Synway SMG Series Digital Gateway

SMG2030, SMG2030S, SMG2030L,

SMG2060, SMG2060S, SMG2060L

SMG2120, SMG2120S

SMG3008, SMG3016

SMG3008B, SMG3016B

SMG3000-B1, SMG3000-B2，SMG3000-B4

SMG3000-B1L, SMG3000-B2L

SMG3000-C1L

Digital Gateway

User Manual

Version 1.8.0

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

Content

Copyright Declaration

Revision History

Version	Date	Comments
Version 1.3.0	2014-06	Initial publication.
Version 1.3.1	2014-08	New revision
Version 1.3.2	2014-10	New revision
Version 1.5.0	2014-12	Add description on the new series SMG3016
Version 1.5.1	2015-01	Add description on the new series SMG3008
Version 1.6.0	2015-03	New revision
Version 1.6.1	2015-06	New revision
Version 1.6.2	2015-09	New revision
Version 1.6.3	2016-01	New revision
Version 1.6.4	2016-09	New revision
Version 1.6.5	2017-06	New revision
Version 1.7.0	2018-06	New revision
Version 1.8.0	2019-11	New revision

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

Chapter 1 Product Introduction

Thank you for choosing Synway 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.

The SMG series digital gateway has eight models:

- SMG2030, SMG2030S, SMG2030L, SMG3000-B1L, SMG3000-C1L: 1 E1/T1 interface (30 digital ports)
- SMG2060, SMG2060S, SMG2060L, SMG3000-B2L: 2 E1/T1 interfaces (60 digital ports)
- SMG2120, SMG2120S: 4 E1/T1 interfaces (120 digital ports)
- SMG3008: 8 E1/T1 interfaces (240 digital ports)
- SMG3016: 16 E1/T1 interfaces (480 digital ports)
- SMG3000-B1: 1 E1 interface (30 digital ports)
- SMG3000-B2: 2 E1 interfaces (60 digital ports)
- SMG3000-B4: 4 E1 interfaces (120 digital ports)

1.1 Typical Application

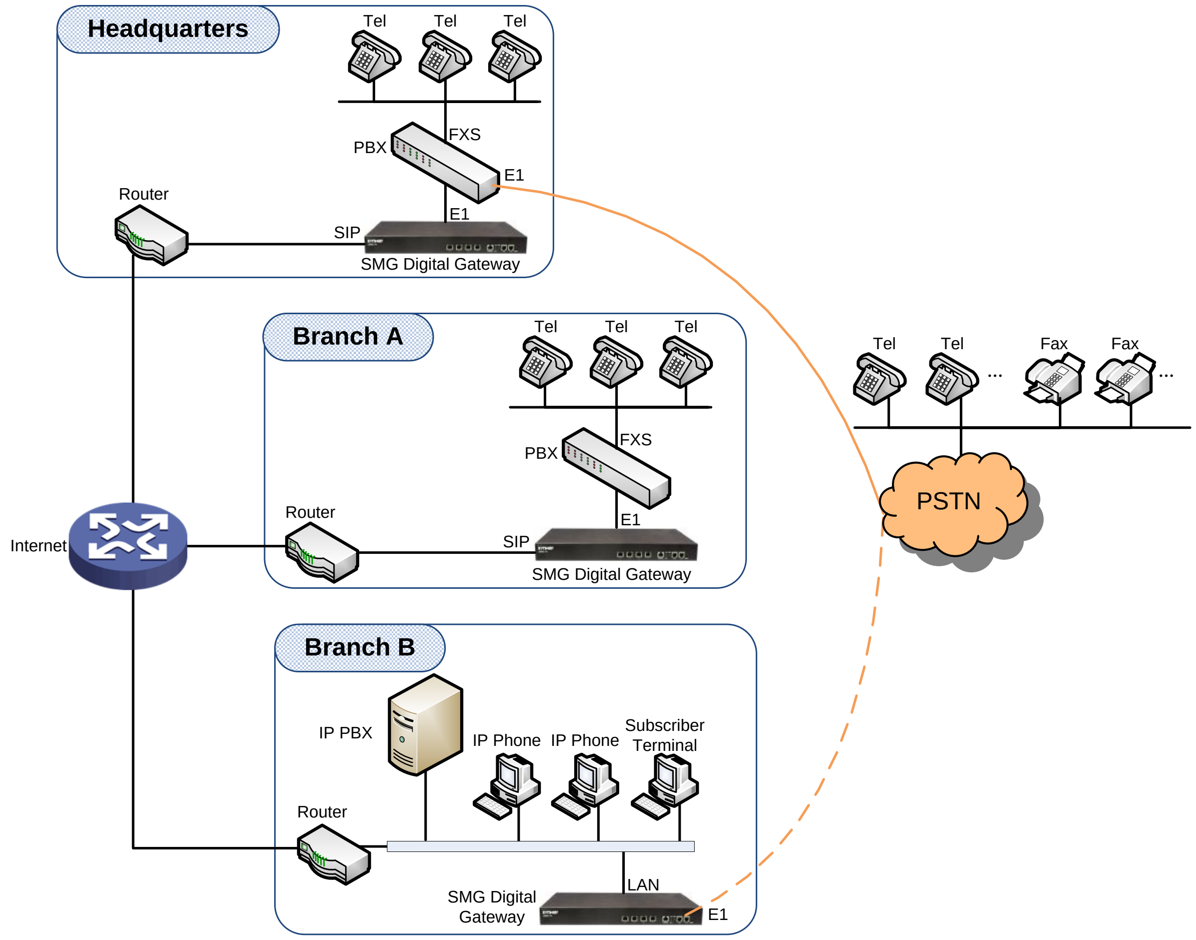


Figure 1-1 Typical Application

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**
SS7	SS7-TUP, SS7-ISUP
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-NB, 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

Note: The gateways in different types support different features, please pay attention to the actual device version.

1.3 Hardware Description

The SMG digital gateway features 1U rackmount design and integrates embedded LINUX system within the POWERPC+DSP hardware architecture. It has 1/2/4/8/16 E1/T1 ports and 2 Kilomega-Ethernet ports (LAN1 and LAN2) on the chassis.

(a) See the figures below for SMG2000 series' appearance:

Figure 1-2 Front View

Figure 1-3 Rear View

Figure 1-4 Left View

(b) See the figures below for SMG3000 series' appearance:

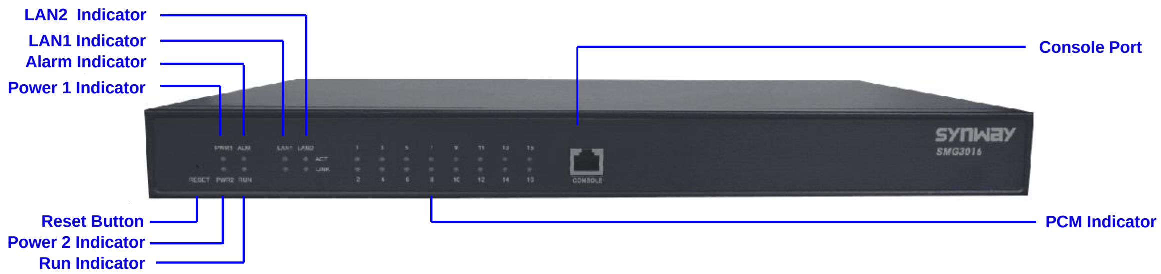


Figure 1-5 Front View

Figure 1-6 Rear View

Note: The left view for SMG3000 series is same as that for SMG2000 series, refer to Figure 1-4.

(c) See the figures below for SMG3000B series' appearance:

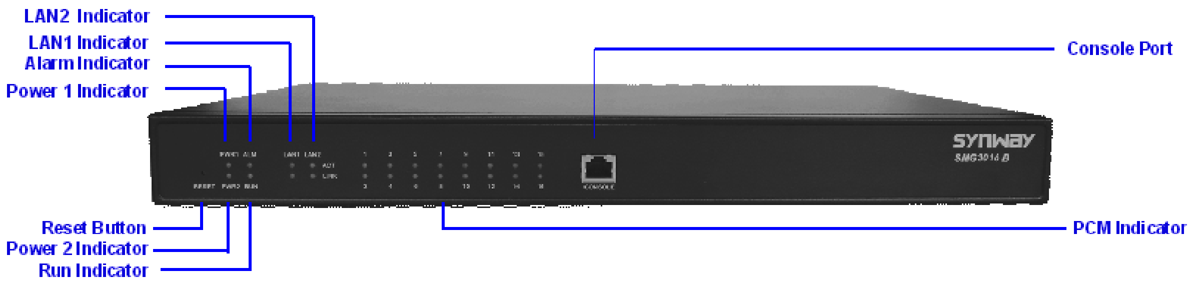


Figure 1-7 Front View

Figure 1-8 Rear View

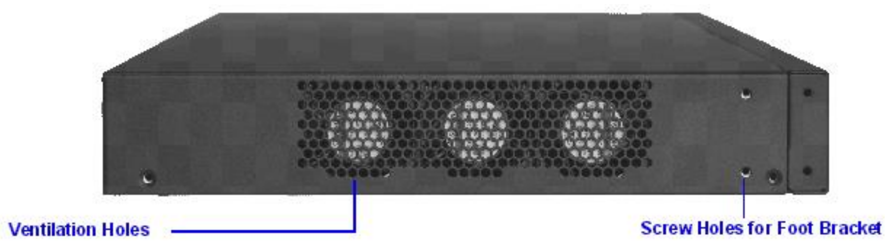


Figure 1-9 Left View

(d) See the figures below for SMG L series' appearance:

Figure 1-10 Front View

Figure 1-11 Rear View

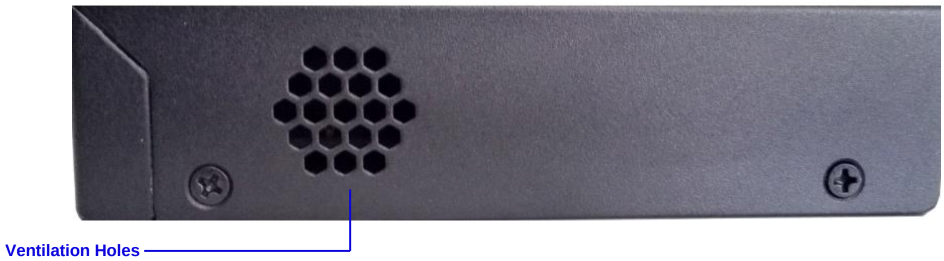


Figure 1-12 Left View

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

Interface	Description
LAN	Amount: 2
	Type: RJ-45
	Bandwidth: 10/100/1000Mbps (L-type: 100Mbps)
	Self-Adaptive Bandwidth Supported
	Auto MDI/MDIX Supported
E1/T1	Amount: 1/2/4/8/16
	Type: RJ-45
Console Port	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-13 for signal definition)
	Data Bits: 8 bits

	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
Button	**Description**
Power Key	Power on/off the SMG digital gateway. You can turn on the two power keys at the same time to have the power supply working in the hot-backup mode. (Note: The SMG L series products don't have the power key.)
Reset Button	Restore the gateway to factory settings.
LED	**Description**
Power Indicator	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
Run Indicator	Indicates the running status. For more details, refer to Alarm Info.
Alarm Indicator	Alarms the device malfunction. For more details, refer to Alarm Info.
Link Indicator	The green LED on the left of LAN, indicating the network connection status.
ACT Indicator	The orange LED on the right of LAN, whose flashing tells data are being transmitted.
E1/T1 Indicators	The green LED on the right of E1/T1 interface lights up and keeps on after the E1/T1 module is successfully synchronized.
Channel Indicators	Indicates the synchronization status of E1/T1 channels. It will light up and keep on if E1/T1 is synchronized; otherwise, it will go out.

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

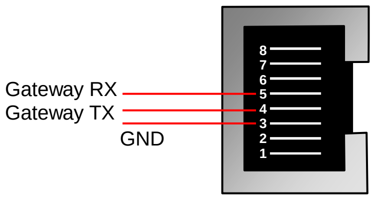


Figure 1-13 Console Port Signal Definition

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

Step 2: Properly fix the SMG digital gateway.

If you do not need to place the gateway on the rack, simply fix the 4 rubber foot pads. Otherwise, you should first fix the 2 angle brackets onto the chassis and then place the chassis on the rack.

Step 3: Connect the power cord.

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

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

Step 4: Connect the network cable.

Step 5: 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.

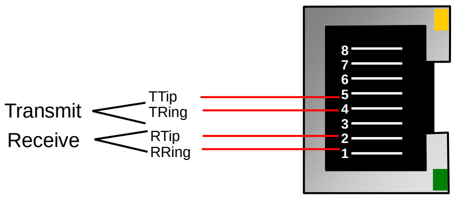


Figure 2-1 Pin Layout for E1 Interface

Step 6: 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 System Login. We suggest you change the initial username and password via 'System Tools → Change Password' on the WEB interface as soon as possible after your first login. For detailed instructions about changing the password, refer to Change Password. After changing the password, you are required to log in again.

Step 7: Modify IP address of the gateway.

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

Step8: 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 PCM for detailed instructions about PCM Settings.

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

Step 9: Configure signaling protocol parameters.

Further configure the signaling protocol you set in Step 8. Different protocols are configured on different interfaces. See below for detailed instructions.

- **SS7-ISUP:**

Note: For your easy understanding and manipulation, this step does not involve the ISUP quasi-associated mode configuration and the dual gateway feature. For descriptions about these configurations, refer to SS7 Settings.

The configuration interfaces related to SS7-ISUP include: SS7, ISUP and SS7 Server.

On your initial use of the SMG digital gateway, you may adopt the default values of the configuration items on the SS7 and ISUP interfaces. Note that the SS7 Server interface must be configured properly. Otherwise, the PSTN trunks may be unavailable. Follow the instructions here to configure the SS7 Server:

Step 1: Set OPC, Server IP and Signaling Point Code Standard. The OPC is generally allocated by the central office. The Server IP is the IP address of the SS7 server and you may use its default value. The Signaling Point Code Standard, which varies on the PBX model, can be set to 24 or 14. After modification, click the 'Modify' button on the right to save the settings.

Step 2: Modify the current link or click the 'Add New' button below the signaling link list to add a new link. Enter the physical address of the actually used signaling PCM (E1 interface) and click 'Save' to save the modification. If only one PCM is used for signaling in the gateway, you need just configure one signaling link.

Step 3: Modify the current linkset or click the 'Add New' button below the signaling linkset list to add a new linkset. You shall select the link configured in Step 2 for 'Link' and use the default values for the other configuration items. After modification, click 'Save'.

Step 4: Modify the current DPC or click the 'Add New' button below the DPC list to add a new DPC. Fill in 'SP Code' with the signaling point code of the remote end (i.e. signaling destination), select the linkset configured in Step 3 for 'Linkset' and use the default values for the other configuration items. After modification, click 'Save'.

Step 5: Modify the current UP_DPC or click the ‘Add New’ button below the UP_DPC list to add a new UP_DPC.

Step 6: Modify the current CIC routing rule or click the ‘Add New’ button below the ISUP_CIC routing rule list to add a new CIC routing rule. Select the DPC configured in Step 4 for ‘DPC’, fill in ‘CIC_PCM’ according to the actual allocation and use the default values for the other configuration items. After modification, click ‘Save’. Note that if multiple PCMs in the gateway are used for voice transmission, they should be configured with multiple CIC routing rules accordingly.

Note: After configuring SS7-ISUP related interfaces, you shall restart the service to validate the settings. Refer to Restart for detailed instructions.

- **SS7-TUP:**

Note: For your easy understanding and manipulation, this step does not involve the TUP quasi-associated mode configuration and the dual gateway feature. For descriptions about these configurations, refer to SS7 Settings.

The configuration interfaces related to SS7-TUP include: SS7, TUP and SS7 Server.

On your initial use of the SMG digital gateway, you may adopt the default value of the configuration items on the SS7 and TUP interfaces. Note that the SS7 Server interface must be configured properly. Otherwise, the PSTN trunks may be unavailable. Follow the instructions here to configure the SS7 Server:

Step 1: Set OPC, Server IP and Signaling Point Code Standard. The OPC is generally allocated by the central office. The Server IP is the IP address of the SS7 server and you may use its default value. The Signaling Point Code Standard, which varies on the PBX model, can be set to 24 or 14. After modification, click the ‘Modify’ button on the right to save the settings.

Step 2: Modify the current link or click the ‘Add New’ button below the signaling link list to add a new link. Enter the physical address of the actually used signaling PCM (E1 interface) and click ‘Save’ to save the modification. If only one PCM is used for signaling in the gateway, you need just configure one signaling link.

Step 3: Modify the current linkset or click the ‘Add New’ button below the signaling linkset list to add a new linkset. You shall select the link configured in Step 2 for ‘Link’ and use the default values for the other configuration items. After modification, click ‘Save’.

Step 4: Modify the current DPC or click the ‘Add New’ button below the DPC list to add a new DPC. Fill in ‘SP Code’ with the signaling point code of the remote end (i.e. signaling destination), select the linkset configured in Step 3 for ‘Linkset’ and use the default values for the other configuration items. After modification, click ‘Save’.

Step 5: Modify the current UP_DPC or click the ‘Add New’ button below the UP_DPC list to add a new UP_DPC.

Step 6: Modify the current CIC routing rule or click the ‘Add New’ button below the TUP_CIC routing rule list to add a new CIC routing rule. Select the DPC configured in Step 4 for ‘DPC’, fill in ‘CIC_PCM’ according to the actual allocation and use the default values for the other configuration items. After modification, click ‘Save’. Note that if multiple PCMs in the gateway are used for voice transmission, they should be configured with multiple CIC routing rules accordingly.

Note: After configuring SS7-TUP related interfaces, you shall restart the service to validate the settings. Refer to Restart 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 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 Restart for detailed instructions.

Step 10: 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 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 11: 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 Change Password.

After login, you can see the main interface.

3.2 Operation Info

Operation Info includes eight parts: ***System Info***, ***PSTN Status***, ***PCM Info***, ***SS7 Server***, ***IP Call Monitor***, ***SMG Call Monitor***, ***Call Count*** and ***Warning Info*** showing the current running status of the gateway.

3.2.1 System Info

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

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>MAC Address</td><td>MAC address of LAN 1 or LAN 2.</td></tr>
<tr><td>IP Address</td><td>The three parameters from left to right are IP address, subnet mask and default gateway of LAN 1 or LAN 2.</td></tr>
<tr><td>IPV6 Address</td><td>IPV6 address.</td></tr>
<tr><td>DNS Server</td><td>DNS server address of LAN 1 or LAN 2.</td></tr>
<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 six options: 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 1000 Mbps Full Duplex and Disconnected.</td></tr>
<tr><td>Network Type</td><td>The type of the network, including three options: Static, DHCP and PPPoE.</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>Master Server</td><td>The current gateway applies the SS7 protocol and is used for both signaling and voice transmission. If the dual gateway feature is enabled, the current gateway serves as the master server.</td></tr>
<tr><td>Slave Server</td><td>The current gateway applies the SS7 protocol and is used for both signaling and voice transmission. This operating mode works only when the dual gateway feature is enabled and the current gateway serves as the slave server.</td></tr>
<tr><td>Client</td><td>The current gateway applies the SS7 protocol and is only used for voice transmission.</td></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>
</table>

CPU Temperature	Display the real time temperature of the CPU. Note: This feature is unavailable for SMG2000 series.
CPU Usage Rate	Display the real time usage rate of the CPU.
Current RTP Message Data	Display the receiving and sending information of the current RTP data.
DCMS Working Status	Display the connecting status of the gateway and DCMS.
Recording Work Status	Display the working status of the recording server connected with the gateway.
Authorization Status	Display the features of the SBC device, which requires authorization.
Authorization Numbers	Display the number of authorized devices.
Remaining Time	Display the remaining time after successful authorization.
Serial Number	Unique serial number of an SMG digital gateway.
WEB	Current version of the WEB interface.
Gateway	Current version of the gateway service.
Uboot	Current version of Uboot.
Kernel	Current version of the system kernel on the gateway.
Firmware	Current version of the firmware on the gateway.

3.2.2 PSTN Status

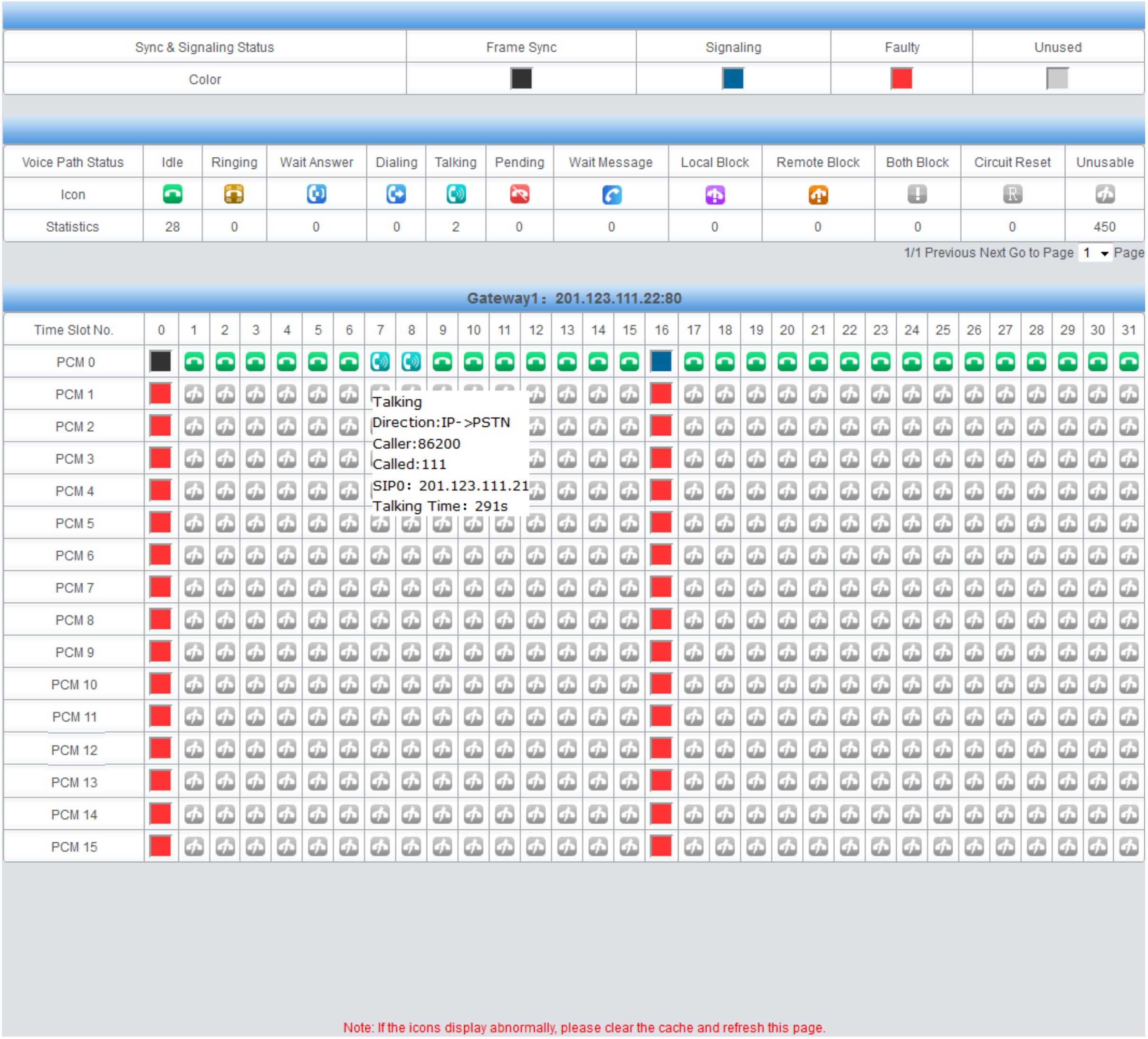


Figure 3-2 PSTN Status Interface for E1 Lines

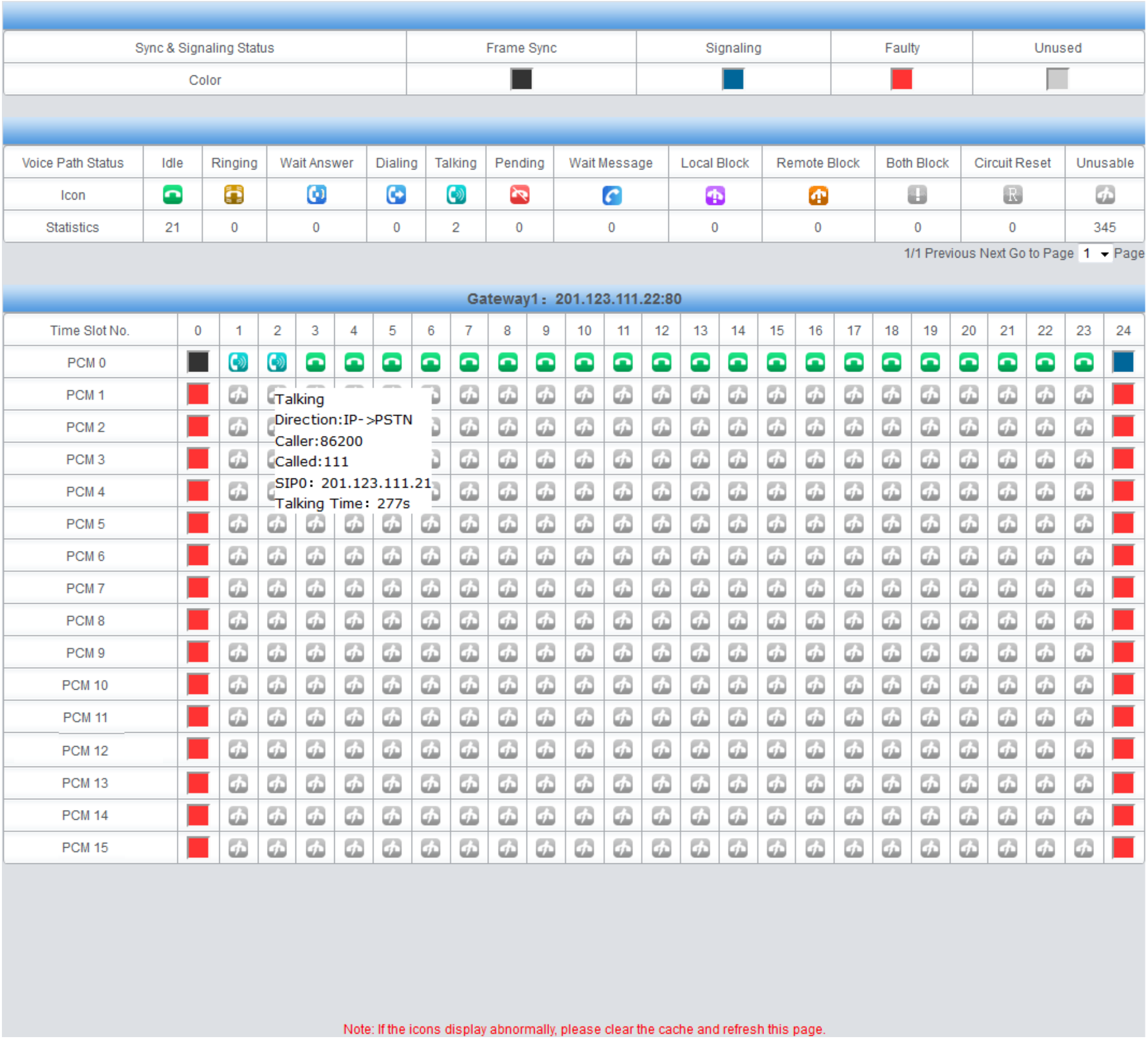


Figure 3-3 PSTN Status Interface for T1 Lines

See Figure 3-2 and Figure 3-3 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.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Port</td><td>Serial number of the E1/T1 port on the device.</td></tr>
<tr><td>Time Slot No.</td><td>PCM time slot number in the port.</td></tr>
<tr><td>State</td><td>Displays the channel state in real time. You can move the mouse onto the channel state icon for detailed information about the channel and the call, such as: call direction, calling party number and called party number.
● For Time Slot 0, the channel state indicates the synchronization status of E1/T1.<table><tr><th>State</th><th>Color</th><th>Description</th></tr><tr><td>Frame Sync</td><td></td><td>Frame synchronization normal. The synchronization status is 0x0.</td></tr></table></td></tr>
</table>

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 SS7, this state indicates ‘SS7 in service’. 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 SS7, this state indicates ‘SS7 out of service’, ‘initial alignment’, ‘aligned ready’, ‘aligned not ready’ or ‘processor outage’. 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	R	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 3-2, Figure 3-3, 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 3-4, after we input the character 111 to the search box, and click the ***Search*** button, the gateway does a fuzzy search and locates that the ongoing call whose CalledID contains the character 111 occurs on Time Slot No. 8 of PCM 0.

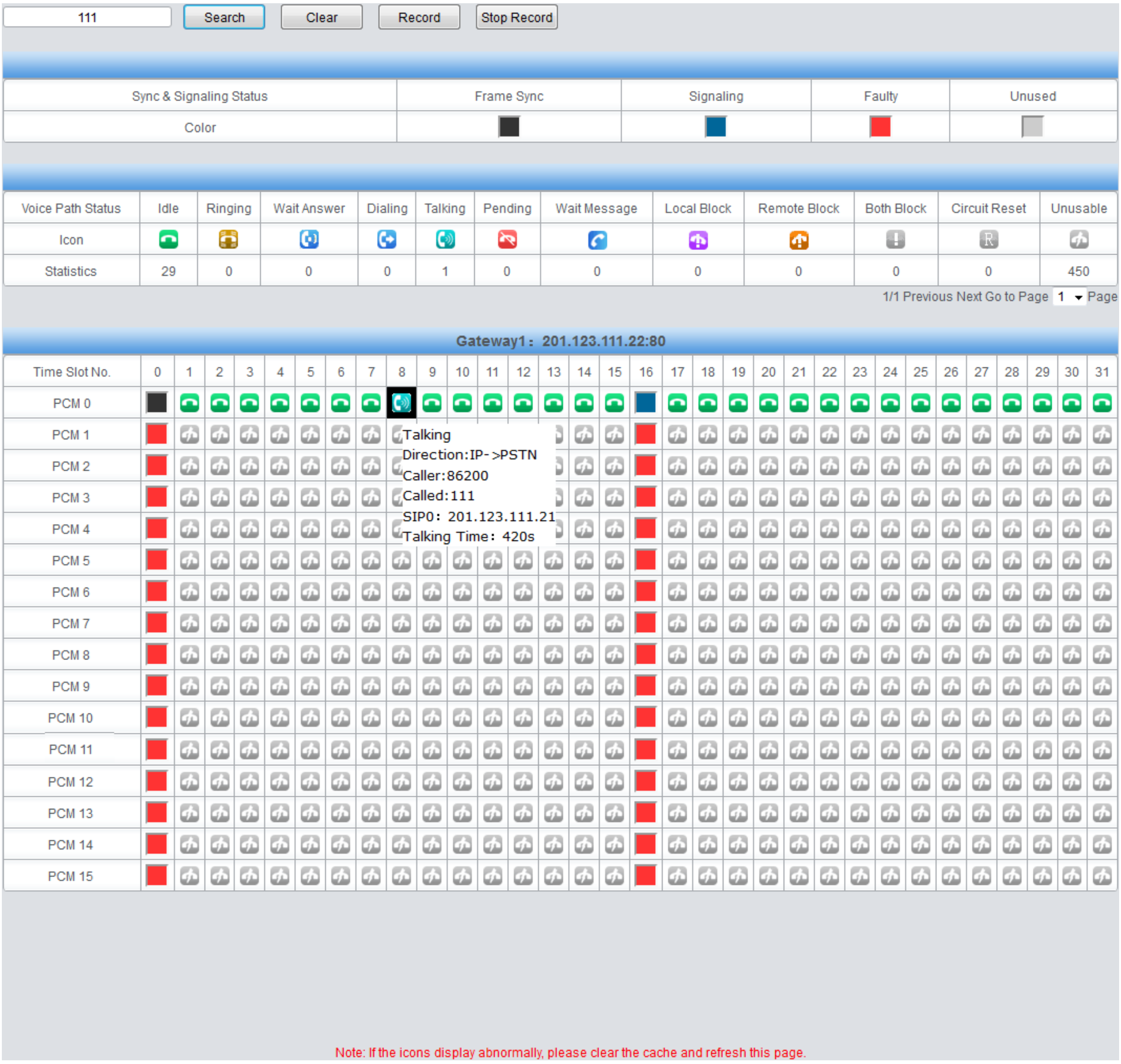


Figure 3-4 Search Calls

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

The PCM Info interface 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 SS7 Server

Users can see the SS7 Server option in the menu only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *SS7-TUP* or *SS7-ISUP*. The SMG2030S, SMG2060S and SMG2120S series don't support SS7.

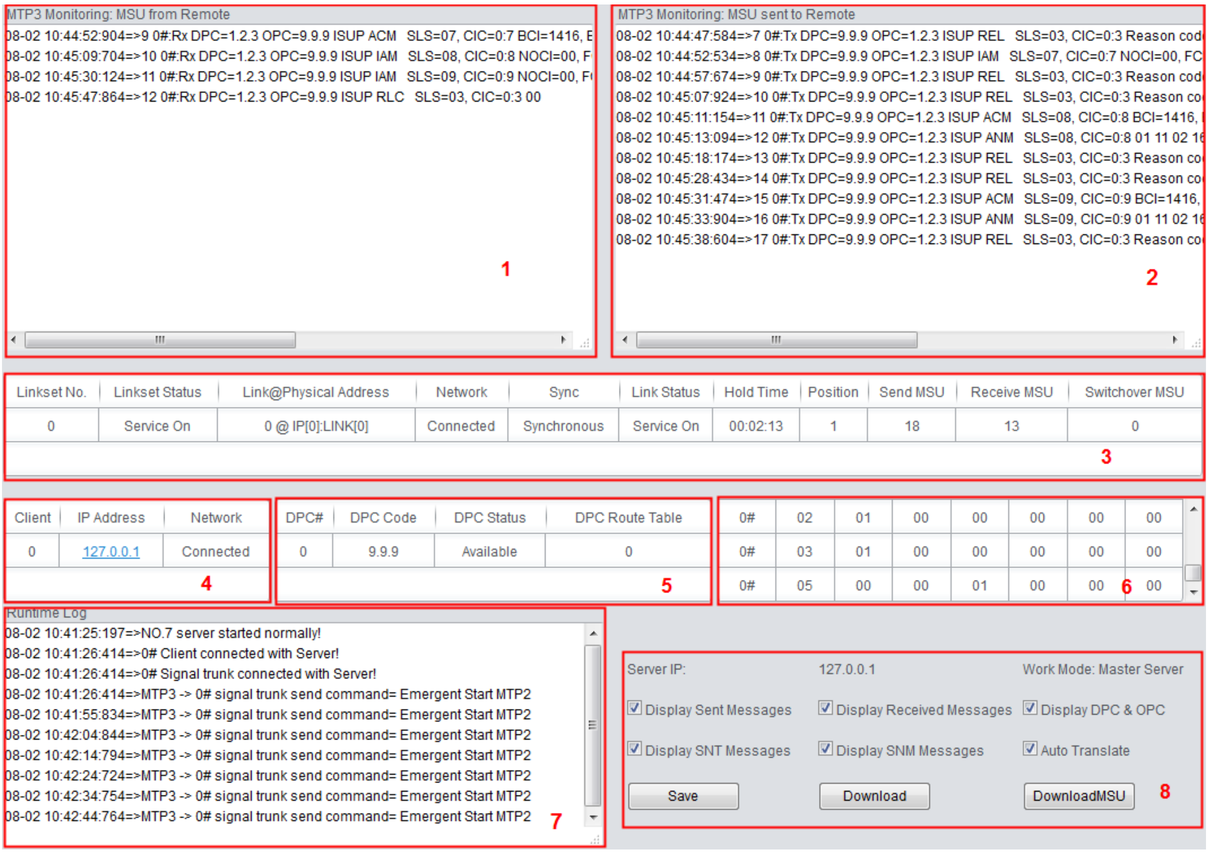


Figure 3-5 SS7 Server Info Interface

See Figure 3-5 for the SS7 server info interface. This interface contains 7 status bars (Status Bar 1~7 in the above figure) and a configuration region (Region 8 in the above figure). Below are the detailed introductions.

- **Status Bar 1 & 2: Receive/transmit message list**

The receive/transmit message lists display the received and sent messages respectively, used for gateway debugging. The display content in these lists can be set by the configuration items in Region 8.

- **Configuration Region 8: Properties configuration for receive/transmit message list**

The table below explains the items in Configuration Region 8.

Item	Description
Server IP	IP address of the SS7 server, this item can be configured on the SS7 interface.
Work Mode	Work mode of the SS7 server which includes three modes: Master Server, Slave Server and Client.
Display Sent Messages	If this item is ticked, the transmit message list will display the message sent to the remote end.
Display Received Messages	If this item is ticked, the receive message list will display the message received from the remote end.
Display DPC & OPC	If this item is ticked, the receive/transmit message list will display DPC and OPC.
Display SNT Messages	If this item is ticked, the receive/transmit message list will display the SNT messages.
Display SNM Messages	If this item is ticked, the receive/transmit message list will display the SNM messages.

Auto Translate	If this item is ticked, the received/sent messages displayed on this interface will be translated automatically in the following format: Date Time Total number Signaling link number# SIO Content For the TUP messages, SIO is just 'TUP' (0x84), followed by the message content. It is usually in the following format: Title code CIC=PCM:TS Message body If this item is not ticked, the received/sent messages displayed on this interface will be hexadecimal raw data.

Users can configure the display content of the receive/transmit message list via the checkbox before each configuration item. After modification, click ***Save*** to apply the configurations. The changes will be shown in the list in real time. Click ***Download*** and you can download the log information of the SS7 server.

- **Status Bar 3: Linkset/signaling link information**

This region displays the information about signaling links and linksets. The table below explains the information items in Status Bar 3.

Item	Description
Linkset No.	Linkset number.
Linkset Status	Working state of the linkset, including *In service* and *Out of service*. A signaling linkset will go into the state *In service* as long as one link in it is at the state of *In service*.
Link@Physical Address	Signaling link number and its physical position. For example, '0 @ IP[0]:PCM[0]' means the physical position of Link 0 in this gateway is the E1 with the local PCM numbered 0 on Client 0.
Network	Whether the signaling link is registered to the gateway, including two states: *Connected* and *Disconnected* (or no display). The signaling link can be used normally only in the state of *Connected*.
Sync	Basic frame synchronization (Time Slot 0), including two states: *Sync* and *Async*. The signaling link can be used only in the state of *Sync*.
Link Status	Working state of the signaling link, including *In service* and *Initial alignment*. You can refer to 'Status Bar 6: Link information' for detailed information about link status.
Hold Time	Duration since the last time the signaling link enters into the state of *In service*.
Position	Times of positioning that occurs on the signaling link since the program starts.
Send MSU	Total number of messages sent on the signaling link since the program starts.
Receive MSU	Total number of messages received on the signaling link after the program starts.
Switchover MSU	Total number of messages switched over on the signaling link since the program starts.

- **Status Bar 4: Client information**

This region displays the information about client IP address and connection state. The table below explains the information items in Status Bar 4.

Item	Description
Client	Client number.

IP Address	IP address of the client. You can click the link of the IP address to visit the WEB interface of the client.
Network	Whether the client has been successfully connected to the gateway, including two states: *Connected* and *Disconnected* (or no display).

- **Status Bar 5: DPC Information**

This region displays the information about DPC. The table below explains the information items in Status Bar 5.

Item	Description
DPC#	DPC number which starts from 0.
DPC Code	Destination point code which is usually allocated by the central office.
DPC Status	Indicates whether the route to this DPC is available, involving two states *Available* and *Unavailable*. The message can be sent to the DPC only when the route to this DPC is at the state of *Available*. The DPC will turn into the state of *Available* as long as one of the linksets reaching the DPC is at the state of *In Service*.
DPC Route Table	Route to the DPC, i.e. linkset number.

- **Status Bar 6: Link information**

This status bar displays the detailed information on the state of all signaling links, usually used for searching the cause of service interrupt on a signaling link.

Link#	STA	L2	POC	LSC	FSN	ERR	CHO
Link Number	Link States 0-6	Link Failure Causes (interrupt)	Processor Failures 0-3	Live Communication Server Service 0-1	Forward Sequence Number	spare	spare
	0: uploaded but not started	0: normal	0: normal	0: service is unavailable			
	1: service interrupt	1: BSNR illegal	1: the local end processor failure	1: service is available			
	2: initial positioning	2: FIBR illegal	2: the remote end processor failure				
	3: positioned/ ready	3: T2 timeout	3: both ends processor failure				
	4: positioned/ not ready	4: T6 timeout, the remote end busy					

	5: service on	5: L3 sends a command to stop					
	6: processor failure	6: signaling error rate too high					
		7: during the course of initial positioning, fail to enter a normal position					
		8: Timer 1 timeout					
		9: positioned and ready, receive the interrupt signal of the remote end					
		10: positioned but not ready, receive the interrupt signal of the remote end					
		11: in the state of Service On, receive the interrupt signal of the remote end					
		12: in a processor failure, receive the interrupt signal of the remote end					

- **Status Bar 7: Runtime Log**

Runtime log records all MTP3 commands and error information that pops up during the operation. This status bar displays all the log records generated after the digital gateway starts.

3.2.5 IP/SMG Call Monitor

On the Call Monitor interface, you can set a condition for call monitoring. For example, 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 on this interface.

Item	Description

Monitored CallerID, Monitored CalleeID, Monitored Remote Address	Sets the condition for the call monitoring. You can set to monitor the calls by CallerID, CalleeID or remote address.
Monitoring LAN Port	Selects the LAN port which is used to monitor the calls.
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, *IP Call Monitor* including only one option IPCallIn while *SMG Call Monitor* 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.

3.2.6 Call Count

The Call Count interface lists the detailed information about all the calls counted from the startup of the gateway service to the latest open or refresh of this interface. 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 on this interface.

Item	Description
SIP Index	The index of the SIP trunk.
Description	More information about each SIP trunk group.
SIP Trunk Address	Address of the SIP trunk, i.e. the IP address or domain name of the remote SIP terminal which will establish a call conversation with the gateway.
Current	The number of the current incoming/outgoing SIP calls.
Sum	The total number of the incoming 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, SS7-TUP, SS7-ISUP, 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.

3.2.7 Warning Info

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

3.3 SIP Settings

SIP Settings includes seven parts: ***SIP***, ***SIP Trunk***, **SIP Register**, ***SIP Account***, ***SIP Trunk Group***, ***Media*** and ***Hang Up Reason***. ***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. ***Hang Up Reason*** is used to set the suspension reason.

3.3.1 SIP

On the SIP Settings interface, you can configure the general SIP parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to Restart for detailed instructions. The table below explains the items on this interface.

Item	Description
SIP Address of WAN	IP address of WAN for SIP signaling, using LAN 1 by default.
SIP 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.
TLS	After this feature is enabled, TLS will be available in *Transport Protocol* under *SIP trunk*, which is disabled by default.
SIP TLS Signaling Port	Port of TLS signaling. Range of value: 2000~65535, with the default value of 5061.
Send 180 before 183	When the gateway SIP side is used as the called party, it will send the 180 message first and then the 183. By default it is disabled.
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 180/183 message. The default setting is disabled.
IP Call in First Route	The SBC device features authorized by the gateway, two options available: IP->IP or IP->PSTN. The default setting is IP->PSTN.
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 four optional ways to obtain the calling party number: Username of "From" Field, Displayname of "From" Field, *P-Preferred-Identity Field, P-Asserted-Identity Field*. The default value is *Username of "From" Field*.
Obtain/Send CalleeID from	There are two optional ways to obtain or send the called party number: from "To" Field or from "Request" Field. The default value is from "*Request" Field*.
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.
Prack Send Mode	Sets whether to return the prack message while receiving the 180/183 message which carries the 100rel field. Three options are available: Disable, Supported and Require, and the default setting is Disable.
DisplayName	Sets whether to carry the actual calling number in the DisplayName field of the SIP message sent by the gateway. The default setting is Hide.
UserName	Sets whether to carry the gateway registered number in the UserName field of the SIP message. The default setting is Change Caller.
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*.
Set Redirection Parameter of REL Message When Receive Refer Message	If this feature is enabled, once receiving the Refer message, the SIP side will send the REL message carrying the redirection parameter to the E1 side.
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*.
Multiple Audio Selection	Since the SDP message carries multiple audio types, you can choose RTP or SRTP as the voice port.
Send Response by Former Via	To IP->PSTN calls, enabling this feature means to close the automatic modification on the Via header of the response message. By default it is disabled.
Registration Related Settings	When this feature is enabled, the available call time for each SIP registered account as well as the SIP Registered Number Polling feature can be set. By default it is disabled.
Time (min/month)	Specifies the call time for a SIP registered account.
SIP Registered Number Polling	When this feature is enabled, the call is polled among SIP registered accounts. By default it is disabled.
Failed Count	It is valid only when the feature *SIP Registered Number Polling* is enabled. After a number is called out and fails for set times, it will be kicked out of the cycle and then allowed to re-join after *Recover Time of Disable Account*.
Recover Time of Disable Account (m)	See the description of *Failed Count*.

Caller Prefix Grouping	When this feature is enabled, only if the calling number of the call matches the caller prefix on the page of the SIP registered account will the rated time be used.
Caller over Clocking (IP OUT)	Limit on the number of calls in a cycle for the calling number. By default this feature is disabled.
Cycle (min)	The time of a cycle. It is only valid when the feature *Caller over Clocking* is enabled.
Count Values	The allowed incoming calls within the set time of a cycle. It is only valid when the feature *Caller over Clocking* is enabled.
Interval (ms)	The interval time for calls from a same calling number. After hangup, the gateway needs to wait for some time before using this account. It is only valid when the feature *Caller over Clocking* is enabled.
Eth Resource	The limit on the RTP resources occupied simultaneously by a single network port. It can be configured in the SIP settings. By default it is disabled.
Eth Resource Num	The number of network port resources is an integer greater than 0. The default value is 2.
SIP Account Numbers	The maximum number of SIP accounts must be set greater than the number of existing SIP accounts. The default value is 2000.
SIP Account Registration Interval	The interval between registrations of multiple SIP accounts. Range of value: 0~10000, with the default value of 0.
DSCP	Sets whether to enable the DSCP differentiated services code point. By default, it is *disabled*.
Voice Media	Sets the priority of the voice media for DSCP. The voice media with a bigger value has a higher priority. The value range is 0~63, with the default value of *46*.
Signal Control	Sets the priority of the signal control for DSCP. The signal control with a bigger value has a higher priority. The value range is 0~63, with the default value of *26*.
Calls from SIP Trunk Address only	Once this feature is enabled, the gateway will only accept the calls from the IP addresses set in SIP Settings → SIP Trunk. By default, it is *disabled*.
Match Call Count to SIP Trunk based on Source Address of INVITE	Performs call count by matching the source address of the INVITE message. By default it is disabled.
Switch Signal Port if SIP Registration Failed	If the SIP registration fails, the SIP signaling port N will switch to N+1 for a new registration. It will continue until the registration succeeds.
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*.
Sip Trunk Heart	Sets whether to send the option message to the SIP trunk. The calls routed to this trunk will be rejected directly if the times of no answer from the MGCF trunk exceed the set value.
Trunk Heartbeat Cycle	The cycle to send the option message to the SIP trunk.
Allowed Times of NoResponse	The allowed times of SIP's no answer to the option message.
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*.
Support 100rel	Sets whether to carry 100rel in the Supported field of the request message for IP calls out. By default it is disabled.
Not Wait ACK after Sending 200 OK	Once this feature is enabled, the gateway does not need to wait the ACK message after sending the 200OK message. The default value is *disabled*.
Match SIP Trunk Port	Sets whether to search SIP trunks by matching port number for IP calls in. By default it 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, you need to set the TO field in "Add Content". By default it is disabled.
Add Content	Customizes the content added to the TO field, such as user=phone.

UserAgent Field	Sets the content of the UserAgent field. Currently, it only supports the English uppercase and lowercase letters.

3.3.2 SIP Trunk

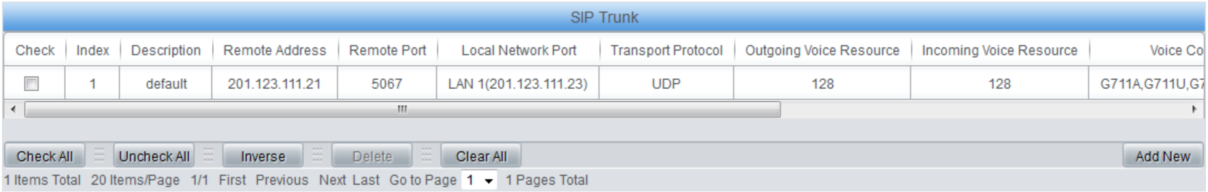


Figure 3-6 SIP Trunk Settings Interface

See Figure 3-6 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 3-7 for the SIP trunk adding interface.

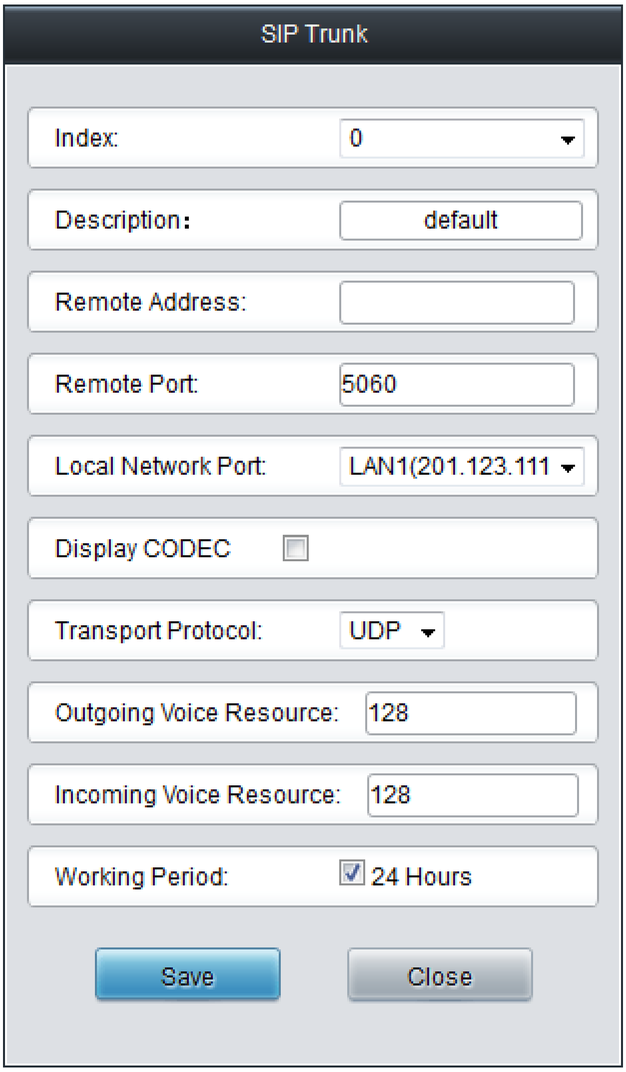


Figure 3-7 Add New SIP Trunk

The table below explains the items shown in Figure 3-7.

Item	Description
Index	The unique index of each SIP trunk.
Description	More information about each SIP trunk group.

<table>
<tr><td>SIP Agent</td><td>The SBC feature needs to be authorized. After this feature is enabled, the SIP terminal can register to the gateway and become the SIP agent of the gateway. By default it is disabled.</td></tr>
<tr><td>Username</td><td>When SIP Agent is enabled, it is the username for the SIP terminal to register with the gateway.</td></tr>
<tr><td>Password</td><td>When SIP Agent is enabled, it is the password for the SIP terminal to register with the gateway.</td></tr>
<tr><td>Remote Address</td><td>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.</td></tr>
<tr><td>Remote Port</td><td>Port of the SIP trunk.</td></tr>
<tr><td>Local Network Port</td><td>The network port where the SIP trunk locates.</td></tr>
<tr><td>Display CODEC</td><td>Used to hide or unhide the CODECs with the packing time.</td></tr>
<tr><td>Transport Protocol</td><td>SIP transport protocol, providing two modes UDP and TCP. The default value is UDP.</td></tr>
<tr><td>SRTP Mode</td><td>Sets the way, RTP or SRTP, to send the voice package in IP outgoing calls.</td></tr>
<tr><td>Outgoing Voice Resource</td><td>Maximum number of voice channels for the outgoing calls allocated by the SIP trunk to the gateway.</td></tr>
<tr><td>Incoming Voice Resource</td><td>Maximum number of voice channels for the incoming calls allocated by the SIP trunk to the gateway.</td></tr>
<tr><td>DTMF Transmit Mode</td><td>Sets the mode, RFC2833 or in-band, for the SIP trunk to send DTMF signals. If here is set Global, the DTMF transmit mode configured on the Media Settings interface will be used.</td></tr>
<tr><td>Fax Mode</td><td>Sets the mode, T30 or T38, for the SIP trunk to fax. If here is set Global, the fax mode configured on the Fax Settings interface will be used.</td></tr>
<tr><td>Working Period, Period</td><td>The work period for the gateway, You can specify a certain period for the gateway to make calls. By default, the gateway is allowed to make calls any time in the day (24 Hours).</td></tr>
<tr><td>CODEC</td><td>Supported CODECs and their corresponding priorities for the SIP trunk to establish a call conversation. The table below explains the sub-items:
<table>
<tr><th>Sub-item</th><th>Description</th></tr>
<tr><td>Priority</td><td>Priority for choosing the CODEC in an SIP conversation. The smaller the value is, the higher the priority will be.</td></tr>
<tr><td>CODEC</td><td>Seven optional CODECs are supported: G711A, G711U, G729 G722, G723, iLBC, AMR, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K).</td></tr>
</table>
See Media Settings for the detailed parameters for each CODEC.
The default CODEC for the SIP trunk is the same as that set in Media Settings.</td></tr>
<tr><td>VOS1.1 SIP Encryption</td><td>Set whether to perform VOS1.1 encryption for SIP signaling, including three modes: No Encryption, Gateway Encryption, and Client Encryption. The default setting is No Encryption.</td></tr>
<tr><td>Encrypt Key</td><td>A key that encrypts SIP signaling.</td></tr>
</table>

VOS1.1 RTP Encryption	Set whether to perform VOS1.1 encryption for RTP. By default it is disabled.
Externally Bound Enable	Sets whether to enable the Proxy feature. Once it is enabled, SIP messages will be sent to the proxy address.
Externally Bound Address	The proxy address.
Externally Bound Port	The proxy port.
SIP Trunk Heart Mode	Only when this feature is enabled will the destination address configured for the OPTION message appear. There are three options available: ***Disable, MGCF*** and ***GWC***. GWC means the destination address of the OPTION message is just the trunk address while MGCF means the destination address of the OPTION message is configurable. This feature is disabled by default.

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

Click ***Modify*** in Figure 3-6 to modify a SIP trunk. The configuration items on the SIP trunk modification interface are the same as those on the ***Add New SIP Trunk*** interface.
To delete a SIP trunk, check the checkbox before the corresponding index in Figure 3-6 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 3-6.

3.3.3 SIP Register

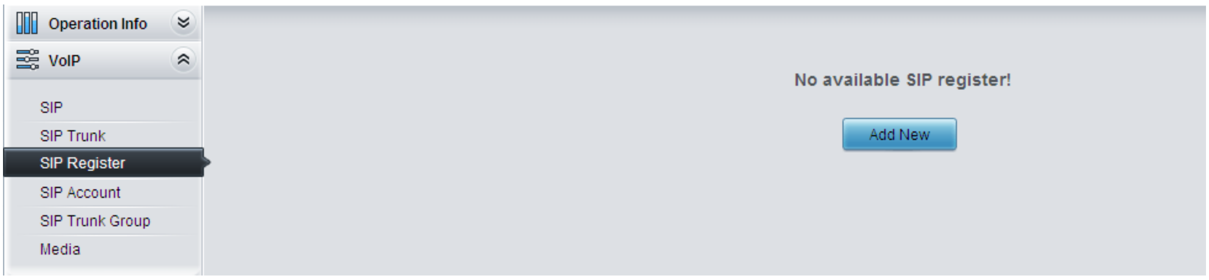


Figure 3-8 SIP Register Configuration Interface

See Figure 3-8 for the SIP Register Configuration interface. By default, there is no SIP register available on the gateway. Click ***Add New*** to add them manually.

The table below explains the items shown on the interface.

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

Register Port	The signaling port of the SIP trunk.
Domain Name	Domain name of the gateway used for SIP registry.
Register Expires	Validity period of the SIP registry. Once the registry is overdue, the gateway should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
Authentication Username	Authentication username for registration.

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

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

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

3.3.4 SIP Account

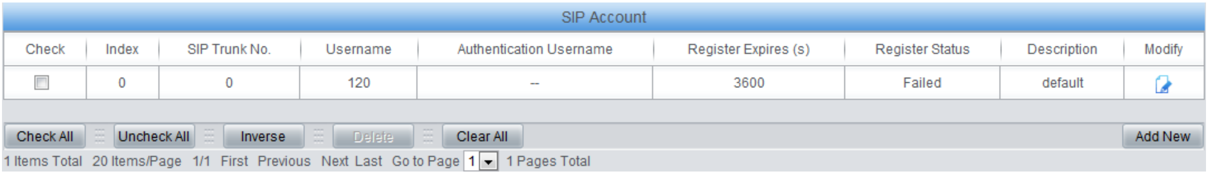


Figure 3-9 SIP Account Settings Interface

See Figure 3-9 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.

The table below explains the items shown on the interface.

Item	Description
Index	The unique index of each SIP account.
SIP Trunk No.	The number of the SIP trunk to which the SIP account is registered.
Username	The registration username of the SIP account. Once the SIP account is successfully registered, the SIP server can initiate calls to the gateway via ***Username***.
Password	The registration password of the SIP account. To register the SIP account to the SIP trunk, both configuration items ***Username*** and ***Password*** should be filled in.
Register Expires	The validity period of the SIP account registry. Once the registry is overdue, the SIP account should be registered again. Range of value: 10~3600, calculated by s, with the default value of 3600.
Register Status	The registration status of the SIP account. It is either *Registered* or *Failed*.
Authentication Username	Authentication username of a port, used to register the port to the SIP server when IMS network is enabled.
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 3-9 to modify a SIP account. The configuration items on the SIP account modification are the same as those on the ***Add New SIP Account*** interface.

To delete a SIP account, check the checkbox before the corresponding index in Figure 3-9 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 3-9.

3.3.5 SIP Trunk Group

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

The table below explains the items shown on the interface.

Item	Description
Index	The unique index of each SIP trunk group, which is mainly used in the configuration of routing rules and number manipulation rules to correspond to SIP trunk groups.
Description	More information about each SIP trunk group.
SIP Trunk Select Mode	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.
Outgoing/Incoming Call Restriction	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.
SIP Trunks	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'.

Option	Description
Increase	Search for an idle SIP trunk in the ascending order of the SIP trunk number, starting from the minimum.
Decrease	Search for an idle SIP trunk in the descending order of the SIP trunk number, starting from the maximum.
Cyclic Increase	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.
Cyclic Decrease	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.

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

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

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

3.3.6 Media Settings

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

Item	Description
DTMF Transmit Mode	Sets the mode for the IP channel to send DTMF signals. The optional values are *RFC2833*, *In-band*, *Signaling*, *RFC2833+Signaling* and *In-band+Signaling*, with the default value of *RFC2833*.
RFC2833 Payload	Payload of the RFC2833 formatted DTMF signals on the IP channel. Range of value: 90~127, with the default value of *101*.
RTP Port Range	Supported RTP port range for the IP end to establish a call conversation. Range of value: 5000~60000, with the lower limit of 6000 and the upper limit of 10000.The difference between for SMG2000 series (2030, 2060, 2120) is not less than 512 and that for SMG3000 series (3008, 3016) is not less than 2048.
Silence Suppression	Sets whether to send comfort noise packets to replace RTP packets or never to send RTP packets to reduce the bandwidth usage when there is no voice signal throughout an IP conversation. The optional values are *Enable* and *Disable*, with the default value of *Disable*. **Note:** When G723 is selected as CODEC, this configuration setting will turn to Enable automatically.
Noise Reduction	Once this feature is enabled, the volume of the noise accompanied with the line will be reduced automatically. The default setting is *Enable*.
JitterMode	Sets the working mode of JitterBuffer. The optional values are *Static Mode* and *Adaptive Mode*, with the default value of *Static Mode.*
JitterBuffer	Acceptable jitter for data packets transmission over IP, which indicates the buffering capacity. A larger JitterBuffer means a higher jitter processing capability but as well as an increased voice delay, while a smaller JitterBuffer means a lower jitter processing capability but as well as a decreased voice delay. Range of value: 0~280, calculated by ms, with the default value of 100.
JitterUnderrunLead	Sets the initial delay applied to 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 set to *Static Mode* will this item be shown.
JitterOverrunLead	Sets the beforehand time inserted if receiving packets is ahead of time (the time of receiving is earlier than 300 minus the value set in JitterBuffer). Rnage of value: 0~280, calculated by ms, with the default value of *50*, **Note:** Only when JitterMode is set to *Static Mode* will this item be shown.
JitterMin	Sets the minimum delay that can be set by the adaptive jitter function. It 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 set to *Adaptive Mode* will this item be shown.

<table>
<tr><td>JitterDecreaseRatio</td><td>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 set to Adaptive Mode will this item be shown.</td></tr>
<tr><td>JitterIncreaseMax</td><td>Sets the maximum delay that can be increased during one silence period. Range of value: 0~280, calculated by ms, with the default value of 30,
Note: Only when JitterMode is set to Adaptive Mode will this item be shown.</td></tr>
<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>Use Default Value if Packtime Negotiation fails</td><td>The default setting is Yes. The default value will be used if the RTP packing time negotiation fails. Please refer to the packing time set for the codec in the SIP trunk.</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-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K).</td></tr>
</table>
By default, all of the eleven CODECs are supported and ordered G711A, G711U, G729, G722, G723, iLBC, AMR-NB, SILK(16K), OPUS(16K), SILK(8K), OPUS(8K) by priority from high to low. The CODECs set here will be the default CODEC for the new added SIP trunks.
The packing time and bit rate supported by different CODECs are listed in the table below. Those values in bold face are the default values.
<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>
</table>
</td></tr>
</table>

	OPUS(16K)	10 / **20** / 40 / 60	**20**
	SILK(8K)	**20** /40 / 60 / 80 / 100	**20**
	OPUS(8K)	10 / **20** / 40 / 60	**20**
	Note: SMG3000-B1L, SMG3000-B2L and SMG3000-C1L only support G711A, G711U and G729 encoding.		

3.3.7 Hang Up Reason

SIP Code To ISUP/ISDN displays the corresponding release cause code set at the digital side when the IP side receives the status code. ***ISUP/ISDN Code To SIP*** displays the corresponding SIP status code set at the IP side when the digital side receives the release cause code. Press ***Default Add*** to add the default relationship between the release cause code and the SIP status code.

3.4 PCM Settings

PCM Settings includes nine parts: ***PSTN***, ***E1 Outgoing Call Timer***, ***Circuit Maintenance***, ***PCM***, ***PCM Trunk***, ***PCM Trunk Group***, ***Number-Receiving Rule***, ***Reception Timeout*** and ***PSTN Forwarding***.

3.4.1 PSTN

The table below explains the items shown on the PSTN Settings interface.

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	Sets whether to enable the Ringback Tone feature for the E1 or IP side. The default setting is *No Ringback Tone*.
Frequency 1, Frequency 2	Sets the first and second center frequency for the ringback tone, calculated by HZ. The default value of Frequency 1 is *450* and that of Frequency 2 is *0*.
High Level Duration, Low Level Duration	Sets the duration of the ringback tone respectively at on and off, calculated by ms.

PSTN->IP Call Ringback Tone Self-adaption	When it is enabled, the E1 side of the gateway will provide ringback tones if the received 180/183 message doesn't include P-Early-Media or the parameter value is inactive.
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*.
UUI Protocol Discriminator	Acquire the *user to user* field from the message in an incoming call, and assign it to the *Usr2UsrInfo* field in an outgoing call.
Protocol Discriminator	The protocol discriminator of Usr2UsrInfo for ISUP/ISDN, with the default value of 4.
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.
PCM Value Range for Hot Backup	Sets the value range of PCM for E1 hot backup.
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.
Caller Number Barring	The limit on the number of calls from the caller in the direction of IP->PSTN. Once the call times exceeds the set value, the call will be rejected directly.
Cycle	The number of the calls allowed for the caller to make during a time period.
Access Threshold for Caller Number	The number of the calls allowed for the caller to make.
SIP Respond Code	The message code returned by the IP side once the call times exceeds the set value.
Time Limit for E1 Outgoing Calls per Month	Once this feature is enabled, the call time for each E1 per month will be limited, with the default value of *disable*. It will be re-timed on the 1st day of each month. **Note:** This item is only supported by the SMG3016 series gateway.

Mode Selection	The mode to limit the call time for each E1, including two options: By Minute (The call time less than 1 min will be considered as 1 min) and By Second, with the default value of *By Minute*.
Time Limit	Set the call time for each E1, calculated by minute. The value must be greater than 1. If the schedule time is spent, the call on the E1 can go on as long as you reset the value to be greater than the previous one,
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.
Remote SIP Trunk ID	Sets the number of the remote SIP trunk group which is used for call forwarding as the E1 to E1 call fails.
Heart Beat Check Remote SIP Trunk	Sets whether to send the OPTION message to the SIP trunk.
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.
Send Ring to PSTN when Receive REFER	After receiving the REFER message, the gateway needs to play the sound to the E1 side, and the sound file can be uploaded in the backup loading interface (REFER sound file). By default it is disabled.
Send Ring to PSTN when Receive re-invite with SDP 'sendonly'	After receiving the re-invite message with sendonly, the gateway needs to play the sound file to the E1 side, and the sound file can be uploaded in the backup loading interface (REFER sound file). By default it is disabled.

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

3.4.2 E1 Outgoing Call Timer

The E1 Outgoing Call Timer interface displays all the available time for each E1 to make outgoing calls. The calls occur on the E1 which uses up the time and is blocked will be routed to other E1. Moreover, the gateway will forbid all E1 to make outgoing calls and reply the 404 message directly once the call time for all E1 runs out.

Note: This interface will be displayed only when the configuration item "***Time Limit for E1 Outgoing Calls per Month***" in PSTN setting is enabled.

3.4.3 Circuit Maintenance

On the Circuit Maintenance interface, you can block, unblock, physical connect or disconnect PCMs, ports and channels. 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.

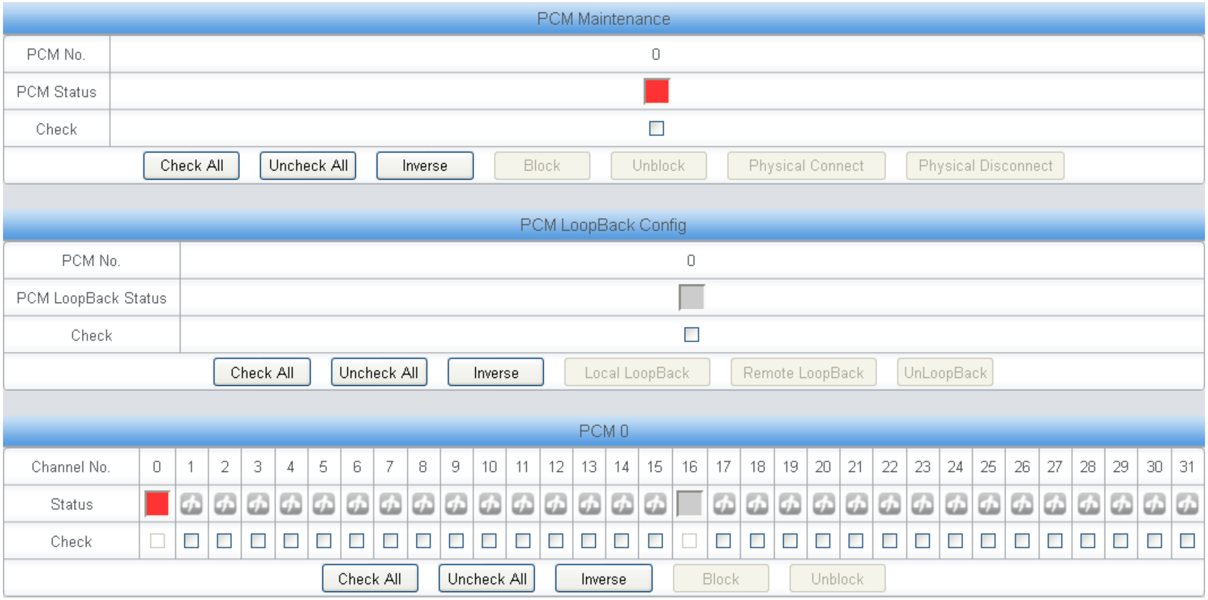


Figure 3-10 Circuit Maintenance Interface

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.

3.4.4 PCM

The PCM settings interface 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 Side, SS7-TUP, SS7-ISUP, and 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. 2, For SMG3008, a single gateway can be configured with two different signaling modes simultaneously. 3, For SMG3016, a single gateway can be configured with three different signaling modes simultaneously. 4, The SMG2030S, SMG2060S and SMG2120S series gateways don't support SS7. 5, The SMG2030L, SMG2060L, SMG3000-B1L, SMG3000-B2L and SMG3000-C1L series support SS7 after being authorized.

Control Mode	The way to select timeslots for outgoing calls at the SS7 side, with the default setting of None which means searching idle channels by point code: the party with a large point code controls even time slots while the party with a small point code controls odd time slots. If you select the mode 'Control Even Time Slots', channels will be searched following the even time slots in a 0, 2, 4, …, 30, 31, 29, 27, …, 1 sequence (except TS0, TS1 and TS16); if you select the mode 'Control Odd Time Slots', channels will be searched following the odd time slots in a 1, 3, 5, …, 31, 30, 28, 26, …, 0 sequence (except TS0, TS1 and TS16).
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. For SS7 signaling, up to 4 signaling time slots can be set.
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 or the channel blocks.

Click ***Modify*** to modify a PCM. Most configuration items on the PCM modification interface are the same as those on the ***PCM Settings*** interface.

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

Item	Description
Use 'Signaling Time Slot' for Signaling	If this item is checked, it indicates that the signaling time slot configured in ***Signaling Time Slot*** is used for signaling transmission. You can see this item only when the configuration item ***Signaling Protocol*** is set to *SS7-TUP* or *SS7-ISUP*.
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.

3.4.5 PCM Trunk

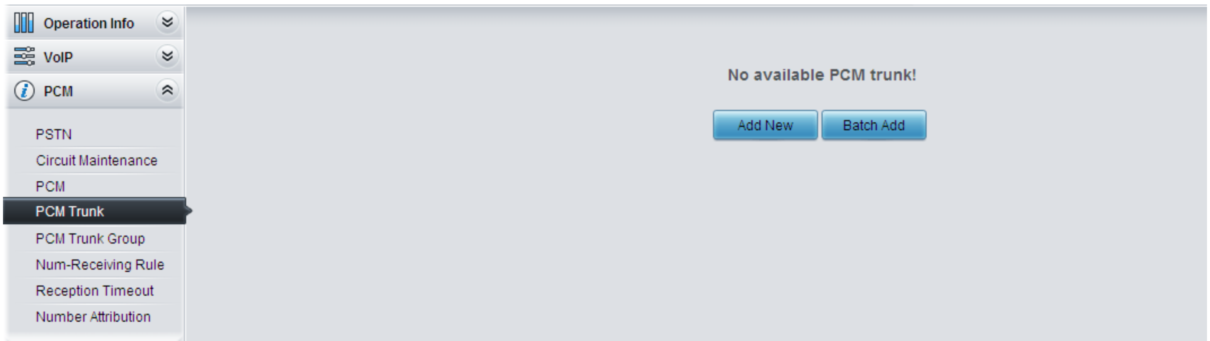


Figure 3-11 PCM Trunk Configuration Interface

See Figure 3-11 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.

The table below explains the items shown on the interface.

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.

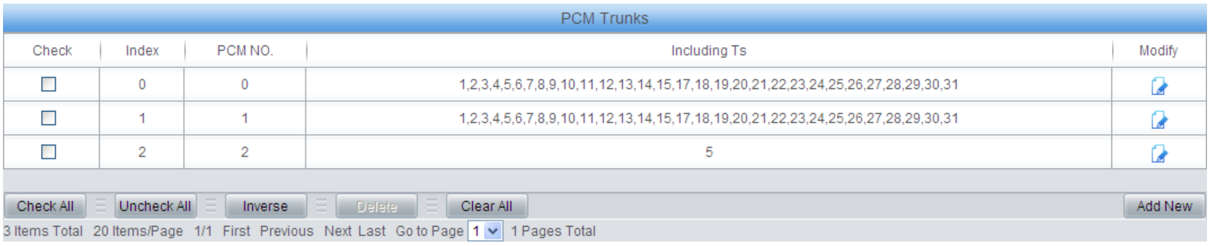


Figure 3-12 PCM Trunks List

Click ***Modify*** in Figure 3-12 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.

To delete a PCM trunk, check the checkbox before the corresponding index in Figure 3-12 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 3-12.

3.4.6 PCM Trunk Group

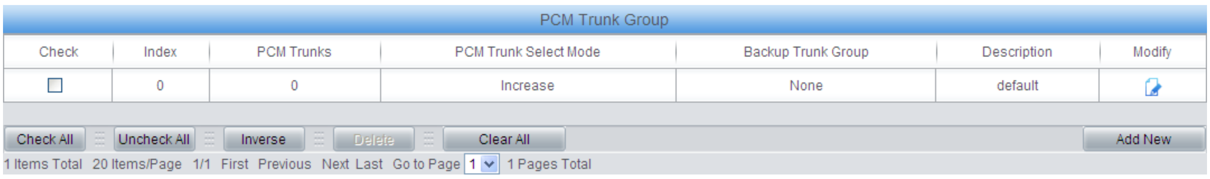


Figure 3-13 PCM Trunk Group Settings

See Figure 3-13 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.

The table below explains the items shown on the interface.

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Index</td><td>The unique index of each PCM trunk group, which is mainly used in the configuration of routing rules and number manipulation rules to correspond to PCM trunk groups.</td></tr>
<tr><td>Description</td><td>More information about each PCM trunk group.</td></tr>
<tr><td>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 3-13.</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 3-13 to modify a PCM trunk group. The configuration items on the PCM trunk group modification interface are the same as those on the ***Add New PCM Trunk Group*** interface.

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

3.4.7 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.

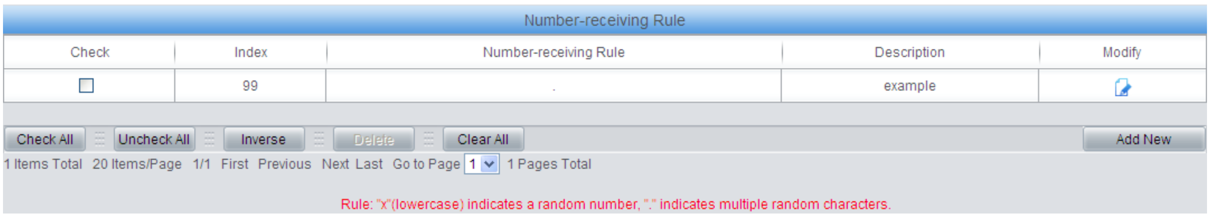


Figure 3-14 Number-Receiving Rule Configuration Interface

See Figure 3-14 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.

The table below explains the items shown on the interface.

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 3-14 to modify the number-receiving rules. The configuration items on the number-receiving rule modification interface are the same as those on the ***Add New Number-receiving Rule*** interface.

To delete a number-receiving rule, 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 number-receiving rules at a time, click the ***Clear All*** button in Figure 3-14.

3.4.8 Reception Timeout

The table below explains the items shown on the number-receiving timeout info interface.

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*** to modify the number-receiving timeout info. The configuration items on the number-receiving timeout info modification interface are the same as those on the ***Number-receiving Timeout Info Interface***.

3.4.9 PSTN Forwarding

The PSTN Forwarding Number Table 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.

The table below explains the items shown on the interface.

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.
Redirection Information	Sets the Redirection Information field in the IAM message. It consists of 2 bytes and only displays in ISUP, with the parameter type of 0x13. The default value is 0x0331 which means Call Forward No Reply. Refer to the stipulations in the ISUP protocol for meanings of each bye.

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

Click ***Modify*** to modify the number table. The configuration items on the PSTN forwarding number table modification interface are the same as those on the ***Add PSTN Forwarding Number Table*** interface. Note that the item ***No.*** cannot be modified.

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

3.5 SS7 Settings

Users can see the SS7 option in the menu only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *SS7-TUP* or *SS7-ISUP* (The SMG2030S, SMG2060S and SMG2120S series don't support SS7.). SS7 Settings includes eight parts: ***SS7***, ***TUP***, ***TUP Number Param***, ***ISUP***, ***Number Param***, ***Original CalleeID Pool***, ***Redirecting Number Pool (Hidden item)*** and ***SS7 Server***.

3.5.1 SS7

On the SS7 settings interface, you can configure the general SS7 parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to Restart for detailed instructions. The table below explains the items shown on the interface.

Item	Description
As Client Only	Sets whether the gateway serves as Client only or not. If it is set to *No* (default), the SS7 server will be disabled.
Master IP	Sets the IP address of the master SS7 server, with the default value of 127.0.0.1, which indicates that there is only one SS7 server available.
Slave IP	Sets the IP address of the slave SS7 server. Only when the item ***Dual Gateway*** is ticked can this item be configured.
Local IP Address	Sets the IP address of the local PC, with the default value of 127.0.0.1.
Dual Gateway	If this feature is enabled, two SS7 servers are used at the same time in the system. The configuration items ***Master IP*** and ***Slave IP*** are respectively used to set the IP addresses of the master and slave servers.

Pass SS7 Message in Shared Memory Mode	Only applicable to the mode of single device. Enabling this feaure will improve the efficiency in SS7 signaling transmission.

3.5.2 TUP

Users can see the TUP settings interface and configure the general TUP parameters only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *SS7-TUP*. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to Restart for detailed instructions. The table below explains the items shown on the interface.

Item	Description
Send GRM Group Message Using All-0 Field	If this configuration item is enabled, when the local driver sends the circuit group message to the remote PBX, this message covers all time slots TS1~31. By default this item is enabled.
Send ST Signal with CallerID in Outgoing Call	If this configuration item is enabled, the calling party number string sent by the gateway contains the ST signal in the outgoing call. By default this item is disabled.
Send ST Signal with CalleeID in Outgoing Call	If this configuration item is enabled, the called party number string sent by the gateway contains the ST signal in the outgoing call. By default this item is disabled.
Setting Spare Address Codes	Sets the corresponding character for each spare address code to establish a rule between the address codes and the mapped ASCII characters. **Note:** The character corresponding to each spare address code can't be any one of '0'~'9'. If there is more than one character, what the spare address code corresponds to is the first character.
Default Caller Parameter	Sets the address indicator in the calling line identification field in the IAI message. The optional values are: Local subscriber number, Spare national number, Valid national number and International number, with the default value of *Valid national number*.
Set Caller Parameter in case of Original CalleeID	Once this feature is enabled, if the IP end carries the original CalleeID in a call from IP to PSTN, you shall set a separate value for the address indicator in the calling line identification field in the IAI message, i.e. **Caller Parameter (with Original CalleeID)**. By default this configuration item is disabled.
Caller Parameter (with Original CalleeID)	This item is valid only when **Set Caller Parameter in case of Original CalleeID** is enabled. It sets the address indicator in the calling line identification field in the IAI message when the IP end carries the original CalleeID in a call from IP to PSTN. The optional values are: Local subscriber number, Spare national number, Valid national number and International number, with the default value of *Valid national number*.

Default Original Callee Parameter	Sets the address indicator in the original called party address field of the IAI message. The optional values are: Local subscriber number, Spare national number, Valid national number and International number, with the default value of *Valid national number*.
Maximum Wait Answer Time (s)	Sets the maximum time to wait for the answer from the called party of an outgoing call. 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.
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≤n≤40, with the default value of *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.

3.5.3 TUP Number Parameter

The TUP Number Parameter Configuration interface is used to set the corresponding parameters for the calling party number in TUP.

A new TUP number parameter can be added by the ***Add New*** button.

The table below explains the items shown on the interface.

Item	Description
Judge 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 party number parameter, which starts from 0.
CallerID/CalleeID Prefix	A string of numbers at the beginning of a calling/called party number.
Parameter	Sets the parameter for a calling party number.
Set Parameter if Original CalleeID Available	Set whether to enable the feature of setting this parameter only if the original CalleeID is available.

After configuration, click ***Save*** to save the above settings into the gateway or click ***Close*** to cancel the settings.Click ***Modify*** to modify the calling party number parameter. The configuration items on the calling party number parameter modification interface are the same as those on the ***Add New Calling Party Number Parameter*** interface.

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

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

3.5.4 ISUP

Users can see the ISUP settings interface and configure the general ISUP parameters only when the configuration item ***Signaling Protocol*** on the PCM settings interface is set to *SS7-ISUP*. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to Restart for detailed instructions. The table below explains the items shown on the interface.

Item	Description
Calling Party's Category	Sets the calling party's category indicator in the IAM message. The optional values are: National operator, Ordinary subscriber, Calling subscriber with priority, Data call, Test call, Payphone/Others and Ordinary calling subscriber, with the default value of *Ordinary subscriber*.
Default Caller Parameter	Sets the calling party number parameter field in the IAM message. The optional values are: Subscriber number, National number, and International number, with the default value of *Subscriber number*.
Default Callee Parameter	Sets the called party number parameter field in the IAM message. The optional values are: Subscriber number, National number, and International number, with the default value of *National number*.
Set Caller/Callee Parameter in case of Original CalleeID	Once this feature is enabled, if the IP end carries the original CalleeID in a call from IP to PSTN, you shall set separate values for the caller and callee parameters in the IAM message, i.e. **Caller Parameter (with Original CalleeID)** and **Callee Parameter (with Original CalleeID)**. By default this configuration item is disabled.
Caller Parameter (with Original CalleeID)	This item is valid only when **Set Caller/Callee Parameter in case of Original CalleeID** is enabled. It sets the calling party number parameter field in the IAM message when the IP end carries the original CalleeID in a call from IP to PSTN. The optional values are: Subscriber number, National number, and International number, with the default value of *Subscriber number*.
Callee Parameter (with Original CalleeID)	This item is valid only when **Set Caller/Callee Parameter in case of Original CalleeID** is enabled. It sets the called party number parameter field in the IAM message when the IP end carries the original CalleeID in a call from IP to PSTN. The optional values are: Subscriber number, National number, and International number, with the default value of *National number*.
Default Original Callee Parameter	Sets the first two bytes of the original called party number in the IAM message, including the nature of address indicator, numbering plan indicator and address presentation restricted indicator, with the default value of 0x1001.
Send Generic Number	Sets the generic number parameter in IAM message, with the default value of *disabled*.
Generic Number Property	Sets the generic number for the IAM message, it is valid only when the feature of Send Generic Number is enabled.
Transmission Medium Requirement	Sets the transmission medium requirement parameter in the IAM message. The optional values are: Speech, 64 kb/s unrestricted, 3.1khz audio, Alternative: peech (service 2)/ 64kbit/s unrestricted (service 1) (Spare), Alternative: 64kbit/s unrestricted (service 1)/ speech (service 2) (Spare), 64kb/s preferred, 2*64kb/s unrestricted, 384 kb/s unrestricted, 1920 kb/s unrestricted and Spare, with the default value of *Speech*.
Add Original CalleeID to 'To'	For calls in the direction of PSTN->IP, the original called number will be written into the To field of the SIP message. By default it is disabled.

Obtain Original CalleeID from	Sets where the original CalleeID is obtained from. The optional values are: Only original CalleeID and Original CalleeID/ Redirecting number, with the default value of *Only original CalleeID/redirecting number*.
Reset Circuit upon Service Start before Entering Idle State	If this feature is enabled, the circuit will send a circuit reset message before entering the idle state after the ISUP service is enabled. By default this feature is enabled.
Reply Multiple 180/183 Messages upon eceiving CPG	Mode 1: Receiving the ACM message will trigger the reply of the 183 message; receiving the first CPG message will trigger the reply of the 180 message while the second CPG message will trigger the reply of the 183 message, and the later CPG will trigger no reply of messages. Mode 2: Receiving the ACM message will trigger the reply of the 183 message; receiving a CPG message before the ANM call will trigger a reply of the 183 message while receiving a CPG message after the ANM call will trigger none. By default this feature is disabled.
Send ST Signal with CallerID in Outgoing Call	If this configuration item is enabled, the calling party number string sent by the gateway will contain the ST signal in the outgoing call. By default this item is disabled.
Send ST Signal with CalleeID in Outgoing Call	If this configuration item is enabled, the called party number string sent by the gateway will contain the ST signal in the outgoing call. By default this item is disabled.
Setting Spare Address Codes	Sets the corresponding character for each spare address code to establish a rule between the address codes and the mapped ASCII characters. **Note:** The character corresponding to each spare address code can't be any one of '0'~'9'. If there is more than one character, what the spare address code corresponds to is the first character.
Send Original Called Number	Sets whether to send the switch of the original called number in ISUP. By default it is enabled.
Send Redirecting Number	Sets whether to send the ISUP redirecting number. It is enabled by default.
Information on First Two Bytes of Redirecting Number	Sets the first two bytes of the redirecting number in the IAM message, including the nature of address indicator, numbering plan indicator and address presentation restricted indicator, with the default value of 0x1001**.**
Redirection Information	Add the redirection information to the IAM message. The parameter type is 0x13. It includes two bytes and has the default value of *0x0331*. **Note:** This configuration item is valid only for call testing but not normal calls. What's more, the value of this configuration item will be overlaid automatically if the configuration item Redirection Information in Redirecting Number Pool changes.
Maximum Wait Answer Time (s)	Sets the maximum time to wait for the answer from the called party of an outgoing call. If the call is not answered within the specified time period, it will be canceled by the channel automatically. The default value is 180, 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≤n≤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.
Forward Call Indicator	Sets the forward call indicator in the IAM message, with the default value of 0x0040.
Backward Call Indicator	Sets the backward call indicator in the ACM and CON messages.
Charge Indicator	Sets the Charge Indicator. 00: No indication, 01: No charge, 10: Charge, 11: Spare
Called Party's Status Indicator	Sets the Called Party's Status Indicator. 00: No indication, 01: Subscriber free, 10: Connect when free, 11: Spare
Called Party's Category Indicator	Sets the Called Party's Category Indicator. 00: No indication, 01: Ordinary subscriber, 10: payphone, 11: Spare
End-to-end Method Indicator	Sets the End-to-end Method Indicator. 00: No end-to-end method available (only link-by-link method available), 01: Pass-along method available, 10: SCCP method available, 11: Pass-along and SCCP methods available
Interworking Indicator	Sets the Interworking Indicator. 0: No interworking encountered, 1: Interworking encountered
End-to-end Information Indicator	Sets the End-to-end Information Indicator. 0: No end-to-end information available, 1: End-to-end information available
ISDN User Part Indicator	Sets the ISDN User Part Indicator. 0: ISDN user part not used all the way, 1: ISDN user part used all the way
Holding Indicator	Sets the Holding Indicator. 0: Holding not requested, 1: Holding requested
ISDN Access Indicator	Sets the ISDN Access Indicator. 0: Terminating access non-ISDN, 1: Terminating access ISDN
Echo Control Device Indicator	Sets the Echo Control Device Indicator. 0: Incoming half-echo control device not included, 1: Incoming half-echo control device included
SCCP Method Indicator	Sets the SCCP Method Indicator. 00: No indication, 01: Connectionless method available, 10: Connection oriented method available, 11: Connectionless and connection oriented methods available.
Nature of Connection Indicator	Sets the nature of connection indicator in the IAM message, with the default value of 0x00.
User Service Information	Sets whether the IAM message contains the user service information. By default this feature is disabled. If this feature is enabled, its value is usually determined by the remote PBX, with the default value of 0x80, 0x90, 0xa3. This default value is applicable to Huawei PBXes.
Optional Forward Call Indicator	Sets whether the IAM message contains the optional forward call indicator. By default this feature is disabled. If this feature is enabled, its value is usually determined by the remote PBX, with the default value of 0x00.

3.5.5 ISUP Number Parameter

The ISUP Number Parameter Configuration interface 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.

The table below explains the items shown on the interface.

Item	Description
Judge 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.
Prefix	A string of numbers at the beginning of a calling/called party number.
Parameter	Sets the parameter for a calling/called party number.
Set Parameter if Original CalleeID Available	Set whether to enable the feature of setting this parameter only if the original CalleeID is available.

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

Click ***Modify*** to modify the calling/called party number parameter. The configuration items on the calling/called party number parameter modification interface are the same as those on the ***Add New Calling/Called Party Number Parameter*** interface.

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.

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.

3.5.6 Original CalleeID Pool

The Original CalleeID Pool interface is used to add the original CalleeID for all outgoing calls or some special calls which contain the specified calling/called prefix.

A new original CalleeID can be added by the ***Add New*** button.

The table below explains the items shown on the interface.

Item	Description
No.	The corresponding number for an added original CalleeID. 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).
Original CalleeID Range	The range of the original CalleeID in the Original CalleeID Pool. It must be filled in with numbers and can not be left empty.
PCM Trunk	Sets the PCM included in the Original CalleeID Pool.

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

Click ***Modify*** to modify the calling/called party number parameter. The configuration items on the original CalleeID modification interface are the same as those on the ***Add New Original CalleeID*** interface. Note that the item ***No.*** cannot be modified.

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

3.5.7 Redirecting Number Pool (Hidden item)

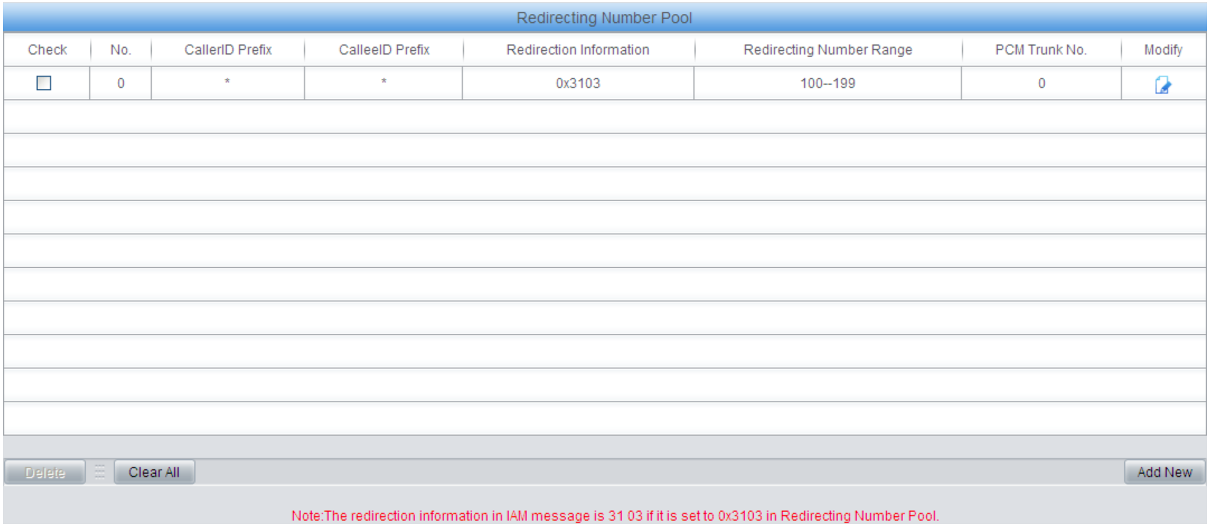


Figure 3-15 Redirecting Number Pool Interface

After you enter http://the IP address of your gateway/gfdhmc.php in the address column of the browser, the redirecting number pool will appear on the web. See Figure 3-15 for the Redirecting Number Pool interface, which is used to set the redirecting number in the setup message for all outgoing calls or some calls which contain a specified calling/called prefix. This feature is only applicable to ISUP calls.

A new redirecting number can be added by the Add New button. See Figure 3-16 for the redirecting number adding interface.

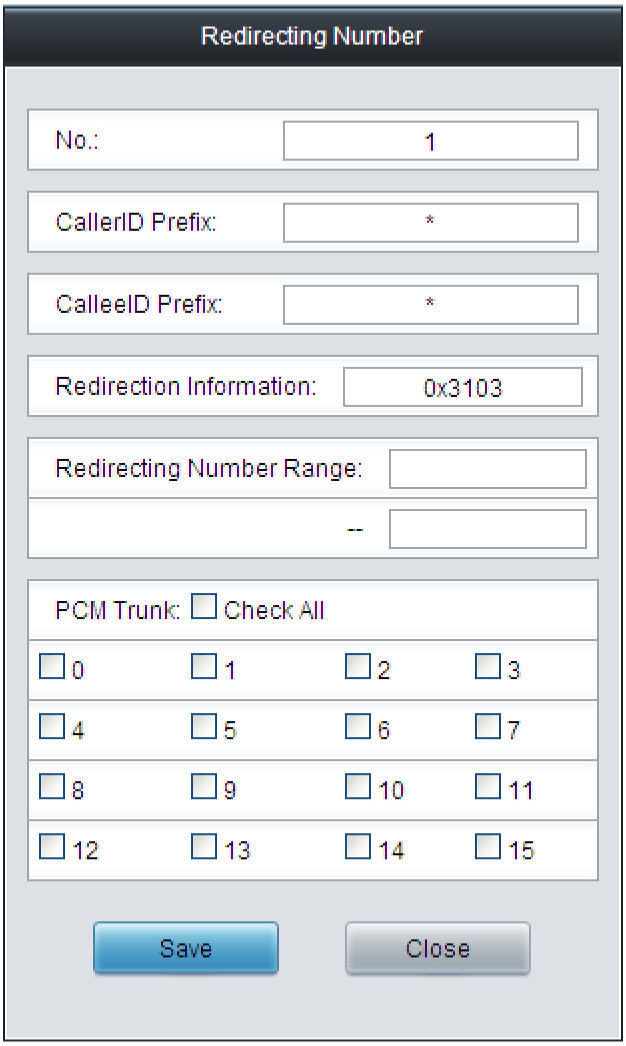


Figure 3-16 Add New Redirecting Number

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).
Redirecting Information	Sets the redirection information field in the IAM message. The parameter type of the redirection information field is 0x13, which contains 2 bytes. By default, it is set to *0x0331*, i.e. call forwarding on no answer. Refer to the ISUP protocol standard for the detailed description of each byte.
Redirecting Number Range	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 No.	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 3-15 to modify the redirecting number parameter. The configuration items on the redirecting number modification interface are the same as those on the ***Add New Redirecting Number*** interface. Note that the item ***No.*** cannot be modified.

To delete a redirecting number parameter, check the checkbox before the corresponding index in Figure 3-15 and click the '***Delete***' button. To clear all redirecting number parameters at a time, click the ***Clear All*** button in Figure 3-15.

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

3.5.8 SS7 Server

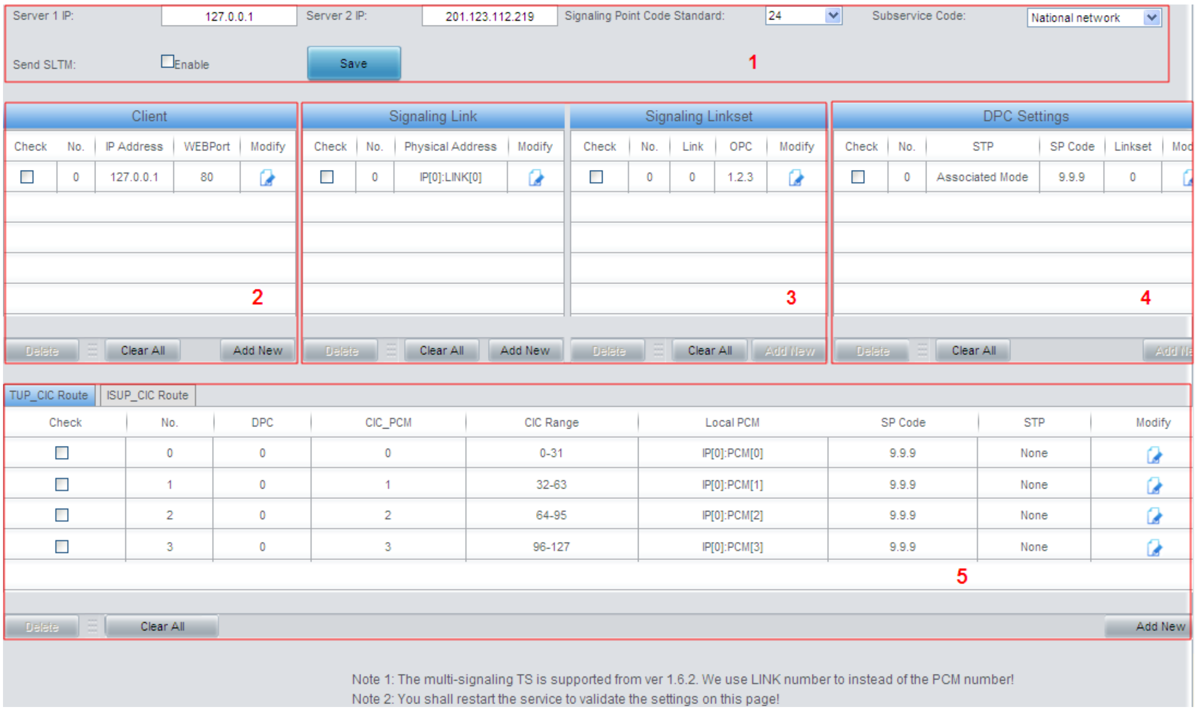


Figure 3-17 SS7 Server Configuration Interface

When the gateway uses the SS7 signaling, it must run the SS7 server first. See Figure 3-17 for the SS7 configuration interface, where you can set the SS7 server configuration file (Ss7server.ini). Follow the instructions below to accomplish the configurations step by step.

Step 1: Set Server IP and Signaling Point Code Standard. See Region 1 in Figure 3-17.

The table below explains these configuration items.

Item	Description
Server 1 IP	Sets the IP address for the master SS7 server. If only one server is used in the system, there is no need to set the configuration item ***Server 2 IP***.
Server 2 IP	Sets the IP address for the slave SS7 server.
Signaling Point Code Standard	The value of this item varies on the PBX model. The optional values are 14 and 24, with the default value of 24. The China SS7 uses 24.
Subservice Code	Sets the SS7 subservice code. The optional values are: *International network*, *Spare international network*, *National network*, *Spare national network*, with the default value of *National network*.

Send SLTM	Sets whether to regularly send the Signaling Link Test Message (SLTM) to the remote PBX. By default it is disabled.

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

Step 2: Configure the client. See Region 2 in Figure 3-17.

A new client can be added by the ***Add New*** button on the bottom right corner of the client list. See Figure 3-18 for the new client adding interface.

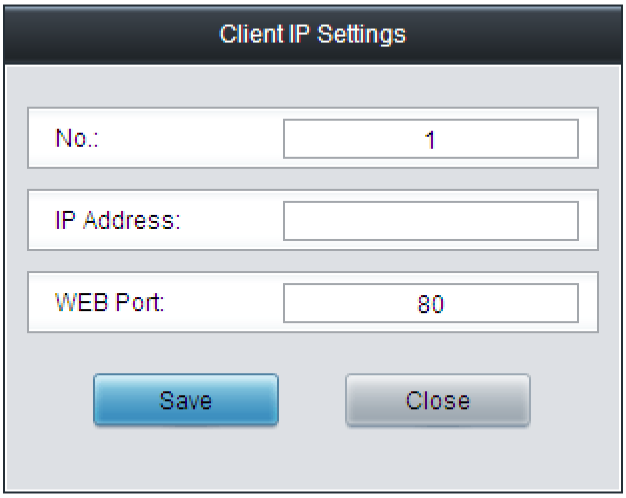


Figure 3-18 Add New Client

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

Item	Description
No.	The unique index of each client, which is mainly used in the configuration of signaling links to correspond to the client, numbered from 0.
IP Address	IP address of the client.
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.

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

To modify a client, click ***Modify*** in the client list. The configuration items on the modification interface are the same as those on the ***Add New Client*** interface.

To delete a client, check the checkbox before the corresponding index and click the ***Delete*** button under the list. To clear all clients at a time, click the ***Clear All*** button. Note: If a client is occupied by a signaling link, it cannot be deleted or cleared unless you delete the signaling link first. You can only delete the clients in turn from back to front.

Step 3: Configure signaling links and linksets. See Region 3 in Figure 3-17.

The link used to transmit signaling messages between two signaling points is called Signaling Link. Each signaling link maps a physical address. A new signaling link can be added by the ***Add New*** button on the bottom right corner of the signaling link list. See Figure 3-19 for the new signaling link adding interface.

Figure 3-19 Add New Signaling Link

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

Item	Description
No.	The unique index of each signaling link, which is mainly used in the configuration of signaling linksets to correspond to the signaling link, numbered from 0.
Client	Client number. This configuration item together with ***PCM*** determines the physical address of the E1 interface of the signaling link. Each physical address maps a signaling link.
LINK	The number of the signaling time slot, which starts from 0.

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

To modify a signaling link, click ***Modify*** in the signaling link list. The configuration items on the modification interface are the same as those on the ***Add New Signaling Link*** interface.

To delete a signaling link, check the checkbox before the corresponding index and click the ***Delete*** button under the list. To clear all signaling links at a time, click the ***Clear All*** button. Note: If a signaling link is occupied by a signaling linkset, it cannot be deleted or cleared unless you delete the signaling linkset first. You can only delete the signaling links in turn from back to front.

A group of signaling links used to connect two signaling points directly constitute a signaling linkset. A new signaling linkset can be added by the ***Add New*** button on the bottom right corner of the signaling linkset list. See Figure 3-20 for the new signaling linkset adding interface.

Figure 3-20 Add New Signaling Linkset

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

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>No.</td><td>The unique index of each signaling linkset, which is mainly used in the configuration of DPC to correspond to the signaling linkset, numbered from 0.</td></tr>
<tr><td>Link</td><td>The signaling links in the linkset. If the checkbox before a link is grey, it indicates that the link has been occupied.</td></tr>
<tr><td>OPC</td><td>Originating Point Code for the signaling server which is usually allocated by the central office,. See the table below for the format and the value range:
<table>
<tr><th></th><th>14 bit</th><th>24 bit</th></tr>
<tr><td>Decimal (a.b.c)</td><td>a, c: 0~7, b: 0~255</td><td>a, b, c: 0~255</td></tr>
<tr><td>Hexadecimal (abc)</td><td>a, c: 3-digit hexadecimal number, b: 8-digit hexadecimal number</td><td>a, b, c: hexadecimal number inbetween 00~ff</td></tr>
</table></td></tr>
</table>

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

To modify a signaling linkset, click ***Modify*** in the signaling linkset list. The configuration items on the modification interface are the same as those on the ***Add New Signaling Linkset*** interface.

To delete a signaling linkset, check the checkbox before the corresponding index and click the ***Delete*** button under the list. To clear all signaling linkset at a time, click the ***Clear All*** button. Note: If a signaling linkset is occupied by a DPC, it cannot be deleted or cleared unless you delete the DPC first. You can only delete the signaling linksets in turn from back to front.

Step 4: Configure DPC. See Region 4 in Figure 3-17.

The signaling point that receives messages is called Destination Point Code (DPC). A new DPC can be added by the ***Add New*** button on the bottom right corner of the DPC list. See Figure 3-21 for the new DPC adding interface.

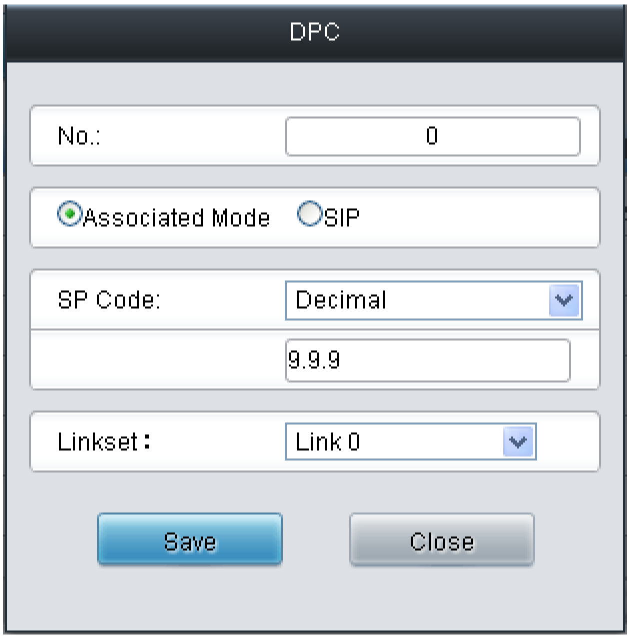
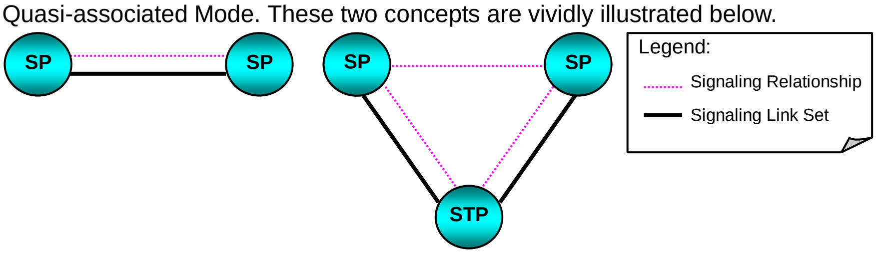


Figure 3-21 Add New DPC

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

Item	Description
No.	The unique index of each DPC, which is mainly used in the configuration of TUP_CIC Route or ISUP_CIC Route to correspond to the DPC, numbered from 0.
Associated Mode/ SIP	Sets the way to transmit signaling messages between two signaling points, including *Associated Mode* and *Quasi-associated Mode*. Directly connecting the signaling links between two signaling points to transmit the inbetween signaling messages is called Associated Mode. Connecting two or more than two signaling links serially via one or more than one signaling transport points to transmit signaling messages, provided the path of signaling messages through the signaling network is predetermined and fixed within a certain period of time, is called Quasi-associated Mode. These two concepts are vividly illustrated below.  (a) Associated Mode (b) Quasi-associated Mode In Associated mode, the DPC[x] configuration will be marked as a non-signaling transport point. To set the Quasi-associated mode, select *SIP* on the DPC settings interface and DPC[x] will be marked as the signaling transport point. **Note:** The option *SIP* on the DPC setting interface represents the Quasi-associated mode.
SP Code	Signaling point code of the DPC, usually allocated by the central office.
STP	Sets the first STP (signaling transport point) the signaling message reaches during the transmission under the quasi-associated mode. Only when you select the quasi-associated mode can this item be seen and configured.

Linkset	The linkset which is used to transmit signaling messages. For the associated mode, this item sets the signaling linksets between the OPC and the DPC. For the quasi-associated mode, this item sets the signaling linksets between the OPC and the first STP (signaling transport point).

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

To modify a DPC, click ***Modify*** in the DPC list. The configuration items on the modification interface are the same as those on the ***Add New DPC*** interface.

To delete a DPC, check the checkbox before the corresponding index and click the ***Delete*** button under the list. To clear all DPCs at a time, click the ***Clear All*** button. Note: If a DPC is occupied by a CIC routing rule, it cannot be deleted or cleared unless you delete the routing rule first. You can only delete the DPCs in turn from back to front.

Step 5: Configure UP_DPC.

A new UP_DPC can be added by the ***Add New*** button on the bottom right corner of the UP_DPC Settings region. See Figure 3-22 for the UP_DPC Settings interface.

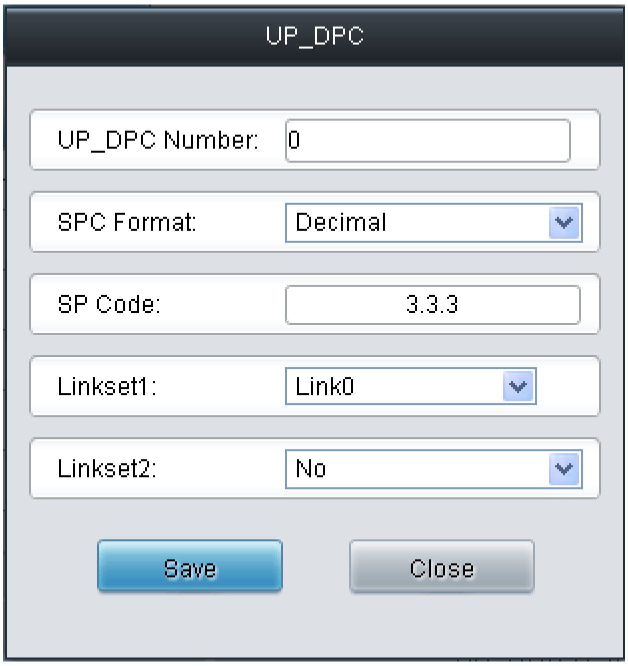


Figure 3-22 UP_DPC Settings Interface

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

Item	Description
UP_DPC Number	The number starts from 0.
SPC Format	You can choose *Decimal* or *Hexadecimal*.
SP Code	Signaling point code encoding (decimal). x.y.z: x is the main signal area code, y is the sub-signal area code, and z is the signal point code, which are assigned by the telecommunication office.
Linkset1	The information of the link in the link group, selected according to the number.
Linkset2	Same as *Linkset1*. You can choose or not.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. To modify a UP_DPC, click ***Modify*** in the UP_DPC list. The configuration items on the modification interface are the same as those on the ***Add New UP_DPC*** interface.

Note:

1. If there are both *Associated* and *SIP* modes available in the DPC settings, the corresponding Associated mode must be configured in the UP_DPC settings.

2. If the UP_DPC setting is configured, the configuration of the corresponding DPC in the CIC routing list is subject to the number set by UP_DPC.

Step 6: Configure TUP_CIC or ISUP_CIC Route. See Region 6 in Figure 3-17.

A new TUP_CIC routing rule can be added by the ***Add New*** button on the bottom right corner of the TUP_CIC routing rule list. See Figure 3-23 for the new TUP_CIC routing rule adding interface.

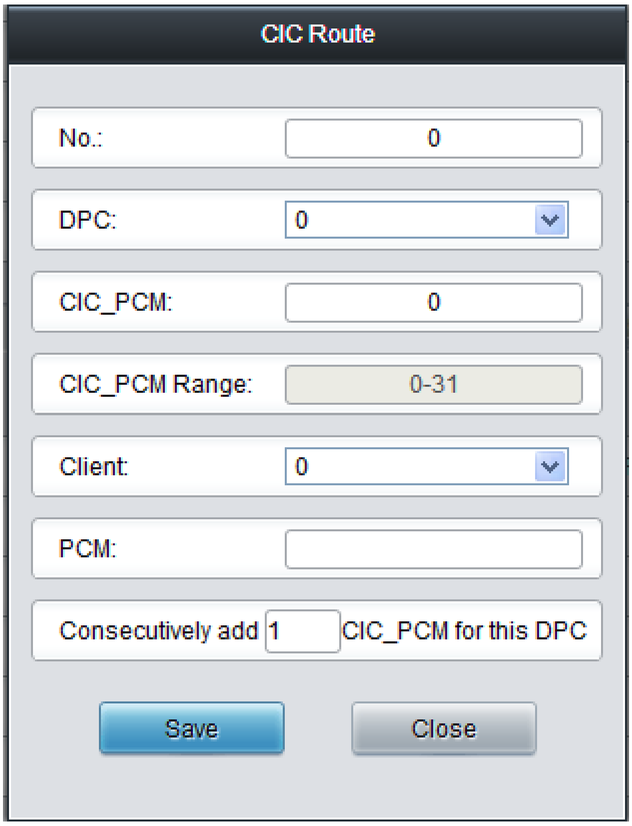


Figure 3-23 Add New TUP_CIC Routing Rule

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

Item	Description
No.	The unique index of each CIC routing rule, which is numbered from 0.
DPC	DPC used in the routing rule.
CIC_PCM	PCM number in the CIC field and the value is obtained by dividing the initial CIC number from the central office by 32.
CIC_PCM Range	Range of the PCM time slots corresponding to CIC.
Client	Client number. This configuration item together with ***PCM*** determines the local PCM in the CIC routing rule.
PCM	PCM number on the client.
Consecutively add _CIC_PCM for this DPC	Consecutively adds one or more CIC_PCM routes for a DPC.

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

To modify a routing rule, click ***Modify*** in the TUP_CIC routing rule list. The configuration items on the modification interface are the same as those on the ***Add New TUP_CIC Routing Rule*** interface.

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

For the ISUP_CIC route settings, click the ISUP_CIC Route tab in Region 5 in Figure 3-17. See Figure 3-24 for the ISUP_CIC route settings interface. The configuration items and operations on this interface are absolutely the same as those in the TUP_CIC route settings interface. Note: Besides the default setting, the CIC Range for ISUP_CIC route can also be user-defined.

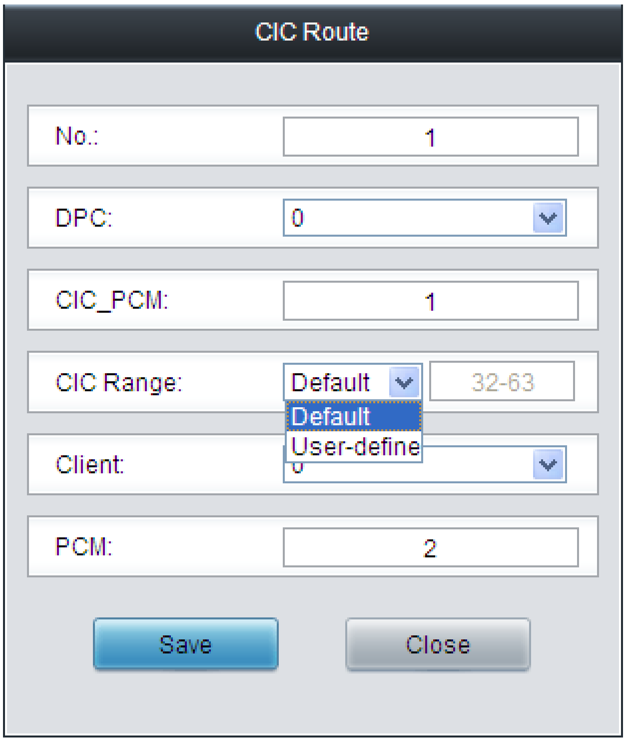


Figure 3-24 ISUP_CIC Route Settings Interface

After completing the configurations on ***SS7 Server Configuration Interface*** (Figure 3-17), you shall restart the service to validate them. Refer to Restart for detailed instructions.

3.6 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*.

3.6.1 ISDN

On the ISDN settings interface, 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 Restart for detailed instructions. The table below explains the items on the interface.

Item	Description

TEI	Terminal Equipment Identifier, which is used to identify the service access point in the point-to-point data link connection. The default value is 0 which cannot be modified so far. 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.
Decode ISDN Debugging Message before Outputting	If this item is checked, the system will decode the ISDN debugging message before outputting it.
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≤n≤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*.
Collect Call	Only when the SETUP message of a PSTN incoming call brings the field *reverse charging indication* will this item work. Three options are available: Default, Reject and Notify IP-PBX. If the option *Notify IP-PBX* is selected, the INVITE message of a SIP outgoing call will bring the *x-BRCollectCall* field.
Send the 'Called Party Number Complete' Parameter	Sets whether to include or not the 'Called Number Complete' parameter in the SETUP message during an outgoing call.
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 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.
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).

Allow the Preferential Channel Selection	Sets whether to select the preferential channel. By default it is disabled.
Send ISDN Redirecting Number	Sets whether to send the ISDN redirecting number. By default it is enabled.

3.6.2 Number Parameter

Number Parameter for ISDN is almost the same as that for SS7; only the calling/called party number changes from SS7 to ISDN; “set parameter if original CalleeID available” changes to “set parameter if redirecting number available” in ISDN. The configuration items on Number Parameter for ISDN interface are the same as those on the Number Parameter for SS7 interface.

3.6.3 Redirecting Number (Hidden item)

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. It is almost the same as Original CalleeID Pool for SS7; only the calling/called party number changes from SS7 to ISDN. The configuration items on the Redirecting Number Pool for ISDN interface are the same as those on the Original CalleeID Pool for SS7 interface.

3.7 SS1 Settings

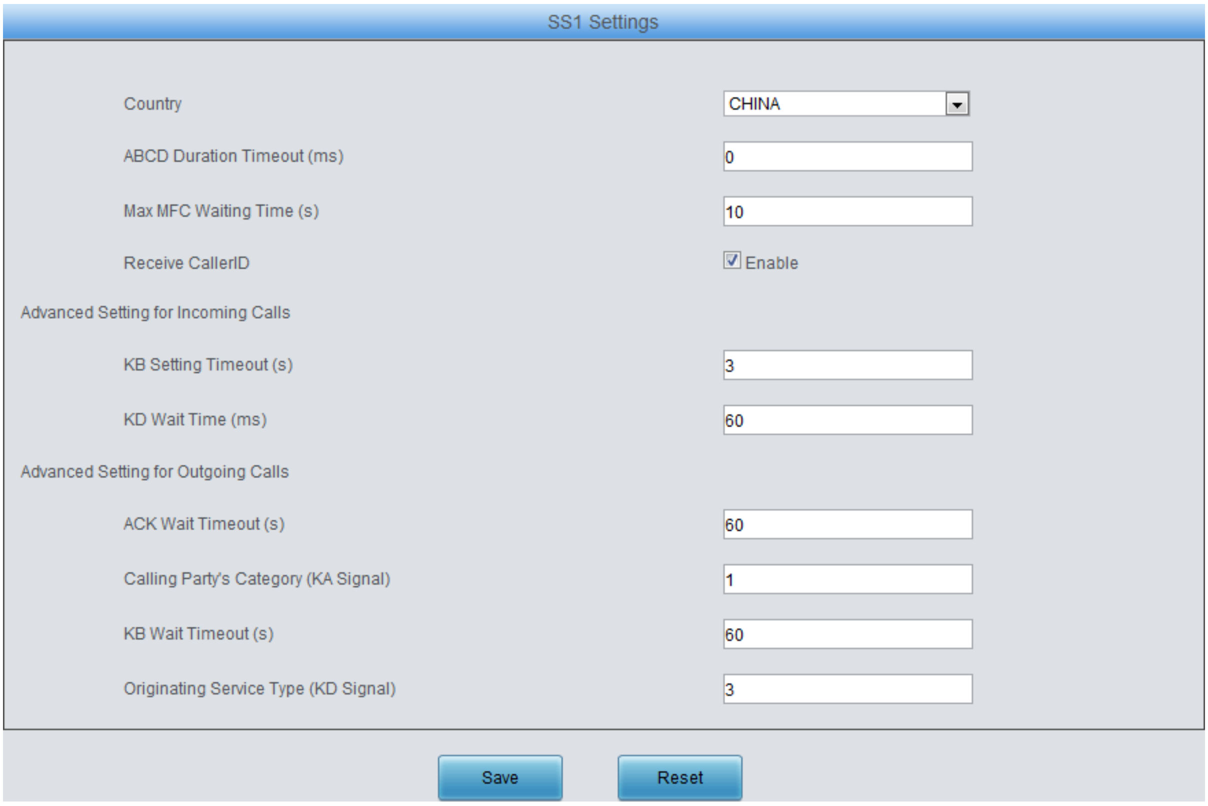


Figure 3-25 SS1 Settings Interface

See Figure 3-25 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 Restart for detailed instructions. The table below explains the items shown in Figure 3-25.

Item	Description
SS1 HotLine	After this item is enabled, if the gateway receives CAS=0xd, a SIP call goes out and the calling number is the same as the channel number at the digital side; when this call hangs up, the gateway will receive 0x5 and the SIP side will send the BYE message. If an IP call comes in and the gateway receives the INVITE message, the corresponding PCM will send CAS=0xd; when the gateway receives the BYE message, the corresponding PCM will send CAS=0x5 to end the call.
Country	Sets the country to use SS1, with the default value of *CHINA*.
KB Signal Value	The KB value sent by the SS1 channel to the remote PBX in answering an incoming call automatically.
Backward A Signal (tonesrepeatrequest)	Used by the call incoming end to request the call outgoing end to send the backward A signal again.
Backward A Signal (tonesgroupA)	Used by the driver to send the request of backward A signal in MFC (Multiple Frequency Control)
Backward Signal (tonesgroupB)	Used to end the MFC indication.
Backward Signal (tonesanswer)	Used to indicate the call receiving.
Forward Signal (tonesendofinfo)	Used to indicate some signal to end or to be unavailable.
R2 Signal (tonesanswerA)	Sets the parameters of R2 signaling.
C/D Value	Sets the CD value of the ABCD signaling code sent from the local end to the remote PBX.
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)*.

3.8 Fax Settings

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

3.8.1 Fax

On the fax configuration interface, users can configure the general fax parameters. After configuration, click ***Save*** to save your settings into the gateway or click ***Reset*** to restore the configurations. If a dialog box pops up after you save your settings asking you to restart the service, do it immediately to apply the changes. Refer to Restart for detailed instructions. The table below explains the configuration items on the interface.

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

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

Item	Description

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

3.9 Route Settings

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

3.9.1 Routing Parameters

On the routing parameters configuration 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.

3.9.2 IP to PSTN

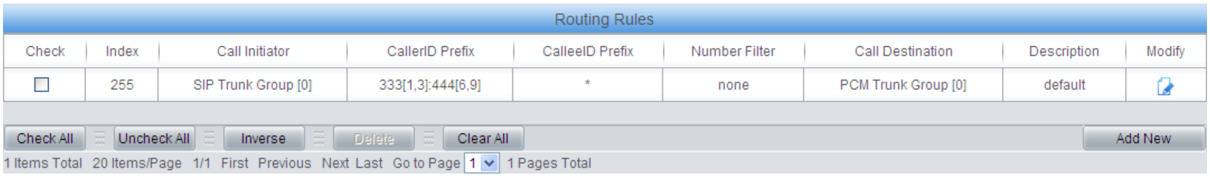


Figure 3-26 IP→PSTN Routing Rule Configuration Interface

See Figure 3-26 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.

The table below explains the items shown on the interface.

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 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 3-26 to modify a routing rule. The configuration items on the IP→PSTN routing rule modification interface are the same as those on the ***Add New Routing Rule (IP→PSTN)*** interface. Note that the item ***Index*** cannot be modified.

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-26 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 3-26.

3.9.3 PSTN to IP

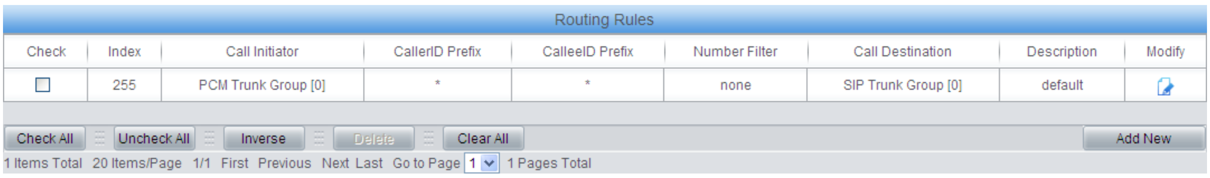


Figure 3-27 PSTN→IP Routing Rule Configuration Interface

See Figure 3-27 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.

The table below explains the items shown on the interface.

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 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 3-27 to modify a routing rule. The configuration items on the PSTN→IP routing rule modification interface are the same as those on the ***Add New Routing Rule (PSTN→IP)*** interface. Note that the item ***Index*** cannot be modified.

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-27 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 3-27.

3.9.4 IP to IP

IP->IP routing is supported only if the SBC device feature has been authorized.

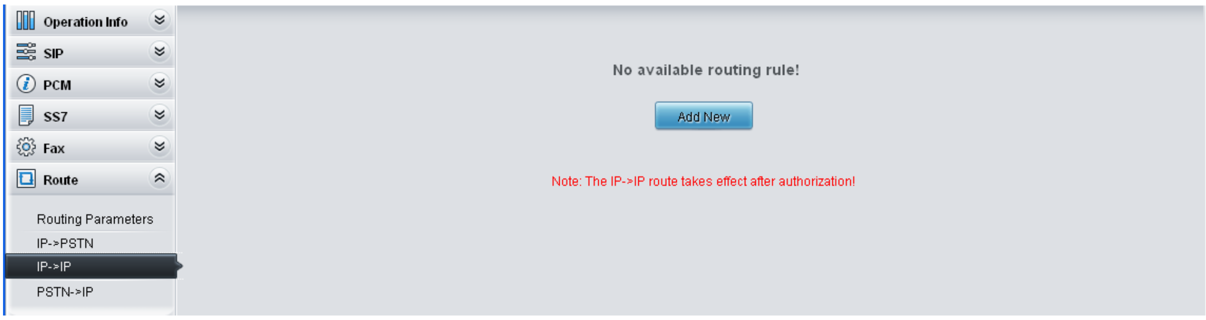


Figure 3-28 IP→IP Routing Rule Configuration Interface

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 3-29 for the IP→IP Routing Rule Adding interface.

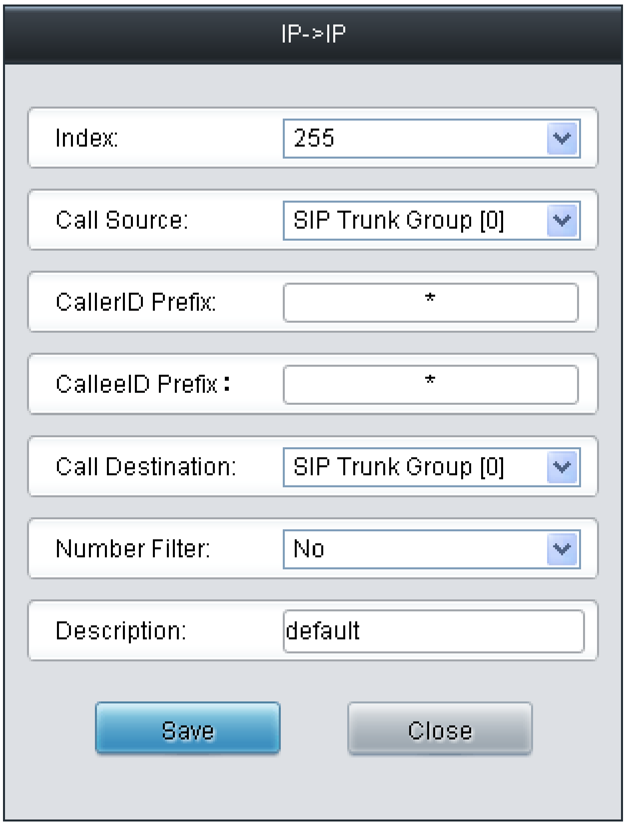


Figure 3-29 IP→IP Routing Rule Adding Interface

The table below explains the items shown on the interface.

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 Source	SIP trunk group from which the call is initiated. This item can be set to a specific SIP trunk group or SIP Trunk Group [ANY] to indicate 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 "*" to indicate 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 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. See the figure below for the IP->IP Routing Rule list.

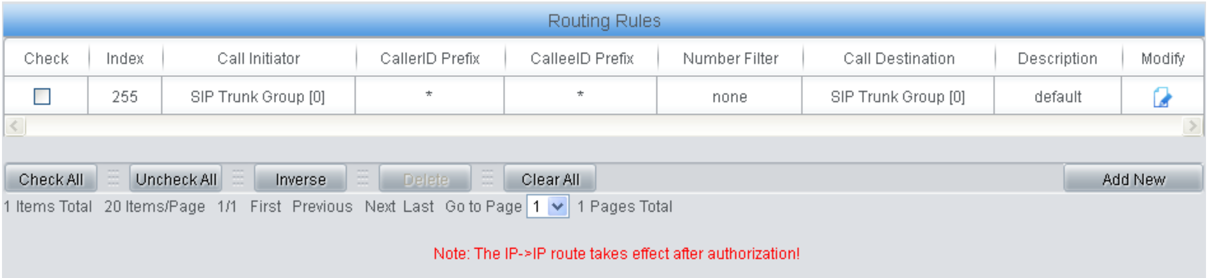


Figure 3-30 IP->IP Routing Rule List

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

3.10 Number Filter

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

3.10.1 Whitelist

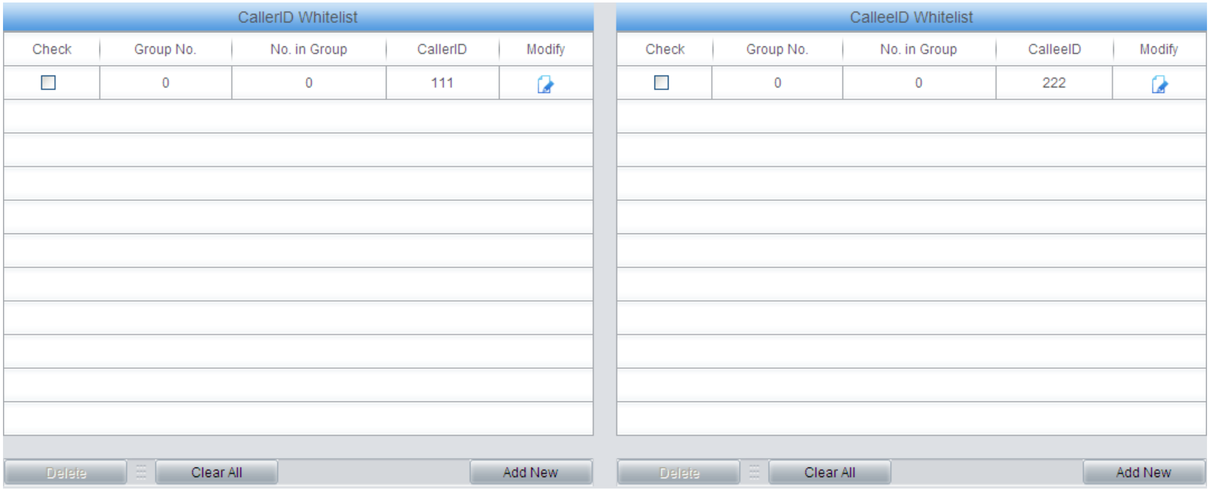


Figure 3-31 Whitelist Setting Interface

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

A new CallerID/CalleeID whitelist can be added by the ***Add New*** button.

The table below explains the items shown on the interface.

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

<table>
<tr><td rowspan="1">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 3-31 to modify the CallerID or CalleeID whitelist. The configuration items on the CallerIDs/CalleeIDs on the Whitelist Modification interface are the same as those on the ***Add New CallerIDs/CalleeIDs in Whitelist*** interface. The item *Group No.* cannot be modified.

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

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

Note: If a CallerID or CalleeID set in the whitelist is the same as one in the blacklist, it will go invalid. That is, the blacklist has a higher priority than the whitelist. The total amount of numbers in both whitelist and blacklist cannot exceed 200000.

3.10.2 Blacklist

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

3.10.3 Number Pool

On the Number Pool Setting interface, a new number pool can be added by the ***Add New*** button on the bottom right corner of the list.

The table below explains the items shown on the interface.

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

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

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

Click ***Modify*** to modify the number pool. The configuration items on the number pool modification interface are the same as those on the ***Add New Number Pool*** interface.

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

3.10.4 Filtering Rule

On the Filtering Rule Setting Interface, a new filtering rule can be added by the ***Add New*** button on the bottom right corner of the list.

The table below explains the items shown on the interface.

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

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

Click ***Modify*** to modify the filtering rule. The configuration items on the filtering rule modification interface are the same as those on the ***Add New Filtering Rule*** interface.

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

3.11 Number Manipulation

Number Manipulation includes eight parts: **IP Call In CallerID**, **IP Call In CalleeID**, **IP Call In Original CalleeID**, **PSTN Call In CallerID**, **PSTN Call In CalleeID**, **PSTN Call In Original CalleeID**, **CallerID Pool** and **CallerID Reserve Pool**.

3.11.1 IP Call In CallerID

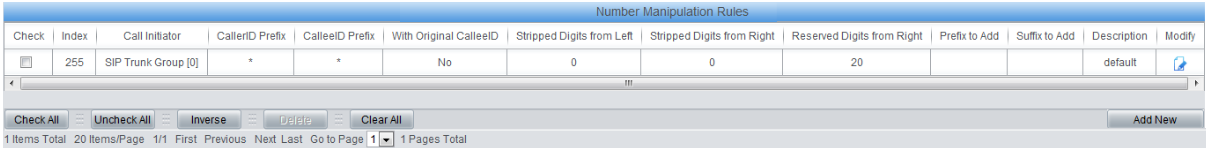


Figure 3-32 IP Call In CallerID Manipulation Interface

See Figure 3-32 for the IP Call In 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.

The table below explains the items shown on the interface.

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

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

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

Click ***Modify*** in Figure 3-32 to modify a number manipulation rule. The configuration items on the

IP Call In CallerID manipulation rule modification interface are the same as those on the ***Add IP Call In CallerID Manipulation Rule*** interface. Note that the item ***Index*** cannot be modified.

To delete a number manipulation rule, check the checkbox before the corresponding index in Figure 3-32 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 3-32.

3.11.2 IP Call In CalleeID

The number manipulation process for IP Call In CalleeID is almost the same as that for IP Call In CallerID; only the number to be manipulated changes from CallerID to CalleeID. The configuration items on this interface are the same as those on ***IP Call In CallerID Manipulation Interface*** (Figure 3-32).

3.11.3 IP Call In Original CalleeID

The number manipulation process for IP Call In Original CalleeID is almost the same as that for IP Call In CallerID; only the number to be manipulated changes from CallerID to Original CalleeID. The configuration items on the IP Call In Original CalleeID manipulation interface are the same as those on ***IP Call In CallerID Manipulation Interface*** (Figure 3-32).

3.11.4 PSTN Call In CallerID

On the PSTN Call In 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.

The table below explains the items shown on the interface.

Item	Description
Index	The unique index of each number manipulation rule, which denotes its priority. A number manipulation rule with a smaller index value has a higher priority. If a call matches several number manipulation rules, it will be processed according to the one with the highest priority.
Call Initiator	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*** to modify a number manipulation rule. The configuration items on the PSTN Call In CallerID manipulation rule modification interface are the same as those on the ***Add PSTN Call In CallerID Manipulation Rule*** interface. Note that the item ***Index*** cannot be modified.

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

3.11.5 PSTN Call In CalleeID

The number manipulation process for PSTN Call In CalleeID is almost the same as that for PSTN Call In CallerID; only the number to be manipulated changes from CallerID to CalleeID. The configuration items on the PSTN Call In CalleeID manipulation interface are the same as those on ***PSTN Call In CallerID Manipulation Interface***.

3.11.6 PSTN Call In Original CalleeID

The number manipulation process for PSTN Call In Original CalleeID is almost the same as that for PSTN Call In CallerID; only the number to be manipulated changes from CallerID to Original CalleeID. The configuration items on the PSTN Call In Original CalleeID manipulation interface are the same as those on ***PSTN Call In CallerID Manipulation Interface***.

3.11.7 CallerID Pool

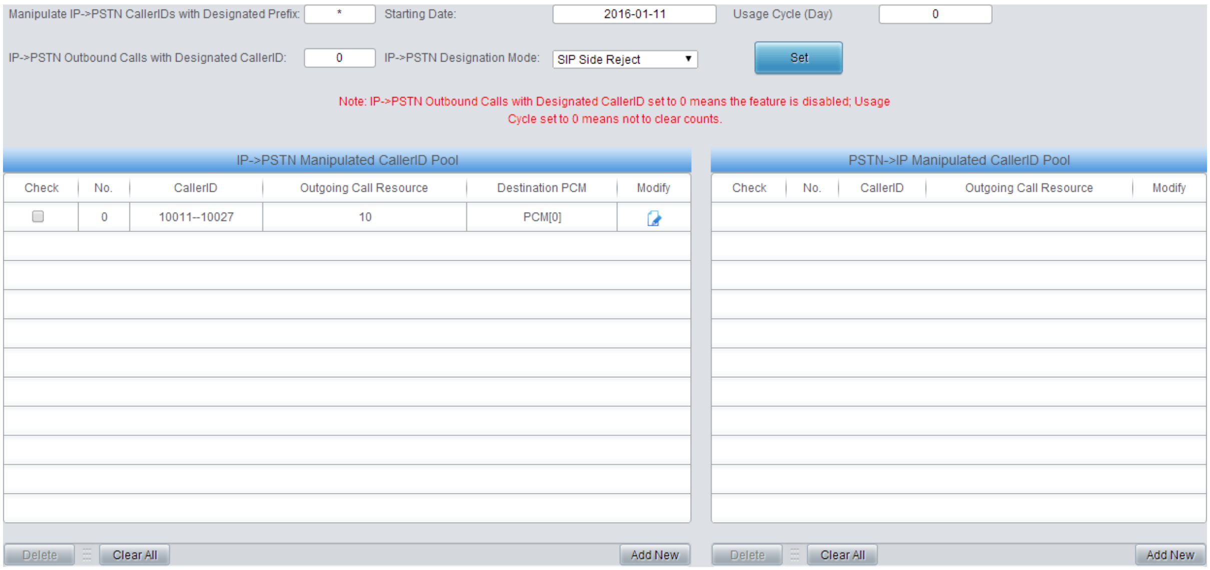


Figure 3-33 CallerID Pool Interface

See Figure 3-33 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.

The table below explains the items shown on the interface.

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.
Destination PCM	You can select PCM or PCM group.
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.
Source PCM	Only the calls from this PCM are allowed to do the CallerID 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 3-33 to modify the CallerID information. The configuration items on the CallerID modification interface are the same as those on the ***Add New CallerID*** interface. The item *No.* cannot be modified.

To delete a CallerID in the pool, check the checkbox before the corresponding index in Figure 3-33 and click the '***Delete***' button. To clear all CallerIDs in the pool at a time, click the ***Clear All*** button in Figure 3-33.

3.11.8 CallerID Reserve Pool

All the CallerIDs in this reserve pool will not be manipulated.

3.12 DHCP

See Figure 3-34 for the DHCP settings. The DHCP server controls a range of IP addresses. When the client logs in to the server, it can automatically obtain the IP address and subnet mask assigned by the server. It is mainly used for centralized management and allocation of IP addresses, so that hosts in the network environment can obtain such information as IP addresses, gateway addresses and DNS server addresses dynamically, which can improve the usage rate of addresses. The 3016 and 2120 Series gateways provide a DHCP setting interface.

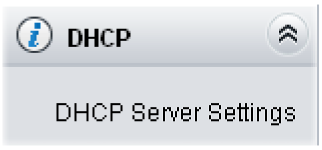


Figure 3-34 DHCP Settings

3.12.1 DHCP Server Settings

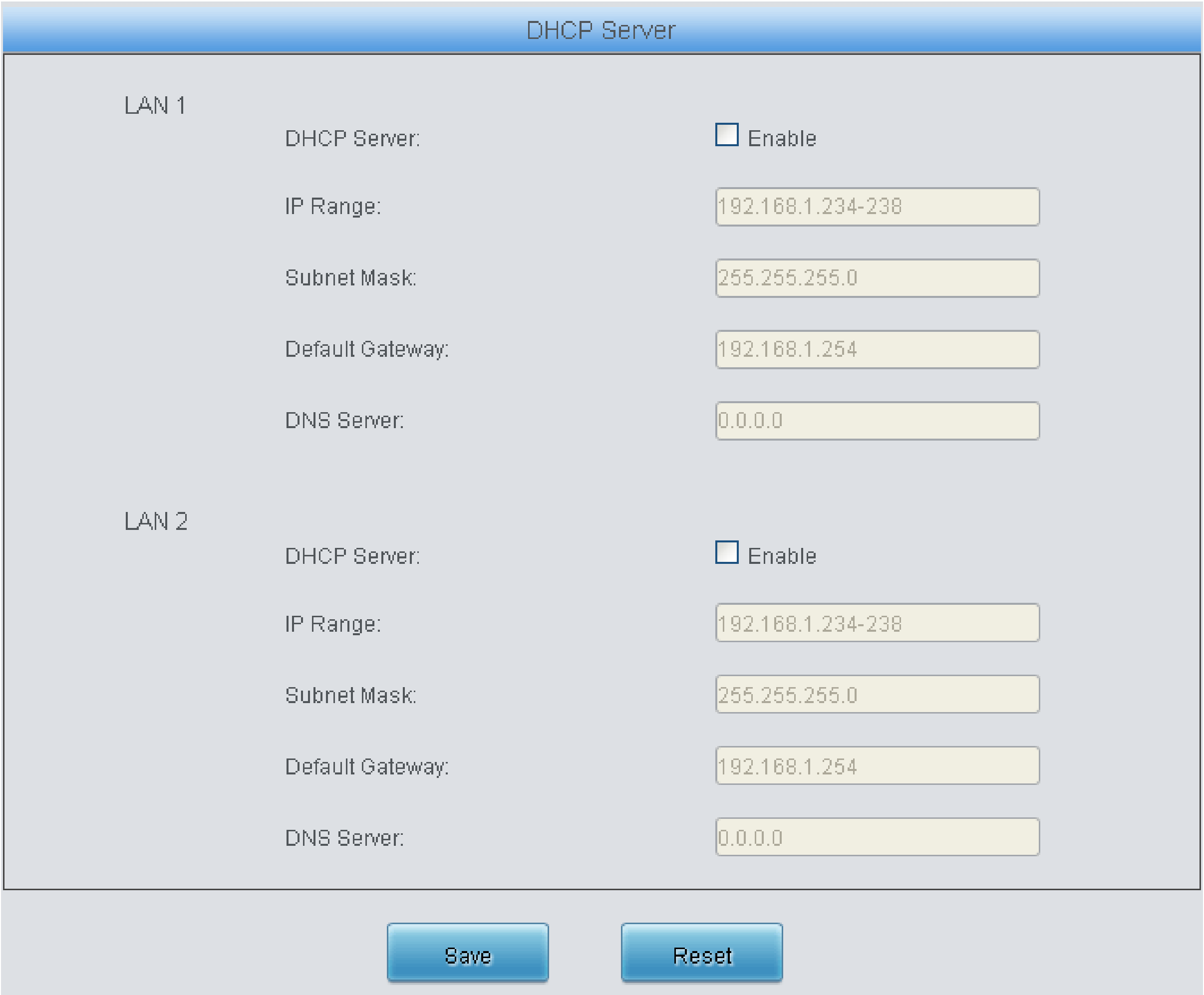


Figure 3-35 DHCP Server Settings Interface

The table below explains the items shown on the interface.

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

The DHCP server is disabled by default. According to the settings of Network Port 1 and Network Port 2, select Enable and fill in the correct IP address. After configuration, click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations.

3.13 System Tools

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

3.13.1 Network

The network settings interface is used to configure parameters about network. A gateway has two LANs, each of which can be configured with independent IP address (IPv4, IPv6), subnet mask and default gateway. It supports the 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.

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

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

3.13.2 Authorization

On the Authorization Management interface, you can import a trial or formal authorization just by uploading the authorization file which is provided by Synway and cannot be modified.

3.13.3 Management

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

Item	Description
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.
Access Setting	Sets the IP addresses which can access the gateway via WEB. By default, all IPs are allowed. You can set an IP whitelist to allow all the IPs within it to access the gateway freely. Also you can set an IP blacklist to forbid all the IPs within it to access the gateway.
Time to Log Out	The gateway will log out automatically if it is not operated during a time longer than the value of this item, calculated by s, with the default value of 1800.
SSH	Sets whether to enable the gateway to be accessed via SSH, with the default value of *No*.
SSH Port	The port which is used to access the gateway via SSH.
Remote Data Capture	After this feature is enabled, you can obtain the gateway data via a remote capture tool. The default value is *No*.
Capture RTP	Sets whether to capture RTP. Once this feature is enabled, the RTP package will also be captured by the selected network.
FTP	Sets whether to enable the FTP server, with the default value of *Yes*.
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 Failed Call Record	Once this feature is enabled, the gateway will send the CDR for both successful and unsuccessful calls; otherwise, it will only send the CDR data for successful calls.
Add Hangup Side	Add hangup information to CDR.
Monitor Self-adaption	Enable the NAT stun between the gateway and the monitor tool. By default, it is disabled.
Send Number Classification Data	Sets whether to send the classification data. It is disabled by default.
Server IP	Sets the server IP to receive the classification data.
Server Port	Sets the server port to receive the classification data.
Enable Call Control Server	The calls in both directions of IP->PSTN and PSTN->IP send such information as UUID, gateway IP address, CallerID and CalleeID to the customer's service system by HTTP POST before routing. Then the customer's service system will decide whether to allow the routing or reject the call after querying the database.
Server URL	Sets the server URL to receive the call information.
Encrypt Character String	The encryption key in clear text, used to verify the CallerID and CalleeID
Keep Routing in Server Error	Sets whether to keep routing if server errors occur.
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.

3.13.4 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.

The table below explains the items shown on the interface.

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

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

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

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

3.13.5 Access Control

On 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. For easy viewing, the interface provides a display of iptables information. Click ***Add New*** to add a new piece of command.

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*** to modify a command. The configuration items on the Access Control Command Modification interface are the same as those on the ***Add Access Control Command*** interface. Note that the item ***Index*** cannot be modified.

To delete an Access Control Command, check the checkbox before the corresponding index 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.

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.

3.13.6 Firewall

By default, there is no firewall information available on the gateway, click ***Add New*** to add it manually.

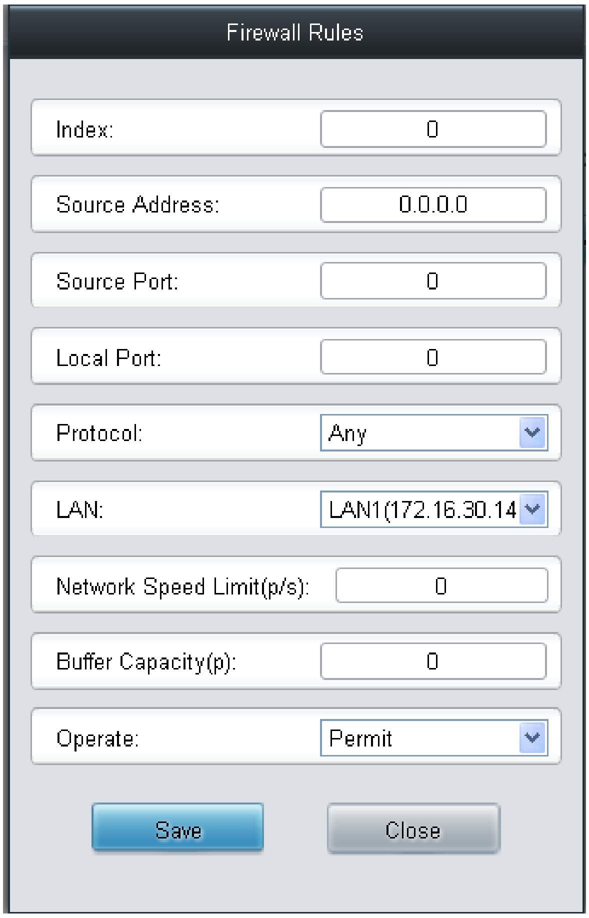


Figure 3-36 Firewall Rules Adding Interface

See below for the configuration items on the interface.

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

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

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

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

Note: 1. Only after selecting a firewall rule and clicking Apply, the firewall rule will take effect.

2. An IP that is determined to be abnormal by DDOS or IDS, will be added to the temporary blacklist, even if the firewall is set to allow access.

3.13.7 IDS Settings

IDS (Intrusion Detection Systems) is an intrusion detection system. According to certain security policies, the network and system running status are monitored through software and hardware, and various attack attempts, attack behaviors or attack results are discovered as much as possible to ensure the confidentiality, integrity and availability of network system resources. IDS is used to detect whether the incoming SIP message complies with the protocol specification. For a SIP message that does not conform to the specification, the gateway will add its source IP address to the blacklist. The IDS settings interface is shown in Figure 3-37.

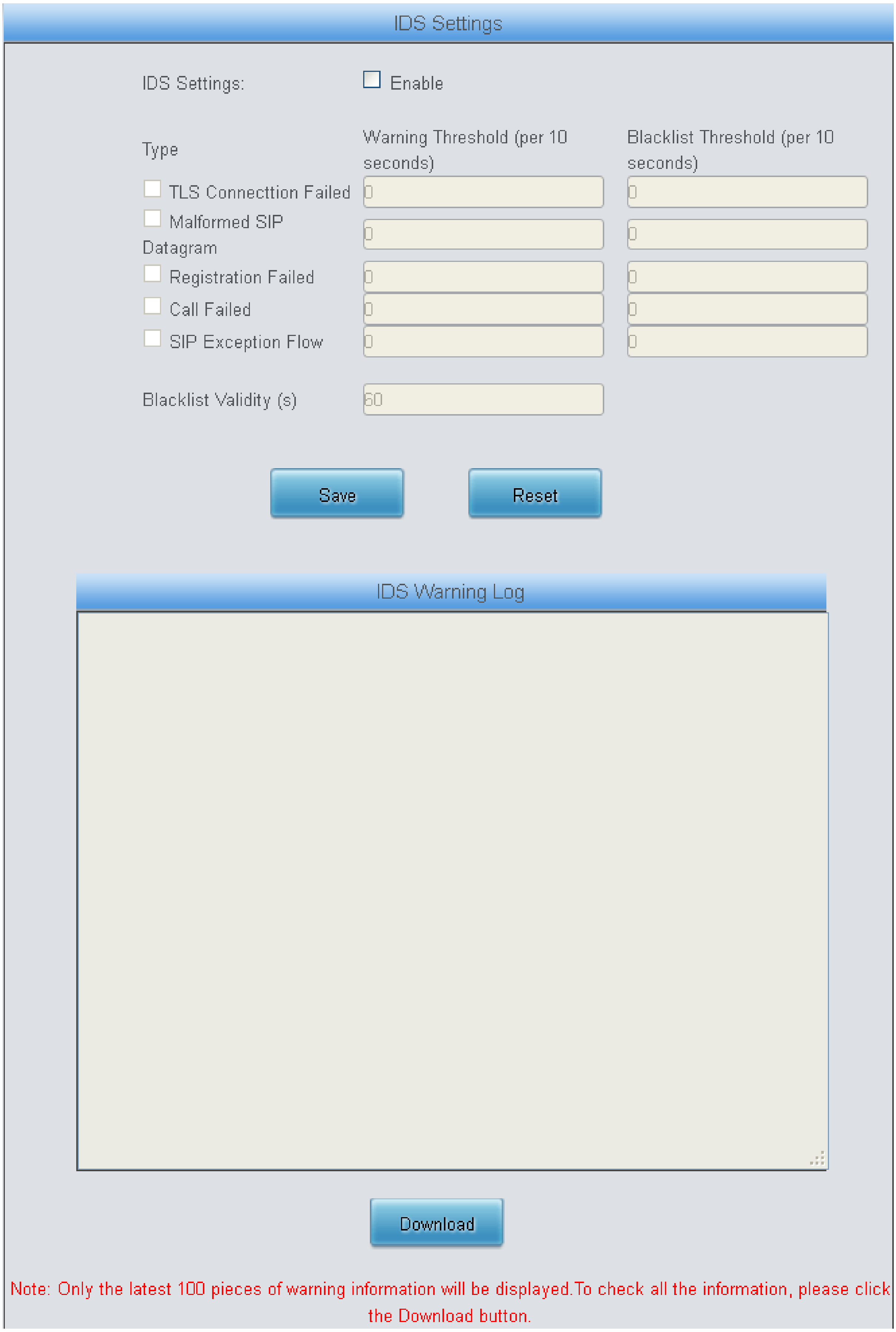


Figure 3-37 IDS Settings Interface

IDS Settings is disabled by default. Check Enable to activate the IDS configuration. Five types are selectable, including *TLS Connection Failed*, *Malformed SIP Datagram*, *Registration Failed*, *Call Failed* and *SIP Exception Flow*. Each type can be configured with Warning Threshold and Blacklist Threshold. The threshold is in the range of 1 to 2048 and the warning threshold should be less than the blacklist threshold. The blacklist validity period can be configured, during which the blacklist is valid. If it is exceeded, the blacklist will be removed immediately.

The table below explains the items shown on the interface.

Item	Description
Type	Sets the type for detecting whether the SIP message conforms to the specification or the condition of blacklist, including *TLS Connection Failed*, *Malformed SIP Datagram*, *Registration Failed*, *Call Failed* and *SIP Exception Flow*.
Warning Threshold	Once the detection times of a type reaches the warning threshold, the source IP address contained in the SIP message will be recorded to the IDS warning log.
Blacklist Threshold	Once the detection times of a type reaches the blacklist threshold, the source IP address contained in the SIP message will be recorded to the blacklist.
Blacklist Validity	Set the effective time for the blacklist to work.

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

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

3.13.8 DDOS Settings

DDoS refers to Distributed Denial of Service (DDoS). Multiple attackers in different locations simultaneously launch attacks on one or several targets, or an attacker controls multiple machines in different locations and uses these machines to simultaneously attack the victim. Since the origin of attacks is distributed in different places, such attacks are called distributed denial of service attacks, and there can be multiple attackers. (Refer to "Distributed Denial of Service Attacks and the Defense Measures")

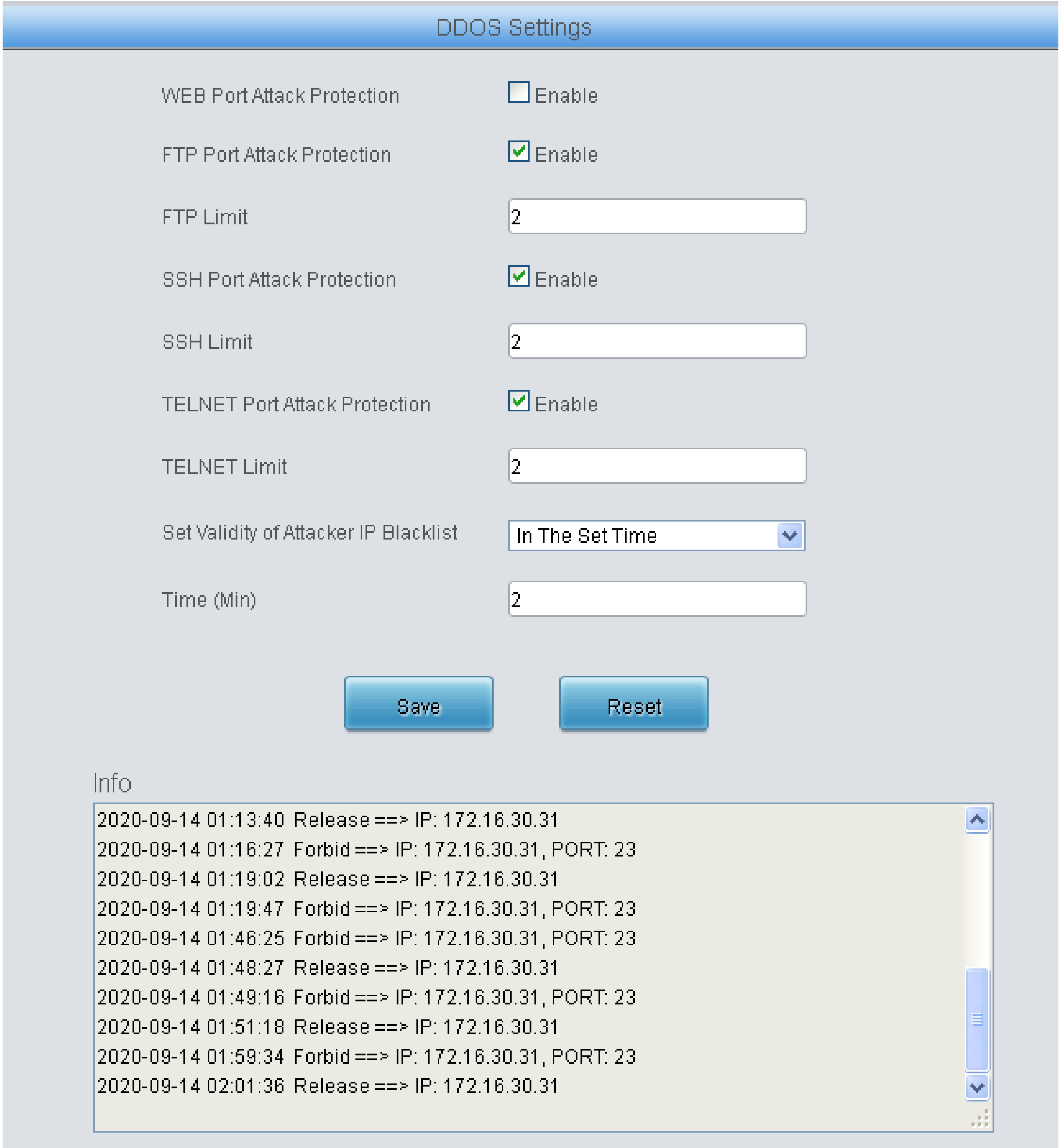


Figure 3-38 DDOS Settings Interface

The DDOS settings interface, as shown in Figure 3-38, can set the defense feature of some ports against DDOS attacks. The table below explains the items shown on the above interface.

Item	Description
WEB Port Attack Protection	When this feature is enabled, the WEB port will have the ability to block DDOS attacks.
WEB Limit	When the same IP address accesses the gateway through WEB, it will be forbidden to log in once the times exceed this set value (the number of access processes is /5).
FTP Port Attack Protection	When this feature is enabled, the FTP port will have the ability to block DDOS attacks.

FTP Limit	When the same IP address accesses the gateway through FTP, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
SSH Port Attack Protection	When this feature is enabled, the SSH port will have the ability to block DDOS attacks.
SSH Limit	When the same IP address accesses the gateway through SSH, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
TELNET Port Attack Protection	When this feature is enabled, the TELNET port will have the ability to block DDOS attacks.
TELNET Limit	When the same IP address accesses the gateway through TELNET, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
Set Validity of Attacker IP Blacklist	Sets the effective time of the attack blacklist, including two options *Forever* and *In the Set Time*.
Time	Sets the effective time for the blacklist to work.

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

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

3.13.9 Certificate Management

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

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

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

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

3.13.10 Centralized Manage

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

Item	Description
Notification Setting	If it is enabled, the gateway will send the SNMP TRAP warning information automatically.
Trap Server Port	The server port to receive the warning information, with the default value of 162.
CPU Temperature Threshold	The warning on high CPU temperature. Note: This feature is unavailable for SMG2000 series.
CPU Usage Threshold	The warning on high CPU utilization.
Memory Usage Threshold	The warning on high memory usage.
High CPS Threshold	The warning on high CPS.
Low Connection Rate Threshold	The warning on low connection rate.
Auto Change Default Gateway	Once this feature is enabled, the gateway will connect the DCMS via another network port automatically once the connected network cable is loosen or drawn out. The default value is disabled.
Management Platform	Select a management platform for the gateway to register.
Company Name	The company name used to register the gateway to DCMS, only valid when DCMS is selected.
Gateway Description	The description displayed on DCMS after the gateway is registered to DCMS, giving an easy identification of the gateway in device grouping. This item is only valid when DCMS is selected.
Centralized Management Protocol	Sets the centralized management protocol. It only supports SNMP currently.
SNMP Version	Sets the version of SNMP, three options available: V1, V2 and V3, with the default value of V2.
SNMP Server Address	IP address of SNMP.
Monitoring Port	Monitoring Port for SNMP on the gateway.
Community String	Community string used for information acquisition.
Account	The account of SNMP, only valid when the SNMP version is set to V3.
Grade	The grade of SNMP, three options available: Neither authenticated nor encrypted, Authenticated but not encrypted and Authenticated and encrypted, with the default value of *Neither authenticated nor encrypted*. It is only valid when the SNMP version is set to V3.
Authentication Password	The authentication password required to enter when the item Grade is set to Authenticated but not encrypted or Authenticated and encrypted.
Encryption Password	The encryption password required to enter when the item Grade is set to Authenticated and encrypted.
Working Status	The status of the connection between the gateway and the centralized management server. It is only valid when DCMS is selected.

3.13.11 Radius

The Radius Configuration interface is used to configure parameters about Radius. Once the

Radius feature is enabled, the gateway will serve as the Radius client and send messages to the Radius server at the start and end of each call to fulfill the charge business.

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

Item	Description
Radius	Sets whether to enable Radius or not, with the default setting of *disabled.*
Certification	Sets whether to send the certification message before sending the charge message, with the default setting of *enabled.*
Allow Calls even if Server doesn't Respond	Once this feature is enabled, the calls will be allowed even if the Radius server doesn't respond the certification message. The default value is *disabled*.
Local IP	Display the local IP address.
Master Server	Sets the IP address and port of the master Radius server. **Note:** If the port isn't designated, the default port 1813 will be used.
Shared Key	Sets the shared key used for the communication encryption between the master Radius server and the Radius client. **Note:** The key should be appointed by both the client and the server end ahead of time, and be configured the same at both sides.
Spare Server	Sets the IP address and the port of the spare Radius server which will be automatically started upon the occurrence of malfunction on the communications between the gateway and Radius master server. **Note:** If the port isn't designated, the default port 1813 will be used.
Timeout	Sets the maximum time to wait for the response after the message is sent out by Radius, with the default value of 3s. To guarantee the accuracy of the charge, the gateway will start the message retransmission mechanism once the charge message sent from the gateway to the Radius server is timeout without any response.
Retransmission Times	Sets the retransmission times on no response to the Radius message, with the default value of 1.
Transmit Interval of Charge Alive Package	Sets the transmit interval of the charge alive package, calculated by s. Range of value: 20~300, with the default value of *20*.

<table>
<tr><td>Call Type (Records output required)</td><td>Sets the type of calls which are required to output call records, including four options: PSTN→IP, IP→PSTN, conversion start and access failure.
<table>
<tr><th>Type</th><th>Meaning</th></tr>
<tr><td>PSTN→IP</td><td>Whether to send the Radius charge message for the calls from PSTN to IP</td></tr>
<tr><td>IP→PSTN</td><td>Whether to send the Radius charge message for the calls from IP to PSTN</td></tr>
<tr><td>Conversion Start</td><td>Whether to send the record of the initial conversion, that is, whether to have the gateway send the record information about the initial conversion to the Radius server upon the connection of the conversion.</td></tr>
<tr><td>Access Failure</td><td>Whether to send the record of the calls in access failure, that is, whether to have the gateway send the record information about the calls in access failure to the Radius server upon the access failure occurs.</td></tr>
</table></td></tr>
</table>

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

3.13.12 SIP Account Generator

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

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

3.13.13 Recording Manage

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

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

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

3.13.14 Configuration File

Via the Configuration File interface, you can check and modify configuration files about the gateway, including SMGConfig.ini, ShConfig.ini, Ss7Server.ini, hosts and Chcaller.ini. Configurations about the gateway server, such as route rules, number manipulation, number filter and so on, are included in SMGConfig.ini; configurations about the board are included in ShConfig.ini; and configurations about the SS7 server are included in Ss7Server.ini. hosts is the system file relating a domain name and its corresponding IP address. Chcaller.ini is used to configure the calling party number you require to a channel, in which EnableChCaller is the switch and pcmChX indicates the calling party number. Once the switch is on, the CallerID manipulation in the direction of PSTN->IP will go invalid. 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.

3.13.15 Signaling Capture

On the Signaling Capture interface, Data Capture is used to capture data on the network interface you choose. Click ***Start*** to start capturing data (up to 400M for SMG2000 series; up to 800M for SMG3000 series) on the corresponding network interface. SIP, ISDN, SS7 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.

3.13.16 Signaling Call Test

The Signaling Call Test interface mainly helps to test whether the route and the number manipulation already configured are proper or not, and whether the call can succeed or not.

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

Item	Description
Test Type	The 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	Sets the generic number in the IAM message.
Generic Number Property	Sets the properties of the generic number in 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, FieldName, 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.

3.13.17 Signaling Call Track

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

3.13.18 Network Speed Tester

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

Note: Only the SMG3000 series support this feature.

3.13.19 PING Test

Via the Ping Test interface, a Ping test can be initiated from the gateway on a designated IP address to check the connection status between them. The table below explains the configuration items shown on the interface.

Item	Description
Source IP Address	Source IP address where the Ping test is initiated.
Destination Address	Destination IP address on which the Ping test is executed.
Ping Count	The number of times that the Ping test should be executed. Range of value: 1~100.

Package Length	Length of a data package used in the Ping test. Range of value: 56~1024 bytes.
Info	The information returned during the Ping test, helping you to learn the network connection status between the gateway and the destination address.

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

3.13.20 TRACERT Test

Via the Tracert Test interface, a Tracert test can be initiated from the gateway on a designated IP address to check the routing status between them. The table below explains the configuration items shown on the interface.

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

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

3.13.21 Modification Record

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

3.13.22 Backup & Upload

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

3.13.23 Factory Reset

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

3.13.24 Upgrade

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

3.13.25 Account Manage

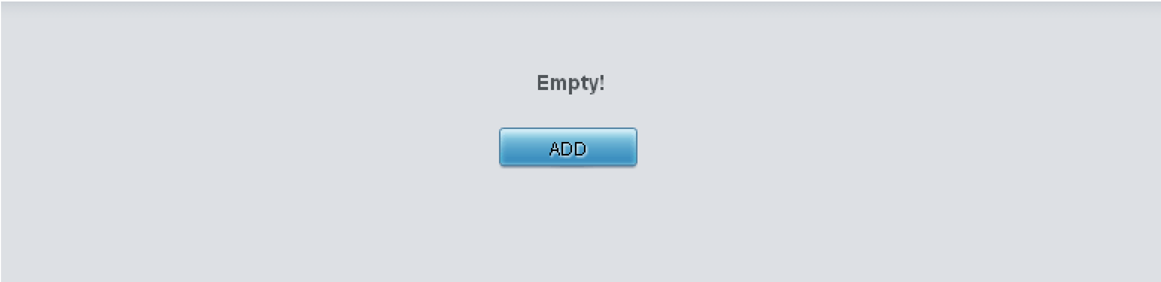


Figure 3-39 Account Management Interface

See Figure 3-39 for the Account Management interface. By default, there is no user information available on the gateway, click ***Add*** to add a piece of information.

Figure 3-40 User Information Adding Interface

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

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

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-41 for the user information list.

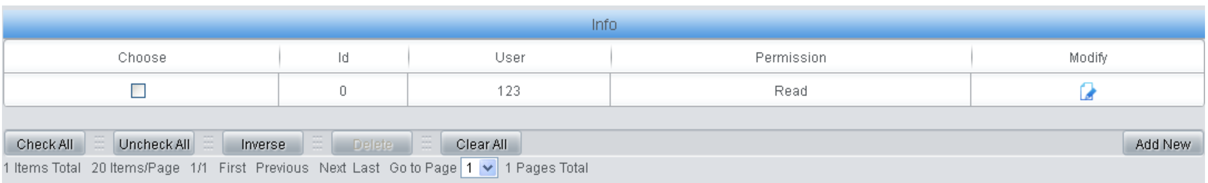


Figure 3-41 User Information List

Click ***Modify*** in Figure 3-41 to modify a piece of user information. The configuration items on the user information modification interface are the same as those on the ***User Information Adding*** interface. Note that the item ***Index*** cannot be modified.

To delete a piece of user information, check the checkbox before the corresponding index in Figure 3-42 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all user information at a time, click the ***Clear All*** button.

3.13.26 Change Password

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

3.13.27 Device Lock

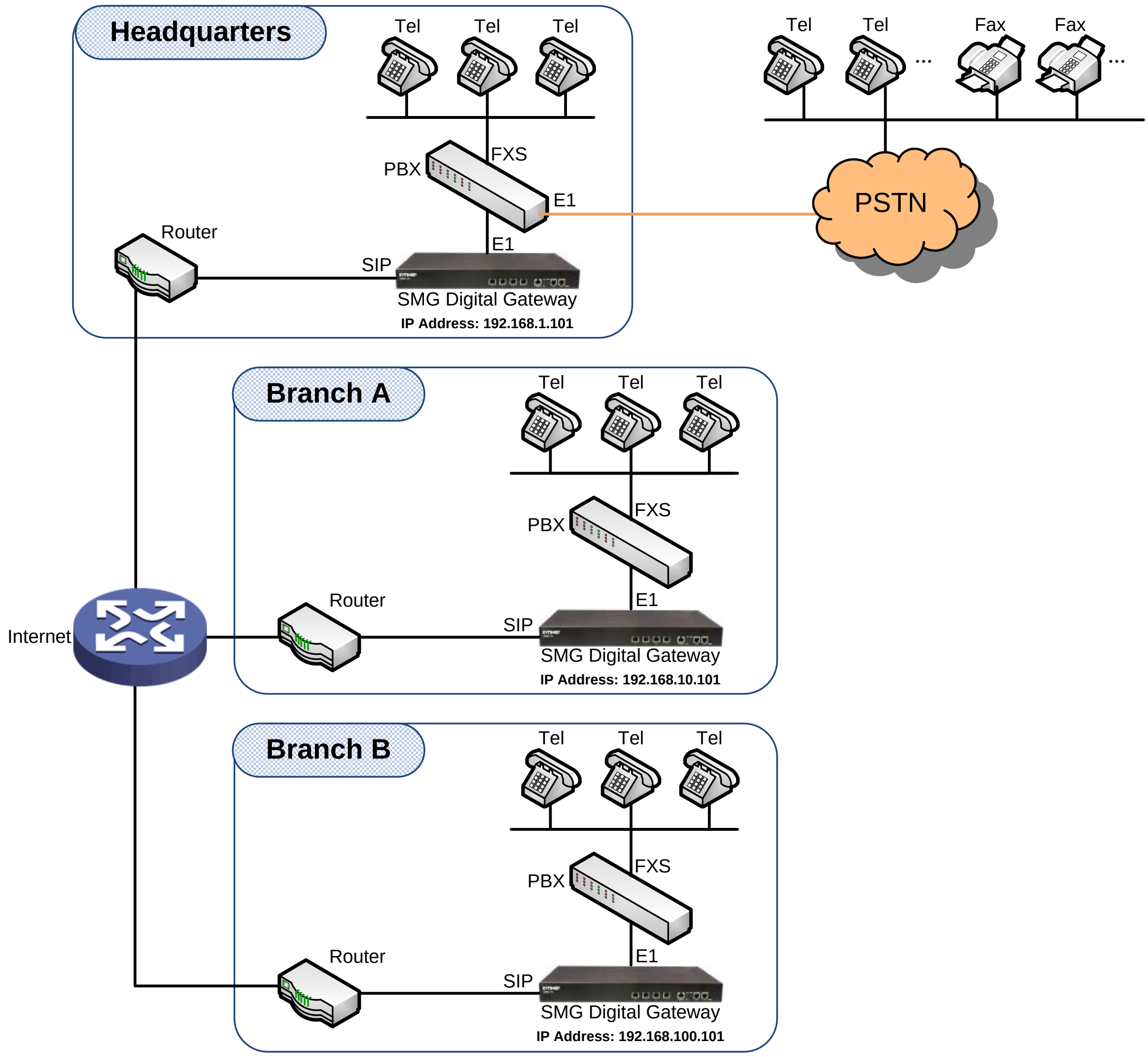
On the Device Lock Configuration interface, when you select one or more than one conditions to lock the gateway, the configurations of the gateway related to the selected conditions will be locked. That is, to modify any one of those configurations, you are required to input the lock password. Click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

3.13.28 Restart

On the Restart interface, click ***Restart*** on the service restart interface to restart the gateway service or click ***Restart*** on the system restart interface to restart the whole gateway system.

Chapter 4 Typical Applications

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.

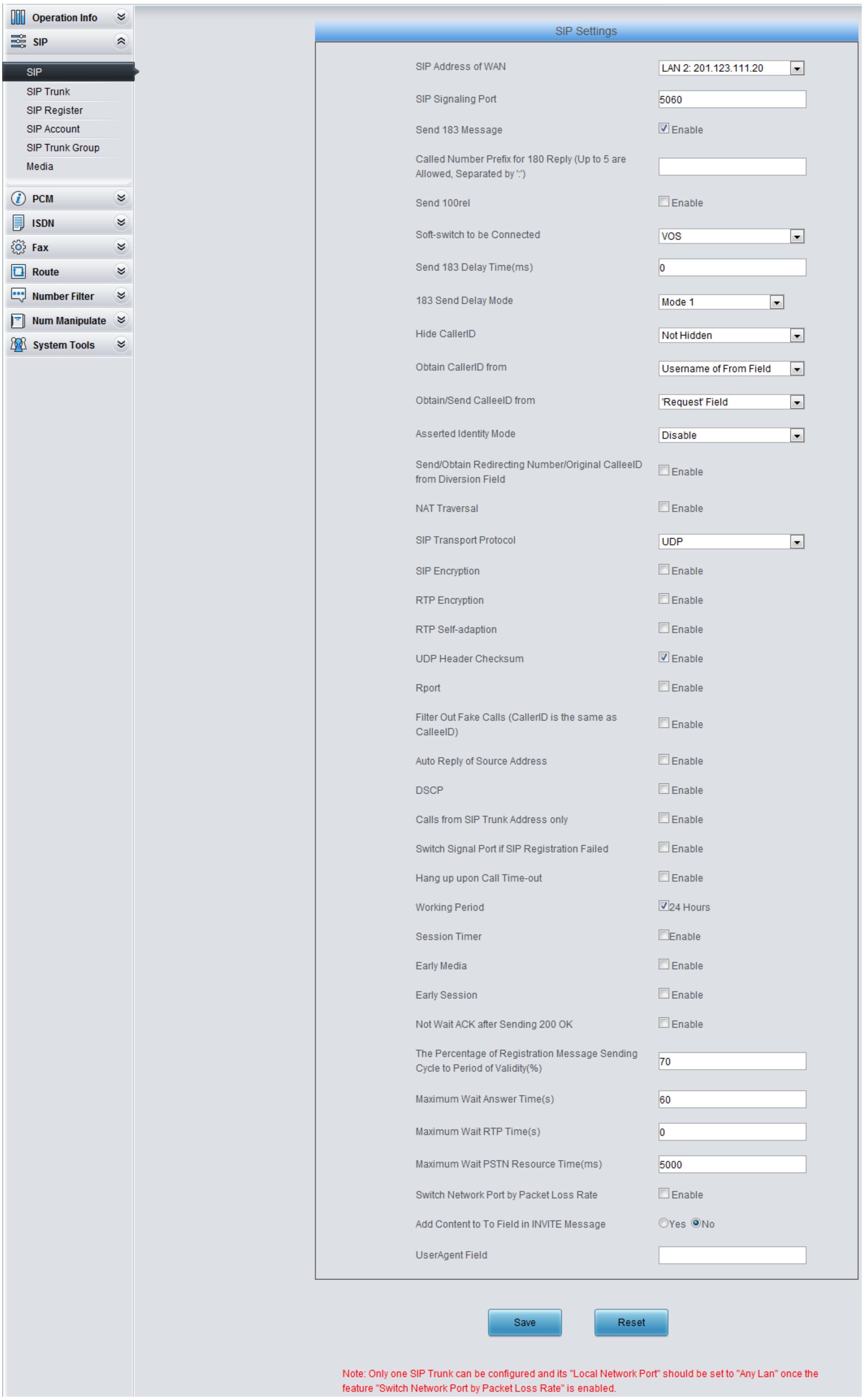
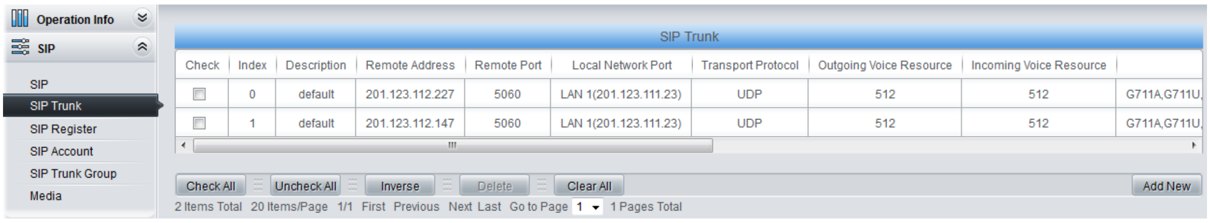

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated 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

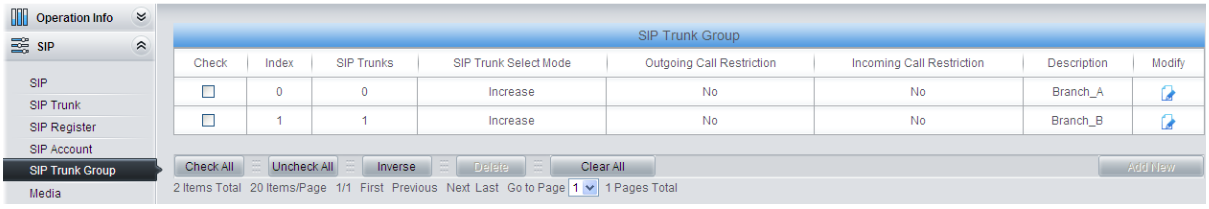
2. Add the IP addresses of the gateways at Branch A and Branch B into the SIP trunks.



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

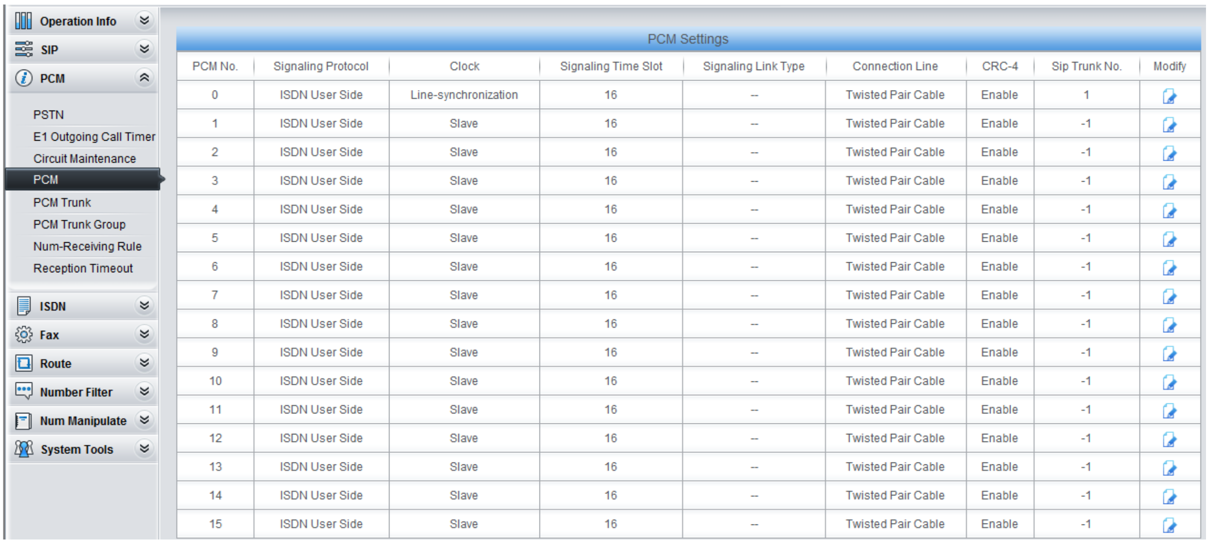
3. Add the SIP trunks at Branch A and Branch B into the corresponding SIP trunk groups.



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

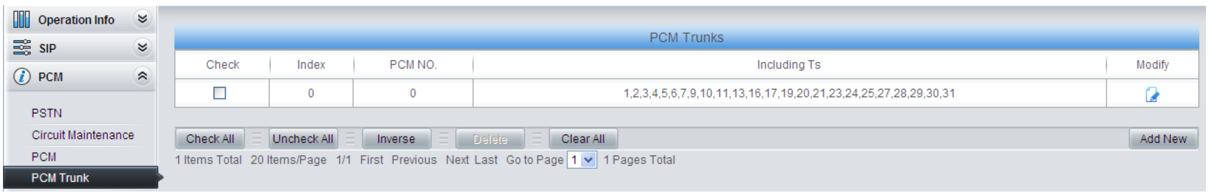
4. Set PCM.



PCM 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



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.

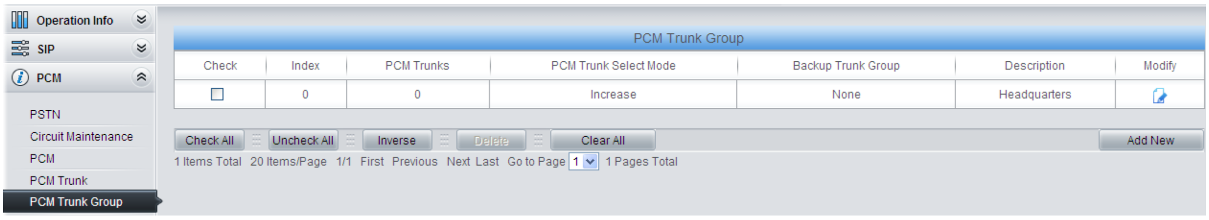


Figure 4-7

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

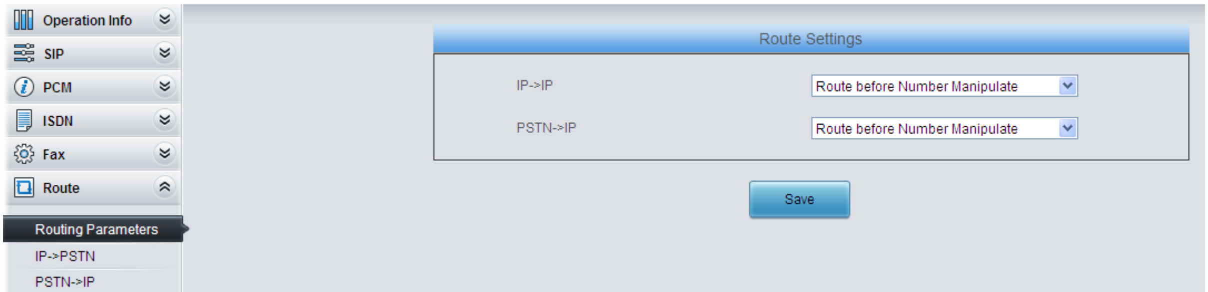


Figure 4-8

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.

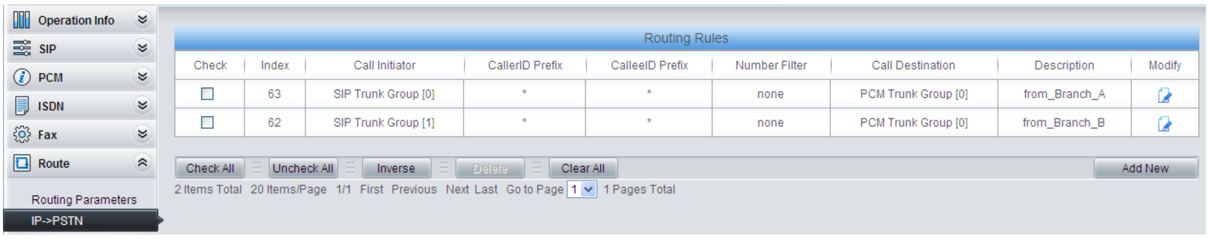


Figure 4-9

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.

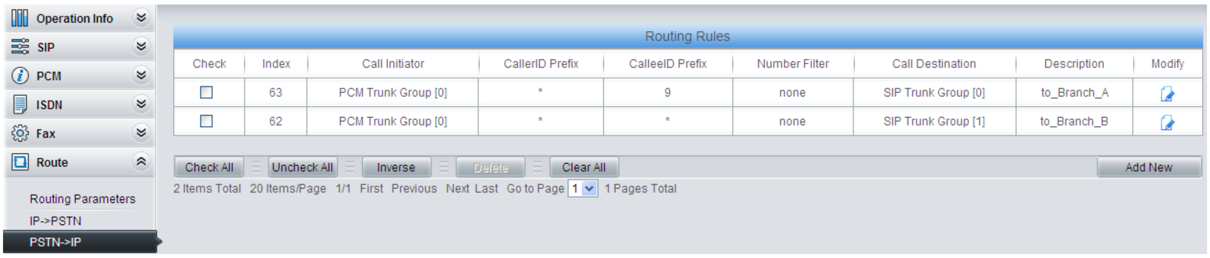


Figure 4-10

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.

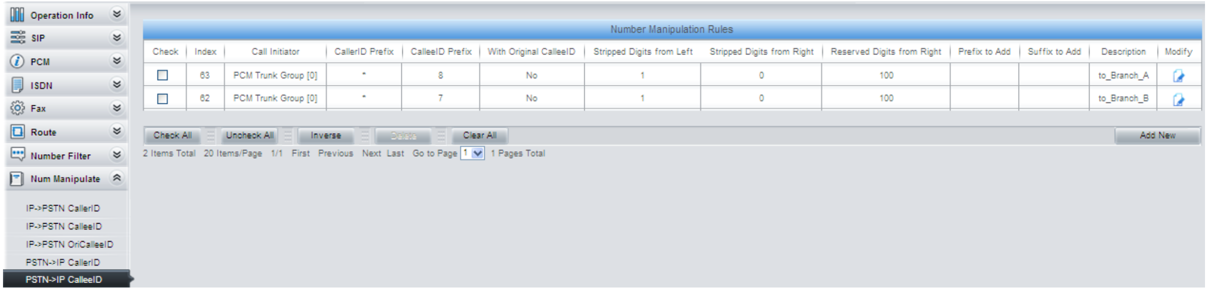


Figure 4-11

4.1.2 Configurations for Branch A

1. Configure SIP Settings for Branch A.

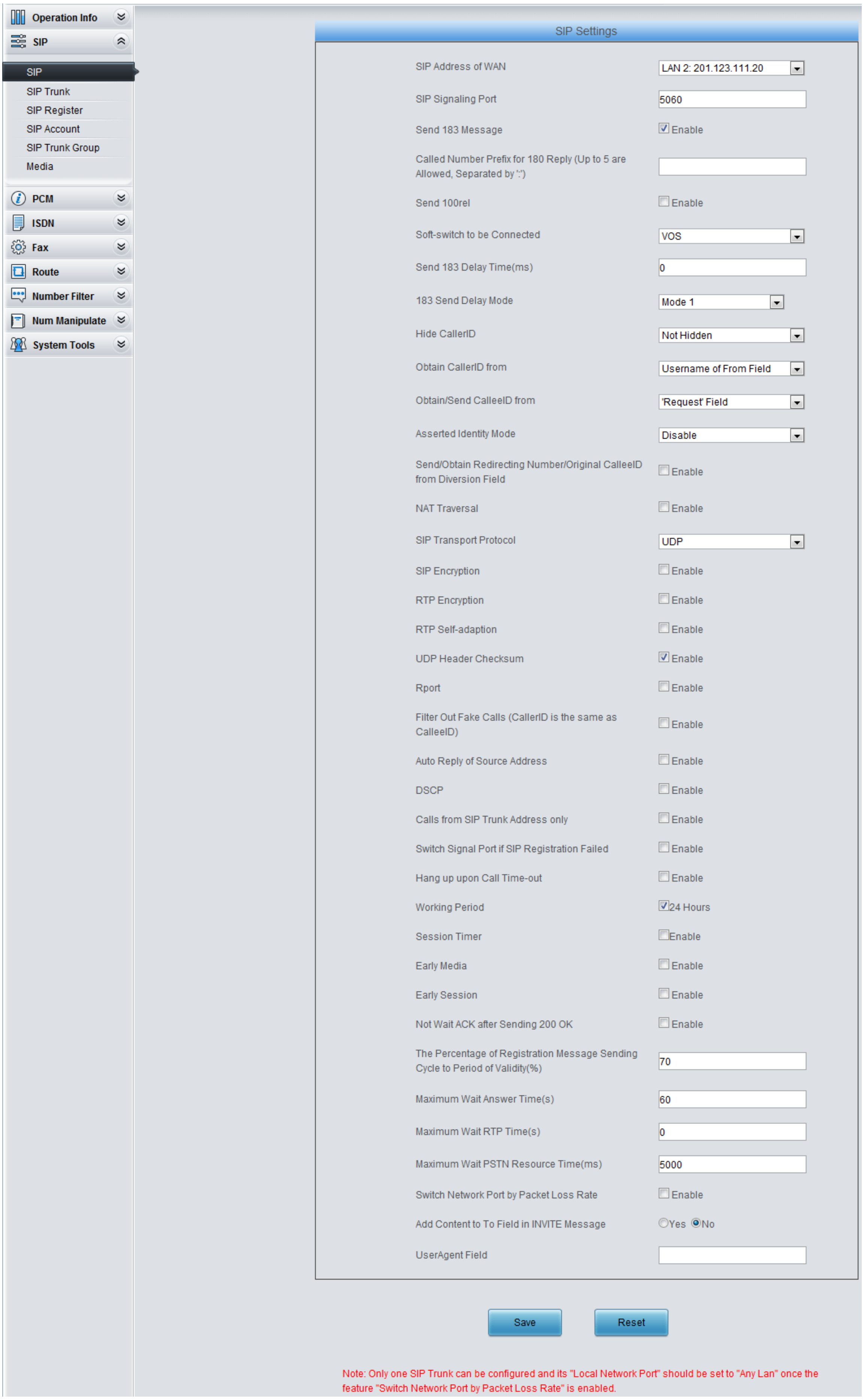

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated 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.

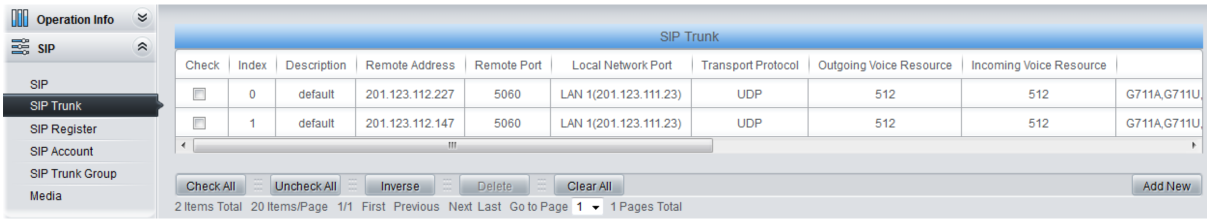


Figure 4-13

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

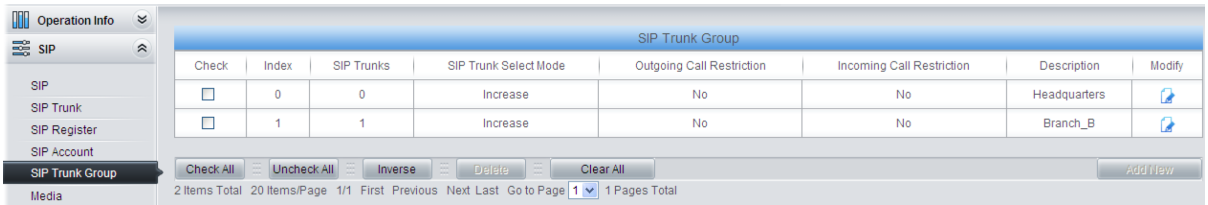


Figure 4-14

4. Set PCM.

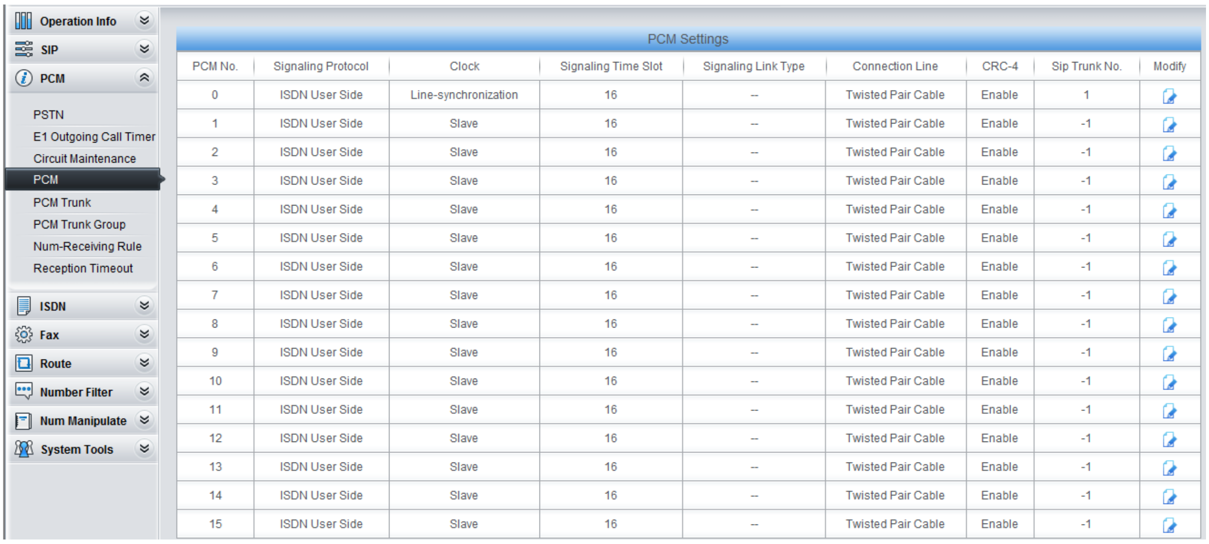


Figure 4-15

5. Add PCM trunk

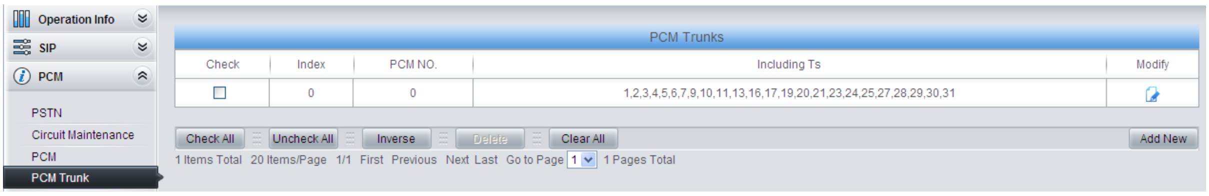


Figure 4-16

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

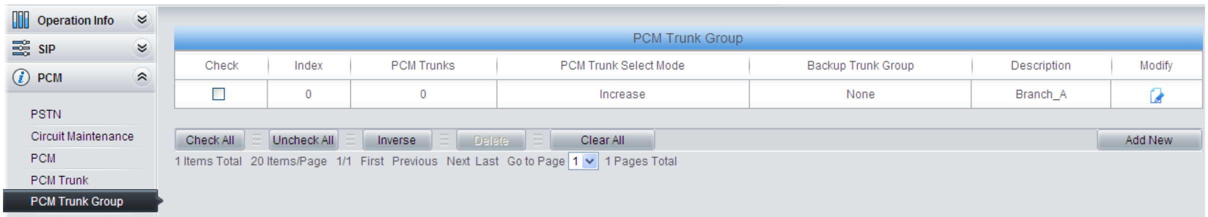


Figure 4-17

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

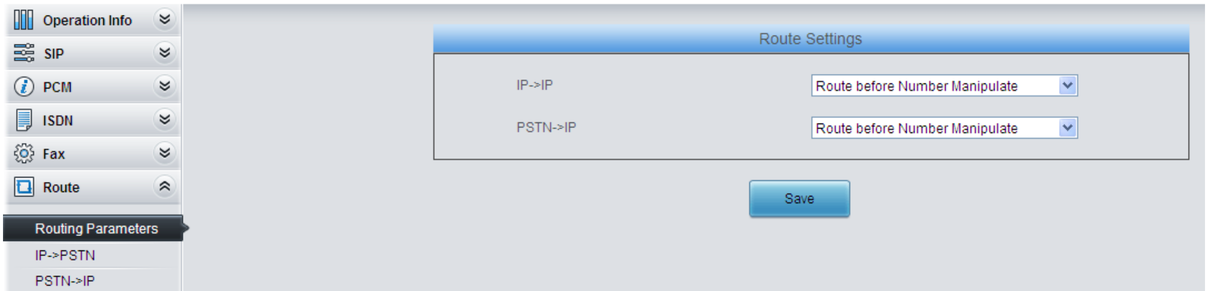


Figure 4-18

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.

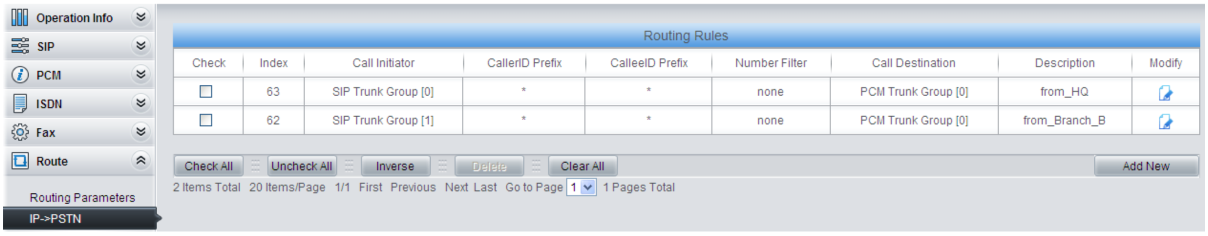


Figure 4-19

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.

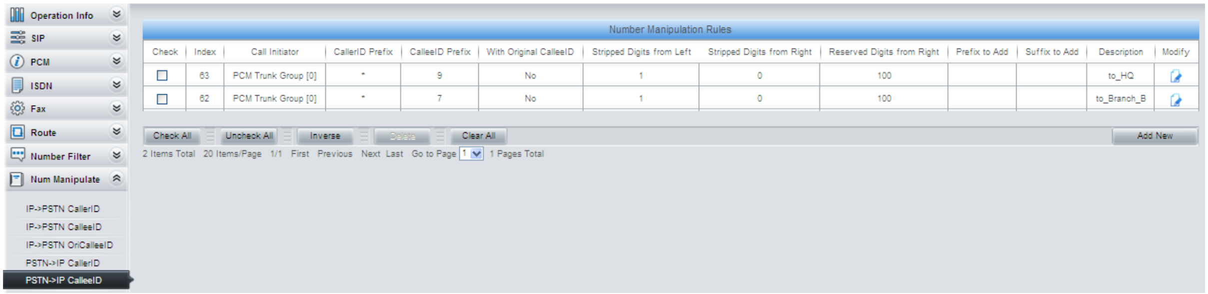


Figure 4-21

4.1.3 Configurations for Branch B

1. Configure SIP Settings for Branch B.

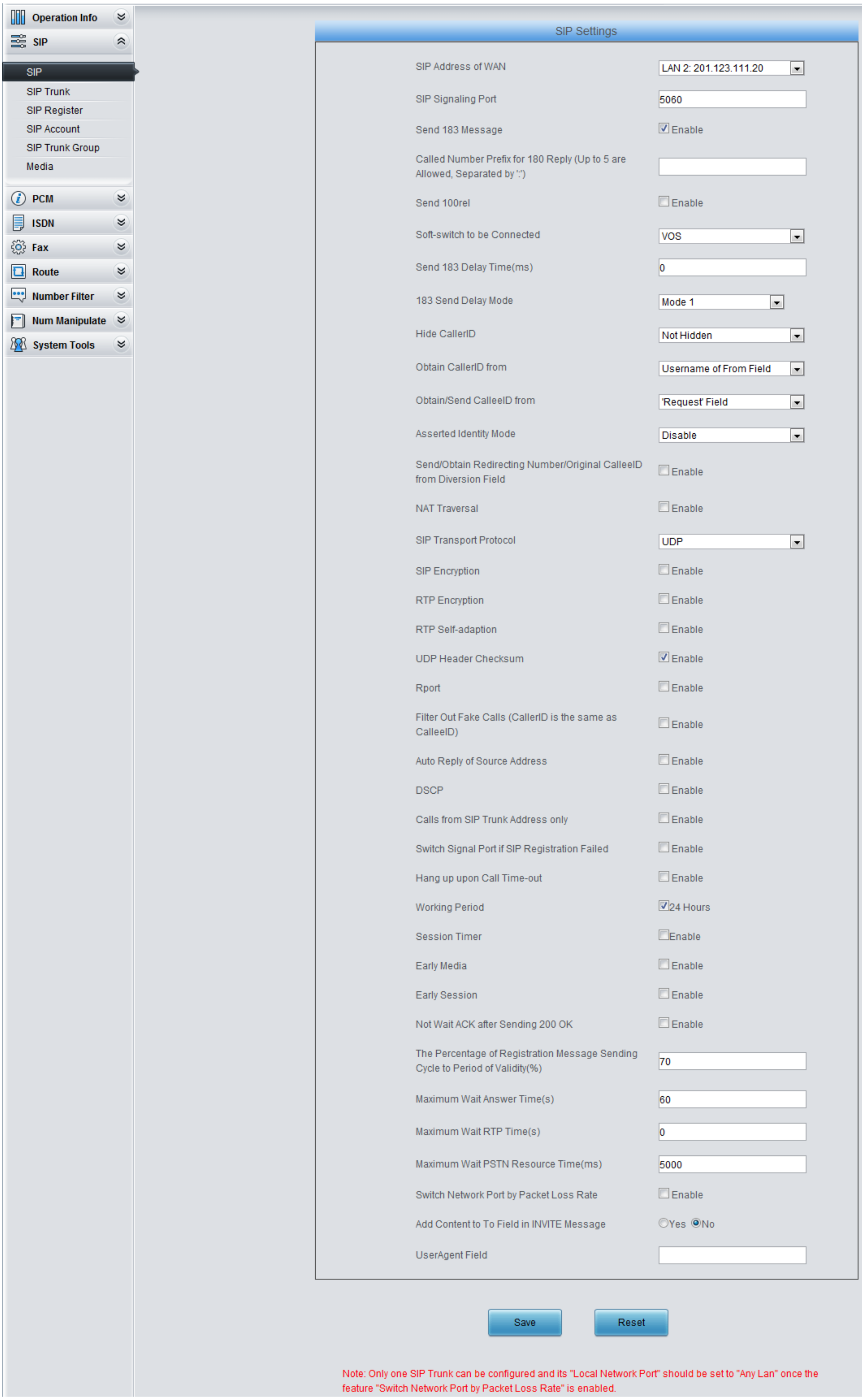

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated 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.

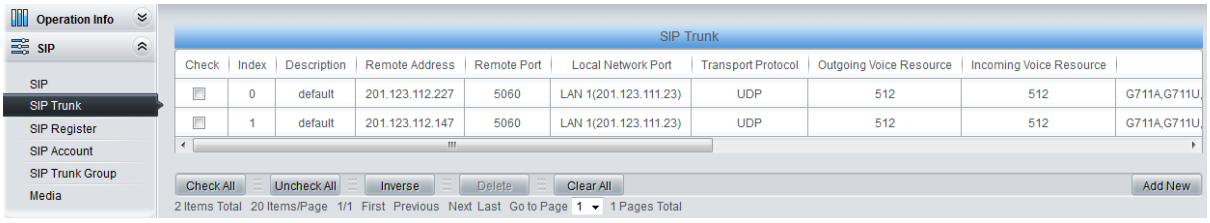


Figure 4-23

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

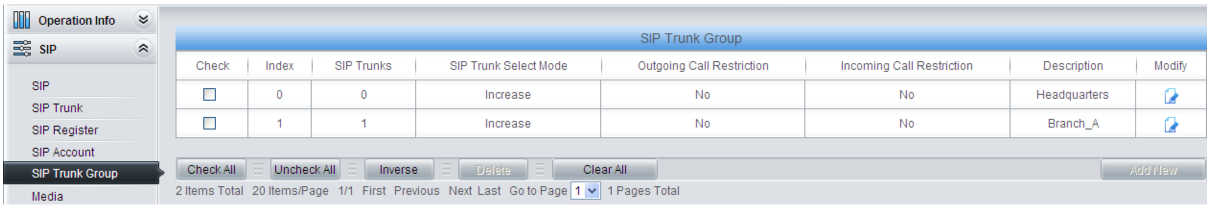


Figure 4-24

4. Set PCM.

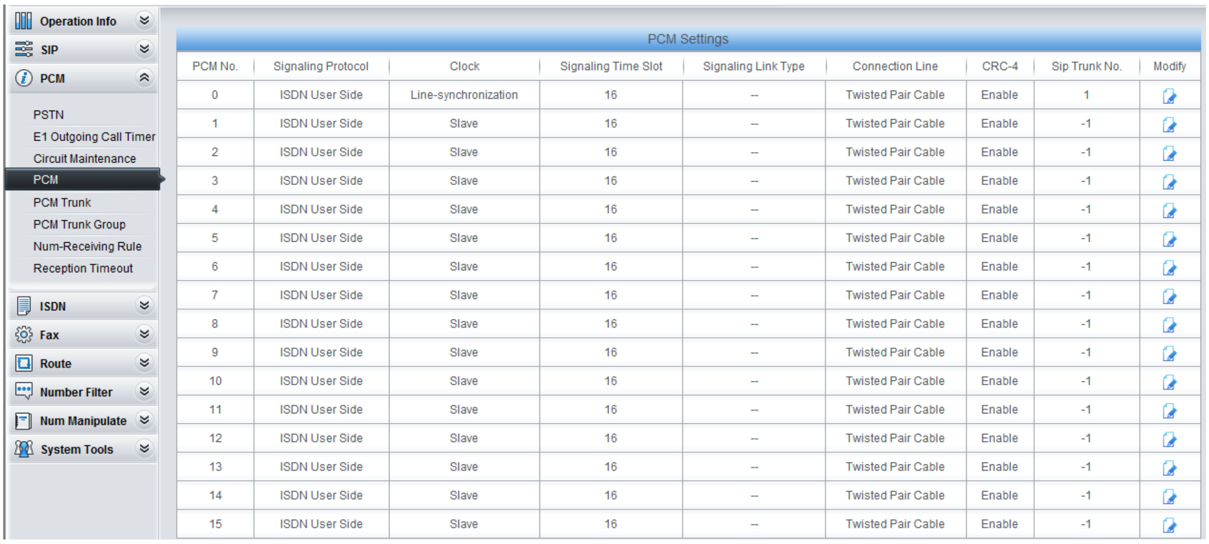


Figure 4-25

5. Add PCM trunk

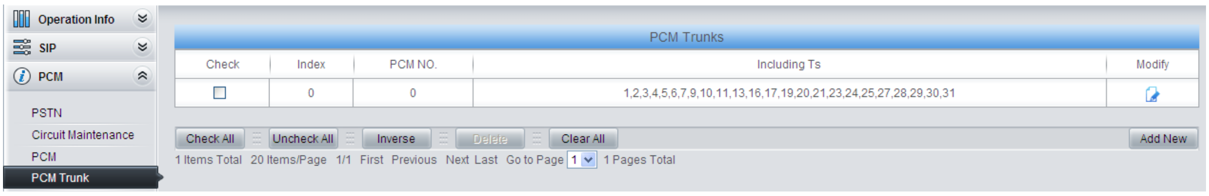


Figure 4-26

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

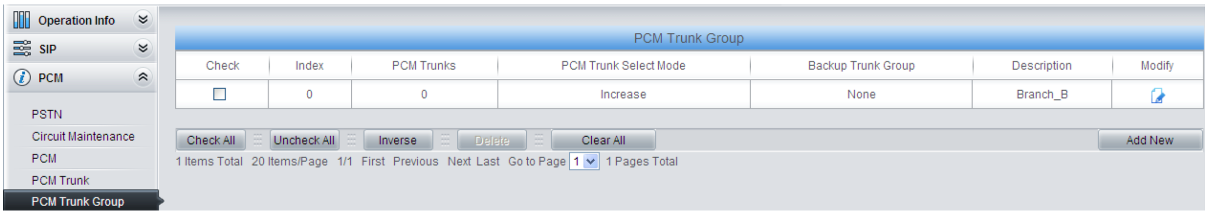


Figure 4-27

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

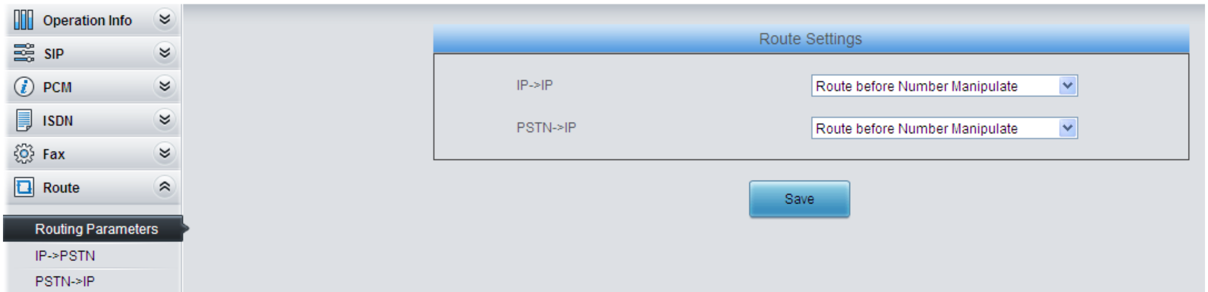


Figure 4-28

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.

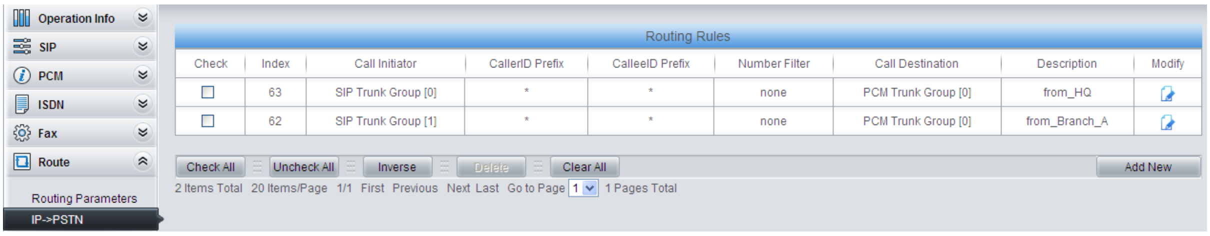


Figure 4-29

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.

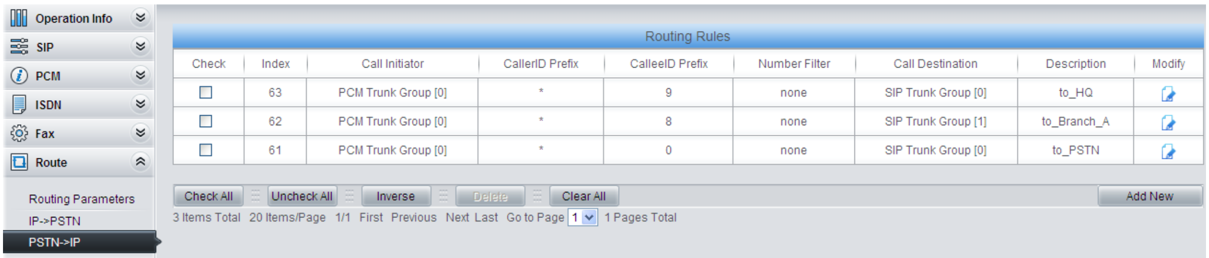


Figure 4-30

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.

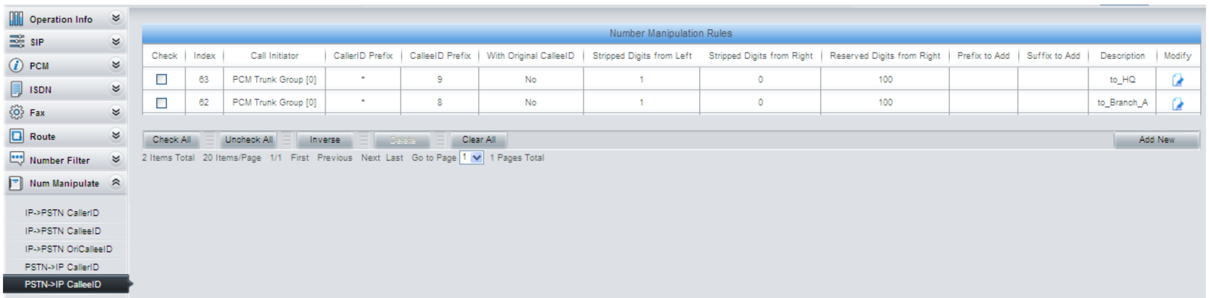


Figure 4-31

4.2 Application 2

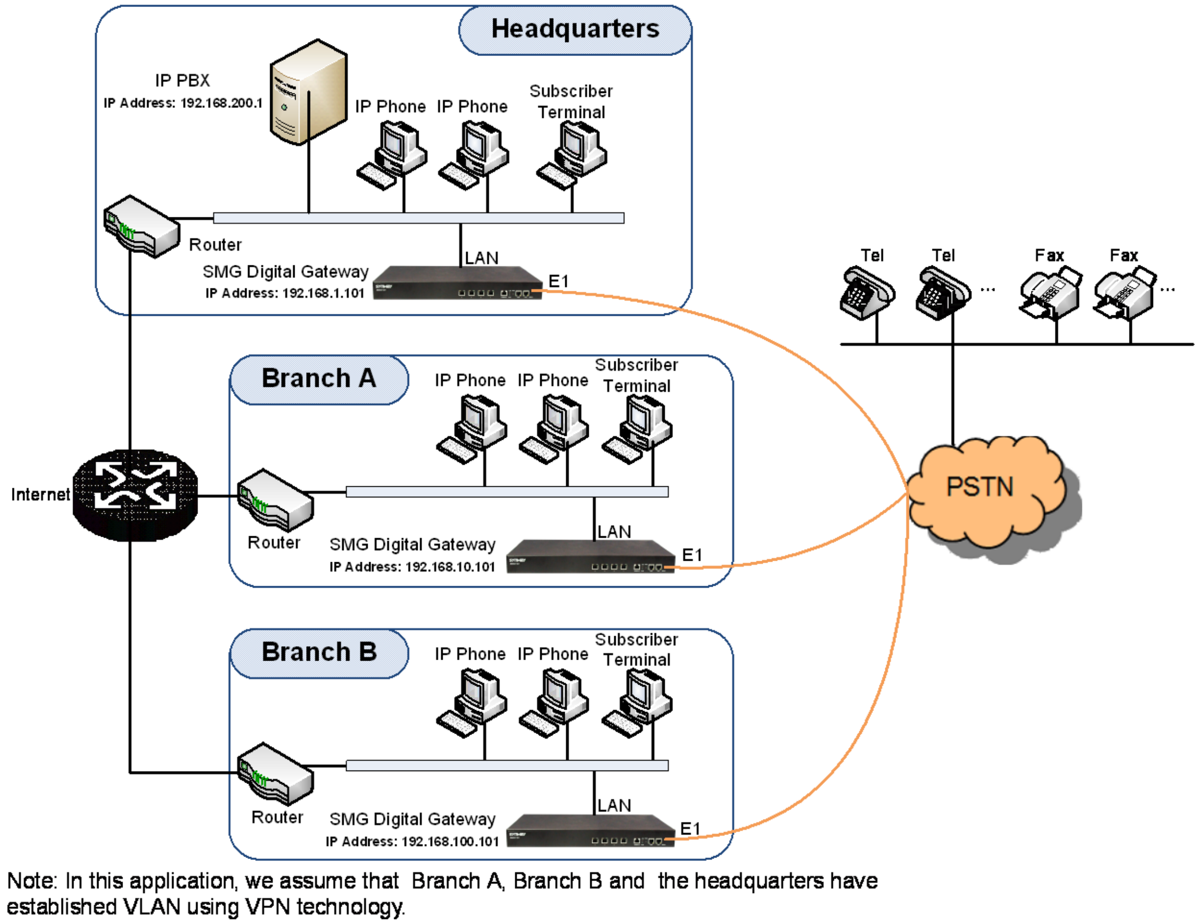


Figure 4-32 Application 2

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.

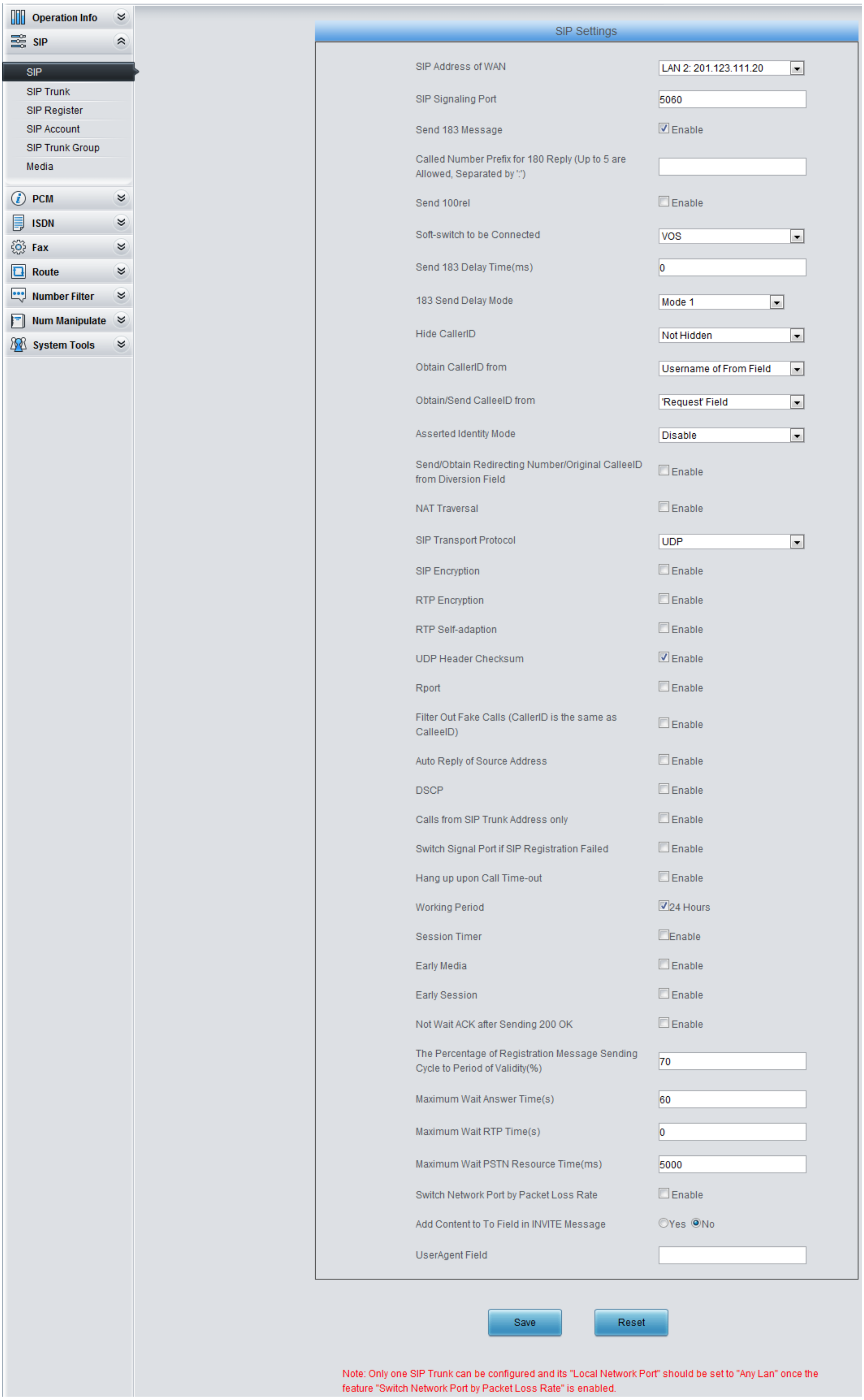
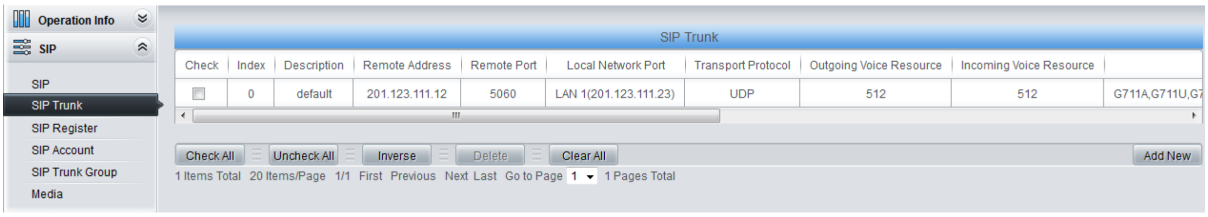

Operation Info
SIP
SIP
SIP Trunk
SIP Register
SIP Account
SIP Trunk Group
Media
PCM
ISDN
Fax
Route
Number Filter
Num Manipulate
System Tools
SIP Settings
SIP Address of WAN
LAN 2: 201.123.111.20
SIP Signaling Port
5060
Send 183 Message
Enable
Called Number Prefix for 180 Reply (Up to 5 are Allowed, Separated 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

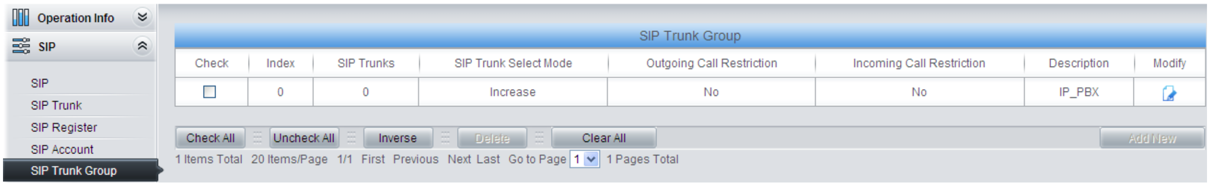
2. Add the IP address of the IP PBX into the SIP trunk.



Check	Index	Description	Remote Address	Remote Port	Local Network Port	Transport Protocol	Outgoing Voice Resource	Incoming Voice Resource	
☐	0	default	201.123.111.12	5060	LAN 1(201.123.111.23)	UDP	512	512	G711A,G711U,G7

Figure 4-34

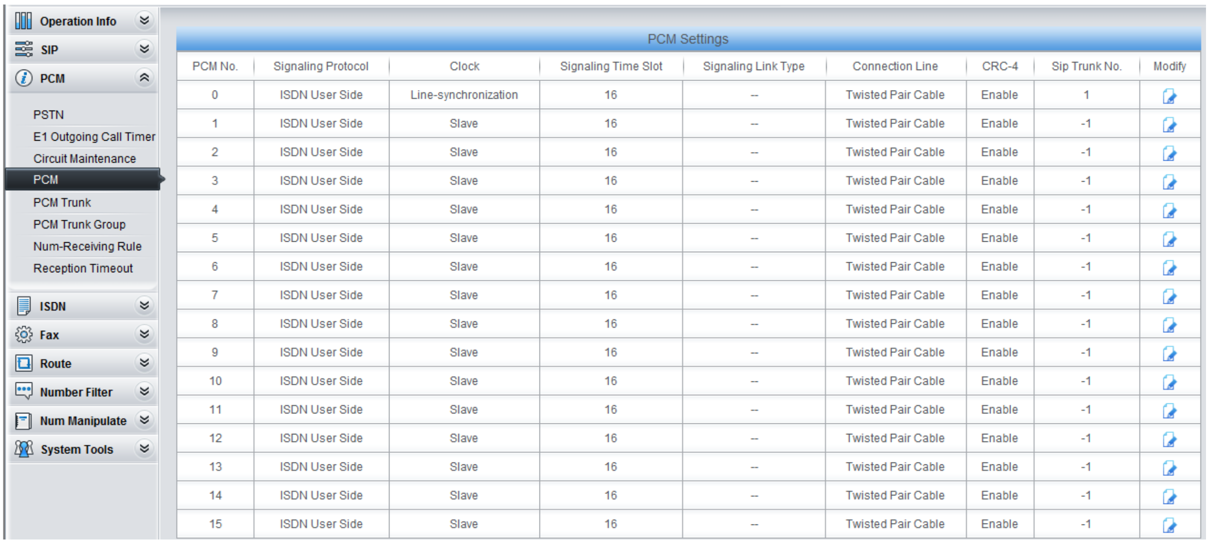
3. Add the SIP trunk into the corresponding SIP trunk group.



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

Figure 4-35

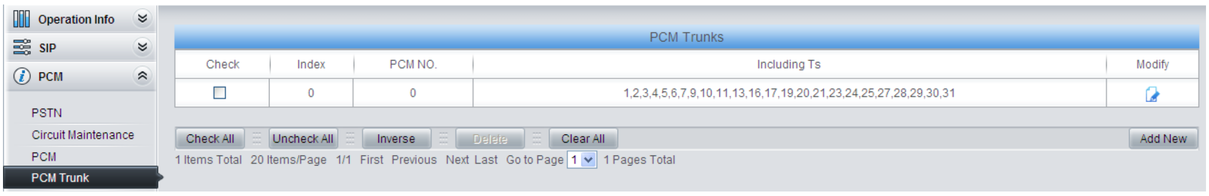
4. Set PCM.



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 4-36

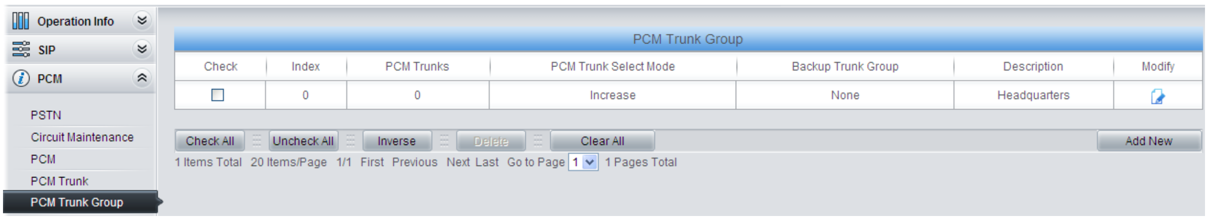
5. Add PCM trunk



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 4-37

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



Check	Index	PCM Trunks	PCM Trunk Select Mode	Backup Trunk Group	Description	Modify
☐	0	0	Increase	None	Headquarters	

Figure 4-38

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

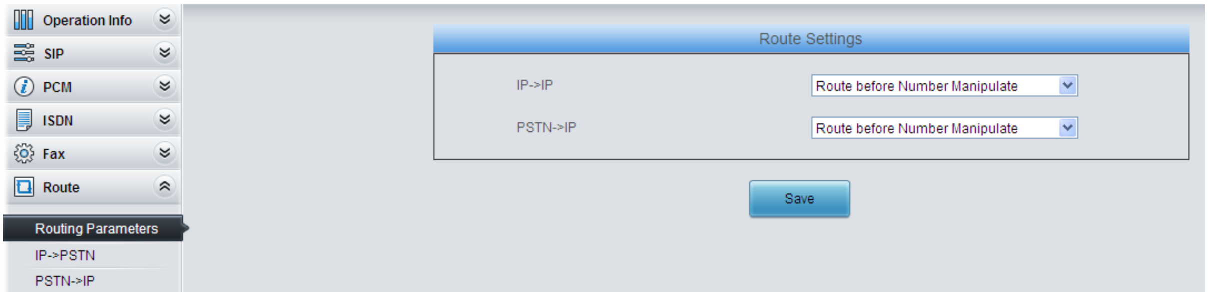


Figure 4-39

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.

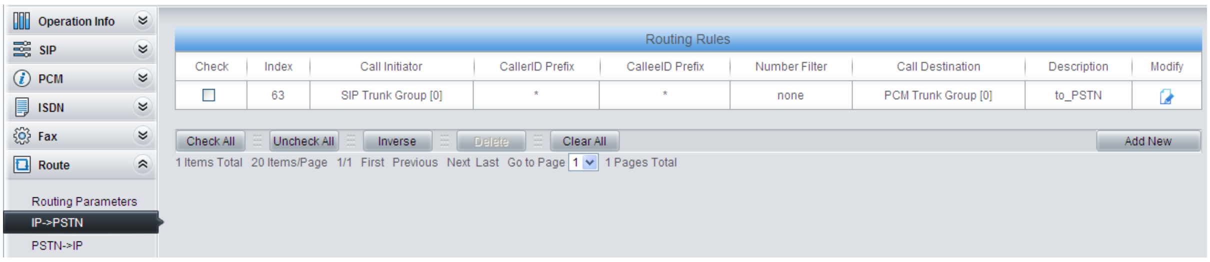


Figure 4-40

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.

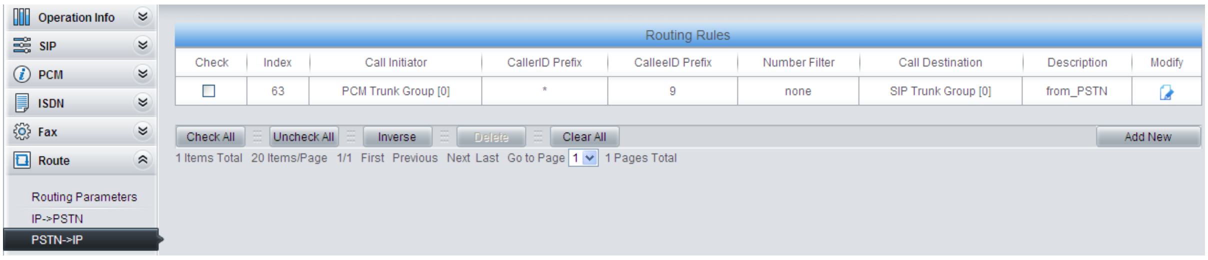


Figure 4-41

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

440×44×267 mm^3

(190×30×123 mm^3 for L-type)

Weight

SMG2000 Series: About 3.5kg

SMG3008/3016: About 3.75kg

SMG3000-B1/B2/B4: About 3.4kg

SMG3000-B1L/B2L: About 0.65kg

SMG3000-C1L: About 3.4kg

Environment

Operating temperature: 0℃—40℃

Storage temperature: -20℃—85℃

Humidity: 8%— 90% non-condensing

Storage humidity: 8%— 90% non-condensing

LAN

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

Self-adaptive bandwidth supported

Auto MDI/MDIX supported

E1/T1 Port

Amount: 1/2/4/8/16

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 power: 100~240V AC

Note: The input power of SMG3008B/SMG3016B is +48V DC; SMG3000-B1L/B2L and SMG3000-C1L use the +12V power adapter.

Maximum power consumption：

SMG2000 series: ≤12W

SMG3000, SMG3000B series: ≤22W

SMG2000L series: ≤10W

Signaling & Protocol

SS7: TUP, ISUP

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-NB	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

Note: SMG3000-B1/B2/B4 only supports the encoding formats G711A, G711U, G729, G723 (30), AMR (20), ILBC (20/30).

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 ISUP (ISDN) Pending Cause to SIP Status Code

ISUP (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 TUP Pending Cause to SIP Status Code

TUP Return Value	Cause	SIP Status Code	Implication
11	SS7 signaling: receives SSB message from remote PBX	486	Busy here
12	SS7 signaling: receives SLB message from remote PBX	486	Busy here
13	SS7 signaling: receives STB message from remote PBX	486	Busy here
67	TUP: receives CBK message from remote PBX	403	Forbidden
21	SS7 signaling: receives ACB message from remote PBX	403	Forbidden
18	SS7 signaling: receives CFL message from remote PBX	504	Forbidden
14	SS7 signaling: receives UNN message from remote PBX	488	Not acceptable here
16	SS7 signaling: receives CGC message from remote PBX	406	Not acceptable
17	SS7 signaling: receives NNC message from remote PBX	406	Not acceptable
19	SS7 signaling: receives LOS message from remote PBX	406	Not acceptable
20	SS7 signaling: receives SST message from remote PBX	406	Not acceptable
22	SS7 signaling: receives DPN message from remote PBX	406	Not acceptable
23	SS7 signaling: receives EUM message from remote PBX	406	Not acceptable
24	SS7 signaling: receives ADI message from remote PBX	484	Address incomplete

Appendix E 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 F Technical/sales Support

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

Headquarters

Synway Information Engineering Co., Ltd

http://www.synway.net/

9F, Building 1, Joinhands Science Park, No.4028, Nanhuan Road, Binjiang District, Hangzhou, P.R.China, 310053

Tel: +86-571-88860561

Fax: +86-571-88850923

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

Technical Support

Tel: +86-571-88864579

Mobile: +86-18905817070

Email: techsupport@sanhuid.com

Email: techsupport@synway.net

MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: sales@synway.net