Redstone Systems, Inc.

DGW100, SIP-Trunking Gateway Series

User Manual

Website: http://www.redstonesystems.com
Tech support: 4259006680
Email: gs@redstonesystems.com

Document Version: 202308

Contents

Contents of Figure

Contents of Table

1 Overview

1.1 Product Introduction

The DGW100 SIP trunking gateway (hereinafter the DGW100) is a VoIP product series developed by Redstone Systems, Inc. It uses the SIP and T1/E1 interfaces for the inter-conversion of IP packets and PCM signals, allowing the interworking of the IP-based new-generation voice network to legacy Public Switched Telephone Network (PSTN), and the private branch exchange (PBX) of an enterprise.

As a carrier-class VoIP gateway, the DGW100 is designed under the requirements of telecom operators, integrators, value-added service providers as well as large and medium-sized enterprises for VoIP services. The DGW100 has distinctive advantages over other similar products in terms of performance, system reliability, compatibility and cost performance. In addition, the DGW100 has efficient software and hardware architecture and powerful DSP processing capabilities, ensuring the realization of major functions (including the conversion between PCM signals and IP packets, G.711 or G.729A encoding and decoding of voice signal, and echo cancellation, etc.) even under full load conditions.

By supporting the ISDN PRI and T1 CAS signaling, the DGW100 can control its calls with the PSTN or PBX. The call control between the DGW100 and media gateway controller (softswitch) is carried out through Session Initiation Protocol (SIP). By now, the DGW100 has successfully passed the interoperability test with various popular softswitch platforms and IP PBX products.

1.2 Features

The DGW100 has the following characteristics:

High performance

The DGW100 adopts the DSP chip with high powerful voice processing. Its DSP daughter card ensures a 6000 MIPS processing capability for each gateway, enabling the DGW100 to provide functions of voice signal processing (G.711, G.729A, and G.723.1), echo cancellation, and fax relay (T.38) under full load conditions (120 calls).

High security

To ensure security, the DGW100 supports SSH and HTTPS for remote access, and provides functions including signaling and media stream encryption, automatic password strength test, brute-force password cracking prevention, cipher text data storage, access whitelist, and system log backup.

High reliability

The DGW100 provides Dual-LAN ports redundancy protection to ensure the calls aren't affected by local network failures, meanwhile, 1+1 AC/DC power supplies (optional) can be equipped to meet with the requirement of customer for high reliability. In terms of deployment, DGW100 provides a disaster recovery mechanism including the registration and switching of primary and standby SIP servers.

Remote Management and Maintainability

The Redstone Cloud client inside the DGW100 allows the DGW100 located behind an enterprise NAT or firewall to be accessed across Internet securely. Real-time monitoring, alarm notification, remote packet capture and software upgrades can be performed with the Redstone Network Management System.In addition, it also supports the third-party element management systems with TR-069.

Low cost and protect investment

How to reduce cost and investment risk is one of the major challenges a user faces when choosing an IP-based new generation of voice device. In the lifetime cycle, the DGW100 helps to follow the ongoing evolution of VoIP technologies by software upgrading, and it increases new functions and applications continuously in the same time.

It supports multiple protocols

The DGW100 supports different kinds of protocols including Session Initiation Protocol (SIP), Real-time Transport Protocol (RTP), Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Session Traversal Utilities for NAT (STUN), Also, the DGW100 supports different technologies including ISDN PRI and T1 CAS signaling, G.711, G.729A, or G.723.1 encoding and decoding, G.168 echo cancellation, Dual-Tone Multi-frequency (DTMF) message transmission (RFC 2833), and fax relay (T.38).

High interoperability

By now, the DGW100 has successfully passed the interoperability test with various softswitch platforms and IP PBX products both in the domestic and overseas market.

1.3 Hardware Performances

1.3.1 Appearance

Front Panel

Table 1-1 Front Panel

Mark	Description
RST	Pressing the RST button for less than three seconds: no action will be taken. Pressing the RST button for more than three seconds: the factory settings will be restored.
PWR	Indicators for power supply, system status and alarm. See Table 1-2 for the meaning of indicators.
STU	
ALM	
CON	Configuration interface. See 1.3.2 Configuration interface.
ETH	Specifies an RJ45 module interface. Interfaces ETH1 and ETH2 share the same IP address for allowing access to the external

Mark	Description
	network. Dual-LAN redundancy is supported. See Table 1-2(indicators) and Table 1-4(Pinouts of T1/E1 Module) for other details.
AUX	An RJ45 interface. Interfaces AUX1 and AUX2 share the same IP address for local management and configuration. See Table 1-2(indicators) and Table 1-4(Pinouts of T1/E1 Module) for other details.
T1/E1	An RJ45 interface, in support of 1 T1/E1, 2 T1/E1, and 4 T1/E1. Each T1 interface supports the maximum 24 voice channels; each E1 interface supports the maximum 30 voice channels. See Table 1-2(indicators) and Table 1-4(Pinouts of T1/E1 Module) for other details.
SD	A SD card socket.

Table 1-2 Indicators

Mark	Function	Status	Description
PWR (red, green)	Power Indication	Steady green	The power supply is working.
		Off	No power supply.
		Steady red	The power supply is abnormal.
STU (red, green)	Status Indication	Off	The device is locked.
		Blinking red	System is in a diagnostic mode and you can execute limited operation (e.g. Log in to system through Telnet)
		Steady Red	The device is starting.
		Blinking green	System is operating normally
ALM (red, green)	Alarm Indication	Steady green	No alarms
		Blinking red	Device startup failure
		Steady red	Network failure or app exited
ETH/ AUX	Interface state indicator	Steady green (right side)	The transmit speed is 1000M bit/s.
		Off (right side)	The transmit speed is 10M bit/s or 100M bit/s.
		Steady green (left side)	The link has been established but no service traffic is transmitted.
		Blinking green (left side)	Service traffic is being transmitted on the link.
		Off (left side)	The link is not established.
T1/E1 (red, green)	Interface state indicator	Steady green	The connection works normally.
		Blinking red	A remote alarm is generated.
		Steady red	A local alarm is generated.
		Off	No connection is established.

Table 1-3Pinouts of Ethernet Ports

Pinouts No.	1	2	3	6
Description	TX+	TX-	RX+	RX-

Table 1-4 Pinouts of T1/E1 Module

RJ45 Pinouts No.	1	2	3	4	5	6	7	8
Description	RX Ring	RX Tip	NC	TX Ring	TX Tip	NC	NC	NC

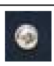
Back Panel (AC)

Table 1-5 Description of Back Panel

#	Description
① 	AC power socket, 100-240 VAC voltage input.
② 	Ground pole.

Back Panel (DC)

Table 1-6 Description of Back Panel

#	Description
① 	DC power socket, -36 to -72 VDC voltage input.
② 	Ground pole.

1.3.2 CON Port

The DGW100 provides one configuration interface (CON) of RJ45 interface.

Table 1-7 Standard Table for Lead Wire of Pin at Configuration Port (CON)

Pin number of RJ45 plug	1	2	3	4	5	6	7	8
Description	NC	NC	TXD	GND	GND	RXD	NC	NC
Pairing connection with DB9 female plug	-	-	2	-	5	3	-	-
Pairing connection with DB25 male plug	-	-	3	-	7	2	-	-

This configured interface is for local management and try out.The configured interface is connected to the RS232 port on the PC, allowing the PC to establish the connection with the DGW100 by configuring a terminal emulator. The configured interface of DGW100 is in a 3-wire configuration: one TXD (data transmission terminal), one RXD (data reception terminal), and one GND (ground terminal).

Please use a RJ45-RS232 serial cable for connecting the CON port on DGW100 side and the RS232 port on PC side. This connection cable shall be purchased by user. If the connection is established between DGW100 and the mobile PC with no RS232 ports, please use the cable together with USB to RS232 converter cable. Please see the figures below for the two kinds of cables above.

Figure 1-4 RJ45-RS232 serial cable

Figure 1-5 USB to RS232 serial cable

Table 1-8 Attributes of CON Port

Attributes	Description
Connector	RJ45
Interface count	1
Interface standard	RS232
Baud rate	115200
Data bit	8
Parity	No
Stop bit	1
Traffic control	No

1.3.3 Technical Specifications

Table 1-9 Specifications

Items	Description
Standard Specifications	
Ethernet	RJ45, 4×10/100/1000M Base-T, self-adaptive

Items	Description
E1/T1Interface	4pcs(Max. 120 simultaneous VoIP calls)
SD Interface	1pc
CON Interface	RJ45
System Memory	256MB
System Flash	32MB
Processor	TI AM3352
DSP	TI C5509
AC power supplies	~100 to 240V, 50/60Hz, 1A
DC power supplies	-36 to -72 VDC, 2.5A
Power Consumption	18 W (Max)
Size (H×W×D)	44×440×300 mm,1U height, suit for wide rack(19 inch) installation
Weight	net weight:3 kg gross weight(with box):5 kg
Environment Requirements	
Operating Environment	0 to 40℃, Non-Condensing Humidity 10 to 90%
Storage Environment	-10 to 60℃, Non-Condensing Humidity 5 to 90%

2 Installation Preparation

For avoidance of personal injury and device damage, please read this chapter carefully before installation.

2.1 Safety Precautions

For your safety, please follow the precautions when DGW100 is installed and used.

- Keep the site far from the heat and humidity;
- Take precautions with use of high-voltage electricity;
- Please let the experienced or trained operator to install and maintain DGW100;
- Wear static discharge wrist strap;
- Ensure the proper electric ground of installed equipment;
- Properly connect the power cable to DGW100
- Do not plug the power cable when in use;
- UPS is advised.

2.2 Requirements of installation

2.2.1 Temperature and Humidity

Check the temperature and humidity of equipment room to ensure the normal operation and long service life of the gateway, the temperature and humidity in the room should be kept at the proper range.

The humidity in the equipment room should be kept between 10% and 90% (non-condensing).

- Long term high humidity may lead to bad insulation and even cause electricity leakage, and it may cause metal corrosion,too.
- Low humidity is likely to leave captive screws to loose due to static electricity built up and the insulation washer shrunk.

The temperature in the equipment room should be kept between 0℃ and 40℃.

- High temperature acceralets aging of electrical parts and insulation materials.
- Low temperature, however, may destabilize the operation of gateway.

2.2.2 Cleanliness and Ventilation

Dust is very harmful to the safe operation of the gateway. Dust that is adsorbed by static electricity acts as insulator may cause poor contact between metal components and contacts, which not only affects the service life of the gateway but also leads to communication failure. Therefore, the room for the gateway must be kept clean.

In addition, keep at least 5cm clearance at the air intake and air exhaust vent of the gateway to ensure perfect ventilation for heat dissipation. The rack for DGW100 also must with good ventilation system.

2.2.3 Power Supplier

Check whether the voltage of the power supply system is stable or not, and whether the power rate can meet with the requirement or not.

The speficiation of DGW100 power supply:100V~240V(AC),50~60Hz,1A,or -36V~-72V(DC),2.5A.

2.2.4 Grounding

For AC power supply system

When the installation site without independent grounding system, the AC power supply system must ensure:

- The AC power outlet has a protection ground contact.
- The ground contact of AC supplier must be grounded properly.
- Avoid sharing the multi-outlet power strip with other devices that may generate electrical interference.

In an installation equipment room that can provide indepedent grounding, the specialized ground terminal which provided by DGW100 shall be connected reliably with the independent grounding system in the equipment room. And this can not only ensure the safety of equipment during operation, but also can avoid the voice quality being disturbed by the environment.

For DC power supply system

The DC power working ground (the positive pole of the -48V DC power supply or negative pole of the 24V DC power supply) of the communications site should be connected with the indoor collective grounding cables nearby, and the grounding cables should meet the requirement for the maximum load of the equipment.

The power supply equipment of the communications site should be connected with from the collective ground cable in the communications building (or from the protection grounding bar of the equipment) to the DC working ground cable.

2.2.5 Electromagnetic Environment

Any possible interference source, wherever it is from, impacts the gateway negatively. In order to improve the ability of resist the interference and lightning protection of the gateway, make sure that:

- Keeping the gateway far from high power wireless radio station, radar station, and high-frequency large current devices.
- The gateway is capable for 2nd class of lightning protection on wires and cables, if there is outdoor wire,then it must adopts 1st class of lighten protection.
- The power supply system should be used independently as much as possible and effective measures of preventing electric grid from interference should be adopted.
- Ensure a good power grounding effect of equipment or add a lightning protector.

2.2.6 Other Facilities

- **Rack**

  DGW100 requires an installation site with good air-flow system to cool down the gateway, and should be firm enough to support the weight of the gateway. It is also recommended the rack is earth grounded properly.

- **PSTN Line**

  Be sure to subscribe PSTN lines from local telephone company and activate the lines prior to the installation.

- **IP Network**

  The gateway is connected to IP network through its 10/100/1000M Standard Ethernet port and communicate with other equipments through the network. Check IP network on the site, including route, Ethernet switch installation, cable wiring,etc to make sure the gateway can be connected to the IP network properly.

- **AC Power Outlets**

  When supply AC to the gateway by using power supply socket outlet nearby, verify that each socket outlet is equipped with protective earth contact and ensure the reliable grounding for the protection point of the power supply in the building.

2.3 Opening Inspection

After the completion of installation preparation, you should open the box for inspection. Make sure the gateway and all in-box accessories match the description below.

An DGW100 with basic configuration should include components as shown in following table.

Table 2-1 Standard Configuration

Specification & Type	Quantity
Gateway	1

Specification & Type	Quantity
19-inch Rack Mounting Kits	1
T1/E1 Cable	1/2/4
Power Cord (AC) or Plug-in Wiring Terminal (DC)	1 or 2 Note: 2 for dual power supplies
Grounding Cable	1
Installation Guidelines	1

Note

The package list is only for reference. Changes may be made according to actual condition by us. The detailed inclusions are on the shipping list enclosed in the device package. Please contact your supplier if you have any question or any mistake.

3 Installation

3.1 Main Tools and Meters for Installation

- Screwdriver
- Antistatic wrist strap
- Ethernet and console port cables
- Power cable
- HUB,telephone set,fax machine or PBX
- Terminals (a PC with super terminal simulating program can be used)
- Multimeter

3.2 Install the Gateway to the Standard Rack

The DGW100 series chassis are designed to be mounted on a standard 19-inch rack, and each gateway occupies 1U height in the 19-inch standard rack.

3.2.1 Attaching the Brackets

Place the DGW100 series chassis on the workbench, take two L-shape rack mounting brackets and screws, install the brackets at the left and right sides of the equipment by screws.

Note: The L-shape brackets are used to secure the gateway to the rack. The brackets cannot support the weight of the equipment alone. Therefore, a supporting shelf must be installed in place to support the gateway.

Installation of L-shape Brackets

3.2.2 Mounting the Gateway

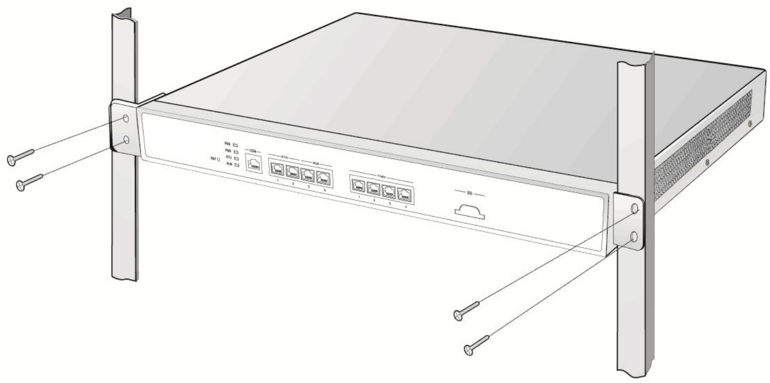
Following attentions should be paid during the installation:

- Ensure that the rack is stable and firmly attached to the ground.
- Ensure the rack with good ventilation and heat dissipation.
- If multiple gateways are installed in a standard rack, it is recommended to keep enough space between gateways for heat dissipation.

Follow the steps to install the gateway:

- Place the gateway on a shelf in the rack, and the gateway must locates in the middle and with right direction.
- Slide it to a proper position along the guide rails, adjust location of gateway to align the fixing holes on the L-shape brackets with the locating holes on the rack or fixing vertical beam of the rack.
- Fix the L-shape brackets to the fixing vertical beam on the both sides of the rack by supplied screws.

Mount Gateway to Rack



3.3 Connecting Cables

3.3.1 Connecting Console (CON) Port Cables

A CON should be provided by DGW100 to check errors of the device. Connect the CON with computer’s RS232 serial ports, then local computers can interwork with the device through simulating terminal program.

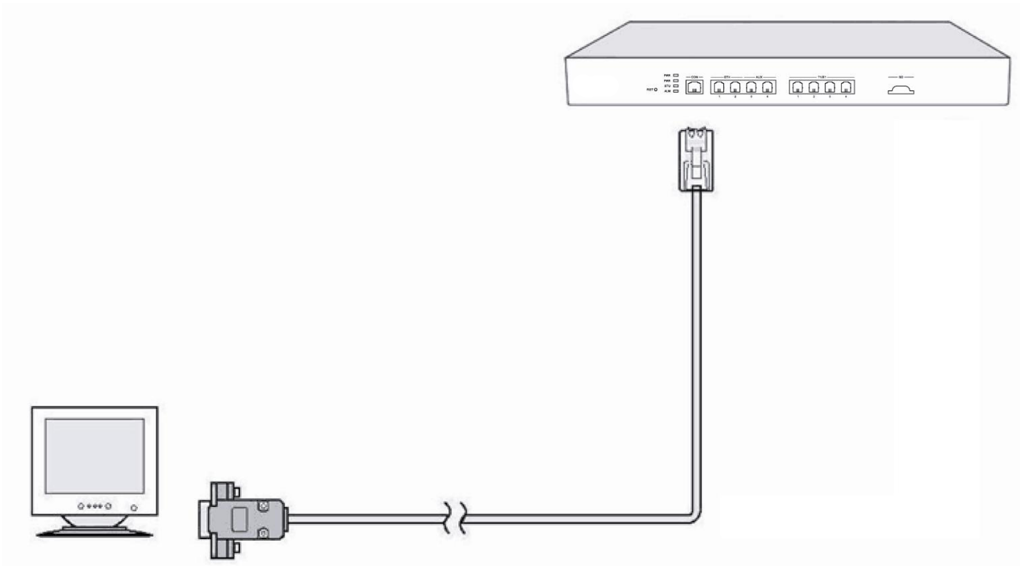
RJ45 Plug is used to connect with the CON cable to connect with one of the CON port of the gateway, and another port is applied for DB9 Adapter to insert serial ports of configuration terminal. CON Ratio: 115200.

Console Port cable installation procedure is as following:

Step1 Choose a terminal (PC).

Step2 Power off the terminal and connect RS232 port with the Console port(CON) of the gateway by the Console port cable.

Cable of Connecting CON



3.3.2 Connecting the Ethernet Cable

The DGW100 has the dual-network-interface redundancy function. When one of the network interfaces is disconnected or does not work well, traffic services can be switched seamlessly to the other one.

The DGW100 has two service interfaces, namely ETH1 and ETH2. These two interfaces need to be connected to the same HUB, LAN, or WAN. Only one of them works at a time. After Ethernet cables are inserted, check the indicator state of the interface that is connected first. If the indicator is steady green or blinking green, it indicates that the connection is established properly.

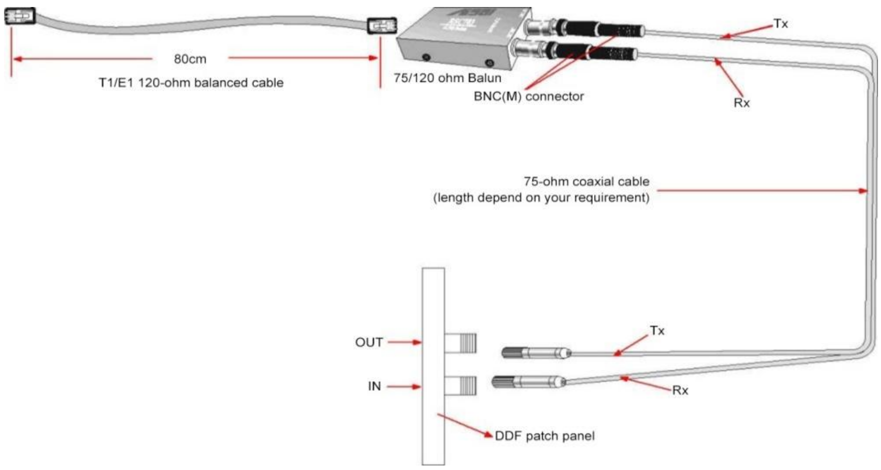
The DGW100 has two auxiliary interfaces, namely AUX1 and AUX2. In most cases, no connection is required.

3.3.3 Connecting the T1/E1 Cable

T1/E1 terminal of DGW100 provides Trunk port for connection with PBX or PSTN.

Plug one end of the T1/E1 cable into the T1/E1 port of DGW100,and plug another end into the PBX or the digital port of the PSTN,if it is RJ45 port,then the order of wire shall be adjusted, if it uses coax cable,then follow the figure to make the connection.

Connecting the T1/E1 Cable



Note

The T1/E1 ports are numbered 1 to 4 from left to right. If the hardware configuration is 1 T1/E1, insert one end of the T1/E1 cable to the leftmost T1/E1 port on the DGW100.

3.3.4 Connecting the Grounding Cable

When install in equipment room facility providing independent grounding, it is required to connect the chassis ground tab on DGW100 with the protective grounding system in this environment. Proper grounding not only provides a guarantee for safe operation of the equipment but also enhances the capacity of the equipment to resist disturbance and ensures the quality of voice communication.

The DGW100 series main chassis and expansion chassis are equipped with a M4 grounding screw with a mark in their backs. Please use the M4 screw to connect the grounding wire.

3.3.5 Connecting the Power Cord

Before connect the power cord, we suggest to use the 3-core power socket with neutral point connector or multi-function micro power socket, and make sure that the grounding point is proper grounded.

Note

Please contact the gateway supplier if the power LED does not light up after the power is turned on. Please contact with the Customer Service Center and never install and uninstall the gateway or plug and unplug any cable on the gateway when the power is turned on.

The steps to connect AC power cord is as following:

Step 1: Turn off the switch of AC power outlet.

Step 2: connect one end of the shipped power cord to the AC power inlet at rear of the chassis and plug another end of AC power cord into the 220V power supply outlet.

Follow the steps to connect DC power cord:

Step 1: Turn off the switch of DC power outlet.

Step 2: Insert DC power cords to the hole of the socket shipped with the DGW100 and fasten the cables (notice the positive and negative). Then insert the socket to the device and fasten it.

3.3.6 Verifying Installation

Installation verification is extremely important, because operations of the gateway depend on its stability, grounding, and power supply.

Each time you turn on the power during the installation, verify that:

- Enough clearance has been reserved around the ventilation openings of the gateway and the workbench/rack is stable enough.
- The protection ground is connected properly.
- Proper power supply which connect with power cord is used as specified.
- The gateway is correctly connected to console terminal and other devices.

4 Powering up the Gateway

4.1 Verification before Power-up

4.1.1 Checking Appearance

This is a review process of the installation work, including the chassis, wiring, connectors, ports, labels and site as described in the subsections.

Gateway

- Check whether there is adequate clearance around the gateway for thermal, and whether the workbench or rack for the mounting of the gateway is firm enough.
- Check whether the gateway is correctly connected to the configuration terminal and other devices.

Cable

- Check whether the Ethernet cable, the T1/E1 cables are connected properly.
- Check whether the grounding cable is connected properly.
- Check whether the power cord is connected to the proper power supply as required.

Port and Connector

- Check whether the ports and connectors are secured.

Equipment Room

- Check whether the temperature and humidity in the equipment room are within the proper range. The humidity should be kept at 10% to 90%(non-condensing) and the temperature should be kept at 0-4^{o}C.

4.1.2 Checking Power Supply

Check whether the power supply is in normal operation with a multimeter.

4.2 Powering up the Gateway

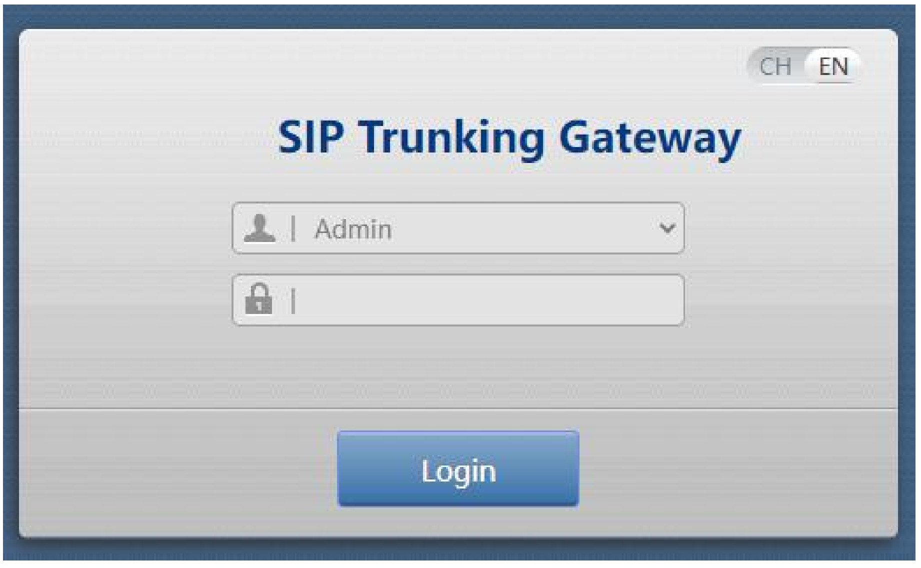
Turn on the power switch. Check whether the status of PWR LED is green, and if it is, then the gateway is powered properly.

5 Function Introduction

5.1 Login

Enter the gateway IP address in the browser address bar (For example, the default IP address 192.168.2.240), you can enter the login interface for gateway configuration by entering a password on the login interface.

Figure 5-1 Login Interface for DGW100 Gateway Configuration



Both Chinese and English Languages are provided for the Web interface.

Login users are classified into **administrator** and **operator**. The default passwords are **voip** (lowercase letters required) and **operator**. The password is shown in a cipher for safety.

- The administrator can browse and modify all configuration parameters, and modify login passwords.
- The operator can browse and modify part of configuration parameters.

The gateways allow multiple users to log in:

- The administrator has permission for modification and the operator only has permission for browsing;
- When multiple users with same level of permission log in, the first has permission for modification, while the others only have permission for browsing.

Note

- The system will confirm timeout if users do not conduct any operation within 10 minutes after login. They are required to log in again for continuing operations.
- Remember to change administrator password at your first login.
- The device is only allowed to access using HTTPS. For example, when using IE Explorer, since the factory default certificate is used a prompt like "There is a problem with this website's security certificate" may occur. Click Continue to this website to access the login page.

5.2 Buttons Used on Gateway Management Interface

Save buttons are at the bottom of the configuration screens. It is used to submit configuration information. Users click **Save** button after completion of parameter configuration on a page. A success prompt will appear if configuration information is accepted by the system; if a “The configuration takes effect after the system is restarted” dialog box appears, it means that the parameters are valid only after a system restart; you are adviced to click the **Reboot** button on the top right corner to enable the configuration after changing all parameters to be modified.

5.3 Basic Configuration

5.3.1 Network Configuration

Click **Basic** > **Network** to open the configuration interface.

Figure 5-2 Network Configuration Interface

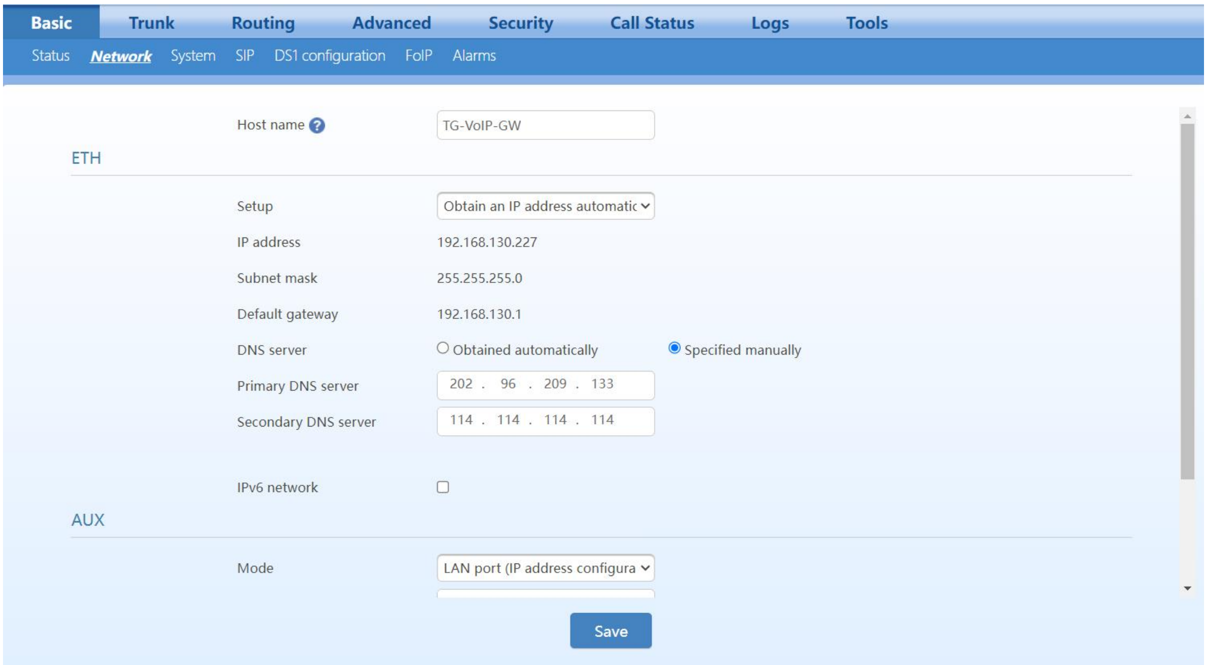


Table 5-1 Network Configuration Interface

Name	Description
Host name	This is the equipment name of a configuration gateway. The default value is TG-VoIP-GW. Users can set a different name for each gateway to distinguish from each other according to the deployment plan. A host name can be a maximum of 48 characters, either letters (A-Z or a-z), numbers (0-9) and minus sign (-). It may not be null or space and it must start with a letter.And minus sign(-) isn’t allowed to be used as ending.
ETH	
Setup	Methods for obtaining an IP address. ● Static IP address: static IP address is used; ● Obtain an IP address automatically: use the dynamic host configuration protocol (DHCP) to obtain IP addresses and other network parameters;

Name	Description
	● PPPoE: PPPoE service is used.
IP address	The IP address of the gateway. If "Static IP" is selected, this address can be specified manually. If the gateways obtain an IP address automatically, then this IP address cannot be specified manually, but when it was failed to obtain the IP address manually, the gateway will adopt the exist Static IP address.
Subnet mask	The subnet mask is used with an IP address. When the gateway uses a static IP address, this parameter must be entered; when an IP address is automatically obtained through DHCP, the system will display the subnet mask automatically obtained by DHCP.
Default gateway	The IP address of LAN gateway. When the gateway obtains an IP address through DHCP, the system will display the LAN gateway address automatically obtained through DHCP. It has no default value.
DNS server	Obtained automatically: When the connection mode is "DHCP" or "PPPoE", the device uses the automatically obtained IP address of the DNS server. This only can be selected when the network connection configuration is "Obtain IP address automatically" or "PPPoE". Specified manually: Use the DNS server addresses specified manually.
Primary DNS Server	If **Specified manually** is selected, the network IP address of the **Primary DNS server** must be entered.
Secondary DNS Server	If **Specified manually** is selected, the network IP address of the **Secondary DNS server** can be entered, and this is optional.
AUX	
Mode	● Switching port: AUX and ETH ports are switching ports. The two ports share the IP address of ETH port. This mode is the factory default. ● LAN port (with independent IP address): In this mode, you can configure an IP address for AUX port.
IP address	The IP address used by an AUX interface to access the network gateway, which must be in different network segment with the IP address of the ETH interface.
Netmask	The subnet mask is used with an IP address. When the gateways use a IP address of AUX, this parameter must be entered.

5.3.2 STUN (RFC3489)

Go to **Basic** > **Network**, and set to obtain the public IP address of the front-end router by using the STUN function.

Figure 5-3 STUN configuration interface

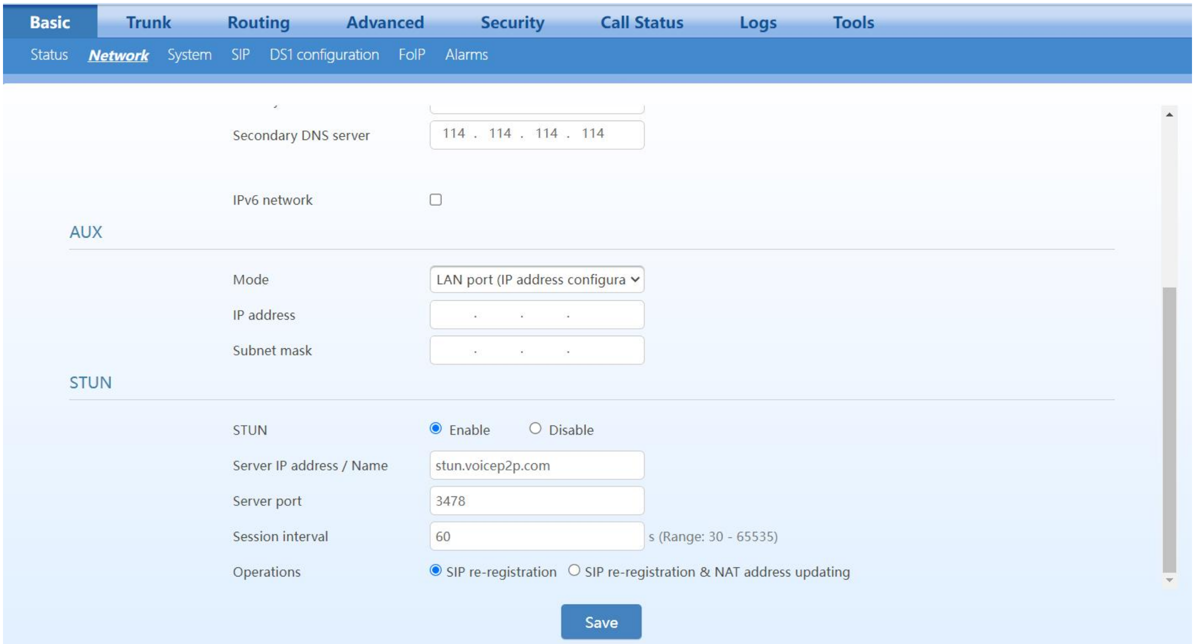


Table 5-2 STUN Parameters

Item	Description
STUN	After opened the STUN, the device periodically sends a STUN request to the STUN server to obtain the public IP address for the front-end router.
Server IP address / Name	Set the IP address or domain name of the STUN server. The default STUN server is the Redstone STUN server at stun.voicep2p.com
Server port	Set the port of STUN server. It is 3478 by default.
Session interval	The interval at which the device sends a STUN request ranges from 30 to 3600 seconds. It is 60 seconds by default.
Operations	● **SIP re-registration**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. Normally, the session interval of STUN request should be shorter than the registration period to discover the modification of external address of the router and re-registration timely. Note: The Via,CONTACT and SDP C field are still the address of the gateway itself and it won't be replaced with the public IP address in the STUN response message. ● **SIP re-registration & NAT address updating**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. And the IP address obtained through STUN is used in SIP message fields such as Via and Contact and SDP C field.

5.3.3 System Configuration

Click **Basic** > **System** tab to open the system configuration interface.

Figure 5-4 System Configuration Interface

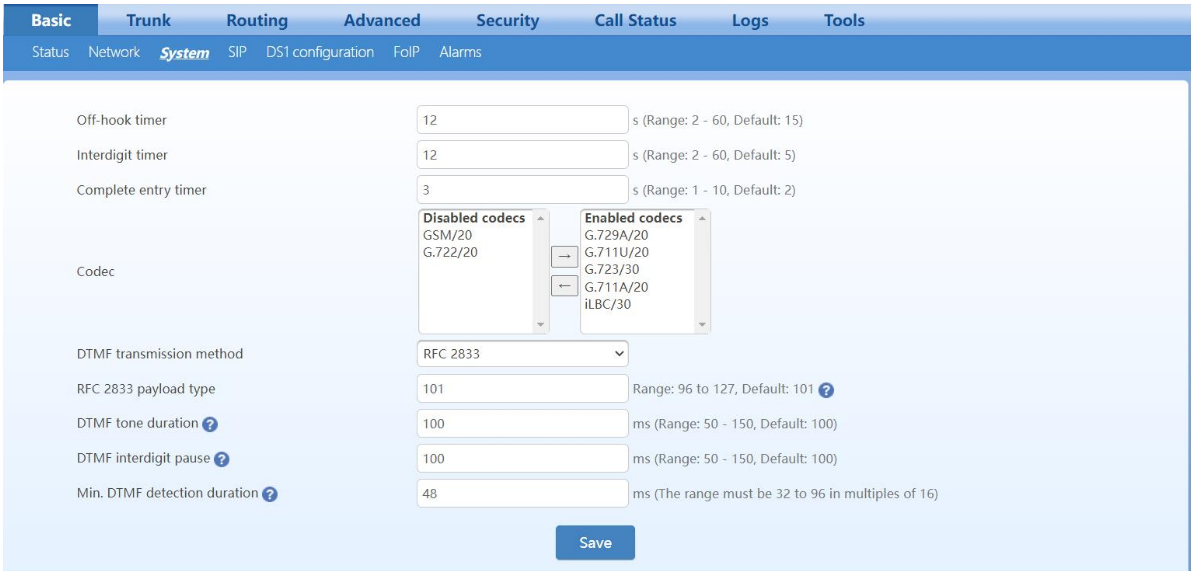


Table 5-2 System Configuration Parameters

Name	Description
Off-hook timer	If a subscriber does not dial any digit within the specified time by this parameter after off-hook, the gateway will consider the subscriber to give up this call and prompt to hang up with a busy tone. Unit: Seconds; Default value: 15 seconds.
Interdigit timer	The maximum time interval to dial the next digit. After timeout, the gateways will call out with the collected number. Unit: Seconds; Default value: 5 seconds.
Complete entry timer	Unit: Seconds; Default value: 2 seconds. This parameter is used with the "x.T" rule set in dialing rules. For example, there is "021.T" in the dialing rules table. When a subscriber has dialed 021 and has not dialed the next number within a set time by this parameter (e.g., 5 seconds), the gateways will consider that the subscriber has ended dial-up and call out the dialed number 021.
Codec	Codecs methods supported by the gateways include G729A/20, G723/30, PCMU/20, PCMA/20, iLBC/30 and GSM/20. Several encoding methods can configure in this item at the same time, separated with "," in the middle; the gateways will negotiate with the platform in the order from front to back when configuring the codec methods
DTMF transmission method	Transmission modes of DTMF signal supported by the gateways include RFC 2833, Audio and SIP INFO. The default value is Audio. ● Audio: DTMF signal is transmitted to the platform with sessions; ● SIP INFO: Separate DTMF signal from sessions and transmit it to the platform in the form of SIP INFO messages; ● RFC 2833 + SIP INFO: DTMF signal is transmitted simultaneously via RFC 2833 and SIP INFO.
RFC 2833 payload type	Used with **RFC 2833** in the DTMF transmission modes. The default value of 2833 payload type is 101. The effective range available: 96-127. This parameter should match the setting of the 2833 packet which supported by the far-end device (e.g. soft switch platform).
DTMF tone duration	This parameter sets the on time (in ms) of DTMF signal sent from FXO port. The default value is 100ms. Generally, the duration time should be set in the range of 80-150ms.
DTMF interdigit pause	This parameter sets the off time (ms) of DTMF signal sent from FXO port. The default value is 100ms. Generally, the interval time should be set in the range of 80-150ms.
Min. DTMF detection threshold	Minimum duration time of effective DTMF signal. Its effective range is 32-96ms and the default value is 48ms. The greater the value is set, the more stringent the detection is.

Table 5-3 Codec Methods Supported by Gateway

Codec Supported	Bit Rate (Kbit/s)	Time Intervals of RTP Package Sending (ms)
G729A	8	10/20/30/40
PCMU/PCMA	64	10/20/30/40
G723	5.3/6.3	30/60
iLBC	13.3/15.2	20/30
GSM	13	20

5.3.4 SIP Configuration

Click **Basic> SIP** tab to open the SIP configuration interface.

Figure 5-5 SIP Configuration Interace

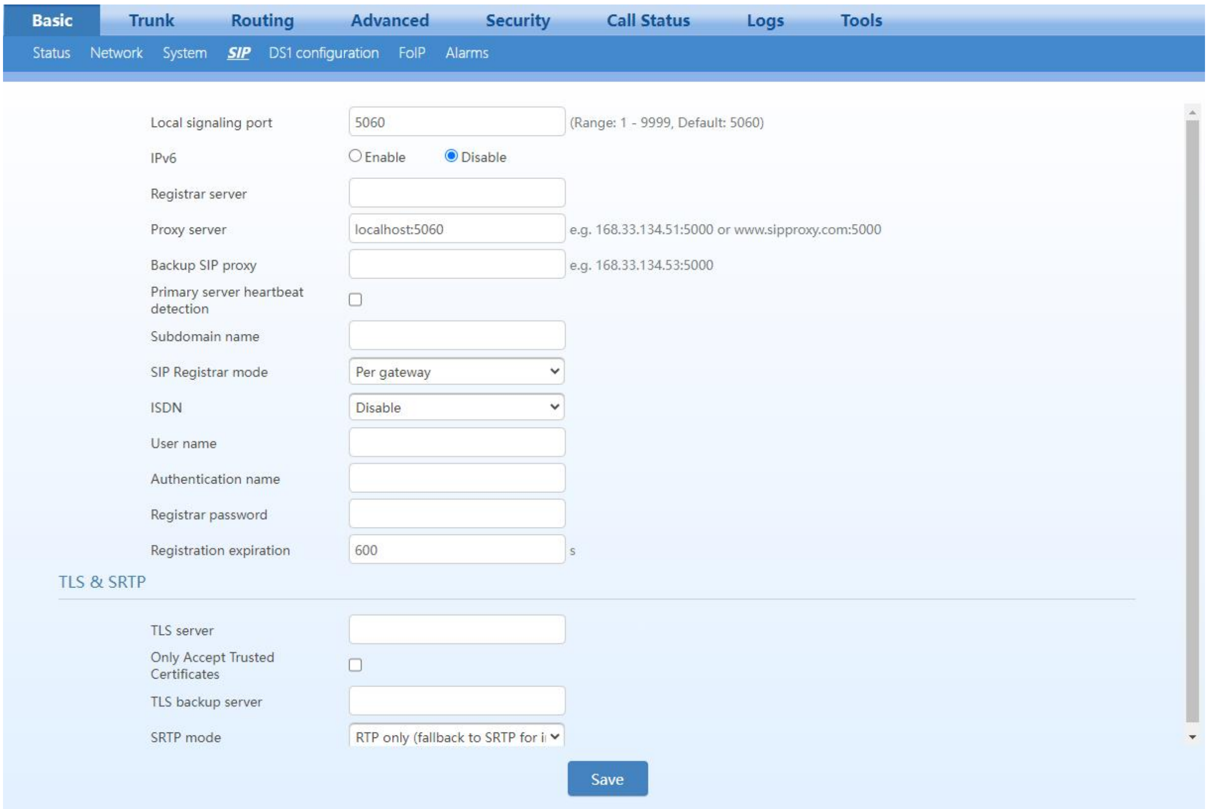


Table 5-4 SIP Configuration Parameters

Name	Description
Local signaling port	Configure the UDP port for transmitting and receiving SIP messages, with its default value 5060.If the DGW100 is connected directly to the Internet, it's recommended to change the default port value to prevent hacker attacks. Note: The signaling port number can be set in the range of 1-9999, but cannot conflict with the other port numbers used by the equipment.
IPv6	Enable or diable the IPv6 Function.
Register server	Configure the address and port number of SIP register server, and the address and port number are separated by ":". The register server address can be an IP address or a domain name. For example: 201.30.170.38:5060, register.com:5060. When a domain name is used, it is required to activate DNS service and configure DNS server parameters on the page of "Basic>Network".
Proxy server	Configure the IP address and port number of SIP proxy server, and the address and port number are separated by ":". The proxy server address can be set to an IP address or a domain name according to the requirement of the user. When a domain name is used, it is required to activate

Name	Description
	DNS service and configure DNS server parameters on the page of configuring network parameters. Examples of complete and effective configuration: 201.30.170.38:5060, softswitch.com:5060.
Backup SIP proxy server	Configure the IP address of backup SIP proxy server for disaster recovery.
Primary server heartbeat detection	Select the check box to enable and set the parameter OPTIONS request period, the device detects the condition of the proxy server (primary server) by periodically sends OPTIONS request to it. If the gateway does not receive the response from the primary server, then the connection to the primary server is broken, it will switchover to the backup proxy server. When the connection to the primary server recovered, then it will switch back to the primary server once the response to the OPTIONS request is received.
Subdomain name	This domain name will be used in INVITE messages. If it is not set here, the gateways will use the IP address or domain name of the proxy server as the user-agent domain name. Suggestion: Don’t set it to a LAN IP address.
Registrar mode	● **Per gateway**: authenticate and register per gateway. ● **Per SIP trunk**: authenticate and register per SIP trunk provided by IMS platform. After this mode is selected and saved, a page of **SIP Repeater** is available under **Basic** sub-menu for configuring SIP trunk details.
User name	Configure the user name as part of the account for registration.
Authentication name	Configure the user name as part of the account for authentication.
Registrar password	Password as part of account information is used for soft switch authentication. It can be digit or character and case-sensitive.
Registration expiration	Valid time of SIP re-registration in second. Its default value 3600.
TLS&SRTP	The device supports the ability to encrypt SIP protocol signaling by TLS to ensure the safety of Sip singalling. And it also supports SRTP to ensure the transmission of encrypted audio RTP data stream during the call.
TLS server	Set to the address of a softswitch or IMS platform that supports TLS. The TLS License can be uploaded on: Advanced>License.
Only accept trusted certificates	If selected, then the gateway will only accept the trusted TLS License.
TLS backup server	Set to the address of the TLS backup server for disaster recovery.
SRTP mode	Set to one of the following 6 negotiation modes: ● **Prefer RTP (negotiation with RTP only)**: RTP negotiation is used for outgoing calls, if the opposite device only supports SRTP, then can’t estabilish the calls. When incoming calls, if the opposite device supports RTP and SRTP, then use RTP first, if the opposite device only supports SRTP, then SRTP can be used as well. ● **Prefer SRTP (negotiation with SRTP only)**: SRTP negotiation is used for outgoing calls, if the opposite device only supports RTP, then can’t estabilish the calls. When incoming calls, if the opposite device supports RTP and SRTP, then use SRTP first, if the opposite device only supports RTP, then RTP can be used as well. ● **Prefer RTP (negotiation with both RTP and SRTP)**: both RTP and SRTP negotiations are supported for outgoing calls, RTP negotiation is preferred for incoming calls when the opposite device supports both RTP and SRTP, and if the opposite only supports SRTP, then SRTP can be used as well. ● **Prefer SRTP (negotiation with both RTP and SRTP)**: both RTP and SRTP negotiation are supported for outgoing calls, SRTP negotiation is preferred for incoming calls when the opposite device supports both RTP and SRTP, and if the opposite only supports RTP, then RTP can be used as well. ● **Disable**: Disable SRTP, support only RTP

Name	Description
	● **Mandatory**: SRTP

5.3.5 DS1 Configuration

In case of full configurations, the DGW100 has one 4T1/E1 card, with four interfaces numbering TDM1 to TDM4 from left to right. You are recommended to set parameters corresponding to the interface configured. Parameters for each interface are identical. You can set different parameter values for each interface as needed. For parameter setting, take the TDM1 as an example:

Click **Basic** > **DS1 configuration** to open the configuration interface.

Figure 5-6 DS1 Configuration Interface

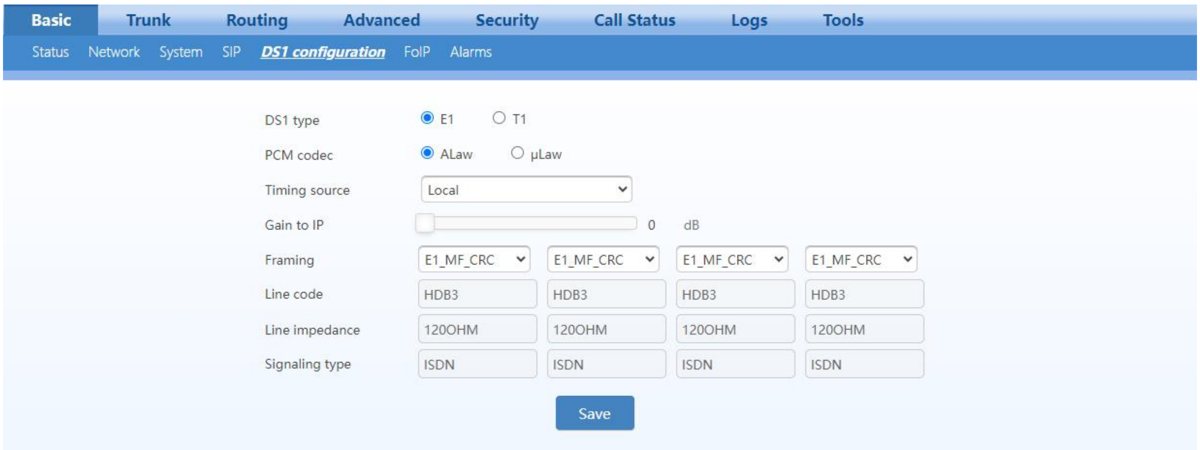


Table 5-5 DS1 Configuration Parameters

Name	Description
DS1 type	Select the type of interface (E1 or T1).
PCM codec	Allows configuring the PCM encoding type. It is ALaw for E1 by default and ULaw for T1 by default.
Timing source	Set the clock synchronization source. It is TDM1 by default. ● If the TDM1/2/3/4 is chosen, it indicates that the DGW100 synchronizes its clock with the opposite device connected to the first/second/third/forth TDM interface. ● If the Local is chosen, it indicates that the DGW100 synchronizes with the local device.
Gain to IP	You can increase the value of this parameter to increase the voice volume received from ISDN network and sent to IP network.
Framing	It is the framing of line type. It is E1_MF_CRC for E1 by default and ESF for T1 by default.
Line code	It is the code of line. It is HDB3 for E1 by default and B8ZS for T1 by default.
Line impedance	The configuration is displayed when E1 is chosen, with the value of 120OHM.
Line length	The configuration is displayed when T1 is chosen, with 0 dB and 7.5 dB for long line and 36.67 m for short line.
Signaling type	● ISDN ● T1 CAS ● NONE

5.3.6 FoIP

Click **Basic >FoIP** to open the configuration interface.

Figure 5-7 FoIP Configuration Interface

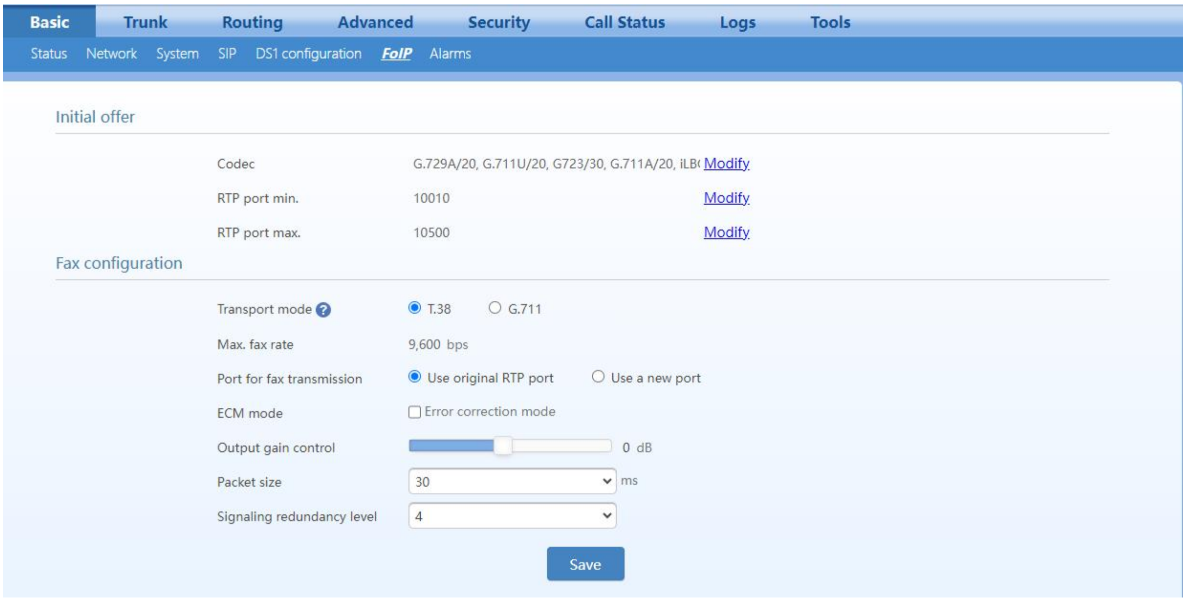


Table 5-6 FoIP Configuration Parameters

Name	Description
Initial offer	
Codec	Click **Edit**, go to **Basic**>**System** page to configure. For details, see 5.3.4 System Configuration. When transport mode is set to G.711 passthrough, make sure that **G.711U/20** or **G.711A/20** is selected in **Codec**.
RTP port Min.	Click **Edit**, go to **Advanced**>**Media stream** page to configure. For details, see 5.6.2 Media Stream.
RTP port Max.	Click **Edit**, go to **Advanced**>**Media stream** page to configure. For details, see 5.6.2 Media Stream.
Fax configuration	
Transport mode	The device supports two fax modes: T.38 and G.711 pass-through. When fax messages are received or sent through an analog trunk, the G.711 pass-through mode is required. When fax messages are received or sent through an SIP trunk, a T.38 or a G.711 pass-through mode needs to be selected according to an actual requirement and the mode supported by the IP phone operation platform. If both T.38 and G.711 pass-through modes are supported, T.38 is recommended because it is more stable.
Adjustable parameters when G.711 pass-through is enabled (default values are recommended):	
Allow opposite device to switch to T.38	When the device sends a fax message in G.711 pass-through mode, if the other party sends a T.38 negotiation request, the device will respond to the request and automatically switch to the T.38 mode.
Receiving terminal	● **Re-INVITE**: automatically select the codec according to the Re-INVITE negotiation result. ● **Pass-through**: To ensure normal operation of the pass-through function, make sure that

Name	Description
	G.711U/20 or **G.711A/20** is selected in **Codec**.
Adjustable parameters when the T.38 is enabled (Default values are recommended.)	
Max. fax rate	9,600bps is the maximum transmission rate of the fax service.
Port for fax transmission	Set whether to use a new RTP port when the gateway switches to the T.38 mode. The default value is **Use original RTP port**. We suggest to use the default configuration. ● **Use a new port:** Indicates that a new RTP port is used. ● **Use original RTP port:** Indicates that the original RTP port established during the call is used.
ECM mode	Enable the fax ECM mode. Disabled by default.
Output gain control	Set the increment and decrement of the T.38 fax transmission gain. The value ranges from –6 to +6 dB. The default value is 0 dB. –6 dB indicates an attenuation of 6 dB, and +6 dB indicates an amplification of 6 dB.
Packet size	Set a data frame packet interval for T.38. The options include 30ms and 40ms. The default value is 30ms.
Signaling redundancy level	Set the number of redundant data frames in T.38 data packets. The value range is 0–6 frames, and the default value is 4 frames.

5.4 Trunk

In case of full configurations, the DGW100 has one 4T1/E1 card, with four interfaces numbering Trunk 1 to Trunk 4 from left to right. You are recommended to set parameters corresponding to the interface configured. Parameters for each interface are identical. You can set different parameter values for each interface as needed.

For parameter setting, take the Trunk 1 as an example, use ISDN PRI signaling

Click **Trunk > Trunk 1** to open the configuration interface.

Figure 5-8 Trunk 1 Config uration Interface

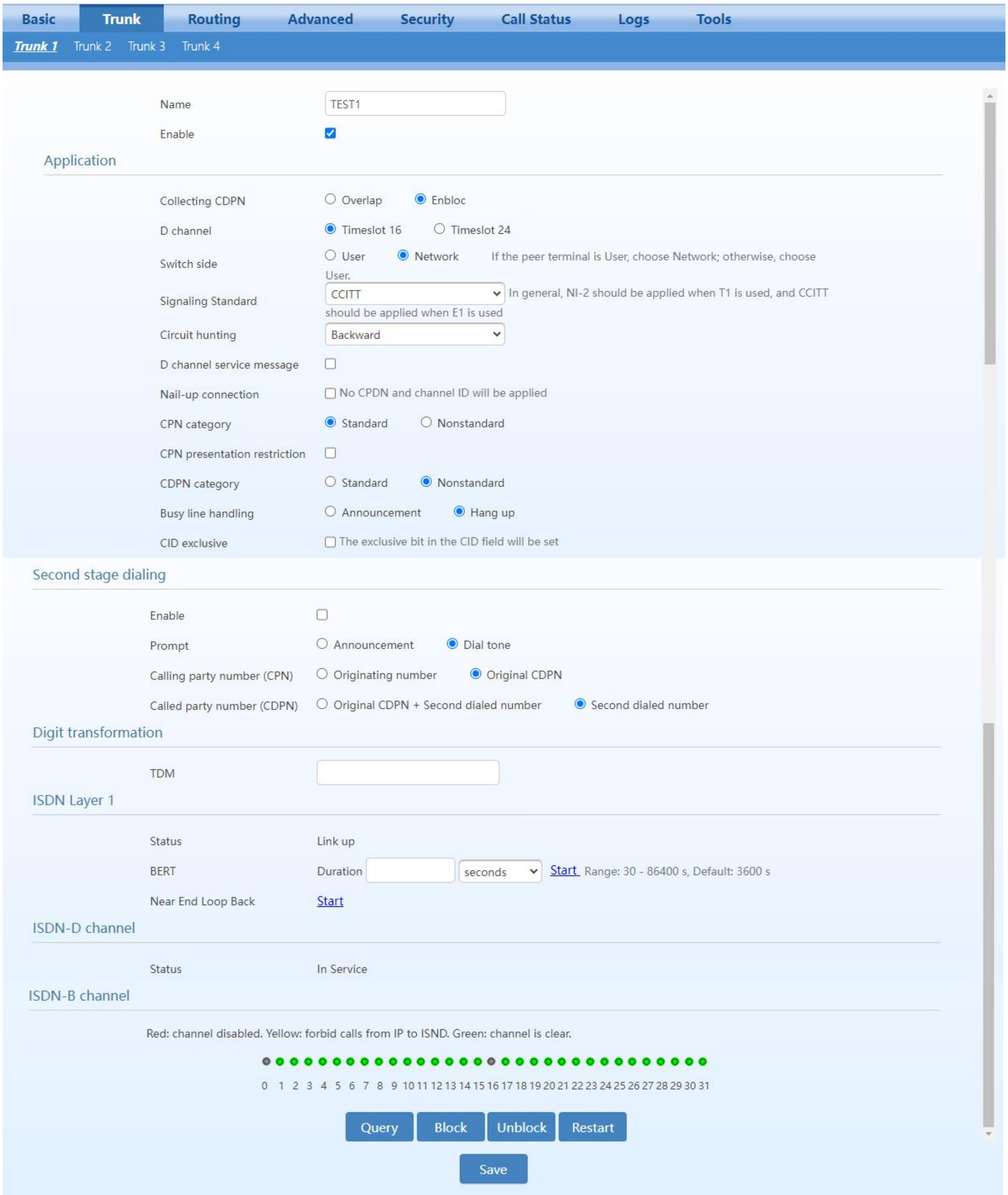


Table 5-7 Trunk 1 Configuration Parameters

Name	Description
Name	Display the name of a trunk interface.
Enable	Enable a trunk interface.
Application	
Collecting CDPN	Choose a collecting mode: Overlap or En-bloc.
D channel	A signaling channel. The default value is timeslot 16 for E1 services and timeslot 24 for T1 services.

Name	Description
Switch type	Set the interface protocol on the user side or network side. If the opposite device uses network side, the local terminal should choose user side.
Signaling Standard	The variation of ISDN PRI signaling standards: CCITT, NI-2, DMS100, DMS250 and 5ESS. You are recommended to select NI-2 for T1 card and CCITT for E1 card.
Circuit hunting	Search mode of idle timeslot: Forward, Backward and Cycle. Users can choose from the drop-down box. ● Forward: In the case of an incoming call, the DGW100 first checks whether timeslot 1 is idle. If not,then checks whether timeslot 2 is idle. The process proceeds in the ascending order until an idle timeslot is found. ● Backward: The DGW100 searches for an idle timeslot in the descending order. ● Cycle: The DGW100 searches for the next idle timeslot from left to right.
D channel service message	Setting for enabling the D channel service message.
Nail-up connection	Setting for enabling P2P connection (the called party number and channel ID are not required).
CPN category	Setting the Standard CPN calling party number category subfield. For the details, please refer to the ITU-T Q.931 protocol.
CPN presentation	Setting CPN calling party number presentation subfield. For the details, please refer to the ITU-T Q.931 protocol.
CDPN category	Setting the Standard CDPN called party number category subfield.
Busy line handing	The call processing mode for busy line is Announcement or Hang up.
CID exclusive	For the opposite device to change the line, choose Exclusive in CID.
Second stage dialing	
Enable	Enable the second dial tone and detect the DTMF number.
Prompt	Set the mode of second dial tone: Announcement or Dial tone.
Calling party number (CPN)	Set the display mode of calling party number: Originating number or Original CDPN.
Called party number (CDPN)	Set the display mode of called party number: Original CDPN + Second dialled number or Second dialled number.
Digit transformation	Number Transformation on each T1/E1 link. Rule format for number transformation on a single T1/E1 link: Operated number: Operation rule set/Operated number: Operation rule set For details about operated numbers and translation rules, see Table 5-11 Operated Numbers and Translation Rules.
ISDN Layer 1	
Status	Indicates whether the E1/T1 port is connected. “Link up” indicates connected, “Link down” indicates disconnected.
BERT	Set the duration, in the unit of seconds, minutes, hours, or days. After that, you can click Start to view the progress bar and the Stop button, as shown in the following figure. You can click Stop to cancel the testing process.
Near End Loop Back	Enable the loop back function for the remote device by clicking **Start**.

Name	Description
ISDN-D channel	Display the state of the ISDN-D channel: In service or Out of service.
ISDN-B channel	Displays the indicator state of a specific ISDN-B channel. ● If you click the channel in green, the indicator turns yellow and the call from IP to ISDN on the T1/E1 line is prohibited. The call from ISDN is not affected. ● If you click **Block** and choose a specific channel, the indicator of the chosen channel turns red. ● If you click **Unblock** and choose a blocked channel, the indicator of the chosen indicator turns green. ● If you click **Query** and choose a channel, the channel state is refreshed. ● If you click **Restart** and choose a channel, the choose channel restarts.

For parameter setting, take the Trunk 2 as an example, use T1 CAS signaling.

Figure 5-9 Trunk 2 Config uration Interface

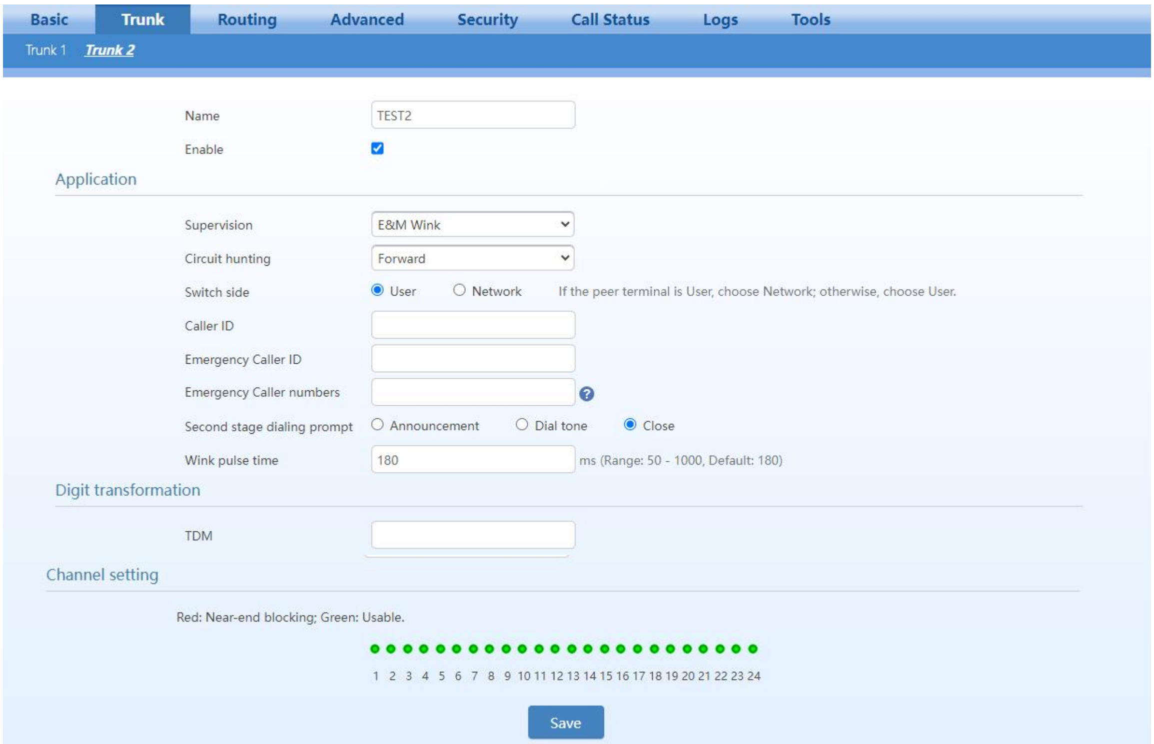


Table 5-8 Trunk 2 Configuration Parameters

Name	Description
Name	Display the name of a trunk interface.
Enable	Enable a trunk interface.
Application	
Supervision	● E&M Wink ● E&M Immediate
Circuit hunting	Search mode of idle timeslot: Forward, Backward and Cycle. Users can choose from the drop-down box. ● Forward: In the case of an incoming call, the DGW100 first checks whether timeslot

Name	Description
	1 is idle. If not,then checks whether timeslot 2 is idle. The process proceeds in the ascending order until an idle timeslot is found. ● Backward: The DGW100 searches for an idle timeslot in the descending order. ● Cycle: The DGW100 searches for the next idle timeslot from left to right.
Switch side	Set the interface protocol on the user side or network side. If the opposite device uses network side, the local terminal should choose user side.
Caller ID	Set a calling number from TDM to IP.
Emergency Caller ID	Set the calling number for emergency calls.
Emergency Caller numbers	Set emergency call numbers,you can fill in up to 20 numbers,separated by comma ",".
Second stage dialing prompt	Set the mode of second dial tone: Announcement、Dial tone or Close.
Wink pulse time	Wink pulse time is a specific duration of an electrical signal used in telecommunications to provide signaling and trigger system actions.
Digit transformation	Number Transformation on each T1/E1 link. Rule format for number transformation on a single T1/E1 link: Operated number: Operation rule set/Operated number: Operation rule set For details about operated numbers and translation rules, see Table 5-11 Operated Numbers and Translation Rules.
Channel setting	Displays the indicator state of a specific channel. ● If you click the channel in green, the indicator turns yellow and the call from IP to TDM on the T1 line is prohibited. The call from TDM is not affected. ● If you click **Unblock** and choose a blocked channel, the indicator of the chosen indicator turns green.

5.5 Routing

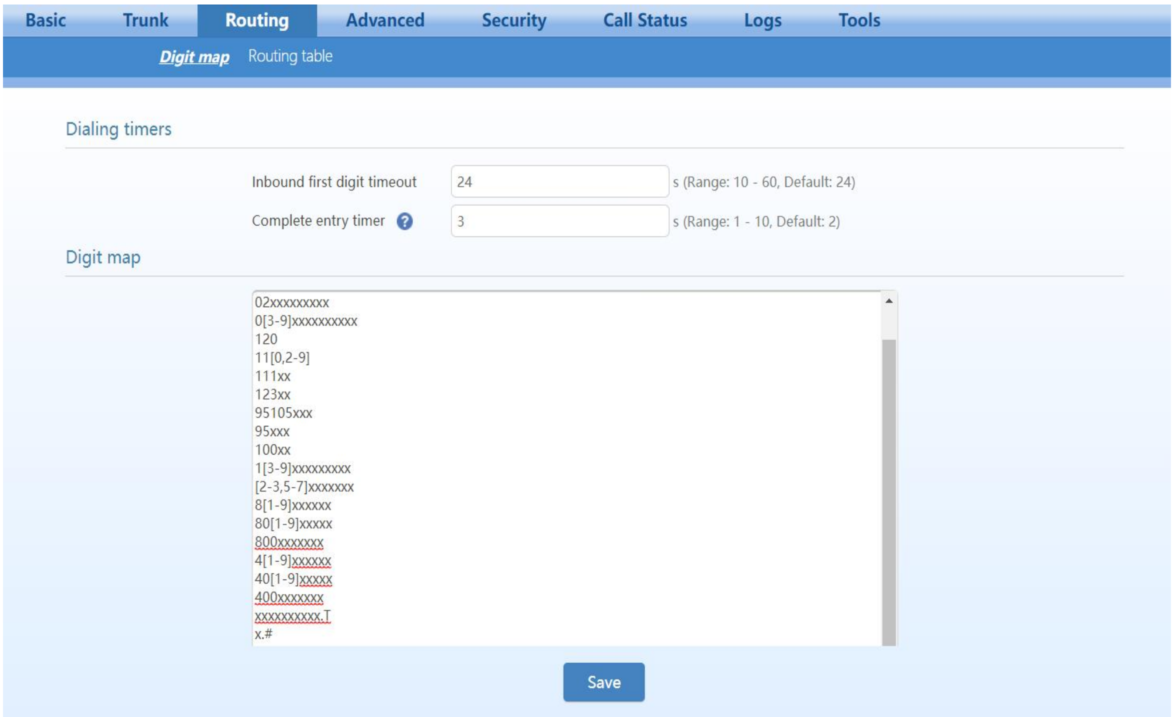
5.5.1 Digit Map

Note

In most situations, dialing rules need to be configured only for second dial on the DGW100.

Click **Routing> DigitMap** to open the digit map interface.

Figure 5-10 Configuration Interface for Dialing timers and Digit Map



Digit map rules are used to effectively judge if the received number sequence is completed, for the purpose of ending up receiving numbers and sending out the received numbers. The proper use of digit map rules can help to reduce the connection time of telephone calls.

The maximum number of rules that can be stored in gateways is 520. The total length of dialing rules table (the total length of all dialing rules) cannot be more than 3000 bytes.

The default digit map only contains system function rules,and the user needn't to modify it if there is no special application. To customize the digit map, please choose the country in **Advanced** >**Tones** and input the rules you want in the text box.

The following provides a description of typical rules:

Table 5-9 Description of Digit map

Name	Description
Dialing timers	
Inboud first digit timeout	Inbound first digit timeout is a feature in telephony systems that sets a time limit for the caller to enter the first digit of their input after a call is connected.
Complete entry timer	Used for x.T rule in digitmap.The device will make outgoing call with the collected digits you have dialed if no other digits are dialed within the specified number of seconds afterwards.
Digit map	
x	Represents any number between 0-9.
.	Represents more than one digit between 0-9.
xxxxxxxxxx.T	The gateway will detect the telephone number of any length which start by digit, and sends detected numbers if the duration of no dialing period exceeded the value of the Interdigit timer parameter and no new number has been received.
x.#	Any length of telephone number starting with any number between 0-9. If subscribers press # key after dial-up, the gateways will immediately end up receiving numbers and send all the numbers before # key.
[2-8]xxxxxx	The gateway terminates receiving digits after receiving 7 digits starting with a digit between 2 to 8.
02xxxxxxxxx	The gateway terminates receiving digits after receiving 11 digits starting with 02.

Name	Description
013xxxxxxxxx	The gateway terminates receiving digits after receiving 12 digits starting with 013.
13xxxxxxxxx	The gateway terminates receiving digits after receiving 11 digits starting with 13.
11x	The gateway terminates receiving digits after receiving three digits starting with 11.
9xxxx	The gateway terminates receiving digits after receiving five digits starting with 9.
17911 (e.g.)	Send away when the set number, e.g. 17911, is received. This example illustrates the mothod to end the specific number.

Dial rules by default as follows:

01[3-9] xxxxxxxxx

010xxxxxxxx

02xxxxxxxxx

0[3-9] xxxxxxxxxx

120

11[0, 2-9]

111xx

123xx

95105xxx

95xxx

100xx

1[3-9] xxxxxxxxx

[2-3, 5-7] xxxxxxx

8[1-9] xxxxxx

80[1-9] xxxxx

800xxxxxxx

4[1-9] xxxxxx

40[1-9] xxxxx

400xxxxxxx

xxxxxxxxxx.T

x.#

#xx

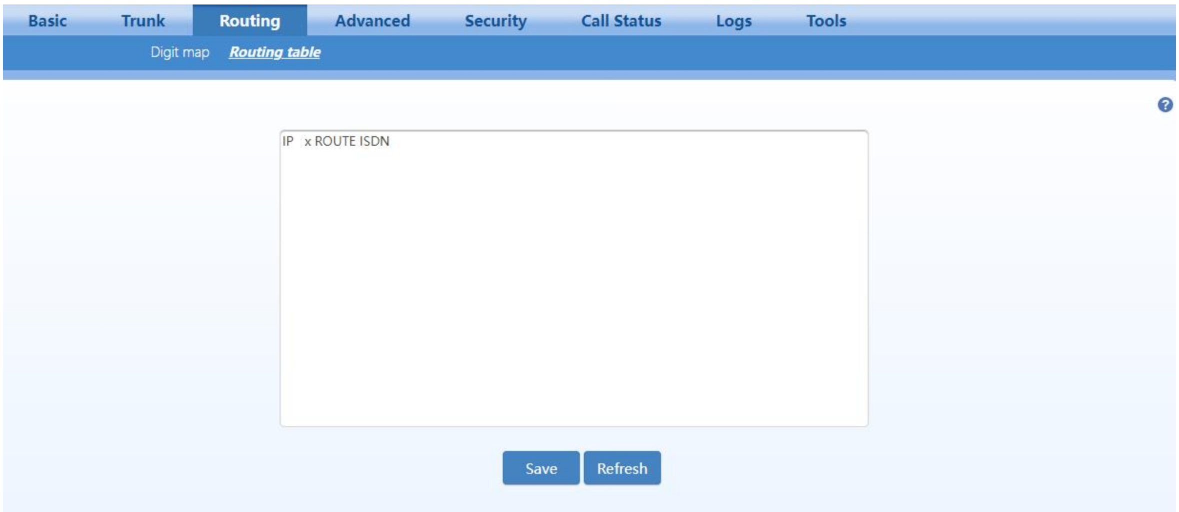
*xx

##

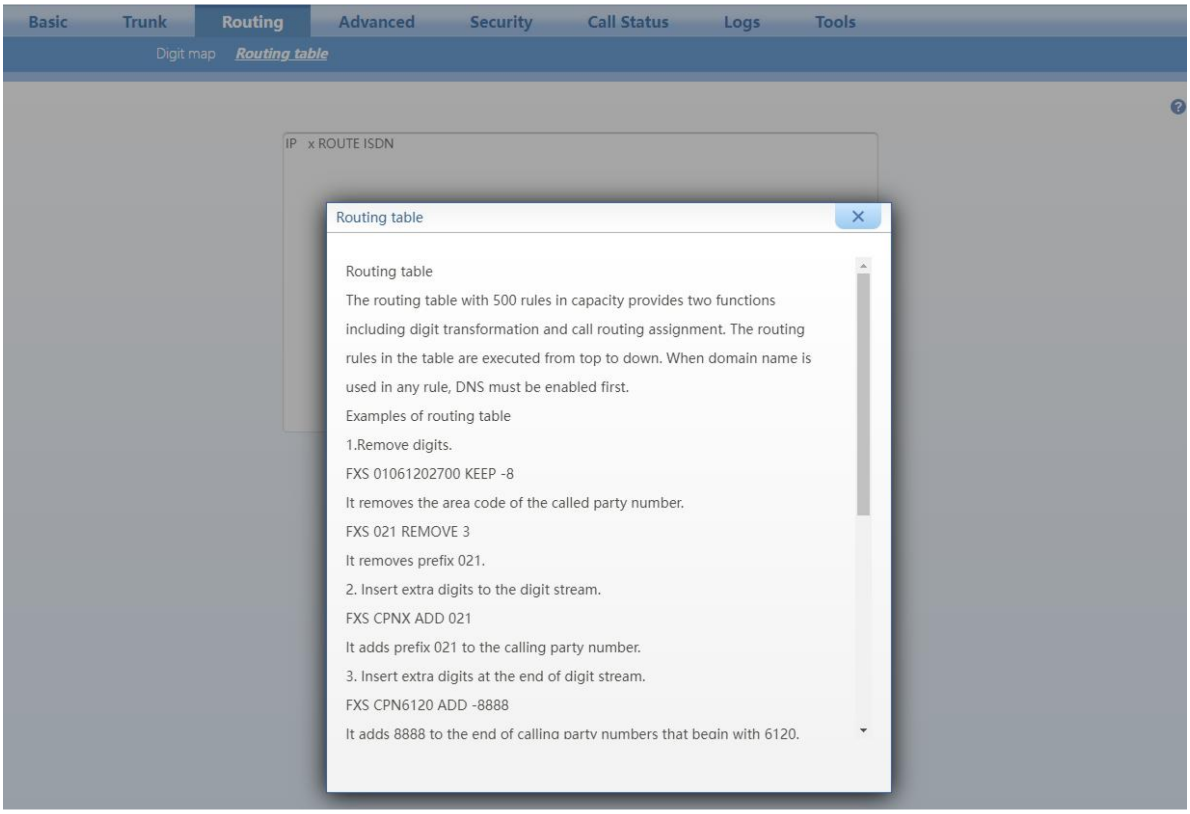
5.5.2 Routing Table

Click **Advaced > Routing Table** tab to open the configuration interface.

Figure 5-11 Configuration Interface for Routing Table



Click  to open the illustrative interface for routing configuration.



The routing table with 500 rules in capacity provides two functions including digit transformation and call routing assignment, and its capacity (sum of the number of replacing rule and routing rule) is 500.The applying sequence of the routing table is from up to down and the matching of digit shall comply with the rule of shortest priority.

Note

- Rules must be filled out without any blank at the beginning of each line; otherwise, the data can't be validated even if the system prompts successful submittal.
- The routing table is empty by default. The gateways will point a call to the SIP proxy server when there is no matched rule for the call.

The format of number replacement is

Source Number Replacement Method

For example: **FXS 021 REMOVE 3** means remove the prefix 021 of the called number for calls from the IP.

The format of routing rules is:

Source Number ROUTE Destination

For example:

IP 8621 ROUTE ISDN 1

IP 8621 ROUTE CAS 1

Indicates that the call with the called party number starting with 8621 is sent from the IP network to the first ISDN or CAS interface.

Detailed definitions of source and number, number replacement mode and routing destination type are shown below.

Table 5-10 Routing Table Format

Name	Description
Source	There are two source types: IP and ISDN. The IP source can be any of the following: ● Any IP address, represented by IP. ● A specified IP address, represented by IP[xxx.xxx.xxx.xxx]. ● A specified IP address and port number, represented by IP[xxx.xxx.xxx.xxx:port] (port specifies a source port number, such as 5060).
Number	It is a called number by default. And it also could be a calling party number with the form of CPN + number, such as CPN6034340633 or a called party number with the form of number. The number may be denoted with digit 0-9, "*",".","#","x", etc., and uses the same regular expression as that of dialing rules. Here are examples of the form of number: ● Designate a specific number: eg.114, 61202700 ● Designate a number matching a prefix: such as 61xxxxxx. Note: the matching effect of 61xxxxxx is different from that of 61x or 61. Number matching follows the principle of minimum priority matching ● Specify a number scope. For example, 268[0-1, 3-9] specifies any 4-digit number starting with 268 and followed by a digit between 0-1or 3-9 Note: Number matching follows the principle of minimum matching. For example: x matches any number with at least one digit; xx matches any number with at least two-digit; 12x matches any number with at least 3-digit starting with 12.

Table 5-11 Number Transformations

Processing Mode	Description and Example
KEEP	Keep number. The positive number behind KEEP means to keep several digits in front of the number; the negative number means to keep several digits at the end of the number. Example: IP 02161202700 KEEP -8 Keep the last 8 digits of the called number 02161202700 for calls from IP. The transformed called number is 61202700.
REMOVE	Remove number. The positive number behind REMOVE means to remove several digits in the front of the number; the negative number means to remove several digits at the end of the number. For example: IP 021 REMOVE 3

Processing Mode	Description and Example
	Any number start with 021, the 021 prefix is removed.
ADD	Add prefix or suffix to number. The positive number behind ADD is the prefix; the negative number is suffix. Example 1: IP CPN6120 ADD 021 CPN number start with 6120, prefix 021 is added. Example 2: IP CPN6120 ADD -8888 CPN number start with 6120, 8888 is appended.
REPLACE	Number replacement. The replaced number is behind REPLACE. Example: ISDN CPN88 REPLACE 2682000 CPN number started with 88, the prefix "88" is replaced with 2682000. Other use of REPLACE is to replace the specific number based on other number associated with the call. For example, replacing the calling party number according to the called party number. Examples: ISDN 12345 REPLACE CPN-1 Indicates that the tail digit is deleted from the caller number in correspondence with the called party number 12345 from ISDN. Note:Please refer to the Table 5-11 TDM Digit Transformation Rule if you want to replace the single ISDN line.
END or ROUTE	End of number transformation. From top to bottom, number transformation will be stopped when END or ROUTE is encountered; the gateways will route the call to the default routing after meeting END, or route the call to the designed routing after meeting ROUTE. Example 1: IP 12345 ADD -8001 IP 12345 REMOVE 4 IP 12345 END Indicates that the called party number from an IP network starting with 12345. The first order indicates it is suffixed with 8001, the second order indicates it removes 4 digits and the third order indicates it ends the previous operations. Example 2: IP[222.34.55.1] CPNX REPLACE 2680000 IP[222.34.55.1] CPNX HIDE IP[222.34.55.1] CPNX ROUTE ISDN 2 Indicates that any calling party number from the IP address 222.34.55.1 is replaced by 2680000. The calling party number is hidden and the call is sent to the second E1. Note: The hiding of the calling party number can be enabled only when the operator can provide the corresponding support as well.
CODEC	Designate the use of codec and followed by detailed codec mode, such as PCMU/20/16, where PCMU denotes G.711, /20 denotes RTP package interval of 20 milliseconds, and /16 denote echo cancellation with 16 milliseconds window. PCMU/20/0 should be used if echo cancellation is not required to activate. Example: IP 6120 CODEC PCMU/20/16 PCMU/20/16 codec will be applied to calls from IP with called party number starting with 6120, enable echo cancellation and the tail length is 16ms.
RELAY	Insert prefix of called party number when calling out. The inserted prefix number follows behind RELAY. Example: IP 010 RELAY 17909 For calls from IP with called party number starting with 010, digit stream 17909 will be outpulsed before the original called party number is being sending out.

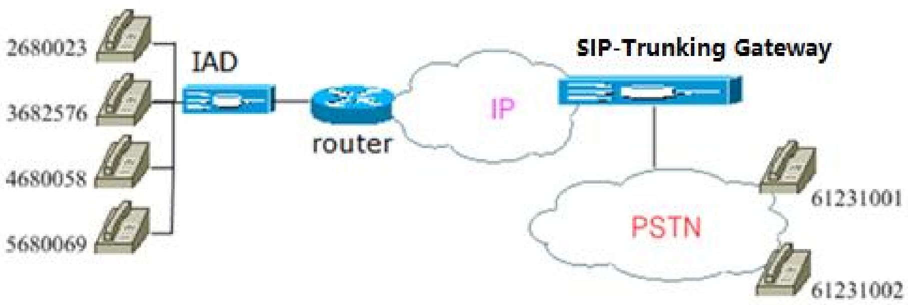
Processing Mode	Description and Example
SEND180	Force sends 180 on ring back Example: IP CPN2 SEND180 CPN number start with 2, always send 180 on ring back.
SEND183	Force sends 183 on ring back. Example: IP CPN3 SEND183 CPN number start with 3, always send 183 on ring back.
HIDE	Calling party number hide. Example: IP [61.2.44.53:5060] CPNX HIDE Hide any call number of any length from the port 5060 of the IP address 61.2.44.53:5060. Note: The hiding of the calling party number can be enabled only when the operator can provide the corresponding support as well.

Table 5-12 Routing Destination

Destination	Description and Example
ROUTE NONE	Calling barring. Example: IP CPN [1,3-5] ROUTE NONE Bar all calls from IP, of which the calling numbers start with 1, 3, 4, 5.
ROUTE ISDN	Route a call to ISDN. IP 8621 ROUTE ISDN 1 IP CPN8620 ROUTE ISDN 2 call has 8621 prefix , route to ISDN span 1 calling party number started with 8620, route to ISDN span 2
ROUTE IP	ISDN 021 ROUTE IP 228.167.22.34:5060 ISDN 020 ROUTE IP 61.234.67.89:5060 Indicates that the call from the PSTN, with the called party number starting with 021 will be sent to the platform with the IP address of 228.167.22.34; the call with the called party number starting with 020 will be sent to the platform with the IP address of 61.234.67.89.

5.5.3 Application Examples of Routing Table

Application requirements



- Selecting an E1 line based on calls from the IP network.
- Replacing the calling party number section of an IP call with a shared number.
- Permitting the IP call with the number only in the calling party number section, not other ID sections.
- Hiding the calling party number of an IP call by replacing the entire calling party number section with one digit number.

- Specifying a voice coding for a certain kind of clients.

Routing setting

IP CPNX REPLACE 18710095 (B)

IP CPN2 CODEC PCMU/20/64 (E)

IP CPNX HIDE (D)

IP [221.38.112.26] CPN2 ROUTE ISDN 3 (A)

IP CPN [1,4-5] ROUTE NONE (C)

- Calls from 2680023 to 61231001 are matched with configurations of (B), (E), (D), and (A). The calling party number 2680023 is replaced with 18710095, with the codec of pcmu/20/64. The calling party number is hidden and the call is sent to the third E1 line.
- Calls from 3682576 calls 61231002 are matched with configurations of (B) and (D). The calling party number 3682576 is replaced with 18710095 and is then hidden. Configurations (A), (E), and (C) are not matched.
- Calls from 4680058 and 5680069 to 61231001 are matched with the configuration (C), and calls are prohibited.

5.6 Advanced Configurations

5.6.1 System

Click **Advanced** > **System** to open this interface.

Figure 5-12 System Advanced Configuraiton Interface

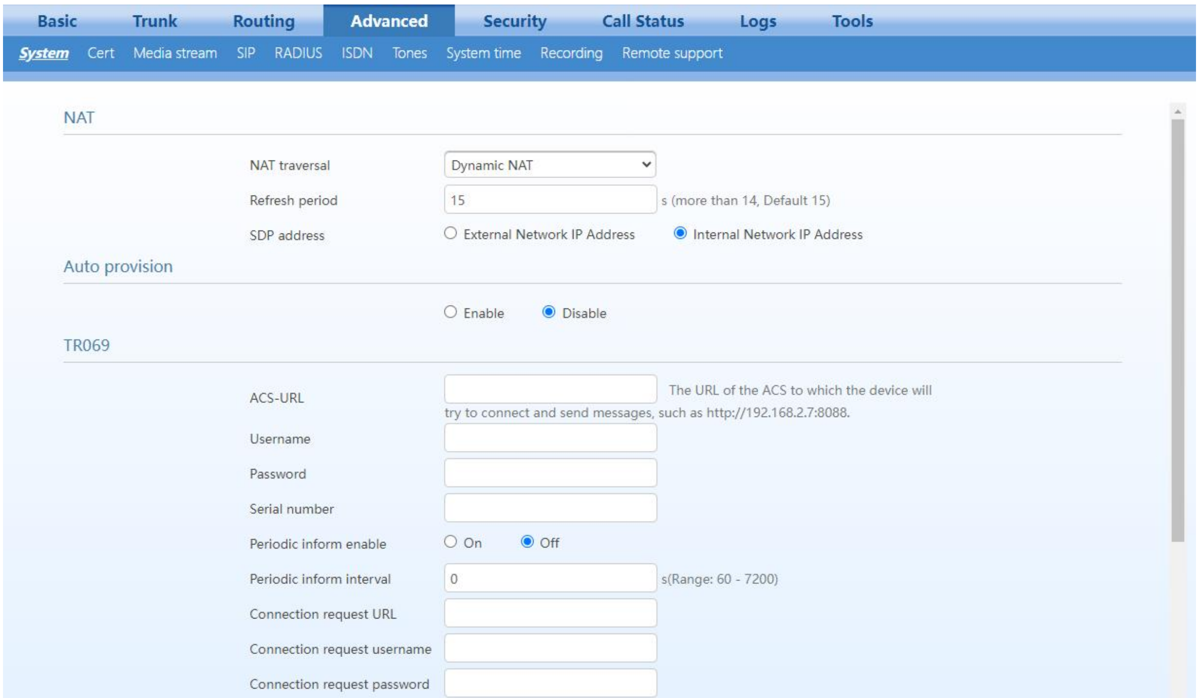


Table 5-13 Advaced System Configuration Parameters

Name	Description
NAT	

Name	Description
NAT traversal	Gateways support several mechanisms for NAT traversal,they are:Unable,Static NAT,Dynamic NAT. Usually, static NAT is used when fixed public IP address is available. It's necessary to perform port mapping or DMZ function on router when choosing dynamic or static NAT.
Refresh period	The refresh time must be filled in here when choosing dynamic NAT traversal. Besides, refresh time interval shall be determined by giving consideration into the NAT refresh time of the LAN router which the gateway is located. Gateway's NAT holding function will carry out periodically operation according to this parameter. With second as its unit, default value of 60 seconds.
SDP Address	This parameter determines the IP address used in transmitted SDP. ● NAT IP Address: Apply NAT address into the transmitted SDP; ● Local IP Address: Apply the gateway's IP address into the transmitted SDP. Note: The parameter should come into effect only on condition that gateway successfully obtained NAT address.
NAT IP address	This parameter must be filled when using static NAT traversal, in which IAD works under LAN and the WAN address is fixed. The related IP address segment in the signaling can be mapped as assigned NAT IP address by setup this parameter. This parameter can be set in IP address format or hostname format (note: DNS service should be activated when hostname format is used). There is no default value for this field. Note: if you don't know the NAT IP address of the network which gateway is located, then you can use the IP address query server on the internet.
Auto Provision	Note: For detailed configurations, refer to the RGW Gateway Auto Provisioning Configuration Manual: www.redstonesystems.com
Enable	Tick it to use the auto provisioning function to carry out the concentrated management for devices.
Obtain ACS address via DHCP option 66	ACS (Auto Provisioning Server) address is obtained by using DHCP option66.
ACS URL	Manually configure the ACS address, which can be the TFTP, FTP, HTTP or HTTPS server. ● *tftp://ACS address* ● *ftp:// ACS address* ● *http:// ACS address* ● https://ACS address
User name	Input a user name for accessing the ACS. Note: If the ACS is a TFTP server, the username and the password are not displayed.
Password	Input a password for accessing the ACS.
Firmware upgrade	Enable firmware download and update using ACS. Note: The firmware can be a **tar.gz** file or an **img** file.
Upgrade mode	The following modes are available. ● Power on: the gateway detects whether there are configurations and firmware to be updated when the device is powered on. ● Power on + Periodical: when the device is powered on, the gateway first checks whether there are configurations and firmware to be updated, and then periodically performs checking based on the set times.
Upgrade period	When **Power on+Periodical** is set, this parameter specifies the interval for periodic automatic upgrades. The default range is 3600 seconds. The value range is 5 to 84600 second.
TR069	
ACS-URL	Use TR069 to carry out concentrated management for devices, input the IP address of the remote management server here.
Username	Set the username used by the device to authenticate with the ACS.

Name	Description
Password	Set the password used by the device to authenticate with the ACS.
Serial number	Information of the device vendor, which may be used to indicate the primary service provider and other provisioning information to the ACS. It can be numbers or English letters.
Periodic inform enable	A switch used to specify whether to periodically report to the ACS.
Periodic inform interval	The interval for reporting to the ACS.
Connection request URL	The address used for the ACS to connect back to the device.
Connection request username	The account used for the ACS to connect back to the device.
Connection request password	The password used for the network management server to connect back to the device.
RTP Traverse	
Enable	Select to enable the RTP traverse function.

5.6.2 Media Stream

Click the label of **Advanced > Media Stream** to open this interface.

Figure 5-13 Media Stream Configuration Interface

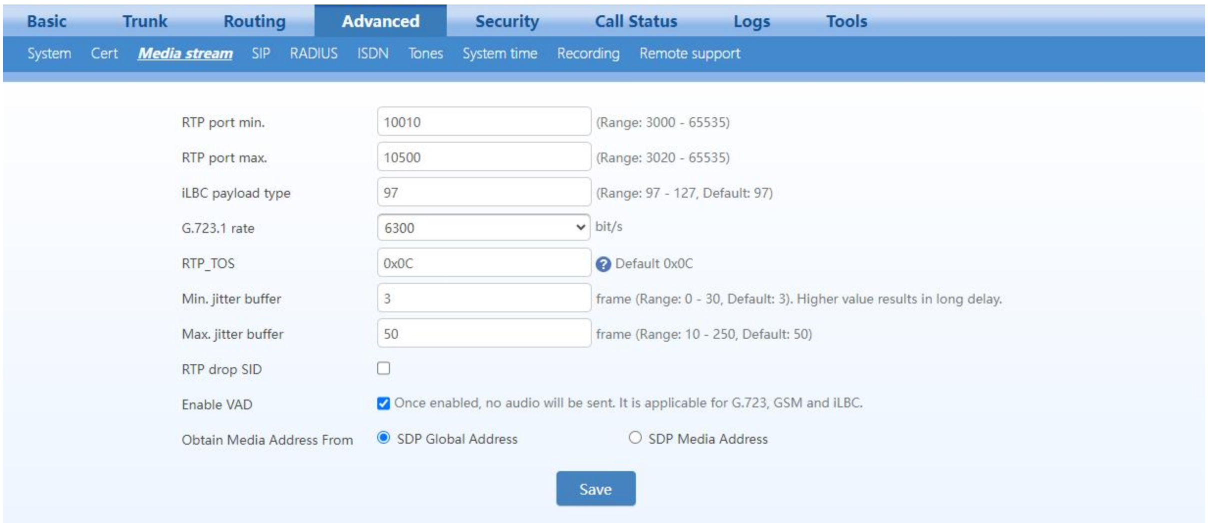


Table 5-14 Media Stream Configuration Parameters

Name	Description
RTP port Min.	The minimum value of UDP ports for RTP transmission and receiving, and the parameter must be greater than or equal to 3000. The value is recommended to be equal or greater than 10000. Note: each phone call will occupy RTP and RTCP ports.
RTP port Max.	The maximum values of UDP ports for RTP's transmission and receiving. It's advisable to be greater than or equal to "2×number of lines+min. RTP port".
iLBC payload type	Set the RTP payload type of iLBC, and the default value is 97. Accepted value is 97-127. The parameter shall be configured in conformity to that of platform.
G.723.1 rate	Set G.723.1 coding rate, the default value is 6300(Byte/s). The optional parameters are followings: ● 5300(Byte/s): The Bit rate is 5.3k per second; ● 6300(Byte/s): The Bit rate is 6.3k per second.

Name	Description
RTP_TOS	This parameter specifies the quality assurance of services with different priorities. The factory setting is 0x0C. For example, TOS=0xB8 indicates that the priority of the service quality is 5, with a requirement on low delay and high throughput. There is no requirement on the reliability.
Min. Jitter buffer	RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This default value is 3.
Max. Jitter buffer	RTP Jitter Buffer helps to reduce the influence brought by network transmitting jitter. The default value is 50.
RTP drop SID	Determine whether to discard received RTP SID voice packets. By default, SID voice packets will not be dropped. Note: RTP SID packets should be dropped only when they are in unconformity to the specifications. Nonstandard RTP SID data with different data length could generate noise for calls.
Enable VAD	Only applicable to G.723, GSM, iLBC. In case of selecting this parameter, it will not send any voice packet during mute period. By default, this is selected,it is recommended to select this parameter to save the network bandwidth.
RTP destination address	This parameter determines where to obtain the IP address of the receiving side for RTP packets. By default, the IP address is obtained “From SDP global connection”. ● From SDP global connection address(default): Obtain the IP address from SDP global connection; ● From SDP media connection: Obtain the IP address from the Connection Information behind the SDP Media Description.

5.6.3 SIP Configuration

Click the label of **Advanced > SIP** to open this interface.

Figure 5-14 SIP Related Configuration Interface

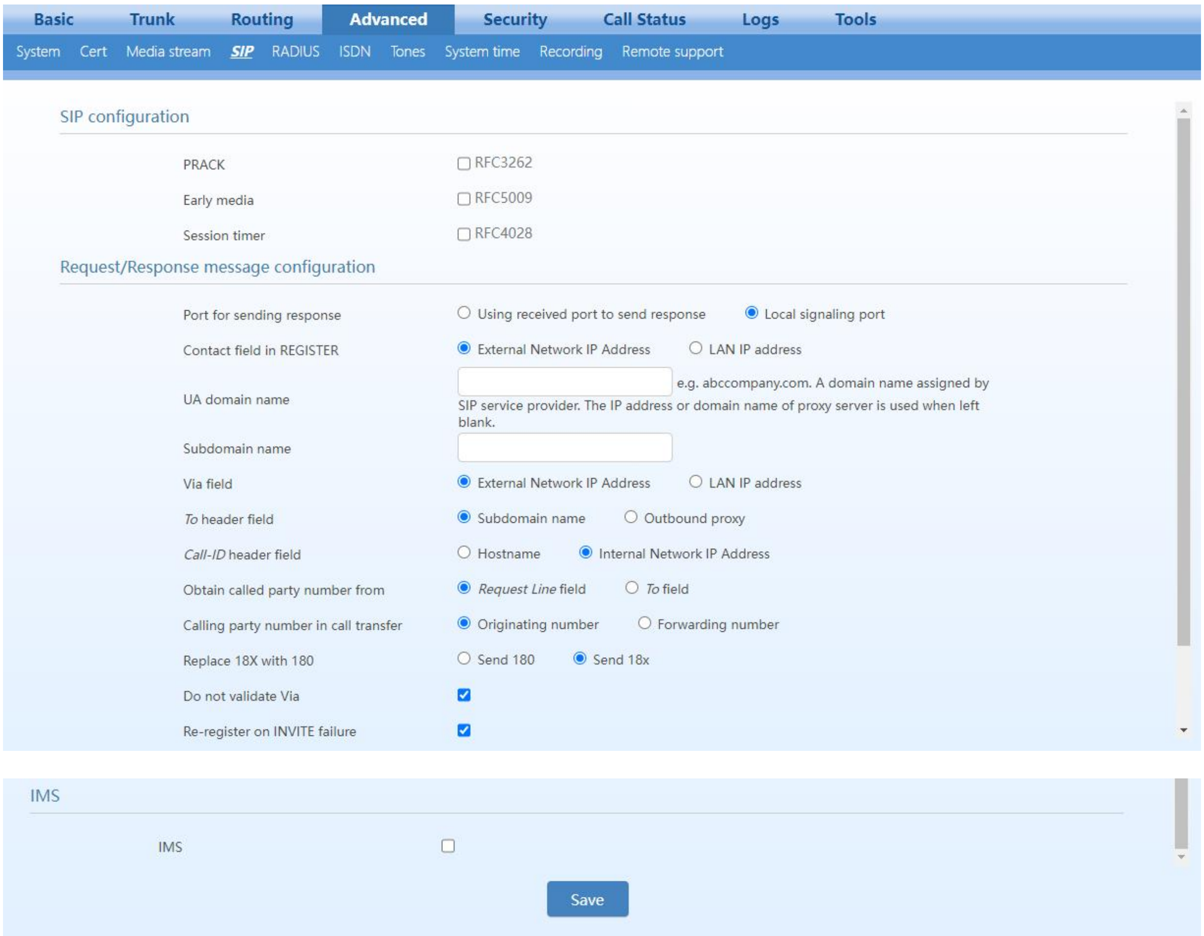


Table 5-15 SIP Related Configuration Parameters

Name	Description
SIP configuration	
PRACK	Determine whether to activate RFC 3262 and PRACK.
Early media	Enable RFC5009. It is not enabled by default.
Session timer	Choose to activate session refresh (Session Timer, RFC 4028). By default, session timer is not activated.
Session interval	Set the session refresh interval(period), the gateway will enclose the value of Session-Expires into INVITE or UPDATE messages. Default value is 1800 in second.
Minimum timer	Set the minimum value of session refresh interval.
Request/Response message Configuration	
Port for sending response	Select the port for sending SIP signaling responses: ● Using received port to send response ● Using 5060
Contact field in REGISTER	Choose the registration mode of gateway under LAN traversal circumstance, the default is **NAT IP Address**. ● LAN IP address: Keep original content of **Contact** when register; ● NAT IP address: Use the NAT information returned by registration server.
Domain name in REGISTER	This **Domain name is provided by SIP Operator and it uses proxy server address or domain name when it hasn't been configured**. ● Subdomain name: Only use the common part of the name of domain (for example: 8801@redstonesystems.com).

Name	Description
Via field	Choose whether to use NAT IP address or LAN IP address for "Via" header field value, the default is **LAN address**.
To header field	Choose whether to apply Domain name or Outbound proxy to "To" header field, the default is **Client Terminal Domain name**.
Call-ID header field	Choose whether to fill Call ID field with host name or local IP, the default is **local IP address**.
Obtain called party number from	Choose whether the gateway acquires the called number from **Request Line header field** or **To header field**. The default is **from Request Line**.
Calling party number in call transfer	Choose the type of the calling number while calling transfer from **Originating number** or **Forwading number** for calling sending. The default is from **Forwarding number**. For example: the subscriber line 2551111 on the gateway activates call forwarding feature and set the destination to 3224422. When caller with 13055553333 calls 2551111, the call will be forwarded to 3224422: ● If choose **Originating number**, the number 13055553333 will be sent to 3224422 as calling party number. ● If choose **Forwarding number**, the number 2551111 will be sent to 3224422 as calling party number.
Replace 18X with 180	While the gateway shall send 18x message, then setup whether use 180 message to substitute 18x message. The default value is **sends 18x message**. ● Send 180: It still sends the 180 message while the gateway shall send 18x message. ● Send 18x: If this parameter is set to enable, the 18x message will be sent.
Do not validate Via	Set whether to ignore Via field. By default, Via is ignored.
Re-register on INVITE failure	Set whether to activate registration when SIP message of INVITE is failed or time expired, and by default, re-registration is not selected.
IMS	
IMS	Enable interworking with IMS.
Obtain caller ID info from	While receiving two header domains with **From** and **P-Asserted-Id,** you can select the method of obtain the caller IP by this configuration. It obtains the Caller ID in the **From** if the **INVITE** without **P-Asserted-Id**. ● It is recommended to obtain from **P-Asserted-Id:** You can set to get the Caller ID from P-Asserted-Identity segment in the **INVITE message**. ● Obtain from **From** domain: You can set to get the Caller ID from the From segment in the **INVITE message.**
Access network info	The IP address and port number of the access network. For example: 192.168.100.200:5060. It is optional, input only when the IMS service provider requires.

5.6.4 RADIUS

Click the label of **Advanced > RADIUS** to open this interface.

Figure 5-15 RADIUS Configuration Interface

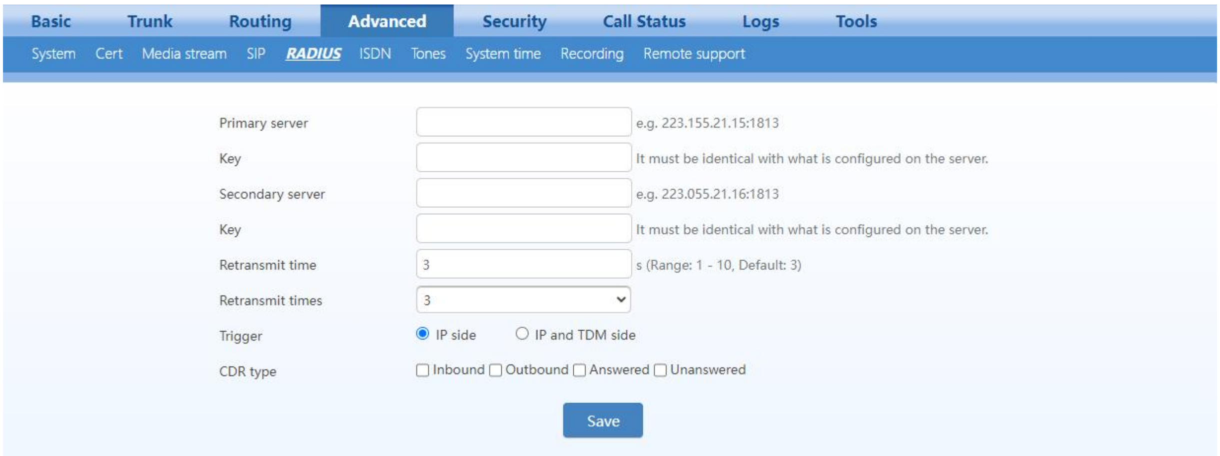


Table 5-16 RADIUS Configuration Parameter

Name	Description
Primary server	Set IP address and port number of preferred Radius server. Note: if the port number is not configured yet, please use Radius default port number of 1813.
Key	Set the share key to be used for encrypted communications between Radius client and server. Note: the share key should be configured the same for both client and server side
Secondary server	Set the IP address and port number of standby Radius server. When the fault appears in communications between gateway and preferred Radius server, the gateway will automatically activate standby RADIUS server. Note: in case of no configuration of port number, use default port number of 1813.
Key	The share key for communications between Radius client and standby Radius server. Note: the key should be configured the same for both client and server side
Retransmit timer	Set the amount of overtime on response after transmission of Radius message, the default is 3 seconds. The retransmission will be performed to ensure correct charging if no response is given after the timeout.
Retransmit times	Set the times of retransmission of Radius message when no response is received default is 3 times.
Trigger	● IP side: when this is selected the call information on the SIP side will be sent to the Radius server. ● IP and TDM side: when this selected the call information on the SIP side as well as on the ISDN side will be sent to the Radius server.
CDR type	● Outbound: Set whether to send RADIUS charge message for outbound calls; ● Inbound: Set whether to send RADIUS charge message for inbound calls; ● Answered: Set whether to send RADIUS charge message when calls are connected (i.e. when the calls are connected, the gateway sends the record information of calls answered to the RADIUS Server); ● Unanswered: Set whether to send RADIUS charge message for unanswered calls (i.e. when the calls aren't connected, the gateway sends the record information of calls unanswered to the RADIUS Server).

5.6.5 ISDN

Click the label of **Advanced** > **ISDN** to open this interface.

Figure 5-16 ISDN Configuration Interface

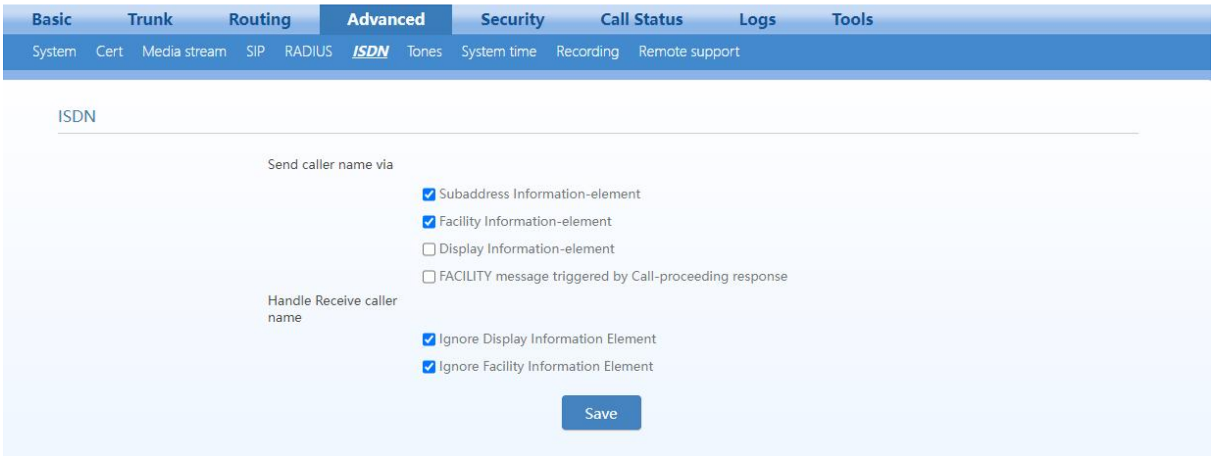


Table 5-17 ISDN Configuration Parameters

Name	Description
Send caller name via	● Subaddress Information-element ● Facility Information-element ● Display Information-element ● FACILITY message triggered by Call-proceeding response
Handle Receive caller name	● Ignore Display Information Element ● Ignore Facility Information Element

5.6.6 Tones

Click the label of **Advanced** > **Tones** to open this interface.

Figure 5-17 Tones Configuration Interface

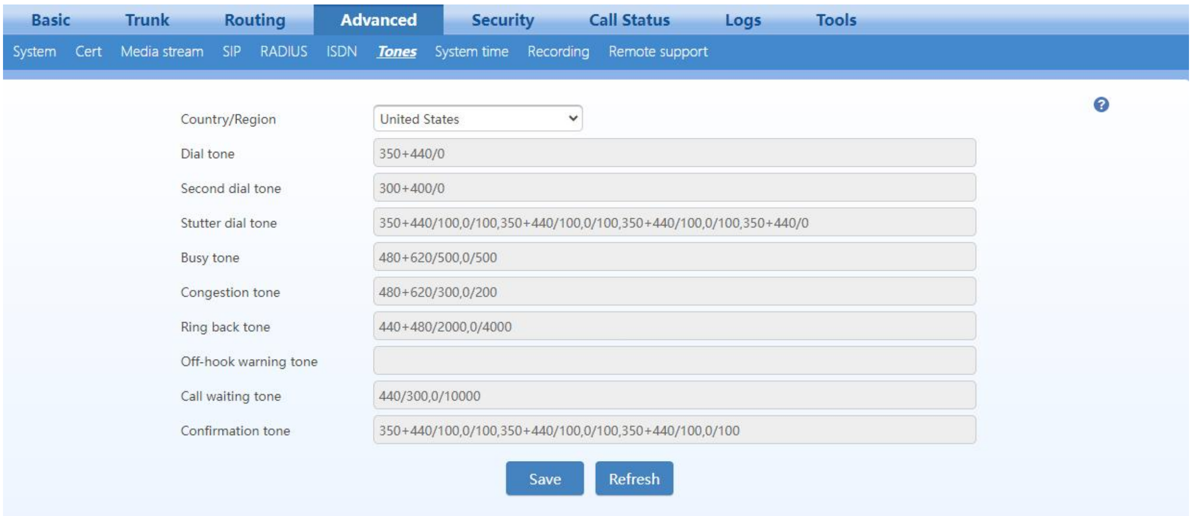


Table 5-18 Tones Configuration Parameters

Name	Description
Country/region	Users may also specify the call-progress tone standard which adopted by the gateway, its default value is China. Gateways provide calling tone standard for the following countries and regions: China, the United States, Singapore, Israel, Malaysia, Indonesia, United Arab Emirates, Australia,

Name	Description
	Zimbabwe, France, Italy, Germany, Mexico, Chile, Russia, Japan, South Korea, Hong Kong, Taiwan, India, Sudan, Iran, Algeria, Pakistan, Philippines, Kazakhstan. Self-defined by users: Users can define the following signal tone parameters.
Dial tone	Prompt tone of off-hook dialup.
Second dial tone	Second stage dial tone.
Stutter dial tone	Prompt of voice mail, or when the subscriber line is set with “Do not Disturb Service and Call Transfer”.
Busy tone	Busy line prompt.
Congestion tone	Notification of call set up failure due to resource limit.
Ring back tone	The tone sent to caller when ringing is on.
Off-hook warning tone	Reminds the subscriber when the phone is off-hook and no dialup has occurred.
Call waiting tone	Prompt the subscriber that another caller is attempting to call.
Confirmation tone	Confirms function codes are being entered.

Here are examples that illustrate the various call-progress tones

- 350+440 (dial tone)

  Indicates the dual–frequency tone consisting of 350 and 440 Hz

- 480+620/500,0/500 (busy)

  Indicates the dual–frequency tone consisting of 480 and 620 Hz, repeated playing with 500 ms on and 500 milliseconds off.

  Note: 0/500 indicates 500ms mute.

- 440/300,0/10000,440/300,0/10000

  Indicates 440 Hz single frequency tone, repeated twice in terms of 300ms on and 10 seconds off.

- 950/333,1400/333,1800/333,0/1000

  Indicates repeated playing 333ms of 950 Hz, 333ms of 1400 Hz, 333ms of 1800 Hz, and mute of 1 second.

5.6.7 System time

After login, click **Advanced** > **System time** to open this interface.

Figure 5-18 Clock Service Interface

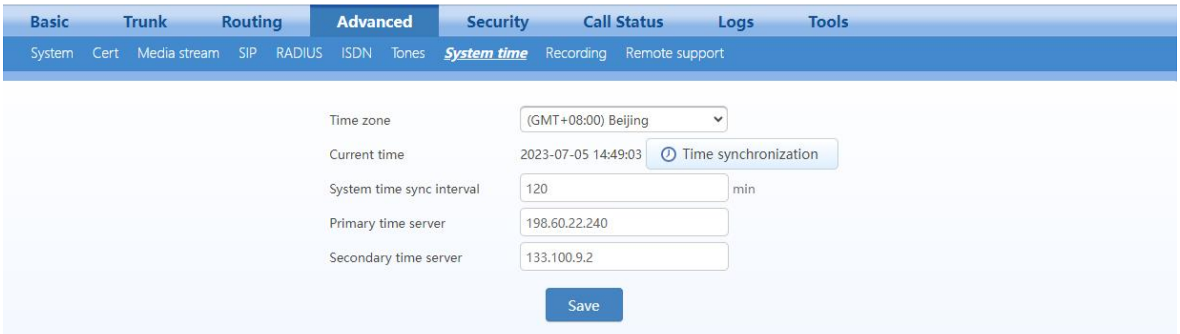


Table 5-19 Clock Service Parameters

Name	Description
Time Zone	Select a time zone, the parameter values include: • (GMT-11:00) Midway Island • (GMT-10:00) Honolulu. Hawaii • (GMT-09:00) Anchorage, Alaska • (GMT-08:00) Tijuana • (GMT-06:00) Denver • (GMT-06:00) Mexico City • (GMT-05:00) Indianapolis • (GMT-04:00) Glace_Bay • (GMT-04:00) South Georgia • (GMT-03:30) Newfoundland • (GMT-03:00) Buenos Aires • (GMT-02:00) Cape_Verde • (GMT) London • (GMT+01:00) Amsterdam • (GMT+02:00) Cairo • (GMT+02:00) Israel • (GMT+02:00) Zimbabwe • (GMT+03:00) Moscow • (GMT+03:30) Teheran • (GMT+04:00) Muscat • (GMT+04:00) United Arab Emirates • (GMT+04:30) Kabul • (GMT+05:30) Calcutta • (GMT+05:00) Karachi • (GMT+06:00) Almaty • (GMT+07:00) Bangkok • (GMT+07:00) Indonesia • (GMT+08:00) Beijing • (GMT+08:00) Taipei • (GMT+08:00) Singapore • (GMT+08:00) Malaysia • (GMT+09:00) Tokyo • (GMT+10:00) Canberra • (GMT+10:00) Adelaide • (GMT+11:00) Magadan • (GMT+12:00) Auckland
Current time	Display current time for the device. Click **Clock calibration** to calibrate the time.
System time sync interval	Set the synchronization period of the time. It is 120 minutes by default.
Primary time server	Enter the IP address of preferred time server here. It has no default value.

Name	Description
Secondary time server	Enter the IP address of Secondary time server here. It has no default value.

5.7 Security

5.7.1 Access Security

The administrator is recommended to perform the following operations to prevent mostly illegal accessing to the device:

- Regularly change the admin/operator password and improve the password strength for accessing Web GUI;
- Regularly change the root/operator password for accessing the device through Telnet/SSH, and improve the password strength;
- Regularly change the HTTP/HTTPS/Telnet/SSH port for accessing the device;
- Disable Telnet/SSH once accessing is completed.

All of the above are available on **Security**>**Access** page and this can facilitate the regular modification of the admin.

Figure 5-19 Access Configuration Interface

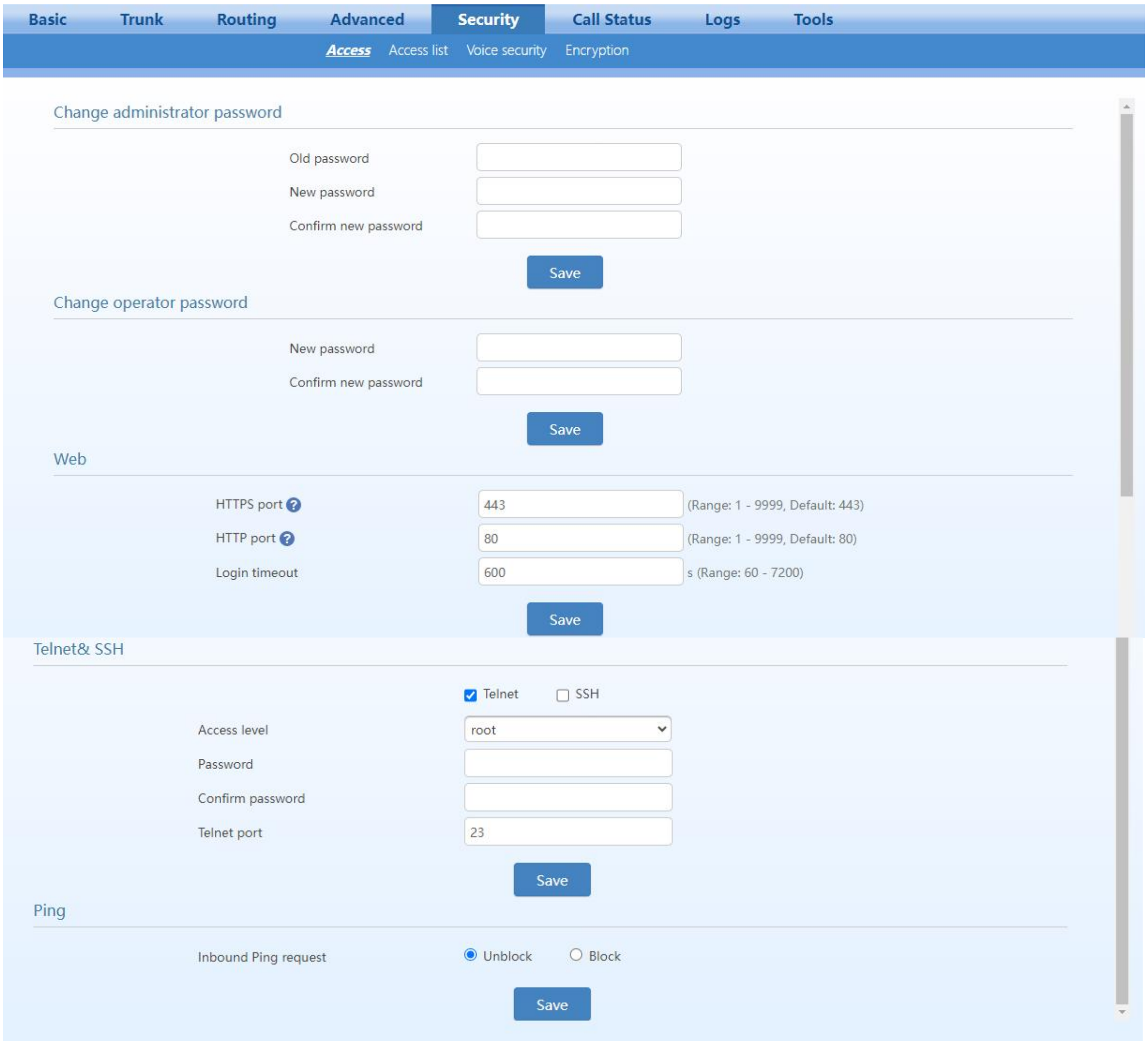


Table 5-20 Access security setting parameters

Name	Description
Change administrator /operator password	Set the administrator/operator password by entering the current password, it needs to enter the old password. The password must meet the following requirements: ● 8 to 16 characters ● At least two of the following: letters, numbers, and symbols ● Excluding &, =, and “ Please change the initial password at first time login.
Web	
HTTP/HTTPS port	Set the HTTP/HTTPS port for the device. The default value is 80 for HTTP and 443 for HTTPS. HTTP/HTTPS port is use for: ● Web accessing (XML command interface) ● Auto Provisioning
Login time out	Set the login timeout interval, if you don’t operate within timeout interval, you will log out. The default value is 600s.
Telnet/SSH	
Telent or SSH	If this parameter is selected, terminals are allowed to access the device through Telnet/SSH. It is not selected by default.

Name	Description
	When accessing the device through SSH, you should login with user **operator**, and use **su root** command to change to user **root**. Please disable Telnet/SSH in time after accessing is finished.
Access level	With two kinds of access authentications: operator and root.
Change Telnet/SSH password	Set password of **user or operator**. Password must meet the following requirements: ● 6 to 20 characters; ● At least the two of following: English letters, numbers, and symbols ● Excluding &, =, and “
Telnet port	Set the Telnet port for the device. The default value is 23.
SSH port	Set the SSH port for the device. The default value is 22.
Ping	
Inbound Ping request	Block or unblock the Ping requests. The device blocks the ping requests by default.

5.7.2 Access list

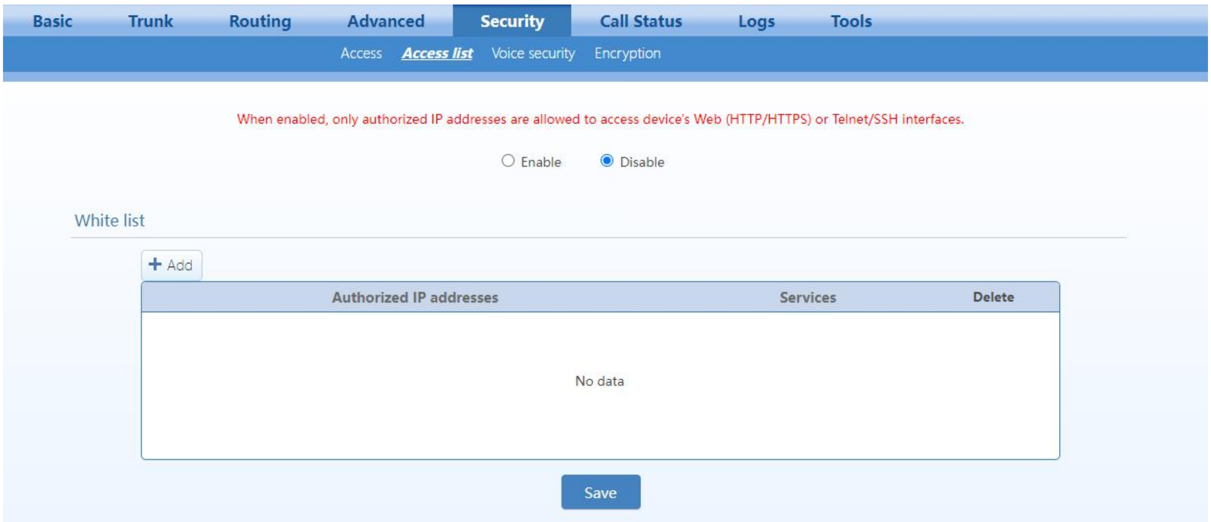
Access list is used to specify the source addresses which are allowed to access the device through Web GUI (HTTP/HTTPS) or Telnet/SSH to ensure legal access to the device and prevent illegal login.

After login, click **Security**>**Access list** to open the configuration interface.

Note

Once access list is enabled, only IP addresses specified here are allowed to access the device through Web GUI or SSH.

Figure 5-20 Access list configuration Interface



Step 1 Click **Add**.

Step 2 In the input box, enter IP addresses and select types of service.

Step 3 Select **Enable**, and click **Save**.

Note

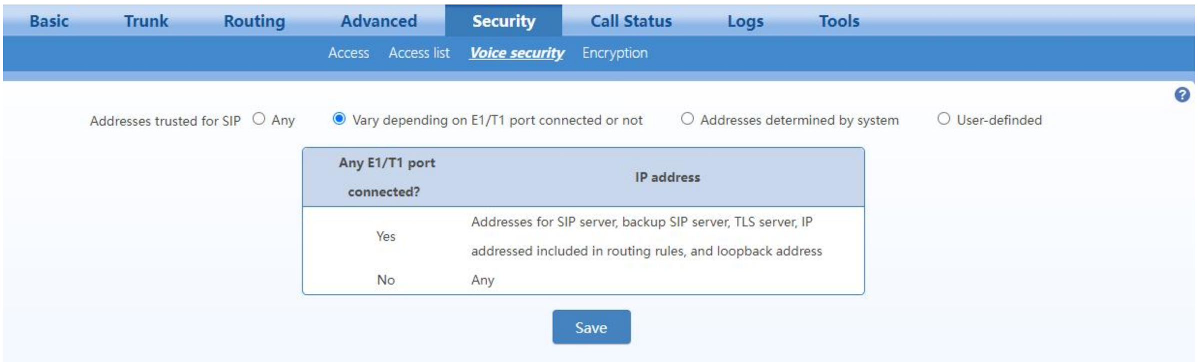
- This function takes effect after the system reboots.
- If access the device by Telnet/SSH, please enable Telnet/SSH on **Security**>**Access** page.
- The device allows an access list of up to 20 entries.

5.7.3 Voice Security

When the device is deployed in Internet, it is possible to suffer from toll fraud. But you can use the Voice Security function to configure the SIP-allowed IP address for the device to prevent toll fraud. The device will only treat the SIP signalings from these IP address to prevent outbound from illegal user.

After login, go to **Security**>**Voice Security** to add the SIP-allowed addresses.

Figure 5-21 Voice Security Configuration Interface



- Any：Trust any random address, but with low security.
- Vary depending on E1/T1 port connected or not: Trust the E1/T1 port according to its connection status.
- Address determinded by system: The trusted address will be determinded by system.
- User-definded: Defined by user.

5.7.4 Encryption

After login, click **Security**>**Encryption** to open this interface.

Figure 5-22 Encryption Configuration Interface

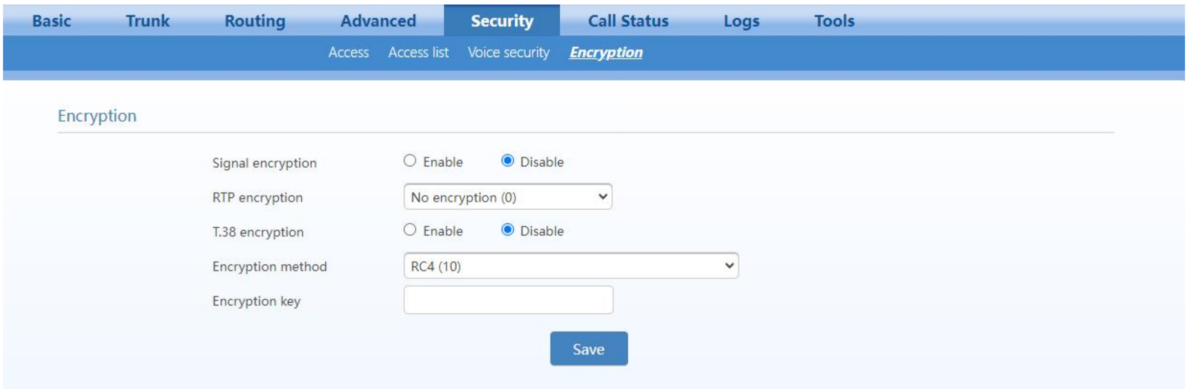


Table 5-21 Encryption Configuration Parameters

Name	Description
Signal encryption	Choose whether to encrypt signaling. By default, this is not selected.
RTP encryption	Choose whether to encrypt RTP voice pack, the default is 0. ● 0: no encryption ● 1: entire message ● 2: header only ● 3: the data body only
T.38 encrypt	Select to encrypt T.38 fax media stream packets. By default, this is not selected.
Encryption method	Set the gateway encryption method, default is 10. The optional parameters as below: ● 10: Adopt RC4 Encryption, use UDP Protocol;
Encryption key	You may obtain this from service provider or admin.

5.8 Call Status

In case of full configurations, the DGW100 has one 4T1/E1 card, with four interfaces numbering Trunk 1 to Trunk 4 from left to right. Users can view the calling state on the interface in usage. The calling information about Trunk (1) is used as an example.

After login, click **Call Status > Trunk 1** to open the interface.

Figure 5-23 Call Status Interface

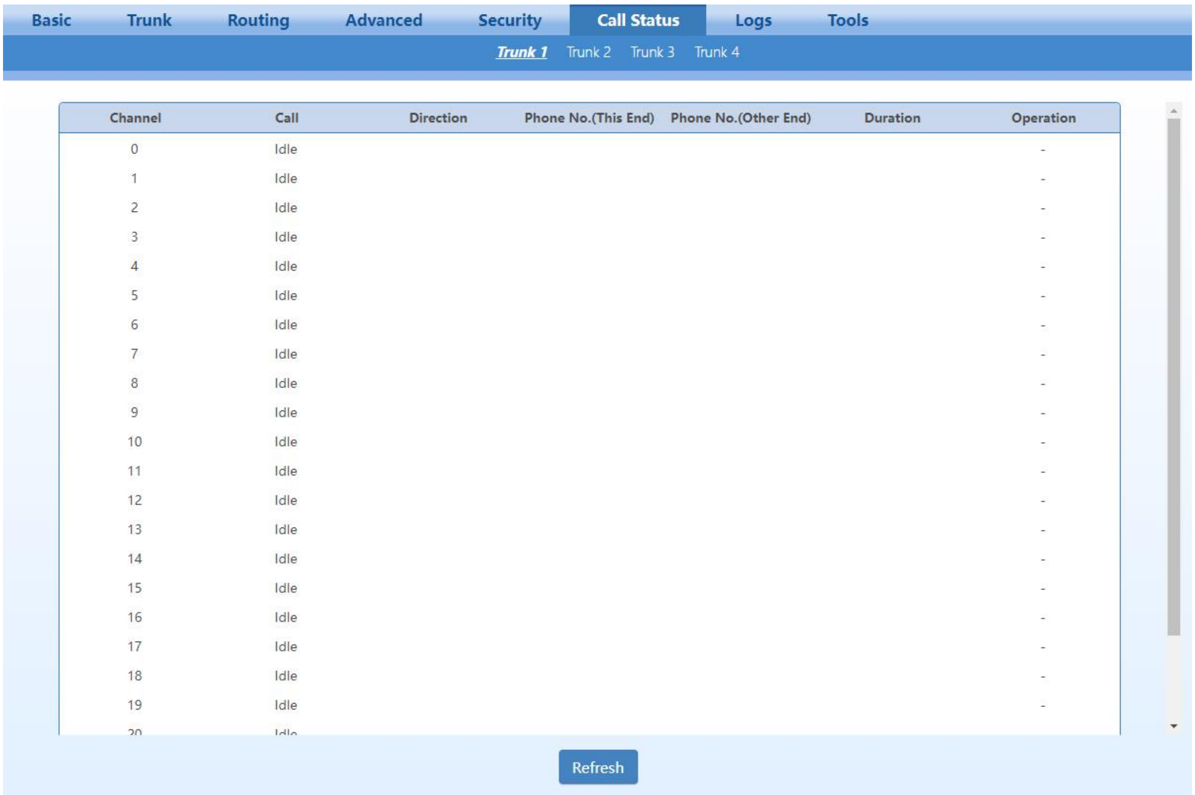


Table 5-22 Status Parameters

Name	Description
Call	The call state includes idle, outpulsing, ringing, dialling, initiating a call, ring back, talking, on-hook on the local end, and on-hook on the opposite device.

5.9 Log Management

5.9.1 System Status

Critical runtime information of gateways can be obtained in this interface, including:

- The information about login interface (including IP address and permissions of the user)
- SIP registration status
- Call-related signaling and media (RTP) information

Click the label of **Logs> System Status** to open this interface.

Figure 5-24 System Status Interface

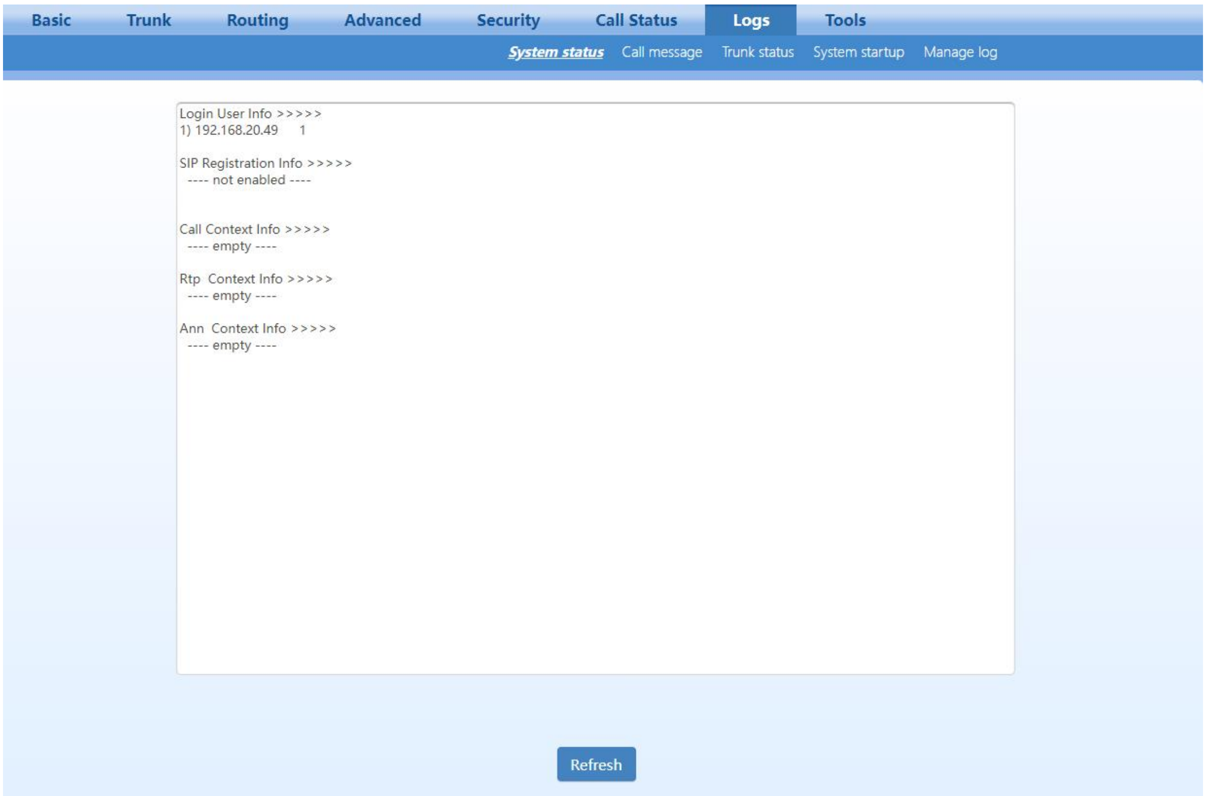


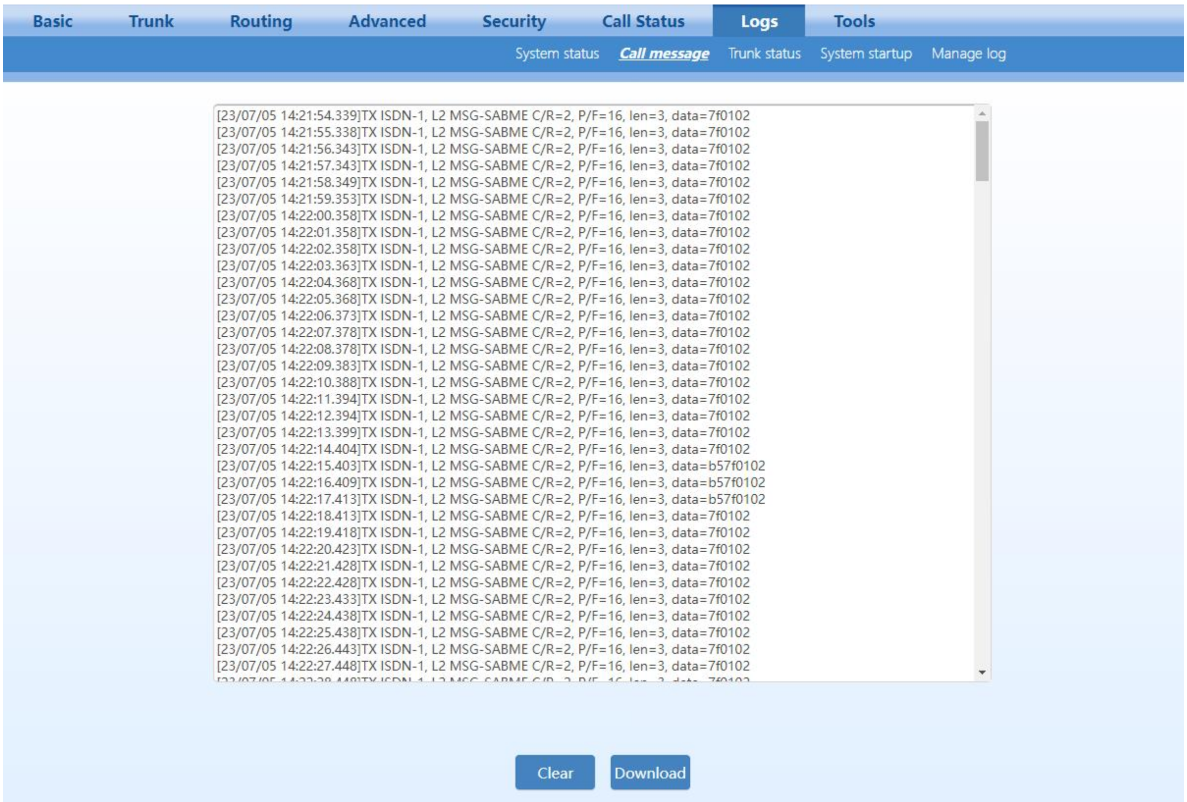
Table 5-23 System Status Parameters

Name	Description
Login User Info	Show the IP address and jurisdiction of login user. The numbers following the IP address show the online jurisdiction of the user: 1- administrator; 2 - operator; 3 – viewer. The viewer can only read the configuration, but is not allowed to modify it. Note: When more than one administrator login at the same time, the first login's jurisdiction is 1, others are 3; also, when more than one operator login at the same time, the first one's jurisdiction is 2, others are 3.
SIP Registration Info	Show registration status: ● Not enabled: The registration server's address is not entered yet; ● Latest response: The latest response message for the registration. 200 means registered successfully; ● No response: No response from registration server. The cause may contribute to 1) incorrect address for the registration server; 2) IP network fault; or, 3) the registration server is not reachable.
Call Context Info	Show the call status.
Rtp Context Info	Show the voice channel related to the calls.
Ann Context Info	Display the playing voice message.

5.9.2 Call Message

Click the label of **Logs > Call Message** to open this interface.

Figure 5-25 Call Message Interface



5.9.3 Trunk status

Click **Logs > Trunk status** to open this interface.

Figure 5-26 Trunk status Interface

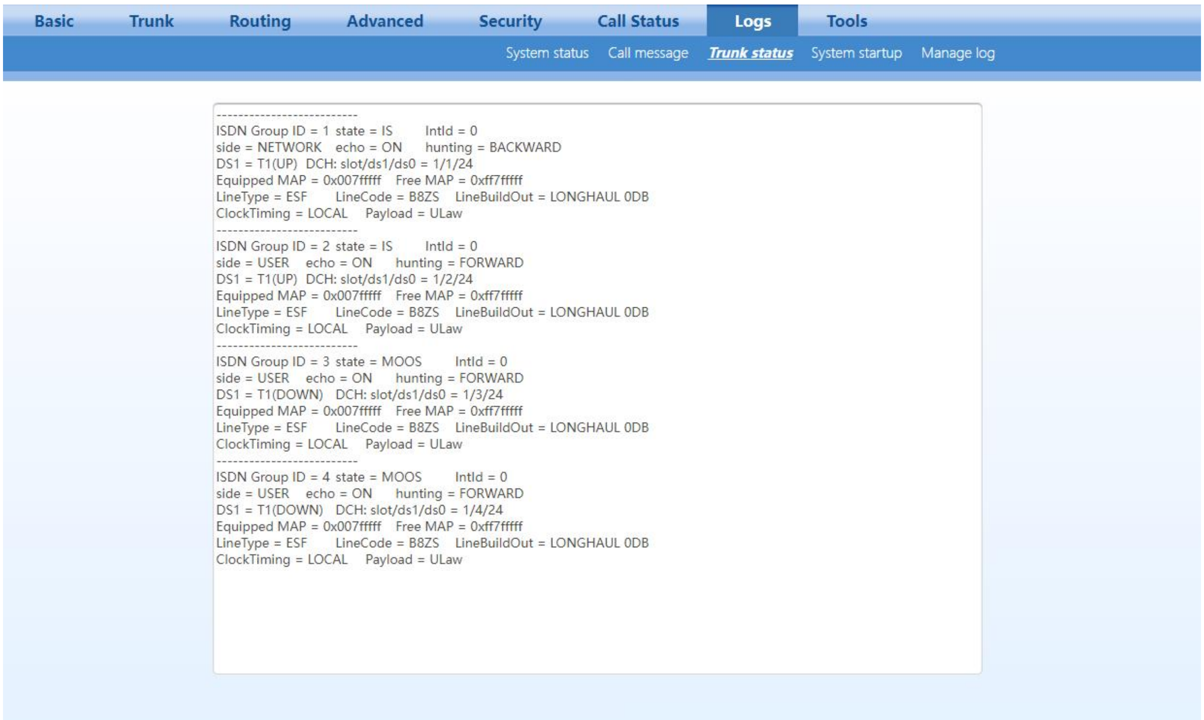


Table 5-24 Trunk status Parameters

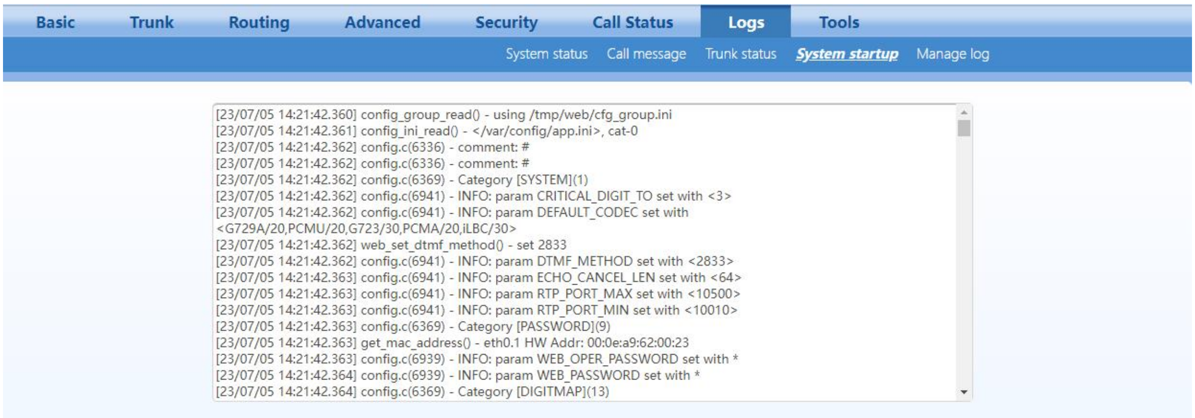
Name	Description
Group ID	The ID of an trunk group. ● If ISDN signaling is used, it will display the ISDN Group ID. ● If T1 CAS signaling is used, it will display the CAS Group ID. ● If not configured, it will display the Trunk Group ID.
ISDN state	State. ● IS indicates both the physical channel and signaling channel are enabled. ● OOS indicates the physical channel is enabled and the signaling channel is disabled. ● MOOS indicates the manually taken-out-of service state, i.e. the physical channel and signaling channel are disabled.
Int Id	The ID of an interface card, which is 0.
side	Two sides of the ISDN: user and network side, which must be set in pairs, with one side being User and the other side being Network.
echo	The echo cancellation function. On: indicates that the echo cancellation is enabled. Off: indicates that the echo cancellation is disabled.
hunting	Two search modes of idle timeslot: ● FORWARD ● BACKWARD
DS1	The type of an interface card: T1 or E1. The connection state of the interface card can be: ● UP (connected) ● DOWN (not connected)
slot/ds1/ds0	One of interfaces (represented by ds1) on a certain slot (represented by slot) into which the T1 or E1 interface card is inserted. “ds0” specifies a signaling channel(DChannel). The signaling channel for the E1 card is 16 timeslots and the signaling channel for the T1 card is 24 timeslots.
Equipped MAP	The available state of the remaining 30 timeslots on the E1 card, except timeslots 0 and 16. If the binary value in 0xfffefffe is 1, the timeslot is available.
Free MAP	The state of an idle timeslot.
LineType	The frame format, including SF, D4, T1_UNFRAMED, SF, E1, E1_MF, E1_CRC and

Name	Description
	E1_UNFRAMED.
LineCode	The line code, including B8ZS, AMI, JBZS, HDB3, ZBTSI, B6ZS, JBZS, etc.
LineBuildOut	The line build-out, which is 120 or 75 Ohm.
ClockTiming	The clock source: Local or Through.
Payload	The PCM encoding type: ALAW or ULAW.

5.9.4 System Startup

Click **Logs** > **System Startup** to open this interface. The gateway boots up information is available in this page, including the hardware configuration.

Figure 5-27 System Startup Interface



5.9.5 Manage Log

Click the label of **Logs** > **Manage Log** to open this interface. Log files can be downloaded through this interface.

Figure 5-28 Manage Log Interface

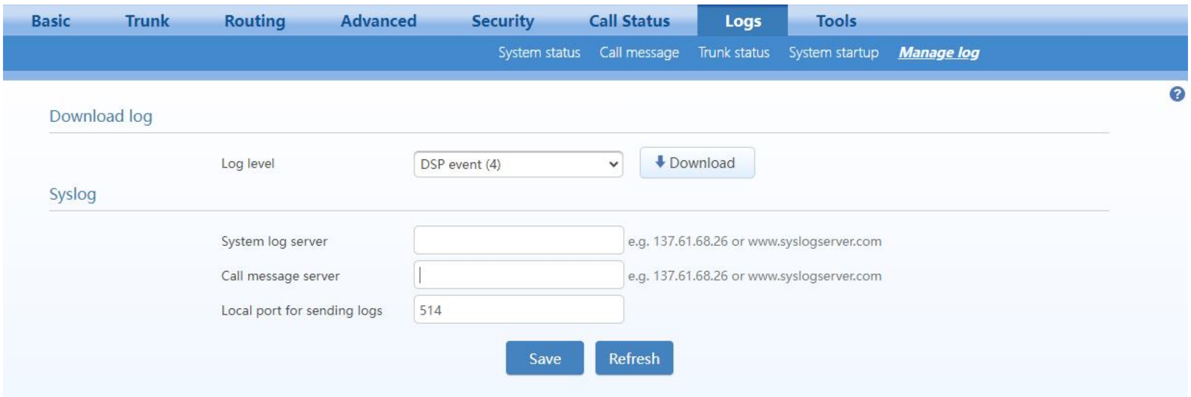


Table 5-25 Manage Log Parameters

Name	Description
Download log	
Log level	Select the log file level of gateway, default is 4. The higher the level goes, the more details the log file will be. Note: log level should be set to be 4 or lower when gateway is used in normal operation, avoiding influencing the system performance.
Syslog	
System log server	The IP address of the syslog server which receives the logs.

Name	Description
Call message server	The IP address of the syslog server which receives the calling message.
Local port for sending logs	The port used to send logs.

Procedure for downloading the log:

Step1 Click **Download**, the gateway begins to assemble the logs.

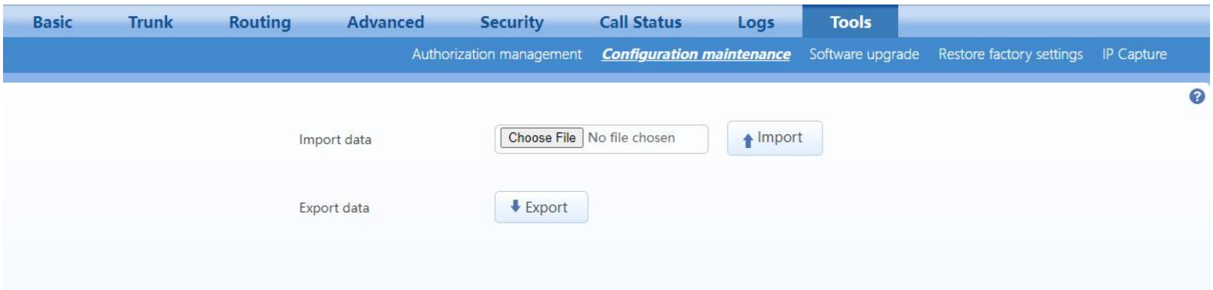
Step2 The user may review the log from the server after finished the download.

5.10 System Tool

5.10.1 Configuration Maintenance

Click **Tools>Configuration maintenance** to open this interface. It's allowed to import or export the configuration files through this interface. The Importing procedure is the same as that of software upgrade. The exporting procedure is similar to the downloading procedure of log files.

Figure 5-29 Configuration Maintenance Interface



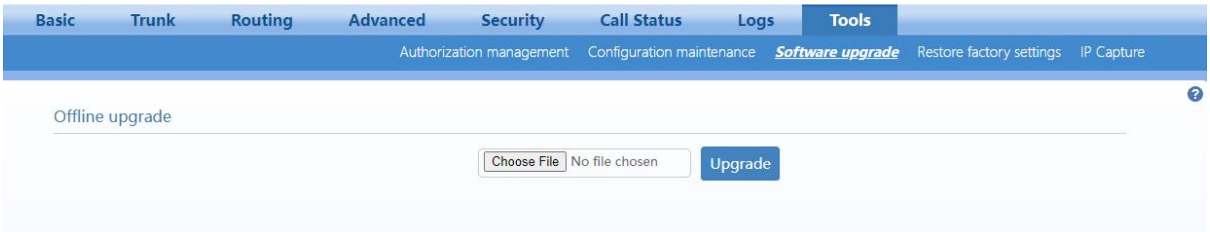
5.10.2 Upgrade

The device supports two upgrading methods: upgrading by .img file or upgrading by tar.gz file.

Please select the upgrading file by actual demand.

Click **Tools>Software Upgrade** to open this interface.

Figure 5-30 Upgrade Interface



Upgrading by .img file

Step 1 Click **Tools**>**Software upgrade**>**Choose file** to choose an .img file.

Step 2 Click **Backup** to save the current configuration after upgrading.

Step 3 Follow the instructions to finish the upgrading.

Note: Please contact the supplier to obtain the latest firmware release file.

Upgrading by tar.gz file

The upgrading by tar.gz file will not change the current configurations. But you are advised to backup the configurations by clicking **Export** on **Tools**>**Configuration maintenance** page before upgrading.

Step 1 Click **Tools**>**Software upgrade**, browse and select a tar.gz file (it needn't decompressing and upload directly).

Step 2 Click **Browse,** select the upgrading file in the local path.

Step 3 Click **Upload**, upload the upgrading file to the device.

Step 4 Follow prompts to complete the upgrade after upload successed.

Note: Please contact the supplier to obtain the latest firmware release file.

Note

- The device upgrade process may last for several minutes. Do not power off, disconnect (from the network), or restart the device during the process. Otherwise, the system may be damaged, and the device cannot be started.
- After the upgrade is successful, the device automatically restarts. Access the gateway management system interface again, click **Info** to view and check whether the software version is the upgrade target version.

5.10.3 Restore Factory Settings

Click **Tools> Restore factory settings>Restore factory settings button** to restore the parameters of gateway into the factory settings.

The factory settings are designed based on common applications, and therefore, no need to modify them in many deployment situations.

5.10.4 IP Capture

After login, click **Tools** > **IP capture** to open this interface. You are allowed to capture up to three IP voice data files, each with up to 2M bytes. The capture is stored in the downloaded file t1.tar.gz under /var/log in dump.cap format after decompressing.

Figure 5-31 IP Capture Interface

Step 1 Go to **Tools** > **IP capture**, and click Start.

Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Stop** to finish the capture procedure. A download request window will pop up to allow you to download the captured packets to your PC.

Step 4 If you need help with problem analysis, you can send the captured file and your problem to support@redstonesystems.com, and the technicians of Redstone will analyze and solve the problem for you. You can open the file by using Wireshark if you want to check it.

5.10.5 Version Information

Click **Info** to view the gateway hardware and software version information.

Figure 5-32 Version Information Interface

5.10.6 Reboot

Click **Reboot** on the top right corner to restart the gateway. As this is a system wide reset, it takes longer time.

5.11 Logout

Click the **Logout** at top right to exit the gateway management system and return to the login interface.