NXGW-XET1 User Manual

INDEX

Introduction	4	Language Settings	11
Sample Application	4	Scheduled Reboot	11
The Front Panel	5	Tools	11
Main Features	6	Reboot Tools	11
Logging In	6	Description of reboots	12
System Status	7	Update Firmware	12
Description of System Status	7	Upload and Backup Configuration	12
Call Status	8	Restore Configuration	12
Time Settings	8	System Information	13
Example Time Settings	9	T1/E1	13
Login Settings	9	General Settings	13
Description of Web Login Settings	10	Advanced interface type	14
Login Settings	10	Port Details	14
General	11	PRI	15

Definition of Signaling 15
MFC/R2 17
Modify R2 variant 18
General 18
Description of General 19
Timer 20
Description of Timer 20
Group A 21
Group B 22
Group C 22
Group 1 22
Group 2 23
Chan-SS7 23
Link Set Settings 23
Chan-SS7 Link Set Settings 24
Definition of SS7 Link Set Settings 25
Link Settings 26
SS7 Edit Link Settings 26
SS7 Configuration file backup and restore 26
VOIP 27
SIP Endpoints 27
Main Endpoint Settings 27
None Registration 27
Endpoint Register with Gateway 28
This Gateway Register with the Endpoint 28
Definition of SIP Options 29
Advanced Registration Options 29
Call Settings 30
Advanced Signaling Settings 30
Advanced Timer Settings 31
Fax Options 32
IAX2 Endpoint 32
Edit IAX Endpoint “9001” 33
Definition of IAX2 Endpoint 33
Advanced SIP Settings 35
Advanced NAT Settings 35
Advanced RTP Settings 36
Parsing and Compatibility 37
Security 38
Media 39
Codec Settings 39
Advanced IAX2 Settings 39
Instruction of Music on Hold 40
Instruction of Codec Settings 41
Instruction of Jitter Buffer 41
Instruction of Misc Settings 42
Instruction of Quality of Service 42
Advanced fax settings 42
Routing 43
Call Routing Rule 43
Example for routing rules number conversion 44
Example Setup of Routing Rule 44
Definition of Routing Options 45
Description of Advanced Routing Rule 45
Time Patterns that will use this Route 46
Forward Number 46
Failover Call Through Number 46
Groups 47
Establish Group 47
Network 47
Network Settings 47
Definition of WAN/LAN Settings 48
DNS Servers 48
DDNS Settings 48
Definition of DDNS Settings 49
Toolkit 49
Network Connectivity Checking 49
Static Route Settings 50

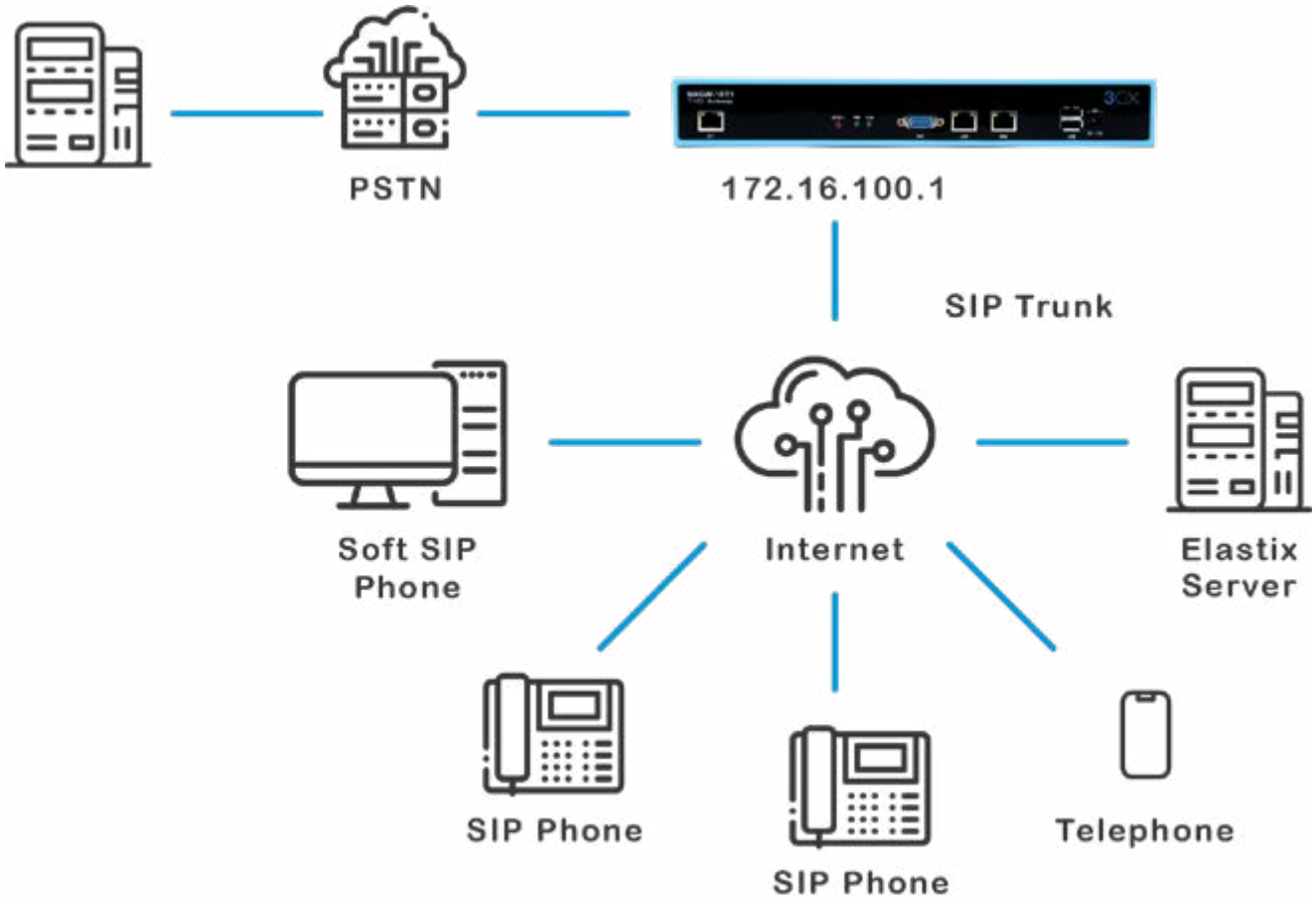
Advanced 50
Asterisk API 50
Definition of Asterisk API 51
Asterisk CLI 52
Definition of Asterisk CLI 52
Definition of Lock/unlock channels 52
Asterisk File Editor 53
Auto Provisioning 53
Preparation 54
Configuring gateway 54
Definition of Auto Provision 54
Definition of system notice 55
Auto Provision interface 55
Configuring ACS 55
Definition of ACS files 56
Provisioning example 57
SNMP 62
Parameters in SNMP setting 62
Activating SNMP 63
Verify SNMP 63
TR069 65
Network Capture 67
Definition of Network capture 67
Network capture interface 67
Signal Capture interface 68
Port Recording interface 68
Cloud 68
Connecting to the Cloud 68
Definition of Cloud Management 69
User 69
Add User 69
User List 69
User Permissions 70
Logs 70
Log Settings 70
System Logs Output 71
Definition of Logs 72
System log 73
Asterisk logs 74
Call Statistics 74
System Notice 75

INTRODUCTION

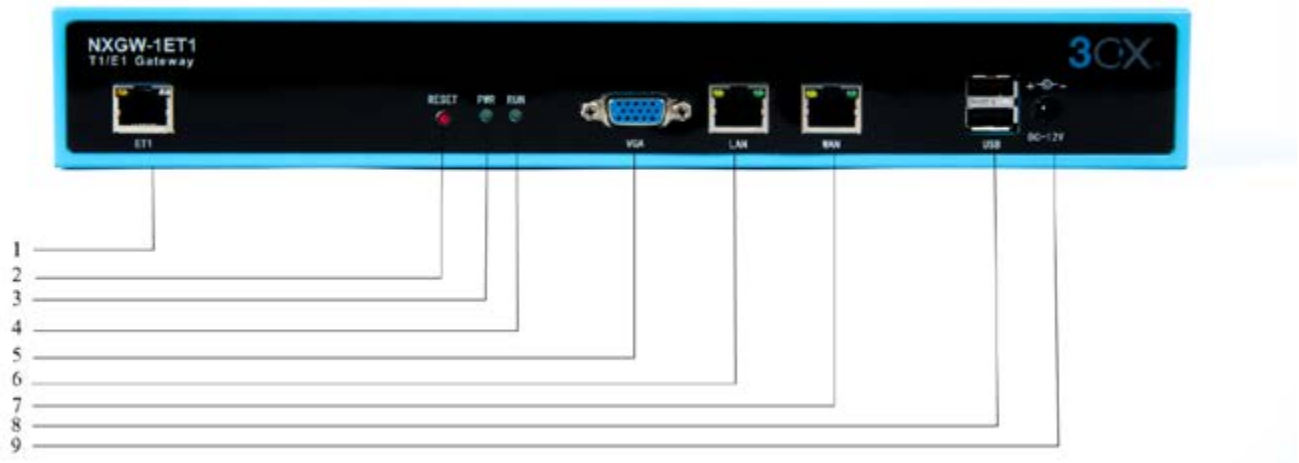
NXGW-XET1 Gateway is an open-source Asterisk-based VoIP Gateway. It is a converged media gateway product. This kind of gateway connects traditional telephone systems to IP networks and integrates VoIP PBX with the PSTN seamlessly. With a friendly GUI, users may easily set up their customized Gateway. Also, secondary development can be completed through AMI (Asterisk Management Interface).

It is developed with a wide selection of codecs and signaling protocol, including G.711A, G.711U, G.729, G.722, G.723 and GSM. It supports PRI/SS7/R2 protocol. The NXGW-XET1 Gateway has good processing ability and stability. The NXGW-XET1 gateway is 100% compatible with Asterisk, Elastix, 3CX, FreeSWITCH SIP server and VOS VoIP operating platform.

Sample Application



Front Panel



Interface	Function	Color	Work Status
1 Port 1-Port4	ET1 ports. There is only one port.		
2 Reset	Reset button is used to restore the device.		
3 RUN	Register indicator	Green	Slow blinking (Green 2s and Flash 0.1s): Work normally.
			Fast blinking (Green 0.5s and Flash 0.5s): Work abnormally.
			Fast blinking (Green 0.5s and Flash 0.5s): Work abnormally.
4 PWR	Power Status indicator	Green	No blinking: DAHDI Error.
			On: Power is on.
			Off: Power is off.
5 VGA	VGA monitor connector.		
6 LAN	Network interface.		
7 WAN	Network interface.		
8 USB	USB interface.		
9 DC-12V	Power supply.		

MAIN FEATURES

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

LOGGING IN

- Default IP: 172.16.100.1(WAN),

  192.168.100.1(LAN)
- Username: admin
- Password: admin
- Notice: Log in

SYSTEM STATUS

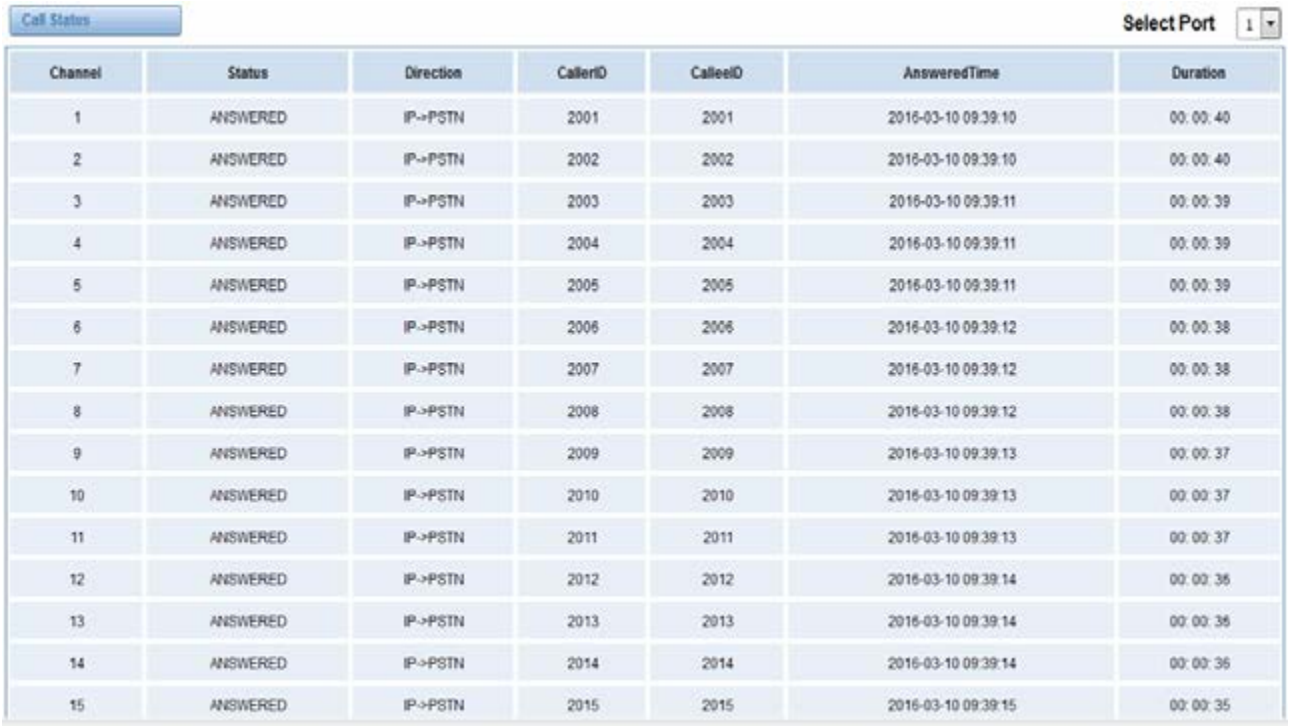
Once logged in navigate to the "System Status" page. Here you will find all Interface status, channels status, SIP, IAX2, Routing rules, and Network information.

DESCRIPTION OF SYSTEM STATUS

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

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.



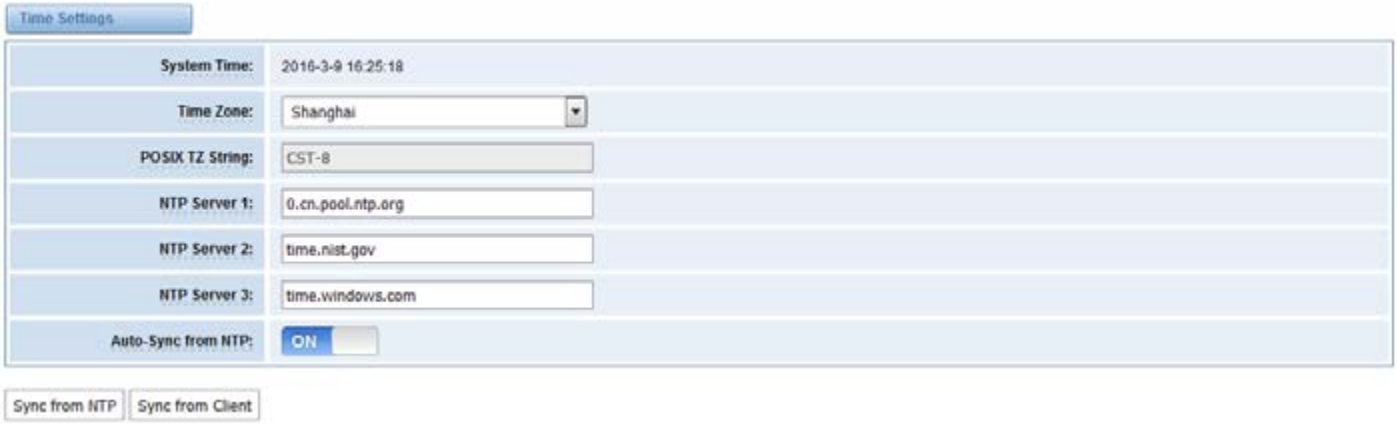
Channel	Status	Direction	CallerID	CalleeID	AnsweredTime	Duration
1	ANSWERED	IP->PSTN	2001	2001	2016-03-10 09:39:10	00: 00: 40
2	ANSWERED	IP->PSTN	2002	2002	2016-03-10 09:39:10	00: 00: 40
3	ANSWERED	IP->PSTN	2003	2003	2016-03-10 09:39:11	00: 00: 39
4	ANSWERED	IP->PSTN	2004	2004	2016-03-10 09:39:11	00: 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

TIME SETTINGS

Options	Definition
System Time	Your gateway system time.
Time Zone	The world time zone. Please select the one which is the same or the closest as your city.
POSIX TZ String	Posix timezone strings.
NTP Server 1	Time server domain or hostname. For example, [0.cn.pool.ntp.org].

NTP Server 2	The first reserved NTP server. For example, [time.windows.com].
NTP Server 3	The second reserved NTP server. For example, [time.nist.gov].
Auto-Sync from NTP	Whether enable automatically synchronize from NTP server or not. ON is enable, OFF is disable this function.
Sync from NTP	Sync time from NTP server.
Sync from Client	Sync time from local machine.

Example Time Settings



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

LOGIN SETTINGS

Your gateway doesn't have administration role. All you can do here is reset a new username and password to manage your gateway. You can modify “Web Login Settings” and “SSH Login Settings”. If you have changed these settings, you don't need to logout, simply re-enter your new username and password. Also, you can specify the web server port number. Usually, the web login default mode is “http and https”. For safety purposes, you can switch to “only https” mode.

Description of Web Login Settings

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

Login Settings

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

GENERAL

Language Settings

You can select your language preference for your system. If you want to change the language, switch on the "Advanced" option and then "Download" your current language package. After that, you can modify the package with the language you need. Upload your modified packages, "Choose File" and "Add".

Scheduled Reboot

If this option is enabled, you can configure your gateway to reboot automatically. There are four reboot types for you to choose, "By Day, By Week, By Month and By Running Time".

TOOLS

On the "Tools" pages, there are reboot tools, update Firmware, upload Configuration, backup Configuration and Restore Configuration toolkits.

Reboot Tools

You can choose system reboot or Asterisk reboot separately.

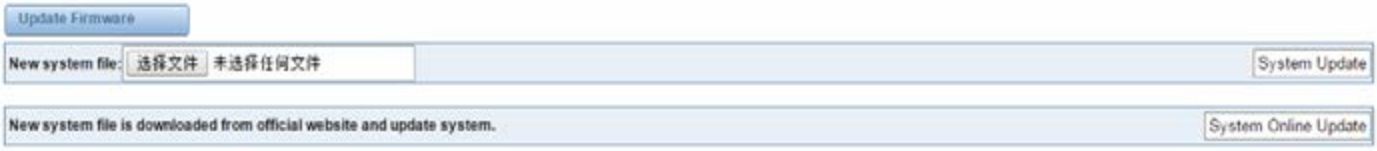
If you press "OK", your system will reboot and all current calls will be dropped. Asterisk Reboot is the same.

Description of reboots

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

Update Firmware

We offer two types of update options. You can choose System Update or System Online Update. System Online Update is an easier way to update your system.

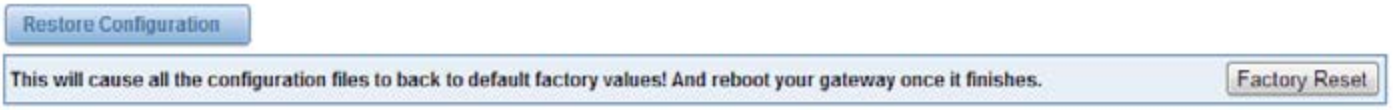


Upload and Backup Configuration

If you want to update your system and keep your previous configuration, you must first backup your current configuration and once the update is completed upload the configuration.

Restore Configuration

In the event that you need to factory reset your gateway simply click on the button as shown below and your gateway will be reset to the factory status.

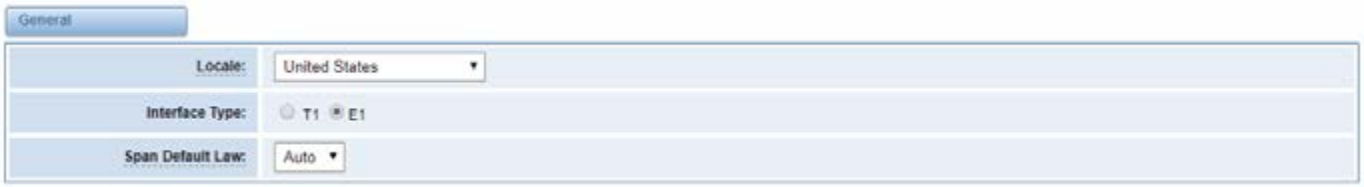


System Information

On the "Information" page, you will find basic information about the T1/E1 gateway. You can see the software and hardware version, storage usage, memory usage and some help information.

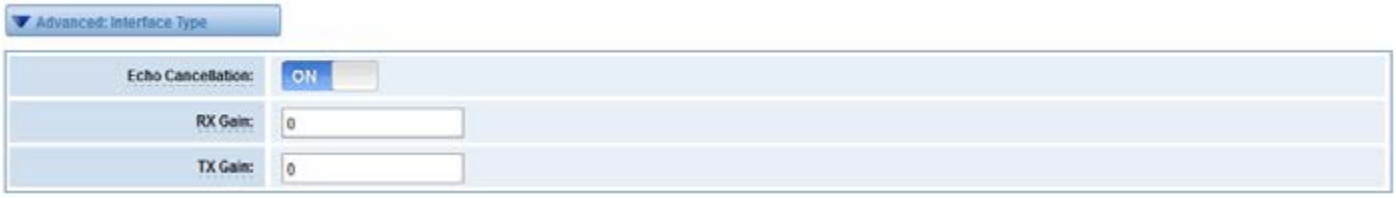
T1/E1

General Settings



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

Advanced interface type



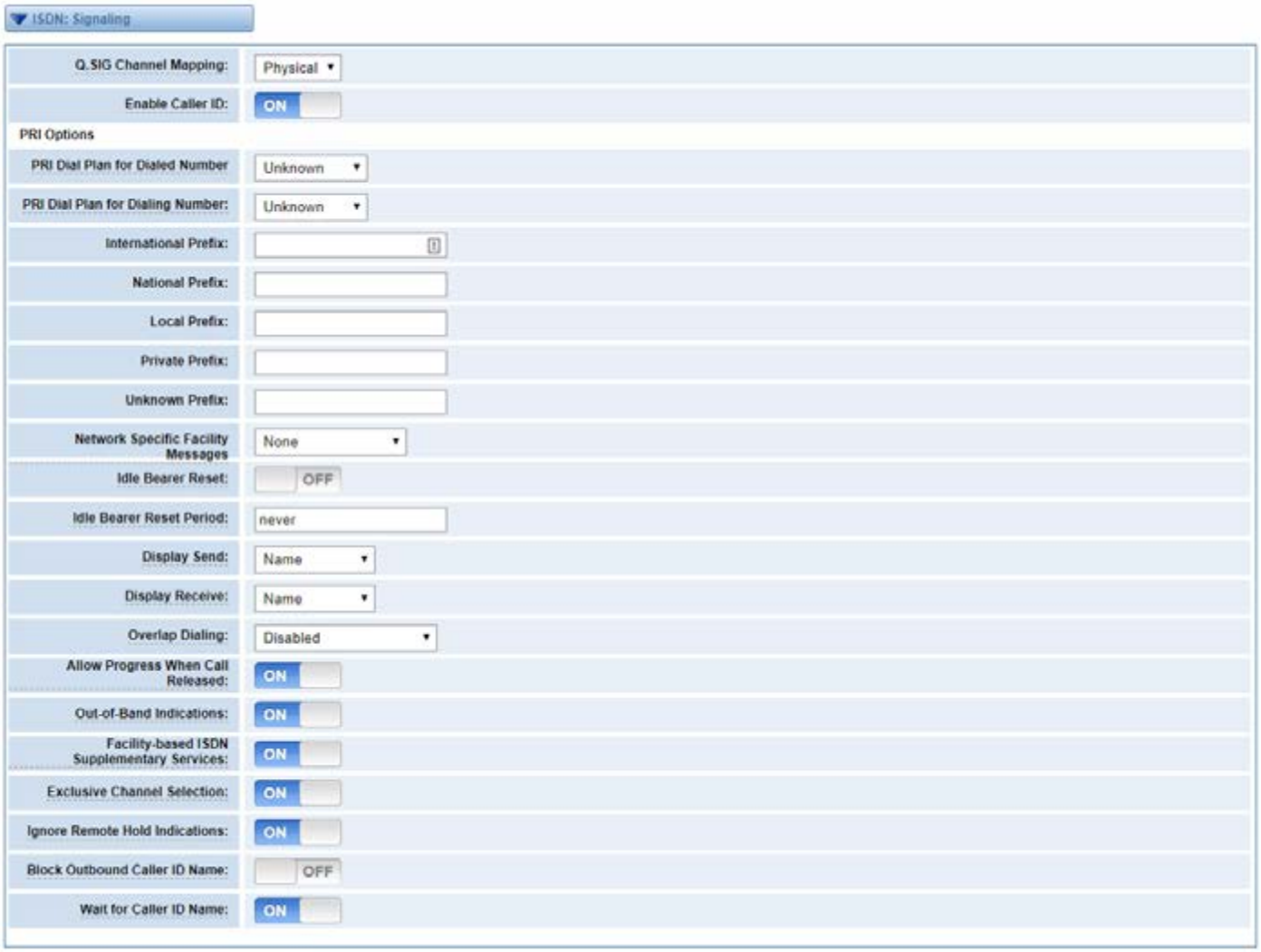
Options	Definition
RX Gain	Gain for the RX (receive -into Asterisk) channel.Default:0.0.
TX Gain	Gain for the TX (transmit -out of Asterisk Asterisk) channel.Default:0.0.

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.

PRI



Definition of Signaling

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 digits; caller ID number and setting the prilocaldialplan to 'national' (the default). Only VERY rarely will you need to change this.
Network Specific Facility (NSF) Messages	Some switches (AT&T especially) require network specific facility IE. 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. 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 mode-sending overlap digits.

Allow Progress When Call Released	Allow inband audio (progress) when a call is DISCONNECT Ted by the end of a PRI.
Out-of-Band Indications	PRI Out of band indications. Enable this to report Busy and congestion on a PRI using out_ of_ band notification. Inband indication, as used by the gateway doesn't seem to work with all telcos.
Facility-based ISDN Supplementary Services	To enable transmission of facility-based ISDN 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.

MFC/R2

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.

Modify R2 variant

R2 Variant

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

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

General

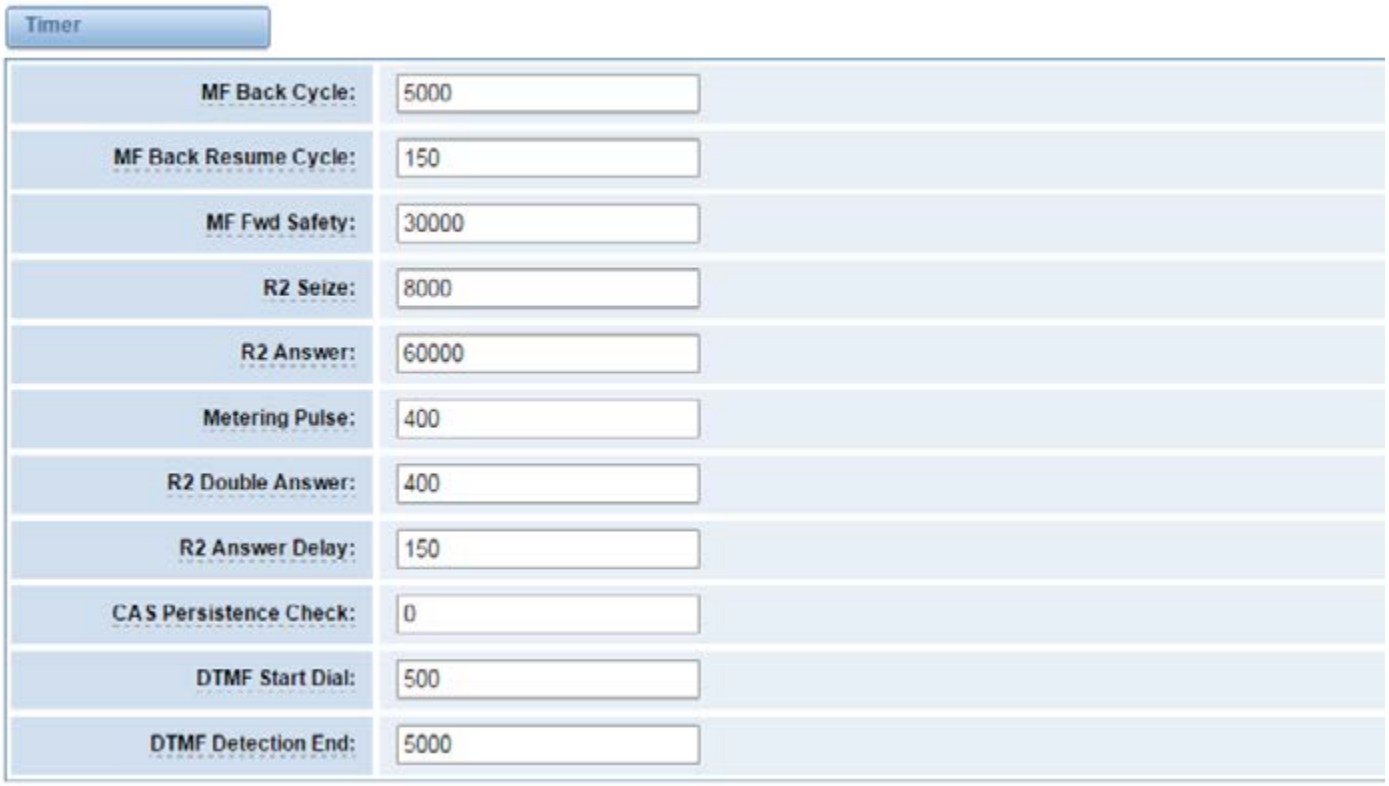
General

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

Description of General

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

Timer

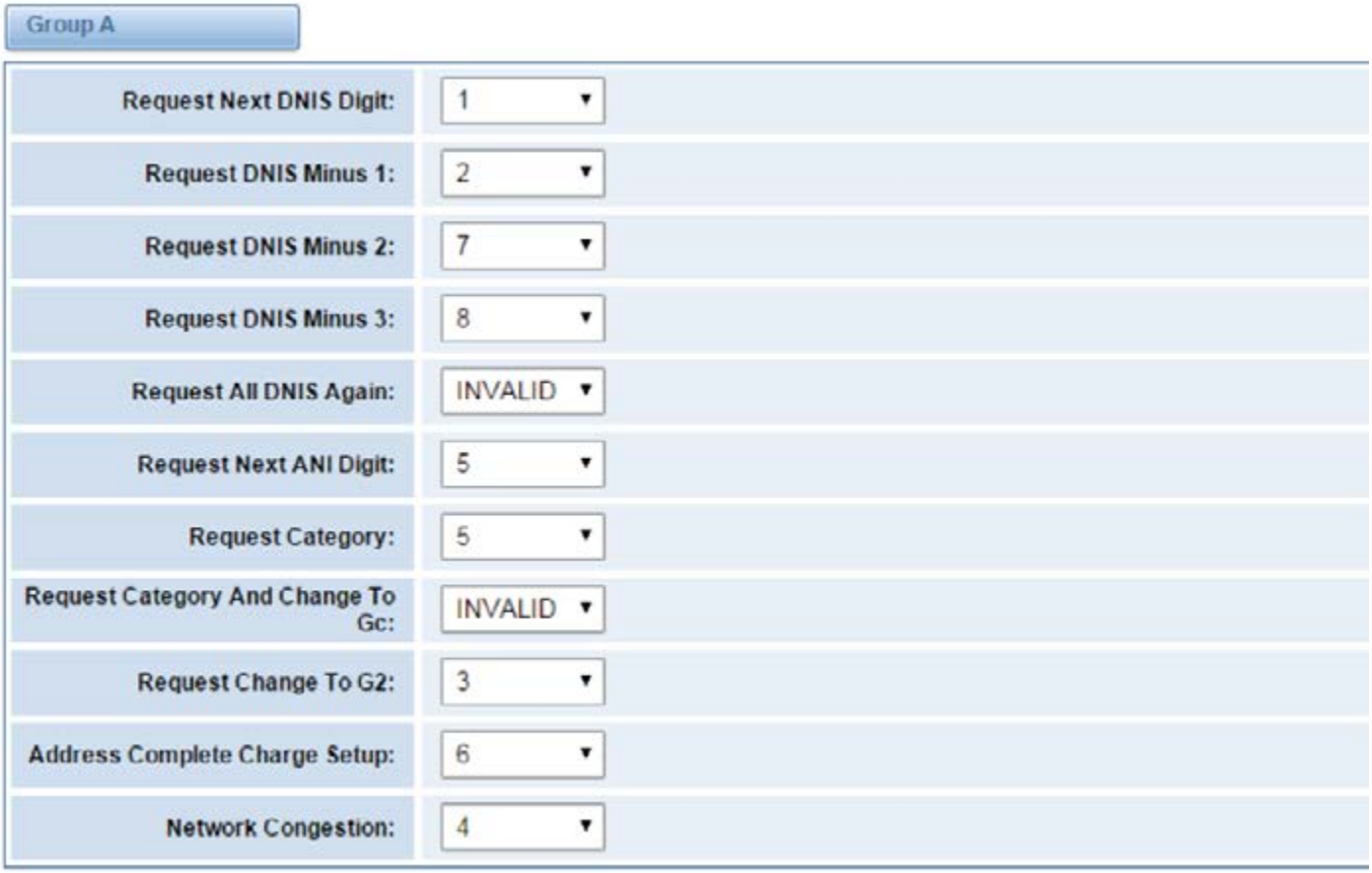


Description of Timer

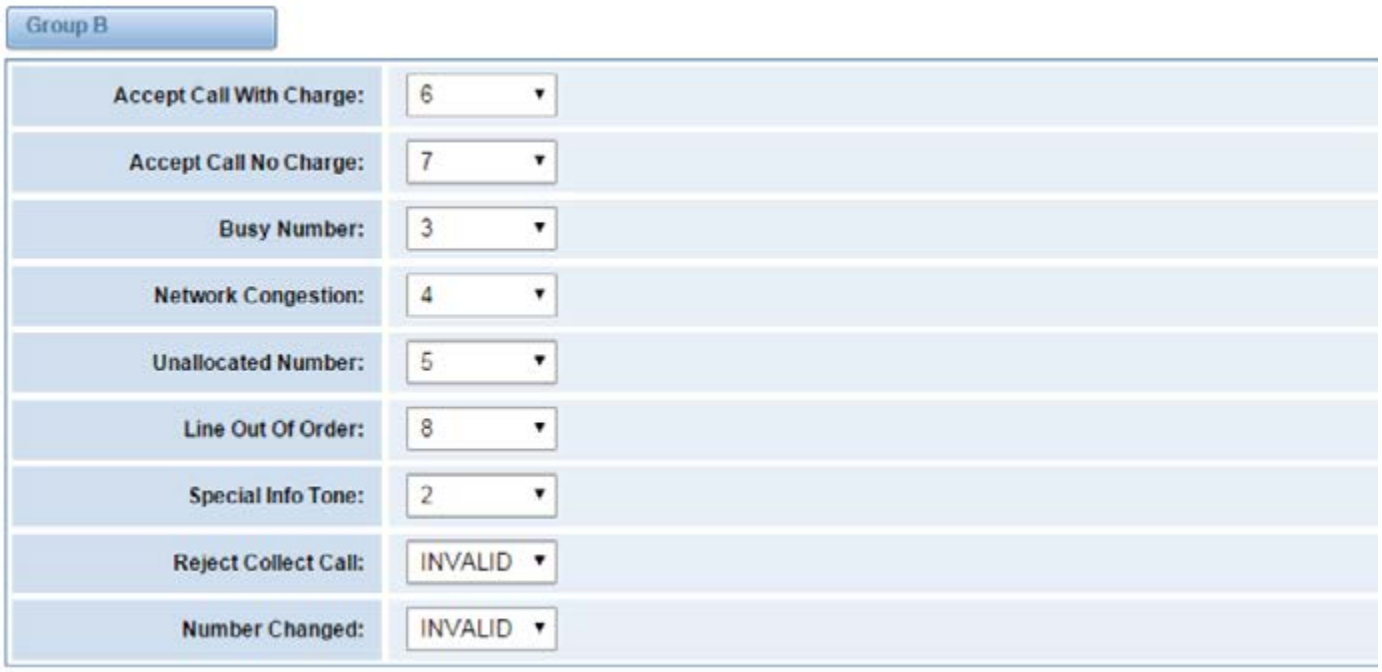
Options	Definition
MF Back Cycle	Max amount of time our backward MF signal can last.
MF Back Resume Cycle	Amount of time we set MF signal ON to resume the MF cycle with a MF pulse.
MF Fwd Safety	Safety FORWARD timer.
R2 Seize	How much time do we wait for a response to our seize signal.
R2 Answer	How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

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.

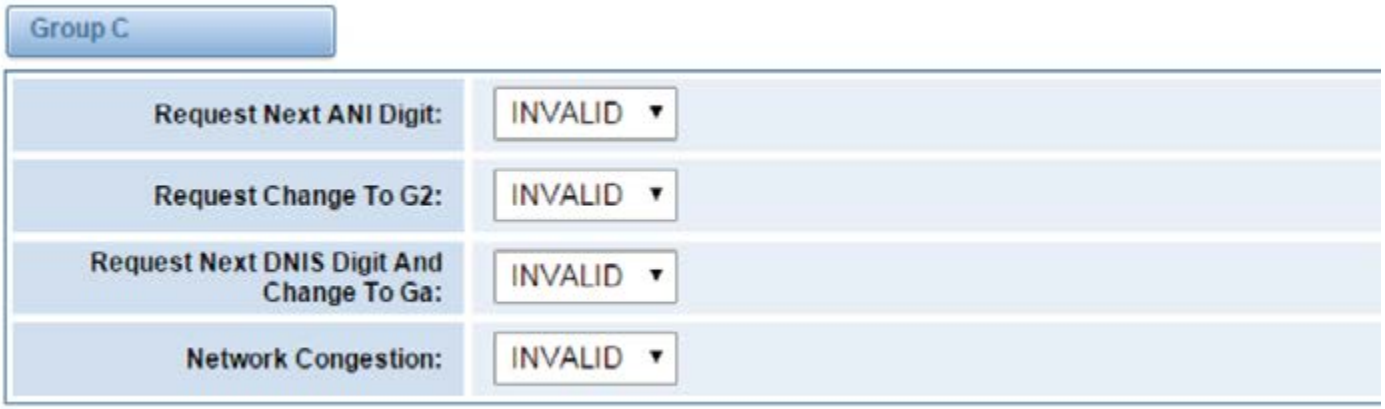
Group A



Group B

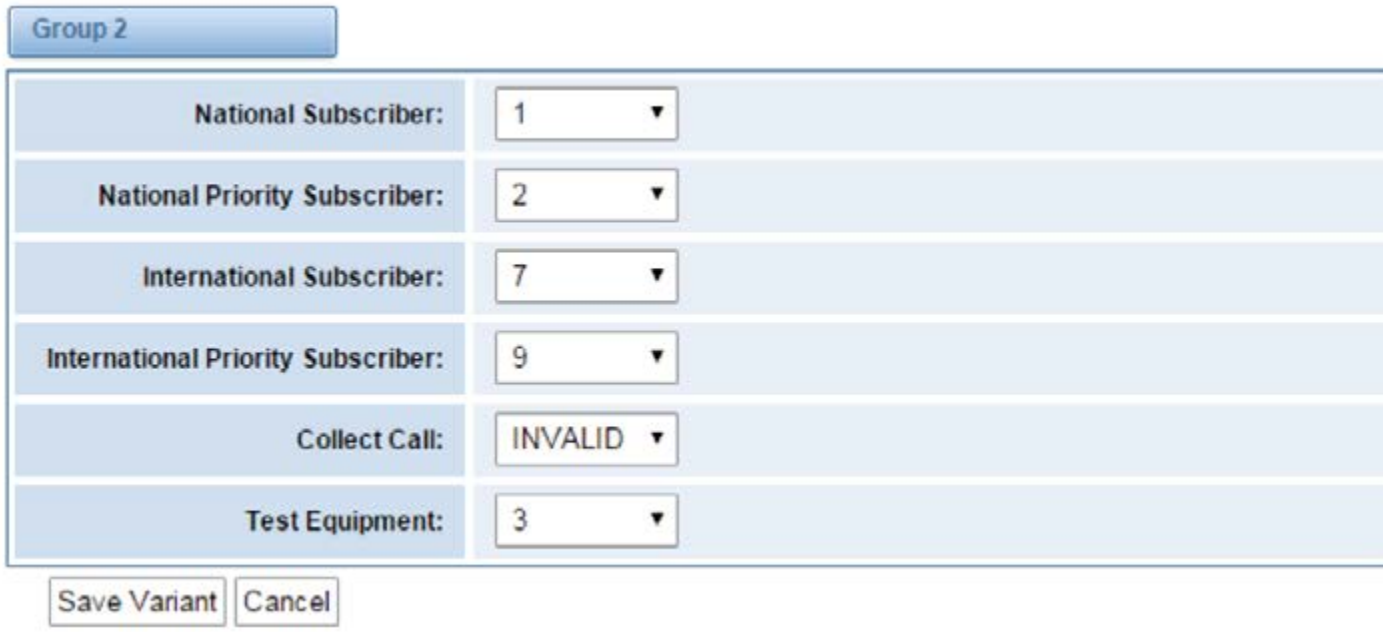


Group C



Group 1

Group 2



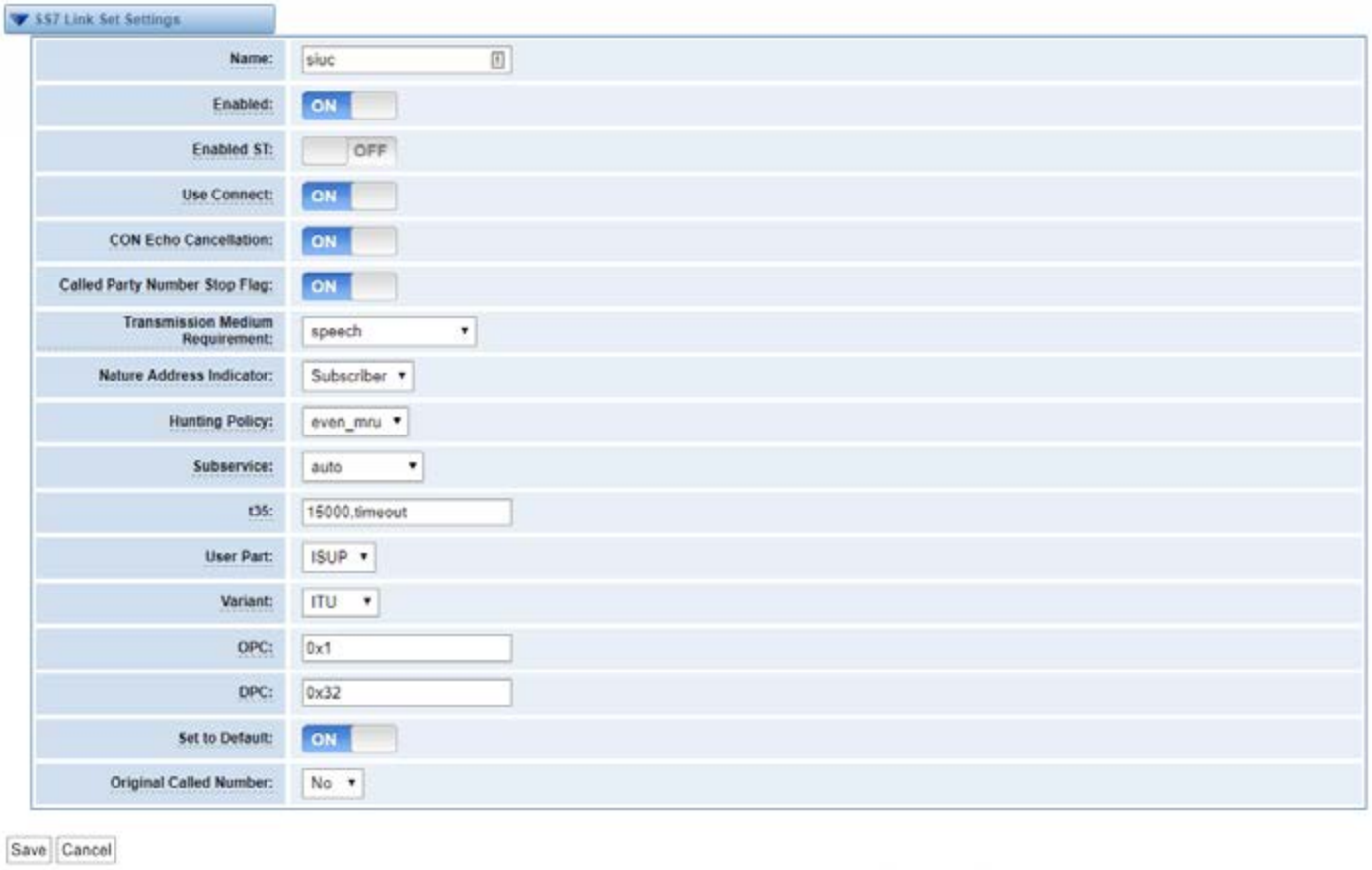
CHAN-SS7

Link Set Settings

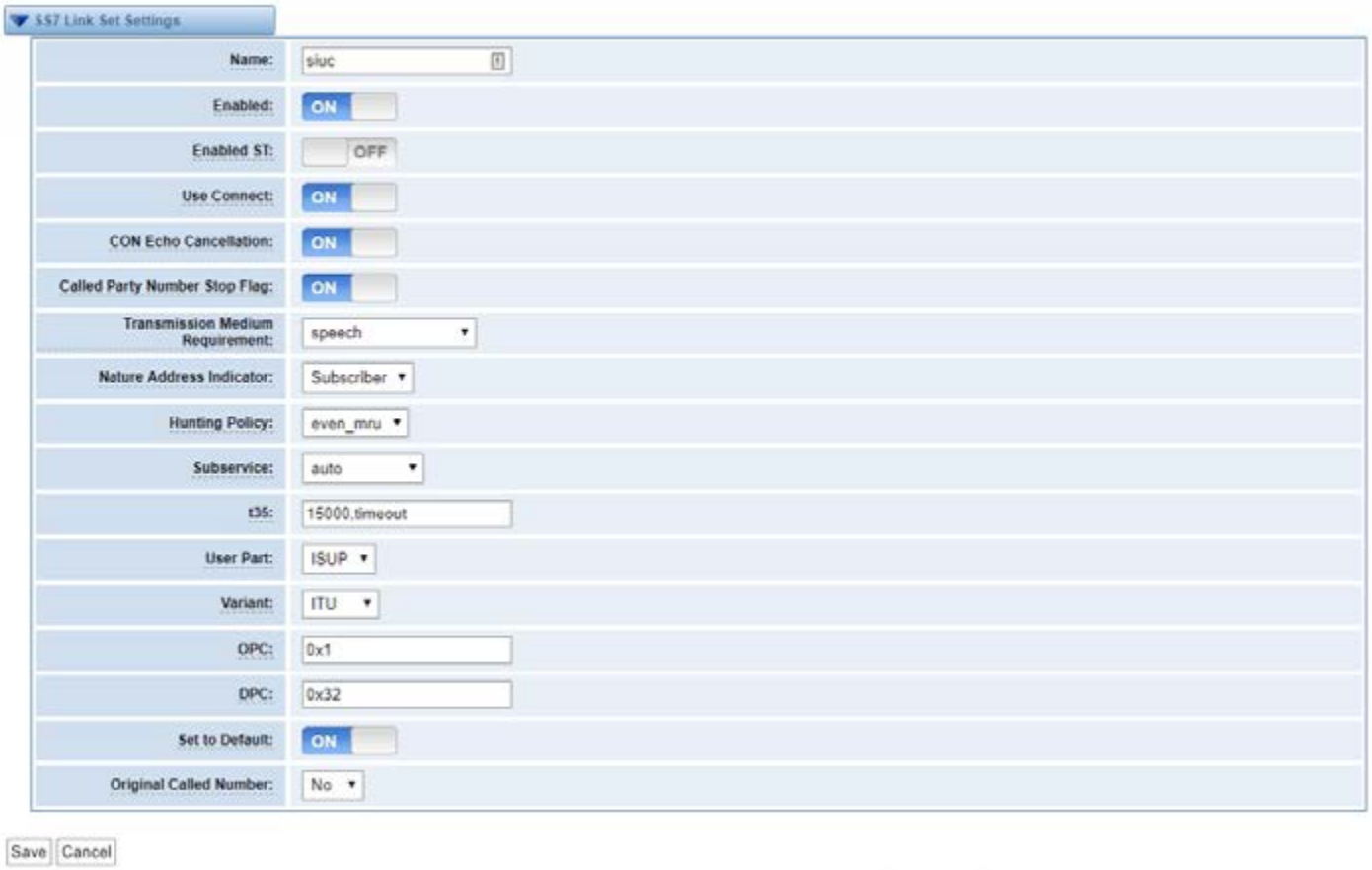
You can click button as shown above, when there are several link sets, only one can be set to the default.

Chan-SS7 Link Set Settings

Edit Link Set "linkset-siuc"



Edit Link Set "linkset-siuc"



Definition of SS7 Link Set Settings

Options	Definition
Name	The link set name.
Type	SS7 variant.
Enabled ST	This is used to decide whether end-of-pulsing is not used to determine when incoming address is complete.
Use Connect	This setting specifies whether to reply incoming call with CON rather than ACM and ANM.
CON Echo Cancellation	This setting will enable Echo Cancellation when 'Use Connect' is enabled.
Called Party Number Stop Flag	Add a stop flag 'F' before called number send.
Transmission Medium Requirement	Specify the bearer circuit capabilities (speech, 3.1-kHz audio, 64-Kb unrestricted, and so forth) that are needed for the call being set up.
Nature Address Indicator	The nature of address indicator field is national or subscriber(default).
Subservice	The subservice field: national, international, auto or decimal/hex value The auto means that the subservice is obtained from first received SLTM.
t35	The value and action for t35. Value is in msec, action is either st or time-out, If you use overlapped dialling dial plan, you might choose:4000,st.
User Part	The type of User Part.
Variant	Running under SS7 standard.
OPC	The point code for this SS7 signalling point.
DPC	The destination point code.
Set to Default	Set the linkset as the default linkset.
Original Called Number	Information sent in the forward direction when a call is redirected and identifies the original called party.

LINK SETTINGS

Link Settings

Link Name	iftype	Enabled	LinkSet	Channels	Schannel	First CIC	Echo Cancel	Echo Cancel Train	Echo Cancel Taps	SLS	SLTM	Port	Action
l1	E1	yes	siuc	1-15,17-31	16	1	no	350	128	0	yes	1	
l2	E1	yes	siuc	1-31		32	no	350	128	0	yes	2	
l3	E1	yes	siuc	1-31		63	no	350	128	0	yes	3	
l4	E1	yes	siuc	1-31		94	no	350	128	0	yes	4	

You can click button as shown above.

SS7 Edit Link Settings

Edit Link "link-l1"

SS7 Link Settings

Name:	l1
Enabled:	ON
Interface Type:	E1
Link Set:	siuc
Channels:	1-15,17-31
Schannel:	16
First CIC:	1
Echo Cancel:	no (default)
Echocan Train:	350 Range: 10-10000 Default value: 300
Echocan Taps:	128 (default)
SLS:	0
SLTM:	ON
Port:	1

Save Cancel

SS7 Configuration file backup and restore

SS7 Config. File Backup

Download SS7 Configuration File — Download Backup

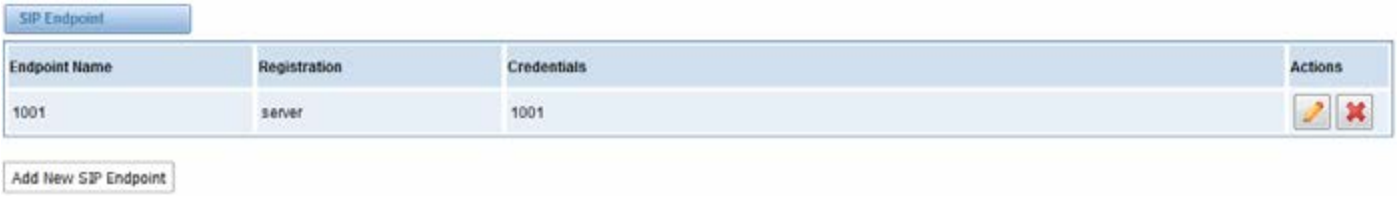
SS7 Config. File Restore

New configuration file: 选择文件 未选择任何文件 — File Upload

VOIP

SIP Endpoints

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



Main Endpoint Settings

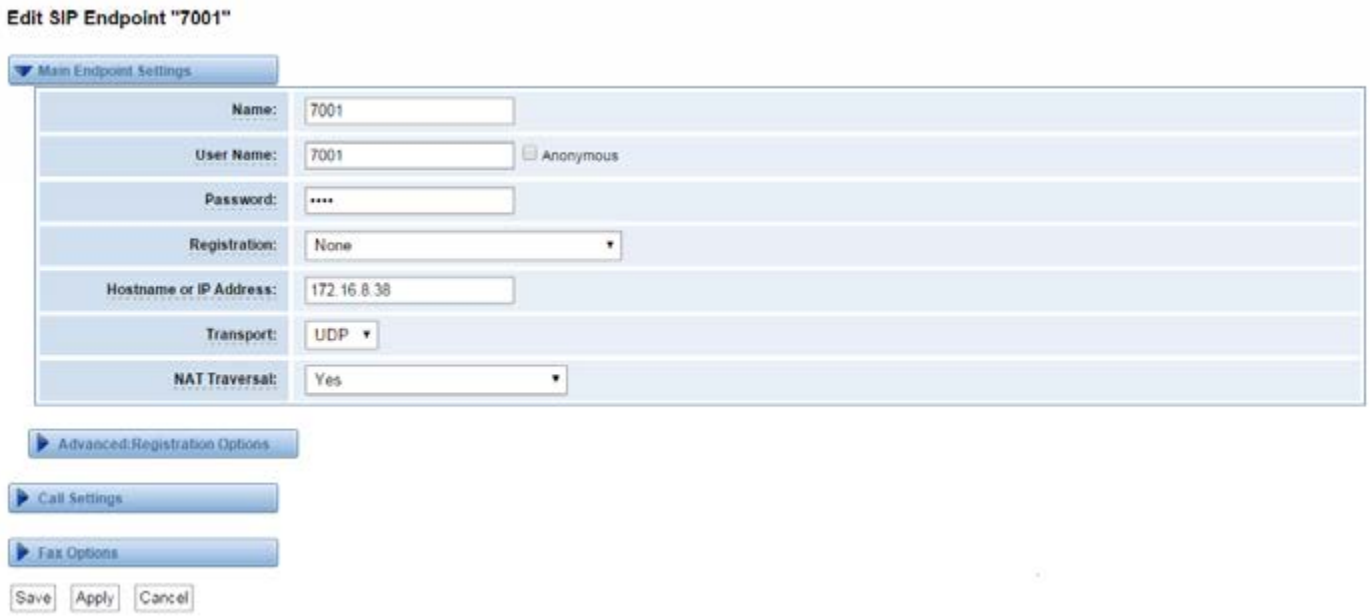
Click on the Add New SIP Endpoint button to add a new SIP endpoint, and if you want to modify existed endpoints, you can click the button.

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

You can configure as follows:

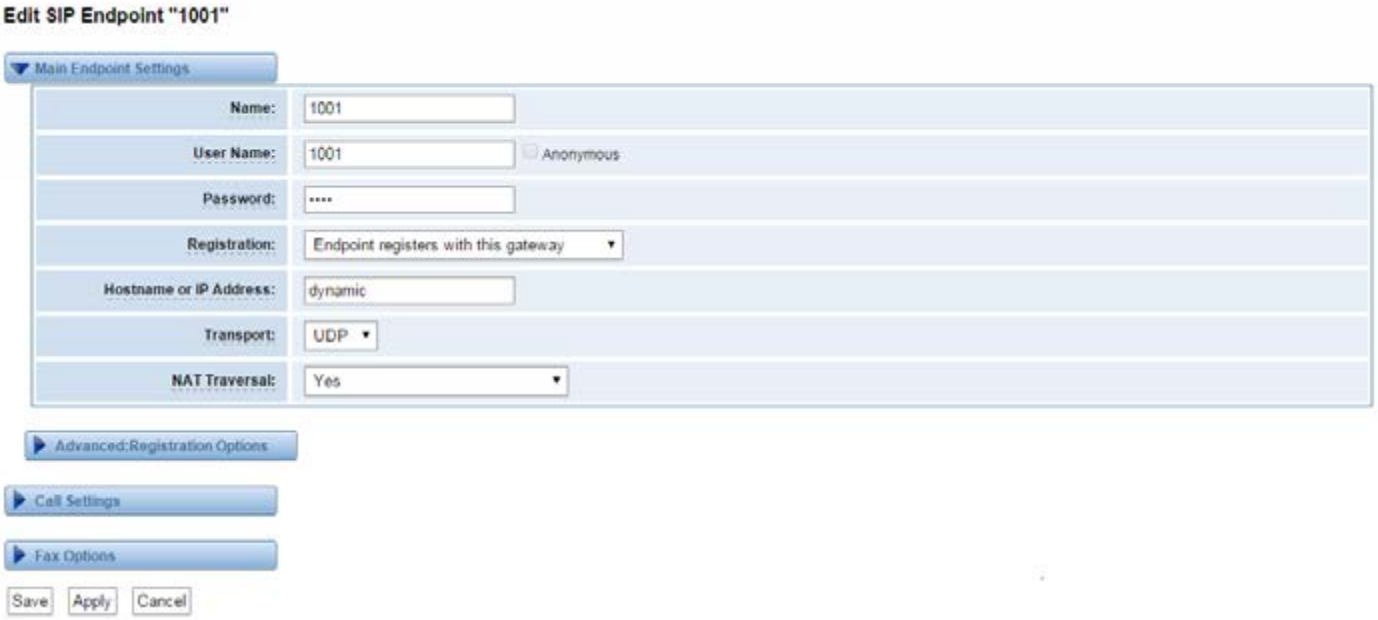
If you set up a SIP endpoint by registration “None” to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confusion.)

None Registration



For convenience, you can register your SIP endpoint to your gateway, thus your gateway just works as a server.

Endpoint Register with Gateway



You can choose registration by “This gateway registers with the endpoint”, it's the same with “None”, except for the name and password.

This Gateway Register with the Endpoint

Definition of SIP Options

Options	Definition
Name	A name which is able to read by human. And it's only used for user's reference.
Username	User name the end point use to authenticate with the gateway.
Password	Password the endpoint will use to authenticate with the gateway. Allowed characters.
Registration	Whether this endpoint will register with this gateway.
Hostname or IP Address	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a dynamic IP address. This will require registration. Notice: if the input here is hostname and your DNS has changed, you must reboot asterisk.
Transport	This sets the possible transport types for outgoing. Order of usage, when the respective transport protocols are enabled, is UDP, TCP, TLS. The first enabled transport type is only used for outbound messages until a Registration takes place. During the peer Registration the transport type may change to another supported type if the peer requests so.
Transmission Medium Requirement	Specify the bearer circuit capabilities (speech, 3.1-kHz audio, 64-Kb unrestricted, and so forth) that are needed for the call being set up.
NAT Traversal	Addresses NAT-related issues in incoming SIP or media sessions.

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 side.
Port	The port number the gateway will connect to at this endpoint.
Qualify	Whether or not to check the endpoint's connection status.
Qualify frequency Frequency	How often, in seconds, to check the endpoint's connection status.
Outbound Proxy	A proxy to which the gateway will send all outbound signaling instead of sending signaling directly to endpoints.

CALL SETTINGS

Options	Definition
DTMF Mode	Set default DTMF Mode for sending DTMF. Default: rfc2833. Other options: 'info', SIP INFO message (application/ dtmf-relay); 'Inband', Inband audio (require 64kbit codec - alaw, ulaw).
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.

ADVANCED SIGNALING SETTINGS

Options	Definition
Progress Inband	If we should generate in-band ringing. Always use 'never' to never use in-band signaling, Even in cases where some buggy devices might not render it. Valid values: yes, no, never. Default: never.
Append user=phone to URI	Whether or not to add;' user=phone' to URIs that contain a valid phone number.

Add Q.850 Reason Headers	Whether or not to add Reason header and to use it if it is available.
Honor SDP Version	By default, the gateway will honor the session version number in SDP packets and will only modify the SDP session if the version number changes. Turn This option off to force the SDP session version number and treat all SDP data as new data. This is require for devices that send non-standard SDP packets (observed with Microsoft OC S).By default This option is on.
Allow Transfers	Whether or not to globally enable transfers. Choosing 'no' will disable all transfers (unless enable in peers or users). Default is enabled.
Allow Promiscuous Redirects	Whether or not to allow 302 or REDIR to non-local SIP address. Note that promiscredir when redirects are made to the local system will cause loops since this gateway is incapable of performing a 'hairpin' call.
Max Forwards	Setting for the SIP Max-Forwards header (loop prevention).
Send TRYING on REGISTER	Send 100 Trying when the endpoint registers.

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

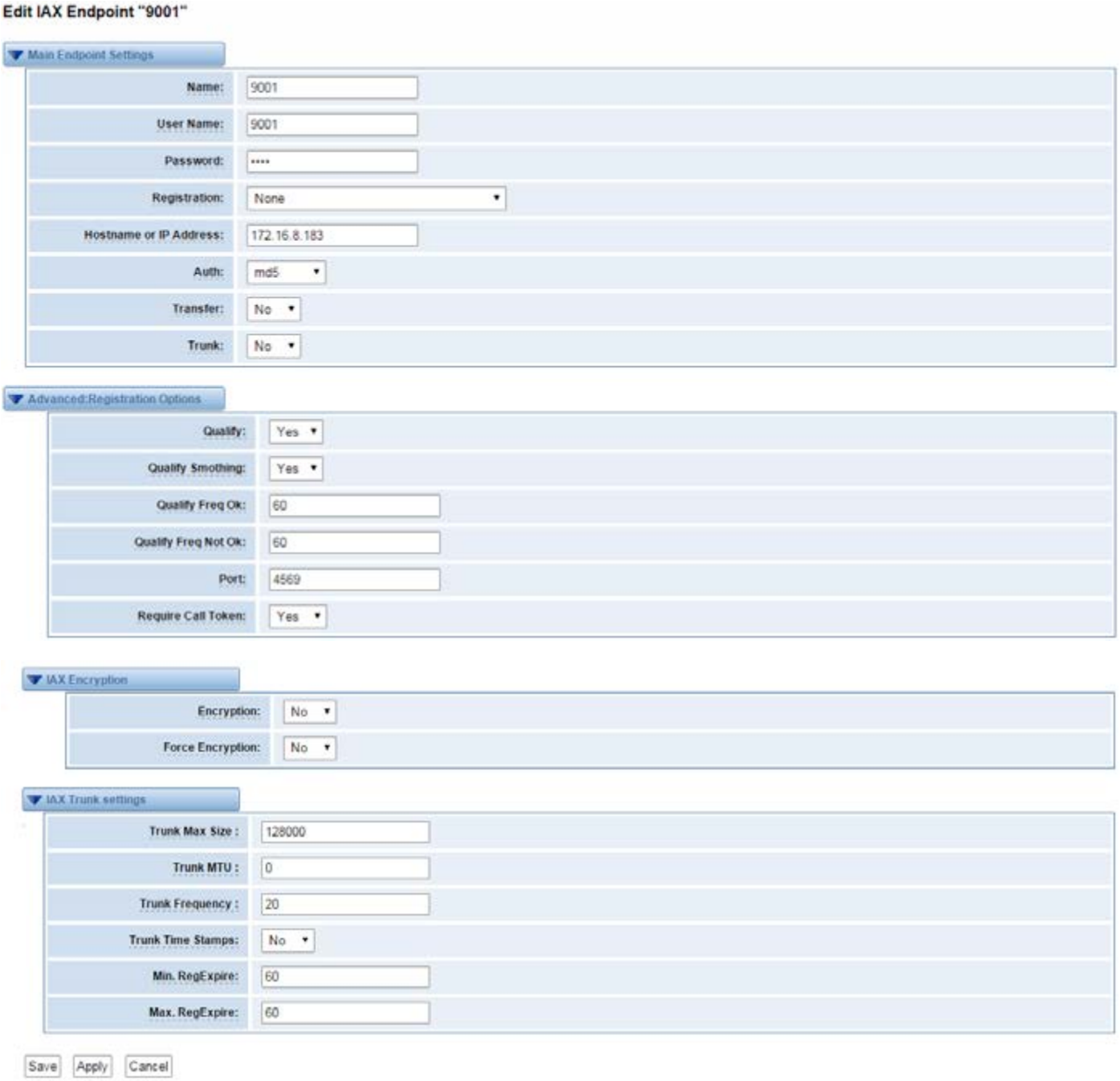
FAX OPTIONS

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 be-lieve 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.

IAX2 ENDPOINT

You can click button as shown above.

Edit IAX Endpoint “9001”



Definition of IAX2 Endpoint

Options	Definition
Name	A name which is able to read by human. And it’s only used for user’s reference.
User name	User name the endpoint will use to authenticate with the gateway.
Password	Password the endpoint will use to authenticate with gateway. Allowed characters.

Registration	Whether this endpoint will register to this gateway or this gateway to the endpoint.
Hostname or IP Address	IP address or hostname of the endpoint or 'dynamic' if the endpoint has a dynamic IP address. This will require registration. Notice: If the input here is hostname and your DNS has changed, you must reboot asterisk.
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.
Port	The port number the gateway will connect to at this endpoint.
Encryption	Enable IAX2 encryption. The default is no.
Force Encryption	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).

ADVANCED SIP SETTINGS

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.
TCP Authentication Timeout	The maximum number of seconds a client has to authenticate. If the client does not authenticate before this timeout expires, the client will be disconnected. (default value is: 30 seconds).
TCP Authentication Limit	The maximum number of unauthenticated sessions that will be allowed to connect at any given time (default is: 50).
Enable Hostname Lookup	Enable DNS SRV lookups on outbound calls Note: the gateway only uses the first host in SRV records Disabling DNS SRV lookups disables the ability to place SIP calls based on domain names to some other SIP users on the Internet specifying a port in a SIP peer definition or when dialing outbound calls with suppress SRV lookups for that peer or call.

ADVANCED NAT SETTINGS

Options	Definition
Local Network	Format:192.168.0.0/255.255.0.0 or 172.16.0.0/12. A list of IP address or IP ranges which are located inside a NATed network. This gateway will replace the internal IP address in SIP and SDP messages with the external IP address when a NAT exists between the gateway and other endpoints.
Local Network List	Local IP address list that you added.
Subscribe Network Change Event	Through the use of the test_stun_monitor module, the gateway has the ability to detect when the perceived external network address has changed. When the stun_ monitor is installed and configured, chan_sip will renew all outbound registrations when the monitor detects any sort of network change has occurred. By default this option is enabled, but only takes effect once res_stun_monitor is configured. If res_stun_monitor is enabled and you wish to not generate all outbound registrations on a network change, use the option below to disable this feature.
Match External Address Locally	Only substitute the exeternaddr or externhost setting if it matches.
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address used for staticly defined hosts. This helps avoid the configuration error of allowing your users to register at the same address as a SIP provide.
Externally Mapped TCP Port	The externally mapped TCP port, when the gateway is behind a static NAT or PAI.
External Address	The external address (and optional TCP port) of the NAT. External address=hostname [:port] specifies a static address[:port] to be used in SIP and SDP messages. Examples: External address=12.34.56.78 External address=12.34.56.78.9900.
External Hostname	The external hostname (and optional TCP port) of the NAT. External Hostname=hostname[:port] is similar to "External address". Examples: External Hostname=foo.dyndns.net
Hostname Refresh Interval	How often to perform a hostname lookup. This can be useful when your NAT device lets you choose the port mapping, but the IP address is dynamic. Beware you might suffer from service disruption when the name server resolution fails.

ADVANCED RTP SETTINGS

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

PARSING AND COMPATIBILITY

Options	Definition
Strict RFC	Check header tags, character conversion in URIs, and multiline headers for strict SIP compatibility (default is yes).
Send Compac	Send compact SIP headers.
SDP Owner	Allows you to change the username filed in the SDP owner string. This filed MUST NOT contain spaces.
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.
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 Registration	Maximum allowed time of incoming registrations and subscriptions (seconds).

Minimum Registration Expiry	Minimum length of registrations/subscriptions (default 60).
Default	Default length of incoming/outgoing registration.
Registration Timeout	How often, in seconds, to retry registration calls. Default 20 seconds.
Number of Registration	Number of registrations attempts before we give up.0=continue forever, hammering the other server until it accepts the registration. Default is 0 tries, continue forever.

SECURITY

Options	Definition
Match Auth	If available, match user entry using the 'username' field from the authentication line instead of the 'from' field.
Realm	Realm for digest authentication. Realms MUST be globally unique according to RFC 3261. Set this to your host name or domain name.
Use Domain as Realm	Use the domain from the SIP Domains setting as the realm. In this case, the realm will be based on the request 'to' or 'from' header and should match one of the domain. Otherwise, the configured 'realm' value will be used.
Always Auth Reject	When an incoming INVITE or REGISTER is to be rejected, for any reason, always reject with an identical response equivalent to valid username and invalid password/hash instead of letting the requester know whether there was a matching user or peer for their request. This reduces the ability of an attacker to scan for valid SIP usernames. This option is set to 'yes' by default.
Authenticate Options Requests	Enabling this option will authenticate OPTIONS requests just like INVITE requests are. By default this option is disabled.
Allow Guest Calling	Allow or reject guest calls (default is yes, to allow). If your gateway is connected to the Internet and you allow guest calls, you want to check which services you offer everyone out there, by enabling them in the default context.

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.

CODEC SETTINGS

Select codecs from the list below.

Advanced IAX2 Settings

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

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

Instruction of Music on Hold

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

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.

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 notices a significant change in delay that continue over a few frames, it will resync, assuming that the change in delay was caused by a timestamping mix-up. The threshold for noticing a change in delay is measured as twice the measured jitter plus this resync threshold.
Max Jitter Interps	The maximum number of interpolations frames the jitter buffer should return in a row. Since some clients do not send CNG/DTX frames to indicate silence, the jitter buffer will assume silence has begun after returning these many interpolations. This 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.

Instruction of Misc Settings

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.

Instruction of Quality of Service

Options	Definition
Tos	Type of service
Cos	Class of service

ADVANCED FAX SETTINGS

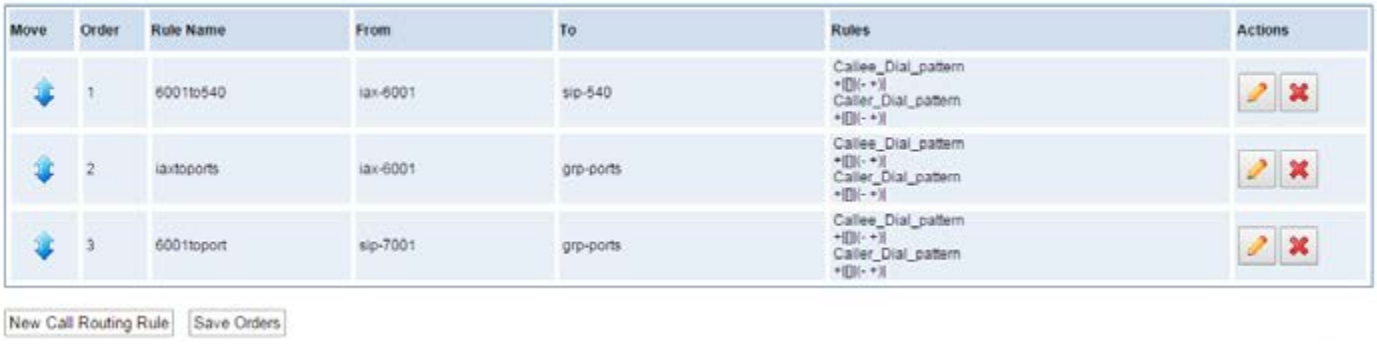
Options	Definition
Udptl Start	DPTL start configure addresses.
Udptl End	DPTL end configure addresses.
Udptl Checksums	Whether to enable or disable UDP checksums on UDPTL traffic.

Udptl FEC Entries	The number of error correction entries in a UDPTL packet.
Udptl FEC Span	The span over which parity is calculated for FEC in a UDPTL packet.
Use Even Ports	Some VoIP providers will only accept an offer with an even-numbered UDPTL port. Set this option so that Asterisk will only attempt to use even-numbered ports when negotiating T.38. Default is no.
Maximum Transmission Rate	Maximum Transmission Rate.
Minimum Transmission Rate	Minimum Transmission Rate.
Send Progress/Status events to manager session	Manager events with 'call' class permissions will receive events indicating the steps to initiate a fax session. Fax completion events are always sent to manager sessions with 'call' class permissions, regardless of the value of this option.
Modem Capabilities	Set this value to modify the default modem options. Defasult:v17,v27,v29.
ECM	Enable/disable T.30 ECM(error correction mode) by default.

ROUTING

The gateway offers flexible and friendly routing settings. It supports up to 512 routing rules and about 100 pairs of calleeID/callerID manipulations can be set in a rule. It supports DID function (The usage of DID function: How to use DID function with NXGW-XET1 Gateway). The gateway support trunk group and trunk priority management.

Call Routing Rule



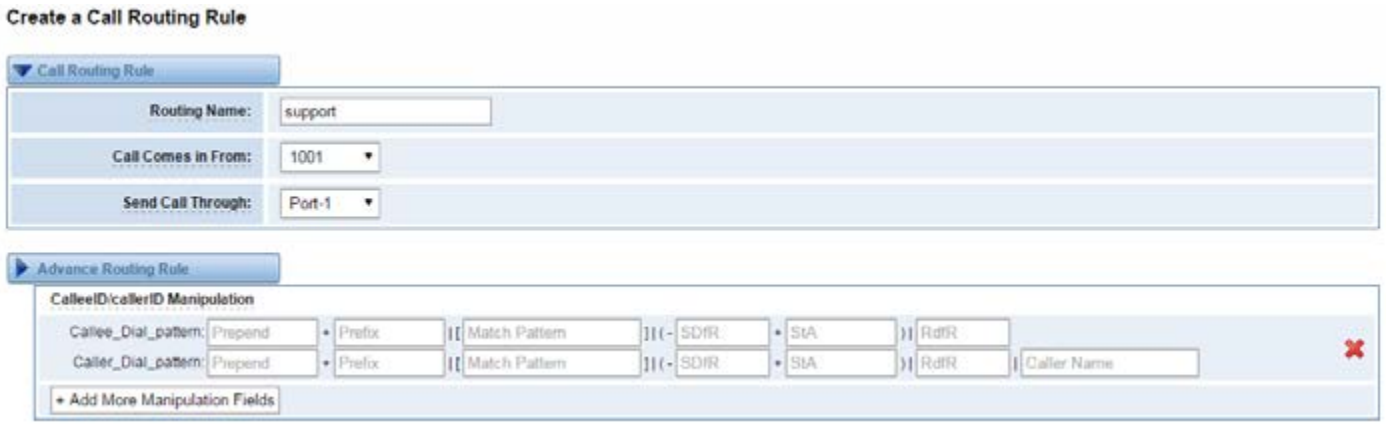
To set up new routing rule click on New Call Routing Rule , and after setting routing rules, move rules' order by pulling up and down, click button to edit the routing and to delete it. Finally, click the Save Orders button to save what you set. Rules will show current routing rules. Otherwise, you can set up unlimited routing rules.

There is an example for routing rules number conversion, it transforms calling and called number at the same time. Suppose you want eleven numbers that begin with the 159 prefix to call the eleven numbers with the 136 prefix. Calling transform delete the three numbers from left, then write number 086 as the prefix, and delete the last four numbers. 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 numbers to 88.

Example for routing rules number conversion

processing rules	prepend	prefix	Match pattern	SdfR	StA	RdfR	Caller Name
Calling Transformation	086	159	xxxxxxxx	4	0755		China telecom
Called Transformation	086	136	xxxxxxxx	2	88		N/A

Example Setup of Routing Rule



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.

Definition of Routing Options

Options	Definition
Routing Name	The name of this route. Should be used to describe what types of calls. 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.

Description of Advanced Routing Rule

Options	Definition
Dial Patterns that will use this Route	A Dial Pattern is a unique set of digits that will select this route and send the call to the designated trunks. If a dialed pattern matches this route, no subsequent routes will be tried. If Time Groups are enabled, subsequent routes will be checked for matches outside of the designated time(s). Rules: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (example: 1,2,3,7,8,9) . wildcard, matches one or more dialed digits Prepend: Digits to prepend to a successful match. If the dialed number matches the patterns specified by the subsequent columns, then this will be prepended before sending to the trunks. 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 number of digits to be deleted from the right end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted. StA (Suffix to Add): Designated information to be added to the right end of the current number. RDfR (Reserved Digits from Right): The number of digits to be reserved from the right end of the number. If the value of this item under the length of the current number, the whole number will be reserved. Caller Name: What caller name would you like to set before sending this call to the endpoint. Sets Caller*ID data on the channel: SIP_FROM(name),SIP_FROM(number) : defalut:Sip From and Number eg: When selecting SIP From, Name is Peter and Number is 402. The From mode is: \"Peter\"<sip:402@172.16.6.239;transport=UDP>;tag=bd481672 SIP_TO(name),SIP_TO(number) : defalut: EXTEN eg: When selecting SIP To, Name is Jason and Number is 401. To mode is: \"Jason\"<sip:401@172.16.6.239;transport=UDP> None: Set Caller*ID number which is to be send on the channel from PBX(manipulated if it sets).

Forward Number	**What destination number will you dial? This is very useful when you have a transfer call.**
Failover Call Through Number	**The gateway will attempt to send the call out each of these in the order you specify.**

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

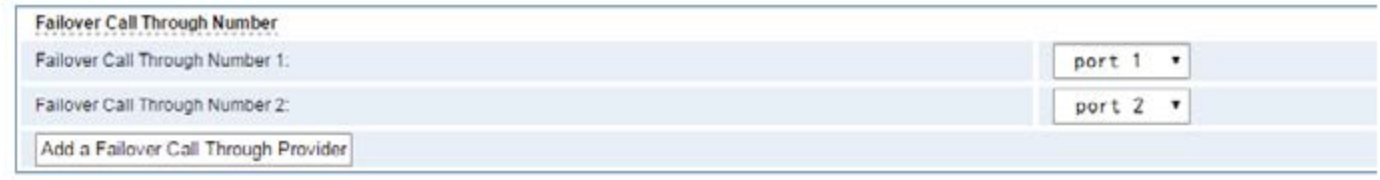
Time Patterns that will use this Route

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.

Forward Number

You can configure forward number when you have a transfer call. You can also set your custom context as you like before sending the call to the endpoint.

Failover Call Through Number

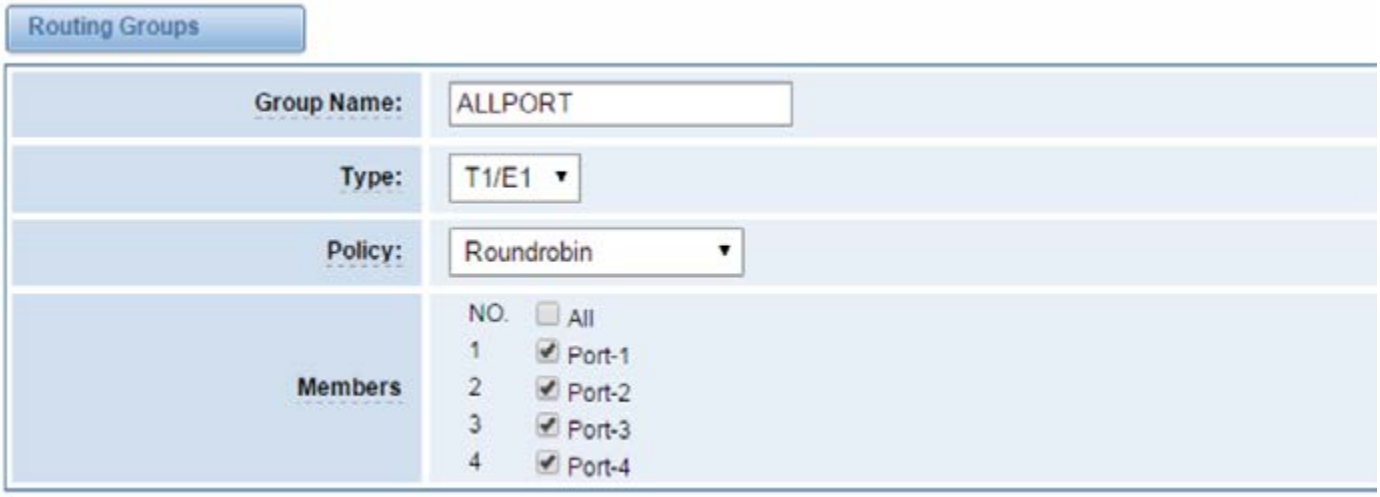


You can add one or more “Failover Call Through Numbers”.

GROUPS

This gateway allows you to combine many Ports or SIP to groups. Then if you want to make a call, it will find an available port automatically.

Establish Group

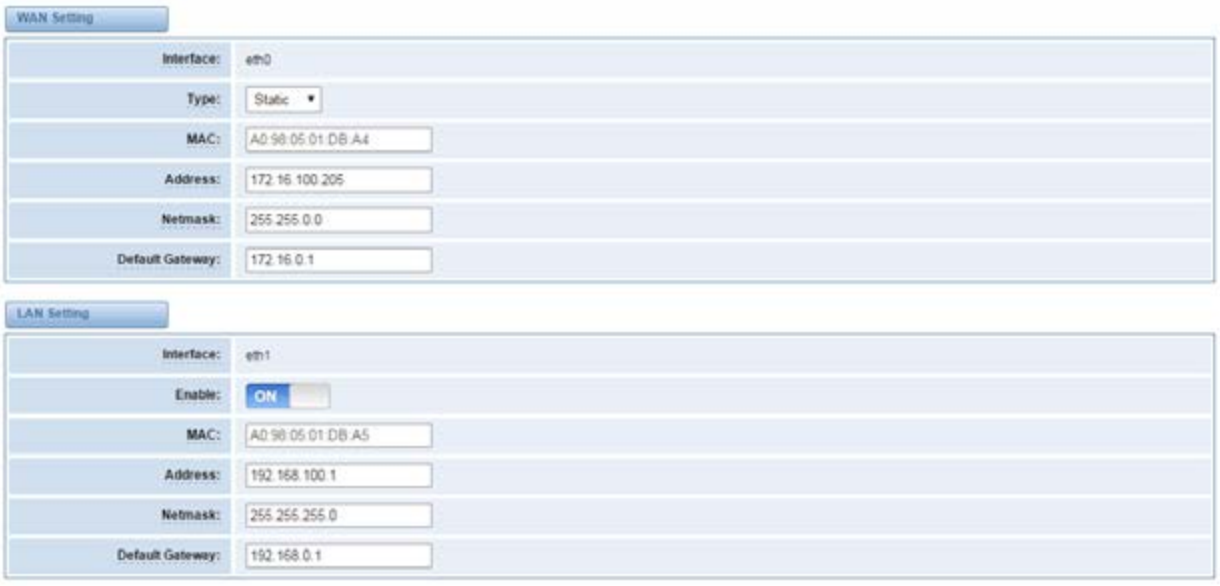


NETWORK

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

Network Settings

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

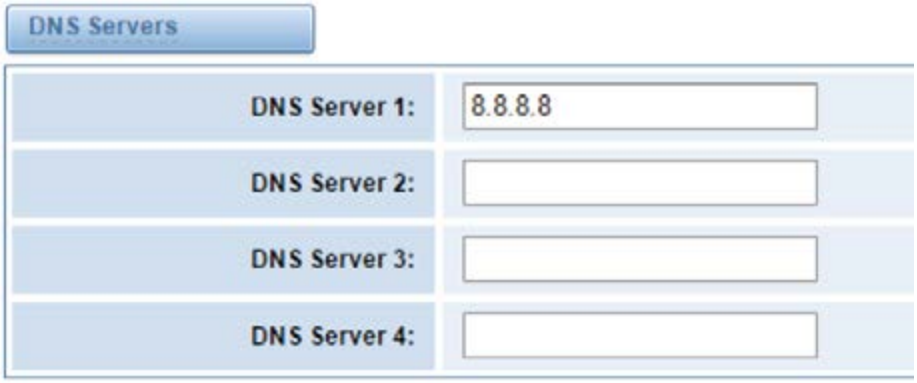


Definition of WAN/LAN Settings

Interface	**The name of network interface.**
Type	**The method to get IP.** **Static: manually set up your gateway IP.** **DHCP: automatically get IP from your local LAN.**
MAC	**Physical address of your network interface.**
Address	**The IP address of your gateway.**
Network	**The subnet mask of your gateway.**
Default Gateway	**Default getaway IP address.**

DNS SERVERS

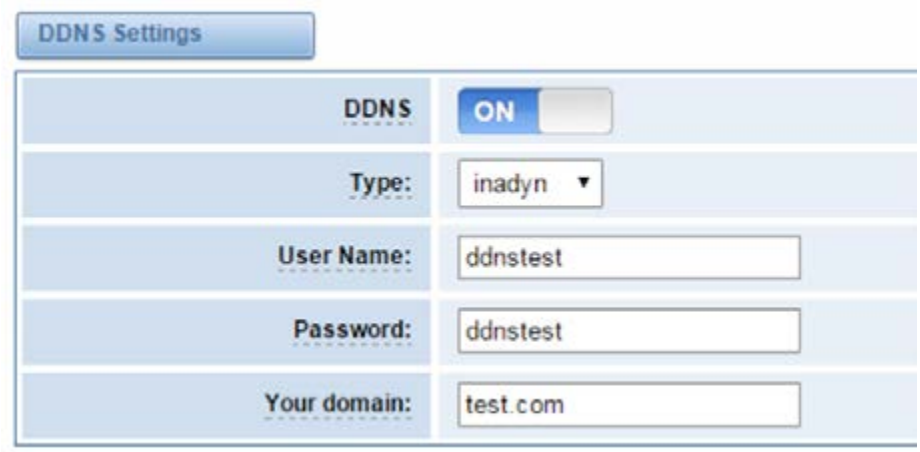
A list of DNS IP address. This info is from your local network service provider. Note that you must restart the gateway if you changed the DNS server.



DDNS SETTINGS

You can set a static domain.

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



Definition of DDNS Settings

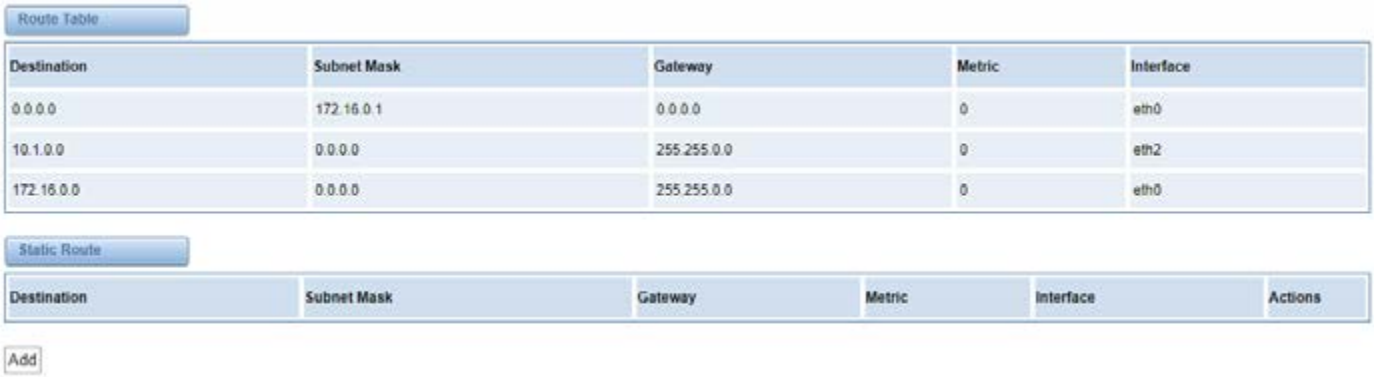
Options	Definition
DDNS	Enable/Disable DDNS (dynamic domain name server).
Type	Set the type of DDNS server.
Username	Your DDNS account's login name.
Password	Your DDNS account's password.
Your domain	The domain to which your web server will belong.

TOOLKIT

Used to check network connectivity. Support Ping command on web GUI.

Network Connectivity Checking

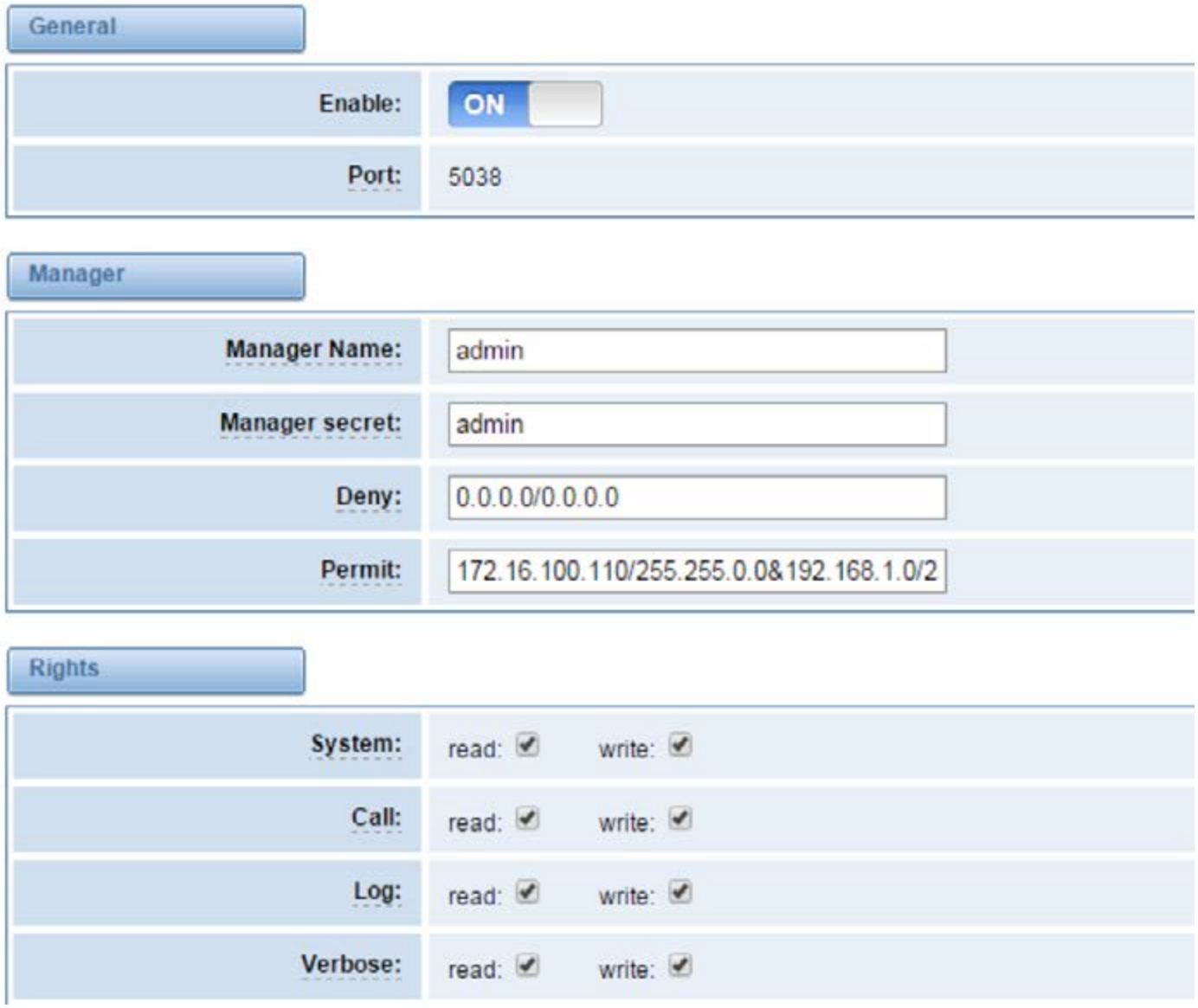
Static Route Settings



ADVANCED

Asterisk API

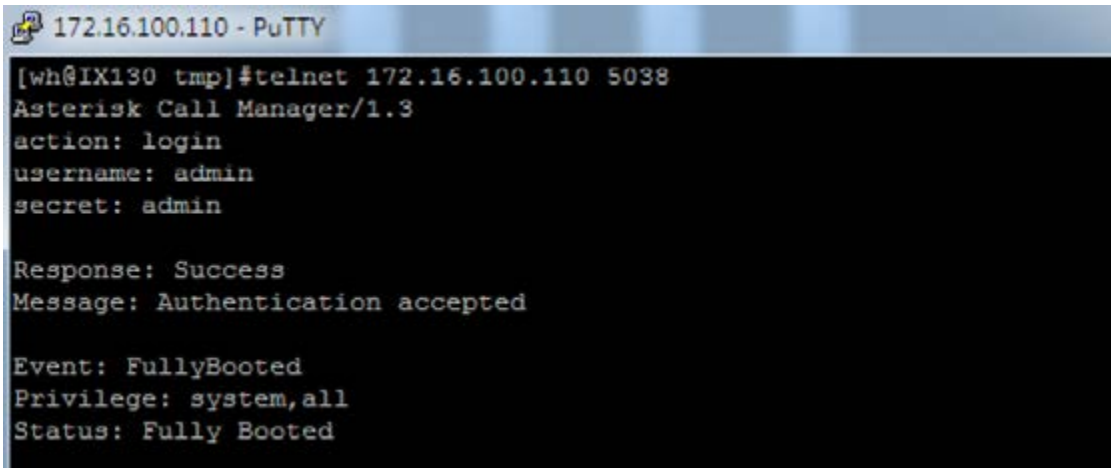
When you click "Enable" as shown below, this page is available.



Definition of Asterisk API

Options	Definition
Port	Network port number.
Manager Name	Name of the manager without space.
Manager secret	Password for the manager. Characters: Allowed characters “-_+.<>&0-9a-zA-Z”. Length:4-32 characters.
Deny	If you want to deny many hosts or networks, use char & as separator. Example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
Permit	If you want to permit many hosts or network, use char & as separator. Example: 0.0.0.0/0.0.0.0 or 192.168.1.0/255.255.255.0&10.0.0.0/255.0.0.0.
System	General information about the system and ability to run system management commands, such as Shutdown, Restart, and Reload.
Call	Information about channels and ability to set information in a running channel.
Log	Logging information. Read-only. (Defined but not yet used.)
Verbose	Verbose information. Read-only. (Defined but not yet used.)
Command	Permission to run CLI commands. Write-only.
Agent	Information about queues and agents and ability to add queue members to a queue.
User	Permission to send and receive UserEvent.
Config	Ability to read and write configuration files.
DTMF	Receive DTMF events. Read-only.
Reporting	Ability to get information about the system.
Dialplan	Receive NewExten and Var Set events. Read-only.
Originate	Permission to originate new calls. Write-only.
All	Select all or deselect all.

Once you configure as shown above, the host 172.16.100.110/255.255.0.0 is allowed to access the gateway API. Please refer to the below image to access the gateway API by putty. 172.16.100.110 is the gateway's IP, and 5038 is its API port.



Asterisk CLI

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

Definition of Asterisk CLI

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

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

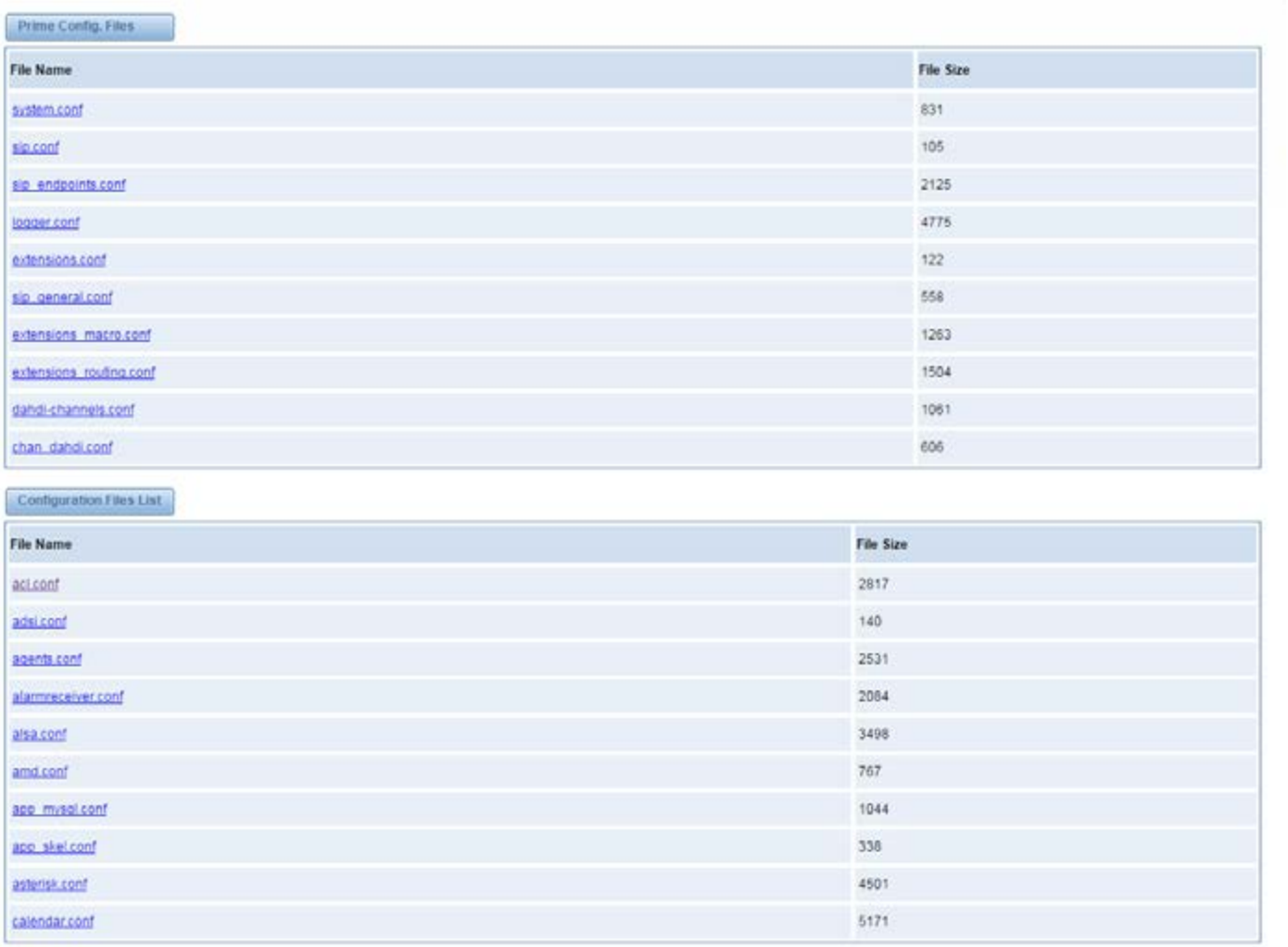
Definition of Lock/unlock channels

Options	Definition
Signaling	Current signaling in use.

Operation	**The advanced operations for lock and unlock channels.**
Channel	**The channel to be lock or unlock.**

ASTERISK FILE EDITOR

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



Click “New Configuration File” to create a new configuration file. After editing or creating, please reload Asterisk.

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 during the next power on or restart of the system.

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

Preparation

The following should be prepared before auto provisioning being applied.

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

Configuring gateway

Usually, the feature is disabled by default. To activate the auto provisioning function, please follow the procedures as below.

Step 1 ADVANCED-> Auto Provision interface

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

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

Definition of Auto Provision

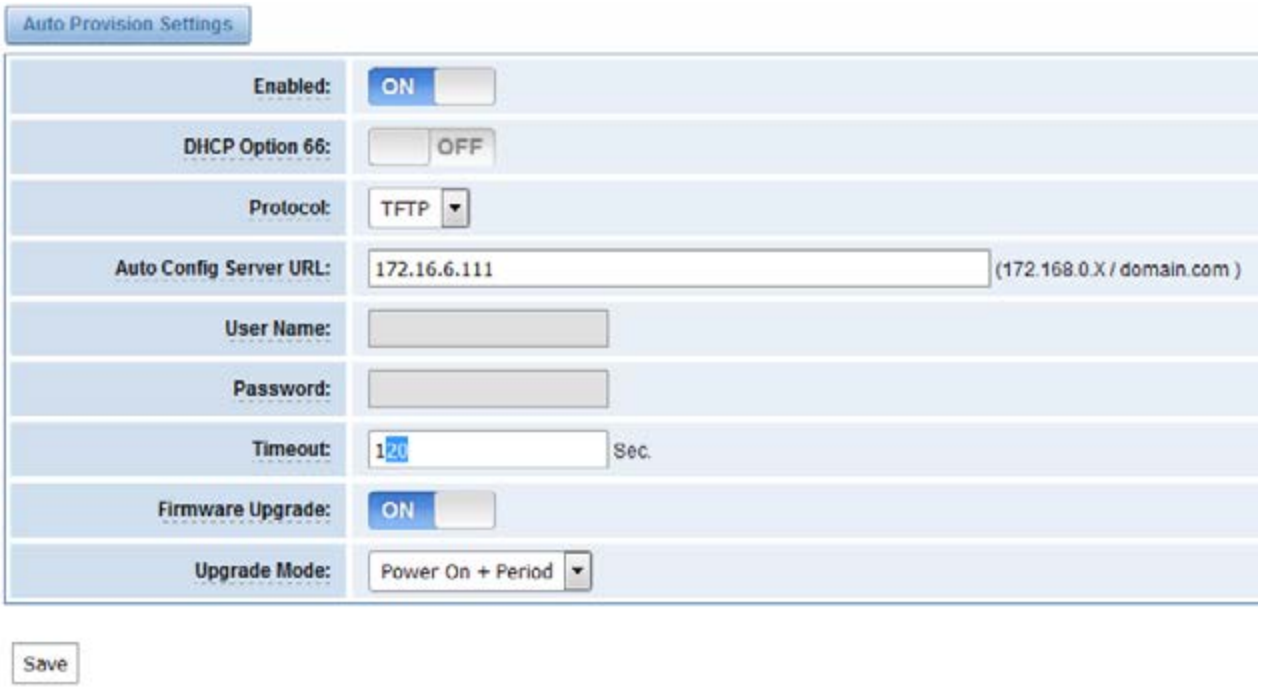
Options	Definition
Enabled	Whether to enable or disable Auto Provision.
DHCP Option 66	Get ACS server address from Option 66 via DHCP.
Protocol	Set protocol of connection.
Auto Config Server URL	The config server domain or IP address.
User Name	The account of downloading from ACS.

Password	The password of downloading from ACS.
Timeout	The max limit time for downloading firmware.
Firmware Upgrade	Enable/disable the mode of downloading firmware.
Upgrade Mode	Select upgrade time. Power: start upgrade configuration when Power on. Power + Period: Set the frequency of checking the latest configuration when gateway running.

Definition of system notice

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

Auto Provision interface



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:

Definition of ACS files

Options	Definition
DGW100x-current.bin	The firmware image.
common.conf	The wildcard configuration file for the whole gateway.
defconfig.tar.gz	The default(factory) configuration file.
EPC-{mac}.conf	The private configuration file for the specified gateway. Naming rules: "EPC-" + "mac" +".conf". The naming prefix of "EPC-" stands for the private configuration file, "mac" is the physical address of network interface card but removed semicolon and ".conf" is the suffix. For example, the EPC-a0980501dbca.conf, 'a0980501dbca' is the MAC address (A0:98:05:01:DB:CA).

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

(1). Common.conf

[firmware]

FW_NAME=DGW100x-current.bin //Firmware image name

FW_MD5=b3603f3c3b5e7eb6326498640f151c79 //The md5 of firmware image

FW_VERSION=1.1.2 //Firmware version

[configs]

CONFIG_NAME=defconfig.tar.gz // default configuration file(compressed)

CONFIG_MD5KEY=2cd2dfbe52482405350816e3698cb530 // the md5 of default configuration file

(2).EPC-{mac}.conf

[dns]

DNS_SERVER1=8.8.8.8

DNS_SERVER2=8.8.4.4

DNS_SERVER3=

DNS_SERVER4=

[ntp]

NTP_SERVER1= 0.cn.pool.ntp.org

NTP_SERVER2= time.nist.gov

NTP_SERVER3= time.windows.com

[eth0]

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

The overview of defconfig.tar.gz

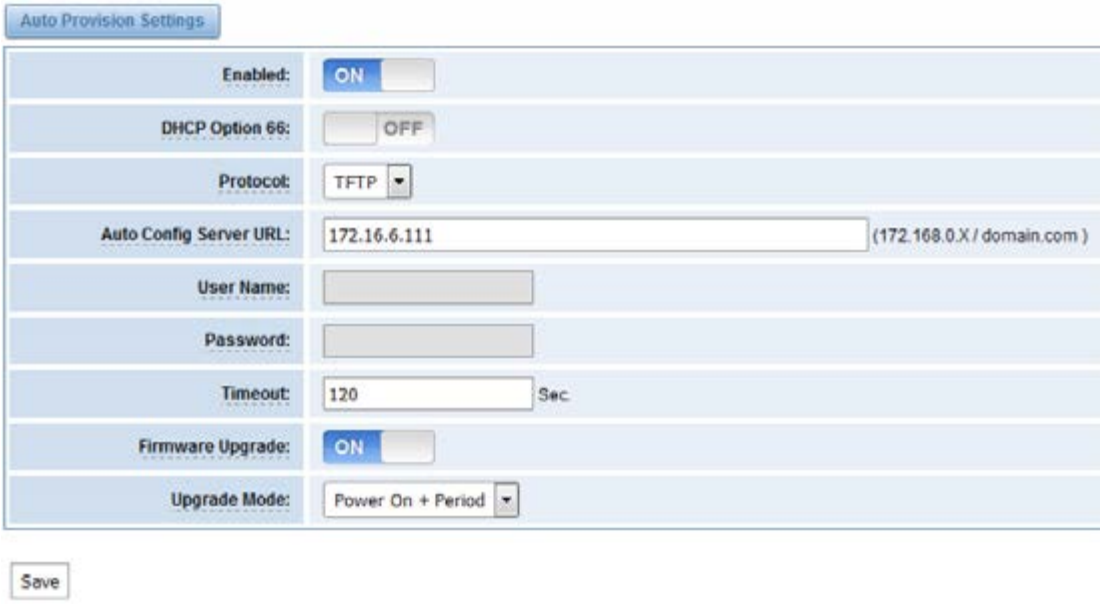
```
[root@dgw100x /defconfig]#ls
config.info    group-         passwd         resolv.conf    sysconfig
fstab          hosts          passwd-        shadow         tmp
group          nsswitch.conf  profile        shadow-
[root@dgw100x /defconfig]#ls sysconfig/
NTP             hostname        nsswitch.conf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

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, and the message will be displayed in the system notice (LOGS->System Notice).

Auto provisioning will not take effect immediately but in the next time system is powered up or restarted. 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 7-4-3 Auto provision settings



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

Figure 7-4-4 Check interval setting

3. Configure the ACS (Generate the md5 of firmware and defconfig.tar.gz)

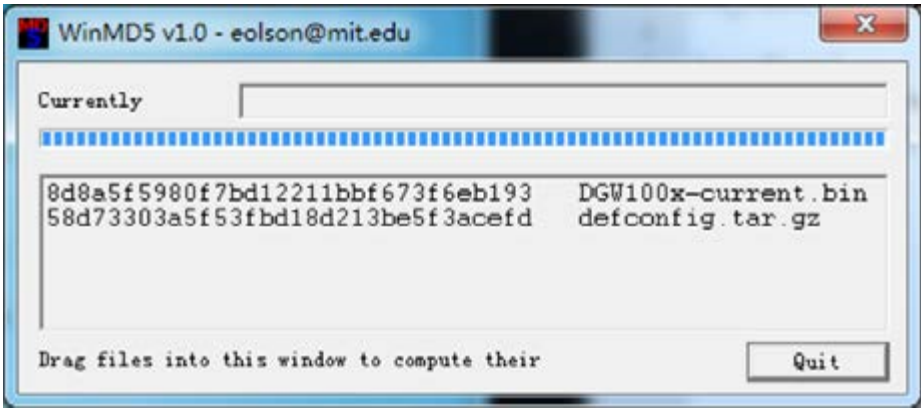
Copy the firmware, defconfig.tar.gz, common.conf and EPC-{mac}.conf to the working directory of TFTP server.

The working directory of TFTP server

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.

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

Generate the md5 of firmware and configuration



Common.conf

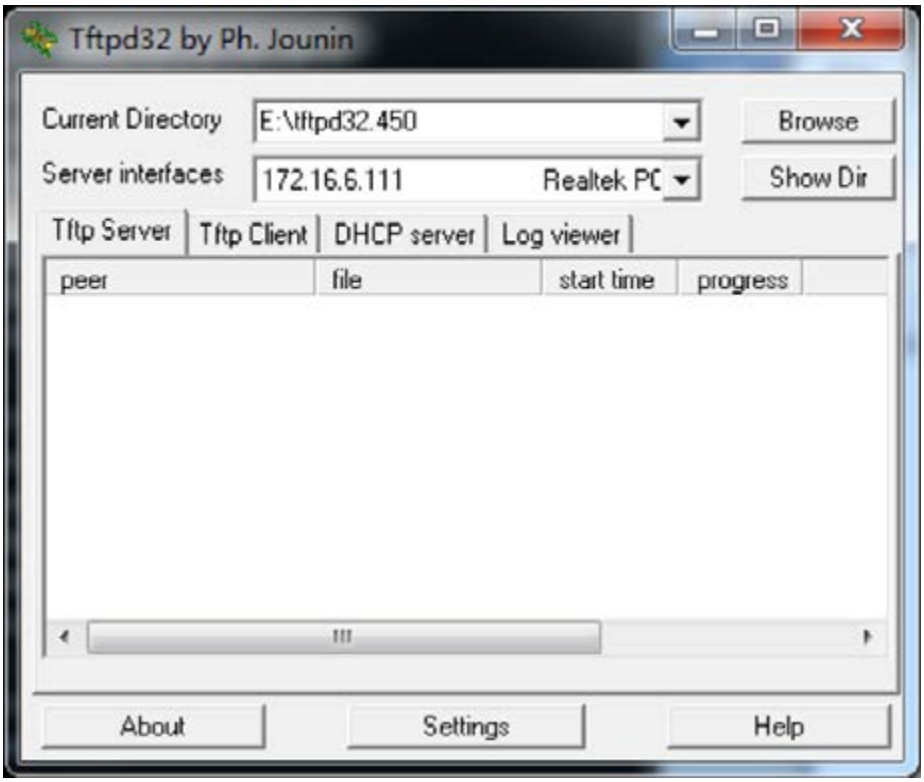
```
[root@localhost build]# cat common.conf
[firmware]
FW_NAME=DGW100x-current.bin
FW_MD5=8d8a5f5980f7bd12211bbf673f6eb193
FW_VERSION=1.1.2

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

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]#
```

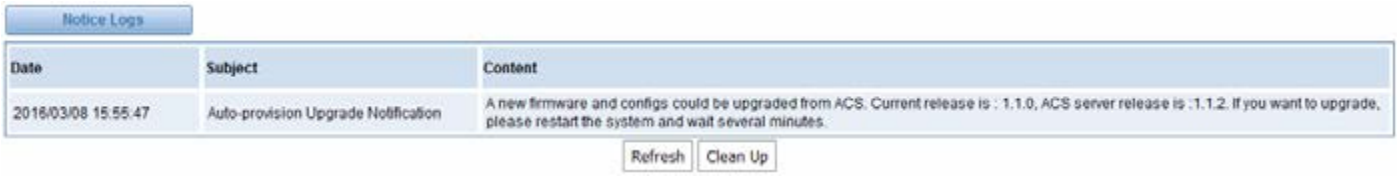
5. Start TFTP service. Tftpd32.exe is a useful TFTP tools in windows7, then make sure TFTP server is select.

A demo TFTP server

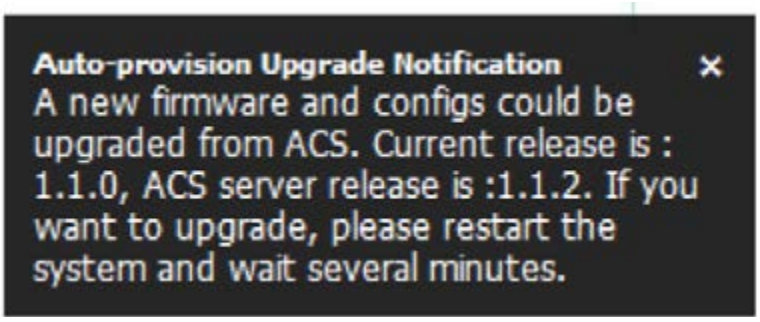


6. The system will receive an auto provision message in web GUI.

System notice logs

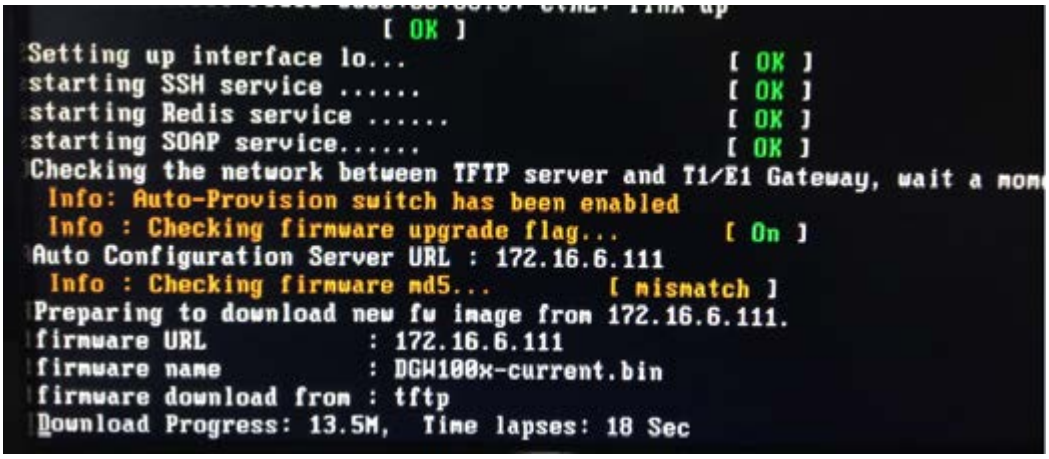


Auto provision upgrade notification

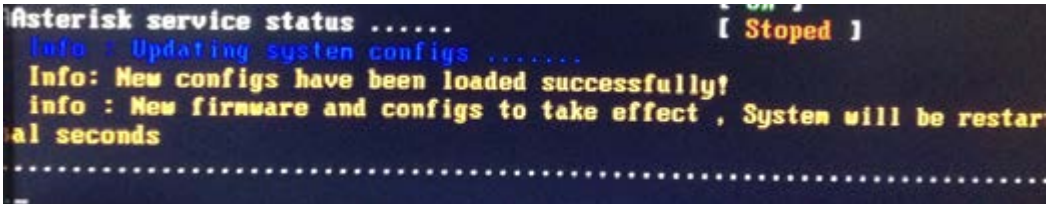


7. Restart the system. It will take about 3 minutes to download, upgrade Firmware and update configurations.

Downloading the firmware and configs



Applying the firmware and configs



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.

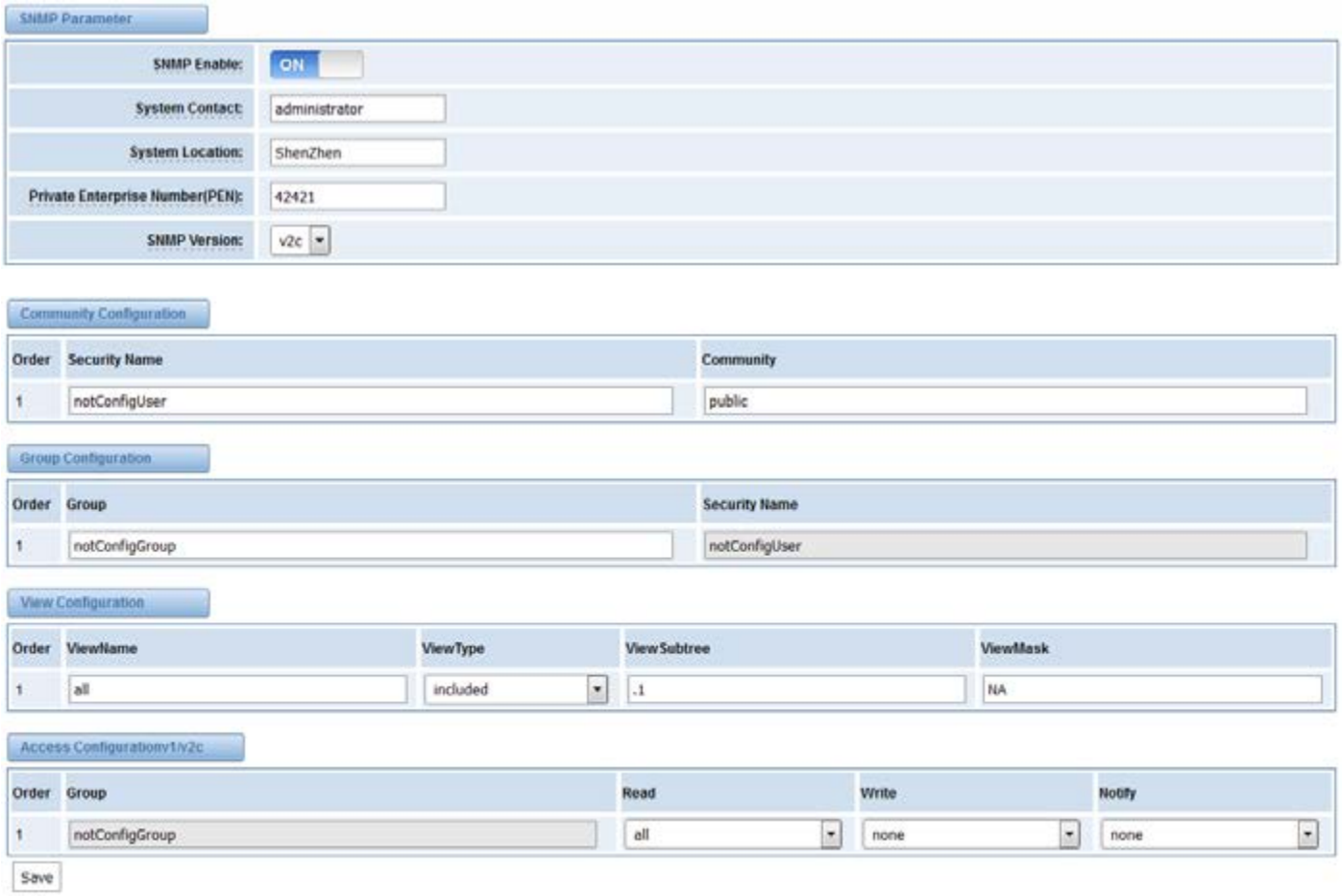
Since the inception SNMP, it embraces three versions: v1, v2c and v3. V1 and v2c are the most implemented version of SNMP; v3 is target at the high security when compare to its older versions. The gateway support private SNMP MIBs (private enterprise number) to access.

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

Activating SNMP

Usually, the feature is disabled by default. To activate the SNMP feature. Follow the image below to activate. 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.



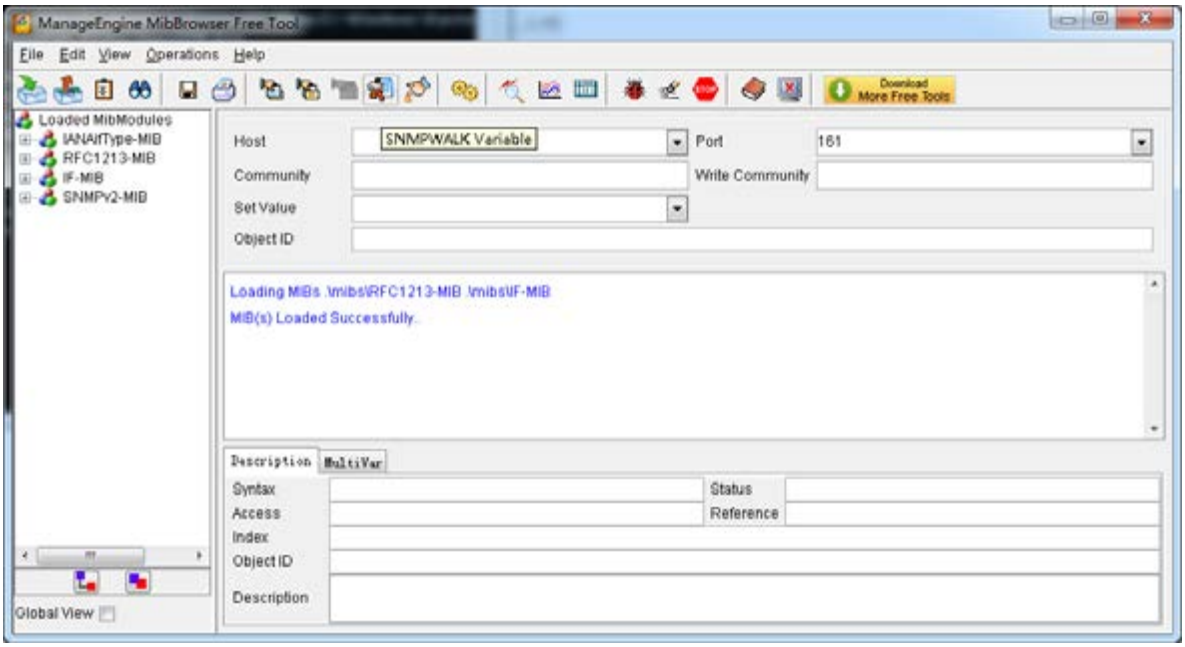
Note: Do not forget to click 'Save' after configuration, The SNMP feature is activated immediately.

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.

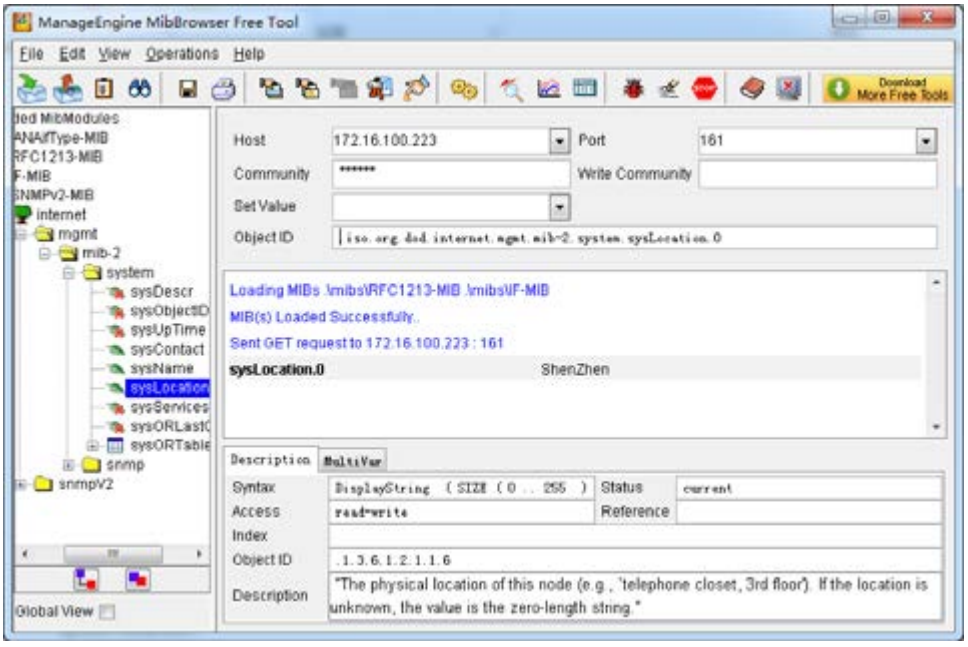
1. Get SNMP parameters via SNMP MIB browser. The Manage Engine MIB browser is installed perfectly. Below you will see the main interface of Manage Engine MIB browser.

Manage Engine MIB browser



2. 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.

Get system location

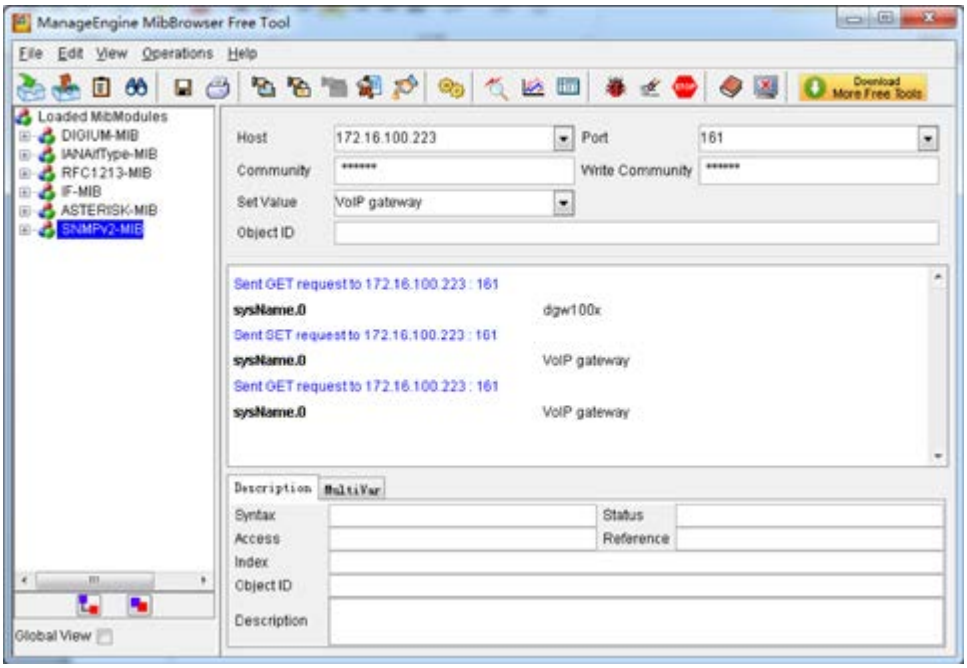


3. After the rest field has been filled, then verify it. Click Operations->GET to get the value of system location and it returns the value which we just set.

4. 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.

Set system name

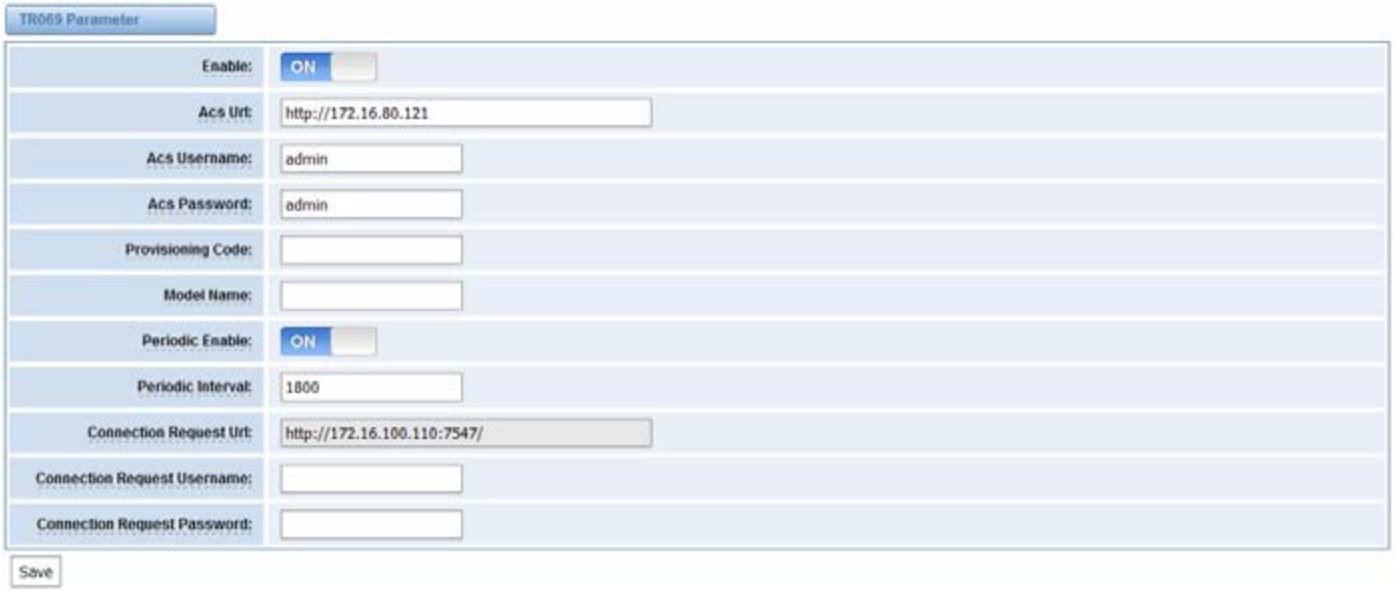


TR069

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. Below is TR069 configuration interface and its definition.

Options	Definition
Acs Url	Specify the URL of the ACS
Acs Username	Specify the user name to be used by the device to authenticate with the ACS.
Acs Password	Specify the password to be used by the device to authenticate with the file server

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



NETWORK CAPTURE

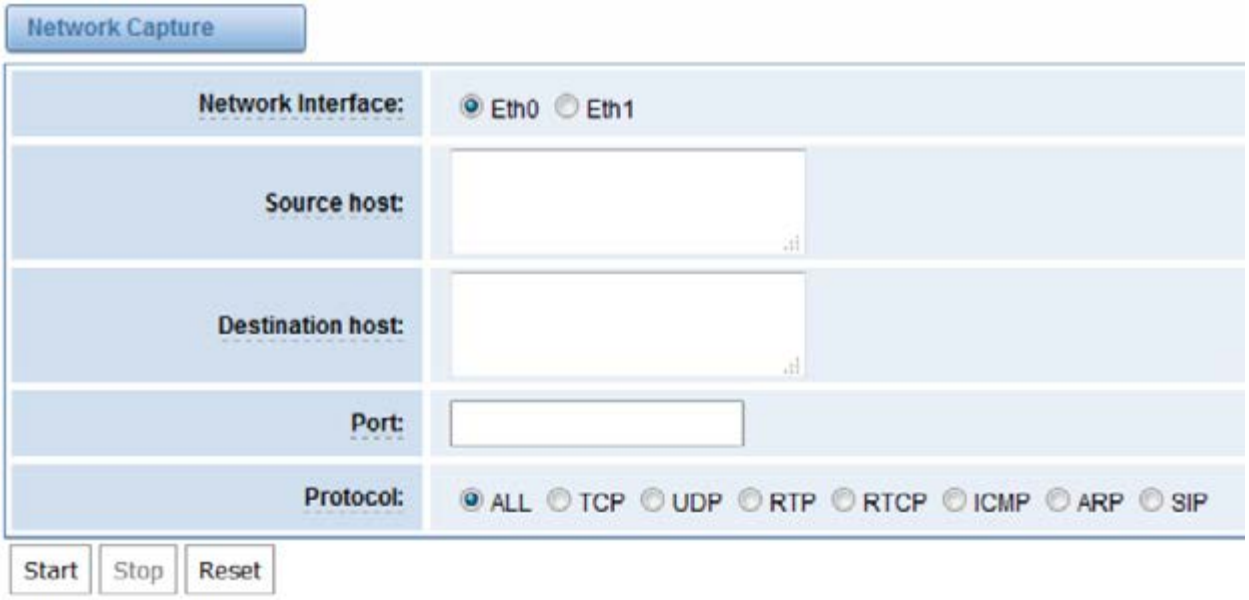
The gateway has been supplied a network packet capture in the web for easy analysis, capturing and monitoring of the gateway's network status, RTP flows, protocol analysis and so on.

Definition of Network capture

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

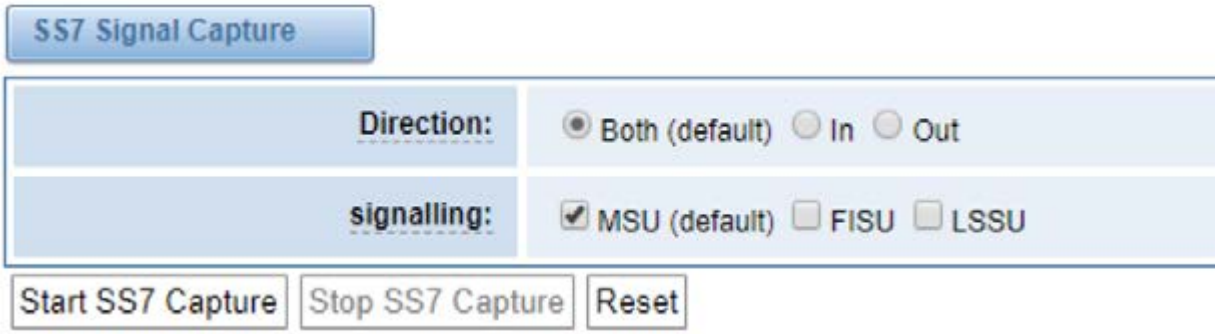
The interface is in ADVANCED->Network Capture.

Network capture interface



Moreover, user can capture SS7 signal and record port.

Signal Capture interface



Port Recording interface

CLOUD

NXGW-XET1 gateways support Cloud Management.

Connecting to the Cloud

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

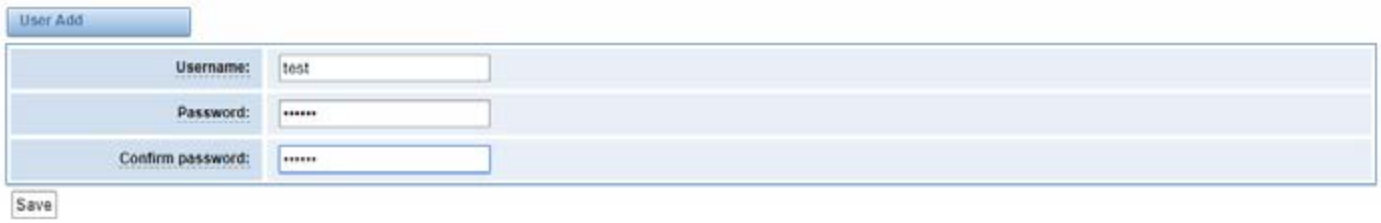
Definition of Cloud Management

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

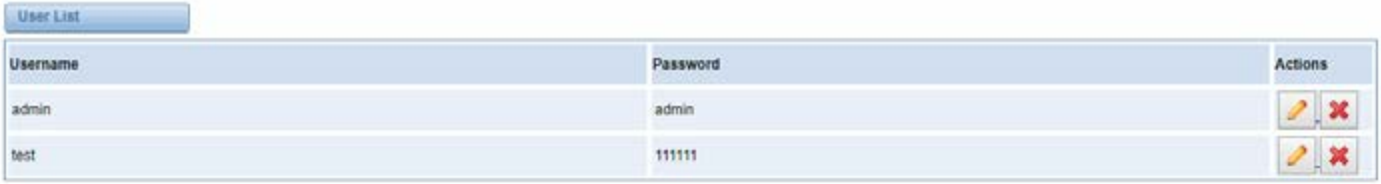
USER

The NXGW-XET1 Gateway allows you to create users and modify the permissions of users accessing the web interface.

Add User



User List

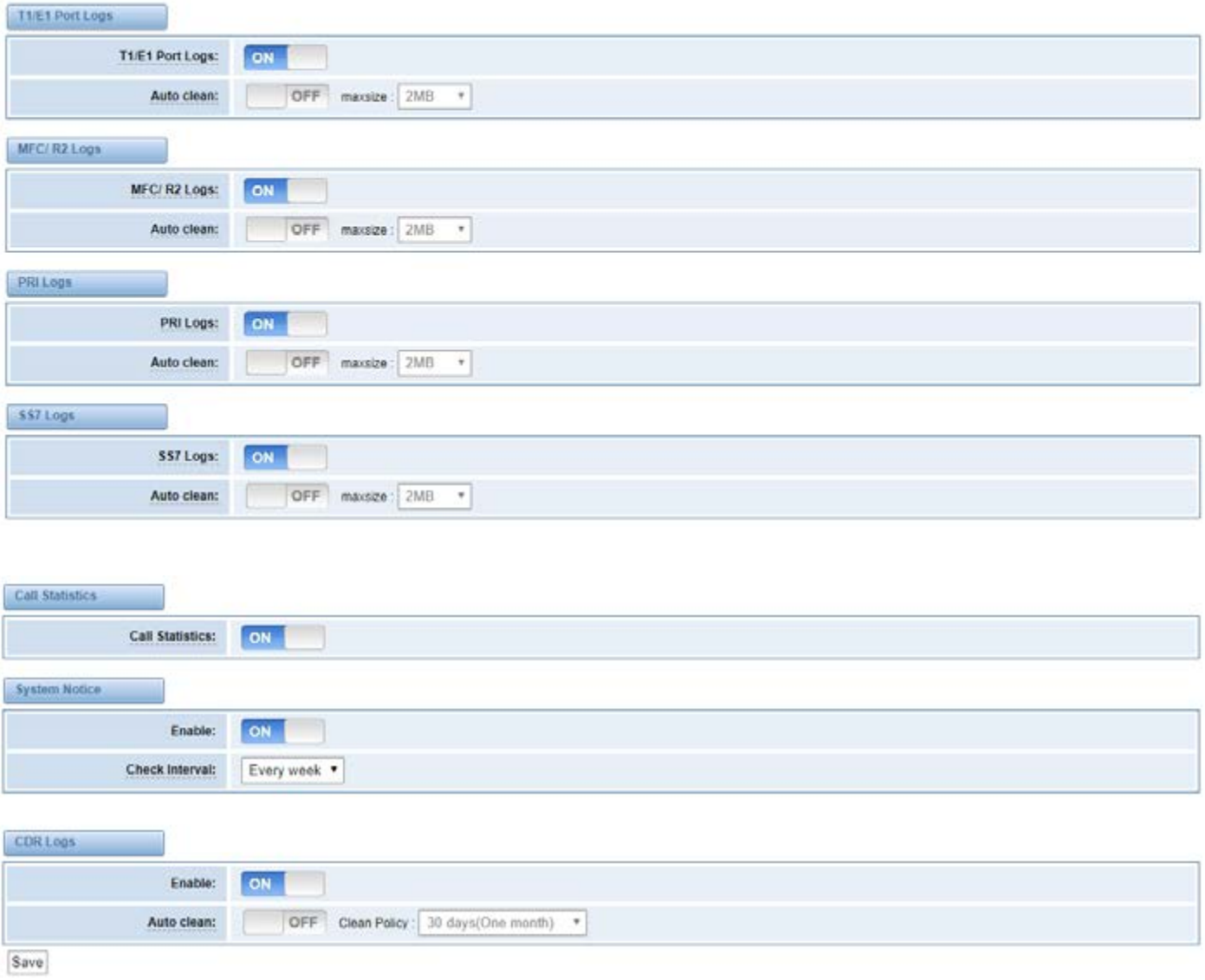


User Permissions

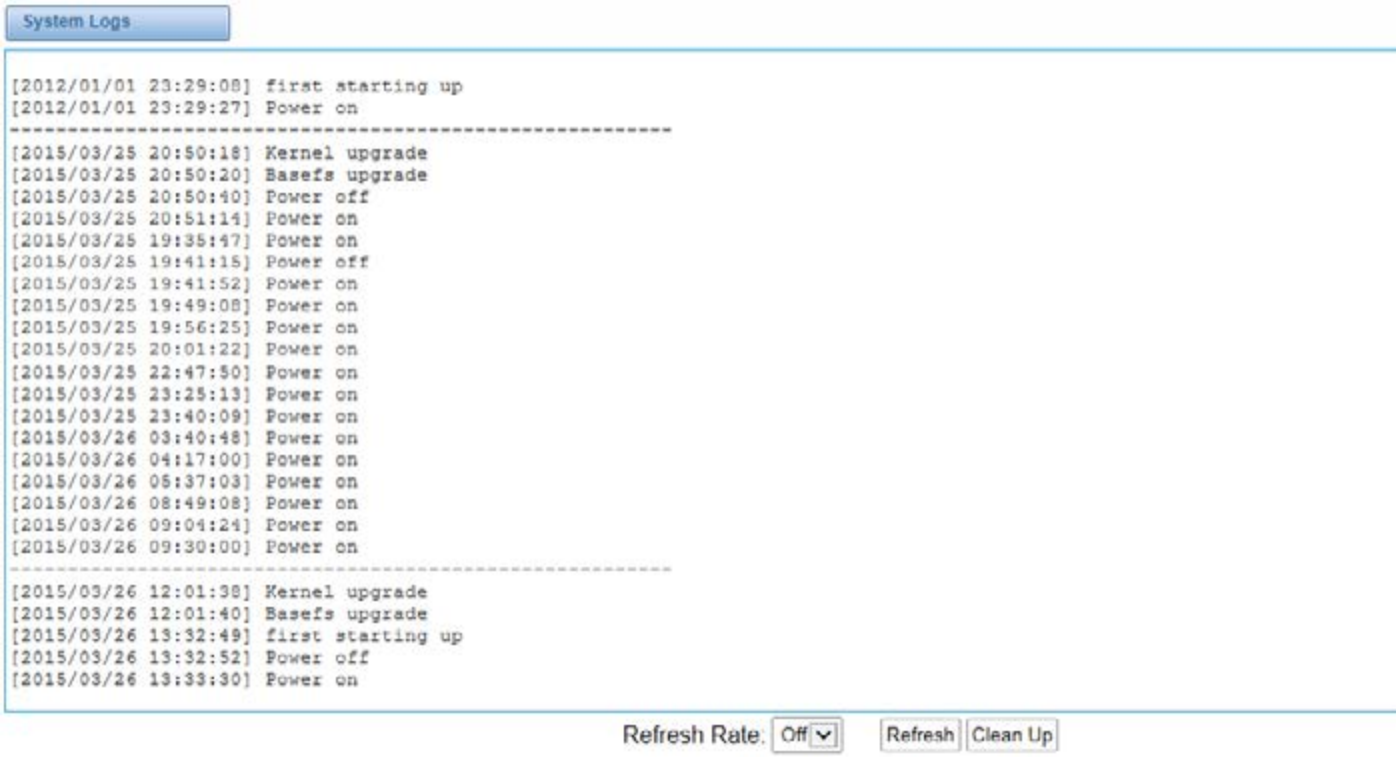
LOGS

Log Settings

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



System Logs Output



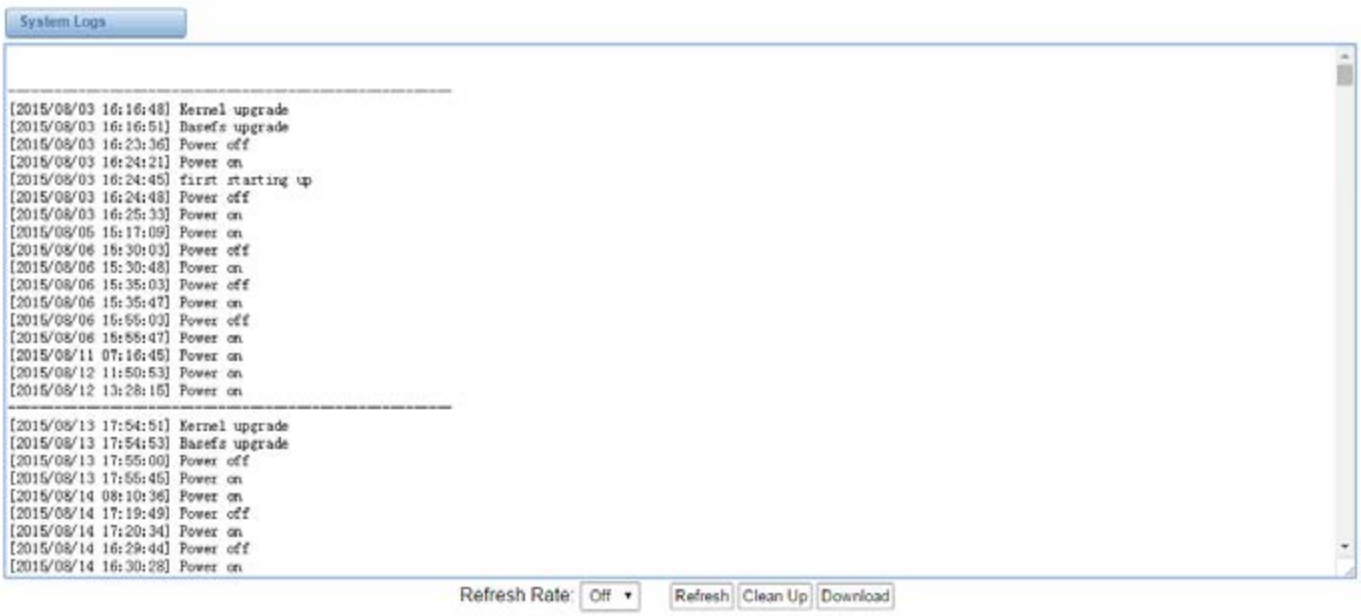
Definition of Logs

Options	Definition
Auto clean (System Logs)	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. Switch off: logs will remain, and the file size will increase gradually. default on, default size=1MB.
Verbose	Asterisk console verbose message switch.
Notice	Asterisk console notice message switch.
Warning	Asterisk console warning message switch.
Debug	Asterisk console debug message switch.
Error	Asterisk console error message switch.
DTMF	Asterisk console DTMF info switch.
Auto clean: (asterisk logs)	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. 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.
Auto clean: (SIP logs)	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. Switch off: logs will remain, and the file size will increase gradually. default on, default size=2 MB.
IAX2 Logs	Whether enable or disable IAX log.
Auto clean	Switch on: when the size of log file reaches the max size, The system will cut a half of the file. New logs will be retained. Switch off: logs will remain, and the file size will increase gradually. default on, default size=2 MB.
MFC/ R2 Logs	Whether enable or disable MFC/ R2 Logs log.
Auto clean	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. Switch off: logs will remain, and the file size will increase gradually. default on, default size=2 MB.
PRI Logs	PRI port logs. You can choose one or more ports. If you choose “All”, the “PRI” page will show you the logs about all the ports.

Auto clean (PRI logs)	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. Switch off: logs will remain, and the file size will increase gradually. default on, default size=2 MB.
.SS7 Logs	Whether enable or disable SS7 log.
Auto clean	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. 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.

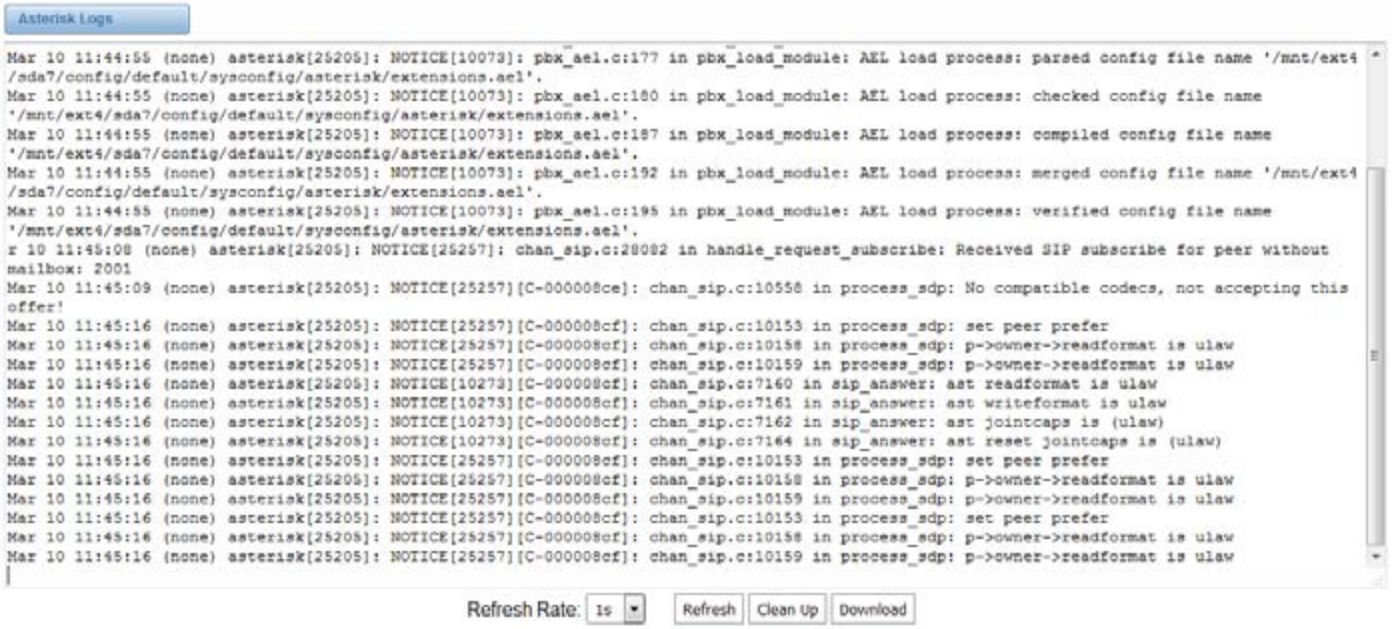
SYSTEM LOG

System log records every time the device is powered on or off and firmware upgrade information.



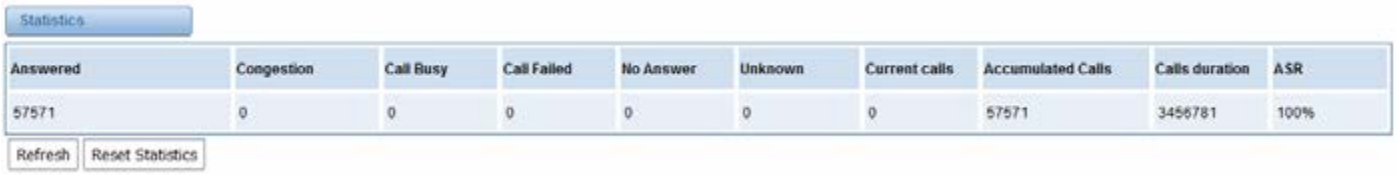
ASTERISK LOGS

On the pages of “Asterisk”, “SIP”, “IAX2”, “SS7”, “PRI” and “MFC/R2”, you will find the same functions –Displays the log by port, refresh regularly and log download.



CALL STATISTICS

Here 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 all the 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.



Note: Do not forget to enable call statistics in “Log Settings”.

SYSTEM NOTICE

The system notice is generated by the system to keep the network manager informed of any firmware up-gradesand auto provisioning messages from ACS. Enable the system notice function in “Log Setting” page as ahown below.

After about an hour, a system message is received in the web.

Note: Do not forget to enable system notice and check interval in “Log Setting” if you want to receive system messages.