Outbound Proxy Address	<input type="text"/>
Secondary Outbound Proxy Port	<input type="text" value="5060"/>
Registration	
Retry Interval when Registration failed	<input type="text" value="30"/> s
Registration Limit (counts/time, time: 0 means unlimited)	<input type="text" value="1"/> / <input type="text" value="0"/> s
Send SIP Unregistration Request when the Device Restart	<input type="checkbox"/> Enable
MOH	
MOH Dial Number	<input type="text" value="~~mh~u"/>
SIP Transport Type	
	<input type="text" value="UDP"/>
Local SIP Port	
Use Random Port	<input type="checkbox"/> Enable
SIP UDP/TCP Local Port	<input type="text" value="5060"/>
SIP TLS Local Port	<input type="text" value="5061"/>

Figure 3.8-1 Configuration Interface for SIP Server

Explanation for SIP parameters:

Primary SIP Server Address	The IP address or domain name of the primary SIP server. They are provided by VoIP service provider.
Primary SIP Server port	The Service port of the primary SIP server. It is 5060 by default.
Registration Expires	It is used to avoid excessively frequent registrations. When the time that is set expires, terminals will send register request to the

	primary SIP server. The time is 1800s by default.
Heartbeat	Heartbeat is used to check the connection between terminal and SIP server.
Secondary SIP Server address	The IP address or domain name of the backup SIP server. They are 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, terminals will send register request to the backup SIP server. The time is 1800s by default.
Secondary SIP heartbeat	Heartbeat is used to check the connection between terminal and SIP server.
Outbound Proxy Address	Outbound proxy IP address or domain name provided by VoIP service provider.
Outbound Proxy Port	Default outbound proxy port is 5060.
Retry Interval when Registration failed	The retry interval time 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 and Auto. Default: UDP.
Use Random Port	The SIP port for providing services for terminal is chosen by random.
SIP Local Port	Default SIP local service port is 5060.

3.6 IP Profile

On the following interface, you can configure IP profiles which can be used on the Port configuration, IP trunk configuration as well as call & routing configuration.

IP Profile - Add

Index

Description

SIP Server

SIP Server Address

SIP Server Port (Default: 5060)

Registration Expires (Default: 300) s

Heartbeat Enable

Primary Outbound Proxy

Primary Outbound Proxy Address

Primary Outbound Proxy Port (Default: 5060)

Secondary Outbound Proxy

Secondary Outbound Proxy Address

Secondary Outbound Proxy Port (Default: 5060)

MOH Enable

MOH Dial Number

Digit Map

Match Failed(When the registration is successful)

Digit Map

Service Parameter

Echo Cancel Tail ms

SIP Compatibility

PRACK(RFC3262) Enable

PRACK Only for 18x with SDP Enable

Early Media Enable

Early Answer Enable

DTMF Parameter

DTMF Method

RFC2833 Payload Type Preferred(Incoming Call)

RFC2833 Payload Type

DTMF Gain

RTP Event of Flash

Preferred Vocoder

Codecs Preferred

	Coder Name	Payload Type	Packetization Time(ms)	Rate(kbps)	Silence Suppression
1	<input type="text" value="G.711U"/>	<input type="text" value="0"/>	<input type="text" value="20"/>	<input type="text" value="64"/>	<input type="text" value="Disable"/>
2	<input type="text" value="G.711A"/>	<input type="text" value="8"/>	<input type="text" value="20"/>	<input type="text" value="64"/>	<input type="text" value="Disable"/>
3	<input type="text" value="G.729"/>	<input type="text" value="18"/>	<input type="text" value="20"/>	<input type="text" value="8"/>	<input type="text" value="Disable"/>
4	<input type="text" value="G.723"/>	<input type="text" value="4"/>	<input type="text" value="30"/>	<input type="text" value="63"/>	<input type="text" value="Disable"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Encryption Configuration

SIP Encrypt

RTP Encrypt

Encrypt Mode

3.7 TEL Profile

On the following interface, you can configure Tel profiles which can be used on the Port configuration, IP trunk configuration as well as call & routing configuration.

Tel Profile - Add

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Line Parameter	
Work Mode	<input type="text" value="Voice and Fax"/>
Config Mode(Gain)	<input type="radio"/> Basic <input checked="" type="radio"/> Advanced
Tx Gain	<input type="text" value="0dB"/>
Rx Gain	<input type="text" value="+2dB"/>
Fax Config	
Fax Mode	<input type="text" value="T.38"/>
ECM	<input type="checkbox"/> Enable
Rate	<input type="text" value="14400 bps"/>
Tone Detection by	<input type="text" value="Local"/>
Switch into Fax Mode When Detected CNG or CED	<input checked="" type="checkbox"/>

3.8 Port

On this interface, you can configure the port information.

Port Add

Port	<input style="width: 80%;" type="text" value="0"/>
Disable Port	<input type="checkbox"/>
Registration	<input checked="" type="checkbox"/> Enable
IP Profile	<input style="width: 80%;" type="text" value="0 <default>"/>
Tel Profile	<input style="width: 80%;" type="text" value="0 <default>"/>
Display Name	<input style="width: 80%;" type="text"/>
SIP User ID	<input style="width: 80%;" type="text"/>
Authenticate ID	<input style="width: 80%;" type="text"/>
Authenticate Password	<input style="width: 80%;" type="text"/>
Offhook Auto-Dial	<input style="width: 80%;" type="text"/>
Auto-Dial Delay Time	<input style="width: 80%;" type="text"/> s

Figure 3.9-1 Port Configuration Interface

Explanations for port parameters:

Port	Port number
Disable port	Whether to disable port temporarily
Registration	Whether to enable registration for the port
IP Profile	Choose an IP profile
Tel Profile	Choose a Tel profile
Display name	It is used to identify the SIP account
SIP User ID	User account information provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Authenticate ID	SIP service subscriber's authenticate ID used for authentication. It can be identical to or different from SIP User ID.
Authenticate password	SIP password which registers to soft switch/SIP server

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.

3.9 Advanced

3.9.1 Line Parameter

Line Parameter

Call Progress Tone UK ▼

Ring Back Tone 400,180,450,180,400,200,400,2000

Busy Tone 400,180,400,630,375,375,0,0

Dial Tone 350,180,440,180,0,0,0,0

Call Waiting Tone

Call Waiting Tone Duration 800 ms

Call Waiting Tone Gap 2000 ms

Call Waiting Tone Repeat Count 5

Auto Gain Control Enable

Line Parameter(Default Tel Profile Parameter)

Work Mode Voice and Fax ▼

Voice Output Mode Telephone Headset

Config Mode(Gain) Basic Advanced

Tx Gain 0dB ▼

Rx Gain +2dB ▼

FAX Parameter

Fax Mode T.38 ▼

ECM Enable

Rate 14400 bps ▼

Tone Detection by Local ▼

Switch into Fax Mode When Detected CNG or CED

3.9.2 FXO Parameters

FXO Parameter	
Incoming Call from PSTN	
Configuration by FXO	<input checked="" type="checkbox"/> Enable
Detect CID	After Ring
Send Original CID when Call from PSTN	<input checked="" type="checkbox"/> Enable
Format of "From" field when CID is Available	Name/CID
Format of "From" field when CID is Unavailable	Display/User ID
CID : Calling Number Name : Calling Name	
FXO Keep Onhook until Callee Answered	<input checked="" type="checkbox"/> Enable
Interval of Offhook and Onhook When Callee Rejected	600 ms
Allow Call to SIP Server without Registration	<input checked="" type="checkbox"/> Enable
Outgoing Call to PSTN	
Hook Flash	<input checked="" type="checkbox"/> Enable
Called Number Preferred	P-Called-Party-ID Header
One Stage Dialing	<input checked="" type="checkbox"/> Enable
Add '#' As Ending Key	<input checked="" type="checkbox"/> Enable
Offhook Delay	400 ms
Dial Delay	200 ms
Answer to Caller when Polarity Reversal Detected	<input checked="" type="checkbox"/> Enable
Delay Time after FXO Offhook	2 s
Dial Mode	DTMF
Onhook when	
Busy Tone Detected	<input checked="" type="checkbox"/> Enable
Current Detected	<input type="checkbox"/> Enable
Current Disconnect Threshold	200 ms
DC Impedance	50 Ohm
Busy Tone Detect	
Cadence	0,0,0,0,0,0,0,0
Cadence Count	4
Delta	50
On->Off Energy Threshold	-34
Off->On Energy Threshold	-30
Acim	(0)600 Ohm
Hybrid	0

Figure 3.10-1 Configuration Interface for FXO Parameters

3.9.3 Media Parameter

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

Media Parameter

Use Random Port Enable

RTP Start Port

UDP Checksum Validation Enable

SRTP Mode

DTMF Parameter

DTMF Method

RFC2833 Payload Type Preferred(Incoming Call)

RFC2833 Payload Type

DTMF Gain

DTMF Send Cadence

RTP Event of Flash

Preferred Vocoder

	Coder Name	Payload Type	Packetization Time(ms)	Rate(kbps)	Silence Suppression
1st	<input type="text" value="G.711U"/>	<input type="text" value="0"/>	<input type="text" value="20"/>	<input type="text" value="64"/>	<input type="text" value="Disable"/>
2nd	<input type="text" value="G.711A"/>	<input type="text" value="8"/>	<input type="text" value="20"/>	<input type="text" value="64"/>	<input type="text" value="Disable"/>
3rd	<input type="text" value="G.729"/>	<input type="text" value="18"/>	<input type="text" value="20"/>	<input type="text" value="8"/>	<input type="text" value="Disable"/>
4th	<input type="text" value="G.723"/>	<input type="text" value="4"/>	<input type="text" value="30"/>	<input type="text" value="63"/>	<input type="text" value="Disable"/>
5th	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Codecs Preferred

Figure 3.10-2 Configuration Interface for Media Parameters

Explanation of media parameters:

Use Random Port	If this parameter is enabled, the gateway will choose a port by random as the start port for RTP.
RTP Start Port	Default RTP start port is 8000
DTMF Method	Include SINGAL, INBAND and RFC2833
RFC2833 Payload Type	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 gateway will send flash event to remote terminal, and thus user does need to handle it locally

Coder Name	The gateway supports G729, G711U, G711A and G723. 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.

3.9.4 Service Parameter

Service Parameter

Timeout for Off-hook	<input type="text" value="10"/>	s
Timeout for Dialing	<input type="text" value="4"/>	s
Timeout for Answer(Outgoing Call)	<input type="text" value="55"/>	s
Timeout for Answer(Incoming Call)	<input type="text" value="55"/>	s
No RTP Detected	<input type="checkbox"/> Enable	
Period without RTP Packet	<input type="text" value="60"/>	s
IP-to-IP Call	<input checked="" type="checkbox"/> Enable	
Only Accept Calls from ACL(SIP Server or IP Trunk)	<input type="checkbox"/> Enable	
Anonymous Call	<input type="checkbox"/> Enable	
Reject Anonymous Call	<input type="checkbox"/> Enable	
Call Confirm Tone	<input type="checkbox"/> Enable	
Howl Tone Interval After Busytone(0:No Send)	<input type="text" value="0"/>	s
Domain Query Type	<input type="text" value="A Query"/>	
DNS Cache	<input checked="" type="checkbox"/> Enable	
Domain Re-resolution Inteval(0-3600,0:No Refresh)	<input type="text" value="0"/>	s
Echo Cancel Tail	<input type="text" value="128"/>	ms

Digit Map

Match Failed(When the registration is successful)

```
[*#]T[*#][*#]*x.T]**x.#[*#]xx#]*xx#[[*#][0-9*#]x[0-9*].x#|x.#|x.T
```

3.9.5 SIP Compatibility

SIP Compatibility	
RFC3407 Support	<input type="checkbox"/> Enable
URI includes "user=phone"	<input type="checkbox"/> Enable
INVITE with "P-Preferred-Identity" Header (RFC3325)	<input type="checkbox"/> Enable
Value of "Refer To" refers to "Contact"	<input type="checkbox"/> Enable
Third Party Do Not Send 18x Response	<input type="checkbox"/> Enable
REFER Delay	<input type="checkbox"/> Enable
Send BYE when Recv REFER Response(Unattended)	<input type="checkbox"/> Enable
Send New REGISTER when Recv 423 Response	<input checked="" type="checkbox"/> Enable
Cseq Start with 1	<input type="checkbox"/> Enable
Forbid Invalid m=line in reINVITE	<input type="checkbox"/> Enable
Call Waiting Response Code	180 Response ▾
RTP Mode in SDP when Call Holding	sendonly ▾
Support Call Waiting of Huawei IPPBX	<input type="checkbox"/> Enable
Accept Orphan 200 Ok	<input type="checkbox"/> Enable
Called Number Preferred	P-Called-Party-ID Header ▾
Caller-ID Preferred	P-Asserted-Identity Header ▾
Report SDP Whatever	<input type="checkbox"/> Enable
18x Response Preferred	18x Response with SDP ▾
FlashHook Operation Mode	Mode one ▾
Attended Transfer Trigger	Onhook ▾
Multipart Payload Support	<input type="checkbox"/> Enable
Local Extension is Preferred(Tel in)	<input type="checkbox"/> Enable
PRACK(RFC3262)	<input type="checkbox"/> Enable
PRACK Only for 18x with SDP	<input type="checkbox"/> Enable
Early Media	<input checked="" type="checkbox"/> Enable
Early Answer	<input type="checkbox"/> Enable
Session Timer(RFC4028)	<input type="checkbox"/> Enable
Session-Expires	1800 s
Min-SE	1800 s
Session Refresh Method	INVITE ▾

T1	500	ms
T2	4000	ms
T4	5000	ms
Max Timeout	32000	ms
Heartbeat Interval(1 - 3600)	10	s
Heartbeat Timeout(4 - (64*T1-1))	16	s
Username of OPTION(Heartbeat) for 'SIP Server'	heartbeat	
Username of OPTION(Heartbeat) for 'IP Trunk'	heartbeato	
Release all call when Heartbeat Timeout	<input type="checkbox"/> Enable	

Figure 3.10-3 SIP Parameter Configuration Interface

Explanation of SIP parameters:

SUBSCRIBE for MWI (Message Waiting Indicator)	Whether to enable 'voicemail message waiting indicator'; it is realized in the way of NOTIFY
MWI Subscription Expires	MWI subscription expiry time; Default value is 3600s.
Voicemail User ID	The user ID for access to voicemail box
RFC3407 Support	Whether to enable RFC3407 support.
IP-to-IP Call	If this parameter is enabled, user can dial IP address through a phone to call destination gateway.
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 gateway 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	'#' 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.
Value of "Refer To" refers to "Contact"	If this parameter is enabled, 'contract header' needs to be filled in in the 'refer to' field of a SIP message.
Third Party Do Not Send 18x	If this parameter is enabled, the third party will not send 18x response

Response	during a 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.
Implicit Subscribe	If this parameter is enabled, the gateway will accept implicit subscription.
CSeq Start with 1	If this parameter is enabled, the value of CSeq starts with '1'.
Forbid Invalad m=line in reINVITE	If this parameter is enabled, the gateway will prevent 'invalid m=line' from being carried in the SDP of re-INVITE.
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 gateway will support call waiting of Huawei IPPBX.
Accept Orphan 200 OK	If this parameter is enabled, the gateway will support different 'to-tag 200 OK' in a INVITE session
Domain Query Type	There are two modes: A QUERY and SRV QUERY. Default is 'A QUERY'.
Domain Re-resolution Interval	Default 0: forbidden
DNS cache	If this parameter is enabled, the gateway will cache the DNS query results.
Early Media	Support the receiving of Early Media.
PRACK(RFC3262)	Support reliable transmission of provisional response
PRACK Only for 18x with SDP	Send PRACK only when there's SDP in 18x response
Early Answer	If this parameter is enabled, SDP will be contained in 18x
Session Timer (RFC4028)	Whether to enable 'session timer', default value is ' no'.
Session-Expires	The Session-Expires header field conveys the session interval for a SIP session.
Min-SE	Min-SE header field indicates the minimum value for the session interval.
T1	T1 timer of SIP protocol, default is 500ms
T2	T2 timer of SIP protocol, default is 400ms
T4	T4 timer of SIP protocol, default is 500ms

Max Timeout	The max timeout of sending or receiving, default is 32s
Heartbeat Interval	Default is 10s.
Heartbeat Timeout	Default to 16s
Username of OPTION(Heartbeat) for "SIP Server"	The user ID part of OPTION SIP message in the heartbeat request for SIP server

3.9.6 NAT Parameter

If NAT Traversal is enabled, the IP address of SIP extension in LAN (local-area network) will be turned into the outbound IP address of the public network, thus making NAT traversal possible.

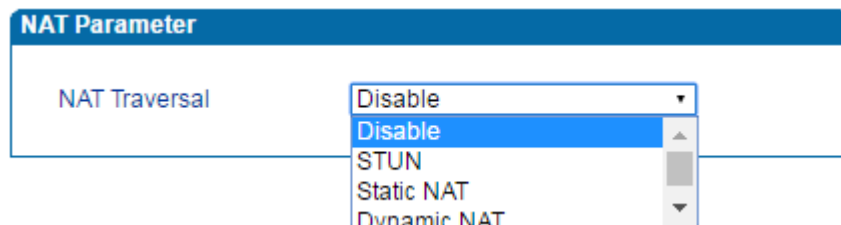


Figure 3.10-4 Configuration Interface for NAT Parameter

STUN (Simple Traversal of UDP over NATs): STUN is a lightweight protocol that allows applications to discover the presence and types of NATs as well as 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.

Static NAT: the IP address of the device in the LAN will be changed into the outbound IP address of the public network which is a static IP. The NAT IP will be carried in the SIP messages sent by the device afterwards. If you selected static NAT, you need to enter an IP address (that is the outbound IP address of the public network) manually.

Dynamic NAT: the IP address of the device in the LAN will be changed into the outbound IP address of the public network that is a dynamic IP. The device will check the dynamic IP automatically and will update the IP in the SIP messages sent by itself.

3.9.7 Speed Dial

This function is used under the "two-stage dialing" application scenario. When an inbound call comes into the FXO port of the DAG device, you will hear a PSTN's dialing tone and then you can dial the speed-dial number to let the call goes out. In this case, the original number is replaced by the speed-dial number to save time and trouble.

Speed Dial - Add

Index	0
Speed Dial Number	123
Original Number	13645278963

3.9.8 Feature Code

Please make reference to the Feature Codes interface and the following table.

Inquiry LAN port IP address	Dial*158# to obtain device WAN port IP address
Inquiry WAN port IP address	Dial*159# to obtain device WAN port IP address
Inquiry Phone Number	Dial*114# to obtain port account
Inquiry PortGroup Number	Dial *115# to obtain port group number
Setting IP Mode	*150*0#, means pppmodem, *150*1#, means static IP, *150*2#, means obtain IP address by DHCP, *150*3#, means pppoe.
Network Work Mode	*157*0#, set network work mode to routing mode; *157*1#, set network work mode to bridge mode
Configure IP Address	*152*+IP, set gateway IP address
Network subnet mask configure	*153*+subnet mask, set gateway subnet mask
Network Gateway Configure	*156*+gateway IP, set gateway
Renew DHCP	*193#, set dynamic IP again
Access Web by Wan in Rout Mode	Allow access web through WAN port: *160*1#; don't allow access web through WAN port: *160*0#
Reset Basic Configuration	Dial *165*000000# to restore default username/password and network configuration
Reset Factory Configuration	*166*000000#, reset factory
Restart Device	*111#, restart device
Call holding	During a call, dial*# into call hold. (Recovery the call through hook flash or *#)
Call by IP	Directly dial the end user IP to call
Call Waiting Activate	*51#, enable call waiting function

Call Waiting Deactivate	*50#, forbid call waiting function
Blind Transfer	If the call transfer to 801, first hook flash and then dial the * 87 * 801#
Call Forward Unconditional Activate	*72*+ phone number#, transfer the call from the phone number
Call Forward Unconditional Deactivate	*73#, forbid call forward unconditional
Call Forward Busy Activate	*90*+ forward busy number#
Call Forward Busy Deactivate	*91#, forbid call forward busy
Call Forward No Reply Activate	*92*+ forward no reply number#
Call Forward No Reply Deactivate	*93#, close this function
Do Not Disturb Activate	*78#, enable DND function
Do Not Disturb Deactivate	*79#, close DND function
Dial Voicemail	*200#, visit voice mail box

3.9.9 System Parameter

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

- 1) STUN: 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.
- 2) NTP: Network Time Protocol (NTP) is a computer time synchronization protocol.
- 3) Provision: provision is used to make the gateway automatically upgrade with the latest firmware stored on an http server an ftp server or a tftp server.

System Parameter

Hint Language English ▼

NAT Traversal Disable ▼

NTP Enable

Primary NTP Server Address 10.10.3.146

Primary NTP Server Port 123

Secondary NTP Server Address

Secondary NTP Server Port 123

SYN Interval 3600 s

Time Zone GMT+1:00 (Paris, Berlin, Rome, Brussels) ▼

Daylight Saving Time Enable

Daily Reboot Enable

Reboot Time 0 ▼ : 0 ▼

Summary Config Enable

Summary

WEB Parameter

WEB Port 80

SSL Port 443

Telnet Parameter

Telnet Port 23

Remote Management

Access WEB by WAN Enable

Access WEB by LAN Enable

Access Telnet by WAN Enable

Access Telnet by LAN Enable

Figure 3.10-7 Configuration Interface for System Parameters

Explanation for related parameters:

Hint Language	IVR language of the gateway
NAT Traversal	User can choose 'Disable', 'STUN', 'static NAT' and 'dynamic NAT'.
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 18.145.0.30
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 DAG FXO. Default value is 3600s.
Time Zone	The time zone of the gateway; 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 gateway daily
WEB Port	The web port of the gateway; Default port is 80
Telnet port	Listening port of telnet service; Default port is 23
Access WEB by WAN	Enable or disable 'Access web service from WAN'
Access WEB by LAN	Enable or disable 'Access web service from LAN'
Access Telnet by WAN	Enable or disable 'telnet service from WAN'
Access Telnet by LAN	Enable or disable 'telnet web service from LAN'

3.10 Call & Routing

3.10.1 Wildcard Group

Wildcard Group	
Wildcarded IMPU	Associated IMPU
---	---

Figure 3.11-1 Wildcard Group

3.10.2 Port Group

On the **Port Group** interface, you can group several ports together and then set a strategy for port selection of the group. Parameters of port group include registration, primary display name, primary SIP user id, primary authentication ID and password, secondary display name, secondary SIP user id, secondary authentication ID and password, off-hook auto dial, auto dial delay time, port select and so on.

Port Group Add

Index	<input style="width: 90%;" type="text" value="3"/>
Registration	<input checked="" type="checkbox"/> Enable
Description	<input style="width: 95%;" type="text"/>
Primary Display Name	<input style="width: 95%;" type="text"/>
Primary SIP User ID	<input style="width: 95%;" type="text"/>
Primary Authenticate ID	<input style="width: 95%;" type="text"/>
Primary Authenticate Password	<input style="width: 95%;" type="text"/>
Secondary Display Name	<input style="width: 95%;" type="text"/>
Secondary SIP User ID	<input style="width: 95%;" type="text"/>
Secondary Authenticate ID	<input style="width: 95%;" type="text"/>
Secondary Authenticate Password	<input style="width: 95%;" type="text"/>
Offhook Auto-Dial	<input style="width: 95%;" type="text"/>
Auto-Dial Delay Time	<input style="width: 95%;" type="text"/>
Port Select	<input style="width: 90%;" type="text" value="Cyclic Ascending"/>
Pick Up on Group	<input style="width: 95%;" type="text" value="*#"/>
Port	<input type="button" value="Click to Select Ports for this Group"/>

Figure 3.11-2 Configuration Interface for Port group

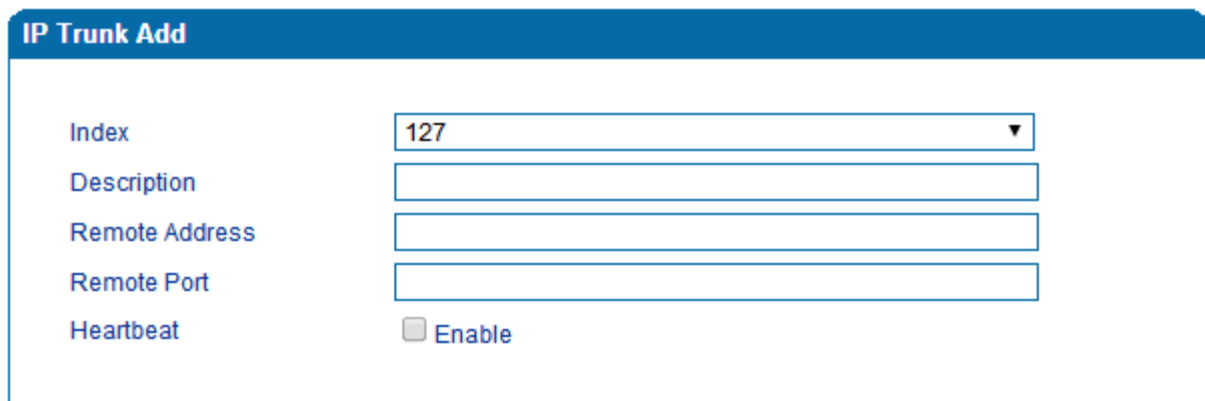
Explanation of related parameters

Index	The NO. of the port group ; It uniquely identifies a route, range from 0-7
Description	The description of the port group; it is used to identify the port group
Primary/Secondary Display Name	Port group display, 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=z9hG4bK776asdhs

	<p>Max-Forwards: 70</p> <p>To: Bob <sip:bob@biloxi.com></p> <p>From: Alice <sip:alice@atlanta.com>;tag=1928301774</p> <p>Here Bob and Alice is the display</p>
Primary/Secondary SIP User ID	User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Primary/Secondary Authenticate ID	SIP service subscriber's authentication ID, it can be identical to or different from SIP User ID.
Primary/Secondary Authenticate Password	Password of SIP user ID
Offhook Auto-Dial	To enter offhook auto-dial number
Auto-dial Delay time	How long auto-dialing will be delayed
Port Select	<p>It specifies the policy for selecting a port for ringing in the port group</p> <ul style="list-style-type: none"> • Ascending: the gateway always selects a port from the minimum number. • Cyclic ascending: the gateway 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 gateway always selects a port from the maximum number. • Cyclic descending: the gateway 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

3.10.3 IP Trunk

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



The image shows a web configuration interface titled "IP Trunk Add". It contains the following fields:

- Index:** A dropdown menu with the value "127" selected.
- Description:** An empty text input field.
- Remote Address:** An empty text input field.
- Remote Port:** An empty text input field.
- Heartbeat:** A checkbox labeled "Enable" which is currently unchecked.

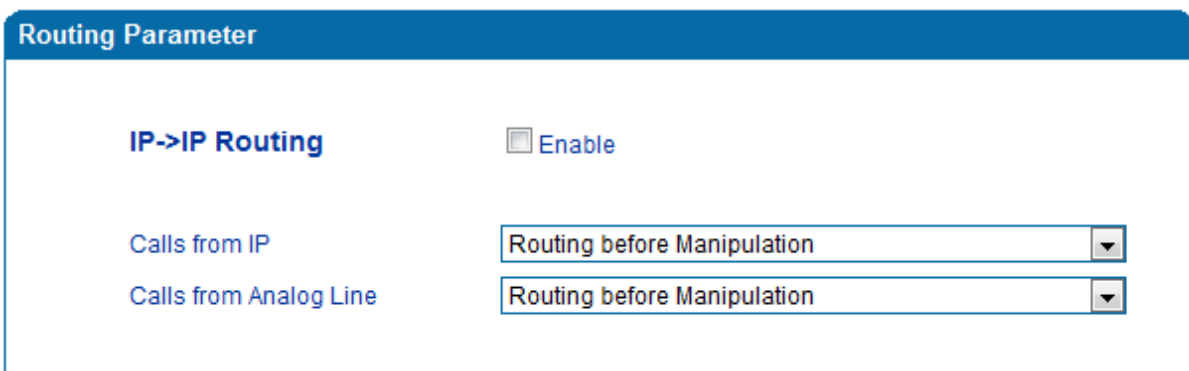
Figure 3.11-3 IP Trunk Configuration Interface

Explanation of related parameters:

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

3.10.4 Routing Parameter

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



The image shows a web configuration interface titled "Routing Parameter". It contains the following fields:

- IP->IP Routing:** A checkbox labeled "Enable" which is currently unchecked.
- Calls from IP:** A dropdown menu with the value "Routing before Manipulation" selected.
- Calls from Analog Line:** A dropdown menu with the value "Routing before Manipulation" selected.

Figure 3.11-4 Configuration Interface for Routing Parameter

3.10.5 IP → Tel Routing

Calls from the IP network to the GSM network is defined as IP → Tel calls, and those calls need to be routed by IP → Tel routing.

The screenshot shows the 'IP->Tel Routing Modify' configuration window. It contains the following fields and options:

- Index:** 127
- Description:** IP_TEL
- Calls from:** Radio buttons for 'IP Trunk' and 'SIP Server'. The 'SIP Server' option is selected. A dropdown menu next to it shows 'Any'.
- Caller Prefix:** 10013
- Callee Prefix:** any
- Calls to:** Radio buttons for 'Port' and 'Port Group'. The 'Port Group' option is selected. A dropdown menu next to it shows '15 <10013>'.

At the bottom of the window are three buttons: 'Save', 'Reset', and 'Cancel'.

Figure 3.11-5 Configuration Interface for IP-Tel Routing

Explanation of related parameters:

Index	IP → Tel Routing priority: from 0 to 127; 0 is the highest priority.
Description	It is used to identify the IP → Tel routing
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

3.10.6 Tel-IP/Tel Routing

Calls from the GSM network to the IP network are defined as Tel → IP calls, and those calls need to be routed by Tel → IP routing. Calls from a GSM network to another GSM network are defined as Tel → Tel calls, and those calls need to be routed by Tel → Tel routing.

Tel->IP/Tel Routing Add

Index: 127

Description: [Empty]

Calls from:

- Port: 0
- Port Group: [Empty]

Caller Prefix: [Empty]

Callee Prefix: [Empty]

Calls to:

- Port: [Empty]
- Port Group: [Empty]
- IP Trunk: [Empty]
- SIP Server

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

Explanation of related parameters:

Index	The index of this Tel →IP/Tel routing, from 0 to 127. Each index cannot be used repeatedly. Routing priority: 0 is the highest priority.
Description	It is used to identify the routing
Calls From	Tel →IP 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	Calls are routed to a port, port group, IP trunk or SIP server

Internal Call Function: When there is no SIP server for registration, calls can be given from one FXO port to another FXO port of a same access gateway of DAG1000, DAG2000, DAG2500 and DAG3000.

3.11 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.

3.11.1 IP -> Tel Callee

On the following interface, you can set a manipulation rule to change callee numbers of IP → Tel calls.

IP->Tel Callee Add

Index	<input style="width: 90%;" type="text" value="127"/>
Description	<input style="width: 90%;" type="text"/>
Calls from	<input type="radio"/> IP Trunk <input style="width: 50%;" type="text" value="Any"/>
	<input checked="" type="radio"/> SIP Server
Caller Prefix	<input style="width: 90%;" type="text"/>
Callee Prefix	<input style="width: 90%;" type="text"/>
Calls to	<input checked="" type="radio"/> Port <input style="width: 50%;" type="text" value="0"/>
	<input type="radio"/> Port Group <input style="width: 50%;" type="text"/>
Stripped Digits from Left	<input style="width: 90%;" type="text"/>
Stripped Digits from Right	<input style="width: 90%;" type="text"/>
Prefix to Add	<input style="width: 90%;" type="text"/>
Suffix to Add	<input style="width: 90%;" type="text"/>
Number of Digits to Leave from Right	<input style="width: 90%;" type="text"/>

Figure 3.12-1 Add IP -> IP Callee

Index	The index of this manipulation, from 0 to 127. Each index cannot be used repeatedly. 0 is the highest priority
Description	Name of this IP ->Tel manipulation name
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 routing. 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 routing. If called number is 008675526456659, the called prefix can be 0086755 or 00., "any" means match any called number
Calls to	Determine the port or port group to which the call is routed.
Stripped Digits from Left	The number of digits which are lessened from the left of the callee number

Stripped Digits from Right	The number of digits which are lessened from the right of the callee number
Prefix to Add	The prefix added to the callee number after its digits are lessened.
Suffix to Add	The suffix added to the callee number after its digits are lessened.
Number of Digits to Leave from Right	The number of the retained digits which. are counted from the right of the callee number

3.11.2 Tel -> IP/Tel Caller

On the following interface, you can set a manipulation rule to change caller numbers of Tel → IP/Tel calls.

Tel->IP/Tel Caller Add

Index	<input style="width: 90%;" type="text" value="127"/>
Description	<input style="width: 90%;" type="text"/>
Calls from	<input checked="" type="radio"/> Port <input style="width: 50px;" type="text" value="0"/> <input type="radio"/> Port Group <input style="width: 50px;" type="text"/>
Caller Prefix	<input style="width: 90%;" type="text"/>
Callee Prefix	<input style="width: 90%;" type="text"/>
Calls to	<input type="radio"/> Port <input style="width: 50px;" type="text" value="0"/> <input type="radio"/> Port Group <input style="width: 50px;" type="text"/> <input type="radio"/> IP Trunk <input style="width: 50px;" type="text" value="Any"/> <input checked="" type="radio"/> SIP Server
Stripped Digits from Left	<input style="width: 90%;" type="text"/>
Stripped Digits from Right	<input style="width: 90%;" type="text"/>
Prefix to Add	<input style="width: 90%;" type="text"/>
Suffix to Add	<input style="width: 90%;" type="text"/>
Number of Digits to Leave from Right	<input style="width: 90%;" type="text"/>

Figure 3.12-2 Add Tel -> IP Caller

Configuration parameters are the same with those of 'IP->Tel Callee'.

3.11.3 Tel-IP/Tel Callee

On the following interface, you can set a manipulation rule to change callee numbers of Tel → IP/Tel calls.

Tel->IP/Tel Callee Add	
Index	127
Description	
Calls from	<input checked="" type="radio"/> Port 0 <input type="radio"/> Port Group
Caller Prefix	
Callee Prefix	
Calls to	<input type="radio"/> Port 0 <input type="radio"/> Port Group <input type="radio"/> IP Trunk Any <input checked="" type="radio"/> SIP Server
Stripped Digits from Left	
Stripped Digits from Right	
Prefix to Add	
Suffix to Add	
Number of Digits to Leave from Right	

Figure 3.12-3 Add Tel-IP Callee

Configuration parameters are the same with those of 'Tel->IP Caller'.

3.12 Routing rule examples

3.12.1 Route any calls from any IP to specific port

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

IP->Tel Routing Add

Index	<input type="text" value="127"/>
Description	<input type="text" value="any"/>
Calls from	<input checked="" type="radio"/> IP Trunk <input type="text" value="Any"/> <input type="radio"/> SIP Server
Caller Prefix	<input type="text" value="any"/>
Callee Prefix	<input type="text" value="any"/>
Calls to	<input checked="" type="radio"/> Port <input type="text" value="0"/> <input type="radio"/> Port Group <input type="text"/>

NOTES:

1. 'any' in 'Callee Prefix' or 'Caller Prefix' means wildcard string.

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

3.12.2 Route any calls from any IP to specified port group

► Create port group

Before we can route calls to a port group, create the port group first as below. On the **Call & Routing → Port Group**, click **Add** to create a new port group, and then click **Click to Select Ports to This Group**.

Port Group Add

Index: 7

Registration: Enable

Description: [Empty]

Select Port for this Group

<input checked="" type="checkbox"/> Port 0(FXS)	<input checked="" type="checkbox"/> Port 1(FXS)	<input type="checkbox"/> Port 2(FXS)	<input type="checkbox"/> Port 3(FXS)
<input type="checkbox"/> Port 4(FXS)	<input checked="" type="checkbox"/> Port 5(FXS)	<input checked="" type="checkbox"/> Port 6(FXS)	<input checked="" type="checkbox"/> Port 7(FXS)
<input type="checkbox"/> Port 8(FXS)	<input type="checkbox"/> Port 9(FXS)	<input type="checkbox"/> Port 10(FXS)	<input type="checkbox"/> Port 11(FXS)
<input type="checkbox"/> Port 12(FXS)	<input type="checkbox"/> Port 13(FXS)	<input type="checkbox"/> Port 14(FXS)	<input type="checkbox"/> Port 15(FXS)

Buttons: Select All, Select Inver, Clean, Cancel, Ok

Ports for this Group: [Highlighted]

Port 0, port 1, port 5, port 6 and port7 are assigned to port group 7.

► Route any calls to the port group

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

IP->Tel Routing Add

Index: 127

Description: any to port group

Calls from: IP Trunk (Any) SIP Server

Caller Prefix: any

Callee Prefix: any

Calls to: Port (0) Port Group (7 <port group 1>)

Buttons: Save, Reset, Cancel

NOTES:

1. 'any' in 'Callee Prefix' or 'Caller Prefix' means wildcard string.

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

3.12.3 Route any calls from any port to specific SIP IP trunk

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

IP Trunk Add

Index	<input type="text" value="127"/>
Description	<input type="text" value="To_Elastix"/>
Remote Address	<input type="text" value="172.16.125.125"/>
Remote Port	<input type="text" value="5060"/>
Heartbeat	<input type="checkbox"/> Enable

After IP Trunk is created, check the following configuration:

IP Trunk					
	Index	Description	Remote Address	Remote Port	Heartbeat
<input type="checkbox"/>	127	To_Elastix	172.16.125.125	5060	Disable

Total: 1 entry Page 1 ▼

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

Create Tel -> IP routing rule

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

Tel->IP/Tel Routing Add

Index	<input type="text" value="127"/>	
Description	<input type="text" value="Tel to IP trunk"/>	
Calls from	<input checked="" type="radio"/> Port <input type="text" value="Any"/>	
	<input type="radio"/> Port Group <input type="text" value="7 <port group 1>"/>	
Caller Prefix	<input type="text" value="any"/>	
Callee Prefix	<input type="text" value="any"/>	
Calls to	<input type="radio"/> Port <input type="text" value="0"/>	
	<input type="radio"/> Port Group <input type="text" value="7 <port group 1>"/>	
	<input checked="" type="radio"/> IP Trunk <input type="text" value="127 <To_Elastix>"/>	
	<input type="radio"/> SIP Server	

NOTES:

1. 'any' in 'Callee Prefix' or 'Caller Prefix' means wildcard string.

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

3.13 Management

3.13.1 TR069

ACS URL (auto-configuration server URL address) is provided by service provider. The ACS URL generally starts with http:// or https://, while username and password are used for ACS authentication.

TR069 Parameter

TR069 Enable

ACS Configuration

ACS URL

User Name

Password

Periodic Inform Enable

Periodic Inform Interval s

Connect Request

User Name

Password

Port

Figure 3.14-1 TR069 Parameters

3.13.2 SNMP (Simple Network Management Protocol)

SNMP Parameters:

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

SNMP Parameter

Snmp
 Enable

Snmp Version
v1

Community Configuration

	Community	Source
1st	<input type="text"/>	<input type="text"/>
2nd	<input type="text"/>	<input type="text"/>
3rd	<input type="text"/>	<input type="text"/>

Note: Value of 'Source' is 'default' or IP Address(eg:192.168.1.1)!

Group Configuration

	Group	Community
1st	<input type="text"/>	<input type="text"/>
2nd	<input type="text"/>	<input type="text"/>
3rd	<input type="text"/>	<input type="text"/>

View Configuration

	ViewName	ViewType	ViewSubtree	ViewMask
1st	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2nd	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3rd	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Note: Value style of 'ViewSubtree' is 'x.x.x.x.x'(multi-nodes) or '.x'(one node).

Access Configuration(v1/v2c)

	Group	Read	Write	Notify
1st	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2nd	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3rd	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Note: The value of Read/Write/Notify references to 'ViewName' in View Configuration. Access Configuration is base on Group Configuration and View Configuration.

Trap Configuration

	Trap Type	Trap IP	Trap Port	Trap Community
1st	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 3.14-2 SNMP Parameters

User configuration is only available on SNMP v3.

SNMP Version

User Configuration

User AuthType AuthPassword PrivacyType PrivacyPassword

1st

Notice:The length of AuthPassword and PrivacyPassword are more than 8!

Group configuration

Group: community group name which consist of character string.

Community: let community join the community group which configured above

Group Configuration

	Group	Community
1st	<input type="text" value="grouppublic"/>	<input type="text" value="public"/>
2nd	<input type="text"/>	<input type="text"/>
3rd	<input type="text"/>	<input type="text"/>

Trap configuration

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

Trap Configuration

	TrapFlag	TrapIP	TrapPort	TrapCommunity
1st	<input type="text" value="v2c"/>	<input type="text" value="172.16.22.222"/>	<input type="text" value="162"/>	<input type="text" value="public"/>

3.13.3 Syslog

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

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

- SD, hardware debug
- SIP, SIP signaling trace
- STUN, STUN logs
- ECC, detail information of call control module
- RE, the common communication module for SCP and SIM
- SCP, the communication protocol between gateway and cloud server

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

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

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

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

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

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

Server Syslog:

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

Syslog Parameter

Local Syslog Enable

Server Address

Server Port

Syslog Level

Signal Log Enable

Media Log Enable

System Log Enable

Management Log Enable

CDR Enable

Server Syslog Enable

Figure 3.14-3 Syslog Parameter

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

3.13.4 Provision

Provision is used to make the DAG FXO automatically upgrade with the latest firmware stored on an http server an ftp server or a tftp server.

Provision

URL

Check Interval s

Account

Password

Proxy Domain

Proxy Port

Proxy Account

Proxy Password

Install updates automatically(recommended) Enable

Figure 3.14-4 Provision

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

3.13.5 Cloud server

You can register the gateway to cloud server, and then the gateway will be managed by cloud server.

Figure 3.14-5 Cloud Server

Explanation of related parameters

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

3.13.6 User manage

Click **Management** → **User Manager**, and you can modify the username name. Meanwhile, if you are the administrator of the device, you can assign a role (a user or a guest) for other users. That is to say, this function allows you to create multiple users with multiple levels of privileges. The device supports to create admin, user and guest privileges for different users.

User			
	User Name	Group	Enabled
<input type="checkbox"/>	admin	Admin	enable

Add a User

User Name

Group

Enabled

Password

Confirm Password

3.13.7 Remote server

Remote server is a type of cloud service which develop for Dinstar devices, aim to helps user manage web and telnet remotely. Please provide your device's SN and contact with support to get server link.

Remote Server

Server URL/IP

Server Port

3.13.8 Record Parameter

On the following interface, you can fill in the IP address of the recording server and then you record the conversations of calls.

Record Parameter

RCD	<input checked="" type="checkbox"/> Enable
Server Address	<input type="text"/>
Rcd Port	<input type="text" value="2999"/>
Rcd Period Select	<input type="text" value="Disable"/>

3.13.9 Radius Parameter

Radius Parameter

Radius	<input checked="" type="checkbox"/> Enable
Local Port	<input type="text" value="1645"/>
Device Behavior Upon RADIUS Timeout	<input type="text" value="Verify Access Locally"/>
Server IP	<input type="text" value="172.16.0.5"/>
Server Auth Port	<input type="text" value="1645"/>
Server Key	<input type="text" value="*****"/>

3.13.10 Action URL

Action URL allows VoIP platforms to obtain the status and other information of the DAG device and report the information of the DAG device to other devices.

Startup: To report the startup of the DAG device.

Offhook: To report the Offhook status of an FXO port.

Onhook: To report the onhook status of an FXO port.

Incoming call: an incoming call is received by an FXO port of the DAG device.

Outgoing call: a call is going out from an FXO port of the DAG device.

Call built: a call is being establishing in an FXO port of the DAG device.

Call Terminate: a call is terminated in an FXO port of the DAG device.

Action URL Configuration

Event	Action URI
Startup	<input type="text"/>
Offhook	<input type="text"/>
Onhook	<input type="text"/>
Incoming Call	<input type="text"/>
Outgoing Call	<input type="text"/>
Call Build	<input type="text"/>
Call Terminate	<input type="text"/>
Register Status	<input type="text"/>
Heartbeat	<input type="text"/>
Heartbeat Interval	<input type="text" value="10"/> s

3.14 Security

3.14.1 WEB ACL

ACL (Access Control List) for WEB is used to configure IP addresses (users) that are allowed to access the WEB page of the gateway. The IP address list can't be null once ACL is enabled.

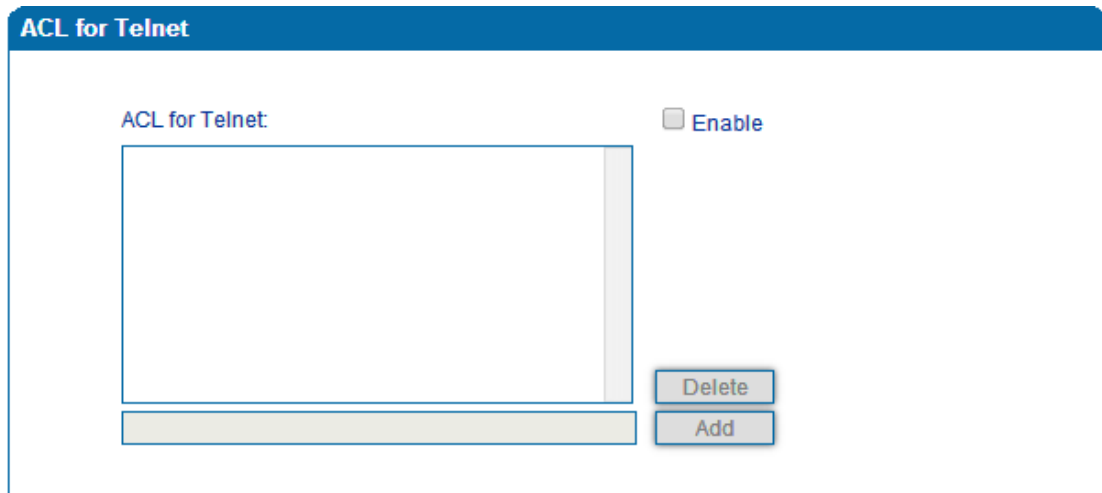
ACL

ACL for WEB: Enable

Figure 3.15-1 ACL for WEB

3.14.2 Telnet ACL

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



ACL for Telnet

ACL for Telnet:

Enable

Delete

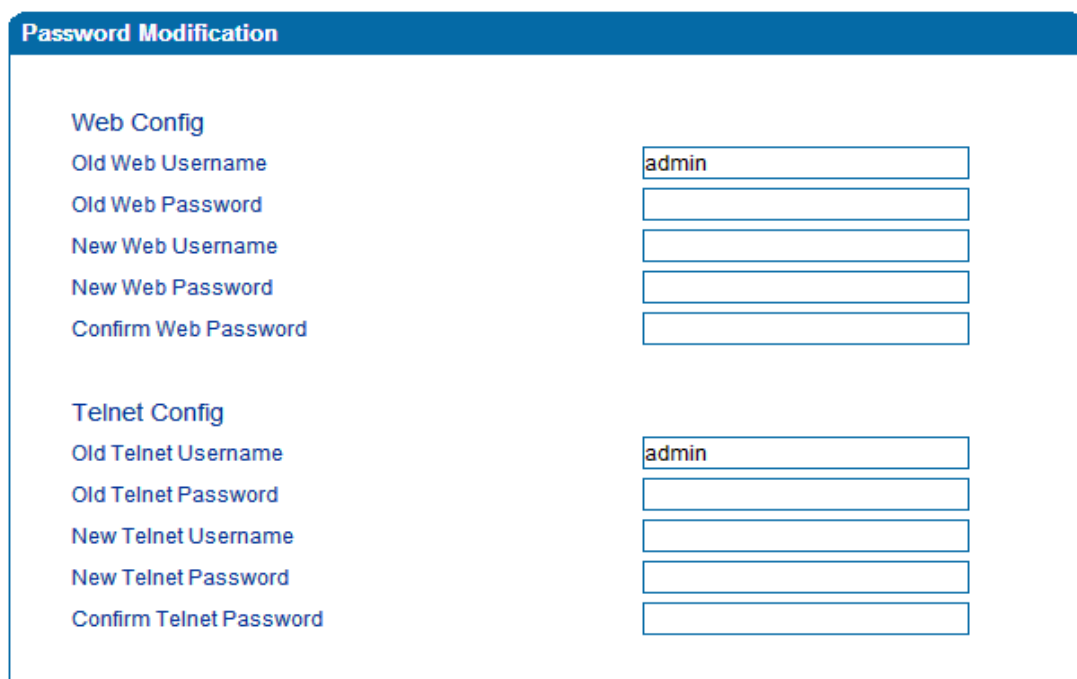
Add

Figure 3.15-2 ACL for Telnet

3.14.3 Passwords

On the following interface, user can configure or modify the username and password for access the WEB interface and the Telnet interface.

Note: Both the username and password of Web and Telnet are 'admin' and 'admin'.



Password Modification

Web Config

Old Web Username: admin

Old Web Password:

New Web Username:

New Web Password:

Confirm Web Password:

Telnet Config

Old Telnet Username: admin

Old Telnet Password:

New Telnet Username:

New Telnet Password:

Confirm Telnet Password:

Figure 3.15-3 Password Modification

3.14.4 Encrypt

On the following interface, you can enable or disable SIP encryption and RTP encryption. The encryption mode is defaulted as VOS RC4.

Encryption Configuration	
SIP Encrypt	Enable ▼
RTP Encrypt	Disable ▼
Encrypt Mode	VOS RC4 ▼

save

3.15 Tools

3.15.1 Firmware upload

Firmware upload steps:

Step 1.

Check the current firmware version on the ***System Information page***

Current Software Version	IAD-160 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40
Backup Software Version	IAD-160 1.81.10.06 PCB 13 LOGIC 0 BIOS 1, 2018-07-30 16:44:40
DSP Version	ARM_32_9 Mar 9 2018 10:46:34

Figure 3.16-1 Firmware Version

Step 2.

Prepare firmware package. The most important is that the package must match with the existing version. Package version consists of the following parts:

2.81.xx.xx

01/02 is vendor name

81 is hardware version, xx.xx is version number

Step 3.

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

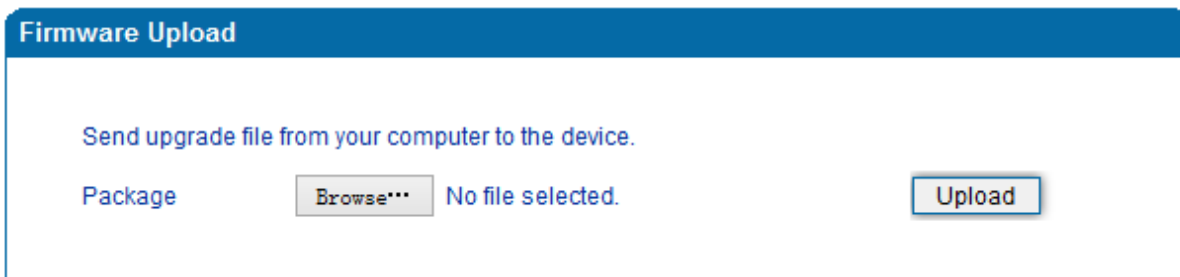


Figure 3.16-2 Firmware Upload

Step 4.

Keep waiting until it prompts 'Software loaded successfully!'

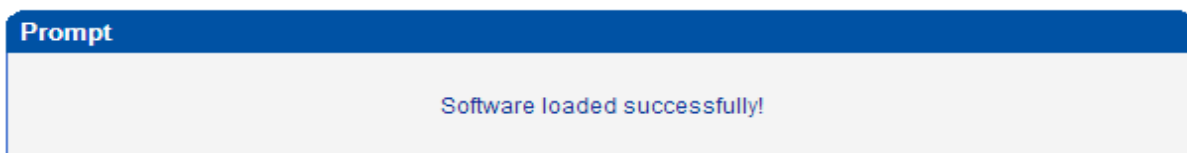


Figure 3.16-3 Successful Firmware Upload

Step 5.

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

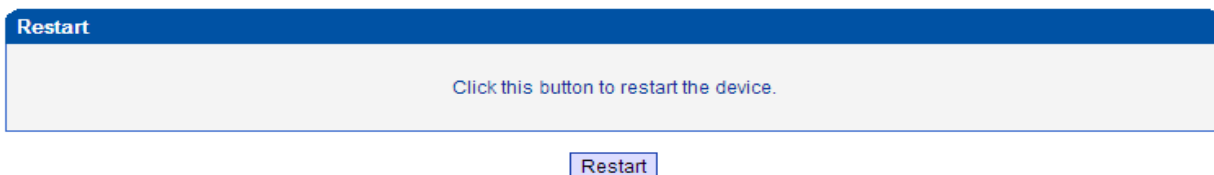
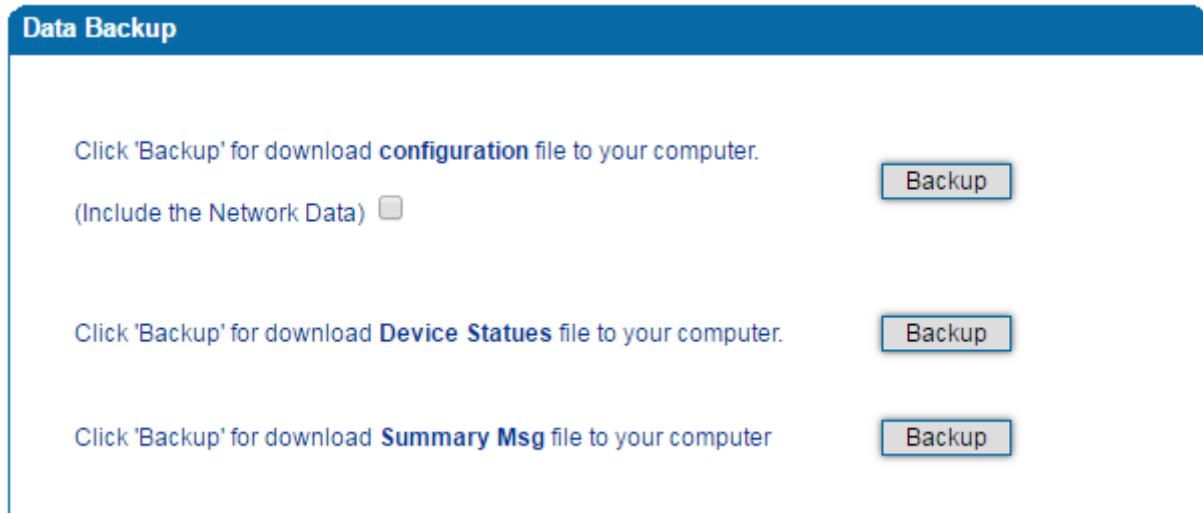


Figure 3.16-4 Restart Gateway

3.15.2 Data Backup

The process data backup:

- 1) Click "Data Backup"
- 2) Click "Backup" to backup data to PC.



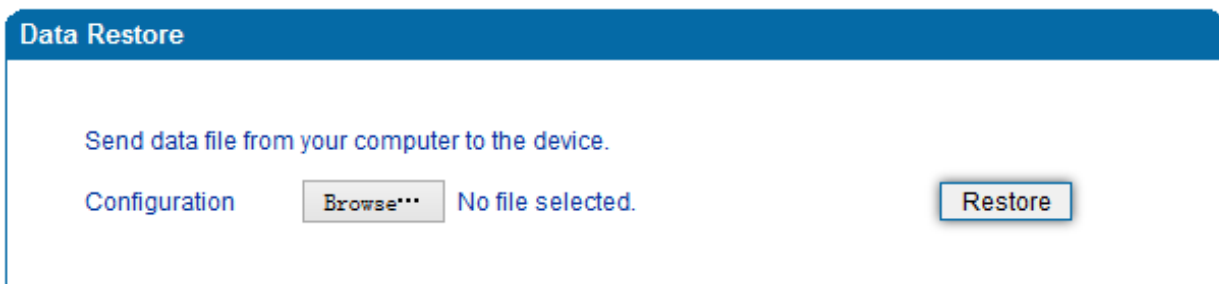
The screenshot shows a web interface titled "Data Backup" with a blue header. Below the header, there are three rows of instructions and buttons. The first row says "Click 'Backup' for download **configuration** file to your computer." followed by a "Backup" button. Below this is a checkbox labeled "(Include the Network Data)" which is currently unchecked. The second row says "Click 'Backup' for download **Device Statuses** file to your computer." followed by a "Backup" button. The third row says "Click 'Backup' for download **Summary Msg** file to your computer" followed by a "Backup" button.

Figure 3.16-5 Data Backup

3.15.3 Data Restore

The processes of data restore:

- ▶ Click 'Data Restore';
- ▶ Browse file, select data file.
- ▶ Click 'Restore' and then import successfully, the device will restart automatically.



The screenshot shows a web interface titled "Data Restore" with a blue header. Below the header, there is a text instruction: "Send data file from your computer to the device." Below this, there is a label "Configuration" followed by a "Browse..." button and the text "No file selected." To the right of this is a "Restore" button.

Figure 3.16-6 Data Restore

3.15.4 FXO Test

1. FXO ports impedance test is mainly to the technical personnel of O for impedance matching
2. Dial test number can configure by yourself, but avoid using * service the same number, and must all digit
3. You can just select online status port to test
4. If you don't know dial timeout time, can to test dial timeout time first, lasts about 10 seconds, finished the test will show timeout. Error is up to 30 seconds.
5. 'Match Mode': 'Simple' takes about 15 minutes, 'Standard' takes about 30 minutes, 'Exact' takes about 45 minutes.
6. If you want to give up the test result, click 'Clear'.
7. If you don't click 'Save', after the restart, test number, dial timeout and impedance will be invalid.
8. Before testing is completed, please don't leave the page, in order to avoid mistakes.

This function is used to automatically check the impedance of the PSTN line. The steps of how to use this function is as follows

1. Connect the PSTN line with the FXO port.
2. Select the the FXO port that is to be checked.
3. Select a mode. There are three modes: Simple, Standard and Exact. It is advised to use to the simple mode so as to save time.
4. Fill in the test digits instead of filling in a real number.
5. Click Start to test the port and wait for more than 15 minutes. During the time, please do not refresh the web.
6. After the test is completed, confirm the value in the "Acim" field.
7. Configure the value of "Acim" on the Advance ->FXO Parameter interface.
8. Restart the device to make the configurations to take effect.

3.15.5 Ping Test

On the **Tools** → **Ping Test** interface, user can use Ping to check whether the network is working or not.

Ping instructions:

- 1) Click 'Tools → Ping Test' on the navigation tree on the left;
- 2) Fill in IP address or domain whose connection needs to be checked, click **start**.

If a message is received, it indicates that network connection is normal. Otherwise the network connection is faulty.

The screenshot displays the 'Ping Test' configuration window. It features three input fields: 'Destination' with the value 'www.google.com', 'Number of Ping(1-100)' with the value '4', and 'Packet Size(56-1024 bytes)' with the value '56'. Below these fields are two buttons: 'Start' and 'Stop'. The 'Information' section below shows the test results: 'Pinging www.google.com[Resolve: 173.194.127.240] with 56 bytes of data: Reply seq=0 from 173.194.127.240: bytes=56 time=20ms TTL=54'.

Figure 3.16-7 Ping Test

3.15.6 Tracert Test

Tracert is a trace router used to track routing.

Tracert sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host. Determining the intermediate routers traversed involves adjusting the time-to-live (TTL), aka hop limit, Internet Protocol parameter. Frequently starting with a value like 128 (Windows) or 64 (Linux), routers decrement this and discard a packet when the TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded.

Tracert works by increasing the TTL value of each successive set of packets sent. The first set of packets sent have a hop limit value of 1, expecting that they are not forwarded by the first router. The next set have a hop limit value of 2, so that the second router will send the error reply. This continues until the destination host receives the packets and returns an ICMP Echo Reply message.

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

Tracert introduce:

- ▶ Click 'Tracert Test' in the navigation tree;
- ▶ Fill in IP address or domain whose route needs to be tracked, and then click **start**.

Tracert Test

Destination

Max Hops(1-255)

Information

```

Tracing route to www.google.com[Resolve:
173.194.127.240] over a maximum of 30 hops:
 1  10 ms  172.16.1.1
 2   1 ms  113.106.38.109
 3  *    Request timed out.
 4  10 ms  121.34.242.234
 5  10 ms  202.97.33.242
 6  10 ms  202.97.60.50
 7  *    Request timed out.
 8  *    Request timed out.

```

Figure 3.16-8 Tracert Test

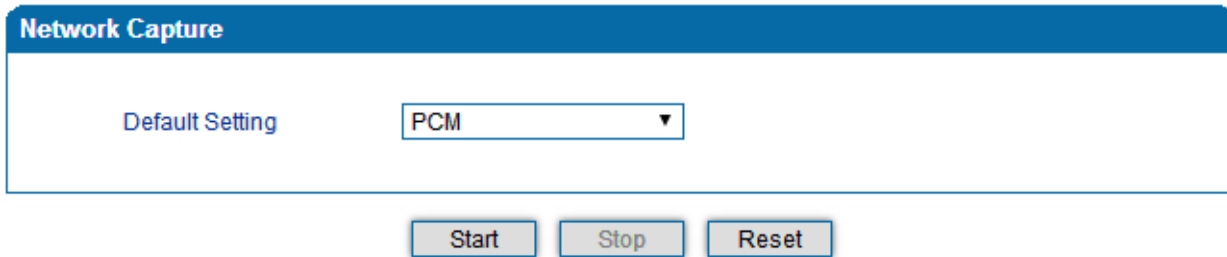
3.15.7 Network Capture

Network capture is a very important diagnostic tool for maintenance. It can be used to capture data packages of the available network ports.

Default Setting is PCM capture

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

- ▶ **To enable PCM capture**
 - ◆ Select 'PCM' on Network Capture page



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

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

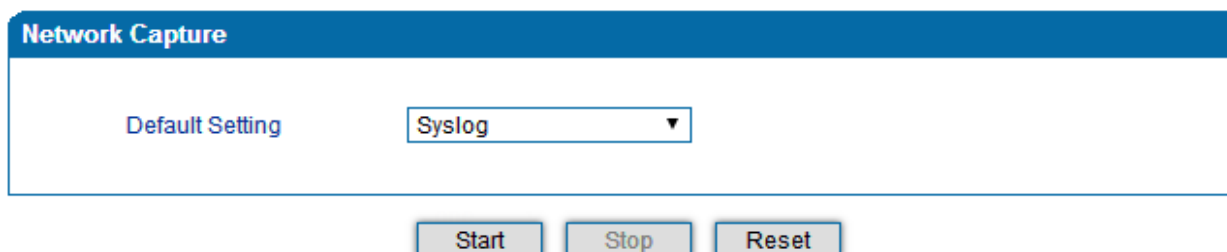
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x0021	Ch: 0xFFFF, Seq: 8 (From Host)
2	0.000131	Cimsys_33:44:55	Motorola_1c:1d:1e	Ethernet	20	Ethernet II[Malformed Packet]	
3	0.000245	Cimsys_33:44:55	Motorola_1c:1d:1e	CSM_ENCABS	44	--> 0x0021	Ch: 0xFFFF, Seq: 11 (From Host)
4	1.320893	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x0e00	Ch: 0x0003, Seq: 1 (From Host)
7	1.329890	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x0e01	Ch: 0x0003, Seq: 2 (From Host)
10	1.330472	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x0802	Ch: 0x0003, Seq: 3 (From Host)
13	1.330820	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x0803	Ch: 0x0003, Seq: 4 (From Host)
16	1.337791	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x9010	Ch: 0x0003, Seq: 5 (To Host)
19	1.338369	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x9000	Ch: 0x0003, Seq: 6 (To Host)
22	1.343521	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	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_ENCABS	30	--> 0x8084	Ch: 0x0003, Seq: 7 (To Host)
25	1.344060	Motorola_1c:1d:1e	Cimsys_33:44:55	CSM_ENCABS	104	--> 0x8001	Ch: 0x0003, Seq: 7 (From Host)

► Getting start to Syslog capture

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

► To enable syslog capture

- ◆ Select Syslog special only on Network Capture page



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

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

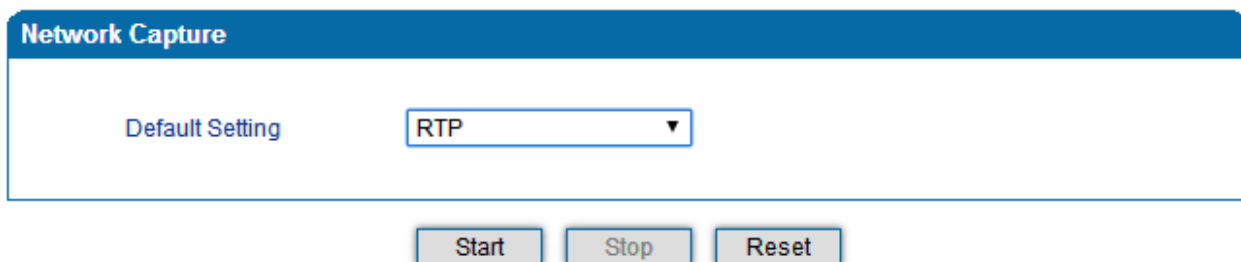
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 0> [DEBUG] --->> to 172.16.222.22/5060 crypt:FALSE Phone
2	0.000344	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 1> [DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\n
3	0.013432	172.16.222.22	1.1.1.1	Syslog	595	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 2> [DEBUG] <<---*** message from 172.16.222.22/5060,crypt
4	0.013750	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 3> [DEBUG] <<--- from 172.16.222.22/5060,crypt:FALSE, Phc
5	0.014036	172.16.222.22	1.1.1.1	Syslog	520	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 4> [DEBUG] OPTIONS sip:heartbeat@172.16.222.22 SIP/2.0\r\n
6	0.014512	172.16.222.22	1.1.1.1	Syslog	172	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 5> [DEBUG] --->> to 172.16.222.22/5060 crypt:FALSE Phone
7	0.014806	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 6> [DEBUG] SIP/2.0 200 OK\r\nvia: SIP/2.0/UDP 172.16.222.
8	0.028396	172.16.222.22	1.1.1.1	Syslog	662	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 7> [DEBUG] <<---*** message from 172.16.222.22/5060,crypt
9	0.028759	172.16.222.22	1.1.1.1	Syslog	176	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 8> [DEBUG] <<--- from 172.16.222.22/5060,crypt:FALSE, Phc
10	0.029052	172.16.222.22	1.1.1.1	Syslog	587	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 9> [DEBUG] SIP/2.0 200 OK\r\nvia: SIP/2.0/UDP 172.16.222.
11	0.030017	172.16.222.22	1.1.1.1	Syslog	233	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 10> [DEBUG] sip-->app: msgtype:ST_SIP_SERVER_CONN \r\n cal
12	0.331167	172.16.222.22	1.1.1.1	Syslog	983	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 11> [DEBUG] <<---*** message from 172.16.222.127/5060,cryp
13	0.331498	172.16.222.22	1.1.1.1	Syslog	177	USER.DEBUG: Jul 23 06:52:05 172.16.222.22 mpe_sip: < 12> [DEBUG] <<--- from 172.16.222.127/5060,crypt:FALSE, PF
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\n
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, PF
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\n
26	7.234596	172.16.222.22	1.1.1.1	Syslog	287	USER.DEBUG: Jul 23 06:52:12 172.16.222.22 mpe_sip: < 25> [DEBUG] sip-->app: localindex:69, msgtype:SIP_CALL_BYE

▶ Getting start to RTP capture

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

▶ To enable RTP capture:

- ◆ Select RTP special on Network Capture page



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

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

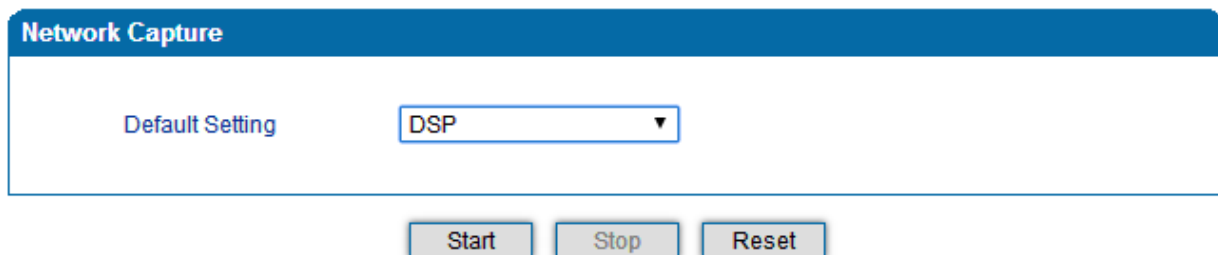
No.	Time	Source	Destination	Protocol	Length	Info
176	7.020000	172.16.221.228	116.204.105.50	SIP	365	Request: REGISTER sip:116.204.105.50
178	7.030000	116.204.105.50	172.16.221.228	SIP	411	Status: 200 OK (1 bindings)
244	11.610000	172.16.221.228	58.56.64.101	SIP/SDP	814	Request: INVITE sip:201@58.56.64.101
248	11.710000	58.56.64.101	172.16.221.228	SIP	480	Status: 100 Trying
249	11.710000	58.56.64.101	172.16.221.228	SIP/SDP	733	Status: 183 Session Progress
250	11.710000	58.56.64.101	172.16.221.228	SIP/SDP	719	Status: 200 OK
252	11.720000	172.16.221.228	58.56.64.101	RTP	66	unknown RTP version 1
253	11.720000	172.16.221.228	58.56.64.101	RTP	66	unknown RTP version 1
254	11.720000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1000, Time=160, Mark
255	11.720000	172.16.221.228	58.56.64.101	RTP	66	unknown RTP version 1
256	11.730000	172.16.221.228	58.56.64.101	RTP	66	unknown RTP version 1
257	11.730000	172.16.221.228	58.56.64.101	RTP	66	unknown RTP version 1
258	11.740000	172.16.221.228	58.56.64.101	SIP	434	Request: ACK sip:201@58.56.64.101:5060
259	11.740000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1001, Time=320
261	11.770000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1002, Time=480
263	11.780000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1003, Time=640
264	11.810000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1004, Time=800
265	11.830000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1005, Time=960
266	11.840000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1006, Time=1120
267	11.870000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1007, Time=1280
268	11.890000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1008, Time=1440
270	11.900000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1009, Time=1600
271	11.930000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31521, Time=1806312883
273	11.930000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1010, Time=1760
274	11.940000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1011, Time=1920
275	11.950000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31522, Time=1806313043
277	11.970000	58.56.64.101	172.16.221.228	RTP	74	PT=ITU-T G.729, SSRC=0x497E6D15, Seq=1012, Time=2080
278	11.970000	172.16.221.228	58.56.64.101	RTP	74	PT=ITU-T G.729, SSRC=0x43455AA6, Seq=31523, Time=1806313203

► Getting start to DSP capture

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

► To enable DSP capture:

- ◆ Select DSP only on Network Capture page



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

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

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

► Configurable capture options

► Getting start to custom capture

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

Network Capture

Default Setting Custom ▼

Include ARP Packet

Select Port None ▼

Protocol(s) TCP UDP RTP ICMP

Start
Stop
Reset

3.15.8 Factory Reset

Click 'Apply' to restore the factory settings.

Factory Reset

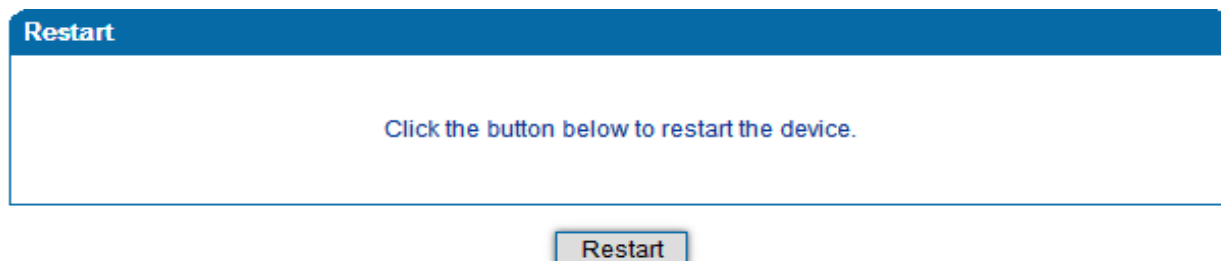
Click the button below to reset to factory default settings.

Apply

Factory Reset

3.15.9 Device Restart

After saving all the configurations or changes to the equipment, user can restart the DAG FXO gateway for the changes to take effect.



4 Glossary

- DNS: Domain Name System
- SIP: Session Initiation Protocol
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- RTP: Real Time Protocol
- PPPOE: point-to-point protocol over Ethernet
- VLAN: Virtual Local Area Network
- ARP: Address Resolution Protocol
- CID: Caller Identity
- DND: Do NOT Disturb
- DTMF: Dual Tone Multi Frequency
- NTP: Network Time Protocol

- DMZ: Demilitarized Zone
- STUN: Simple Traversal of UDP over NAT
- PSTN: Public Switched Telephone Network
- IMS: IP Multimedia Subsystem
- ACL: access rule list
- SNMP: Simple Network Management Protocol
- FXO: Foreign Exchange Station
- FXO: Foreign Exchange Office