Synway SBO Series Gateway

SBO500 Gateway

SBO2000 Gateway

User Manual

Version 1.6.5

Synway Information Engineering Co., Ltd

www.synway.net

Content

Copyright Declaration

Revision History

Version	Date	Comments
Version 1.0.0	2015-05	Initial publication.
Version 1.6.2	2015-09	New revision
Version 1.6.3	2016-01	New revision
Version 1.6.4	2016-09	New revision
Version 1.6.5	2017-06	New revision

Note: Please visit our website http://www.synway.net to obtain the latest version of this document.

Chapter 1 Product Introduction

Thank you for choosing Synway SBO Series Gateway!

The Synway SBO series gateway products (hereinafter referred to as ‘SBO gateway’) are mainly used for connecting IP or enterprise PBX with the IP telephony network or IP PBX. It provides such functions as transcoding, routing, number filtration, number manipulation and so on. Currently, only SBO500 and SBO2000 are available for you.

1.1 Typical Application

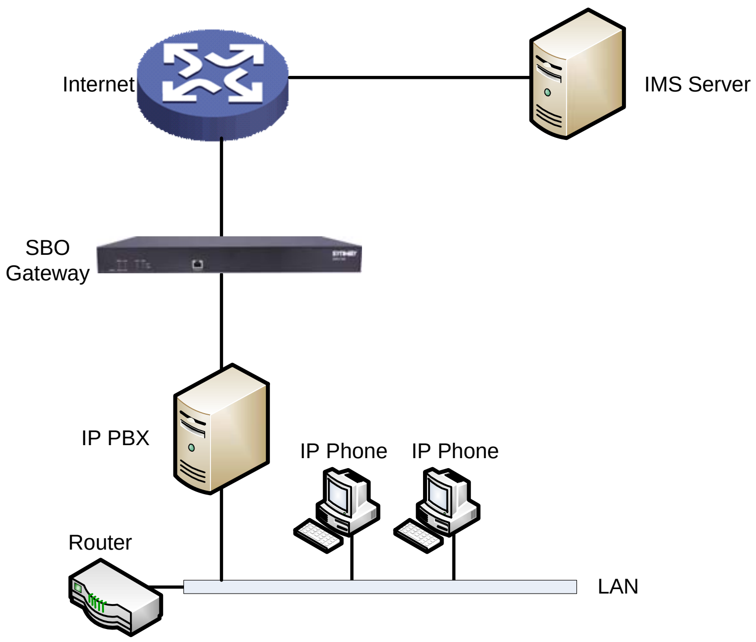


Figure 1-1 Typical Application

1.2 Feature List

Basic Features	Description
IP Call	Call initiated from IP to a designated SIP trunk, via routing and number manipulation.
Number Manipulation	Peels off some digits of a phone number from left/right, or adds a prefix/suffix to a phone number.
VoIP Routing	Routing path: from IP to IP.
Signaling & Protocol	**Description**
SIP Signaling	Supported protocol: SIP V1.0/2.0, RFC3261
Voice	CODEC: G.711A, G.711U, G.729, G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K) DTMF Mode: RFC2833, SIP INFO, INBAND, *RFC2833+Signaling*, *In-band+Signaling*
Network	**Description**
Network Protocol	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN
Static IP	IP address modification support
DNS	Domain Name Service support
Security	**Description**
Admin Authentication	Support admin authentication to guarantee the resource and data security
Maintain & Upgrade	**Description**
WEB Configuration	Support of configurations through the WEB user interface
Language	Chinese, English
Software Upgrade	Support of user interface, gateway service, kernel and firmware upgrades based on WEB
Tracking Test	Support of Ping and Tracert tests based on WEB
SysLog Type	Three options available: ERROR, WARNING, INFO

1.3 Hardware Description

The SBO gateway features 1U rackmount design and integrates embedded LINUX system within the POWERPC+DSP hardware architecture. It has 2 Kilomega-Ethernet ports (NET1 and NET2) on the chassis. See the figures below for product appearance：

Figure 1-2 Front View for SBO500

Figure 1-3 Rear View for SBO500

Figure 1-4 Left View for SBO500

Figure 1-5 Front View for SBO2000

Figure 1-6 Rear View for SBO2000

Figure 1-7 Left View for SBO2000

The table below gives a detailed introduction to the interfaces, buttons and LEDs illustrated above:

Interface	Description
NET	Amount: 2
	Type: RJ-45
	Bandwidth: 10/100/1000Mbps
	Self-Adaptive Bandwidth Supported
	Auto MDI/MDIX Supported
Console Port	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-8 for signal definition) , USB
	Data Bits: 8 bits
	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
Button	**Description**
Power Key	Power on/off the SBO gateway. You can turn on the two power keys at the same time to have the power supply working in the hot-backup mode.
Reset Button	Restore the gateway to factory settings.
LED	**Description**
Power Indicator	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
Run Indicator	Indicates the running status. For more details, refer to 1.4 Alarm Info.
Alarm Indicator	Alarms the device malfunction. For more details, refer to 1.4 Alarm Info.
Link Indicator	The green LED on the left of NET, indicating the network connection status.
ACT Indicator	The orange LED on the right of NET, whose flashing tells data are being transmitted.

Note: The console port is used for debugging. For the connection of SBO500, the transmitting and receiving lines of the gateway and the remote device should be cross-linked. That is, connect the transmitting line of the gateway to the receiving line of the remote device, and vice verse. The figure below illustrates the signal definition of the console port on the gateway.

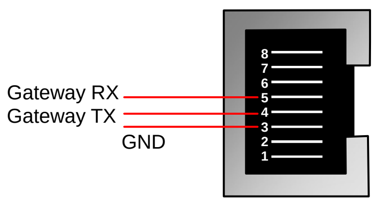


Figure 1-8 Console Port Signal Definition

The SBO2000 gateway is connected via a two male end USB cable which can convert to 8 consoles (each USB port converts to 4).

For other hardware parameters, refer to Appendix A Technical Specifications.

1.4 Alarm Info

The SBO gateway is equipped with two indicators denoting the system's running status: Run Indicator (green) and Alarm Indicator (red). The table below explains the states and meanings of the two indicators.

LED	State	Description
Run Indicator	Go out	System is not yet started.
	Light up	System is starting.
	Flash	Device is running normally.
Alarm Indicator	Go out	Device is working normally.
	Light up	Upon startup: Device is running normally. In runtime: Device goes abnormal.
	Flash	System is abnormal.

Note:

- The startup process consists of two stages: System Booting and Gateway Service Startup. The system booting costs about 1 minute and once it succeeds, both the run indicator and the alarm indicator light up. Then after the gateway service is successfully started and the device begins to work normally, the run indicator flashes and the alarm indicator goes out.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Go to Appendix C Technical/sales Support to find the contact way.

Chapter 2 Quick Guide

This chapter is intended to help you grasp the basic operations of the SBO gateway in the shortest time.

Step 1: Confirm that your packing box contains all the following things.

- SBO Series Gateway *1
- SBO500: Angle Bracket *2, Rubber Foot Pad *4, Screw for Angle Bracket *8; SBO2000: Rubber Foot Pad *6, Screw for Angle Bracket *8, Front Angle Plate *2, Back Angle Plate *2, Earth Wire *1, Shielded Straight Through Cable *2
- 220V Power Cord *2
- Warranty Card *1
- Installation Manual *1

Step 2: Properly fix the SBO gateway.

If you do not need to place the gateway on the rack, simply fix the rubber foot pads. Otherwise, for the SBO500 gateway, you should first fix the 2 angle brackets onto the chassis and then place the chassis on the rack; for the SBO2000 gateway, you should first fix the front angle plates onto the chassis and then fix the chassis on the rack with the help of the back angle plates.

Step 3: Connect the power cord.

Make sure the device is well grounded before you connect the power cord. Check if the power socket has the ground wire. If it doesn't, use the grounding stud on the rear panel of the device (See Figure 1-3) for earthing.

Note: Each SBO gateway has two power interfaces to meet the requirement for power supply hot backup. As long as you properly connect and turn on these two power keys, either power supply can guarantee the normal operation of the gateway even if the other fails.

Step 4: Connect the network cable.

Step 5: Log in the gateway.

Enter the original IP address (NET 1: 192.168.1.101 or NET 2: 192.168.0.101) of the SBO gateway in the browser to go to the WEB interface. The original username and password of the gateway are both 'admin'. For detailed instructions about login, refer to 3.1 System Login. We suggest you change the initial username and password via 'System Tools → Change Password' on the WEB interface as soon as possible after your first login. For detailed instructions about changing the password, refer to 3.7.18 Change Password. After changing the password, you are required to log in again.

Step 6: Modify IP address of the gateway.

You can modify the IP address of the gateway via 'System Tools → Network' on the WEB interface to put it within your company's NET. Refer to 3.7.1 Network for detailed instructions about IP modification. After changing the IP address, you shall log in the gateway again using your new IP address.

Step 7: Check the channel status.

You can check the status of the channels via 'Operation Info → IP Status'. Refer to 3.2.2 IP Status for detailed introductions.

Step 8: Set routing rules for calls.

Note: For your easy understanding and manipulation, all examples given in this step do not involve registration.

Step 1: Configure the IP address of the remote SIP terminal which can establish conversations with the gateway so that the calls from other terminals will be ignored. Refer to 'SIP Settings → SIP Trunk' for detailed instructions. Click **Add New** to add a new SIP trunk, fill in 'Remote IP' and 'Remote Port' with the IP address and port of the remote SIP terminal which will initiate calls to the gateway. You may use the default values for the other configuration items.

Example: Provided the incoming IP address of the SIP trunk is 192.168.0.111 and the port is 5060. Add **SIP Trunk 0**; set **Remote IP** to **192.168.0.111** and **Remote Port** to **5060**. The outgoing IP address of the SIP trunk is 192.168.0.222 and the port is 5060. Add **SIP Trunk 1**; set **Remote IP** to **192.168.0.222** and **Remote Port** to **5060**.

Step 2: Add the IP address of the SIP trunks configured in Step 1 into the corresponding SIP trunk group. Refer to SIP Settings → SIP Trunk Group' for detailed instructions. Click **Add New** to add the SIP trunk group. Select the SIP trunk configured in Step 1 as 'SIP Trunks'. You may use the default values for the other configuration items.

Example: Add **SIP Trunk Group 0**. Check the checkbox before **0** for **SIP Trunks** and keep the default values for the other configuration items. Add **SIP Trunk Group 1**. Check the checkbox before **1** for **SIP Trunks** and keep the default values for the other configuration items.

Step 3: Add routing rules. Refer to 'Route Settings → IP→IP' for detailed instructions. Select the SIP trunk group 0 set in Step 2 as 'Call Initiator' and the SIP trunk group 1 set in Step 2 as 'Call Destination'. You may use the default values for the other configuration items.

Example: Select **SIP Trunk Group[0]** as **Call Initiator** and **SIP Trunk Group[1]** as **Call Destination.** Keep the default values for the other configuration items.

Step 4: Initiate a call from the SIP trunk 0 configured in Step 1 to the IP address and port of the SBO gateway. Thus you can establish a call conversation via SIP trunk[1] with the IP terminal. (Note: The format used for calling an IP address via SIP trunk is as follows: username@IP address.)

Example: Provided the IP address of the SBO gateway is 192.168.0.101 and the port is 5060. Provided 123 is a number which conforms to the number receiving rule of the remote device. Initiate a call from SIP trunk 0 to the IP address 192.168.0.101 (in the format: 123@192.168.0.101) and you can establish a call conversation via SIP trunk[1] to the number 123.

Special Instructions:

- The chassis of the SBO gateway must be grounded for safety reasons, according to standard industry requirements. A simple way is earthing with the third pin on the plug or the grounding studs on the machine. No or improper grounding may cause instability in operation as well as decrease in lightning resistance.
- As the device will gradually heat up while being used, please maintain good ventilation to prevent sudden failure, ensuring that the ventilation holes (see Figure 1-4) are never jammed.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Otherwise it may lead to a drop in performance or unexpected errors.

Chapter 3 WEB Configuration

3.1 System Login

Type the IP address into the browser and enter the login interface. See Figure 3-1.

Figure 3-1 Login Interface

The gateway only serves one user, whose original username and password are both 'admin'. You can change the username and the password via 'System Tools → Change Password' on the WEB interface. For detailed instructions, refer to 3.7.18 Change Password.

After login, you can see the main interface as below.

Figure 3-2 Main Interface

3.2 Operation Info

Operation Info includes five parts: ***System Info***, ***IP Status***, ***Call Count***, ***Call Count*** and ***Warning Info***, showing the current running status of the gateway. See Figure 3-3.

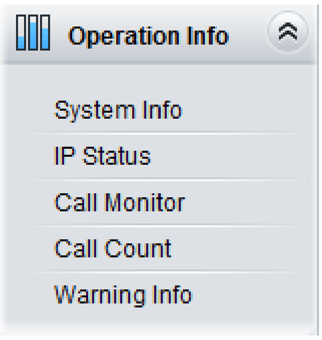


Figure 3-3 Operation Info

3.2.1 System Info

Figure 3-4 System Info Interface

See Figure 3-4 for the system info interface. You can click ***Refresh*** to obtain the latest system information. The table below explains the items shown in Figure 3-4.

Item	Description
MAC Address	MAC address of NET 1 or NET 2.
IP Address	The three parameters from left to right are IP address, subnet mask and default gateway of NET 1 or NET 2.
DNS Server	DNS server address of NET 1 or NET 2.
Receive Packets, Transmit Packets	The amount of receive/transmit packets after the gateway's startup, including three categories: All, Error and Drop.

Current Speed	The current speed of data receiving and transmitting.
Work Mode	The work mode of the network, including six options: 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 1000 Mbps Full Duplex and Disconnected.
Runtime	Time of the gateway keeping running normally after startup. This parameter updates every 2s.
CPU Temperature	Display the real time temperature of the CPU.
CPU Usage Rate	Display the real time usage rate of the CPU.
Current RTP Message Data	Display the receiving and sending information of the current RTP data.
Serial Number	Unique serial number of a SBO gateway.
WEB	Current version of the WEB interface.
Gateway	Current version of the gateway service.
Uboot	Current version of Uboot.
Kernel	Current version of the system kernel on the gateway.
Firmware	Current version of the firmware on the gateway.

3.2.2 IP Status

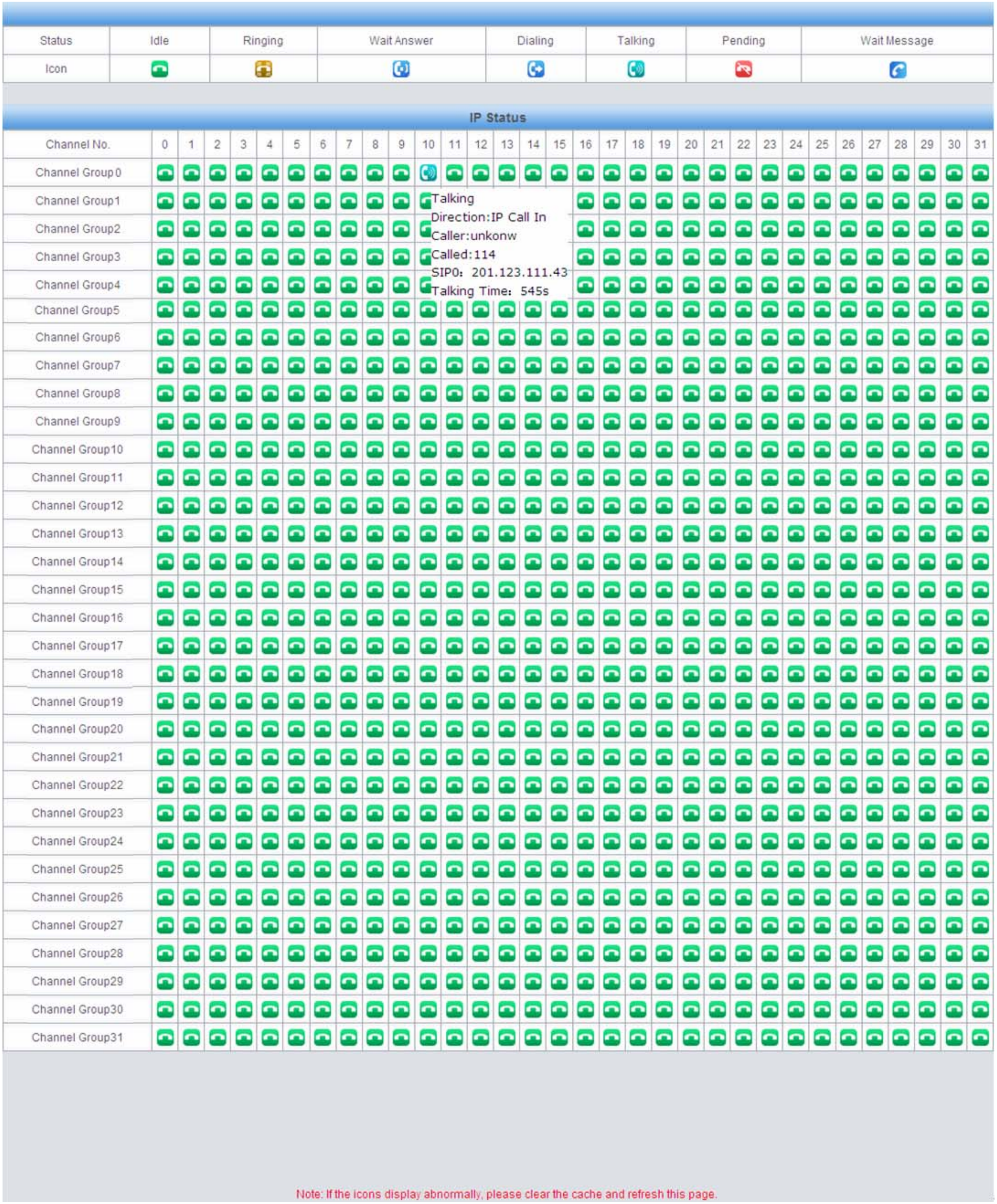


Figure 3-5 IP Status Interface

See Figure 3-5 for the IP status interface which shows the real-time status of each IP channel on the gateway.

Item	Description
Channel No.	The corresponding serial number of IP on the device.
State	Displays the channel state in real time. You can move the mouse onto the channel state icon for detailed information about the channel and the call, such as: call

direction, calling party number and called party number. The channel states include:

State	Icon	Description
Idle		The channel is available.
Wait Answer		The channel receives the ringback tone and is waiting for the called party to pick up the phone.
Ringing		The channel is in the ringing state.
Talking		The channel is in a conversation.
Pending		The channel is in the pending state
Dialing		The channel is dialing.
Wait Message		The channel is waiting for the message from remote PBX.

Note: The gateway provides the fuzzy search feature on this interface. After you click any characters on Figure 3-5 and press the 'F' button, the search box will emerge on the right top of this page. Then you can input the key characters and the gateway will locate the channel on which there is an ongoing call that conforms to the fuzzy search condition.

Take an example: As shown in Figure 3-6, after we input the character 114 to the search box, and click the ***Search*** button, the gateway does a fuzzy search and locates that the ongoing call whose CalledID contains the character 114 occurs on Channel 10 of Channel Group 1.

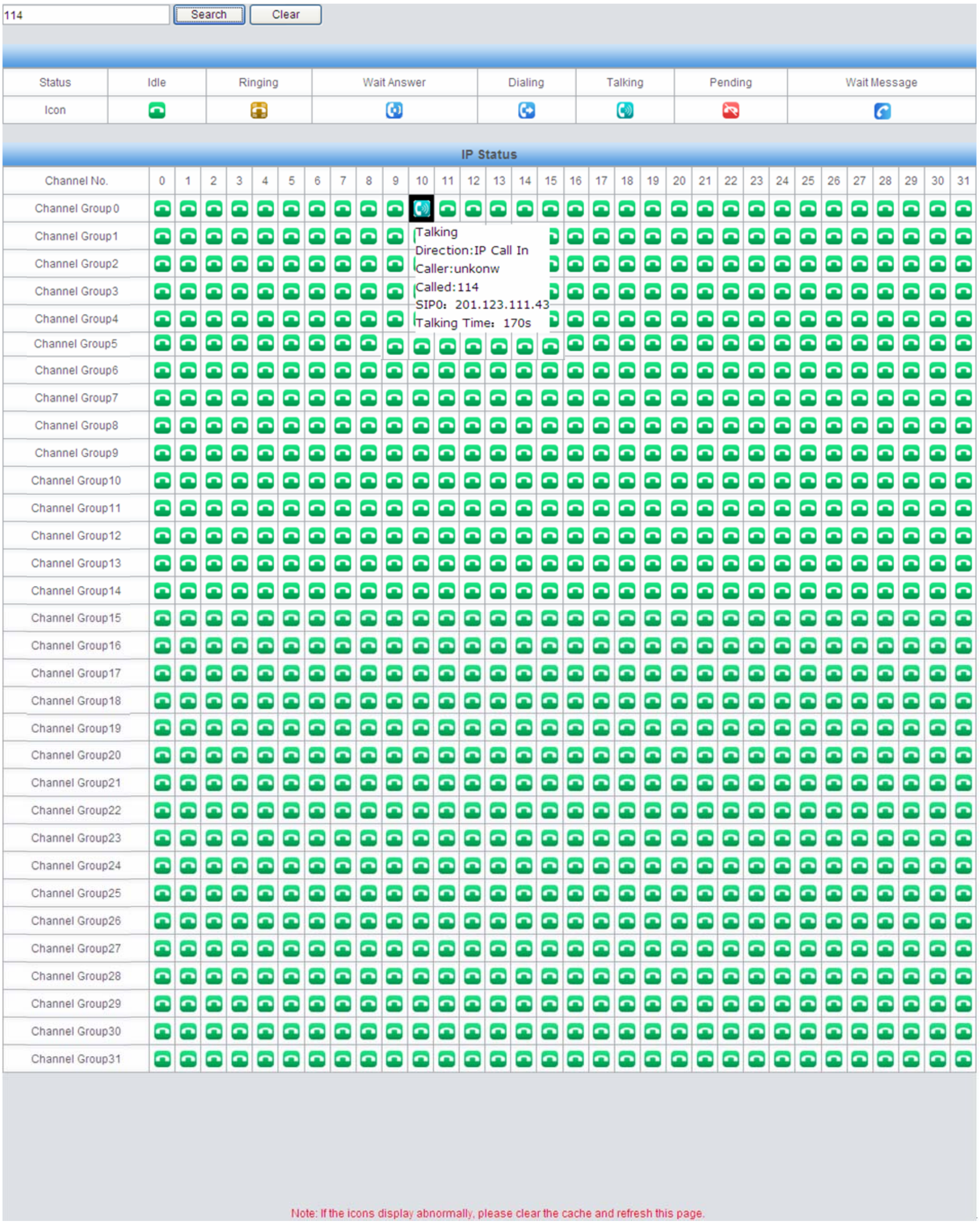


Figure 3-6 Search Calls

3.2.3 Call Monitor

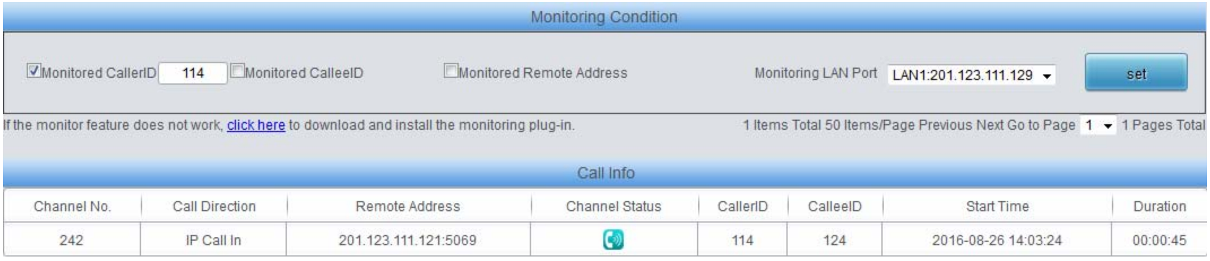


Figure 3-7 Call Monitor Interface

See Figure 3-7 for the call monitor Interface. Here you can set a condition for call monitoring. For example, as shown in Figure 3-7, set the CallerID 114 as the monitoring condition, and after you click the ***Set*** button, all the calls containing the CallerID 114 will display in the Call Info list. The table below explains the items shown in Figure 3-7.

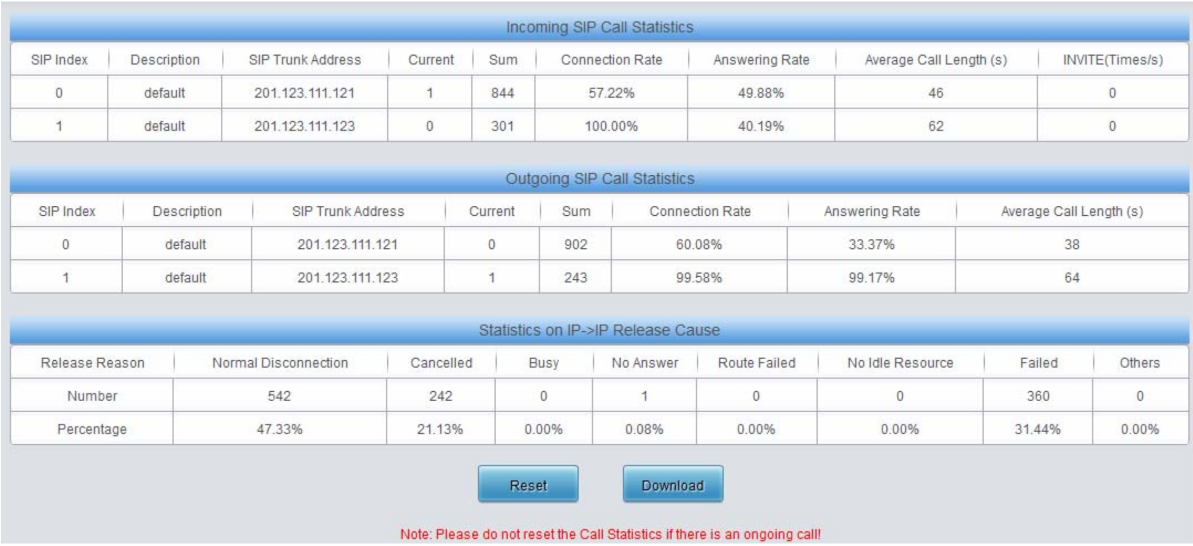
Item	Description
Monitored CallerID, Monitored CalleeID, Monitored Remote Address	Sets the condition for the call monitoring. You can set to monitor the calls by CallerID, CalleeID or remote address.
Monitoring LAN Port	Selects the LAN port which is used to monitor the calls.
Channel No.	The number of the channel, which starts from 0.
Call Direction	The direction of the monitored call.
Remote Address	The remote address of the monitored call.
Channel Status	The status of the channel which the monitored call locates at.
CallerID	The CallerID of the monitored call.
CalleeID	The CalleeID of the monitored call.
Start Time	The start time of the monitored call.
Duration	The duration of the monitored call.

Click the icon in the channel status column, and you can monitor the call in real-time. If your computer is not installed with the monitoring plug-in, click the icon and you will see a prompt asking you to set the security level. Follow the instructions to configure the IE explorer: Open it and click 'Tools > Internet Options >Security Tab'; then click 'Custom Level' and enable 'Initialize and script ActiveX controls not marked as safe for scripting'. If there is a shadow showing under the icon, such as '', it means the monitoring goes successful. Click the icon again to cancel the monitoring.

Note: If a channel has been monitored from the very beginning, the monitoring, even if not yet cancelled, will terminate once the channel is removed from the monitor list.

Note: This feature is unavailable for SBO2000.

3.2.4 Call Count



Incoming SIP Call Statistics

SIP Index	Description	SIP Trunk Address	Current	Sum	Connection Rate	Answering Rate	Average Call Length (s)	INVITE(Times/s)
0	default	201.123.111.121	1	844	57.22%	49.88%	46	0
1	default	201.123.111.123	0	301	100.00%	40.19%	62	0

Outgoing SIP Call Statistics

SIP Index	Description	SIP Trunk Address	Current	Sum	Connection Rate	Answering Rate	Average Call Length (s)
0	default	201.123.111.121	0	902	60.08%	33.37%	38
1	default	201.123.111.123	1	243	99.58%	99.17%	64

Statistics on IP->IP Release Cause

Release Reason	Normal Disconnection	Cancelled	Busy	No Answer	Route Failed	No Idle Resource	Failed	Others
Number	542	242	0	1	0	0	360	0
Percentage	47.33%	21.13%	0.00%	0.08%	0.00%	0.00%	31.44%	0.00%

Reset Download

Note: Please do not reset the Call Statistics if there is an ongoing call!

Figure 3-8 Call Count Interface

See Figure 3-8 for the call count Interface. The above list shows the detailed information about all the calls counted from the startup of the gateway service to the latest open or refresh of this interface. You can click ***Reset*** to count the call information again, click ***Download*** to download the call count logs. The table below explains the items shown in Figure 3-8.

Item	Description
SIP Index	The index of the SIP trunk.
Description	More information about each SIP trunk group.
SIP Trunk Address	Address of the SIP trunk, i.e. the IP address or domain name of the remote SIP terminal which will establish a call conversation with the gateway.
Current	The number of the current incoming/outgoing SIP calls.
Sum	The total number of the incoming SIP calls/ outgoing SIP calls/ IP→ PSTN calls/ PSTN→ IP calls.
Connection Rate	The percentage of successful calls to total calls by all method. The call methods include SIP Incoming Call, SIP Outgoing Call, IP→ PSTN call and PSTN→ IP call.
Answering Rate	The percentage of answered calls to total calls by all methods. The call methods include SIP Incoming Call, SIP Outgoing Call, IP→ PSTN call and PSTN→ IP call.
Average Call Length	The average call length for all connected calls.
INVITE	The number of the invite messages received per second.
Release Reason	Reason to release the call.
Normal Disconnection	Total number of the calls which are normally cleared. The corresponding SIP status code is 200.
Cancelled	Total number of the calls which are cancelled by the calling party. The corresponding SIP status code is 487.
Busy	Total number of the calls which fail as the called party has been occupied and replies a busy message. The corresponding SIP status code is 603.

No Answer	Total number of the calls which fail as the called party does not pick up the call in a long time or the calling party hangs up the call before the called party picks it up. The corresponding SIP status code is 403.
Routing Failed	Total number of the calls which fail because no routing rules are matched. The corresponding SIP status code is 488.
No Idle Resource	Total number of the calls which fail because no voice channel is available. The corresponding SIP status code is 486.
Failed	Total number of the calls which fail as the called party number does not conform to the number-receiving rule or for relative reasons. The corresponding SIP status code is other 4xx, 5xx, 6xx.
Others	Total number of the calls which fail because of other reasons. The corresponding SIP status code is 493.
Number	Total number of the calls on each state.
Percentage	The percentage of the calls with a release cause to total calls.

Note: This feature is unavailable for SBO2000.

3.2.5 Warning Information

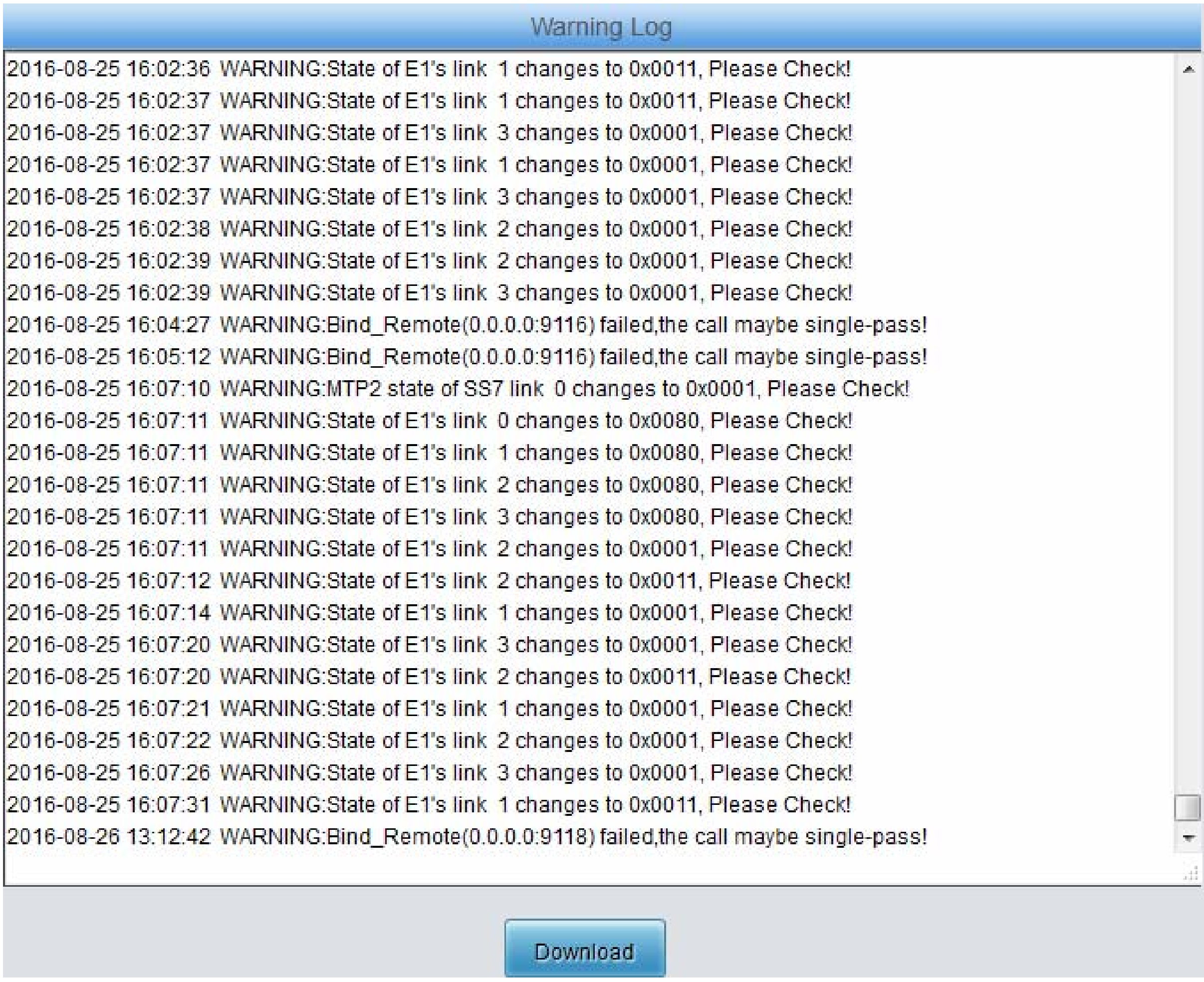


Figure 3-9 Warning Information Interface

See Figure 3-9 for the Warning Information interface. All the warning information will be output and displayed on this interface.

3.3 SIP Settings

SIP Settings includes six parts: ***SIP***, ***SIP Trunk***, ***SIP Register***, ***SIP Account***, ***SIP Trunk Group*** and ***Media***. See Figure 3-10. ***SIP*** is used to configure the general SIP parameters; ***SIP Trunk*** is used to set the basic and register information of the SIP trunk; ***SIP Register*** is used for the registration of SIP; ***SIP Account*** is used for registering SIP accounts to the SIP server; ***SIP Trunk Group*** is to manage SIP trunks by group; and ***Media*** is to set the RTP port and the payload type.

Figure 3-10 SIP Settings

3.3.1 SIP Settings

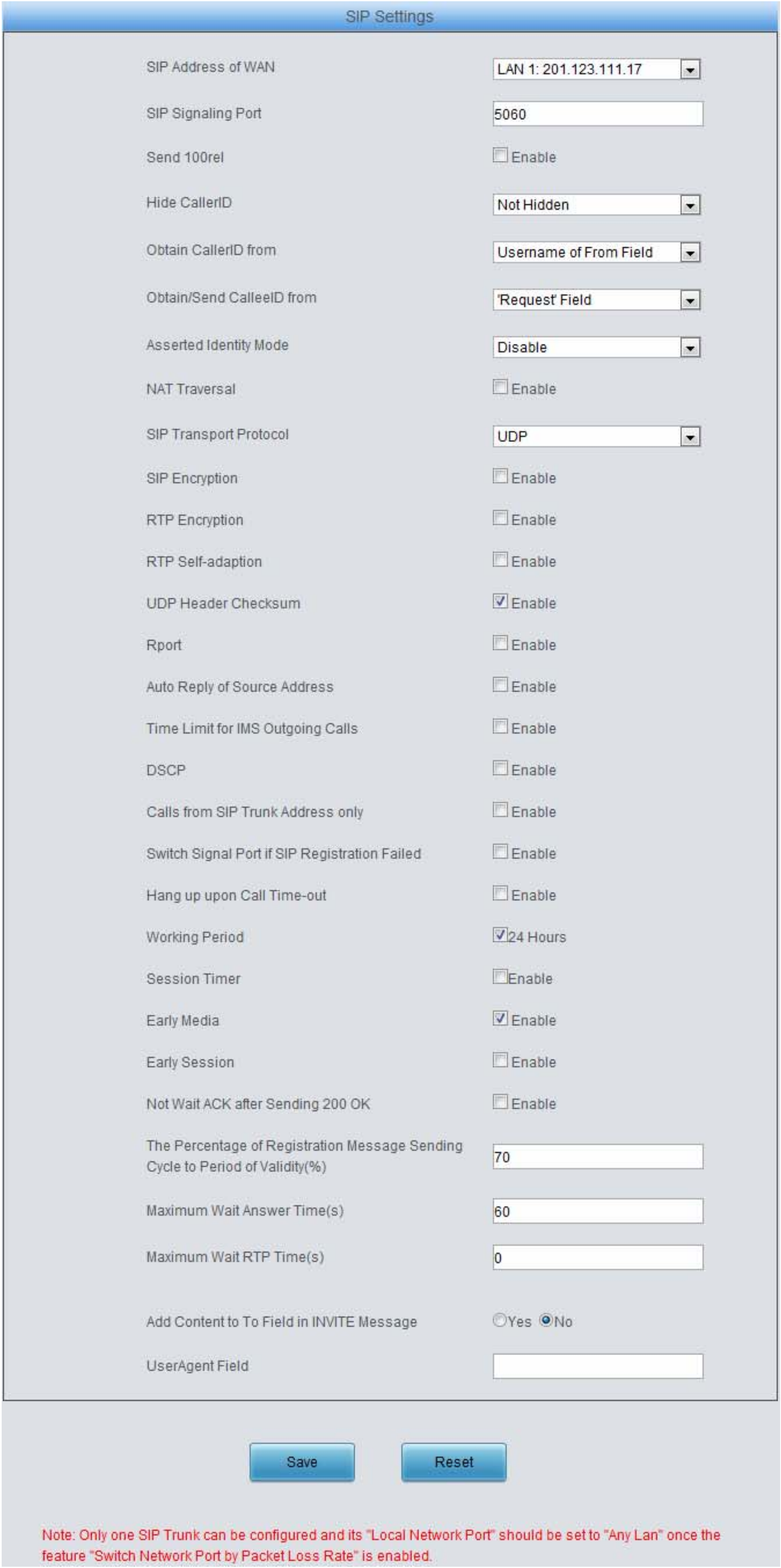

SIP Settings
SIP Address of WAN
LAN 1: 201.123.111.17
SIP Signaling Port
5060
Send 100rel
Enable
Hide CallerID
Not Hidden
Obtain CallerID from
Username of From Field
Obtain/Send CalleeID from
'Request' Field
Asserted Identity Mode
Disable
NAT Traversal
Enable
SIP Transport Protocol
UDP
SIP Encryption
Enable
RTP Encryption
Enable
RTP Self-adaption
Enable
UDP Header Checksum
Enable
Rport
Enable
Auto Reply of Source Address
Enable
Time Limit for IMS Outgoing Calls
Enable
DSCP
Enable
Calls from SIP Trunk Address only
Enable
Switch Signal Port if SIP Registration Failed
Enable
Hang up upon Call Time-out
Enable
Working Period
24 Hours
Session Timer
Enable
Early Media
Enable
Early Session
Enable
Not Wait ACK after Sending 200 OK
Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%)
70
Maximum Wait Answer Time(s)
60
Maximum Wait RTP Time(s)
0
Add Content to To Field in INVITE Message
Yes No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 3-11 SIP Settings Interface

See Figure 3-11 for the SIP settings interface where you can configure the general SIP parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.7.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-11.

Item	Description
SIP Address of WAN	IP address of SIP signaling for WAN, using NET 1 by default.
SIP Signaling Port	Monitoring port of SIP signaling. Range of value: 2000~65535, with the default value of 5060. **Note:** The value range of this configuration item and that of the RTP port set in Media Settings cannot be overlapped.
Send 100rel	Sets whether to send the 100rel field, with the default value of disabled.
Hide CallerID	Sets whether to hide the CallerID, with the default value of *Not Hidden*.
Obtain CallerID from	There are two optional ways to obtain the calling party number: from Username of “From” Field or from Displayname of “From” Field. The default value is from *Username of “From” Field*.
Obtain/Send CalleeID from	There are two optional ways to obtain or send the called party number: from “To” Field or from “Request” Field. The default value is from “*Request” Field*.
Asserted Identity Mode	Sets whether to have the invite message include some header information, two options available now: P-Asserted-Identity and P-Preferred-Identity. The default value is *disabled*.
Number in From Field not Manipulated	Once this feature is enabled, the callerID in the From field will not be manipulated, with the default value of *disabled*. **Note:** It is valid only when the configuration item Asserted Identity Mode is enabled.
NAT Traversal, Traversal Type	Sets whether to enable the NAT traversal. By default this feature is disabled. There is only one traversal type: *Port Mapping*.
LAN1 Mapping Address, LAN2 Mapping Address	The mapping addresses of LAN1 and LAN2 in case the NAT traversal is enabled. If the port mapping is selected as the traversal type, you are required to set the mapping address on the router and fill in the corresponding information here as well. By default, only the IP address need be filled in, and the port value is just the same as the SIP signaling port.
Always Use Mapping Address	Once this feature is enabled, the gateway will be enforced to use the mapping address set in the above configuration item to initiate calls. By default it is *disabled*.
SIP Transport Protocol	There are two modes *UDP* and *TCP* available for running the SIP protocol. The default value is *UDP*. **Note:** This item is unsupported by SBO2000.
SIP Encryption	Once this feature is enabled, you can encrypt the SIP signal following selecting an encryption criterion and setting a key. By default it is *disabled*.
Encryption Criterion	The criterion used to encrypt the SIP signal. At present only VOS1.1 is supported.

Key	The key to encrypt the SIP signal.
RTP Encryption	Once this feature is enabled, you can encrypt the RTP package. By default it is *disabled*.
RTP Self-adaption	When this feature is enabled, the RTP reception address or port carried by the signaling message from the remote end, if not consistent with the actual state, will be updated to the actual RTP reception address or port. By default, this feature is *disabled*.
UDP Header Checksum	When this feature is enabled, the gateway will automatically calculate the check sum of the UDP header during RTP transmission.
Rport	When this feature is enabled, a corresponding Rport field will be added to the Via message of SIP. Meanwhile, the IP address and the port of the outer network will be filled into the CONTACT and VIA fields. By default, it is *disabled*.
Auto Reply of Source Address	Once this feature is enabled, the source address will be used by the gateway in its reply message, with the default value of *disabled*.
Time Limit for IMS Outgoing Calls	Once this feature is enabled, The gateway can set the time limit for the outgoing calls from the SIP registered account, with the default value of *disabled*. **Note:** This item is unsupported by SBO2000..
Rated Time	The limited time for the calls from the SIP registered account.
SIP Registered Number Polling	Once this feature is enabled, the registered account will carry out the call in a polling mode, with the default value of *disabled*.
DSCP	Sets whether to enable the DSCP differentiated services code point. By default, it is *disabled*.
Voice Media	Sets the priority of the voice media for DSCP. The voice media with a bigger value has a higher priority. The value range is 0~63, with the default value of *46*.
Signal Control	Sets the priority of the signal control for DSCP. The signal control with a bigger value has a higher priority. The value range is 0~63, with the default value of *26*.
Calls from SIP Trunk Address only	Once this feature is enabled, the gateway will only accept the calls from the IP addresses set in SIP Settings → SIP Trunk. By default, it is *disabled*.
Switch Signal Port if SIP Registration Failed	If the SIP registration fails, the SIP signaling port N will switch to N+1 for a new registration. It will continue until the registration succeeds. **Note:** This item is unsupported by SBO2000..
Hang up if a Call Time-out	Sets whether to enable the feature to hang up the call once it is time-out, with the default value of *No*,
Maximum Call Overtime	Sets the maximum overtime for a call. Calculated by minute.
Working Period, Period	The work period for the gateway. You can specify a certain period for the gateway to make calls. By default, the gateway is allowed to make calls any time in the day (24 Hours).

Session Timer	Sets whether to enable the session refresh feature, with the default value of *disabled*. Once this feature is enabled, you are required to enter the minimum time and the timeout value.
Minimum Time	Sets the minimum time for refreshing the session. Value of range: 90~65535, with the default value of *150*.
Timeout	Sets the timeout value for refreshing the session. The value cannot be less than that of Minimum Time, with the default value of *600*.
Early Media	Once this feature is enabled, the P-Early-Media field will be included in the Invite message. The default value is *disabled*.
Early Session	Once this feature is enabled, the early-session field will be included in the Invite message. The default value is *disabled*.
Not Wait ACK after Sending 200 OK	Once this feature is enabled, the gateway does not need to wait the ACK message after sending the 200OK message. The default value is *disabled*.
The Percentage of Registration Message Sending Cycle to Period of Validity	Sets the percentage of the sending cycle of the SIP registration message to the validity period. Value of range: 1~200, with the default value of *70*.
Maximum Wait Answer Time	Sets the maximum time for the SIP channel to wait for the answer from the called party of the outgoing call it initiates. If the call is not answered within the specified time period, it will be canceled by the channel automatically. The default value is 60, calculated by s.
Maximum Wait RTP Time	Sets the maximum time for the SIP channel to wait for the RTP packet. If no RTP packet is received within the specified time period, the channel will enter the pending state automatically and release the call. The default value is 0, calculated by s.
Add Content to To Field in INVITE Message	Once this feature is enabled, “user=phone” will be added to the TO field of the INVITE message. The default value is *disabled*.
Add Content	Sets the content to add to the TO field.
UserAgent Field	Sets the content of the UserAgent field. Currently, it only supports the English uppercase and lowercase letters.

3.3.2 SIP Trunk

By default, there is no available SIP trunk information. Click ***Add New*** to add a new SIP trunk. See Figure 3-12 for the SIP trunk adding interface.

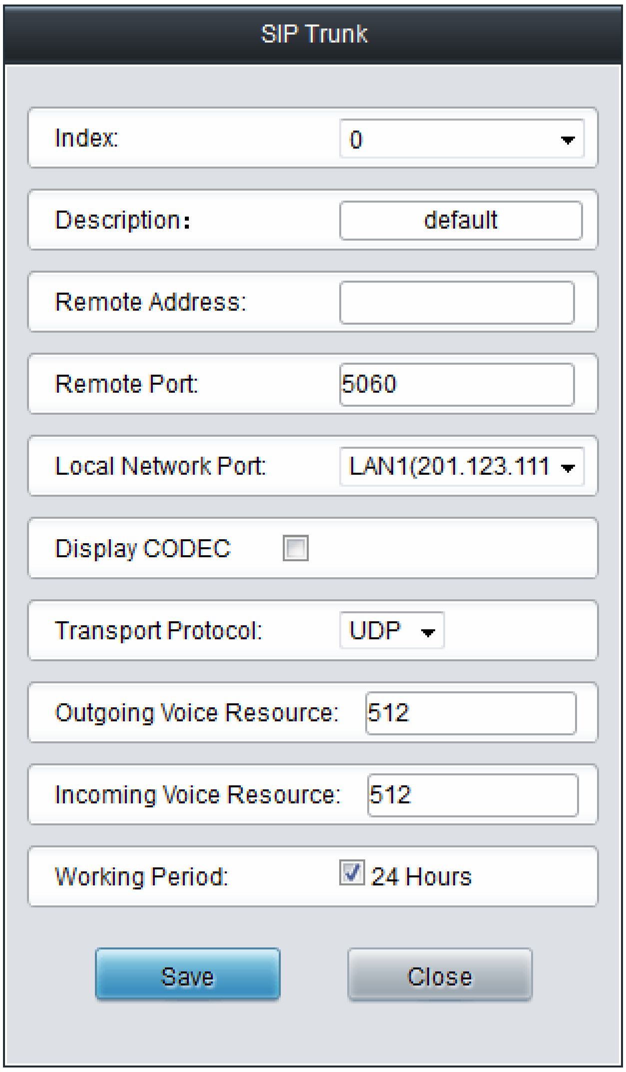


Figure 3-12 Add New SIP Trunk

The table below explains the items shown in Figure 3-12.

Item	Description
Index	The unique index of each SIP trunk.
Description	More information about each SIP trunk group.
Remote Address	Address of the SIP trunk, i.e. the IP address or domain name of the remote SIP terminal which will establish call conversation with the gateway.
Remote Port	Port of the SIP trunk.
Local Network Port	The network port where the SIP trunk locates.
Transport Protocol	SIP transport protocol, providing two modes *UDP* and *TCP*. The default value is *UDP*.
Outgoing Voice Resource	Maximum number of voice channels for the outgoing calls allocated by the SIP trunk to the gateway.
Incoming Voice Resource	Maximum number of voice channels for the incoming calls allocated by the SIP trunk to the gateway.

<table>
<tr><td>Working Period, Period</td><td>The work period for the gateway, You can specify a certain period for the gateway to make calls. By default, the gateway is allowed to make calls any time in the day (24 Hours).</td></tr>
<tr><td>Display CODEC</td><td>Supported CODECs and their corresponding priorities for the SIP trunk to establish a call conversation. The table below explains the sub-items:
<table>
<tr><th>Sub-item</th><th>Description</th></tr>
<tr><td>Priority</td><td>Priority for choosing the CODEC in an SIP conversation. The smaller the value is, the higher the priority will be.</td></tr>
<tr><td>CODEC</td><td>Seven optional CODECs are supported: G711A, G711U, G729, G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K).</td></tr>
</table>
See 3.3.6 Media Settings for the detailed parameters for each CODEC.
The default CODEC for the SIP trunk is the same as that set in 3.3.6 Media Settings.</td></tr>
</table>

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-13 for the SIP Trunk Settings Interface

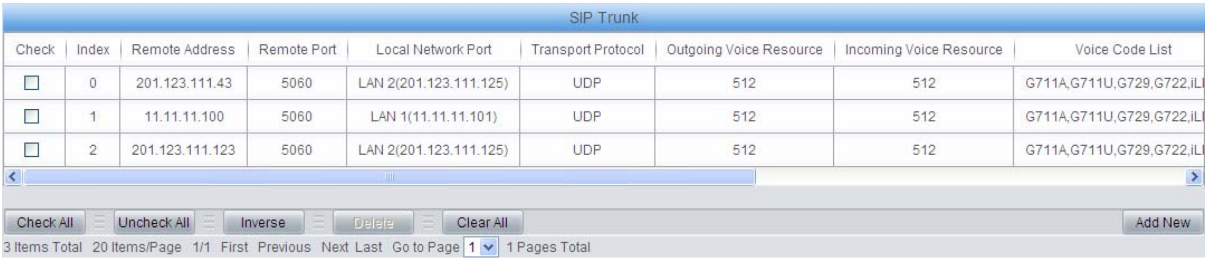


Figure 3-13 SIP Trunk Settings Interface

Click ***Modify*** in Figure 3-13 to modify a SIP trunk. See Figure 3-14 for the SIP trunk modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Trunk*** interface.

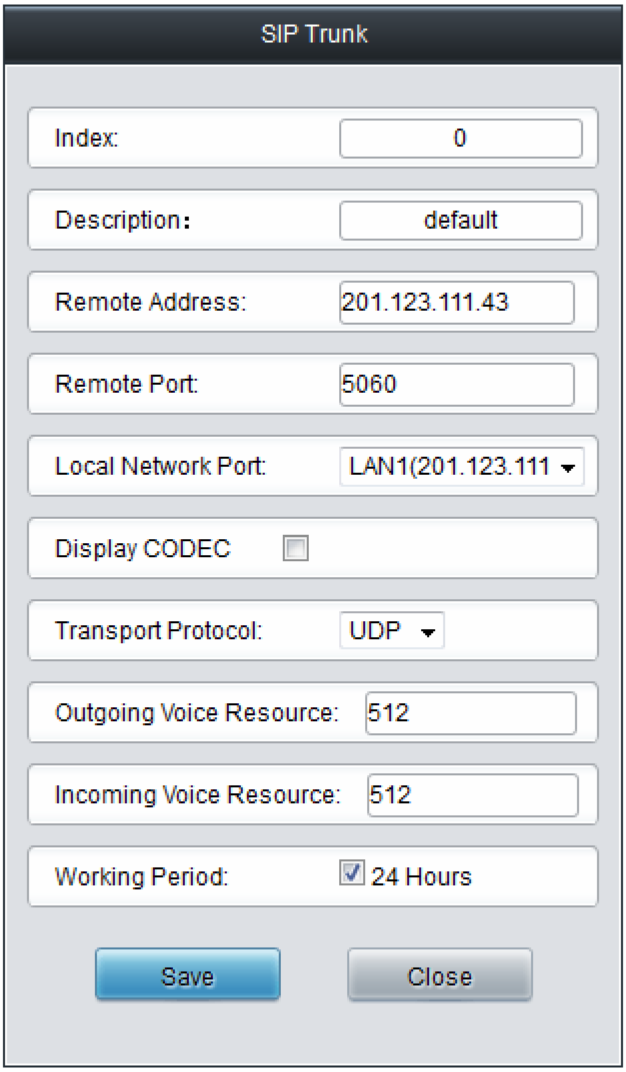


Figure 3-14 Modify SIP Trunk

To delete a SIP trunk, check the checkbox before the corresponding index in Figure 3-13 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP trunks at a time, click the ***Clear All*** button in Figure 3-13.

3.3.3 SIP Register

By default, there is no SIP register available on the gateway. Click ***Add New*** to add them manually. See Figure 3-15.

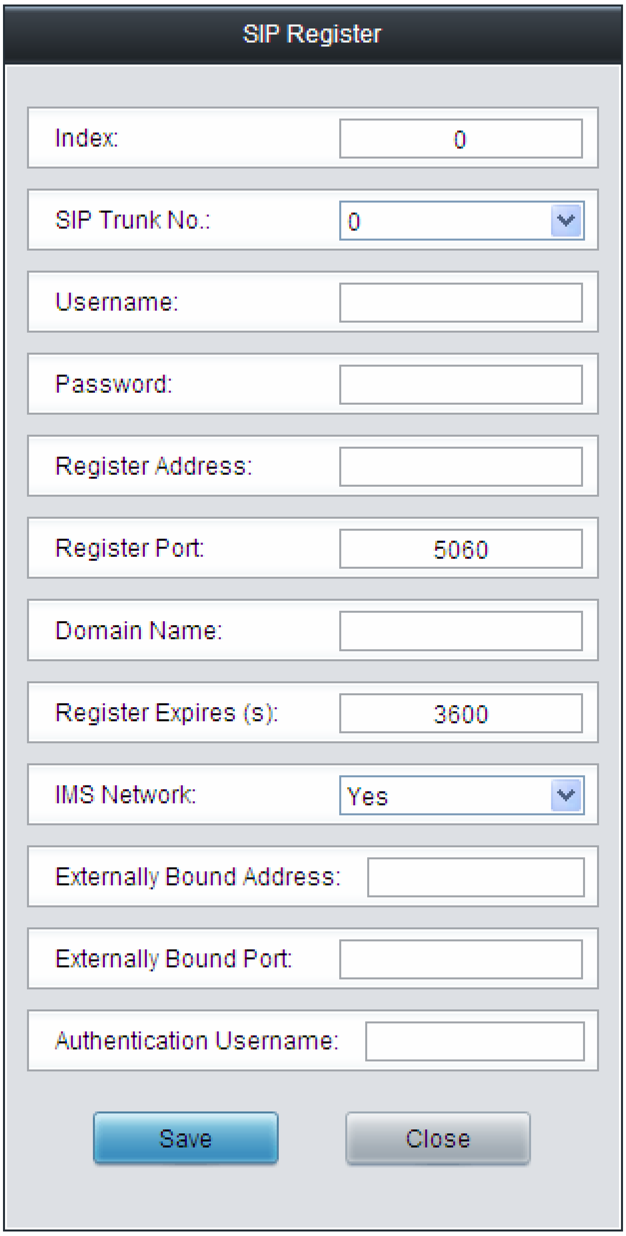


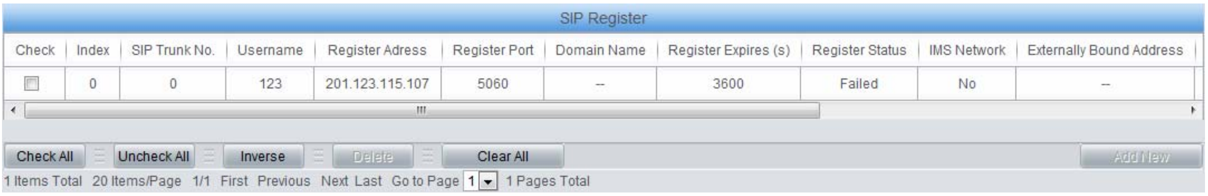
Figure 3-15 Add SIP Register Interface

The table below explains the items shown in the above figure.

Item	Description
Index	The unique index of each SIP register.
SIP Trunk No.	The number of the SIP trunk which registers to the SIP server.
Username	When the gateway initiates a call to SIP, this item corresponds to the username of SIP; when the gateway initiates a call to IP, this item corresponds to the displayed CallerID.
Password	Registration password of the gateway. To register the gateway to the SIP server, both configuration items ***Username*** and ***Password*** should be filled in.
Register Address	Address of the SIP server to which the SIP trunk is registered.
Register Port	The signaling port of the SIP trunk.
Domain Name	Domain name of the gateway used for SIP registry.

Register Expires	Validity period of the SIP registry. Once the registry is overdue, the gateway should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
IMS Network	Once this feature is enabled, the gateway will send signaling messages to the corresponding externally bound address and port when it registers to the server. Only when this feature is *enabled* will these items **Externally Bound Address**, **Externally Bound Port** and **Authentication Username** be shown.
Externally Bound Address	Externally bound IP address for registration.
Externally Bound Port	Externally bound port for registration.
Authentication Username	Authentication username for registration.
Remaining Time	Sets the remaining available time for this SIP account to make calls. **Note:** This configuration item will be displayed only when the configuration item “Time Limit for IMS Outgoing Calls” under SIP Settings is enabled.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-16 for the SIP Register Information List.


SIP Register

Check	Index	SIP Trunk No.	Username	Register Adress	Register Port	Domain Name	Register Expires (s)	Register Status	IMS Network	Externally Bound Address
☐	0	0	123	201.123.115.107	5060	--	3600	Failed	No	--

Check All | Uncheck All | Inverse | Delete | Clear All | Add New

1 Items Total 20 Items/Page 1/1 First Previous Next Last Go to Page 1 1 Pages Total

Figure 3-16 SIP Register Information List

Click ***Modify*** in Figure 3-16 to modify a SIP register. The configuration items on the SIP Register Modification Interface are the same as those on the ***Add New SIP Register*** interface.

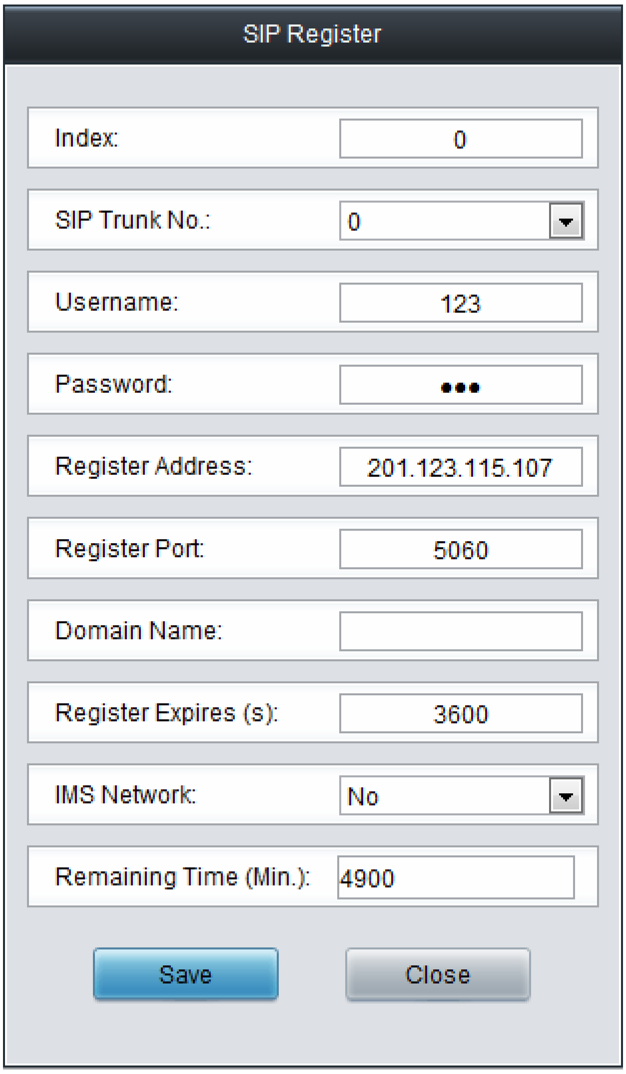


Figure 3-17 SIP Register Modification Interface

To delete a SIP register, check the checkbox before the corresponding index in Figure 3-16 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP registers at a time, click the ***Clear All*** button in Figure 3-16.

3.3.4 SIP Account

By default, there is no SIP account available on the gateway. Click ***Add New*** to add them manually. See Figure 3-18.

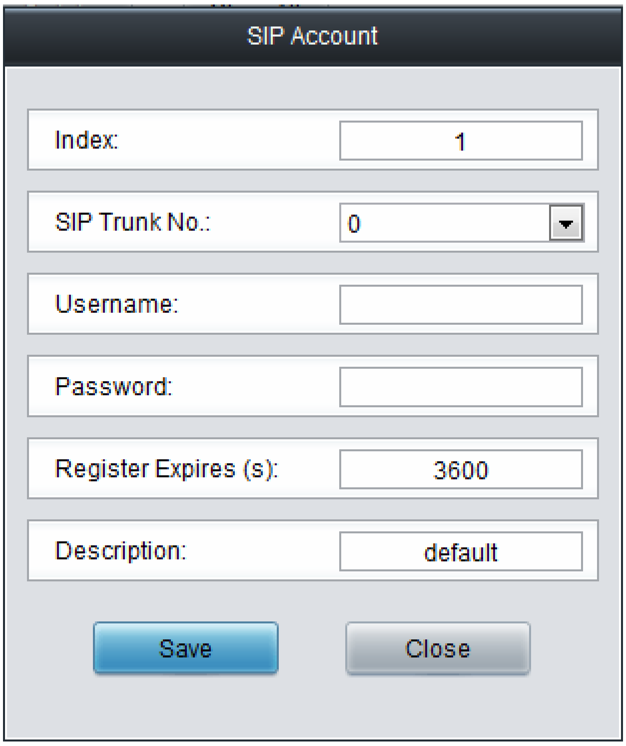


Figure 3-18 Add New SIP Account

The table below explains the items shown in above figures.

Item	Description
Index	The unique index of each SIP account.
SIP Trunk No.	The number of the SIP trunk to which the SIP account is registered.
Username	The registration username of the SIP account. Once the SIP account is successfully registered, the SIP server can initiate calls to the gateway via ***Username***.
Password	The registration password of the SIP account. To register the SIP account to the SIP trunk, both configuration items ***Username*** and ***Password*** should be filled in.
Register Expires	The validity period of the SIP account registry. Once the registry is overdue, the SIP account should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
Register Status	The registration status of the SIP account. It is either *Registered* or *Failed*.
Authentication Username	Authentication username of a port, used to register the port to the SIP server when IMS network is enabled. **Note: This item appears only when IMS Network is enabled on the SIP trunk corresponding to this SIP account.**
Description	More information about each SIP account.
Remaining Time	Sets the remaining available time for this SIP account to make calls. **Note:** This configuration item will be displayed only when the configuration item “Time Limit for IMS Outgoing Calls” under SIP Settings is enabled.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-19 for the SIP Account Settings Interface

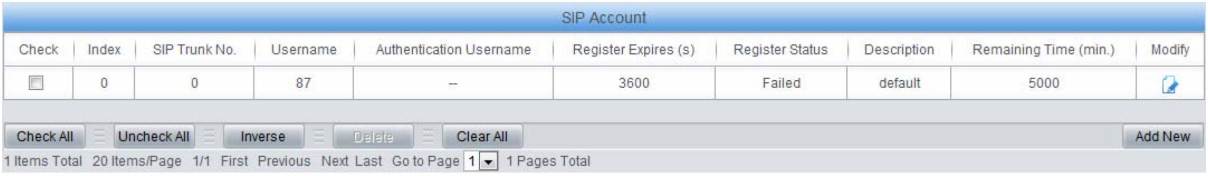


Figure 3-19 SIP Account Settings Interface

Click ***Modify*** in Figure 3-19 to modify a SIP account. See Figure 3-20 for the SIP account modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Account*** interface.

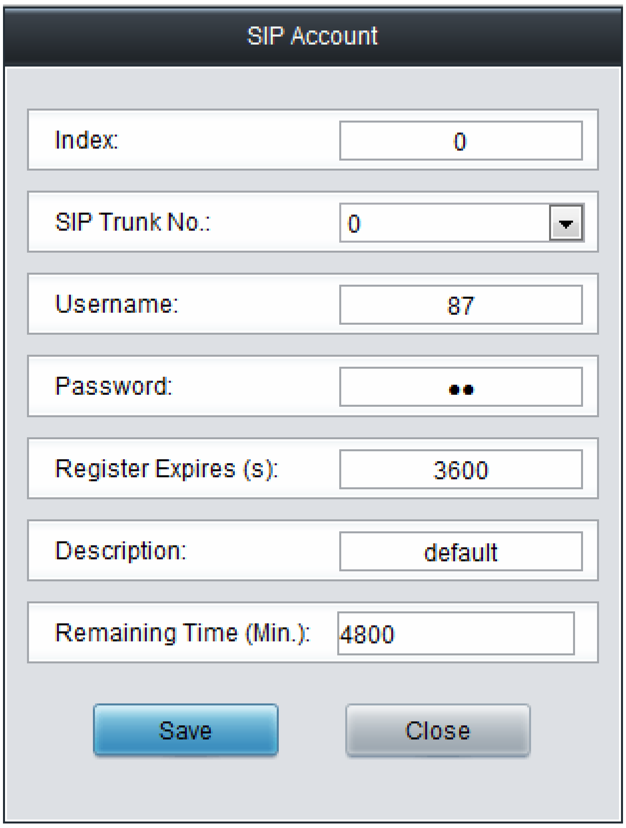


Figure 3-20 Modify SIP Account

To delete a SIP account, check the checkbox before the corresponding index in Figure 3-19 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP accounts at a time, click the ***Clear All*** button in Figure 3-19.

3.3.5 SIP Trunk Group

By default, there is no SIP trunk group available on the gateway. Click ***Add New*** to add them manually. See Figure 3-21.

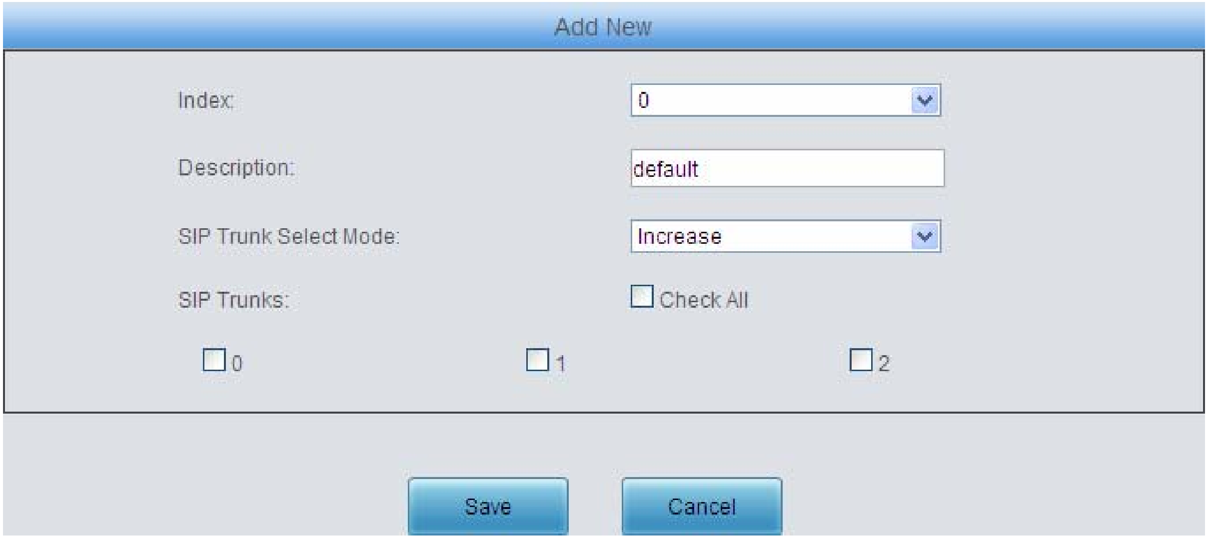


Figure 3-21 Add New SIP Trunk Group

The table below explains the items shown in Figure 3-21.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Index</td><td>The unique index of each SIP trunk group, which is mainly used in the configuration of routing rules and number manipulation rules to correspond to SIP trunk groups.</td></tr>
<tr><td>Description</td><td>More information about each SIP trunk group.</td></tr>
<tr><td>SIP Trunk Select Mode</td><td>When the SIP trunk group receives a call, it will choose a SIP trunk based on the select mode set by this configuration item to ring. The optional values and their corresponding meanings are described in the table below.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Increase</td><td>Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.</td></tr>
<tr><td>Decrease</td><td>Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.</td></tr>
<tr><td>Cyclic Increase</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from SIP Trunk N+1.</td></tr>
<tr><td>Cyclic Decrease</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from SIP Trunk N-1.</td></tr>
</table></td></tr>
<tr><td>SIP Trunks</td><td>The SIP trunks in the SIP trunk group. If the checkbox before a SIP trunk is grey, it indicates that the SIP trunk has been occupied. The ticked SIP trunks herein will be displayed in the column ‘SIP Trunks’ in Figure 3-22.</td></tr>
</table>

After configuration, click ***Save*** to save the settings into the gateway or click ***Cancel*** to cancel the settings. See Figure 3-22 for the SIP Trunk Group Setting Interface.

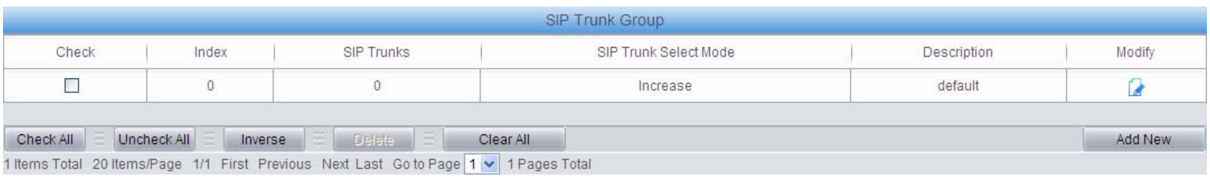


Figure 3-22 SIP Trunk Group Settings Interface

Click ***Modify*** in Figure 3-22 to modify a SIP trunk group. See Figure 3-23 for the SIP trunk group modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Trunk Group*** interface.

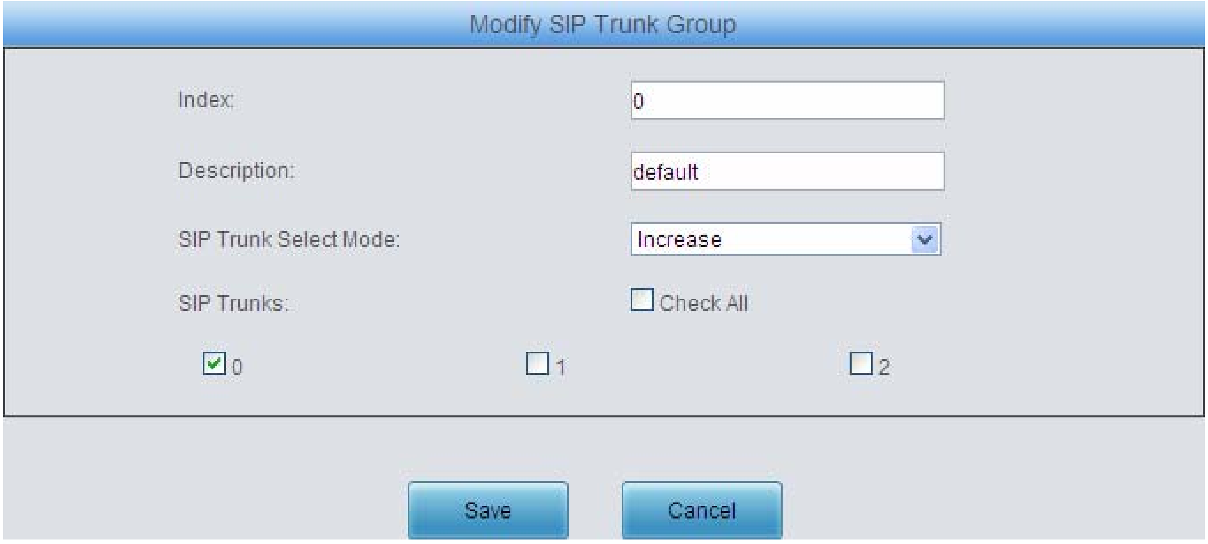


Figure 3-23 Modify SIP Trunk Group

To delete a SIP trunk group, check the checkbox before the corresponding index in Figure 3-22 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP trunk groups at a time, click the ***Clear All*** button in Figure 3-22.

3.3.6 Media Settings

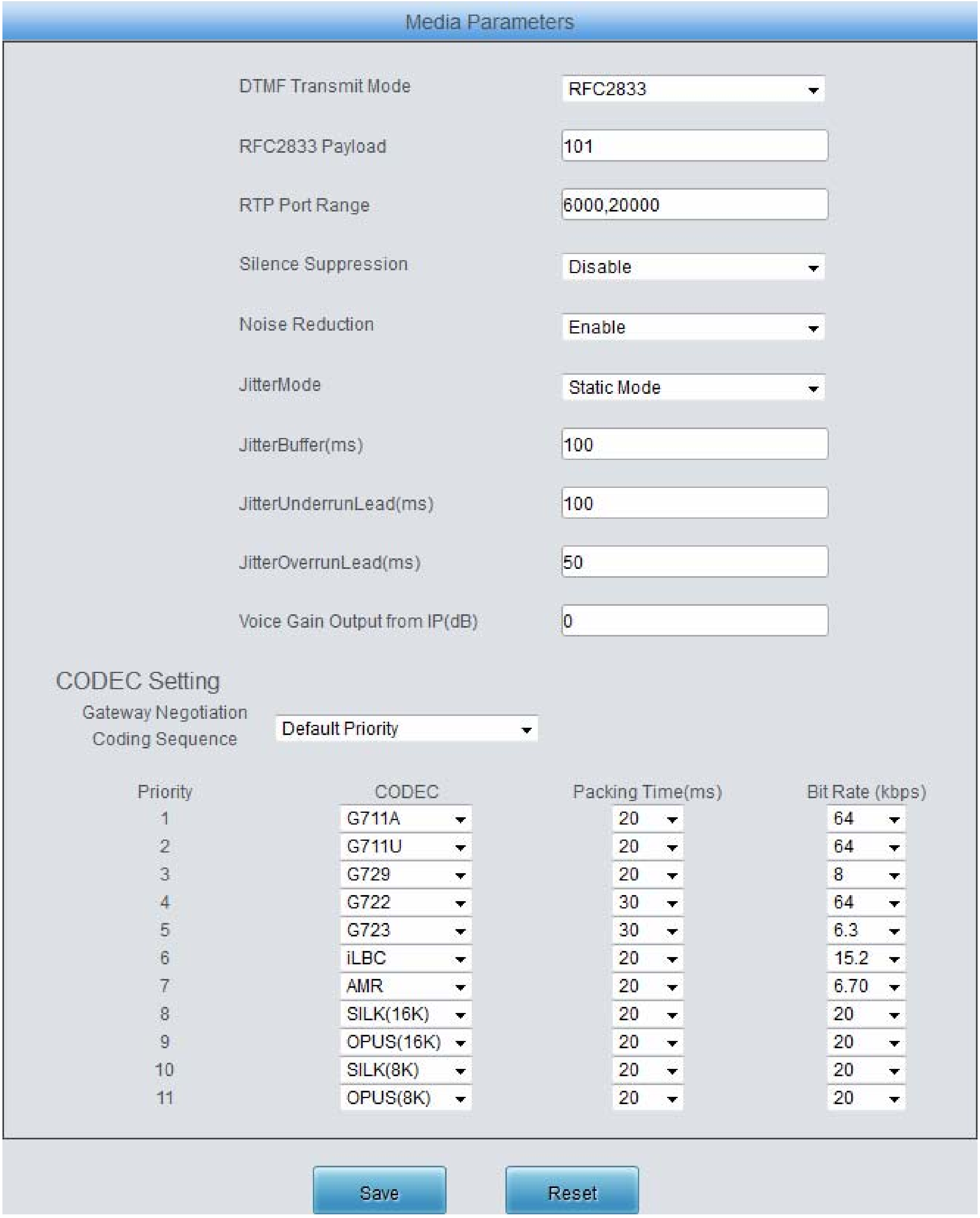


Figure 3-24 Media Settings Interface

See Figure 3-24 for the media settings interface where you can configure the RTP port and payload type depending on your requirements. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.7.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-24.

Item	Description
DTMF Transmit Mode	Sets the mode for the IP channel to send DTMF signals. The optional values are *RFC2833*, *In-band*, *Signaling*, *RFC2833+Signaling* and *In-band+Signaling*, with the default value of *RFC2833*.
RFC2833 Payload	Payload of the RFC2833 formatted DTMF signals on the IP channel. Range of value: 90~127, with the default value of 101.
RTP Port Range	Supported RTP port range for the IP end to establish a call conversation, Range of value: 5000~60000, with the lower limit of 5000 and the upper limit of 60000 and the difference between larger than 2048.
Silence Suppression	Sets whether to send comfort noise packets to replace RTP packets or never to send RTP packets to reduce the bandwidth usage when there is no voice signal throughout an IP conversation. The optional values are *Enable* and *Disable*, with the default value of *Disable*. **Note:** When G723 is selected as CODEC, this configuration setting will turn to Enable automatically.
Noise Reduction	Once this feature is enabled, the volume of the noise accompanied with the line will be reduced automatically. The default setting is *Enable*.
JitterMode	Sets the working mode of JitterBuffer. The optional values are *Static Mode* and *Adaptive Mode*, with the default value of *Static Mode.*
JitterBuffer	Acceptable jitter for data packets transmission over IP, which indicates the buffering capacity. A larger JitterBuffer means a higher jitter processing capability but as well as an increased voice delay, while a smaller JitterBuffer means a lower jitter processing capability but as well as a decreased voice delay. Range of value: 0~280, calculated by ms, with the default value of 100.
JitterUnderrunLead	Sets the initial delay applied to received packets upon accepting packets later than the expected value set in JitterBuffer Item. Range of value: 0~280, calculated by ms, with the default value of *100*, **Note:** Only when JitterMode is set to *Static Mode* will this item be shown.
JitterOverrunLead	Sets the beforehand time inserted if receiving packets is ahead of time (the time of receiving is earlier than 300 minus the value set in JitterBuffer). Rnage of value: 0~280, calculated by ms, with the default value of *50*, **Note:** Only when JitterMode is set to *Static Mode* will this item be shown.
JitterMin	Sets the minimum delay that can be set by the adaptive jitter function. It must be smaller than the value set in JitterBuffer. Range of value: 0~280, calculated by ms, with the default value of 80. **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.
JitterDecreaseRatio	Sets the rate of delay reduction under the adaptive mode. It defines the maximum percentage of the silence that can be removed in delay reduction. Range of value: 0~100, with the default value of *50*, **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.
JitterIncreaseMax	Sets the maximum delay increased during a silence period. Range of value: 0~280, calculated by ms, with the default value of *30*, **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.

<table>
<tr><td>Voice Gain Output from IP</td><td>Adjusts the voice gain of call from IP to IP. The value must be a multiple of 3. Range of value: -24~24, calculated by dB, with the default value of 0.</td></tr>
<tr><td>CODEC Setting</td><td>Sets CODECs for the IP end to establish a call conversation. The table below explains the sub-items:
<table>
<tr><th>Sub-item</th><th>Description</th></tr>
<tr><td>Gateway Negotiation Coding Sequence</td><td>Sets the coding sequence, including two options: Default Priority and User-defined Priority, with the default value of Default Priority.</td></tr>
<tr><td>Priority</td><td>Priority for choosing the CODEC in an SIP conversation. The smaller the value is, the higher the priority will be.</td></tr>
<tr><td>CODEC</td><td>Seven optional CODECs are supported: G711A, G711U, G729, G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K).</td></tr>
<tr><td>Packing Time</td><td>Time interval for packing an RTP packet, calculated by ms.</td></tr>
<tr><td>Bit Rate</td><td>The number of thousand bits (excluding the packet header) that are conveyed per second.</td></tr>
</table>
By default, all of the eleven CODECs are supported and ordered G711A, G711U, G729, G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K). by priority from high to low. The CODECs set here will be the default CODEC for the new added SIP trunks.
The packing time and bit rate supported by different CODECs are listed in the table below. Those values in bold face are the default values.
<table>
<tr><th>COEDC</th><th>Packing Time (ms)</th><th>Bit Rate (kbps)</th></tr>
<tr><td>G711A</td><td>10 / 20 / 30 / 40 / 50 / 60</td><td>64</td></tr>
<tr><td>G711U</td><td>10 / 20 / 30 / 40 / 50 / 60</td><td>64</td></tr>
<tr><td>G729</td><td>10 / 20 / 30 / 40 / 50 / 60</td><td>8</td></tr>
<tr><td>G722</td><td>10 / 20 / 30 / 40</td><td>64</td></tr>
<tr><td>G723</td><td>30 / 60</td><td>5.3 / 6.3</td></tr>
<tr><td rowspan="3">iLBC</td><td>20 / 40</td><td>15.2</td></tr>
<tr><td>30</td><td>13.3</td></tr>
<tr><td>60</td><td>13.3 / 15.2</td></tr>
<tr><td>AMR</td><td>20 / 40 / 60</td><td>4.75 / 5.15 / 5.90 / 6.70 / 7.40 / 7.95 / 10.20 / 12.20</td></tr>
<tr><td>SILK(16K)</td><td>20 /40 / 60 / 80 / 100</td><td>20</td></tr>
<tr><td>OPUS(16K)</td><td>10 / 20 / 40 / 60</td><td>20</td></tr>
<tr><td>SILK(8K)</td><td>20 /40 / 60 / 80 / 100</td><td>20</td></tr>
<tr><td>OPUS(8K)</td><td>10 / 20 / 40 / 60</td><td>20</td></tr>
</table>
</td></tr>
</table>

3.4 Route Settings

Route Settings is used to specify the routing rules for calls from IP→IP. See Figure 3-25.

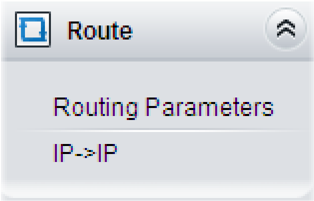


Figure 3-25 Route Settings

3.4.1 Routing Parameters

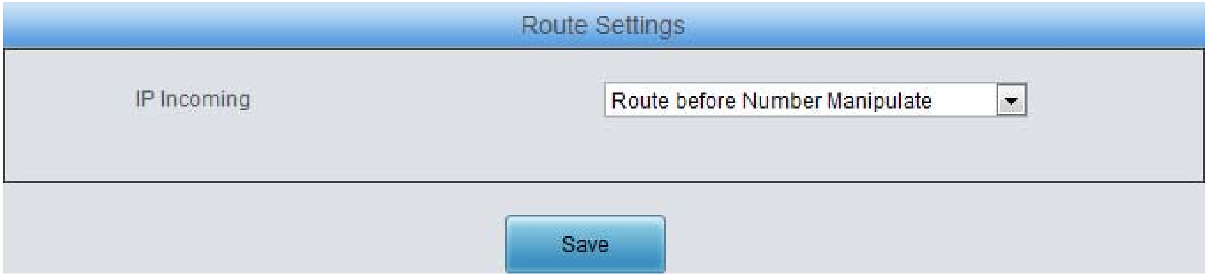


Figure 3-26 Routing Parameters Configuration Interface

See Figure 3-26 for the routing parameters configuration interface. On this interface, you can set the routing rules for calls from IP→IP to be routing before or after number manipulation. The default value is *Route before Number Manipulate*.

After configuration, click ***Save*** to save the above settings into the gateway.

Note: This feature is unavailable for SBO2000.

3.4.2 IP to IP

By default, there is no IP→IP routing rule available on the gateway. Click ***Add New*** to add them manually. See Figure 3-27 for the IP→IP routing rule adding interface.

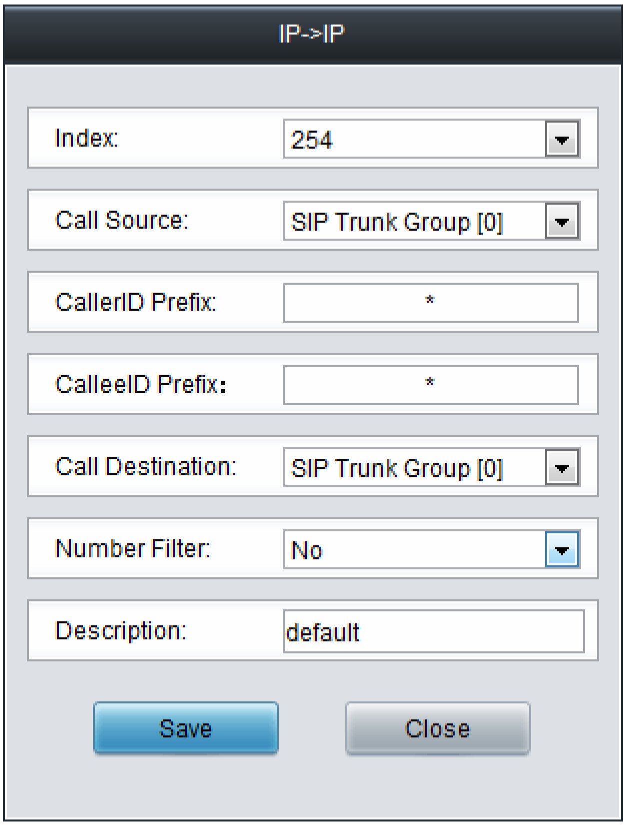


Figure 3-27 Add New Routing Rule (IP→IP)

The table below explains the items shown in the above figure.

Item	Description
Index	The unique index of each routing rule, which denotes its priority. A routing rule with a smaller index value has a higher priority. If a call matches several routing rules, it will be processed according to the one with the highest priority.
Call Initiator	SIP trunk group from where the call is initiated. This item can be set to a specific SIP trunk group or SIP Trunk Group [ANY] which indicates any SIP trunk group.

<table>
<tr><td>CallerID Prefix,
CalleeID Prefix</td><td>A string of numbers at the beginning of the calling/called party number. This item can be set to a specific string or “*” which indicates any string. These two configuration items together with Call Initiator can specify the calls which apply to a routing rule.
Rule Explanation:
<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>“0”~”9”</td><td>Digits 0～9.</td></tr>
<tr><td>“[ ]”</td><td>‘[ ]’ is used to define the range for a number. Values within it only can be digits ‘0~9’, punctuations ‘-’ and ‘,’. For example, [1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.</td></tr>
<tr><td>“-”</td><td>’-’ is used only in ‘[ ]’ between two numbers to indicates any number between these two numbers.</td></tr>
<tr><td>“,”</td><td>’,’ is used to separate numbers or number ranges, representing alternatives.</td></tr>
</table>
Example: Rule “0[0-3,7][6-9]” denotes the prefix is 006, 016, 026, 036, 007, 017, 027, 037, 008, 018, 028, 038, 009, 019, 029, 039, 076, 077, 078, 079.
Note: Multiple rules are supported for CallerID/CalleeID prefix. They are separated by “:”.</td></tr>
<tr><td>Call Destination</td><td>SIP trunk group to which the call will be routed.</td></tr>
<tr><td>Number Filter</td><td>Number filter rule which will be applicable to this route. It is set in Number Filter. See 3.5.4 Filtering Rule for details.</td></tr>
<tr><td>Description</td><td>More information about each routing rule.</td></tr>
</table>

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-28 for the IP→IP Routing Rule Configuration Interface.

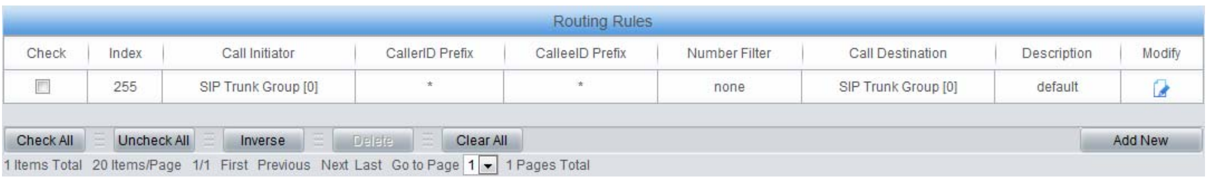


Figure 3-28 IP→IP Routing Rule Configuration Interface

Click ***Modify*** in Figure 3-28 to modify a routing rule. See Figure 3-29 for the IP→IP routing rule modification interface. The configuration items on this interface are the same as those on the ***Add New Routing Rule (IP→IP)*** interface. Note that the item ***Index*** cannot be modified.

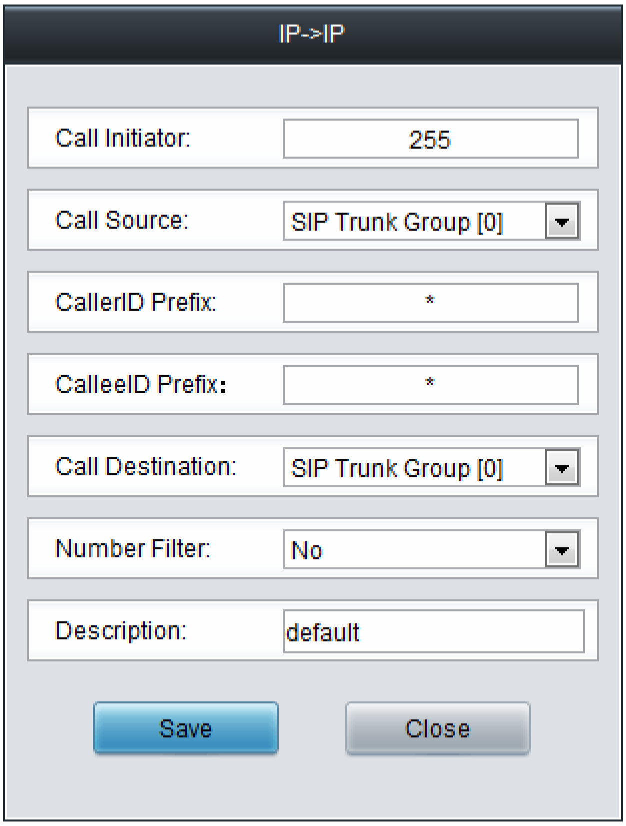


Figure 3-29 Modify Routing Rule (IP→IP)

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-28 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all routing rules at a time, click the ***Clear All*** button in Figure 3-28.

3.5 Number Filter

Number Filter includes four parts: ***Whitelist***, ***Blacklist***, ***Number Pool*** and ***Filtering Rule***. See Figure 3-30.

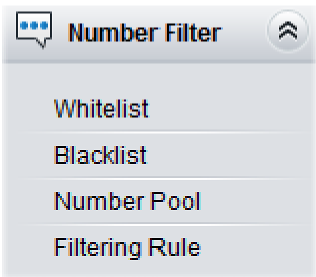


Figure 3-30 Number Filter Interface

3.5.1 Whitelist

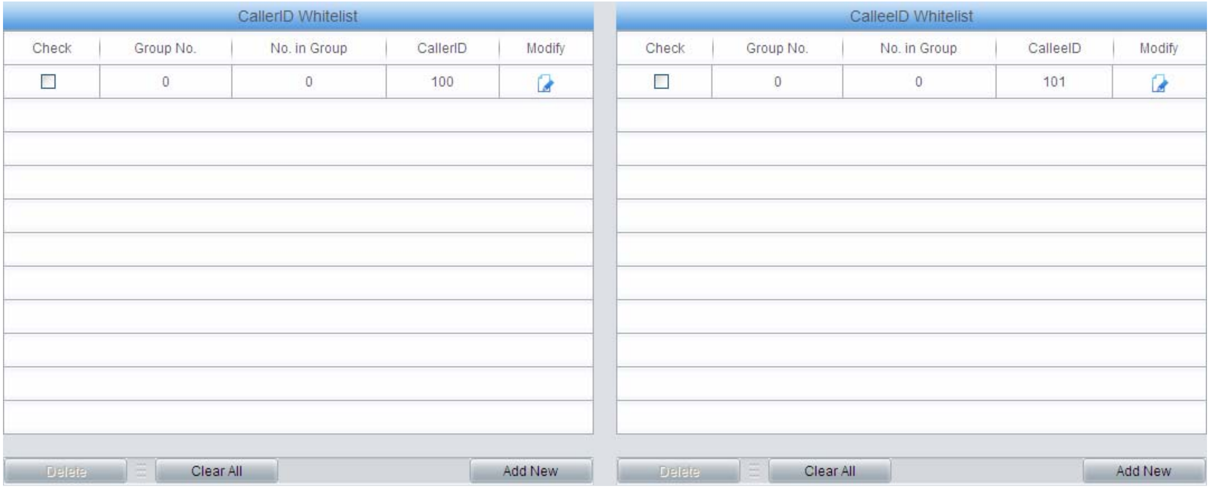


Figure 3-31 Whitelist Setting Interface

See Figure 3-31 for the Whitelist Setting Interface, which includes two parts: ***CallerID Whitelist*** and ***CalleeID Whitelist***.

A new CallerID/CalleeID whitelist can be added by the ***Add New*** button. See Figure 3-32, Figure 3-33 for CallerID/CalleeID whitelist adding interface.

Figure 3-32 Add New CallerIDs in Whitelist Interface

Figure 3-33 Add New CalleeIDs in Whitelist Interface

The table below explains the items shown in above figures.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Group</td><td>The corresponding Group ID for CallerIDs/CalleeIDs in the whitelist. The value range is 0~7.</td></tr>
<tr><td>No. in Group</td><td>The corresponding No. for different CallerIDs/CalleeIDs in a same group.</td></tr>
<tr><td>CallerID</td><td>CallerID in the whitelist, which must be filled in with numbers or “*” (indicating any string) and can not be left empty.
Rule explanation:
<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>“*”</td><td>indicating any string</td></tr>
<tr><td>“0”~”9”</td><td>Digits 0~9.</td></tr>
<tr><td>“x”</td><td>A random number. A string of ‘x’s represents several random numbers. For example, ‘xxx’ denotes 3 random numbers.</td></tr>
<tr><td>“[ ]”</td><td>‘[ ]’ is used to define the range for a number. Values within it only can be digits ‘0~9’, punctuations ‘-’ and ‘,’. For example, [1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.</td></tr>
<tr><td>“-”</td><td>’-’ is used only in ‘[ ]’ between two numbers to indicates any number between these two numbers.</td></tr>
<tr><td>“,”</td><td>’,’ is used to separate numbers or number ranges, representing alternatives.</td></tr>
</table></td></tr>
<tr><td>CalleeID</td><td>CalleeID in the whitelist, which must be filled in with numbers or “*” (indicating any string) and can not be left empty. The rules are the same as that of CallerID.</td></tr>
</table>

After configuration, click ***Save*** to save the above settings into the gateway or click ***Close*** to cancel the settings.

Click ***Modify*** in Figure 3-31 to modify the CallerID or CalleeID whitelist. See Figure 3-34, Figure 3-35 for CallerIDs/CalleeIDs on the Whitelist Modification interface. The configuration items on this interface are the same as those on the ***Add New CallerIDs/CalleeIDs in Whitelist*** interface. The item *Group No.* cannot be modified.

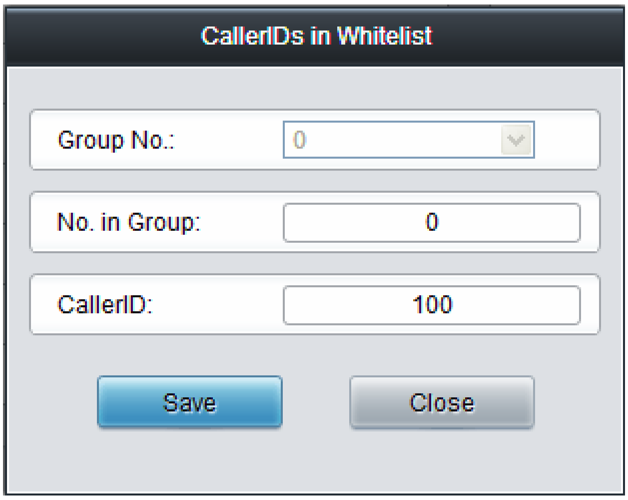


Figure 3-34 Modify CallerIDs in Whitelist

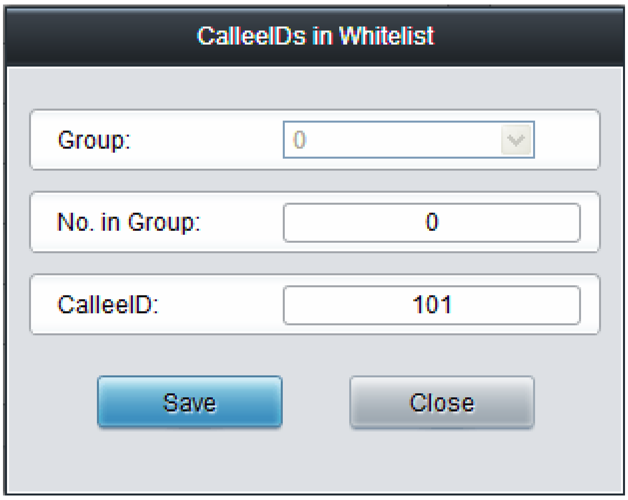


Figure 3-35 Modify CalleeIDs in Whitelist

To delete a CallerIDs/CalleeIDs in the whitelist, check the checkbox before the corresponding index in Figure 3-31 and click the '***Delete***' button. To clear all CallerIDs/CalleeIDs in the whitelist at a time, click the ***Clear All*** button in Figure 3-31.

Note: If a CallerID or CalleeID set in the whitelist is the same as one in the blacklist, it will go invalid. That is, the blacklist has a higher priority than the whitelist. The total amount of numbers in both whitelist and blacklist cannot exceed 5000.

3.5.2 Blacklist

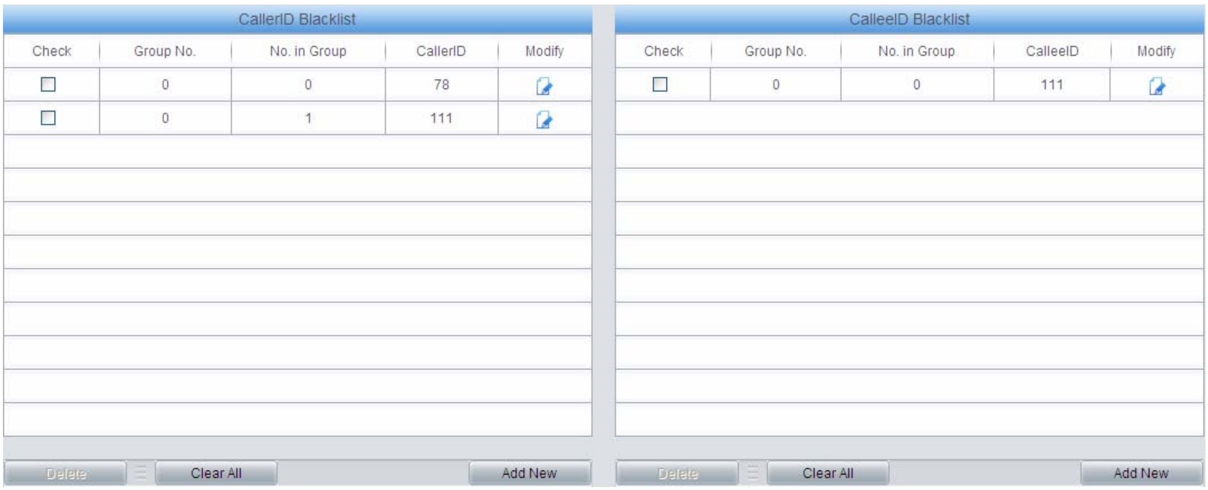


Figure 3-36 Blacklist Setting Interface

The Blacklist Setting interface is almost the same as the Whitelist Setting interface; only the whitelist changes to the blacklist. See Figure 3-36. The configuration items on this interface are the same as those on the Whitelist Setting interface (Figure 3-32, Figure 3-33).

Note: The lacklist has a higher priority than the whitelist. That is, if the same number exists in both blacklist and whitelist, the number in blacklist has priority.

3.5.3 Number Pool

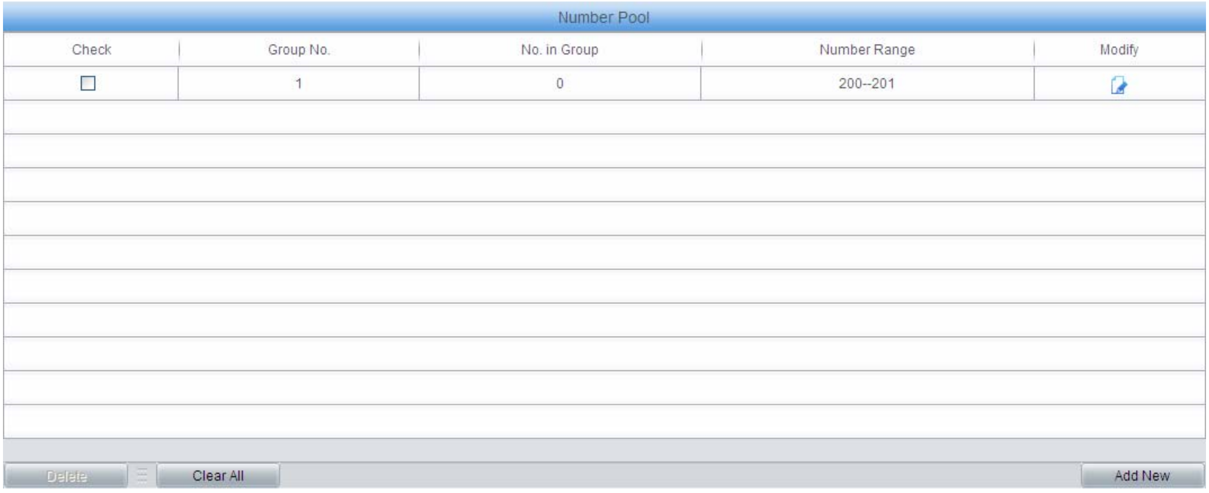


Figure 3-37 Number Pool Setting Interface

See Figure 3-37 for the Number Pool Setting interface. A new number pool can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-38 for the Number Pool adding interface.

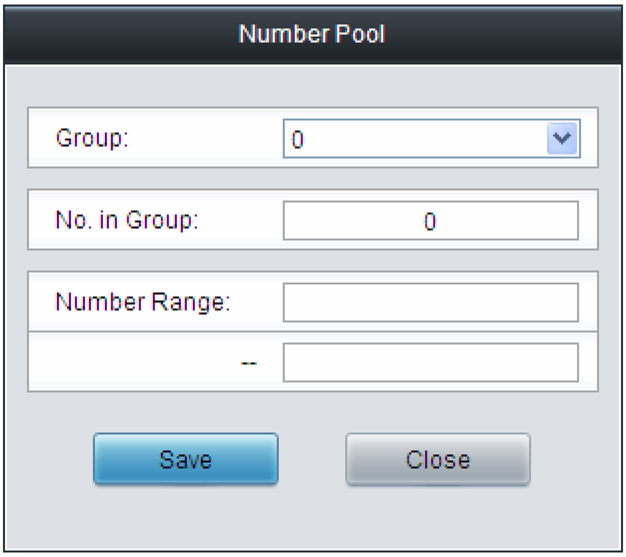


Figure 3-38 Add New Number Pool

The table below explains the items shown in the above figure.

Item	Description
Group	The corresponding Group ID for numbers in the number pool. The value range is 0~15.
No. in Group	The corresponding No. for different numbers in a same group. It supports up to 100 number s in one group.
Number Range	The range of the numbers in a number Pool. It must be filled in with numbers and can not be left empty.

After configuration, click ***Save*** to save the above settings into the gateway or click ***Close*** to cancel the settings.

Click ***Modify*** in Figure 3-37 to modify the number pool. See Figure 3-39 for the number pool modification interface. The configuration items on this interface are the same as those on the ***Add***

New Number Pool interface.

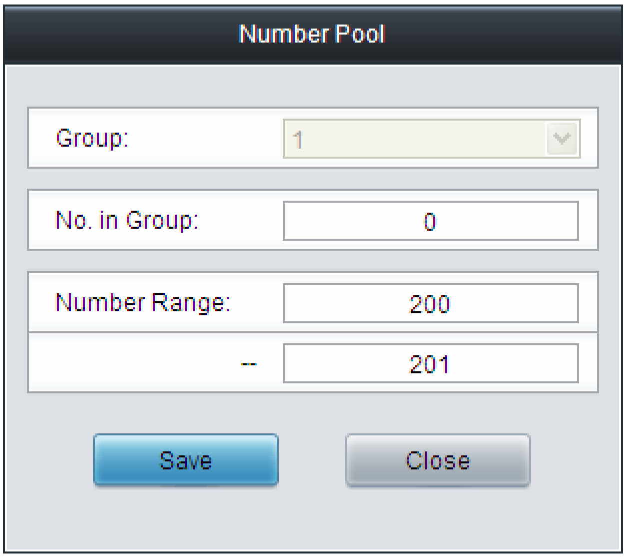
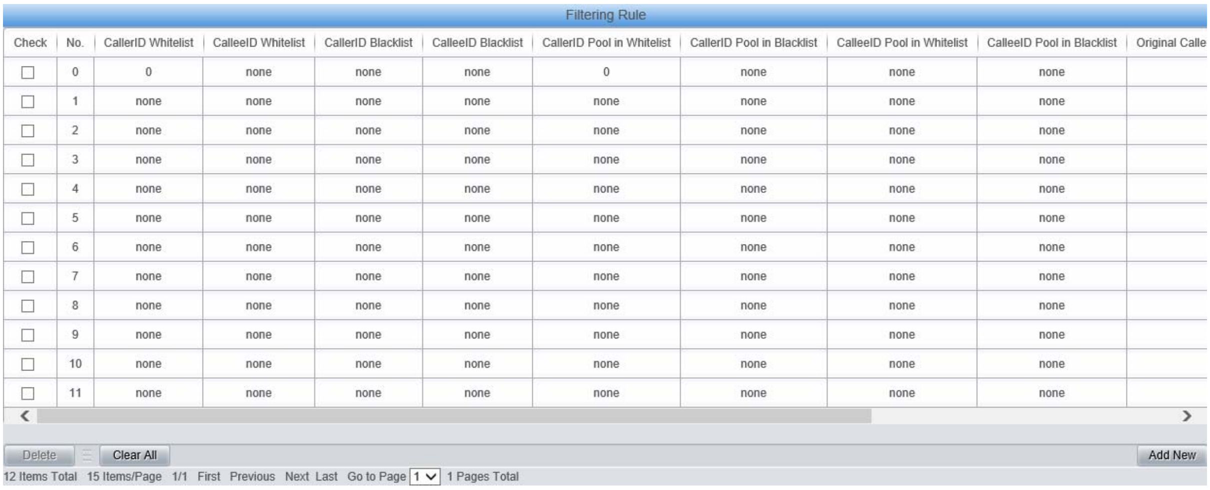


Figure 3-39 Modify Number Pool Interface

To delete a number pool, check the checkbox before the corresponding index in Figure 3-37 and click the '***Delete***' button. To clear all number pools at a time, click the ***Clear All*** button in Figure 3-37.

3.5.4 Filtering Rule



Filtering Rule

Check	No.	CallerID Whitelist	CalleeID Whitelist	CallerID Blacklist	CalleeID Blacklist	CallerID Pool in Whitelist	CallerID Pool in Blacklist	CalleeID Pool in Whitelist	CalleeID Pool in Blacklist	Original Calle
☐	0	0	none	none	none	0	none	none	none	
☐	1	none	none	none	none	none	none	none	none	
☐	2	none	none	none	none	none	none	none	none	
☐	3	none	none	none	none	none	none	none	none	
☐	4	none	none	none	none	none	none	none	none	
☐	5	none	none	none	none	none	none	none	none	
☐	6	none	none	none	none	none	none	none	none	
☐	7	none	none	none	none	none	none	none	none	
☐	8	none	none	none	none	none	none	none	none	
☐	9	none	none	none	none	none	none	none	none	
☐	10	none	none	none	none	none	none	none	none	
☐	11	none	none	none	none	none	none	none	none	

Delete Clear All Add New
12 Items Total 15 Items/Page 1/1 First Previous Next Last Go to Page 1 1 Pages Total

Figure 3-40 Filtering Rule Setting Interface

See Figure 3-40 for the Filtering Rule Setting Interface. A new filtering rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-41 for the Filtering Rule Adding interface.

Figure 3-41 Add New Filtering Rule

The table below explains the items shown in the above figure.

Item	Description
No.	The corresponding number for a filtering rule. The value range is 0~99.
CallerID Whitelist	The Group No. of CallerIDs saved on the whitelist setting interface.
CalleeID Whitelist	The Group No. of CalleeIDs saved on the whitelist setting interface.
CallerID Blacklist	The Group No. of CallerIDs saved on the blacklist setting interface.
CalleeID Blacklist	The Group No. of CalleeIDs saved on the blacklist setting interface.
CallerID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the CallerID pool in whitelist.
CallerID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the CallerID pool in blacklist.
CalleeID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the CalleeID pool in whitelist.

CalleeID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the CalleeID pool in blacklist.
Original CalleeID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the original CalleeID pool in whitelist.
Original CalleeID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the original CalleeID pool in blacklist.
Description	Remarks for the filtering rule. It can be any information, but can not be left empty.

After configuration, click ***Save*** to save the above settings into the gateway or click ***Close*** to cancel the settings.

Click ***Modify*** in Figure 3-40 to modify the filtering rule. See Figure 3-42 for the filtering rule modification interface. The configuration items on this interface are the same as those on the ***Add New Filtering Rule*** interface.

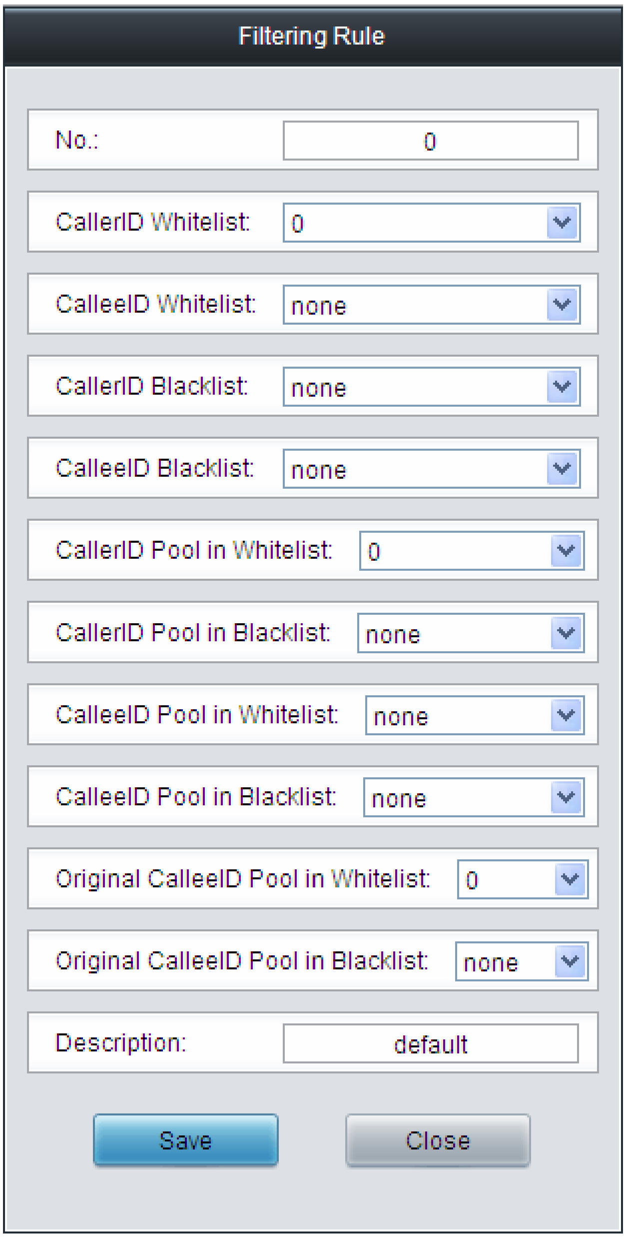


Figure 3-42 Modify Filtering Rule Interface

To delete a filtering rule, check the checkbox before the corresponding index in Figure 3-40 and click the ‘***Delete***’ button. To clear all filtering rules at a time, click the ***Clear All*** button in Figure 3-40.

3.6 Number Manipulation

Number Manipulation includes two parts: **IP→IP CallerID** and **IP→IP CalleeID**. See Figure 3-43.

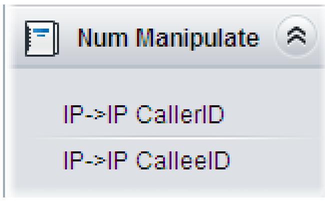


Figure 3-43 Number Manipulation

3.6.1 IP to IP CallerID

By default, there is no IP→IP CallerID manipulation available on the gateway. Click ***Add New*** to add them manually. See Figure 3-44 for the IP→IP CallerID manipulation rule adding interface.

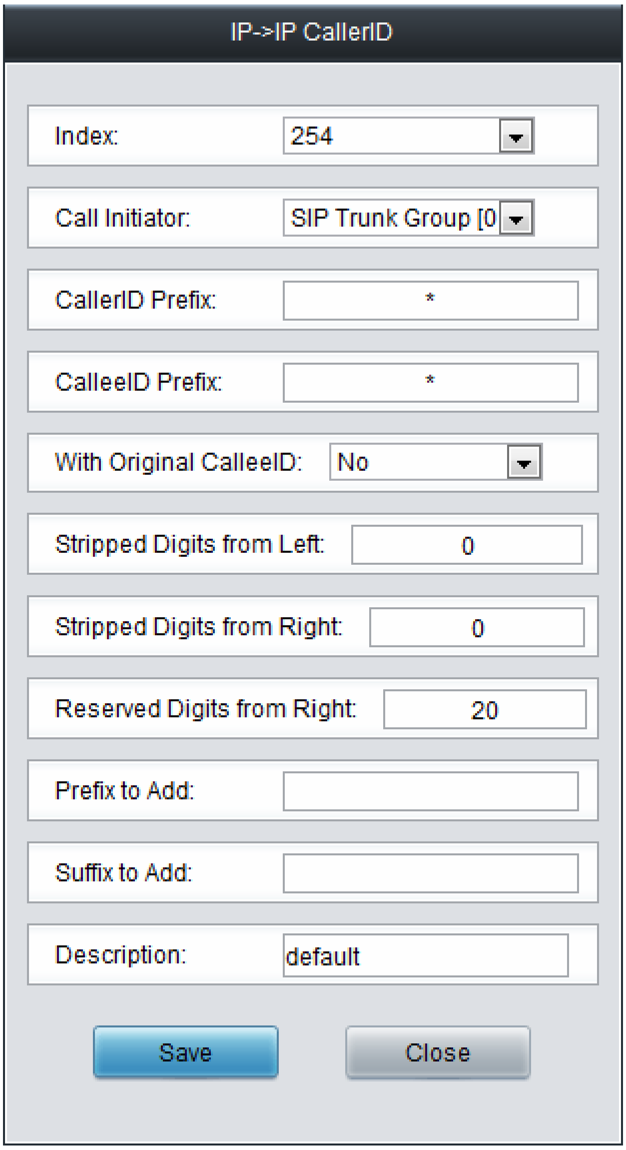


Figure 3-44 Add IP→IP CallerID Manipulation Rule

The table below explains the items shown in the above figure.

Item	Description
Index	The unique index of each number manipulation rule, which denotes its priority. A number manipulation rule with a smaller index value has a higher priority. If a call matches several number manipulation rules, it will be processed according to the one with the highest priority.
Call Initiator	SIP trunk group from where the call is initiated. This item can be set to a specific SIP trunk group or SIP Trunk Group[ANY] which indicates any SIP trunk group.
CallerID Prefix, CalleeID Prefix	A string of numbers at the beginning of the calling/called party number. This item can be set to a specific string or "*" which indicates any string. These two configuration items together with ***Call Initiator*** and ***With Original CalleeID*** can specify the calls which apply to a number manipulation rule. **Note:** Multiple CallerID/CalleeID Prefixes can be added simultaneously. They are separated by ":".
With Original CalleeID	If this item is set to *Yes*, it indicates that the number manipulation rule is only applicable to the calls with original CalleeID/redirecting number. The default value is *No*.
Stripped Digits from Left	The amount of digits to be deleted from the left end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted.
Stripped Digits from Right	The amount of digits to be deleted from the right end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted.
Reserved Digits from Right	The amount of digits to be reserved from the right end of the number. Only when the value of this item is less than the length of the current number will some digits be deleted from left; otherwise, the number will not be manipulated.
Prefix to Add	Designated information to be added to the left end of the current number.
Suffix to Add	Designated information to be added to the right end of the current number.
Description	More information about each number manipulation rule.

Note: The number manipulation is performed in 5 steps by the order of the following configuration items: *Stripped Digits from Left*, *Stripped Digits from Right*, *Reserved Digits from Right*, *Prefix to Add* and *Suffix to Add*.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-45 for IP→IP CallerID Manipulation Interface.

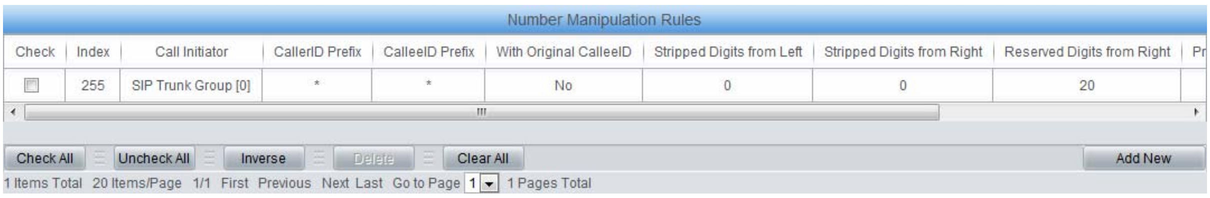


Figure 3-45 IP→IP CallerID Manipulation Interface

Click ***Modify*** in Figure 3-45 to modify a number manipulation rule. See Figure 3-46 for the IP→IP CallerID manipulation rule modification interface. The configuration items on this interface are the same as those on the ***Add IP→IP CallerID Manipulation Rule*** interface. Note that the item ***Index*** cannot be modified.

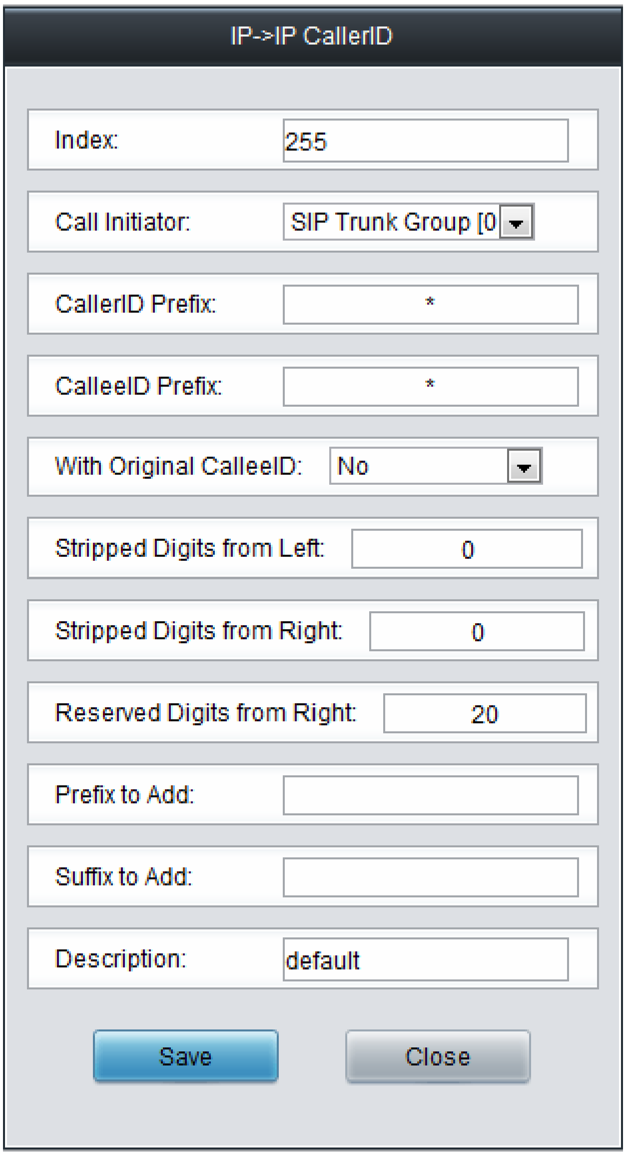


Figure 3-46 Modify IP→IP CallerID Manipulation Rule

To delete a number manipulation rule, check the checkbox before the corresponding index in Figure 3-45 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all number manipulation rules at a time, click the ***Clear All*** button in Figure 3-45.

3.6.2 IP to IP CalleeID

The number manipulation process for IP→IP CalleeID is almost the same as that for IP→IP CallerID; only the number to be manipulated changes from CallerID to CalleeID. See Figure 3-47 for IP→IP CalleeID manipulation interface. The configuration items on this interface are the same as those on ***IP→IP CallerID Manipulation Interface*** (Figure 3-45).

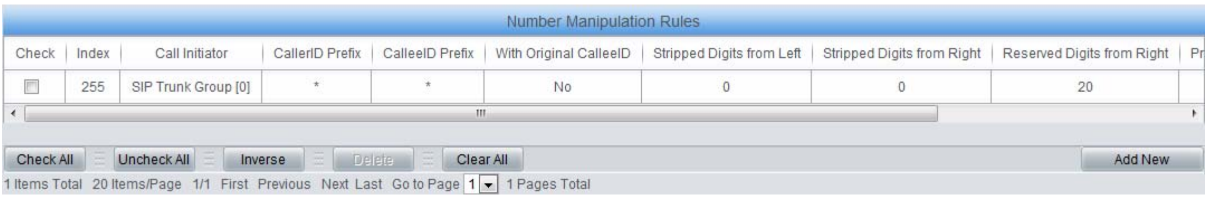


Figure 3-47 IP→IP CalleeID Manipulation Interface

3.7 System Tools

System Tools is mainly for gateway maintenance. It provides such features as IP modification, time synchronization, data backup, log inquiry and connectivity check. See Figure 3-48 for details.

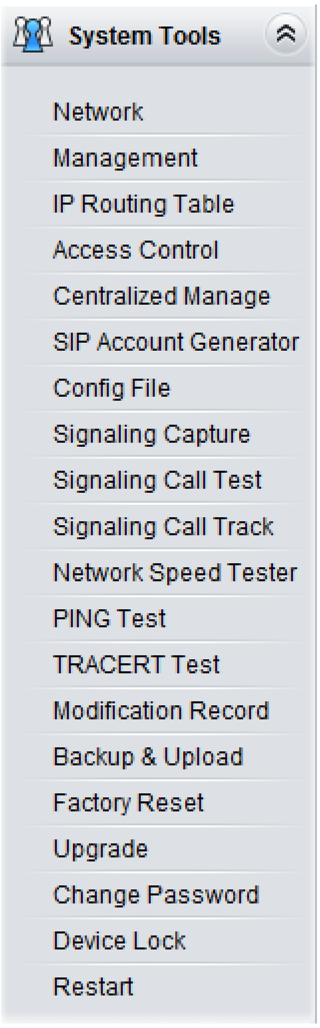


Figure 3-48 System Tools

3.7.1 Network

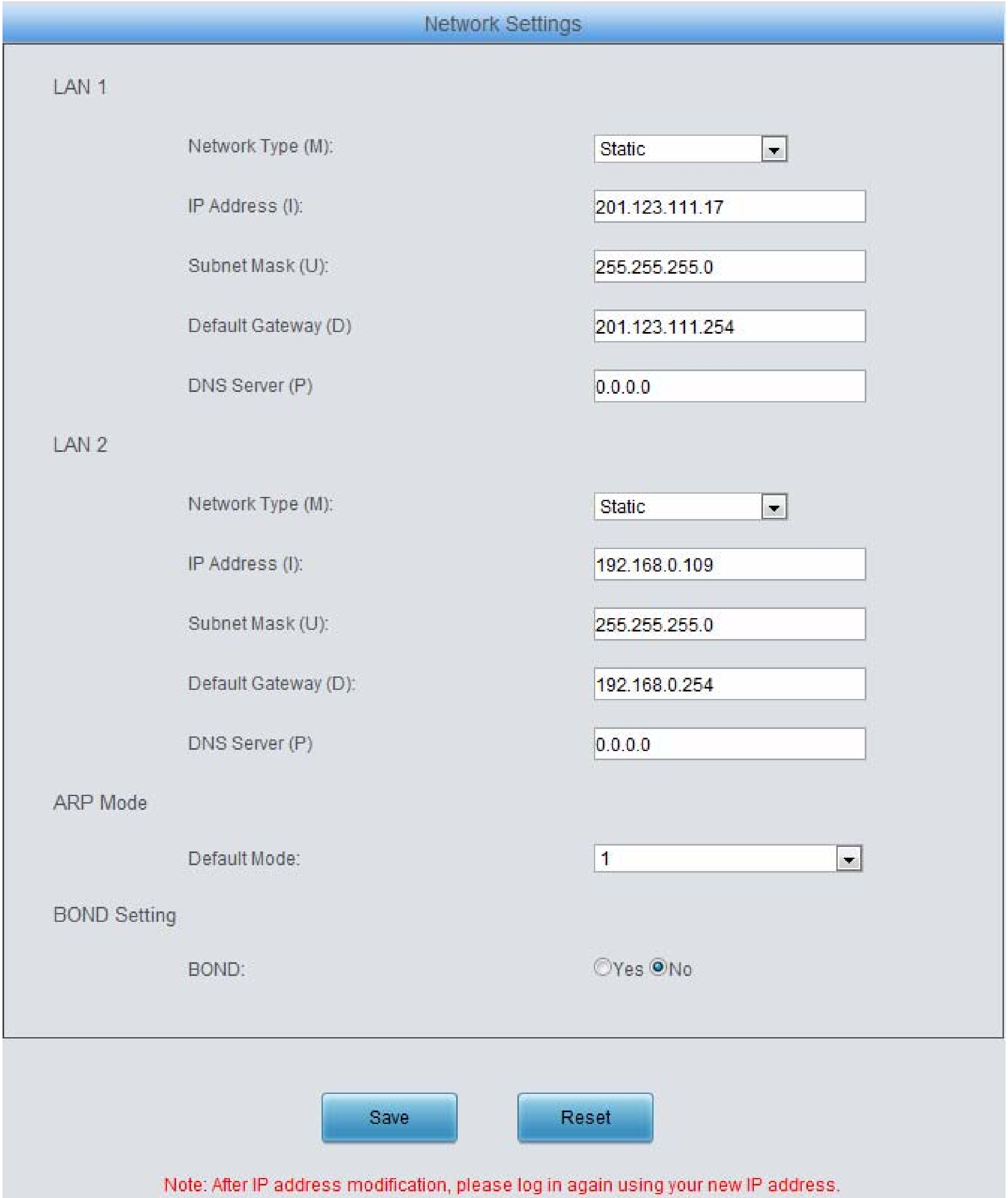


Figure 3-49 Network Settings Interface

See Figure 3-49 for the Network Settings interface. A gateway has two network ports, each of which can be configured with independent IP address, subnet mask, default gateway and DNS server. The Bond feature when enabled will make the information of LAN1 and LAN2 duplicated and backed up so as to realize the hot-backup function for LAN1 and LAN2. By default, this feature is *disabled*.

Note: 1. The two configuration items IP Address and Default Gateway cannot be the same for NET 1 and NET 2.

2. By default, *Speed and Duplex Mode* is hidden, set to Automatic Detection. You can

click 'F' to let it display. We suggest you do not modify it because the non-automatic detection may cause abnormity in network interface.

If the Network Detect feature is enabled, a ping test will automatically be initiated from this IP address to the gateway to check the connection status between them. By default, this feature is disabled.

After configuration, click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations. After changing the IP address, you shall log in the gateway again using your new IP address.

Note: The BOND setting is unsupported by SBO2000.

3.7.2 Management

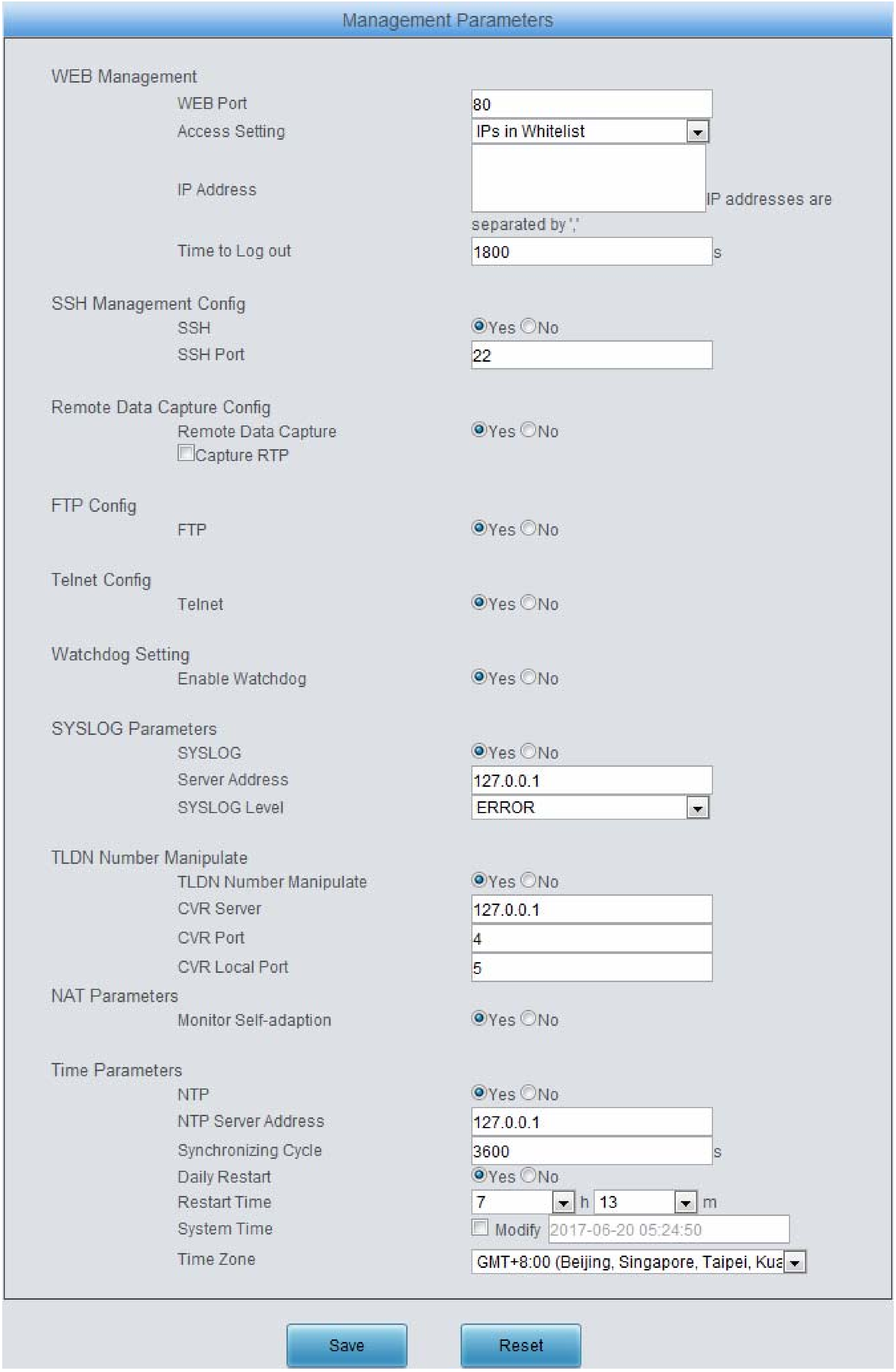

Management Parameters
WEB Management
WEB Port
80
Access Setting
IPs in Whitelist
IP Address
IP addresses are separated by ','
Time to Log out
1800
s
SSH Management Config
SSH
Yes No
SSH Port
22
Remote Data Capture Config
Remote Data Capture
Yes No
Capture RTP
FTP Config
FTP
Yes No
Telnet Config
Telnet
Yes No
Watchdog Setting
Enable Watchdog
Yes No
SYSLOG Parameters
SYSLOG
Yes No
Server Address
127.0.0.1
SYSLOG Level
ERROR
TLDN Number Manipulate
TLDN Number Manipulate
Yes No
CVR Server
127.0.0.1
CVR Port
4
CVR Local Port
5
NAT Parameters
Monitor Self-adaption
Yes No
Time Parameters
NTP
Yes No
NTP Server Address
127.0.0.1
Synchronizing Cycle
3600
s
Daily Restart
Yes No
Restart Time
7
h
13
m
System Time
Modify
2017-06-20 05:24:50
Time Zone
GMT+8:00 (Beijing, Singapore, Taipei, Kua
Save
Reset

Figure 3-50 Management Parameters Setting Interface

See Figure 3-50 for the Management Parameters Setting interface. The table below explains the items shown in the above figure.

Item	Description
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.
Access Setting	Sets the IP addresses which can access the gateway via WEB. By default, all IPs are allowed. You can set an IP whitelist to allow all IPs within it to access the gateway freely. Also can set an IP blacklist to forbid all IPs within it to access the gateway.
Time to Log Out	The gateway will log out automatically if it is not operated during a time longer than the value of this item, calculated by s, with the default value of 1800.
SSH	Sets whether to enable the gateway to be accessed via SSH, with the default value of *No*.
SSH Port	The port which is used to access the gateway via SSH.
Remote Data Capture	After this feature is enabled, you can obtain the gateway data via a remote capture tool, with the default value of *No*.
Capture RTP	Sets whether to capture the RTP. Once this feature is enabled, the RTP package will also be captured by the selected network.
FTP	Sets whether to enable the FTP server, with the default value of *Yes*.
Telnet	Sets whether to enable the Telnet feature, with the default value of *Yes*. **Note:** By default, this configuration item is hidden. To display or hide it, you should click any part of the interface and press the “F” button.
Enable Watchdog	Sets whether to enable the watchdog feature, with the default value of *Yes*.
SYSLOG	Sets whether to enable SYSLOG. It is required to fill in ***SYSLOG Server Address*** and ***SYSLOG Level*** in case SYSLOG is enabled. By default, ***SYSLOG*** is disabled.
Server Address	Sets the SYSLOG server address for log reception.
SYSLOG Level	Sets the SYSLOG level. There are three options: *ERROR*, *WARNING* and *INFO*.
TLDN Number Manipulate	Once this feature is enabled, the gateway will send the CalleeID to the number manipulation server and continue the SIP call progress using the manipulated number when it receives E1 calls. By default, it is *disabled.* **Note:** The feature is unsupported by SBO2000.
CVR Server, CVR Port	The IP address/ port of the server to manipulate the CalleeID.
CVR Local Port	The port of the SBO gateway.
Monitor Self-adaption	Enable the NAT stun between the gateway and the monitor tool. By default, it is disabled.
NTP	Sets whether to enable the NTP time synchronization feature. It is required to fill in ***NTP Server Address***, ***Synchronizing Cycle*** and ***Time Zone*** in case NTP is enabled. By default, ***NTP*** is disabled.
NTP Server Address	Sets the Server address for NTP time synchronization.
Synchronizing Cycle	Sets the cycle for NTP time synchronization.

Daily Restart	Sets whether to restart the gateway regularly every day at the preset ***Restart Time***. By default, this feature is disabled.
Restart Time	Sets the time to restart the gateway regularly.
System Time	The system time. Check the checkbox before ***Modify*** and change the time in the edit box.
Time Zone	The time zone of the gateway.

3.7.3 IP Routing Table

IP Routing Table is used to set the route for the LAN port when these two network ports both transport SIP. Thus, the LAN can access some IPs in other different network segment. By default, there is no routing table available on the gateway, click ***Add New*** to add them manually. See Figure 3-51.

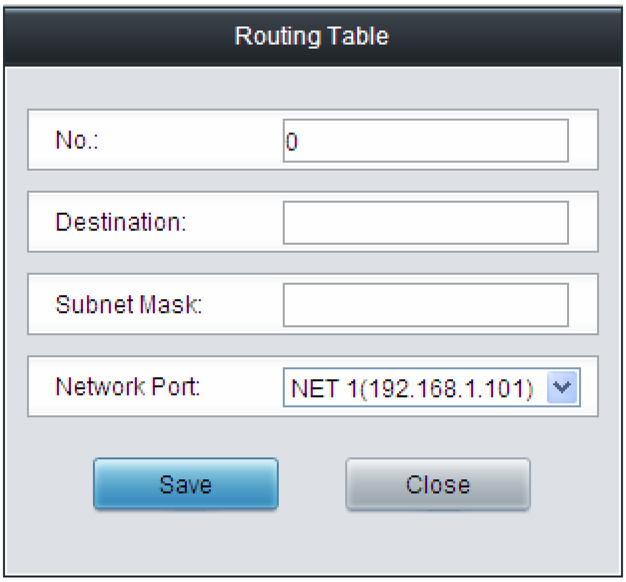


Figure 3-51 Routing Table Adding Interface

The table below explains the items shown in above figures.

Item	Description
No.	The number of the routing for the LAN in routing table.
Destination	The network segment in which the IP address is accessible for the network port.
Subnet Mask	The subnet mask of the network segment.
Network Port	The corresponding network port of the routing.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-52 for the Routing Table List.

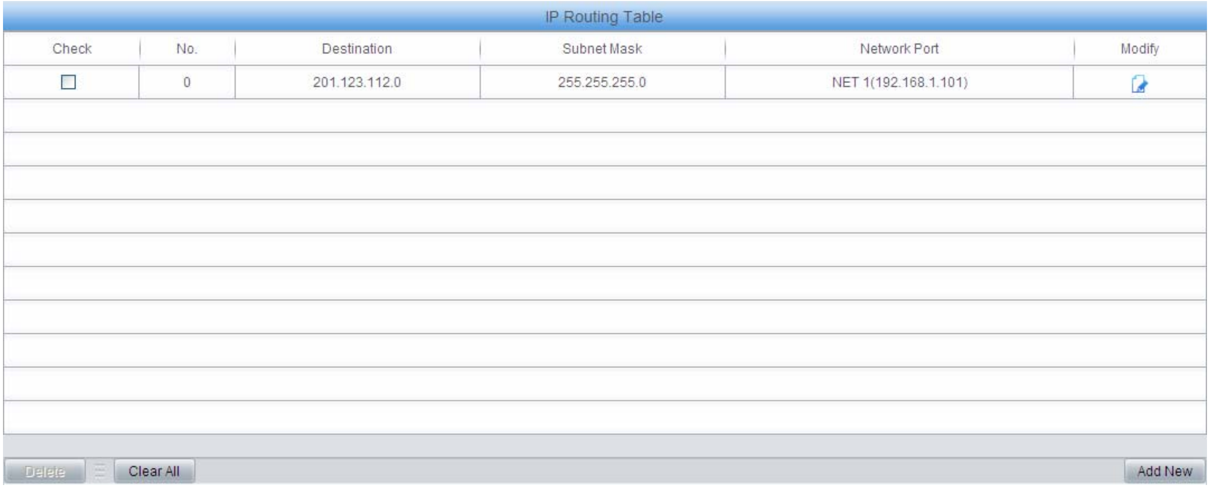


Figure 3-52 Routing Table List

Click ***Modify*** in Figure 3-52 to modify a routing. See Figure 3-53 for the routing table modification interface. The configuration items on this interface are the same as those on the ***Add Routing Table*** interface. Note that the item ***No.*** cannot be modified.

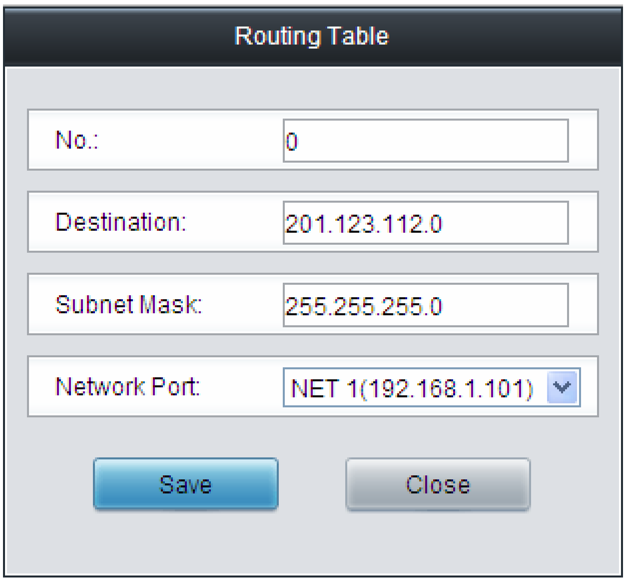


Figure 3-53 Routing Table Modification Interface

To delete a routing, check the checkbox before the corresponding index in Figure 3-52 and click the ***Delete*** button. To clear all number manipulation rules at a time, click the ***Clear All*** button in Figure 3-52.

3.7.4 Access Control

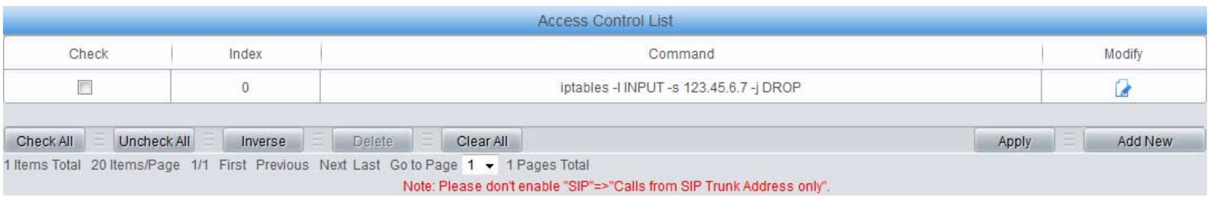


Figure 3-54 Access Control List Interface

See Figure 3-54 for the Access Control List interface. Once you add a piece of command to ACL, the network flow will be restricted, only the particular devices allowed to visit the gateway and only the data packages on the designated ports be forwarded. Click ***Add New*** to add a new piece of command. See Figure 3-55.

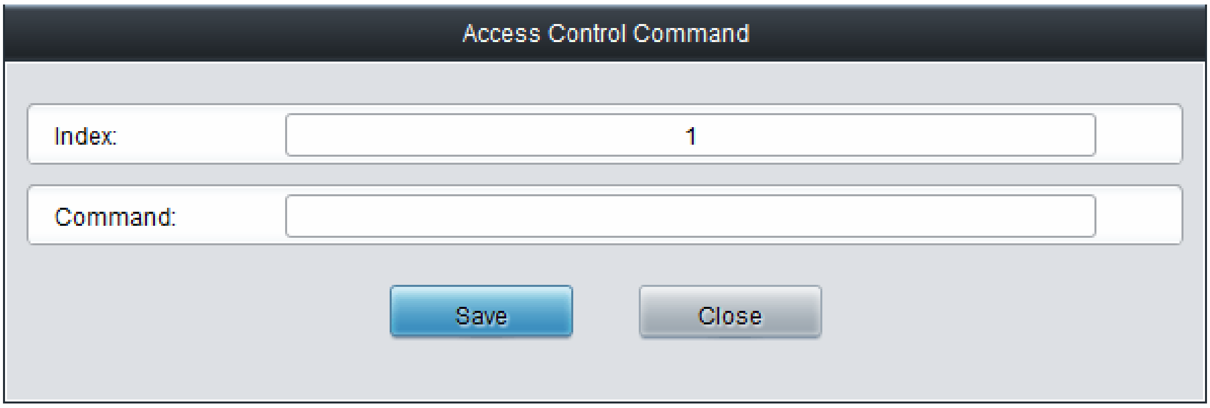


Figure 3-55 Add Access Control Command Interface

Input a piece of command into the Command item and click ***Save*** to save the settings to the gateway. Click ***Close*** to cancel your settings. After that. click ***Apply*** to make the new command valid.

Click ***Modify*** in Figure 3-54 to modify a command. See Figure 3-56 for the Access Control Command Modification interface. The configuration items on this interface are the same as those on the ***Add Access Control Command*** interface. Note that the item ***Index*** cannot be modified.

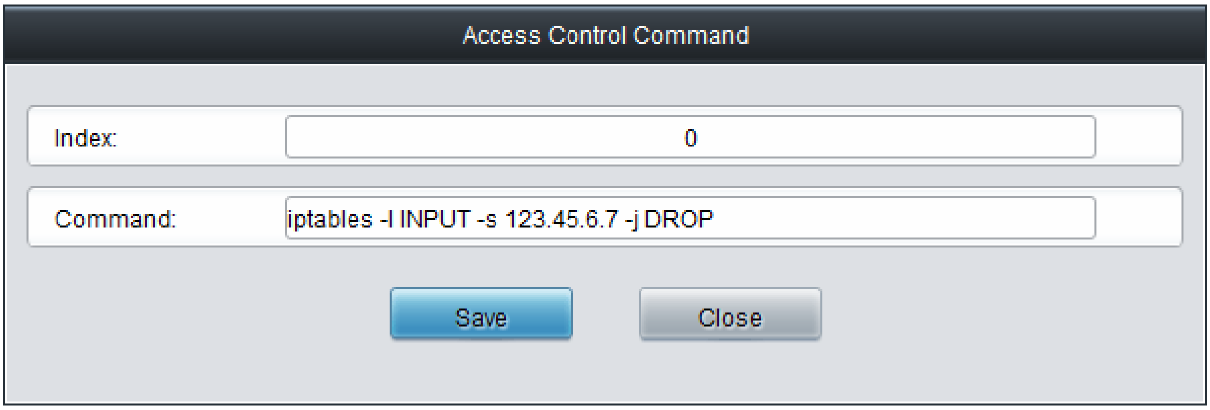


Figure 3-56 Access Control Command Modification Interface

To delete an Access Control Command, check the checkbox before the corresponding index in Figure 3-54 and click the ***Delete*** button, and then click the ***Apply*** button to make the deleted command invalid. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all access control commands at a time, click the ***Clear All*** button in Figure 3-54.

Note: 1, Currently, only the command iptables is supported by the gateway.

2, When you add or modify or delete commands manually, don't forget to click the ***Apply*** button to make your settings valid. However, when the gateway restarts or the configuration is leading-in, you need not click the ***Apply*** button and the commands will get valid automatically.

3.7.5 Centralized Manage

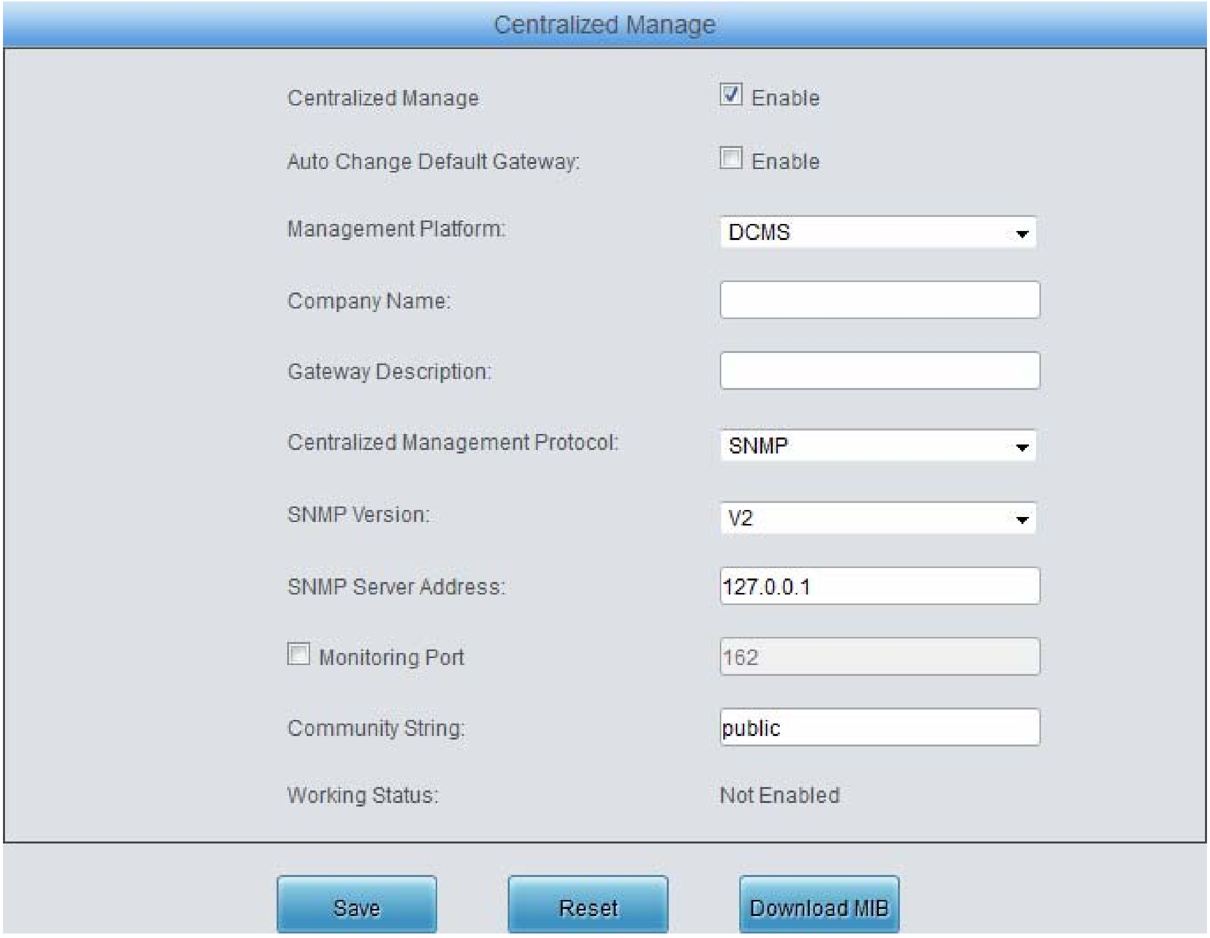


Figure 3-57 Centralized Manage Setting Interface

See Figure 3-57 for the Centralized Manage Setting interface. The gateway can register to a centralized management platform and accept the management of the platform. The table below explains the items shown in above figures.

Item	Description
Auto Change Default Gateway	Once this feature is enabled, the gateway will connect the DCMS via another network port automatically once the connected network cable is loosen or drawn out. The default value is disabled.
Management Platform	Select a management platform for the gateway to register.
Company Name	The company name used to register the gateway to DCMS, only valid when DCMS is selected.
Gateway Description	The description displayed on DCMS after the gateway is registered to DCMS, giving an easy identification of the gateway in device grouping. This item is only valid when DCMS is selected.
Centralized Management Protocol	Sets the centralized management protocol. It only supports SNMP currently.
SNMP Version	Sets the version of SNMP, three options available: V1, V2 and V3, with the default value of V2.
SNMP Server Address	IP address of SNMP.

Monitoring Port	Monitoring Port for SNMP on the gateway.
Community String	Community string used for information acquisition.
Account	The account of SNMP, only valid when the SNMP version is set to V3.
Grade	The grade of SNMP, three options available: Neither authenticated nor encrypted, Authenticated but not encrypted and Authenticated and encrypted, with the default value of *Neither authenticated nor encrypted*. It is only valid when the SNMP version is set to V3.
Authentication Password	The authentication password required to enter when the item Grade is set to Authenticated but not encrypted or Authenticated and encrypted.
Encryption Password	The encryption password required to enter when the item Grade is set to Authenticated and encrypted.
Working Status	The status of the connection between the gateway and the centralized management server. It is only valid when DCMS is selected.

3.7.6 SIP Account Generator

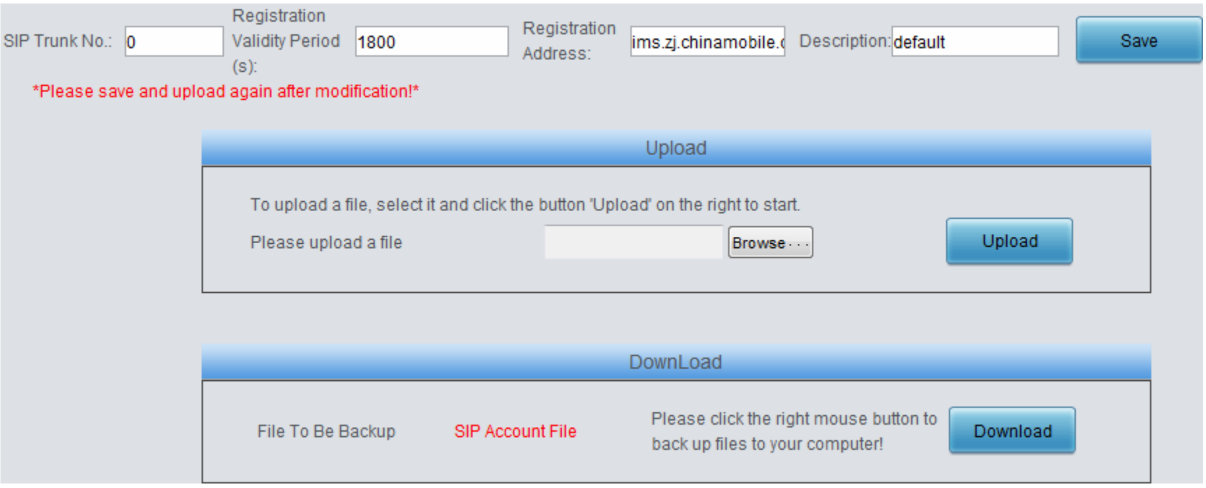


Figure 3-58 SIP Account Generator Interface

See Figure 3-58 for the SIP Account Generator interface. The gateway allows to transform the common SIP account and password to the specific format it supports, upload a file containing the SIP account and password, and modify the SIP Trunk No., Registration Validity Period, Registration Address and Description according to your requirement. Click ***Save*** to save your settings and upload the SIP account source file again. Then the SIP account in the format that the gateway supports will be generated. Click ***Download*** to check the generated SIP account.

Note: As to the upload file, only the txt. format is supported at present, and the SIP account and password must be separated by “,”.

3.7.7 Configuration File

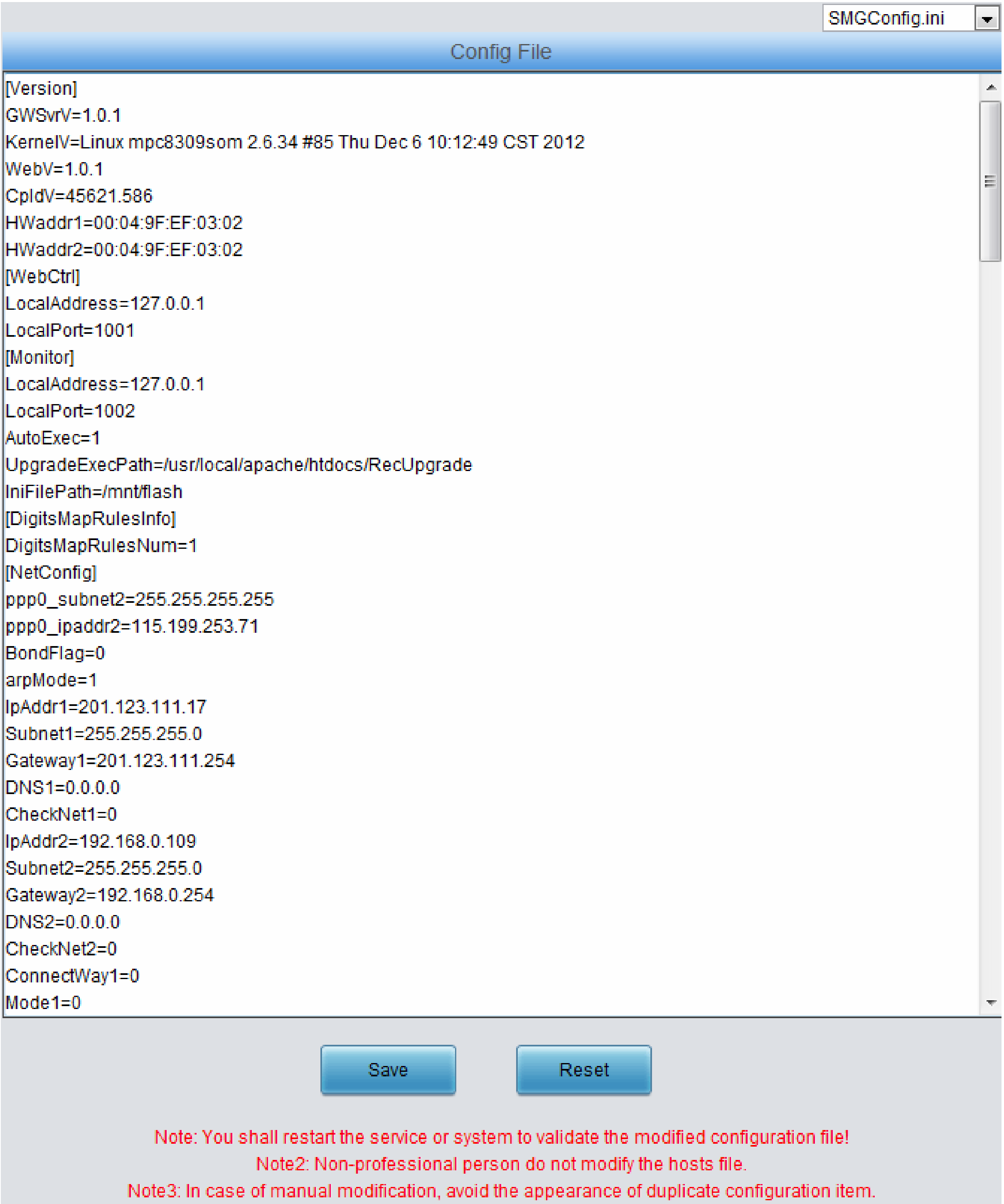


Figure 3-59 Configuration File Interface

See Figure 3-59 for the Configuration File interface, including two files: SMGConfig.ini and ShConfig.ini. You can check and modify the items in these configuration files through this interface. Configurations about the gateway server, such as route rules, number manipulation, number filter and so on, are included in SMGConfig.ini; Configurations about the board are included in ShConfig.ini. You can modify these configurations on the interface directly, and then click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations.

3.7.8 Signaling Capture

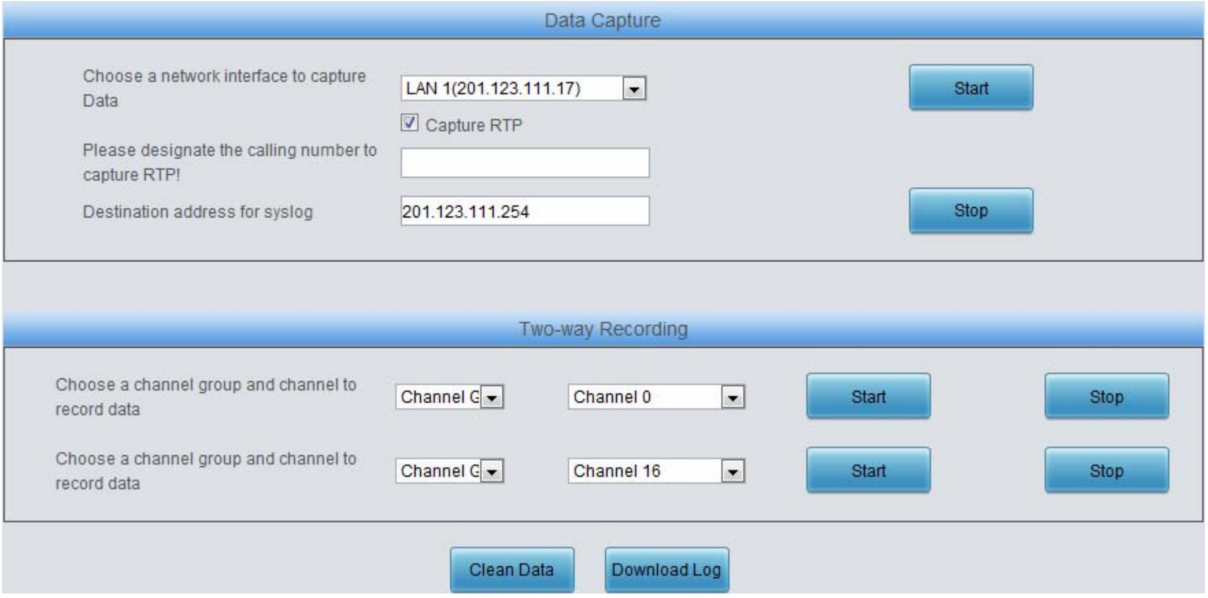


Figure 3-60 Signaling Capture Interface

See Figure 3-60 for the Signaling Capture interface. Data Capture is used to capture data on the network interface you choose. Click ***Start*** to start capturing data (up to 800M) on the corresponding network interface. SIP and SysLog are supported at present. You can input a destination address for syslog to which the syslog file will be sent. Click ***Stop*** to stop data capture and download the captured packets. Once the option Capture RTP is ticked, you are required to input the calling number of the RTP to be captured.

IP Two-way Recording is used to make recording of a designated channel in a specified channel group. Click ***Start*** to start recording data (maximum consecutively recording time: 1 minute). Click ***Stop*** to stop data recording and download the recorded data.

Click ***Clean Data*** to clean all the recording files and captured packages. Click ***Download Log*** to download such logs as core files, configuration files, error information and so on.

3.7.9 Signaling Call Test

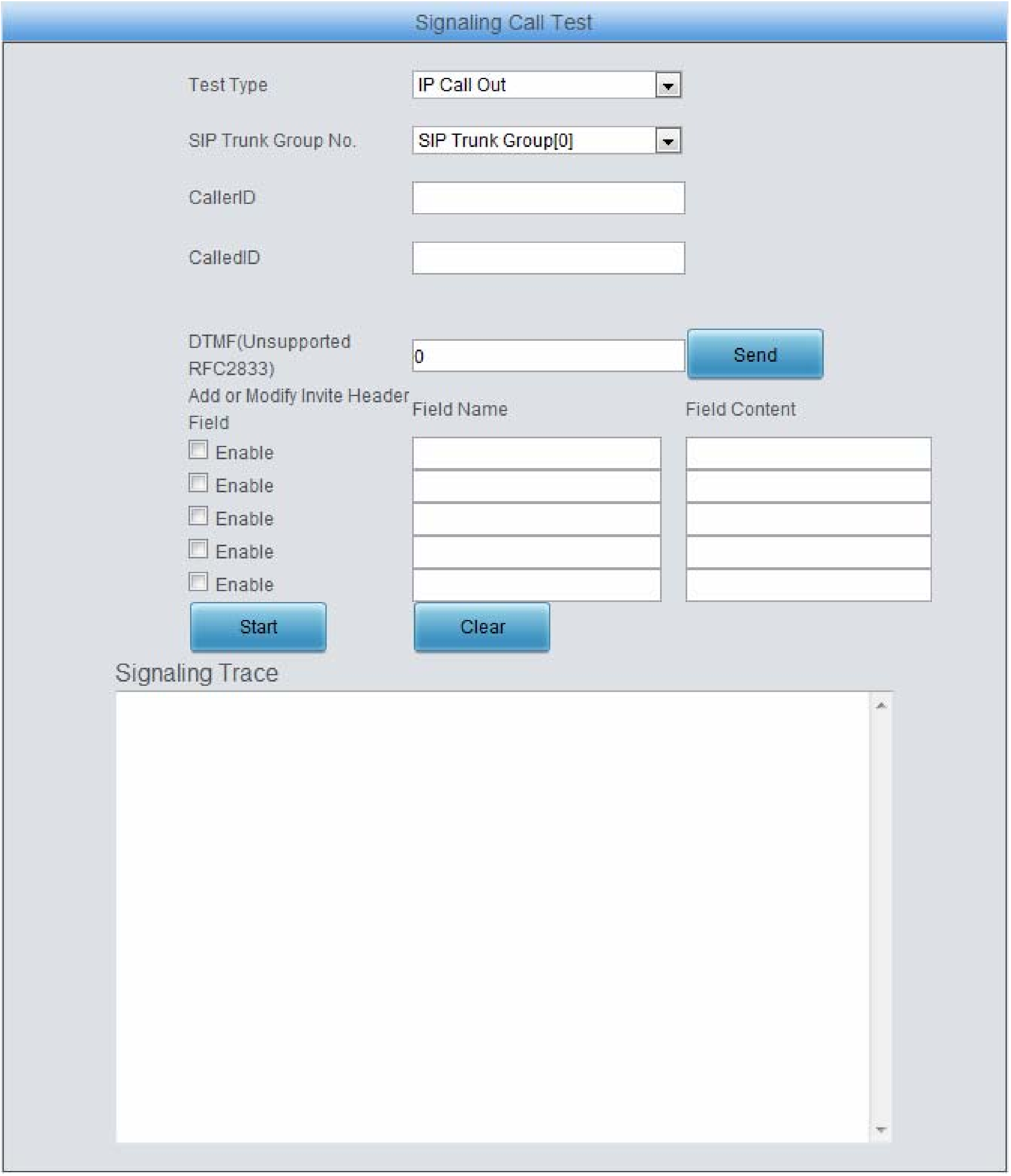


Figure 3-61 Signaling Call Test Interface

See Figure 3-61 for the Signaling Call Test interface. This feature can help to test whether the route and the number manipulation already configured are proper or not, and whether the call can succeed or not.

The table below explains the configuration items shown in the above figure.

Item	Description
Test Type	The source trunk type for signaling call test.
SIP Trunk Group No.	The SIP trunk group number you are required to select.

CallerID	The CallerID for the signaling call test.
CalleeID	The CalleeID for the signaling call test.
DTMF	You can select this item to send DTMFs after the establishment of call conversation on the channel for call test.
Add Invite Header, Field Name, Field Content	You can add the invite header and its corresponding content.
Signaling Trace	The information returned during the signaling call test, helping you to learn the detailed information about the test call.

After configuration, click ***Start*** to execute the signaling call test; click ***Clear*** to clear the signaling trace information.

Note: The call test will be finished only if the called party ends it. That is, the gateway can not stop the testing.

3.7.10 Signaling Call Track

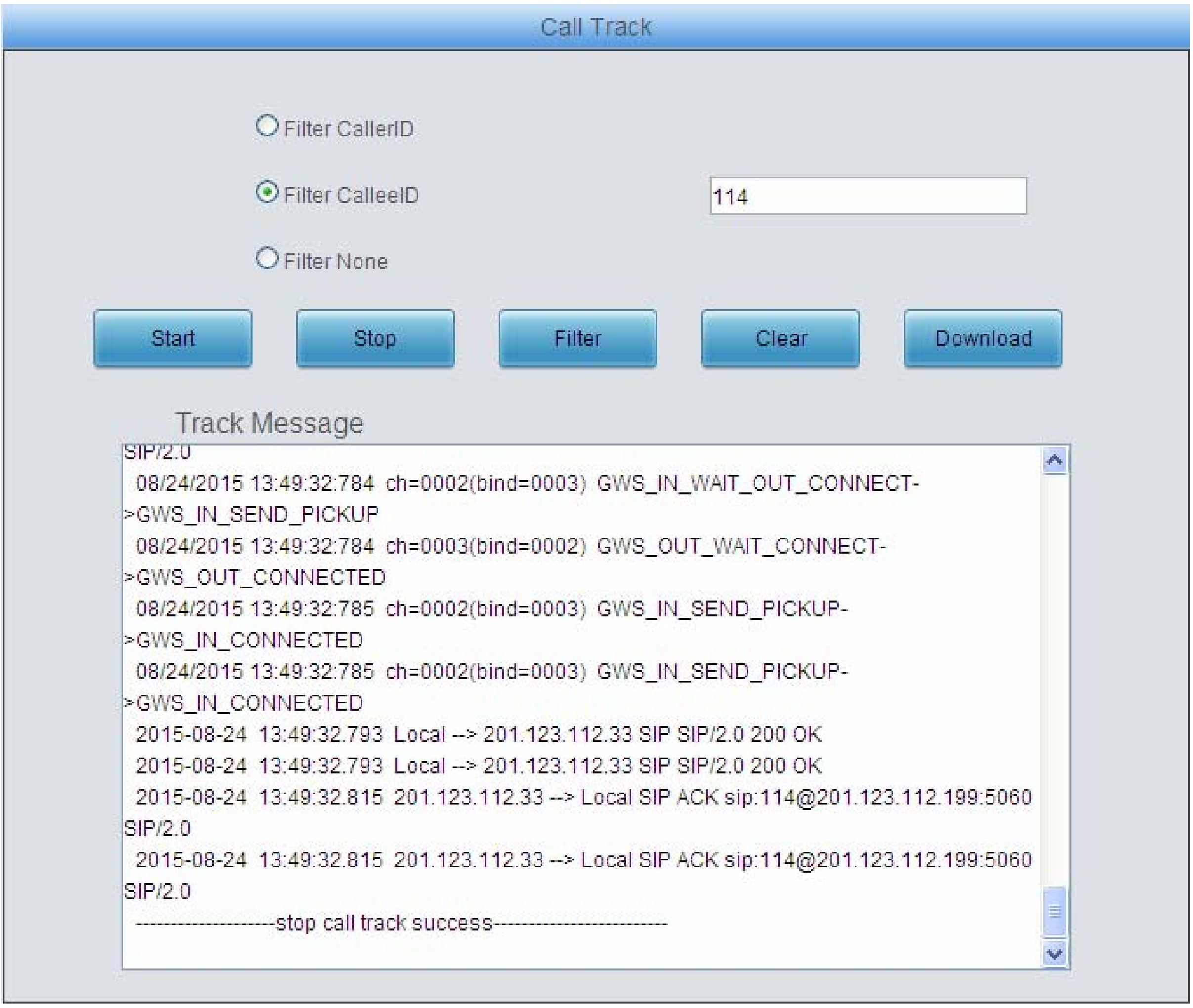


Figure 3-62 Call Track Interface

See Figure 3-62 for the Call Track Interface, including three modes: Filter CallerID, Filter CalleeID and Filter None. This is mainly used to output and save call information, facilitating call trace and problem debugging. Click ***Start*** to track calls, and the trace logs will be shown in the “Track Message” field; click ***Stop*** to stop the call track; click ***Filter*** to filter the trace logs according to the condition you set; click ***Clear*** to clear all trace logs; click ***download*** to download trace logs.

3.7.11 Network Speed Tester

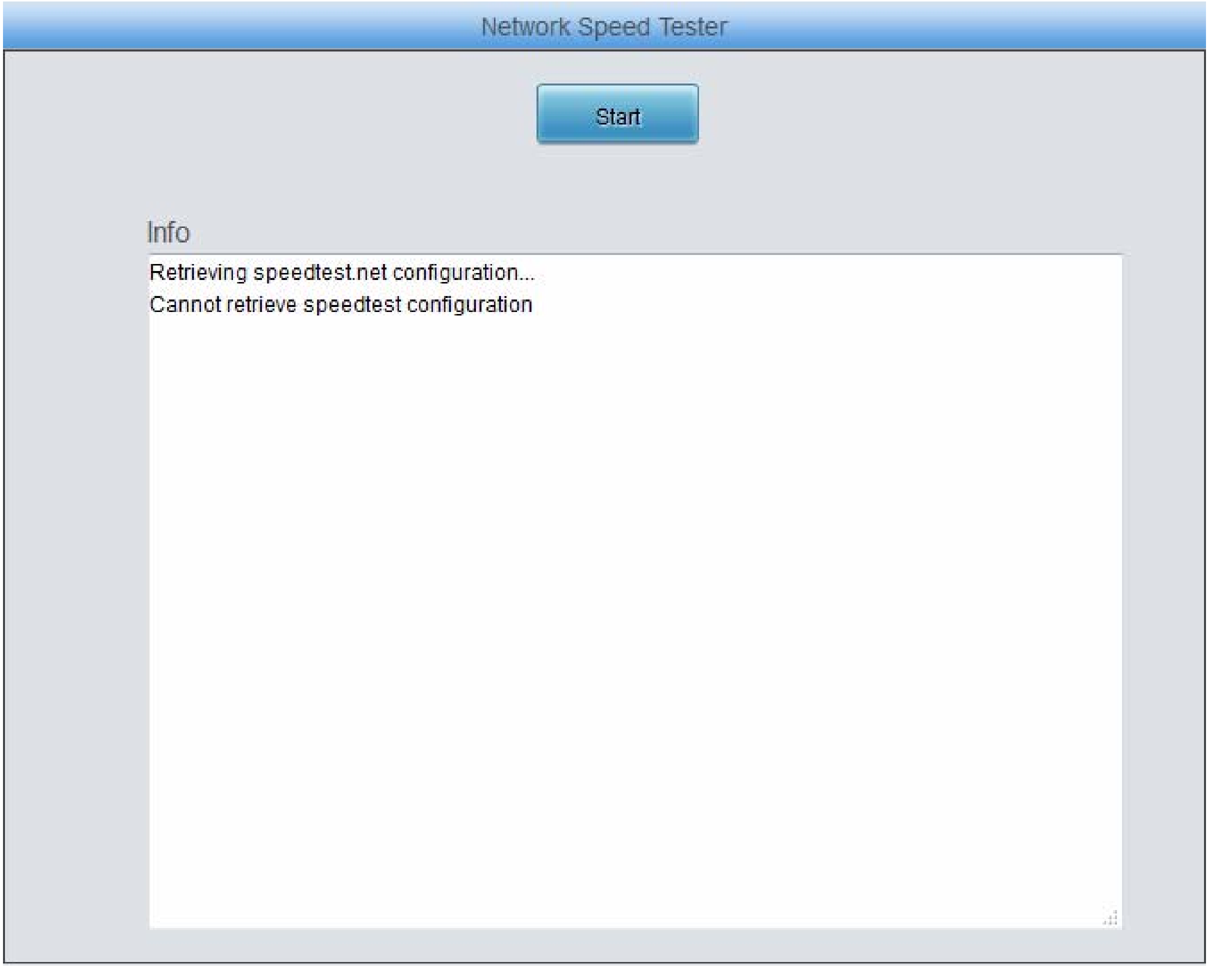


Figure 3-63 Network Speed Tester Interface

See Figure 3-63 for the Network Speed Tester interface, which is used to test the network speed of the outer net where the gateway locates. Click ***start***, it will select an optimal outer net to do the test. All the testing information will be displayed in the Info column.

3.7.12 PING Test

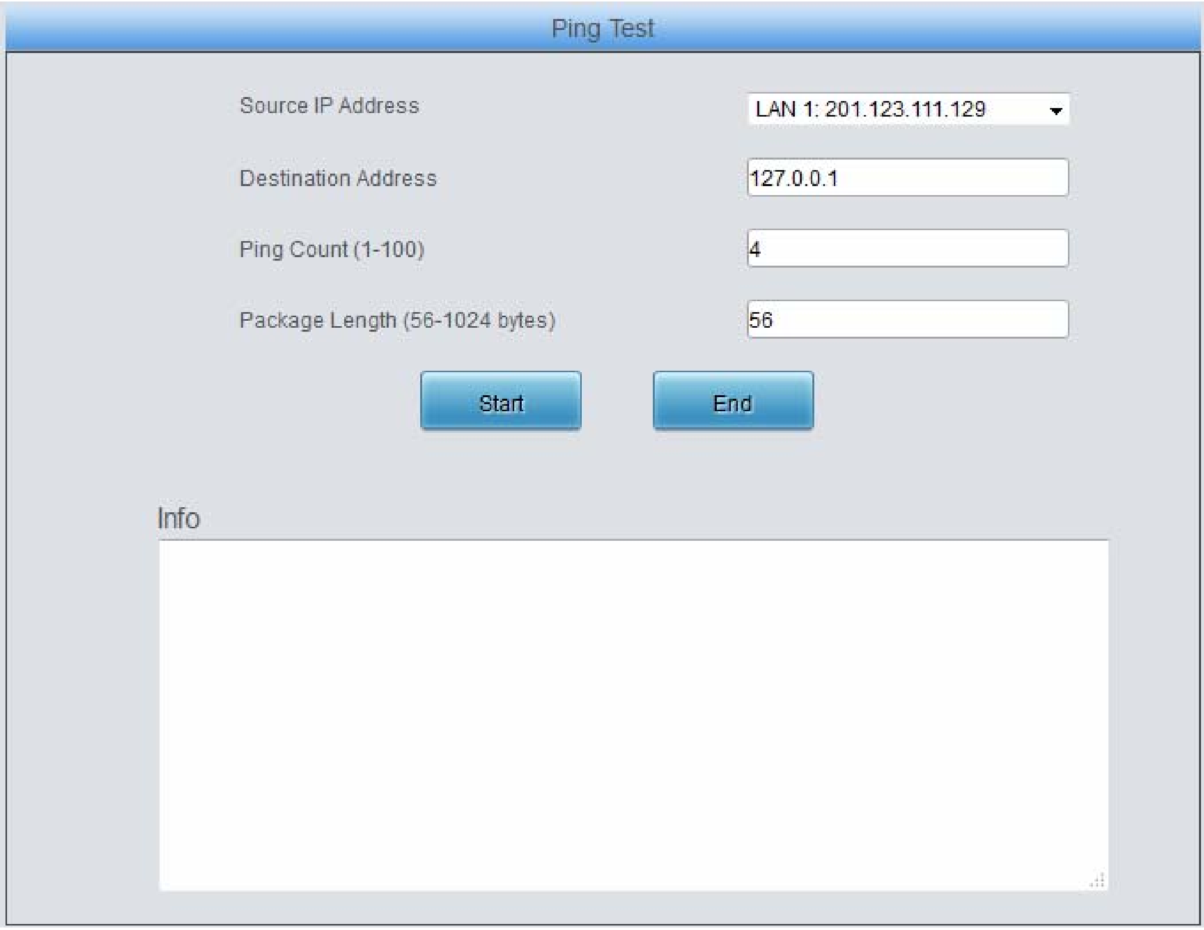


Figure 3-64 Ping Test Interface

See Figure 3-64 for the Ping Test interface. A Ping test can be initiated from the gateway on a designated IP address to check the connection status between them. The table below explains the configuration items shown in the above figure.

Item	Description
Source IP Address	Source IP address where the Ping test is initiated.
Destination Address	Destination IP address on which the Ping test is executed.
Ping Count	The number of times that the Ping test should be executed. Range of value: 1~100.
Package Length	Length of a data package used in the Ping test. Range of value: 56~1024 bytes.
Info	The information returned during the Ping test, helping you to learn the network connection status between the gateway and the destination address.

After configuration, click ***Start*** to execute the Ping test; click ***End*** to terminate it immediately.

3.7.13 TRACERT Test

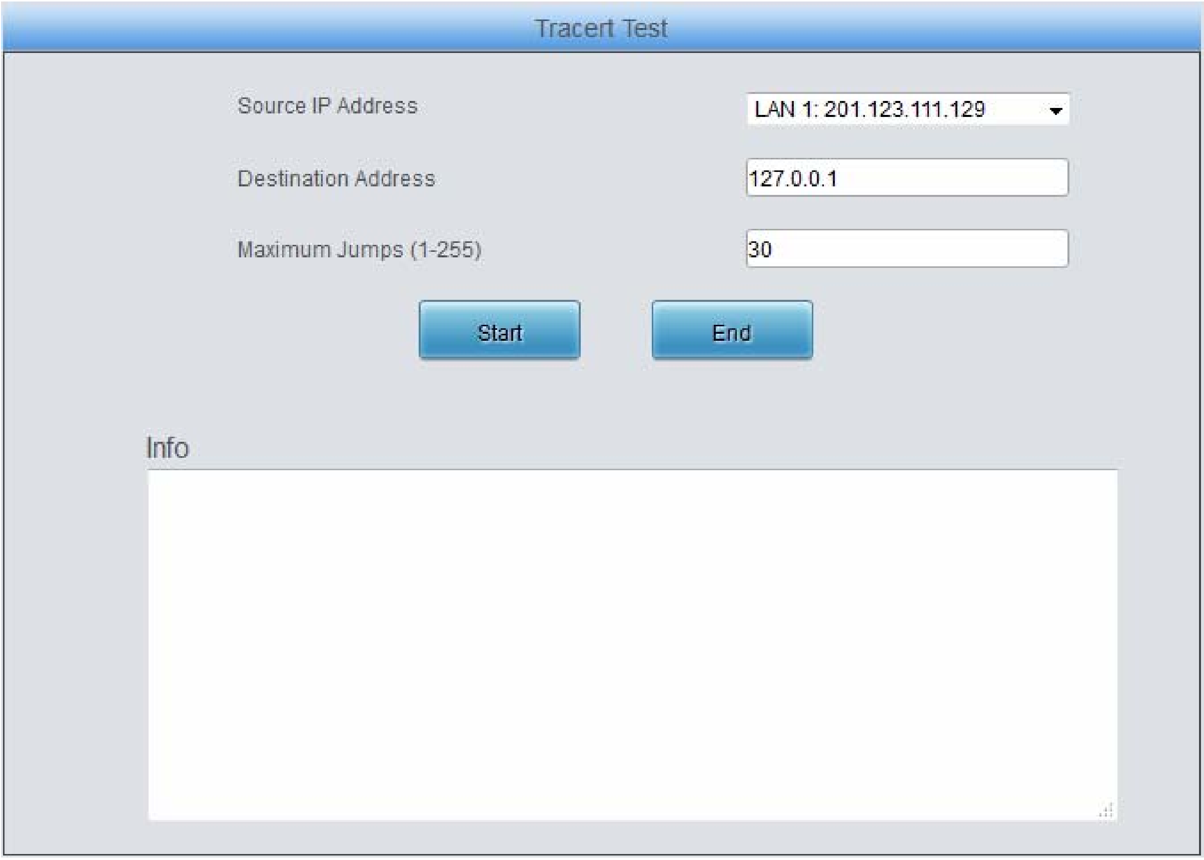


Figure 3-65 Tracert Test Interface

See Figure 3-65 for the Tracert Test interface. A Tracert test can be initiated from the gateway on a designated IP address to check the routing status between them. The table below explains the configuration items shown in the above figure.

Item	Description
Source IP Address	Source IP address where the Tracert test is initiated.
Destination Address	Destination IP address on which the Tracert test is executed.
Maximum Jumps	Maximum number of jumps between the gateway and the destination address, which can be returned in the Tracert test. Range of value: 1~255.
Info	The information returned during the Tracert test, helping you to learn the detailed information about the jumps between the gateway and the destination address.

After configuration, click ***Start*** to execute the Tracert test; click ***End*** to terminate it immediately.

3.7.14 Modification Record

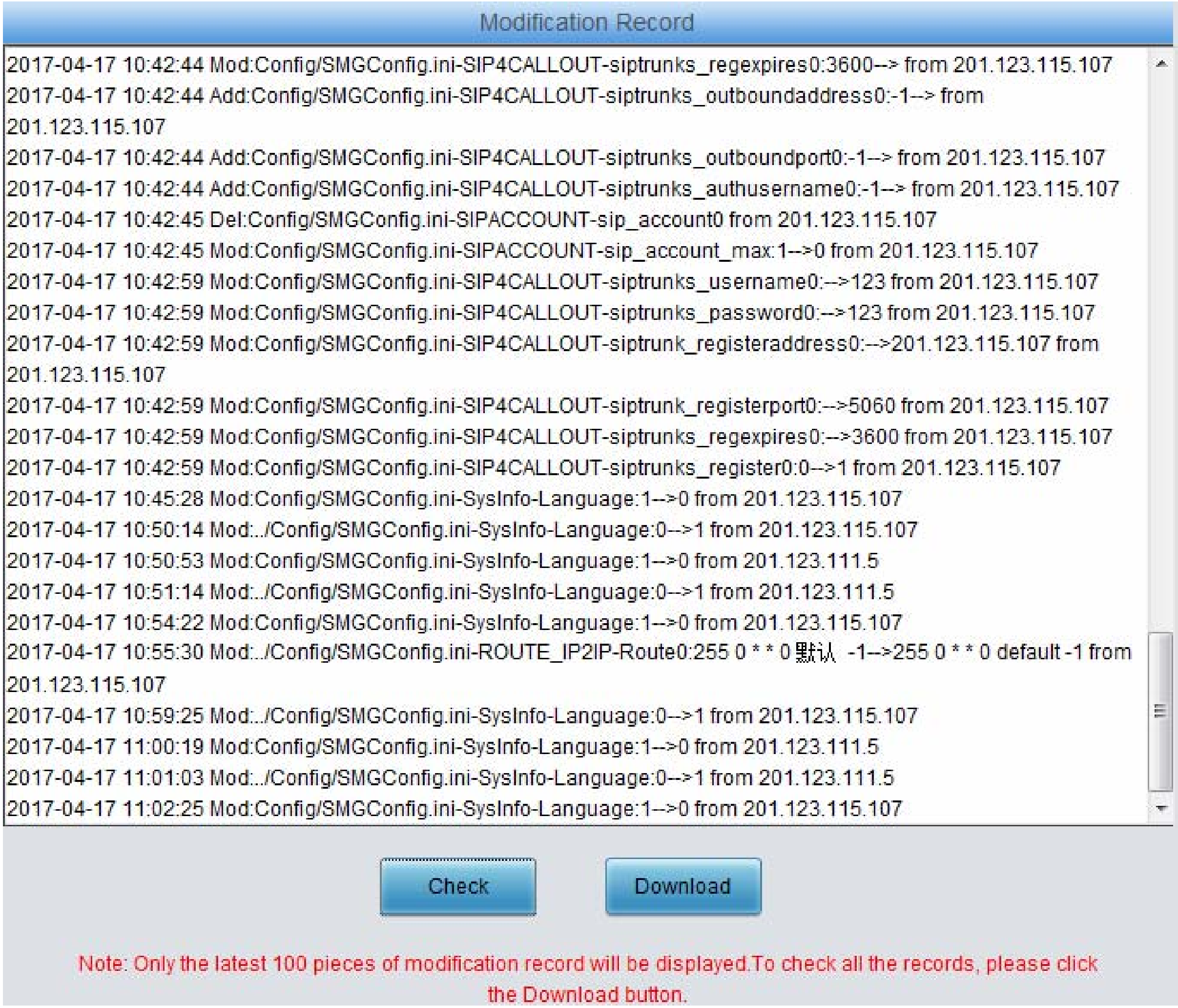


Figure 3-66 Modification Interface

The Modification Record interface is used to check the modification record on the web configuration. Click ***Check*** and the modification record will be shown on the dialog box. See Figure 3-66. Click ***Download*** to download the record file.

3.7.15 Backup & Upload

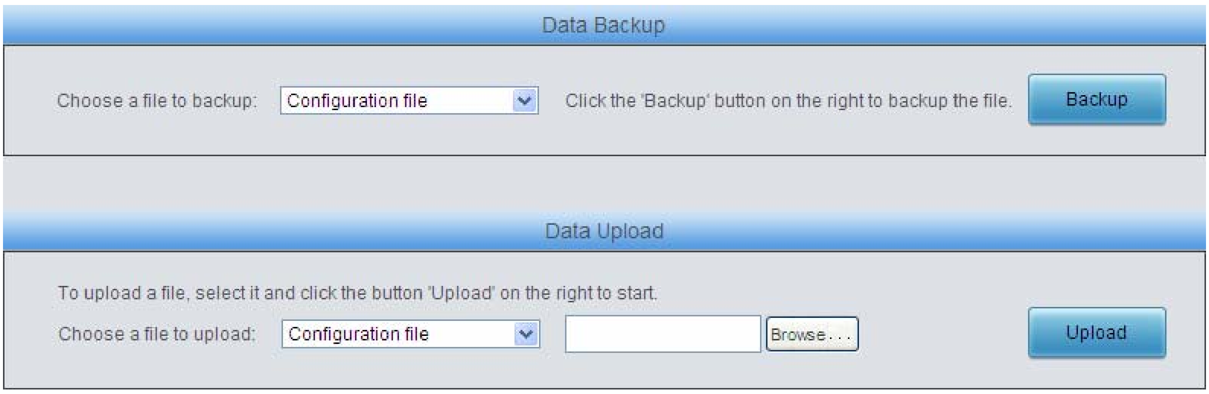


Figure 3-67 Backup & Upload Interface

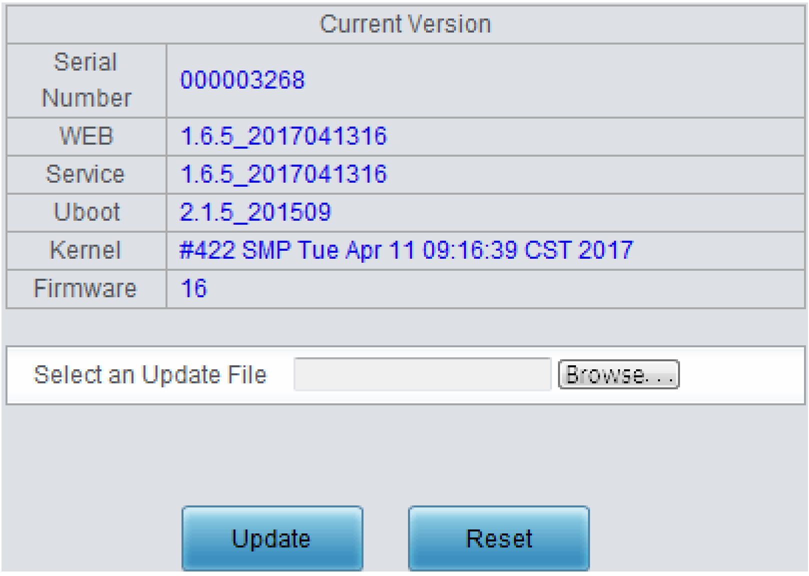
See Figure 3-67 for the Backup and Upload interface. To back up data to your PC, you shall first choose the file in the pull-down list and then click ***Backup*** to start. To upload a file to the gateway, you shall first choose the file type in the pull-down list, then select it via ***Browse…***, and at last click ***Upload***. The gateway will automatically apply the uploaded data to overwrite the current configurations.

3.7.16 Factory Reset

Figure 3-68 Factory Reset Interface

See Figure 3-68 for the Factory Reset interface. Click ***Reset*** to restore all configurations on the gateway to factory settings.

3.7.17 Upgrade



Current Version	
Serial Number	000003268
WEB	1.6.5_2017041316
Service	1.6.5_2017041316
Uboot	2.1.5_201509
Kernel	#422 SMP Tue Apr 11 09:16:39 CST 2017
Firmware	16

Figure 3-69 Upgrade Interface

See Figure 3-69 for the upgrade interface where you can upgrade the WEB, gateway service, kernel and firmware to new versions. Select the upgrade package “*.tar.gz” via ***Browse…*** and click ***Update*** (The gateway will do MD5 verification before upgrading and will not start to upgrade until it passes the verification). Wait for a while and the gateway will finish the upgrade automatically. Note that clicking ***Reset*** can only delete the selected update file but not cancel the operation of ***Update***.

3.7.18 Change Password

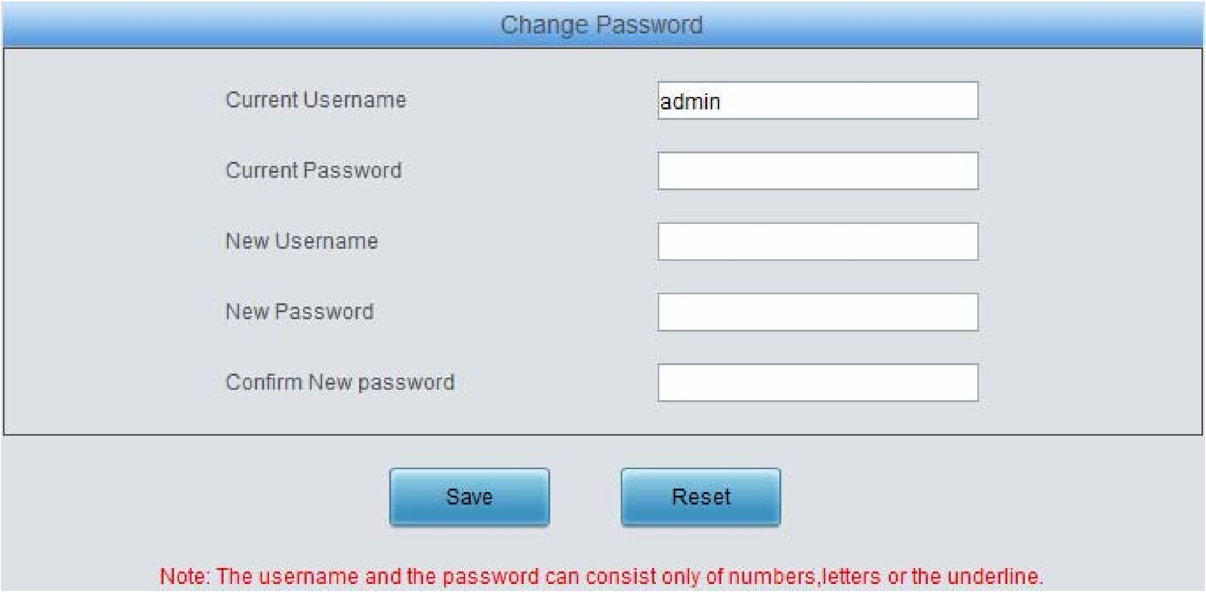


Figure 3-70 Password Changing Interface

See Figure 3-70 for the Password Changing interface where you can change username and password of the gateway. Enter the current password, the new username and password, and then confirm the new password. After configuration, click ***Save*** to apply the new username and password or click ***Reset*** to restore the configurations. After changing the username and password, you are required to log in again.

3.7.19 Device Lock

Figure 3-71 Device Lock Configuration Interface

See Figure 3-71 for the Device Lock Configuration interface. When you select one or more than one conditions to lock the gateway, the configurations of the gateway related to the selected conditions will be locked. That is, to modify any one of those configurations, you are required to input the lock password. Click ***Lock*** after setting and the device lock interface will be locked. To unlock the interface, enter your password (just the lock password) and click the ***Unlock*** button.

Figure 3-72 Unlock Device Interface

3.7.20 Restart

Figure 3-73 Service/System Restart Interface

See Figure 3-73 for the Restart interface. Click ***Restart*** on the service restart interface to restart the gateway service or click ***Restart*** on the system restart interface to restart the whole gateway system.

Chapter 4 Typical Applications

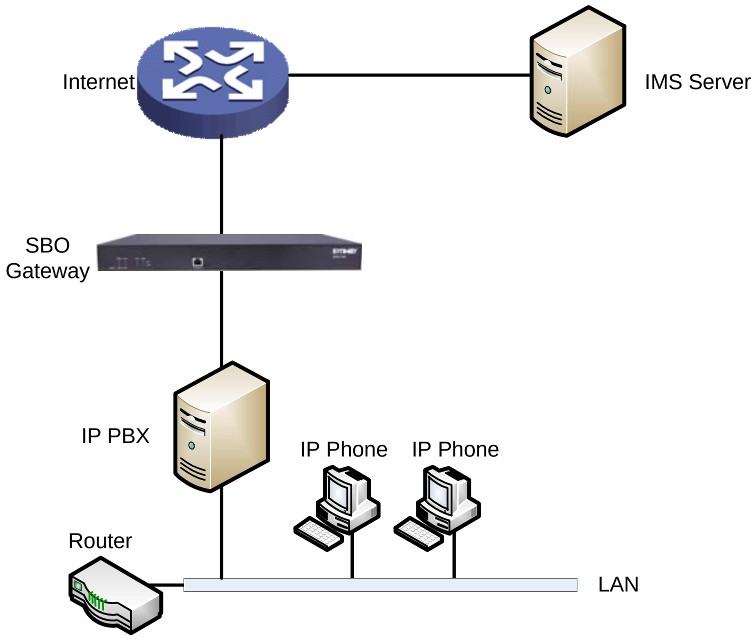


Figure 4-1 Application 1

1. Configure SIP Settings.

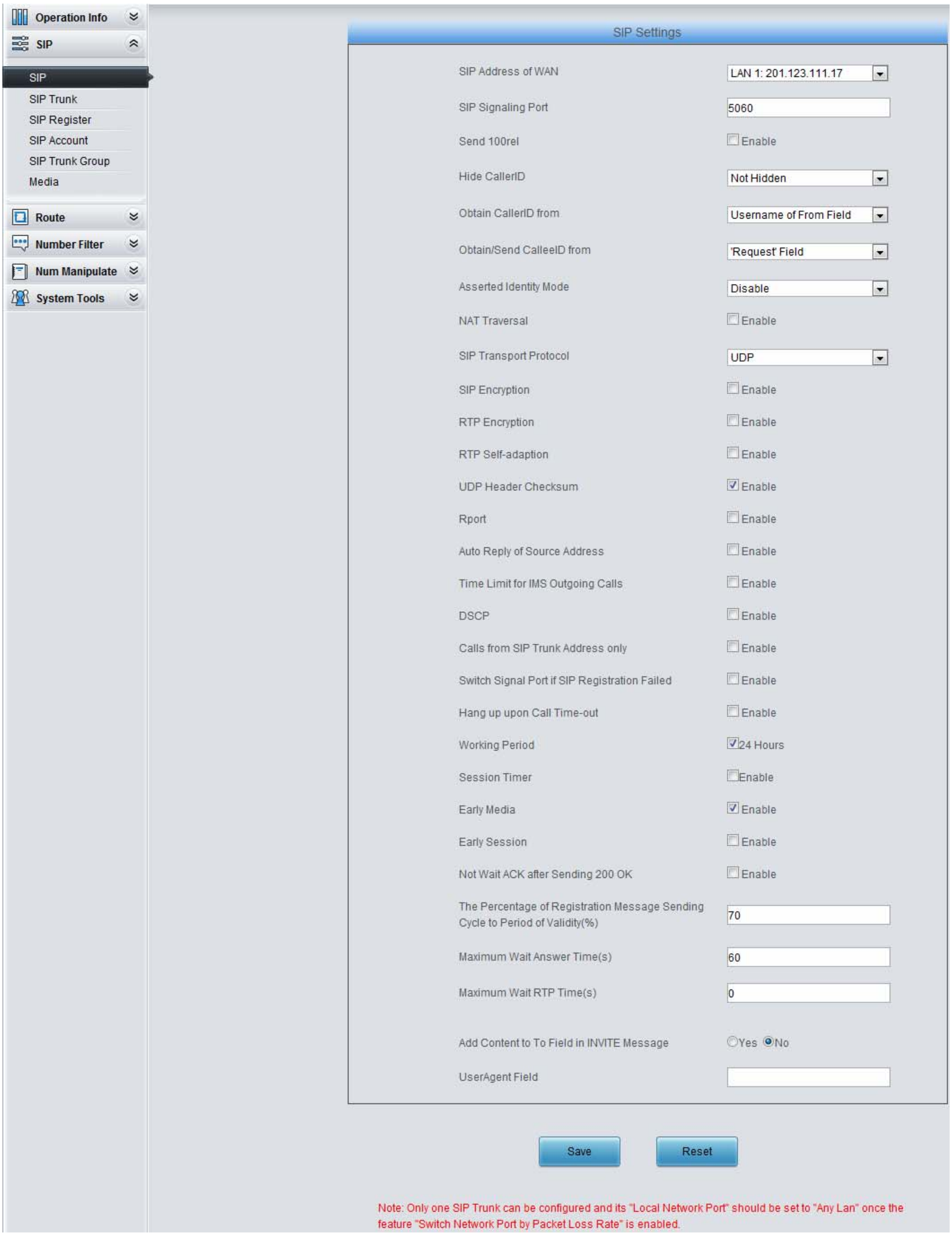


Figure 4-2

2. Add the IP addresses of the SIP terminal.

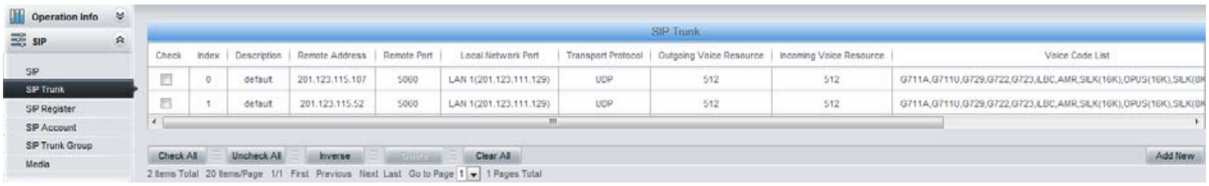


Figure 4-3

3. Add the SIP trunks into the corresponding SIP trunk groups.

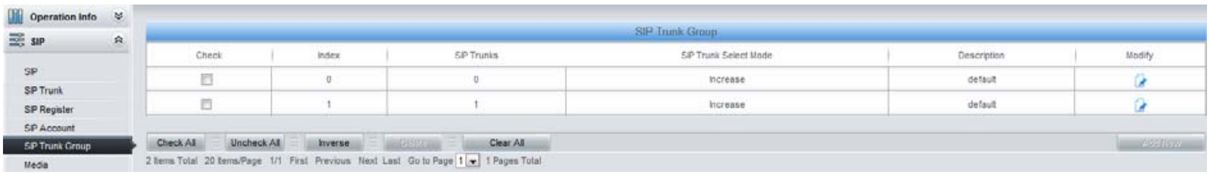


Figure 4-4

4. Set routing parameters. You may adopt the default value ‘Route before Number Manipulate’ for both configuration items.

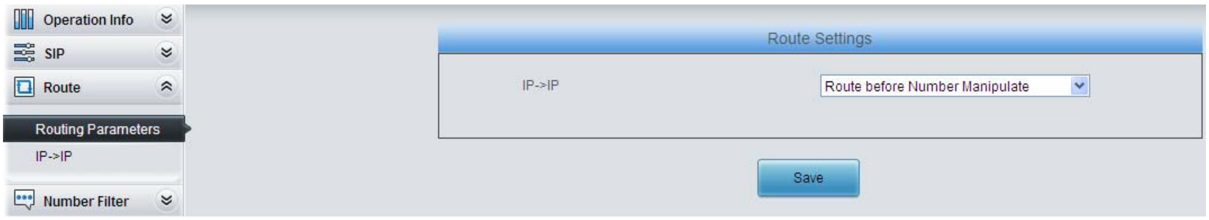


Figure 4-5

5. Set IP→IP routing rules to route calls from different SIP trunk groups to the corresponding SIP trunk groups.

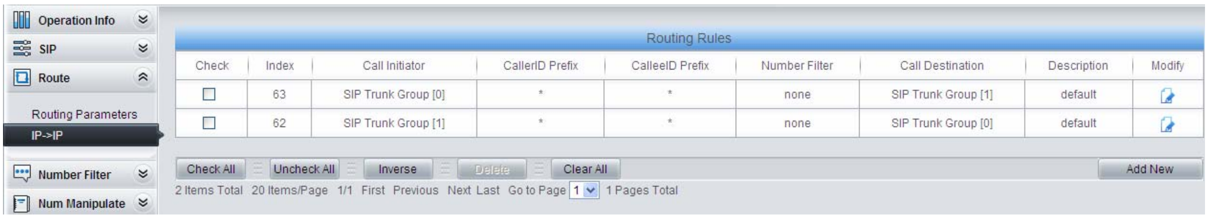


Figure 4-6

6. Set number manipulation rules. When the gateway receives a call from IP, it will first check the CalleeID prefix. If the CalleeID prefix is 7 or 8, the gateway will delete it before routing the call to the corresponding SIP trunk group.

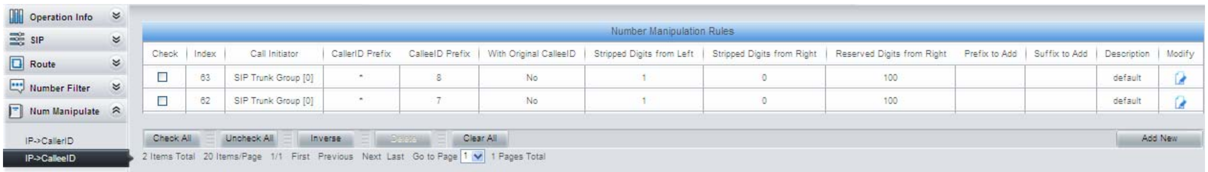


Figure 4-7

Appendix A Technical Specifications

Dimensions

SBO500: 440×44×267 mm^3

SBO2000: 440×44×690 mm^3

Weight

SBO500: About 3.1 kg

SBO2000: About 12kg

Environment

Operating temperature: 0℃—40℃

Storage temperature: -20℃—85℃

Humidity: 8%— 90% non-condensing

Storage humidity: 8%— 90% non-condensing

NET

Amount: 2 (10/100/1000 BASE-TX (RJ-45))

Self-adaptive bandwidth supported

Auto MDI/MDIX supported

Console Port

*Amount: 1 (RS-232), 8 (USB*2)*

Baud rate: 115200bps

Connector: RJ45 （See Hardware Description for signal definition）

Data bits: 8 bits

Stop bit: 1 bit

Parity unsupported

Flow control unsupported

Note: Follow the above settings to configure the console port; or it may work abnormally.

Power Requirements

Input power: 100~240V AC

Maximum power consumption:

SBO500: ≤22W

SBO2000: ≤167W

Signaling & Protocol

SIP signaling: SIP V1.0/2.0, RFC3261

Audio Encoding & Decoding

G.711A	64 kbps
G.711U	64 kbps
G.729	8 kbps
G723	5.3/6.3 kbps
G722	64 kbps
AMR	4.75/5.15/5.90/6.70/7.40/7.95/10.20/12.20 kbps
iLBC	15.2 kbps
SILK(16K)	20 kbps
OPUS(16K)	20 kbps
SILK(8K)	20 kbps
OPUS(8K)	20 kbps

Sampling Rate

8kHz

Safety

Lightning resistance: Level 4

Appendix B Troubleshooting

1. What to do if I forget the IP address of the SBO gateway?

Long press the Reset button on the gateway to restore to factory settings. Thus the IP address will be restored to its default value:

NET1: 192.168.1.101

NET2: 192.168.0.101

2. In what cases can I conclude that the SBO gateway is abnormal and turn to Synway's technicians for help?

a) During runtime, the run indicator does not flash or the alarm indicator lights up or flashes, and such error still exists even after you restart the device or restore it to factory settings.

b) Voice problems occur during call conversation, such as that one party or both parties cannot hear the voice or the voice quality is unacceptable.

Other problems such as abnormal SIP trunk status, inaccessible calls, failed registrations and incorrect numbers are probably caused by configuration errors. We suggest you refer to Chapter 3 WEB Configuration for further examination. If you still cannot figure out or solve your problems, please feel free to contact our technicians.

3. What to do if I cannot enter the WEB interface of the SBO gateway after login?

This problem may happen on some browsers. To settle it, follow the instructions here to configure your browser. Enter 'Tools > Internet Options >Security Tab', and add the current IP address of the gateway into 'Trusted Sites'. If you change the IP address of the gateway, add your new IP address into the above settings.

Appendix C Technical/sales Support

Thank you for choosing Synway. Please contact us should you have any inquiry regarding our products. We shall do our best to help you.

Headquarters

Synway Information Engineering Co., Ltd

http://www.synway.net/

9F, Synway D&R Center, No.3756, Nanhuan Road, Binjiang District, Hangzhou, P.R.China, 310053

Tel: +86-571-88860561

Fax: +86-571-88850923

Wechat QR Code: Scan the QR code below to add us on Wechat.

Technical Support

Tel: +86-571-88864579

Mobile: +86-18905817070

Email: techsupport@sanhuid.com

Email: techsupport@synway.net

MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: sales@synway.net