DINSTAR

UC100-1V1S1O Universal Gateway

User Manual V1.0

Shenzhen Dinstar Co., Ltd.

Address: 9th Floor, Guoxing Building, Changxing Road, Nanshan District, Shenzhen, China

Postal Code: 518052

Telephone: +86 755 61919966

Fax: +86 755 2645 6659

Emails: sales@dinstar.com, support@dinstar.com

Website: www.dinstar.com

Preface

Welcome

Thanks for choosing the **UC100-1V1S1O Universal Gateway**! We hope you will make full use of this rich-feature gateway. Contact us if you need any technical support: 86-755-26456110/112.

About This Manual

This manual provides information about the introduction of the gateway, and about how to install, configure or use the gateway. Please read this document carefully before install the gateway.

Intended Audience

This manual is aimed primarily at the following people:

- Users
- Engineers who install, configure and maintain the gateway.

Revision Record

Document Name	Document Version	Firmware Version
UC100-1V1S1O Universal Gateway User Manual V1.0	V1.0 (2018/05/07)	2.53.4.0

Conventions

Gateway or device mentioned in this document refers to the UC100-1V1S1O gateway. Those words in blue are the contents that users need to pay attention to.

Contents

1 Product Introduction

1.1 Overview

The UC100-1V1S1O gateway is a multi-functional and all-in-one gateway, which integrates voice service (VoLTE, VoIP and PSTN) and data service (LTE 4G/WCDMA 3G). It provides three interfaces (including LTE, FXS and FXO), offering seamless connectivity to VoIP Network, PLMN and PSTN.

Based on SIP, UC100-1V1S1O not only can interact with IPPBX, softswitch and SIP-based network platforms, but also supports types of GSM/WCDMA/LTE frequency ranges, thus meeting the worldwide requirements about the mobile network.

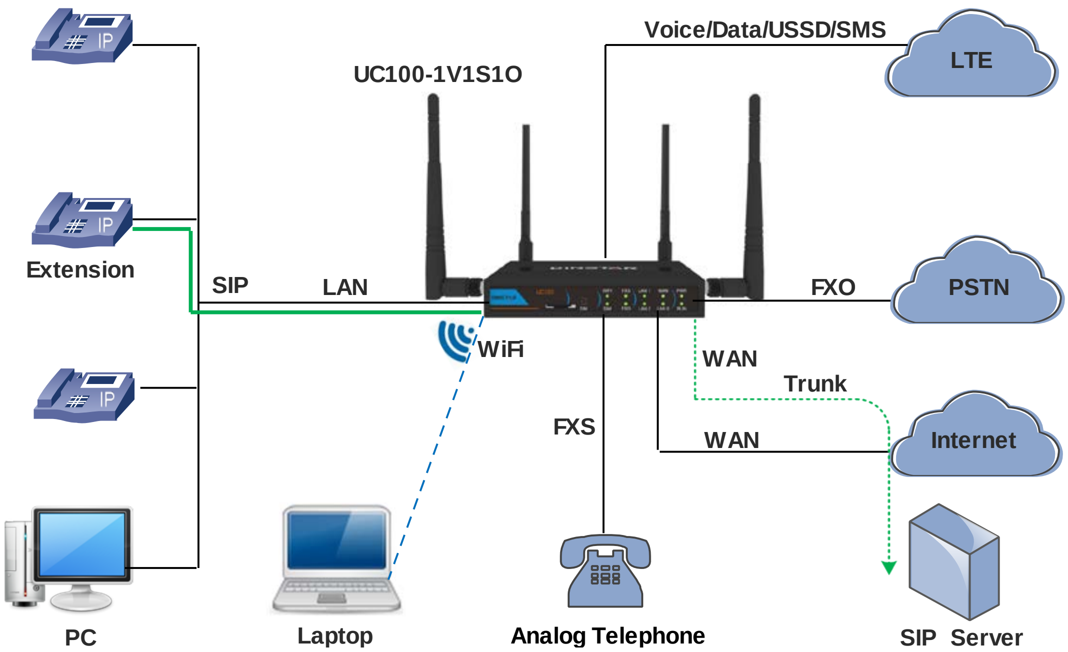
Besides, the gateway has built-in WiFi and high-speed data handling capacity, allowing users to enjoy high-speed internet surfing through WiFi or LAN ports.

UC100-1V1S1O is ideally suitable for personal use. Meanwhile, it is perfect for small and micro enterprises, offering high-speed internet access, good voice service and message service.

1.2 Application Scenario

The application scenario of UC100-1V1S1O universal gateway is shown as follows:

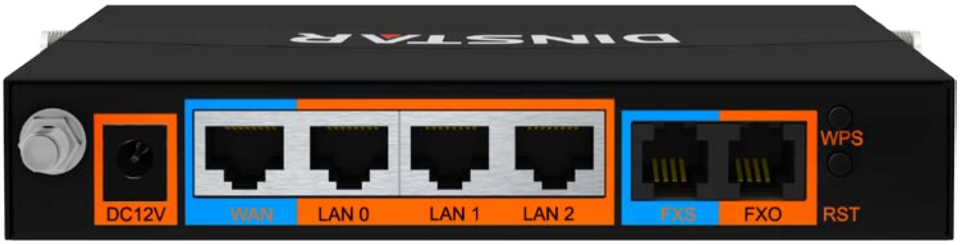
Figure 1 Application Scenario of UC100-1V1S1O



1.3 Product Appearance

Front View:

Back View:



1.4 Description of Indicators

Indicator	Definition	Status	Description
PWR	Power Indicator	Off	There is no power supply or power supply is abnormal.
		On	The UC100 device is powered on.
RUN	Running Indicator	Slow Flashing	The device is initialized successfully and is running normally
		On	The device is being initialized.
		Off	The device is not running normally.
WiFi	WiFi Indicator	Fast Flashing	WiFi is in normal running.
		Off	WiFi is not turned on.
		On	The WiFi module is faulty.
FXS	FXS In-use Indicator	Slow Flashing	The FXS port is in idle status.
		On	The FXS port is in off-hook status.
		Off	The FXS port is faulty
FXO	FXO In-use Indicator	Slow Flashing	The FXO port is initialized successfully and is in idle status.
		On	The FXO port is currently occupied by a call.

		Off	The FXO port is faulty.
WAN/LAN	Network Connection Indicator	Off	Network does not work or network cable is not connected.
		Fast Flashing	Network is successfully connected.
SIM	LTE 4G Indicator	Slow Flashing	The LTE module or the SIM card cannot be detected. (Flash every four seconds)
		Fast Flashing	It is detected that the SIM card has been inserted and registered successfully. (Flash every two seconds)

1.5 Features & Functions

1.5.1 Key Features

- FXS/FXO/LTE interface on a single gateway
- Send/receive calls from LTE and from PSTN/PLMN via FXO
- Flexible dial plan and routing strategies based on time, number and source IP etc.
- IVR Customization
- Support high-speed NAT forwarding and WIFI hotspot
- Serve as VPN client
- Built-in SIP server, support up to 32 SIP extensions and 8 concurrent calls
- User-friendly web interface, multiple management ways

1.5.2 Physical Interfaces

- FXS Port: 1
- FXO Port: 1
- SIM Slot: 1
- Network Port：1 WAN Port & 3 LAN Ports（10/100 Base-T RJ45）
- WiFi：2.4Ghz 802.11n

1.5.3 Voice Capabilities

- VoIP Protocols: SIP over UDP/TCP/TLS, SDP, RTP/SRTP
- Codecs: G.711a/μ law, G.723.1, G.729A/B
- Silence Suppression
- Comfort Noise Generator(CNG)

- Voice Activity Detection(VAD)
- Echo Cancellation: G.168 with up to 128ms
- Dynamic Jitter Buffer
- Adjustable Gain Control
- Automatic Gain Control （AGC）
- Call Progress Tones: Dial Tone, Ring Back Tone, Busy Tone
- FAX: T.38 and Pass-through
- NAT Traversal: STUN/UPnP
- DTMF: RFC2833/Signal/Inband

1.5.4 FXS

- FXS Connector: RJ11
- Caller ID: Bellcore Type 1&2, ETSI, BT, NTT and DTMF
- Answer and Disconnect Signaling: Answer, Disconnect, Busy Tone
- Polarity Reversal
- Hook Flash

1.5.5 FXO

- FXO Connector: RJ11
- Caller ID: FSK and DTMF
- Polarity Reversal
- Answer Delay
- Busy Tone Detection
- No Current Detection

1.5.6 Software Features

- Ring Group
- Routing Groups
- Caller/Called Number Manipulation
- Routing Based on Time Period
- Routing Based on Caller/Called Number Prefix
- Routing Based on Source Trunks
- Dial Rules
- Failover Routing
- FXO Impedance Auto Match
- IVR Customization

- Auto Attendant Function
- CDRs

1.5.7 Supplementary Services

- Call Forwarding （Unconditional/Busy/No Reply）
- Call Waiting and Call Holding
- Call Transfer (Blind & Attended)
- Intra-group Pick-up
- Hotline
- No Disturbing
- Three-way Conversation

1.5.8 Environmental

- Power Supply: 12VDC, 1A
- Power Consumption: 10W
- Operating Temperature: 0 ℃ ~ 45 ℃

  Storage Temperature: -20 ℃~80 ℃
- Humidity: 10%-90% (Non-Condensing)
- Dimensions：143×86×25mm（W/D/H）
- Weight：0.4kg

1.5.9 Maintenance

- Web GUI for Configuration
- Telnet Management
- Configuration Restore & Backup
- Multiple Languages
- Firmware Upgrade: support HTTP/HTTPS/TFTP/FTP
- Auto Provision
- CDR Query and Export
- Syslog Query and Export
- Network Tools: Ping,Traceroute and Nslookup
- Network Capture

2 Quick Installation

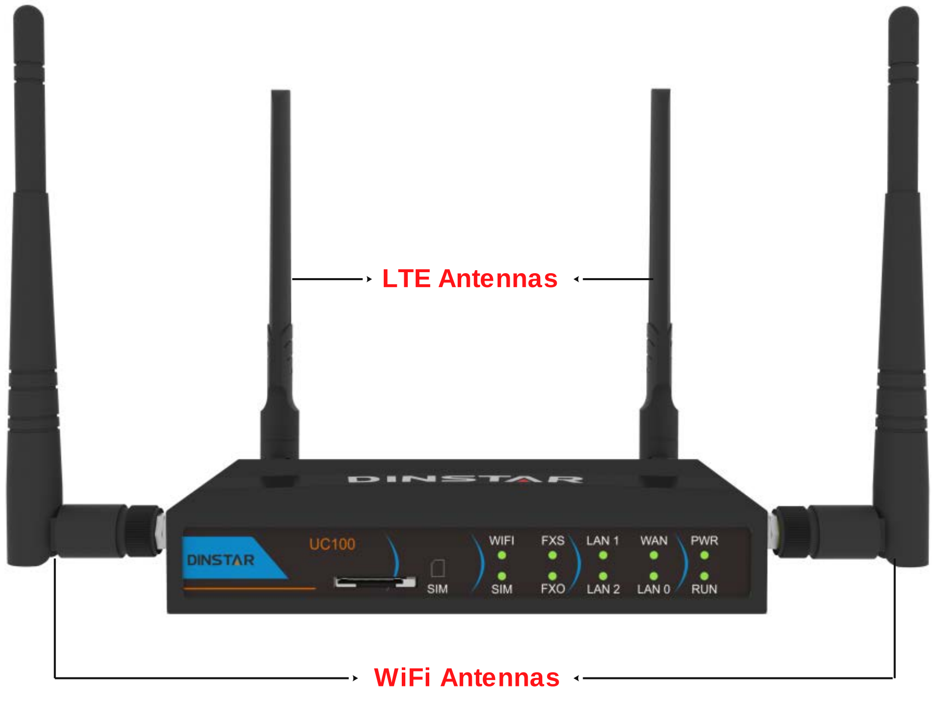
2.1 Installation Attentions

To avoid unexpected accident or device damage, please read the following instructions before installing the UC100-1V1S1O gateway.

- The adapter of the gateway accepts DC input voltage of 12V. Please ensure stable and safe power supply;
- To reduce the interference to telephone calls, please separate power cables from telephone lines.
- To guarantee stable running of the gateway, please make sure that there is enough network bandwidth.
- For better heat dissipation, please place the gateway on a flat surface and do not pile up
- If WiFi is turned on, please ensure the WiFi antennas are well connected with the gateway
- If you want the gateway to communicate with the LTE network, please insert an SIM card.

2.2 Installation Steps

- Connect WiFi antennas to the left and right side of the gateway, and then connect the LTE antenna to the back panel of the gateway.



- Connect the power adapter to the power jack;
- Connect telephone line to the FXS port and connect PSTN line to the FXO port;
- Connect network cable to the LAN port(s) and WAN port (please refer to 2.3 Network Connection);
- Insert a SIM card to the SIM slot.

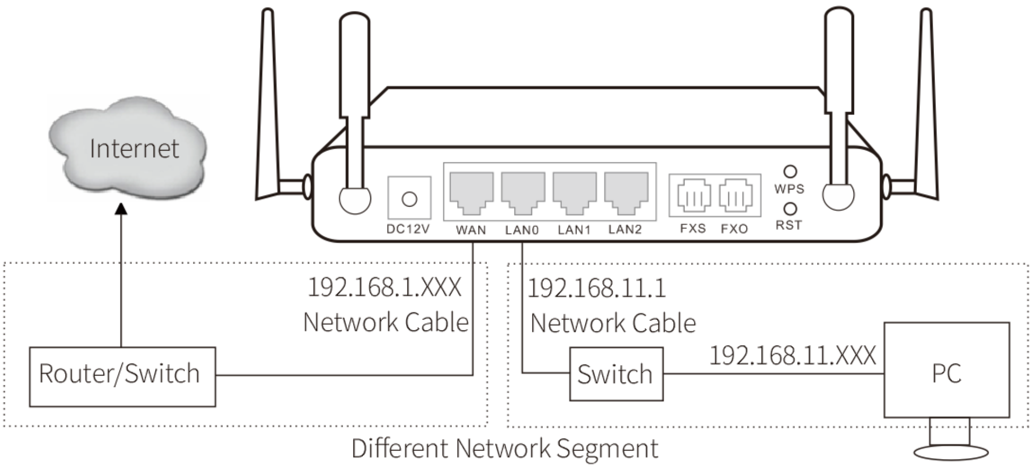
2.3 Network Connection

UC100-1V1S1O works in two network modes: route mode and bridge mode. When it is under the route mode, the IP address of WAN port must be different from the IP address of LAN port. But when it is under the bridge mode, the IP address of WAN port and that of LAN port are the same.

2.3.1 Network Connection Diagram under Route Mode

Under the route mode, the default IP address of WAN port is a DHCP IP address, while the default IP address of the LAN port is a static IP address, namely 192.168.11.1.

Figure 2 Network Connection Diagram under Route Mode

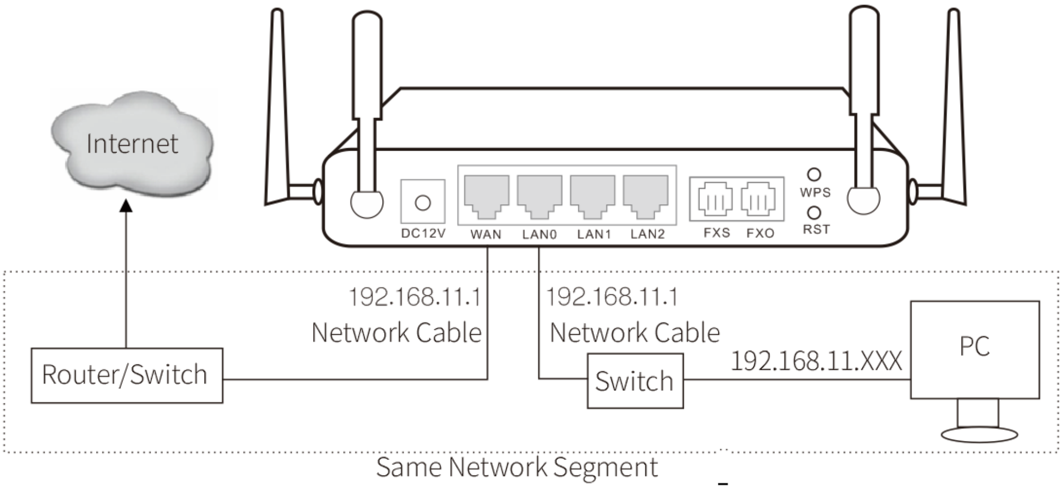


Note: The IP address of LAN port of the gateway and the IP address of PC must be at the same network segment, while that of WAN port is at a different network segment.

2.3.2 Network Connection Diagram under Bridge Mode

Under the Bridge mode, the IP address of WAN port is the same with that of LAN port. Generally, when the gateway works under the bridge mode, the IP address of the gateway has been modified. In the following diagram, it is assumed that the IP address has been modified into 172.16.80.1.

Figure 3 Network Connection Diagram under Bridge Mode



Note: The IP address of PC and that of WAN port of the UC100-1V1S1O gateway are at the same network segment.

2.4 Connect Gateway to Network

The above network diagrams show how to connect the gateway to network through network ports. In fact, the gateway can also be connected to network through WiFi.

2.4.1 Connect Gateway to Network via Network Port

Please connect the UC100-1V1S1O gateway to network according to the network diagrams in Section 2.3 Network Connection. Then connect a telephone to the FXS port. Dial *158# to query the IP address of LAN port. Modify the IP address of PC to make it at the same network segment of LAN port of the gateway.

2.4.2 Connect Gateway to Network via WiFi

Connect power source to the gateway, and then use a laptop to search the SSID of the gateway. The default SSID is domain_the last six characters of the Mac address, for example, if the mac address is F8-A0-3D-59-09-A3, the default SSID is domain_5909a3.

By default, there is no password for WiFi, and the built-in DHCP server is turned on.

2.4.3 Preparations for Login

Modify the IP address of the PC to make it at the same network segment with the UC100-1V1S1O gateway, since the default IP address of LAN port of the gateway is 192.168.11.1.

Check the connectivity between the PC and the UC100-1V1S1O. Click **Start → Run** of PC and enter cmd to execute 'ping 192.168.11.1' to check whether the IP address of LAN port runs normally.

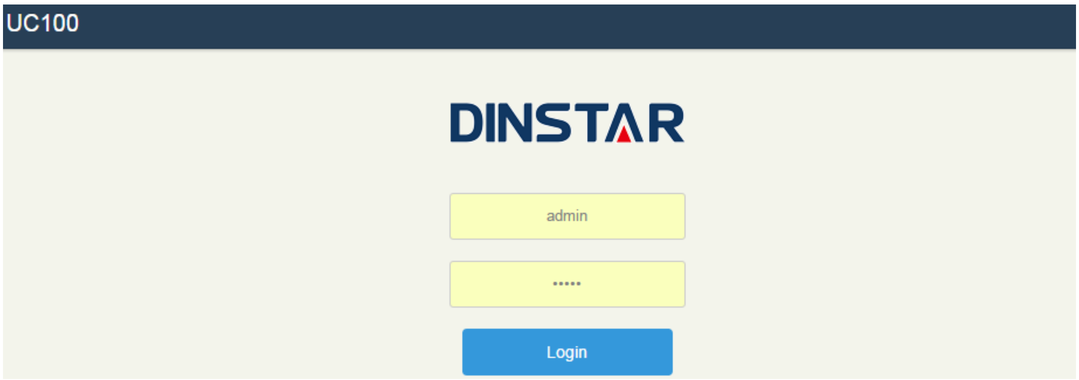
2.4.4 Log In Web Interfacer

Open a web browser and enter the IP address of LAN port (the default IP is 192.168.11.1). Then the login GUI will be displayed.

You also can enter the IP address of WAN port, but it's required to modify the IP address of PC to make it at the same network segment with that of WAN port.

It is suggested that you should modify the username and password for security consideration.

Figure 4 Login GUI of UC100-1V1S1O



Both the default username and password are admin. Click **Login** to enter into the web interface.

Under some circumstances, login of the Web will be limited：

- For three consecutive login failures, you need to slide to validate your user account;
- Failing to log in the Web for ten times consecutively, the IP address of the UC100 device will be put into the blacklist, and you need to reset a new IP address for the device；
- Successful login or device restart will wipe out login failure records.

3 Basic Operation

3.1 Methods to Number Dialing

There are two methods to dial telephone number or extension number:

- Dial the called number and wait for 4 seconds for dialing timeout, or dial the called number directly (the system will judge whether the dialing is completed according to Digitmap and Regular Expression dialplans).
- Dial the called number and press #.

3.2 Call Holding

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call holding feature enabled, the called party is able to switch to the new incoming call while keeping the current call holding on by pressing the flash button or the flash hook.

When the called party presses the flash button or the flash hook once again, he or she will switch back to the first call.

3.3 Call Waiting

If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear a IVR voice 'Please hold on, the subscriber you dialed is busy' and the called party will hear three beeps.

By pressing the flash button or the flash hook, the called party is able to switch between the new incoming call and the current call.

3.4 Call Transfer

3.4.1 Blind Transfer

Blind transfer is a call transfer in which the transferring party connects the call to a third party without notifying the third party.

Example: A gives a call to B and B wants to blindly transfer the call to C. Operation instructions are as follows:

1. A dials the extension number of B;

2. The extension of B rings, and B picks up the phone. Then A and B go into conversation;

3. B presses *1 to trigger blind transfer (at the same time, A can hear the waiting tone). Then B dials the extension number of C (end up with # or wait for 4 seconds);

4. The extension of C rings, B hangs up the phone and C picks up the phone. Then C and A goes into conversation.

Note:

- On the ‘Call Control →Feature Code’ page, feature code service should be ‘On’.
- If B hears continuous busy tones after he dials the extension number of C, it means the call has timed out.

3.4.2 Attended Transfer

Attended transfer is a call transfer in which the transferring party connects the call to a third party after he confirms that the third party agrees to answer the call.

Example: A gives a call to B and B wants to attended transfer the call to C. Operation instructions are as follows:

1. A dials the extension number of B;

2. The extension of B rings, and B picks up the phone. Then A and B go into conversation;

3. B presses *2 to trigger attended transfer (at the same time, A can hear a waiting tone). Then B dials the extension number of C;

4. Then one of the following situations will happen:

a. If the extension of C cannot be reached because the dialing/call has timed out, C rejects the call or C is busy, B will automatically switch to the conversation with A.

b. The extension of C rings (at the same time, B can hear a ringback tone). If B hangs up the phone at this moment, A will continue to hear the waiting tone. Then if A also hangs up the phone, the extension of C will continue to ring. If C picks up the phone at this moment, the call will end directly.

c. The extension of C rings and then C picks up the phone. C and B go into conversation, and A will continue to hear a waiting tone. If it’s B that hangs up the phone at this moment, C and A go into conversation. If it’s C that hangs up the phone, B and A go into conversation.

3.5 Function of Flash-hook

Assume A and B are in a call conversation:

If A presses the flash hook, and then dial the number of C, A and C go into conversation and meanwhile the call between A and B is kept holding.

Then, if A presses the flash hook and dial 1, the conversation will switch back to A and B; if A presses the flash hook and dial 2 , the conversation will switch to A and C; if A presses the flash hook and dial 3, the conversation will switch to A , B and C (three parties conversation).

3.6 Description of Feature Code

UC100-1V1S1O provides convenient telephone functions. Connect a telephone to the FXS port and dial a specific feature code, and you can query conrresponding information.

Code	Corresponding Function
***159**	Dial *159 to inquiry WAN IP
***158**	Dial *158 to inquiry LAN IP
***114**	Dial *114 to inquiry phone number
157	Dial *157*0 to set route mode; dial *157*1 to set bride mode
150	Dial *150*1 to set IP address as static IP address; dial *150*2 to set IP address as DHCP IP address
152	Dial *152* to set IPv4 address, for example: Dial *152*192*168*1*10# to set IPv4 address as 192.168.1.10
156	Dial *156* to set IPv4 gateway, for example: Dial *156*192*168*1*1# to set IPv4 gateway as 192.168.1.1
153	Dial *153* to set IPv4 netmask, for example: Dial *153*255*255*0*0*# to set IPv4 netmask as 255.255.0.0
***111**	Dial *111 to restart the UC100 devic
***51**	Dial *51 to enable the call waiting service
***50**	Dial *50 to disable the call waiting service
***1**	Dial *1 to trigger blind transfer, for example: Dial *18000, and you can blind transfer to the extension number 8000
***2**	Dial *2 to trigger attended transfer, for example: Dial *28000#, and you can attended transfer to the extension number 8000

72	Enable unconditional call forwarding service. Example: Dial *72*8000, and calls will be unconditionally forwarded to extension number 8000
***73**	Disable unconditional call forwarding service
90	Enable the 'call forwarding on busy' service. Example: Dial *90*8000, and calls will be forwarded to extension number 8000 when the called number is busy
***91**	Disable the 'call forwarding on busy' service
92	Enable the 'call forwarding on no reply' service. Example: Dial *92*8000, and calls will be forwarded to extension number 8000 when there is no reply from the called number
***93**	Disable the 'call forwarding on no reply' service
***78**	Enable the 'No Disturbing' service
***79**	Disable the 'No Disturbing' service
******	Pick up the ringing extension which is in the same ringgroup. Example: Dial**8000, and you can take the incoming call of extension number 8000
160	Dial *160*1# to allow HTTP WAN access, Dial *160*0# to deny HTTP WAN access

Note:

A voice prompt indicating successful configuration will be given after each configuration procedure. Please do not hang up until hearing this voice prompt.

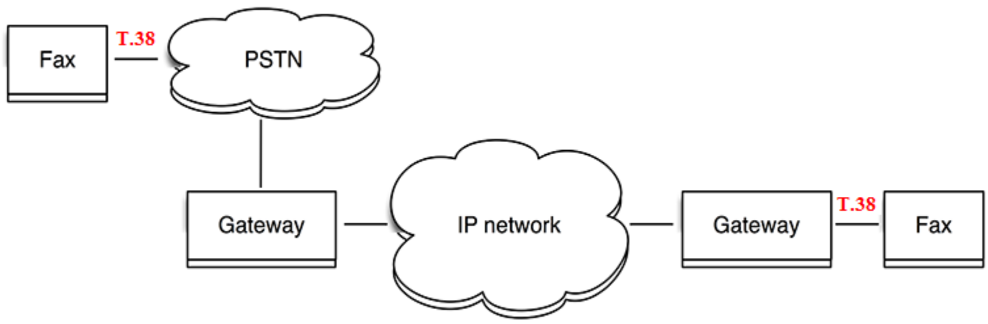
3.7 Send or Receive Fax

3.7.1 Fax Mode Supported

- T.38（IP-based）
- T.30（Pass-Through）

3.7.2 Explanation of T.38 and Pass-through

T.38 is an ITU recommendation for allowing transmission of fax over IP networks in real time. Under the T.38 mode, analog fax signal is converted into digital signal and fax signal tone is restored according to the signal of peer device. Under the T.38 mode, fax traffic is carried in T.38 packages.



Pass-through: Under the pass-through mode, fax signal is not converted and fax traffic is carried in RTP packets. It uses the G.711 A or G711U codec in order to reduce the damage to fax signal.

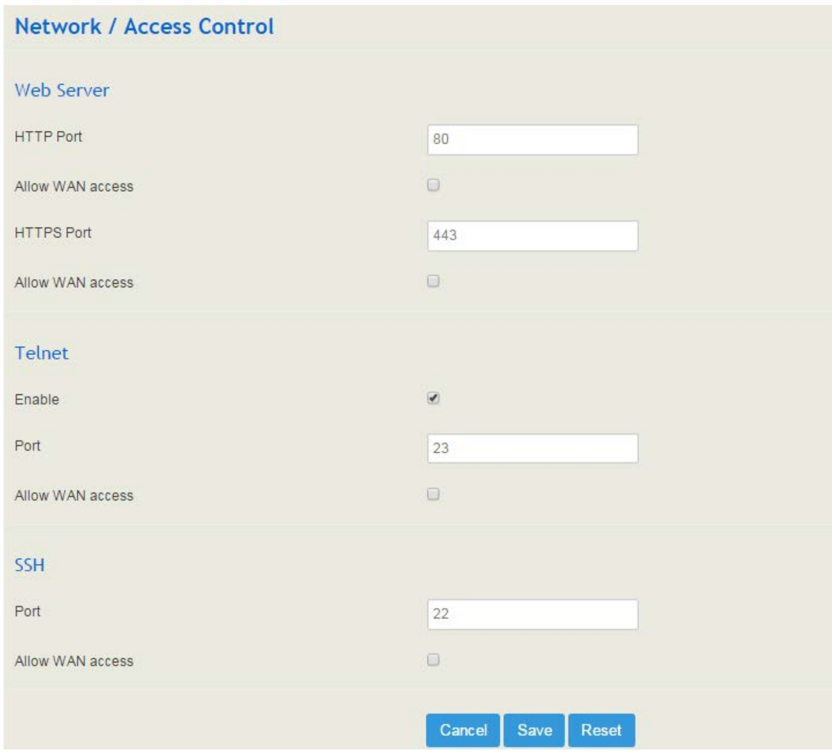
3.8 Function of RST Button

Press the RST button for different time length, and the UC100-1V1S1O device will execute different function:

1. On the condition that the device is running normally, press the RST button for 0 to 3 seconds, the system will not execute any function.

2. On the condition that the device is running normally, press the RST button for 3 seconds to 6 seconds, the IP address, username and password of the device will be restored to factory defaults, and meanwhile the access ports of Http, Https, Telnet and SSH are restored to the default settings.

Figure 5 Default settings of Http, Https, Telnet and SSH



3. On the condition that the device is running normally, press the RST button for more than 6 seconds, and all configurations are restored to the default settings.

4. On the condition that the device is powered off, press the RST button for more than 30 seconds, the device will wipe out all configurations, rebuild a file system and then re-load a firmware version (this method is used in case of version fault).

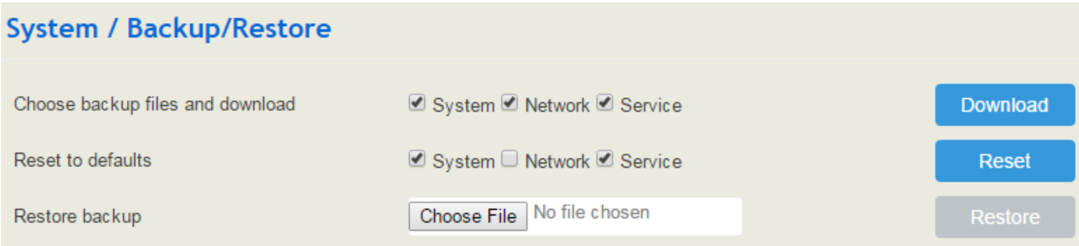
3.9 Query IP Address and Restore Default Setting

After connecting a telephone to the FXS port, you can dial *158 to query the IP address of LAN port and dial *159 to query the IP address of WAN port.

If you want to restore UC100-1V1S1O to default settings, you can press the **RST** button for more than 6 seconds or you can configure it on the Web interface.

On the Web interface, click **System → Backup/Restore/Upgrade** and then select the parts (system, network or service) that need to be restored to default settings. Click **Reset** and then restart the device, and the selected parts will be restored to default settings.

Figure 6 Reset to Defaults



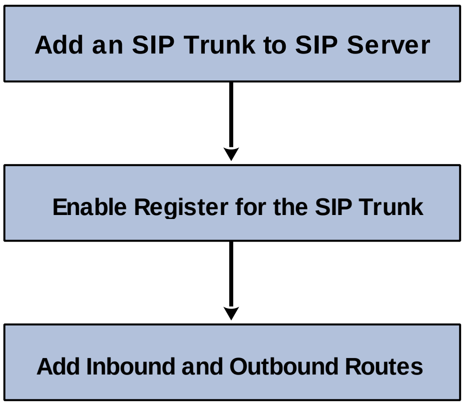
4 Configuration Wizard

4.1 Configuration Wizard

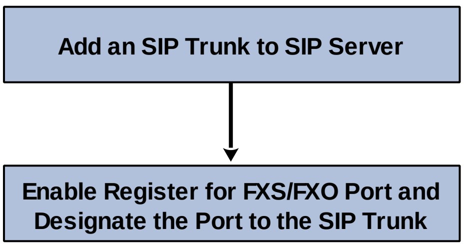
The following are the common ways to configure the UC100-1V1S1O gateway.

4.1.1 UC100 Regarded as Terminal and Registered to SIP Server

1. UC100-1V1S1O Registered to SIP Server



2. FXS/FXO Port Registered to SIP Server

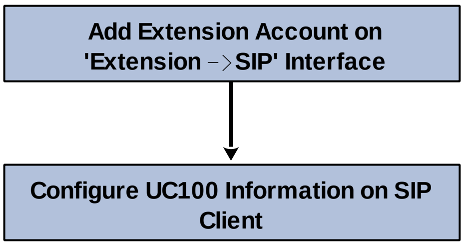


Note: Although 'Register' has been enabled for FXS/FXO port, calls through FXS/FXO port will take inbound and outbound routes as first priority. For outgoing calls, if outbound route cannot be matched, then the registered SIP trunk will be selected. For incoming calls, if inbound route cannot be matched, then the registered FXS/FXO port will be selected.

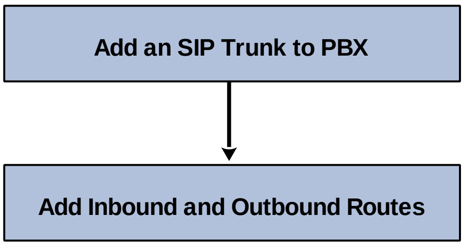
Generally, local extension number is taken as first prioriy for call routing selection, followed by DID, route and then registered port.

4.1.2 Other SIP Clients registered to UC100

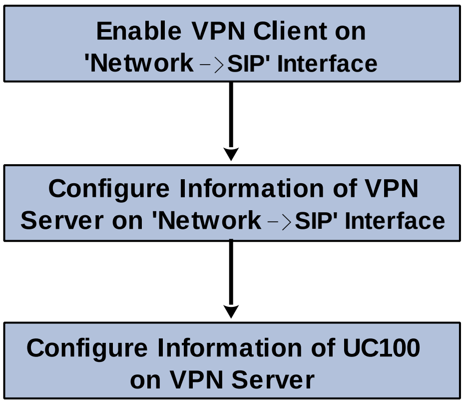
Under this mode, UC100-1V1S1O is regarded as an SIP Server. Create an extension account first on the **Extension →SIP** interface, and configure listening port on the **Profile → SIP** interface. Then, configure the IP address, extension account and listening port of UC100-1V1S1O on SIP client.



4.1.3 UC100 Connected to PBX through Trunking



4.1.4 UC100 Serving as VPN Client



5 Configurations on Web Interface

5.1 Introduction to Web Interface

Modify the IP address of PC to make it at the same network segment with that of LAN port of the UC100-1V1S1O gateway (the default IP of LAN port is 192.168.11.1).

Open a web browser on the PC and then enter the IP address of LAN port. Click **Login**, and the login GUI is displayed. Both the default username and password are admin.

The displayed login GUI is shown as follows:

Figure 7 Introduction to login GUI

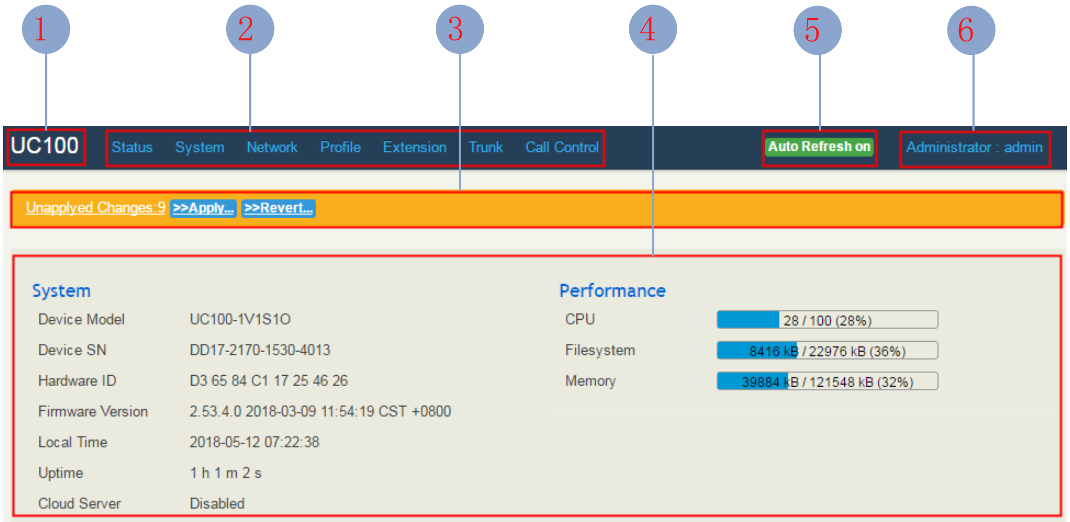


Table 5-1 Introduction of Web Interface

Index	Item	Description
1	UC100	The name of the gateway; it can be edited on the **System → Setting** interface
2	Menu Bar	The menu bar of UC100-1V1S1O
3	Unsaved Changes	All changes to the configuration of the gateway need to be saved. Click **Apply** to enter into the page to save the changes; click **Revert** to return to original configuration.
4	Detailed Interface	The detailed configuration interface or display interface
5	Auto Refresh	The button can be enabled or disabled. If it is enabled, the information on the **Status → Overview/SIP/PSTN/Current**

	Button	**Call** interfaces will be refreshed automatically
6	User Role	The role of the current user logging into the Web. And the “exit” sign will pop up when the mouse moves over there. You can log out of the web from there

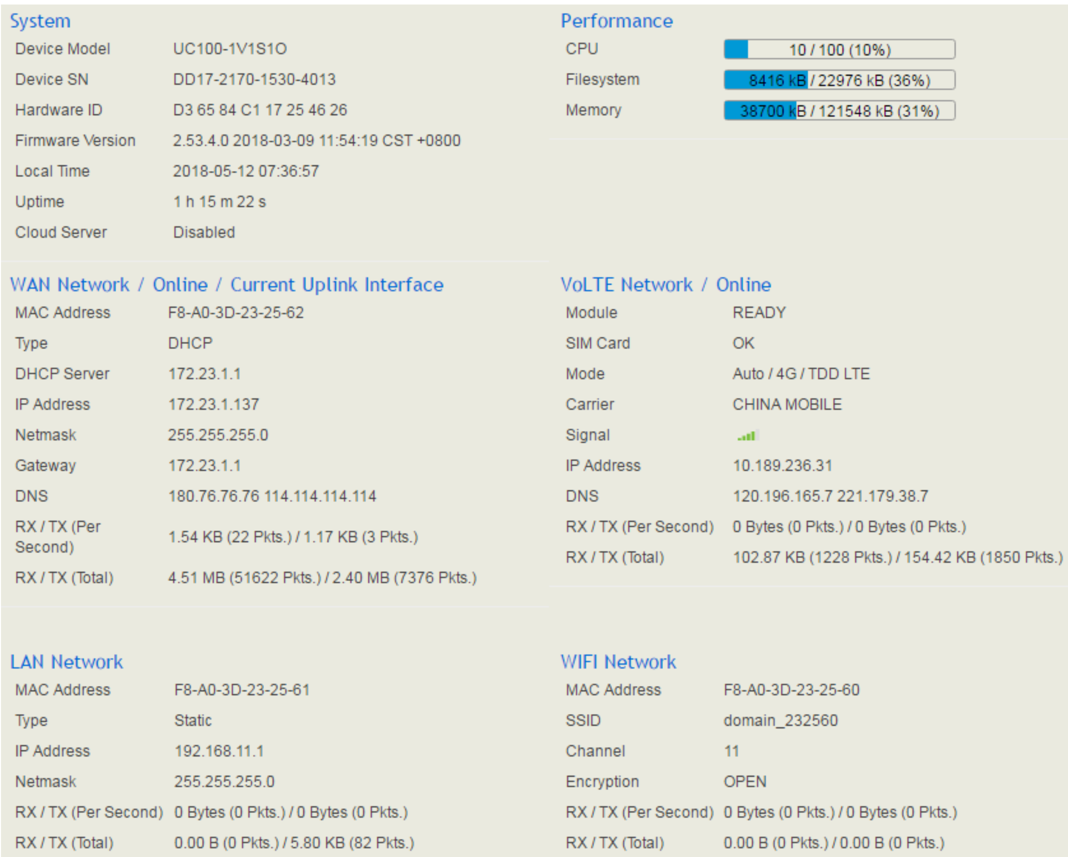
5.2 Status

The ‘Status’ meun mainly displays all kinds of status information. It includes the following sub-menus: Overview, SIP, PSTN, DHCP Client List, VPN, Wireless AP List, Current Call, CDRs, Service and About.

5.2.1 Overview

Log in the Web interface of UC100-1V1S1O, click **Status → Overview**, and the following interface will be displayed. On the interface, divice model, firmware version as well as information about performance, WAN network, LTE network, LAN network, WiFi and DHCP server are shown.

Figure 8 Overview



5.2.2 SIP

Click **Status → SIP**, and the following interface will be displayed. On the interface, information of SIP profile, SIP Trunk and SIP extension is shown.

Figure 9 Status of SIP Profile, SIP Trunk and SIP Extension

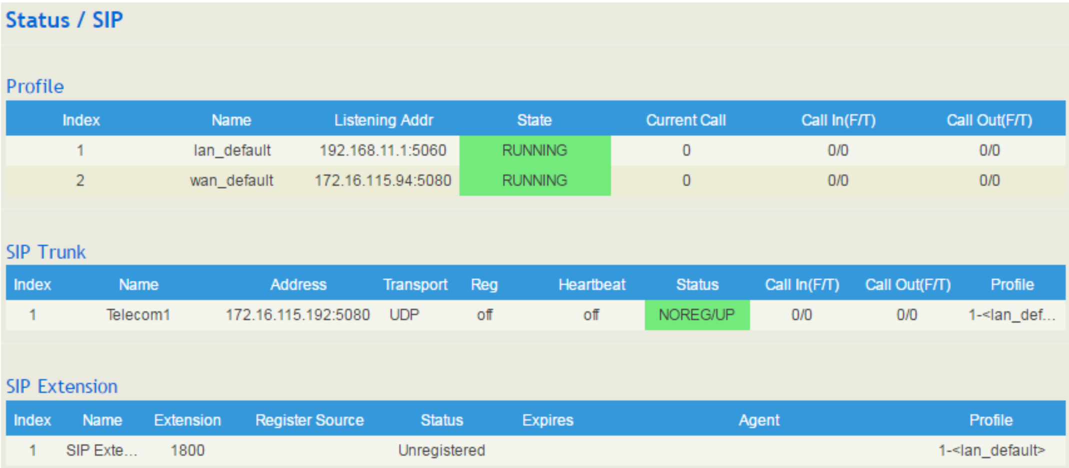


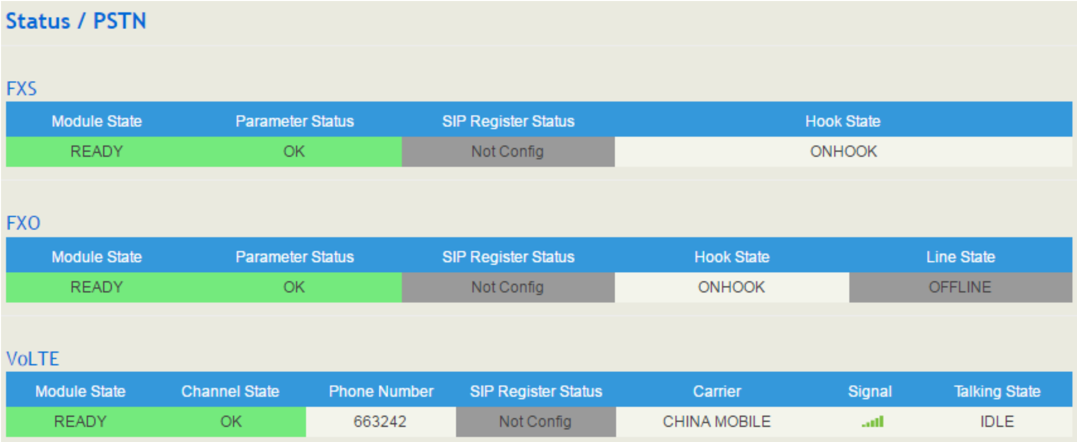
Table 5-2 Explanation of SIP Parameters

Belong To	Parameter	Explanation
Profile	Name	The name of the SIP profile
	Listening Address	The current listening address and port of SIP
	State	Green color means normal running, while red color means listening address and port of SIP is unavailable. There are two states :Running and Down
SIP Trunk	Heartbeat	If heartbeat is enabled, option message will be sent to peer device (the peer device is reachable)
	Status	Green color means available, while red color means abnormal, unavailable or prohibited. There are five statuses: Running, Reged/Up, Noreg/Up, Trying-Down, Fail-Wait
	Profile	The profile that is used by the SIP trunk
SIP Extension	Profile	The profile that is used by the SIP extension
	Status	SIP extension is registered or not. There are two statuses: Registered. Unregistered

5.2.3 PSTN

On the **Status → PSTN** interface, information of FXS and FXO is shown. Green color means available or registered, while red color means abnormal, unregistered or prohibited.

Figure 10 Status of FXS and FXO



If 'SIP Register Status' is 'Registered', it means FXS and FXO have been **registered to SIP server** on the **Trunk → SIP/FXO** interface respectively. FXS can also be registered to SIP server on the **Extension → FXS** interface.

Table 5-2 Status Explanation of FXS and FXO

Belong To	Parameter	Explanation
FXS	Module Status	There are two module statuses: Ready and Config Failed
	Parameter Status	There are two parameter statuses: OK and error
	SIP Register Status	There are two SIP register statuses: Registered and Unregistered
	Hook State	There are two hook states: Onhook and Offhook
FXO	Module Status	There are two module statuses: Ready and Config Failed
	Parameter Status	There are two parameter statuses: OK and error
	SIP Register Status	There are two SIP register statuses: Registered and Unregistered
	Hook State	There are two hook states: Onhook and Offhook
	Line State	There are two hook states: Online and Offline
VoLTE	Channel State	The state of the VoLTE channel. If the VoLTE SIM card is successfully registered, it means the channel state is OK.
	Phone Number	The number of the VoLTE SIM card
	SIP Register Status	The register status of the VoLTE trunk in use

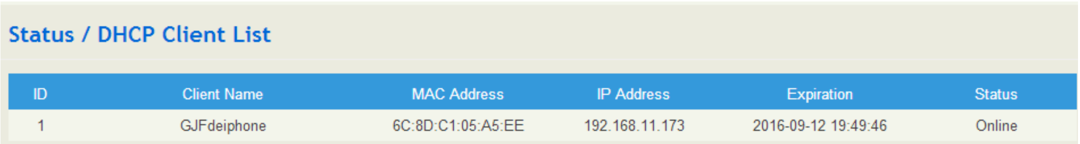
	Carrier	The carrier of the VoLTE SIM card
	Signal	The signal strength of the VoLTE SIM card
	Talking State	Whether the SIM card is on call or not

5.2.4 DHCP Client List

UC100-1V1S1O has a built-in DHCP server. When the DHCP server is enabled, it can assign IP addresses to the clients connected to it.

On the **Status →DHCP Client List** interface, information of DHCP clients connected to the UC100-1V1S1O gateway, such as client name, Mac address and IP address, is shown.

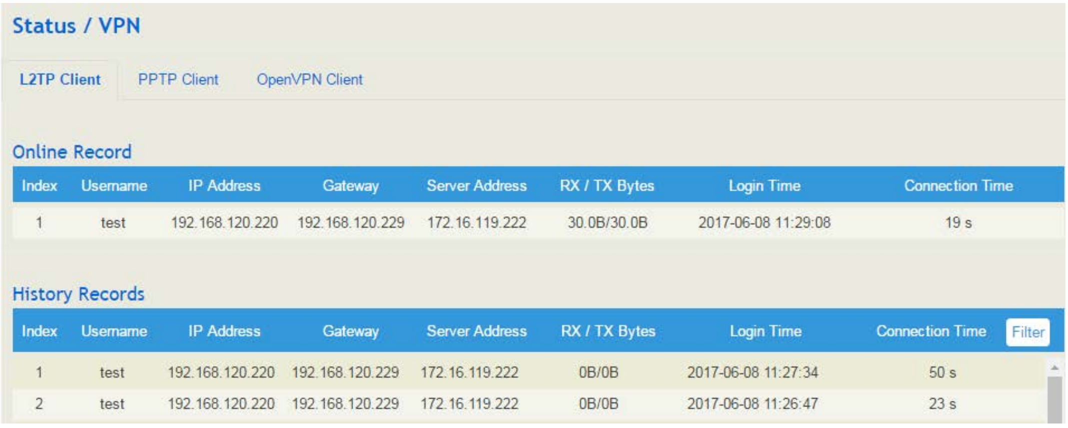
Figure 11 DHCP Client List



5.2.5 VPN

The UC100-1V1S1O gateway can serve as a VPN client to connect to a VPN server. On the **Status →VPN** page, the online records and the historical records of working as a L2TP client, a PPTP client and an OpenVPN client are displayed.

Figure 5-6 VPN Connection Records



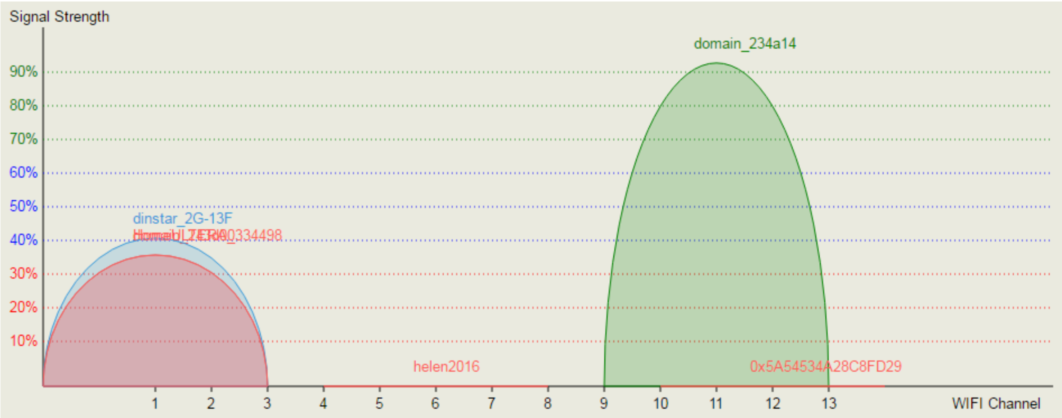
5.2.6 Wireless AP List

On the **Status →Wireless AP List** page, the wireless SSID, encryption methods, signal strength of neighboring access points are shown, when the WLAN function of UC100-1V1S1O WLAN is enabled.

The explanations of WiFi parameters are as follows:

- WiFi Channel：Each SSID corresponds to a curve. The horizontal axis value of the peak refers to the WiFi channel that is used .The range of channels is from 1 to 13.
- Signal Strength：Each SSID corresponds to a curve. The vertical axis value of the peak refers to the signal strength. Signal intensity is shown in the form of percentage.
- Channel: The channel used for the SSID search.
- Encryption: The encryption methods used for the SSID search. Currently , UC100-1V1S1O supports three encryption methods, including WPA2+PSK, WPA+PSK and NONE.
- Filter: Click the Filter button, and you can query the APs that you need can be filtered from the list according to the index, channel, SSID, BSSID/MAC, encryption methods and signal.

Figure 5-7 Wireless AP List



Wireless AP List

Index	Channel	SSID	BSSID / MAC	Encryption	Signal	Filter
1	1	HomeULTERA_334498	A0:F1:22:33:44:98	WPA2+PSK	39%	
2	1	domain_243d00	F8:10:3D:24:3D:00	NONE	39%	
3	1	dinstar_2G-13F	F8:A0:3D:59:0A:8C	WPA2+PSK	44%	
4	6	helen2016	6C:E8:73:B2:62:98	WPA2+PSK	0%	
5	11	domain_234a14	F8:10:3D:23:4A:14	NONE	96%	
6	12	0x5A54534A28C8FD29	BC:D1:77:52:5B:AA	WPA2+PSK	0%	

5.2.7 Current Call

On **Status →Current Call** interface, the source, destination, calling number, called number, start time, answer time, state and duration of the current real-time call are shown. If there is no current call, no information will be shown

Figure 5-8 Current Call Information

Status / Current Call

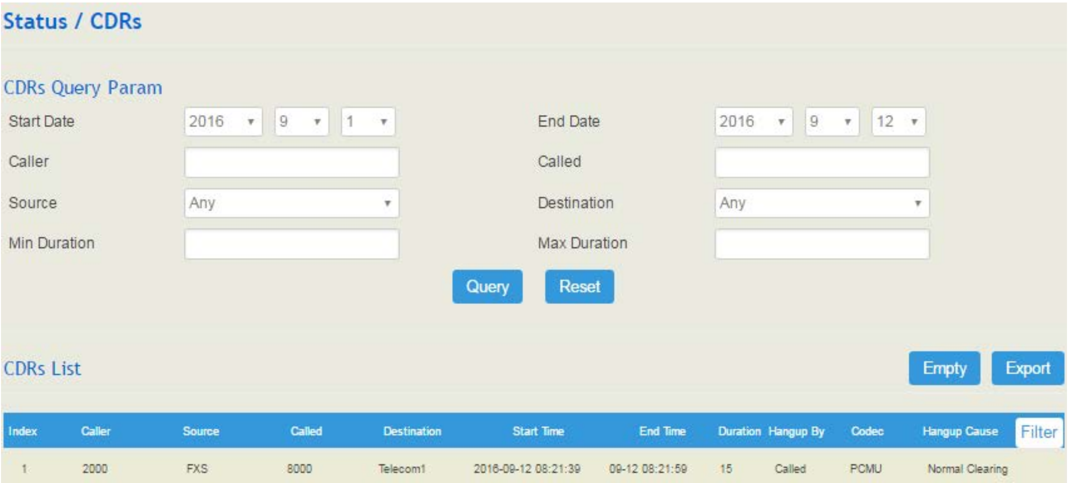
Index	Src	Dest	Caller	Called	Start Time	Answer Time	State	Duration	Filter

5.2.8 CDRs

Click **Status → CDRs,** and you can set query criteria to query the CDRs (Call Detailed Records) that you want on the displayed interface. Meanwhile, you are allowed to clear CDRs or export CDRs through clicking the **Empty** or **Export** button. The maximum number of CDRs that can be saved is 5000.

CDRs cannot be saved on the **Status → CDRs** interface unless the CDRs function has been enabled on the **System → Setting** interface.

Figure 5-9 CDRs



5.2.9 Service

Click **Status → Service**, and the service status of UC100-1V1S1O is displayed. This function is enabled by default. The Web, SSH and Telnet service can be disabled and their ports can be modified on the **Network → Access Control** interface. If no running status is shown, it means exception has occurred on UC100.

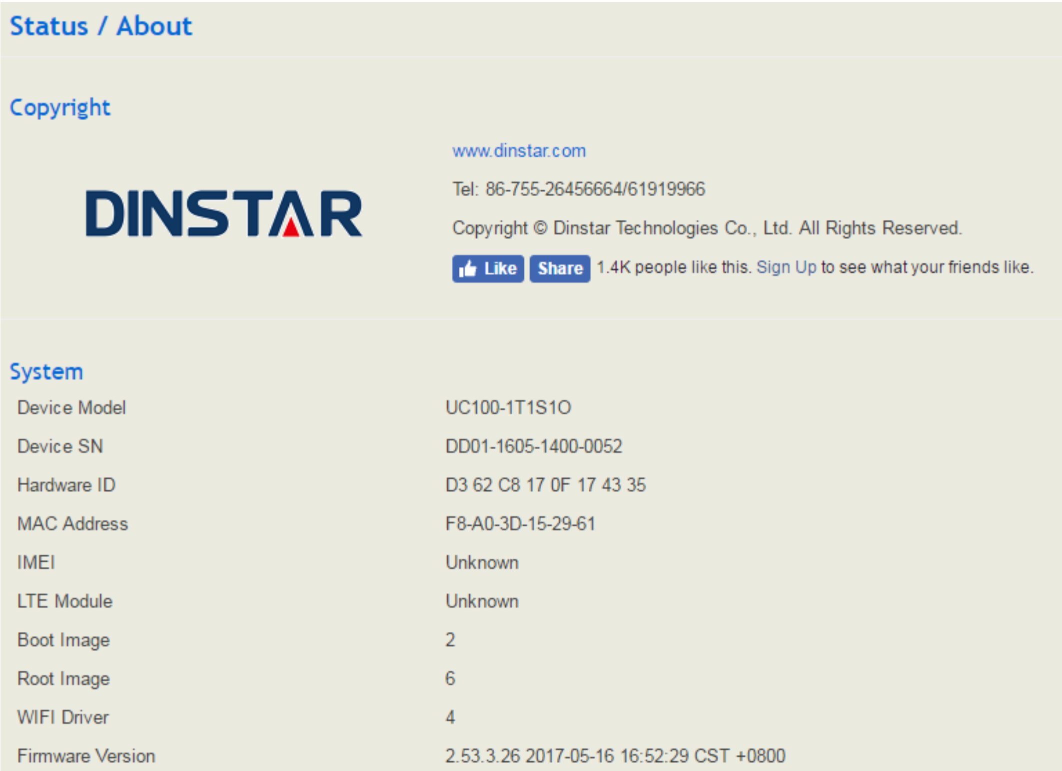
Besides, if syslog is disabled on the **System → Setting** interface, the logs cannot be uploaded to the server, but log service is still running.

Figure 5-10 Service Status

5.2.10 About

On the **Status** → **About** page, the device model, device SN, hardware ID, MAC address, IMEI, VoLTE module, boot image, root image, WIFI driver , firmware Version of the UC100-1V1S1O device are displayed.

Figure 5-11 About Status



5.3 System

Configurations for hostname, timezone, NTP, login username & password, other user name,provision, TR069,operation log, service log, upgrade/backup/restore, IVR upload, Command Line,cloud server and device reboot can be carried out in the System section.

5.3.1 Setting

On the System → Setting interface, you can modify the device name, set a new timezone, synchronize local time and enable CDRs, Syslog as well as built-in NTP server.

Figure 5-12 Basic Setting

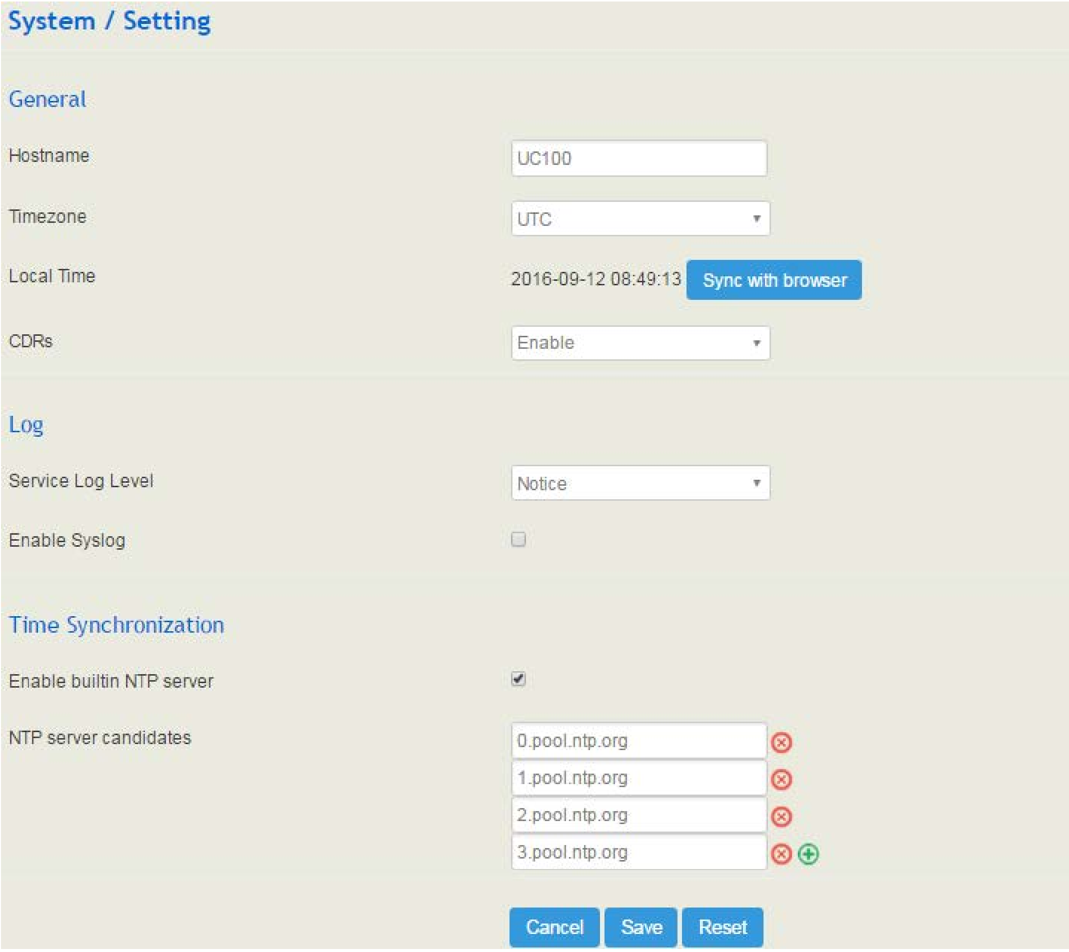


Figure 5-4 Explanation of Basic Setting Paratermers

Parameter	**Explanation**
Hostname	The name of the gateway. After it is configured, the name will be displayed on the left of the menu bar.
Timezone	You can choose a time zone you want. The default value is UTC (Universal Time Coordinated)
Local Time	The current time based on current time zone. It is synchronized with NTP.
CDRs	If it is enabled, CDRs will be saved automatically. 5000 CDRs call be saved at most and they can be queried on the **Status → CDRs** interface. If it is disabled, CDRs will not be saved
Service Log Level	There are eight levels, including Debug, Info, Notify, Warning, Error, Critical, Alert and Emergency
Enable Syslog	Whether to enable syslog
Time	If NTP server is enabled, the UC100-1V1S1O can be synchronized with the world standard time. Meanwhile, you’re able to add or

Synchronization	reduce NTP servers. Please consult local telecom operators or surf the internet for the address of NTP servers.
	Delete a NTP Server
	Add a NTP Server

5.3.2 User Manager

Click **System → User Manager**, and you can modify the username name and password for logging in the UC100-1V1S1O gateway. Factory defaults for username name and password are both admin, so it is advised to modify them for security consideration.

The abovementioned username and password are also used to log in Web Interface, Telnet and SSH.

The user can establish observer, operator and administrator users under super administrator. Setting names, passwords, expiration dates, and Setting up the view and the edit permission for all functions for the user.

Figure 5-13 Modify Username ,Password and Manager Users

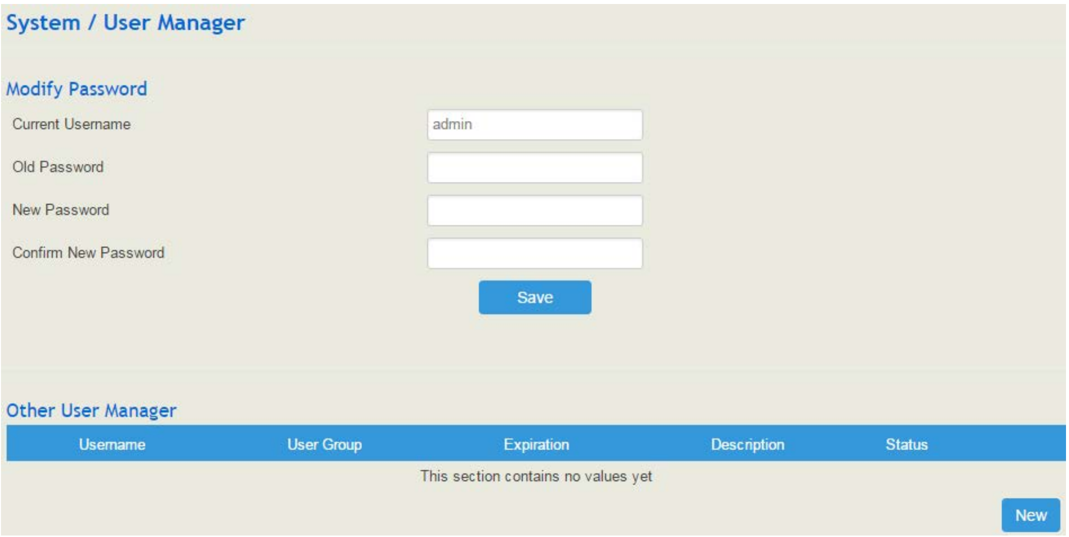


Figure 5-14 New User Manager

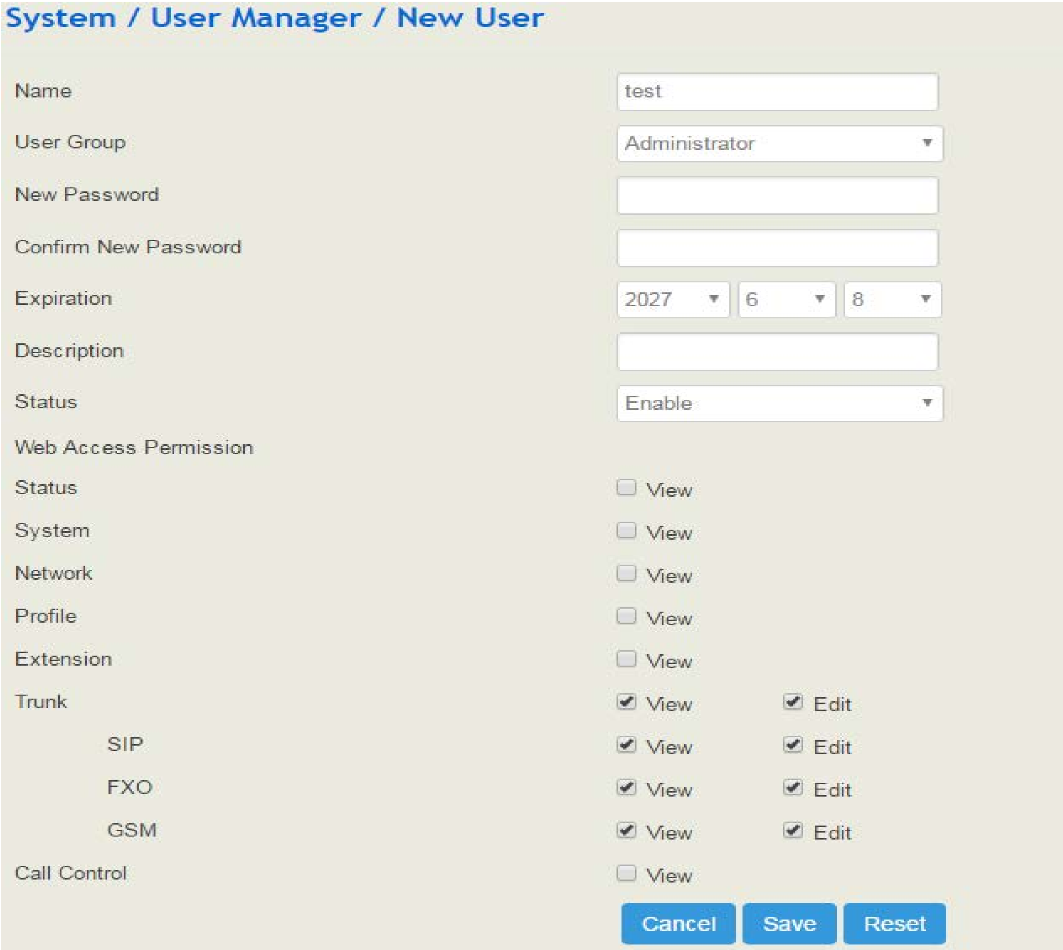


Figure 5-5 Explanation of Provision Parameters

Parameter	**Explanation**
Name	The name of the new user. After it is established, the name and the password will log onto the web page.
User Group	You can set up the administrator,the operator or the observers for the new user. The default value is the administrator.
New Password	Setting the login password for the user.The password should not be too short for 8-32 characters.
Expiration	The User login or operational expiry date.
Status	Choose enable or disable.
Web Access Permission	The ability to use hooks to provide users with the ability to edit or view the functionality of the web.

5.3.3 Provision

Provision is used to make UC100-1V1S1O automatically upgrade with the latest firmware stored on an http server, an ftp server or a tftp server.

As for how to configure UC100-1V1S1O and http/ftp/tftp server for Provision, please make reference to the instruction guide of Provision.

Select the checkbox on the right of **Enable**, and you will see the following interface:

Figure 5-15 Provision

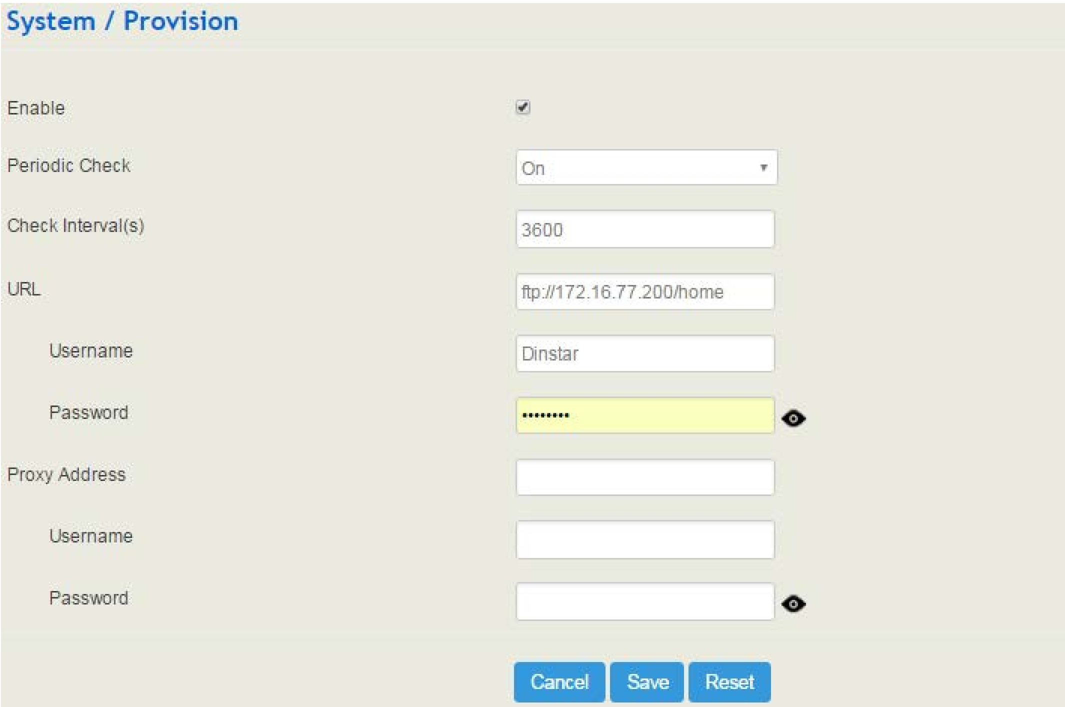


Table 5-6 Explanation of Provision Parameters

Parameter	Explanation
Periodic Check	Whether to enable periodic check. If it is enabled, the gateway will automatically check whether the firmware vesion stored on the URL is updated.
Check Interval	The interval to check whether the firmware vesion stored on the URL is updated. If it is 3600s, the gateway will check every 3600s.
URL	The URL of the http/ftp/tftp server: For example: ftp://172.16.77.200/home tftp://172.16.77.200/provision.xml http://test.domain.com/test
Username	The login username of the http/ftp/tftp server

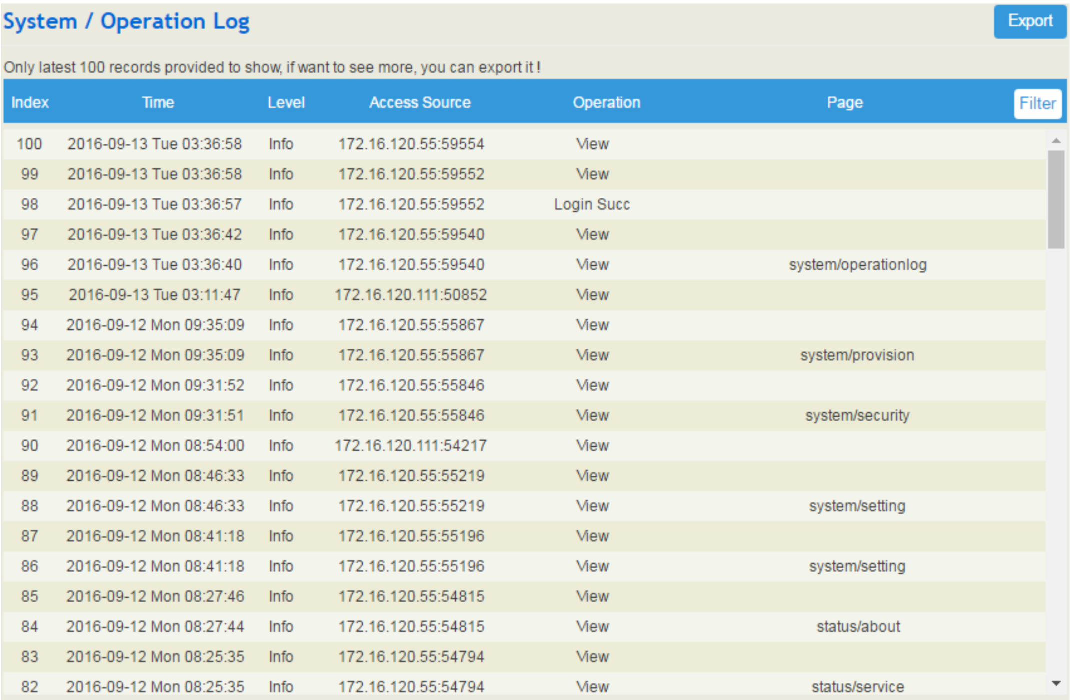
Password	The login password of the http/ftp/tftp server

Note: Proxy Address, Proxy Username and Proxy Password are optional to be configured.

5.3.4 Operation Log

The logs tracing the operations carried out on the Web can be queried on the **System → Operation Log** interface. You are allowed to set query criteria to query the logs that you want and to export the logs through clicking the **Export** button at the top-right corner.

Figure 5-16 Operation Logs



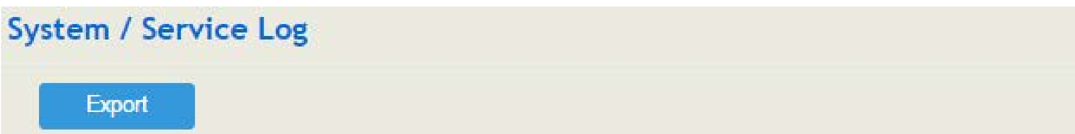
Index	Time	Level	Access Source	Operation	Page
100	2016-09-13 Tue 03:36:58	Info	172.16.120.55:59554	View	
99	2016-09-13 Tue 03:36:58	Info	172.16.120.55:59552	View	
98	2016-09-13 Tue 03:36:57	Info	172.16.120.55:59552	Login Succ	
97	2016-09-13 Tue 03:36:42	Info	172.16.120.55:59540	View	
96	2016-09-13 Tue 03:36:40	Info	172.16.120.55:59540	View	system/operationlog
95	2016-09-13 Tue 03:11:47	Info	172.16.120.111:50852	View	
94	2016-09-12 Mon 09:35:09	Info	172.16.120.55:55867	View	
93	2016-09-12 Mon 09:35:09	Info	172.16.120.55:55867	View	system/provision
92	2016-09-12 Mon 09:31:52	Info	172.16.120.55:55846	View	
91	2016-09-12 Mon 09:31:51	Info	172.16.120.55:55846	View	system/security
90	2016-09-12 Mon 08:54:00	Info	172.16.120.111:54217	View	
89	2016-09-12 Mon 08:46:33	Info	172.16.120.55:55219	View	
88	2016-09-12 Mon 08:46:33	Info	172.16.120.55:55219	View	system/setting
87	2016-09-12 Mon 08:41:18	Info	172.16.120.55:55196	View	
86	2016-09-12 Mon 08:41:18	Info	172.16.120.55:55196	View	system/setting
85	2016-09-12 Mon 08:27:46	Info	172.16.120.55:54815	View	
84	2016-09-12 Mon 08:27:44	Info	172.16.120.55:54815	View	status/about
83	2016-09-12 Mon 08:25:35	Info	172.16.120.55:54794	View	
82	2016-09-12 Mon 08:25:35	Info	172.16.120.55:54794	View	status/service

Note: Operation logs are generally used to locate faults by device manufacturer.

5.3.5 Service Log

Service logs (the running logs of UC100-1V1S1O) can be exported on the **System → Service Log** interface. Those logs are used for analyzing where a problem has occurred on the gateway.

Figure 5-17 Service Log



5.3.6 Config Changes Log

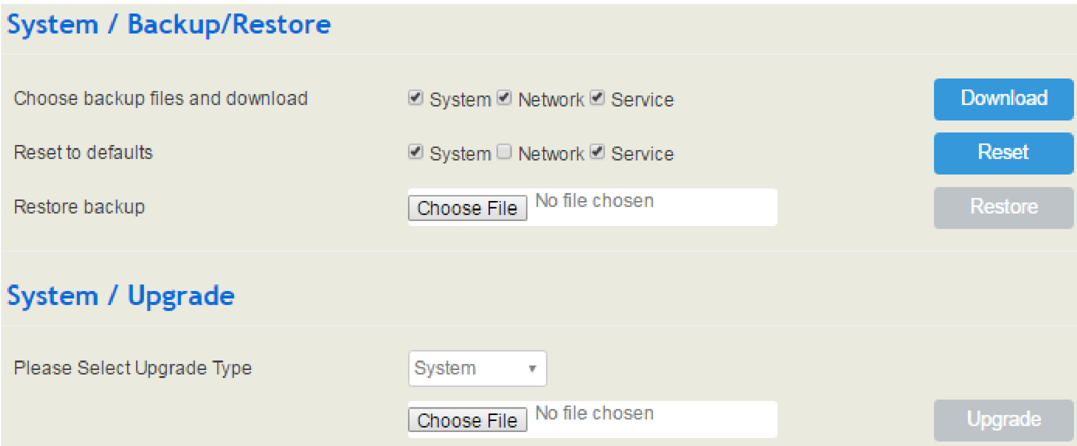
On the **System →Config Changes Log** interface, the configurations changed by administrator on the Web of the gateway are recorded.

Figure 5-18 Config Changes Log

5.3.7 Backup/Restore/Upgrade

On the **System → Backup/Restore/Upgrade** interface, you can back up or restore configuration data, and can upgrade UC100 to a new version. But you need to restart the device for the change to take effect after executing restore or upgrade.

Figure 5-19 Backup/Resotre/Upgrade



Note: the file you choose to be upgraded on the above interface is a local file, while the version file upgraded through the Provision function is a file from http/ftp/tftp server.

Table 5-7 Explanation of Backup/Resotre/Upgrade Button

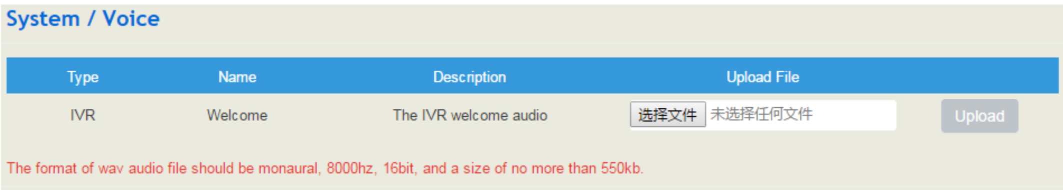
Download	You can download the configuration data to be backuped. Select any of the checkboxes on the left of System, Network and Service, and then click

	Download
Reset	Select any of the checkboxes on the left of System, Network and Service, and then click **Reset**, and configurations related to the selected part will be restored to factory defaults.
Restore	Choose a backup file, and then click **Restore**.
Upgrade	Choose a file to be upgraded (which is provided by Shenzhen Dinstar Co., Ltd.), and then click **Upgrade**.

5.3.8 Voice

On the **System → Voice** interface, you can upload an IVR file according to your needs. At present, only wav audio file is allowed. The format of the uploaded wav audio file must be: monaural, 8000hz, 16bit, and size of no more than 550KB.

Figure 5-20 Upload IVR File

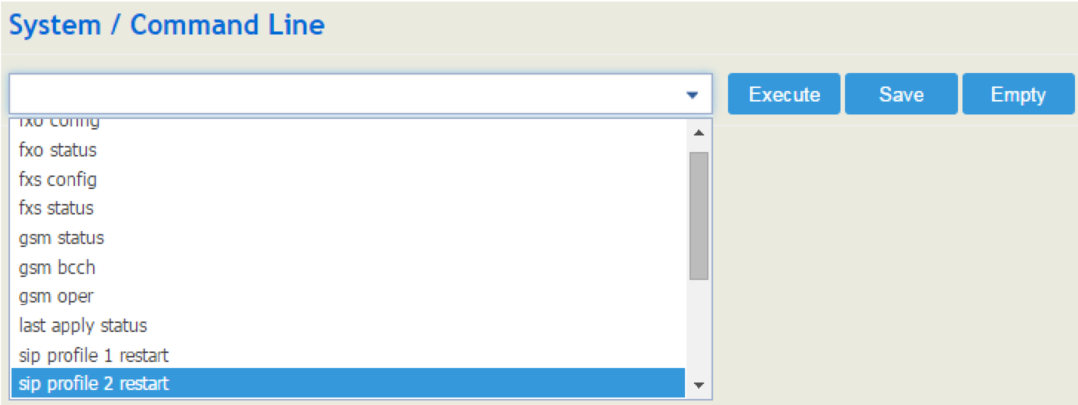


5.3.9 Command Line

On the **System → Command Line** interface, some commonly-used command lines can be directly selected in the draw-down box, and therefore user has no need to enter command lines on Telnet. In this way, the efficiency of problem diagnostics is greatly improved.

Commonly-used command lines include fxo config, fxo status, fxs config, fxs status, gsm status, gsm bcch, gsm oper, sip status, sip profile and so on.

Figure 5-21 Command Line



5.3.10 Diagnostics

Use a telephone line to connect the FXS port and the FXO port, and then insert SIM card. On the **System → Diagnostics** interface, select a module (FXS/FXO or LTE) that you want to diagnose. Click Start, and the gateway will begin to diagnose the selected module(s).

If the progress bar of diagnostics is green, it means the module that is diagnosed works well; if the progress bar is red, it means the module that is diagnosed is faulty.

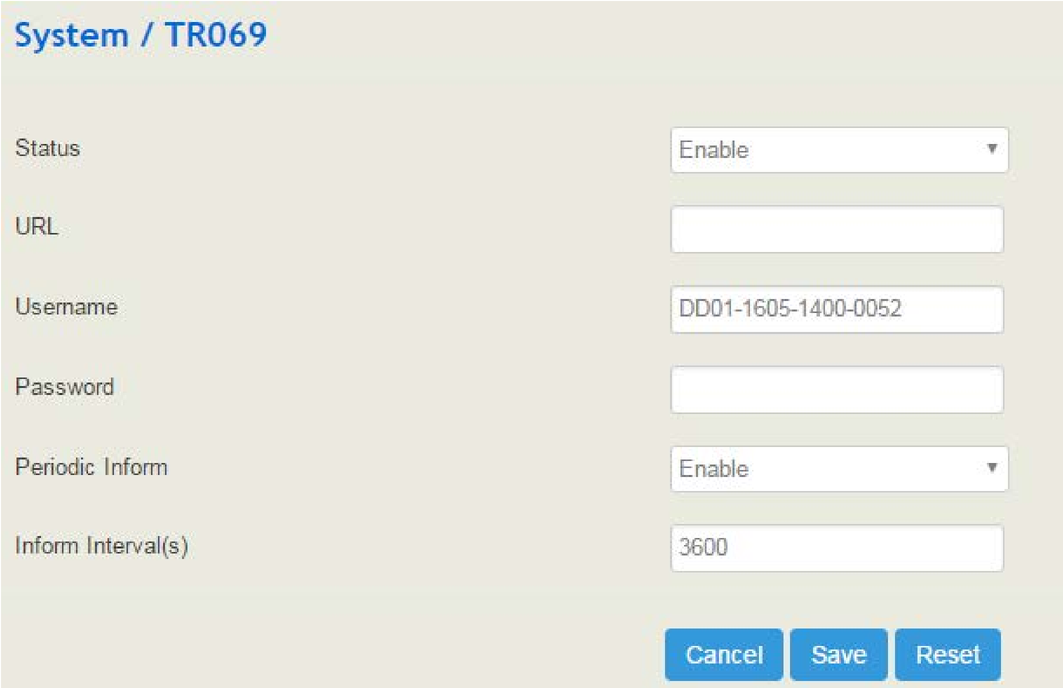
Figure 5-22 Diagnostics

5.3.11 TR069

TR069 is a communication protocol between CPE and ACS. CPE can use this agreement to complete service opening, function setting, file upload and download, system test, and so on.

The UC100-1V1S1O gateway can work as a TR069 client. Enter the IP address, service username and password of TR069 server, the gateway will connect to the TR069server. On the System →TR069 page, you can enable the 'Periodic Inform' and set a report interval. When TR069 is used or related configuration is changed, you will be informed.

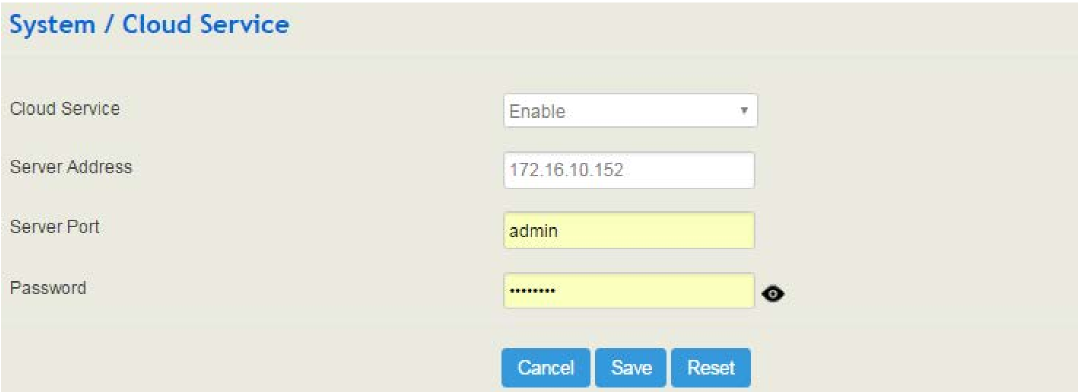
Figure 5-23 Diagnostics



5.3.12 Cloud Server

Cloud service is mainly used to centrally manage all kinds of devices. Through cloud service, you can query the status of a device, upgrade devices at batch, log in or configure a device remotely. The UC100-1V1S1O gateway provides Cloud service. Enter the IP address, service port and password of Cloud server, the gateway will connect to the Cloud server.

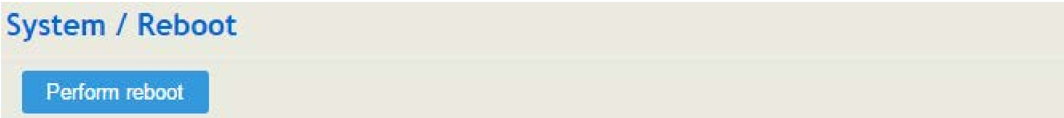
Figure 5-24 Cloud Server



5.3.13 Reboot

On the **System → Reboot** interface, you can click **Perform Reboot** to reboot the UC100-1V1S1O gateway. After the device is rebooted, those configurations that have been saved will remain unchanged.

Figure 5-25 Reboot Device



5.4 Network

UC100-1V1S1O works in two modes: route mode and bridge mode. When it is under the route mode, the IP of WAN must be different from the IP of LAN. But when it is under the bridge mode, the IP of WAN and the IP of LAN are the same.

5.4.1 Setting

On the **Network → Setting** interface, you can set the IP address of WAN port and LAN port, and can turn on WiFi.

Under the route mode, the default IP address of WAN port is a DHCP IP address, while the default IP address of the LAN port is 192.168.11.1.

In fact, there are three kinds of IP addresses for selection for WAN port and LAN port, including Static IP address, DHCP and PPPOE.

DHCP: Obtain IP address automatically.

UC100-1V1S1O is regarded as a DHCP client, which sends a broadcast request and looks for a DHCP server to answer. Then the DHCP server automatically assigns an IP address to the UC100-1V1S1O from a defined range of numbers.

Figure 5-26 Default IP Address under Route Mode

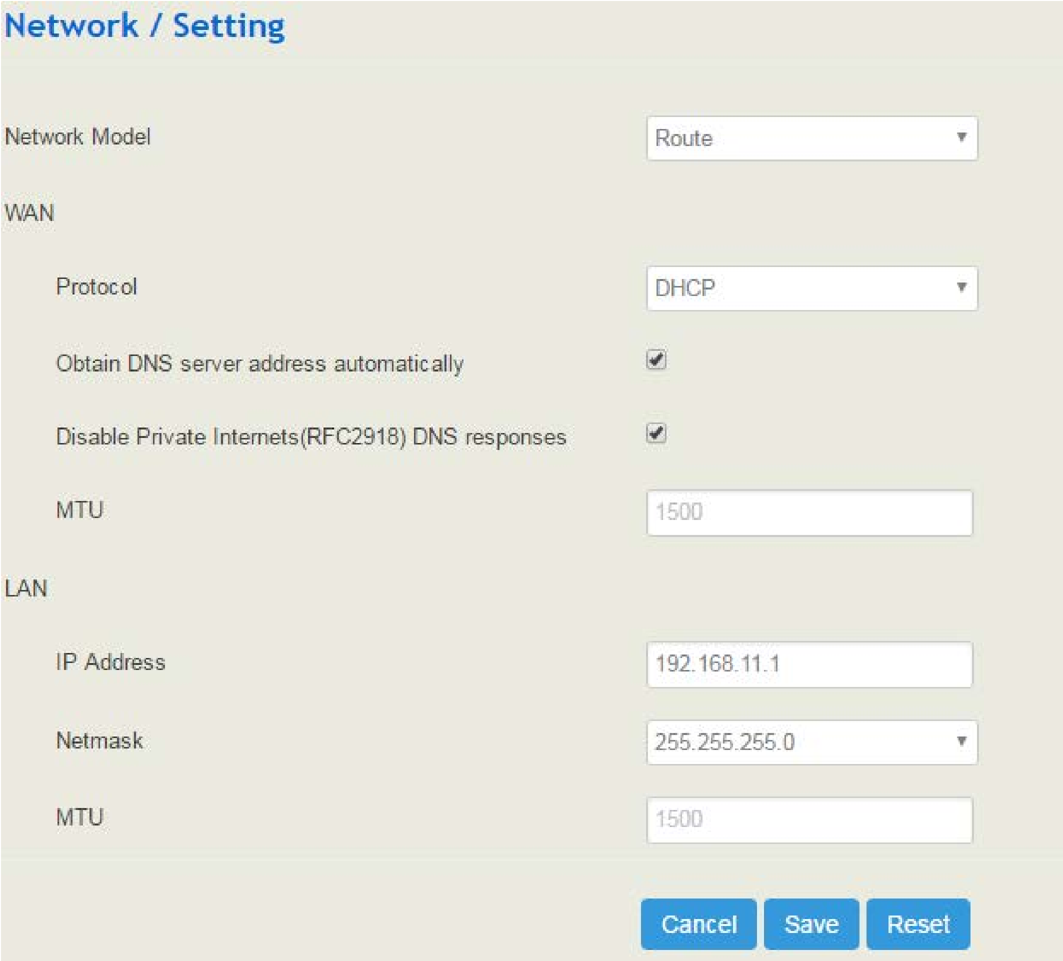
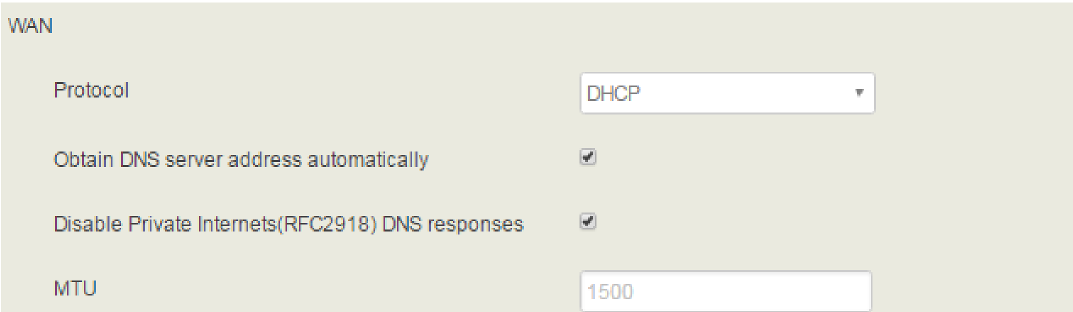


Figure 5-27 Set WAN IP as DHCP IP



Note: When WAN IP is set as DHCP IP, please ensure that there is DHCP server working normally in the network.

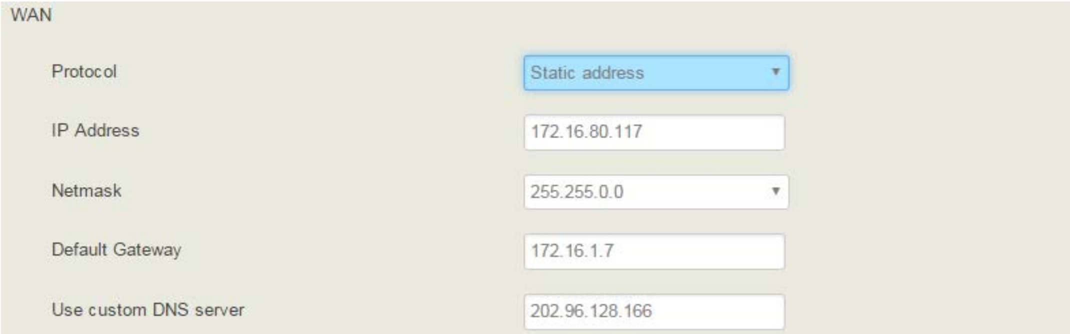
Static IP Address:

Static IP address is a semi-permanent IP address and remains associated with a single computer over an extended period of time. This differs from a dynamic IP address**,** which is assigned *ad hoc* at the start of each session, normally changing from one session to the next.

If you choose static IP address, you need to fill in the following information:

- IP Address: the IP address of the WAN port of the UC100-1V1S1O;
- Netmask: the netmask of the router connected the UC100-1V1S1O;
- Default Gateway: the IP address of the router connected the UC100-1V1S1O;
- Use custom DNS server: the IP address of the DNS server

Figure 5-28 Set WAN IP as Static Address



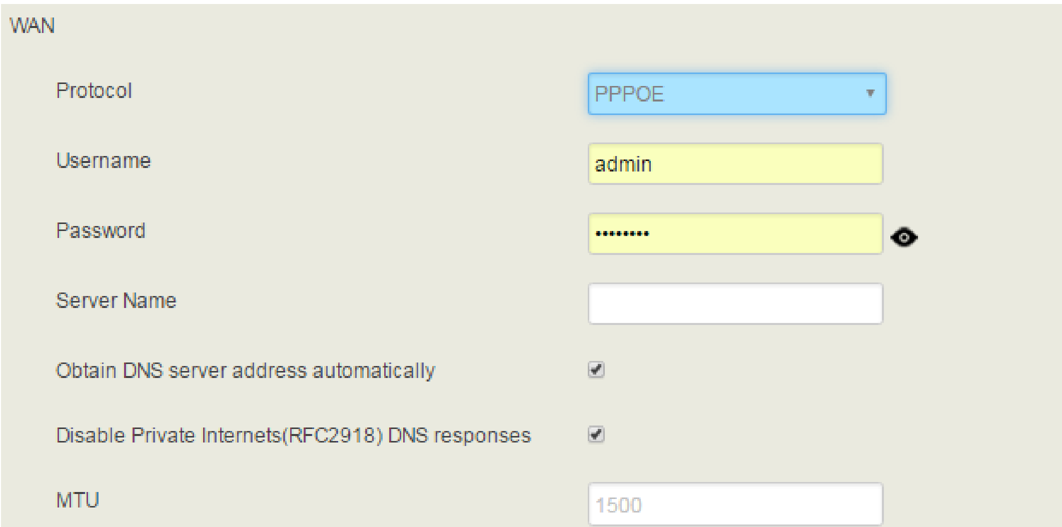
PPPoE:

PPPoE is an acronym for point-to-point protocol over Ethernet, which relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. PPPOE IP address refers to IP address assigned through the PPPoE mode.

If you choose PPPoE, you need to fill in to fill in the following information:

- Username: the account name of PPPoE
- Password: the password of PPPoE
- Server Name: the name of the server where PPPoE is placed

Figure 5-29 Set WAN IP as PPPoE IP



5.4.2 WLAN

On the **Network → WLAN** page, you can enable WLAN service and fill in information of the wireless channel, TX Power and so on. By default, there is a SSID, and you can create three new SSIDs.

WLAN: Wireless local Area Networks, it use wireless technology to transmit data, voice and video signals in the air.

Figure 5-30 WLAN config

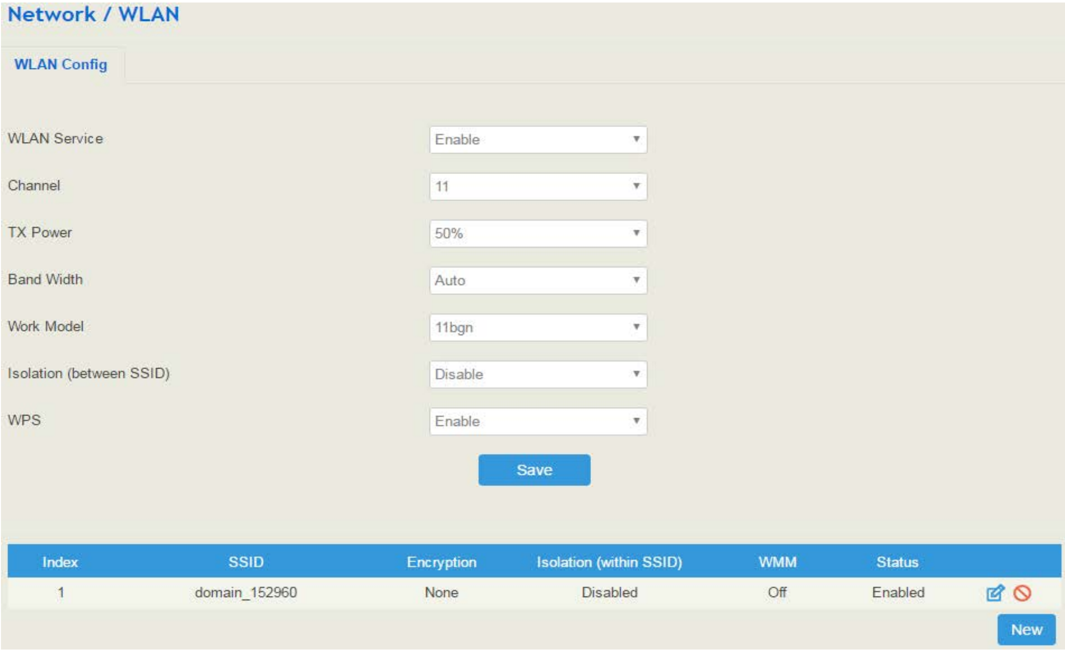


Table 5-8 Explanation of Parameters for WLAN

WLAN service	Chose enable or disable
channel	There are 1-11channels and auto options. It will automatically select one from the 1-11 channel for wireless use when you select auto.
TX Power	The signal strength of the SSID. The range is 10% to 100%.
Band Width	The band width of the signal can be configured 20MHz, 40MHz and automatic.
Work Model	WLAN has a working pattern of 11bg, 11b, 11b, 11g, 11abgn, 11bgn, and 11agn.
Isolation (between SSID)	Chose enable or disable. If the wireless isolation is enabled, different SSID cannot communicate with one another.
WPS	WPS is a WiFi Protected Setup and allows for a WIFi connection. Choose enable or disable.

Figure 5-31 SSID Configuration

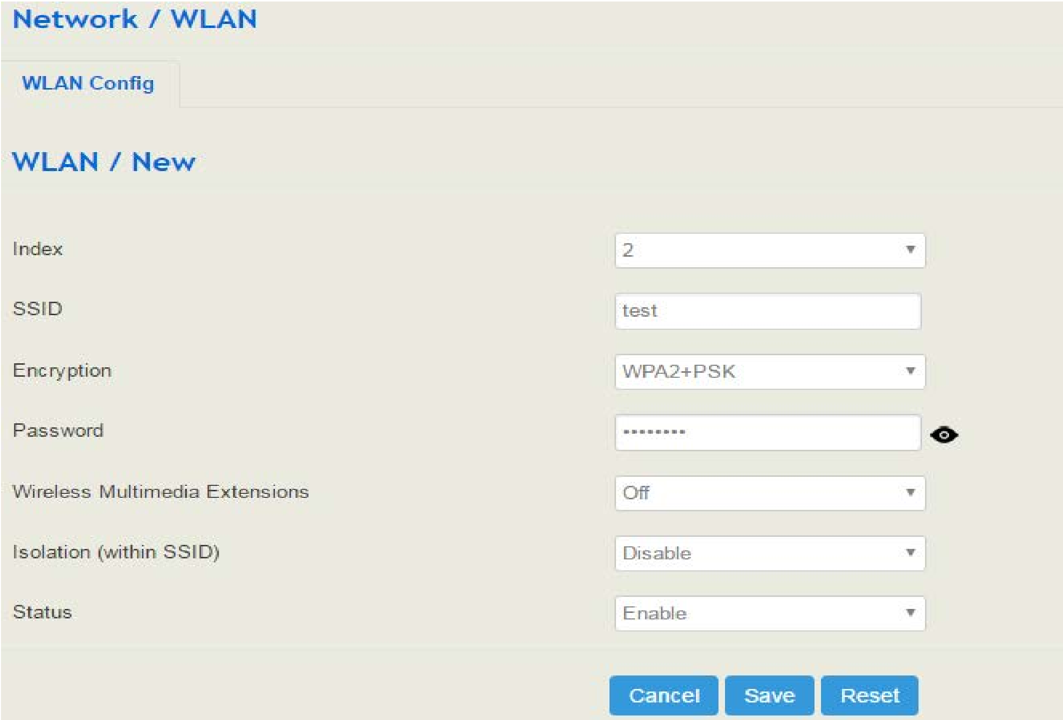


Table 5-9 Explanation of Parameters for SSID Configuration

SSID	Short for Service Set Identifier. The SSID contains letters, digits or underscore, and its length cannot be more than 32 characters, It cannot conflict with local other SSIDs!
Encryption	There are three types of WiFi encryption, None, WPA + PSK and WPA2 + PSK.
Password	When you configure the encryption, you can set the password here.
Wireless Multimedia Extensions	
Isolation (within SSID)	Chose enable or disable. If the wireless isolation is enabled, Different devices connected to the same SSID cannot communicate with each other.
Status	Chose enable or disable.

5.4.3 VoLTE

On the **Network → VoLTE** page , you can enable the VoLTE service, and fill in information of APN， username， password, mode, PIN code, dial number and so on.

Figure 5-32 VoLTE Config

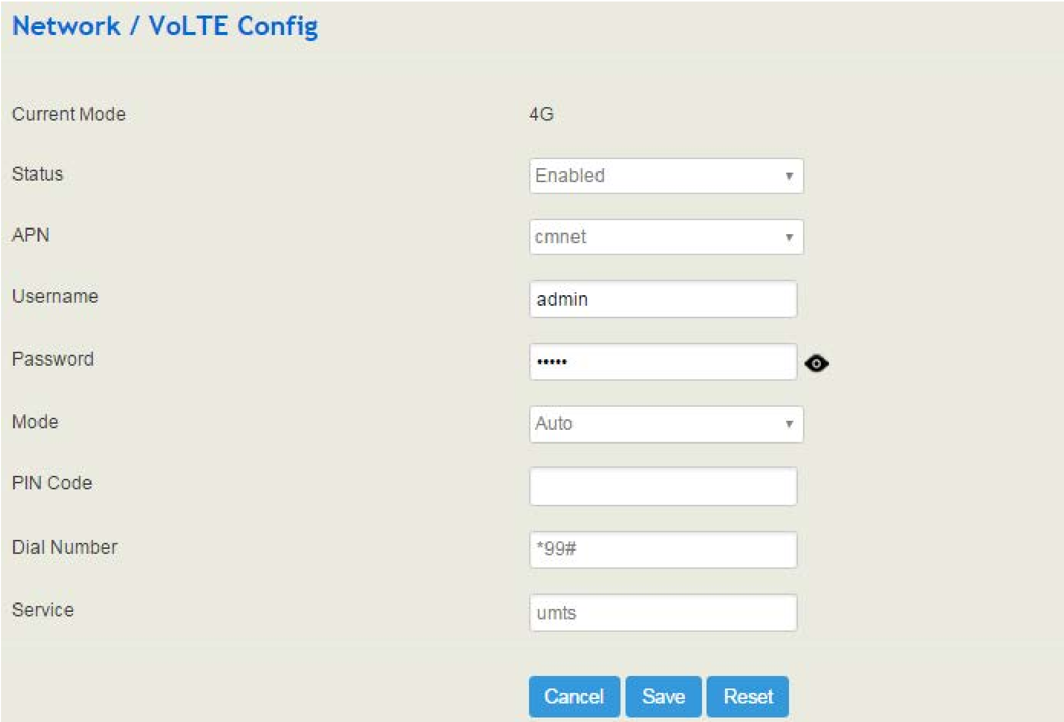


Table 5-10 Explanation of Parameters for VoLTE Config

Current Mode	4G
Status	The LTE module is enabled or not. There are two statuses: Enabled. Disabled
APN	The name of access point, you can select 3GNET. Cmnet or custom.
Username	The name of VoLTE module, used to access network
Password	The password of VoLTE module, used to access network
Mode	The mobile network has 2g & 3g, 4g, or automatic configuration.
PIN Code	The SIM card's personal identification number.
Dial Number	The LTE network's dialing number.
Service	The LTE service type is UMTS.

5.4.4 Uplink Config

On the **Network → Uplink Config** page, you can configure an uplink strategy based on the priority between WAN and VoLTE. The "WAN Master, VoLTE Slave" means that the data from the UC100-1V1S1O will be transmitted through the WAN port, and when the WAN fails, the data will be transmitted through LTE, while the "VoLTE Master, WAN Slave" is the opposite.

Figure 5-33 LTE Config

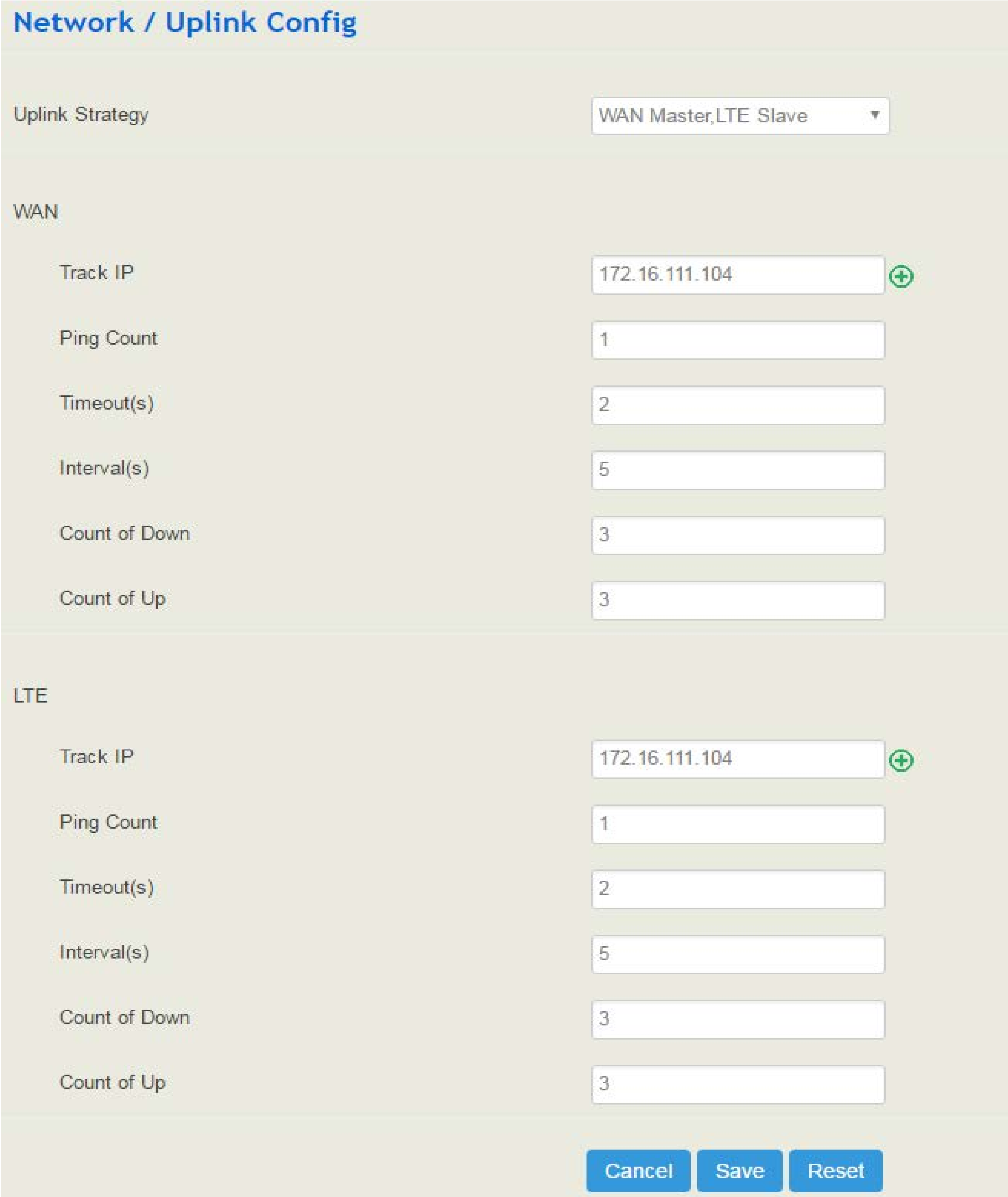


Table 5-11 Explanation of Parameters for Uplink Config

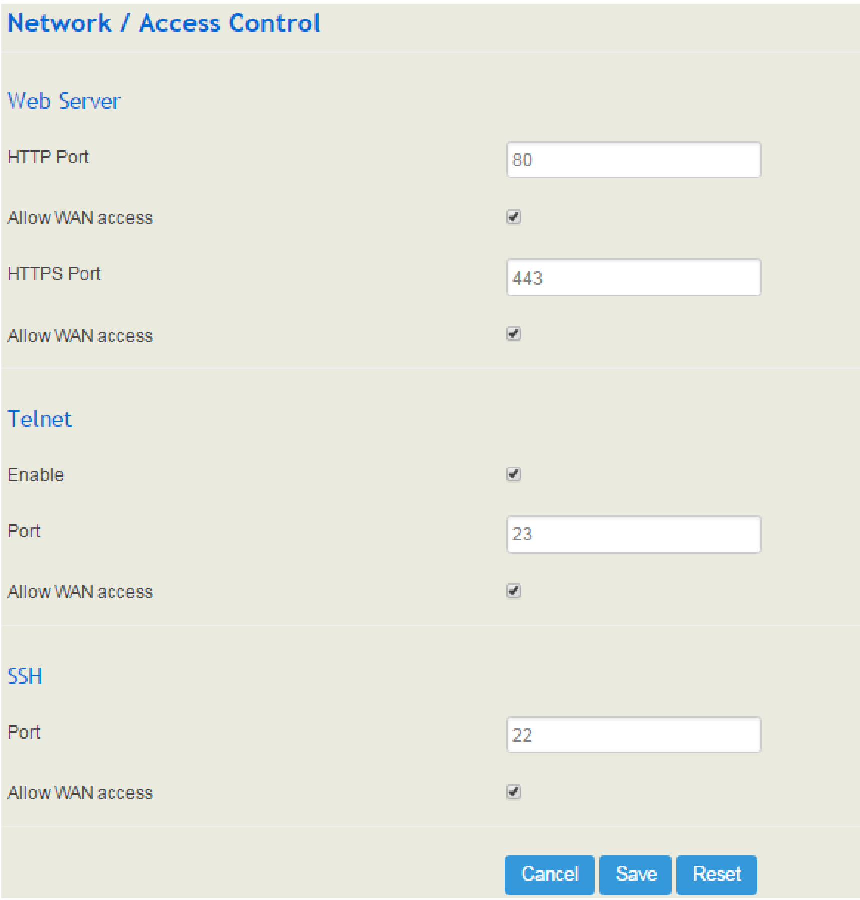
Uplink Strategy	WAN Master,LTE Slave or LTE Master,WAN Slave
Track IP	A WAN (or LTE) tracking IP address (which can be more than one), when this address is not available, it is thought that the network of WAN (or LTE) is not available, switching to LTE (or WAN). If this IP is 0.0.0.0.0, it means the current configured DNS address and gateway is being tracked by PING .
Ping Count	The times of checking IP addresses by PING.
Timeout(s)	If the Ping does not respond during the timeout period, it is thought as a connection failure. For example, the timeout period

	is set as 2 seconds, which means if there is no response after the IP is checked by Ping for 2 seconds, it is a connection failure
Interval(s)	The interval for the device to check IP address by PING
Count of Down	The number of consecutive failures (by PING), if this value is reached, it means the network connection fails
Count of Up	The number of consecutive successes (by PING), if this value is reached, it means the network is available

5.4.5 Access Control

The access ports of Web, Telnet and SSH, as well as relevant on-off controls, can be configured on the **Network → Access Control** interface. Web supports http and https, while SSH supports OAuth 2.0 protocol.

Figure 5-34 Access Control



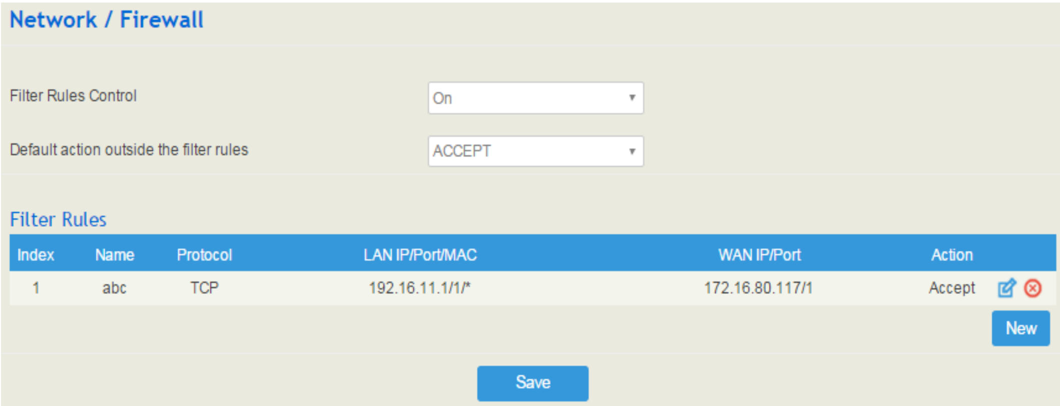
5.4.6 Firewall

If the UC100-1V1S1O works under the route mode, you can choose to enable the firewall and set filter rules to accept or reject certain destination IP addresses.

Configuration Procedures:

1. Select **On** in the drop-down box on the right of **Filter Rules Control**
2. Select filter action, accept or reject;
3. Click the **New** button;
4. Fill in information of filter rule;
5. Click the **Save** button to save the configuration.

Figure 5-35 Firewall



Note:

: Edit information for the corresponding filter rule.

: Delete the corresponding filter rule.

/*: Information of Source or Destination is not completely filled in.

Figure 5-36 Create Filter Rule

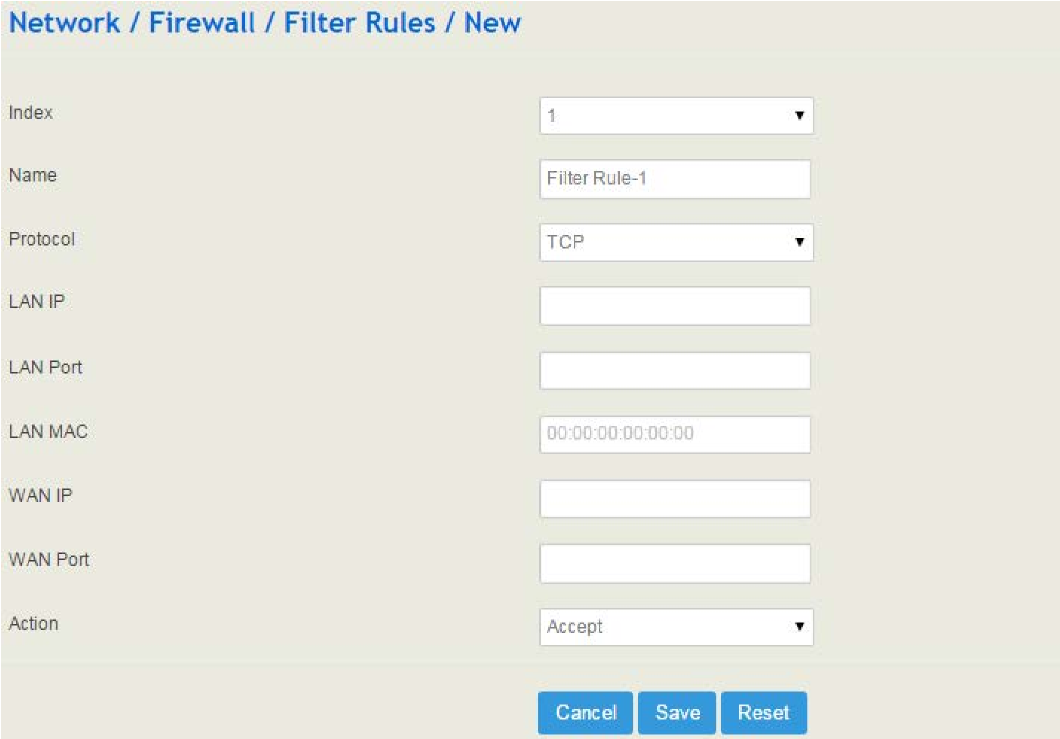


Table 5-12 Explanation of Parameters for Filter Rule

LAN IP	The IP address that you want UC100 to accept or reject. It is the IP address of a host from local-area network; it can also be a string of IP addresses, for example, 172.16.11.1/15.
LAN Port	The port of LAN host which the accepted or rejected IP address belongs to
LAN MAC	The Mac of the LAN host twhich the accepted or rejected IP address belongs to
WAN IP	The IP address that you want UC100 to accept or reject. It is the IP address of a host from wide-area network; it can also be a string of IP addresses, for example, 152.16.11.11/19.
WAN Port	The port of WAN host which the accepted or rejected IP address belongs to
Action	Choose accept ot reject

5.4.7 DHCP Server

If there is a need, you can choose to enable the built-in DHCP server of UC100-1V1S1O to assign IP addresses to PC or other clients that are in the same local-area network with UC100. Under this condition, the UC100-1V1S1O gateway works like a router.

Figure 5-37 Enable DHCP Server

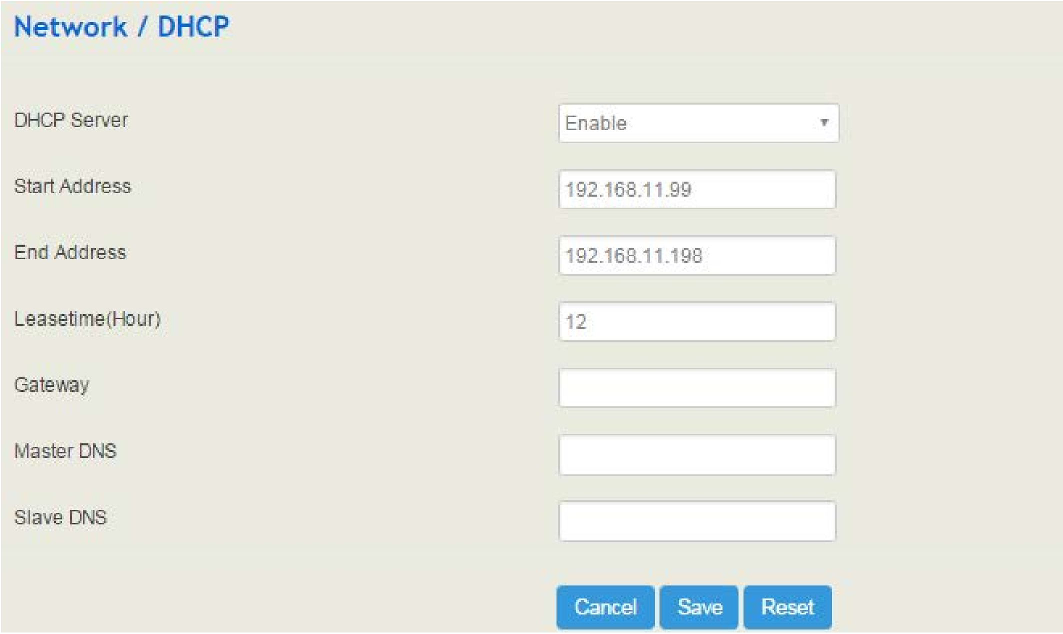


Table 5-13 Explanation of Parameters for DHCP Server

Start Address	The start IP address of the address pool to be assigned
End Address	The end IP address of the address pool to be assigned
Lease Time	The validity period of the assigned IP address
Gateway	The gateway of the IP address pool to to be assigned, it is optional to fill in
Master DNS	The master DNS of the client whose IP address is assigned by the built-in DHCP server; it is optional to fill in
Slave DNS	The slave DNS of the client whose IP address is assigned by the built-in DHCP server; it is optional to fill in

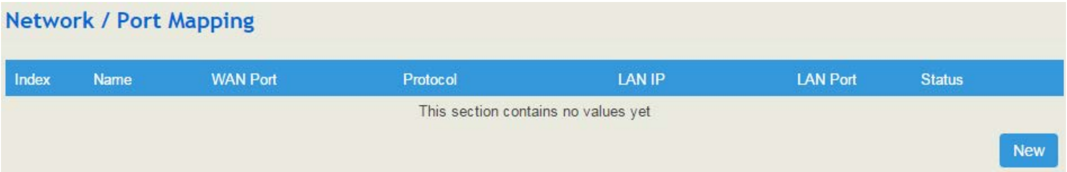
5.4.8 Port Mapping

When the UC100-1V1S1O works under the route mode, port mapping allows a client in the wide-area network to visit a client in the local-area network.

Configuration Procedures:

1. Click **Network → Port Mapping**, and the following interface will be shown.

Figure 5-38 Port Mapping



2. Click the **New** button.

3. Fill in information on the following interface.

Figure 5-39 Create New Port Mapping

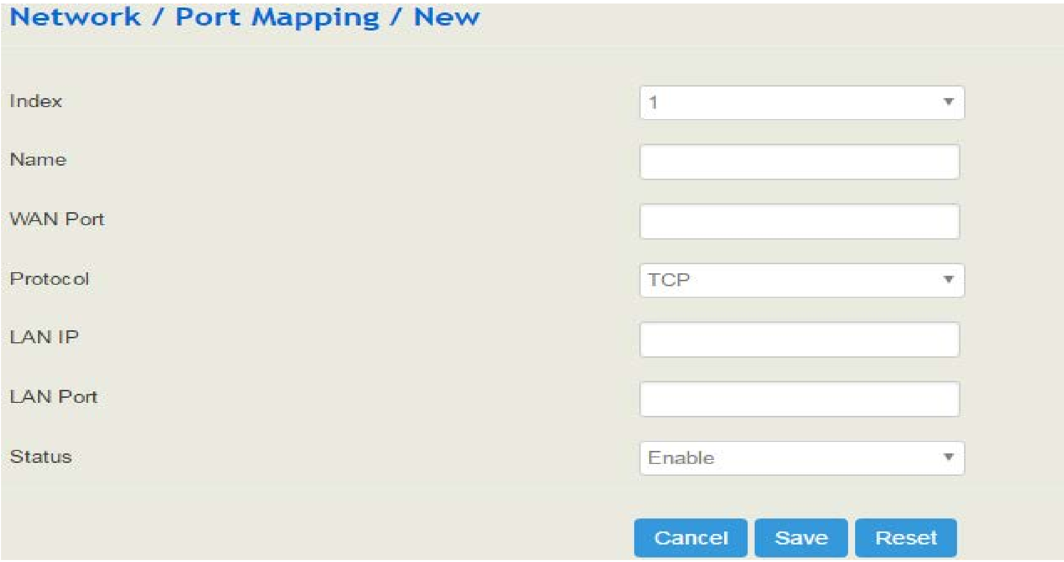


Table 5-14 Explanation of Parameters for Port Mapping

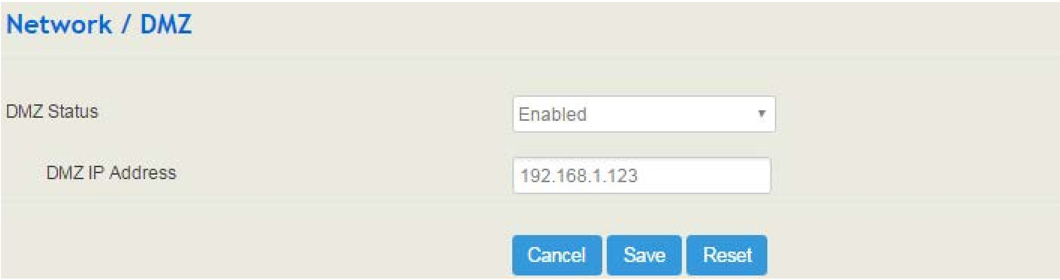
Name	The name of this port mapping
WAN Port	The port of the client in the wide-area network, which is to visit local-area network
Protocol	Choose TCP, UDP or TCP/UDP
LAN IP	The IP address of the to-be-visited client in local-area network
LAN Port	The port of the to-be-visited client in local-area network (this port cannot conflict with the port of UC100-1G1S1O)
Status	Chose enable or disable.

4. Click the **Save** button to save the above configurations.

5.4.9 DMZ Setting

When the UC100-1V1S1O gateway works under the route mode and the DMZ service is enabled, the clients in the wide-area network are allowed to have direct access to the clients in the DMZ (**demilitarized zone**).

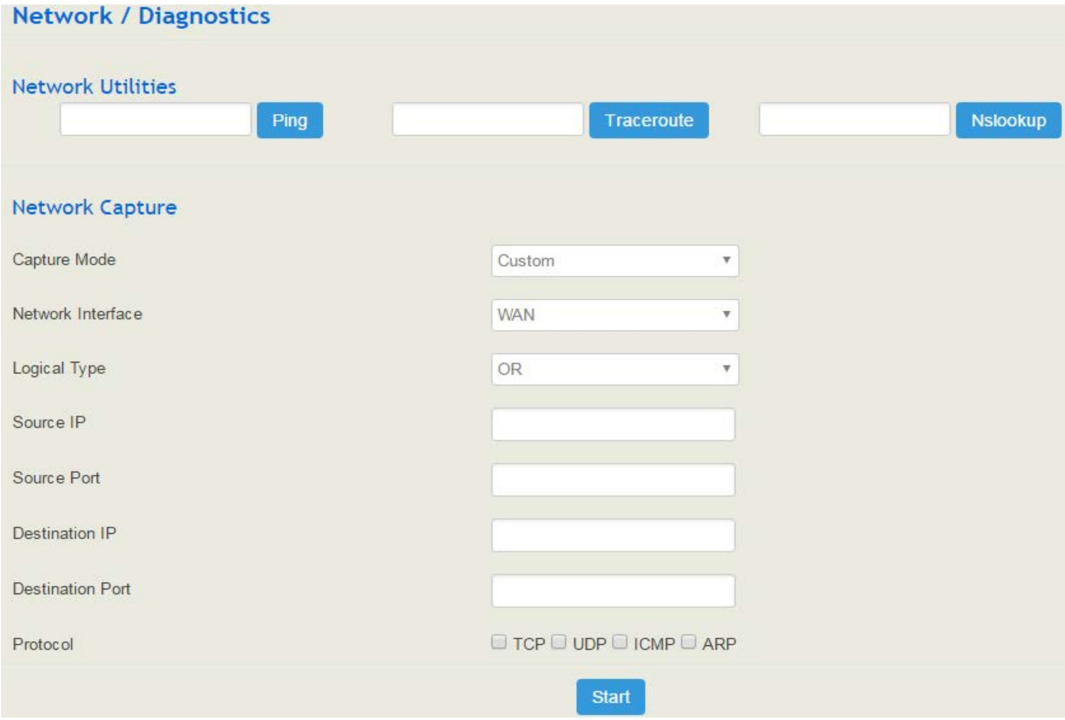
Figure 5-40 Enable DMZ Service



5.4.10 Diagnostics

On the **Network → Diagnostics** interface, you can use three network utilities including Ping, Traceroute and Nslookup to diagnose the network, and can capture data packages of the available network ports.

Figure 5-41 Network Diagnostics



Ping is used to examine whether a network works normally through sending test packets and calculating response time.

Instructions for using Ping:

1. Enter the IP address or domain name of a network, a website or a device in the input box of Ping, and then click **Ping**.

2. If related messages are received, it means the network works normally; otherwise, the network is not connected or is connected faultily.

Traceroute is used to determine a route from one IP address to another.

Instruction for using Traceroute:

1. Enter the IP address or domain name of a destination device in the input box of Traceroute, and then click **Traceroute**.

2. View the route information from the returned message.

Nslookup (Name Server Lookup) is a network command-line tool to obtain domain name of internet or to diagnose the problems of DNS.

Instruction for using Nslookup:

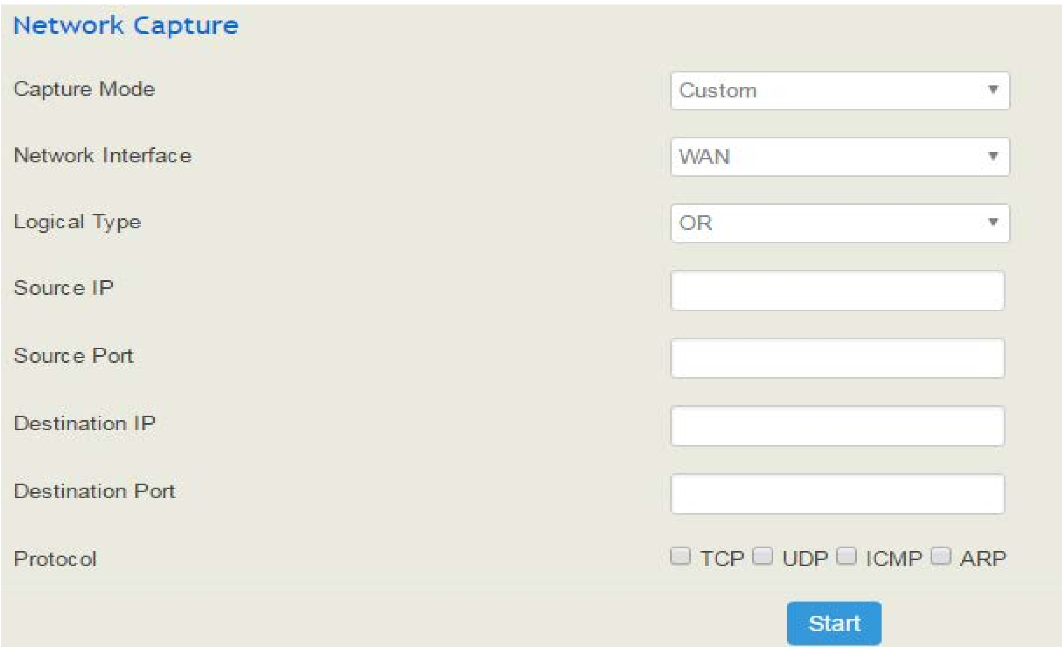
1. Enter a domain name and then click **Nslookup**.
2. View the DNS information from the returned message.

Network Capture

On the following interface, you can capture data packages of the available network ports. You can also set source IP, source port, destination IP or destination port to capture the packages that you want.

There is a "and"/" or "logical type. The "and" relationship can only capture a one-way message, or "or" relationship to fetch the interaction message between a particular IP.

Figure 5-42 Network Capture



Note: If there are multiple source or destination IP addresses, please use '|' to separate them, for example, 172.16.115.12|172.16.115.15.

After package capturing is completed, save the captured packages on a computer and then use a tool to analyze them.

5.4.11 DDNS

If DDNS（Dynamic Domain Name Server）service is enabled , when the IP address bound to a domain name changes, the new IP address will be sent to the DDNS, and thus user can visit the device via the new IP address or domain name and incoming calls can arrive the device via the domain name.

Figure 5-43 Enable DDNS Service

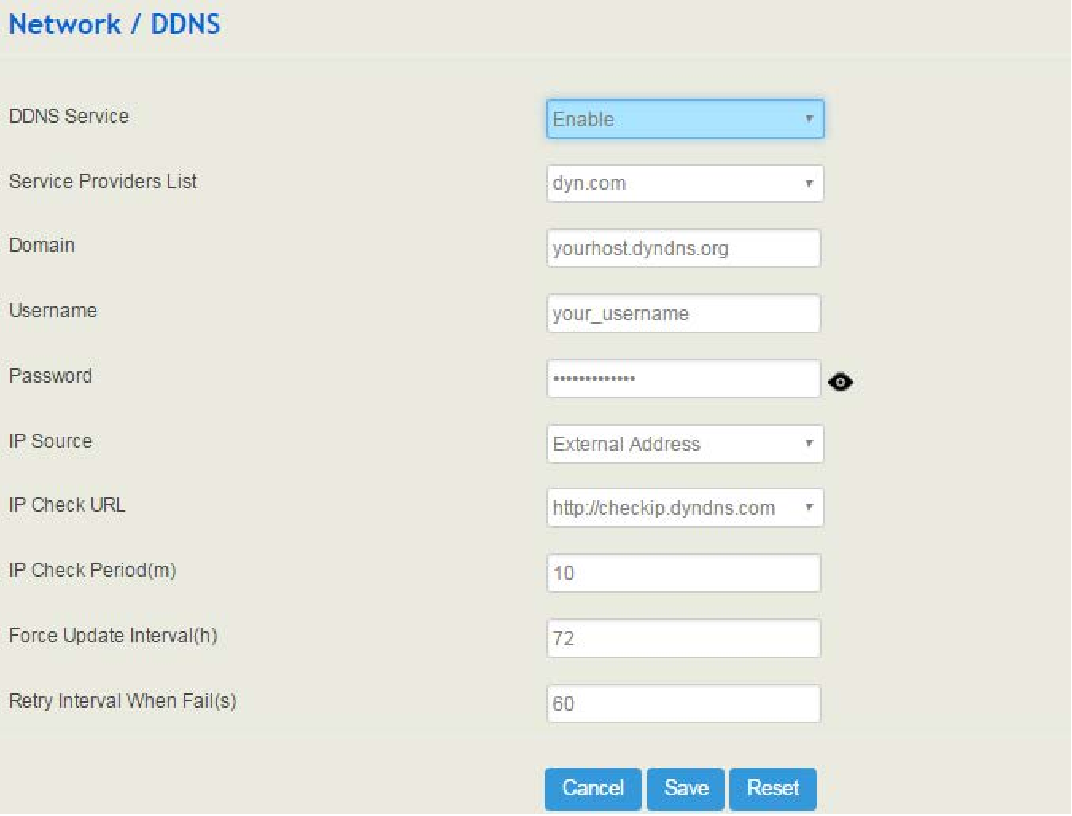


Table 5-15 Explanation of Parameters for DDNS Service

DDNS Service	To enable or disable DDNS service
Service Providers List	Select a service provider from the draw-down box or customize a service provider. The service providers on the list include: dyn.com, changeip.com, he.net, ovh.com, dnsomatic.com, 3322.org, easydns.com and oray.com.
Domain	The domain of DDNS, which is offered by service provider

	When service provider is a customized service provider, the format of domain is as follows: domain->[DOMAIN],ip->[IP],username->[USERNAME],password->[PASSWORD],whereby domain, ip, username and password are variables， you need to turn it into fixed values, namely [DOMAIN],[IP],[USERNAME]and [PASSWORD]. For example, if the service provider offers the following update-url： http://bob:password@dynupdate.no-ip.com/nic/update?hostname=mytest.testdomain.com&myip=172.16.80.113 You need to turn it into: http://[USERNAME]:[PASSWORD]@dynupdate.no-ip.com/nic/update?hostname=[DOMAIN] &myip=[IP]
Username	The username for logging in DDNS, which is offered by service provider
Password	The password for logging in DDNS, which is offered by service provider
IP Source	The source of IP address bound to the domain name, including external address and device address
IP Check URL	When IP source is an external address, user visit this URL and he can know the current public IP address.
IP Check Period(m)	The period for checking whether IP address has changed
Force Update Interval (h)	The interval for forcibly updating DDNS service (in other words, the interval for sending IP update request to DDNS)
Retry Interval When Fail (s)	The interval for retrying to send IP update request to DDNS when IP update fails

5.4.12 Static Route

On the **Network → Static Route** interface, you can configure static routes for the network.

Figure 5-44 Create New Static Route

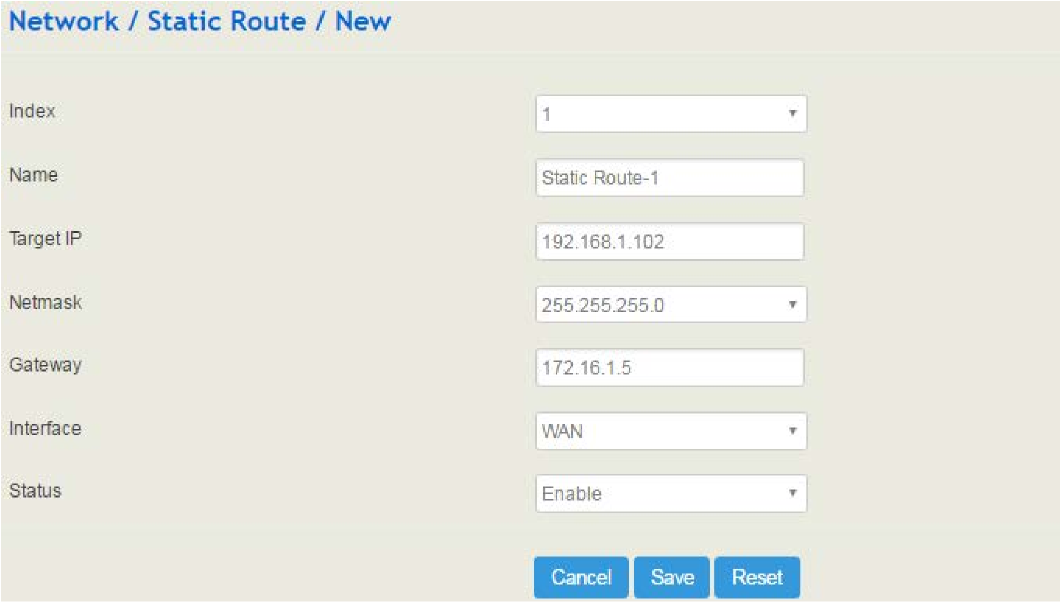


Table 5-16 Explanation of Parameters for Static Route

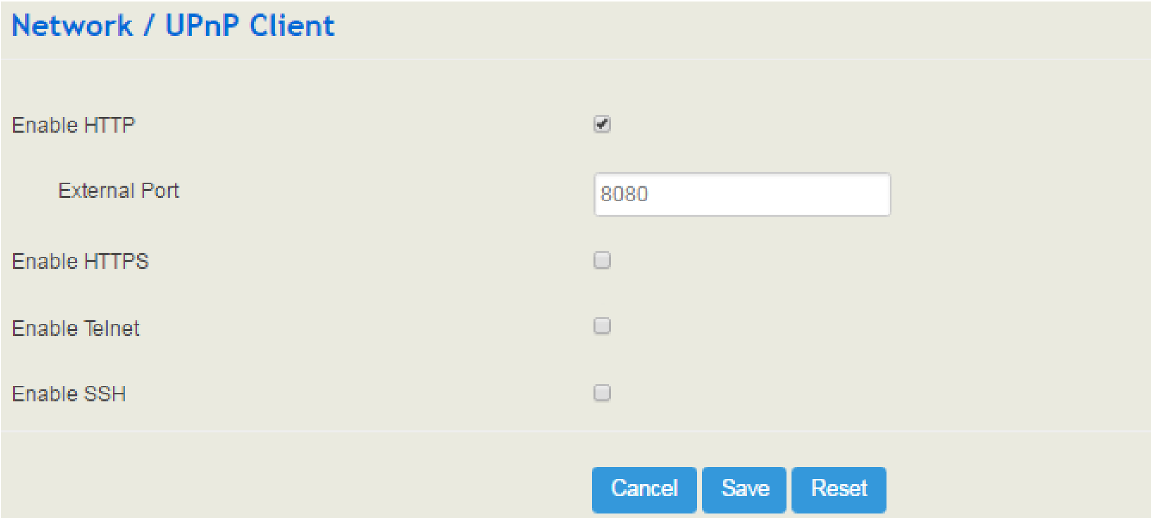
Name	The name of the static route
Target IP	The destination IP address of the static route
Netmask	The netmask of the static route, default: 255.255.255.0
Gateway	The IP address of the outbound gateway of the static route
Interface	The outbound interface of the static route, namely WAN port or LAN port
Status	The static route is enabled or disabled

5.4.13 UPnP Client

UC100-1V1S1O can serve as an UPnP client. When UC100-1V1S1O is deployed at a local-area network and its outbound router supports the UPnP function, you can enable the UPnP function on the **Network → UPnP** Client interface of the UC100-1V1S1O device, and thus its outbound router is notified by the UPnP protocol to carry out port mapping.

For example, the public IP address of outbound router is 172.16.20.12, and the external port configured on UC100-1V1S1O is 8080. When UPnP HTTP is enabled, the router will create a port mapping from external HTTP port 8080 to intranet HTTP port 80, and thus clients in public network can visit the UC100-1V1S1O gateway which is in local-area network through entering 72.16.20.12:8080.

Figure 5-45 UPnP Client



5.4.14 VPN Client

VPN（Virtual Private Network）is a network technology that creates a secure remote network connection over a public network through encrypted tunnel and conversion of data's destination address. UC100-1V1S1O can serve as a VPN client to connect with VPN server.

UC100-1V1S1O supports the following VPN protocols:

Layer 2 Tunneling Protocol (L2TP) is a protocol used to package data of PPP link layer and transmit the data between two sites over the Internet through a tunnel.

Point-To-Point Tunneling Protocol (PPTP) is another tunneling protocol used to connect a remote client to a private server over the Internet. PPTP is an enhanced security protocol which supports VPN. And its security can be enhanced through PAP (Password Authentication Protocol) and EAP (Extensible Authentication Protocol).

OpenVPN is a kind of VPN based on the application layer of OpenSSL. It allows VPN clients to use a sahred key, certificates or username/password to authenticate themselves.

PPTP： UC100-1V1S1O works as a PPTP client and is connected to PPTP server.

Figure 5-46 UC100 Works as PPTP Client

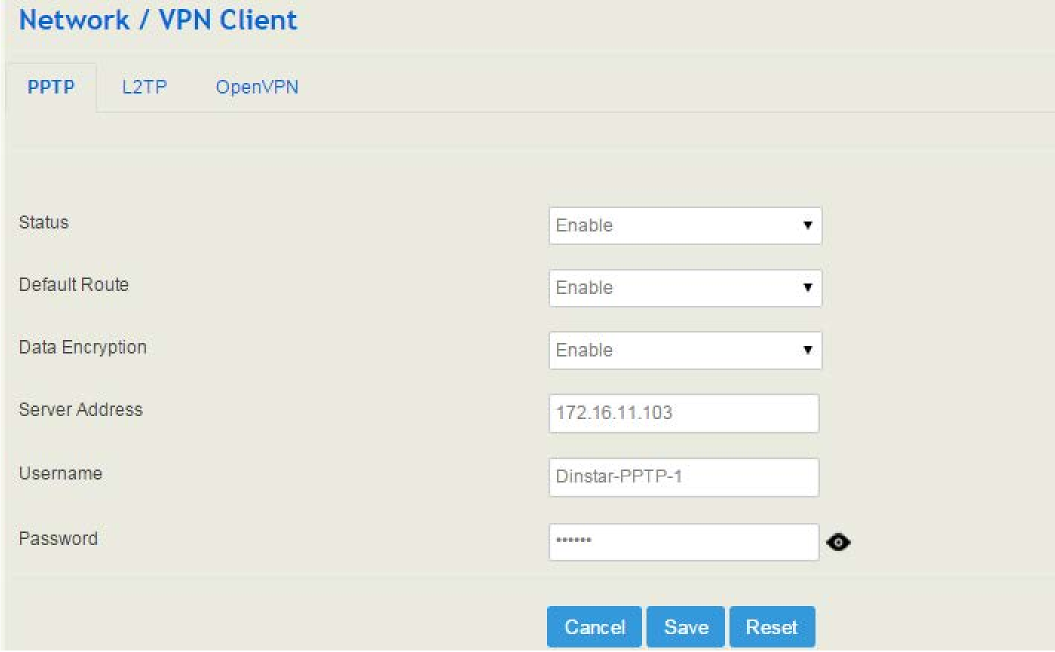


Table 5-17 Explanation of Parameters for PPTP Client

Status	Whether to enable the PPTP client function (UC100-1V1S1O works as PPTP client)
Default Route	Whether to enable default route; If default route is enabled, data are transmitted between PPTP client and PPTP server through VPN route; if it is not enabled, data are transmitted between PPTP client and PPTP server through network's outbound route.
Data Encryption	Whether to encrypt data during data transmission
Server Address	The IP address of the PPTP server that assigns account to PPTP client
Username	The username of the account assigned by PPTP server to PPTP client
Password	The password of the account assigned by PPTP server to PPTP client

L2TP: UC100-1V1S1O works as a L2TP client and is connected to L2TP server.

Figure 5-47 UC100 Works as L2TP Client

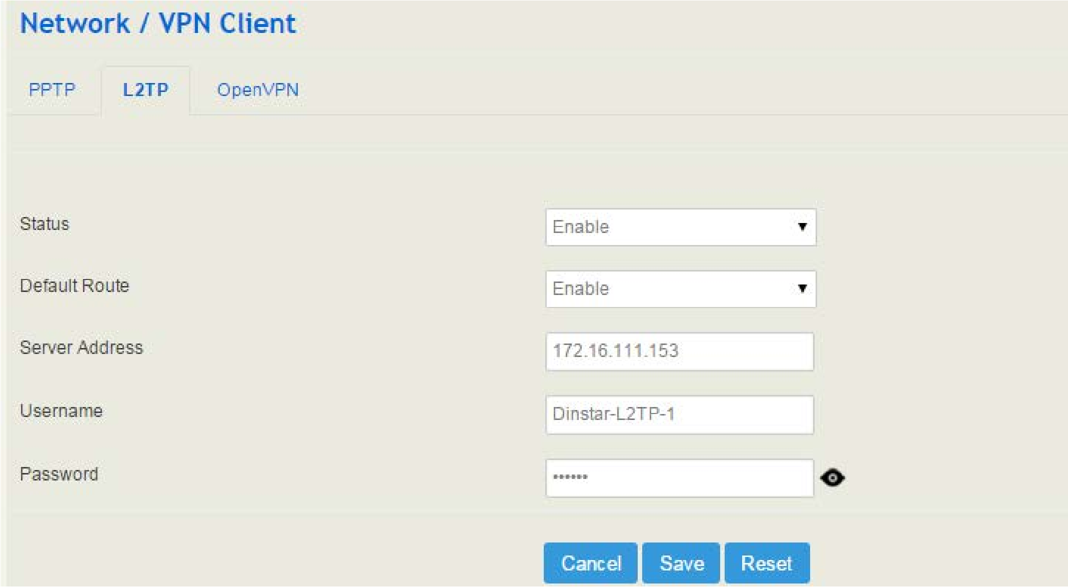
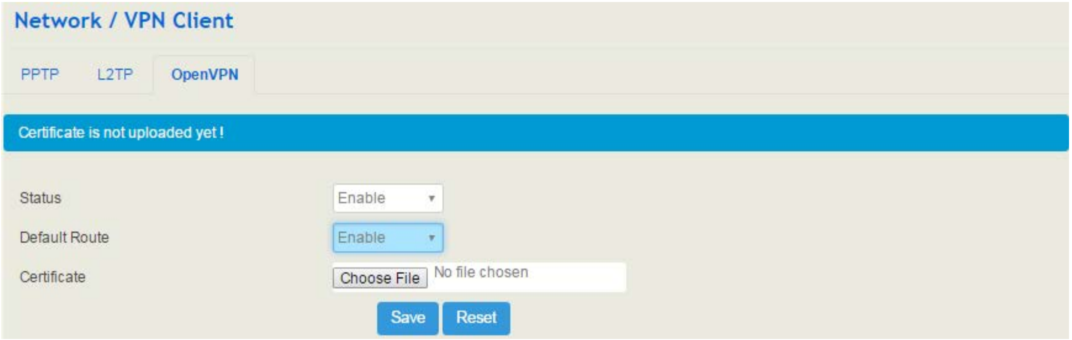


Table 5-18 Explanation of Parameters for L2TP Client

Status	Whether to enable the L2TP client function (UC100-1V1S1O works as L2TP client)
Default Route	Whether to enable default route; If default route is enabled, data are transmitted between L2TP client and L2TP server through VPN route; if it is not enabled, data are transmitted between L2TP client and L2TP server through network's outbound route.
Data Encryption	Whether to encrypt data during data transmission
Server Address	The IP address of the L2TP server that assigns account to L2TP client
Username	The username of the account assigned by L2TP server to L2TP client
Password	The password of the account assigned by L2TP server to L2TP client

OpenVPN: Allow a single point of VPN to use certificates authenticate itself.

Figure 5-48 OpenVPN

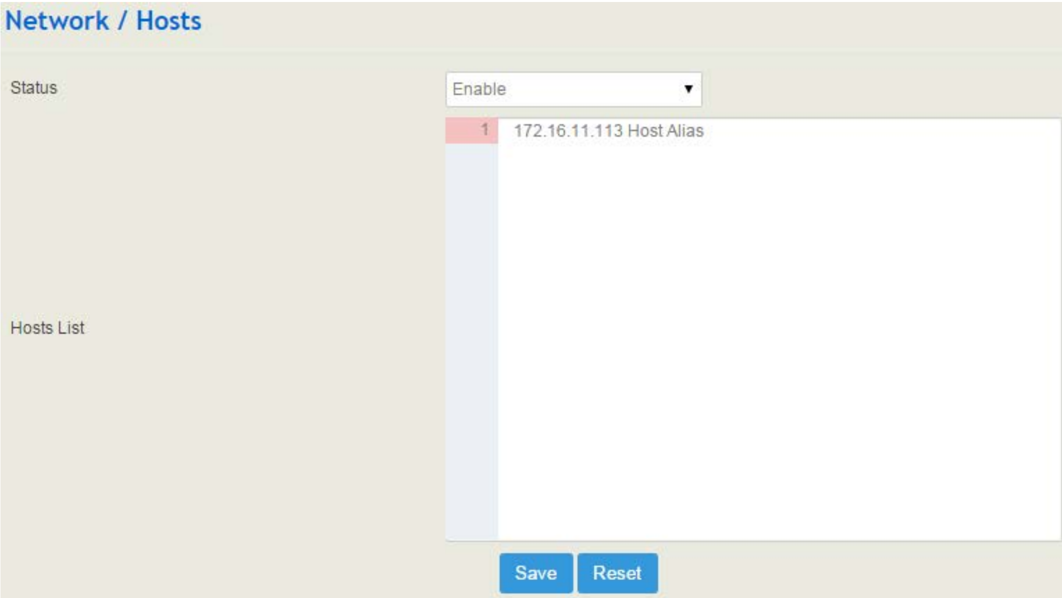


5.4.15 Hosts

On the **Network → Hosts** interface, you can add a host file. After enabling the hosts file, you can visit the corresponding host by inputting the alias or domain name of the host. The format of the hosts file is as follows: IP address host alias/domain name.

The hosts file contains the mapping relationship between IP address and host name/alias /domain name. And the mapping relationship allows quick and convenient access to the host.

Figure 5-49 Enable Hosts File



5.5 Profile

The Profile menu includes the following sub-menus: SIP, FXS/FXO, Codec, Number, Time, Manipulation and Dalplan.

5.5.1 SIP

On the **Profile → SIP** interface, you can set SIP information such as listening port, which will be used in extension and trunk. Multiple SIP profiles can be configured for one UC100-1V1S1O device, so you can choose different SIP profiles according to different needs.

Figure 5-50 Configure SIP Profile

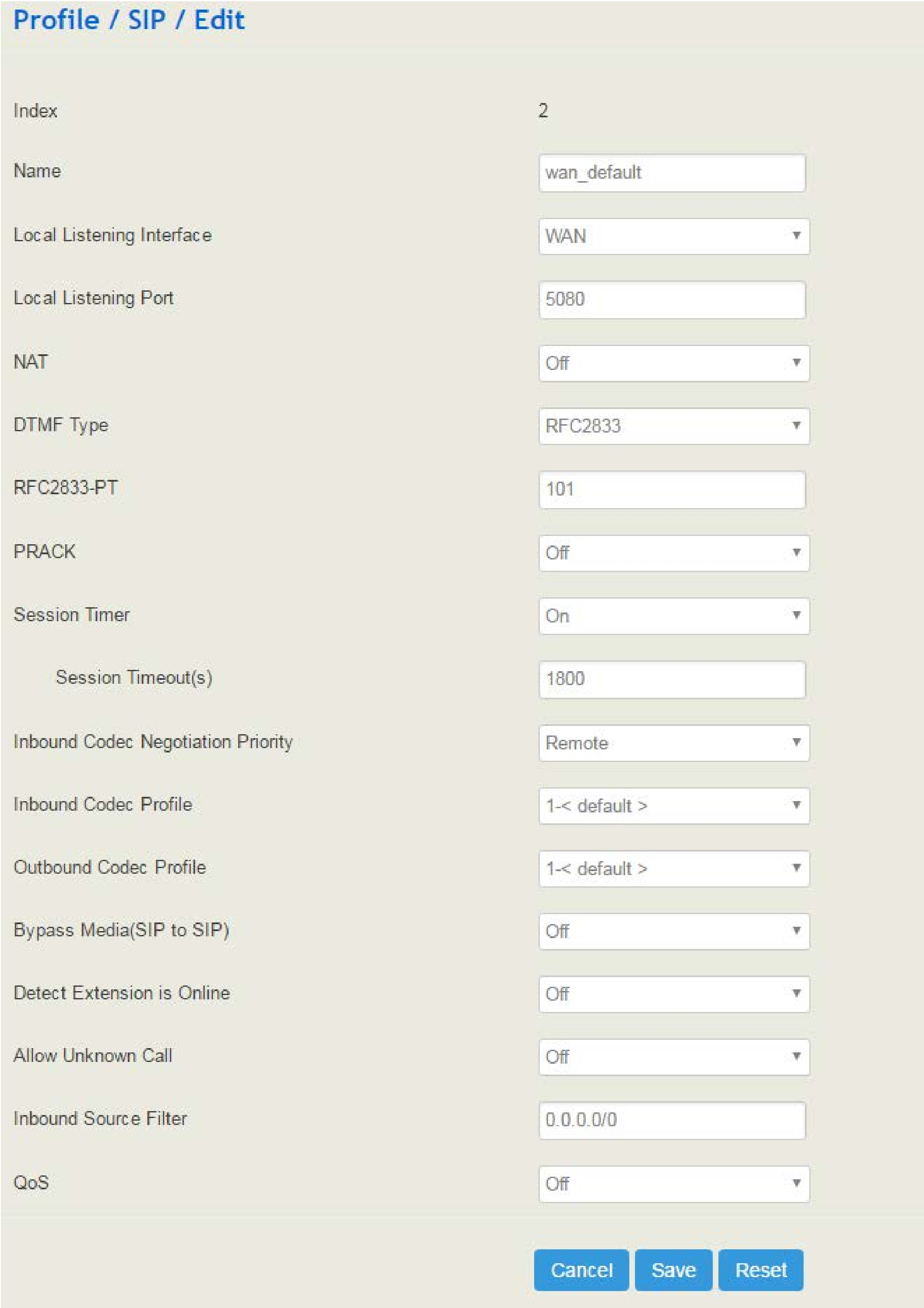


Table 5-19 Explanation of Parameters for SIP Profile

Name	The name of the SIP profile
Local Listening Interface	The local listening interface of this SIP profile. It can be WAN port, LAN port, Open VPN, L2TP and PPTP.

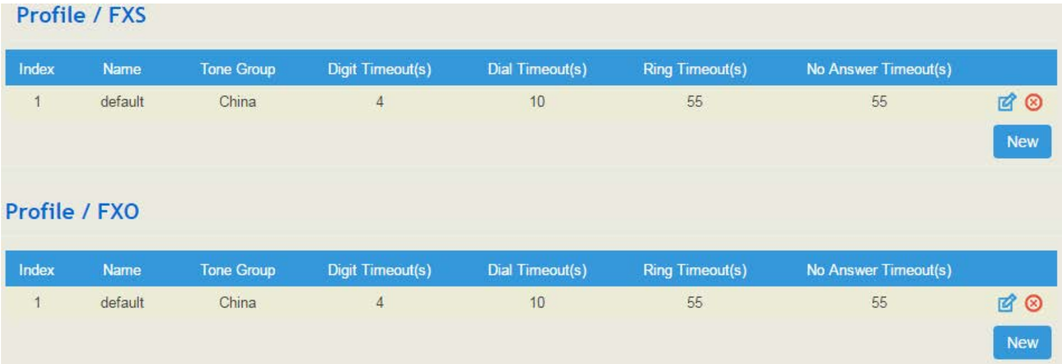
	If the SIP profile is used by a SIP trunk, the interface filled in here is the listening port for the SIP trunk.
Local Listening Port	The local listening port of this SIP profile. If the SIP profile is used by a SIP trunk, the port filled in here is the listening port for the SIP trunk.
NAT	Starting NAT can speak on different networks, including four:uPNP/NAT-PMP、IP Address、Stun、DDNS
DTMF Type	DTMF is short for Dual Tone Multi Frequency There are three DTMF modes, including SIP Info, INBAND, RFC2833
RFC2833-PT	RFC2833 payload coding
PRACK	Provisional Response ACKnowledgement
Session Timeout	The validity period of a SIP session. When a SIP session times out, an invite message needs to be sent to refresh the session, otherwise, the session ends; It is 1800 seconds by default
Inbound Codec Negotiation Priority	To take the remote device or the local device as priority for inbound codec negotiation Assume local device supports PCMA, PCMU, G.729 and G.723, while the remote device supports G.723 and G.729 If remote device is taken as codec negotiation priority, G.723 will be the codec mode, since the remote device supports G.723 and G.729 and G.723 is prior to G.729
Inbound Codec Profile	The codec supported by SIP for inbound calls
Outbound Codec Profile	The codec supported by SIP for outbound calls
Bypass Media(SIP to SIP)	Whether or not to allow SIP to communicate with the server directly
Detect Extension is Online	Whether to detect the SIP extension using this SIP profile is online or not
Allow Unknown Call	If this function is enabled, incoming calls from unknown sources are allowed. Unknown sources are those IP addresses that do not fall into the source range configured for SIP trunks or SIP extensions

Inbound Source Filter	The source of inbound calls, which is allowed. It can be an IP address or a network segment. If it is a network segment, the format is 172.16.0.0/16 or 172.16.0.0/255.255.0.0, which means calls from the network segment of 172.16 is allowed to come in. 0.0.0.0 means calls of any source is allowed to come in
QoS	Whether to enable QoS. QoS is a technology used to solve network delay or congestion

5.5.2 **FXS/FXO**

On the **Profile → FXS/FXO** interface, you can configure the driving parameters of FXS port and FXO port, including tone standard, dial timeout, ring timeout, hook-flash detection, DTMF parameters, CID-related parameters, impedance, dialplan and so on.

Figure 5-51 FXS/FXO Profile



Click , and corresponding configuration interface will pop up.

Figure 5-52 Configure FXS Parameters

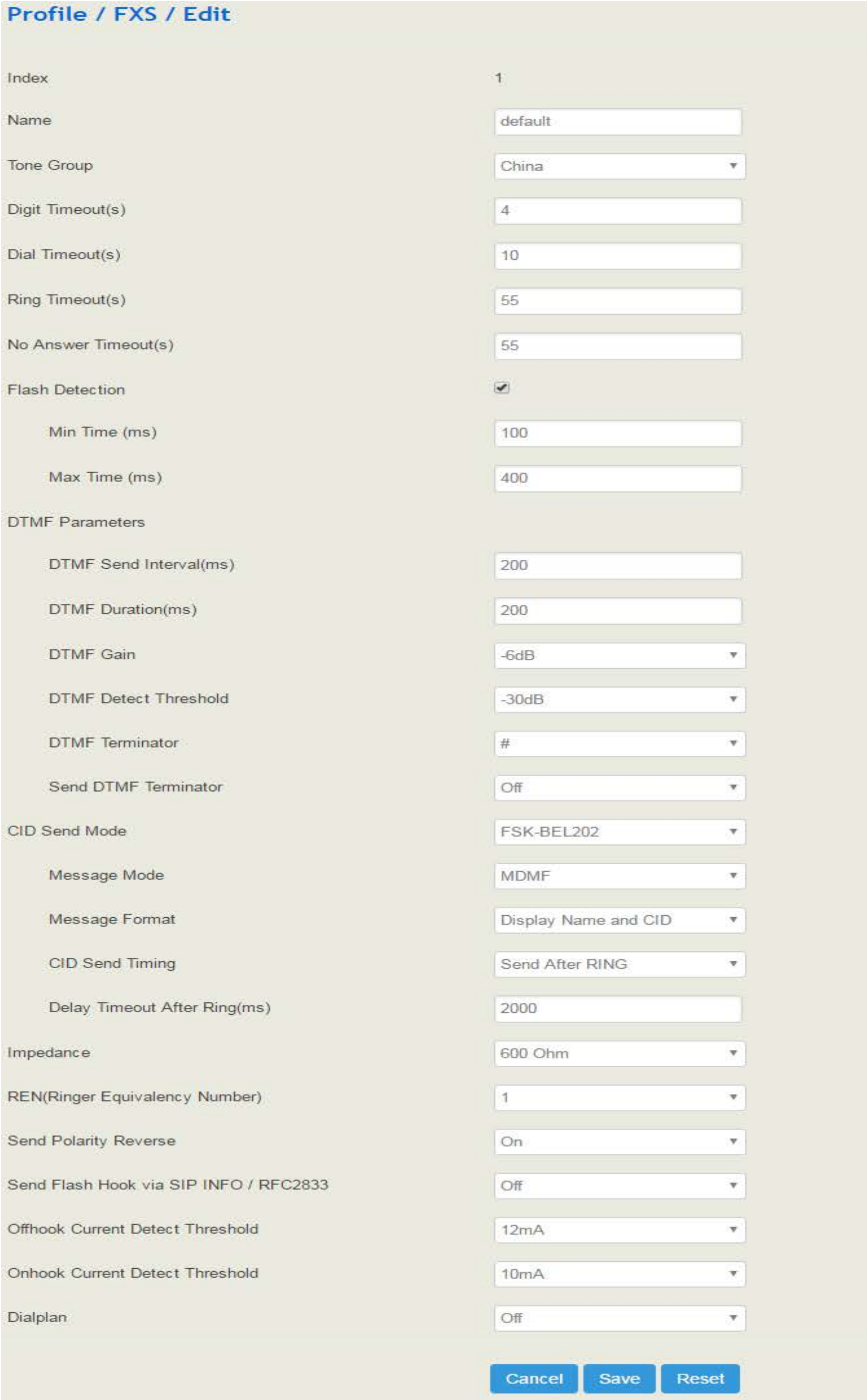


Table 5-20 Explanation of FXS Parameters

Name	The name of this FXS profile
Tone Group	The national standard of dialing tone, busy tone and ring tone; default value is China
Digit Timeout (s)	The timeout value for dialing a digit of a telephone number; When the time of dialing a digit exceeds this value, the system will think the dialing has completed; Default value is 4 seconds
Dial Timeout (s)	The timeout value for dialing the first telephone number after off-hook; Default value is 10 seconds
Ring Timeout (s)	The timeout value for the ringing of the analog phones of the FXS port when there are incoming calls
No Answer Timeout (s)	The timeout value for ending a call which goes out through the FXS port, when nobody answers the call.
Flash Detection	Whether to enable flash-hook detection; If flash detection is not enabled, the press on flash-hook will be ignored and won't be processed.
Min Time(ms)/ Max Time(ms)	Min Time: when flash-hook detection is enabled, if the time of the press on the flash-hook is less than this minimum time, the press will be ignored and won't be processed. Max Time: when flash-hook detection is enabled, if the time of the press on the flash-hook is longer than this maximum time, the phone will be hanged up.
DTMF Send Interval(ms)	The minimum interval between the sending of two DTMF tone DTMF: Dual Tone Multi Frequency
DTMF Gain	Signal gain of DTMF
DTMF Duration (ms)	The minimum duration of a DTMF tone
DTMF Detect Threshold	The threshold for the device to detect DTMF
DTMF Teminator	The terminator for ending DTMF detection. It means when the terminator is detected, the system will think the dialing is completed and begin to process call.
Send DTMF Terminator	Whether to send DTMF terminator
CID Send Mode	The modes of sending CID to the called phone when there are incoming calls, including FSK and DTMF; FSK: Frequency-shift keying; CID: Caller ID
Message Mode	The message modes to display caller information, including SDMF and MDMF

Message Format	The message formats to display caller information, including Display Name and CID, Only display Name, Only display CID
Send CID Before Ring	If it is enabled, the CID will be shown before ringing; otherwise, CID will be displayed after ringing
Send CID After Ring(ms)	If it is enabled, the CID will be shown after ringing; otherwise, CID will be displayed before ringing
Delay Timeout After Ring (ms)	The maximum interval between ringing and displaying of CID
Impedance	The impedance （SLIC） matched with analog phones
REN(Ringer Equivalency Number)	The equivalent number of ringing bells is used to determine how many devices can be connected by telephone lines, supporting 1-4 stations
Polarity Reverse	If polarity reverse is on, call tolls will be calculated based on the changes in voltage. If polarity reverse is off, you need to set the time for offhook detect and call tolls will be calculated starting from the set time.
Send Flash Hook via SIP INFO	If this parameter is on, signal of flash-hook is sent via SIP INFO
Offhook Current Detect Threshold	According the set of current threshold to check the machine's status
Onhook Current Detect Threshold	According the set of current threshold to check the status of the phone machine
Dialplan	The rules for dialing. The UC100-1G1S1O device supports regular expression. Please make reference to **Profile → Dianplan** section.

Figure 5-53 Configure FXO Parameters

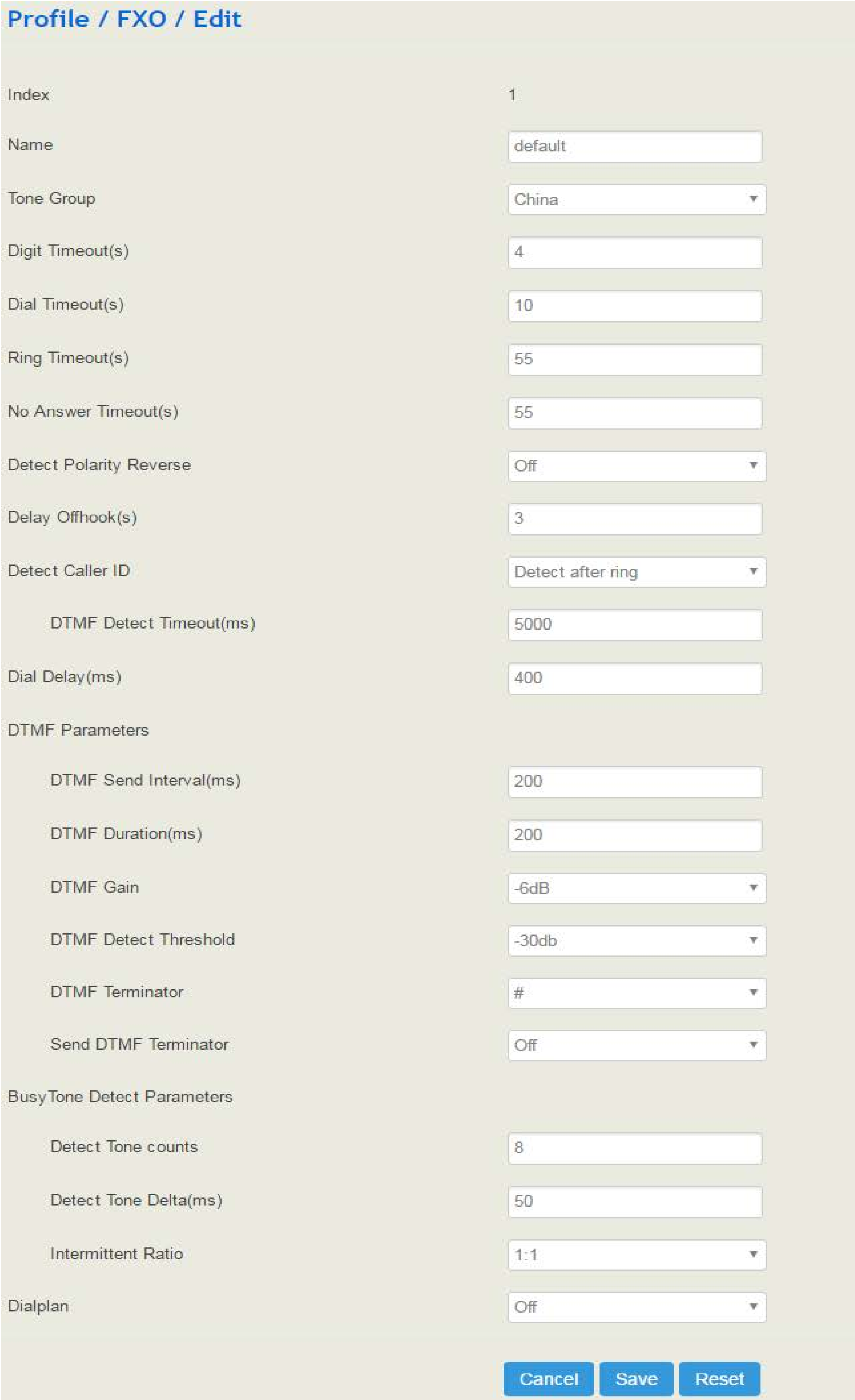


Table 5-21 Explanation of FXO Parameters

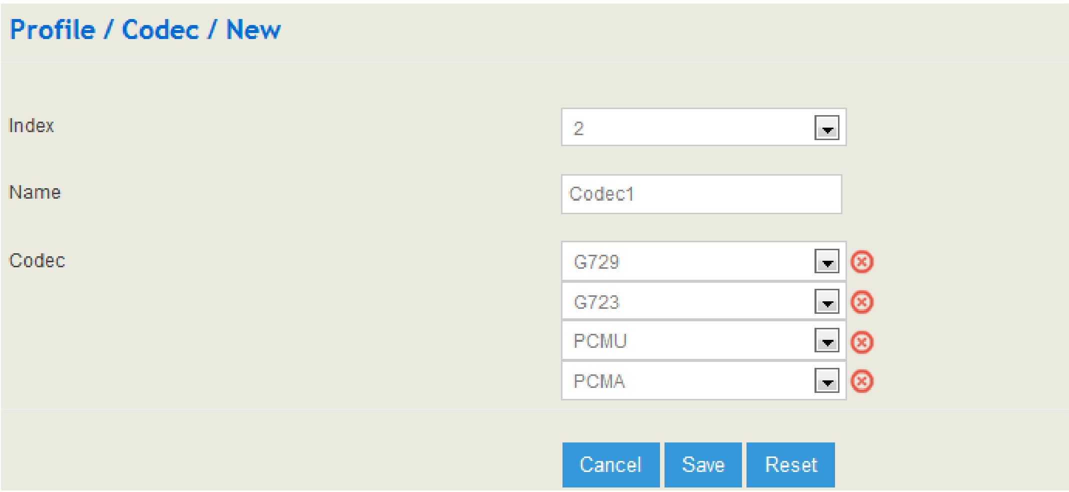
Name	The name of this FXO profile
Tone Group	The national standard of dialing tone, busy tone and ring tone; default value is China
Digit Timeout (s)	The timeout value for dialing a digit of a telephone number; When the time of dialing a digit exceeds this value, the system will think the dialing has completed; Default value is 4 seconds
Dial Timeout (s)	The timeout value for dialing the first telephone number after off-hook; Default value is 10 seconds
Ring Timeout (s)	The timeout value for the ringing of the analog phones of the FXS port when there are incoming calls
No Answer Timeout (s)	The timeout value for ending a call which goes out through the FXS port, when nobody answers the call.
Detect Polarity Reverse	Whether to enable 'detect polarity reverse'. If 'detect polarity reverse' is on, call tolls will be calculated based on the changes in voltage. If 'detect polarity reverse' is off, you need to set the time for offhook delay and call tolls will be calculated starting from the set time.
Delay Offhook(s)	The user can set how long to send the pick signal
Detect Caller ID	Detect before ring: the CID will be shown before ringing; otherwise, CID will be displayed after ringing; Detect after ring: the CID will be shown after ringing; otherwise, CID will be displayed before ringing Off: the CID will not be shown
DTMF Detect Timeout(s)	The timeout value to detect CID (in DTMF format)
Dial Delay(ms)	The user can set FXO dial time
DTMF Send Interval(ms)	The minimum interval between the sending of two DTMF tone DTMF: Dual Tone Multi Frequency
DTMF Gain	Signal gain of DTMF
DTMF Duration (ms)	The minimum duration of a DTMF tone
DTMF Detect Threshold	The threshold for the device to detect DTMF
DTMF Teminator	The terminator for ending DTMF detection. It means when the terminator is detected, the system will think the dialing is completed and begin to process call.

Send DTMF Terminator	Whether to send DTMF terminator
Detect Tone counts	Set the number of busy notes to check
Detect Tone Delta	Set the error size to check the busy tone
Intermittent Ratio	The intermittent ratio to detect busy tone
Dialplan	The rules for dialing. The UC100-1G1S1O device supports regular expression. Please make reference to **Profile → Dianplan** section.

5.5.3 Codec

UC100-1V1S1O supports four codec modes, including G729, G723, PCMU and PCMA. You can adjust the priority of these four modes according to you needs.

Figure 5-54 Add or Delect Codec Profile



: Edit codec profile.

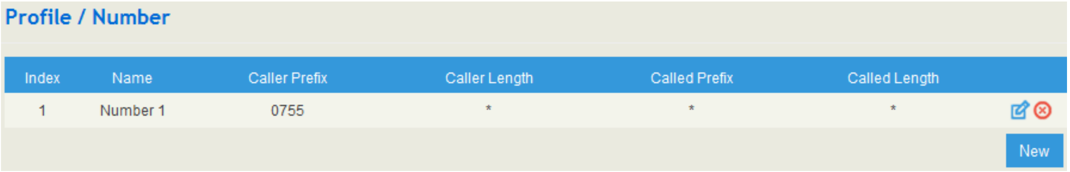
: Delete the corresponding codec profile or a codec mode.

: Create a new codec profile.

5.5.4 Number

On the **Profile →Number** interface, you can set a prefix for calling numbers or called numbers. When the prefix of a calling number or a called number matches the set prefix, the call will be passed to choose a route.

Figure 5-55 Number Profile



: Edit number profile.

: Delete the corresponding number profile

Click , and you will see the following interface:

Figure 5-56 Create Number Profile

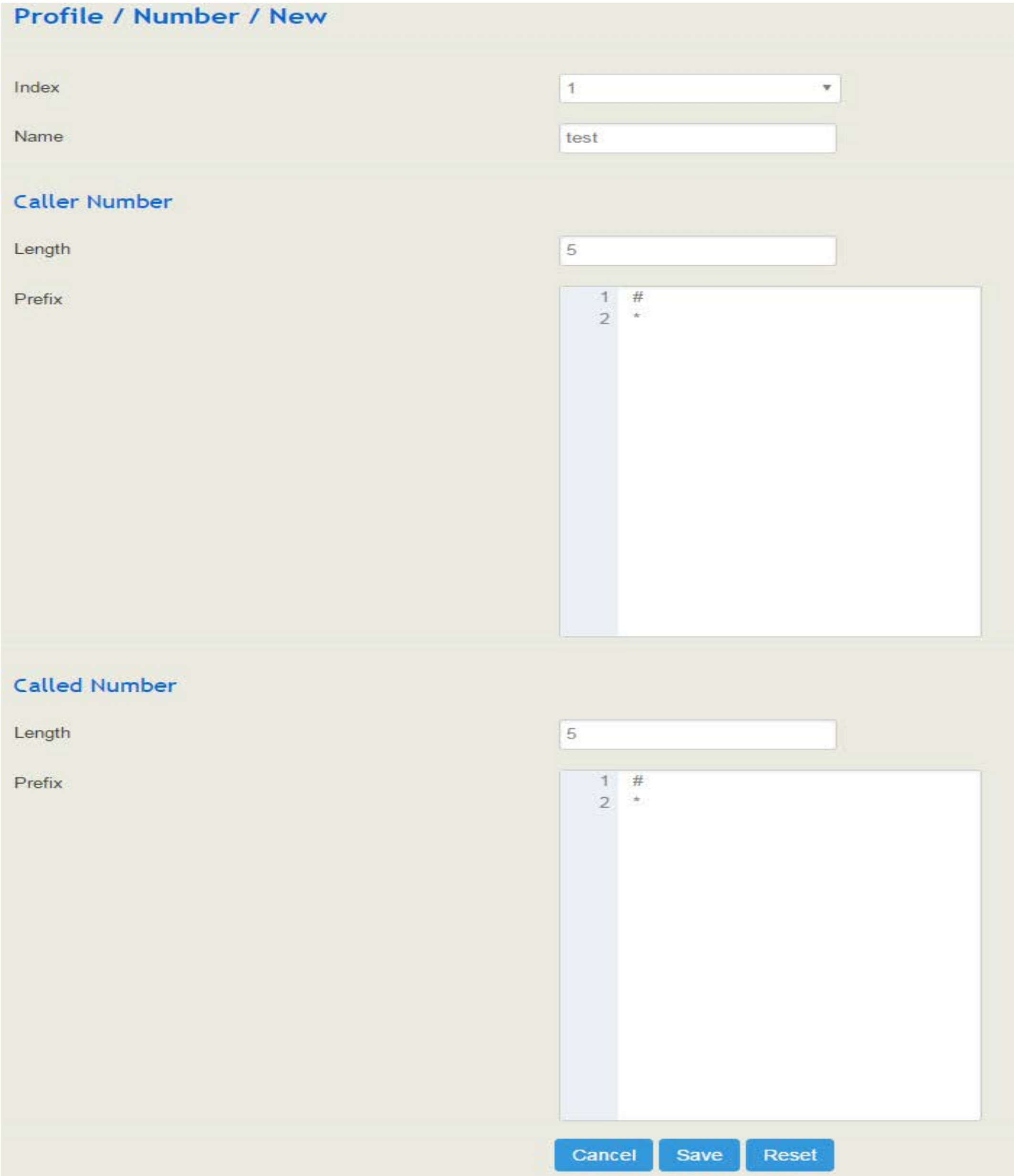


Table 5-22 Explanation of Number Parameters

Name	The name of the number profile
Prefix of Caller Number	The prefix of the calling number. It supports multiple prefixes, multiple rules for "or" relationships .It supports regular expression
Prefix of Called Number	The prefix of the called number. It supports regular expression.It Supports multiple prefixes, multiple rules for "or" relationships.
Length	The length of the calling number or called number. For example, ： 4|6|7 means the calling number or called number must be 4 digits, 6 digits or 7 digits except the prefix

Regex (Regular Expression) Syntax

Table 5-3 Explanation of frequently-used metacharacters in Regex

^	Matches the starting position in a number string. For example, ^134 matches the numbers starting with 134
$	Matches the ending position of a string. For example, 2$ matches the numbers ending with 2.
|	Separates alternate possibilities. For example, 2|3|4 means 2,3or 4.
\	Marks the next character as a special character, a literal, a backreference, or an octal escape
[ ]	Matches a single character that is contained within the bracket. For example, [123] matches 1, 2, or 3. [0-9] matches any digit from "0" to "9".
[^]	Matches any one character except those enclosed in [ ]. For example, [^9] matches any character except 9.
.	Matches any single character except the newline character. For example, 3.4 matches 314, 324, 334, 344.
?	Indicates there is zero or one of the preceding element. For example, colou?r matches both color and colour
*	Indicates there is zero or more of the preceding element. For example, ab*c matches ac, abc, abbc, abbbc, and so on.
+	Indicates there is one or more of the preceding element. For example, ab+c matches abc, abbc, abbbc, and so on, but not ac
\d	Mark any digit, equal to [0-9]
\D	Mark any character that is not a digit, equal to [^0-9]
\s	Mark any blank character such as a space or a tab.
\S	Mark any character that is not a blank character

Examples:

^0755	Matches the phone numbers with starting digits of 0755.
^0755|^8899|^0110	Matches the phone numbers with starting digits of 0755, 8899 or 0110.
^[1][358][0-9]{9}$	Matches the phone numbers with the first digit as 1, the second digit as 3, 5 or 8, the left nine digits as any of 0 to 9.

Note: the matching of number prefix also supports some digits that are not conform to the format of regular expression. For example, 0755 matches the numbers starting with 0755, and 0755|8899|0110 matches the numbers starting with 0755, 8899 or 0110.

5.5.5 Time

On the **Profile → Time** interface, you can set a time period for calls to choose routes. If the local time when a call is initiated falls into the set time period, the call will be passed to choose the corresponding route.

Click the **New** button, and you will see the following interface:

Figure 5-57 CreateTime Profile

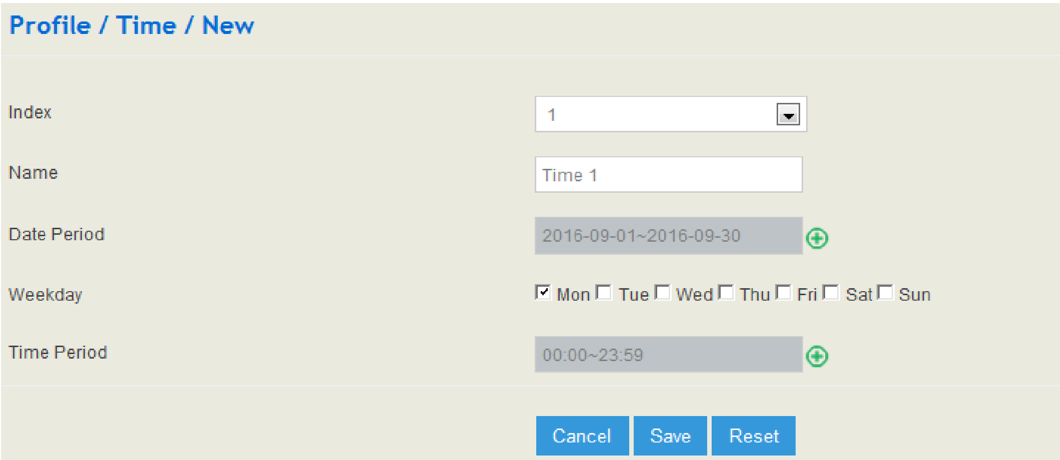


Table 5-23 Explanation of Time Parameters

Name	The name of the number profile
Date Period	Configure the starting date and ending date of a period : Add a date period : Delete a date period
Weekdate	Choose a weekdate
Time Period	Choose the starting time and ending time of a day

5.5.6 Manipulation

Number manipulation refers to the change of a called number or a caller number during calling process when the called number or the caller number matches the preset rules.

Click the **New** button, and you will see the following interface:

Figure 5-58 Create Minipulation Profile

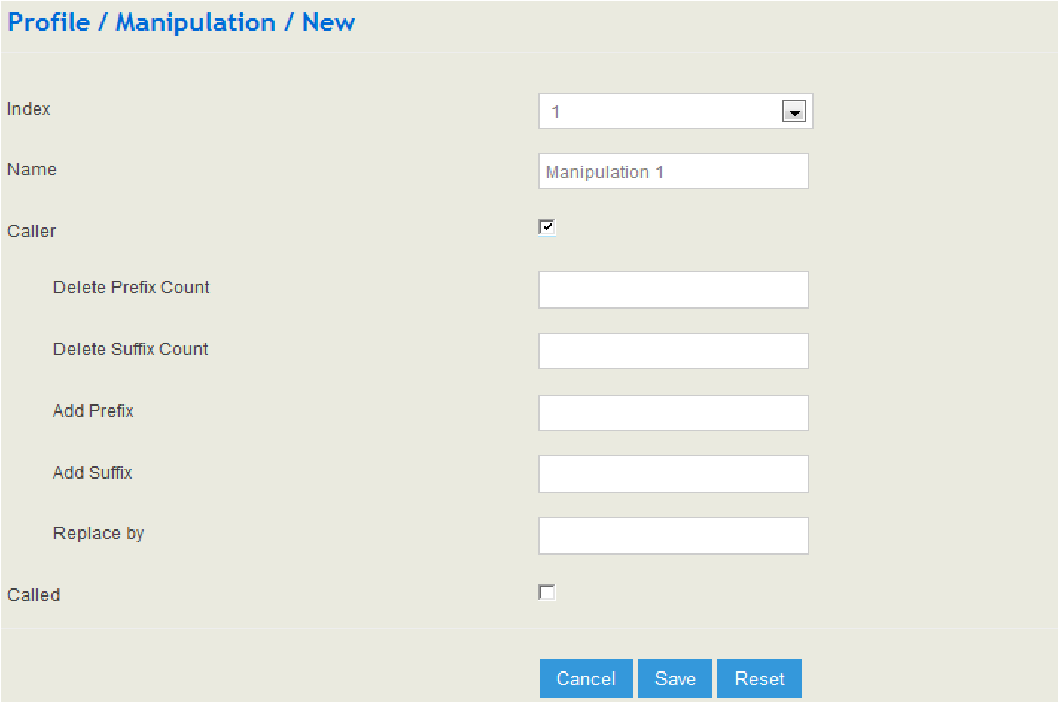


Table 5-24 Explanation of Manipulation Parameters

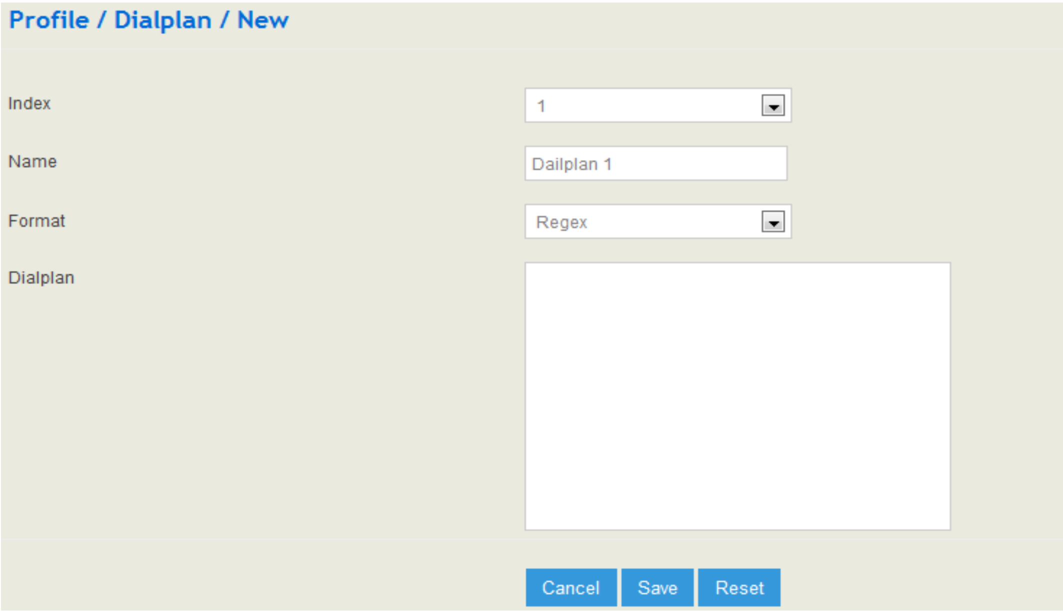
Name	The name of this manipulation profile
Delete Prefix Count	The number of digits that are deleted from the left of the caller number or calling number
Delete Suffix Count	The number of digits that are deleted from the right of the caller number or calling number
Add Prefix	The prefix added to the caller number or the calling number
Add Suffix	The suffix added to the caller number or the calling number
Replace by	The number which replace the caller number or the calling number
	If the checkbox on the right of Caller is selected, it means the caller number will be manipulated; if the checkbox on the right of Called is selected, it means the called number will be manipulated.

Note: During number manipulation, deletion rules are carried out first, followed by adding rules. If 'Replace by' has been set, deletion rules and adding rules are invalid.

5.5.7 Dialplan

Dialplan is used for number dialing of calls through FXS and FXO ports. It supports Regular Expression (Regex) and DigitMap.

Figure 5-59 Add Dialplan



Regex (Regular Expression) Syntax

<table>
<tr><td>^</td><td>Matches the starting position in a number string. For example, ^134 matches the numbers starting with 134</td></tr>
<tr><td>$</td><td>Matches the ending position of a string. For example, 2$ matches the numbers ending with 2.</td></tr>
<tr><td>|</td><td>Separates alternate possibilities. For example, 2|3|4 means 2,3or 4.</td></tr>
<tr><td>\</td><td>Marks the next character as a special character, a literal, a backreference, or an octal escape</td></tr>
<tr><td>[ ]</td><td>Matches a single character that is contained within the bracket. For example, [123] matches 1, 2, or 3. [0-9] matches any digit from "0" to "9".</td></tr>
<tr><td>[^]</td><td>Matches any one character except those enclosed in [ ]. For example, [^9] matches any character except 9.</td></tr>
<tr><td>.</td><td>Matches any single character except the newline character. For example, 3.4 matches 314, 324, 334, 344.</td></tr>
<tr><td>?</td><td>Indicates there is zero or one of the preceding element. For example, colou?r matches both color and colour</td></tr>
<tr><td>*</td><td>Indicates there is zero or more of the preceding element. For example, ab*c matches ac, abc, abbc, abbbc, and so on.</td></tr>
<tr><td>+</td><td>Indicates there is one or more of the preceding element. For</td></tr>
</table>

	example, ab+c matches abc, abbc, abbbc, and so on, but not ac
/d	Mark any digit, equal to [0-9]
/D	Mark any character that is not a digit, equal to [^0-9]
/s	Mark any blank character such as a space or a tab.
/S	Mark any character that is not a blank character

Examples of Regex Syntax:

^0755	Matches the phone numbers with starting digits of 0755.
^0755|^8899|^0110	Matches the phone numbers with starting digits of 0755, 8899 or 0110.
^[1][358][0-9]{9}$	Matches the phone numbers with the first digit as 1, the second digit as 3, 5 or 8, the left nine digits as any of 0 to 9.

DigitMap Syntax:

Supported Objects	Digit	0-9
	T	Timer
	DTMF	A digit, a timer, or one of the symbols of A, B, C, D, #, or *
Range	[ ]	One or more DTMF symbols enclosed in the [], but only one DTMF symbol can be selected
Range	()	One or more expressions enclosed the (), but only one can be selected
Separator	|	Separate expressions or DTMF symbols.
Subrange	-	Two digits separated by hyphen (-) which matches a ny digit between and including the two digits.
Wildcard	x	Matches any digit of 0 to 9
Modifiers	.	Matches 0 or more times of the preceding element
Modifiers	?	Matches 0 or 1 times of the preceding element

Examples of DigitMap Syntax

(13 | 15 | 18)xxxxxxxxx	Matches the phone numbers with stating digits as 13, 15 or 18 and the left nine digits as any of 0 to 9
[2-8] xxxxxx | 13xxxxxxxxx	Matches the phone numbers starting with any digit of 2 to 8 and the left six digits as any of 0 to 9; or matches the phone numbers starting with 13 and the left nine digits as any of 0 to 9

5.6 Extension

5.6.1 SIP

On the **Extension → SIP** interface, you can configure the SIP accounts registered in the UC100-1V1S1O by SIP clients (hereby UC100-1V1S1O is regarded as a SIP server).

Figure 5-60 Configure SIP Extension

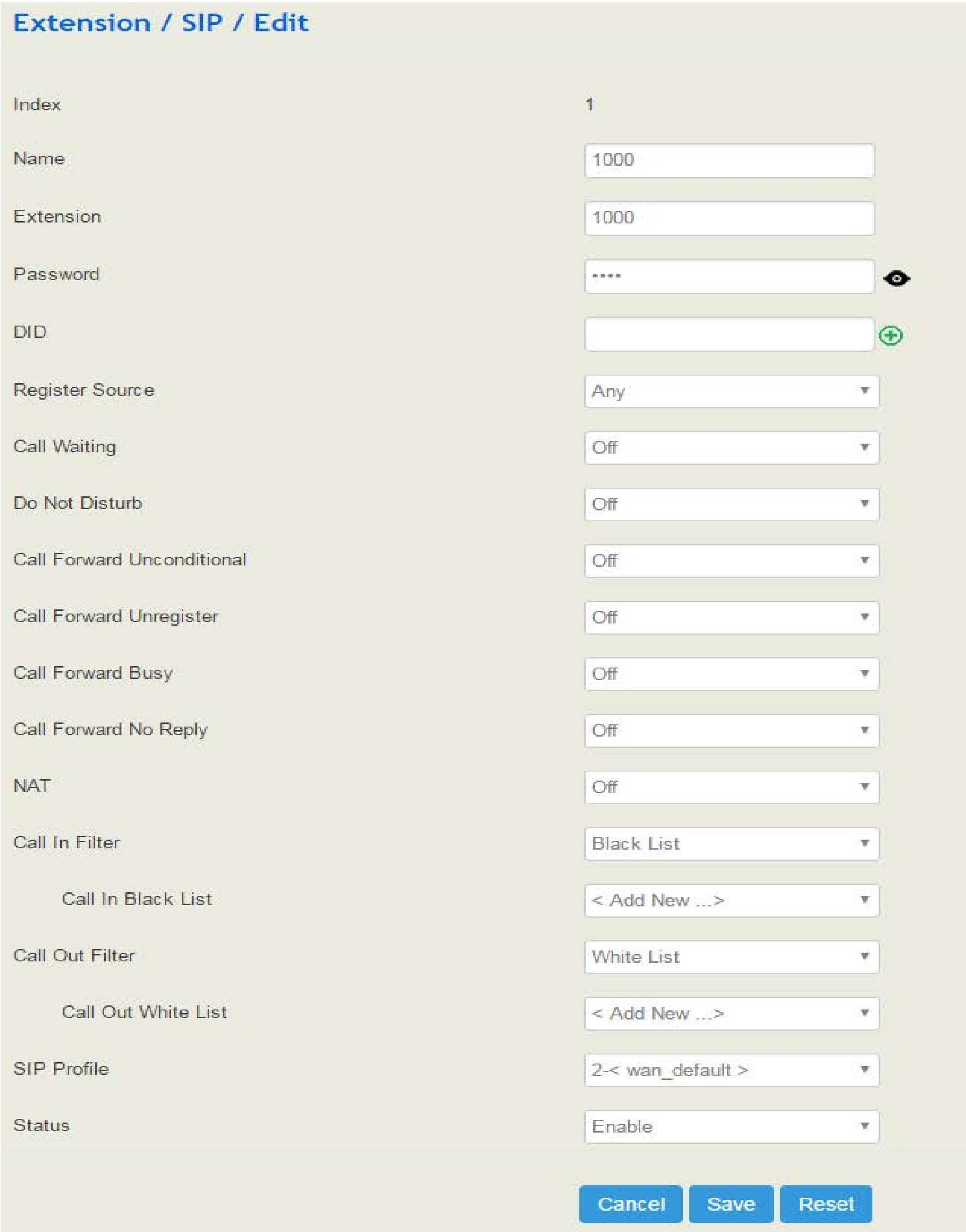


Table 5-25 Explanation of Parameters for SIP Extension

Name	The name of this SIP extension
Extension	The SIP account of the extension registered in UC100 by a SIP client
Password	The password of the SIP account registered in UC100 by a SIP client
DID	Direct Inward Dialing; if the called number is same with DID, the call will be directly forwarded to the extension, rather than choosing a route.Users can set multiple DID.
Register Source	If 'Any' is chosen, all SIP clients are allowed to register the SIP account of this extension; if 'Specified' is chosen, only the SIP client with the specified IP address or network segment is allowed to register the SIP account of this extension. For example, 172.16.0.0/16 means the register source is 172.16
Call Waiting	If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear an IVR voice.
Do Not Disturb	If 'Do Not Disturb' feature is enabled, calls cannot reach the called party.
Call Forward Unconditional	If 'Call Forward Unconditional' feature is enabled, all coming calls will be forwarded to a preset number.
Call Forward Unregister	When the SIP extension is not registered, you can transfer all the calls to the set number
Call Forward Busy	If 'Call Forward Busy' feature is enabled, new coming call will be forwarded when the corresponding local port is busy.
Call Forward No Reply	If 'Call Forward No Reply' feature is enabled, calls will be forwarded when nobody answer the calls during a specified period.
NAT	If NAT is enabled, the IP address of SIP extension in LAN will be turned into the outbound IP address of public network, thus making NAT traversal possible
Call In Filter	When you breathe in to SIP, you match the relevant filter conditions
Call Out Filter	When the SIP is called out,The filter conditions are matched
Call In Black List	The rules in the list will not take effect
Call Out White List	The rules in the list take effect
SIP Profile	The SIP profile that is selected for the extension
Status	If it is enabled, this SIP extension is registered to UC100-1G1S1O;

	Otherwise the SIP extension is not registered

5.6.2 FXS

On the **Extension → FXS** interface, you can configure the parameters of the FXS extension.

Figure 5-61 Configure Parameters of FXS Extension

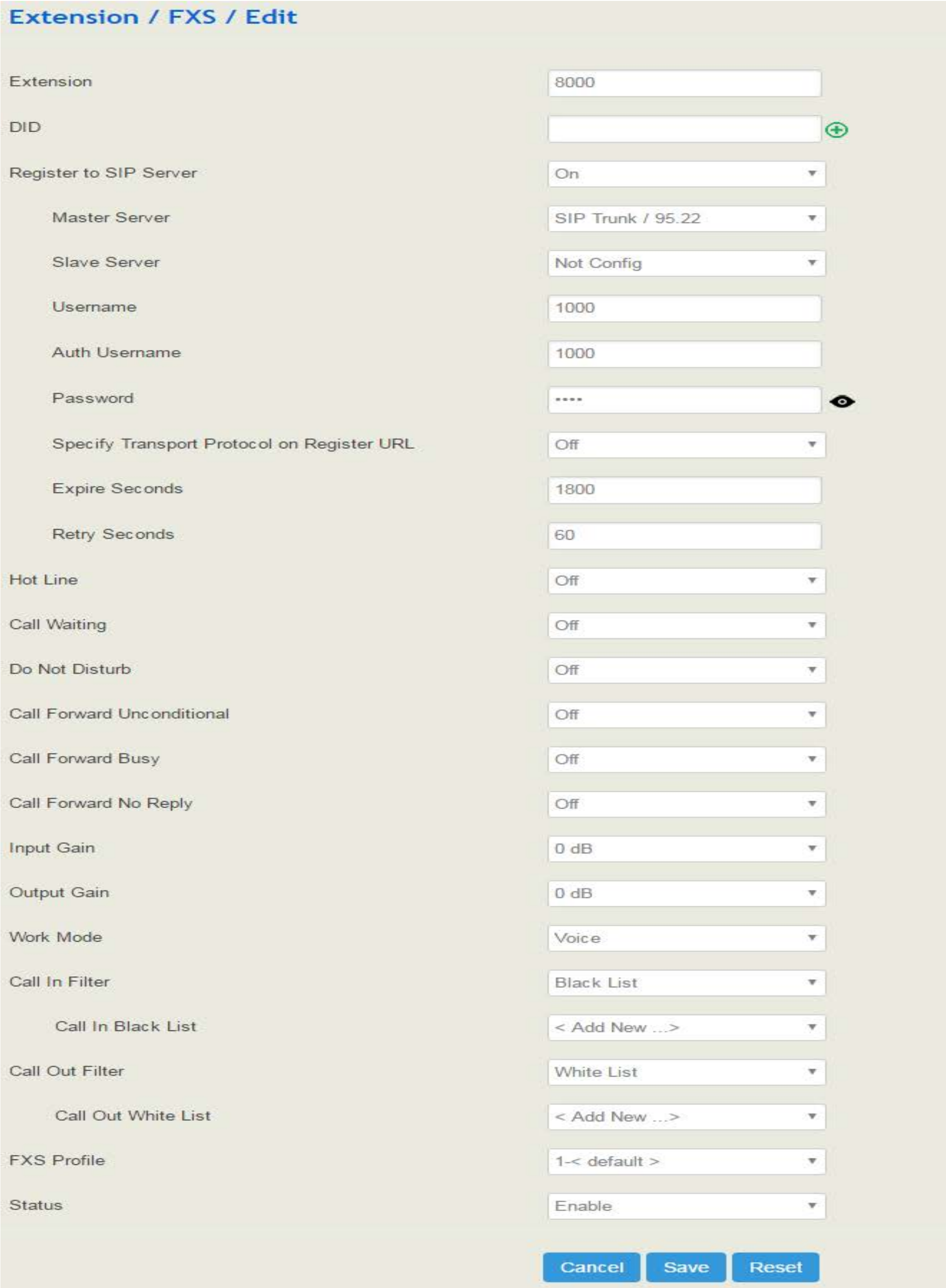


Table 5-26 Explanation of Parameters for FXS Extension

Extension	The extension account of FXS port, which is used to register
DID	Direct Inward Dialing; if the called number is same with DID, the call will be directly forwarded to the extension, rather than choosing a route.
Register to SIP Server	If it is enabled, the FXS extension account will be registered to the SIP trunk that has been set. Default is off.
Master Server	The address and port of the master SIP server; it is generally the IP address of a SIP trunk. Please make reference to Trunk → SIP section
Slave Server	The address and port of the slave SIP server
Username	User name when the FXS port account is registered
Auth Username	The username of this FXS extension account, which is used during register authentication
Password	The password of this FXS extension account, which is used during register authentication
Specify Transport Protocol on Register URL	Whether to specify transport protocol on register URL.
Expire Seconds	The validity period after the FXO trunk is registered successfully. When the time expires, the FXO trunk will send register request to the server. Default value is 1800s
Retry Seconds	When the FXO trunk fails to be registered, the interval to send register request; Default value is 60s
Hot line	If hotline is enabled, calls will directly go to the hotline number
Number	Holine number
Delay	The delay time for a call to be send out after dialing is completed
Call Waiting	If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the calling party will hear an IVR voice.
Do Not Disturb	If 'Do Not Disturb' feature is enabled, calls cannot reach the called party.
Call Forward Unconditional	If 'Call Forward Unconditional' feature is enabled, all coming calls will be forwarded to a preset number.

Call Forward Busy	If ‘Call Forward Busy’ feature is enabled, new coming call will be forwarded when the corresponding local port is busy.
Call Forward No Reply	If ‘Call Forward No Reply’ feature is enabled, calls will be forwarded when nobody answer the calls during a specified period.
Input Gain	The receiving gain of the FXS port
Output Gain	The sending gain of the FXS port
Work Mode	The working mode of the FXS port, including Voice and POS
Call In Filter	When a call is given to the FXS port of UC100-1V1S1O, the call will not be connected to the FXO port if it is in the blacklist
Call Out Filter	When a call goes out from the FXS port of UC100-1V1S1O, the call cannot go out if it is in the blacklist
Call In Black List	Calls from the number profiles in the blacklist will be blocked
Call Out White List	Calls from the number profiles in the whitelist will be not blocked
FXS Profile	The FXS profile that is selected for this FXS extension
Status	If it is on, this FXS extension can be used, otherwise, the FXS extension is unavailable.

5.6.3 Ring Group

On the **Extension → Ring Group** interface, you can group FXS extension and SIP extension(s) together and set strategy for choosing the FXS extension and which SIP extension to ring under a ring group. The ring group function is widely used in call centers.

Figure 5-62 Configure Ring Group

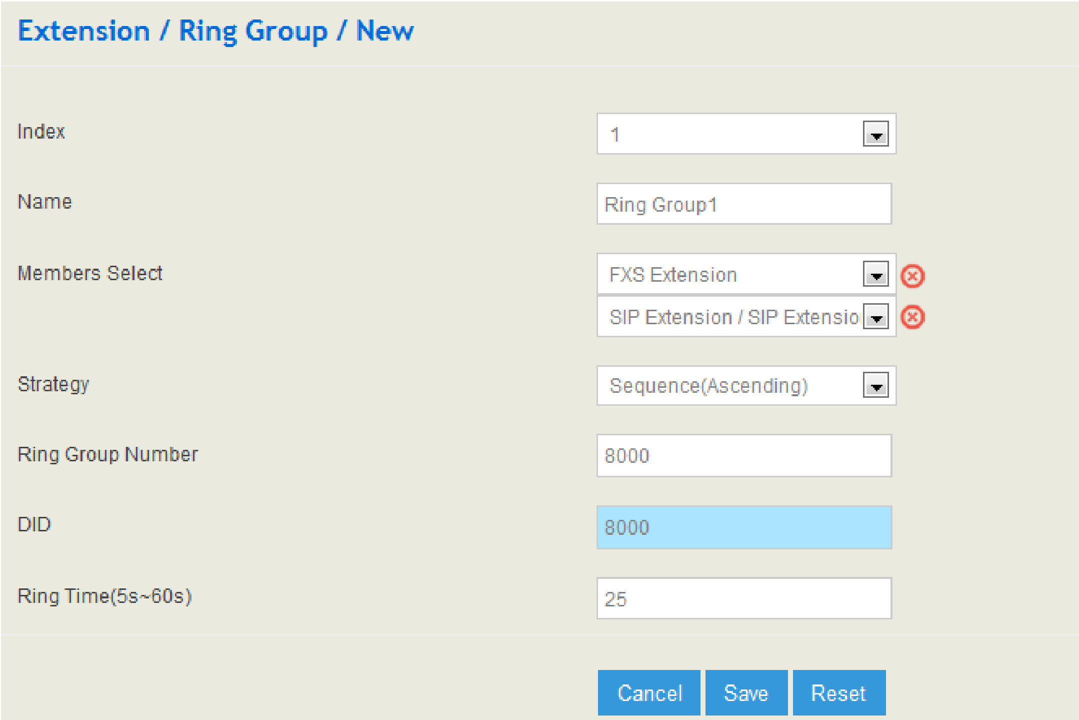


Table 5-27 Explanation of Parameters for Ring Group

Name	The name of this ring group
Members Select	Select the FXS extension and an SIP extension or several SIP extensions; : Add an extension to the ring group : Delete an extension from the ring group
Strategy	The strategies for choosing which SIP extension to ring, including Sequence (Ascending), Sequence (Cyclic Ascending), Simultaneous and Random
Ring Group Number	The number of the ring group; it is generally the same with DID.
DID	Same with Ring Group Number; it is optional to fill in
Ring Time（5-60s）	The duration of ring when there is a coming call. Range: 5s to 60s

Note: If ring group function has been set, the call forwarding function is unavailable.

5.7 Trunk

5.7.1 SIP

SIP trunk can realize the connection between UC100-1V1S1O and IPPBX or SIP servers.

Figure 5-63 Cofigure SIP Trunk

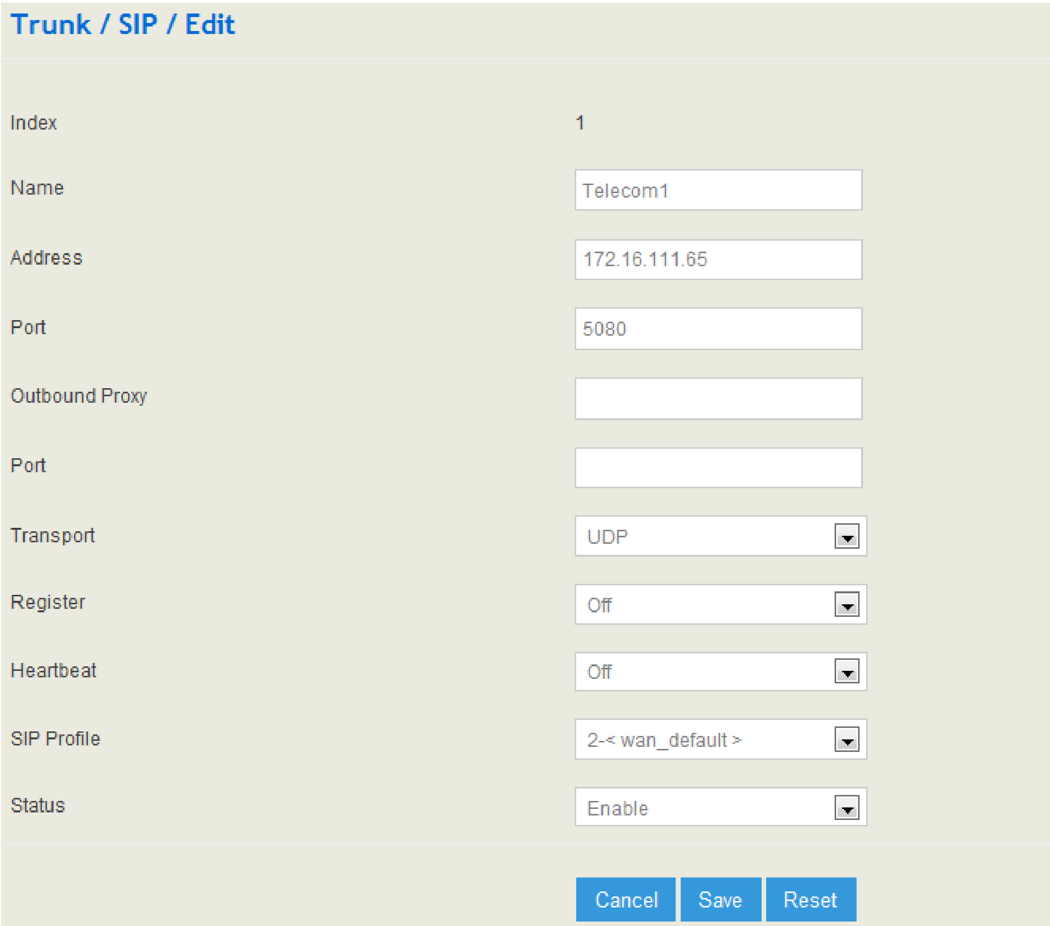


Table 5-28 Explanation of Parameters for SIP Trunk

Name	The name of the SIP trunk
Address	The IP address or domain name of the peer SIP devices or servers
Port	The SIP listening port of the peer SIP devices or servers; 5060 is the default port
Outbound Proxy	If outbound proxy is used, enter the IP address or domain name of the proxy server
Port	If outbound proxy is used, enter the listening port of the proxy server
Transport	Transport protocol: TCP or UDP
Register	If it is on, the SIP trunk will send register request to the peer device

Username	The username of this SIP trunk, it is generally a phone number
Auth Username	The username used for register authentication by this SIP trunk
Password	The password used for register authentication by this SIP trunk
From Header Username	Choose the registered username or the true caller ID for the 'from header' of the invite message when a call goes out.
Expire Seconds	The validity period after the SIP trunk is registered successfully. When the time expires, the SIP trunk will send register request to the server. Default value is 1800s
Retry Seconds	When the SIP trunk fails to be registered, the interval to send register request; Default value is 60s
Heartbeat	If heartbeat in on, heartbeat (options) messageswill be sent to examine the connection with servers; The default value is 'Off'
Heartbeat Period	The interval of sending heartbeat (options) messages
SIP Profile	he SIP profile of the SIP Trunk; make reference to Profile → SIP section
Status	If it is enabled, it means the SIP Trunk can be used; otherwise, the SIP trunk is unavailable

Note:

If UC100-1V1S1O is regarded as a terminal and intends to register to a server, you need to configure a SIP trunk connecting UC100-1V1S1O and the server, and then enable register for the SIP trunk.

If the FXS f UC100-1V1S1O intends to register to a server, you need to configure a SIP trunk connecting UC100-1V1S1O and the server, then enable register for the port and designate the SIP trunk to it.

5.7.2 FXO

FXO Trunk interconnects the PSTN with UC100-1V1S1O. Calls from the PSTN can come into the gateway and calls can go out from the gateway to search telephone numbers under the PSTN.

Different from the FXO ports of other gateways, the FXO port of UC100-1V1S1O only allows one-time dialing, which means called numbers needs to be dialed directly for calls that go out from the FXO port.

Figure 5-64 Configure FXO Trunk

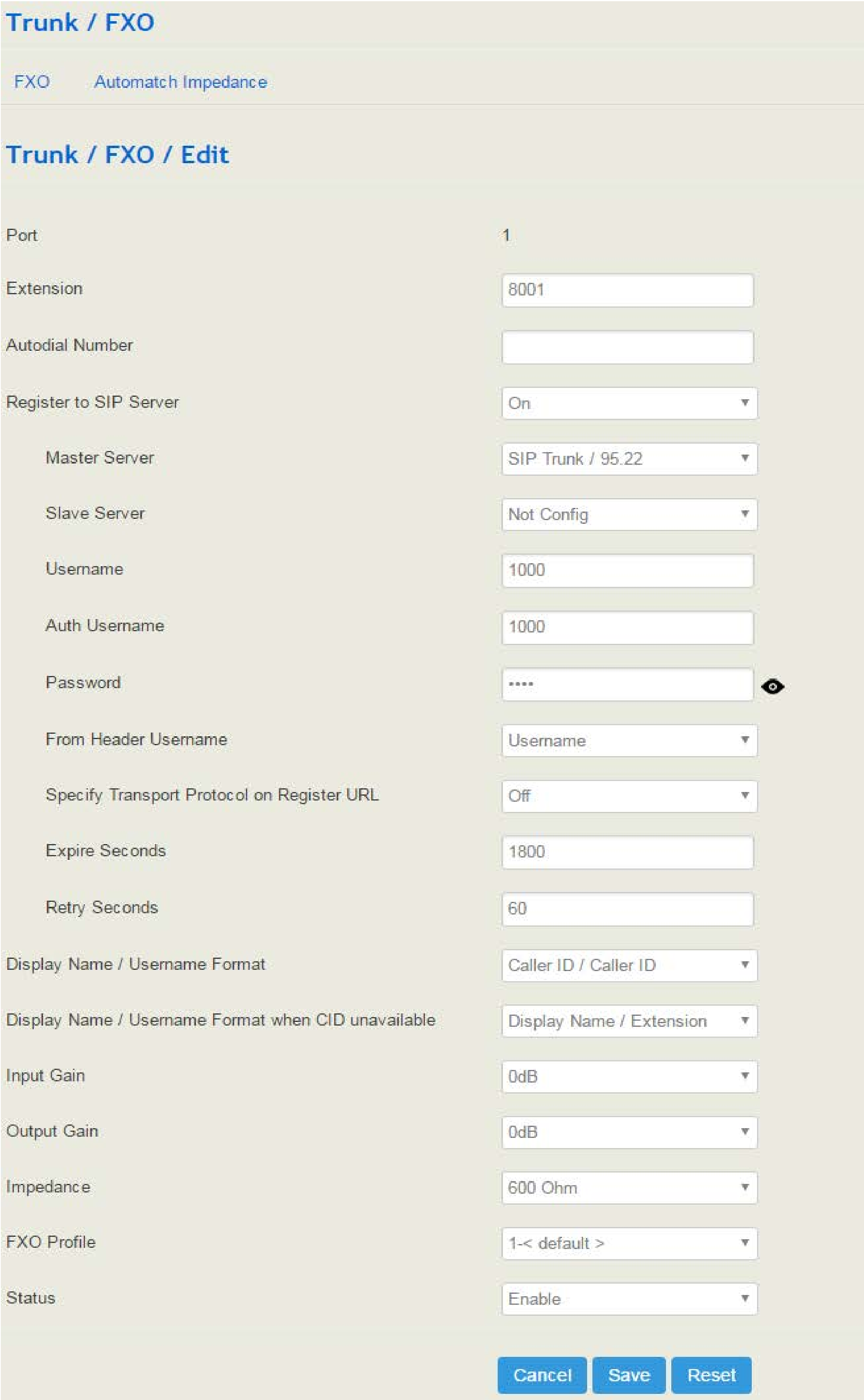


Table 5-29 Explanation of Parameters for FXO Trunk

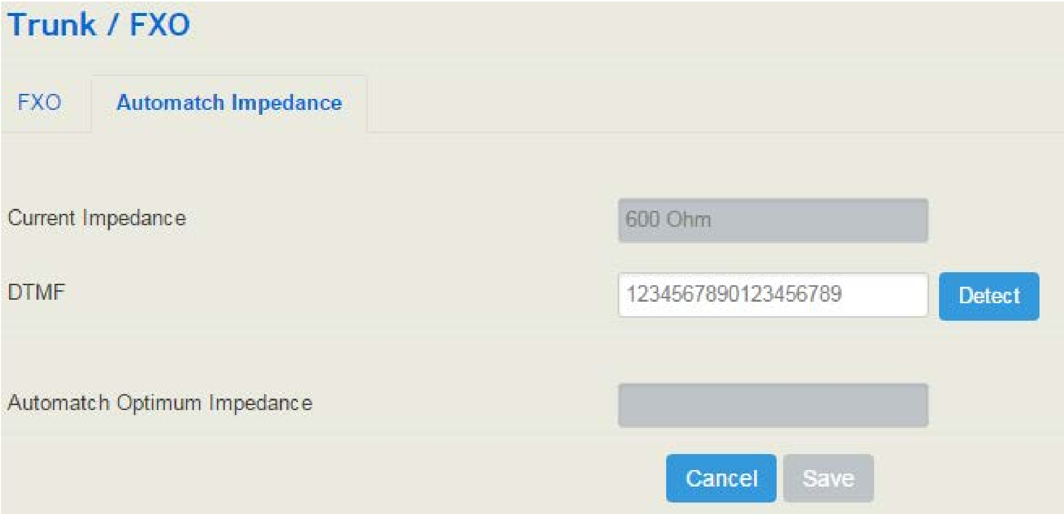
Port	The FXO portl number
Extension	The extension account of the FXO port, which is used to register
Autodial Number	The autodial number of the FXO port when there are incoming calls
Register to SIP Server	If it is enabled, the FXO trunk will be registered to the SIP trunk that has been set. Default is off.
Master Server	The address and port of the master SIP server; it is generally the IP address of a SIP trunk. Please make reference to Trunk → SIP section
Slave Server	The address and port of the slave SIP server
Username	Username of the FXO port account, used for the authentication of registration
Auth Username	The username of this FXO trunk, which is used during register authentication
Password	The password of this FXO trunk, which is used during register authentication
From Header Username	Choose the registered username or the true caller ID for the ‘from header’ of the invite message when a call goes out.
Specify Transport Protocol on Register URL	Whether to specify transport protocol on register URL.
Expire Seconds	The validity period after the FXO trunk is registered successfully. When the time expires, the FXO trunk will send register request to the server. Default value is 1800s
Retry Seconds	When the FXO trunk fails to be registered, the interval to send register request; Default value is 60s
Display Name/Username Format	The format to display caller information, including: Caller ID/Caller ID Display Name/ Caller ID Extension/ Caller ID Caller ID/ Extension Anonymous
Display Name / Username Format when CID unavailable	Set the caller's caller id format when the main number is not detected
Input Gain	The receiving gain of the FXO port
Output Gain	The sending gain of the FXO port

Impedance	The impedance （SLIC） matched with phones
FXO Profile	The FXS profile that is selected for this FXS extension
Status	If it is on, this FXO trunk can be used, otherwise, the FXO trunk is unavailable.

FXO Automatch Impedance:

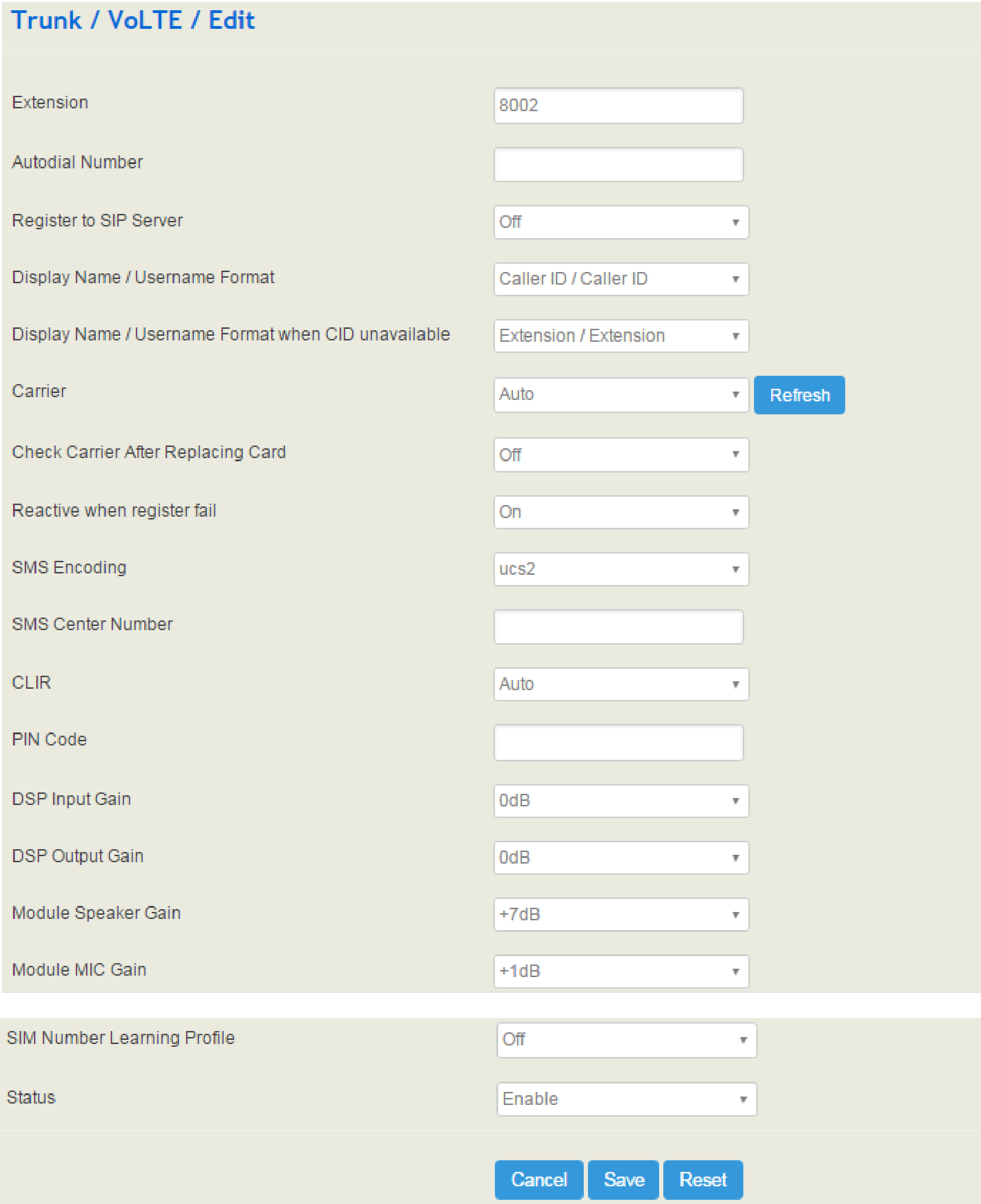
Click the **Detection** button, and the UC100-1V1S1O gateway will automatically detect the most-matched impedance.

Figure 5-65 FXO Automatch Impedance



5.7.3 VoLTE Trunk

VoLTE trunk helps interconnect the LTE network with the IP network. The VoLTE function allows calls or SMS from the IP network to be transmitted to mobile network, and packs voice or SMS from mobile network into IP packages and send them to IP network.



Extension	The extension account of the VoLTE trunk, which is used to register
Autodial Number	The autodial number of the The address and port of the master SIP server; it is generally the IP address of a SIP trunk. Please make reference to Trunk → SIP section when there are incoming calls
Register to SIP Server	If it is enabled, the GSM trunk will be registered to the SIP trunk that has been set. Default is off.
Master Server	The master SIP server to which the VoLTE trunk is registered.

	Enter the address and port of the master SIP server; it is generally the IP address of a SIP trunk. Please make reference to Trunk → SIP section
Slave Server	The slave SIP server to which the VoLTE trunk is registered. Enter the address and port of the slave SIP server
Username	The username of this VoLTE trunk used for registration; it is generally a phone number
Auth Username	The username of this VoLTE trunk, which is used during register authentication
Password	The password of this VoLTE trunk, which is used during register authentication
From Header Username	Choose the registered username or the true caller ID for the 'from header' of the invite message when a call goes out.
Specify Transport Protocol on Register URL	Whether to specify transport protocol on register URL.
Expire Seconds	The validity period after the VoLTE trunk is registered successfully. When the time expires, the GSM trunk will send register request to the server. Default value is 1800s
Retry Seconds	When the VoLTE trunk fails to be registered, the interval to send register request; Default value is 60s
Display Name/Username Format	The format to display caller information, including: Caller ID/Caller ID Display Name/ Caller ID Extension/ Caller ID Caller ID/ Extension Anonymous
Display Name/Username Format when CID unavailable	The format to display caller information when CID is unavailable
Carrier	Click the Refresh button, and the gateway will automatically to identify the carrier of the inserted SIM card.
Reactive when register fail	Whether to reactivate the VoLTE trunk when register fails
SMS Encoding	ucs2 or 7bit， 7-bit is used to send original ASCII, while UCS2 is used to send various languages
SMS Center Number	Generally, the GSM module can automatically detect the SMS center number. This parameter will be used when the LTE

	module cannot detect the SMS center number.
CLIR	Whether to enable Calling Line Identification Restriction
PIN Code	PIN code is personal identification code. When SIM card is locked, you can modify the PIN code to prevent the SIM infor from being stolen
DSP Input Gain	Volume control of DSP input
DSP Output Gain	Volume control of DSP output
Module Speaker Gain	Volume control of module speaker
SIM Number Learning Profile	Choose a number learning profile for the SIM card. The SIM number will be displayed on the Status →PSTN→VOLTE page
Status	If it is on, this VoLTE trunk can be used, otherwise, the VoLTE trunk is unavailable

5.8 **Call Control**

This section is to configure routes or route groups for incoming and outgoing calls through UC100-1V1S1O, as well as IVR, SMS, USSD and so on.

5.8.1 Setting

Figure 5-66 Basic Setting of Call Control

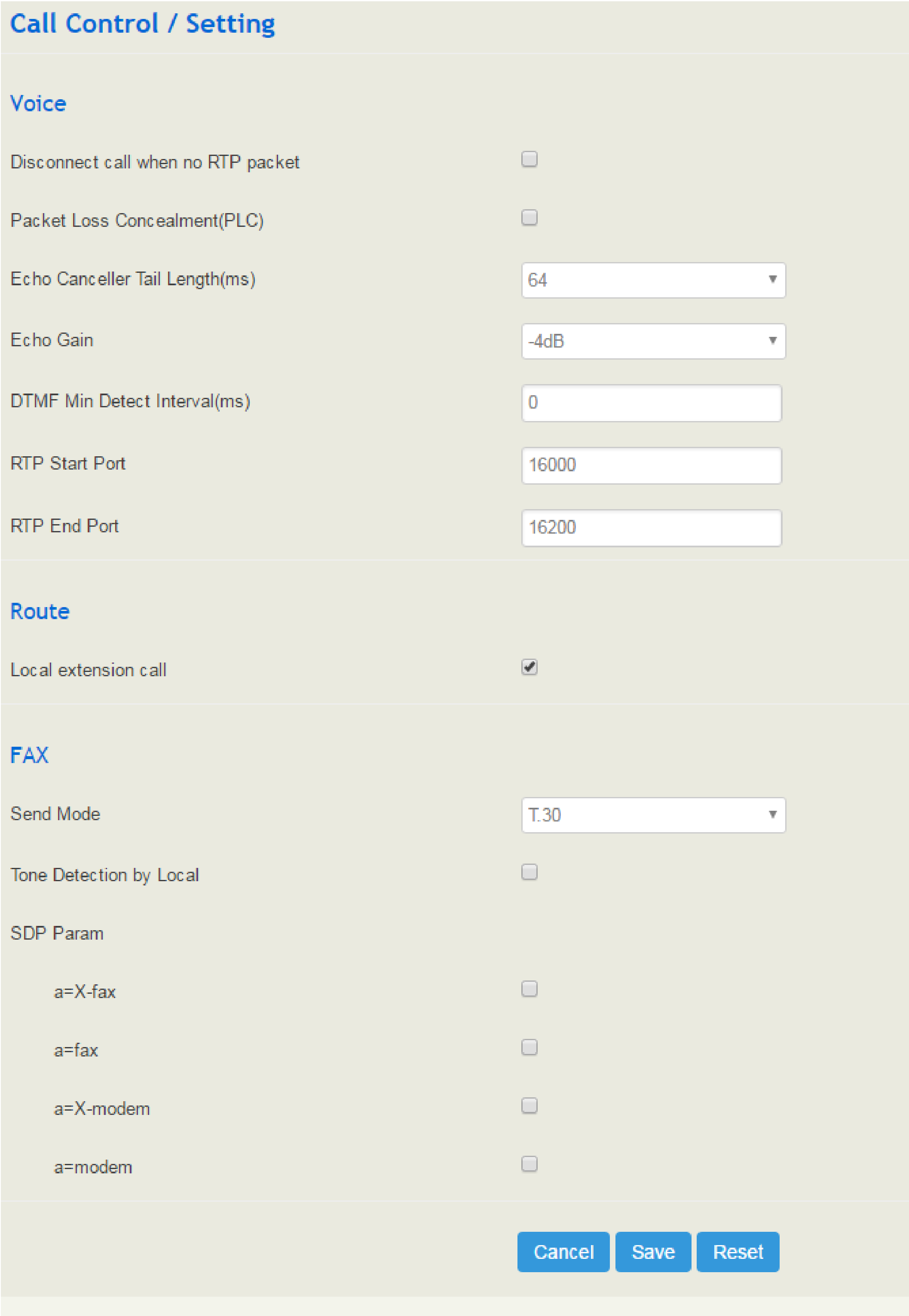


Table 5-30 Explanation of Parameters for Call Control

Disconnect call when no RTP packet	If it is enabled, and no RTP packets are received within the preset time, calls will be disconnected
Packet Loss Concealment (PLC)	Whether to enable the 'Packet Loss Concealment' function
Echo Canceller Tail Length (ms)	Default value: 64ms
DTMF Min Detect Interval (ms)	The minimum time for DTMF detection
Echo Gain	Default value: -4dB
RTP Start Port	The start port of RTP packets
RTP End Port	The end port of RTP packets
Local extension call	If it is enabled, calls between local extensions do not need routes.
Fax Mode	T38 or T30（Pass-through）
Tone Detection by Local	If it is enabled, UC100-1V1S1O will detect fax tones automatically during a call and the call will be switched into fax mode after a fax tone is detected.
SDP Param 'a=X-fax'	Attribute parameter 'a=X-fax' is carried in SDP
SDP Param 'a=fax'	Attribute parameter 'a=fax' is carried in SDP
SDP Param 'a=X-modem'	Attribute parameter 'a=X-modem' is carried in SDP

5.8.2 Route Group

On the **Call Control →Route Group** interface, you can group SIP trunks, SIP extensions, FXS extension and FXO trunk together according to your needs and set strategy for choosing which trunk or extension as the destination route under a route group.

Figure 5-67 Create Route Group

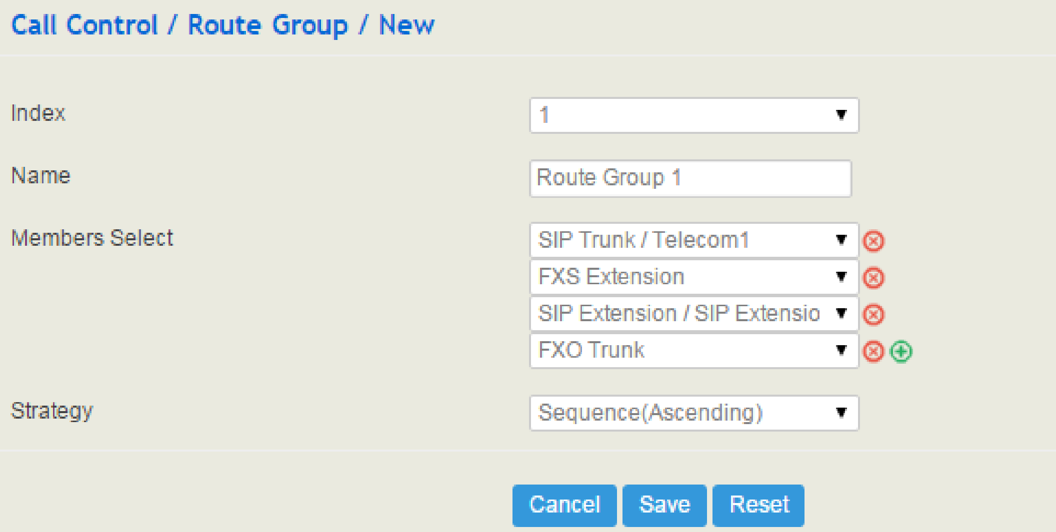


Table 5-31 Explanation of Parameters for Route Group

Name	The name of the route group
Members Select	Select FXS extension, SIP extension, SIP trunk, FXO trunk or GSM trunk
Strategy	The strategies for choosing which route under the route group as the destination route, including Sequence (Ascending), Sequence (Cyclic Ascending), Simultaneous and Random

5.8.3 Route

On the **Call Control → Route** interface, you can configure routes for incoming calls and outgoing calls.

Figure 5-68 Create a Route

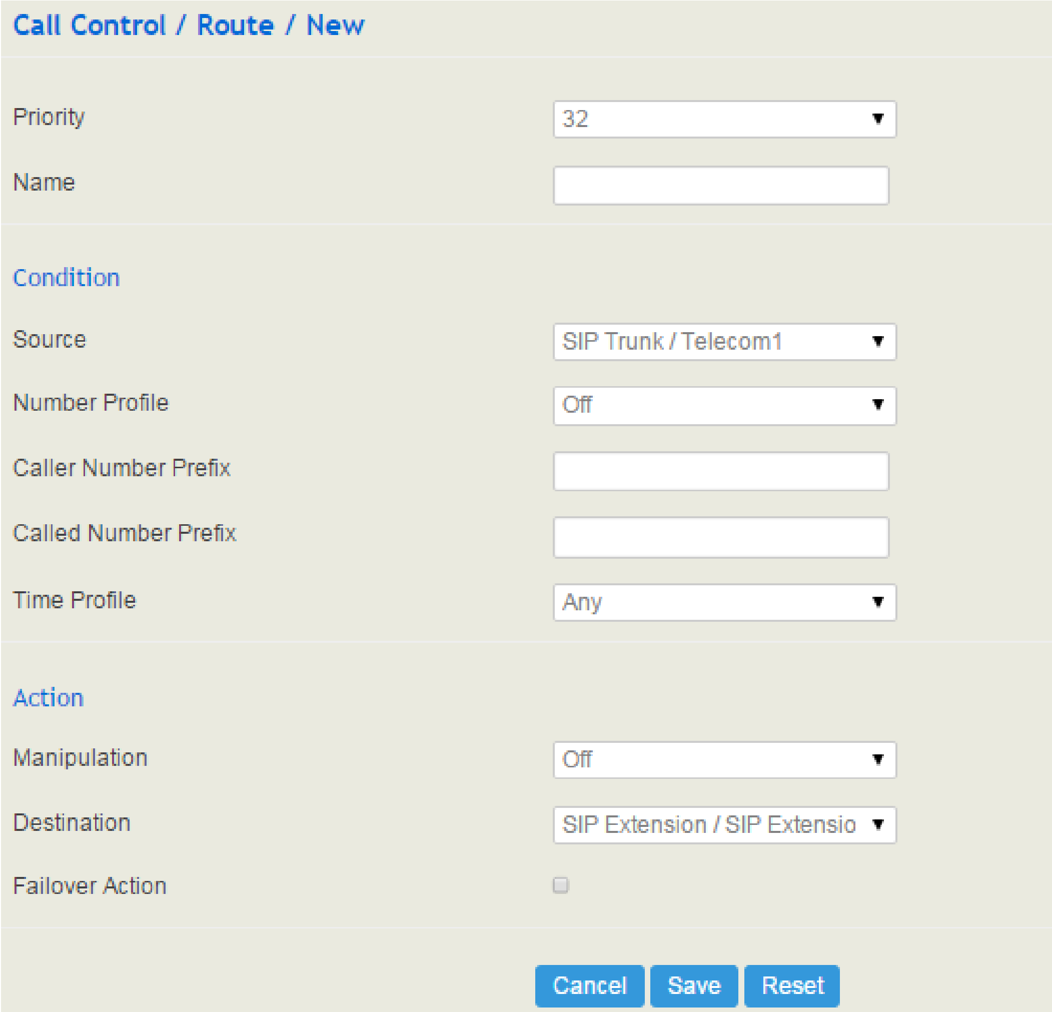


Table 5-32 Explanation of Route Parameters

Priority	The priority for choosing the route; the higher value, the lower priority
Name	The name of the route
Condition	The condition under which the route will be used
Source	The source of the call; it can be the FXS extension, SIP extension, FXO trunk ,GSM trunk, a customized source or any
Number Profile	The profile of the caller number and the called number; please make reference to the Profile → Number section.The default value is ‘Off’ Note: it cannot be simultaneously used with the following parameters of ‘caller number prefix’ and ‘called number prefix’
Caller Number Prefix	The prefix of caller number; it supports regular expression

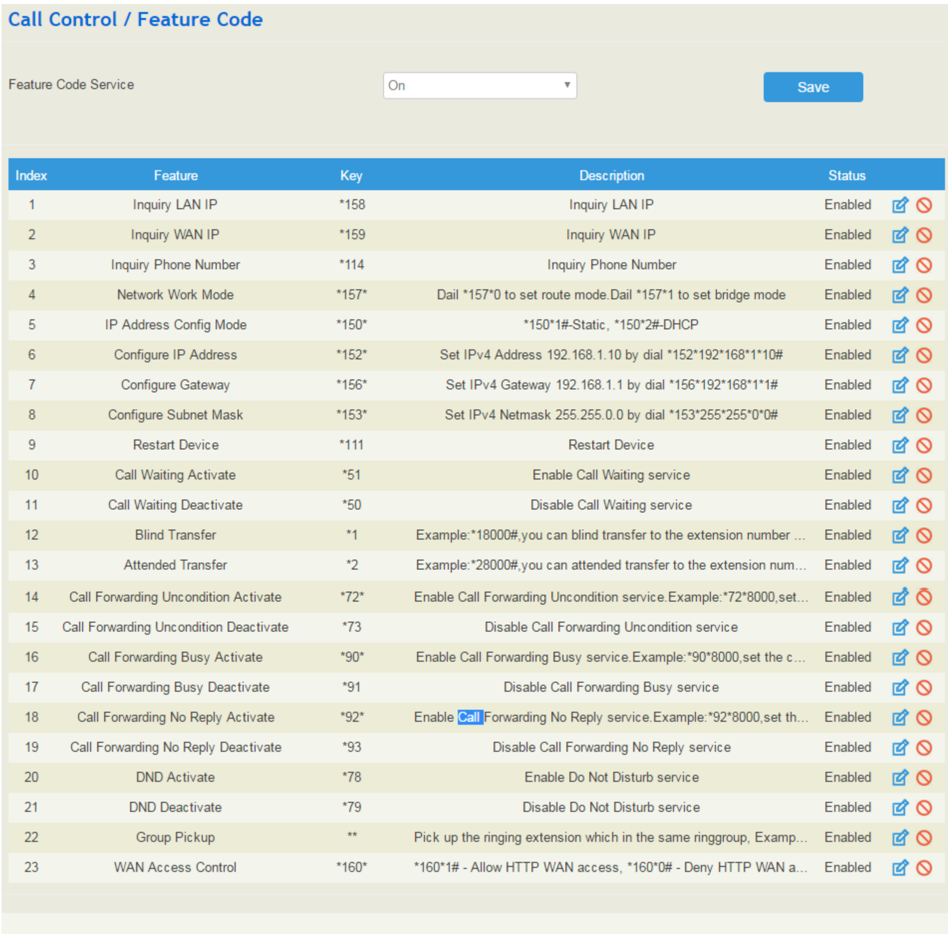
Called Number Prefix	The prefix of called number; it supports regular expression
Time Profile	The profile of time during which the route can be used; make reference to the Profile → Time section
Action	Include manipulating number and sending call to destination
Manipulation	If it is on, the caller number or called number of the route will be manipulated; make reference to the Profile→ Manipulation section
Destination	The destination of the route
Failover Action	The processing when a call through this route fails

5.8.4 Feature Code

UC100-1V1S1O provides convenient telephone functions. Connect a telephone to the FXS port and dial a specific feature code, and you can query conrresponding information.

The following is the corresponding function of each feature code:

Figure 5-69 Feature Code



Index	Feature	Key	Description	Status
1	Inquiry LAN IP	*158	Inquiry LAN IP	Enabled
2	Inquiry WAN IP	*159	Inquiry WAN IP	Enabled
3	Inquiry Phone Number	*114	Inquiry Phone Number	Enabled
4	Network Work Mode	*157*	Dail *157*0 to set route mode.Dail *157*1 to set bridge mode	Enabled
5	IP Address Config Mode	*150*	*150*1#-Static, *150*2#-DHCP	Enabled
6	Configure IP Address	*152*	Set IPv4 Address 192.168.1.10 by dial *152*192*168*1*10#	Enabled
7	Configure Gateway	*156*	Set IPv4 Gateway 192.168.1.1 by dial *156*192*168*1*1#	Enabled
8	Configure Subnet Mask	*153*	Set IPv4 Netmask 255.255.0.0 by dial *153*255*255*0*0#	Enabled
9	Restart Device	*111	Restart Device	Enabled
10	Call Waiting Activate	*51	Enable Call Waiting service	Enabled
11	Call Waiting Deactivate	*50	Disable Call Waiting service	Enabled
12	Blind Transfer	*1	Example:*18000#,you can blind transfer to the extension number ...	Enabled
13	Attended Transfer	*2	Example:*28000#,you can attended transfer to the extension num...	Enabled
14	Call Forwarding Uncondition Activate	*72*	Enable Call Forwarding Uncondition service.Example:*72*8000,set...	Enabled
15	Call Forwarding Uncondition Deactivate	*73	Disable Call Forwarding Uncondition service	Enabled
16	Call Forwarding Busy Activate	*90*	Enable Call Forwarding Busy service.Example:*90*8000,set the c...	Enabled
17	Call Forwarding Busy Deactivate	*91	Disable Call Forwarding Busy service	Enabled
18	Call Forwarding No Reply Activate	*92*	Enable Call Forwarding No Reply service.Example:*92*8000,set th...	Enabled
19	Call Forwarding No Reply Deactivate	*93	Disable Call Forwarding No Reply service	Enabled
20	DND Activate	*78	Enable Do Not Disturb service	Enabled
21	DND Deactivate	*79	Disable Do Not Disturb service	Enabled
22	Group Pickup	**	Pick up the ringing extension which in the same ringgroup, Examp...	Enabled
23	WAN Access Control	*160*	*160*1# - Allow HTTP WAN access, *160*0# - Deny HTTP WAN a...	Enabled

Note: All feature codes are enabled by default.

5.8.5 IVR

On the **Call Control → IVR** interface, you can carry out specific configurations for the IVR which has been uploaded from the **System → Voice** interface.

Figure 5-70 IVR Setting

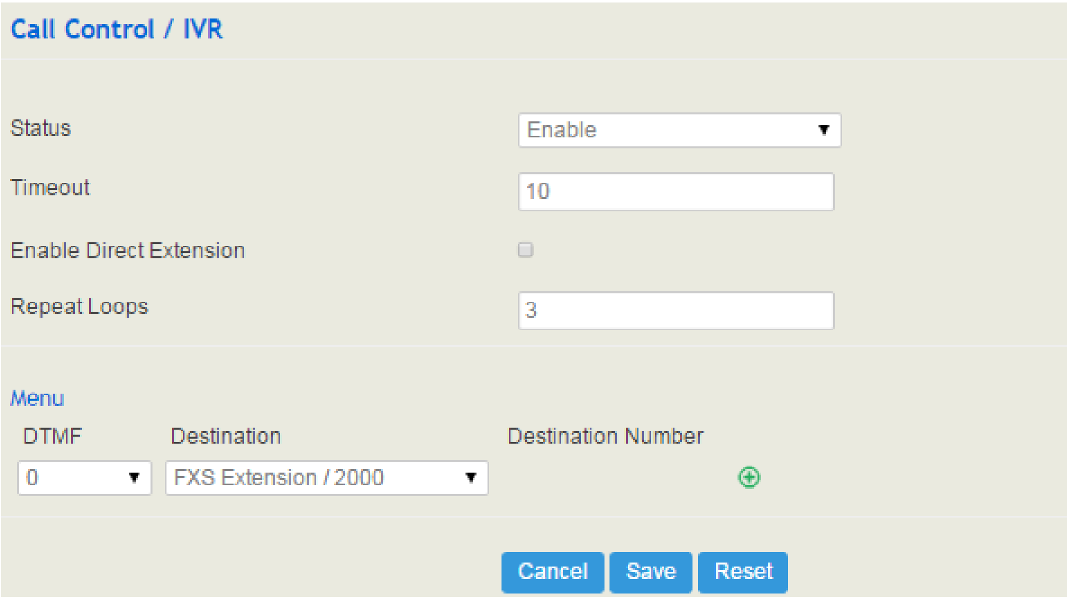


Table 5-33 Explanation of IVR Parameters

Status	If it is disabled, the IVR cannot be seen in the destination of route.
Timeout	If it is set as '10', it means if no DTMF tone is received during 10 seconds, the IVR will be played repeatedly or the call will be hanged up. The default value is 10 seconds.
Enable Direct Extension	Whether to allow direct dialing of extensions during the playing of IVR
Repeat Loops	If it is set as '3', the call will be hanged up after the IVR has been repeated for three times during timeout.
Menu	DTMF: It can be 0-9 quick-dial numbers, *, #, others or timeout. Destination: the destination of the IVR; it can be an extension or a trunk. For example, if DTMF is configured as 1,2,3 and others, and the telephone key that is pressed is not 1, 2 or 3, the IVR will choose the destination of 'others'. When the the playing of the IVR times out, and user does not press any telephone key, the IVR will choose the destination of 'timeout'. When the destination is a trunk, user does not need to pre-configure the

	called number, and the system will prompt the user to dial the called number.

5.8.6 SMS Route

UC100-1V1S1O allows SMS to be sent between SIP clients, and meanwhile allow SMS to be sent between IP network/GSM network and GSM network. On the **Call Control→ SMS Route** interface, you can establish route for these SMS.

For example, you can download a softphone on a PC which is connected to UC100-1V1S1O, and type the content of the SMS through the softphone. Then configure a SMS route on the **Call Call Control→ SMS Route** interface. The source of the SMS route is the number of the softphone.

Figure 5-71 Create SMS Route

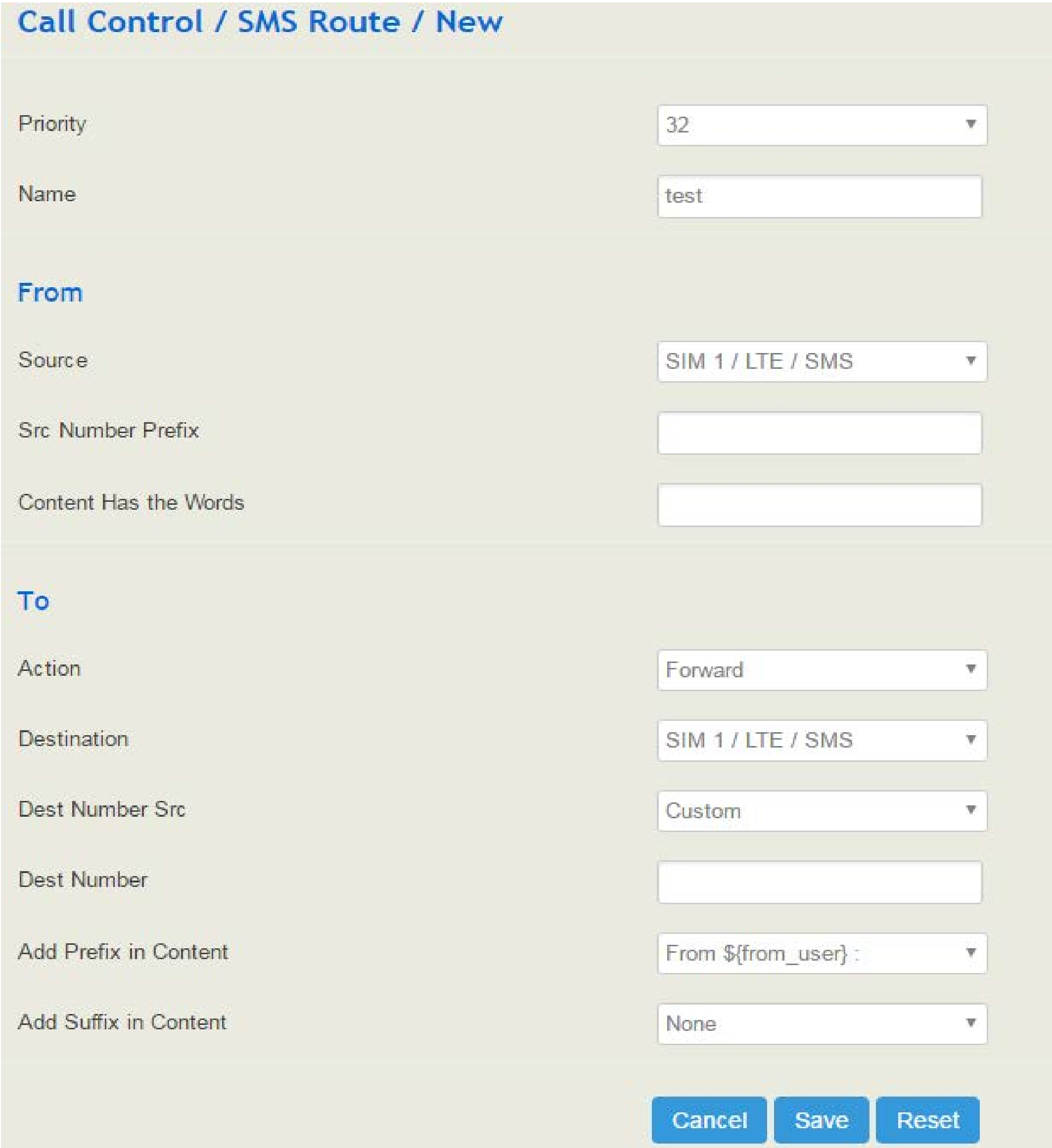


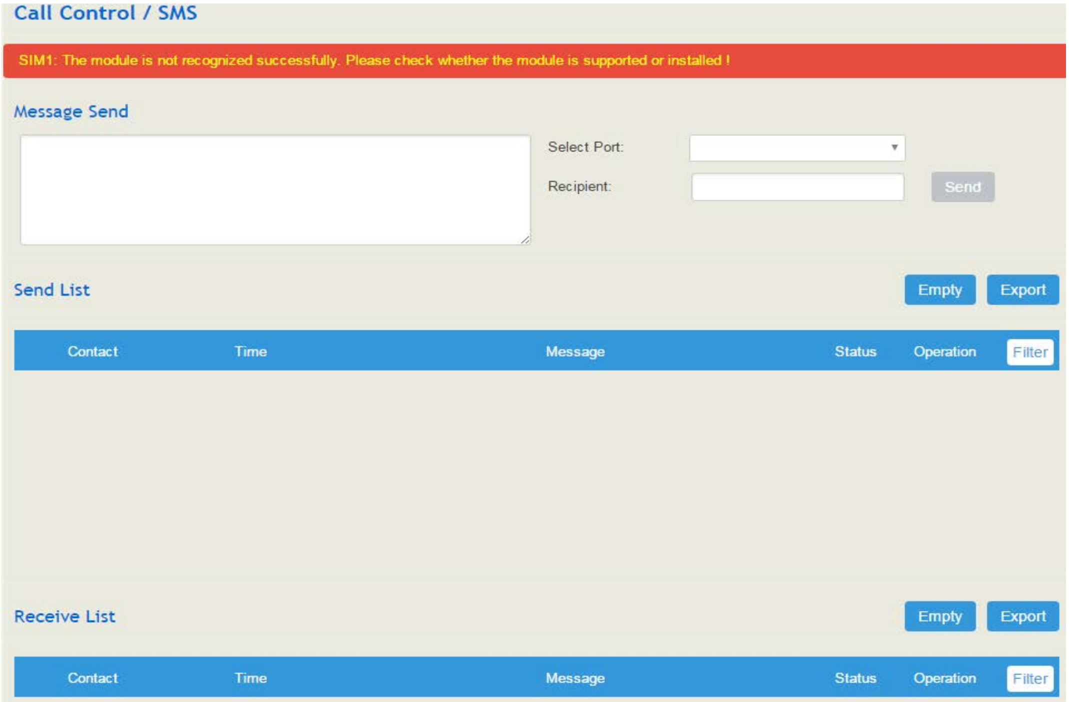
Table 5-34 Explanation of SMS Route Parameters

Priority	The priority for the SMS route; the higher value, the lower priority
Name	The name of the SMS route
Source	The source of the SMS route. It can be a trunk or an extension.It also can be a LTE SMS and USSD.
Src Number Prefix	Prefix the source number to support regular expressions
Content Has the Words	Match key words in text message content
Action	The text message action can choose whether to forward or reply
Destination	The destination of the SMS route. It can be a trunk or an extension.
Dest Number Src	The source of the destination number.There are two sources:custom and get from content.
Add Prefix in Content	The prefix of the SMS content. It is generally 'none', which means there is no prefix to be matched.
Add Suffix in Content	The suffix of the SMS content. It is generally 'none', which means there is no suffix to be matched.

5.8.7 SMS

If an SIM card has been inserted into the SIM slot, you can send or receive SMS on the **SMS** interface. The length of a SMS can not be more than 170 characters.

Figure 5-72 Send and Receive SMS



Notice

If the SIM fails, you will get a notice:SIM1: The module is not recognized successfully. Please check whether the module is supported or installed !

Send Message

Enter contents into the box on the left, and then input the number of recipient . Click **Send** in the last.

Note: If there are mutilple recipients , use | to separate them, for example, 13151103146|18954405566.

Receive Message

All SMS received by UC100 are displayed on the Receive List.

Read Message

Click on the Receive List to read SMS contents.

Reply Message

Click , and then enter SMS contents in the box on the left. Click Send in the last.

Delete Message

Click to delete an SMS.

Note: Group sending of SMS is not allowed.

5.8.8 USSD

USSD (Unstructured Supplementary Service Data) is a global system service for mobile (GSM) communication technology that is used to send text between a mobile phone and an application program in the network.

USSD is similar to Short Messaging Service (SMS), but, unlike SMS, USSD transactions occur during the session only. With SMS, messages can be sent to a mobile phone and stored for several days if the phone is not activated or within range.

Figure 5-73 USSD

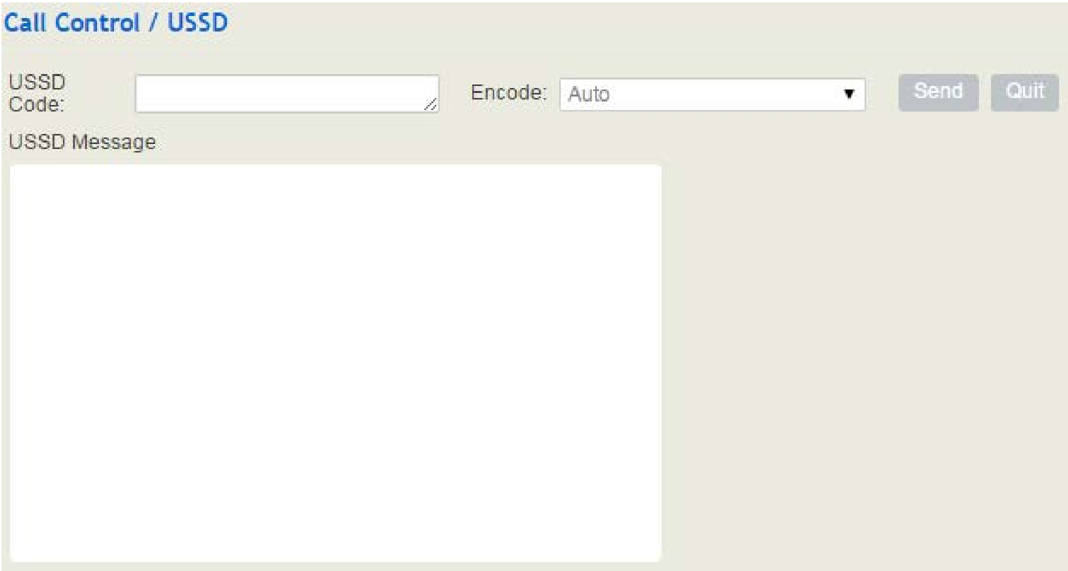


Table 5-35 Explanation of USSD Parameters

USSD Code	USSD code is a special number starting with * or #, followed by 2~3 digits, then ending with #; Service provider feedbacks a service menu to user according to this USSD code.
Encode	Supports auto, 7-bit and UCS2; 7-bit is used to send original ASCII, while UCS2 is used to send any languages
USSD Message	The Content of the USSD message

5.8.9 Diagnostics

In case that call cannot be connected or voice has quality problem, you can enter into the **Call Control →Diagnostics** interface to collect fault-related information and then send it to technical support to locate fault.

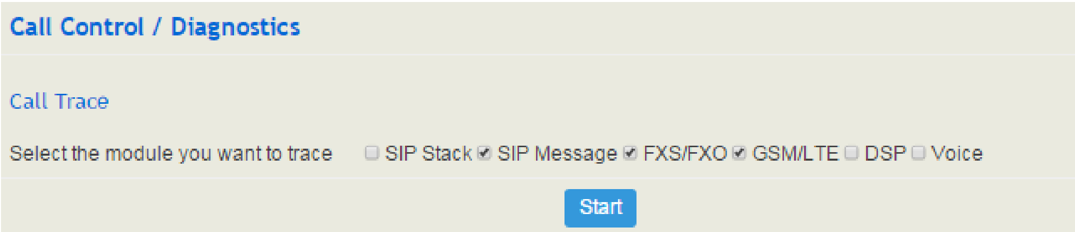
Operation Procedures:

1． Select the module that needd to be traced. For example, if a call from SIP to FXS has voice problem, you can select SIP message, FXS/FXO and Voice, and then click the **Start** button.

2． Give a call, and come back to the **Call Control →Diagnostics** interface after the call ends. Then click Stop and download the tracing file.

3. In order to locate faluts more quickly, you sometimes need to enter into the **System →Service** Log interface, click export, and then send this exported file and the tracing file to technical support,

Figure 5-74 Call Tracing for Diagnostics



6 Glossary

Glossary	Description
ARP	Address Resolution Protocol
CID	Caller Identity
DNS	Domain Name System
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DND	Do NOT Disturb
DTMF	DTMF： Dual Tone Multi Frequency
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
PPTP	Point-to-Point Tunneling Protocol
MAC Address	Media Access Control Adress
NAT	Network Address Translation
Ping	Packet Internet Grope
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RTP	Real Time Protocol
PPPOE	Point-to-point Protocol over Ethernet
QoS	Quality of Service
UPnP	Universial Plug and Play
VLAN	Virtual Local Area Network

Glossary	Description
NTP	Network Time Protocol
STUN	Simple Traversal of UDP over NAT
PSTN	Public Switched Telephone Network
WLAN	Wireless Local Area Network