Synway SMG Series Digital Gateway

SMG2030L

SMG2060L

Digital Gateway

User Manual

Version 1.6.5

Synway Information Engineering Co., Ltd

www.synway.net

Content

Copyright Declaration

Revision History

Version	Date	Comments
Version 1.6.5	2017-06	Initial publication.

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 SMG Series Digital Gateway!

The Synway SMG series digital gateway products (hereinafter referred to as 'SMG digital gateway') are mainly used for connecting PSTN or enterprise PBX with the IP telephony network or IP PBX. It provides a powerful, reliable and cost-effective VoIP solution for such occasions as IP call centers and multi-branch agencies.

1.1 Typical Application

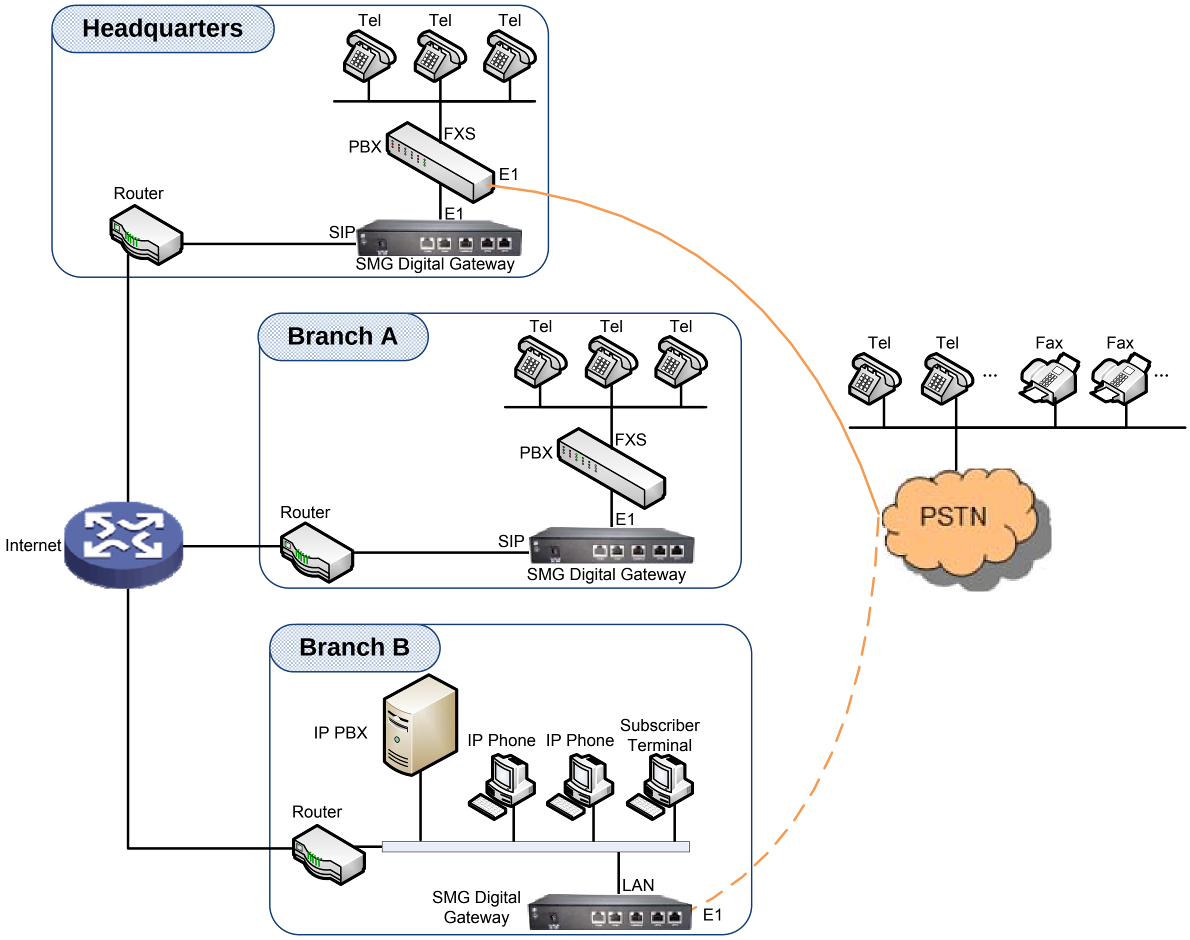


Figure 1-1 Typical Application

1.2 Feature List

Basic Features	Description	
PSTN Call	Call initiated from PSTN to a designated SIP trunk, via routing and number manipulation.	
IP Call	Call initiated from IP to a designated PCM 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.	
PSTN/ VoIP Routing	Routing path: from IP to PSTN or from PSTN to IP.	
Fax	Multiple fax parameters: fax mode, maximum fax rate, fax train mode, error correction mode, etc.	
Echo Cancellation	Provides the echo cancellation feature for a call conversation.	
Signaling & Protocol	**Description**	
ISDN	ISDN User Side, ISDN Network Side	
SS1	SS1 Signaling	
SIP Signaling	Supported protocol: SIP V1.0/2.0, RFC3261	
Voice	CODEC	G.711A, G.711U, G.729, G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K)
	DTMF Mode	RFC2833, SIP INFO, INBAND, RFC2833+Signaling, In-band+Signaling
Fax	Fax Mode	T.38, Pass-Through
	Baud Rate	14400bps, 9600bps, 4800bps
Network	**Description**	
Network Protocol	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN	
Static IP	IP address modification support	
DNS	Domain Name Service support	
Security	**Description**	
Admin Authentication	Support admin authentication to guarantee the resource and data security	
Maintain & Upgrade	**Description**	
WEB Configuration	Support of configurations through the WEB user interface	
Language	Chinese, English	
Software Upgrade	Support of user interface, gateway service, kernel and firmware upgrades based on WEB	
Tracking Test	Support of Ping and Tracert tests based on WEB	

SysLog Type	Three options available: ERROR, WARNING, INFO

1.3 Hardware Description

The SMG digital gateway integrates embedded LINUX system within the POWERPC+DSP hardware architecture. It has 1/2 E1/T1 ports and 2 100Mb/s Ethernet ports (LAN1 and LAN2) on the chassis.

See below figures for SMG2030L series appearance：

Figure 1-2 Front View

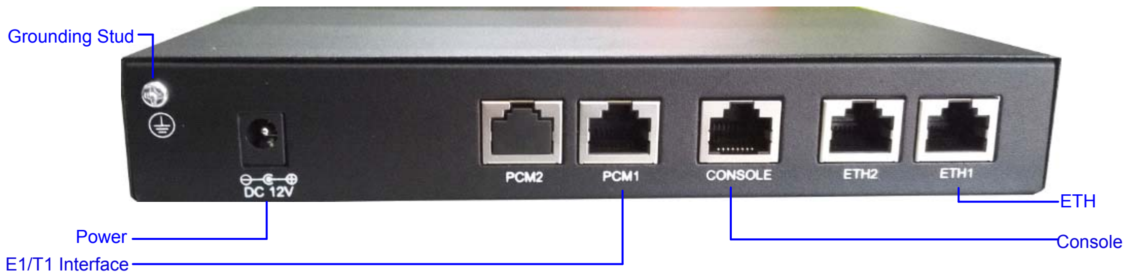


Figure 1-3 Rear View

Figure 1-4 Left View

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

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

Console Port	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-5 for signal definition)
	Data Bits: 8 bits
	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
External Power Supply Interface	Voltage: 12V, positive inside and negative outside; Current: ≥3A.
Button	**Description**
Reset Button	Restore the gateway to factory settings.
LED	**Description**
Power Indicator	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
Run Indicator	Indicates the running status. For more details, refer to 1.4 Alarm Info.
Alarm Indicator	Alarms the device malfunction. For more details, refer to 1.4 Alarm Info.
Link Indicator	The green LED on the left of LAN, indicating the network connection status.
ACT Indicator	The orange LED on the right of LAN, whose flashing tells data are being transmitted.
E1 Indicators	The green LED on the right of E1 interface lights up and keeps on after the E1 module is successfully synchronized.

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

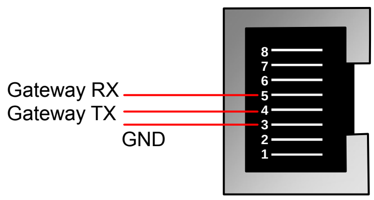


Figure 1-5 Console Port Signal Definition

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

1.4 Alarm Info

The SMG digital 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 E 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 SMG digital gateway in the shortest time.

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

- SMG Series Digital Gateway *1
- External 12V Power Adapter *1
- Warranty Card *1
- Installation Manual *1

Step 2: 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.

Step 3: Connect the network cable.

Step 4: Connect the E1/T1 trunk. Connect the E1/T1 interface of the digital gateway to that of the remote device by E1/T1 trunk. After connection, check if the synchronization indicator (green LED) is lit and keeps on, which indicates that the E1/T1 trunk is well connected and the E1/T1 module is successfully synchronized.

For the 75Ω-unbalanced coaxial cable, in consideration of various line conditions, each PCM on the digital gateway is equipped with two grounding jumpers which respectively control the grounding of the transmitting and the receiving end. Under normal condition, that is, the chassis of the gateway is well grounded, the grounding jumpers at the receiving end should be disconnected and the ones at the transmitting end should be short-circuited. This configuration is the factory default setting and applicable in most situations so that there is usually no need to change it. For the 120Ω-balanced twisted pair cable, the grounding jumpers at both ends should be disconnected.

You can construct an E1 trunk according to Figure 2-1. Prevent reverse connection of the transmitting and receiving lines. The state of the receiving line can be checked by the synchronization indicator (green LED) of the E1 interface. When the receiving line is in a normal state, the indicator is lit and keeps on. If the indicator is off or flashing, it means that the connection of the receiving line may probably be reversed. However, the state of the transmitting line can only be examined by the opposite terminal. The synchronization indicator starts working only after the device is powered on and successfully initialized.

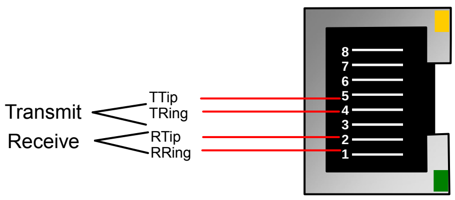


Figure 2-1 Pin Layout for E1 Interface

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 SMG digital gateway in the browser to go to the WEB interface. The original username and password of the gateway are both 'admin'. For detailed instructions about login, refer to 3.1 System Login. We suggest you change the initial username and password via 'System Tools → Change Password' on the WEB interface as soon as possible after your first login. For detailed instructions about changing the password, refer to 3.11.18 Change Password. After changing the password, you are required to log in again.

Step 6: Modify IP address of the gateway.

You can modify the IP address of the gateway via 'System Tools → Network' on the WEB interface to put it within your company's LAN. Refer to 3.11.1 Network for detailed instructions about IP modification. After changing the IP address, you shall log in the gateway again using your new IP address.

Step 7: Set PCM.

On your initial use of the SMG digital gateway, you shall enter the PCM interface and set the configuration items 'Signaling Protocol' and 'Interface'. These items must be in conformity with the physical connection. You may use the default values of other configuration items. Refer to 3.4.3 PCM for detailed instructions about PCM Settings.

Note: You shall restart the service to validate the settings in this step. Refer to 3.11.20 Restart for detailed instructions.

Step 8: Configure signaling protocol parameters.

Further configure the signaling protocol you set in Step 7. Different protocols are configured on different interfaces. See below for detailed instructions.

- **ISDN User Side/Network Side:**

The configuration interface related to ISDN User Side/Network Side is ISDN. On your initial use of the SMG digital gateway, you may adopt the default value of the configuration items on this interface.

Note: After configuring the ISDN interface, you shall restart the service to validate the settings. Refer to 3.11.20 Restart for detailed instructions.

- **SS1:**

The configuration interface related to SS1 is SS1. On your initial use of the SMG digital gateway, you may adopt the default value of the configuration items on this interface.

Note: After configuring the SS1 interface, you shall restart the service to validate the settings. Refer to 3.11.20 Restart for detailed instructions.

Step 9: Check the PSTN status.

After the configuration of signaling protocols, you can check the status of the PSTN trunks via 'Operation Info → PSTN Status'. Refer to 3.2.2 PSTN Status for detailed introductions. When Time Slot 0 shows 'Frame Synchronized', the signaling time slot is in the state of 'Signaling Channel' and all the other channels are 'Idle', it indicates the PCM is well configured. If Time Slot 0 or the signaling time slot shows 'Faulty' or the other channels are in the state of 'Unavailable', there may be errors in the signaling protocol configurations and we suggest you return to Step 9 for check.

Step 10: Set routing rules for calls.

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

Situation 1: IP → PSTN

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 remote SIP terminal 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**.

Step 2: Add the IP address of the remote SIP terminal 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.

Step 3: Add PCM into the corresponding PCM Group. Refer to 'PCM Settings → PCM Trunk Group' for detailed instructions. Select the PCM used for call conversation as 'PCM'. You may use the default values for the other configuration items.

Example: Provided the PCM used for call conversation is PCM[1]. Add **PCM Trunk Group 0**, check the checkbox before **PCM[1]** and keep the default values for the other configuration items.

Step 4: Add routing rules. Refer to 'Route Settings → IP→PSTN' for detailed instructions. Select the SIP trunk group set in Step 2 as 'Call Initiator' and the PCM trunk group 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 **PCM Trunk Group[0]** as **Call Destination.** Keep the default values for the other configuration items.

Step 5: Initiate a call from the SIP terminal configured in Step 1 to the IP address and port of the SMG digital gateway. Thus you can establish a call conversation via PCM[1] with the PSTN terminal. (Note: The format used for calling an IP address via SIP trunk is as follows: username@IP address, in which, 'username' is a called party number which conforms to the number-receiving rule of the remote device.)

Example: Provided the IP address of the SMG digital 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 terminal 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 PCM[1] to the number 123.

Situation 2: PSTN → IP

Step 1: Configure the called party numbers which are received from PSTN and will be processed by the gateway. Refer to 'Advanced Settings → Number-receiving Rule' for detailed instructions. Enter either a particular number or a string of 'x's to represent several random numbers. For example, 'xxx' denotes 3 random numbers. You may use the default value for 'Index'.

Example: Set **Index** to **99** and configure **Dial Rule** to **123**.

Step 2: Set the IP address of the SIP terminal to be called by the gateway. Refer to 'SIP Settings → SIP Trunk' for detailed instructions. Fill in 'Remote IP' and 'Remote Port' with the IP address and port of the SIP trunk. You may use the default values for the other configuration items.

Example: Provided the IP address of the SIP trunk to be called 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**.

Step 3: Add the IP address of the remote SIP terminal configured in Step 2 into the corresponding SIP trunk group. Refer to 'SIP Settings → SIP Trunk Group' for detailed instructions. Select the SIP trunk configured in Step 2 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.

Step 4: Add PCM into the corresponding PCM Group. Refer to 'PCM Settings → PCM Trunk Group' for detailed instructions. Select the PCM used for call conversation as 'PCM'. You may use the default values for the other configuration items.

Example: Provided the PCM used for call conversation is PCM[1]. Add **PCM Trunk Group 0**, check the checkbox before **PCM[1]** and keep the default values for the other configuration items.

Step 5: Add routing rules. Refer to ‘Route Settings → PSTN→IP’ for detailed instructions. Select the PCM trunk group set in Step 4 as ‘Call Initiator’ and the SIP trunk group set in Step 3 as ‘Call Destination’. You may use the default values for the other configuration items.

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

Step 6: Once PCM[1] receives a call from PSTN and the called party number conforms to the number-receiving rules set in Step 1, it can establish a call conversation with the remote SIP terminal via the gateway.

Example: Once PCM[1] receives a call from PSTN with the called party number 123, it will route the call to SIP Trunk 0 of the gateway.

Special Instructions:

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

Chapter 3 WEB Configuration

3.1 System Login

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

Figure 3-1 Login Interface

The gateway only serves one user, whose original username and password are both 'admin'. You can change the username and the password via 'System Tools → Change Password' on the WEB interface. For detailed instructions, refer to 3.11.18 Change Password.

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

Figure 3-2 Main Interface

3.2 Operation Info

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

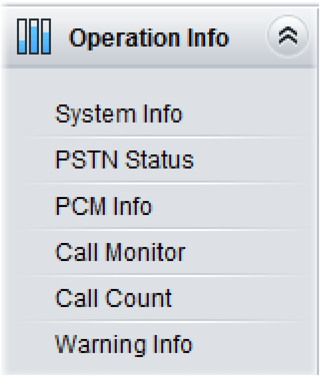


Figure 3-3 Operation Info

3.2.1 System Info

Figure 3-4 System Info Interface

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

Item	Description
MAC Address	MAC address of 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.
DNS Server	DNS server address of LAN 1 or LAN 2.

<table>
<tr><td>Receive Packets</td><td>The amount of receive packets after the gateway's startup, including three categories: All, Error and Drop.</td></tr>
<tr><td>Transmit Packets</td><td>The amount of transmit packets after the gateway's startup, including three categories: All, Error and Drop.</td></tr>
<tr><td>Current Speed</td><td>The current speed of data receiving and transmitting.</td></tr>
<tr><td>Work Mode</td><td>The work mode of the network, including five options: 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex and Disconnected.</td></tr>
<tr><td>Runtime</td><td>Time of the gateway keeping running normally after startup. This parameter updates every 2s.</td></tr>
<tr><td>Operating Mode</td><td>The operating mode of the gateway includes:
<table>
<tr><th>Operating Mode</th><th>Description</th></tr>
<tr><td>ISDN(User-side)</td><td>The current gateway is configured to be ISDN user-side..</td></tr>
<tr><td>ISDN(Network-side)</td><td>The current gateway is configured to be ISDN network-side.</td></tr>
<tr><td>SS1</td><td>The current gateway is configured to be SS1.</td></tr>
</table></td></tr>
<tr><td>CPU Temperature</td><td>Display the real time temperature of the CPU.</td></tr>
<tr><td>CPU Usage Rate</td><td>Display the real time usage rate of the CPU.</td></tr>
<tr><td>Current RTP Message Data</td><td>Display the receiving and sending information of the current RTP data.</td></tr>
<tr><td>DCMS Working Status</td><td>Display the connecting status of the gateway and DCMS.</td></tr>
<tr><td>Serial Number</td><td>Unique serial number of an SMG digital gateway.</td></tr>
<tr><td>WEB</td><td>Current version of the WEB interface.</td></tr>
<tr><td>Gateway</td><td>Current version of the gateway service.</td></tr>
<tr><td>Uboot</td><td>Current version of Uboot.</td></tr>
<tr><td>Kernel</td><td>Current version of the system kernel on the gateway.</td></tr>
<tr><td>Firmware</td><td>Current version of the firmware on the gateway.</td></tr>
</table>

3.2.2 PSTN Status

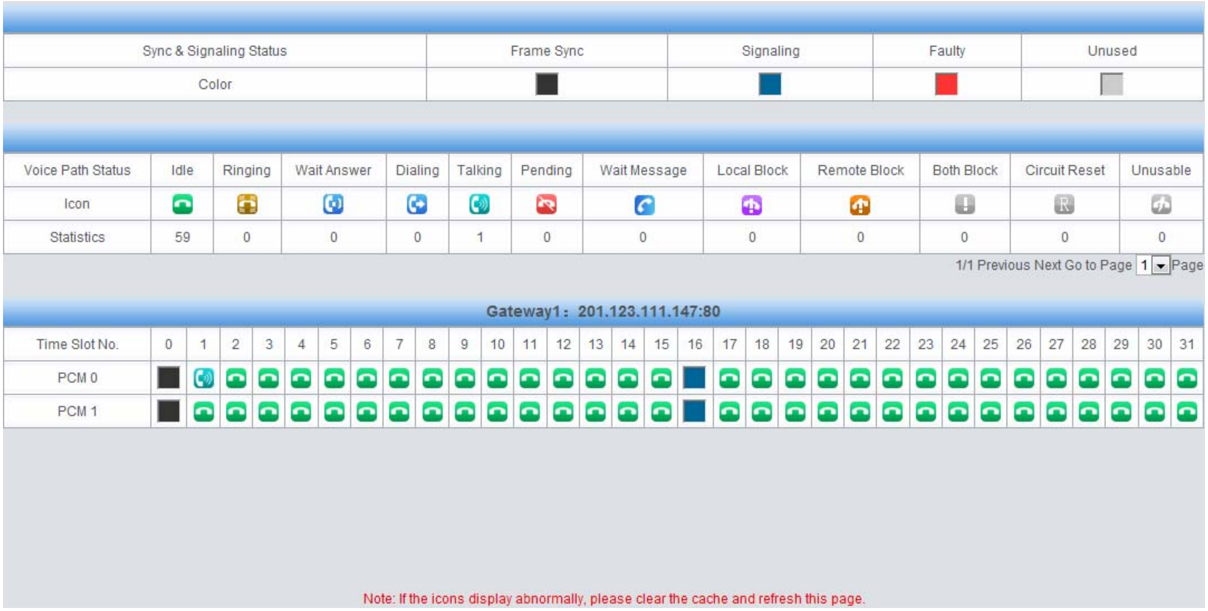


Figure 3-5 PSTN Status Interface for E1 Lines

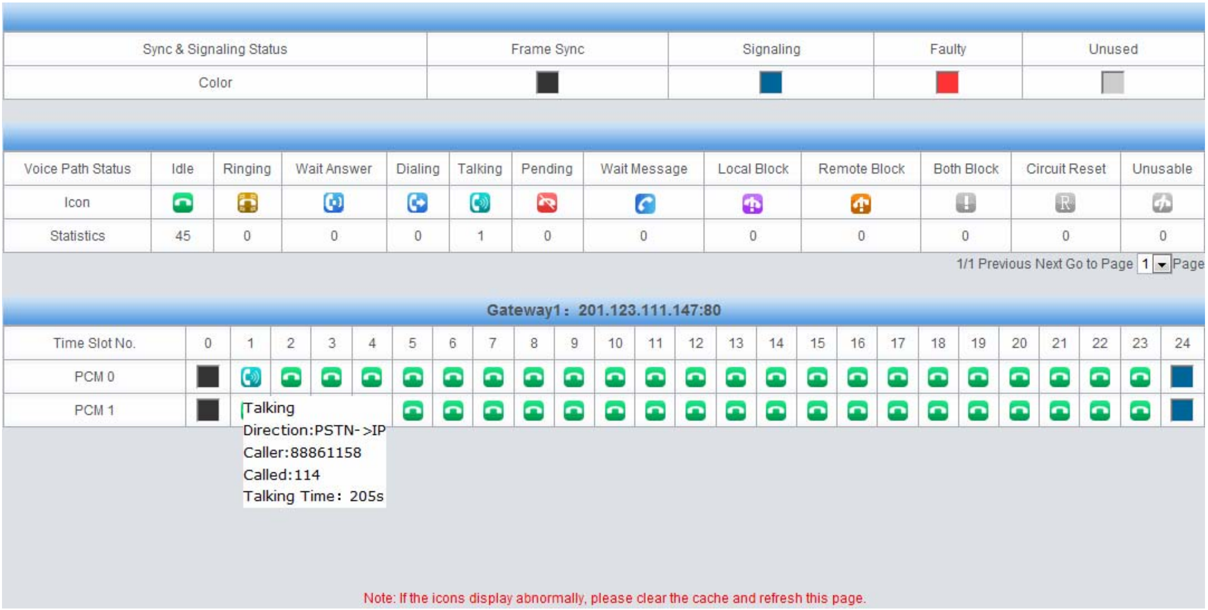


Figure 3-6 PSTN Status Interface for T1 Lines

See Figure 3-5 and Figure 3-6 for the PSTN status interface which shows the real-time status of each PCM on the gateway, including line synchronization, signaling link information and channel states.

Item	Description
Port	Serial number of the E1/T1 port on the device.
Time Slot No.	PCM time slot number in the port.
State	Displays the channel state in real time. You can move the mouse onto the channel state icon for detailed information about the channel and the call, such as: call direction, calling party number and called party number. ● For Time Slot 0, the channel state indicates the synchronization status of

E1/T1.

State	Color	Description
Frame Sync		Frame synchronization normal. The synchronization status is 0x0.
Faulty		Configuration errors or hardware failure. You can move the mouse onto the icon for the hexadecimal value for synchronization status which consists of 16 bits and bit 0 is the lowest valid bit. If the bit value is equal to 0, it indicates that the synchronization status is normal; if the bit value is equal to 1, see below for details: bit0=1: basic frame synchronization loss bit1=1: duration of the basic frame synchronization loss exceeds 100ms bit2=1: CAS re-synchronization bit3=1: CRC re-synchronization bit4=1: remote alarm indication bit5=1: signal alarm indication bit6=1: all-ones alarm signal of time slot 16 bit7=1: signal loss bit9=1: MF alarm from the remote end bit10=1: open circuit bit11=1: short circuit Other bits: reserved, all remain 0

- For the signaling time slot, the channel states include:

State	Color	Description
Signaling		For ISDN, this state indicates ‘multiple frames established’ or ‘timer recovery’. For SS1, this state indicates ‘time slot synchronization normal’.
Faulty		Configuration errors or hardware failure. For ISDN, this state indicates ‘TEI unassigned’, ‘assign awaiting TEI’, ‘establish awaiting TEI’, ‘TEI assigned’, ‘awaiting establishment ‘or ‘awaiting release’. For SS1, this state indicates ‘time slot synchronization abnormal’.
Unused		This state indicates the signaling time slot on this E1/T1 is not used.

- For the other channels, the channel states include:

State	Icon	Description
Unusable		The channel is unavailable.
Circuit Reset		The circuit is being reset.
Idle		The channel is available.

	Local Block	The channel is blocked by the local application program and cannot receive incoming calls.
	Remote Block	The channel is blocked by the specific circuit/circuit group blocking messages sent from the remote PBX and cannot make outgoing calls.
	Both Block	The channel is blocked by the local end so as not to receive incoming calls, meanwhile, it is blocked by the remote PBX so as not to make outgoing calls either.
	Wait Answer	The channel receives the ringback tone and is waiting for the called party to pick up the phone.
	Ringing	The channel is in the ringing state.
	Talking	The channel is in a conversation.
	Pending	The channel is in the pending state
	Dialing	The channel is dialing.
	Wait Message	The channel is waiting for the message from remote PBX.
Statistics	The total amount of the channels for the corresponding status.	

Note: The gateway provides the fuzzy search feature on this interface. After you click any characters on Figure 3-5, Figure 3-6, 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 3-7, after we input the character 114 to the search box, and click the ***Search*** button, the gateway does a fuzzy search and locates that the ongoing call whose CalledID contains the character 114 occurs on Time Slot No. 1 of PCM 0.

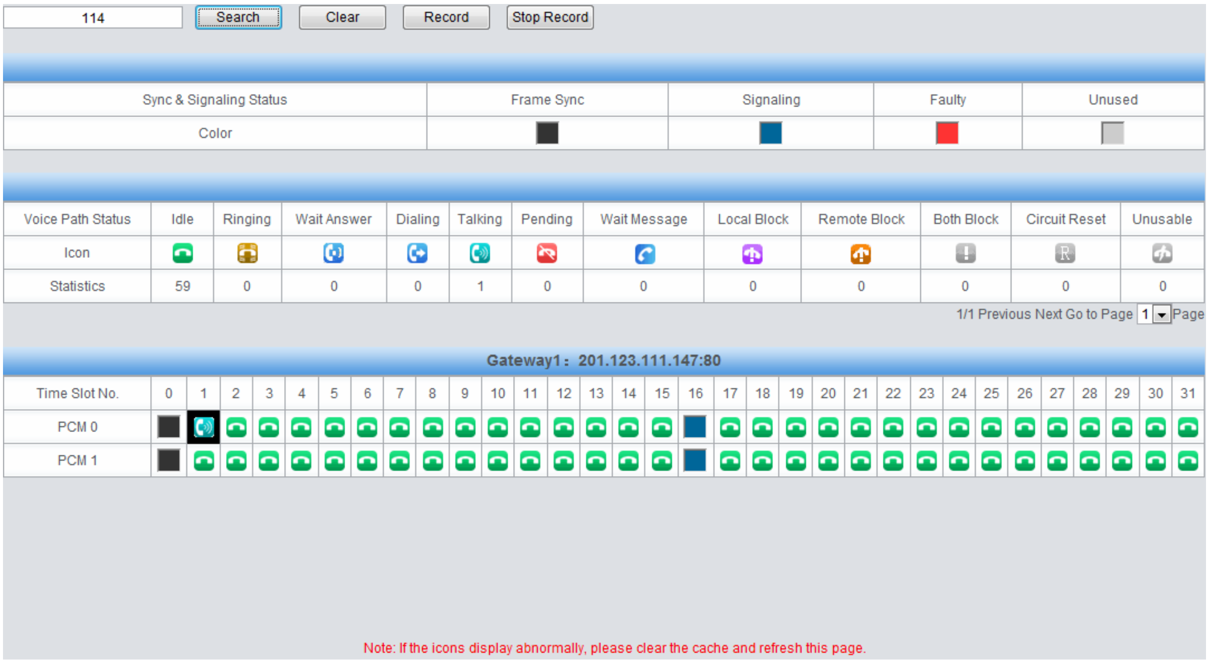


Figure 3-7 Search Calls

Note: Click ***Record*** to start recording on the matched channel. If more than one channel match a condition, only the channel with the largest number among them will be recorded.

3.2.3 PCM Info

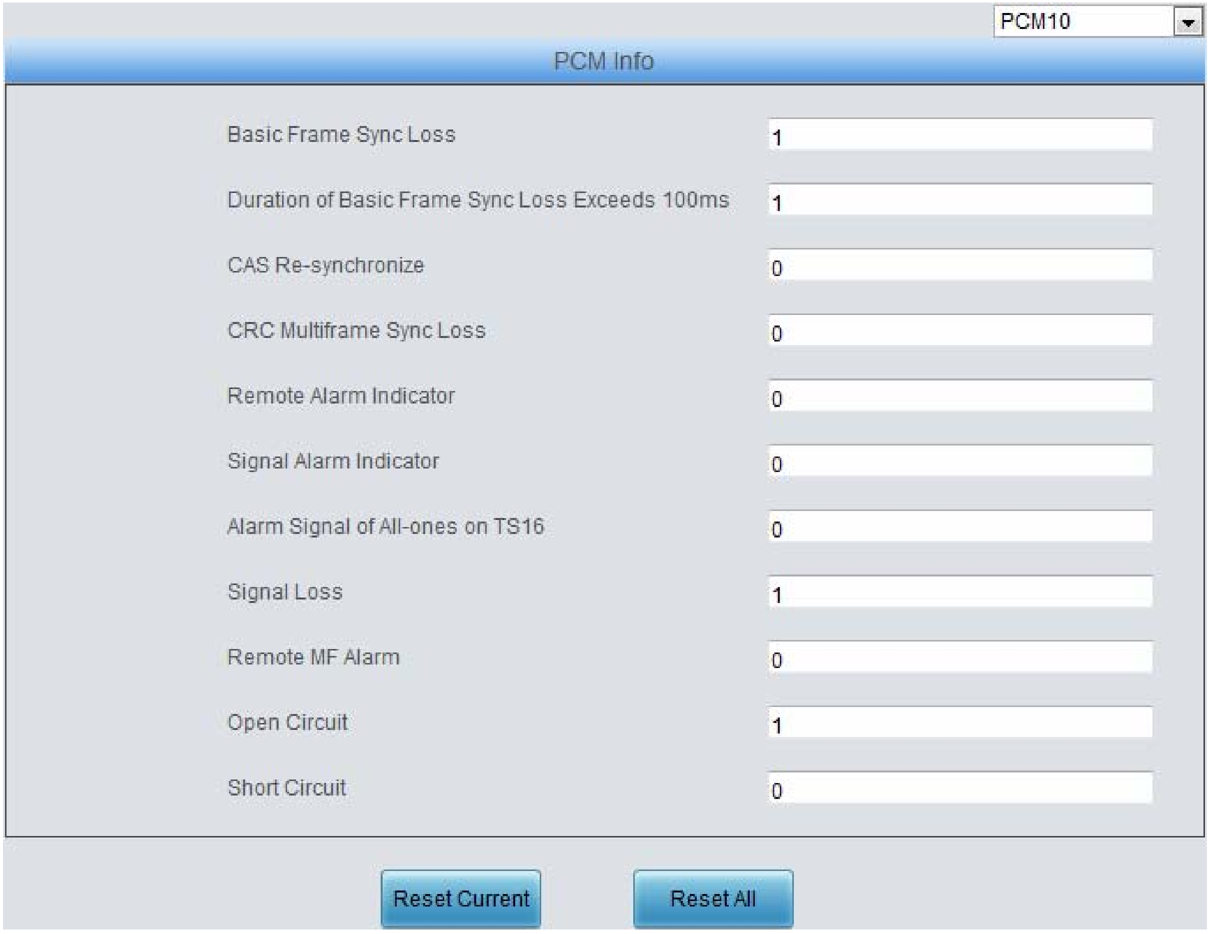


Figure 3-8 PCM Info Interface

See Figure 3-8 for the PCM Info interface. It displays the detailed information of E1 lines, facilitating the check on whether the PCM line is stable as well as the troubleshooting. Select a PCM channel via the drop down list on the right top corner. The statistics counters will add 1 each time once the alarm occurs.

3.2.4 Call Monitor

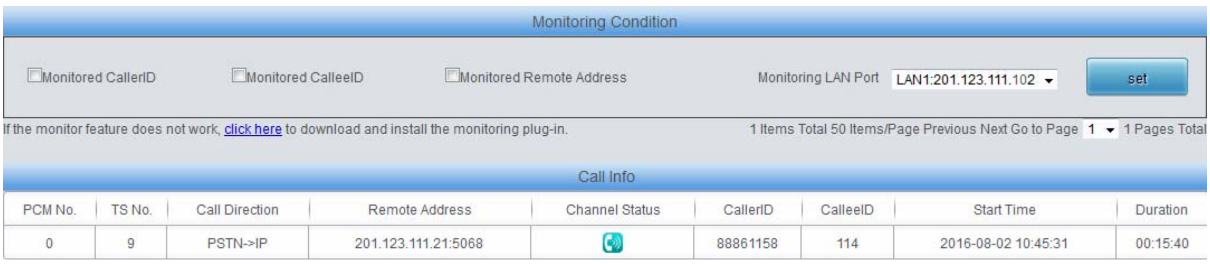


Figure 3-9 Call Monitor Interface

See Figure 3-9 for the call monitor Interface. Here you can set a condition for call monitoring. For example, as shown in Figure 3-9, set the CalleeID 114 as the monitoring condition, and after you click the ***Set*** button, all the calls containing the CalleeID 114 will display in the Call Info list. The table below explains the items shown in Figure 3-9.

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.
PCM No.	The number of the PCM, which starts from 0.
TS No.	PCM time slot number in the port.
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 the monitoring plug-in, click the icon and you will see a prompt asking you to set the security level. Follow the instructions to configure the IE explorer: Open it and click 'Tools > Internet Options >Security Tab'; then click 'Custom Level' and enable 'Initialize and script ActiveX controls not marked as safe for scripting'. If there is a shadow showing under the icon, such as '', it means the monitoring goes successful. Click the icon again to cancel the monitoring.

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

3.2.5 Call Count

Incoming SIP Call Statistics

SIP Index	Description	SIP Trunk Address	Current	Sum	Connection Rate	Answering Rate	Average Call Length (s)	INVITE(Times/s)
1	default	201.123.112.80	0	0	--	--	0	0

Outgoing SIP Call Statistics

SIP Index	Description	SIP Trunk Address	Current	Sum	Connection Rate	Answering Rate	Average Call Length (s)
1	default	201.123.112.80	0	0	--	--	0

PSTN Call Statistics

Trunk No.	Signaling Type	Current Number of IP->PSTN	Sum	Connection Rate	Answering Rate	Current Number of PSTN->IP	Sum	Connection Rate	Answering Rate
0	SS7-ISUP	0	0	--	--	0	0	--	--
1	SS7-ISUP	0	0	--	--	0	0	--	--
2	SS7-ISUP	0	0	--	--	0	0	--	--
3	SS7-ISUP	0	0	--	--	0	0	--	--
Total	---	0	0	--	--	0	0	--	--

Statistics on IP->PSTN Release Cause

Release Cause	Normal Disconnection	Cancelled	Busy	No Answer	Route Failed	No Idle Resource	Unallocated Number	Rejected	Unspecified	Failed	Others
Amount	0	0	0	0	0	0	0	0	0	0	0
Percentage	--	--	--	--	--	--	--	--	--	--	--

Statistics on PSTN->IP Release Cause

Release Reason	Normal Disconnection	Cancelled	Busy	No Answer	Route Failed	No Idle Resource	Failed	Others
Number	0	0	0	0	0	0	0	0
Percentage	--	--	--	--	--	--	--	--

Figure 3-10 Call Count Interface

See Figure 3-10 for the call count Interface. The above list shows the detailed information about all the calls counted from the startup of the gateway service to the latest open or refresh of this interface. This interface includes three parts: PSTN Call Statistics, Statistics on PSTN Release Cause and Statistics on Sip Release Cause. You can click ***Reset*** to count the call information again, click ***Download*** to download all the call logs and ISDN logs. The table below explains the items shown in Figure 3-10.

Item	Description
SIP Index	The index of the SIP trunk.
Description	More information about each SIP trunk group.
SIP Trunk Address	Address of the SIP trunk, i.e. the IP address or domain name of the remote SIP terminal which will establish a call conversation with the gateway.
Current	The number of the current incoming/outgoing SIP calls.
Sum	The total number of the incoming SIP calls/ outgoing SIP calls/ IP→ PSTN calls/ PSTN→ IP calls.
Connection Rate	The percentage of successful calls to total calls by all method. The call methods include SIP Incoming Call, SIP Outgoing Call, IP→ PSTN call and PSTN→ IP call.
Answering Rate	The percentage of answered calls to total calls by all methods. The call methods include SIP Incoming Call, SIP Outgoing Call, IP→ PSTN call and PSTN→ IP call.
Average Call Length	The average call length for all connected calls.

INVITE	The number of the invite messages received per second.
Trunk No.	The number of the PCM trunk, numbered from 0
Signaling Type	The signaling protocol applied on the digital trunk, including: ISDN User Side, ISDN Network Side and SS1.
Current Number of IP→PSTN	The number of current calls from IP to PSTN.
Current Number of PSTN →IP	The number of current calls from PSTN to IP.
Total	Total number and connection rate of calls on all available trunks
Release Cause	Reason to release the call.
Normal Disconnection	Total number of the calls which are normally cleared.
Cancelled	Total number of the calls which are cancelled by the calling party.
Busy	Total number of the calls which fail as the called party has been occupied and replies a busy message.
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.
Routing Failed	Total number of the calls which fail because no routing rules are matched.
No Idle Resource	Total number of the calls which fail because no voice channel is available.
Unallocated Number	Total number of the calls which fail as the called party number is unallocated.
Rejected	Total number of the calls which fail as the called party replies a rejection message.
Unspecified	Total number of the calls which fail as the called party number is normal but unspecified.
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.
Others	Total number of the calls which fail due to other unknown reasons.
Percentage	The percentage of the calls with a release cause to total calls.

3.2.6 Warning Info

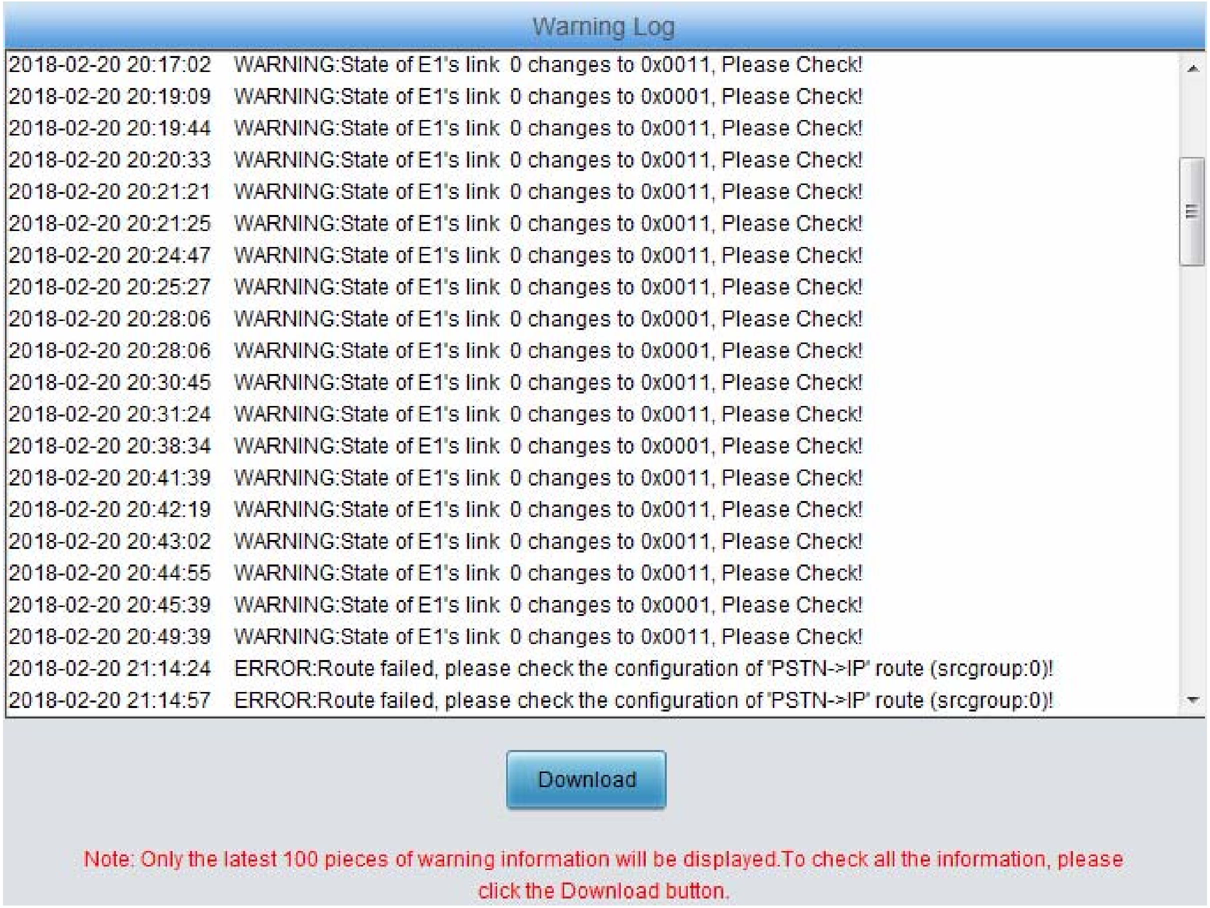


Figure 3-11 Warning Information Interface

See Figure 3-11 for the Warning Information interface. All the warning information will be output and displayed on this interface.

3.3 SIP Settings

SIP Settings includes five parts: ***SIP***, ***SIP Trunk***, **SIP Register**, ***SIP Account***, ***SIP Trunk Group*** and ***Media***. See Figure 3-12. ***SIP*** is used to configure the general SIP parameters; ***SIP Trunk*** is used to set the basic and register information of the SIP trunk; ***SIP Register*** is used for the registration of SIP; ***SIP Account*** is used for registering SIP accounts to the SIP server; ***SIP Trunk Group*** is to manage SIP trunks by group; and ***Media*** is to set the RTP port and the payload type.

Figure 3-12 SIP Settings

3.3.1 SIP Settings

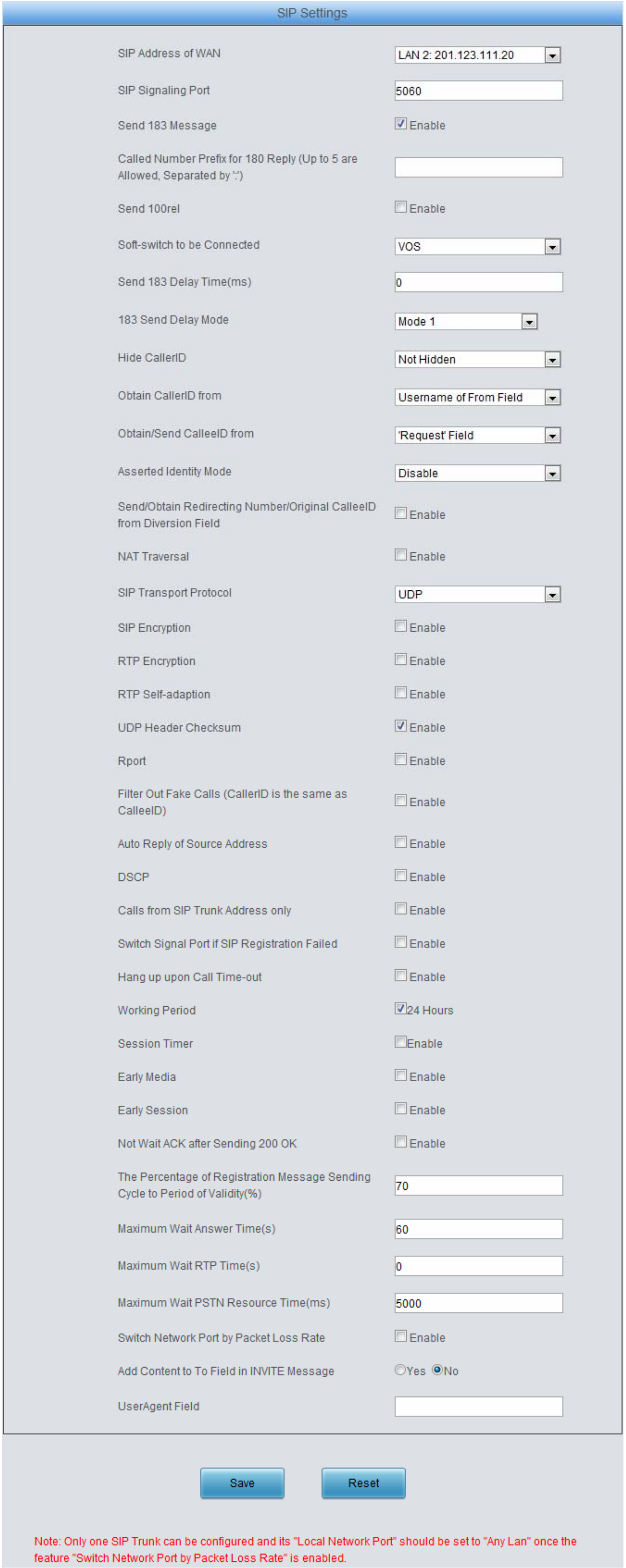

SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated by ',')
Send 100rel
Enable
Soft-switch to be Connected
VOS
Send 183 Delay Time(ms)
0
183 Send Delay Mode
Mode 1
Hide CallerID
Not Hidden
Obtain CallerID from
Username of From Field
Obtain/Send CalleeID from
'Request' Field
Asserted Identity Mode
Disable
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field
Enable
NAT Traversal
Enable
SIP Transport Protocol
UDP
SIP Encryption
Enable
RTP Encryption
Enable
RTP Self-adaption
Enable
UDP Header Checksum
Enable
Rport
Enable
Filter Out Fake Calls (CallerID is the same as CalleeID)
Enable
Auto Reply of Source Address
Enable
DSCP
Enable
Calls from SIP Trunk Address only
Enable
Switch Signal Port if SIP Registration Failed
Enable
Hang up upon Call Time-out
Enable
Working Period
24 Hours
Session Timer
Enable
Early Media
Enable
Early Session
Enable
Not Wait ACK after Sending 200 OK
Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%)
70
Maximum Wait Answer Time(s)
60
Maximum Wait RTP Time(s)
0
Maximum Wait PSTN Resource Time(ms)
5000
Switch Network Port by Packet Loss Rate
Enable
Add Content to To Field in INVITE Message
Yes
No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 3-13 SIP Settings Interface

See Figure 3-13 for the SIP settings interface where you can configure the general SIP parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-13.

Item	Description
SIP Address of WAN	IP address of WAN for SIP signaling, using LAN 1 by default.
SIP Signaling Port	Monitoring port of SIP signaling. Range of value: 2000~65535, with the default value of 5060. **Note:** The value range of this configuration item and that of the RTP port set in Media Settings cannot be overlapped.
Send 183 Message	Sets whether to send the 183 message instead of 180 to respond to the ringing tone when the SIP end serves as the called party. By default this feature is enabled.
Called Number Prefix for 180 Reply	Once the feature “Send 183 Message” is enabled, the gateway will reply the 180 message to those calls which have the calleeID with the designated prefix; otherwise, it will reply the 183 message. By default, the value is null, that is, replying the 183 message to all calls. Up to 5 prefixes are allowed to fill in this item, which are separated by ':'
Send 100rel	Sets whether to send the 100rel field, with the default value of disabled.
Soft-switch to be Connected	Sets the soft telephony device which will be connected to the gateway, including Others and VOS two options, with the default value of *Others*.
Send 183 Delay Time	Sets the delay time for sending the 183 message. Range of value: 0~10000, with the default value of 0. **Note:** It is valid only when the configuration item Soft-switch to be Connected is set to VOS.
183 Send Delay Mode	Sets the delay mode for sending the 183 message, including two options: Mode 1 and Mode 2, with the default value of Mode 1. Mode 1: The PSTN side will send the IAM message and wait for the ACM message once it receives an Invite message from vos. If the ACM message isn’t received within the preset-time, the SIP side will reply the 183 message; if the PSTN side receives the ACM message later, the SIP side will send the 183 message once again. If the ACM message is received within the preset-time, the SIP side will reply the 183 message only once. Mode 2: The SIP side will send the 183 message only once upon timeout; it won’t send the 183 message if the ACM message is received within the overtime. **Note:** It is valid only when the configuration item *Soft-switch to be Connected* is set to VOS.
Hide CallerID	Sets whether to hide the CallerID, with the default value of *Not Hidden*.
Obtain CallerID from	There are two optional ways to obtain the calling party number: from Username of “From” Field or from Displayname of “From” Field. The default value is from *Username of “From” Field*.

Obtain/Send CalleeID from	There are two optional ways to obtain or send the called party number: from "To" Field or from "Request" Field. The default value is from "*Request" Field*.
Asserted Identity Mode	Sets whether to have the invite message include some header information, two options available now: P-Asserted-Identity and P-Preferred-Identity. The default value is *disabled*.
Number in From Field not Manipulated	Once this feature is enabled, the callerID in the From field will not be manipulated, with the default value of *disabled*. **Note:** It is valid only when the configuration item Asserted Identity Mode is enabled.
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field	Sets whether to enable the feature of sending or obtaining the Redirecting Number/Original CalleeID from Diversion Field. By default, the feature is disabled.
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*.
SIP Transport Protocol	There are two modes *UDP* and *TCP* available for running the SIP protocol. The default value is *UDP*.
SIP Encryption	Once this feature is enabled, you can encrypt the SIP signal following selecting an encryption criterion and setting a key. By default it is *disabled*.
Encryption Criterion	The criterion used to encrypt the SIP signal. At present only VOS1.1 is supported.
Key	The key to encrypt the SIP signal.
RTP Encryption	Once this feature is enabled, you can encrypt the RTP package. By default it is *disabled*.
RTP Self-adaption	When this feature is enabled, the RTP reception address or port carried by the signaling message from the remote end, if not consistent with the actual state, will be updated to the actual RTP reception address or port. By default, this feature is *disabled*.
UDP Header Checksum	When this feature is enabled, the gateway will automatically calculate the check sum of the UDP header during RTP transmission.
Rport	When this feature is enabled, a corresponding Rport field will be added to the Via message of SIP. By default, it is *disabled*.

Filter Out Fake Calls (CallerID is the same as CalleeID)	Once this feature is enabled, those outgoing calls from PSTN whose callerID is the same as calleeID will be forbidden. The default value 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*.
DSCP	Sets whether to enable the DSCP differentiated services code point. By default, it is *disabled*.
Voice Media	Sets the priority of the voice media for DSCP. The voice media with a bigger value has a higher priority. The value range is 0~63, with the default value of *46*.
Signal Control	Sets the priority of the signal control for DSCP. The signal control with a bigger value has a higher priority. The value range is 0~63, with the default value of *26*.
Calls from SIP Trunk Address only	Once this feature is enabled, the gateway will only accept the calls from the IP addresses set in SIP Settings → SIP Trunk. By default, it is *disabled*.
Switch Signal Port if SIP Registration Failed	If the SIP registration fails, the SIP signaling port N will switch to N+1 for a new registration. It will continue until the registration succeeds.
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).
Session Timer	Sets whether to enable the session refresh feature, with the default value of *disabled*. Once this feature is enabled, you are required to enter the minimum time and the timeout value.
Minimum Time	Sets the minimum time for refreshing the session. Value of range: 90~65535, with the default value of *150*.
Timeout	Sets the timeout value for refreshing the session. The value cannot be less than that of Minimum Time, with the default value of *600*.
Early Media	Once this feature is enabled, the P-Early-Media field will be included in the Invite message. The default value is *disabled*.
Early Session	Once this feature is enabled, the early-session field will be included in the Invite message. The default value is *disabled*.
Not Wait ACK after Sending 200 OK	Once this feature is enabled, the gateway does not need to wait the ACK message after sending the 200OK message. The default value is *disabled*.
The Percentage of Registration Message Sending Cycle to Period of Validity	Sets the percentage of the sending cycle of the SIP registration message to the validity period. Value of range: 1~200, with the default value of *70*.
Maximum Wait Answer Time	Sets the maximum time for the SIP channel to wait for the answer from the called party of the outgoing call it initiates. If the call is not answered within the specified time period, it will be canceled by the channel automatically. The default value is *60*, calculated by s.

Maximum Wait RTP Time	Sets the maximum time for the SIP channel to wait for the RTP packet. If no RTP packet is received within the specified time period, the channel will enter the pending state automatically and release the call. The default value is *0*, calculated by s.
Maximum Wait PSTN Resource Time	Sets the maximum wait time to search the idle PSTN resource for the incoming call from IP. The call will be failed if no channel is found during this time. The value range is 0~10000, calculated by ms, with the default value of *5000*.
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*.
Add Content to To Field in INVITE Message	Once this feature is enabled, “user=phone” will be added to the TO field of the INVITE message. The default value is *disabled*.
Add Content	Sets the content to add to the TO field.
UserAgent Field	Sets the content of the UserAgent field. Currently, it only supports the English uppercase and lowercase letters.

3.3.2 SIP Trunk

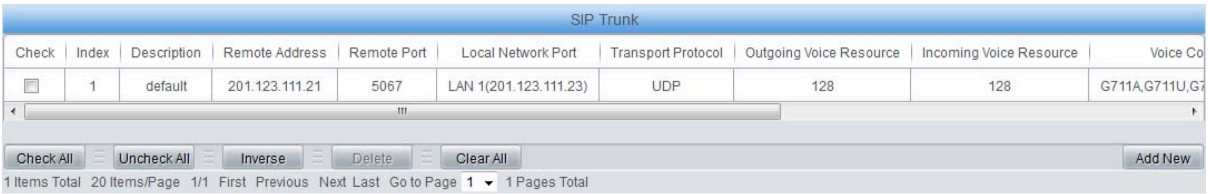


Figure 3-14 SIP Trunk Settings Interface

See Figure 3-14 for the SIP trunk settings interface. A new SIP trunk can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-15 for the SIP trunk adding interface.

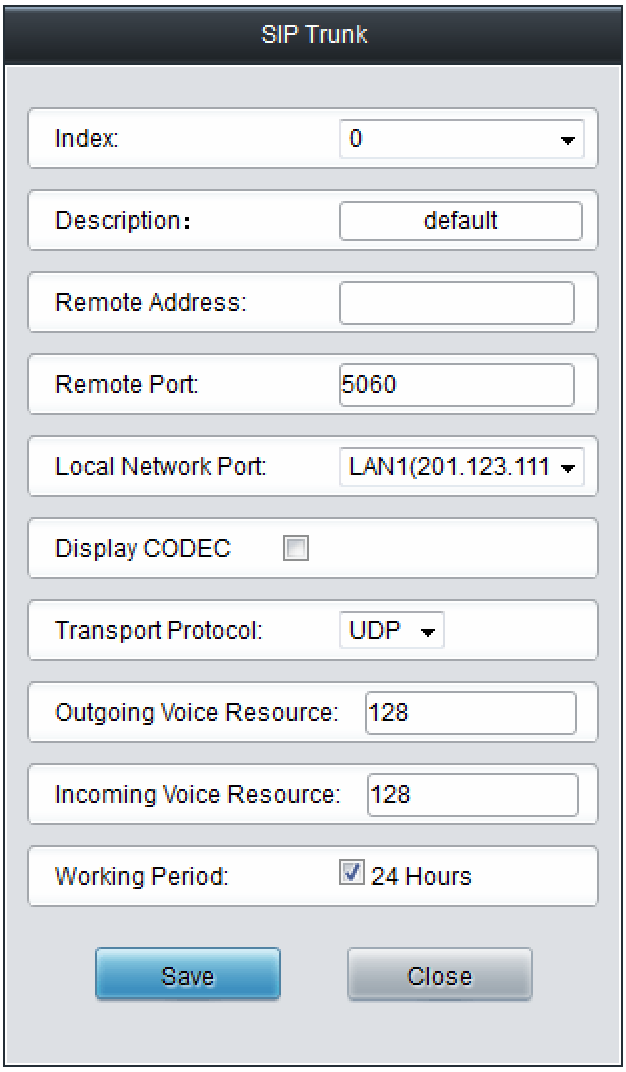


Figure 3-15 Add New SIP Trunk

The table below explains the items shown in Figure 3-15.

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

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).
CODEC	Supported CODECs and their corresponding priorities for the SIP trunk to establish a call conversation. The table below explains the sub-items: **Sub-item** — **Description** *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*, *G729* *G722*, *G723*, *iLBC*, *AMR*, *SILK(16K)*, *OPUS(16K)*, *SILK(8K)*, *OPUS(8K)*. See 3.3.6 Media Settings for the detailed parameters for each CODEC. The default CODEC for the SIP trunk is the same as that set in 3.3.6 Media Settings.

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

Click ***Modify*** in Figure 3-14 to modify a SIP trunk. See Figure 3-16 for the SIP trunk modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Trunk*** interface.

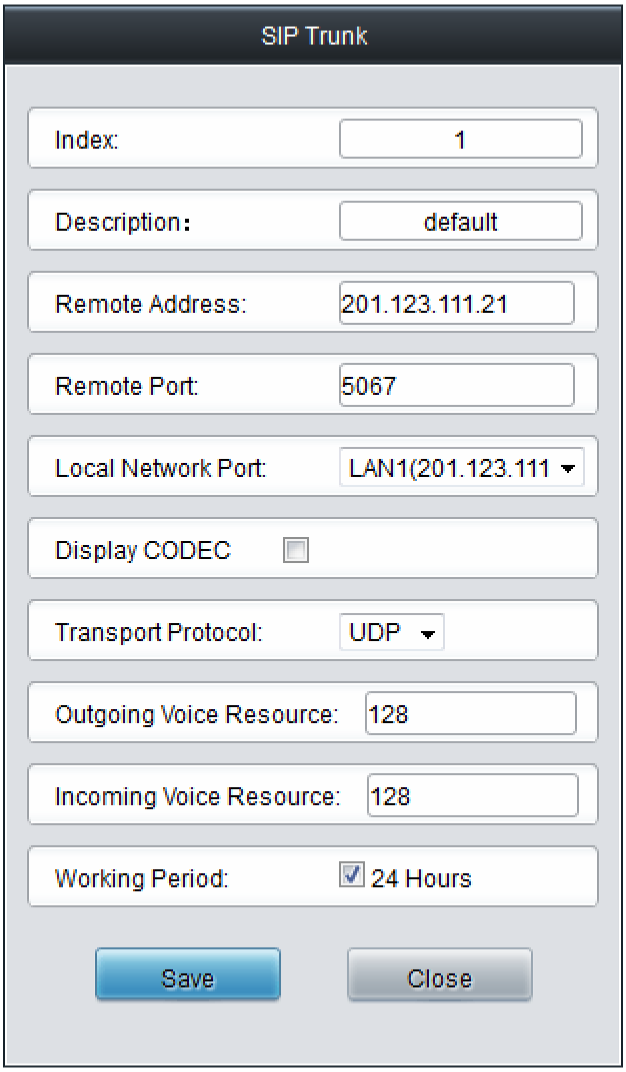


Figure 3-16 Modify SIP Trunk

To delete a SIP trunk, check the checkbox before the corresponding index in Figure 3-14 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP trunks at a time, click the ***Clear All*** button in Figure 3-14.

3.3.3 SIP Register

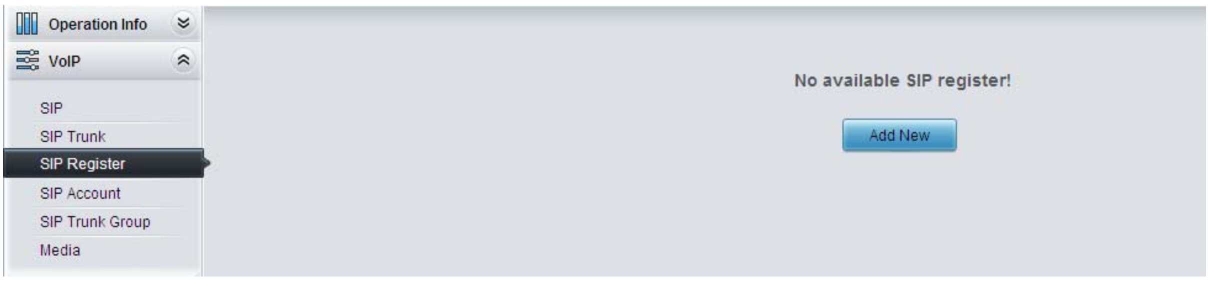


Figure 3-17 SIP Register Configuration Interface

See Figure 3-17 for the SIP Register Configuration interface. By default, there is no SIP register available on the gateway. Click ***Add New*** to add them manually. See Figure 3-18.

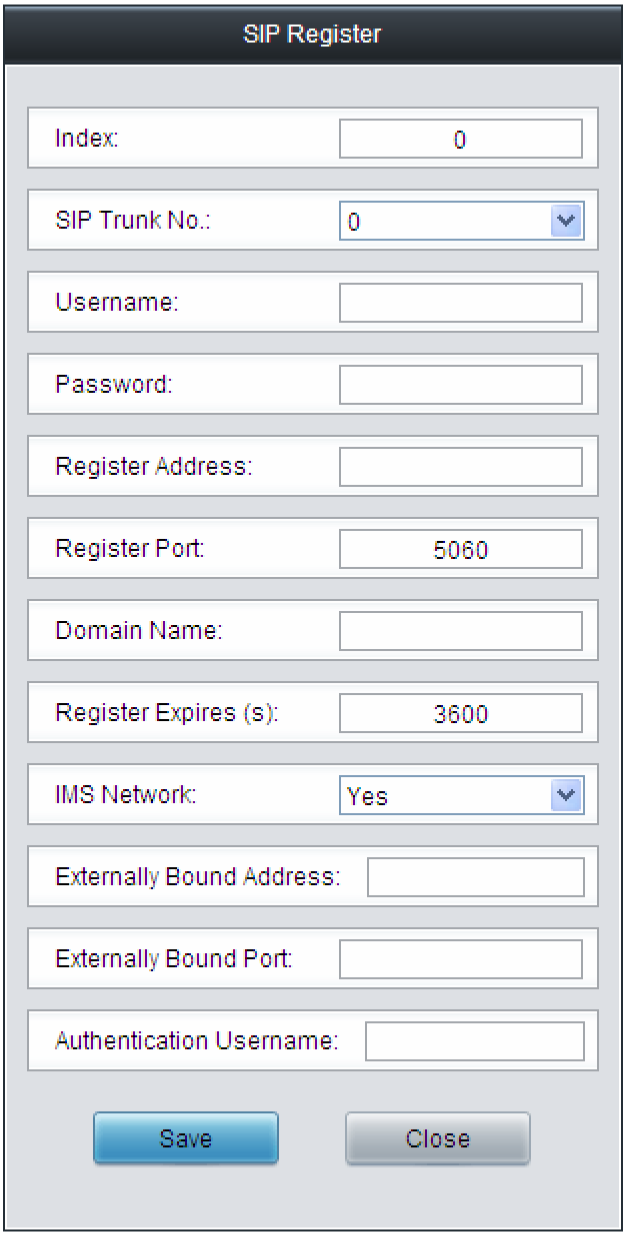


Figure 3-18 Add SIP Register Interface

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

Item	Description
Index	The unique index of each SIP register.
SIP Trunk No.	The number of the SIP trunk which registers to the SIP server.
Username	When the gateway initiates a call to SIP, this item corresponds to the username of SIP; when the gateway initiates a call to 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.
IMS Network	Once this feature is enabled, the gateway will send signaling messages to the corresponding externally bound address and port when it registers to the server. Only when this feature is *enabled* will these items **Externally Bound Address**, **Externally Bound Port** and **Authentication Username** be shown.
Externally Bound Address	Externally bound IP address for registration.
Externally Bound Port	Externally bound port for registration.
Authentication Username	Authentication username for registration.

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

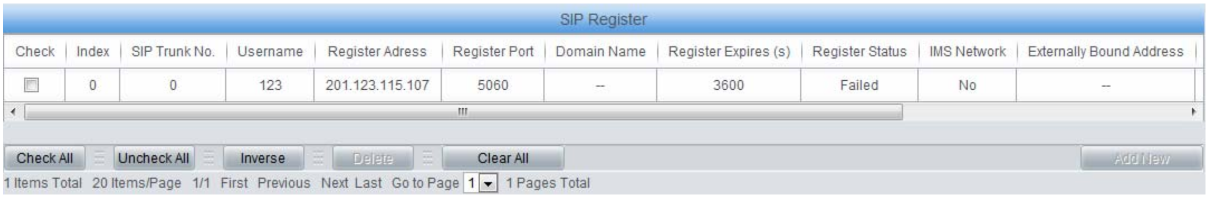


Figure 3-19 SIP Register Information List

Click ***Modify*** in Figure 3-19 to modify a SIP register. The configuration items on the SIP Register Modification Interface are the same as those on the ***Add New SIP Register*** interface.

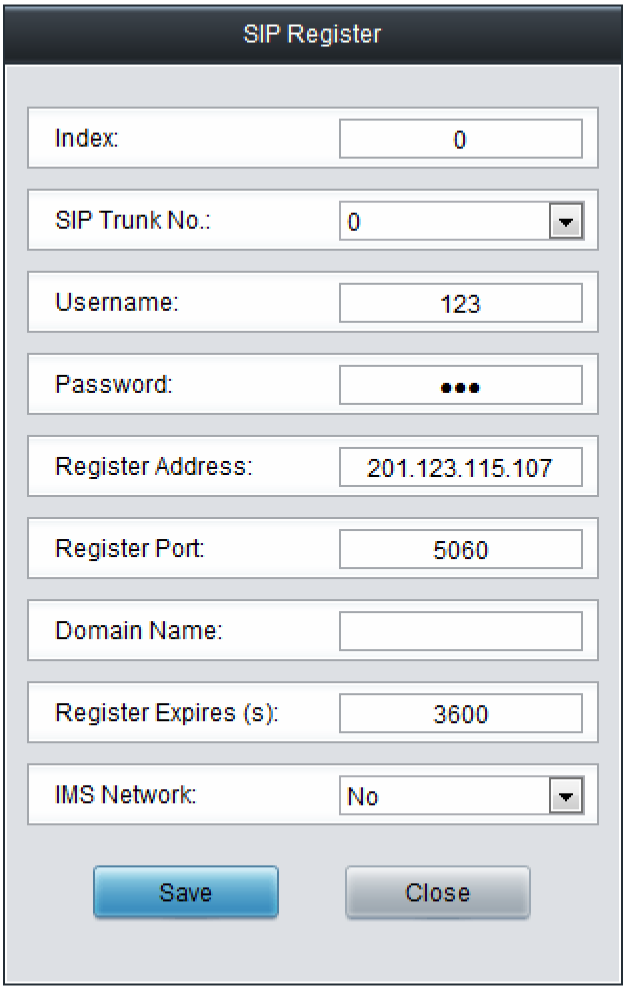


Figure 3-20 SIP Register Modification Interface

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

3.3.4 SIP Account

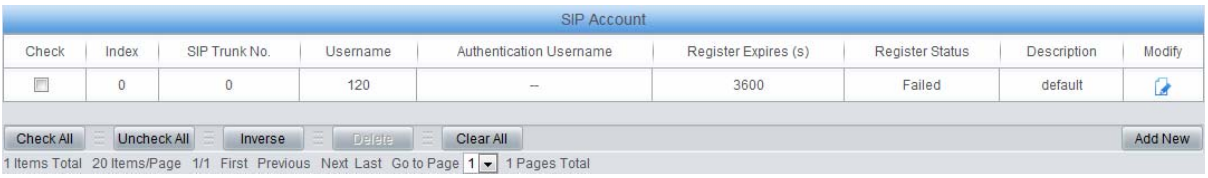


Figure 3-21 SIP Account Settings Interface

See Figure 3-21 for the SIP account settings interface. A new SIP account can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-22 for the SIP account adding interface.

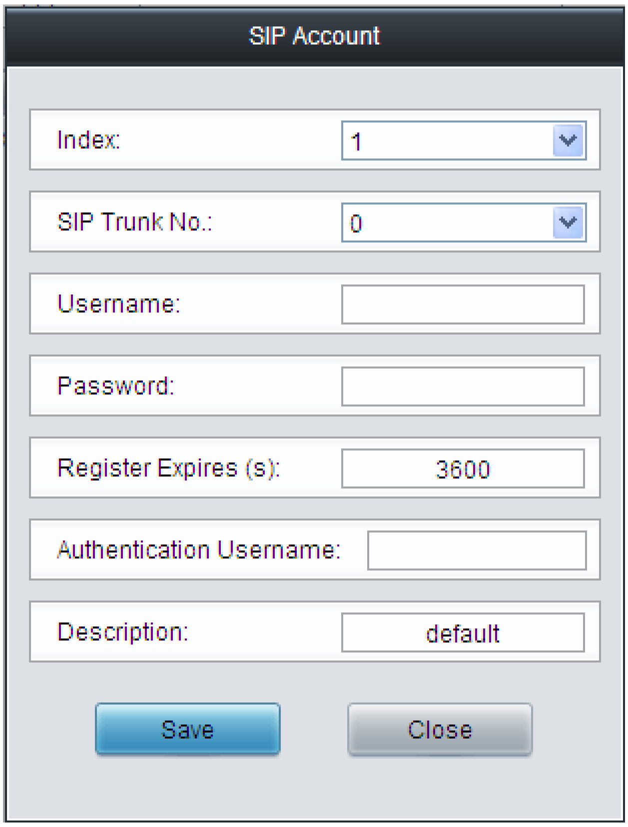


Figure 3-22 Add New SIP Account

The table below explains the items shown in above figures.

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

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

Click ***Modify*** in Figure 3-21 to modify a SIP account. See Figure 3-23 for the SIP account modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Account*** interface.

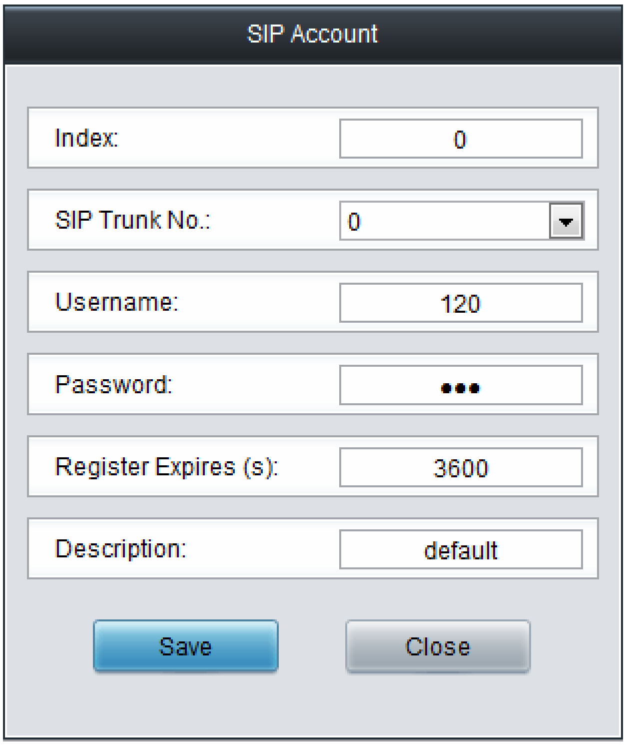


Figure 3-23 Modify SIP Account

To delete a SIP account, check the checkbox before the corresponding index in Figure 3-21 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP accounts at a time, click the ***Clear All*** button in Figure 3-21.

3.3.5 SIP Trunk Group

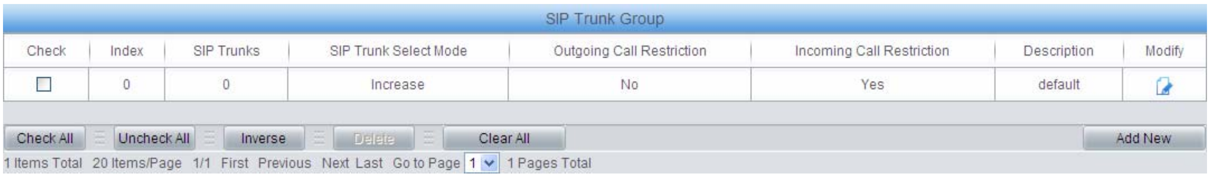


Figure 3-24 SIP Trunk Group Settings Interface

See Figure 3-24 for SIP trunk group settings interface. A new SIP trunk group can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-25 for the SIP trunk group adding interface.

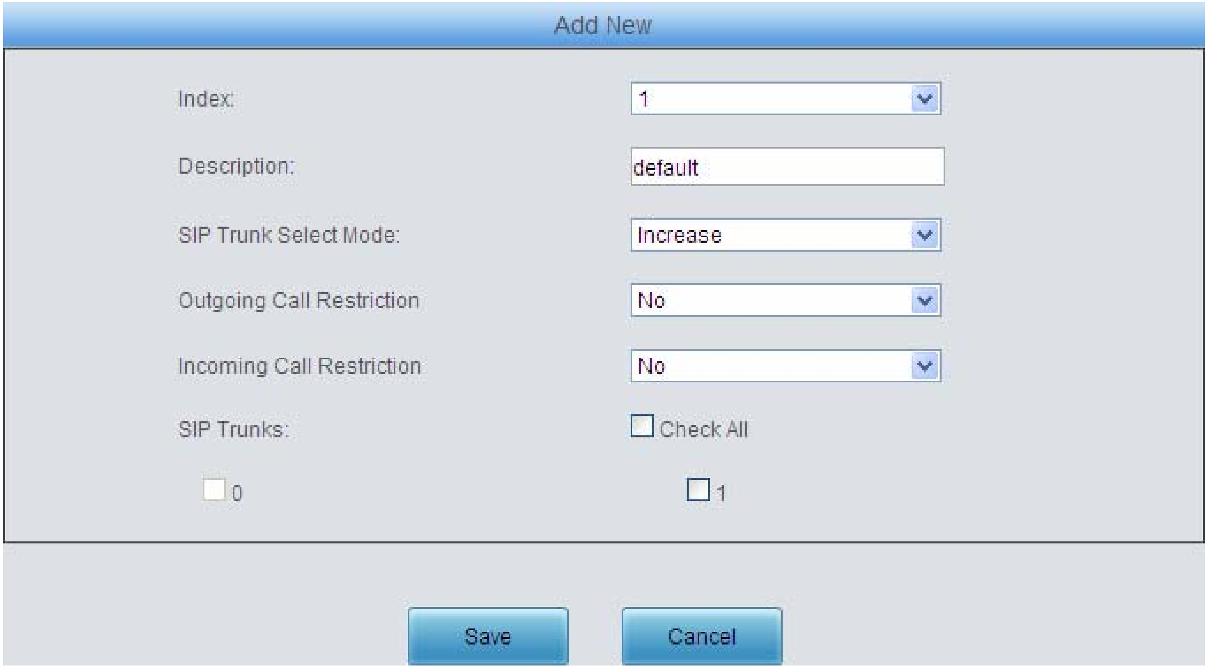


Figure 3-25 Add New SIP Trunk Group

The table below explains the items shown in Figure 3-25.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Index</td><td>The unique index of each SIP trunk group, which is mainly used in the configuration of routing rules and number manipulation rules to correspond to SIP trunk groups.</td></tr>
<tr><td>Description</td><td>More information about each SIP trunk group.</td></tr>
<tr><td>SIP Trunk Select Mode</td><td>When the SIP trunk group receives a call, it will choose a SIP trunk based on the select mode set by this configuration item to ring. The optional values and their corresponding meanings are described in the table below.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Increase</td><td>Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.</td></tr>
<tr><td>Decrease</td><td>Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.</td></tr>
<tr><td>Cyclic Increase</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from SIP Trunk N+1.</td></tr>
<tr><td>Cyclic Decrease</td><td>Provided SIP Trunk N is the available SIP trunk found last time. Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from SIP Trunk N-1.</td></tr>
</table></td></tr>
<tr><td>Outgoing/Incoming Call Restriction</td><td>Sets whether to restrict the number of channels for the outgoing/incoming calls, with the default value of No. If you select ‘Yes’, you are required to input the number of restricted channels.</td></tr>
<tr><td>SIP Trunks</td><td>The SIP trunks in the SIP trunk group. If the checkbox before a SIP trunk is grey, it indicates that the SIP trunk has been occupied. The ticked SIP trunks herein will be displayed in the column ‘SIP Trunks’ in Figure 3-24.</td></tr>
</table>

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

Click ***Modify*** in Figure 3-24 to modify a SIP trunk group. See Figure 3-26 for the SIP trunk group modification interface. The configuration items on this interface are the same as those on the ***Add New SIP Trunk Group*** interface.

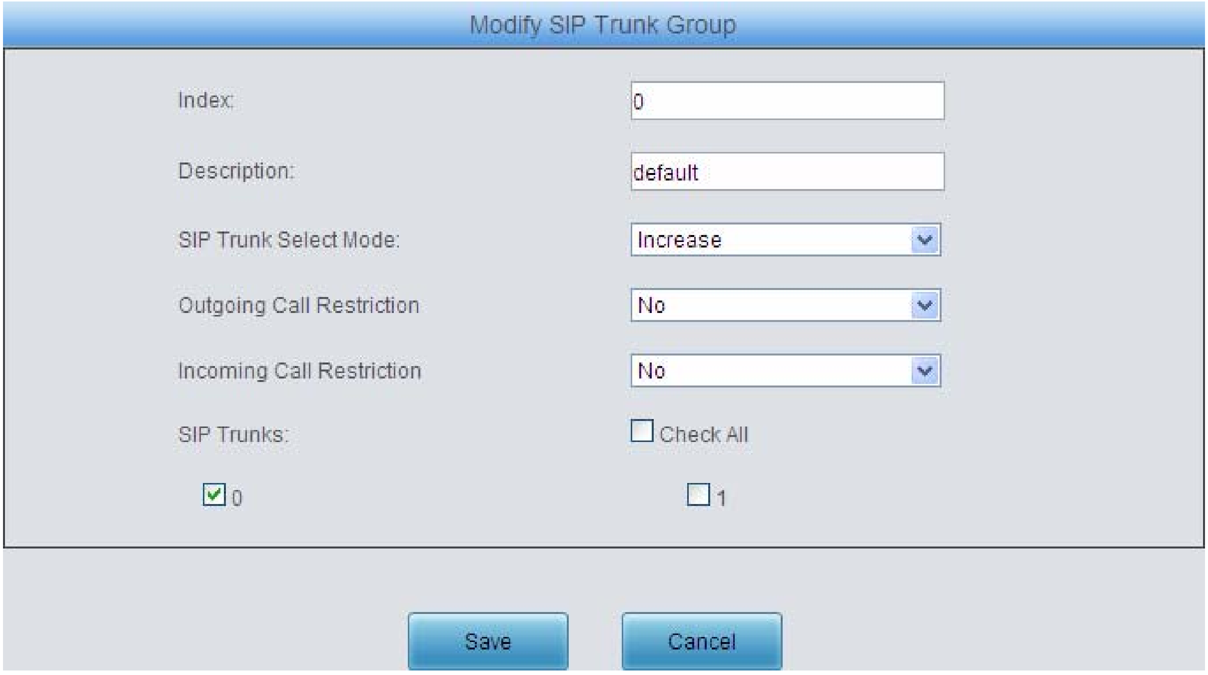


Figure 3-26 Modify SIP Trunk Group

To delete a SIP trunk group, check the checkbox before the corresponding index in Figure 3-24 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all SIP trunk groups at a time, click the ***Clear All*** button in Figure 3-24.

3.3.6 Media Settings

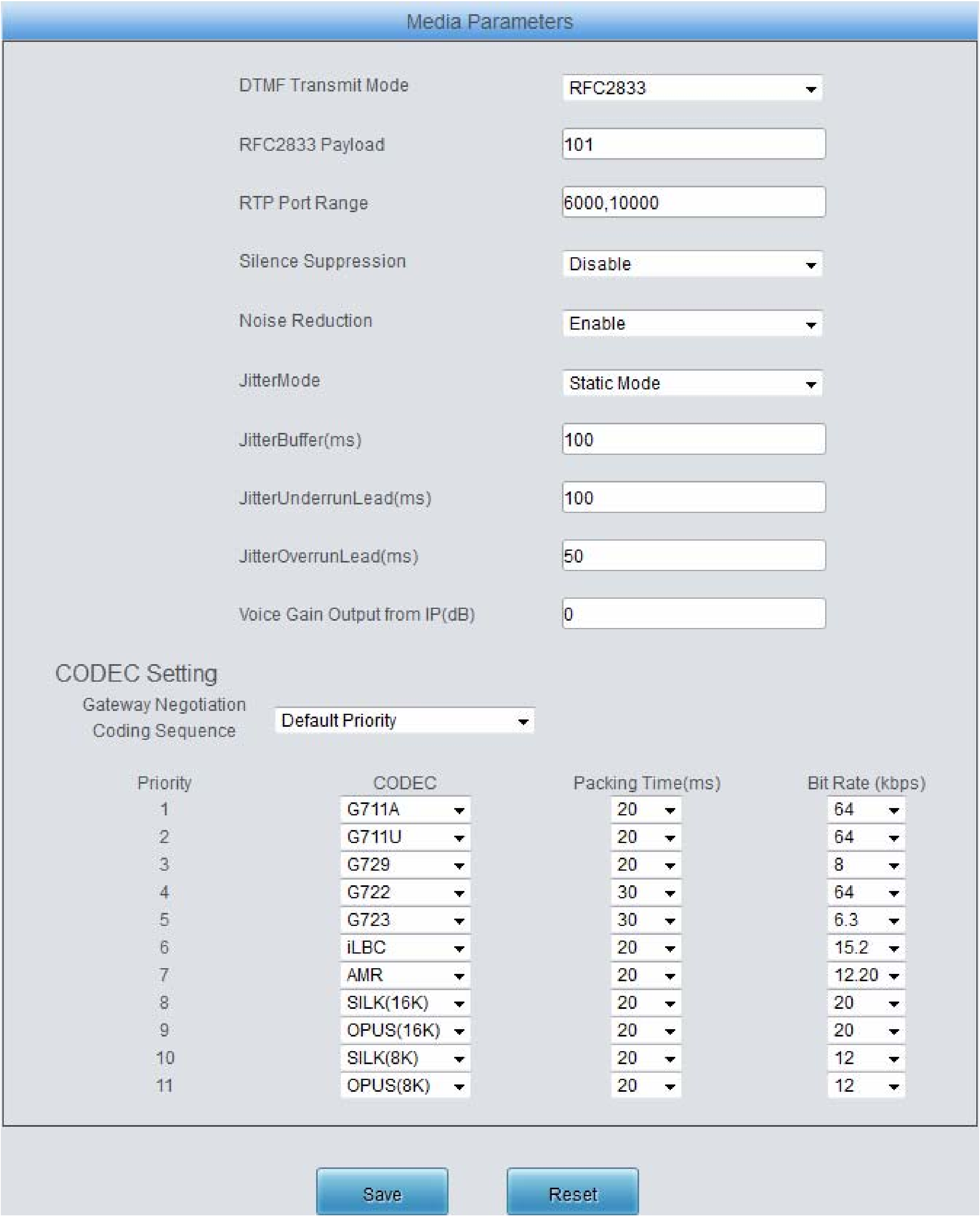


Figure 3-27 Media Settings Interface

See Figure 3-27 for the media settings interface where you can configure the RTP port and payload type depending on your requirements. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-27.

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 10000 and the difference between larger than 512.
Silence Suppression	Sets whether to send comfort noise packets to replace RTP packets or never to send RTP packets to reduce the bandwidth usage when there is no voice signal throughout an IP conversation. The optional values are *Enable* and *Disable*, with the default value of *Disable*. **Note:** When G723 is selected as CODEC, this configuration setting will turn to Enable automatically.
Noise Reduction	Once this feature is enabled, the volume of the noise accompanied with the line will be reduced automatically. The default setting is *Enable*.
JitterMode	Sets the working mode of JitterBuffer. The optional values are *Static Mode* and *Adaptive Mode*, with the default value of *Static Mode.*
JitterBuffer	Acceptable jitter for data packets transmission over IP, which indicates the buffering capacity. A larger JitterBuffer means a higher jitter processing capability but as well as an increased voice delay, while a smaller JitterBuffer means a lower jitter processing capability but as well as a decreased voice delay. Range of value: 0~280, calculated by ms, with the default value of 100.
JitterUnderrunLead	Sets the initial delay applied to receive packets upon accepting packets later than the expected value set in JitterBuffer Item. Rnage of value: 0~280, calculated by ms, with the default value of *100*, **Note:** Only when JitterMode is to *Static Mode* will this item be shown.
JitterOverrunLead	Sets the beforehand time inserted if receiving packets is ahead of time (the time of receiving is earlier than 300 minus the value set in JitterBuffer). Rnage of value: 0~280, calculated by ms, with the default value of *50*, **Note:** Only when JitterMode is to *Static Mode* will this item be shown.
JitterMin	Sets the minimum delay that can be set by the adaptive jitter function. It can not be larger than the value set in JitterBuffer. Rnage of value: 0~280, calculated by ms, with the default value of 80. **Note:** Only when JitterMode is 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. Rnage of value: 0~100, with the default value of *50*, **Note:** Only when JitterMode is to *Adaptive Mode* will this item be shown.
JitterIncreaseMax	Sets the maximum delay can be increased during one silence period. Rnage of value: 0~280, calculated by ms, with the default value of *30*, **Note:** Only when JitterMode is to *Adaptive Mode* will this item be shown.

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

3.4 PCM Settings

PCM Settings includes eight parts: ***PSTN***, ***Circuit Maintenance***, ***PCM***, ***PCM Trunk***, ***PCM Trunk Group***, ***Number-Receiving Rule***, ***Reception Timeout*** and ***PSTN Forwarding***. See Figure 3-28.

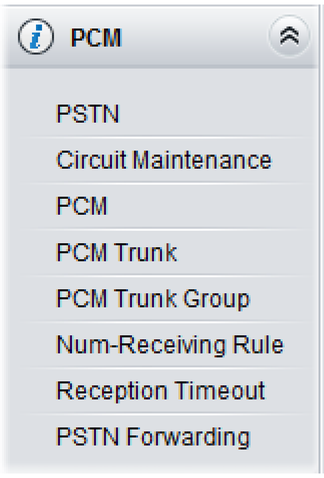


Figure 3-28 PCM Settings

3.4.1 PSTN

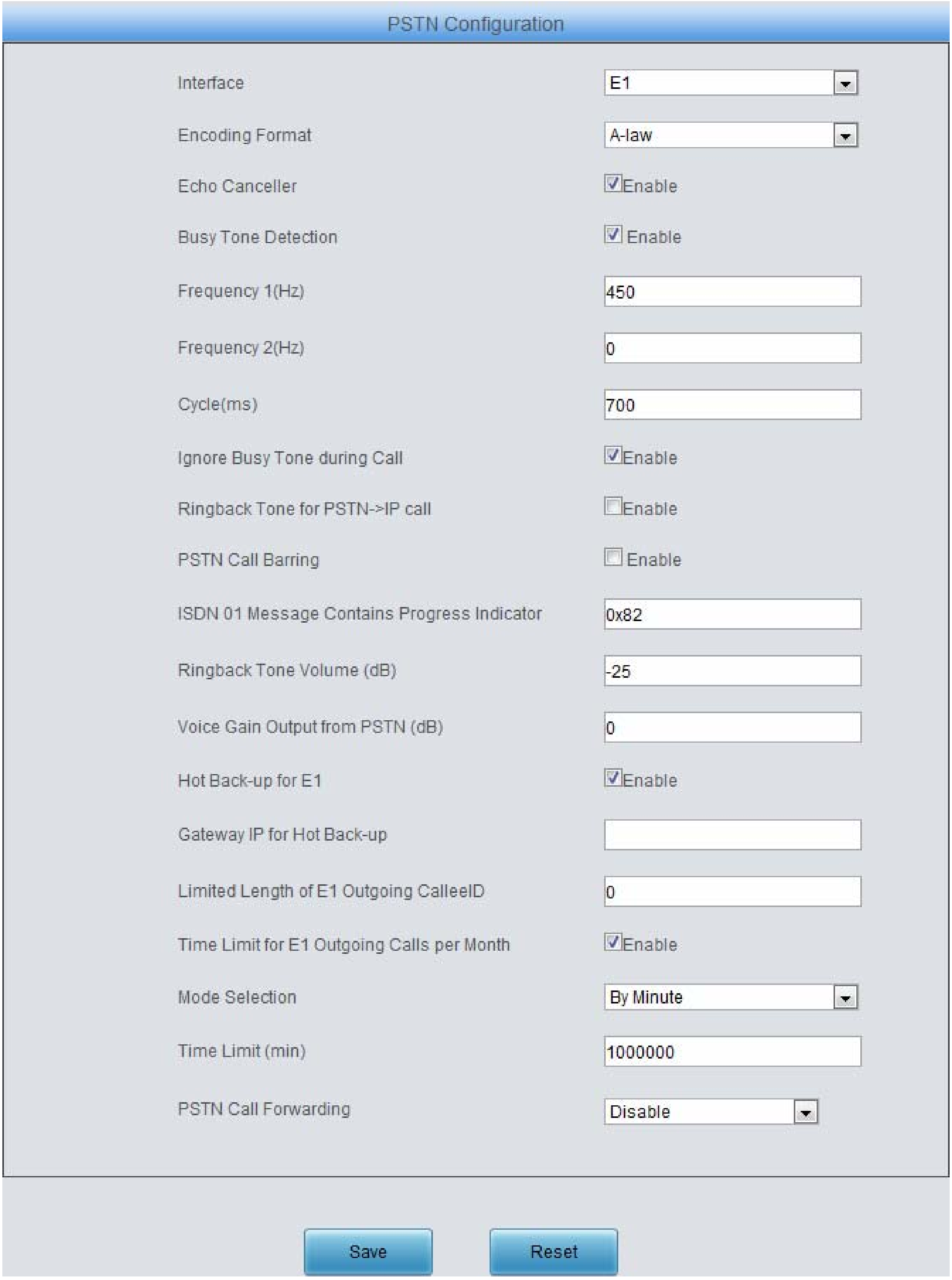


Figure 3-29 PSTN Settings Interface

See Figure 3-29 for the PSTN Settings interface. The table below explains the items shown in the above figure.

Item	Description
Interface	Actual type of the line connected with the E1/T1 interface on the gateway. Currently, only E1/T1 is supported.
Encoding Format	Sets the voice data encoding format for the voice channels on the digital trunk. The optional values are *A-law* and *u-law*, with the default value of *A-law*.
Echo Canceller	Sets whether to enable the echo cancellation feature for call conversations over the digital trunk. By default, this feature is enabled and the effect can reach 128ms.
Busy Tone Detection	Once this feature is enabled, the IP side will reply the 486 message once the E1 side detects the busy tone. The default value is *disabled*.
Frequency 1, Frequency 2	Sets the first and second center frequency for the busy tone, calculated by HZ. The default value of Frequency 1 is *450* and that of Frequency 2 is *0*.
Cycle	Sets the busy tone cycle, calculated by ms. 4 different cycles can be added at the same time, sequencing from small to large and separated by ‘,’ (e.g. 700,1400,2000,3200). Range of value: 25-5000, with the default value of *700*,
Ignore Busy Tone during Call	Once this feature is enabled, the gateway will not hang up the call when detecting the busy tone during the call. The default value is *enabled*.
Ringback Tone for PSTN→IP Call	Sets whether to enable the E1 end to provide the ringback tone, with the default value of *disable*.
PSTN Call Barring	Once this feature is enabled, you can set how many outgoing calls will be started to the same calledID, with the default value of *disable*.
Access Threshold for Called Number	Sets the maximum times for starting outgoing calls to the same CalledID.
Cycle	Sets the cycle for outgoing calls.
SIP Respond Code	Define the SIP code returned from PSTN to SIP when the times of outgoing calls exceed the threshold value.
ISDN 01 Message Contain Progress Indicator	Sets the value of the progress indicator within the ISDN 01 message. Value of range: 0x80 ~ 0xff, with the default value of *0x82*. The value 0x0 means the ISDN 01 message does not contain the progress indicator.
Ringback Tone Volume	Sets the volume of the ringback tone. Range of value: -35~-2, calculated by dB, with the default value of -25.
Voice Gain Output from PSTN	Adjusts the voice gain of call from PSTN 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*.
Hot Back-up for E1	Sets whether to enable the feature of hot back-up for E1, with the default value of *disable*.
Gateway IP for Hot Back-up	Set the IP of the gateway for the hot back-up for E1.
Limited Length of E1 Outgoing CalleeID	Limits the CalleeID length of the outgoing calls from PSTN side. The calleeID will be divided into two parts if its length is greater than the value set in this item. Range of value: 0~50. The default value is 0, not limited.

PSTN Call Forwarding	Sets whether to forward the call back to the PSTN side as it fails to start from PSTN to IP, including three options: Disable, SIP call forwarding unavailable and Enable call forwarding immediately, with the default value of *disable*.
Number of Local SIP Trunk Group	Sets the local SIP trunk group No. used for forwarding the PSTN incoming call when it cannot get through.
Max No-Answer Times	Sets the maximum times of the PSTN incoming calls which cannot get through. The calls will not be forwarded until the times exceed the set value.

After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions.

3.4.2 Circuit Maintenance

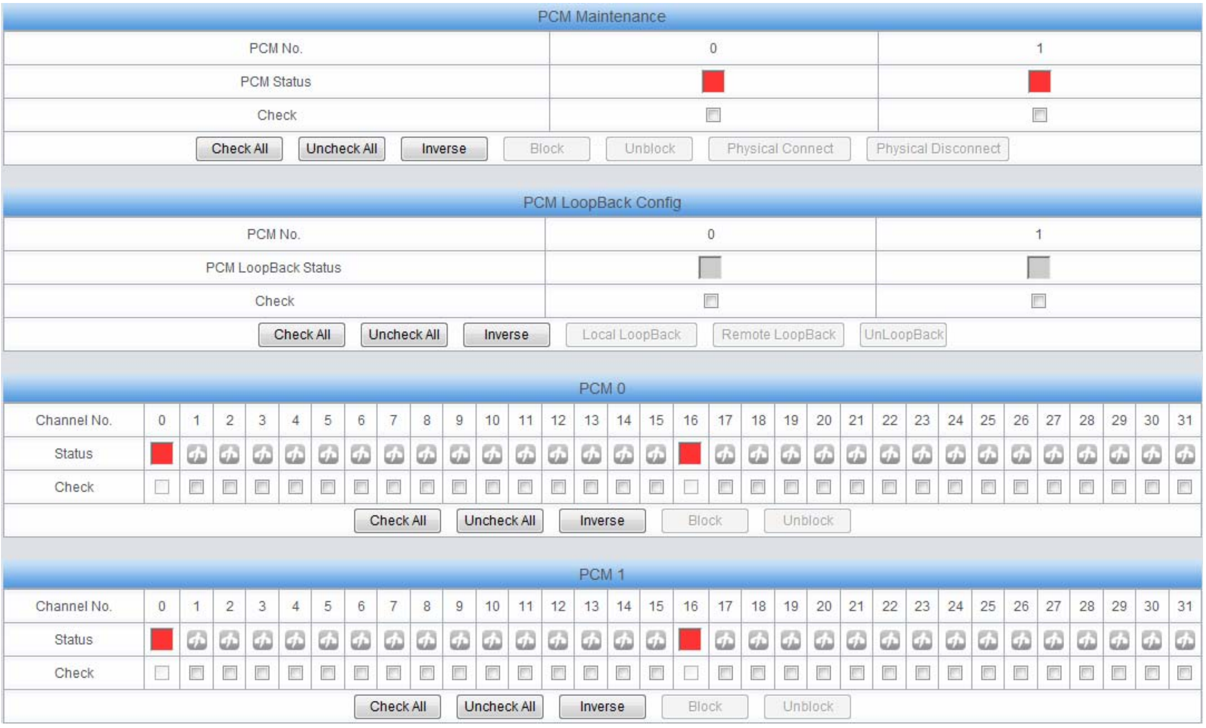


Figure 3-30 Circuit Maintenance Interface

See Figure 3-30 for the Circuit Maintenance interface. You can block, unblock, physical connect or disconnect PCMs, ports and channels on this interface. You can set the loopback feature of trunks for diagnoses or debugging. ***Local LoopBack*** means the transmitted data loop back from the LIU transmitter to the LIU receiver; ***Remote LoopBack*** means the transmitted data loop back to the LIU transmitter after being decoded in the LIU receiver. ***UnLoopBack*** is used to disable the features of local loopback and remote loopback.

Check All means to select all available items for the current port; ***Uncheck All*** means to cancel all selections for the current port; ***Inverse*** means to uncheck the selected items and check the unselected.

3.4.3 PCM

PCM Settings

PCM No.	Signaling Protocol	Clock	Signaling Time Slot	Signaling Link Type	Connection Line	CRC-4	Sip Trunk No.	Modify
0	ISDN User Side	Line-synchronization	16	--	Twisted Pair Cable	Enable	-1	
1	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	

Figure 3-31 PCM Settings Interface

See Figure 3-31 for the PCM settings interface. The above list shows the detailed information and configurations of each PCM. The table below explains the items shown in the above figure.

Item	Description
PCM No.	The number of the PCM, numbered from 0. This item is not configurable.
Signaling Protocol	The signaling protocol applied on the digital trunk. It includes ISDN User Side, ISDN Network Sideand SS1 in E1, and only includes ISDN User Side, ISDN Network Side in T1. **Note:** 1, Changing the interface type from E1 to T1 will forbid those non-ISDN signaling modes in E1. And in such case, the gateway will by default set this item to *ISDN User Side*.
Clock	The clock mode for the digital trunk, including Line-synchronization, Free-run and Slave.
Signaling Time Slot	Sets the time slot used for signaling transmission on the digital trunk. If the configuration item ***Signaling Protocol*** is set to *ISDN* and *SS1*, the signaling time slot is Time Slot 16 in E1 or Time Slot 24 in T1 (SS1 not supported in T1 by far), which cannot be modified.
Signaling Link Type	Indicates whether the PCM is used as a signaling link or a voice link. If no time slot is used to transmit signaling, the PCM is a voice link.
Connection Line	Physical connection line type.
Incoming Call Start TS, Amount	Sets a certain amount of channels which starts from a certain TS to process the incoming calls and others on the PCM to process outgoing calls. This is valid only when the configuration item ***Signaling Protocol*** is set to *SS1.*
CRC-4	Sets whether to enable the CRC-4 verification feature. By default, this feature is Enabled.
SIP Trunk No.	The bound SIP trunk No. used to send the option notify message once the status of the PCM trunk changes.

Click ***Modify*** in Figure 3-31 to modify a PCM. See Figure 3-32 for the PCM modification interface. Most configuration items on this interface are the same as those on the ***PCM Settings*** interface.

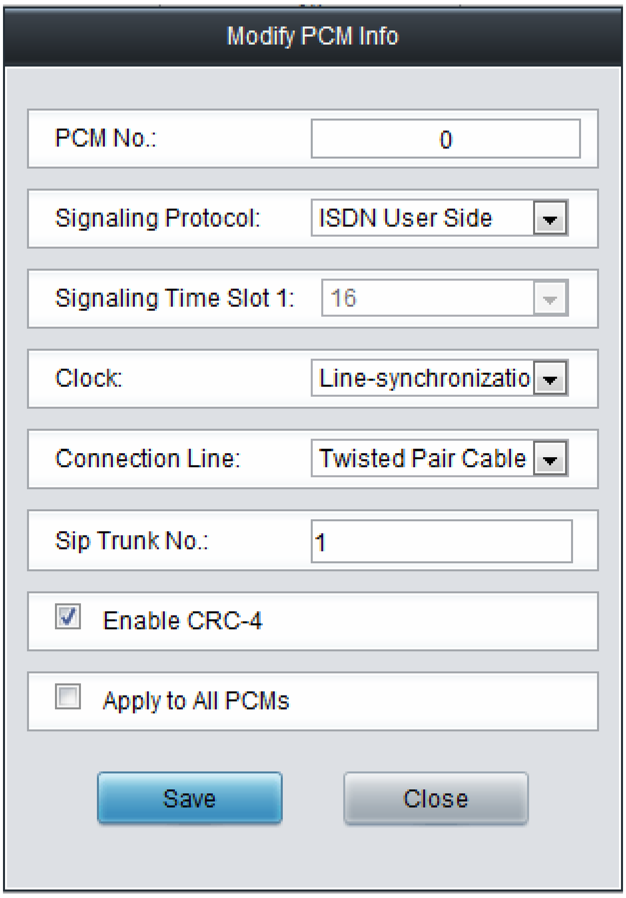


Figure 3-32 Modify PCM

The table below explains the other configuration items on the PCM modification interface.

Item	Description
Apply to All PCMs	Check this item to apply the above settings (excluding ***Clock***) to all PCMs.

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

3.4.4 PCM Trunk

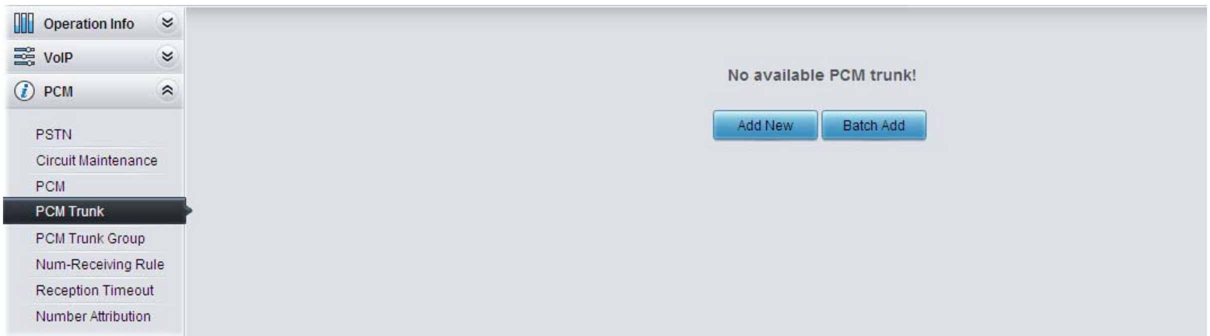


Figure 3-33 PCM Trunk Configuration Interface

See Figure 3-33 for the PCM Trunk Configuration interface. By default, there is no PCM trunk available on the gateway. Click ***Add New*** or ***Batch Add*** to add them manually. See Figure 3-34, Figure 3-35.

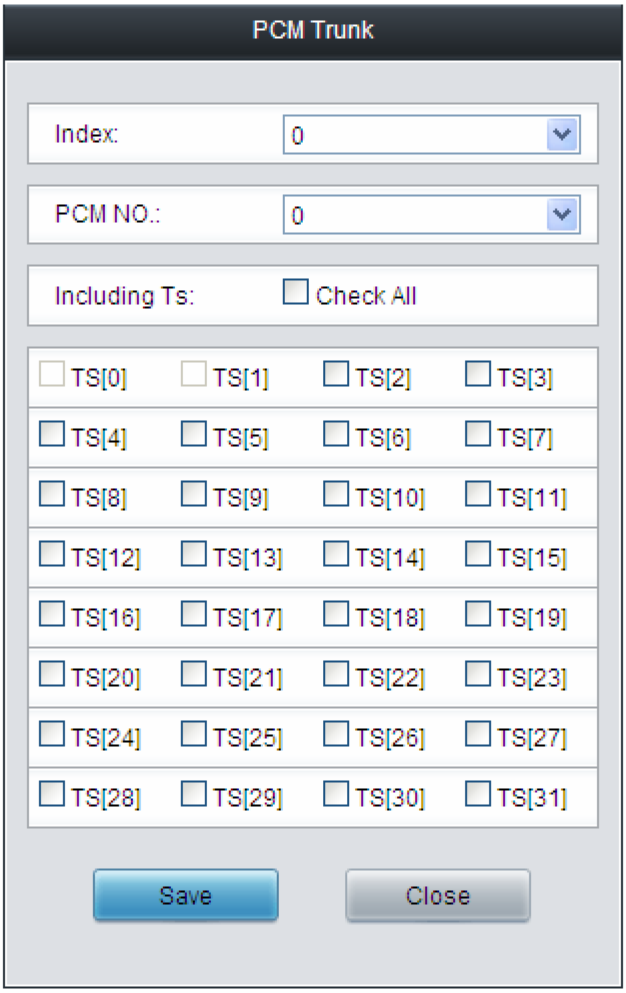


Figure 3-34 Add PCM Trunk Interface

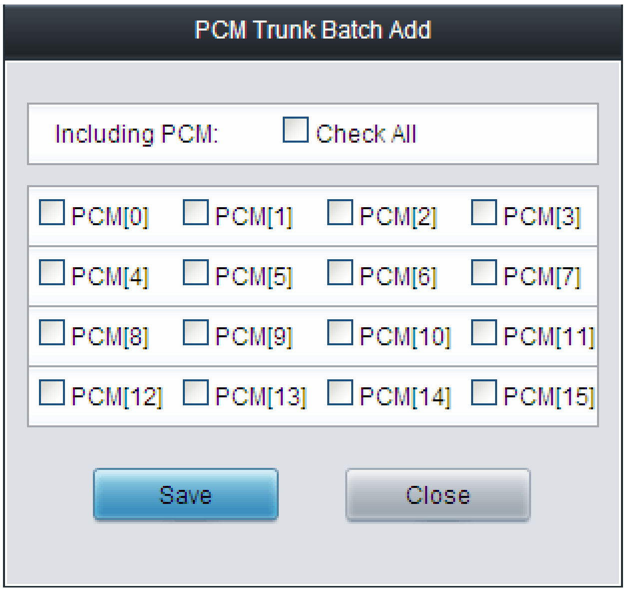


Figure 3-35 PCM Trunk Batch Add Interface

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

Item	Description
Index	The unique index of each PCM trunk

PCM NO.	The number of the PCM, numbered from 0.
Including Ts	Sets the TS included in this PCM which can make incoming/outgoing calls.
Including PCM	Sets the PCM included in the PCM trunk.

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

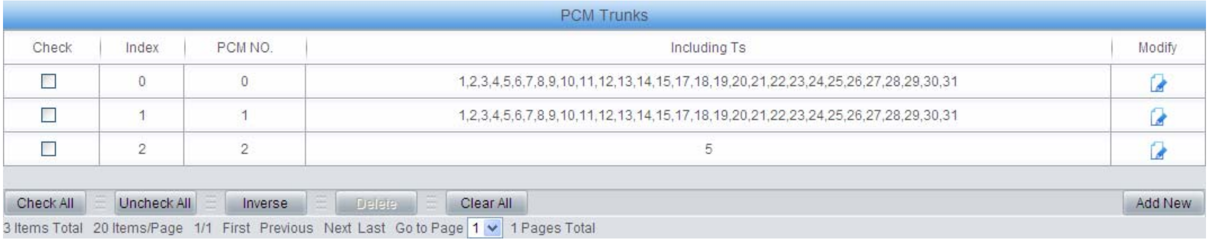


Figure 3-36 PCM Trunks List

Click ***Modify*** in Figure 3-36 to modify a PCM trunk. The configuration items on the PCM Trunk Modification Interface are the same as those on the ***Add PCM Trunk*** interface.

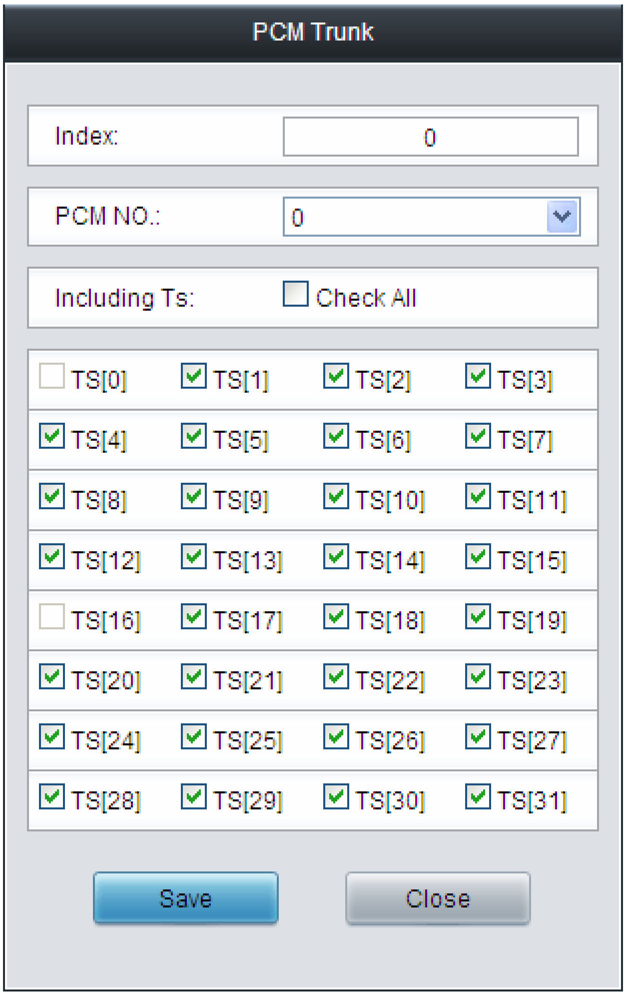


Figure 3-37 PCM Trunk Modification Interface

To delete a PCM trunk, check the checkbox before the corresponding index in Figure 3-36 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 PCM trunks at a time, click the ***Clear All*** button in Figure 3-36.

3.4.5 PCM Trunk Group

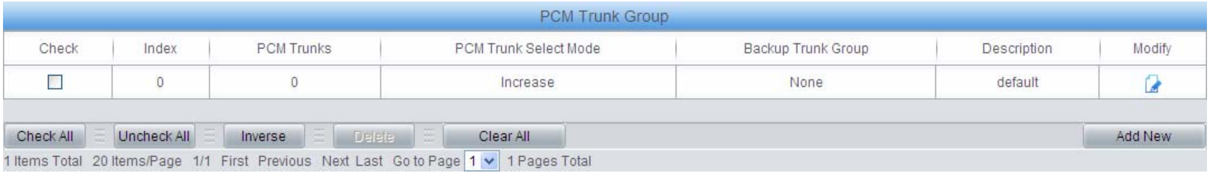


Figure 3-38 PCM Trunk Group Settings

See Figure 3-38 for the PCM trunk group settings interface. A new PCM trunk group can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-39 for the PCM trunk group adding interface.

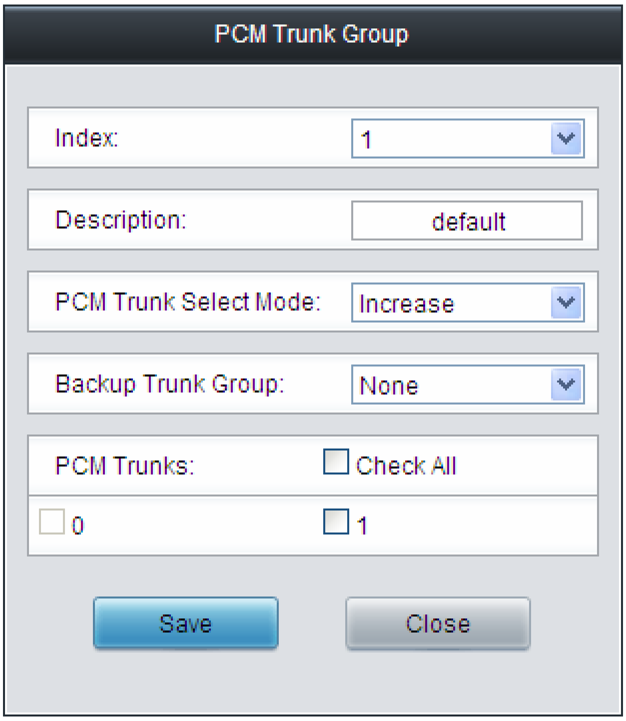


Figure 3-39 Add New PCM Trunk Group

The table below explains the items shown in Figure 3-39.

Item	Description
Index	The unique index of each PCM trunk group, which is mainly used in the configuration of routing rules and number manipulation rules to correspond to PCM trunk groups.
Description	More information about each PCM trunk group.

<table>
<tr><td rowspan="1">PCM Trunk Select Mode</td><td>When the PCM trunk group receives a call, it will choose a PCM 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 PCM trunk in the ascending order of the PCM number, starting from the minimum.</td></tr>
<tr><td>Decrease</td><td>Search for an idle PCM trunk in the descending order of the PCM number, starting from the maximum.</td></tr>
<tr><td>Cyclic Increase</td><td>Provided PCM Trunk N is the available PCM trunk found last time. Search for an idle PCM trunk in the ascending order of the PCM number, starting from PCM Trunk N+1.</td></tr>
<tr><td>Cyclic Decrease</td><td>Provided PCM Trunk N is the available PCM trunk found last time. Search for an idle PCM trunk in the descending order of the PCM number, starting from PCM trunk N-1.</td></tr>
</table></td></tr>
<tr><td>Backup Trunk Group</td><td>A trunk group used as the backup one.</td></tr>
<tr><td>PCM Trunks</td><td>The PCM trunks in the PCM trunk group. If the checkbox before a PCM trunk is grey, it indicates that the PCM trunk has been occupied. The ticked PCM trunks herein will be displayed in the column ‘PCM Trunks’ in Figure 3-38.</td></tr>
</table>

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

Click ***Modify*** in Figure 3-38 to modify a PCM trunk group. See Figure 3-40 for the PCM trunk group modification interface. The configuration items on this interface are the same as those on the ***Add New PCM Trunk Group*** interface.

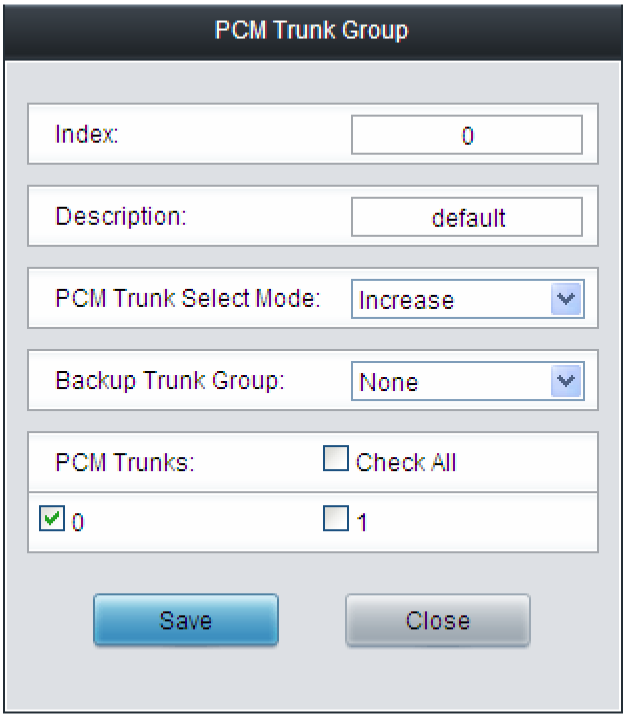


Figure 3-40 Modify PCM Trunk Group

To delete a PCM trunk group, check the checkbox before the corresponding index in Figure 3-38 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 PCM trunk groups at a time, click the ***Clear All*** button in Figure 3-38.

3.4.6 Number-receiving Rule

The gateway uses a number-receiving plan to filter the numbers received from PSTN. Only those numbers which match the plan will be processed. The number-receiving plan consists of multiple number-receiving rules, each of which has a priority in sequence to avoid conflict.

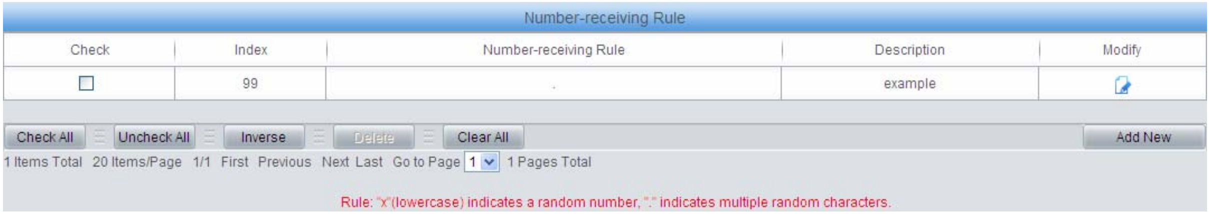


Figure 3-41 Number-Receiving Rule Configuration Interface

See Figure 3-41 for the Number-receiving Rule Configuration interface. The list in the above figure shows the number-receiving rules with their priorities and description. A new number-receiving rule can be added by the ***Add New*** button on the bottom right corner. See Figure 3-42 for the number-receiving rule adding interface.

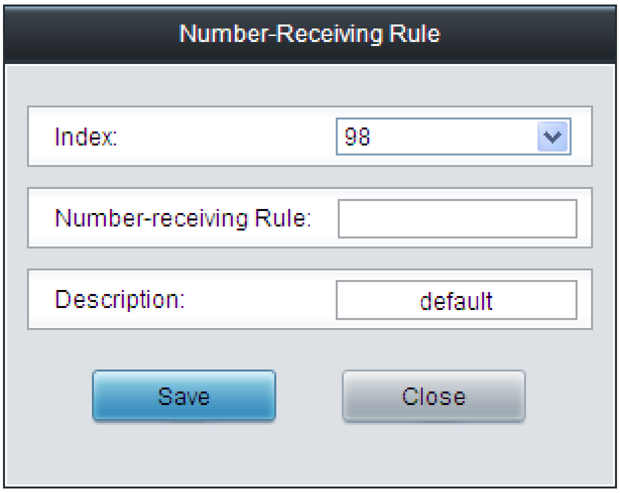


Figure 3-42 Add New Number-Receiving Rule

The table below explains the items shown in Figure 3-42.

Item	Description
Index	The unique index of each number-receiving rule, which denotes its priority. A number-receiving rule with a smaller index value has a higher priority and will be checked earlier while matching.

Number-Receiving Rule

Up to 200 number-receiving rules can be configured in the gateway, and the maximum length of each number-receiving rule is 64 characters. See below for the meaning of each character in the number-receiving rule. The gateway will do instant matching for your receiving number based on the number-receiving rule and regard your receiving as finished upon receiving ‘#’ or reception timeout.

Character	Description
“0”~”9”	Digits 0~9.
“x”	A random number. A string of ‘x’s represents several random numbers. For example, ‘xxx’ denotes 3 random numbers.
“.”	‘.’ indicates a random amount (including zero) of characters after it.
“[ ]”	‘[ ]’ is used to define the range for a number. Values within it only can be digits ‘0~9’, punctuations ‘-’ and ‘,’. For example, [1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.
“-”	’-’ is used only in ‘[ ]’ between two numbers to indicates any number between these two numbers.
“,”	’,’ is used to separate numbers or number ranges, representing alternatives.

By default, there is only one rule configured on the gateway. The table below lists 20 rules as example for your easy use and understanding. See below for detailed information.

Priority	Dialing Rule	Description
99	.	Any number in any length.
98	01[3,5,8]xxxxxxxxx.	Any 12-digit number starting with 013, 015 or 018
97	010xxxxxxxx	Any 11-digit number starting with 010
96	02xxxxxxxxx	Any 11-digit number starting with 02
95	0[3-9]xxxxxxxxxx	Any 12-digit number starting with 03, 04, 05, 06, 07, 08 or 09
94	120	Number 120
93	11[0,2-9]	Number 110, 112, 113, 114, 115, 116, 117, 118 or 119
92	111xx	Any 5-digit number starting with 111
91	123xx	Any 5-digit number starting with 123
90	95xxx	Any 5-digit number starting with 95
89	100xx	Any 5-digit number starting with 100
88	1[3-5,8]xxxxxxxxx	Any 11-digit number starting with 13, 14, 15 or 18
87	[2-3,5-7]xxxxxxx	Any 8-digit number starting with 2, 3, 5, 6 or 7
86	8[1-9]xxxxxx	Any 8-digit number starting with 81, 82, 83, 84, 85, 86, 87, 88 or 89

	85	80[1-9]xxxxx	Any 8-digit number starting with 801, 802, 803, 804, 805,.806, 807, 808 or 809
	84	800xxxxxxx	Any 10-digit number starting with 800
	83	4[1-9]xxxxxx	Any 8-digit number starting with 41, 42, 43, 44, 45, 46, 47, 48 or 49.
	82	40[1-9]xxxxx	Any 8-digit number starting with 401, 402, 403, 404, 405, 406, 407, 408 or 409
	81	400xxxxxxx	Any 10-digit number starting with 400
	80	8xxx	Any 4-digit number starting with 8
Description	Remarks for the number-receiving rule. It can be any information, but can not be left empty.		

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

Click ***Modify*** in Figure 3-41 to modify the number-receiving rules. See Figure 3-43 for the number-receiving rule modification interface. The configuration items on this interface are the same as those on the ***Add New Number-receiving Rule*** interface.

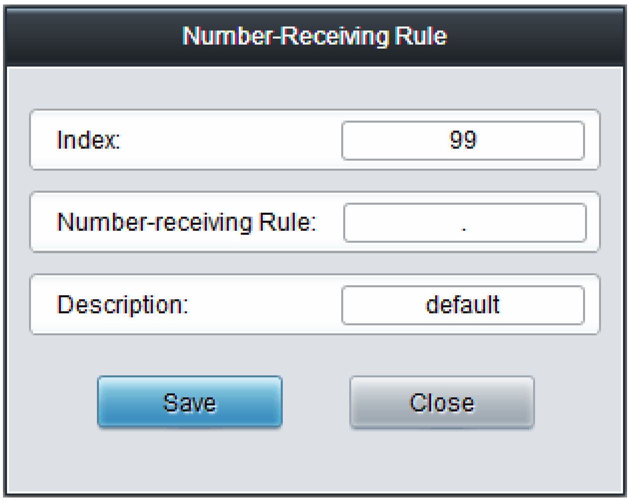


Figure 3-43 Modify Number-receiving Rule

To delete a number-receiving rule, check the checkbox before the corresponding index in Figure 3-41 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-receiving rules at a time, click the ***Clear All*** button in Figure 3-41.

3.4.7 Reception Timeout

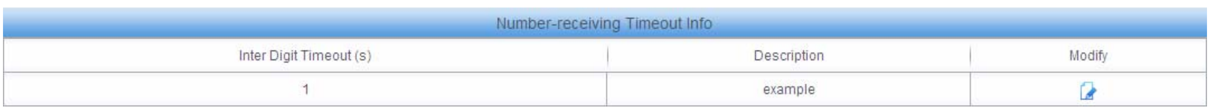


Figure 3-44 Number-receiving Timeout Info Interface

See Figure 3-44 for the number-receiving timeout info interface. The table below explains the items shown in the above figure.

Item	Description
Inter Digit Timeout	Sets the largest interval between two digits of a receiving number. Range of value: 0~10, calculated by s, with the default value of 1. In case your number-receiving rules do not include "**.**", the call will fail if there is no digit received or no number-receiving rule matched during this interval; in case your number-receiving rules include "**.**", the gateway will wait until this interval ends and match to the number-receiving rule "**.**" if there is no digit received or no other number-receiving rule matched during this interval.
Description	More information about the configuration item ***Inter Digit Timeout***, such as the reason for adopting the current value.

Click ***Modify*** in Figure 3-44 to modify the number-receiving timeout info. See Figure 3-45 for the number-receiving timeout info modification interface. The configuration items on this interface are the same as those on the ***Number-receiving Timeout Info Interface***.

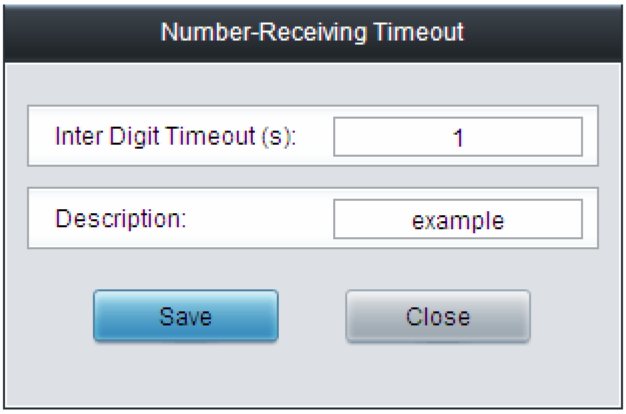


Figure 3-45 Modify Number-receiving Timeout Info

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

3.4.8 PSTN Forwarding

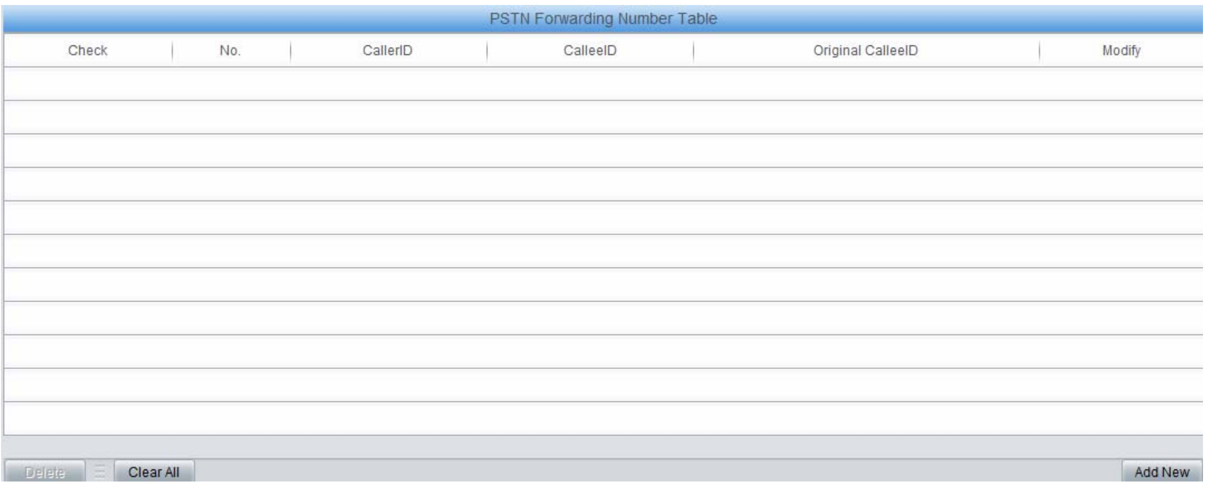


Figure 3-46 PSTN Forwarding Number Table Interface

See Figure 3-47 for the PSTN Forwarding Number Table interface. This interface will be displayed only when the feature of PSTN Call Forwarding in the PSTN setting interface is enabled. It is used to set the corresponding number for the call from PSTN to IP which fails and is forwarded back to PSTN. Click ***Add New*** to add them manually.

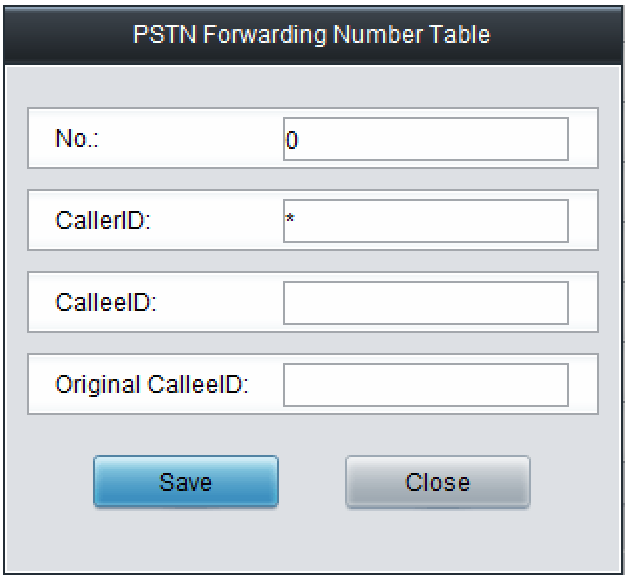


Figure 3-47 PSTN Forwarding Number Table Adding Interface

The table below explains the items shown in above figures.

Item	Description
No.	The corresponding number for the call to be forwarded.
CallerID	The CallerID of the PSTN→IP incoming call.
CalleeID	The CalleeID of the IP→PSTN outgoing call.
Original CalleeID	The original CalleeID of the PSTN→IP incoming call.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-48 for the PSTN Forwarding Number Table.

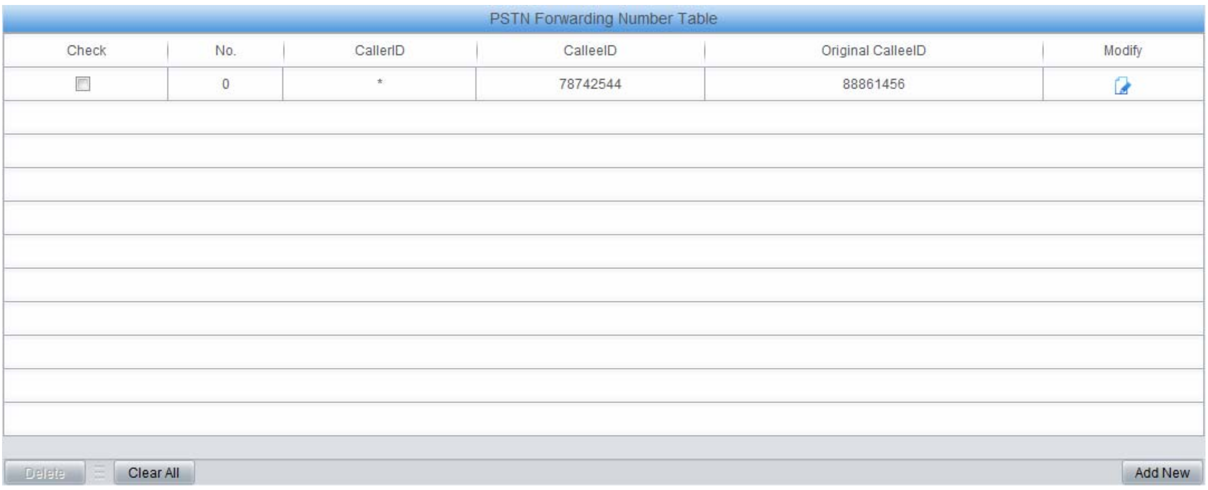


Figure 3-48 PSTN Forwarding Number Table

Click ***Modify*** in Figure 3-48 to modify the number table. See Figure 3-49 for the PSTN forwarding number table modification interface. The configuration items on this interface are the same as those on the ***Add PSTN Forwarding Number Table*** interface. Note that the item ***No.*** cannot be modified.

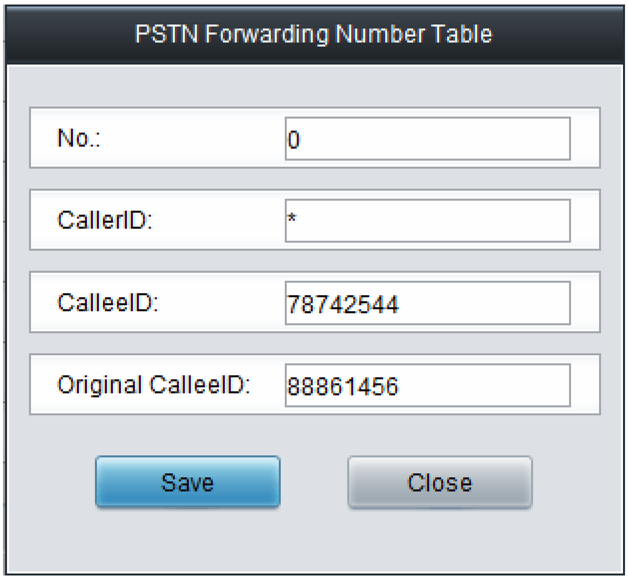


Figure 3-49 PSTN Forwarding Number Table Modification Interface

To delete a piece of number table, check the checkbox before the corresponding index in Figure 3-48 and click the ***Delete*** button. To clear all forwarding number tables at a time, click the ***Clear All*** button in Figure 3-48.

3.5 ISDN Settings

Users can see the ISDN option in the menu only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *ISDN User Side* or *ISDN Network Side*. See Figure 3-50.

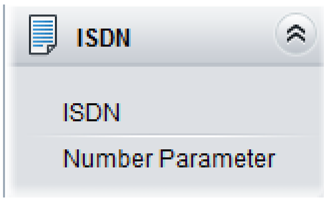


Figure 3-50 ISDN Settings

3.5.1 ISDN

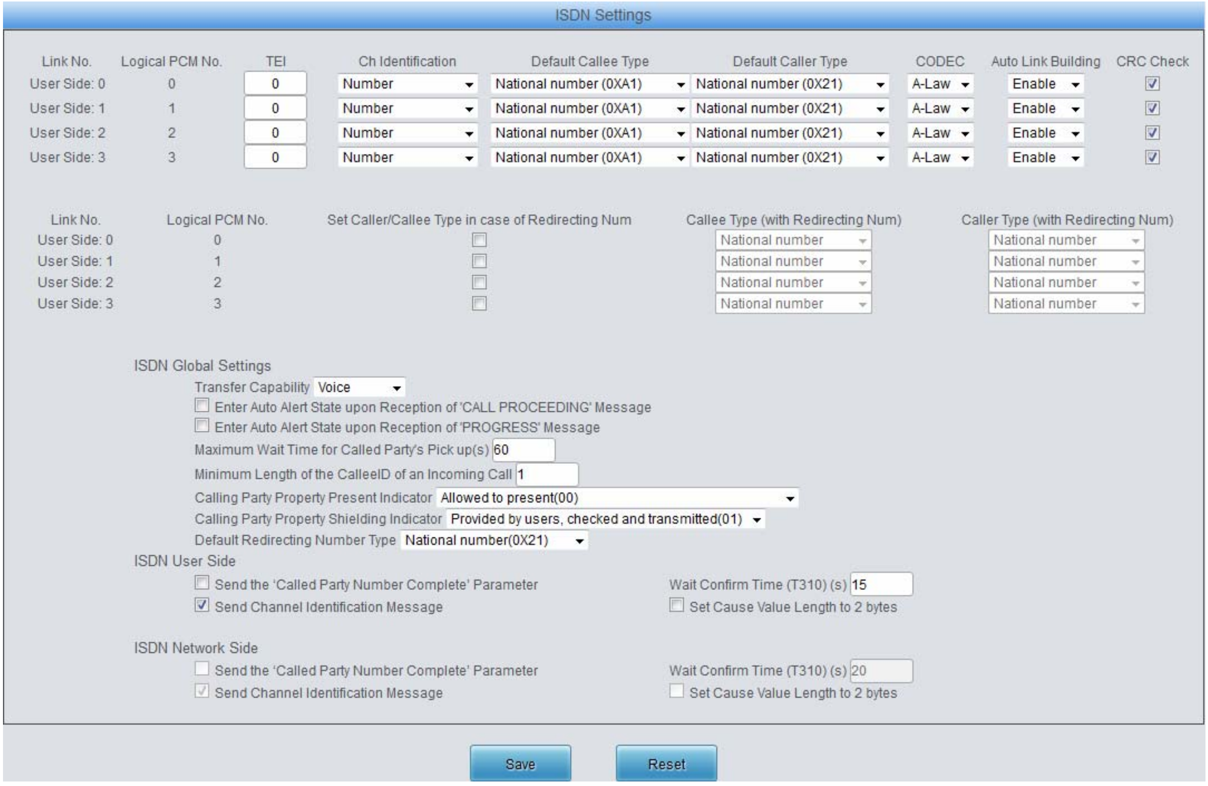


Figure 3-51 ISDN Settings Interface

See Figure 3-51 for the ISDN settings interface where users can configure the general ISDN parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-51.

Item	Description
TEI	Terminal Equipment Identifier, which is used to identify the service access point in the point-to-point data link connection. Range of value: 0~63, with the default value of 0. Note: The TEI values at the corresponding user side and the network side must be the same.
Ch Identification	Sets the way to represent channel identification messages on the digital trunk. The optional values are: *Number* and *Time slot diagram*, with the default value of *Number*.
Default Callee Type	Sets the type of number and numbering scheme for the called party numbers in the SETUP message during the outgoing call. The optional values are: National number, International number, Network number, Subscriber number and Unknown, with the default value of *National number*.
Default Caller Type	Sets the type of number and numbering scheme for the calling party numbers in the SETUP message during the outgoing call. The optional values are: National number, International number, Network number, Subscriber number and Unknown, with the default value of *National number*.
CODEC	Sets the voice CODEC used on the digital trunk. The optional values are *A-Law* and *u-Law*, with the default value of *A-Law*.

Auto Link Building	Sets whether to send the message of automatic link building for the ISDN at ISDN user side or network side. By default this feature is enabled.
CRC Check	Sets whether to enable the feature of CRC check for the digital trunk at ISDN user side or network side. By default this feature is enabled.
Set Caller/Callee Type in case of Redirecting Num	Once this feature is enabled, if the IP end carries the redirecting number in a call from IP to PSTN, you shall set separate values for the type of number and numbering scheme for the calling and called party numbers in the SETUP message, i.e. **Callee Type (with Redirecting Num)** and **Caller Type (with Redirecting Num)**. By default this configuration item is disabled.
Callee Type (with Redirecting Num)	This item is valid only when **Set Caller/Callee Type in case of Redirecting Num** is enabled. It sets the type of number and numbering scheme for the called party numbers in the SETUP message when the IP end carries the redirecting number in a call from IP to PSTN. The optional values are: National number, International number, Network number, Subscriber number and Unknown, with the default value of *National number*.
Caller Type (with Redirecting Num)	This item is valid only when **Set Caller/Callee Type in case of Redirecting Num** is enabled. It sets the type of number and numbering scheme for the calling party numbers in the SETUP message when the IP end carries the redirecting number in a call from IP to PSTN. The optional values are: National number, International number, Network number, Subscriber number and Unknown, with the default value of *National number*.
Transfer Capability	Sets the 'Transfer Capability' filed in the signaling message. The optional values are *Voice* and *3.1k Audio*, with the default value of *Voice*.
Enter Auto Alert State upon Reception of 'CALL PROCEEDING' Message	If this item is checked, the system will go into the state of auto alert when it receives the 02 (CALL PROCEEDING) message and the progress indicator turns to be 8 or 1. By default this item is disabled.
Enter Auto Alert State upon Reception of 'PROGRESS' Message	If this item is checked, the system will go into the state of auto alert when it receives the 03 (PROGRESS) message and the progress indicator turns to be 8 or 1. By default this item is disabled.
Maximum Wait Time for Called Party's Pick up	The maximum time waiting for the called party to pick up the call after the channel state turns to 'WaitAnswer' during an outgoing call. The default value is 60, calculated by s.
Minimum Length of the CalleeID of an Incoming Call	Sets the minimum length of the CalleeID under the fixed-length mode. The value range is $1 \le n \le 40$. Provided it is set to n, that is, the local end has received all the n digits of the called party number of the incoming call, the number reception will be regarded as finished.
Calling Party Property Present Indicator	Sets the calling party property present indicator, including four options: Allowed to present, Restricted to present, Fail to provide numbers due to intercommunication and Reserved, with the default value of *Allowed to present*.
Calling Party Property Shielding Indicator	Sets the calling party property shielding indicator, including three options: Provide by users, unchecked; Provide by users, checked and transmitted; Provide by network. The default value is *Provide by users, checked and transmitted*.

Default Redirecting Number Type	Sets the number type and numbering scheme for the redirecting number in the SETUP message during the outgoing call, The optional values are: National number, International number, Network number, Subscriber number and Unknown, with the default value of *National number*.
Send Channel Identification Message	Sets whether the channel identification message is included in the corresponding reply message (such as CALL PROCEEDING, ALERT, etc.) after the local end receives the SETUP message from the remote PBX during an incoming call. By default this item is checked.
Wait Confirm Time (T310)	Sets the maximum time that the local end waits for the remote end to send back the acknowledgement message in an outgoing call. If no acknowledgement message is received within the specified time period, the local end will disconnect the call automatically. For ISDN User Side, the default value is 15; for ISDN Network Side, the default value is 20, calculated by s.
Send the 'Called Party Number Completed' Parameter	Sets whether to include or not the 'Called Number Complete' parameter in the SETUP message during an outgoing call.
Set Cause Value Length to 2 bytes	Once this feature is enabled, the cause field in such messages as status (0x7d), release (0x4d), disconnect (0x45) will be 2 bytes. By default this item is disabled (3 bytes).

3.5.2 Number Parameter

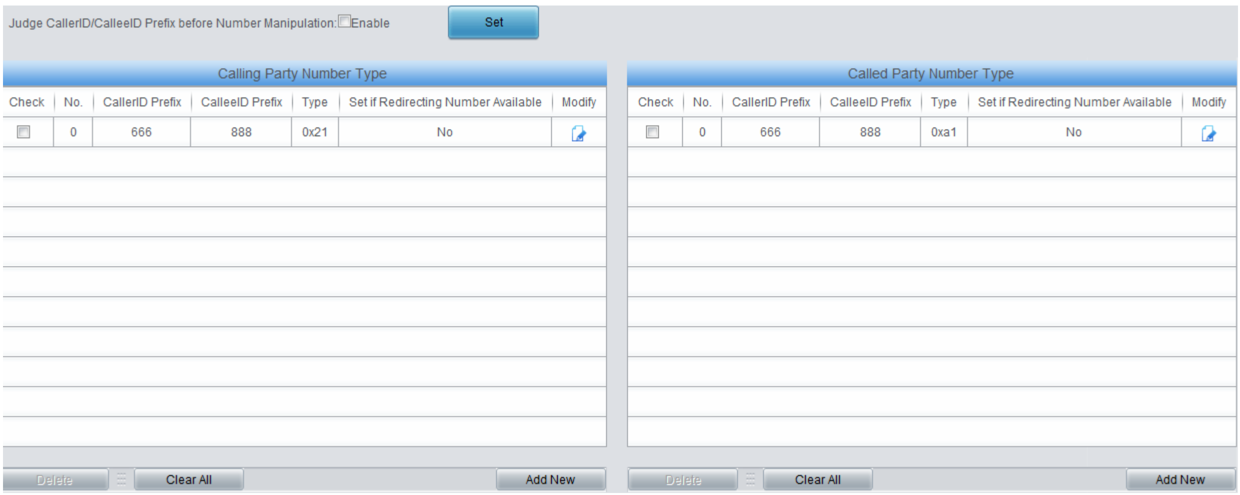


Figure 3-52 ISDN Number Parameter Configuration Interface

See Figure 3-52 for the ISDN Number Parameter Configuration interface, which includes two parts: ***Calling Party Number Parameter*** and ***Called Party Number Parameter***.

A new calling/called party number parameter can be added by the ***Add New*** button. See Figure 3-53, Figure 3-54 for the calling/called party number parameter adding interface.

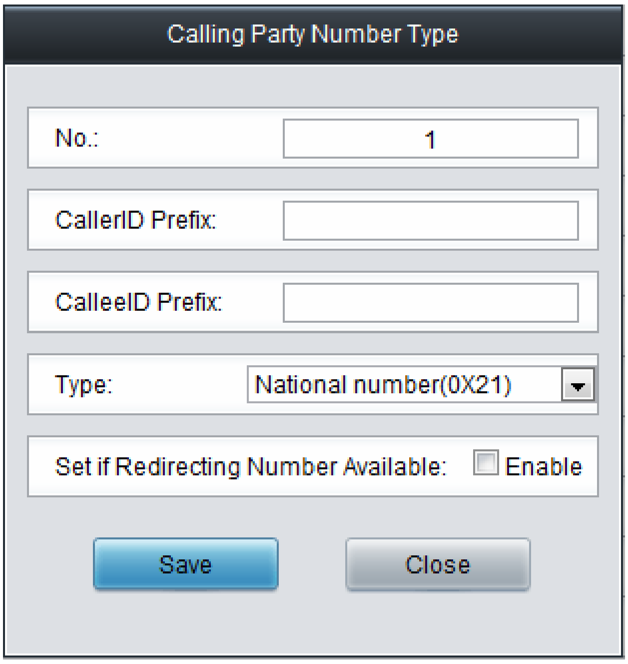


Figure 3-53 Add New Calling Party Number Parameter

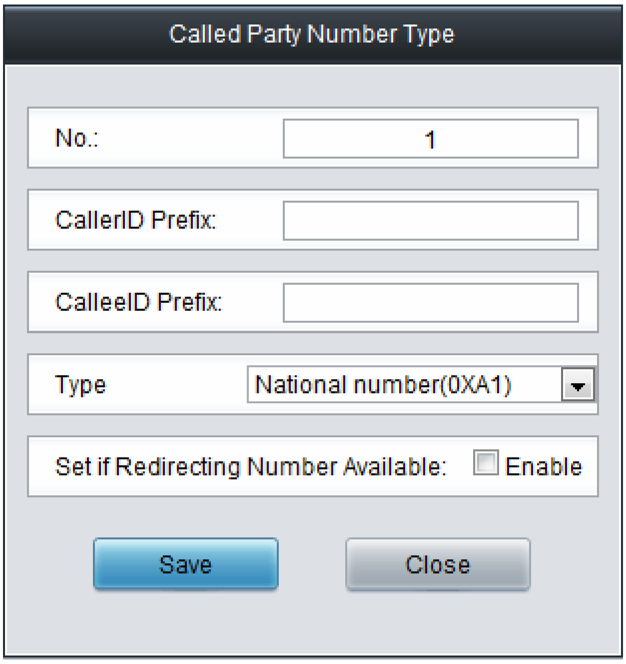


Figure 3-54 Add New Called Party Number Parameter

The table below explains the items shown in above figures.

Item	Description
CallerID/CalleeID Prefix before Number Manipulation	Sets whether to judge the prefix of the CallerID/CalleeID which hasn't been manipulated, with the default value of *disabled*, that is, only judge the prefix of the CallerID/CalleeID which has been manipulated.
No.	The corresponding number for a calling/called party number parameter, which starts from 0.
CallerID/CalledIDPrefix	A string of numbers at the beginning of a calling/called party number.

Set if Redirecting Number Available	Set whether to enable the feature of setting this parameter only if the Redirecting Number is available.

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

Click ***Modify*** in Figure 3-52 to modify the calling/called party number parameter. See Figure 3-55, Figure 3-56 for the calling/called party number parameter modification interface. The configuration items on this interface are the same as those on the ***Add New Calling/Called Party Number Parameter*** interface.

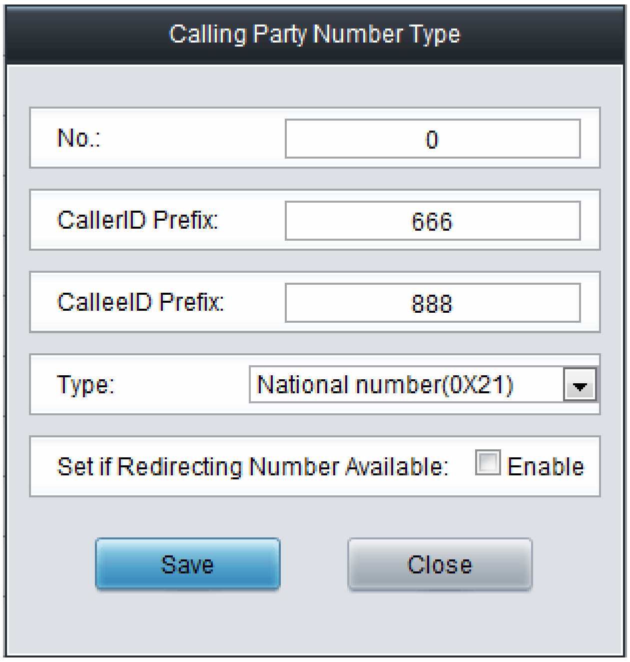


Figure 3-55 Modify Calling Party Number Parameter

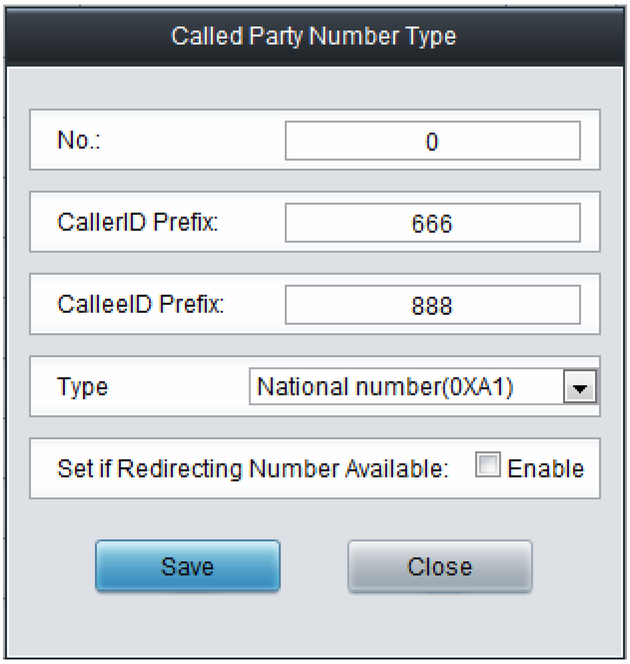


Figure 3-56 Modify Called Party Number Parameter

To delete a calling/called party number parameter, check the checkbox before the corresponding index and click the '***Delete***' button. To clear all calling/called party number parameters at a time, click the ***Clear All*** button in Figure 3-52.

Note: If there are two or more calling/called party numbers with the same prefix, the one numbered the smallest is valid and all the others become invalid.

3.5.3 Redirecting Number (Hidden item)

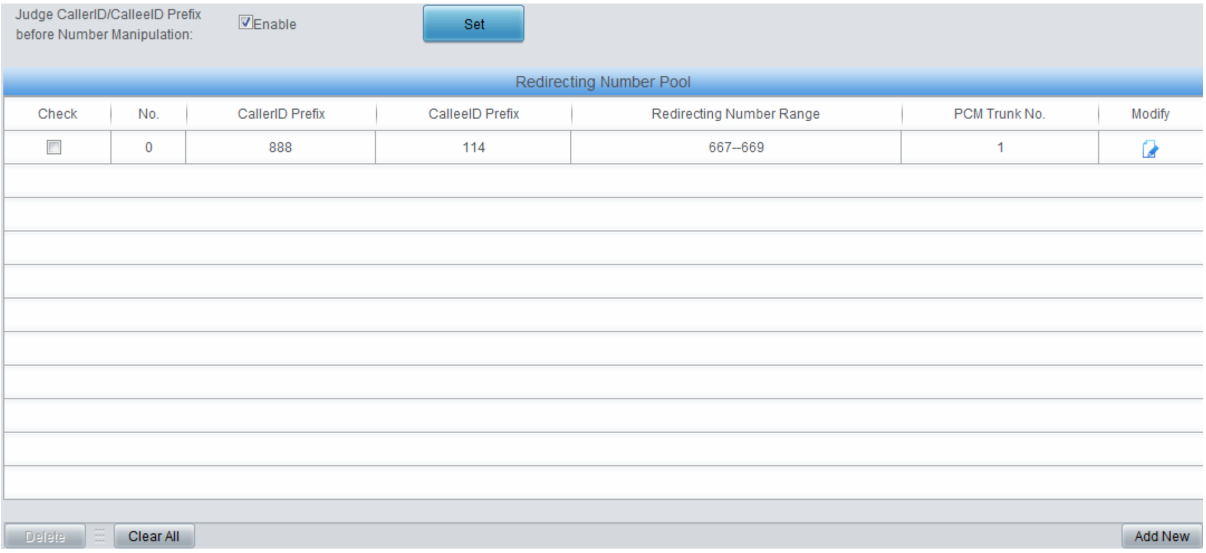


Figure 3-57 Redirecting Number Pool Interface

After you enter http://the IP address of your gateway/gfhmc.php in the address column of the browser, the Redirecting Number Pool for ISDN will appear on the web. See Figure 3-57 for the Redirecting Number Pool interface. A new redirecting number can be added by the Add New button. See Figure 3-58 for the redirecting number adding interface.

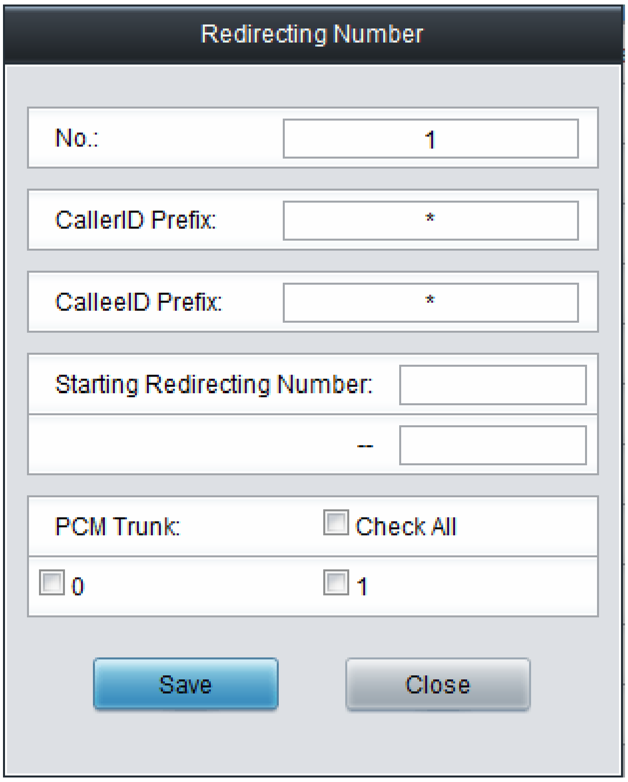


Figure 3-58 Add New Redirecting Number

The table below explains the items shown in above figures.

Item	Description

No.	The corresponding number for an added redirecting number. The value range is 0~99.
CallerID Prefix	A string of numbers at the beginning of a calling party number, which can be numbers or "*" (indicating any string).
CalleeID Prefix	A string of numbers at the beginning of a called party number, which can be numbers or "*" (indicating any string).
Starting Redirecting Number	The range of the redirecting number in the Redirecting Number Pool. It must be filled in with numbers and can not be left empty.
PCM Trunk	Sets the PCM included in the Redirecting Number Pool.

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

Click ***Modify*** in Figure 3-57 to modify the redirecting number parameter. See Figure 3-59 for the redirecting number modification interface. The configuration items on this interface are the same as those on the ***Add New Redirecting Number*** interface. Note that the item ***No.*** cannot be modified.

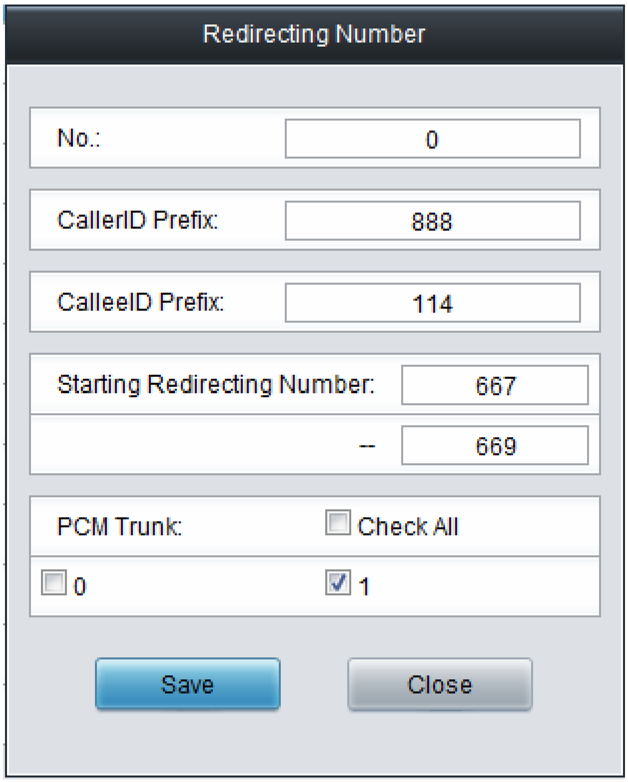


Figure 3-59 Modify Redirecting Number

To delete a redirecting number parameter, check the checkbox before the corresponding index Figure 3-57 and click the '***Delete***' button. To clear all redirecting number parameters at a time, click the ***Clear All*** button in Figure 3-57.

Note: If there are two or more calling/called party numbers with the same prefix, the Starting Redirecting Number will increase to be 1 plus the previous one, starting from that with the smallest number.

3.6 SS1 Settings

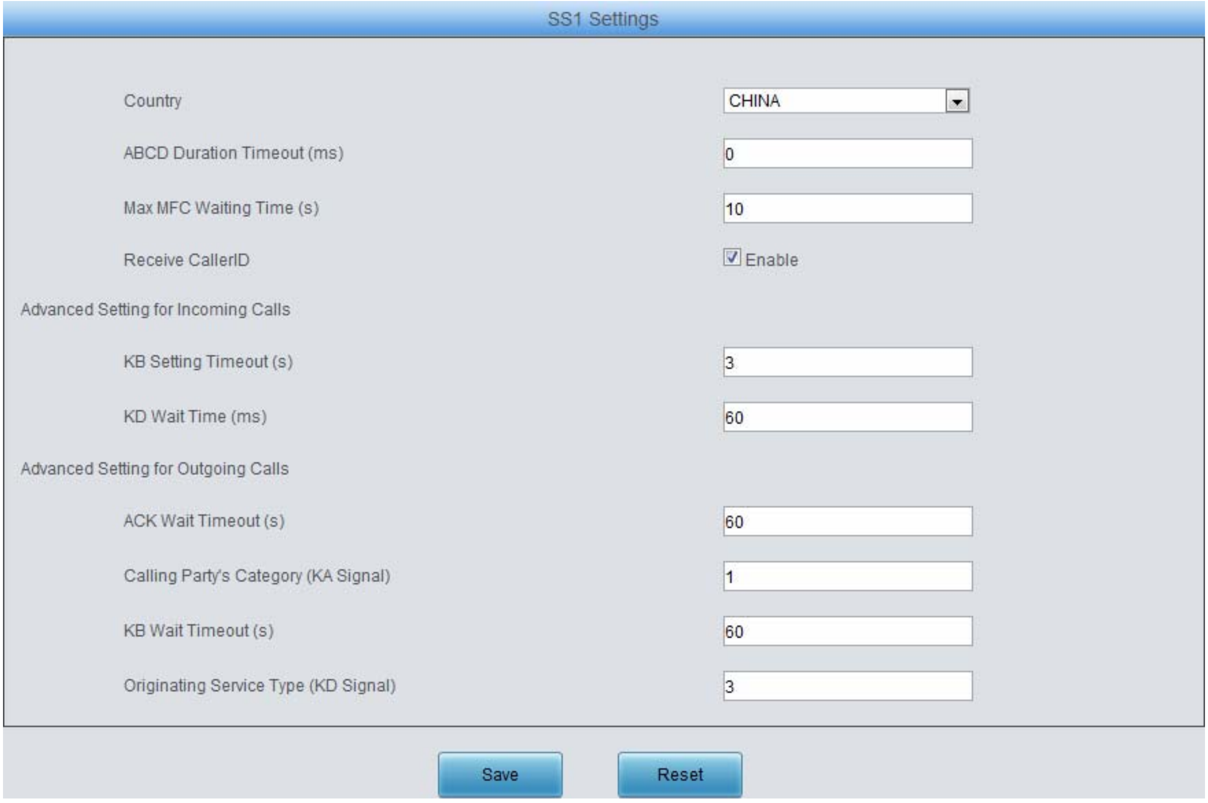


Figure 3-60 SS1 Settings Interface

See Figure 3-60 for the SS1 settings interface. This interface appears only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *SS1*. You can set general information of SS1. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions. The table below explains the items shown in Figure 3-60.

Item	Description
Country	Sets the country to use SS1, with the default value of *CHINA*.
ABCD Duration Timeout	Sets the minimum duration of ABCD signaling codes sent out by the remote PBX, calculated by millisecond (ms), which has to be the multiple of 8, with the default value of 0. Only when the on-line ABCD signaling codes vary and the new value keeps for more than the time specified by this configuration item will the gateway confirm the change of ABCD codes, Otherwise, the driver will believe there are undesired dithering signals on the line.
Max MFC Waiting Time	Sets the maximum waiting time, i.e. the timer T2 for the SS1 state machine, calculated by second, with the default value of *10*.
Receive CallerID	Sets whether to receive the calling party number. The default value is *enabled*.
KB Setting Timeout	Sets the maximum time to wait for the application to configure the KB signal, calculated by second, with the default value of *3*.
KD Wait Time	Sets the maximum time to wait for the remote PBX to send the KD signal (i.e. the timer T3) in the SS1 channel state machine, calculated by second, with the default value of *60*.

ACK Wait Timeout	Sets the value of the timer T5, calculated by second, with the default value of *60*.
Calling Party's Category (KA Signal)	Sets the KA signal (calling party's category at the local end) sent in an outgoing call. The value range is 1~10, with the default value of *1 (ordinary/regular)*.
KB Wait Timeout	Sets the maximum time to wait for the KB signal from the remote PBX, calculated by second, with the default value of *60*.
Originating Service Type (KD Signal)	Sets the originating service type, i.e. KD, for an outgoing call. The value range is 1~6, with the default value of *3 (local call)*.

3.7 Fax Settings

See Figure 3-61 for the Fax Settings interface which is used to modify the special fax configurations.

Figure 3-61 Fax Settings

3.7.1 Fax

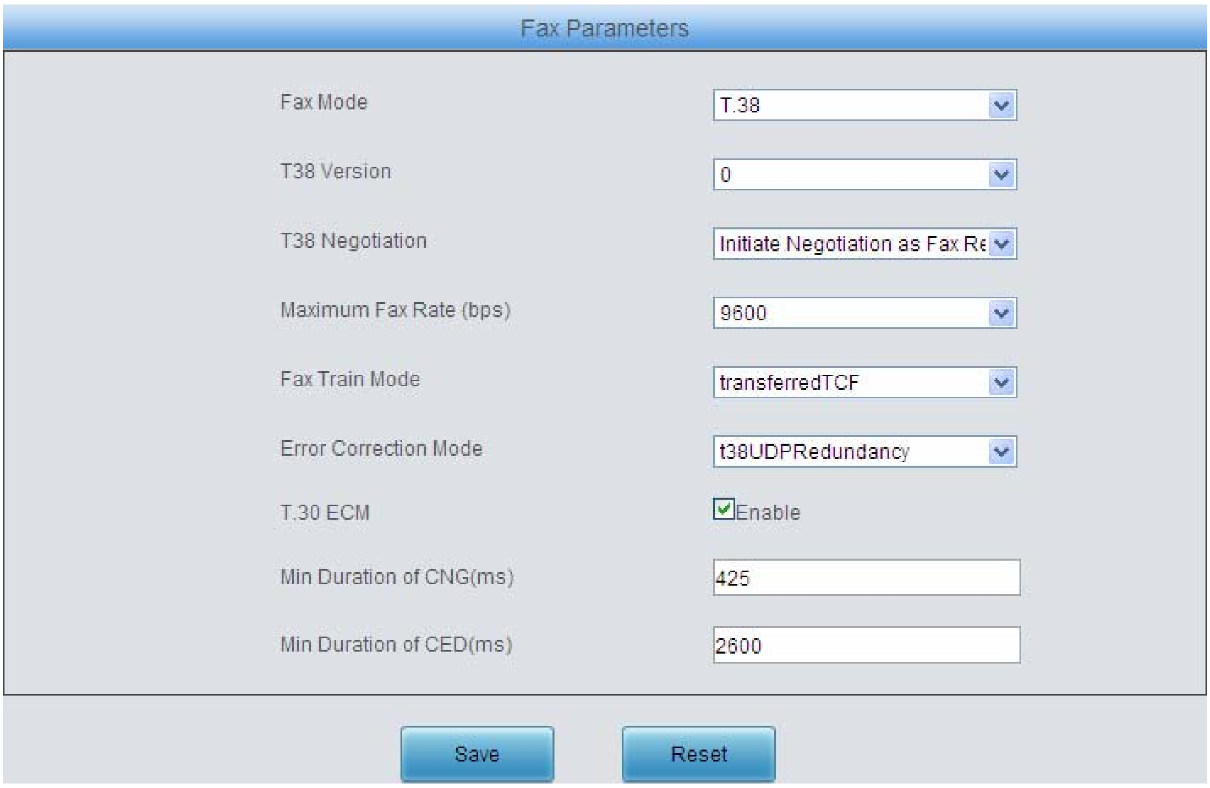


Figure 3-62 Fax Configuration Interface (T.38 Mode)

See Figure 3-62 for the fax configuration interface with all default settings under the T.38 fax mode. Users can configure the general fax parameters via this interface. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to 3.11.20 Restart for detailed instructions. The table below explains the configuration items in Figure 3-62.

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 can see the interface shown as Figure 3-63.

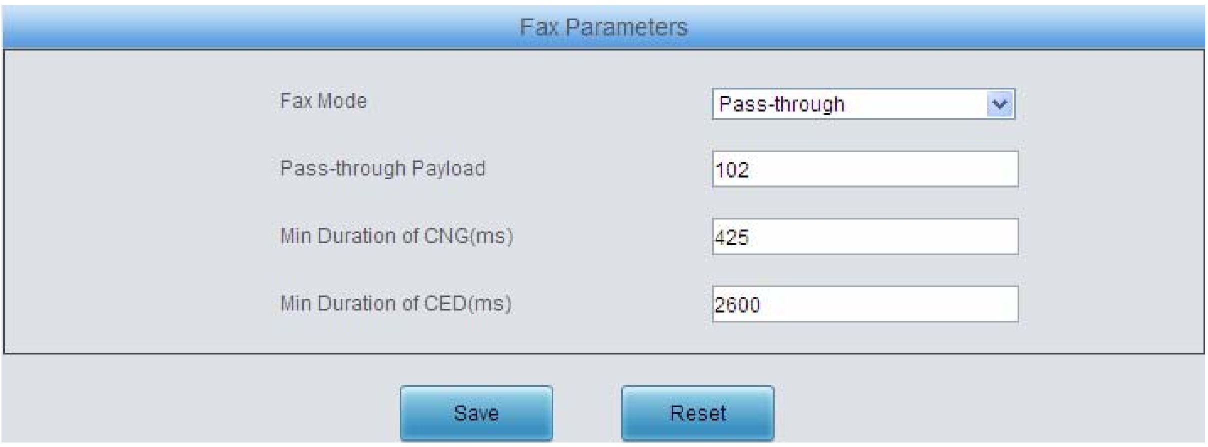


Figure 3-63 Fax Configuration Interface (Pass-through Mode)

The table below explains the configuration item in the above figure.

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

3.8 Route Settings

Route Settings is used to specify the routing rules for calls on two directions: IP→PSTN and PSTN→IP. See Figure 3-64.

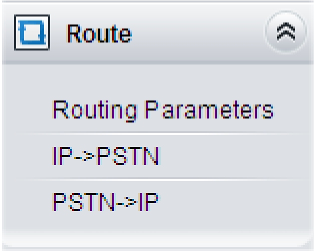


Figure 3-64 Route Settings

3.8.1 Routing Parameters

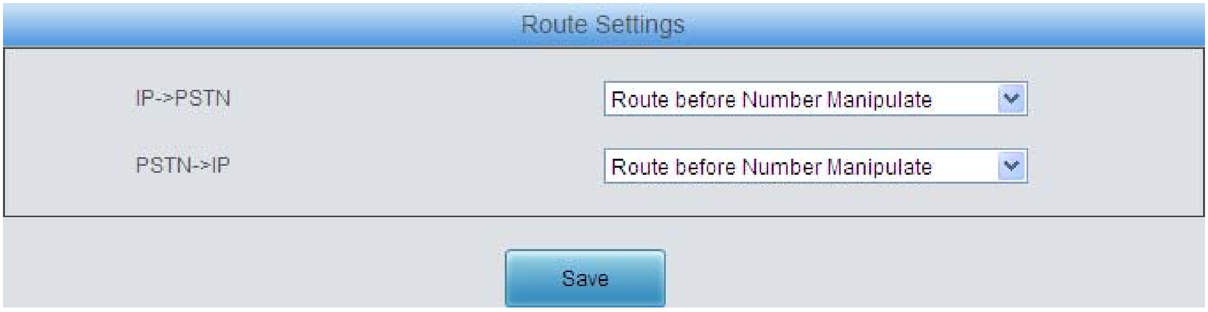


Figure 3-65 Routing Parameters Configuration Interface

See Figure 3-65 for the routing parameters configuration interface. On this interface, you can set the routing rules for calls respectively on two directions IP→PSTN and PSTN→IP to be routing before or after number manipulation. The default value is *Route before Number Manipulate*.

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

3.8.2 IP to PSTN

Figure 3-66 IP→PSTN Routing Rule Configuration Interface

See Figure 3-66 for the IP→PSTN routing rule configuration interface. A new routing rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-67 for the IP→PSTN routing rule adding interface.

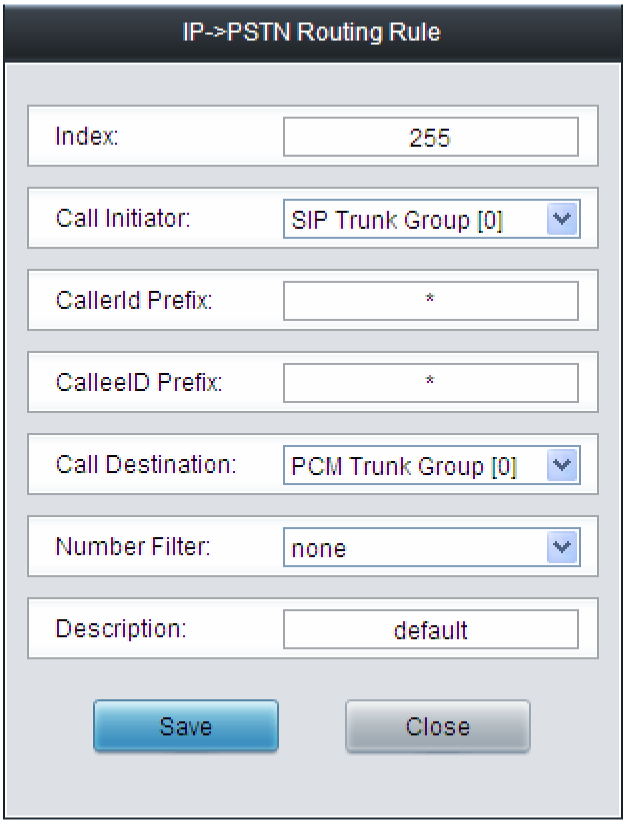


Figure 3-67 Add New Routing Rule (IP→PSTN)

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

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

<table>
<tr><td>CallerID Prefix,
CalleeID Prefix</td><td>A string of numbers at the beginning of the calling/called party number. This item can be set to a specific string or “*” which indicates any string. These two configuration items together with Call Initiator can specify the calls which apply to a routing rule.
Rule Explanation:
<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>“0”~”9”</td><td>Digits 0～9.</td></tr>
<tr><td>“[ ]”</td><td>‘[ ]’ is used to define the range for a number. Values within it only can be digits ‘0~9’, punctuations ‘-’ and ‘,’. For example, [1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.</td></tr>
<tr><td>“-”</td><td>’-’ is used only in ‘[ ]’ between two numbers to indicates any number between these two numbers.</td></tr>
<tr><td>“,”</td><td>’,’ is used to separate numbers or number ranges, representing alternatives.</td></tr>
</table>
Example: Rule “0[0-3,7][6-9]” denotes the prefix is 006, 016, 026, 036, 007, 017, 027, 037, 008, 018, 028, 038, 009, 019, 029, 039, 076, 077, 078, 079.
Note: Multiple rules are supported for CallerID/CalleeID prefix. They are separated by “:”.</td></tr>
<tr><td>Call Destination</td><td>PCM trunk group to which the call will be routed.</td></tr>
<tr><td>Number Filter</td><td>Number filter rule which will be applicable to this route. It is set in Number Filter. See 3.9.4 Filtering Rule for details.</td></tr>
<tr><td>Description</td><td>More information about each routing rule.</td></tr>
</table>

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

Click ***Modify*** in Figure 3-66 to modify a routing rule. See Figure 3-68 for the IP→PSTN routing rule modification interface. The configuration items on this interface are the same as those on the ***Add New Routing Rule (IP→PSTN)*** interface. Note that the item ***Index*** cannot be modified.

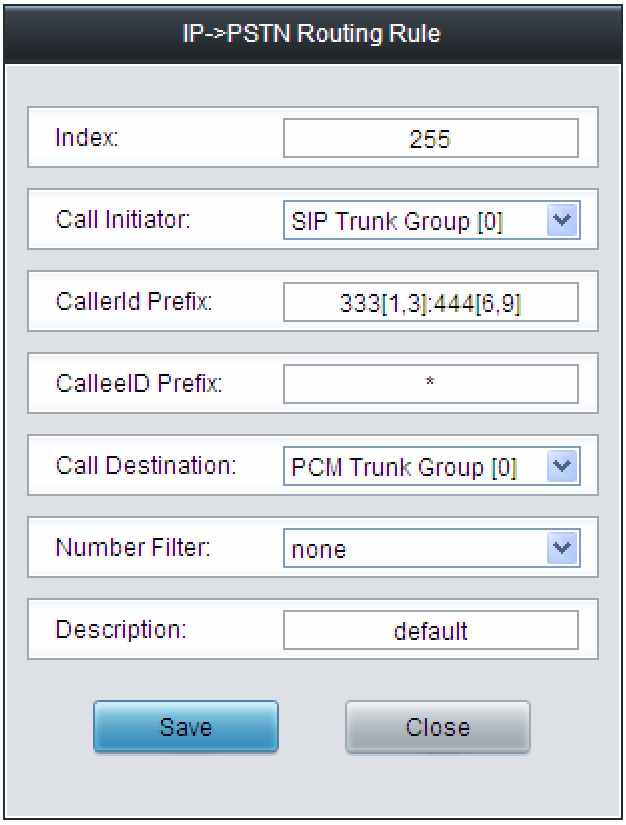
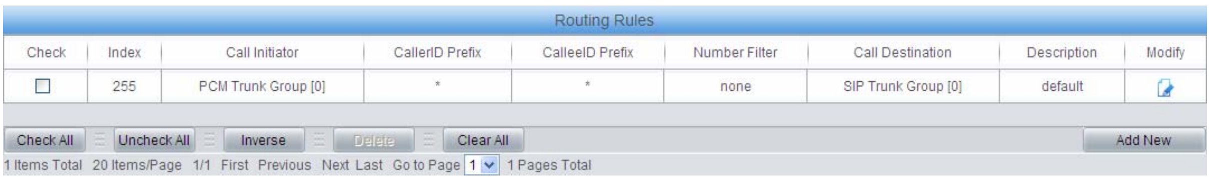


Figure 3-68 Modify Routing Rule (IP→PSTN)

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-66 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all routing rules at a time, click the ***Clear All*** button in Figure 3-66.

3.8.3 PSTN to IP


Routing Rules

Check	Index	Call Initiator	CallerID Prefix	CalleeID Prefix	Number Filter	Call Destination	Description	Modify
☐	255	PCM Trunk Group [0]	*	*	none	SIP Trunk Group [0]	default	

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

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

Figure 3-69 PSTN→IP Routing Rule Configuration Interface

See Figure 3-69 for the PSTN→IP routing rule configuration interface. A new routing rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-70 for the PSTN→IP routing rule adding interface.

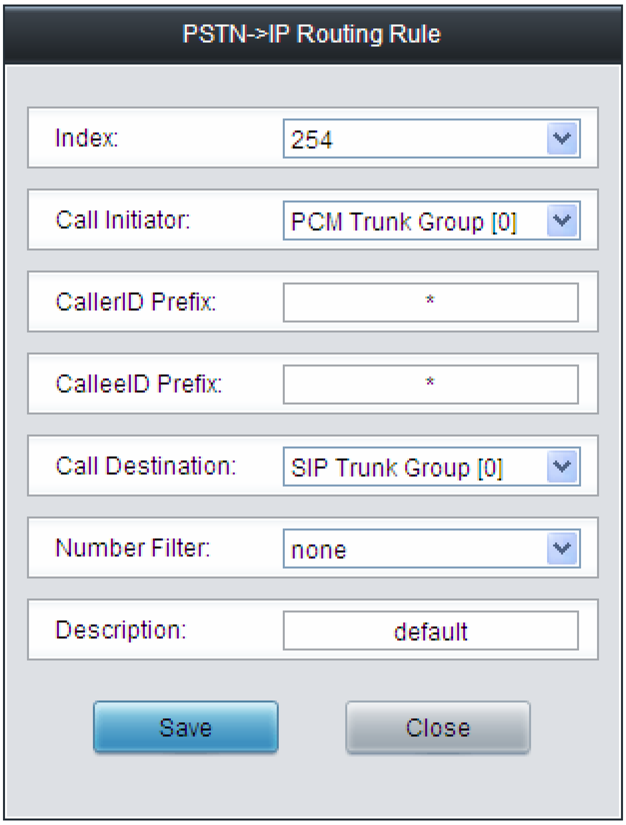


Figure 3-70 Add New Routing Rule (PSTN→IP)

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

Item	Description
Index	The unique index of each routing rule, which denotes its priority. A routing rule with a smaller index value has a higher priority. If a call matches several routing rules, it will be processed according to the one with the highest priority.
Call Initiator	PCM trunk group from which the call is initiated. This item can be set to a specific PCM trunk group or PCM Trunk Group [ANY] which indicates any PCM 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*** can specify the calls which apply to a routing rule. See the rule explanation of CallerID/CalleeID Prefix in IP to PSTN. **Note:** Multiple rules are supported in callerID/calleeID prefix. They should be separated by ":".
Call Destination	SIP trunk group to which the call will be routed.
Number Filter	Number filter rule which will be applicable to this route. It is set in ***Number Filter***. See 3.9.4 Filtering Rule for detailed setting.
Description	More information about each routing rule.

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

Click ***Modify*** in Figure 3-69 to modify a routing rule. See Figure 3-71 for the PSTN→IP routing rule modification interface. The configuration items on this interface are the same as those on the ***Add New Routing Rule (PSTN→IP)*** interface. Note that the item ***Index*** cannot be modified.

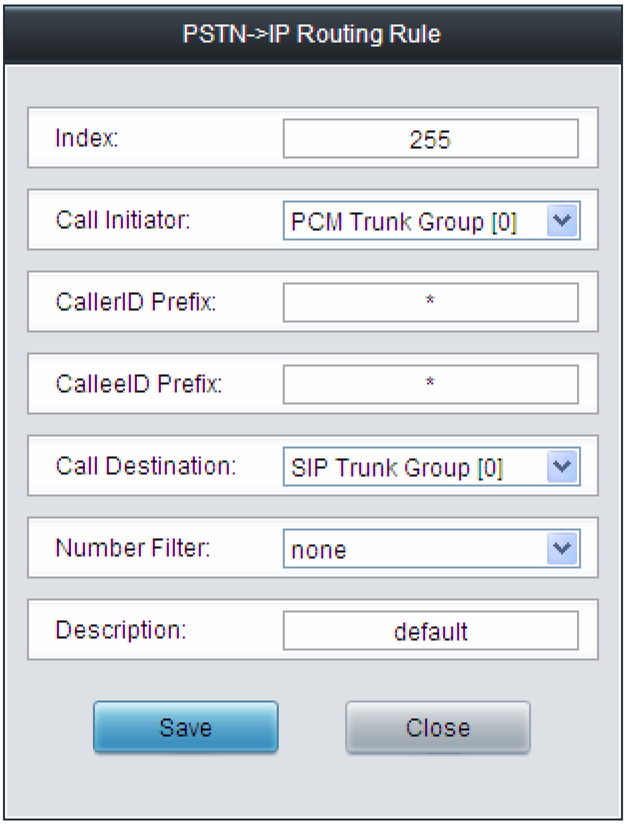


Figure 3-71 Modify Routing Rule (PSTN→IP)

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-69 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all routing rules at a time, click the ***Clear All*** button in Figure 3-69.

3.9 Number Filter

Number Filter includes four parts: ***Whitelist***, ***Blacklist***, ***Number Pool*** and ***Filtering Rule***. See Figure 3-72.

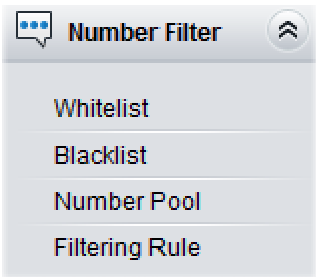


Figure 3-72 Number Filter Interface

3.9.1 Whitelist

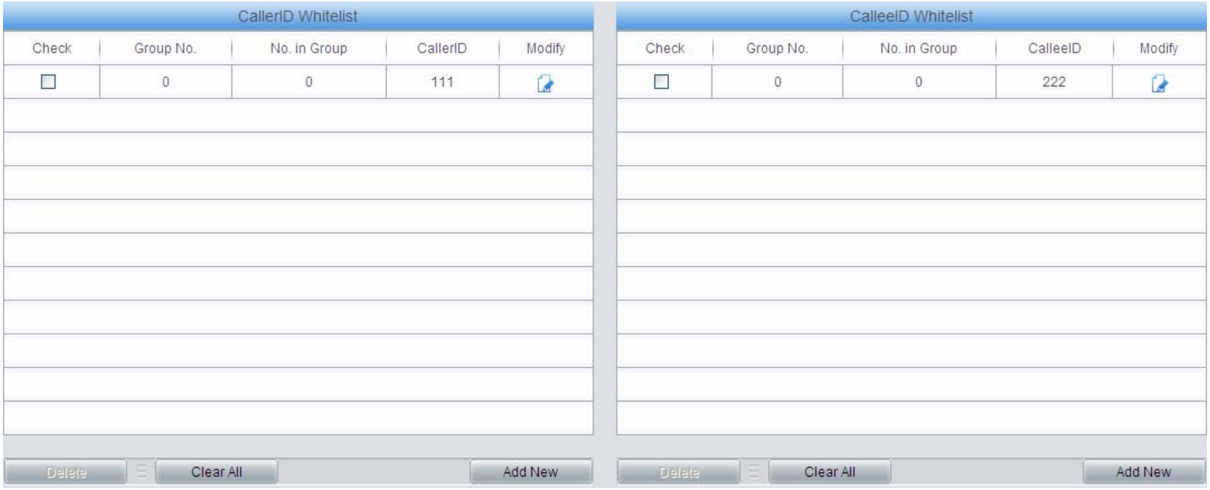


Figure 3-73 Whitelist Setting Interface

See Figure 3-73 for the Whitelist Setting Interface, which includes two parts: ***CallerID Whitelist*** and ***CalleeID Whitelist***.

A new CallerID/CalleeID whitelist can be added by the ***Add New*** button. See Figure 3-74, Figure 3-75 for CallerID/CalleeID whitelist adding interface.

Figure 3-74 Add New CallerIDs in Whitelist Interface

Figure 3-75 Add New CalleeIDs in Whitelist Interface

The table below explains the items shown in above figures.

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

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

Click ***Modify*** in Figure 3-73 to modify the CallerID or CalleeID whitelist. See Figure 3-76, Figure 3-77 for CallerIDs/CalleeIDs on the Whitelist Modification interface. The configuration items on this interface are the same as those on the ***Add New CallerIDs/CalleeIDs in Whitelist*** interface. The item *Group No.* cannot be modified.

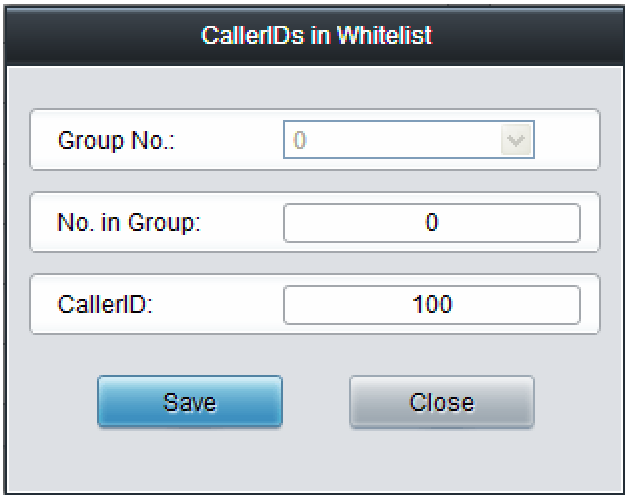


Figure 3-76 Modify CallerIDs in Whitelist

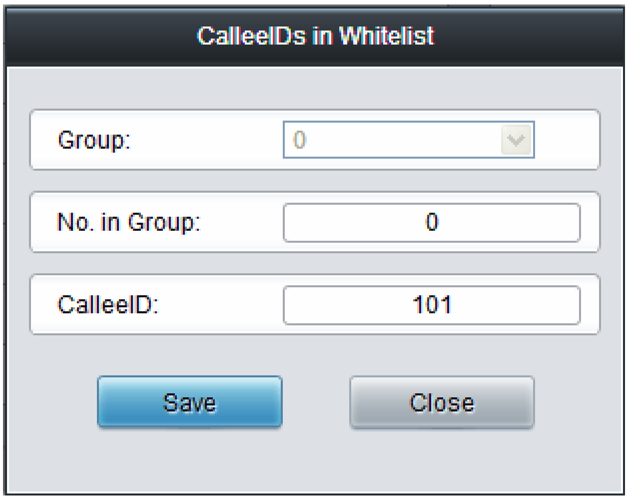


Figure 3-77 Modify CalleeIDs in Whitelist

To delete a CallerIDs/CalleeIDs in the whitelist, check the checkbox before the corresponding index in Figure 3-73 and click the '***Delete***' button. To clear all CallerIDs/CalleeIDs in the whitelist at a time, click the ***Clear All*** button in Figure 3-73.

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

3.9.2 Blacklist

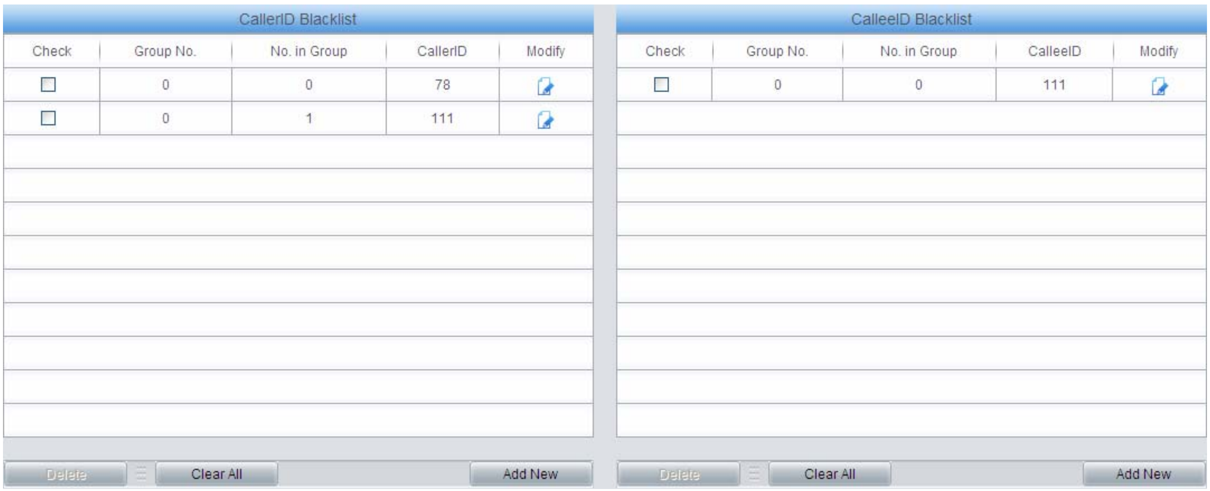


Figure 3-78 Blacklist Setting Interface

The Blacklist Setting interface is almost the same as the Whitelist Setting interface; only the whitelist changes to the blacklist. See Figure 3-78. The configuration items on this interface are the same as those on the Whitelist Setting interface (Figure 3-74, Figure 3-75).

3.9.3 Number Pool

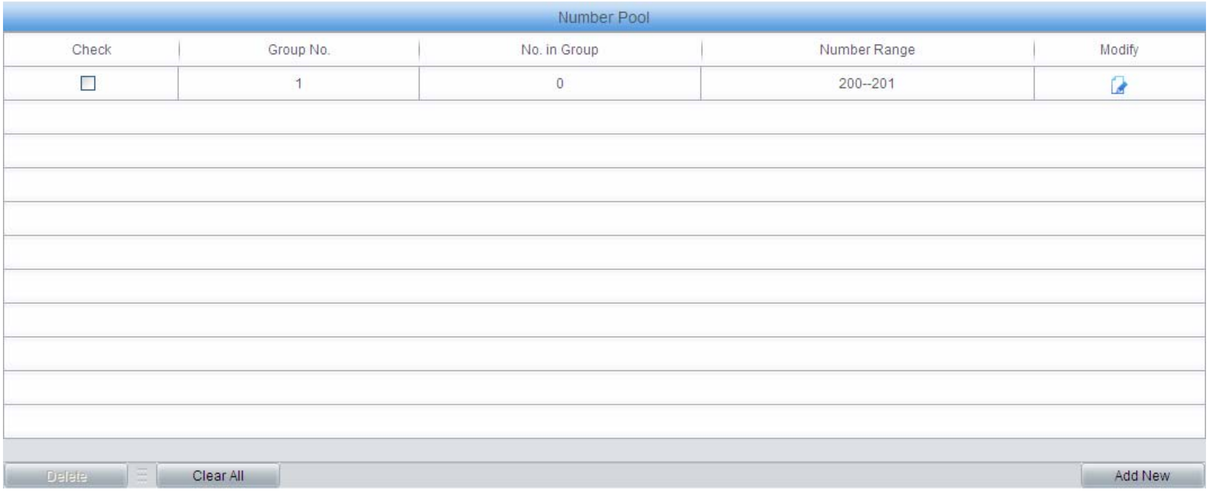


Figure 3-79 Number Pool Setting Interface

See Figure 3-79 for the Number Pool Setting interface. A new number pool can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-80 for the Number Pool adding interface.

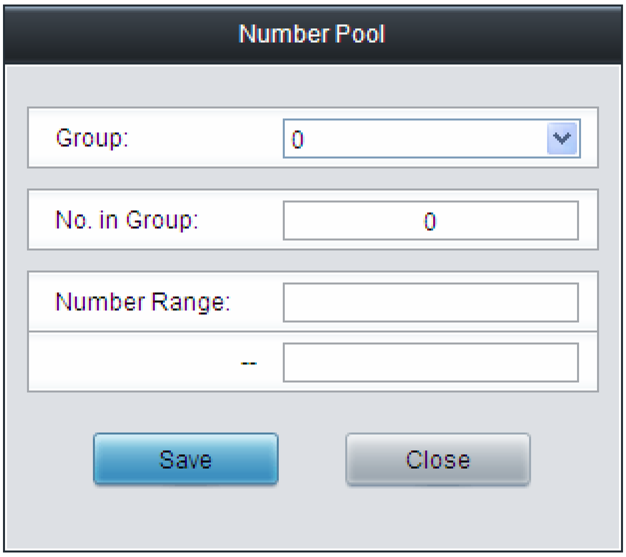


Figure 3-80 Add New Number Pool

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

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

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

Click ***Modify*** in Figure 3-79 to modify the number pool. See Figure 3-81 for the number pool modification interface. The configuration items on this interface are the same as those on the ***Add***

New Number Pool interface.

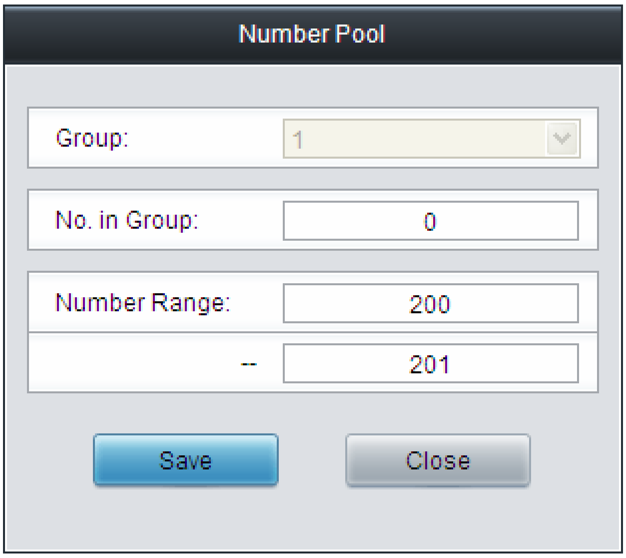


Figure 3-81 Modify Number Pool Interface

To delete a number pool, check the checkbox before the corresponding index in Figure 3-79 and click the '***Delete***' button. To clear all number pools at a time, click the ***Clear All*** button in Figure 3-79.

3.9.4 Filtering Rule

Filtering Rule

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

Delete Clear All Add New

12 Items Total 15 Items/Page 1/1 First Previous Next Last Go to Page 1 1 Pages Total

Figure 3-82 Filtering Rule Setting Interface

See Figure 3-82 for the Filtering Rule Setting Interface. A new filtering rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-83 for the Filtering Rule Adding interface.

Figure 3-83 Add New Filtering Rule

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

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

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

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

Click ***Modify*** in Figure 3-82 to modify the filtering rule. See Figure 3-84 for the filtering rule modification interface. The configuration items on this interface are the same as those on the ***Add New Filtering Rule*** interface.

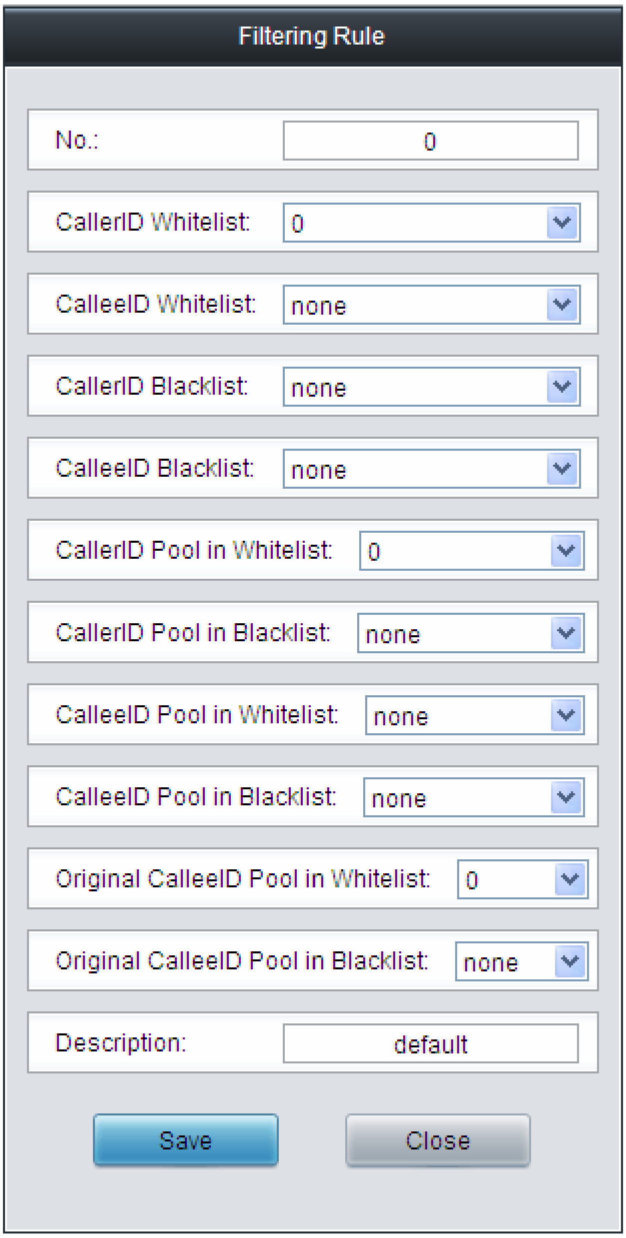


Figure 3-84 Modify Filtering Rule Interface

To delete a filtering rule, check the checkbox before the corresponding index in Figure 3-82 and click the ‘***Delete***’ button. To clear all filtering rules at a time, click the ***Clear All*** button in Figure 3-82.

3.10 Number Manipulation

Number Manipulation includes seven parts: **IP→PSTN CallerID**, **IP→PSTN CalleeID**, **IP→PSTN Original CalleeID**, **PSTN→IP CallerID**, **PSTN→IP CalleeID**, **PSTN→IP Original CalleeID** and **CallerID Pool**. See Figure 3-85.

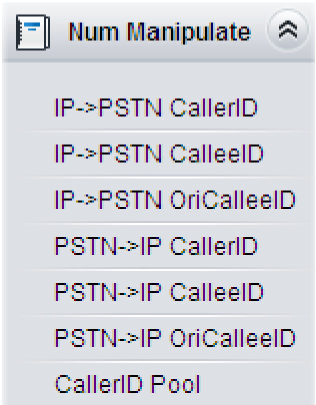


Figure 3-85 Number Manipulation

3.10.1 IP to PSTN CallerID

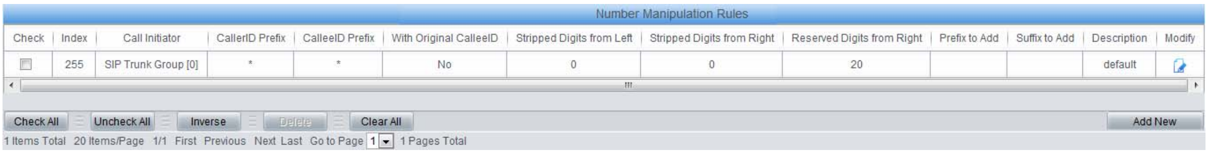


Figure 3-86 IP→PSTN CallerID Manipulation Interface

See Figure 3-86 for the IP→PSTN CallerID manipulation interface. A new number manipulation rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-87 for the IP→PSTN CallerID manipulation rule adding interface.

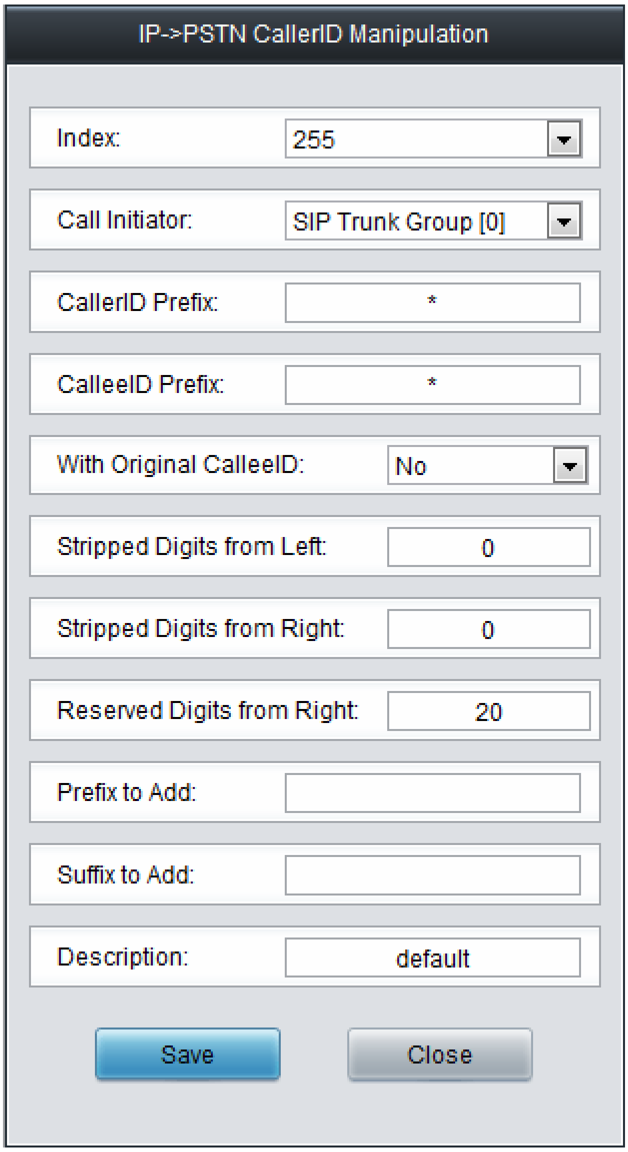


Figure 3-87 Add IP→PSTN CallerID Manipulation Rule

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

Item	Description
Index	The unique index of each number manipulation rule, which denotes its priority. A number manipulation rule with a smaller index value has a higher priority. If a call matches several number manipulation rules, it will be processed according to the one with the highest priority.
Call Initiator	SIP trunk group from where the call is initiated. This item can be set to a specific SIP trunk group or SIP Trunk Group[ANY] which indicates any SIP trunk group.
CallerID Prefix, CalleeID Prefix	A string of numbers at the beginning of the calling/called party number. This item can be set to a specific string or "*" which indicates any string. These two configuration items together with ***Call Initiator*** and ***With Original CalleeID*** can specify the calls which apply to a number manipulation rule. **Note:** Multiple CallerID/CalleeID prefixes can be added simultaneously. They are separated by ":".

With Original CalleeID	If this item is set to *Yes*, it indicates that the number manipulation rule is only applicable to the calls with original CalleeID/redirecting number. The default value is *No*.
Stripped Digits from Left	The amount of digits to be deleted from the left end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted.
Stripped Digits from Right	The amount of digits to be deleted from the right end of the number. If the value of this item exceeds the length of the current number, the whole number will be deleted.
Reserved Digits from Right	The amount of digits to be reserved from the right end of the number. Only when the value of this item is less than the length of the current number will some digits be deleted from left; otherwise, the number will not be manipulated.
Prefix to Add	Designated information to be added to the left end of the current number.
Suffix to Add	Designated information to be added to the right end of the current number.
Description	More information about each number manipulation rule.

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

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

Click ***Modify*** in Figure 3-86 to modify a number manipulation rule. See Figure 3-88 for the IP→PSTN CallerID manipulation rule modification interface. The configuration items on this interface are the same as those on the ***Add IP→PSTN CallerID Manipulation Rule*** interface. Note that the item ***Index*** cannot be modified.

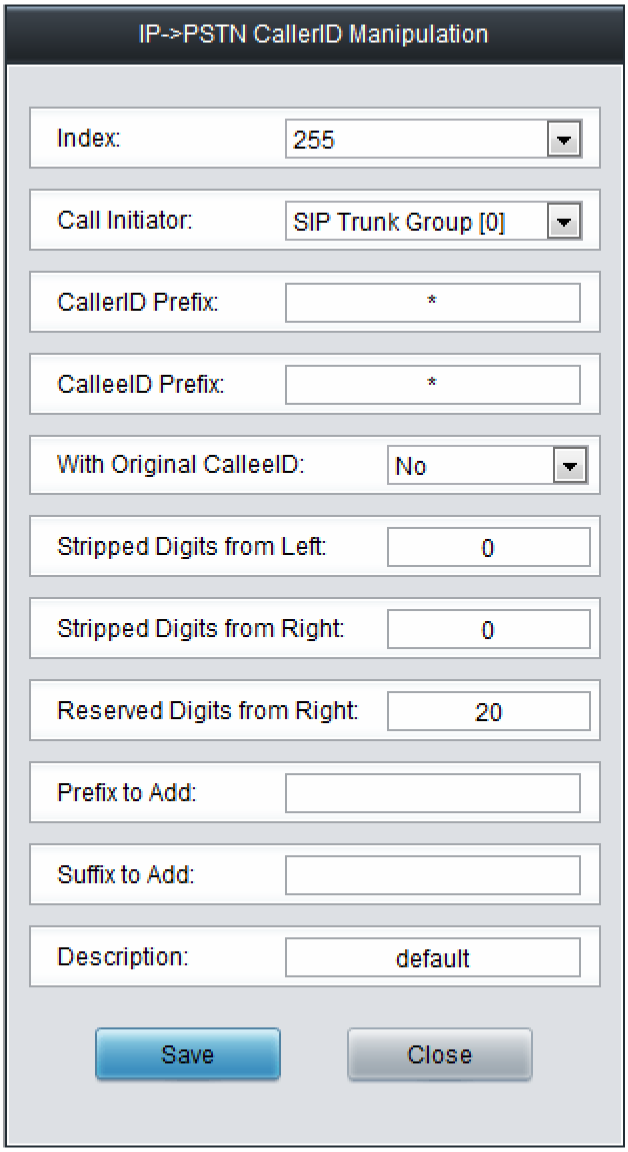


Figure 3-88 Modify IP→PSTN CallerID Manipulation Rule

To delete a number manipulation rule, check the checkbox before the corresponding index in Figure 3-86 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all number manipulation rules at a time, click the ***Clear All*** button in Figure 3-86.

3.10.2 IP to PSTN CalleeID

The number manipulation process for IP→PSTN CalleeID is almost the same as that for IP→PSTN CallerID; only the number to be manipulated changes from CallerID to CalleeID. See Figure 3-89 for IP→PSTN CalleeID manipulation interface. The configuration items on this interface are the same as those on ***IP→PSTN CallerID Manipulation Interface*** (Figure 3-86).

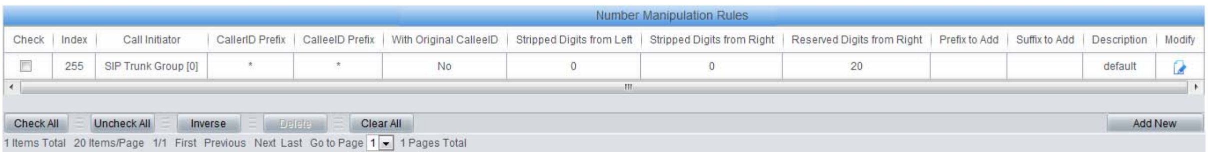


Figure 3-89 IP→PSTN CalleeID Manipulation Interface

3.10.3 IP to PSTN Original CalleeID

The number manipulation process for IP→PSTN Original CalleeID is almost the same as that for IP→PSTN CallerID; only the number to be manipulated changes from CallerID to Original CalleeID. See Figure 3-90 for IP→PSTN Original CalleeID manipulation interface. The configuration items on this interface are the same as those on ***IP→PSTN CallerID Manipulation Interface*** (Figure 3-86).

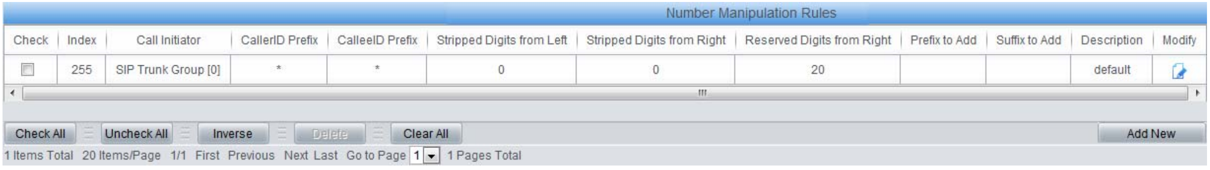


Figure 3-90 IP→PSTN Original CalleeID Manipulation Interface

3.10.4 PSTN to IP CallerID

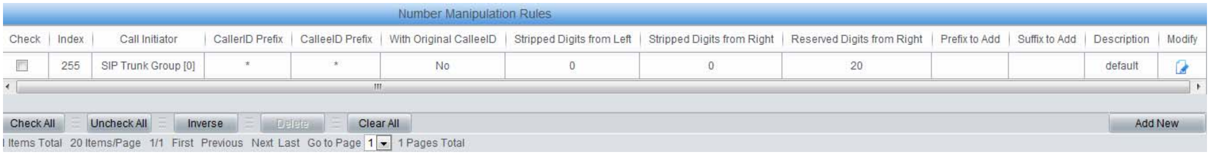


Figure 3-91 PSTN→IP CallerID Manipulation Interface

See Figure 3-91 for the PSTN→IP CallerID manipulation interface. A new number manipulation rule can be added by the ***Add New*** button on the bottom right corner of the list in the above figure. See Figure 3-92 for the PSTN→IP CallerID manipulation rule adding interface.

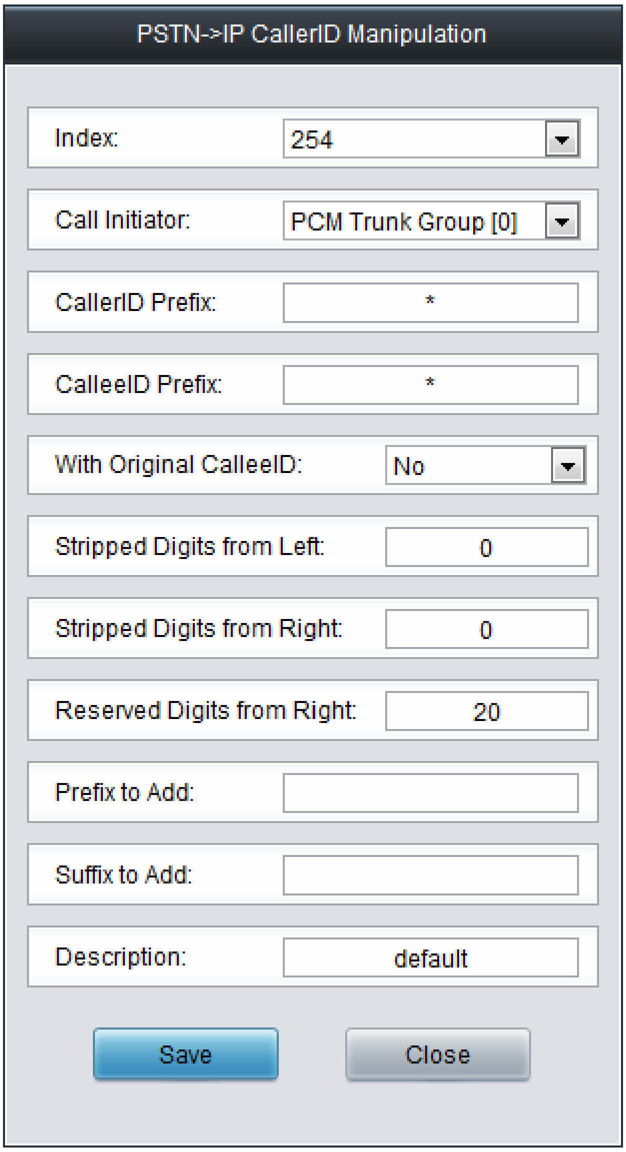


Figure 3-92 Add PSTN→IP CallerID Manipulation Rule

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

Item	Description
Index	The unique index of each number manipulation rule, which denotes its priority. A number manipulation rule with a smaller index value has a higher priority. If a call matches several number manipulation rules, it will be processed according to the one with the highest priority.
Call Initiator	PCM trunk group from where the call is initiated. This item can be set to a specific PCM trunk group or PCM Trunk Group[ANY] which indicates any PCM 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 the 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*** in Figure 3-91 to modify a number manipulation rule. See Figure 3-93 for the PSTN→IP CallerID manipulation rule modification interface. The configuration items on this interface are the same as those on the ***Add PSTN→IP CallerID Manipulation Rule*** interface. Note that the item ***Index*** cannot be modified.

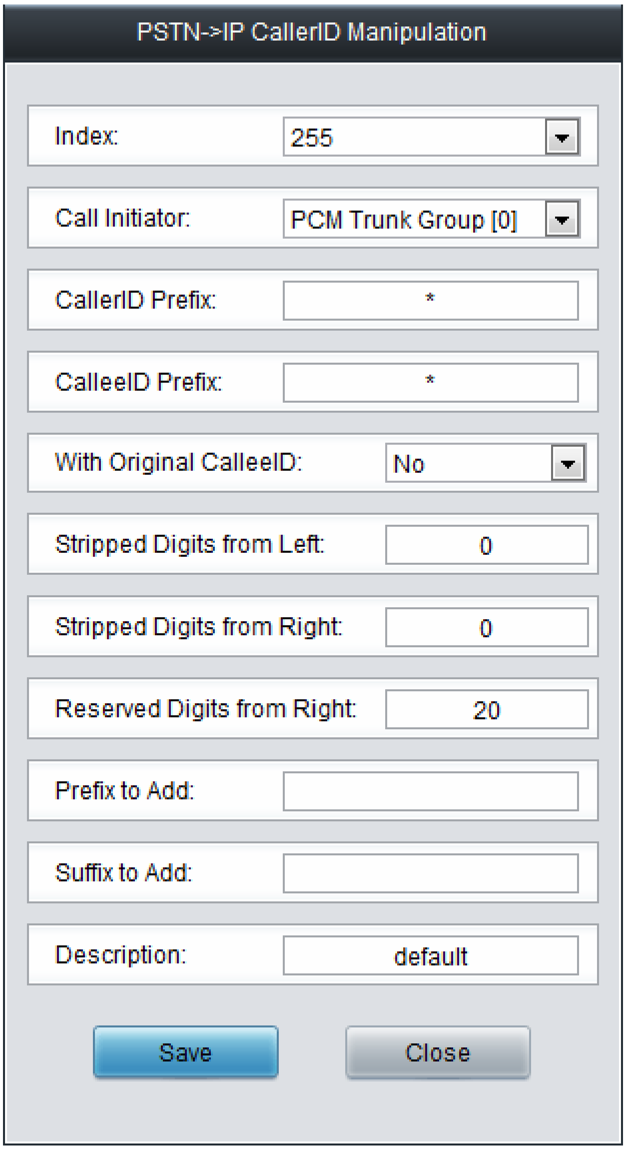


Figure 3-93 Modify PSTN→IP CallerID Manipulation Rule

To delete a number manipulation rule, check the checkbox before the corresponding index in Figure 3-91 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all number manipulation rules at a time, click the ***Clear All*** button in Figure 3-91.

3.10.5 PSTN to IP CalleeID

The number manipulation process for PSTN→IP CalleeID is almost the same as that for PSTN→IP CallerID; only the number to be manipulated changes from CallerID to CalleeID. See Figure 3-94 for the PSTN→IP CalleeID manipulation interface. The configuration items on this interface are the same as those on ***PSTN→IP CallerID Manipulation Interface*** (Figure 3-91).

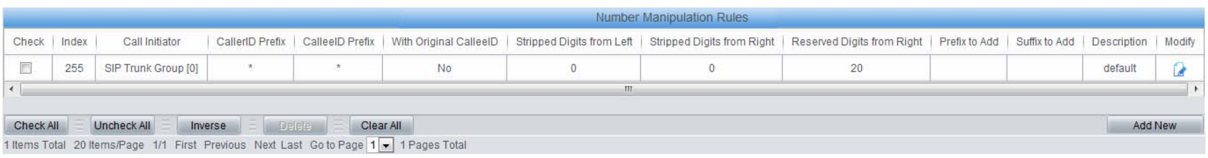


Figure 3-94 PSTN→IP CalleeID Manipulation Interface

3.10.6 PSTN to IP Original CalleeID

The number manipulation process for PSTN→IP Original CalleeID is almost the same as that for PSTN→IP CallerID; only the number to be manipulated changes from CallerID to Original CalleeID. See Figure 3-95 for the PSTN→IP Original CalleeID manipulation interface. The configuration items on this interface are the same as those on ***PSTN→IP CallerID Manipulation Interface*** (Figure 3-91).

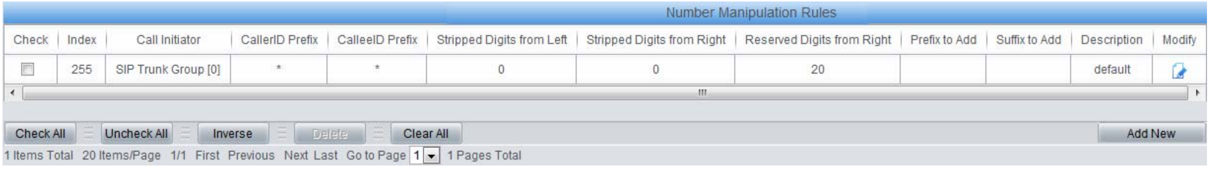


Figure 3-95 PSTN→IP Original CalleeID Manipulation Interface

3.10.7 CallerID Pool

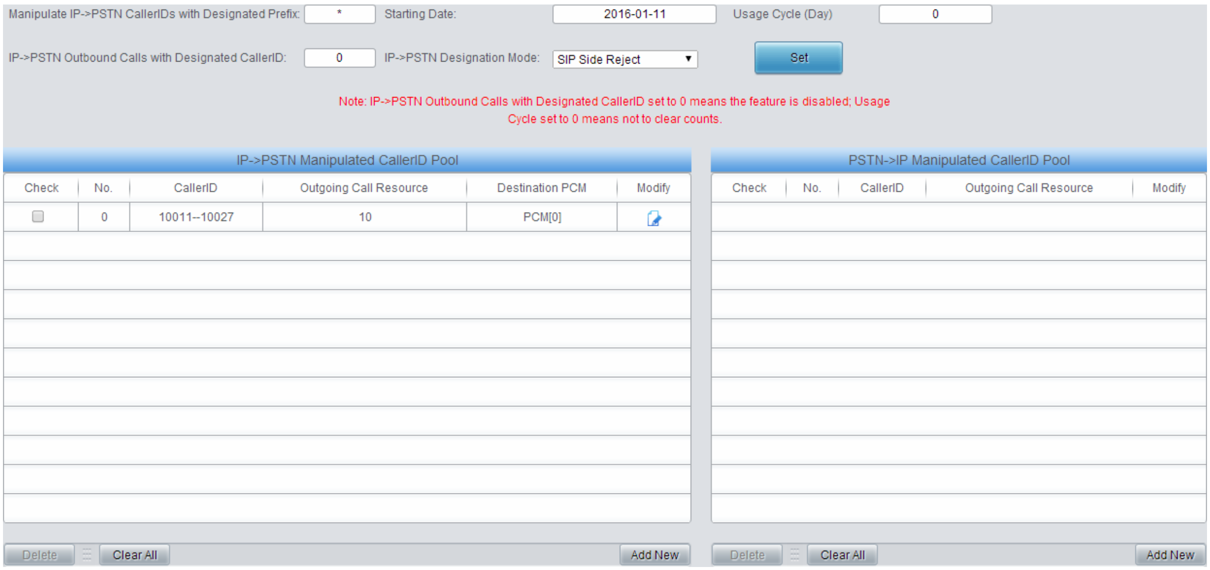


Figure 3-96 CallerID Pool Interface

See Figure 3-96 for the CallerID Pool interface, including two parts: PSTN→IP Manipulated CallerID Pool and IP→PSTN Manipulated CallerID Pool. It is used to designate the CallerID for outgoing calls and restrict the call amount for each designated callerID at the same time. If it is set to manipulate IP→PSTN CallerIDs with the designated prefix, only those calls with the CallerID prefix set in the CallerID pool meeting the requirement can be able to go out. The item *Manipulate IP→PSTN CallerIDs with Designated Prefix* can not be left empty. By default it is set to "*", that is, calls with any CallerID prefix can go out. A new CallerID can be added by the ***Add New*** button. See Figure 3-97 for the CallerID adding interface.

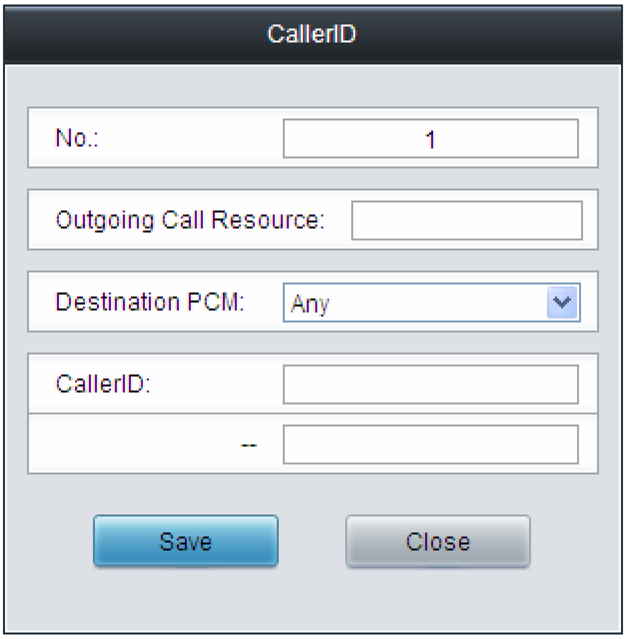


Figure 3-97 Add New CallerID Interface

The table below explains the items shown in above figures.

Item	Description
IP→PSTN Outbound Calls with Designated CallerID	Sets the times of the outbound calls for the numbers in IP→PSTN CallerID Pool.
Starting Date	Sets the starting time to start the IP→PSTN Outbound Calls with Designated CallerID.
Usage Cycle	Sets the execution cycle when the feature of IP→PSTN Outbound Calls with Designated CallerID is enabled.
IP→PSTN Designation Mode	Sets a mode for an IP→PSTN outbound call after all the IP→PSTN outbound calls within the Usage Cycle reach the designated times, two options available: Sip Side Reject and Designated CallerID.
Set Spare CallerID	Sets the space CallerId for an outbound call. **Note:** This item is only valid when IP →PSTN Designation Mode is set to Designated CallerID.
No.	The unique index of the CallerID in the pool, which starts from 0 and denotes its priority. A CallerID with a smaller index value has a higher priority.
Outgoing Call Resource	Sets the maximum number of the outgoing calls for each CallerID.
Destination PCM	The calls outgoing from the PCM designated in this item will do the manipulation.
CallerID	Sets the range of the CallerID used for an outgoing call.

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

Click ***Modify*** in Figure 3-96 to modify the CallerID information. See Figure 3-98 for the CallerID modification interface. The configuration items on this interface are the same as those on the ***Add New CallerID*** interface. The item *No.* cannot be modified.

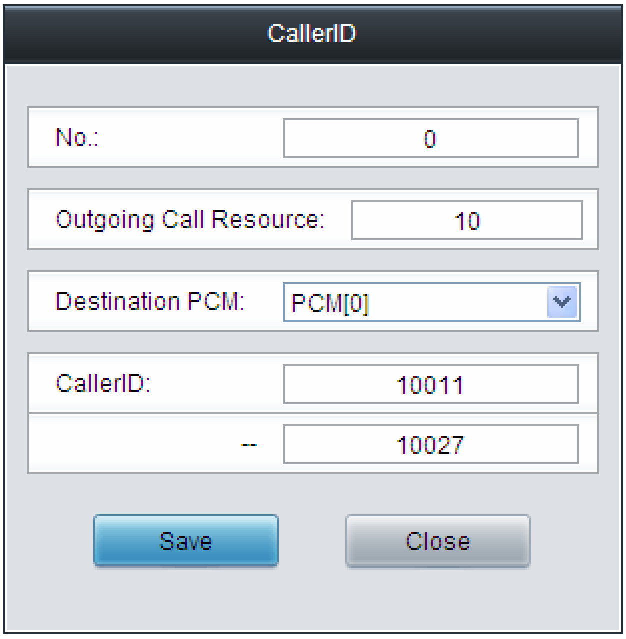


Figure 3-98 Modify CallerID Interface

To delete a CallerID in the pool, check the checkbox before the corresponding index in Figure 3-96 and click the ‘***Delete***’ button. To clear all CallerIDs in the pool at a time, click the ***Clear All*** button in Figure 3-96.

3.11 System Tools

System Tools is mainly for gateway maintenance. It provides such features as IP modification, time synchronization, data backup, log inquiry and connectivity check. See Figure 3-99 for details.

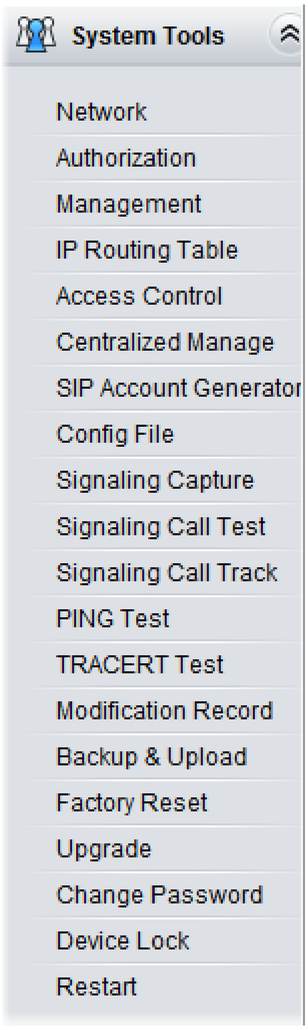


Figure 3-99 System Tools

3.11.1 Network

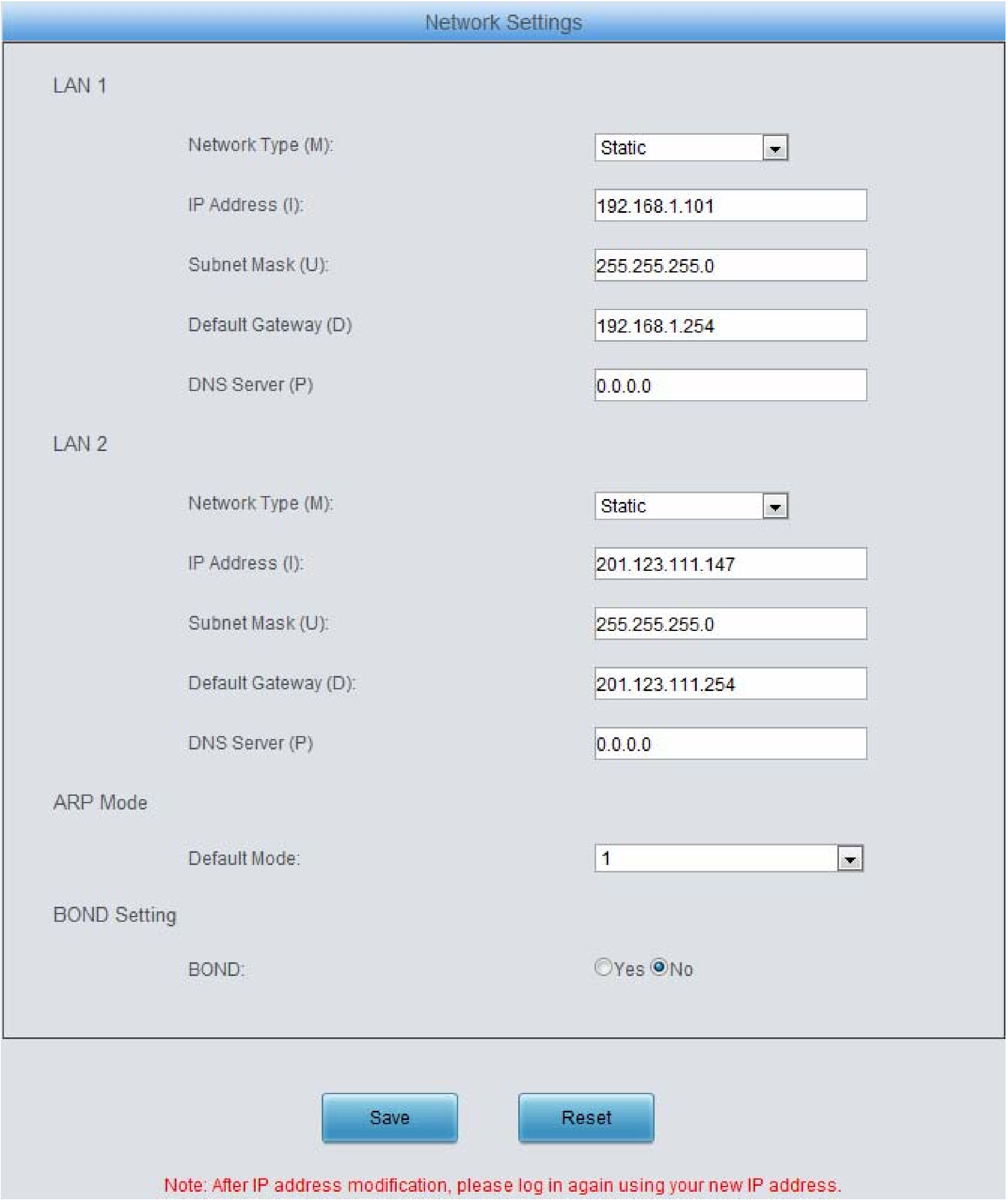


Figure 3-100 Network Settings Interface

See Figure 3-100 for the network settings interface. A gateway has two LANs, each of which can be configured with independent IP address, subnet mask, default gateway and DNS server. The Bond feature when enabled will make the information of LAN1 and LAN2 duplicated and backed up.so as to realize the hot-backup function between LAN1 and LAN2. By default, this feature is *disabled*.

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

2. By default, *Speed and Duplex Mode* is hidden, set to Automatic Detection, you can click 'F' to let it display. We suggest you do not modify it because the non-automatic

detection may cause abnormity in network interface.

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.

3.11.2 Authorization

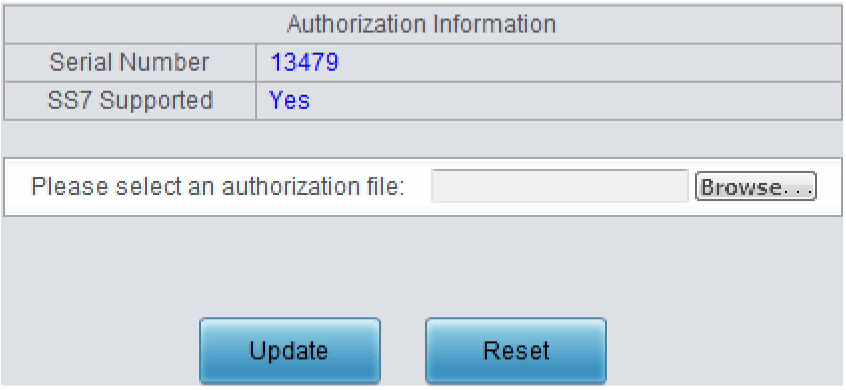


Figure 3-101 Authorization Interface

See Figure 3-101 for the Authorization interface. The SS7 signaling (ISUP and TUP included) can be supported by uploading an authorization file which is provided by our company and cannot be modified by users.

Click ***Browse*** to selset an authorization file, then click the ***Update*** button to upload it. Click ***Reset*** to restore the configurations.

3.11.3 Management

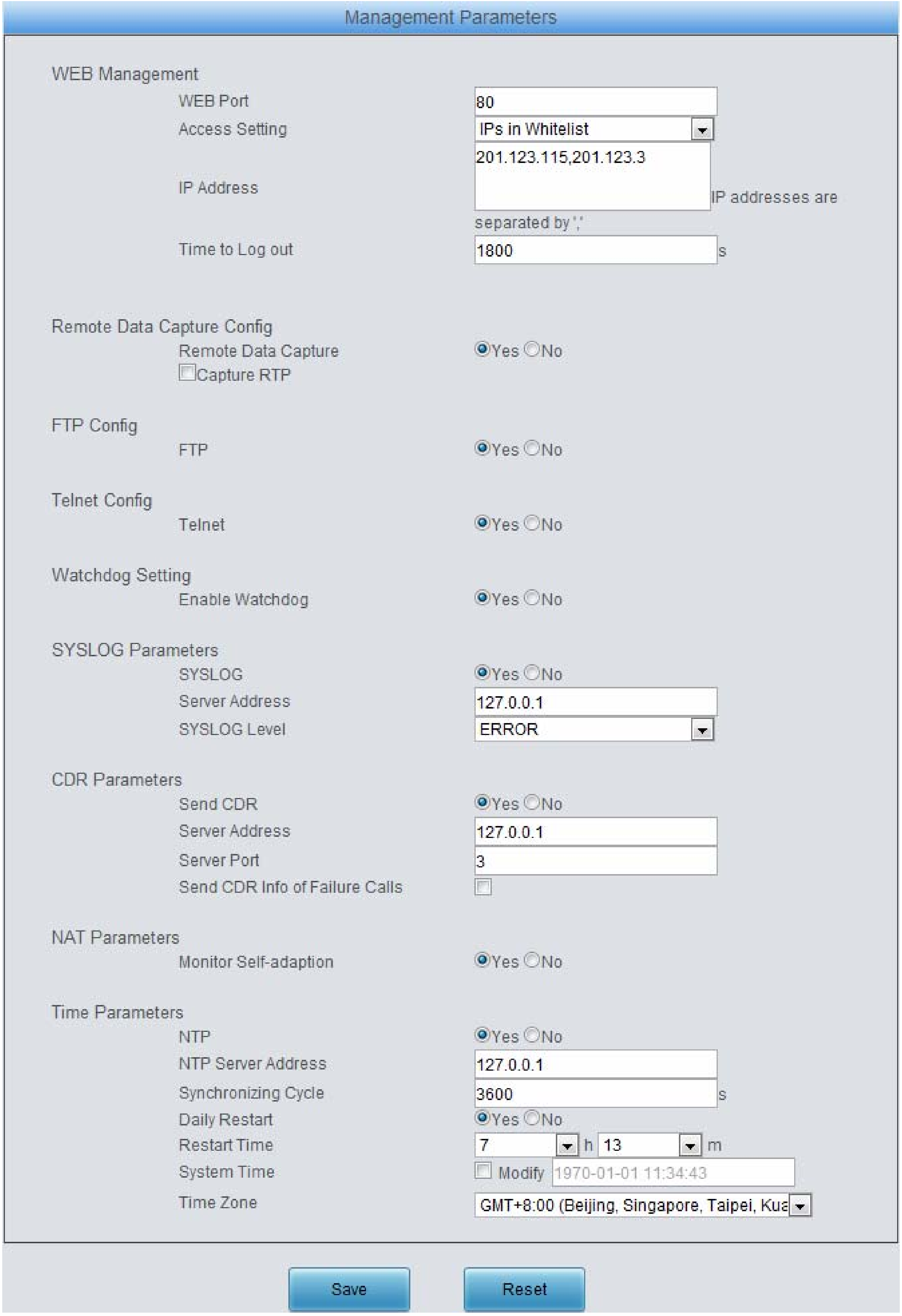


Figure 3-102 Management Parameters Setting Interface

See Figure 3-102 for the Management Parameters Setting interface. The table below explains the items shown in the above figure.

Item	Description
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.
Access Setting	Sets the IP addresses which can access the gateway via WEB. By default, all IPs are allowed. You can set an IP whitelist to allow all 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.
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*.
Telnet	Sets whether to enable the Telnet feature, with the default value of *Yes*. **Note:** By default, this configuration item is hidden. To display or hide it, you should click any part of the interface and press the “F” button.
Enable Watchdog	Sets whether to enable the watchdog feature, with the default value of *Yes*.
SYSLOG	Sets whether to enable SYSLOG. It is required to fill in ***SYSLOG Server Address*** and ***SYSLOG Level*** in case SYSLOG is enabled. By default, ***SYSLOG*** is disabled.
Server Address	Sets the SYSLOG server address for log reception.
SYSLOG Level	Sets the SYSLOG level. There are three options: *ERROR*, *WARNING* and *INFO*.
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 CDR Info of Failure Calls	Once this feature is enabled, the gateway will send the CDR for unsuccessful calls; otherwise, it will only send the CDR data for successful calls.
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.

3.11.4 IP Routing Table

IP Routing Table is used to set the route for the LAN port when two network ports both transport SIP. Thus, the LAN can access some IPs in other different network segment. By default, there is no routing table available on the gateway, click ***Add New*** to add them manually. See Figure 3-103.

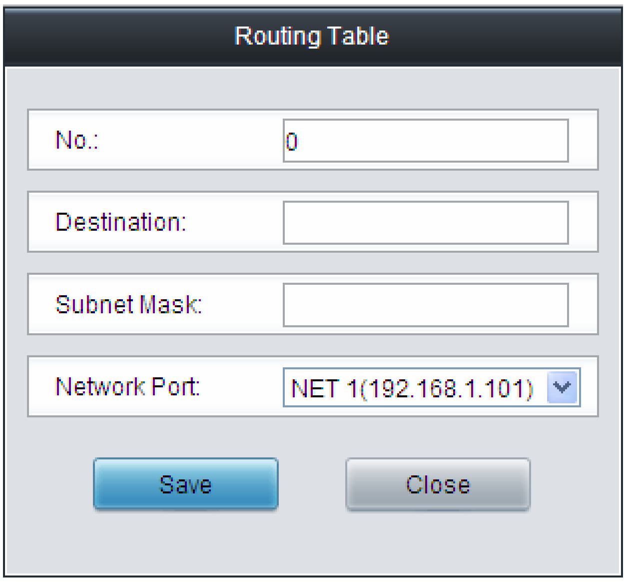


Figure 3-103 Routing Table Adding Interface

The table below explains the items shown in above figures.

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

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-104 for the Routing Table List.

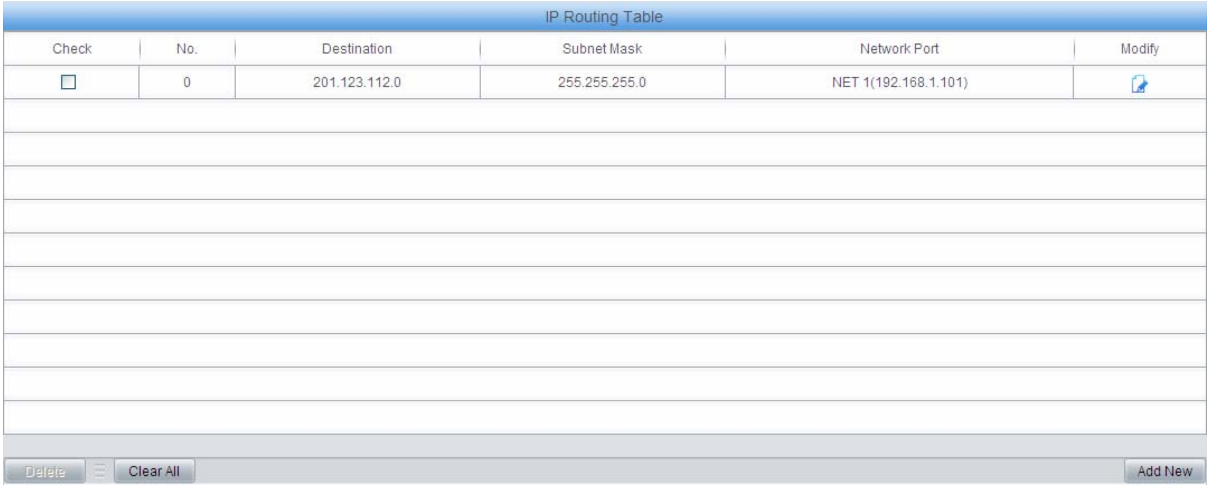


Figure 3-104 Routing Table List

Click ***Modify*** in Figure 3-104 to modify a routing. See Figure 3-105 for the routing table modification interface. The configuration items on this interface are the same as those on the ***Add Routing Table*** interface. Note that the item ***No.*** cannot be modified.

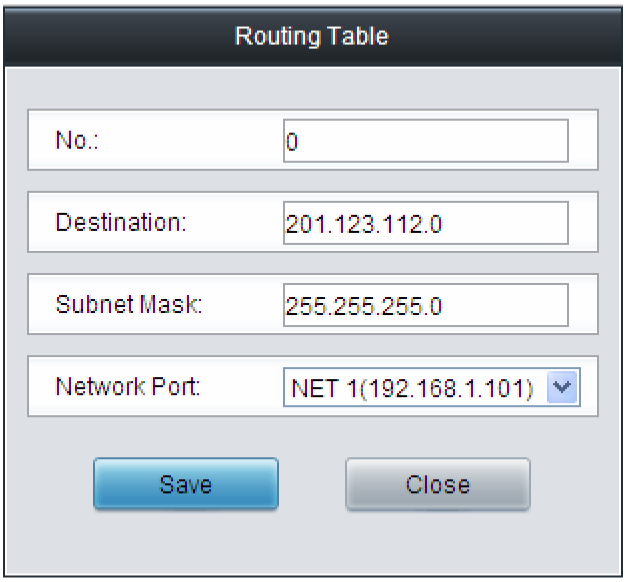


Figure 3-105 Routing Table Modification Interface

To delete a routing, check the checkbox before the corresponding index in Figure 3-104 and click the ***Delete*** button. To clear all routing tables at a time, click the ***Clear All*** button in Figure 3-104.

3.11.5 Access Control

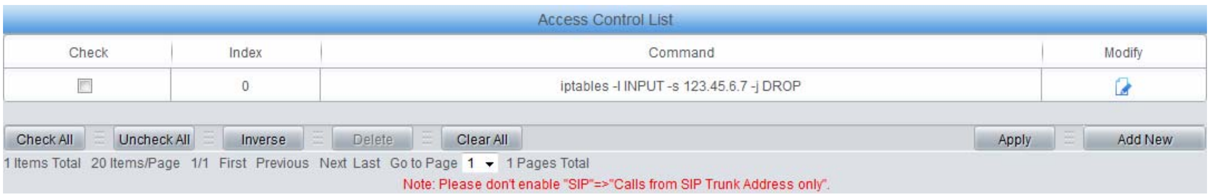


Figure 3-106 Access Control List Interface

See Figure 3-106 for the Access Control List interface. Once you add a piece of command to ACL, the network flow will be restricted, only the particular devices allowed to visit the gateway and only the data packages on the designated ports be forwarded. Click ***Add New*** to add a new piece of command. See Figure 3-107.

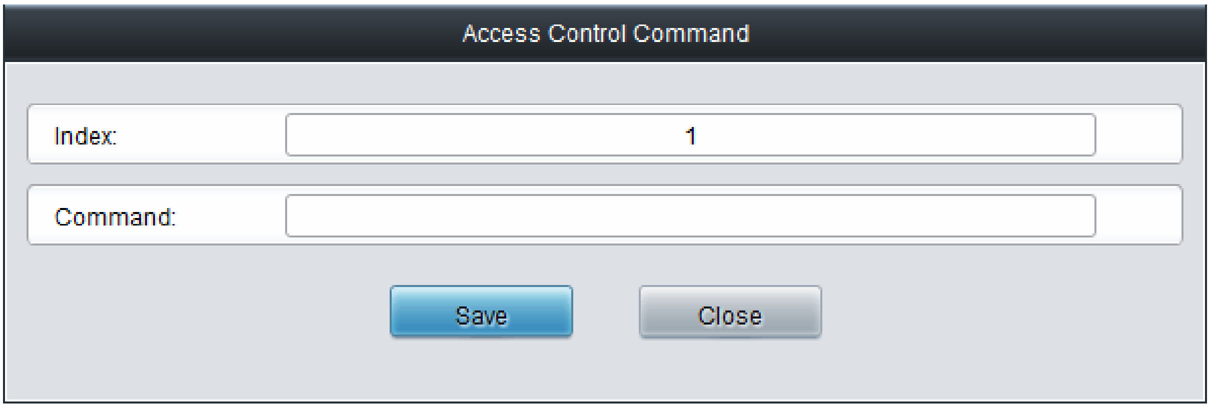


Figure 3-107 Add Access Control Command Interface

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

Click ***Modify*** in Figure 3-106 to modify a command. See Figure 3-108 for the Access Control Command Modification interface. The configuration items on this interface are the same as those on the ***Add Access Control Command*** interface. Note that the item ***Index*** cannot be modified.

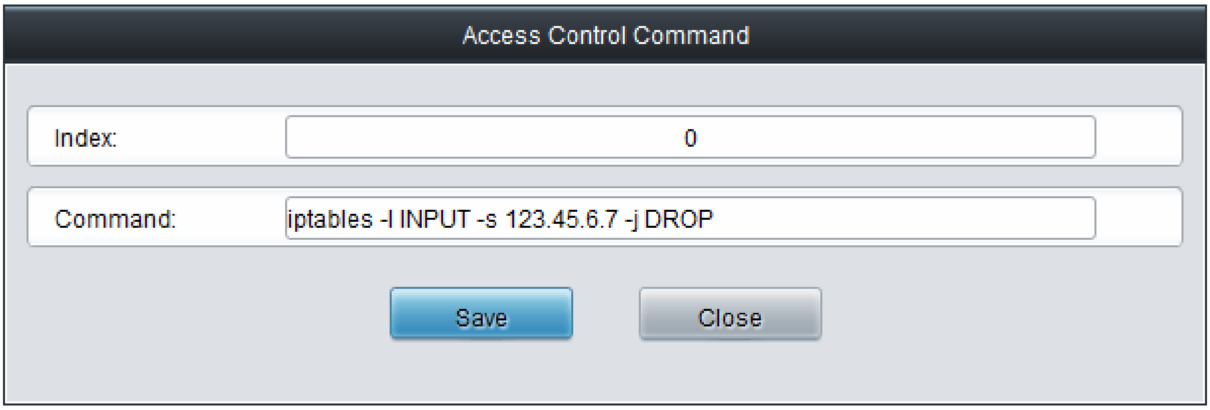


Figure 3-108 Access Control Command Modification Interface

To delete an Access Control Command, check the checkbox before the corresponding index in Figure 3-106 and click the ***Delete*** button, and then click the ***Apply*** button to make the deleted command invalid. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all access control commands at a time, click the ***Clear All*** button in Figure 3-106.

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

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

3.11.6 Centralized Manage

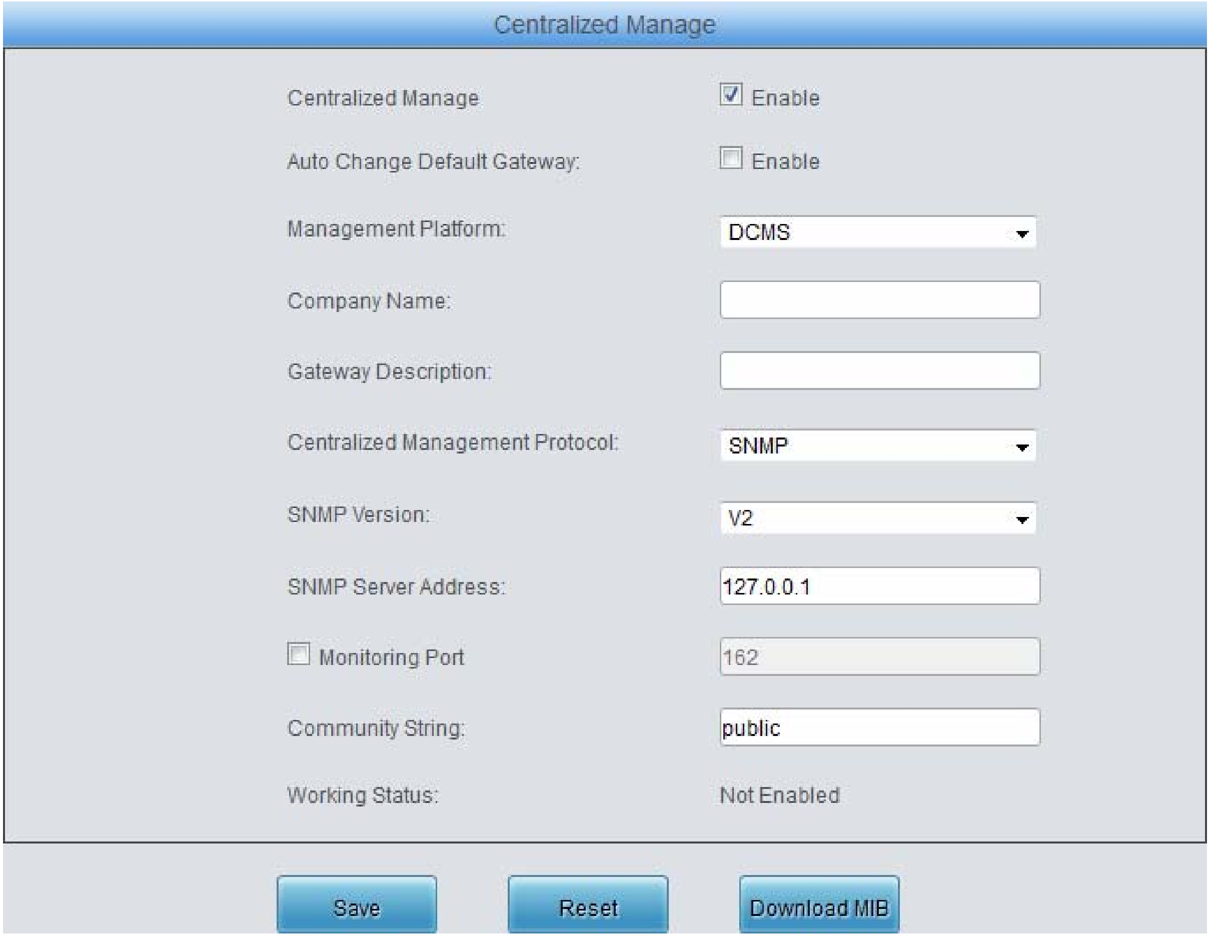


Figure 3-109 Centralized Manage Setting Interface

See Figure 3-109 for the Centralized Manage Setting interface. The gateway can register to a centralized management platform and accept the management of the platform. The table below explains the items shown in above figures.

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

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

3.11.7 SIP Account Generator

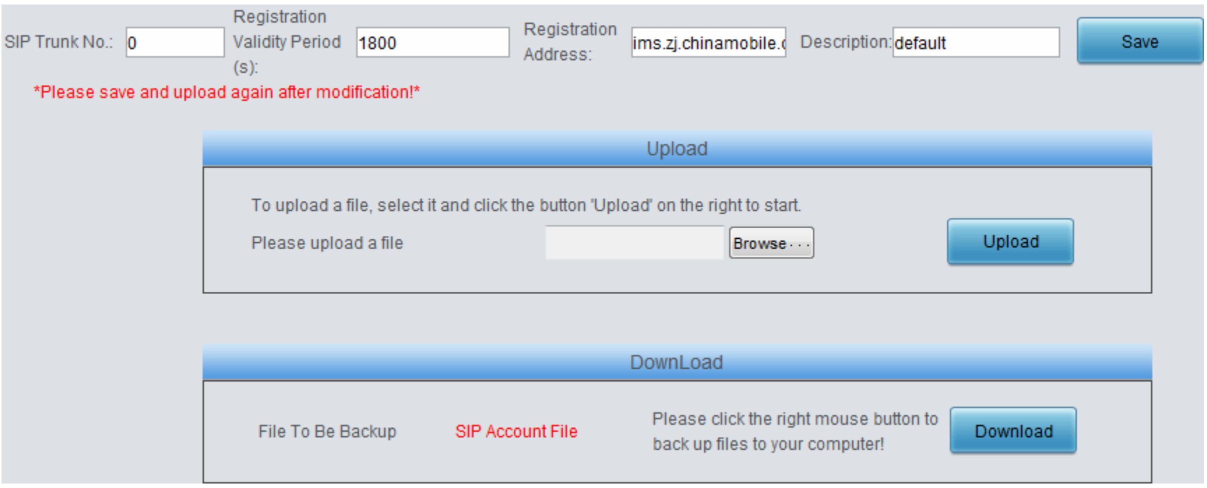


Figure 3-110 SIP Account Generator Interface

See Figure 3-110 for the SIP Account Generator interface. The gateway allows to transform the common SIP account and password to the specific format it supports, upload a file containing the SIP account and password, and modify the SIP Trunk No., Registration Validity Period, Registration Address and Description according to your requirement. Click ***Save*** to save your settings and upload the SIP account source file again. Then the SIP account in the format that the gateway supports will be generated. Click ***Download*** to check the generated SIP account.

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

3.11.8 Configuration File

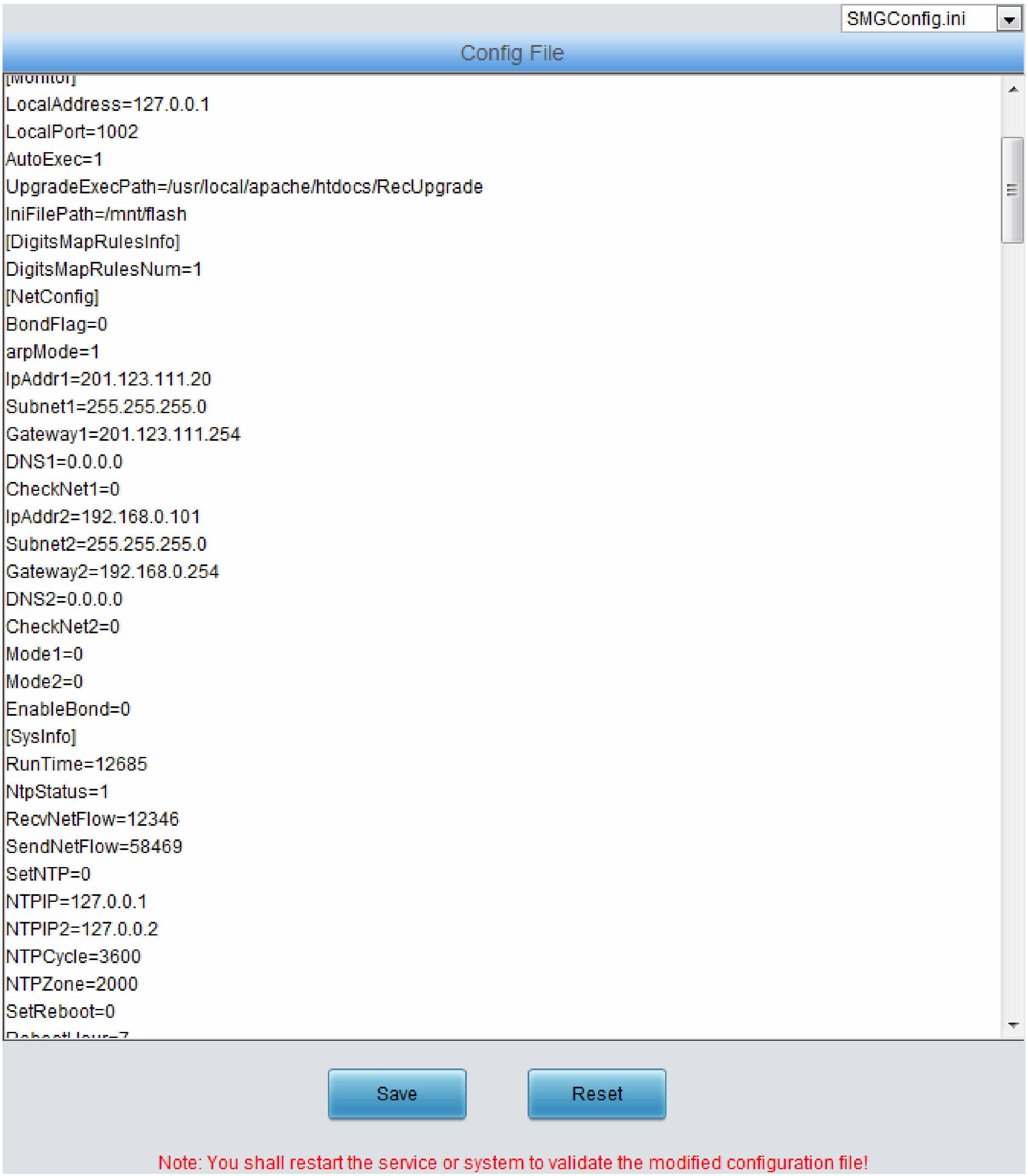


Figure 3-111 Configuration File Interface

See Figure 3-111 for the Configuration File interface, including three files: SMGConfig.ini, ShConfig.ini. You can check and modify the items in these configuration files through this interface. Configurations about the gateway server, such as route rules, number manipulation, number filter and so on, are included in SMGConfig.ini; Configurations about the board are included in ShConfig.ini. You can modify these configurations on the interface directly, and then click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations.

3.11.9 Signaling Capture

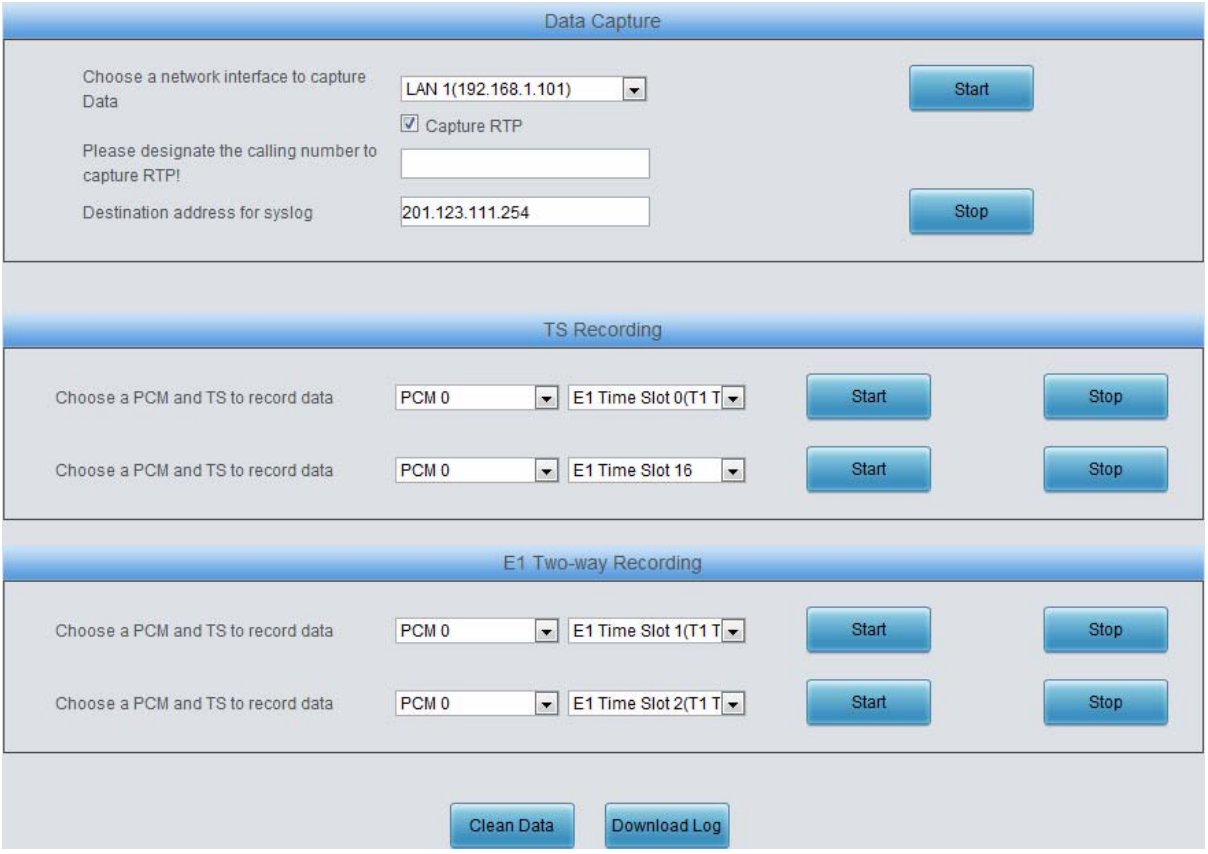


Figure 3-112 Signaling Capture Interface

See Figure 3-112 for the Signaling Capture interface. Data Capture is used to capture data on the network interface you choose. Click ***Start*** to start capturing data (up to 400M for SMG2000 series; up to 800M for SMG3000 series) on the corresponding network interface. SIP, ISDN and SysLog are supported at present. You can enter the Syslog destination address to send Syslog to wherever required. Click ***Stop*** to stop data capture and download the captured packets. Once the option Capture RTP is ticked, you are required to input the calling number of the RTP to be captured.

Data Recording (one-way) and E1 Two-way Recording (two-way) are used to record data on the time slot you choose. Click ***Start*** to start recording data (maximum consecutively recording time: data recording is100 minutes and two-way recording is 1 minutes) on the corresponding port and time slot. Click ***Stop*** to stop data recording and download the recorded data.

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

3.11.10 Signaling Call Test

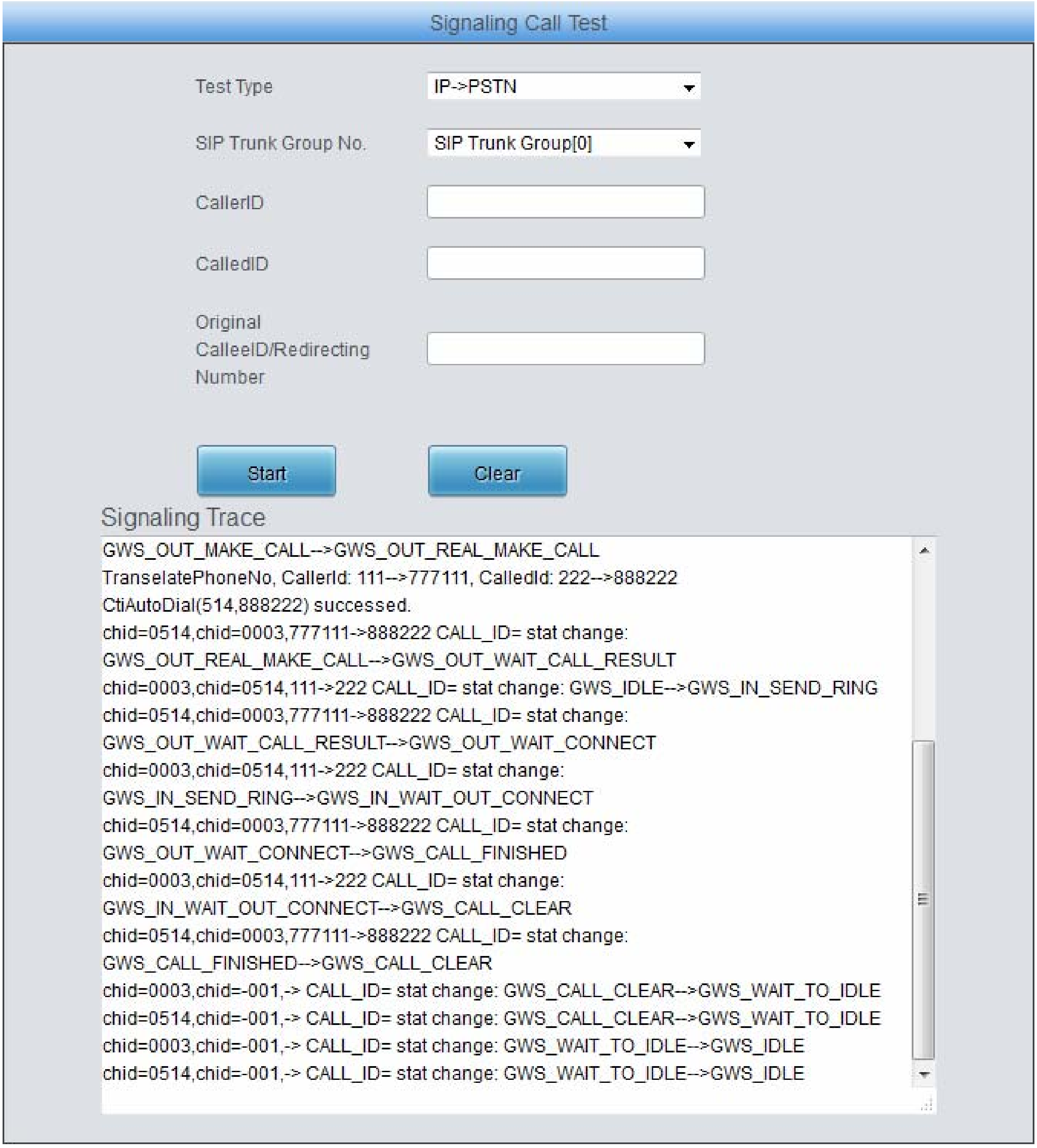


Figure 3-113 Signaling Call Test Interface

See Figure 3-113 for the Signaling Call Test interface. This feature can help to test whether the route and the number manipulation already configured are proper or not, and whether the call can succeed or not.

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

Item	Description
Test Type	The source trunk type for signaling call test. There are three options: **IP→PSTN**, **PSTN→IP, PSTN Call Out** and **IP Call Out.**
SIP Trunk Group No.	The SIP trunk group number you are required to select if choosing **IP→PSTN** or **IP Call Out** in **Test Type.**

PCM Trunk Group No.	The PCM trunk group number you are required to select if choosing **PSTN→IP** in **Test Type.**
CallerID	The CallerID for the signaling call test.
CalleeID	The CalleeID for the signaling call test.
Original CalleeID/Redirecting Number	The original CalleeID/Redirecting Number for the signaling call test.
PCM Port	You are required to select the PCM port if choosing **PSTN Call Out** in **Test Type**. **Note:** This item will appear only if you choose **PSTN Call Out** in **Test Type**.
PCM Channel	You are required to select the PCM channel if choosing **PSTN Call Out** in **Test Type**. **Note:** This item will appear only if you choose **PSTN Call Out** in **Test Type**.
Send Generic Number	Sets whether the IAM message will send the generic number or not. **Note:** This item will appear only if you choose **PSTN Call Out** in **Test Type**.
Generic Number Property	Sets the generic number for the IAM message, This configuration item is valid only when the feature of Send Generic Number is enabled.
DTMF	You can select this item to send DTMFs after the establishment of call conversation on the channel for call test, if choosing **PSTN Call Out** or **IP Call Out** in **Test Type**. **Note:** This item will appear only if you choose **PSTN Call Out** or **IP Call Out** in **Test Type**, and RFC2833 is unsupported for **IP Call Out**.
Add Invite Header, Field Name, Field Content	You can add the invite header and its corresponding content if choosing **IP Call Out** in **Test Type**. **Note:** This item will appear only if you choose **IP Call Out** in **Test Type**.
Signaling Trace	The information returned during the signaling call test, helping you to learn the detailed information about the test call.

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

Note: The gateway can stop the testing only when the Test Type is set to PSTN Call Out; otherwise, the call test will not terminate until the called party ends it.

3.11.11 Signaling Call Track

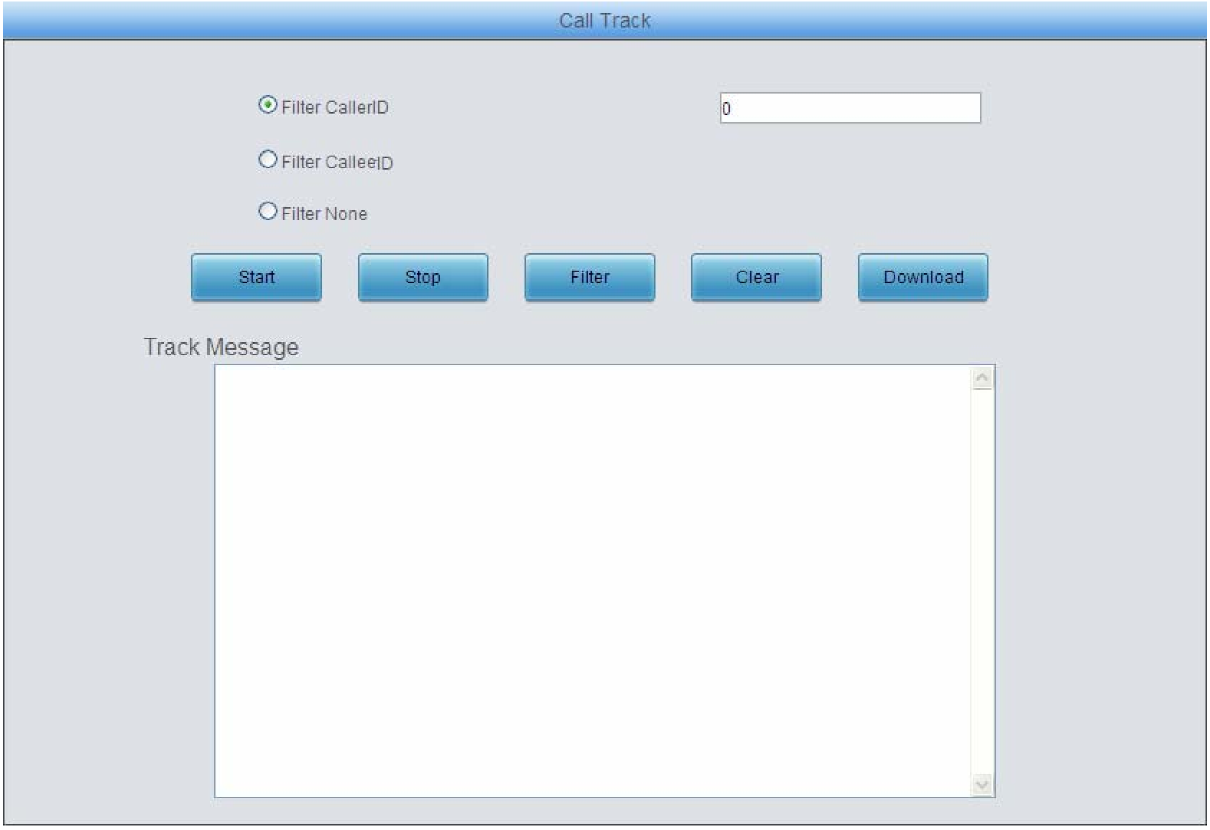


Figure 3-114 Call Track Interface

See Figure 3-114 for the Call Track Interface, including three modes: Filter CallerID, Filter CalleeID and Filter None. This is mainly used to output and save call information, facilitating call trace and problem debugging. Click ***Start*** to track calls, and the trace logs will be shown in the "Track Message" field; click ***Stop*** to stop the call track; click ***Filter*** to filter the trace logs according to the condition you set; click ***Clear*** to clear all trace logs; click ***download*** to download trace logs.

3.11.12 PING Test

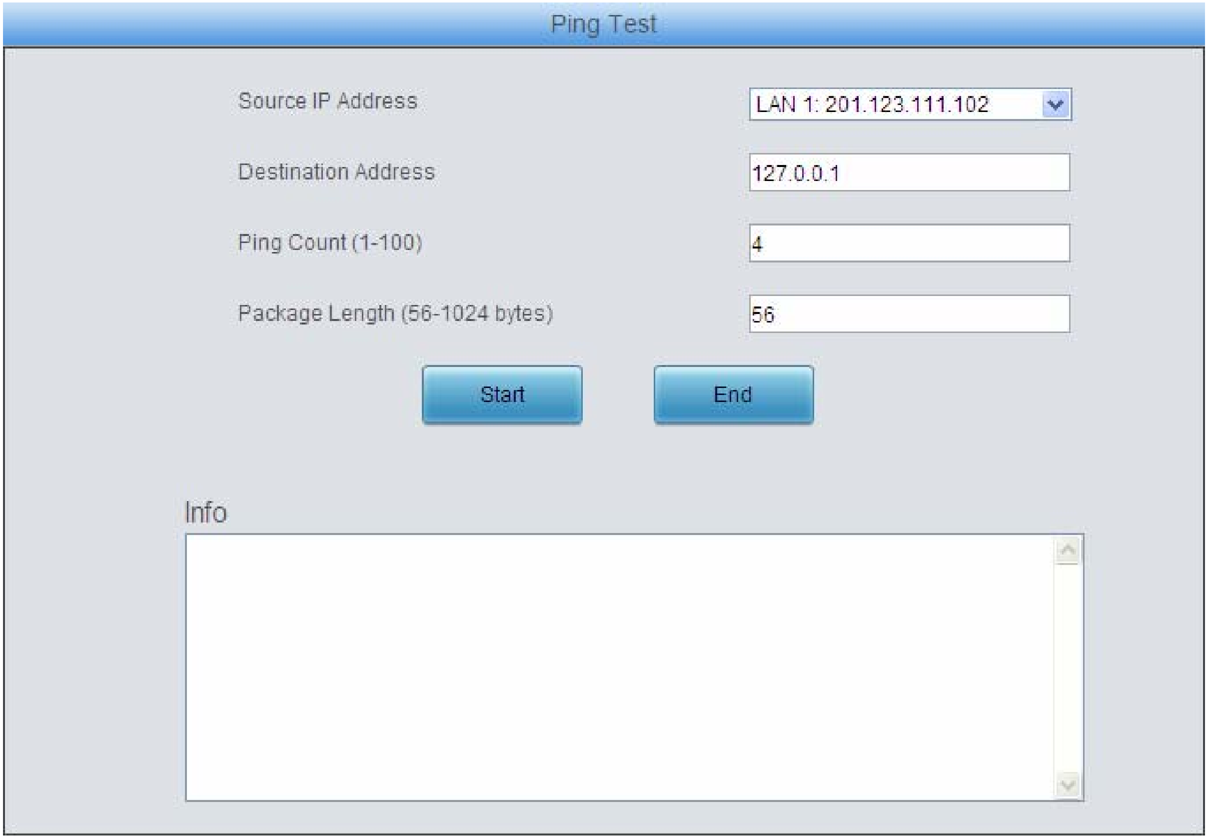


Figure 3-115 Ping Test Interface

See Figure 3-115 for the Ping Test interface. A Ping test can be initiated from the gateway on a designated IP address to check the connection status between them. The table below explains the configuration items shown in the above figure.

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

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

3.11.13 TRACERT Test

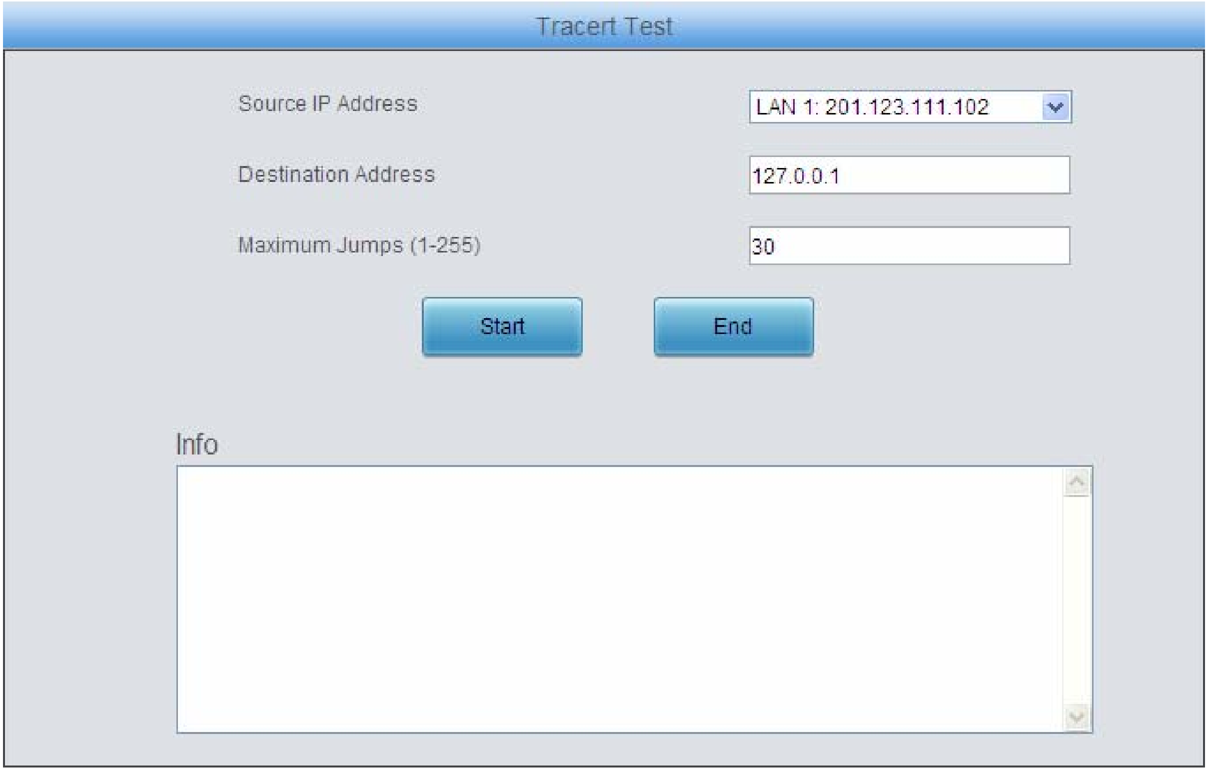


Figure 3-116 Tracert Test Interface

See Figure 3-116 for the Tracert Test interface. A Tracert test can be initiated from the gateway on a designated IP address to check the routing status between them. The table below explains the configuration items shown in the above figure.

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

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

3.11.14 Modification Record

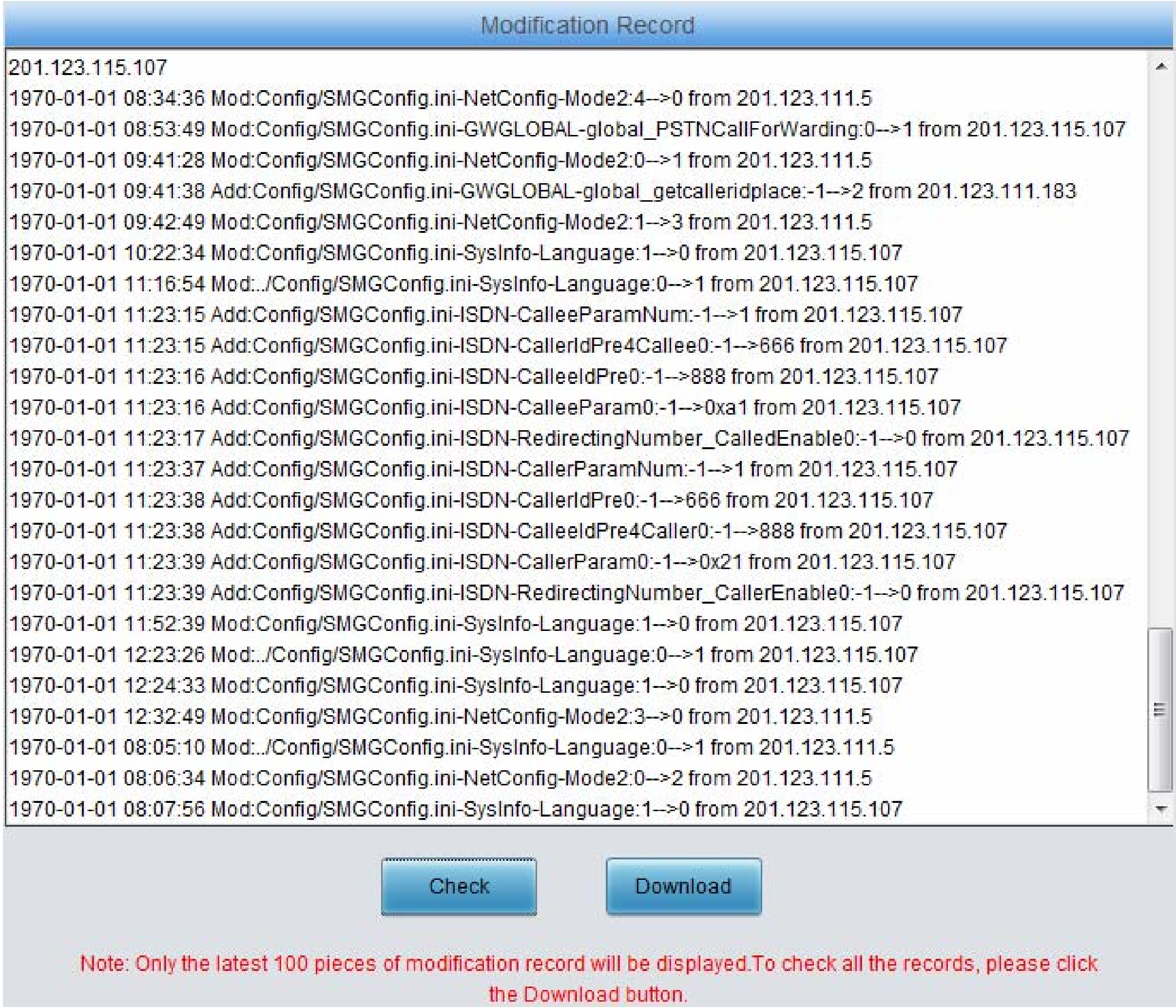


Figure 3-117 Modification Interface

The Modification Record interface is used to check the modification record on the web configuration. Click ***Check*** and the modification record will be shown on the dialog box. See Figure 3-117. Click ***Download*** to download the record file.

3.11.15 Backup & Upload

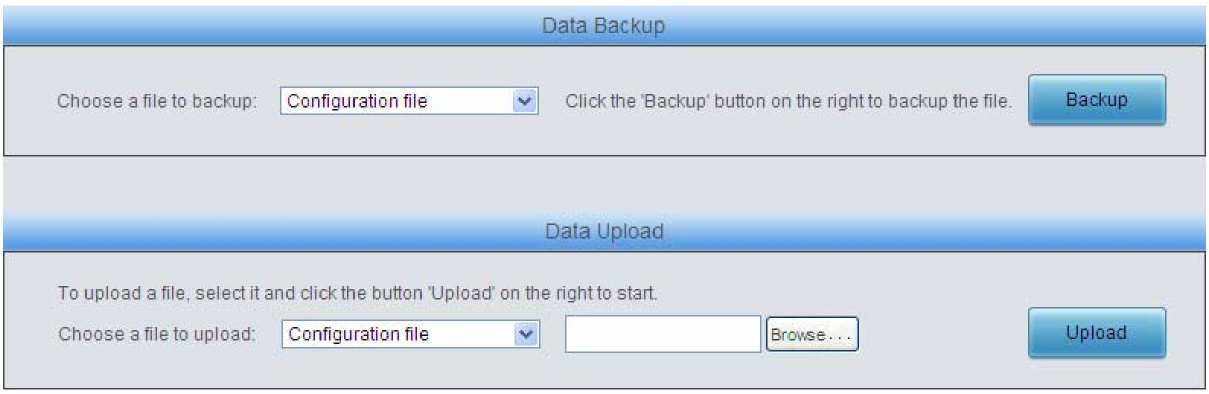


Figure 3-118 Backup & Upload Interface

See Figure 3-118 for the Backup and Upload interface. To back up data to your PC, you shall first choose the file in the pull-down list and then click ***Backup*** to start. To upload a file to the gateway, you shall first choose the file type in the pull-down list, then select it via ***Browse…***, and at last click ***Upload***. The gateway will automatically apply the uploaded data to overwrite the current configurations.

3.11.16 Factory Reset

Figure 3-119 Factory Reset Interface

See Figure 3-119 for the Factory Reset interface. Click ***Reset*** to restore all configurations on the gateway to factory settings.

3.11.17 Upgrade

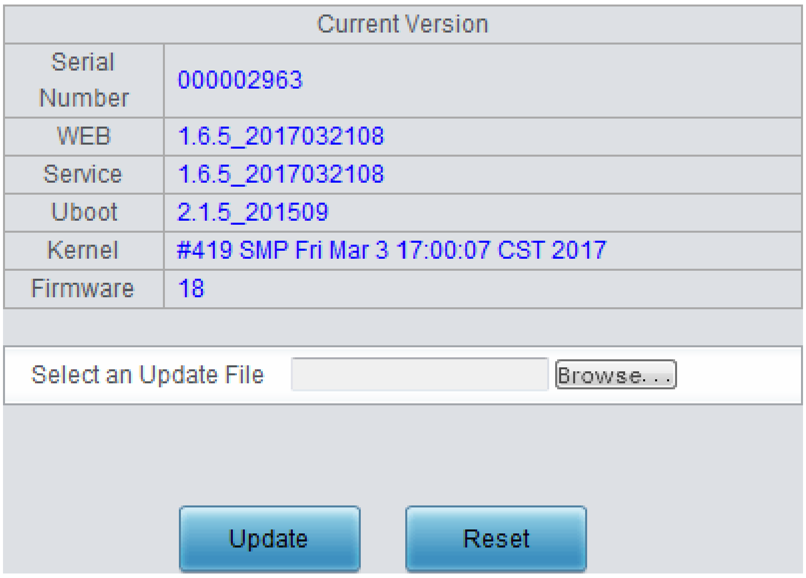


Figure 3-120 Upgrade Interface

See Figure 3-120 for the upgrade interface where you can upgrade the WEB, gateway service, kernel and firmware to new versions. Select the upgrade package "*.tar.gz" via ***Browse…*** and click ***Update*** (The gateway will do MD5 verification before upgrading and will not start to upgrade until it passes the verification). Wait for a while and the gateway will finish the upgrade automatically. Note that clicking ***Reset*** can only delete the selected update file but not cancel the operation of ***Update***.

3.11.18 Change Password

Figure 3-121 Password Changing Interface

See Figure 3-121 for the Password Changing interface where you can change username and password of the gateway. Enter the current password, the new username and password, and then confirm the new password. After configuration, click ***Save*** to apply the new username and password or click ***Reset*** to restore the configurations. After changing the username and password, you are required to log in again.

3.11.19 Device Lock

Figure 3-122 Device Lock Configuration Interface

See Figure 3-122 for the Device Lock Configuration interface. When you select one or more than one conditions to lock the gateway, the configurations of the gateway related to the selected conditions will be locked. That is, to modify any one of those configurations, you are required to input the lock password. Click ***Lock*** after setting and the device lock interface will be locked. To unlock the interface, enter your password (just the lock password) and click the ***Unlock*** button.

Figure 3-123 Unlock Device Interface

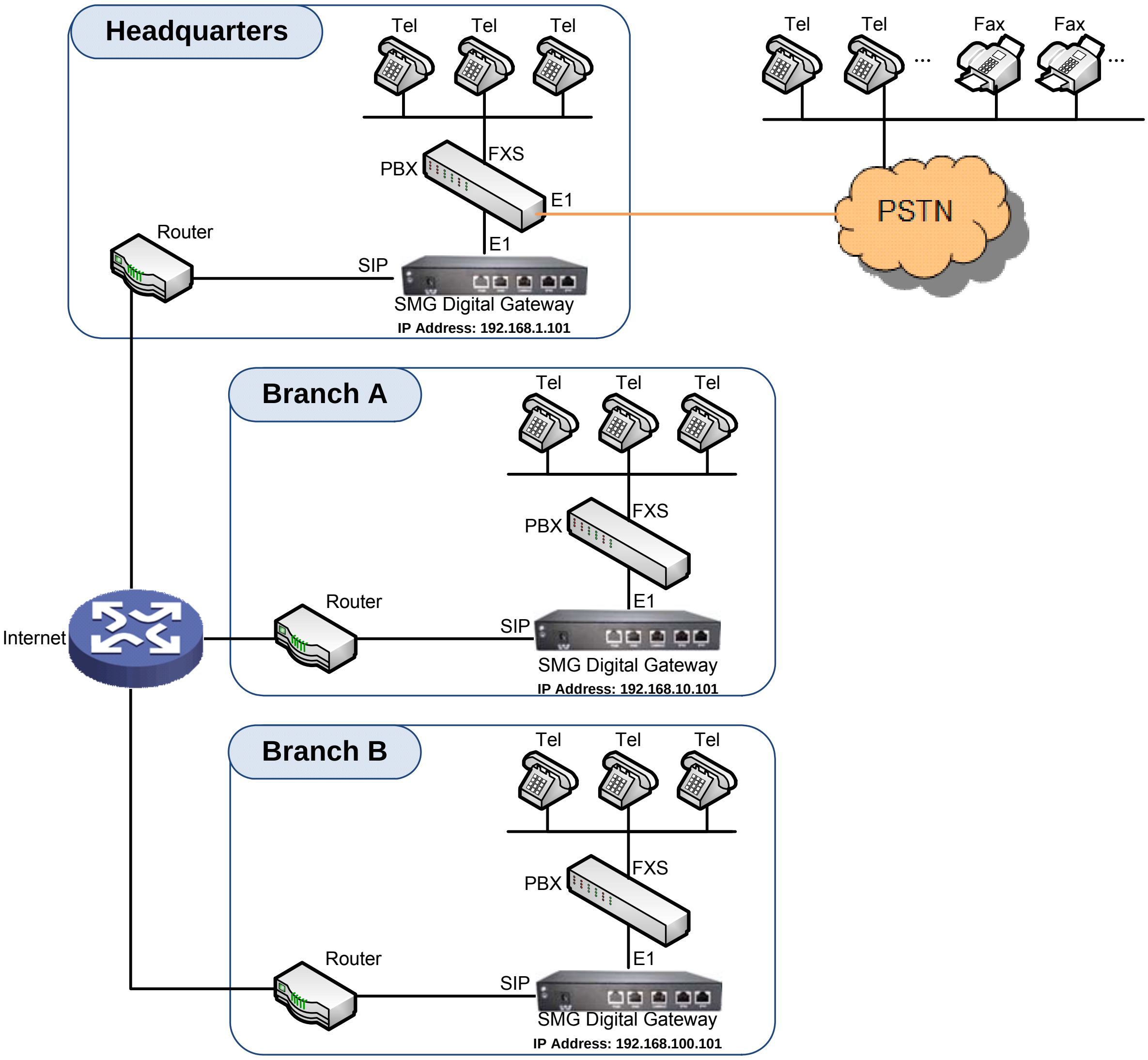
3.11.20 Restart

Figure 3-124 Service/System Restart Interface

See Figure 3-124 for the Restart interface. Click ***Restart*** on the service restart interface to restart the gateway service or click ***Restart*** on the system restart interface to restart the whole gateway system.

Chapter 4 Typical Applications

4.1 Application 1



Note: In this application, we assume that Branch A, Branch B and the headquarter have established VLAN using VPN technology.

Figure 4-1 Application 1

In this application, calls within the enterprise, i.e. calls among the headquarters, Branch A and Branch B, are all carried via SIP without PSTN. Outbound calls from the enterprise are all processed by the PBX at the headquarters. This application provides an enterprise with a unified interface for outbound call communications, and facilitates their call recording management as well.

This section takes SMG2120 as an example and introduces the configurations for the gateway application with the following dialing plan:

Call from the headquarters to Branch A: 8+EXT (extension number)

Call from the headquarters to Branch B: 7+EXT

Make an outbound call from the headquarters: 0+Number

Call from Branch A to the headquarters: 9+EXT

Call from Branch A to Branch B: 7+EXT

Make an outbound call from Branch A: 0+Number

Call from Branch B to the headquarters: 9+EXT

Call from Branch B to Branch A: 8+EXT

Make an outbound call from Branch B: 0+Number

4.1.1 Configurations for Headquarters

1. Configure SIP Settings for the headquarters.

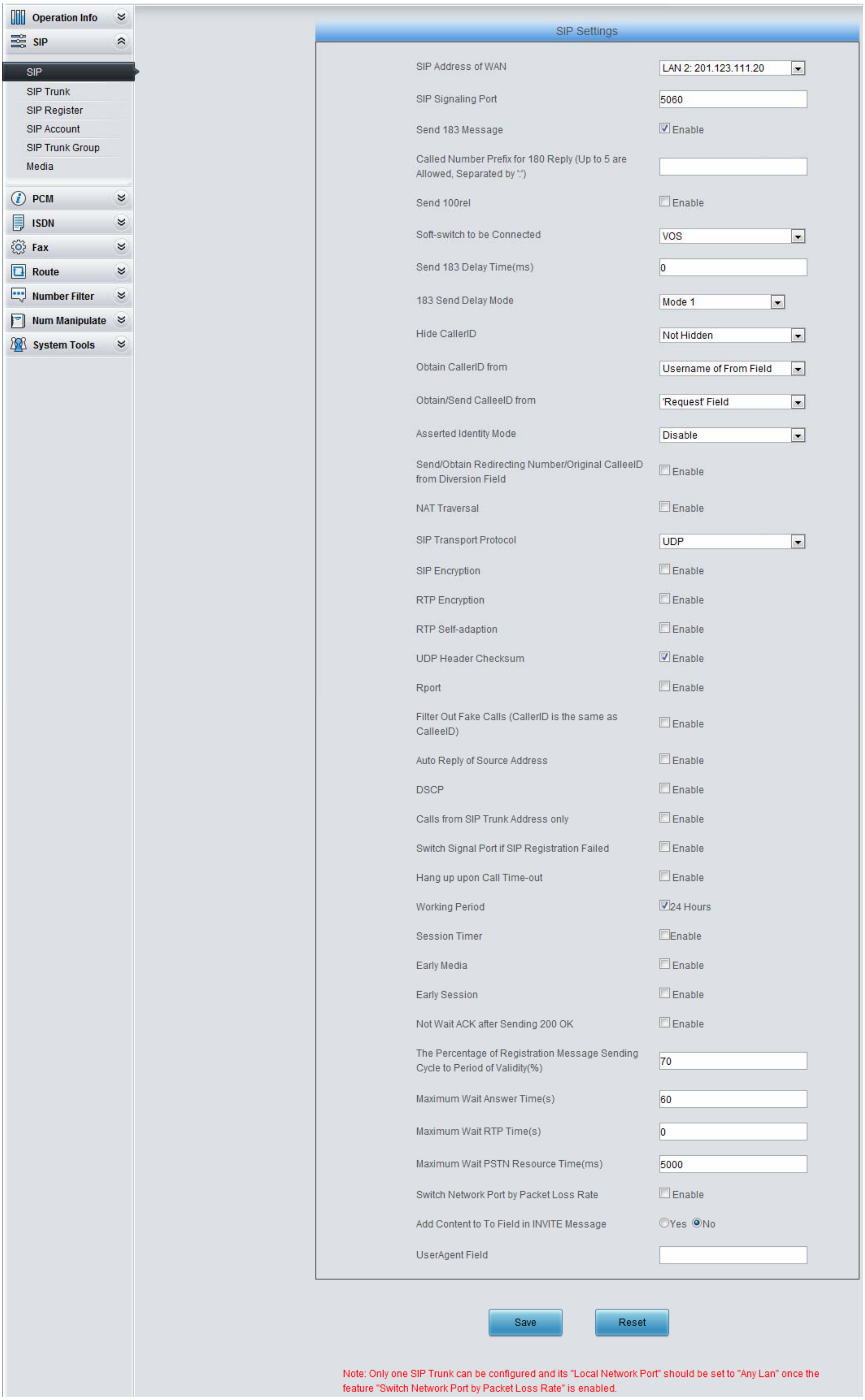
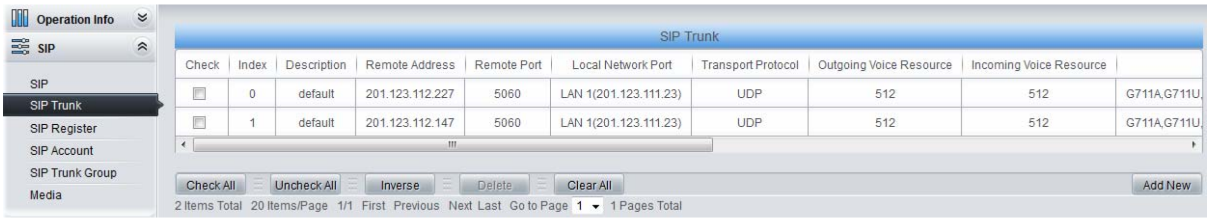

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated by ',')
Send 100rel
Enable
Soft-switch to be Connected
VOS
Send 183 Delay Time(ms)
0
183 Send Delay Mode
Mode 1
Hide CallerID
Not Hidden
Obtain CallerID from
Username of From Field
Obtain/Send CalleeID from
'Request' Field
Asserted Identity Mode
Disable
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field
Enable
NAT Traversal
Enable
SIP Transport Protocol
UDP
SIP Encryption
Enable
RTP Encryption
Enable
RTP Self-adaption
Enable
UDP Header Checksum
Enable
Rport
Enable
Filter Out Fake Calls (CallerID is the same as CalleeID)
Enable
Auto Reply of Source Address
Enable
DSCP
Enable
Calls from SIP Trunk Address only
Enable
Switch Signal Port if SIP Registration Failed
Enable
Hang up upon Call Time-out
Enable
Working Period
24 Hours
Session Timer
Enable
Early Media
Enable
Early Session
Enable
Not Wait ACK after Sending 200 OK
Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%)
70
Maximum Wait Answer Time(s)
60
Maximum Wait RTP Time(s)
0
Maximum Wait PSTN Resource Time(ms)
5000
Switch Network Port by Packet Loss Rate
Enable
Add Content to To Field in INVITE Message
Yes No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 4-2

2. Add the IP addresses of the gateways at Branch A and Branch B into the SIP trunks.

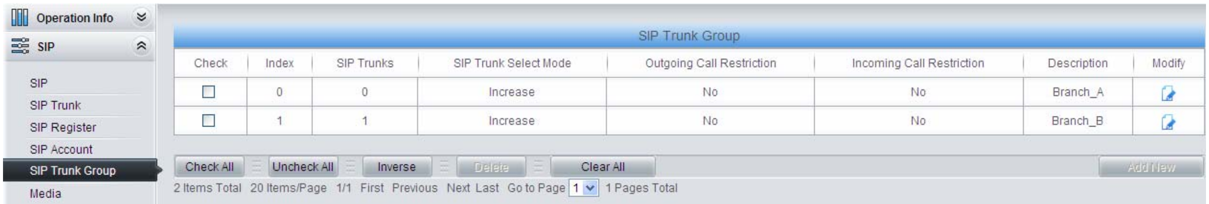


SIP Trunk

Check	Index	Description	Remote Address	Remote Port	Local Network Port	Transport Protocol	Outgoing Voice Resource	Incoming Voice Resource	
☐	0	default	201.123.112.227	5060	LAN 1(201.123.111.23)	UDP	512	512	G711A,G711U,
☐	1	default	201.123.112.147	5060	LAN 1(201.123.111.23)	UDP	512	512	G711A,G711U,

Figure 4-3

3. Add the SIP trunks at Branch A and Branch B into the corresponding SIP trunk groups.

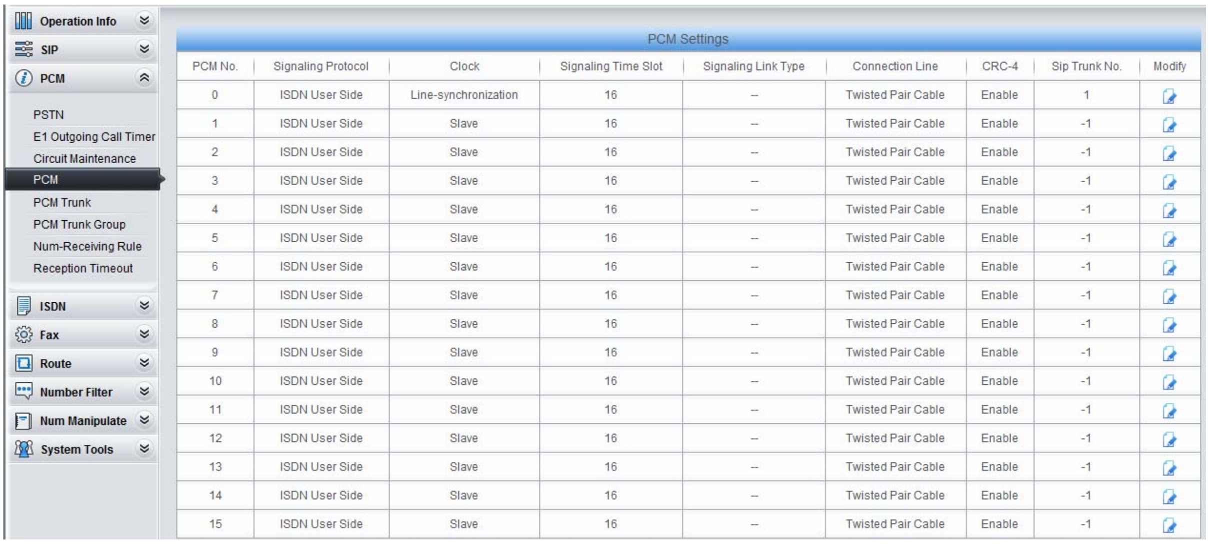


SIP Trunk Group

Check	Index	SIP Trunks	SIP Trunk Select Mode	Outgoing Call Restriction	Incoming Call Restriction	Description	Modify
☐	0	0	Increase	No	No	Branch_A	
☐	1	1	Increase	No	No	Branch_B	

Figure 4-4

4. Set PCM.

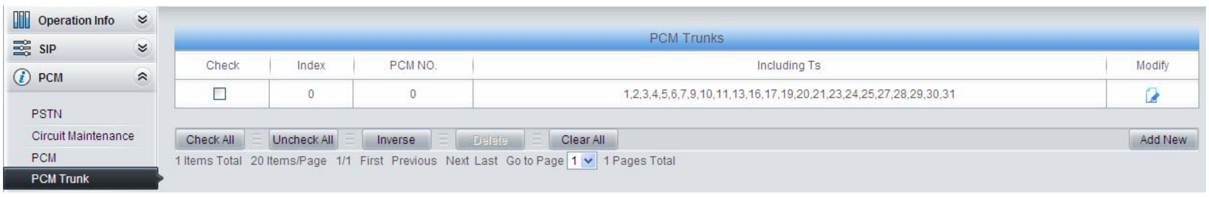


PCM Settings

PCM No.	Signaling Protocol	Clock	Signaling Time Slot	Signaling Link Type	Connection Line	CRC-4	Sip Trunk No.	Modify
0	ISDN User Side	Line-synchronization	16	--	Twisted Pair Cable	Enable	1	
1	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
2	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
3	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
4	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
5	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
6	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
7	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
8	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
9	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
10	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
11	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
12	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
13	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
14	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
15	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	

Figure 4-5

5. Add PCM trunk



PCM Trunks

Check	Index	PCM NO.	Including Ts	Modify
☐	0	0	1,2,3,4,5,6,7,9,10,11,13,16,17,19,20,21,23,24,25,27,28,29,30,31	

Figure 4-6

6. Add PCM trunk into the corresponding PCM trunk group.

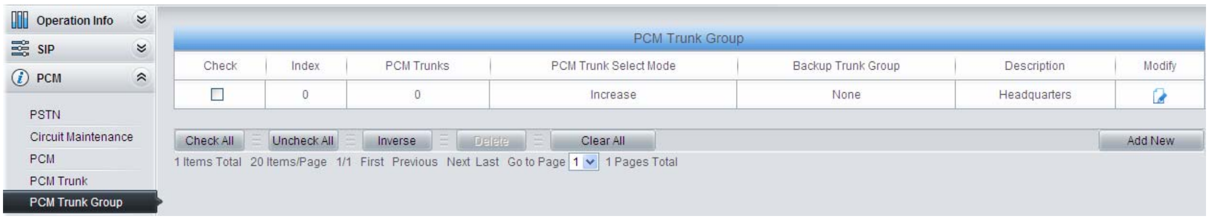


Figure 4-7

7. Set routing parameters. You may adopt the default value 'Route before Number Manipulate' for both configuration items.

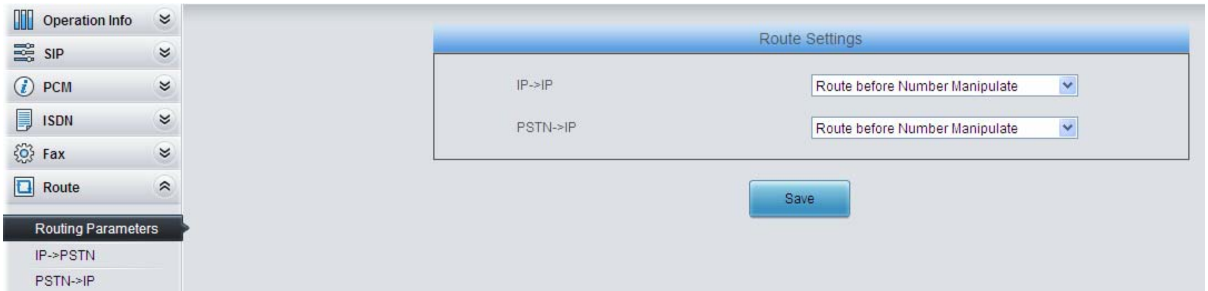


Figure 4-8

8. Set IP→PSTN routing rules to route calls from different SIP trunk groups to the corresponding PCM trunk groups. In this step, all incoming IP calls will be routed to PCM Trunk Group 0 regardless of the CalleeID prefix.

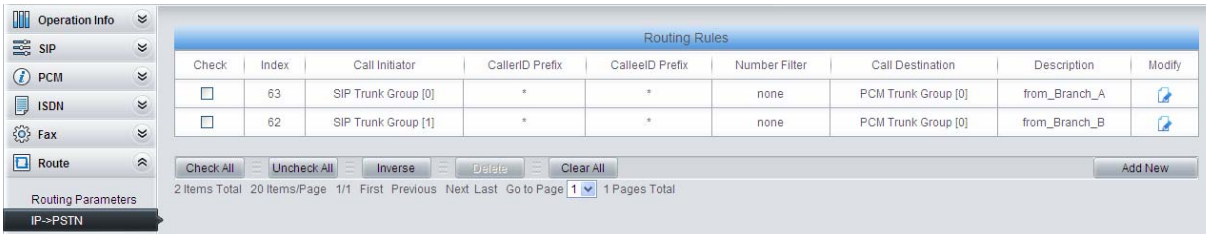


Figure 4-9

9. Set PSTN→IP routing rules to route calls from different PCM trunk groups to the corresponding SIP trunk groups. In this step, those calls with the CalleeID prefix 8 will be routed to SIP Trunk Group 0 while those with the CalleeID prefix 7 will be routed to SIP Trunk Group 1.

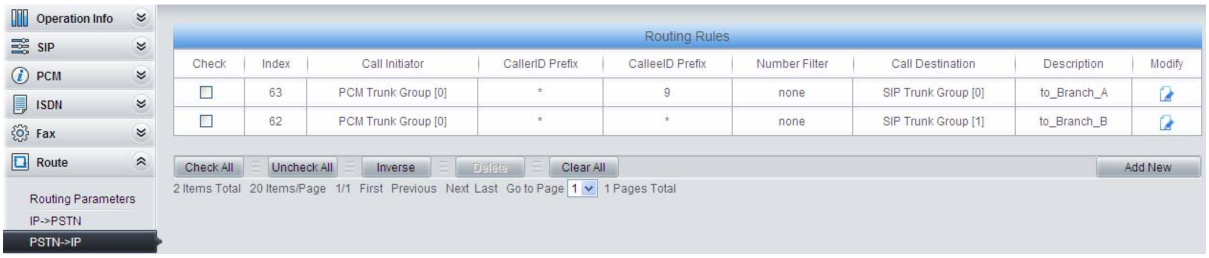


Figure 4-10

10. Set number manipulation rules. When the gateway receives a call from PSTN, 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.

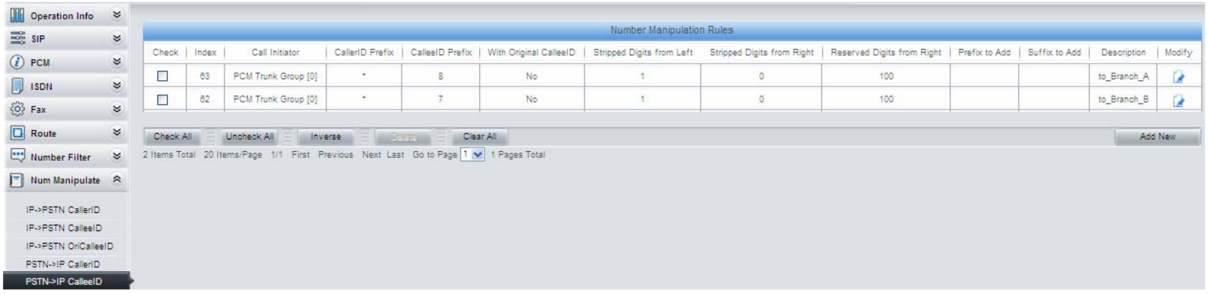


Figure 4-11

4.1.2 Configurations for Branch A

1. Configure SIP Settings for Branch A.

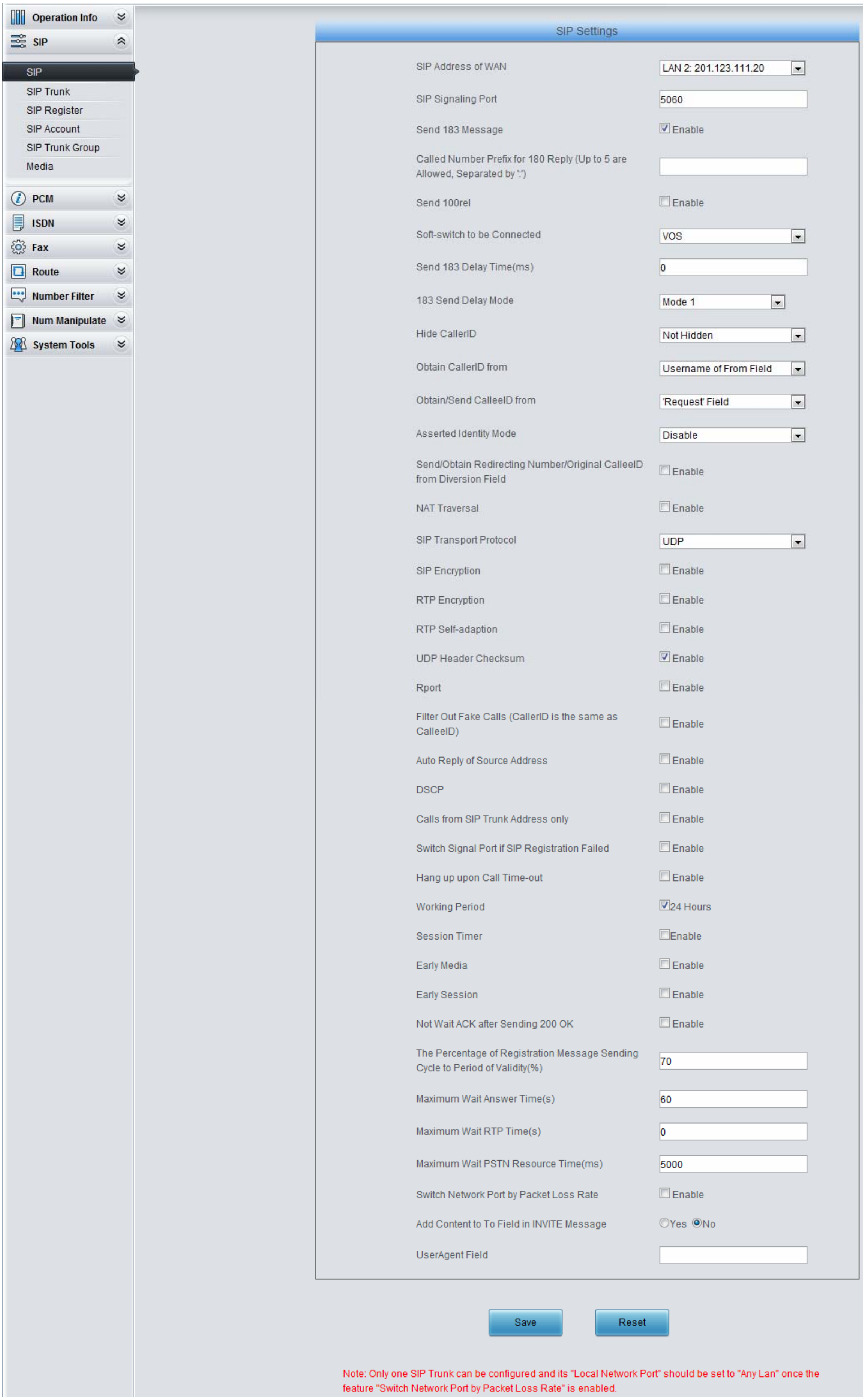
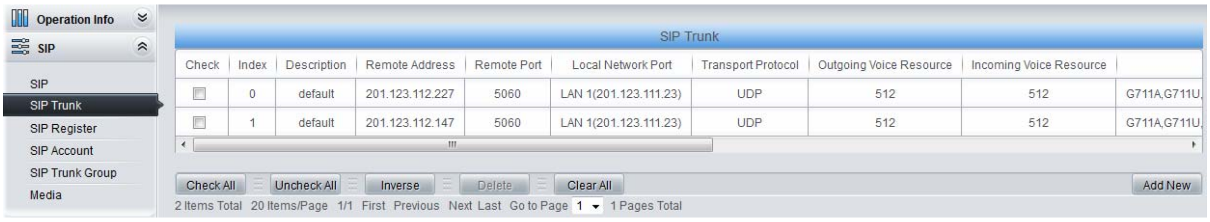

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN: LAN 2: 201.123.111.20
SIP Signaling Port: 5060
Send 183 Message: Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated by ',')
Send 100rel: Enable
Soft-switch to be Connected: VOS
Send 183 Delay Time(ms): 0
183 Send Delay Mode: Mode 1
Hide CallerID: Not Hidden
Obtain CallerID from: Username of From Field
Obtain/Send CalleeID from: 'Request' Field
Asserted Identity Mode: Disable
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field: Enable
NAT Traversal: Enable
SIP Transport Protocol: UDP
SIP Encryption: Enable
RTP Encryption: Enable
RTP Self-adaption: Enable
UDP Header Checksum: Enable
Rport: Enable
Filter Out Fake Calls (CallerID is the same as CalleeID): Enable
Auto Reply of Source Address: Enable
DSCP: Enable
Calls from SIP Trunk Address only: Enable
Switch Signal Port if SIP Registration Failed: Enable
Hang up upon Call Time-out: Enable
Working Period: 24 Hours
Session Timer: Enable
Early Media: Enable
Early Session: Enable
Not Wait ACK after Sending 200 OK: Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%): 70
Maximum Wait Answer Time(s): 60
Maximum Wait RTP Time(s): 0
Maximum Wait PSTN Resource Time(ms): 5000
Switch Network Port by Packet Loss Rate: Enable
Add Content to To Field in INVITE Message: Yes No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 4-12

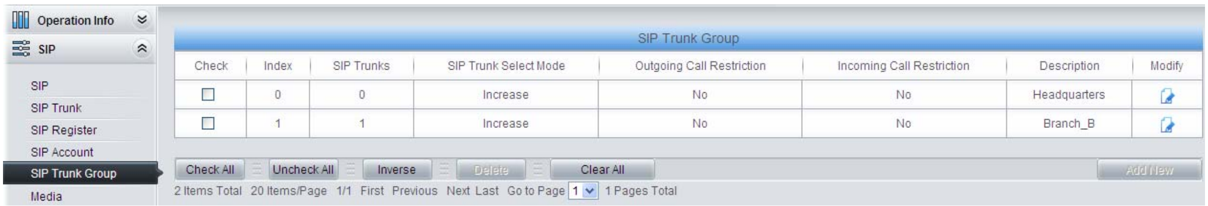
2. Add the IP addresses of the gateways at the headquarters and Branch B into the SIP trunks.



Check	Index	Description	Remote Address	Remote Port	Local Network Port	Transport Protocol	Outgoing Voice Resource	Incoming Voice Resource	
☐	0	default	201.123.112.227	5060	LAN 1(201.123.111.23)	UDP	512	512	G711A,G711U,
☐	1	default	201.123.112.147	5060	LAN 1(201.123.111.23)	UDP	512	512	G711A,G711U,

Figure 4-13

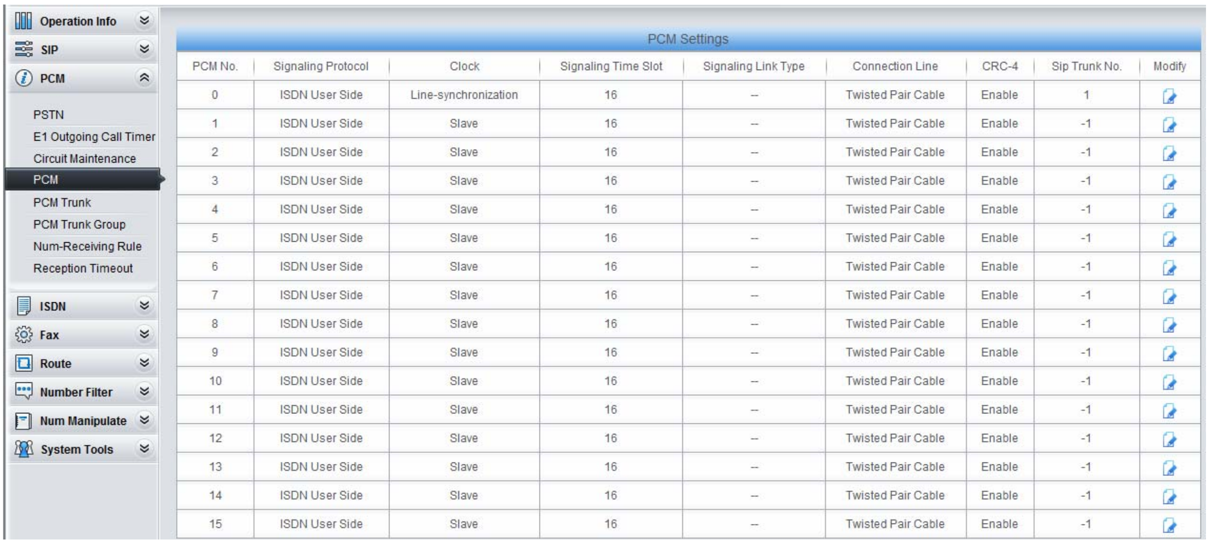
3. Add the SIP trunks at the headquarters and Branch B into the corresponding SIP trunk groups.



Check	Index	SIP Trunks	SIP Trunk Select Mode	Outgoing Call Restriction	Incoming Call Restriction	Description	Modify
☐	0	0	Increase	No	No	Headquarters	
☐	1	1	Increase	No	No	Branch_B	

Figure 4-14

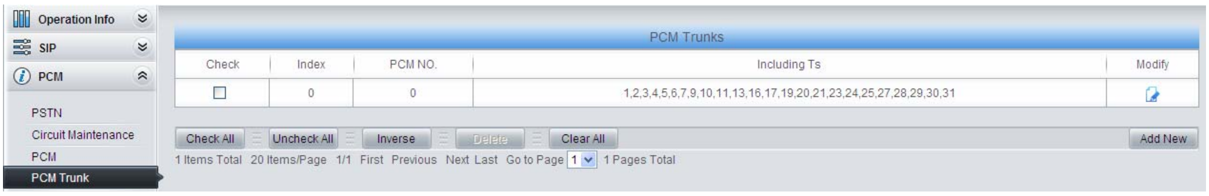
4. Set PCM.



PCM No.	Signaling Protocol	Clock	Signaling Time Slot	Signaling Link Type	Connection Line	CRC-4	Sip Trunk No.	Modify
0	ISDN User Side	Line-synchronization	16	--	Twisted Pair Cable	Enable	1	
1	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
2	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
3	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
4	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
5	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
6	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
7	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
8	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
9	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
10	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
11	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
12	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
13	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
14	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	
15	ISDN User Side	Slave	16	--	Twisted Pair Cable	Enable	-1	

Figure 4-15

5. Add PCM trunk



Check	Index	PCM NO.	Including Ts	Modify
☐	0	0	1,2,3,4,5,6,7,9,10,11,13,16,17,19,20,21,23,24,25,27,28,29,30,31	

Figure 4-16

6. Add PCM trunk into the corresponding PCM trunk group.

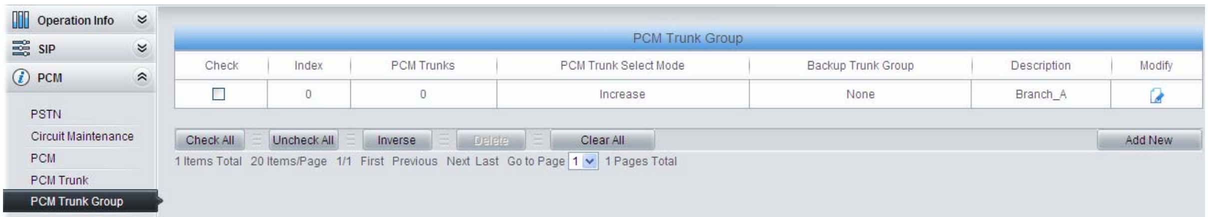


Figure 4-17

7. Set routing parameters. You may adopt the default value 'Route before Number Manipulate' for both configuration items.

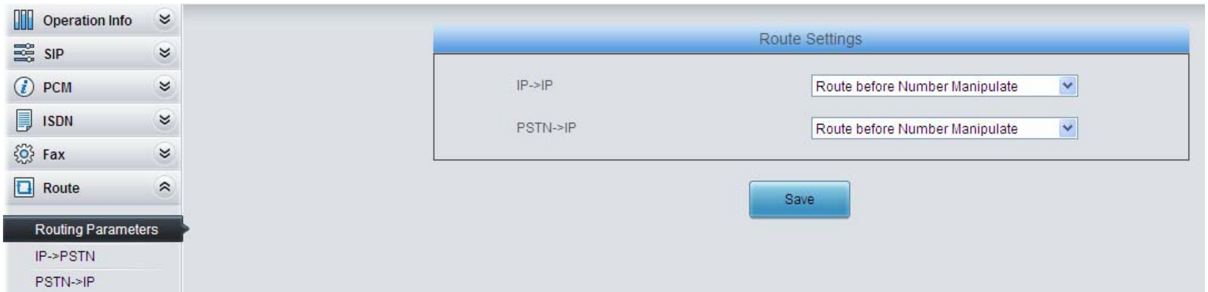


Figure 4-18

8. Set IP→PSTN routing rules to route calls from different SIP trunk groups to the corresponding PCM trunk groups. In this step, all incoming IP calls will be routed to PCM Trunk Group 0 regardless of the CalleeID prefix.

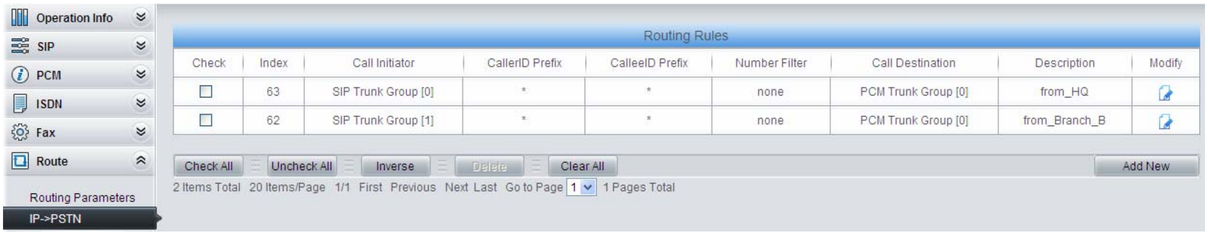


Figure 4-19

9. Set PSTN→IP routing rules to route calls from different PCM trunk groups to the corresponding SIP trunk groups. In this step, those calls with the CalleeID prefix 9 or 0 will be routed to SIP Trunk Group 0 while those with the CalleeID prefix 7 will be routed to SIP Trunk Group 1.

Figure 4-20

10. Set number manipulation rules. When the gateway receives a call from PSTN, it will first check the CalleeID prefix. If the CalleeID prefix is 9 or 7, the gateway will delete it before routing the call to the corresponding SIP trunk group.

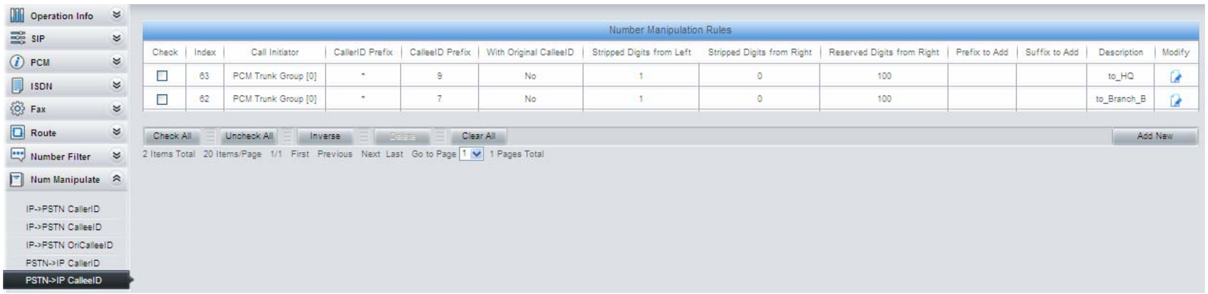


Figure 4-21

4.1.3 Configurations for Branch B

1. Configure SIP Settings for Branch B.

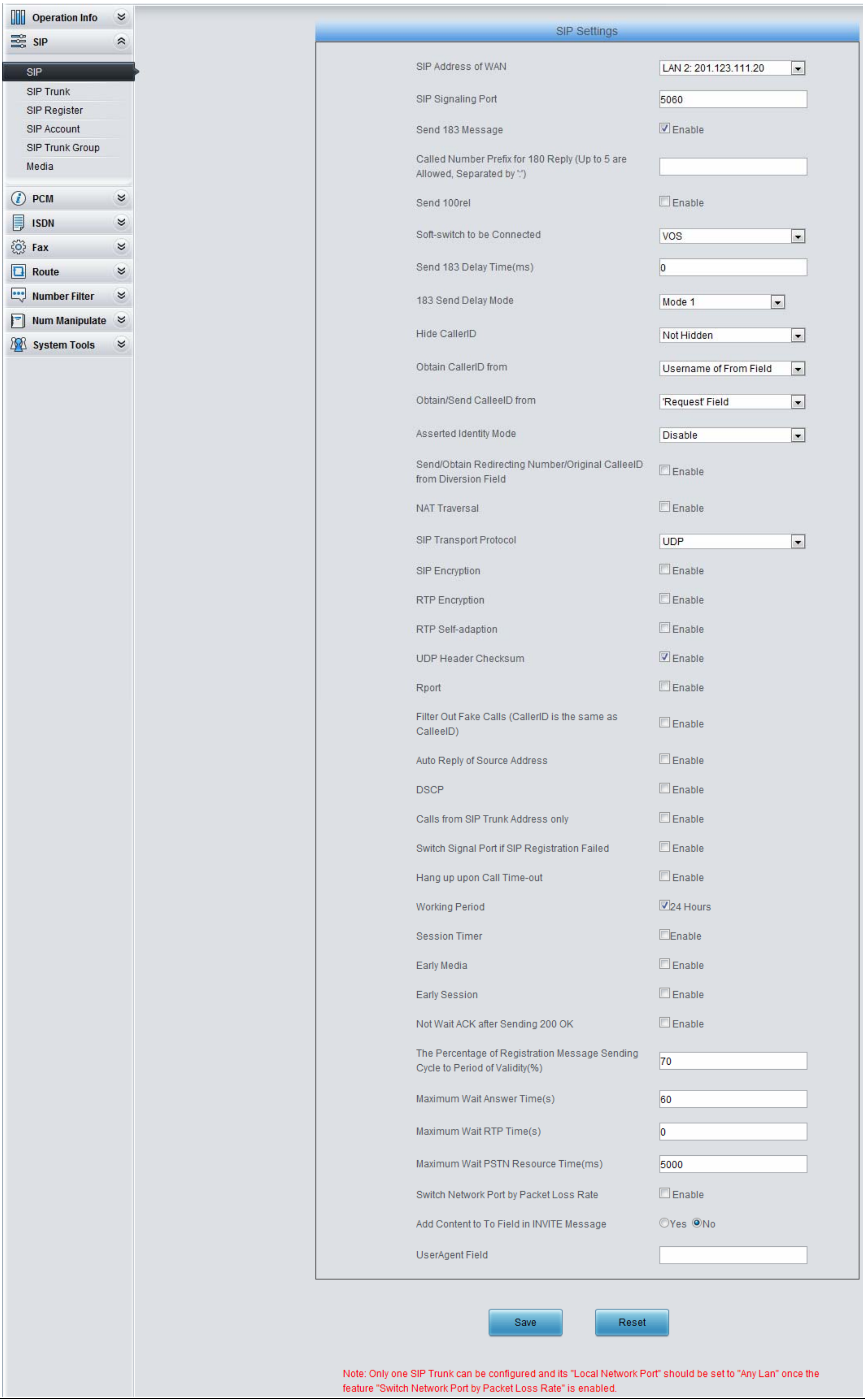

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated by ',')
Send 100rel
Enable
Soft-switch to be Connected
VOS
Send 183 Delay Time(ms)
0
183 Send Delay Mode
Mode 1
Hide CallerID
Not Hidden
Obtain CallerID from
Username of From Field
Obtain/Send CalleeID from
'Request' Field
Asserted Identity Mode
Disable
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field
Enable
NAT Traversal
Enable
SIP Transport Protocol
UDP
SIP Encryption
Enable
RTP Encryption
Enable
RTP Self-adaption
Enable
UDP Header Checksum
Enable
Rport
Enable
Filter Out Fake Calls (CallerID is the same as CalleeID)
Enable
Auto Reply of Source Address
Enable
DSCP
Enable
Calls from SIP Trunk Address only
Enable
Switch Signal Port if SIP Registration Failed
Enable
Hang up upon Call Time-out
Enable
Working Period
24 Hours
Session Timer
Enable
Early Media
Enable
Early Session
Enable
Not Wait ACK after Sending 200 OK
Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%)
70
Maximum Wait Answer Time(s)
60
Maximum Wait RTP Time(s)
0
Maximum Wait PSTN Resource Time(ms)
5000
Switch Network Port by Packet Loss Rate
Enable
Add Content to To Field in INVITE Message
Yes
No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 4-22

2. Add the IP addresses of the gateways at the headquarters and Branch A into the SIP trunks.

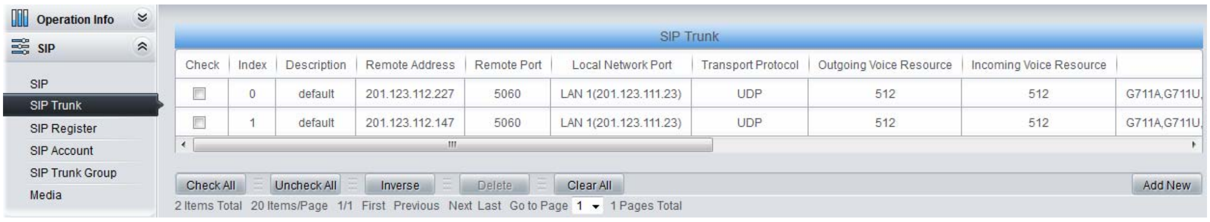


Figure 4-23

3. Add the SIP trunks at the headquarters and Branch A into the corresponding SIP trunk groups.

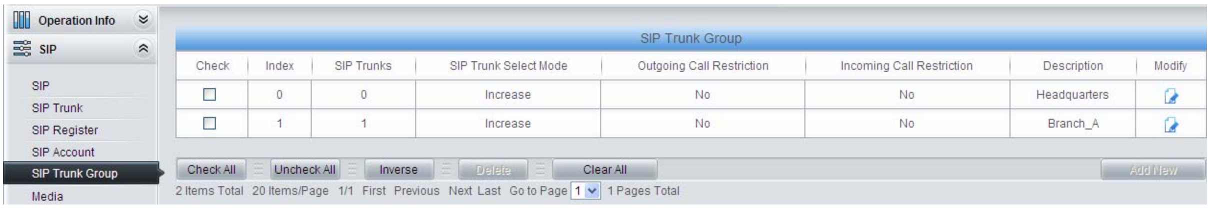


Figure 4-24

4. Set PCM.

Figure 4-25

5. Add PCM trunk

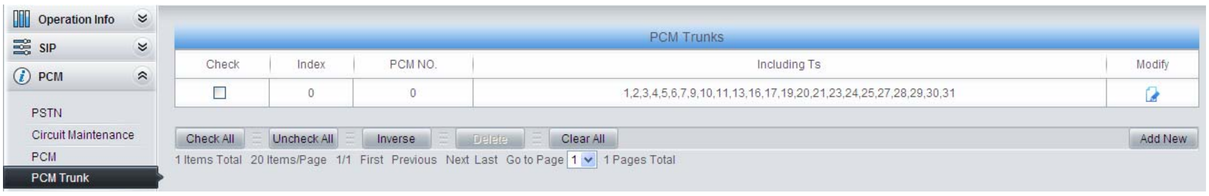


Figure 4-26

6. Add PCM trunk into the corresponding PCM trunk group.

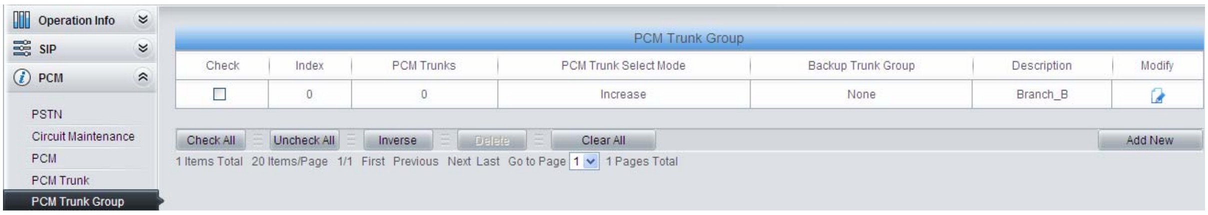


Figure 4-27

7. Set routing parameters. You may adopt the default value 'Route before Number Manipulate' for both configuration items.

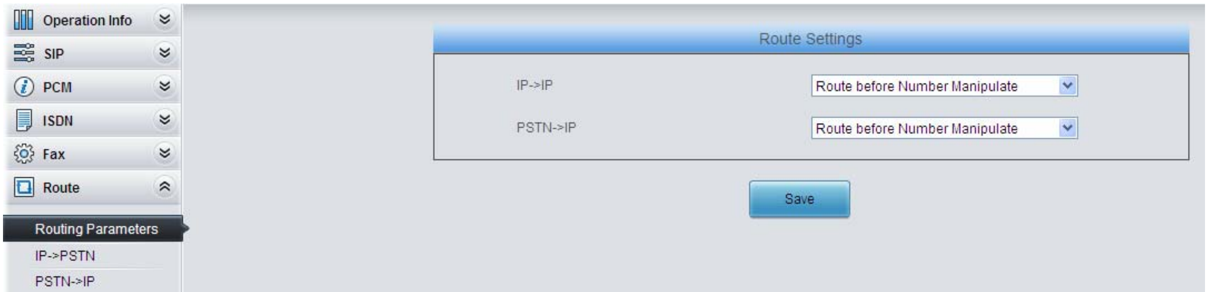


Figure 4-28

8. Set IP→PSTN routing rules to route calls from different SIP trunk groups to the corresponding PCM trunk groups. In this step, all incoming IP calls will be routed to PCM Trunk Group 0 regardless of the CalleeID prefix.

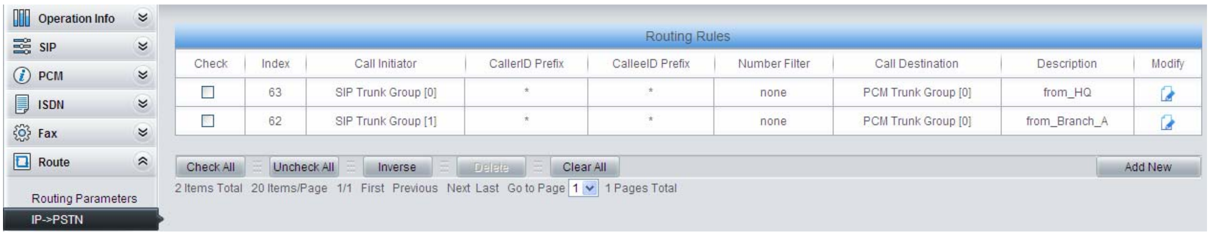


Figure 4-29

9. Set PSTN→IP routing rules to route calls from different PCM trunk groups to the corresponding SIP trunk groups. In this step, those calls with the CalleeID prefix 9 or 0 will be routed to SIP Trunk Group 0 while those with the CalleeID prefix 8 will be routed to SIP Trunk Group 1.

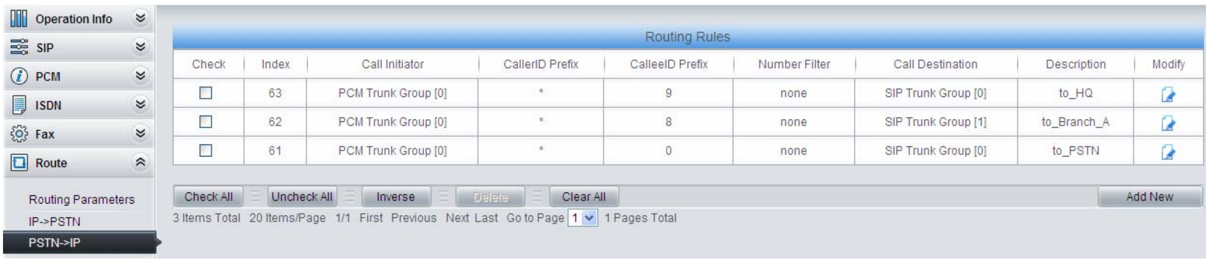


Figure 4-30

10. Set number manipulation rules. When the gateway receives a call from PSTN, it will first check the CalleeID prefix. If the CalleeID prefix is 9 or 8, the gateway will delete it before routing the call to the corresponding SIP trunk group.

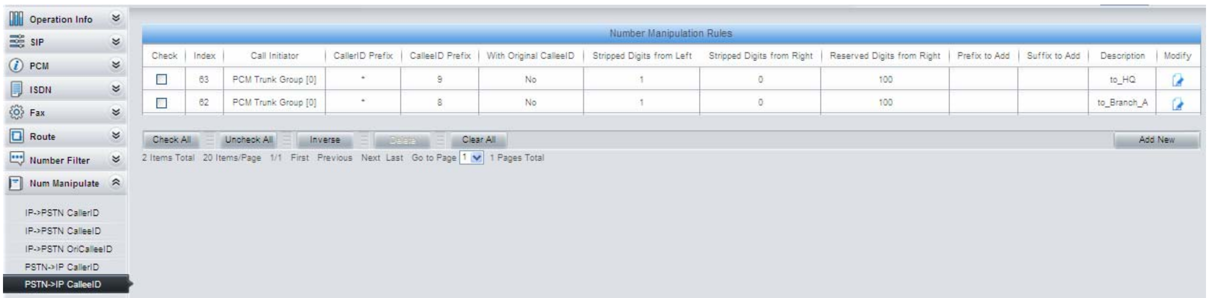
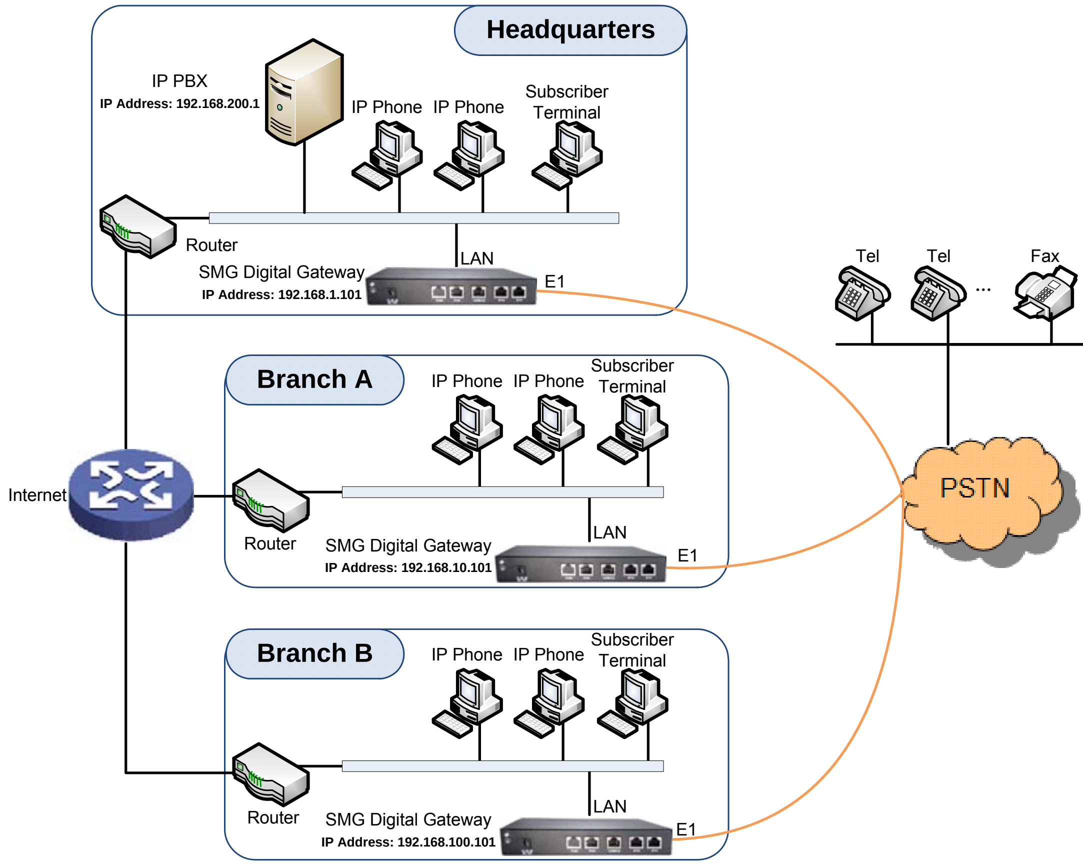


Figure 4-31

4.2 Application 2



Note: In this application, we assume that Branch A, Branch B and the headquarters have established VLAN using VPN technology.

Figure 4-32 Application 2

In this application, the headquarters, Branch A and Branch B all have their own independent digital gateways to connect with the PSTN. Calls within the enterprise are all carried via SIP. Outbound calls to PSTN can be allocated to different gateways by the IP PBX. This application makes a full use of each E1/T1 trunk, helps an enterprise to eliminate the single point failure caused by device or network malfunction and enhance the stability of the IP telephony network.

This section takes SMG2120 as an example and introduces the configurations for the gateway application with the following dialing plan:

Make an outbound call from the headquarters: 0+Number

Make an outbound call from Branch A or Branch B: 0+Number

4.2.1 Configurations for Headquarters

1. Configure SIP Settings for the headquarters.

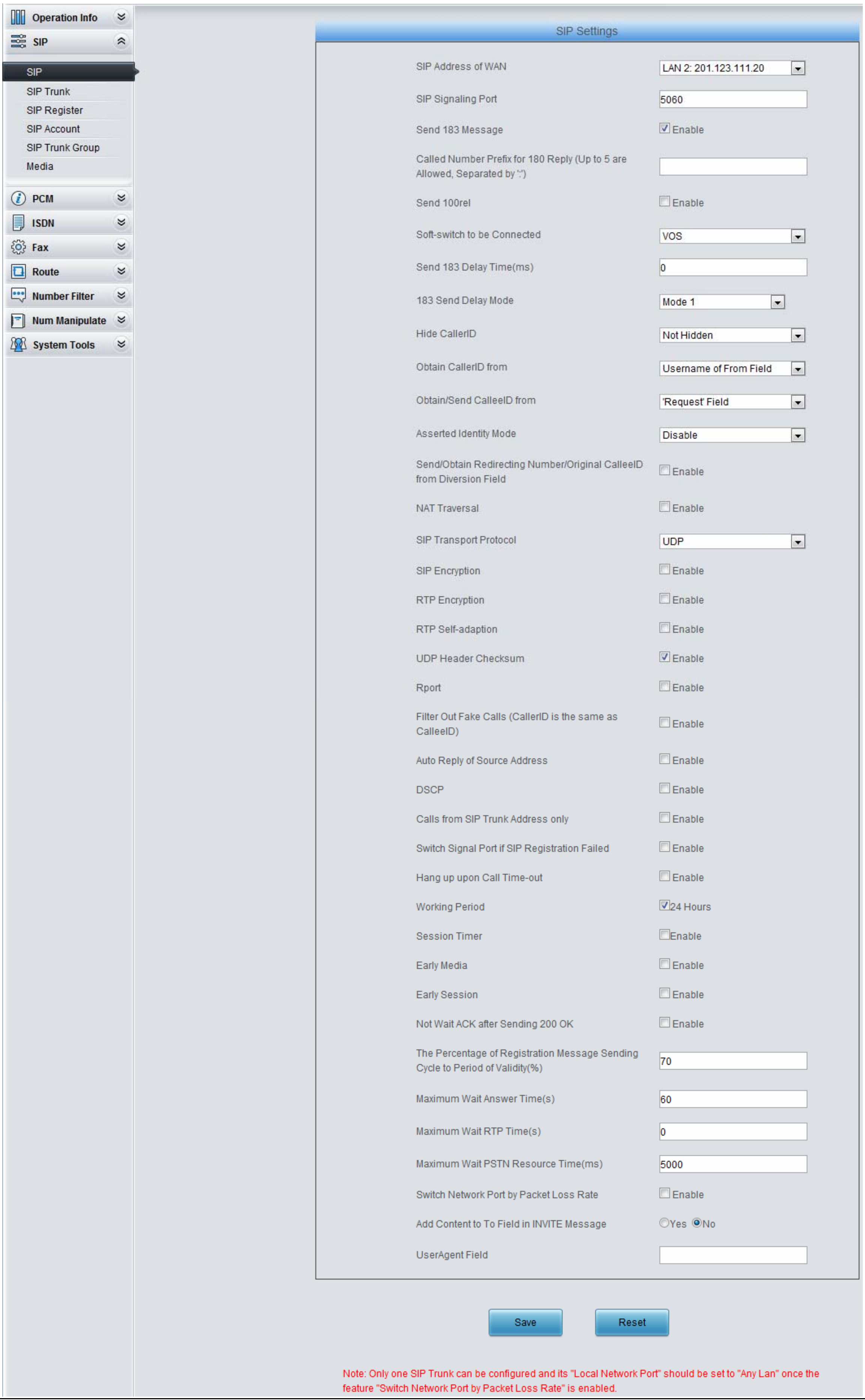

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated by ',')
Send 100rel
Enable
Soft-switch to be Connected
VOS
Send 183 Delay Time(ms)
0
183 Send Delay Mode
Mode 1
Hide CallerID
Not Hidden
Obtain CallerID from
Username of From Field
Obtain/Send CalleeID from
'Request' Field
Asserted Identity Mode
Disable
Send/Obtain Redirecting Number/Original CalleeID from Diversion Field
Enable
NAT Traversal
Enable
SIP Transport Protocol
UDP
SIP Encryption
Enable
RTP Encryption
Enable
RTP Self-adaption
Enable
UDP Header Checksum
Enable
Rport
Enable
Filter Out Fake Calls (CallerID is the same as CalleeID)
Enable
Auto Reply of Source Address
Enable
DSCP
Enable
Calls from SIP Trunk Address only
Enable
Switch Signal Port if SIP Registration Failed
Enable
Hang up upon Call Time-out
Enable
Working Period
24 Hours
Session Timer
Enable
Early Media
Enable
Early Session
Enable
Not Wait ACK after Sending 200 OK
Enable
The Percentage of Registration Message Sending Cycle to Period of Validity(%)
70
Maximum Wait Answer Time(s)
60
Maximum Wait RTP Time(s)
0
Maximum Wait PSTN Resource Time(ms)
5000
Switch Network Port by Packet Loss Rate
Enable
Add Content to To Field in INVITE Message
Yes
No
UserAgent Field
Save
Reset
Note: Only one SIP Trunk can be configured and its "Local Network Port" should be set to "Any Lan" once the feature "Switch Network Port by Packet Loss Rate" is enabled.

Figure 4-33

2. Add the IP address of the IP PBX into the SIP trunk.

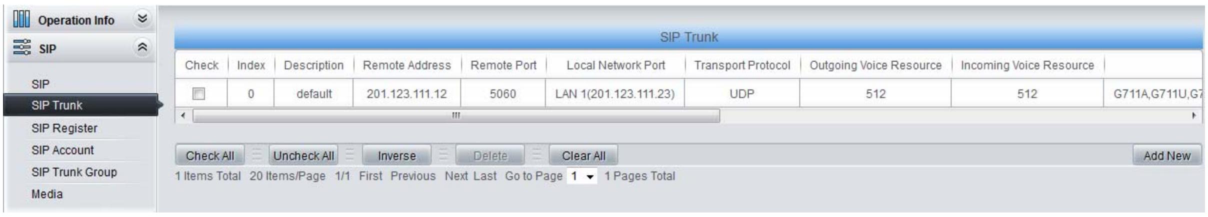


Figure 4-34

3. Add the SIP trunk into the corresponding SIP trunk group.

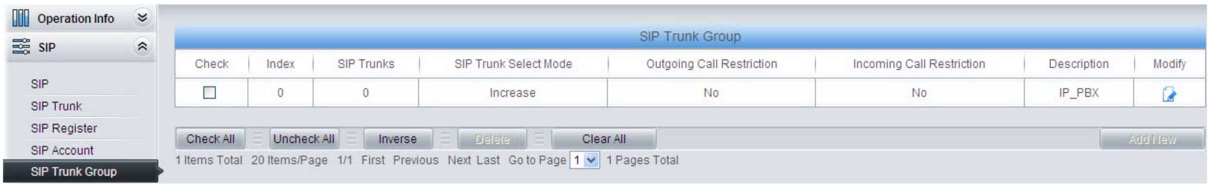


Figure 4-35

4. Set PCM.

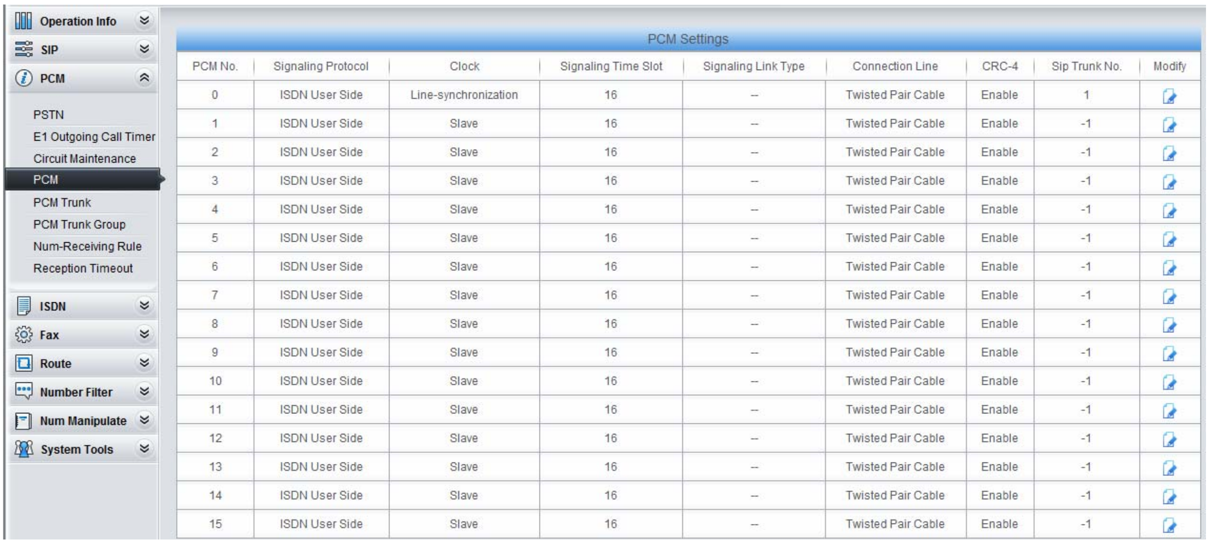


Figure 4-36

5. Add PCM trunk

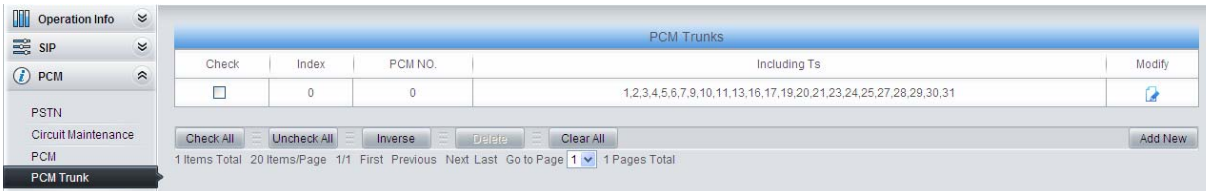


Figure 4-37

6. Add PCM trunk into the corresponding PCM trunk group.

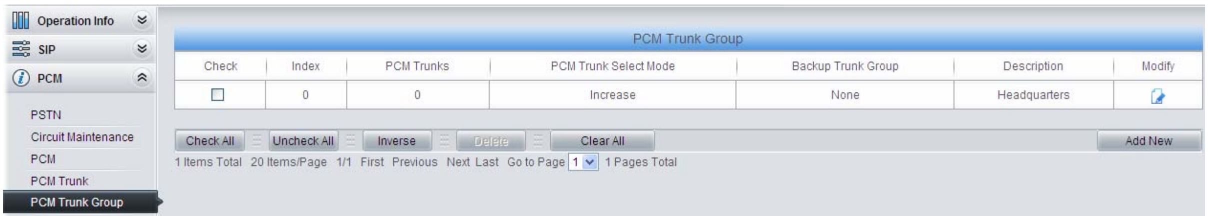


Figure 4-38

7. Set routing parameters. You may adopt the default value 'Route before Number Manipulate' for both configuration items.

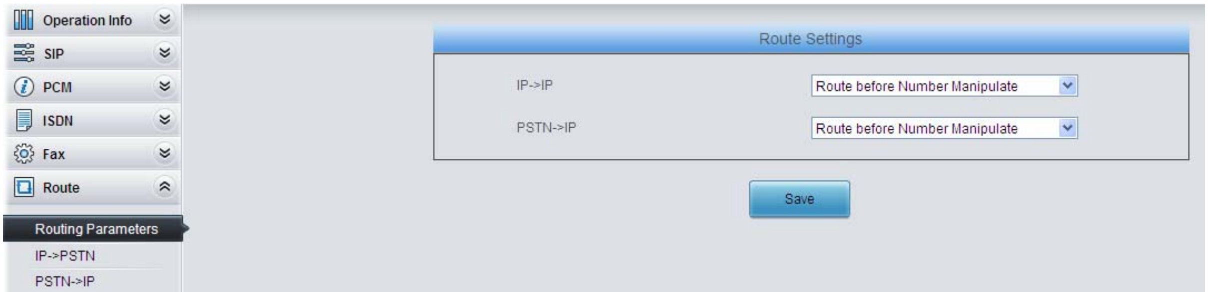


Figure 4-39

8. Set IP→PSTN routing rules to route calls from different SIP trunk groups to the corresponding PCM trunk groups. In this step, all incoming IP calls will be routed to PCM Trunk Group 0 regardless of the CalleeID prefix.

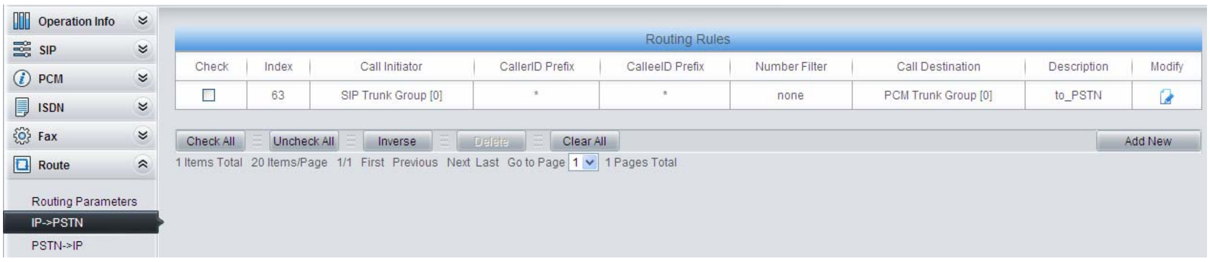


Figure 4-40

9. Set PSTN→IP routing rules to route calls from different PCM trunk groups to corresponding SIP trunk groups. In this step, all incoming calls from PSTN will be routed to SIP Trunk Group 0 regardless of the CalleeID prefix.

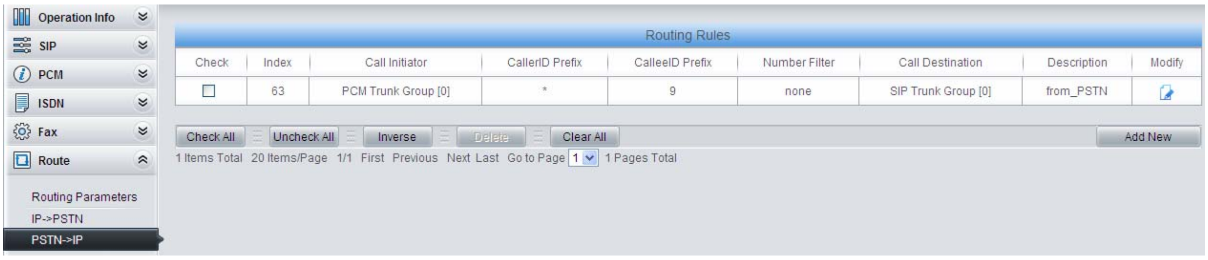


Figure 4-41

Note: In this application, the number manipulation feature is implemented by the IP PBX. That is, when a subscriber at the headquarters makes an outbound call dialing "0+Number", the IP PBX will delete the prefix 0 before rooting it to the gateway. Therefore, it is not necessary to configure the number manipulation rules on the gateway. However, you shall add to the IP PBX the number manipulation rule of deleting the CalleeID prefix 0.

4.2.2 Configurations for Branches

For the gateways at Branch A and Branch B, you shall fill in their actual IP addresses to the configuration item 'SIP Address'. All the other configurations are the same as those for the headquarters.

Appendix A Technical Specifications

Dimensions

190×30×120 mm^3

Weight

About 0.65 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 BASE-TX (RJ-45))

Self-adaptive bandwidth supported

Auto MDI/MDIX supported

E1/T1 Port

Amount: 1/2

Type: RJ45

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 voltage: 12V DC ±10%

Input power: ≥3A DC

Maximum power consumption：≤8W

Signaling & Protocol

ISDN: ISDN User Side, ISDN Network Side

SS1: SS1 Signaling

SIP signaling: SIP V1.0/2.0, RFC3261

Audio Encoding & Decoding

G.711A	64 kbps
G.711U	64 kbps
G.729A/B	8 kbps
G723	5.3/6.3 kbps
G722	64 kbps
AMR	4.75/5.15/5.90/6.70/7.40/7.95/10.20/12.20 kbps
iLBC	13.3/15.2 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 SMG digital 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 SMG digital 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.

c) The E1/T1 trunk of the gateway is well connected, but the E1/T1 indicators never light up after the gateway startup or their indications do not comply with the actual state.

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

3. What to do if I cannot enter the WEB interface of the SMG digital 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 ISDN Pending Cause to SIP Status Code

ISDN Return Value	Cause	SIP Status Code	Implication
1	Unallocated (unassigned) number	404	Not found
2	No route to specified transit network	404	Not found
3	No route to destination	404	Not found
26	Non-selected user clearing	404	Not found
16	Normal call clearing (and the failure reason is that Waiting for off-hook signal from called party is overtime)	603	Decline
16	Normal call clearing	500	Decline
17	User busy	486	Busy here
132	Network busy (internal definition, only applies to ISDN)	486	Busy here
21	Call rejected	486	Busy here
18	No user responding	408	Request timeout
19	No answer from user (user alerted)	480	Temporarily unavailable
20	Subscriber absent	480	Temporarily unavailable
31	Normal, unspecified	480	Temporarily unavailable
136	Connection after pickup failed (internal definition, only applies to ISDN)	480	Temporarily unavailable
137	Pickup time out (internal definition, only apply to ISDN)	480	Temporarily unavailable
55	Incoming calls barred within CUG	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
87	User not member of CUG	403	Forbidden
22	Number changed	410	Gone
27	Destination out of order	502	Bad gateway
28	Invalid number format	484	Address incomplete
29	Facility rejected	501	Not implemented
79	Service or option not implemented, unspecified	501	Not implemented
34	No circuit/channel available	503	Service unavailable

38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
47	Resource unavailable, unspecified	503	Service unavailable
58	Bearer capability not presently available	503	Service unavailable
88	Incompatible destination	503	Service unavailable
133	Circuit restarted (internal definition, only applies to ISDN)	503	Service unavailable
134	Temporary fault (internal definition, only applies to ISDN)	503	Service unavailable
135	Data link failure (internal definition, only applies to ISDN)	503	Service unavailable
65	Bearer capability not implemented	488	Not acceptable here
70	Only restricted digital information bearer capability is available	488	Not acceptable here
102	Recovery on timer expiry	504	Server time-out
128	T303 time out (internal definition, only applies to ISDN)	504	Server time-out
129	T304 time out (internal definition, only applies to ISDN)	504	Server time-out
130	T310 time out (internal definition, only applies to ISDN)	504	Server time-out
111	Protocol error, unspecified	500	Server internal error
127	Interworking, unspecified	500	Server internal error
Others	Others	408	Request timeout

Appendix D Direction for CDR Use

CDR is a call detail record. The digital gateway can record the CDR to the memory and send them to the designated server in real time.

Methods:

1. By using the TCP protocol, the gateway works as a client to configure a CDR server, and then sends the CDR to the server regularly.
2. The gateway sends the CDR to the server every 3 seconds.
3. The gateway will connect the CDR server again every 30 seconds if lossing connection from it.
4. There are up to 2000 pieces of CDR saved in the server, and the first 100 pieces of the record will be deleted once the pieces exceed 2000.
5. Example CDR format:

   Outgoing example:(ip->pstn)

   “2014-12-20 14:55:33.345”, ”2014-12-20 14:57:43.627”, ”1000”, ”5551234”, ”SIP/1000”, “Zap/444”, “”, “”

   Incoming example:(pstn->ip)

   “2014-12-20 14:55:33.345”, ”2014-12-20 14:57:43.627”, ”5551234”, ”1000”, ”Zap/444”, “SIP/1000”, “1234”, “”

#	Field Name	Format	Description
1	Start Time	YYYY-MM-DD HH:MM:SS.mmm	Call start timestamp
2	End Time	YYYY-MM-DD HH:MM:SS.mmm	Call end timestamp
3	Calling Number (A)		Calling Number
4	Dialed Number (B)		Dialed Number
5	Incoming Call Leg		Incoming Call Leg
6	Outgoing Call Leg		Outgoing Call Leg
7	DNIS		DNIS (incoming only)
8	Queue		Queue (incoming only)

Appendix E Technical/sales Support

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

Headquarters

Synway Information Engineering Co., Ltd

http://www.synway.net/

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

Tel: +86-571-88860561

Fax: +86-571-88850923

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

Technical Support

Tel: +86-571-88864579

Mobile: +86-18905817070

Email: techsupport@sanhuid.com

Email: techsupport@synway.net

MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: sales@synway.net