ReadyNet

CONNECTIVITY SIMPLIFIED

User Manual

AC1000M | AC1000MS | AC1300MS

V1.20210315

Contents

Table

About This User Guide

Thank you for choosing the AC1000M/AC1000MS/AC1300MS wireless router with VoIP. The AC1000M/AC1000MS/AC1300MS includes extended functions which support, USB memory card, this design not only provides users with a conventional VoIP and routing capabilities. Users can also take AC1000M/AC1000MS/AC1300MS as an FTP server, to share LAN files, pictures and other resources. The AC1000M/AC1000MS/AC1300MS VoIP wireless router is ideally suited for small and medium enterprises (SMB) to build wireless workspaces. The AC1000M/AC1000MS/AC1300MS supports IEEE802.11ac gigabit wireless LAN standard, the highest wireless speed is up to 867Mbps and it supports both 2.4GHz and 5GHz bands. For VoIP end users, the 5G band can reduce interference and improve transmission quality. This enables users to enjoy greater bandwidth and enhanced data throughput. The AC1000MS/AC1300MS is the ideal choice for VoIP communication and integrates Internet sharing for daily application. It is an advanced VoIP wireless router, that provides high quality voice communications and wired Internet sharing capabilities but also offers Access Point (AP) function for daily wireless communication.

This guide contains the following chapters:

Contacting ReadyNet

Main Phone Line: +1 (801) 566-0100
Sales Department: +1 (801) 984-5133, +1 (801) 984-5130
Customer Service: +1 (801) 566-0100, Option 1
Service Provider Support: +1 (855) 671-7932

Sales: sales@readynetsolutions.com
Customer Support: customerservice@readynetsolutions.com
Service Provider Technical Support: engineering@readynetsolutions.com

ReadyNet Address
6952 S. High Tech Drive, Suite B
Midvale, UT 84047

Purpose

This document is intended to instruct and assist personnel in the operation, installation and maintenance of the ReadyNet equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained. ReadyNet disclaims all liability whatsoever, implied or expressed, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents.

Send feedback to customerservice@readynetsolutions.com

Declaration of Conformity

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.

Class B Digital Device or Peripheral

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 can generate, use and radiate radio frequency energy. If not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference does not occur in a particular installation.

Note

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

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 interferences 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.

Warnings and Notes

The following describes how warnings and notes are used in this document and in all documents of the ReadyNet document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Notes

Notes text and consequence for not following the instructions in the Notes.

GNU GPL Information
ReadyNet firmware contains third-party software under the GNU General Public License (GPL). Please refer to the GPL for the exact terms and conditions of the license. See links below for important regulatory information.

GNU General Public License (GPL): https://www.readynetsolutions.com/gnu-general-public-license
GPL Support: https://www.readynetsolutions.com/gpl-support

Chapter 1 Product description

This chapter covers:

- AC1000M/AC1000MS/AC1300MS
- LED Indicators and Interfaces
- Hardware Installation
- Voice Prompt

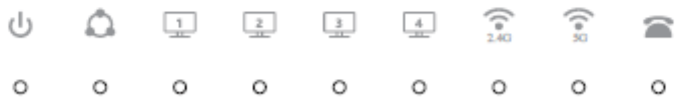
AC1000M/AC1000MS/AC1300MS

Table 1 Features at-a-glance

Port/Model	AC1000M/MS	AC1300MS
picture		
WAN	1	1
LAN	4	4
FXS	2 (AC1000MS)	1
USB	YES	NO
Ethernet interface	5* RJ45 10/100M	5* RJ45 10/100/1000M
Fax	T.30, T.38 Fax	
Wi-Fi	2.4G 2T2R (300Mbps) 5G 2T2R (867Mbps)	2.4G 2T2R(300Mbps) 5G 2T2R (867Mbps)
Voice Code	G.711 (A-law, U-law), G.729A/B, G.723, G.722 (Wide band)	
Management	Voice menu, Web Management, Provision: TFTP/HTTP/HTTPS, TR069, SNMP	
VLAN	Supported	

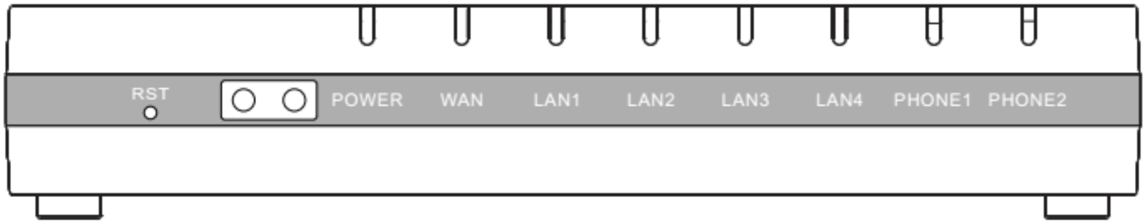
LED Indicators and Interfaces

Table 2 LED Indicators



LED	Status	Explanation
Power	on Green	System is powered on
	off	System is powered off
WAN	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
LAN（1-4）	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
2.4G	on Green	Wireless access point is ready.
	Blinking Green	2.4g is connected, and there is data transmitted
	off	2.4g Wi-Fi off or system is powered off
5G	on Green	Wireless access point is ready.
	Blinking Green	5g is connected, and there is data transmitted
	off	5g Wi-Fi off or system is powered off
FXS(1-2)	on Green	Registered successfully, but no data transfer
	Blinking Green	There is data being transmitted or FXS port is registering
	off	Power is off or registered failed

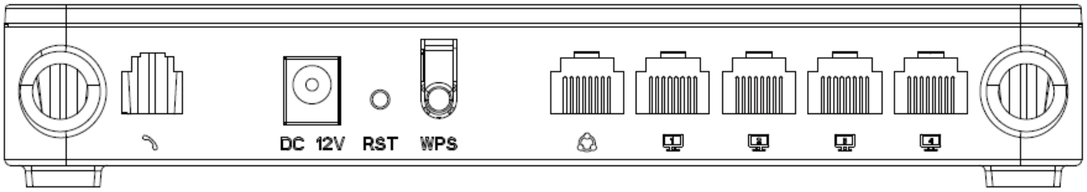
AC1000M/MS



LED	Status	Explanation
FXS(1-2)	on Green	Registered successfully, but no data transfer
	Blinking Green	There is data being transmitted or FXS port is registering
	off	Power is off or registered failed
LAN1/2/3/4	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
WAN	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
POWER	On (Green)	The router is powered on and running normally.
	Off	The router is powered off.
2.4G	on Green	Wireless access point is ready.
	Blinking Green	2.4g is connected, and there is data transmitted
	off	2.4g Wi-Fi off or system is powered off
5G	on Green	Wireless access point is ready.
	Blinking Green	5g is connected, and there is data transmitted
	off	5g Wi-Fi off or system is powered off
RST	Restore the factory settings button, press and hold the device after 5s to restore the factory settings	

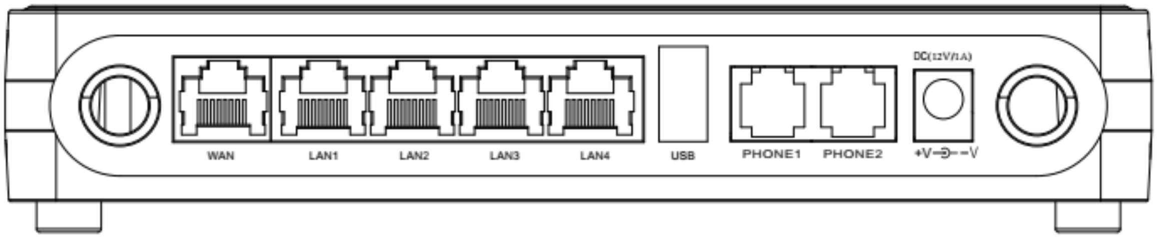
Table 3 Interfaces

AC1300MS



Interface	Description
Phone1	ATA Analog phone connector
POWER	Connector for a power adapter
RESET	Restore the factory settings button, press and hold the device after 5s to restore
WPS	Wi-Fi security settings, when mobile phones, laptops and other wireless devices to find the wireless router Wi-Fi signal, when connected, click the WPS button on the router to complete the wireless router and wireless device encryption authentication and connection.
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices

AC1000MS



POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
USB	Connect USB
LAN 1/2/3/4	Connectors for local networked devices
WAN	Connector for accessing the Internet

Hardware Installation

Before configuring your router, please see the procedure below for instructions on connecting the device in your network.

Procedure 1 Configuring the Router

1. Connect analog phone to ATA Port with an RJ11 cable.
2. Connect the WAN port to the Interne your network’s modem/switch/router/ADSL
3. equipment using an Ethernet cable.
4. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
5. Check the Power, WAN, and LAN LED to confirm network connectivity.

Warning

Please do not attempt to use unsupported power adapters and do not remove power during configuring or updating the device. Using other power adapters may damage the

Warning

Changes or modifications not expressly approved by the party responsible for

compliance can 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 cause harmful interference to radio communications. However, there is no energy and, if not installed and used in accordance with the instructions, may 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.

IVR Voice Prompt

The devices may be configured by navigating the unit's voice menu. By using your phone and dialing a sequence of commands, the device can be configured for operation. Each device configuration section may be accessed by entering a certain operation code, as shown below.

Table 4 IVR Menu Setting Options

Operation code	Menu Navigation
1 Network port configuration (1) WAN Port Connection Type	1. Pick up phone and press "****" to start IVR 2. Choose "1", and The router reports the current WAN port connection type 3. Prompt "Please enter password", user needs to input password and press "#" key, if user wants to configuration WAN port connection type. The password in IVR is same as web management interface login, the user may use phone keypad to enter password directly For example: WEB login password is "admin", so the password in IVR is "admin". The user may "23646" to access and then configure the WAN connection port. The unit reports "Operation Successful" if the password is correct. 4. Prompt "Please enter password", user needs to input password and press "#" key if user wants to configuration WAN port connection type. 5. Choose the new WAN port connection type (1) DHCP or (2) Static The unit reports "Operation Successful" if the changes are successful. The router returns to the prompt "please enter your option …" 6. To quit, enter "*"

(2) WAN Port IP Address	1. Pick up phone and press "****" to start IVR 2. Choose "2", and The router reports current WAN Port IP Address 3. Input the new WAN port IP address and press "#" key: 4. Use "*" to replace ".", for exampleuser can input 192*168*20*168 to set the new IP address 192.168.20.168 5. Press # key to indicate that you have finished 6. Report "operation successful" if user operation is ok. 7. To quit, enter "**".
(3) WAN Port Subnet Mask	1. Pick up phone and press "****" to start IVR 2. Choose "3", and router reports current WAN port subnet mask 3. Input a new WAN port subnet mask and press # key: 4. Use "*" to replace ".", user can input 255*255*255*0 to set the new WAN port subnet mask 255.255.255.0 5. Press "#" key to indicate that you have finished 6. Report "operation successful" if user operation is ok. 7. To quit, enter "**".
(4) Gateway	1. Pick up phone and press "****" to start IVR 2. Choose "4", and the router reports current gateway 3. Input the new gateway and press "#" key: 4. Use "*" to replace ".", user can input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press "#" key to indicate that you have finished. 6. Report "operation successful" if user operation is ok. 7. To quit, press "**".

(5) DNS	1. Pick up phone and press “****” to start IVR 2. Choose “5”, and the router reports current DNS 3. Input the new DNS and press # key: 4. Use “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press “#” key to indicate that you have finished.
2 Phone port configuration	1. Pick up phone and press “****” to start IVR 2. Select "2", then the device will continue to broadcast prompts the user to select current phone number; 2. registration server address; 3. registration port; 4. call forwarding configuration，5. DNS configuration ; 3. Continue pressing "1" and the unit will continue to broadcast the phone number of the current phone port. The device will then broadcast "1. Phone number ..." again.
3 Factory Reset	1. Pick up phone and press “****” to start IVR 2. Choose “3”, and the router reports “Factory Reset” 3. Prompt "Please enter password", the method of inputting password is the same as operation 1. 4. If you want to quit, press “*”. 5. Prompt “operation successful” if password is right and then the router will be in factory default configuration.
4 Reboot	1. Pick up phone and press “****” to start IVR 2. Choose “4”, and the router reports “Reboot” 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. the router reboots if password is right and operation
5 WAN Port Login	1. Pick up phone and press “****” to start IVR 2. Choose “5”, and the router reports “WAN Port Login” 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. If user wants to quit, press “*”.

6 WEB Access Port	1. Pick up phone and press “****” to start IVR 2. Choose “6”, and the router reports “ WEB Access Port” 3. Prompt “Please enter password”, the method of inputting password is same as operation 1. 4. Report “operation successful” if user operation is ok. 5. Report the current WEB Access Port
7 Firmware Version	1. Pick up phone and press “****” to start IVR 2. Choose “7” and the router reports the current Firmware version

Note

1.While using Voice menu, press * (star) to return to the main menu.

2.If any changes are made in the IP assignment mode, the router must be rebooted in order for the settings to take effect.

3.While entering an IP address or subnet mask, use "*" (star) to enter "." (Dot) and use "#" (hash) key to finish entering IP address or subnet mask:

4.For example, to enter the IP address 192.168.20.159 by keypad, press these keys: 192*168*20*159, use the #(hash) key to indicate that you have finished entering the IP address.

5.Use the # (hash) key to indicate that you have finish entering the IP address or subnet mask

6.While assigning an IP address in Static IP mode, setting the IP address, subnet mask and default gateway is required to complete the configuration. If in DHCP mode, please make sure that a DHCP server is available in your existing broadband connection to which WAN port of AC1000M/AC1000MS/AC1300MS is connected.

7.The default LAN port IP address of the AC1000M/AC1000MS/AC1300MS is 192.168.11.1 and this address should not be assigned to the WAN port IP address of the AC1000M/AC1000MS/AC1300MS in the same network segment of LAN port.

8.The password can be entered using phone keypad, the mapping 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’,

Chapter 2 Basic Settings

This chapter covers:

- Two-Level Management
- Web Management Interface
- Configuring
- Making a Call

Two-Level Management

This section explains how to setup a password for an administrator or user and how to adjust basic and advanced settings.

AC1000M/AC1000MS/AC1300MS supports two-level management:

(1) administrator mode operation: please type “admin/admin” on Username/Password and click Login button to begin configuration.

(2) user mode operation, please type “user/user” on Username/Password and click Login button to begin configuration.

Web Management Interface

The devices feature a web browser-based interface that may be used to configure and manage the device. See below for information

Login in from the LAN port

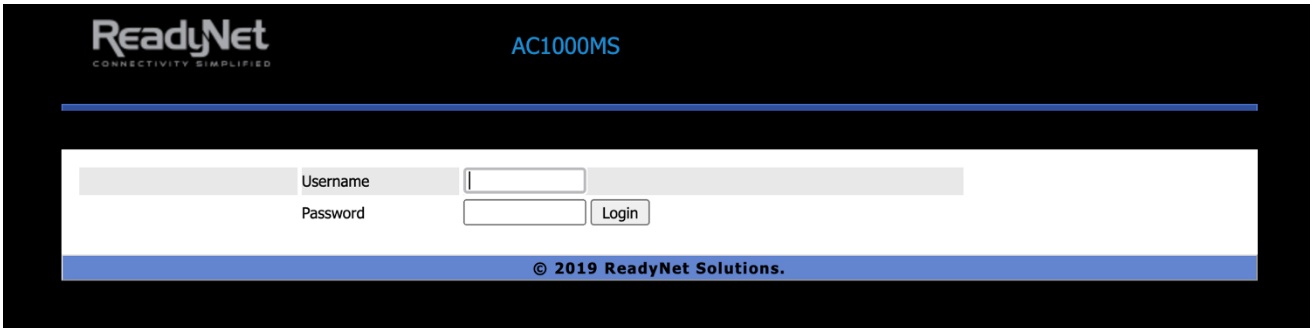
1. Ensure your PC is connected to the router’s LAN port correctly.

Note

You may either set up your PC to get an IP dynamically from the router or set up the IP address of the PC to be the same subnet as the default IP address of router is 192.168.11.1. For detailed information, see Chapter 5: Troubleshooting Guide.

2. Open a web browser on your PC and type “http://192.168.11.1”.

3. The following window appears and prompts for username, password.



4. For administrator mode operation, please type admin/admin on Username/Password and click Login to begin configuration.

5. For user mode operation, please type user/user on Username/Password and click Login to begin configuration.

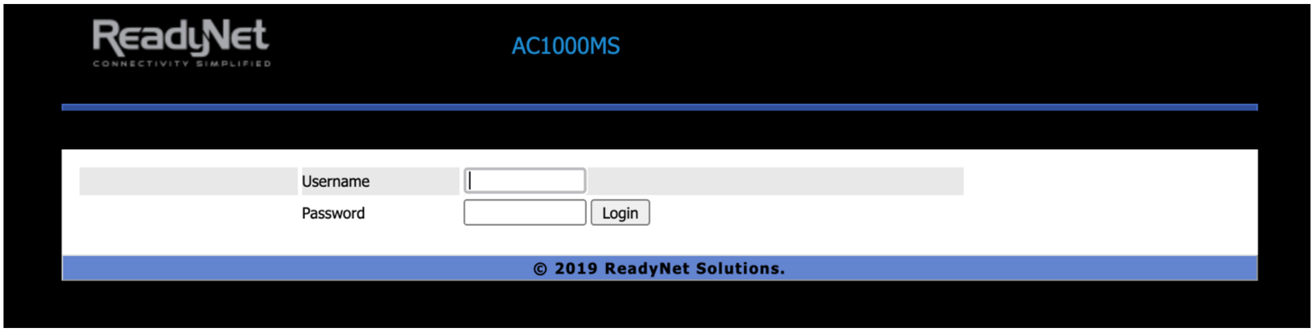
Note

If you are unable to access the web configuration, please see Chapter 5 Troubleshooting Guide for more information.

6.The web management interface automatically logs out the user after 5 minutes of inactivity.

Login in from the WAN port

1. Ensure your PC is connected to the router’s WAN port correctly.
2. Obtain the IP addresses of WAN port using Voice prompt or by logging into the device web management interface via a LAN port and navigating to Network > WAN.
3. Open a web browser on your PC and type http://<IP address of WAN port>. The following login page will be opened to enter username and password.



4. For administrator mode operation, type admin/admin on Username/Password and click Login to begin configuration.
5. For user mode operation, type user/user on Username/Password and click Login to begin configuration.

Note

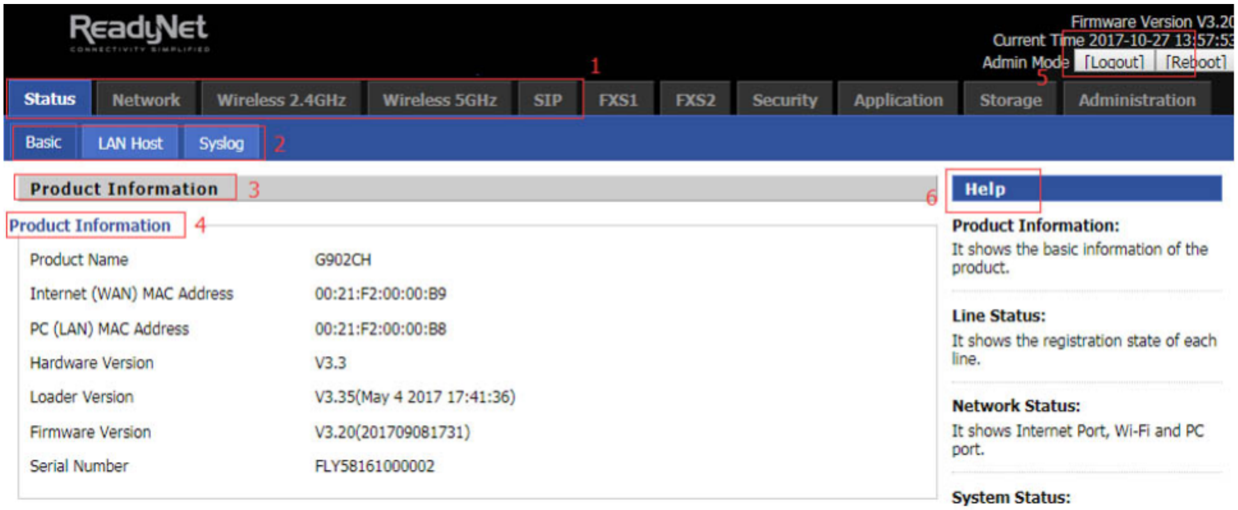
If you fail to access to the web configuration, see Chapter 5 Troubleshooting Guide for more information.

6. The web management interface automatically logs out the user after 5 minutes of inactivity.

Web Management Interface Details

Status

Table 5 Web management interface



Firmware Version V3.20
Current Time 2017-10-27 13:57:53
Admin Mode [Logout] [Reboot]

Product Information

Product Information

Product Name	G902CH
Internet (WAN) MAC Address	00:21:F2:00:00:B9
PC (LAN) MAC Address	00:21:F2:00:00:B8
Hardware Version	V3.3
Loader Version	V3.35(May 4 2017 17:41:36)
Firmware Version	V3.20(201709081731)
Serial Number	FLY58161000002

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

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

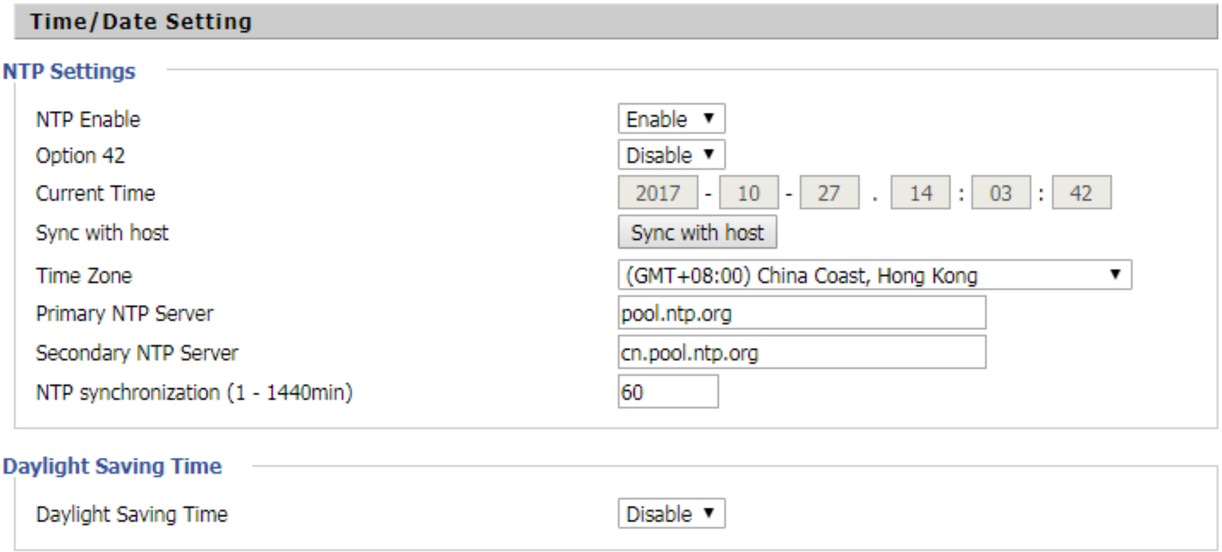
Network Status:
It shows Internet Port, Wi-Fi and PC port.

System Status:

Serial number	Name	Description
Position 1	Main navigation bar	Click this navigation bar to bring up the corresponding child navigation bar
Position 2	navigation bar	Click the sub navigation bar to enter the configuration page
Position 3	Product Information	Device Information Configuration Title
Position 4	Product Information	Show product information
Position 5	Login/Logout	main information shows the firmware version, DSP version, current time and management mode.
Position 6	Help	help to display help information, users can get some help here
	Save & Apply	Use this button, config will be saved and take effect immediately
	Save	After changing the parameters, you need to click this button to save. After you click Save, there is a need to restart the device.
	Cancel	Click to cancel the change
	Reboot	Click to restart
	Refresh	Refresh current page

Setting the Time Zone

Table 6 Setting time zone



Time/Date Setting

NTP Settings

NTP Enable	Enable ▼
Option 42	Disable ▼
Current Time	2017 - 10 - 27 . 14 : 03 : 42
Sync with host	Sync with host
Time Zone	(GMT+08:00) China Coast, Hong Kong ▼
Primary NTP Server	pool.ntp.org
Secondary NTP Server	cn.pool.ntp.org
NTP synchronization (1 - 1440min)	60

Daylight Saving Time

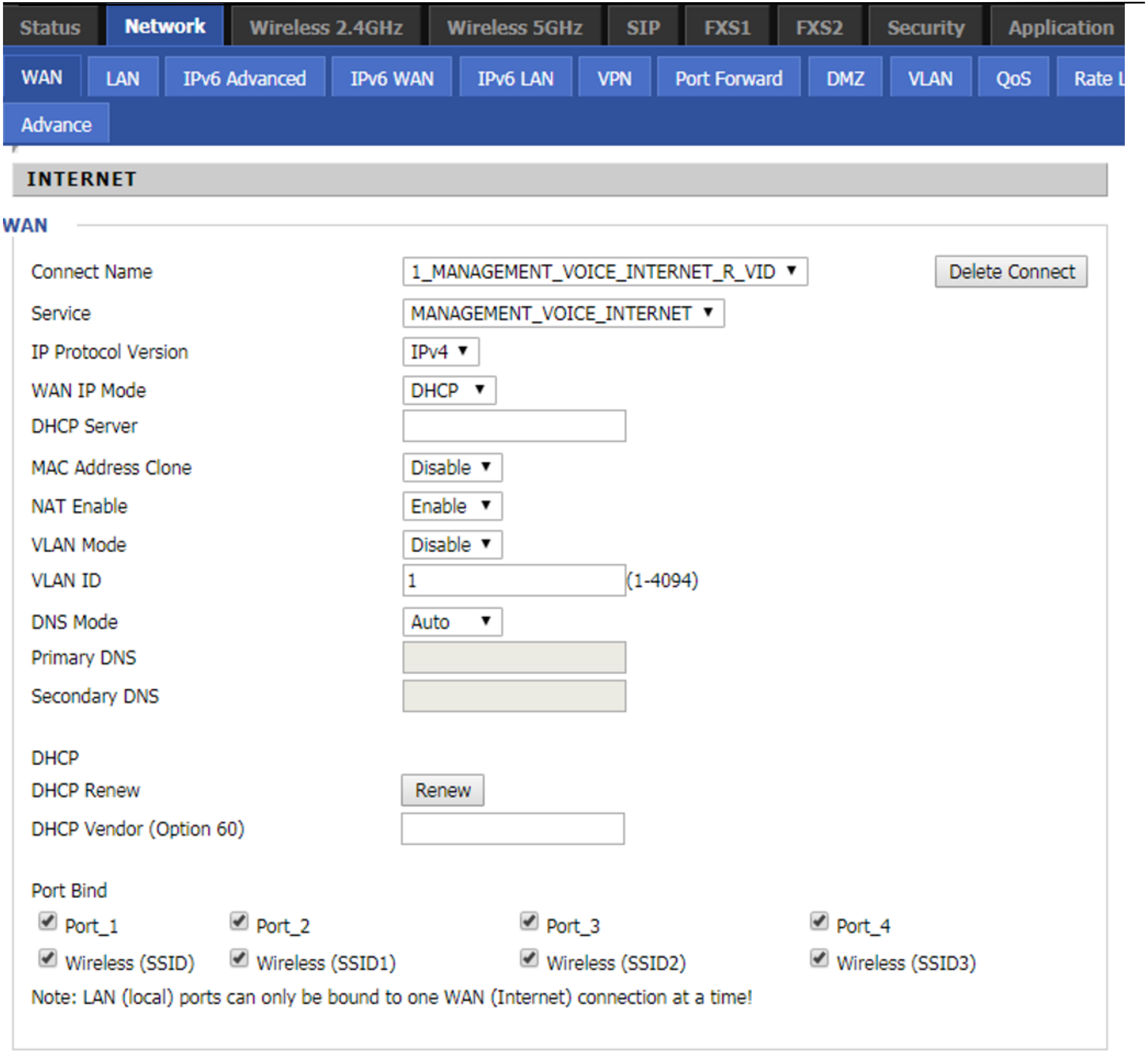
Daylight Saving Time	Disable ▼

Field Name	Description
NTP Enable	Enable NTP (Network Time Protocol) to automatically retrieve time and date settings for the device
Option 42	Whether to enable Option 42
Current Time	When NTP Enable is set to "Disable", manually configure the time and date via the Current Time parameter
Sync with host	Press Sync with host button to synchronize the host PC date, time and time zone.
Time Zone	Select the desired time zone
Primary NTP Server	Primary and secondary NTP server address for clock synchronization. A valid NTP server must be reachable for full NTP
Secondary NTP Server	
NTP Synchronization(1 - 1440min)	The synchronization period with NTP (1-1440 minutes), default is 60

Configuring an Internet Connection

From the Network > WAN page, WAN connections may be inserted or deleted. For more information on Internet Connection setting, see Table 10 below.

Table 7 Configuring an internet connection



INTERNET

WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼
Service	MANAGEMENT_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	DHCP ▼
DHCP Server	
MAC Address Clone	Disable ▼
NAT Enable	Enable ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)
DNS Mode	Auto ▼
Primary DNS	
Secondary DNS	

DHCP

DHCP Renew	Renew
DHCP Vendor (Option 60)	

Port Bind

☑ Port_1	☑ Port_2	☑ Port_3	☑ Port_4
☑ Wireless (SSID)	☑ Wireless (SSID1)	☑ Wireless (SSID2)	☑ Wireless (SSID3)

Note: LAN (local) ports can only be bound to one WAN (Internet) connection at a time!

Field Name	Description
Connect Name	Use keywords to indicate WAN port service model (the parameters are defined in Network--> multi-WAN page)
Service	Chose the service mode for the created connection
IP Protocol Version	IPv4 and IPv6 are supported
WAN IP Mode	Choose Internet connection mode, DHCP, PPPoE, or Bridge
NAT Enable	Enable or disable NAT
VLAN ID	Multiple WAN connections may be created with the same VLAN ID
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. 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
DHCP	**(Displayed when WAN IP Mode is set to DHCP)**
DHCP Renew	Refresh the DHCP IP
DHCP Vendor	Specify the DHCP Vendor field Display the vendor and product name

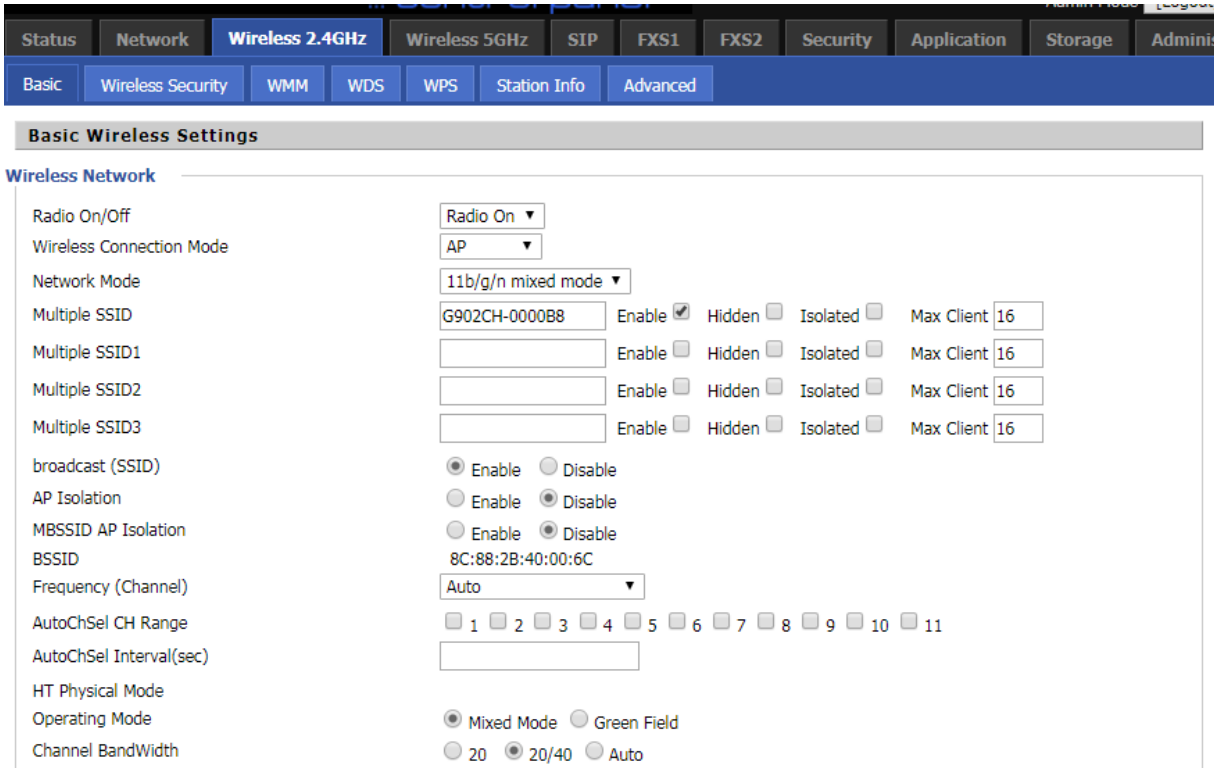
Setting up Wireless Connections

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

1.Enable Wireless and Setting SSID

2.Open Wireless > Basic webpage as shown below:

Table 8 Wireless > Basic web page (user view)



Basic Wireless Settings

Wireless Network

Radio On/Off	Radio On ▼
Wireless Connection Mode	AP ▼
Network Mode	11b/g/n mixed mode ▼
Multiple SSID	G902CH-0000B8 Enable ☑ Hidden □ Isolated □ Max Client 16
Multiple SSID1	Enable □ Hidden □ Isolated □ Max Client 16
Multiple SSID2	Enable □ Hidden □ Isolated □ Max Client 16
Multiple SSID3	Enable □ Hidden □ Isolated □ Max Client 16
broadcast (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	8C:88:2B:40:00:6C
Frequency (Channel)	Auto ▼
AutoChSel CH Range	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11
AutoChSel Interval(sec)	
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40 ○ Auto

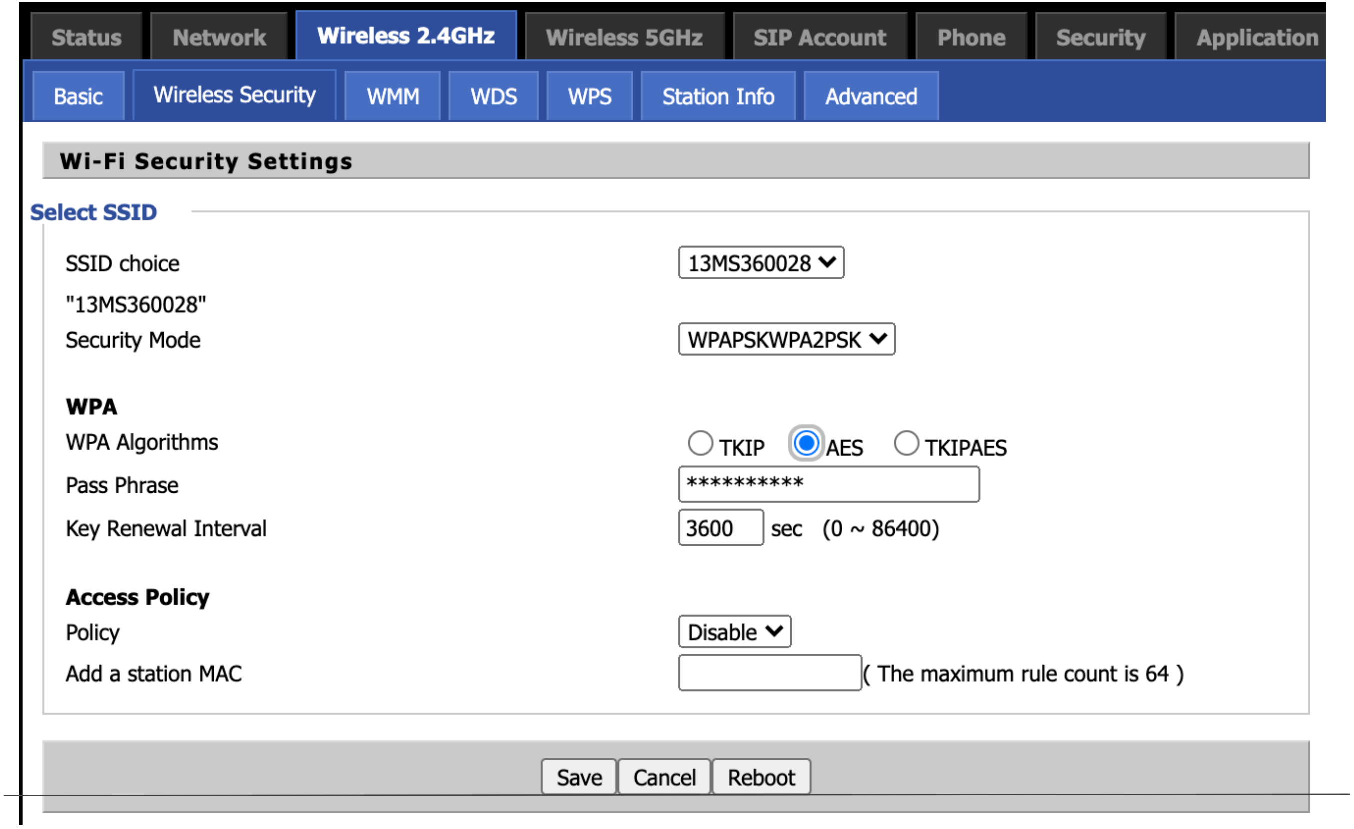
Field Name	Description
Radio On/Off	Select “Radio Off” to disable wireless operation Select “Radio On” to enable wireless operation Please note: “Save” required for this parameter change
Network Mode	Choose one network mode from the drop down list.
SSID	The logical name of the wireless connection (text, numbers or various special characters)
Multiple SSID 1-4	Multiple SSID 1 - 4, configure up to 4 unique SSIDs
broadcast(SSID)	Enabled: The device SSID is broadcast at regular intervals Disabled: The device SSID is not broadcast at regular intervals, disallowing wi-fi clients from automatically connecting to the AC1000M/AC1000MS/AC1300MS
AP Isolation	Enabled: Devices connected to the router are isolated from one another on virtual networks Disabled: Devices connected to the router are visible on the network to each other

MBSSID AP Isolation	Enabled: Devices connected to the router via one of the Multiple SSIDs are isolated from one another on virtual networks Disabled: Devices connected to the router via one of the Multiple SSIDs are visible on
BSSID	Basic Service Set Identifier – AP MAC Address Listing
Frequency (Channel)	Select the channel of operation for the device from the drop-down list
Operating Mode	Mixed Mode: Packet preamble (only) is transmitted in a format compatible with legacy 802.11a/g (for 802.11a/g receivers). Green Field: High throughput packet preambles do not contain legacy formatting
Channel Bandwidth	20: the device operates with a 20 MHz channel size 20/40: the device operates with a 40 MHz channel size

Encryption

Open Wireless/Wireless Security webpage to configure custom security parameters.

Table 9 Wireless Security web page



Wi-Fi Security Settings

Select SSID

SSID choice	13MS360028
"13MS360028"	
Security Mode	WPAPSKWPA2PSK
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	**********
Key Renewal Interval	3600 sec (0 ~ 86400)
Access Policy	
Policy	Disable
Add a station MAC	(The maximum rule count is 64)

Field Name	Description
SSID Choice	Choose the SSID from the drop-drown list for which security will be configured
Security Mode	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets. Each encryption mode will launch an additional web page and ask you to offer additional configuration. For high security, the device can be configured for Security Mode as WPA2-PSK and WPA Algorithms as AES.
WPA Algorithms	This parameter is used to select the encryption of wireless home gateway algorithms; options are TKIP, AES and TKIPAES.
Pass Phrase	Configure the WPA-PSK security password.
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.
Access Policy	
Policy	Disable: Access policy rules are not enforced Allow: Only allow the clients in the station MAC list to access Rejected: Block the clients in the station MAC list from registering
Add a Station MAC	Enter the MAC address of the clients which you want to allow or reject

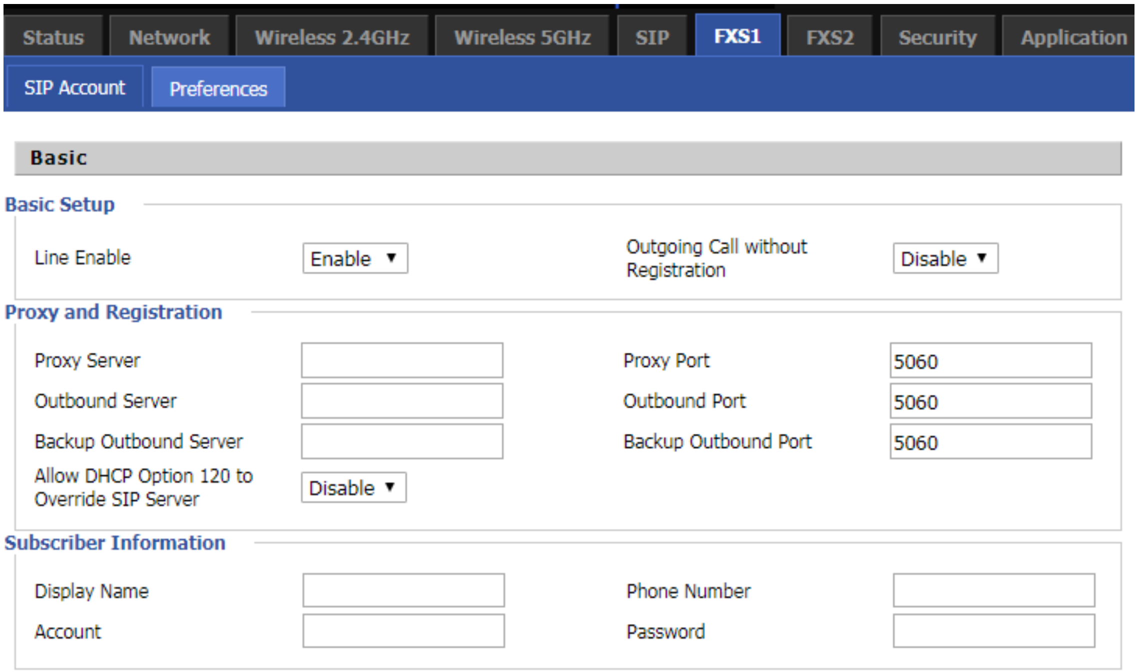
Configuring Session Initiation Protocol

SIP Accounts

AC1000M/AC1000MS/AC1300MS have 1 Line to make SIP (Session Initiation Protocol) calls. Before registering, the device user should have a SIP account configured by the system administrator or provider. See the section below for more information.

Configuring SIP the Web Management Interface

Table 10 Configuring SIP the Web Management Interface



Basic

Basic Setup

Line Enable	Enable ▼	Outgoing Call without Registration	Disable ▼

Proxy and Registration

Proxy Server		Proxy Port	5060
Outbound Server		Outbound Port	5060
Backup Outbound Server		Backup Outbound Port	5060
Allow DHCP Option 120 to Override SIP Server	Disable ▼		

Subscriber Information

Display Name		Phone Number	
Account		Password	

Procedure

1. Open the Line1/SIP Account webpage, as illustrated above.

2. Fill the SIP Server address and SIP Server port number (from administrator or provider) into Proxy Server Name and into Proxy Port parameters.

3. Fill account details received from your administrator into Display Name, Phone Number and Account details.

4. Type the password received from your administrator into the Password parameter.

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

Note

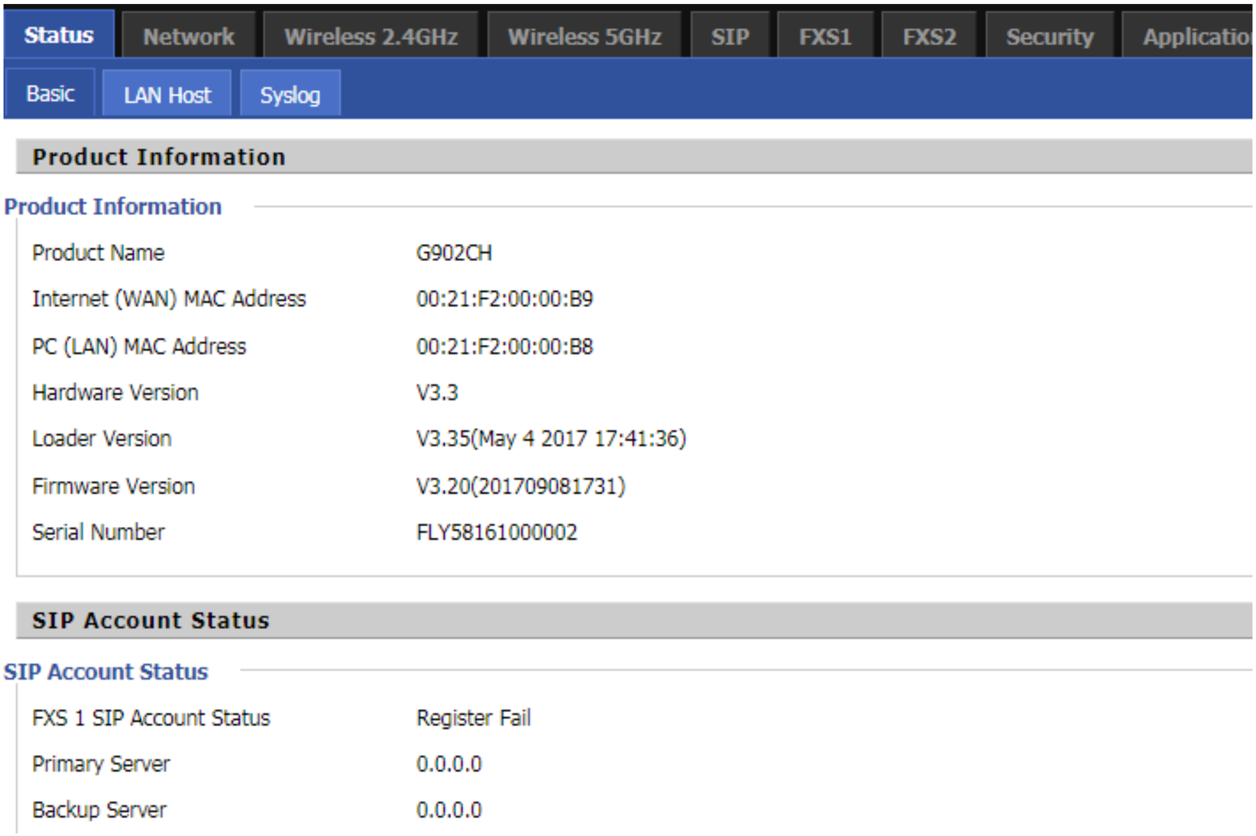
Upon the following dialogue:

Please REBOOT to make the changes effective!

Please press Reboot button to make changes effective.

Viewing the Registration Status

Table 11 Registration status



Product Information

Product Information

Product Name	G902CH
Internet (WAN) MAC Address	00:21:F2:00:00:B9
PC (LAN) MAC Address	00:21:F2:00:00:B8
Hardware Version	V3.3
Loader Version	V3.35(May 4 2017 17:41:36)
Firmware Version	V3.20(201709081731)
Serial Number	FLY58161000002

SIP Account Status

SIP Account Status

FXS 1 SIP Account Status	Register Fail
Primary Server	0.0.0.0
Backup Server	0.0.0.0

Procedure
To view the SIP account status of device, open the Status webpage and view the value of registration status.

Making a Call

Calling phone or extension numbers

To make a phone or extension number call:

- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) must have public IP addresses, or
- 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
- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) can be connected through a router using a 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 #.

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:

- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) have public IP addresses, or
- 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
- 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 "#".

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.

Blind Transfer

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

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.

A can hang up.

Attended Transfer

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

Party A dials "*77" to hold the party B, when hear the dial tone, A dials C's number, then party A and party C are in conversation.

Party A dials "*78" to transfer to C, then B and C now in conversation.

If the transfer is not completed successfully, then A and B are in conversation again.

Conference

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

Party A dials "*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.

Party A dials "*88" to add C, then A and B, for conference.

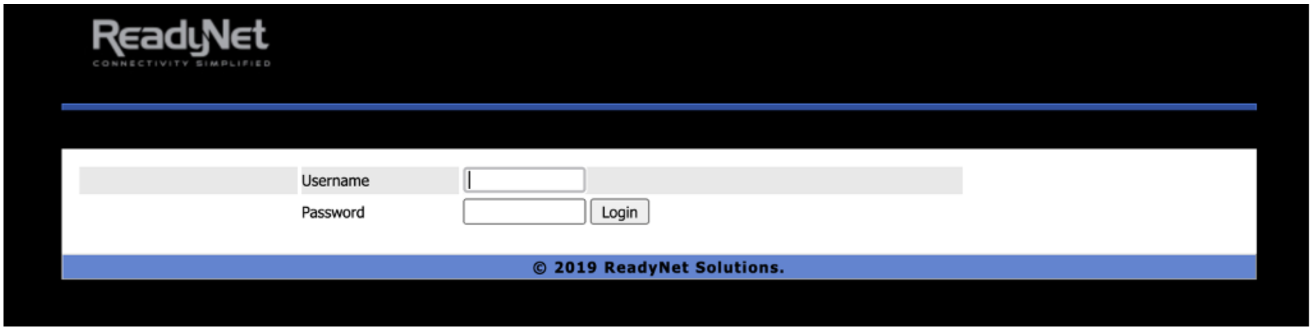
Chapter 3 Web Interface

This chapter guides users to execute advanced (full) configuration through admin mode operation. This chapter covers:

- Login
- Status
- Network and Security
- Wireless
- SIP
- FXS1
- Security
- Application
- Administration
- Management
- System Log
- Logout
- Reboot

Login

Table 12 Login details

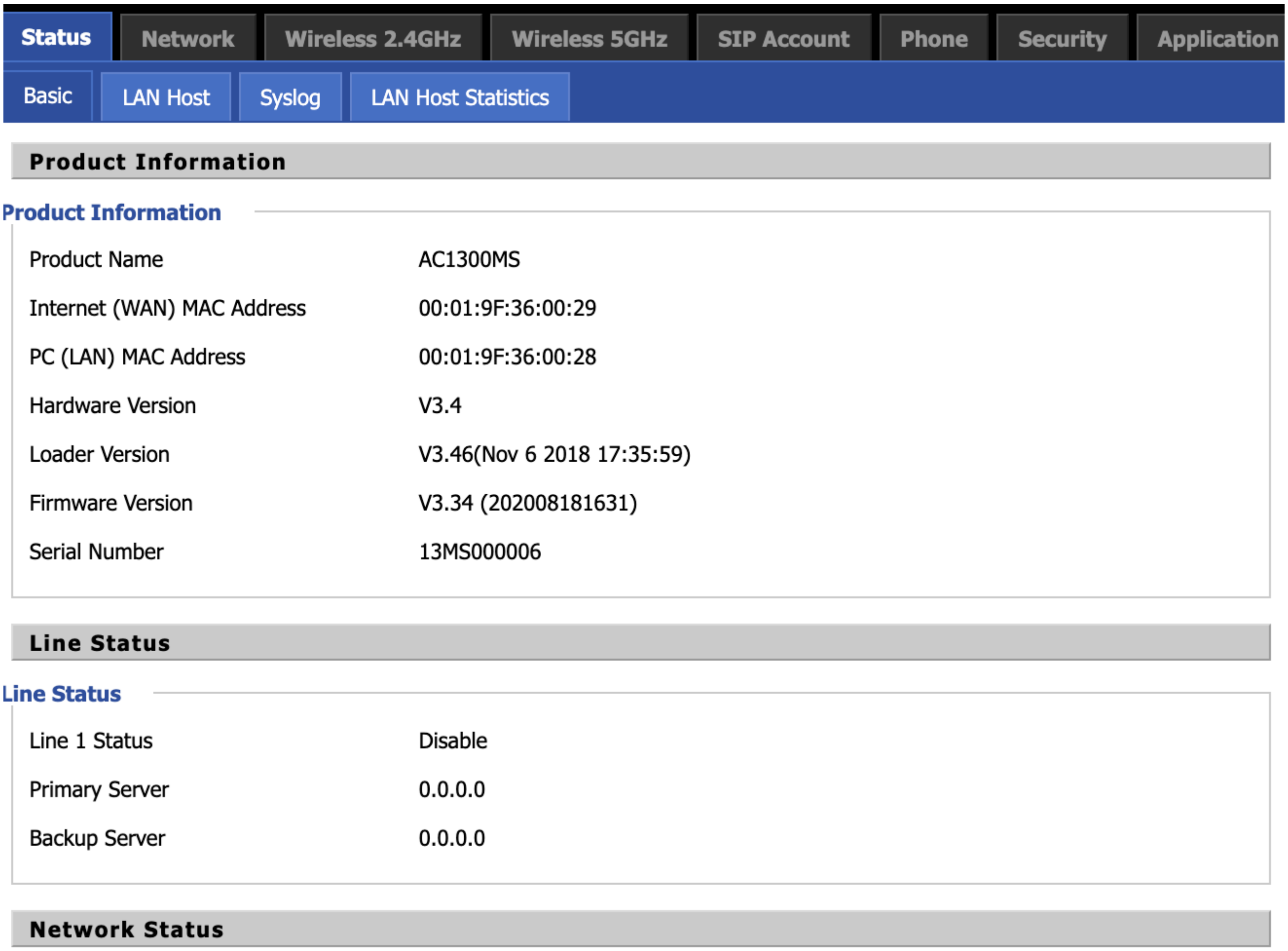


Procedure
1. Connect the LAN port of the router to your PC an Ethernet cable
2. Open a web browser on your PC and type http://192.168.11.1.
3. Enter Username admin and Password admin.
4. Click Login

Status

This webpage shows the status information about the Product, Network, SIP Account Status, FXS Port Status, Network Status, Wireless Info and System Status

Table 13 Status



Product Information

Product Information

Product Name	AC1300MS
Internet (WAN) MAC Address	00:01:9F:36:00:29
PC (LAN) MAC Address	00:01:9F:36:00:28
Hardware Version	V3.4
Loader Version	V3.46(Nov 6 2018 17:35:59)
Firmware Version	V3.34 (202008181631)
Serial Number	13MS000006

Line Status

Line Status

Line 1 Status	Disable
Primary Server	0.0.0.0
Backup Server	0.0.0.0

Network Status

Network and Security

You can configure the WAN port, LAN port, DDNS, Multi WAN, DMZ, MAC Clone, Port Forward and other parameters in this section of the web management interface.

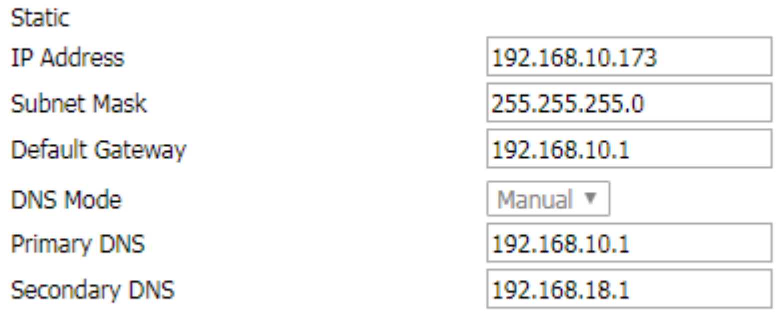
WAN

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.

Static IP

This configuration may be utilized when a user receives a fixed public IP address or a public subnet, namely multiple public IP addresses from the Internet 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 can assign an IP address to the WAN interface.

Table 14 Internet



Static

IP Address	192.168.10.173
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Mode	Manual ▼
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1

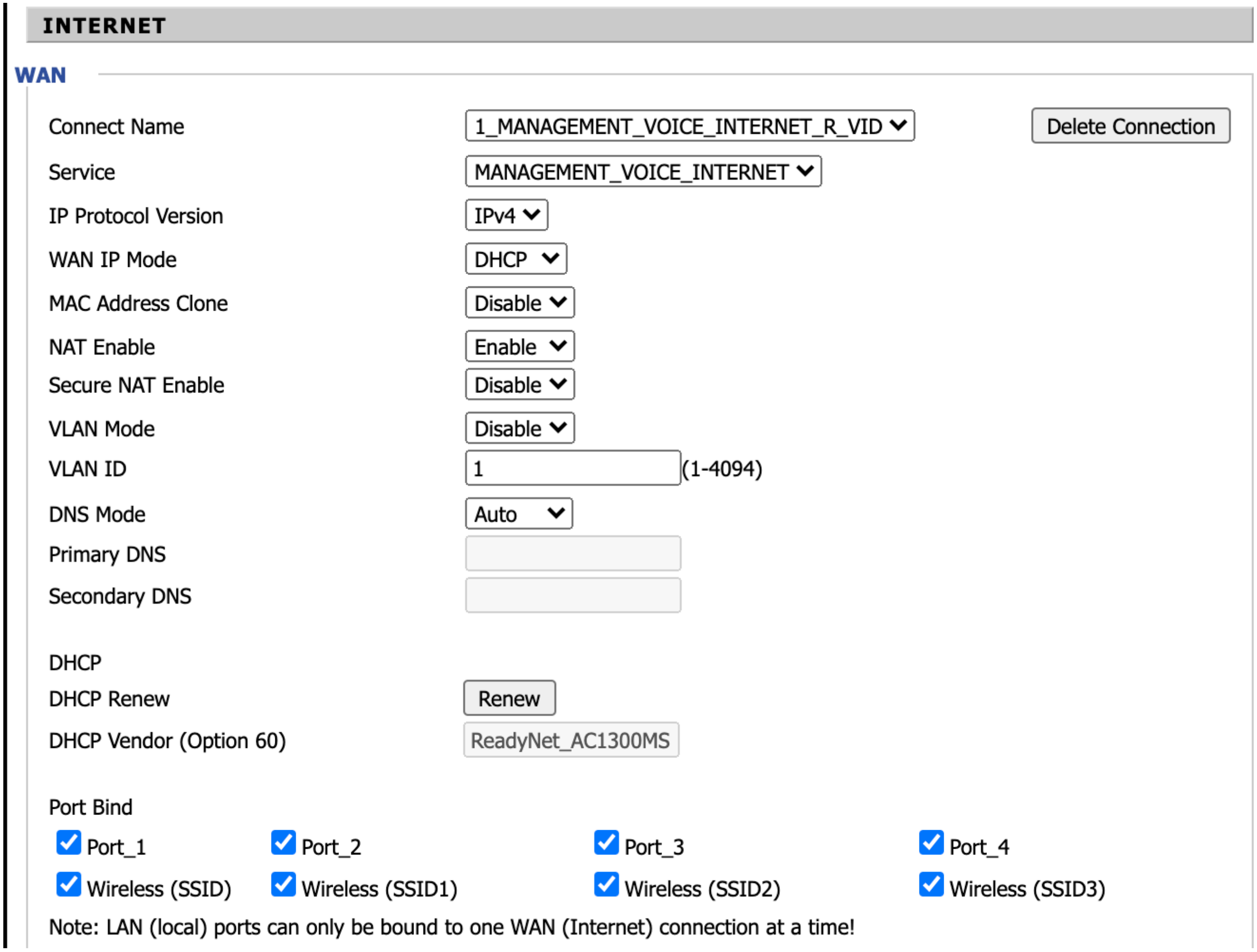
Field Name	Descripti
IP Address	The IP address of Internet port
Subnet Mask	The subnet mask of Internet port
Default Gateway	The default gateway of Internet port
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user manually configures the preferred DNS and alternate DNS information
Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port

DHCP

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

The DHCP feature allows to the router to obtain an IP address automatically from a DHCP server. In this case, it is not necessary to assign an IP address to the client manually.

Table 15 DHCP



INTERNET

WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID	Delete Connection
Service	MANAGEMENT_VOICE_INTERNET	
IP Protocol Version	IPv4	
WAN IP Mode	DHCP	
MAC Address Clone	Disable	
NAT Enable	Enable	
Secure NAT Enable	Disable	
VLAN Mode	Disable	
VLAN ID	1 (1-4094)	
DNS Mode	Auto	
Primary DNS		
Secondary DNS		
DHCP		
DHCP Renew	Renew	
DHCP Vendor (Option 60)	ReadyNet_AC1300MS	

Port Bind

☑ Port_1 ☑ Port_2 ☑ Port_3 ☑ Port_4

☑ Wireless (SSID) ☑ Wireless (SSID1) ☑ Wireless (SSID2) ☑ Wireless (SSID3)

Note: LAN (local) ports can only be bound to one WAN (Internet) connection at a time!

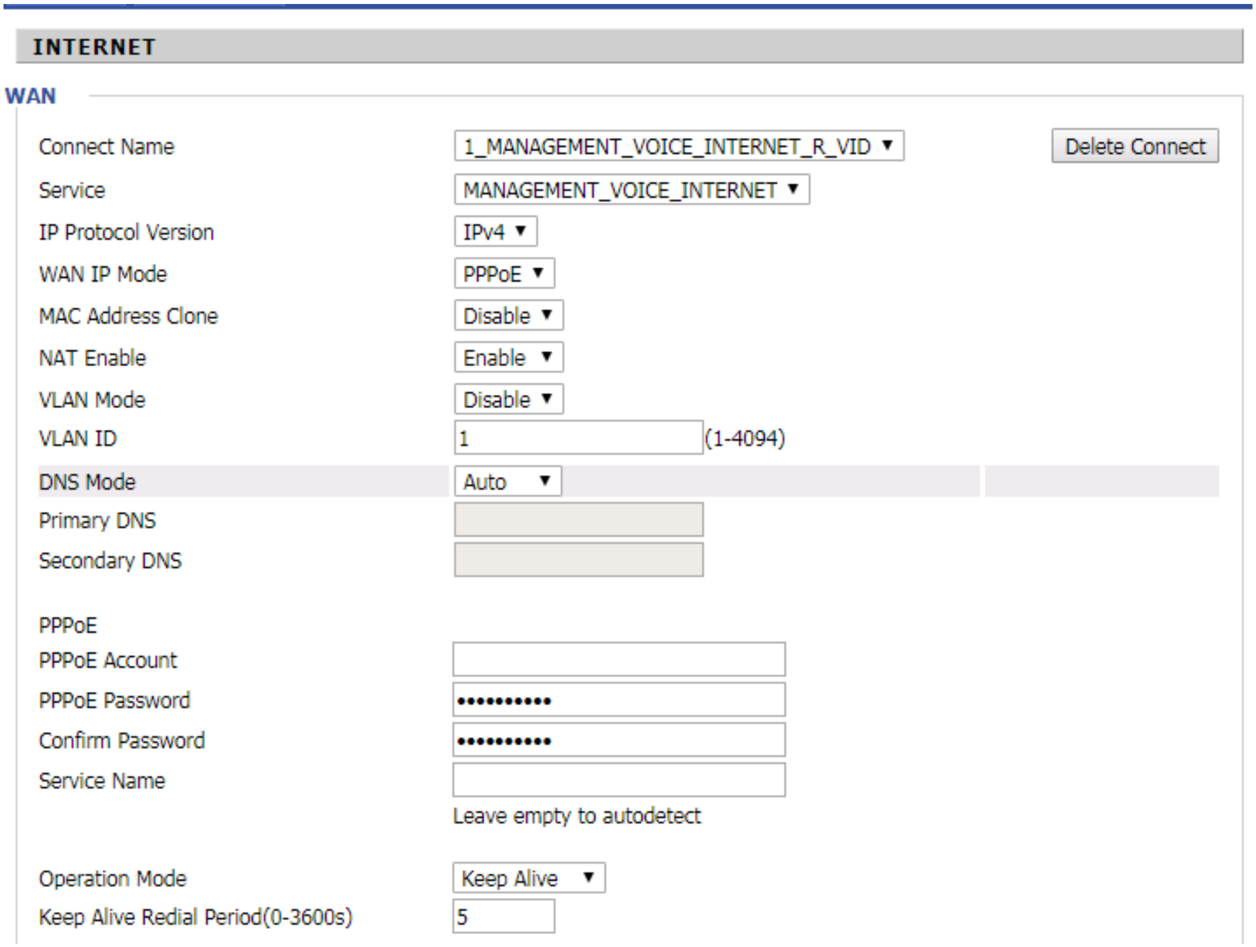
Field Name	Description
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. When DNS mode is Manual, the user should manually configure the
Primary DNS Address	Primary DNS of Internet port.
Secondary DNS Address	Secondary DNS of Internet port.
DHCP Renew	Refresh the DHCP IP address
DHCP Vendor (Option60)	Specify the DHCP Vendor field. Display the vendor and product name.

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.

Table 16 PPPoE



INTERNET

WAN

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

Field Name	Description
PPPoE Account	Enter a valid user name provided by the ISP

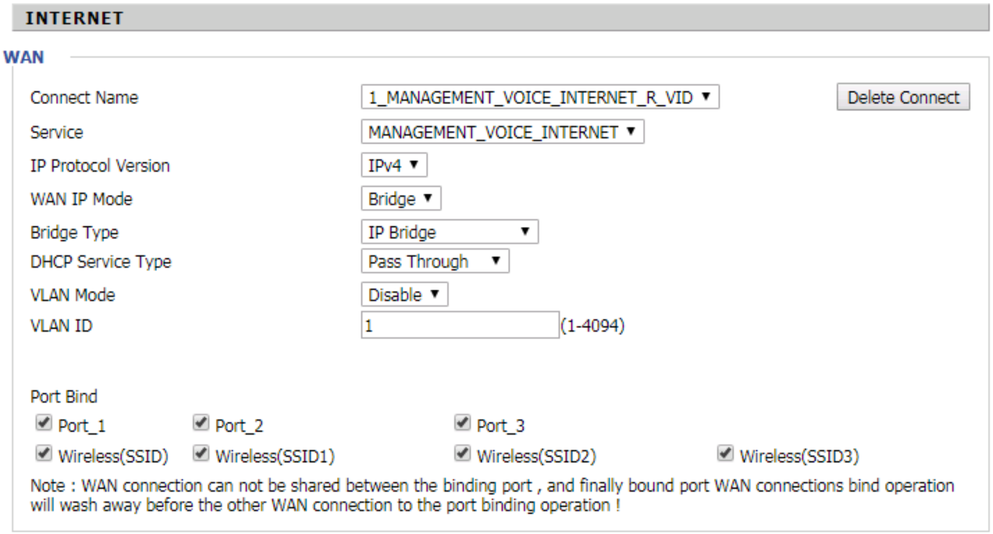
PPPoE Password	Enter a valid password provided by the ISP. The password can contain special characters and allowed special characters are $, +, *, #, @ and ! For example, the password can be entered as #net123@IT!$+*.

Confirm Password	Enter your PPPoE password again
Service Name	Enter a service name for PPPoE authentication. If it is left empty, the service name is auto detected.
Operation Mode	Select the mode of operation, options are Keep Alive, On Demand and Manual: When the mode is Keep Alive, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; When the mode is On Demand, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; Operation Mode: On Demand On Demand Idle Time(0-60m): 5 When the mode is Manual, there are no additional settings to configure
Keep Alive Redial	Set the interval to send Keep Alive messaging
PPPoE Account	Assign a valid user name provided by the ISP

Bridge Mode

Bridge Mode under Multi WAN is different with traditional bridge setting. Bridge mode employs no IP addressing and the device operates as a bridge between the WAN port and the LAN port. Route Connection has to be built to give IP address to local service on device.

Table 17 Bridge Mode



INTERNET

WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID
Service	MANAGEMENT_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	Bridge
Bridge Type	IP Bridge
DHCP Service Type	Pass Through
VLAN Mode	Disable
VLAN ID	1 (1-4094)

Port Bind

☑ Port_1 ☑ Port_2 ☑ Port_3

☑ Wireless(SSID) ☑ Wireless(SSID1) ☑ Wireless(SSID2) ☑ Wireless(SSID3)

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 to pass. PC can connect to upper network directly.
PPPoE Bridge	Only Allow PPPoE packets pass. PC needs PPPoE dial-up software.
Hardware IP Bridge	Packets pass through hardware switch with wired speed. Does not support wireless port binding
DHCP Service Type	
Pass Through	DHCP packets can be forwarded between WAN and LAN, DHCP server in gateway will not allocate IP to clients 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 forwarding DHCP packet from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to clients of LAN port.
Local Service	Gateway will not forward DHCP packets between LAN and WAN, it also blocks DHCP packets from the WAN port. Clients connected to the 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, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN.
VLAN ID	Set the VLAN ID.
802.1p	Set the priority of VLAN, Options are 0~7.

Note

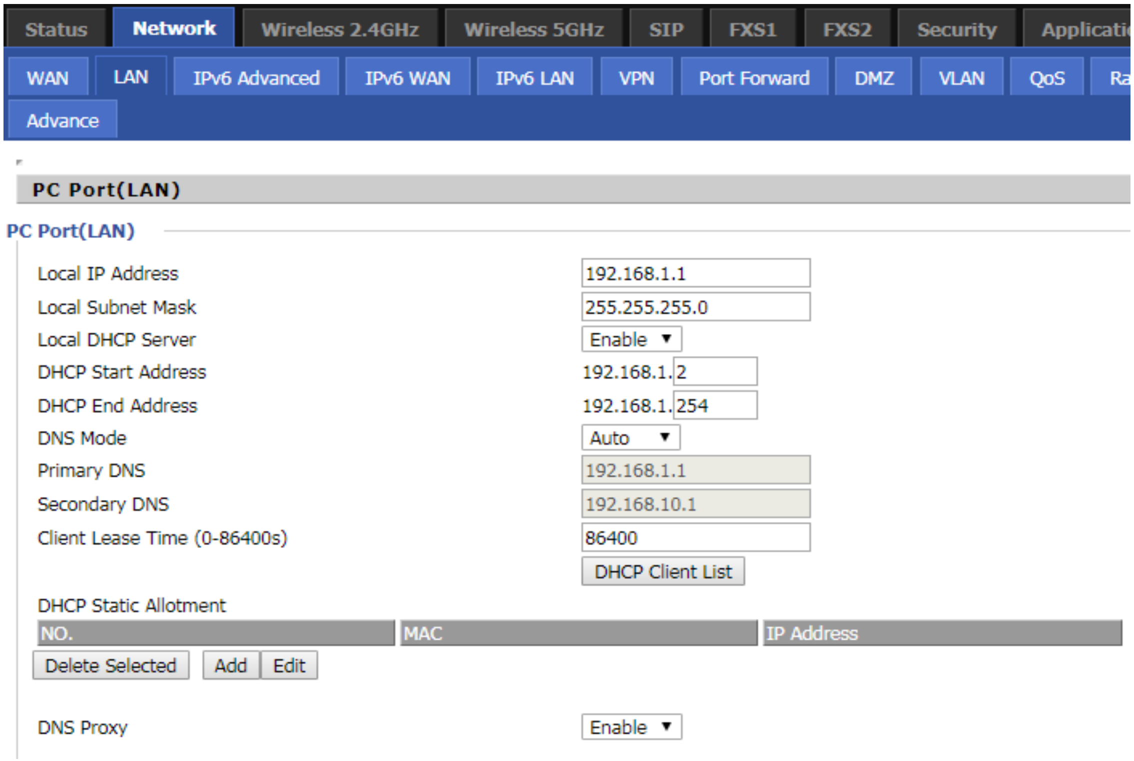
Multiple WAN connections may be created with the same VLAN ID

LAN

LAN Port

NAT translates the packets from public IP address to local IP address to forward packets to the proper destination.

Table 18 LAN port



PC Port(LAN)

PC Port(LAN)

Local IP Address	192.168.1.1
Local Subnet Mask	255.255.255.0
Local DHCP Server	Enable ▼
DHCP Start Address	192.168.1.2
DHCP End Address	192.168.1.254
DNS Mode	Auto ▼
Primary DNS	192.168.1.1
Secondary DNS	192.168.10.1
Client Lease Time (0-86400s)	86400

DHCP Static Allotment

NO.	MAC	IP Address

DNS Proxy	Enable ▼

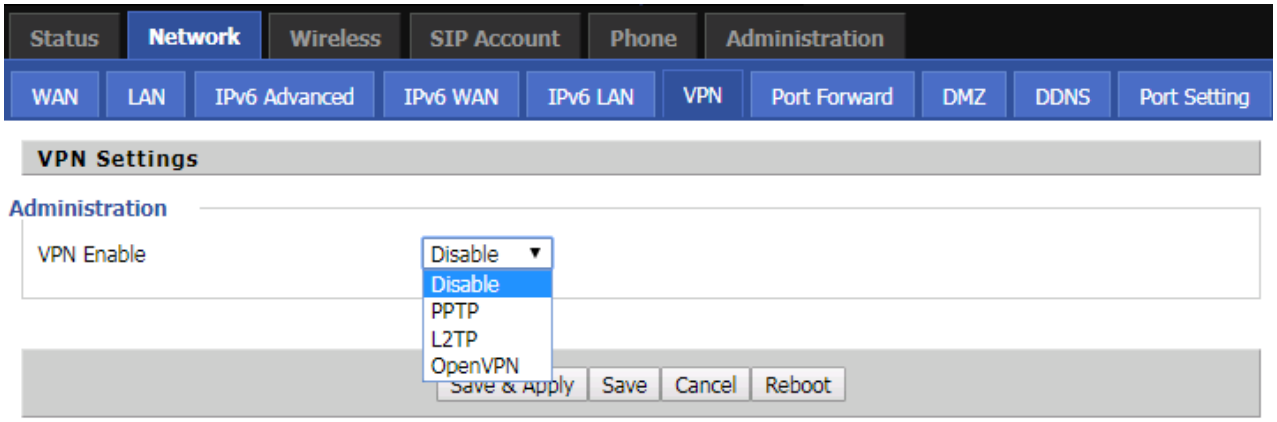
Field Name	Description
IP Address	Enter the IP address of the router on the local area network. All the IP addresses of the computers which are in the router's LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (The default is 192.168.11.1).
Local Subnet Mask	Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24).
Local DHCP Server	Enable/Disable 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 192.168.11.1, starting IP address can be 192.168.11.2 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: When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. 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.

VPN

The router supports VPN connections with PPTP-based VPN servers.

Table 19 VPN

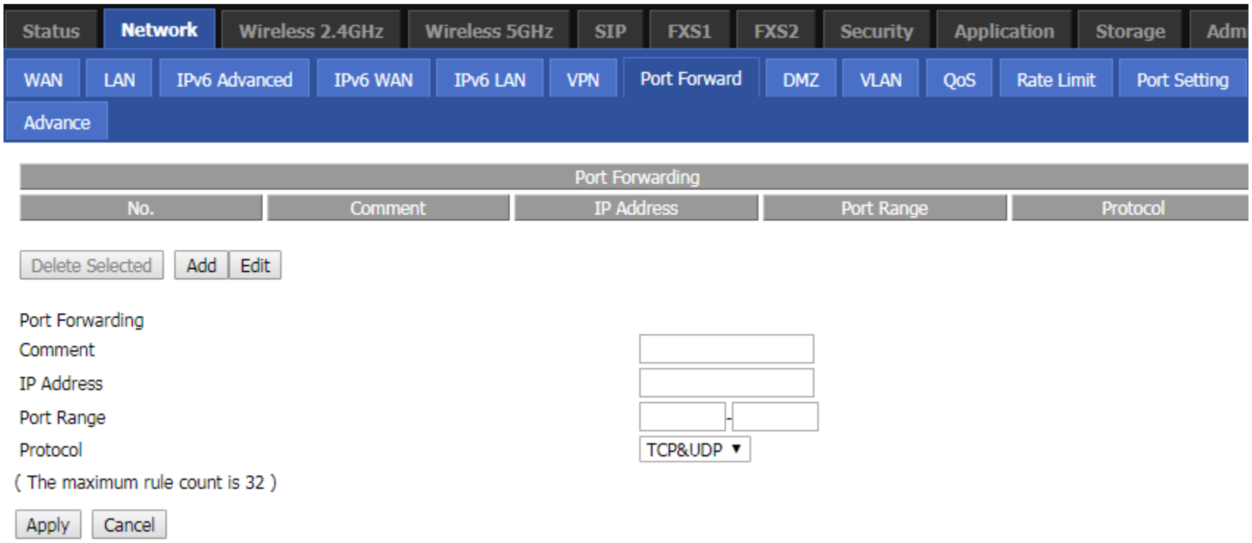


VPN Enable: Disable

Field Name	Description
VPN Enable	Enable/Disable VPN. If the VPN is enabled, user can select PPTP and L2TP mode VPN.
Initial Service IP	Enter VPN server IP address.
User Name	Enter authentication username.
Password	Enter authentication password.

Port Forward

Table 20 Port Forward



Port Forwarding

No.	Comment	IP Address	Port Range	Protocol

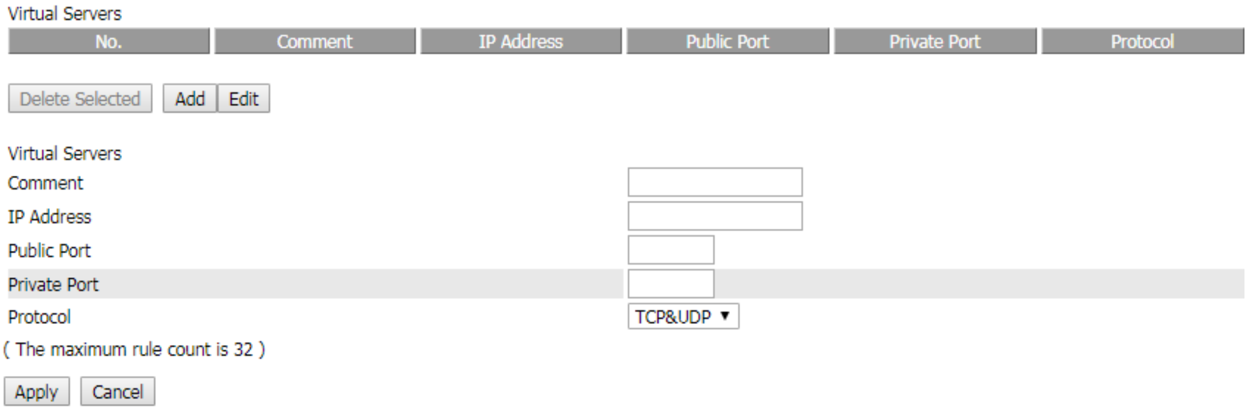
Port Forwarding

Comment	
IP Address	
Port Range	-
Protocol	TCP&UDP ▼

(The maximum rule count is 32)

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.

Table 21 Virtual Servers



Virtual Servers

No.	Comment	IP Address	Public Port	Private Port	Protocol

Virtual Servers

Comment	
IP Address	
Public Port	
Private Port	
Protocol	TCP&UDP ▼

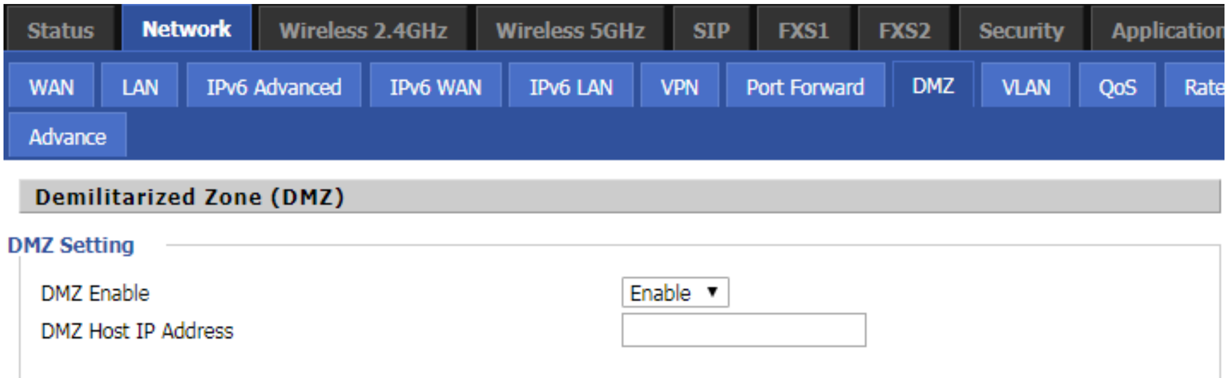
(The maximum rule count is 32)

Field Name	Description
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.

DMZ

Table 22 DMZ



Demilitarized Zone (DMZ)

DMZ Setting

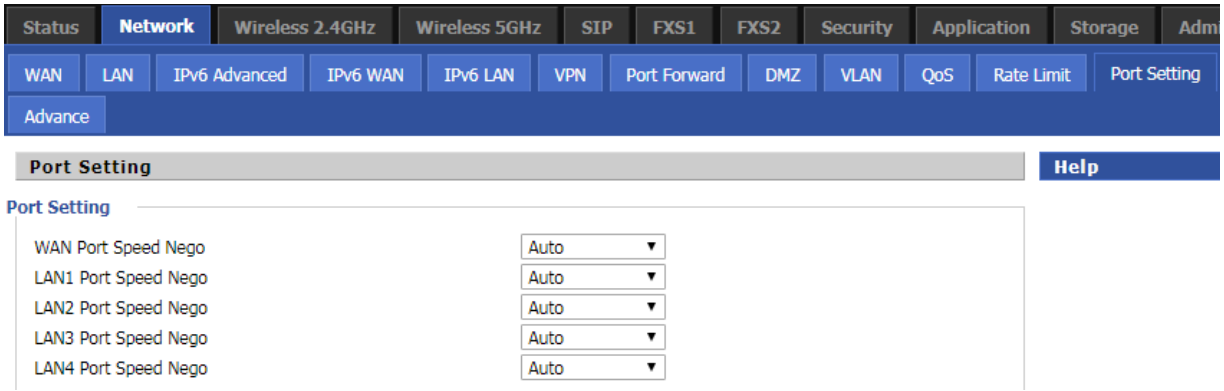
DMZ Enable: Enable ▼

DMZ Host IP Address:

Field Name	Description
DMZ Enable	Enable/Disable DMZ.
DMZ Host IP Address	Enter the private IP address of the DMZ host.

Port Setting

Table 23 Port setting



Port Setting

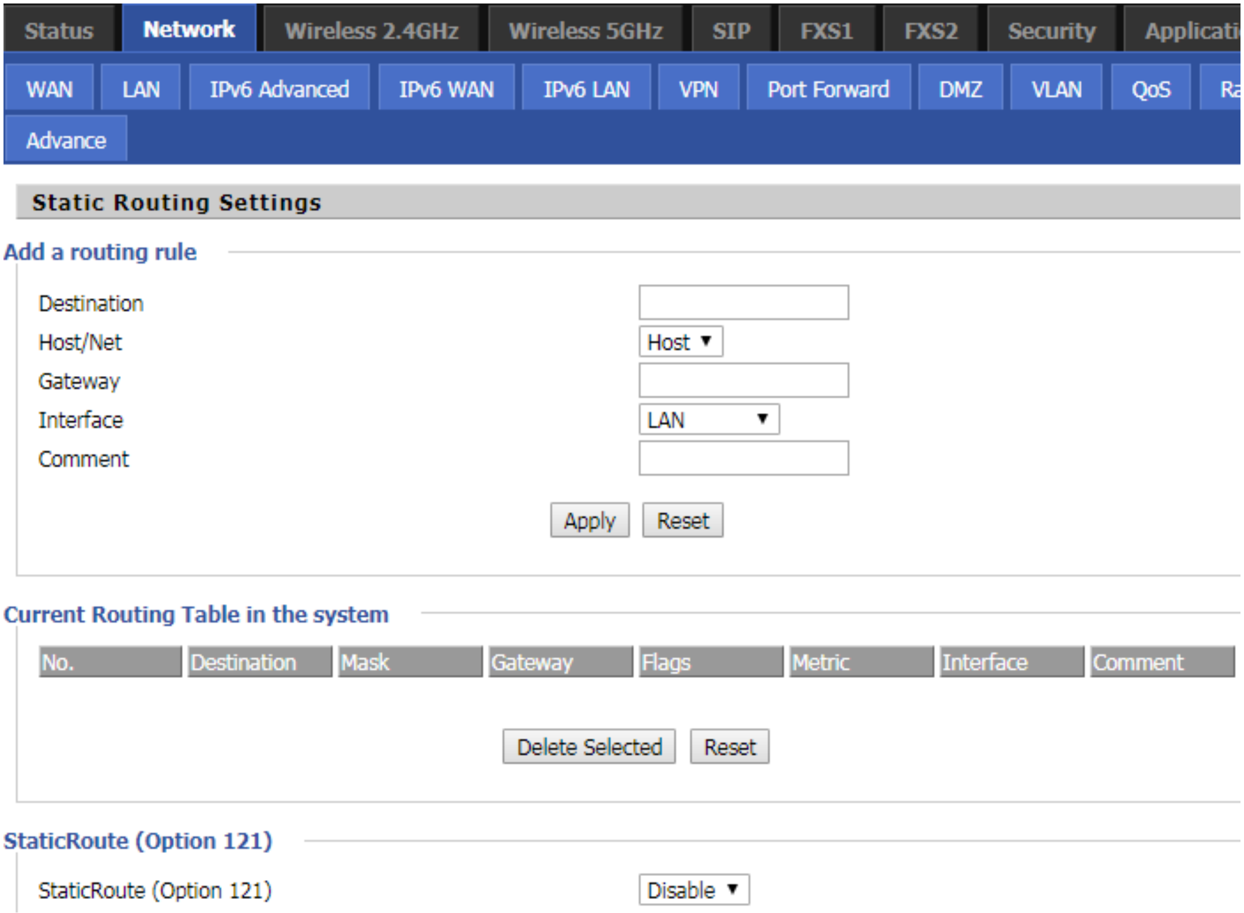
Port Setting

WAN Port Speed Nego	Auto
LAN1 Port Speed Nego	Auto
LAN2 Port Speed Nego	Auto
LAN3 Port Speed Nego	Auto
LAN4 Port Speed Nego	Auto

Field Name	Description
WAN Port speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half-duplex, 10M half and full.
LAN1~LAN3 Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full.

Routing

Table 24 Routing



Static Routing Settings

Add a routing rule

Destination	
Host/Net	Host
Gateway	
Interface	LAN
Comment	

Current Routing Table in the system

No.	Destination	Mask	Gateway	Flags	Metric	Interface	Comment

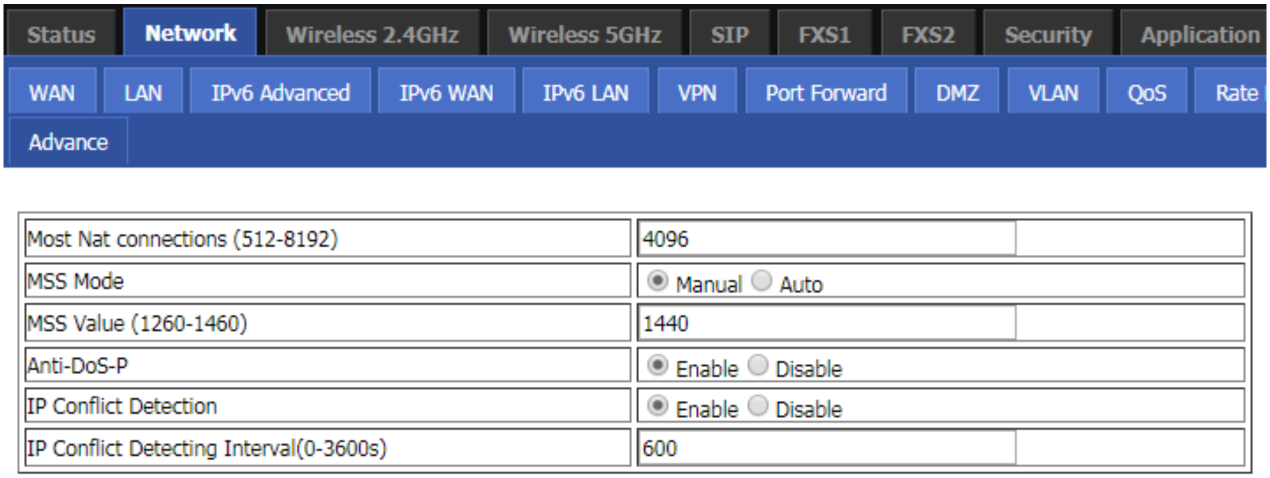
StaticRoute (Option 121)

StaticRoute (Option 121)	Disable

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

Advance

Table 25 Advance



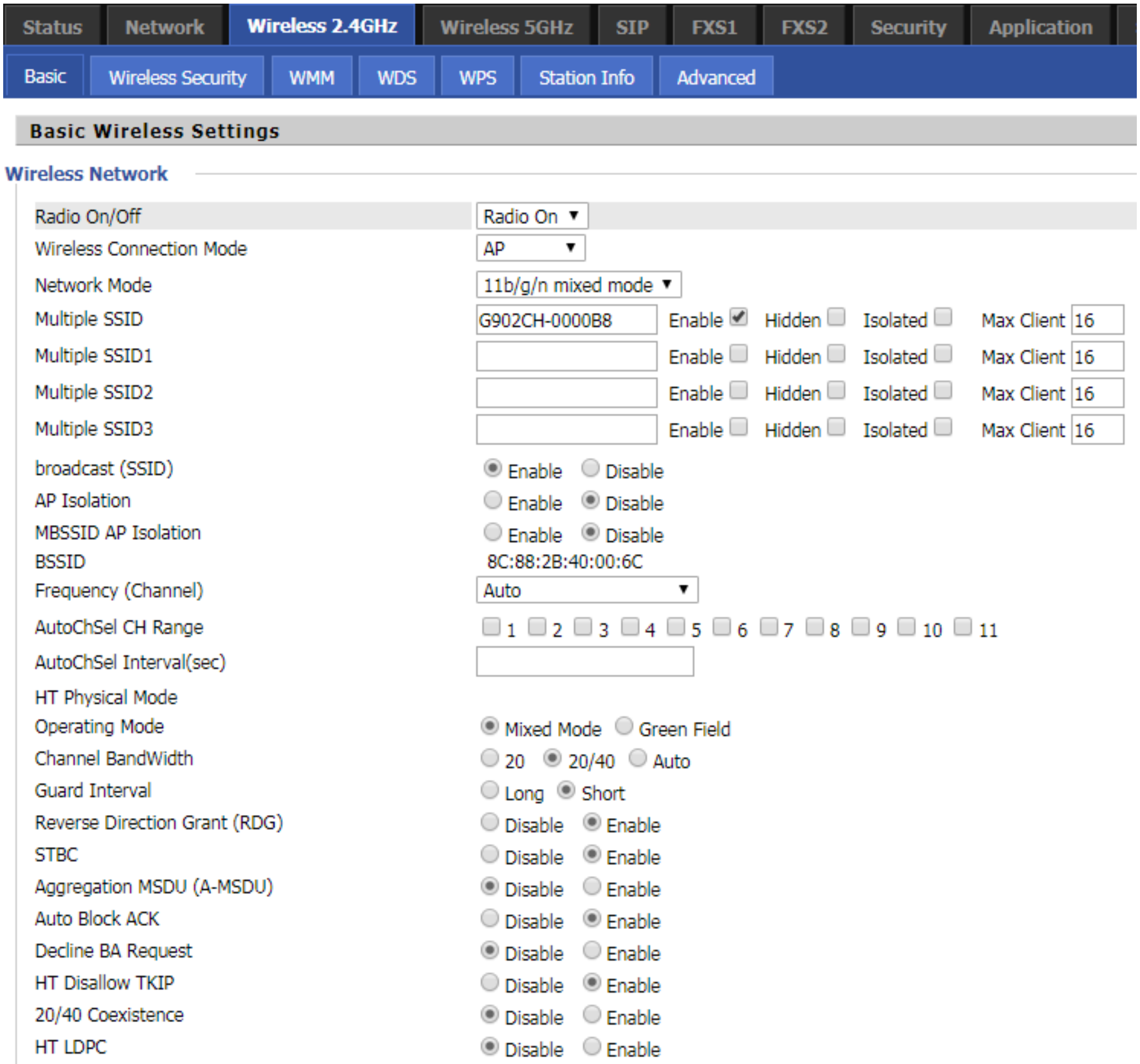
Most Nat connections (512-8192)	4096
MSS Mode	● Manual ○ Auto
MSS Value (1260-1460)	1440
Anti-DoS-P	● Enable ○ Disable
IP Conflict Detection	● Enable ○ Disable
IP Conflict Detecting Interval(0-3600s)	600

Field Name	Description
Most Nat connections	The largest value which the AC1000M/AC1000MS/AC1300MS 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

Wireless 2.4GHz

Basic

Table 26 Basic

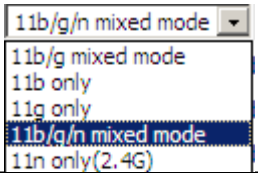


Basic Wireless Settings

Wireless Network

Radio On/Off	Radio On ▼
Wireless Connection Mode	AP ▼
Network Mode	11b/g/n mixed mode ▼
Multiple SSID	G902CH-0000B8 Enable ☑ Hidden □ Isolated □ Max Client 16
Multiple SSID1	Enable □ Hidden □ Isolated □ Max Client 16
Multiple SSID2	Enable □ Hidden □ Isolated □ Max Client 16
Multiple SSID3	Enable □ Hidden □ Isolated □ Max Client 16
broadcast (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	8C:88:2B:40:00:6C
Frequency (Channel)	Auto ▼
AutoChSel CH Range	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11
AutoChSel Interval(sec)	
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40 ○ Auto
Guard Interval	○ Long ● Short
Reverse Direction Grant (RDG)	○ Disable ● Enable
STBC	○ Disable ● Enable
Aggregation MSDU (A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
20/40 Coexistence	● Disable ○ Enable
HT LDPC	● Disable ○ Enable

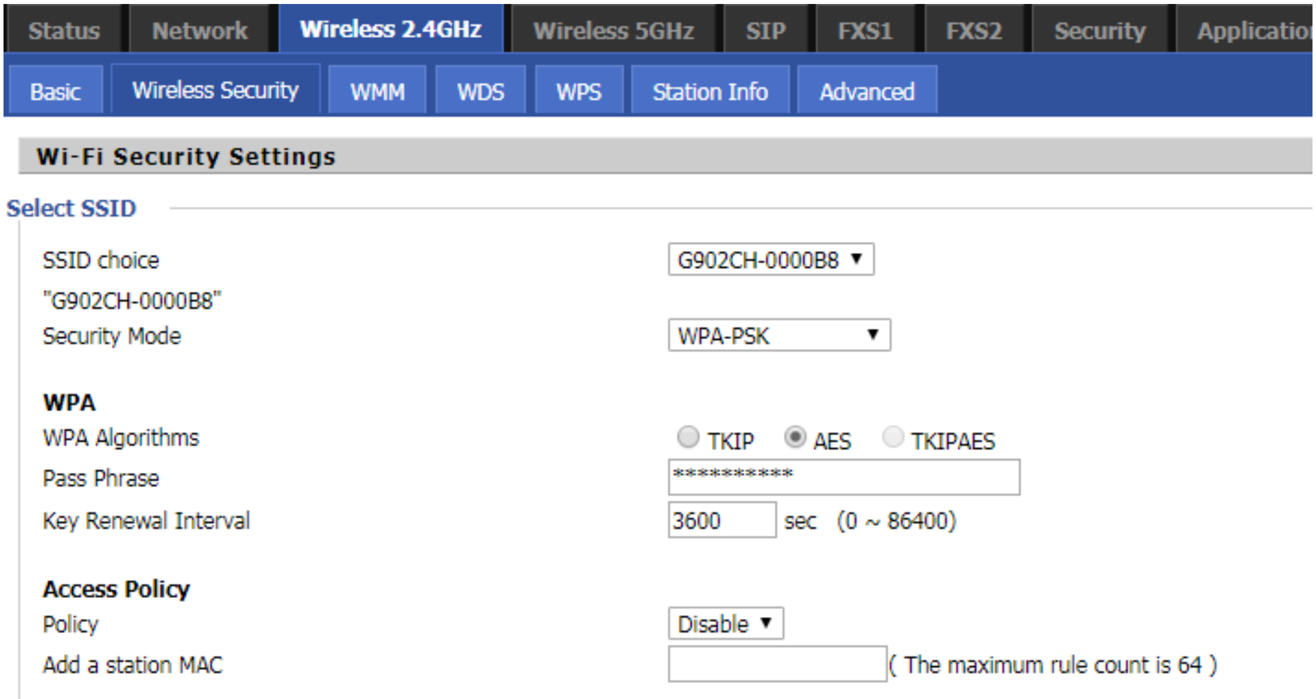
Field Name	Description
Radio on/off	Select "Radio Off" to disable wireless. Select "Radio On" to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP
Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed mode

	 11b/g/n mixed mode 11b/g mixed mode 11b only 11g only 11b/g/n mixed mode 11n only(2.4G)
SSID	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~SSID3	The device supports 4 SSIDs.
Hidden	After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list
Broadcast(SSID)	After initial State opening, the device broadcasts the SSID of the router to wireless network
AP Isolation	If AP isolation is enabled, the clients of the AP cannot access each other
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	Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 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 20 MHz and 20/40 MHz.
Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval
Reverse Direction Grant (RDG)	Enabled: Devices on the WLAN are able to transmit to each other without requiring an additional contention-based request to transfer (i.e. devices are able to transmit to another device on the network during TXOP) Disabled: Devices on the WLAN must make a request for transmit when communicating with another device on the network
STBC	Space-time Block Code

	Enabled: Multiple copies of signals are transmitted to increase the chance of successful delivery
Aggregation MSDU (A-MSDU)	Enabled: Allows the device to aggregate multiple Ethernet frames into a single 802.11n, thereby improving the ratio of frame data to frame overhead Disabled: No frame aggregation is employed at the router
Auto Block Ack	Enabled: Multiple frames are acknowledged together using a single Block Acknowledgement frame. Disabled: Auto block acknowledgement is not used by the device – use this configuration when low throughput/connectivity issues are experienced by
Decline BA Request	Enabled: Disallow block acknowledgement requests from devices Disabled: Allow block acknowledgement requests from devices
HT Disallow TKIP	Enabled: Disallow the use of Temporal Key Integrity Protocol for connected devices Disabled: Allow the use of Temporal Key Integrity Protocol for connected devices
HT LDPC	Enabled: Enable Low-Density Parity Check mechanism for increasing chance of successful delivery in challenging wireless environments Disabled: Disable Low-Density Parity Check mechanism

Wireless Security

Table 27 Wireless security



Wi-Fi Security Settings

Select SSID

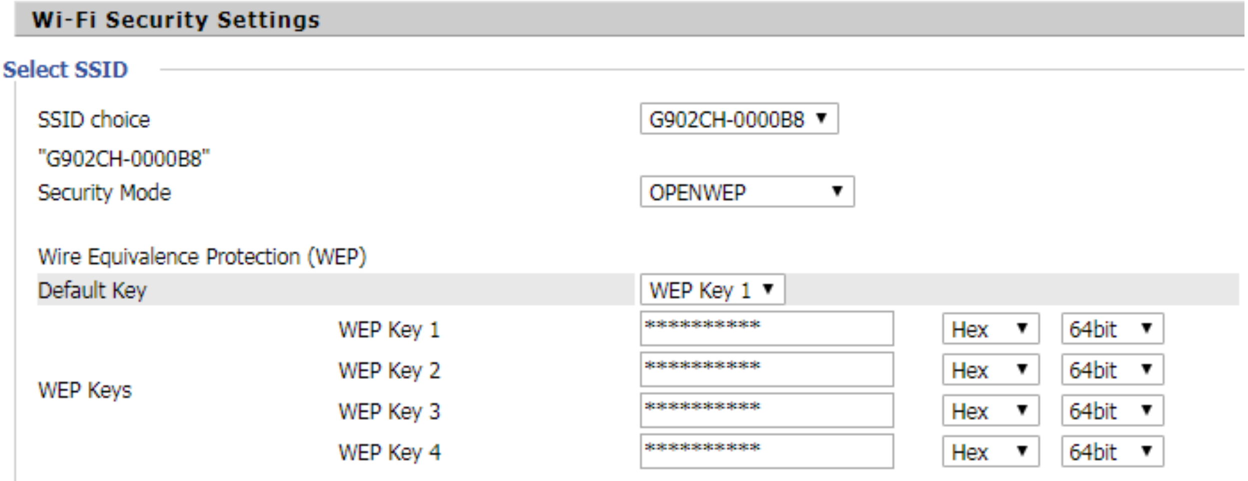
SSID choice	G902CH-0000B8 ▼
"G902CH-0000B8"	
Security Mode	WPA-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	***********
Key Renewal Interval	3600 sec (0 ~ 86400)
Access Policy	
Policy	Disable ▼
Add a station MAC	(The maximum rule count is 64)

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.

User can configure the corresponding parameters. Here are some common encryption methods:

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

Table 28 Wi-Fi Security Setting



Wi-Fi Security Settings

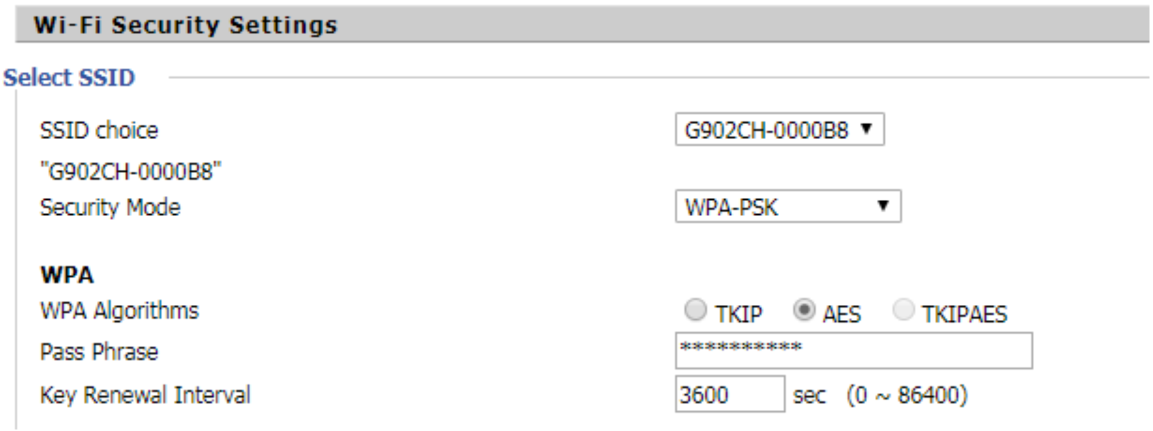
Select SSID

SSID choice	G902CH-0000B8 ▼		
"G902CH-0000B8"			
Security Mode	OPENWEP ▼		
Wire Equivalence Protection (WEP)			
Default Key	WEP Key 1 ▼		
WEP Keys WEP Key 1	***********	Hex ▼	64bit ▼
WEP Key 2	***********	Hex ▼	64bit ▼
WEP Key 3	***********	Hex ▼	64bit ▼
WEP Key 4	***********	Hex ▼	64bit ▼

Field Name	Description
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 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.	

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

Table 29 WPA-PSK



Wi-Fi Security Settings

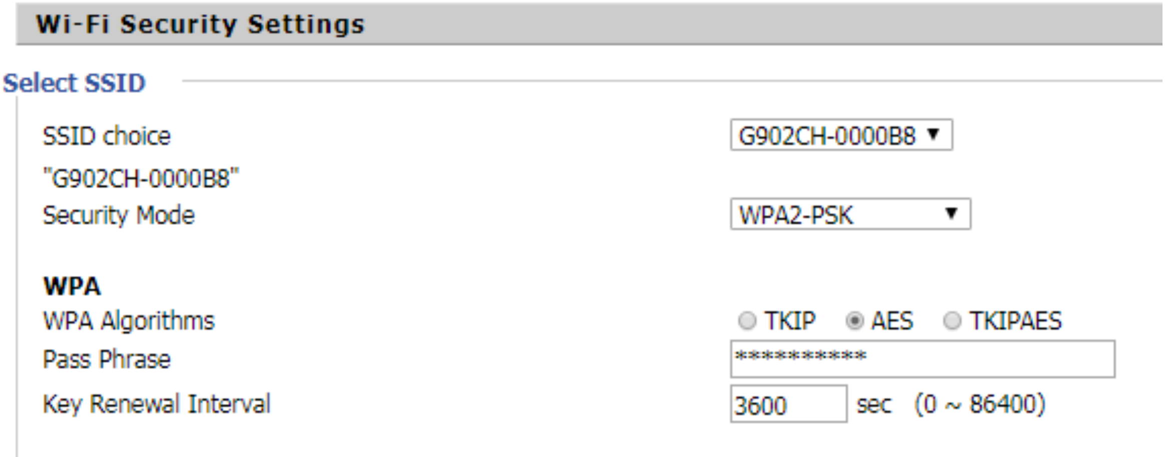
Select SSID

SSID choice	G902CH-0000B8 ▼
"G902CH-0000B8"	
Security Mode	WPA-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	***********
Key Renewal Interval	3600 sec (0 ~ 86400)

Field Name	Description
WPA Algorithms	This item is used to select the encryption of wireless home 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.

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 30 WPAPSKWPA2PSK



Wi-Fi Security Settings

Select SSID

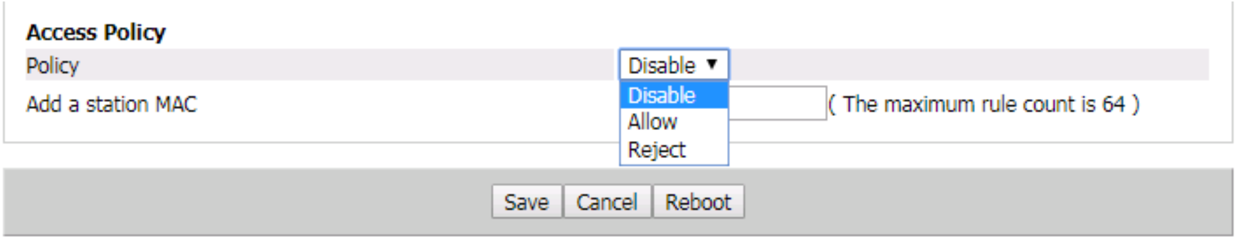
SSID choice	G902CH-0000B8 ▼
"G902CH-0000B8"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	************
Key Renewal Interval	3600 sec (0 ~ 86400)

Field Name	Description
WPA Algorithms	The home gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms.
Pass Phrase	Set WPA-PSK/WPA2-PSK security code
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s

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.

Wireless Access Policy:

Table 31 Wireless Access Policy



Access Policy

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

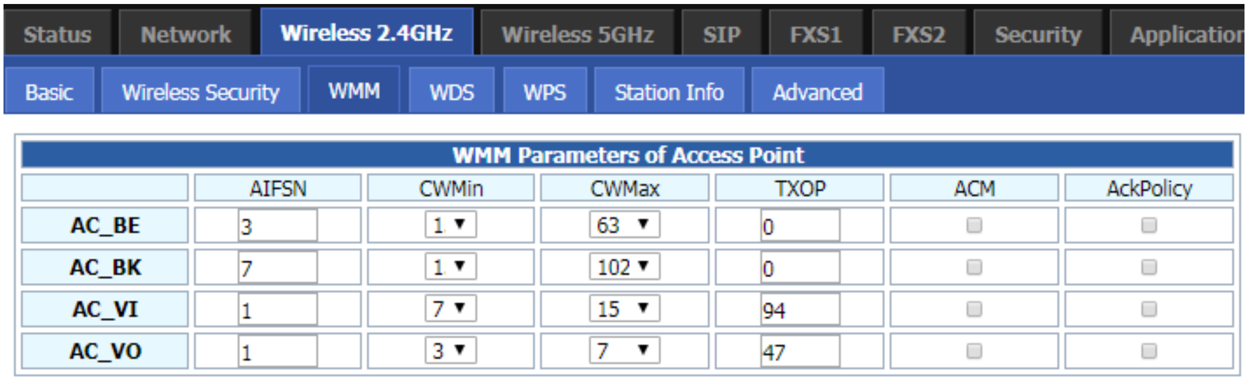
Field Name	Description
Access policy	Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address.
Policy	Disable : Prohibition: wireless access control policy. Allow: only allow the clients in the list to access. Rejected: block 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

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 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.

WMM

WMM (Wi-Fi Multi-Media) 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 home gateway type. To make WMM effective, the wireless clients must also support WMM.

Table 32 WMM

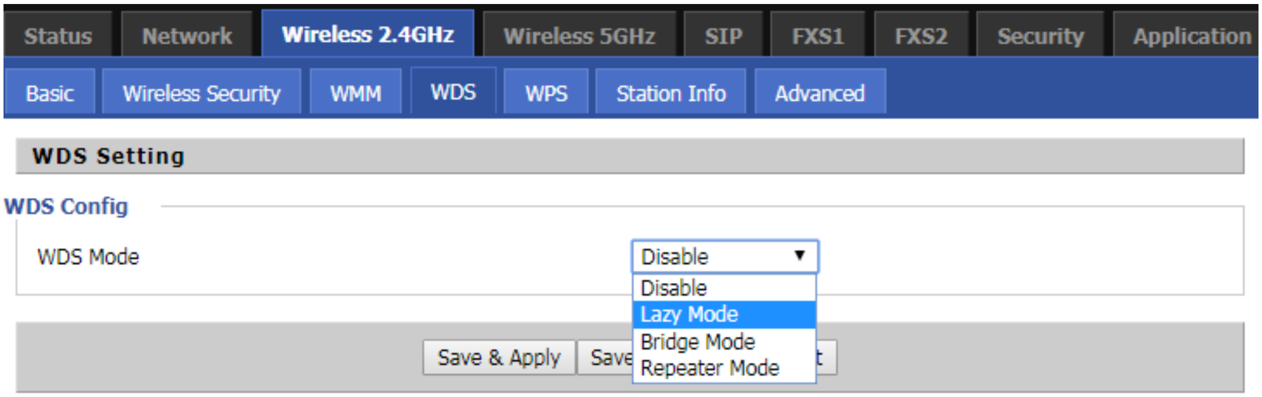


WMM Parameters of Access Point

	AIFSN	CWMin	CWMax	TXOP	ACM	AckPolicy
AC_BE	3	1	63	0	☐	☐
AC_BK	7	1	102	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WDS

Table 33 WDS



WDS Setting

WDS Config

WDS Mode: Disable

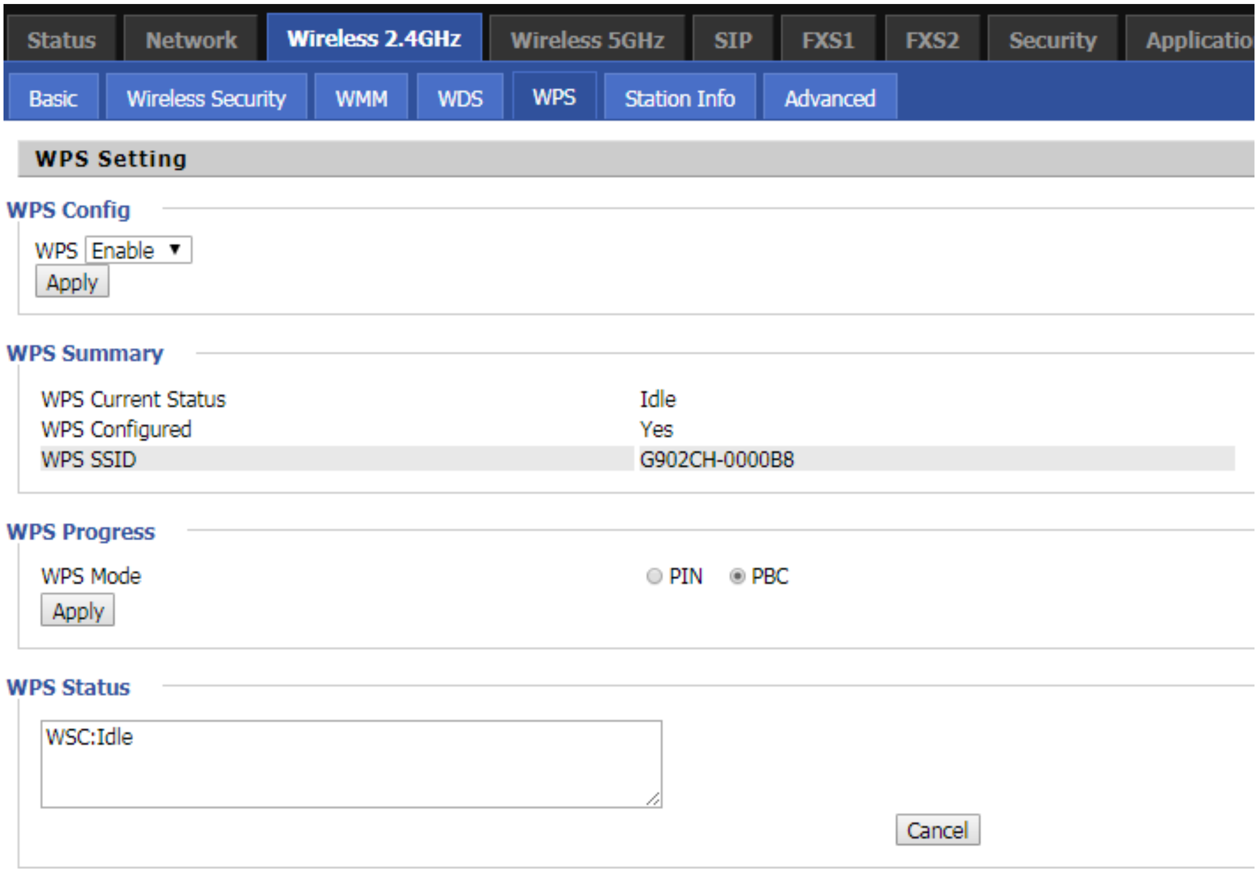
Description
WDS stands for Wireless Distribution System, enabling WDS access points to be interconnected to expand a wireless network.

WPS

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

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

Table 34 WPS



WPS Enable

WPS Current Status Idle
WPS Configured Yes
WPS SSID G902CH-0000B8

WPS Mode ○ PIN ● PBC

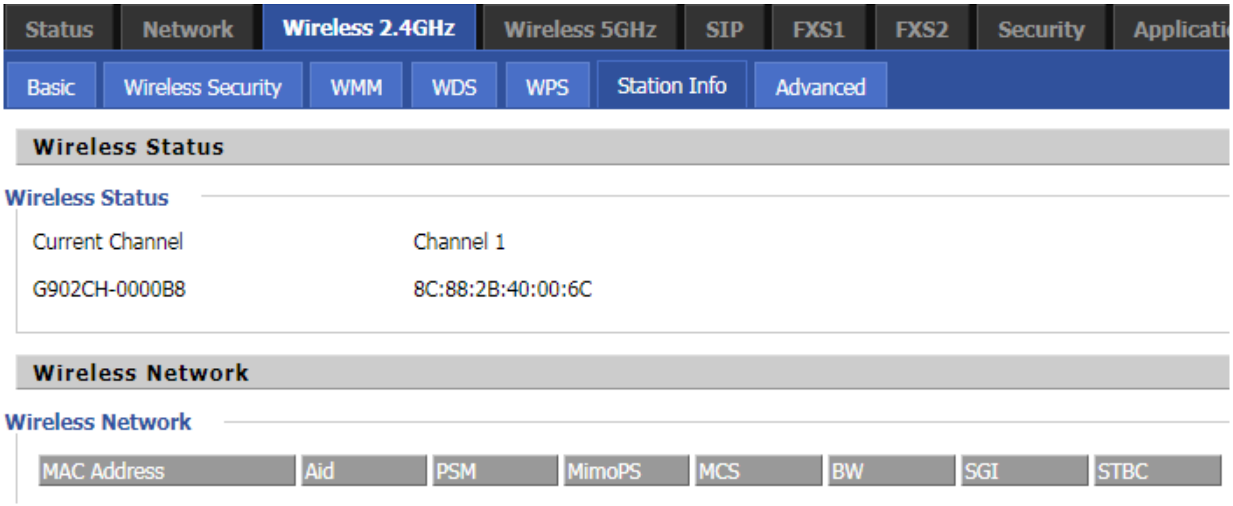
WSC:Idle

Field Name	Description
WPS Config	
WPS	Enable/Disable WPS function
WPS Summary	

WPS Current Status	Display the current status of WPS
WPS Configured	Display the configure the status information of WPS
WPS SSID	Display WPS SSID
WPS Progress	
WPS Mode	PIN： Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then router begins to send signals, turn on the PIN accessing method on the clients, and then it can access the wireless AP automatically. PBC： There are two ways to start PBC mode, user can press the PBC button directly on the device, or select PBC mode on the software and apply. Users can activate WPS connection in WPS mode through these two methods, only when the clients choose PBC access, the clients can connect the AP automatically.
WPS Status	WPS shows status in three ways: WSC: Idle WSC: Start WSC process (begin to send messages) WSC: Success; this means clients have accessed the AP successfully

Station Info

Table 35 Station info



Wireless Status

Wireless Status

Current Channel	Channel 1
G902CH-0000B8	8C:88:2B:40:00:6C

Wireless Network

Wireless Network

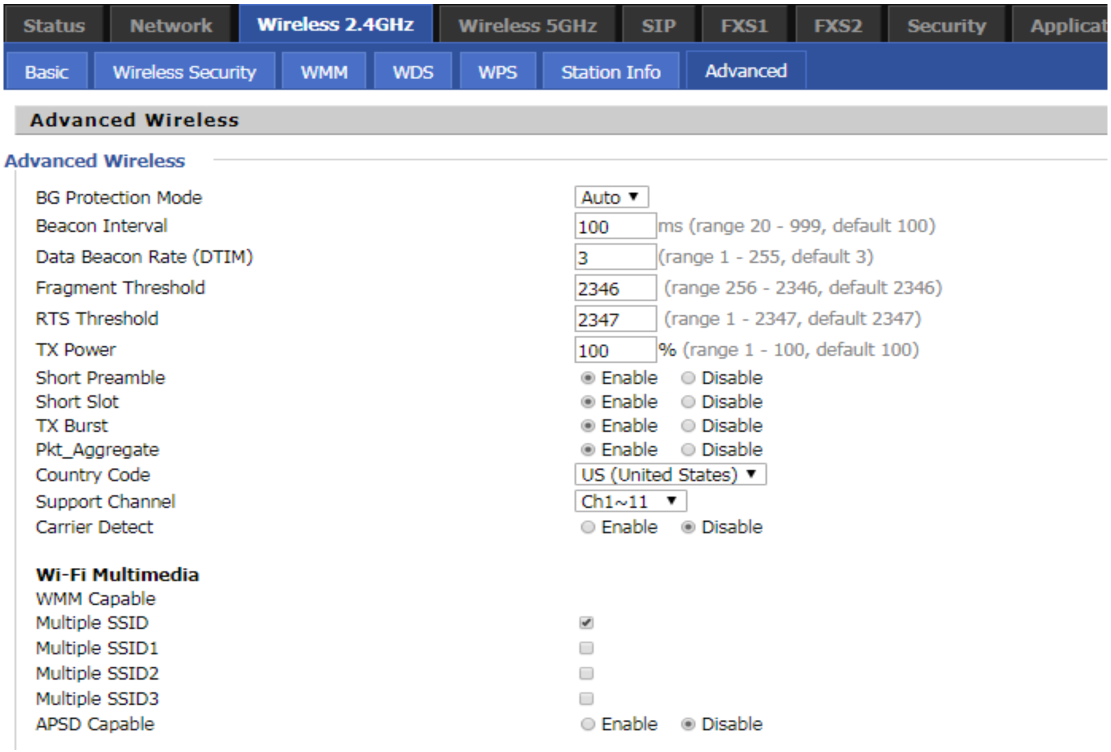
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

Description

This page displays information about the current registered clients' connections including operating MAC address and operating statistics.

Advanced

Table 36 Advanced



Advanced Wireless

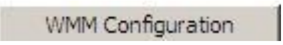
Advanced Wireless

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

Wi-Fi Multimedia

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

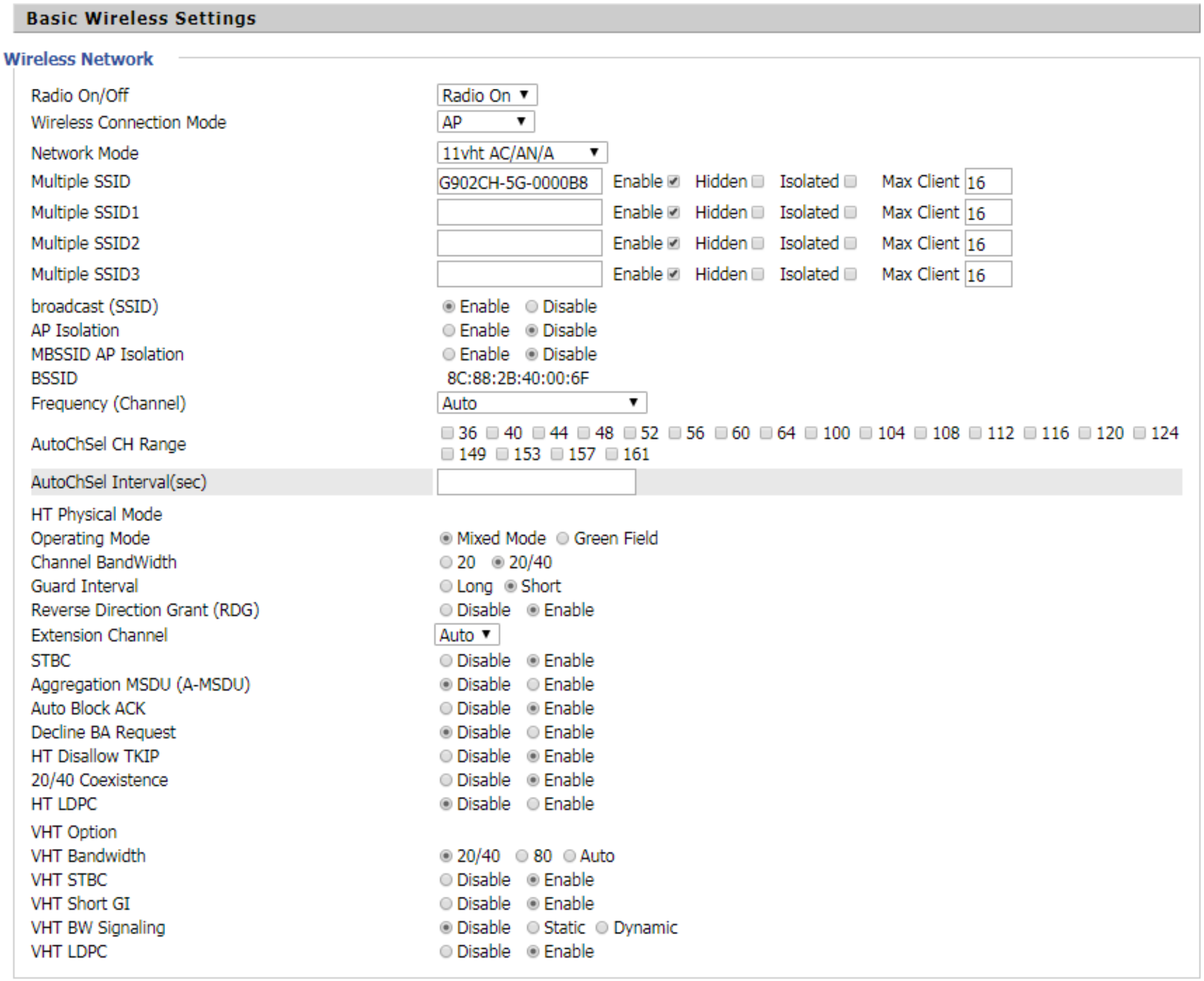
Field Name	Description
BG Protection Mode	Select G protection mode, options are on, off and automatic.
Beacon Interval	The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.
Data Beacon Rate(DTIM)	Specify the 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	Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet is divided.
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	Define the transmission power of the current AP, the greater it is, the stronger the signal is.
Short Preamble	Choose enable or disable
Short Slot	Enable/Disable short slot. By default it is enabled, 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 home gateway packets are sent to the destination correctly.
Support Channel	Choose appropriate channel
Wi-Fi Multimedia (WMM)	
WMM Capable	Enable/Disable WMM.
APSD Capable	Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power
WMM Parameters	Press , the webpage will jump to the configuration page of Wi-Fi multimedia.
Multicast-to-Unicast Converter	Enable/Disable Multicast-to-Unicast. By default, it is Disabled.

Wireless 5GHz

Basic

Table 37 Basic



Basic Wireless Settings

Wireless Network

Radio On/Off	Radio On ▼
Wireless Connection Mode	AP ▼
Network Mode	11vht AC/AN/A ▼
Multiple SSID	G902CH-5G-0000B8 Enable ☑ Hidden □ Isolated □ Max Client 16
Multiple SSID1	Enable ☑ Hidden □ Isolated □ Max Client 16
Multiple SSID2	Enable ☑ Hidden □ Isolated □ Max Client 16
Multiple SSID3	Enable ☑ Hidden □ Isolated □ Max Client 16
broadcast (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	8C:88:2B:40:00:6F
Frequency (Channel)	Auto ▼
AutoChSel CH Range	□ 36 □ 40 □ 44 □ 48 □ 52 □ 56 □ 60 □ 64 □ 100 □ 104 □ 108 □ 112 □ 116 □ 120 □ 124 □ 149 □ 153 □ 157 □ 161
AutoChSel Interval(sec)	
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Short
Reverse Direction Grant (RDG)	○ Disable ● Enable
Extension Channel	Auto ▼
STBC	○ Disable ● Enable
Aggregation MSDU (A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
20/40 Coexistence	○ Disable ● Enable
HT LDPC	● Disable ○ Enable
VHT Option	
VHT Bandwidth	● 20/40 ○ 80 ○ Auto
VHT STBC	○ Disable ● Enable
VHT Short GI	○ Disable ● Enable
VHT BW Signaling	● Disable ○ Static ○ Dynamic
VHT LDPC	○ Disable ● Enable

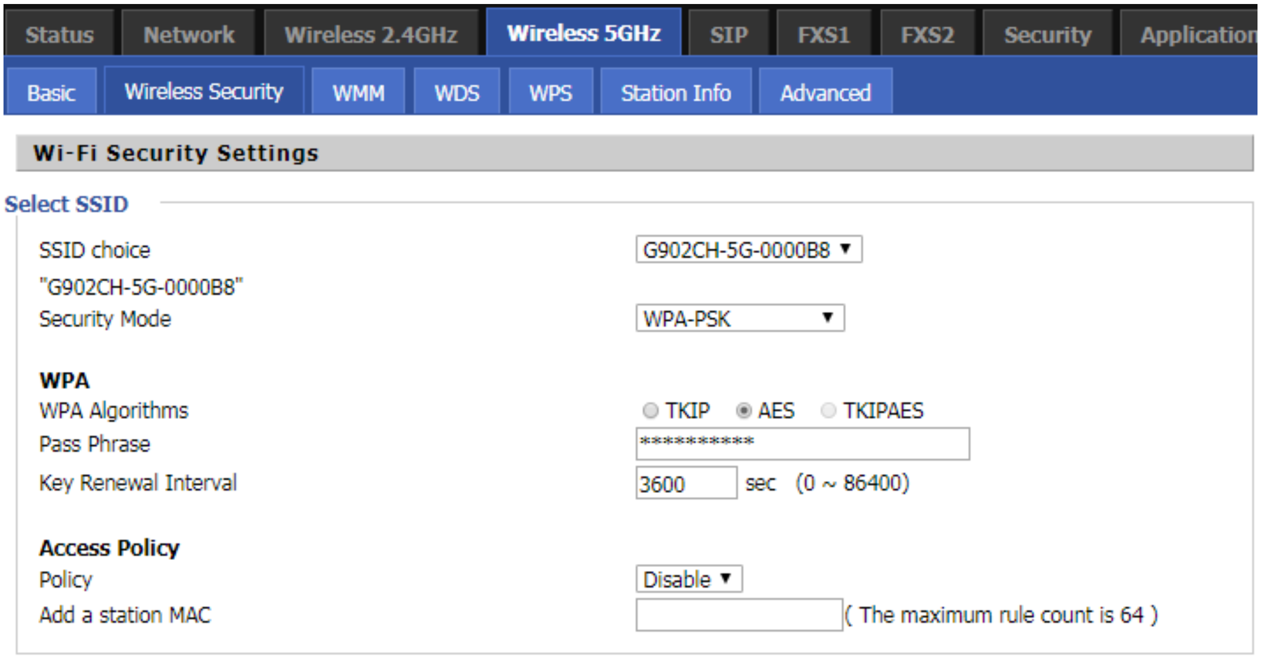
Field Name	Description
Radio on/off	Select “Radio off” to disable wireless. Select “Radio on” to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP
Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed mode

Multiple 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~SSID3	The device supports 4 SSIDs.
Broadcast(SSID)	After initial State opening, the device broadcasts the SSID of the router to wireless network
AP Isolation	If AP isolation is enabled, the clients of the AP cannot access each other
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.
Operating Mode	Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 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 20 MHz and 20/40 MHz.
Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval
Reverse Direction Grant (RDG)	Enabled: Devices on the WLAN are able to transmit to each other without requiring an additional contention-based request to transfer (i.e. devices are able to transmit to another device on the network during TXOP) Disabled: Devices on the WLAN must make a request for transmit when communicating with another device on the network
STBC	Space-time Block Code Enabled: Multiple copies of signals are transmitted to increase the chance of successful delivery Disabled: STBC is not employed for signal transmission
Aggregation MSDU (A-MSDU)	Enabled: Allows the device to aggregate multiple Ethernet frames into a single 802.11n, thereby improving the ratio of frame data to frame overhead Disabled: No frame aggregation is employed at the router

Auto Block Ack	Enabled: Multiple frames are acknowledged together using a single Block Acknowledgement frame. Disabled: Auto block acknowledgement is not used by the device – use this configuration when low throughput/connectivity issues are experienced by mobile devices
Decline BA Request	Enabled: Disallow block acknowledgement requests from devices Disabled: Allow block acknowledgement requests from devices
HT Disallow TKIP	Enabled: Disallow the use of Temporal Key Integrity Protocol for connected devices Disabled: Allow the use of Temporal Key Integrity Protocol for connected devices
HT LDPC	Enabled: Enable Low-Density Parity Check mechanism for increasing chance of successful delivery in challenging wireless environments Disabled: Disable Low-Density Parity Check mechanism

Wireless Security

Table 38 Wireless security



Wi-Fi Security Settings

Select SSID

SSID choice	G902CH-5G-0000B8 ▼
"G902CH-5G-0000B8" Security Mode	WPA-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	***********
Key Renewal Interval	3600 sec (0 ~ 86400)
Access Policy	
Policy	Disable ▼
Add a station MAC	(The maximum rule count is 64)

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.

WMM

Please refer to 4.4.3 section.

WDS

Please refer to 4.4.4 section.

WPS

Please refer to 4.4.5 section.

Station Info

Please refer to 4.4.6 section.

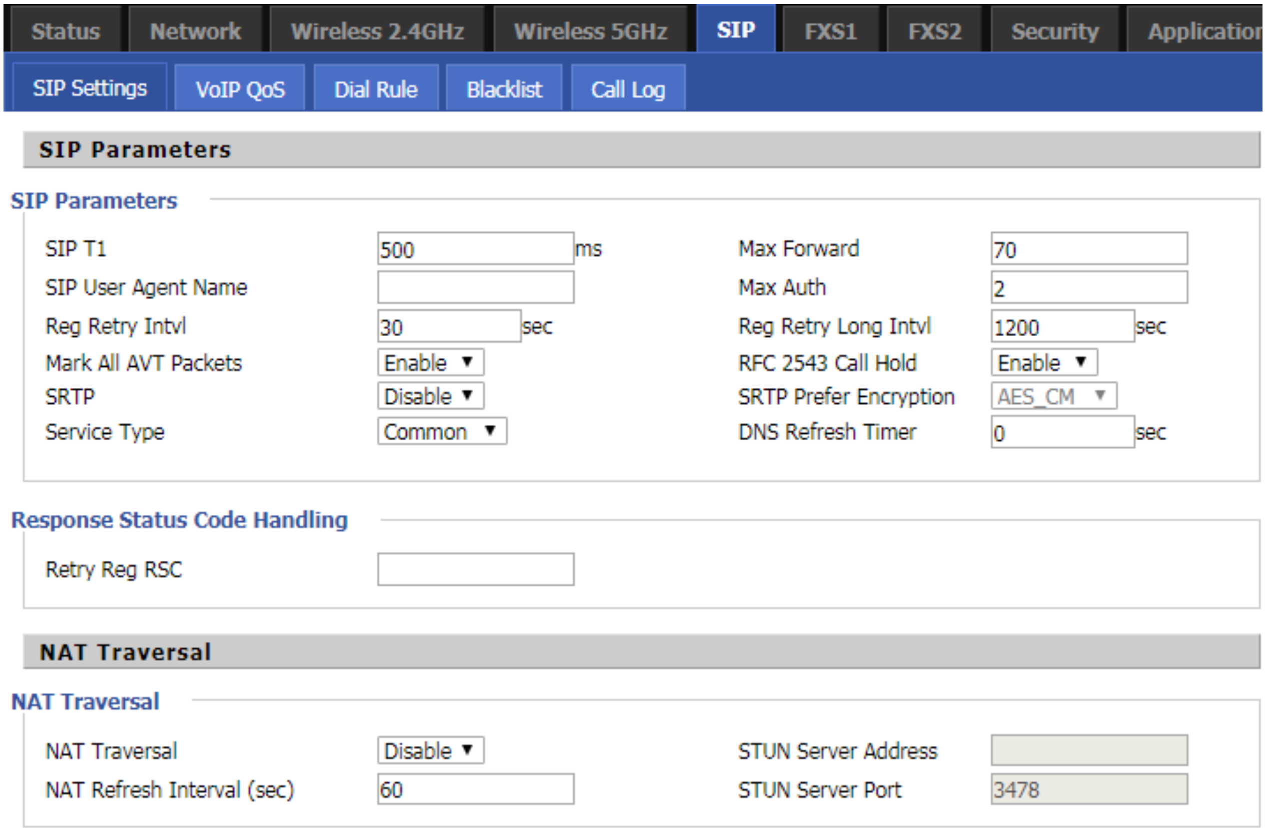
Advanced

Please refer to 4.4.7 section.

SIP

SIP Settings

Table 39 SIP Settings



SIP Parameters

SIP Parameters

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

Response Status Code Handling

Retry Reg RSC

NAT Traversal

NAT Traversal

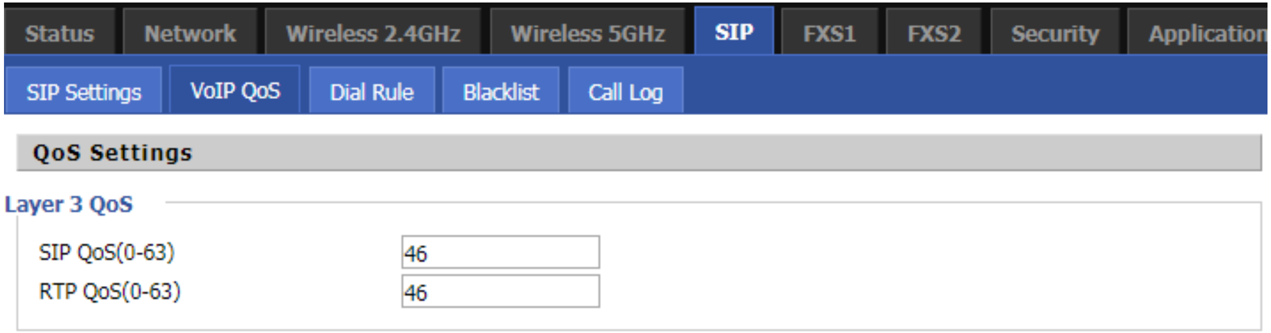
NAT Traversal	Disable ▼	STUN Server Address	
NAT Refresh Interval (sec)	60	STUN Server Port	3478

Parameters name	Description
SIP Parameters	
SIP T1	The default value is 500
SIP User Agent Name	Enter the SIP User Agent header field
Max Forward	Modify the maximum hop value, the default is 70
Max Auth	Change the number of authentication failures, the default value is 2
Reg Retry Intvl	Registration failed again registration interval, default is 30
Reg Retry Long Intvl	Registration failed Register again for the long interval Default 1200
Mark All AVT Packets	The default enable is on
RFC 2543 Call Hold	The default enable is on
SRTP	The default is disabled

SRTP Prefer Encryption	Support for AES_CM and ARIA_CM
Service Type	Default general
DNS Refresh Timer	Modify the DNS refresh time, the default value of 0
Transport	The transmission type defaults to UDP
Response Status Code Handling	
Retry Reg RSC	Fall in Retry Reg RSC
NAT Traversal	
NAT Traversal	Whether to enable NAT mode, or select STUN to penetrate
STUN Server Address	STUN server IP address
NAT Refresh Interval(sec)	Refresh interval
STUN Server Port	STUN port, the default is 3478

VoIP QoS

Table 40 VoIP QoS



QoS Settings

Layer 3 QoS

SIP QoS(0-63) 46

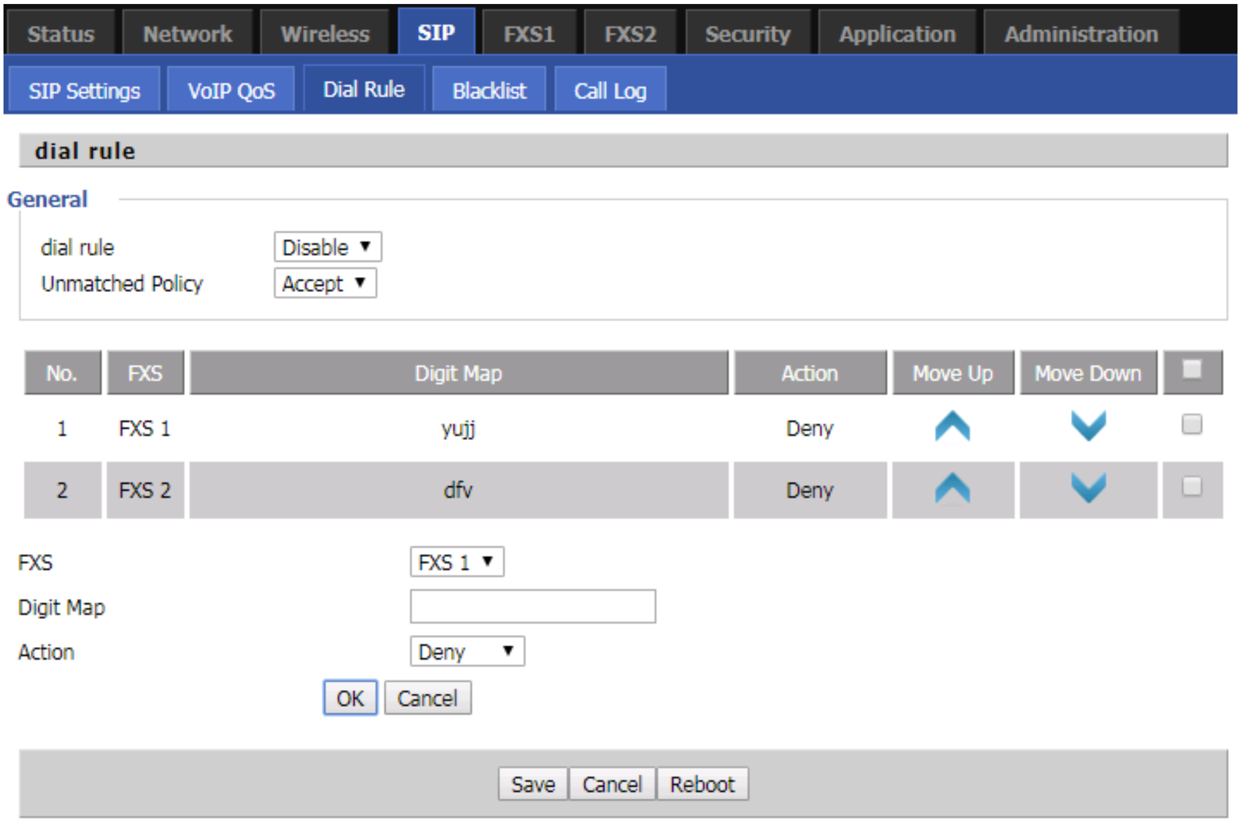
RTP QoS(0-63) 46

Parameters name	Description
SIP QoS(0-63)	Defaults to 46,you can set a range of values is 0~63
RTP QoS(0-63)	Defaults to 46,you can set a range of values is 0~63

Configuration can be based on the scene environment to modify the parameters

Dial Plan

Table 41 Dial Plan



dial rule

General

dial rule	Disable ▼
Unmatched Policy	Accept ▼

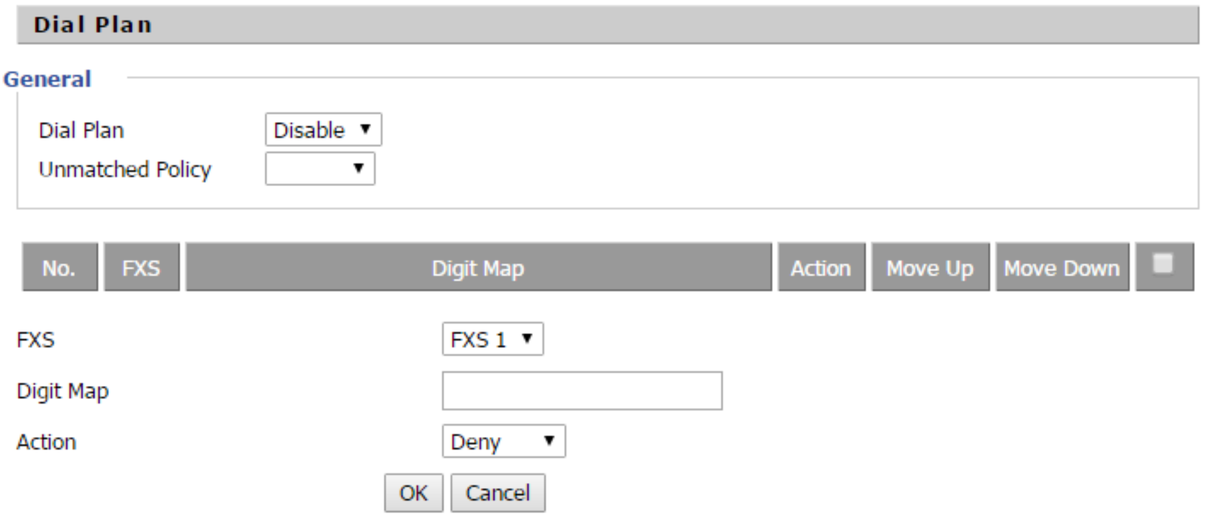
No.	FXS	Digit Map	Action	Move Up	Move Down	☐
1	FXS 1	yujj	Deny	∧	∨	☐
2	FXS 2	dfv	Deny	∧	∨	☐

FXS	FXS 1 ▼
Digit Map	
Action	Deny ▼

Field Name	Description
Dial Plan	Enable/Disable dial plan.
Line	Set the line.
Digit Map	Enter 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 router will reject the matched number, while Dial Out means router will dial out the matched number.
Move Up	Move the dial plan up the list.
Move Down	Move the dial plan down the list.

Adding one Dial Plan

Table 42 Adding one dial plan



Dial Plan

General

Dial Plan	Disable
Unmatched Policy	

No.	FXS	Digit Map	Action	Move Up	Move Down	☐

FXS	FXS 1
Digit Map	
Action	Deny

Description
Step 1. Enable Dial Plan.
Step 2. Click Add button, and the configuration table.
Step 3. Fill in the value of parameters.
Step 4. Press OK button to end configuration.

Dial Plan Syntactic

Table 43 Dial Plan Syntactic

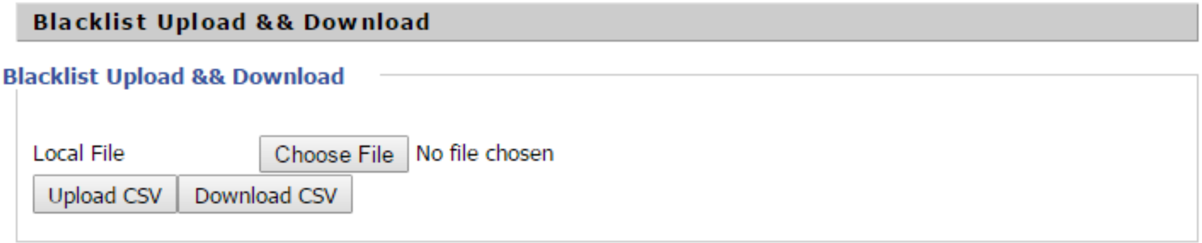
No.	String	Description
1	0 1 2 3 4 5 6 7 8 9 * #	Allowed characters
2	x	Lowercase letter “x” stands for one legal character
3	[sequence]	To match one character form sequence. For example: [0-9]: match one digit form 0 to 9 [23-5*]: match one character from 2 or 3 or 4 or 5 or *
4	x.	Match to x, xx, xxx, xxxx and so on. For example: “01” can be match to “0”,”01”,”011”...”011111...” and so on
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: “9,1xxxxxxxxxx” :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.

Blacklist

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

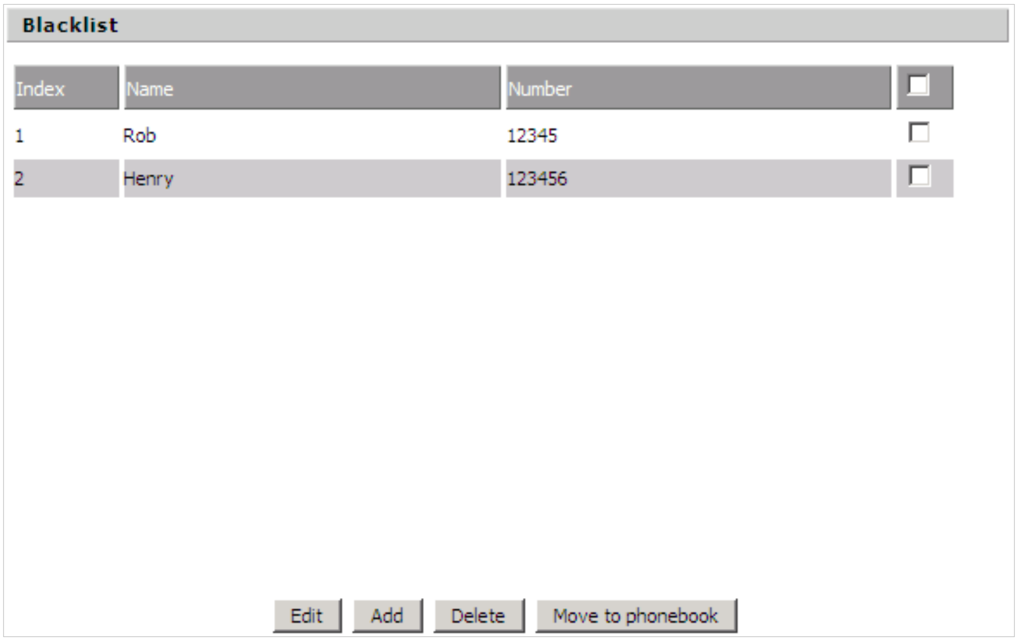
Table 44 Blacklist



Blacklist Upload && Download

Blacklist Upload && Download

Local File	Choose File No file chosen



Blacklist

Index	Name	Number	□
1	Rob	12345	□
2	Henry	123456	□

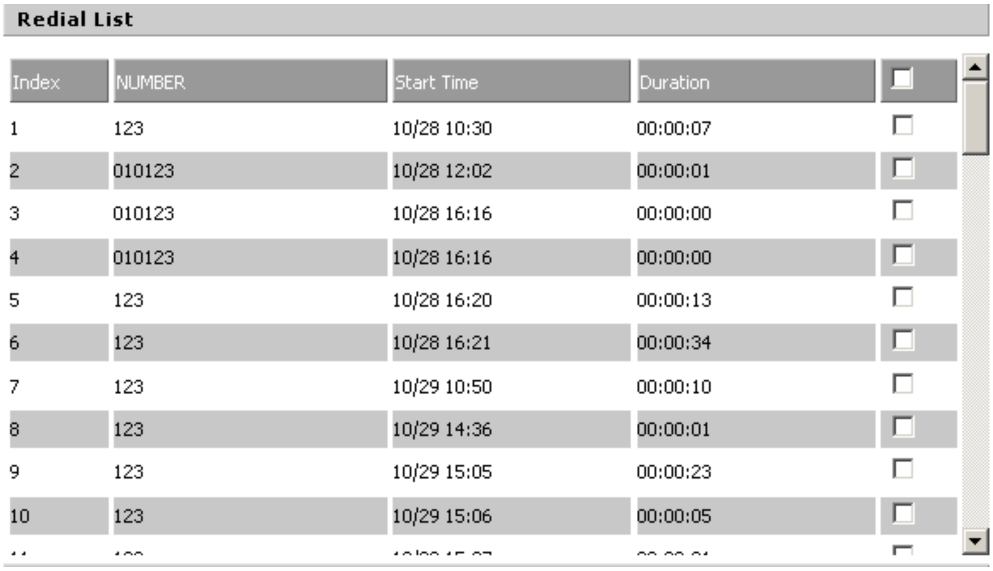
Description
Click **Choose File** to select the blacklist file and **Upload CSV** to upload it to device; **Click Download CSV** to save the blacklist file to your local computer.
Select one contact and click edit to change the information, click delete to delete the contact, click Move to phonebook to move the contact to phonebook. Click Add to add one blacklist, enter the name and phone number, click OK to confirm and click cancel to cancel.

Call Log

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

Table 45 Call log

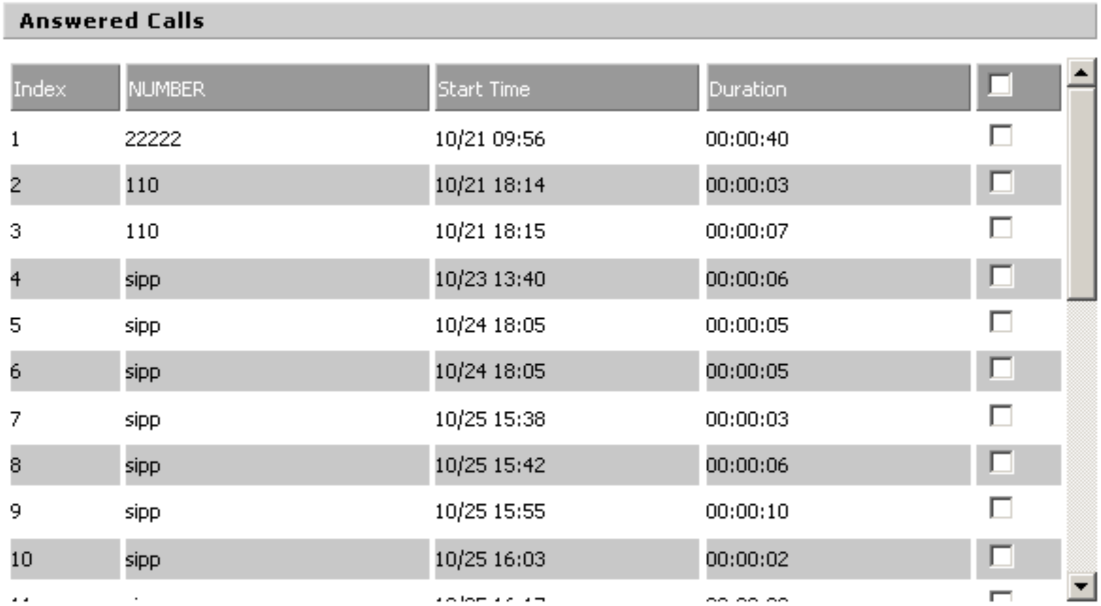
Redial Calls



Redial List

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

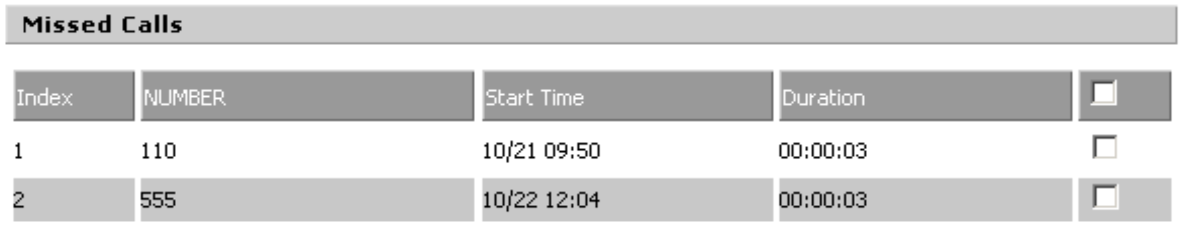
Answered Calls



Answered Calls

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

Missed Calls



Missed Calls

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

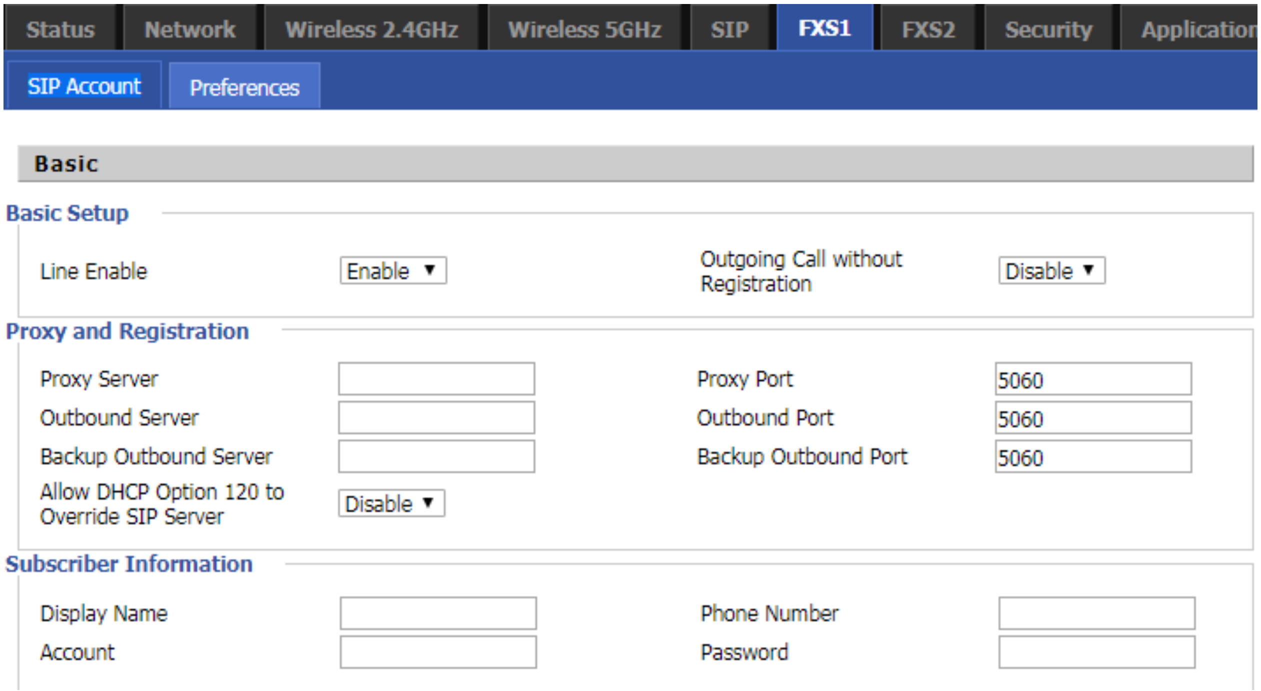
FXS 1

SIP Account

Basic

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

Table 46 Line



Basic

Basic Setup

Line Enable	Enable ▼	Outgoing Call without Registration	Disable ▼

Proxy and Registration

Proxy Server		Proxy Port	5060
Outbound Server		Outbound Port	5060
Backup Outbound Server		Backup Outbound Port	5060
Allow DHCP Option 120 to Override SIP Server	Disable ▼		

Subscriber Information

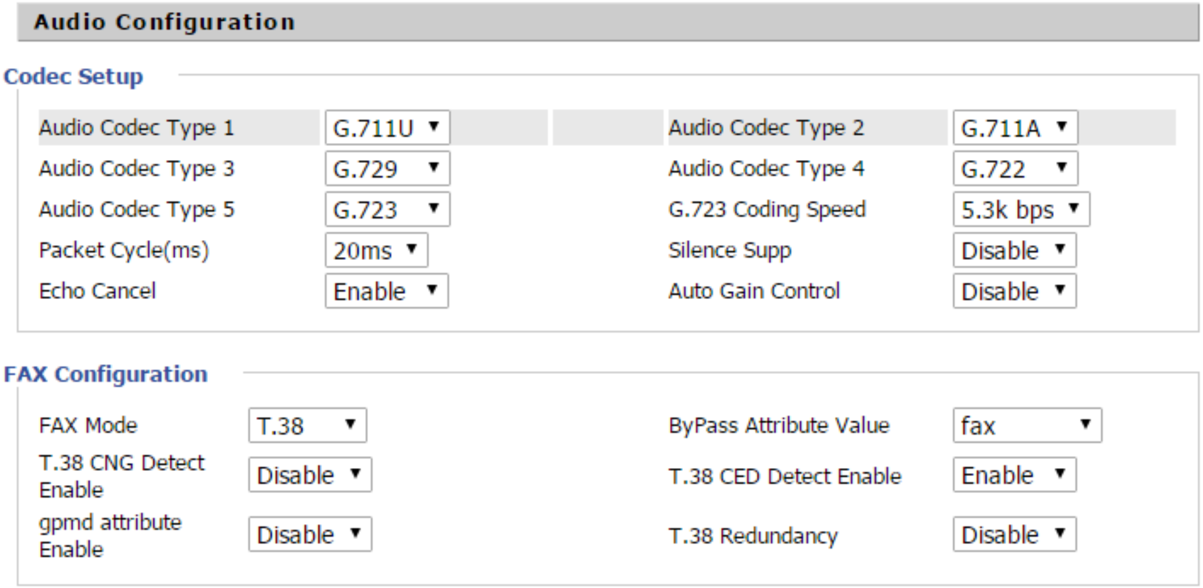
Display Name		Phone Number	
Account		Password	

Field Name	Description
Line Enable	Enable/Disable the line.
Peer To Peer	Enable/Disable PEER to PEER. If enabled, 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.

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

Audio Configuration

Table 47 Audio configuration



Audio Configuration

Codec Setup

Audio Codec Type 1	G.711U	Audio Codec Type 2	G.711A
Audio Codec Type 3	G.729	Audio Codec Type 4	G.722
Audio Codec Type 5	G.723	G.723 Coding Speed	5.3k bps
Packet Cycle(ms)	20ms	Silence Supp	Disable
Echo Cancel	Enable	Auto Gain Control	Disable

FAX Configuration

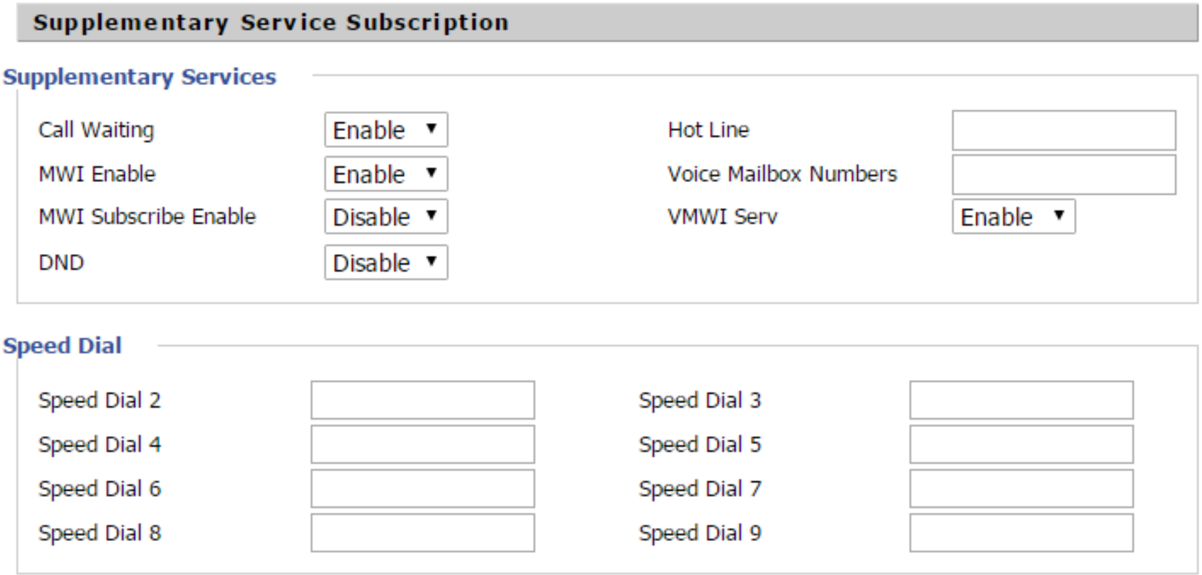
FAX Mode	T.38	ByPass Attribute Value	fax
T.38 CNG Detect Enable	Disable	T.38 CED Detect Enable	Enable
gpmd attribute Enable	Disable	T.38 Redundancy	Disable

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	Enable/Disable silence support
Echo Cancel	Enable/Disable echo cancel. By default, it is enabled
Auto Gain Control	Enable/Disable auto gain
T.38 Enable	Enable/Disable T.38
T.38 Redundancy	Enable/Disable T.38 Redundancy
T.38 CNG Detect Enable	Enable/Disable T.38 CNG Detect
gpmd attribute Enable	Enable/Disable gpmd attribute

Supplementary Service Subscription

Table 48 Supplementary service



Supplementary Service Subscription

Supplementary Services

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

Speed Dial

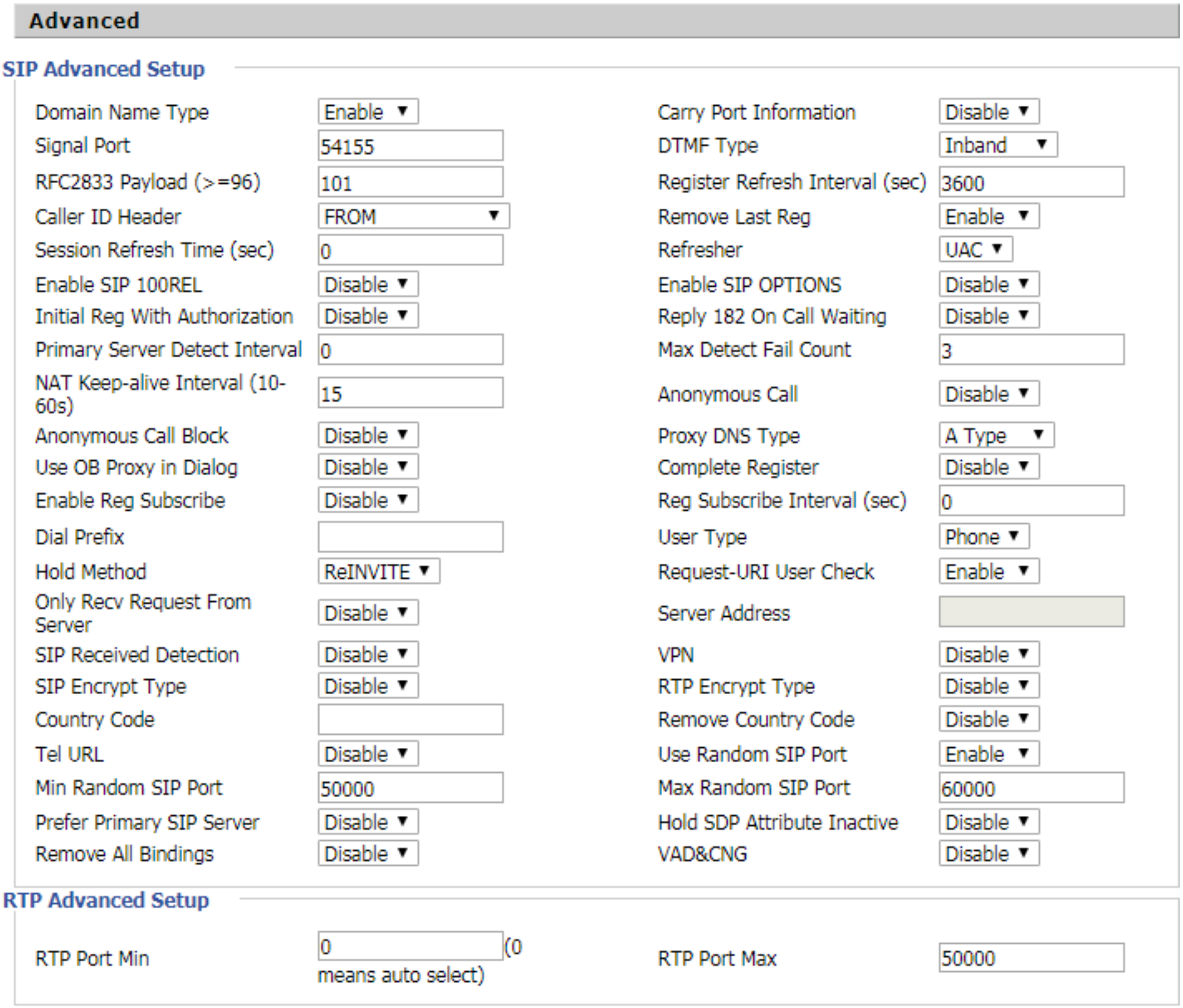
Speed Dial 2		Speed Dial 3	
Speed Dial 4		Speed Dial 5	
Speed Dial 6		Speed Dial 7	
Speed Dial 8		Speed Dial 9	

Field Name	Description
Call Waiting	Enable/Disable Call Waiting
Hot Line	Fill in the hotline number, pickup handset or press hands-free or headset button, the device will dial out the hotline number automatically
MWI Enable	Enable/Disable MWI (message waiting indicate). If the user needs to user voice mail, please enable this feature
MWI Subscribe Enable	Enable/Disable MWI Subscribe

Voice Mailbox Numbers	Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice mail is *97
VMWI Serv	Enable/Disable VMWI service
DND	Enable/Disable DND (do not disturb) If enable, any phone call cannot arrive at the device; default is disable
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 dials 075526099365 directly

Advanced

Table 49 Advanced



Advanced

SIP Advanced Setup

Domain Name Type	Enable ▼	Carry Port Information	Disable ▼
Signal Port	54155	DTMF Type	Inband ▼
RFC2833 Payload (>=96)	101	Register Refresh Interval (sec)	3600
Caller ID Header	FROM ▼	Remove Last Reg	Enable ▼
Session Refresh Time (sec)	0	Refresher	UAC ▼
Enable SIP 100REL	Disable ▼	Enable SIP OPTIONS	Disable ▼
Initial Reg With Authorization	Disable ▼	Reply 182 On Call Waiting	Disable ▼
Primary Server Detect Interval	0	Max Detect Fail Count	3
NAT Keep-alive Interval (10-60s)	15	Anonymous Call	Disable ▼
Anonymous Call Block	Disable ▼	Proxy DNS Type	A Type ▼
Use OB Proxy in Dialog	Disable ▼	Complete Register	Disable ▼
Enable Reg Subscribe	Disable ▼	Reg Subscribe Interval (sec)	0
Dial Prefix		User Type	Phone ▼
Hold Method	ReINVITE ▼	Request-URI User Check	Enable ▼
Only Recv Request From Server	Disable ▼	Server Address	
SIP Received Detection	Disable ▼	VPN	Disable ▼
SIP Encrypt Type	Disable ▼	RTP Encrypt Type	Disable ▼
Country Code		Remove Country Code	Disable ▼
Tel URL	Disable ▼	Use Random SIP Port	Enable ▼
Min Random SIP Port	50000	Max Random SIP Port	60000
Prefer Primary SIP Server	Disable ▼	Hold SDP Attribute Inactive	Disable ▼
Remove All Bindings	Disable ▼	VAD&CNG	Disable ▼

RTP Advanced Setup

RTP Port Min	0 (0 means auto select)	RTP Port Max	50000

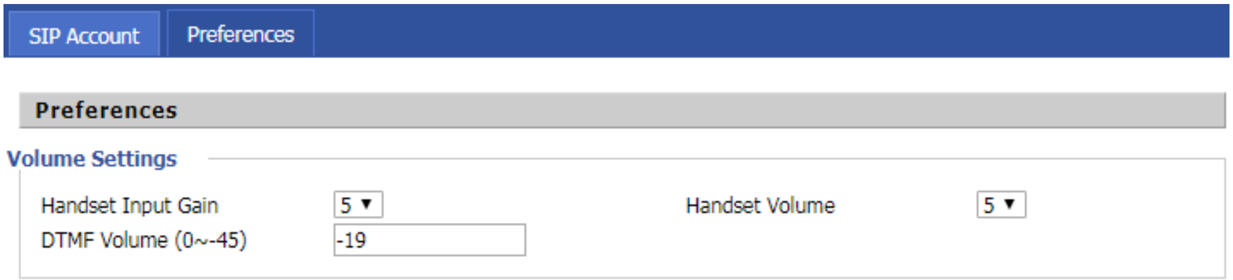
Parameter name	Description
Domain Name Type	Whether to enable domain name recognition in SIP URIs
Carry Port Information	Whether to carry the SIP URI port information
Signal Port	The local port number of the SIP protocol
DTMF Type	Select the second way of dialing, optional items are In-band, RFC2833 and SIP Info.
RFC2833 Payload(>=96)	The user can use the default settings
Register Refresh Interval(sec)	The time interval between two normal registration messages. The user can use the default settings.
Caller ID Header	When enabled, an unregistered message will be sent before the registration is disabled, and no unregistered messages will be sent before registration; should be set according to the different server requirements
Remove Last Reg	Whether to remove the last registration message
Session Refresh Time(sec)	The interval between two sessions, the user can use the default settings
Refresher	Select Refresh from UAC and UAS
SIP 100REL Enable	If this option is enabled, the IP phone will send SIP-OPTION to the server instead of sending Hello messages on a regular basis. The interval for sending is the parameter set for the "NAT Hold Interval" parameter.
SIP OPTIONS Enable	Whether to open the SIP OPTION function
Initial Reg With Authorization	Whether to carry the certification information when registering
Reply 182 On Call Waiting	Whether or not to send 182 when the call is waiting
NAT Keep-alive Interval(10-60s)	The time interval for sending empty packets
Anonymous Call	Whether anonymous calls are enabled
Anonymous Call Block	Whether to enable anonymous call blocking
Proxy DNS Type	Set the DNS server type, the optional items are Type A, DNS SRV, and Auto
Use OB Proxy In Dialog	Whether the OB agent is used in the conversation
Complete Register	Whether to enable full registration
Reg Subscribe Enable	When enabled, the subscription message is sent after the registration message; the subscription message is not sent when disabled
Reg Subscribe Interval(sec)	
Dial Prefix	Dial before prefix
User Type	Whether the end user is IP or Phone

Hold Method	Call hold is REINVITE or INFO
Request-URI User Check	Whether to allow the user to check
Only Recv Request From Server	If enabled, will only accept requests from the server, do not accept other requests
Server Address	SIP server address
SIP Received Detection	Whether to allow SIP receive detection
VPN	Whether to enable VPN
SIP Encrypt Type	Whether to allow SIP message encryption
RTP Encrypt Type	Whether to allow RTP message encryption
Country Code	Country code
Remove Country Code	Whether to allow the removal of national codes
Tel URL	Whether to open the Tel URL
Use Random SIP Port	Whether to use the minimum random port
Min Random SIP Port	SIP minimum random port
Max Random SIP Port	SIP maximum random port
Prefer Primary SIP Server	Whether to enable the preferred primary server
Hold SDP Attribute Inactive	Whether to enable the call to keep the inactive attribute
Remove All Bindings	
VAD&CNG	
RTP Port Min	RTP minimum port
RTP Port Max	RTP's maximum port

Preferences

Preferences

Table 50 Preferences



Preferences

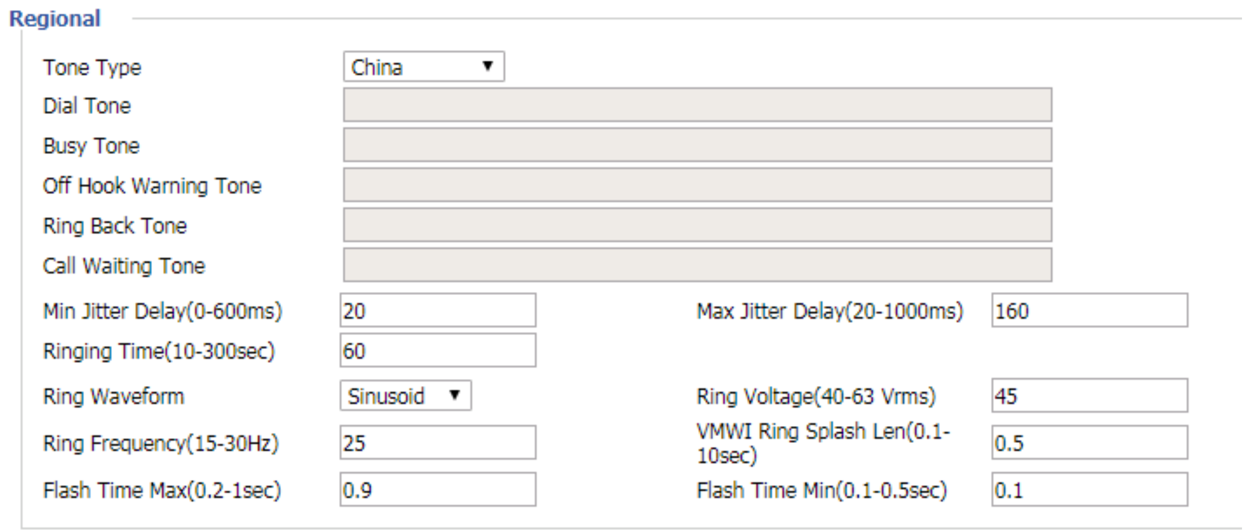
Volume Settings

Handset Input Gain	5	Handset Volume	5
DTMF Volume (0~-45)	-19		

Field Name	Description
Handset Input Gain	Adjust the handset input gain from 0 to 7.
Handset Volume	Adjust the output gain from 0 to 7.
DTMF Volume (0~-45)	Default is -19, you can set a range of values is 0~ -45

Regional

Table 51 Regional



Regional

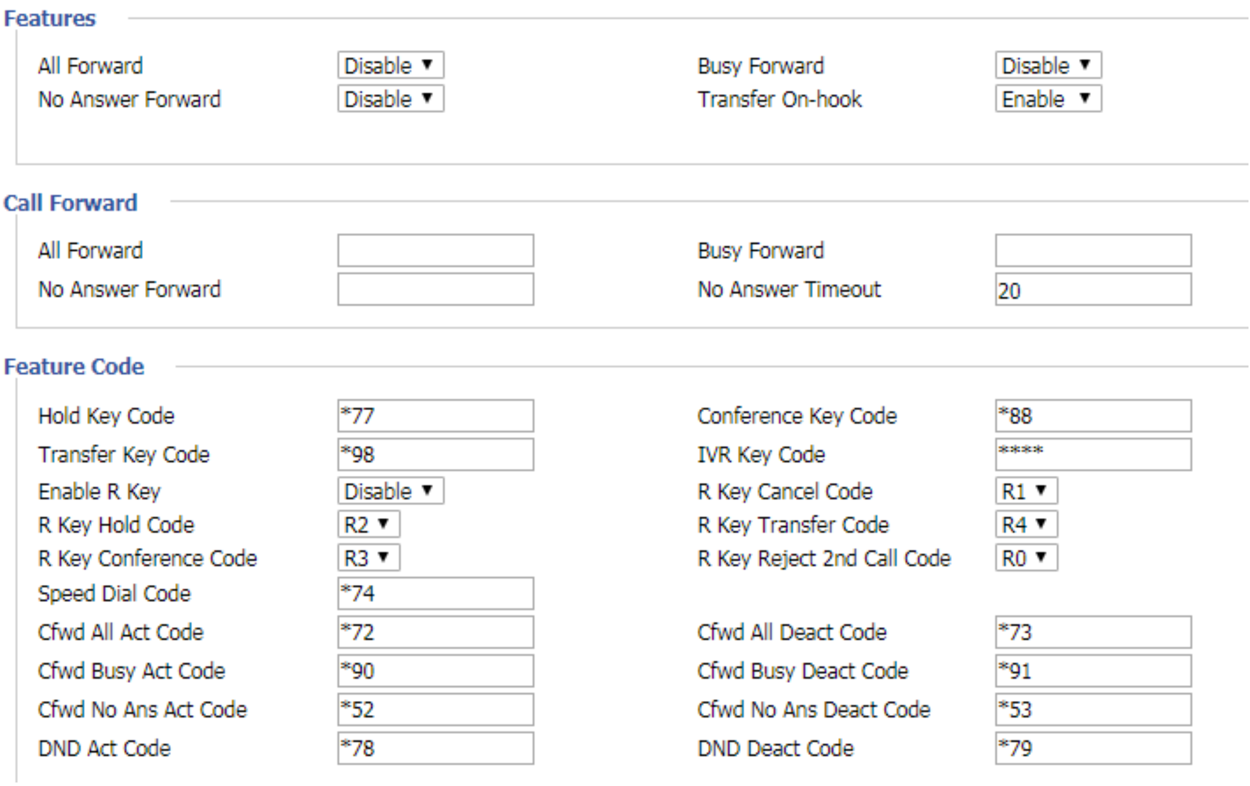
Tone Type	China		
Dial Tone			
Busy Tone			
Off Hook Warning Tone			
Ring Back Tone			
Call Waiting Tone			
Min Jitter Delay(0-600ms)	20	Max Jitter Delay(20-1000ms)	160
Ringing Time(10-300sec)	60		
Ring Waveform	Sinusoid	Ring Voltage(40-63 Vrms)	45
Ring Frequency(15-30Hz)	25	VMWI Ring Splash Len(0.1-10sec)	0.5
Flash Time Max(0.2-1sec)	0.9	Flash Time Min(0.1-0.5sec)	0.1

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 CnPilot Home R190/R200x 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

Features and Call Forward

Table 52 Features and call forward



Features

All Forward	Disable ▼	Busy Forward	Disable ▼
No Answer Forward	Disable ▼	Transfer On-hook	Enable ▼

Call Forward

All Forward		Busy Forward	
No Answer Forward		No Answer Timeout	20

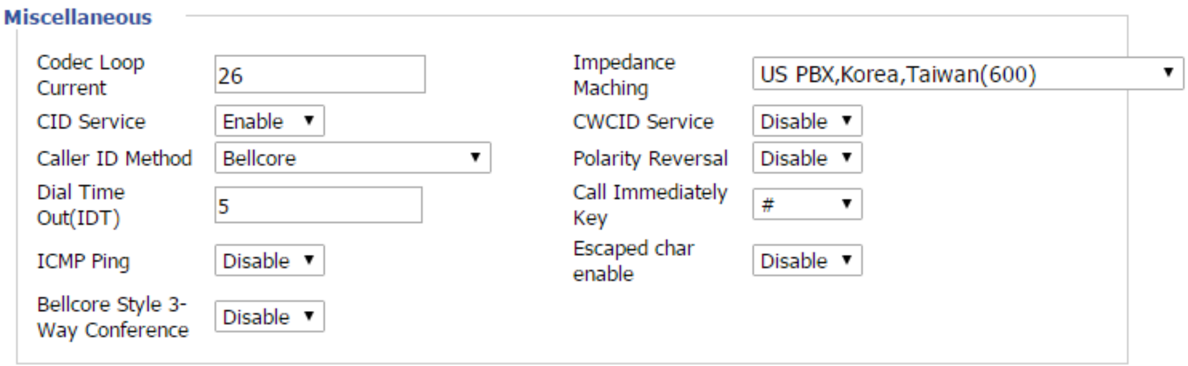
Feature Code

Hold Key Code	*77	Conference Key Code	*88
Transfer Key Code	*98	IVR Key Code	****
Enable R Key	Disable ▼	R Key Cancel Code	R1 ▼
R Key Hold Code	R2 ▼	R Key Transfer Code	R4 ▼
R Key Conference Code	R3 ▼	R Key Reject 2nd Call Code	R0 ▼
Speed Dial Code	*74		
Cfwd All Act Code	*72	Cfwd All Deact Code	*73
Cfwd Busy Act Code	*90	Cfwd Busy Deact Code	*91
Cfwd No Ans Act Code	*52	Cfwd No Ans Deact Code	*53
DND Act Code	*78	DND Deact Code	*79

Field Name		Description
Features	All Forward	Enable/Disable forward all calls
	Busy Forward	Enable/Disable busy forward.
	No Answer Forward	Enable/Disable no answer forward.
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	Call hold signatures, default is *77.
	Conference key	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	Enable/Disable 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.
	R Key Reject 2nd Call Code	Set the R key Reject 2nd Call code, options are ranged from R1 to R9, default value is R0.
	Speed Dial Code	Speed dial code, default is *74.

Miscellaneous

Table 53 Miscellaneous



Miscellaneous

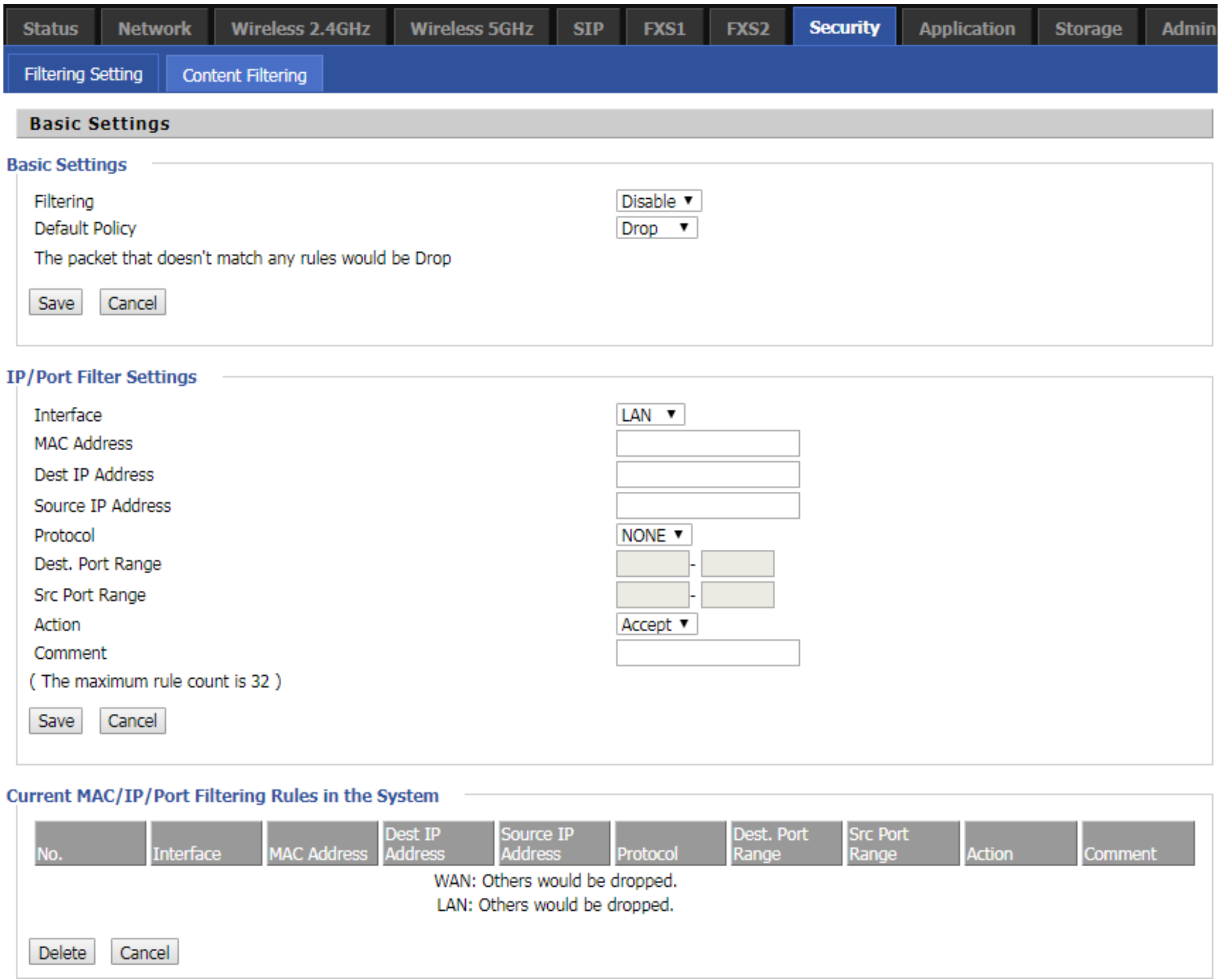
Codec Loop Current	26	Impedance Maching	US PBX,Korea,Taiwan(600)
CID Service	Enable	CWCID Service	Disable
Caller ID Method	Bellcore	Polarity Reversal	Disable
Dial Time Out(IDT)	5	Call Immediately Key	#
ICMP Ping	Disable	Escaped char enable	Disable
Bellcore Style 3-Way Conference	Disable		

Field Name	Description
Codec Loop Current	Set off-hook loop current, default is 26
Impedance Matching	Set impedance matching, default is US PBX, Korea, Taiwan(600).
CID service	Enable/Disable 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	Enable/Disable CWCID. If enable, the device will display the waiting call's caller ID, or it won't display. Default is disable.
Dial Time Out	How long device will sound dial out tone when device dials a number.
Call Immediately Key	Choose call immediately key form * or #.
ICMP Ping	Enable/Disable 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.
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 #

Security

Filtering Setting

Table 54 Filtering Setting



Basic Settings

Basic Settings

Filtering	Disable ▾
Default Policy	Drop ▾

The packet that doesn't match any rules would be Drop

IP/Port Filter Settings

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

(The maximum rule count is 32)

Current MAC/IP/Port Filtering Rules in the System

No.	Interface	MAC Address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Comment

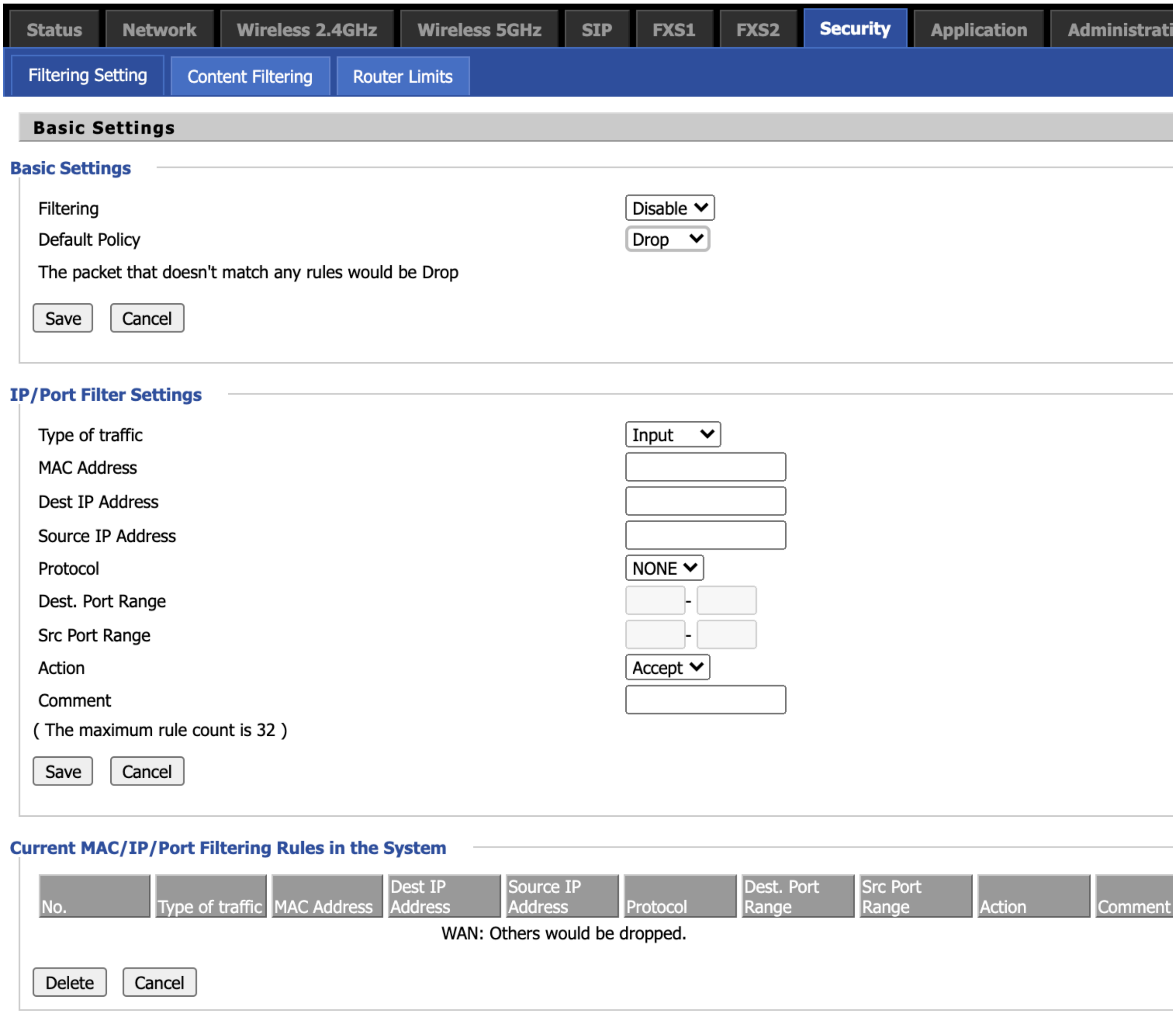
WAN: Others would be dropped.
LAN: Others would be dropped.

Field Name	Description
Filtering	If or not enable filter function
Default Policy	Choose to give up or accept
Mac address	Add the Mac address filtering
Dest IP address	Dest IP address
Source IP address	Source IP address
Protocol	Select a protocol name, support for TCP, UDP and TCP&UDP
Dest. Port Range	Destination port ranges
Src Port Range	Source port range

Action	You can choose to receive or give up; this should be consistent with the default policy.
Comment	Add callout
Delete	Delete selected item

Content Filtering

Table 55 Content Filtering



Basic Settings

Basic Settings

Filtering: Disable

Default Policy: Drop

The packet that doesn't match any rules would be Drop

Save Cancel

IP/Port Filter Settings

Type of traffic: Input

MAC Address:

Dest IP Address:

Source IP Address:

Protocol: NONE

Dest. Port Range: -

Src Port Range: -

Action: Accept

Comment:

(The maximum rule count is 32)

Save Cancel

Current MAC/IP/Port Filtering Rules in the System

No.	Type of traffic	MAC Address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Comment

WAN: Others would be dropped.

Delete Cancel

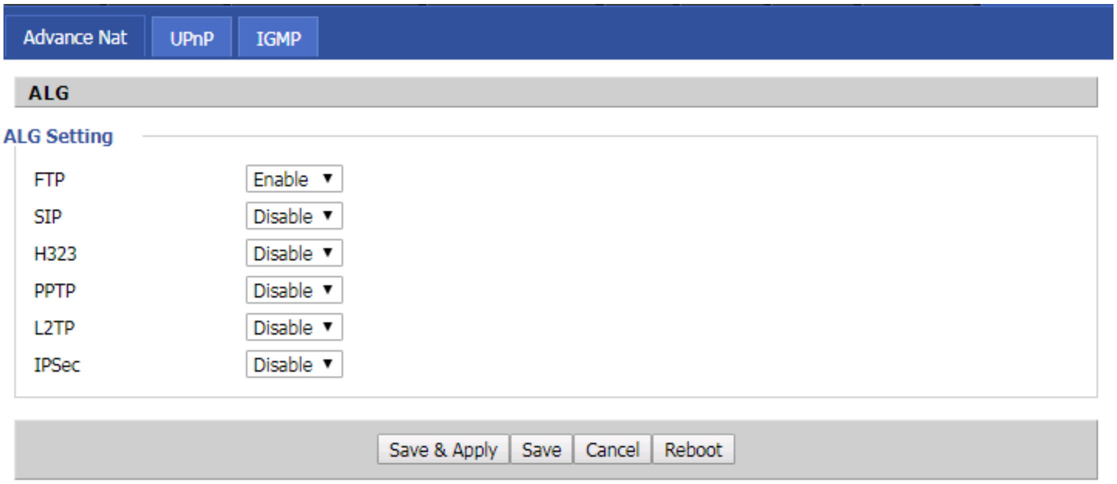
Field Name	Description
Filtering	Enable/Disable content Filtering
Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL Filters	List the URL filtering rules that already existed (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules

Add a URL Filter	Add URL filtering rules
Add/Cancel	Click adds to add one rule or click cancel
Current Website Host Filters	List the keywords that already exist (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules the existing keywords
Add a Host Filter	Add keywords
Add/Cancel	Click the Add or cancel

Application

Advance NAT

Table56 advance NAT



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

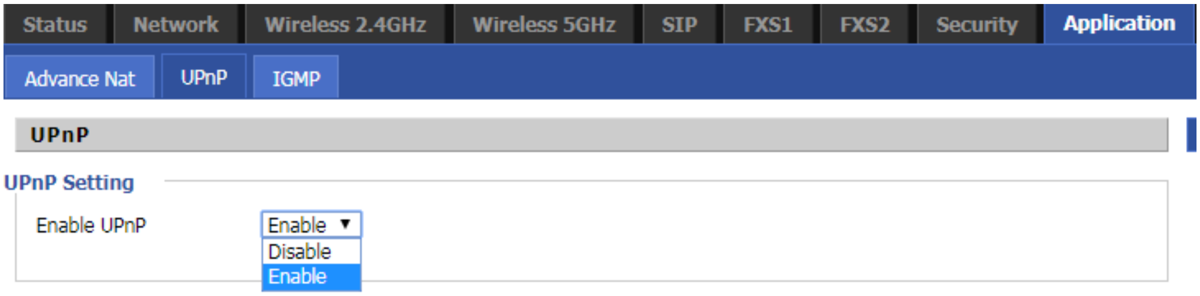
Description
Enable/Disable these function(FTP/SIP/H323/PPTP/L2TP/IPSec).

UPnP

UPnP (Universal Plug and Play) supports zero-configuration networking, and can automatically discover a variety of networked devices. When UPnP is enabled, the connected device is allowed to access the network, obtain an IP address, and convey performance information. If the network has a DHCP and DNS server, the connected device can automatically obtain DHCP and DNS services.

UPnP devices can be automatically added to the network without affecting previously-connected devices.

Table 57 UPnP



Enable UPnP Enable

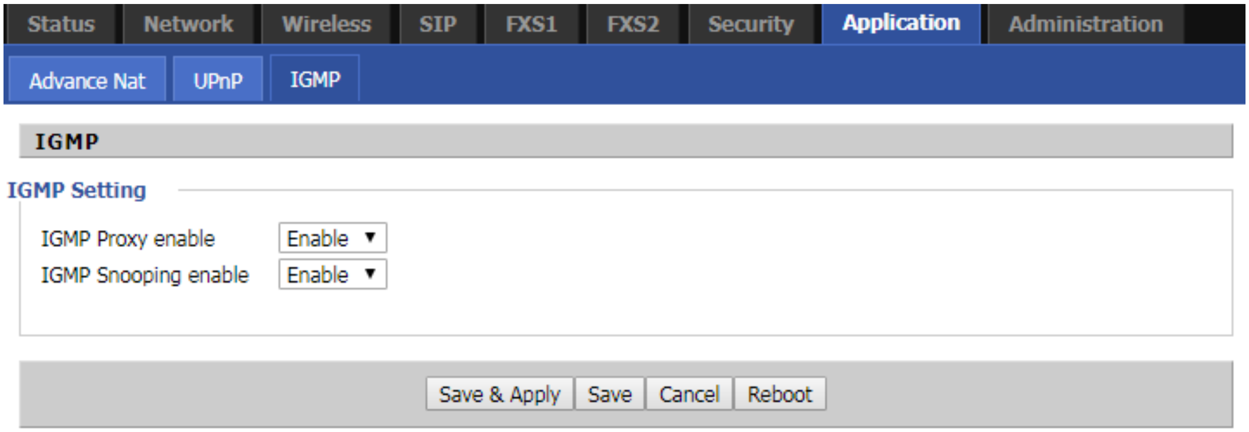
Field Name	Description
UPnP enable	Enable/Disable UPnP function.

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.

Table 58 IGMP



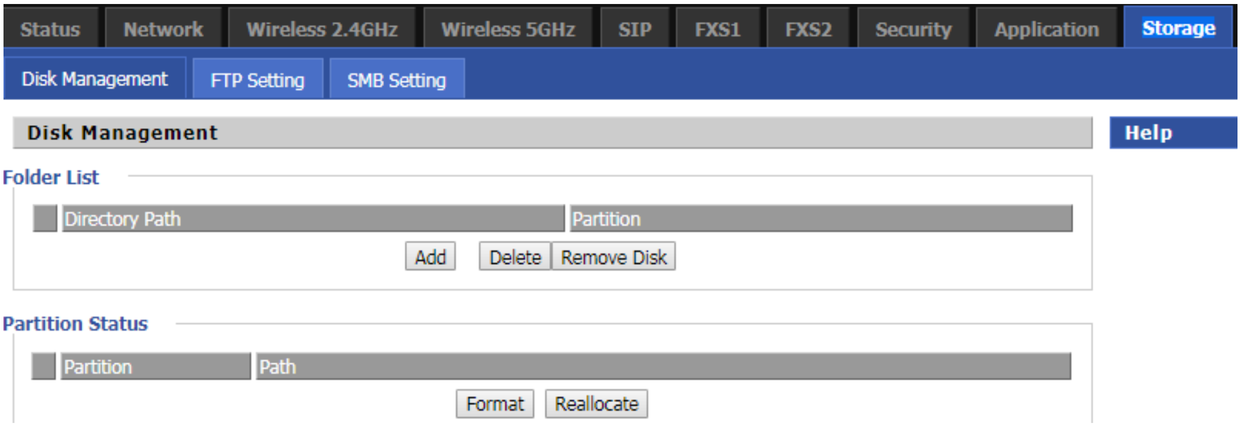
IGMP Proxy enable: Enable
IGMP Snooping enable: Enable

Field Name	Description
IGMP Proxy Enable	Enable/Disable IGMP Proxy function.
IGMP Snooping Enable	Enable/Disable IGMP Snooping function.

Storage(Only for AC1000M/MS)

Disk Management

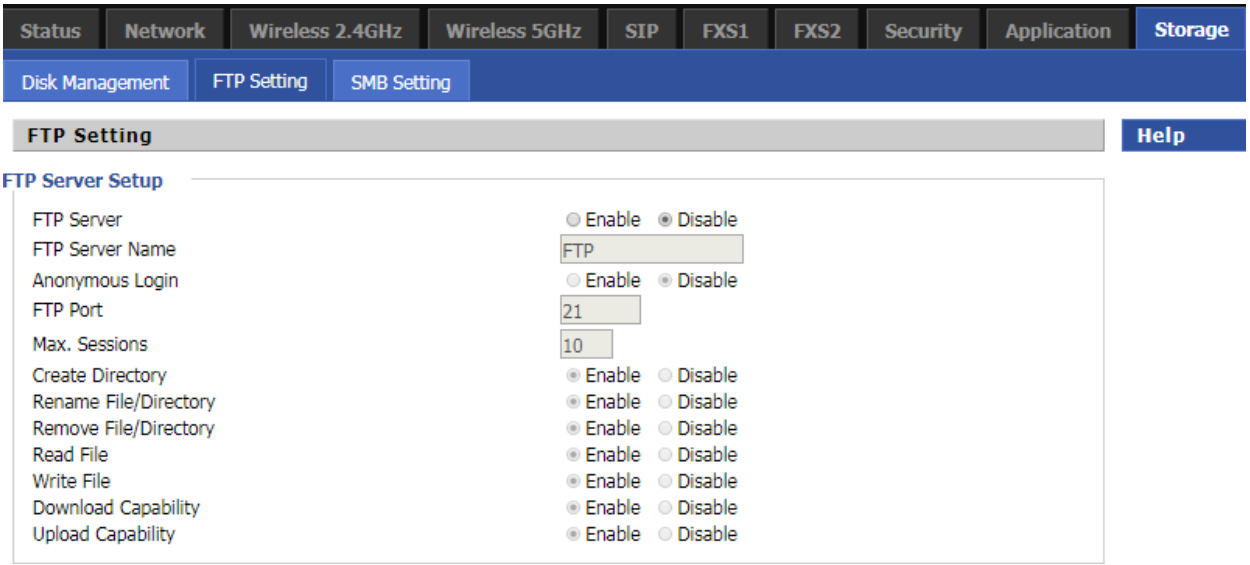
Table 59 Disk Management



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

FTP Setting

Table 60 FTP Setting



FTP Setting

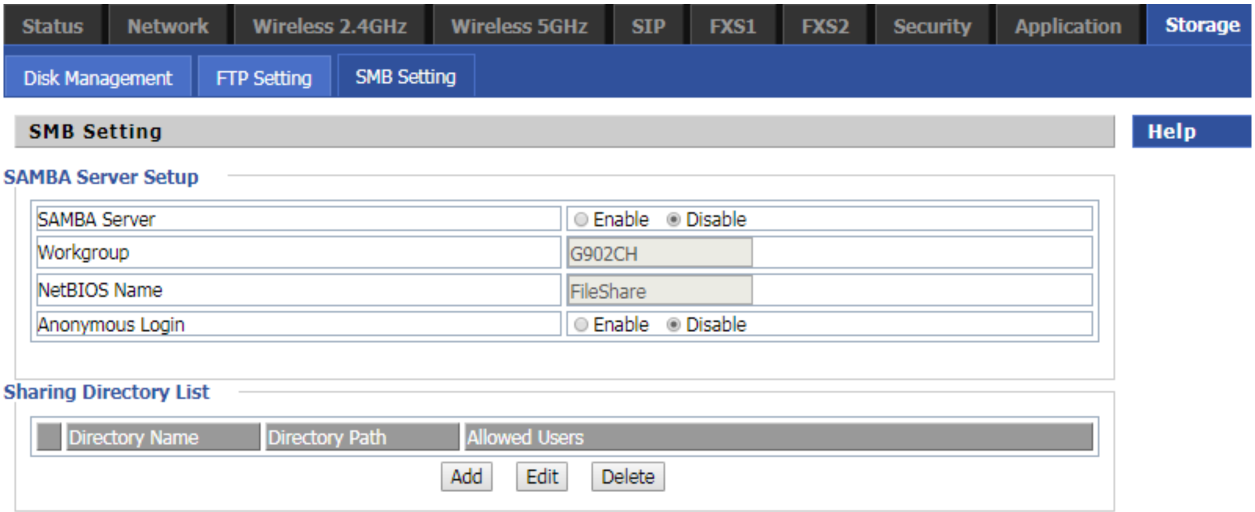
FTP Server Setup

FTP Server	○ Enable ● Disable
FTP Server Name	FTP
Anonymous Login	○ Enable ● Disable
FTP Port	21
Max. Sessions	10
Create Directory	● Enable ○ Disable
Rename File/Directory	● Enable ○ Disable
Remove File/Directory	● Enable ○ Disable
Read File	● Enable ○ Disable
Write File	● Enable ○ Disable
Download Capability	● Enable ○ Disable
Upload Capability	● Enable ○ Disable

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

SMB Setting

Table 61 SMB Setting



SMB Setting

SAMBA Server Setup

SAMBA Server	○ Enable ● Disable
Workgroup	G902CH
NetBIOS Name	FileShare
Anonymous Login	○ Enable ● Disable

Sharing Directory List

	Directory Name	Directory Path	Allowed Users

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

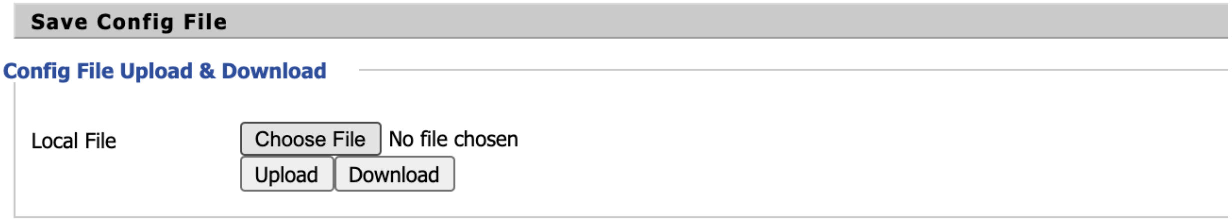
Administration

The user can manage the device in these webpages; you can configure the Time/Date, password, web access, system log and associated configuration TR069.

Management

Save config file

Table 62 Save Config File

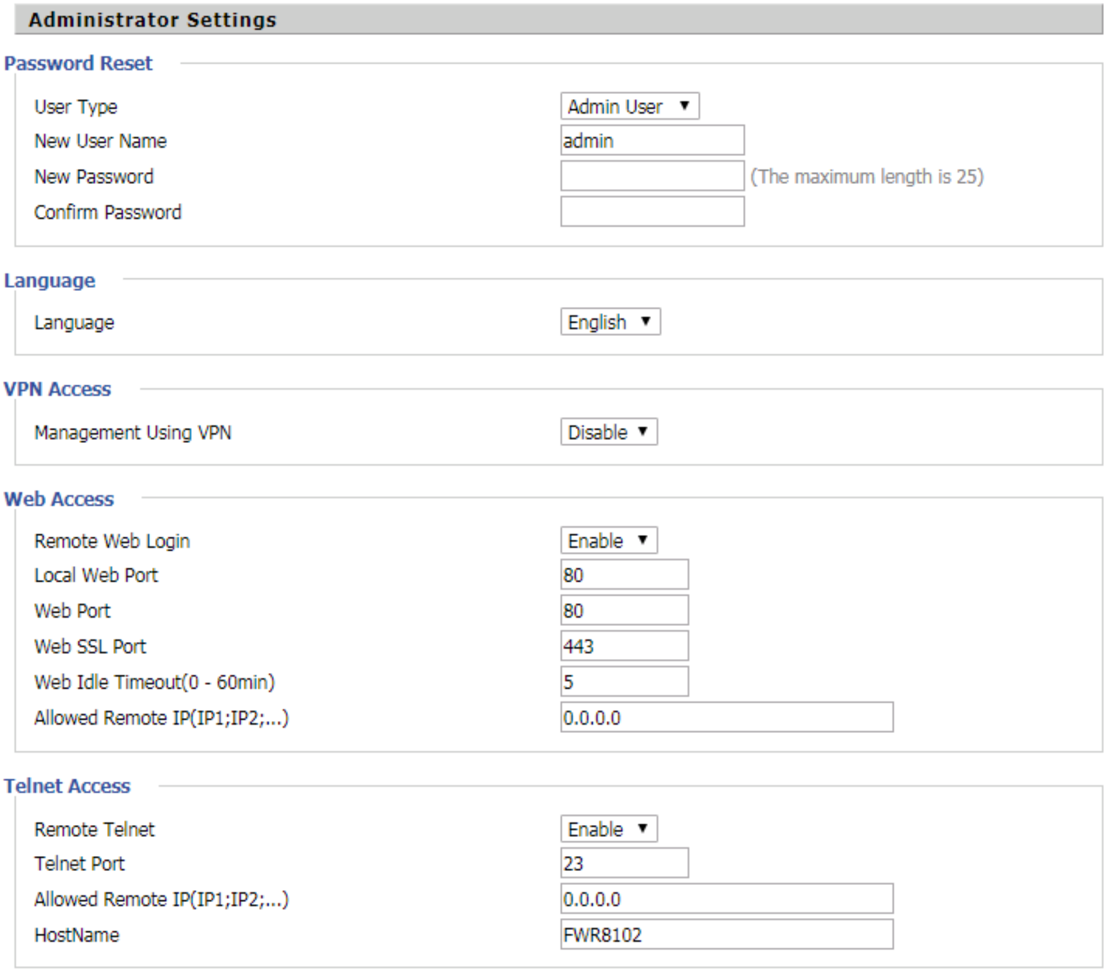


Local File No file chosen

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

Administrator settings

Table 63 Administrator settings



Administrator Settings

Password Reset

User Type	Admin User ▼
New User Name	admin
New Password	(The maximum length is 25)
Confirm Password	

Language

Language	English ▼

VPN Access

Management Using VPN	Disable ▼

Web Access

Remote Web Login	Enable ▼
Local Web Port	80
Web Port	80
Web SSL Port	443
Web Idle Timeout(0 - 60min)	5
Allowed Remote IP(IP1;IP2;...)	0.0.0.0

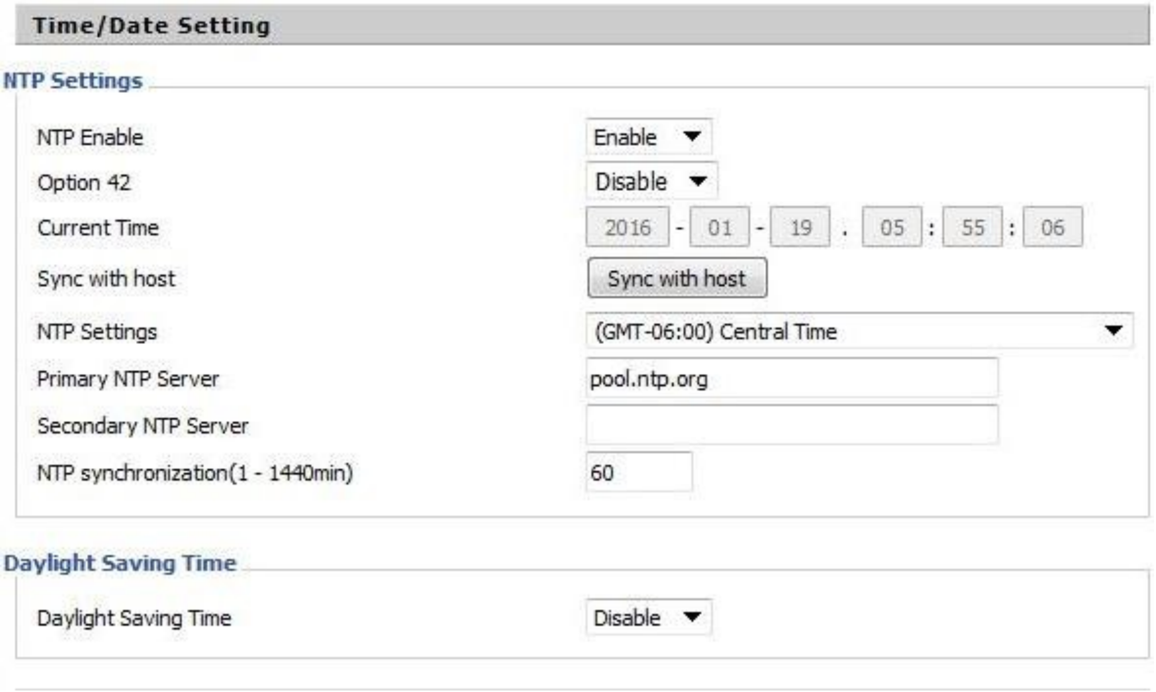
Telnet Access

Remote Telnet	Enable ▼
Telnet Port	23
Allowed Remote IP(IP1;IP2;...)	0.0.0.0
HostName	FWR8102

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	Enable/Disable 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 from which a user can login the device remotely
Telnet Port	Set the port value which is used to telnet to the device

NTP settings

Table 64 NTP settings



Time/Date Setting

NTP Settings

NTP Enable	Enable
Option 42	Disable
Current Time	2016 - 01 - 19 . 05 : 55 : 06
Sync with host	Sync with host
NTP Settings	(GMT-06:00) Central Time
Primary NTP Server	pool.ntp.org
Secondary NTP Server	
NTP synchronization(1 - 1440min)	60

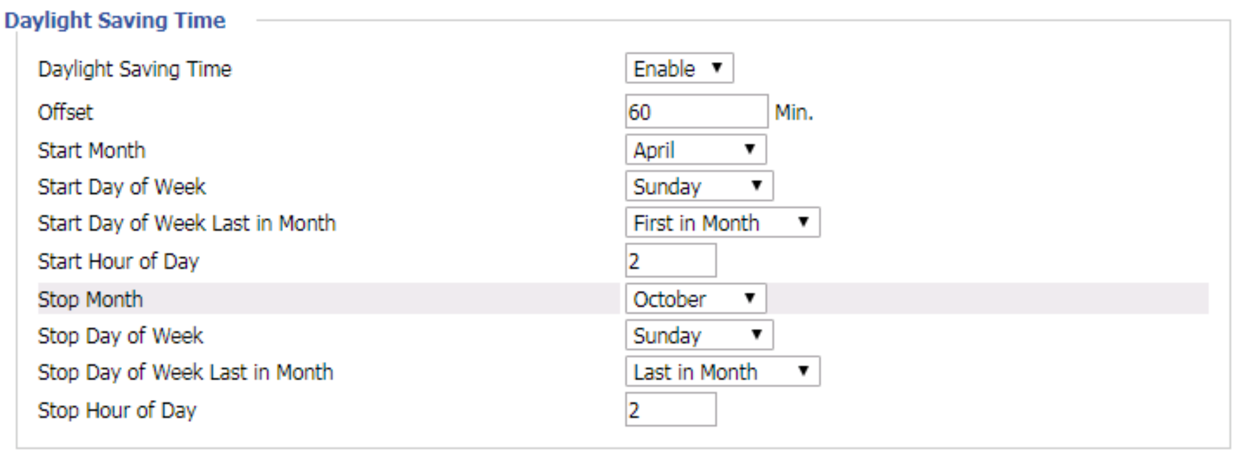
Daylight Saving Time

Daylight Saving Time	Disable

Field Name	Description
NTP Enable	Enable/Disable NTP
Option 42	Enable/Disable DHCP option 42. This option specifies a list of the NTP servers available to the client by IP address
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

Daylight Saving Time

Table 65 Daylight Saving Time



Daylight Saving Time

Daylight Saving Time	Enable ▼
Offset	60 Min.
Start Month	April ▼
Start Day of Week	Sunday ▼
Start Day of Week Last in Month	First in Month ▼
Start Hour of Day	2
Stop Month	October ▼
Stop Day of Week	Sunday ▼
Stop Day of Week Last in Month	Last in Month ▼
Stop Hour of Day	2

Procedure

Step 1. Enable Daylight Savings Time.

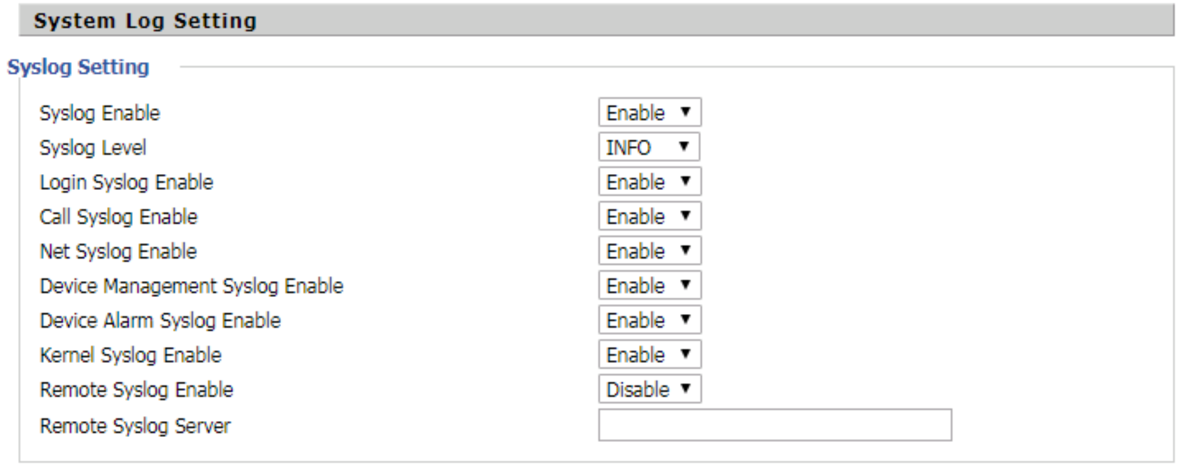
Step 2. Set value of offset for Daylight Savings Time

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.

Step 4.Press Saving button to save and press Reboot button to active changes.

System Log Setting

Table 66 System log Setting



System Log Setting

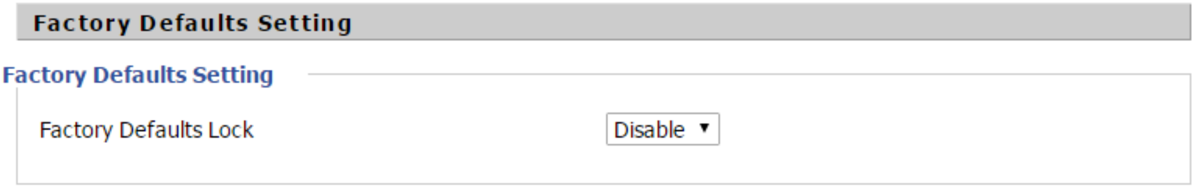
Syslog Setting

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

Field Name	Description
Syslog Enable	Enable/Disable 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	Enable/Disable remote syslog function
Remote Syslog server	Add a remote server IP address
Syslog Enable	Enable/Disable syslog function

Factory Defaults Setting

Table 67 Factory Defaults Setting



Factory Defaults Setting

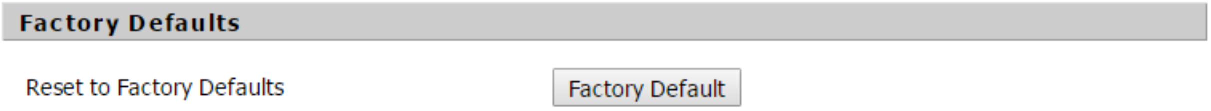
Factory Defaults Setting

Factory Defaults Lock: Disable

Description
When enabled, the device may not be reset to factory defaults until this parameter is reset to Disable

Factory Defaults

Table 68 Factory Defaults



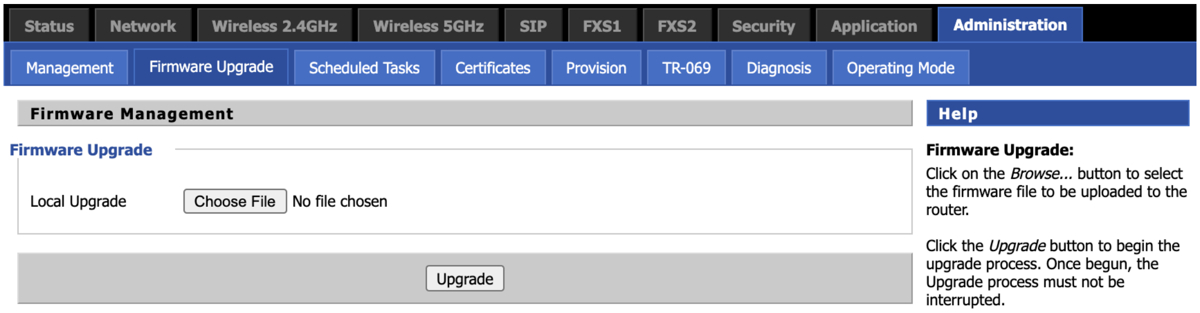
Factory Defaults

Reset to Factory Defaults

Description
Click Factory Default to restore the residential gateway to factory settings

Firmware Upgrade

Table 69 Firmware upgrade



Firmware Management

Firmware Upgrade

Local Upgrade Choose File No file chosen

Help

Firmware Upgrade:
Click on the *Browse...* button to select the firmware file to be uploaded to the router.

Click the *Upgrade* button to begin the upgrade process. Once begun, the Upgrade process must not be interrupted.

Description
1. Choose upgrade file type from Image File and Dial Rule
2. Press “Browse..” button to browser file
3. Press Upgrade to start upgrading

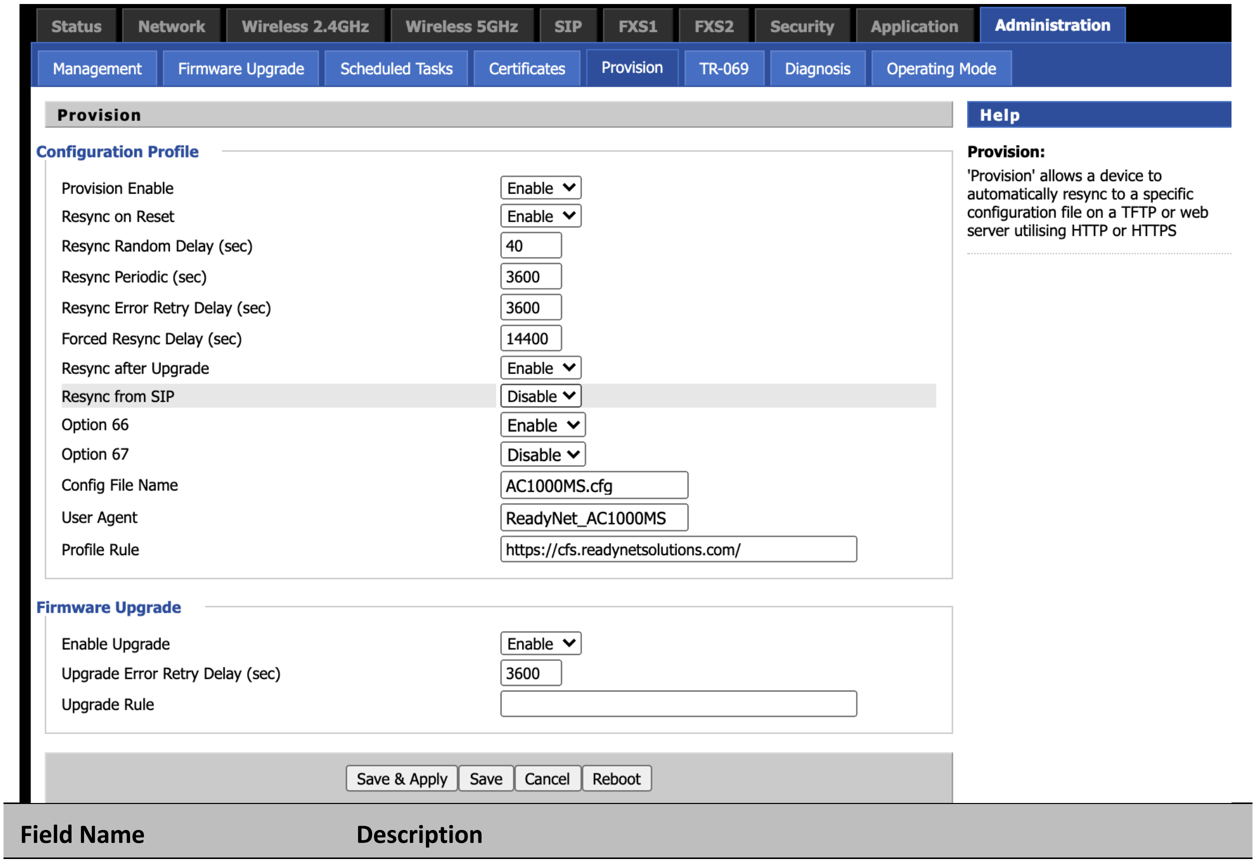
Provision

Provisioning allows the router to auto-upgrade and auto-configure devices which support TFTP, HTTP and HTTPs .

- Before testing or using TFTP, user should have tftp server and upgrading file and configuring file.
- Before testing or using HTTP, user should have http server and upgrading file and configuring file.
- 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

User can upload a CA Certificate file and Client Certificate file and Private Key file in the Security page.

Table 70 Provision



Provision

Configuration Profile

Provision Enable	Enable
Resync on Reset	Enable
Resync Random Delay (sec)	40
Resync Periodic (sec)	3600
Resync Error Retry Delay (sec)	3600
Forced Resync Delay (sec)	14400
Resync after Upgrade	Enable
Resync from SIP	Disable
Option 66	Enable
Option 67	Disable
Config File Name	AC1000MS.cfg
User Agent	ReadyNet_AC1000MS
Profile Rule	https://cfs.readynetsolutions.com/

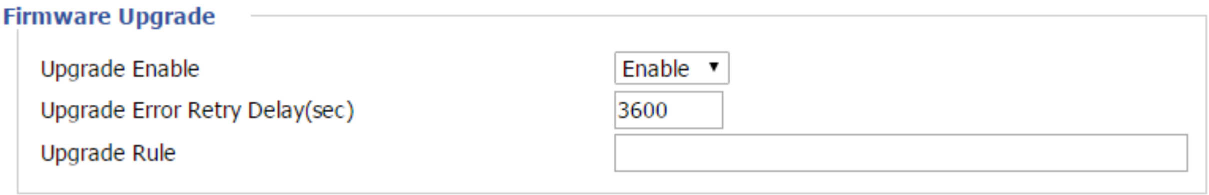
Firmware Upgrade

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

Provision:
'Provision' allows a device to automatically resync to a specific configuration file on a TFTP or web server utilising HTTP or HTTPS

Field Name	Description
Provision Enable	Enable provision or not.
Resync on Reset	Enable resync after restart or not
Resync Random	Set the maximum delay for the request of synchronization file. The default is 40
Resync Periodic(sec)	If the last resync was failure, The router will retry resync after the "Resync Error
Resync Error Retry	Set the periodic time for resync, default is 3600s
Forced Resync	If it's time to resync, but the device is busy now, in this case, the router will wait
Resync After	Enable firmware upgrade after resync or not. The default is Enabled
Resync From SIP	Enable/Disable resync from SIP
Option 66	It is used for In-house provision mode only. When use TFTP with option 66 to
Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to
Profile Rule	URL of profile provision file

Table 71 Firmware Upgrade



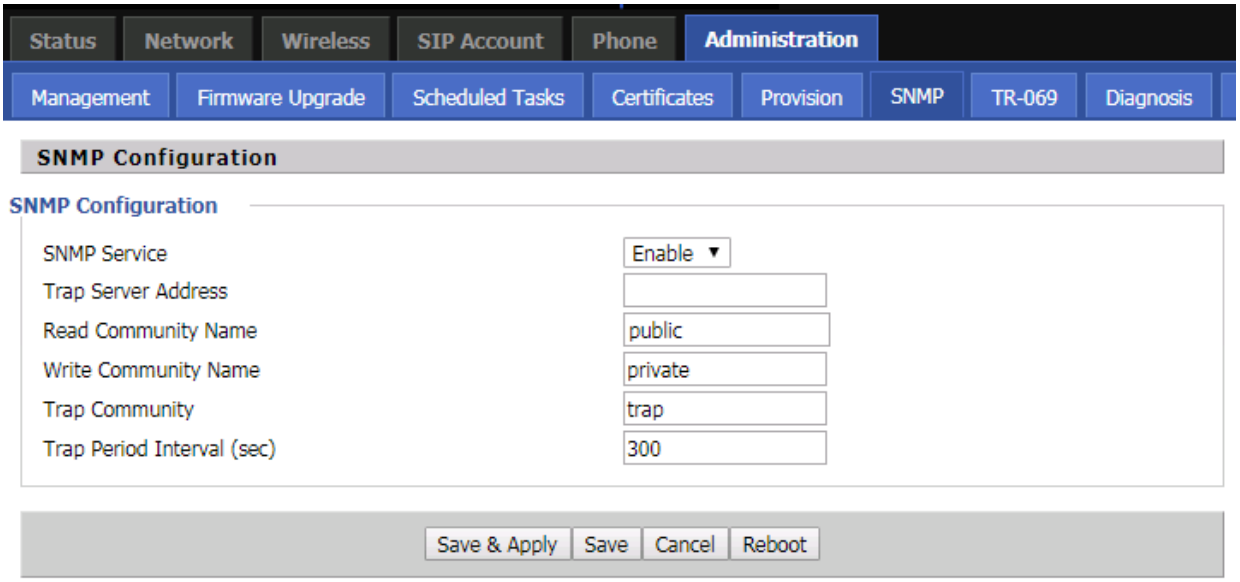
Firmware Upgrade

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

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

SNMP

Table 72 SNMP



SNMP Configuration

SNMP Configuration

SNMP Service	Enable ▼
Trap Server Address	
Read Community Name	public
Write Community Name	private
Trap Community	trap
Trap Period Interval (sec)	300

Field Name	Description
SNMP Service	Enable or Disable the SNMP service
Trap Server Address	Enter the trap server address for sending SNMP traps
Read Community Name	String value that is used as a password to request information via SNMP from the device
Write Community Name	String value that is used as a password to write configuration values to the device SNMP
Trap Community	String value used as a password for retrieving traps from the device
Trap period interval(sec)	The interval for which traps are sent from the device

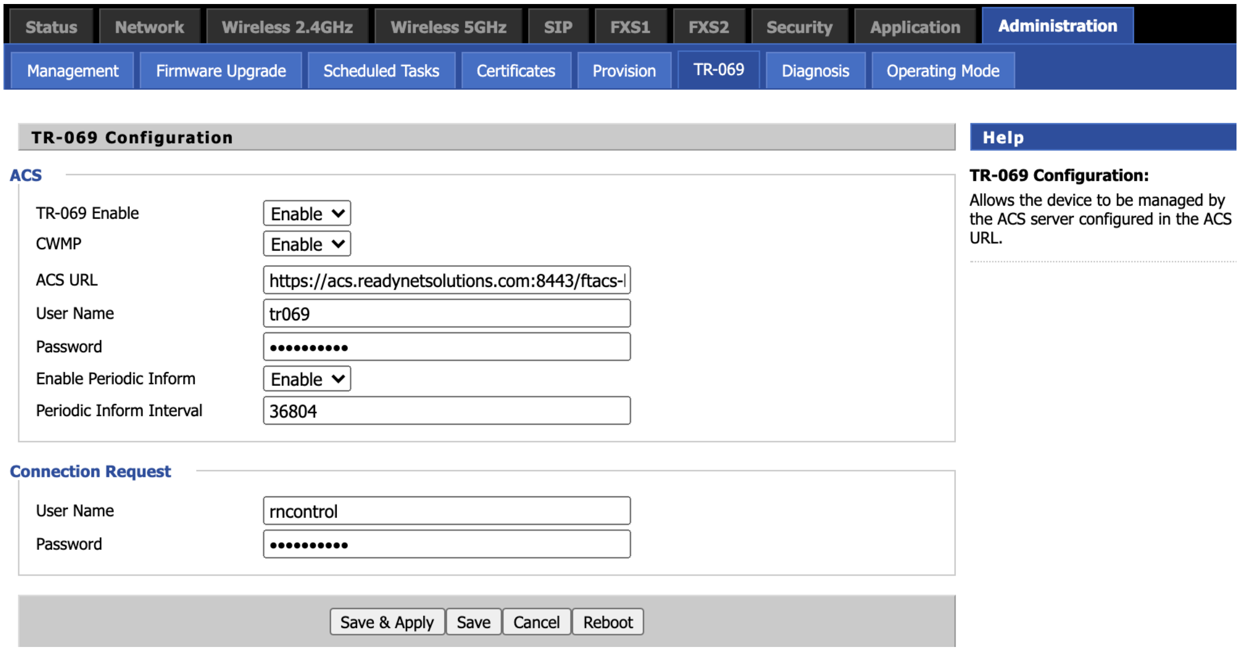
TR-069

TR-069 provides the possibility of auto configuration of internet access devices and reduces the cost of management. TR-069 (short for Technical Report 069) is a DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. Using TR-069, the terminals establish connection with the Auto Configuration Servers (ACS) and get configured automatically.

Device Configuration using TR-069

The TR-069 configuration page is available under Administration menu.

Table 73 TR069



TR-069 Configuration

ACS

TR-069 Enable	Enable
CWMP	Enable
ACS URL	https://acs.readynetsolutions.com:8443/ftacs-|
User Name	tr069
Password	••••••••••
Enable Periodic Inform	Enable
Periodic Inform Interval	36804

Connection Request

User Name	rncontrol
Password	••••••••••

Help

TR-069 Configuration:
Allows the device to be managed by the ACS server configured in the ACS URL.

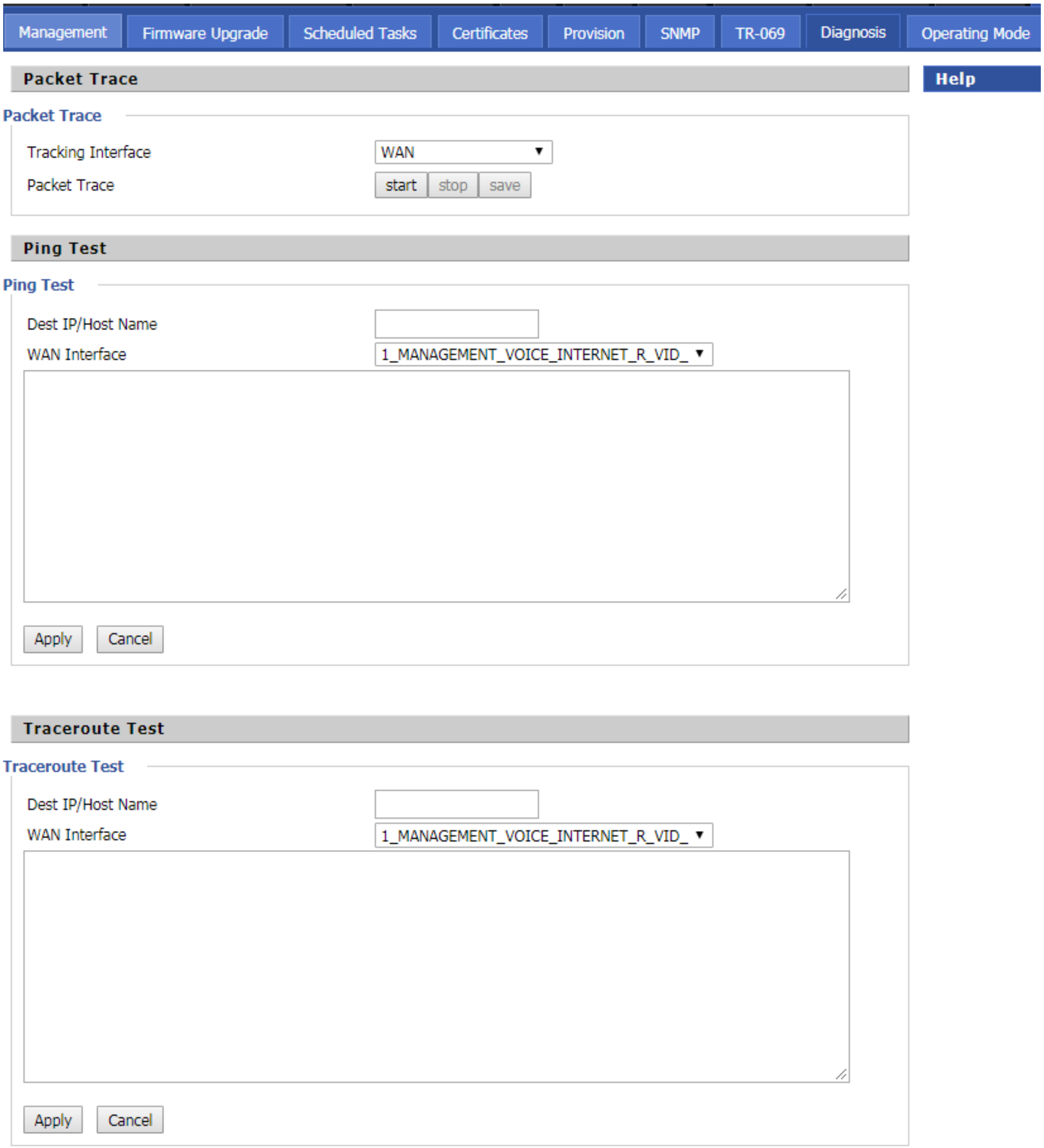
Field Name	Description
ACS parameters	
TR069 Enable	Enable or Disable TR069
CWMP	Enable or Disable CWMP
ACS URL	ACS URL address
User Name	ACS username
Password	ACS password

Periodic Inform Enable	Enable the function of periodic inform or not. By default it is Enabled
Periodic Inform Interval	Periodic notification interval with the unit in seconds. The default value is 3600s
Connect Request parameters	
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.

Diagnosis

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

Table 74 Diagnosis



Packet Trace

Packet Trace

Tracking Interface: WAN

Packet Trace

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface: 1_MANAGEMENT_VOICE_INTERNET_R_VID_

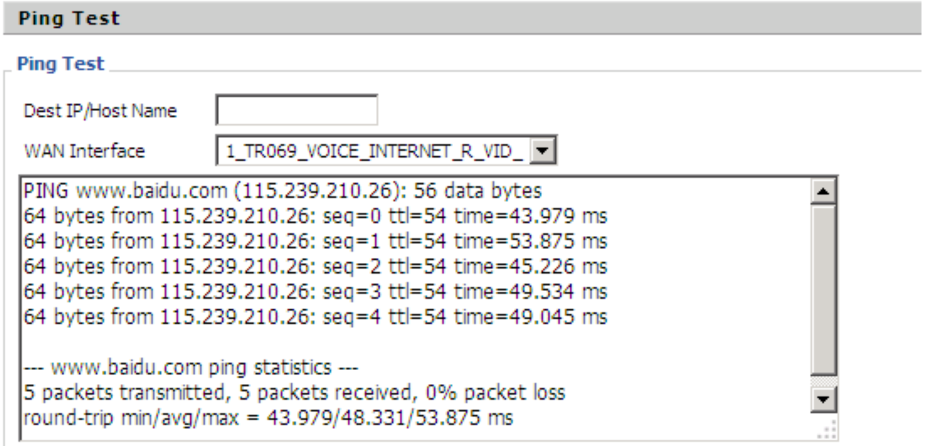
Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface: 1_MANAGEMENT_VOICE_INTERNET_R_VID_

Description
1. Packet Trace
Users can use the packet trace feature to intercept packets which traverse the device. Click the Start button to start home gateway tracking and keep refreshing the page until the message trace shows to stop, click the Save button to save captured packets.
2. Ping Test
Enter the destination IP or host name, and then click Apply, device will perform ping test.



Ping Test

Ping Test

Dest IP/Host Name

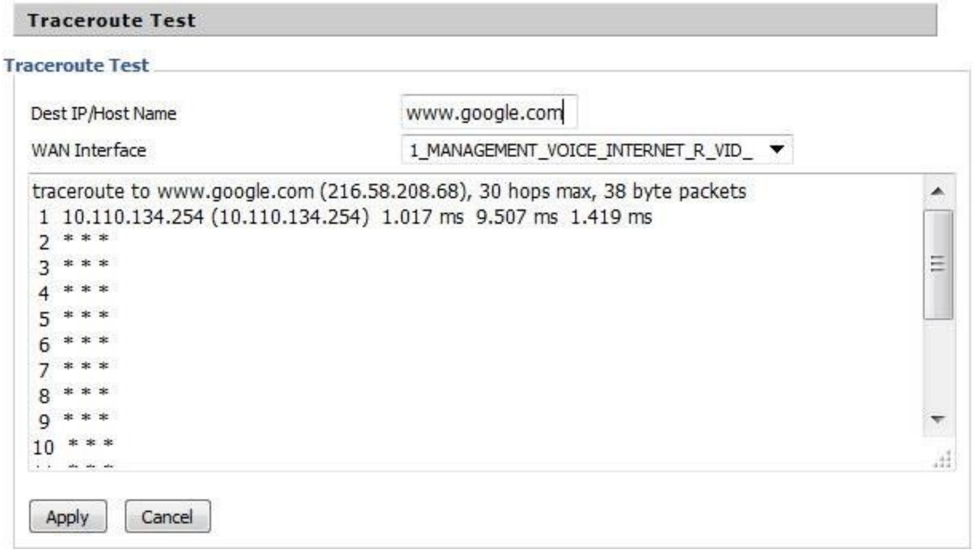
WAN Interface 1_TR069_VOICE_INTERNET_R_VID_

```
PING www.baidu.com (115.239.210.26): 56 data bytes
64 bytes from 115.239.210.26: seq=0 ttl=54 time=43.979 ms
64 bytes from 115.239.210.26: seq=1 ttl=54 time=53.875 ms
64 bytes from 115.239.210.26: seq=2 ttl=54 time=45.226 ms
64 bytes from 115.239.210.26: seq=3 ttl=54 time=49.534 ms
64 bytes from 115.239.210.26: seq=4 ttl=54 time=49.045 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 43.979/48.331/53.875 ms
```

3. Traceroute Test

Enter the destination IP or host name, and then click Apply, device will perform traceroute test.



Traceroute Test

Traceroute Test

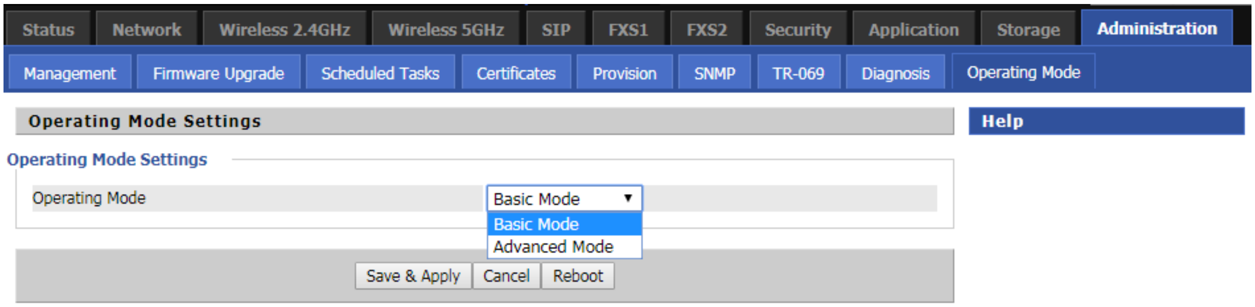
Dest IP/Host Name www.google.com

WAN Interface 1_MANAGEMENT_VOICE_INTERNET_R_VID_

```
traceroute to www.google.com (216.58.208.68), 30 hops max, 38 byte packets
 1  10.110.134.254 (10.110.134.254)  1.017 ms  9.507 ms  1.419 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Operating Mode

Table 75 Operating mode

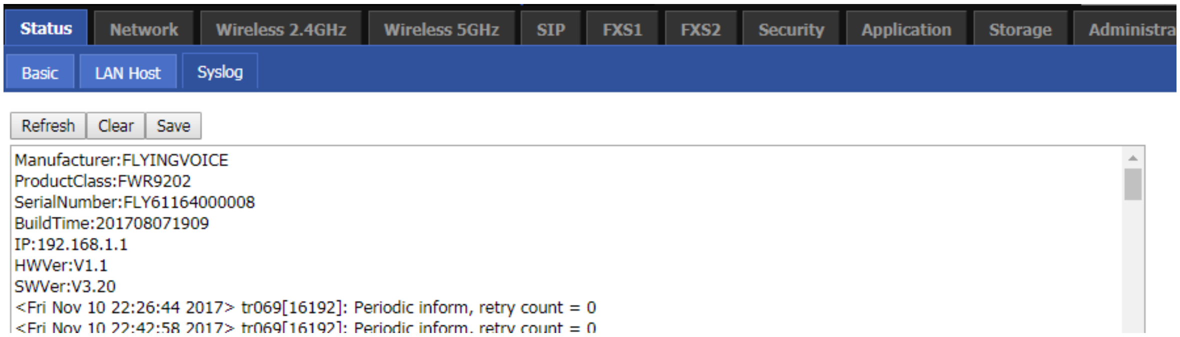


Operating Mode: Basic Mode

Description
Choose the Operation Mode as Basic Mode or Advanced Mode

System Log

Table 76 System log

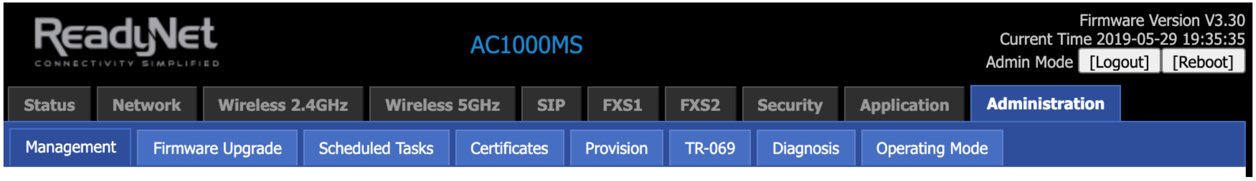


```
Manufacturer:FLYINGVOICE
ProductClass:FWR9202
SerialNumber:FLY61164000008
BuildTime:201708071909
IP:192.168.1.1
HWVer:V1.1
SWVer:V3.20
<Fri Nov 10 22:26:44 2017> tr069[16192]: Periodic inform, retry count = 0
<Fri Nov 10 22:42:58 2017> tr069[16192]: Periodic inform, retry count = 0
```

Description
If you enable the system log in Status/syslog webpage, you can view the system log in this webpage.

Logout

Table 77 Logout



Firmware Version V3.30
Current Time 2019-05-29 19:35:35

Description
Press the logout button to logout, and then the login window will appear.

Reboot

Press the Reboot button to reboot the device.

Chapter 4 IPv6 address configuration

The router devices support IPv6 addressing. This chapter covers:

- Introduction
- IPv6 Advance
- Configuring IPv6
- Viewing WAN port status
- IPv6 DHCP configuration for LAN/WLAN clients
- LAN DHCPv6

Introduction

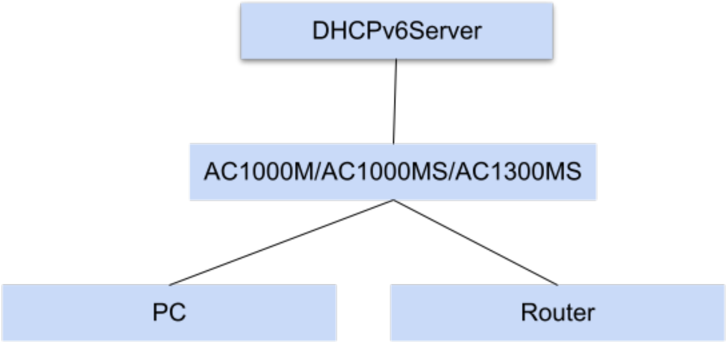
DHCPv6 protocol is used to automatically provision/configure IPv6 capable end points in a local network. In addition to acquiring an IPv6 IP address for the WAN interface and its associated LAN/WLAN clients, the devices are also capable of prefix delegation.

The Routers devices support the following types of modes of IPv6 addresses:

- Stateless DHCPv6
- Statefull DHCPv6

Table 78 IPv6 Modes

Mode	Description
Stateless	In Stateless DHCPv6 mode, the Routers devices listen for ICMPv6 Router Advertisements messages which are periodically sent out by the routers on the local link or requested by the node using a Router Advertisements solicitation message. The device derives a unique IPv6 address using prefix receives from the router and its own MAC address.
Statefull	In Statefull DHCPv6 mode, the client works exactly as IPv4 DHCP, in which hosts receive both their IPv6 addresses and additional parameters from the DHCP server.



IPv6 Advance

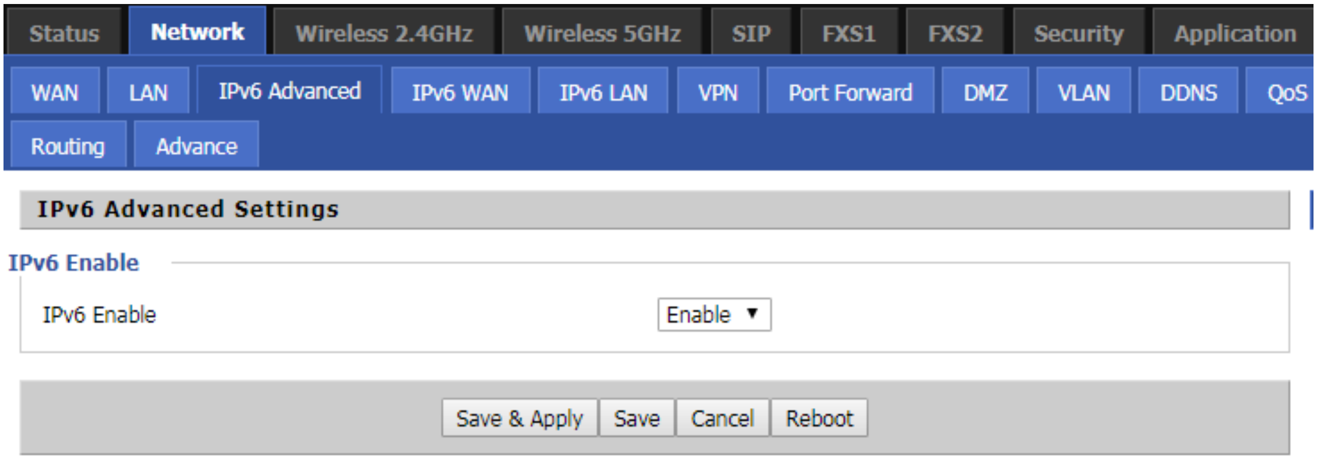
To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

Table 79 Enabling IPv6



IPv6 Advanced Settings

IPv6 Enable

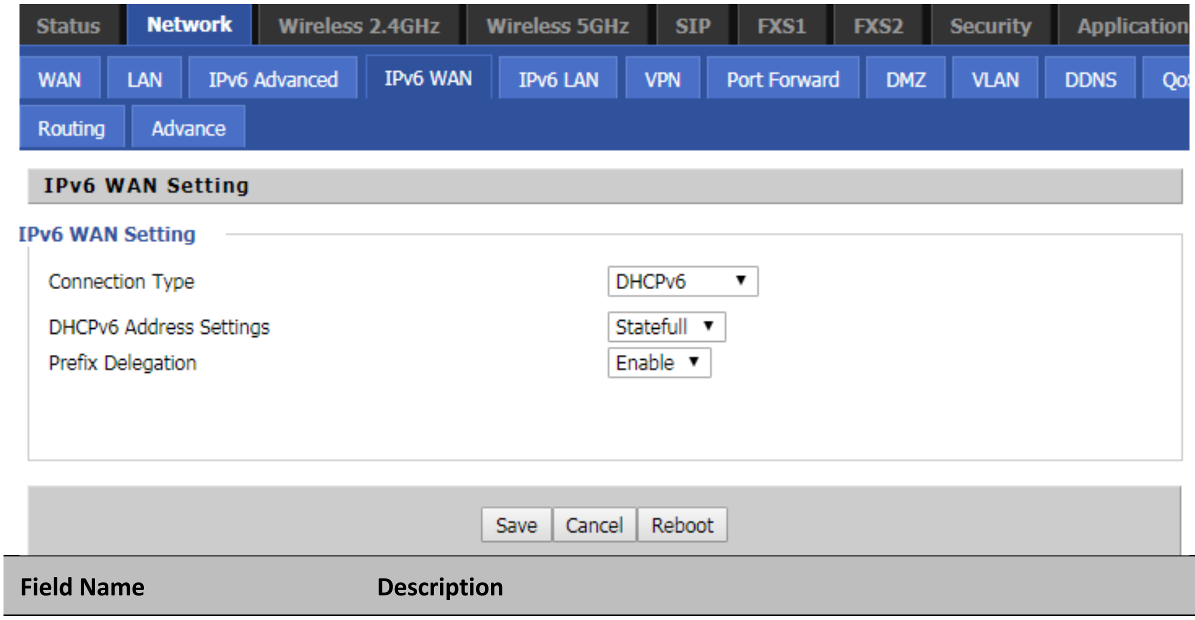
IPv6 Enable: Enable ▼

Configuring IPv6

Configuring Statefull IPv6

1. Navigate to Network > IPv6WAN page. The following window is displayed:

Table 80 Configuring Statefull IPv6



IPv6 WAN Setting

IPv6 WAN Setting

Connection Type: DHCPv6 ▼

DHCPv6 Address Settings: Statefull ▼

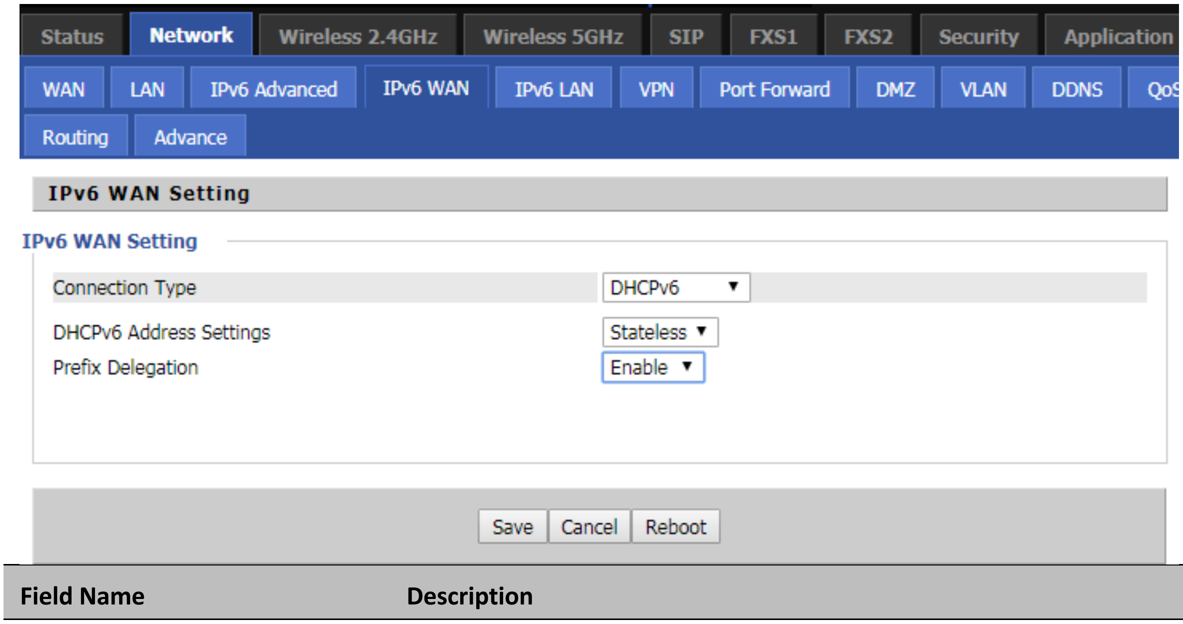
Prefix Delegation: Enable ▼

Field Name	Description
Connection Type	Select connection type

DHCPv6 Address Settings	Set it to statefull mode.
Prefix Delegation	Select Enable.

Configuring Stateless IPv6

Table 81 Configuring Stateless IPv6



IPv6 WAN Setting

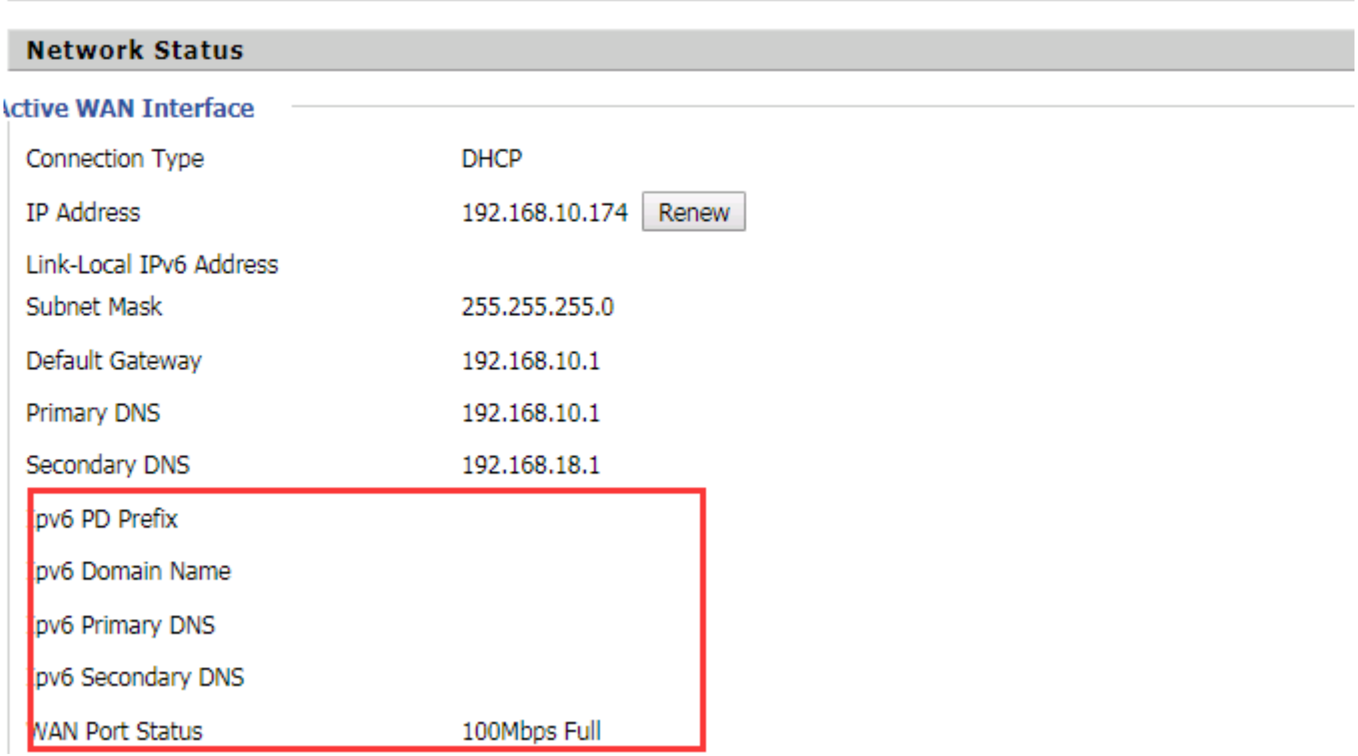
IPv6 WAN Setting

Connection Type	DHCPv6 ▼
DHCPv6 Address Settings	Stateless ▼
Prefix Delegation	Enable ▼

Field Name	Description
Connection Type	Select connection type
DHCPv6 Address Settings	Set it to stateless mode.
Prefix Delegation	Select Enable.

Viewing WAN port status

To view the status of WAN port:
Navigate to Status page.



Network Status

Active WAN Interface

Connection Type	DHCP
IP Address	192.168.10.174 Renew
Link-Local IPv6 Address	
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1
Ipv6 PD Prefix	
Ipv6 Domain Name	
Ipv6 Primary DNS	
Ipv6 Secondary DNS	
WAN Port Status	100Mbps Full

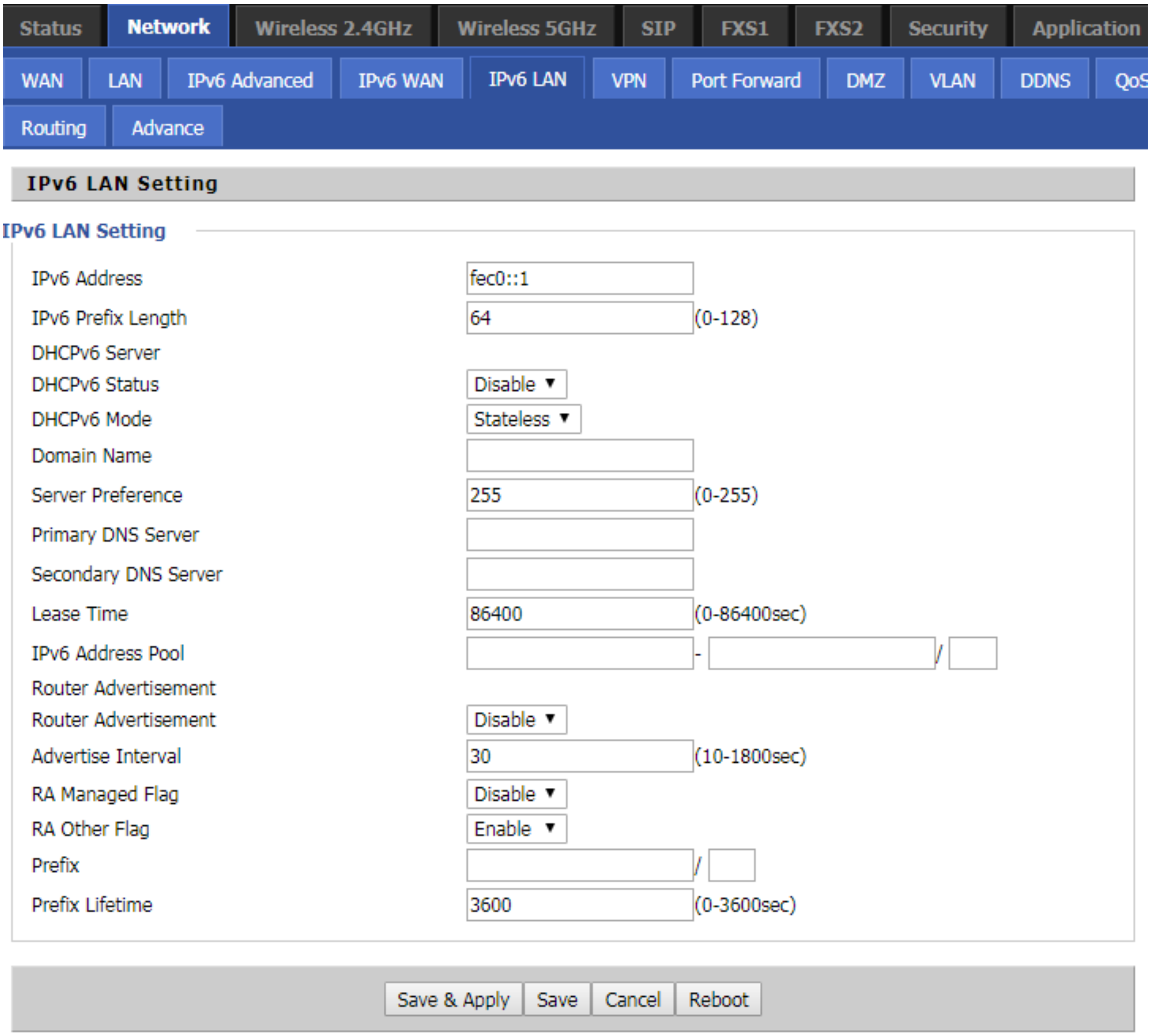
IPv6 DHCP configuration for LAN/WLAN clients

Wired and wireless clients connected to the Routers can obtain their IPv6 addresses based on how the LAN s ide DHCPv6 parameters are configured. The Routers can be either configured as a DHCPv6 server in which the LAN/WLAN clients get IPv6 addresses from the configured pool. If DHCP server is disabled on the Routers, the clients will get IPv6 addresses from the external DHCPv6 server configured in the network.

LAN DHCPv6

When IPv6 is enabled, the LAN/WLAN clients of Routers can be configured to receive IPv6 addresses from locally configured IPv6 pool or from an external DHCPv6 server.

To enable LAN DHCPv6 service:



IPv6 LAN Setting

IPv6 LAN Setting

IPv6 Address	fec0::1
IPv6 Prefix Length	64 (0-128)
DHCPv6 Server	
DHCPv6 Status	Disable ▼
DHCPv6 Mode	Stateless ▼
Domain Name	
Server Preference	255 (0-255)
Primary DNS Server	
Secondary DNS Server	
Lease Time	86400 (0-86400sec)
IPv6 Address Pool	- /
Router Advertisement	
Router Advertisement	Disable ▼
Advertise Interval	30 (10-1800sec)
RA Managed Flag	Disable ▼
RA Other Flag	Enable ▼
Prefix	/
Prefix Lifetime	3600 (0-3600sec)

Chapter 5 Troubleshooting Guide

This chapter covers:

- Configuring PC to get IP Address automatically
- Cannot connect to the Web GUI
- Forgotten Password

Configuring PC to get IP Address automatically

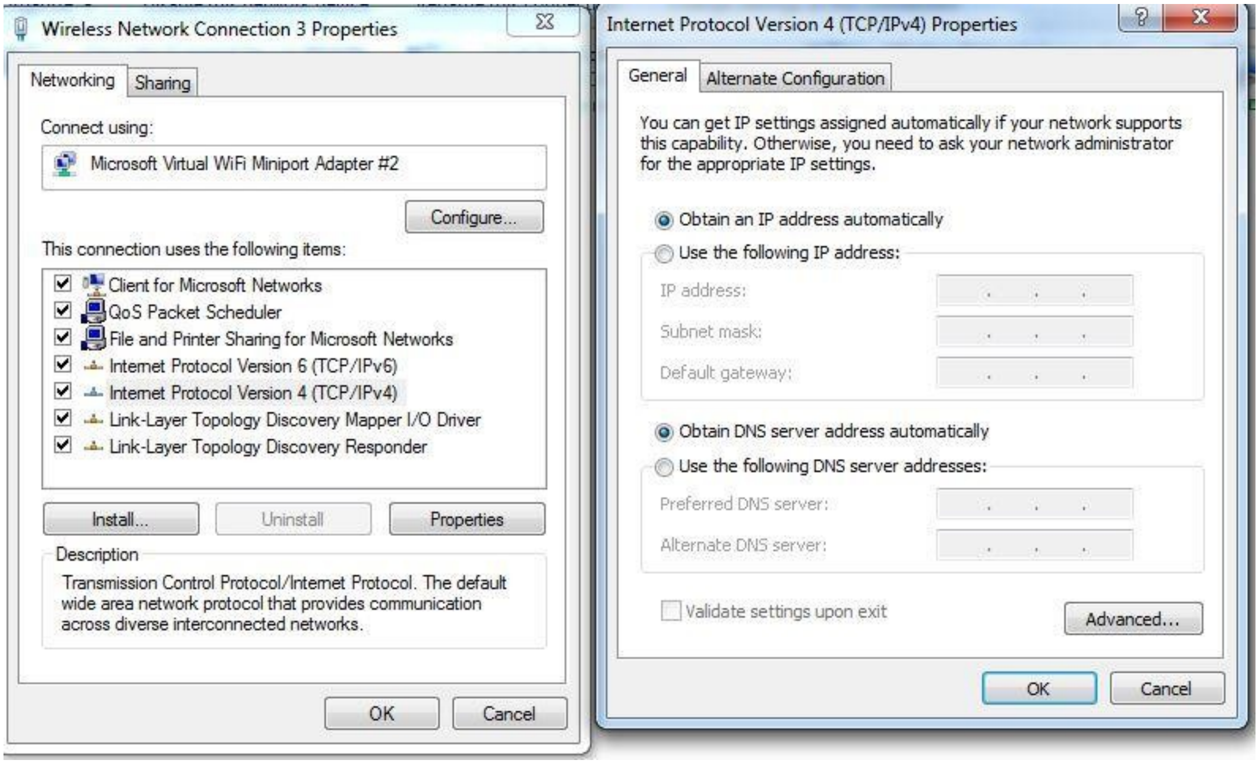
Follow the below process to set your PC to get an IP address automatically:

Step 1 : Click the “Start” button

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

Step 3 : Right click the “network connection” that your PC uses, select “attribute” and you can see the interface as shown in Figure 3.

Step 4.: Select “Internet Protocol (TCP/IP)”, click “attribute” button, then click the “Get IP address automatically”.



Wireless Network Connection 3 Properties

Connect using:

Microsoft Virtual WiFi Miniport Adapter #2

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Cannot connect to the Web

Solution:

- Check if the Ethernet cable is properly connected
- Check if the URL is correct. The format of URL is: http:// the IP address
- Check on any other browser apart from Internet explorer such as Chrome.
- Contact your administrator, supplier or ITSP for more information or assistance.

Forgotten Password

If you have forgotten the management password, you cannot access the configuration web GUI. Solution:

To factory default: press and hold reset button for 10 seconds.

Appendix A

Auto-Provisioning Manual

AC1000 l AC1000MS l AC1300MS

Table of Contents

Auto-Provisioning of ReadyNet Router ATAs

Introduction

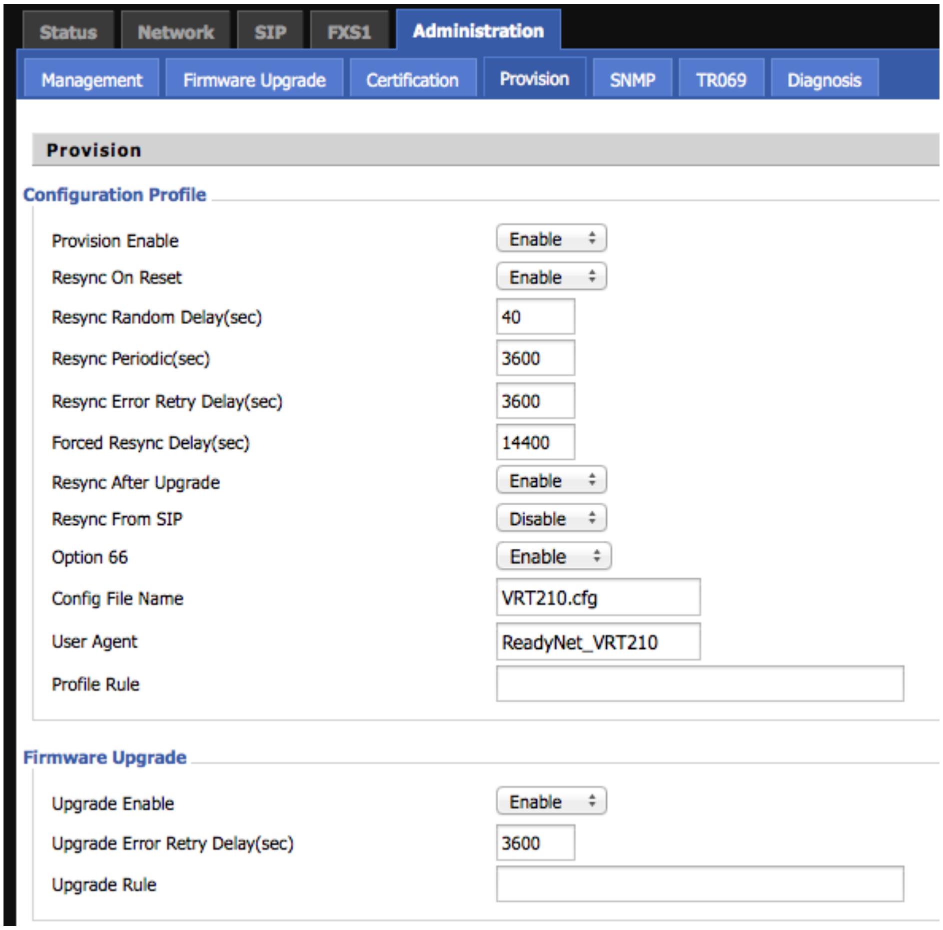
This document is targeted to developers and system integrators who intend to include support for the ReadyNet ATAs in their VoIP provisioning systems. It provides details for auto-provisioning ReadyNet routers with one or more ATA ports. Auto-provisioning is supported via TFTP, HTTP and HTTPS as well as DHCP Option 66, allowing for true zero-touch remote provisioning.

Configure Provisioning Parameters

This section first describes how to enable provisioning via the web interface and then describes the various parameters that can be set to control provisioning.

Enable Provisioning

To enable provisioning, log into the ReadyNet router and navigate to Administration -> Provision. The image below shows the default values for the QX202.
With the default settings, provisioning is enabled but the parameter ‘Profile Rule’, which is the provisioning URL, is blank. Similarly, firmware upgrade is enabled but ‘Upgrade Rule’ has no value.



Provision

Configuration Profile

Provision Enable	Enable
Resync On Reset	Enable
Resync Random Delay(sec)	40
Resync Periodic(sec)	3600
Resync Error Retry Delay(sec)	3600
Forced Resync Delay(sec)	14400
Resync After Upgrade	Enable
Resync From SIP	Disable
Option 66	Enable
Config File Name	VRT210.cfg
User Agent	ReadyNet_VRT210
Profile Rule	

Firmware Upgrade

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

The table below describes the various provisioning parameters and provides their default values.

Parameter Name	Description	Default Value
Provision Enable	Enable or disable the Provision functions.	Yes
Resync on Reset	Triggers a resync after every reboot except for reboot caused by parameter updates and firmware upgrades.	Yes
Resync Random Delay	The maximum value for a random time interval that the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. This parameter is in units of 1 second; the default value of 40 represents 40 seconds. This feature is disabled when this parameter is set to zero. It can be used to prevent an overload of the provisioning server when a large number of devices power on simultaneously.	40 seconds
Resync Periodic	The number of seconds between periodic resyncs with the provisioning server. Set this parameter to zero to disable periodic resyncing.	3600 seconds
Resync Error Retry Delay	If the last resync failed, the device will retry resync after the "Resync Error Retry Delay" seconds.	3600 seconds
Forced Resync Delay	Maximum delay in seconds the device waits before performing a resync. The device will not resync while any of its phone lines are active. Because a resync can take several seconds, wait until the device has been idle for an extended period before resyncing. This allows a user to make calls in succession without interruption. The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero.	14400 seconds
Resync After Upgrade	Triggers a resync after every firmware upgrade attempt.	Yes
Option 66	If enabled, the device will also request DHCP Option 66 with its DHCP request. When enabled, the parameter 'Profile Rule' is ignored.	Yes
Config File Name	This parameter is appended to the DHCP Option 66 value returned by the DHCP server to create the TFTP provisioning URL. e.g. if the DHCP Option 66 return value is 123.45.67.89 and the 'Config File Name' parameter is a.conf , then the device will request a provisioning file from the TFTP server located at123.45.67.89 for a file named, a.conf. This parameter is ignored when the parameter 'Option 66' is set to 'No'.	Changes for different models. For the QX202, it will be QX202.conf. For engineering samples, .cnf
Profile Rule	This parameter is a URI that evaluates to the provisioning resync command. The protocol can be TFTP and HTTP. The file name component of this parameter can make use of macros allowing the device to make requests for unique provisioning files. This parameter is ignored if the parameter 'Option 66' is enabled.	Empty

The table below describes the various firmware upgrade parameters and provides their default values.

Parameter	Description	Default Value
Enable Upgrading	Enables firmware upgrade operations independently of resync actions	Enable
Upgrade Error Retry Delay	The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero.	3600 seconds
Upgrade Rule	This parameter sets the URL for the new firmware file. It follows the same syntax as the 'Profile Rule' parameter. e.g. http://192.168.100.1/QX202_v3.1.bin	Empty

Syntax of Profile Rule and Upgrade Rule

The two parameters 'Profile Rule' and 'Upgrade Rule' must follow the following syntax.

[scheme://][server IP or domain[:port]]/file_path

The scheme can be one of the following;

http
https
tftp

The 'file_path' component follows macro expansion rules as described in the section 'Macro Expansion' below.

Examples:

tftp://prov.mydomain.com/cpe/$MAU.conf
http://dev.easyvoip.com:8080/prov/$PN/$MA.conf

Macro Expansion

Macro expansion can be used with the parameters ‘Profile Rule’ and ‘Upgrade Rule’. The table below list the macros variables and to what they expand.

Macro Name	Expansion
$	The form $$ expands to a single $ character. The form $$MAU expands to $00019F16B1B2. The form $MAU expands to 00019F16B1B2.
MA	MAC address with lower case hex digits, e.g. 00019F16b1b2.
MAU	MAC address with upper case hex digits, e.g. 00019F16B1B2.
MAC	MAC address with lower case hex digits, and colons to separate hex digit pairs, e.g. 00:01:9F:16:B1:B2.
PN	Product Name, e.g. QX202
SN	Serial Number, e.g. QX2123456
IP	WAN IP address , e.g. 123.45.67.89
SWVER	Software version, e.g. v3.0.1
HWVER	Hardware version, e.g. v1.0.1

Macro variables are invoked by prefixing the macro name with the ‘$’ character (e.g. $MAC). Macro substitution works even within a quoted sting, without requiring additional escapes. If the macro is immediately followed by an alphanumeric character, enclose the variable name in parentheses (e.g.‘$(MAC)config.conf’).

Please note the following additional points with regards to macro expansion;

1) During macro expansion, expressions of the form $NAME and $(NAME) are replaced by the contents of the named variables. For example, a router with a MAC address of 00:01:9F:16:B1:B2, the macro $(MAU)config.cfg expands to 00019F16B1B2config.cfg.
2) If the macro name is not recognized, it will remain unexpanded. For example, if you try to use STRANGE as a macro name it will remain unexpanded. Thus the expression $STRANGE$MAC.cfg expands to $STRANGE00:01:9F:16:B1:B2.cfg.
3) Macro expansion is not applied recursively. This means that the macro expression $$MAU expands to $MAU and not 00019F16B1B2.
4) Macro expressions can have optional qualifiers that allow you specify a substring of the macro variable. The syntax for macro substring expansion is $(NAME:p) and $(NAME:p:q) where p and q are non-negative integers. The resulting expansion results in the macro variable substring starting at the character offset p, and of length q (or till end-of-string if q is not specified). So, for our example device with a MAC address of 00019F16B1B2, the expression $(MAU:4) expands to the string 9F13B1B2, and the expression $(MAU:8:2) expands to the string B1.

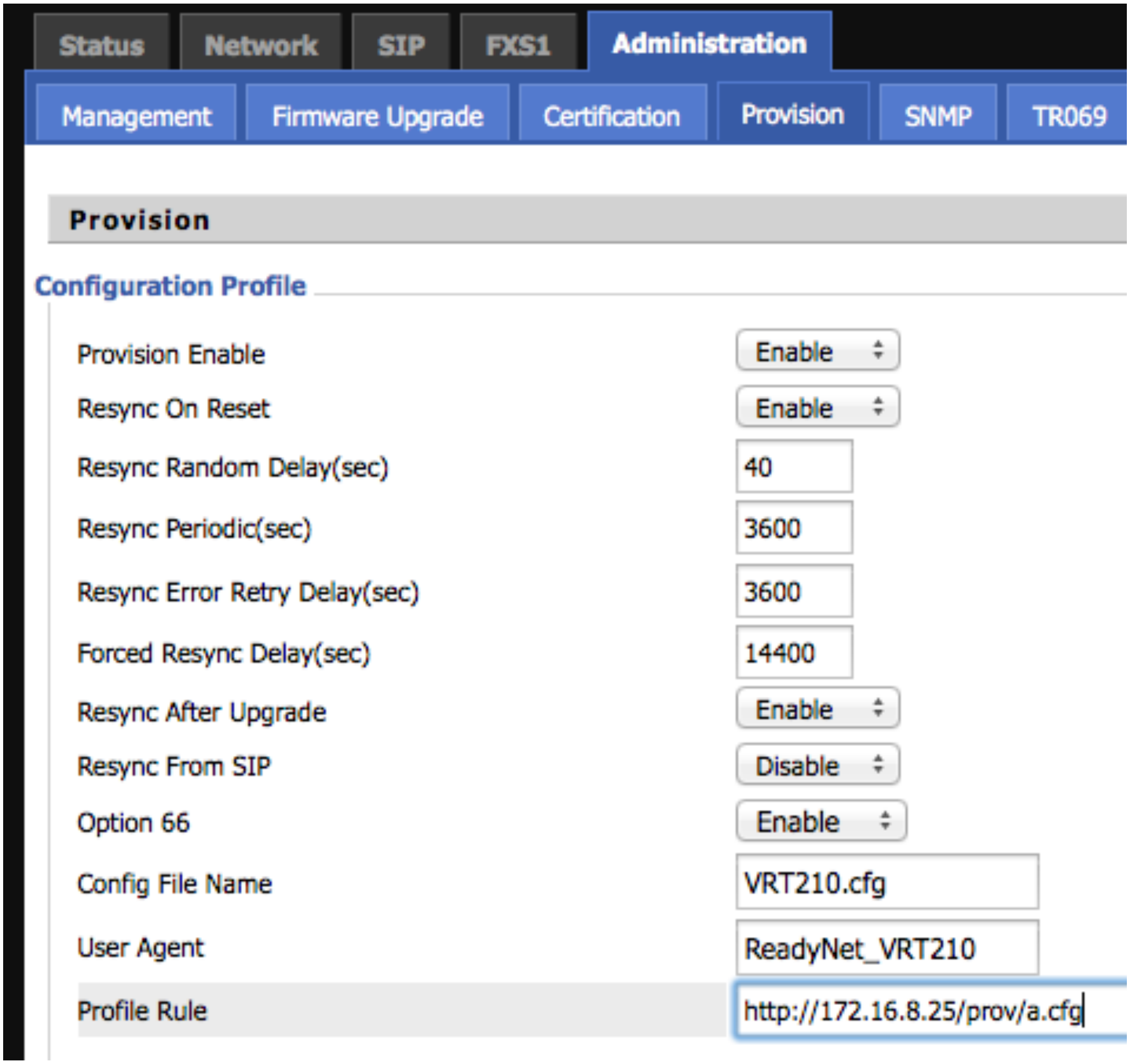
Provisioning

Provision with HTTP

Begin by resetting a ReadyNet router to factory defaults.
1) Install an HTTP server on the WAN side of the router.
2) In the DocumentRoot of the HTTP server, create a directory named ‘prov’ for provisioning files. So if the path to the DocumentRoot is /var/www/html, the path to the directory for the provisioning files will be /var/www/html/prov .
In the prov directory, create a file named a.cfg with the following contents and save it.

```
DBID_SUPER_WEB_PASSWORD=newpass1
```

3) From a PC connected to a LAN port of the device, you should be able to view the file contents of a.cfg by browsing to; http://HTTP_SERVER/prov/a.cfg.

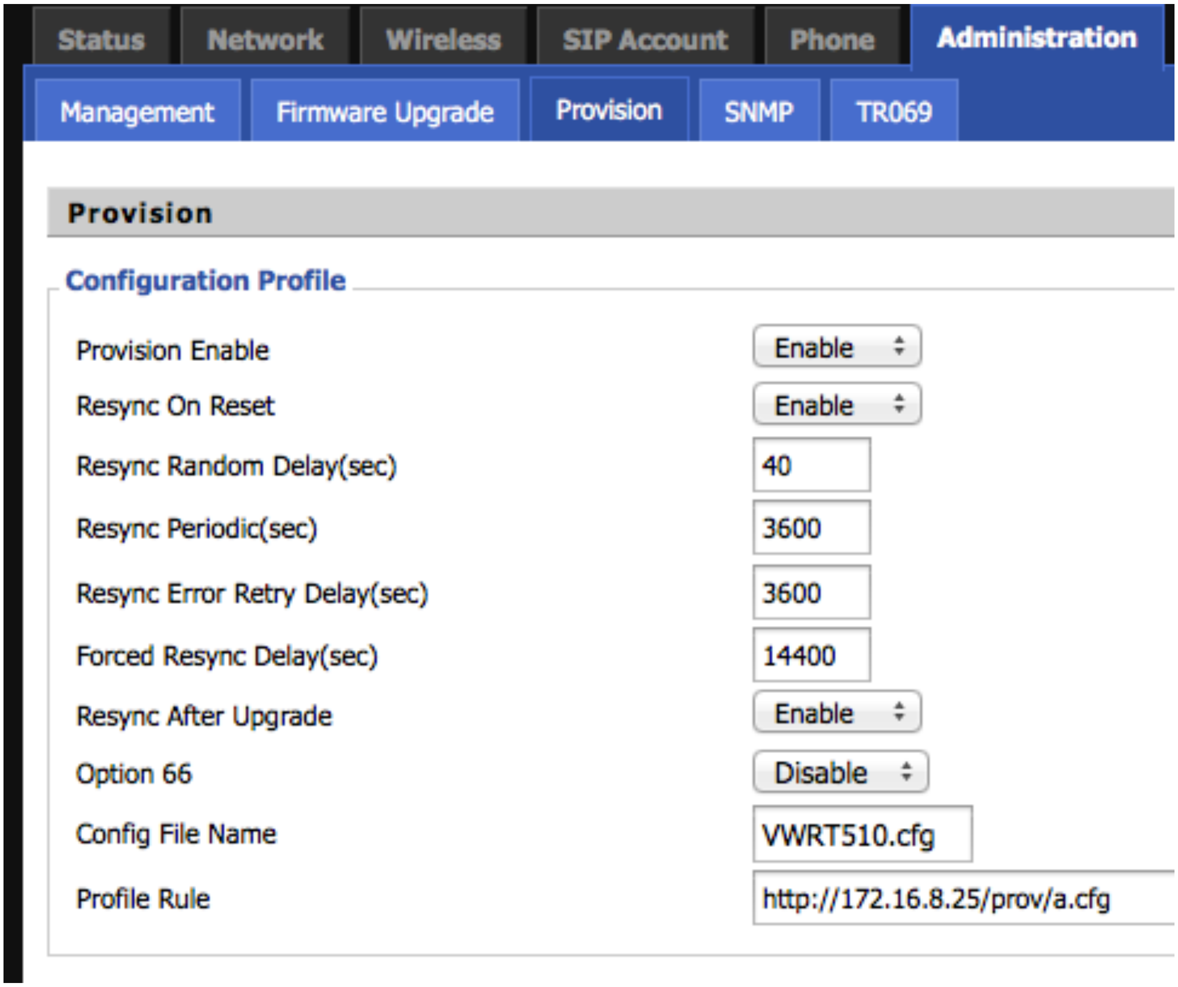


Provision

Configuration Profile

Provision Enable	Enable
Resync On Reset	Enable
Resync Random Delay(sec)	40
Resync Periodic(sec)	3600
Resync Error Retry Delay(sec)	3600
Forced Resync Delay(sec)	14400
Resync After Upgrade	Enable
Resync From SIP	Disable
Option 66	Enable
Config File Name	VRT210.cfg
User Agent	ReadyNet_VRT210
Profile Rule	http://172.16.8.25/prov/a.cfg

4) Log into the ReadyNet router, navigate to Administration -> Provision and set the ‘Option 66’ field to Disable and in the Profile Rule field enter: http://HTTP_SERVER/prov/a.cfg .



Provision

Configuration Profile

Provision Enable	Enable
Resync On Reset	Enable
Resync Random Delay(sec)	40
Resync Periodic(sec)	3600
Resync Error Retry Delay(sec)	3600
Forced Resync Delay(sec)	14400
Resync After Upgrade	Enable
Option 66	Disable
Config File Name	VWRT510.cfg
Profile Rule	http://172.16.8.25/prov/a.cfg

5) Click save and then do a reboot.
6) When the device boots and its WAN interface is up, it will retrieve the file located at Profile Rule. The ATA will reboot to apply the new parameters.
7) When you now login to the web interface with the user ‘admin’ you will need to enter the password: newpass1.

Provision with DHCP and TFTP

In the example above, we had to manually configure the Profile Rule of the router by logging into the web interface of the device as the admin user and entering a valid location for the provisioning URI. Using DHCP Option 66 together with a TFTP server, the Profile Rule parameter can be automatically set. The ReadyNet router with its default, out-of-the-box configuration is set for 1) DHCP on the WAN interface and 2) Option 66 enabled. A correctly configured DHCP server will provide the IP address of a TFTP server when the router includes a request for Option 66 together with its DHCP request. e.g. if the DHCP server sends back ‘172.16.8.25’ as the Option 66 response and **DBID_PRV_CONFIGFILE** is ‘QX202.cfg’, the device will make a TFTP request to the server at IP address 172.16.8.25, for a file named ‘QX202.cfg’.

8) Configure DHCP server to include Option 66 response.
9) Configure TFTP server. Create the initial provisioning file named ‘.cfg’ with the following contents.

```
DBID_RESYNC_PERIODIC=60
DBID_PRV_OPTION66_ENABLED=0
DBID_PROFILE_RULE=http://172.16.8.25/prov/$MAU.conf
```

Note: We change DBID_RESYNC_PERIODIC to 60 seconds only during testing and development.

10) In the prov directory of the HTTP server create a file named 00019F16XXXX.conf, replacing XX:XX in the file name to match the WAN MAC address of the router.

```
DBID_SUPER_WEB_PASSWORD=newpass2
```

So if the WAN MAC address is 00:01:9F:16:00:01, the file would be named, '00019F160001.conf'.

11) Reset the router to factory defaults. On boot-up, we should expect the following events to occur;
    a. The ReadyNet router includes Option 66 in its DHCP request on the WAN port.
    b. The DHCP server includes the Option 66 response with the other DHCP parameters.
    c. The router makes a TFTP connection to the IP address that it received as the Option 66 value and requests a file named .cfg.
    d. On receiving the file named '.cfg', the device will set the Option 66 parameter to 'Disable' and set the Profile Rule to '`http://172.16.8.25/prov/$MAU.conf`' and do a reboot.
    e. This time when the devices boots up, it will not include Option 66 with its DHCP request. Once the WAN interface is up, the router will expand the macro $MAU to its WAN MAC address in uppercase. So if the WAN MAC address of the router is 00:01:9F:16:00:01, then the device will request a provisioning file from the URI; http://172.16.8.25/prov/00019F160001.conf.
    f. The request URI uniquely identifies the device allowing the provisioning server to customize the provisioning file returned. In this example we set the password for the user admin to 'newpass2'.
    g. The device will reboot again.
12) When you now log in to the web interface with the user 'admin', you will need to enter the password 'newpass2'.

Provisioning Examples

This section provides example provisioning files for the ReadyNet router. Refer to the Appendix for a listing of the provisioning parameters and their descriptions.
Note 1: The provisioning file only contains the parameters that need changing.
Note 2: The ATA calculates a checksum of the provisioning file. It compares this checksum with the checksum of each new provisioning file it receives. If the checksums are different, the ATA will apply the changes in the new provisioning file and reboot.

Provisioning WAN Parameters

In this example provisioning file, the WAN connection mode is changed from DHCP to STATIC. Further we change, `mdns_mode` from 0 (Auto) to 1 ('Manual') and define a primary and secondary DNS server that the router itself will use.

```
mwanConnectionMode=STATIC
mwan_ipaddr=172.16.8.60
mwan_netmask=255.255.255.0
mwan_gateway=172.16.8.1
mdns_mode=1
```

```
mwan_primary_dns=8.8.8.8
```

Provisioning LAN Parameters

This remote provisioning example file changes the network parameters on the LAN side of the router. In addition, this file changes the username and passwords of the two administrative access levels of the web interface of the router.

```
lan_ipaddr=192.168.88.1
lan_netmask=255.255.255.0
dhcpGateway=192.168.88.1
dhcpStart=192.168.88.200
dhcpEnd=192.168.88.220
dhcpLease=3600
NormalUser=Alice
DBID_NORMAL_WEB_PASSWORD=Alice123Pass
AdminUser=Jack
DBID_SUPER_WEB_PASSWORD=Jack123pass
```

Provisioning SIP Parameters

This example provisioning file configures the SIP port of the router. You will need to change the actual parameters in the file to match your SIP server.

```
DBID_DNSSRV_DOMAIN=12.34.56.78
DBID_SIP_SERVER_HOST_NAME=12.34.56.79
DBID_SIP_DIS_NAME=Customer Name
DBID_SIP_PHONE_NUM=1234
DBID_SIP_ACCOUNT=1234
DBID_SIP_PASSWORD=SIPpass
```

Appendix B

WAN *Network Parameters*

Parameter	Valid Values	Description
mwanConnectionMode	**DHCP** STATIC PPPOE	This parameter defines the WAN connection method. It can be one of the following; Static, DHCP or PPPOE.
mdns_mode	**0** 1	With the default setting of 0, the device will use the DNS server provided by the DHCP server. Setting this parameter to 1 allows you to define m**wan_primary_dns** and m**wan_secondary_dns** manually.
mwan_primary_dns	*IP Address*	When mdns_mode is set to 1 or m**wanConnectionMode** is set to Static, this parameter can be defined to set the primary DNS server used by the router.
mwan_secondary_dns	*IP Address*	When mdns_mode is set to 1 or **mwanConnectionMode** is set to Static, this parameter can be defined to set the secondary DNS server used by the router.
mwan_ipaddr	*IP Address*	This parameter sets the WAN IP address and must be set when **mwanConnectionMode** is set to Static.
mwan_netmask	*Netmask*	This parameter sets the WAN Netmask and must be set when **mwanConnectionMode** is set to Static.
mwan_gateway	*IP Address*	This parameter sets the WAN Netmask and must be set when **mwanConnectionMode** is set to Static.
mwan_pppoe_user	Empty	This parameter is the PPPoE username and must be defined when **mwanConnectionMode** is set to PPPoE.
mwan_pppoe_pass	Empty	This parameter is the PPPoE password and must be defined when **mwanConnectionMode** is set to PPPoE.
mwan_pppoe_opmode	**KeepAlive** On Demand Manual	This parameter is the PPPoE Operation mode and defaults to KeepAlive.
mwan_pppoe_optime	**60**	This parameter defines the PPPoE Keep Alive Redial period in seconds when PPPoE is the **wanConnectionMode**. Range is between 0 - 3600.

LAN Network Parameters

Parameter	Valid Values	Description
natEnabled	**NAT** Bridge	When in natEnabled is set to NAT, the router operates as a router and when set to Bridge, all network interfaces are bridged.
lan_ipaddr	IP Address	This parameter sets the IP address of the LAN interface when **natEnabled** is set to NAT. This IP address is also the gateway address for the devices connected to the LAN side of the router.
lan_netmask	*Subnet Mask*	This parameter sets the subnet mask of the LAN subnet when **natEnabled** is set to NAT.
dhcpEnabled	**Enable** Disable	Use this parameter to enable or disable running a DHCP server on the router.
dhcpStart	*IP Address*	If **dhcpEnabled** is set to Enable, this parameter sets the starting IP address of the DHCP pool.
dhcpGateway	*IP Address*	**dhcpGateway** defines the gateway address for DHCP requests from the LAN network.
dhcpEnd	*IP Address*	If **dhcpEnabled** is set to Enable, this parameter sets the ending IP address of the DHCP pool.
dhcpDnsMode	**Auto** Manual	When this parameter is set to Auto, DHCP clients are assigned the
dhcpPriDns		When **dhcpDnsMode** is set to Manual, this parameter defines the IP address of DNS server that will be provided as the primary DNS server with DHCP requests.
dhcpSecDns		When **dhcpDnsMode** is set to Manual, this parameter defines the IP address of DNS server that will be provided as the secondary DNS server with DHCP requests.
dhcpLease	**86400**	This parameter defines the DHCP lease time.
lan_vid	1	This parameter defines the VLAN ID of the LAN port. VLAN IDs are defined under Network -> VLAN in the web interface.

SIP Parameters

These parameters configure the SIP settings and correspond to the settings seen on the ‘SIP Account’ menu of the web interface.

Parameter	Description
DBID_DNSSRV_DOMAIN	This parameter defines the ‘Proxy Server’ for the SIP account.
DBID_SIP_OUTBOUND_PORT	This parameter defines the ‘Proxy Port’. The default port is 5060.
DBID_SIP_SERVER_HOST_NAME	This parameter defines the ‘Outbound Server’ for the SIP account.
DBID_SIP_SERVER_PORT	This parameter defines the ‘Outbound Port’. Default value is 5060.
DBID_ALTER_SIP_SERVER_HOSTNAME	This parameter defines the ‘Backup Outbound Server’ for the SIP account.
DBID_ALTER_SIP_SERVER_PORT	This parameter defines the ‘Backup Outbound Port’. The default port is 5060.
DBID_SIP_DIS_NAME	This parameter defines the ‘Display name’ for the SIP account.
DBID_SIP_PHONE_NUM	This parameter defines the ‘Phone Number’ for the SIP account.
DBID_SIP_ACCOUNT	This parameter defines the ‘Account’ attribute associated with the SIP account.
DBID_SIP_PASSWORD	This parameter defines the ‘Password’ assigned to the particular SIP account.
DBID_SIP_TOS	This parameter sets the DHCP mark for Layer 3 QoS for SIP packets. Range is 0 through 63.
DBID_RTP_TOS	This parameter sets the DHCP mark for Layer 3 QoS for RTP packets. Range is 0 through 63.
DBID_DATA_TOS	This parameter sets the DHCP mark for Layer 3 QoS for Data packets. Range is 0 through 63.
sip_vid	This parameter defines the VLAN ID over which SIP packets will be sent. VLAN IDs are defined under Network -> VLAN in the web interface. The default is 2.
rtp_vid	This parameter defines the VLAN ID over which RTP packets will be sent. VLAN IDs are defined under Network -> VLAN in the web interface. The default is 2.

Administration Parameters

Parameter		Description
BasicUser	**useradmin**	This parameter defines a web login username of type 'Basic'.
BasicPass	**admin**	This parameter defines the password for **BasicUser**.
NormalUser	**user**	This parameter defines a web login username of type 'Normal'.
DBID_NORMAL_WEB_PASSWORD	**user**	This parameter defines the password for NormalUser.
AdminUser	**admin**	This parameter defines a web login username of type 'Admin'.
DBID_SUPER_WEB_PASSWORD	**admin**	This parameter defines the password for AdminUser.
DBID_LAN_LOGIN_ONLY	**0**	The default for this parameter is 0 which allows access to the web interface of the device from the WAN interface. To only allow access to the web interface set this parameter to 1.
DBID_WEB_PORT	**80**	This parameter set the port that web server on the device listens to requests on both the LAN side and WAN (if DBI_LAN_LOGIN_ONLY =0) side.
DBID_WEB_IDLE_TIMEOUT	**5**	Whilst logged into the web interface of the device this parameter sets the value in minutes of inactivity that results in getting logged out.

Provisioning Parameters

Parameter	Default	Description
DBID_PROVISION_ENABLED	**1** 0	The default value for this parameter is 1 which enables provisioning for the device.
DBID_RESYNC_ON_RESET	**1** 0	The default value for this parameter is 1 which triggers a resync after every reboot except for reboot caused by parameter updates and firmware upgrade.
DBID_RANDOM_DELAY	**40**	This parameter defines the maximum number of seconds the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. The default value is 40 and setting this parameter to 0, disables this feature.
DBID_RESYNC_PERIODIC	**3600**	This parameter is used to define the number of seconds between periodic resyncs with the provisioning server. Set this parameter to zero to disable periodic resyncing.
DBID_RESYNC_RETRY_DELAY	**3600**	This parameter defines the number of seconds the device will wait to retry a resync after the last attempt to resync failed.
DBID_RESYNC_DELAY	**14400**	This is the starting value of a counter in seconds that is decremented when all its line become idle. Resync events are delayed until this counter decrements to zero.
DBID_RESYNC_AFTER_UPGRADE	**1** 0	When set to 1, the device will trigger a resync after every firmware upgrade attempt. Set this parameter to disable.
DBID_PRV_OPTION66_ENABLED	**1** 0	When this parameter is set to 1 (default), the device will include DHCP Option 66 with its DHCP request. When enabled, the parameter DBID_PROFILE_RULE is ignored.
DBID_PRV_CONFIGFILE	**.cfg**	This is the name of the provisioning file retrieved from the TFTP server when DHCP Option 66 is enabled.
DBID_PROFILE_RULE		This parameter sets the URI that the device will reterive its provisioning file from. This parameter is ignored when DBID_PRV_OPTION66_ENABLED is set to 0.
DBID_UPGRADE_ENABLED	**1** 0	The default value for this parameter is 1, which enables firmware upgrades. Set to 0 to disable this function.
DBID_UPGRADE_RETRY_DELAY	**3600**	On a firmware upgarde failure this parameter is set to the value defined in seconds and a countdown begins. Once the timer reaches zero, the next attempt at firmware upgrade will occur.
DBID_UPGRADE_RULE		This parameter sets the URI from which the new firmware file is requested from.

Default Provisioning Template File

```
mwanConnectionMode=DHCP
dhcpDnsMode=Auto
mwan_primary_dns=
mwan_secondary_dns=
mwan_ipaddr=
mwan_netmask=
wan_gateway=
wan_pppoe_user=
wan_pppoe_pass=
wan_pppoe_opmode=KeepAlive
wan_pppoeoptime=5
wan_vid=2
natEnabled=1
lan_ipaddr=192.168.11.1
lan_netmask=255.255.255.0
dhcpEnabled=1
dhcpStart=192.168.11.2
dhcpEnd=192.168.11.24
dhcpGateway=192.168.11.1
dhcpDnsMode=Auto
dhcpPriDns=192.168.11.1
dhcpSecDns=8.8.8.8
dhcpLease=86400
lan_vid=1
DBID_DNSSRV_DOMAIN=
DBID_SIP_OUTBOUND_PORT=5060
DBID_SIP_SERVER_HOST_NAME=
DBID_SIP_SERVER_PORT=5060
DBID_ALTER_SIP_SERVER_HOSTNAME=
DBID_ALTER_SIP_SERVER_PORT=5060
DBID_SIP_DIS_NAME=
DBID_SIP_PHONE_NUM=
DBID_SIP_ACCOUNT=
DBID_SIP_PASSWORD=
DBID_SIP_TOS=0
DBID_RTP_TOS=0
DBID_DATA_TOS=0
sip_vid=2
rtp_vid=2
DBID_PROVISION_ENABLED=1
DBID_RESYNC_ON_RESET=1
DBID_RANDOM_DELAY=40
```

```
DBID_RESYNC_PERIODIC=3600
DBID_RESYNC_RETRY_DELAY=3600
DBID_RESYNC_DELAY=14400
DBID_RESYNC_AFTER_UPGRADE=1
DBID_PRV_OPTION66_ENABLED=1
DBID_PRV_CONFIGFILE=QX202.cfg
DBID_PROFILE_RULE=
DBID_UPGRADE_ENABLED=0
DBID_UPGRADE_RETRY_DELAY=3600
DBID_UPGRADE_RULE=
```