LVswitch IPPBX800
User Manual

Version

ii

Product Version：1.6.0.2

Document Version：A

Contents

1 Product Overview

Summary

This chapter describes LVswitch IPPBX in detail. It describes the appearance, indicator status, interface attributes, and performance of the main board.

1.1 Product Introduction

- LVswitch IPPBX is a IP voice Gateway targeted at office phone applications of small to medium enterprises.

- LVswitch IPPBX supports analog trunk and SIP trunking,Web-based management interface, it provides applications such as home location "One number", multi-level voice navigation and VoIP multi-branch networking to meets the basic voice communications demand of small and medium-sized enterprises.

- LVswitch IPPBX products using softswitch core technology to support local access to analog phones and IP phone users, it can remote access IP phone or IAD analog users through IP bearer network to achieve a mixed networking of analog phone and IP phone; through simulation Trunking and broadband SIP trunking, LVswitch IPPBX products link to PSTN or private network voice switching equipment to improve the efficiency of enterprise deployment and communications, and help enterprises to enhance their value.

- IPPBX 800 can support up to 4FXO,12FXS

1.2 Hardware Specification

item	Description
Network interface	1 WAN,3 LAN,RJ45, rate 10/100/1000MBS
FXS	Channel 1-12 RJ11 port
FXO PORT	4 or 8,RJ11
Console	1,RJ45,115200 bps
USB	1usb 2.0,full speed
Working power	100VAC-240V AC;60/60HZ

CASE	1U,metal material
Power	26w
Dimension(L*W*H)	430*180*44mm
Weight	≦2.6KG
Working Environment	Working environment temperature -6°C-66°C
	Environmental relative humidity ≦96%
	Performance doesn't decrease within 3000m above sea level
	Atmospheric pressure 86KPa-106KPa
	The level of the fine article in the air is less than 180mg/M^3

1.3 Hardware Frame

（1）Front Panel
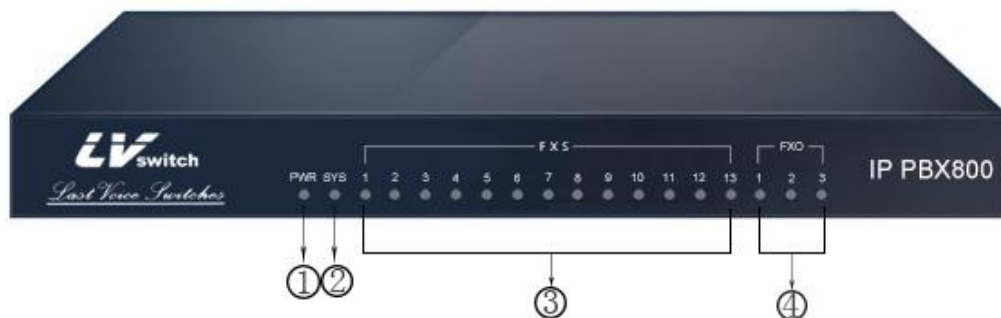
1.Power indicator   2.System indicator 3.FXS indicator 4.FXO indicator

Figure1- 1 LVswitch IPPBX800 Front Panel View

（2）Back Panel
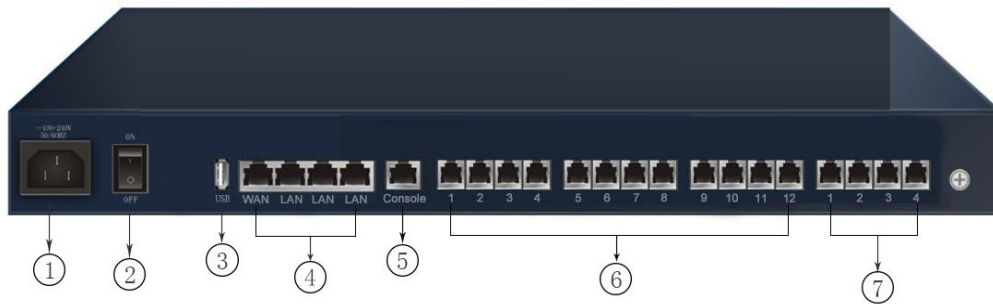
Figure1- 2 LVswitch IPPBX-800 Back Panel View

Indicator

（1）Front Panel Indicator

Table 1- 1 LVswitch IPPBX Front Panel Indicator

Name		Functions
Power Indicator	Power	The light on shows the equipment is working properly. The light off shows the power is off or faulty.
System Status Indicator	Status	Lights solid green to indicate that the system is starting up. Fast blinking green indicates system normal operation. The light is off means the system is not started.

（2）Back panel Interface Introduction

1	Power jack	2	Power switch
3	USB 2.0	4	WAN,LAN1-3
6	CONSOLE	6	12* FXS PORT
7	4*FXO PORT		

Major Boards Intruduction

（1）Ethernet Interface

Table 1- 2 LVswitch IPPBX control board interface

Item	Attributes
WAN	1
LAN	3

Item	Attributes
Console	1

（2）Console Interface

Table1- 5 Console interface Attributes Table

Attributes	Description
Connection Type	RJ45
Port Standard	RS232
Baud Rate	9600bps~116200bps；default 116200bps
Support Service	Connect to the character terminal, Connect to the local PC serial port, and run the terminal emulator command interface on the PC.

（3）Ethernet Interface

The LVswitch IPPBX provides 3 10M / 100M / 1000M GE Ethernet electrical interfaces (1 WAN port and 2 LAN ports, Gigabit Ethernet ports).

Table 1- 3 Gigabit Ethernet interface Attributes

Attributes	Description
Connection Type	RJ45
Interface Type	MD/MDIX adaptive
Support Frame Format	Ethernet_II Ethernet_SNAP
Word mode	10M/100M/1000M adaptive

2　Device Installation

Overall

This chapter describes the preparation work and installation process before equipment installation, including the tools used in the installation process and the specific steps of equipment installation.

2.1　Safety precautions

	In case of thunderstorm,please stop using the equipment, disconnect the power supply and unplug the power cable and telephone line to avoid the equipment being damaged by lightning.		Please place the equipment on a stable working table and place it in a ventilated environment without direct sunlight.
	The equipment must be kept strictly dry during storage, transportation and use. In case of accidental liquid flow into the case, please immediately disconnect the power supply and contact the designated service point.		Please use the power source adaptor and other accessories with the equipment. Please keep the plug clean and dry to avoid electric shock or other hazards. Do not use damaged or aged power cords.
	Do not allow children to use the equipment without supervision; Do not allow children to play with equipment and swallowing.		If there are abnormal phenomena, such as smoke, abnormal sound, peculiar smell, etc., please immediately stop using and disconnect the power

	When installing the equipment, please leave a heat dissipation space above 10cm around and on the top, and keep away from heat sources or exposed fire sources, such as electric heaters and candles		Do not place any object on the device or on the power cord or plug. Please do not cover the vents of the cabinet with objects
	Before cleaning, please stop using the equipment and cut off the power supply. To clean, use a soft, dry cloth to wipe down the equipment enclosure.		Do not disassemble the equipment by yourself. In case of equipment failure, please contact the designated maintenance point.

If the equipment is used for a long time, the shell will have a certain degree of heat. Please do not worry, this is a normal phenomenon, the equipment can still work normally.

2.2 Preparations before installation

2.2.1 Humidity/temperature requirements

In order to ensure the normal operation of equipment, the machine needs to maintain a certain temperature and humidity.

If the relative humidity is too low, the insulation gasket will dry shrink and cause the fastening screw to become loose. In the dry climate, it is also easy to generate static electricity and harm the CMOS circuit.

If the long-term humidity of the machine room is too high, it is easy to cause poor insulation of insulating materials or even electricity leakage.

High temperature is more harmful, because high temperature will accelerate the aging process of insulation materials.

Work environment should satisfy the temperature range: 0 ~ 40 ℃. Relative humidity range: 6 ~ 90% (non-condensation), it is recommended to install temperature and humidity monitoring system in the machine room.

2.2.2 Cleanliness requirements

When indoor dust falling on the body ,it will cause electrostatic adsorption, making the metal connector or metal contact bad, not only will affect the life of the equipment, but also easy to cause communication failure. When indoor relative humidity is low, it is easier to produce this kind of electrostatic adsorption.

Work environment should be dustproof, the concentration of particulates in the air is less than 180 mg /m³, the printer, copier should be placed away from the router cabinet place, so as not to condense the paper, toner equipment.

In addition to dust, the room on the air containing salt, acid, sulfide also has strict requirements, because these harmful gases will accelerate the corrosion of metal and the aging process of some parts.

The limits of other hazardous substances in the machine room are: SO2 less than 0.2mg/m³,H2S less than 0.006mg/m³,NH3 less than 0.06mg/m³,Cl2 less than 0.01mg/m³.

2.2.3 Anti-static requirements of machine room/ persons

The equipment has taken a variety of measures to prevent static electricity, but if the static electricity in the environment exceeds a certain tolerance, it is still easy to damage the circuit and even the whole machine, so in the design of the room environment should also consider the anti-static. Electrostatic induction mainly comes from two aspects: one is the outdoor high-voltage transmission line, lightning and other external electric field; Second, the indoor environment, floor materials, machine structure and other internal systems.

Therefore, in order to prevent electrostatic damage, the machine room/personnel should meet the following anti-static requirements:

- When laying the anti-static floor in the machine room, it shall comply with the technical requirements stipulated by the communication industry. The surface resistance and system resistance are as follows: 1 x $1 \times 10^{6}\Omega$ to $1*10^{9}\,\Omega$.

- Machine room wall and ceiling surface should be smooth, reduce dust. Materials and equipment with anti-static property and good grounding of floor are allowed.

- The worktable, chair and terminal in the machine room shall be anti - static. Mesa electrostatic leakage system resistance and surface resistance are as follows: $1 \times 10^{6}\Omega$ to $1*10^{9}\,\Omega$.

- Maintain appropriate temperature and humidity condition

- Before entering the communication room with anti-static requirements, please wear anti-static clothes and anti-static shoes, and do not change clothes directly in the room. Do not touch or plug PCB components or other components and spare parts without permission or without wearing an anti-static wristband.

- The anti-static cover on the frame (or printed circuit board component), with the frame installed in a fixed position and connected with static ground wire, can be opened.

- Spare PCB components and components for maintenance must be stored on the rack or in an anti-static shielding cabinet/bag.

2.2.4 Anti-magnetic interference requirements

All kinds of interference sources, whether from outside or inside the equipment application system, all affect the equipment in the way of capacitance coupling, inductance coupling, electromagnetic radiation, common impedance (including grounding system) coupling and conductor (power line, signal line and output line, etc.) conduction.

The machine room shall meet the following anti-interference requirements:

- It is necessary to take effective measures to prevent the interference of the power system.

- The working place of the equipment should not be Shared with the grounding device or lightning protection grounding device of the power equipment, and should be as far apart as possible;

- Far away from high-power radio transmitter, radar transmitter, high-frequency high-current equipment;

- Electromagnetic shielding shall be adopted when necessary.

2.2.5 Lightning protection requirements

Although a great deal of consideration and necessary measures have been taken in lightning protection, the equipment may still be damaged when the lightning intensity exceeds a certain range. In order to achieve better lightning protection effect, it is recommended that users:

- Ensure the protective ground of the chassis is in good contact with the ground with protective ground wire.

- Make sure that the ground point of the ac socket is in good contact with the ground.

- It can be considered that to add power arrester at the front of the power input,which can increase the power lightening resistance.

- In order to achieve better lightening protection effect, For the signal line connected to outdoor, such as ISDN line, telephone line, the users can consider adding professional lightning protection device in the input end of the signal cable.

2.2.6 Installation platform requirements

When installing on the installation table, the following conditions shall be ensured:

- Make sure that there is enough space for the inlet and vent of the equipment so as to facilitate the heat dissipation of the equipment chassis

- Make sure the installation table has good ventilation and cooling system..

- Make sure the mounting table is strong enough to support the weight of the equipment and its mounting accessories.

- Make sure the installation table is grounded well.

Other requirements such as shockproof, fireproof, waterproof, moistureproof, theft-proof, flooring, fireproof facilities, grounding system, etc., please strictly comply with the "China telecom data room code", "China mobile data room code", "China unicom computer room standard code".

2.3 Equipment installation flow chart
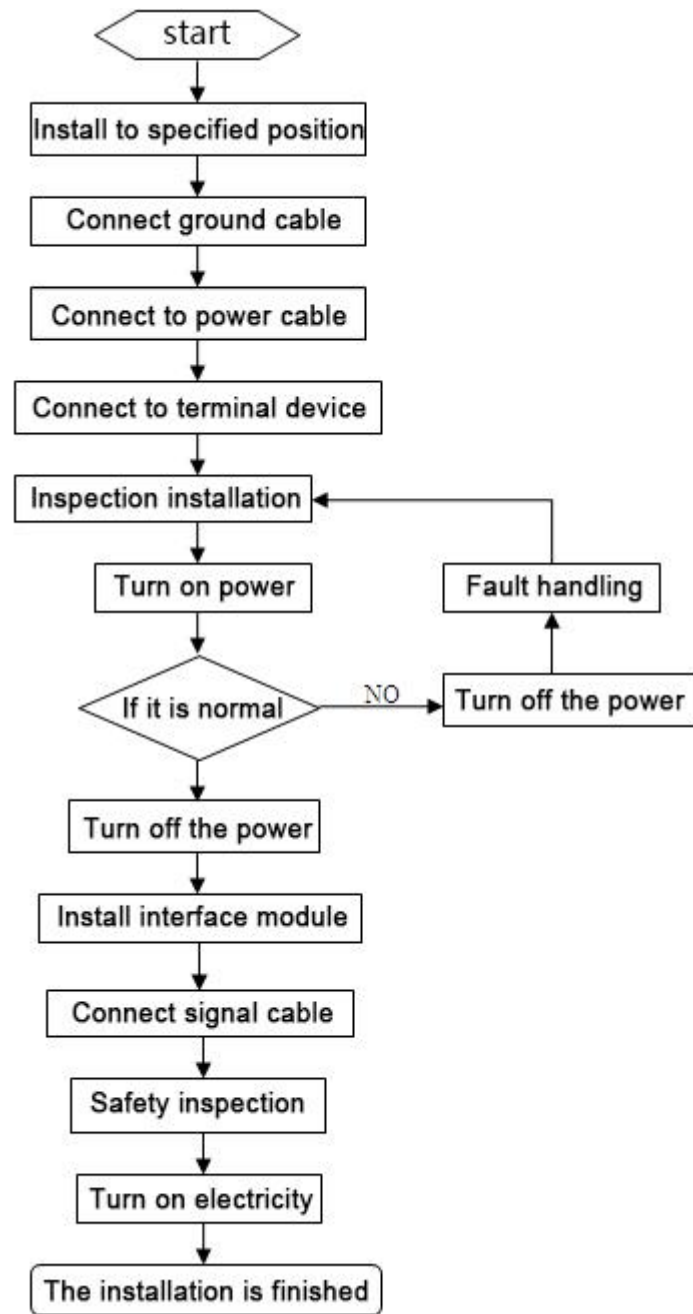
Figure 2-1 Equipment installation flow chart

2.4 Installation tools, equipment and instruments

Before equipment installation, prepare the following basic tools and instruments.

(1) Measuring tools

A tape measure	Tape measure
Generally used for long distance measurement. It is usually used indoors to locate the rack and install the wiring rack	Generally used for long distance measurement. It is used to check and measure the length of the circuit before work.

(2) Crimping tool

Cable clamp	
It is mainly suitable for the production of rj-46 network wire connector and telephone wire connector.	

(3) Essential tools

Card line gun	Vise
The front card cutter is used to insert the cable into the card slot.	Mainly used for clamping and cutting all kinds of wire.

Long nose pliers Mainly used for clamping and cutting all kinds of wire. 	Diagonal cutting pliers Mainly used for clamping and cutting all kinds of wire.
The screwdriver Mainly used for all kinds of screws, screws to disassemble. 	
Medium knife It is usually used when making cables and stripping them. 	Sharp knife A burr, as on the surface of a piece of metal.

2.5 Install the equipment to the specified location

After the preparation and confirmation work is completed, the equipment shall be installed. According to the installation location, it can be divided into the following two situations:

1.Install the equipment directly on the platform.

2.Install the equipment on the cabinet.

2.5.1 Install to work platform

If the customer doesn't have standard cabinet,the normal way is to place the equipment on the clean platform.Pay attentions to the following terms during the operation:

1. Ensure the smooth and good grounding of the work table.

2. Ensure that the mounting table is strong enough to bear the weight of the chassis and cables.

3. There are no other obstacles around the working table.

4. Lift the chassis to a position slightly higher than the work table, and put the chassis on the work table. At least 10cm space is left on the left and right sides of the chassis to ensure the smooth flow of heat dissipation and wind; At least 20cm of space is reserved at the back of the case to ensure the layout and wiring of power lines and user lines.

5. Don't put any heavy things on the device.

⚠ Note：

When installing to the work platform, please use one protector ground cable(PGND cable)to connect the ground terminals and ground wires together.The grounding resistance is less than 6 Ω.

2.5.2 Install to cabinet

Confirm that the installation cabinet has been fixed, the installation position of the cabinet has been arranged, and there are no obstacles affecting the installation of equipment inside and around the cabinet. Check the grounding and stability of the cabinet.

1. The chassis to be installed is ready and transported to a place close to the cabinet for easy handling.

2. Lift the case and slowly transfer it to the installation cabinet.

3. Lift the chassis to a position slightly higher than the rail or slide of the cabinet, put the chassis on the rail or slide and push it into the cabinet.

4. Use the screws that meets the cabinet installation size to fix the equipment on the cabinet through fixed hangers and to keep the equipment horizontal and firm.(The screws size can not be over National standard M6, with rust treatment on the surface)
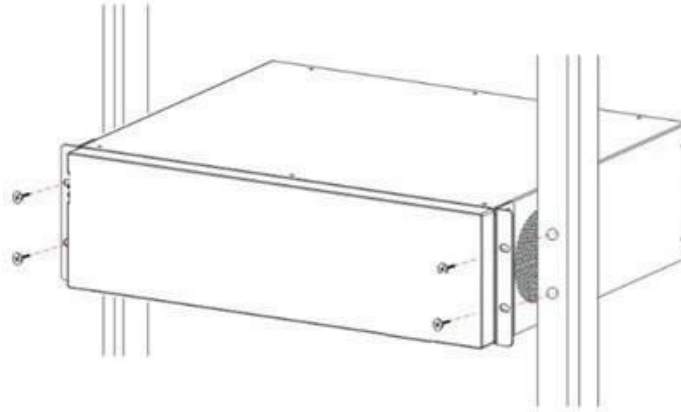
Figure 2-2 Install the equipment to the Cabinet

2.6 Install ground cable

2.6.1 Ground cable installation principles

1.The chassis must be well connected to the ground, so that the induction and leakage electricity can flow into the ground safely, and improve the anti-electromagnetic interference ability of the whole machine.

2.The normal connection of equipment ground wire is the primary guarantee of lightning protection and interference prevention.

2.6.2 The steps to install ground cable

There is a ground terminal behind the device. The steps of the ground wire connection are as following:

1.Screw down the nut on the ground terminal of the chassis.

2. Put one end of the grounding wire on the grounding post of the rear panel.Tighten the retaining nut.

3. Connect the other end of the ground wire to the wiring terminal.

Warning: the equipment must be well grounded (protection ground), otherwise the equipment can not be reliable lightning protection, may cause damage to the equipment and the end of the equipment!

2.7 Install power cable

2.7.1 Working with power principles:

When working with electricity,one should obey the following principles:

1.Before operation, remove jewelry such as ring, watch, bracelet, etc. Metal items may cause short circuit when they come into contact with "power" and "ground", which may lead to damage of components.

2.The wrong connection between device and power socket may cause dangerous situation.

3. Only trained and qualified personnel are allowed to operate and maintain the equipment.

📖 It is recommended to use a single-phase three-wire power socket with a ground point.

2.7.2 The steps to install power cable

Before installing the equipment, it is necessary to confirm whether the ground point of the building's power supply system is buried, and then install the equipment after confirming the burial. It is recommended to use a single-phase three-wire power socket with a ground connector, and the ground should be reliably grounded.

Confirm the AC power input range: 100V-240V AC;60HZ-60HZ.

1. Make sure the ground cable has been installed right.

2. Cut off the AC supply power ,keep the power switch being off.

3. Plug the power cable onto the power socket.

4. Plug the other end of power cable on the socket on the device.

5. Turn on the power switch on the device.

6. Check whether the power indicator on the front panel is on or not,if it is on that states the power connection is right.

⚠️ Attention:

Please keep the power plug horizontal to the power socket.

2.8 Connect the signal cable

2.8.1 Connect Ethernet port

Ethernet electrical interface generally adopts 5 types of twisted pair wires to connect Ethernet, as shown in the figure below:
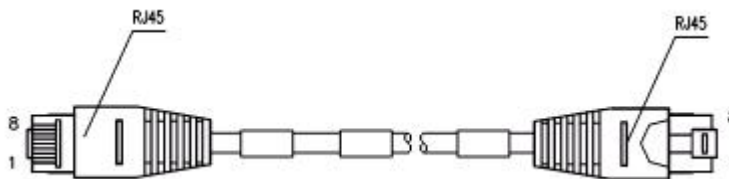
Figure 2-3 Ethernet cable

Depending on the usage, Ethernet cables can be divided into standard network cables (i.e., straight-through network cables) and cross-over network cables. There are 8 wires in the cables, which are divided into 4 pairs. Each pair is a pair of twisted-pair cables, sorted as follows:

Table 2-1 568A/568B sort rule:

568A	White green	green	White orange	Blue	White blue	Orange	White brown	Brown
568B	White	Orange	White	Blue	White	Green	White	Brown

	orange		green		blue		brown	

1. Standard network cable: also known as straight-through network cable, both ends of twisted pair cable compressed by RJ45 connector are 568A or 568B standard twisted pair cables, used for connecting terminal equipment (such as PC) to HUB or LAN Switch.

2. Intersecting network cable: the twisted pair cable compressed by RJ45 connector at both ends is standard 568A at one end and standard 568B at the other end, which is used for connecting terminal equipment (such as PC) to terminal equipment. Users need to be able to make their own.

3. When connecting the device with other IP terminals, standard network cables are used. The connection steps are as follows:

Step1: Connect the ethernet cable to the ethernet interface and another end to the device

Step2: When the power's on please check the link indicator status. Once the link light's on shows that the connection is right.When the link indicator is off, please check the connection.

Please do not plug the phone line socket into any RJ45 network interface, or it will damage the device; Use CE standard Ethernet cable with RJ45 connector.

2.9 The installation caution

In the process of installation and operation of the equipment, the following safety recommendations are put forward：

- Avoid shaking. Recommend use of standard cabinet;

- Please place the equipment far away from the damp area and away from the heat source;

- Please confirm the correct grounding of the equipment;

- Please install the anti-static wrist during the installation & maintenance of the equipment, and ensure that the anti-static wrist is in good contact with the skin;

- Please do not plug in the device's interface boards and modules.

- Please correctly connect the interface cable of the device, especially do not connect the telephone line to the serial port;

- It is recommended that users use UPS (Power Supply, uninterruptible Power Supply).

3 Device Startup and Configuration

Summary

This chapter describes the procedure for powering on the device and describes how to log in to the device management system through the Web interface.

The default IP address of the device LAN port is 192.168.100.1/255.255.255.0. Connect the LAN port of the device to the network port of the PC through a network cable, keep the IP address of the configuration PC and the LAN port IP address of the device are on the same network Paragraph, configure the device through the Web page.

3.1 Powering on the device

3.1.1 Check before power

The following checks should be performed before the device is powered on:

1. Check to make sure the power cord and ground connection is correct.

2. Check to make sure the supply voltage and equipment requirements are the same

3. Check to make sure the configure the cable connection is correct, configure the end of the PC is already open.

3.1.2 Powering on the device

1. Turn on the power switch

2. Turn on the power switch of the device

3.1.3 Inspection / operation after powering the device.

1. Check the indicator on the front panel of the device is normal or not

2. Check the Configure terminal display is normal or not

3. The device will perform normal operation after be powered on 1 ~ 2 minutes and the hardware self-test copleted, please be patient

3.2 Build WEB configuration environment

3.2.1 Configuration Preparation

Users need to confirm the following items before the configuration:

- Using Crossover or Direct Connect Ethernet cable to connect LVswitch IPPBX network interface of LAN with the user's computer

- TCP / IP protocol installed and started

- Web browser (IE6.0 or higher) installed

- Prohibiting proxy server settings of the browser

● Data access is necessary

3.2.2Connect LVswitch IPPBX and the Network Administration Terminal

Before accessing the settings page, it is recommended that users set the computer to "obtain IP address automatically" and "obtain DNS server address automatically" and the IP address to be distributed by LVswitch IPPBX.

1. Obtain IP address automatically

In the Internet Protocol (TCP / IP) Properties dialog box, click Obtain an IP address automatically and Obtain DNS server address automatically.

2. Click the OK button to save the settings.

3. The step is over.

Figure3‑1 Connect LVswitch IPPBX and Terminal PC

If users need to specify static IP address to the PC, users need to configure the IP address of the network management PC to be in the same network segment of LVswitch IPPBX LAN interface. The default IP address of LVswitch IPPBX LAN interface is 192.168.100.1, and the subnet mask is255.255.255.0; for instant, you can set an IP address 192.168.100. X/255.255.255.0(X could be 2～254) for you PC.

3.2.3 Login WEB Management System

Run the browser on the PC and enter http://192.168.100.1 in the address bar of the browser (enter the IP address of the LAN port of the device here. The default value is 192.168.100.1.Enter the login interface as shown in Figure 3-2. Users can click "Chinese " or "English" to select the interface language.

Figure 3- 2 Login Page

Enter the default administrator user name "admin" and password "admin" for the first login. Fill in the verification code shown in the system and click <Login> to open the web settings page as shown in Figure3- 3.

Figure3- 3 Web Setting Page

Top of the page is the function button. The left side of the page is the setting navigation bar corresponding to the function button. The right side of the page is the settings region. The following Chapters will introduce each details.

● Function module: Display the main function partition of the device. Click Function Module to pop up the navigation bar. Click "Exit"button to exit the Web Management System.

● Navigation Bar: Click Function Module. The navigation bar of the module pops up and corresponding function list is displayed. You can view, configure, manage, and maintain the device.

● Setting area: This area displays the panel view of the device or information about related functions. The running status of the device can be checked through the panel view, and the function parameters of the device can be configured here.

3.2.4 User self-service system login

Users log in the self-service system to view the basic user information and personal business processing.

Users need to maintain network interoperability with IPPBX devices and enter the following information in the browser address bar :

"Http: // device IP address /users.php"

Press the Enter key to enter the login interface as shown in Figure3-4.

Figure3- 4 User self-service system login Page

Users can click "Chinese" or "English" to select the interface language, enter the user name, password (user name and password refers to the management system 6.2.1.1 Add User, as shown in Figure3-5), and enter the correct verification code.The default password is 111111.
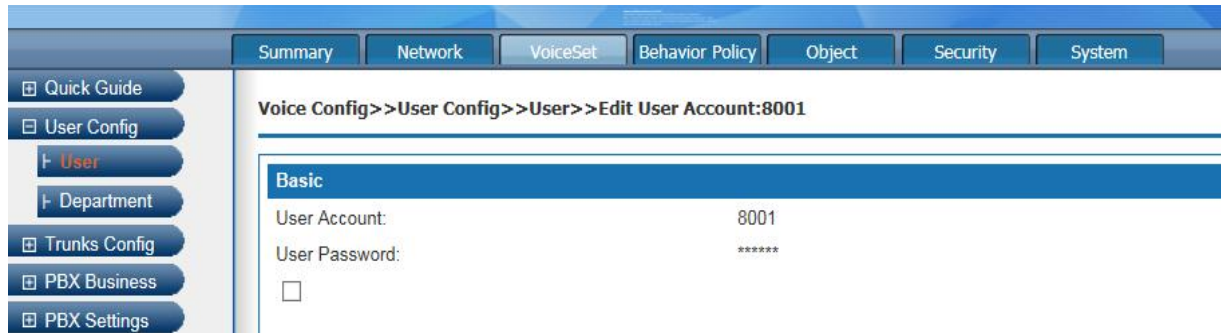
Figure3- 5 User Name and Password

Click<Login> button to enter the User self-service system, as show in Figure3-6
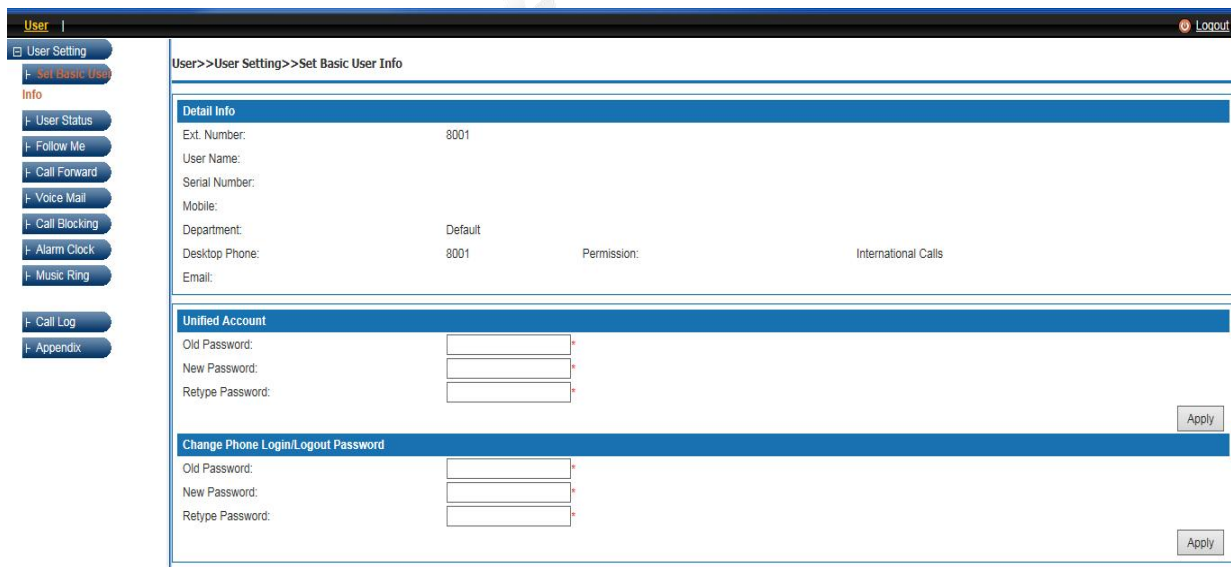
Figure3- 5 User Self-service System Page

Functions of the User Self-service System are described as follow：

Table 3- 1 Functions of the User Self-service System

Items	Description
Basic User Info	
Detail Info	Display user's user name, name, job number, mobile phone, department, landline, Email and other information.
Unified Account	Modify the user account password, the initial user password is 111111, please change the password after login. The password can be 6-20 ASSIC characters, but can not contain spaces and special characters such as ~!% ^ & *? "'/ \ │ ^.
SIP Registration Password	If you are using SIP extension, the SIP extension password can be changed in Basic User info. The registration password needs to be as complex as possible. The password is required to be 8-20 English characters long and must contain both uppercase and lowercase letters and numbers. For example, LjlA08u96Q.The default value is Aa111111.

Items	Description
User Status	
Absent	The extension enable absent status,other users who dial the number of the extension will hear the absence prompt. Outbound calls are not restricted.
DND	DND Activate, other users who dial the number of this extension will hear the busy tone. Outbound calls are not restricted.
Phone Login/Logout	Phone Logout：Other users who dial the number of the extension will hear the logout prompt. Phone Login：if activate,the extension can normally answer inboundcall, and give outboundcall .If not checked this term ,the extension can not make inboundcall or outboundcall.
Activate Call Waiting	This feature allows a person to receive a call while he or she is already on the line with someone else. After selecting this setting, if you are on a SIP call and a new call is coming in, you can choose to answer or reject the call. If you choose to receive, you can also switch back and forth between the two incoming calls. If you are a analog phone, you will hear a beep prompt, hang up the phone and rings the bell, you can pick up.
Call failure Settings	When someone calls A and A is no answer, several options are provided for A : Hang up , forward to the voice mailbox or forward to the extension and transfer to IVR.
Follow Me	
Follow Me	Follow Me service enable users to bind personal extensions to other extensions as well as outside numbers (such as cell phones, phones, etc.). When inbound call to your personal extension number, the numbers you bind will ring according to the set ringing mode, such as ringing at the same time, ringing in sequence, ringing in memory, etc.
Call Transfer	
Note： When Follow Me service activated, the Call Forwarding No Answer and Call Forwarding Unconditional service are deactivated.	
Call Forwarding Unconditional	Activate this service, set call forwarding unconditional to extension B. When someone calls A, the call will automatically transfer to extension B.
Call Forwarding on Busy	Set call forwarding on busy to extension B. When someone calls B, the call will automatically transfer to extension B.
Call Forwarding No Answer	Set call forwarding no answer to extension B. When someone calls A, the call will automatically transfer to extension B.
Voice Mail	
Voice Mail Settings	Transfer call voice message to voice mail box when busy,Voice messages can be saved in system's voice mail box or send voice message to specific email box.
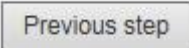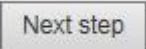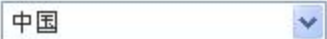
Items	Description
Listen to voice message	（1）Dial *97 on extension to listen to local voice message for the extension which open the voice mail settings function. （2）Dial *98 on extension to listen to voice message remotely and follow the voice prompt to listen to the voice message on the extensions which open the voice mail setting function.
Black List	
Black List	This service enable user to reject calls against certain number.
Alarm Clock	
Alarm Clock	Users can set alarm clock with the extension .
Record File/CRBT service	
Generate music record	You can dial "*77" on the extension dial panel to record music.
Record File settings	Select music and set as Record File.
Call log	
Call log	Shows the call log of user extension
Appendix	
Appendix	Described the services of Call Forwarding Unconditional, Call Forwarding on Busy, Call Forwarding No Answer, No disturb, Absent, Phone Login/Logout,Record，Blacklist，listen to local voice message in detail.

3.2.5 Web Page Operation Button Instructions

The following controls often appear in web setting page. The demonstration and use of these controls are shown below：

Table 3- 2 Web Web Page Operation Button Instructions

Items	Description
OK Apply	When finish the setting, click <OK> or <Apply> to enable settings
Save	Save the configuration data.
Cancel	Cancel the current configuration data.
Apply	Enable the settings
Cancel	Click <Cancel> button to cancel the information entered, and the page will jump to the "Display" page or the previous page of this function.
Add	Click <Add> to display the configuration interface and configure the system.
Delete	Click the <Delete> button to delete the selected configuration or other information.

Items	Description
Previous step	Click the <Previous Step> button to display the wizard's previous step.
Next step	Click <Next Step> button to check the validity of the configuration data. If the check is passed, save the configuration and go to the next step of the wizard.
refresh	Click <Refresh> to refresh the current page information.
Import	Click <Import> to import the format file according to the system requirements into the system.
Search/Export	Click <Export> to export the content you want.
Search	Click <Search> button, enter the keyword to search, provide precise search and fuzzy search, you can display the list of items that meet the specified conditions.
Show All	Used together with the <Search> button to search for a configuration item by criteria and click the <Show All> button to display all the configuration items.
	Click the < > icon of an item in the list box to enter the modification page of the item and modify the corresponding configuration.
	Click the icon in the list box of a <>, you can delete the item.
☑	Check the radio button to enable this feature or service.
	Text bar, enter text.
中国	Click the drop-down list will pop up a drop-down menu, move the mouse pointer to an item, left-click to select it.
‹ ›	Page view function: Click below the page or browse page before and after.
‹‹ ››	Specify the first page and last page browsing function: Click the bottom ‹‹ or ›› of the browsing interface to browse the first page and the last page.

4 Equipment Summary

Summary

The equipment Summary includes System Status and Info Statistics.

4.1 System Status

The System Status includes Device overview and the Interface status.

4.1.1 Device Overview

Select "System Status > Device" to enter the Device page as shown in Figure 4-1.
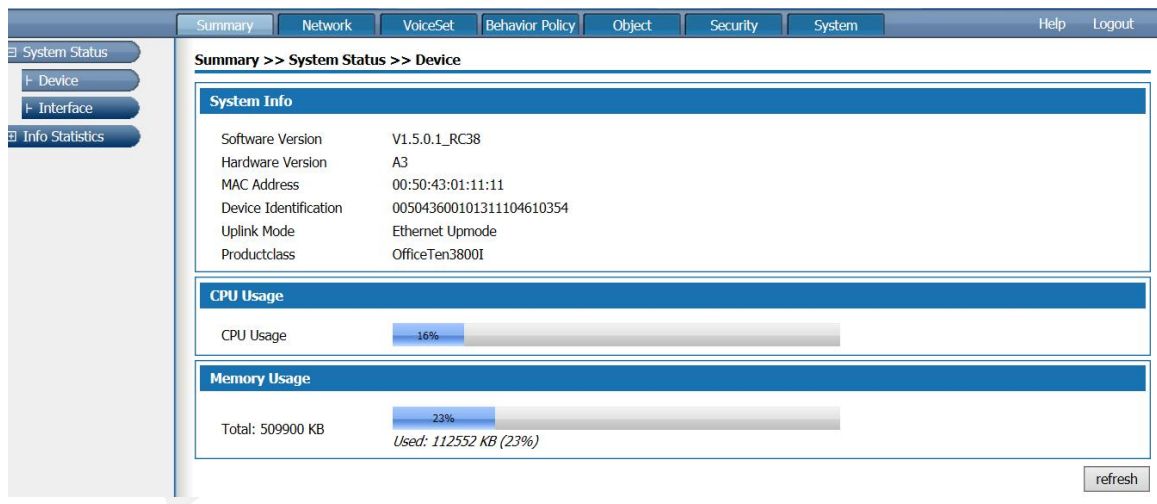
Figure4- 1 Device Overview

The Device overview shows the software version, hardware version, MAC address, Device ID, Uplink mode, Productclass,CPU usage, Memory Usage. Click < Refresh> to display the current CPU usage and memory usage.

4.1.2 Interface Status

Select "System Status > Interface" to enter the Interface page as shown in Figure 4-2.

Figure4- 2 Interface Page

The interface page shows the MAC address, Ipv4 address,Netmask of the LAN port, the size of packets sent and received, the connection mode of the WAN port, protocol type, Ipv4 address, Netmask, gateway, size of packets sent and received. For PPPOE dial-up lines, manual connection and disconnection buttons are provided. Click <Refresh> to display the current interface information.

4.2 Info Statistics

Info Statistics include DHCP Client, Interface, Online User.

4.2.1 DHCP Client

Select "Infor Statistics > DHCP Client" to enter the DHCP Client page as shown in Figure 4-3

Figure4- 3 DHCP Client

DHCP Client page displays information of client which obtaining IP address through the DHCP service of this product, the information includes name, IP address and MAC address.

4.2.2 Interface

Select "Info Statistics > Interface" to enter the Interface page as shown in Figure 4-4.

Summary >> Info Statistics >> Interface

VirtualPort				
Interface	Uplink Rate	Downlink Rate	Uplink Flow	Downlink Flow
vlan1	0B/s	0B/s	0B	669.1KB
LAN	0B/s	0B/s	0B	669.1KB
wan5	56B/s	196B/s	40.5MB	157.9MB

refresh

Figure4- 4 VirtualPort

The VirtualPort page shows the uplink and downlink rates and traffic of the VLAN interfaces and WAN sub-interfaces enabled. If the WAN sub-interface is not enabled, the uplink and downlink rates and traffic of the WAN interface are displayed. Click <Refresh> to display the current virtual interface information.

Click <PhysicalPort >, the page as shown in Figure4-6 will pop up.

Summary >> Info Statistics >> Interface

PhysicalPort			
PhysicalPort	TxTraffic	RxTraffic	Connection Status
OT3800I-port2	0B	0B	Unlinked
OT3800I-port3	0B	0B	Unlinked
OT3800I-port4	42.7MB	206.6MB	Linked

refresh

Figure4- 5 PhysicalPort page

The physicalport page shows the TxTraffic, RxTraffic, and connection status of the three physical ports of the device. Click <Refresh> to display the physical port information of the curLease Time.

4.2.3 Online User

Select "Info Statistics> Online User" and enter the "WireUser" page as shown in Figure4-6.

Summary >> Info Statistics >> OnlineUser

WireUsers(Total number 0)							
Serial No.	HostName	IP Address	Uplink Rate	Downlink Rate	Uplink Flow	Downlink Flow	Session Numbers
			No online user				

refresh

Figure4- 5 WireUser Statistics

Wireuser page visually shows Hostname, IP address, uplink and downlink rates, uplink and downlink flow, session numbers of all the wireusers. Click <Refresh> to display the current information of the Wire user.

Click <VPN User >,the page as shown in Figure4-7 is displayed.

Figur4- 6 VPN User

In VPN User page, the number of the users who log in via PPTP VPN, L2TP VPN, and IPSEC VPN is desplayed. Click <Refresh> to display the information on number of VPN users logged in at the curLease Time.

5 Network

Summary
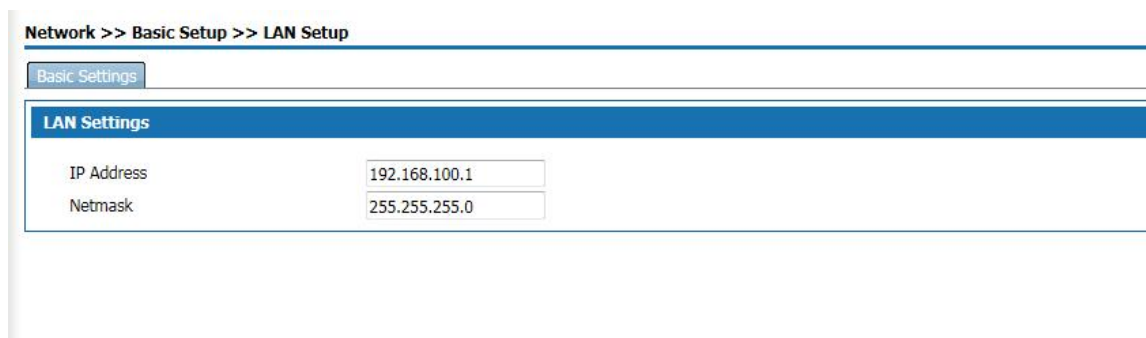
The Network module provides the basic setup configurations for LVswitch IPPBX , including LAN Setup, WAN Setup, DHCP configuration and PortSet. Advanced Options includes Static Route, NAT, Port Mapping, DDNS, Host Name and ALG configuration. VPN configuration, includes configuration of IPsec VPN, L2TP VPN and PPTP VPN.

5.1   Basic Setup

Basic Setup includes LAN Setup, WAN Setup, DHCP.

5.1.1   LAN Setup

Select " Basic Setup >>LAN Setup", click <Basic Settings> to the page as shown below Figure5-1.

Figure5- 1 LAN Setup

Configure IP address and Netmask of the LAN port. The default "IP Address"of Lan is 192.168.100.1, and "Netmask" is 255.255.255.0

After configuring LAN IP, users need to re-login with the new
IP address.

5.1.2 WAN Setup

Select " Basic Setup >>WAN Setup", click < Basic Settings > to the page as shown below.

Figure5- 2 WAN Basic Settings page

WAN Mode：

Single WAN(WAN):Ethernet Uplink

Single WAN(3G): Not support yet

Dual WAN(3G): Not support yet

Operating Mode：

Gateway: This product is used as the routing device for enterprise networks. It is generally deployed in the internal network of an enterprise for export. It internally bears the internal user gateway of the enterprise and accesses to the operator network through various links externally.

Bridge: This product is used as a bridge with a filtering function. It is generally used when an enterprise already has an Internet gateway device for exporting. It can connect the device to the gateway of the enterprise gateway and monitor the Internet traffic of employees. Bridge mode allows easy access to the user's network without changing the user's network configuration. In bridged mode, the connection type defaults to static addresses, sets the intranet address assigned to the device from which the administrator can manage the device. 3G interface does not support bridging mode.

> The address of administrator's computer and the management address set in bridge mode are required to be on the same network segment.
> In bridge mode, the bridge contains a WAN port, which can added VLAN to the bridge through LAN / WAN bonding to realize network access and traffic control of the VLAN segments.
> In the Routing Settings, NAT Settings, Port Mapping, IPsec Policy Settings section, the WAN interface will be Hidden in bridge mode.

Four Connection Types are PPPoE, Static IP, DHCP and IPoE.

● PPPOE dial-up to access to the WAN port address

Select "PPPOE" in the "Connection Type" drop-down box on the "Basic Settings " page as shown in Figure 5-3.

Figure5- 3 PPPOE to access IP address

Select **"IPv4"** as the protocol type and enter the user name and password of the user's broadband account in the Username and Password fields. The interval of the redial and MTU are default. The IPv4 DNS mode can be selected according to the actual network configuration, options are"Dynamically obtained DNS"or manually specify the primary and secondary DNS server address.

Select **"IPv6"** as the protocol type and enter the user name and password of the user's broadband account in the user name and password fields. The interval of the redial and MTU are default. Configure the IPv6 global address obtain way, IPv6 option, the default method of obtaining IPv6 gateway. The Ipv6 DNS mode can be selected according to the actual network configuration, options are"Dynamically obtained DNS"or manually specify the primary and secondary DNS server address.

IPv6 Configuration Item Description:

IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below. DHCPv6: Obtain an IPv6 address through DHCPv6 with status.
IPv6 Options	Request LAN Prefix: If this option selected, the route advertisement options and DHCPv6 options in IPv6> Basic Configuration> LAN can be obtained by WAN Authorization.
IPv6 Default Gateway Obtaining Method	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the

	text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

● Static IP

In the "Basic Settings" page, select "Static IP" from the drop-down list box as shown in Figure 4-4.

Figure5- 4 Static IP Page

Select "IPv4" as the protocol type. ISP will provide fixed WAN port IP address, subnet mask, gateway address and IPv4 DNS server address. Users should manually set these options.

Select the protocol type as IPv6 and set IPv6 global address and IPv6 default gateway access mode. Select the IPv6 DNS mode to use Dynamic DNS or manually specify the primary and secondary DNS server addresses. If the MTU is not set, There is a default value.

IPv6 Configuration Item Description:

IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below.
IPv6 Default Gateway Obtaining Method	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

● DHCP way to obtain the WAN port address

Select "DHCP" in the "Connection Type" drop-down list on the "Basic Settings " page as shown in Figure5-6.

Figure5- 5 DHCP way to obtain IP

Select IPv4 as the protocol type. Select DNS using dynamic DNS. If you need to configure it manually, select Use specified DNS and enter the DNS server address provided by the ISP.

Select IPv6 as the IPv6 address and IPv6 default gateway. In IPv6 DNS mode, select Use DNS Dynamically. If you need to configure it manually, select Use Specified DNS. Then, Enter the DNS server address provided by your ISP.

IPv6 Configuration Item Description:

IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below. DHCPv6: Obtain an IPv6 address through DHCPv6 with status.
IPv6 Options	Request LAN Prefix: If this option selected, the route advertisement options and DHCPv6 options in IPv6> Basic Configuration> LAN can be obtained by WAN Authorization.
IPv6 Default Gateway Obtaining Method	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

● IPoE way to obtain WAN Port Address

Select " IPoE " in the "Connection Type" drop-down list on the "Basic Settings " page as shown in Figure5-7.

Figur5-6 IPoE way to obtain IP Address

Select IPv4 as the protocol type. Select DNS using dynamic DNS. If you need to configure it manually, select Use specified DNS and enter the DNS server address provided by the ISP.

Select IPv6 as the IPv6 address and IPv6 default gateway. In IPv6 DNS mode, select Use DNS Dynamically. If you need to configure it manually, select Use Specified DNS. Then, Enter the DNS server address provided by your ISP.

IPv6 Configuration Item Description:

Service Identity	Negotiate with the peer routing device to exchange authentication information.
IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below. DHCPv6: Obtain an IPv6 address through DHCPv6 with status.
IPv6 Options	Request LAN Prefix: If this option selected, the route advertisement options and DHCPv6 options in IPv6> Basic Configuration> LAN can be obtained by WAN Authorization.
IPv6 Default Gateway Obtaining Method	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

WAN Subinterfaces

When multiple services, such as Internet, IPTV, and VoIP services, need separate WAN ports as their own channels, multiple WAN subinterfaces should be enabled to configure LAN / WAN bonding. Select "Basic Setup> WAN Setup" and click the "Subinterfaces" tab. The page as shown in Figure 5-8 is displayed.
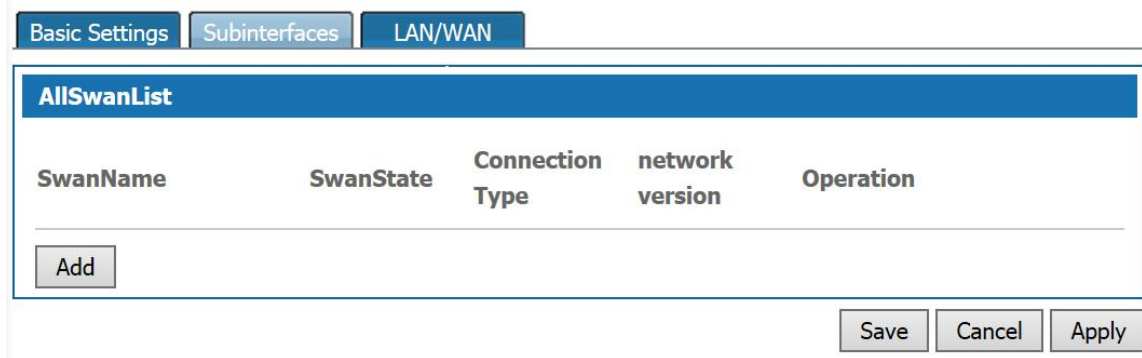
Figure5- 7 WAN Subinterfaces page

Click <Add> to pop up the page for adding a WAN sub-interface as shown in Figure 5-8.

Figure5- 8 WAN Subinterfaces Configuration

WAN Subinterfaces Configuration description

Table 5- 1 Sub-interface Configuration

Item	Description
Enable Subinterface	Enable subinterface option or not
VID	Negotiate with the WAN port switch equipment in consensus
802.1P	Negotiate with the WAN port switch equipment in consensus

Item	Description
Binding Type	• Internet：The sub-interface for Internet access； • Management：This subinterface is used to manage the channel. When this type is set, the subinterface will be hidden in the LAN / WAN binding part； • IPTV：This sub-interface is for IPTV channel； • Management-Internet：This type is compatible with Internet access and management；； • Voice：This sub-interface is used for voice channel； • Management-Voice：This type is compatible with management and voice；； • Voice-Internet: This type is compatible with voice and Internet access； • Management-Voice-Internet: This type of compatible management, Internet access and voice； • Other：Other types.
Subinterface Mode	Options: Gateway, Bridge
Connection Type	Options include static IP, DHCP, PPPOE, configuration method is same with the one of WAN port.

Enable "Subinterface" mode, the WAN port "Basic Settings" will not be available.

LAN/WAN Binding

In WAN Subinterface mode or Bridge mode, the connection between VLAN network segment or LAN port and WAN side port can be achieve by adding a LAN / WAN binding.

Select "Basic Setup> WAN Setup" and click the "LAN / WAN" tab. The page shown in Figure5-9 is displayed.

Figure5- 9 LAN/WAN Binding

VLAN binding: Select "VLAN binding" mode, and select from the drop-down box to bind the enabled VLAN with WAN subinterface.

Port binding: Select "Port binding" mode, and select from the drop-down box to bind the two internal network ports on the LAN side of the device withthe WAN subinterface.

> When "Port binding" is selected,the "VLAN Settings", "Port VLAN Settings" and "VLAN Isolation" under "Basic Setup> LAN Setup".

5.1.3 DHCP Configuration

Select "Basic Setup> DHCP". The DHCP Settings page is displayed as shown in Figure 5-10.

Figure5- 10 DHCP SERVER Configuration

- When DHCP service is select as " Disabled", the DHCP function on the LAN port is disabled.
- DHCP service is select as "DHCP SERVER", a page pop-up shown as Figure 5-10. This product acts as a DHCP (Dynamic Host Configuration Protocol) server and assigns IP addresses to computers in the LAN.

DHCP SERVER Configuration：

Table 5- 2DHCP SERVER Configuration

Item	Description
Lease Time	Enter the lease time of the assigned IP address for computer, after the lease time, the computer must re-apply for an address (usually a computer will automatically apply). Unit: second, the default value is 18000 seconds.
IP Range	The DHCP server IP address pool configuration requires that the IP address of the LAN is on the same network segment. You can add multiple IP address pools to set the initial IP and end IP addresses of the address pool.

Item	Description
IP/MAC Address Binding	Add MAC and IP address bindings to meet the fixed IP needs of some machines. When the product receives a DHCP client request for an IP address, it first looks for the binding table. If the computer is in a binding table, it assigns the corresponding IP address to the computer.

Figure5-11 DHCP RELAY Configuration

- DHCP Service: Selecte "DHCP RELAY" to open page shown in Figure6-11. If the DHCP client and DHCP server are not on the same physical segment, the DCHP Relay Agent (Relay Agent) is required. In this case, the LAN acts as a DHCP RELAY proxy to communicate with DHCP servers on other subnets to allocate IP addresses to DHCP clients.

DHCP RELAY Configuration Description：

Table 5- 2 DHCP RELAY Configuration

Item	Description
Server side IP Address	IP address of DHCP server connected
Server side interface	The interface that connect DHCP RELAY with DHCP server

5.2 Advanced Options

Advanced Options include DDNS, Static Route,Dynamic routing, NAT, Port Mapping,UpnP, Host Name,ALG.Page push, multicast Settings.

5.2.1Static Route

After defining the LAN port address, WAN port address and gateway, the device will automatically generate the interface network segment route and a default routing, with these routes,basic service needs can be meet in normal circumstances. Select" Advanced Options> Static Route". The "Static Route" page is displayed as shown in Figure 5-12.

Figure5-12 Static Route

Add route configuration description：

Table 5- 3 Add Routing

Item	Description
Name	User defined route name.
Destination IP	The destination address need to reach, it could be network address or host address.
Gateway	The IP address of the next router to pass before the data reaches the destination address.
NetMask	The destination address subnet mask to be reached.
Network Type	Select the static route out interface, including the LAN port and WAN port.

5.2.2 Dynamic routing

Dynamic routing means that the router can automatically set up its own routing table and adjust it according to the actual situation. The routing information exchange between the product and the docking device is realized based on RIP routing protocol. Route: network >advanced options>dynamic route, the page pops up as following:

Figure 5-13   Dynamic Route

Dynamic route setting description as:

Table 5-5 dynamic route setting

Interface	Instruction
RIP	Click "enable" to enable Routing Information Protocol
Version	Consistent with docking routing devices, optional "default", "RIPv1" And "RIPv2".
Encryption	Select " RIPv1" ,no need to encrypt. Select "RIPv2",negotiated with the docking device whether to encrypt or not.The device supports plaintext encryption and MD5 encryption. Set the encrypted password in the password box below.

5.2.3 NAT Configuration

Network Address Translation (NAT) enables multiple computers in the LAN to access the Internet through a small number of public IP addresses and save public IP addresses. As LANs are isolated from the Internet, NAT can also provide some assurance of Security. Select "Advanced Options> NAT", and enter the NAT Configuration page as shown in Figure5-14

Figure5-14 NAT Configuration

NAT Configuration Description：

Table 5- 4 NAT Configuration

Item	Description
Enable	Select"Enable" to activate NAT service
The router maps all private hosts to publicly exposed IP addresses	Select this item to enable NAT function, all the internal network IP address converted into WAN port IP address through the NAT function to ensure that users access the Internet. The NAT rule added later by the user takes precedence over this rule.

Click <Add> button to open the "Add NAT Configuration"page as shown in Figure5-15

Figure 5-15　Add NAT Configuration

Add NAT Configuration：

Table 5- 7 Add NAT Configuration

Item	Description
Interface	Select WAN port.or wan sub interface port.　NAT configuration added is valid when the WAN port address is static, otherwise it shows no static interface.
Extranet IP	IP address range used after address translation, the address range must be in the same network segment as the above network interface.
Intranet IP	Intranet IP address need to be translated. Select "Apply to all Intranet IP"，all Intranet IP are translated to the extranet IP through NAT function,select "Apply to the specified Intranet IP."　Set the intranet addresses that need NAT to translated in the following text box .
status	Optional, Enable or Disable.

5.2.4　Port Mapping

Port mapping is used to map the WAN IP of the device to specific server IP of the intranet. To access the IP of the intranet specific server, user only need to access the WAN side IP.

Choose "Advanced Options> Port Mapping", and enter the "Port Mapping" page shown in Figure5-16.

Figure5-16 Port Mapping Configuration

Click <Add> button to open Add Port Mapping page shown in Figure 5-17.

Figur5-17 Add Port Mapping

Add Port Mapping Description：

Table 5- 8 Add Port Mapping

Item	Description
Port	Any ports：In this mode, all ports will be mapped. Designated port：Users need to configure the "Intranet port" and "Extranet port".
Protocol	The data connection protocol used when port mapping，options include All,TCP or UDP.
Internal IP	The intranet IP that need port mapping
Internal Port	When selecting designated port,the internal port to be mapped externally,for example,www port is 80,ftp port is 21.
Interface	WAN port、WAN 3G or User Defined are available.
External IP	Network Interface selected as " External IP", set the IP address of the extranet used by the port mapping, which must belong to the NAT address pool.
External Port	When selecting "specify port", set the external network service port of the port mapping, such as WWW port 80, FTP port 21, and generally keep the same with the internal network port.
Status	Optional, Enable or Disable.

5.2.5 UpnP Setting

Upnp can be optional enable or disable.

5.2.6 Host Name setting

Virtual domain Settings allow users to set the domain name to access the corresponding Intranet IP address. Select Network >Advance options> Host name, the page will pops up as the figure 5-18.
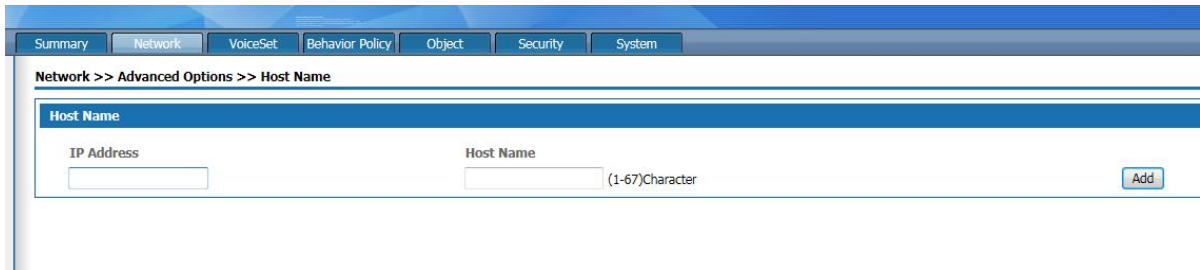
Figure 5-18 Host name setting page

Host name setting description as following:

Table 5-8   Host name setting description

Interface	Instruction
IP address	Intranet IP address
Host name	Set the host name of the intranet IP,the length is 1-67 characters

5.2.7 ALG setting

The ALG(Application Layer Gateway) is a type of firewall made by a an augmented firewall or computer network Application or firewall containing of security components for NAT.Enable ALG function to realize private network traversal function of SIP, FTP, H323, L2TP, RTSP, IPSEC and PPTP protocols.

Select "advanced options >ALG" and enter the "ALG" page as shown in figure 5-19.
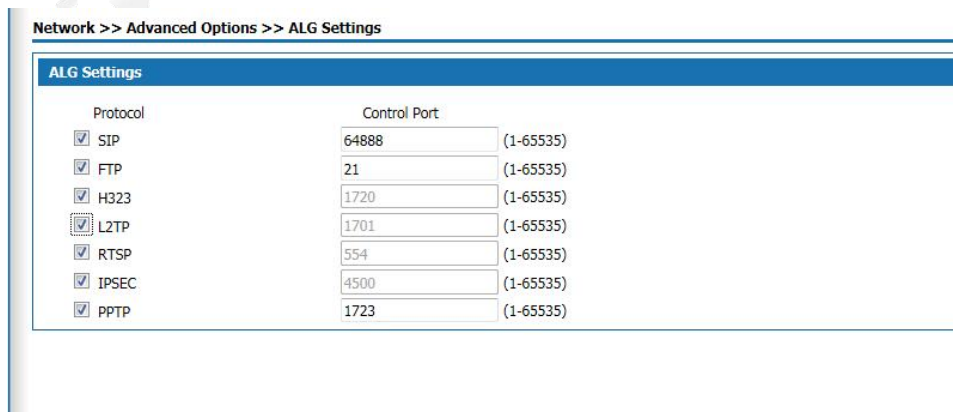
Figure 5-19 ALG setting

Select the radio box and enable the ALG function of the corresponding protocol.

5.2.8 Push Portal

The page push is the website address opened by the user who logs on the Internet through this product when they first log on the Internet.   Select <network> <advanced options> and <push portal> the push portal setting page appears as follows:
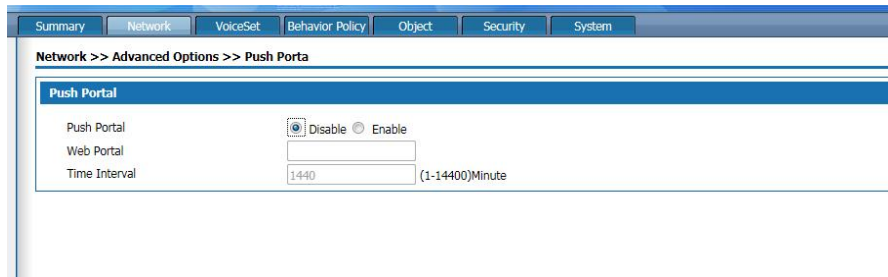
Figure 5-20 Push portal

Push portal setting description as following:

Table 5-9 Push portal setting

Interface	Instruction
Push portal	To enable or disable,default disable
Web Portal	The first time to open the website address when log in the internet through this product
Time interval	The interval time logs in the push website page again

5.2.9 IGMP PROXY

Select advanced options> IGMP Proxy setting,the page pops up as figure 5-21
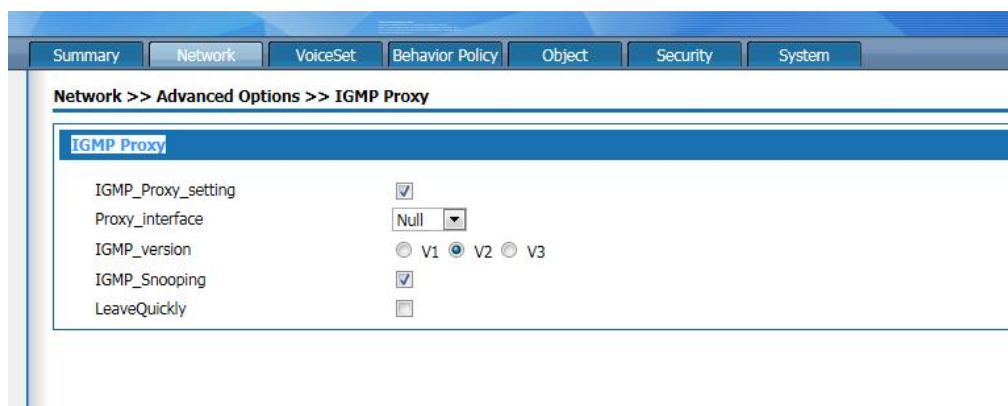
Figure 5-21 IGMP Proxy setting

This product supports IGMP proxy and IGMP listen function,click the radio box to enable the function. The proxy interface is the interface connect with IGMP router,which can be WAN 5 or WAN sub-interface according to the drop-down box.

5.2.10 IGMP VLAN

Select "advanced option > IGMP vlan" and enter the "IGMP vlan" page as shown in figure 5-22.

Figure 5-22 IGMP VLAN setting

Enter Global IGMP VID then click save button .

Click <add>button ,the popup page of adding multicast vlan is shown in figure 5-23

Figure 5-23   IGMP VLAN

Add IGMP VLAN setting as below:

Table 5-10 IGMAP VLAN SETTING

Interface	Instructions
All Swan list	Display only the enabled Wan-subinterface with connecting pattern "bridge",and generally select the sub-interface of the IPTV property, that is, the binding type Subinterface for "IPTV" or "Other".
IGMP_vid	Configure the ID of the livestreaming channel and bind it to the WAN subinterface. After connecting the IPTV set-top box with the internal network port bound to the WAN sub-interface, you can watch live TV.

Save	Click the <save > button to add a multicast vlan policy.

5.3 VPN Setting

5.3.1 IPsec

IPsec (Internet Protocol Security), or Internet Security Protocol, is a series of specifications of Internet Security communication provided by IETF, which provides IP data packets with high-quality, interoperable and cryptographic-based Security functions. In the IP layer, encryption and data source authentication are used to ensure the privacy, integrity and security of data packets when they are transmitted over the network.

As IPsec VPN server, the configuration steps of this product are as follows:

Step 1: Add a new policy on the IPsec policy page

Step2: On the Ipsec application page, modify and delete the added policy.

Step 3: On the Ipsec status page, connect or disconnect the enabled policy.

Step 4:On the Ipsec log page to check the log of the connect or disconnect of the Ipsec policy. Select " VPN setup >IPsec " click the <Ipsec policy> tab enter the <IPSEC Policy > page as following figure 5-24

Figure 5-24   IPsec VPN-ipsec policy

Ipsec strategy description as following:

Table 5-11 IPsec policy description

Interface	Description
IPsec policy	By setting up the IPsec policy, a secure channel is established between the local end and the opposite end.
Policy name	Enter the policy name,1-32 characters long
Policy status	Enable or disable
Connection type	Lan to Lan: The connection between two equipment Remote access:Connection between PC with the product
Interface	Specify the interface of the secure channel,default is the WAN 5
Remote address	Specifies the opposite address of the secure channel connection, which can be set to an IP address or domain name
Local Subnet	Specifies the local network segment for the safe channel.
Remote Subnet	Specifies the opposing network segment for the safe channel.

IKE(Internal key exchange) description as below:

Table 5-12 Internal key exchange

Interface items	Description
IKE(Internal key exchange)	Configure IKE, which uses two phases to negotiate and establish the key for IPsec SA.
Exchange mode	When it is the first phase for exchange, the optional mode "Main" or " Aggressive" .The Main difference between the Main and Aggressive pattern exchanges is that the Aggressive exchange provides no identity protection and exchanges only three messages. In cases where identity protection is less important, using Aggressive mode can speed up negotiations. In situations where identity protection is high, use the Main mode.

Exchange direction	Select "Initiate" This end is the initiating end of IKE negotiation; Select "receive" this end is the receiving end of IKE negotiation.
Authentication	Select the authentication mode of the both communications parties. Optional "preshared key"or RSA Signature
Key group	DH2(1024) OR DH5(1536)
Dead Peer Detection(DPD)	Click and to enable this function,Interval: sets how long it is before an IPsec message is received from the opposite side, triggering DPD queries.The default value is 30s,the range 1-180 s. Timeout: after sending the DPD query, set how long it is before the DPD response is received, and delete IKE SA and the corresponding IPsec SA. The default value is "120 seconds", ranging from 1 to 600 seconds.

Phase 1 setting description as following:

Table 5-13　Phase 1 configuration as below

Interface items	Description
Phase 1	In the first phase of configuration, the communicating parties establish an authenticated and secured channel among themselves, that is, establish an IKE SA.
Local ID type	The ID type is used by the product during IKE's first phase of negotiation used to identify itself to the opposite product. Optional IPaddress or FQDN
Local ID	When selecting IP address here it enters local IP address here, when selecting domain name, it enters domain name here.
Remote ID Type	The type of ID used by the end device during IKE phase 1 negotiation. Optional "IP Address or domain name" Between two docking devices, the home end ID set by one device should be the same as the opposite end ID set by the other device.
Remote ID	When selecting IP address here it enters local IP address here, when selecting domain name, it enters

	domain name here.
Encryption Algorithm	DES（Data Encryption Standard）The 64bit key is used to encrypt the message block.
	3DES（Triple DES）Three 64bit DES keys are used to encrypt the message block. AES（Advanced Encryption Standard）This product supports 128bit, 192bit, 256bit key length AES algorithm; Default value is DES
Authentication Algorithm	MD5: MD5 generates a 128bit message digest by entering messages of any length;SHA1: the 160bit message digest is generated by input messages with the length less than 2 64 bits. The digest of SHA1 is longer than MD5, so it is more secure.The default value is "MD5".
IKE SA Lifetime	Before the life cycle timeout of the set IKE SA, an SA will be negotiated in advance to replace the old SA. Before the new SA is completed, the old SA will still be used. After the new SA is established, the new SA will be used immediately. Default value is 3600s ,the range is (1200-86400) Seconds

Phase 2 setting description as below

Table 5-14 phase 2 setting description as below

Interface items	Description
Phase 2	Configure the second stage, use the SA established in the first stage to provide IPsec negotiation security service, that is, negotiate specific SA for IPsec, and establish IPsec SA for final IP data packet security transmission.
ESP mode	In tunnel mode, AH or ESP is inserted before the original IP packet header, and a new packet header is generated before AH or ESP. In transport mode, AH or ESP is inserted behind the IP packet header, but before all transport layer protocols, or before all other IPsec protocols; Default value is "Tunnel "

Protocol types	AH or ESP Default value is " ESP". AH is the authentication header protocol and the protocol number is 51. The main functions include data source authentication, data integrity verification and message retransmission prevention. ESP: ESP is a packet security encapsulation protocol with a protocol number of 50. Unlike the AH protocol, ESP encrypts the data packets that need to be protected and then encapsulates them in the IP packet to ensure the confidentiality of the data.
Encryption Algorithm	Optional DES、3DES、AES128、AES192、AES256,with default "DES"
Authentication Algorithm	MD5 or SHA1 ,default " MD5"
IPSec SA Lifetime	Set the lifetime for "IPsec SA" if over the lifetime,it needs to negotiate the IPsec SA again .Default value is 28800s.
PFS	Select the radio box and enable perfect forward secrecy; With this feature enabled, the connection time will be longer but the privacy will be better.
Compression	Select this if you want to compress the header of IPsec.
Save	Click save button to save and the IPsec policy will appear in the page of application page.

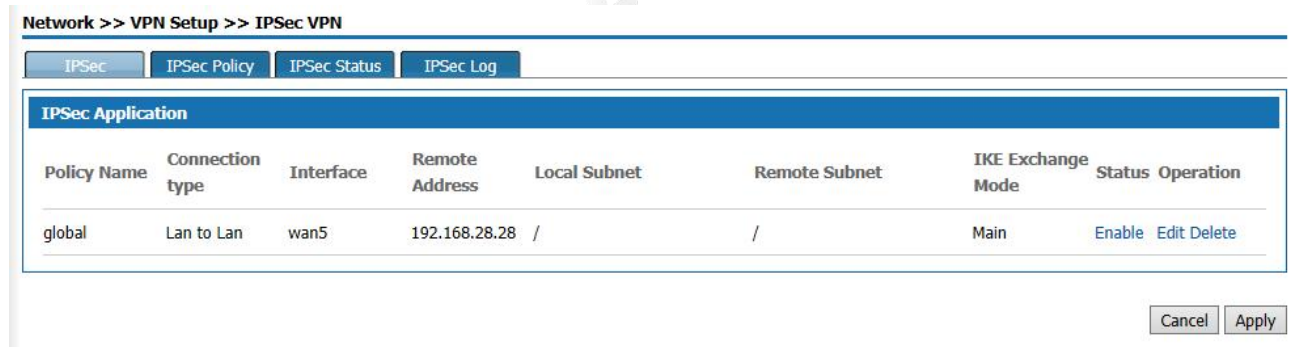Click the IPsec tab ,and the IPsec application will pops up as figure 5-26 shown.

Figure 5-25   IPsec VPN-IPsec Application

On this page, you can see all the IPsec policies set, modify the policies, or directly modify the status of the policies or delete the policies.

Click< IPsec status> you can see the IPsec status as figure 5-26 shown

Figure 5-26 IPSEC status

On this page,it shows the connect status of the enabled IPsec, to connect or disconnect.

Clicking <IPsec log> tab, it shows the page as figure 5-28.

Figure 5-27   IPsec log

You can see log information about IPsec connections and disconnections on this page.

After the correct configuration of the server-side setting for accessing IPsec VPN, when establishing IPsec VPN connection, the client computer shall be able to access the Internet and complete the connection setting of IPsec VPN client. Due to compatibility issues with the "vpn-ah" mode, "AH" is not recommended for protocol type in the phase 2 configuration of the IPsec policy.

5.3.2 L2TP

  L2TP (Layer 2 Tunneling Protocol) is the most widely used protocol of the VPDN (Virtual Private dial-up Network) tunnel protocols. Here to introduce how to configure L2TP VPN.

L2TP Client configuration

This product can be configured as L2TP client, which can send connection request actively, establish VPN tunnel and obtain private IP address. Select "VPN configuration >L2TP VPN" and enter the "L2TP VPN" page as shown in figure 5-28.

Figure 5-28   L2TP client set

L2TP client setting description as following:

Table 5-17 L2TP client setting

Interface items	Description
Enable L2TP client	Select the radio box to enable the L2TP client function and turn off the server function
Connection name	Set the name of connection
Tunnel Authentication	This item needs to be agreed with the server side. Select the radio box, enable tunnel authentication, and configure authentication that is consistent with the server.
Server IP Address	The client connects to the L2TP server IP address.
User name	The L2TP server user name that connected to L2TP client
Password	The L2TP server user password that connected to L2TP client

Click < save > to save client configuration information, and click < apply > to connect to the server.

L2TP server configuration

This product can be configured as an L2TP server, allowing authenticated L2TP clients to connect in.

Click the"L2TP server" TAB to enter the L2TP page as shown in figure 5-29.

Figure 5-29 L2TP server setting

L2TP server setting description as :

Interface items	Description
Basic setting	Select the radio box to enable the server function while close the client function; IP pool: Sets the IP address pool assigned to the client
Authentication Method	Local
Authentication Algorithm	Optional PAP,CHAP,MS-CHAP-V1,MS-CHAP-V2 When the client connects to the L2TP server, the authentication algorithm selected must be consistent with the authentication algorithm provided with the client.
DNS Server	Be consistent with what operators are offering
L2TP-IPSec Tunnel Settings	Click the radio box to enable L2TP-IPSec tunnel setting.Select the Shared key authentication mode and enter the share key in the text box below; Now when the client connects to the server, it can use the IPSec encrypted VPN tunnel.

Click <save> button to save the server configuration information and <apply> to apply the setting.

L2TP status

After the VPN connection operation, click the <VPN status>label to pop up as shown in figure 5-31. Show the ID number, IP address of the opposite device, IP address of the device, and connection status automatically assigned by the established VPN tunnel.
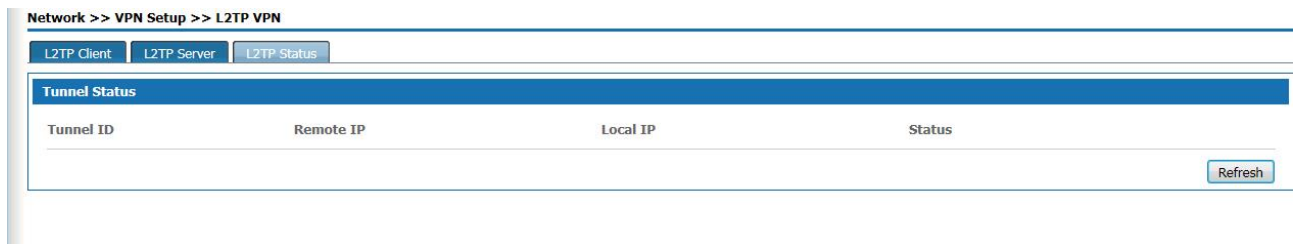
Figure 5-30 L2TP status

5.3.3 PPTP

PPTP (Point to Point Tunneling Protocol) is a Point to Point tunnel Protocol. PPTP is a network technology which supports multi-protocol virtual private network and works on the second layer. Through the protocol, remote users can secure access to corporate networks through Microsoft Windows operating systems and other systems with point-to-point protocols.

Select <Network> and <VPN Setup> and <PP2P VPN> then appears the page as figure 5-31
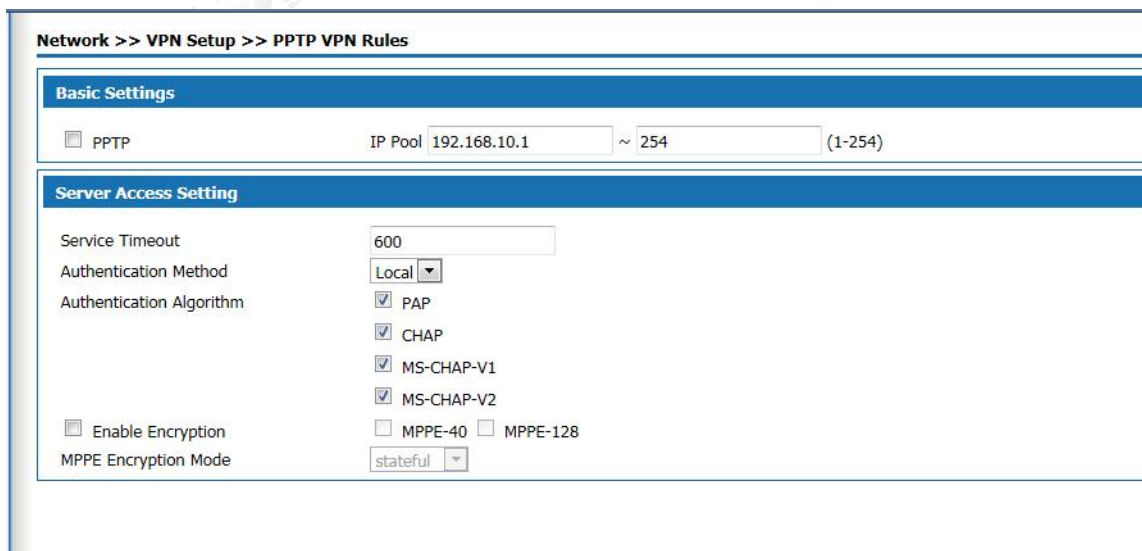
Figure 5-31PPTP VPN setup

The basic setting description as below:

Table 5-19   PPTP VPN Setup

Interface items	Description

Enable PPTP	Click the box to enable PPTP
IP pool	The IP address obtained by the client after dialing the VPN is in the form of XX.XX.XX.XX
Service Timeout	The VPN connection is idle continuously, that is, no packet has been sent/received for longer than the set time. If the service is considered to be timeout, the VPN connection will be disconnected.
Authentication Method	Default value Local
Authentication Algorithm	PAP、CHAP、MS-CHAP-V1 and MS-CHAP-V2
Enable Encryption	Encryption can only be enabled under ms-chap -V1/V2 authentication algorithm, password length support MPPE-40 and MPPE-128; MPPE encryption mode supports stateless and stateful.

6 Voice Configuration

Voice configuration includes Quick Guide, User Config, Trunks Config, PBX Features, PBX Settings and Status Report.

6.1 Quick Guide

The quick setup module guides you to configure the product in the form of wizard. According to the steps provided, you set up the extension number, analog relay or SIP relay and exhalation routing in the setup wizard, enabling basic internal call and external call. The SIP relay needs to input specific information to the end-to-end gateway or ISP, such as IP address, port number, SIP account and SIP password.

Before configuration, click the "Quick Guide" of the page to enter the quick setting page as shown in Figure 6-1.
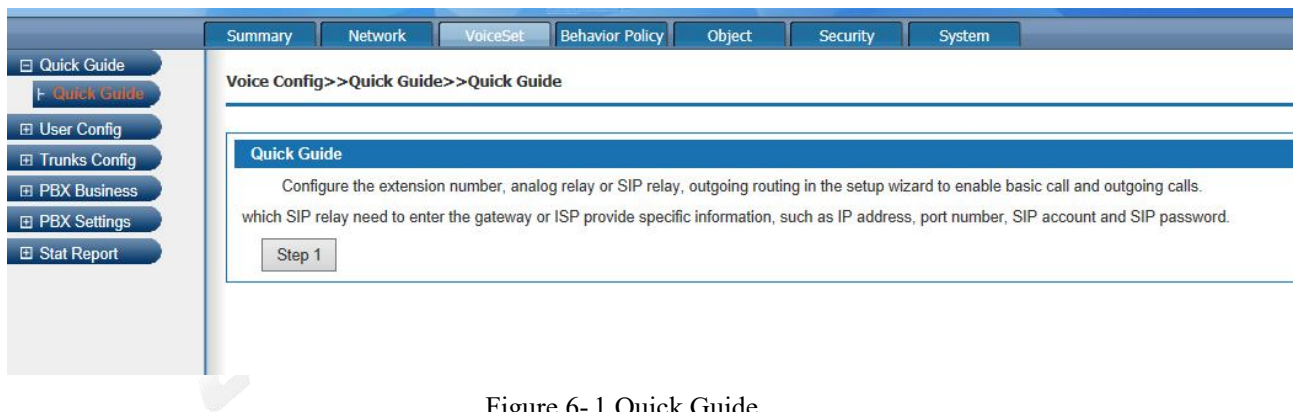
Figure 6- 1 Quick Guide

The Click<Step 1> button to pop out as the page shown in Figure 6-2, and configure extensons.
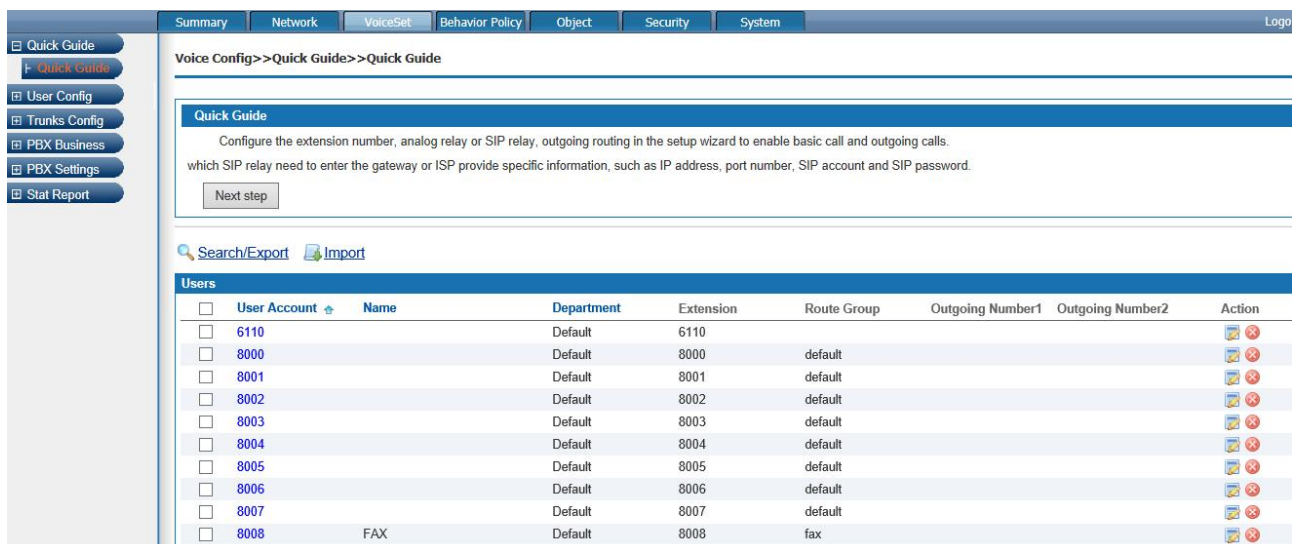
Figure 6- 2 Extesion Settings

Click the <next step> to pop up the page shown in Figure 6-3, and configure trunks

Figure 6- 3 Trunk Settings

Click the <next step> to pop up the page shown in Figure 6-4, and configure routes

Figure 6- 4 Route Settings

Click <Finish> to finish configuration.

6.2 User Config

User Config includes User and Department

6.2.1 User

Click "Voice Config>>User Config>>User" to pop up the page shown in Figure 6-4; add user information, create the only user that the device can identify, and manage and restrict the user's behavior effectively

Figure6- 5 User

6.2.1.1 Add a single user

Click "Add" to pop up the page shown in Figure 6-6

Figure6- 6 Add user information

1. Basic Settings

Basic configuration page is shown in the following figure 6-7.

Figure6- 7 User-Basic

Interface items are described as follows:

Table 0- 1 User Information – Basic

Items	Description
User Account	This is the basic information for employees. As a unique ID, it can't be modified. Statistic reports about users' status are generated in the name of this parameter. You can input digit (0-9), char (a-z A-Z) or _! @#$%^&*() with the length 1-20.
Password	Password of the user account. You can input ASSIC character with length 6-20.The default value is 111111.
Retype Password	You're required to input the password again.
SIP Registry password	If the user is using a SIP extension, the password for the SIP extension can be changed in the user's basic information. Registration password requires as complex as possible, do not have regular easy to guess password, password length 8-20 English characters, must contain both upper and lower case letters and Numbers, such as LjlA08u95Q (factory default: Aa111111)
Name	Input user's name.
Employee ID	Input user's Employee ID.
Cell Number	Input user's cell phone number.
Home Number	Input user's home number.
Department	Select department of the user.Add an extension to the selected department. A user can only be in one department. The system default department is "default".
Route Group	Add an extension to the selected routing group. A user can only be in one routing group. The system default routing group is "default".
User permission	Internal Enterprise Local National Long Distance International Long Distance

Items	Description
VIP class	Select the VIP level of the user from the drop-down box, and the system will provide ordinary users, VIP1~VIP5, and the level will be increased successively. This option needs to turn on the VIP switch in "Voiceset >PBX setting > global setting".

2. Extension Settings

Click <Enable Extension> to enable extension settings; configuration page is shown in the following figure 6-8.You can also activate "voice mail Settings", "call failure setting", "ring setting".FIG. 6-8 setting of the extensions
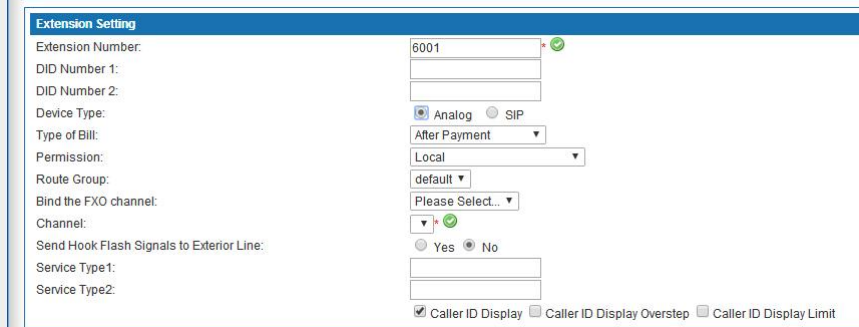

Figure0- 8 Extension Settings

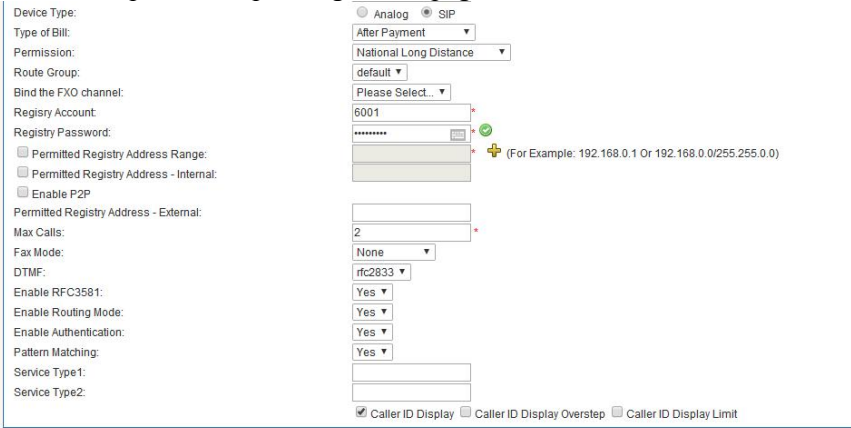Interface items are described as follows:

Table 0- 2 User-Extension Settings

Item	Description
Extension Number	Extension number for analog or SIP user
DID Number1/2	Sets the user's outside line number, which is optional

Item	Description
Type of Bill	The selectable types include after payment, advance payment, card user pay, and default value for "after payment". (1) After payment: the after payment does not restrict the length of the call, and the bill is settled after the end of the call. (2) advance payment: the balance of the user's account is insufficient, the call can not be successfully carried out, and the balance of the query is called *203. (3) card users pay: "card users pay" on the extension to input the corresponding card number and password, in the case of adequate balance in the card, the call. When you select the card user payment type, you need to set up the card user payment mode at the same time, providing three ways: no binding, authentication, binding, authentication and binding without authentication. Do not bind but need to be authenticated: enter card number and password when make a call account to the system prompt tone. Bind and need to be authenticated: enter card number in the "card number account" text box, enter password when make a call account to the system prompt tone. Bind but no need to be authenticated: enter card number and password in the "card number account" text box, no need to enter again when make calls **Call code:** card number, call business code *201, users dial *201, enter the card number and password according to the prompt tone, such as binding, do not need to enter again, then enter the called number. **Business Code:** business code *202, users call *202, according to the tone input card number, password (as has been bound, again without input) according to sound business system, provide business change password, balance inquiries, binding (extension and number binding) and cancel binding. Related configuration: billing settings in the 6.6.1 global settings.
Permission	Internal Enterprise Local National Long Distance International Long Distance Device internal refers to the extensions internal the device can call to each other. Enterprise internal refers to the authority to call each other through different devices of the enterprise; The default value is "national long distance". If no international call is required, the international call permission must be turned off. Select the corresponding permissions, and the user can call out the corresponding calls. High permissions include low permissions. For example, if you choose international call, then you can make international call, domestic call, local call, enterprise call and internal call. Note: The calling permission of an extension is also limited by the calling route. For example, if the extension needs to make an international call, the permission of the extension should be "international call", and the calling route should be configured at the same time. Only when both conditions are met can the extension make an international call.
Route Group	Select route group from the drop-down box. A user can only be in one routing group. The system default routing group is "default".

Item	Description
Bind the FXO channel	Select FXO channels The device supports analog phone, SIP phones to bind FXO channel. 1. Inbound routing: the inbound routing strategy has a higher priority than FXO channel binding. If the trunk corresponding to FXO port has set the inbound routing, it will give priority to calling according to the inbound routing; If the FXO port corresponding relay is not configured with inbound routing, but the FXO port is bound by the sub-extension, the inbound call directly to the bound sub-extension. 2. Exhalation: when the extension is exhaled by FXO port, select the FXO channel bound for exhalation. 3. If the channel number is not selected, all channels will be default.
Device Type	Select Analog or SIP extensions
Type(Analog)	When select analog, **Extension Setting** Extension Number: 6001 DID Number 1: DID Number 2: Device Type: ● Analog ○ SIP Type of Bill: After Payment Permission: Local Route Group: default Bind the FXO channel: Please Select... Channel: Send Hook Flash Signals to Exterior Line: ○ Yes ● No Service Type1: Service Type2: ☑ Caller ID Display ☐ Caller ID Display Overstep ☐ Caller ID Display Limit 1) Channel:channel number needs to be specified. Select unoccupied channel from the drop-down box.Channel number needs to be the same with the FXS port. 2) Inbound and outbound call restriction: by default, "no restriction" is adopted, and the extension can see the caller id number when there is no number display restriction service. Note: Inbound and outbound call restriction is only limited to analog phones, while sip phones are not limited. 3) Send Hook Flash Signals to Exterior Line: Select yes, it can send hook flash signal to exterior line; no, it can not. Default value is no.

Item	Description
Type(SIP)	If select the phone to sip,configuration page as follow: Register account/password :Sip registered authentication user account and password can be different with the unified account.The registry password should be complicated which is not easy to guess.8-20 characters long,and must contain both upper and lower letters and number.Such as LjlA08u96Q. The default registration password is Aa111111 Permitted Registry Address Range:add registration address limit, you can add more than one registration address. Can add most 5 addresses and you should fill in subnet mask. IP address: selecting a SIP phone requires assigning an IP address. If you use static or external IP, you need to fill in the specified IP; Without an IP address, the system dynamically assigns an IP address to the IP phone Enable P2P: enable P2P protocol, exchange media stream directly when SIP phone calls, no longer through the device.It can improve audio and video quality, reduce the pressure of the server. The master SIP client is called and the P2P is started simultaneously. Note: voice calls using P2P cannot be recorded. Max call:set the maximum number of simultaneous calls for a single SIP phone, default value 2. Fax mode: NONE,T.30 by pass,T.38. Default value none. T.30 by pass is telephone line fax and IP point to point transmission.T.38 is used for IP network transmission, that is IP FAX. When none, it doesn't support fax. (7)DTMF mode: Set the sending mode of DTMF and to configure the sending dial way of the phone.There are Info, inband, rfc2833 three types, default Type "rfc2833". (8)Enable RFC3681:select "yes" to enable the rport mechanism, which requires SIP Terminal support, default value is "yes". (9)Enable Routing Mode:The default value is "yes",enabling the routing mode. (10)Enable Authentication: Select yes to enable authentication service to improve the security of voice connection (11) Pattern matching: select "yes" to enable port matching. The default value is"YES"
Service Type1/Service Type2	The reserved function

3. Call Time Limit Set

Click <Enable Call Time Limit Set> to enable settings; configuration page is shown in the following figure 6-9.

Figure0- 9 Call Time Limit Set

Default values as shown below ("0" means no limitation):

- Internale call: 0 minutes

- Local: 1440 minutes

- National Long Distance: 480 minutes

- International Long Distance: 120 minutes

4. Voice Mailbox Setting

Voice mailbox settings page is shown in the following figure 6-10

Figure 0- 10 Voice Mailbox Setting

Interface items are described as follows:

Table 6- 3 User- Voice Mailbox Setting

Items	Description
Enable Voice Mailbox	Select the single-box to enable voice mailbox.
Email Address	The email address of receiving the voice message should be filled in here.
PIN	Set the password to listen to the voice message. When using the phone to listen to the message, enter the PIN code for verification. The default value is "0000".
Voicemail Size	Maximum size of voice messages (by MB, 1MB in minimum, and 1000MB in maximum)

📖Note：

（1）Local listen to voice message: listen to the voice message on local extension, dial feature code *97.

（2）Remote listen to voice message: listen to the voice message on remote extension, dial feature code *98 and operate according to the prompt tone

（3）Before setting up voice mail box, you need to set up the SMTP settings, please refer the PBX settings-SMTP settings.

5. Unanswered Call Setting

Unanswered Call Setting is shown in the following figure 6-11

Figure 6- 11 Unanswered Call Setting

Interface items are described as follows:

Table 6- 4 User-Unanswered Call Setting

Items	Description
Unanswered Setting	Automatic Transfer to IVR, Voicemail or Hang up; default "Hang up"
Policy Time List	Default "No Data"
	Select "Automatic Transfer to IVR"then select the defined IVR policy from the drop-down box; Select "voicemail" then select the defined extension from the drop-down box, that is, select the email address of the extension user; Select "extension" and select the extension number from the drop-down box. Select "hang up" and hang up when called fail. The default value is none.

6. Music Ring Setting

Select the radio box to enable the user ring function.When calling the user it can hear the ringtone, the user can set up personalized ring in the self-service system.

After completing the setting, click the < ok > button. After the user information is added successfully, it will be displayed in the user management list, which can be sorted by user name, name and department.

Note: when registering a SIP user, please keep the registered SIP port of the SIP phone consistent with the SIP port of the system. Currently, the default SIP port of the system is "64888".

6.2.1.2 Batch import user data

It is recommended that users export user data in the Excel format. Information should include user name, name, employee ID, cell number and department.

Click the <Import> button in and go to interface as shown in the following figure.

Figure 6-12 Import User Data

Click the <Browser> button and a pop-up dialog appears as shown in the following figure.
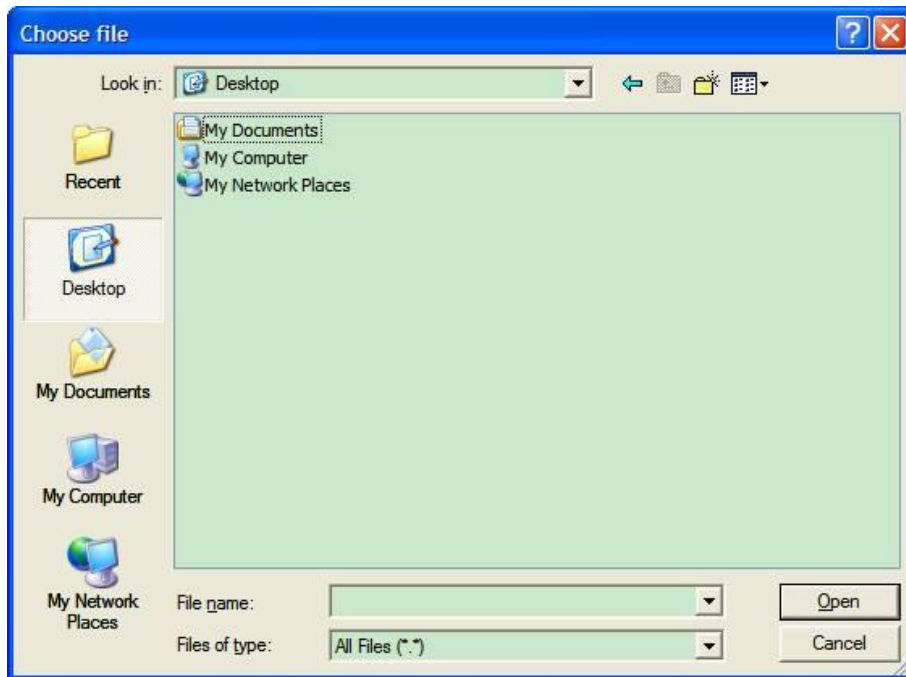
Figure 6-13 Select a File

Users will see the following figure after successfully importing data. Click the <Reload> button to make the data effective.

Figure 6-14 Import User Data Successfully

6.2.1.3 Search/Export User Data

Export User Data

Click the <Export> button in the search/export page, a pop-up dialog appears as shown in the following figure.
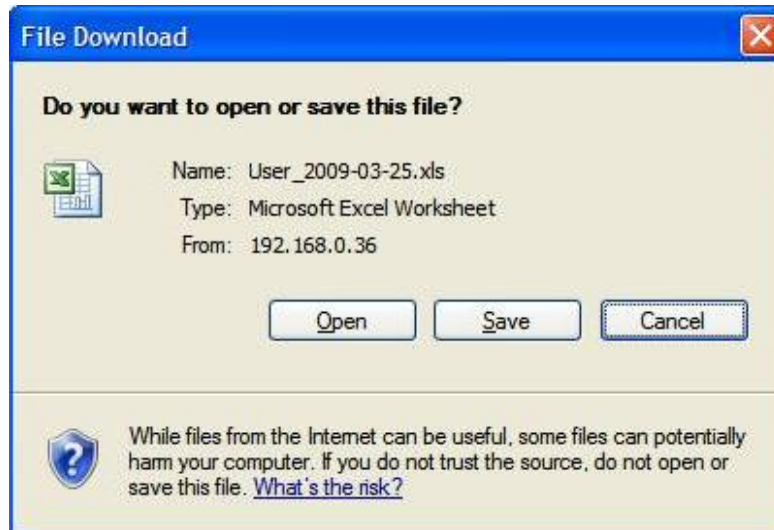
Figure 6- 15 File Download

Click <Save> button to save user data to local computer.

Batch Delete Users

Select the check box of user name, click" Delete" button to delete selected users

Search Users

Click the <Search> button in the search/export page to open the page as shown in the following figure.

Figure 6- 16 Search Users

Users can search the user by username, name, extension and department.

6.2.1.4 Delete/Edit User Data

Click "delete" and "edit" to delete and edit users as shown below.

Users								
☐	User Account ⇧	Name	Department	Extension	Route Group	Outgoing Number1	Outgoing Number2	Action
☐	6110		Default	6110				☐ ⊗
☐	8000		Default	8000	default			☐ ⊗
☐	8001		Default	8001	default			☐ ⊗
☐	8002		Default	8002	default			☐ ⊗
☐	8003		Default	8003	default			☐ ⊗
☐	8004		Default	8004	default			☐ ⊗
☐	8005		Default	8005	default			☐ ⊗
☐	8006		Default	8006	default			☐ ⊗
☐	8007		Default	8007	default			☐ ⊗
☐	8008	FAX	Default	8008	fax			☐ ⊗
☐	8009		Default	8009	default			☐ ⊗
☐	8010		Default	8010	default			☐ ⊗
☐	8011		Default	8011	default			☐ ⊗
☐	8012		Default	8012	default			☐ ⊗
☐	8013		Default	8013	default			☐ ⊗
☐	8014		Default	8014	default			☐ ⊗
☐	8015		Default	8015	default			☐ ⊗
☐	8016		Default	8016	default			☐ ⊗
☐	8017		Default	8017	default			☐ ⊗

Figure 6- 17 Delete/Edit User Data

6.2.2 Department

Users are classified according to different user groups to facilitate the management and monitoring of user information. When the user group is defined, when the user is added, the user's department is selected from the user group drop-down box.

Click "Voice Config>>User Config>>Department" to pop up figure 6-18 below. There's a default department "default"; it can't be edited and deleted.

Figure 6- 18 Department

1. Add a department

Click <Add> to pop up the figure 6-19.

Figure 6- 19 Add a department

Interface items are described as follows:

Item	Description
Name	Define the name of department, such as the marketing department.
Permission Setting	Set the subscriber group's dialing permissions. Select "allow the outside line to call the radio box, the user group can listen to the outside calls, otherwise you can only listen to the internal calls;" Select the "allow group to dial each other", the members of the user group can call each other, otherwise the members of the group can not dial each other.
Grouping Permissions Setting	Choose whether the user group and the other user groups can call each other.

Table 6- 4 Add a department

Figure 6- 20 Department List

6.3 Trunks Config

Trunks Config includes trunks config, SIP registry, inbound call, outbound call, Number transfer, dial rule, DNIS and CNIS.

6.3.1 Trunks Config

An operator system or an upper device that is registered to the upper level by trunks. The device's VoIP system, as a terminal, is registered remotely to the upper softswitch. It can make the SIP terminal of lower level manage the domestic or international long-distance calls through the successful registered operators, or connect with the upper level system, so as to realize the voice interworking between the two platforms.

Select "Voice Config>>Trunks Config>>Trunk Config" to pop the Figure 6-21 below.

Figure 6- 21 Trunk Setting

6.3.1.1 Analog Trunk

Add analog trunk

Click <Add> button to open the page as shown in the following figure.
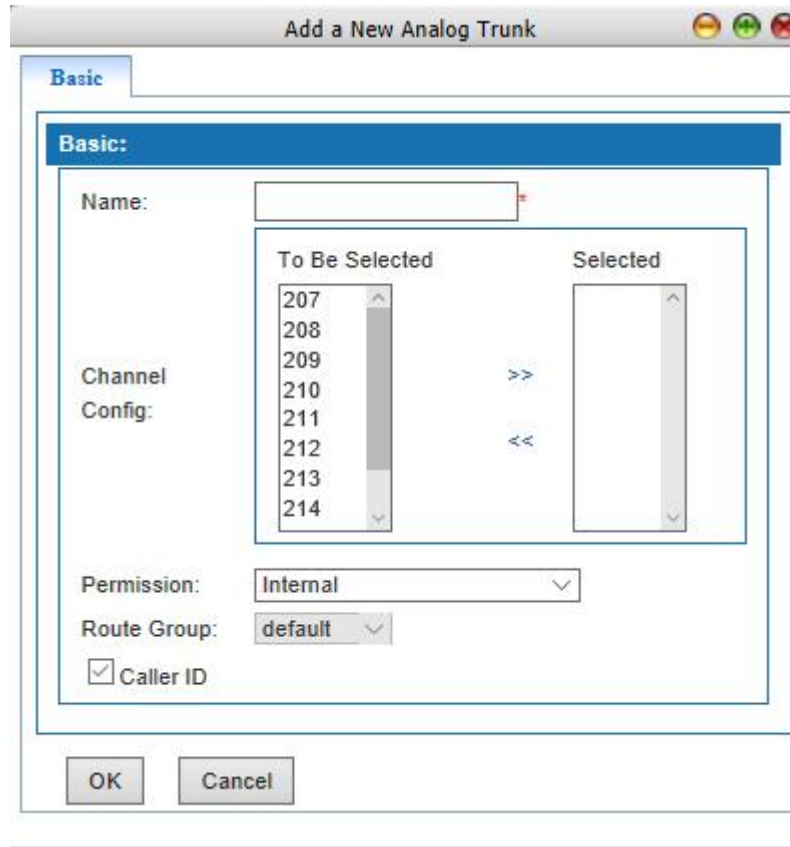
Figure 6- 22 Add Analog Trunk

Interface items are described as follows:

Table 6- 5 Add analog trunk – Basic Setting

Item	Description
Name	Name of this analog trunk
Channel Config	The channel number of the FXO port connected by the analog relay line. The option to be selected with the mouse, the continuous channel can be dragged by the mouse, multiple channels can be pressed to hold the CTRL keyboard with the mouse choice. Click "> >" after selection, and click "<< " after selecting the list. Note: The to be selected channel is the not used channel and selected channels are channels that used.
Permission	Authority of this trunk
Routes Group	Select route group in the drop-down box, default route group is "Default"
Caller ID	Select this option to display calling number,Default yes.

6.3.1.2 SIP Trunk

Add SIP Trunk

Click <Add> button to open the page as shown in the following figure.

Figure 6- 43 Add SIP Trunk – Basic Setting

1.Basic

Interface items are described as follows:

Table 6- 5 Add SIP Trunk - Basic

Item	Description
Type	Select SIP trunk type
Name	Name of this SIP trunk
Master Agent Address /Domain Name	Domain name or IP address of opposite terminal equipment
Address/Domain Name	Use for multiple host addresses, up to 5 IP addresses.
Port	Port of opposite terminal equipment filling 64888
Transport protocol	TCP, UDP,must be the same with opposite terminal equipment
URI Program	Option: SIP, TEL default value SIP
The main case type	Default value "none"

Item	Description
Permission	Authority of this trunk: Internal,Enterprise,Local,National long distance,International Long distance
DID Number	The left button in the drop-down box selects the exit number of the dial out from this trunk, and the default value is "none". Generally, the "DID number 1" can be selected.
Route Group	Select a route group, DEFAULT value is "default"
Interface Type	NNI or UNI UNI is the user side interface and NNI is the network side interface. If selecting NNI,it can choose to fill in the user name and password.If not filled ,use IP authentication; NNI docking, IP PBX A calls IP PBX B through NNI.The caller number of A can not be the same with any one number of B. Select UNI user to register, if THE CALLING NUMBER PASS THROUGH mode selected, the calling number of the extension will be taken out with a custom set number, if the radio box is not selected, the caller number of the extension will follows the number which is the register number in <PBX Features><SIP Registry>
Max Calls	Fill in the maximum number of simultaneous calls allowed on the relay, the maximum number is 32768, if more than this number of calls will be discarded, please fill in according to the actual demand, the default value of "10".
Username	Input username which provided by opposite
Password	Input password which provided by opposite

2.Advanced setting

Click < advanced> it then pops out the page as 6-24a/b
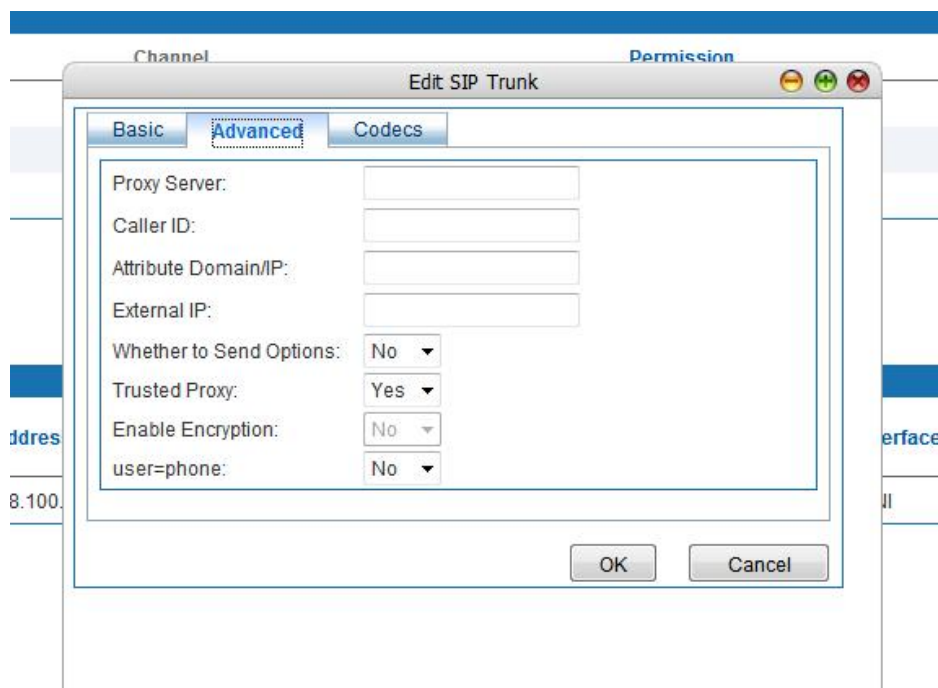
Figure 6-24a   Newly built-up   SIP advanced setting(UNI side)
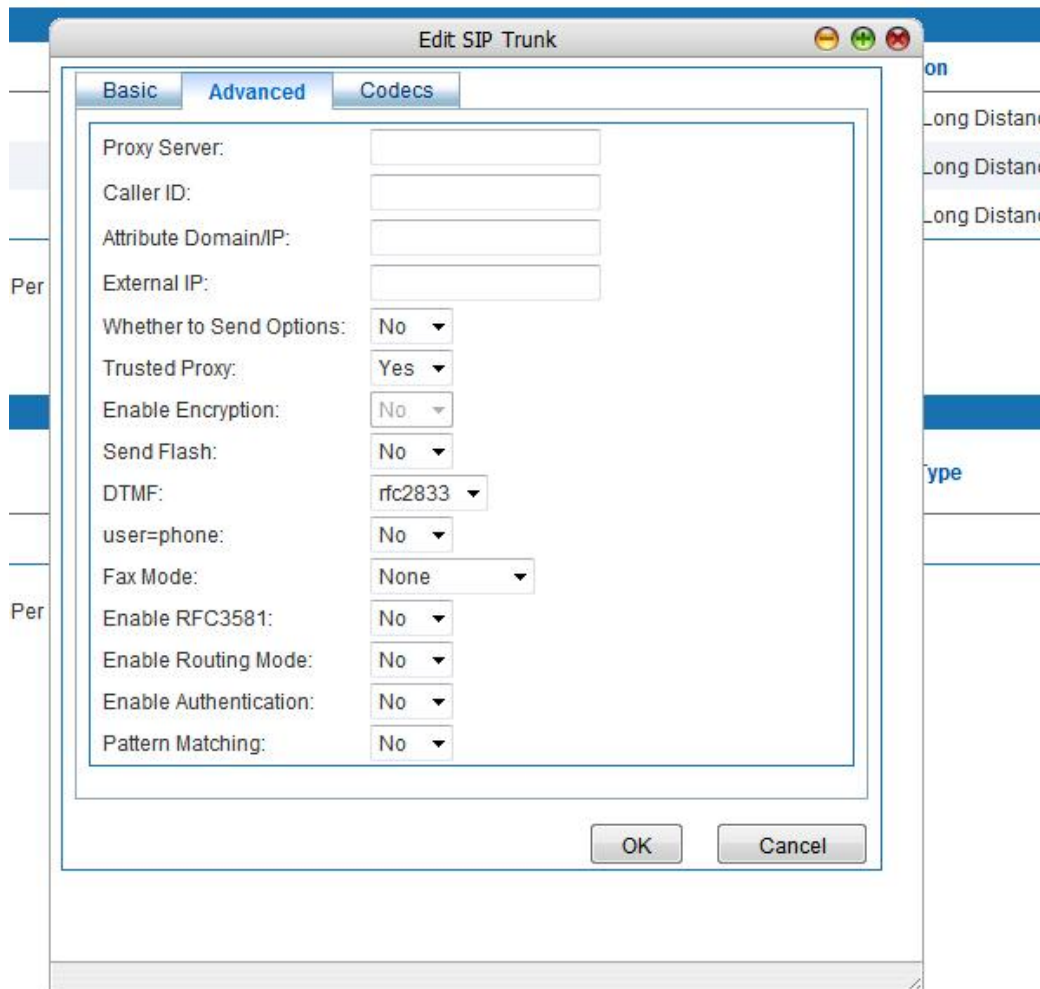
Figure 6-24b   Newly-built SIP advanced setting(NNI side)

The instruction of the interface terms is as following

Name	Function instruction
Proxy Server	When you need to connect to the registration server through the proxy, fill in the proxy server IP
Caller ID	All incoming calls from this relay call number display
Attribute Domain/IP	Fill in the domain name or IP of the home network.When it is IMS relay register,it must be filled in.
External IP	External IP address
Whether to Send Options	Select whether to send options. To select "yes", you need to fill in the following two items. Send "options" to inquire each other's ability, and the default value is "no".

Send options frequency in usual	Set the frequency of normal sending options more than 30s, and the default value is "60s".
Send options frequency in expection	Set the frequency of abnormal transmission options, over the range of 10s, and the default value is "60s".
Trusted Proxy:	Whether to open a trusted agent. Select "yes", and when the direct route to the destination is interrupted, it can be transferred by another proxy server of the device.The default value is "yes"
Enable Encryption	Default value no
Send the beat fork message	Select "yes",to send the beat fork message to the opposite;no,not send. Default "no"
DTMF	Set the sending mode of DTMF signal, the options are rfc2833, inband, info.The default is rfc2833
User=phone	When the URI scheme is SIP, this parameter determines the form of the user name, with the default value "no". Select "yes" and the user name is in the form phone@host, such as Sip: 81091143@61.142.197.38 sip / 2.0 User = phone. Select "no", the user name is in the form of user@host, such as: superman@ims.js.chinamobile.com
Fax mode	None T.30 by pass or T.38
Enable RFC3681	Default value "yes"
Enable Routing Mode	Default value "yes"
Enable Authentication	Default value "yes"
Pattern Matching	Default value "yes"

1. Codec

Click <Add> button to open the page as shown in the following figure.
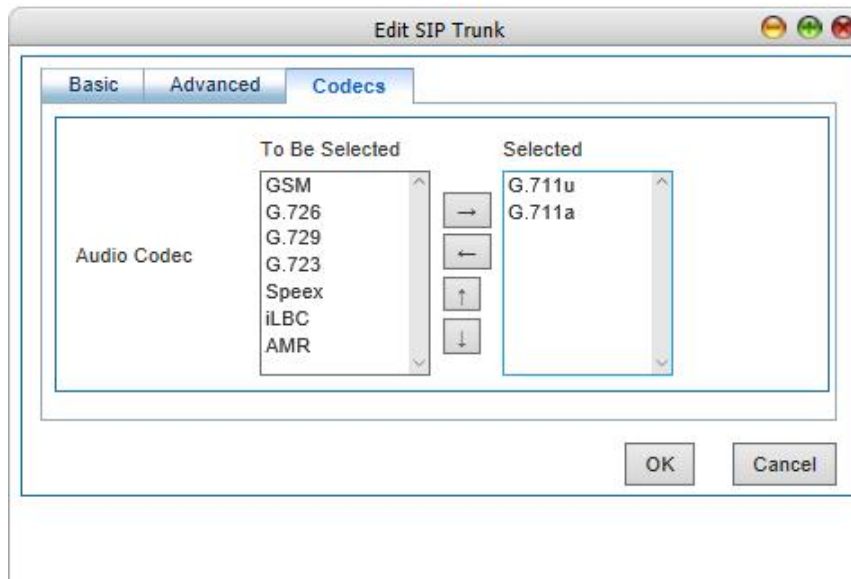
Figure 6- 24 Add SIP Trunk -Codec

Codec: GSM, G.711U, G.711A, G.723, G.726, G.729, Speex, Ilbc and AMR.

6.3.2 SIP Regitry

SIP Registry used when SIP trunk type is UNI mode.

Click "Voice Config>>Trunks Config>>SIP Registry" to open the page as shown in the following figure.
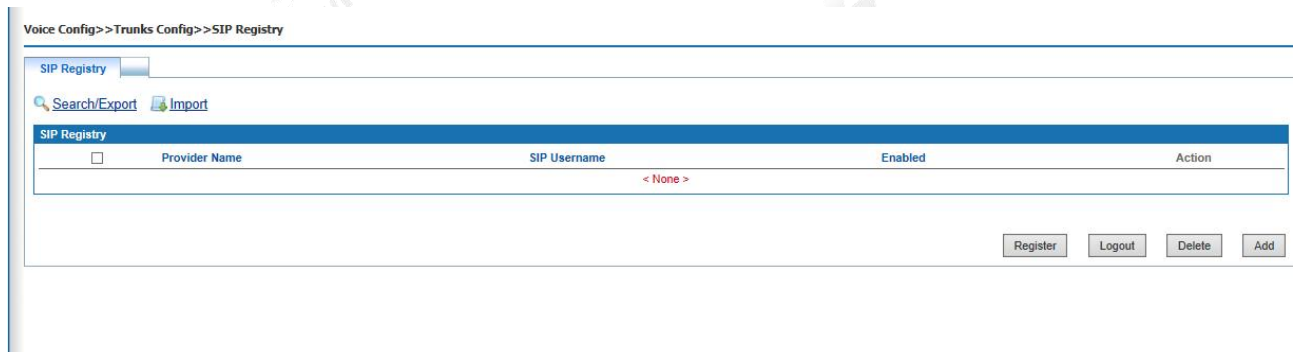
Figure 6- 25 SIP Registry

6.3.2.1 SIP Registry

Click <Add> button to open the page as shown in the following figure.

Figure 6- 26 SIP Add a New SIP Registry - Basic

Interface items are described as follows:

Table 6- 7 SIP Add a New SIP Registry - Basic

Item	Description
Provider Name	Select from provider name list, only used for SIP UNI
SIP Username	Name of SIP user
Registry Name	Registry name of SIP user
Registry Password	Password of the SIP user
Call Registry Name	Name of call registry user
Call Registry Password	Password of call registry user
Registry or not	Select "Yes", this account will be registered; select "No", this account will not be registered
Registry Time	Set the registration time, and the registration time is how often to register with the SIP agent, in unit seconds, the default is "1800" seconds

Click <Advanced> button to open the page as shown in the following figure.
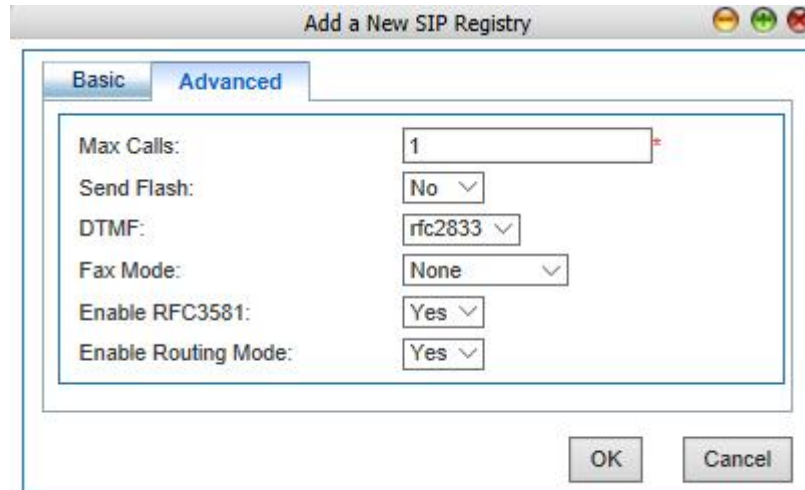
Figure 6- 27 SIP Add a New SIP Registry - Advanced

Interface items are described as follows:

Table 6- 8 Add a New SIP Registry - Advanced

Item	Description
Max Calls	Default value is "1"The maximum number of calls is configured according to the actual situation. If 10 users share this number to dial the outside line, the maximum number of calls can be configured to 10, and the default is 1. If the number is used as a fax, you need to configure DTMF as "inband" and fax type as "T30 transparent transmission".
Send Flash	Type and select "Yes" if you want to send Flash
DTMF	Option: RFC 2833, info and inband
Fax Mode	Option: T.38, T.30
Enable RFC3581	Yes or No, default Yes
Enable Routing Mode	Yes or No, default Yes

Register/Logout SIP account

Select SIP account and click <Register> button to register SIP account.

Select SIP account and click <Logout> button to log out the SIP account.

Edit SIP account

Select SIP account and click <Edit> button to edit SIP account.

Delete SIP account

Select SIP account and click <Delete> button to delete SIP account.

Batch Import SIP Account

Click <import> botton and select Excel file to import.
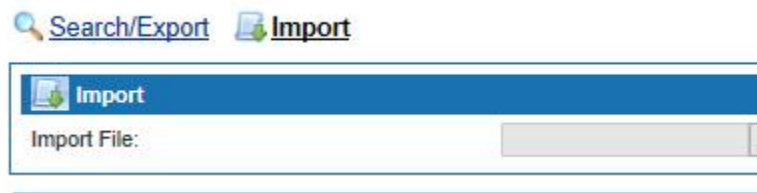
Figure6- 28 Batch Import SIP Account

Search SIP Registry

Click <Search> button to open the page as shown in the following figure.
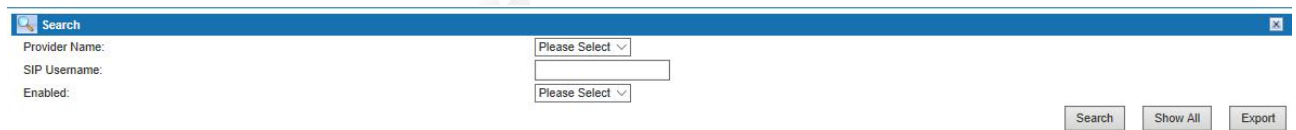
Figure 6- 29 Search SIP Registry

6.3.3 Inbound Call Routing

By setting inbound call routing, incoming calls from analog trunk can be transferred to internal extensions, IVR or agents. Users can set different inbound call routing in different time period.

Select " Voice Config>>Trunks Config>>Inbound Call " to open the page as shown in the following figure.
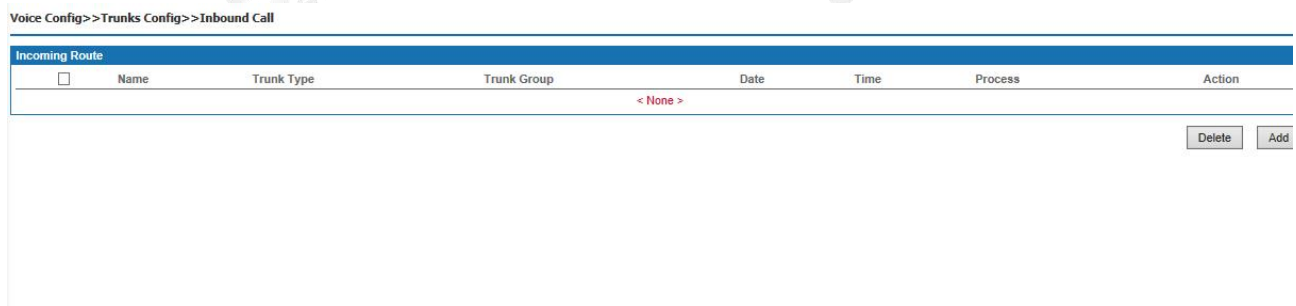
Figure 6-30 Inbound Call Routing

Add inboud call routing

Click <Add> button to open the page as shown in the following figure.

Figure 6-31 Inbound Call Routing - Basic

1. Basic

Interface items are described as follows:

Table 6- 10 Add a New Inbound Route - Basic

Items	Description
Name	Name of new inbound route.
Week	Set effective time of this route: Monday to Sunday
Hour	Set effective time of this route: 24 hours

2. Trunk Type

Click <Trunk> button to open the page as shown in the following figure.

Figure 6-32 Inbound Call Routing – Trunk Group

Interface items are described as follows:

Table 6- 11 Inbound Call Routing – Trunk Group

Items	Description
Type	Trunk type
Trunk	Trunk name

3.   Click <Action> button to open the page as shown in the following figure.

Figure 6-33 Inbound Call Routing – Action

Interface items are described as follows:

Table 6-12 Inbound Call Routing – Action

Items	Description
Extension	If the option is selected, the external call will be automatically transferred to the specified extension.
IVR	If the option is selected, the external calls will be automatically transferred to IVR.
Automatic Transfer to Operator	If the option is selected, the external calls will be automatically transferred to the specified operator.

6.3.4 Outbound Call Routing

By setting outbound call routing, users can make outbound calls through different trunks. For example, when users make local calls, they can use analog trunk; when users make long-distance calls, they can use SIP trunk. By setting reasonable outbound call routing, enterprise can reduce communication costs.

Click "Voice Config>>Trunks Config>>Outbound Call" to open the page as shown in the following figure.
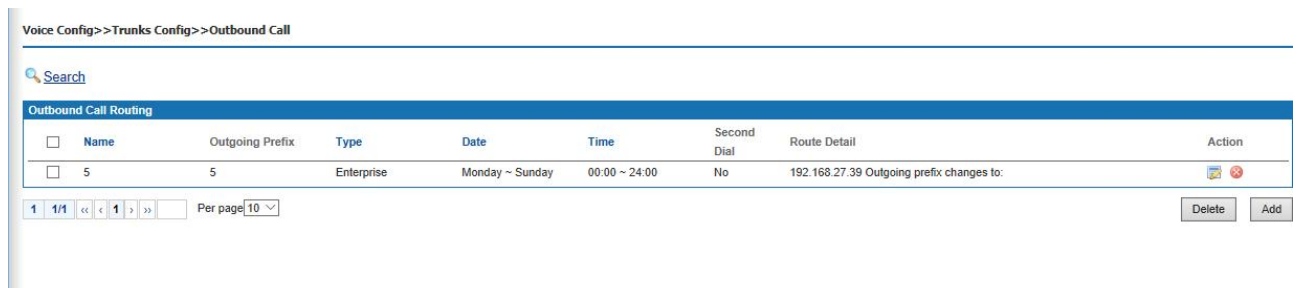
Figure 6- 34 Outbound Call Routing

Add New Outbound Route

1. Click <Action> button to open the page as shown in the following figure.

Figure 6- 35Outbound Call Routing - Basic

Interface items are described as follows:

Table 6-13 Add New Outbound Route - Basic

Items	Description
Name	Name of outbound route, 1-20 characters, can be used including a-z, A-Z, 0-9, _ and! @ # $% ^ & * ().
Linear Routing	When select,There's no outgoing prefix when enabling linear routing.When the straight line exhales, the out prefix and plays the second dial tone does not take effect;
Outgoing Prefix	Prefix of outgoing call, 0-9 and "#" . No other symbols are allowed, prefix number 0-9 and#, select the radio box, enable the playback of the second dial tone function. SIP phones have no secondary dial tone.
Call Type	Options: Enterprise, Local, National Long Distance and International Long Distance
Week	Set effective time of this route: Monday to Sunday

Attention:

(1) Linear routing does not support playback the secondary dial tone. The outgoing code and the number to be dialed should be dialed continuously. A # at the end of a number speeds up dialing.

(2) The permission of the user needs to be greater than or equal to the permission of the calling route before it can be called out from the corresponding route. For example, if the outbound route is set by the call type to "domestic long-distance", then if the user's permission is "local telephone" or other lower than "domestic long-distance" permission, it cannot be called out through this route.

(3) The setting of the effective time of the week, according to Chinese custom, if all the time is effective, please choose from "Monday" to "Sunday", remember not to choose "Sunday" to "Monday", otherwise only "Sunday" and "Monday" to take effect.

2. Click <Route> button to open the page as show in the following figure.

Figure 6- 36 Outbund Call Routing - Route

Interface items are described as follows:

Table 6-14 Add New Outbound Rout - Route

Items	Description
Type	Trunk type, sip trunk or analog trunk
Route Name	Trunk Name
Outgoing prefix changes to	0-9 can be typed.The call number after exit is the number after conversion.Blank, means match all Numbers, that is, do not transform all Numbers. If it needs to change the number,for example, needs to add 0 after the dial out ,it enters 0 here.
Router trunk configuration box	After selecting the type and name, click the < add > button to add the trunk to the text box. Select the added relay and click the < delete > button to delete the relay. Select the added relay and click the button < move up > and < move down > to change the relay priority.

Click <route group> to pops up the page as following
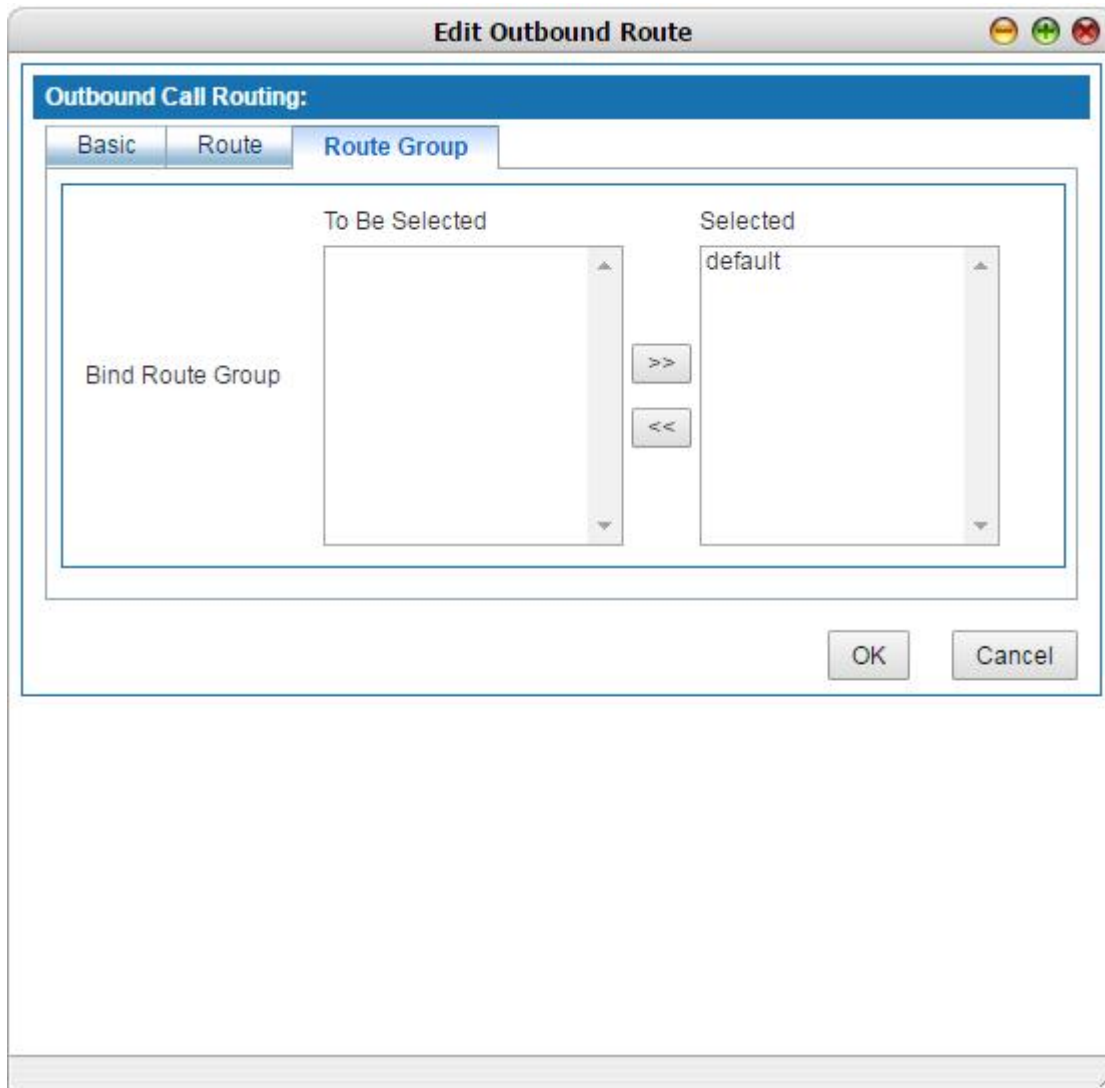
Figure 6-37　New outbound route

Select the routing group to which the routing belongs and add the routing to the selected　routing　group System default routing group "default", click the selected routing group in the group to be selected, click [>>] and add to the right box; Click the unwanted routing group in the right box and click [<<] back to the left box does not take effect. A route can be assigned to multiple routing groups.

Modify and delete the outbound route, click the [✎] button to modify the route information. Click the unwanted　route and click [✖] button to delete the outbound route.

Search outbound route

Click the < search > button, and the page as shown in figure 6-37 will pop up. The user can search the set outbound　route according to the name.
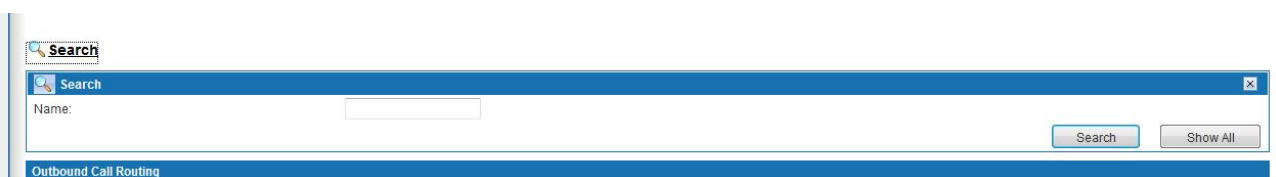
Figure 6-38 Search outbound call route

Examples:

Linear outbound call route :

Figure 6-39　Linear outbound call route example

Dial "0" outbound call route

Figure 6-40 Outgoing prefix 0 call outbound example

Dial "9" outbound call route

Figure 6-41 Outgoing prefix 9 call outbound example

6.3.5 Number Transfer

When make outbound and inbound calls, number can be changed by rules. Select "Voice Config>>Trunks Config>>Number Transfer" to open the page as shown in the following figure. Outgoing does not support analog extensions.

Figure 6-42 Number Transfer

Add Number Transfer

Click <Add> button to open the page as shown in the following figure.

Figure 6- 43 Add Number Transfer

Interface items are described as follows:

Table 6-15 Add Number Transfer

Items	Description
Name	Name of this rule
Transform conditions	
Call Type	Select Call in or Call out number
Route Group	When call type is "call in", select route group, default "all"
Outbound call routing	When call type is "call out", select route group, default "all"
Trunk	Select trunks, default "All"
Caller Number	Caller number before transfer
Called Number	Called number before transfer
Objective	

Items	Description
Transfer Type	How to change the former number, options: add, delete and edit.
Initial Position	Set initial position which need to be changed
Length	Length of the call number need to be changed, change type of "Add" cannot be filled.
Number Transfer to	Type added call number or revised call number; change type of "delete" cannot be filled.

📖 **Note:**

Original number uses 1-9, "X", "N", "Z", "*", etc. it is applied for the same regular expressions with the dial-up rule. The collective description is as follows:

- ➢ To designate a specific number, such as 114, 61202700;

- ➢ To designate the call number with a specific beginning; for example 61xxxxxx, can also be written for 61 or 61x;

- ➢ To designate this kind of expression for 268[0-1, 3-9], that means the call number beginning with 268 and the next number is 0-1 or 3-9

X can be any digit between 0-9

N can be any digit between 1-9

Z can be any digit between 2-9

Search Number Transfer

Click <🔍 **Search**> button to open the page as shown in the following figure.

Figure 6-44 Search Number Transfer

Users can search number transfer by trunk name, original number, objective and transfer type.

6.3.6 Dial Rule

Select " Voice Config>>Trunks Config>>Dial Rule" to open the page as shown in the following figure.

Voice Config>>Trunks Config>>Dial Rule

🔍 Search

	Name	Route Group	Outbound Call	Dial Rule	Does not match the strategy	Enable	Action
				< None >			

Delete   Add

Dial Rule:
Dial rule only uses 0-9, X, Z, N,[-].NOTE:
1. X: Represent any one digit number from 0 to 9.
2. N: Represent any one digit number from 2 to 9.
3. Z: Represent any one digit number from 1 to 9.
4. [2-8]XXXXXX: A seven digits number used to sending the local call,which should begin with a number from 2 to 8.
5. 02XXXXXXXXX: A eleven digits number used to sending the long-distance call.The number should begin with"02".
6. 013XXXXXXXXX: A twelve digits number used to sending the long-distance mobile phone call.The number should begin with"013".
7. 13XXXXXXXXX: A eleven digits number used to sending the local mobile phone call.The number should begin with"13".
8. 11X: A three digits number used to sending emergency call.The number should begin with"11".
9. 17911(eg.): Send the number out immediately after receiving the predifined number. 17911 here is an example, this example is to illustrate the ways of a sending a specific number out.

Figure 6-45 Dial Rule

Add a New Dial Rule

Click <Add> button to open the page as shown in the following figure.

Figure 6-46 Add a New Dial Rule

Interface items are described as follows:

Table 6-16 Add a New Dial Rule

Items	Description
Name	Name of this dial rule.It can contain upper and lower case letters, numbers and underscores
Route Group	Select route group
Outbound Route	Select configured outbound route

Items	Description
Dial Rule	Please refer to dial rule description
Does not match the strategy	Select "send out does not match", and when dialing and dialing rules do not match, the signal is sent out over reaction time. Select "send immediately when does not match", when dialing and dialing rules do not match, send out the signal immediately. Select "does not match then hang up immediately ", when dialing and dial rules do not match, immediately hang up, the default value is "send out does not match"
Enable Dial Rule	Each time only one rule can be enabled

Dialing rule is described as follows:

Dialing rules can use the "0-9", "X", "Z", "N", and "-" symbols

Table 6-17 Dial Rule

Items	Description
"X"	Any digit between 0 to 9
"N"	Any digit between 2 to 9
"Z"	Any digit between 1 to 9
[2-8] XXXXXX	A seven digits number used to send local call which first digit should from 2 to 8.
02XXXXXXXXX	An eleven digits number used to send long-distance call which first two digits should begin with"02".
013XXXXXXXXX	A twelve digits number used to send long-distance mobile phone call. The number should begin with"013".
13XXXXXXXXX	An eleven digits number used to send local mobile phone call. The number should begin with"13".
11X	A three digits number used to send an emergency call. The number should begin with"11".
17911 (an example)	Send the number out immediately after receiving the predefined number. 17911 here is an example, this example is to illustrate the ways of a sending a specific number out.

6.3.7 DNIS

It is allowed that different "Call In" policies can be used according to the incoming DNIS (Destination Number Identification Service), which is usually used for the extension number with multiple routing policies. For instance, one extension is forwarded to extension A in a certain time, and forwarded to extension B in another certain time, or will prompt the client that user is not in the company during holidays.

Select " Voice Config>>Trunks Config>>DNIS" to open the page as shown in the following figure.

Figure 6-47 DNIS

Click <Add> button to open the page as shown in the following figure.

Figure 6-48 DNIS

Interface items are described as follows:

Table 6-18 DNIS

Items	Description
Name	Name of this rule
DNIS Number	DNIS number
Action	The selection boxes under the number are the action selection boxes. Calling DNIS number triggers the selected action. The options of the action include IVR, extension, conference, play prompt tone(can't be

Items	Description
	interrupted) play prompt tone(can be interrupted)voicemail, group call, queue, wait, hang up and dial (not forwarded to voice mail).
Action List	Click <Add> after the selected action and its content, the selected action will be displayed in the action list. If there is more than one action, they will be arranged in line from top according to the sequence of the actions. The order of the action list can be adjusted with the buttons <Up> and <Down>. The unnecessary actions can be deleted with the <Remove> button.
Time	Set the time when the rule takes effect. By default, select week, from Monday to Sunday, and 24 hours, or all times.

&instructions

(1) The setting of the effective time of the week, according to Chinese custom, if all selected, please choose from "Monday" to "Sunday", remember not to choose "Sunday" to "Monday", otherwise only "Sunday" and "Monday" will take effect.

(2) DNIS is only applicable to SIP trunk.

6.3.8 CNIS

Select " Voice Config>>Trunks Config>>DNIS" to open the page as shown in the following figure.
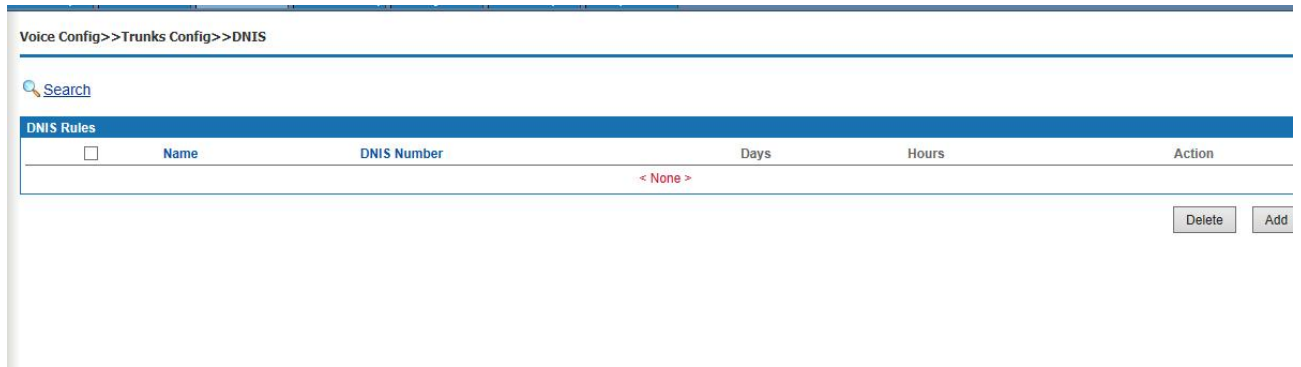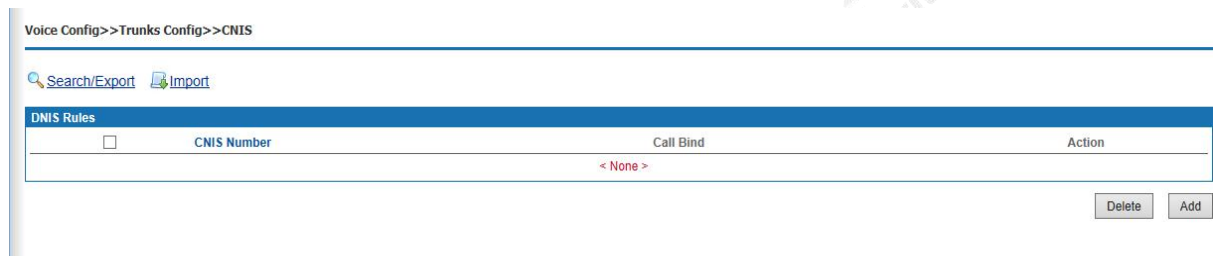

Figure 6-49 CNIS

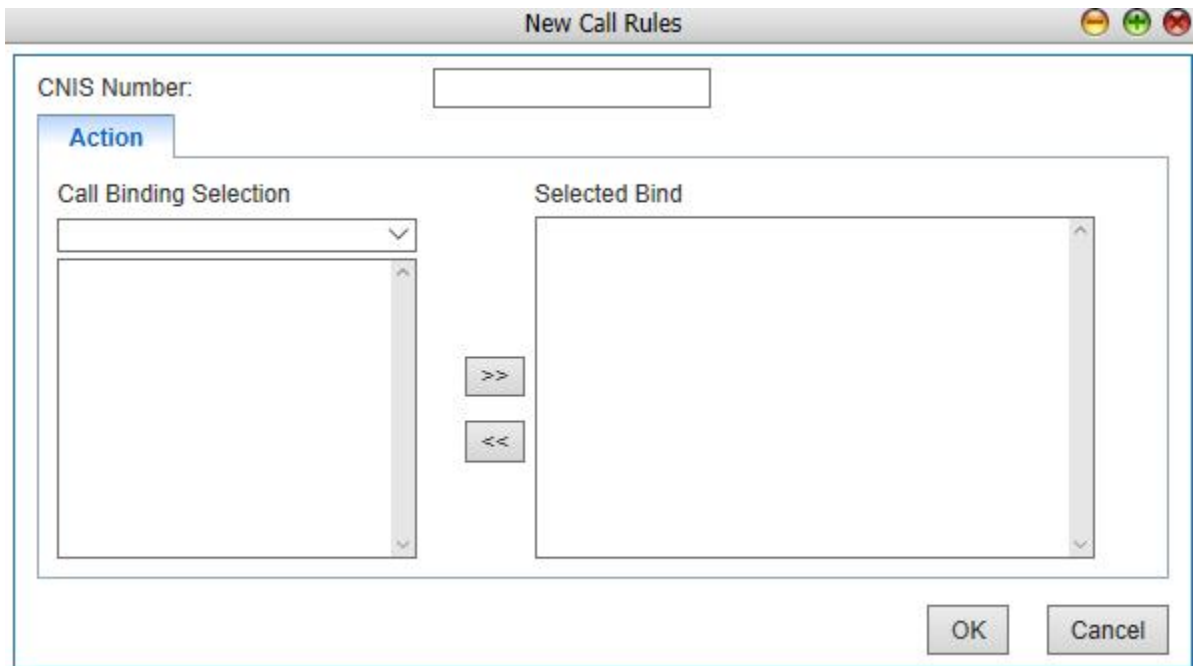Click <Add> button to open the page as shown in the following figure.

Figure 6-50 Add New Rule

Interface items are described as follows:

Table 6-19 Add New Rule

Items	Description
CNIS Number	CNIS number is defined according to demand. It can not repeat with internal system number，such as extension number, extension outgoing number, DNIS number, queue number, etc.
Action	1) Call binding selection: Currently, it can support FXO port，IMS trunk and SIP UNI trunk 2) Selected bind: same type can only bind 1 port, and this bind is bidirectional, for example, when the FXO port 1 is selected, it is indicated that the CNIS number is out of the FXO port 1, while the call coming in from the FXO port 1 is turned to the CNIS number.

Note:

(1) the called number must meet the dialing rules (see 6.3.6 dialing rules for details), in order to be eliminated from the designated relay set by the calling number identification.

(2) Called number identification priority is higher than calling number identification

(3) If the called number is the internal number of the device system, the calling number identification rule is invalid; Called number is the number outside the system, then it is according to the calling number identification rules to call out.

6.4 PBX Features

PBX features include call transfer, call waiting, three-way call, hotline, call pickup, clock, speed dial, blacklist, follow me, voicemail, IVR, queue, billing, etc.

6.4.1 Feature Code

Select "Voice Config>>PBX Features>>Feature Code" to open the page as shown in the following figure.

Figure 6-51 Basic Features

6.4.2 Basic Features

The basic page is as shown in the above figure which introduces the operation method of basic configuration by using extension. Characteristic number begins with "*" or "#", dialing characteristic number is able to trigger corresponding function.

Interface items are described as follows:

Table 6-20 Basic Features

Items	Description
Appointed Pickup	The characteristic number is **. A certain extension rings, while other extensions can dial "** + the number of the ringing extension" to pick up the phone call.
Group Call Pickup	The characteristic number is *115. If one of the extensions in the same group rings, you can press *115 on other extensions to answer the phone. If there is more than one extension ring, the order of pickup is the sequence of ringing.
Speed Dial Prefix	The characteristic number is *0. For example, to dial 999 with the fast dial whose prefix is set to 1 for the number 999, just dial "*01".
Speed Dial	The characteristic number is *75. The ten numbers from 0 to 9 can replace ten special telephone numbers. Users need only dial "*0 + the corresponding number" to call those users. For the business registration, dial *75 on the extension, enter a shortcut key after the prompt tone, and enter the number the shortcut key represents after the other prompt tone.
Record	The characteristic number is *77. Dial the number with the extension, and you can record after the prompt tone. Hang up the phone to end recording.
DND Activate	The characteristic number is *78. Dial the number, and other users who dial the number of this extension will hear the busy tone.

Items	Description
DND Deactivate	The characteristic number is *79. Dial the number with the extension, which can deactivate DND service.
Check Recording	The characteristic number is *99. Dial the number to listen to the recording on the extension. Press 1 to listen to it again after the recording is finished. Press * to record again. The new recording will replace the original one.
Phone Login	The characteristic number is *105. Dial the number with the logout extension, and enter the password after the prompt tone to login the extension.
Phone Logout	The characteristic number is *106. Dial the number with the extension, and enter the password after the prompt tone to logout the extension. Other users who dial the number of the extension will hear the logout prompt.
Absent Activate	The characteristic number is *103. Dial the number, and the extension will enable absent status. Other users who dial the number of the extension will hear the absence prompt.
Absent Deactivate	The characteristic number is *104. Dial the number with the extension, which can deactivate absent status.
Check Own Number	The characteristic number is *111. Dial the number with the extension to check extension number.
Calling Line ID Blocking	The characteristic number is *114. Dial the number with the extension to hide the extension number.
Alarm Clock Setting	The characteristic number is *66. Dial the number with the extension to set alarm clock.
Password Dialing	The characteristic number is *88. Dial *88 enter password, prefix+outbound call number to make calls
Set Secretary	The characteristic number is *67. Dial the number with the extension to enable secretary service
Cancel Secretary	The characteristic number is *68. Dial the number with the extension to cancel secretary service
Card to dial	The characteristic number is *201, enter card number and password according to the prompt tone
Card number password modification and balance inquiries	The characteristic number is *202. Dial the number with the extension to change card number and password or check balance
Query extension balance	The characteristic number is *203. Dial the number with the extension to check balance.
Remaining on the domestic and international duration	The characteristic number is *204. Dial the number with the extension to check remaining domestic and internation call duration
Extension ringing test	The characteristic number is *116. When dialing *116, you can hear the prompt "please hang up" and the bell will ring.
Monitor	*33+extension number The user can monitor the call of this extension,only listen to not talk in
Barge	*34+extension number Users can strongly plug in the extension in real time. Strong plug definition: participate in the extension call
Force release	*35+extension number The user can forcibly disassemble the extension to talk

6.4.1.1 Call Transfer

Call transfer page is as shown in the following figure which introduces the operation method of basic configuration by using extension. Characteristic number begins with "*" or "#" , dialing characteristic number is able to trigger corresponding function.

Figure 6-52 Call Transfer

Interface items are described as follows:

Table 6-21 Call Transfer

Items	Description
Activate Call Transfer No Answer	Characteristic number is *52. Extension A dials *52, and set call Transfer no answer to extension B. When someone calls A, the call will automatically transfer to extension B.
Deactivate Call Transfer No Answer	Characteristic number is *53. Dial *53 on extension can deactivate call Transfer no answer.
Activate Call Transfer Unconditional	Characteristic number is *72. Extension A dials *72, and set call Transfer unconditional to extension B. When someone calls A, the call will automatically transfer to extension B.
Deactivate Call Transfer Unconditional	Characteristic number is *73. Dial *73 on extension can deactivate call Transfer unconditional.
Activate Call Transfer on Busy	Characteristic number is *90. Extension A dials *90, and set call Transfer on busy to extension B. When someone calls B, the call will automatically transfer to extension B.
Deactivate Call Transfer on Busy	Characteristic number is *91. Dial *91 on extension can deactivate call Transfer on busy.
Blind Transfer	Characteristic number is *26. Enable this service on the page; during a call between extension A and extension B; extension A dials *26, after listen to the prompt tone, extension A dials extension C. Extension B and C can establish a call, and extension A hangs up automatically.
Attended Transfer	Characteristic number is *26. Enable this service on the page; during a call between extension A and extension B; extension A dials *26, after listen to the prompt tone, extension A dials extension C. Extension A hangs up, and extension B and C can establish a call.

6.4.1.2Call Waiting

Call forwarding page is as shown in the following figure which introduces the operation method of basic configuration by using extension. Characteristic number begins with "*" or "#", dialing characteristic number is able to trigger corresponding function.

Voice Config>>PBX Features>>Feature Code

Figure 6-53 Call Waiting

Interface items are described as follows:

Table 6- 22 Call Waiting

Items	Description
Activate Call Waiting	The characteristic number is *70. Dial *70 on extension to activate this service, this handy feature allows a person to receive a call while he or she is already on the line with someone else.If you are a SIP call and a new call is coming in, you can choose to listen or reject. If you choose to receive, you can also switch back and forth between two incoming calls. If you are a analogue phone, you will hear a beep. When the phone rings, you can pick it up again
Deactivate Call Waiting	The characteristic number is *71. Dial *71 on extension to deactivate this service

6.4.1.3 Black List

Call blocking page is as shown in the following figure which introduces the operation method of basic configuration by using extension. Characteristic number begins with "*" or "#", dialing characteristic number is able to trigger corresponding function.

Voice Config>>PBX Features>>Feature Code

Figure 6-54 Black List

Interface items are described as follows:

Table 6-23 – Black List

Items	Description
Activate Blacklist	The characteristic number is *30. Dial *30 and enter the blacklist number after prompt tone, press 1 to confirm the setting.
Deactivate Blacklist	The characteristic number is *31. Dial *31 and enter the number which need to be removed from blacklist, press 1 to confirm the setting.

Items	Description
Add last incoming call number into blacklist	The characteristic number is *32. Dial*32 to put last income call number into blacklist, press 1 to confirm the setting.

6.4.1.4 Call Busy Back

Figure 6-55 Call Busy Back

Interface items are described as follows:

Table 6-24 Call Busy Back

Items	Description
Call Busy Back Activate	Press *37 to activate call busy back service
Call Busy Back Deactivate	Press *38 to deactivate call busy back service
Call Busy Back	Press *69 to register callbusy back service

Steps:

1. Extension A calls extension B, B is on the phone, and extension A has enabled call back service.

Step:

1. Extension A calls extension B, B is on the phone

2. Extension press *69 to register call busy back service and then hang up

3. Extension B finish the previous call and hang up

4. Extension A answer the   system back

5. Extension B answer the   system back

6. Extension A and B build the call successful.

Attention:

(1)Call busy back service can be only used between extensions.

(2)The called extension should be in condition of on the phone,if the called extension is just picking up the phone or other status,the call busy back affair doesn't take effect.

6.4.1.5 Three Party Call

Service Process:

1. Extension A makes a call with extension B

2. Extension A press hookswitch and call extension C, A and C establish calls; at this time extension is holded

3. Extension A press hookswitch and press digital key 3; A, B and C establish three party calls

6.4.1.6 Inquire Transfer

Service Process:

1.   A call front desk B, B answers, B needs to transfer the phone to the colleague extension C.

2.   B   press hookswitch and call C, C answers, B and C establish a call, and then B hang up

3.   A and C establish a call

6.4.1.7 Blind Transfer

Service Process:

1.   A call front desk B, B answers, B needs to transfer the phone to the colleague extension C.

2.   B   press hookswitch and call C, B hears ring back tone and hang up before C pickup the phone; extension A hear the ring back tone

3.   A and C establish a call

6.4.2 Hotline

Hotline (also called an automatic signaling service, ringdown, or off-hook service) is a point-to-point communications link in which a call is automatically directed to the preselected destination without any additional action by the user when the end instrument goes off-hook. Hotline includes instant hotline and delayed hotline.

Select " Voice Config>>PBX Features>>Hotline" to open the page as shown in the following figure.
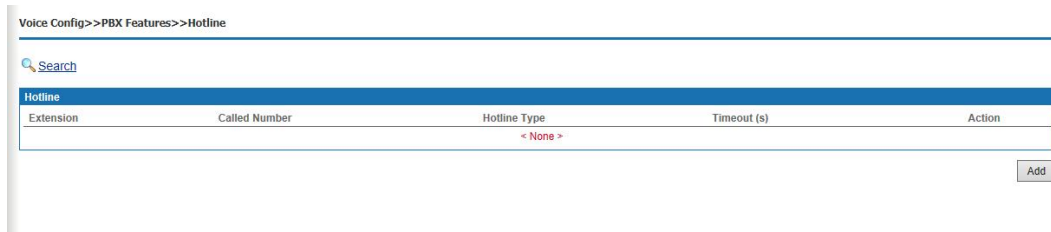
Figure 6-56 Hotline

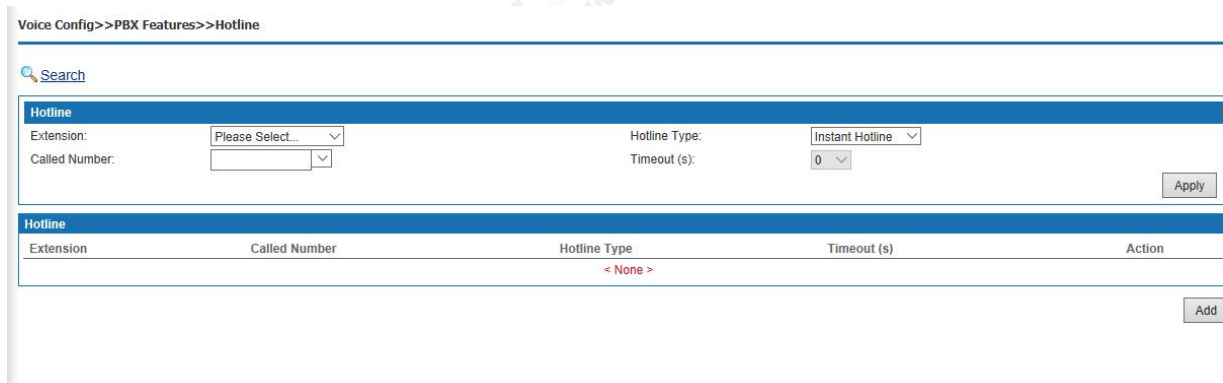Click <Add> button to open the page as shown in the following figure.

Figure 6-57 Add New Hotline

Interface items are described as follows:

Table 6-25 Add New Hotline

Items	Description
Extension	Select which extension enables hotline service
Hotline Type	Delayed hotline or instant hotline
Called Number	Destination number
Timeout	When selected delayed hotline, select delay time from 0-10 seconds.

6.4.3Group Pickup

Select " Voice Config>>PBX Features>>Group Pickup" to open the page as shown in the following figure.

Group Call Pickup:

If there is no answer when an extension is ringing in a group, other members could pickup for him as the following operation.

1. Usage: In a group, if there is no answer when an extension is ringing, including outbound and inbound calls, members can pick up the phone and press *115 after hearing the dial tone.

2. NOTE: The extension does not need to designate the called extension number; he just needs to follow the above operation. If several extensions ringing simultaneously; users can pick up according to calling sequence.
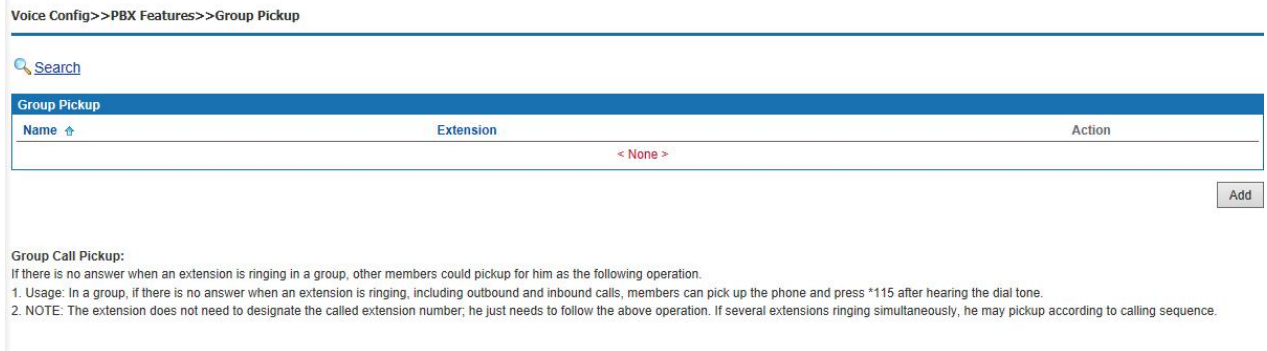
Figure 6-58 Group Pickup

Add Extensions to a Group

Click <Add> to open the page as shown in the following figure.

Figure 6- 59 Add Extensions to a Group

Interface items are described as follows:

Table 6-26 Add Extension to a group

Items	Description
Name	Name of this group
Extension	Add extension numbers to this group

6.4.4 Music Ring

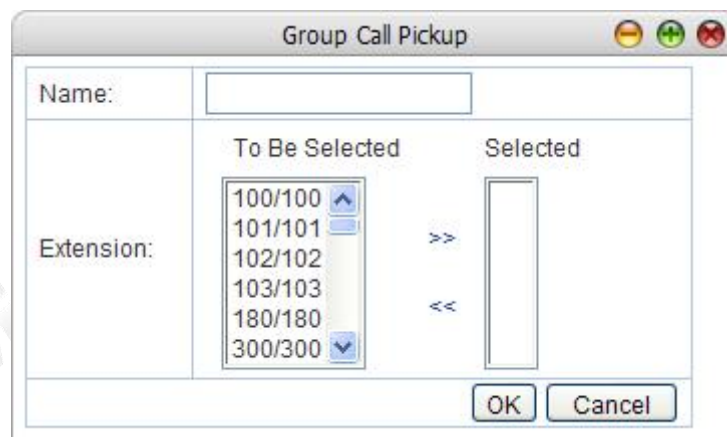Select "Supplement Service>Music ringtone Back Tone" to open the page as shown in the following figure.
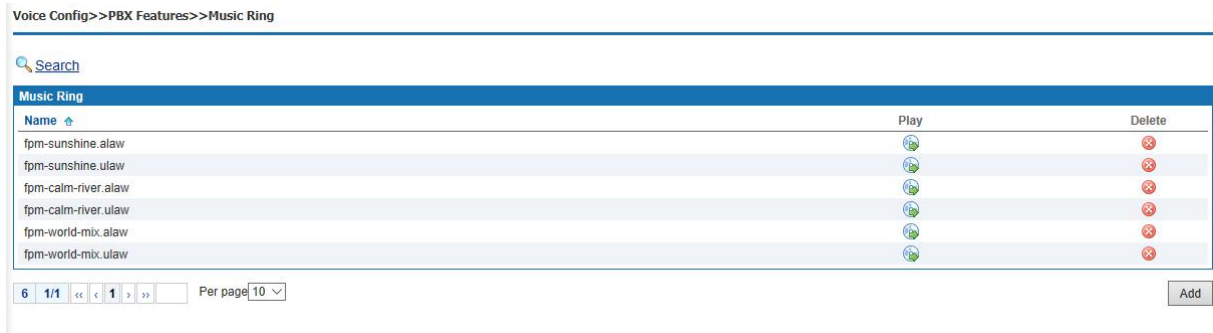
Figure 6- 60 Music Ring

Add a CRBT

Click <Add> to open the page as shown in the following figure.

Figure 6- 61 Add Music ringtone Back Tone

Click <Browser> button to select local music files, and then click the <Upload> button to upload the music to system.

Play CRBT

Click <▶> button to play CRBT.

Search CRBT

Click <🔍 **Search**> button to open the page as shown in the following figure.

Figure 6- 62 Search CRBT

Users can search CRBT by name.

Note:

(1) Users can upload or record personalized color ringtones in the self-service system.

(2) Upload audio files in 8kHz, 16bit, mono format of wav, alaw, ulaw and GSM file.

6.4.5 Alarm Clock

Users can set the alarm clock to make the extension ring at the specified time, thus to prevent missing any important arrangement.

Select " Voice Config>>PBX Features>>Alarm Clock" to open the page as shown in the following figure.
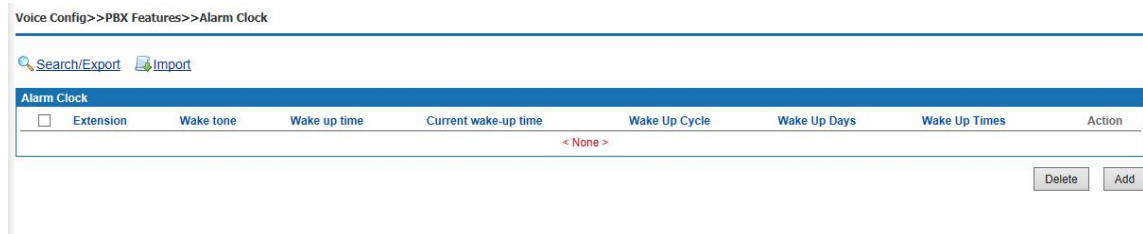
Figure 6- 63 Alarm Clock

Add Alarm Clock Service

Click <Add> to open the page as shown in the following figure.

Figure 6- 64 Add Alarm Clock Service

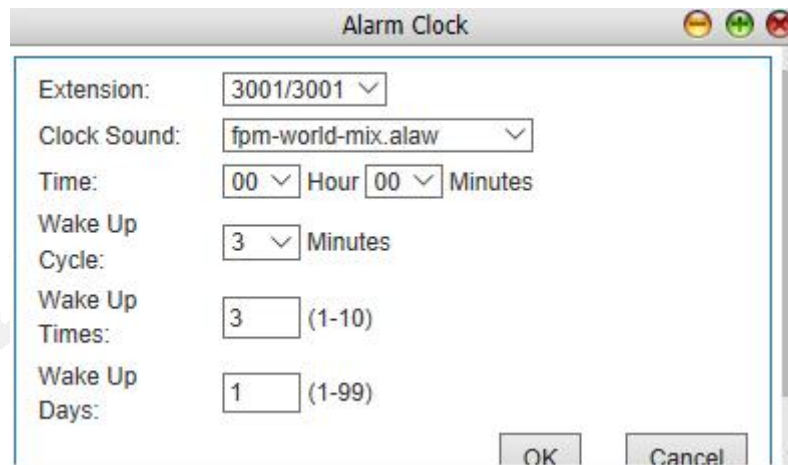Configure extension number, clock sound and effective time of alarm clock service.

Search Alarm Clock Service

Click < Search> button to open the page as shown in the following figure.

Figure 6- 65 Search Alarm Clock

Users can search the alarm clock that has been set in accordance with extension.

6.4.6 Speed Dial

Speed dial is a function, which allows the user to place a call by pressing a reduced number of keys.

Select " Voice Config>>PBX Features>>Speed Dial" to open the page as shown in the following figure.
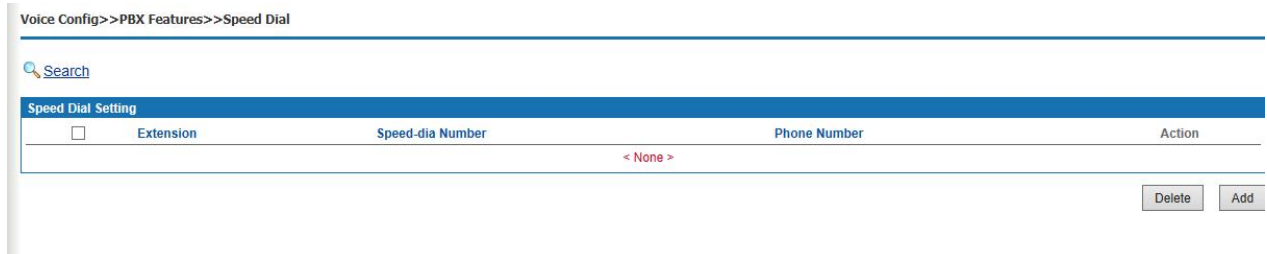
Figure 6- 66 Speed Dail

Add a Speed Dial

Click <Add> to open the page as shown in the following figure.

Figure 6- 67 Add a Speed Dial

Interface items are described as follows:

Table 6- 27 Add New Speed-dial

Items	Description
Extension	Select extension number
Speed-dial Number	The corresponding speed-dial key for the phone number.
Phone Number	Phone number which needed to be dialed with the speed-dial number

Search Speed-dial

Click < 🔍 **Search**> button to open the page as shown in the following figure.

Figure 6- 68 Search Speed-dial Policy

Users can search the speed dial by extension number, speed-dial number and phone number.

6.4.7 Call Transfer

Select " Voice Config>>PBX Features>>Call Transfer" to open the page as shown in the following figure.

Figure 6- 69 Call Transfer

Configure Call Forwarding

Click < > button to open the page as shown in the following figure.
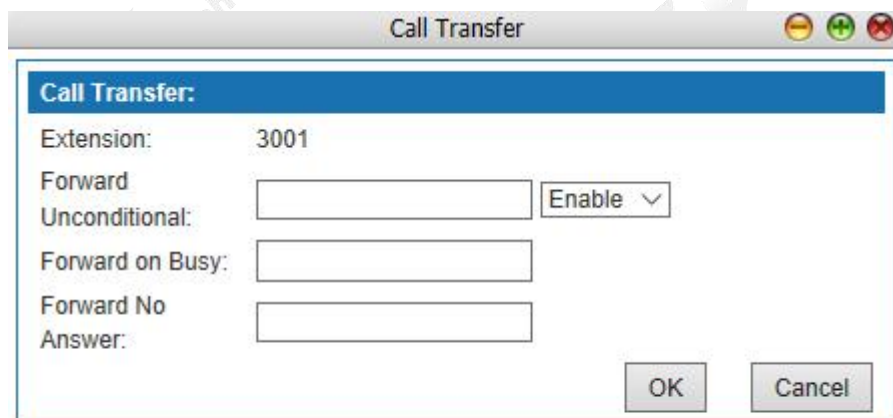
Figure 6-70 Edit Call Transfer

Interface items are described as follows:

Table 6- 18 Call Forwarding Configuration

Items	Description
Extension	Extension number
Forward Unconditional	Incoming calls will be forwarded to another preset phone number.
Forward on Busy	Incoming calls will be forwarded to another preset number when the line is busy.
Forward No Answer	Incoming calls will be forwarded to another preset number when no one answers the call.

Search Call Forwarding

Click <🔍 **Search**> button to open the page as shown in the following figure.

Figure 6- 71 Search Call Forwarding Policy

Users can search call-forwarding policy by extension number, forward unconditional, forward on busy and forward no answer.

6.4.8 Black List

Users can refuse the incoming calls from some certain numbers to prevent users from unacceptable calls.

Select " Voice Config>>PBX Features>>Black List" to open the page as shown in the following figure.

Figure 6-72 Black List

Add Blacklist

Click <Add> to open the page as shown in the following figure.

Figure 6- 73 Blacklist Configuration

Interface items are described as follows:

Table 6- 29 Blacklist Configuration

Items	Description
Extension	Select extension number
Block Number	Phone number that the extension is designated not answer.

Search Blacklist

Click <🔍 **Search**> button to open the page as shown in the following figure.

Figure 6- 74 Search Blacklist

Users can search blacklist by extension number and block number.

6.4.9 White List

Select " Voice Config>>PBX Features>>White List" to open the page as shown in the following figure.
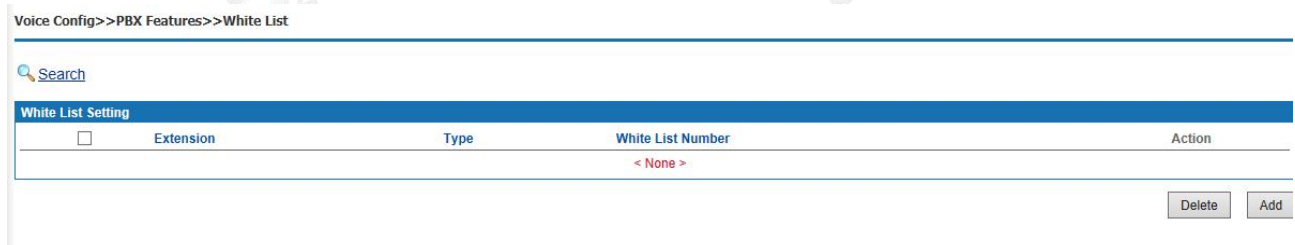
Figure 6-75 White List

Add Whitelist

Click <Add> to open the page as shown in the following figure.
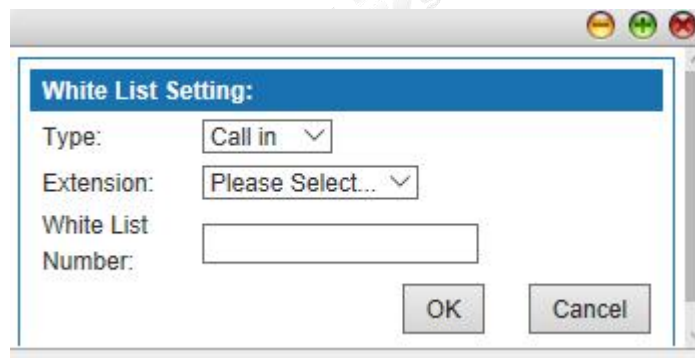
Figure 6- 76 Whitelist Configuration

Interface items are described as follows:

Table 6- 30 Blacklist Configuration

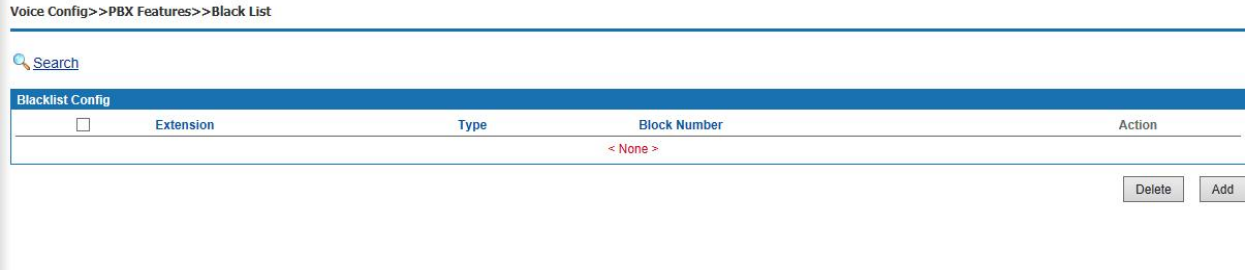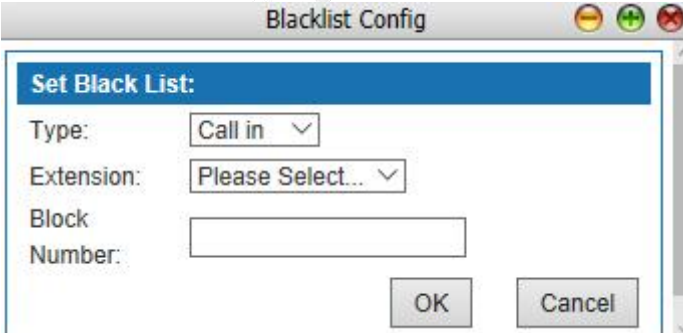| Items	Description
Extension	Select extension number
White List Number	Phone number that the extension is designated answer and call out

Search Blacklist

Click <🔍 **Search**> button to open the page as shown in the following figure.

🔍 **Search**

🔍 Search	
Extension:	
White List Number:	

Figure 6- 77 Search Whitelist

Users can search blacklist by extension number and white list number.

6.4.10 Secretary

According to the set rules, the call can be filtered through the secretary extension and then transferred to the manager extension, which greatly saves the manager's time and avoids unnecessary interruptions.The secretary can decide whether to transfer to the manager or not just by hook flashing to the manager extension .Select the " Voice Config>>PBX Features>>Secretary", the pop-up page as shown in the figure below.

Voice Config>>PBX Features>>Secretary

🔍 Search

Secretary Business Setting		
Manager Extension ⇩	Secretary Extension	Action
	< None >	
		Add

Figure 6-78 Secretary

Steps:

1. Business Settings (in global parameters)

Seleect "Voice Config>>PBX Settings>>Global Setting"

Business Setting		
Secretary:	Global / Internal / External	
		Apply

Figure 6-79 Business Setting

● Global: internal extension or outside number call manager number, all calls reach the secretary first;

● Internal: refers to the internal extension call manager number, reach the secretary first; outside number calls manager number, directly to the manager;

● External: refers to the outside number call manager number, reach the secretary first; internal extension calls manager number, directly to the manager;

1. Add Secretary Number

Click <Add> to open the page as shown in the following figure.

Figure 6-80 Add Secretary Number

Interface items are described as follows:

Table6-31 Add Secretary Number

Items	Description
Manager Extension	Extension of manager
Secretary Extension	Extension of secretary

6.4.11 Follow Me

When user is being called, phones will concurrently or sequentially vibrate accord to the setting. In the circumstance of concurrent vibration, if one terminal picks up the phone, then other ringing will stop. Under the circumstance of sequential vibration, if one terminal doesn't answer the phone in the setting time, then the call will transfer to next terminal.Note: when the analog outside line rings, the inside line will not ring.

Select "Voice Config>>PBX Features>>Follow Me" to open the page as shown in the following figure.

Figure 6-81 Follow Me

Interface items are described as follows:

Table 6-32 Follow Me

Items	Description
Extension	Extension number of follow me strategy
Strategy Name	Name of this strategy
Ringing Mode	Options: Ring All, Ring one by one, RR with memory Ring all: All the extensions ring together Ring one by one: Ring in the sequence of number 1-to number 4th.
Ringing Interval	Ringing duration of each phone
Timeout	Total ringing time
Extension	Extension number
Number	You can choose the extension number or directly click on the number bar to input the outside line number (note that you need to add outlet prefix before the outside line number), you can set five Numbers, the number one is the default extension number of the device.
Enable	Enable the strategy

6.4.12 Voice Mail

Voice to Email breaks traditional method of checking voice message, which provides users good mobility. Wherever you are – on vacation, a business trip or just traveling in your hometown; you'll never miss any voice message.

Functions of voice mail are as follows:

1) Transfer to voice mail box when call failed

2) Voice messages can be saved in system's voice mail box

3) Send voice message to specific email box

4) Supports locally and remotely listen to the voice message

Select "Voice Config>>PBX Features>>Voice Maill" to open the page as shown in the following figure.

Figure 6-82 Voice Mail

Interface items are described as follows:

Table 6-33 Voice Mail

Items	Description
Listen to voicemail	Dial *97 on extension to listen to local voice message
Listen to voicemail	Dial *98 on extension to listen to voice message remotely
Seconds before Voicemail	The call will be forwarded to the voice mail if the destination user does not answer for the defined time. To open voicemail, you need to select the call failure policy as voicemail.The value should be the same with the ring time setted in the PBX settings> Global setting,default time is 30s.
Max Messages	The maximum pieces of message can be 1000，default value is 1000.
Min Length (sec)	The minimum length of the message can be from 1 to 60 seconds
Max Length (sec)	The maximum length of the message can be from 1 to 60 seconds
Subject	The destination users can receive the message in the voice mail with the subject The default value "Voicemail".
Signature	The signature of the sender. The default value is "Admin"

(1) when listening to the voice message, the system may prompt you to input the password, the password is the PIN code in the voice message, the initial password is "0000", please contact the administrator for details, please refer to 6.2.1.1 to add the voice mail box Settings of a single user.

(2) before setting up voice mail, SMTP server needs to be set up first. See 6.6.9 SMTP setting for details

6.4.13IVR

Device uses convenient auto-answer system. Users can customize IVR flow according to their needs. Through in-house software platform, the unit can provide IVR service, and users don't need additional IVR server and related boards, which can reduce investment. Through Graphical User Interface, users can easily customize the IVR flow, and modify IVR flow according to the change of services.

Enterprise attendant functions as follow:

1) Play greetings and announcements when there're incoming calls

2) Customize IVR, and supports nesting IVRs

3) Enterprise attendant can trigger events as follows: IVR, extension, play greeting, group call, queue, hang up, audio conferencing, etc.

Select " Voice Config>>PBX Features>>IVR" to open the page as shown in the following figure.

Figure 6-83 IVR Setting

Add a New IVR

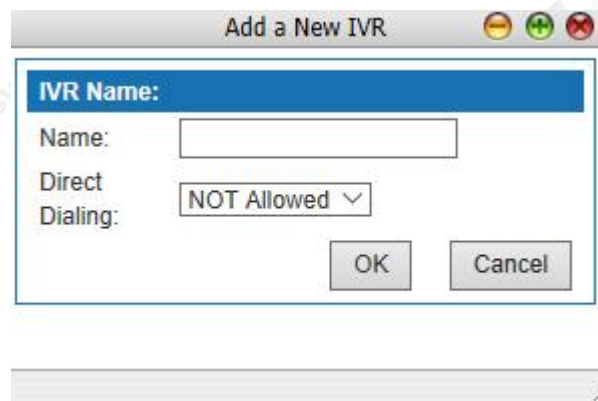1. Click <Add> button to open the page as shown in the following figure.

Figure 6-84 New IVR Setting

2. Enter the name of new IVR, then click <OK> button to open the page as shown in the following figure.

Figure 6-85 New IVR

IVR Setting

1. Click <Add> button to open the page as shown in the following figure.

Figure 6-86 IVR Setting

Interface items are described as follows:

Table 6-34 IVR Setting

Items	Description
Number	It is the number dialed by the external user after connecting to the system switchboard. It can be divided into "start" "invalid" or "delay" .It can be used to trigger a special event of the process. "Start", means start, stands for the IVR event triggered by the users when they put through the external switchboard. "Invalid", means invalid, represents the IVR event triggered by the users when the number they dialed is invalid. "Time out ", means timeout, refers to the IVR event triggered by the users when there is no operation carried out in the specified time after they put it through to the switchboard.
Action	The selection boxes under the number are the action selection box and the selection box of action content, which represents the action triggered in the number and its content. The options of the action include automatic transfer to IVR, extension number, play prompt tone (cannot be interrupted), play prompt tone (interrupted), voice mail, group call, queue, hang up, answer and conference. The action content selection box changes accordingly according to the action. For example, action select "extension.", the optional content in the action content selection box is all existing extensions.
Action list	After selecting the action and the content of the action Click the< add > button and the selected action will be added to the action list box. If there are more than one actions, they will take place according to the order. The order is from the top to down. The order of the action list can be adjusted by clicking the < up > and < down > buttons

Items	Description
	Click the< delete > button to remove unwanted actions from the action list.

Complete the settings, click <OK> button to add a new IVR.

Search Enterprise Attendant

Click <🔍 **Search**> button to open the page as shown in the following figure.

Figure 6-87 Search IVR Setting

Users can search enterprise attendant by name.

6.4.14 SoftConsole

Select " Voice Config>>PBX Features>>SoftConsle" to open the page as shown in the following figure.

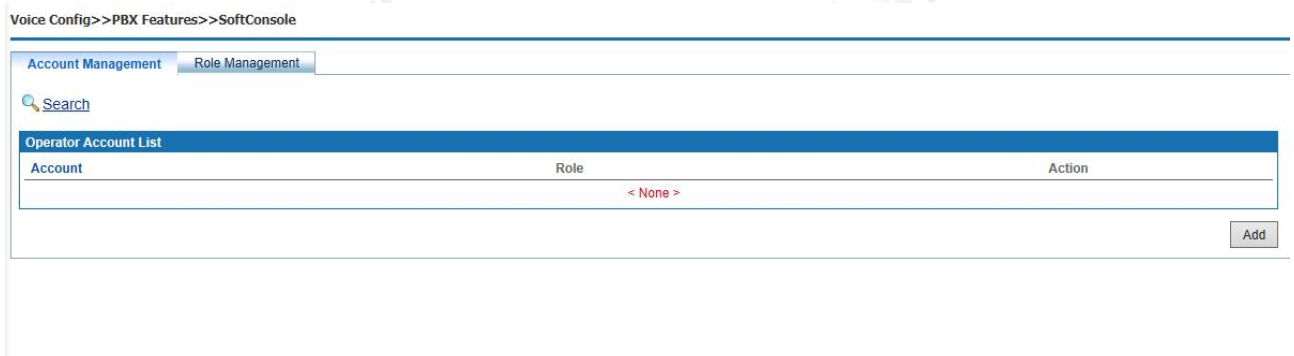It needs to use with the soft console software provided by the vendor.

Figure 6-88 SoftConsole

Add a Role

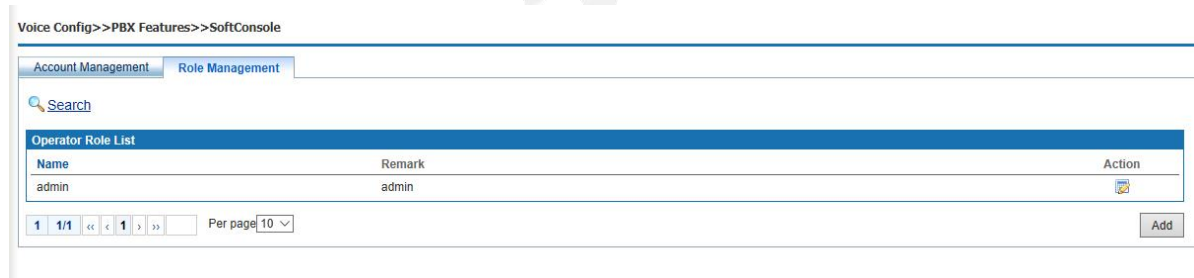Click <Role Management> to pop up the figure below.

Figure 6-89 SoftConsole – Role Management

Click <Add> button to open the page as shown in the following figure.

Figure 6-90 Add New Operator

Interface items are described as follows:

Table 6-35 Operator Role

Items	Description
Name	Name of operator,using digits 0-9, characters a-z, A-Z,the length is 4-30 characters.
Remark	Description of role
Permission Setting	Select operator permission.* is the special privileges,please set carefully.Client permission:Wake up management,hidden extension,Modify the extension dial-up access,Modify the extension name. Server permission:Status push ,Billing

Add a account

Click <Account Management> to pop up the figure below.

Figure 6-91 SoftConsole – Account Management

Click <Add> button to open the page as shown in the following figure.

Figure 6-92 Add Operator Account

Interface items are described as follows:

Figure 6-93 Add Operator Account

Items	Description
Account	Name of operator account
Password	Password of operator account
Role	Select relevant role
Permission Setting	Show operator permission

6.4.15 Queue

This function is widely used in call center. Usually, the extensions of the operators are set in a queue; while only one extension number is used. When the subscriber dials the number, all the extensions in the queue will ring according to the ringing policy, such as simultaneous ringing, circular ringing, etc. If there is an outside number in the queue, the inside number will only ring once or not ring.

Select " Voice Config>>PBX Features>>Queue" to open the page as shown in the following figure.

Figure 6-94 Queue

Add a New Queue

1.　　　Click <Add> button to open the page as shown in the following figure.

Figure 6-95 Add a New Queue

Interface items are described as follows:

Table 6-36 Add New Queue

Items	Description
Name	Name of this queue
Extension Number	Set the extension number of the queue, that is, the number to call the queue. The queue number cannot be the same with other extension Numbers of IPPBX.

Items	Description
Announce Position Frequency (sec)	When the line is busy, prompt time interval, default value is 30 seconds
Ringing Mode	Options: Ring All, Round Robin, Least Recent, Fewest Calls, Random and RR with memory Ring all:All extensions in the queue ring together,default value is "ring all" Round robin:The extension takes turns to ring Least Recent:The most recently least answered extension has the priority of ringing Fewest calls:The extension with the least answering should ring first Random :Randomly select the extension to ring RR with memory:Remember the last extension which rings and the extension which not ring last time has the priority.
Max Waiting Callers	Maximum number of calls in the queue can hold simultaneously
Ringing Time	Time duration of the ring when there is no answer from the agent,default value is 30s.
Retry Wait Time (sec)	When all the lines are busy, the callers can select waiting. Hearing the prompt tone after the waiting time, users can select to continue waiting or hang up.Default value is 5seconds.
Max Waiting Time (sec)	Maximum waiting time for users who select continue waiting.The default value is 60s.
Priority	The priority level compared to other queues.Low,medium,high and very high four degrees.
Timeout	Options: Extension, Play prompt tone (can be interrupted), Play prompt tone (cannot be interrupted), Queue and Hang up.Default value is hang up.
Member Foreign Display Number	Set the number displayed when the queue members calls out.Member number,queue number or Customized number.

Click <OK> button, and click <Add> button to add queue member, the page as shown in the following figure.
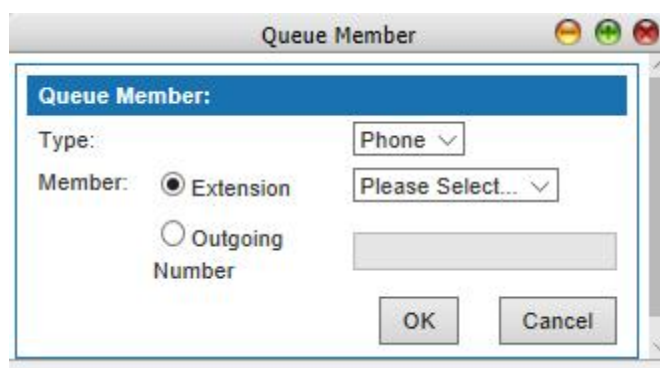

Figure 6-96 Queue Member

Interface items are described as follows:

Figure 6-37 Add Queue Member

Items	Description
Type	Options: Agent or Phone
Member	Select the member according to the type.

Search Queue

Click < 🔍 **Search**> button to open the page as shown in the following figure.

Figure 6-97 Search Queue

Users can search the queue by name and extension number.

Note: the queue number cannot be duplicated with the existing user extension number or conference call number or other business Numbers.

6.4.16 Call Recording

Select "Voice Config>>PBX Features>>Call Recording" to open the page as shown in the following figure.
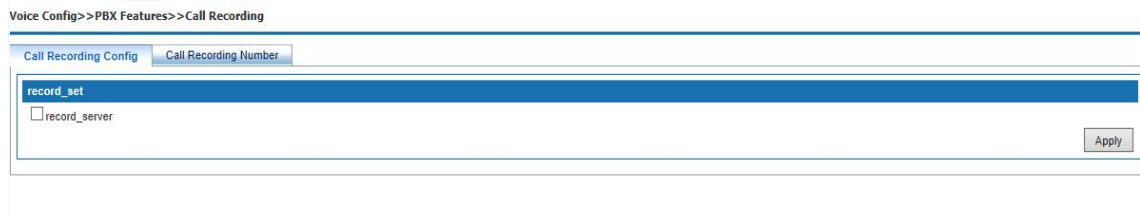

Figure 6-98 Call Recording

Interface items are described as follows:

Figure 6-38 Call Recording

Call Reording	
Enable Record	Click to enable record
Service IP/Port	The recording server IP address and port of record server

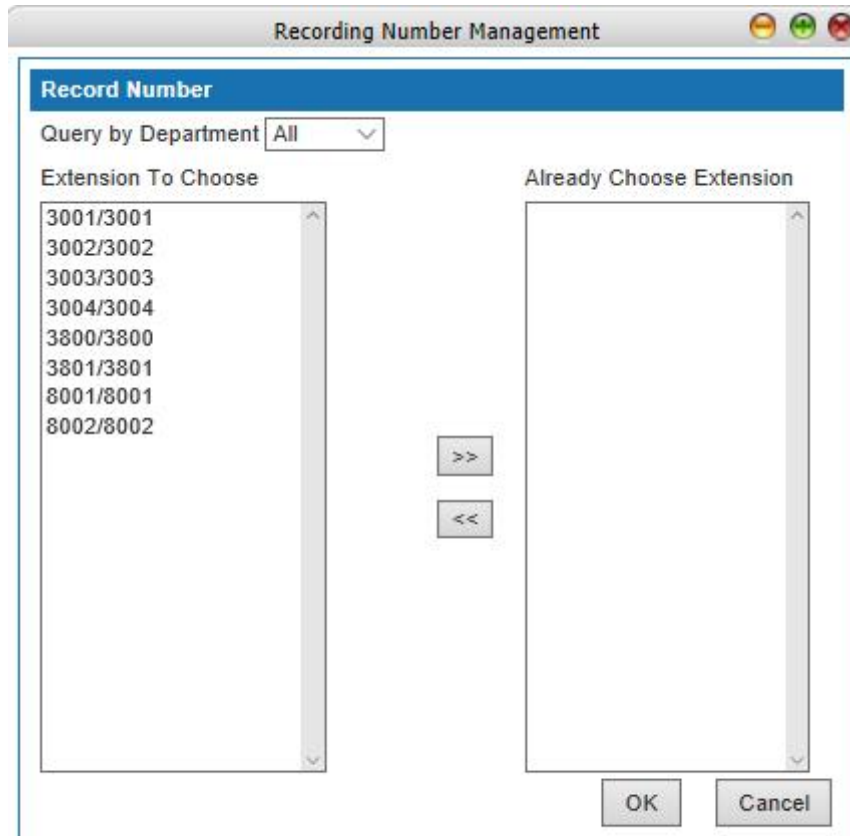Click <Edit> button to open the page as shown in the following figure.

Figure 6-99 Recording Number Management

Interface items are described as follows:

Table 6-39 Recording Number Management

Items	Description
Query by Department	Select extensions according to departments
Extension	Select extensions

Recording server and IP PBX device must configure docking information at the same time. After successful docking, recording function can be used.

Recording server can be a single computer installed with Linux system and recording software, then connected through IP and equipment, through the web browser login to view, play, download recording and so on.

If you don't have a recording server, you can also install the "setup.exe" attached to the CD with installation instructions. After installation, you need to run "Recording Management System", log in with the default password of "admin", fill in the IP address of IP PBX, and click on "Start Receiving". Most of the functions of the recording software will be shut down after 30 days'trial, and it can continue to be used. If you want to continue full-featured use, please contact the vendor for payment.

6.4.17 Billing Setting

Select "Voice Config>>PBX Features>>Billing Setting" to open the page as shown in the following figure.

Figure 6-100 Billing Setting

Interface items are described as follows:

Table 6-40 Billing Setting

Items	Description
Docking Server Setting	
Billing interface setting	Default is V1.0; if users select V2.0, following items should be configured
Billing server IP address	IP address of billing server
Billing server port	Port of billing server
Username/password	Username and pswword of billing server
Card Access Control	Set local, domestic long distance, international long distance

6.5 PBX Setting

PBX Setting includes Global setting, route group, VoIP setting, DSP setting, analog setting, prompt tone, etc

6.5.1 Global Setting

Select "Voice Config>>PBX Settings>>Global Setting" to open the page as shown in the following figure.

Figure 6-101 Global Setting

Interface items are described as follows:

Table 6-41 Global Setting

Items	Description
Global Reloading	Reload all voice configurations

Items	Description
PCM	This device supports A-law and μ-law; default value is A-law. A-law: A-law is the ITU-T (International Telecommunication Bureau of Standards) defined on a pulse code compression / decompression algorithm. A majority of the world countries have adopted laws compression algorithm. μ-law: μ-law is a standard digital multimedia codec's (compression / decompression) algorithms by the International Telephone and Telegraph promulgated Advisory Committee.
Region Code Setting	Select the country of the user, the system default value will follow the national standard, default "China". If you don't want to lose current configuration information, be sure to take a backup.
Voice Prompt Language	According to the user needs to select the type of voice prompt, can choose "Chinese" and "English" two prompt sound.
Ring Time	Type the value of the ring time, the range is 1~200s, and the default value is 30s. It should be the same with the ring time before voicemail. Pbx Features>Voice mail
Enable Service	Select "open" to enable self-switch Select "closed" to disable self-switch
Enable Basic Service	VIP: Select "Open" to enable VIP function. DNS SRV: Select "Open" to enable DNS SRV function. Whether to Send Ponder: Select "Open" to send "#" to upper switch.Default value"no"
Max Forward Times	The limit of the number of times that the forward service accumulates for a single initiated call. The default value is "3".
RTP Timeout Setting	If the audio channel has no RTP or RTCP activity within the default time, the phone will hang up, default value "0" in seconds. It is mainly used when the other party loses power or forgets to hang up the phone.
Outgoing Call - Quick Setting	National Long Distance: 0 International Long Distance: 00
Incoming call display settings	Set the content displayed when there is no caller id service. Default value is "anonymous"
Area Code Setting	Enter area code, for example, Suzhou is "0512"

6.5.2 Route Group

Route group can classify the users and trunks on device, and control the call through binding routes; route group has the following features:

1. a user can only correspond to one route group, and the user and the routing group can only one to one relationship.

2. a route group can bind multiple routes, and a route can also be classified into multiple routing groups. Route group and routing are multi to many relations. Route is grouped into routing groups to take effect.

3.a route can bind multiple trunks, and a trunk can also belong to multiple routes.

Select "Voice Config>>PBX Settings>>Route Group" to open the page as shown in the following figure.
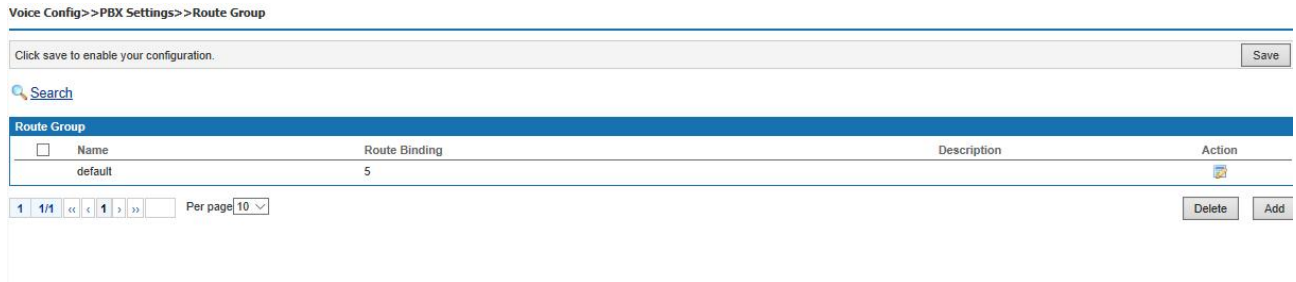
Figure6-102 Route Group

1. Click <Add> button to open the page as shown in the following figure.
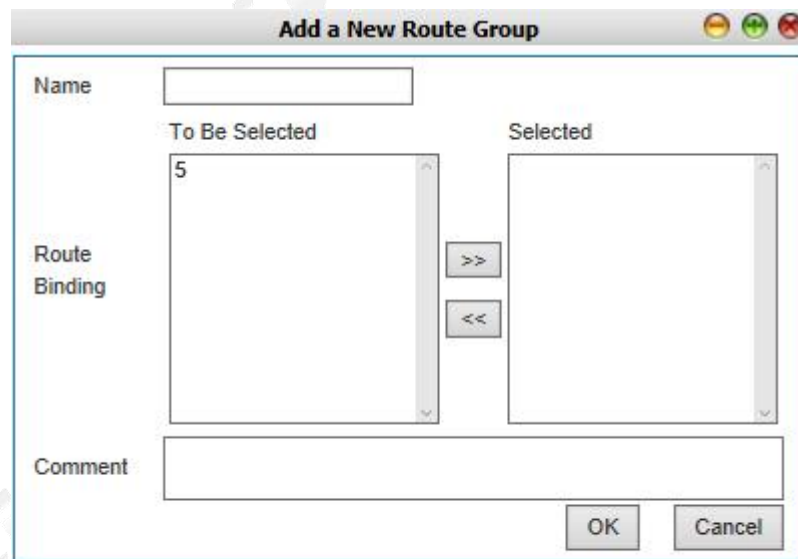
Figure 6-103 Add a New Route Group

Interface items are described as follows:

Table 6-42 Add a New Route Group

Items	Description
Name	Name of route group.
Route Binding	"To Be Select" or "Selected". Select the route from the to be selected box, click" >>" to select the routes, click " <<" to remove the selected routes.
Comment	Description of the route group.

Click<OK> button to finish configuration.

Delete Route Group

Delete a route group from this list. After selecting the entry, click < ⊗ > button to delete it from this list.

Edit Route Group

This option allows user to change a route group configuration. Select an entry from the list, click < > button.

Search Route Group

Click <Search> button in search/export page to open the page as shown in the following figure.

Figure 6-104 Search Route Group

Users can search route group by name.

6.5.3 Prompt Tone

All prompt tones used in system are managed in this page. Select "Voice Config>>PBX Settings>>Prompt Tone" to open the page as shown in the following figure.
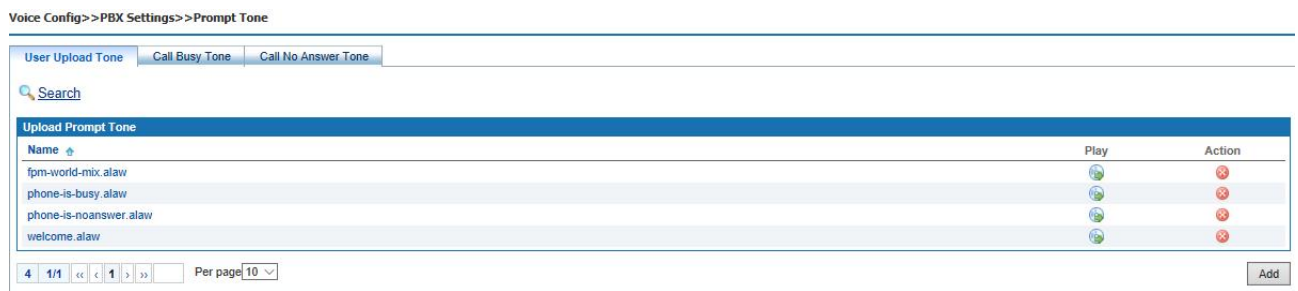
Figure 6-105 Prompt Tone

Add a new voice prompt file

Click <Add> button to open the page as shown in the following figure.
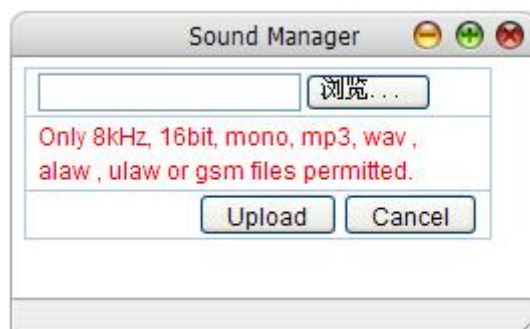
Figure 6- 106 Add a Voice Prompt File

Click the <Browser> button to select local file, and then click the <Upload> button to upload the voice file.

2. Search voice prompt tone

Click < Search> button to open the page as shown in the following figure.

Figure 6- 107 Search Voice Prompt Tone

2. Play the tone

Click the button to play the prompt tone.In the list of "user upload prompt tone", click the button in the operation bar to delete the corresponding prompt tone.

Note: the uploaded audio formats are wav, alaw, ulaw and GSM, and are PCM type 8Khz, 16bit, mono files.

The prompt sound can be converted from the recording file or directly recorded by the software. Method 1: recording file conversion, see 6.5.4 recording file for details. Method two: through the software recording (such as Microsoft's own recording software "recorder").

6.5.4 Record File

You can dial "*77" on the dial panel to record, and dial "#" to finish the recording. Select "Voice Config>>PBX Settings>>Record File" to open the page as shown in the following figure.

Figure 6-108 Record File

sers can manage the generated voice record in this page, click <> button to play it. After playing, there will be a popup window. If users want to transfer it into prompt tone, rename it and click <Transfer> button. Then the transferred file will be forwarded to the prompt tone, and the original record will be deleted.

6.5.5 VoIP Security

Select " Voice Config>>PBX Settings>>VOIP Security" to open the page as shown in the following figure.

Figure 6-109 VoIP Security

Interface items are described as follows:

Table 6-43 VoIP Security

Items	Description
Verifying State Switch	If enabled, system will lock SIP account if SIP registry not accord with security policy. Default enabled
Verification Cycle	Default 3 minutes
Maximum number of registered failures during the period	Default 3
SIP account lock time	Default 3 minutes
SIP registered IP address verification configuration	
Verifying State Switch	If enabled, system will lock SIP account if SIP registry not accord with security policy. Default enabled
Verification Cycle	Default 3 minutes
Maximum number of registered failures during the period	Default 3
IP Address Lock Time	Default 3 minutes
IP address is added to blacklist conditions	If the IP address is locked over the set value within the set time, the system adds the IP address to the blacklist. The default is that the same IP address is locked in more than 3 times in "30 minutes", and the system adds the IP address to the blacklist.

Figure 6-110 VoIP Security

Total Call Duration Limitation	Select the "call time limit" radio box to enable the long - day long - distance traffic function to be limited. Administrators need to set the daily warning time and outage value for long distance traffic. The outage value needs to be greater than the warning value. The unit is: minute / day, the range is 0~9999 minutes / day, of which 0 indicates no time limit. Early warning value: when the daily toll traffic total length reached early warning value when the user answers after dialing the first voice warning system. Interrupt value: the user will not be able to make long distance calls when the daily long distance traffic is always up to the interrupt value. The default values are as follows: Domestic long distance: the early warning value is 3600 minutes / day, and the interruption value is 3700 minutes / day. International Distance: the early-warning value is 10 minutes / day, and the interruption value is 20 minutes / day. Query remainder long: The user can dial the business code *204 for the long query of the remaining calls.

6.5.6 VoIP Config

Select "Voice Config>>PBX Settings>>VoIP Config" to open the page as shown in the following figure.

Figure 6-111 VoIP Config

Interface items are described as follows:

Table 6-44 VoIP Config

Items	Description
SIP Port	Default value is 60780，TCP port 5060.
RTP Port	10000-20000
IP Address	WAN IP address of device
Enable STUN	Enable STUN service
STUN Main IP	IP address of main STUN server
STUN Main Port	Port of main STUN server
STUN Standby IP	IP address of standby STUN server

Items	Description
STUN Standby Port	Port of standby STUN server

6.5.7Analog Setting

FXS - Foreign eXchange Subscriber interface (the plug on the wall) delivers POTS service from the local phone company's Central Office (CO) and must be connected to subscriber equipment (telephones, modems, and fax machines). In other words an FXS interface points to the subscriber.

6.5.7.1 Basic Setting

Select "Voice Config>>PBX Settings>>Analog Setting" to open the page as shown in following figure.

Figure 6-112 Analog Interface – Basic Setting

Interface items are described as follows:

Table 6- 45 Analog Interface Configuration-Basic Settings

Items	Description
Time Setting for FXS Port Number Sending	
Interval of Sending Number to PSTN	Default value is 3 seconds
Interval of Sending Hook Flash Signal	
Sensing Interval of Hook switch Flash Signal of FXS Port	Range of 300 ~ 2000ms, default value is 800ms.
Interval of Sending FXO Hook switch Signal	Range of 300 ~ 2000ms, default value is500ms.
Analog Setting	
DTMF Length	Time of sending number to remote equipment,determined by the opposite equipment,default time is 100ms.
FXO/FXS Impedance	Multiple options.According to different national standards and user requirements. China's general use "600" Ω, consult your network operator for details.

6.5.7.2 Batch Edit FXO/FXS Ports

The page is shown in the following figure.

Figure 6-113 Batch Edit FXO/FXS Ports

Interface items are described as follows:

Table 6-46 Batch Edit FXO/FXS Ports Parameters Description

Items	Description
Selected/to be selected	Select the FXO/FXS interface to be modified, and select the options to be selected with the mouse. For continuous channels, drag and drop with the mouse, and for multiple channels, hold down the CTRL keyboard and use the mouse to select. After selecting, click ">>" to enter the selected channel. After selecting channels from the selection list, single-click "<<" to enter the to be selected.
Activate	Activate FXO/FXS interface.
TX Gain	Adjustment of the strength of the emission signal with the effective parameter set from 0 dB to 9 db. The default setting is 5 dB.
RX Gain	Used to adjust the strength of the received signal with the effective parameter setting from 0dB to 9dB.The default setting is 5dB.
Protocol	Select from Loop Start, Ground Start and Kool start.Default value is Loop start. Loop start signaling, a method of signaling in telephony.In this way, DC shut-off is used in the telephone circuit, and the beginning of DC current shows the turntable change from hang-up to turn-on, mainly used between the telephone and the switch. Ground Start signaling is a type of analog voice level interface signaling in telephone systems. It requires the user interface to provide a foundation at the annular conductor end of the network interface so that service requests can be made to detect the grounding condition of both ends of the line and to identify the state of the pickup in the voice network. It is mainly used to transmit the pickup signaling between switches.
Fax	The parameter of this item decides to support FAX or not. Default value no,that means not support FAX.If select yes,that means support FAX.
CID Type	Options: BELL, V23, and DTMF.Calling Identity Delivery (CID) the Calling Identity Delivery and display service, this equipment supports BELL, V23, DTMF. FSK is divided into BELL and V23 and other specifications, among which BELL FSK is mainly used in China, the United States, Canada and Singapore. ETSI V23 FSK is mainly used in Europe and other places. DTMF is mainly used in places like Taiwan and India. The default value is "BELL".
Anti-polarity Signal	Select "yes" to enable this function. When the phone is connected, a reverse polarity signal number will be provided and the phone billing server will start working. The default value is "no" and the function is not enabled.
Enable VMWI	Choose "yes", light the voice mail message lamp of the analog phone (the premise analog phone has a voice mail message light), the default value is "yes".
Loop Current	This parameter can be adjusted when the line distance is relatively long or when one FXS is connected to multiple phones at the same time and the voice quality is poor.The default "20mA" provides options for 20mA, 26mA, 30mA, 36mA, and 40mA.

Items	Description
Feed Voltage	When the telephone is automatically ringing, the parameter can be adjusted. The default "48V" provides options for 38V, 43V, 48V, 63V, and 68V
Cross DC Current	The three parameters of intercepting dc current, intercepting ac current and unshaking time of the pickup need to be used together to affect the automatic picking operation of the cut-off bell and the telephone. When the sound of "ziz" is heard and the port automatic picking up, the three parameters need to be adjusted. The current interception current defaults to "6mA". Available options 4mA, 6mA, 8mA, 10mA, 12mA. The intercepting dc current is used to hear the sound of "ziz" when picking up the phone during ringing. This is because the cut-off function is not in effect and this value needs to be lowered.
Cross AC Current	The current interception AC current acquiescence the "60mA". Available options 40mA, 60mA, 80mA, 100mA, 120mA.
Hook Debounce	The default value is "100 ms". The range of value is 50ms-200ms

6.5.7.3 FXS/FXO Information

FXO - Foreign eXchange Office interface (the plug on the phone) receives POTS service, typically from a Central Office of the Public Switched Telephone Network (PSTN). In other words an FXO interface points to the Telco office.

FXS - Foreign eXchange Subscriber interface (the plug on the wall) delivers POTS service from the local phone company's Central Office (CO) and must be connected to subscriber equipment (telephones, modems, and fax machines). In other words an FXS interface points to the subscriber.

The page is shown as in the following figure. The FXO port list is automatically generated according to the hardware configuration.

FXO

Port	Activated	TX Gain	RX Gain	Protocol	Fax	Anti-polarity Signal	CID Type	Action
Frame:1 Port:201	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:202	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:203	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:204	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:205	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:206	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:207	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:208	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:209	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:210	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:211	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:212	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:213	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:214	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:215	Yes	5	5	FXS Loop Start	No	No	BELL	
Frame:1 Port:216	Yes	5	5	FXS Loop Start	No	No	BELL	

FXS

Port	Activated	TX Gain	RX Gain	Protocol	Fax	Anti-polarity Signal	CID Type	Action
Frame:1 Port:1	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:2	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:3	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:4	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:5	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:6	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:7	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:8	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:9	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:10	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:11	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:12	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:13	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:14	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:15	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:16	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:17	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:18	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:19	Yes	5	5	FXO Loop Start	No	No	BELL	
Frame:1 Port:20	Yes	5	5	FXO Loop Start	No	No	BELL	

Figure 6-114 FXS/FXO Information

Click < > button to open the page as shown in the following figure.

Figure 6-115 FXS Setting

6.5.8 DSP Setting

Select "Voice Config>>PBX Settings>>DSP Setting" to open the page as shown in the following figure.

Figure 6-116 DSP Setting – Basic Setting

Interface items are described as follows:

Table 6-117 DSP Setting – Basic Setting

Items	Description
Echo Cancellation	The echo cancellation mode of DSP is selected to eliminate the influence of echo transmission on the opposite end. Three modes are provided: STDEC, std-ec with ECPD and DFEC ETC three modes.The default value is "STDEC" mode.
Echo Cancellation Length (ms)	Set echo cancellation length, default value: 64ms
Mute Compression	Enable mute compression can save network bandwidth.The default value is not open mute compression.
Comfort Noise Generator	CNG is synthetic background noise used in radio and wireless communications to fill the artificial silence in a transmission resulting from voice activity detection or from the audio clarity of modern digital lines
Voice Volume	Telephone voice volume size of receiver. Range is from-14dB to 6db; default value is 0dB.
Input Gain	Telephone voice volume size of caller. Range is from -14dB to 6dB; default value is 0dB.
DTMF Volume	Sound level of the user's keys. Range is from -63dB to 0dB.Default value is -3dB
Minimum Delay of Dynamic Jitter Buffer (ms)	Range is from 0ms to 280ms, default value is 160ms.
Maximum Fax Rate	Options: 2400bps, 4800bps, 7200 bps, 9600 bps, and 12000 bps, 14400 bps. Default value is 14400bps
Fax Redundancy	Set the number of redundant packets, providing four types 0,1,2,3.
Error Correction Type	Set error correction type of T.38.
Max Packet Value	Set maximum packet value of T.38 fax; range is from 200 to 600 bytes, default value is 400 bytes.
Busy Tone Detection	Provide BQD and FFT, default use FFT
Times of Busy Tone Detection	Select the number of times the busy tone is detected from the drop-down box,default value is 3

Figure 6-118 DSP Setting – Basic Setting

Interface items are described as follows:

Table 6-47 DSP Setting – Basic Setting

Items	Description
Dial Tone	Dial tone is a continuous sound. The range 400~460hz is composed of single frequency or multiple frequencies (up to three, the interval between different frequencies is at least 26Hz). The level of the dial tone should be -10dBm + 6dB. The Chinese standard dial-up sounds are composed of a single frequency of 460hz, and the duration is generally 10 seconds. Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "0" Ms, the pronunciation time "0" ms.
Busy Tone	The busy tone is periodic sounds fast-paced, produced by tone and mute alternately, and the signal is equal to the basic tone cycle of the silent period. The duration of signal tone and mute is relatively short, and the complete cycle time composed of a single tone and mute is 300~1100 milliseconds, and the ratio between signal duration and silent time should be between 0.67~1.6. Generally use the single tone frequency range is 400~600hz, Chinese using single frequency 460hz signal China standard; busy for 360 milliseconds, mute for 360 milliseconds complete busy period of 700 Ms. Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "360" Ms, the pronunciation time "360" ms.
Ring Tone	Ring back tone is a slow rhythmic periodic voice, which is generated alternately by tone and mute, and the period of signal tone is shorter than that of mute. The period of signal tone is in 0.67~1.6 sec, and the period of silence is 3~6 seconds, and a complete ringing period is between 3.67~7.6 second. The user first heard the signal cycle, followed by the mute cycle. Back tone usually uses a single frequency, and the frequency range is between 400~600hz. Chinese standard ring back tone and bell sound is 1 second stop 4 seconds, ringback tone using a single frequency 460hz. Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "4000" ms, the pronunciation time "1000" ms.
Congestion Tone	Busy rhythm can also slower than congestion tone rhythm. Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "360" ms, the pronunciation time "360" ms.
Call Waiting Tone	Call waiting tone is a slow rhythm. There are two kinds of voice: one is the duration of signal tone in 300~600 milliseconds, the second is 8~10 100~200, the other is the signal tone lasts for 100~200 milliseconds, and then the mute 8~10 seconds after mute 100~200 milliseconds. The Chinese standard waits, in which the sound of the signal lasts for 0.4 seconds, and the mute is 4 seconds. The signal sounds usually use a single frequency 460hz. The call waiting tone is played in the two directions of the call and the call, and the characteristics of the play are slightly different in different directions. Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "4000" ms, the pronunciation time "400" ms.
Second Dial Tone	Default value: voice low frequency "410" HZ, voice high frequency "0" HZ, mute time "0" ms, the pronunciation time "0" ms.
Record tone	Default value: voice low frequency "960" HZ, voice high frequency "0" HZ, mute time "1000" ms, the pronunciation time "400" ms.
Info	Default value: voice low frequency "460" HZ, voice high frequency "0" HZ, mute time "400" ms, the pronunciation time "400" ms.
Stutter	Default value: voice low frequency "410" HZ, voice high frequency "460" HZ, mute time "0" ms, the pronunciation time "0" ms.

The signal sound is composed of four tuples, including low frequency of speech, high frequency of voice, time of silence and time of pronunciation.

1. in addition to the high frequency value of "0", the low frequency value should be less than the high frequency value. The high frequency value is "0", which means that the signal does not use high frequency. The unit of high frequency and low frequency is Hz.

2. the four tuples can not be all the same between different signals.

3. the unit of the mute time and the pronunciation time is MS, such as the silence time and the pronunciation time set to "0", indicating the continuous signal sound.

6.5.9 SMTP Setting

Select "Voice Config>>PBX Settings>>SMTP Setting" to open the page as shown in the following figure.

Figure 6-119 SMTP Setting

Interface items are described as follows:

Table 6-47 SMTP Setting

Items	Description
SMTP settings: when using voicemail and sending mail, users need to configure SMTP information	
SMTP Server Address	Enter server address or domain name.The address format is generally smtp.XXXX.com. Generally, SMTP server address is added smtp before email address. For example, the SMTP address of email@126.com is smtp.126.com. For example:163 email address smtp.163.com,yahoo email address smtp.mail.yahoo
SMTP Server Name	SMTP name, for example abcd@163.com
SMTP Server Password	Password of SMTP server

6.5.10 License

Select "Voice Config>>PBX Settings>>License" to open the page as shown in the following figure.

Voice Config>>PBX Settings>>License

Import license file

Import license file: [_____] [浏览...]

[Import]

System License Information

Hardware Serial Number	600101311104610354
SIP Extension Number	5
SIP Trunk Number	1

Figure 6-120 License Update

Click <Browse> button to open "Choose File" dialog box, select the License file; click <Import> button to import license file.

📖Note:

Please contact supplier to get License file.

6.6 Start Report

Start report includes call log,service voice status,data capture etc.

6.6.1 Call Log

Select "Voice Config>>Stat Report>>Call Log" to open the page as shown in the following figure.

Figure 6-121 Call Log

interface items are described as follows:

Table 6-48 Call Log

Items	Description
Caller Number	Display caller number
Called Number	Display called number
Trunk	Display trunk type and name
Call Length	Call from start to end
Call Type	Display call type
Result	Not answered means ringing but not answered; answered means call successful; call busy means called number is busy and not answered
Report	Export log information to excel file
Search	Search calls by time, phone number, trunk, call type, call duration, service type and department.

6.6.2 Service Voice Status

Select "Voice Config>>Stat Report>>Call Log" to open the page as shown in the following figure.

Voice Config>>Stat Report>>Service Voice Status

Service Voice Status

core show channels
dahdi show channels
sip show channels
core show hints
sip show registry
sip show peers
sip show users
sip show inuse
queue show
core show sysinfo
core show uptime

Confirm
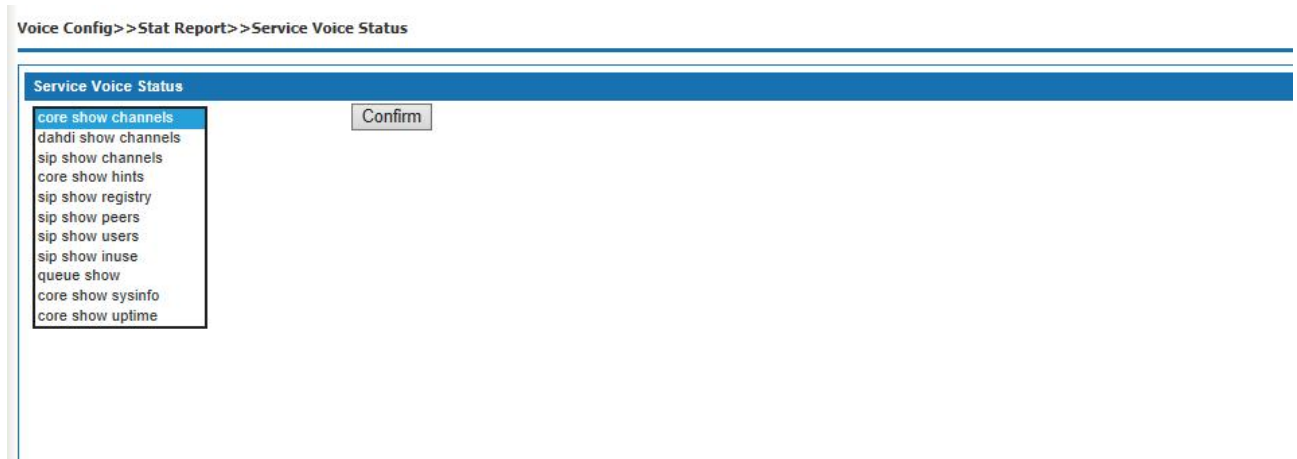
Figure 6-122 Service Voice Status

6.6.3 Data Capture

Select <Voiceset>Start report>Data capture,it shows the capture interface as Figure 6-123,to fill in the content click start capture to start capture, then the device starts to work.Click stop and download it pops up the page as Figure 6-124 and to save the file.This document is for the analysis of engineers. Do not open directly for non-engineers.

| Summary | Network | VoiceSet | Behavior Policy | Object | Security | System |

Voice Config>>Stat Report>>Data Capture

Data Capture

Device: WAN ▾

IP Address (Optional):

Port (Optional):

Start Capture   Stop and download
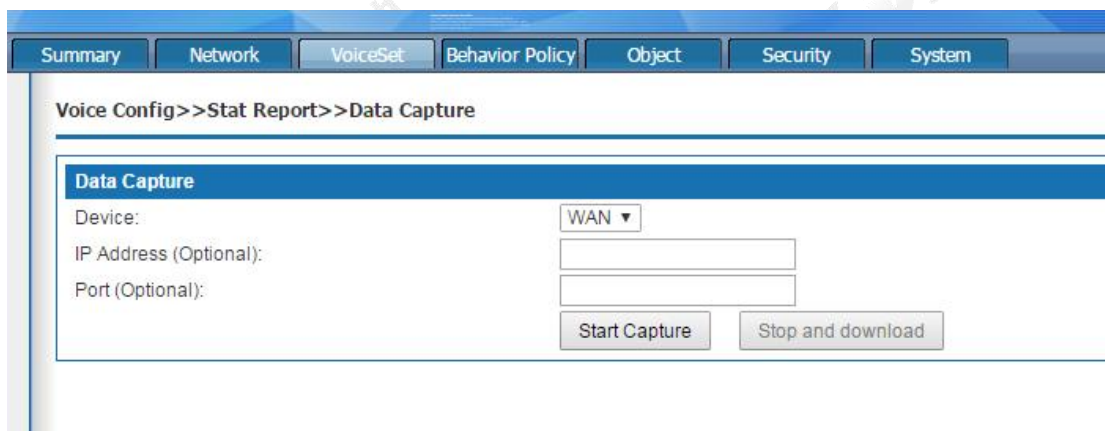
Figure 6-123 Data capture

文件名   tcpdump_br-lan1_10870498a856df7f21297a5489dec5dc.cap

下载到   D:\桌面   剩余370GB ▾   浏览...

打开   下载 ▾   取消
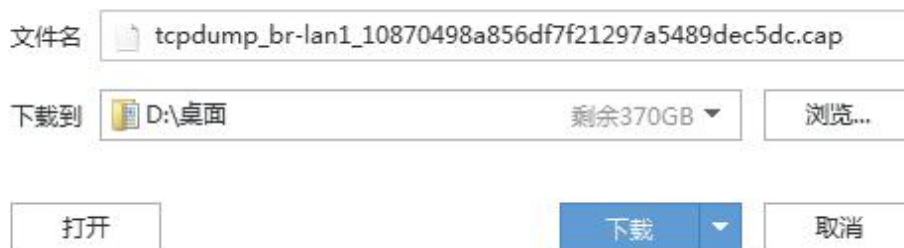
Figure 6-124 Data packet saving

The data capture interface items are described below:

Table 6-49 Data capture

Terms	Description
Network interface	Select the network WAN or LAN port that you want to capture。
IP address(optional)	Fill in the ip address(optional)
Port(optional)	Fill in the port(optional)
Start capture	Click and start capture
Stop and download	Click and to stop capture

7.Behavior Policy

Internet behavior management is used to restrict access to the Internet by users accessing the Internet through this product. Behavior management strategy and flow management.

Before configuration, please click "Behavior policy" at the top of the page to enter the Internet behavior management page.

7.1 Device QOS

When the device is at the exit of enterprise network as a router, hardware QoS needs to be set to guarantee VoIP call quality. The uplinking Ethernet of the WAN port of the equipment is connected to the Internet of the operator. The equipment needs to adopt routing mode, and the LAN port can be connected to enterprise side network switches, computers, IP phones, etc.

7.1.1 Hardware QOS state

QoS state can display the flow histogram of the current four queue priorities in real time.

Behavior Policy >> DeviceQOS >> dvcbasic

低　　　　　　　中　　　　　　　高　　　　　　　最高
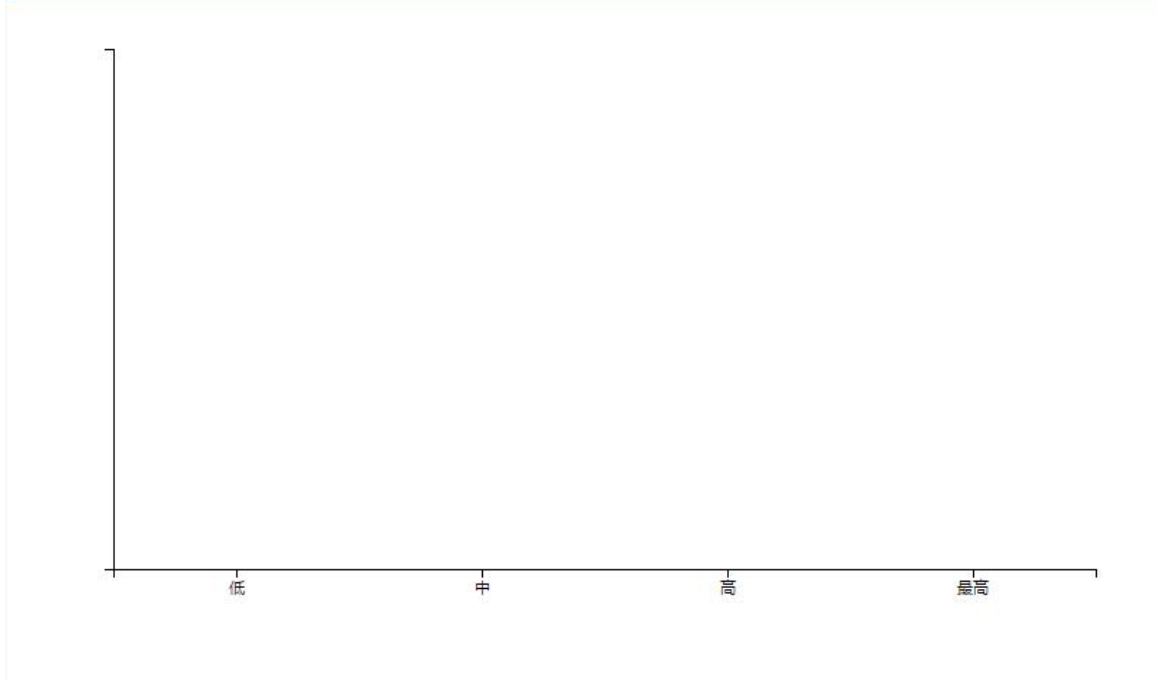
7.1.2 Basic setting

WAN port upstream and downstream speed is not enabled by default, which requires users to set according to the actual rate. Using hardware QoS, the rate limit of WAN port must be set to the actual bandwidth allocated by operator or uplink network device.

Upstream speed:set the max upstream speed of the Wan port,unit:Mbps

7.1.3 Advanced setting

The default traffic priority template used by the system is: low priority occupies 7% of WAN speed limit bandwidth, medium priority occupies 13% of WAN speed limit bandwidth, high priority occupies 27% of WAN speed limit bandwidth, and the highest priority occupies 53% of WAN speed limit bandwidth.

Mapping of traffic priority and DSCP: the packet marked by default 56-63dscp has the highest priority and is forwarded first. The system supports speed limit of downlink bandwidth of 2 LAN ports, which can be set by users themselves. Internal VoIP packet priority forwarding: enabled by default, all FXS phone calls generated by the packet system default on high quality DSCP mark of first grade, priority forwarding.

LAN1 gateway high priority forwarding: not enabled by default, after enabled, packets from LAN1 port are marked with high priority DSCP.

LAN2 gateway high priority forwarding: not enabled by default, after enabled, packets from LAN2 port are marked with high priority DSCP.

7.2 Behavior policy

Behavioral management strategies include Internet access limits, connection limits, IP quintuple filtering, and MAC address filtering.

7.2.1 Internet access limit

This is a macro control of the number of Internet access, there are three options: do not enable business, mode 1, mode 2. Mode 1 is simply targeted at the number limit, mode 2 is targeted at specific terminals, including set-top box, camera, computer and phone.

7.2.2 Total devices linked limits

Select behavior policy>behavior policy>link limit,the page pops up as the figure7-1

Figure 7-1 linked limits

Total devices connected limit:Set the total number of connections of the device, the value range is 1-65536, and the default value of the system is 65536. With this feature enabled, the total number of connections on the current device exceeds the set value, and you must wait for a connection to break somewhere before you can establish a new connection.

Click the < add > button, and the add policy page will pop up as shown in figure 7-2.

Figure 7-2 Add connection limit policy

Add connection limit policy description as follows:

Table 7-1 add connection numbers restriction policies

Terms	Description
Limit policy name	define a policy name by entering 1-32 characters. Status: select "enable", the policy is in effect; select

	"disable", the policy is not in effect.
Connection status	Select enable or disable
Issued objects	Physical port: Select physical ports and set the physical ports that are limited by this policy
	VLAN ID:Select "VLAN ID" and set the VLAN network segment limited by this policy. For the network segment corresponding to VLAN ID, please refer to "Lan setting >VLAN setting for LAN interface".
	IP address: select "IP address" and set the IP address restricted by this policy. IP range: select "IP range" and set the IP range restricted by this policy.
Connection mode	Single IP connection limit: limit the number of connections of each user in the distribution object. When the number of connections of a single user exceeds the set value, it must wait until the connection is broken to establish a new connection.
	Total connection limit: limits the number of connections for all users in the distribution object
Connection type	Select "all" to limit all connections and "TCP" to limit TCP connections. Select "UDP" to limit UDP connections, and select "other" to limit other connections.
Save	Click the < save > button to add a policy to the page

After successfully adding the policy, click the < edit > button to modify the policy; Click the < delete > button to delete the policy. Match the strategy according to the order from the top down, and adjust the strategy order by < move > up, < move > down.

7.2.3 5-Turple Filter

When a quintuple filtering strategy is added, the device will filter the data message matching the quintuple strategy, that is, the data message matching the quintuple strategy is discarded.

Select <behavior policy> and <5-turple filter>,it pops up the 5-turple filter page as following:
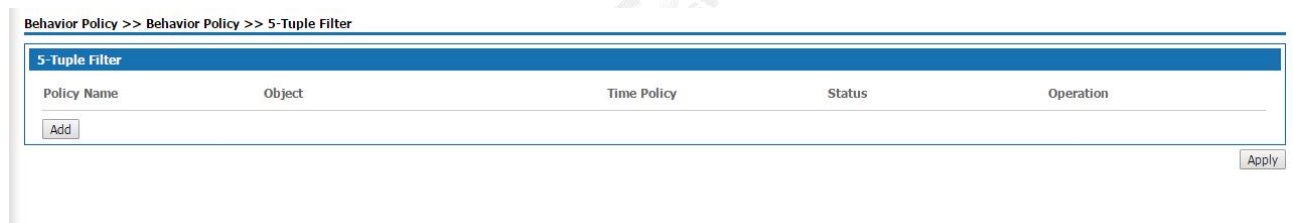
Figure7-3 5-tuple filter page

Click < add > button, and the "add IP five-tuple filter" page will pop up, as shown in figure 7-4.

Figure 7-4 Adding IP 5-turple filter

Add IP quintuple filtering instructions below

Table 7-2 add the IP quintuple filtering strategy

Terms	Description
Policy name	Set the quintuple policy name.
Protocol	Set the protocol needed to be filtered ,selected TCP/UDP、TCP、UDP、ICMP
Source IP	Set the source IP address or IP range needed to be filtered
Destination IP	Set the destination IP address or IP range needed to be filtered
Source port	Set the source ports to be filtered, and you can set a single port or a port range
Destination port	Set the destination port to be filtered, and you can set a single port or a port range
Time policy	Set the valid time of the five-tuple filtering policy from the drop-down box. "Always" means that any time works, see "object management > time group" for setting the time policy.
Status	Select "enable", the policy is effective; Select disable, the policy is invalid

7.2.4 Mac filter

Add a MAC address filtering strategy, and the device will filter the datagram that matches the MAC address, i.e., the matched datagram is discarded. Select "behavior policy >MAC address filtering", and the "MAC address filtering" page pops up, as shown in figure 7-5.
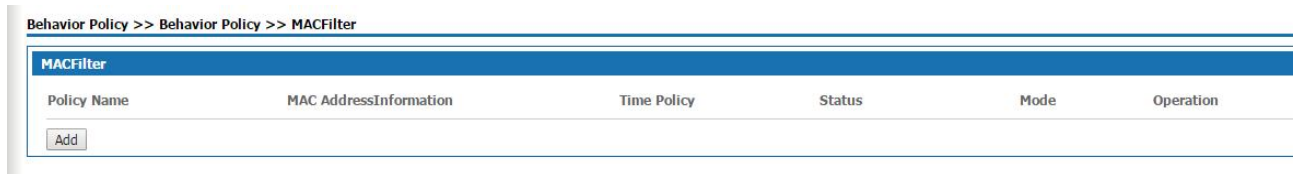
Figure 7-5 MAC address filtering

Click < add > button, and the "add MAC address filtering" page will pop up, as shown in figure 7-6.

Figure 7-6 Add Mac address filter

Add MAC address filtering instructions below:

Table 7-3 Add Mac address filter

Terms	Description
Name	Set Mac address filter name
Source MAC address	Set the source MAC address to be filtered.
Destination MAC address	Set the destination MAC address to filter。
Time policy	Set the effective time of the MAC address filtering policy from the drop-down box. "Always" means that any time works, see "object management > time group" for setting the time policy.
Status	Select enable, the policy is effective, and select disable, the policy is not
Mode	Engineering staff background use, the customer can not use.

8.Object management

Abstract

Object management manage time groups, user management, common ports. Before configuration, click "object management" at the top of the page to enter the object management page.

8.1 Object management

8.1.1 Scheduler

Select<object management> <scheduler> and enters the page as following figure 8-1
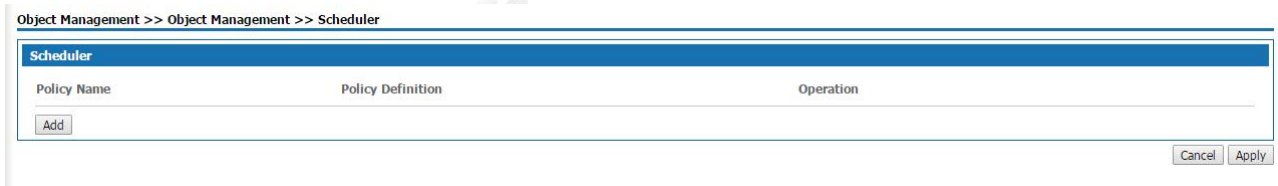
Figure 8-1 scheduler

Click<add>button,it pops out the page as following figure 8-2

FIgure 8-2 Adding scheduler policy

Table 8-1 add time group policies

Terms	Description
Policy name	Set the time group policy name; When adding an application control policy in the application control, or adding a firewall rule in the firewall setting, the defined policy is displayed in the "time policy" drop-down box.
The policy definition	Set the scheduler　policy time, select the corresponding radio box.

8.1.2 Account

Add users in user management, and give users relevant business permissions. When using VPN service, users with corresponding permissions can use the service after authentication. Select "object management >account" and enter the "account" page as shown in figure 8-3.

Figure 8-3 USER management page

Click < add > button, and the "add user management" page will pop up, as shown in figure 8-4.

Figure 8-4 Add user management page

Table 8-2 add user management

Terms	Description
User name	Set the user name
Password	Set the password
Retype	Retype the password
User level	Select "superadmin"and "useradmin" to log into the device as an ordinary user, and the device can be configured; Select business admin. After logging into the device, you can only see the business configured for this account.
Services	The business the user can use, select the radio box。
Web permission	Select "enable" to allow log on to the device through the Web management page; Select "disable" and "this user has no access to the page" will pop up.
Status	Select "enable" and the user can use it normally; Select disable, currently unavailable for this user.

8.1.3 Common ports

Standard protocol port Numbers can be edited through the management of common ports.

Object Management >> Object Management >> CommonPort

CommonPort

Protocol Types	PortNumber	Operation
FTP	20 ~ 21	Edit
SSH	22	Edit
Telnet	23	Edit
SMTP	25	Edit
TFTP	69	Edit
HTTP	80	Edit
POP3	110	Edit
SNMP	161	Edit
SNMPTrap	162	Edit
HTTPS	443	Edit
WebProxy	8080	Edit

Add

Cancel   Apply
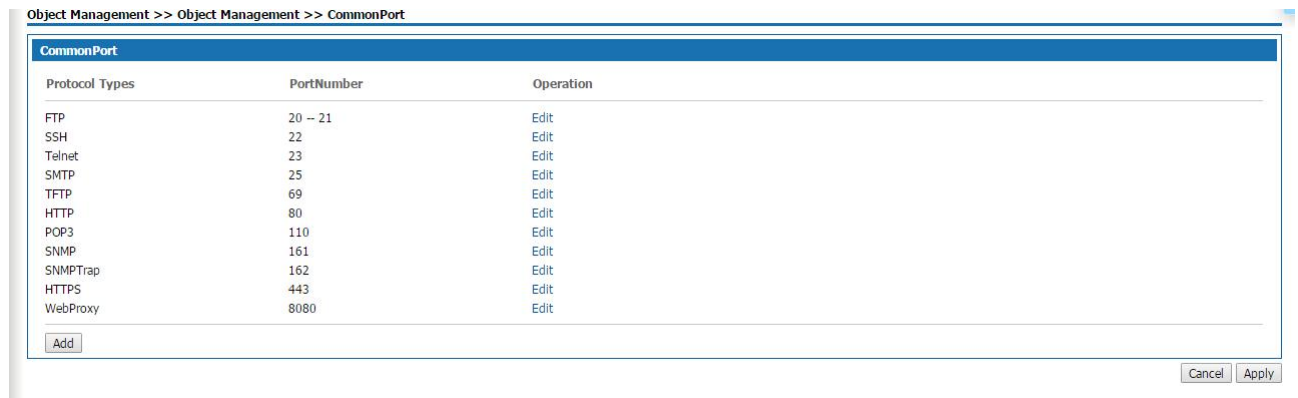
9 Security

Summary

Security includes **Basic Settings,Firewall, ARP Defense,DDoS and Interauth.**

Before the configuration, please first click the function button on the top of the Web Configuration page < Security> to enter into the Security page.

9.1 Basic Settings

Select "Security > Basic Settings " to open the page as shown in Figure 9-1

Figure9- 1 Basic Settings

Basic Settings Description：

Table 9- 1 Basic Settings

Item	Description
Only_wan	Whether to allow the administrator to log in web management page of this product from the WAN port, the default value is off. Port: The port number of the product, ranging from 1 to 66636. The default value is 443.
Only_lan	Whether to allow the administrator to log in web management page of this product from the WLAN port, the default value is off.
Enable Firewall	Whether enable the firewall function or not, enable is the default status
Respond to PING on WAN	Whether to allow the device on Internet to ping the WAN port address of LVswitch IPPBX, the default value is off.

9.2 Firewall

Firewall is applicable to users in various industries such as enterprises, governments and schools. Users can create diversified security policies based on the functions of Firewall. Choose "Security> Firewall" to enter the Firewall page as shown in Figure 9-2.

Figure9- 2 Firewall

This product has predefined Firewall policies for packets originating from the basic interface. Users can modify the policy by clicking the target item.

Click <Add>. The"Firewall Settings" page displayed as shown in Figure 7-3.

Figure9- 3 Firewall Settings

Add Firewall Rule Settings description：

Table 9- 2 Firewall Settings

Item	Description
Policy Name	Define the policy name, enter 1-32 characters.
From--to--	From the data packet source interface to the destination interface. Options: ANY, LAN, WAN, ANY refers to any interface
Target	Set the action of packet matching the rules: Allowed: Allows matched packets to pass. Prohibited: Prohibit the matching of data packets.

Item	Description
Protocol	Set the protocol that needs to be controlled. The value is: TCP UDP All：This rule applies to any protocol.
Source IP	Set the source IP address of data packet that matches this rule. When this parameter is not set by the user, this rule applies to any source IP address.
Destination IP	Set the destination IP address of data packet that matches the rule. When this parameter is not set by the user, this rule applies to any destination IP address.
Time Policy	Set the effective time of the rule, select from the drop-down box. "Always" means that it works at any time. For details on time policy, see "Object Management> Time Group".
Status	Optional, Enable or Disable.

After the rules are successfully added, the rules are sequentially matched from top to bottom. Users can change the order of access control rules by using the< Up >and< Down> buttons.

9.3 ARP Defense

The ARP Defense function mainly used to prevent a large number of invalid ARP request packets in the LAN which causing the ARP entry of the device to fill up, so that the normal computer can not access the device or the external network. This function is used in conjunction with IP / MAC binding. After this function is enabled, the system only processes ARP packets that match the IP / MAC binding rules and directly discards other ARP packets to prevent malicious ARP attacks. Therefore, before enabling ARP Defense, you need to bind a valid IP / MAC address to the IP / MAC binding table first.

9.3.1 IP/MAC Binding

Select "Security> ARP Defense" to enter the "IP / MAC Binding" page as shown in Figure 9-4

Figure9- 4 IP/MAC Binding

Click <Import From System>. The device automatically learns the IP / MAC binding information in the ARP list and displays it on the IP / MAC binding page.

You can also add IP / MAC binding information manually, set IP address and MAC address and then clicking <Add> button to add IP / MAC binding information in IP / MAC binding page.

The intranet LAN IP / MAC binding table can be easily obtained by importing from the system. However, due to ARP aging and other reasons,it can not be guaranteed to import all the computer information. After importing in this method, it is recommended to check whether the computers you want to bind are in the binding table. If not, add them manually.

9.3.2 ARP Defense

Click <ARP Defense > to enter "ARP Defense" page as shown in Figure9- 5.

Figure9- 5 ARP Defense

ARP Defense Configuration description：

Table 9- 4 ARP Defense

Item	Description
Clients who do not match IP / MAC binding rule can not access Internet	Set whether users in the IP / MAC list can access external networks or not. Selected to indicate that only the addresses enabled in the IP / MAC list can access the external network.
Enable ARP Attack Defense	ARP Defense can be enabled when "Prohibit Clients that do Not Meet IP / MAC Bonding Rules to Access External Networks." is enabled When this function is enabled, ARP packets that do not conform to the IP / MAC list will be discarded.
Auto_ipmacbound	Check the radio button to enable automatic binding.

Item	Description
Enable broadcast storm suppression in intranet	Select the radio button to enable the suppression function of broadcast storm and set the suppression threshold. After the broadcast traffic exceeds the threshold, the system discards the broadcast packets.
Anti-ARP-Spoofing	Check the radio button to enable ARP anti-spoofing. By regularly sending gratuitous ARP packets, all users' ARP tables are updated to prevent ARP spoofing. Sending gratuitous ARP packets Interval: The default is 10 seconds.

⚠ NOTE
Enable the " Clients who do not match IP / MAC binding rule can not access Internet ", please make sure the IP / MAC information is bound to the IP / MAC binding table. Without any binding information, it will not be possible to log in to the device from the WAN / LAN port.

9.4 DDoS

DDoS provides anti-DDOS attacks, which can dynamically filter malicious traffic and prevent heavy traffic attacks based on various protocols, thus effectively ensuring the stable operation of the network. Select "Security > DDoS", and enter the "DDoS" page as shown in Figure 9-6.

Figure9- 6 DDoS

The WAN page is used to configure defense to DDoS attacks on devices by external users. The LAN page is used to configure defense to DDoS attacks on devices by intranet users.

Select "DdoS Defense" to enable this function. If there are no special requirements, it is recommended to turn on all prevention functions. Enable TCP Flood attack defense, UDP Flood attack defense and ping Of Death attack defense. Users can set the connection limit according to the server's normal traffic, generally, keep the default value is ok.

9.5 Authentication access

Click<security> and <interauth> ,the page is shown as figure 9-7
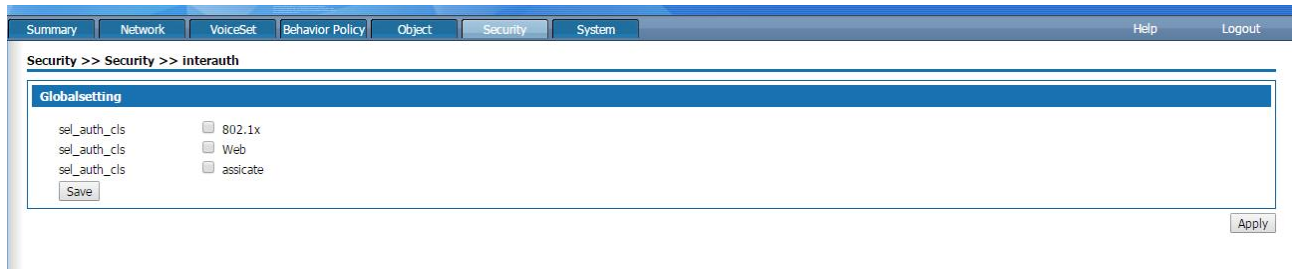
Figure 9-7 Authentication access

After selecting the corresponding authentication type, click save and the corresponding contents will pop up for users to modify, as shown in figure 9-8.
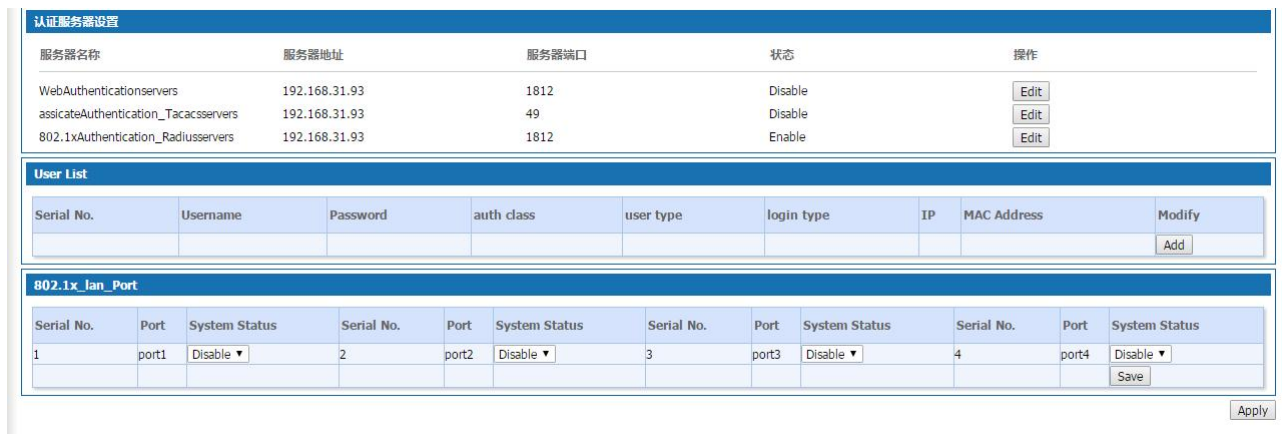
Figure 9-8 authentication server Settings

Authentication access interface description

Interface terms	Description
Global Settings	Server is divided into local and network, if you choose local, there will be no server Settings Items. Login mode is divided into single login and multi-login. If it is single login, only one user is allowed Login from one place. If multi-login, allow the same user to log in from more than one place
Authentication server Settings	Click edit to modify the server's IP address, port, enable state, and Shared key. The default address is 192.168.31.93, and the default key is Testgroup. Modify and click Save.
User list	Change the list to display the information of existing users, click add to add new users.

| 802.1x Ethernet port | Displays port1~4 port information. |

10 System Management

Summary

Before configuring, click "System" at the top of the page to enter the system page.

System is Used to manage the host name, time, password, backup and restore, upgrade, remote management, reboot, factory reset, diagnostic tools, Bypass settings and logs of this product.

10.1 Basic Settings

Select "System >Basic Settings" to enter "Basic Settings"page as shown in Figure10- 1.

System >> System >> Basic Settings

System Configuration

Host Name   ITIBIA

Figure10- 1 Basic Settings

Define the name of this product.

10.2 WebManage

Select "System > Web Manage" to enter "Web Manage "page as shown in Figure10- 2.

System >> System >> WebManage

Web Manage Config

HTTPS Port	443	(1-65535)
HTTP Port	80	(1-65535)

Web Timeout Config

Web Timeout	60	(1-60)Minute

IP_whitelist_management

☐ Enable

IP1	
IP2	
IP3	
IP4	

Figure10- 2 Web Manage Page

The System default value of http port is 80, and the one of https port is 443, users can modify the WEB management port according to their needs, modification is not need under normal circumstances. The configuration to the device is not completed during the management timeout period, user need to log in to the device again to continue configuration.

10.3 Maintain

If you have previously backed up the system setup information, you may restore the current configuration to the one you previously backed up in the event of a misoperation or other circumstances that result in the loss of system setup information for this product to ensure proper operation of the product and reduce loss of information loss. Backing up system setup information is also helpful for troubleshooting.

Select "System > Maintain" to enter "Maintain" page is as shown in Figure 10-3.

Figure10- 3 Backup and Restore Configuration

Back up the configuration information to the computer:

Step 1 Select Backup to PC on the "Maintain" page, enter the name of the configuration file to be saved, and click "Backup",the "Save as" dialog box is displayed.

Step 2 Click <Save> button in the "File Download" dialog box to open the "Save As "dialog box.

Step 3 Select the path for backup the configuration information in the "Save As" dialog box and click the "Save" button.

Result   The configuration information is successfully saved to the computer and the configuration can be restored if needed.

Back up configuration information to USB device:

Step 1 Insert a USB device into the USB port of LVswitch IPPBX. The USB connection status is displayed as USB connected.

Step 2 Select "Backup to USB" on the "Maintain" page, and then click <Backup> to start the backup.

The result is as shown in Figure8-4.

Figure10- 4 Backup to USB completed

 Please do not modify the backed up configuration information file. The configuration file is encrypted and can not be restored to the device if modified.

Restore configuration information via local import is operated as follows:

Step 1 Click "Browse" button on the "Maintain" page,the "Select File" dialog box is displayed.

Step 2 In the "Select File" dialog box, locate the backed up configuration file and click "Open".

Step 3 Click <Restore> button on the Maintain page, to display the "Restore configuration information successfully" page as shown in Figure 8-5.
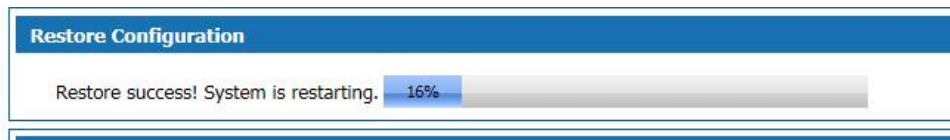
Figure10- 5 Restore configuration information successfully

Results   The system reboot and returned to the imported configuration information.

Restore configuration information via USB import is operated as follows:

Click <Restore> button after selecting the configurtioation file in the USB device to display the "Configuration information restore successful" page as shown in Figure 10-6. After the system reboots, the system will revert to the imported configuration information.

⚠ NOTE — The current configuration information will be lost after restoring the configuration information. If you do not want to lose current configuration information, please back it up.

Restore installation configuration:

Click <Start> to save the installation configuration to the device, and the configuration save time will be displayed.

Click <Start> to restore the saved configuration information. After the configuration is restored, all the configuration information from the latest configuration save time to the curLease Time will be lost. Please pay attention to the backup.

10.4 Upgrade

Users of this product can contact the manufacturer for the latest version to upgrade the system for more functions and more stable performance.

Select "System > System Upgrade",the "System Upgrade" page is displayed as shown in Figure 10-6.

Figure10- 5 System Upgrade

The version upgrade operation is described as follows:

Step 1 Click <Browse> on the "Upgrade" page, the "Select File" dialog box is displayed.

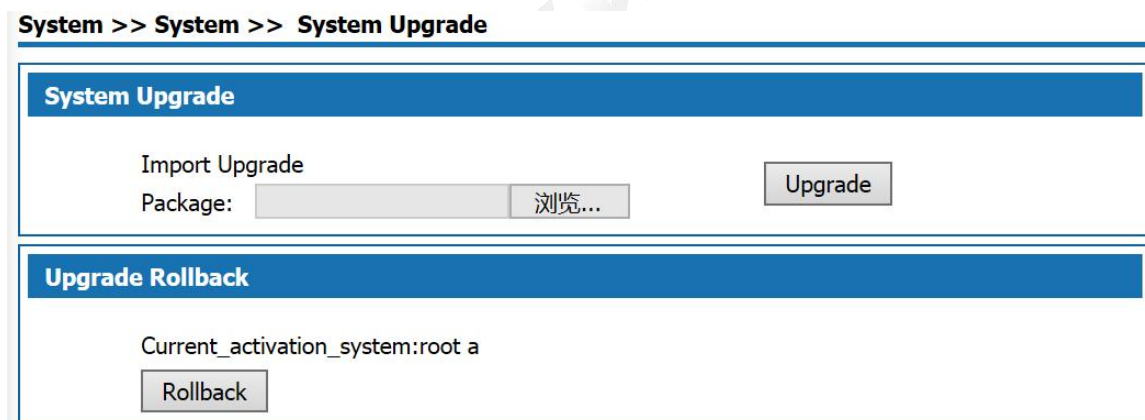Step 2 Locate the latest version file and click the <Open> button in the "Select File" dialog box.

Step 3 Click <Upgrade> on the "Upgrade" page to start the upgrade. The upgrade process may take some time. Wait patiently. After the upgrade is successful, the upgrade success page is displayed as shown in Figure 8-7.
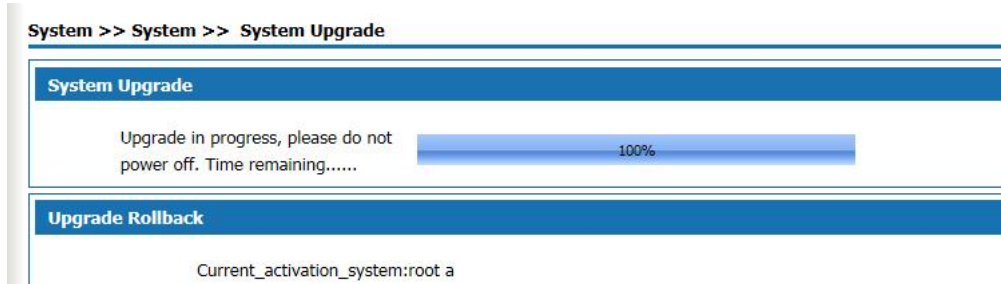
Figure10- 6 System Upgrade Successful

Result   The system restart completed, the system upgrade to the latest version.

During the upgrade process, the system indicator blinks red slowly. After the upgrade is completed, the device restarts and the system indicator light flashes green rapidly. After the login page is displayed, the system indicator light flashes green slowly when it is working properly.

10.5 SNMP

SNMP (Simple Network Management Protocol) is the most popular kind of network management protocol. Through this protocol, access and management by the management equipment to the managed equipment can be achieved.

SNMP protocol is based on server and client management, the back-end network management server serves as an SNMP server, the front-end network devices serve as SNMP clients. The front-end and the back-end share the same MIB management library, and communicate through the SNMP protocol.

Select "System > SNMP" to enter "SNMP" page as shown in Figure 10-8.

Figure10- 7 SNMP Management

SNMP Configuration：

Table 10- 1 SNMP Configuration

Item	Description
SNMP Configuration	
SNMP Status	SNMP Optional, Enabled or Disabled, default status is Enabled
SNMP Version	SNMP Version is optional,options are V1、 V2、 V3 and All，default value is V3.
Read Community	
Configuration Community	Set the password used for read / write access when "SNMPV1 & V2" is selected for the SNMP version.
SNMP Server IP Address	The remote SNMP server's IP address, which is the receiving address of TRAP. The default value is 192.168.3.193.
SNMP Trust Host	IP address trusted by this device,the allows only the management device of the specified address allowed to access this device. If not set, the IP address of management device is not limited.
Private TRAP Setting	
CPU Utilization Threshold	Send TRAP alarms when the device CPU usage exceeds the threshold. Enabled by default, the default value is 99.
Memory Utilization Threshold	Send TRAP alarms when the device memory usage exceeds the threshold. Enabled by default, the default value is 99.
RX Threshhold	Send TRAP alarms when the network interface incoming traffic exceeding the threshold. Enabled by default, the default is 20480.
TX Threshhold	Send TRAP alarms when the network interface outgoing traffic exceeding the threshold.

Item	Description
	Enabled by default, the default is 20480.
Notice Before Restart	The device runs the reboot command, send TRAP alarms before the device restarts. Enabled by default.
WAN Port Address Change Notification	TRAP alarm is sent when WAN port address change, TRAP content includes the new WAN port IP address. Enabled by default.
Device Information Notification	Send TRAP alarm when WAN address change, reboot device, access device or SNMP program is started. Enabled by default.

The configuration on the management device and the one on the managed device need to be the same. Otherwise, the operation can not be performed.

10.6 TR069 Configuration

TR-069 (CPE Wide Area Network Management Protocol) provides a common framework and protocols for managing the configuration of user network devices in next generation networks. The device can be centrally and remotely managed via ACS (Auto Configuration Server) on the network side.

Select "System > TR-069" to enter the "TR-069" page, as shown in Figure 10-9.

Figure10- 8 TR-069 Settings

Figure10- 9 STUN Settings

TR-069 Settings Description：

Table 10- 2 TR-069 Settings

Item	Description
TR069 Settings	The Setting items are described below.
TR-069 Status	TR-069 Status Options "Enable" or "Disable", Enable by default.
Authenticate	Optional, Yes or No, the default is No.
Report Periodically	Select "No", not report periodically, Select "Yes" and set the interval of periodic report in the text box below.
ACS URL	The URL used when connecting to the ACS (Auto-Confi CPE (Customer Premise Equipment) guration Server), using the CPE WAN Management Protocol. This parameter should be set in valid HTTP or HTTP URL form.
ACS UserName	The user name of CPE when the CPE is connected to the ACS using the CPE WAN Management Protocol. The username is valid only when the CPE uses HTTP-based authentication. Value range: 1 ~ 32 characters.
ACS Password	CPE Password used at the time of authentication when connecting to the ACS using the CPE WAN Management Protocol. The password is valid only when the CPE uses HTTP-based authentication. Value range: 1 ~ 32 characters.
CPE Username	Authentication user name used by the ACS to initiate a connection request to the CPE. Value range: 1 ~ 32 characters.CPE username is provided by ACS server.
CPE Password	The authentication password used by the ACS to initiate a connection request to the CPE. Value range: 1 ~ 32 characters.CPE password is provided by ACS server.
STUN Settings	When this product is in a private network, it uses the datagram protocol to establish a port mapping on the product that interacts with the ACS through the STUN (Simple Network Address Translation) mechanism, so that the ACS can configure and manage the product. By default, STUN status is "Disable". After selecting "Enable", the page shown in Figure 10-10 is displayed. The configuration items are described as follows.

Item	Description
STUN server address	Address of the STUN server
STUN Server Port	The port number of the STUN server.
Minimum Retention Time of STUN Connection	The minimum holding time for the client to establish a connection with the STUN server.
STUN Username	User name used to log in to the STUN server.
STUN Password	Password for logging in the STUN server.
Request Upload	Click <Upload> to request to upload the device configuration to ACS server, The sending result of the request will pop-up on the right side.

The CPE refered in this manual is the 1800 device. ACS server address is provided by the telecommunications, make sure the port number and URL address must be correct.

10.7 Reboot

Select "System > Reboot". The Reboot page is displayed as shown in Figure 10-11.

Figure 10- 10 Reboot Page

Click <Confirm Reboot> to reboot the system.

⚠ NOTE

● Do not power off during resboot.
● Network communication will be temporarily interrupted during resboot.

10.8 Restore Factory Default

Run Restore Factory Default, all the setting information of the product will be deleted and return to the factory default configuration status. This function is generally used when the equipment is changed from one network environment to another different network environment. The device is restored to the factory default configuration and then reset to better suit the current networking.

Select "System > Restore" and go to " Restore" page as shown in Figure 10-12.
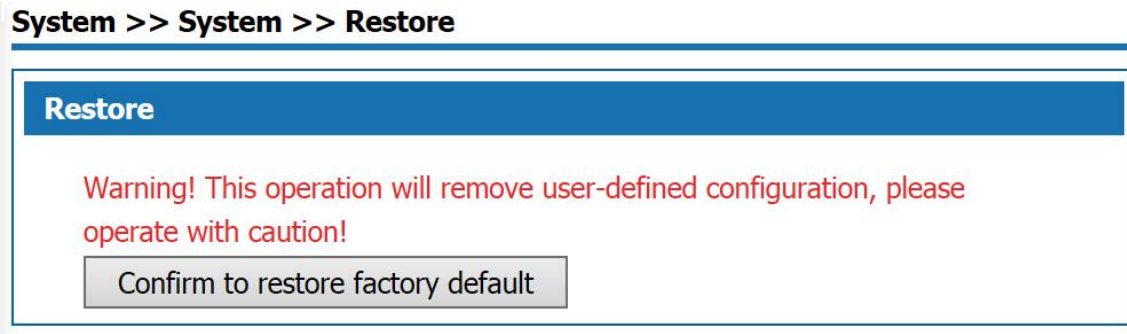
Figure10- 11 Restore Factory Default

⚠️ NOTE	• User will lose configuration when restore to the factory default. Please backup before the restore. • After restoring to the factory default, the system will resboot.

10.9 System Debug

This product provides four kinds of diagnostic tools which include ping communication test, TraceRoute (route tracking), httpGet and DnsQuery. The Ping function is used to test whether the connection between the product and other network devices is normal or not. The TraceRoute function is used to test whether the link between the product and a computer or network device is normal. The HttpGet function is used for testing whether users of this product can access the Internet normally or not; DnsQuery function is used to test whether the DNS server is valid.

Step 1 Select "System > Debug" to enter "Debug" page as shown in Figure 10-13.
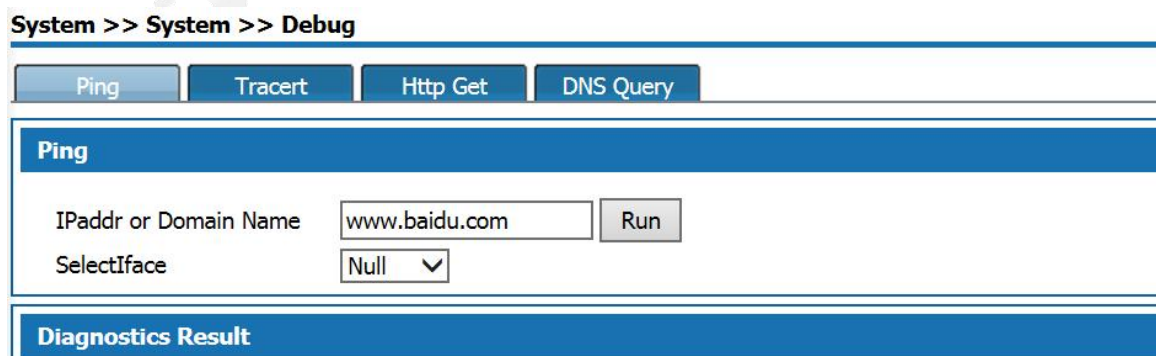
Figure10- 12 Debug

Step 2 Select the diagnostic tool needed and enter the IP addr or Domain Name of the destination device in the   Diagnostic Address text box.

Step 3 Click the "Run"button to start the debug.

Result   The result will be displayed in the text box below.

10.10 Time Settings

Select "System > Time Settings" to enter "Time Setting" page as shown in Figure 10-14.

There are two ways to set the system time. Obtain time through internet and manually set the system time. By default, the product obtains the time through NTP server.

Network Time Protocol (NTP) is used to provide time synchronization between routers, switches, and workstations. The function of time synchronization is to look at the related event records of multiple network devices to help analyze more complicated faults and security incidents.

NTP server to obtain time in two ways:

● When the product is connected to the Internet, it automatically obtains the time from the default NTP server of the device (this method is adopted by default).

● Enter the specified NTP server address, the product obtains the time from the specified NTP server.

Figure10- 13 Time Settings

System Basic Configuration Page description:

Table   10- 3 Time

Item	Description
Enable NTP Time Zone	Check to enable NTP service function. The default value is Enable.
Time zone	Select the time zone of the product, the default is GMT + 08: 00 China standard time.
Time server	Automatic: Update the time from the default NTP server. Manual: If you need to set other NTP server, select "Manual", set NTP server, the product will update time from the specified NTP server. The default is automatic.
NTP Server 1 / NTP Server 2	In manual mode, you can manually set 2 NTP servers
Manually set the date and time	After selecting, manually set the time, turn off the NTP service function. The default is disabled.

Configuration

10.11 Log Manage

Select "System > Log Manage" to enter "Log Manage" page as shown in Figure 10-16.

System >> System >> Log Manage

Check Log   Log Settings

Check Log Information

| Query Term | Time/Date ▼ | Range | _____ ~ _____ | Query |

Time/Date	Module	Level	Summary	Description
2018-01-19 10:36:19	WEB	Warning	Access	Account:admin; IP Address:192.168.23.73; Movement:WEB_Login
2018-01-19 10:32:28	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Login
2018-01-19 10:32:25	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Logout
2018-01-19 08:46:06	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Login
2018-01-19 08:46:02	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Logout
2018-01-19 08:45:58	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Login
2018-01-18 16:03:50	WEB	Warning	Access	Account:admin; IP Address:192.168.27.168; Movement:WEB_Login
2018-01-18 10:20:36	SystemError	Warning	Alarm	104059
2018-01-18 10:19:36	SystemError	Warning	Alarm	104059
2018-01-18 09:48:02	WEB	Warning	Operate	user=admin;set=1
2018-01-18 09:48:02	WEB	Warning	Operate	user=admin;set=4
2018-01-18 09:46:08	DHCP	Warning	Alarm	104005
2018-01-18 09:41:02	DHCP	Warning	Alarm	104005
2018-01-18 09:35:56	DHCP	Warning	Alarm	104005
2018-01-18 09:35:40	WEB	Warning	Access	Account:admin; IP Address:192.168.27.37; Movement:WEB_Login
2018-01-18 09:31:34	system	Warning	Alarm	104001

Total: 182 Item

Clear   Sort Ascending   Refresh   Export

Figure10-16 Log Manage—Check Log

Check Log description as follows:

Table 10-4 Check Log Information

Item	Description
Query items	The system provides five query items: Time / Date, Module, Level, Summary, Description. Select a query item, set the content need to query. If select "Time", set the time range in the Time Range box and click <Query>, the query result will be shown in the following list.
Log information list	The log information displayed is five query items: Time / date: when the log occurred; Module: the log module; Level: The level of the log, including the five levels which are "warning", "err", "crit", "alert", and "emerg". Summary: The type of the log. "Alarm" is the alarm log. "Access" is the access log. "Operate" is the operation log. "URL-Filter" is the URL filtering log. "Flow" is the traffic log. Description: Displays the log information to analyze the operation.
Button Description	Clear: Click <Clear> to clear all the log information. Positive sequence display: Click the "Positive Sequence" button, the log information is displayed in chronological order, and the button is changed to "Reverse Order display". Refresh: Click the " Refresh" button to display the latest log information.

In the log page, users can specify the log information to be displayed in "Log Information View" or set the remote log sending function. Click the [Log Settings] tab to enter page shown in Figure 8-17.

Figure10-17 Log Manage - Log Settings

Log Settings page:

Table 10- 5 Log Settings

Item	Description
Basic Settings: Specify the log information to be displayed.	
RecordType	Specify the log type to be displayed. Select the radio button to display the corresponding log information.
Logging Level	Select to display the log information level, including "warning", "err", "crit", "alert", "emerg" five levels, the level of severity increases in order. Logs greater than or equal to the setting level are displayed.
Maximum number of log reservations	Set the maximum number of log reservations, the value range: 600 ~ 2000. When the number of system log reaches the set value, it will automatically delete the old log information according to the time of sending the log.
Remote Syslog: Set log upload information of remote server.	
Enable IPv6 Log	Check the radio button to enable IPv6 log function.
Server IPv6 address	IPv6 address of server which receives upload logs.
Server IP address	IP address of server which receives upload logs.
Server Port	Server-defined port which receives log upload. Value range: 0 ~ 66636 integer. Default: 514.
Items of sending logs	The number of logs sent to server each time. Value range:

Item	Description
each time	1~600 integer.
Sending interval	Time Interval for uploading logs, in seconds. The value ranges from 1 to 60

Network   information

SIP UNI
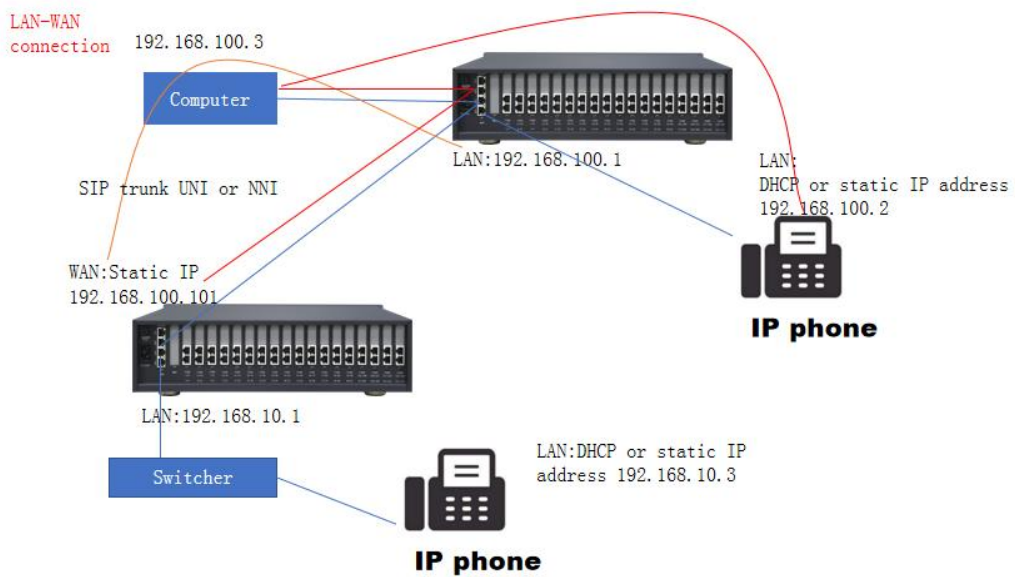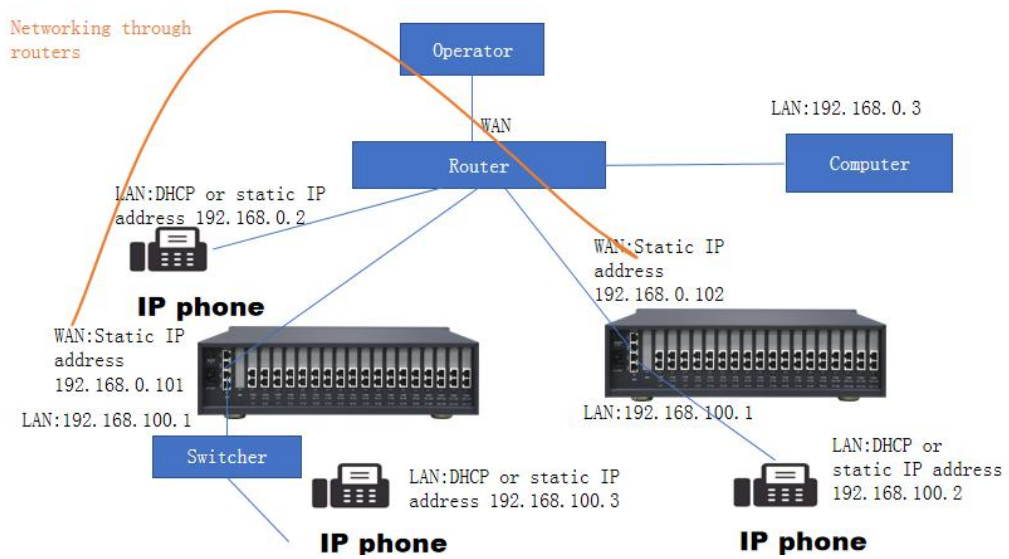
One operator is on the public network
and one on the internal network

Operator

Operator

WAN

Router

WAN static public IP
address:58.211.149.100

LAN:DHCP or static IP
address 192.168.100.2

IP phone

WAN:static IP address:192.168.1.1

WAN-WAN
connection

SIP trunk
NNI or UNI

LAN:192.168.100.1

WAN:static IP address:192.168.1.2

LAN:DHCP or static IP
address 192.168.100.2

LAN:192.168.100.1

IP phone

LAN:DHCP or static IP
address 192.168.100.3

Switcher

IP phone
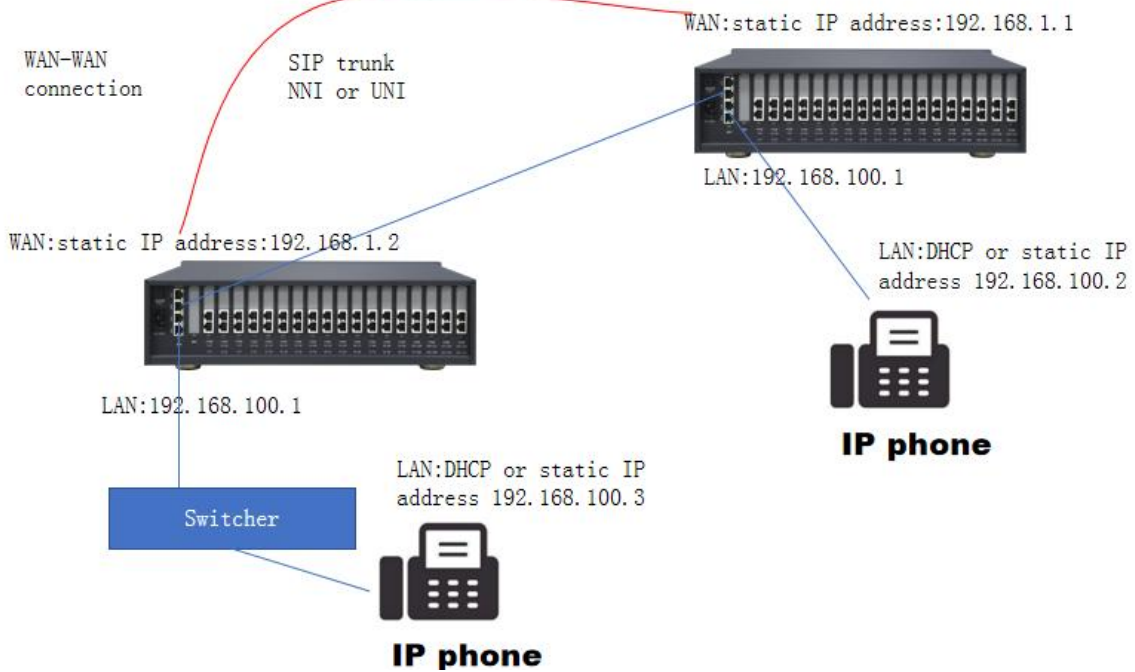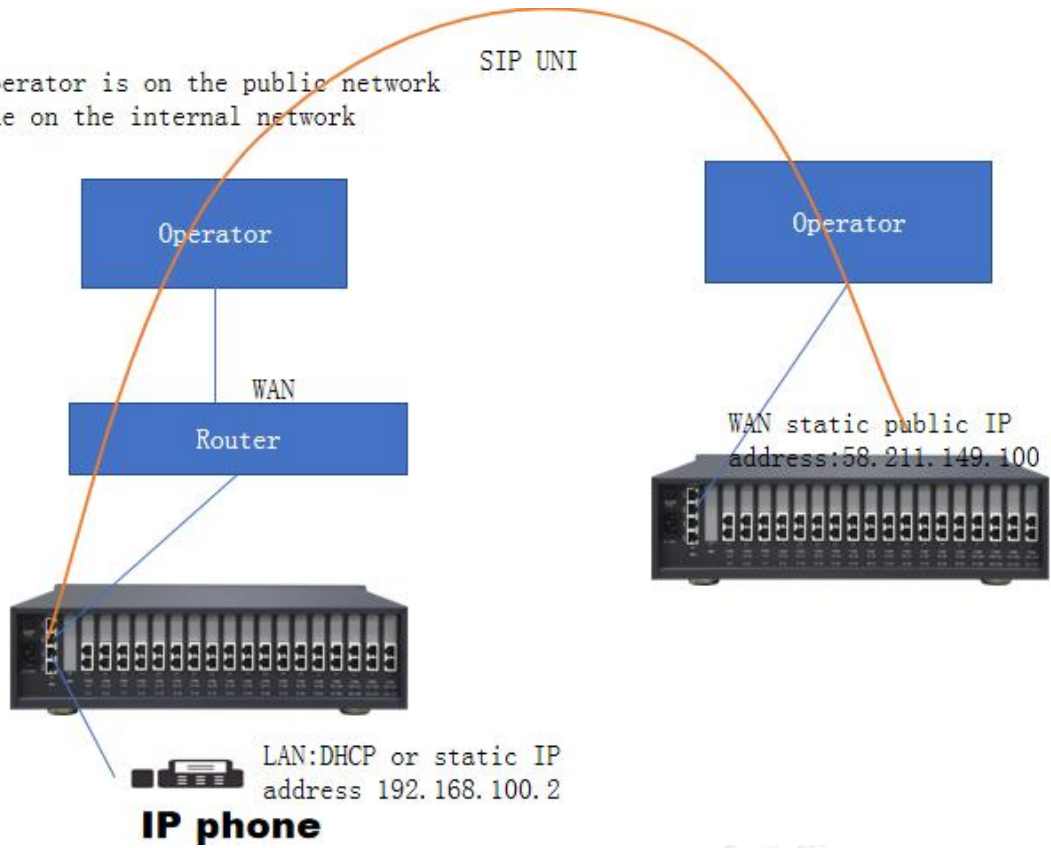
11. Trouble shooting

Appendix 1 Simple failure and troubleshooting

The fault phenomenon	The cause of the problem	The solution
the indicator light is not on	Power off	Check plug and power supply
The extension of silent	Connection failed	Connect the line or troubleshoot the phone
A noise	Poor contact/improper wiring	Tighten/remove the connection from the source
Poor quality	A mixture of phone	Unified telephone standard
No caller id	Outside line without caller id function	Apply to the telecommunication office to set up bell extension
Silent outside call	A bad connection/outside line	Connect an outside line/check that the wires are connected properly
The call was disconnected regularly	Set the time limit	Remove limit
Unable to log in system	Using the wrong account or password	Use the correct account and password
Extension no dial tone	Crystal head loose/circuit fault (open or short)	Change the crystal head, change the line
Extension doesn't ring	Set the do not disturb function/the phone is damaged	Cancel the DND function and replace the line
Outside dial-in extension does not ring	Turn off the outside line/Connect the phone before the outside line	Turn on the outside line /clear and answer calls
Extension can't dial out	Outside line is ISDN line/or outside line voltage is low set limit outside line class	Some components need permission to change outside line
The switch can't connect to the computer	The default network port of the software does not match the actual network port	Set software network port is consistent with using network port
	The computer network port has been damaged	Replace the computer
	The switch network port has been damaged	Replace the switch interface card

Appendix 2 technical parameters

Power voltage	AC200V–240V 50/60Hz
Power consumption	≤50VA
Telephone type	Dual tone multiple frequency /IP phone
Electricity lines	All rope way
Feeding voltage	DC48V 20~40mA
Distortion degree	≤10%
Ringing current	AC70V±10% 50Hz
FXO line sound	Telecom office audio source
Internal dial tone	450Hz square wave continuity
Inside ring tone	450Hz square waves pass in one second and break in four seconds
Internal busy signal error	450Hz square wave 0.3 second pass 0.3 second break
Inside voice confirmation	450Hz square wave one second pass
Outside reminder	450Hz square wave passes 2 seconds and breaks 5 seconds