

WSS100-TG Trunk Gateway Series

## **User Configuration Guide**

Document Rev. 1.0 (Oct 10, 2009)

Chapter 4

Modifications are made according to the updated Web-based interface.

**Copyright © 2010 Realtone Technology Co.,Ltd. All Rights Reserved**

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

# Contents of Table

---

<b>Amendment Records .....</b>	<b>2</b>
<b>Contents of Table.....</b>	<b>3</b>
<b>Contents of Figure .....</b>	<b>6</b>
<b>Contents of Table.....</b>	<b>7</b>
<b>1 Overview .....</b>	<b>8</b>
1.1 Product Introduction.....	8
1.2 Functions and Features .....	8
1.3 Equipment Structure.....	9
<b>2 Overview Installation Preparation .....</b>	<b>11</b>
2.1 Installation Preparations .....	11
2.1.1 Collecting the Technical Documents.....	11
2.1.2 Tools and Meters.....	11
2.2 Site Requirements .....	11
2.2.1 Temperature and Humidity .....	11
2.2.2 Cleanliness .....	12
2.2.3 Power Supplier .....	12
2.2.4 Grounding .....	12
2.2.5 Electromagnetic Environment .....	12
2.2.6 Other Facilities .....	13
2.3 Opening Inspection.....	13
2.4 Installation Precautions .....	13
2.5 Rack Mounting.....	14
2.5.1 Attaching the Brackets .....	14
2.5.2 Mounting the Gateway .....	14
2.6 Connecting the Ethernet Cable.....	15
2.7 Connecting the T1/E1 Cable .....	15
2.8 Connecting the Grounding Cable .....	16
2.9 Connecting the Power Cord.....	16
2.10 Verifying Installation .....	16
<b>3 Powering up the Gateway.....</b>	<b>18</b>
3.1 Verification Before Power-up .....	18
3.1.1 Checking Appearance .....	18

3.1.2 Checking Power Supply .....	18
3.2 Powering up the Gateway .....	18
<b>4 Parameter Setting.....</b>	<b>19</b>
Login.....	19
4.1.1 Obtain Gateway IP Address .....	19
4.1.2 Log on Gateway .....	19
4.1.3 Permission of Gateway Administrator .....	19
4.2 Buttons Used on Gateway Management Interface.....	20
4.3 Basic Configuration.....	20
4.3.1 Network Configuration .....	20
4.3.2 System Configuration.....	23
4.3.3 SIP Configuration.....	25
4.3.4 TDM Configuration .....	26
4.4 ISDN Configuration .....	27
4.5 Advanced Configuration .....	28
4.5.1 Routing Table.....	28
4.5.2 Application Examples of Routing Table .....	32
4.5.3 IP Table .....	32
4.5.4 Digit Map .....	33
4.5.5 Media Stream .....	34
4.5.6 SIP related configuration.....	37
4.5.7 System.....	38
4.5.8 Radius call logs .....	41
4.5.9 Encryption.....	42
4.5.10 Call progress tone plan.....	43
4.6 Status.....	44
4.6.1 ISDNn .....	44
4.7 Log management .....	45
4.7.1 System status.....	45
4.7.2 Call message .....	46
4.7.3 ISDN status .....	46
4.7.4 System Startup .....	47
4.7.5 Manage log.....	47
4.8 System tool.....	48
4.8.1 Change password .....	48
4.8.2 Configuration import.....	48
4.8.3 Configuration export .....	49
4.8.4 Software upgrade .....	49
4.8.5 Software restart .....	51
4.8.6 System reboot.....	51
4.8.7 Restore factory settings .....	51
4.9 Version information .....	52
4.10 Logout .....	52



## Contents of Figure

---

Figure1-1 WSS100-TG Front Panel .....	9
Figure1-2 WSS100-TG Back Panel .....	10
Figure2-1 Installation of WSS100-TG Series L-shape brackets.....	14
Figure2-2 Mount WSS100-TG to Rack.....	15
Figure2-3 Connecting the T1/E1 cable.....	16
Figure4-1 Login Interface for WSS100-TG Gateway Configuration .....	19
Figure4-2 Network Configuration Interface .....	21
Figure4-3 System Configuration Interface .....	24
Figure4-4 SIP Configuration Interface .....	25
Figure4-5 TDM Configuration Interface .....	26
Figure4-6 ISDN Configuration Interface.....	27
Figure4-7 Configuration Interface for Routing Table .....	28
Figure4-8 Configuration Interface for IP Table.....	32
Figure4-9 Configuration Interface for Digit Map.....	33
Figure4-10 Media stream configuration interface .....	35
Figure4-11 SIP related configuration interface .....	37
Figure4-12 Interface of system advanced configuraiton .....	39
Figure4-13 Configuration interface of Radius call logs .....	41
Figure4-14 Encryption configuration interface .....	42
Figure4-15 Call progress tone configuration interface .....	43
Figure4-16 ISDN Status Interface .....	44
Figure4-17 Call message interface .....	46
Figure4-18 Interface of ISDN status .....	47
Figure4-19 Interface of system startup.....	47
Figure4-20 Interface of debugging log management.....	47
Figure4-21 Interface of password changing .....	48
Figure4-22 Interface of import data.....	49
Figure4-23 Interface of export data.....	49
Figure4-24 Interface of software upgrade .....	50
Figure4-25 Interface of file upload.....	50
Figure4-26 Upgrade interface.....	50
Figure4-27 Prompt of upgrade process .....	50
Figure4-28 Interface of successful upgrade.....	51

# Contents of Table

---

Table1-1 Description of WSS100-TG Front Panel.....	9
Table1-2 Indicators of WSS100-TG.....	9
Table1-3 Pinouts of T1/E1 Module.....	10
Table1-4 Description of WSS100-TG Back Panel.....	10
Table2-1 Tools and Meters for the Project.....	11
Table2-2 Power Requirements of WSS Gateway Series.....	12
Table2-3 Standard Configuration of WSS100-TG.....	13
Table4-1 Default IP Address of Gateway.....	19
Table4-2 Default Passwords of Gateway.....	19
Table4-3 Network Configuration Parameters.....	21
Table4-4 System Configuration Parameters.....	24
Table4-5 Codec Methods Supported by Gateways.....	24
Table4-6 SIP Configuration Parameters.....	25
Table4-7 TDM Configuration Parameters.....	26
Table4-8 ISDN Configuration Parameters.....	27
Table4-9 Routing Table Format.....	29
Table4-10 Number Transformations.....	30
Table4-11 Routing Destination.....	31
Table4-12 Description of Digit map.....	33
Table4-13 Media stream configuration parameter.....	35
Table4-14 Mapping between the reliability requirement and the TOS value.....	36
Table4-15 SIP related configuration parameter.....	37
Table4-16 Parameters of system advanced configuration.....	39
Table4-17 Configuration parameter of Radius call logs.....	41
Table4-18 Encryption configuration parameters.....	42
Table4-19 Call progress tone configuration parameters.....	43
Table4-20 Parameters of system status.....	45
Table4-21 Configuration parameters of debugging log management.....	47

## 1.1 Product Introduction

This chapter presents a high-level introduction to the WSS100-TG gateway. The WSS100-TG gateway provides voice transmission that enables high-quality, cost-efficient Technologies VoIP service.

Realtone's WSS100-TG product is designed to bridge the gap between traditional, circuit-based Public Switched Telephone Networks (PSTNs) and the emerging packet-switched networks. The WSS100-TG provides an excellent solution for merging digital broadband access networks with the legacy telephone network in a seamless, reliable manner.

## 1.2 Functions and Features

This section presents high-level information about the features of the WSS100-TG platform. It has been designed to serve smaller, cost efficient deployment environments that require a rich feature set.

### One to Four T1/E1 Span Capacity

The WSS100-TG's platform provides one to four T1/E1 spans of capacity (up to 240 voice channels). This allows carriers to identify the ideal size of their deployment and roll out appropriate levels of service.

### Scalability

The WSS100-TG supports 1, 2 or 4 T1/E1 per chassis. This enables carriers to size the gateway to fit their specific need.

### Processing Power

The WSS100-TG possesses 4800 MIPS processing power and supports multiple voice codec (G.711, G.729A, G.723, iLBC, GSM) as well as echo cancellation (G.168), DTMF relay (RFC2833), and fax relay (T.30, T.38).

### Quick and Easy Installation

The WSS100-TG is packaged in a 1U chassis and can be quickly and easily installed using standard tools. It has been designed using industry standards and interoperates with major vendor's soft-switches.

### Simple Configuration

The WSS100-TG is configured and monitored via an intuitive built-in web GUI. The GUI provides password protected access from anywhere on the network.

### Redundant Power Supply Modules

These modules require no special tools or training to perform a field replacement.



## 1.3 Equipment Structure

The WSS100-TG chassis consists of a control module, T1/E1 module, power supply modules, and two fans. Interconnection is performed via a mid-plane which is functionally equivalent to a backplane.

The WSS100-TG chassis is one rack unit (1RU) high, or 1.75 inches (4.4 cm) high x 17.25 inches (43.82 cm) wide x 17.00 inches (43.18 cm) deep. It can be mounted on an Electronics Industry Association (EIA) standard 19inch relay rack or optionally, on a rack shelf or table.

Figure1-1 WSS100-TG Front Panel

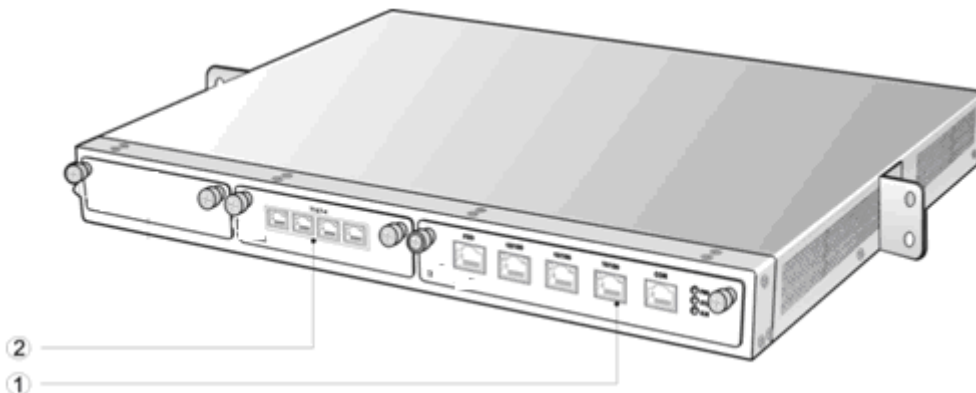


Table1-1 Description of WSS100-TG Front Panel

#	Description
①	Main control module. It offers two 10/100M Ethernet port and one configuration interface (CON).
②	T1/E1 module

Note: DO NOT plug or remove the main control module and interface cards of WSS100 when equipment is powered on.

Table1-2 Indicators of WSS100-TG

Mark	Function	Status	Description
PWR	Power Indication	Green	Power on
		Off	Power off
STU	Status Indication	Off	System locked and inactive
		Green Flash	Normal operation
		Constant Red	System in the process of powerup and not in the normal normal operation mode
		Red Flash	System in a diagnostic mode and able to execute limited operation
ALM	Alarm Indication	Green	No alarms
		Red Flash	New alarms occurred but not confirmed
		Red	Alarms existed and all alarm information confirmed

The T1/E1 Module always has four active RJ-45 connections. Pinouts are shown as follows:

Table1-3 Pinouts of T1/E1 Module

RJ45 Pin-out	1	2	3	4	5	6	7	8
Description	RX_Ring	RX_Tip	NC	TX_Ring	TX_Tip	NC	NC	NC

Figure1-2 WSS100-TG Back Panel

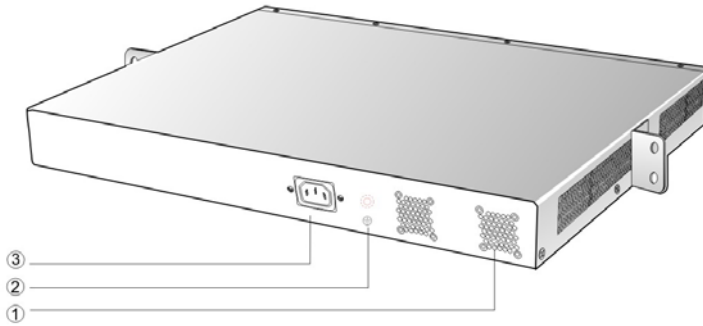


Table1-4 Description of WSS100-TG Back Panel

#	Description
①	Two cooling fans
②	Ground pole
③	AC power socket, 100-240 VAC voltage input.

# 2 Overview Installation Preparation

---

## 2.1 Installation Preparations

### 2.1.1 Collecting the Technical Documents

The technical documents, include network diagram, equipment room facility plan, installation design drawings, wiring drawings, etc, should be provided by the party who is responsible for preparing the documents under the request of purchasing party. Copies of the documents should be provided by the purchasing party to the gateway supplier prior to the shipment.

### 2.1.2 Tools and Meters

The tools and meters listed in following table are required for the installation.

Table2-1 Tools and Meters for the Project

Items
Philips Screwdriver
Slotted Screwdrivers
Diagonal Cutter
RJ45 & RJ11 Crimping Tool
Wire Stripper
RJ45/RJ11 Cable Tester
Angle Square
Spirit Level
Multimeter
Antistatic wrist strap
Cable Tie
Gloves
Antistatic Gloves

## 2.2 Site Requirements

### 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). Abnormal humidity condition may cause problems to the gateway:

- Long term high humidity may lead to bad insulation and even cause electricity leakage, mechanical property change and corrosion.
- 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°C and 40°C. Abnormal temperature condition may cause problems to the gateway:

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

## 2.2.2 Cleanliness

Dust is very harmful to the safe operation of the gateway. Dust that is adsorbed by static electricity acts as insulator, 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.

To ensure adequate ventilation to keep the gateway from overheating, there should be adequate clearance for the air intake and the air exhaust vents. Keep at least 6 cm clearance at the left and right side of the chassis where the air intake is and at least 15 cm clearance at the rear of the chassis where the exhaust vents located.

The rack for WSS100-TG should have a good ventilation system.

## 2.2.3 Power Supplier

Check the power supply system against the electrical specification of the gateway.

The electrical specification is listed in fowling table.

Table2-2 Power Requirements of WSS Gateway Series

Model	Rated Voltage	Input Voltage Range	Power Frequency Range	Max Power Consumption
WSS100-TG	110V or 220V	100V~240V	47Hz~63Hz	75W

## 2.2.4 Grounding

To maintain good voice quality, proper grounding of the AC supply is critical to minimize the noise from the AC interference. Therefore, the following conditions must be ensured:

- 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 elctrical interference.

WSS100-TG is chassis based with ground tab.

In a site that can provide ground for the chassis, the ground tab at the rear panel of chassis for WSS100-TG must be properly grounded.

## 2.2.5 Electromagnetic Environment

Any possible interference source, wherever it is from, impacts the gateway negatively. To resist the interference, make sure that:

- Keeping the gateway far from radio transmitting station, radar station, and high-frequency devices. Use electromagnetic shielding when necessary.
- The gateway is capable for secondary lighten protection on wires and cables that connected to outside buildings.The site must provide the primary 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/Workbench

WSS100-TG is designed to be installed in a standard 19-inch rack, which should provide adequate air-flow 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

If the gateway is equipped with T1/E1 interface, 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 base-T Ethernet port and communicate with other equipments through the network. Inspect IP network on the site, including router, switch, cable wiring and etc, and make sure they are ready for the gateway.

### AC Power Outlets

The gateway needs AC power supply, and sometimes the power is provided through a power strip with extension cord. Verify that each socket outlet on the power strip is equipped with protective earth contact and the protective action is not negated by using extension power cord.

## 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 WSS100-TG with basic configuration should include components as shown in following table.

Table2-3 Standard Configuration of WSS100-TG

Part Name	Quantity	Unit
WSS100-TG Gateway	1	Set
Power Cord, 3 Meters, AC250V/10A	1	Set
Rack Mounting Kits	1	Set
T1/E1 Cable	1 or 2 or 4	Set

### Note:

The quantity of analog line cable should match the number of analog interface card installed in the equipment.

## 2.4 Installation Precautions

Please pay special attention to the safety guidelines during installation and operation:

- Keep the site far from the heat and humidity.
- Take precautions with use of high-voltage electricity.
- Connect the interface cables correctly.

## 2.5 Rack Mounting

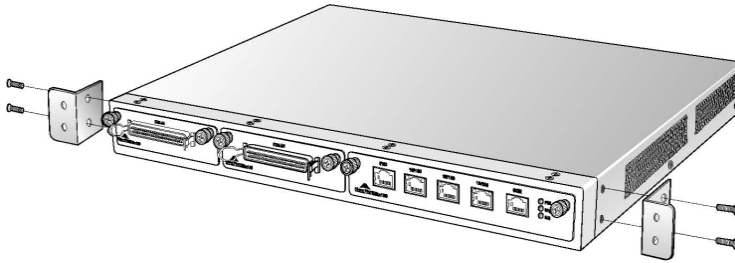
The WSS100-TG series chassis are designed to be mounted on a standard 19-inch rack with 1U height.

### 2.5.1 Attaching the Brackets

Place the WSS100-TG 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, as shown in the following figure.

The L-shape brackets are used to secure the gateway to the rack. The brackets cannot support the weight of the equipment alone. Prior to install the WSS100-TG series chassis into rack, a supporting shelf must be installed in place where the gateway will sit.

Figure2-1 Installation of WSS100-TG Series L-shape brackets



### 2.5.2 Mounting the Gateway

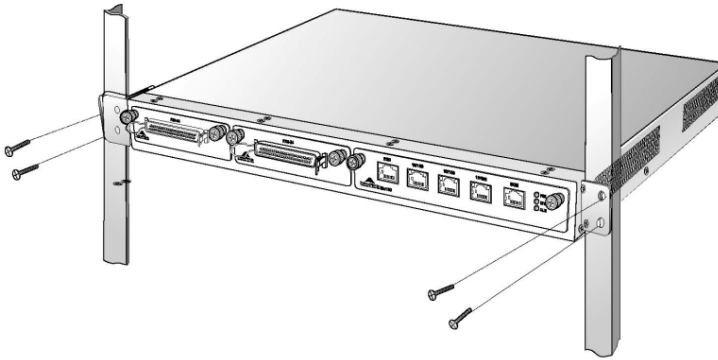
Attention should be paid during the installation:

- Ensure that the rack is firmly attached to the ground and stable.
- If the gateway is installed in a closed cabinet shelf, the cabinet must provide adequate air-flow so the equipments inside can be well ventilated.
- If multiple gateways are installed in a rack, it is recommended to keep at least 1/2U space between gateways for heat dissipation.

Follow the steps to install the gateway:

- Place the gateway on a shelf in the rack.
- Slide it to a proper position along the guide rails.
- Fix the rack-mount brackets to the rack posts with supplied Phillips screws. Make sure that the gateway is in level position and securely fixed as shown in following figure.

Figure2-2 Mount WSS100-TG to Rack



The gateway chassis is securely attached to the rack by the rack mounting brackets and the supporting shelf.

## 2.6 Connecting the Ethernet Cable

Connect one end of the Ethernet cable to the Ethernet port of the gateway and connect the other end to the peer Ethernet switch or router. Check that the ETH LED on the front panel is lit, which indicates that the network cable is correctly connected.

## 2.7 Connecting the T1/E1 Cable

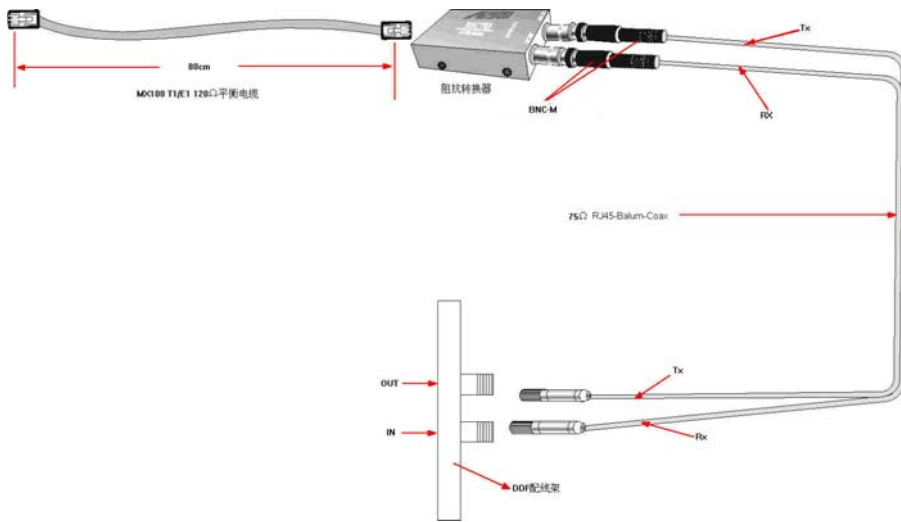
WSS100-TG offers RJ45 jack as T1/E1 connector for making ISDN connection with PBX or PSTN.

Please identify the connector type and interface impedance of the other side equipment before making T1/E1 connection.

If the other side equipment offers same RJ45 jack, use CAT5 cable with RJ45 plugs on both side to make T1/E1 cable connection. Be sure to match TX and RX pair according to the PIN specification when making the CAT5 cable.

If the other side equipment offers separate TX/RX coax connectors for T1/E1 connection, use RJ45-Balun-Coax cable sets and follow the figure to make the connection.

Figure2-3 Connecting the T1/E1 cable



## 2.8 Connecting the Grounding Cable

When install in equipment room facility providing independent grounding, it is required to connect the chassis ground tab on WSS100-TG 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 WSS100-TG 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.

## 2.9 Connecting the Power Cord

Before connect the power cord, make sure the AC power outlet is provided with a protective earth contact and the earth contact of the AC power source is proper grounded.



### CAUTION

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

Follow the steps to connect power cord:

Turn the switch of AC power outlet to “OFF” position.

WSS100-TG use the shipped power cord to connect between the AC input at rear of the chassis and the AC power outlet.

## 2.10 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 is used as specified.
- The gateway is correctly connected to console terminal and other devices.

# 3 Powering up the Gateway

---

## 3.1 Verification Before Power-up

### 3.1.1 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 0-40°C.

### 3.1.2 Checking Power Supply

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

## 3.2 Powering up the Gateway

Turn the power switch to “ON” position. Check the status of PWR LED, and if it is lit the gateway is powered properly.

# 4 Parameter Setting

## Login

### 4.1.1 Obtain Gateway IP Address

WSS100-TG Gateways use a static IP address by default.

Table4-1 Default IP Address of Gateway

Type	Default DHCP Service	Default IP Address	Default Subnet Mask
WSS100-TG	Disabled	192.168.2.240	255.255.0.0

### 4.1.2 Log on Gateway


Double-click the icon  to open IE browser, and enter the gateway IP address in the browser address bar (eg. 192.168.2.240); you can enter the login interface for gateway configuration by entering a password on the login interface.

Figure4-1 Login Interface for WSS100-TG Gateway Configuration



### 4.1.3 Permission of Gateway Administrator

Logon users are classified into “administrator” and “operator”. The default password is seen Table4-2. The password is shown in a cipher for safety.

Table4-2 Default Passwords of Gateway

Type	Default Administrator Passwords (lowercase letters required)	Default Operator Password
WSS100-TG	voip	operator

- 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 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.



## CAUTION

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.

Upon completion of configuration, click "Logout" button to return to the login page, so as not to affect the login permission of other users.

---

## 4.2 Buttons Used on Gateway Management Interface

“Submit” and “Restore Default Configuration” buttons are at the bottom of configuration interface.

- “Submit” Button: Submit configuration information. Users click “Submit” 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 system restart; it is recommended that users press the “Restart” button on the “Tool” page to validate the configuration after changing all parameters to be modified.
- “Default” Button: Click this button to use default configuration of gateway. A success prompt will appear on the interface after the system restores parameters on the configuration page to default configuration. For part of parameters, it is required to restart the software to validate the default configuration, and in this case “The configuration takes effect after the system is restarted” will appear on the interface. Subscribers can click “Restart” on the “Tool” page to restart.

## 4.3 Basic Configuration

### 4.3.1 Network Configuration

After login, click “Basic > Network” tab to open the configuration interface.

Figure4-2 Network Configuration Interface

ne view		
Date: 2010-03-05 09:20:29		Network   System   SIP   TDM
Host name	TG-VoIP-GW	Contain letter, number and "." but must start with letter
Logical IP address	192.168.13.130	
ETH3		
MAC address	00:0E:A9:00:EE:EF	
IP address assignment	PPPoE	
User name		
Password		
IP address	192.168.13.130	
Netmask	255.255.0.0	
Gateway IP address	192.168.2.1	
ETH1		
MAC address	00:0E:A9:10:EE:EF	
IP address		
Netmask		
DNS		
Enable	<input type="checkbox"/>	
Primary server		e.g. 202.96.209.6
Secondary server		e.g. 202.96.209.133
SNTP		
Primary server	192.43.244.18	
Secondary server	198.60.22.240	
Time zone	(GMT+08:00) Beijing	

Table4-3 Network Configuration Parameters

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.
Logical IP address	This parameter only exists in WSS100, used to display the actual gateway IP address in use.
ETHn	
MAC address	Display the MAC address of gateway.
IP address assignment	Methods for obtaining an IP address <ul style="list-style-type: none"> <li>● Fixed: Static IP address is used;</li> <li>● DHCP: Activate DHCP service and use the dynamic host configuration protocol (DHCP) to allocate IP addresses and other network parameters;</li> <li>● PPPoE: PPPoE service is used.</li> </ul>
User name	Enter an authentication user name if PPPoE service is selected, and there is no default value.
Password	Enter an authentication password if PPPoE service is selected, and there is no default value.
IP address	If "Static" or "DHCP" is selected for the network type but an address fails to be obtained, the gateways will use the IP address filled in here. If the gateways obtain an IP address through DHCP, the system will display the current IP address automatically obtained from DHCP by the gateways. This parameter must be set due to no default value.

Name	Description
Netmask	The subnet mask is used with an IP address. When the gateways use 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. This parameter must be set due to no default value.
Gateway IP address	LAN gateway IP address where the gateways are located. When the gateways obtain an IP address through DHCP, the system will display the LAN gateway address automatically obtained through DHCP. This parameter must be set due to no default value.
<b>DNS</b>	
Enable	Activate DNS service.
Primary Server	If DNS service is activated, the network IP address of preferred DNS server must be entered, and there is no default value.
Secondary Server	If DNS service is activated, the network IP address of standby DNS server can be entered here. It is optional and there is no default value.
<b>SNTP</b>	
Primary Server	Enter the IP address of preferred time server here. This parameter must be set due to no default value.
Secondary Server	Enter the IP address of standby time server here. This parameter must be set due to no default value.

Name	Description
Time Zone	<p>Select a time zone, and the parameter values include:</p> <ul style="list-style-type: none"> <li>• (GMT-11:00) Midway Island</li> <li>• (GMT-10:00) Honolulu. Hawaii</li> <li>• (GMT-09:00) Anchorage, Alaska</li> <li>• (GMT-08:00) Tijuana</li> <li>• (GMT-06:00) Denver</li> <li>• (GMT-06:00) Mexico City</li> <li>• (GMT-05:00) Indianapolis</li> <li>• (GMT-04:00) Glace_Bay</li> <li>• (GMT-04:00) South Georgia</li> <li>• (GMT-03:30) Newfoundland</li> <li>• (GMT-03:00) Buenos Aires</li> <li>• (GMT-02:00) Cape_Verde</li> <li>• (GMT) London</li> <li>• (GMT+01:00) Amsterdam</li> <li>• (GMT+02:00) Cairo</li> <li>• (GMT+03:00) Moscow</li> <li>• (GMT+03:30) Teheran</li> <li>• (GMT+04:00) Muscat</li> <li>• (GMT+04:30) Kabul</li> <li>• (GMT+05:30) Calcutta</li> <li>• (GMT+05:00) Karachi</li> <li>• (GMT+06:00) Almaty</li> <li>• (GMT+07:00) Bangkok</li> <li>• (GMT+08:00) Beijing</li> <li>• (GMT+09:00) Tokyo</li> <li>• (GMT+10:00) Canberra</li> <li>• (GMT+10:00) Adelaide</li> <li>• (GMT+11:00) Magadan</li> <li>• (GMT+12:00) Auckland</li> </ul>

### 4.3.2 System Configuration

After login, click “Basic > System” tab to open the system configuration interface.

Figure4-3 System Configuration Interface

ne view  
 2010-03-05 09:20:29 Network | System | SIP | TDM | Lc

Application	Support T38 (CED) Data application includes modem, POS and FoIP
Codec	G729A/20,PCMU/20,PCMA/20,G723/30 G729A/20,G723/30,PCMU/20,PCMA/20,iLBC/30,GSM/20
DTMF method	RFC 2833
2833 payload type	100 96-127, default: 100. This value should be set as the same as the value in server
DTMF on-time	100 80-150(ms), default: 100. This is the on-time of sending DTMF digit
DTMF off-time	100 80-150(ms), default: 100. This is the off-time of sending DTMF digit
DTMF detection threshold	48 32~96(ms),default: 48.This is the dection threshold for receiving DTMF digit

Table4-4 System Configuration Parameters

Name	Description
Application	Select a gateway application scenario in this field: Audio only, Support T38 (Fax) and Voice-band Data, Support T38 (CED), Support T38 (CNG), Support Voice-band Data. Voice-band Data service including Modem, POS and T.30 fax. The gateways support voice service in any mode.
Codec	Codecs methods supported by the gateways include G729A/20, G723/30, PCMU/20, PCMA/20, iLBC/30 and GSM/20 (as shown in table 2-5). This parameter must be set due to no default value. 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 method	Transmission modes of DTMF signal supported by the gateways include Audio, RFC 2833 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: Separate DTMF signal from sessions and transmit it to the platform through RTP data package in the format of RFC2833.
2833 payload type	Used with “RFC 2833” in the DTMF transmission modes. The default value of 2833 payload type is 100. The effective range available: 96 ~ 127. This parameter should match the setting of far-end device (eg. platform).
DTMF on-time	This parameter sets the on time (in ms) of DTMF signal sent from FXO port. The default value is 100 ms. Generally, the duration time should be set in the range of 80 ~ 150 ms.
DTMF off-time	This parameter sets the off time (ms) of DTMF signal sent from FXO port. The default value is 100 ms. Generally, the interval time should be set in the range of 80 ~ 150 ms.
DTMF detection threshold	Minimum duration time of effective DTMF signal. Its effective range is 32-96 ms and the default valie is 48 ms. The greater the value is set, the more stringent the detection is.

Table4-5 Codec Methods Supported by Gateways

Codec Supported by WSS	Bit Rate (Kbit/s)	Time Intervals of RTP Package Sending (ms)
iLBC	13.3/15.2	20/30



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

### 4.3.3 SIP Configuration

After login, click “Basic> SIP” tab to open the SIP configuration interface.

Figure4-4 SIP Configuration Interface

9:20:29		Network   System   SIP   TDM
Signaling port	5060	1~9999, default 5060
Registrar server		e.g. 168.33.134.50:5060 or www.sip.com:5060
Proxy server	localhost:5060	e.g. 168.33.134.51:5000 or www.sipproxy.com:5000
Backup proxy server		e.g. 168.33.134.53:5060
User agent domain name		e.g. www.gatewaysip.com
User name		You may obtain it from service provider
Password		You may obtain it from service provider
Registration period	3600	15~86400(s)

Table4-6 SIP Configuration Parameters

Name	Description
Signaling port	Configure the UDP port for transmitting and receiving SIP messages, with its default value 5060. 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.
Register server	Configure the address and port number of SIP register server, and the address and port number are separated by “:”. It has no default value. The register server address can be an IP address or a domain name. When a domain name is used, it is required to activate DNS service and configure DNS server parameters on the page of configuring network parameters. For example: “201.30.170.38:5060”, “register.com: 5060”.
Proxy server	Configure the IP address and port number of SIP proxy server, and the address and port number are separated by “:”. It has no default value. The proxy server address can be set to an IP address or a domain name. When a domain name is used, it is required to activate 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 proxy server	Configure the IP address and port number of backup proxy server. It has no default value. Add the address of calling proxy server here, and the gateways can support selection function of multiple softswitch addresses through IP address. The format must be IP address format and complete and effective configuration, eg. “202.202.2.202:2727”. The proxy and register servers must be identical.  Conditions for falling over to the backup proxy server (any): 1) Gateway register is timeout; 2) No response to master server calls is timeout;

Name	Description
User agent domain 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 proxy server as user agent domain name. It has no default value. It is recommended that subscribers not use LAN IP address to set domain name parameter.
User name	Configure the user name as part of the account for registration, and it has no default value. Note: If “Register by gateway” or “Line Reg/GW Auth”, is selected, the user name must be entered here. If “register by line” is selected the user name should be set on “Line > Feature” page (Refer to “Feature”).
Password	Password as part of account information is used for authentication by platform. It has no default value. It is formed with either numbers or characters, and case sensitive. Note: If “Register by gateway” or “Line Reg/GW Auth”, is selected, the password must be entered here. If “register by line” is selected the password should be set on “Line > Feature” page (Refer to “Feature”).
Registration period	Valid time of SIP re-registration in second.

### 4.3.4 TDM Configuration

After login, click “Basic > TDM” tab to open the configuration interface.

Figure4-5 TDM Configuration Interface

The screenshot shows the TDM Configuration Interface with the following settings:

- DS1 type:  E1,  T1
- PCM codec:  ALaw,  μLaw
- Timing source: Local
- Table for TDM channels (TDM1-TDM4):
 

	TDM1	TDM2	TDM3	TDM4
Framing	E1_MF_CRC	E1_MF_CRC	E1_MF_CRC	E1_MF_CRC
Line code	HDB3	HDB3	HDB3	HDB3
Line length	120OHM	120OHM	120OHM	120OHM
Digit adjust				

Table4-7 TDM Configuration Parameters

Name	Description
DS1 type	DS1 Type configures if the T1/E1 interface operates as a T1 or E1 interface.
PCM codec	Allows configuring the PCM encoding type. Allowed settings are ULaw and ALaw.
Timing source	The Timing Source parameter can be configured as Local (use local clock) or SPAN (use recovered clock from the interface). Note: If one interface is configured to use SPAN clock, all other interfaces will use the same recovered clock. When more than one interface is configured to use SPAN clock, TG will adopt the recovered clock from the first upped interface.

Name	Description
Framing	If the WSS100-TG DS1 Type is set to T1 then Line Framing can be set to D4, SF (Superframe), ESF (Extended Superframe) mode. If the WSS100-TG DS1 Type is set to E1 then Line Framing can be set to E1_MF_CRC mode.
Line code	If the WSS100-TG DS1 Type is set to T1 then Line Code can be set to B8ZS or AMI. If the WSS100-TG DS1 Type is set to E1 then Line Code can be set to HDB3.
Line length	Setting configures the line build out (LBO) of the T1/E1 line. The default for T1 is Shorthaul / 110 FT. The default for E1 is 120 Ohm.

## 4.4 ISDN Configuration

After login, click “ISDN > ISDN1” tab to open the configuration interface.

Figure4-6 ISDN Configuration Interface

The screenshot shows the ISDN Configuration Interface for a trunk named TEST2. The interface includes the following settings:

- Name:** TEST2
- Enable:**
- Application:**
  - Collecting CDPN:  Overlap,  Enbloc
  - D channel:  Timeslot 16,  Timeslot 24
  - Switch type:  User,  Network
  - Signaling Standard: CCITT (dropdown)
  - Circuit hunting: Forward (dropdown)
  - D channel service message:
  - Nail-up connection:  No CPDN and channel ID will be applied
  - CPN category:  Standard,  Nonstandard
  - CPN presentation:
  - CDPN category:  Standard,  Nonstandard
  - Busy line handling:  Announcement,  Hang up
  - CID exclusive:  The exclusive bit in the CID field will be set
- Second stage dialing:**
  - Enable:
  - Prompt:  Announcement,  Dial tone
  - Calling party number (CPN):  Originating number,  Original CDPN
  - Called party number (CDPN):  Original CDPN + Second dialed number,  Second dialed number
- Timeslot management:** A row of 32 timeslots (0-31) is shown, with timeslots 16 through 31 being active (indicated by green dots).

Table4-8 ISDN Configuration Parameters

Name	Description
Name	Trunk name.
Enable	Select to activate the trunk.
Application	
Collecting CDPN	
D channel	The D Channel parameter defines the signaling channel. Typically the signaling channel for a T1 interface is 24, and 16 for an E1 interface.

Name	Description
Switch type	Switch Side defines the ISDN behavior. The setting of Switch Side for the other side of the T1/E1 line must be opposite that of the WSS100-TG. The settings for Switch Side are User and Network.
Signaling standard	Used to set which the WSS100-TG use standard. Protocol Standard can be set to CCITT or NI2.
Circuit hunting	The Hunting parameter is used to set how the WSS100-TG searches an idle time-slot. Hunting can be set to Forward or Backward.
D channel service message	
Nail-up connection	No CPDN and channel ID will be applied.
CPN category	
CDPN category	
Busy line handling	
CID exclusive	The exclusive bit in the CID field will be set.
Second stage dialing	
Enable	When a telephone call comes to the ISDN, the gateways will provide the second dial tone and route the call according to the extension number pressed in.
Prompt	Set the dialing tone or voice prompt file.
Calling party number (CPN)	
Called party number (CDPN)	
Timeslot management	

## 4.5 Advanced Configuration

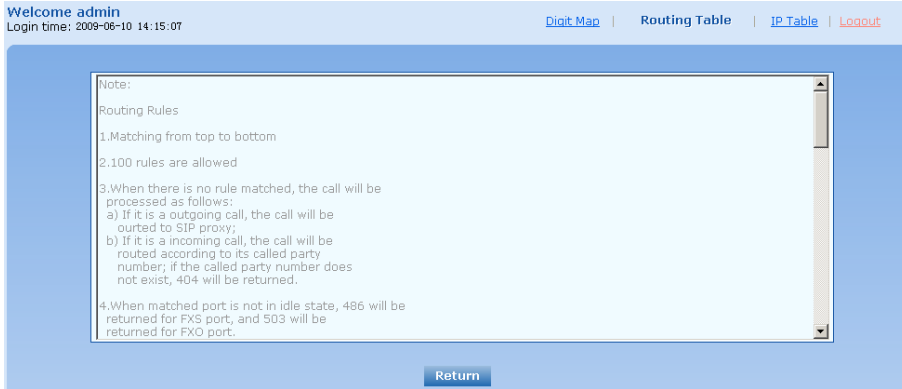
### 4.5.1 Routing Table

After login, click “Advanced > “Routing Table” tab to open the configuration interface.

Figure4-7 Configuration Interface for Routing Table



Click “Help” to open the illustrative interface for routing configuration



The routing table with 100 rules in capacity provides two functions including digit transformation and call routing assignment. Here are the general rules applied by gateways when executing the routing table:

- 1) The routing rules in the table are executed from top to down, and the number matching follows the principle of minimum & priority matching;
- 2) When there is no rule matched, the call will be processed as follows:
  - a) For outbound calls, calls will be routed to SIP proxy;
  - b) For inbound calls, calls will be routed according to its called party number, and if the called party number does not exist, 404 will be returned.
- 3) When domain name is used in rule, DNS must be selected and enabled first.



### CAUTION

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 transformation is

**Source Number Handle [Parameter]**

or

**Source Number ROUTE Destination [Parameter]**

Table4-9 Routing Table Format

Name	Description
Source	Source can be ISDN or IP. When source is IP, an address can optionally be specified, e.g., [xxx.xxx.xxx.xxx] or [xxx.xxx.xxx.xxx:port]
Number	The default number is called party number. If the calling party number is being used, add CPN in front of the number. The Number can be: <ul style="list-style-type: none"> <li>● A specific number like (114, 83501950)</li> <li>● A number prefix like (61., 61x5 or 61)</li> <li>● A number range like (268[0-1,3-9])</li> </ul>

Table4-10 Number Transformations

Processing Mode	Description and Example
KEEP	<p>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.</p> <p>Example: IP 02183501950 KEEP -8; 83501950</p> <p>Keep the last 8 digits of the called number 02183501950 for calls from IP. The transformed called number is 02183501950.</p> <p>Example: IP 12 KEEP -3</p> <p>won't take effect, but any number start with 12 other than 12345 will take effect</p>
REMOVE	<p>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.</p> <p>For example: IP 021 REMOVE 3</p> <p>Any number start with 021, the 021 prefix is removed.</p> <p>For example: IP 12345 REMOVE 4</p> <p>then remove first 4 digits</p>
ADD	<p>Add prefix or suffix to number. The positive number behind ADD is the prefix; the negative number is suffix.</p> <p>Example 1:</p> <p>IP CPN6120 ADD 021</p> <p>CPN number start with 6120, prefix 021 is added.</p> <p>Example 2:</p> <p>IP CPN6120 ADD -8888</p> <p>CPN number start with 6120, 8888 is appended.</p> <p>Example 3:</p> <p>IP 12345 ADD -8001</p> <p>number started with 12345 add suffix 8001</p> <p>Example 4:</p> <p>IP 123456 ADD -8002</p> <p>won't take effect, if this rule is needed it should be moved before the 12345 rule and put an END statement after it</p>
REPLACE	<p>Number replacement. The replaced number is behind REPLACE.</p> <p>Example:</p> <p>ISDN CPN88 REPLACE 2682000</p> <p>CPN number started with 88, the prefix "88" is replaced with 2682000.</p> <p>ISDN CPN88. REPLACE 2682000</p> <p>CPN number started with 88, the whole number is replaced with 2682000.</p>
REPLACE	<p>Other use of REPLACE is to replace the specific number based on other number associated with the call. For example, replacing the calling number according to the called number.</p> <p>Examples:</p> <p>IP 12345 REPLACE 777</p> <p>won't take effect for 12345x</p> <p>IP[222.34.55.1] CPNX. REPLACE 2680000</p> <p>Calls from 222.34.55.1, Calling party number is replaced with 2680000</p>

Processing Mode	Description and Example
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 EDN, or route the call to the designed routing after meeting ROUTE. Example: IP 12345 END stop digit manipulation, no change on later matching condition
SEND180	Force send 180 on ring back Example: IP CPN2 SEND180 CPN number start with 2, always send 180 on ring back.
SEND183	Force send 183 on ring back. Example: IP CPN3 SEND183 CPN number start with 3, always send 183 on ring back (voice cut through).
HIDE	Calling party number presentation. Example: IP[61.2.44.53:5060] CPNX. HIDE Any call from 61.2.44.53:5060, calling party number presentation restriction is applied. IP[222.34.55.1] CPNX. HIDE then calling party number presentation restriction is applied
CODEC	Designate the use of codec, such as PCMU/20/16, where PCMU denotes G.711, /20 denotes RTP package interval of 20 milliseconds, and /16 denotes 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.
RELAY	Insert prefix of called party number when calling out. The inserted prefix number follows behind REPLAY. 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 being sending out.

Table4-11 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 IP	Route a call to the IP platform. Example: FXS 021 ROUTE IP 228.167.22.34:5060 228.167.22.34:5060 is the IP address of the platform.

Destination	
ROUTE ISDN	<p>Route a call to ISDN.</p> <p>Example: IP 8621 ROUTE ISDN 1 call has 8621 prefix, route to ISDN span 1</p> <p>Example: IP CPN8620 ROUTE ISDN 2 calling party number started with 8620, route to ISDN span 2</p> <p>Example: IP 12345 ROUTE ISDN 2 then stop further matching digit manipulation and route to ISDN span 2 IP[222.34.55.1] CPNX. ROUTE ISDN 2 then route to ISDN span 2.</p>

## 4.5.2 Application Examples of Routing Table

- 1) In the following example, traffic will be moved to another VoIP platform that has a common access number (e.g. 17909).

```
IP[222.34.55.1] CPNX. REPLACE 2680000
```

```
IP[222.34.55.1] CPNX. RELAY 17909
```

All calls from 222.34.55.1 will have their calling party number replaced with 2680000. Next, after 17909 cut-through, the WSS100-TG will pulse out the CDPN (in-band DTMF) and let the 17909 platform make the final connection.

- 2) Sometimes the IP traffic to the WSS100-TG has a CDPN prefix that tells us where to relay the traffic.

```
IP 17909 REMOVE 5
```

```
IP 17909 RELAY 17909
```

```
IP 17909 ROUTE ISDN 2,3
```

First the WSS100-TG removes the CDPN prefix that is used for routing (17909 is removed). Next the WSS100-TG calls the 17909 access number.

After connecting to the 17909 platform, the rest of the CDPN is pulsed out (in-band DTMF) and the connection is made by the 17909 platform.

## 4.5.3 IP Table

After login, click “Advanced > “IP Table” tab to open the configuration interface.

Figure4-8 Configuration Interface for IP Table



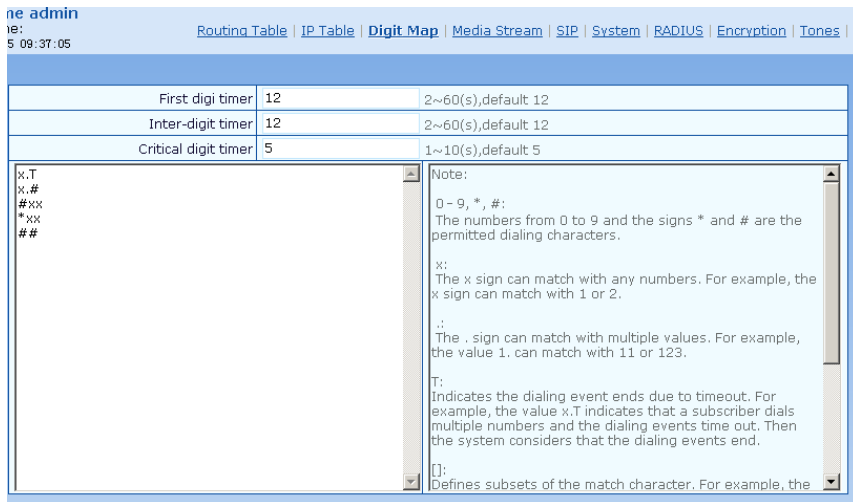
This table is designed to ensure the safe use of gateways. Administrators can add the authorized IP addresses to this table, and the gateways will only process the information from authorized IP addresses. If the IP table is empty, the gateways will not perform IP address-based message filtering.

For example: the gateway will only process the messages from 202.96.209.133 after adding 202.96.209.133 to its IP table.

## 4.5.4 Digit Map

After login, click “Advanced > Digit Map” tab to open the dialing rules interface as shown in Figure4-9.

Figure4-9 Configuration Interface for Digit Map



Dialing 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 dialing rules can help to reduce the connection time of telephone calls.

The maximum number of rules that can be stored in gateways is 60. Each rule can hold not more than 32 numbers and 38 characters. The total length of dialing rules table (the total length of all dialing rules) cannot be more than 2280 bytes.

The following provides a description of typical rules:

Table4-12 Description of Digit map

Digit map	Description
First digit timer	If a subscriber hasn't dialed any number within a specified time by this parameter after offhook, the gateways will consider that the subscriber has given up the call and prompt to hang up in busy tone. Unit: second, default value: 12 seconds.
Inter-digit timer	If a subscriber hasn't dialed the next number key from the time of dialing the last number key to the set time by this parameter, the gateways will consider that the subscriber has ended dial-up and call out the dialed number. The default value is 12 seconds, unit: second.
Critical digit timer	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 hasn't dialed the next number within a set time by this parameter (eg. 5 seconds), the gateways will consider that the subscriber has ended dial-up and call out the dialed number 021. The default value is 5 seconds, unit: second.

Digit map	Description
“x”	Represents any number between 0-9. The x sign can match with any numbers. For example, the x sign can match with 1 or 2.
“.”	Represents more than one digit between 0-9. The . sign can match with number with any length. For example, the value 1. can match with 11 or 123.
“##”	End after receiving two-digit dialing “##”. “##” is a special dialing for users to receive gateway IP address and version number of firmware by default.
“x.T”	The gateways will detect any length of telephone number starting with any number between 0-9. The gateways will send the detected number when it has exceeded the dialing end time set in system parameter configuration and hasn't received a new number.
“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.
“*xx”	End after receiving * and any two-digit number. “* xx” is primarily used to activate function keys for supplementary services, such as CRBT, Call Transfer, Do not Disturb, etc.
“#xx”	End after receiving # and any two-digit number. “#xx” is primarily used to stop function keys for supplementary services, such as CRBT, Call Transfer, Do not Disturb, etc.
[2-8]xxxxxx	A 7-digit number starting with any number between 2-8, used to end the dialing.
02xxxxxxxx	A 11-digit number starting with 02, used to end the dialings starting with “02”.
13xxxxxxxx	A 11-digit number starting with 13, used to end the dialings.
11x	A 3-digit number starting with 11, used to end the special service calls.
9xxxx	A 5-digit number starting with 9, used to end special service calls.

#### 4.5.5 Media Stream

After login, click the label of “Advanced > Media Stream” to open this interface.

Figure4-10 Media stream configuration interface

18:05 09:37:05 [Routing Table](#) | [IP Table](#) | [Digit Map](#) | [Media Stream](#) | [SIP](#) | [System](#) | [RADIUS](#) | [Encryption](#) | [Tones](#)

Voice	
Min.RTP port	10010 3000~65535
Max.RTP port	10250 3020~65535
iLBC payload type	97 97~127, default 97
G.723.1 rate	6300(bit/s)
TOS bits	0x0C Normally 0x0C
Min.jitter buffer	3 0~30(frame), default 3. Higher value results in more delay, set the value with caution
Max.jitter buffer	50 10~250(frame), default 50. Higher value results in more delay, set the value with caution
RTP drop SID	<input type="checkbox"/>
Enable VAD	<input checked="" type="checkbox"/>
RTP destination address	<input checked="" type="radio"/> From SDP global connection <input type="radio"/> From SDP media connection
FoIP	
	<input checked="" type="radio"/> T.38 <input type="radio"/> T.30
Jitter buffer	250 0~1000(ms), default 250
Receiving port for FoIP	<input type="radio"/> Open a new port <input checked="" type="radio"/> Use original voice port
ECM	<input type="checkbox"/> Error Correction Mode
Receive gain	-6(dB)
Transmit gain	0(dB)
Packet size	30(ms)
Redundancy	4

Table4-13 Media stream configuration parameter

Title	Explanation
Min. RTP port	The minimum value of UDP ports for RTP transmission and receiving, and the parameter must be greater than or equal to 3000. This field must be filled in.  Note: each phone call will occupy RTP and RTCP ports. If the gateway is equipped with 4 subscriber lines (or trunk line), then at least 8 UDP ports are needed.
Max. RTP port	The maximum values of UDP ports for RTP's transmission and receiving.  This field must be filled in. It's advisable to be greater than or equal to "2× number of lines + min. RPT 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. The optional parameters are followings: <ul style="list-style-type: none"> <li>• 5300: the Bit rate is 5.3k per second;</li> <li>• 6300: the Bit rate is 6.3k per second</li> </ul>
TOS bits	This parameter specifies the quality assurance of services with different priorities. The factory setting is 0x0C. For the mapping between the level that has no reliability requirement and the TOS value, seeTable4-14.
Min. Jitter buffer	RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This default value is 3. Higher value of this parameter could result in longer delay, therefore, it should be set with caution.
Max. Jitter buffer	RTP Jitter Buffer helps to reduce the influence brought by network jitter. The default value is 50.

Title	Explanation
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 un conformity to the specifications. Nonstandard RTP SID data 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.
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". <ul style="list-style-type: none"><li>• From SDP global connection: Obtain the IP address from SDP global connection;</li><li>• From SDP media connection: Obtain the IP address from SDP Media Description.</li></ul>
FoIP	
	Select fax mode: T.38 or T.30
Jitter buffer	Set the extent of T.38 jitter buffer, and the default is 250. The valid range is 40 ~ 1000 in milliseconds.
Receiving port for FoIP	Set whether to open a new port when the gateway is switching to T.38 mode, and by default, original voice port will be used. <ul style="list-style-type: none"><li>• Open a new port: Use the new RTP port;</li><li>• Use original voice port: Use the original RTP port that created on call set.</li></ul>
ECM	Determine whether to use corrective mode of fax. By default, it is not selected.
Receive gain	Set the receiving gain of T.38 fax, with the default of -6dB.
Transmit gain	Set the transmission gain of T.38 fax, with the default of 0dB.
Packet size	Set the packet size of T.38. 30 milliseconds is the default value.
Redundancy	Set the number of the redundant frames in T.38 data package, default is 4.

Table4-14 Mapping between the reliability requirement and the TOS value

Level	TOS Value (High Delay and High Throughput)	TOS Value (Low Delay and Low Throughput)	TOS Value (Low Delay and High Throughput)
0	0x08	0x10	0x18
1	0x28	0x30	0x38
2	0x48	0x50	0x58
3	0x68	0x70	0x78
4	0x88	0x90	0x98
5	0xA8	0xB0	0xB8
6	0xC8	0xD0	0xD8
7	0xE8	0xF0	0xF8

## 4.5.6 SIP related configuration

The SIP messages consist of request message and response message. Both include SIP message header field and SIP message body field. SIP message header mainly describes the message sender and receiver; SIP message body mainly describes the specific implementation method of the dialog.

**Message of request:** the SIP message sent by a client to the server, for the purpose of activating the given operation, including INVITE, ACK, BYE, CANCEL, OPTION and UPDATE etc.

**Message of response:** the SIP message sent by a server to the client as response to the request, including 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses.

**Message header:** Call-id.

**Parameter line:** Via, From, To, Contact, Csq, Content-length, Max-forward, Content-type, White Space, and SDP etc.

WSS gateways provide good flexibility in content setting in order to improve the compatibility with the platform.

After login, click the label of “Advanced > SIP” to open this interface.

Figure4-11 SIP related configuration interface

SIP related configuration	
MWI subscription	86400 RFC3842: 60~172800(s), default: 86400. Also see "Subscribe MWI" in page "Line > Feature"
PRACK	<input type="checkbox"/> RFC3262
Session timer	<input type="checkbox"/> RFC4028
Session interval	1800 Max 10 digits, default: 1800(s)
Minimum timer	1800
Request/Response Configure	
Contact field in REGISTER	<input checked="" type="radio"/> NAT IP address <input type="radio"/> LAN IP address
Domain name in REGISTER	<input checked="" type="radio"/> Domain name <input type="radio"/> Subdomain name
Via field	<input checked="" type="radio"/> NAT IP address <input type="radio"/> LAN IP address
To field	<input checked="" type="radio"/> Subdomain name <input type="radio"/> Outbound proxy
Address in Call ID field	<input type="radio"/> Host name <input checked="" type="radio"/> Local IP address
Called party number	<input checked="" type="radio"/> From <b>Request Line</b> field <input type="radio"/> From <b>To</b> field
Calling party number in call transfer	<input type="radio"/> Originating number <input checked="" type="radio"/> Forwarding number
Replace 18X with 180	<input type="radio"/> Send 180 <input checked="" type="radio"/> Send 18x
Do not validate Via	<input checked="" type="checkbox"/>
Register upon invite timeout	<input type="checkbox"/>

Table4-15 SIP related configuration parameter

Title	Explanation
SIP related configuration	
MWI subscription	The default is 86400 seconds. The gateway will send platform a message to confirm that has subscribed MWI service at intervals of the time period set here. This parameter should be used in conjunction with voice mail subscription on the page of subscriber line.
PRACK	Determine whether to activate Reliable Provisional Responses. (RFC 3262)
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, 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.

Title	Explanation
Request/Response Configure	
Contact field in REGISTER	<p>Choose the registration mode of gateway under LAN traversal circumstance, the default is “NAT IP Address”.</p> <ul style="list-style-type: none"> <li>• LAN IP address: Keep original content of “Contact” when register;</li> <li>• NAT IP address: Use the NAT information returned by registration server.</li> </ul>
Domain name in REGISTER	<p>The default is “Domain name”.</p> <ul style="list-style-type: none"> <li>• Domain name: Complete domain name used for registration (for example: <a href="mailto:8801@registrar.realtone.com">8801@registrar.realtone.com</a>);</li> <li>• Subdomain name: Only use the common part of the name of domain (for example: <a href="mailto:8801@realtone.com">8801@realtone.com</a>).</li> </ul>
Via field	Choose whether to use NAT IP address or LAN IP address for “Via” header field value, the default is “NAT IP address”.
To field	Choose whether to apply Domain name or Outbound proxy to “To” header field, the default is “Domain name”.
Address in Call ID field	Choose whether to fill Call ID field with host name or local IP, the default is “local IP address”.
Called party number	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	<p>Under call forwarding, the calling party number sent can be choose from Originating number or Forwarding number being set for sending, the default is “Forwarding number”.</p> <p>For example: the subscriber line 2551111 on the gateway activates call forwarding feature and set the destination to 3224422. When caller with 1305553333 calls 2551111, the call will be forwarded to 3224422:</p> <ul style="list-style-type: none"> <li>• if choose “Originating number”, the number 1305553333 will be sent to 3224422 as calling party number;</li> <li>• if choose “Forwarding number”, the number 2551111 will be sent to 3224422 as calling party number;</li> </ul>
Replace 18X with 180	<ul style="list-style-type: none"> <li>• Send 180: If this parameter is set to Enable, the WSS100-TG will map all alerting messages (ALERTING with and without in-band indicator) to 180. An example of when this parameter would be Enabled is when an IAD does not support a 183 message.</li> <li>• Send 18x: If this parameter is set to Enable, the 18x message will be sent.</li> </ul>
Do not validate Via	Set whether to ignore Via field, By default, Via is ignored.
Register upon INVITE timeout	Set whether to activate registration when SIP message of INVITE is failed or time expired, and by default, re-registration is not selected.

#### 4.5.7 System

After login, click the label of “Advanced > System” to open this interface.

Figure4-12 Interface of system advanced configuration

System	
<a href="#">Routing Table</a>   <a href="#">IP Table</a>   <a href="#">Digit Map</a>   <a href="#">Media Stream</a>   <a href="#">SIP</a>   <b>System</b>   <a href="#">RADIUS</a>   <a href="#">Encrypt</a>	
5 09:37:05	
NAT	
NAT traversal	Dynamic NAT ▼
Refresh period	60 <small>more than 14 s,default 60</small>
SDP address	<input type="radio"/> NAT IP address <input checked="" type="radio"/> Local IP address
Session border proxy	
Server	<small>e.g. 201.30.170.38:1020 or sbc.com:1020</small>
Signaling port	4660 <small>1~65535,default 4660</small>
RTP traverse	
Enable	<input checked="" type="checkbox"/>
Remote management	
Remote management	EMS ▼
Primary server	<small>e.g. 222.157.13.71</small>
Secondary server	<small>e.g. 222.157.13.73</small>
Log level	4
Message retransfer interval	3
Registration period	15
Status update period	900

Table4-16 Parameters of system advanced configuration

Title	Explanation
NAT	
NAT traversal	Gateways support several mechanisms for NAT traversal. 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 or STUN 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 and STUN 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. <ul style="list-style-type: none"> <li>• NAT IP Address: Apply NAT address into the transmitted SDP;</li> <li>• Local IP Address: Apply the gateway's IP address into the transmitted SDP.</li> </ul> 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 WAN address should be filled in this field, which will be used in SDP. 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.
STUN server	Set the IP or domain name of STUN server. No default value. If the set is empty, the gateway will adopt the STUN server address configured at factory. When choosing STUN for NAT traversal, the gateway will carry out STUN operation periodically according to the configured interval time of NAT refresh.

Title	Explanation
RTP Receiving Port	<p>The gateways will send the RTP receiving port selected here to the remote side.</p> <ul style="list-style-type: none"> <li>• NAT port: Use NAT mapped port, which is obtained through STUN, for example;</li> <li>• Local port: Use local SIP and RTP port.</li> </ul>
Session border proxy	
Server	<p>Set the IP address and port number of session border proxy server. The character of “:” must be used between IP address and port number.</p> <p>Server address could be set into IP address or domain name. When domain name is used, “DNS service” must be activated as shown in the page of “Configure network parameter”, and “DNS server” must be configured. Examples: 201.30.170.38:5060 and “softswitch.com:5060”.</p>
Signaling port	<p>Signaling port value of the gateway, the default value is 4660. Signaling port number could be set at will, but can not conflict with other ports of equipment.</p>
RTP traversal	
Enable	<p>When this is selected, the address of the received RTP packets will be used as the IP address for sending RTP packets.</p>
Remote management	
Remote management	<p>The gateways support EMS which is a centralized gateway management server provided by New Rocj, and Auto-provision.</p>
EMS	
Primary server	<p>User needs to enter the IP address and port of EMS server for activating EMS service.</p>
Secondary server	<p>User needs to enter the IP address and port of standby EMS server for activating EMS service. EMS server address could be set into IP or domain name according to the user’s requirement. If adopt domain name as the address, the user should activate the “DNS service” as shown in the page of “Configure network parameter”, and configure the parameter(s) of “DNS server”. The complete and valid configurations are exemplified as: 201.30.170.38:5060 and “softswitch.com:5060”.</p>
Log level	<p>Gateway sends the log file level to EMS server, and the default value is 4. The parameter is controlled by EMS server, and users should not make any modification.</p>
Message retransfer interval	<p>This is the retransmission counter for message transmitting between the gateway and EMS server. The default is 3. The parameter is set by EMS server, and users should not make any modification.</p>
Registration period	<p>Gateways will perform registration to the EMS server periodically based on the time interval set here. With second as unit, default is 15. The parameter is set by EMS server, and users should not make any modification.</p>
Auto provision	
Server	<p>Gateways may download software upgrade packages and configuration files automatically through auto-provision server. Once the auto provision is selected, you have to enter the IP address of ACS here.</p>



## 4.5.8 Radius call logs

After login, click the label of “Advanced > RADIUS” to open this interface.

Figure4-13 Configuration interface of Radius call logs

<a href="#">Routing Table</a>   <a href="#">IP Table</a>   <a href="#">Digit Map</a>   <a href="#">Media Stream</a>   <a href="#">SIP</a>   <a href="#">System</a>   <b><a href="#">RADIUS</a></b>   <a href="#">Er</a>		
Primary server	<input type="text"/>	e.g. 223.155.21.15:1813
Key	<input type="text"/>	
Secondary server	<input type="text"/>	e.g. 223.055.21.16:1813
Key	<input type="text"/>	
Retransmit timer	<input type="text" value="3"/>	1~10(s), default 3
Retransmit times	<input type="text" value="3"/> ▼	
Trigger	<input checked="" type="radio"/> IP side <input type="radio"/> IP and TDM side	
Request conditions	<input type="checkbox"/> Outbound <input type="checkbox"/> Inbound <input type="checkbox"/> Answered <input type="checkbox"/> Unanswered	

Table4-17 Configuration parameter of Radius call logs

Title	Explanation
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 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	<ul style="list-style-type: none"> <li>• IP side: when this is selected the call information on the SIP side will be sent to the Radius server.</li> <li>• IP and TDM side: when this is selected the call information on the SIP side as well as on the ISDN side will be sent to the Radius server.</li> </ul>

Title	Explanation
CDR type	<ul style="list-style-type: none"> <li>• Outbound: Set whether to send RADIUS charge message for outbound calls;</li> <li>• Inbound: Set whether to send RADIUS charge message for inbound calls;</li> <li>• Answered: Set whether to send RADIUS charge message when calls are connected;</li> <li>• Unanswered: Set whether to send RADIUS charge message for unanswered calls.</li> </ul>

## 4.5.9 Encryption

After login, click the label of “Advanced > Encryption” to open this interface.

Figure4-14 Encryption configuration interface

Singnal encrypt	<input type="checkbox"/>	
T.38 encrypt	<input type="checkbox"/>	
RTP encrypt	0	You may obtain it from service provider
Encryption method	7	You may obtain it from service provider
Encryption key		You may obtain it from service provider

Table4-18 Encryption configuration parameters

Title	Explanation
Singnaling encrypt	Choose whether to encrypt signaling. By default, this is not selected.
T.38 encrypt	Choose whether to encrypt T38 data. By default, this is not selected.
RTP encrypt	<p>Choose whether to encrypt RTP voice pack, the default is “0”</p> <ul style="list-style-type: none"> <li>• 0: None (not to activate);</li> <li>• 1: RTP (fully encryption to RTP package);</li> <li>• 2: RTP Header (only encrypt RTP header);</li> <li>• 3: RTP Body (only encrypt RTP payload);</li> <li>• 13: Encrypt with Realtone specific algorithm.</li> </ul>

Title	Explanation
Encryption mode	<p>Set the gateway encryption method, default is 7. The optional parameters as below:</p> <ul style="list-style-type: none"> <li>• 2: TCP Not Encrypted;</li> <li>• 3: TCP Encrypted;</li> <li>• 6: UDP Not Encrypted;</li> <li>• 7: UDP Encrypted (Real tone) ;</li> <li>• 8: Using Keyword;</li> <li>• 9: Using Keyword2;</li> <li>• 10: RC4;</li> <li>• 11: Using Keyword 3;</li> <li>• 12: Encrypt12;</li> <li>• 13: Encrypt13;</li> <li>• 14: Encrypt14 (Real tone) ;</li> <li>• 16: Word Reverse;</li> <li>• 17: Word Exchange (263) ;</li> <li>• 18: Byte Reverse;</li> <li>• 19: Byte Exchange.</li> </ul>
Encryption key	You may obtain it from service provider

#### 4.5.10 Call progress tone plan

After login, click the label of “Advanced > Tones” to open this interface.

Figure4-15 Call progress tone configuration interface

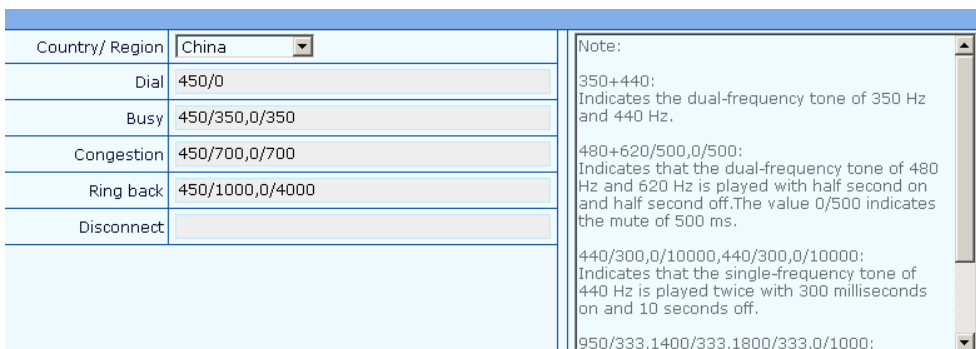


Table4-19 Call progress tone configuration parameters

Title	Explanation
Country/region	<p>There are progress tone plans for several countries and regions which are pre-programmed in gateways. Users may also specify the tone plan according to the national standard. Gateways provide tone plan for the following countries and regions:</p> <p>China; the United States; France; Italy; Germany; Mexico; Chile; Russia; Japan; South Korea; Hong Kong; Taiwan; India; Sudan; Iran; Algeria; Pakistan; Philippines; Kazakhstan;</p>

Title	Explanation
Dial	Prompt tone of off-hook dialup
Busy	Used for busy line prompt
Congestion	Used for notification of call set up failure due to resource limit
Ring back	The prompt tone sent to caller when ring
Disconnect	Used for reminding the subscriber of off-hook and no dialup status of the phone

Here are examples which illustrate the rules of defining call progress tone.

- 350+440  
Indicates the dual–frequency tone consisting of 350 and 440 Hz
- 480+620/500,0/500  
Indicates the dual–frequency tone consisting of 480 and 620 Hz, repeated playing with 500 milliseconds on and 500 milliseconds off. Note: 0/500 indicates 500 milliseconds mute.
- 440/300,0/10000,440/300,0/10000  
Indicates 440 Hz single frequency tone, repeated playing 2 times in terms of 300 milliseconds on and 10 seconds off.
- 950/333,1400/333,1800/333,0/1000  
Indicates repeated playing 333 milliseconds of 950 Hz, 333 milliseconds of 1400 Hz, 333 milliseconds of 1800 Hz, and mute of 1 second

## 4.6 Status

### 4.6.1 ISDNn

After login, click “Status > ISDNn” tab to open the configuration interface.

Figure4-16 ISDN Status Interface

Channel	Call	Direction	Phone No.(This End)	Phone No.(Other End)	Duration	Operation
1	Active	SIP->ISDN	29	629	69	<a href="#">Details</a>
2	Idle					-
3	Idle					-
4	Idle					-
5	Active	SIP->ISDN	04	604	87	<a href="#">Details</a>
6	Active	SIP->ISDN	05	605	87	<a href="#">Details</a>
7	Active	SIP->ISDN	06	606	86	<a href="#">Details</a>
8	Active	SIP->ISDN	07	607	86	<a href="#">Details</a>
9	Active	SIP->ISDN	08	608	85	<a href="#">Details</a>
10	Active	SIP->ISDN	09	609	85	<a href="#">Details</a>
11	Active	SIP->ISDN	10	610	85	<a href="#">Details</a>
12	Active	SIP->ISDN	11	611	84	<a href="#">Details</a>
13	Active	SIP->ISDN	12	612	84	<a href="#">Details</a>
14	Active	SIP->ISDN	13	613	83	<a href="#">Details</a>
15	Active	SIP->ISDN	14	614	83	<a href="#">Details</a>
17	Active	SIP->ISDN	15	615	83	<a href="#">Details</a>
18	Active	SIP->ISDN	16	616	82	<a href="#">Details</a>
19	Active	SIP->ISDN	17	617	82	<a href="#">Details</a>
20	Active	SIP->ISDN	18	618	82	<a href="#">Details</a>
21	Active	SIP->ISDN	19	619	81	<a href="#">Details</a>
22	Active	SIP->ISDN	20	620	80	<a href="#">Details</a>
23	Active	SIP->ISDN	21	621	79	<a href="#">Details</a>
24	Active	SIP->ISDN	22	622	78	<a href="#">Details</a>
25	Active	SIP->ISDN	23	623	77	<a href="#">Details</a>

## 4.7 Log management

### 4.7.1 System status

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

- 1) The information about login of interface (including IP address and jurisdiction of the user);
- 2) SIP registration status;
- 3) Call related signaling and media (RTP) information;

After login, click the label of “Logst > System Status” to open this interface.

```

Basic      ISDN      Advanced   Status     Logs       Tools      Info
-----
Home view
Time: 15:09:58:05
System Status | Call Message | ISDN Status | System Startup | Manage Log | L

Login User Info >>>>>
1) 192.168.250.2  1
2) 192.168.250.10 3

SIP Registration Info >>>>>
---- not enabled ----

Call Context Info >>>>>
66) 5043 67 SIP->ISDN 192.168.2.90:10205 10142 PCMA/20 1/3/1 ACTIVE 40->640
67) 5044 68 ISDN->SIP 192.168.2.88:6000 10144 PCMU/20 1/4/1 ACTIVE 40->640
68) 5045 69 SIP->ISDN 192.168.2.90:10209 10146 PCMA/20 1/3/2 ACTIVE 41->641
69) 5046 70 ISDN->SIP 192.168.2.88:6000 10148 PCMU/20 1/4/2 ACTIVE 41->641
70) 5047 71 SIP->ISDN 192.168.2.90:10213 10150 PCMA/20 1/3/3 ACTIVE 42->642
71) 5048 72 ISDN->SIP 192.168.2.88:6000 10152 PCMU/20 1/4/3 ACTIVE 42->642
72) 5049 73 SIP->ISDN 192.168.2.90:10217 10154 PCMA/20 1/3/4 ACTIVE 43->643
73) 504A 74 ISDN->SIP 192.168.2.88:6000 10156 PCMU/20 1/4/4 ACTIVE 43->643
74) 504B 75 SIP->ISDN 192.168.2.90:10221 10158 PCMA/20 1/3/5 ACTIVE 44->644
75) 504C 76 ISDN->SIP 192.168.2.88:6000 10160 PCMU/20 1/4/5 ACTIVE 44->644
76) 504D 77 SIP->ISDN 192.168.2.90:10225 10162 PCMA/20 1/3/6 ACTIVE 45->645
  
```

Table4-20 Parameters of system status

Title	Explanation
Login User Info	<p>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.</p> <p>When more than one administrator log in at the same time, the first login’s jurisdiction is 1, others are 3; also, when more than one operators log in at the same time, the first one’s jurisdiction is 2, others are 3.</p> <p>For example:            Login User Info &gt;&gt;&gt;&gt;&gt;            1) 192.168.2.247 1</p>

Title	Explanation
SIP Registration Info	<p>Show registration status:</p> <ul style="list-style-type: none"> <li>• Not enabled: The registration server's address is not entered yet;</li> <li>• Latest response: The latest response message for the registration. 200 means registered successfully;</li> <li>• No response: Not received 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.</li> </ul> <p>For example:</p> <pre>SIP Registration Info &gt;&gt;&gt;&gt; ---- Not enabled ---- SIP Registration Info &gt;&gt;&gt;&gt; Contact: &lt;sip:2681403@220.234.27.70:1003; user=phone&gt;         latest response: 200 (timeout-555) Contact: &lt;sip:2681402@220.234.27.70:1003; user=phone&gt;         latest response: 200 (timeout-555)</pre>
Call Context Info	Show the call status.
Rtp Context Info	<p>Show the voice channel related to the calls.</p> <p>For example:</p> <pre>Rtp Context Info &gt;&gt;&gt;&gt; 3) created, call =e011</pre>

## 4.7.2 Call message

After login, click the label of “Logs > Call Message” to open this interface.

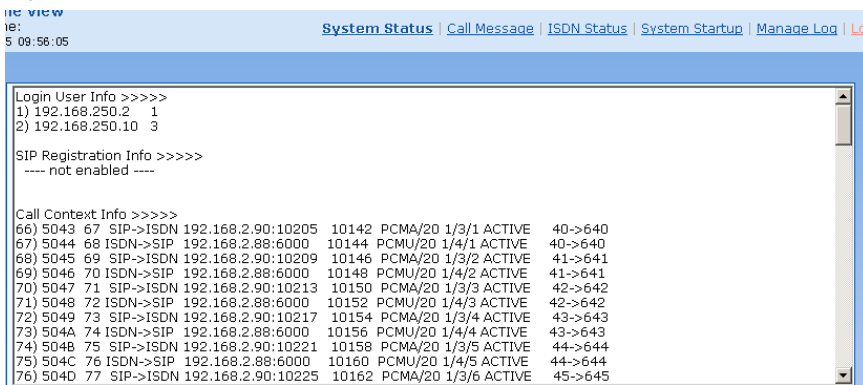
Figure4-17 Call message interface



## 4.7.3 ISDN status

After login, click the label of “Logs > ISDN Status” to open this interface.

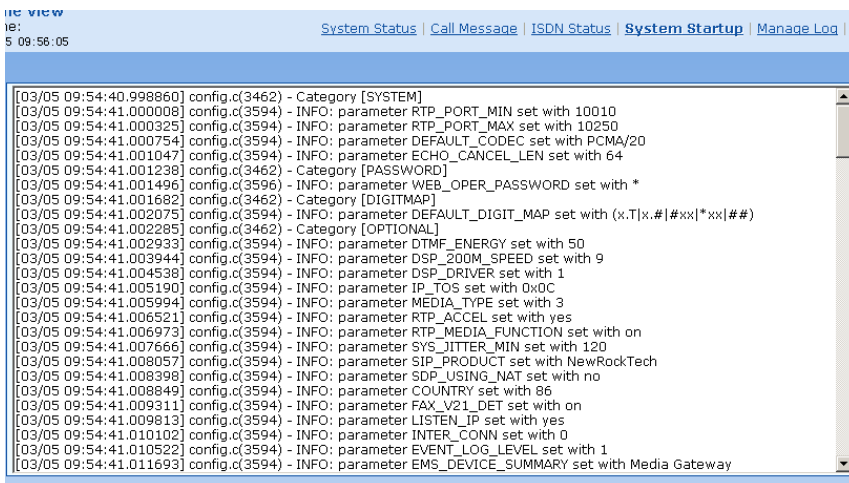
Figure4-18 Interface of ISDN status



#### 4.7.4 System Startup

After login, click the label of “Logs > System Startup” to open this interface. The gateway boot up information is available in this page, including the hardware configuration.

Figure4-19 Interface of system startup



#### 4.7.5 Manage log

After login, click the label of “Logs > Manage Log” to open this interface. Log files can be downloaded through this interface.

Figure4-20 Interface of debugging log management

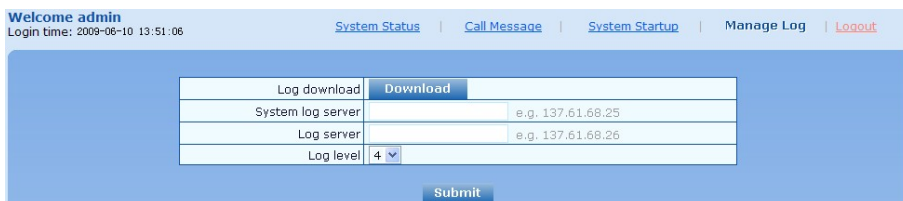


Table4-21 Configuration parameters of debugging log management

Title	Explanation
Log download	See the description below.
System log server	Set the IP address of system log server.

Title	
Log server	IP address of debugging log server.
Log level	Select the log file level of gateway, default is 3. The setting range is 1 ~ 5, the higher the level goes, the more details the log file will be. Note: log level should be set to be 3 or lower when gateway is used in normal operation, avoiding influencing the system performance.

Procedure of downloading the debugging log:

Step 1: Click “download”, the gateway starts pack the logs.

Step 2: After few seconds, the interface of log save will appear.

Step 3: click “Save”, and select path to save.

Step 4: The user may review the log from the server concerned.



## WARNING

The procedure of downloading log files described hereof is only applicable to release 1.9.x.238 of WSS series or updated version of software.

## 4.8 System tool

### 4.8.1 Change password

After login, click the label of “Tools” to open this interface. Only administrator is entitled to change the password of login.

For changing administrator password, it’s required to enter new password into “New password” field and “Confirm new password” field, then click “Submit”.

The password being used by operator will be displayed as hidden codes, which could be changed by administrator at any time. The administrator is allowed to change the operator’s password by entering new password into “Operator password>password”.

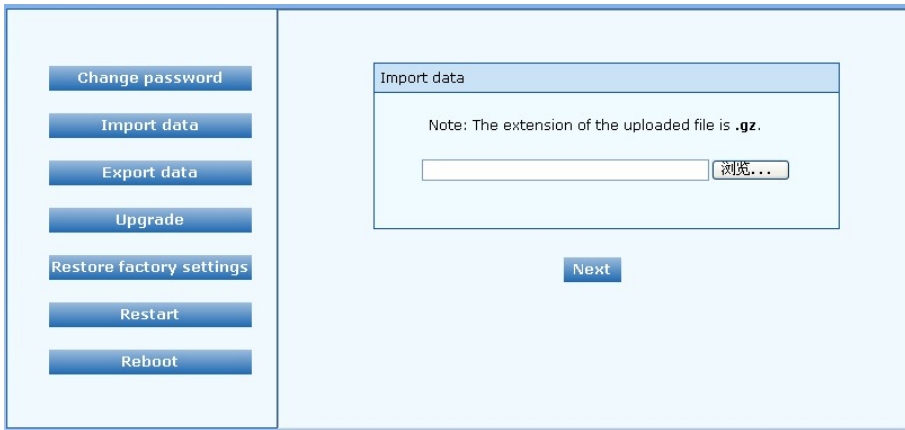
Figure4-21 Interface of password changing

### 4.8.2 Configuration import

After login, click “Tools>Import data” to open this interface. Operating procedure is the same as that of “software upgrade”.



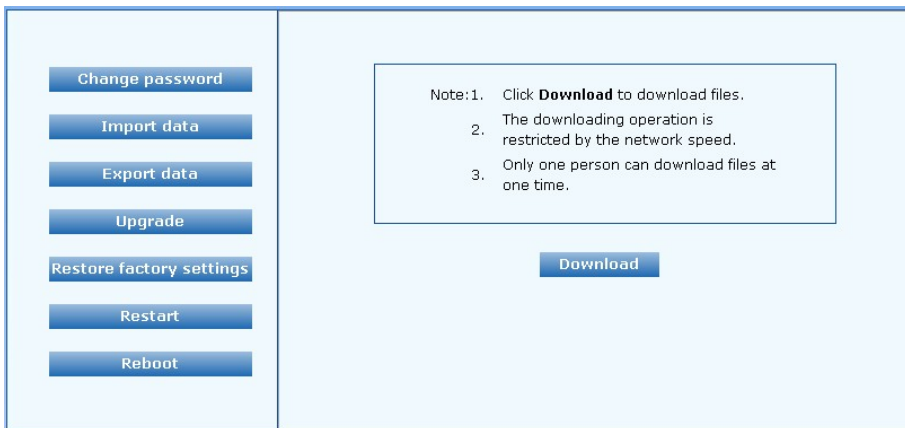
Figure4-22 Interface of import data



### 4.8.3 Configuration export

After login, click “Tools >Export of configuration” to open this interface. It’s allowed to download the configuration files from the gateway through this interface. The downloading procedure is similar to the downloading procedure of log files..

Figure4-23 Interface of export data



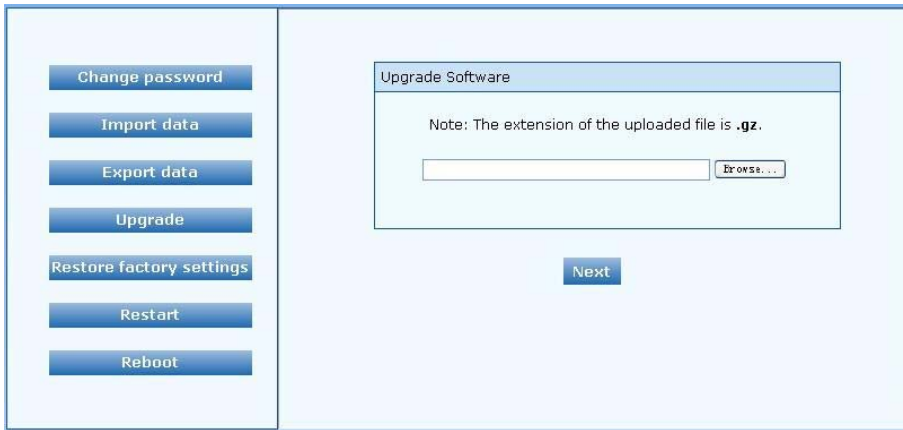
### 4.8.4 Software upgrade

After login, click “Tools > Upgrade” to open this interface. The software upgrading procedure is presented as below:

Step 1: Obtain the upgrade files (tar.gz file), and save the file onto a local computer.

Step 2: Click “System tool > software upgrade” to access to the page of software upgrade.

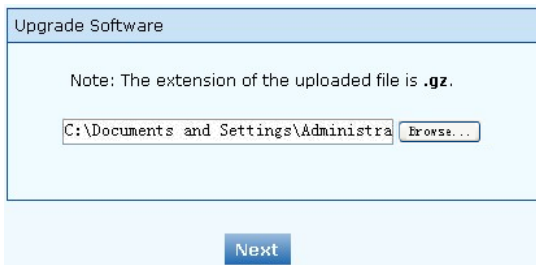
Figure4-24 Interface of software upgrade



Step 3: Click “Browse” to select the upgrade files and click “Open”.

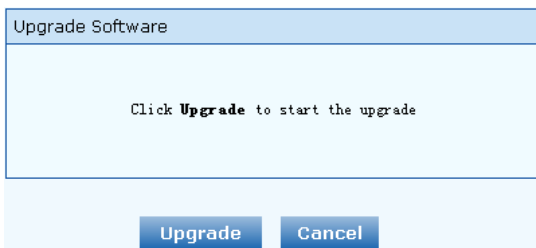
Step 4: Click “Next” when the following interface appears, and start uploading the upgrade files to the gateway.

Figure4-25 Interface of file upload



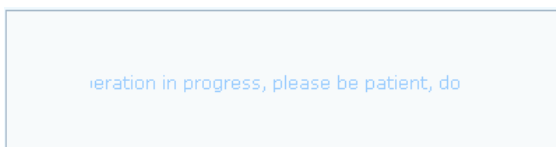
Step 5: Uploading will be completed in about 30 seconds, and click “Upgrade” on following dialog.

Figure4-26 Upgrade interface



Step 6: The following prompt appears during the upgrade.

Figure4-27 Prompt of upgrade process





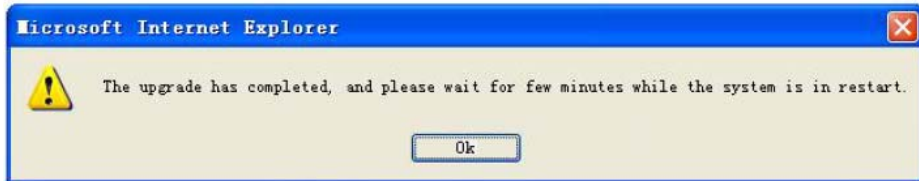
## WARNING

A few minutes are needed to upgrade the gateway. Don't operate the gateway during this period.

---

Step 7: After success in upgrade, the following dialog will appear, click "Confirm".

Figure4-28 Interface of successful upgrade



Step 8: The gateway will reboot, and the interface will be disappeared.

Step 9: Wait for about 2 minutes, and access to the interface of gateway management system, click "Info" and check the software version.



## WARNING

For WSS100 and WSS120 gateways, the software upgrade operation must be conducted on an 100M Ethernet port.

---

### 4.8.5 Software restart

After login, click "Tools > Restart" to restart the gateway, making modified configuration come into effect.



## CAUTION

In most cases, there is no need to reset the gateway, and the modified parameters will come into effect upon confirming the "submit".

---

### 4.8.6 System reboot

After login, click "Tools > Reboot" to restart the gateway. As this is a system wide reset, it takes longer time.



## CAUTION

Generally, it's sufficient to restart software when the gateway confirms to reset; the system reboot will be required only when network settings of the gateway are changed.

---

### 4.8.7 Restore factory settings

After login, click "Tools > Restore factory settings" 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.

## 4.9 Version information

After login, click “Info” to view the gateway hardware and software version information.

Welcome admin  
Login time: 2010-03-08 18:23:59

Software version	Rev 1.9.81.289
Hardware version	Rev 1.1.2 M100
Kernel version	Kernel 8.3.4.14 (F)
DSP version	Rev 1.8.193

## 4.10 Logout

After login, click the “Logout” at top right to exit the gateway management system and return to the login interface.