

The G902 High Speed Router User's Guide



V1.1

Table of Contents

1	Preface	5
1.1	Declaration of Conformity	5
1.1.1	Part 15 FCC Rules	5
1.1.2	Class B Digital Device or Perpheral	5
1.2	GNU GPL Information	6
1.3	Warning	6
2	Overview	7
2.1	G900 series	7
2.1.1	G900 series	7
2.1.2	Power Adapter	7
2.2	LED Indicators	8
2.3	Hardware Installation	8
2.4	Voice Prompt	11
3	Configuring Basic Settings	14
3.1	Two-Level Management	14
3.2	Accessing Web Page	14
3.2.1	From LAN port	14
3.2.2	From WAN port	15
3.3	Web Page	15
3.4	Setting up the Time Zone	16
3.5	Setting up the Internet Connection	17
3.6	Setting up the Wireless Connection	17
3.6.1	Enable Wireless and Setting SSID	17
3.6.2	Encryption	19
3.7	Register	19
3.7.1	Get the Accounts	19
3.7.2	Connections	19
3.7.3	Configuration SIP from Webpage	20
3.7.4	View the Register Status	20
3.8	Make Call	21
3.8.1	Calling phone or extension numbers	21
3.8.2	Direct IP calls	21
3.8.3	Call Hold	21
3.8.4	Blind Transfer	21
3.8.5	Attended Transfer	22
3.8.6	Conference	22
4	Web Configuration	22
4.1	Login	22

4.2	Status	23
4.3	Network&Security	24
4.3.1	WAN	24
4.3.2	LAN	29
4.3.3	MAC Clone	31
4.3.4	VPN	31
4.3.5	DMZ	32
4.3.6	DDNS Setting	32
4.3.7	Port Forward	33
4.3.8	Advance	34
4.3.9	Port Setting	34
4.3.10	QoS	35
4.3.11	Routing	35
4.4	Wireless	36
4.4.1	Basic	36
4.4.2	Wireless Security	37
4.4.3	WMM	40
4.4.4	WDS	41
4.4.5	WPS	41
4.4.6	Station Info	43
4.4.7	Advanced	43
4.5	Wireless 5G	45
4.5.1	Basic	45
4.5.2	Wireless Security	47
4.5.3	WMM	47
4.5.4	WDS	47
4.5.5	WPS	47
4.5.6	Station Info	48
4.5.7	Advanced	48
4.6	SIP	49
4.6.1	SIP Settings	49
4.6.2	VoIP Qos	50
4.7	FXS1	50
4.7.1	SIP Account	50
4.7.2	Preferences	55
4.7.3	Dial Plan	59
4.7.4	Blacklist	61
4.7.5	Call Log	61
4.8	FXS2	63
4.9	Security	63
4.9.1	Filtering Setting	63
4.9.2	Content Filtering	64



4.10	Application	65
4.10.1	UPnP	65
4.10.2	IGMP	65
4.10.3	MLD	66
4.11	Storage	66
4.11.1	Disk Management	66
4.11.2	FTP Setting	67
4.11.3	Smb Setting	67
4.12	Administration	68
4.12.1	Management	68
4.12.2	Firmware Upgrade	71
4.12.3	Provision	71
4.12.4	SNMP	72
4.12.5	TR069	73
4.12.6	Diagnosis	74
4.12.7	Operation Mode	74
4.13	System Log	75
4.14	Logout	75
4.15	Reboot	76
5	Trouble shooting of the guide	77
5.1	Setting your PC gets IP automatically	77
5.2	Can not connect to the configuration Website	78
5.3	Forget the Password	78
5.4	Fast Bridge Setting	78

1 Preface

Thank you for choosing G902 wireless router with VoIP. This product will allow you to make ATA call using your broadband connection, and provides Wi-Fi router function.

This manual provides basic information on how to install and connect G902 wireless router with VoIP to the Internet. It also includes features and functions of wireless router with VoIP components, and how to use it correctly.

Before you can connect G902 to the Internet and use it, you must have a high-speed broadband connection installed. A high-speed connection includes environments such as DSL, cable modem, and a leased line.

G902 wireless router with VoIP is a stand-alone device, which requires no PC to make Internet calls. This product guarantees clear and reliable voice quality on Internet, which is fully compatible with SIP industry standard and able to interoperate with many other SIP devices and software on the market.

1.1 Declaration of Conformity

1.1.1 Part 15 FCC Rules

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

This device may not cause harmful interference, and

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

1.1.2 Class B Digital Device or Peripheral

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

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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

1.2 GNU GPL Information

G902 firmware contains third-party software under the GNU General Public License (GPL). FLYINGVOICE uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license. The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded online:

<http://www.flyingvoice.com/index.php?m=content&c=index&a=lists&catid=169>

1.3 Warning

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

2 Overview

Before you use the high speed router, please get acquainted with the LED indicators and connectors first.

2.1 G900 series

2.1.1 G900 series

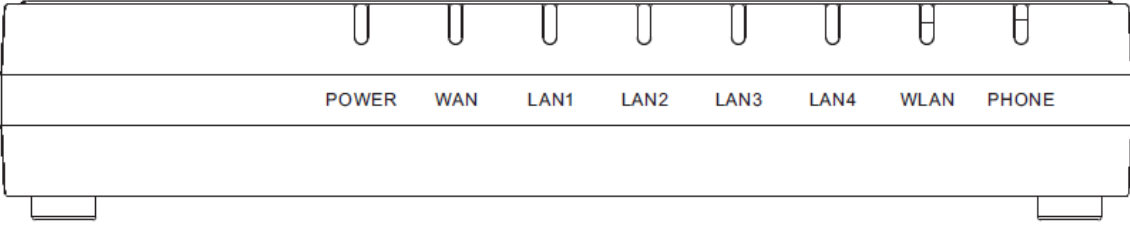
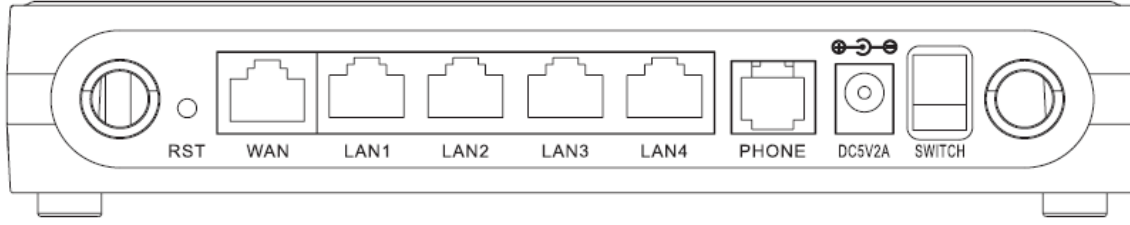
	G902	G902P	G901	G901P	G900	G900P
WAN				1xGE in RJ45		
LAN	4xGE in RJ45					
WiFi	2X2 2.4G 802.11 b/g/n					
	2X2 5G 802.11ac					
USB	1X USB 2.0					
FXS	2xFXS in RJ11		1xFXS in RJ11		No	
PoE	No	Yes	No	Yes	No	Yes
Power Adapter	12V/2A	12V/3A	12V/2A	12V/3A	12V/2A	15V/3A

Trade Mark: Flyingvoive.

2.1.2 Power Adapter

Model	Type	Trade Mark	Features
S24B13-120A200-Y4	EU	GONGJIN	INPUT: 100-240VAC/50-60HZ/MAX 0.7A OUTPUT: 12VDC/2A
S24B12-120A200-Y4	UL	GONGJIN	INPUT: 100-240VAC/50-60HZ/MAX 0.7A OUTPUT: 12VDC/2A
F12W 3-120100SPAU	UL	FRECOM	INPUT: 100-240VAC/50-60HZ/MAX 0.3A OUTPUT: 12VDC/1A
F12W 3-120100SPAV	EU	FRECOM	INPUT: 100-240VAC/50-60HZ/MAX 0.3A OUTPUT: 12VDC/1A
SWPP-12003000-W	UL&EU	TOP-ASIA	INPUT: 100-240VAC/50-60HZ/MAX 1.5A OUTPUT: 12VDC/3A

2.2 LED Indicators

Front Panel	LED	Status	Explanation
	PHONE	Blinking(Green)	Not registered.
		On (Green)	Registered
	WLAN	On (Green)	Wireless access point is ready.
		Blinking(Green)	It will blink while wireless traffic goes through.
	LAN 1/2/3/4	On (Green)	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking(Green)	The data is transmitting.
	WAN	On(Green)	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking(Green)	It will blink while transmitting data.
	POWER	On(Red)	The router is powered on and running normally.
		Off	The router is powered off.
Rear Panel	Interface	Description	
	ON/OFF	Power Switch.	
	DC 5V/2A	Connector for a power adapter.	
	FXS	Connect to the phone.	
	WAN	Connector for accessing the Internet.	
	LAN (1/2/3/4)	Connectors for local networked devices.	

2.3 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

Step 1. Connect Line port to land line jack with a RJ-11 cable.

Step 2. Connect the WAN port to a modem or switch or router or Internet with an Ethernet cable.

Step 3. Connect one port of 4 LAN ports to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.

Step 4. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.

Step 5. Push the ON/OFF button to power on the router.

Step 6. Check the Power and WAN, LAN LEDs to assure network connections.



Warning: Please do not attempt to use other different power adapter or cut off power supply during configuration or updating the G201N4 VoIP home gateway. Using other power adapter may damage G201N4 and will void the manufacturer warranty.



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

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.*

2.4 Voice Prompt

In any circumstance, pressing the following command to enter relevant function. The following table lists command, and description.

Voice Menu Setting Options

Operation code	Contents
1	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “1”, and G902 report the current WAN port connection type</p> <p>Step 3.Prompt "Please enter password", user need to input password with end char # if user want to configuration WAN</p>
2	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “2”, and G902 report current WAN Port IP Address</p> <p>Step 3.Input the new WAN port IP address and with the end char #, using “*” to replace “.”, user can input 192*168*20*168 to set the new IP address 192.168.20.168 press # key to indicate that you have finished</p> <p>Step 4.Report “operation successful” if user operation properly.</p>
3	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “3”, and G902 report current WAN port subnet mask</p> <p>Step 3.Input a new WAN port subnet mask and with the end char # using “*” to replace “.”, user can input 255*255*255*0 to set the new WAN port subnet mask 255.255.255.0 press # key to indicate that you have finished</p> <p>3) Report “operation successful” if user operation properly.</p>
4	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “4”, and G902 report current gateway</p> <p>Step 3.Input the new gateway and with the end char # using “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1 press # (pound) key to indicate that you have finished</p> <p>3) Report “operation successful” if user operation properly.</p>

5	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “5”, and G902 report current DNS</p> <p>Step 3.Input the new DNS and with the end char # using “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1</p> <p>press # (pound) key to indicate that you have finished</p> <p>3) Report “operation successful” if user operation properly.</p>
6	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “6”, and G902 report “Factory Reset”</p> <p>Step 3.Prompt "Please enter password", the method of inputting password is the same as operation 1. If you want to quit by the wayside, press “*”.</p> <p>Step 4.Prompt “operation successful” if password is right and then G902 will be factory setting.</p>
7	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “7”, and G902 report “Reboot”</p> <p>Step 3.Prompt "Please enter password", the method of inputting password is same as operation 1.</p> <p>Step 4.G902 will reboot if password is right and operation is properly.</p>
8	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “8”, and G902 report “WAN Port Login”</p> <p>Step 3.Prompt "Please enter password", the method of inputting password is same as operation 1. If you want to quit by the wayside, press “*”.</p> <p>Step 4.Report “operation successful” if user operation properly.</p> <p>Step 5.Prompt “1enable 2disable”,choose 1 or 2, and with confirm char #</p>
9	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “9”, and G902 report “ WEB Access Port”</p> <p>Step 3.Prompt “Please enter password”, the method of inputting password is same as operation 1.</p> <p>Step 4.Report “operation successful” if user operation properly.</p> <p>Step 5.Report the current WEB Access Port</p> <p>Step 6.Set the new WEB access port and with end char #</p>
0	<p>Step 1.Pick up phone and press “****” to start IVR</p> <p>Step 2.Choose “0”, and G902 report current Firmware version</p>

Notice:

1. When using Voice Menu, press * (star) to return the main menu.
2. If any changes made in the IP assignment mode, please reboot the G902 to take the setting into effect.

3. When enter IP address or subnet mask, use "*" (Star) to replace "." (Dot).
4. For example, to enter the IP address 192.168.20.159 by keypad, press these keys: 192*168*20*159, use the #(pound) key to indicate that you have finished entering the IP address.
5. #(pound) key to indicate that you have finish entering the IP address or subnet mask
6. When assigning IP address in Static IP mode, setting IP address, subnet mask and default gateway is a must. If in DHCP mode, please make sure that DHCP SERVER is available in your existing broadband connection to which WAN port of G902 is connected.
7. The default LAN port IP address of G902 is 192.168.1.1 and do not set the WAN port IP address of G902 in the same network segment of LAN port of G902, otherwise it may lead to the G902 fail to work properly.
8. You can enter the password by phone keypad, the matching table between number and letters as follows:
 - To input: D, E, F, d, e, f -- press '3'
 - To input: G, H, I, g, h, i -- press '4'
 - To input: J, K, L, j, k, l -- press '5'
 - To input: M, N, O, m, n, o -- press '6'
 - To input: P, Q, R, S, p, q, r, s -- press '7'
 - To input: T, U, V, t, u, v -- press '8'
 - To input: W, X, Y, Z, w, x, y, z -- press '9'
 - To input all other characters in the administrator password-----press '0',E.g. password is 'admin-admin', press '236460263'

3 Configuring Basic Settings

3.1 Two-Level Management

This chapter explains how to setup a password for an administrator/root user and how to adjust basic/advanced settings for accessing Internet successfully.

G902 supports two-level management: administrator and user. For administrator mode operation, please type “admin/admin” on Username/Password and click Login button to configuration. While for user mode operation, please type “user/user” on Username/Password and click Login button for full configuration.

3.2 Accessing Web Page

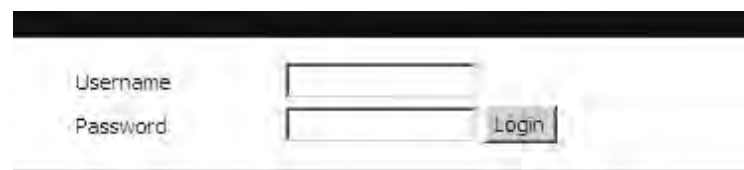
3.2.1 From LAN port

1. Make sure your PC have connected to the router’s LAN port correctly.



Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of router is 192.168.1.1**. For the detailed information, please refer to the later section - **Trouble shooting of the guide**.

2. Open a web browser on your PC and type <http://192.168.1.1> The following window will be open to ask for username and password, and you can choose language.



The screenshot shows a web browser window with a black title bar. Below the title bar, there are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. To the right of the Password field is a 'Login' button. The background of the page is light gray.

3. For administrator mode operation, please type “**admin/admin**” on Username/Password and click Login to configuration. Yet, for root user mode operation, please type “**user/user**” on Username/Password and click Login for full configuration.

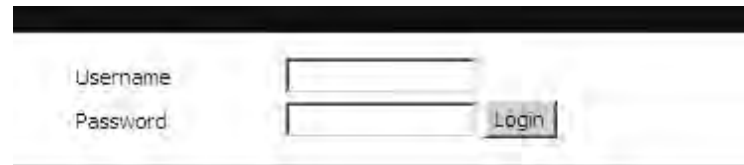


Notice: If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

4. The web page can be logged out after 5 minutes without any operation.

3.2.2 From WAN port

1. Make sure your PC can connect to the router's WAN port correctly.
2. Getting the IP addresses of WAN port using Voice prompt.
3. Open a web browser on your PC and type <http://the IP address of WAN port>. The following window will be open to ask for username and password.



4. For administrator mode operation, please type **“admin/admin”** on Username/Password and click Login to configuration. Yet, for root user mode operation, please type **“user/user”** on Username/Password and click Login for full configuration.



Notice: If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

5. The web page can be logged out after 5 minutes without any operation.

3.3 Web Page

	Field Name	Description
	Navigation bar	Click navigation bar, many sub-navigation bar will appear in the place 2
	Title	Click sub-navigation bar to choose one configuration page
	Parameter	To configuration the parameters
	Save	<ol style="list-style-type: none"> 1. Every time making some changes, user should press this button to confirm the changes. 2. After pressing the button, the red

<p>Management Firmware Upgrade Provision</p> <p>Please REBOOT to make the changes effective!</p>		Please REBOOT to make the changes effective will appear to notice rebooting.
	Cancel	To cancel the changes.
	Reboot	Press it to reboot the router

3.4 Setting up the Time Zone

<p>Time/Date Setting</p> <p>NTP Settings</p> <p>NTP Enable <input type="text" value="Enable"/></p> <p>Current Time <input type="text" value="Fri Aug 16 15:46:59 GMT 2013"/> <input type="button" value="Sync with host"/></p> <p>NTP Settings <input type="text" value="(GMT+08:00) China Coast, Hong Kong"/></p> <p>Primary NTP Server <input type="text" value="pool.ntp.org"/></p> <p>Secondary NTP Server <input type="text" value="cn.pool.ntp.org"/></p> <p>NTP synchronization(1 - 1440m) <input type="text" value="60"/></p>	<p>Open Administration/Management webpage as shown left, please select the Time Zone for the router installed and specify the NTP server and set the update interval in NTP synchronization.</p>
---	--

3.5 Setting up the Internet Connection

From WAN page, multi wan connection could be built or deteted. If you want to know more information about Internet Connection setting, please refer to 5.3 section.

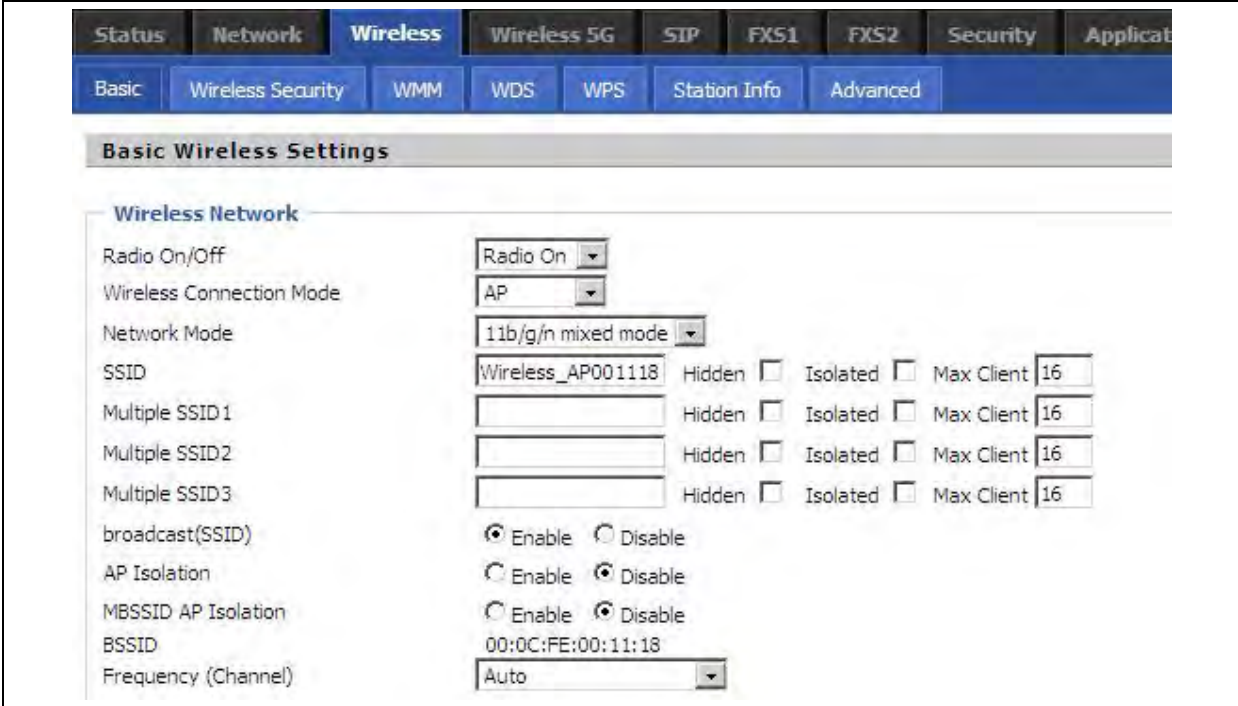
Field Name	Description
Connect Name	Use keywords to indicate WAN port service model (the parameters are defined in Network--> multi-WAN page). Please refer to 5.3.1 section.
Service	Chose the service mode. Please refer to 5.3.1 section.
IP Protocol Version	Only IPv4 for G902
INTERNET	Choose Internet connection mode.
NAT Enable	If or not enable NAT.
VLAN Mode	If or not enable VLAN Mode.
VLAN ID	Set the VLAN ID.
802.1p	Set the priority of VLAN, Options are 0~7.
DNS Mode	The default is Manual.
Primary DNS Address	The primary DNS of Internet port.
Secondary DNS Address	The secondary DNS of Internet port.
Port Bind	Port bind is used for binding the service for different LAN ports and SSIDs.

3.6 Setting up the Wireless Connection

To set up the wireless connection, please skip the following steps.

3.6.1 Enable Wireless and Setting SSID

Open **Wireless/Basic** webpage as shown below

	Field Name	Description
Radio On/Off	Radio On/Off	Select “Radio Off” to disable wireless. Select “Radio on”to enable wireless.
Network Mode	Network Mode	Choose one network mode from the drop down list.
SSID	SSID	The name of the wireless name, it can be any text numbers or various special characters.
Multiple SSID1-3	Multiple SSSD1-3	Set more wireless network.
Frequency (Channel)	Frequency	Choose channel frequency.

3.6.2 Encryption

Open Wireless/Wireless Security webpage to set the encryption of routers.

Basic Wireless Security WMM WDS WPS Station Info Advanced	Field Name	Description
<p>WIFI Security Setting</p> <p>Select SSID</p> <p>SSID choice: <input type="text" value="Wireless_AP001118"/></p> <p>"Wireless_AP001118"</p> <p>Security Mode: <input type="text" value="WPA-PSK"/></p> <p>WPA Algorithms: <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES</p> <p>Pass Phrase: <input type="text" value="23123123"/></p> <p>Key Renewal Interval: <input type="text" value="3600"/> Second in Month (0 ~ 4194303)</p> <p>Access policy: <input type="text" value="Disable"/></p> <p>Policy: <input type="text" value="Disable"/></p> <p>Add a station MAC: <input type="text"/></p>	<p>SSID Choice</p> <p>Security Mode</p>	<p>Choose one SSID from Off-premises 1, off-premises 2 and Premises.</p> <p>Select an appropriate encryption mode to improve the security and privacy of your wireless data packets. Each encryption mode will bring out different web page and ask you to offer additional configuration.</p>

3.7 Register

3.7.1 Get the Accounts

G902 have a FXS port, you can use it to make SIP call, and before registering, you should get the SIP account from you administrator or provider.

3.7.2 Connections

Connect G902 to the Internet properly

3.7.3 Configuration SIP from Webpage



Step 1. Open FXS1(FXS2)/SIP Account webpage, as the picture in the right side.

Step 2. Fill the SIP Server domain and SIP Server address (which get from you administrator or provider) into Domain Name parameter, into SIP Server

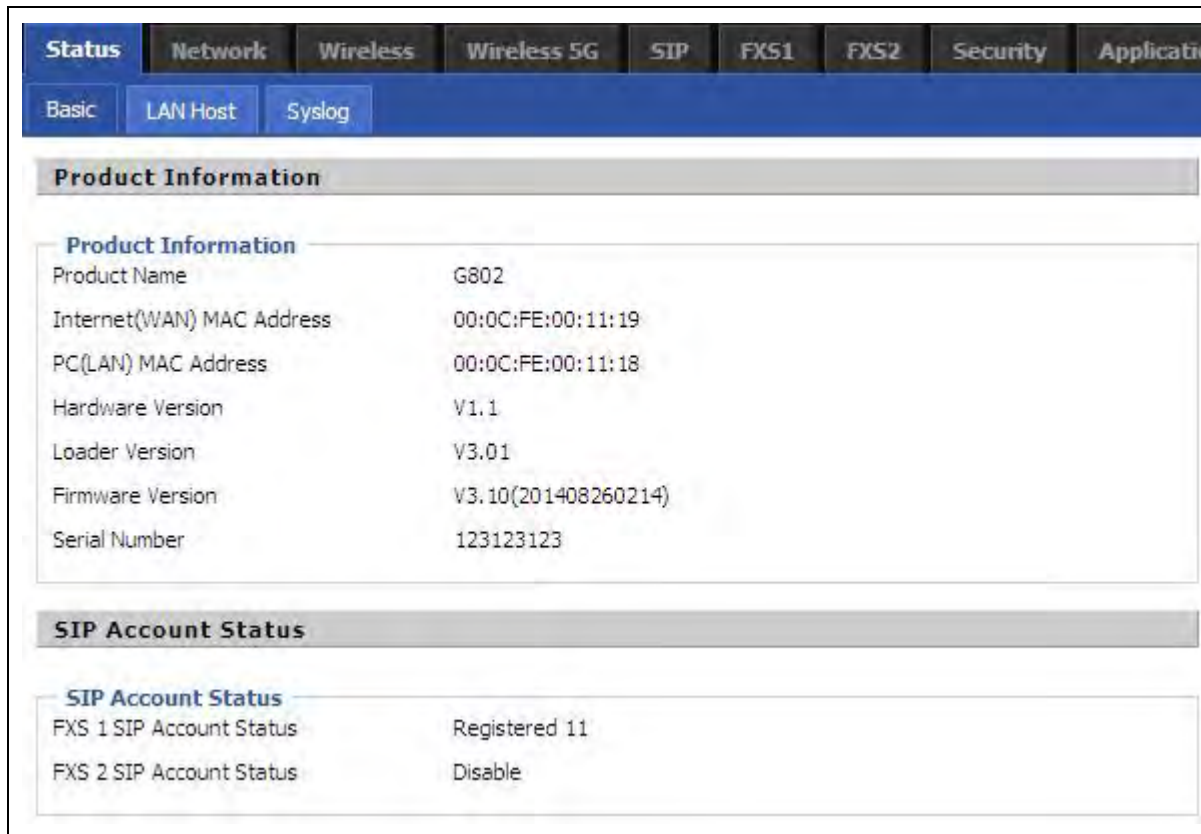
Step 3. Fill account which get from you administrator into Display Name parameter, Phone Number parameter, and Account parameter.

Step 4. Fill password which get from you administrator into Password parameter.

Step 5. Press **Save** button in the bottom of the webpage to save changes.

Note: if there is **Please REBOOT to make the changes effective!**, please press **Reboot** button to make changes effective.

3.7.4 View the Register Status



To view the status, please open Status webpage and view the value of register status. The value is registered like the following picture which means G902 have registered normally and you can make calls.

3.8 Make Call

3.8.1 Calling phone or extension numbers

To make a phone or extension number call:

1. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) have public IP addresses, or
2. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) are on the same LAN using private or public IP addresses, or
3. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) can be connected through a router using public or private IP addresses.

To make a call, first pick up the analog phone or turn on the speakerphone on the analog phone, input the IP address directly, end with #.

3.8.2 Direct IP calls

Direct IP calling allows two phones, that is, an ATA with an analog phone and another VoIP Device, to talk to each other without a SIP proxy. VoIP calls can be made between two phones if:

1. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) have public IP addresses, or
2. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) are on the same LAN using private or public IP addresses, or
3. Both ATA and the other VoIP device (i.e., another ATA or other SIP products) can be connected through a router using public or private IP addresses.

To make a direct IP call, first pick up the analog phone or turn on the speakerphone on the analog phone, Input the IP address directly, with the end “#”.

3.8.3 Call Hold

While in conversation, pressing the “*77” to put the remote end on hold, then you will hear the dial tone and the remote party will hear hold tone at the same time.

Pressing the “*77” again to release the previously hold state and resume the bi-directional media.

3.8.4 Blind Transfer

Assuming that call party A and party B are in conversation. A wants to Blind Transfer B to C:

Step 1. Party A dials “*78” to get a dial tone, then dials party C’s number, and then press immediately key # (or wait for 4 seconds) to dial out.

Step 2. A can hang up.

3.8.5 Attended Transfer

Assuming that call party A and B are in conversation. A wants to Attend Transfer B to C:

Step 1. Party A dial “*77” to hold the party B, when hear the dial tone, A dial C’s number, then party A and party C are in conversation.

Step 2. Party A dial “*78” to transfer to C, then B and C now in conversation.

Step 3. If the transfer doesn’t success, then A and B in conversation again.

3.8.6 Conference

Assuming that call party A and B are in conversation. A wants to add C to the conference:

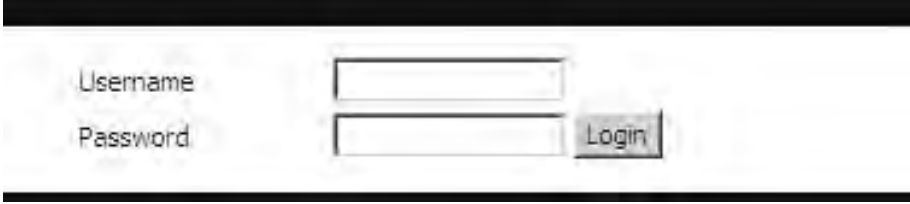
Step 1. Party A dial “*77” to hold the party B, when hear the dial tone, A dial C’s number, then party A and party C are in conversation.

Step 2. Party A dial “*88” to add C, then A, B and C now in conference.

4 Web Configuration

This chapter will guide users to execute advanced (full) configuration through admin mode operation.

4.1 Login

	Step 1. Connect the LAN port of the router to your PC
	Step 2. Open a web browser on your PC and type in http://192.168.1.1 . The window will ask for typing username and password. And you can choose language, too.
	Step 3. Please type “ admin/admin ” on Username/Password for administration operation.

4.2 Status

<p>Product Information</p> <p>Product Information</p> <table border="1"> <tr><td>Product Name</td><td>G802</td></tr> <tr><td>Internet(WAN) MAC Address</td><td>00:0C:FE:00:11:19</td></tr> <tr><td>PC(LAN) MAC Address</td><td>00:0C:FE:00:11:18</td></tr> <tr><td>Hardware Version</td><td>V1.1</td></tr> <tr><td>Loader Version</td><td>V3.01</td></tr> <tr><td>Firmware Version</td><td>V3.10(201408260214)</td></tr> <tr><td>Serial Number</td><td>123123123</td></tr> </table>	Product Name	G802	Internet(WAN) MAC Address	00:0C:FE:00:11:19	PC(LAN) MAC Address	00:0C:FE:00:11:18	Hardware Version	V1.1	Loader Version	V3.01	Firmware Version	V3.10(201408260214)	Serial Number	123123123	<p>This webpage shows the status information about product information, Network and system.</p>
Product Name	G802														
Internet(WAN) MAC Address	00:0C:FE:00:11:19														
PC(LAN) MAC Address	00:0C:FE:00:11:18														
Hardware Version	V1.1														
Loader Version	V3.01														
Firmware Version	V3.10(201408260214)														
Serial Number	123123123														
<p>SIP Account Status</p> <p>SIP Account Status</p> <table border="1"> <tr><td>FXS 1 SIP Account Status</td><td>Registered 11</td></tr> <tr><td>FXS 2 SIP Account Status</td><td>Disable</td></tr> </table>	FXS 1 SIP Account Status	Registered 11	FXS 2 SIP Account Status	Disable	<p>It shows the basic information of the product, such as product name, serial number, MAC address, hardware version and software version</p>										
FXS 1 SIP Account Status	Registered 11														
FXS 2 SIP Account Status	Disable														
<p>FXS Port Status</p> <p>FXS Port Status</p> <table border="1"> <tr><td>FXS 1 Hook State</td><td>On</td></tr> <tr><td>FXS 1 Port Status</td><td>Idle</td></tr> <tr><td>FXS 2 Hook State</td><td>On</td></tr> <tr><td>FXS 2 Port Status</td><td>Idle</td></tr> </table>	FXS 1 Hook State	On	FXS 1 Port Status	Idle	FXS 2 Hook State	On	FXS 2 Port Status	Idle	<p>It also shows the information of Link Status, WAN Port Status, and LAN Port Status.</p>						
FXS 1 Hook State	On														
FXS 1 Port Status	Idle														
FXS 2 Hook State	On														
FXS 2 Port Status	Idle														
<p>Network Status</p> <p>Internet Port Status</p> <table border="1"> <tr><td>Connection Type</td><td>STATIC</td></tr> <tr><td>IP Address</td><td>192.168.10.209</td></tr> <tr><td>Subnet Mask</td><td>255.255.255.0</td></tr> <tr><td>Default Gateway</td><td>192.168.10.1</td></tr> <tr><td>Primary DNS</td><td>8.8.8.8</td></tr> <tr><td>Secondary DNS</td><td></td></tr> <tr><td>WAN Port Status</td><td>100Mbps Full</td></tr> </table>	Connection Type	STATIC	IP Address	192.168.10.209	Subnet Mask	255.255.255.0	Default Gateway	192.168.10.1	Primary DNS	8.8.8.8	Secondary DNS		WAN Port Status	100Mbps Full	<p>And it shows the current time and the running time of the product.</p>
Connection Type	STATIC														
IP Address	192.168.10.209														
Subnet Mask	255.255.255.0														
Default Gateway	192.168.10.1														
Primary DNS	8.8.8.8														
Secondary DNS															
WAN Port Status	100Mbps Full														
	<p>The picture in the left side is the G902's Status webpage.</p>														

4.3 Network & Security

You can configuration the WAN port, LAN port, DDNS, Multi WAN, DMZ, MAC Clone, Port Forward and so on in these two bars.

4.3.1 WAN

This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one WAN mode and then the corresponding page will be displayed.

1. Static IP

You will receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address to the WAN interface.

INTERNET	Field Name	Description
INTERNET Connect Name: 1_TR069_VOICE_INTERNET_R_VID_ <input type="button" value="Delete Connect"/>	IP Address	The IP address of Internet port
Service: TR069_VOICE_INTERNET	Subnet Mask	The subnet mask of Internet port.
IP Protocol Version: IPv4	Default Gateway	The default gateway of Internet port.
INTERNET: Static	DNS Mode	In Static mode, user need set the DNS manually.
NAT Enable: Enable	Primary DNS Address	The primary DNS of Internet port.
VLAN Mode: Disable	Secondary DNS Address	The secondary DNS of Internet port.
VLAN ID: 1 (1-4094)		
Static:		
IP Address: 192.168.10.209		
Subnet Mask: 255.255.255.0		
Default Gateway: 192.168.10.1		
DNS Mode: Manual		
Primary DNS Address: 8.8.8.8		
Secondary DNS Address:		

2. DHCP

It is not necessary for you to type any IP address manually. Simply choose this type and the system will obtain the IP address automatically from DHCP server.

Field Name	Description
DNS Mode	The Default is Manual
Primary DNS Address	The primary DNS of Internet port.
Secondary DNS Address	The secondary DNS of Internet port.
DHCP Renew	Refresh DHCP IP
DHCP Vendor (Option 60)	Specify DHCP Vendor field Display the vendor and product name

INTERNET	
INTERNET	
Connect Name	1_TR069_VOICE_INTERNET_R_VID_ Delete Connect
Service	TR069_VOICE_INTERNET
IP Protocol Version	IPv4
INTERNET	DHCP
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Manual
Primary DNS Address	8.8.8.8
Secondary DNS Address	
DHCP	
DHCP Renew	Renew
DHCP Vendor (Option 60)	VOIP-G802

3. PPPoE

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

INTERNET	Field Name	Description
INTERNET Connect Name: 1_TR069_VOICE_INTERNET_R_VID_ <input type="button" value="Delete Connect"/> Service: TR069_VOICE_INTERNET IP Protocol Version: IPv4 INTERNET: PPPoE NAT Enable: Enable VLAN Mode: Disable VLAN ID: 1 (1-4094) DNS Mode: Manual Primary DNS Address: 8.8.8.8 Secondary DNS Address: <input type="text"/> PPPoE PPPoE Account: <input type="text"/> PPPoE Password: <input type="text"/> Confirm Password: <input type="text"/> Service Name: <input type="text"/> Leave empty to autodetect Operation Mode: Keep Alive Keep Alive Redial Period(0-3600s): 5 Port Bind <input checked="" type="checkbox"/> Port_1 <input checked="" type="checkbox"/> Port_2 <input checked="" type="checkbox"/> Port_3 <input checked="" type="checkbox"/> Port_4 <input checked="" type="checkbox"/> Wireless(SSID1) <input checked="" type="checkbox"/> Wireless(SSID2) <input checked="" type="checkbox"/> Wireless(SSID3) <input checked="" type="checkbox"/> Wireless(SSID4) <small>Note : WAN connection can not be shared between the binding port , and finally bound port WAN connections bind operation will wash away before the other WAN connection to the port binding operation !</small>	PPPoE Account	Assign a valid user name provided by the ISP
	PPPoE Password	Assign a valid password provided by the ISP
	Confirm Password	Enter your PPPoE password again
	Operation Mode	Select the mode of operation, options are Keep Alive, On Demand and Manual: 1. When the mode is Keep Alive, user need to set the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; 2. When the mode is On Demand, user need to set the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; Operation Mode: <input type="text" value="On Demand"/> On Demand Idle Time(0-60m): <input type="text" value="5"/> 3. When the mode is Manual, no need to do other settings.
	Keep Alive Redial Period	Set the interval to send Keep Alive

4. Bridge Mode

Bridge Mode under Multi WAN is different with traditional bridge setting. Bridge mode has no ip address and only work as a bridge between WAN port and LAN port. So Route Connection has to be build to give ip address to local service on device.

Under is example of bridge mode:

1_TR069_VOICE_INTERNET_R_VID_ is router connection for local service.

2_Other_B_VID_ is bridge connection for host of LAN port.

If bridge setting is complex, please refer to 6.4 section for fast setting of bridge mode.

INTERNET

Connect Name: 1_TR069_VOICE_INTERNET_R_VID_ Delete Connect

Service: TR069_VOICE_INTERNET

IP Protocol Version: IPv4

INTERNET Type: Bridge

Bridge Type: Hardware IP Bridge

DHCP Service Type: Pass Through

VLAN Mode: Enable

VLAN ID: 1 (1-4094)

802.1p: 0

Port Bind

Port_1 Port_2 Port_3 Port_4

Wireless(SSID1) Wireless(SSID2) Wireless(SSID3) Wireless(SSID4)

Note : WAN connection can not be shared between the binding port , and finally bound port WAN connections bind operation will wash away before the other WAN connection to the port binding operation !

Field Name		Description
Bridge Type	IP Bridge	Allow all ethernet packets pass. PC could connect to upper network directly.
	PPPoE Bridge	Only Allow PPPoE packets pass. PC need PPPoE dial-up software.
	Hardware IP Bridge	Packets pass through hardware switch with wired speed. Do not support wireless port bind.
DHCP Service Type	Pass Through	Dhcp packets can be forwarded between WAN and LAN, dhcp server in gateway will not allocate IP to hosts of LAN port.
	DHCP Snooping	When gateway forwards dhcp packets form LAN to WAN it will add option82 to dhcp packet, and it will remove option82 when forward dhcp packet form WAN to LAN. Local dhcp service will not allocate ip to hosts of LAN port.
	Local Service	Gateway will not forward dhcp packets between Lan and Wan, it also block dhcp packet from WAN port. Hosts of LAN port can get ip from dhcp server run in gateway.
VLAN Mode	Disable	The WAN interface is untagged. LAN is untagged.
	Enable	The WAN interface is tagged. LAN is untagged.
	Trunk	Only valid in bridge mode. All ports, include WAN and LAN, belong to this VLAN Id and all ports are tagged in this VLAN id. Tagged packets could pass through WAN and LAN.
VLAN ID		Set the VLAN ID.
802.1p		Set the priority of VLAN, Options are 0~7.

5. Connect Name and Service

Connect Name Table is as below:

Content	Define	Comment
No	1~99	WAN Connection id
Service	TR069	The connection only support management application, like TR069, WEB, SNMP and Provision
	INTERNET	The connection only support internet service
	TR069_INTERNET	The connection support management and internet application
	VOICE	The connection only support voice application, like sip and rtp
	TR069_VOICE	The connection support both management and voice application
	VOICE_INTERNET	The connection support voice and internet application
	TR069_VOICE_INTERNET	The connection support management, voice and internet application
	Other	The connection support STB
NAT Mode	B	Bridge
	R	Router
VLAN ID	VID	VLAN ID

For example:

1. 1_TR069_R_VID_2 (First Interface, Service is TR069, NAT Mode, VLAN ID is 2)
2. 2_INTERNET_B_VID_ (Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

4.3.2 LAN

1. LAN Port:

The most generic function of router is NAT. What NAT does is to translate the packets from public IP address to local IP address to forward the right packets to the right host and vice versa.

Field Name	Description
IP Address	Enter the IP address of the router on the local area network, all the IP addresses of the computers which are in the router's LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (The default is 192.168.1.1)
Local Subnet Mask	Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24)
Local DHCP Server	If or not enable Local DHCP Server
DHCP Start Address	Enter a valid IP address as a starting IP address of the DHCP server, and if the router's LAN IP address is 192.168.1.1, starting IP address can be 192.168.1.2 or greater, but should be less than the ending IP address.
DHCP End Address	Enter a valid IP address as an end IP address of the DHCP server.
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS
Primary DNS	Enter the preferred DNS address.
Secondary DNS	Enter the secondary DNS address.
Client Lease Time	This option defines how long the address will be assigned to the computer within the network. In that period, the server does not assign the IP address to the other computer.
DNS Proxy	Enable or disable; If enabled, the device will forward the DNS request of LAN-side network to the WAN side network

2. DHCP Server:

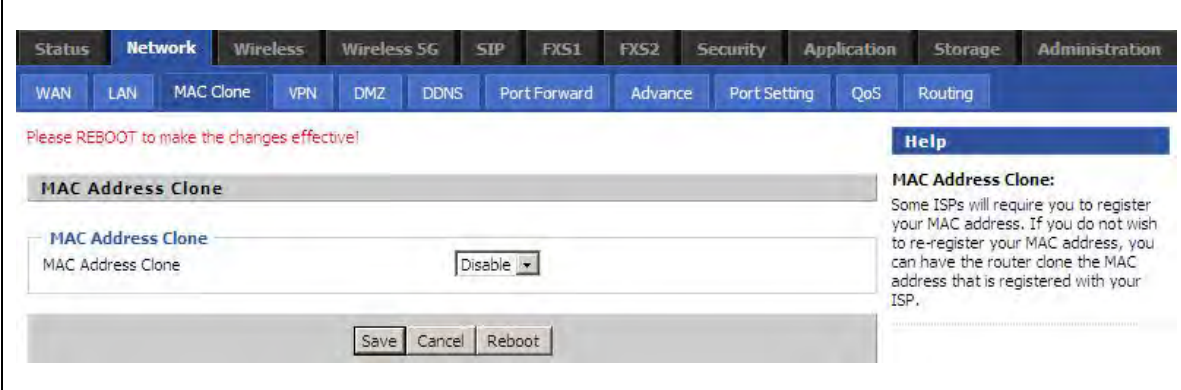
Router has a built-in DHCP server that assigns private IP address to each local host.

DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

	Field Name	Description
<p>IP Address <input type="text" value="192.168.11.1"/></p> <p>Local Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Local DHCP Server <input type="text" value="Enable"/></p> <p>DHCP Start Address <input type="text" value="192.168.11.2"/></p> <p>DHCP End Address <input type="text" value="192.168.11.254"/></p> <p>DNS Mode <input type="text" value="Auto"/></p>	Local DHCP Server	If or not enable DHCP server.
	DHCP Start Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the LAN Interface IP
	DHCP End Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
	DNS Mode	You should set “manual” in the “DNS Mode” if you set “DNS” by yourself. And then fill the DNS in the two following texts. Generally speaking, you can set “Auto” in the “DNS Mode” and the device will get “DNS” from DHCP Server automatically.
<p>Primary DNS <input type="text" value="192.168.1.1"/></p> <p>Secondary DNS <input type="text" value="8.8.8.8"/></p> <p>Client Lease Time(0-86400s) <input type="text" value="86400"/></p>	Primary DNS	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 202.96.134.33 to this field.
	Secondary DNS	You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 202.96.128.86 to this field. If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
	Client Lease Time	It allows you to set the leased time for the specified PC.

4.3.3 MAC Clone

Some ISPs will require you to register your MAC address. If you do not wish to re-register your MAC address, you can have the router clone the MAC address that is registered with your ISP. To use the Clone Address button, the computer viewing the Web-base utility screen will have the MAC address automatically entered in the Clone WAN MAC field.

	<p>Enabling MAC address cloning</p> <ol style="list-style-type: none"> 1. Press the button Get Current PC MAC gets PC's MAC address 2. Press the button Save to save your changes if users don't want to use MAC clone, press the button Cancel to cancel the changes 3. Press the button Reboot to make the changes effective.
--	--

4.3.4 VPN

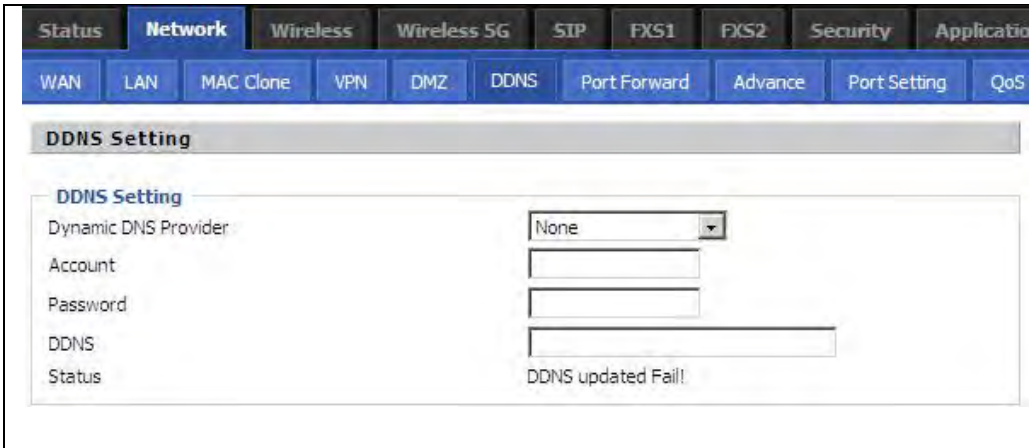
A VPN is a kind of technology which establish a private network based on the public network. VPN network connection between any two nodes does not require the end to end physical connection as the traditional private network; it is structured on the network platform provided by the public network services, the user dhome gateway are transmitted in the logical link. Through VPN technology, users can establish connection between any two devices which are connected to public network and transmit dhome gateway.

VPN Settings	Field Name	Description
<p>Administration</p> <p>VPN Enable <input type="text" value="PPTP"/></p> <p>Initial Service IP <input type="text"/></p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p>	VPN Enable	If or not enable VPN.If enable, you can select PPTP and L2TP mode VPN.
	Initial Service IP	Fill in the VPN server IP address
	User Name	Fill in the authentication username
	Password	Fill in the authentication password

4.3.5 DMZ

	Field Name	Description
	DMZ Enable	If or not enable DMZ.
	DMZ Host IP Address	Enter the private IP address of the DMZ host

4.3.6 DDNS Setting

	Field Name	Description
	Dynamic DNS Provider	DDNS is enabled and select a DDNS service provider
	Account	Enter the DDNS service account
	Password	Enter the DDNS service account password
	DDNS	Enter the DDNS domain name or IP address
	Status	See if DDNS is successfully upgraded

4.3.7 Port Forward

Field Name	Description
Comment	Sets the name of a port mapping rule or comment
IP Address	The IP address of devices under the LAN port.
Port Range	Set the port range for the devices under the LAN port. (1-65535)
Protocol	You can select TCP, UDP, TCP & UDP three cases
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes.
Comment	To set up a virtual server notes
IP Address	Virtual server IP address
Public Port	Public port of virtual server
Private Port	Private port of virtual servers ports
Protocol	You can select from TCP, UDP, and TCP&UDP.
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes.

4.3.8 Advance

Field Name	Description
Most Nat connections	The largest value which the G902 can provide
Mss Mode	Choose Mss Mode from Manual and Auto
Mss Value	Set the value of TCP
AntiDos-p	You can choose to enable or prohibit
IP conflict detection	Select enable if enabled, phone IP conflict will have tips or prohibit;
IP conflict Detecting Interval	Detect IP address conflicts of the time interval

Status	Network	Wireless	Wireless 5G	SIP	FXS1	FXS2	Security	Application	
WAN	LAN	MAC Clone	VPN	DMZ	DDNS	Port Forward	Advance	Port Setting	QoS

Please REBOOT to make the changes effective!

Most Nat connections(512-8192)	4096
Mss Mode	<input type="radio"/> Manual <input checked="" type="radio"/> Auto
Mss Value(1260-1460)	1260
AntiDos-P	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP conflict detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detecting Interval(0-3600)	0

Save Cancel Reboot

4.3.9 Port Setting

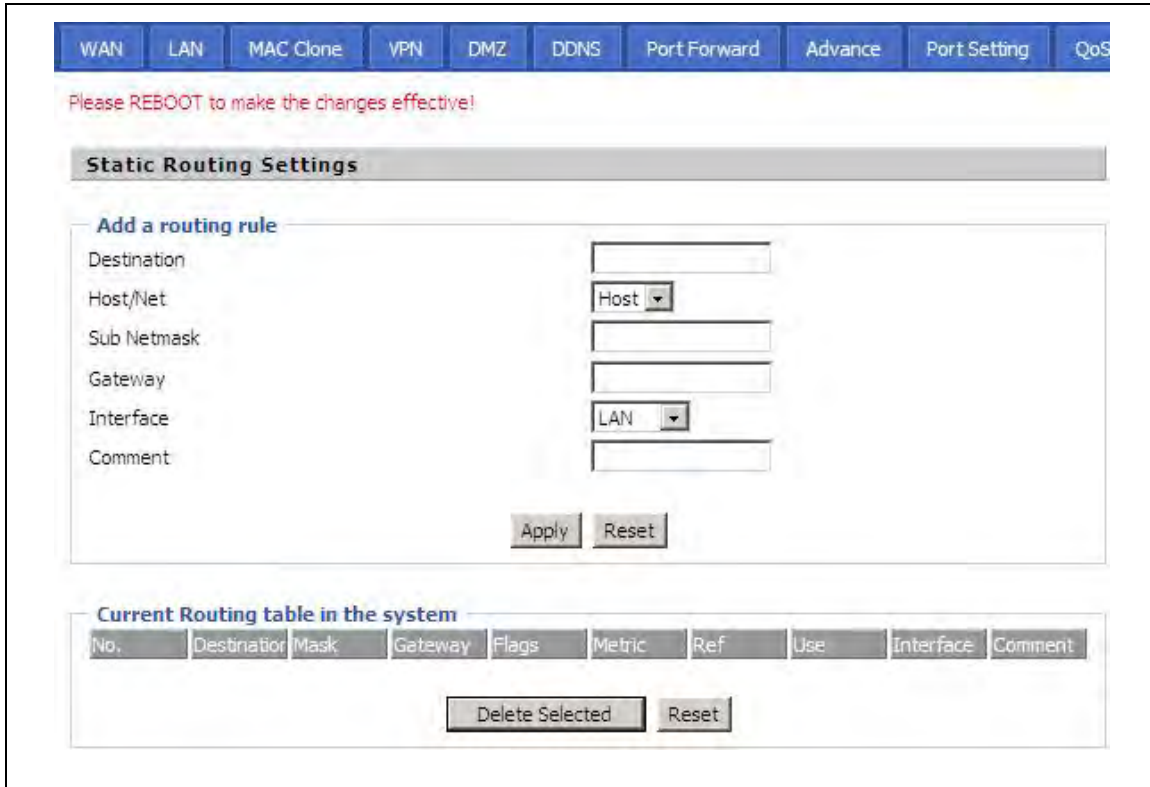
Field Name	Description
WAN Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half-duplex, 10M half and full, select port speed negotiation supported by methods.
LAN1~LAN4Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full, select port speed negotiation methods.

WAN	LAN	MAC Clone	VPN	DMZ	DDNS	Port Forward	Advance	Port Setting	QoS
Please REBOOT to make the changes effective!									
Port Setting									
Port Setting									
WANPort Speed Nego	Auto								
LAN1Port Speed Nego	Auto								
LAN2Port Speed Nego	Auto								
LAN3Port Speed Nego	Auto								
LAN4Port Speed Nego	Auto								

4.3.10 QoS

 <p>The screenshot shows the QoS setting interface. At the top, there are navigation tabs: WAN, LAN, MAC Clone, VPN, DMZ, DDNS, Port Forward, Advance, Port Setting, QoS, and Routing. Below the tabs, a red message says "Please REBOOT to make the changes effective!". The main section is titled "QoS setting" and contains a "QoS setting" sub-section with a "QoS Enable" dropdown menu set to "Disable" and an "Upstream" input field with a "(0-102400)kbps" label. There are "Save" and "Cancel" buttons. Below this is a table with columns for "Condition" and "Action". The "Condition" columns include Name, Src. IP Addr, Dst. IP Addr, Proto, Src. Port, Dst. Port, Phys. Port, DSCP, 802.1, VLAN ID, Rema DSCP, Rema 802.1, and Rema VLAN. The "Action" columns include Priority, Drop, and Rate Limit. There are "Delete Selected" and "Add" buttons at the bottom of the table.</p>	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>QoS Enable</td> <td>If or not enable Qos function</td> </tr> <tr> <td>Upstream</td> <td>Set the upstream bandwidth</td> </tr> <tr> <td>Delete Selected</td> <td>In NO., Check the items you want to delete, click the Delete option</td> </tr> <tr> <td>Add</td> <td>Click Add to add a new parameter</td> </tr> </tbody> </table>	Field Name	Description	QoS Enable	If or not enable Qos function	Upstream	Set the upstream bandwidth	Delete Selected	In NO., Check the items you want to delete, click the Delete option	Add	Click Add to add a new parameter
Field Name	Description										
QoS Enable	If or not enable Qos function										
Upstream	Set the upstream bandwidth										
Delete Selected	In NO., Check the items you want to delete, click the Delete option										
Add	Click Add to add a new parameter										

4.3.11 Routing

 <p>The screenshot shows the Static Routing Settings interface. At the top, there are navigation tabs: WAN, LAN, MAC Clone, VPN, DMZ, DDNS, Port Forward, Advance, Port Setting, and QoS. Below the tabs, a red message says "Please REBOOT to make the changes effective!". The main section is titled "Static Routing Settings" and contains an "Add a routing rule" sub-section with input fields for Destination, Host/Net (dropdown menu set to "Host"), Sub Netmask, Gateway, Interface (dropdown menu set to "LAN"), and Comment. There are "Apply" and "Reset" buttons. Below this is a section titled "Current Routing table in the system" with a table with columns: No., Destination, Mask, Gateway, Flags, Metric, Ref, Use, Interface, and Comment. There are "Delete Selected" and "Reset" buttons at the bottom.</p>	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Destination</td> <td>Destination address</td> </tr> <tr> <td>Host/Net</td> <td>Both Host and Net selection</td> </tr> <tr> <td>Gateway</td> <td>Gateway IP address</td> </tr> <tr> <td>Interface</td> <td>LAN/WAN/Custom three options, and add the corresponding address</td> </tr> <tr> <td>Comment</td> <td>Comment</td> </tr> </tbody> </table>	Field Name	Description	Destination	Destination address	Host/Net	Both Host and Net selection	Gateway	Gateway IP address	Interface	LAN/WAN/Custom three options, and add the corresponding address	Comment	Comment
Field Name	Description												
Destination	Destination address												
Host/Net	Both Host and Net selection												
Gateway	Gateway IP address												
Interface	LAN/WAN/Custom three options, and add the corresponding address												
Comment	Comment												

4.4 Wireless

4.4.1 Basic

Basic Wireless Settings	Field Name	Description
Wireless Network Radio On/Off: Radio On Wireless Connection Mode: AP	Radio on/off	Select “Radio Off” to disable wireless. Select “Radio on” to enable wireless.
Network Mode: 11b/g/n mixed mode SSID: Wireless_AP001118 Multiple SSID1: [] Multiple SSID2: [] Multiple SSID3: [] broadcast(SSID): <input checked="" type="radio"/> Enable <input type="radio"/> Disable AP Isolation: <input type="radio"/> Enable <input checked="" type="radio"/> Disable MBSSID AP Isolation: <input type="radio"/> Enable <input checked="" type="radio"/> Disable BSSID: 00:0C:FE:00:11:18 Frequency (Channel): Auto HT Physical Mode: <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field Operating Mode: <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 Channel BandWidth: <input type="radio"/> Long <input checked="" type="radio"/> Auto MCS: Auto Reverse Direction Grant(RDG): <input type="radio"/> Disable <input checked="" type="radio"/> Enable STBC: <input type="radio"/> Disable <input checked="" type="radio"/> Enable Aggregation MSDU(A-MSDU): <input checked="" type="radio"/> Disable <input type="radio"/> Enable Auto Block ACK: <input type="radio"/> Disable <input checked="" type="radio"/> Enable Decline BA Request: <input checked="" type="radio"/> Disable <input type="radio"/> Enable HT Disallow TKIP: <input type="radio"/> Disable <input checked="" type="radio"/> Enable HT LDPC: <input checked="" type="radio"/> Disable <input type="radio"/> Enable Other: [] HT TxStream: [2] HT RxStream: [2]	Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP Choose one network mode from the drop down list. Default is 11b/g/n mixed mode 11b/g/n mixed mode 11b/g mixed mode 11b only 11g only 11b/g/n mixed mode 11n only(2.4G)
SSID: [] Hidden: <input type="checkbox"/> Isolated: <input type="checkbox"/> Max Client: [16]	SSID	It is the basic identity of wireless LAN. SSID can be any alphanumeric or a combination of special characters. It will appear in the wireless network access list.
Multiple SSID1: [] Hidden: <input type="checkbox"/> Isolated: <input type="checkbox"/> Max Client: [16]	Multiple SSID1~SSID3	G902 supports multiple SSIDs.
Multiple SSID2: [] Hidden: <input type="checkbox"/> Isolated: <input type="checkbox"/> Max Client: [16]	Hidden	After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list
Multiple SSID3: [] Hidden: <input type="checkbox"/> Isolated: <input type="checkbox"/> Max Client: [16]	Broadcast(SSID)	After initial State opening, the device broadcasts the SSID of the router to wireless network
broadcast(SSID): <input checked="" type="radio"/> Enable <input type="radio"/> Disable	AP Isolation	If AP isolation is enabled, the clients of the AP cannot access each other.
AP Isolation: <input type="radio"/> Enable <input checked="" type="radio"/> Disable MBSSID AP Isolation: <input type="radio"/> Enable <input checked="" type="radio"/> Disable Save Cancel Reboot	MBSSID AP Isolation	AP isolation among the devices which are not belong to this AP and along to, when the option is enabled, the devices which do not belong to this AP cannot access the devices which are

		within the AP.
	BSSID	A group of wireless stations and a WLAN access point (AP) consists of a basic access device (BSS), each computer in the BSS must be configured with the same BSSID, that is, the wireless AP logo.
	Frequency (Channel)	You can select Auto Select and channel 1/2/3/4/5/6/7/8/9/10/11.
	HT Physical Mode Operating Mode	<ol style="list-style-type: none"> 1. Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 2. Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system
	Channel Bandwidth	Select channel bandwidth, default is 20MHz and 20/40MHz.
	Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval
	MCS	Position control signal, options are 0 to 32, the default is automatic
	Reverse Direction (RDG)	You can choose to enable or disable this privilege

4.4.2 Wireless Security

Field Name	Description
SSID Choice	Choose one SSID from SSID, Multiple SSID1, Multiple SSID2 and Multiple SSID3.

Please REBOOT to make the changes effective!

WIFI Security Setting

Select SSID

SSID choice: Wireless_AP001118

"Wireless_AP001118"

Security Mode: WPA-PSK

WPA Algorithms: TKIP AES TKIPAES

Pass Phrase: 23123123

Key Renewal Interval: 3600 Second in Month (0 ~ 4194303)

Access policy: Policy: Disable

Add a station MAC:

	Security Mode	<p>Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.</p> <p>Each encryption mode will bring out different web page and ask you to offer additional configuration.</p>
--	----------------------	--

Select a different encryption mode, the web interface will be different, user can configure the corresponding parameters under the mode you select. Here are some common encryption method:

1. OPENWEP: A handshake way of WEP encryption, encryption via the WEP key:

WIFI Security Setting	Field Name	Description												
<p>Select SSID</p> <p>SSID choice: Wireless_AP001118</p> <p>Security Mode: OPENWEP</p> <p>Wire Equivalence Protection (WEP)</p> <p>Default Key: WEP Key 1</p> <p>WEP Keys:</p> <table border="0"> <tr> <td>WEP Key 1</td> <td><input type="text"/></td> <td>Hex</td> </tr> <tr> <td>WEP Key 2</td> <td><input type="text"/></td> <td>Hex</td> </tr> <tr> <td>WEP Key 3</td> <td><input type="text"/></td> <td>Hex</td> </tr> <tr> <td>WEP Key 4</td> <td><input type="text"/></td> <td>Hex</td> </tr> </table>	WEP Key 1	<input type="text"/>	Hex	WEP Key 2	<input type="text"/>	Hex	WEP Key 3	<input type="text"/>	Hex	WEP Key 4	<input type="text"/>	Hex	Security Mode	This is used to select one of the 4 WEP keys, key settings on the clients should be the same with this when connecting.
WEP Key 1	<input type="text"/>	Hex												
WEP Key 2	<input type="text"/>	Hex												
WEP Key 3	<input type="text"/>	Hex												
WEP Key 4	<input type="text"/>	Hex												
	WEP Keys	Set the WEP key. A-64 key need 10 Hex characters or 5 ASCII characters; choose A-128 key need 26 Hex characters or 13 ASCII characters.												
		WEP represents Wired Equivalent Privacy, which is a basic encryption method.												

2. WPA-PSK, the router will use WPA way which is based on the shared key-based mode:

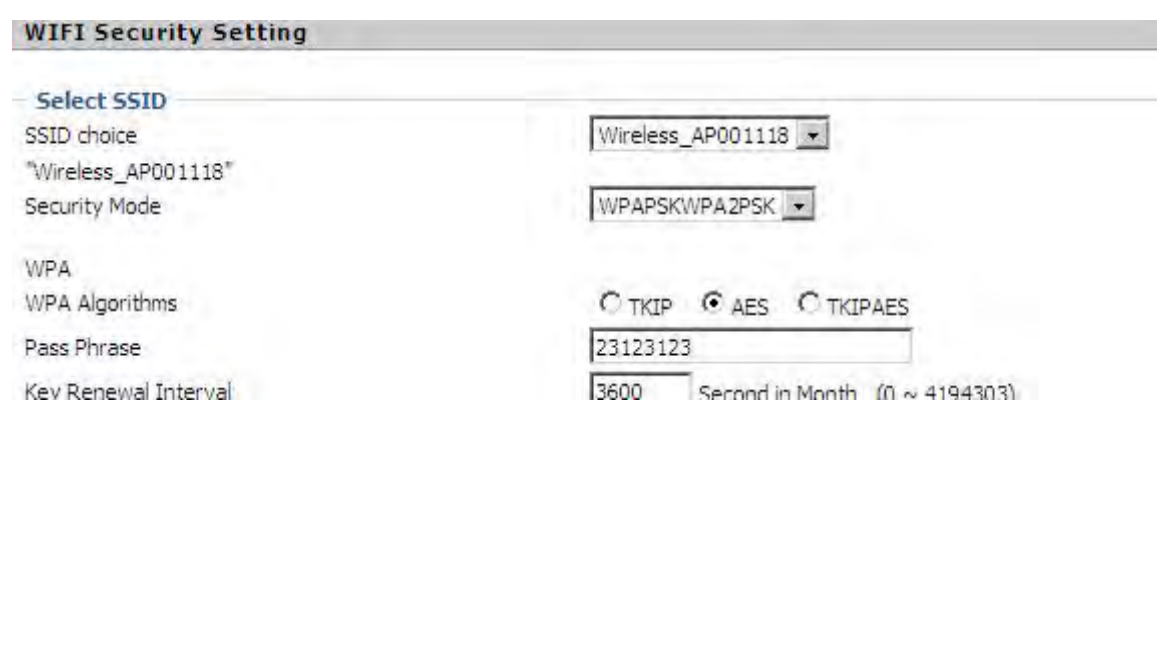
WIFI Security Setting	Field Name	Description
<p>Select SSID</p> <p>SSID choice: Wireless_AP001118</p> <p>Security Mode: WPA-PSK</p> <p>WPA Algorithms: <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES</p> <p>Pass Phrase: 23123123</p> <p>Key Renewal Interval: 3600 Second in Month (0 ~ 4194303)</p>	WPA Algorithms	This item is used to select the encryption of wireless dhome gateway algorithms, options are TKIP, AES and TKIPAES.
	Pass Phrase	Setting up WPA-PSK security password.
	Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.

3. WPA2-PSK, the router will be based on shared key WPA2 modes:

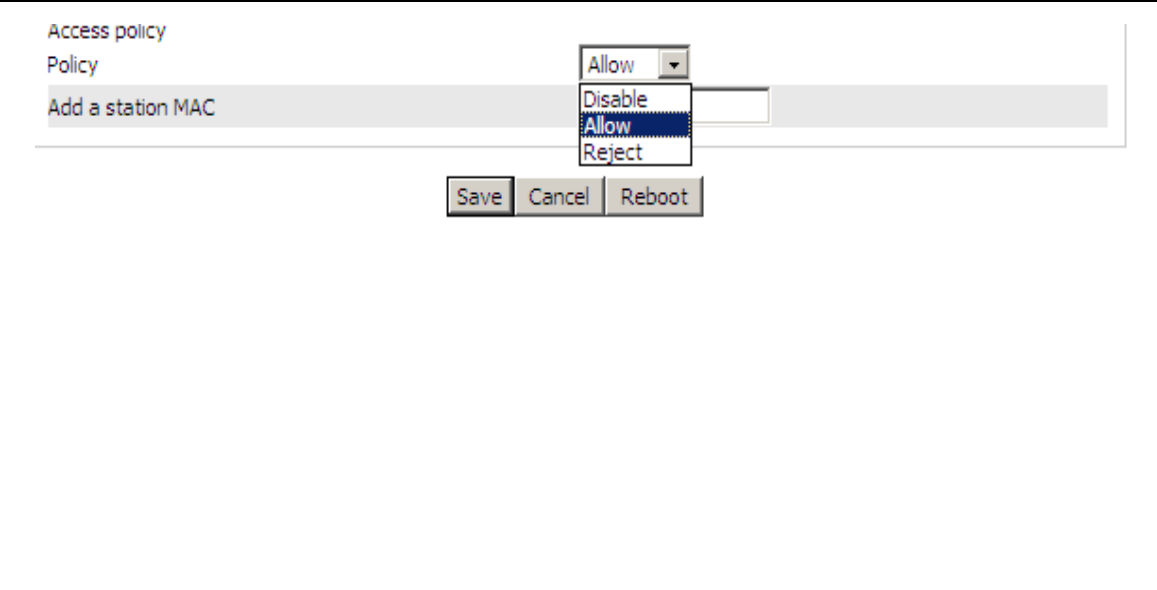
WIFI Security Setting	Field Name	Description
<p>Select SSID</p> <p>SSID choice: Wireless_AP001118</p> <p>Security Mode: WPA2-PSK</p> <p>WPA Algorithms: <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES</p> <p>Pass Phrase: 23123123</p>		

	WPA Algorithms	This item is used to select the security algorithm for encryption of wireless dhome gateway, options are TKIP, AES, TKIPAES three
	Pass phrase	Setting up WPA2-PSK security password
	Key Renewal Interval	Set the key scheduled update cycle, default is 3600s

4. WPAPSKWPA2PSK manner is consistent with WPA2PSK settings

Field Name	Description
	<p>The dhome gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms.</p>
Pass Phrase	Set WPA-PSK/WPA2-PSK security code
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s
<p>WPA-PSK/WPA2-PSK WPA/WPA2 security type is actually a simplified version, which is based on the WPA shared key mode, higher security setting is also relatively simple, suitable for ordinary home users and small businesses.</p>	

5. Wireless Access Policy:

Field Name	Description
	<p>Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address.</p>
Policy	Prohibition: disable wireless access control policy; allow: only allow the clients in the list to access, rejected: block the clients in the list to access.
Add a station MAC	Enter the MAC address of the clients which you want to allow or prohibit
<p>Example: Prohibit the device whose wireless network card MAC address is 00:1F: D0: 62: BA: FF's to access the wireless network, and allow other</p>	

computers to access the network.

Implementation: As shown, the Policy is Reject, add 00:1F: D0: 62: BA: FF to the MAC, click Save and reboot the device settings to take effect.

4.4.3 WMM

Status Network **Wireless** Wireless 5G SIP FXS1 FXS2 Security Application

Basic Wireless Security **WMM** WDS WPS Station Info Advanced

Please REBOOT to make the changes effective!

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Apply Cancel Close

WMM (Wi-Fi MultiMedia) is the QoS certificate of Wi-Fi Alliance (WFA). This provides you to configure the parameters of wireless multimedia; WMM allows wireless communication to define a priority according to the dhome gateway type. To make WMM effective, the wireless clients must also support WMM.

4.4.4 WDS

<div style="background-color: #4a7ebb; color: white; padding: 2px;"> Basic Wireless Security WMM WDS WPS Station Info Advanced </div> <p style="color: red; font-size: small;">Please REBOOT to make the changes effective!</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>WPS Config</p> <p>WPS Config</p> <p>Wireless Distribution System(WDS)</p> <p>WDS Mode Disable ▾</p> <p style="text-align: center; margin-top: 10px;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/> </p> </div>	<p>If or not enable WDS mode</p>
---	----------------------------------

4.4.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

WPS Setting	Field Name	Description
<p>WPS Config</p> <p>WPS <input type="button" value="Enable"/> <input type="button" value="Apply"/></p>	WPS Setting	If or not enable WPS function
<p>WPS Summary</p> <p>WPS Current Status: Idle WPS Configured: Yes WPS SSID: Wireless_AP001118 WPS Auth Mode: WPA-PSK WPS Encryp Type: AES WPS Default Key Index: 2 WPS Key(ASCII): 23123123 AP PIN: 00043762 <input type="button" value="Generate"/></p> <p><input type="button" value="Reset OOB"/></p>	WPS Summary	Display the current status of WPS, including current state, SSSID name, authentication methods, encryption type and the PIN code of this AP.
<p>WPS Progress</p> <p>WPS Mode: <input checked="" type="radio"/> PIN <input type="radio"/> PBC</p> <p>PIN: <input type="text"/></p> <p><input type="button" value="Apply"/></p>	Generate	Generate a new PIN code
<p>WPS Status</p> <p>WSC: Idle</p> <p><input type="button" value="Cancel"/></p>	Reset OOB	G902 uses default security policy to allow other non-WPS users to access and apply.
	WPS Mode	<p>PIN: Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then G902 begins to send signals, turn on the PIN accessing method on the clients, and then it can access the wireless AP automatically.</p> <p>PBC: There are two ways to start PCB mode, user can press the PCB button directly on the device, or select PCB mode on the software and apply. Users can activate WPS connection in WPS mode through these two methods, only when the clients choose PCB access, the clients can connect the AP automatically.</p>
	WPS Status	<p>WPS shows status in three ways:</p> <p>WSC: Idle</p> <p>WSC: Start WSC Process(begin to send messages)</p> <p>WSC: Success; this means clients have accessed the AP successfully, WPS connects well.</p>

4.4.6 Station Info

 <p>Please REBOOT to make the changes effective!</p> <p>Wireless Status</p> <p>Wireless Status Current Channel: Channel 8</p> <p>Wireless Network</p> <p>Wireless Network MAC Address Aid PSM MimoPS MCS BW SGI STBC</p>	<p>This page shows user the clients' information which connects to the AP.</p>
--	--

4.4.7 Advanced

Advanced Wireless	Field Name	Description
BG Protection Mode: <input type="text" value="Auto"/>	BG Protection Mode	Select G protection mode, options are on, off and automatic.
Beacon Interval: <input type="text" value="100"/> ms (range 20 - 999, default 100)	Beacon Interval	The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.
Data Beacon Rate (DTIM): <input type="text" value="3"/> ms (range 1 - 255, default 3)	Data Beacon Rate(DTIM)	Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive broadcast multi-cast.
Fragment Threshold: <input type="text" value="2346"/> (range 256 - 2346, default 2346)	Fragment Threshold	Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet will be divided into multiple packets.
RTS Threshold: <input type="text" value="2347"/> (range 1 - 2347, default 2347)	RTS Threshold	Specify the packet RTS threshold, when the packet exceeds this value, the router will send RTS to the destination site consultation
TX Power: <input type="text" value="100"/> (range 1 - 100, default 100)	TX Power	Define the transmission power of the current AP, the greater it is, the stronger the signal is.
Short Preamble: <input checked="" type="radio"/> Enable <input type="radio"/> Disable	Short Preamble	Default is enable, G902 system is not compatible with traditional IEEE802.11, the operation rate can be 1,2Mpbs

	Short Slot	If or not enable short slot, default is enable, it is helpful in improving the transmission rate of wireless communication.
	Tx Burst	One of the features of MAC layer, it is used to improve the fairness for transmitting TCP.
	Pkt_Aggregate	It is a mechanism that is used to enhance the LAN, in order to ensure that the dhome gateway packets are sent to the destination correctly.
	IEEE802.11H support	If or not enable IEEE802.11H Support, default is disable.
	Country Code	Select country code, options are CN, US, JP, FR, TW, IE, HK and NONE.
	Wi-Fi Multimedia(WMM)	
	WMM Capable	If or not enable WMM. WMM take effects when it is enabled.
	APSD Capable	After enable this, it may affect wireless performance, but can play a role in energy-saving power
	WMM Parameters	Press <input type="button" value="WMM Configuration"/> , the webpage will jump to the configuration page of Wi-Fi multimedia.
	Multicast-to-Unicast Converter	
	Multicast-to-Unicast	If or not enable Multicast-to-Unicast, by default, it is disabled, you can enable it.

4.5 Wireless 5G

4.5.1 Basic

Basic Wireless Settings	Field Name	Description
<p>Wireless Network</p> <p>Radio On/Off <input type="radio"/> Radio On</p> <p>Network Mode <input type="text" value="11vht AC/AN/A"/></p> <p>SSID <input type="text" value="Wireless_AP_5G"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/></p> <p>Multiple SSID1 <input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/></p> <p>Multiple SSID2 <input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/></p> <p>Multiple SSID3 <input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/></p> <p>broadcast(SSID) <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>AP Isolation <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>MBSSID AP Isolation <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>BSSID <input type="text" value="00:0C:FE:00:11:20"/></p> <p>Frequency (Channel) <input type="text" value="5220MHz (Channel 44)"/></p> <p>HT Physical Mode</p> <p>Operating Mode <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field</p> <p>Channel BandWidth <input type="radio"/> 20 <input checked="" type="radio"/> 20/40</p> <p>Guard Interval <input type="radio"/> Long <input checked="" type="radio"/> Auto</p> <p>MCS <input type="text" value="Auto"/></p> <p>Reverse Direction Grant(RDG) <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Extension Channel <input type="text" value="5240MHz (Channel 48)"/></p> <p>STBC <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Aggregation MSDU(A-MSDU) <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Auto Block ACK <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Decline BA Request <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>HT Disallow TKIP <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>20/40 Coexistence <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>HT LDPC <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>VHT Option</p> <p>VHT BandWidth <input checked="" type="radio"/> 20/40 <input type="radio"/> 80</p> <p>VHT STBC <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>VHT Short GI <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>VHT BW Signaling <input checked="" type="radio"/> Disable <input type="radio"/> Static <input type="radio"/> Dynamic</p> <p>VHT LDPC <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>Other</p> <p>HT TxStream <input type="text" value="2"/></p> <p>HT RxStream <input type="text" value="2"/></p>	<p>Radio on/off</p>	<p>Select “Radio Off” to disable wireless.</p> <p>Select “Radio on”to enable wireless.</p>
	<p>Network Mode</p>	<p>Choose one network mode from the drop down</p> <p><input type="text" value="11a/n mixed mode"/></p> <p>11b/g mixed mode</p> <p>11b only</p> <p>11g only</p> <p>11b/g/n mixed mode</p> <p>11a only</p> <p>11a/n mixed mode</p> <p>11vht AC/AN/A</p> <p>11vht AC/AN</p> <p>list</p>
	<p>SSID</p>	<p>It is the basic identity of wireless LAN. SSID can be any alphanumeric or a combination of special characters. It will appear in the wireless network access list.</p>
	<p>Multiple SSID1~SSID3</p>	<p>G902 supports multiple SSIDs.</p>
	<p>Hidden</p>	<p>After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list</p>
	<p>Broadcast(SSID)</p>	<p>After initial State opening, the device broadcasts the SSID of the router to wireless network</p>
	<p>AP Isolation</p>	<p>If AP isolation is enabled, the clients of the AP cannot access each other.</p>
	<p>MBSSID AP Isolation</p>	<p>AP isolation among the devices which are not belong to this AP and along to, when the option is enabled, the devices which do not belong to this AP cannot access the devices which are within the AP.</p>

	BSSID	A group of wireless stations and a WLAN access point (AP) consists of a basic access device (BSS), each computer in the BSS must be configured with the same BSSID, that is, the wireless AP logo.
	Frequency (Channel)	You can select Auto Select and channel 1/2/3/4/5/6/7/8/9/10/11.
	HT Physical Mode Operating Mode	<ol style="list-style-type: none"> 1. Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 2. Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system
	Channel Bandwidth	Select channel bandwidth, default is 20MHz and 20/40MHz.
	Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval
	MCS	Position control signal, options are 0 to 32, the default is automatic
	Reverse Direction (RDG)	You can choose to enable or disable this privilege
	STBC	
	VHT Bandwidth	
	VHT STBC	
	VHT Short GI	
	VHT BW Signaling	
	VHT LDPC	

4.5.2 Wireless Security

Field Name	Description
SSID Choice	Choose one SSID from SSID, Multiple SSID1, Multiple SSID2 and Multiple SSID3.
Security Mode	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets. Each encryption mode will bring out different web page and ask you to offer additional configuration.

Select a different encryption mode, the web interface will be different, user can configure the corresponding parameters under the mode you select. Please refer to 4.4.2 section.

4.5.3 WMM

Please refer to 4.4.3 section.

4.5.4 WDS

Please refer to 4.4.4 section

4.5.5 WPS

Please refer to 4.4.5 section.

4.5.6 Station Info

Please refer to 4.4.6 section.

4.5.7 Advanced

Please refer to 4.4.7 section.

4.6 SIP

4.6.1 SIP Settings

Status	Network	Wireless	Wireless 5G	SIP	FXS1	FXS2	Security	Applicat
SIP Settings VoIP QoS								
Please REBOOT to make the changes effective!								
SIP Parameters								
SIP Parameters								
SIP T1	500	MS	Max Forward	70				
SIP Reg User Agent Name			Max Auth	2				
Mark All AVT Packets	Enable		RFC 2543 Call Hold	Enable				
SRTP	Disable		SRTP Prefer Encryption	AES_CM				
Service Type	Common							
NAT Traversal								
NAT Traversal								
NAT Traversal	Disable		STUN Server Address					
NAT Refresh Interval(sec)	60		STUN Server Port	3478				

Field Name	Description
SIP T1	The minimum scale of retransmission time
Max Forward	Sip packets Max Forward message header fields used to limit the request which jump in his destination . To limit the number that forwarding a request to the proxy or gateway of next node intermediate.
SIP Reg User Agent Name	The agent name of SIP registered user
Max Auth	The maximum number of retransmissions
Mark All AVT Packets	Voice packet marking,to enable this item will see the mark on the voice message when the call environment changed (such as press a key during the call)
RFC 2543 Call Hold	Enable,the Connection Information field displays the address is 0.0.0.0 in the invite message of Hold. Disable,the Connection Information field displays the device ip address in the invite message of Hold.
SRTP	Whether to enable the call packet encryption function
SRTP Prefer Encryption	The preferred encryption type of calling packet (the Message body of INVITE Message)
Service Type	Choose the server type
NAT Traversal	1. If or not enable NAT Traversal 2. G902 supports STUN Traversal; If you want to traverse NAT/Firewall, select the STUN.

	STUN Server Address	Add the correct STUN service provider IP address.
	NAT Refresh Interval	Set NAT Refresh Interval, default is 60s.
	STUN Server Port	Set STUN Server Port, default is 5060.

4.6.2 VoIP Qos

QoS Settings	Field Name	Description
<p>Layer 3 QoS</p> <p>SIP QoS(0-63) <input type="text" value="0"/></p> <p>RTP QoS(0-63) <input type="text" value="0"/></p>	SIP /RTP QoS	The default value is 0,you can set a range of values is 0~63

4.7 FXS1

4.7.1 SIP Account

1. Basic

Set the basic information provided by your VOIP Service Provider, such as Phone Number, Account, password, SIP Proxy and so on.

Basic	Field Name	Description
Basic Setup Line Enable <input type="text" value="Enable"/> Peer To Peer <input type="text" value="Disable"/>	Line Enable	If or not enable the line.
Proxy and Registration Proxy Server <input type="text" value="192.168.10.208"/> Proxy Port <input type="text" value="5060"/> Outbound Server <input type="text"/> Outbound Port <input type="text" value="5060"/> Backup Outbound Server <input type="text"/> Backup Outbound Port <input type="text" value="5060"/>	Peer To Peer	If or not enable PEER to PEER. If enable, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dialed line1.
Subscriber Information Display Name <input type="text" value="11"/> Phone Number <input type="text" value="11"/> Account <input type="text" value="11"/> Password <input type="text" value="••"/>	Proxy Server	The IP address or the domain of SIP Server
	Outbound Server	The IP address or the domain of Outbound Server
	Backup Outbound Server	The IP address or the domain of Backup Outbound Server
	Proxy port	SIP Service port, default is 5060
	Outbound Port	Outbound Proxy's Service port, default is 5060
	Backup Outbound Port	Backup Outbound Proxy's Service port, default is 5060
	Display Name	The number will be displayed on LCD
	Phone Number	Enter telephone number provided by SIP Proxy
	Account	Enter SIP account provided by SIP Proxy
	Password	Enter SIP password provided by SIP Proxy

2. Audio Configuration

Field Name	Description
Audio Codec Type1	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type2	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type3	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type4	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type5	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
G.723 Coding Speed	Choose the speed of G.723 from 5.3kbps and 6.3kbps
Packet Cycle	The RTP packet cycle time, default is 20ms
Silence Supp	If or not enable silence
Echo Cancel	If or not enable echo cancel, default is enable
Auto Gain Control	If or not enable auto gain.
T.38 Enable	If or not enable T.38
T.38 Redundancy	If or not enable T.38 Redundancy
T.38 CNG Detect Enable	If or not enable T.38 CNG Detect
gmd attribute Enable	If or not enable gmd attribute.

3. Supplementary Service Subscription

Supplementary Service Subscription	Field Name	Description
<p>Supplementary Services</p> <p>Call Waiting <input type="button" value="Enable"/> Hot Line <input type="text"/></p> <p>MWI Enable <input type="button" value="Enable"/> Voice Mailbox Numbers <input type="text"/></p> <p>MWI Subscribe Enable <input type="button" value="Disable"/> VMWI Serv <input type="button" value="Enable"/></p> <p>DND <input type="button" value="Disable"/></p>	Call Waiting	If or not enable Call Waiting
	Hot Line	Fill in the hotline number. Pickup handset or press handsfree/headset button, the device will dial out the hotline number automatically.
	MWI Enable	If or not enable MWI (message waiting indicate). If the user needs to user voice mail, please enable this feature.
	MWI Subscribe Enable	If or not enable MWI Subscribe
	Voice Mailbox Numbers	Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice mail is *97
	VMWI Serv	If or not enable VMWI service.
	DND	If or not enable DND (do not disturb). If enable, any phone call cannot arrive at the device; default is disable.
<p>Speed Dial</p> <p>Speed Dial 2 <input type="text"/> Speed Dial 3 <input type="text"/></p> <p>Speed Dial 4 <input type="text"/> Speed Dial 5 <input type="text"/></p> <p>Speed Dial 6 <input type="text"/> Speed Dial 7 <input type="text"/></p> <p>Speed Dial 8 <input type="text"/> Speed Dial 9 <input type="text"/></p>	Speed Dial	Enter the speed dial phone numbers. Dial *74 to active speed dial function. Then press the speed dial numbers, for example, press 2, phone will dial 075526099365 directly.

4. Advanced

Advanced		Field Name	Description
Advanced Setup Domain Name Type: Enable Signal Port: 5060 RFC2833 Payload(>=96): 101 RTP Port: 0 (=0 auto select) Session Refresh Time(sec): 0 Prack Enable: Disable Primary SER Detect Interval: 0 Keep-alive Interval(10-60s): 15 Anonymous Call Block: Disable Use OB Proxy In Dialog: Disable Dial Prefix: <input type="text"/> Hold Method: ReINVITE Only Recv Request From Server: Disable SIP Received Detection: Disable Country Code: <input type="text"/> Caller ID Header: FROM			
Carry Port Information: Disable DTMF Type: RFC2833 Register Refresh Interval(sec): 3600 Cancel Message Enable: Disable Refresher: UAC SIP OPTIONS Enable: Disable Max Detect Fail Count: 3 Anonymous Call: Disable Proxy DNS Type: A Type Reg Subscribe Enable: Disable User Type: IP Request-URI User Check: Disable Server Address: <input type="text"/> VPN: Disable Remove Country Code: Disable			
	Domain Name Type	If or not use domain name in the SIP URI.	
	Carry Port Information	If or not carry port information in the SIP URI.	
	Signal Port	The local port of SIP protocol, default is 5060.	
	DTMF Type	Choose the DTMF type from Inbound, RFC2833 and SIP INFO.	
	RFC2833 Payload(>=96)	User can use the default setting.	
	Register Refresh Interval	The interval between two normal Register messages. You can use the default setting.	
	RTP Port	Set the port to send RTP. The device will select one idle port for RTP if you set "0"; otherwise use the value which user sets.	
	Cancel Message Enable	When you set enable, an unregistered message will be sent before registration, while you set disable, unregistered message will not be sent before registration. You should set the option for different Proxy.	
	Session Refresh Time(sec)	Time interval between two sessions, you can use the default settings.	
	Refresher	Choose refresher from UAC and UAS.	
	Prack Enable	If or not enable prack.	
	SIP OPTIONS Enable	When you set enable, the device will send SIP-OPTION to the server, instead of sending periodic Hello message. The sending interval is Keep-alive interval.	
	Primary SER Detect Interval	Test interval of the primary server, the default value is 0, it represents disable.	
	Max Detect Fail Count	Interval of detection of the primary server fail; the default value is 3, it means that if detect 3	

	times fail; the device will no longer detect the primary server.
Keep-alive Interval(10-60s)	The interval that the device will send an empty packet to proxy.
Anonymous Call	If or not enable anonymous call.
Anonymous Call Block	If or not enable anonymous call block.
Proxy DNS Type	Set the DNS server type, choose from A type and DNS SRV.
Use OB Proxy In Dialog	If or not use OB Proxy In Dialog.
Reg Subscribe Enable	If enable, subscribing will be sent after registration message, if not enable, do not send subscription.
Dial Prefix	The number will be added before your telephone number when making calls.
User Type	Choose the User Type from IP and Phone.
Hold Method	Choose the Hold Method from ReINVITE and INFO.
Request-URI User Check	If or not enable the user request URI check.
Only Recv request from server	If or not enable the only receive request from server.
Server Address	The IP address of SIP server.
SIP Received Detection	If or not enable SIP Received Detection, if enable, use it to confirm the public network address of the device.

4.7.2 Preferences

1. Volume Settings

Preferences	Field Name	Description
<p>Volume Settings</p> <p>Handset Input Gain <input type="text" value="5"/> Handset Volume <input type="text" value="5"/></p>	Handset Input Gain	Adjust the handset input gain from 0 to 7.
	Handset Volume	Adjust the output gain from 0 to 7.

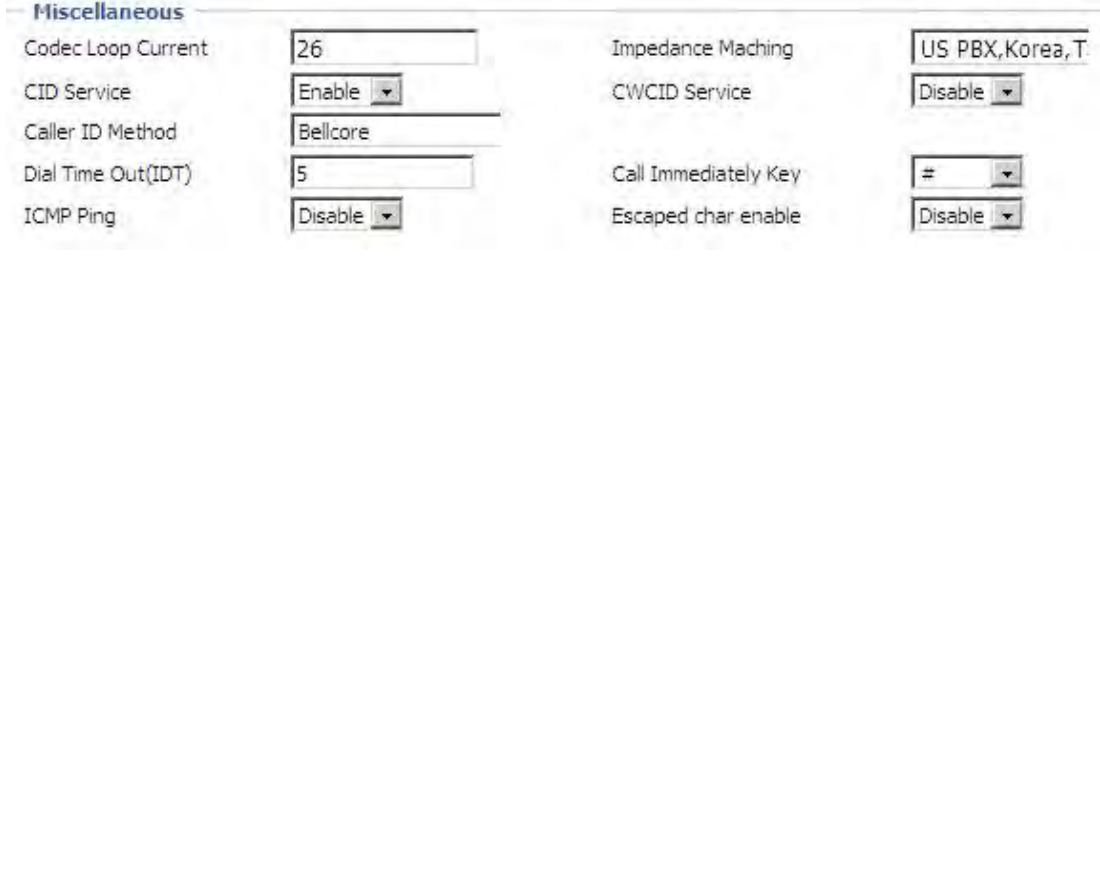
2. Regional

Field Name	Description
Tone Type	Choose tone type form China, US, Hong Kong and so on.
Dial Tone	Dial Tone
Busy Tone	Busy Tone
Off Hook Warning Tone	Off Hook warning tone
Ring Back Tone	Ring back tone
Call Waiting Tone	Call waiting tone
Min Jitter Delay	The Min value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Max Jitter Delay	The Max value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Ringing Time	How long G902 will ring when there is an incoming call.
Ring Waveform	Select regional ring waveform, options are Sinusoid and Trapezoid, the default Sinusoid.
Ring Voltage	Set ringing voltage, the default value is 70
Ring Frequency	Set ring frequency, the default value is 25
VMWI Ring Splash Len(sec)	Set the VMWI ring splash length, default is 0.5s.
Flash Time Max(sec)	Set the Max value of the device's flash time, the default value is 0.9
Flash Time Min(sec)	Set the Min value of the device's flash time, the default value is 0.1

3. Features and Call Forward

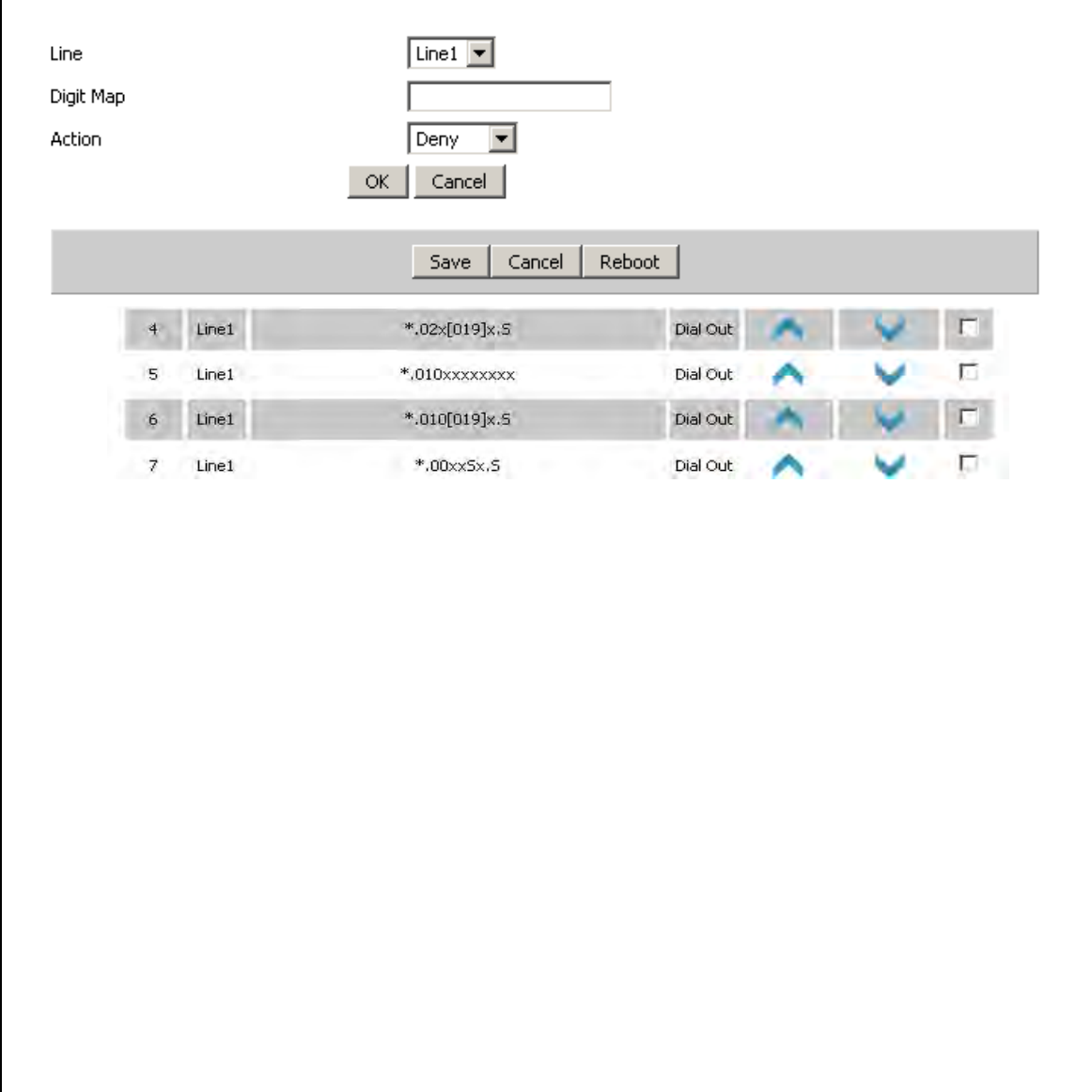
		Field Name	Description
Features All Forward <input type="text" value="Disable"/> Busy Forward <input type="text" value="Disable"/> No Answer Forward <input type="text" value="Disable"/>	Features	All Forward	If or not enable forward all calls
		Busy Forward	If or not enable busy forward.
		No Answer Forward	If or not enable no answer forward.
Call Forward All Forward <input type="text"/> No Answer Forward <input type="text"/> Busy Forward <input type="text"/> No Answer Timeout <input type="text" value="20"/>	Call Forward	All Forward	Set the target phone number for all forward. The device will forward all calls to the phone number immediately when there is an incoming call.
		Busy Forward	The phone number which the calls will be forwarded to when line is busy.
		No Answer Forward	The phone number which the call will be forwarded to when there's no answer.
		No Answer Timeout	The seconds to delay forwarding calls, if there is no answer at your phone.
Feature Code Hold Key Code <input type="text" value="*77"/> Conference Key Code <input type="text" value="*88"/> Transfer Key Code <input type="text" value="*98"/> IVR Key Code <input type="text" value="****"/> R Key Enable <input type="text" value="Disable"/> R Key Cancel Code <input type="text" value="R1"/> R Key Hold Code <input type="text" value="R2"/> R Key Transfer Code <input type="text" value="R4"/> R Key Conference Code <input type="text" value="R3"/> Speed Dial Code <input type="text" value="*74"/>	Feature Code	Hold key code	Call hold signatures, default is *77.
		Conference key code	Signature of the tripartite session, default is *88.
		Transfer key code	Call forwarding signatures ,default is *98.
		IVR key code	Signatures of the voice menu, default is ****.
		R key enable	If or not enable R key way call features.
		R key cancel code	Set the R key cancel code, option are ranged from R1 to R9, default value is R1.
		R key hold code	Set the R key hold code, options are ranged from R1 to R9, default value is R2.
		R key transfer code	Set the R key transfer code, options are ranged from R1 to R9, default value is R4.
		R key conference code	Set the R key conference code, options are ranged from R1 to R9, default value is R3.
	Speed Dial Code	Speed dial code, default is *74.	

4. Miscellaneous

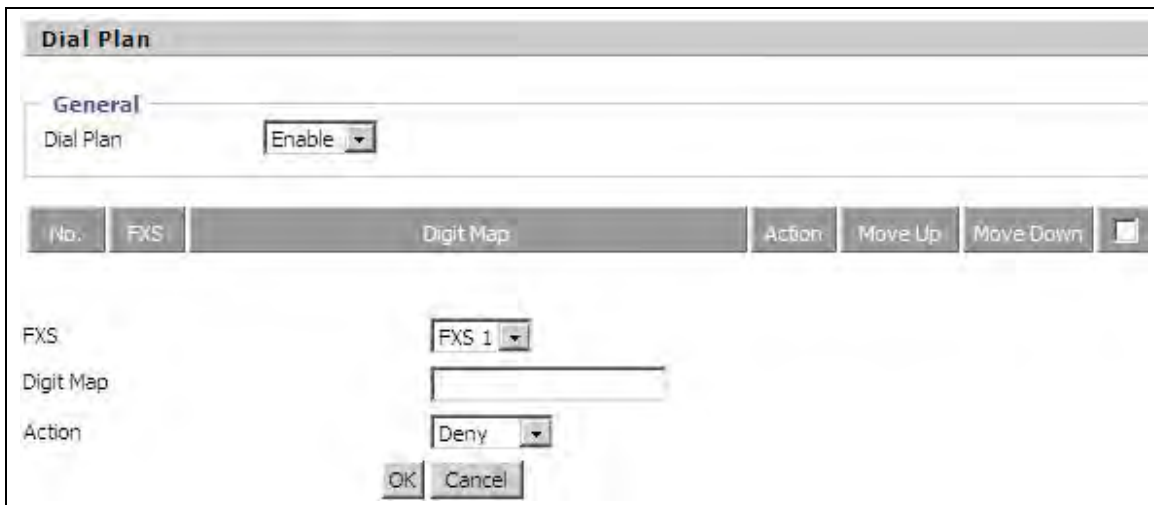
	Field Name	Description
Codec Loop Current: 26	Codec Loop Current	Set off-hook loop current, default is 26
Impedance Maching: US PBX,Korea, T	Impedance Maching	Set impedance matching, default is US PBX,Korea,Taiwan(600).
CID Service: Enable	CID service	If or not enable displaying caller ID; If enable, caller ID is displayed when there is an incoming call or it won't be displayed. Default is enable.
CWCID Service: Disable	CWCID Service	If or not enable CWCID. If enable, the device will display the waiting call's caller ID, or it won't display. Default is disable.
Caller ID Method: Bellcore	Dial Time Out	How long G902 will sound dial out tone when G902 dials a number.
Dial Time Out(IDT): 5	Call Immediately Key	Choose call immediately key form * or #.
ICMP Ping: Disable	ICMP Ping	If or not enable ICMP Ping. If enable this option, home gateway will ping the SIP Server every interval time, otherwise, It will send "hello" empty packet to the SIP Server.
Call Immediately Key: #	Escaped char enable	Open special character translation function; if enable, when you press the # key, it will be translated to 23%, when disable, it is just #

4.7.3 Dial Plan

1. Parameters and Settings

	Field Name	Description
	Dial Plan	If or not enable dial plan.
	Line	Set the line.
	Digit Map	Fill in the sequence used to match input number The syntactic, please refer to the following Dial Plan Syntactic
	Action	Choose the dial plan mode from Deny and Dial Out. Deny means G902 will reject the matched number, while Dial Out means G902 will dial out the matched number.
	Move Up	Press it to move up.
	Move Down	Press it to move down.

2. Adding one dial plan:

	<p>Step 1. Enable Dial Plan</p> <p>Step 2. Click Add button, and the configuration table</p> <p>Step 3. Fill in the value of parameters.</p> <p>Step 4. Press OK button to end configuration.</p> <p>Step 5. Press Save button to save changes</p>
--	---

3. Dial Plan Syntactic

No.	String	Description
1	0 1 2 3 4 5 6 7 8 9 * #	Legal characters
2	x	Lowercase letter x stands for one legal character
3	[sequence]	To match one character form sequence. For example: 6. [0-9]: match one digit form 0 to 9 7. [23-5*]: match one character from 2 or 3 or 4 or 5 or *
4	x.	Match to $x^0, x^1, x^2, x^3, \dots, x^n$ For example: "01.":can match "0", "01", "011", "0111",, "01111..."
5	<dialed:substituted>	Replace dialed with substituted. For example: <8:1650>123456: input is "85551212", output is"16505551212"
6	x,y	Make outside dial tone after dialing "x", stop until dialing character "y" For example: "9,1xxxxxxxxx":the device reports dial tone after inputting "9", stops tone until inputting "1" "9,8,010x": make outside dial tone after inputting "9", stop tone until inputting "0"
7	T	Set the delayed time. For example: "<9:111>T2": The device will dial out the matched number "111" after 2 seconds.

4.7.4 Blacklist

In this page, user can upload or download blacklist file, and can add or delete or edit blacklist one by one.

<p>Blacklist Upload && Download</p> <p>Blacklist Upload && Download</p> <p>Local File <input type="text"/> <input type="button" value="浏览..."/></p> <p><input type="button" value="Upload CSV"/> <input type="button" value="Download CSV"/></p>	<p>Click <input type="button" value="浏览..."/> to select the blacklist file and click <input type="button" value="upload CSV"/> to upload it to G902; Click <input type="button" value="download CSV"/> to save the blacklist file to your local computer.</p>												
<p>Blacklist</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Name</th> <th>Number</th> <th><input type="checkbox"/></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Rob</td> <td>12345</td> <td><input type="checkbox"/></td> </tr> <tr> <td>2</td> <td>Henry</td> <td>123456</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p><input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Move to phonebook"/></p>	Index	Name	Number	<input type="checkbox"/>	1	Rob	12345	<input type="checkbox"/>	2	Henry	123456	<input type="checkbox"/>	<p>Select one contact and click edit to change the information, click delete to delete the contact, click Move to phonebook to move the contact to phonebook.</p> <p>Click Add to add one blacklist, enter the name and phone number, click OK to confirm and click cancel to cancel.</p> <p>Name <input type="text" value="Ded"/></p> <p>Number <input type="text" value="123589"/></p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p>
Index	Name	Number	<input type="checkbox"/>										
1	Rob	12345	<input type="checkbox"/>										
2	Henry	123456	<input type="checkbox"/>										

4.7.5 Call Log

To view the call log information such as redial list (incoming call), answered call and missed call

Redial List				
Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	123	10/28 10:30	00:00:07	<input type="checkbox"/>
2	010123	10/28 12:02	00:00:01	<input type="checkbox"/>
3	010123	10/28 16:16	00:00:00	<input type="checkbox"/>
4	010123	10/28 16:16	00:00:00	<input type="checkbox"/>
5	123	10/28 16:20	00:00:13	<input type="checkbox"/>
6	123	10/28 16:21	00:00:34	<input type="checkbox"/>
7	123	10/29 10:50	00:00:10	<input type="checkbox"/>
8	123	10/29 14:36	00:00:01	<input type="checkbox"/>
9	123	10/29 15:05	00:00:23	<input type="checkbox"/>
10	123	10/29 15:06	00:00:05	<input type="checkbox"/>
..	<input type="checkbox"/>

Answered Calls				
Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	22222	10/21 09:56	00:00:40	<input type="checkbox"/>
2	110	10/21 18:14	00:00:03	<input type="checkbox"/>
3	110	10/21 18:15	00:00:07	<input type="checkbox"/>
4	sipp	10/23 13:40	00:00:06	<input type="checkbox"/>
5	sipp	10/24 18:05	00:00:05	<input type="checkbox"/>
6	sipp	10/24 18:05	00:00:05	<input type="checkbox"/>
7	sipp	10/25 15:38	00:00:03	<input type="checkbox"/>
8	sipp	10/25 15:42	00:00:06	<input type="checkbox"/>
9	sipp	10/25 15:55	00:00:10	<input type="checkbox"/>
10	sipp	10/25 16:03	00:00:02	<input type="checkbox"/>
..	<input type="checkbox"/>

Missed Calls				
Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	110	10/21 09:50	00:00:03	<input type="checkbox"/>
2	555	10/22 12:04	00:00:03	<input type="checkbox"/>

4.8 FXS2

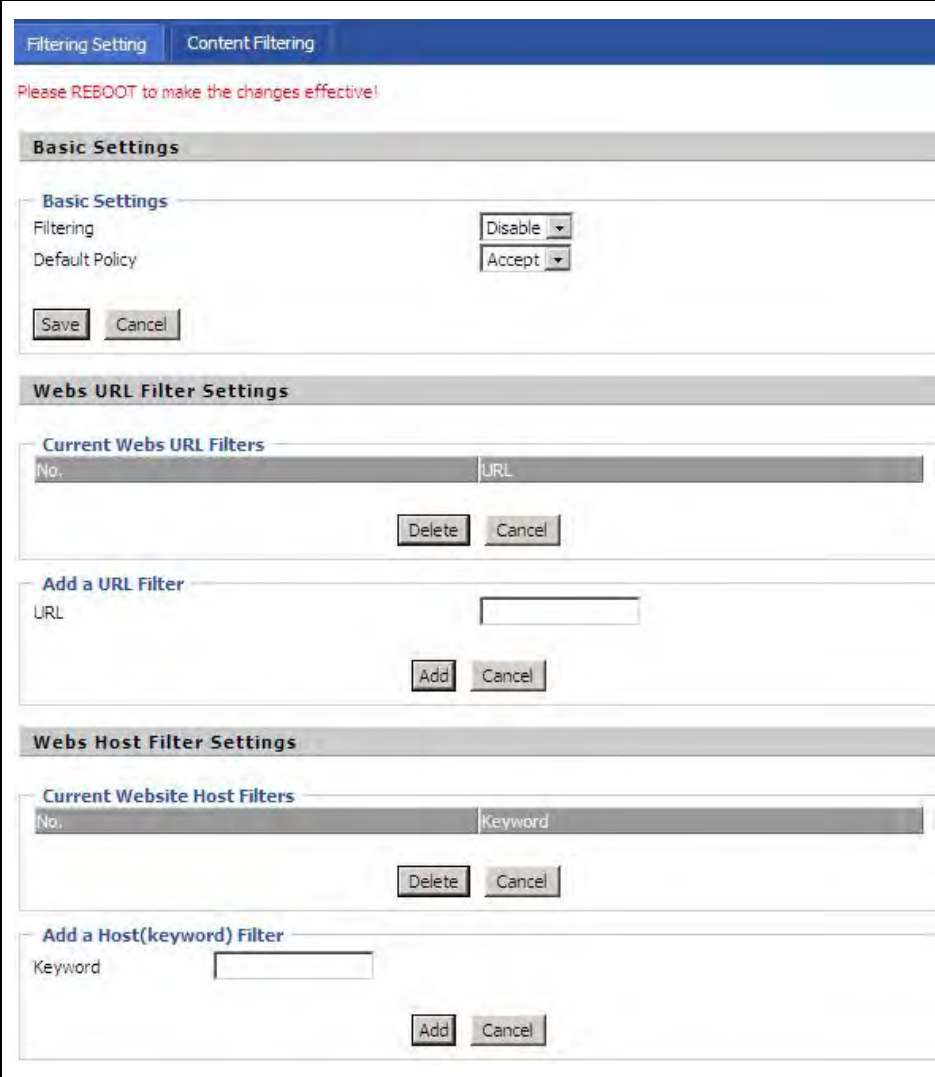
The settings of FXS2 are the same as FXS1.

4.9 Security

4.9.1 Filtering Setting

<p>Basic Settings</p> <p>Basic Settings</p> <p>Filtering <input type="text" value="Disable"/></p> <p>Default Policy <input type="text" value="Drop"/></p> <p>The packet that don't match with any rules would be</p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>	<p>Field Name</p>	<p>Description</p>																
<p>IP/Port Filter Settings</p> <p>Mac address <input type="text"/></p> <p>Dest IP Address <input type="text"/></p> <p>Source IP Address <input type="text"/></p> <p>Protocol <input type="text" value="NONE"/></p> <p>Dest. Port Range <input type="text"/> - <input type="text"/></p> <p>Src Port Range <input type="text"/> - <input type="text"/></p> <p>Action <input type="text" value="Drop"/></p> <p>Comment <input type="text"/></p> <p>(The maximum rule count is 32)</p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>	<p>Filtering</p>	<p>If or not enable filter function</p>																
<p>Current MAC/IP/Port filtering rules in system</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Mac address</th> <th>Dest IP Address</th> <th>Source IP Address</th> <th>Protocol</th> <th>Dest. Port Range</th> <th>Src Port Range</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="8" style="text-align: center;">Others would be dropped.</td> </tr> </tbody> </table> <p><input type="button" value="Delete"/> <input type="button" value="Cancel"/></p>	No.	Mac address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Others would be dropped.								<p>Default Policy</p>	<p>Choose to give up or accept</p>
No.	Mac address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action											
Others would be dropped.																		
	<p>Mac address</p>	<p>Add the Mac address filtering</p>																
	<p>Dest IP address</p>	<p>Dest IP address</p>																
	<p>Source IP address</p>	<p>Source IP address</p>																
	<p>Protocol</p>	<p>Select a protocol name, support for TCP, UDP and TCP&UDP</p>																
	<p>Dest. Port Range</p>	<p>Destination port ranges</p>																
	<p>Src Port Range</p>	<p>Source port range</p>																
	<p>Action</p>	<p>You can choose to receive or give up; this should be consistent with the default policy.</p>																
	<p>Comment</p>	<p>Add callout</p>																
	<p>Delete</p>	<p>Delete selected item</p>																

4.9.2 Content Filtering

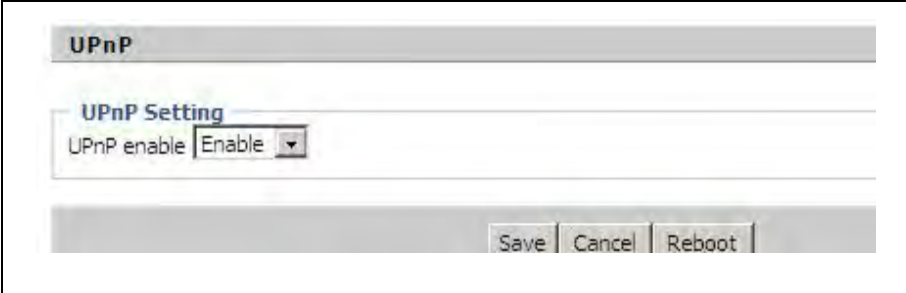
	Field Name	Description				
Please REBOOT to make the changes effective!	Filtering	If or not enable content Filtering				
Basic Settings	Default Policy	The default policy is to accept or to prohibit filtering rules				
Basic Settings Filtering: <input type="button" value="Disable"/> <input type="button" value="Accept"/> Default Policy: <input type="button" value="Accept"/>	Current Webs URL Filters	List the URL filtering rules that already existed (blacklist)				
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	Delete/Cancel	You can choose to delete or cancel the existing filter rules				
Webs URL Filter Settings	Add a URL Filter	Add URL filtering rules				
Current Webs URL Filters <table border="1"> <thead> <tr> <th>No.</th> <th>URL</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>	No.	URL			Add/Cancel	Click adds to add one rule or click cancel.
No.	URL					
Add a URL Filter URL: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Cancel"/>	Current Website Host Filters	List the keywords that already exist (blacklist)				
Webs Host Filter Settings	Delete/Cancel	You can choose to delete or cancel the existing filter rules the existing keywords.				
Current Website Host Filters <table border="1"> <thead> <tr> <th>No.</th> <th>Keyword</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>	No.	Keyword			Add a Host Filter (Keyword)	Add keywords
No.	Keyword					
Add a Host(keyword) Filter Keyword: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Cancel"/>	Add/Cancel	Click the Add or cancel				

4.10 Application

4.10.1 UPnP

UPnP (Universal Plug and Play) support zero setting networking, and can automatically discover a variety of networked devices. UPnP is enabled, allows the device supports UPnP function dynamically access network, obtain an IP address, and convey its performance information. If the network has a DHCP and DNS server, you can automatically obtain DHCP and DNS services.

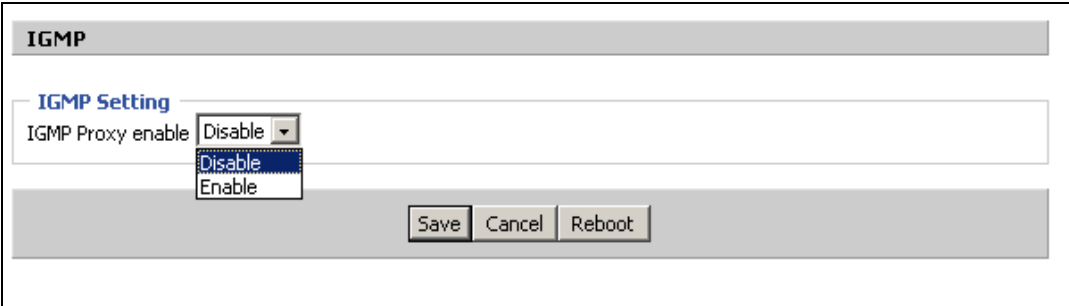
Supports UPnP devices can be automatically off the network, the device or other devices on the network without affecting.

 <p>The screenshot shows the UPnP configuration page. At the top, there is a header 'UPnP'. Below it, under 'UPnP Setting', there is a dropdown menu for 'UPnP enable' which is currently set to 'Enable'. At the bottom of the page, there are three buttons: 'Save', 'Cancel', and 'Reboot'.</p>	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>UPnP enable</td> <td>If or not enable UPnP function.</td> </tr> </tbody> </table>	Field Name	Description	UPnP enable	If or not enable UPnP function.	
Field Name	Description					
UPnP enable	If or not enable UPnP function.					

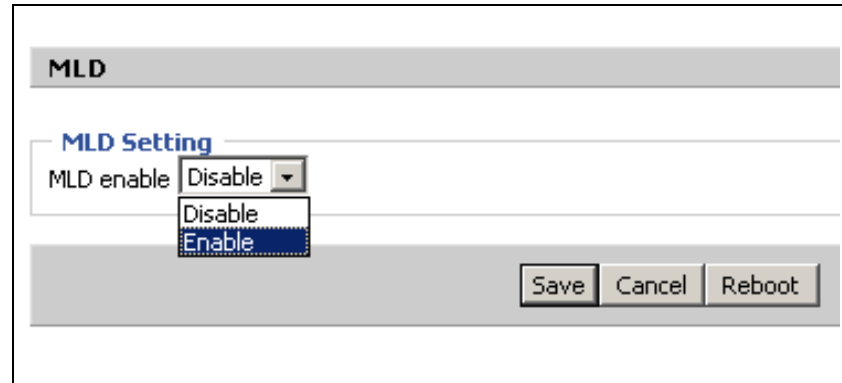
4.10.2 IGMP

Multicast has the ability to send the same data to multiple devices.

IP hosts use IGMP (Internet Group Management Protocol) report multicast group memberships to the neighboring routers to transmit data, at the same time, the multicast router use IGMP to discover which hosts belong to the same multicast group.

 <p>The screenshot shows the IGMP configuration page. At the top, there is a header 'IGMP'. Below it, under 'IGMP Setting', there is a dropdown menu for 'IGMP Proxy enable' which is currently set to 'Disable'. At the bottom of the page, there are three buttons: 'Save', 'Cancel', and 'Reboot'.</p>	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>IGMP Proxy enable</td> <td>If or not enable IGMP function.</td> </tr> </tbody> </table>	Field Name	Description	IGMP Proxy enable	If or not enable IGMP function.	
Field Name	Description					
IGMP Proxy enable	If or not enable IGMP function.					

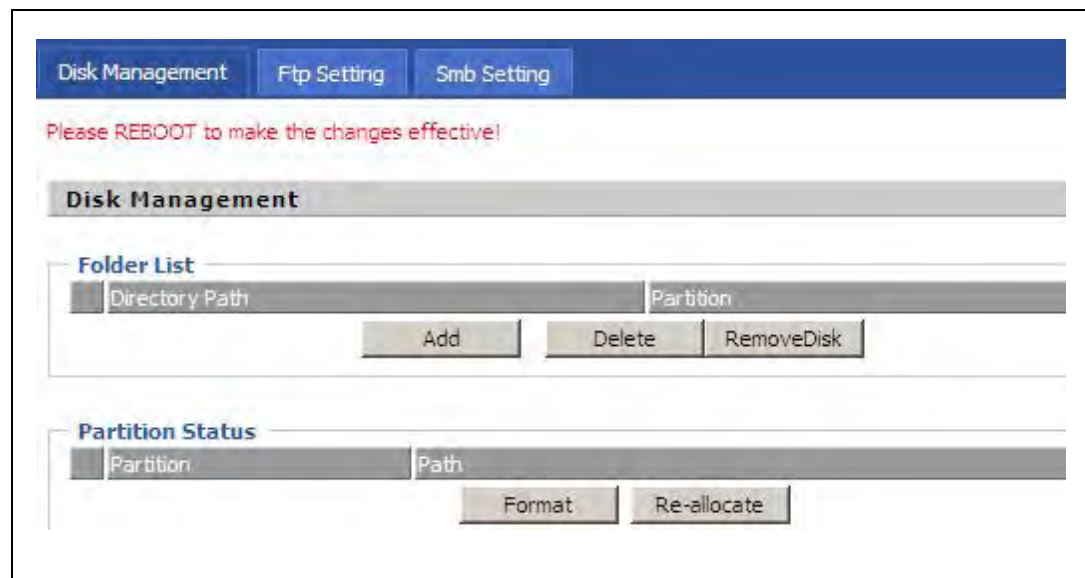
4.10.3 MLD

	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>MLD enable</td> <td>If or not enable MLD function</td> </tr> </tbody> </table>	Field Name	Description	MLD enable	If or not enable MLD function	
Field Name	Description					
MLD enable	If or not enable MLD function					

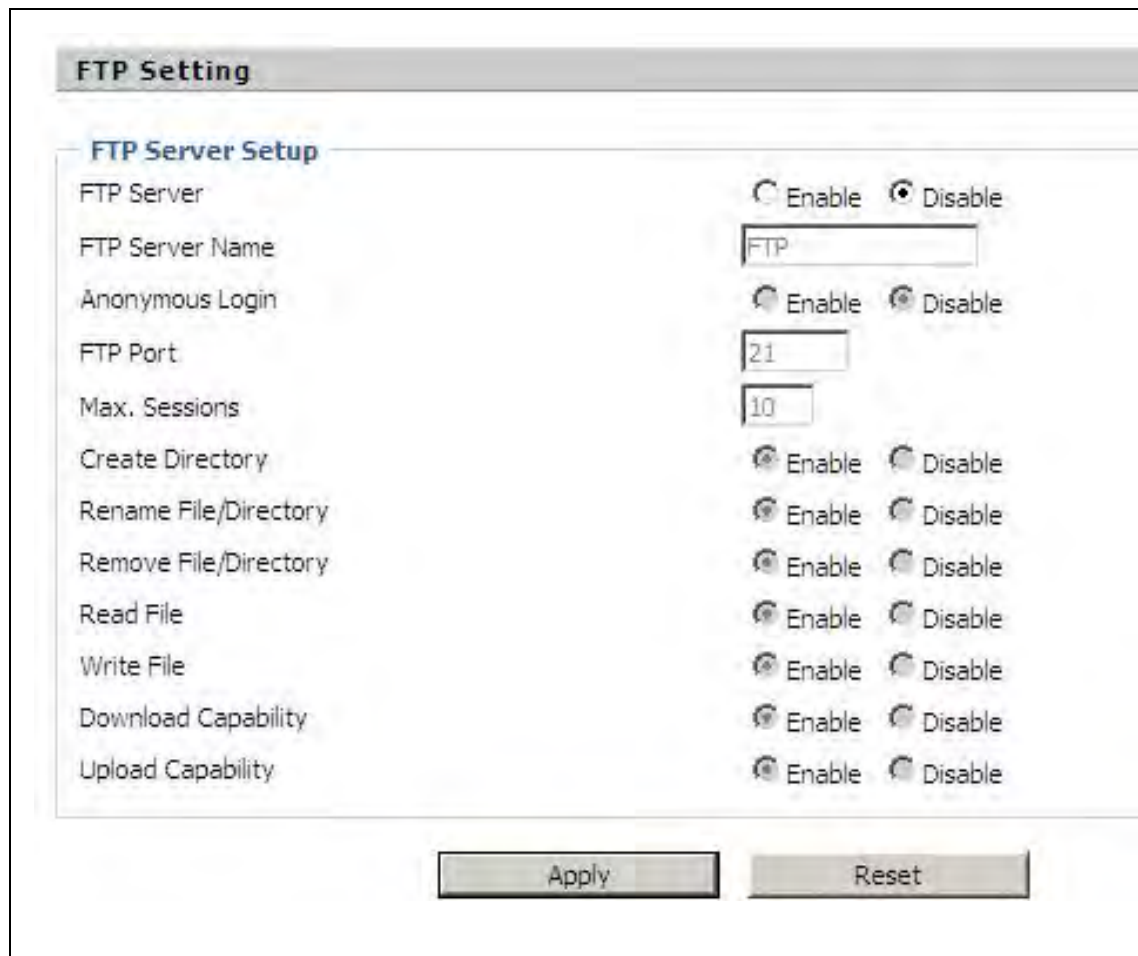
4.11 Storage

4.11.1 Disk Management

This page is used to manage the USB storage device.

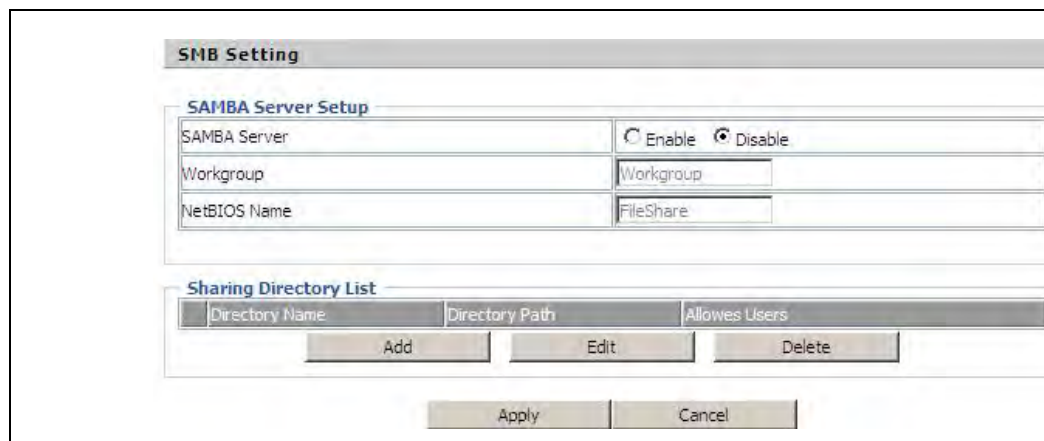
	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Add</td> <td>Adding files to the USB storage device</td> </tr> <tr> <td>Delete</td> <td>Remove the USB storage device file</td> </tr> <tr> <td>Remove Disk</td> <td>Transfer files within a USB storage device</td> </tr> <tr> <td>Format</td> <td>Format the USB storage device</td> </tr> <tr> <td>Re-allocate</td> <td>Resetting the USB storage device</td> </tr> </tbody> </table>	Field Name	Description	Add	Adding files to the USB storage device	Delete	Remove the USB storage device file	Remove Disk	Transfer files within a USB storage device	Format	Format the USB storage device	Re-allocate	Resetting the USB storage device	
Field Name	Description													
Add	Adding files to the USB storage device													
Delete	Remove the USB storage device file													
Remove Disk	Transfer files within a USB storage device													
Format	Format the USB storage device													
Re-allocate	Resetting the USB storage device													

4.11.2 FTP Setting



Field Name	Description
FTP Server	If or not enable FTP server
FTP Server Name	Set the FTP server name
Anonymous Login	If or not support anonymous login
FTP Port	Set FTP server port number
Max. Sessions	Maximum number of connections
Create Directory	If or not enable create directory
Rename File/Directory	If or not enable rename file/directory
Remove File/Directory	If or not enable transfer of files/directories
Read File	If or not enable read files
Write File	If or not enable write files
Download Capability	If or not enable download capability function.
Upload Capability	If or not enable upload capability function

4.11.3 Smb Setting



Field Name	Description
SAMBA Server	If or not enable SAMBA server
Workgroup	Fill in the working group
NetBIOS Name	Network basic input/output system name
Add	Add a shared file
Edit	Edit a shared file
Del	Delete a shared file

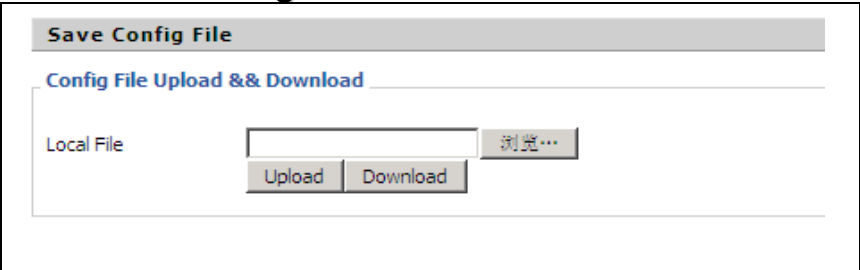
4.12 Administration

Use can manage the device in these webpage; you can configure the Time/Date, password, web access, system log and associated configuration TR069

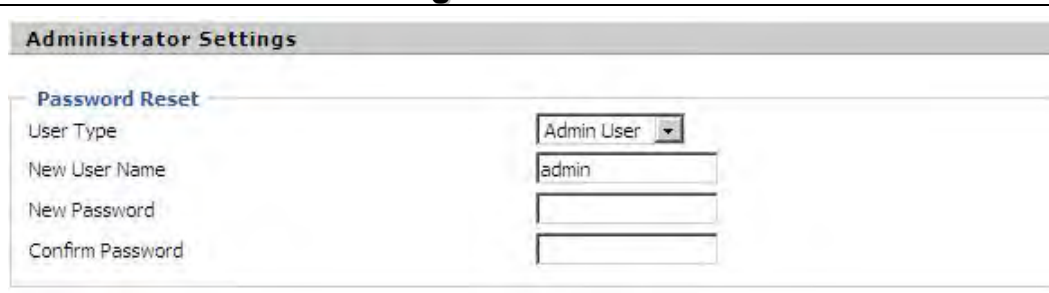

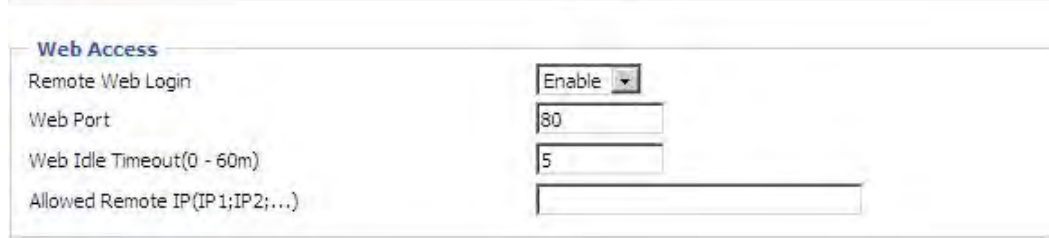
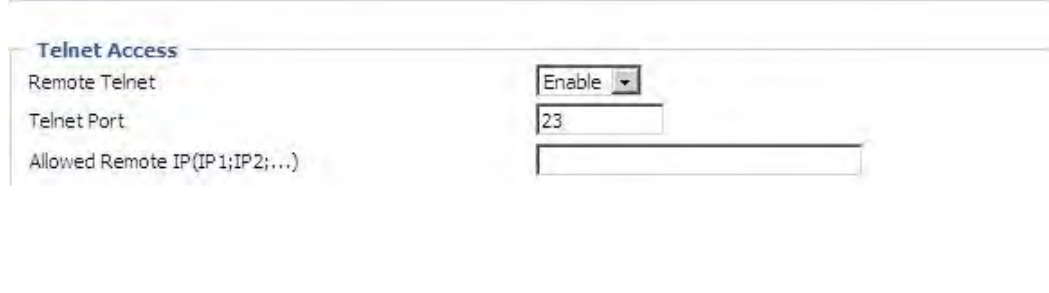
4.12.1 Management

You can configure the value of Time/Date, password, web access, and system log and so on.

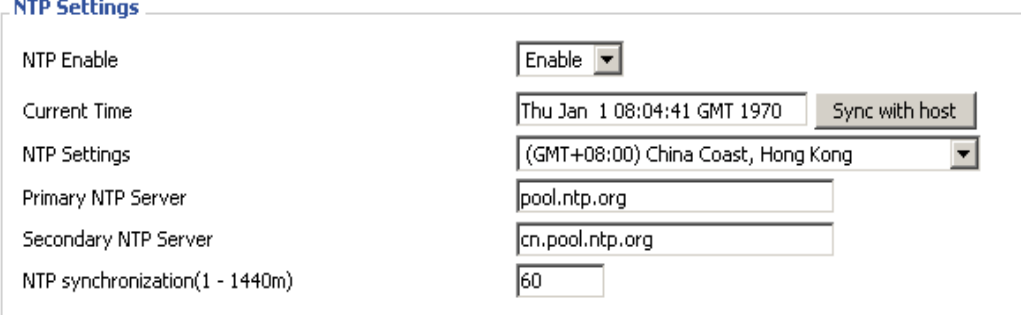
1. Save config file

Save Config File	Field Name	Description
	Config file upload and download	Upload: click on browse, select file in the local, press the upload button to begin uploading files Download: click to download, and then select contains the path to download the configuration file

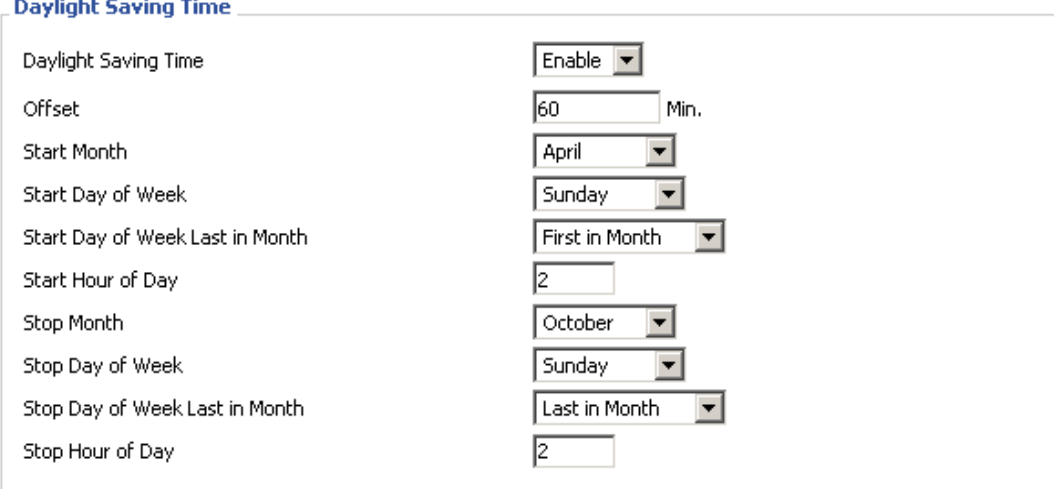
2. Administrator settings

Administrator Settings	Field Name	Description
	User type	Choose the user type from admin user and normal user and basic user.
	New User Name	You can modify the user name, set up a new user name
	New Password	Input the new password
	Confirm Password	Input the new password again
	Language	Select the language for the web, the device support Chinese, English, and Spanish and so on.
	Remote Web Login	If or not enable remote Web login
	Web Port	Set the port value which is used to login from Internet port and PC port, default is 80.
	Web Idle timeout	Set the Web Idle timeout time. The webpage can be logged out after Web Idle Timeout without any operation.
	Allowed Remote IP(IP1,IP2,...)	Set the IP which can login the device remotely.
	Remote Telnet	If or not enable remote telnet login
	Telnet Port	Set the port value which is used to telnet the device.

3. NTP settings

	Field Name	Description
	NTP Enable	If or not enable NTP
	Current Time	Display current time
	NTP Settings	Setting the Time Zone
	Primary NTP Server	Primary NTP server's IP address or domain name
	Secondary NTP Server	Options for NTP server's IP address or domain name
	NTP synchronization	NTP synchronization cycle, cycle time can be 1 to 1440 minutes in any one, the default setting is 60 minutes

4. Daylight Saving Time

	<p>Set the summer time steps:</p> <p>Step 1. Enable Daylight Saving Time.</p> <p>Step 2. Set value of offset, like the upon picture</p> <p>Step 3: Set starting Month/Week/Day/Hour in Start Month/Start Day of Week Last in Month/Start Day of Week/Start Hour of Day, analogously set stopping Month/Week/Day/Hour in Stop Month/Stop Day of Week Last in Month/Stop Day of Week/Stop Hour of Day.</p> <p>Step 4. Press Saving button to save and press Reboot button to active changes.</p>
--	--

5. System Log Setting

	Field Name	Description
<p>Syslog Setting</p> <p>Syslog Enable <input type="button" value="Enable"/></p> <p>Syslog Level <input type="button" value="INFO"/></p> <p>Remote Syslog Enable <input type="button" value="Enable"/></p> <p>Remote Syslog Server <input type="text" value="192.168.10.101"/></p>	Syslog Enable	If or not enable syslog function
	Syslog Level	Select the system log, there is INFO and Debug two grades, the Debug INFO can provide more information.
	Remote Syslog Enable	If or not enable remote syslog function.
	Remote Syslog server	Add a remote server IP address.

6. Factory Defaults Setting

<p>Factory Defaults Setting</p> <p>Factory Defaults Lock <input type="button" value="Disable"/></p>	If enable this function ,the device will not be restore factory settings
--	--

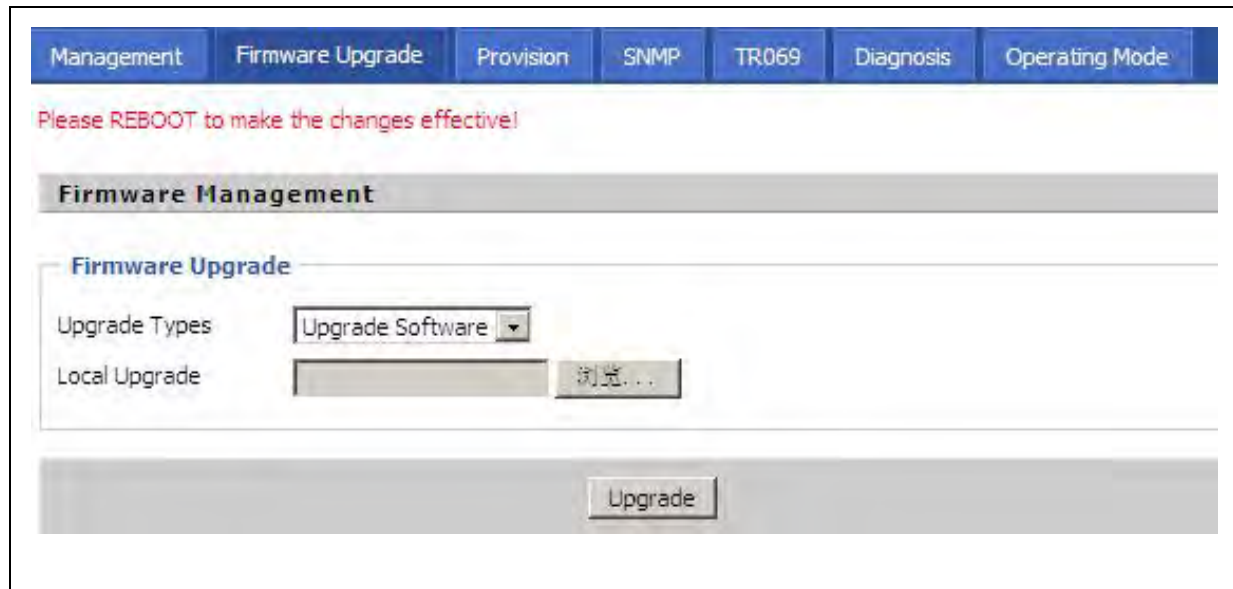
7. Packet Trace

<p>Packet Trace</p> <p>Tracking Interface <input type="button" value="eth2"/></p> <p>Packet Trace <input type="button" value="start"/> <input type="button" value="stop"/> <input type="button" value="save"/></p>	Users can use the packet trace feature intercepts the packets that were sent. Click the Start button, start dhome gateway tracking and keep refreshing the page until the message trace shows to stop, click the Save button to save captured packets.
---	--

8. Factory Defaults

<p>Factory Defaults</p> <p>Reset to Factory Defaults <input type="button" value="Factory Default"/></p>	Click Factory Default to restore the residential gateway to factory settings.
--	---

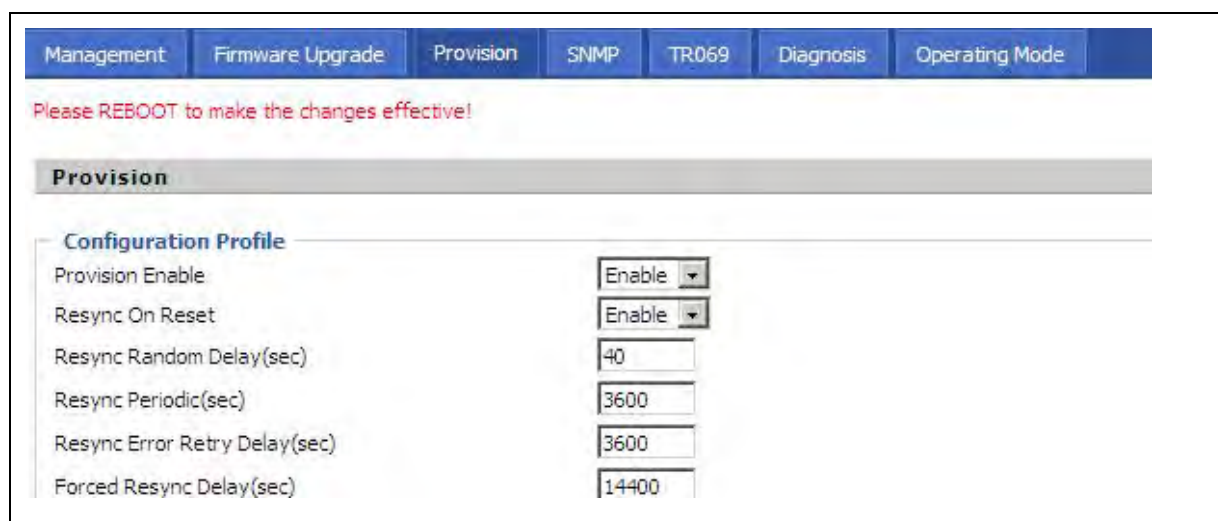
4.12.2 Firmware Upgrade

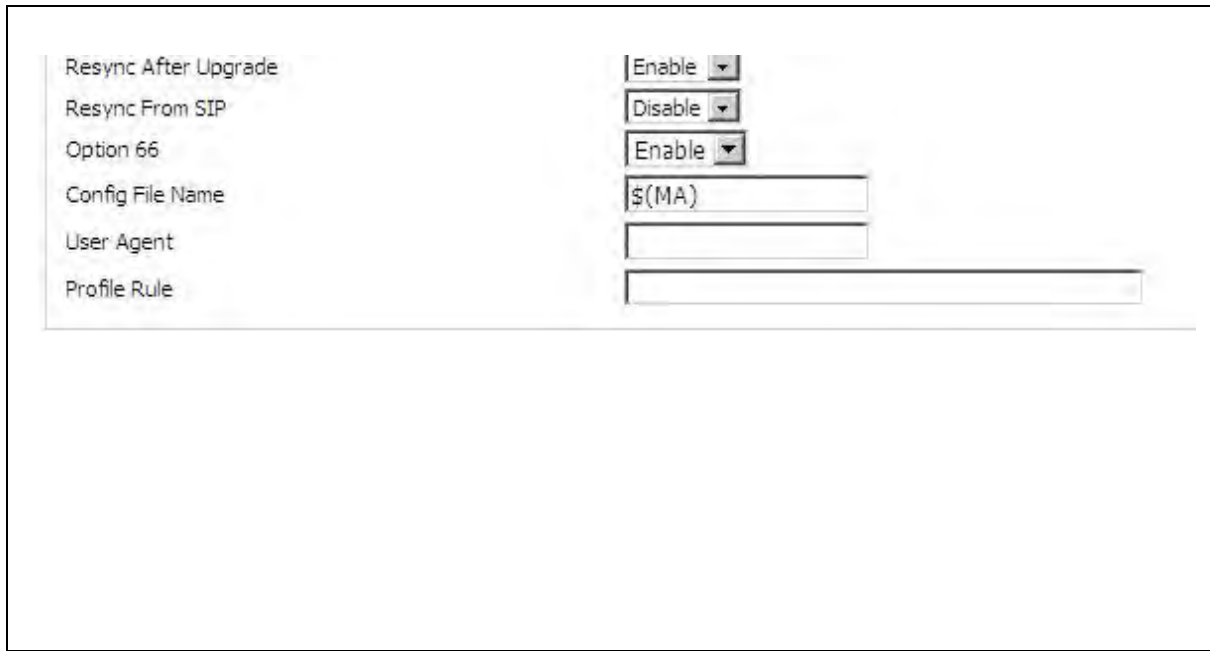
	<ol style="list-style-type: none"> 1. Choose upgrade file type from Image File and Dial Rule 2. Press <input type="button" value="浏览..."/> to browser file. 3. Press <input type="button" value="Upgrade"/> to start upgrading.
--	--

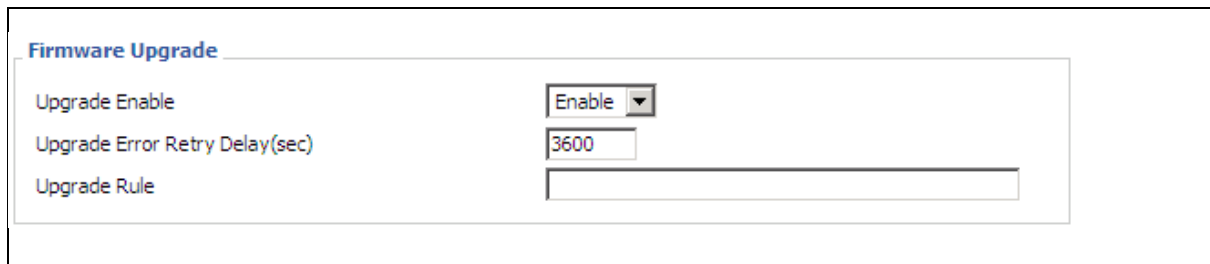
4.12.3 Provision

Provisioning allows G902 auto-upgrading and auto-configuring, and Flyingvoice devices support TFTP, HTTP and HTTPS three ways.

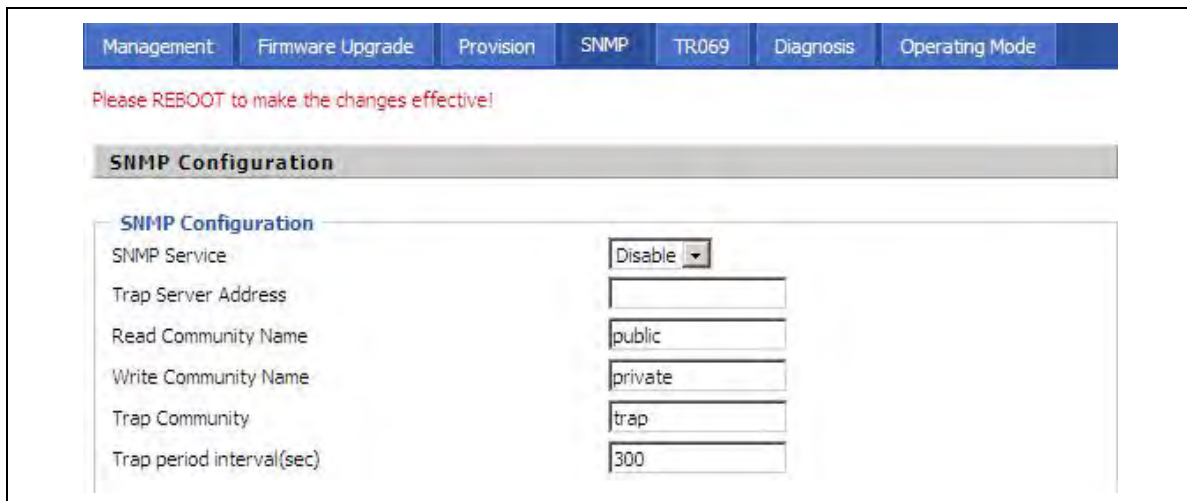
1. Before testing or using TFTP, user should have tftp server and upgrading file and configuring file.
 2. Before testing or using HTTP, user should have http server and upgrading file and configuring file.
 3. Before testing or using HTTPS, user should have https server and upgrading file and configuring file and CA Certificate file(should same as https server's) and Client Certificate file and Private key file(HTTPS provision will be supported soon)
- User can uploading CA Certificate file and Client Certificate file and Private Key file in Security page.

	<table border="1"> <thead> <tr> <th>Field Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Provision Enable</td> <td>If or not enable provision.</td> </tr> <tr> <td>Resync on Reset</td> <td>If or not enable resync after restart</td> </tr> <tr> <td>Resync Random Delay(sec)</td> <td>Set the maximum delay for request the synchronization file, default is 40.</td> </tr> <tr> <td>Resync Periodic(sec)</td> <td>If the last resync was failure, G902 will retry resync after the “Resync Error Retry Delay ” time, default is 3600s.</td> </tr> <tr> <td>Resync Error Retry Delay(rec)</td> <td>Set the periodic time for resync, default is 3600s.</td> </tr> <tr> <td>Forced Resync Delay(sec)</td> <td>If it's time to resync, but G902 is busy now, in this case, G902 will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over,</td> </tr> </tbody> </table>	Field Name	Description	Provision Enable	If or not enable provision.	Resync on Reset	If or not enable resync after restart	Resync Random Delay(sec)	Set the maximum delay for request the synchronization file, default is 40.	Resync Periodic(sec)	If the last resync was failure, G902 will retry resync after the “Resync Error Retry Delay ” time, default is 3600s.	Resync Error Retry Delay(rec)	Set the periodic time for resync, default is 3600s.	Forced Resync Delay(sec)	If it's time to resync, but G902 is busy now, in this case, G902 will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over,
Field Name	Description														
Provision Enable	If or not enable provision.														
Resync on Reset	If or not enable resync after restart														
Resync Random Delay(sec)	Set the maximum delay for request the synchronization file, default is 40.														
Resync Periodic(sec)	If the last resync was failure, G902 will retry resync after the “Resync Error Retry Delay ” time, default is 3600s.														
Resync Error Retry Delay(rec)	Set the periodic time for resync, default is 3600s.														
Forced Resync Delay(sec)	If it's time to resync, but G902 is busy now, in this case, G902 will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over,														

		G902 will forced to resync.
	Resync After Upgrade	If or not enable firmware upgrade after resync, by default it is enabled.
	Resync From SIP	If or not enable resync from SIP.
	Option 66	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in IP542N's webpage. When disable Option 66 , this parameter has no effect.
	Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66 , this parameter has no effect.
	Profile Rule	URL of profile provision file Note that the specified file path is relative to the TFTP server's virtual root directory.

	Field Name	Description
	Upgrade Enable	If or not enable firmware upgrade via provision.
	Upgrade Error Retry Delay(sec)	If the last upgrade fails, G902 will try upgrading again after "Upgrade Error Retry Delay" period, default is 3600s.
	Upgrade Rule	URL of upgrade file

4.12.4 SNMP

	Field Name	Description
	SNMP Service	If or not enable SNMP.
	Trap Server Address	Enter the trap server address.
	Read Community Name	String, as an express password between management progress and agent progress.
	Write Community Name	String, as an express password between management progress and agent progress.
	Trap Community	The community field in trap.
	Trap period interval(sec)	The interval of sending trap.

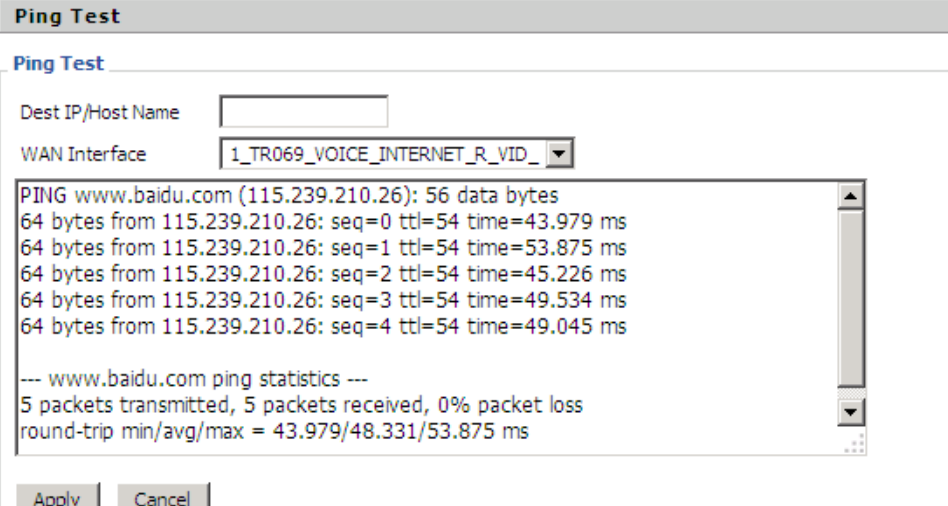
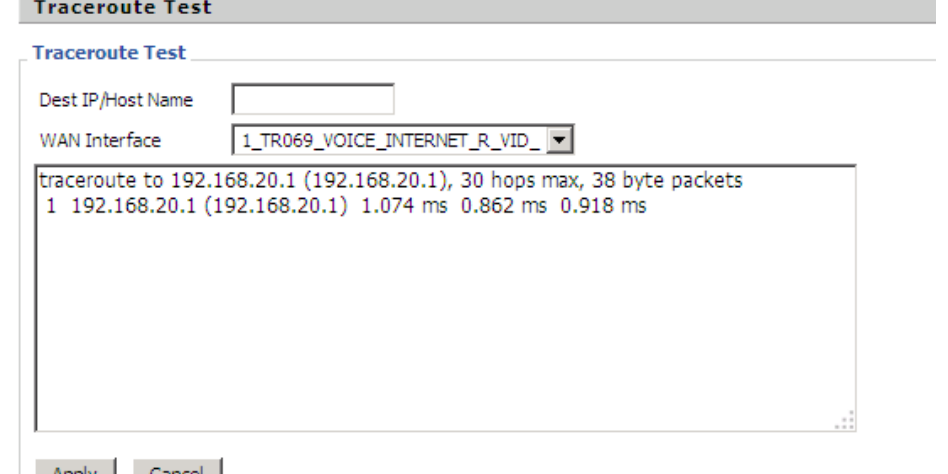
4.12.5 TR069

Field Name	Description
TR069 Enable	If or not enable TR069
CWMP	If or not enable CWMP
ACS URL	ACS URL address
User Name	ACS username
Password	ACS password
Periodic Inform Enable	If or not enable the function of periodic inform, default is enable
Periodic Inform Interval	Periodic notification interval, the unit is seconds, default is 43200s
User Name	The username used to connect the TR069 server to the DUT.
Password	The password used to connect the TR069 server to the DUT.

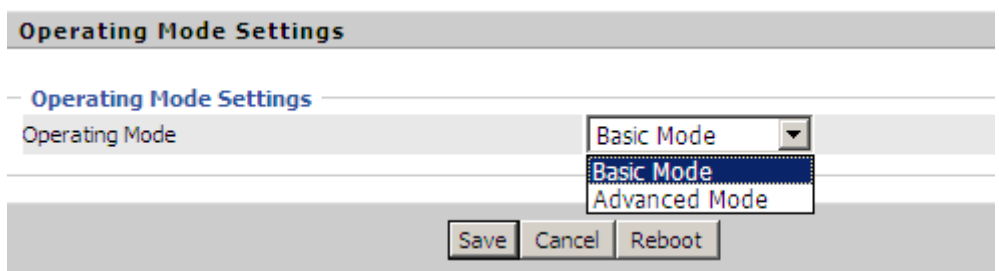
Management	Firmware Upgrade	Provision	SNMP	TR069	Diagnosis	Operating Mode
Please REBOOT to make the changes effective!						
TR069 Configuration						
ACS						
TR069 Enable	Disable ▾					
CWMP	Enable ▾					
ACS URL	<input type="text"/>					
User Name	<input type="text"/>					
Password	<input type="text"/>					
Periodic Inform Enable	Enable ▾					
Periodic Inform Interval	30					
Connect Request						
User Name	<input type="text"/>					
Password	<input type="text"/>					

4.12.6 Diagnosis

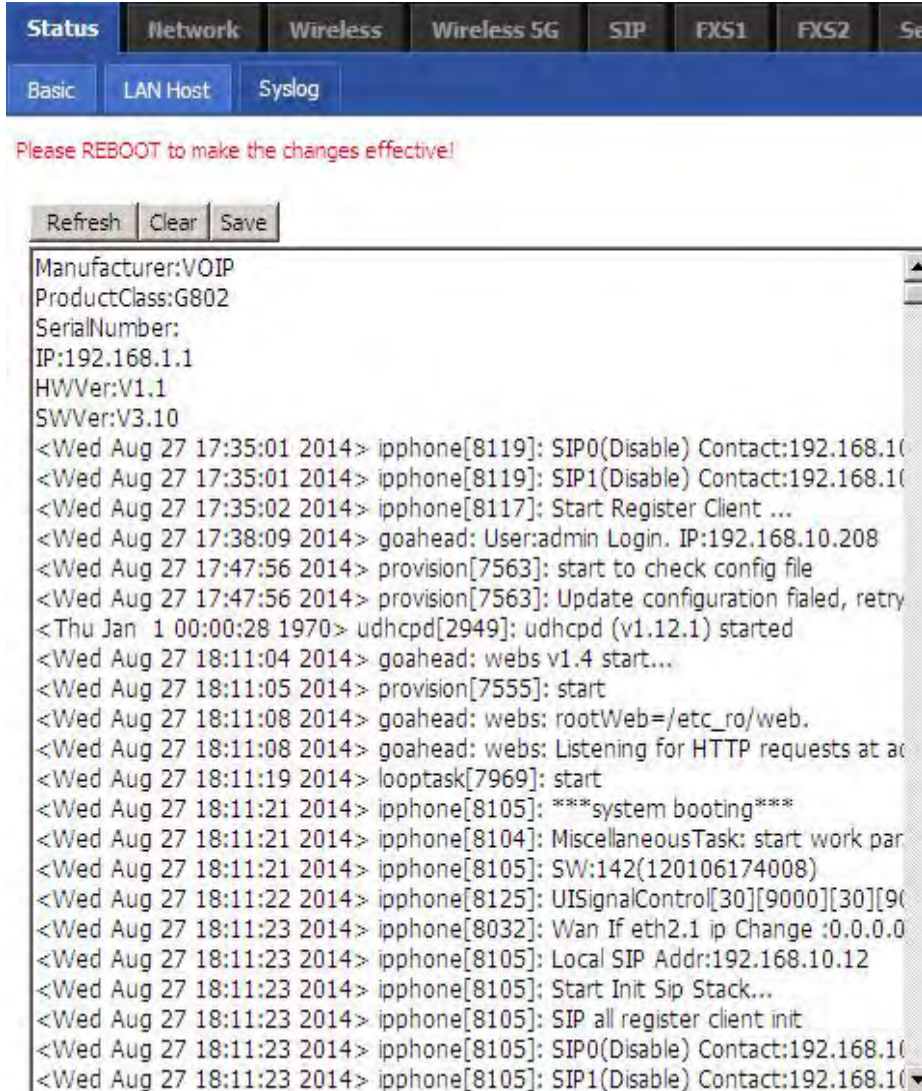
In this page, user can do ping test and traceroute test to diagnose the device's connection status.

	<p>1. Ping Test Enter the destination IP or host name, and then click Apply, device will perform ping test.</p>
	<p>2. Traceroute Test Enter the destination IP or host name, and then click Apply, device will perform traceroute test.</p>


4.12.7 Operation Mode

	<p>Choose the Operation Mode as Basic Mode or Advance Mode.</p>
--	---

4.13 System Log

 <p>The screenshot shows a web interface with tabs for Status, Network, Wireless, Wireless 5G, SIP, FXS1, and FXS2. Under the Status tab, there are sub-tabs for Basic, LAN Host, and Syslog. A red message says "Please REBOOT to make the changes effective!". Below that are buttons for Refresh, Clear, and Save. The log content includes:</p> <pre> Manufacturer:VOIP ProductClass:G802 SerialNumber: IP:192.168.1.1 HWVer:V1.1 SWVer:V3.10 <Wed Aug 27 17:35:01 2014> ipphone[8119]: SIP0(Disable) Contact:192.168.10.208 <Wed Aug 27 17:35:01 2014> ipphone[8119]: SIP1(Disable) Contact:192.168.10.208 <Wed Aug 27 17:35:02 2014> ipphone[8117]: Start Register Client ... <Wed Aug 27 17:38:09 2014> goahead: User:admin Login. IP:192.168.10.208 <Wed Aug 27 17:47:56 2014> provision[7563]: start to check config file <Wed Aug 27 17:47:56 2014> provision[7563]: Update configuration failed, retry <Thu Jan 1 00:00:28 1970> udhcpd[2949]: udhcpd (v1.12.1) started <Wed Aug 27 18:11:04 2014> goahead: webs v1.4 start... <Wed Aug 27 18:11:05 2014> provision[7555]: start <Wed Aug 27 18:11:08 2014> goahead: webs: rootWeb=/etc_ro/web. <Wed Aug 27 18:11:08 2014> goahead: webs: Listening for HTTP requests at ac <Wed Aug 27 18:11:19 2014> looptask[7969]: start <Wed Aug 27 18:11:21 2014> ipphone[8105]: ***system booting*** <Wed Aug 27 18:11:21 2014> ipphone[8104]: MiscellaneousTask: start work par <Wed Aug 27 18:11:21 2014> ipphone[8105]: SW:142(120106174008) <Wed Aug 27 18:11:22 2014> ipphone[8125]: UISignalControl[30][9000][30][9000] <Wed Aug 27 18:11:23 2014> ipphone[8032]: Wan If eth2.1 ip Change :0.0.0.0 <Wed Aug 27 18:11:23 2014> ipphone[8105]: Local SIP Addr:192.168.10.12 <Wed Aug 27 18:11:23 2014> ipphone[8105]: Start Init Sip Stack... <Wed Aug 27 18:11:23 2014> ipphone[8105]: SIP all register client init <Wed Aug 27 18:11:23 2014> ipphone[8105]: SIP0(Disable) Contact:192.168.10.208 <Wed Aug 27 18:11:23 2014> ipphone[8105]: SIP1(Disable) Contact:192.168.10.208 </pre>	<p>If you enable the system log in Status/syslog webpage, you can view the system log in this webpage.</p>
--	--

4.14 Logout

 <p>The screenshot shows a status bar with the following text: "Firmware Version V3.10", "Current Time Fri Aug 29 09:05:53 GMT 2014", "Admin Mode", and a "Logout" button.</p>	<p>Press the logout button to logout, and then the login window will appear.</p>
---	--

4.15 Reboot

Press the  button to reboot G902.

5 Trouble shooting of the guide

5.1 Setting your PC gets IP automatically

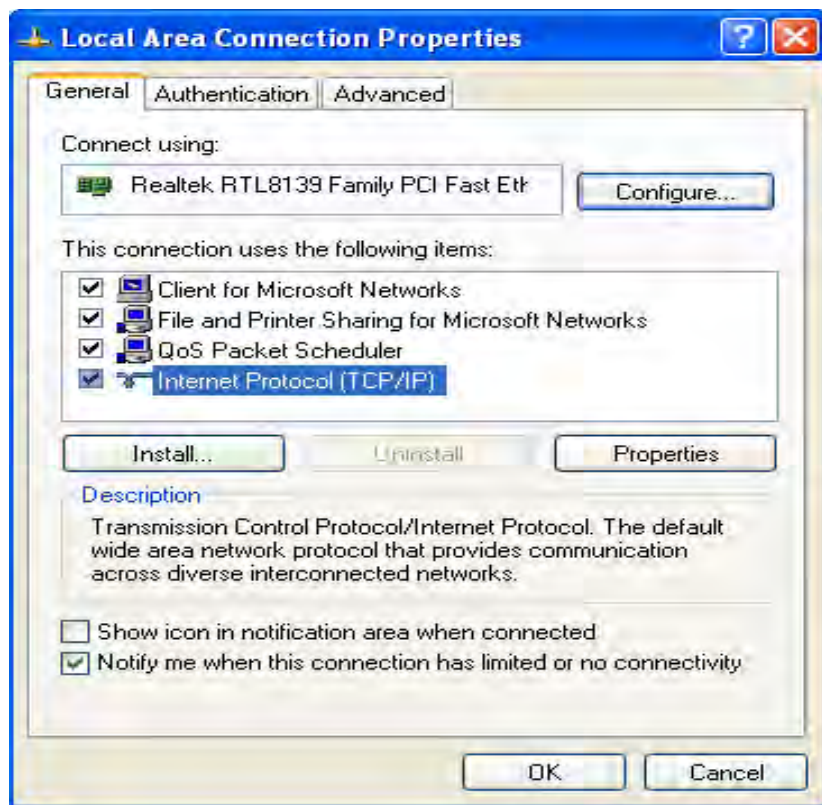
Following are the process of setting your PC gets IP automatically

Step 1. Click the “begin”

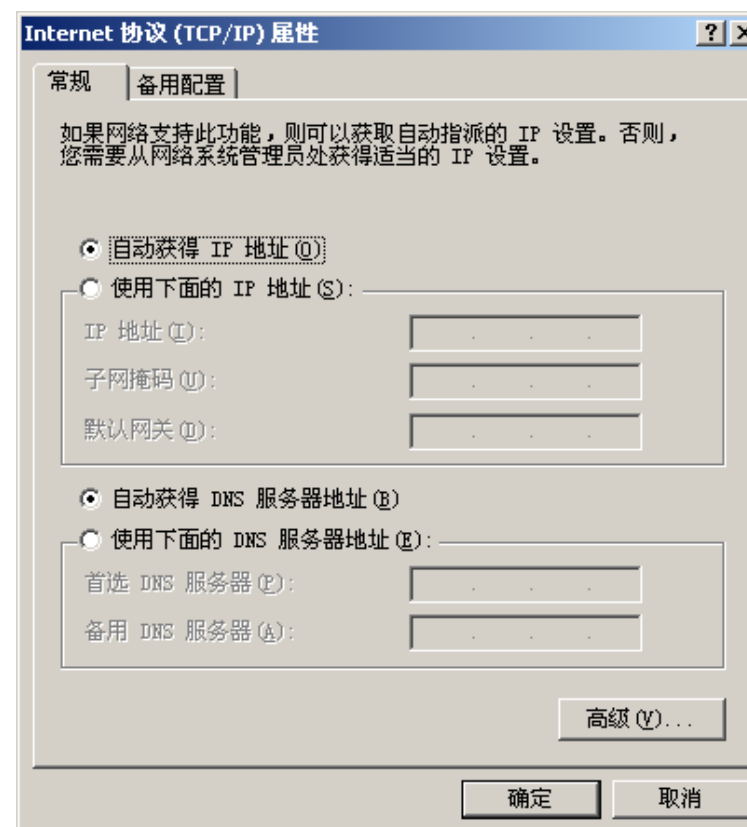
Step 2. Select “control panel”, then double click “network connections” in the “control panel”

Step 3. Right clicks the “network connection” that your PC uses, select “attribute” and you can see the interface as picture 1:

Step 4. Select “Internet Protocol (TCP/IP)”, click “attribute” button, and you can see the interface as following Picture 2 and you should click the “Get IP address automatically”.



Picture 1



Picture 2

5.2 Can not connect to the configuration Website

Solution:

Check if the Ethernet cable is properly connected, then

Check if the URL is right wrote, the format of URL is: http:// the IP address: 8080, 8080 must be added, then

Check if the version of IE is IE8, or use other browser such as Firefox or Mozilla, then

Contact your administrator, supplier, or ITSP for more information or assistance.

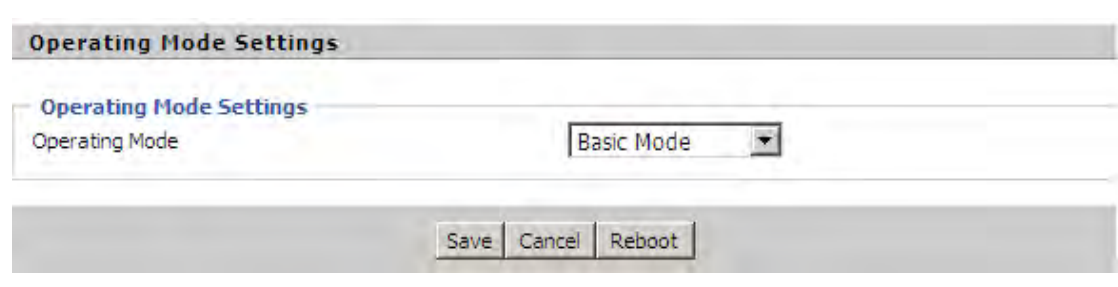
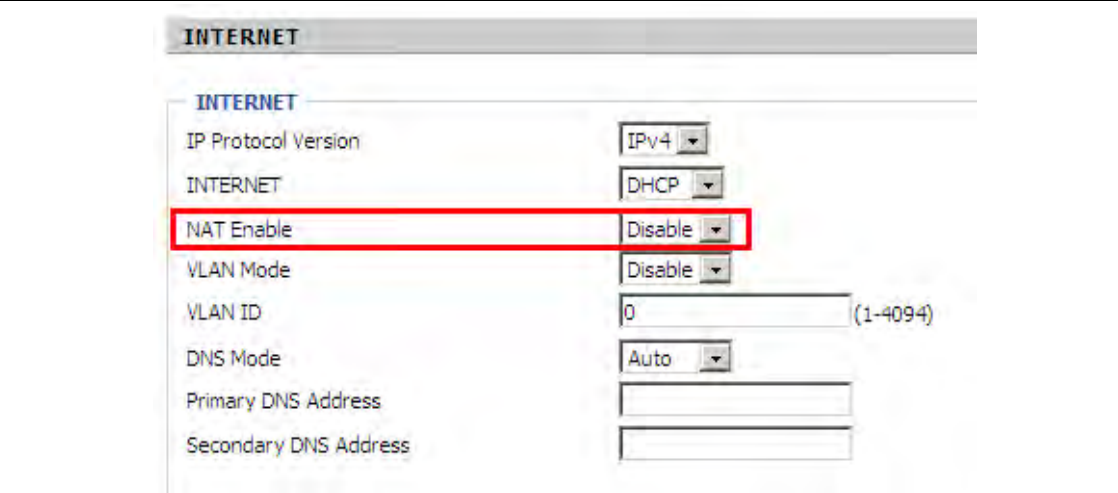
5.3 Forget the Password

If user changed the password and then forgot, you can not access to the configuration website.

Solution:

To factory default: press reset button 10s.

5.4 Fast Bridge Setting

 <p>The screenshot shows the 'Operating Mode Settings' page. At the top, there is a section titled 'Operating Mode Settings' with a dropdown menu set to 'Basic Mode'. Below this, there are three buttons: 'Save', 'Cancel', and 'Reboot'.</p>	<p>Step 1: Login WEB of Device. Turn to Page Administration->Operating Mode. Set Operating mode to Basic Mode. Save.</p>
 <p>The screenshot shows the 'INTERNET' settings page. The 'NAT Enable' option is highlighted with a red box and is set to 'Disable'. Other settings include IP Protocol Version (IPv4), INTERNET (DHCP), VLAN Mode (Disable), VLAN ID (0), and DNS Mode (Auto).</p>	<p>Step 2: Open Network->wan, Change Nat Enable to Disable. Save and Reboot. Now Device works in Bridge mode.</p>

<p>TR069_VOICE_INTERNET Vlan Status</p> <table border="1"> <tr><td>Connection Type</td><td>DHCP</td></tr> <tr><td>MAC Address</td><td>00:21:F2:14:08:13</td></tr> <tr><td>IP Address</td><td>192.168.10.225</td></tr> <tr><td>Subnet Mask</td><td>255.255.255.0</td></tr> <tr><td>Default Gateway</td><td>192.168.10.1</td></tr> <tr><td>Primary DNS</td><td>192.168.10.1</td></tr> <tr><td>Secondary DNS</td><td></td></tr> </table>	Connection Type	DHCP	MAC Address	00:21:F2:14:08:13	IP Address	192.168.10.225	Subnet Mask	255.255.255.0	Default Gateway	192.168.10.1	Primary DNS	192.168.10.1	Secondary DNS		<p>Step 3: Please Login from WAN port. Under is example of Page Status->Basic.</p>
Connection Type	DHCP														
MAC Address	00:21:F2:14:08:13														
IP Address	192.168.10.225														
Subnet Mask	255.255.255.0														
Default Gateway	192.168.10.1														
Primary DNS	192.168.10.1														
Secondary DNS															
<p>Other Vlan Status</p> <table border="1"> <tr><td>Connection Type</td><td>Bridge</td></tr> <tr><td>MAC Address</td><td></td></tr> <tr><td>IP Address</td><td></td></tr> <tr><td>Subnet Mask</td><td></td></tr> <tr><td>Default Gateway</td><td></td></tr> <tr><td>Primary DNS</td><td></td></tr> <tr><td>Secondary DNS</td><td></td></tr> </table>	Connection Type	Bridge	MAC Address		IP Address		Subnet Mask		Default Gateway		Primary DNS		Secondary DNS		
Connection Type	Bridge														
MAC Address															
IP Address															
Subnet Mask															
Default Gateway															
Primary DNS															
Secondary DNS															
<p>VPN Status</p> <table border="1"> <tr><td>VPN Type</td><td>Disable</td></tr> <tr><td>Initial Service IP</td><td></td></tr> <tr><td>Virtual IP Address</td><td></td></tr> </table>	VPN Type	Disable	Initial Service IP		Virtual IP Address										
VPN Type	Disable														
Initial Service IP															
Virtual IP Address															
<p>PC Port Status</p> <table border="1"> <tr><td>IP Address</td><td>192.168.0.1</td></tr> <tr><td>Subnet Mask</td><td>255.255.255.0</td></tr> <tr><td>Port Status</td><td>Link Down</td></tr> </table>	IP Address	192.168.0.1	Subnet Mask	255.255.255.0	Port Status	Link Down									
IP Address	192.168.0.1														
Subnet Mask	255.255.255.0														
Port Status	Link Down														