TA1600/TA2400/TA3200

User Manual





Sales Tel: +86-592-5503309
E-mail: sales@yeastar.com
Support Tel: +86-592-5503301
E-mail: support@yeastar.com
Web: http://www.yeastar.com

Version: 40.19.0.14
Revised: January 25, 2016

Copyright

Copyright 2006-2015 Yeastar Information Technology Co., Ltd. All rights reserved.
No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yeastar Information Technology Co., Ltd. Under the law, reproducing includes translating into another language or format.

Declaration of Conformity

Hereby, Yeastar Information Technology Co., Ltd. declares that TA1600/2400/3200 is in conformity with the essential requirements and other relevant provisions of the CE, FCC.

Warranty

The information in this document is subject to change without notice.
Yeastar Information Technology Co., Ltd. makes no warranty of any kind with regard to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Yeastar Information Technology Co., Ltd. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this guide.

WEEE Warning



In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

Contents

About This Guide 5

Getting Started 7

Accessing Web GUI 7
Web Configuration Panel 8
Making and Receiving Calls 8

Basic Operations 9

Voice Menu 9
Call Hold 10
Call Waiting 10
Call Transfer 10
Three-party Conference 11
Direct IP Call 11
Change TA1600/2400/3200's IP Address Using Analog Phones 11

FXS Port Settings 13

General Settings 13
Other Settings 15
Hunt Group 16

VoIP Settings 19

VoIP Server Settings 19
Dial Pattern Template 21
SIP Settings 22
IAX Settings 27

Gateway Settings 29

Basic Preferences 29
Feature Codes 30
Speed Dial 33

Prompt Settings 34

Custom Prompts 34
Music on Hold Prompts 35
System Prompts 35

Advanced Settings 37

Distinctive Ringtones 37
Tone Zone Settings 37
RADIUS Settings 38

Network Preferences 40

LAN Settings 40
Service 41
VLAN Settings 42
VPN Settings 42
DDNS Settings 43
Static Route 44
SNMP Settings 45
TR-069 Settings 45

Security Center 47

Security Center 47
Alert Settings 48
AMI Settings 50
Certificates 51
Firewall Rules 52
IP Blacklist 54

System Preferences 56

Password Settings 56
Date and Time 56
Auto Provision Settings 57
Firmware Upgrade 59
Upgrade through HTTP 59
Upgrade through TFTP 60
Backup and Restore 61
Reset and Reboot 61

Status 63

FXS Port Status 63
Network status 64
System Info 64

Reports 65

Call Logs 65
System Logs 65
Packet Tool 66
Port Monitor Tool 66

About This Guide

YeastarTA1600/2400/3200 FXS Analog VoIP Gateways are cutting-edge products that connect legacy telephones, fax machines and PBX systems with IP telephony networks and IP-based PBX systems. Featuring rich functionalities and easy configuration, Yeastar TA is ideal for small and medium enterprises that wish to integrate a traditional phone system into IP-based system. Yeastar TA helps them to preserve previous investment on legacy telephone system and reduce communication costs significantly with the true benefits of VoIP.

Audience

This manual will help you learn how to operate and manage your TA1600/2400/3200 FXS Analog VoIP Gateway. In this guide, we describe every detail on the functionality and configuration of TA1600/2400/3200. We begin by assuming that you are interested in TA1600/2400/3200 and familiar with networking and other IT disciplines.

Safety when working with electricity



- Do not open the device when the device is powered on.
- Do not work on the device, connect or disconnect cables when lightning strikes.

Features Highlights

- 16/24/32 FXS ports
- Fully compliant with SIP and IAX2
- Hunt Group
- Configurable VoIP Server templates
- Reliable FAX performance with T.38
- 3-party conference
- Direct IP Calling
- Inter-port Calling
- Attended Transfer
- Blind Transfer
- Support RADIUS protocol
- Support SNMP
- Support TR-069

Check the TA1600/2400/3200 Installation Guide here:
http://www.yeastar.com/downloadFile/Yeastar_TA_Series_Installation_Guide_en.pdf

For more information, please click:
http://www.yeastar.com/Products.html/Analog-VoIP-Gateways

Getting Started

In this chapter, we guide you through the basic steps to start with a new TA1600/2400/3200:

- Accessing Web GUI
- Web Configuration Panel
- Making and Receiving Calls

Accessing Web GUI

The TA1600/2400/3200 attempts to contact a DHCP server in your network to obtain valid network settings (e.g., the IP address, subnet mask, default gateway address and DNS address) by default.
Please enable DHCP Server in your network to obtain the TA1600/2400/3200 IP address.

How to check TA1600/2400/3200 IP address:

1. Pick up the analog phone, then access the voice menu prompt by dialing "***".
2. Dial "**1**" to check the IP address.
3. Dial "**2**" for web access address.

After entering the IP address in the web browser, users will see a log-in screen.
Check the default settings below:
Username: admin
Password: password

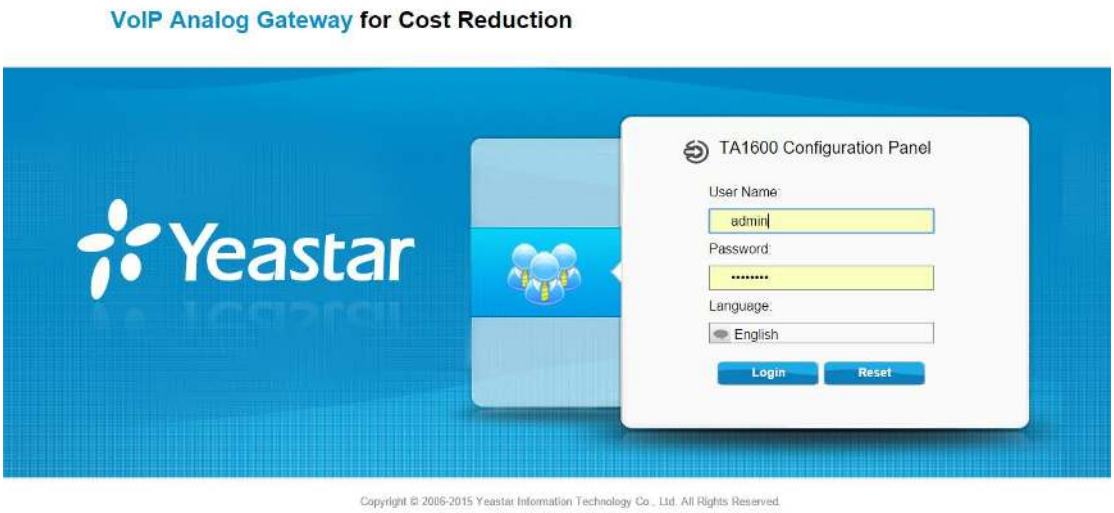


Figure 2-1 TA1600/2400/3200 Login page

Web Configuration Panel

There are 4 main sections on the Web Configuration Panel for users to check the TA1600/2400/3200's status and configure it.

- **Status:** check System Status, Port Status, Trunk Status, Network Status and check call logs, system logs.
- **System:** configure Network Settings, Security related Settings, System Date and Time, Password, Backup and Restore, etc.
- **Gateway:** configure FXS ports, gateway settings and SIP settings, etc.
- **Logout:** log out TA1600/2400/3200.

Note:
After saving the changes, remember to click the "Apply changes" button on the upper right corner of the Web GUI to make the changes take effect.

Making and Receiving Calls

You will need an active VoIP account from a VoIP service provider or PBX, which provides a VoIP telephone number to allow you to make and receive calls.

- **Making internal calls**
  To place an internal call, pick up the analog phone and dial the other port's caller ID number or dial *99 followed by the port number.
  For example, to reach the other port with caller ID number 300, dial "300".
  To reach port 2, you can dial *9902 to ring the phone connected to port 2.

- **Making outbound calls**
  To make an outbound call, you need to dial according to the FXS port dial pattern. By the default dial pattern, you can dial the desired outgoing number directly.

- **Answering calls**
  To answer a call, pick up the handset as you usually do.

Basic Operations

In this chapter, we give instructions about how to operate on analog phones connected to TA1600/2400/3200 to use some features.

- Voice Menu
- Call Hold
- Call Waiting
- Call Transfer
- Three-party Conference
- Direct IP Call
- Change TA1600/2400/3200's IP Address

Voice Menu

TA1600/2400/3200 provides a voice menu to guide you to configure the network settings for the device. You need to press *** on the analog phone which is connected to TA1600/2400/3200's FXS port to enter the voice menu.

The default password to enter "Advanced Settings" is 123456. You can change the password on TA1600/2400/3200 Web page.(Gateway→Gateway Settings→Feature Codes→Voice Menu Password Settings)

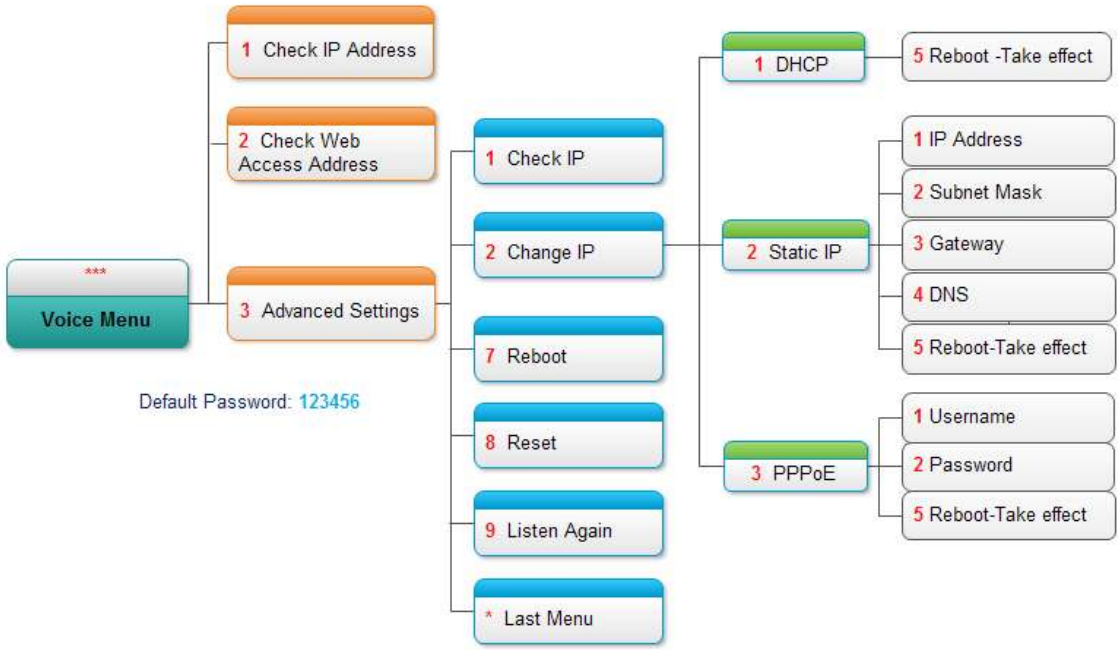


Figure 3-1 TA1600/2400/3200 Voice Menu

Tips:

1. Press “9” to listen to the prompt again.
2. Press “*” to return to the last menu.

Call Hold

An active call can be held by pressing "flash" key on the analog phone. Press the key again to resume the call.
If there is no "flash" key on the phone, you can use "hook flash" (quickly toggle on-off hook) to hold a call. The call may be disconnected by chance if using "hook flash".

Call Waiting

If the call waiting is activated for the FXS port, the FXS user who is in a call can hear a call waiting tone "beep" when there is a new incoming call. The user can press "hook flash" to toggle between the active call and the incoming call.

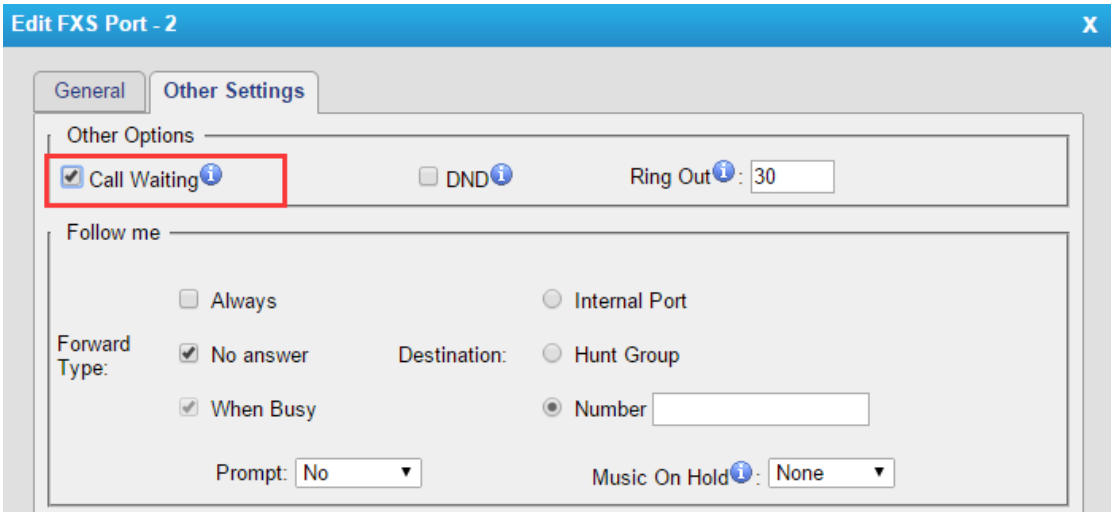


Figure 3-2 Enable Call Waiting

Call Transfer

Blind transfer and attended transfer are supported on TA1600/2400/3200. Users can achieve call transfer by pressing the feature code during the call.

Blind Transfer

Default feature code: *03

1. Dial "*03" during the call;
2. Dial the called number after hearing a prompt "transfer";
3. The call will be transferred after the number is dialed.

Attended Transfer
Default feature code: *3
1. Dial "*3" during the call;
2. Dial the called number after hearing a prompt "transfer";
3. Talk to the transfer recipient;
4. The call will be transferred after hanging up.

Three-party Conference

Users can make a three-party conference call on TA1600/2400/3200.
Assuming that A and B are in the call and B wants to invite C to a conference. Please check the following steps of how to establish a conference.

1. B presses "flash" key or taps hook flash to get a dial tone; A will hear the on hold music meanwhile;
2. B dials C's number;
3. If C answers the call, then B presses "flash" key or tap hook flash, the conference will be established, including A, B, and C.
4. If there is no answer on C, A can press "flash" key or tap hook flash to resume the call with A.
5. C will be ejected if B presses "flash" key or taps flash hook during the conference call.

Direct IP Call

Direct IP call allows two parties, that is, a FXS Port with an analog phone and another VoIP Device, to talk to each other in an ad hoc fashion without a SIP proxy. The default "Direct IP Calling" feature code is *96.
Example:
Target IP address: 192.168.2.123
Destination port: 5060
To call the IP phone, you should dial *96192*168*2*123*5060 on the analog phone.

Change TA1600/2400/3200's IP Address Using Analog Phones

By default, TA1600/2400/3200 obtains a dynamic IP address from the DHCP server. You can change the device's IP address via the analog phone which is connected to the FXS port.
There are 3 modes supported on TA1600/2400/3200 access the internet.
- DHCP

- Static IP Address
- PPPoE

Here we introduce how to set a static IP address for TA1600/2400/3200.
IP address: 192.168.10.125
Subnet mask: 255.255.255.0
Gateway: 192.168.10.1
DNS: 8.8.8.8

1. Press *** to enter the voice menu.
2. Press 3 to enter the “Advanced Settings”.
3. Enter the password follow by the pound key: 123456# (The default password is 123456).
4. Press 2 to change the IP address.
5. Press 2 to enable the static IP.
6. Press 1 to change the IP address and follow by the new IP address (1192*168*10*125).
7. Press 2 to change the subnet mask and follow by the new subnet mask (2255*255*255*0).
8. Press 3 to change the gateway and follow by the new gateway (3192*168*10*1).
9. Press 4 to change the DNS and followed by the new DNS (48*8*8*8).
10. Press 5 to reboot the device.
11. After reboot, you can access the device by the new IP address.

FXS Port Settings

This chapter explains how to configure FXS port on TA1600/2400/3200, go to **Gateway→ Port List→ Port List** page to configure the FXS ports.

- General Settings
- Other Settings
- Hunt Group

Click "Edit" button  to configure the FXS port.

General Settings

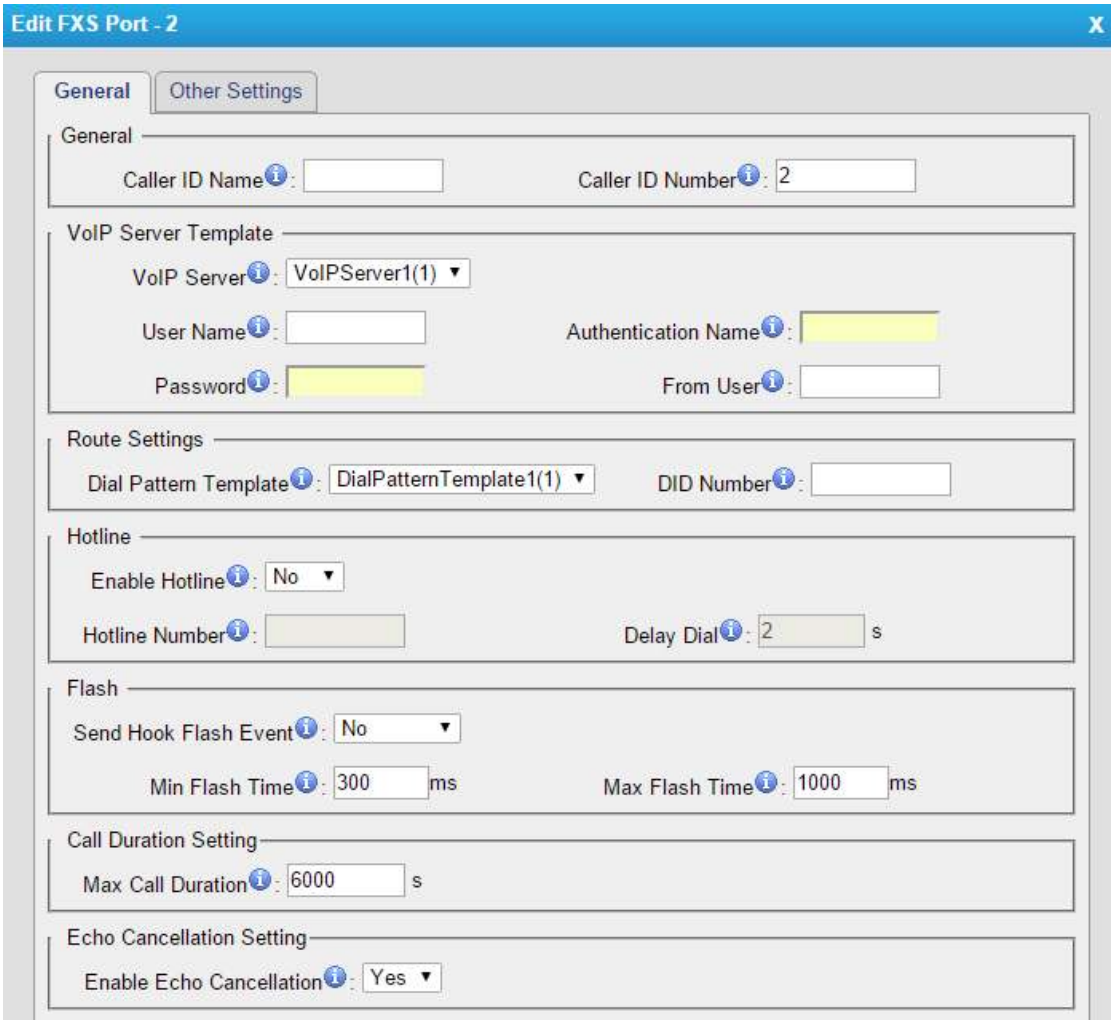


Figure 4-1 FXS Port General Settings

Table 4-1 Description of FXS Port General Settings

Items		Description
General	Caller ID Name	A character-based name for this user. For

		example, Bob Jones.
	Caller ID Number	The Caller ID string used when this user calls another user.
VoIP Serer Template	VoIP Server	Choose a VoIP server, where the account will be registered.
	User Name	User name provided by VoIP server.
	Authentication Name	Authentication name provided by VoIP server.
	Password	Authentication password provided by VoIP server.
	From User	Provided by VoIP server. Keep this field blank if not needed.
Route Settings	Dial Pattern Template	The account will be allowed to make outbound calls according to the selected template.
	DID Number	Defines the expected DID number if this trunk passes DID on incoming calls. Leave this field blank to match calls with any or no DID info.
Hotline	Enable Hotline	Select whether to use Hotline or not. Hotline is disabled by default. If this feature is enabled, the system will dial out the hotline number automatically after off-hook.
	Hotline Number	Set the number to dial out automatically after off-hook.
	Delay Dial	Define how long to make Hotline take effect after you pick up the phone.
Flash	Send Hook Flash Event	If the option “Send Hook Flash Event” is set to “Yes”, when pressing the flash key on the analog phone during an active call. TA will send a SIP DTMF flash event to the VoIP server. It can be an interoperation with a FXO gateway which is used for informing FXO gateway to generate the flash signal to the CO line.
	Min Flash Time	Sets the minimum time the phone is on hook before being detected as a hook flash.
	Max Flash Time	Sets the maximum flash time.
Call Duration Setting		Setup the max cull duration for every call of this user, but it’s only valid for outbound calls. **Note**: this setting will not be valid for internal calls.
Echo Cancellation Setting		To disable or enable echo cancellation. If the line is used to connect POS machine, it is suggested that echo cancellation is disabled.

Other Settings

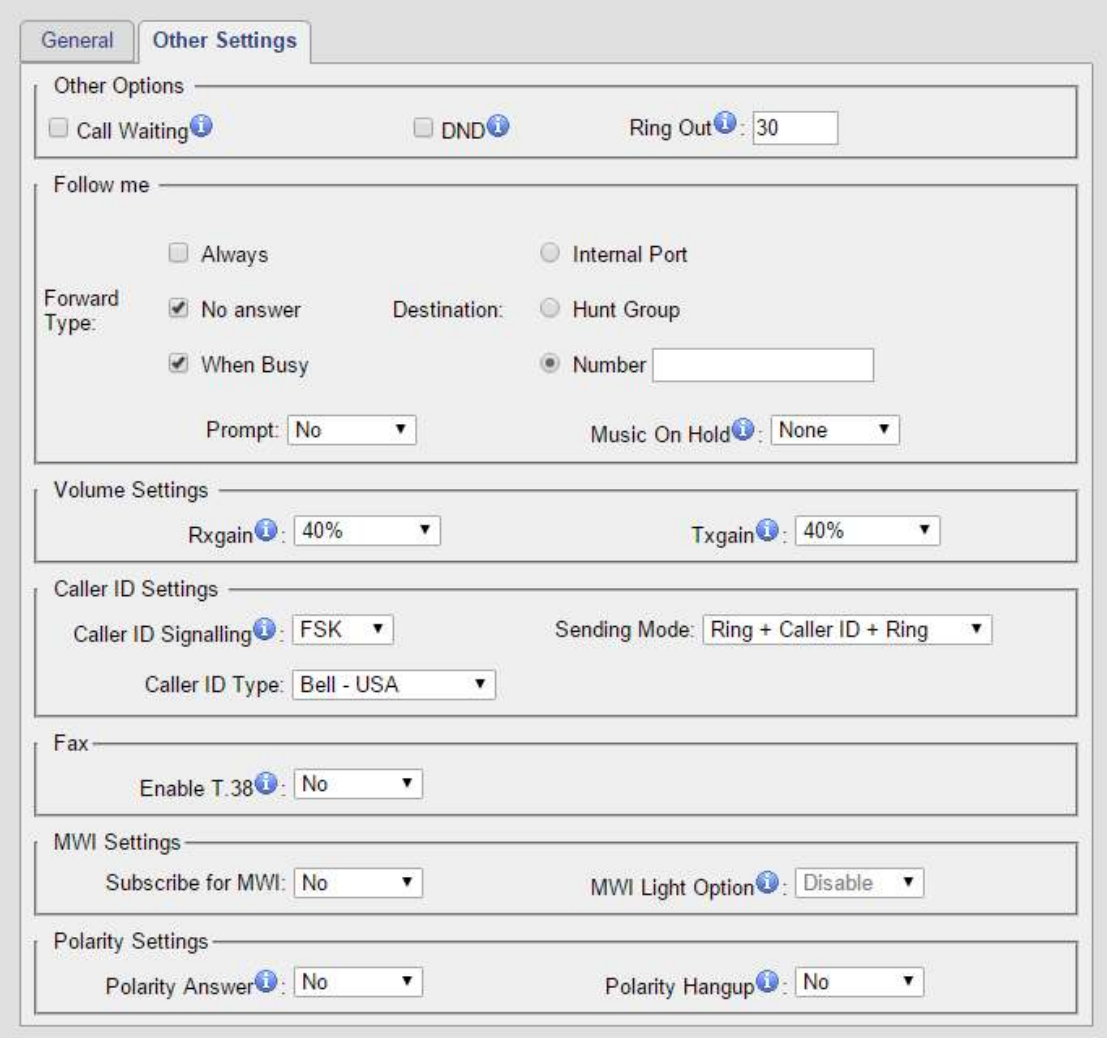


Figure 4-2 FXS Port Other Settings

Table 4-2 Description of FXS Port Other Settings

Follow Me	
Choose the forward type and configure the relevant destination number. In different conditions, the incoming calls to the account will be forwarded to different destinations. • Always: always forward calls to the destination number. • No Answer: forward calls when no one answers the call. • When Busy: forward the call when the account is busy.	
Features	
Call Waiting	Check this option if the extension should have Call Waiting capability. If this option is checked, the “When busy” follow me options will not be available.
DND	Don’t Disturb. When DND is enabled for an extension, the extension will not be available.

Ring Timeout	Check this option if you want to customize the ring time. Ring tone will stop over the time defined.
Volume Settings	
Rxgain	Adjust receive gain.
Txgain	Adjust transmit gain.
Caller ID Settings	
Caller ID Signalling	choose the Caller ID signaling: • FSK • DTMF.
Sending Mode	choose the Caller ID Sending mode: • Ring + Caller ID + Ring • Caller ID + Ring • Polarity + Caller ID + Ring Note: if the FXS port is connected to a device's FXO port, Caller ID settings on FXS port and FXO port should be the same, or the call cannot be established.
Caller ID Type	choose the Caller ID Type: • Bell-USA • V23-UK • V23-NTT Japan
Fax	
Enable T.38	If the FXS port is connected to a Fax machine, this option should be checked.
MWI Settings	
Subscribe for MWI	Message Waiting Indicator (MWI) refers to a special LED on the analog phone, which indicates the voice mail status.
MWI Light Option	There are three lighting methods supported on TA FXS Gateway: neon, FSK and Polarity. Choose the lighting method according to your phone. TA FXS Gateway will light the lamp up once receiving a new message; the lamp will goes off if there is no unread voice mail.
Polarity Settings	
A polarity signal is required on some systems for reverse polarity billing. Select if reverse polarity signal is activated on this FXS port. It is not activated by default. • Polarity Answer: Whether to send polarity signal while picking up the phone. • Polarity Hangup: Whether to send polarity signal while hanging up the phone.	

Hunt Group

Hunt group is a feature that allows a call reaching multiple FXS ports. The FXS ports will act as a single group, called a hunt group. The number of hunt groups is limited by the number of ports each TA FXS Gateway model has. For example, there are 24 hunt groups on TA FXS Gateway2400.

Hunt group will be chosen when configuring the FXS port "Follow Me". The hunt group will work when a call reaches the FXS port associated user which is busy or no answer.

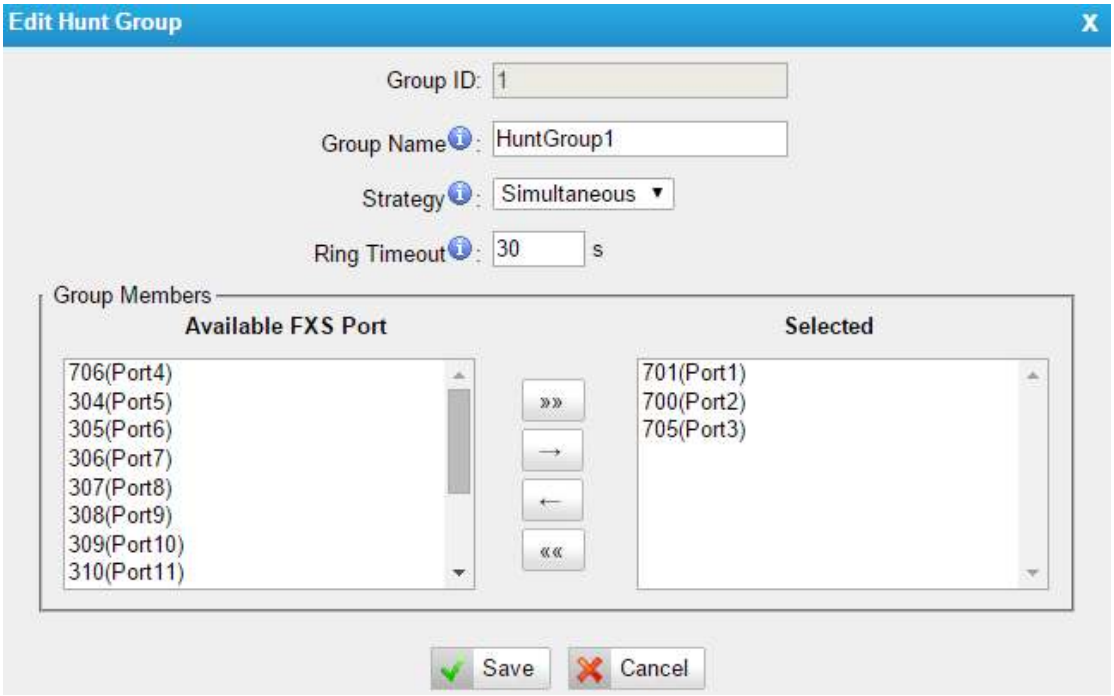


Figure 4-3 Hunt Group

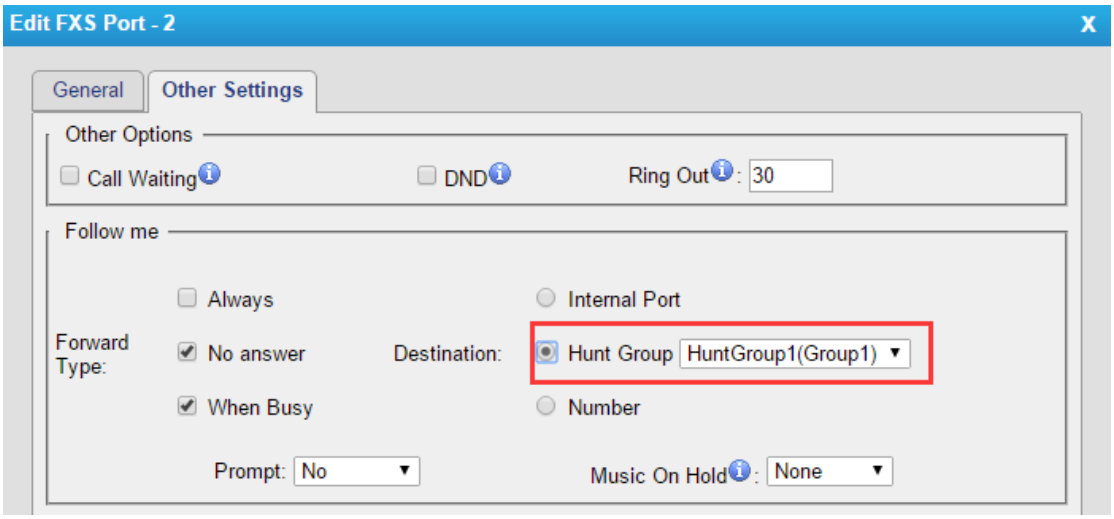


Figure 4-4 Set Hount Group on "FXS Port" Page

There are 3 strategies for hunt group on TA FXS Gateway.

- **Simultaneous**
  All the FXS users will ring at the same time.
- **Circular**
  In circular hunting, the calls are processed "round-robin". If a call is delivered to FXS port1, the next call will go to 2, the next to 3. The succession throughout each of the FXS users even if one of the previous local users becomes free. When the

end of the hunting group is reached, the hunting starts over at the first local users.

- **Linear**
  Linear hunting is also referred to serial hunting. In linear hunting, calls are always delivered to the first FXS users, unless it is busy, then the second, third, and so on.

VoIP Settings

To integrate with other IPPBX, we need to configure the VoIP settings in TA FXS Gateway to set up VoIP trunk (SIP and IAX). In this chapter, we introduce the following settings:

- VoIP Server Settings
- Dial Pattern Template
- SIP Settings
- IAX Settings

VoIP Server Settings

There are some configurable VoIP (SIP/IAX) Server templates on this page. The number of VoIP Server templates is the half of FXS ports on TA FXS Gateway. The VoIP server settings help the FXS ports to register to the VoIP server. Once configured, the templates can be chosen on FXS port setting page.
There are 3 register modes for VoIP server. Users could select one mode for the VoIP server and apply it to FXS ports.

- **Service Provider** - IP Based VoIP Provider, do not generally require the TA gateway to register with the provider. Only IP address or domain is needed to configure on TA gateway.
  Note: this is a peer-to-peer mode to connect VoIP server and TA gateway, you also need to create a service provider trunk connecting to TA gateway on your VoIP server.
- **Port Register** – the VoIP server requires TA gateway to register with the provider using an authentication ID and password.
  If you choose the VoIP server, you need to fill in User Name, Authentication Name and Password to register the FXS port.

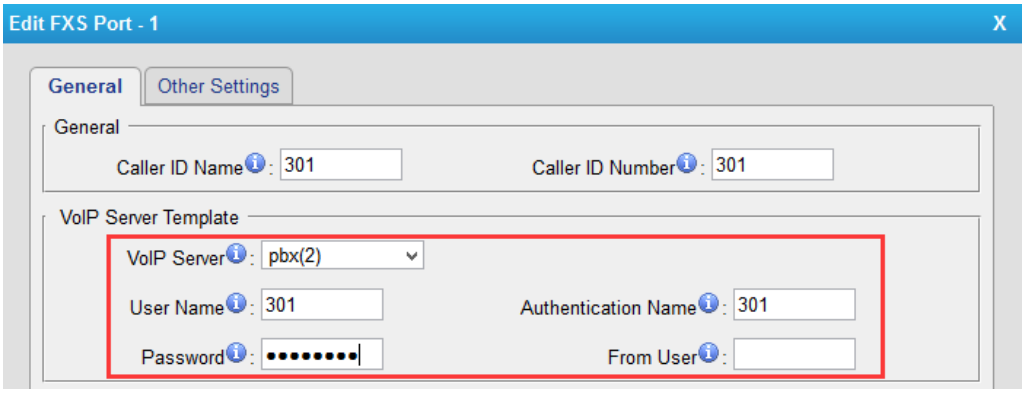


Figure 5-1 Port Register

- **Template Register** – register to your VoIP server and apply the template to FXS ports. The FXS ports will register to the server with the same account.

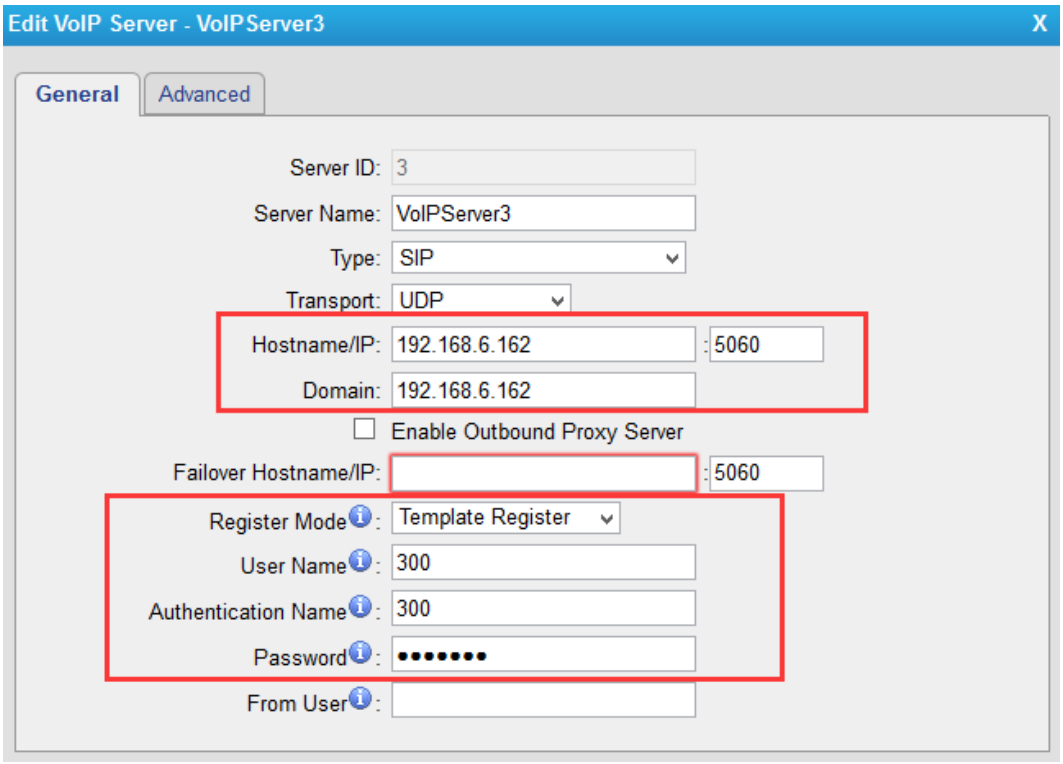


Figure 5-2 Template Register

Check VoIP settings below.

➢ **General**

Table 5-1 Description of VoIP Server General Settings

Items	Description
Server ID	The ID for the VoIP server template.
Server Name	The name for the VoIP server template.
Type	Choose the type of the VoIP server, SIP or IAX.
Transport	This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default),TCP ,and TLS.
Hostname/IP	VoIP server hostname or IP address.5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.
Domain	VoIP server hostname. An IP address also can be filled here.
Enable Outbound Proxy Server	A proxy that receives requests from a client. Even though it may not be the server resolved by the Request-URI.
Failover Hostname/IP	Set the failover server. This server will be used if the primary server is unavailable.
Register Mode	• Port Register: ports will register to this server with individual accounts. • Template Register: ports will register to this server with the

	same account. • Service Provider: disable registration.

➢ **Advanced**

Table 5-2 Description of VoIP Server Advanced Settings

Items	Description
Enable SRTP	Define if SRTP is enabled for this VoIP server.
Qualify	Send check alive packets to the SIP provider.
Caller ID	Specify the caller ID to use when making outbound calls over this VoIP server.
Maxmum Channels	Control the maximum number of simultaneous calls. Set as 0 to specify no maximum.
Realm	Realm is a string to be displayed to users so they know which username and password to use.
Authenticating Incoming Call	When an incoming call reaches TA device and sends INVITE packet to TA, TA responds 401, but the Realm info in 401 Response does not match the Realm set on TA VoIP Server, the provider will refuse to authenticate. If you set this option to No, TA will not reply a 401 Response to the provider to authenticate the incoming call.
DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833
Codec	Define the codec for this sip trunk and its priority. TA1600/2400/3200 supports the following codec: u-law, a-law, G726, G729A/B, GSM, ADPCM, G722, G723, iLBC.

Dial Pattern Template

Dial pattern template specifying how to route the calls from FXS ports to VoIP server extensions or external numbers. The number of dial pattern templates is limited by the number of ports each TA FXS Gateway model has.

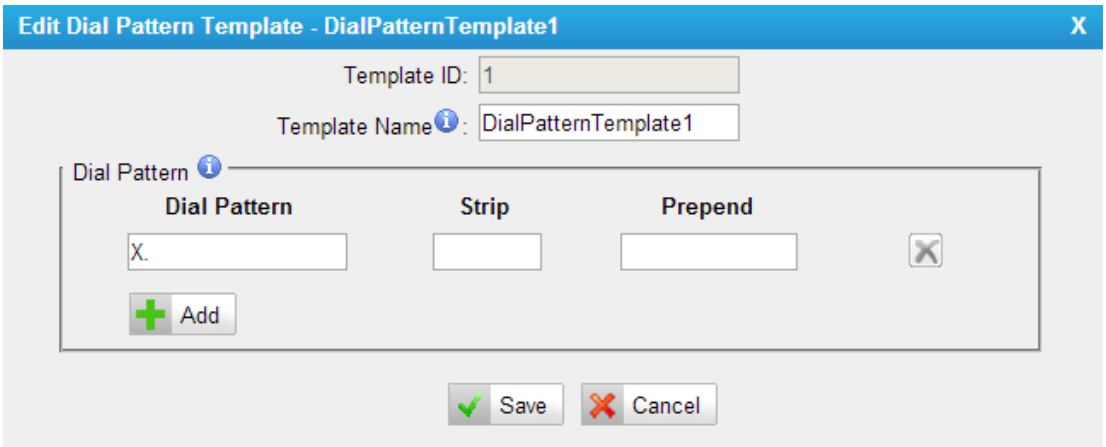


Figure 5-3 Dial Pattern Template

Table 5-3 Description of Dial Pattern Template Settings

Items	Description
Template ID	The ID for this template.
Template Name	A name for this template.
Dial Pattern	Calls from the FXS port should match the dial pattern set on this template, or the call cannot be established. Hover the pointer over to read tips.
Strip	Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed.
Prepend	The digits will be appended to the phone number before the call is placed.
DTMF Mode	Set default mode for sending DTMF of this trunk. Default setting: rfc2833.
Codec	Define the codec for this sip trunk and its priority.

SIP Settings

It is wise to leave the default setting as provided on this page. However, for a few fields, you need to change them to suit your situation.

1) General

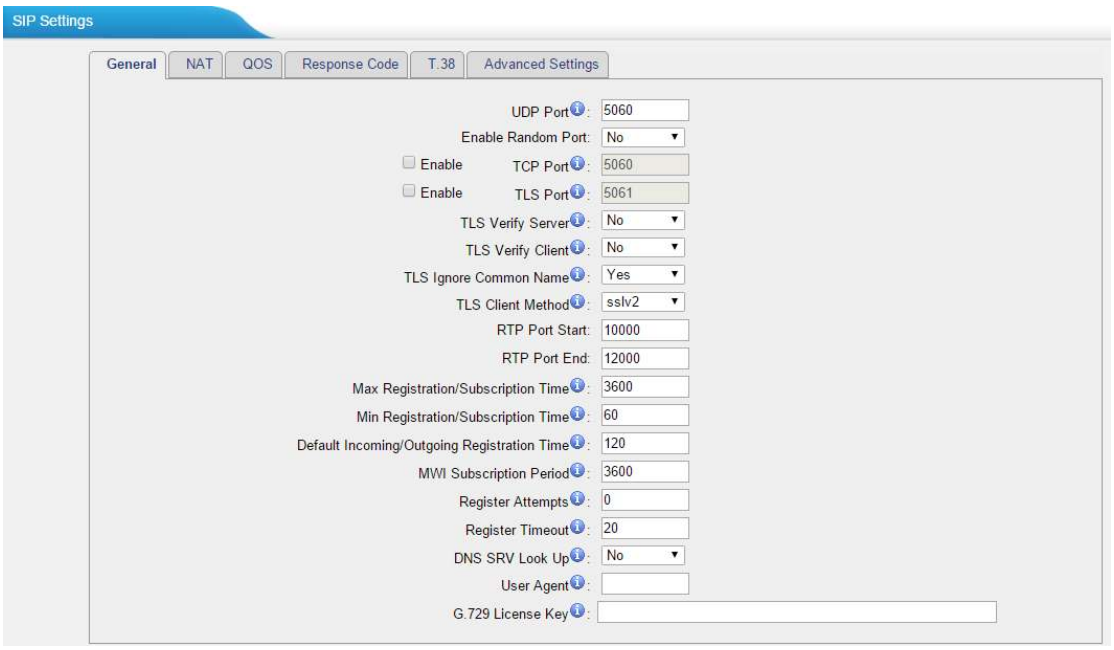


Figure 5-4 SIP General Settings

Table 5-4 Description of SIP General Settings

Items	Description
UDP Port	Port used for SIP registrations. The default is 5060.
Enable Random Port	Enable or Disable Random SIP port.
Random Port Update Interval	Set the Random Port Update Interval.
TCP Port	Port used for SIP registrations. The default is 5060.
TLS Port	Port used for SIP registrations. The default is 5061.
TLS Verify Server	When using TA FXS Gateway as a TLS client, whether or not to verify server's certificate. It is "No" by default.
TLS Verify Client	When using TA FXS Gateway as a TLS server, whether or not to verify client's certificate. It is "No" by default.
TLS Ignore Common Name	Set this parameter as "No", then common name must be the same with IP or domain name.
TLS Client Method	When using TA FXS Gateway as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.
RTP Port Start	Beginning of the RTP port range.
RTP Port End	End of the RTP port range.
DTMF Mode	Set the default mode for sending DTMF. Default setting: rfc2833
Max Registration/Subscription Time	Maximum duration (in seconds) of a SIP registration. The default is 3600 seconds.
Min Registration/Subscription Time	Minimum duration (in seconds) of a SIP registration. The default is 60 seconds.
Default Incoming/Outgoing Registration Time	Default Incoming/Outgoing Registration Time: the default duration (in seconds) of incoming/outgoing registration.
Register Attempts	The number of SIP REGISTER messages to send to a SIP Registrar before giving up. The default is 0 (no limit).
Register Timeout	Number of seconds to wait for a response from a SIP Registrar before classifying the register has timed out. The default is 20 seconds.
Calling Channel Codec Priority	Once enabled, when dialing out via SIP/SPS trunks, the codec of calling channel will be selected preferentially. If not, TA FXS Gateway will follow the priority order in your SIP/SPS trunks.
Video Support	Support SIP video or no. The default is yes.
Max Bit Rate	Configure the max bit rate for video stream. The default: 384kb/s.
DNS SRV Look Up	Please enable this option when your SIP trunk contains

	more than one IP address.
User Agent	To change the user agent parameter of asterisk, the default is “TA FXS Gateway”; you can change it if needed.
G.729 License Key	If you would like to use G.729 codec, please buy the license and enter the license key here.

2) NAT

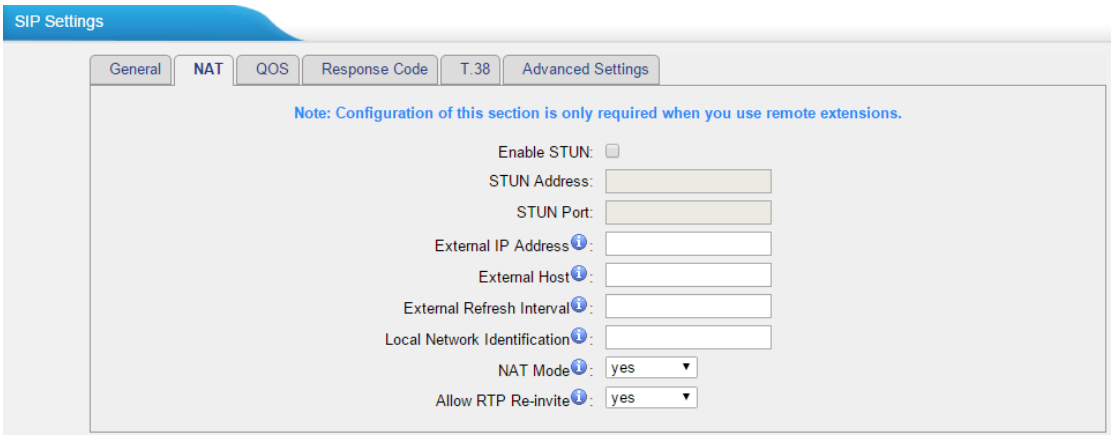


Figure 5-5 NAT Settings

Table 5-5 Description of SIP General Settings

Items	Description
Enable STUN	STUN (Simple Traversal of UDP through NATs) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.
STUN Address	The STUN server allows clients to find out their public address, the type of NAT they are behind and the internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between the client and the VOIP provider and so establish a call.
External IP Address	The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.
External Host	Alternatively you can specify an external host, and the system will perform DNS queries periodically. This setting is only required when your public IP address is not static. It is recommended that a static public IP address is used with this system. Please contact your ISP for more information.
External Refresh Interval	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples of this are as follows: “192.168.0.0/255.255.0.0”: All RFC 1918 addresses are local networks; “10.0.0.0/255.0.0.0”: Also RFC1918; “172.16.0.0/12”:Another RFC1918 with CIDR notation;

	“169.254.0.0/255.255.0.0”: Zero conf local network. Please refer to RFC1918 for more information.
NAT Mode	Global NAT configuration for the system; the options for this setting are as follows: Yes = Use NAT. Ignore address information in the SIP/SDP headers and reply to the sender's IP address/port. No = Use NAT mode only according to RFC3581. Never = Never attempt NAT mode or RFC3581 support. Route = Use NAT but do not include rport in headers.
Allow RTP Reinvite	By default, the system will route media steams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing.

3) Qos

QoS (Quality of Service) is a major issue in VoIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due interference from other lower priority traffic. When the network capacity is insufficient, QoS could provide priority to users by setting the value.

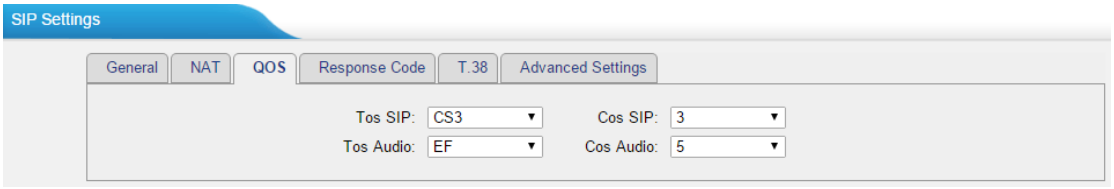


Figure 5-6 Qos

Note: It’s recommended that you configure the QoS in your router or switch instead of TA FXS Gateway side.

4) Response Code

You can change the response code on TA FXS Gateway to the one you want before sending it to the VoIP server. It helps the VoIP server understands better the exact call status, like busy, no response and others.

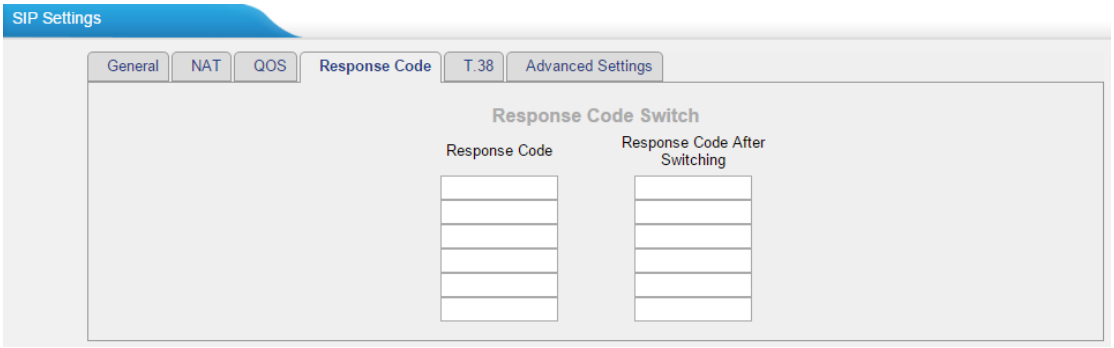


Figure 5-7 Response Code

Note: We don't' recommend configuing this if you are not familiar with the code of call status from the VoIP server.

5) T.38

Settings on this page is for the purpose of improving receiving and sending T.38 FAX.

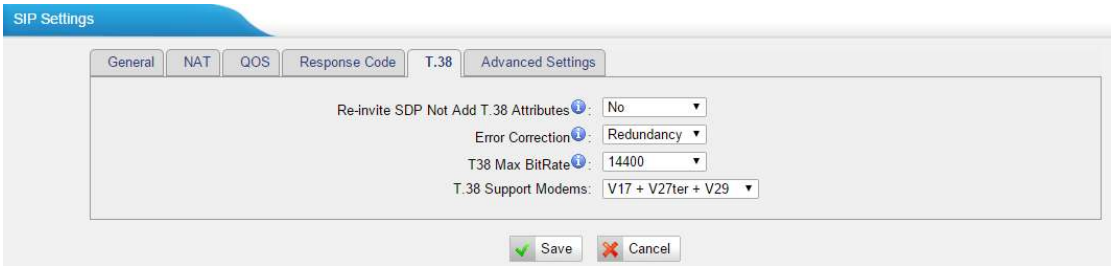


Figure 5-8 T.38 Settings

Table 5-6 Description of T.38 Settings

Items	Description
Re-invite SDP Not Add T.38 Attributes	If set to Yes, SDP in re-invite packet will not add T.38 attributes.
Error Correction	Re-invite SDP T38FaxUdpEc.
T.38 Max BitRate	Set T38 Max BitRate.
T.38 Support Modems	Choose the T.38 modems: • V27ter • V29 • V17 • V27ter + V29 • V17 + V29 • V17 + V27ter + V29

7) Advanced Settings

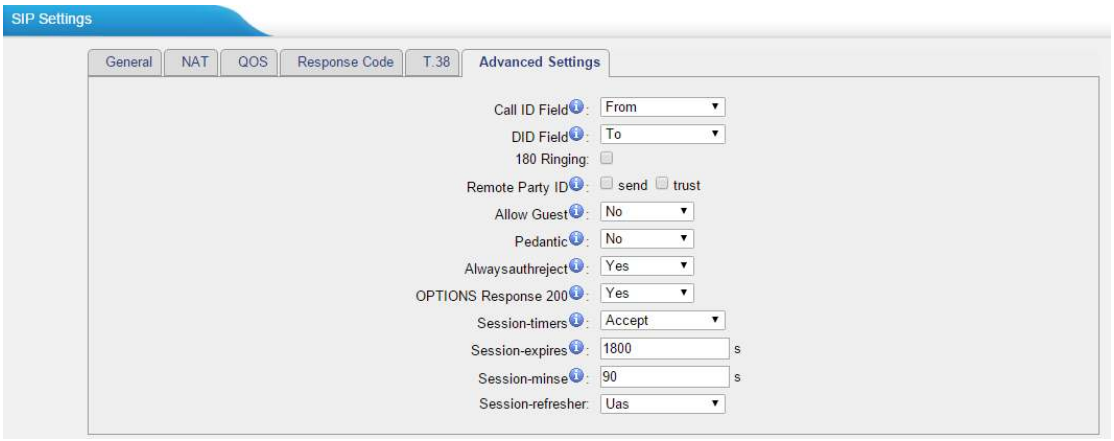


Figure 5-9 SIP Advanced Settings

Table 5-7 Description of SIP Advanced Settings

Items	Description
Call ID Field	Where to get the caller ID in SIP packet.
DID Field	Where to get the DID in SIP packet.
180 Ringing	It is set when the telecom provider needs. Usually it is not needed.
Remote Party ID	Whether to send Remote-Party-ID on SIP header or not. Default: no.
Allow Guest	Whether to allow anonymous registration extension or not. Default: no. It's recommended that it is disabled for security reason.
Pedantic	Enable pedantic parameter. Default: no.
Alwaysauthreject	If enabled, when TA FXS Gateway rejects "Register" or "Invite" packets, TA FXS Gateway always respond the packets using "SIP404 NOT FOUND". It's recommended that it is enabled for security reason.
OPTIONS Response 200	If set to yes, the response to an OPTIONS is always 200OK.
Session-timers	Enable session-timer mode, default: yes. If you find the call is cut off every 15 minutes every time, please disable this.
Session-expires	The max refresh interval
Session-minse	The min refresh interval, which mustn't be shorter than 90s.
Session-refresher	Choose the session-refresher, the default is Uas.

IAX Settings

IAX is the Internal Asterisk Exchange protocol, you can connect to TA FXS Gateway or register IAX trunk to another IAX server. It's supported by the asterisk-based IPPBX.

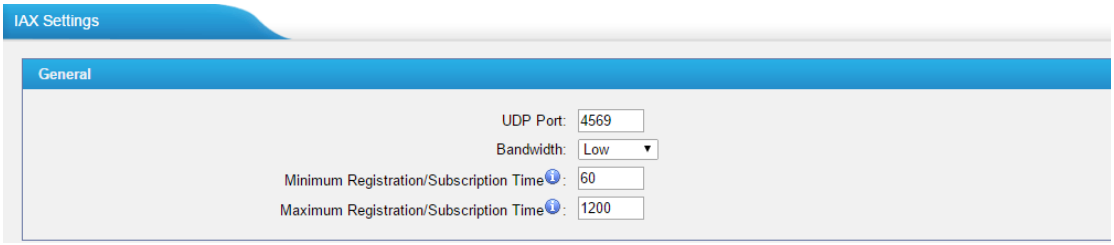


Figure 5-10 IAX Settings

Table 5-8 Description of IAX Settings

Items	Description
UDP Port	Port used for IAX2 registrations. Default is 4569.
Bandwidth	Low/medium/high with this option you can control which codec to be used.
Minimum Registration Time/Subscription Time	Minimum duration (in seconds) of an IAX2 registration. Default is 60 seconds
Maximum Registration Time/Subscription Time	Maximum duration (in seconds) of an IAX2 registration. Default is 1200 seconds.

Gateway Settings

This chapter explains Gateway settings, which can be applied globally to TA1600/2400/3200. The gateway settings can be configured under **Gateway→ Gateway Settings**.

- Basic Preferences
- Feature Codes
- Speed Dial

Basic Preferences

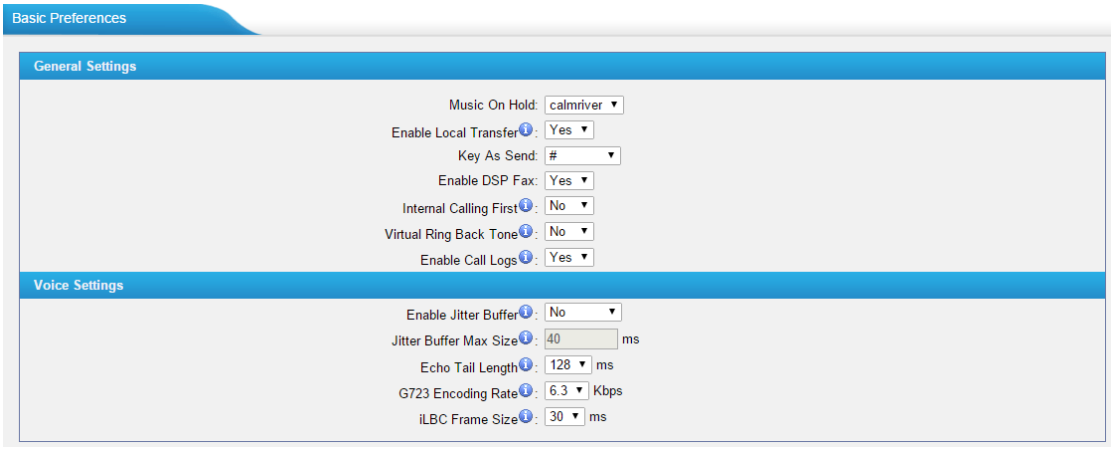


Figure 6-1 Basic Preferences

Table 6-1 Basci Preferences

General Settings	
Music On Hold	Set hold music for the system.
Enable Local Transfer	By default, the system will use the transfer rules set in TA1600/2400/3200. If the option is set to “No”, the system will use the transfer mechanism of the SIP trunk.
Key As Send	Set the "#" or "*" to perform as a send key while dialing. Default is "#".
Enable DSP Fax	Enable DSP to optimize Fax reception.
Internal Calling First	If set to “Yes”, when making calls between internal ports (through Caller ID Number), system will call the destination port directly without VoIP server, or through VoIP server as priority if set to “No”.
Virtual Ring Back Tone	Once enabled, when the caller dials out, the caller will only hear the virtual ring back tone generated by the system before the callee answers the call.
Enable Call Logs	If set to “Yes”, the system will store the call logs.

	If set to “No”, the call logs will not be kept anymore, but the call logs stored previously will be there.
Voice Settings	
Enable Jitter Buffer	Forces the use of a jitter buffer on the received side of a SIP channel. The call quality will be improved if this option is enabled.
Jitter Buffer Max Size	Max length of the jitter buffer. Default is 40 milliseconds
Echo Tail Length	In some cases, the echo canceller doesn’t train quickly enough and there is echo at the beginning of the call which then quickly fades out.
G723 Encoding Rate	Set the G723 encoding rate.
iLBC Frame Size	Set the iLBC packet frame size.

Feature Codes

There are various feature codes on TA1600/2400/3200. The feature codes are used to acquire the gateway info or activate and inactivate supplementary services. The default feature codes are illustrated below. The parameters for feature codes are configurable.

- **General**

Table 6-2 Description of General Feature Code

Items	Default	Description
Internal Call Prefix	*99	Dial the feature code and the FXS port number when making calls between the analog phones connected to multiple ports of the TA FXS Gateway without the use of a VoIP server.
Speed Dial Prefix	*98	The prefix number for applying a speed dialing. The prefix should be added ahead of the speed dial number.
Attended Transfer	*3	Users may transfer an incoming call by dialing *3 on their phone.
Blind Transfer	*03	Users may blind transfer an incoming call by dialing*03 on their phone.
Direct IP Calling	*96	Direct IP calling allows two parties, that is, a FXS Port with an analog phone and another VoIP Device, to talk to each other in an ad hoc fashion without a SIP proxy. The default "Direct IP Calling" feature code is *96. For detailed instruction, please refer to Basic Operation.
Check Number	*97	Users can check the analog phone's number by simply dialing the "Check Number" feature code on the phone. The default "Check Number" feature code is *97.
Voice Menu	***	Users may enter the voice prompt menu by pressing ***

		on their phone.
Voice Menu Password Settings	123456	The password of voice menu is required before entering the advanced settings. The default password is 123456.

- **Call Forwarding Preferences**

Table 6-3 Description of Call Forwarding Preferences

Items	Default	Description
Reset to Defaults	*70	Users may reset all call forwarding defaults by calling *70 on their phone.
Enable Forward All Calls	*71	Users may enable always forward by calling *71 on their phone.
Disable Forward All Calls	*071	Users may disable always forward by calling *071 on their phone.
Enable Forward When Busy	*72	Users may enable busy forward by dialing *72 on their phone.
Disable Forward When Busy	*072	Users may disable busy forward by calling *072 on their phone.
Enable Forward No Answer	*73	Users may enable no answer forward by calling *73 on their phone.
Disable Forward No Answer	*073	Users may disable no answer forward by calling *073 on their phone.
Forward to Internal Port	*74	Users may activate call forwarding to port by dialing this feature code, followed by the port ID to forward all calls to.
Forward to Number	*75	Users may activate call forwarding by dialing this feature code, followed by the extension or phone number to forward all calls to this number. **Note**: users may activate Forward to number by dialing *75 + phone number. E.g. by dialing *75501, all calls will be forwarded to extension 501.
Forward to Hunt Group	*76	Users may activate call forwarding to hunt group by dialing code, followed by the hunt group ID to forward all calls to.
Enable Do Not Disturb	*77	Activate "Do Not Disturb". Once activated, the FXS port will reject all incoming calls.
Disable Do Not Disturb	*077	Disable "Do Not Disturb" for the FXS port by pressing the feature code on the phone. It will recover normal ringing upon the arrival of incoming calls.

Speed Dial

Speed Dial feature is available on TA1600/2400/3200 that allowing you to place a call by pressing a reduced number of keys. There are 16 configurable Speed Dial templates available on TA1600/2400/3200.

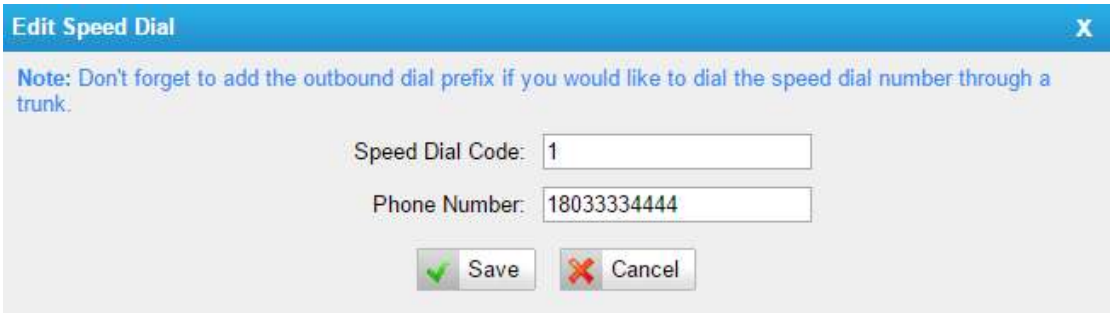


Figure 6-2 Speed Dial

- **Speed Dial Code**
  The speed dialing number.
- **Phone Number**
  The number you want to call.

To make a speed dial, e.g. you want to call 18033334444, simply dial *981. The *98 tells TA1600/2400/3200 that you want to use the Speed Dial and the 1 is the Speed Dial Code for destination number 18033334444.

Note: do not forget to add the dial pattern according to the selected dial pattern template. That is the destination number should match the FXS port dial pattern.

Prompt Settings

This chapter explains prompt settings on TA1600/2400/3200.

- Custom Prompts
- Music on Hold Prompts
- System Prompts

Custom Prompts

We can upload the prompts in this page; you can also download it and save it as a backup.

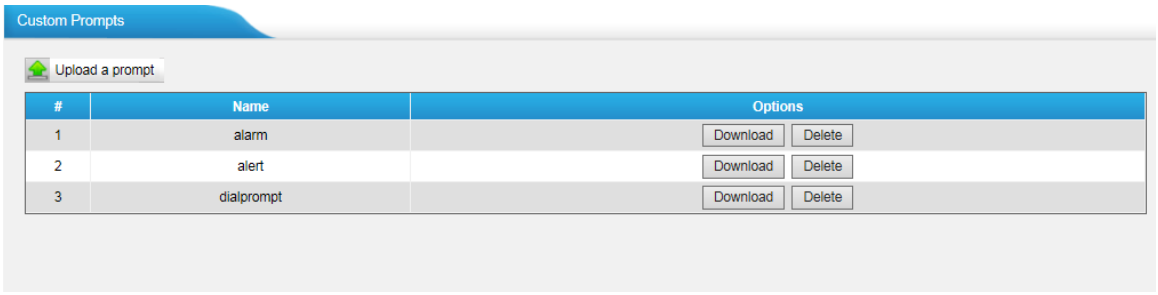


Figure 7-1 Custom Prompts

The administrator can upload prompts by doing the following:

1) Click “Upload Prompt”.
2) Click “Browse” to choose the desired prompt.
3) Click “Upload” to upload the selected prompt.

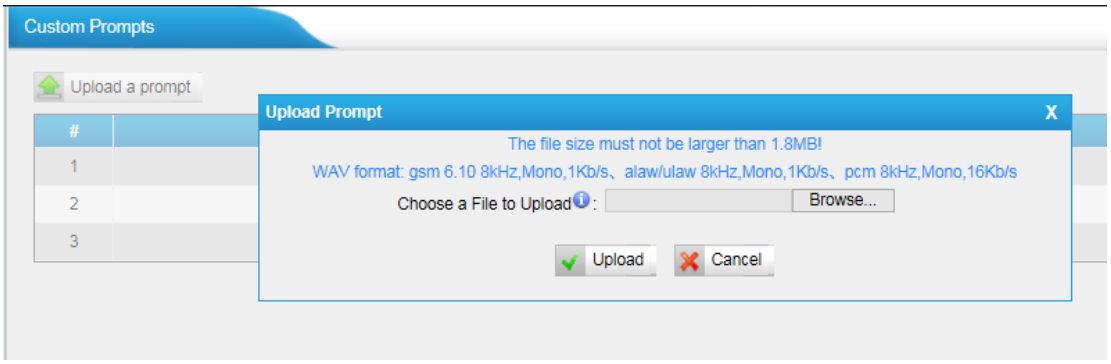


Figure 7-2 Upload A Prompt

Note: The file size must not be larger than 1.8 MB, and the file must be WAV format:
GSM 6.10 8 kHz, Mono, 1 Kb/s;
Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
PCM 8 kHz, Mono, 16 Kb/s.

Music on Hold Prompts

In this page, we can upload the music on hold prompts.

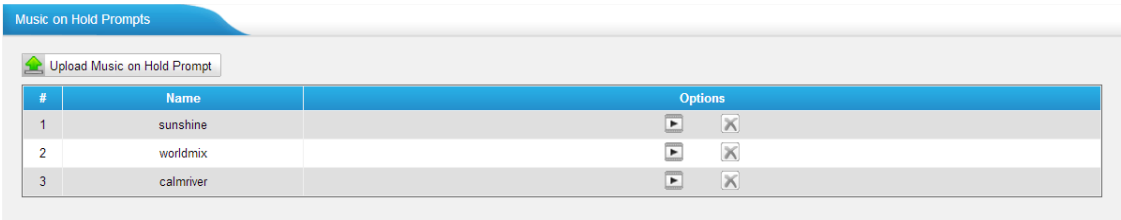


Figure 7-3 Music On Hold

The administrator can upload on hold music as follows:
1) Click “Upload Music on Prompt”.
2) Click “Browse” to choose the desired audio file.
3) Click “Upload” to upload the selected file.

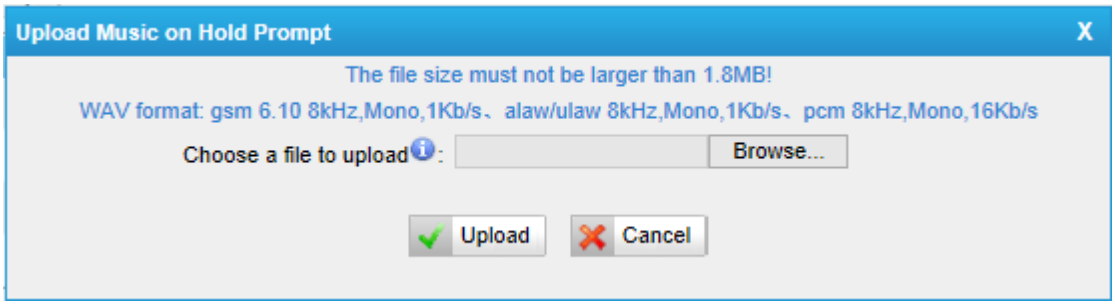


Figure 7-4 Upload Music on Hold Prompt

Note: The file size must not be larger than 1.8 MB, and the file must be WAV format:
GSM 6.10 8 kHz, Mono, 1 Kb/s;
Alaw/Ulaw 8 kHz, Mono, 1 Kb/s;
PCM 8 kHz, Mono, 16 Kb/s.

System Prompts

TA FXS Gateway supports Chinese and English system prompts. You can download the appropriate language you need.

Notes:

1. Auto-detection is highly recommended. But if you prefer to download via HTTP or TFTP server, please contact the local dealer for the prompts.
2. When update successfully, just click “Apply Changes” on Web then it will take effect, there is no need to reboot.



Figure 7-5 System Prompts Settings Page

Advanced Settings

This chapter explains SIP settings and Distinctive Ringtones.

- Distinctive Ringtones
- Tone Zone Settings
- RADIUS Settings

Distinctive Ringtones

TA1600/2400/3200 provides 10 configurable distinctive ringtones. Users could configure different ringtones to match different incoming caller ID.

For example, if Inbound Caller Pattern is configured as “100.”, all the incoming calls start with digits “100” will ring using cadence “2000,4000” as the following figure shows.

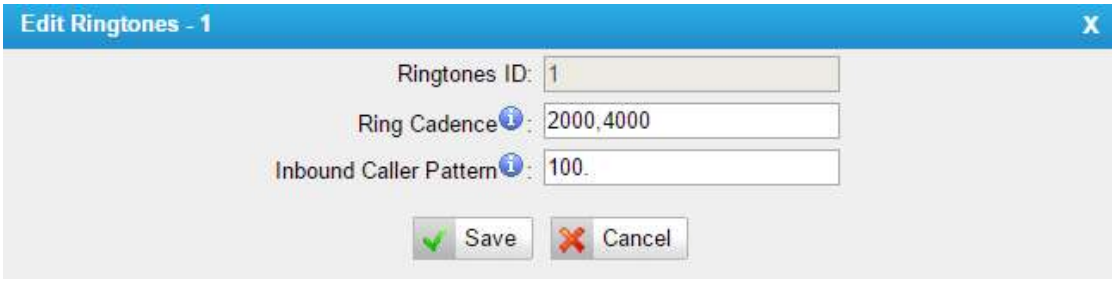


Figure 8-1 Distinctive Ringtones

Tone Zone Settings

Advanced ring tones for all the FXS ports can be configured on this page. There are pre-grogrammed tone zone settings for some countries and regions. Users can simply find and select thier country to get tone zone settings for the gateway.

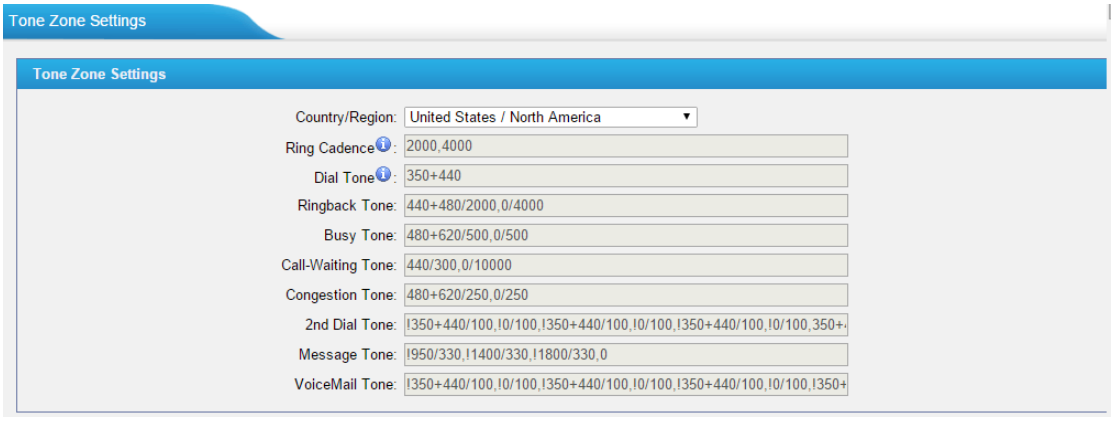


Figure 8-2 Tone Zone Settings

Users may also configure the tone zone according to the national standard by selecting "User custom for Tone Zone". Please refer to the document below and

configure the tone zone settings on TA FXS Gateway:
http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf

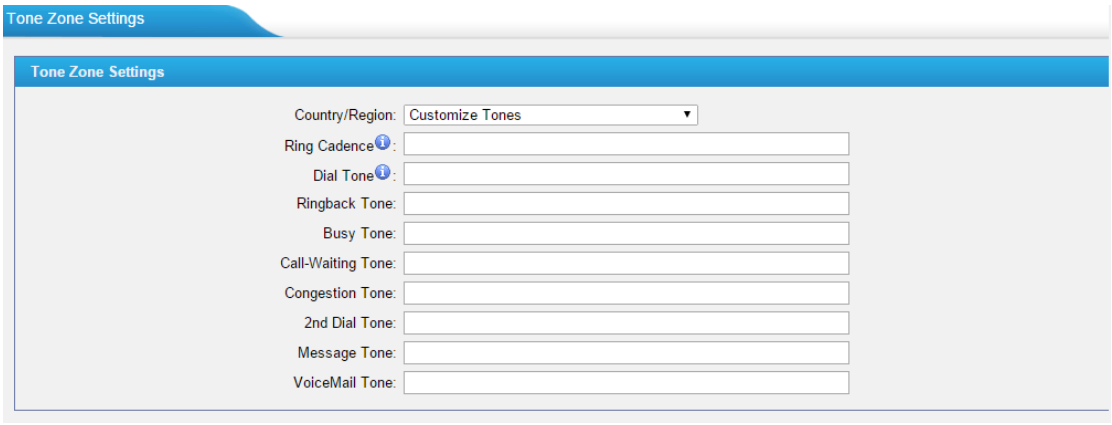


Figure 8-3 Customize Tones

Table 8-1 Description of Tone Zone Settings

Items	Description
Country/Region	Choose the country to get pre-programmed tone zone settings or choose "User custom for Tone Zone" to configure the settings manually.
Ring Cadence	Configuration option for all FXS ports ring cadence for all incoming calls.
Dial Tone	Prompt tone of off-hook dial tone.
Ringback Tone	The tone sent to caller when ringing is on.
Busy Tone	Used for busy line prompt.
Call-Waiting Tone	Used for notification in call waiting.
Congestion Tone	Used to indicate that an invalid code has been dialed, or that all circuits (trunks) are busy and/or the call is unroutable.
2nd Dial Tone	Used for the second stage dial tone.
Message Tone	Used for message tone.
VoiceMail Tone	Used for voicemail tone.

RADIUS Settings

TA FXS Gatewaysupports RADIUS (Remote Authentication Dial In UserService) protocol. RADIUS feature is mainly for billing purpose on TA FXS Gateway. There areprimary and secondary RADIUS server configurations available. Once the primary server is unreachale, the RADIUS requests will be sent to the secondary server.

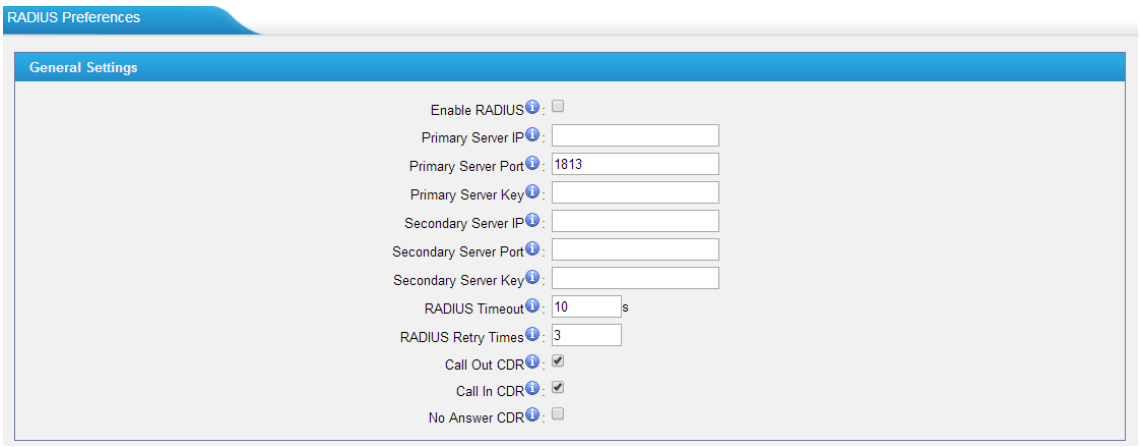


Figure 8-4 RADIUS Settings

Table 8-2 Description of RADIUS Settings

Items	Description
Enable RADIUS	Enable RADIUS on TA FXS Gateway.
Primary Server IP	Set IP address of the primary server.
Primary Server Port	Default is 1813. Specifies the port to be used for the primary RADIUS account.
Primary Server Key	Specifies the key to be used to authenticate the RADIUS connection to the Primary server. The key is set according to the RADIUS server.
Secondry Server IP	Set IP address of the primary server. The second sever will be activated the primary one becomes unusable.
Secondry Server Port	Default is 1813. Specifies the port to be used for the second RADIUS account.
Secondry Server Key	Specifies the key to be used to authenticate the RADIUS connection to the second server. The key is set according to the RADIUS server.
RADIUS Timeout	Specifies the number of seconds to wait for a response after the RADIUS message is sent to the server. Default: 10 seconds. The retransmission will be performed if there is no response after the timeout.
RADIUS Retry Times	Specifies the number of times the RADIUS messages will send to the RADIUS server before giving up. Default: 3.
Call Out CDR	Whether to send "Call Out CDR" to RADIUS server or not.
Call In CDR	Whether to send "Call In CDR" to RADIUS server or not.
No Answer CDR	Whether to send "Call Out CDR" to RADIUS server or not.

Network Preferences

This chapter explains network settings on TA1600/2400/3200. Click the main menu 

on the top of the Web GUI to check the network settings.

- LAN Settings
- Service
- VLAN Settings
- VPN Settings
- DDNS Settings
- Static Route
- SNMP Settings
- TR-069 Settings

LAN Settings

After successfully logging in the TA1600/2400/3200 Web GUI for the first time, users could go **System→Network Preferences→LAN Settings** to configure the network for TA1600/2400/3200.

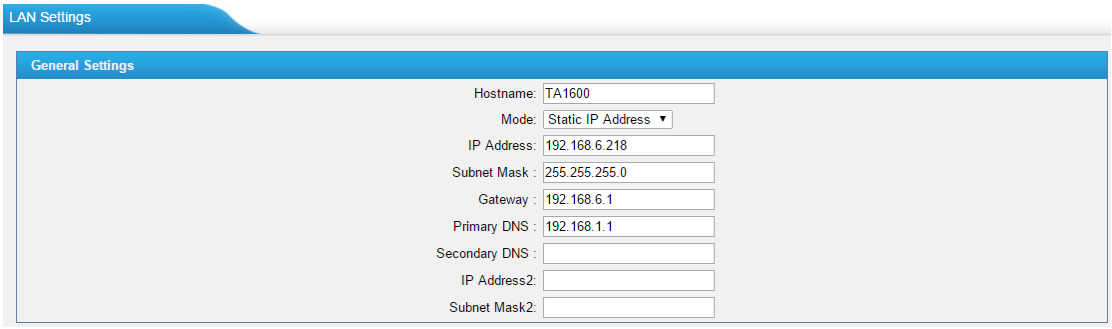


Figure 9-1 LAN Settings

Table 9-1 LAN Settings

Items	Description
Hostname	Set the host name for TA1600/2400/3200.
Mode	Choose the network mode: • Static IP Address • DHCP • PPPoE
IP Address	Set the IP Address for TA1600/2400/3200.
Subnet Mask	Set the subnet mask for TA1600/2400/3200.
Gateway	Set the gateway for TA1600/2400/3200.
Primary DNS	Set the primary DNS for TA1600/2400/3200.

Secondary DNS	Set the secondary DNS for TA1600/2400/3200.
IP Address2	Set the second IP Address for TA1600/2400/3200.
Subnet Mask2	Set the second subnet mask for TA1600/2400/3200.

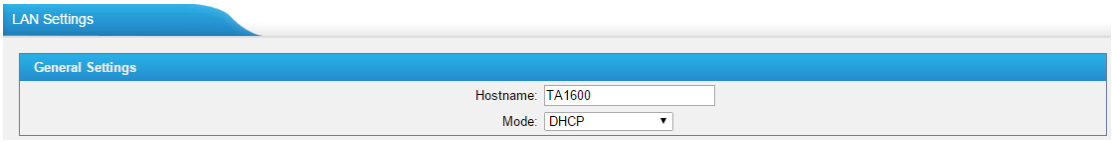


Figure 9-2 DHCP Mode

Select DHCP mode to get network automatically from the local network.

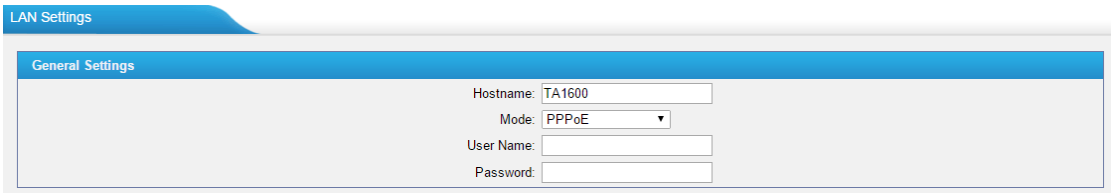


Figure 9-3 PPPoE

Fill in user name and password to access the Internet via PPPoE.

Service

The administrator can manage all the access methods on TA on the "Service" page.

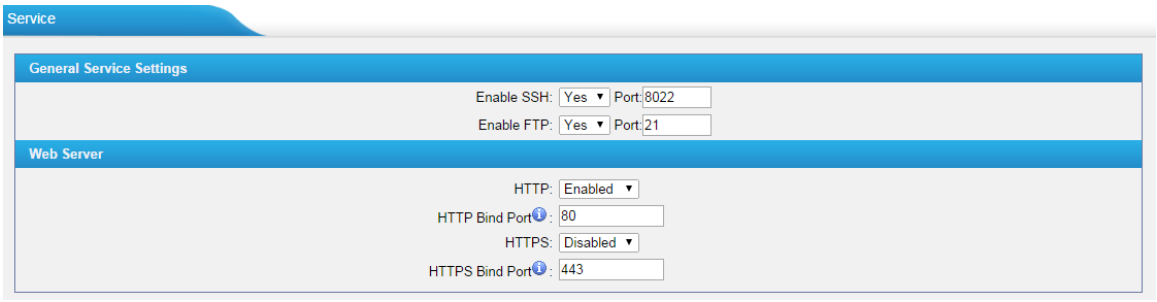


Figure 9-4 Service Settings

Table 9-2 Description of Service Settings

Items	Description
SSH	By using SSH, you can log in to TA1600/2400/3200 and run commands. It's disabled by default. We don't recommend enabling it if not needed. The default port for SSH is 8022.
FTP	FTP access; The default port is 21.
HTTP	HTTP web access; The default port is 80.

HTTPS	HTTPS web access, it is disabled by default, and you can enable it to get safer web access.

VLAN Settings

VLAN (Virtual Local Area Network) is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.
A VLAN is a broadcast domain created by switches. This means the VLAN is configured on switches, layer 3 switches. Note that some of the switches don't support VLAN.

Note:
TA1600/2400/3200 acts as a VLAN client, a 3-layer switch is needed.

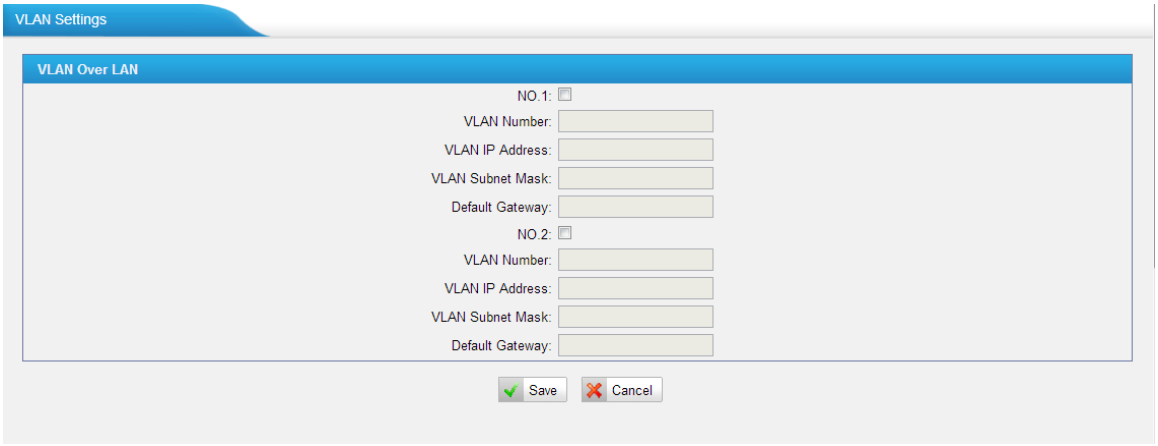


Figure 9-5 VLAN Settings

Please follow the steps below to set up VLAN on TA1600/2400/3200.
Step1. Create VLANs on your switch.
Step2. Allocate a VLAN ID and IP address for TA1600/2400/3200.
Step3. Configure VLAN settings page on TA1600/2400/3200.

VPN Settings

A virtual private network (VPN) is a method of computer networking typically using the public internet that allows users to privately share information between remote locations, or between a remote location and a business' home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely. TA1600/2400/3200 supports OpenVPN.

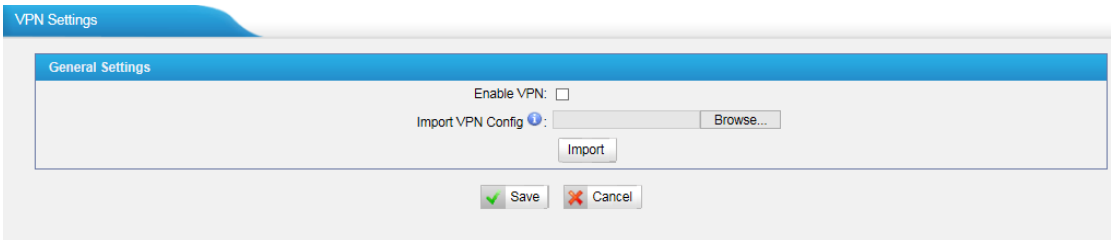


Figure 9-6 VPN Settings

- **Enable VPN**
  Enable VPN feature.

- **Import VPN Config**
  Import configuration file of OpenVPN.

Notes:

1. Uncomment “user” and “group” in the “config” file. You can get the config package from the OpenVPN provider.
2. TA1600/2400/3200 works as VPN client mode only.

DDNS Settings

DDNS(Dynamic DNS) is a method/protocol/network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information.

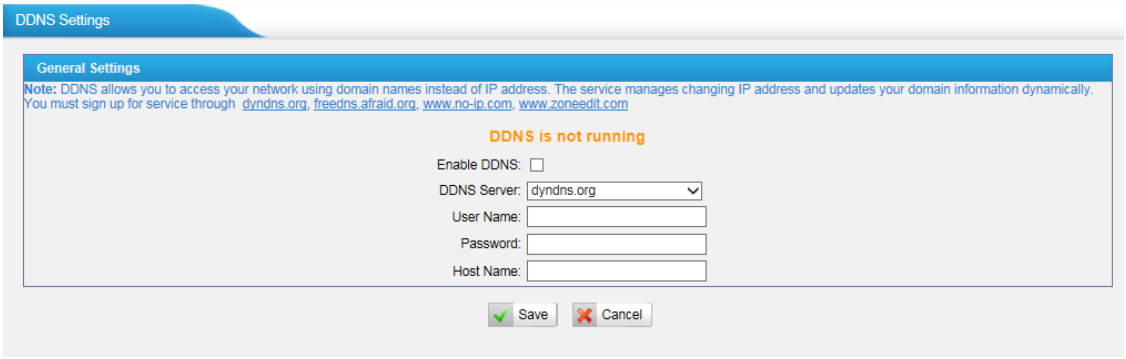


Figure 9-7 DDNS Settings

Table 9-3 Description of DDNS Settings

Items	Description
DDNS Server	Select the DDNS server you sign up for service.
User Name	User name the DDNS server provides you.
Password	User account’s password.

Host Name	The host name you have got from the DDNS server

Note: DDNS allows you to access your network using domain names instead of IP address. The service manages changing IP address and updates your domain information dynamically. You must sign up for service through dyndns.org, freedns.afraid.org, www.no-ip.com, www.zoneedit.com.

Static Route

TA FXS Gateway will have more than one Internet connection in some situations but it has only one default gateway. You will need to set some Static Route for TA FXS Gateway to force it to go out through different gateway when accessing to different internet.

The default gateway priority of TA FXS Gateway from high to low is VPN/VLAN →LAN port.

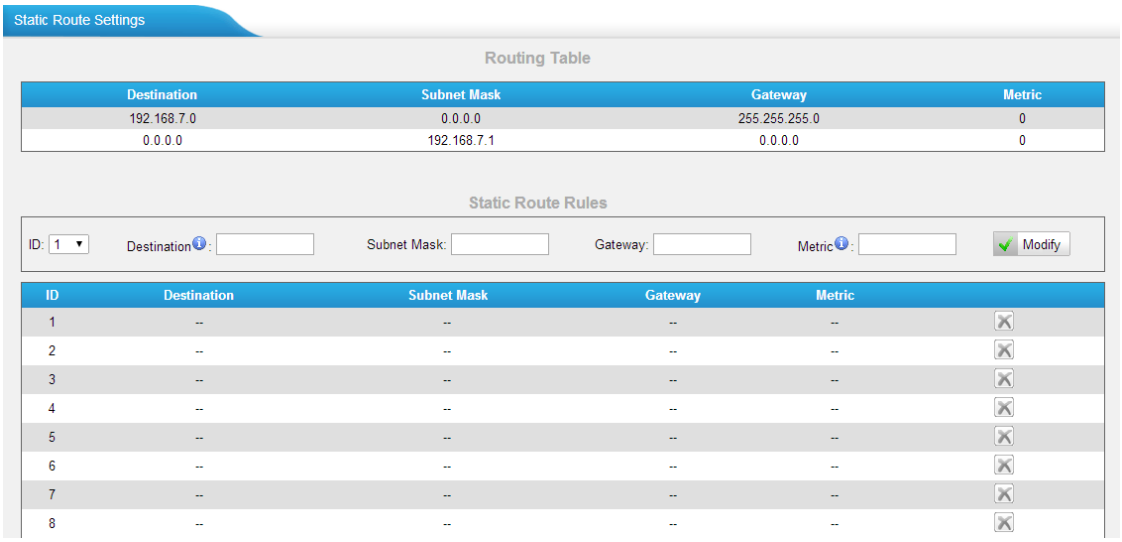


Figure 9-8 Static Route

1) Route Table

The current route rules of TA FXS Gateway.

2) Static Route Rules

You can add new static route rules here.

Table 9-4 Description of Static Route Settings

Items	Description
Destination	The destination network to be accessed to by TA FXS Gateway.
Subnet Mask	Specify the destination network portion.
Gateway	Define which gateway TA FXS Gateway will go through when accessing the destination network.
Metric	The cost of a route is calculated by using what are called routing

	metric. Routing metrics are assigned to routes by routing protocols to provide measurable statistic which can be used to judge how useful (how low cost) a route is.
Interface	Define which internet port to go through.

SNMP Settings

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. TA FXS gateway supports three versions: V1, V2C and V3.

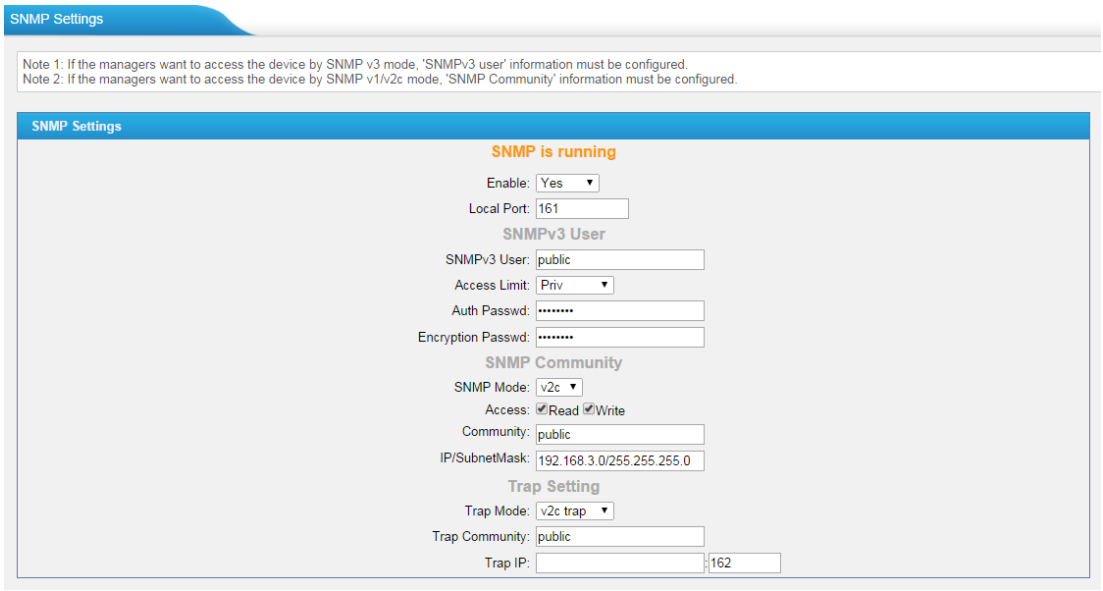


Figure 9-9 SNMP Settings

TR-069 Settings

TR-069 (Technical Report 069) is a Broadband Forum (formerly known as DSL Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS).

Yeastar TA1600/2400/3200 acts as a CPE, enable TR-069 and configure the parameters in the corresponding fields, if configured correctly, the gateway will establish the TR-069 session with the ACS.

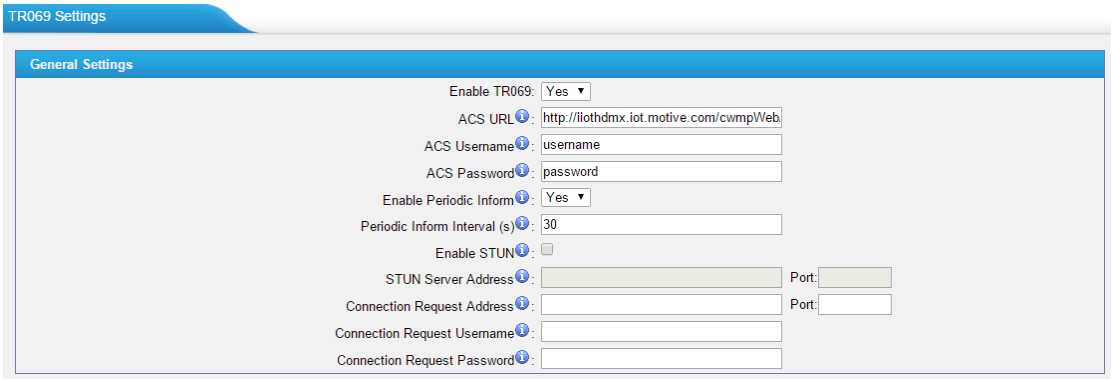


Figure 9-10 TR-069 Settings

Table 9-5 Description of TR-069 Settings

Items	Description
ACS URL	URL of the TR-069 ACS. This is the URL the Yeastar CPEs will send TR-069 messages to.
ACS Username	Username for HTTP authentication against the ACS. Leave it blank if no ASC username.
ACS Password	Password for HTTP authentication against the ACS. Leave it blank if no ASC password.
Enable Periodic Inform	Set the Yeastar device to start a new session after “Periodic Inform Interval”.
Periodic Inform Interval(s)	Time in seconds where the CPE will initiate a new session against the ACS.
Enable STUN	Enable this option to discover the CPE’s public IP address if it is located behind a NAT.
STUN Server Address/Port	The STUN Server address and port.
STUN Server Username	The STUN Server username.
STUN Server Password	The STUN server password.
Connection Request Address	HTTP URL for an ACS to make a Connection Request notification to the CPE.
Connection Request Username	Username used to authenticate an ACS making a Connection Request to the CPE. Leave it blank if no username.
Connection Request Password	Password used to authenticate an ACS making a Connection Request to the CPE. Leave it blank if no password.

Security Center

This chapter describes how to secure your TA1600/2400/3200. It is strongly recommended that users configure firewall and other security options on TA1600/2400/3200 to prevent the attack fraud and the system failure or calls loss.

- Security Center
- Alert Settings
- AMI Settings
- Certificates
- Firewall Rules
- IP Blacklist

Security Center

All the security settings including Firewall, Service, Port Settings in TA1600/2400/3200 are displayed in Security Center. Users could rapidly check and configure the relevant security settings here.

1) Firewall

In the “Firewall” tab, users could check firewall configuration and alert settings. By clicking the relevant button, you can enter the configuration page directly.

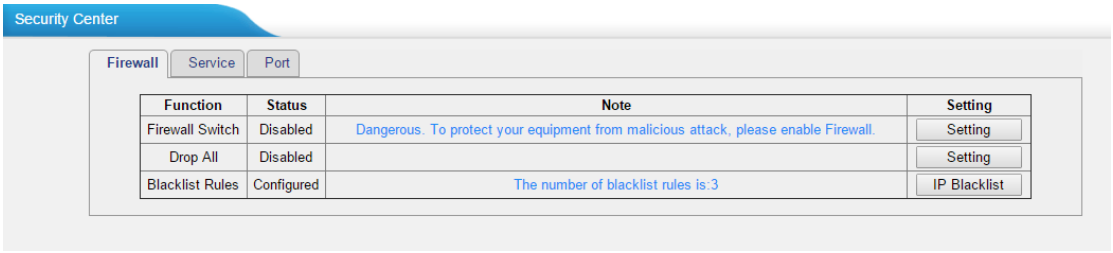


Figure 10-1 Security Center—Firewall

2) Service

In “Service” tab, you can check AMI/SSH status. For AMI/SSH, you can enter the according page by clicking the button in “Setting” column.

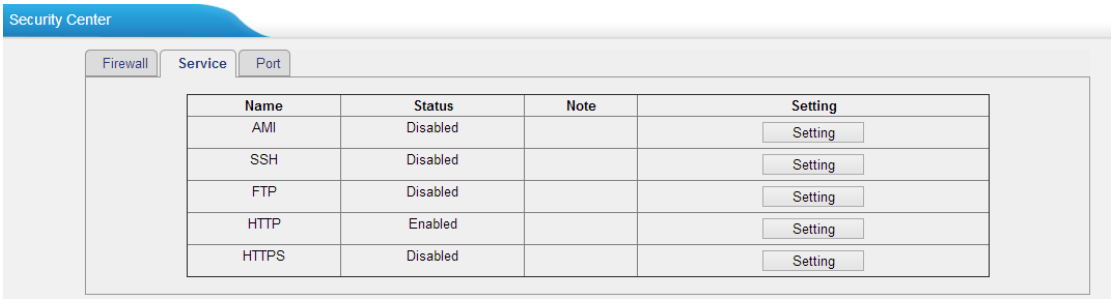


Figure 10-2 Security Center—Service

3) Port

In “Port” tab, you can check SIP port and HTTP port. You can also enter the relevant page by clicking the button in “Setting” column.

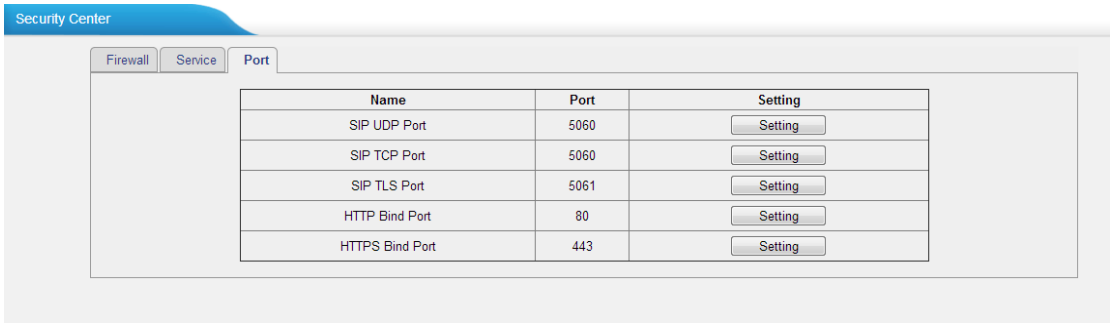


Figure 10-3 Security Center—Port

Alert Settings

If the device is under attack, the system will alert users via call or E-mail.
The attack modes include IP attack and Web Login.

- **IPATTACK**
  When the system is attacked by IP address, the firewall will add the IP to auto IP Blacklist and notify the user if it matches the protection rule.
- **WEBLOGIN**
  Web Login Alert Notification: entering the wrong password consecutively for five times when logging in TA FXS Gateway Web interface will be deemed as an attack, the system will limit the IP login within 10 minutes and notify the user.

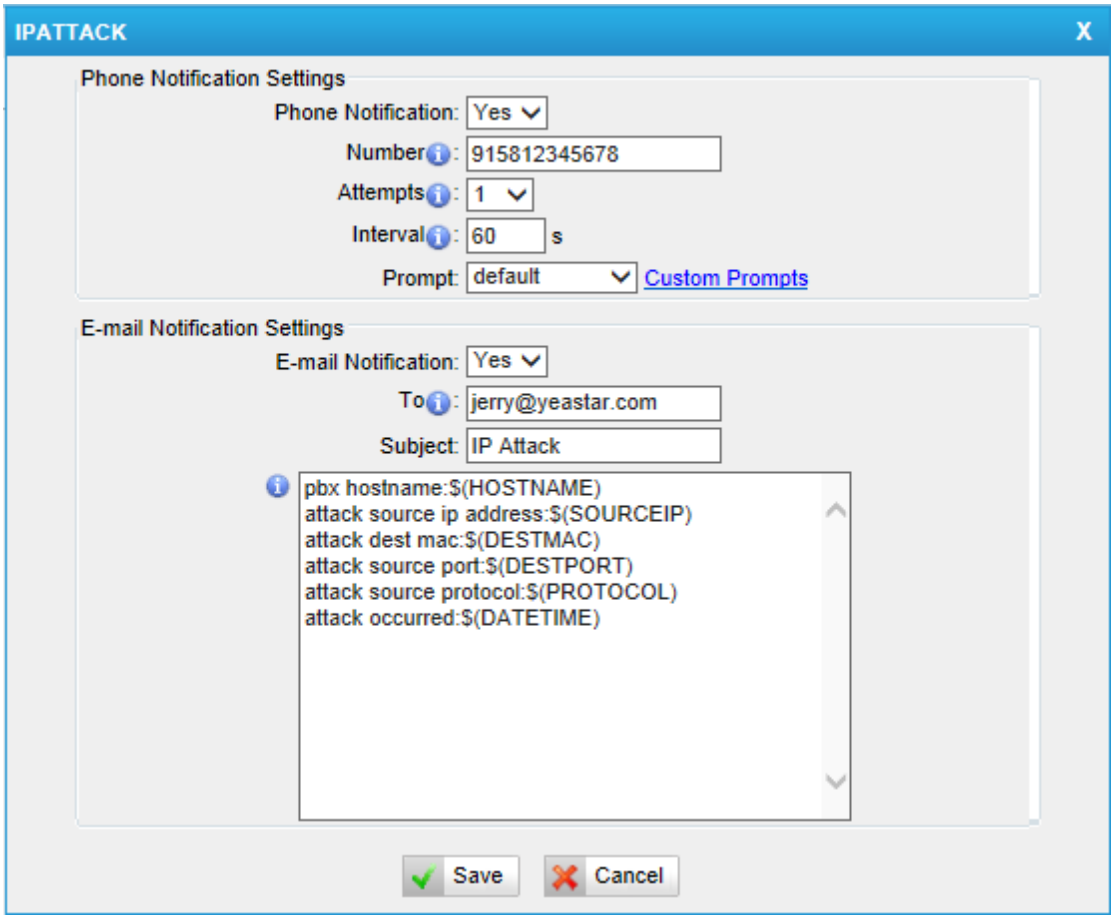


Figure 10-4 Alert Settings

Table 10-1 Description of Alert Settings

Phone Notification Settings	
PHONE Notification	Whether to enable phone notification or not.
Number	The numbers could be set for alert notification; users can setup multiple extension and outbound phone numbers. Please separate them by ";". Example: "500;9911", if the extension has configured Follow Me Settings, the call would go to the forwarded number directly.
Attempts	The attempts to dial a phone number when there is no answer.
Interval	The interval between each attempt to dial the phone number. Must be longer than 3 seconds, the default value is 60 seconds.
Prompt	Users will hear the prompt while receiving the phone notification.
Email Notification Settings	
E-mail Notification	Whether to enable E-mail Notification or not.

Recipient's Name	The recipients for the alert notification, and multiple email addresses are allowed, please separate them by ";". E.g. jerry@yeastar.com;jason@yeastar.com,456@sina.com
Subject	The subject of the alert email.
Email Content	Text content supports predefined variables. Variable names and corresponding instructions are as follows: gateway hostname:$(HOSTNAME) attack source ip address:$(SOURCEIP) attack dest mac:$(DESTMAC) attack source port:$(DESTPORT) attack source protocol:$(PROTOCOL) attack occurred:$(DATETIME)

AMI Settings

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. It allows live monitoring of events that occur in the system, as well enabling you to request that Asterisk perform some action. The actions that are available are wide-ranging and include things such as returning status information and originating new calls. Many interesting applications have been developed on top of Asterisk that take advantage of the AMI as their primary interface to Asterisk.

There are two main types of messages on the Asterisk Manager Interface: manager events and manager actions.

The 3rd party software can work with TA1600/2400/3200 using AMI interface. It is disabled by default. If necessary, you can enable it.

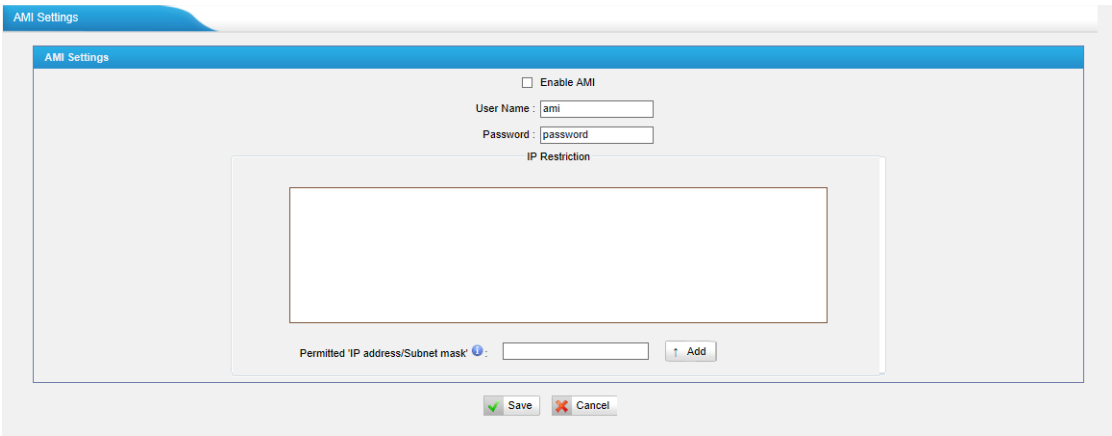


Figure 10-5 AMI Settings

- **User Name, Password & Port**
  After enabling AMI, you can use this username and password to log in TA1600/2400/3200. The default port is 5038.

- **Permitted "IP address/Subnet mask"**
  You can set which IP is allowed to log in TA1600/2400/3200 AMI interface.

Certificates

TA1600/2400/3200 supports TLS transport, you can configure FXS port with TLS transport. To use TLS, you should upload certificates first.

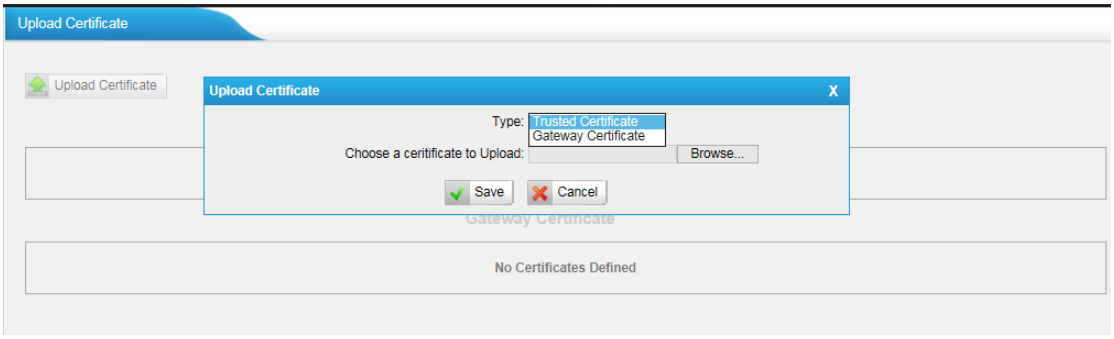


Figure 10-6 Upload Certificate

- **Trusted Certificate**
  This certificate is a CA certificate. When selecting “TLS Verify Client” as “Yes”, you should upload a CA. The relevant VoIP provider should also have this certificate.
- **Gateway Certificate**
  This certificate is server certificate. No matter selecting “TLS Verify Client” as “Yes” or “NO”, you should upload this certificate to TA1600/2400/3200. If the VoIP provider enables “TLS Verify server”, you should also upload the relevant CA certificate on the VoIP provider.

Firewall Rules

Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.



Figure 10-7 Firewall Settings

1) General Settings

Table 10-2 Description of Firewall General Settings

Items	Description
Enable Firewall	Enable the firewall to protect the device.
Disable Ping	Enable this item to drop net ping from remote hosts.
Drop All	When you enable “Drop All” feature, the system will drop all packets or connection from other hosts if there are no other rules defined. To avoid locking the devices, at least one “TCP” accept common rule must be created for port used for SSH access, port used for HTTP access and port sued for CGI access.

2) Common Rules

There is no default rule; you can create one as required.

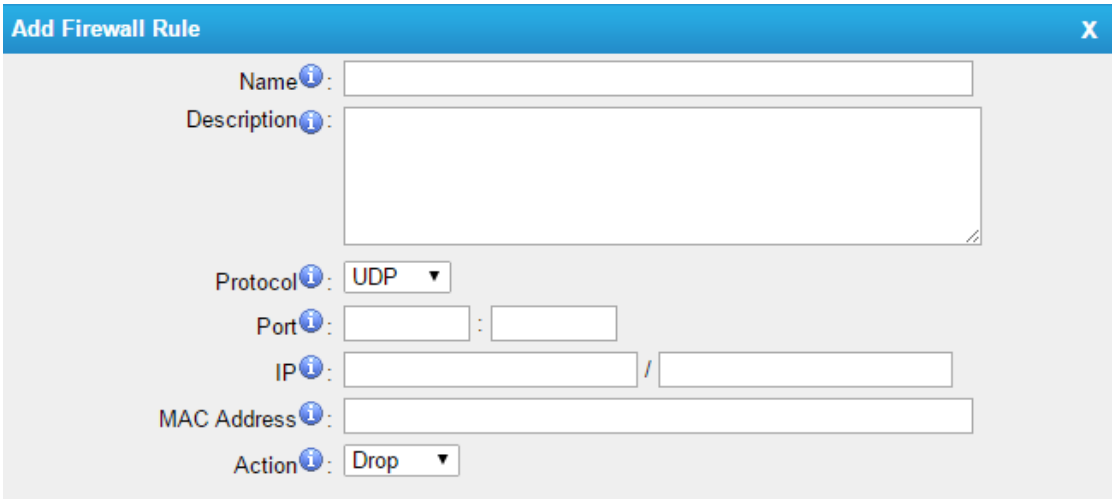


Figure 10-8 Common Rules

Table 10-3 Description of Common Rules

Items	Description
Name	A name for this rule, e.g. “HTTP”.
Description	Simple description for this rule. E.g. accept the specific host to access the Web interface for configuration.
Protocol	The protocols for this rule.
Port	Initial port should be on the left and end port should be on the right. The end port must be equal to or greater than start port.
IP	The IP address for this rule. The format of IP address is: IP/mask E.g. 192.168.5.100/255.255.255.255 for IP 192.168.5.100 E.g. 192.168.5.0/255.255.255.0 for IP from 192.168.5.0to 192.168.5.255.
MAC Address	The format of MAC Address is XX:XX:XX:XX:XX:XX, X means 0~9 or A~F in hex, the A~F are not case sensitive.
Action	Accept: Accept the access from remote hosts. Drop: Drop the access from remote hosts. Ignore: Ignore the access.

Note: the MAC address will be changed when it’s a remote device, so it will not be working to filter using MAC for remote devices.

3) Auto Defense

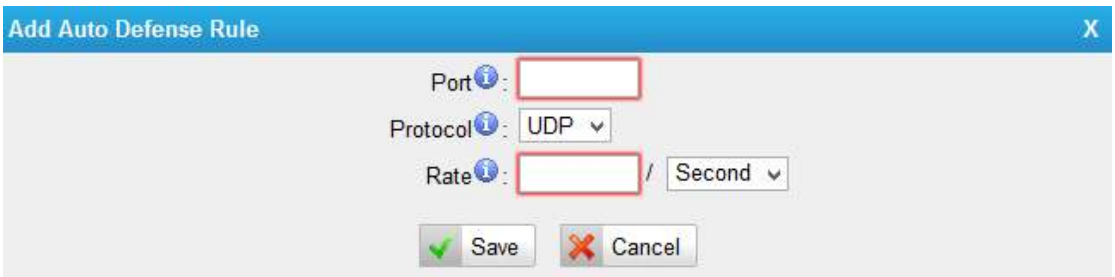


Figure 10-9 Auto Defense

Table 10-4 Description of Auto Defense

Items	Description
Port	The port you want to auto defense, for example, 8022.
Protocol	Select the protocol. You can select UDP or TCP.
Rate	The maximum packets or connections can be handled per unit time. For example, if you configure it as below: Port: 8022 Protocol: TCP Rate: 10/min Then, it means maximum 10 TCP connections can be handled in 1 minute. The 11th connection will be dropped.

IP Blacklist

You can set some packets accept speed rules here. When an IP address, which hasn't been accepted in common rules, sends packets faster than the allowed speed, it will be set as a black IP address and be blocked automatically.

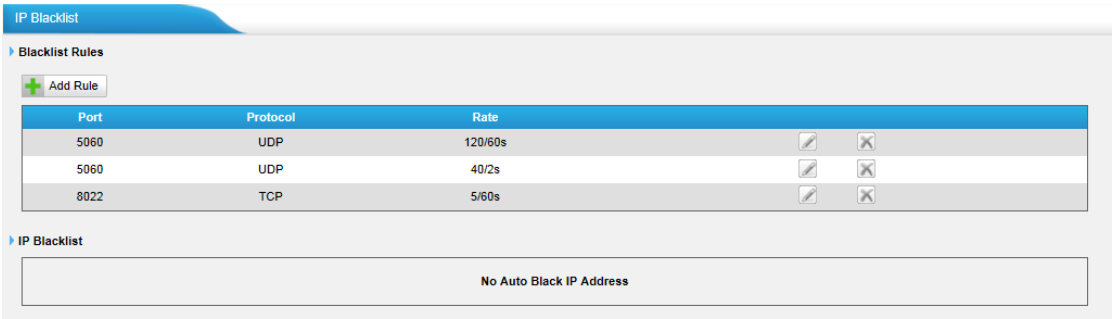


Figure 10-10 IP Blacklist Settings Page

1) Blacklist rules

We can add the rules for IP blacklist rate as demanded.

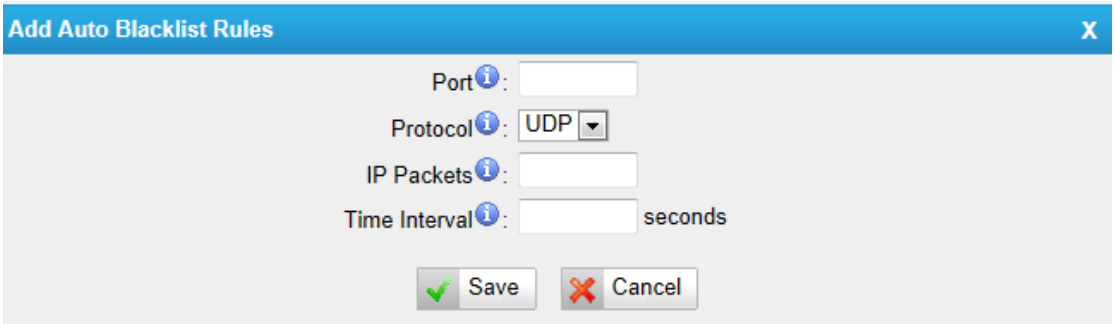


Figure 10-11 Add Blacklist Rule

Table 10-5 Description of Auto Blacklist Rules

Items	Description
Port	Auto defense port
Protocol	Auto defense protocol. TCP or UDP.
IP Packets	Allowed IP packets number in the specific time interval.
Time interval	The time interval to receive IP packets. For example, IP packets 90, time interval 60 means 90 IP packets are allowed in 60 seconds.

2) IP blacklist

The blocked IP address will display here, you can edit or delete it as youwish.

System Preferences

This chapter describes system maintenance settings including the followings:

- Password Settings
- Date and Time
- Auto Provision Settings
- Firmware Update
- Backup and Restore
- Reset and Reboot

Password Settings

It is highly recommended to change the system's password after first login. Go to **System→System Preferences→Password Settings** to change the password.

1. Enter the old password first.
2. Enter a new password and retype the new password to confirm. The password complexity will be detected, which will help users to set a strong password and make TA1600/2400/3200 safer. A strong password is comprised of letters, numbers and characters.
3. Save the changes, the user will be automatically logged out.
4. Log in TA1600/2400/3200 using the new password.

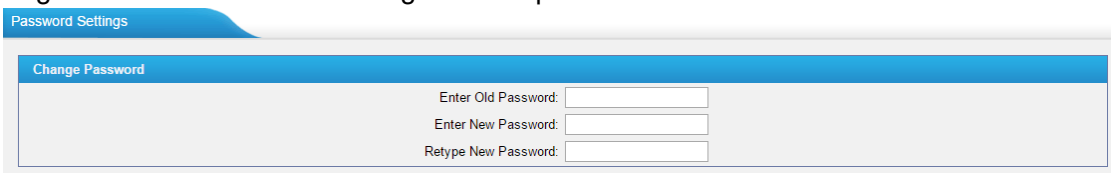


Figure 11-1 Password Settings

Date and Time

Please adjust the time of TA1600/2400/3200 (including the time zone) consistent with your local time. Go to **System→System Preferences→Date and Time** to configure the system date and time.

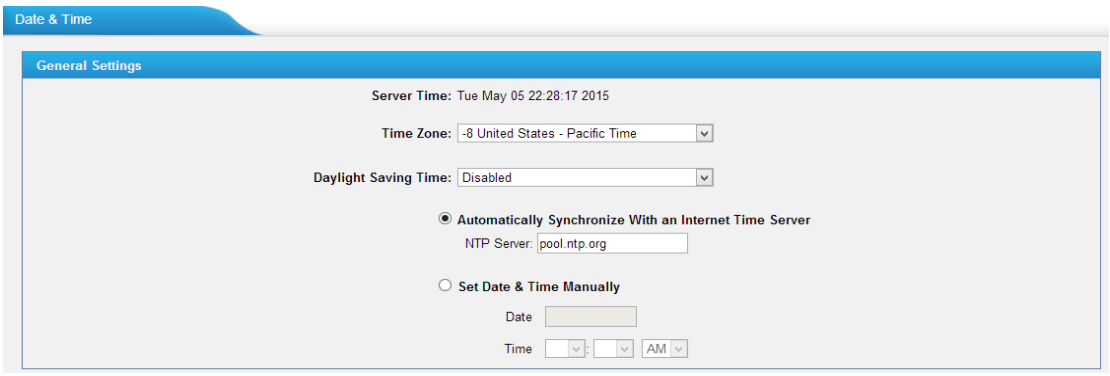


Figure 11-2 Date and Time

- **Time Zone**
  Select your current and correct time zone on TA1600/2400/3200.
- **Daylight Saving Time**
  The option is disabled by default. Enable it when necessary.
- **Automatically Synchronize with an Internet Time Server**
  TA1600/2400/3200 will adjust its internal clock to a central network server. Please note the TA1600/2400/3200 should be able to access to the Internet if you choose this method.
- **Set Date & Time Manually**
  Enter the time using the numbers on your keyboard.

Note: you have to reboot the system to make the changes take effect.

Auto Provision Settings

Three methods are supported for Auto Provision: PNP, DHCP and you can manually configure a server URL to get the configuration file from the server. Go to **System→System Preferences→Auto Provision Settings** to configure.

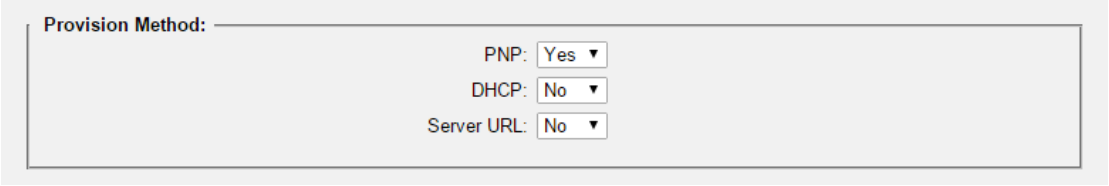


Figure 11-3 Auto Provision Methods

PNP and **DHCP** modes work along with MyPBX "TA Provisioning".Firstly, users need to configure TA1600/2400/3200 on MyPBX "TA Provisioning" page. Then TA1600/2400/3200 will find and get the configuration file from MyPBX during boots up.

In **PNP** mode, you just need to place the TA1600/2400/3200 in the same IP range network with MyPBX, then you can find the TA1600/2400/3200 and provision it on MyPBX ”TA Provisioning” page.



Figure 11-4 MyPBX TA Provisioning

If you use **DHCP** mode to do auto provision, you should enable DHCP Server on MyPBX to make it as a DHCP server. (System→Network Preferences→DHCP Server).

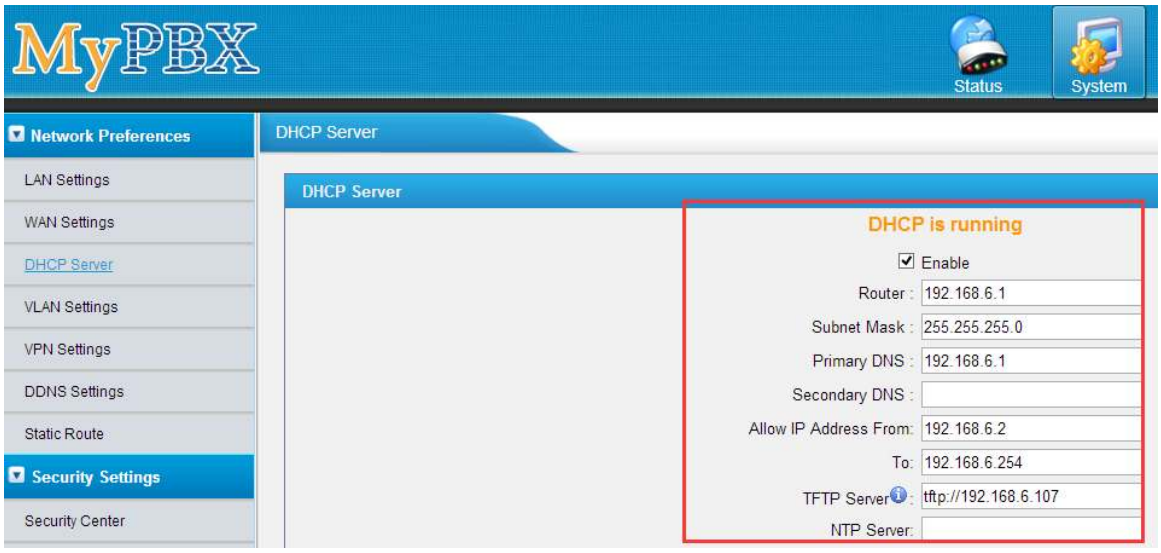


Figure 11-5 Set MyPBX as a DHCP Server

Then select DHCP mode on LAN settings page to make TA1600/2400/3200 as a DHCP client.

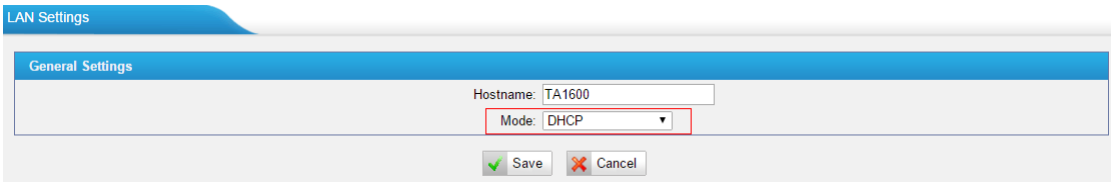


Figure 11-6 Set TA1600/2400/3200 as a DHCP Client

Another way to do auto provision is to download configuration file from the configured server URL. Fill in the URL, user name, password, and set the time, TA1600/2400/3200 will get the configuration file from the server automatically and regularly.

Note: if there is no user name and password for the server, leave these fields blank.

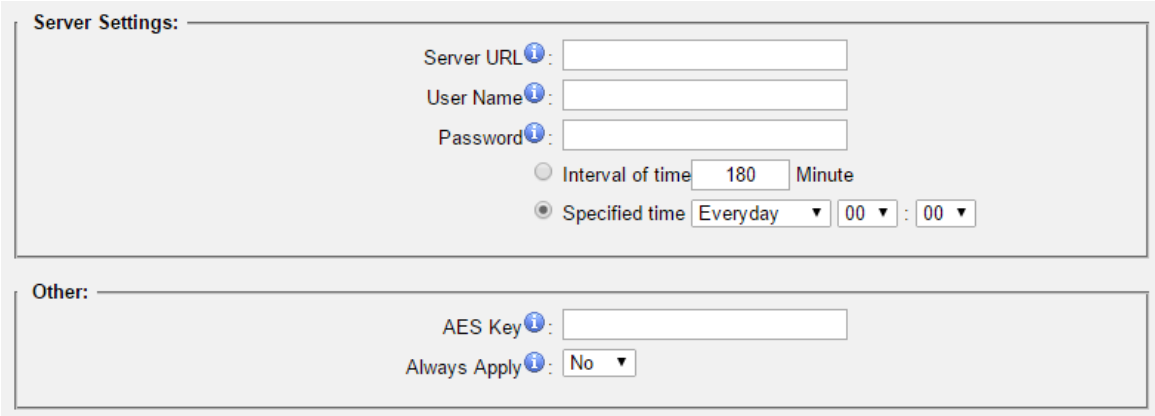


Figure 11-7 Server Address

- **AES Key**
  If the configuration file is encrypted by AES key, you need to fill the key in this field.
- **Always Apply**
  With No, it will compare the current configuration file with the last updated one, if the contents are the same no update will be applied. With Yes, it will always apply the updated configuration file.

Firmware Upgrade

TA1600/2400/3200 can be upgraded to a new firmware version via network or locally. Users could upgrade firmware via HTTP or TFTP. Please go to **System→ System Preferences→ Firmware Update** to do upgrade.

Notes:

1. If "Reset configuration to Factory Defaults" is enabled, the system will be restored to factory default settings.
2. When updating the firmware, please don't turn off the power. Or the system will be damaged.
3. If you are trying to upgrade through HTTP, please make sure that your TA1600/2400/3200 is able to visit external network, or it cannot access Yeastar website to get the firmware file, causing the upgrade fail.

Upgrade through HTTP

On the Firmware Upgrade page, choose **HTTP URL**.
Step1. Enter the download link of the firmware file.
Note: the HTTP URL should be a **BIN** file download link.

Step2. Click "Start" to upgrade.

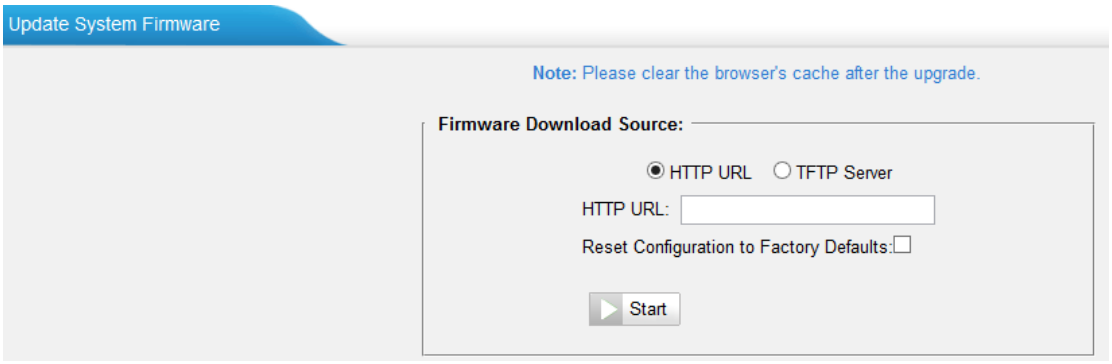


Figure 11-8 Upgrade through HTTP

Upgrade through TFTP

Step1. Download firmware file from Yeastar website.

Step2. Create a tftp Server (For example, tftpd on Windows).

1) Install tftpd32 software on computer.
   Download link: http://tftpd32.jounin.net/tftpd32_download.html
2) Configure tftpd32.
   On option "**Current Directory**", click "**Browse**" button, choose the firmware file (BIN file) upgraded patch.

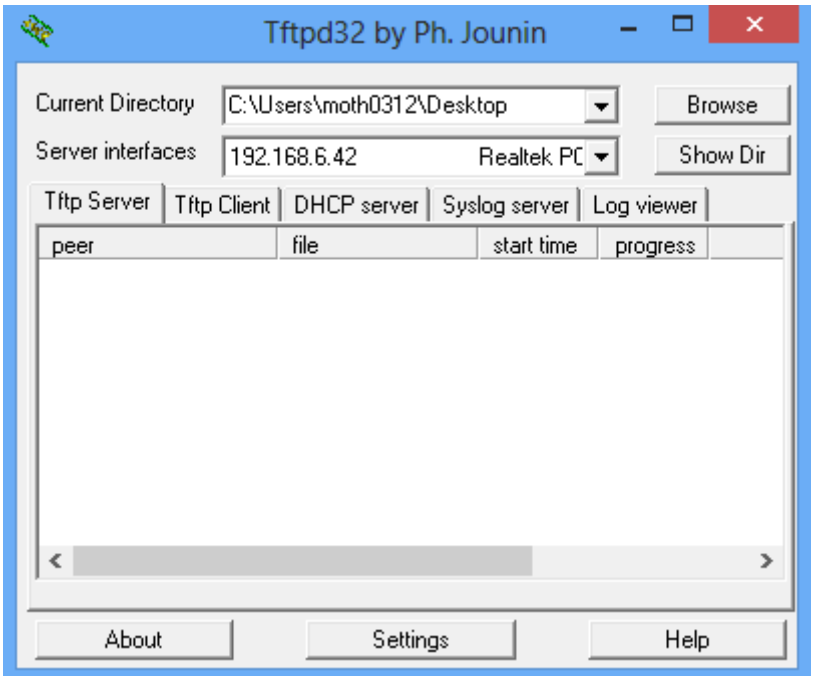


Figure 11-9 Configure Tftpd32

Step3. Logon the TA1600/2400/3200's Web page and go to **System→System Preferences→Firmware Update**, choose "**TFTP Server**".

1) TFTP Server: fill in IP address of tftpd32 server (your PC's IP address).
2) File Name: enter the name of firmware update. It should be a BIN file name.

3) Click “Start” to upgrade.

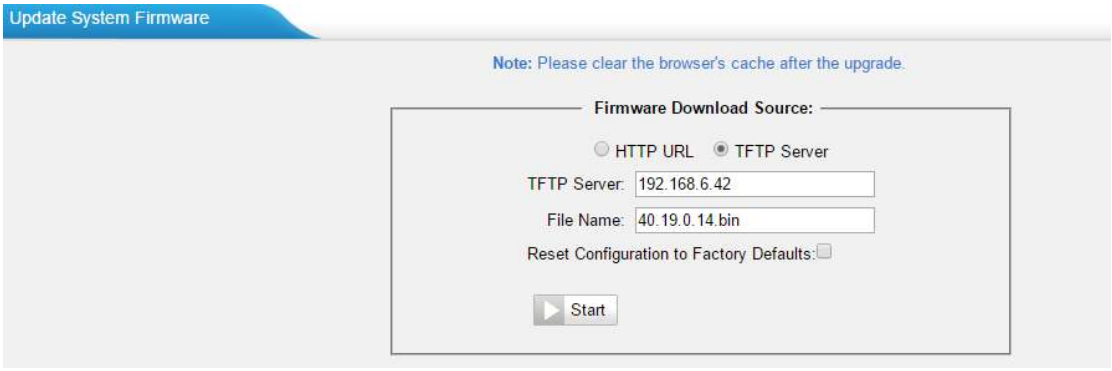


Figure 11-10 Upgrade through HTTP

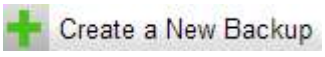
Backup and Restore

TA1600/2400/3200 provides Backup and Restore feature, which allows you to create a complete backup of TA1600/2400/3200 configurations to a file.

Notes:

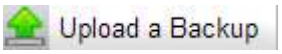
1. When you have updated the firmware version, it’s not recommended to restore using an old package.
2. Backup from an earlier version cannot be restored on TA1600/2400/3200 of a later version.

- **Create a New Backup**

  Click 

 to create a new backup.

- **Upload a Backup**

  Click 

 to upload a backup.

- **Restore**

  To restore TA1600/2400/3200 configuration data, upload the backup file to TA1600/2400/3200 and click. Reboot the system to take effect.

  Please note the current configurations will be OVERWRITTEN with the backup data.

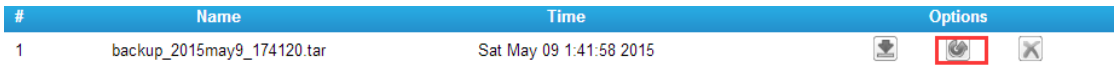


Figure 11-11 Restore Backup

Reset and Reboot

Users could reset and reboot the system under **System→ System Preferences→ Reset and Reboot**.

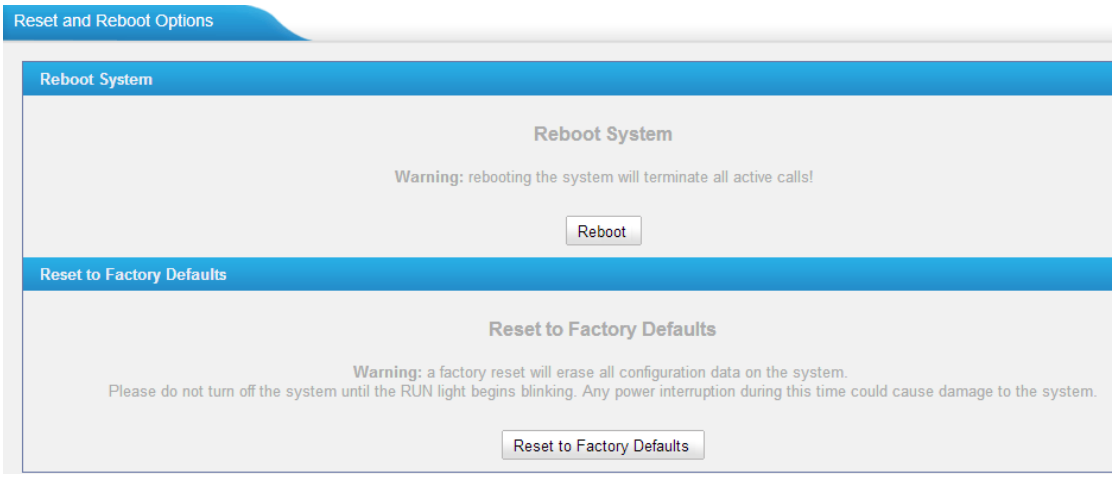


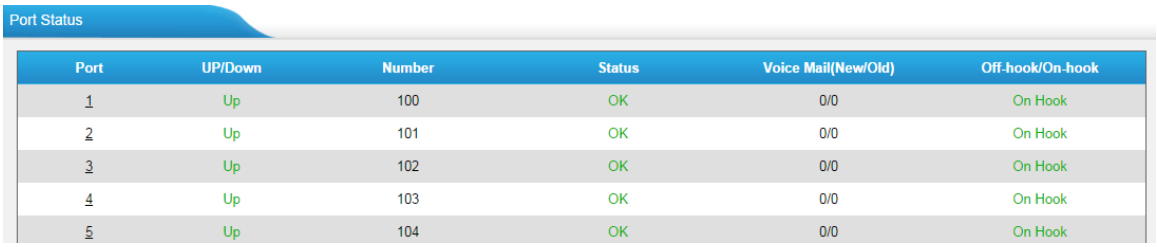
Figure 11-12 Reset and Reboot

Status

Users could check the system status on **Status→System Status**, where FXS Port Status, Network Status and System Info can be checked.

- FXS Port Status
- Network Status
- System Info

FXS Port Status


Port Status

Port	UP/Down	Number	Status	Voice Mail(New/Old)	Off-hook/On-hook
1	Up	100	OK	0/0	On Hook
2	Up	101	OK	0/0	On Hook
3	Up	102	OK	0/0	On Hook
4	Up	103	OK	0/0	On Hook
5	Up	104	OK	0/0	On Hook

Figure 12-1 FXS Port Status

Table 12-1 Description of FXS Port Status

Up/Down	
Up	The FXS module works well.
Down	The FXS module is broken.
Status	
OK	Successful registration, trunk is ready for use
Unreachable	The trunk is unreachable.
Request Send	Registering.
Waiting for authentication	Wrong password or user name.
Failed	Trunk registration failed.
Voice Mail (New/Old)	
Showing the number of unread voicemail and old voicemail. *Only when the FXS port is registered as one of the VoIP Server's accounts, can you see the voice mail status.	
Hook	
On Hook	The FXS port is idle.
Off Hook	The FXS port is busy.

Network status

In this page, the IP address of LAN port will appear with their status.

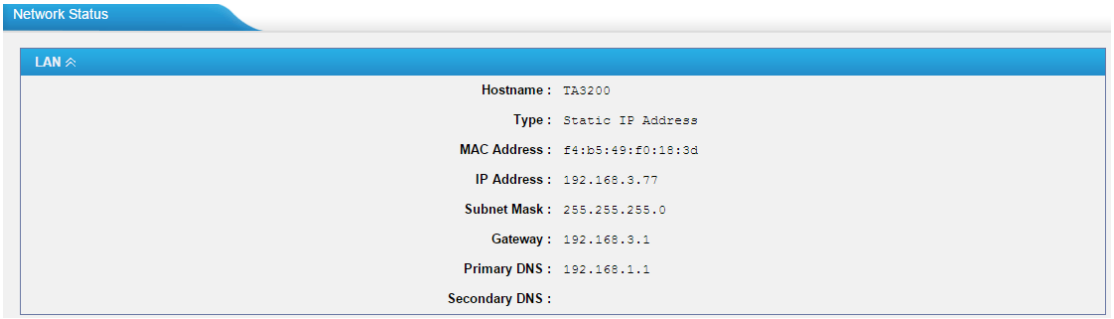


Figure 12-2 Network Status

If your VLAN or VPN are configured, you can check the status in this page also.

System Info

In this page, we can check the hardware/firmware version, or the disk usage of TA FXS Gateway.



Figure 12-3 System Info

Reports

Users could check the call logs, system logs on **Status→Reports** page, and use the packet Tool and Port Monitor Tool to capture debug logs from TA1600/2400/3200.

- Call Logs
- System Logs
- Packet Tool
- Port Monitor Tool

Call Logs

The call log captures all call details, including call time, caller number, callee number, call type, call duration, etc. An administrator can search and filter call data by call date, caller/callee, trunk, duration, billing duration, status, or communication type.

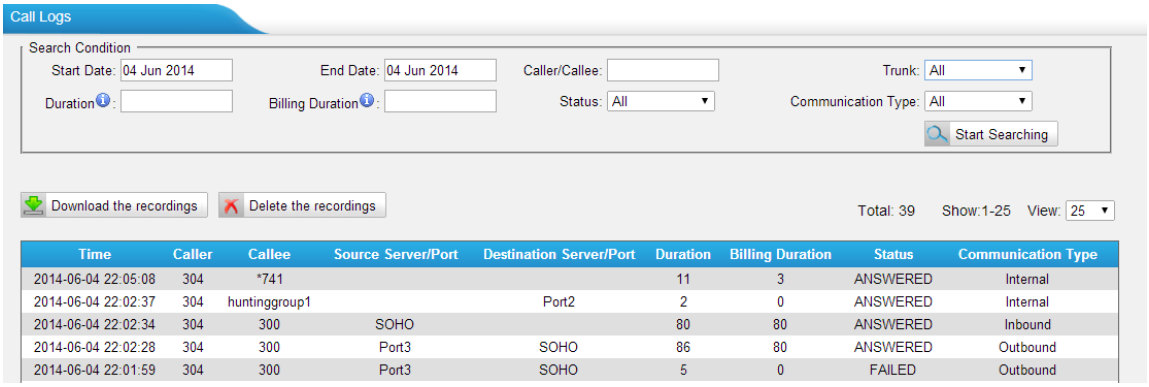


Figure 13-1 Call Logs

System Logs

You can download and delete the system logs of TA1600/2400/3200.

- **Enable Hardware Log**
  Save the information of hardware; (up to 4 log files)
- **Enable Normal Log**
  Save the prompt information; (up to 16 log files)
- **Enable Web Log**
  Save the history of web operations (up to 2 log files)
- **Enable Debug Log**
  Save debug information (up to 2 log files)

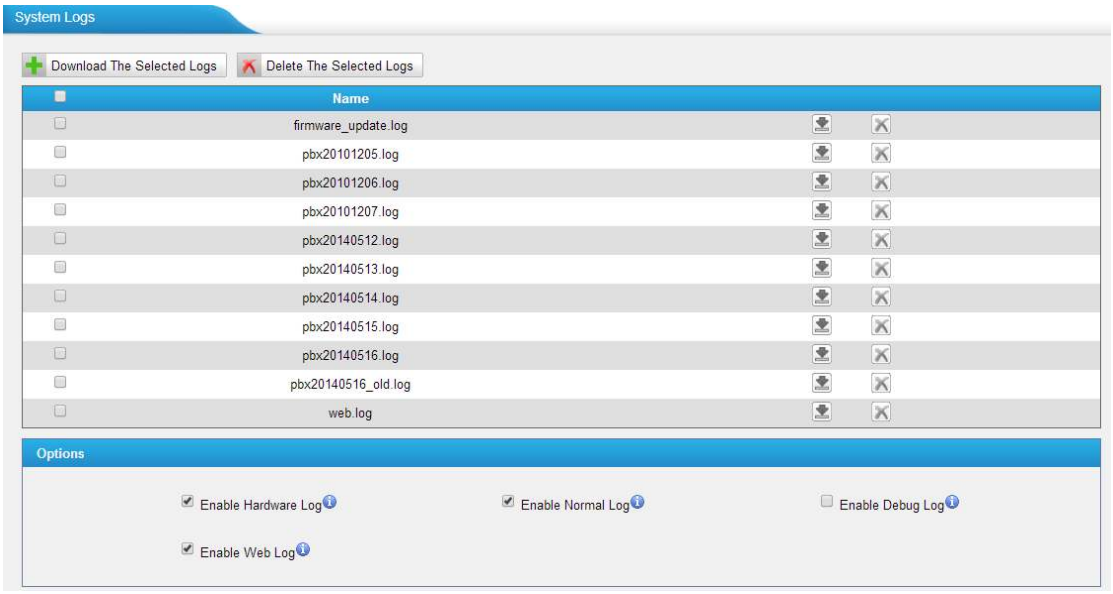


Figure 13-2 System Logs

Packet Tool

This feature is used to capture packets for technician. Integrate packet capture tool "Wireshark" in TA1600/2400/3200. Users also could specify the destination IP address and port to get the packets.

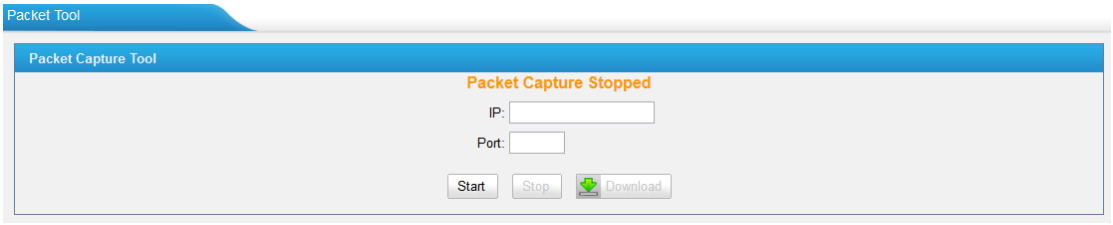


Figure 13-3 Packet Tool

- **IP**
  Specify the destination IP address to get the packets.
- **Port**
  Specify the destination Port to get the packets.

Port Monitor Tool

This tool is used to debug a FXS port. Select a FXS port and click "Start" to monitor the FXS port, stop monitoring by clicking "Stop" button.



Figure 13-4 Port Monitor Tool