



# **DGW-L20X User Manual**



Address: Room 624, 6/F, Tsinghua Information Port, Book Building, Qingxiang Road, Longhua

Street, Longhua District, Shenzhen, Guangdong, China 518109

**Tel:** +86-755-82535461, 82535095, 82535362

**Fax:** +86-755-83823074

Business Contact: <a href="mailto:sales@openvox.cn">sales@openvox.cn</a>

Technical Support: <a href="mailto:support@openvox.cn">support@openvox.cn</a>

Business Hours: 09:00-18:00(GMT+8) from Monday to Friday

URL: www.openvoxtech.com



# Legal Information

# Copyright

Copyright<sup>©</sup> 2019 OpenVox Inc. All rights reserved. No part of this document may be reproduced without prior written permission.

# Confidentiality

Information contained herein is of a highly sensitive nature and is confidential and proprietary to OpenVox Inc. No part may be distributed, reproduced or disclosed orally or in written form to any party other than the direct recipients without the express written consent of OpenVox Inc.

# Disclaimer

OpenVox Inc. reserves the right to modify the design, characteristics, and products at any time without notification or obligation and shall not be held liable for any error or damage of any kind resulting from the use of this document.

OpenVox has made every effort to ensure that the information contained in this document is accurate and complete; however, the contents of this document are subject to revision without notice. Please contact OpenVox to ensure you have the latest version of this document.

# Trademarks

All other trademarks mentioned in this document are the property of their respective owners.



# **Revision History**

Issue version	Issue date	Detail of change
1.0	Jul 12 2019	Initial



# Content

Legal Information	
Copyright	
Confidentiality	2
Disclaimer	2
Trademarks	2
Revision History	
1 Overview	9
1.1 What is DGW-L20X?	9
1.2 Sample Application	
1.3 Product Appearance	
1.4 Main Features	
1.5 Physical Information	
1.6 Software	
2 System	14
2.1 Status	
2.2 Call Status	
2.3 Time	
2.4 Login Settings	
2.5 General	

# **OpenVox**

2.5.1 Language Settings	
2.5.2 Scheduled Reboot	
2.6 Tools	
2.6.1 Reboot Tools	
2.6.2 Update Firmware	
2.6.3 Upload and Backup Configuration	21
2.6.4 Restore Configuration	
2.7 System Information	
3 T1/E1	23
3.1 General	
3.2 PRI	
3.3 MFC/R2	
3.3.1 MFC/R2 Signaling	
3.3.2 Modify R2 variant	
3.4 Chan-SS7	
3.4.1 Link Set Settings	
3.4.2 Link Settings	
3.4.3 SS7 Configuration file backup and restore	
4 VOIP	
4.1 VOIP Endpoints	
4.1.1 SIP Endpoints	
4.1.2 Main Endpoint Settings	

# **OpenVox**

4.1.3 Advanced Registration Options	
4.1.4 Call Settings	
4.1.5 Advanced Signaling Settings	
4.1.6 Advanced Timer Settings	
4.1.7 Fax Options	45
4.2 IAX2 Endpoint	
4.3 Advanced SIP Settings	
4.3.1 Networking	
4.3.2 Advanced NAT Settings	
4.3.3 Advanced RTP Settings	
4.3.4 Parsing and Compatibility	
4.3.5 Security	
4.3.6 Media	
4.3.7 Codec Settings	55
4.4 Advanced IAX2 Settings	55
4.5 Advanced fax setting	
5 Routing	61
5.1 Call Routing Rule	61
5.2 Groups	
6 Network	67
6.1 Network Settings	67
6.2 DDNS Settings	

# **OpenVox**

6.3 Toolkit	
6.4 Static Route Settings	
7 Advanced	
7.1 Asterisk API	
7.2 Asterisk CLI	
7.3 Asterisk File Editor	
7.4 Auto Provisioning	
7.4.1 Preparation	
7.4.2 Configuring gateway	
7.4.3 Configuring ACS	
7.4.4 Provisioning example	
7.5 SNMP	
7.5.1 Parameters in SNMP setting	
7.5.2 Activating SNMP	
7.5.3 Verify SNMP	
7.6 TR069	
7.7 Network Capture	
7.8 Cloud	
8 User	93
8.1 User Add	
8.2 User List	



8.3 Pern	rmissions	
9 Logs		94
9.1 Log :	g Settings	
9.2 Syste	stem log	
9.3 Aste	terisk logs	
9.4 Call .	ll Statistics	
9.5 Syste	stem Notice	

# 1 Overview

# 1.1 What is DGW-L20X?

OpenVox T1/E1 Gateway is an open source asterisk-based VoIP Gateway solution for operators and call centers. It is a converged media gateway product. This kind of gateway connects traditional telephone system to IP networks and integrates VoIP PBX with the PSTN seamlessly. With friendly GUI, users may easily setup their customized Gateway. Also, secondary development can be completed through AMI (Asterisk Management Interface).

It is developed with a wide selection of codecs and signaling protocol, including G.711A, G.711U, G.729, G.722, G.723 and GSM. It supports PRI/SS7/R2 protocol. OpenVox T1/E1 Gateway has good processing ability and stability. The T1/E1 gateway will be 100% compatible with Asterisk, Elastix, 3CX, FreeSWITCH SIP server and VOS VoIP operating platform.



# **1.2 Sample Application**



#### Figure 1-2-1 Topological Graph

# **1.3 Product Appearance**

The picture below is appearance of DGW-L20X.







#### Figure 1-3-2 Front Panel



Interface	Function	Color	Work Status	
1 Port 1-Port4	E1/T1 ports. There is only one port.			
2 Reset	Reset button is used to restore the device.			
3 RUN	Register indicator	Green	Slow blinking (Green 2s and Flash 0.1s): Work normally. Fast blinking (Green 0.5s and Flash 0.5s): Work abnormally. Fast blinking (Green 0.5s and Flash 0.5s): Work abnormally. No blinking: DAHDI Error.	
4 PWR	Power Status indicator	Green	On: Power is on. Off: Power is off.	
5 VGA	VGA monitor connector.			
6 Eth1	Network interface.			

## Table 1-3-1 Description of Front Panel



7 Eth0	Network interface.
8 USB	USB interface.
9 DC-12V	Power supply.

# **1.4 Main Features**

- Based on Asterisk<sup>®</sup>
- > Editable Asterisk<sup>®</sup> configuration file
- > Wide selection of codecs and signaling protocol
- Support 512 routing rules and flexible routing settings
- > Stable performance, flexible dialing, friendly GUI
- Codecs support: G.711A, G.711U, G.729, G.723, G.722, GSM
- Support ports group management
- Support call status information
- Support T.38/Pass-through fax
- Support Auto Provision, SNMP and TR069
- Connect legacy PBX systems to low-cost VoIP services
- Connect legacy PBX systems to remote sites over private VoIP links
- Connect IP PBX systems to legacy TDM services

# **1.5 Physical Information**

Table 1-5-1	Description	of Physical	Information
-------------	-------------	-------------	-------------

Weight	1352g
Size	31cm*16.25cm*4.4cm
	-40~85°C (Storage)
Temperature	0~40°C (Operation)



Operation humidity	5%~95% non-condensing
Max power	18W
LAN port	1
WAN port	1

# 1.6 Software

Default IP: 172.16.100.1(WAN), 192.168.100.1(LAN)

Username: admin

Password: admin

Notice: Log in



Windows 安全		_ <b>x</b> _
位于 T1/E1 Ga	teway 的服务器 172.16.100.1 要求用户名和密码。	
	admin ●●●●● 回 记住我的凭据	
	确定取	<b>۴</b>

# OpenVox 2 System

# 2.1 Status

On the "System Status" page, you will find all Interface status, channels status, SIP, IAX2, Routing

rules, and Network information.

Interr	Interface status																														
Port1 F				Po	ort2							Po	ort3						P	ort4											
	•				(	)							•																		
😑 oi	🕽 OK 🛑 Down 💛 Reload																														
Chan	Channels Status																														
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1		2	3 ())	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2	32	33	34	35	36	37	38	39	40	41	42	43 ()	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
3	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93
4	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124
😑 Id	e 🔴 E	Busy (	🕖 Sa	ame N	ode Ty	ype 🧲	Disa	ble 🦲	S ch	annel																					
				-																											
SIP Ir	iformati	ion															_														
Endpo	int Nam	ne				User N	lame				H	ost					Reg	istrati	on		!	Status									
Voip-te	st					12345					19	92.168	.3.100				clie	nt				UNRE/	ACHAE	BLE							
IAX2	Informa	ation																													
Endpo	Endpoint Name User Name Host Registration Status																														
Routi	ng Info	rmatio	on																												
Rule N	ame					From					То	)					Rule	es													
E1-to-	/oip					Port-1					si	p-Voip∙	test				Cal + [] Cal + []	lee_Di (- +)  ler_Dia (- +)	al_patt al_patte	ern ern											
Voip-to-E1 sip-Voip-test					Port-1				Callee_Dial_pattern +[[]((- +)) Caller_Dial_pattern +[[](- +)]]																						
Netw	ork Info	ormati	on																												
Name		мас	C Addi	ress					IP	Addre	<b>S</b> S			Ма	sk				Gatev	vay			RX F	Packet	S		Т	X Pack	ets		
eth0		A0:9	98:05:0	01:DB:	A6				17	2.16.2	10.2			25	5.255.0	0.0			172.1	6.0.1			2514	49104			3	346105			

Figure	2-1-1	System	Status
--------	-------	--------	--------

Options	Definition
Interface	Show the status of port, include "OK" and "Down". "Down" means no trunk.
Channels	Show the Channels status of port, include "Idle". "Busy". "Disable" and "S
Status	channel". "Idle" means it is available;
	"Busy" means the channel is busy.

#### Table 2-1-1 Description of System Status

# 2.2 Call Status

The verbose of the system call status will be present on the "Call Status" page. You can select the

specified T1/E1 port which you are care for.

Call Status						Select Port 1 -
Channel	Status	Direction	CallerID	CalleelD	AnsweredTime	Duration
1	ANSWERED	IP->PSTN	2001	2001	2016-03-10 09:39:10	00: 00: 40
2	ANSWERED	IP->PSTN	2002	2002	2016-03-10 09:39:10	00: 00: 40
3	ANSWERED	IP->PSTN	2003	2003	2016-03-10 09:39:11	00: 00: 39
4	ANSWERED	IP->PSTN	2004	2004	2016-03-10 09:39:11	00: 00: 39
5	ANSWERED	IP->PSTN	2005	2005	2016-03-10 09:39:11	00: 00: 39
6	ANSWERED	IP->PSTN	2006	2006	2016-03-10 09:39:12	00: 00: 38
7	ANSWERED	IP->PSTN	2007	2007	2016-03-10 09:39:12	00: 00: 38
8	ANSWERED	IP->PSTN	2008	2008	2016-03-10 09:39:12	00: 00: 38
9	ANSWERED	IP->PSTN	2009	2009	2016-03-10 09:39:13	00: 00: 37
10	ANSWERED	IP->PSTN	2010	2010	2016-03-10 09:39:13	00: 00: 37
11	ANSWERED	IP->PSTN	2011	2011	2016-03-10 09:39:13	00: 00: 37
12	ANSWERED	IP->PSTN	2012	2012	2016-03-10 09:39:14	00: 00: 36
13	ANSWERED	IP->PSTN	2013	2013	2016-03-10 09:39:14	00: 00: 36
14	ANSWERED	IP->PSTN	2014	2014	2016-03-10 09:39:14	00: 00: 36
15	ANSWERED	IP->PSTN	2015	2015	2016-03-10 09:39:15	00: 00: 35

Figure 2-2-1 verbose of Call Status	Figure	2-2-1	Verbose	of	call	status
-------------------------------------	--------	-------	---------	----	------	--------



# 2.3 Time

Options	Definition
System Time	Your gateway system time.
Time Zone	The world time zone. Please select the one which is the same or the
	closest as your city.
POSIX TZ String	Posix timezone strings.
NTP Server 1	Time server domain or hostname. For example, [0.cn.pool.ntp.org].
NTP Server 2	The first reserved NTP server. For example, [time.windows.com].
NTP Server 3	The second reserved NTP server. For example, [time.nist.gov].
Auto Sync from NTD	Whether enable automatically synchronize from NTP server or not. ON
Auto-Sync holli NTF	is enable, OFF is disable this function.
Sync from NTP	Sync time from NTP server.
Sync from Client	Sync time from local machine.

Table 2-3-1 Description of Time Settings

For example, you can configure like this:

#### Figure 2-3-1 Time Settings

Time Settings	
System Time:	2016-3-9 16:25:18
Time Zone:	Shanghai
POSIX TZ String:	CST-8
NTP Server 1:	0.cn.pool.ntp.org
NTP Server 2:	time.nist.gov
NTP Server 3:	time.windows.com
Auto-Sync from NTP:	ON

Sync from NTP Sync from Client

You can set your gateway time Sync from NTP or Sync from Client by pressing different buttons.



# 2.4 Login Settings

Your gateway doesn't have administration role. All you can do here is to reset what new username and password to manage your gateway. And it has all privileges to operate your gateway. You can modify "**Web Login Settings**" and "**SSH Login Settings**". If you have changed these settings, you don't need to logout, just rewriting your new user name and password will be OK. Also you can specify the web server port number. Usually the web login default mode is "http and https". For safety, you can switch to "only https" mode.

Options	Definition
	Your gateway does not have administration role.
	All you can do here is defining the user name and password to manage your
User Name	gateway.
	And it has all privileges to operate your gateway .User Name: Allowed
	characters "+<>&0-9a-zA-Z".Length:1-32 characters.
Password	Allowed characters "+. <>&0-9a-zA-Z".
1 4350010	Length: 4-32 characters.
Confirm Password	Please input the same password as 'Password' above.
Login Mode	Specify the web login mode: http and https, only https. Default is http and
Login Mode	https.
Port	Specify the web server port number. Do not use port 443 which is reserved for
	HTTPS.

#### Table 2-4-1 Description of Web Login Settings

Figure	2-4-1	Login	Settings
--------	-------	-------	----------

Web Login Settings	
User Name:	admin
Password:	••••
Confirm Password:	••••
Login Mode:	http and https 🔻
HTTP Port:	80
HTTPS Port:	443
SSH Login Settings	
Enable:	ON
User Name:	admin
Password:	admin
Port:	12345

Notice: Whenever you do some changes, do not forget to save your configuration.



# 2.5 General

# 2.5.1 Language Settings

You can choose different languages for your system. If you want to change language, you can switch "Advanced" on, then "Download" your current language package. After that, you can modify the package with the language you need. Then upload your modified packages, "Choose File" and "Add".

Figure 2-5-1	Language Settings

**~** ...

~ - . .

-----

Language:	English •
Advanced:	
Language Debug:	TURN ON TURN OFF
Download:	Download selected language package.
Delete:	Delete selected language.
Add New Language:	New language Package:         选择文件         未选择任何文件         Add

# 2.5.2 Scheduled Reboot

If switch it on, you can manage your gateway to reboot automatically as you like. There are four

reboot types for you to choose, "By Day, By Week, By Month and By Running Time".

#### Figure 2-5-2 Reboot Types

Scheduled Reboot				
Enable:				
Reboot Type:	By Day 🔻			
Time:	Hour: 23  Minute: 59			

If use your system frequently, you can set this enable, it can helps system work more efficient.

# 2.6 Tools

On the "Tools" pages, there are reboot tools, update Firmware, upload Configuration, backup



Configuration and Restore Configuration toolkits.

# 2.6.1 Reboot Tools

You can choose system reboot and Asterisk reboot separately.

Figure 2-6-1 Reboot Prompt

Reboot Tools	-	
Reboot the gateway and all the current calls will be dropped.	Are you sure to reboot your gateway now?	System Reboot
Reboot the asterisk and all the current calls will be dropped.	You will lose all data in memory!	Asterisk Reboot
Update Firmware	确定 取消	
New system file: 浏览 未选择文件。		System Update

If you press "OK", your system will reboot and all current calls will be dropped. Asterisk Reboot is

the same.

Options	Definition
System Reboot	This will turn off your gateway and then turn it back on. This will drop all current calls.
Asterisk Reboot	This will restart Asterisk and drop all current calls.

#### Table 2-6-1 Instruction of reboots

# 2.6.2 Update Firmware

We offer two kinds of update types for you. You can choose System Update or System Online Update. System Online Update is an easier way to update your system, if you choose that, you will see some information below.

#### Figure 2-6-2 Prompt Information

Update Firmware	
New system file: 选择文件 未选择任何文件	System Update
New system file is downloaded from official website and update	e system. System Online Update



# 2.6.3 Upload and Backup Configuration

If you want to update your system and remain your previous configuration, you can first backup

configuration, then you can upload configuration directly. That will be very convenient for you.

#### Figure 2-6-3 Upload and Backup

Upload Configuration	
New configuration file: 选择文件 未选择任何文件	File Upload
Backup Configuration	
Current configuration file version: 0.02.03	Download Backup

# **2.6.4 Restore Configuration**

Sometimes there is something wrong with your gateway that you don't know how to solve it, mostly you will select factory reset. Then you just need to press a button, your gateway will be reset to the factory status.

#### Figure 2-6-4 Factory Reset





# 2.7 System Information

On the "Information" page, there shows some basic information about the T1/E1 gateway. You can

see software and hardware version, storage usage, memory usage and some help information.

Figure 2-7-1 System Information

Model Name:	DGW-1004
Firmware Version:	2.5.3
Firmware Build:	1907
Hardware Version:	1.1
Port Amount:	4
Storage Usage:	100.2M/193.5M (56%)
Memory Usage:	11.107 % Memory Clean
Kernel Build Time:	2019-Jul-2-17:10:59
Contact Address:	10/F, Building 6-A, Baoneng Science and Technology Industrial Park, Longhua New District, Shenzhen, Guangdong, China
Tel:	+86-755-82535461
Fax:	+86-755-83823074
E-Mail:	support@openvox.cn
Web Site:	http://www.openvox.cn
System Time:	2019-7-11 12:22:21
System Uptime:	7 days 18:16:14



# 3.1 General

#### Figure 3-1-1 General Settings

General	
Locale:	United States
Interface Type:	○ T1 <sup>®</sup> E1
Span Default Law:	Auto 🔻

#### **Table 3-1-1 Definition of General Settings**

Options	Definition
Locale	Your locale. This will be used for the tone style. Used when in-call indications
	need to be generated such as ring back, busy, congestion, and other
	call-oriented inband tone signals.
Interface Type	It shows you the current type of port. It has two type: E1 and T1.

#### Figure 3-1-2 Advanced interface type

V Advanced: Interface Type	
Echo Cancellation:	
RX Gain:	0
TX Gain:	0

#### Table 3-1-2 Definition of advanced interface type

Options	Definition
RX Gain	Gain for the RX (receive -into Asterisk) channel.Default:0.0.
TX Gain	Gain for the TX (transmit -out of Asterisk Asterisk) channel.Default:0.0.

## Figure 3-1-3 Port Details

Port Details										
	Port #	Timing Source	Interface	Framing	Coding	Line Build-out	CRC4	Signalling	Switch Type	Description
	Port 1	0 -	E1	CCS 💌	HDB3 -	0-133 feet ( DSX-1 ) and 0 db (CSU) $\fbox$	Off 💌	PRI(Network side)	EuroIsdn 💌	
	Port 2	0 -	E1	CCS 💌	HDB3 -	0-133 feet ( DSX-1 ) and 0 db (CSU) $\fbox$	Off 🔻	PRI(Network side)	EuroIsdn 💌	
	Port 3	0 -	E1	CCS 💌	HDB3 -	0-133 feet ( DSX-1 ) and 0 db (CSU) $\fbox$	Off 🔻	PRI(Network side) 🔻	EuroIsdn 💌	
	Port 4	0 -	E1	CCS 🔻	HDB3 -	0-133 feet ( DSX-1 ) and 0 db (CSU) $\checkmark$	Off 🔻	PRI(Network side)	EuroIsdn 💌	

#### Table 3-1-3 Definition of Port Details

Options	Definition
	Timing Source indicate the ports as to which should be used to recover the
Timing Source	clock. (0 for master mode, upper for client mode, small number have higher
	priority).
Interface	Choose a line type for the interface.
Framing	Framing method for this interface.
Coding	Coding method for this interface.
Line Build-out	Line build-out represents the length of the cable form the port on this gateway
	to the next device.
	Enable cyclic redundancy checking for error checking on line. CRC-4 support is
CRC4	required for all network switches in Europe, but many older switches and PBXs
	don't support it.
Signaling	It shows you what signaling the port uses.
Switch Type	Only used for PRI.
Description	An optional description of this interface to be used for reference only.



# 3.2 PRI

▼ ISDN: Signaling	
Q.SIG Channel Mapping:	Physical 🔻
Enable Caller ID:	ON
PRI Options	
PRI Dial Plan for Dialed Number	Unknown
PRI Dial Plan for Dialing Number:	Unknown
International Prefix:	
National Prefix:	
Local Prefix:	
Private Prefix:	
Unknown Prefix:	
Network Specific Facility Messages	None
Idle Bearer Reset:	OFF
Idle Bearer Reset Period:	never
Display Send:	Name
Display Receive:	Name
Overlap Dialing:	Disabled •
Allow Progress When Call Released:	ON
Out-of-Band Indications:	
Facility-based ISDN Supplementary Services:	
Exclusive Channel Selection:	
Ignore Remote Hold Indications:	
Block Outbound Caller ID Name:	OFF
Wait for Caller ID Name:	

# Figure 3-2-1 ISDN: Signaling

#### Table 3-2-1 Definition of Signaling

Options	Definition
	Sets logical or physical channel mapping. In logical channel mapping,
Q.SIG Channel	channels are mapped to 1-30. In physical channel mapping, channels are
Mapping	mapped to 1-15,17-31, skipping the number used for the data channel,
	Default is physical.
Enable Caller ID	Whether or not to use caller ID.



г

-

	PRI Dialplan: The ISDN-level Type of Number (TON) or numbering plan,
PRI Dial Plan for	used for the dialed number. Leaving this as 'unknown' (the default) works for
Dialed Number	most cases. In some very unusual circumstances, you may need to set this
	to; 'dynamic' or 'redundant'.
	PRI Local Dialplan: Only RARELY used for PRI (sets the calling number's
PRI Dial Plan for	numbering plan). In North America, the typical use is sending the 10 digits;
Dialing Number	caller ID number and setting the prilocaldialplan to 'national' (the default).
	Only VERY rarely will you need to change this.
Network Specific	Some switches (AT&T especially) require network specific facility IE.
Facility (NSF)	Supported values are currently 'none', 'sdn', 'megacom',' tollfreemgacom','
Messages	account'.
Idle Bearer Reset	Whether or not to reset unused B channels.
Idle Bearer Reset	Sets the time in seconds between restart of unused B channels; defaults to
Period	'never'.
	Send/receive ISDN display IE options, the display options are a comma
	separated list of the following options:
	<b>block</b> : Do not pass display text data.
	name_initial: Use display text in SETUP/CONNECT messages as the party
Display Send	name.
	name_update: Use display text in other messages (NOTIFY/FACILITY) for
	COLP name update.
	<b>name</b> : Combined name_ initial and name_ update options.
	text: Pass any unused display text data as an arbitrary display message



	during a call. Sent text goes out in default to 'name'.
Display Receive	Send/receive ISDN display IE options. The display options are a comma separated list of the following options: block: Do not pass display text data. name_initial: Use display text in SETUP/CONNECT messages as the party name. bame_update: Use display text in other messages (NOTIFY/FACILITY) for COLP name update. name: Combined name_ initial and name_ update options. text: Pass any unused display text data as an arbitrary display message during a call. Sent text goes out in default to 'name'.
Overlap Dialing	Enable overlap dialing modesending overlap digits.
Allow Progress When Call Released	Allow inband audio (progress) when a call is DISCONNECT Ted by the end of a PRI.
Out-of-Band Indications	PRI Out of band indications. Enable this to report Busy and congestion on a PRI using out_ of_ band notification. Inband indication, as used by the gateway doesn't seem to work with all telcos.
Facility-based ISDN	To enable transmission of facility-based ISDN supplementary services (such
Supplementary	as caller name form CPE over facility), enable this option. Cannot be
Services	changed on a reload.
Exclusive Channel	If you need to override the existing channels selection routine and force all
Selection	PRI channels to be marked as exclusively selected, set this to yes.



Т

-

	priexclusive cannot be changed on a reload.			
Ignore Remote Hold	If you wish to ignore remote hold indications (and use MOH that is supplied			
Indications	over the B channel) enable this option.			
Block Outbound	Enable if you need to hide just the name and the number for legacy PB>			
Caller ID Name	use. Only applies to PRI channels.			
Wait for Caller ID				
Name	Support caller ID on call waiting.			

# 3.3 MFC/R2

# 3.3.1 MFC/R2 Signaling

#### Figure 3-3-1 MFC/R2 Signaling

WFC/R2: Signaling	
Enable Caller ID:	ON
Init CAS Bit:	1101
Variant:	TTU T

## Table 3-3-1 Definition of MFC/R2 Signaling

options	Definition
Enable Caller ID	Whether or not to use caller ID.
Init CAS Bit	The initial position of the CAS bits.
Variant	The standard of MFCR2: ITU, ANSI and China.



# 3.3.2 Modify R2 variant

R2 Variant										
Variant Name	CDbits	Get ANI First	Req Next DNIS	Req Next ANI	Request Category	DNIS End	ANI End	Address Complete	Actions	
Argentina	01	yes	1	5	5	x	с	3	2	*
Bolivia	01	yes	1	5	5	F	F	3	2	×
Brazil	01	no	1	5	5	x	F	3	2	*
China	11	yes	1	1	6	x	F	3	2	*
Colombia	01	yes	1	5	5	F	F	3	2	×
Costa_rica	01	yes	1	5	5	x	F	3	2	*
Czech_republic	01	yes	1	5	5	F	F	3	2	×
Ecuador	01	yes	1	5	5	F	F	3	2	×
India	01	yes	1	4	5	x	F	3	2	*
Indonesia	01	yes	1	6	6	F	F	3	2	×
Israel	01	yes	1	9	9	x	F	3	2	*
ITU	01	yes	1	5	5	F	F	3	2	
Korea	01	yes	1	5	5	x	F	3	2	×
Malaysia	01	yes	1	6	6	F	F	3	2	×
Malta	01	yes	1	0	5	x	F	3	2	×

#### Figure 3-3-2 R2 Variant

You can click

button, then you could fine the below.

#### Figure 3-3-3 General

General	
Variant Name:	argentina
R2 Category:	national_subscriber
Allow Collect Calls:	No T
Accept On Offer:	Yes •
Forced Release:	No
Charge Calls:	Yes •
Max DNIS:	4
Max ANI:	10
Get ANI First:	Yes •
Immediate Accept:	No T
Double Answer:	No T
Skip Category:	No T
CAS NonR2 Bits:	01 •
CAS_R2_Bits:	11 •

#### Table 3-3-2 Definition of General

Options	Definition
Variant Name	The variant name.
R2 Category	national subscriber works just fine usually.
Allow Collect Calls	Default is to block collect calls.
Accept On Offer	With this set to 'no' then the call will NOT be accepted on offered, and the call will start irs execution in extensions. Conf until the channel is answered.
Forced Release	Brazil use a special signal to force the release of the line instead of the normal clear back signal.
Charge Calls	Whether or not report to the other end 'accept call with charge', when interconnecting with old PBXs this may be useful.
Max DNIS	Max amount of DNIS to ask for.
Max ANI	Max amount of ANI to ask for.
Get ANI First	Whether or not get the ANI before getting DNIS.
Immediate Accept	This feature allows to skip the use of Group B/II signals and go directly to the accepted state for incoming calls.
Double Answer	This will cause that every answer signal is changed by answer->clear back->answer, sort of flash.
Skip Category	Skip request of calling party category and ANI.
CASNonR2 Bits	Which bits are never used.
CAS_R2_Bits	Which bits will be used.



#### Figure 3-3-4 Timer

Timer	
MF Back Cycle:	5000
MF Back Resume Cycle:	150
MF Fwd Safety:	30000
R2 Seize:	8000
R2 Answer:	60000
Metering Pulse:	400
R2 Double Answer:	400
R2 Answer Delay:	150
CAS Persistence Check:	0
DTMF Start Dial:	500
DTMF Detection End:	5000

#### Table 3-3-3 Definition of Timer

Options	Definition		
MF Back Cycle	Max amount of time our backward MF signal can last.		
MF Back Resume Cycle	Amount of time we set MF signal ON to resume the MF cycle with a MF pulse.		
MF Fwd Safety	Safety FORWARD timer.		
R2 Seize	How much time do we wait for a response to our seize signal.		
R2 Answer	How much to wait for an answer once the call has been accepted.		
Metering Pulse	Hoe much to wait for metering pulse detection.		
R2 Double Answer	Interval between ANSWER-CLEAR BACK-ANSWER when double answer is in effect.		
R2 Answer Delay	Minimum delay time between the Accept tone signal and the R2 answer signal.		



Γ

CAS Persistence Check	Time to wait for to CAS signaling before handing the new signal.
DTMF Start Dial	Safety time before starting to dial DTMF.
DTMF Detection End	Safety time to decide when to stop detecting DTMF DNIS.

#### Figure 3-3-5 Group A

Group A	
Request Next DNIS Digit:	1 •
Request DNIS Minus 1:	2 •
Request DNIS Minus 2:	7 •
Request DNIS Minus 3:	8 •
Request All DNIS Again:	INVALID •
Request Next ANI Digit:	5 •
Request Category:	5 •
Request Category And Change To Gc:	INVALID •
Request Change To G2:	3 •
Address Complete Charge Setup:	6 •
Network Congestion:	4 •



# Figure 3-3-6 Group B

Group B	
Accept Call With Charge:	6 •
Accept Call No Charge:	7 •
Busy Number:	3 •
Network Congestion:	4
Unallocated Number:	5 •
Line Out Of Order:	8 •
Special Info Tone:	2 •
Reject Collect Call:	INVALID •
Number Changed:	INVALID •



Group C	
Request Next ANI Digit:	INVALID V
Request Change To G2:	INVALID V
Request Next DNIS Digit And Change To Ga:	INVALID V
Network Congestion:	INVALID V

#### Figure 3-3-8 Group 1

Group 1		
No More Dnis Available:	INVALID 🔻	
No More ANI Available:	C •	
Caller ANI Is Restricted:	F T	



#### Figure 3-3-9 Group 2

Group 2	
National Subscriber:	1 •
National Priority Subscriber:	2 •
International Subscriber:	7 •
International Priority Subscriber:	9 🔻
Collect Call:	INVALID •
Test Equipment:	3 🔻
Save Variant Cancel	

# 3.4 Chan-SS7

# 3.4.1 Link Set Settings

#### Figure 3-4-1 Link Set Settings

Link Set Settings											
Link Set Name	Enabled	Enabled ST	Use Connect	Hunting Policy	Subservice	t35	User Part	Variant	OPC	DPC	Action
siuc (default)	yes	no	yes	even_mru	auto	15000,timeout		ITU	0x1	0×32	0
Add Now SS7 Link Sot											
Add New SS/ Link Set											
You can click Ibutton as shown below, when there are several link sets, only one can be set to											

the default.



## Figure 3-4-2 Chan-SS7 Link Set Settings

#### Edit Link Set "linkset-siuc"

▼ SS7 Link Set Settings		
	Name:	siuc
	Enabled:	
	Enabled ST:	OFF
	Use Connect:	
	CON Echo Cancellation:	
	Called Party Number Stop Flag:	
	Transmission Medium Requirement:	speech
	Nature Address Indicator:	Subscriber •
	Hunting Policy:	even_mru 🔻
	Subservice:	auto

<u>t35:</u>	15000,timeout
User Part:	ISUP •
Variant:	ITU •
OPC:	0x1
DPC:	0x32
Set to Default:	
Original Called Number:	No •

Save Cancel

options	Definition			
Name	The link set name.			
Туре	SS7 variant.			
Enabled ST	This is used to decide whether end-of-pulsing is not used to determine			
	when incoming address is complete.			
Use Connect	This setting specifies whether to reply incoming call with CON rather			
	than ACM and ANM.			
CON Echo	This setting will enable Echo Cancellation when 'Use Connect' is			
Cancellation	enabled.			

### Table 3-4-1 Definition of SS7 Link Set Settings



Called Party	
Number Stop	Add a stop flag 'F' before called number send.
Flag	
Transmission Medium Requirement	Specify the bearer circuit capabilities (speech, 3.1-kHz audio, 64-Kb unrestricted, and so forth) that are needed for the call being set up.
Nature Address Indicator	the nature of address indicator field is national or subscriber(default).
Hunting Policy	This sets the hunting policy, ie. the algorithm used to allocate a circuit for outgoing calls. This should be configured appropriately at each end of the SS7 link to minimize the risk of call collision, both ends try to make an outgoing call on the same circuit at the same time.
Subservice	The subservice field: national, international, auto or decimal/hex value The auto means that the subservice is obtained from first received SLTM.
t35	The value and action for t35. Value is in msec, action is either st or timeout, If you use overlapped dialling dial plan, you might choose:4000,st.
User Part	The type of User Part.
Variant	running under SS7 standard.
OPC	The point code for this SS7 signalling point.
DPC	The destination point code.
1



T

Set to Default	Set the linkset as the default linkset.
Original Called	Information sent in the forward direction when a call is redirected and
Number	identifies the original called party.

## 3.4.2 Link Settings

Link Settings	Link Settings												
Link Name	iftype	Enabled	LinkSet	Channels	Schannel	First CIC	Echo Cancel	Echo Cancel Train	Echo Cancel Taps	<b>SLS</b>	SLTM	Port	Action
11	E1	yes	siuc	1-15,17-31	16	1	no	350	128	0	yes	1	0
12	E1	yes	siuc	1-31		32	no	350	128	0	yes	2	0
13	E1	yes	siuc	1-31		63	no	350	128	0	yes	3	0
14	E1	yes	siuc	1-31		94	no	350	128	0	yes	4	0

Figure 3-4-3 Link Settings

You can click button as shown below.

### Figure 3-4-4 SS7 Edit Link Settings

Edit Link "link-I1"	
<b>V</b> SS7 Link Settings	
Name:	n
Enabled:	
Interface Type:	E1
Link Set:	siuc 🔻
Channels:	1-15,17-31
Schannel:	16
First CIC:	1
Echo Cancel:	no (default) 🔻
Echocan Train:	350 Range: 10-10000.Default value: 300
Echocan Taps:	128 (default) 🔻
SLS:	0
SLTM:	
Port:	1.

Save Cancel



## 3.4.3 SS7 Configuration file backup and restore

### Figure 3-4-5 Configuration file backup and restore

🖤 SS7 Config. File Backup	
Download SS7 Configuration File	Download Backup
S\$7 Config. File Restore	
New configuration file: 选择文件 未选择任何文件	File Upload

# 4 VOIP

## **4.1 VOIP Endpoints**

## 4.1.1 SIP Endpoints

This page shows everything about your SIP, you can see status of each SIP.

#### Figure 4-1-1 SIP Status

SIP Endpoint			
Endpoint Name	Registration	Credentials	Actions
1001	server	1001	2
Add New SIP Endpoint			

## 4.1.2 Main Endpoint Settings

You can click Add New SIP Endpoint button to add a new SIP endpoint, and if you want to modify

existed endpoints, you can click *local* button.

There are three kinds of registration types for choose. You can choose Anonymous, Endpoint registers with this gateway or This gateway registers with the endpoint.

You can configure as follows:

If you set up a SIP endpoint by registration "None" to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)



#### Figure 4-1-2 None Registration

Edi	t SIP Endpoint "7001"	
	Main Endpoint Settings	
	Name:	7001
	User Name:	7001 Anonymous
	Password:	
	Registration:	None
	Hostname or IP Address:	172.16.8.38
	Transport:	UDP V
	NAT Traversal:	Yes •
	Advanced:Registration Options	
	Call Settings	
	Fax Options	
Sa	ve Apply Cancel	

For convenience, we have designed a method that you can register your SIP endpoint to your gateway, thus your gateway just works as a server.

#### Figure 4-1-3 Endpoint Register with Gateway

#### Edit SIP Endpoint "1001"

	Main Endpoint Settings					
	Name:	1001				
	User Name:	1001 Anonymous				
	Password:					
	Registration:	Endpoint registers with this gateway				
	Hostname or IP Address:	dynamic				
	Transport:	UDP •				
	NAT Traversal:	Yes •				
	Advanced:Registration Options					
	Call Settings					
	Fax Options					
Sa	ve Apply Cancel					

Also you can choose registration by "This gateway registers with the endpoint", it's the same with

"None", except name and password.



### Figure 4-1-4 This Gateway Register with the Endpoint

Add New SIP Endpoint

	Main Endpoint Settings				
	Name:	6001			
	User Name:	6001 Anonymous			
	Password:	••••			
	Registration:	This gateway registers with the endpoint			
	Hostname or IP Address:	172.16.8.38			
	Transport:	UDP •			
	NAT Traversal:	Yes			
	Advanced:Registration Options				
	Call Settings				
	Fax Options				
Sa	ve Apply Cancel				

Options	Definition
Name	A name which is able to read by human. And it's only used for user's reference.
Username	User name the end point use to authenticate with the gateway.
Password	Password the endpoint will use to authenticate with the gateway. Allowed characters.
Registration	Whether this endpoint will register with this gateway.
Hostname or IP Address	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a dynamic IP address. This will require registration. Notice: if the input here is hostname and your DNS has changed, you must reboot asterisk.
Transport	This sets the possible transport types for outgoing. Order of usage, when the respective transport protocols are enabled, is UDP, TCP, TLS. The first enabled transport type is only used for outbound messages until a Registration takes place. During the peer Registration the transport type may change to another supported type if the peer requests so.
NAT Traversal	Addresses NAT-related issues in incoming SIP or media sessions.

### Table 4-1-1 Definition of SIP Options



## 4.1.3 Advanced Registration Options

Options	Definition		
Authentication User	A username to use only for registration.		
Register Extension When Gateway registers as a SIP user agent to a (provider), calls from this provider connect to this local extension			
From User	om User A username to identify the gateway to this endpoint.		
From Domain A domain to identify the gateway to this endpoint.			
Remote Secret	A password which is only used if the gateway registers to the remote side.		
Port	The port number the gateway will connect to at this endpoint.		
Qualify	Whether or not to check the endpoint's connection status.		
Qualify frequency Frequency	How often, in seconds, to check the endpoint's connection status.		
Outbound Proxy	A proxy to which the gateway will send all outbound signaling instead of sending signaling directly to endpoints.		

Table 4-1-2 Definition of Registration Options

## 4.1.4 Call Settings

Options	Definition			
	Set default DTMF Mode for sending DTMF. Default: rfc2833.			
DTMF Mode	Other options: 'info', SIP INFO message (application/ dtmf-relay);			
	'Inband', Inband audio (require 64kbit codec - alaw, ulaw).			
Trust	Whether or not the Remote-Party-ID header should be trusted.			

Table 4-1-3 Definition of Call Options



Remote-Party-ID	
Send	Whether or not to send the Remote-Party-ID header
Remote-Party-ID	
Caller ID	Whether or not to diaplay Caller ID
Presentation	whether or not to display Caller ID.

## 4.1.5 Advanced Signaling Settings

Table 4-1-4 Definition	of Signaling	Options
------------------------	--------------	---------

Options	Definition
Progress Inband	If we should generate in-band ringing. Always use 'never' to never use in-band signaling, Even in cases where some buggy devices might not render it. Valid values: yes, no, never. Default: never.
Append user=phone to URI	Whether or not to add;' user=phone' to URIs that contain a valid phone number.
Add Q.850 Reason Headers	Whether or not to add Reason header and to use it if it is available.
Honor SDP Version	By default, the gateway will honor the session version number in SDP packets and will only modify the SDP session if the version number changes. Turn This option off to force the SDP session version number and treat all SDP data as new data. This is require for devices that send non-standard SDP packets (observed with Microsoft OC S).By default This option is on.

-



É

Allow Transfers	Whether or not to globally enable transfers. Choosing 'no' will disable all transfers (unless enable in peers or users). Default is enabled.
Allow Promiscuous Redirects	Whether or not to allow 302 or REDIR to non-local SIP address. Note that promiscredir when redirects are made to the local system will cause loops since this gateway is incapable of performing a 'hairpin' call.
Max Forwards	Setting for the SIP Max-Forwards header (loop prevention).
Send TRYING on REGISTER	Send 100 Trying when the endpoint registers.

## 4.1.6 Advanced Timer Settings

Table 4-1-5 Definition	of Timer Options
------------------------	------------------

Options	Definition	
Default T1 Timer	This timer is used primarily in INVITE transactions. The default for Timer T1 is 500ms or the measured run-trip time between the gateway and the device if you have qualify=yes for the device.	
Call Setup Timer	If a provisional response is not received in this amount of time, the call will auto-congest. Defaults to 64 times the default T1 timer.	
Session Timers	Session-Timers feature operates in the following three modes: originate, Request and run session-timers always; accept, run session-timers only when requested by other UA; refuse, do not run session timers in any case.	
Minimum Session Refresh Interval	Minimum session refresh interval in seconds. Default is 90secs.	



Г

Maximum	
Session Refresh	Maximum session refresh interval in seconds. Defaults to 1800s.
Interval	
Session Refresher	The session refresher, uac or uas. Defaults to uas.

## 4.1.7 Fax Options

### Table 4-1-6 Definition of Fax Options

Options	Definition
Mode	Working mode T.38 and T.30.
Enabled	Enabled.
Error Correction	Error Correction.
	In some cases,T.38 endpoints will provide a T38FaxMxDatagram value (during
	T.38 setup) that is based on an incorrect interpretation of the T.38
	recommendation, and result in failures because Asterisk does not believe it can
Max Datagram	send T.38 packets of a reasonable size to that endpoint (Cisco media gateway
Max Datagram	are one example of this situation).In these cases, during a T.38 call you will see
	warring messages on The console/in the logs from the Asterisk UDPTL stack
	complaining about lack of buffer space to send T.38FaxMaxDatagram value
	specified by the other end[point, and use a configured value instead.
	FAX detection will cause the SIP channel to jump to the 'faX' extension (if exists)
Fax Detect	based one or more events being detected. The events that can be detected are
	an incoming CNG tone or an incoming T.38 re-INVITE request.



Fax Activity	activate T38 fax gateway with 'timeout' seconds.
Fax Timeout	activate T38 fax gateway with 'timeout' seconds.

## 4.2 IAX2 Endpoint

#### Figure 4-2-1 IAX2 Endpoint

IAX2 Endpoint			
Endpoint Name	Registration	Credentials	Actions
9001	none	9001@172.16.8.183	2 🗙
9002	none	9002@172.16.8.183	2 🗙
9003	none	9003@172.16.8.181	2 🗙

Add New IAX2 Endpoint



#### Figure 4-2-2 Edit IAX Endpoint "9001"

#### Edit IAX Endpoint "9001" Main Endpoint Settings 9001 Name: User Name: 9001 Password: •••• Registration: None • Hostname or IP Address: 172.16.8.183 Auth: md5 ۲ No 🔻 Transfer: No 🔻 Trunk: Advanced:Registration Options

Qualify:	Yes v
Qualify Smothing:	Yes T
Qualify Freq Ok:	60
Qualify Freq Not Ok:	60
Port:	4569
Require Call Token:	Yes T



VIAX Encryption			
	Encryption	n: No 🔻	
	Force Encryption	n: No T	
	VIAX Trunk settings		
•	Trunk Max Size :	128000	
	Trunk MTU :	0	
	Trunk Frequency :	20	
	Trunk Time Stamps:	No T	
	Min. RegExpire:	60	
	Max. RegExpire:	60	

Save Apply Cancel

#### Table 4-2-1 Definition of IAX2 Endpoint

Options	Definition
Name	A name which is able to read by human. And it's only used for user's reference.
User name	User name the endpoint will use to authenticate with the gateway.
Password	Password the endpoint will use to authenticate with gateway.
1 8550010	Allowed characters.
Pegistration	Whether this endpoint will register to this gateway or this gateway to the
Registration	endpoint.
	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a
Hostname or IP	dynamic IP address. This will require registration.
Address	Notice: If the input here is hostname and your DNS has changed, you must
	reboot asterisk.
Auth	Authentication method for connections.
Transfer	Disable or not IAX2 native transfer.
Trunk	Use IAX2 trunking with this host.
Qualify	Whether or not to check the endpoint's connection status.



Г

-

Qualify Smothing	Use an average of the last two PONG result to reduce falsely detected LAGGED host. The default is 'no'.	
Qualify Freq Ok	How frequently to ping the peer when everything seems to be OK, in milliseconds.	
Qualify Freq not	How frequently to ping the peer when it's either;	
Ok	LAGGED or UNAVAILABLE, in milliseconds.	
Port	The port number the gateway will connect to at this endpoint.	
Encryption	Enable IAX2 encryption. The default is no.	
Force Encryption	Force encryption insures no connection is established unless both sides support encryption. By turning this option on, encryption is automatically; turned on as well. The default is no.	
Trunk Max Size	Defaults to 128000 bytes, which supports up to 800; calls of ulaw at 20ms a frame.	
Trunk MTU	With a large amount of traffic on IAX2 trunk, there is a risk of bad voice quality when allowing the Linux system to handle fragmentation of UDP packets. Depending on the side of each payload, allowing the OS to handle fragmentation may not be very efficient. This setting sets the maximum transmission unit for AIX2 UDP trunking. The default is 1240 bytes which means if a trunk's payload is over 1240 bytes for every 20ms it will be broken into multiple 1240 bytes messages. Zero disables this functionality and let's the OS handle fragmentation.	
Trunk Frequency	How frequently to send trunk msgs (in ms). This is 20ms by default.	



-

	Should we send timestamps for the individual sub_frames within trunk frames	
	There is a small bandwith use for these (less than 1kbps/call), but they ensure	
Trunk Time	that frame timestamps get sent end-to-end properly. If both ends of all your	
Stamps	trunks go directly to TDM, _and_your trunkfreq equals the frame length for your	
	codecs, you can probably suppress these. The receiver must also need to have	
	it enabled.	
Min. RegExpire	Minimum amounts of time that IAX2 peers can request as a registration interval	
	(in seconds).	
Max. RegExpire	Maximum amounts of time that IAX2 peers can request as a registration	
	expiration interval (in seconds).	

# 4.3 Advanced SIP Settings

## 4.3.1 Networking

Options	Definition
UDP Bind Port	Choose a port on which to listen for UDP traffic.
Enable TCP	Enable server for incoming TCP connection (default is no).
TCP Bind Port	Choose a port on which to listen for TCP traffic.
ТСР	The maximum number of seconds a client has to authenticate. If the client
Authentication	does not authenticate before this timeout expires, the client will be
Timeout	disconnected. (default value is: 30 seconds).
ТСР	The measure purpher of uncuthenticated econics that will be
Authentication	
Limit	allowed to connect at any given time (default is: 50).

### Table 4-3-1 Definition of Networking Options



Enable Hostname Lookup	Enable DNS SRV lookups on outbound calls Note: the gateway only uses the
	first host in SRV records Disabling DNS SRV lookups disables the ability to
	place SIP calls based on domain names to some other SIP users on the
	Internet specifying a port in a SIP peer definition or when dialing outbound
	calls with suppress SRV lookups for that peer or call.

## 4.3.2 Advanced NAT Settings

Options	Definition
Local Network	Format:192.168.0.0/255.255.0.0 or 172.16.0.0/12. A list of IP address or IP ranges which are located inside a NATed network. This gateway will replace the internal IP address in SIP and SDP messages with the external IP address when a NAT exists between the gateway and other endpoints.
Local Network List	Local IP address list that you added.
Subscribe Network Change Event	Through the use of the test_stun_monitor module, the gateway has the ability to detect when the perceived external network address has changed. When the stun_ monitor is installed and configured, chan_sip will renew all outbound registrations when the monitor detects any sort of network change has occurred. By default this option is enabled, but only takes effect once res_stun_monitor is configured. If res_stun_monitor is enabled and you wish to not generate all outbound registrations on a network change, use the option below to disable this

### Table 4-3-2 Definition of NAT Settings Options



	feature.
Match External Address Locally	Only substitute the exeternaddr or externhost setting if it matches.
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address used for staticly defined hosts. This helps avoid the configuration error of allowing your users to register at the same address as a SIP provide.
Externally Mapped	The externally mapped TCP port, when the gateway is behind a static NAT or PAI.
External Address	The external address (and optional TCP port) of the NAT. External address=hostname [:port] specifies a static address[:port] to be used in SIP and SDP messages. Examples: External address=12.34.56.78 External address=12.34.56.78.9900.
External Hostname	The external hostname (and optional TCP port) of the NAT. External Hostname=hostname[:port] is similar to "External address". Examples: External Hostname=foo.dyndns.net
Hostname Refresh Interval	How often to perform a hostname lookup. This can be useful when your NAT device lets you choose the port mapping, but the IP address is dynamic. Beware you might suffer from service disruption when the name server resolution fails.



## 4.3.3 Advanced RTP Settings

Options	Definition
Start of RTP Port Range	Start of range of port numbers to be used for RTP.
End of RTP port Range	End of range of port numbers to be used for RTP.

Table 4-3-3 Definition of RTP Settings Options

## 4.3.4 Parsing and Compatibility

Options	Definition
Strict RFC	Check header tags, character conversion in URIs, and multiline headers for
	strict SIP compatibility (default is yes).
Send Compac	Send compact SIP headers.
SDP Owner	Allows you to change the username filed in the SDP owner string.
	This filed MUST NOT contain spaces.
	When a dialog is started with another SIP endpoint, the other endpoint should
	include an Allow header telling us what SIP methods the endpoint implements.
Disallowed SIP Methods	However, some endpoint either do not include an Allow header or lie about
	what methods they implement. In the former case, the gateway makes the
	assumption that the endpoint support all known SIP methods. If you know that
	your SIP endpoint does not provide support for a specific method, then you
	may provide a list of methods that your endpoint does not implement in the
	disallowed_ methods option. Note that if your endpoint is truthful with its Allow
	header, then there is need to set this option.
Shrink Caller ID	The shrinkcallerid function removes '(', ' ', ')', non-trailing '.', and '-' not in square

#### Table 4-3-4 Instruction of Parsing and Compatibility



Г

-

	brackets. For example, the caller id value 555.5555 becomes 5555555 when	
	this option is enabled. Disabling this option results in no modification of the	
	caller id value, which is necessary when the caller id represents something that	
	must be preserved. By default, this option is on.	
Maximum Registration	Maximum allowed time of incoming registrations and subscriptions (seconds).	
Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).	
Default	Default length of incoming/outgoing registration.	
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.	
Number of Registration	Number of registrations attempts before we give up.0=continue forever, hammering the other server until it accepts the registration. Default is 0 tries, continue forever.	

## 4.3.5 Security

#### Table 4-3-5 Instruction of Security

Option	Definition
Match Auth	If available, match user entry using the 'username' field from the authentication line instead of the 'from' field.
Realm	Realm for digest authentication. Realms MUST be globally unique according to RFC 3261. Set this to your host name or domain name.
Use Domain as Realm	Use the domain from the SIP Domains setting as the realm. In this case,



Г

	the realm will be based on the request 'to' or 'from' header and should match one of the domain. Otherwise, the configured 'realm' value will be used.
Always Auth Reject	When an incoming INVITE or REGISTER is to be rejected, for any reason, always reject with an identical response equivalent to valid username and invalid password/hash instead of letting the requester know whether there was a matching user or peer for their request. This reduces the ability of an attacker to scan for valid SIP usernames. This option is set to 'yes' by default.
Authenticate Options Requests	Enabling this option will authenticate OPTIONS requests just like INVITE requests are. By default this option is disabled.
Allow Guest Calling	Allow or reject guest calls (default is yes, to allow). If your gateway is connected to the Internet and you allow guest calls, you want to check which services you offer everyone out there, by enabling them in the default context.

## 4.3.6 Media

#### Table 4-3-6 Instruction of Media

Options	Definition
TOS for SIP Packets	Sets type of service for SIP packets.
TOS for RTP Packets	Sets type of service for RTP packets.



## 4.3.7 Codec Settings

Select codecs from the list below.

▼ Codec Settings	
Codec Priority 1:	G.711 u-law 🔻
Codec Priority 2:	G.711 a-law 🔻
Codec Priority 3:	GSM T
Codec Priority 4:	G.722 •
Codec Priority 5:	G.723 •
Codec Priority 6:	G.729 <b>•</b>

#### Figure 4-3-1 Codec Settings

# 4.4 Advanced IAX2 Settings

Options	Definition
Bind Port	Bind port and bindaddr may be specified.
Enable IAXCompat	More than once to bind to multiple addresses, but the first will be the default.
Enable No Checksums	Set iaxcompat to yes if you plan to use layered switches or some other scenario which may cause some delay when doing a lookup in the dialplan. It incurs a small performance hit to enable it. This option cause Asterisk to spawn a separate thread when it receives an IAX DPREQ (Dialplan Request) instead of blocking while it waits for a response.
Enable Delay Reject	Disable UDP checksums (if no checksums is set, then no checksums will be calculated/checked on system supporting the feature).
ADSI	ADSI (Analog Display Services Interface) can be enable if you have (or may



	have) ADSI compatible CPE equipment.
SRV Lookup	Whether or not to perform an SRV lookup on outbound calls.
AMA Flags	You may specify a global default AMA flag for iaxtel calls. These flags are used in the generation of call detail records.
Auto Kill	If we don't get ACK to our NEW within 2000ms,and autokill is set to yes, then we cancel the whole thing(that's enough time for one retransmission only ).This is used to keep things from stalling for a long time for a host that is not available for bad connections.
Language	You may specify a global default language for users. This can be specified also on a per-user basis. If omitted, will fallback to English(en).
Account Code	You may specify a default account for Call Detail Records (CDRs) in addition specifying on a per-user basis.

#### Table 4-4-2 Instruction of Music on Hold

Options	Definition
Mohsuggest	The 'Mohsuggest' option specifies which music on hold class to suggest to the peer
	channel when this channel place the peer on hold. It may be specified globally or
	on a per-user or per-peer basis.
Mohinterpret	You may specify a global default language for users. This can be specified also on
	a per-user basis. If omitted, will fall back to English(en).

#### Table 4-4-3 Instruction of Codec Settings

Options	Definition
Band Width	Specify bandwith of low, medium, or high to control which codes are used in

-



Г

	general.
Disallow	Fine tune codes here using "allow" and "disallow" clause with specific codes.
Allow	Fine tune codes here using "allow" and "disallow" clause with specific codes.
Codec Priority	Codec priority controls the codec negotiation of an inbound IAX2 call. This
	option is inherited to all user entity separately which will override the setting in
	general.

Options	Definition
Jitter Buffer	Global default as to whether you want the jitter buffer at all.
	In the ideal world, when we bridge VoIP channels we don't want to jitter buffering on
Force Jitter	the switch, since the endpoints can each handle this. However, some endpoints may
Buffer	have poor jitter buffers themselves, so this option will force to always jitter buffer,
	even in this case.
Max Jitter	A maximum size for the iitter buffer
Buffers	
Resyncthreshold	When the jitter buffer notices a significant change in delay that continue over a few
	frames, it will resync, assuming that the change in delay was caused by a
	timestamping mix-up. The threshold for noticing a change in delay is measured as
	twice the measured jitter plus this resync threshold.
Max Jitter Interps	The maximum number of interpolations frames the jitter buffer should return in a row.
	Since some clients do not send CNG/DTX frames to indicate silence, the jitter buffer
	will assume silence has begun after returning these many interpolations. This

#### Table 4-4-4 Instruction of Jitter Buffer



Ι

Г

	prevents interpolating throughout a long silence.
Jitter Target Extra	Number of milliseconds by which the new jitter buffer will pad its size. The default is
	40, so without modification, the new jitter buffer will set its size to the jitter value may
	help if your network normally has low jitter, but occasionally has spikes.

Options	Definition
IAX Thread Count	Establishes the number of iax helper thread to handle I/O.
IAX Max Thread	Establishes the number of extra dynamic threads that may by spawned to
Count	handle I/O.
	The 'maxcallnumbers' option limits the amount of call numbers allowed for
	each individual remote IP address. Once an IP address reaches its call
Max Call Number	number limit, no more new connections are allowed until the previous ones
	close. This option can be used in a peer definition as well, but only takes effect
	for the IP of a dynamic peer after it completes registration.
	The 'maxcallnumbers-nonvalidated' is used to set the combined number of call
	numbers that can be allocated for connections where call token validation has
MaxCallNumbers_	been disabled. Unlike the 'maxcallnumbers' option, this limit is not separate for
Nonvalidated	each individual IP address. Any connection resulting in a non-call token
	validated call number being allocated contributes to this limit. For use cases,
	see the call should be sufficient in most cases.

### Table 4-4-5 Instruction of Misc Settings



#### Table 4-4-6 Instruction of Quality of Service

Options	Definition
Tos	Type of service
Cos	Class of service

# 4.5 Advanced fax setting

#### Table 4-5-1 Instruction of Quality of Fax Settings

Options	Definition
Udptl Start	DPTL start configure addresses.
Udptl End	DPTL end configure addresses.
Udptl Checksums	Whether to enable or disable UDP checksums on UDPTL traffic.
Udptl FEC Entries	The number of error correction entries in a UDPTL packet.
Udptl FEC Span	The span over which parity is calculated for FEC in a UDPTL packet.
Use Even Ports	Some VoIP providers will only accept an offer with an even-numbered
	UDPTL port. Set this option so that Asterisk will only attempt to use
	even-numbered ports when negotiating T.38. Default is no.
Maximum	Maximum Transmission Rate.
Transmission Rate	
Minimum	
Transmission Rate	
Send Progress/Status	Manager events with 'call' class permissions will receive events indicating



Γ

events to manager	the steps to initiate a fax session. Fax completion events are always sent to
session	manager sessions with 'call' class permissions, regardless of the value of
	this option.
Modem Capabilities	Set this value to modify the default modem options. Defasult:v17,v27,v29.
ECM	Enable/disable T.30 ECM(error correction mode) by default.



# **5** Routing

The gateway embraces the flexible and friendly routing settings for user. It supports up to 512 routing rules and about 100 pairs of calleeID/callerID manipulations can be set in a rule. It supports DID function (The usage of DID function: <u>How to use DID function with OpenVox T1/E1 Gateway</u>). The gateway support trunk group and trunk priority management.

## 5.1 Call Routing Rule

	Move	Order	Rule Name	From	То	Rules	Actions
	\$	1	6001to540	iax-6001	sip-540	Callee_Dial_pattern +[[](-+)] Caller_Dial_pattern +[][(-+)]	2 🗙
	\$	2	iaxtoports	iax-6001	grp-ports	Callee_Dial_pattern +I[](-*)] Caller_Dial_pattern +I[](-*)]	2 🗙
	\$	3	6001toport	sip-7001	grp-ports	Callee_Dial_pattern +[[][(-+)] Caller_Dial_pattern +[[][(-+)]	2 🗙
	New Call	Routing R	ule Save Orders				
Yc	ou are	e allov	wed to set up r	ew routing rule	e by New Call Routi	ing Rule, and after setting rou	uting rules.
			·	5	, 		<b>J</b>
m		uloc'	ordor by pullip	n up and down	click 2 button t	in adit the routing and	a dalata it
	oven	ules		g up and down			J delete It.
Finally click the Save Orders button to save what you set. Rules will show current routing rules.							
Oi	herw	ise yo	ou can set up เ	unlimited routin	ng rules.		
Tł	nere i	s an o	example for ro	uting rules num	nber conversion, it t	ransforms calling, called num	ber at the
same time. Suppose you want eleven numbers start at 159 to call the eleven numbers of start at							
136. Calling transform delete the three numbers from left, then writing number 086 as prefix, delete							
th	he last four numbers, and then add number 0755 at the end, it will show caller name is China						
Te	Telecom. Called transform adds 086 as prefix, and Change the last two number to 88.						

#### Figure 5-1-1 Routing Rules



processing rules	prepend	prefix	Match pattern	SdfR	StA	RdfR	Caller Name
Calling	086	159	xxxxxxx	4	0755		China
							lelecom
Called transformation	086	136	xxxxxx	2	88		N/A

#### Table 5-1-1 Example for routing rules number conversion

You can click

New Call Routing Rule button to set up your routings.

#### Figure 5-1-2 Example of Setup Routing Rule

#### Create a Call Routing Rule

Call Routing Rule	
Routing Name:	support
Call Comes in From:	1001 •
Send Call Through:	Port-1 T
Advance Routing Rule	
CalleeID/callerID Manipulation	
Callee_Dial_pattern: Prepend	+ Prefix II Match Pattern II (- SDfR + StA )I RdfR
Caller_Dial_pattern: Prepend	+ Prefix II Match Pattern II (- SDfR + StA )I RdfR I Caller Name
+ Add More Manipulation Fields	

The figure above realizes that calls from "support" SIP endpoint switch you have registered will be transferred to Port-1. When "Call Comes in From" is 1001, "prepend", "prefix" and "match pattern" in

"Advanced Routing Rule" are ineffective, and just "CallerID" option is available.

Table	5-1-2	Definition	of Routing	Options
-------	-------	------------	------------	---------

Options	Definition
Routing Name	The name of this route. Should be used to describe what types of calls.
Call Comes in From	The launching point of incoming calls.
Send call Through	The destination to receive the incoming calls.



Γ

Options	Definition
	A Dial Pattern is a unique set of digits that will select this route and send the call
	to the designated trunks. If a dialed pattern matches this route, no subsequent
	routes will be tried. If Time Groups are enabled, subsequent routes will be
	checked for matches outside of the designated time(s). Rules:
	X matches any digit from 0-9
	Z matches any digit from 1-9
	N matches any digit from 2-9
	[1237-9] matches any digit in the brackets (example: 1,2,3,7,8,9)
	. wildcard, matches one or more dialed digits
Dial Patterns	<b>Prepend</b> : Digits to prepend to a successful match. If the dialed number matches
that will use this	the patterns specified by the subsequent columns, then this will be prepended
Route	before sending to the trunks.
	<b>Prefix</b> : Prefix to remove on a successful match. The dialed number is compared
	to this and the subsequent columns for a match. Upon a match, this prefix is
	removed from the dialed number before sending it to the trunks.
	Match Pattern: The dialed number will be compared against the prefix + this
	match pattern. Upon a match, the match pattern portion of the dialed number will
	be sent to the trunks.
	SDfR (Stripped Digits from Right): The number of digits to be deleted from the
	right end of the number. If the value of this item exceeds the length of the current
	number, the whole number will be deleted.
	StA (Suffix to Add): Designated information to be added to the right end of the

### Table 5-1-3 Description of Advanced Routing Rule



	current number.			
	RDfR (Reserved Digits from Right): The number of digits to be reserved from			
	the right end of the number. If the value of this item under the length of the			
	current number, the whole number will be reserved.			
	Caller Name: What caller name would you like to set before sending this call to			
	the endpoint.			
	Sets Caller*ID data on t	he channel:		
	SIP_FROM(name),SIP_FROM(number) :			
	defalut:Sip From and Number			
	eg: When selecting SIP From, Name is Peter and Number is 402.			
	The From mode			
	\"Peter\" <sip:402@172.16.6.239;transport=udp>;tag=bd481672</sip:402@172.16.6.239;transport=udp>			
	SIP_TO(name),SIP_TO(number) :			
	defalut: EXTEN			
	eg: When selecting SIP To, Name is Jason and Number is 401.			
	To mode is: \"Jason\" <s< td=""><td>ip:401@172.16.6.239;tran</td><td>sport=UDP&gt;</td><td></td></s<>	ip:401@172.16.6.239;tran	sport=UDP>	
	<b>Non</b> e: Set Caller*ID	number which is to be	send on the channel fror	m
	PBX(manipulated if it se	ets).		
Forward	What destination number	er will you dial?		
Number	This is very useful when you have a transfer call.			
Failover Call				
Through	The gateway will attempt to send the call out each of these in the order you		u	
Number	specify.			



You can create various time routes and use these time conditions to limit some specific calls.

#### Figure 5-1-3 Time Patterns that will use this Route

Time Patterns that will use this Route					
Time to start: 00 ▼ : 00 ▼	Week Day start: Monday	Month Day start: 01 🔻	Month start: January		
Time to finish: 02 ▼ : 00 ▼	Week Day finish: Thursday 🔻	Month Day finish: 31 🔻	Month finish: March 🔹	*	
+ Add More Time Pattern Fields					

If you configure like this, then from January to March, from the first day to the last day of these

months, from Monday to Thursday, from 00:00 to 02:00, during this time (meet all above time

conditions), all calls will follow this route. And the time will synchronize with your Sever time.

#### Figure 5-1-4 Forward Number

Forward Number	
Forward Number	
Custom Context	

You can configure forward number when you have a transfer call. You can also set your custom

context as you like before sending the call to the endpoint.

#### Figure 5-1-5 Failover Call Through Number

Failover Call Through Number	
Failover Call Through Number 1:	port 1 🔻
Failover Call Through Number 2:	port 2 🔻
Add a Failover Call Through Provider	

You can add one or more "Failover Call Through Numbers".

## 5.2 Groups

Sometimes you want to make a call through one port, but you don't know if it is available, so you have to check which port is free. That would be troublesome. But with our product, you don't need to worry about it. You can combine many Ports or SIP to groups. Then if you want to make a call, it will find available port automatically.



### Figure 5-2-1 Establish Group

Routing Groups	
Group Name:	ALLPORT
Туре:	T1/E1 V
Policy:	Roundrobin •
Members	NO.       All         1



# 6 Network

On "Network" page, there are three sub-pages, "Network Settings", "DDNS Settings", "Toolkit" and "Static Route Settings".

## **6.1 Network Settings**

There are two types of WAN port IP, Static and DHCP. Static is the default type, and it is 172.16.100.1. The LAN port is a fixed IP and it is 192.168.100.1.

#### Figure 6-1-1 WAN/LAN Settings Interface

WAN Setting	
Interface:	eth0
Туре:	Static •
MAC:	A0:98:05:01:DB:A4
Address:	172.16.100.205
Netmask:	255.255.0.0
Default Gateway:	172.16.0.1
LAN Setting	
Interface:	eth1
Enable:	
MAC:	A0:98:05:01:DB:A5
Address:	192.168.100.1
Netmask:	
	255.255.0

#### Table 6-1-1 Definition of WAN/LAN Settings

Options	Definition
Interface	The name of network interface.
	The method to get IP.
Туре	Static: manually set up your gateway IP.
	DHCP: automatically get IP from your local LAN.
MAC	Physical address of your network interface.



Address	The IP address of your gateway.
Network	The subnet mask of your gateway.
Default Gateway	Default getaway IP address.

DNS Servers: A list of DNS IP address. Basically, this info is from your local network service

provider. Note that please restart the gateway if you changed the DNS server.

Figure 6-1-2 DNS Interface

DNS Servers	
DNS Server 1:	8.8.8.8
DNS Server 2:	
DNS Server 3:	
DNS Server 4:	

## 6.2 DDNS Settings

You can set some static domain.

#### Figure 6-2-1 Static Domain Interface

Static Domain Settings		
(P	Domain	action
127.0.0.1	localhost.localdomain	×
127.0.0.1	dgw100x	×
		+



Also, you can enable or disable DDNS (dynamic domain name server).

### Figure 6-2-2 DDNS Interface

DDNS Settings	
DDNS	ON
Туре:	inadyn 🔻
User Name:	ddnstest
Password:	ddnstest
Your domain:	test.com

### Table 6-2-1 Definition of DDNS Settings

Options	Definition
DDNS	Enable/Disable DDNS (dynamic domain name server).
Туре	Set the type of DDNS server.
Username	Your DDNS account's login name.
Password	Your DDNS account's password.
Your domain	The domain to which your web server will belong.



## 6.3 Toolkit

It is used to check network connectivity. Support Ping command on web GUI.

#### Figure 6-3-1 Network Connectivity Checking

NETWORK Free Commun Catio	n
www.google.com Ping www.google.com Traceroute	
Report ping -c 4 www.google.com	
PING www.google.com (64.233.162.83) 56(84) bytes of data. 64 bytes from II-In-R3.1e100.net (64.233.162.83); icmp_seq=2 tII=41 time=306 ms 64 bytes from II-In-R3.1e100.net (64.233.162.83); icmp_seq=2 tII=41 time=306 ms 64 bytes from II-In-R3.1e100.net (64.233.162.83); icmp_seq=3 tII=41 time=357 ms 64 bytes from II-In-R3.1e100.net (64.233.162.83); icmp_seq=4 tII=41 time=303 ms 	
Result Successfully ping [ www.google.com ] .	

## **6.4 Static Route Settings**

#### Figure 6-4-1 Static Route Settings

Route Table							
Destination	Subnet Mask	Gateway		Metric		Interface	
0.0.0.0	172.16.0.1	0.0.0.0		0		eth0	
10.1.0.0	0.0.0.0	255.255.0.0		0		eth2	
172.16.0.0	0.0.0.0	255.255.0.0		0		eth0	
Static Route							
Destination	Subnet Mask	Gateway	Metric		Interface		Actions
Add							



# 7 Advanced

## 7.1 Asterisk API

When you make "Enable" switch to "ON", this page is available.

General	
Enable:	ON
Port:	5038
Manager	
Manager Name:	admin
Manager secret:	admin
Deny:	0.0.0/0.0.0
Permit:	172.16.100.110/255.255.0.0&192.168.1.0/2
Rights	
System:	read: 🗹 write: 🗹
Call:	read: 🗹 write: 🗹
Log:	read: 🗹 write: 🗹
Verbose:	read: 🗹 write: 🗹

#### Figure 7-1-1 API Interface



Options	Definition
Port	Network port number.
Manager Name	Name of the manager without space.
Manager secret	Password for the manager. Characters: Allowed characters "+.<>&0-9a-zA-Z". Length:4-32 characters.
Deny	If you want to deny many hosts or networks, use char & as separator. Example: 0.0.0.0/0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
Permit	If you want to permit many hosts or network, use char & as separator. Example: 0.0.0.0/0.0.0 or 192.168.1.0/255.255.255.0&10.0.0/255.0.0.0.



System	General information about the system and ability to run system management commands, such as Shutdown, Restart, and Reload.		
Call	Information about channels and ability to set information in a running channel.		
Log	Logging information. Read-only. (Defined but not yet used.)		
Verbose	Verbose information. Read-only. (Defined but not yet used.)		
Command	Permission to run CLI commands. Write-only.		
Agent	Information about queues and agents and ability to add queue members to a queue.		
User	Permission to send and receive UserEvent.		
Config	Ability to read and write configuration files.		
DTMF	Receive DTMF events. Read-only.		
Reporting	Ability to get information about the system.		
Dialplan	Receive NewExten and Var Set events. Read-only.		
Originate	Permission to originate new calls. Write-only.		
All	Select all or deselect all.		


Once you set like the above figure, the host 172.16.100.110/255.255.0.0 is allowed to access the

gateway API. Please refer to the following figure to access the gateway API by putty.

172.16.100.110 is the gateway's IP, and 5038 is its API port.

### Figure 7-1-2 Putty Access

# 7.2 Asterisk CLI

In this page, you are allowed to run Asterisk commands.

# Figure 7-2-1 Asterisk Command Interface Asterisk CLI Command: Execute Signalling: pri Operation: Lock / Unlock channel: Execute

Table 7-2-1 Definition of Asterisk CLI

Options	Definition
Command	Type your Asterisk CLI commands here to check or debug your gateway.

If you type "help" or "?" and execute it, the page will show you the executable commands.



Options	Definition
Signaling	Current signaling in use.
Operation	The advanced operations for lock and unlock channels.
Channel:	The channel to be lock or unlock.

### Table 7-2-2 Definition of Lock/unlock channels

# 7.3 Asterisk File Editor

On this page, you are allowed to edit and create configuration files. Click the file to edit.

Prime Config. Files		
File Name		File Size
system.conf		831
sip.conf		105
sip_endpoints.conf		2125
loager.conf		4775
extensions.conf		122
sip_general.conf		558
extensions_macro.conf		1263
extensions_routing.conf		1504
dahdi-channels.conf		1061
chan_dahdi.conf		606
Configuration Files List		
File Name	File Size	
aci.conf	2817	
adsiconf	140	
agents.conf	2531	
Immediver.conf 2084		
alsa conf 3498		
md.conf 767		
app_mysql.conf	1044	
338 338		
sterisk.conf 4501		
calendar.conf 5171		

### Figure 7-3-1 Configuration Files List

Click "New Configuration File" to create a new configuration file. After editing or creating, please

reload Asterisk.

# 7.4 Auto Provisioning

Auto provisioning or auto-configuration is an easy, flexible and time-saving way to upgrade firmware



and configurations for E1 gateways in mass deployment. With auto provisioning, all user information can be entered via the central ACS (Auto Configuration Server). ACS can be DHCP server or TFTP, HTTP and FTP server. It will not take effects immediately but in the next time system is power on. It could be postponed the execution of restart system also.

Note that system will not be upgrade the firmware and update configurations if the connection between ACS and gateway is disconnect.

### 7.4.1 Preparation

The following should be prepared before auto provisioning being applied.

- Enable the auto provisioning in gateway
- The ACS has been prepared
- The network between gateway and ACS is connected

### 7.4.2 Configuring gateway

Usually, the feature is disabled before being on sale. To activate the auto provisioning function, please follow the procedures as below.

### Step 1 On the ADVANCED-> Auto Provision interface

**Step 2** Enable the 'Enabled' option and select ACS. DHCP option 66 can be enabled if ACS has been working as DHCP server, otherwise please select protocol of provisioning and fill the value of '*Auto Config Server URL*'. Username and password may need to be filled in FTP/HTTP for the purpose of system safety. Do not forget to select Firmware upgrade, upgrade mode and fill the value of timeout, and click '*Save*'.

Step 3 Set interval of checking in LOGS->System notice then enable it, and click 'Save'.



Table 7-4-1 Definition	of Auto	Provision
------------------------	---------	-----------

Options	Definition
Enabled	Whether to enable or disable Auto Provision.
DHCP Option 66	Get ACS server address from Option 66 via DHCP.
Protocol	Set protocol of connection.
Auto Config Server URL	The config server domain or IP address.
User Name	The account of downloading from ACS.
Password	The password of downloading from ACS.
Timeout	The max limit time for downloading firmware.
Firmware Upgrade	Enable/disable the mode of downloading firmware.
	Select upgrade time.
	Power: start upgrade configuration when Power on. Power + Period:
opgrade mode	Set the frequency of checking the latest configuration when gateway
	running.

## Table 7-4-2 Definition of system notice

Options	Definition
Enable	Whether to enable or disable system notice.
Check Interval	When Upgrade Mode is set, this parameter specifies the interval of Checking.



### Figure 7-4-1 Auto Provision interface

Auto Provision Settings	
Enabled:	ON
DHCP Option 66:	OFF
Protocol:	TFTP -
Auto Config Server URL:	172.16.6.111 (172.168.0.X / domain.com )
User Name:	
Password:	
Timeout:	120 Sec.
Firmware Upgrade:	ON
Upgrade Mode:	Power On + Period
L	

# 7.4.3 Configuring ACS

Save

Г

The Auto Configuration Server can be the one of TFTP, FTP and HTTP server. The ACS is used to store the firmware release and configurations files of the devices under management.

List the primary files in ACS download directory as table 7-4-3:

Options	Definition
DGW100x-current.bin	The firmware image.
common.conf	The wildcard configuration file for the whole gateway.
defconfig.tar.gz	The default(factory) configuration file.
EPC-{mac}.conf	The private configuration file for the specified gateway. Naming rules: "EPC-" + "mac" +".conf". The naming prefix of "EPC-" stands for the private configuration file, "mac" is the physical address of network interface card but removed semicolon

### Table 7-4-3 Definition of ACS files



and ".conf" is the suffix. For example, the
EPC-a0980501dbca.conf, 'a0980501dbca' is the MAC address
(A0:98:05:01:DB:CA).

The format of common.conf , EPC-{mac}.conf and defconfig.tar.gz:

(1). Common.conf

[firmware]

FW\_NAME=DGW100x-current.bin //Firmware image name

FW\_MD5=b3603f3c3b5e7eb6326498640f151c79 //The md5 of firmware image

FW\_VERSION=1.1.2 //Firmware version

[configs]

CONFIG\_NAME=defconfig.tar.gz // default configuration file(compressed)

CONFIG\_MD5KEY=2cd2dfbe52482405350816e3698cb530 // the md5 of default configuration

file

### (2).EPC-{mac}.conf

[dns]

DNS\_SERVER1=8.8.8.8

DNS\_SERVER2=8.8.4.4

DNS\_SERVER3=

DNS\_SERVER4=

[ntp]

NTP\_SERVER1= 0.cn.pool.ntp.org

NTP\_SERVER2= time.nist.gov

NTP\_SERVER3= time.windows.com

### [eth0]

OPENVOX



ENABLE=yes

TYPE=static

DHCP=no

IPADDRESS=172.16.100.223

NETMASK=255.255.0.0

GATEWAY=172.16.0.1

[eth1]

ENABLE=yes

TYPE=static

DHCP=no

IPADDRESS=192.168.100.223

NETMASK=255.255.0.0

GATEWAY=192.168.0.1

[web\_login]

username=admin

password=admin

(3). Defconfig.tar.gz

### Figure 7-4-2 the overview of defconfig.tar.gz

[root@dgw100x	/defconfig]#ls			
config.info	group-	passwd	resolv.conf	sysconfig
fstab	hosts	passwd-	shadow	tmp
group	nsswitch.conf	profile	shadow-	
[root@dgw100x	/defconfig]#ls s	ysconfig/		
NTP	hostname	nsswitch.conf	f simple.scri	pt
asterisk	lighttpd	ntp.conf	syslog.conf	
cron	logrotate.conf	f php.ini	udhcpd.conf	
dahdi	logrotate.d	redis.conf	zoneinfo	
dnsmasq	network	services		
[root@dgw100x	/defconfiq]#			



### 7.4.4 Provisioning example

After auto provisioning is enabled, the gateway will visit the Auto Configuration Server and download the updated files periodically based on the timer *Check Interval* (LOGS->System **notice**). By default, the timer is set as every hour. System will receive a message from ACS, like figure 7-4-3, and the message will be display in the system notice (LOGS->System Notice). Auto provisioning will not take effects immediately but in the next time system is power on. It could be postponed the execution of restart system also.

Now, an example of using Auto Provisioning will be given in the following.

1. Activate the auto provision (TFTP) in **ADVANCED-> Auto Provision** like figure 7-4-4.

Auto Provision Settings	
Enabled:	ON
DHCP Option 66:	OFF
Protocol:	TFTP -
Auto Config Server URL:	172.16.6.111 (172.168.0.X / domain.com )
User Name:	
Password:	
Timeout:	120 Sec.
Firmware Upgrade:	ON
Upgrade Mode:	Power On + Period
-	

Figure 7-4-3 Auto provision settings

- Save
- 2. Enable the check interval in LOGS->Log settings->System Notice like figure 7-4-5.

Figure 7-4-4 Check interval setting

System Notice	
Enable:	ON
Check Interval:	Every hour
Save	



- 3. Configuring the ACS (Generate the md5 of firmware and defconfig.tar.gz)
  - Copy the firmware, defconfig.tar.gz, common.conf and EPC-{mac}.conf to the working

directory of TFTP server.

Figure	7-4-5	The	workina	directorv	of	TFTP	server
					•••		

generate_md5_tool	2016/3/8 15:14	文件夹	
퉬 Tftpd32汉化版	2016/3/8 15:14	文件夹	
🖉 common.conf	2016/3/8 15:17	CONF 文件	1 KB
defconfig.tar.gz	2015/12/10 11:28	GZ 文件	390 KB
DGW100x-current.bin	2016/3/8 15:04	KuaiZipMount.bin	42,641 KB
EPC-a0980501dbca.conf	2015/9/22 13:25	CONF 文件	1 KB
😭 tftpd32.chm	2015/8/31 16:50	编译的 HTML 帮	330 KB
🏘 tftpd32.exe	2015/8/31 16:50	应用程序	211 KB
ittpd32.ini	2015/12/10 18:25	配置设置	3 KB

Notice: The demo of E1 gateway mac address is A0:98:05:01:DB:CA (eth0), therefore the private

configuration file is EPC-a0980501dbca.conf.

 Generate the md5 of firmware and defconfig.tar.gz. Then fill in common.conf and EPC-{mac}.config.

WinMD5 v1.0 - eolson@mit.edu	X
Currently	
8d8a5f5980f7bd12211bbf673f6eb193 58d73303a5f53fbd18d213be5f3acefd	DGW100x-current.bin defconfig.tar.gz
Drag files into this window to compute their	Quit

### Figure 7-4-6 Generate the md5 of firmware and configuration

### Figure 7-4-7 Common.conf

[root@localhost build]# cat common.conf
[firmware]
FW\_NAME=DGW100x-current.bin
FW\_MD5=8d8a5f5980f7bd12211bbf673f6eb193
FW\_VERSION=1.1.2

```
[configs]
CONFIG_NAME=defconfig.tar.gz
CONFIG_MD5KEY=58d73303a5f53fbd18d213be5f3acefd
[root@localhost_build]#
```

Figure 7-4-8 EPC- a0980501dbca.conf

[root@localhost build]# cat EPC-a0980501dbca.conf
[dns]
DNS SERVER1=8.8.8.8
DNS SERVER2=8.8.4.4
DNS SERVER3=
DNS SERVER4=
[ntp]
NTP SERVER1= 0.cn.pool.ntp.org
NTP SERVER2= time.nist.gov
NTP_SERVER3= time.windows.com
[eth0]
ENABLE=yes
TYPE=static
DHCP=no
IPADDRESS=172.16.100.223
NETMASK=255.255.0.0
GATEWAY=172.16.0.1
[eth1]
ENABLE=yes
TYPE=static
DHCP=no
IPADDRESS=192.168.100.223
NETMASK=255.255.0.0
GATEWAY=192.168.0.1
[web_login]
username=admin
password=admin
[root@localhost build]# _

• Start TFTP service. Tftpd32.exe is a useful TFTP tools in windows7, then make sure

TFTP server is select.



Figure 7-4-9 A demo TFTP server

Tftpd32 by Pł	n. Jounin		- 🗆 🗙
Current Directory	E:\tftpd32.450	-	Browse
Server interfaces	172.16.6.111	Realtek PC 🔻	Show Dir
Tftp Server Tftp	Client DHCP server Lo	og viewer	
peer	file	start time p	progress
•	III		۱.
About	Settings		Help

4. The system will receive an auto provision message in web GUI.

### Figure 7-4-10 System notice logs

Notice Logs		
Date	Subject	Content
2016/03/08 15:55:47	Auto-provision Upgrade Notification	A new firmware and configs could be upgraded from ACS. Current release is : 1.1.0, ACS server release is : 1.1.2. If you want to upgrade, please restart the system and wait several minutes.
		Refresh Clean Up

### Figure 7-4-11 Auto provision upgrade notification





5. Restart the system. It will take about 3 minutes almost to download, upgrade Firmware and

update configurations.

Figure 7-4-12 Downloading the firmware and configs

C OK 1 Setting up interface lo... [ OK ] starting SSH service . . . . . . [ OK ] starting Redis service ..... [ OK ] starting SOAP service..... C OK J Checking the network between IFTP server and T1/E1 Gateway, wait a mom Info: Auto-Provision switch has been enabled Info : Checking firmware upgrade flag... [ On ] Auto Configuration Server URL : 172.16.6.111 Info : Checking firmware md5... [ mismatch ] Preparing to download new fw image from 172.16.6.111. firmware URL : 172.16.6.111 DGW100x-current.bin firmware name firmware download from : tftp Download Progress: 13.5M, Time lapses: 18 Sec

Figure 7-4-13 Applying the firmware and configs



# **7.5 SNMP**

Simple Network Management Protocol (SNMP) is an application–layer protocol, which is used to manage and monitor network elements and exchange management information between network devices. By default, SNMP uses port 161 for communication.

Since the inception SNMP, it embraces three versions: v1, v2c and v3. V1 and v2c are the most implemented version of SNMP; v3 is target at the high security when compare to its older versions.

The gateway support private SNMP MIBs (private enterprise number) to access.



# 7.5.1 Parameters in SNMP setting

Table 7-5-1 Definition of SNMP Settin	Table	7-5-1	Definition	of SNMP	setting
---------------------------------------	-------	-------	------------	---------	---------

Options	Definition
SNMP Enable	Whether to enable SNMP.
System Contact	System contact information(optional).
System Location	The locale of system contact(optional).
	The number is used for defining private SNMP MIBs which is
Private Enterprise Number	assigned by Internet Assigned Numbers Authority (IANA). For
	more information, please access:
	http://pen.iana.org/pen/PenApplication.page.
SNMP Version	Select version of SNMP.
Community Configuration	Define a community name to security name.
Group Configuration	Define the security name to a group.
View Configuration	Set a view to let the group have rights to do.
Access Configuration	Grant the group can access to the view(read/write/notify).
User Configuration	Only exist in v3. Add a v3 account to SNMP. Notice that the
ooor oorniguration	length of auth password and privacy password are more than 8.

# 7.5.2 Activating SNMP

Usually, the feature is disabled by default. To activate the SNMP feature, please follow the Figure

7-5-1.



The Interface is in the ADVANCED->SNMP. System contact, location and private enterprise

number are optional. Figure 7-5-1 is the SNMP setting interface.

Figure	7-5-1	Activating	the	SNMP
		/		•••••

SNMP	Parameter									
	SNMP Enable:	ON	ON							
	System Contact:	administrator	administrator							
	System Location:	ShenZhen								
Priva	te Enterprise Number(PEN):	42421								
	SNMP Version:	v2c 💌								
Comm	unity Configuration									
Order	Security Name				Community					
1	notConfigUser				public					
Group	Configuration									
Order	Group				Security Name					
1	notConfigGroup				notConfigUser					
View (	Configuration									
Order	ViewName		ViewType	View Subtro	ee			ViewMask		
1	all	included .1		.1			NA			
Acces	s Configurationv1/v2c									
Order	Group			Read			Write		Notify	
1	notConfigGroup			all		•	none	•	none	•
Save										

**Note:** Do not forget to click '*Save*' to take effect. After configuration, The SNMP feature is activated immediately.

### 7.5.3 Verify SNMP

A powerful, indispensable and easy-to-use MIB browser is convenient for engineer/manager to manage SNMP enabled network devices and applications. In this session, Manage Engine MIB browser is selected. It allows user to issue SNMP requests to retrieve agent's data, or make changes to the agent. It is free tool for Windows, Mac and Linux.

(1). Get SNMP parameters via SNMP MIB browser. It's supposed that Manage Engine MIB browser is installed perfectly. Figure 7-5-2 is the main interface of Manage Engine MIB browser.



			~
ManageEngine MibBrowse	er Free Tool		×
<u>File Edit View Operations</u>	<u>H</u> elp		
ۇ 🖬 🗞 🗉 🌜	3 🖻 🖌	" 🗊 🔊 🧠 🏹 途 💷 🕷 🛫 🚭 🧇 🖾 🚺 Dounload More Free Tools	
Caaded MibModules	Host Community Set Value Object ID	SNMPWALK Variable <ul> <li>Port</li> <li>161</li> <li>Write Community</li> <li>Image: Community</li></ul>	
	Loading MIBs .\r MIB(s) Loaded S	mibs\RFC1213-MIB_\mibs\IF-MIB Successfully	*
	Description Ma	ultiVar	
	Syntax	Status	
	Access	Reference	
	Index		
	Object ID		
Global View 🕅	Description		

Figure 7-5-2 Manage Engine MIB browser

And the field of *Host*, *Port* and *Community* are filled with **172.16.100.223**, **161** and **public** respectively. Object ID is the node of SNMP MIBs, e.g. ".1.3.6.1.2.1.1.6.0" is system location and ".1.3.6.1.2.1.1.1.0" is system description.

Figure 7-5-3 Get system location

ManageEngine MibBrowser Free Tool					
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>O</u> perations <u>H</u> elp					
ي 🖬 🚷 🖻 🍓	5 🖻	🔚 🙀 🔊 🕺 🏷 🕸 🛅 🕷 🛫 🐵 🖉 🥥 🚺 Download More Free Tools			
ded MibModules ANAirType-MIB RFC1213-MIB F-MIB SIMPV2-MIB internet 	Host Community Set Value Object ID	172.16.100.223       Port       161         *******       Write Community         iso. org. dod. internet. mgmt. mib=2. system. sysLocation. 0         /mibs/RFC1213-MIB./mibs/IF-MIB			
sysObjectID % sysUpTime sysContact	tD MIB(s) Loaded Successfully ec Sent GET request to 172.16.100.223 : 161				
≪ sysName ≪ sysLocation ≪ sysServices ≪ sysORLast(	sysLocation.0 ShenZhen				
i⊡⊞ sysORTable ⊛⊡ snmp	Description	MultiVar			
i≟⊶Cii snmpV2	Syntax Access	DisplayString (SIZE (0255)) Status current read-write Reference			
Global View	Object ID Description	.1.3.6.1.2.1.1.6 "The physical location of this node (e.g., `telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string."			

After the rest field has been filled, then verify it. Click **Operations->GET** to get the value of system

location and it returns the value which we just set.

(2). Set SNMP parameters via SNMP MIB browser. For example, set the system name. system



name is "dgw100x" by default, then set it as "VoIP gateway". See figure 7-5-4.

- Click **Operations->GET** to attain the current system name.
- Fill the field of Set Value with "VoIP gateway".
- Click **Operations**->**SET** to set the system name.
- Click **Operations->GET** to attain the modified system name.

ManageEngine MibBrowser Free Tool					
<u>File E</u> dit <u>V</u> iew <u>O</u> perations <u>H</u> elp					
ے 🖬 🖄 🗈 🍰	🗿 🖻 🖷 🗊 🜮 🧠 🏹 🕸 🛅 👋 🛫 🚭 🧼 💹 🚺 Download				
Loaded MibModules DIGIUM-MIB ANAirType-MIB RFC1213-MIB Gradies F-MIB ASTERISK-MIB SNMPv2-MIB	Host     172.16.100.223     Port     161       Community     ******     Write Community     ******       Set Value     VoIP gateway     •       Object ID				
	Sent GET request to 172.16.100.223 : 161           sysName.0         dgw100x           Sent SET request to 172.16.100.223 : 161           sysName 0         VoIP rateway				
	Sent GET request to 172.16.100.223 : 161 SysName.0 VoIP gateway				
	Description     MultiVar       Syntax     Status       Access     Reference				
<	Index Object ID Description				

### Figure 7-5-4 Set system name

# 7.6 TR069

TR069 is a remote management solution which offers a single interface to manage the ACS and automate the deployment and support of data, voice and video services, thereby reducing operation and support costs, while enhancing customer satisfaction. Its user-friendly interface covers the entire service lifecycle, from centralized remote provisioning of services, to inventory management, group updates, monitoring, event triggering, and support automation. Figure 7-6-1 is TR069 configuration interface and table 7-6-1 is its definition.



Options	Definition		
Acs Url	Specify the URL of the ACS		
Acs Username	Specify the user name to be used by the device to authenticate with the ACS.		
Acs Password	Specify the password to be used by the device to authenticate with the file server		
Provisioning Code	Information of the device vendor, which may be used to indicate the primary service provider and other provisioning information to the ACS. It can be numbers or English letters.		
Model Name	A brief description of the interface type or name. It is a string of characters.		
Periodic Enable	Used to specify whether to periodically report to the ACS.		
Periodic Interval	The interval for reporting to the ACS.		
Connection Request	The address used for the ACS to connect back to the device.		
Connection Request Username	The account used for the ACS to connect back to the device, for example, admin.		
Connection Request Password	The password used for the network management server to connect back to the device.		

### Table 7-6-1 Definition of TR069 configuration interface



### Figure 7-6-1 TR069 configuration interface

TR069 Parameter	
Enable:	ON
Acs Url:	http://172.16.80.121
Acs Username:	admin
Acs Password:	admin
Provisioning Code:	
Model Name:	
Periodic Enable:	ON
Periodic Interval:	1800
Connection Request Url:	http://172.16.100.110:7547/
Connection Request Username:	
Connection Request Password:	
Save	

# 7.7 Network Capture

The gateway has been supplied a network packets capture in the web for ease of user to analysis,

capture and monitor the gateway's network status, RTP flows, protocol analysis and so on.

Options	Definition			
Network Interface	Specify which interface to be capture packets from. 'All' means			
	capture packets from all interfaces.			
Source host	Specify which source host IP address to listen for.			
Destination host	Specify which destination host IP address to listen for.			
Port	To specify a port that is either source or destination direction.			
	To specify which protocol to be captured, 'All' stands for capture			
Protocol	multi-protocols, the SIP default port is 5060, If you are using a			
	different port, please amend it.			

 Table 7-7-1 Definition of Network capture



The interface is in **ADVANCED->Network Capture**.

Figure	7-7-1	Network	capture	interface
1.9410			oupturo	

Network Capture	
Network Interface:	● Eth0 ◎ Eth1
Source host:	ii.
Destination host:	it.
Port:	
Protocol:	● ALL ◎ TCP ◎ UDP ◎ RTP ◎ RTCP ◎ ICMP ◎ ARP ◎ SIP
Start Stop Reset	

Moreover, user can capture SS7 signal and record port.

### Figure 7-7-2 Signal Capture interface

SS7 Signal Capture	
Direction:	● Both (default)   ◯ In   ◯ Out
signalling:	🗹 MSU (default) 🔲 FISU 🔲 LSSU
Start SS7 Capture Stop SS7 Capt	ure Reset

### Figure 7-7-3 Port Recording interface

Port Recording	
Span and Channel:	1 • 1 •
Start Stop	



# 7.8 Cloud

OpenVox E1/T1 gateways support OpenVox Cloud Management.

### Figure 7-8-1 Cloud interface

Cloud		
Enable Cloud Service:	OFF	
Account:	tot	
* Password:		
* Server:	Europe •	
	China America Europe	Don't have an account? Sign up
	IP	

If your device is connected to the cloud management, the SSH and the web pages of the gateway can be accessed through the cloud management, and it can be monitored whether the device is connected to the cloud management platform. On the cloud management platform, you can also count your device model, quantity, distribution area, and so on which can provide you with efficient and excellent service and experience.

Options	Definition	
Enable Cloud	Turn on/off the cloud management	
Service	Tum on/on the cloud management.	
Choose Service	Currently supports three servers, China, the United States and Europe.	
Account	Registered account or email on the cloud management platform.	
Password	The password of the account registered on the cloud management platform.	
Connection	Whether surrently connected to the cloud management platform or not	
Status		

Table 7-8-1	Definition	of Cloud	Management
-------------	------------	----------	------------



# 8 User

DGW Series T1/E1 Gateway allows you to create users and modify the permissions of users accessing the web interface.

# 8.1 User Add

### Figure 8-1-1 User Add interface

User Add	
Username:	test
Password:	
Confirm password:	
Save	

# 8.2 User List

### Figure 8-2-1 User List interface

User List		
Username	Password	Actions
admin	admin	2 🗙
test	111111	2 🗙

# 8.3 Permissions

### Figure 8-3-1 Permissions

Set User Permissions	
Username	test
Submenu	Status The file name
system	
System Status	OFF/system-status.php
Call Status	OFF/system-callstatus.php
Time	OFF/system-time.php
Login Settings	OFF/system-login.php
General	OFF/system-general.php
Tools	OFF/system-tools.php
Information	OFF/system-into.php



# 9 Logs

# 9.1 Log Settings

On the "**Log Settings**" page, you should set the related logs on to scan the responding logs page. For example, set "**SIP Logs**" on like the following, then you can turn to "**SIP**" page for sip logs, otherwise, sip logs are unavailable. And the same with other log pages.

System Logs	
Auto clean:	ON maxsize : 500KB V
Asterisk Logs	
Verbose:	
Notice:	
Warning:	
Debug:	
Error:	
DTMF:	
Auto clean:	ON maxsize : 2MB V
SIP Logs	
SIP Logs:	
Auto clean:	OFF maxsize : 2MB V
IAX2 Logs	
IAX2 Logs:	
Auto clean:	OFF maxsize : 2MB

### Figure 9-1-1 Logs Settings



T1/E1 Port Logs	
T1/E1 Port Logs:	
Auto clean:	OFF maxsize : 2MB
MFC/ R2 Logs	
MFC/ R2 Logs:	
Auto clean:	OFF maxsize : 2MB V
PRI Logs	
PRI Logs:	
Auto clean:	OFF maxsize : 2MB
SS7 Logs	
SS7 Logs:	
Auto clean:	OFF maxsize : 2MB V
Call Statistics	
Call Statistics:	ON

System Notice	
Enable:	
Check Interval:	Every week •

CDR Logs	
Enable:	
Auto clean:	OFF Clean Policy : 30 days(One month)

Save

### Figure 9-1-2 System Logs Output

System Logs		
[2012/01/01	23:29:081	first starting up
[2012/01/01	23:29:27]	Power on
[2015/03/25	20:50:18]	Kernel upgrade
[2015/03/25	20:50:20]	Basefs upgrade
[2015/03/25	20:50:40]	Power off
[2015/03/25	20:51:14]	Power on
[2015/03/25	19:35:47]	Power on
[2015/03/25	19:41:15]	Power off
[2015/03/25	19:41:52]	Power on
[2015/03/25	19:49:08]	Power on
[2015/03/25	19:56:25]	Power on
[2015/03/25	20:01:22]	Power on
[2015/03/25	22:47:50]	Power on
[2015/03/25	23:25:13]	Power on
[2015/03/25	23:40:09]	Power on
[2015/03/26	03:40:48]	Power on
[2015/03/26	04:17:00]	Power on
[2015/03/26	05:37:03]	Power on
[2015/03/26	08:49:08]	Power on
[2015/03/26	09:04:24]	Power on
[2015/03/26	09:30:00]	Power on
[2015/02/26	12.01.201	Vernel ungrade
[2015/03/20	12.01.30]	
[2015/03/26	13.32.491	first starting un
[2015/03/26	13:32:521	Dover off
[2015/03/26	13:33:301	Power on
12020,00,20	201001001	

Refresh Rate: Off 
Refresh Clean Up



### Table 9-1-1 Definition of Logs

Options	Definition
	Switch on: when the size of log file reaches the max size,
Auto clean	The system will cut a half of the file. New logs will be retained.
(System Logs)	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=1MB.
Verbose	Asterisk console verbose message switch.
Notice	Asterisk console notice message switch.
Warning	Asterisk console warning message switch.
Debug	Asterisk console debug message switch.
Error	Asterisk console error message switch.
DTMF	Asterisk console DTMF info switch.
	Switch on: when the size of log file reaches the max size,
Auto clean:	The system will cut a half of the file. New logs will be retained.
(asterisk logs)	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
SIP Logs:	Whether enable or disable SIP log.
	Switch on: when the size of log file reaches the max size,
Auto clean:	The system will cut a half of the file. New logs will be retained.
(SIP logs)	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
IAX2 Logs	Whether enable or disable IAX log.
Auto clean	Switch on: when the size of log file reaches the max size,



г

	The system will cut a half of the file. New logs will be retained.
	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
MFC/ R2 Logs	Whether enable or disable MFC/ R2 Logs log.
	Switch on: when the size of log file reaches the max size,
	The system will cut a half of the file. New logs will be retained.
Auto clean	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
PPI Logs	PRI port logs. You can choose one or more ports. If you choose "All", the
	"PRI" page will show you the logs about all the ports.
	Switch on: when the size of log file reaches the max size,
Auto clean (PRI	The system will cut a half of the file. New logs will be retained.
logs)	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
.SS7 Logs	Whether enable or disable SS7 log.
	switch on : when the size of log file reaches the max size,
Auto clean	The system will cut a half of the file. New logs will be retained.
	Switch off: logs will remain, and the file size will increase gradually.
	default on, default size=2 MB.
Call Statistics	Whether enable or disable Call Statistics.
System Notice	The notification from system firmware upgrade and Auto provisioning.



# 9.2 System log

System log record every time power on, power off and firmware upgrade information.

System Logs		
	A	1
[2015/08/03 16:16:48] Kernel upgrade		L
[2015/08/03 16:16:51] Basefs upgrade [2015/08/03 16:23:36] Pewer off		L
[2015/08/03 16:24:21] Power on		L
[2015/08/03 16:24:45] first starting up		L
[2015/08/03 16:24:48] Power off		L
[2015/08/03 16:25:33] Power an		L
[2015/08/05 15:17:09] Power on [2015/08/06 15:30:03] Power off		L
[2015/08/06 15:30:03] Power on		L
[2015/08/06 15:35:03] Power off		L
[2015/08/06 15:35:47] Power an		L
[2015/08/06 15:55:03] Power off		L
[2015/08/06 15:55:47] Power on [2015/08/11 07:16:45] Power on		L
[2015/08/12 11:50:53] Power on		L
[2015/08/12 13:28:15] Power an		L
	-	L
[2015/08/13 17:54:51] Kernel upgrade		L
[2015/08/13 17:55:00] Power off		L
[2015/08/13 17:55:45] Power an		L
[2015/08/14 08:10:36] Power an		L
[2015/08/14 17:19:49] Power off		L
[2015/08/14 17:20:34] Power on [2015/08/14 16:20:44] Power off		L
[2015/08/14 16:30:28] Power on		
<b></b>	Refresh Rate: Off  Refresh Clean Up Download	1

### Figure 9-2-1 System Log

# 9.3 Asterisk logs

On the pages of "Asterisk", "SIP", "IAX2", "SS7", "PRI" and "MFC/R2", there owns the some

functions—Displays the log by port, refresh regularly and log download.

### Figure 9-3-1 Asterisk Log

Astensk Logs
Mar 10 11:44:55 (none) asterisk[25205]: NOTICE[10073]: pbx_ael.c:177 in pbx_load_module: AEL load process: parsed config file name '/mnt/ext4 ^
/sda7/config/default/sysconfig/asterisk/extensions.ael'.
Mar 10 11:44:55 (none) asterisk[25205]: NOTICE[10073]: pbx_ael.c:180 in pbx_load_module: AEL load process: checked config file name
<pre>'/mnt/ext4/sda7/config/default/sysconfig/asterisk/extensions.ael'.</pre>
Mar 10 11:44:55 (none) asterisk[25205]: NOTICE[10073]: pbx_ael.c:187 in pbx_load_module: AEL load process: compiled config file name
'/mnt/ext4/sda7/config/default/sysconfig/asterisk/extensions.ael'.
Mar 10 11:44:55 (none) asterisk[25205]: NOTICE[10073]: pbx_ael.c:192 in pbx_load_module: AEL load process: merged config file name '/mnt/ext4
/sda7/config/default/sysconfig/asterisk/extensions.ael'.
Mar 10 11:44:55 (none) asterisk[25205]: NOTICE[10073]: pbx_ael.c:195 in pbx_load_module: AEL load process: verified config file name
<pre>'/mnt/ext4/sda7/config/default/sysconfig/asterisk/extensions.ael'.</pre>
r 10 11:45:08 (none) asterisk[25205]: NOTICE[25257]: chan_sip.c:28082 in handle_request_subscribe: Received SIP subscribe for peer without
mailbox: 2001
Mar 10 11:45:09 (none) asterisk[25205]: NOTICE[25257][C-000008ce]: chan_sip.c:10558 in process_sdp: No compatible codecs, not accepting this
offer!
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10153 in process_sdp: set peer prefer
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10158 in process_sdp: p->owner->readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10159 in process_sdp: p->owner->readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[10273][C-000008cf]: chan_sip.c:7160 in sip_answer: ast readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[10273][C-000008cf]: chan_sip.c:7161 in sip_answer: ast writeformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[10273][C-000008cf]: chan_sip.c:7162 in sip_answer: ast jointcaps is (ulaw)
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[10273][C-000008cf]: chan_sip.c:7164 in sip_answer: ast reset jointcaps is (ulaw)
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10153 in process_sdp: set peer prefer
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10158 in process_sdp: p->owner->readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10159 in process_sdp: p->owner->readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10153 in process_sdp: set peer prefer
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10158 in process_sdp: p->owner->readformat is ulaw
Mar 10 11:45:16 (none) asterisk[25205]: NOTICE[25257][C-000008cf]: chan_sip.c:10159 in process_sdp: p->owner->readformat is ulaw
Pofroch Pate: 1c V Refrech Clean III Download
ivenesii vale. 15 iiii velesii clear op Download



# 9.4 Call Statistics

The figure of call statistics, you'll find "Answered", "congestion", "Call busy", "Call failed", "No answer", "Current calls", "accumulated calls", "Calls duration" and "ASR". "ASR" stands for Answer Seizure Ratio. "Calls duration" will count the whole calls in the gateway. The call statistics will be saved before power off. It will be loaded after power on. It can be refreshed by itself. You can reset the statistics manually.

Figure	9-4-1	Call	Statistics

Statistics									
Answered	Congestion	Call Busy	Call Failed	No Answer	Unknown	Current calls	Accumulated Calls	Calls duration	ASR
57571	0	0	0	0	0	0	57571	3456781	100%
Refresh Reset Statistics									

Note: Do not forget to enable call statistics in "Log Setting" if you want to statistics the calls.

# 9.5 System Notice

The system notice could be generated by system to inform the network manager of what is going on if it has been enabled. Firmware upgrade messages from official website and auto provisioning messages from ACS are main notice right now. And at first, enable the system notice function in "**Log Setting**" page like figure 9-5-1.



System Notice	
Enable:	ON
Check Interval:	Every hour
Save	

After about an hour, a system message is received in the web like 9-5-2.



### Figure 9-5-2 enable system notice function

Notice Logs			
Date	Subject	Content	
2016/03/10 12:06:13	System Upgrade Notification	A new firmware could be downloaded from system online. Current release is : 1.0.9, OpenVox latest release is :1.1.0. If you want to upgra de, please transfer to SYSTEM->tools pages.	
2016/03/10 12:06:10	Auto-provision Upgrade Notification	A new firmware and configs could be upgraded from ACS. Current release is : 1.0.9, ACS server release is :1.1.2. If you want to upgrade, please restart the system and wait several minutes.	
		Refresh Clean Up	

Note: Do not forget to enable system notice and check interval in "Log Setting" if you want to

receive system messages.