DGW-100XR User Manual

Version1.0 (2015-03-26)

Full text

The overall layout adjustment

Copyright

Confidentiality

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

Disclaimer

OpenVox Inc. reserves the right to modify the design, characteristics, and products at any time without notification or obligation and shall not be held liable for any error or damage of any kind resulting from the use of this document.
OpenVox has made every effort to ensure that the information contained in this document is accurate and complete; however, the contents of this document are subject to revision without notice. Please contact OpenVox to ensure you have the latest version of this document.

Trademarks

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

Table of Contents

1. **Overview** **1**
What is DGW-100XR? 1
Sample Application 1
Product Appearance 2
Main Features 3
Physical Information 4
Software 4
2. System **5**
Status 5
Time 6
Login Settings 7
General 8
Language Settings 8
Scheduled Reboot 9
Tools and Information 9
Reboot Tools 9
Update Firmware 10
Upload and Backup Configuration 10
Restore Configuration 10
Information 11
3. T1/E1 .... **11**
General 11
Ports 12
Interface 13
Advanced Interface Type 13
Signaling 14
Advanced Signaling 14
ISDN Timer 17

Save to Other Ports 18
4. SIP....18
SIP Endpoints 18
Main Endpoint Settings 18
Advanced: Registration Options 21
Call Settings 21
Advanced: Timer Settings 22
Advanced SIP Settings 23
Networking 23
Advanced: NAT Settings 23
Advanced: RTP Settings 24
Parsing and Compatibility 25
Security 26
Media 26
Codec Settings 27
5. Routing 27
Call Routing Rule 28
Groups 30
MNP Settings 31
6. Network....31
WAN/LAN Settings 32
DDNS Settings 33
Toolkit 34
7. Advanced 34
Asterisk API 34
Asterisk CLI 36
Asterisk File Editor 36
8. Logs....37

1. Overview

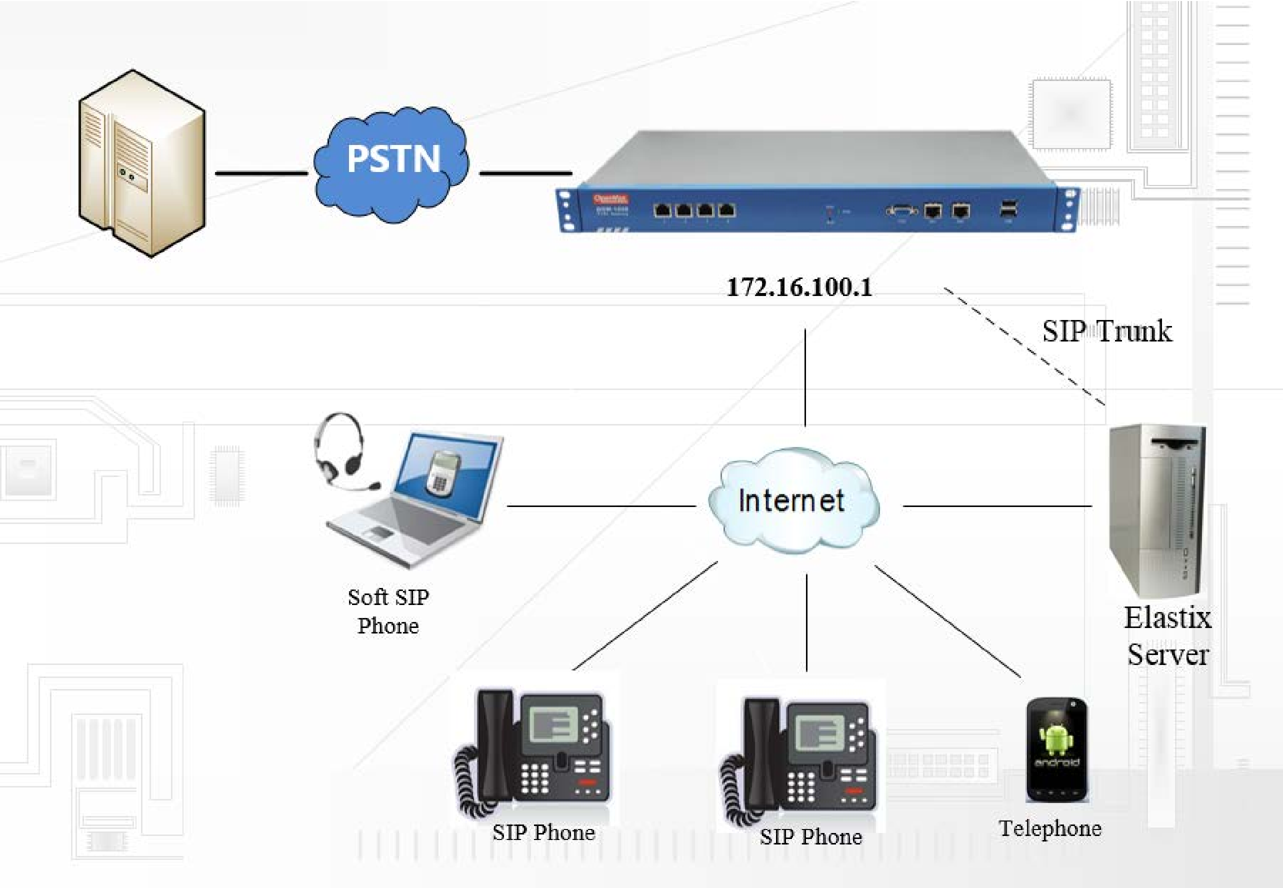
What is DGW-100XR?

OpenVox T1/E1 Gateway is an open source asterisk-based VoIP Gateway solution for operators and call centers. It is a converged media gateway product. This kind of gateway connects traditional telephone system to IP networks and integrates VoIP PBX with the PSTN seamlessly. With friendly GUI, users may easily setup their customized Gateway. Also secondary development can be completed through AMI (Asterisk Management Interface). The DGW-100XR could supports redundant power supply and DGW-100X series gateway support one power supply only.

It is developed with a wide selection of codecs and signaling protocol, including G.711A, G.711U, G.729A, G.722, G.723 and GSM. It supports PRI protocol. OpenVox T1/E1 Gateway has good processing ability and stability and we provides 1/2/4 T1/E1 interface for your choice. The DGW-100XR series gateways will be 100% compatible with all kind of SIP servers, such as Asterisk, Elastix, trixbox, 3CX, FreeSWITCH and other VoIP operating platforms.

Sample Application

Figure 1-2-1TopologicalGraph



Product Appearance

The picture below is appearance of DGW-1004.

Figure 1-3-1 Product Appearance

Figure 1-3-2 Front Panel

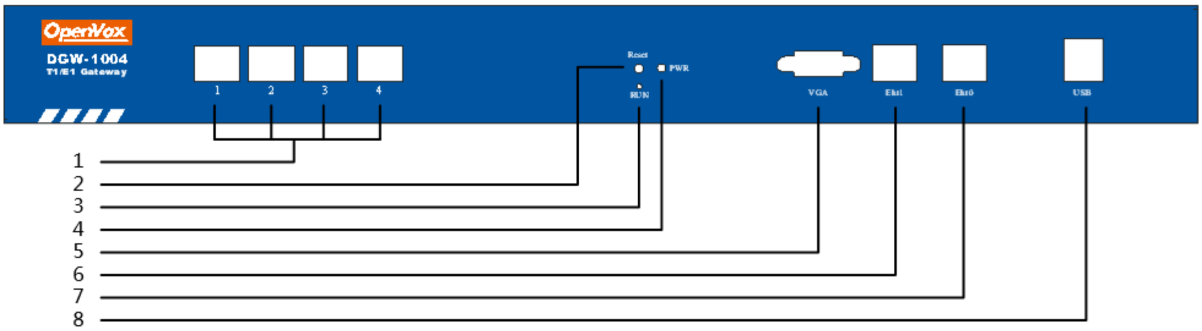
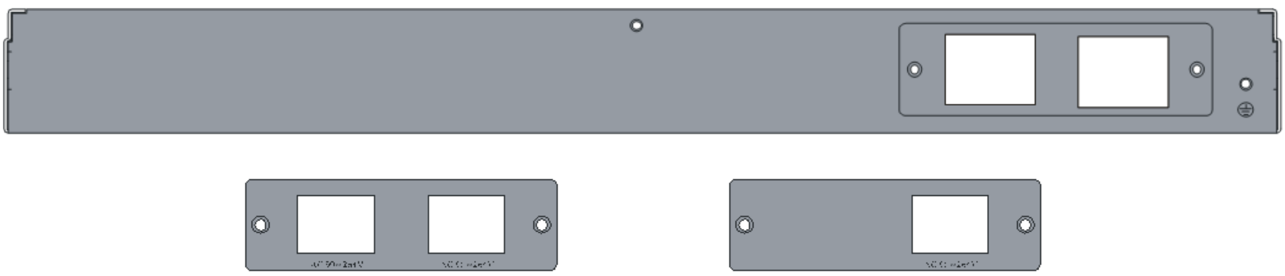


Table 1-3-1Description of Front Panel

Interface	Function	Color	Work Status
1 Port 1-Port4	E1/T1 ports. The port numbers are different on different models, from 1 to 4.		
2 Reset	Reset button is used to restart the device.		
3 RUN	Register indicator	Green	Slow blinking: Unregister
			Fast blinking: Register
4 PWR	Power Status indicator	Green	On: Power is on
			Off: Power is off
5 VGA	VGA monitor connector		
6 Eth1	Network interface		
7 Eth0	Network interface		
8 USB	USB interface		

Figure 1-3-2 Backup Panel



The OpenVox DGW-100X series gateways support one or two power supply, one power named DGW-100X and two power named DGW-100XR.

Main Features

- Based on Asterisk®
- Editable Asterisk® configuration file

- Wide selection of codecs and signaling protocol
- Support unlimited routing rules and flexible routing settings
- Stable performance, flexible dialing, friendly GUI
- Codecs support: G.711A, G.711U, G.729A, G.723.1, G.722, GSM
- Support ports group management
- 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

Physical Information

Table 1-5-1Description of Physical Information

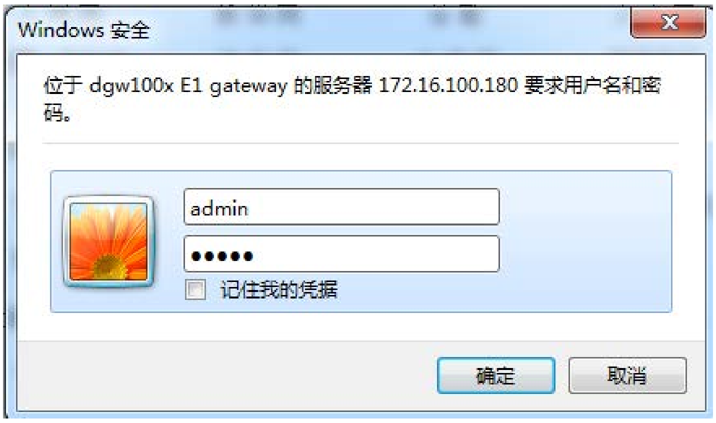
Weight	2813g ~ 3005g
Size	44cm*4.3cm*23cm
Temperature	-40~85°C (Storage)
	0~70°C (Operation)
Operation humidity	5%~95% non-condensing
Power supply specification	100-240V/AC
Max power	20W
WAN interface (Eth0)	1
LAN interface (Eth1)	1
VGA interface	1
USB 2.0 interface	2

Software

Default IP: 172.16.100.1
Username: admin
Password: admin

Notice: Log in

Figure 1-6-1 LOG IN Interface



2. System

Status

On the “Status” page, you will find all GSM, SIP, Routing, Network information and status.

Figure 2-1-1 System Status

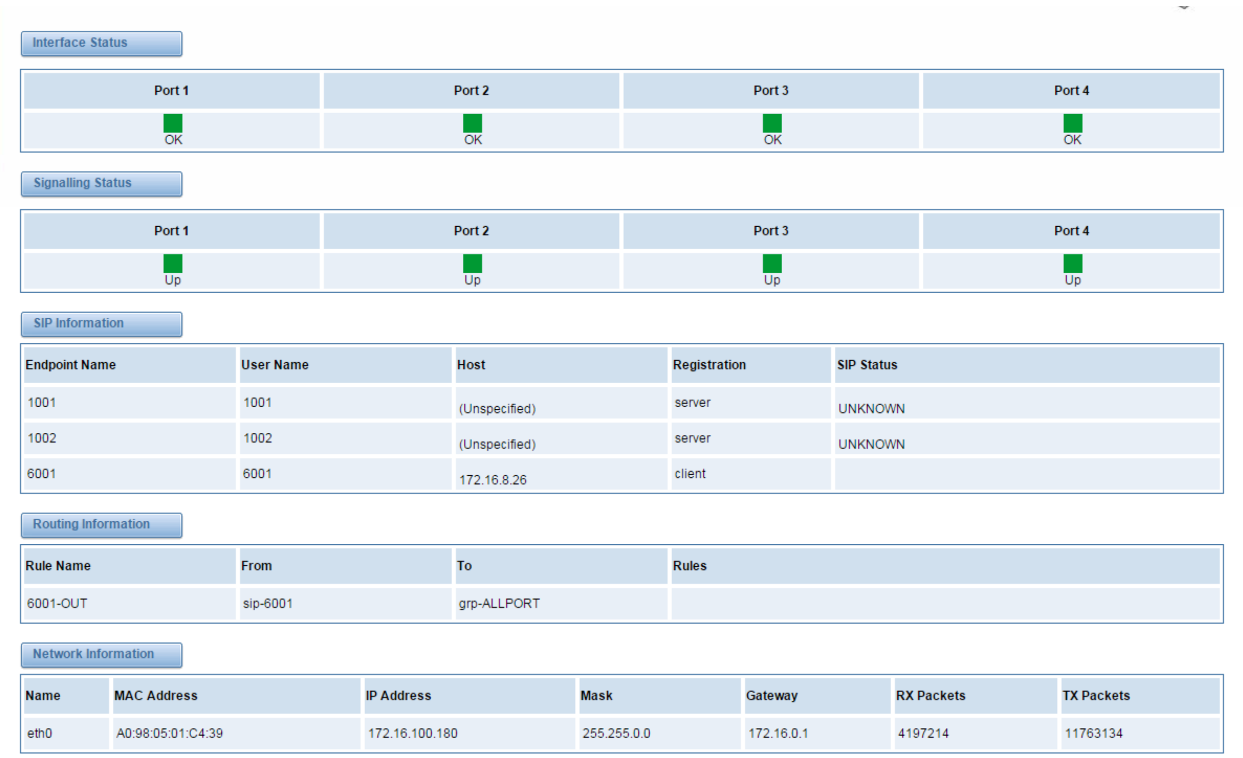


Table 2-1-1 Description of System Status

Options	Definition

Interface Status	Show the status of port, include "RED" and "OK". "RED" means no trunk line connected; "OK" means the trunk line of port is available.
Signaling Status	Show the signaling status of port, include "Down" and "UP". "Down" means it is unavailable; "UP" means the port is available.

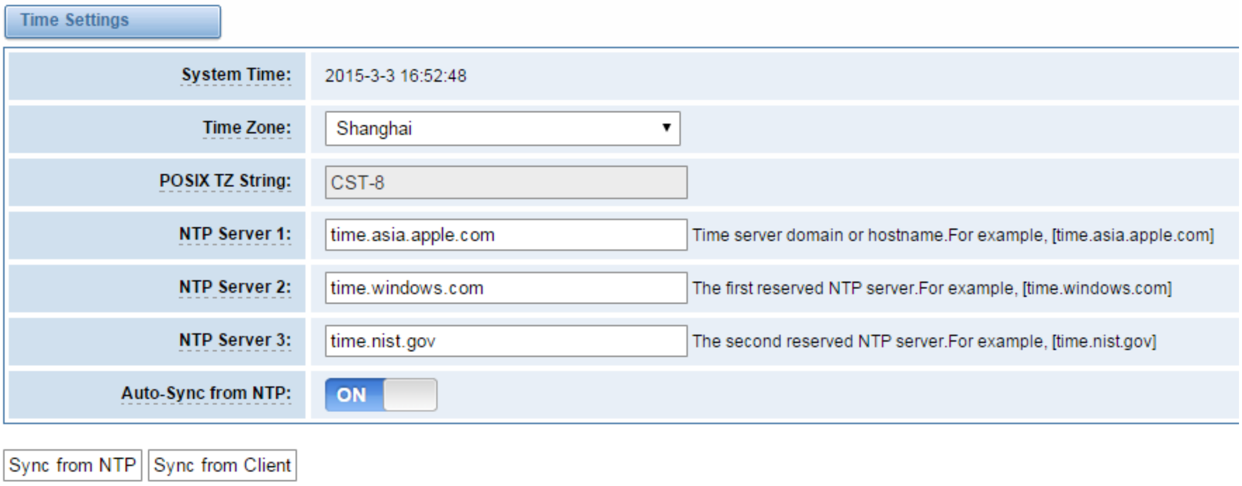
Time

Table 2-2-1Description of 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, [time.asia.apple.com].
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.

For example, you can configure like this:

Figure 2-2-1 Time Settings



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

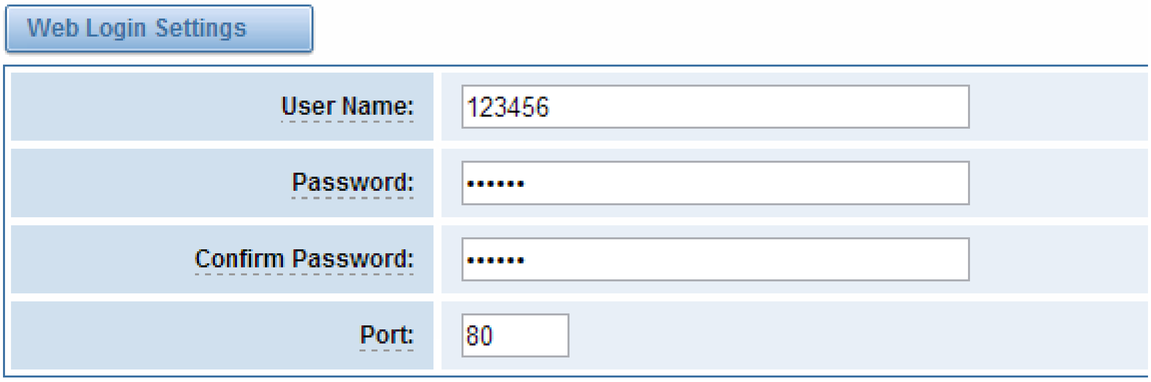
Login Settings

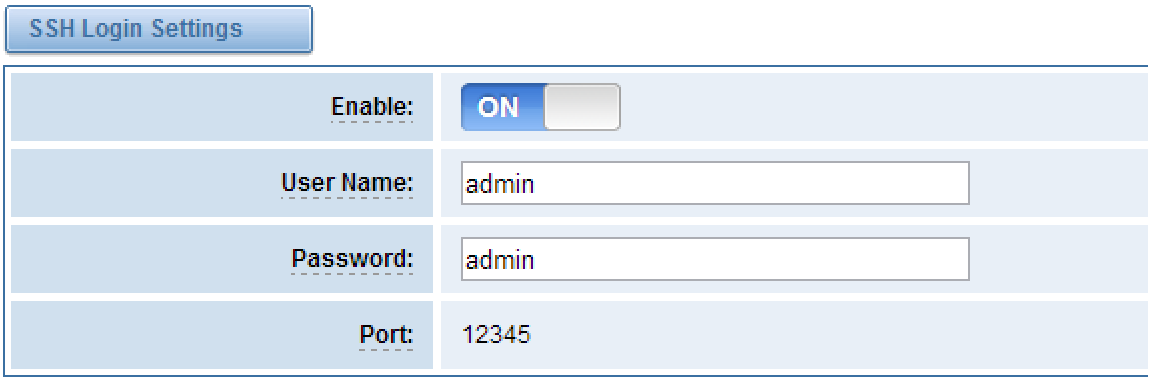
Your gateway doesn't have administration role. All you can do here is to reset what new username and password to manage your gateway. And it has all privileges to operate your gateway. You can modify "Web Login Settings" and "SSH Login Settings". If you have changed these settings, you don't need to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

Table 2-3-1Description of Login Settings

Options	Definition
User Name	Define your username and password to manage your gateway, without space here. 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.
Port	Specify the web server port number.

Figure 2-3-1 Login Settings





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

General

Language Settings

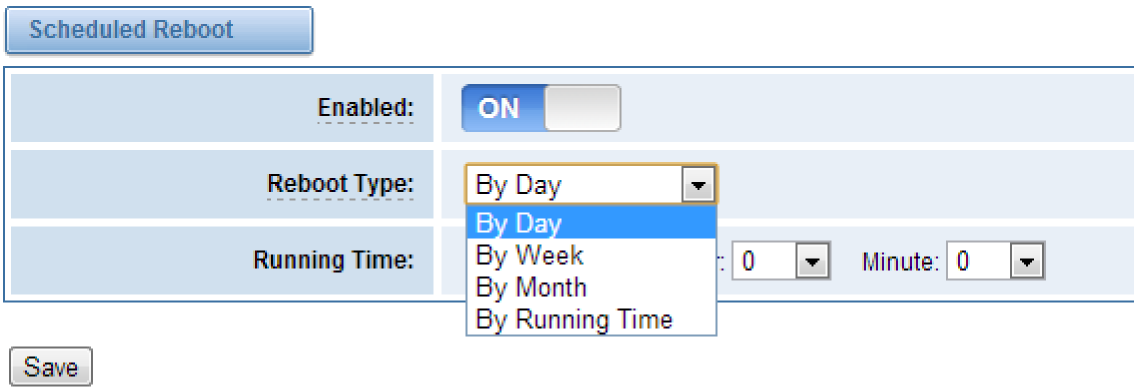
You can choose different languages for your system. If you want to change language, you can switch “Advanced” on, then “Download” your current language package. After that, you can modify the package with the language you need. Then upload your modified packages, “Choose File” and “Add”.

Figure 2-4-1 Language Settings

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 2-4-2 Reboot Types



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

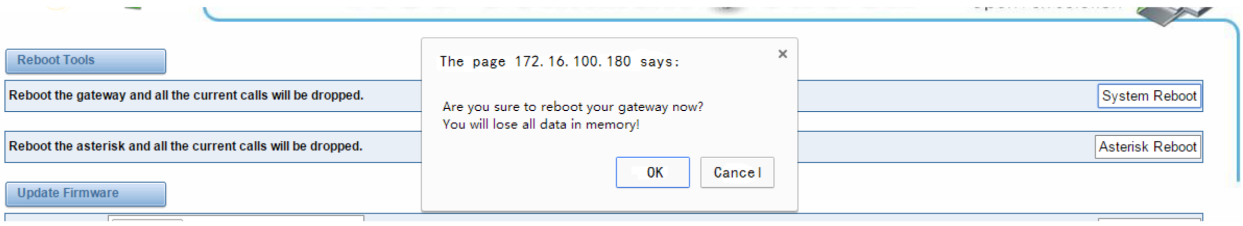
Tools and Information

On the “Tools” pages, there are reboot, update, upload, backup and reset toolkits.

Reboot Tools

You can choose system reboot and Asterisk reboot separately.

Figure 2-5-1 Reboot Prompt



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

Table 2-5-1 Instruction 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

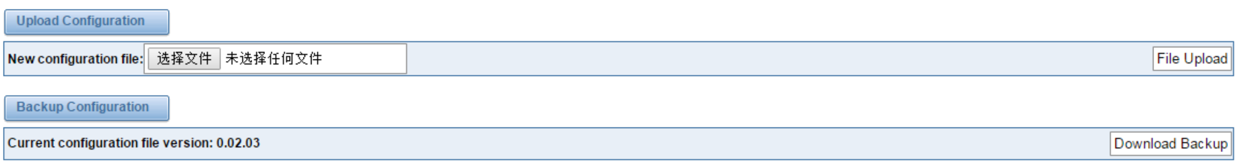
We offer 2 kinds of update types for you, you can choose System Update or System Online Update. System Online Update is an easier way to update your system, if you choose it, you will see some information below.

Figure 2-5-2Prompt Information

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.

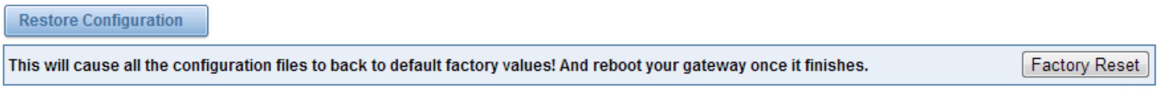
Figure 2-5-3 Upload and Backup



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 2-5-4 Factory Reset



Information

On the "Information" page, there shows some basic information about the GSM gateway. You can see software and hardware version, storage usage, memory usage and some help information.

Figure 2-5-5 System Information

3. T1/E1

General

Figure 3-1-1 General Settings

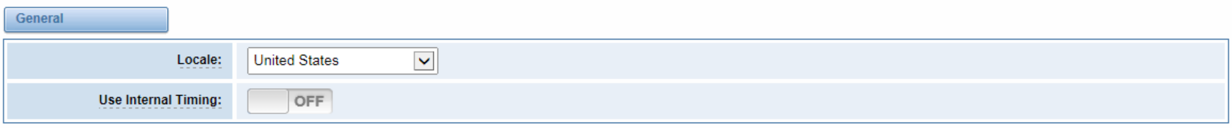


Table 3-1-1 Definition of General Settings

Options	Definition
Local	Your local. 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.

Use Internal Timing	ON: Disable clock recovery from the T1/E1 spans. All spans use internal timing. OFF: Enable clock recovery from the T1/E1 spans. Default is OFF. And you can see the following figure 2-2.

Figure 3-1-2 Clock Recovery

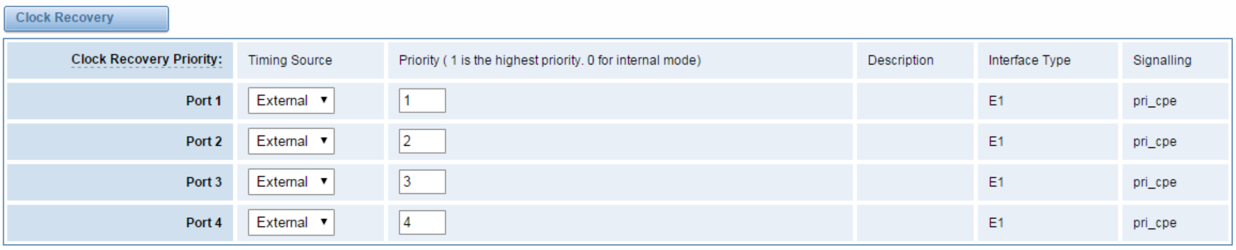


Table 3-1-2 Definition of Clock Recovery

Options	Definition
Clock Recovery Priority	Prioritize the ports as to which should be used to recover the clock. (Priority 1 is the highest priority. 0 is for Internal mode.)
Timing Source	It allows you to choose the timing source mode. It has two options, "External" and "Internal". default value is "External"
Priority	Show the priority of port and allow you to edit it.
Interface Type	It shows you the current type of port. It has two types: E1 and T1
Signaling	It shows you what signaling the port uses.

Ports

Figure 3-2-1 Port 1 Modify

Select which port you want to config. You can click the Port 1 button to modify the port 1 configuration. Then you will go to the port 1 configuration page. Here below is the description of Port 1 configuration options.

Interface

Figure 3-2-2 Interface Settings

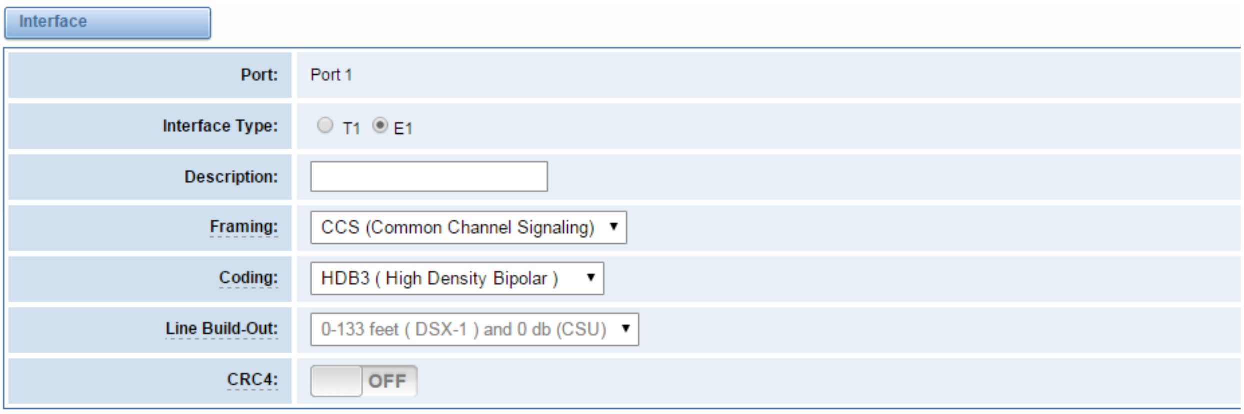


Table 3-2-1 Definition of Interface Settings

Options	Definition
Interface Type	Choose a line type for this interface.
Description	An optional description of this interface to be used for reference only.
Framing	Framing method for this interface.
Coding	Coding method for this interface.
Line Build-Out	Line build-out represents the length of the cable from the port on this gateway to the next device.
CRC4	Enable cyclic redundancy checking for error checking on the line. CRC-4 support is required for all network switches in Europe, but many older switches and PBXs don't support it.

Advanced Interface Type

Figure 3-2-3 Interface Type

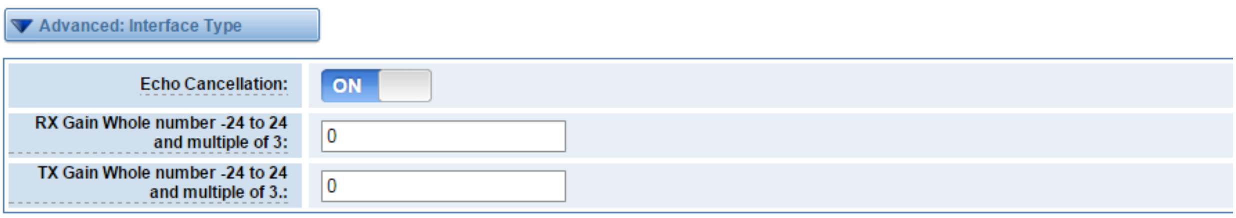


Table 3-2-2 Definition of Interface Type

Options	Definition
Echo Cancellation	Whether or not to enable echo cancellation on this line.
RX Gain	Adjust the gain for audio received on this interface.
TX Gain	Adjust the gain for audio sent on this interface.

Signaling

Figure 3-2-4 Signaling

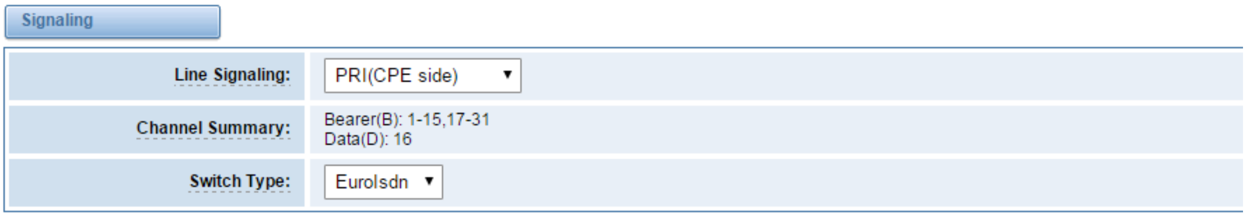


Table 3-2-3 Definition of Signaling

Options	Definition
Line Signaling	Line signaling for this interface.
Channel Summary	This is a summary of the number of channels and their configuration. Click the 'Edit' icon in order to change this, but save your changes to this page first.
Switch Type	For PRI only, specify the signaling type of the switch the line is connected to.

Advanced Signaling

Figure 3-2-5 Advanced Signaling

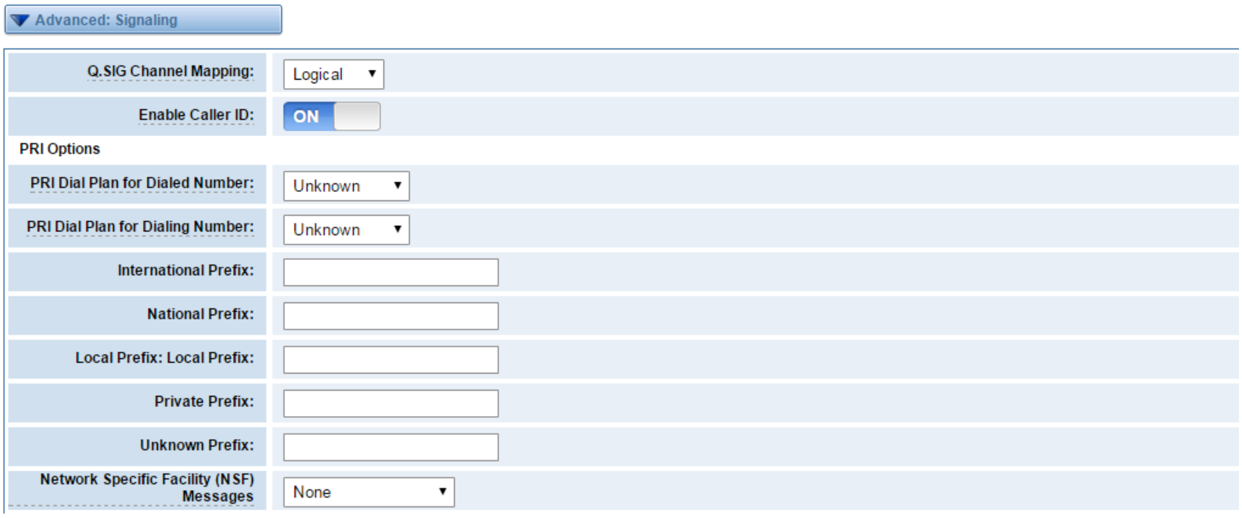


Table 3-2-4 Definition of Advanced Signaling

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 enable caller ID.

Table 3-2-5 Definition of PRI Options

Options	Definition
PRI Dial Plan for Dialed Number	Dialing specifications for this interface, which is normally dependent on geographical location.
PRI Dial Plan for Dialing Number	PRI Local Dialplan: Only RARELY used for PRI(sets the calling numbre's numbering plan). In North America, the typical use is sending the 10 digit; callerID number and setting the prilocaldialplan to 'national' (the default); Only VERY rarely will you need to change this.

PRI Prefixes	Prefixes for international, national, private, local, and unknown numbers, for use with dynamic dialing plans. The prefixes specified will be used to dynamically select how the ISDN Type Of Number bits are set. In the case of the international prefix, if the international prefix matches the beginning digits of the calling number (if your "PRI Dial Plan for Dialing Number" is set to dynamic), it will automatically set the ISDN TON on the calling number to international. Likewise for national and local prefixes. This will also have the behavior of stripping off the digits in the prefix from the called number as well. Note: Digit stripping occurs ONLY if the national or international prefix is matched - NOT in the case of the local prefix matching successfully. In any case though, the TON will be set properly. Digit stripping is not cumulative with international and national prefixes; so if you always receive E.164 format numbers with a plus and country code, e.g. +44, and you would like to set the international prefix as the "+" character, and your country code happens to be 44, and you would like to convert that number to be a national number, you must make the national prefix "+44".
Network Specific Facility (NSF) Messages	Some switches (AT&T especially) require network specific facility IE supported values are currently 'none', 'sdn', 'megacom', 'tollfreemegacom', 'accunet'
Idle Bearer Reset	Whether or not to reset unused B channels.
Idle Bearer Reset Period	Time in seconds between reset of unused B channels.
Overlap Dialing	Enable overlap dialing mode--sending overlap digits.
Allow Progress When Call Released	Allow inband audio (progress) when a call is RELEASEd by the far 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	Enables transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility). 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	Ignores remote hold indications and use music on hold that is supplied over the B channel.

Block Outbound Caller ID Name	Enable if you need to hide the name and not the number for legacy PPBX use. Only applies to PRI channels.
Wait for Caller ID Name	Support Caller ID on call waiting.

ISDN Timer

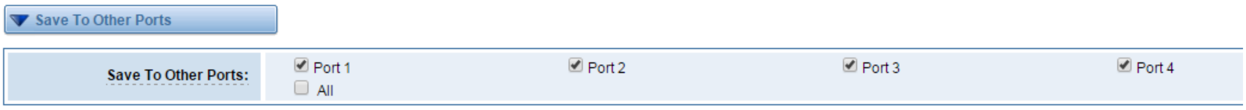
Table 3-2-6 Definition of ISDN Timer

Options	Definition
Layer 2 Outstanding Unacknowledged I-Frames - K	Layer 2 maximum number of outstanding unacknowledged I frames.
Layer 2 Number of Frame Retransmissions - N200	Layer 2 maximum number of retransmissions of a frame.
Layer 2 Frame Retransmission Time - T200	Layer 2 maximum time before retransmission of a frame.
Layer 2 Time Without Frame Exchange - T203	Layer 2 maximum time without frames being exchanged.
Disconnect Acknowledge - T305	Maximum time to wait for DISCONNECT acknowledge.
Release Acknowledge - T308	Maximum time to wait for RELEASE acknowledge.
Enable Maintain Calls on Layer 2 Disconnection	Whether or not to maintain active calls on Layer 2 disconnection.
Maintain Calls on Layer 2 Disconnection - T309	Maximum length of Layer 2 disconnection which may occur and have the call continue to be maintained.
Connect Acknowledge - T313	Maximum time to wait for CONNECT acknowledge, CPE side only.

Save to Other Ports

Save all of the above configuration to other ports selected.

Figure 3-2-6 Save to Other Ports

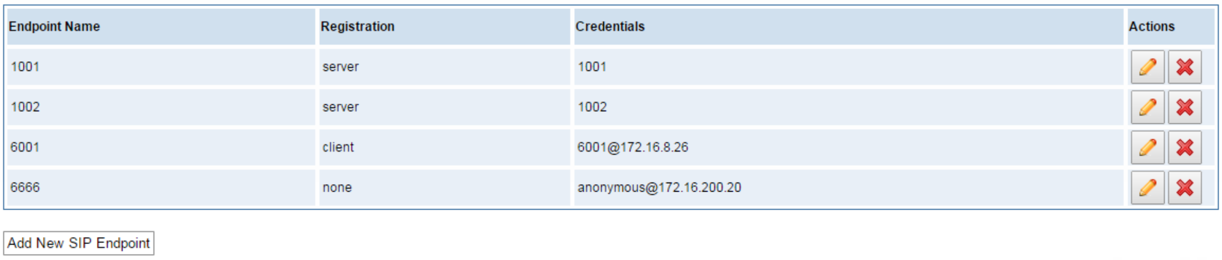


4. SIP

SIP Endpoints

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

Figure 4-1-1 SIP Status



Endpoint Name	Registration	Credentials	Actions
1001	server	1001	
1002	server	1002	
6001	client	6001@172.16.8.26	
6666	none	anonymous@172.16.200.20	

Add New SIP Endpoint

Main Endpoint Settings

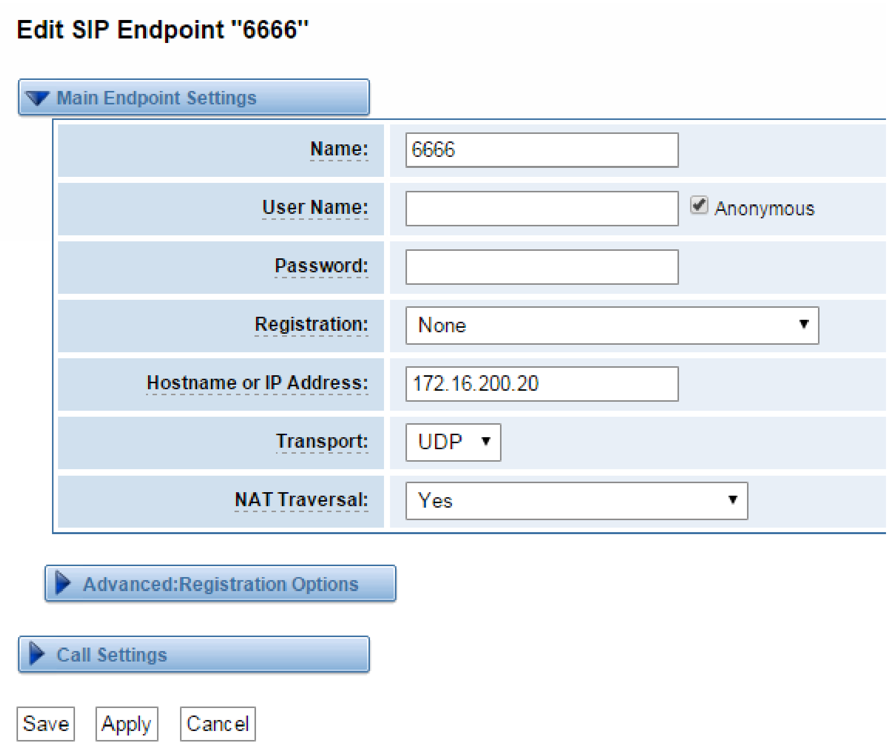
You can click Add New SIP Endpoint button to add a new SIP endpoint, and if you want to modify existed endpoints, you can click button.

There are 3 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:

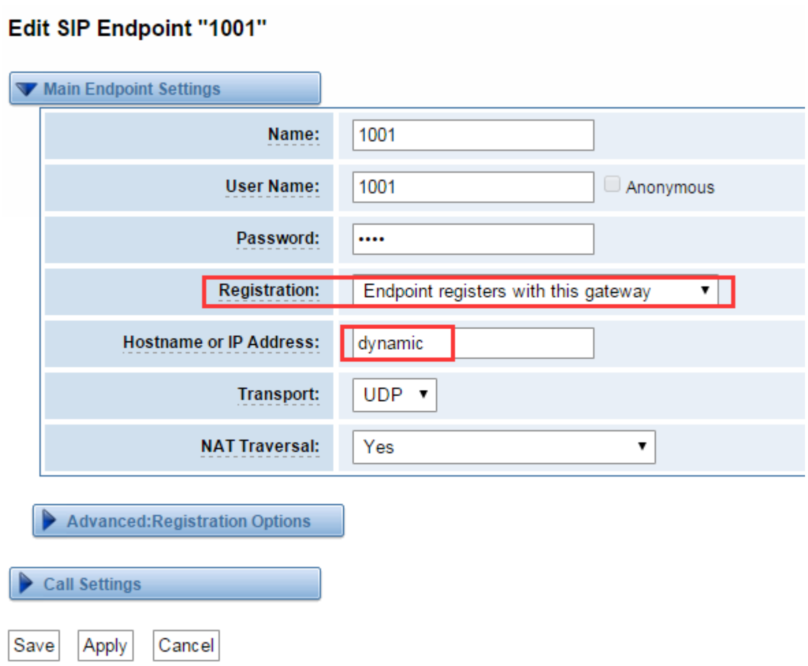
If you set up a SIP endpoint by registration "None" to a server, then you can't register other SIP endpoints to this server. (If you add other SIP endpoints, this will cause Out-band Routes and Trunks confused.)

Figure 4-1-2 None Registration



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.

Figure 4-1-3 Endpoint Register with Gateway



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

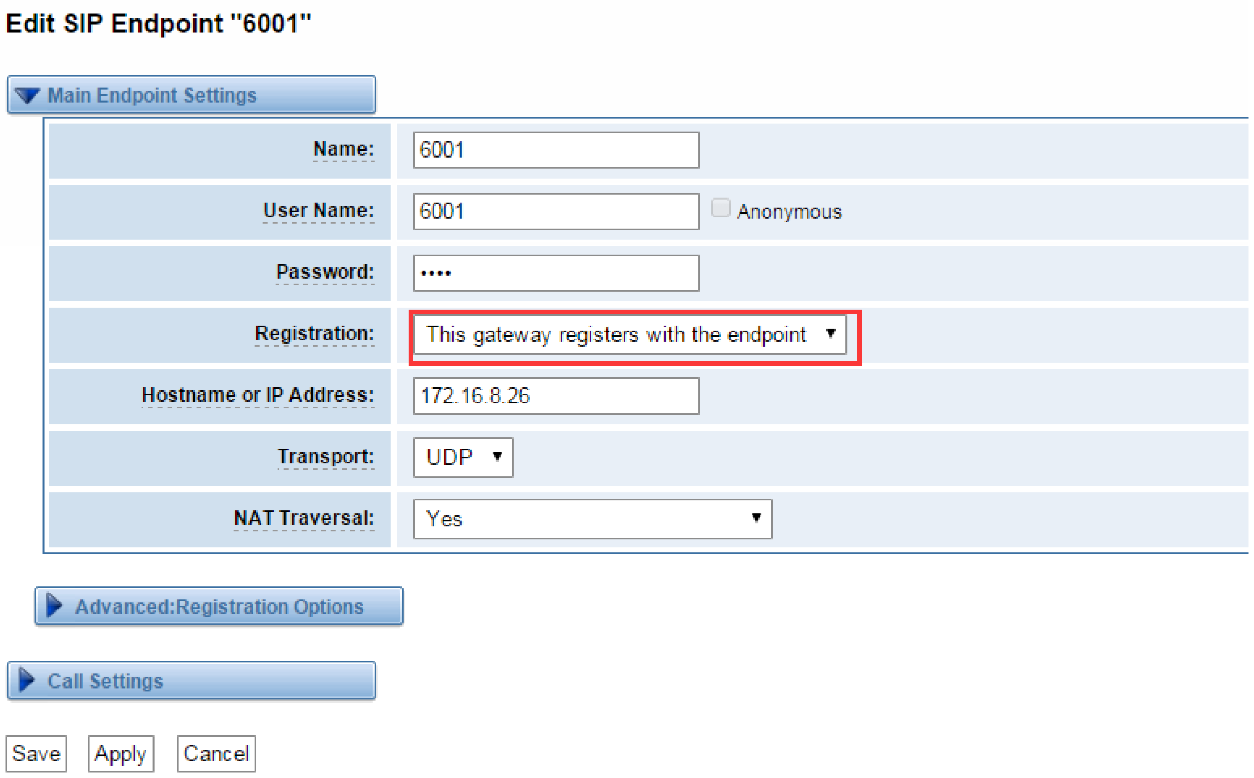


Table 4-1-1 Definition of SIP Options

Options	Definition
Name	Display name.
Username	Register name in your SIP server.
Password	Authenticating with the gateway and characters are allowed.
Registration	**None**---Not registering; **Endpoint registers with this gateway**---When register as this type, it means the GSM gateway acts as a SIP server, and SIP endpoints register to the gateway; **This gateway registers with the endpoint**---When register as this type, it means the GSM gateway acts as a client, and the endpoint should be register to a SIP server;
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.

Transport	This sets the possible transport types for outgoing. Order of usage, when the respective transport protocols are enabled, is UDP, TCP, TLS. The first enabled transport type is only used for outbound messages until a Registration takes place. During the peer Registration the transport type may change to another supported type if the peer requests so.
NAT Traversal	**No**---Use Report if the remote side says to use it. **Force Report on**---Force Report to always be on. **Yes**---Force Report to always be on and perform comedia RTP handling. **Report if requested and comedia**---Use Rport if the remote side says to use it and perform comedia RTP handling.

Advanced: Registration Options

Table 4-1-2 Definition of 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.
Quality	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.

Call Settings

Table 4-1-3 Definition of Call Options

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.
Remote Party ID Format	How to set the Remote-Party-ID header: from Remote-Party-ID or from P-Asserted-Identity.
Caller ID Presentation	Whether or not to display Caller ID.

Advanced: Timer Settings

Table 4-1-4 Definition of Timer Options

Options	Definition
Default T1 Timer	This timer is used primarily in INVITE transactions. The default for Timer T1 is 500ms or the measured run-trip time between the gateway and the device if you have qualify=yes for the device.
Call Setup Timer	If a provisional response is not received in this amount of time, the call will auto-congest. Defaults to 64 times the default T1 timer.
Session Timers	Session-Timers feature operates in the following three modes: originate, Request and run session-timers always; accept, run session-timers only when requested by other UA; refuse, do not run session timers in any case.
Minimum Session	Minimum session refresh interval in seconds. Default is 90secs.
Maximum Session Refresh Interval	Maximum session refresh interval in seconds. Defaults to 1800secs.
Session Refresher	The session refresher, uac or uas. Defaults to uas.

Advanced SIP Settings

Networking

Table 4-2-1 Definition of Networking Options

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.
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.

Advanced: NAT Settings

Table 4-2-2 Definition of NAT Settings Options

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 externaddr or externhost setting if it matches.
Dynamic Exclude Static	Disallow all dynamic hosts from registering as any IP address used for statically defined hosts. This helps avoid the configuration error of allowing your users to register at the same address as a SIP provider.
Externally Mapped TCP Port	The externally mapped TCP port, when the gateway is behind a static NAT or PAT.
External Hostname	The external hostname (and optional TCP port) of the NAT.
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.
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.

Advanced: RTP Settings

Table 4-2-3 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.

Parsing and Compatibility

Table 4-2-4 Instruction of Parsing and Compatibility

Options	Definition
Strict RFC Interpretation	Check header tags, character conversion in URIs, and multiline 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	The external hostname (and optional TCP port) of the NAT.
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 Expiry	Maximum allowed time of incoming registrations and subscriptions (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	Attempts Enter '0' for unlimited 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.

Security

Table 4-2-5 Instruction of Security

Options	Definition
Match Auth Username	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

Table 4-2-6 Instruction of Media

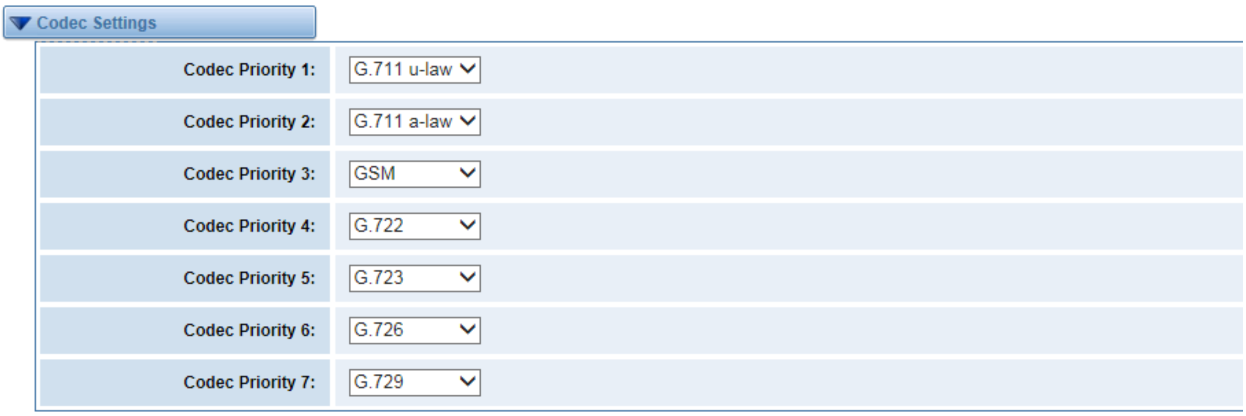
Options	Definition

Premature Media	Some ISDN links send empty media frames before the call is in ringing or progress state. The SIP channel will then send 183 indicating early media which will be empty - thus users get no ring signal. Setting this to "yes" will stop any media before we have call progress (meaning the SIP channel will not send 183 Session Progress for early media). Default is 'yes'. Also make sure that the SIP peer is configured with progressinband=never. In order for 'noanswer' applications to work, you need to run the progress() application in the priority before the app.
TOS for SIP Packets	Sets type of service for SIP packets
TOS for RTP Packets	Sets type of service for RTP packets

Codec Settings

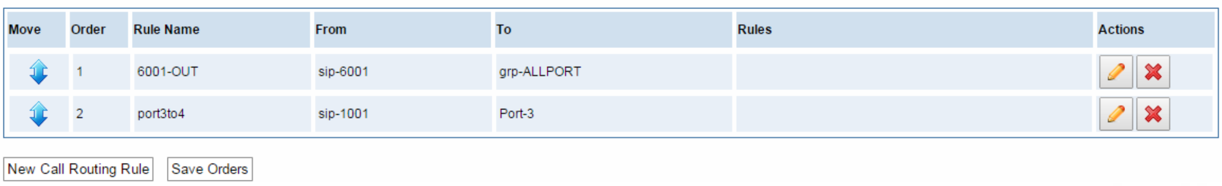
Select codecs from the list below.

Figure 4-2-1 Codec Settings



5. Routing

Figure 5-1-1 Routing Rules

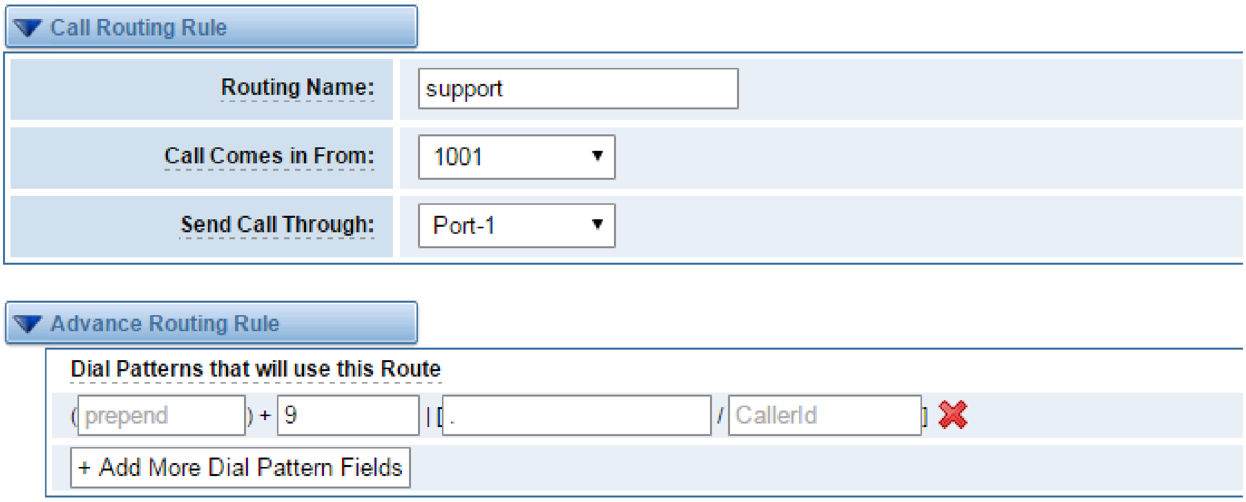


You are allowed to set up new routing rule by New Call Routing Rule, and after setting routing rules, move rules' order by pulling up and down, click button to edit the routing and to delete it. Finally click the Save Orders button to save what you set. Rules shows current routing rules. Otherwise you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

Call Routing Rule

You can click New Call Routing Rule button to set up your routings.

Figure 5-1-2 Example of Set Up Routing Rule



The figure above realizes that calls from "support" SIP endpoint switch you have registered will be transferred to gsm-1. When "Call Comes in From" is gsm, "prepend", "prefix" and "match pattern" in "Advanced Routing Rule" are ineffective, and just "CallerID" option is available.

Table 5-1-1 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, 'SIP2GSM' or 'GSM2SIP').
Call Comes in From	The launching point of incoming calls.
Send Call Through	The destination to receive the incoming calls.

Table 5-1-2 Description of Advanced Routing Rule

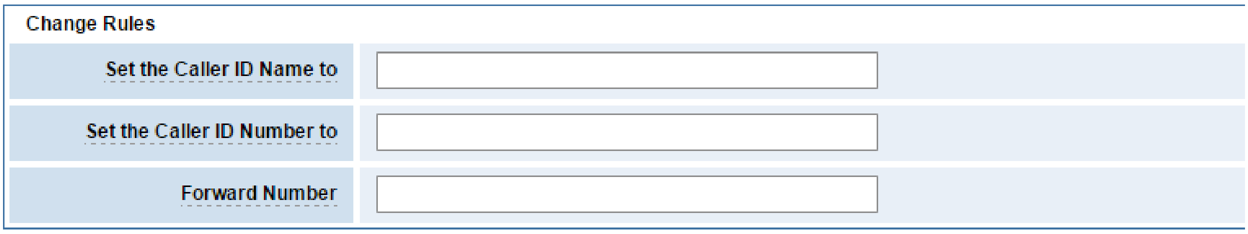
Options	Definition
Dial Patterns that will use this Route	A Dial Pattern is a unique set of digits that will select this route and send the call to the designated trunks. If a dialed pattern matches this route, no subsequent routes will be tried. If Time Groups are enabled, subsequent routes will be 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 **CallerID**: If CallerID is supplied, the dialed number will only match the prefix + match pattern if the CallerID has been transmitted matches this. When extensions make outbound calls, the CallerID will be their extension number and NOT their Outbound CID. The above special matching sequences can be used for CallerID matching similar to other number matches.
Set the Caller ID Name to	What caller ID name would you like to set before sending this call to the endpoint.
Set the Caller ID Number to	What caller number would you like to set before sending this call to the endpoint.
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.

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

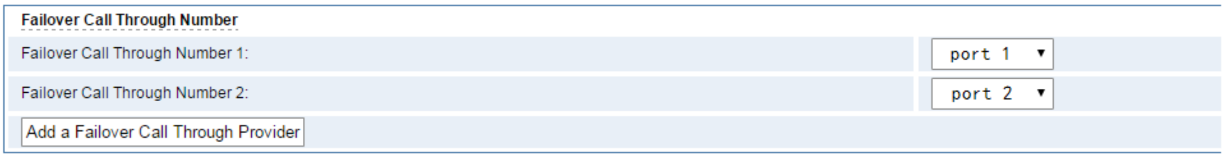
If you configure like this, then from January to March, from the first day to the last day of these months, from Monday to Thursday, from 00:00 to 02:00, during this time (meet all above time conditions), all calls will follow this route. And the time will synchronize with your Sever time.

Figure 5-1-4 Change Rules



You can set your caller ID name and caller number as you like before sending the call to the endpoint. You can also configure forward number when you have a transfer call.

Figure 5-1-5 Failover Call Through Number

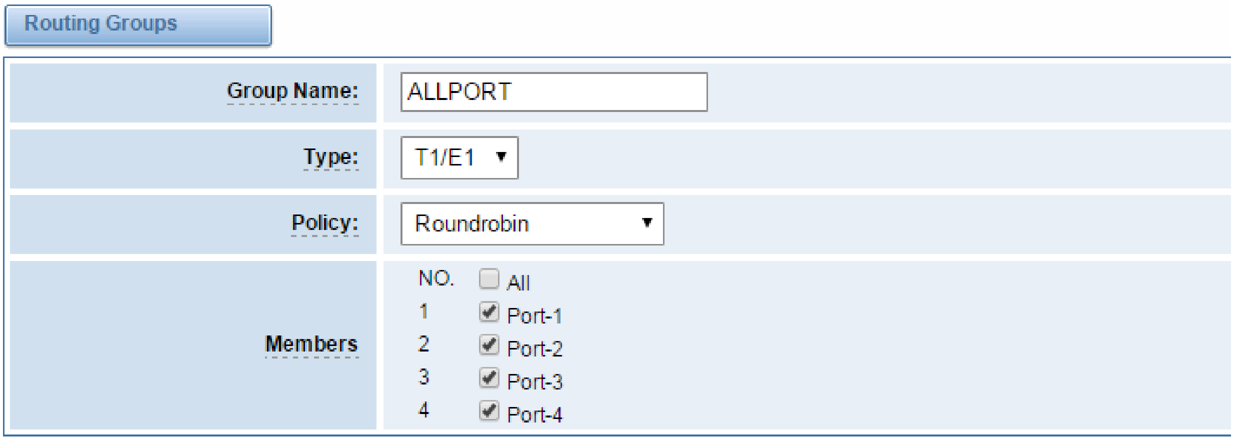


You can add one or more “Failover Call Through Numbers”.

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 GSM or SIP to groups. Then if you want to make a call, it will find available port automatically.

Figure 5-2-1 Establish Group



MNP Settings

Mobile Number Portability allows switching between mobile phone operators without changing the mobile number. Sounds simple, but there are loads of tasks performed behind the scene at the operator end.

The URL is shown in the password string way. So please type the url in other place such a txt file, check it, then copy it to the gateway. The outgoing number in the url should be replaced by the variables ${num}.

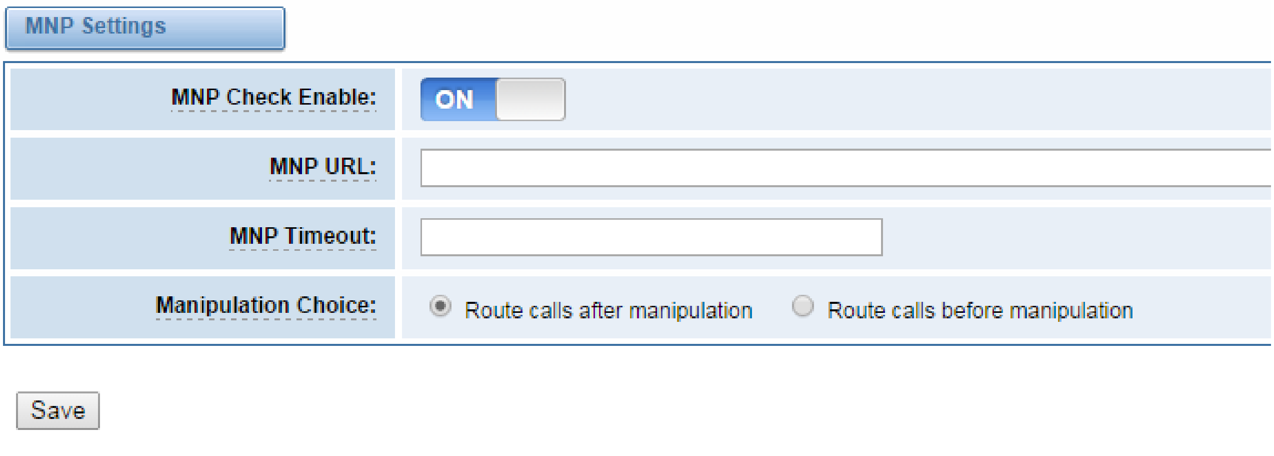
Here is an example of the MNP url:

https://s1.bichara.com.br:8181/chkporta.php?user=832700&pwd=sdsfdg&tn=8388166902

The 8388166902 is the outgoing phone number, when config the MNP url, should replce it with ${num}. Then it turns to

https://s1.bichara.com.br:8181/chkporta.php?user=832700&pwd=sdsfdg&tn=${num }.

Figure 5-3-1 MNP Settings



6. Network

On “Network” page, there are five sub-pages, “LAN Settings”, “DDNS Settings”, and “Toolkit”.

WAN/LAN Settings

There are three types of WAN/LAN port IP, Factory, Static and DHCP. Factory is the default type, and it is 172.16.99.1. When you Choose LAN IPv4 type is “Factory”, this page is not editable.

Figure 6-1-1 WAN/LAN Settings Interface

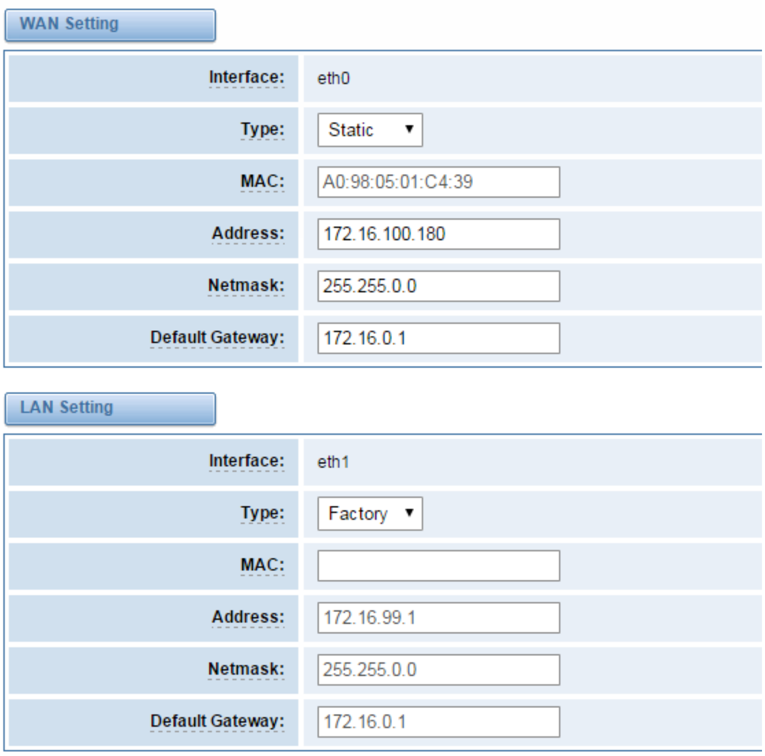
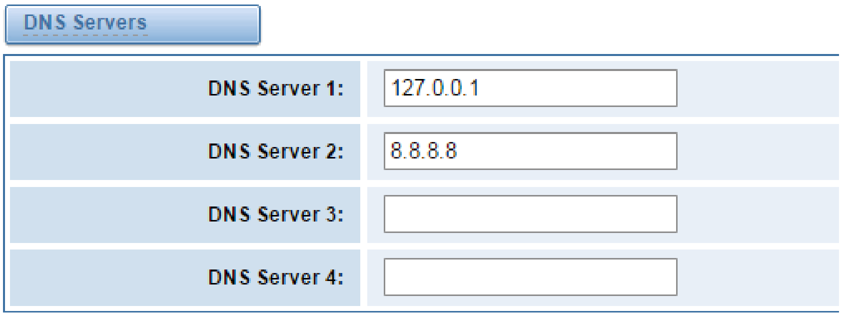


Table6-1-1Definition of LAN Settings

Options	Definition
Interface	The name of network interface.
Type	The method to get IP. Factory: Getting IP address by Slot Number (System → information to check slot number). 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.

Basically this info is from your local network service provider, and you can fill in four DNS servers.

Figure 6-1-2 DNS Interface



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

DDNS Settings

You can enable or disable DDNS (dynamic domain name server).

Figure 6-2-1 DDNS Interface

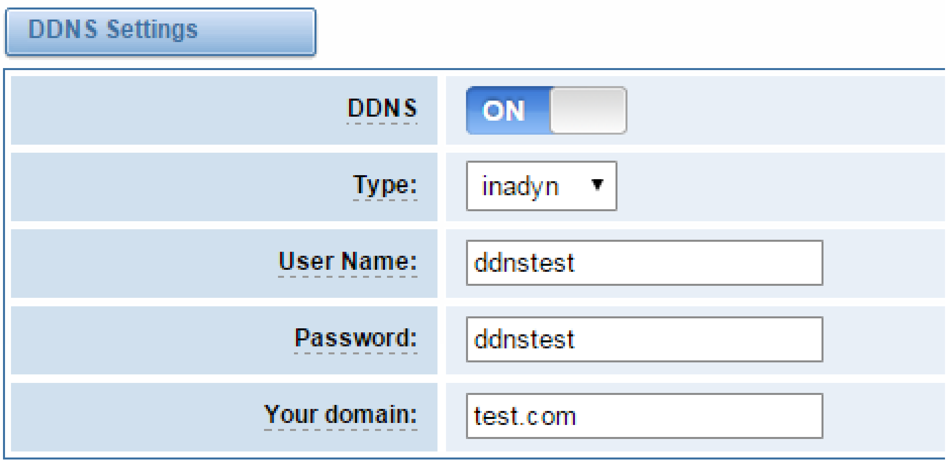


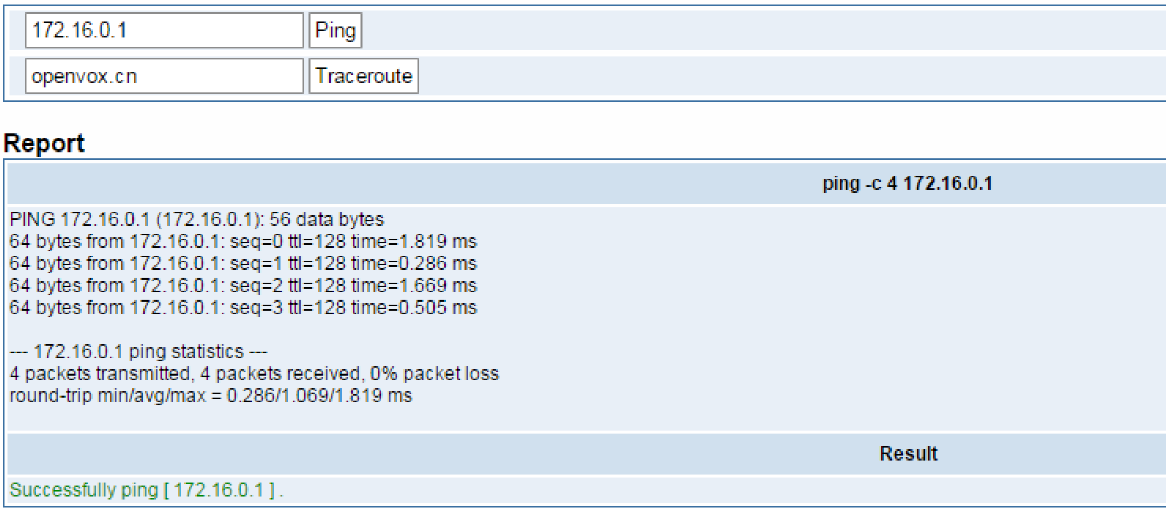
Table 6-2-1 Definition of DDNS Settings

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

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

Figure 6-3-1 Network Connectivity Checking



7. Advanced

Asterisk API

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

Figure 7-1-1 API Interface

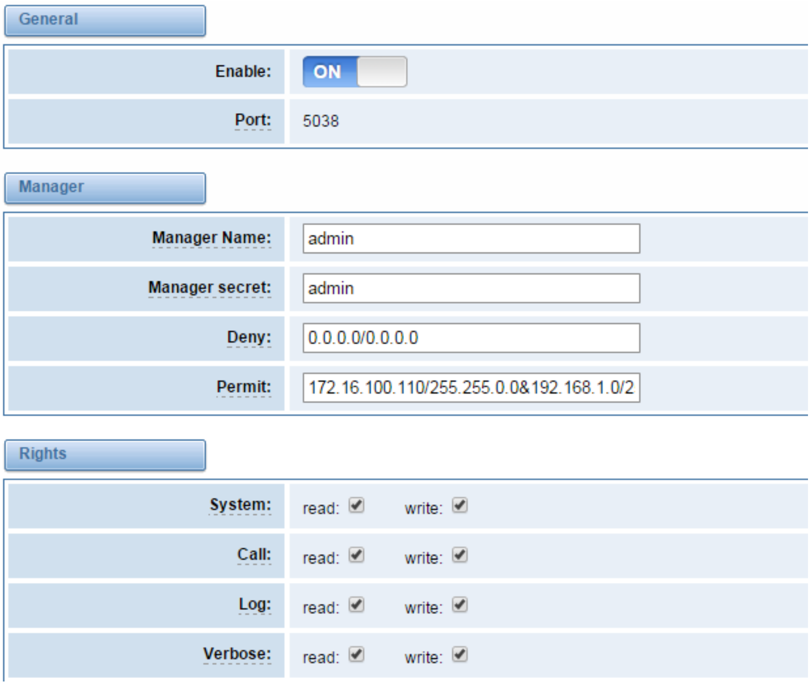
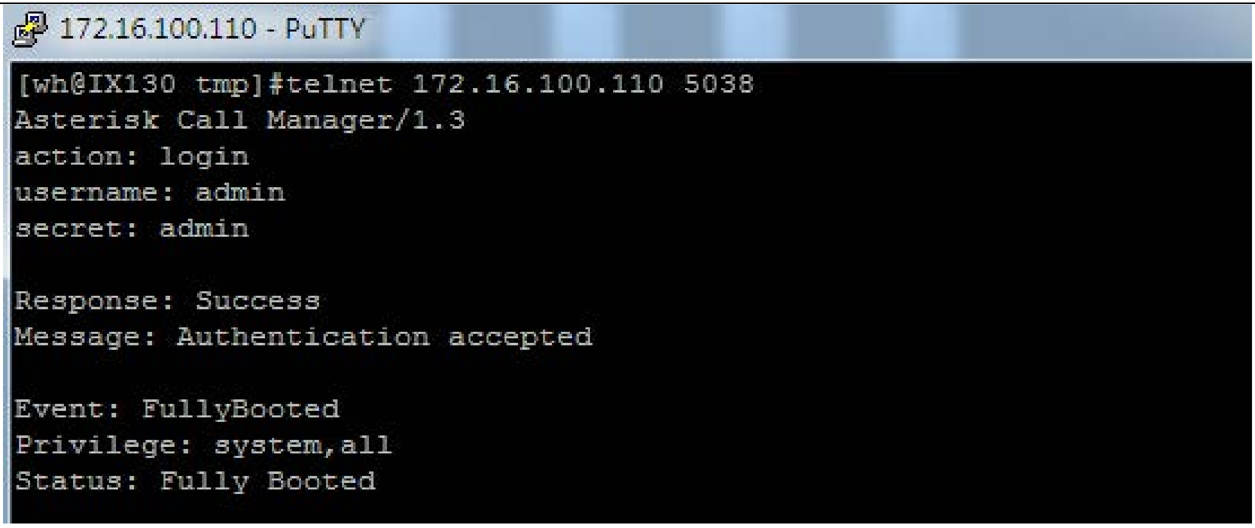


Table 7-1-1 Definition of Asterisk API

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 Varset 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



Asterisk CLI

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

Figure 7-2-1 Asterisk Command Interface

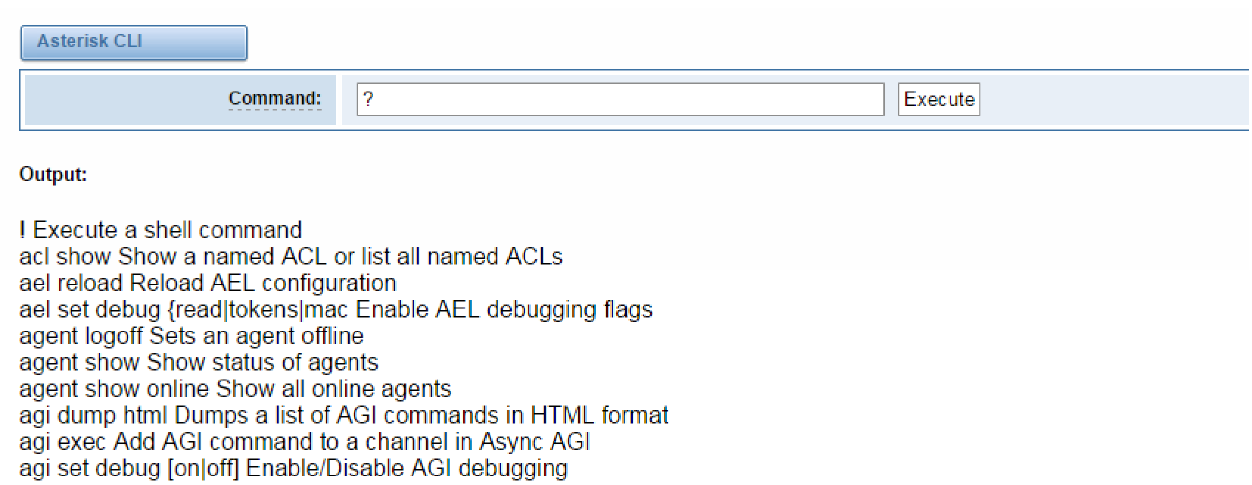


Table 7-2-1 Definition of Asterisk API

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.

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

File Name	File Size
acl.conf	2817
adsi.conf	140
agents.conf	2531
alarmreceiver.conf	2084
alsa.conf	3498
amd.conf	767
app_mysql.conf	1044
app_skel.conf	338
asterisk.conf	4501
calendar.conf	5171

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

8. Logs

On the “Log Settings” page, you should set the related logs on to scan the responding logs page. For example, set “System Logs” on like the following, then you can turn to “System” page for system logs, otherwise, system logs is unavailable. And the same with other log pages.

Figure 8-1-1 Logs Settings

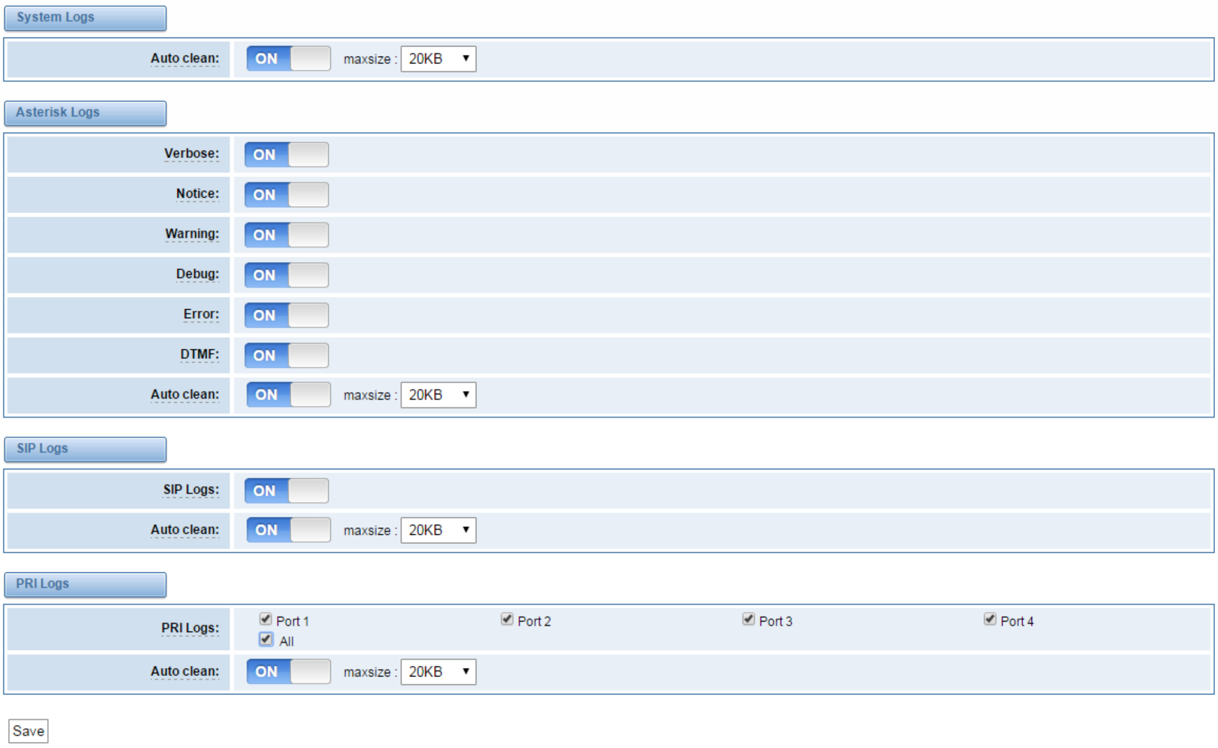


Figure 8-1-2 System Logs Output

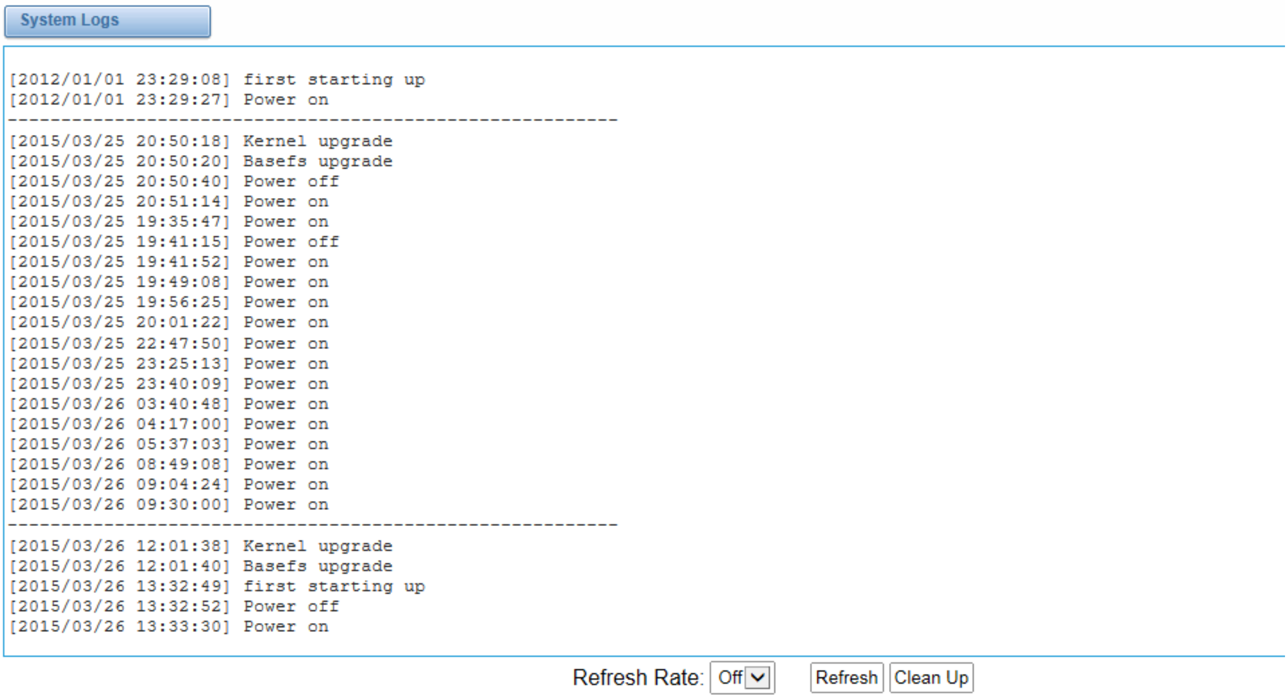


Table 8-1-1 Definition of Logs

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, maxsize=20KB
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, maxsize=20.
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, maxsize=20KB
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, maxsize=20KB.