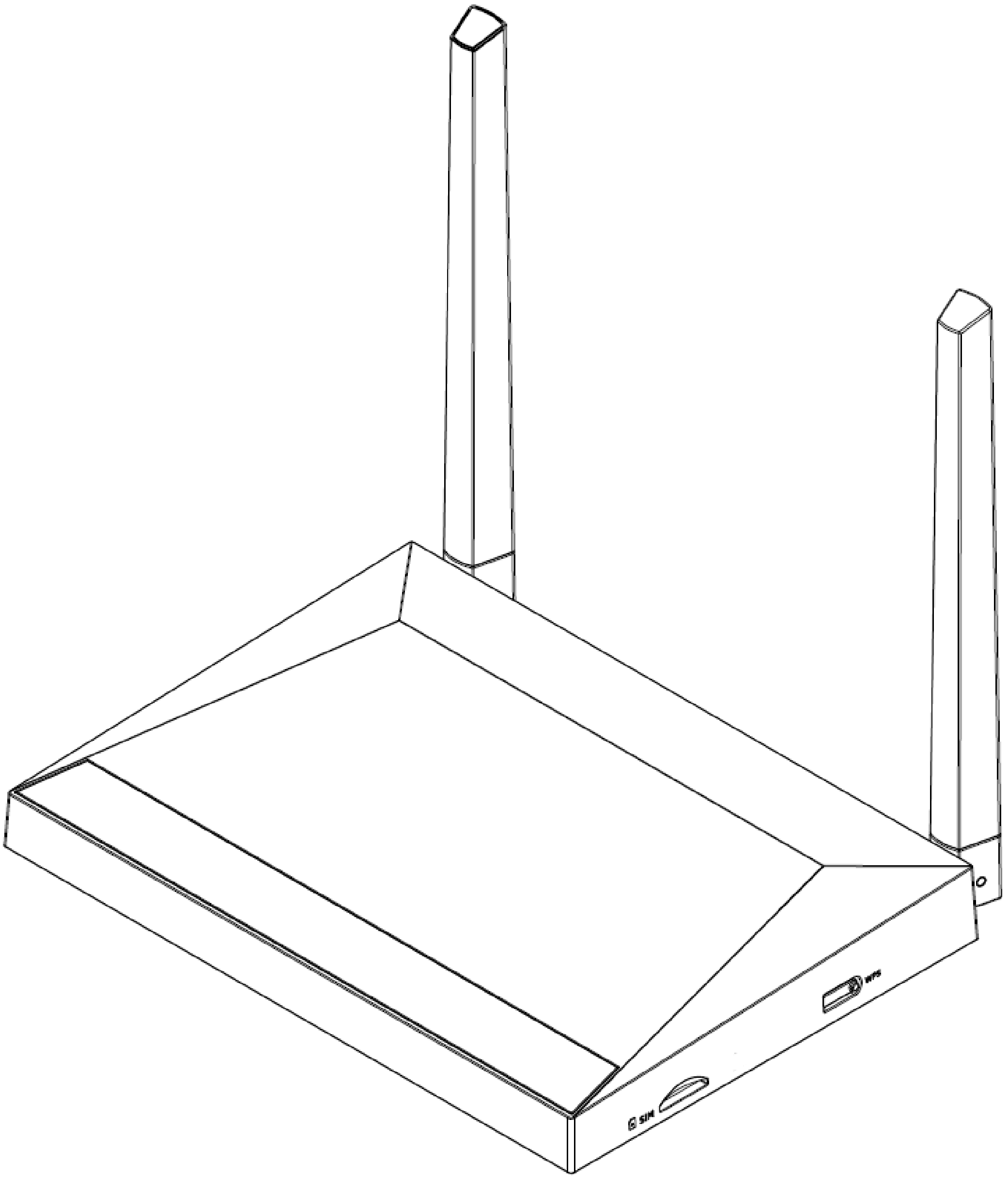
TPX820 User Manual

V1.0

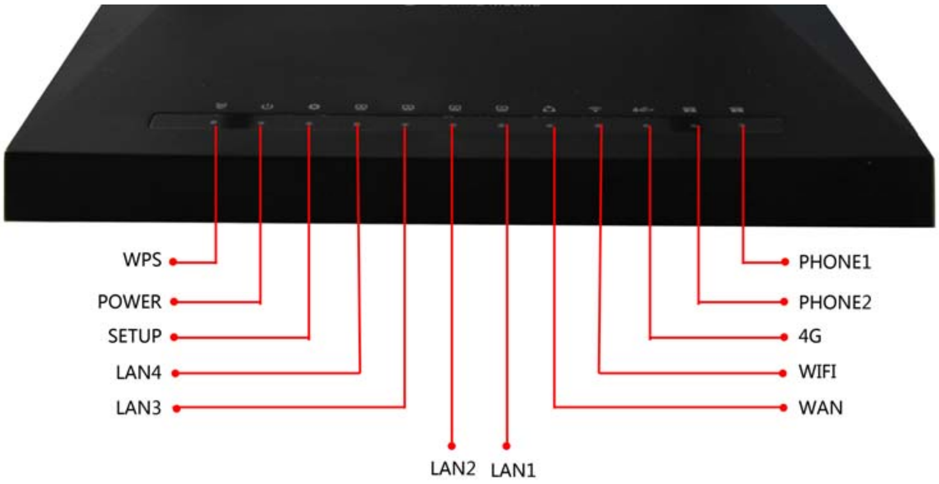


1.LEDIndicators& Cables

Before you use this product, you must first have a general understanding of LED indicators, and how to connect.

1.1 LED indicator

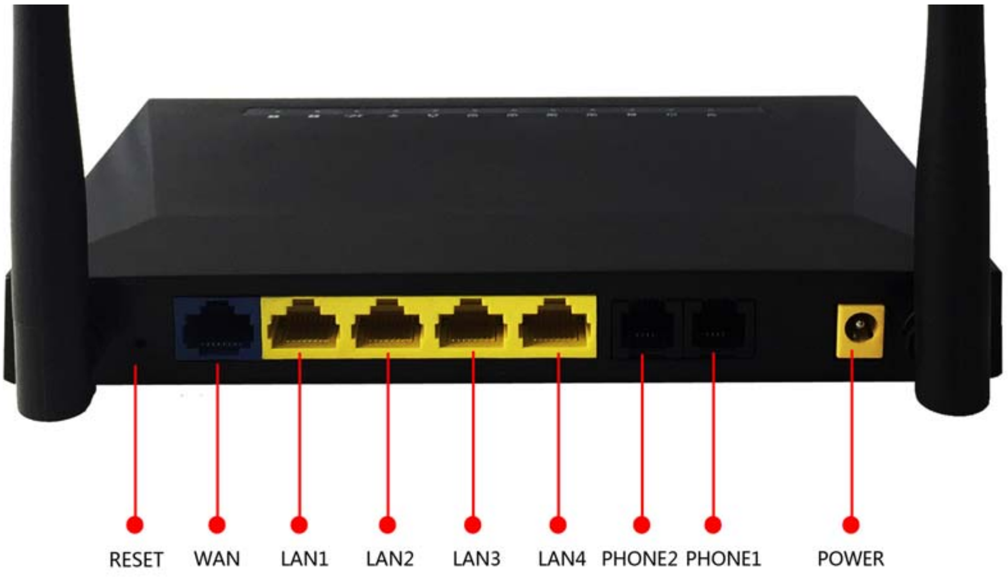
(1)Front View



LED	Status	Description
Phone1 / 2	Flashing (green)	There is a service stream or is being registered
	Steady (Green)	Successfully registered to the soft switch, but no business flow
LAN 1/2/3/4	Steady (Green)	Network interface is connected, but no data transmission.
	Off	The system is not powered on or the network interface is not connected to the network device

	Flashing (green)	There is data transmission
WAN	Steady (Green)	The network connection is successful and the physical connection has been established
	Off	The network is not connected or the connection fails
	Flashing (green)	There is data transmission
POWER	Steady (red)	The system is powered up normally
	Off	The system is not powered on
WLAN	Steady (Green)	WIFI switch is turned on, AP work
	Flashing (green)	There is data transmission

(2)Back View



Interface	Description
Power	Connect the power adapter

Phone1 / 2	Connect the phone
USB	USB interface
WAN	Connect access to the Internet
LAN (1/2/3/4)	WIFI network device connected to a local switch

1.2 Hardware Installation

Before setting up your home gateway, you must connect your device correctly:

Use Ethernet as Uplink

1. With RJ-11 cable to connect a telephone to a fixed telephone jack port;
2. Device with an Ethernet cable and a modem connected wan port;
3. The LAN port your computer device connected via RJ-45 cable;
4. One end of the power cord is connected to the power interface of the device and the other end is connected to an electrical outlet;
5. Start the router
6. Check the power, wan LAN port opening and an LED lamp to ensure network connection.

Use LTE as uplink

1. With RJ-11 cable to connect a telephone to a fixed telephone jack port;
2. Check that the SIM card is connected;
3. The LAN port your computer device connected via RJ-45 cable;

4. One end of the power cord is connected to the power interface of the device and the other end is connected to an electrical outlet;
5. Start the router
6. Check power, LTE and LAN port LED lamp to ensure network connection.

Warning –

Part 15.19

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Part 15.21

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Part 15.105

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

2.Web admin page settings

2.1 WEB login page

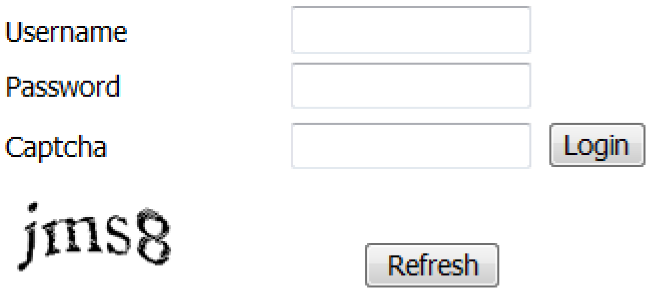
Built-in Web server device in response to HTTP get / post request. Users can use a Web browser, such as Microsoft's IE to the login theWEBadminpage and configure the device.

2.1.1 URL format

URL format login web page is:

http: //LAN port IP address

Usually the default LAN port IP address: 192.168.3.1, enter the appropriate address in the address input field, and the page will jump to the login page for the device, As shown below:



2.1.2 About password

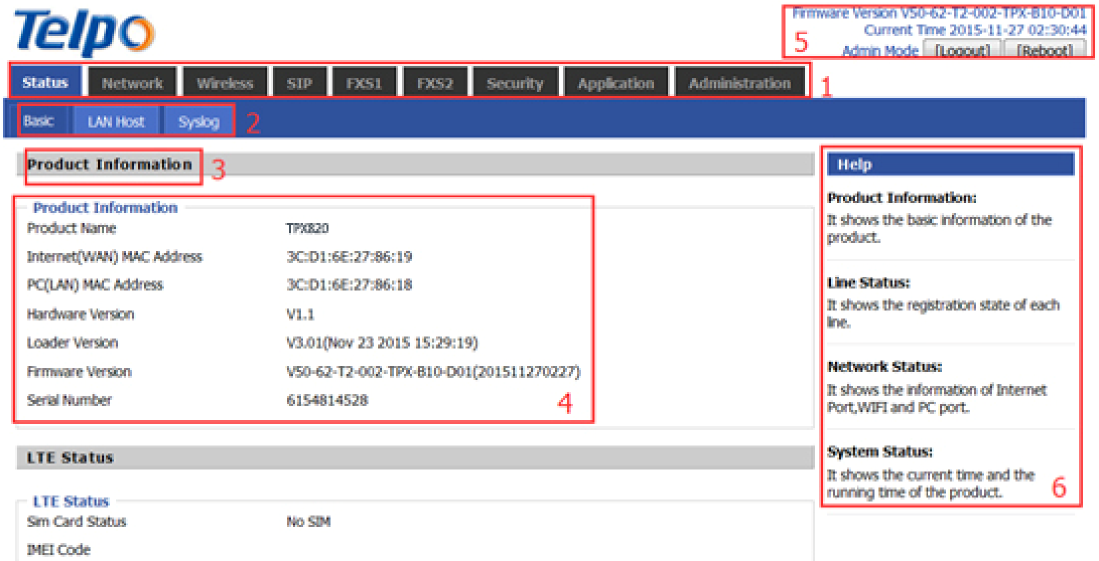
Log level TPX820 has two, namely general and administrator-level user level, different standards have different passwords.

General level users to browse and configure all TPX820 parameters, in addition to the SIP line can not be changed in some parameters, such as server address and port; the administrator level user can configure all other parameters.

TPX820 default management-level password: admin

TPX820 default normal user password: user

2.2 WEB admin page



Firmware Version V50-62-T2-002-TPX-B10-D01
Current Time 2015-11-27 02:30:44
Admin Mode

Product Information

Product Information

Product Name	TPX820
Internet(WAN) MAC Address	3C:D1:6E:27:86:19
PC(LAN) MAC Address	3C:D1:6E:27:86:18
Hardware Version	V1.1
Loader Version	V3.01(Nov 23 2015 15:29:19)
Firmware Version	V50-62-T2-002-TPX-B10-D01(201511270227)
Serial Number	6154814528

LTE Status

LTE Status

Sim Card Status	No SIM
IMEI Code	

Help

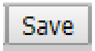
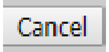
Product Information:
It shows the basic information of the product.

Line Status:
It shows the registration state of each line.

Network Status:
It shows the information of Internet Port,WIFI and PC port.

System Status:
It shows the current time and the running time of the product.

Numbering	name	description
1	Times the navigation bar	Click the secondary navigation bar, the corresponding sub navigation bar will appear
2	Sub navigation bar	Click the child navigation bar to enter the corresponding configuration page
3	title	Configure the title
4	Configuration bar	Configuration bar
5	Device Information	TPX820 display firmware version, DSPversion, the current time and management. The user presses the exit to exit, press restart to restart.
6	Help	Display help information, the user can get help here
	Save & Apply Save Cancel Reboot	
Save & Apply	After the parameters are changed, you need to click the button to save to make it functional. When you see notifications like Please REBOOT to make the changes effective! you are most likely need to reboot the device.	

	The single Save button means your parameters will be saved but it won't be effective until you really apply them or reboot the device.
	Click this button to cancel the change
	Click this button to restart the device

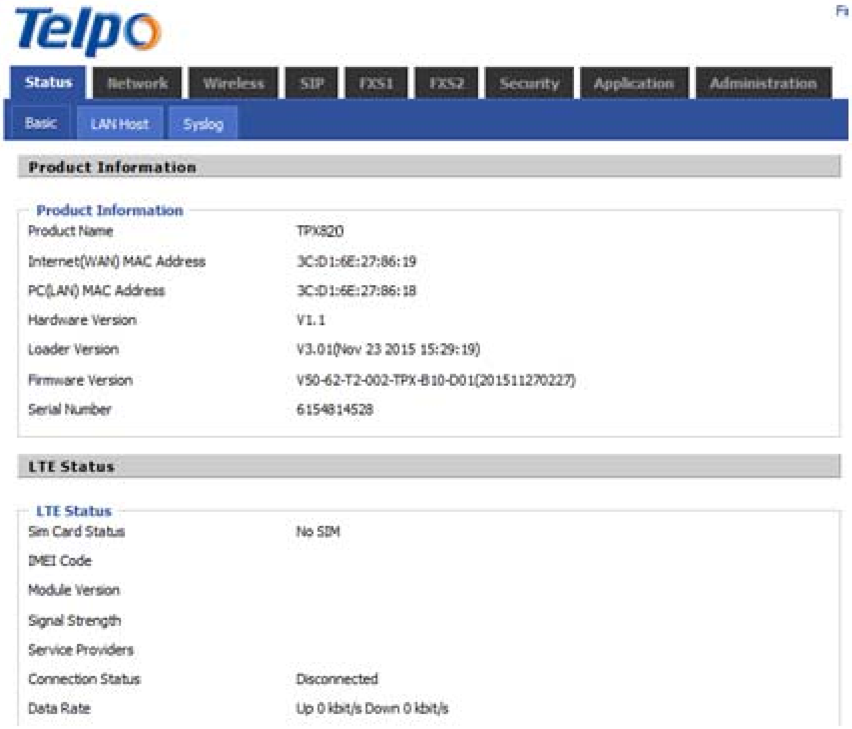
3. Configure from WEBadmin page

3.1 Status

In this page, the user can view the system information and system log information of the home gateway. Users landing through the web page after the first jump is the page.

3.1.1 System Information

In this page, users can view the product information of the home gateway, SIP account status, network status and system status.



Product Information

Product Information

Product Name	TPX820
Internet(WAN) MAC Address	3C:D1:6E:27:86:19
PC(LAN) MAC Address	3C:D1:6E:27:86:18
Hardware Version	V1.1
Loader Version	V3.01(Nov 23 2015 15:29:19)
Firmware Version	V50-62-T2-002-TPX-B10-D01(201511270227)
Serial Number	6154814528

LTE Status

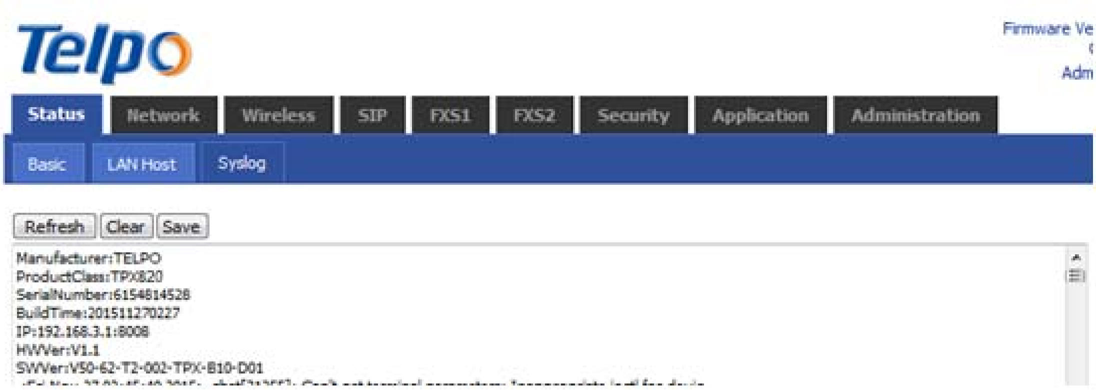
LTE Status

Sim Card Status	No SIM
IMEI Code	
Module Version	
Signal Strength	
Service Providers	
Connection Status	Disconnected
Data Rate	Up 0 kbit/s Down 0 kbit/s

3.1.2 System Log

In this configuration page, the user can view the system records; the system records contain the home gateway important configuration information.

In this page, the user can refresh, clear, and save the relevant system information by clicking the appropriate button.



```
Manufacturer:TELPO
ProductClass:TPX820
SerialNumber:6154814528
BuildTime:201511270227
IP:192.168.3.1:8008
HWVer:V1.1
SWVer:V50-62-T2-002-TPX-B10-D01
```

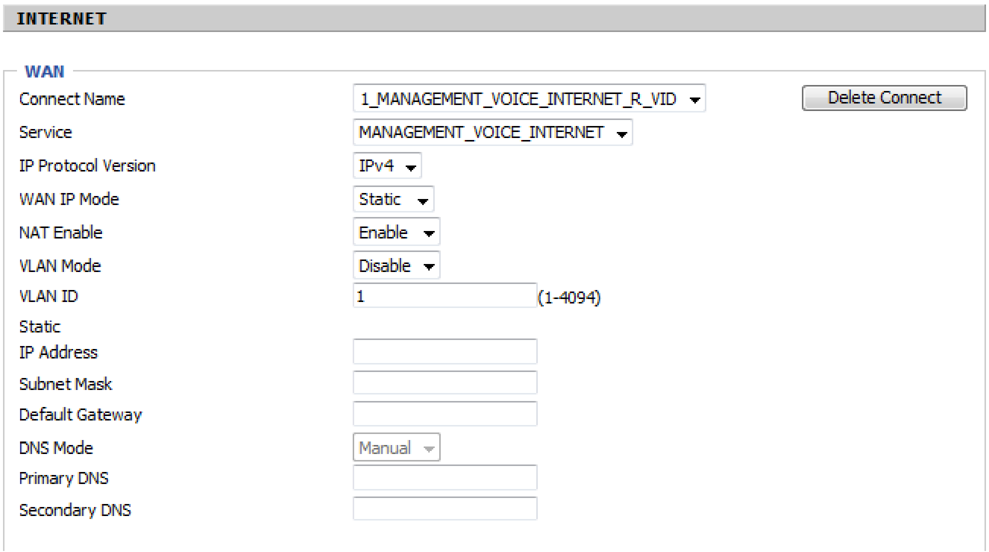
3.2 Network

3.2.1 WAN

(1) Static IP

When the gateway WAN port status is set to static, the user needs to configure an IP address, subnet mask, default

gateway, DNS and the preferred value of the alternative DNS.



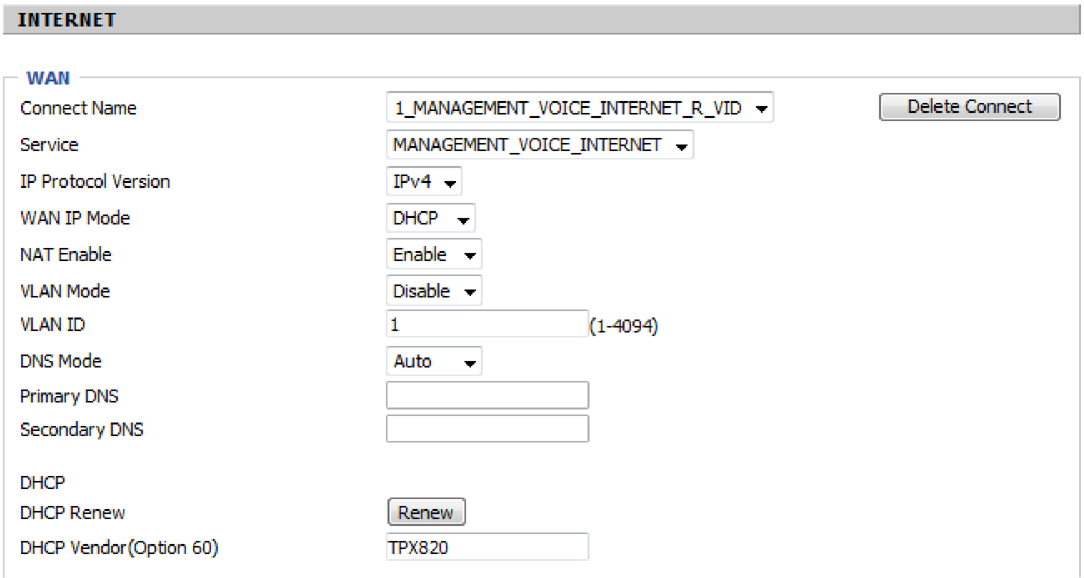
INTERNET

WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID	Delete Connect
Service	MANAGEMENT_VOICE_INTERNET	
IP Protocol Version	IPv4	
WAN IP Mode	Static	
NAT Enable	Enable	
VLAN Mode	Disable	
VLAN ID	1 (1-4094)	
Static		
IP Address		
Subnet Mask		
Default Gateway		
DNS Mode	Manual	
Primary DNS		
Secondary DNS		

parameter name	Description
Service (name)	(Set the parameters in a multi-WAN port settings page) with the keyword marked WAN port service model
IP protocol mode	There are only a temporary connection mode IPv4
INTERNET access	Select Static IP
Enable NAT	WAN port needs to be set in a multi-page, see 3.2.7
DHCP Service Type	Optional "pass-through" "Snooping" "Native service"
VLAN mode	WAN port needs to be set in a multi-page, see 3.2.7
VLAN ID	WAN port needs to be set in a multi-page, see 3.2.7
IP addresses	IP Internet ports
Subnet mask	The subnet mask for the Internet port
Default gateway	The default gateway for the Internet port
DNS Mode	This is an optional option
Primary DNS	Primary DNS Internet port
Secondary DNS	Secondary DNS Internet port

(2) DHCP mode



INTERNET

WAN

Connect Name: 1_MANAGEMENT_VOICE_INTERNET_R_VID

Service: MANAGEMENT_VOICE_INTERNET

IP Protocol Version: IPv4

WAN IP Mode: DHCP

NAT Enable: Enable

VLAN Mode: Disable

VLAN ID: 1 (1-4094)

DNS Mode: Auto

Primary DNS:

Secondary DNS:

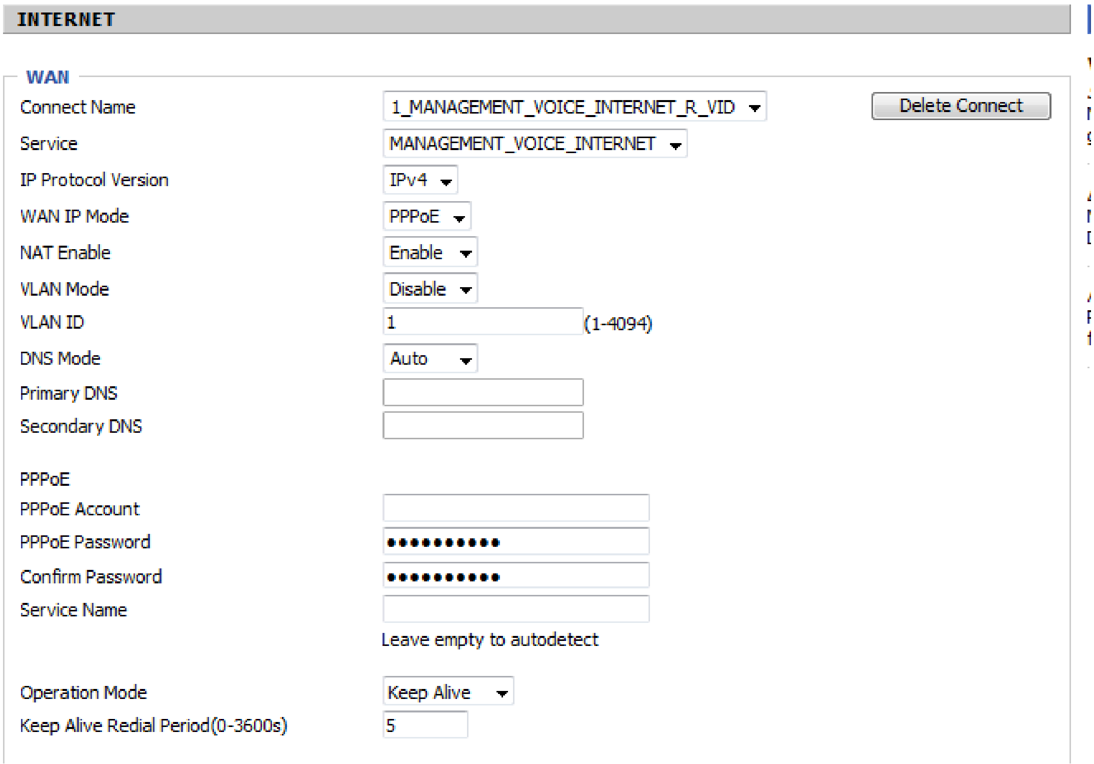
DHCP

DHCP Renew: Renew

DHCP Vendor(Option 60): TPX820

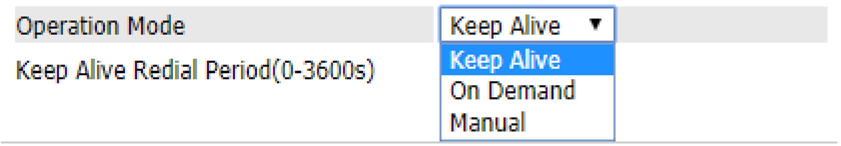
Parameter name	description
service name	Use keywords to indicate service mode WAN1 ~ WAN5(set parameters in the multi-WAN port settings page)
Connection mode	There are only a temporary connection mode IPv4
INTERNET access	Select DHCP
DNS Mode	And automatically selecting from the specified DNS-type two modes. ♦ DNS type to Auto, the home gateway willautomatically obtain preferred DNS and alternateDNS DHCP server. ♦ DNS type is specified, the user should manually configure the preferred and alternative DNS DNS.
Primary DNS	Equipment preferred DNS
From DNS	Equipment Secondary DNS
DHCP update	Refresh DHCP IP
DHCP Vendor (Option60)	Specifies the DHCP Vendor field

(3) PPPOE mode

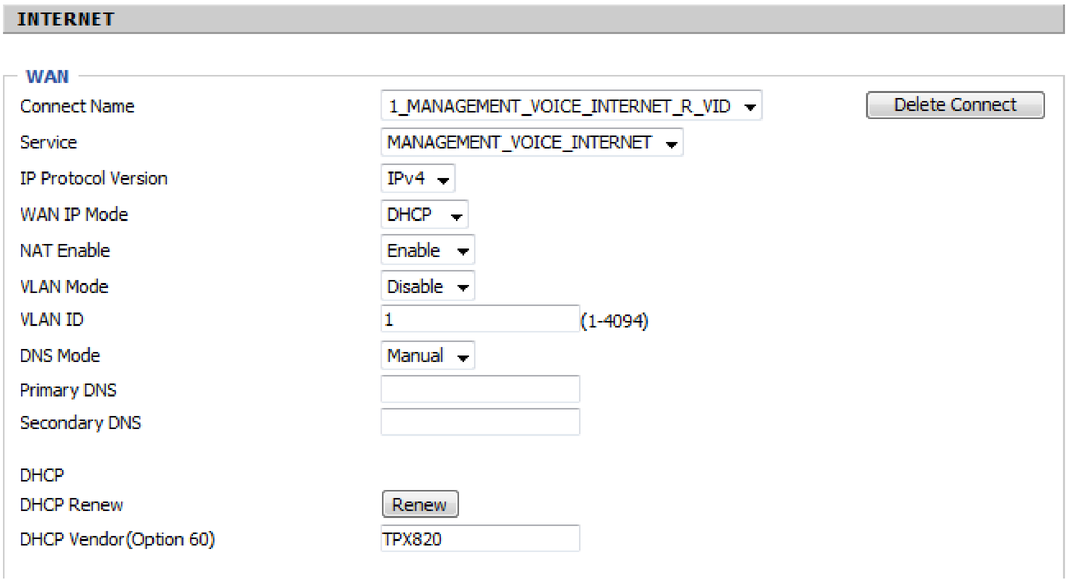


Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID
Service	MANAGEMENT_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	PPPoE
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Auto
Primary DNS	
Secondary DNS	
PPPoE	
PPPoE Account	
PPPoE Password	••••••••••
Confirm Password	••••••••••
Service Name	 Leave empty to autodetect
Operation Mode	Keep Alive
Keep Alive Redial Period(0-3600s)	5

parameter name	Description
service name	Use keywords to indicate service mode WAN1 ~ WAN5(set parameters in the multi-WAN port settings page)
Connection mode	There are only a temporary connection mode IPv4
INTERNET access	Select PPPoE
username	Fill in the PPPoE account obtained from the Internetservice provider
password	Fill in the PPPoE password obtained from your Internetservice provider
confirm password	Enter the PPPoE password again

Running mode	Select Options from the Keep Alive, On Demand, andManual mode in three ways: When the mode is when ♦ Keep Alive, the user needs to set the 'keep alive redial period' value in the range of 0to 3600s, the default setting is 60s; When the mode is ♦ On Demand, users need to set them on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; ♦ When the mode is Manual, which do not need to fill in two settings.
Operation Mode	**Keep Alive,** transmission time interval
 Operation Mode: Keep Alive ▼ Keep Alive Redial Period(0-3600s) Keep Alive On Demand Manual	
Keep Alive Redial Period	Set On demand transmission time interval

(4) Bridge Mode



INTERNET

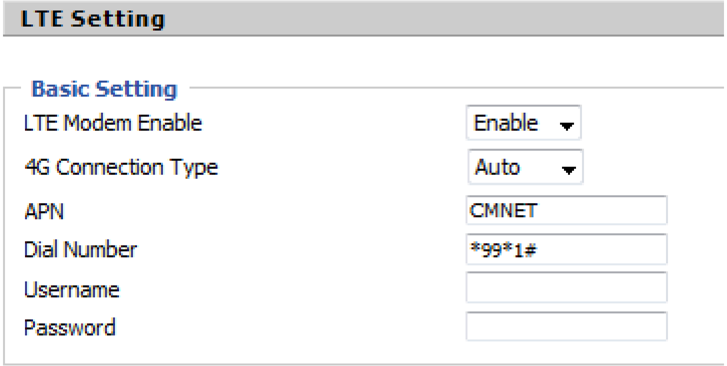
WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID
Service	MANAGEMENT_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	DHCP
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Manual
Primary DNS	
Secondary DNS	
DHCP	
DHCP Renew	Renew
DHCP Vendor(Option 60)	TPX820

parameter name	description
INTERNET access	Optional: DHCP, static IP, PPPoE
LAN connection modes	bridging
DNS Mode	Optional: Automatic or manual configuration

3.2.2 LTE

TPX820 supports using LTE as uplink, In LTE settings you will find:

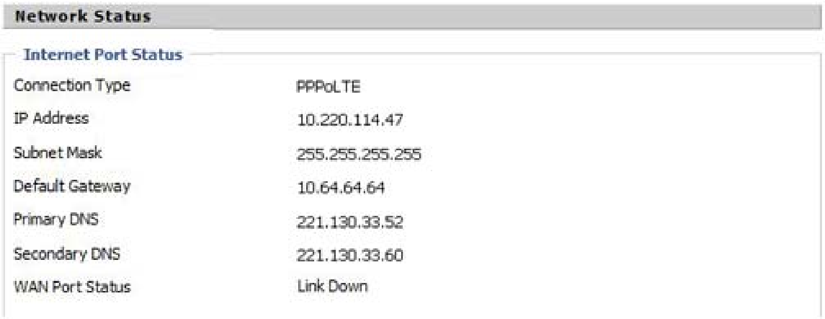


LTE Setting

Basic Setting

LTE Modem Enable	Enable
4G Connection Type	Auto
APN	CMNET
Dial Number	*99*1#
Username	
Password	

After applying and reboot, LTE connection state will show on status page.

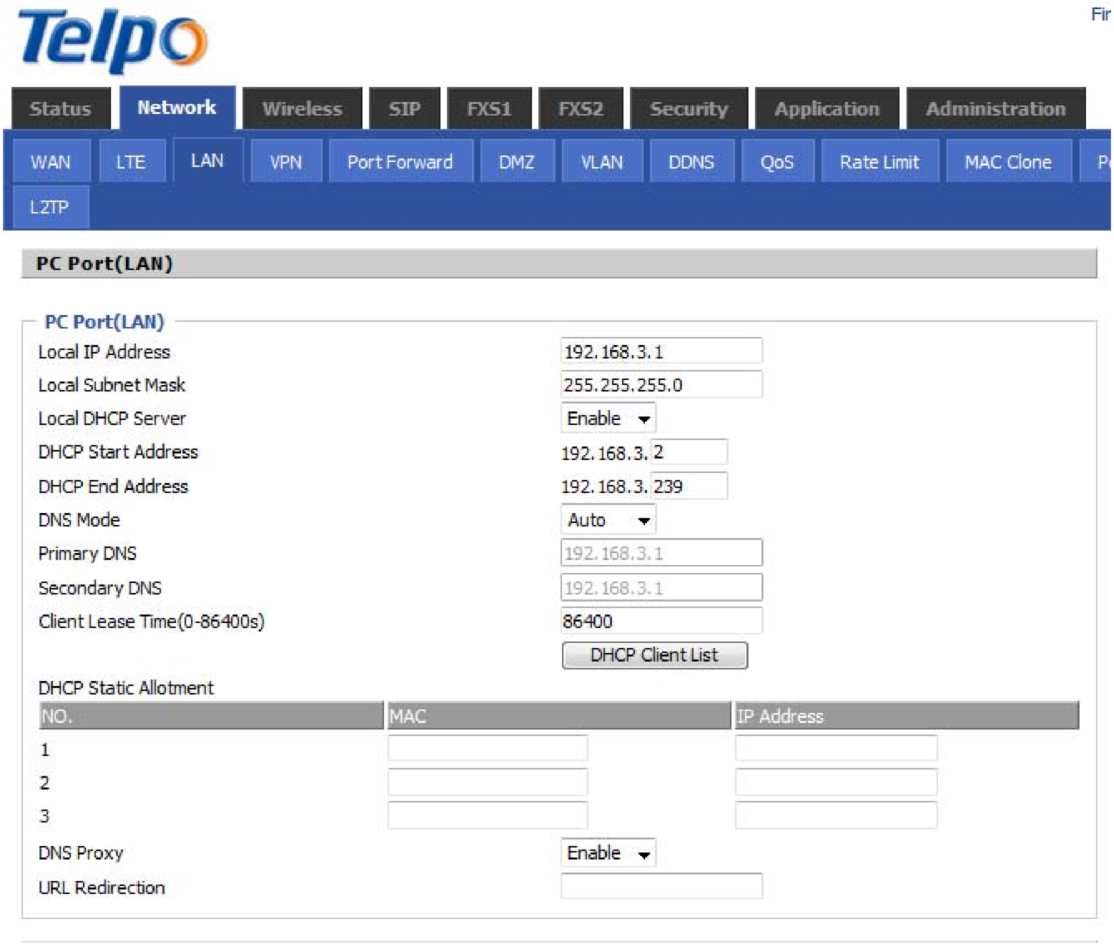


Network Status

Internet Port Status

Connection Type	PPPoLTE
IP Address	10.220.114.47
Subnet Mask	255.255.255.255
Default Gateway	10.64.64.64
Primary DNS	221.130.33.52
Secondary DNS	221.130.33.60
WAN Port Status	Link Down

2.2.3 LAN



PC Port(LAN)

PC Port(LAN)

Local IP Address	192.168.3.1
Local Subnet Mask	255.255.255.0
Local DHCP Server	Enable
DHCP Start Address	192.168.3. 2
DHCP End Address	192.168.3. 239
DNS Mode	Auto
Primary DNS	192.168.3.1
Secondary DNS	192.168.3.1
Client Lease Time(0-86400s)	86400

DHCP Static Allotment

NO.	MAC	IP Address
1		
2		
3		

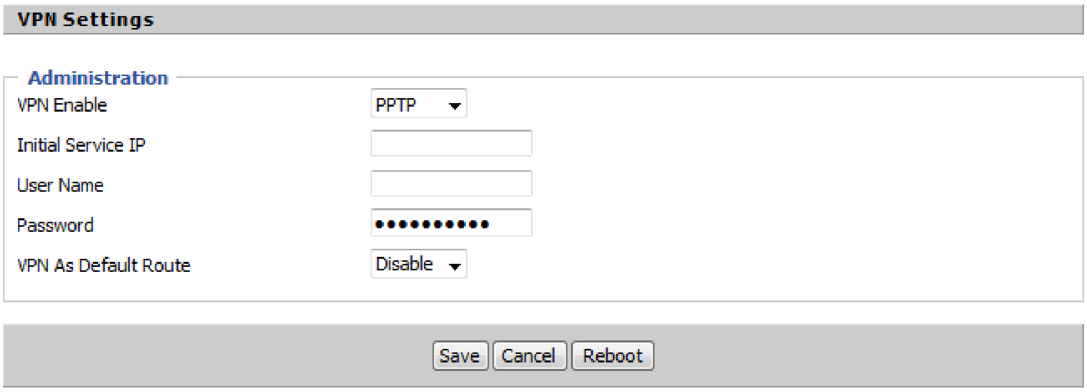
DNS Proxy	Enable
URL Redirection	

parameter name	description
IP addresses	Enter the IP address of the router LAN, LAN IP addresses of all computers must be with this IP address in the same segment, and the default gateway IP address must do this. (Default is192.168.168.1)

Subnet mask	Enter the subnet mask to determine the size of the network (the default is 255.255.255.0/24)
DHCP server	Whether to enable DHCP server
Address pool start address	Start IP address is an IP address pool to enter a valid IP address to DHCP servers as DHCP client, if therouter LAN IP address 192.168.168.1, 192.168.168.2 IPaddress can be the starting or more, but less than the end IP address
Address pool end address	The end of the ip address for the IP address pool enter a valid IP address as the DHCP server sends the DHCP client
DNS Mode	And automatically selecting from the specified DNS-type two modes. ♦ DNS type to Auto, the home gateway device from aLAN port DHCP server automatically Primary DNS and Secondary DNS ♦ DNS type is specified, the user should manually configure the preferred and secondary DNS
Primary DNS	Equipment preferred DNS
Secondary DNS	Equipment Secondary DNS
Customer lease time	Effective use of time the DHCP server IP addressassigned to the computer within the network. Within this period of time, the server does not assign an IPaddress to another computer.
DNS proxy	Select Open or disabled; If enabled, forwarding network LAN side to the WAN side of the network DNSrequest

3.2.4 VPN

VPN technology to establish a private network over a public network. The connection between any two nodes of the VPN network and private network is not required in the conventional end physical link, logical link transmission architecture but the service provider in the public network provided by the network platform, user data. VPN technologies, a user can establish a private connection between any two devices on the public network and transmitting data.



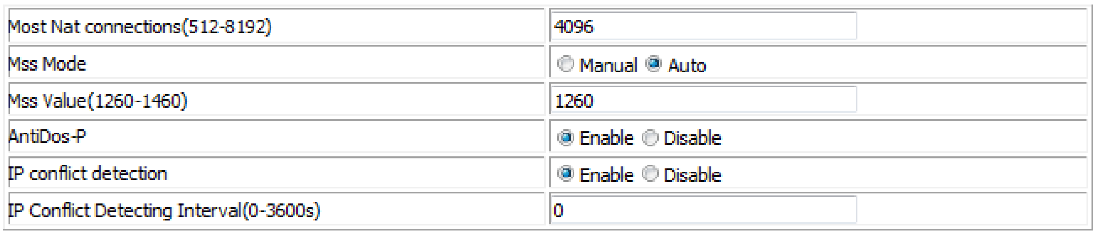
VPN Settings

Administration

VPN Enable	PPTP
Initial Service IP	
User Name	
Password	●●●●●●●●●●●
VPN As Default Route	Disable

parameter name	description
Enable VPN	If VPN is enabled. VPN mode the user can select fromtwo modes PPTP and L2TP.
IP server	Fill VPN server's IP address
username	Fill in the username required for authentication
password	Fill in the password required for authentication

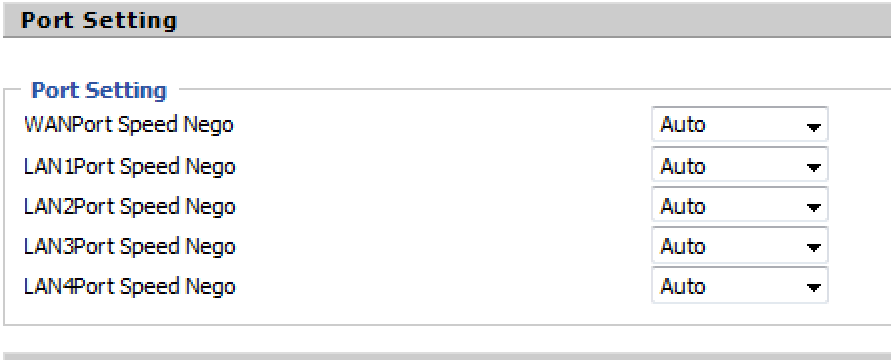
2.2.5 Advanced Settings



Most Nat connections(512-8192)	4096
Mss Mode	○ Manual ● Auto
Mss Value(1260-1460)	1260
AntiDos-P	● Enable ○ Disable
IP conflict detection	● Enable ○ Disable
IP Conflict Detecting Interval(0-3600s)	0

parameter name	description
Nat maximum number of connections	4096 default
Mss mode	There are two options **to specify** and **automatic**
Mss value	Set the value of the TCP
Anti Dos Attack	Can be selected to enable or disable
IP Address Conflict Detection	Select enabled or disabled; if enabled, will promptoccurs IP conflict TPX820
IP address conflict detection interval	IP address conflict detection time interval

3.2.6 Port Management



Port Setting

Port Setting

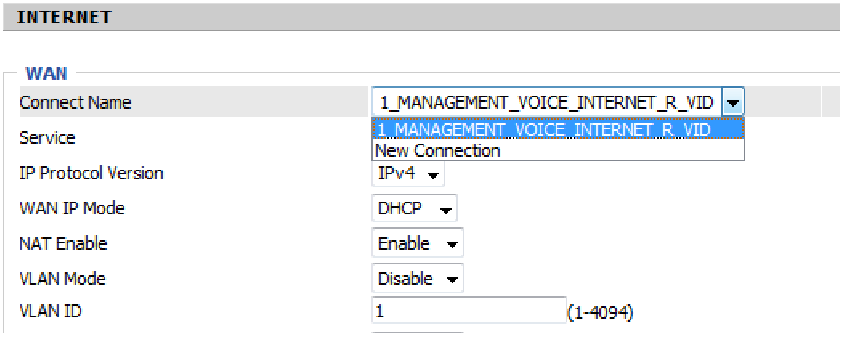
WANPort Speed Nego	Auto
LAN1Port Speed Nego	Auto
LAN2Port Speed Nego	Auto
LAN3Port Speed Nego	Auto
LAN4Port Speed Nego	Auto

parameter name	description
WAN speed negotiation settings	100M Full Duplex, 100M Half-duplex, full-duplex in10M and 10 M half-duplex speed negotiation method of

	selection from the port supports auto-negotiation
LAN1 ~ LAN4 speed negotiation settings	100M Full Duplex, 100M Half-duplex, full-duplex in10M and 10 M half-duplex speed negotiation method of selection from the port supports auto-negotiation

3.2.7 multi-WAN port settings

Page Setup in the management of working mode to Advanced mode
Multiple pages may be provided in a WAN WAN, a click connection mode wan new connection, the page as shown below:

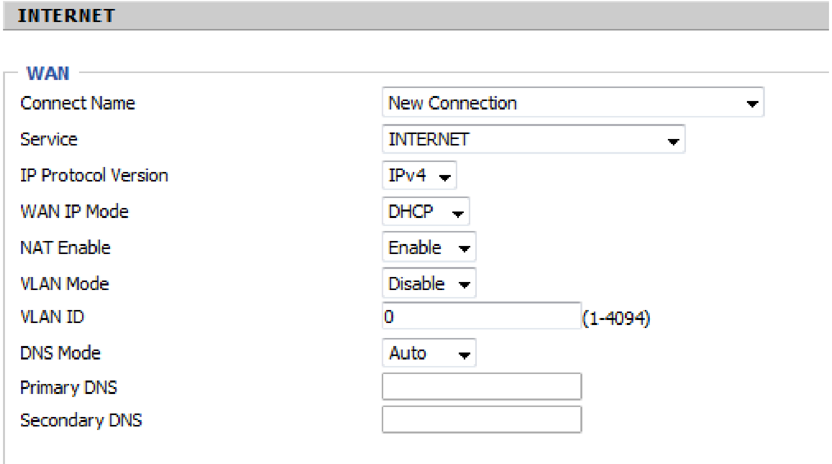


INTERNET

WAN

Connect Name: 1_MANAGEMENT_VOICE_INTERNET_R_VID (options: 1_MANAGEMENT_VOICE_INTERNET_R_VID, New Connection)
Service
IP Protocol Version: IPv4
WAN IP Mode: DHCP
NAT Enable: Enable
VLAN Mode: Disable
VLAN ID: 1 (1-4094)

Click on New wan connection can create another wan2, then select wan2 connected as follows:



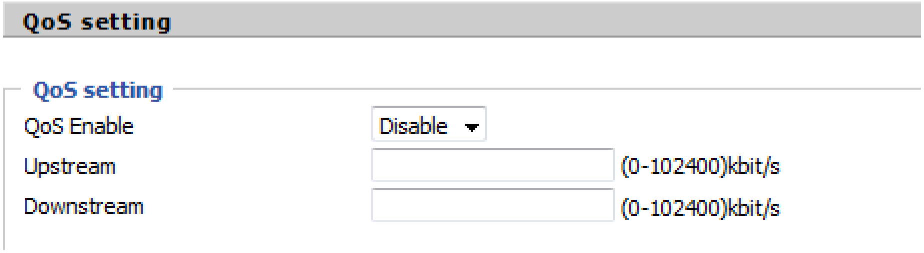
INTERNET

WAN

Connect Name: New Connection
Service: INTERNET
IP Protocol Version: IPv4
WAN IP Mode: DHCP
NAT Enable: Enable
VLAN Mode: Disable
VLAN ID: 0 (1-4094)
DNS Mode: Auto
Primary DNS:
Secondary DNS:

parameter name	description
VLAN mode	Whether to open the VLAN
VLAN ID	Fill in the corresponding id number

3.2.8 QoS



QoS setting

QoS setting

QoS Enable Disable

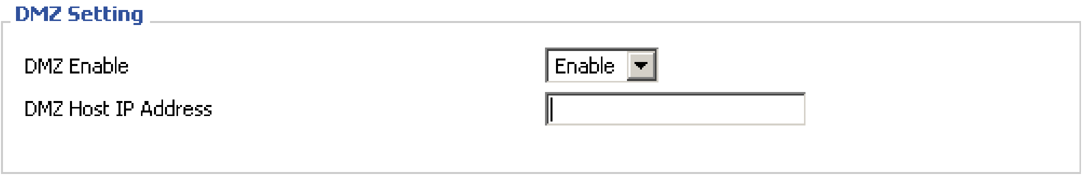
Upstream (0-102400)kbit/s

Downstream (0-102400)kbit/s

parameter name	description
Enable QoS	Whether QoS is enabled
Uplink bandwidth	Set traffic size

3.2.9 DMZ

After setting the LAN DMZ host, which will be completely exposed to the wide area network, you can achieve unlimited two-way communication. Bring insecurity to the DMZ add client may give the local network, so do not use this one.



DMZ Setting

DMZ Enable Enable

DMZ Host IP Address

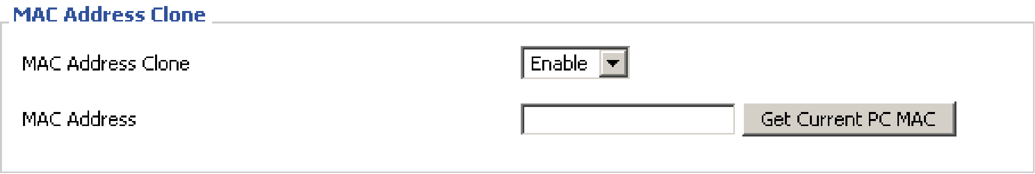
parameter name	description
DMZ settings	Open or prohibit the DMZ settings
DMZ Host IP address	Used to enter the DMZ host IP address needed

3.2.10 MACClone

MAC address is the hardware address of the network device. Sometimes a network provider may MAC names of network devices bound to the network account. So when the user uses the new home gateway may not be certified by the supplier. In this case, the user can clone your computer's physical address of the home gateway to the Internet port to use MAC cloning.

MAC address is an important parameter of network devices, so users should make sure the correct MAC device to prevent home gateway can not be used.

If you make a mistake MAC address, a user can log home gateway pages for viewing and cloned into TPX820 correct address or to restore the factory equipment.



MAC Address Clone

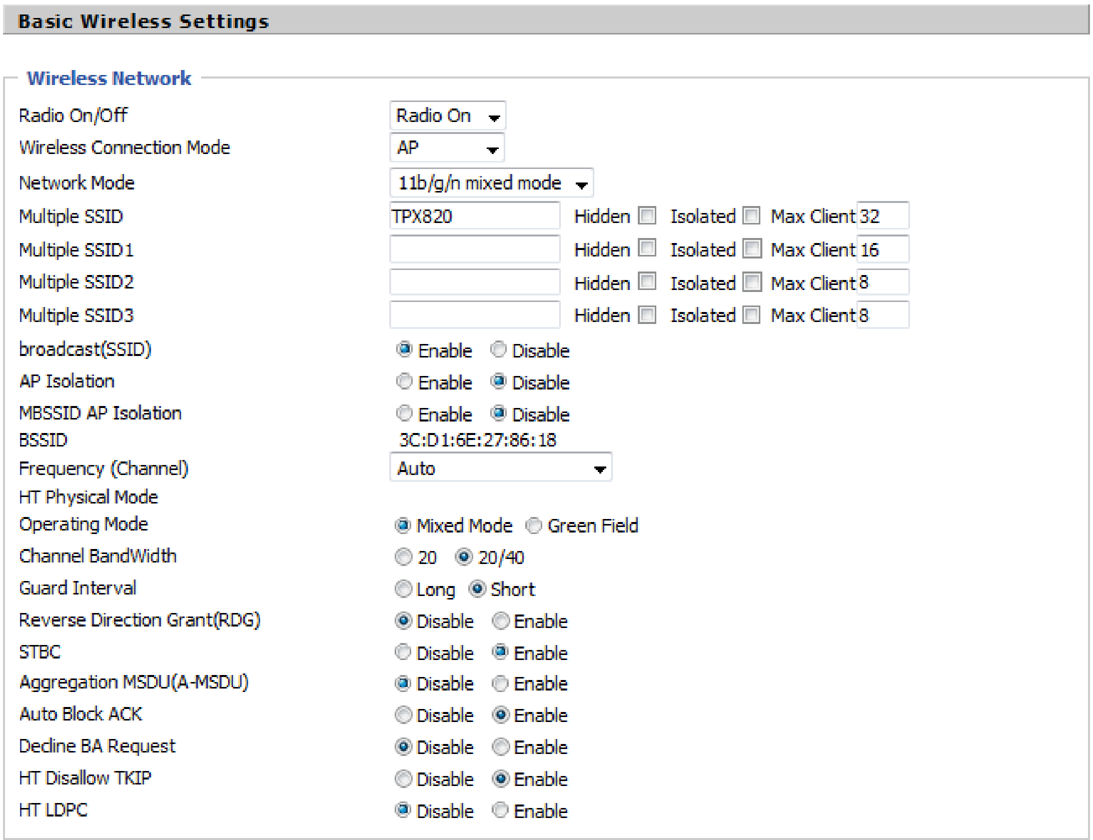
MAC Address Clone: Enable

MAC Address:

Enable MAC address cloning
1.Click Get Current PC MAC button to obtain the MAC address of the PC
2.Click Save button to save the changes; if you do not want to use MAC cloning; or click Cancel button to cancel the change.
3.Click Reboot button to reboot the device.

3.3 Wireless

3.3.1 Basic settings



Basic Wireless Settings

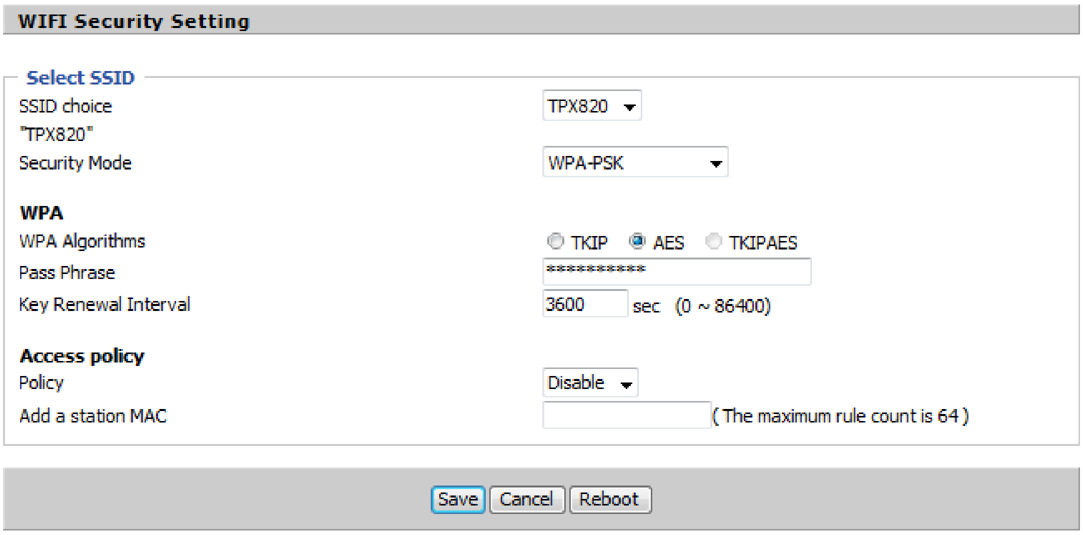
Wireless Network

Radio On/Off	Radio On ▾
Wireless Connection Mode	AP ▾
Network Mode	11b/g/n mixed mode ▾
Multiple SSID	TPX820 Hidden □ Isolated □ Max Client 32
Multiple SSID1	Hidden □ Isolated □ Max Client 16
Multiple SSID2	Hidden □ Isolated □ Max Client 8
Multiple SSID3	Hidden □ Isolated □ Max Client 8
broadcast(SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	3C:D1:6E:27:86:18
Frequency (Channel)	Auto ▾
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Short
Reverse Direction Grant(RDG)	● Disable ○ Enable
STBC	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
HT LDPC	● Disable ○ Enable

parameter name	description
WIFI switch	Select On or Off to enable or disable the wireless connection
Network mode	Select one of the modes based on the wireless client type. The default is 11b / g / n mixed mode
SSID	It is the basic identity of the wireless LAN. SSID can be any combination of alphanumeric or special characters. It will be displayed in the wireless network card search to the wireless network list
Multi SSID1 ~ SSID3	It can be achieved with more than one AP SSID
hide	After checking on the corresponding SSID is no longer displayed in the search to the wireless network card wireless network list
Broadcast Network	Initial open state, for the router into the wireless

Name (SSID)	network broadcast SSID
AP Isolation	AP isolation within this, Enabling customers within the end of this AP can not visit each other
MBSSID AP isolation	This outer barrier AP, AP other clients are not present at the client can not access this AP
BSSID	A set of wireless stations and a wireless LAN access point (AP) composed of a basic access unit (BSS),BSS, each computer must be configured with the same BSSID, an AP shall wireless identification
Frequency (channel)	Can be selected in AutoSelect / 1/2/3/4/5/6/7/8/9/10/11/12/13
Operating mode	1.Mixed Mode: In this mode, the previous wireless network card may be identified and connected to the Pre-N AP, but the throughput will be affected 2.Green Field: to achieve high throughput, but it will affect the safety of backward compatibility, and system
Channel bandwidth	Please select the default settings, divided 20MHz and20 / 40MHz two kinds
Protection interval	The default is automatic, in order to achieve excellent bit error rate performance, you must set the appropriate protection interval
MCS	Pointing control signal has a value in the range 0 to 32, the default is automatic
Reverse direction permission (RDG)	You can choose to enable or disable this permission

3.3.2 Wireless Security



WIFI Security Setting

Select SSID

SSID choice: TPX820

"TPX820"

Security Mode: WPA-PSK

WPA

WPA Algorithms: ○ TKIP ● AES ○ TKIPAES

Pass Phrase: ***********

Key Renewal Interval: 3600 sec (0 ~ 86400)

Access policy

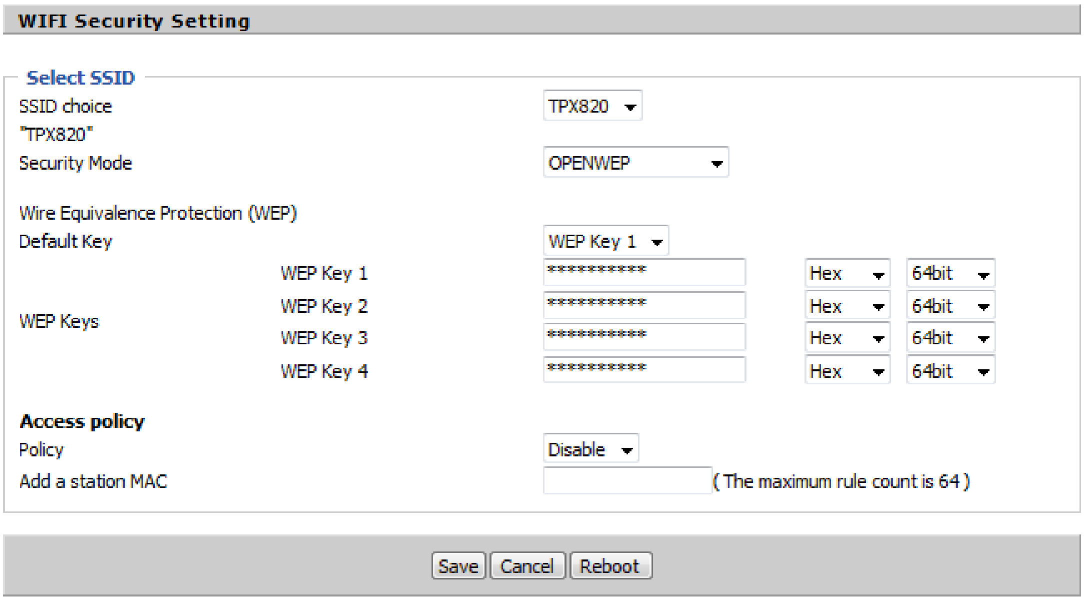
Policy: Disable

Add a station MAC: (The maximum rule count is 64)

SSID Choice	Choose the SSID you want to configure from the dropdown menu.
Security mode	Choose a suitable encryption mode to improve the security and privacy of wireless packets

Different encryption mode is selected will appear different web interface, you can make the appropriate configuration through these web interface. Here are some common ways to encrypt:

(1)OPENWEP：WEP encryption a handshake, is encrypted by a WEP key to:



WIFI Security Setting

Select SSID

SSID choice: TPX820

"TPX820"

Security Mode: OPENWEP

Wire Equivalence Protection (WEP)

Default Key: WEP Key 1

WEP Keys			
WEP Key 1	***********	Hex	64bit
WEP Key 2	***********	Hex	64bit
WEP Key 3	***********	Hex	64bit
WEP Key 4	***********	Hex	64bit

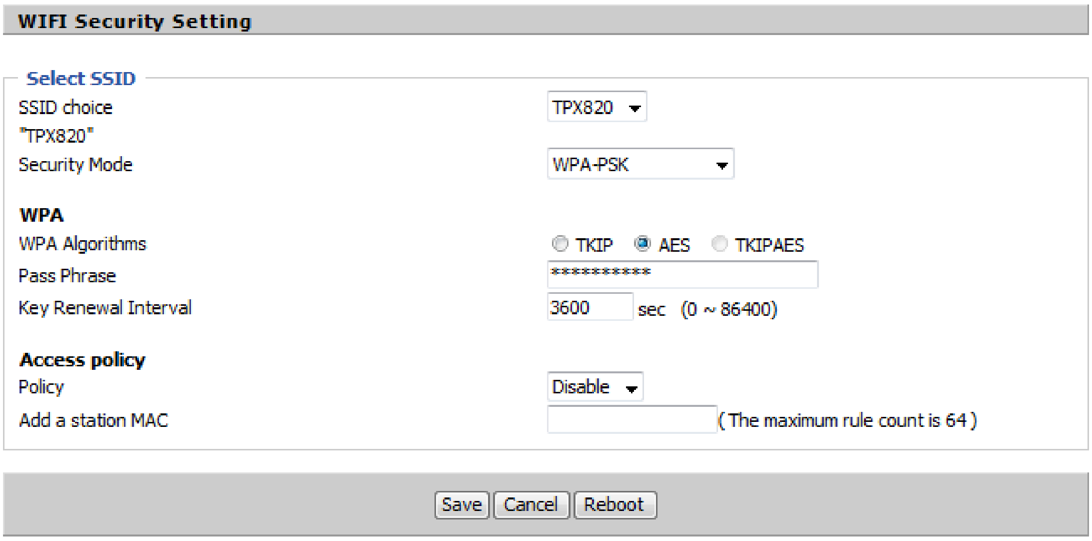
Access policy

Policy: Disable

Add a station MAC: (The maximum rule count is 64)

WEP represents a Wired Equivalent Privacy, which is a basic encryption.	
Default key	4 is used to select a WEP key in the key set on the client card is also required and this corresponds to
WEP key	The WEP key. Select the 64-bit key 10 must enter Hexcharacters, ASCII characters, or 5; 128-bit keyselection for an input character 26 Hex or ASCIIcharacters 13

(2)WPA-PSK, WPA mode router will use a shared key based on:


WIFI Security Setting

Select SSID

SSID choice	TPX820
"TPX820"	
Security Mode	WPA-PSK

WPA

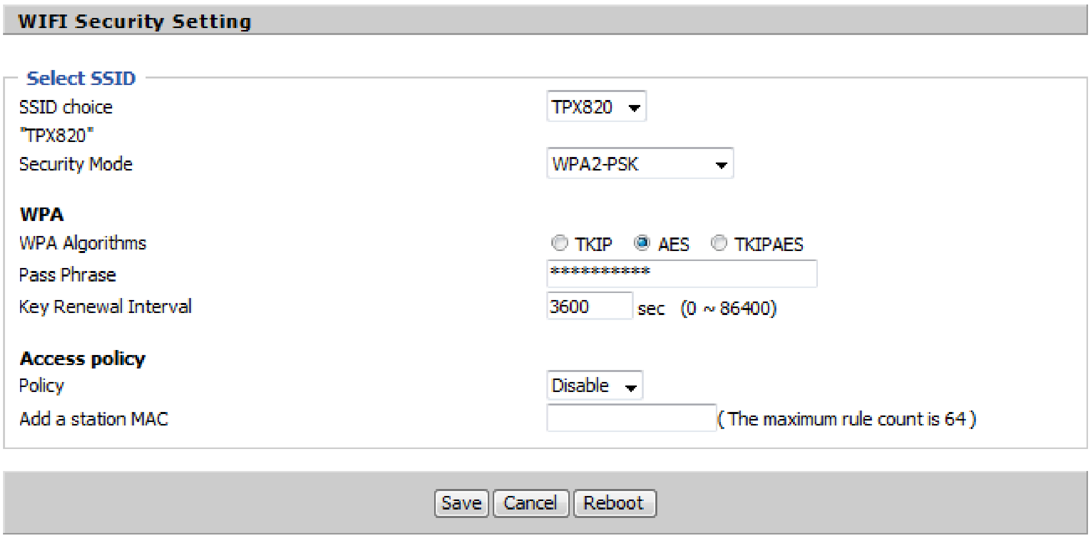
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	***********
Key Renewal Interval	3600 sec (0 ~ 86400)

Access policy

Policy	Disable
Add a station MAC	(The maximum rule count is 64)

WPA Algorithms	The choice for wireless data encryption security algorithm, options are TKIP, AES two kinds
Pass password	Setting WPA-PSK security password
Private key update spacing	A timing setting key update cycle, the default is 3600s

(3)WPA2-PSK, WPA2 mode router will use a shared key based on:



WIFI Security Setting

Select SSID

SSID choice: TPX820

"TPX820"

Security Mode: WPA2-PSK

WPA

WPA Algorithms: ○ TKIP ● AES ○ TKIPAES

Pass Phrase: ***********

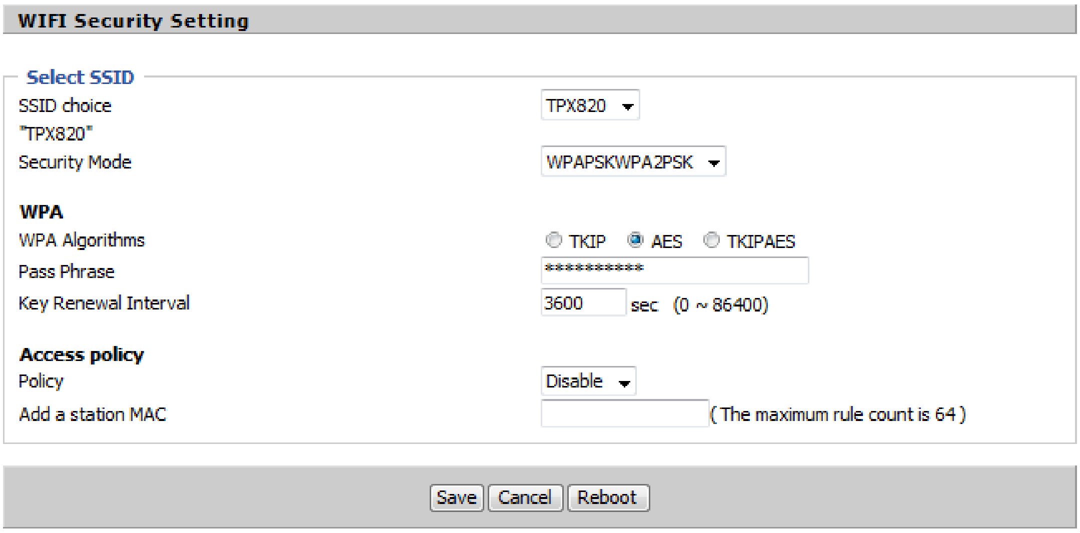
Key Renewal Interval: 3600 sec (0 ~ 86400)

Access policy

Policy: Disable

Add a station MAC: (The maximum rule count is 64)

4)WPAPSKWPA2PSK 与 WPA2PSK 的设置方式一致.



WIFI Security Setting

Select SSID

SSID choice: TPX820

"TPX820"

Security Mode: WPAPSKWPA2PSK

WPA

WPA Algorithms: ○ TKIP ● AES ○ TKIPAES

Pass Phrase: ***********

Key Renewal Interval: 3600 sec (0 ~ 86400)

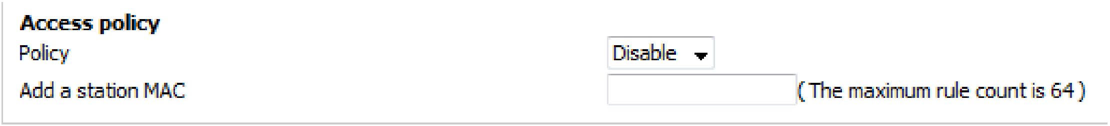
Access policy

Policy: Disable

Add a station MAC: (The maximum rule count is 64)

WPA-PSK / WPA2-PSK security type is actually a simplified version of WPA / WPA2, which is the shared key WPA mode, high security settings are also relatively simple for ordinary home users and small businesses based.	
WPA Algorithms	The choice for wireless data encryption security algorithm, options are TKIP, AES, TKIP / AES. 11N mode is not supported TKIP algorithm
Pass password	Setting WPA-PSK / WPA2-PSK security password
Private key update spacing	A timing setting key update cycle, the default is 3600s

Access Policy:



Access policy

Policy: Disable

Add a station MAC (The maximum rule count is 64)

parameter name	description
Access strategy	Wireless access control based on the MAC address of the specified conditions allow or disallow access to the wireless network client
Strategy	Disable: indicates that the wireless access control policy is not enabled; allows: indicates that only the clients in the list are allowed to access and deny: only the client access in the list is disabled
Added	Enter you want to allow or prohibit wireless client's MAC address
Examples: Disable the wireless network card MAC address 00: 1F: D0: 62: BA: FF computers to access the wireless network and other computers can access this network. Method: As shown, the selection policy is rejected, the new fill 00: 1F: D0: 62: BA : FF, after setting, click the Save and reboot the device to take effect.	

3.3.3 Wi-Fi Multimedia

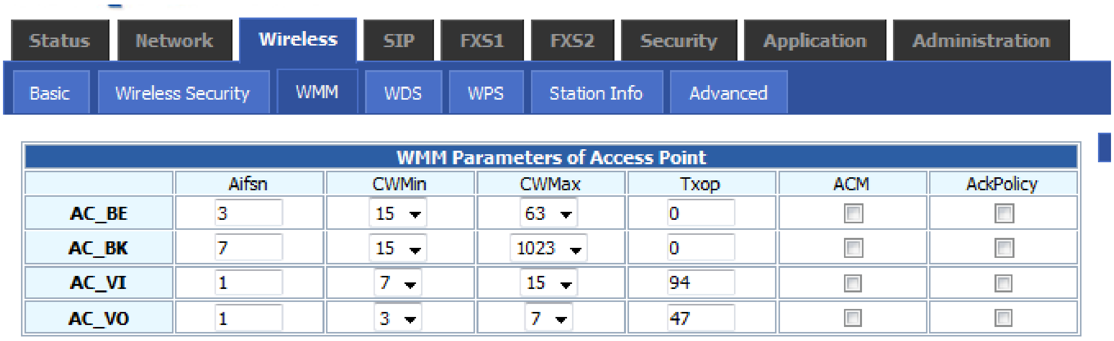
WMM (Wi-Fi Multi-Media) is the Wi-Fi Alliance

(WFA) of QoS certificate. Providing the set of wireless multimedia

parameters, WMM allows wireless communication range in

accordance with a priority of the data type definition. To

make WMM function work, wireless clients must also support WMM.

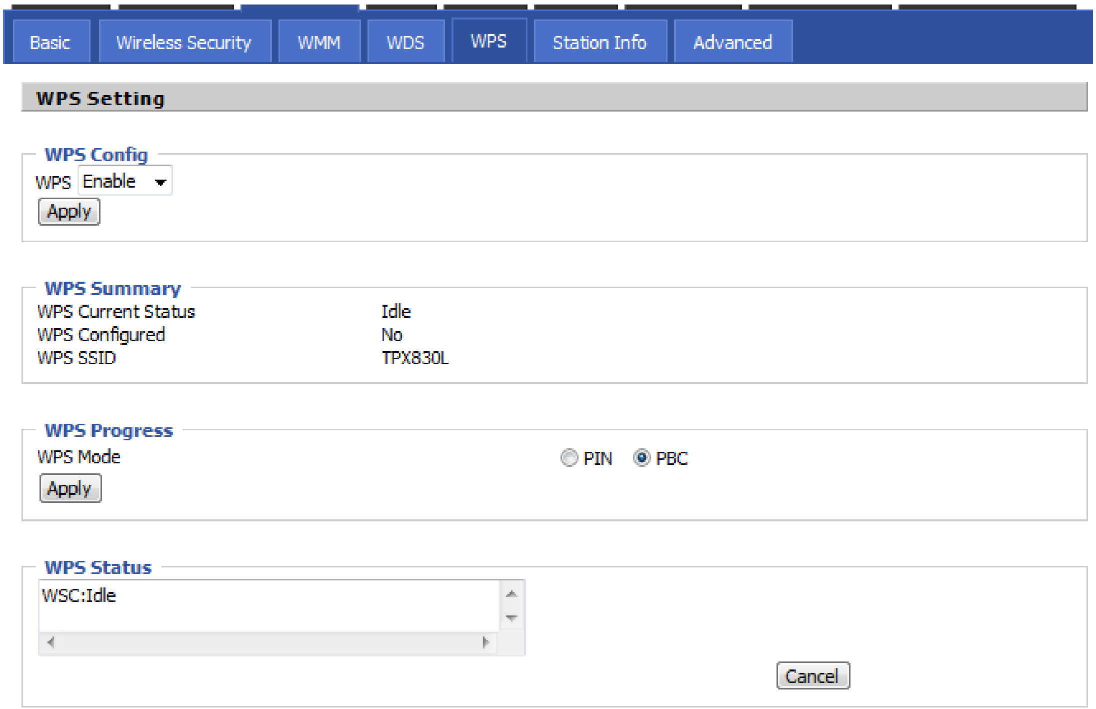


WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

3.3.4 Wi-Fi Protected Setup (WPS)

WPS is Wi-Fi Alliance has launched a new Wi-Fi security settings (Wi-Fi Protected Setup) standard, mainly due to the introduction of this standard is to address long-standing Wi-Fi encryption and authentication procedure too complicated Hard ills The By WPS button on the wireless router allows us to quickly and easily encrypt wireless network to transmit data to prevent unauthorized users invasion. On the one hand both to ensure the safety of the wireless network, on the other hand let us set the encryption easy.



WPS Setting

WPS Config

WPS: Enable

WPS Summary

WPS Current Status: Idle

WPS Configured: No

WPS SSID: TPX830L

WPS Progress

WPS Mode: ○ PIN ● PBC

WPS Status

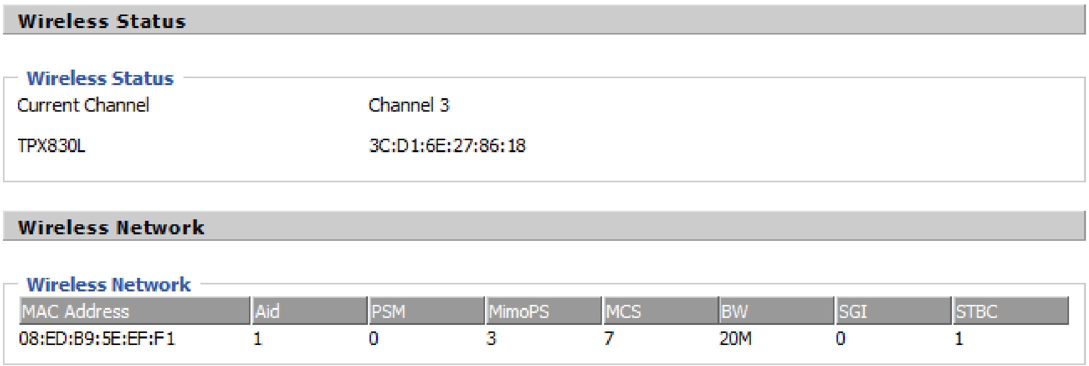
WSC:Idle

parameter name	description
WPS Settings	Open and close the WPS function
WPS Summary	WPS the current display, including the current status, the name of the SSID, authentication, encryption type, and the present AP PIN code
Generate	Generate a new PIN code
Reset OOB	The system uses the default security policy to allow other users access using a non-WPS
WPS mode	1. PIN: PIN options below, fill in the required access clients (wireless LAN) PIN code, and then click Apply. WPS transmission start signal, this time, the client also open on the PINaccess, the client can automatically connect wireless AP 1. PBC: PBC mode, there are two ways to start, you can press the PBC button on the

	hardware directly, or choose from the software to PBCmode, then click Apply. Both approaches can beconnected to activate the WPS PBC mode, at this time only need to select the PBC access client, the client can automatically connect to the wireless AP
WPS status	The current WPS status in three ways: WSC: Idle state WSC: Start WSC Process state information as the start WSC: Success state to have a client access to AP,WPS connection is successful

3.3.5 Wireless Client

The wireless client can display information that has been connected to the apparatus according to the present AP:



Wireless Status

Wireless Status

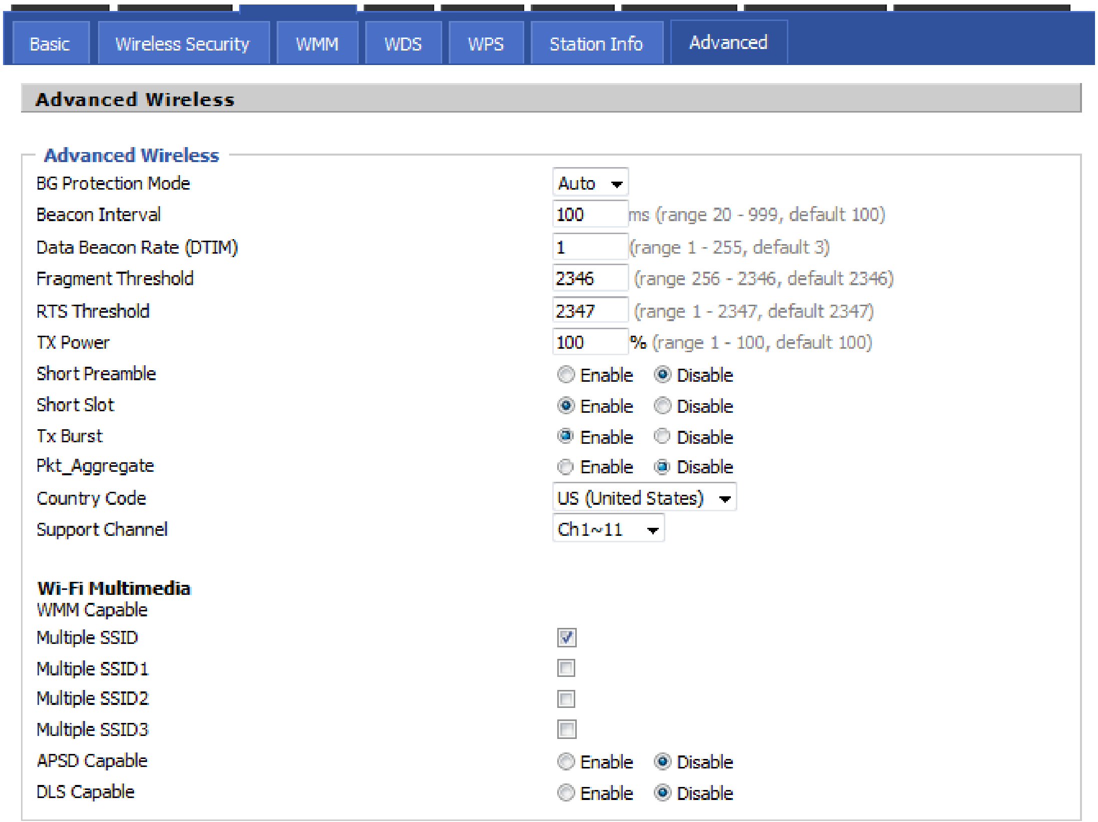
Current Channel	Channel 3
TPX830L	3C:D1:6E:27:86:18

Wireless Network

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
08:ED:B9:5E:EF:F1	1	0	3	7	20M	0	1

3.3.6 Advanced Settings



Advanced Wireless

Advanced Wireless

BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 (range 1 - 255, default 3)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 % (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	○ Enable ● Disable
Country Code	US (United States)
Support Channel	Ch1~11

Wi-Fi Multimedia

WMM Capable	
Multiple SSID	☑
Multiple SSID1	□
Multiple SSID2	□
Multiple SSID3	□
APSD Capable	○ Enable ● Disable
DLS Capable	○ Enable ● Disable

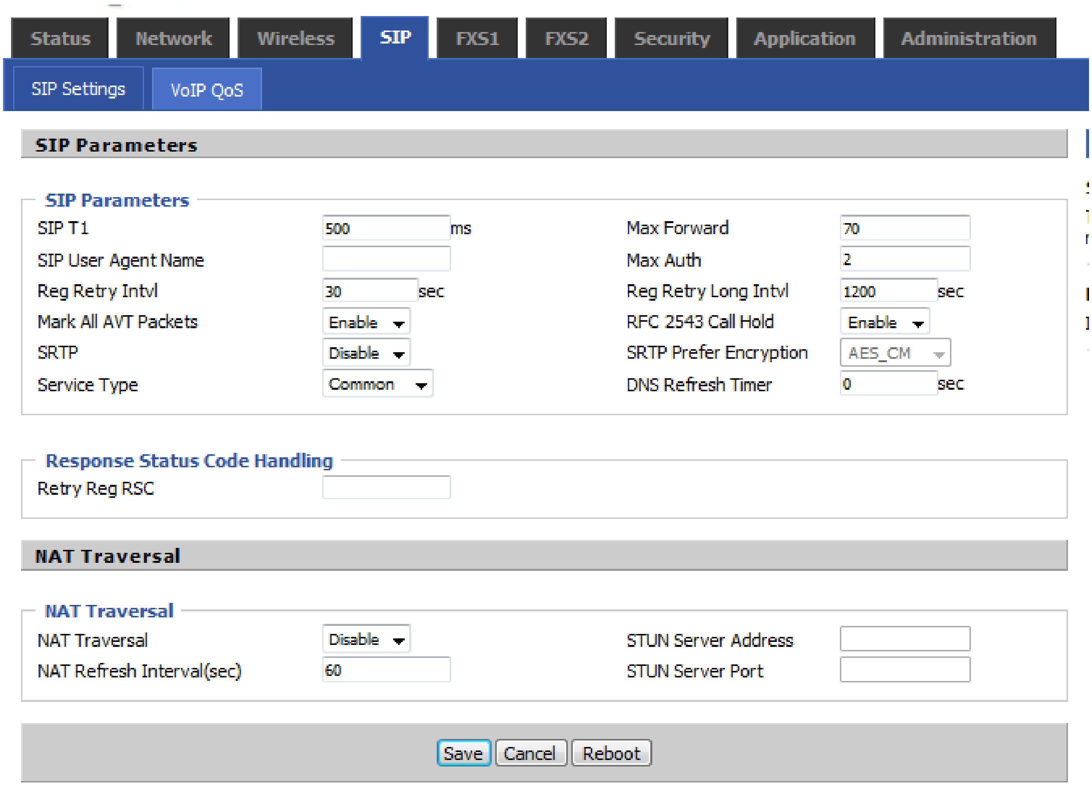
parameter name	description
BG Protection Mode	Select On, Off or automatically, to determine the state of the protected mode BG
Beacon interval	Send the beacon frame time interval, within this time range, will send a beacon frame to obtain the surrounding wireless network access information
Data beacon ratio	Specifies the interval for the transmission of the indication message, which is a countdown job that tells the next client window to receive broadcast and multicast
Split boundaries	Specify the slice threshold for the packet. When the length of the packet exceeds the slice threshold, it is automatically divided into multiple packets
Transfer request limit	RTS threshold value to specify a data packet,when the packet exceeds this value, the router will

	send RTS to the destination site consultations
Transmit power	Define the current SSID for wireless AP transmit stronger power level, the greater the signal
Short preamble	Enabled by default, the system is not compatible with the conventional IEEE 802.1 1, the rate of operation of the system 1, 2Mpbs
Short collision groove	By default, the opening can increase the transmission rate of wireless communication
Transmission burst	MAC address belongs layer characteristics, can improve the TCP transport network fairness
Packet aggregation	Enhanced local area network to ensure that the packet correctly reaches the destination mechanism
Support IEEE802.11 H	By default, it can be turned on
country code	There CN, US, JP, FR, TW, IE, HK, NONE optional
Wi-Fi Multimedia (WMM)	
Wi-Fi Multimedia capability	WMM function is turned on, take effect until open
Automatic power saving mode	Open will reduce the wireless performance, but can play the role of energy saving
WMM Parameters	Click WMM Configuration directly out of Wi-Fi multimedia parameters configuration page
Multicast to unicast conversion	By default, you can choose to turn on

4.SIP related settings

4.1 SIPSettings

In this page, users can set the information related to SIP, NAT and other relevant information.



SIP Parameters

SIP Parameters

SIP T1	500 ms	Max Forward	70
SIP User Agent Name		Max Auth	2
Reg Retry Intvl	30 sec	Reg Retry Long Intvl	1200 sec
Mark All AVT Packets	Enable	RFC 2543 Call Hold	Enable
SRTP	Disable	SRTP Prefer Encryption	AES_CM
Service Type	Common	DNS Refresh Timer	0 sec

Response Status Code Handling

Retry Reg RSC

NAT Traversal

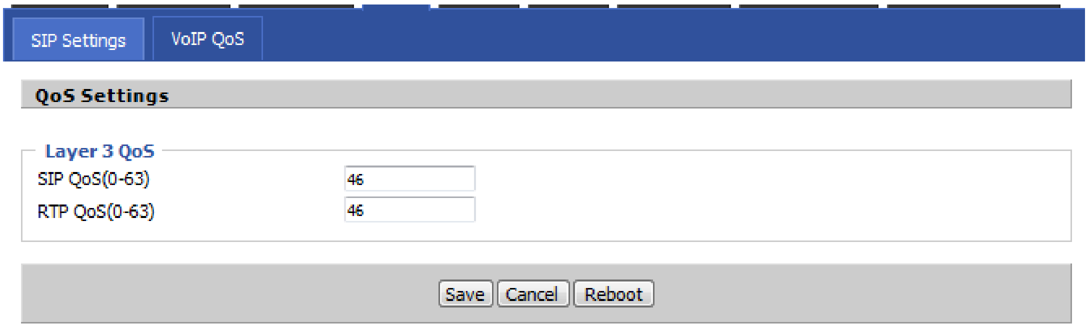
NAT Traversal

NAT Traversal	Disable	STUN Server Address	
NAT Refresh Interval(sec)	60	STUN Server Port	

parameter name	description
NAT Traversal	1. Whether to enable NAT Traversal 2. The device supports STUN Traversal; if you want totraverse NAT / Firewall, choose STUN
STUN server address	Add the correct IP address of the STUN service providers
NAT refresh interval	NAT refresh interval setting, the default configuration is 60s
STUN port services	Setting NAT port number, default 5060

4.2 VoIP QoS

QoScan improve the quality of service for voice applications.



QoS Settings

Layer 3 QoS

SIP QoS(0-63) 46

RTP QoS(0-63) 46

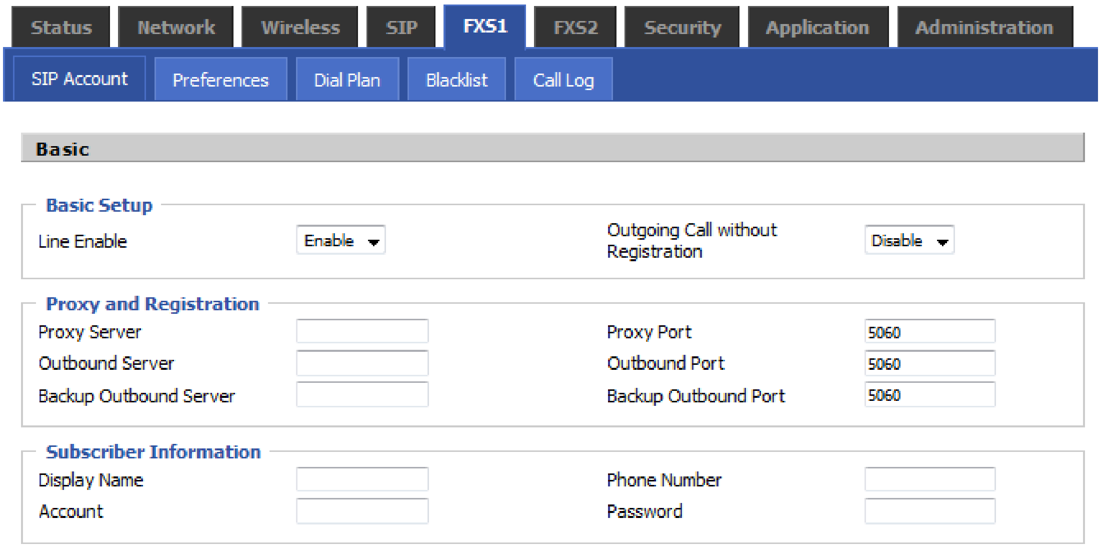
默认值为 0，可以设置值的范围是 0~63.

参数名称	描述
SIP /RTP/Data QoS	默认值为 0，可以设置值的范围是 0~63.

4.3 FXS(FXS1&FXS2)

4.3.1 Basic settings

Set the user's basic information VOIP service provider, such as phone numbers, account numbers, passwords and SIP agents.



Basic

Basic Setup

Line Enable: Enable

Outgoing Call without Registration: Disable

Proxy and Registration

Proxy Server

Outbound Server

Backup Outbound Server

Proxy Port: 5060

Outbound Port: 5060

Backup Outbound Port: 5060

Subscriber Information

Display Name

Account

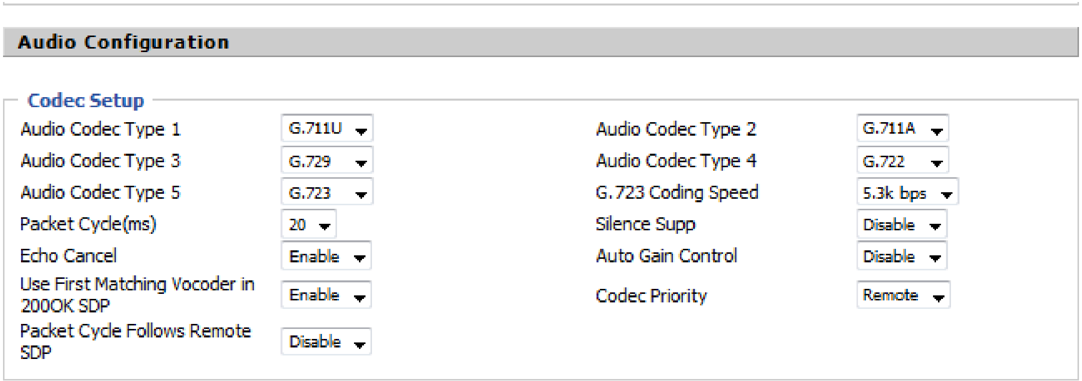
Phone Number

Password

parameter name	description

Account enabled	Line 1 is enabled
End to end	Whether to enable Peer To Peer If enabled, the account will not issue aregistration request to the SIP server; displaying the registration is successful, the line 1 can dial out the status page will, but the number can not be dialed external line 1
Register the server	Fill in the SIP server's domain name or IP address
Proxy server	Fill in the proxy server's domain name or IPaddress
Back up the proxy server	Fill in the domain name or IP address of the backup proxy server
Register the server port	Fill SIP server port number, default is 5060
Proxy server port	Fill in the proxy server port number, default is 5060
Back up the proxy server port	Fill backup proxy server port number, default is 5060
show name	The name of the number
register account	SIP server provides the phone number
Name of certification	SIP server provides the account
password	SIP server provides the SIP password

4.3.2 Audio settings



Audio Configuration

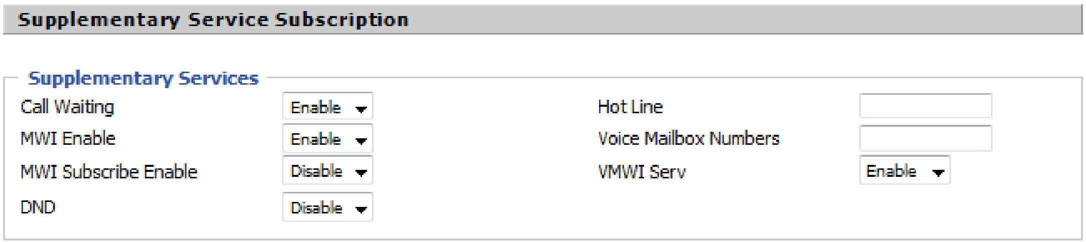
Codec Setup

Audio Codec Type 1	G.711U	Audio Codec Type 2	G.711A
Audio Codec Type 3	G.729	Audio Codec Type 4	G.722
Audio Codec Type 5	G.723	G.723 Coding Speed	5.3k bps
Packet Cycle(ms)	20	Silence Supp	Disable
Echo Cancel	Enable	Auto Gain Control	Disable
Use First Matching Vocoder in 200OK SDP	Enable	Codec Priority	Remote
Packet Cycle Follows Remote SDP	Disable		

parameter name	description
Encoding 1	Select the appropriate coding mode from G.711A,G.711U, G.722, G.729 and G. 723 coding scheme five kinds
2 encoding	Select the appropriate coding mode from G.711A,G.711U, G.722, G.729 and G. 723 coding scheme five kinds
3 encoding	Select the appropriate coding mode from G.711A,G.711U, G.722, G.729 and G. 723 coding scheme five kinds
4 encoding	Select the appropriate coding mode from G.711A,G.711U, G.722, G.729 and G. 723 coding scheme five kinds
Encoding 5	Select the appropriate coding mode from G.711A,G.711U, G.722, G.729 and G. 723 coding scheme five kinds
G.723 coding rate	Selecting a coding rate G.723, there are two kinds of 5.3kbps and 6.3kbps
Packing cycle	Set the RTP wrapping cycle, the default configuration is 20ms
Mute suppression	Whether it is muted
Echo cancellation	Whether to enable echo cancellation, the default is enabled

T.38 enabled	Whether to open T.38
T.38 redundancy	
T.38CNG detection is enabled	

4.3.3 Supplementary Services



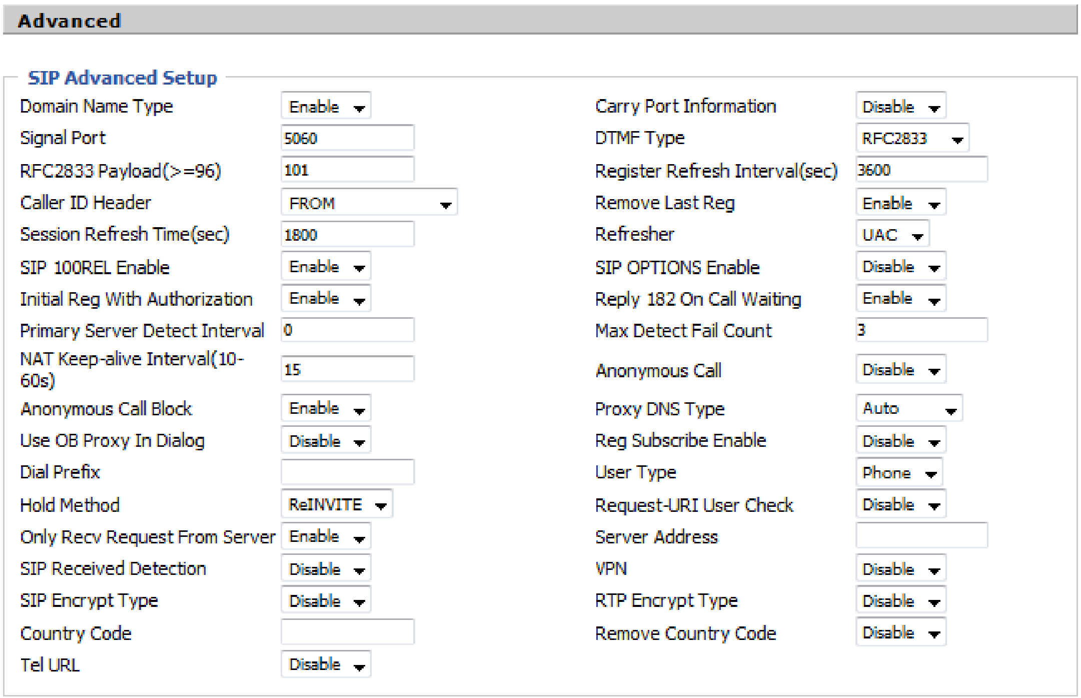
Supplementary Service Subscription

Supplementary Services

Call Waiting	Enable	Hot Line	
MWI Enable	Enable	Voice Mailbox Numbers	
MWI Subscribe Enable	Disable	VMWI Serv	Enable
DND	Disable		

parameter name	description
Call waiting	Whether to enable call waiting
Hotline call number	Fill in the hotline number. After the user set up, hook, once home gateway will automatically dial out the hotline number
MWI Enable	Whether MWI (message waiting indication) is enabled, if the user needs to use voice mail, enable this feature
Voice Mailbox Numbers	Fill SIP service provider voice mail signature toElatix platform as an example, their voice mail signature is 97 *
DND	Whether to open the bother, open any phone can not call; the default is prohibited

4.3.4 Advanced



Advanced

SIP Advanced Setup

Domain Name Type	Enable	Carry Port Information	Disable
Signal Port	5060	DTMF Type	RFC2833
RFC2833 Payload(>=96)	101	Register Refresh Interval(sec)	3600
Caller ID Header	FROM	Remove Last Reg	Enable
Session Refresh Time(sec)	1800	Refresher	UAC
SIP 100REL Enable	Enable	SIP OPTIONS Enable	Disable
Initial Reg With Authorization	Enable	Reply 182 On Call Waiting	Enable
Primary Server Detect Interval	0	Max Detect Fail Count	3
NAT Keep-alive Interval(10-60s)	15	Anonymous Call	Disable
Anonymous Call Block	Enable	Proxy DNS Type	Auto
Use OB Proxy In Dialog	Disable	Reg Subscribe Enable	Disable
Dial Prefix		User Type	Phone
Hold Method	ReINVITE	Request-URI User Check	Disable
Only Recv Request From Server	Enable	Server Address	
SIP Received Detection	Disable	VPN	Disable
SIP Encrypt Type	Disable	RTP Encrypt Type	Disable
Country Code		Remove Country Code	Disable
Tel URL	Disable		

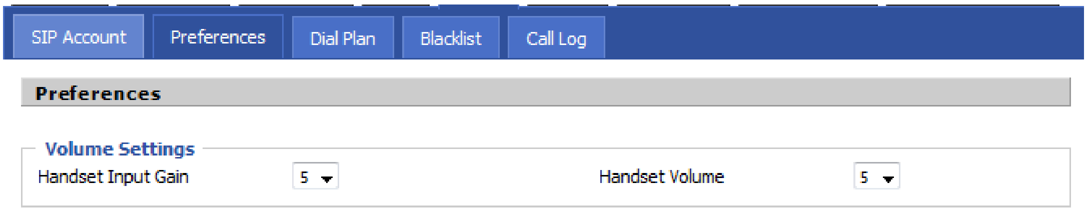
parameter name	description
Domain name format	Whether to enable domain name recognition in the SIP URI
Carry port information	Whether carrying port information of the SIP URI
Signal Port	Local port number of the SIP protocol, the default is 5060
DTMF mode setting	Secondary selection dial mode, selectable items are In-band, RFC2833 and SIP Info.
RFC2833 Payload (> = 96)	The user can use the default settings
Register refresh time	The time interval between two normal registration messages. The user can use the default settings.
RTP port	Transmitting the RTP port is provided; if set to "0", IPphone will select an idle port to send RTP
Cancel Message Enable	When enabled, an unregistered message will be sent before the registration is disabled and no unregistered messages will be sent before registration; should be set according to the different server requirements
Session Refresh Time	The interval between two sessions, the user can use the

(sec)	default settings
Refresher	From the UAC and UAS select Refresh
Prack Enable	Whether Prack enabled
SIP OPTIONS Enable	If this option is enabled, IP phones SIP- OPTION will be sentto the server, rather than periodically send Hellopackets. Transmission time interval Keep-alive Interval
Heartbeat cycle	Detecting time intervals the master server, the default value is 0, represents an enabled
Maximum detection failure count	Detecting the number of times the primary server fails; the default value is no longer detected after 3, i.e., threeprimary server fails
Keep-alive interval (10 -60s)	The time interval for sending empty packets
Anonymous Call	Whether anonymous calls are enabled
Anonymous Call Block	Whether to enable anonymous call blocking
Proxy DNS Type	Set DNS server type, optional items have type A and DNS SRV
Use OB Proxy In Dialog	Whether to use a proxy in a conversation OB
VPN	Whether VPN enabled
Sign up for subscription	When enabled, the subscription message is sent after the registration message; the subscription message is not sent when it is disabled
Dial prefix	Add a prefix before dialing out the number
Peer user type	User mode may be selected or IP Phone
Call hold method	There are two ways to Hold INFO ReINVITE and methods
Request the user to check	URI request check the user
Accept only requests from the server	Whether to enable only requests from the server
server address	SIP server address
SIP Received detection	Whether to detect the response of the registration server to determine the public address of the sending device

5.Preferences

In this page, the user can set the home gateway preferences.

5.1 Volume Settings



Preferences

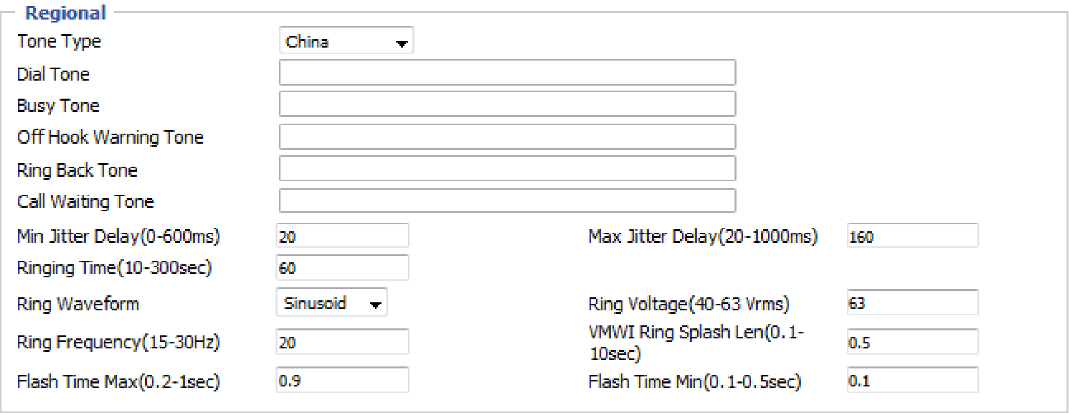
Volume Settings

Handset Input Gain 5

Handset Volume 5

parameter name	description
Enter the volume	MIC volume adjustment handle input sizes, adjustable from 0 to 7
Output volume	Earpiece volume adjustment lever, adjustable from 0 to 7

5.2 Regional



Regional

Tone Type China

Dial Tone

Busy Tone

Off Hook Warning Tone

Ring Back Tone

Call Waiting Tone

Min Jitter Delay(0-600ms) 20

Max Jitter Delay(20-1000ms) 160

Ringing Time(10-300sec) 60

Ring Waveform Sinusoid

Ring Voltage(40-63 Vrms) 63

Ring Frequency(15-30Hz) 20

VMWI Ring Splash Len(0.1-10sec) 0.5

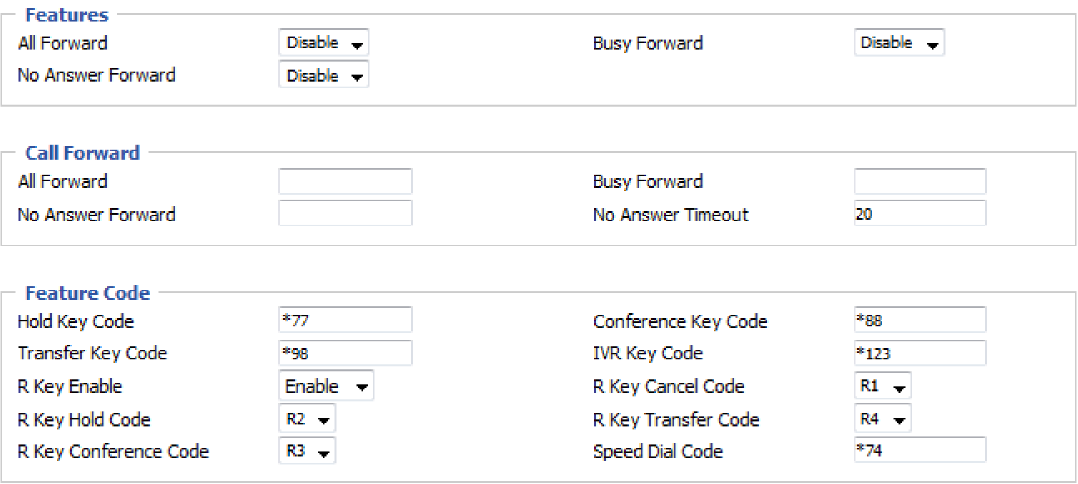
Flash Time Max(0.2-1sec) 0.9

Flash Time Min(0.1-0.5sec) 0.1

parameter name	description
Ringtones standard	Select the type of tones, such as China, USA, India, etc.
Dial tone	Dial tone
busy tone	Busy tone
Tribute tone	Hang up warning tone

Ring back tone	Ringtones tone
Call waiting tone	Call waiting tone
Minimum jitter delay	Minimum Jitter Delay and Jitter delay adaptive mechanism adopted home gateway
Maximum jitter delay	Maximum Jitter Delay and Jitter delay adaptive mechanism adopted home gateway
Ring time	The ringing time of the home gateway
Ringing waveform	Bell choose SINUSOID waveform (sine) and Trapezoid(trapezoidal), the default selection SINUSOID
Ringing voltage	Ringing voltage setting, the default value of 70
Ringing frequency	Ring frequency setting, the default value of 25
Flash Time Max	Flash max time, the default value of 0.9
Flash Time Min	Flash min time, the default value of 0.1

5.3 Call Transfer



Features

All Forward	Disable	Busy Forward	Disable
No Answer Forward	Disable		

Call Forward

All Forward		Busy Forward	
No Answer Forward		No Answer Timeout	20

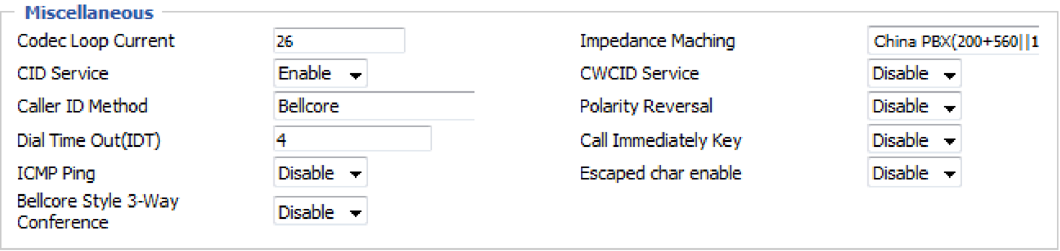
Feature Code

Hold Key Code	*77	Conference Key Code	*88
Transfer Key Code	*98	IVR Key Code	*123
R Key Enable	Enable	R Key Cancel Code	R1
R Key Hold Code	R2	R Key Transfer Code	R4
R Key Conference Code	R3	Speed Dial Code	*74

Page / parameter name		description
Features	All Forward	Whether to enable forwarding all calls
	Busy Forward	Whether to enable busy forwarding calls
	No Answer Forward	Whether to enable unanswered call forwarding
Call forwarding	All Forward	Set the destination number for all calls
	Busy Forward	Set the target number for the busy forwarding call
	No Answer Forward	Set the target number for the unanswered call

	No Answer Timeout	Set the ringing time to be determined as unanswered
Function key setting	Keep the key code	Call Hold feature code, default * 07
	Conference key code	Signature three-way conversation, the default * 09
	Transfer key code	Call forwarding feature code, default * 08
	Voice menu key	Signature voice menu, the default ****
	R key enable	R to select to enable or disable
	R cancel key combination code	R cancel key combination code is provided, in the range of R + 1 ~ R + 9
	R key combination code hold key	R key combination code of the key holder disposed, in the range of R + 1 ~ R + 9
	Transfer key R keycombination code	Transfer R key combination provided key codes, in the range of R + 1 ~ R + 9
	R key combination code session key	R session key provided key combination code, in the range of R + 1 ~ R + 9

5.4 Miscellaneous



Miscellaneous

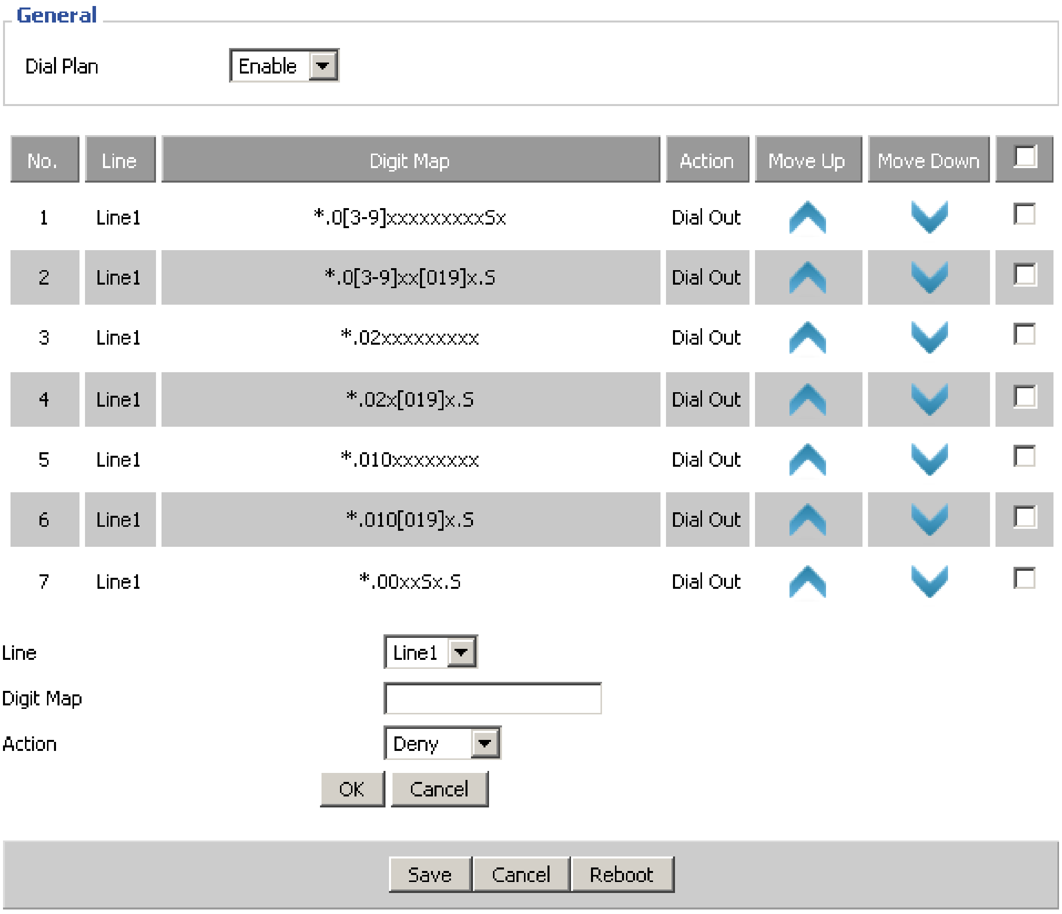
Codec Loop Current	26	Impedance Maching	China PBX(200+560||1
CID Service	Enable	CWCID Service	Disable
Caller ID Method	Bellcore	Polarity Reversal	Disable
Dial Time Out(IDT)	4	Call Immediately Key	Disable
ICMP Ping	Disable	Escaped char enable	Disable
Bellcore Style 3-Way Conference	Disable		

parameter name	description
Codec loop current	Hook loop current default value 26
Impedance matching	Matching set, the default China CO (200 + 680 || 100nF)
Caller ID	Whether to open the caller ID; if turned on, display the phone number of the call, otherwise it is not displayed. Is turned on by default
CWCID Service	Whether to open CWCID service. If the call is on, the phone number waiting for the call is displayed, otherwise it is not displayed;
Dial timeout	After the home gateway dials the number of times to hear the dial tone
Fast dial key	Select the dial key "*" or "#" or disabled

ICMP Ping	Whether to enable ICMP Ping. If enabled, the home gateway at a certain length of time will ping SIP server; if disabled, the home gateway sends "hello" empty packet to the server
Special character escaping	Whether to open the special character translation function; if enabled, when you press the # key will be translated into23%, compared to ban #

5.4.1Digit Map

5.4.1 General Settings



General

Dial Plan: Enable

No.	Line	Digit Map	Action	Move Up	Move Down	□
1	Line1	*.0[3-9]xxxxxxxxxSx	Dial Out	⌃	⌄	□
2	Line1	*.0[3-9]xx[019]x.S	Dial Out	⌃	⌄	□
3	Line1	*.02xxxxxxxxx	Dial Out	⌃	⌄	□
4	Line1	*.02x[019]x.S	Dial Out	⌃	⌄	□
5	Line1	*.010xxxxxxxx	Dial Out	⌃	⌄	□
6	Line1	*.010[019]x.S	Dial Out	⌃	⌄	□
7	Line1	*.00xxSx.S	Dial Out	⌃	⌄	□

Line: Line1

Digit Map:

Action: Deny

parameter name	description
Dial plan	Whether to enable dial plan
line	Set the line

Figure number (expression)	Fill in the expression of the graph, the grammar of the number of words
Features	Select the number of match action figure, Deny represents the home gateway will refuse to match the number dialed, Dial Out represents the home gateway allows outgoing matching numbers
Move up	Move up
Move down	Move down

5.4.2 Add a Dial plan

① enable dial plan;

② click to increase, then the page will jump to the above chart;

③ fill in the relevant parameters;

④ click OK to set the end;

⑤ Click Save to confirm the changes and restart the home gateway to make the changes take effect.

5.4.3 Digitmap rules

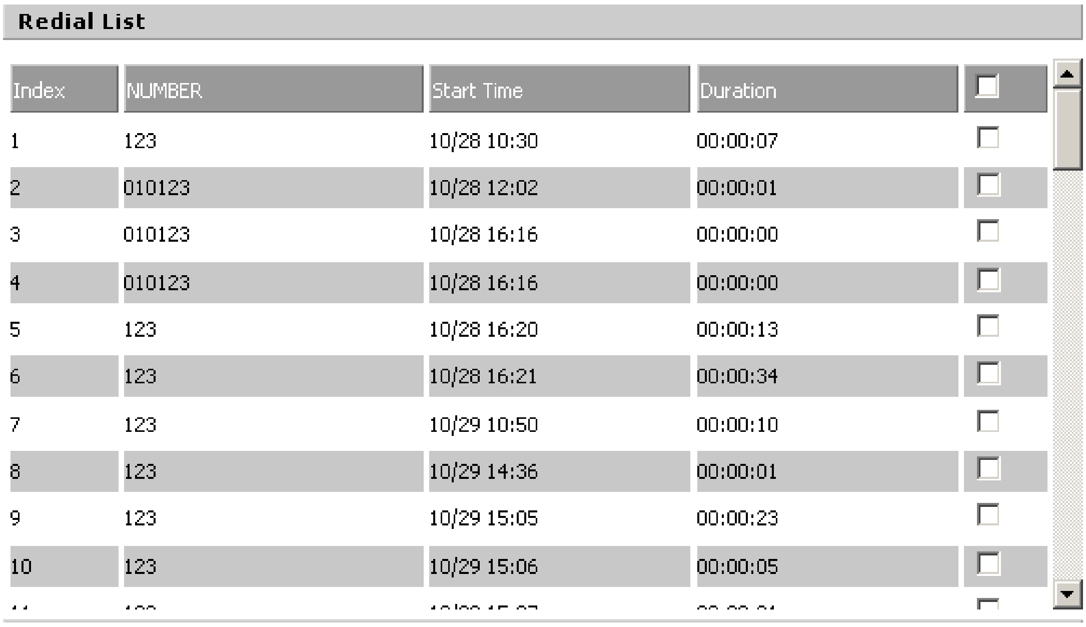
No.	character	description
1	0 1 2 3 4 5 6 7 8 9 * #	Legal characters
2	X	Lowercase letter x matches any character a legitimate
3	[Sequence]	Match a sequence. E.g.: ♦ [0-9]: matches any of the numbers 0 to 9 ♦ [23-5 *]: matching characters or 2 or 3 or 4 or 5 *
4	X	Match x, xx, xxx, xxxx, etc. E.g.: "01." matches "0", "01", "011" ……"011111 ……"
5	<Dialed:	replace

	substituted>	For example: <#: 23%> xx <#: 23%>, # 56 # is input,the output is 23% 5623%
6	X, y	After entering the "x" will be the end of the dial tone, enter "y" after the dial tone. E.g. <5:><: 241 333> 8101 58 101 for the input,output 2413338101. In addition IP601 input 5 will have a dial tone, dial 8 after stopping
7	T	Set the delay time. IP601 will allocate valid number after 2 seconds

5.4.4Call Logs

In this page user can view the replay menu (outgoing calls), received calls and missed calls.

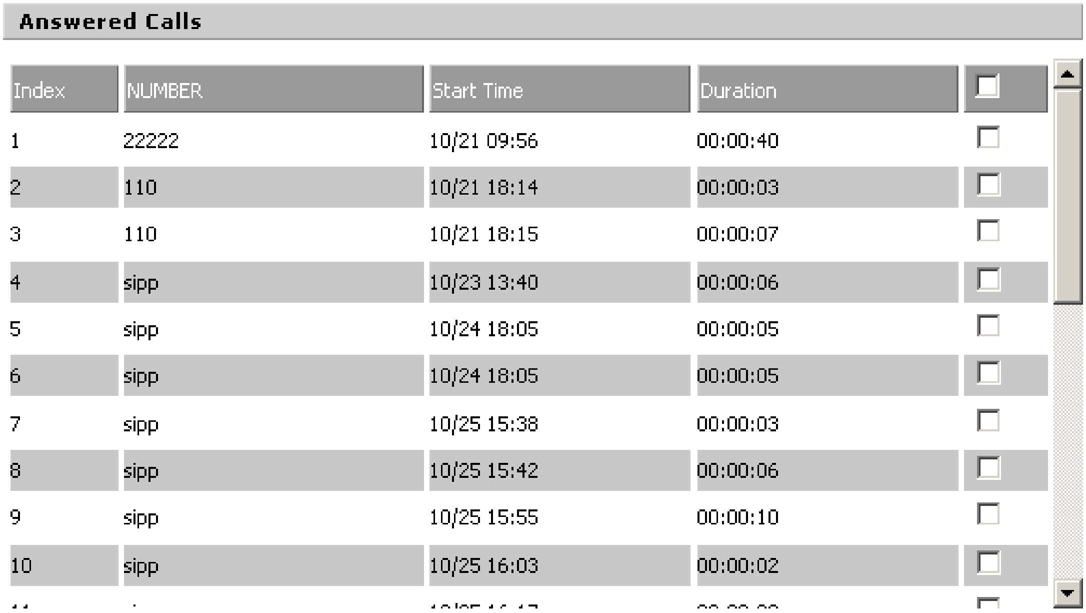
(1) Redial list



Redial List

Index	NUMBER	Start Time	Duration	□
1	123	10/28 10:30	00:00:07	□
2	010123	10/28 12:02	00:00:01	□
3	010123	10/28 16:16	00:00:00	□
4	010123	10/28 16:16	00:00:00	□
5	123	10/28 16:20	00:00:13	□
6	123	10/28 16:21	00:00:34	□
7	123	10/29 10:50	00:00:10	□
8	123	10/29 14:36	00:00:01	□
9	123	10/29 15:05	00:00:23	□
10	123	10/29 15:06	00:00:05	□
11	123	10/29 15:07	[illegible]	□

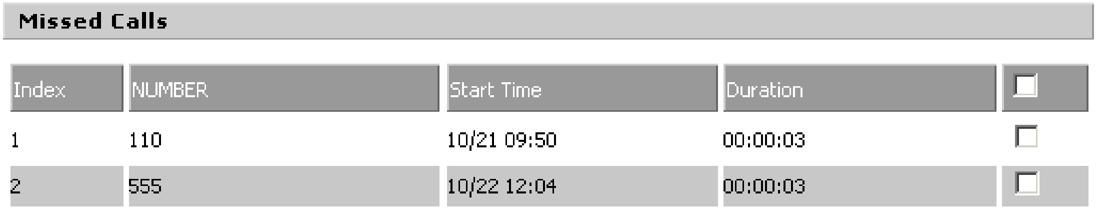
(2)Answered Calls



Answered Calls

Index	NUMBER	Start Time	Duration	□
1	22222	10/21 09:56	00:00:40	□
2	110	10/21 18:14	00:00:03	□
3	110	10/21 18:15	00:00:07	□
4	sipp	10/23 13:40	00:00:06	□
5	sipp	10/24 18:05	00:00:05	□
6	sipp	10/24 18:05	00:00:05	□
7	sipp	10/25 15:38	00:00:03	□
8	sipp	10/25 15:42	00:00:06	□
9	sipp	10/25 15:55	00:00:10	□
10	sipp	10/25 16:03	00:00:02	□
11	sipp	10/25 16:17	[illegible]	□

(3)Missed Calls



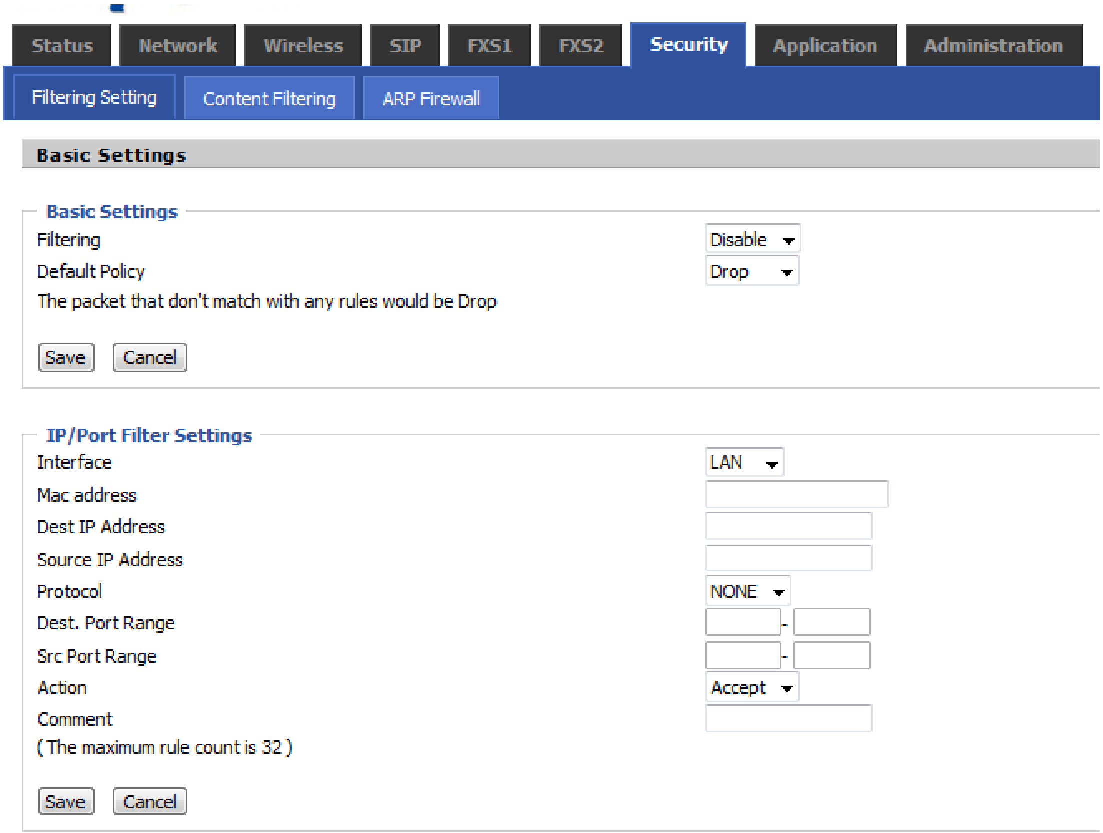
Missed Calls

Index	NUMBER	Start Time	Duration	☐
1	110	10/21 09:50	00:00:03	☐
2	555	10/22 12:04	00:00:03	☐

6.Security

In this page you can filter settings, content filtering.

6.1 IP/MAC/PORT Filtering



Basic Settings

Basic Settings

Filtering	Disable
Default Policy	Drop

The packet that don't match with any rules would be Drop

IP/Port Filter Settings

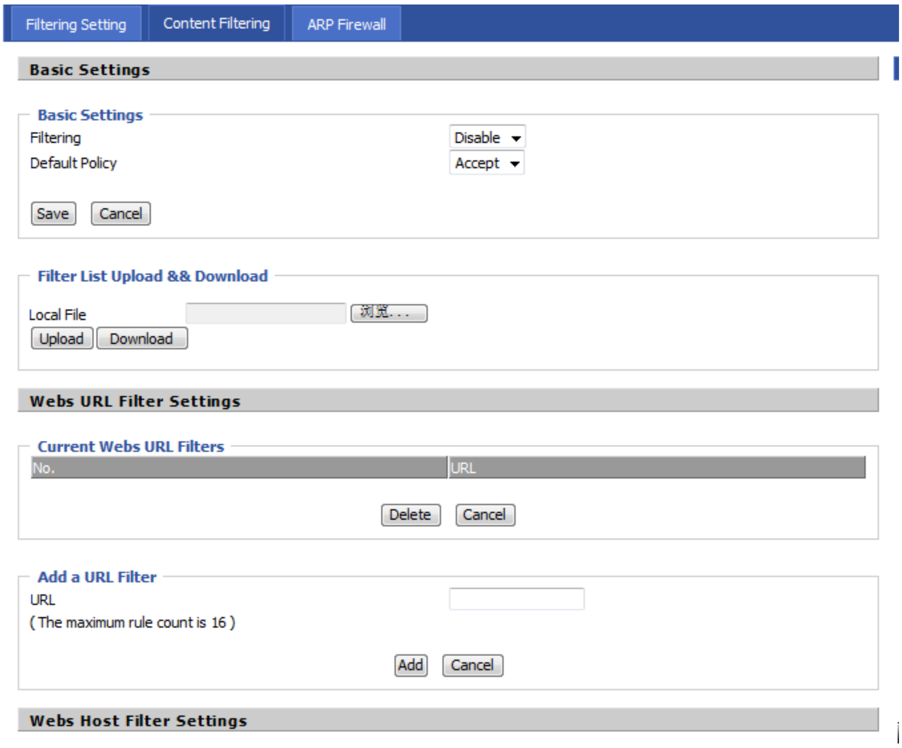
Interface	LAN
Mac address	
Dest IP Address	
Source IP Address	
Protocol	NONE
Dest. Port Range	-
Src Port Range	-
Action	Accept
Comment	

(The maximum rule count is 32)

parameter name	description
Enable filtering	Whether to turn on filtering
Default policy	May choose to give up or accept

Mac Address	Add Mac address filtering required
Destination IP address	Destination IP address
Source IP address	Source IP address
protocol	Select the name of the protocol, support TCP, UDP and TCP & UDP
The purpose Port Interval	Destination port range
Source Port section	Source port range
behavior	You can choose to receive or give up
Annotations	The annotation of the added content
delete	Delete the selected item
cancel	Cancel the settings

6.2 Content Filtering



Basic Settings

Basic Settings

Filtering: Disable

Default Policy: Accept

Filter List Upload && Download

Local File

Webs URL Filter Settings

Current Webs URL Filters

No.	URL

Add a URL Filter

URL

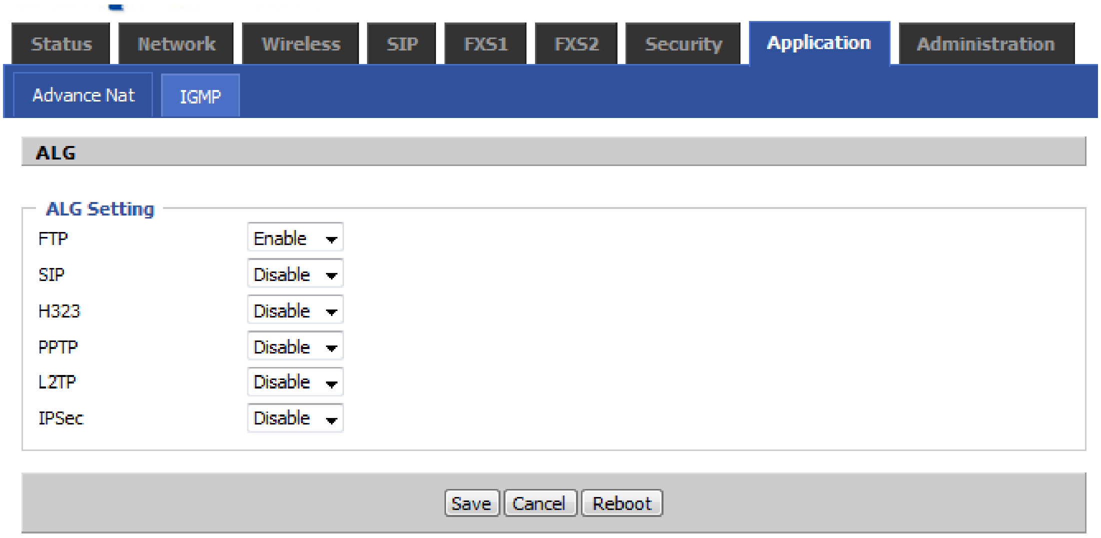
(The maximum rule count is 16)

Webs Host Filter Settings

basic settings	description
Enable filtering	Whether to enable content filtering
Default policy	The default policy is to accept or disable filtering rules
Webs URL filtering	description
URL filter list the current system	URL filtering rules that already exist (black list)
Delete / Cancel	You can choose to delete or cancel an existing filtering rule
Add a URL Filter	Add URL filtering rules
Add / Cancel	Click Add or Cancel
Webs Host Filter Settings	description
Current Website Host Filters	Already existing keywords (blacklist)
Delete / Cancel	You can choose to delete or cancel an existing keyword
Add a Host Filter (Keyword)	Add keywords
Delete / Cancel	Click Add or Cancel

7.Application

You can set advanced Nat, UPnP, IGMP, DMS, MLD in this page.



ALG

ALG Setting

FTP	Enable
SIP	Disable
H323	Disable
PPTP	Disable
L2TP	Disable
IPSec	Disable

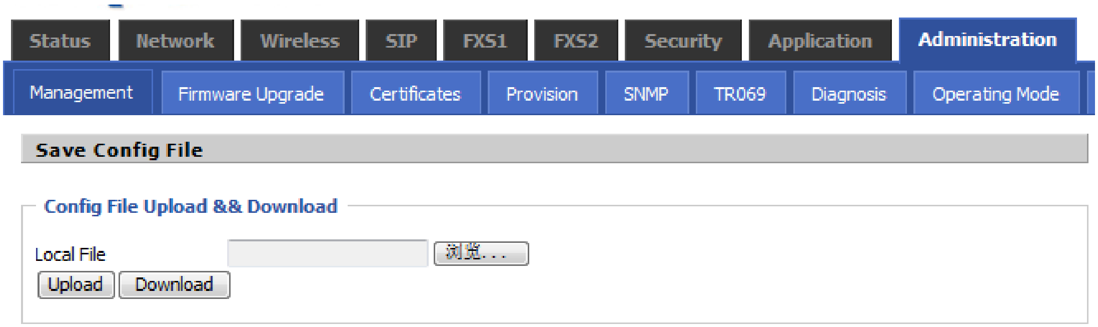
8.Administration

In this page you can manage your home gateway, home gateway users to set the time / date, password, web login, the system logs, and TR069 related configuration.

8.1 Management

In his page, users can manage the home gateway time / date, password, restore factory and so on.

8.1.1Config File Upload & Download



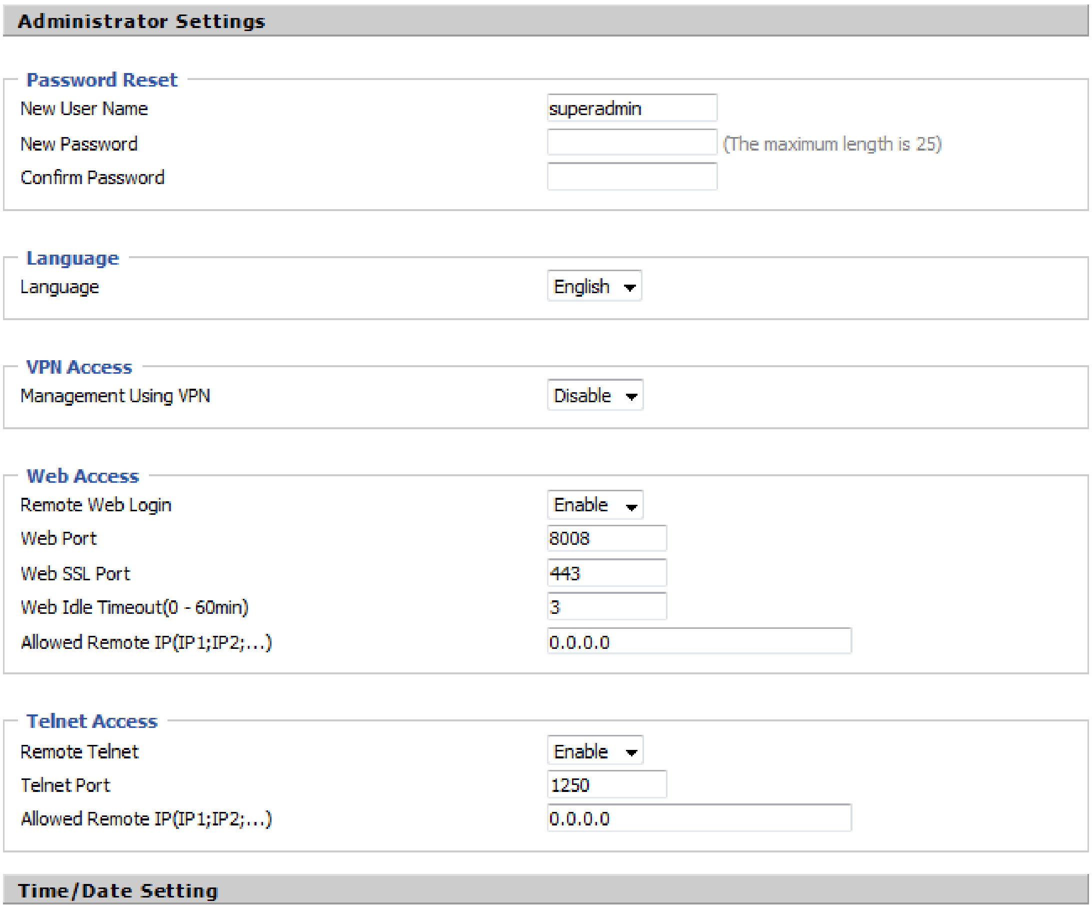
Save Config File

Config File Upload && Download

Local File

parameter name	description
Configuration file upload and download	Upload: Click Browse, select the file locally, press the Upload button to start uploading the file
	Download: Click Download, then select the path to start downloading the configuration file
Dialing rules file upload	Click Browse, select the file locally, press the Upload button to start uploading the file

8.1.2 Administrator Settings



Administrator Settings

Password Reset

New User Name: superadmin

New Password: (The maximum length is 25)

Confirm Password:

Language

Language: English

VPN Access

Management Using VPN: Disable

Web Access

Remote Web Login: Enable

Web Port: 8008

Web SSL Port: 443

Web Idle Timeout(0 - 60min): 3

Allowed Remote IP(IP1;IP2;...): 0.0.0.0

Telnet Access

Remote Telnet: Enable

Telnet Port: 1250

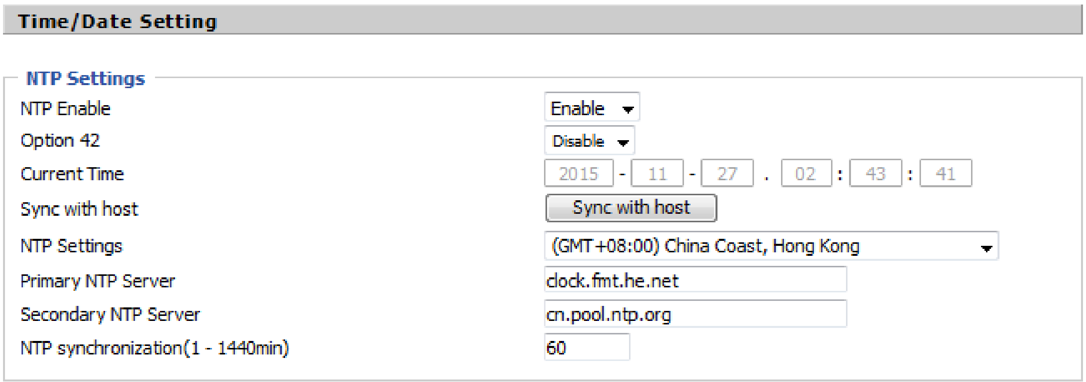
Allowed Remote IP(IP1;IP2;...): 0.0.0.0

Time/Date Setting

parameter name	description
user type	There are two levels of administrator, ordinary users
new user name	You can modify the user name, set a new user name
new password	Add a new user name for the password
confirm password	Add a new password again
Language	There are Chinese, English, Russian, Finnish, Spanish, can be

	selected, Web pages corresponding changes will occur
Remote Web Log	Whether to enable remote Web Log
Web port	Port settings used for logging on via the Internet port and PCport, the default value of 80
Web Idle Timeout	Set the network idle timeout in minutes. If the network idle timeout without any operation, the page automatically log off
Remote Telnet	Whether to enable remote telnet login
Telnet port	Sets the port number by logging onto the remote telnet

8.1.3 NTP settings



Time/Date Setting

NTP Settings

NTP Enable: Enable

Option 42: Disable

Current Time: 2015 - 11 - 27 . 02 : 43 : 41

Sync with host: Sync with host

NTP Settings: (GMT+08:00) China Coast, Hong Kong

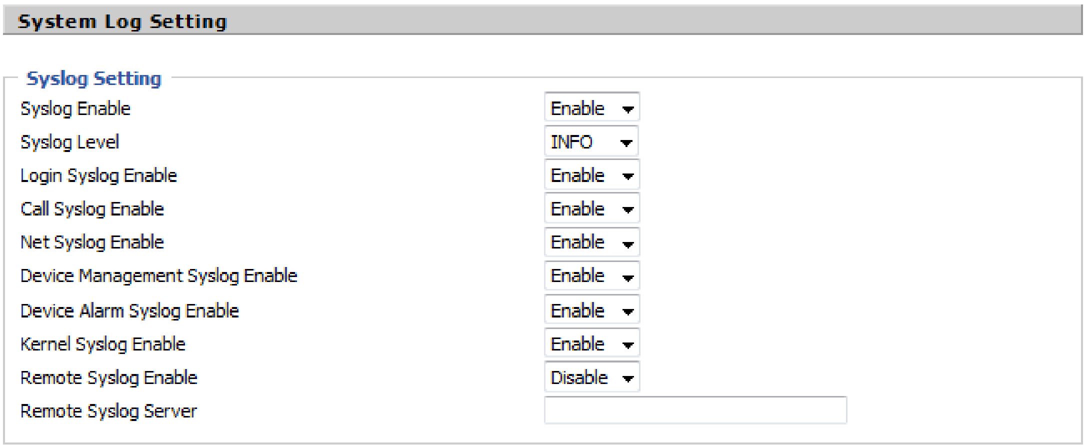
Primary NTP Server: clock.fmt.he.net

Secondary NTP Server: cn.pool.ntp.org

NTP synchronization(1 - 1440min): 60

parameter name	description
NTP switch	Whether NTP is enabled
current time	Show current time
NTP settings	Set the time zone
Primary NTP server	IP address or domain name of choice for NTP server
From the NTP server	IP address or domain name server alternate NTP
NTP Synchronization	NTP synchronous period, when the cycle length may be any one of 1 to 1,440 minutes, the default setting is 60 minutes

8.1.4 System Log Settings



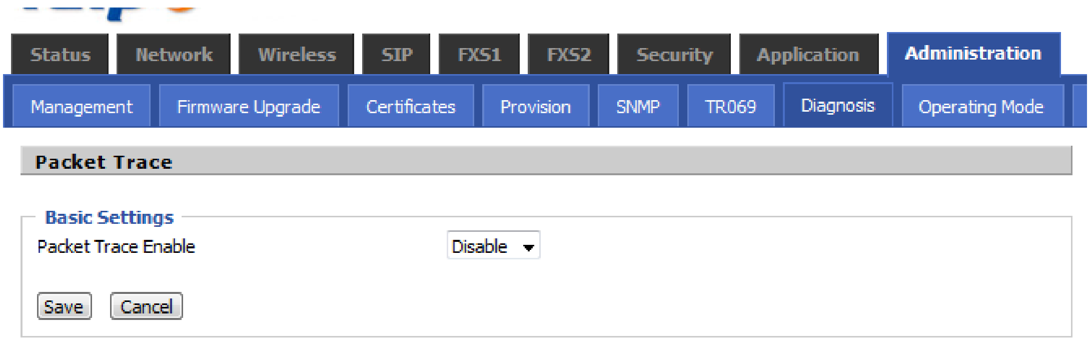
System Log Setting

Syslog Setting

Syslog Enable	Enable
Syslog Level	INFO
Login Syslog Enable	Enable
Call Syslog Enable	Enable
Net Syslog Enable	Enable
Device Management Syslog Enable	Enable
Device Alarm Syslog Enable	Enable
Kernel Syslog Enable	Enable
Remote Syslog Enable	Disable
Remote Syslog Server	

parameter name	description
System log enable	Whether to enable the system log function
System log level	Select the system log level, there are two levels INFO andDebug, Debug which can get more information than INFO
Remote system log enable	Whether to enable remote system logging
Remote system log server	Add the remote server IP address

8.1.5 Packet Trace



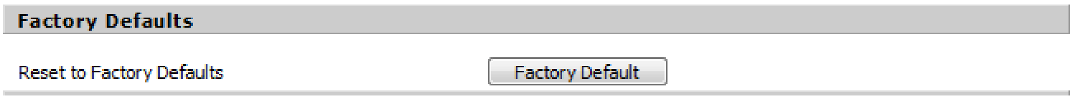
Packet Trace

Basic Settings

Packet Trace Enable: Disable

The user can use the message tracking function to intercept sent packets. Click the Start button to start the data tracking and keep refreshing the page until the message tracking is displayed as stopped. Click the Save button to save the captured packet.

8.1.6 Factory Default

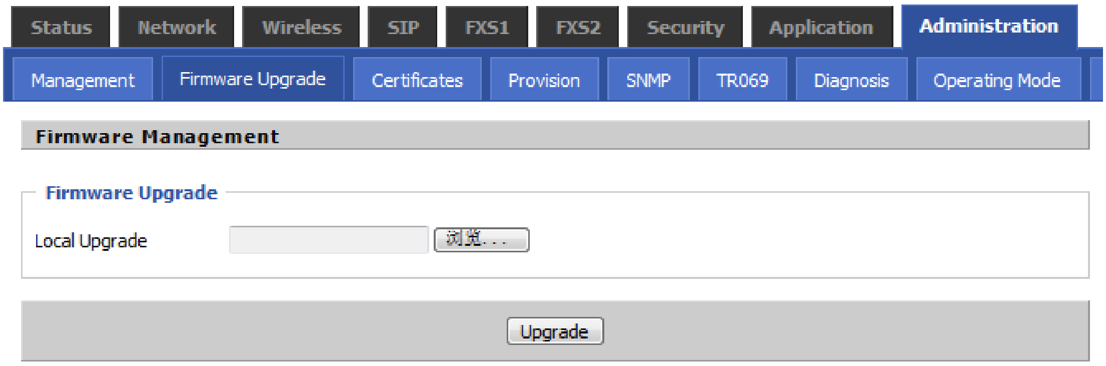


Factory Defaults

Reset to Factory Defaults

Click Factory Default to reset everything back to factory status. Reboot required.

8.2 Firmware Management



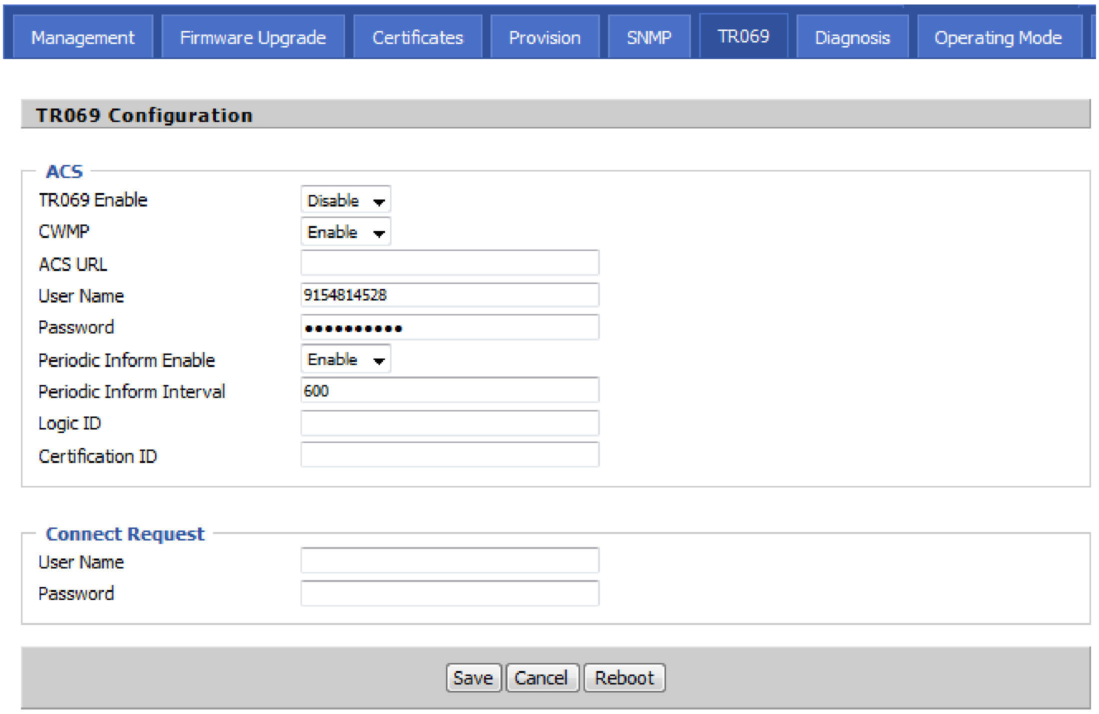
Firmware Management

Firmware Upgrade

Local Upgrade

parameter name	description
Upgrade type	Temporarily only choose to upgrade the software
Local upgrade	Select the local upgrade file, and then click Upgrade to upgrade the software

8.3 TR069



TR069 Configuration

ACS

TR069 Enable	Disable
CWMP	Enable
ACS URL	
User Name	9154814528
Password	●●●●●●●●●●●
Periodic Inform Enable	Enable
Periodic Inform Interval	600
Logic ID	
Certification ID	

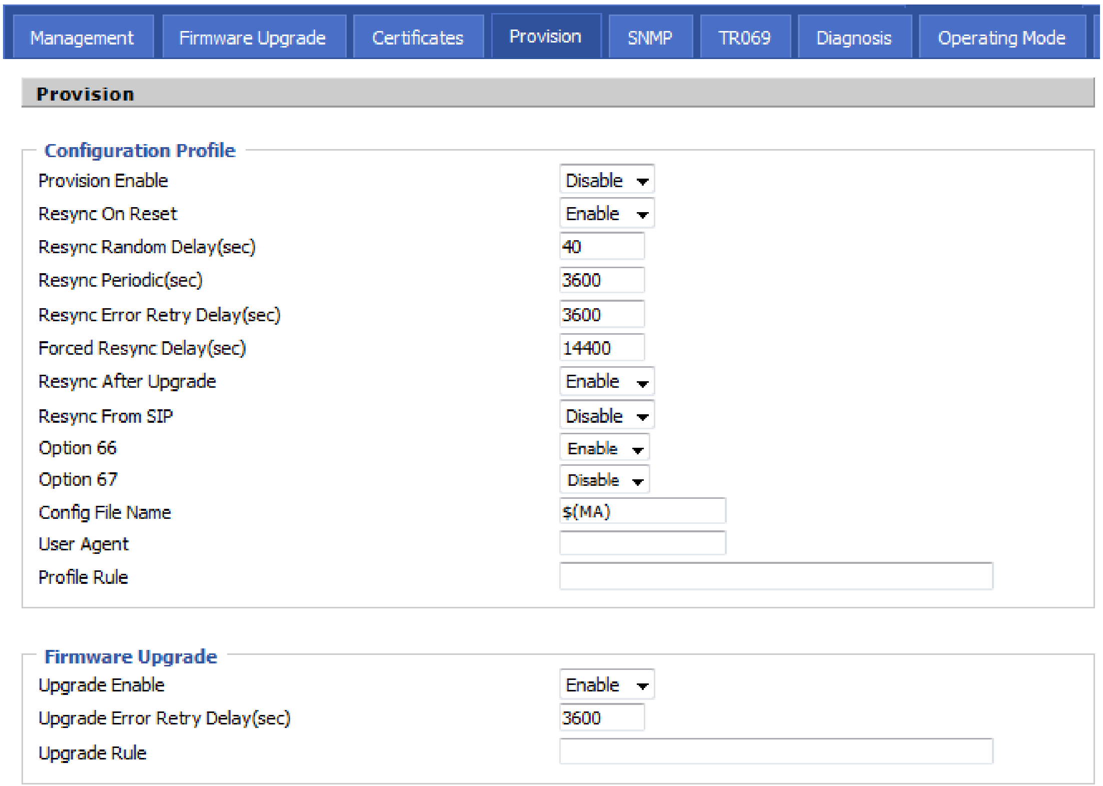
Connect Request

User Name	
Password	

parameter name	description
TR069 Enable	TR069 is enabled
CWMP	Whether to enable TR069 (new version does not have this parameter)
ACS URL	ACS URL address
User Name	ACS user name
Password	ACS Password
Regular notifications are enabled	Whether to open the cycle notification function, the default is open
Regularly notify the time interval	Periodic notification interval, s, default 43200s
User Name	TR069 server username to connect to the DUT
Password	TR069 server is connected to the DUT password
SSL Key	Fill SSL key

8.4 Provision

TPX820 support to deliver the configuration http / https / tftp, firmware upgrades and other operations.



Provision

Configuration Profile

Provision Enable	Disable
Resync On Reset	Enable
Resync Random Delay(sec)	40
Resync Periodic(sec)	3600
Resync Error Retry Delay(sec)	3600
Forced Resync Delay(sec)	14400
Resync After Upgrade	Enable
Resync From SIP	Disable
Option 66	Enable
Option 67	Disable
Config File Name	$(MA)
User Agent	
Profile Rule	

Firmware Upgrade

Upgrade Enable	Enable
Upgrade Error Retry Delay(sec)	3600
Upgrade Rule	

parameter name	description
Provision Enable	Whether to enable provision.
Synchronous reset	DIV378 reboot whether to re-enable sync
Synchronous random delay	Sets the maximum delay request to synchronize files, the default is 40
Synchronization period (sec)	If the last failed resynchronization is in the " Resync Error Retry Delay after" time, G201N4 will retry the

	resynchronization, the default is 3600 seconds.
Synchronization error retry delay	Setting the timing resynchronization, the default value is 3600 seconds.
Force sync delay (sec)	If it is time to re-sync, but G201N4 is busy, in which case, G201N4 will wait for some time, the longest was "forced to re-sync delay" defaults to 14400s , after a time, G201N4 will be forced to re-sync.
Resynchronization after upgrade	After resynchronization, if firmware update feature is enabled, the default is to enable
Resync From SIP	Whether from the SIP resynchronization
Option 66	It is only used mode specified within the company. When using TFTP and options 66 When implementing configuration, the user must IP542N enter the correct profile name of the page. When you disable the option 66 , this argument does not work.
Profile name	Profile name
Profile Rule	Profile URL Note that the specified file path is relative

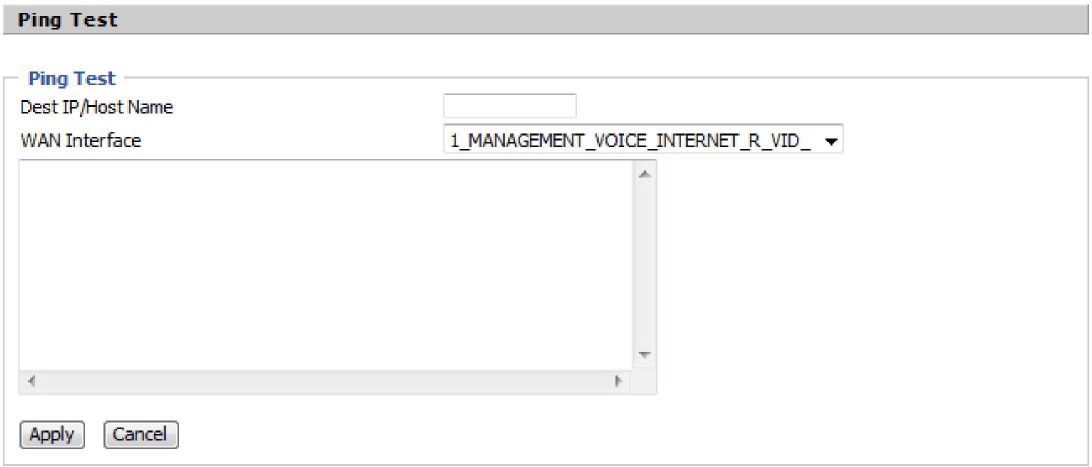
	to the TFTP server's root directory.

8.5 Diagnosis

This page is based on network connection status .

8.5.1 Ping Test

Use ICMP protocol to test network connectivity.



Ping Test

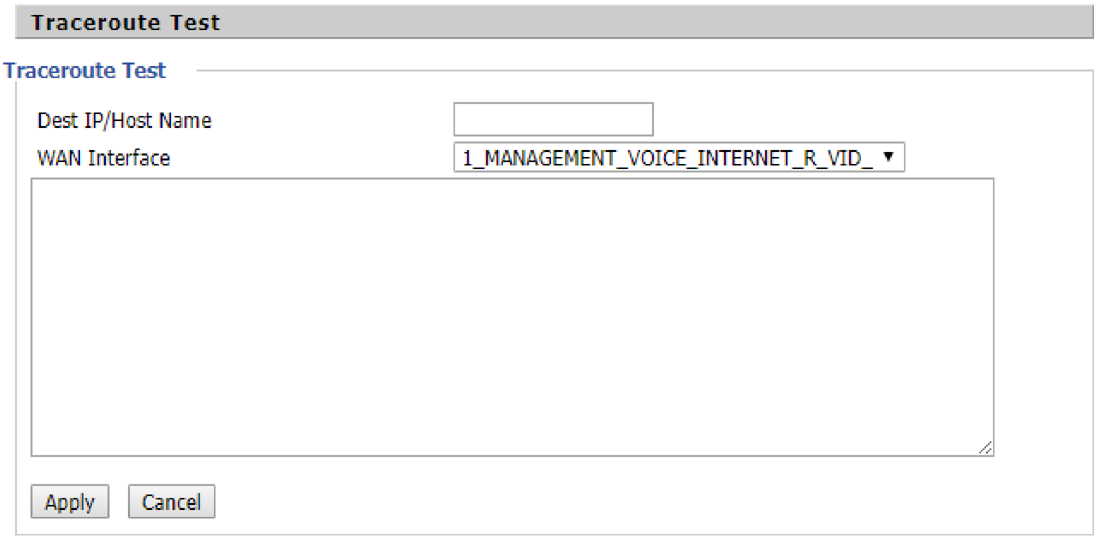
Ping Test

Dest IP/Host Name

WAN Interface 1_MANAGEMENT_VOICE_INTERNET_R_VID_

8.5.2 Traceroute

Use tracert can view the routing nodes in the network.



Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface 1_MANAGEMENT_VOICE_INTERNET_R_VID_