

NeoGate

TE100

Administrator's Guide

Version 16.17.0.32

Yeastar Technology Co., Ltd.

Table of Contents

1. Introduction	4
1.1 Features	4
1.2 Hardware Specification	5
1.2.1 Exterior Appearance	5
2. System setup	6
2.1 Connection Drawing	6
2.2 Connecting Ethernet Line	6
2.3 Supplying Power	6
3 Administrator Login	7
4. Status	8
4.1 System Status	8
4.1.1 Trunk status	8
4.1.2 Network status	9
4.1.3 System info	9
4.2 Reports	10
4.2.1 Call logs	10
4.2.2 System logs	10
5. System	11
5.1 Network Preferences	11
5.1.1 LAN Settings	11
5.1.2 WAN Settings	12
5.1.3 DDNS settings	13
5.1.4 Static Route	14
5.2 Firewall Settings	15
5.2.1 Firewall Rules	15
5.2.2 IP Blacklist	18
5.3 system Preferences	19
5.3.1 Password Settings	19
5.3.2 Date and Time	19
5.3.3 Backup and Restore	20
5.3.4 Reset and Reboot	21
5.3.5 Firmware Update	21
6. Gateway	23
6.1 Digital Trunk	23
6.2 VoIP settings	26
6.2.1 VoIP trunk	26
6.2.2 SIP Settings	29
6.2.3 Trunk Group	35

6.2.4 General Preferences.....	36
6.3 Routes Settings.....	36
6.3.1 Route List	37
6.3.2 Blacklist	40
7. Logout	40
8 Application	41

1. Introduction

NeoGate TE100- Bridge the gap between E1/T1/J1 and VoIP networks

NeoGate TE100 offers SMBs cost effective additions to legacy telephone systems to bring the true benefits of VoIP. TE100 is a single port VoIP E1/T1/J1 gateway (VoIP to E1/T1/J1, and E1/T1/J1 to VoIP) that supports up to 30 concurrent calls. It's designed to bridge the gap between E1/T1/J1 and VoIP networks. Integrating TE100 into an existing network will allow inexpensive communication via SIP trunk. Also, it could connect VoIP systems with E1/T1/J1 service from legacy carriers.

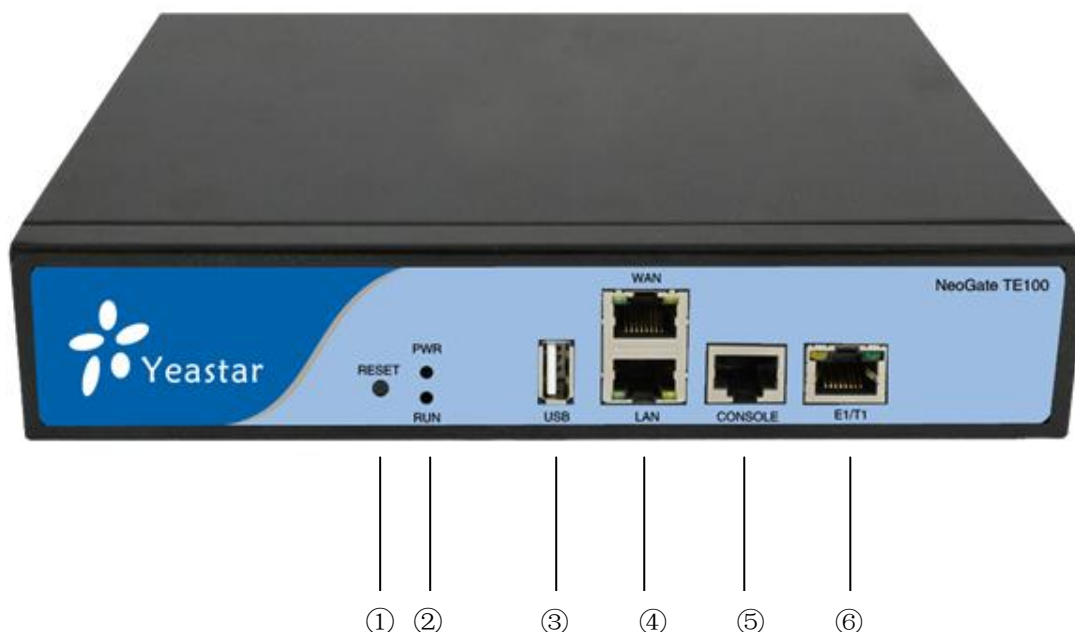
1.1 Features

● Trunk Support
● Call Routing Rules
● Automatic appending and stripping of digits to dialed numbers
● Caller ID name and number support
● FAX support
● Blacklist
● Firewall
● DDNS Support
● Backup and Restore
● Easy to install (web based)
● G729 codec support

More info, please click: <http://www.yeastar.com/Products/NeoGate-TE100.asp>

1.2 Hardware Specification

1.2.1 Exterior Appearance



No.	Identifying
① Reset	The button to reset TE100 to factory defaults.
② Power RUN	Green shining: Connected, correct function. Green flashing: Device error. No light: Disconnected, malfunction. Green Light: Indicates the server system is in working order
③ USB	USB 2.0 interface
④ WAN LAN	WAN port(10/100M) LAN port(10/100M)
⑤ Console	Console interface(RJ45)
⑥ E1/T1	E1/T1 interface

2. System setup

2.1 Connection Drawing

2.2 Connecting Ethernet Line

TE100 provides two 10/100Mbps Ethernet ports with RJ45 interface and LED indicator. Plug Ethernet line into TE100's Ethernet port, and then connect the other end of the Ethernet line with a hub, switch, router, LAN or WAN. Once connected, check the status of the LED indicator. A yellow LED indicates the port is in the connection process, and a green LED indicates the port is properly connected.

2.3 Supplying Power

Please follow the steps below to connect the TE100 unit to a power outlet:

1. Connect the small end of the power cable to the power input port on the TE100 back panel, and plug the other end of the cable into a 100V~240V AC power outlet.
2. Check the Power LED on the front panel. A solid green LED indicates that power is being supplied correctly.

3 Administrator Login

From your web browser, input the IP address of the NeoGate TE100.

If this is the first time you are configuring TE100, please use the default settings below (your PC should be in the same local network with TE100):

IP Address: <http://192.168.5.150>

Username: **admin**

Password: **password**

In this example, the IP address is <http://192.168.5.159>

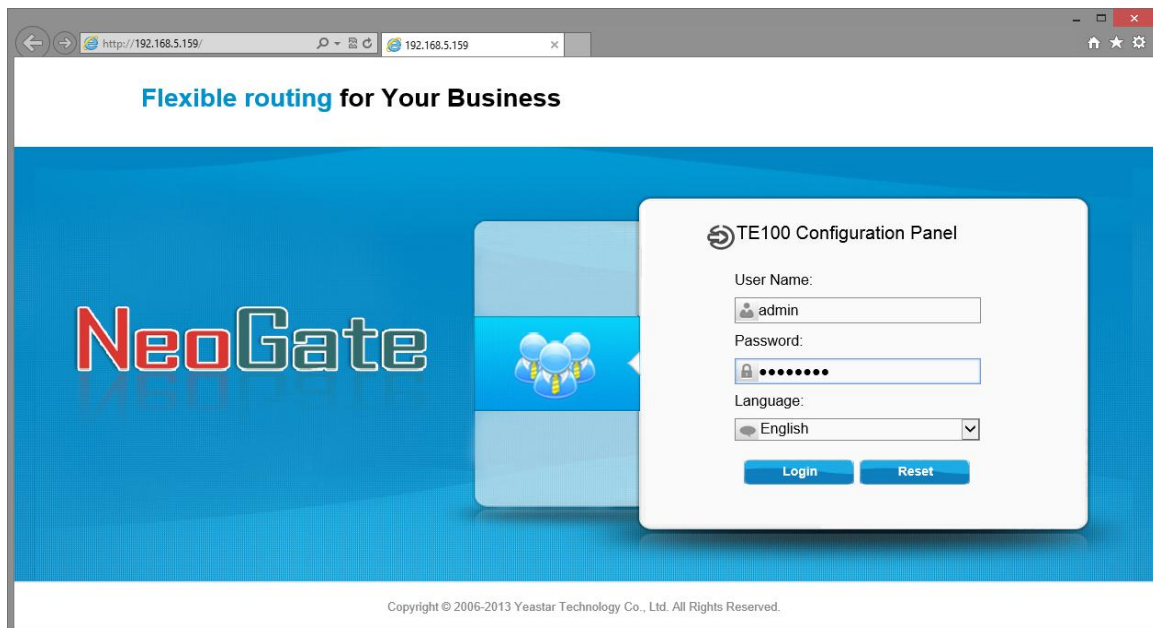


Figure 3-1

This is the welcome page of TE100 after login successfully.

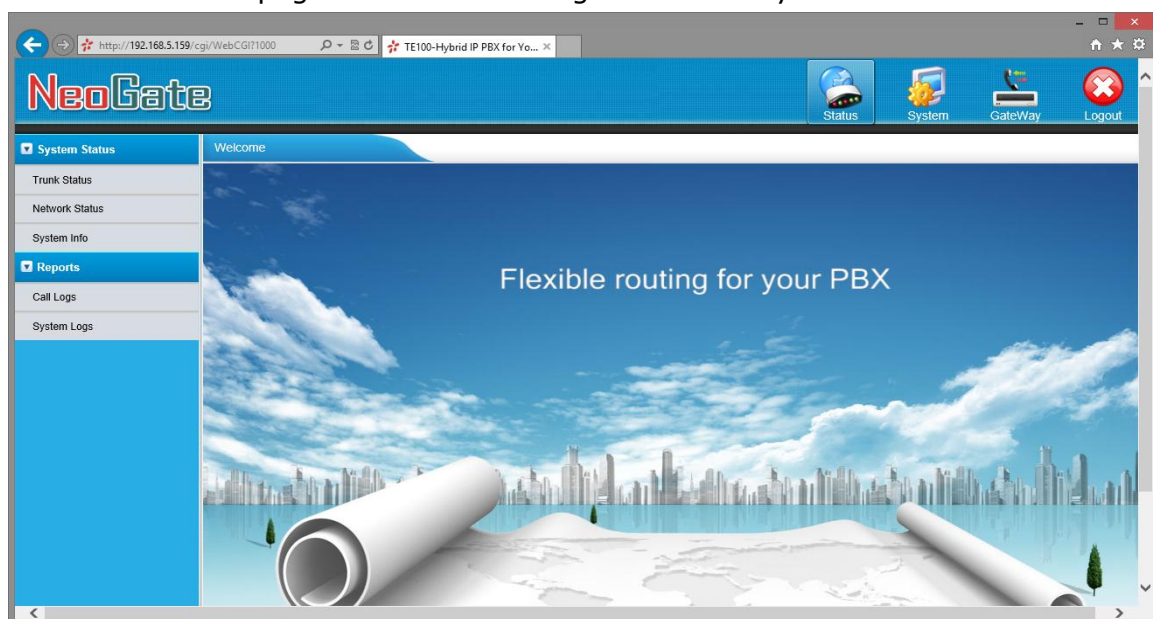



Figure 3-2

4. Status



Click  to start to check the status of TE100, including the system's status and the detailed reports

4.1 System Status

In this page, we can check the status of the system, including trunk status, network status and system information.

4.1.1 Trunk status

Status	Trunk Name	Type	User Name	Hostname/IP	Reachability
Registered	Yeastar	SIP	501	192.168.4.141	OK
OK (7 ms)	Support	SP-SIP		192.168.5.101	OK (7 ms)



Trunk Name	Mode Type	Connected	Alarm
E1Trunk1	E1		

Figure 4-1

Trunks:

VoIP Trunk:

Status

Unregistered: Trunk registration failed.

Registered: Successful registration, trunk is ready for use.

Request Sent: Registering.

Waiting: Waiting for authentication.

Service Provider:







Status

OK: Successful registration, trunk is ready for use.

Unreachable: The trunk is unreachable.

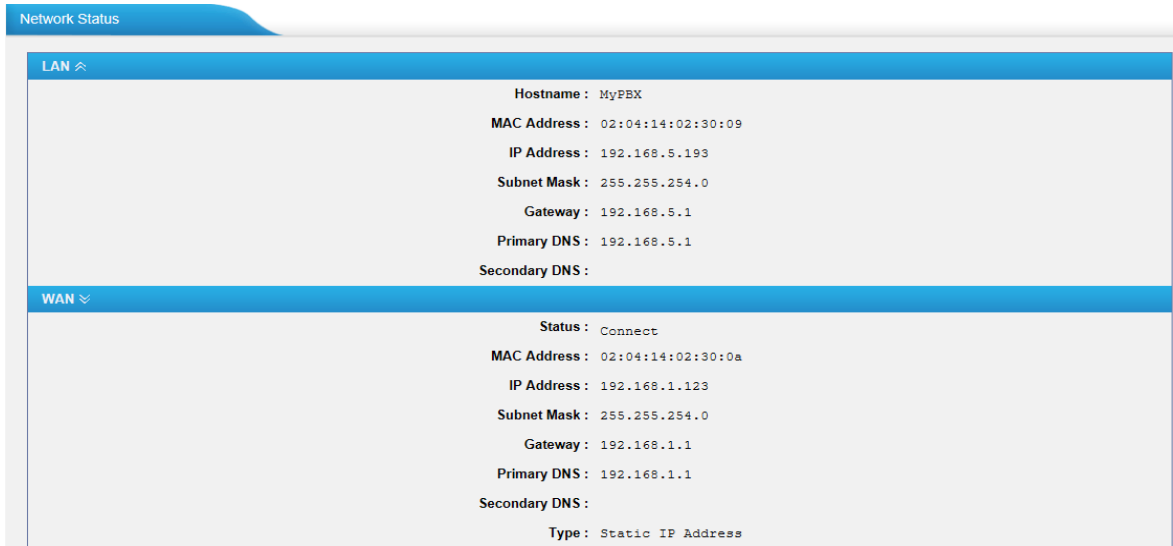
Failed: Trunk registration failed.

E1 Trunk:

Connect	Alarm	Comment
		The port doesn't have E1 line connected.
		E1 line has been connected to the port; PRI is in corresponding or can't communicate.
		Succeed.

4.1.2 Network status

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

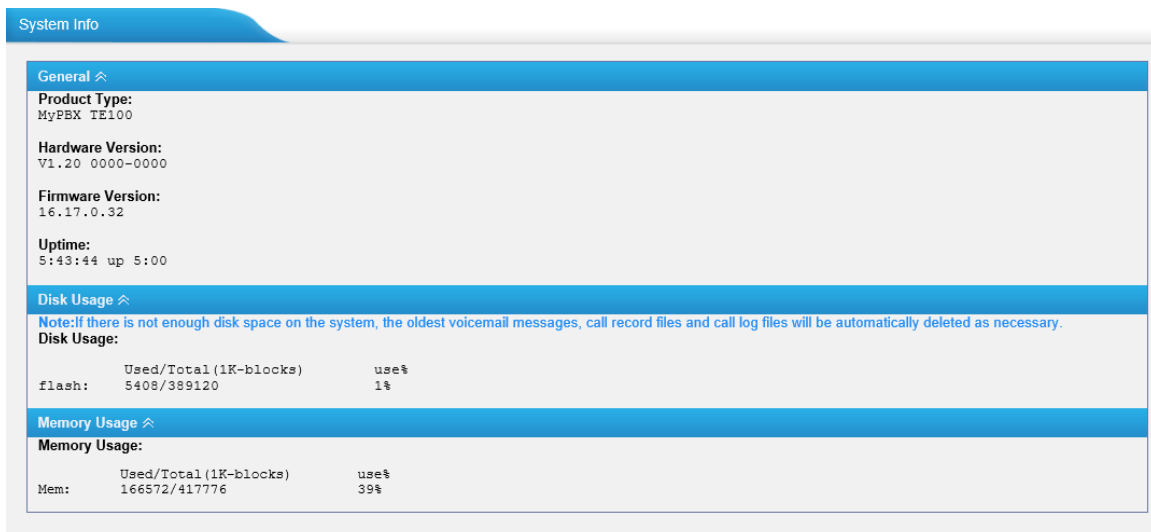


Network Status	
LAN	
Hostname :	MyPBX
MAC Address :	02:04:14:02:30:09
IP Address :	192.168.5.193
Subnet Mask :	255.255.254.0
Gateway :	192.168.5.1
Primary DNS :	192.168.5.1
Secondary DNS :	
WAN	
Status :	Connect
MAC Address :	02:04:14:02:30:0a
IP Address :	192.168.1.123
Subnet Mask :	255.255.254.0
Gateway :	192.168.1.1
Primary DNS :	192.168.1.1
Secondary DNS :	
Type :	Static IP Address

Figure 4-2

4.1.3 System info

In this page, we can check the hardware/firmware version, or the disk usage of TE100.



System Info		
General		
Product Type:	MyPBX TE100	
Hardware Version:	V1.20 0000-0000	
Firmware Version:	16.17.0.32	
Uptime:	5:43:44 up 5:00	
Disk Usage		
Note: If there is not enough disk space on the system, the oldest voicemail messages, call record files and call log files will be automatically deleted as necessary.		
Disk Usage:		
	Used/Total (1K-blocks)	use%
flash:	5408/389120	1%
Memory Usage		
Memory Usage:		
	Used/Total (1K-blocks)	use%
Mem:	166572/417776	39%

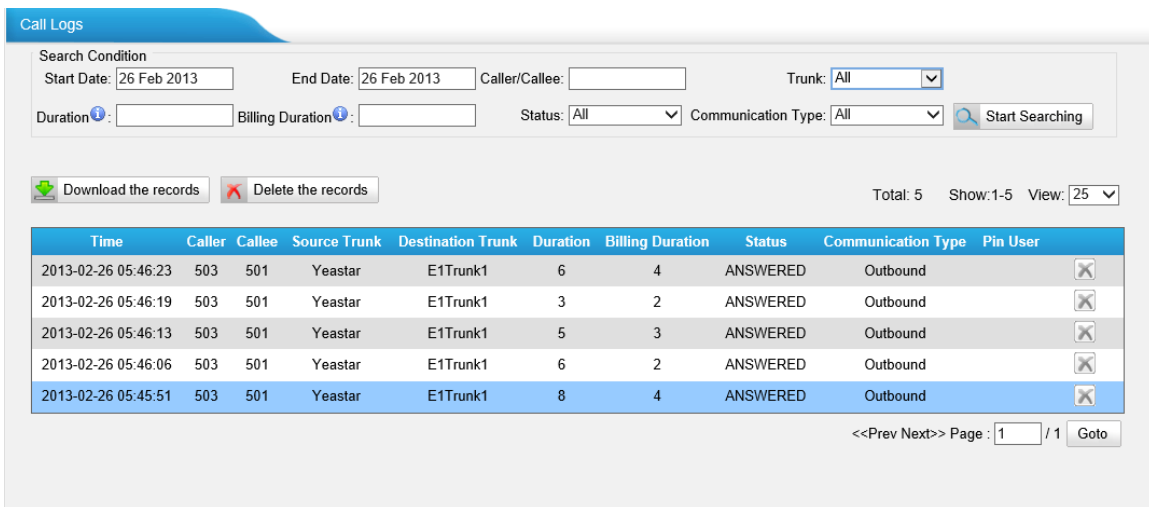
Figure 4-3

4.2 Reports

In this page, we can check the call detailed log and system log, which is used to debug the problem we meet.

4.2.1 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 filter the call logs by call date, caller/callee, trunk, duration, billing duration, status, or communication type.



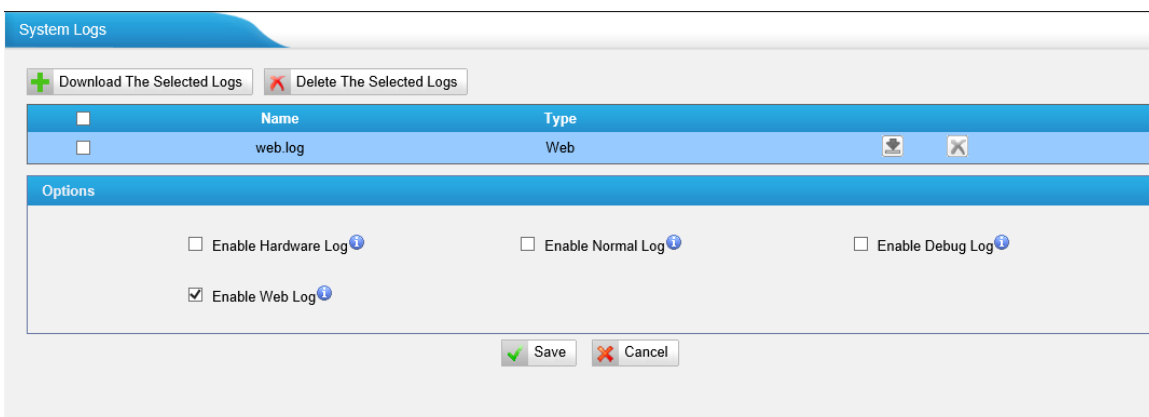
The screenshot shows the 'Call Logs' interface. At the top, there are search filters for Start Date (26 Feb 2013), End Date (26 Feb 2013), Caller/Callee, Trunk (All), Duration, Billing Duration, Status (All), and Communication Type (All). Below the filters are buttons for 'Download the records' and 'Delete the records'. A summary shows 'Total: 5', 'Show: 1-5', and 'View: 25'. The main table lists call records with columns: Time, Caller, Callee, Source Trunk, Destination Trunk, Duration, Billing Duration, Status, Communication Type, and Pin User. The table contains five rows of data, all with 'ANSWERED' status and 'Outbound' communication type.

Time	Caller	Callee	Source Trunk	Destination Trunk	Duration	Billing Duration	Status	Communication Type	Pin User
2013-02-26 05:46:23	503	501	Yeastar	E1Trunk1	6	4	ANSWERED	Outbound	X
2013-02-26 05:46:19	503	501	Yeastar	E1Trunk1	3	2	ANSWERED	Outbound	X
2013-02-26 05:46:13	503	501	Yeastar	E1Trunk1	5	3	ANSWERED	Outbound	X
2013-02-26 05:46:06	503	501	Yeastar	E1Trunk1	6	2	ANSWERED	Outbound	X
2013-02-26 05:45:51	503	501	Yeastar	E1Trunk1	8	4	ANSWERED	Outbound	X

Figure 4-4

4.2.2 System logs

You can download and delete the system logs of TE100.




The screenshot shows the 'System Logs' interface. At the top, there are buttons for 'Download The Selected Logs' and 'Delete The Selected Logs'. Below is a table with columns 'Name' and 'Type'. The table contains one entry: 'web.log' with type 'Web'. Below the table is an 'Options' section with checkboxes for 'Enable Hardware Log', 'Enable Normal Log', 'Enable Debug Log', and 'Enable Web Log'. The 'Enable Web Log' checkbox is checked. At the bottom, there are 'Save' and 'Cancel' buttons.

Name	Type
web.log	Web

Figure 4-5

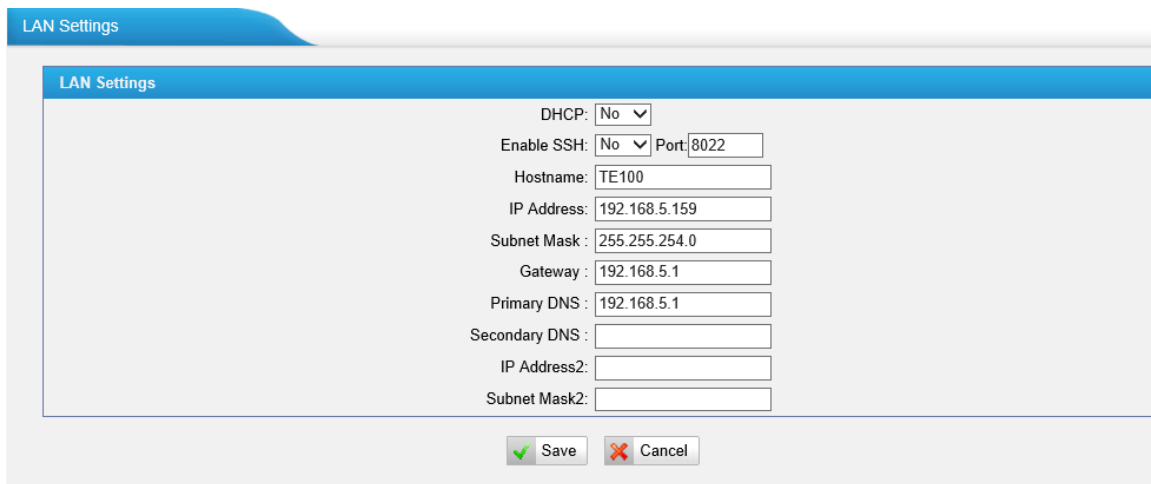
5. System



Click  to access. In this page, we can configure the network settings, firewall rules and some system preferences.

5.1 Network Preferences

5.1.1 LAN Settings



The screenshot shows the 'LAN Settings' configuration page. The settings are as follows:

DHCP:	No
Enable SSH:	No
Port:	8022
Hostname:	TE100
IP Address:	192.168.5.159
Subnet Mask:	255.255.254.0
Gateway:	192.168.5.1
Primary DNS:	192.168.5.1
Secondary DNS:	
IP Address2:	
Subnet Mask2:	

At the bottom of the form, there are two buttons: 'Save' (with a green checkmark icon) and 'Cancel' (with a red X icon).

Figure 5-1

•DHCP

If this option is set as yes, TE100 will act as DHCP client to get an available IP address from your local network. Not recommended or you cannot access TE100 without the right IP address.

•Enable SSH

This is the advance way to access the device, you can use the putty software to access the device. In the SSH access, you can do more advance setting and debug. It's disabled by default.

•**Port:** the default is 8022; you can change it to another one

•Hostname

Set the host name for TE100.

•IP Address

Set the IP Address for TE100.

It is recommended to configure a static IP address for TE100

•Subnet Mask

Set the subnet mask for TE100.

•Gateway

Set the gateway for TE100.

•Primary DNS

Set the primary DNS for TE100.

•Secondary DNS

Set the secondary DNS for TE100.

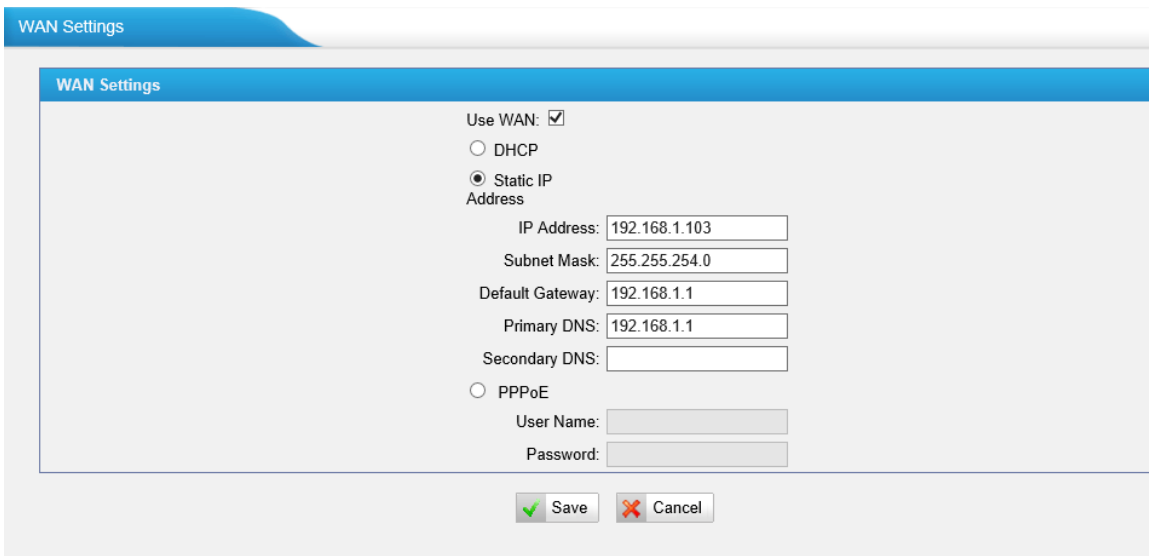
•IP Address2

Set the second IP Address for TE100.

•Subnet Mask2

Set the second subnet mask for TE100.

5.1.2 WAN Settings



The screenshot displays the WAN Settings configuration window. At the top, there is a blue header with the text "WAN Settings". Below this, the main content area contains the following settings:

- Use WAN:** (checked)
- DHCP
- Static IP Address
- IP Address:**
- Subnet Mask:**
- Default Gateway:**
- Primary DNS:**
- Secondary DNS:**
- PPPoE
- User Name:**
- Password:**

At the bottom of the form, there are two buttons: a green "Save" button and a red "Cancel" button.

Figure 5-2

3 connection types are supported: DHCP (obtain an IP automatically), PPPoE, Static IP Address.

Note:

1. WAN port is disabled by default.
2. WAN port cannot be used as a router to route the internet packages from WAN port to LAN port.

·DHCP

If your ISP says that you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:

Step1: Select **DHCP** as the WAN Connection Type.

Step2: Click **Save** button to save the settings.

Step3: Reboot the device.

Step4: Check the WAN's Status (Status→ Network Status).

·Static IP Address

If your ISP says that you are connecting through a static or fixed IP address from your ISP, perform these steps:

Step1: Select **Static IP Address** as the WAN Connection Type.

Step2: Enter the IP Address.

Step3: Enter the Subnet Mask.

Step4: Enter the Gateway Address.

Step5: Enter the Primary DNS and Secondary DNS.

Step6: Click the **Save** button to save the settings.

Step7: Reboot the device.

Step8: Check the WAN's Status (Status→ Network Status).

·PPPoE

If your DSL provider says that you are connecting through PPPoE or if you normally enter a user name and password to access the Internet, perform these steps:

Step1: Select **PPPoE** as the WAN Connection Type.

Step2: Enter the User Name.

Step3: Enter the Password.

Step4: Click the **Save** button to save the settings.

Step5: Reboot the device.

Step6: Check the WAN's Status (Status→ Network Status)

5.1.3 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.

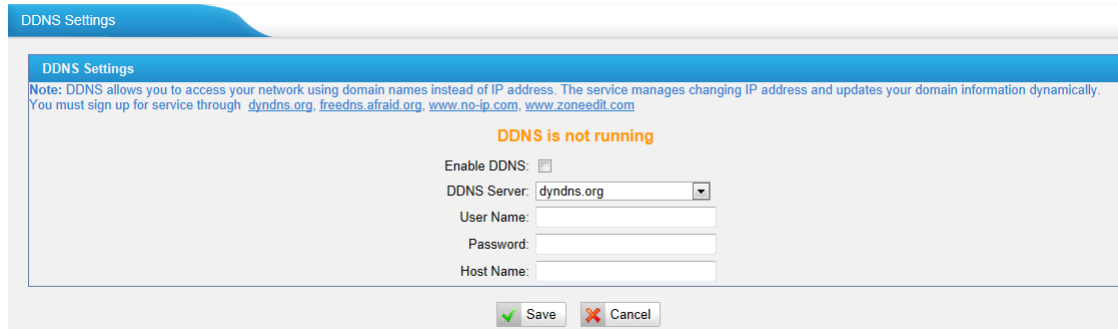
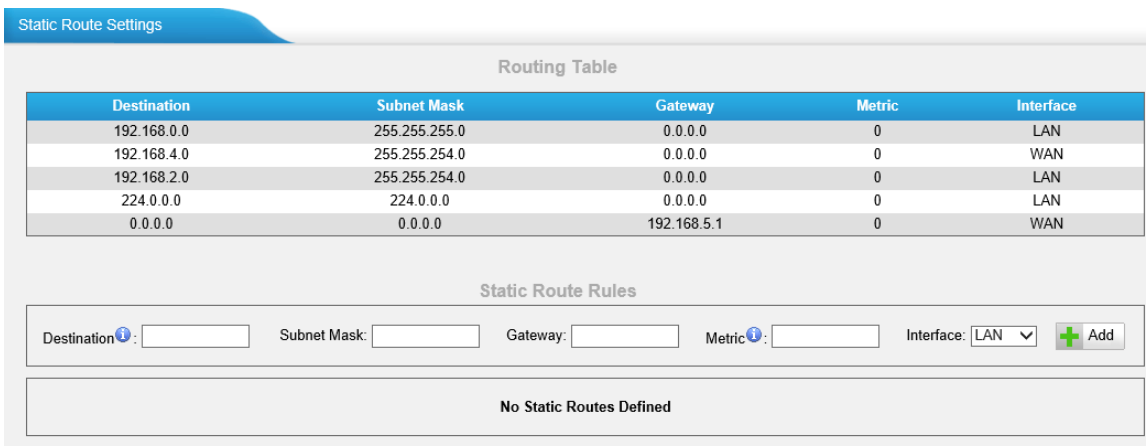


Figure 5-3

5.1.4 Static Route

TE100 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 TE100 to force it to go out through different gateway when access to different internet.

The default gateway priority of TE100 from high to low is WAN port → LAN port.



Destination	Subnet Mask	Gateway	Metric	Interface
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN
192.168.4.0	255.255.254.0	0.0.0.0	0	WAN
192.168.2.0	255.255.254.0	0.0.0.0	0	LAN
224.0.0.0	224.0.0.0	0.0.0.0	0	LAN
0.0.0.0	0.0.0.0	192.168.5.1	0	WAN

Figure 5-4

1) Route Table

The current route rules of TE100.

•Destination

The destination network to be accessed to by TE100.

•Subnet Mask

Specify the destination network portion.

•Gateway

Define which gateway TE100 will go through when access to 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.

2) Static Route Rules

You can add new static route rules here.

5.2 Firewall Settings

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.

5.2.1 Firewall Rules

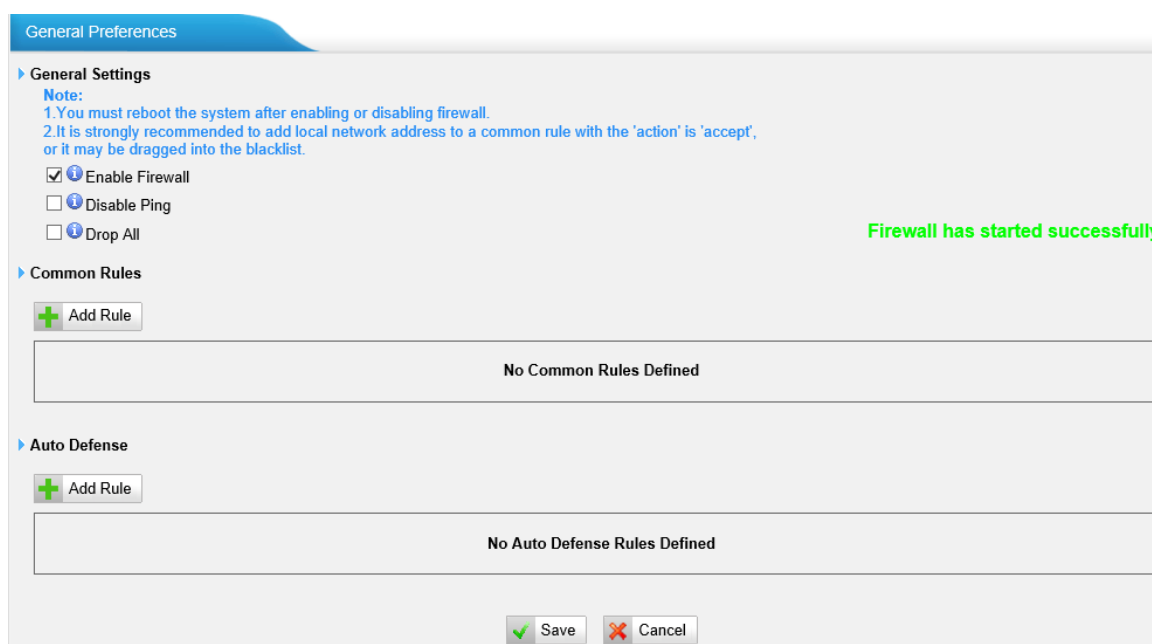


Figure 5-5

1) General Settings

•Enable Firewall

Enable the firewall to protect the device. You should reboot the device to make the firewall run successfully.

•Disable Ping

Enable this item, net ping from remote hosts will be dropped.

•Drop All

When you enable 'Drop All' feature, 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 used for CGI access.

2) Common Rules

There are no default rules inside; you can create them as required

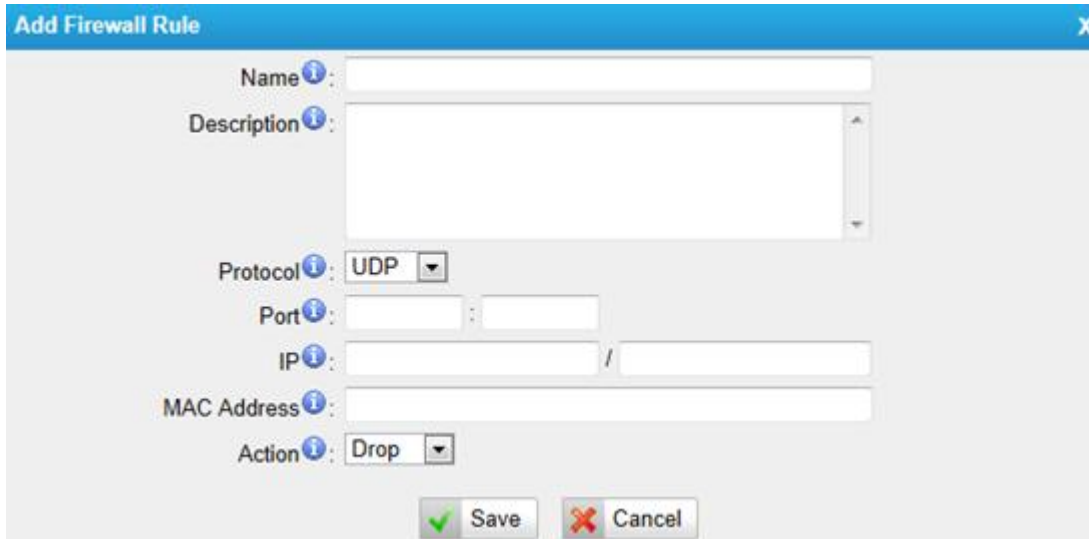


Figure 5-6

•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

Ex:192.168.5.100/255.255.255.255forIP 192.168.5.100

Ex:216.207.245.47/255.255.255.255 for IP 216.207.245.47

Ex:192.168.5.0/255.255.255.0 for IP from 192.168.5.0 to 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.

Note: The MAC address of a remote device will be changed when data reach TE100. So filtering MAC address of remote devices will not work

•Action

Accept: Accept the access from remote hosts.

Drop: Drop the access from remote hosts.

Ignore: Ignore the access.

3) Auto Defense

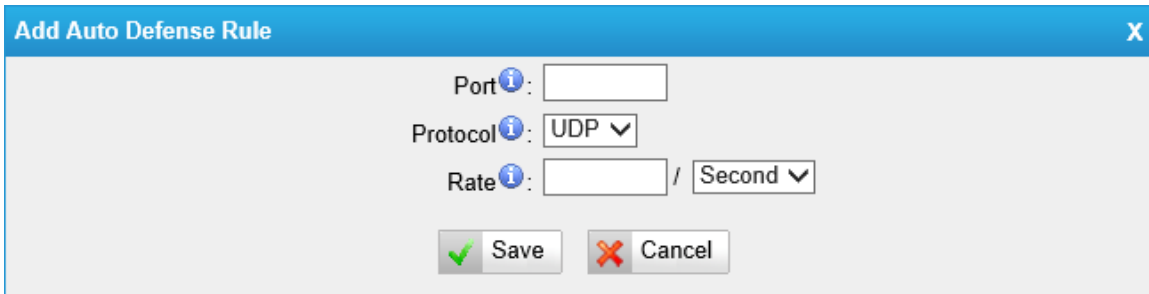


Figure 5-7

•Port

Auto defense port, e.g.: 8022.

•Protocol

Auto defense protocol , TCP or UDP.

•Rate

The maximum packets or connections can be handled per unit time.

E.g.: (Port: 8022 Protocol: TCP Rate: 10/minute) means maximum 10 TCP connections to port 8022 can be handled per minute, the eleventh connection will be refused directly.

5.2.2 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 black IP address and blocked automatically.



Figure 5-8

1) Blacklist rules

We can add the rules for IP blacklist rate as your demand.

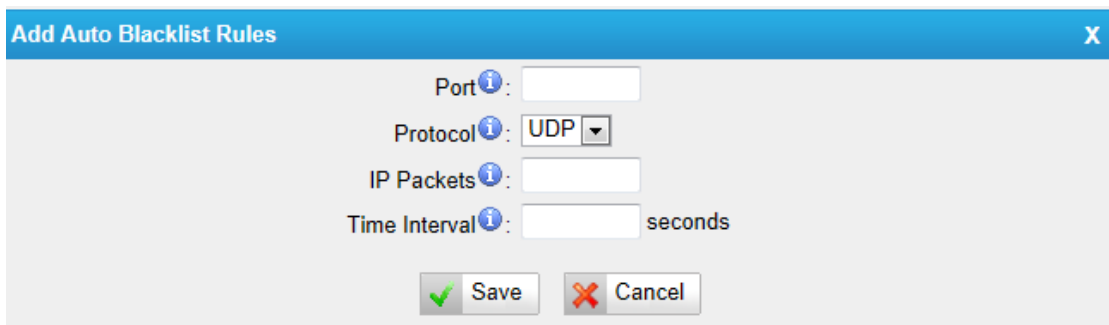


Figure 5-9

•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 your wish.

5.3 system Preferences

5.3.1 Password Settings

We can change the password of account 'admin' in this page, but you need to input the old password before input a new one.

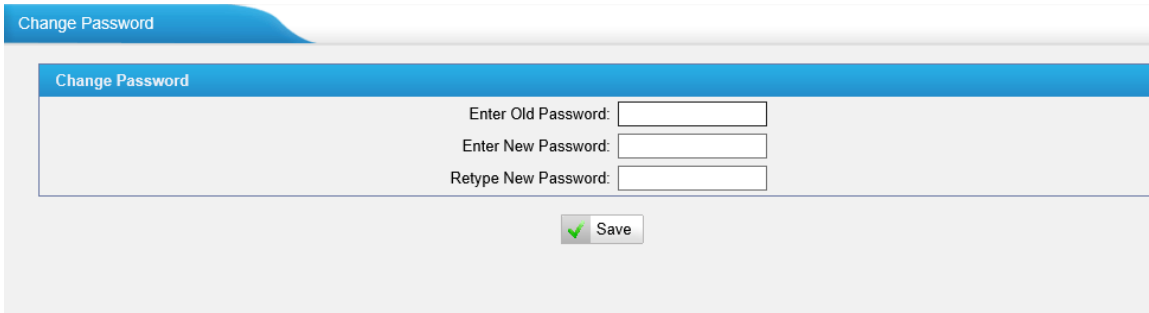


Figure 5-10

●Enter Old Password

The default password of account 'admin' is **'password'**.

●Enter New Password

Input the new password

●Retype New Password

To change the password, enter the new password and click update. The system will then prompt you re-login using your new password.

5.3.2 Date and Time

Set the date and time for TE100.

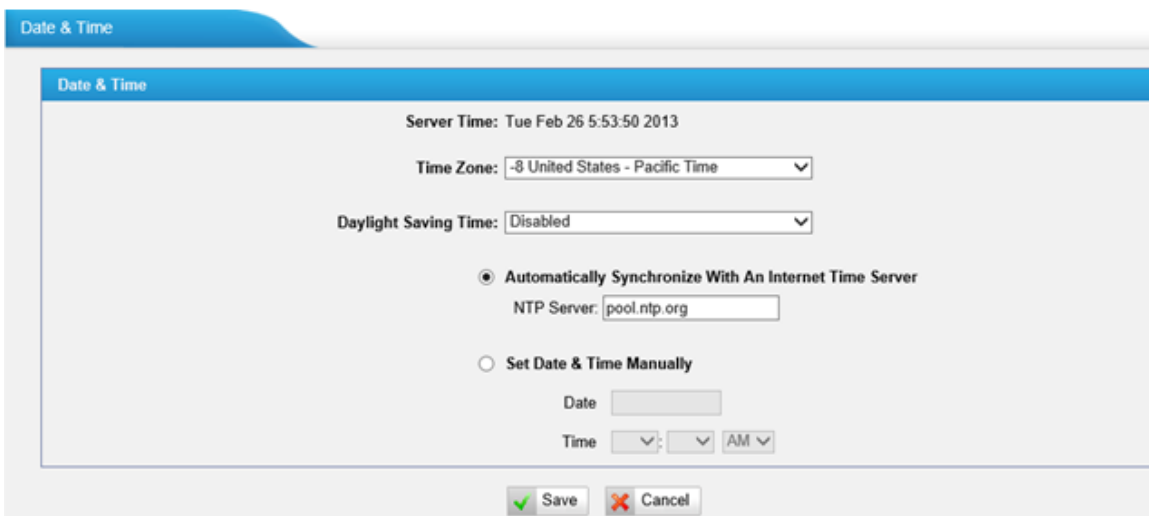


Figure 5-11

•Time Zone

You can choose your time zone here.

•Daylight Saving Time

Set the mode to Automatic or disabled .

•Automatically Synchronize With an Internet Time Server

Input the NTP server so that TE100 will update the time automatically.

•Set Date & Time Manually

You can set the time to your local right time manually here.

5.3.3 Backup and Restore

We can backup up the configurations before reset TE100 to factory defaults, and then restore it using this package.

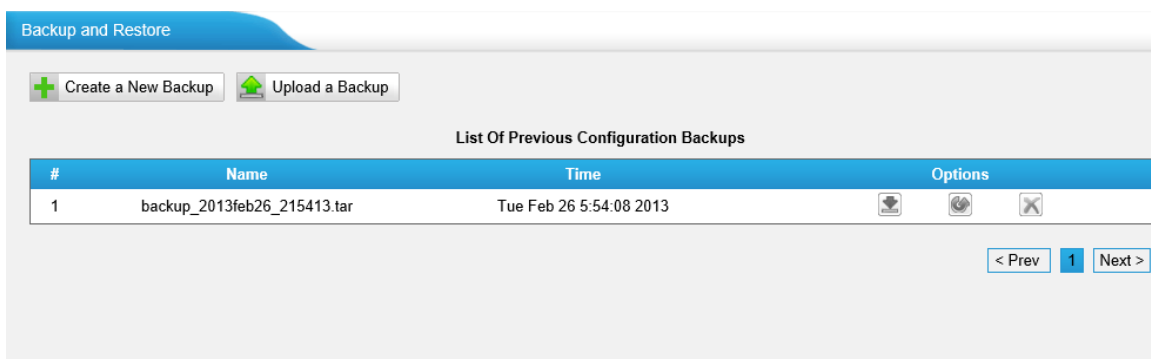


Figure 5-12

To restore the backup package, please click 'Upload a Backup', then upload it from your local PC.

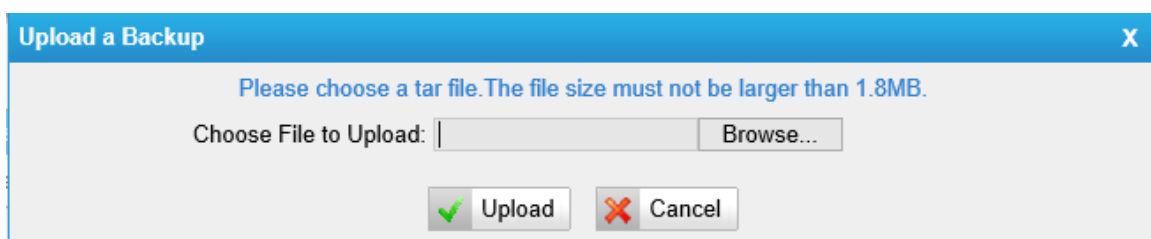


Figure 5-13

Note:

1. Please make sure the file size must not be larger than 1.8MB.
2. When you have updated the firmware version, it's not recommended to restore using old package.

5.3.4 Reset and Reboot

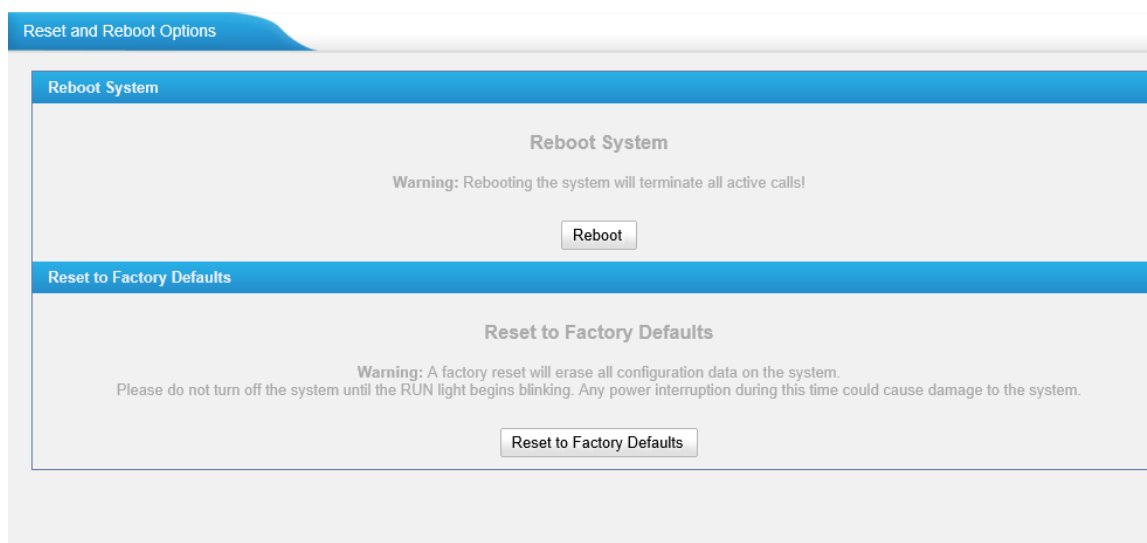


Figure 5-14

•Reboot System

Warning: Rebooting the system will terminate all active calls!

•Reset to Factory Defaults

Warning: A factory reset will erase all configuration data on the system.

Please do not turn off the system until the RUN light begins blinking. Any power interruption during this time could cause damage to the system.

5.3.5 Firmware Update

Upgrading of the firmware is possible through the Administrator web interface using a TFTP Server or an HTTP URL.

Enter your TFTP Server IP address and firmware file location, then click start to update the firmware

Note:

1. If enabled 'Reset configuration to Factory Defaults', System will restore to factory default settings.
2. When update the firmware, please don't turn off the power. Or the system will get damaged.
3. More information for the steps to update the firmware, please refer to this link: http://www.yeastar.com/download/NeoGate_TE100_FirmwareUpgrade_en.pdf

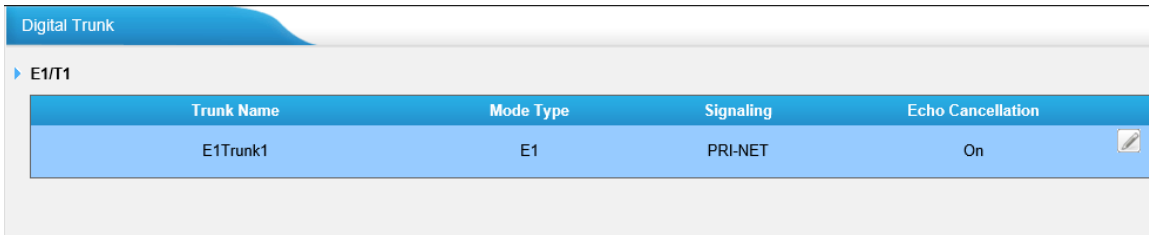


Figure 5-15

6. Gateway

6.1 Digital Trunk

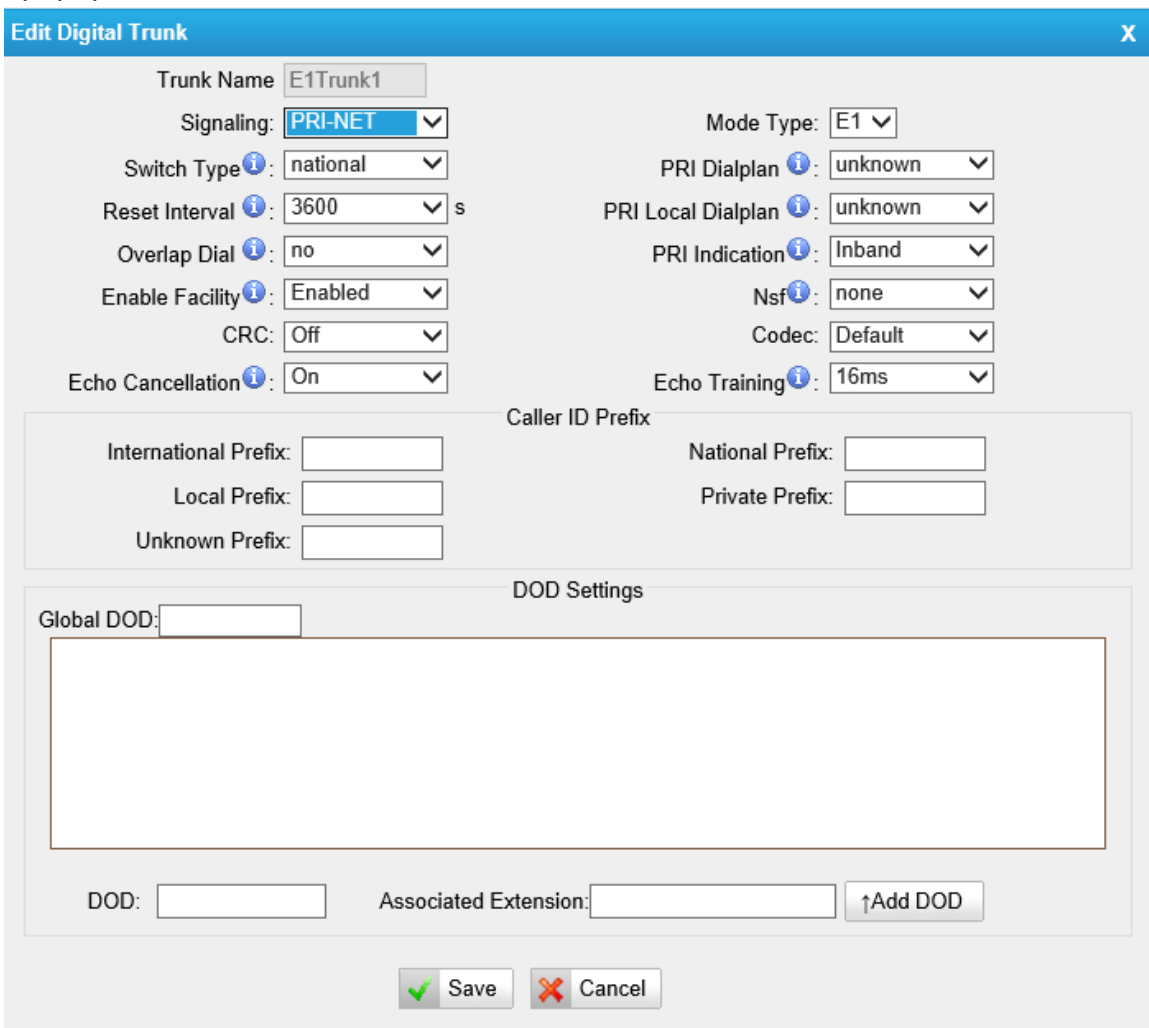
On this page we can configure the details of E1 trunk, before configure anything, please make sure the cable is fine, and you have got enough information from the ISDN provider.



Trunk Name	Mode Type	Signaling	Echo Cancellation
E1Trunk1	E1	PRI-NET	On

Figure 6-1

On the digital trunk page, click 'Edit' on the selected trunk and modify its properties in the popup window:



Edit Digital Trunk

Trunk Name:

Signaling:

Mode Type:

Switch Type:

PRI Dialplan:

Reset Interval: s

PRI Local Dialplan:

Overlap Dial:

PRI Indication:

Enable Facility:

Nsf:

CRC:

Codec:

Echo Cancellation:

Echo Training:

Caller ID Prefix

International Prefix:

National Prefix:

Local Prefix:

Private Prefix:

Unknown Prefix:

DOD Settings

Global DOD:

DOD: Associated Extension:

Figure 6-2

• Trunk name

Set the trunk name

• Signaling

PRI-NET, PRI-CPE, MFC/R2, SS7

• Mode Type

E1 / T1 / J1

• Switch Type

national: National ISDN type2 (common in the US)

ni1: National ISDN type 1

dms100: Nortel DMS100

4ess: AT&T 4ESS

5ess: Lucent 5ESS

euroisdn: EuroISDN

qsig: Minimalistic protocol to build a "network" with two or more PBX of different vendors!

• PRI Dial Plan

Sets an option required for some (rare) switches that require a dial plan parameter to be passed. This option is ignored by most PRI switches. It may be necessary on a few pieces of hardware. This option can almost always be left unchanged from the default.

• Reset interval

Sets the time in seconds between restart of unused channels. Some PBXs don't like channel restarts. so set the interval to a very long interval e.g. 100000000 or 'never' to disable *entirely*. If you are in Israel, the following is important: As Bezeq in Israel doesn't like the B-Channel resets happening on the lines, it is best to set the reset interval to 'never' when installing a box in Israel. Our past experience also shows that this parameter may also cause issues on local switches in the UK and China.

• PRI Local Dial Plan

Sets an option required for some (rare) switches that require a dial plan parameter to be passed. This option is ignored by most BRI switches. It may be necessary on a few pieces of hardware. This option can almost always be left unchanged from the default.

• Over Lap Dial

Define whether TE100 can dial this switch using overlap digits. If you need Direct Dial-in (DDI; in German "Durchwahl") you should change this to yes, then TE100 will wait after the last digit it receives.

• PRI Indication

Tells how Device should indicate Busy() and Congestion() to the switch/user. Accepted

values are:

inband: Device plays indication tones without answering; not available on all PRI/BRI subscription lines .

outofband: Device disconnects with busy/congestion information code so the switch will play the indication tones to the caller. Busy() will now do same as setting PRI_CAUSE=17 and Hangup().

•Facility Enable

To enable transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility).

•NSF

Used with AT&T PRIs. If outbound calls are being rejected due to "Mandatory information element missing" and the missing IE is 0x20, then you need this setting.

•CRC

CRC Verification.

•Codec

Default , A-Law, U-Law.

•Echo Cancellation

Echo cancel Obviously this disables or enables echo cancellation, it is recommended to not turn this off.

•Echo training

In some cases, the echo canceller doesn't train quickly enough and there is echo at the beginning of the call which fades out quickly then.

1) CallerID Prefix

•International Prefix

When there are international calls coming in via this BRI trunk, the International Prefix you have set here will be added before the CID. So you can know this is an international call before you answer it.

•National Prefix

When there are national calls coming in via this BRI trunk, the National Prefix you have set here will be added before the CID. So you can know this is a national call before you answer it.

•Local Prefix

When there are Local calls coming in via this BRI trunk, the Local Prefix you have set here will be added before the CID. So you can know this is a local call before you answer it.

•Private Prefix

When there are Private calls coming in via this BRI trunk, the Private Prefix you have set here will be added before the CID. So you can know this is a Private call before you answer it.

•Unknown Prefix

When there are calls with unknown number coming via this BRI trunk, the Unknown Prefix you set here will be shown as the caller ID.

2) DOD Setting

DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, please make sure the provider supports this feature

•Global DOD

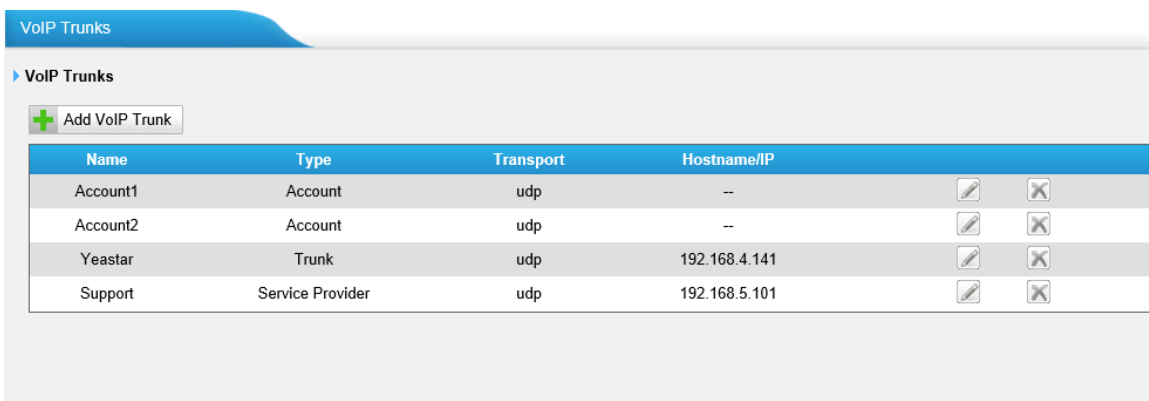
Global direct outward dialing number.

6.2 VoIP settings

In this page, we can create VoIP trunk and the trunk group for routing, and some SIP settings and the general preferences.

6.2.1 VoIP trunk

There are 3 types of trunks listed in this page, 'Account, Trunk and Service Provider'.











Name	Type	Transport	Hostname/IP		
Account1	Account	udp	--		
Account2	Account	udp	--		
Yeastar	Trunk	udp	192.168.4.141		
Support	Service Provider	udp	192.168.5.101		

Figure 6-3

1) Account

Its an SIP account created in TE100 so that the other devices can register SIP trunk at their side using these information.

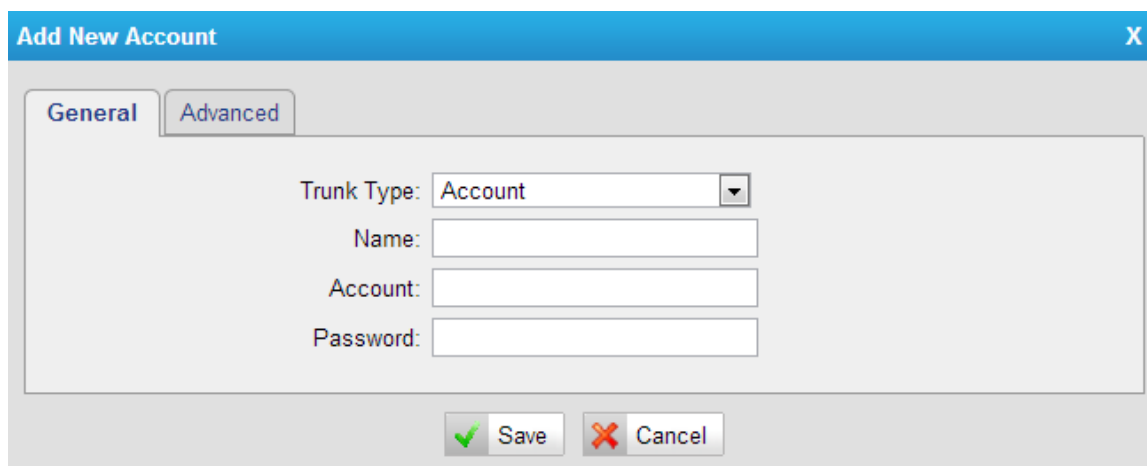


Figure 6-4

•Trunk type:

Choose the type of trunk, for example 'Account'.

•Name:

Input the name of this account trunk.

•Account:

Design the account for other device to register to.

•Password:

Design the password for other device to register to.

•Caller ID:

Design the caller ID to dial out via this account.

2) Trunk

It's a SIP trunk configured in TE100 to register to the SIP provider, please make sure this trunk is working fine in advance with provider before configuring TE100.

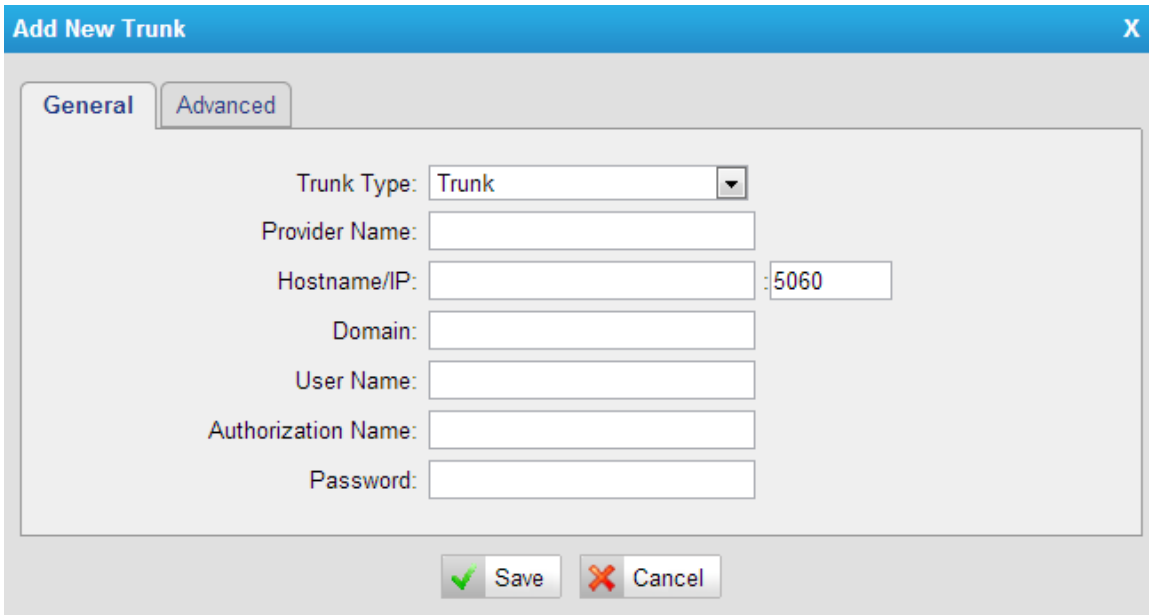


Figure 6-5

•Provider name:

A unique label to help you identify this trunk when listed in outbound rules, incoming rules etc. Ex: 'yeastar'.

•Hostname/IP:

Service provider's 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 provider's server domain name.

•Username

User name of sip account, which is used for sip trunk registration.

•Authorization name

Used for SIP authentication. Leave this blank if not required.

•Password

Password of SIP account.

3) Service provider

This is service provider trunk (peer to peer mode), which authorized using IP address only. If you have got a trunk with IP address only, please choose this type.

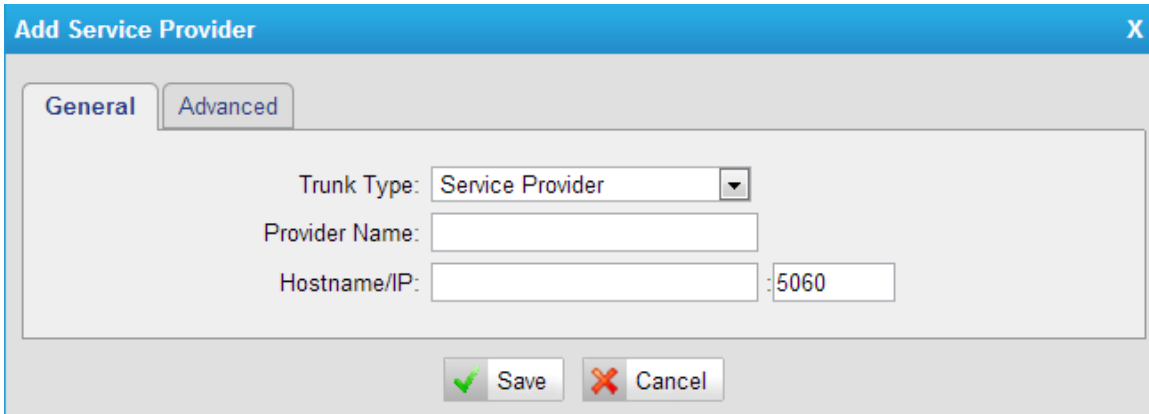


Figure 6-6

•Trunk type:

Choose 'service provider' type.

•Provider Name

A unique label would help to you identify this trunk. Ex: 'Provider2'.

•Hostname/IP

Service provider's hostname or IP address.

Note: 5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.

6.2.2 SIP Settings

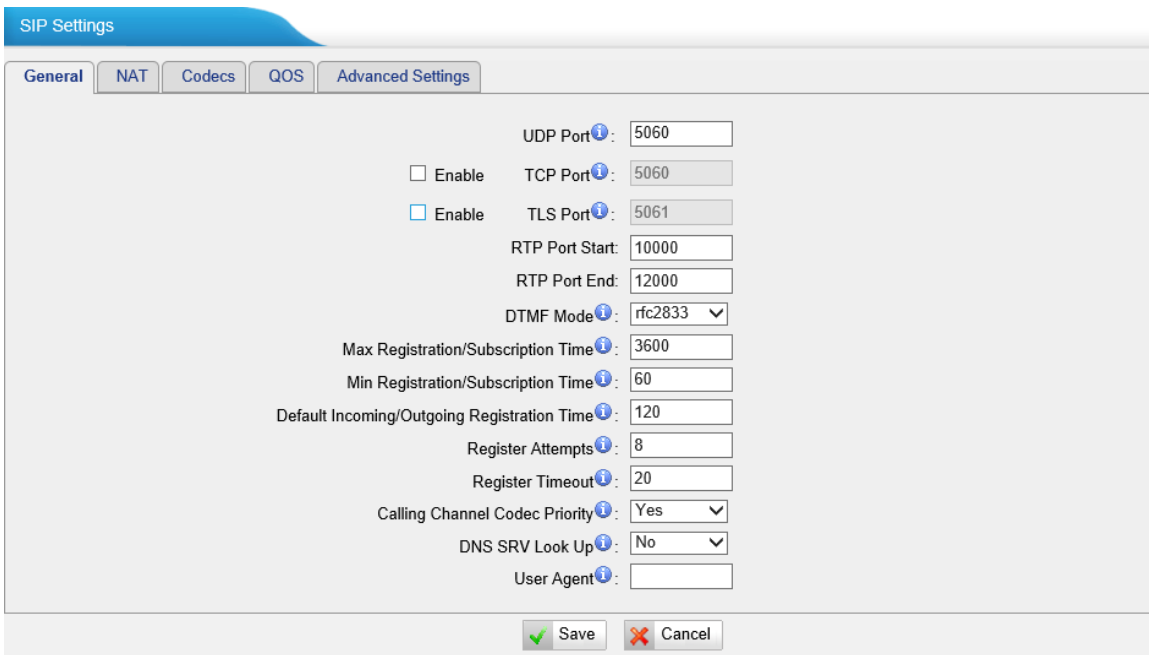


Figure 6-7

1) General

•UDP Port

Port use for sip registrations, Default is 5060.

•TCP Port

Port use for sip registrations, Default is 5060.

•TLS Port

Port use for sip registrations, Default is 5061.

•RTP Port Start

Beginning of RTP port range.

•RTP Port End

End of RTP port range.

•DTMF Mode

Set default mode for sending DTMF. Default setting: rfc2833.

•Max Registration/Subscription Time

Maximum duration (in seconds) of a SIP registration. Default is 3600 seconds.

•Min Registration/Subscription Time

Minimum duration (in seconds) of a SIP registration. Default is 60seconds.

•Default Incoming/Outgoing Registration Time

Default Incoming/Outgoing Registration Time: 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. Default is 8 times.

•Register Timeout

Number of seconds to wait for a response from a SIP Registrar before timed out . 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 in preference. If not, TE100 will follow the priority in your SIP/SPS trunks.

•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, you should change it if needed.

2) NAT

Note: Configuration of this section is only required when using remote registry.

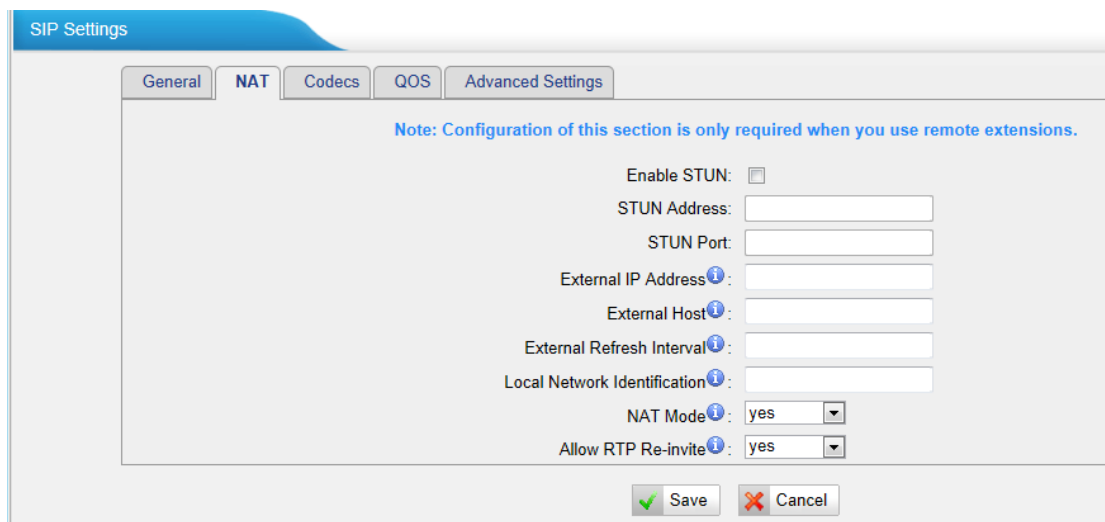


Figure 6-8

•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 be used with this system. Please contact your ISP for more information.

•External Refresh Interval

If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds.

•Local Network Identification

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':AnotherRFC1918withCIDRnotation;

'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 report in headers.

•Allow RTP Reinvite

By default, the system will route media streams 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) Codecs

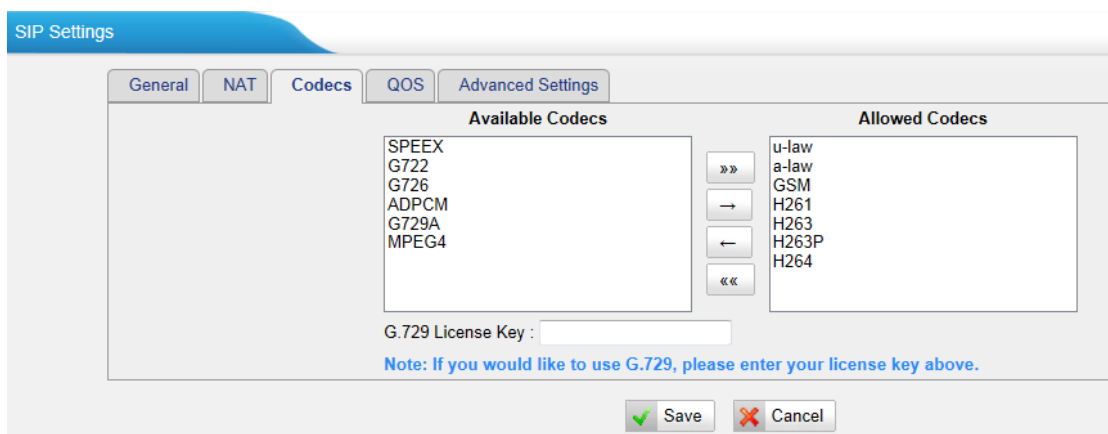


Figure 6-9

A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet.

u-law: A PSTN standard codec, used in North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

a-law: A PSTN standard codec, used outside of North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

GSM: A wireless standard codec, used worldwide, that provides adequate voice quality and consumes 13.3kbit/s in each direction (receiving and transmitting) of a VoIP call. GSM is supported by many VoIP phones.

SPEEX: Speex is an Open Source/Free Software patent-free audio compression format designed for speech. The Speex Project aims to lower the barrier of entry for voice applications by providing a free alternative to expensive proprietary speech codecs. Moreover, Speex is well-adapted to Internet applications and provides useful features that are not present in most other codecs.

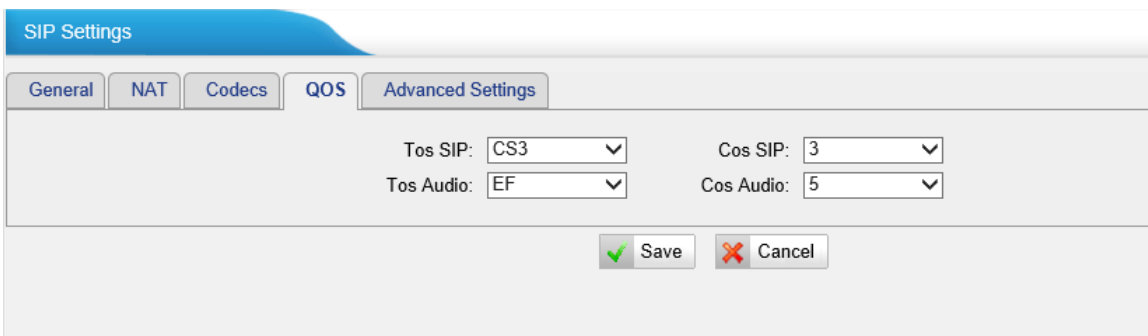
G.722:G.722 is a wideband speech coding algorithms which supports the bit rate of 64, 56 and 48kbps wideband. It's a broadband voice encoding of G series.

G.726: A PSTN codec, used worldwide, that provides good voice quality and consumes 32kbit/s in each direction (receiving and transmitting) of a VoIP call. G.726 is supported by some VoIP phones.

ADPCM, G.729A, H261, H263, H263p, H264,MPEG4.

Note: If you would like to use G.729, please enter your license.

4) QOS



The screenshot shows the 'SIP Settings' window with the 'QOS' tab selected. The 'Advanced Settings' sub-tab is active. The configuration is as follows:

Field	Value
Tos SIP	CS3
Cos SIP	3
Tos Audio	EF
Cos Audio	5

Buttons: Save (green checkmark), Cancel (red X).

Figure 6-10

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.

5) Advanced Settings

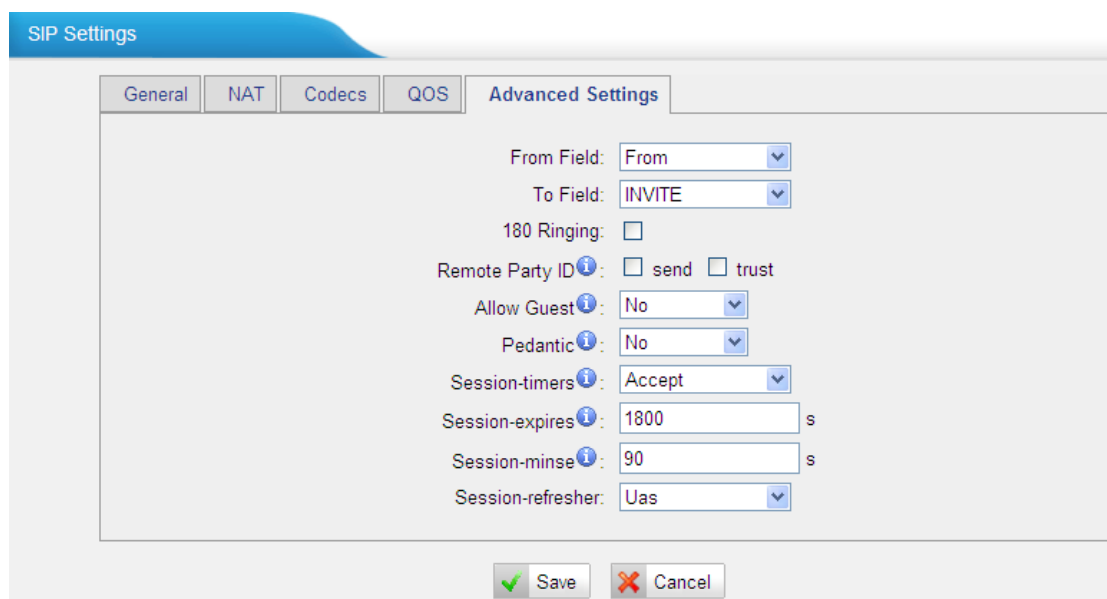


Figure 6-11

•From Field

Where to get the caller ID in sip packet.

•To Field

Where to get the DID in sip packet.

•180 Ringing

It is set when the telecom provider needs. Usually it is not needed.

•Qualify

Send check alive packets to the sip provider.

•Remote Party ID

Whether send Remote-Party-ID on SIP header. Default no.

•Allow Guest

Whether allow anonymous registration extension. Default: no.

This option is used to avoid some anonymous calls by hackers.

•Pedantic

Enable pedantic parameter. Default: no.

•Session -timers

Enable session-timer mode, default: yes.

•Session-expires

The max refresh interval.

•Session-minse

The min refresh interval, which mustn't be less than 90s .

•Session-refresher

Choose session-refersher, the default is Uas.

6.2.3 Trunk Group

Trunk group is a new feature that allowed adding some trunks into a group, which we can use it in the 'routing rules'.

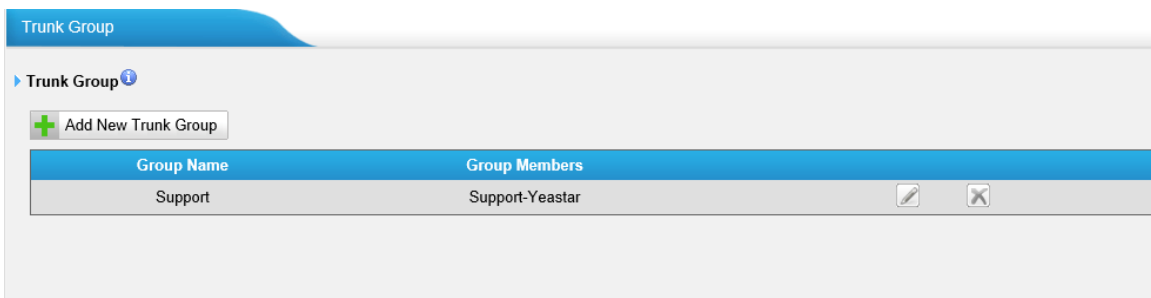


Figure 6-12

Click 'Add New Trunk Group'.

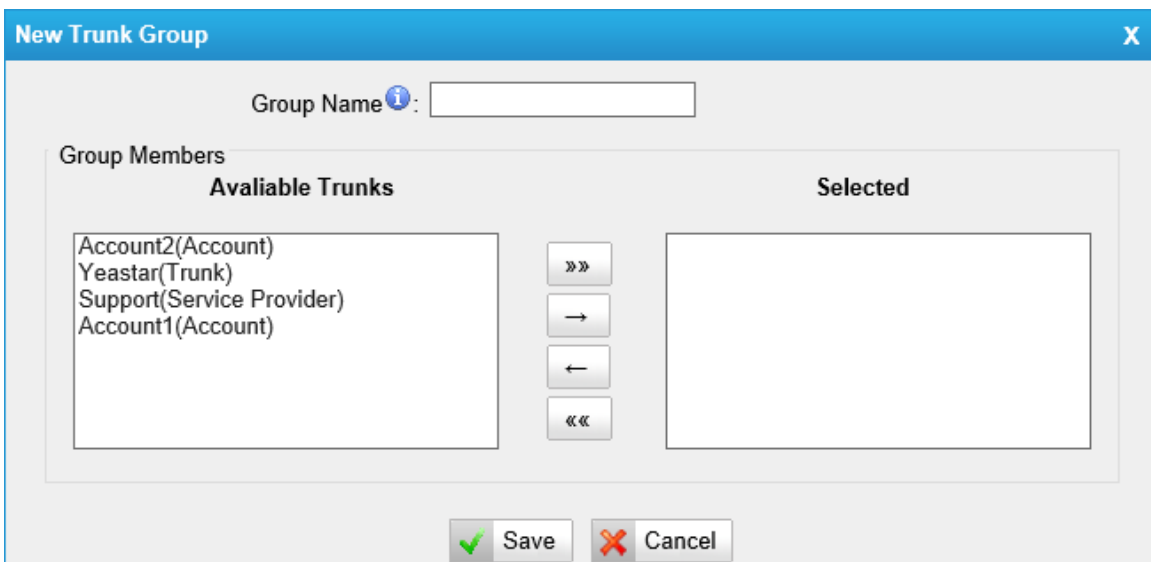


Figure 6-13

Group name

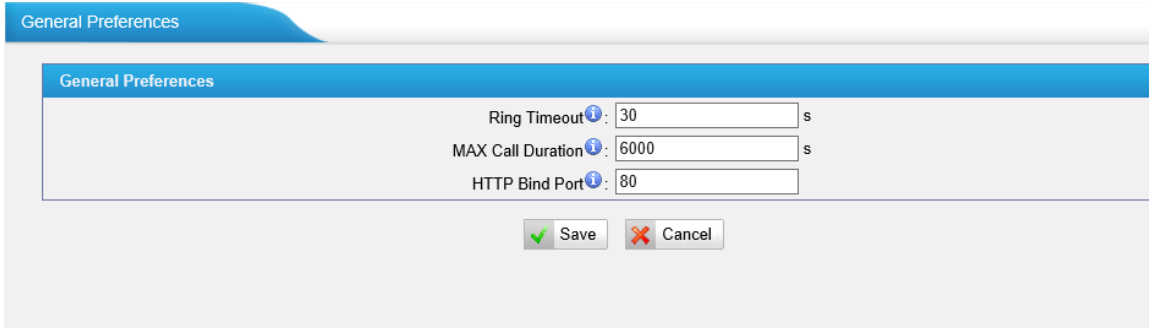
Input the name of this group.

Group members

All the SIP trunk you created will be listed here, please choose the appropriate trunk to the right side as a group.

6.2.4 General Preferences

This is the general preferences of TE100



General Preferences

General Preferences

Ring Timeout: 30 s

MAX Call Duration: 6000 s

HTTP Bind Port: 80

Save Cancel

Figure 6-14

•Ring Timeout

Number of seconds to ring a device before handling the call, default value is 30s.

•MAX call duration

The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout. Default value is 6000s.

•HTTP bind port/Web Access Port

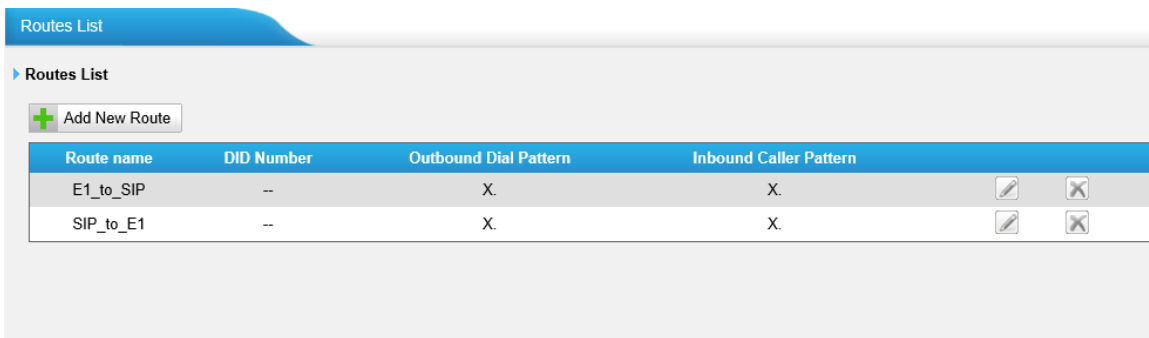
Port to use for HTTP sessions. Default: 80

Note: please reboot the system to take effect.

6.3 Routes Settings

There are two default routes to route the calls from E1 to SIP and SIP to E1.

In this page, we can route the call from one trunk to another trunk or a trunk group.



Routes List

Routes List

+ Add New Route





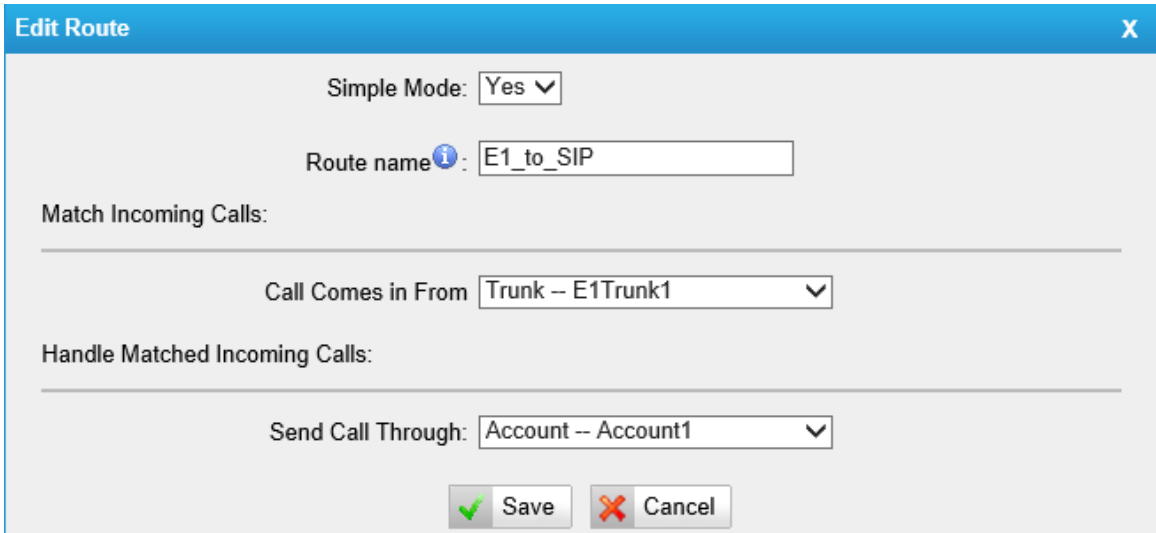
Route name	DID Number	Outbound Dial Pattern	Inbound Caller Pattern		
E1_to_SIP	--	X.	X.		
SIP_to_E1	--	X.	X.		

Figure 6-15

6.3.1 Route List

Click 'edit' to check the details, there are two modes for you.

1) Simple mode



The screenshot shows the 'Edit Route' dialog box in 'Simple Mode'. The 'Simple Mode' dropdown is set to 'Yes'. The 'Route name' field contains 'E1_to_SIP'. Under the 'Match Incoming Calls' section, the 'Call Comes in From' dropdown is set to 'Trunk -- E1Trunk1'. Under the 'Handle Matched Incoming Calls' section, the 'Send Call Through' dropdown is set to 'Account -- Account1'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 6-16

Route name:

A name for this route.

Match incoming calls:

Choose the trunk or trunk group for the incoming calls

Handle matched incoming calls:

choose the trunk or trunk group to route the incoming calls to.

2) Detailed mode

Detailed mode can be accessed to by choosing 'No' for 'Simple mode'.

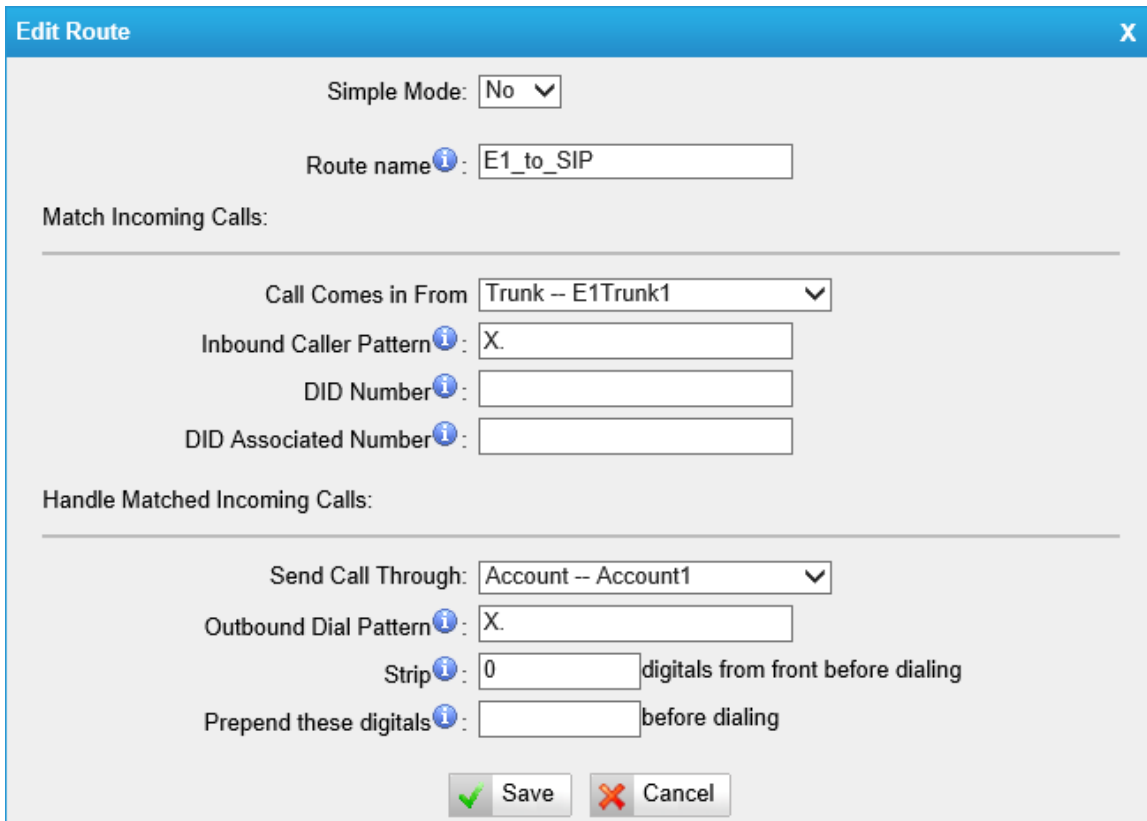


Figure 6-17

Route name:

A name for this route.

Match incoming calls:

Choose the trunk or trunk group for the incoming calls.

Inbound caller pattern:

Match the prefix of caller ID for incoming calls.

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

[12345-9]: Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)

The `.'Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.

The `!' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX** will match any 7 digits phone number.

Example 2: **1NXXNXXXXXX** will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

DID number:

Define 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. You can also use pattern matching to match a range of numbers.

DID Associated Number:

Define the extension for DID number. This field is only valid when you use BRI, SIP, SPS or SPX trunk for this inbound router. You can only input number and '-' in this field, and the format can be xxx or xxx-xxx. The count of the number must be only one or equal the count of the DID number.

Handle matched incoming calls:

choose the trunk or trunk group to route the incoming calls to.

Outbound Dial Pattern

Outbound calls that match this dial pattern will use this outbound route. There are a number of dial pattern characters that have special meanings:

X: Any Digit from 0-9

Z: Any Digit from 1-9

N: Any Digit from 2-9

[12345-9]: Any digit in the brackets (in this example, 1, 2, 3, 4, 5, 6, 7, 8, 9)

The '.' Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.

The '!' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX** will match any 7 digits phone number.

Example 2: **1NXXNXXXXXX** will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

Strip digits from front before dialing

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. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.

Prepend these digits before dialing

These digits will be prepended to the phone number before the call is placed. For example, if a trunk requires 10 digit dialing, but users are more comfortable with 7 digit dialing, this field could be used to prepend a 3 digit area code to all 7 digit phone numbers before calls are placed.

6.3.2 Blacklist

Blacklist is used to block an incoming/outgoing call. If the number of incoming/outgoing call is listed in the number blacklist, the caller will hear the following prompt: "The number you have dialed is not in service. Please check the number and try again". The system will then disconnect the call.

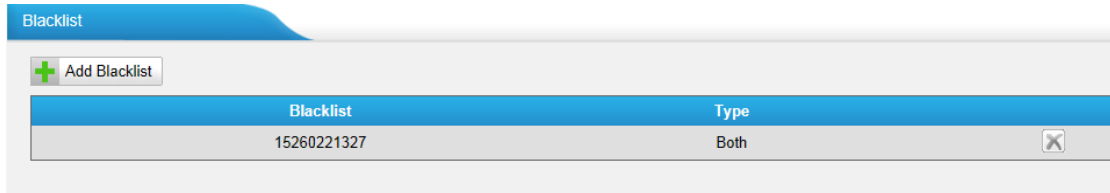


Figure 6-18

We can add a number with the type: inbound, outbound or both

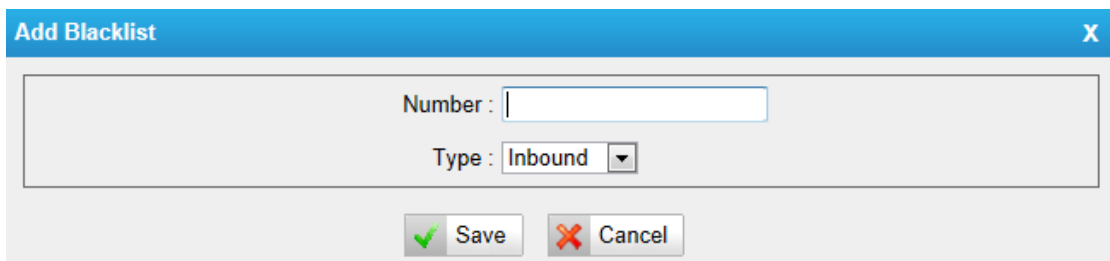


Figure 6-19

7. Logout



Click  to log out safely to the log in page.

8 Application

Application 1

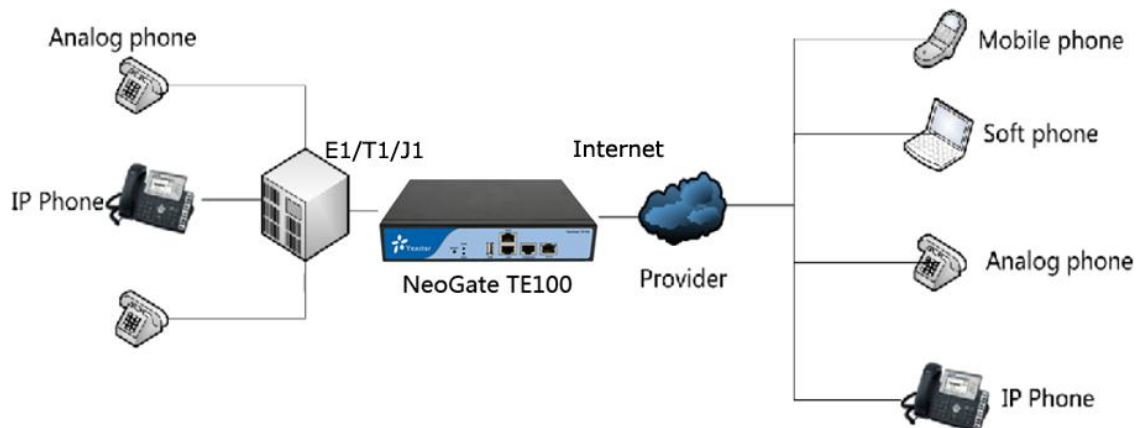


Figure 8-1

Application 2

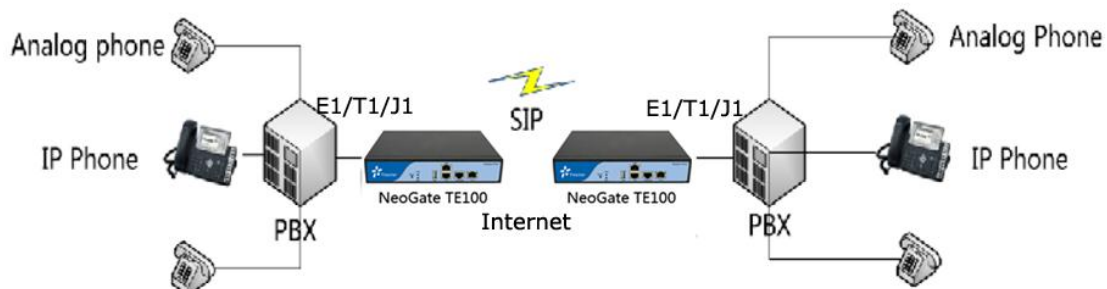


Figure 8-2

<Finish>