



**Synway SBC Series Gateway**

**SBC500**

# **User Manual**

**Version 1.8.0**

**Synway Information Engineering Co., Ltd**  
**[www.synway.net](http://www.synway.net)**

# Content

<b>Content .....</b>	<b>i</b>
<b>Copyright Declaration.....</b>	<b>iii</b>
<b>Revision History.....</b>	<b>iv</b>
<b>Chapter 1 Product Introduction .....</b>	<b>1</b>
1.1 Typical Application .....	1
1.2 Feature List .....	1
1.3 Hardware Description .....	2
1.4 Alarm Info.....	4
<b>Chapter 2 Quick Guide .....</b>	<b>5</b>
<b>Chapter 3 WEB Configuration .....</b>	<b>7</b>
3.1 System Login .....	7
3.2 Operation Info .....	7
3.2.1 System Info .....	7
3.2.2 IP Status .....	9
3.2.3 Call Monitor .....	10
3.2.4 Client Info .....	11
3.2.5 Client Status .....	11
3.2.6 Call Count.....	11
3.2.7 SIP Account Call Count .....	12
3.2.8 Warning Info .....	12
3.3 SIP Settings .....	12
3.3.1 SIP.....	12
3.3.2 Hot Backup (HA) .....	16
3.3.3 SIP Trunk.....	16
3.3.4 SIP Register .....	19
3.3.5 SIP Account.....	19
3.3.6 SIP Trunk Group.....	20
3.3.7 Media Settings.....	21
3.4 Fax Settings .....	23
3.4.1 Fax.....	23
3.5 Route Settings .....	24
3.5.1 Routing Parameters .....	24
3.5.2 IP to IP.....	25
3.6 Number Filter .....	26
3.6.1 Whitelist.....	26
3.6.2 Blacklist .....	27
3.6.3 Number Pool .....	27
3.6.4 Filtering Rule .....	27
3.7 Number Manipulation .....	28
3.7.1 IP to IP CallerID.....	28
3.7.2 IP to IP CalleeID .....	29
3.7.3 CallerIP Pool.....	30
3.8 VPN.....	31
3.8.1 VPN Server Settings .....	31
3.8.2 VPN Account .....	31
3.9 DHCP.....	32
3.10 System Tools.....	32
3.10.1 Network .....	32
3.10.2 Authorization .....	32
3.10.3 Management .....	33

3.10.4	IP Routing Table .....	34
3.10.5	Firewall .....	34
3.10.6	IDS Settings .....	35
3.10.7	DDOS Settings .....	35
3.10.8	Certificate Management .....	36
3.10.9	Centralized Manage .....	36
3.10.10	SIP Account Generator.....	37
3.10.11	Recording Manage .....	38
3.10.12	Configuration File .....	38
3.10.13	Signaling Capture .....	38
3.10.14	Signaling Call Test.....	39
3.10.15	Signaling Call Track.....	39
3.10.16	Network Speed Tester .....	40
3.10.17	PING Test .....	40
3.10.18	TRACERT Test .....	41
3.10.19	Modification Record.....	41
3.10.20	Backup & Upload.....	41
3.10.21	Factory Reset .....	41
3.10.22	Upgrade.....	41
3.10.23	Account Manage.....	41
3.10.24	Change Password .....	43
3.10.25	Device Lock .....	43
3.10.26	Restart .....	43
<b>Chapter 4 Typical Applications .....</b>		<b>44</b>
<b>Appendix A Technical Specifications.....</b>		<b>46</b>
<b>Appendix B Troubleshooting .....</b>		<b>47</b>
<b>Appendix C Technical/sales Support .....</b>		<b>48</b>

# Copyright Declaration

All rights reserved; no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without prior written permission from Synway Information Engineering Co., Ltd (hereinafter referred to as 'Synway').

Synway reserves all rights to modify this document without prior notice. Please contact Synway for the latest version of this document before placing an order.

Synway has made every effort to ensure the accuracy of this document but does not guarantee the absence of errors. Moreover, Synway assumes no responsibility in obtaining permission and authorization of any third party patent, copyright or product involved in relation to the use of this document.

## Revision History

Version	Date	Comments
Version 1.7.0	2018.6	Initial publication
Version 1.8.0	2019.12	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 SBC Series Gateway Products!

The Synway SBC series gateway products (hereinafter referred to as 'SBC gateway') are mainly used for connecting the IP telephony network or IP PBX, providing such features as transcoding, routing, number filtering, number conversion, etc. At present, the SBC series gateway products mainly include the model SBC500.

## 1.1 Typical Application

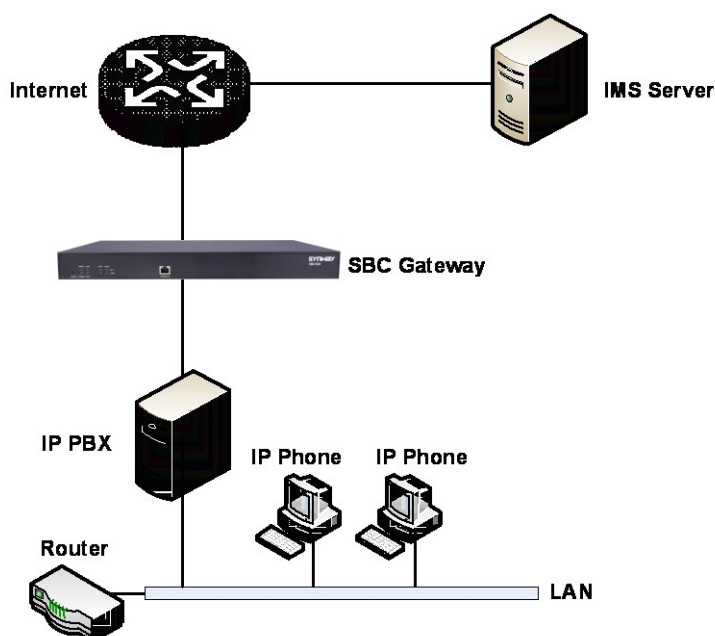


Figure 1-1 SBC Typical Application

## 1.2 Feature List

Basic Features	Description
<b>IP Call</b>	Call initiated from IP to a designated SIP trunk, via routing and number manipulation.
<b>Number Manipulation</b>	Peels off some digits of a phone number from left/right, or adds a prefix/suffix to a phone number.
<b>VoIP Routing</b>	Routing path: from IP to IP.
Signaling & Protocol	Description
<b>SIP Signaling</b>	Supported protocol: SIP V1.0/2.0, RFC3261

<b>Voice</b>	CODEC	G.711A, G.711U, G.729, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K)
	DTMF Mode	RFC2833, SIP INFO, INBAND, RFC2833+Signaling, In-band+Signaling
<b>Network</b>	<b>Description</b>	
<b>Network Protocol</b>	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN	
<b>Static IP</b>	IP address modification support	
<b>DNS</b>	Domain Name Service support	
<b>Firewall</b>	Firewall setting support	
<b>SIP Encryption</b>	SIP TLS encryption support	
<b>RTP Encryption</b>	RTP encryption protocol SRTP support	
<b>DOS/DDOS Protection</b>	Defense from DOS/DDOS attack	
<b>PPPoE</b>	PPPoE support	
<b>IPV4/IPV6</b>	IPV4 and IPV6 support	
<b>Security</b>	<b>Description</b>	
<b>Admin Authentication</b>	Support admin authentication to guarantee the resource and data security	
<b>Maintain &amp; Upgrade</b>	<b>Description</b>	
<b>WEB Configuration</b>	Support of configurations through the WEB user interface	
<b>Language</b>	Chinese, English	
<b>Software Upgrade</b>	Support of user interface, gateway service, kernel and firmware upgrades based on WEB	
<b>Tracking Test</b>	Support of Ping and Tracert tests based on WEB	
<b>SysLog Type</b>	Three options available: ERROR, WARNING, INFO	

## 1.3 Hardware Description

The SBC gateway features 1U rackmount design and integrates embedded LINUX system within the POWERPC+DSP hardware architecture. It has 2 Kilomega-Ethernet ports (LAN1 and LAN2) on the chassis.

See the figures below for SBC500 series' appearance:



Figure 1-2 Front View



Figure 1-3 Rear View



Figure 1-4 Left View

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

Interface	Description
<b>LAN</b>	Amount: 2
	Type: RJ-45
	Bandwidth: 10/100/1000Mbps
	Self-Adaptive Bandwidth Supported
	Auto MDI/MDIX Supported
<b>Console Port</b>	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-5 for signal definition)
	Data Bits: 8 bits
	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
Button	Description
<b>Power Key</b>	Power on/off the SBC gateway. You can turn on the two power keys at the same time to have the power supply working in the hot-backup mode.



<b>Reset Button</b>	Restore the gateway to factory settings.
LED	Description
<b>Power Indicator</b>	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
<b>Run Indicator</b>	Indicates the running status. For more details, refer to <a href="#">Alarm Info</a> .
<b>Alarm Indicator</b>	Alarms the device malfunction. For more details, refer to <a href="#">Alarm Info</a> .
<b>Link Indicator</b>	The green LED on the left of LAN, indicating the network connection status.
<b>ACT Indicator</b>	The orange LED on the right of LAN, whose flashing tells data are being transmitted.

**Note:** The console port is used for debugging. While connection, 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.

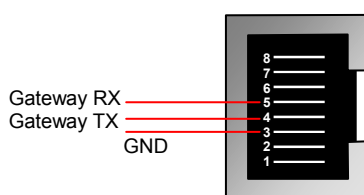


Figure 1-5 Console Port Signal Definition

For other hardware parameters, refer to [Appendix A Technical Specifications](#).

## 1.4 Alarm Info

The SBC 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
<b>Run Indicator</b>	Go out	System is not yet started.
	Light up	System is starting.
	Flash	Device is running normally.
<b>Alarm Indicator</b>	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 SBC gateway in the shortest time.

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

- SBC Series Gateway \*1
- Angle Bracket \*2, Rubber Foot Pad \*4, Screw for Angle Bracket \*8
- 220V Power Cord \*2
- Warranty Card \*1
- Installation Manual \*1

### Step 2: Properly fix the SBC gateway.

If you do not need to place the gateway on the rack, simply fix the 4 rubber foot pads. Otherwise, you should first fix the angle brackets onto the chassis and then place the chassis on the rack.

### 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 SBC 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 (LAN 1: 192.168.1.101 or LAN 2: 192.168.0.101) of the SBC 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 [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 [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 LAN. Refer to [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 IP status.

After the configuration of signaling protocols, you can check the channel state via 'Operation Info → IP Status'. Refer to [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. 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 IP address of the SIP trunk which calls in 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**. Provided the IP address of the SIP trunk which calls out 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 SIP trunk configured in Step 1 into the corresponding SIP trunk group. Refer to 'SIP Settings → [SIP Trunk Group](#)' for detailed instructions. 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 SIP Trunk Group[0] set in Step 2 as 'Call Initiator' and SIP Trunk Group[1] set in Step 3 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 SIP Trunk 0 configured in Step 1 to the IP address and port of the SBC 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 SBC 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 SBC 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.

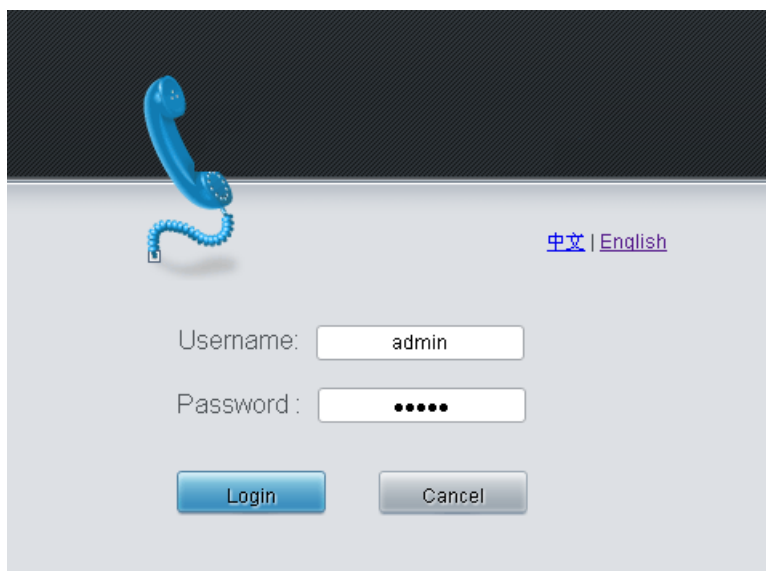


Figure 3-1 Login Interface

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 [Change Password](#).

After login, you can see the main interface.

### 3.2 Operation Info

Operation Info includes the following parts: **System Info**, **IP Status**, **Call Monitor**, **Register Status**, **Client Info**, **Client Status**, **Call Count**, **SIP Account Call Count** and **Warning Info**, showing the current running status of the gateway.

#### 3.2.1 System Info

On the System Info interface, you can click **Refresh** to obtain the latest system information. See below for details.

Item	Description
<b>MAC Address</b>	MAC address of LAN 1 or LAN 2.
<b>IP Address</b>	The three parameters from left to right are IP address, subnet mask and default gateway of LAN 1 or LAN 2.
<b>IPV6 Address</b>	The two parameters from left to right are IPV6 address and IPV6 address prefix of LAN 1 or LAN 2.
<b>DNS Server</b>	DNS server address of LAN 1 or LAN 2.
<b>Receive/Transmit Packets</b>	The amount of receive/transmit packets after the gateway's startup, including three categories: All, Error and Drop.

<b>Current Speed</b>	The current speed of data receiving and transmitting.
<b>Work Mode</b>	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.
<b>Network Type</b>	The type of the network, including three options: Static, DHCP and PPPoE.
<b>Runtime</b>	Time of the gateway keeping running normally after startup. This parameter updates every 2s.
<b>CPU Temperature</b>	Display the real time temperature of the CPU.
<b>CPU Usage Rate</b>	Display the real time usage rate of the CPU.
<b>Current RTP Message Data</b>	Display the receiving and sending information of the current RTP data.
<b>HA State</b>	The dual-system hot backup state in the <i>Call Status Agent</i> mode, including Primary, Backup, and Independent. The original configuration state and heartbeat network port are indicated in parentheses.
<b>DCMS Working Status</b>	Display the connecting status of the gateway and DCMS.
<b>Recording Work Status</b>	Display the working status of the recording server docked by the gateway.
<b>Authorization Status</b>	Display the features of the SBC device, which requires authorization.
<b>Authorization Numbers</b>	Display the number of authorized devices.
<b>Remaining Time</b>	Display the remaining time after successful authorization.
<b>Serial Number</b>	Unique serial number of an SBC gateway.
<b>WEB</b>	Current version of the WEB interface.
<b>Gateway</b>	Current version of the gateway service.
<b>Uboot</b>	Current version of Uboot.
<b>Kernel</b>	Current version of the system kernel on the gateway.
<b>Firmware</b>	Current version of the firmware on the gateway.

### 3.2.2 IP Status

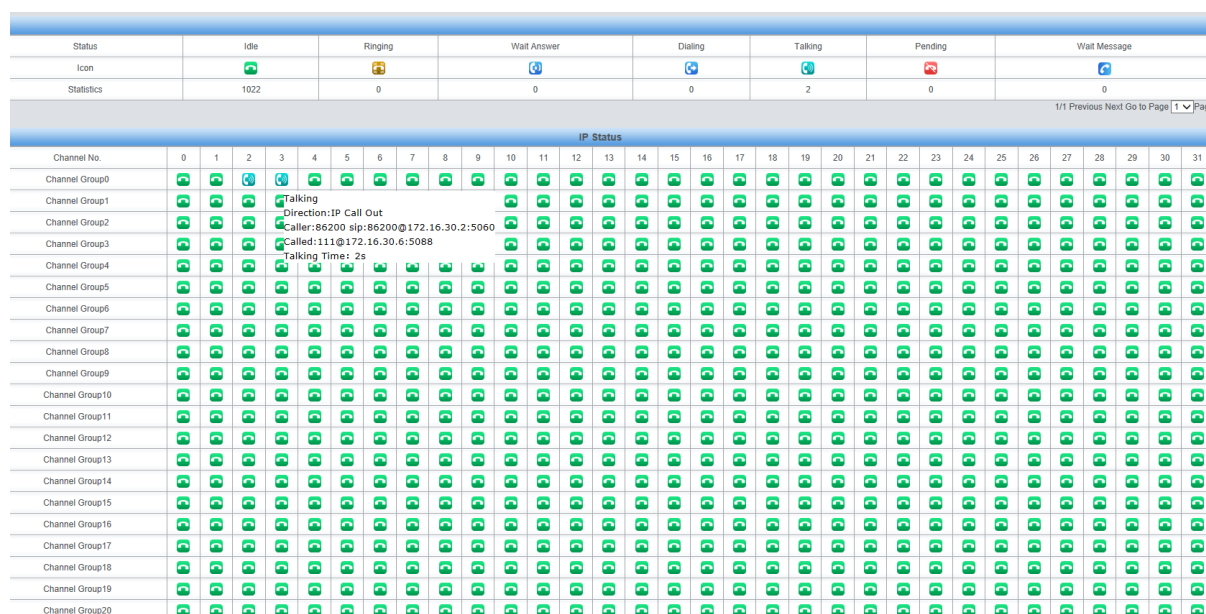























Figure 3-2 IP Status Interface

See Figure 3-2 for the IP status interface which shows the real-time status of each IP channel on the gateway. Note that this interface is unavailable when *SIP Working Mode* on the SIP Settings interface is set to *Call Status Agent*. See below for details.

Item	Description																								
Channel No.	Number of the IP channel on the device.																								
Status	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:																								
	<table><tr><th>State</th><th>Icon</th><th>Description</th></tr><tr><td>Idle</td><td></td><td>The channel is available.</td></tr><tr><td>Wait Answer</td><td></td><td>The channel receives the ringback tone and is waiting for the called party to pick up the phone.</td></tr><tr><td>Ringing</td><td></td><td>The channel is in the ringing state.</td></tr><tr><td>Talking</td><td></td><td>The channel is in a conversation.</td></tr><tr><td>Pending</td><td></td><td>The channel is in the pending state</td></tr><tr><td>Dialing</td><td></td><td>The channel is dialing.</td></tr><tr><td>Wait Message</td><td></td><td>The channel is waiting for the message from remote end.</td></tr></table>	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 end.
	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 end.																							

**Note:** The gateway provides the fuzzy search feature on this interface. After you click any characters on Figure 3-2, 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 3-3, after we input the character 111 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 111 occurs on Channel 12 and Channel 13 of Channel Group 0.

111

Search

Clear

Status	Idle	Ringing	Wait Answer	Dialing	Talking	Pending	Wait Message
Icon							
Statistics	1022	0	0	0	2	0	0

1/1 Previous Next Go to Page 1 Page

IP Status

Channel No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Channel Group0																																
Channel Group1																																
Channel Group2																																
Channel Group3																																
Channel Group4																																
Channel Group5																																
Channel Group6																																
Channel Group7																																
Channel Group8																																
Channel Group9																																
Channel Group10																																
Channel Group11																																
Channel Group12																																
Channel Group13																																
Channel Group14																																
Channel Group15																																
Channel Group16																																
Channel Group17																																


Figure 3-3 Search Calls

### 3.2.3 Call Monitor

On the Call Monitor interface, you can set a condition for call monitoring. For example, set the CalleeID 111 as the monitoring condition, and after you click the **Set** button, all the calls containing the CalleeID 111 will display in the Call Info list. The table below explains the items on this interface.

Item	Description
<b>Monitored CallerID,</b> <b>Monitored CalleeID,</b> <b>Monitored Remote Address</b>	Sets the condition for the call monitoring. You can set to monitor the calls by CallerID, CalleeID or remote address.
<b>Monitoring LAN Port</b>	Selects the LAN port which is used to monitor the calls.
<b>Channel No.</b>	The number of the channel, which starts from 0.
<b>Call Direction</b>	The direction of the monitored call, including two options: IP→ PSTN and PSTN→IP.
<b>Remote Address</b>	The remote address of the monitored call.
<b>Channel Status</b>	The status of the channel which the monitored call locates at.
<b>CallerID</b>	The CallerID of the monitored call.
<b>CalleeID</b>	The CalleeID of the monitored call.
<b>Start Time</b>	The start time of the monitored call.
<b>Duration</b>	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 RemoteListener, 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:

1. 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.
2. This interface is unavailable when *SIP Working Mode* on the SIP Settings interface is set to *Call Status Agent*.

### 3.2.4 Client Info

The Client List is only supported in the Call Status Agent mode. It displays the IMS accounts added by all customers. You can query by client name. See the figure below.

Figure 3-4 Client List Interface

### 3.2.5 Client Status

The Client Status interface displays the name of the encrypted client registered to the IMS server via the SBC server and its online status.

### 3.2.6 Call Count

The Call Count interface lists 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, and click **Download** to download all the call logs. The table below explains the items on this interface.

Item	Description
<b>SIP Index</b>	The index of the SIP trunk.
<b>Description</b>	More information about each SIP trunk group.
<b>SIP Trunk Address</b>	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.
<b>Current</b>	The number of the current incoming/outgoing SIP calls.
<b>Sum</b>	The total number of the incoming/outgoing SIP calls.
<b>Connection Rate</b>	The percentage of successful calls to total calls by all method. The call methods include incoming/outgoing SIP calls.
<b>Answering Rate</b>	The percentage of answered calls to total calls by all methods. The call methods include incoming/outgoing SIP calls.
<b>Average Call Length</b>	The average call length for all connected calls.
<b>INVITE</b>	The number of the invite messages received per second.
<b>Release Cause</b>	Reason to release the call.
<b>Normal Disconnection</b>	Total number of the calls which are normally cleared. The corresponding SIP status code is 200.
<b>Cancelled</b>	Total number of the calls which are cancelled by the calling party. The corresponding SIP status code is 487.



<b>Busy</b>	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.
<b>No Answer</b>	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.
<b>Routing Failed</b>	Total number of the calls which fail because no routing rules are matched. The corresponding SIP status code is 488.
<b>No Idle Resource</b>	Total number of the calls which fail because no voice channel is available. The corresponding SIP status code is 486.
<b>Failed</b>	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 4xx, 5xx or 6xx.
<b>Others</b>	Total number of the calls which fail due to other unknown reasons. The corresponding SIP status code is 493.
<b>Percentage</b>	The percentage of the calls with a release cause to total calls.
<b>Current Number of SIP Call in/out</b>	The number of calls currently coming in to/out from the SIP.
<b>Connected Number of SIP Call in/out</b>	The number of successfully connected calls coming in to/going out from the SIP.
<b>Total Number of SIP Call in/out</b>	The sum of all calls coming in to/going out from the SIP.
<b>Connection Rate of SIP Call in/out</b>	The percentage of the number of successful SIP incoming/outgoing calls to the total number of incoming/outgoing calls.
<b>CPS</b>	The number of new calls per second.

### 3.2.7 SIP Account Call Count

SIP Call Count supports the statistics on the total number of calls, the connection rate and the response rate for each SIP account (only in the sbo-> ims direction), as well as the sort in sequence and reset. It synchronizes the SIP accounts that are added, deleted, or changed.

### 3.2.8 Warning Info

The Warning Information interface displays all the warning information on the gateway.

## 3.3 SIP Settings

SIP Settings includes six parts: **SIP**, **SIP Trunk**, **SIP Register**, **SIP Account**, **SIP Trunk Group** and **Media**. **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.

### 3.3.1 SIP

On the SIP Settings interface, 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 [Restart](#) for detailed instructions. The table below explains the items on this interface.

Item	Description
<b>SIP Address of WAN</b>	IP address of WAN for SIP signaling, using LAN 1 by default.
<b>SIP Working Mode</b>	Set the working mode of SIP, including <i>Back-to-back User Agent</i> and <i>Call Status Agent</i> .
<b>RTP Transcoding</b>	When this feature is enabled, RTP will be transcoded by OCT after negotiation. This feature is disabled by default.
<b>SIP Signaling Port</b>	The port monitored by SIP UDP/TCP. The value range is 2000-65535 and the default value is 5060. <b>Note:</b> It cannot overlap with the RTP port range in the media settings.
<b>SIP TLS Signaling Port</b>	The port monitored by SIP TLS. The value range is 2000-65535 and the default value is 5061. <b>Note:</b> It cannot overlap with the RTP port range in the media settings.
<b>Obtain CallerID from</b>	There are four optional ways to obtain the calling party number: Username of "From" Field, Displayname of "From" Field, <i>P-Preferred-Identity Field</i> , <i>P-Asserted-Identity Field</i> . The default value is <i>Username of "From" Field</i> .
<b>Obtain/Send CalleelD from</b>	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 <i>"Request" Field</i> .
<b>Prack Send Mode</b>	Sets whether to return the pack message while receiving the 180/183 message which carries the 100rel field. Three options are available: Disable, Supported and Require, and the default setting is Disable.
<b>DisplayName</b>	Sets whether to carry the actual calling number in the DisplayName field of the SIP message sent by the gateway.
<b>UserName</b>	Sets whether to carry the gateway registered number in the UserName field of the SIP message.
<b>NAT Traversal, Traversal Type</b>	Sets whether to enable the feature of NAT Traversal. By default, the feature is disabled. There is only one optional traversal type: <i>Port Mapping</i> .
<b>LAN1 Mapping Address, LAN2 Mapping Address</b>	The mapping address of the 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.
<b>Always Use Mapping Address</b>	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 <i>disabled</i> .
<b>RTP Self-adaption</b>	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 <i>disabled</i> .
<b>UDP Header Checksum</b>	When this feature is enabled, the gateway will automatically calculate the check sum of the UDP header during RTP transmission.

<b>Rport</b>	When this feature is enabled, a corresponding Rport field will be added to the Via message of SIP. By default, it is <i>disabled</i> .
<b>Auto Reply of Source Address</b>	Once this feature is enabled, the gateway will reply the source address in the invite message. The default value is <i>disabled</i> .
<b>Multiple Audio Selection</b>	Since the SDP message carries multiple audio types, you can choose RTP or SRTP as the voice port.
<b>Send Response by Former Via</b>	Enabling this feature means to close the automatic modification on the Via header of the response message. By default it is disabled.
<b>Registration Related Settings</b>	When this feature is enabled, the available call time for each SIP registered account as well as the SIP Registered Number Polling feature can be set. By default it is disabled.
<b>Time (min/month)</b>	Specifies the call time for a SIP registered account.
<b>SIP Registered Number Polling</b>	When this feature is enabled, the call is polled among SIP registered accounts. By default it is disabled.
<b>Failed Count</b>	It is valid only when the feature <i>SIP Registered Number Polling</i> is enabled. After a number is called out and fails for set times, it will be kicked out of the cycle and then allowed to re-join after <i>Recover Time of Disable Account</i> .
<b>Recover Time of Disable Account (m)</b>	See the description of <i>Failed Count</i> .
<b>Caller Prefix Grouping</b>	When this feature is enabled, only if the calling number of the call matches the caller prefix on the page of the SIP registered account will the rated time be used.
<b>Caller over Clocking (IP OUT)</b>	Limit on the number of calls in a cycle for the calling number. By default this feature is disabled.
<b>Cycle (min)</b>	The time of a cycle. It is only valid when the feature <i>Caller over Clocking</i> is enabled.
<b>Count Values</b>	The allowed incoming calls within the set time of a cycle. It is only valid when the feature <i>Caller over Clocking</i> is enabled.
<b>Interval (ms)</b>	The interval time for calls from a same calling number. After hangup, the gateway needs to wait for some time before using this account. It is only valid when the feature <i>Caller over Clocking</i> is enabled.
<b>SIP Value of Reply</b>	The abnormal SIP message returned by the gateway. The default value is 503.
<b>Deny SIP Calls when Registration Fails</b>	Unregistered and registration failed SIP accounts as well as the invite message over IP reply 503 for rejection, It is disabled by default.
<b>Eth Resource</b>	The limit on the RTP resources occupied simultaneously by a single network port. It can be configured in the SIP settings. By default it is disabled.
<b>Eth Resource Num</b>	The number of network port resources is an integer greater than 0. The default value is 2.
<b>SIP Account Numbers</b>	The maximum number of SIP accounts, must be set greater than the number of existing SIP accounts. The default value is 2000.
<b>SIP Account Registration Interval</b>	The interval between registrations of multiple SIP accounts. Range of value: 0~10000, with the default value of 0.

<b>DSCP</b>	Sets whether to enable the DSCP differentiated services code point. By default, it is <i>disabled</i> .
<b>Voice Media</b>	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.
<b>Signal Control</b>	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.
<b>Calls from SIP Trunk Address only</b>	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 <i>disabled</i> . And it is only valid when the Firewall feature is not enabled.
<b>Match Call Count to SIP Trunk based on Source Address of INVITE</b>	Performs call count by matching the source address of the INVITE message. By default it is disabled.
<b>Switch Signal Port if SIP Registration Failed</b>	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. By default, it is <i>disabled</i> .
<b>Hang up upon Call Time-out</b>	Sets whether to enable the feature to hang up the call once it is time-out, with the default value of <i>No</i> .
<b>Maximum Call Overtime</b>	Sets the maximum overtime for a call. Calculated by minute.
<b>Working Period, Period</b>	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).
<b>Sip Trunk Heart</b>	Sets whether to send the option message to the SIP trunk. The calls routed to this trunk will be rejected directly if the times of no answer from the MGCF trunk exceed the set value.
<b>Trunk Heartbeat Cycle</b>	The cycle to send the option message to the SIP trunk.
<b>Allowed Times of NoResponse</b>	The allowed times of SIP's no answer to the option message.
<b>Return Value from SIP upon No Response</b>	The SIP trunk did not reply with the SIP value returned by the option message. The default value is 502.
<b>Support 100rel</b>	Sets whether to carry 100rel in the Supported field of the request message for IP calls out. By default it is disabled.
<b>Not Wait ACK after Sending 200 OK</b>	Once this feature is enabled, the gateway does not need to wait the ACK message after sending the 200OK message. The default value is <i>disabled</i> .
<b>Minimum Registration Interval</b>	Used to set the minimum period for registering messages when <i>SIP Working Mode</i> is set to <i>Back-to-back User Agent</i> . The default value is 60.
<b>The Percentage of Registration Message Sending Cycle to Period of Validity</b>	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.

<b>Maximum Wait Answer Time</b>	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.
<b>Maximum Wait RTP Time</b>	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.
<b>Switch Network Port by Packet Loss Rate</b>	Once this feature is enabled, the gateway will switch to other available network port once the RTP packet loss rate gets larger than the set value. The default value is <i>disabled</i> .
<b>RTP Packet Loss Rate</b>	Sets the RTP packet loss rate which is used as the judgment condition to switch the network port, with the default value of 5.
<b>UserAgent Field</b>	Sets the content of the UserAgent field. Currently, it only supports the English uppercase and lowercase letters.

### 3.3.2 Hot Backup (HA)

As to the hot backup feature, the primary SBC is used for all the work and the backup SBC is mainly for synchronizing data with the primary SBC. When the primary SBC fails, the backup SBC can quickly take over all the work of the faulty machine, enabling the SBC to continuously provide VOIP call services. This feature is valid only in the Call Status Agent mode. See below for the configuration items on the interface.

Item	Description
<b>HA</b>	Set whether to enable the hot backup feature.
<b>Remote Address</b>	The IP address of the primary or backup SBC.
<b>Primary/Backup</b>	Set the local PC as the primary or backup SBC.
<b>Heart Beat Lan</b>	Set the network port used for sending and receiving heartbeat packets as well as call data with the remote SBC.

### 3.3.3 SIP Trunk

On the SIP trunk settings interface, there is no SIP trunk information by default. A new SIP trunk can be added by the **Add New** button on the bottom right corner of the list

The table below explains the items shown on the interface.

Item	Description
<b>Index</b>	The unique index of each SIP trunk.
<b>Description</b>	More information about each SIP trunk group.
<b>SIP Agent</b>	After this feature is enabled, the SIP terminal can register to the gateway and become the SIP agent of the gateway. By default it is disabled.
<b>Bulk Adding</b>	After the <b>SIP Agent</b> feature is enabled on the SIP trunk, you can choose to add some in batches. It is disabled by default.
<b>Addition Number</b>	The number of SIP agents added in batches. The SBC supports a maximum of 1024.

<b>UserName Step Size</b>	The interval between adjacent user names, for example, the step size is 1 and the user names are 9000, 9001 ...
<b>Password Step Size</b>	The interval between adjacent passwords, similar to the username step size.
<b>UserName</b>	The username for the SIP terminal to register with the gateway.
<b>Password</b>	The password for the SIP terminal to register with the gateway.
<b>Remote Address</b>	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.
<b>Remote Port</b>	Port of the SIP trunk.
<b>Local Network Port</b>	The network port where the SIP trunk locates.
<b>Local SIP Port</b>	The local signaling port where the SIP trunk locates.
<b>Display CODEC</b>	Used to show/hide the voice codec and the corresponding packing time.
<b>CODEC</b>	Supported CODECs: G711A, G711U, G729, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K).
<b>Packing Time</b>	Time interval for packing an RTP packet, calculated by ms.
<b>Transport Protocol</b>	SIP transport protocol, providing three modes <i>UDP</i> , <i>TCP</i> and <i>TLS</i> . The default value is <i>UDP</i> .
<b>SRTP Mode</b>	Set the SRTP encryption mode, including <i>RTP Prior</i> and <i>SRTP Prior</i> . The default is <i>RTP Prior</i> .
<b>Outgoing Voice Resource</b>	Maximum number of voice channels for the outgoing calls allocated by the SIP trunk to the gateway.
<b>Incoming Voice Resource</b>	Maximum number of voice channels for the incoming calls allocated by the SIP trunk to the gateway.
<b>Send 180 and 183</b>	After receiving the 183 message from the destination trunk, first reply 180 and then 183. <b>Note:</b> Valid only when the SIP working mode is set to Back-to-back User Agent.
<b>DTMF Transmit Mode</b>	Sets the mode, RFC2833 or in-band, for the SIP trunk to send DTMF signals. If here is set Global, the DTMF transmit mode configured on the Media Settings interface will be used. <b>Note:</b> Valid only when the SIP working mode is set to Back-to-back User Agent.
<b>Fax Mode</b>	Sets the mode, T30 or T38, for the SIP trunk to fax. If here is set Global, the fax mode configured on the Fax Settings interface will be used. <b>Note:</b> Valid only when the SIP working mode is set to Back-to-back User Agent.
<b>Working Period, Period</b>	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).
<b>VOS1.1 SIP Encryption</b>	Sets whether to perform VOS1.1 encryption for SIP signaling, including three modes: <b>No Encryption</b> , <b>Gateway Encryption</b> , and <b>Client Encryption</b> . The default setting is <i>No Encryption</i> . <b>Note:</b> Valid only when the SIP working mode is set to Call Status Agent.
<b>Encrypt Key</b>	A key that encrypts SIP signaling.
<b>VOS1.1 RTP Encryption</b>	Sets whether to perform VOS1.1 encryption for RTP. By default it is disabled. <b>Note:</b> Valid only when the SIP working mode is set to Call Status Agent.

<b>Externally Bound Enable</b>	Sets whether to enable the Proxy feature. Once it is enabled, SIP messages will be sent to the proxy address.
<b>Externally Bound Address</b>	The proxy address.
<b>Externally Bound Port</b>	The proxy port.
<b>Asserted Identity Mode</b>	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 <i>disabled</i> .
<b>Number in From Field not Manipulated</b>	Once this feature is enabled, the callerID in the From field will not be manipulated, with the default value of <i>disabled</i> . <b>Note:</b> It is valid only when the configuration item Asserted Identity Mode is enabled.
<b>Add Content to To Field in INVITE Message</b>	Once this feature is enabled, you need to set the TO field in "Add Content". By default it is disabled.
<b>Add Content</b>	Customizes the content added to the TO field, such as user=phone.
<b>Send 100rel</b>	Sets whether to send the 100rel field with the 180/183 message. The default setting is disabled.
<b>Hide CallerID</b>	Sets whether to hide the CallerID. It is disabled by default.
<b>Session Timer</b>	Sets whether to enable the session refresh feature, with the default value of <i>disabled</i> . Once this feature is enabled, you are required to enter the minimum time and the timeout value.
<b>Minimum Time</b>	Sets the minimum time for refreshing the session. Value of range: 90~65535, with the default value of 150.
<b>Timeout</b>	Sets the timeout value for refreshing the session. The value cannot be less than that of Minimum Time, with the default value of 600.
<b>Early Media</b>	Once this feature is enabled, the P-Early-Media field will be included in the Invite message. The default value is <i>disabled</i> .
<b>Early Session</b>	Once this feature is enabled, the early-session field will be included in the Invite message. The default value is <i>disabled</i> .

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

Click **Modify** to modify a SIP account. The configuration items on the SIP account modification are the same as those on the **Add New SIP Account** interface.

To delete a SIP account, check the checkbox before the corresponding index 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.

**Note:** If no SIP trunk is configured, the configuration items such as SIP Register and SIP Trunk Group will not be available.



### 3.3.4 SIP Register

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

The table below explains the items shown on the interface.

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

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

Click **Modify** 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.

To delete a SIP register, check the checkbox before the corresponding index 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.

**Note:** If the SIP register is unconfigured, the configuration item SIP Account will not be available.

### 3.3.5 SIP Account

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

The table below explains the items shown on the interface.

Item	Description
<b>Index</b>	The unique index of each SIP account.
<b>SIP Trunk No.</b>	The number of the SIP trunk to which the SIP account is registered.
<b>Username</b>	The registration username of the SIP account. Once the SIP account is successfully registered, the SIP server can initiate calls to the gateway via <b>Username</b> .
<b>Password</b>	The registration password of the SIP account. To register the SIP account to the SIP trunk, both configuration items <b>Username</b> and <b>Password</b> should be filled in.



<b>Register Expires</b>	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.
<b>Register Status</b>	The registration status of the SIP account. It is either <i>Registered</i> or <i>Failed</i> .
<b>Authentication Username</b>	Authentication username of a port, used to register the port to the SIP server.
<b>Description</b>	More information about each SIP account.

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

Click **Modify** on the interface to modify a SIP account. The configuration items on the SIP account modification are the same as those on the **Add New SIP Account** interface.

To delete a SIP account, check the checkbox before the corresponding index 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.

### 3.3.6 SIP Trunk Group

On the SIP Trunk Group Settings interface, a new SIP trunk group can be added by the **Add New** button on the bottom right corner.

The table below explains the items shown on the interface.

Item	Description										
<b>Index</b>	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.										
<b>Description</b>	More information about each SIP trunk group.										
<b>SIP Trunk Select Mode</b>	<p>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.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><i>Increase</i></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><i>Decrease</i></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><i>Cyclic Increase</i></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><i>Cyclic Decrease</i></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>	Option	Description	<i>Increase</i>	Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.	<i>Decrease</i>	Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.	<i>Cyclic Increase</i>	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.	<i>Cyclic Decrease</i>	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.
Option	Description										
<i>Increase</i>	Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.										
<i>Decrease</i>	Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.										
<i>Cyclic Increase</i>	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.										
<i>Cyclic Decrease</i>	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.										
<b>IP→IP Outgoing Call Forbidden</b>	Sets whether to restrict the calls from IP to IP, with the default value of <i>No</i> . If you select 'Yes', you are required to fill in <i>Called Party Forbidden Rule</i> and <i>Calling Party Forbidden Rule</i> . See the note below for details.										

<b>SIP Trunks</b>	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'.
-------------------	--

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

Click **Modify** to modify a SIP trunk group. The configuration items on the SIP trunk group modification interface are the same as those on the **Add New SIP Trunk Group** interface.

To delete a SIP trunk group, check the checkbox before the corresponding index 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.

### 3.3.7 Media Settings

On the media settings interface, 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 [Restart](#) for detailed instructions. The table below explains the items shown on the interface.

Item	Description
<b>DTMF Transmit Mode</b>	Sets the mode for the IP channel to send DTMF signals. The optional values are <i>RFC2833</i> , <i>In-band</i> , <i>Signaling</i> , <i>RFC2833+Signaling</i> and <i>In-band+Signaling</i> , with the default value of <i>RFC2833</i> .
<b>RFC2833 Payload</b>	Payload of the RFC2833 formatted DTMF signals on the IP channel. Range of value: 90~127, with the default value of 101.
<b>RTP Port Range</b>	Supported RTP port range for the IP end to establish a call conversation. Range of value: 5000~60000, with the lower limit of 6000 and the upper limit of 20000. The difference between is not less than 8192. Note: There is no overlap with the SIP signaling port.
<b>Silence Suppression</b>	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 <i>Enable</i> and <i>Disable</i> , with the default value of <i>Disable</i> . <b>Note:</b> When G723 is selected as CODEC, this configuration setting will turn to <i>Enable</i> automatically.
<b>Noise Reduction</b>	Once this feature is enabled, the volume of the noise accompanied with the line will be reduced automatically. The default setting is <i>Enable</i> .
<b>JitterMode</b>	Sets the working mode of JitterBuffer. The optional values are <i>Static Mode</i> and <i>Adaptive Mode</i> , with the default value of <i>Static Mode</i> .
<b>JitterBuffer(ms)</b>	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.

<b>JitterUnderrunLead(ms)</b>	<p>Sets the initial delay applied to receive 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,</p> <p><b>Note:</b> Only when JitterMode is set to <i>Static Mode</i> will this item be shown.</p>
<b>JitterOverrunLead(ms)</b>	<p>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). Range of value: 0~280, calculated by ms, with the default value of 50,</p> <p><b>Note:</b> Only when JitterMode is set to <i>Static Mode</i> will this item be shown.</p>
<b>JitterMin</b>	<p>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.</p> <p><b>Note:</b> Only when JitterMode is set to <i>Adaptive Mode</i> will this item be shown.</p>
<b>JitterDecreaseRatio</b>	<p>Sets the rate of the delay that can be reduced under the adaptive mode. It defines the maximum percentage of silence that can be removed if reducing the delay. Range of value: 0~100, with the default value of 50,</p> <p><b>Note:</b> Only when JitterMode is set to <i>Adaptive Mode</i> will this item be shown.</p>
<b>JitterIncreaseMax</b>	<p>Sets the maximum delay that can be increased during one silence period. Range of value: 0~280, calculated by ms, with the default value of 30,</p> <p><b>Note:</b> Only when JitterMode is set to <i>Adaptive Mode</i> will this item be shown.</p>
<b>Voice Gain Output from IP</b>	<p>Adjusts the voice gain of call from IP to the remote end. The value must be a multiple of 3. Range of value: -24~24, calculated by dB, with the default value of 0.</p>
<b>Use Default Value if Packtime Negotiation fails</b>	<p>The default setting is Yes. The default value will be used if the RTP packing time negotiation fails. Please refer to the packing time set for the codec in the SIP trunk.</p>

<b>CODEC Setting</b>	Sets CODECs for the IP end to establish a call conversation. The table below explains the sub-items:	
	<b>Sub-item</b>	<b>Description</b>
	<i>Gateway Negotiation Coding Sequence</i>	Sets the coding sequence, including two options: <i>Default Priority</i> and <i>User-defined Priority</i> , with the default value of <i>Default Priority</i> .
	<i>Priority</i>	Priority for choosing the CODEC in an SIP conversation. The smaller the value is, the higher the priority will be.
	<i>CODEC</i>	Seven optional CODECs are supported: <i>G711A</i> , <i>G711U</i> , <i>G729AB</i> , <i>G722</i> , <i>G723</i> , <i>iLBC</i> , <i>AMR-NB</i> , <i>SILK(16K)</i> , <i>OPUS(16K)</i> , <i>SILK(8K)</i> , <i>OPUS(8K)</i> .
	<i>Packing Time</i>	Time interval for packing an RTP packet, calculated by ms.
	<i>Bit Rate</i>	The number of thousand bits (excluding the packet header) that are conveyed per second.
	By default, all of the eleven CODECs are supported and ordered <i>G711A</i> , <i>G711U</i> , <i>G729AB</i> , <i>G722</i> , <i>G723</i> , <i>iLBC</i> , <i>AMR-NB</i> , <i>SILK(16K)</i> , <i>OPUS(16K)</i> , <i>SILK(8K)</i> , <i>OPUS(8K)</i> 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.	
	<b>CODEC</b>	<b>Packing Time (ms)</b>
	<i>G711A</i>	10 / <b>20</b> / 30 / 40 / 50 / 60
	<i>G711U</i>	10 / <b>20</b> / 30 / 40 / 50 / 60
	<i>G729</i>	10 / <b>20</b> / 30 / 40 / 50 / 60
	<i>G722</i>	10 / 20 / <b>30</b> / 40
	<i>G723</i>	<b>30</b> / 60
	<i>iLBC</i>	<b>20</b> / 40
		30
		60
	<i>AMR</i>	<b>20</b> / 40 / 60
	<i>SILK(16K)</i>	<b>20</b> / 40 / 60 / 80 / 100
	<i>OPUS(16K)</i>	10 / <b>20</b> / 40 / 60
	<i>SILK(8K)</i>	<b>20</b> / 40 / 60 / 80 / 100
	<i>OPUS(8K)</i>	10 / <b>20</b> / 40 / 60

## 3.4 Fax Settings

The Fax Settings interface is used to modify the special fax configurations.

### 3.4.1 Fax

On the fax configuration interface, users can configure the general fax parameters. The fax mode

of T.38 is used by default. 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 [Restart](#) for detailed instructions. The table below explains the configuration items on the interface.

Item	Description
<b>Fax Mode</b>	The real-time IP fax mode. The optional values are <i>T.38</i> , <i>Pass-through</i> and <i>Disable</i> , with the default value of <i>T.38</i> . Setting this item to <i>Disable</i> means to disable both T.38 and Pass-through.
<b>T38 Version</b>	Version of T.38 which is defined by ITU-T. Range of value: 0~3, with the default value of 0.
<b>T38 Negotiation</b>	Sets the Negotiation mode of T.38, including: <i>Unsupported</i> , <i>Initiate Negotiation as Fax Sender</i> and <i>Initiate Negotiation as Fax Receiver</i> .
<b>Maximum Fax Rate</b>	Sets the maximum faxing rate for both receiving and transmitting. Range of value: 14400, 9600 and 4800, calculated by bps, with the default value of 9600.
<b>Fax Train Mode</b>	Sets the train mode for T.38 fax. The optional values are <i>transferredTCF</i> and <i>localTCF</i> , with the default value of <i>transferredTCF</i> .
<b>Error Correction Mode</b>	Sets the error correction mode for T.38 fax. The optional values are <i>t38UDPRedundancy</i> (Redundancy Error Correction) and <i>t38UDPFEC</i> (Forward Error Correction), with the default value of <i>t38UDPRedundancy</i> .
<b>T.30 Ecm</b>	Sets whether to enable the T.30 error correction mode. By default this feature is enabled.
<b>Min Duration of CNG</b>	As stipulated in the standard FAX CNG, the minimum duration of CNG is 500ms $\pm$ 15%, calculated by ms, with the default value of 425. <b>Note: Usually there is no need to modify it; please contact our technicians if necessary.</b>
<b>Min Duration of CED</b>	As stipulated in the standard FAX CED, the minimum duration of CED is 2600~4000ms, calculated by ms, with the default value of 2600. <b>Note: Usually there is no need to modify it; please contact our technicians if necessary.</b>

If you set **Fax Mode** to *Pass-through*, you will see some different configuration items as shown below.

Item	Description
<b>Pass-through Payload</b>	RTP Payload under the pass-through fax mode. Range of value: 96~127, with the default value of 102.

## 3.5 Route Settings

Route Settings is used to specify the routing rules for IP→IP calls.

### 3.5.1 Routing Parameters

On the routing parameters configuration interface, you can choose to route calls 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.

### 3.5.2 IP to IP

There is no IP→IP routing rules by default. A new routing rule can be added by the **Add New** button on the bottom right corner of the IP→IP routing rule configuration interface.

The table below explains the items shown on the interface.

Item	Description										
<b>Index</b>	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.										
<b>Call Initiator</b>	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.										
<b>CallerID Prefix, CalleeID Prefix</b>	<p>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 <b>Call Initiator</b> can specify the calls which apply to a routing rule.</p> <p>Rule Explanation:</p> <table border="1"> <thead> <tr> <th>Character</th><th>Description</th></tr> </thead> <tbody> <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 indicate any number between these two numbers.</td></tr> <tr> <td>" , "</td><td>',' is used only in '[' to separate numbers or number ranges, representing alternatives.</td></tr> </tbody> </table> <p>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.</p> <p><b>Note:</b> Multiple rules are supported for CallerID/CalleeID prefix. They are separated by ":".</p>	Character	Description	"0"~"9"	Digits 0~9.	"["	'[' 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.	"_"	'_' is used only in '[' between two numbers to indicate any number between these two numbers.	" , "	',' is used only in '[' to separate numbers or number ranges, representing alternatives.
Character	Description										
"0"~"9"	Digits 0~9.										
"["	'[' 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.										
"_"	'_' is used only in '[' between two numbers to indicate any number between these two numbers.										
" , "	',' is used only in '[' to separate numbers or number ranges, representing alternatives.										
<b>Call Destination</b>	The destination SIP trunk group to which the call will be routed.										
<b>Number Filter</b>	Number filter rule which will be applicable to this route. It is set in <b>Number Filter</b> . See <a href="#">Filtering Rule</a> for details.										
<b>Description</b>	More information about each routing rule.										

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

Routing Rules								
Check	Index	Call Initiator	CallerID Prefix	CalleeID Prefix	Number Filter	Call Destination	Description	Modify
<input type="checkbox"/>	255	SIP Trunk Group [0]	*	*	none	SIP Trunk Group [1]	Default	
<input type="checkbox"/>	254	SIP Trunk Group [1]	*	*	none	SIP Trunk Group [0]	Default	

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

Figure 3-5 IP→IP Routing Rule Configuration Interface

Click **Modify** to modify a routing rule. The configuration items on the IP→IP routing rule

modification interface are the same as those on the **Add New Routing Rule (IP→IP)** interface. Note that the item **Index** cannot be modified.

To delete a routing rule, check the checkbox before the corresponding index 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.

## 3.6 Number Filter

Number Filter includes four parts: **Whitelist**, **Blacklist**, **Number Pool** and **Filtering Rule**.

### 3.6.1 Whitelist

Figure 3-6 Whitelist Setting Interface

The Whitelist Setting Interface includes two parts: **CallerID Whitelist** and **CalleeID Whitelist**. A new CallerID/CalleeID whitelist can be added by the **Add New** button.

The table below explains the items shown on the interface.

Item	Description														
<b>Group</b>	The corresponding Group ID for CallerIDs/CalleeIDs in the whitelist. The value range is 0~7.														
<b>No. in Group</b>	The corresponding No. for different CallerIDs/CalleeIDs in a same group.														
<b>CallerID</b>	<p>CallerID in the whitelist, which can not be left empty. Rule explanation:</p> <table border="1"> <thead> <tr> <th>Character</th><th>Description</th></tr> </thead> <tbody> <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 only in '[ ]' to separate numbers or number ranges, representing alternatives.</td></tr> </tbody> </table>	Character	Description	"*"	indicating any string	"0"~"9"	Digits 0~9.	"x"	A random number. A string of 'x's represents several random numbers. For example, 'xxx' denotes 3 random numbers.	"[ ]"	'[ ]' 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.	"-"	'-' is used only in '[ ]' between two numbers to indicates any number between these two numbers.	","	',' is used only in '[ ]' to separate numbers or number ranges, representing alternatives.
Character	Description														
"*"	indicating any string														
"0"~"9"	Digits 0~9.														
"x"	A random number. A string of 'x's represents several random numbers. For example, 'xxx' denotes 3 random numbers.														
"[ ]"	'[ ]' 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.														
"-"	'-' is used only in '[ ]' between two numbers to indicates any number between these two numbers.														
","	',' is used only in '[ ]' to separate numbers or number ranges, representing alternatives.														
<b>CalleeID</b>	CalleeID in the whitelist, which can not be left empty. The rules are the same as that of CallerID.														



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

Click **Modify** to modify the CallerID or CalleeID whitelist. The configuration items on the CallerIDs/CalleeIDs on the Whitelist Modification interface are the same as those on the **Add New CallerIDs/CalleeIDs in Whitelist** interface. The item *Group No.* cannot be modified.

The search query box on the top of the Whitelist Setting interface can be used to search the CallerID or CalleeID you want.

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

**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 200000.

### 3.6.2 Blacklist

The Blacklist Setting interface is almost the same as the Whitelist Setting interface; only the whitelist changes to the blacklist. The configuration items on this interface are the same as those on the Whitelist Setting interface.

**Note:** The blacklist has a higher priority than the whitelist. If a CallerID or CalleeID set in the whitelist is the same as one in the blacklist, it will be regarded as valid in the blacklist.

### 3.6.3 Number Pool

On 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. The table below explains the items shown on the interface.

Item	Description
<b>Group</b>	The corresponding Group ID for numbers in the number pool. The value range is 0~15.
<b>No. in Group</b>	The corresponding No. for different numbers in a same group. It supports up to 100 numbers in one group.
<b>Number Range</b>	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** to modify the number pool. The configuration items on the number pool modification interface are the same as those on the **Add New Number Pool** interface. The item *Group No.* cannot be modified.

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

### 3.6.4 Filtering Rule

On 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.

The table below explains the items shown on the interface.

Item	Description
<b>No.</b>	The corresponding number for a filtering rule. The value range is 0~99.



<b>CallerID Whitelist</b>	The Group No. of CallerIDs saved on the whitelist setting interface.
<b>CalleeID Whitelist</b>	The Group No. of CalleeIDs saved on the whitelist setting interface.
<b>CallerID Blacklist</b>	The Group No. of CallerIDs saved on the blacklist setting interface.
<b>CalleeID Blacklist</b>	The Group No. of CalleeIDs saved on the blacklist setting interface.
<b>CallerID Pool in Whitelist</b>	Select a Group No. which is set in the whitelist from the number pool as the CallerID pool in whitelist.
<b>CallerID Pool in Blacklist</b>	Select a Group No. which is set in the blacklist from the number pool as the CallerID pool in blacklist.
<b>CalleeID Pool in Whitelist</b>	Select a Group No. which is set in the whitelist from the number pool as the CalleeID pool in whitelist.
<b>CalleeID Pool in Blacklist</b>	Select a Group No. which is set in the blacklist from the number pool as the CalleeID pool in blacklist.
<b>Original CalleeID Pool in Whitelist</b>	Select a Group No. which is set in the whitelist from the number pool as the original CalleeID pool in whitelist.
<b>Original CalleeID Pool in Blacklist</b>	Select a Group No. which is set in the blacklist from the number pool as the original CalleeID pool in blacklist.
<b>Description</b>	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** to modify the filtering rule. The configuration items on the filtering rule modification interface are the same as those on the **Add New Filtering Rule** interface. The item *No.* cannot be modified.

To delete a filtering rule, check the checkbox before the corresponding index and click the '**Delete**' button. To clear all filtering rules at a time, click the **Clear All** button.

## 3.7 Number Manipulation

Number Manipulation includes three parts: **IP→IP CallerID**, **IP→IP CalleeID** and **CallerIP Pool**. This interface is unavailable when the SIP working mode is set to *Call Status Agent*.

### 3.7.1 IP to IP CallerID

By default there is no available number manipulation rule. A new rule can be added by the **Add New** button on the interface. The table below explains the items shown on the interface.

Item	Description
<b>Index</b>	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.
<b>Call Initiator</b>	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.

<b>CallerID Prefix, CalleeID Prefix</b>	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 <b>Call Initiator</b> and <b>With Original CalleeID</b> can specify the calls which apply to a number manipulation rule. <b>Note:</b> Multiple CallerID/CalleeID prefixes can be added simultaneously. They are separated by ".".
<b>With Original CalleeID</b>	If this item is set to <b>Yes</b> , it indicates that the number manipulation rule is only applicable to the calls with original CalleeID/redirecting number. The default value is <b>No</b> .
<b>Stripped Digits from Left</b>	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.
<b>Stripped Digits from Right</b>	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.
<b>Reserved Digits from Right</b>	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.
<b>Prefix to Add</b>	Designated information to be added to the left end of the current number.
<b>Suffix to Add</b>	Designated information to be added to the right end of the current number.
<b>Description</b>	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.

Click **Modify** to modify a number manipulation rule. The configuration items on the IP→IP CallerID manipulation rule modification interface are the same as those on the **Add IP→IP CallerID Manipulation Rule** interface. Note that the item **Index** cannot be modified.

To delete a number manipulation rule, check the checkbox before the corresponding index 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.

### 3.7.2 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. The configuration items on this interface are the same as those on **IP→IP CallerID Manipulation Interface**.

### 3.7.3 CallerIP Pool

SIP Trunk Group : Source SIP Trunk Group SETTING

IP->IP CallerID Manipulated Pool

Check	No.	CallNumber Range	SIP trunk group index	Callout Resource	Modify

Delete Clear All Add New

Note:(1)There are no more than 1000 items for every sip trunk group of the calling number!  
 Note:(2)If you modify the Callerid Pool while calling,the resource would reload.You'd better do not modify this page when the callerid is busy!  
 Note:(3)If the 'SIPTrunkType' is 'SRCSipTrunkGroup',then the callerid pool would work by the source sip trunk group,otherwise the destination sip trunk group.

Figure 3-7 CallerIP Pool Interface

See Figure 3-7 for the CallerIP Pool interface. You can select the source direction of the SIP trunk group. Click **Add New** in the lower right corner of the interface to add a calling number with its callout resource, as shown in the figure below.

CallerNum

No. :

Source SIP trunk group : all ▼

CallerNum :  --

Callout Resource :

save OFF

Figure 3-8 CallerIP Adding Interface

The table below explains the items shown on the interface.

Item	Description
<b>No.</b>	The unique number of the CallerID in the pool, which denotes its priority. A CallerID with a smaller index value has a higher priority.
<b>Source SIP Trunk Group</b>	A specified SIP trunk group. Only calls in this SIP trunk group can be performed with callerIP manipulation.

<b>CallerNum</b>	Sets the range of the CallerIP for the call.
<b>Callout Resource</b>	Set the maximum number of outgoing calls from a same callerIP at a time.

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

Click **Modify** in Figure 3-7 to modify the CallerIP information. The configuration items on the CallerIP modification interface are the same as those on the **CallerIP Adding** interface. The item **No.** cannot be modified.

To delete a CallerIP in the pool, check the checkbox before the corresponding index in Figure 3-7 and click the '**Delete**' button. To clear all CallerIPs in the pool at a time, click the **Clear All** button in Figure 3-7.

## 3.8 VPN

The VPN settings include two parts: *VPN Server Settings* and *VPN Account*.

### 3.8.1 VPN Server Settings

VPN is a remote access technology that enables remote access by encrypting packets and converting the destination address of packets. That is, in brief, set up a private network by using the public network. The SBC gateway has a VPN server to help the client of the outer net access the enterprise's inner devices.

See below for the configuration items on the VPN Server Settings interface.

Item	Description
<b>VPN Server</b>	Set whether to enable the VPN server.
<b>VPN Type</b>	The protocol type of VPN. Currently, only PPTP is supported.
<b>Identify Verification Protocol</b>	Set the protocol for VPN authentication, including MS-CHAPv2+MPPE, MS-CHAPv2 and MS-CHAP.
<b>Client Range</b>	Set the IP range of clients that can be accessed remotely.
<b>Preferred WINS Address/ Spare WINS Address</b>	Set the preferred/spare WINS address.

After configuration, click **Save** to save the settings into the gateway or click **Reset** to restore the configurations.

### 3.8.2 VPN Account

By default, there is no VPN account available on the gateway, click **Add New** to add them manually. See below for the configuration items on the interface.

Item	Description
<b>Index</b>	The unique index of each VPN account.
<b>Username</b>	The username for the client to connect with the VPN server.
<b>Password</b>	The password to connect VPN.

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

Click **Modify** to modify a VPN account. The configuration items on the modification interface are the same as those on the **Add VPN Account** interface.

To delete a VPN account, check the checkbox before the corresponding index 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 accounts at a time, click the **Clear All** button.

## 3.9 DHCP

DHCP is mainly used for centralized management and allocation of IP addresses, enabling the hosts in the network environment to dynamically obtain such information as IP addresses, Gateway addresses, and DNS server addresses, and improving the usage rate of those addresses. The SBC gateway provides an interface for DHCP setting.

See below for the configuration items on the DHCP Server Settings interface.

Item	Description
<b>DHCP Server</b>	Set whether to enable the DHCP server feature.
<b>IP Range</b>	Set the range of IP addresses that the DHCP server can assign.
<b>Subnet Mask</b>	Set the subnet mask required to enable the DHCP server.
<b>Default Gateway</b>	Set the default gateway required to enable the DHCP server.
<b>DNS Server</b>	Set the DNS server required to enable the DHCP server.

After configuration, click **Save** to save the settings into the gateway or click **Reset** to restore the configurations.

## 3.10 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.

### 3.10.1 Network

The network settings interface is used to configure parameters about network. A gateway has two LANs, each of which can be configured with independent IP address, subnet mask and default gateway. It supports the DNS server. The VLAN feature is supported by LAN2 and if enabled will extend LAN2 to three VLAN ports. 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 between LAN1 and LAN2. By default, this feature is *disabled*. The IPV4 network type can be selected as static or PPPoE. However in PPPoE mode, the Bond feature is invalid.

**Note:** 1. The two configuration items IP Address and Default Gateway cannot be the same for LAN1 and LAN2.

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 abnormality in network interface.

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.

### 3.10.2 Authorization

On the Authorization Management interface, you can import a trial or formal authorization just by uploading the authorization file which is provided by Synway and cannot be modified. SBC500 supports up to 512 channels of authorization.

### 3.10.3 Management

The table below explains the items shown on the Management Parameters Setting interface.

Item	Description
<b>WEB Port</b>	The port which is used to access the gateway via WEB. The default value is 80.
<b>Access Setting</b>	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 the IPs within it to access the gateway freely. Also you can set an IP blacklist to forbid all the IPs within it to access the gateway.
<b>Time to Log Out</b>	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.
<b>SSH</b>	Sets whether to enable the gateway to be accessed via SSH, with the default value of <i>No</i> .
<b>SSH Port</b>	The port which is used to access the gateway via SSH.
<b>Remote Data Capture</b>	After this feature is enabled, you can obtain the gateway data via a remote capture tool. The default value is <i>No</i> .
<b>Capture RTP</b>	Sets whether to capture RTP. Once this feature is enabled, the RTP package will also be captured by the selected network.
<b>FTP</b>	Sets whether to enable the FTP server, with the default value of <i>Yes</i> .
<b>Enable Watchdog</b>	Sets whether to enable the watchdog feature, with the default value of <i>Yes</i> .
<b>SYSLOG</b>	Sets whether to enable SYSLOG. It is required to fill in <b>SYSLOG Server Address</b> and <b>SYSLOG Level</b> in case SYSLOG is enabled. By default, <b>SYSLOG</b> is disabled.
<b>Server Address</b>	Sets the SYSLOG server address for log reception.
<b>SYSLOG Level</b>	Sets the SYSLOG level. There are three options: <i>ERROR</i> , <i>WARNING</i> and <i>INFO</i> .
<b>Send CDR</b>	Sets whether to enable the feature of sending CDR. It is required to fill in <b>Server Address</b> and <b>Server Port</b> in case Send CDR is enabled. By default, <b>Send CDR</b> is disabled.
<b>Server Address</b>	The address of the server to receive CDR.
<b>Server Port</b>	The port of the server to receive CDR.
<b>Send Failed Call Record</b>	Once this feature is enabled, the gateway will send the CDR for both successful and unsuccessful calls; otherwise, it will only send the CDR data for successful calls.
<b>Add Hangup Side</b>	Add hangup information to CDR.
<b>Monitor Self-adaption</b>	Enable the NAT stun between the gateway and the monitor tool. By default, it is disabled.
<b>NTP</b>	Sets whether to enable the NTP time synchronization feature. It is required to fill in <b>NTP Server Address</b> , <b>Synchronizing Cycle</b> and <b>Time Zone</b> in case NTP is enabled. By default, <b>NTP</b> is disabled.
<b>NTP Server Address</b>	Sets the Server address for NTP time synchronization.
<b>Synchronizing Cycle</b>	Sets the cycle for NTP time synchronization.
<b>Daily Restart</b>	Sets whether to restart the gateway regularly every day at the preset <b>Restart Time</b> . By default, this feature is disabled.

<b>Restart Time</b>	Sets the time to restart the gateway regularly.
<b>System Time</b>	The system time. Check the checkbox before <b>Modify</b> and change the time in the edit box.
<b>Time Zone</b>	The time zone of the gateway.

### 3.10.4 IP Routing Table

IP Routing Table is used to set the route for the gateway to send the IP packet to the destination network segment. By default, there is no routing table available on the gateway, click **Add New** to add them manually.

The table below explains the items shown on the interface.

Item	Description
<b>No.</b>	The number of the routing in routing table.
<b>Destination</b>	The network segment where the IP packet can reach.
<b>Subnet Mask</b>	The subnet mask of the destination network segment.
<b>Network Port</b>	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.

Click **Modify** to modify a routing. The configuration items on the routing table modification interface are the same as those on the **Add Routing Table** interface. Note that the item **No.** cannot be modified.

To delete a routing, check the checkbox before the corresponding index and click the **Delete** button. To clear all routing tables at a time, click the **Clear All** button.

### 3.10.5 Firewall

By default, there is no firewall information available on the gateway, click **Add New** to add it manually. See below for the configuration items on the interface.

Item	Description
<b>Index</b>	The unique index of a firewall rule, used to specify its priority. The smaller the value, the higher the priority.
<b>Source Address</b>	Set the IP address of the source network or an explicit host name.
<b>Source Port</b>	Set the source UDP/TCP port (remote host) of the packet sent to the gateway.
<b>Local Port</b>	Set the port of the local gateway.
<b>Protocol</b>	Protocol type, including eight options: Any, TCP, UDP, UDPLITE, ICMP, ESP, AH and SCTP.
<b>LAN</b>	Select the network port to which the firewall rule is applied.
<b>Network Speed Limit</b>	Set the expected rate of the network in packs. <b>Note:</b> The network packet exceeding the speed limit will be stored in the buffer until the buffer capacity is full, and the overspeed network packet will be discarded.
<b>Buffer Capacity</b>	Set the buffer capacity of the network rate. The default value is 0.
<b>Operate</b>	Set the execution results of firewall rules, including two options: <i>Permit</i> and <i>Prevent</i> .

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



Click **Modify** to modify a firewall rule. The configuration items on the modification interface are the same as those on the **Add Firewall Rule** interface.

To delete a firewall rule, check the checkbox before the corresponding index 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 rules at a time, click the **Clear All** button.

**Note:** 1. Only after selecting a firewall rule and clicking Apply, the firewall rule will take effect.  
2. An IP that is determined to be abnormal by DDOS or IDS, will be added to the temporary blacklist, even if the firewall is set to allow access.

### 3.10.6 IDS Settings

IDS is used to detect whether the incoming SIP message complies with the protocol specification. For a SIP message that does not conform to the specification, the gateway adds the source IP of the SIP message to the blacklist. See below for the configuration items on the interface.

Item	Description
<b>Type</b>	Sets the type for detecting whether the SIP message conforms to the specification or blacklist, including five conditions: <i>TLS Connection Failed</i> , <i>Malformed SIP Datagram</i> , <i>Registration Failed</i> , <i>Call Failed</i> and <i>SIP Exception Flow</i> .
<b>Warning Threshold</b>	After the number of detecting times of each type reaches the set value, the source IP address contained in the SIP message will be recorded into the IDS warning log.
<b>Blacklist Threshold</b>	After the number of detecting times of each type reaches the set value, the source IP address of the SIP message will be recorded into the blacklist.
<b>Blacklist Validity</b>	Set the effective time for the blacklist to work.

After configuration, click **Save** to save the settings into the gateway or click **Reset** to restore the configurations, and click **Download** to download the IDS log.

**Note:** After restarting the service, rebooting the system, upgrading the software or applying the firewall, the temporary blacklist will be cleared.

### 3.10.7 DDOS Settings

On the DDOS Settings interface, the user can set the defense feature of some ports against DDOS attacks. See below for the configuration items on the interface.

Item	Description
<b>WEB Port Attack Protection</b>	When this feature is enabled, the WEB port will have the ability to block DDOS attacks.
<b>WEB Limit</b>	When the same IP address accesses the SBC through WEB, it will be forbidden to log in after the times reaching the set restrictions (the number of access processes/5).
<b>FTP Port Attack Protection</b>	When this feature is enabled, the FTP port will have the ability to block DDOS attacks.
<b>FTP Limit</b>	When the same IP address accesses the SBC through FTP, it will be forbidden to log in after the times reaching the set restrictions (i.e. the number of access processes).



<b>SSH Port Attack Protection</b>	When this feature is enabled, the SSH port will have the ability to block DDOS attacks.
<b>SSH Limit</b>	When the same IP address accesses the SBC through SSH, it will be forbidden to log in after the times reaching the set restrictions (i.e. the number of access processes).
<b>TELNET Port Attack Protection</b>	When this feature is enabled, the TELNET port will have the ability to block DDOS attacks.
<b>TELNET Limit</b>	When the same IP address accesses the SBC through TELNET, it will be forbidden to log in after the times reaching the set restrictions (i.e. the number of access processes).
<b>Set Validity of Attacker IP Blacklist</b>	Determine whether to enable the attack blacklist effective time setting, including two options: <i>Forever</i> and <i>In the Set Time</i> .
<b>Time</b>	Set the effective time for the blacklist to work.

After configuration, click **Save** to save the settings into the gateway or click **Reset** to restore the configurations.

**Note:** After rebooting the system, upgrading the software or applying the firewall, the temporary blacklist will be cleared.

### 3.10.8 Certificate Management

Certification Management, i.e. Transport Layer Security (TLS) Management, is a security protocol that provides privacy and data integrity for network communications. It is used to protect the gateway's SIP signaling links, WEB interfaces and the Telnet server.

The table below explains the items shown on the Certificate Management interface.

Item	Description
<b>Country</b>	Fill in the country code, represented by 2 capital letters, for example, CN. For the codes for other countries, refer to ISO 3166-1 A2.
<b>Province</b>	Fill in the province, for example, Zhejiang.
<b>City</b>	Fill in the city, for example, Hangzhou.
<b>Company</b>	Fill in the company name.
<b>Department</b>	Fill in the department, for example, IT Dept.
<b>Host Name</b>	Fill in the IP address of SBC.
<b>Email</b>	Fill in the Email address.

After your configuration, click **Generate** to generate the TLS certificate, click **Reset** to restore the current settings, and click **Download** to download the certificate.

### 3.10.9 Centralized Manage

The Centralized Manage Setting interface is used to configure parameters about centralized management. The gateway can register to a centralized management platform and accept the management of the platform. The table below explains the items shown in this interface.

Item	Description
------	-------------

<b>Auto Change Default Gateway</b>	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.
<b>Management Platform</b>	Select a management platform for the gateway to register.
<b>Company Name</b>	The company name used to register the gateway to DCMS, only valid when DCMS is selected.
<b>Gateway Description</b>	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.
<b>Centralized Management Protocol</b>	Sets the centralized management protocol. It only supports SNMP currently.
<b>SNMP Version</b>	Sets the version of SNMP, three options available: V1, V2 and V3, with the default value of V2.
<b>SNMP Server Address</b>	IP address of SNMP.
<b>Monitoring Port</b>	Monitoring Port for SNMP on the gateway.
<b>Community String</b>	Community string used for information acquisition.
<b>Account</b>	The account of SNMP, only valid when the SNMP version is set to V3.
<b>Grade</b>	The grade of SNMP, three options available: Neither authenticated nor encrypted, Authenticated but not encrypted and Authenticated and encrypted, with the default value of <i>Neither authenticated nor encrypted</i> . It is only valid when the SNMP version is set to V3.
<b>Authentication Password</b>	The authentication password required to enter when the item Grade is set to Authenticated but not encrypted or Authenticated and encrypted.
<b>Encryption Password</b>	The encryption password required to enter when the item Grade is set to Authenticated and encrypted.
<b>Authorization Code</b>	The maximum length of the authorization code is 64 bits. There is no limitation on the input content. When connecting to the centralized management server for the first time, you can enter the connection by entering the correct authorization code. After the connection is successful, you can always connect even if you change to the wrong authorization code, but the centralized management feature with the wrong authorization code cannot be turned off.
<b>Working Status</b>	The status of the connection between the gateway and the centralized management server. It is only valid when DCMS is selected.

### 3.10.10 SIP Account Generator

On the SIP Account Generator interface, the gateway can 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 “,”.

### 3.10.11 Recording Manage

After your configuration on the Recording Management Settings interface, the gateway can connect to the designated recording server and forward RTP via a special network port to the recording server so as to realize the RTP data capture on the gateway. The table below explains the configuration items shown on the interface.

Item	Description
<b>Authentication Name</b>	The authentication name for the gateway to connect with the recording server.
<b>Password</b>	The password for the gateway to connect with the recording server.
<b>Recording Server IP</b>	The IP address of the recording server used to connect with the gateway.
<b>Occasion to Start Recording</b>	Sets the time to start recording, with two options available: Ringing and Talking.
<b>The Minimum Talking Time Saved</b>	The calls shorter than the set value will not be saved. The default value is 5 seconds.
<b>Network Port to Forward RTP</b>	The network port used for the gateway to forward RTP.

After configuration, click **Save** to save the above settings into the gateway or click **Reset** to restore the configurations.

### 3.10.12 Configuration File

Via the Configuration File interface, you can check and modify configuration files about the gateway, including SMGConfig.ini, ShConfig.ini and hosts. 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; and hosts is the system file relating a domain name and its corresponding IP address. 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.

### 3.10.13 Signaling Capture

On 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. At present SIP and SysLog are supported for you to choose. If Syslog is selected, you need enter the Syslog destination address to send Syslog to wherever required. Click **Stop** to stop data capture and download the captured packets.

Two-way Recording is used to set the channel group and the channel number for recording. Click **Start** to start recording the corresponding channel in the specified channel group (maximum consecutively recording time is 1 minute). Click **Stop** to stop recording and download the recorded data. Once the option Capture RTP is ticked, you are required to input the calling number of the RTP to be captured.

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.

### 3.10.14 Signaling Call Test

The Signaling Call Test interface mainly helps 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 on the interface.

Item	Description
<b>Test Type</b>	The type of the call test.
<b>SIP Trunk Group No.</b>	The SIP trunk group number you are required to select for call testing.
<b>CallerID</b>	The CallerID for the call test.
<b>CalleeID</b>	The CalleeID for the call test.
<b>DTMF</b>	You can use this item to send DTMFs after the establishment of call conversation on the channel for call test
<b>Add Invite Header, FieldName, Field Content</b>	You can use this item to add the invite header and its corresponding content
<b>Signaling Trace</b>	The information returned during the call test, helping you to learn the detailed information about the call test.

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

**Note:** The gateway cannot stop the call test unless the called party ends it.

### 3.10.15 Signaling Call Track

The Call Track Interface is mainly used to output and save call information, facilitating call trace and problem debugging. It provides three modes: Filter CallerID, Filter CalleeID and Filter None. 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.

### 3.10.16 Network Speed Tester

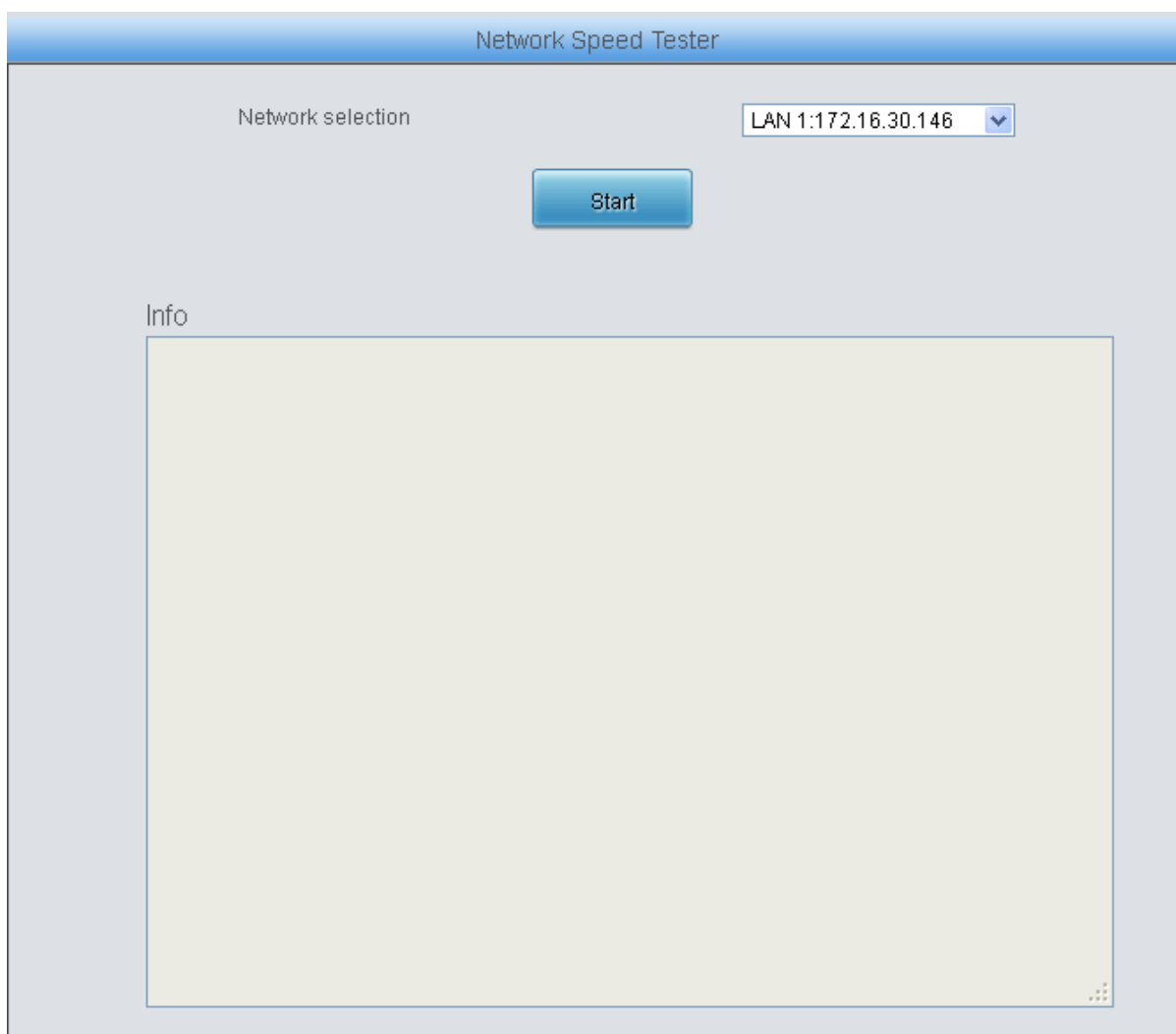


Figure 3-9 Network Speed Tester

The Network Speed Tester interface as shown above 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.

### 3.10.17 PING Test

Via 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 on the interface.

Item	Description
<b>Source IP Address</b>	Source IP address where the Ping test is initiated.
<b>Destination Address</b>	Destination IP address on which the Ping test is executed.
<b>Ping Count</b>	The number of times that the Ping test should be executed. Range of value: 1~100.
<b>Package Length</b>	Length of a data package used in the Ping test. Range of value: 56~1024 bytes.
<b>Info</b>	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.

### 3.10.18 TRACERT Test

Via 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 on the interface.

Item	Description
<b>Source IP Address</b>	Source IP address where the Tracert test is initiated.
<b>Destination Address</b>	Destination IP address on which the Tracert test is executed.
<b>Maximum Jumps</b>	Maximum number of jumps between the gateway and the destination address, which can be returned in the Tracert test. Range of value: 1~255.
<b>Info</b>	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.

### 3.10.19 Modification Record

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. Click **Download** to download the record file.

### 3.10.20 Backup & Upload

On 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.

### 3.10.21 Factory Reset

On the Factory Reset interface, click **Reset** to restore all configurations on the gateway to factory settings.

### 3.10.22 Upgrade

On the upgrade interface, 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**.

### 3.10.23 Account Manage

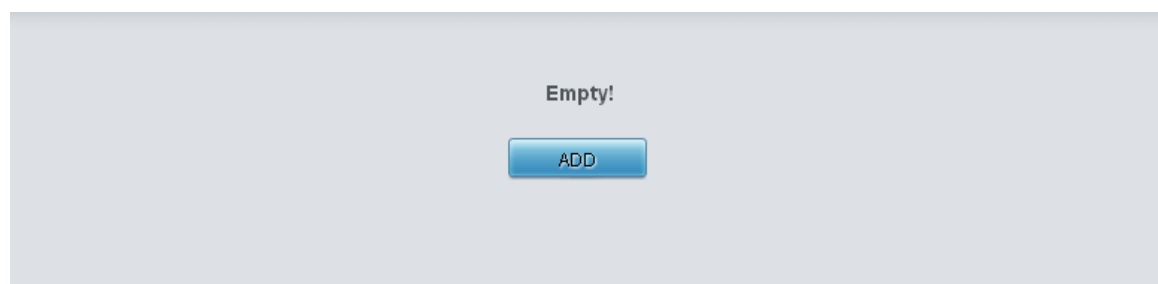


Figure 3-10 Account Management Interface

See Figure 3-10 for the Account Management interface. By default, there is no user information available on the gateway, click **Add** to add a piece of information.

The interface is titled "User Information Adding Interface". It is divided into two main sections: "Info" and "Page Tables".

**Info Section:**

- Index:
- User Name:
- Password:
- Authority:

**Page Tables Section:**

**Operation Info**

- ☐ Check All
- ☐ Call Monitor
- ☐ SIP Account Call Count
- ☐ Call Count
- ☐ IP Status
- ☐ Warning Info

**SIP**

- ☐ Check All
- ☐ SIP
- ☐ SIP Account
- ☐ SIP Trunk
- ☐ SIP Trunk Group
- ☐ SIP Register
- ☐ Media

**Route**

- ☐ Check All
- ☐ Routing Parameters
- ☐ IP->IP

**Number Filter**

- ☐ Check All
- ☐ Whitelist
- ☐ Filtering Rule
- ☐ Blacklist
- ☐ Number Pool

**Num Manipulate**

- ☐ Check All
- ☐ IP->IP CallerID
- ☐ IP->IP CalleeID
- ☐ CallerID Pool

**System Tools**

- ☐ Check All
- ☐ Network
- ☐ IP Routing Table
- ☐ Centralized Manage
- ☐ Signaling Capture
- ☐ Network Speed Tester
- ☐ Modification Record
- ☐ Upgrade
- ☐ Restart
- ☐ Authorization
- ☐ Access Control
- ☐ SIP Account Generator
- ☐ Signaling Call Test
- ☐ PING Test
- ☐ Backup & Upload
- ☐ Device Lock
- ☐ Management
- ☐ Certificate Manage
- ☐ Recording Manage
- ☐ Signaling Call Track
- ☐ TRACERT Test
- ☐ Factory Reset

At the bottom of the interface are two buttons: **Save** and **Cancel**.

Figure 3-11 User Information Adding Interface

The table below explains the configuration items shown on the interface.

Item	Description
------	-------------

<b>Index</b>	The unique index of user information, starting from 0 and supporting up to 64 pieces of user information to add.
<b>User Name/Password</b>	User name and password for WEB login. Only numbers, letters and underscores are supported.
<b>Authority</b>	Operation rights, including two options <i>Read</i> and <i>Read/Write</i> .
<b>Page Tables</b>	Select the page information to display.

After configuration, click **Save** to save the settings into the gateway or click **Close** to cancel the settings. See Figure 3-12 for the user information list.

Info				
Choose	Id	User	Permission	Modify
<input type="checkbox"/>	0	123	Read	

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

Figure 3-12 User Information List

Click **Modify** in Figure 3-12 to modify a piece of user information. The configuration items on the user information modification interface are the same as those on the **User Information Adding** interface. Note that the item **Index** cannot be modified.

To delete a piece of user information, 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 user information at a time, click the **Clear All** button.

### 3.10.24 Change Password

On the Password Changing interface 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.

### 3.10.25 Device Lock

On 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.

### 3.10.26 Restart

On 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

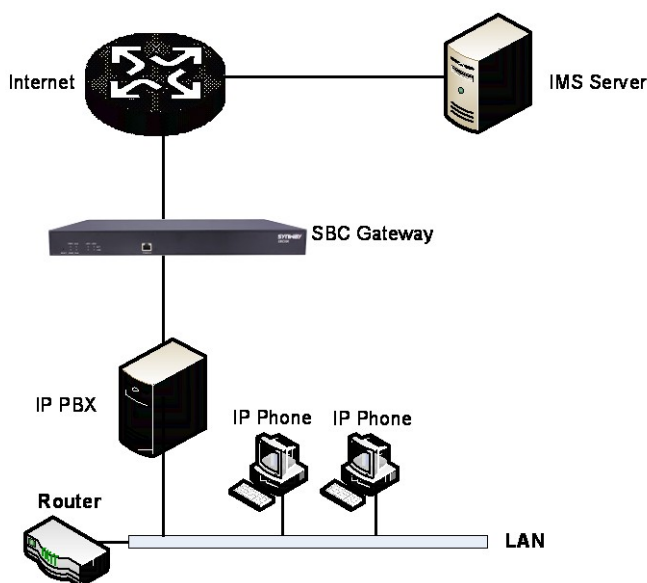


Figure 4-1 Typical Application

### 1. Configure SIP Settings for the SBC gateway.

SIP Settings	
SIP Address of WAN	LAN 1: 172.16.30.2
SIP Working Mode	Back-to-back User Agent
SIP Signaling Port	5060
SIP TLS Signaling Port	5061
Send 100rel	<input type="checkbox"/> Enable
Hide CallerID	Not Hidden
Obtain CallerID from	Username of From Field
Obtain/Send CalleeID from	'Request' Field
Asserted Identity Mode	Disable
Prack Send Mode	Require
NAT Traversal	<input type="checkbox"/> Enable
SIP Encryption	<input type="checkbox"/> Enable
RTP Encryption	<input type="checkbox"/> Enable
RTP Self-adaption	<input type="checkbox"/> Enable
UDP Header Checksum	<input checked="" type="checkbox"/> Enable
Rport	<input type="checkbox"/> Enable

Figure 4-2

### 2. Add the IP address of the SIP terminal.

SIP Trunk															
Check	Index	Description	SIP Agent	Username	Register Status	Remote Address	Remote Port	Local Network Port	Transport Protocol	SRTP Mode	Outgoing Voice Resource	Incoming Voice Resource	Send 180 and 183	DTMF Transmit Mode	Fax Mode
<input type="checkbox"/>	0	default	No	--	--	172.16.30.10	5088	LAN 1(172.16.30.2)	UDP	RTP Prior	512	512	No	Global	Global
<input type="checkbox"/>	1	default	No	--	--	172.16.30.6	5088	LAN 1(172.16.30.2)	UDP	RTP Prior	512	512	No	Global	Global
<div>◀</div>															
<div>▶</div>															
<div>Check All   Uncheck All   Inverse   Delete   Clear All</div>															
2 Items Total   20 Items/Page   1/1   First   Previous   Next   Last   Go to Page   1   1 Pages Total															
<div>Add New</div>															

Figure 4-3

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

Check	Index	SIP Trunks	SIP Trunk Select Mode	Description	Modify
<input type="checkbox"/>	0	0	Increase	default	
<input type="checkbox"/>	1	1	Increase	default	

Check All Uncheck All Inverse Delete Clear All Add New

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

Figure 4-4

4. Set routing parameters. You may adopt the default value 'Route before Number Manipulate' herein.

Operation Info SIP Fax Route Routing Parameters IP->IP Number Filter Num Manipulate VPN DHCP System Tools

Route Settings

IP Incoming Route before Number Manipulate

Save

Figure 4-5

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

Check	Index	Call Initiator	CallerID Prefix	CalleeID Prefix	Number Filter	Call Destination	Description	Modify
<input type="checkbox"/>	255	SIP Trunk Group [0]	*	*	none	SIP Trunk Group [1]	default	
<input type="checkbox"/>	254	SIP Trunk Group [1]	*	*	none	SIP Trunk Group [0]	default	

Check All Uncheck All Inverse Delete Clear All Add New

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

Figure 4-6

6. Set number manipulation rules. When the gateway receives a call from the network, 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.

Check	Index	Call Initiator	CallerID Prefix	CalleeID Prefix	With Original CalleeID	Stripped Digits from Left	Stripped Digits from Right	Reserved Digits from Right	Prefix to Add	Suffix to Add	Description	Modify
<input type="checkbox"/>	255	SIP Trunk Group [0]	*	8	No	1	0	100			default	
<input type="checkbox"/>	254	SIP Trunk Group [0]	*	7	No	1	0	100			default	

Check All Uncheck All Inverse Delete Clear All Add New

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

Figure 4-7

# Appendix A Technical Specifications

## Dimensions

440×44×267 mm<sup>3</sup>

## Weight

About 3.1 kg

## Environment

Operating temperature: 0℃—40℃

Storage temperature: -20℃—85℃

Humidity: 8%—90% non-condensing

Storage humidity: 8%—90% non-condensing

## LAN

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

Self-adaptive bandwidth supported

Auto MDI/MDIX supported

## Console Port

Amount: 1 (RS-232)

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: ≤22W

## 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

G.723 5.3/6.3 kbps

G.722 64 kbps

AMR-NB 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 SBC 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:

LAN1: 192.168.1.101

LAN2: 192.168.0.101

### 2. In what cases can I conclude that the SBC 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 channel 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 SBC 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](mailto:techsupport@sanhuid.com)

Email: [techsupport@synway.net](mailto:techsupport@synway.net)

MSN: [synway.support@hotmail.com](mailto:synway.support@hotmail.com)

### **Sales Department**

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: [sales@synway.net](mailto:sales@synway.net)