



OpenVox Communication Co., Ltd



ET-200X(L) Series Digital Gateway User Manual





OpenVox Communication Co.,Ltd

Address: 10/F, Building 6-A, Baoneng Science and Technology Industrial Park, Longhua New District, Shenzhen, Guangdong, China 518109

> Tel: <u>+86-755-66630978, 82535461, 82535362</u> Business Contact: <u>sales@openvox.cn</u> Technical Support: <u>support@openvox.cn</u> Business Hours: 09:00-18:00(GMT+8) from Monday to Friday URL: www.openvox.cn

Thank You for Choosing OpenVox Products!



Revision History

Document VER	Firmware VER	Explanation	Time
V1.0			



Legal Information

Copyright[®] OpenVox Communication Co. ,LTD. 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 Communication Co. ,LTD.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 Communication Co. ,LTD.

Disclaimer

OpenVox Communication Co. ,LTD. 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 Communication Co. ,LTD. 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 Communication Co. ,LTD. 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.



Table of Contents

Revision History	3
Legal Information	4
Confidentiality	4
Disclaimer	4
Trademarks	4
1 Overview	8
1.1 What is ET-200X(L)	8
1.2 Sample Application	8
1.3 Product Appearance	9
1.4 Main Features	
1.5 Physical Information	11
1.6 Software	11
2 System	12
2.1 Status	
2.2 Call Status	13
2.3 Time	
2.4 Login Settings	14
2.5 General	16
2.5.1 Language Settings	16
2.5.2 Scheduled Reboot	
2.6 Tools	16
2.6.1 Reboot Tools	17
2.6.2 Update Firmware	17
2.6.3 Upload and Backup Configuration	
2.6.4 Restore Configuration	
2.7 System Information	
3 T1/E1	18

OpenVox

3.1 General	
3.2 PRI	
3.3 SS7	
3.3.1 Link Set Settings	
3.3.2 Link Settings	
3.3.3 SS7 Configuration file backup and restore	25
3.4 MFC/R2	25
3.4.1 MFC/R2 Signaling	
3.4.2 Modify R2 variant	
4 VOIP	21
4.1 VOIP ENDPOINTS	
4.1.1 SIP Endpoints	
4.1.2 Main Endpoint Settings	
4.1.3 Advanced Registration Options	
4.1.4 Call Settings	
4.1.5 Advanced Timer Settings	
4.1.6 Advanced Signaling Settings	
4.2 IAX2 ENDPOINT	
4.3 ADVANCED SIP SETTINGS	
4.3.1 Networking	
4.3.2 Advanced NAT Settings	40
4.3.3 Advanced RTP Settings	
4.3.4 Parsing and Compatibility	
4.3.5 Security	43
4.3.6 Media	
4.3.7 Codec Settings	
4.4 Advanced IAX2 Settings	
4.5 Advanced fax setting	
5 Routing	40
/	

OpenVox

ET 200X(L) Series Digital Gateway User Manual

5.1 Call Routing Rule	
5.2 Groups	
6 Network	
6.1 WAN/LAN Settings	
6.2 DDNS Settings	
6.3 Toolkit	55
7 Advanced	55
7.1 Asterisk API	55
7.2 Asterisk CLI	57
7.3 Asterisk File Editor	
7.4 Auto Provisioning	
7.4.1 Preparation	
7.4.2 Configuring gateway	
7.4.3 Configuring ACS	61
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	
8 Logs	
8.1 Log Settings	
8.2 System log	
8.3 Asterisk logs	
8.4 Call Statistics	
8.5 System Notice	



1 Overview

1.1 What is ET-200X(L)

ET-200X(L) Digital 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). 'X' means the number of T1/E1 port. 'L' stands for none hardware codec —— V100 module.

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. ET-200X(L) Digital Gateway has good processing ability and stability and we provides 1/2/4/8 T1/E1 interface for your choice. The T1/E1 gateway will be 100% compatible with Asterisk, Elastix, trixbox, 3CX, FreeSWITCH SIP server and VOS VoIP operating platform.

1.2 Sample Application

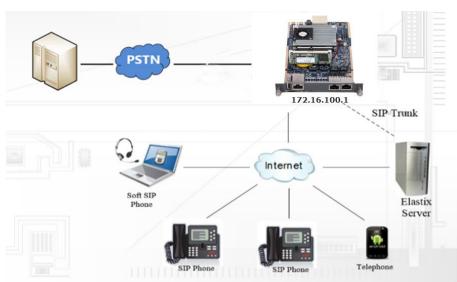


Figure 1-2-1 Topological Graph



1.3 Product Appearance

The picture below is appearance of ET-2002.

Figure 1-3-1 Product Appearance



Figure 1-3-2 Front Panel



Table 1-3-1 Description of Front Panel

Interface	Function	Color	Work Status				
1 USB	USB interface						
2 Eth	Ethernet interface						
3 port 1-2	E1 / T1 ports						
4 HDMI	High definition multimedia interface						
5 ON/OFF	On/off button can be used to	turn on/off the	system.				



6 PWR	Power status indicator	groop	On: power is on				
6 PWK	Power status indicator	green	Off:power is off				
			Slow blinking(Green 2s and				
			Flash 0.1s):Work normally				
			Fast blinking(Green 0.5s				
			and Flash 0.5s): Work				
7 RUN	Register indicator	green	abnormally				
			Fast blinking(Green 0.5s				
			and Flash 0.5s): Work				
			abnormally				
			No blinking: Dahdi Error				
8 RST	Reset button is used to resto	ore the device	S.				

1.4 Main Features

- Based on Asterisk[®]
- > Editable Asterisk[®] configuration file
- > Codecs support: G.711A, G.711U, G.729, G.723, G.722, GSM
- Support PRI/SS7/R2 signling
- > Support 512 routing rules and flexible routing settings
- > Stable performance, flexible dialing, friendly GUI
- > Support ports group management
- > Support call status information
- Support T.38/Pass-through fax
- Support Auto Provision, SNMP V1/V2c/V3 and TR069
- Echo Cancellation
- 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

Model	ET2001	ET2002	ET2004	ET2001L	ET2002L					
E1/T1 port	1	2	1	2						
Codec & EC module	yes no									
dimension			100*162.5mm							
weight	210g	216g	226g	202g 207g						
temperature (°C)	storage: -40~85									
	operation: 0~70									
Operation humidity	umidity 10% ~ 90% non-condensing									
Max power 12W										

Table 1-5-1 Description of Physical Information

1.6 Software

Default IP: 172.16.100.1(Eth)

Username: admin

Password: admin

Notice: Log in

Figure 1-6-1 LOG IN Interface

用户名		
密码		
🛛 记住我的凭握	_	



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.

Port1						Port2								Port3						Port4											
•															•																
0	к 🔴	Down	⊖ R	leload	ļ.																										
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	
1	1	2	3	4	5	6	4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
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	
-	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	
3	0	0	0	0	Ö	0	Ö	O	0	0	Ö	0	Ö	0	$\overline{\mathbf{\Theta}}$	Ö	Ö	0	0	02	Ö	0	0	0	0	Ö	Ö	0	0	0	
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	
Inform	ation					he A	Disa) S cha	annei																					_
Inform oint Na					User I		Disa	Jie	5 012		Host					Reg	gistrati	on			Status										
	ime	1					Disa		5 Cha		Host					Reg	gistrati	on			Status										
oint Na	ime mation	1				Name	Disa		Suna	1	Host						gistrati gistrati				Status Status										
oint Na 2 Infori	ime mation ime				User I	Name	Disa		Scha	1																					
oint Na 2 Inforr oint Na	ime mation ime				User I	Name	Disa			1							gistrati														
oint Na 2 Inform oint Na ting Inf	ime mation ime format	tion			User I User I	Name				1	Host					Reg	gistrati														
oint Na 2 Inform oint Na ting Inf	ime ime format	tion			User I User I	Name			Idress	1	Host			Mask		Reg	gistrati	on	eway			R	NY Pac	kets			TX Pe	ackets			
oint Na 2 Inform oint Na ting Inf Name work In	ame mation ame format	tion	ress		User I User I	Name		IP Ad			Host				÷	Reg	gistrati	on	2.16.0.				XX Pac				TX Pe 4738				

Figure 2-1-1 System Status

Options	Definition
Interface Status	Show the status of port, include "OK" and "Down". "Down" means no trunk line
Interface Status	connected; "OK" means the trunk line of port is available.



	Show the Channels status of port, include "Idle". "Busy". "Disable" and "S
Channels	channel". "Idle" means it is available;
Status	"Busy " means the channel is busy;
Status	"Disable" means it is unavailable;
	"S channel" means signaling channel.

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.

l Status						Select Port
Channel	Status	Direction	CallerID	CalleeID	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

2.3 Time

Table 2-3-1 Description of Time Settings	Table 2-3-1	Description	of Time	Settinas
--	-------------	-------------	---------	----------

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].



ET 200X(L) Series Digital Gateway User Manual

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].
	Whether enable automatically synchronize from NTP server or not. ON
Auto-Sync from NTP	is enable, OFF is disable this function.
Sync from NTP	Sync time from NTP server.
Sync from Client	Sync time from local machine.

For example, you can configure like this:

Figure 2-3-1	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
User Name	your gateway.
	And it has all privileges to operate your gateway .User Name: Allowed
	characters "+<>&0-9a-zA-Z".Length:1-32 characters.
Deserverd	Allowed characters "+. <>&0-9a-zA-Z".
Password	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
Login Mode	and 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

User Name:	admin
Password:	•••••
Confirm Password:	•••••
Login Mode:	http and https
Port:	80
SSH Login Settings	
SSH Login Settings Enable:	
	admin
Enable:	
Enable: User Name:	admin

Save

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 Settings		
Language:	English •	
Advanced:		
Language Debug:	TURN ON TURN OFF	
Download:	Download selected language package.	wnload
Delete:	Delete selected language.	Delete
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

Enable:		
Reboot Type:	By Day	
Time:	Hour: 23 V Minute: 59 V	

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.

Reboot the gateway and all the current calls will be dropped.	Are you sure to reboot your gateway now? You will lose all data in memory!	Sy	stem Reboo
Reboot the asterisk and all the current calls will be dropped.		Ast	erisk Reboo
Update Firmware	确定 取消		

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

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

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

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

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 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

Restore Configuration	
This will cause all the configuration files to back to default factory values! And reboot your gateway once it finishes.	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.

Model Name:	ET-2104
Firmware Version:	2.2.0
Firmware Build:	1709
Hardware Version:	1.2
Port Amount:	4
Storage Usage:	8.6M/2.9G (0%)
Memory Usage:	10.7458 % Memory Clean
Kernel Build Time:	2017-Sep-25-15:29:41
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:	2017-11-24 15:30:57
System Uptime:	0 days 00:29:23

Figure 2-7-1 System Information

3 T1/E1

3.1 General



Figure 3-1-1 General Settings

General	
Locale:	United States
Interface Type:	© T1 ⊛ E1

Table 3-1-1 Definition of General Settings

	Your locale. This will be used for the tone style. Used when in-call
Locale	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:	ON
RX Gain:	0
TX Gain:	0

Table 3-1-2 Definition of advanced interface type

Options	Definition
Echo Cancellation	Whether or not to enable echo cancellation
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 3-1-2 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) \checkmark	Off 💌	PRI(Network side)	EuroIsdn 💌	
Port 2	0 -	E1	CCS 🔻	HDB3 -	0-133 feet (DSX-1) and 0 db (CSU) \checkmark	Off 💌	PRI(Network side)	EuroIsdn 💌	
Port 3	0 -	E1	CCS 🔻	HDB3 -	0-133 feet (DSX-1) and 0 db (CSU) \checkmark	Off •	PRI(Network side)	EuroIsdn 💌	
Port 4	0 -	E1	CCS 🔻	HDB3 💌	0-133 feet (DSX-1) and 0 db (CSU) 💌	Off 🔻	PRI(Network side)	EuroIsdn 💌	

Table 3-1-3 Definition of Port Details

Options	Definition
Timing Source	Timing Source indicate the ports as to which should be used to recover the
	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.
CRC4	Enable cyclic redundancy checking for error checking on line. CRC-4 support is
	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

Figure 3-2-2 ISDN: Signaling

VISDN: Signaling	
Q.SIG Channel Mapping:	Logical
Enable Caller ID:	
PRI Options	
PRI Dial Plan for Dialed Number:	Unknown 🔻
PRI Dial Plan for Dialing Number:	Unknown •
International Prefix:	
National Prefix:	
Local Prefix: Local Prefix:	
Private Prefix:	
Unknown Prefix:	
Network Specific Facility (NSF) 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:	
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:	

Save Apply Cancel

Options	Definition
Q.SIG Channel Mapping	Sets logical or physical channel mapping. In logical channel mapping,
	channels are mapped to 1-30. In physical channel mapping, channels are
	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
PRI Dial Plan for Dialed Number	PRI Dialplan: The ISDN-level Type of Number (TON) or numbering plan,
	used for the dialed number. Leaving this as 'unknown' (the default) works
	for most cases. In some very unusual circumstances, you may need to
	set this to; 'dynamic' or 'redundant'
PRI Dial Plan for Dialing Number	PRI Local Dialplan: Only RARELY used for PRI(sets the calling number's
	numbering plan).In North America, the typical use is sending the 10 digit;
	caller ID number and setting the prilocaldialplan to 'national' (the
	default).Only VERY rarely will you need to change this.
Network Specific Facility (NSF)	Some switches (AT&T especially) require network specific facility IE.
Messages	Supported values are currently 'none', 'sdn', 'megacom', '
	tollfreemgacom', ' account'
Idle Bearer Reset	Whether or not to reset unused B channels
Idle Bearer Reset Period	Sets the time in seconds between restart of unused B channels; defaults
	to 'never'
Display Send	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.

Table 3-2-2 Definition of Signaling



	name_initial: Use display text in SETUP/CONNECT messages as the
	party name.
	name_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'.
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	Allow inband audio (progress) when a call is DISCONNECT Ted by the
Released	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
Supplementary Services	(such as caller name form CPE over facility), enable this option. Cannot
	be changed on a reload.
Exclusive Channel Selection	If you need to override the existing channels selection routine and force
	all PRI channels to be marked as exclusively selected, set this to yes.
	priexclusive cannot be changed on a reload.



Ignore Remote Hold Indications	If you wish to ignore remote hold indications (and use MOH that is
	supplied over the B channel) enable this option.
Block Outbound Caller ID Name	Enable if you need to hide just the name and the number for legacy PBX
	use. Only applies to PRI channels.
Wait for Caller ID Name	Support caller ID on call waiting

3.3 SS7

3.3.1 Link Set Settings

Figure 3-3-1 Link Set Settings

Linkset Index	Linkset Name	Туре	Signalling	Called NAI	Calling NAI	Network Indicator	Point Code	Adj. Point Code	Default DPC	Sig Chan	Action
Linkset-1	linkset1	itu	ss7	national	national	national	0x32	0x1	0x1	16	2

Edit Link Set "linkset-1"

button as shown below, when there are several linkset, only one can be set to the You can click default.

Figure 3-3-2 SS7 Link Set Settings

7 Link Set Settings		
Name:	linkset1	
Туре:	ITU 💌	
Called NAI:	national	
Calling NAI:	national	
Network Indicator:	national	
International Prefix:		
National Prefix:		
Subscriber Prefix:		
Unknow Prefix:		
Point Code:	0x32 (Hint : Code in hexa	adecimal format)
Adj. Point Code:	0x1 (Hint : Code in hexa	adecimal format)
Default DPC:	0x1 (Hint : Code in hexa	adecimal format)
Sig Chan:	16	

Save Cancel



options	Definition
Name	The linkset name
Туре	SS7 variant
Called NAI	SS7 Called Nature of Address Indicator
Calling NAI	SS7 Calling Nature of Address Indicator
Network Indicator	What the MTP3 network indicator bits should be set to
International Prefix	International Prefix
National Prefix	National Prefix
Subscriber Prefix	Subscriber Prefix
Unknown Prefix	Unknown Prefix
Point Code	Origin point code
Adj. Point Code	Point code of node adjacent to this signalling link, Possibly the STP between you and
	your destination
Default DPC	Default DPC
Sig Chan	Signaling Channel

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

3.3.2 Link Settings

Link Settings

Figure 3-3-3 Link Settings

Link Index	Interface	Port	Signaling	Linkset Index	Channel	Action
link-1	E1	port-1	SS7	Linkset-1	1-15,17-31	2
link-2	E1	port-2	SS7	Linkset-1	32-62	2
link-3	E1	port-3	SS7	Linkset-1	63-93	2
link-4	E1	port-4	SS7	Linkset-1	94-124	2

You can click button as shown below.



Figure 3-3-4 SS7 Edit Link Settings

Edit Link "link-1"	Edit	Link	"link-1	"
--------------------	------	------	---------	---

🛡 SS7 Lin	k Settings	
	Link Index:	link-1
	Interface Type:	E1
	Linkset Index:	Linkset-1 💌
	Channel:	1-15,17-31
	Port:	port-1

Save Cancel

Table 3-3-2 Definition of SS7 Edit Link Settings

options	Definition	
Link Index	The link index	
Interface Type	T1/E1 mode	
Linkset Index	The link member set index	
Channel	The voice channel on the link	
Port	The T1/E1 port in used	

3.3.3 SS7 Configuration file backup and restore

Figure 3-3-5 Configuration file backup and restore

Download \$\$7 Configuration File	Download Backup
V SS7 Config. File Restore	
▼ 337 Configuration file: 选择文件 未选择任何文件	

3.4 MFC/R2

3.4.1 MFC/R2 Signaling

WFC/R2: Signaling	
Enable Caller ID:	ON
Init CAS Bit:	1101
Variant:	ITU •

Figure 3-4-1 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

Table 3-4-1 Definition of MFC/R2 Signaling

3.4.2 Modify 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	х	с	3	2 🗙
Bolivia	01	yes	1	5	5	F	F	3	2 🗙
Brazil	01	no	1	5	5	х	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	х	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	х	F	3	2 🗙
Indonesia	01	yes	1	6	6	F	F	3	2 🗙
Israel	01	yes	1	9	9	х	F	3	2 🗙
ITU	01	yes	1	5	5	F	F	3	0
Korea	01	yes	1	5	5	х	F	3	2 🗙
Malaysia	01	yes	1	6	6	F	F	3	2 🗙
Malta	01	yes	1	0	5	х	F	3	2 🗙

Figure 3-4-2 R2 Variant

You can click button, then you could fine the below.



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

Table 3-4-2 Definition of General

Options	Definition	
Variant Name	The variant name	
R2 Category national subscriber works just fine usually		
Allow Collect	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		
	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	This feature allows to skip the use of Group B/II signals and go directly to the accepted	
Accept	state for incoming calls	



ſ

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 3-4-4 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 3-4-3 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
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
R2 Answer Delay	Minimum delay time between the Accept tone signal and the R2
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.

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 3-4-5 Group A

Figure 3-4-6 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 V
Number Changed:	INVALID V



Figure 3-5-7 Group C

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

Figure 3-4-8 Group 1

roup 1	
No More Dnis Available:	INVALID V
No More ANI Available:	C •
Caller ANI Is Restricted:	F •

Figure 3-4-9 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



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 🗙
7001	none	7001@172.16.8.38	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 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

Edit 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 •
NAT Traversal:	Yes v
Advanced:Registration Options	
Call Settings	
Fax Options	
Save Apply Cancel	

For convenience, we have designed a method that you can register your SIP endpoint to your

gateway, thus your gateway just work as a server.



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 v
Advanced:Registration Options	
Call Settings	
Fax Options	
Save 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	

Save 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 registers with this gateway.
	IP address or hostname of the endpoint or 'dynamic' if the endpoint
Hostname or IP Address	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.
	This sets the possible transport types for outgoing. Order of usage,
	when the respective transport protocols are enabled, is UDP, TCP,
Transport	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 SIP proxy	
	(provider), calls from this provider connect to this local extension.	
From 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	
Remote Secret	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	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

Table 4-1-3 Definition	of	Call	Options
------------------------	----	------	---------

Options	Definition	
DTME Made	Set default DTMF Mode for sending DTMF. Default: rfc2833.	
DTMF Mode	Other options: 'info', SIP INFO message (application/ dtmf-relay);	
Trust Remote-Party-ID	Whether or not the Remote-Party-ID header should be trusted.	
Send Remote-Party-ID	Whether or not to send the Remote-Party-ID header.	
Caller ID Presentation	Whether or not to display Caller ID.	

4.1.5 Advanced Timer Settings



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	Minimum session refresh interval in seconds. Default is 90secs.
Maximum	Maximum session refresh interval in seconds. Defaults to 1800s.
Session Refresh	
Session Refresher	The session refresher, uac or uas. Defaults to uas.

Table 4-1-4 Definition of Timer Options

4.1.6 Advanced Signaling Settings

Table 4-1-5 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	Whether or not to add;' user=phone' to URIs that contain a valid phone number.
user=phone to URI	
Add Q.850 Reason	Whether or not to add Reason header and to use it if it is available.
Headers	



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.
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	Whether or not to allow 302 or REDIR to non-local SIP address .Note that promiscredir
Redirects	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	Send 100 Trying when the endpoint registers.
REGISTER	

Table 4-1-6 Definition of Fax Options

Options	Definition
Mode	Working mode T.38 and T.30
Enabled	Enabled
Error Correction	Error Correction
Max Datagram	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 send T.38 packets of a reasonable
	size to that endpoint (Cisco media gateway 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 Detect	FAX detection will cause the SIP channel to jump to the 'faX' extension (if exists) 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

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

You can click elements button as shown below

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

Edit IAX Endpoint "9001"

Wain Endpoint Settings	
Name:	9001
User Name:	9001
Password:	
Registration:	None
Hostname or IP Address:	172.16.8.183
Auth:	md5 T
Transfer:	No T
Trunk:	No

V Advanced:Registration Options	
Qualify:	Yes 🔻
Qualify Smothing:	Yes •
Qualify Freq Ok:	60
Qualify Freq Not Ok:	60
Port:	4569
Require Call Token:	Yes •



VIAX Encryption	
Encryptic	n: No 🔻
Force Encryptio	n: No 🔻
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

	·
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.
	Allowed characters
Registration	Whether this endpoint will register to this gateway or this gateway to the endpoint.
Hostname or IP	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a dynamic IP
Address	address. This will require registration.
	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.
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 Ok	How frequently to ping the peer when it's either;
	LAGGED or UNAVAILABLE, in milliseconds.

Table 4-2-1 Definition of IAX2 Endpoint



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.
Trunk Time Stamps	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 that frame
	timestamps get sent end-to-end properly. If both ends of all your 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.
	The maximum number of seconds a client has to authenticate. If the
TCP Authentication Timeout	client does not authenticate before this timeout expires, the client will be
	disconnected.(default value is: 30 seconds).
TOD Authentication Limit	The maximum number of unauthenticated sessions that will be
TCP Authentication Limit	allowed to connect at any given time (default is: 50).
	Enable DNS SRV lookups on outbound calls Note: the gateway only
	uses the first host in SRV records Disabling DNS SRV lookups disables
Enable Hostname Lookup	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.
Enable Internal SIP Call	Whether enable the internal SIP calls or not when you select the
	registration option "Endpoint registers with this gateway".
Internal SIP Call Prefix	Specify a prefix before routing the internal calls.

Table 4-3-1 Definition of Networking Options

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.

Table 4-3-2 Definition of NAT Settings Options



ET 200X(L) Series Digital Gateway User Manual

	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
Subscribe	the stun_ monitor is installed and configured, chan_sip will renew all outbound
Network Change	registrations when the monitor detects any sort of network change has
Event	occurred. By default this option is enabled, but only takes effect once
Event	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 feature.
Match External	Only substitute the exeternaddr or externhost setting if it matches
Dynamic Exclude	Disallow all dynamic hosts from registering as any IP address used for staticly
Static	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
TCP Port	PAI
	The external address (and optional TCP port) of the NAT. External
External Address	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
	The external hostname (and optional TCP port) of the NAT.
External Hostname	External Hostname=hostname[:port] is similar to
	"External address". Examples:
	External Hostname=foo.dyndns.net
	How often to perform a hostname lookup. This can be useful when your NAT
Hostname Refresh	device lets you choose the port mapping, but the IP address is dynamic.
Interval	Beware you might suffer from service disruption when the name server
	resolution fails.



4.3.3 Advanced RTP Settings

Table 4-3-3 Definition of RTP Settings Options

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.

4.3.4 Parsing and Compatibility

Options	Definition
Strict RFC	Check header tags, character conversion in URIs, and multiline
Interpretation	headers for strict SIP compatibility(default is yes)
Send Compact Headers	Send compact SIP headers
SDP Owner	Allows you to change the username filed in the SDP owner string. This filed MUST NOT contain spaces.
Disallowed SIP Methods	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. 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.

Table 4-3-4 Instruction of Parsing and Compatibility



Shrink Caller ID	The shrinkcallerid function removes '(', '', ')', non-trailing '.', and '-' not in square 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	Maximum allowed time of incoming registrations and subscriptions
Registration Expiry	(seconds).
Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).
Default Registration Expiry	Default length of incoming/outgoing registration.
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.
Number of Registration	Number of registration 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
Definitio	on

Option	Definition
Match Auth	If available, match user entry using the 'username' field from the
Username	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 the domain from the SIP Domains setting as the realm. In this case,
Use Domain as	the realm will be based on the request 'to' or 'from' header and should
Realm	match one of the domain. Otherwise, the configured 'realm' value will be
	used.
	When an incoming INVITE or REGISTER is to be rejected, for any
	reason, always reject with an identical response equivalent to valid
Always Auth Daiast	username and invalid password/hash instead of letting the requester
Always Auth Reject	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	Enabling this option will authenticate OPTIONS requests just like
Options Requests	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.



Figure 4-3-1 Codec Settings

acc 3	ettings	
	Codec Priority 1:	G.711 u-law 🔻
	Codec Priority 2:	G.711 a-law ▼
	Codec Priority 3:	GSM •
	Codec Priority 4:	G.722 •
	Codec Priority 5:	G.723 •
	Codec Priority 6:	G.729 •

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	Set iaxcompat to yes if you plan to use layered switches or some other scenario which
Nochecksums	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 Loopup	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.
autokill	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)

Table 4-4-1 Instruction of General



Account Code	You may specify a default account for Call Detail Records (CDRs) in addition
	specifying on a per-user basis.

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 4-4-2 Instruction of Music on Hold

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 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.

Table 4-4-4 Instruction of Jitter Buffer

Options	Definition
Jitter Buffer	Global default as to whether you want the jitter buffer at all
Force Jitter Buffer	In the ideal world, when we bridge VoIP channels we don't want to jitter buffering on
	the switch, since the endpoints can each handle this. However, some endpoints may
	have poor jitter buffers themselves, so this option will force to always jitter buffer, even
	in this case.
Max Jitter Buffers	A maximum size for the jitter buffer
Resyncthreshold	When the jitter buffer notice 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 interpolation 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 this many interpolations. This 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 Count	Establishes the number of extra dynamic threads that may by spawned to					
	handle I/O					
Max Call Number	The 'maxcallnumbers' option limits the amount of call numbers allowed for					
	each individual remote IP address. Once an IP address reaches its call					
	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.					
MaxCallNumbers_Nonvalidated	The 'maxcallnumbers-nonvalidated' is used to set the combined number of					
	call numbers that can be allocated for connections where call token					
	validation has been disabled. Unlike the 'maxcallnumbers' option, this limit					
	is not separate for 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

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 Transmission	Maximum Transmission Rate					
Rate						
Minimum Transmission	Minimum Transmission Rate					
Rate						
Send Progress/Status	Manager events with 'call' class permissions will receive events indicating the					
events to manager	steps to initiate a fax session. Fax completion events are always sent to manager					
session	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					

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



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 support 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 +[]](:+)] Caller_Dial_pattern +[]](:+)]	2 🗶			
¢	3	6001toport	sip-7001	grp-ports	Callee_Dial_pattern +[]](:+)] Caller_Dial_pattern +[]](:+)]	2 🗙			
New Call Routing Rule Save Orders									
Vou	ara a	llowed to se	t un new rout	ing rule by	Call Routing Rule and after	r setting routing ru			
You a	are a	llowed to se	t up new rout	ing rule by New	[,] Call Routing Rule , and afte	r setting routing ru			
			t up new rout		Call Routing Rule, and afte	r setting routing ru			

Figure 5-1-1 Routing Rules

Finally click the Save Orders button to save what you set. Rules will show current routing rules.

There is an example for routing rules number conversion, it transform calling, called number 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 the last four numbers, and then add number 0755 at the end, it will show caller name is China Telecom. Called transform adds 086 as prefix , and Change the last two number to 88.

Figure 5	5-1-2
----------	-------

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



You can click

New Call Routing Rule button to set up your routings.

Figure 5-1-3 Example of Setup Routing Rule

Create	a	Call	Routing	Rule
orouto	ч	oun	requiring	T Caro

V Call Routing Rule							
Routing Name:	support						
Call Comes in From:	1001 •						
Send Call Through:	Port-1						
Advance Routing Rule							
CalleeID/callerID Manipulation	-						
Callee_Dial_pattern: Prepend	+ Prefix	I Match Pattern	11(-SDfR	+ StA) RdfR		
Caller_Dial_pattern: Prepend	+ Prefix	I Match Pattern]](- SDfR	+ StA) RdfR	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.

Options Definition						
Pouting Name	he name of this route. Should be used to describe what types of calls					
Routing Name	this route matches (for example, 'SIP2Ports' or 'Ports2SIP').					
Call Comes in From	The launching point of incoming calls.					
Send call Through	The destination to receive the incoming calls.					

Table 5-1-1 Definition of Routing Options



Options Definition							
Options							
	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] matche any digit in the brackets (example: 1,2,3,7,8,9)						
	wildcard* : matches one or more dialed digits.						
	prepend: Digits to prepend to a successful match. If the dialed number						
	matches the patterns specified by the subsequent columns, then this will						
Dial Patterns that will	be prepended before sending to the trunks.						
use this Route	prefix: 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 amount 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.						
	RDfR(Reserved Digits from Right) :Designated information to be added						
	to the right end of the current number.						
	StA(Suffix to Add):Designated information to be added to the right end						



	of the current number.						
	Caller Name: What caller name would you like to set before sending						
	his call to the endpoint. Native language charset is allowable, e.g.						
	Chinese charset, Latin charset.						
Forward Number	What destination number will you dial?						
	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						
Number	you specify.						

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

Figure 5-1-4 Time Patterns that will use this Route

Time Patterns that will use this Route										
Time to start: 00 ▼ : 00 ▼	Week Day start: M	1onday	•	Month Day start:	01	۲	Month start:	January	•	
Time to finish: 02 ▼ : 00 ▼	Week Day finish: Th	hursday	•	Month Day finish:	31	۲	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 5-1-5 Forward number

Forward Number	
Forward Number	

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

Figure 5-1-6 Failover Call Through Number

Failover Call Through Number	
Failover Call Through Number 1:	port 1 🔻
Failover Call Through Number 2:	port 2 🔻

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.

Routing Groups	
Group Name:	ALLPORT
Туре:	T1/E1 •
Policy:	Roundrobin
Members	NO. All 1 Port-1 2 Port-2

3

4

Port-3

Port-4

Figure 5-2-1 Establish Group

6 Network

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

6.1 WAN/LAN 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.

WAN Setting Interface: eth0 Type: Static • MAC: A0:98:05:01:DB:A4 172.16.100.205 Address: 255.255.0.0 Netmask: 172.16.0.1 Default Gateway: LAN Setting Interface: eth1 ON Enable: MAC: A0:98:05:01:DB:A5 Address: 192,168,100,1 255.255.255.0 Netmask: Default Gateway: 192.168.0.1

Figure 6-1-1 WAN/LAN Settings Interface



Options	Definition
Interface	The name of network interface.
	The method to get IP.
Туре	Static: manually set up your gateway IP.
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.

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

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 enable or disable DDNS (dynamic domain name server).

Figure 6-2-1 DDNS Interface

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



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.

Table 6-2-1 Definition of DDNS Settings

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 Cation
www.google.com	Ping
www.google.com	Traceroute
PINC www.google.com/6/	ping -C 4 www.google.com
	4.233.162.83) 56(84) bytes of data.
	00.net (64.233.162.83); icmp_seq=1 ttl=41 time=309 ms 00.net (64.233.162.83); icmp_seq=2 ttl=41 time=306 ms
64 bytes from li-in-f83.1e1	00.net (64.233.162.83): icmp_seq=3 ttl=41 time=357 ms
54 bytes from II-In-183.1e1	00.net (64.233.162.83): icmp_seq=4 ttl=41 time=303 ms
www.google.com ping s	
	ceived, 0% packet loss, time 3306ms 3.249/318.970/357.318/22.249 ms
	Result
Successfully ping [www.go	oogle.com].

7 Advanced

7.1 Asterisk API

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



Figure 7-1-1 API Interface

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: 🗹

Table 7-1-1 Definition of Asterisk API

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



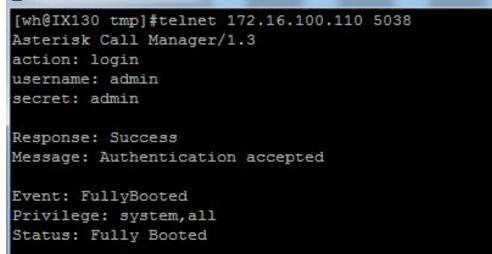
Config	Ability to read and write configuration files.
DTMF	Receive DTMF events. Read-only.
Reporting	Ability to get information about the system.
Dialplan	Receive NewExten and Var Set events. Read-only.
Originate	Permission to originate new calls. Write-only.
All	Select all or deselect all.

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

Putty 172.16.100.110 - Putty



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
Lock / Unlock channels	
Signalling:	pri
Operation:	Lock
Channel:	
	Execute



Table 7-2-1 Definition of Asterisk CLI

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

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

Table 7-2-2 Definition of Lock/unlock chann	els
---	-----

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

7.3 Asterisk File Editor

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

Figure 7-3-1 Configuration Files List

Prime Config. Files		
File Name	File Size	
system.conf	831	
sip.conf	105	
sip endpoints.conf	2125	
logger.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		
Configuration Files List File Name	File Size	
	File Size 2817	
File Name		
File Name acl.conf	2817	
File Name acl.conf adsi.conf	2817 140	
File Name acl.conf adsi.conf agents.conf	2817 140 2531	
File Name acl.conf adsi.conf acents.conf alarmreceiver.conf	2817 140 2531 2084	
File Name acl.conf adsi.conf accents.conf alammeceiver.conf alsa.conf	2817 140 2531 2084 3498	
File Name acticonf adsi.conf actionf actionf actionf alarmreceiver.conf alsa.conf alsa.conf and.conf	2817 140 2531 2084 3498 767	
File Name acl.conf adsi.conf acents.conf alarmreceiver.conf alsa.conf alsa.conf and.conf and.conf app.mysql.conf	2817 140 2531 2084 3498 767 1044	

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 anto 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 work 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'.



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.
Upgrade Mode	Power: start upgrade configuration when Power on. Power + Period: Set the
	frequency of checking the latest configuration when gateway running

Table 7-4-1 Definition of Auto Provision

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	



7.4.3 Configuring ACS

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
	The private configuration file for the specified gateway.
	Naming rules: "EPC-" + "mac" +".conf". The naming prefix of "EPC-" stands for the
EPC-{mac}.conf	private configuration file, "mac" is the physical address of network interface card but
	removed semicolon and ".conf" is the suffix. For example, the EPC-a0980501dbca.conf,
	'a0980501dbca' is the MAC address (A0:98:05:01:DB:CA).

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

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]

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

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.con:	f simple.scr	ipt
asterisk	lighttpd	ntp.conf	syslog.con	f
cron	logrotate.conf	php.ini	udhcpd.con	f
dahdi	logrotate.d	redis.conf	zoneinfo	
dnsmasq	network	services		
[root@dgw100x	/defconfig]#			

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



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.

Auto-provision Upgrade Notification X 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.

Figure 7-4-3 Auto provision notice

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.

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	

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



Figure 7-4-5 Check interval setting

Enable:	ON
Check Interval:	Every hour

- 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 7-4-6 The working directory of TFTP server

generate_md5_tool	2016/3/8 15:14	文件夹	
闄 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	42,64 <mark>1 KB</mark>
😰 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
👔 tftpd32.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.

.bin z

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



Figure 7-4-8 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 7-4-9 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.



Current Directo	ry E:	\tftpd32.450		→ E	Browse
Server interface	es 17	2.16.6.111	Realtek PC	▼ S	how Dir
Tftp Server	Fftp Clie	nt DHCP server	Log viewer		
peer		file	start time	progress	
2					
٩ [m			

Figure 7-4-10 Demo TFTP server

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

Figure 7-4-11 System notice logs

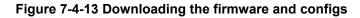
Notice Logs		
Date	Subject	Content
2016/03/08 15:55:47	Auto-provision Upgrade Notification	A new firmware and configs could be upgraded from ACS. Current release is : 1.1.0, ACS server release is :1.1.2. If you want to upgrade, please restart the system and wait several minutes.
		Refresh Clean Un





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

update configurations.



[OK]	
Setting up interface lo	C OK 1
starting SSH service	C OK 1
starting Redis service	C OK J
starting SOAP service	C OK 1
Checking the network between IFTP server a Info: Auto-Provision switch has been enab	nd T1/E1 Gateway, wait a mom led
Info : Checking firmware upgrade flag	[On]
Auto Configuration Server URL : 172.16.6.1 Info : Checking firmware md5	11 nismatch]
Preparing to download new fw image from 172	2.16.6.111.
firmware URL : 172.16.6.111	
firmware name : DGW100x-current.b;	in self the self-state state has been
firmware download from : tftp	
Download Progress: 13.5M, Time lapses: 18	Sec



Figure 7-4-14 Applying the firmware and configs

Asterisk service status Info : Updating system configs	[Stoped]
Info: New configs have been loaded success info : New firmware and configs to take ef al seconds	fully! fect , System will be restar
_	••••••

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

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 assigned by Internet
Private Enterprise Number	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)

Table 7-5-1 Definition of SNMP setting



User Configuration

Only exist in v3. Add a v3 account to SNMP. Notice that the 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.

SNMP	Parameter									
	SNMP Enable:	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					Security Name					
1	notConfigGroup		notConfigUser							
View (Configuration									
Order	ViewName		View Subtr	ubtree ViewMask						
1	all		.1	NA						
Acces	Access Configurationv1/v2c									
Order	7			Read		_	Write		Notify	
1	notConfigGroup			all		-	none	•	none	•
Save										

Figure 7-5-1 Activating the SNMP

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 MibBrow	ser Free Tool	10.		
<u>File Edit ⊻iew Operation</u>	s <u>H</u> elp			
🚵 📥 🗉 🕺 日	3 6 6 1	n 😰 🔊 🧠 🧠 🖬	🐞 🛫 🚥 🧔 🖾 🚺 Download More Free Tools	
 Loaded MibModules IANAifType-MIB RFC1213-MIB IF-MIB SNMPv2-MIB 	Host Community Set Value Object ID	SNMPWALK Variable	Port 161 Write Community	×
	Loading MIBs .tmit MIB(s) Loaded Suc	bs\RFC1213-MIB .\mibs\IF-MIB ccessfully		*
	Description Mult	ti Var		
	Syntax Access Index		Status Reference	
Global View	Object ID Description			

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 MibBrows	er Free Tool				
<u>File Edit View Operations</u>	: <u>H</u> elp				
) 🖬 🚷 🖻 🎂	3 6 6	🐂 🗊 🔊 🧠 💆 🛍 🗉	1 👋 🐋	: 🐵 🔌 🗵	Oownload More Free Tools
Hed MibModules ANAirType-MIB RFC1213-MIB F-MIB SIMMPV2-MIB Printernet System System SysObjectID SysObjectID SysObjectID SysObjectID SysObjectID SysObjectID SysObjectID SysObjectID SysOcation SysServices SysOcatact	MIB(s) Loaded	I successfully Intersection of the second	rite Commur		
in - ⊞ sysORTable	Syntax Access	MultiVar DisplayString (SIZE (0255.) read-write	Status Reference	current	
Index Object ID Image: Description Image: Description					. If the location is

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

OpenVox

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 Tabl	
<u>File Edit View Operations</u>		
法 📥 🗈 ጰ 🖶 🐣) 🖻 🖻 🐃 🗊 秒 🧠 🏹 🗠 🗉	🛙 🐗 🛫 🚥 🧇 🔯 🚺 Download More Free Tools
Loaded MibModules DIGIUM-MIB IANAirType-MIB RFC1213-MIB I-3 IF-MIB ASTERISK-MIB SNMPv2-MIB	Host 172.16.100.223 Community Set Value VoIP gateway Object ID	Port 161 Virite Community
	Sent GET request to 172.16.100.223 : 161	gateway
	sysName.0 VoIP	gateway
	Description MultiVar	
	Syntax	Status
	Access	Reference
×	Index Object ID	
Global View 📄	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 TR-069 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	
	Information of the device vendor, which may be used to indicate the primary service	
Provisioning Code	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 Url	The address used for the ACS to connect back to the device.	
Connection Request	The appoint used for the ACS to connect head to the device, for example, admin	
Username	The account used for the ACS to connect back to the device, for example, admin.	
Connection Request	The password used for the ACS to connect back to the device.	
Password		

Table 7-6-1 Definition of TR069 configuration interface

Figure 7-6-1 TR069 configuration interface

TRU09 Parameter	
Enable:	
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 have 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
Network Interface	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.

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

Figure 7-7-1 Network capture interface

Network Interface:	Eth0 O Eth1
Source host:	
Destination host:	
Port:	
Protocol:	



8 Logs

8.1 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 is unavailable. And the same with other log pages.

System Logs	
Auto clean:	OFF maxsize : 500KB V
Asterisk Logs	
Verbose:	OFF
Notice:	OFF
Warning:	
Debug:	OFF
Error:	
DTMF:	OFF
Auto clean:	OFF maxsize : 2MB V
SIP Logs	
SIP Logs:	OFF
Auto clean:	OFF maxsize : 2MB
IAX2 Logs	
IAX2 Logs:	OFF
Auto clean:	ON maxsize : 2MB 💌
MFC/ R2 Logs	
MFC/ R2 Logs:	OFF
Auto clean:	ON maxsize : 2MB 💌
PRI Logs	
PRI Logs:	OFF
Auto clean:	ON maxsize : 2MB 💌

Figure 8-1-1 Logs Settings



SS7 Logs	
SS7 Logs:	OFF
Auto clean:	ON maxsize : 2MB -
Call Statistics	
Call Statistics:	
System Notice	
Enable:	
Check Interval:	Every day 💌

Save

Figure 8-1-2 System Logs Output

System Logs		
2012/01/01	23:29:08]	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
2015/03/26	12:01:381	Kernel upgrade
		Basefs upgrade
		first starting up
2015/03/26		
2015/03/26		

Refresh Rate: Off

Refresh Clean Up

Table 8-1-1 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.
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		
	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		
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		
	PRI port logs. You can choose one or more ports. If you choose "All", the "PRI"		
PRI Logs	page will show you the logs about all the ports.		
	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 (PRI logs)	Switch off: logs will remain, and the file size will increase gradually.		
	default on, default size=2 MB		
	1		



ET 200X(L) Series Digital Gateway User Manual

.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	

8.2 System log

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

Figure 8-2-1 System Log

System Logs		
		Î
[2015/08/03 16:16:48] Kernel upgrade		
[2015/08/03 16:16:51] Basefs upgrade		
[2015/08/03 16:23:36] Power off		
[2015/08/03 16:24:21] Power on		
[2015/08/03 16:24:45] first starting up		
[2015/08/03 16:24:48] Power off		
[2015/08/03 16:25:33] Power on		
[2015/08/05 15:17:09] Power on		
[2015/08/06 15:30:03] Power off		
[2015/08/06 15:30:48] Power on		
[2015/08/06 15:35:03] Power off [2015/08/06 15:35:47] Power on		
[2015/08/06 15:55:03] Power off		
[2015/08/06 15:55:47] Power on		
[2015/08/11 07:16:45] Power on		
[2015/08/12 11:50:53] Power on		
[2015/08/12 13:28:15] Power on		
[2015/08/13 17:54:51] Kernel upgrade		
[2015/08/13 17:54:53] Basefs upgrade		
[2015/08/13 17:55:00] Power off		
[2015/08/13 17:55:45] Power on		
[2015/08/14 08:10:36] Power on [2015/08/14 17:19:49] Power off		
[2015/08/14 17:19:49] Fower on		
[2015/08/14 16:29:44] Power off		-
[2015/08/14 16:29:44] Fower on		
[2010/00/14 10:30:20] rower OR		//
	Refresh Rate: Off Refresh Clean Up Download	

8.3 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.



Asterisk Logs

		0 0			
				NOTICE[10073]: pbx_ael.c: /extensions.ael'.	:177 in pbx_load_module: AEL load process: parsed config file name '/mnt/ext4
					:180 in pbx load module: AEL load process: checked config file name
				.g/asterisk/extensions.ael	
					:187 in pbx load module: AEL load process: compiled config file name
				.g/asterisk/extensions.ael	
					:192 in pbx load module: AEL load process: merged config file name '/mnt/ext4
				/extensions.ael'.	is in pox_load_module: ALL load process: merged config file name "/mit/exts
					:195 in pbx load module: AEL load process: verified config file name
				.g/asterisk/extensions.ael	
					28082 in handle request subscribe: Received SIP subscribe for peer without
	x: 2001) a	corres[20200]. N	STICE[ESES.]. Chan_Sip.C.	roor in manare_requess_assorise, acceived our subscribe for peer without
		(none)	asterisk[25205]:	NOTICE (25257) [C-000008ce]]: chan sip.c:10558 in process sdp: No compatible codecs, not accepting this
ffer!		,,			·······
		(none)	asterisk[25205]:	NOTICE[252571[C-000008cf]]: chan sip.c:10153 in process sdp: set peer prefer
]: chan sip.c:10158 in process sdp: p->owner->readformat is ulaw
]: chan sip.c:10159 in process sdp: p->owner->readformat is ulaw
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE [10273] [C-000008cf]: chan sip.c:7160 in sip answer: ast readformat is ulaw
]: chan sip.c:7161 in sip answer: ast writeformat is ulaw
]: chan sip.c:7162 in sip answer: ast jointcaps is (ulaw)
]: chan sip.c:7164 in sip answer: ast reset jointcaps is (ulaw)
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE [25257] [C-000008cf]]: chan sip.c:10153 in process sdp: set peer prefer
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE [25257] [C-000008cf]]: chan sip.c:10158 in process sdp: p->owner->readformat is ulaw
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE [25257] [C-000008cf]]: chan_sip.c:10159 in process_sdp: p->owner->readformat is ulaw
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE[25257][C-000008cf]]: chan_sip.c:10153 in process_sdp: set peer prefer
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE[25257][C-000008cf]]: chan_sip.c:10158 in process_sdp: p->owner->readformat is ulaw
far 10	11:45:16	(none)	asterisk[25205]:	NOTICE[25257][C-000008cf]]: chan_sip.c:10159 in process_sdp: p->owner->readformat is ulaw
				Defrech Date:	a Refer the Research and
				Refresh Rate: 1s	Refresh Clean Up Download

8.4 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 8-4-1 Call 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%

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

8.5 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 like figure 8-5-1.



Figure 8-5-1 enable system notice function

ystem Notice Enable:	ON	
Check Interval:	Every hour	

After about an hour, a system message is received in the web like 8-5-2.

Figure 8-5-2 enable system notice function

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 upgr 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.

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

receive system messages.