Synway SBC Series Gateway

SBC500

SBC30, SBC60

SBC120, SBC240

Gateway

User Manual

Version 1.8.0

Synway Information Engineering Co., Ltd
www.synway.net

Content

Content i

Copyright Declaration iii

Revision History iv

Chapter 1 Product Introduction 1

1.1 Typical Application 1
1.2 Feature List 1
1.3 Hardware Description 2
1.4 Alarm Info 5

Chapter 2 Quick Guide 7

Chapter 3 WEB Configuration 9

3.1 System Login 9
3.2 Operation Info 9
3.2.1 System Info 9
3.2.2 IP Status 11
3.2.3 Call Monitor 12
3.2.4 Client Info 13
3.2.5 Client Status 13
3.2.6 Call Count 13
3.2.7 SIP Account Call Count 14
3.2.8 Warning Info 14
3.3 SIP Settings 14
3.3.1 SIP 14
3.3.2 Hot Backup (HA) 18
3.3.3 SIP Trunk 19
3.3.4 SIP Register 21
3.3.5 SIP Account 22
3.3.6 SIP Trunk Group 22
3.3.7 Media Settings 23
3.4 Fax Settings 26
3.4.1 Fax 26
3.5 Route Settings 26
3.5.1 Routing Parameters 27
3.5.2 IP to IP 27
3.6 Number Filter 28
3.6.1 Whitelist 28
3.6.2 Blacklist 29
3.6.3 Number Pool 29
3.6.4 Filtering Rule 30
3.7 Number Manipulation 30
3.7.1 IP to IP CallerID 31
3.7.2 IP to IP CalleeID 32
3.7.3 CallerIP Pool 32
3.8 VPN 33
3.8.1 VPN Server Settings 33
3.8.2 VPN Account 33
3.9 DHCP 34
3.10 System Tools 34
3.10.1 Network 34
3.10.2 Authorization 35
3.10.3 Management 35

3.10.4 IP Routing Table 36
3.10.5 Firewall 36
3.10.6 IDS Settings 37
3.10.7 DDOS Settings 37
3.10.8 Certificate Management 38
3.10.9 Centralized Manage 39
3.10.10 SIP Account Generator 40
3.10.11 Recording Manage 40
3.10.12 Configuration File 40
3.10.13 Signaling Capture 40
3.10.14 Signaling Call Test 41
3.10.15 Signaling Call Track 41
3.10.16 Network Speed Tester 42
3.10.17 PING Test 42
3.10.18 TRACERT Test 43
3.10.19 Modification Record 43
3.10.20 Backup & Upload 43
3.10.21 Factory Reset 43
3.10.22 Upgrade 43
3.10.23 Account Manage 43
3.10.24 Change Password 45
3.10.25 Device Lock 45
3.10.26 Restart 45

Chapter 4 Typical Applications 46

Appendix A Technical Specifications 48

Appendix B Troubleshooting 49

Appendix C Technical/sales Support 50

Copyright Declaration

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 models SBC500, SBC30, SBC60, SBC120, SBC240.

1.1 Typical Application

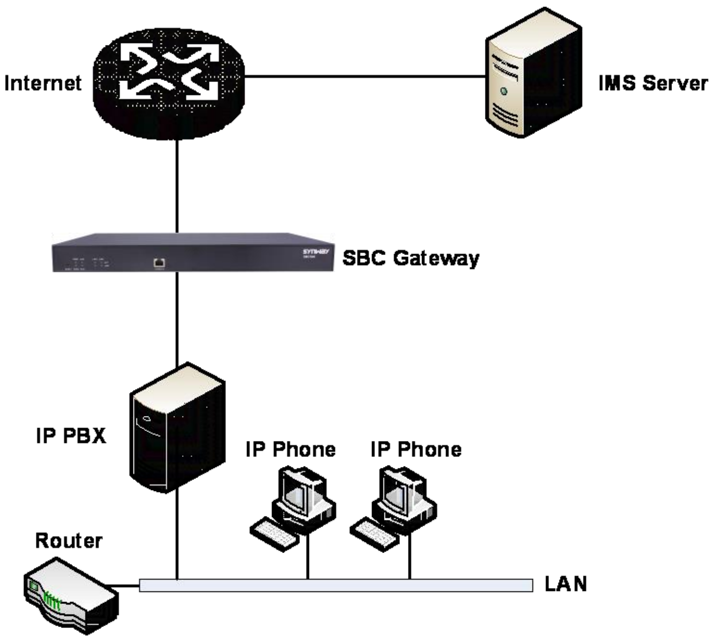

Figure 1-1 SBC Typical Application

1.2 Feature List

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

Voice	CODEC	G.711A, G.711U, G.729, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K) Note: Currently SBC30 and SBC60 only support three RTP codecs Alaw, ulaw, G729
	DTMF Mode	RFC2833, SIP INFO, INBAND, RFC2833+Signaling, In-band+Signaling
Network	**Description**	
Network Protocol	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN	
Static IP	IP address modification support	
DNS	Domain Name Service support	
Firewall	Firewall setting support	
SIP Encryption	SIP TLS encryption support	
RTP Encryption	RTP encryption protocol SRTP support	
DOS/DDOS Protection	Defense from DOS/DDOS attack	
PPPoE	PPPoE support	
IPV4/IPV6	IPV4 and IPV6 support	
Security	**Description**	
Admin Authentication	Support admin authentication to guarantee the resource and data security	
Maintain & Upgrade	**Description**	
WEB Configuration	Support of configurations through the WEB user interface	
Language	Chinese, English	
Software Upgrade	Support of user interface, gateway service, kernel and firmware upgrades based on WEB	
Tracking Test	Support of Ping and Tracert tests based on WEB	
SysLog Type	Three options available: ERROR, WARNING, INFO	

1.3 Hardware Description

The 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.

(a) See the figures below for SBC500 appearance:

Figure 1-2 Front View

Figure 1-3 Rear View

Figure 1-4 Left View

(b) See the figures below for SBC30 and SBC60 appearance:

Figure 1-5 Front View

Figure 1-6 Rear View

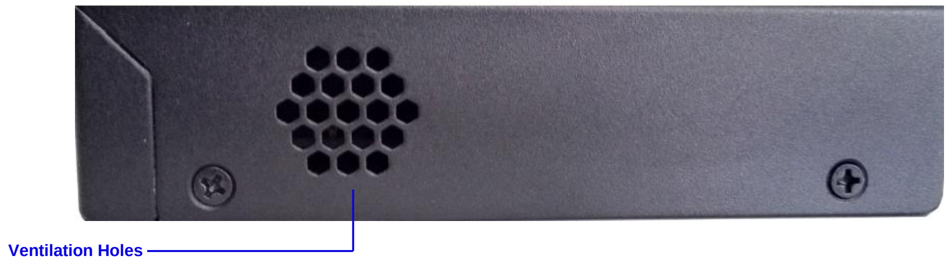

Figure 1-7 Left View

(c) See the figures below for SBC120 and SBC240 appearance:

Figure 1-8 Front View

Figure 1-9 Rear View

Figure 1-10 Left View

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

Interface	Description
LAN	Amount: 2
	Type: RJ-45
	Bandwidth: 10/100/1000Mbps
	Self-Adaptive Bandwidth Supported
	Auto MDI/MDIX Supported
E1/T1	Amount: 1/2/4/8/16

	Type: RJ-45
Console Port	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-11 for signal definition)
	Data Bits: 8 bits
	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
Button	**Description**
Power Key	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.
Reset Button	Restore the gateway to factory settings.
LED	**Description**
Power Indicator	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
Run Indicator	Indicates the running status. For more details, refer to Alarm Info.
Alarm Indicator	Alarms the device malfunction. For more details, refer to Alarm Info.
Link Indicator	The green LED on the left of LAN, indicating the network connection status.
ACT Indicator	The orange LED on the right of LAN, whose flashing tells data are being transmitted.
E1/T1 Indicators	The green LED on the right of E1/T1 interface lights up and keeps on after the E1/T1 module is successfully synchronized.
Channel Indicators	Indicates the synchronization status of E1/T1 channels. It will light up and keep on if E1/T1 is synchronized; otherwise, it will go out.

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.

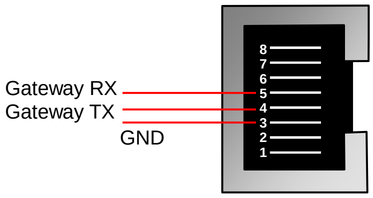

Figure 1-11 Console Port Signal Definition

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
Run Indicator	Go out	System is not yet started.

	Light up	System is starting.
	Flash	Device is running normally.
Alarm Indicator	Go out	Device is working normally.
	Light up	Upon startup: Device is running normally. In runtime: Device goes abnormal.
	Flash	System is abnormal.

Note:

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

Chapter 2 Quick Guide

This chapter is intended to help you grasp the basic operations of the 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.

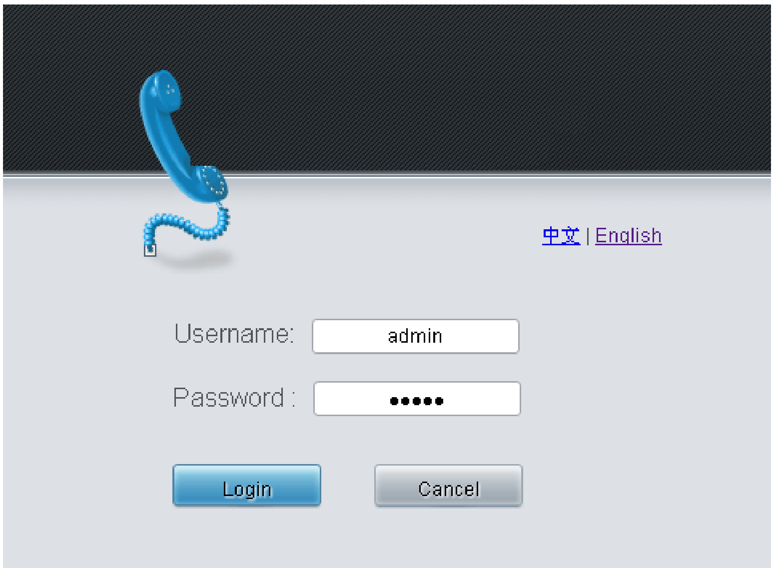

Figure 3-1 Login Interface

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

Current Speed	The current speed of data receiving and transmitting.
Work Mode	The work mode of the network, including six options: 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 1000 Mbps Full Duplex and Disconnected.
Network Type	The type of the network, including three options: Static, DHCP and PPPoE.
Runtime	Time of the gateway keeping running normally after startup. This parameter updates every 2s.
CPU Temperature	Display the real time temperature of the CPU.
CPU Usage Rate	Display the real time usage rate of the CPU.
Current RTP Message Data	Display the receiving and sending information of the current RTP data.
HA State	The dual-system hot backup state in the *Call Status Agent* mode, including Primary, Backup, and Independent. The original configuration state and heartbeat network port are indicated in parentheses.
DCMS Working Status	Display the connecting status of the gateway and DCMS.
Recording Work Status	Display the working status of the recording server docked by the gateway.
Authorization Status	Display the features of the SBC device, which requires authorization.
Authorization Numbers	Display the number of authorized devices.
Remaining Time	Display the remaining time after successful authorization.
Serial Number	Unique serial number of an SBC gateway.
WEB	Current version of the WEB interface.
Gateway	Current version of the gateway service.
Uboot	Current version of Uboot.
Kernel	Current version of the system kernel on the gateway.
Firmware	Current version of the firmware on the gateway.

3.2.2 IP Status

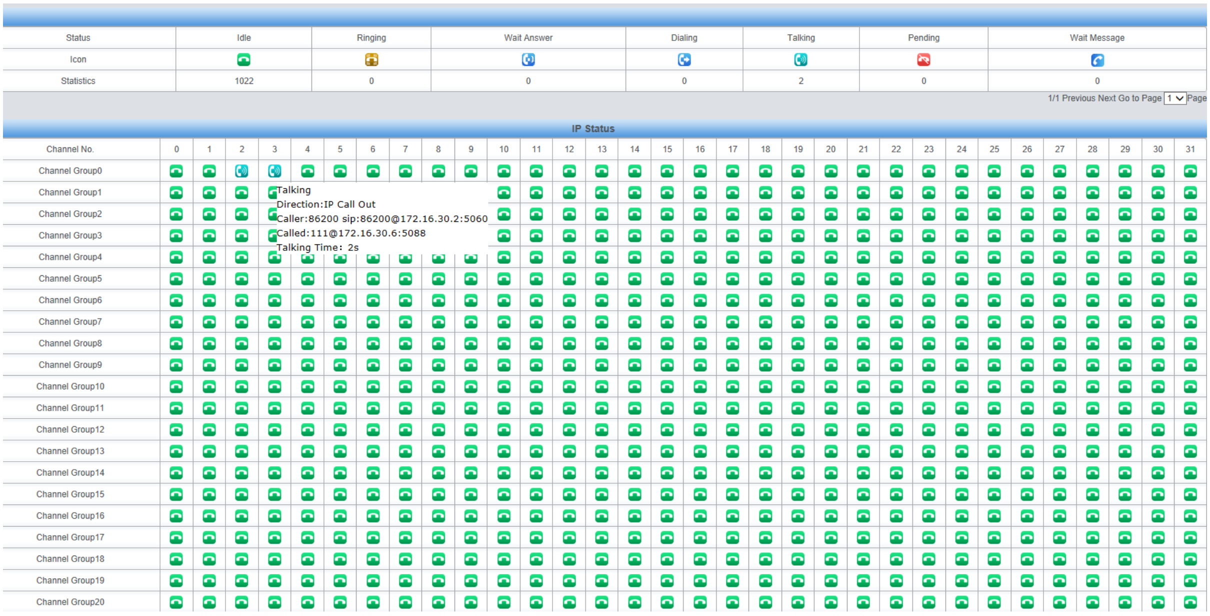

Figure 3-2 IP Status Interface

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.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Channel No.</td><td>Number of the IP channel on the device.</td></tr>
<tr><td>Status</td><td>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>
</td></tr>
</table>

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.

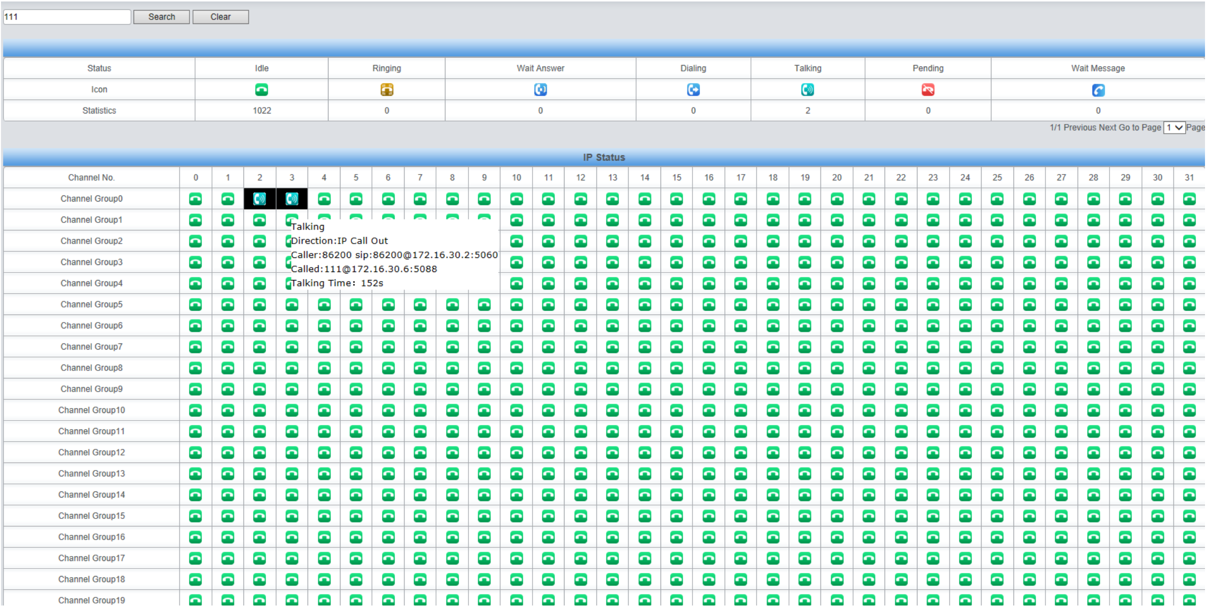

Figure 3-3 Search Calls

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

Click the icon in the channel status column, and you can monitor the call in real-time. If your computer is not installed with 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.

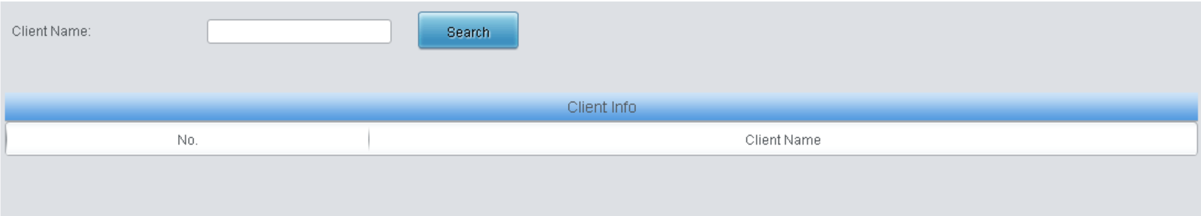

Figure 3-4 Client List Interface

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

Busy	Total number of the calls which fail as the called party has been occupied and replies a busy message. The corresponding SIP status code is 603.
No Answer	Total number of the calls which fail as the called party does not pick up the call in a long time or the calling party hangs up the call before the called party picks it up. The corresponding SIP status code is 403.
Routing Failed	Total number of the calls which fail because no routing rules are matched. The corresponding SIP status code is 488.
No Idle Resource	Total number of the calls which fail because no voice channel is available. The corresponding SIP status code is 486.
Failed	Total number of the calls which fail as the called party number does not conform to the number-receiving rule or for relative reasons. The corresponding SIP status code is 4xx, 5xx or 6xx.
Others	Total number of the calls which fail due to other unknown reasons. The corresponding SIP status code is 493.
Percentage	The percentage of the calls with a release cause to total calls.
Current Number of SIP Call in/out	The number of calls currently coming in to/out from the SIP.
Connected Number of SIP Call in/out	The number of successfully connected calls coming in to/going out from the SIP.
Total Number of SIP Call in/out	The sum of all calls coming in to/going out from the SIP.
Connection Rate of SIP Call in/out	The percentage of the number of successful SIP incoming/outgoing calls to the total number of incoming/outgoing calls.
CPS	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
SIP Address of WAN	IP address of WAN for SIP signaling, using LAN 1 by default.
SIP Working Mode	Set the working mode of SIP, including *Back-to-back User Agent* and *Call Status Agent*.
RTP Transcoding	When this feature is enabled, RTP will be transcoded by OCT after negotiation. This feature is disabled by default.
SIP Signaling Port	The port monitored by SIP UDP/TCP. The value range is 2000-65535 and the default value is 5060. **Note:** It cannot overlap with the RTP port range in the media settings.
SIP TLS Signaling Port	The port monitored by SIP TLS. The value range is 2000-65535 and the default value is 5061. **Note:** It cannot overlap with the RTP port range in the media settings.
Only Match Proxy Address to Confirm SIP Trunk	When external proxy is enabled, the external proxy address will be used instead of the remote address to match the SIP trunk. It is disabled by default.
Ringback Tone Settings	Ringback tone settings include *Common Ringback Tone*, *IMS Ringback Tone* and *Adaptive Ringback Tone*. Select **Common Ringback Tone** and you can enable *Provide All Ringback Tones* or *Provide Ringback Tone at First Recv of 18X (without SDP)*. Select **IMS Ringback Tone** and you can enable *Recv 18X (with SDP) and then 180 (without PEM),* or *Recv 18X (with SDP) and then 180 (PEM being inactive)* as the condition for providing ringback tone. If **Adaptive Ringback Tone** is selected, when receiving the 18X message with the SDP field, the gateway will transparently transmit the RTP message from the remote end, or play the ringback tone in case the remote end does not transmit the RTP message; when receiving the 18X message without the SDP field, the gateway will play the ringback tone and not transparently transmit the RTP message from the remote end.
First Route for Inbound IP Call	Set the priority in routing out the inbound IP calls. The default setting is IP to PSTN.
Hide CallerID	Once enabled, the CallerID will be hidden.
Obtain CallerID from	There are four optional ways to obtain the calling party number: Username of “From” Field, Displayname of “From” Field, *P-Preferred-Identity Field, P-Asserted-Identity Field*. The default value is *Username of “From” Field*.
Obtain/Send CalleeID from	There are two optional ways to obtain or send the called party number: from “To” Field or from “Request” Field. The default value is from *“Request” Field*.
Prack Send Mode	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.

DisplayName	Sets whether to carry the actual calling number in the DisplayName field of the SIP message sent by the gateway.
UserName	Sets whether to carry the gateway registered number in the UserName field of the SIP message.
NAT Traversal, Traversal Type	Sets whether to enable the feature of NAT Traversal. By default, the feature is disabled. There is only one optional traversal type: *Port Mapping*.
LAN1 Mapping Address, LAN2 Mapping Address	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.
Always Use Mapping Address	Once this feature is enabled, the gateway will be enforced to use the mapping address set in the above configuration item to initiate calls. By default it is *disabled*.
RTP Self-adaption	When this feature is enabled, the RTP reception address or port carried by the signaling message from the remote end, if not consistent with the actual state, will be updated to the actual RTP reception address or port. By default, this feature is *disabled*.
UDP Header Checksum	When this feature is enabled, the gateway will automatically calculate the check sum of the UDP header during RTP transmission.
Rport	When this feature is enabled, a corresponding Rport field will be added to the Via message of SIP. By default, it is *disabled*.
Auto Reply of Source Address	Once this feature is enabled, the gateway will reply the source address in the invite message. The default value is *disabled*.
Multiple Audio Selection	Since the SDP message carries multiple audio types, you can choose RTP or SRTP as the voice port.
Send Response by Former Via	Enabling this feature means to close the automatic modification on the Via header of the response message. By default it is disabled.
Registration Related Settings	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.
Time (min/month)	Specifies the call time for a SIP registered account.
SIP Registered Number Polling	When this feature is enabled, the call is polled among SIP registered accounts. By default it is disabled.
Failed Count	It is valid only when the feature *SIP Registered Number Polling* 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 *Recover Time of Disable Account*.
Recover Time of Disable Account (m)	See the description of *Failed Count*.
Caller Prefix Grouping	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.
Caller over Clocking (IP OUT)	Limit on the number of calls in a cycle for the calling number. By default this feature is disabled.

Cycle (min)	The time of a cycle. It is only valid when the feature *Caller over Clocking* is enabled.
Count Values	The allowed incoming calls within the set time of a cycle. It is only valid when the feature *Caller over Clocking* is enabled.
Interval (ms)	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 *Caller over Clocking* is enabled.
SIP Value of Reply	The abnormal SIP message returned by the gateway. The default value is 503.
Deny SIP Calls when Registration Fails	Unregistered and registration failed SIP accounts as well as the invite message over IP reply 503 for rejection, It is disabled by default.
Eth Resource	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.
Eth Resource Num	The number of network port resources is an integer greater than 0. The default value is 2.
SIP Account Numbers	The maximum number of SIP accounts, must be set greater than the number of existing SIP accounts. The default value is 2000.
SIP Account Registration Interval	The interval between registrations of multiple SIP accounts. Range of value: 0~10000, with the default value of 0.
DSCP	Sets whether to enable the DSCP differentiated services code point. By default, it is *disabled*.
Voice Media	Sets the priority of the voice media for DSCP. The voice media with a bigger value has a higher priority. The value range is 0~63, with the default value of *46*.
Signal Control	Sets the priority of the signal control for DSCP. The signal control with a bigger value has a higher priority. The value range is 0~63, with the default value of *26*.
Calls from SIP Trunk Address only	Once this feature is enabled, the gateway will only accept the calls from the IP addresses set in SIP Settings → SIP Trunk. By default, it is *disabled*. And it is only valid when the Firewall feature is not enabled.
Match Call Count to SIP Trunk based on Source Address of INVITE	Performs call count by matching the source address of the INVITE message. By default it is disabled.
Switch Signal Port if SIP Registration Failed	If the SIP registration fails, the SIP signaling port N will switch to N+1 for a new registration. It will continue until the registration succeeds. By default, it is *disabled*.
Hang up upon Call Time-out	Sets whether to enable the feature to hang up the call once it is time-out, with the default value of *No*.
Maximum Call Overtime	Sets the maximum overtime for a call. Calculated by minute.
Working Period, Period	The work period for the gateway, You can specify a certain period for the gateway to make calls. By default, the gateway is allowed to make calls any time in the day (24 Hours).

Sip Trunk Heart	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.
Trunk Heartbeat Cycle	The cycle to send the option message to the SIP trunk.
Allowed Times of NoResponse	The allowed times of SIP's no answer to the option message.
Return Value from SIP upon No Response	The SIP trunk did not reply with the SIP value returned by the option message. The default value is 502.
Support 100rel	Sets whether to carry 100rel in the Supported field of the request message for IP calls out. By default it is disabled.
Not Wait ACK after Sending 200 OK	Once this feature is enabled, the gateway does not need to wait the ACK message after sending the 200OK message. The default value is *disabled*.
Minimum Registration Interval	Used to set the minimum period for registering messages when *SIP Working Mode* is set to *Back-to-back User Agent*. The default value is 60.
The Percentage of Registration Message Sending Cycle to Period of Validity	Sets the percentage of the sending cycle of the SIP registration message to the validity period. Value of range: 1~200, with the default value of *70*.
Maximum Wait Answer Time	Sets the maximum time for the SIP channel to wait for the answer from the called party of the outgoing call it initiates. If the call is not answered within the specified time period, it will be canceled by the channel automatically. The default value is *60*, calculated by s.
Maximum Wait RTP Time	Sets the maximum time for the SIP channel to wait for the RTP packet. If no RTP packet is received within the specified time period, the channel will enter the pending state automatically and release the call. The default value is *0*, calculated by s.
Switch Network Port by Packet Loss Rate	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 *disabled*.
RTP Packet Loss Rate	Sets the RTP packet loss rate which is used as the judgment condition to switch the network port, with the default value of *5*.
UserAgent Field	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
HA	Set whether to enable the hot backup feature.
Remote Address	The IP address of the primary or backup SBC.

Primary/Backup	Set the local PC as the primary or backup SBC.
Heart Beat Lan	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
Index	The unique index of each SIP trunk.
Description	More information about each SIP trunk group.
SIP Agent	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.
Bulk Adding	After the ***SIP Agent*** feature is enabled on the SIP trunk, you can choose to add some in batches. It is disabled by default.
Addition Number	The number of SIP agents added in batches. The SBC supports a maximum of 1024.
UserName Step Size	The interval between adjacent user names, for example, the step size is 1 and the user names are 9000, 9001 ...
Password Step Size	The interval between adjacent passwords, similar to the username step size.
UserName	The username for the SIP terminal to register with the gateway.
Password	The password for the SIP terminal to register with the gateway.
Remote Address	Address of the SIP trunk, i.e. the IP address or domain name of the remote SIP terminal which will establish call conversation with the gateway.
Remote Port	Port of the SIP trunk.
Local Network Port	The network port where the SIP trunk locates.
Local SIP Port	The local signaling port where the SIP trunk locates.
Display CODEC	Used to show/hide the voice codec and the corresponding packing time.
CODEC	Supported CODECs: G711A, G711U, G729, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K). **Note:** Currently SBC30 and SBC60 only support three RTP codecs Alaw, ulaw, G729.
Packing Time	Time interval for packing an RTP packet, calculated by ms.
Transport Protocol	SIP transport protocol, providing three modes *UDP, TCP* and *TLS*. The default value is *UDP*.
SRTP Mode	Set the SRTP encryption mode, including *RTP Prior* and *SRTP Prior*. The default is *RTP Prior*.
Outgoing Voice Resource	Maximum number of voice channels for the outgoing calls allocated by the SIP trunk to the gateway.
Incoming Voice Resource	Maximum number of voice channels for the incoming calls allocated by the SIP trunk to the gateway.

Send 180 and 183	After receiving the 183 message from the destination trunk, first reply 180 and then 183. **Note:** Valid only when the SIP working mode is set to Back-to-back User Agent.
DTMF Transmit Mode	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. **Note:** Valid only when the SIP working mode is set to Back-to-back User Agent.
Fax Mode	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. **Note:** Valid only when the SIP working mode is set to Back-to-back User Agent.
Working Period, Period	The work period for the gateway, You can specify a certain period for the gateway to make calls. By default, the gateway is allowed to make calls any time in the day (24 Hours).
VOS1.1 SIP Encryption	Sets whether to perform VOS1.1 encryption for SIP signaling, including three modes: ***No Encryption, Gateway Encryption***, and ***Client Encryption***. The default setting is *No Encryption*. **Note:** Valid only when the SIP working mode is set to Call Status Agent.
Encrypt Key	A key that encrypts SIP signaling.
VOS1.1 RTP Encryption	Sets whether to perform VOS1.1 encryption for RTP. By default it is disabled. **Note:** Valid only when the SIP working mode is set to Call Status Agent.
Externally Bound Enable	Sets whether to enable the Proxy feature. Once it is enabled, SIP messages will be sent to the proxy address.
Externally Bound Address	The proxy address.
Externally Bound Port	The proxy port.
Asserted Identity Mode	Sets whether to have the invite message include some header information, two options available now: P-Asserted-Identity and P-Preferred-Identity. The default value is *disabled*.
Number in From Field not Manipulated	Once this feature is enabled, the callerID in the From field will not be manipulated, with the default value of *disabled*. **Note:** It is valid only when the configuration item Asserted Identity Mode is enabled.
Add Content to To Field in INVITE Message	Once this feature is enabled, you need to set the TO field in "Add Content". By default it is disabled.
Add Content	Customizes the content added to the TO field, such as user=phone.
Send 100rel	Sets whether to send the 100rel field with the 180/183 message. The default setting is disabled.
Hide CallerID	Sets whether to hide the CallerID. It is disabled by default.
Session Timer	Sets whether to enable the session refresh feature, with the default value of *disabled*. Once this feature is enabled, you are required to enter the minimum time and the timeout value.

Minimum Time	Sets the minimum time for refreshing the session. Value of range: 90~65535, with the default value of *150*.
Timeout	Sets the timeout value for refreshing the session. The value cannot be less than that of Minimum Time, with the default value of *600*.
Early Media	Once this feature is enabled, the P-Early-Media field will be included in the Invite message. The default value is *disabled*.
Early Session	Once this feature is enabled, the early-session field will be included in the Invite message. The default value is *disabled*.

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
Index	The unique index of each SIP register.
SIP Trunk No.	The number of the SIP trunk which registers to the SIP server.
Username	When the gateway initiates a call to SIP, this item corresponds to the username of SIP; when the gateway initiates a call to PSTN, this item corresponds to the displayed CallerID.
Password	Registration password of the gateway. To register the gateway to the SIP server, both configuration items ***Username*** and ***Password*** should be filled in.
Register Address	Address of the SIP server to which the SIP trunk is registered.
Register Port	The signaling port of the SIP trunk.
Domain Name	Domain name of the gateway used for SIP registry.
Register Expires	Validity period of the SIP registry. Once the registry is overdue, the gateway should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
Authentication Username	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
Index	The unique index of each SIP account.
SIP Trunk No.	The number of the SIP trunk to which the SIP account is registered.
Username	The registration username of the SIP account. Once the SIP account is successfully registered, the SIP server can initiate calls to the gateway via ***Username***.
Password	The registration password of the SIP account. To register the SIP account to the SIP trunk, both configuration items ***Username*** and ***Password*** should be filled in.
Register Expires	The validity period of the SIP account registry. Once the registry is overdue, the SIP account should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
Register Status	The registration status of the SIP account. It is either *Registered* or *Failed*.
Authentication Username	Authentication username of a port, used to register the port to the SIP server.
Description	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
Index	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.
Description	More information about each SIP trunk group.

<table>
<tr><td>SIP Trunk Select Mode</td><td>When the SIP trunk group receives a call, it will choose a SIP trunk based on the select mode set by this configuration item to ring. The optional values and their corresponding meanings are described in the table below.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Increase</td><td>Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.</td></tr>
<tr><td>Decrease</td><td>Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.</td></tr>
<tr><td>Cyclic Increase</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from SIP Trunk N+1.</td></tr>
<tr><td>Cyclic Decrease</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from SIP Trunk N-1.</td></tr>
</table></td></tr>
<tr><td>IP→IP Outgoing Call Forbidden</td><td>Sets whether to restrict the calls from IP to IP, with the default value of No. If you select ‘Yes’, you are required to fill in Called Party Forbidden Rule and Calling Party Forbidden Rule. See the note below for details.</td></tr>
<tr><td>SIP Trunks</td><td>The SIP trunks in the SIP trunk group. If the checkbox before a SIP trunk is grey, it indicates that the SIP trunk has been occupied. The ticked SIP trunks herein will be displayed in the column ‘SIP Trunks’.</td></tr>
</table>

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
DTMF Transmit Mode	Sets the mode for the IP channel to send DTMF signals. The optional values are *RFC2833*, *In-band*, *Signaling*, *RFC2833+Signaling* and *In-band+Signaling*, with the default value of *RFC2833*.
RFC2833 Payload	Payload of the RFC2833 formatted DTMF signals on the IP channel. Range of value: 90~127, with the default value of *101*.

RTP Port Range	Supported RTP port range for the IP end to establish a call conversation. Range of value: 5000~60000, with the lower limit of 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.
Silence Suppression	Sets whether to send comfort noise packets to replace RTP packets or never to send RTP packets to reduce the bandwidth usage when there is no voice signal throughout an IP conversation. The optional values are *Enable* and *Disable*, with the default value of *Disable*. **Note:** When G723 is selected as CODEC, this configuration setting will turn to Enable automatically.
Noise Reduction	Once this feature is enabled, the volume of the noise accompanied with the line will be reduced automatically. The default setting is *Enable*.
JitterMode	Sets the working mode of JitterBuffer. The optional values are *Static Mode* and *Adaptive Mode*, with the default value of *Static Mode.*
JitterBuffer(ms)	Acceptable jitter for data packets transmission over IP, which indicates the buffering capacity. A larger JitterBuffer means a higher jitter processing capability but as well as an increased voice delay, while a smaller JitterBuffer means a lower jitter processing capability but as well as a decreased voice delay. Range of value: 0~280, calculated by ms, with the default value of 100.
JitterUnderrunLead(ms)	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*, **Note:** Only when JitterMode is set to *Static Mode* will this item be shown.
JitterOverrunLead(ms)	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*, **Note:** Only when JitterMode is set to *Static Mode* will this item be shown.
JitterMin	Sets the minimum delay that can be set by the adaptive jitter function. It must be smaller than the value set in JitterBuffer. Range of value: 0~280, calculated by ms, with the default value of 80. **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.
JitterDecreaseRatio	Sets the rate of 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*, **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.
JitterIncreaseMax	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*, **Note:** Only when JitterMode is set to *Adaptive Mode* will this item be shown.
Voice Gain Output from IP	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.
Use Default Value if Packtime Negotiation fails	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.

CODEC Setting

Sets CODECs for the IP end to establish a call conversation. The table below explains the sub-items:

Sub-item	Description
Gateway Negotiation Coding Sequence	Sets the coding sequence, including two options: *Default Priority* and *User-defined Priority*, with the default value of *Default Priority*.
Priority	Priority for choosing the CODEC in an SIP conversation. The smaller the value is, the higher the priority will be.
CODEC	Seven optional CODECs are supported: *G711A*, *G711U*, *G729AB*, *G722*, *G723*, *iLBC, AMR-NB, SILK(16K)*, *OPUS(16K)*, *SILK(8K)*, *OPUS(8K).* **Note:** Currently SBC30 and SBC60 only support three RTP codecs Alaw, ulaw, G729.
Packing Time	Time interval for packing an RTP packet, calculated by ms.
Bit Rate	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 G711A, G711U, G729AB, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K) by priority from high to low. The CODECs set here will be the default CODEC for the new added SIP trunks.

The packing time and bit rate supported by different CODECs are listed in the table below. Those values in bold face are the default values.

Note: Currently SBC30 and SBC60 only support three RTP codecs Alaw, ulaw, G729.

COEDC	Packing Time (ms)	Bit Rate (kbps)
G711A	10 / **20** / 30 / 40 / 50 / 60	**64**
G711U	10 / **20** / 30 / 40 / 50 / 60	**64**
G729	10 / **20** / 30 / 40 / 50 / 60	**8**
G722	10 / 20 / **30** / 40	**64**
G723	**30** / 60	5.3 / **6.3**
iLBC	**20** / 40	**15.2**
	30	13.3
	60	13.3 / **15.2**
AMR	**20** / 40 / 60	4.75 / 5.15 / 5.90 / **6.70** / 7.40 / 7.95 / 10.20 / 12.20
SILK(16K)	**20** /40 / 60 / 80 / 100	**20**
OPUS(16K)	10 / **20** / 40 / 60	**20**
SILK(8K)	**20** /40 / 60 / 80 / 100	**20**
OPUS(8K)	10 / **20** / 40 / 60	**20**

3.4 Fax Settings

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

3.4.1Fax

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

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

Item	Description
Pass-through Payload	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.

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

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

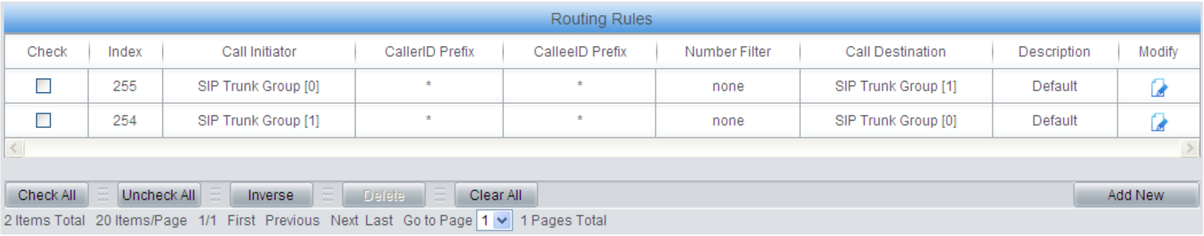

Figure 3-5 IP→IP Routing Rule Configuration Interface

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

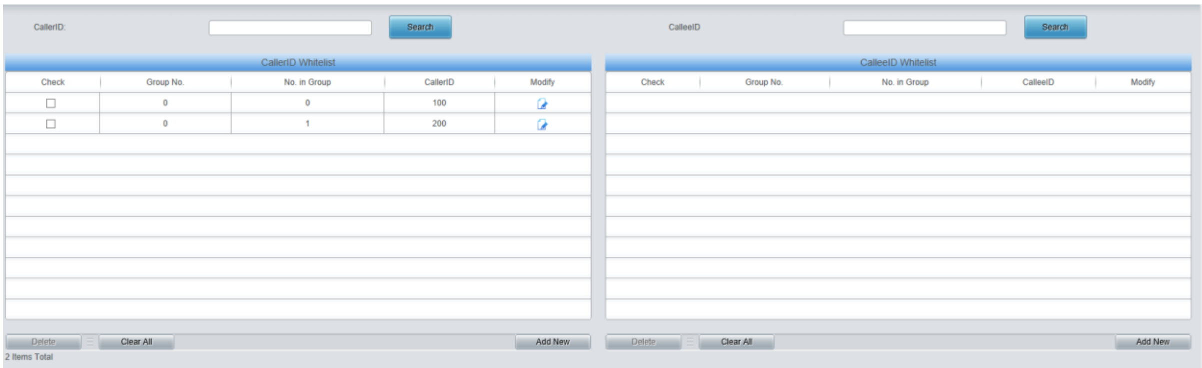

Figure 3-6 Whitelist Setting Interface

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
Group	The corresponding Group ID for CallerIDs/CalleeIDs in the whitelist. The value range is 0~7.
No. in Group	The corresponding No. for different CallerIDs/CalleeIDs in a same group.

<table>
<tr><td>CallerID</td><td>CallerID in the whitelist, which can not be left empty. Rule explanation:
<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>“*”</td><td>indicating any string</td></tr>
<tr><td>“0”~”9”</td><td>Digits 0~9.</td></tr>
<tr><td>“x”</td><td>A random number. A string of ‘x’s represents several random numbers. For example, ‘xxx’ denotes 3 random numbers.</td></tr>
<tr><td>“[ ]”</td><td>‘[ ]’ is used to define the range for a number. Values within it only can be digits ‘0~9’, punctuations ‘-’ and ‘,’. For example, [1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.</td></tr>
<tr><td>“-”</td><td>’-’ is used only in ‘[ ]’ between two numbers to indicates any number between these two numbers.</td></tr>
<tr><td>“,”</td><td>’,’ is used only in ‘[ ]’ to separate numbers or number ranges, representing alternatives.</td></tr>
</table></td></tr>
<tr><td>CalleeID</td><td>CalleeID in the whitelist, which can not be left empty. The rules are the same as that of CallerID.</td></tr>
</table>

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

Click ***Modify*** 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
Group	The corresponding Group ID for numbers in the number pool. The value range is 0~15.
No. in Group	The corresponding No. for different numbers in a same group. It supports up to 100 number s in one group.

Number Range	The range of the numbers in a number Pool. It must be filled in with numbers and can not be left empty.

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

Click ***Modify*** 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
No.	The corresponding number for a filtering rule. The value range is 0~99.
CallerID Whitelist	The Group No. of CallerIDs saved on the whitelist setting interface.
CalleeID Whitelist	The Group No. of CalleeIDs saved on the whitelist setting interface.
CallerID Blacklist	The Group No. of CallerIDs saved on the blacklist setting interface.
CalleeID Blacklist	The Group No. of CalleeIDs saved on the blacklist setting interface.
CallerID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the CallerID pool in whitelist.
CallerID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the CallerID pool in blacklist.
CalleeID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the CalleeID pool in whitelist.
CalleeID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the CalleeID pool in blacklist.
Original CalleeID Pool in Whitelist	Select a Group No. which is set in the whitelist from the number pool as the original CalleeID pool in whitelist.
Original CalleeID Pool in Blacklist	Select a Group No. which is set in the blacklist from the number pool as the original CalleeID pool in blacklist.
Description	Remarks for the filtering rule. It can be any information, but can not be left empty.

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

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

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

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

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

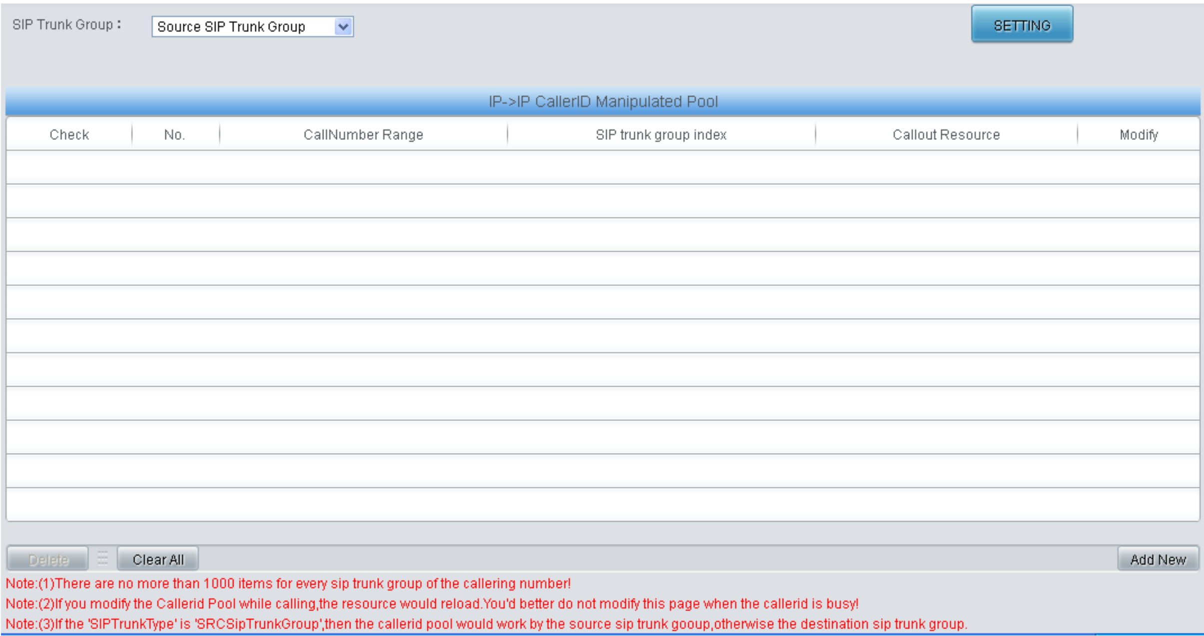

Figure 3-7 CallerIP Pool Interface

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.

Figure 3-8 CallerIP Adding Interface

The table below explains the items shown on the interface.

Item	Description
No.	The unique number of the CallerID in the pool, which denotes its priority. A CallerID with a smaller index value has a higher priority.
Source SIP Trunk Group	A specified SIP trunk group. Only calls in this SIP trunk group can be performed with callerIP manipulation.
CallerNum	Sets the range of the CallerIP for the call.
Callout Resource	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
VPN Server	Set whether to enable the VPN server.
VPN Type	The protocol type of VPN. Currently, only PPTP is supported.
Identify Verification Protocol	Set the protocol for VPN authentication, including MS-CHAPv2+MPPE, MS-CHAPv2 and MS-CHAP.
Client Range	Set the IP range of clients that can be accessed remotely.
Preferred WINS Address/ Spare WINS Address	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
Index	The unique index of each VPN account.

Username	The username for the client to connect with the VPN server.
Password	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
DHCP Server	Set whether to enable the DHCP server feature.
IP Range	Set the range of IP addresses that the DHCP server can assign.
Subnet Mask	Set the subnet mask required to enable the DHCP server.
Default Gateway	Set the default gateway required to enable the DHCP server.
DNS Server	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 abnormity 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, while SBC30 supports up to 30, SBC60 supports up to 60, SBC120 supports up to 120 and SBC240 supports up to 240 channels of authorization.

3.10.3 Management

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

Item	Description
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.
Access Setting	Sets the IP addresses which can access the gateway via WEB. By default, all IPs are allowed. You can set an IP whitelist to allow all 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.
Time to Log Out	The gateway will log out automatically if it is not operated during a time longer than the value of this item, calculated by s, with the default value of 1800.
SSH	Sets whether to enable the gateway to be accessed via SSH, with the default value of *No*.
SSH Port	The port which is used to access the gateway via SSH.
Remote Data Capture	After this feature is enabled, you can obtain the gateway data via a remote capture tool. The default value is *No*.
Capture RTP	Sets whether to capture RTP. Once this feature is enabled, the RTP package will also be captured by the selected network.
FTP	Sets whether to enable the FTP server, with the default value of *Yes*.
Enable Watchdog	Sets whether to enable the watchdog feature, with the default value of *Yes*.
SYSLOG	Sets whether to enable SYSLOG. It is required to fill in ***SYSLOG Server Address*** and ***SYSLOG Level*** in case SYSLOG is enabled. By default, ***SYSLOG*** is disabled.
Server Address	Sets the SYSLOG server address for log reception.
SYSLOG Level	Sets the SYSLOG level. There are three options: *ERROR*, *WARNING* and *INFO*.
Send CDR	Sets whether to enable the feature of sending CDR. It is required to fill in ***Server Address*** and ***Server Port*** in case Send CDR is enabled. By default, ***Send CDR*** is disabled.
Server Address	The address of the server to receive CDR.
Server Port	The port of the server to receive CDR.
Send Failed Call Record	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.
Add Hangup Side	Add hangup information to CDR.
Monitor Self-adaption	Enable the NAT stun between the gateway and the monitor tool. By default, it is disabled.
NTP	Sets whether to enable the NTP time synchronization feature. It is required to fill in ***NTP Server Address***, ***Synchronizing Cycle*** and ***Time Zone*** in case NTP is enabled. By default, ***NTP*** is disabled.

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

3.10.4 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
No.	The number of the routing in routing table.
Destination	The network segment where the IP packet can reach.
Subnet Mask	The subnet mask of the destination network segment.
Network Port	The corresponding network port of the routing.

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

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
Index	The unique index of a firewall rule, used to specify its priority. The smaller the value, the higher the priority.
Source Address	Set the IP address of the source network or an explicit host name.
Source Port	Set the source UDP/TCP port (remote host) of the packet sent to the gateway.
Local Port	Set the port of the local gateway.
Protocol	Protocol type, including eight options: Any, TCP, UDP, UDPLITE, ICMP, ESP, AH and SCTP.
LAN	Select the network port to which the firewall rule is applied.

Network Speed Limit	Set the expected rate of the network in packs. **Note:** 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.
Buffer Capacity	Set the buffer capacity of the network rate. The default value is 0.
Operate	Set the execution results of firewall rules, including two options: *Permit* and *Prevent*.

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
Type	Sets the type for detecting whether the SIP message conforms to the specification or blacklist, including five conditions: *TLS Connection Failed*, *Malformed SIP Datagram*, *Registration Failed*, *Call Failed* and *SIP Exception Flow*.
Warning Threshold	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.
Blacklist Threshold	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.
Blacklist Validity	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
WEB Port Attack Protection	When this feature is enabled, the WEB port will have the ability to block DDOS attacks.

WEB Limit	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).
FTP Port Attack Protection	When this feature is enabled, the FTP port will have the ability to block DDOS attacks.
FTP Limit	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).
SSH Port Attack Protection	When this feature is enabled, the SSH port will have the ability to block DDOS attacks.
SSH Limit	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).
TELNET Port Attack Protection	When this feature is enabled, the TELNET port will have the ability to block DDOS attacks.
TELNET Limit	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).
Set Validity of Attacker IP Blacklist	Determine whether to enable the attack blacklist effective time setting, including two options: *Forever* and *In the Set Time*.
Time	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
Country	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.
Province	Fill in the province, for example, Zhejiang.
City	Fill in the city, for example, Hangzhou.
Company	Fill in the company name.
Department	Fill in the department, for example, IT Dept.
Host Name	Fill in the IP address of SBC.
Email	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
Auto Change Default Gateway	Once this feature is enabled, the gateway will connect the DCMS via another network port automatically once the connected network cable is loosen or drawn out. The default value is disabled.
Management Platform	Select a management platform for the gateway to register.
Company Name	The company name used to register the gateway to DCMS, only valid when DCMS is selected.
Gateway Description	The description displayed on DCMS after the gateway is registered to DCMS, giving an easy identification of the gateway in device grouping. This item is only valid when DCMS is selected.
Centralized Management Protocol	Sets the centralized management protocol. It only supports SNMP currently.
SNMP Version	Sets the version of SNMP, three options available: V1, V2 and V3, with the default value of V2.
SNMP Server Address	IP address of SNMP.
Monitoring Port	Monitoring Port for SNMP on the gateway.
Community String	Community string used for information acquisition.
Account	The account of SNMP, only valid when the SNMP version is set to V3.
Grade	The grade of SNMP, three options available: Neither authenticated nor encrypted, Authenticated but not encrypted and Authenticated and encrypted, with the default value of *Neither authenticated nor encrypted*. It is only valid when the SNMP version is set to V3.
Authentication Password	The authentication password required to enter when the item Grade is set to Authenticated but not encrypted or Authenticated and encrypted.
Encryption Password	The encryption password required to enter when the item Grade is set to Authenticated and encrypted.
Authorization Code	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.
Working Status	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
Authentication Name	The authentication name for the gateway to connect with the recording server.
Password	The password for the gateway to connect with the recording server.
Recording Server IP	The IP address of the recording server used to connect with the gateway.
Occasion to Start Recording	Sets the time to start recording, with two options available: Ringing and Talking.
The Minimum Talking Time Saved	The calls shorter than the set value will not be saved. The default value is 5 seconds.
Network Port to Forward RTP	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
Test Type	The type of the call test.
SIP Trunk Group No.	The SIP trunk group number you are required to select for call testing.
CallerID	The CallerID for the call test.
CalleeID	The CalleeID for the call test.
DTMF	You can use this item to send DTMFs after the establishment of call conversation on the channel for call test
Add Invite Header, FieldName, Field Content	You can use this item to add the invite header and its corresponding content
Signaling Trace	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

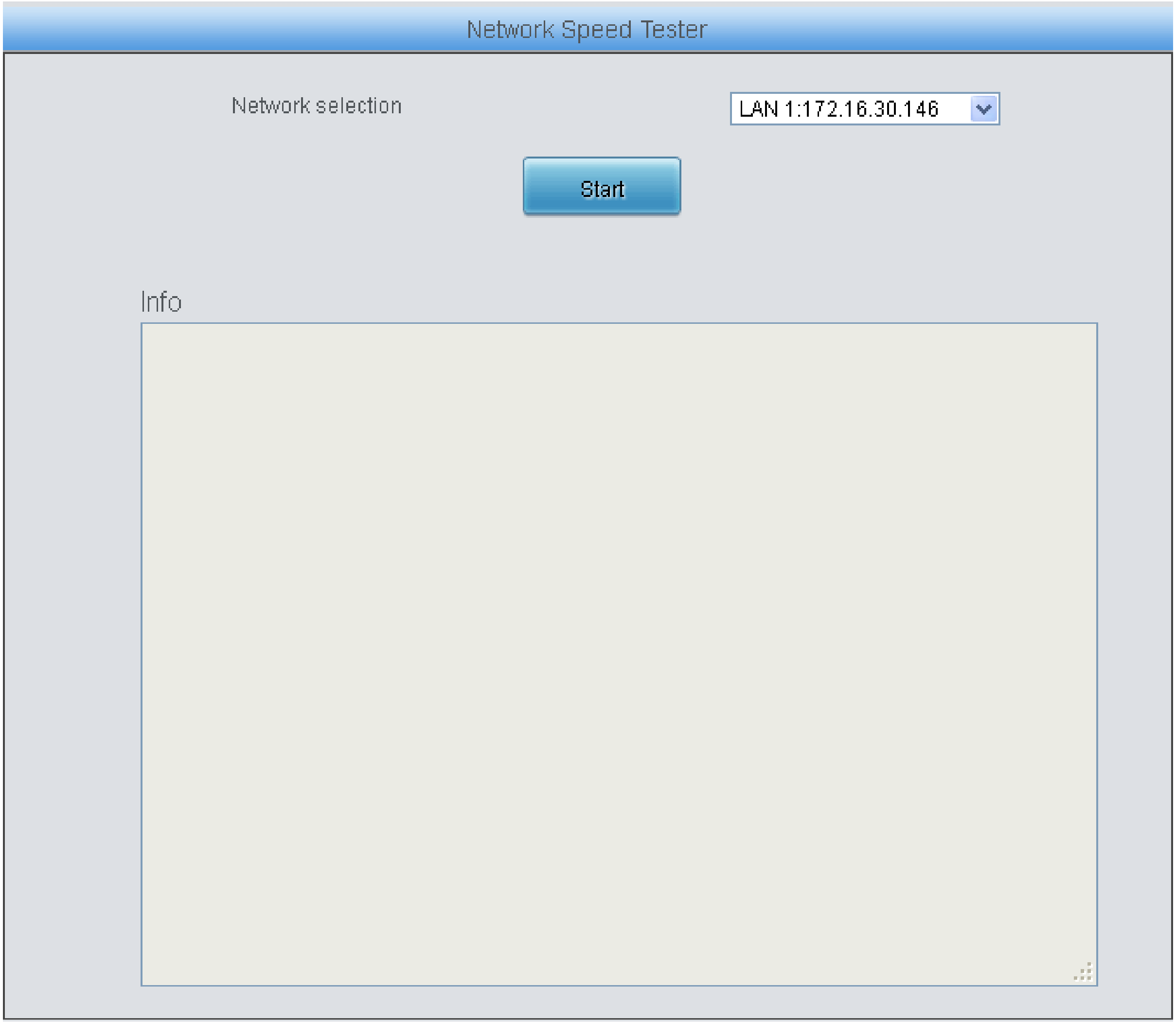

Figure 3-9 Network Speed Tester

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

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

3.10.18 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
Source IP Address	Source IP address where the Tracert test is initiated.
Destination Address	Destination IP address on which the Tracert test is executed.
Maximum Jumps	Maximum number of jumps between the gateway and the destination address, which can be returned in the Tracert test. Range of value: 1~255.
Info	The information returned during the Tracert test, helping you to learn the detailed information about the jumps between the gateway and the destination address.

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

3.10.19 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

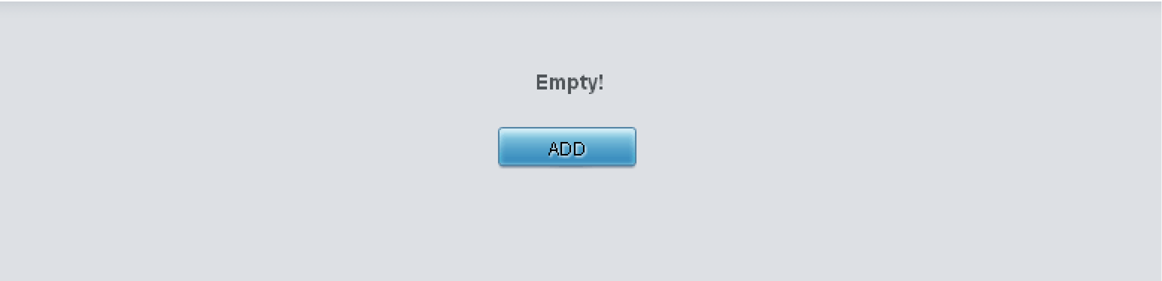

Figure 3-10 Account Management Interface

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.

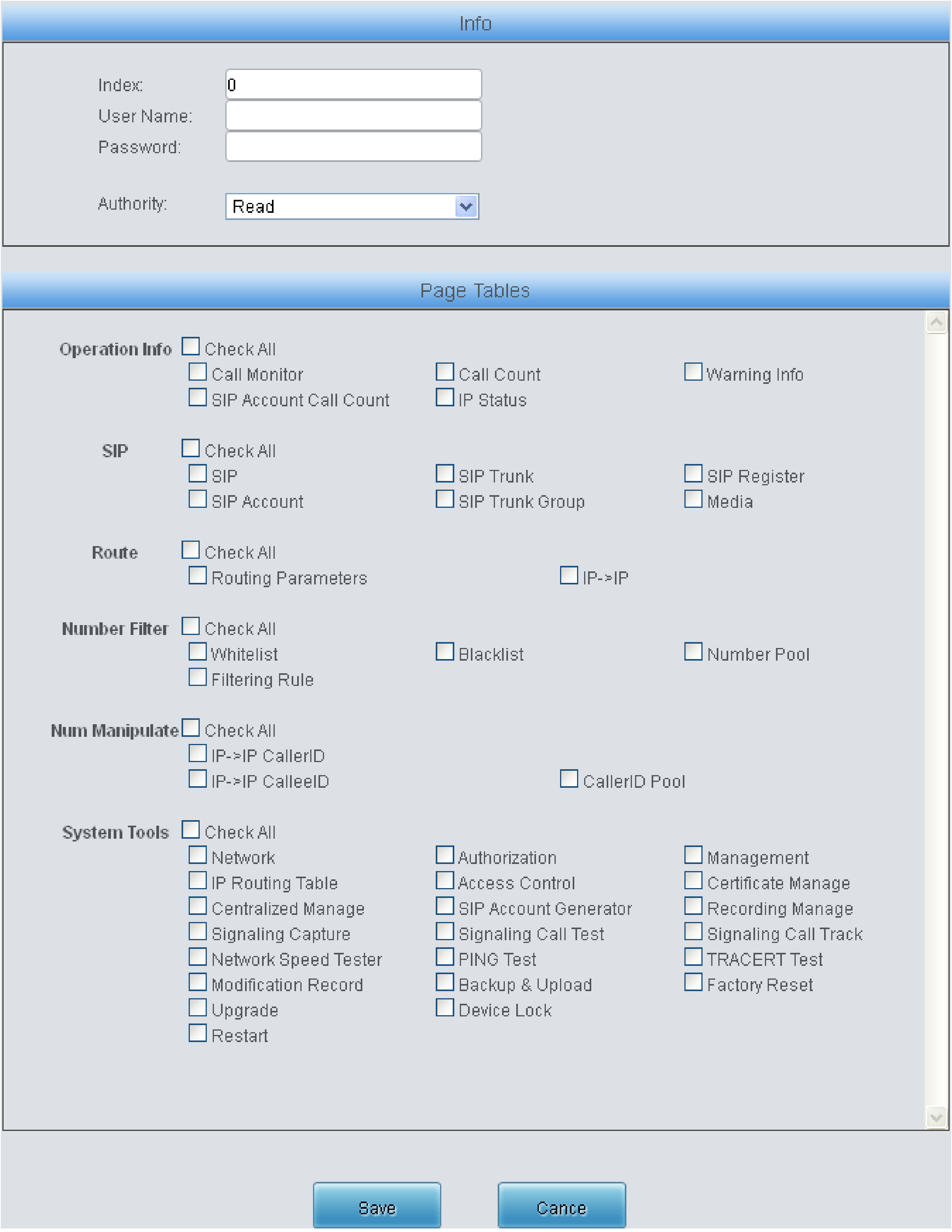

Figure 3-11 User Information Adding Interface

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

Item	Description

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

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

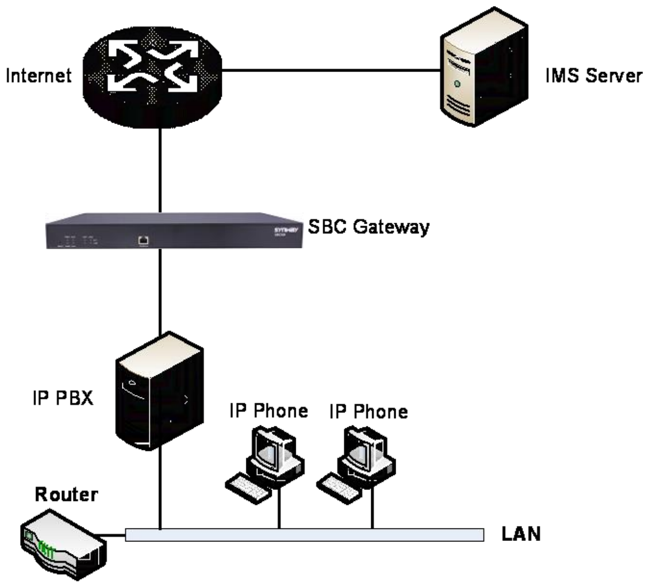

Figure 4-1 Typical Application

1. Configure SIP Settings for the SBC gateway.

Figure 4-2

2. Add the IP address of the SIP terminal.

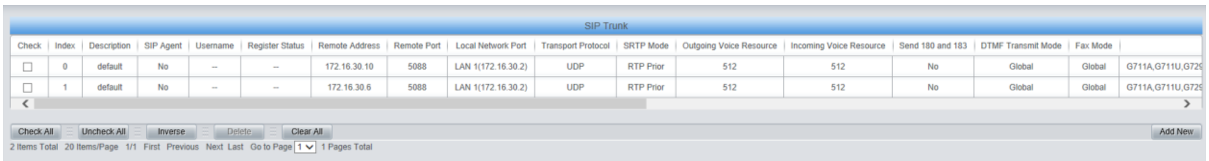

Figure 4-3

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

Figure 4-4

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

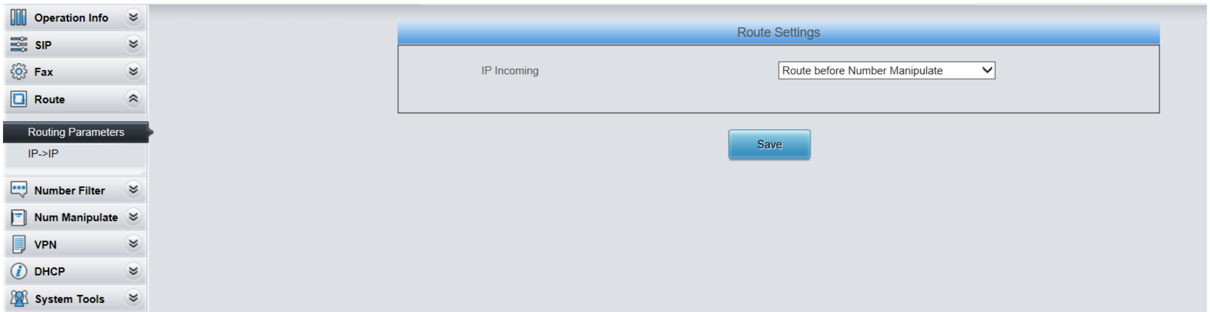

Figure 4-5

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

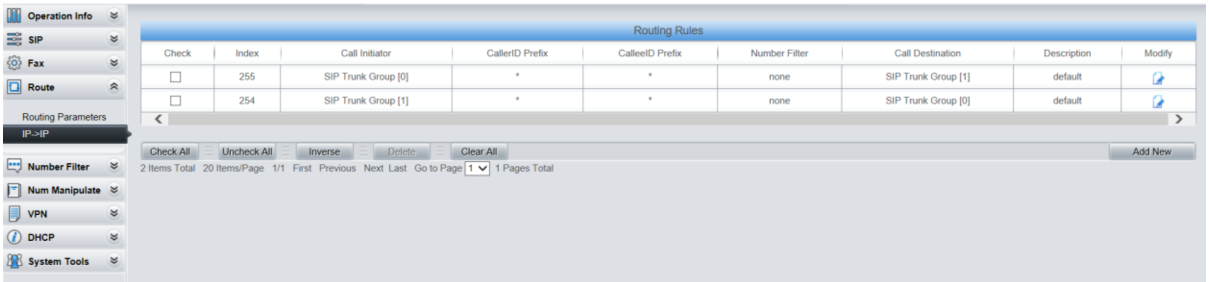

Figure 4-6

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

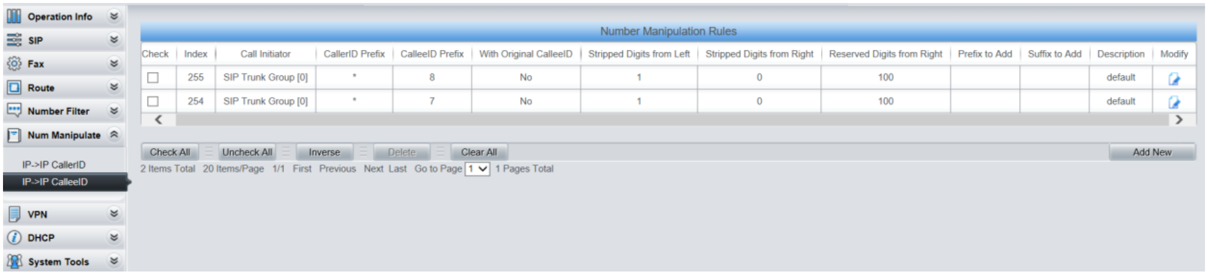

Figure 4-7

Appendix A Technical Specifications

Dimensions

440×44×267 mm^3

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*
G723	*5.3/6.3 kbps*
G722	*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, Building 1, Joinhands Science Park, No.4028, Nanhuan Road, Binjiang District, Hangzhou, P.R.China, 310053

Tel: +86-571-88860561

Fax: +86-571-88850923

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

Technical Support

Tel: +86-571-88864579

Mobile: +86-18905817070

Email: techsupport@sanhuid.com

Email: techsupport@synway.net

MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: sales@synway.net