FLYINGVOICE
VoIP & VoWLAN Solutions

User Manual

FWR7302/FWR8302/FWR9302

Contents

About This User Guide **1**
Contacting FlyingVoice 2
Purpose 3
Cross references 3
Feedback 3
Declaration of Conformity 4
Part 15 FCC Rules 4
Warnings and Notes 5
Warnings 5
Notes 5
Chapter 1: Product description **6**
FWR7302/FWR8302/FWR9302 7
LED Indicators and Interfaces 8
Voice Prompt 15
Chapter 2:Configuring Basic Settings **20**
Two-Level Management 21
Web Management Interface 21
Web Management Interface Details 23
Setting the Time Zone 24
Configuring an Internet Connection 25
Setting up Wireless Connections 27
Configuring Session Initiation Protocol (SIP) 30
Making a Call 32
Chapter 3: Web Interface **34**
Login 35
Status 36
Network and Security 40
WAN 40
LAN 46
Wireless 2.4G 57
Wireless 5G 70
SIP 71
FXS1 79

FXS2 89
Security 90
Application 93
Storage 95
Administration 98
Management 98
Firmware Upgrade 103
LTE Upgrade 104
Provision 105
SNMP 108
TR-069 109
Diagnosis 111
Operating Mode 113
System Log 114
Logout 114
Reboot 114
Chapter 4:IPv6 address configuration 115
Introduction 116
IPv6 Advance 117
Configuring IPv6 117
Viewing WAN port status 120
IPv6 DHCP configuration for LAN/WLAN clients 120
LAN DHCPv6 121
Chapter 5: Troubleshooting Guide 122
Configuring PC to get IP Address automatically 123
Cannot connect to the Web 124
Forgotten Password 124

Tables

Table 1 Features at-a-glance..... 7
Table 2 LED Indicators..... 8
Table 3 Interfaces..... 11
Table 4 Voice Menu Setting Options.....15
Table 5 Web management interface.....23
Table 6 Setting time zone.....24
Table 7 Configuring an internet connection..... 25
Table 9 Wireless Security web page.....29
Table 10 Configuring SIP the Web Management Interface..... 30
Table 11 Registration status.....31
Table 12 Login details..... 35
Table 13 Status Page.....36
Table 14 Internet..... 40
Table 15 DHCP..... 41
Table 16 PPPoE..... 42
Table 17 Bridge Mode..... 44
Table 18 LAN port.....46
Table 19 DHCP server settings..... 48
Table 20 DHCP server, DNS and Client Lease Time.....48
Table 21 LTE.....49
Table 22 VPN.....50
Table 22 Port Forward.....51
Table 23 VLAN.....52
Table 24 DMZ.....53
Table 25 DDNS..... 53
Table 26 QoS.....54
Table 27 Port setting..... 55
Table 28 Routing.....55
Table 29 Advance..... 56
Table 30 Basic..... 57
Table 31 Wireless security.....60
Table 32 WiFI Security Setting.....61
Table 33 WPA-PSK..... 62
Table 34 WPAPSKWPA2PSK..... 62
Table 35 Wireless Access Policy..... 63

Table 36 WMM.....64
Table 37 WDS.....65
Table 38 WPS.....66
Table 39 Station info.....67
Table 40 Advanced.....68
Table 41 SIP settings.....71
Table 42 VoIP QoS.....72
Table 43 Parameters and settings.....73
Table 44 Adding one dial plan.....74
Table 45 Dial Plan.....75
Table 46 Blacklist.....76
Table 47 Call log.....77
Table 48 SIP Account - Basic.....79
Table 49 Audio configuration.....80
Table 50 Supplementary service.....81
Table 51 Advanced.....82
Table 52 Volume settings.....84
Table 53 Regional.....85
Table 54 Features and call forward.....86
Table 55 Miscellaneous.....88
Table 56 Filtering setting.....90
Table 57 Content filtering.....91
Table 58 advance NAT.....93
Table 59 UPnP.....93
Table 60 IGMP.....94
Table 61 Disk Management.....95
Table 62 FTP Setting.....96
Table 63 Smb setting.....97
Table 64 Save Config File.....98
Table 65 Administrator settings.....99
Table 66 NTP settings.....100
Table 67 Daylight Saving Time.....101
Table 68 System log Setting.....102
Table 69 Factory Defaults Setting.....102
Table 70 Factory Defaults.....103
Table 71 Firmware upgrade.....103
Table 72 LTE upgrade.....104
Table 73 Scheduled Tasks.....104
Table 74 Provision.....106
Table 75 Firmware Upgrade.....107
Table 76 SNMP.....108

Table 77 TR069 109
Table 78 Diagnosis..... 111
Table 79 Operating mode..... 113
Table 80 System log..... 114
Table 81 Logout..... 114
Table 82 IPv6 Modes..... 116
Table 83 Enabling IPv6..... 117
Table 84 Configuring Statefull IPv6..... 118
Table 85 Configuring Stateless IPv6..... 119

About This User Guide

Thank you for choosing device wireless router with VoIP. This product will allow you to make ATA call using your broadband connection, and provides Wi-Fi router function.This manual provides basic information on how to install and connect FWR7302/FWR8302/FWR9302 wireless router with VoIP to the Internet. It also includes features and functions of wireless router with VoIP components, and how to use it correctly.Before you can connect FWR7302/FWR8302/FWR9302 to the Internet and use it, you must have a high-speed broadband connection installed. A high-speed connection includes environments such as DSL, cable modem, and a leased line.FWR7302/FWR8302/FWR9302 wireless router with VoIP is a stand-alone device, which requires no PC to make Internet calls. This product guarantees clear and reliable voice quality on Internet, which is fully compatible with SIP industry standard and able to interoperate with many other SIP devices and software on the market.

This guide contains the following chapters:

- Chapter 1: Product description
- Chapter 2: Configuring Basic Settings
- Chapter 3: Web Interface Management
- Chapter 4: Managing device
- Chapter 5: Troubleshooting Guide

Contacting FlyingVoice

Main website:	http://www.flyingvoice.com/
Sales enquiries:	sales1@flyingvoice.com
Support enquiries:	support@flyingvoice.com
Hotline:	010-67886296 0755-26099365
Address:	Room508-509, Bldg#1, Dianshi Business Park, No.49 BadachuRd,Shijingshan District, Beijing, China

Purpose

The documents are intended to instruct and assist personnel in the operation, installation and maintenance of the FlyingVoice equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.FlyingVoice disclaims all liability whatsoever, implied or express, 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 support@flyingvoice.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 FlyingVoice 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.

Chapter 1: Product Description

This chapter covers:

- FWR7302/FWR8302/FWR9302
- LED Indicators and Interfaces
- Hardware Installation
- Voice Prompt

FWR7302/FWR8302/FWR9302

Table 1 Features at-a-glance

Port/Model	FWR7302	FWR8302	FWR9302
picture			
WAN	1	1	1
LAN	4	4	4
FXS	2	2	2
USB	1	0	1
LTE	Yes	No	No
SPF	1	1	1
Speed limit NAT	Yes	Yes	yes
Ethernet interface	5* RJ45 10/100M/1000M	5* RJ45 10/100M/1000M	5* RJ45 10/100M/1000M
Fax	T.30, T.38 Fax		
WiFi	2.4G 2T2R (300Mbps) 5G 2T2R (867Mbps)	2.4G 2T2R(300Mbps)	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	Support		

LED Indicators and Interfaces

Table 2 LED Indicators

FWR9302

LED	Status	Explanation
Power	on Green	System is powereded on
	off	System is powered off
System	on Green	System run normally
	Blinking Green	System trouble
	off	System is powered off
SFP	on Green	SFP module is connected
	off	SFP module has no connection.
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	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 wifi 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 wifi 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

FWR8302

LED	Status	Explanation
Power	on Green	System is powereded on
	off	System is powered off
System	on Green	System run normally
	Blinking Green	System trouble
	off	System is powered off
SFP	on Green	SFP module is connected
	off	SFP module has no connection.
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	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 wifi 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

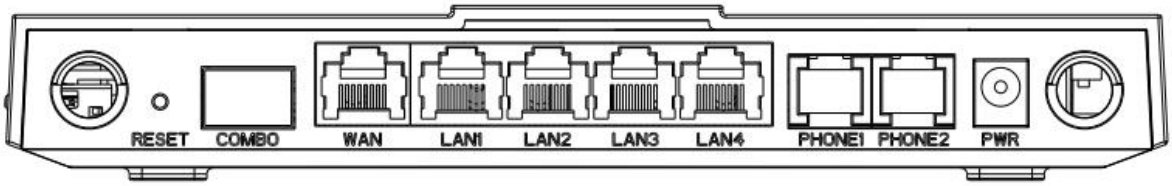
FWR7302

LED	Status	Explanation
Power	on Green	System is powereded on
	off	System is powered off

LTE	on Green	Successful registration of sim card, but no data transfer
	Blinking Green	There is data being transmitted or sim card is registering
	off	There is no sim card or sim card registered failed
SFP	on Green	SFP module is connected
	off	SFP module has no connection.
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 wifi 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 wifi 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

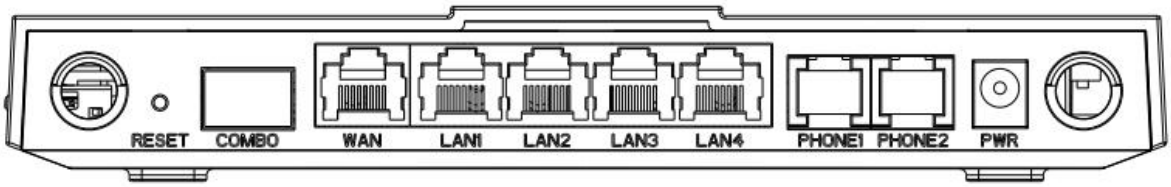
Table 3 Interfaces

FWR9302



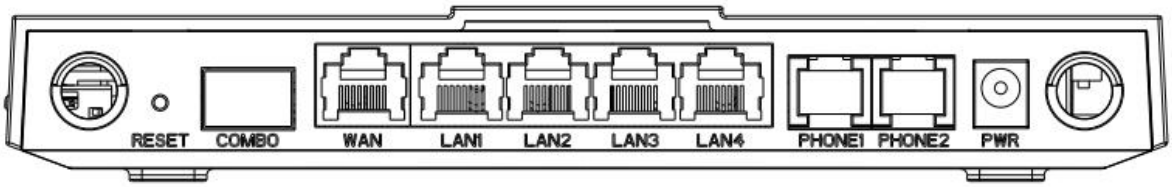
Interface	Description
POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices
COMBO	Connect the optical module
RESET	Restore the factory settings button, press and hold the device after 5s to restore the factory settings

FWR8302



Interface	Description
POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices
COMBO	Connect the optical module
RESET	Restore the factory settings button, press and hold the device after 5s to restore the factory settings

FWR7302



Interface	Description
POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices
COMBO	Connect the optical module
RESET	Restore the factory settings button, press and hold the device after 5s to restore the factory settings

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

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.

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 may be configured for operation. Each device configuration section may be accessed by entering a certain operation code, as shown below.

Table 4 Voice Menu Setting Options

Operation code	Menu Navigation
1(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
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	5. Pick up phone and press “****” to start IVR 6. Choose “6”, and the router reports “ WEB Access Port” 7. Prompt “Please enter password”, the method of inputting password is same as operation 1. 8. Report “operation successful” if user operation is ok. 9. 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 main menu.
2. If any changes 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 FWR8102 is connected.
7. The default LAN port IP address of router is 192.168.11.1 and this address should not be assigned to the WAN port IP address of router 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 Configuring 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.

FWR7302 supports two-level management:

(1) administrator and user. For 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

Logging in from the LAN port

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.

Open a web browser on your PC and type “http://192.168.11.1”. The following window appears that prompts for Username and Password.

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

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

Logging in from the WAN port

Ensure your PC is connected to the router's WAN port correctly.

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.

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.

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

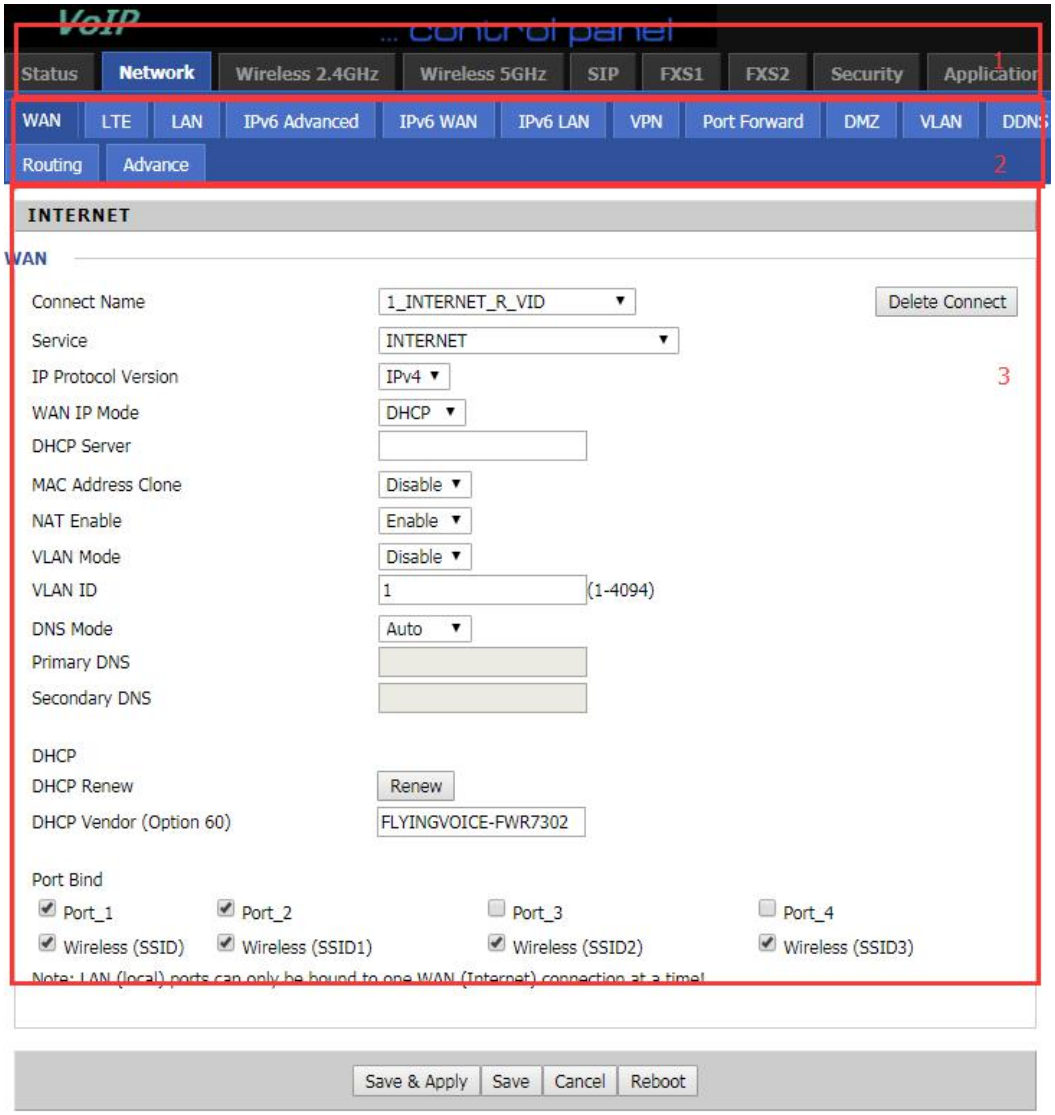
Note

If you fail to access to the web configuration, see Chapter 6: Troubleshooting Guide for more information.

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

Web Management Interface Details

Table 5 Web management interface

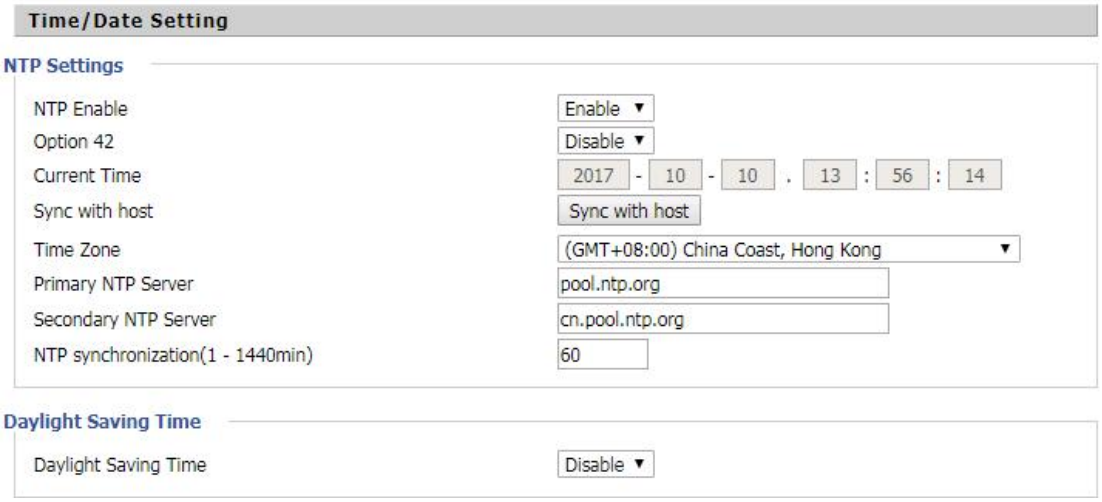


Field Name	Descripti
Top Navigation bar	Click an option in Top Navigation bar (area marked as “1”). Multiple options in the Sub-navigation bar are displayed
Sub-navigation bar	Click the Sub-navigation bar to choose a configuration page (area marked as “2”)
Parameter configuration	This area displays the current parameters for configuration (e.g. area marked as “3”)

Save & Apply	After changing the parameters need to click this button to save&apply, modify the parameters immediately take effect.
Save	Any time changes are made click "Save" to confirm and save the changes. On click of “Save” button, a red message will be displayed as shown below to notify a reboot.
Reboot	Reboot the device to ensure that the modification parameters take effect
Cancel	To cancel the changes.

Setting the Time Zone

Table 6 Setting time zone

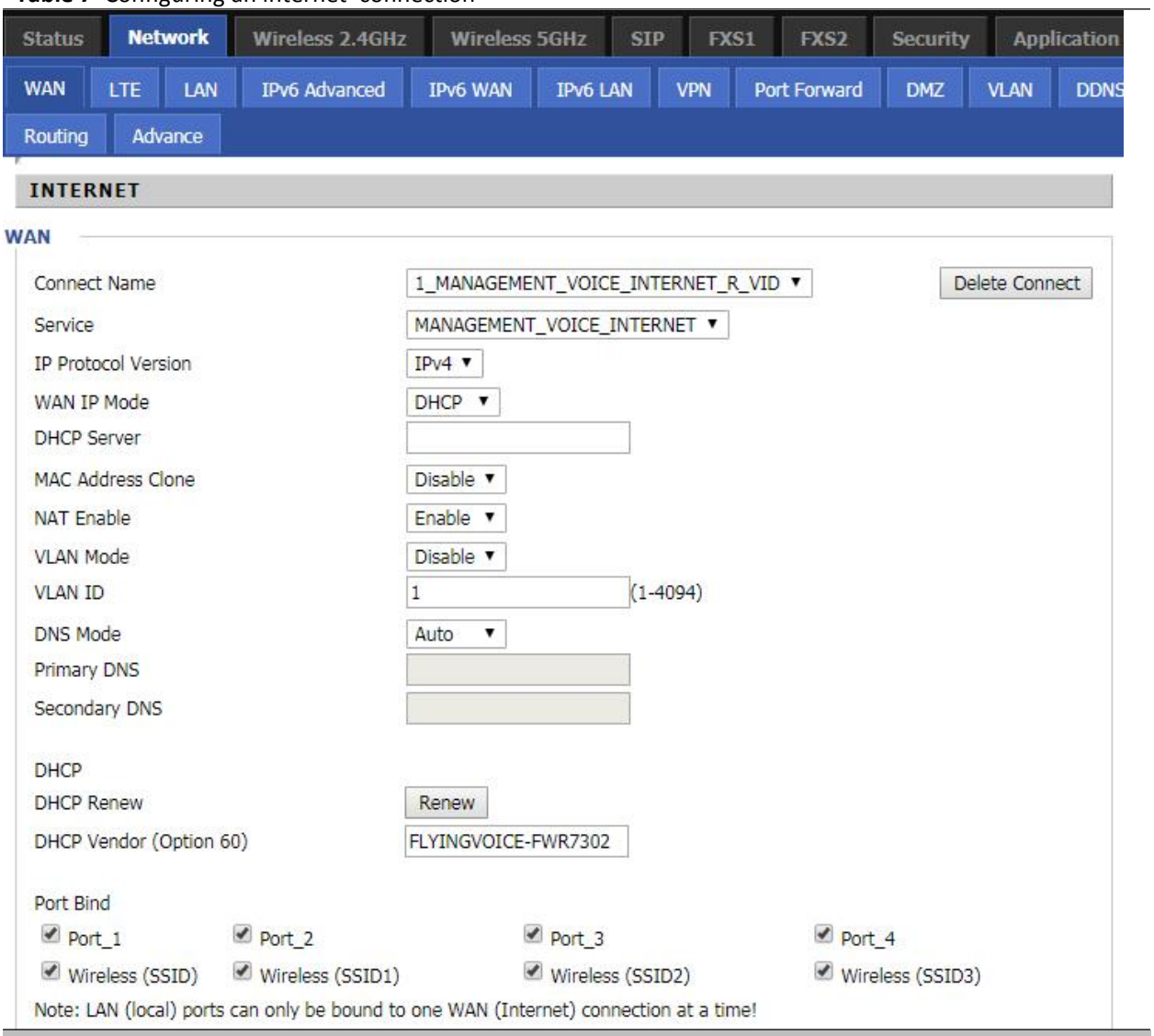


Field Name	Description
NTP Enable	Enable NTP (Network Time Protocol) to automatically retrieve time and date settings for the device
Current Time	When NTP Enable is set to “Disable”, manually configure the time and date via the Current Time parameter
Sync with host	Press Sync with host button to synchronize the host PC date, time and time zone
Primary NTP Server	Primary and secondary NTP server address for clock synchronization. A valid NTP server must be reachable for full NTP functionality
Secondary NTP Server	
NTP Synchronization (1- 1440m)	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 10below.

Table 7 Configuring an internet connection



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	**Note** 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 (Option60)	Specify the DHCP Vendor field Display the vendor and product name

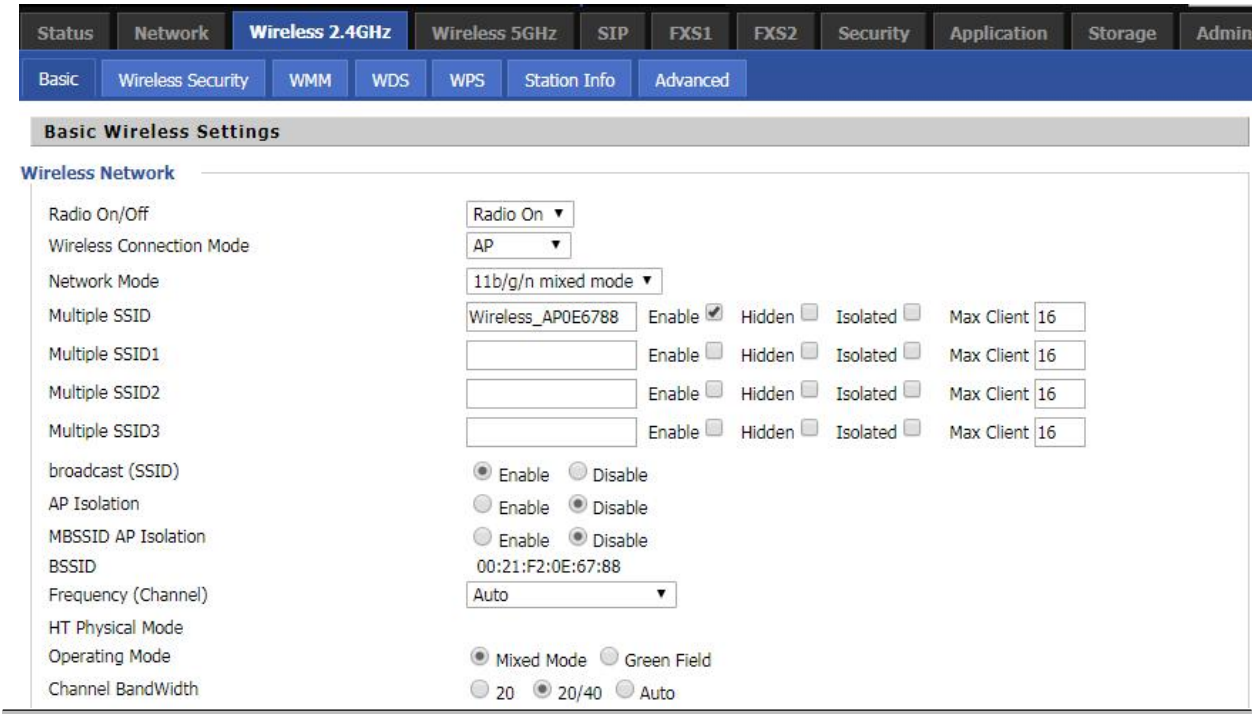
Setting up Wireless Connections

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

Enable Wireless and Setting SSID

Open Wireless > Basic webpage as shown below:

Table 8 Wireless > Basic web page (user view)



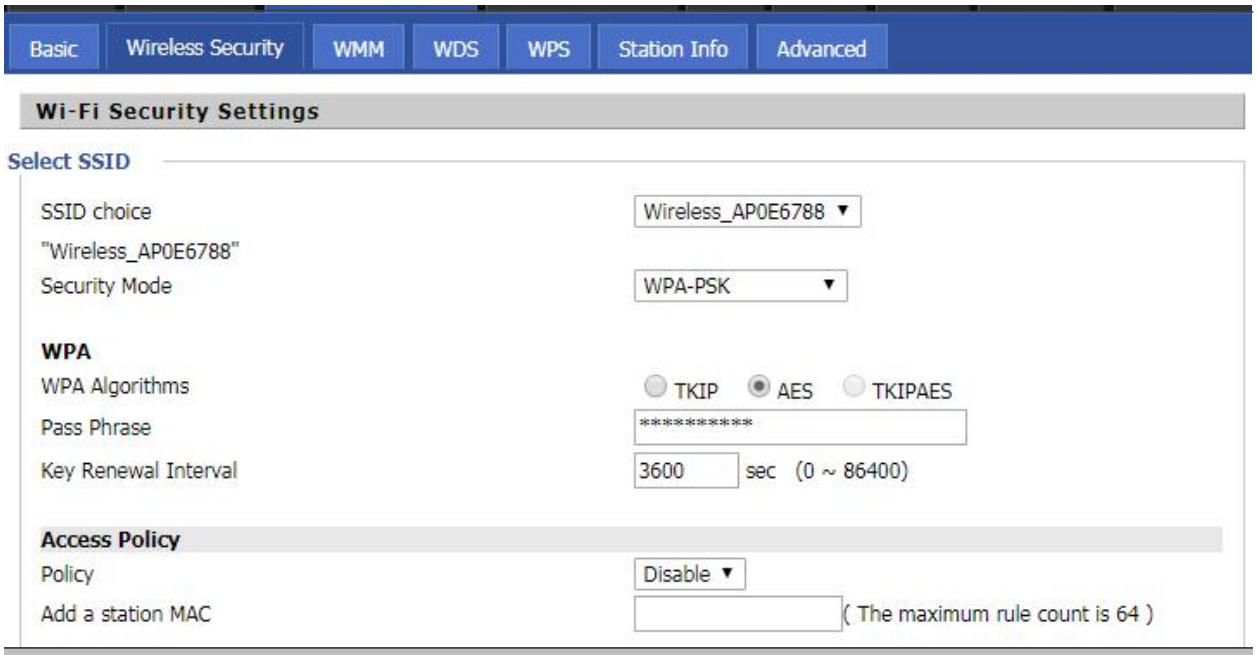
Field Name	Description
Radio On/Off	Select “Radio Off”to disable wireless operation Select “Radio on” to enable wireless operation Please note: “Save” required for this parameter change
Network Mode	Choose one network mode from the drop down list.
SSID	The logical name of the wireless connection (text, 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 regulatr intervals, disallowing wi-fi clients from automatically connecting to the FWR7302

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 the network to each other
BSSID	Basic Service Set Identifier – AP MAC Address Listing
Frquency (Channel)	Select the channel of operation for the device from the drop-down list
HT Physical Mode	
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 (802.11n only network)
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



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

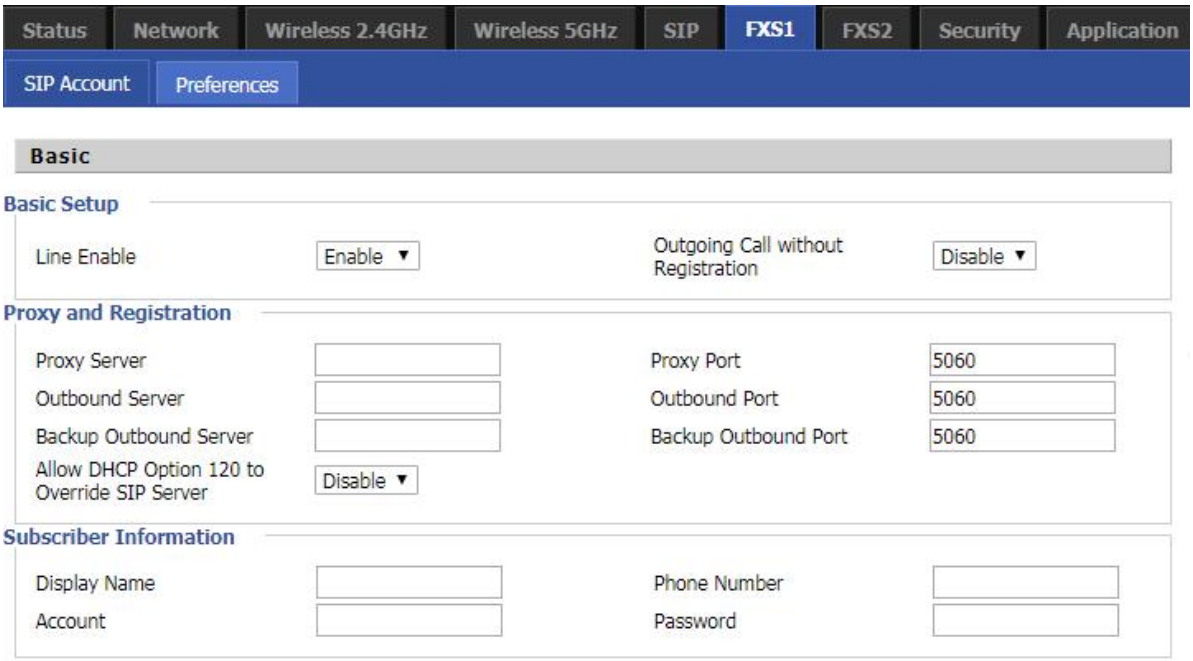
Configuring Session Initiation Protocol (SIP)

SIP Accounts

The device have 2 FXS ports 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 via the Web Management Interface

Table 10 Configuring SIP the Web Management Interface



Procedure

1. Open the FXS1/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

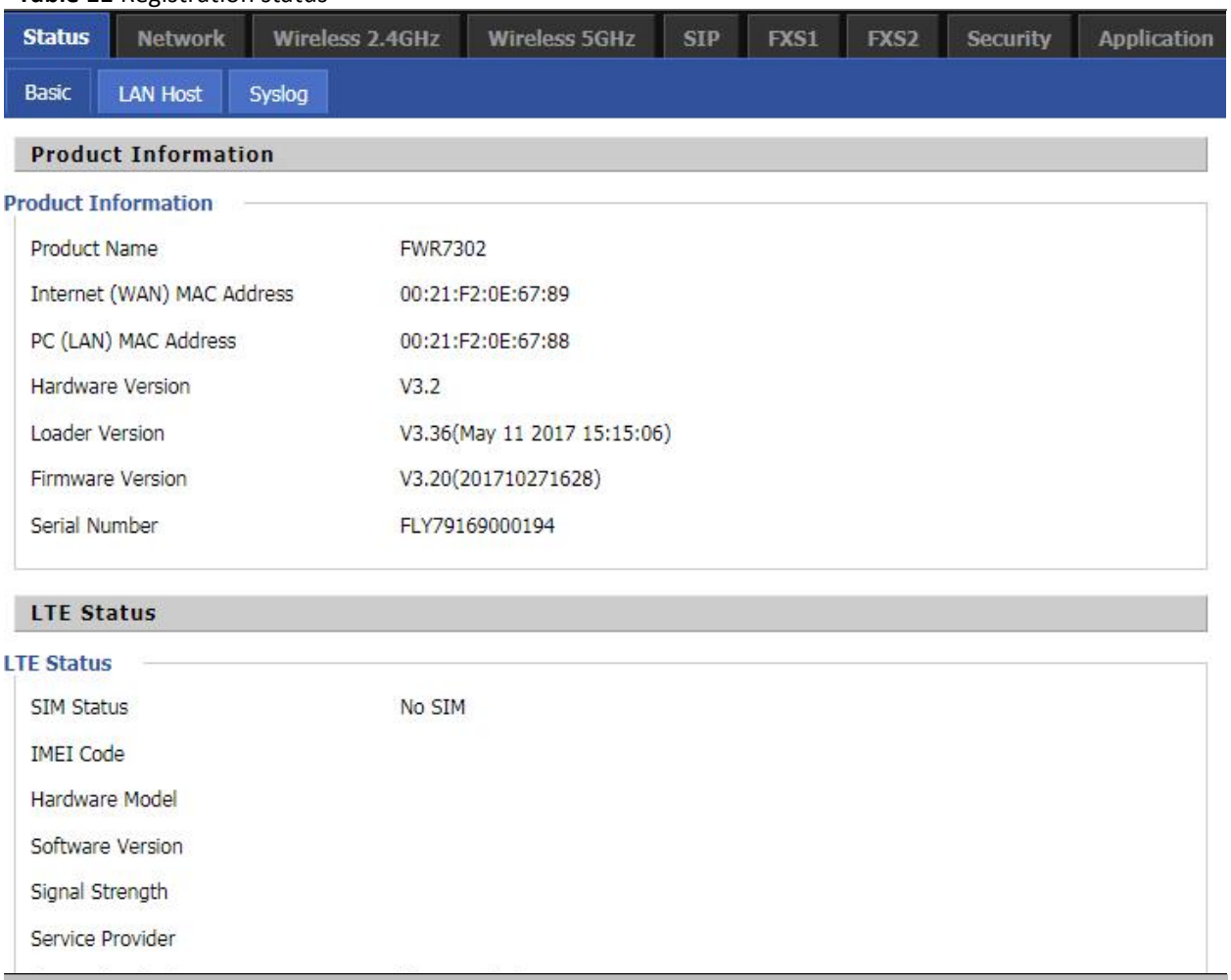
Upon the following dialogue:

Please REBOOT to make the changes effective!

Please press Reboot button to make changes effective.

Viewing the Registration Status

Table 11 Registration status



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.
- 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.

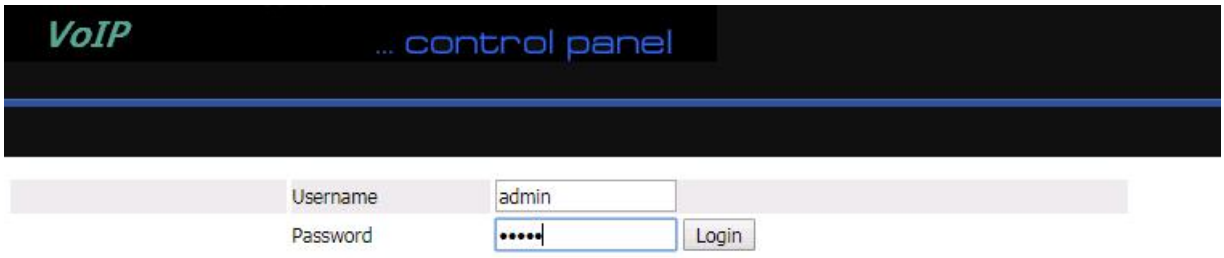
Chapter 3: Web Interface

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

- Login
- Status
- Network and Security
- Wireless
- SIP
- FXS1
- FXS2
- Security
- Application
- Administration
- Management
- System Log
- Logout
- Reboot

Login

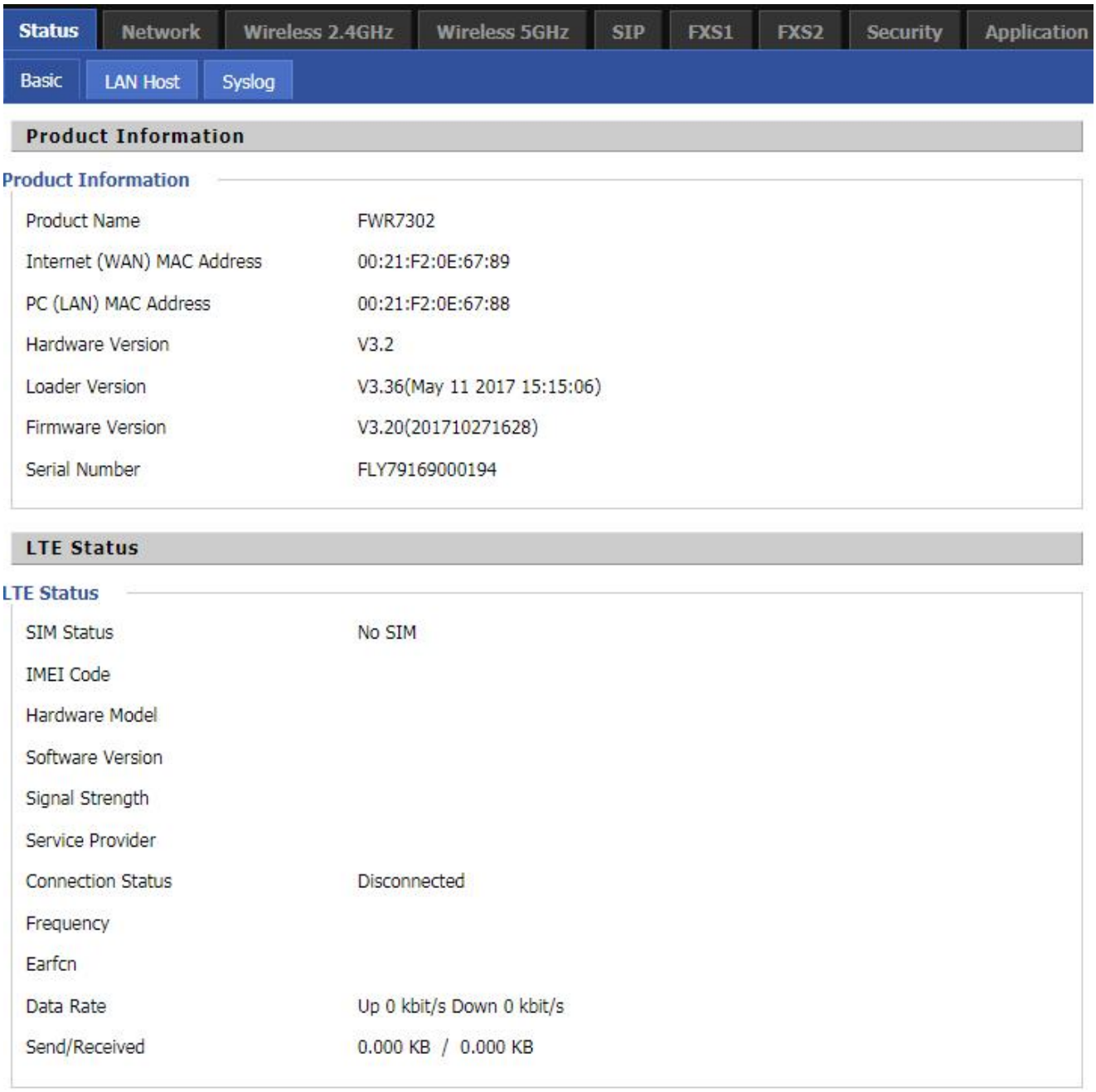
Table 12 Login details



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://192.168.1.1.
3. Enter Username admin and Password admin.
4. Click Login

Status

Table 13 Status Page



SIP Account Status

SIP Account Status

FXS 1 SIP Account Status	Registered 1100
Primary Server	192.168.10.88
Backup Server	192.168.10.88
FXS 2 SIP Account Status	Registered 1111
Primary Server	192.168.10.88
Backup Server	192.168.10.88

FXS Port Status

FXS Port Status

FXS 1 Hook State	On
FXS 1 Port Status	Idle
FXS 2 Hook State	On
FXS 2 Port Status	Idle

Network Status

Active WAN Interface

Connection Type	DHCP
IP Address	192.168.10.124 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
WAN Down Speed	212B/s
WAN Up Speed	628B/s

1 TR069_VOICE_INTERNET Vlan Status

Connection Type	DHCP
MAC Address	00:21:F2:0E:67:89
IP Address	192.168.10.124
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1

VPN Status

VPN Type	Disable
Initial Service IP	
Virtual IP Address	

LAN Port Status

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
LAN1	Link Down
LAN2	1000Mbps Full
LAN3	Link Down
LAN4	Link Down

Wireless Info

Wireless 2.4GHz

Radio On/Off	On
Network Mode	11b/g/n mixed mode
Current Channel	4
Channel Bandwidth	40MHz

Wireless 5GHz

Radio On/Off	On
Network Mode	11vht AC/AN/A
Current Channel	36
Channel Bandwidth	40MHz

Wireless_AP0E6788 (2.4GHz)

BSSID	00:21:F2:0E:67:88
Number of Device	0

Wireless_5G0E6788 (5GHz)

BSSID	00:21:F2:0E:67:8C
Number of Device	0

System Status

System Status

Current Time	2017-11-02 14:06:38
Elapsed Time	4 Hours, 14 Mins

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

Network and Security

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

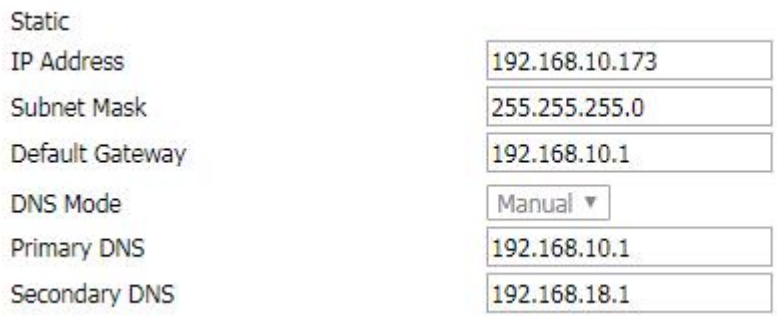
WAN

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



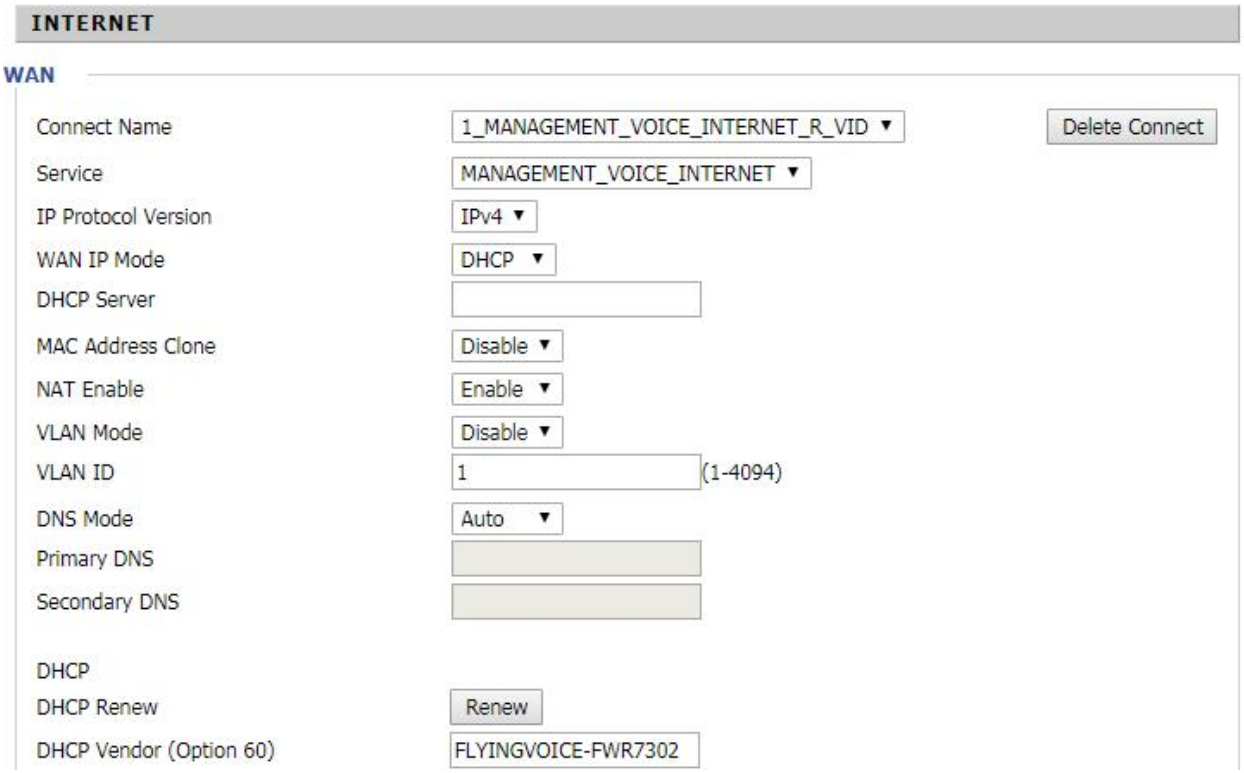
Field Name	Description
IP Address	The IP address of Internet port
Subnet Mask	The subnet mask of Internet port
Default Gateway	The default gateway of Internet port
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtain the 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



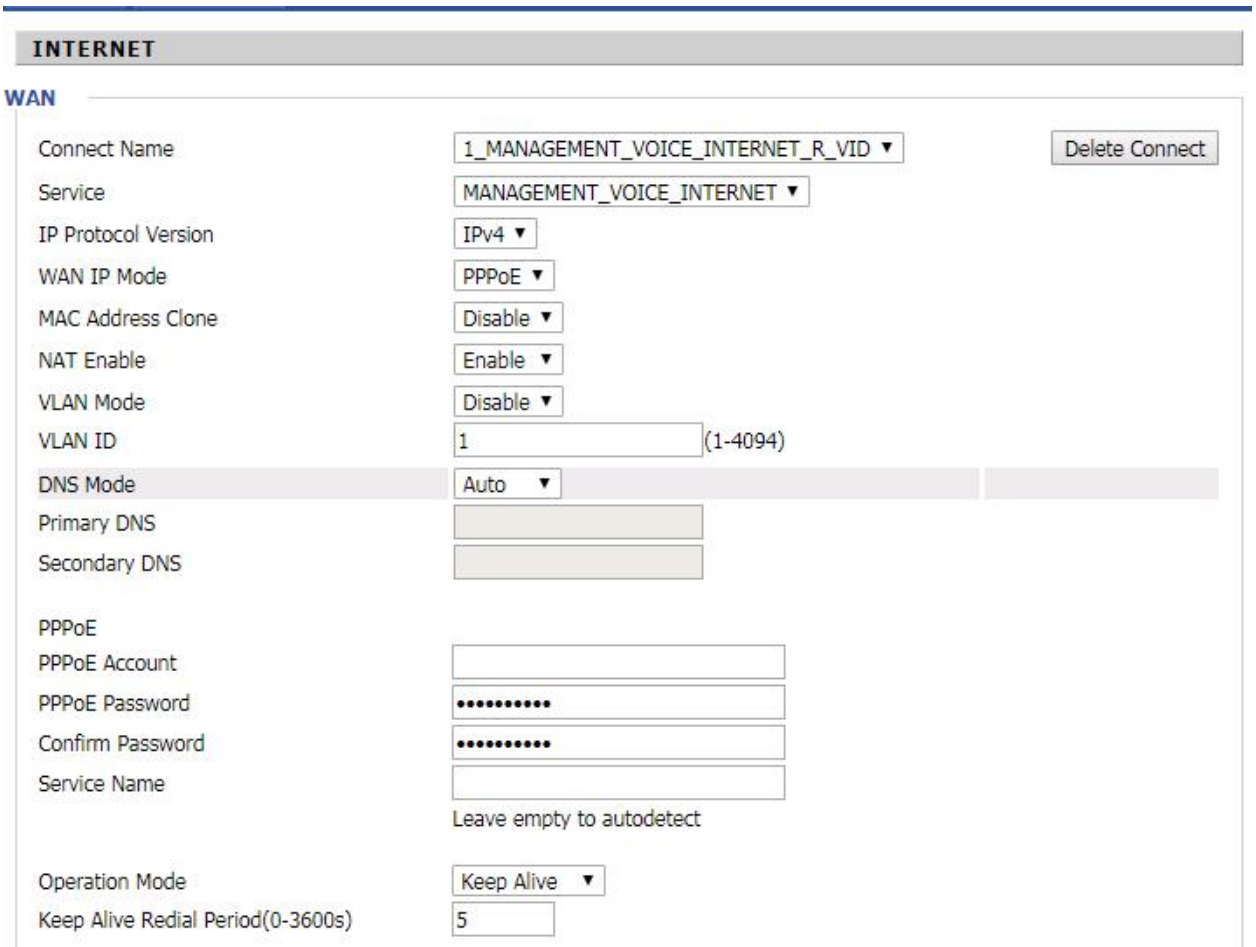
Field Name	Description
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS
Primary DNS Address	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



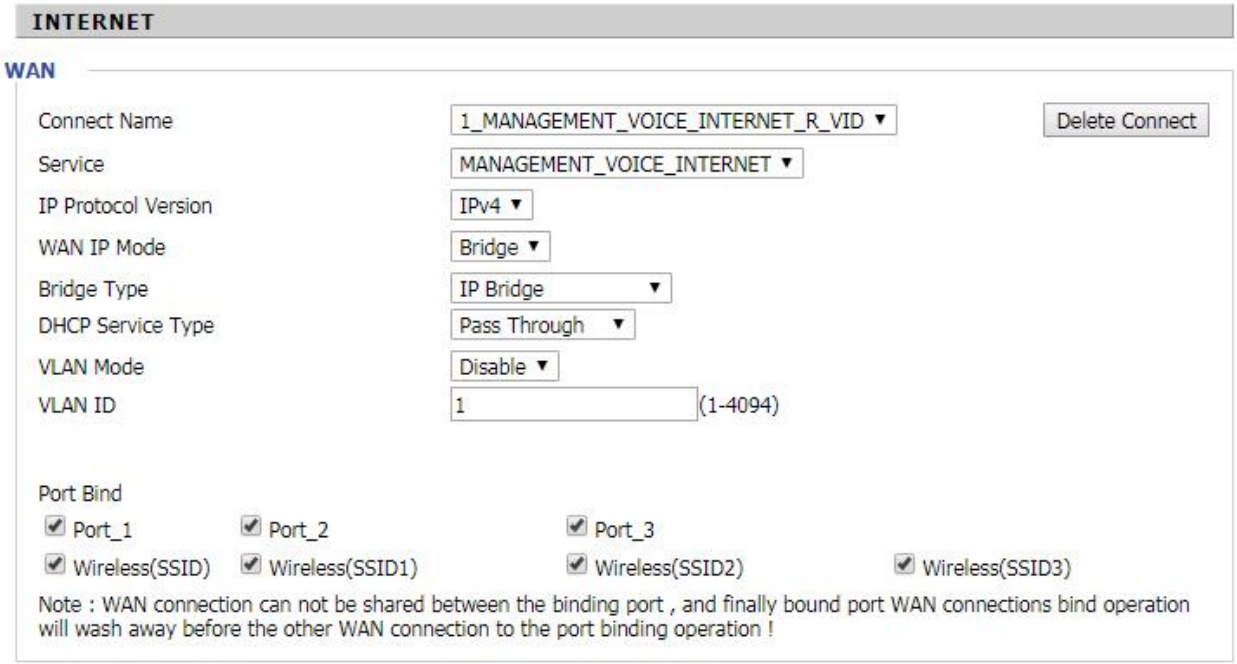
Field Name	Description
PPPoE Account	Enter a valid user name provided by the ISP
PPPoE Password	Enter a valid password provided by the ISP. The password can contain special characters and allowed special characters are $, +, *, #, @ and ! For example, the password can be entered as #net123@IT!$+*.

Confirm Password	Enter your PPPoE password again
Service Name	Enter a service name for PPPoE authentication. If it is left emply, 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 Period	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



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

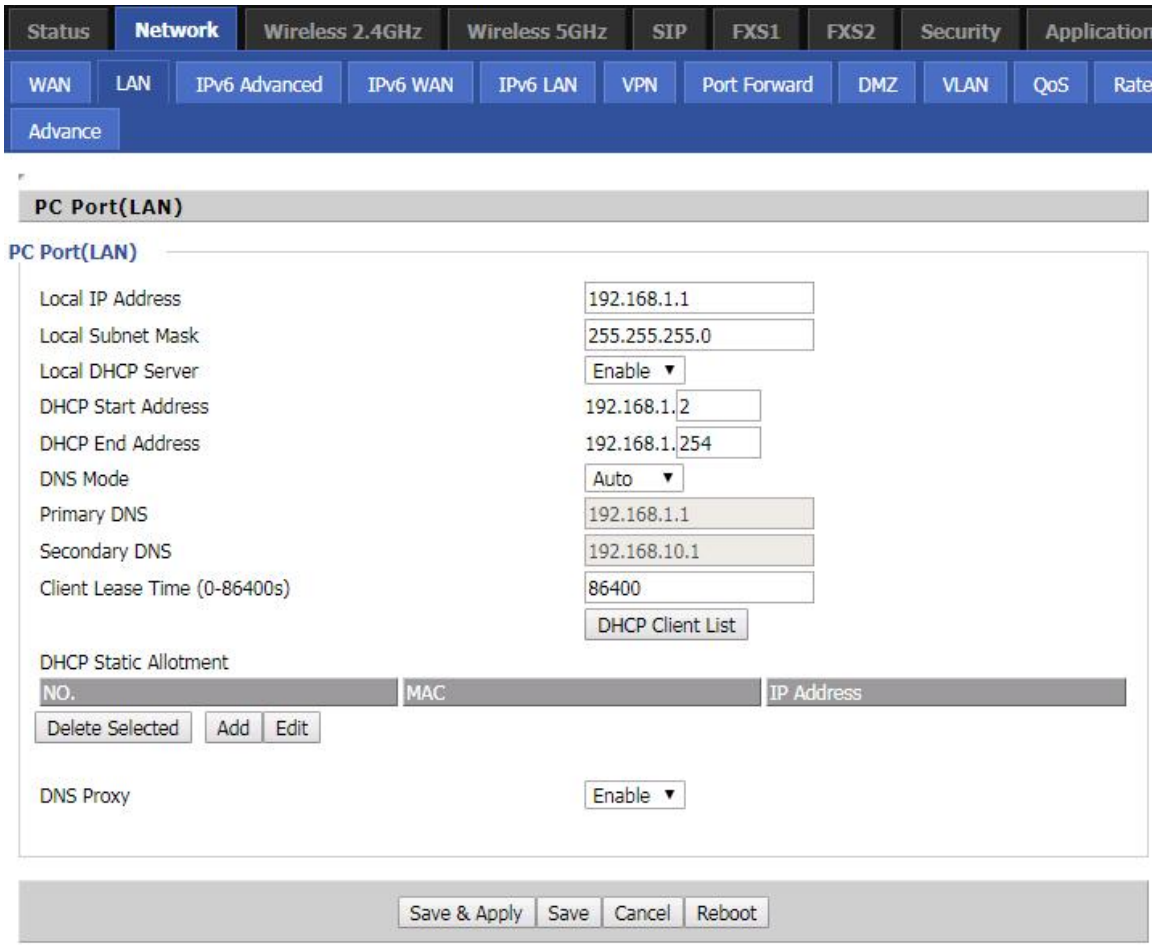
	DHCP packet from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to clients of LAN port.
Local Service	Gateway will not forward DHCP packets between LAN and WAN, it also blocks DHCP packets from the WAN port. Clients connected to the LAN port can get IP from DHCP server 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. **Note** Multiple WAN connections may be created with the same VLAN ID
802.1p	Set the priority of VLAN, Options are 0~7.

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



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.

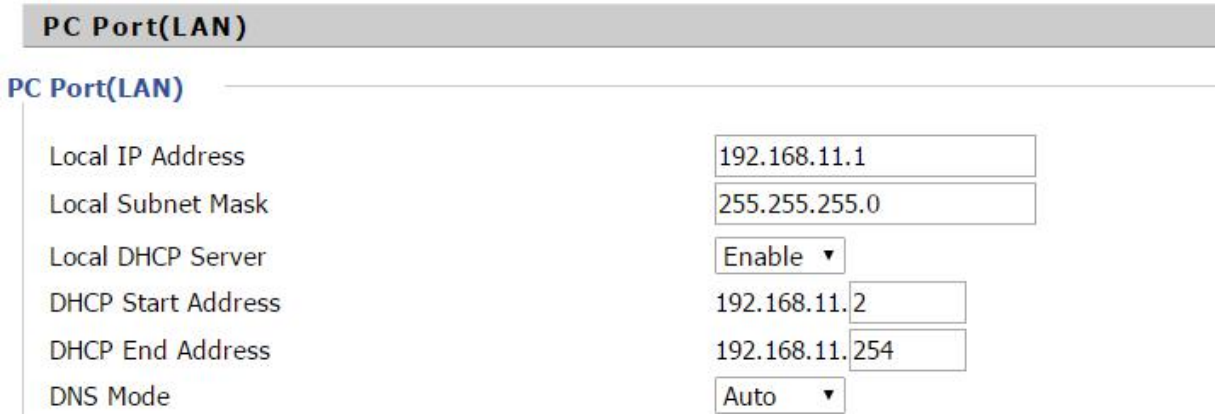
DHCP Start Address	Enter a valid IP address as a starting IP address of the DHCP server, and if the router's LAN IP address is 192.168.11.1, starting IP address can be 192.168.11.2 or greater, but should be less than the ending IP address.
DHCP End Address	Enter a valid IP address as an end IP address 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.

DHCP Server

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

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

Table 19 DHCP server settings



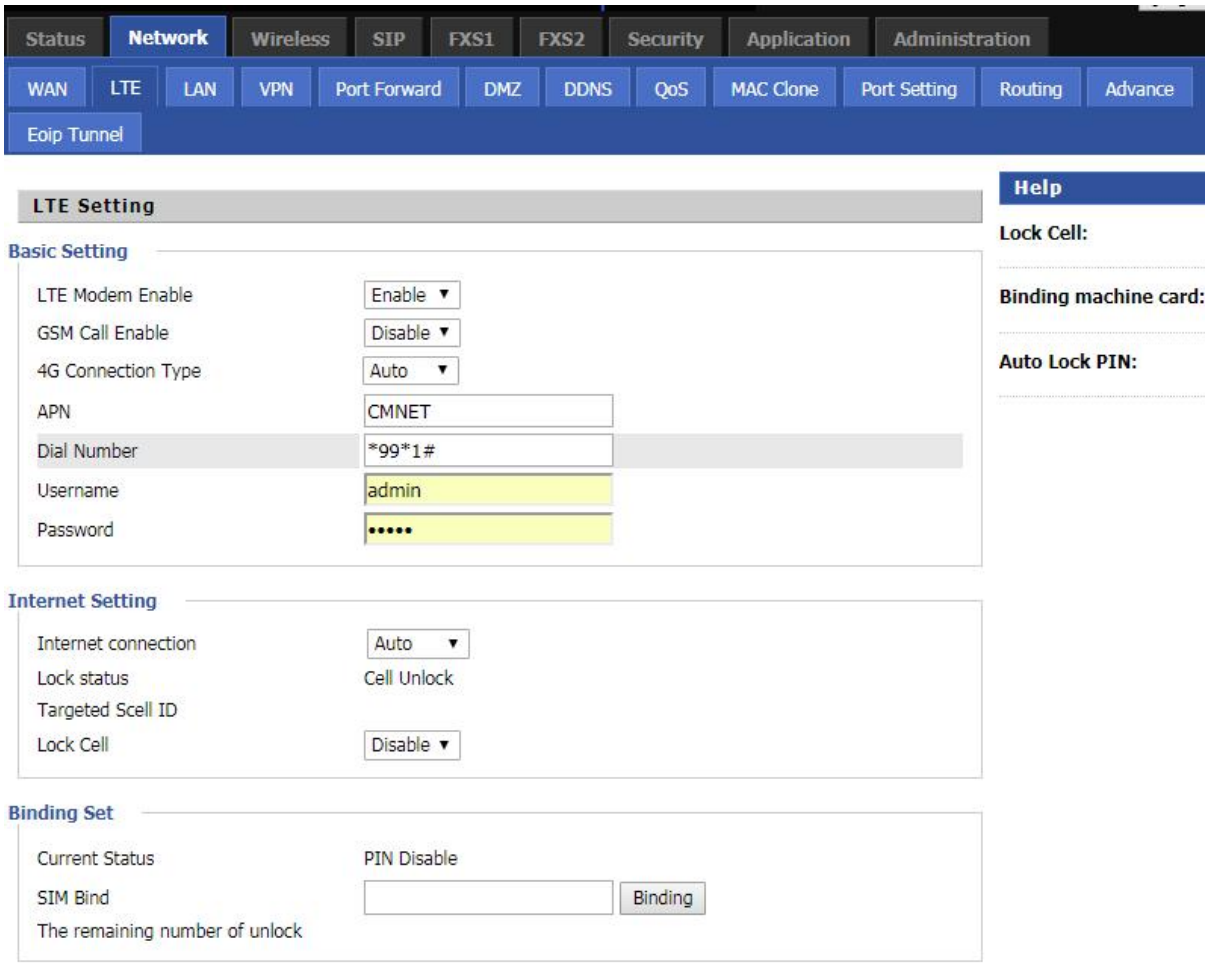
Field Name	Description
Local DHCP Server	Enable/Disable DHCP server.
DHCP Start Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses.
DHCP End Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
DNS Mode	If DNS information is to be received from a network server, set this parameter to Auto. If DNS information is to be configured manually, set this parameter to Manual.

Table 20 DHCP server, DNS and Client Lease Time

Field Name	Description
Primary DNS	Specify the Primary DNS address provided by your ISP. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 202.96.134.33 to this field.
Secondary DNS	Specify the Secondary DNS address provided by your ISP. If your ISP does not provide this address, the router will automatically apply default Secondary DNS Server IP of 202.96.128.86 to this field. If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
Client Lease Time	It allows you to set the leased time for the specified PC.

LTE

Table 21 LTE

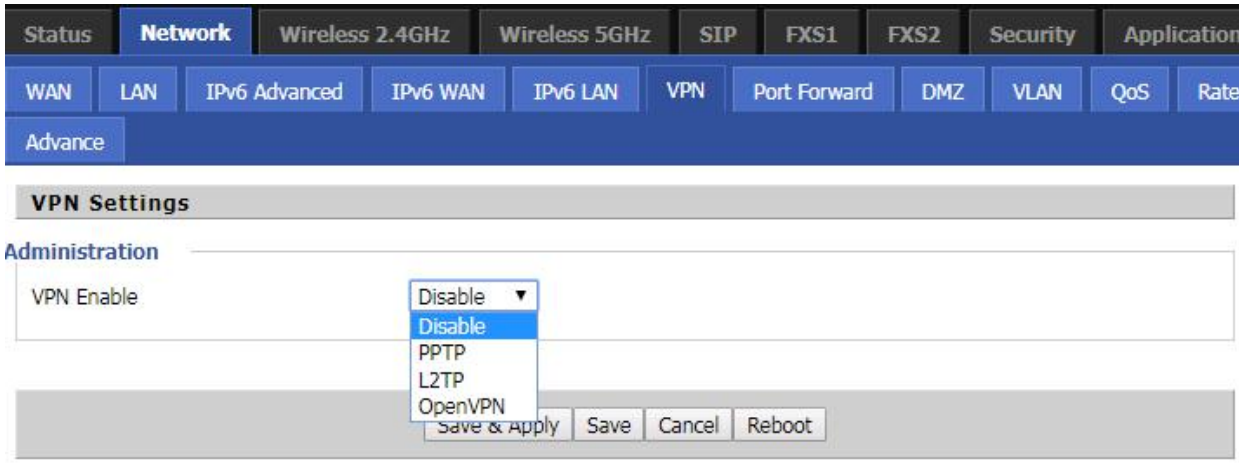


Field Name	Description
Basic Setting	
LTE Modem Enable	Enable the LTE Modem
GSM Call Enable	Enable the GSM Cal
4G Connection Type	Choose the 4G connection method,Auto or Manual
APN	The APN default to CMNET
Dail Number	
Username	Enter the username
Password	Enter the Password
Internet Setting	
Internet connection	Choose the internet connection in Auto/4G only/3G only/
Lock status	Check the lock status of the cell
Targeted Sell ID	Here is Targeted Sell ID
Lock Cell	Enable or Disable lock cell
Binding Set	
Current Status	Check the status of the current PIN here
SIM Bind	Fill in the phone number and Bind the SIM Card

VPN

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

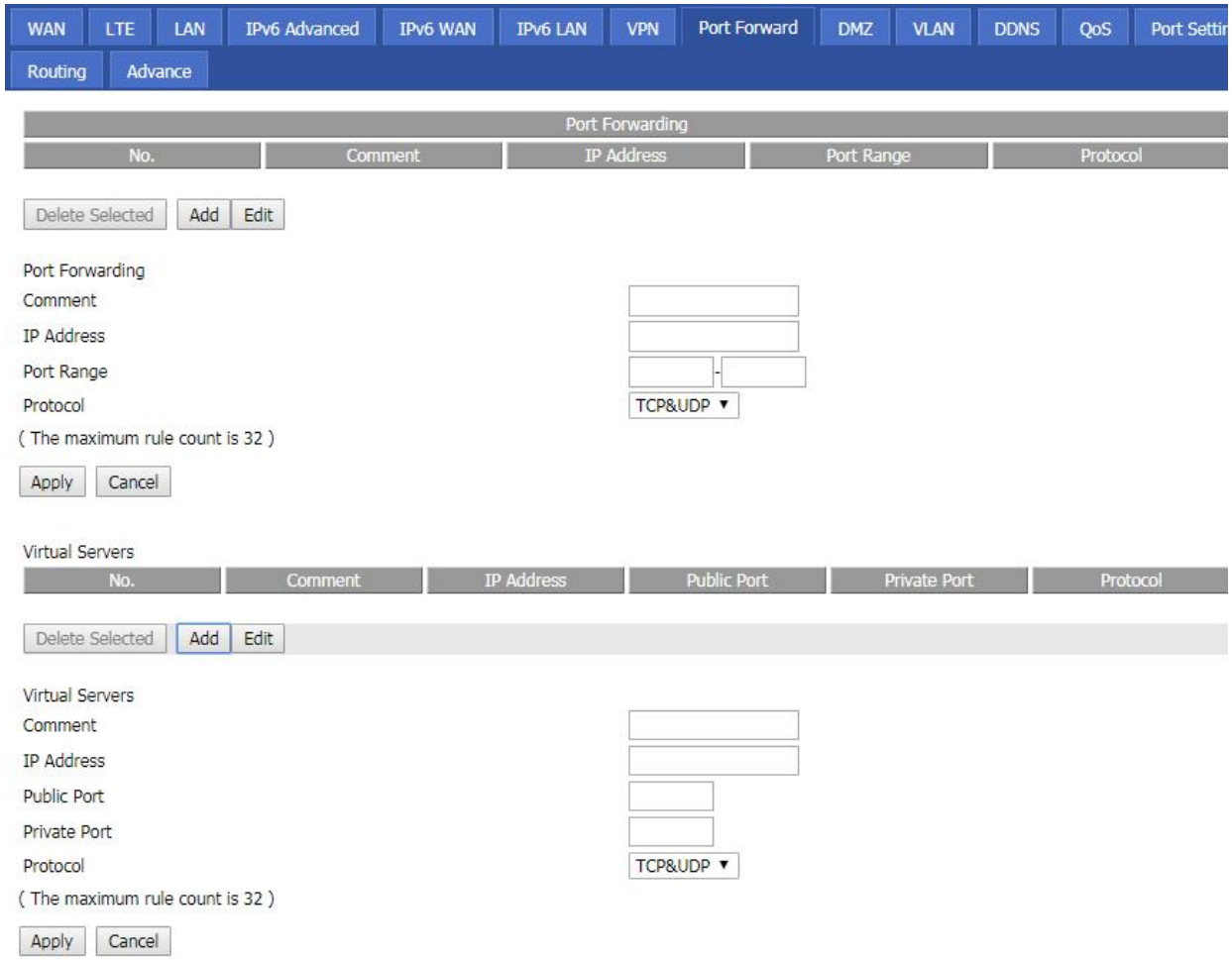
Table 22 VPN



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

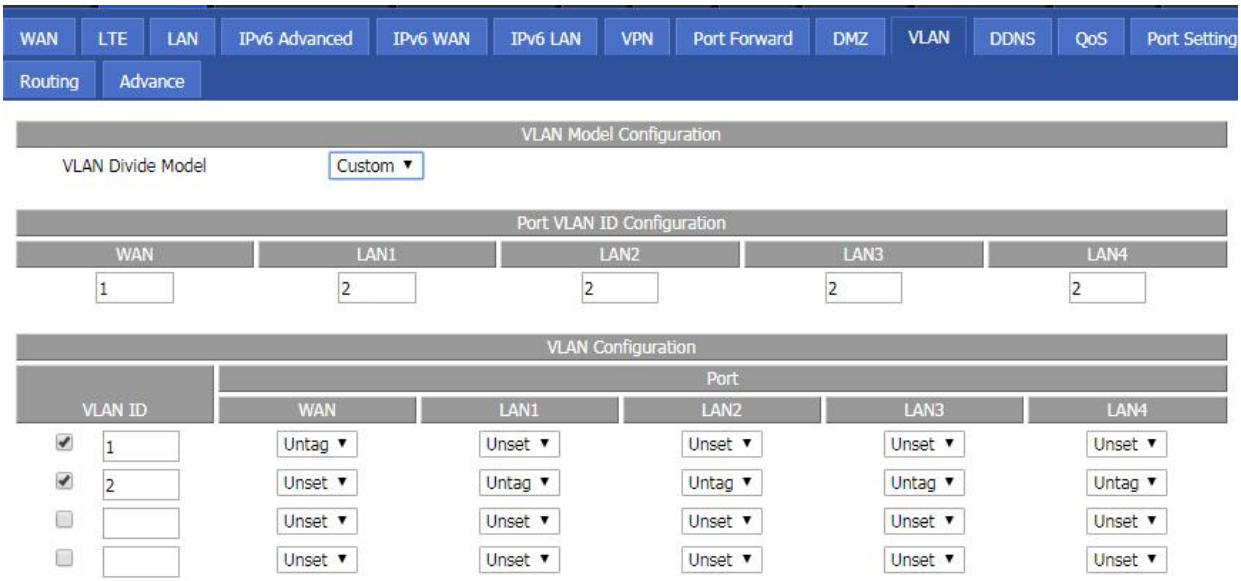
Table 22 Port Forward



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

VLAN

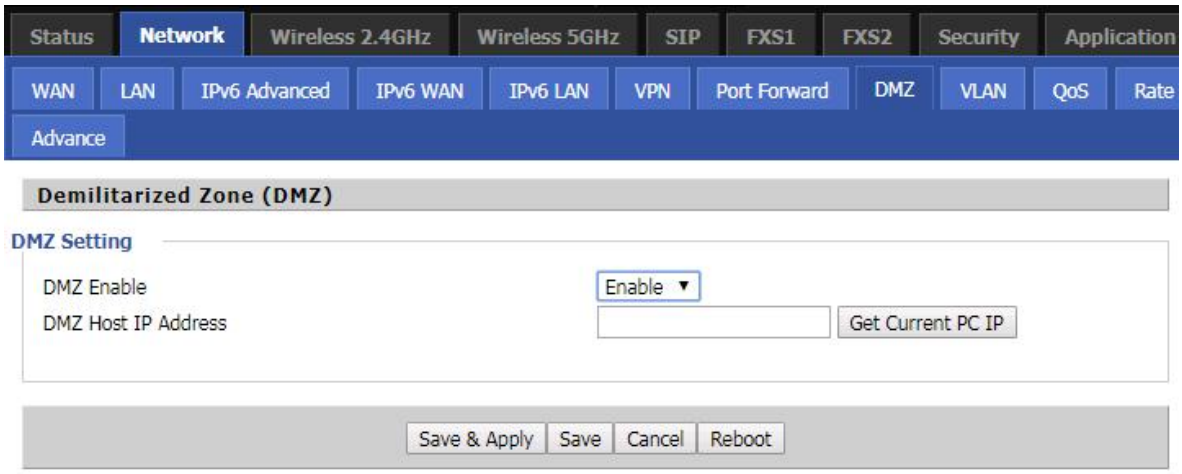
Table 23 VLAN



Field Name	Description
VLAN Divide Model	Select the desired mode
VLAN Configurations	Select the desired configuration, divided into unset / Tagged / unTagged

DMZ

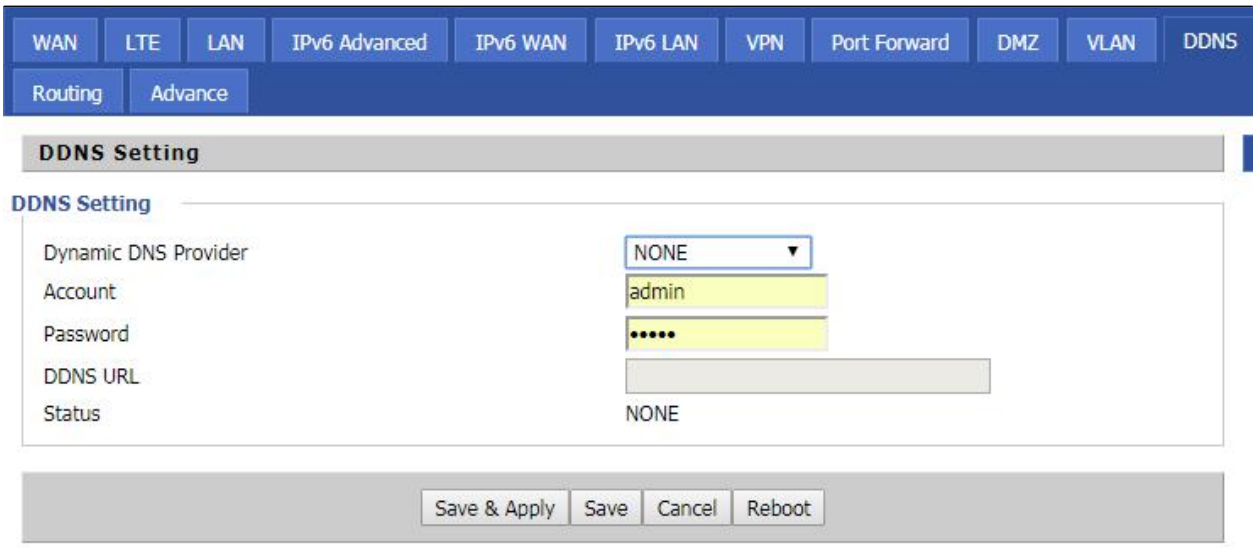
Table 24 DMZ



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

DDNS

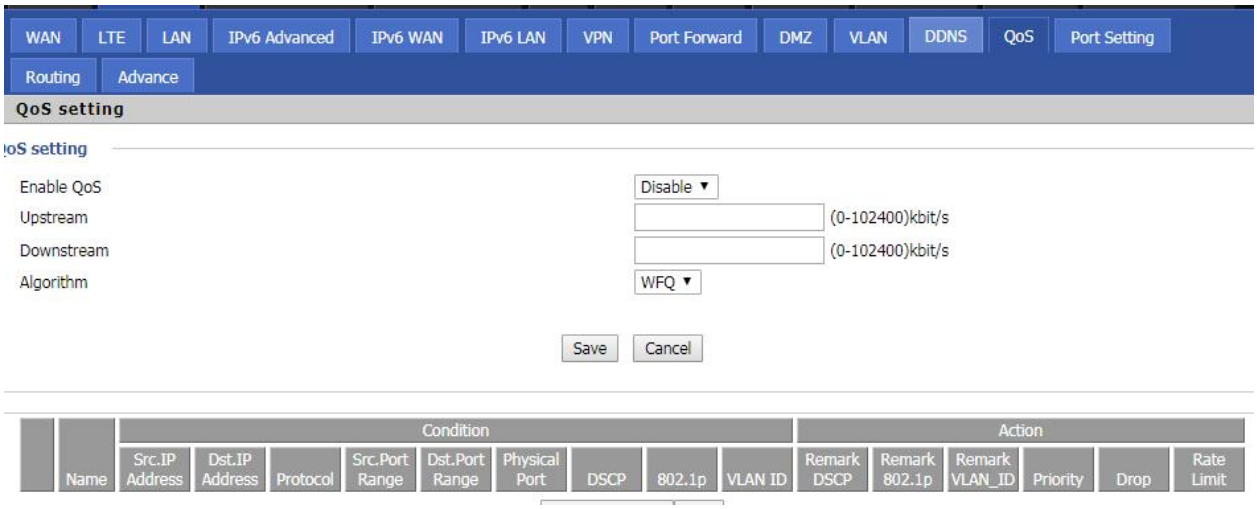
Table 25 DDNS



Field Name	Description
Dynamic DNS	Enable DDNS and select the DDNS service provider
Account	Fill in the DDNS service account
Password	Fill in the DDNS service account password
DDNS URL	Fill in the DDNS domain name or IP address
Status	Check if DDNS is successfully upgraded

QoS

Table 26 QoS



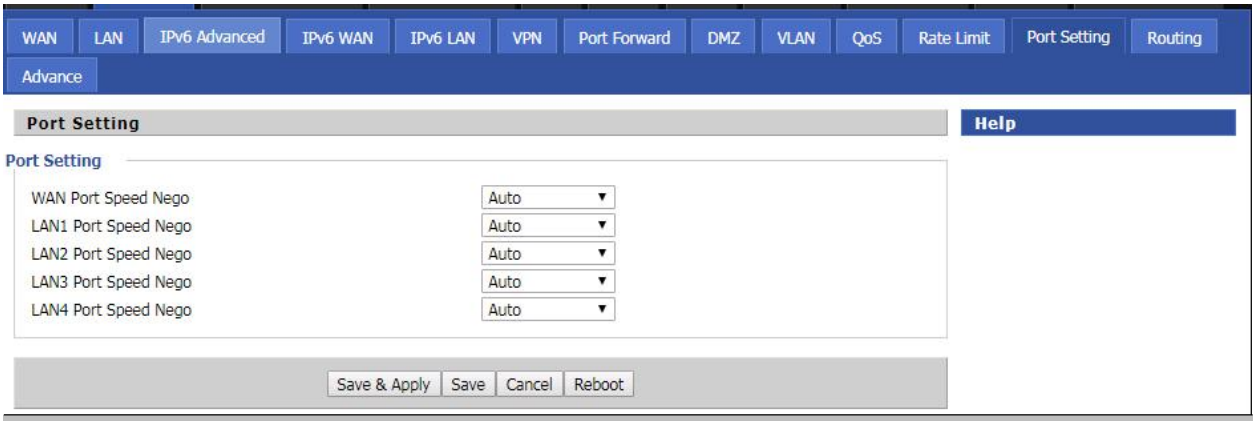
Field Name	Description
QoS Enable	Enable/Disable QoS function
Upstream	Set the upstream bandwidth
Downstream	Set the downstream bandwidth
Delete Selected	In NO., Check the items you want to delete, click the Delete option
Add	Click Add to add a new parameter

Note

From system release 4.2 or later, the QoS bandwidth can be configured for Upstream and Downstream

Port Setting

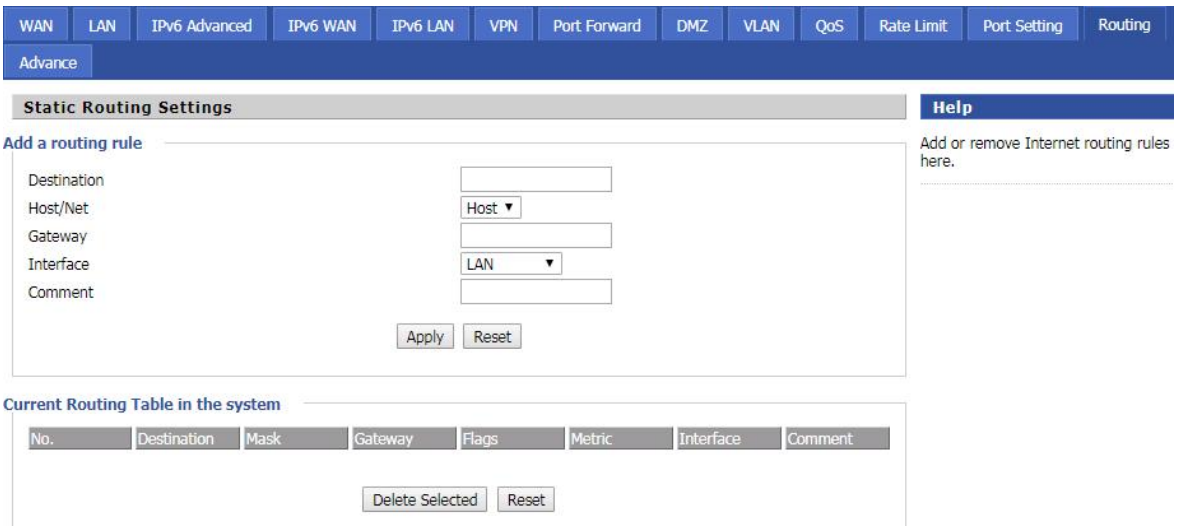
Table 27 Port setting



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 28 Routing

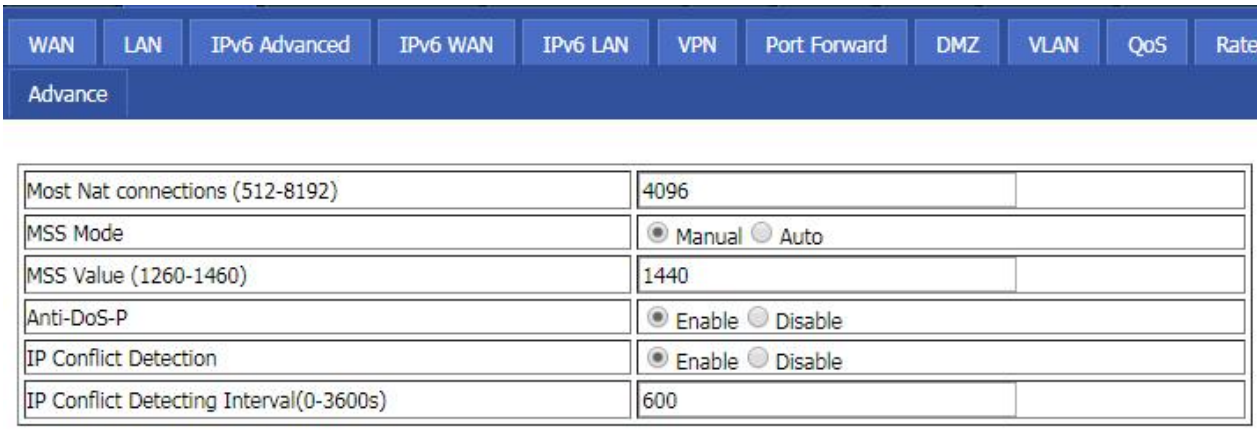


Field Name	Description
Destination	Destination address
Host/Net	Both Host and Net selection
Gateway	Gateway IP address
Interface	LAN/WAN/Custom three options, and add the corresponding address

Comment	Comment

Advance

Table 29 Advance

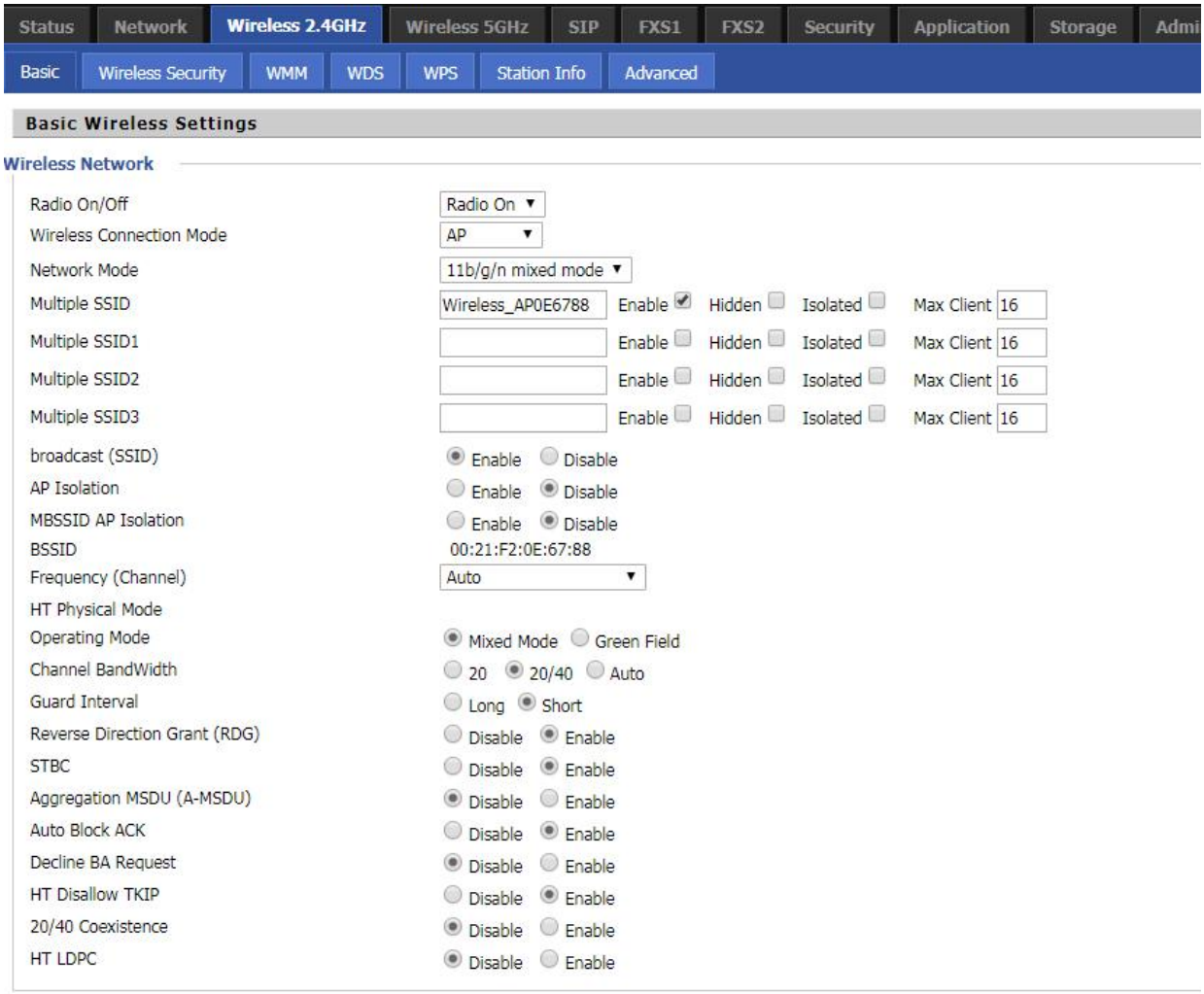


Field Name	Description
Most Nat connections	The largest value which the FWR7302 can provide
Mss Mode	Choose Mss Mode from Manual and Auto
Mss Value	Set the value of TCP
AntiDos-p	You can choose to enable or prohibit
IP conflict detection	Select enable if enabled, phone IP conflict will have tips or prohibit
IP conflict Detecting Interval	Detect IP address conflicts of the time interval

Wireless 2.4G

Basic

Table 30 Basic



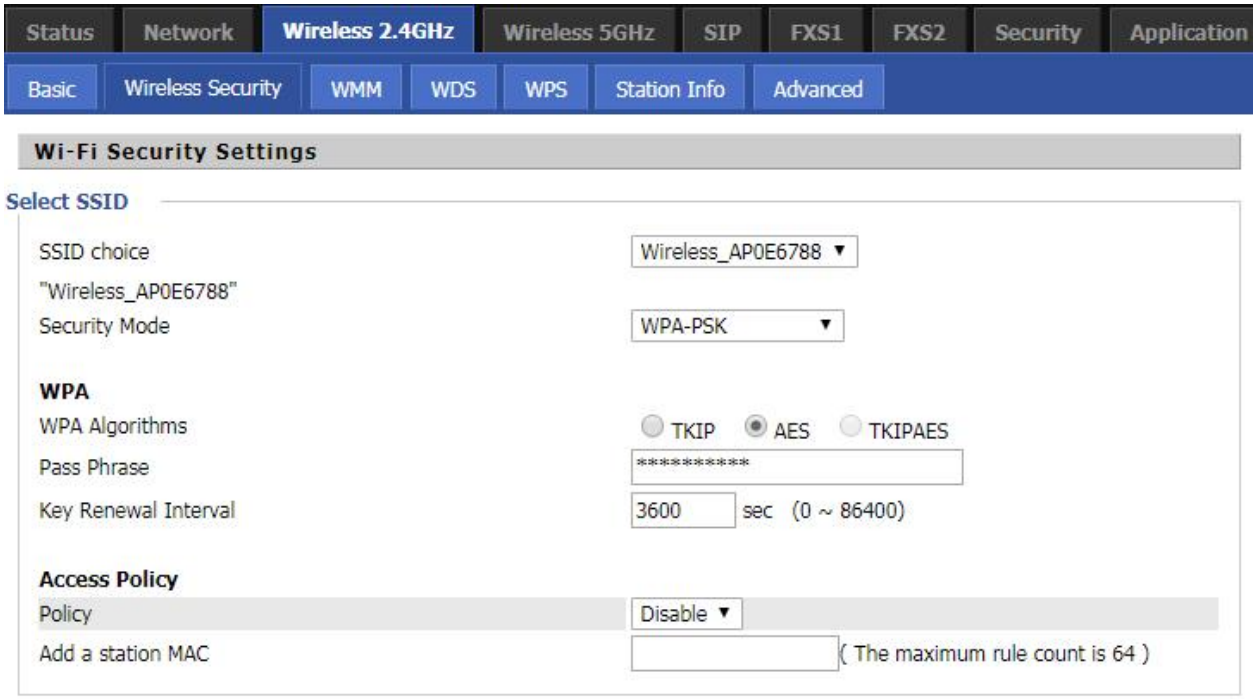
Field Name	Description
Radio on/off	Select “Radio off” to disable wireless. Select “Radio on” to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP
Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed 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 Dirction 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 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 31 Wireless security

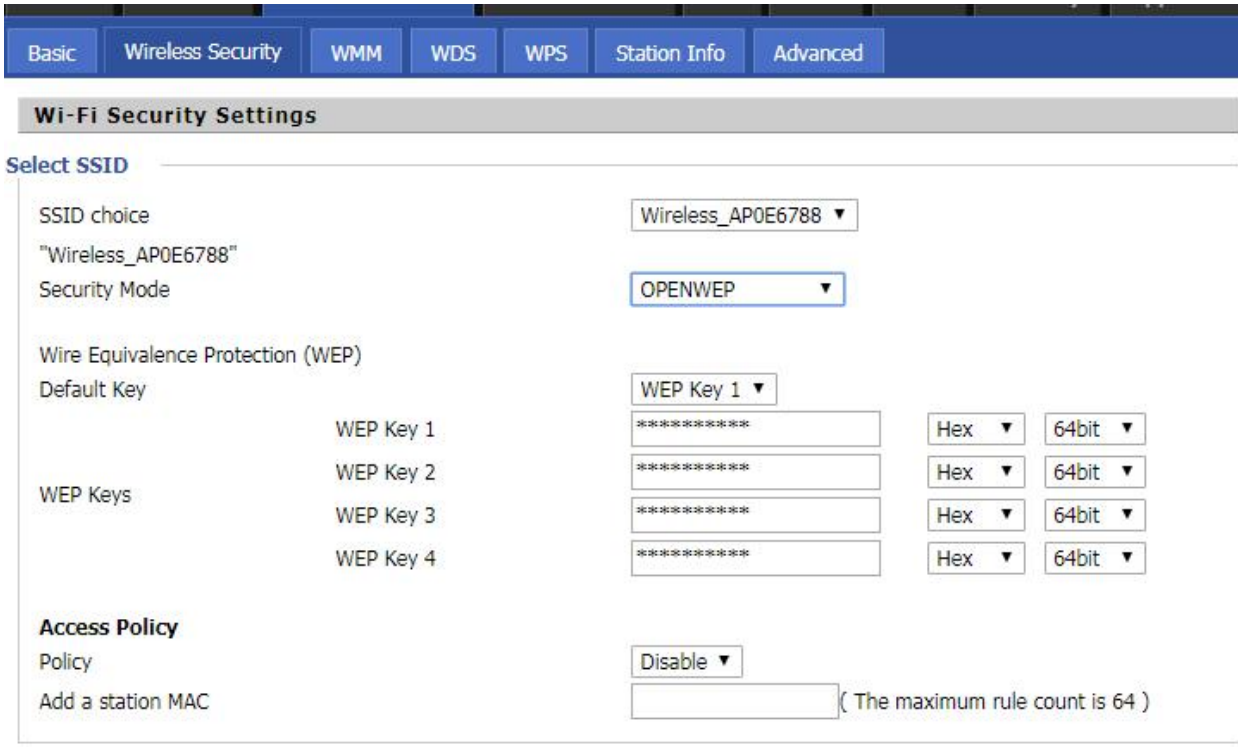


Field Name	Description
SSID Choice	Choose one SSID from SSID, Multiple SSID1, Multiple SSID2 and Multiple SSID3.
Security Mode	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.Each encryption mode will bring out different web page and ask you to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

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 32 WiFI Security Setting

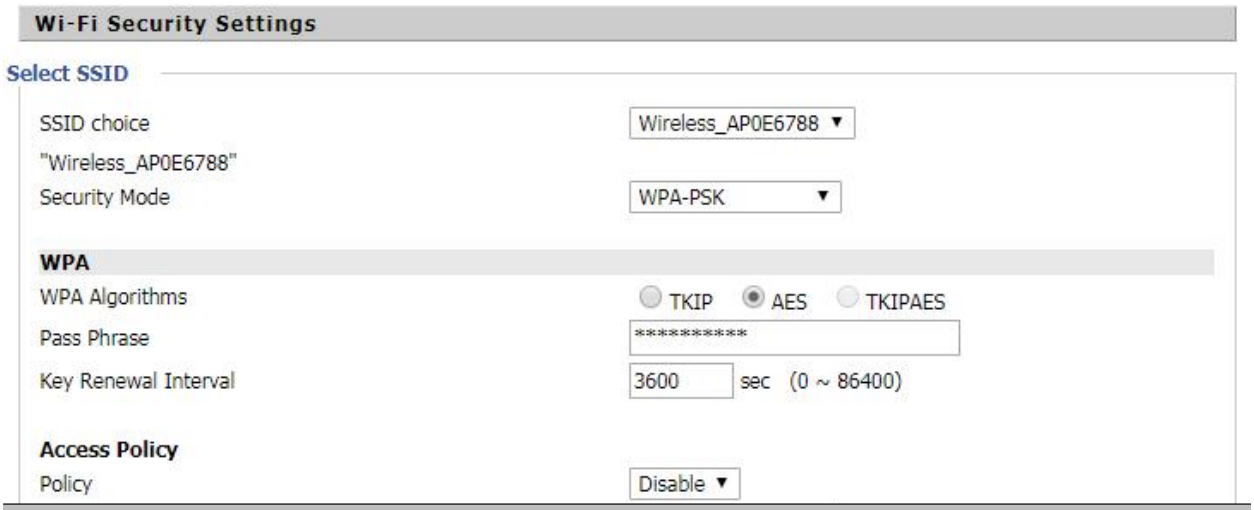


Field Name	Description
Security Mode	This is used to select one of the 4 WEP keys, key settings on the clients should be the same with this when connecting.
WEP Keys	Set the WEP key. A-64 key need 10 Hex characters or 5 ASCII characters; choose A-128 key need 26 Hex characters or 13 ASCII characters.

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 .

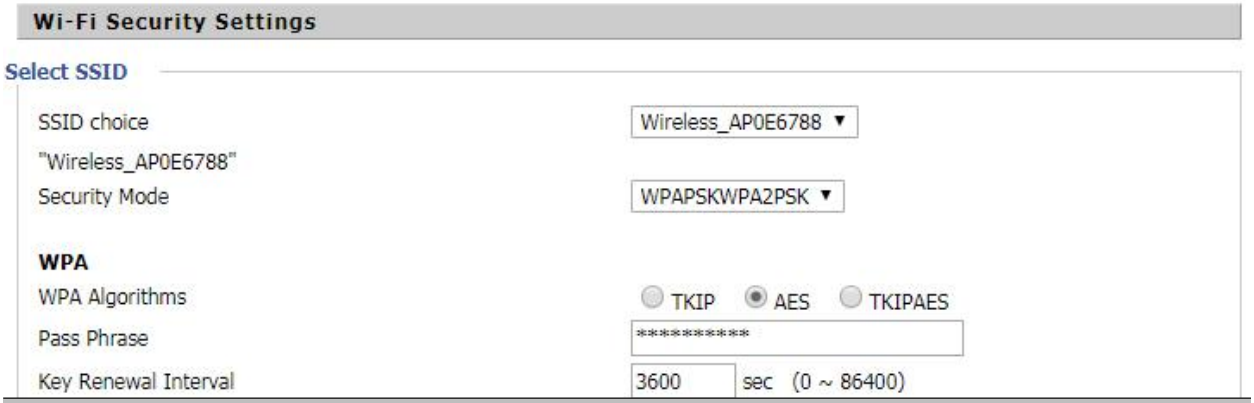
Table 33 WPA-PSK



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.

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 34 WPAPSKWPA2PSK

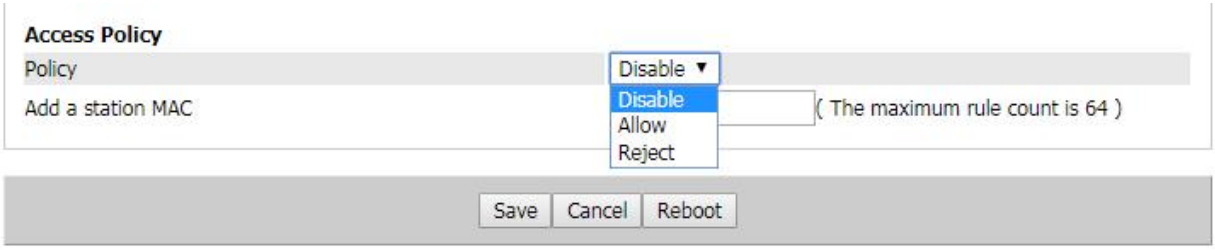


Field Name	Description
WPA Algorithms	The home gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms.
Pass Phrase	Set WPA-PSK/WPA2-PSK security code
Key Renewal Interval	Set the key scheduled update cycle, default 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 35 Wireless Access Policy

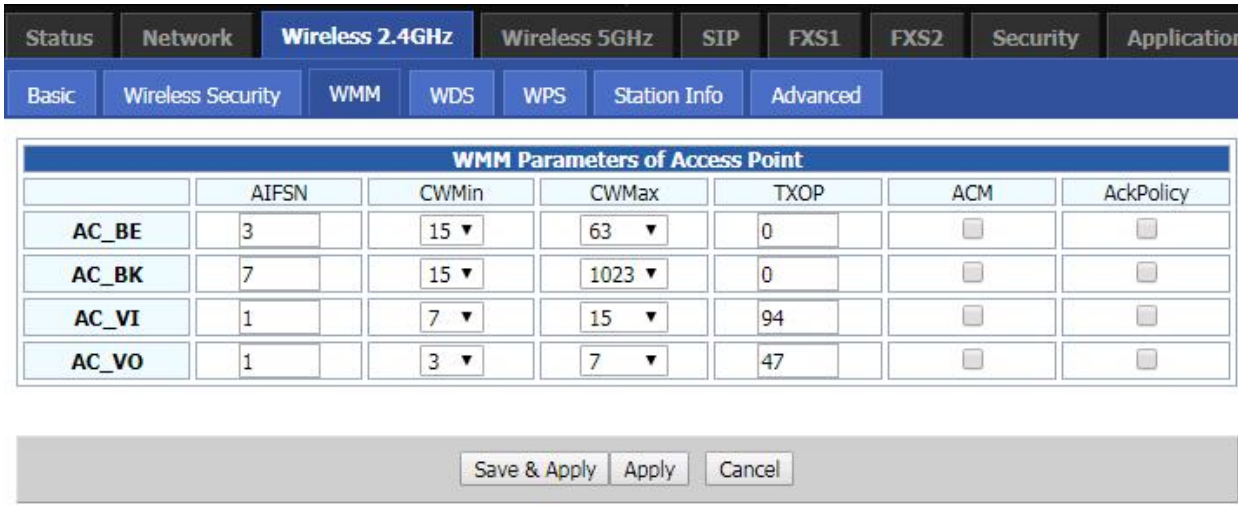


Field Name	Description
Access policy	Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address.
Policy	Disable : Prohibition: wireless access control policy. Allow: only allow the clients in the list to access. Rejected: block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

Table 36 WMM

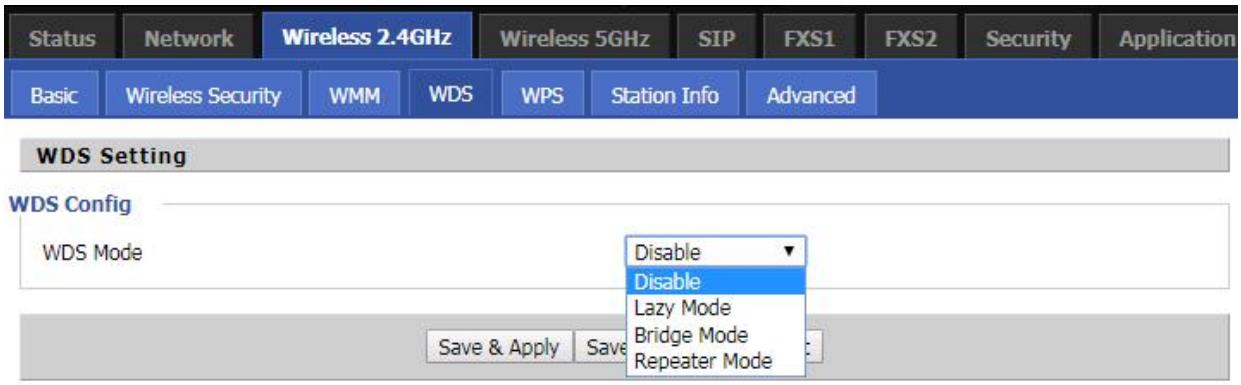


Description

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.

WDS

Table 37 WDS



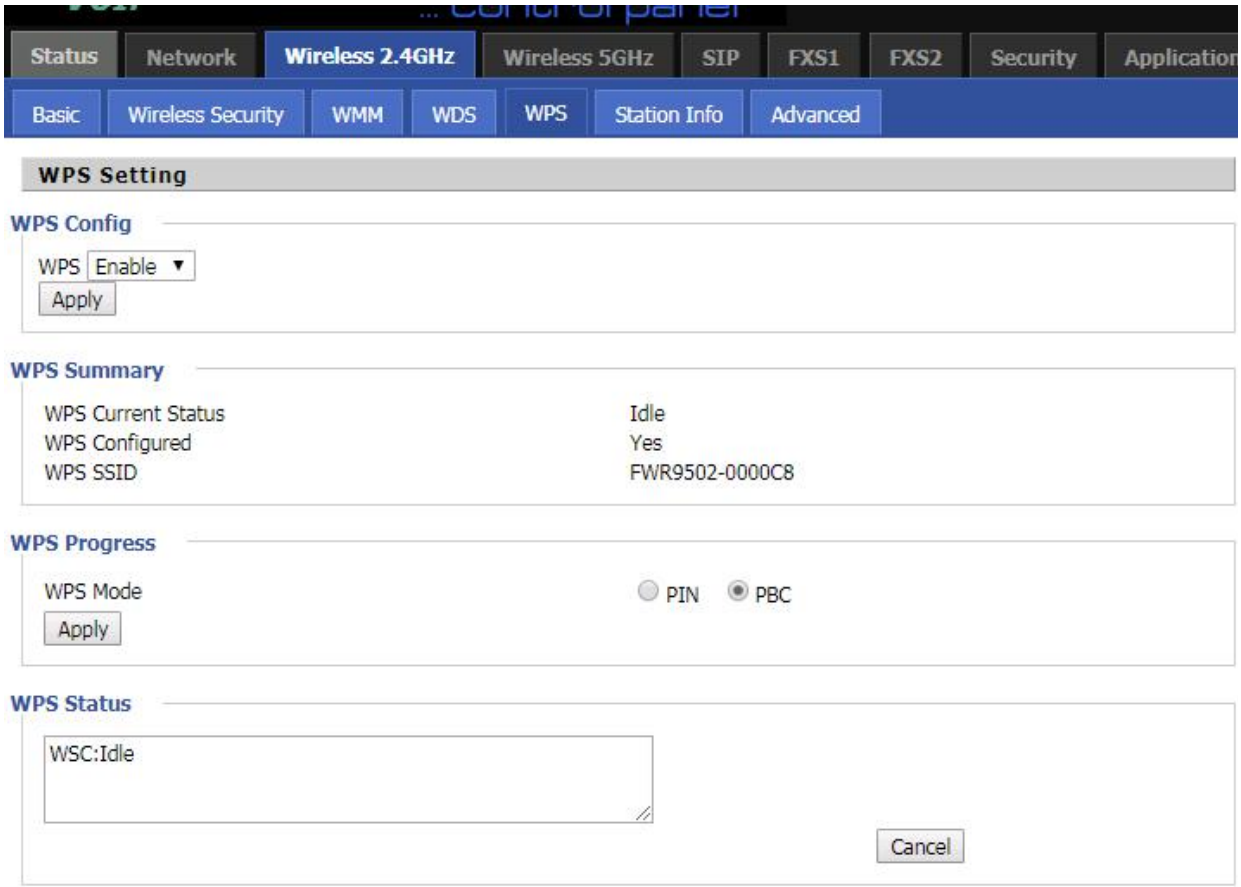
Description
WDS stands for Wireless Distribution System, enabling WDS access points to be interconnected to expand a wireless network.

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 38 WPS

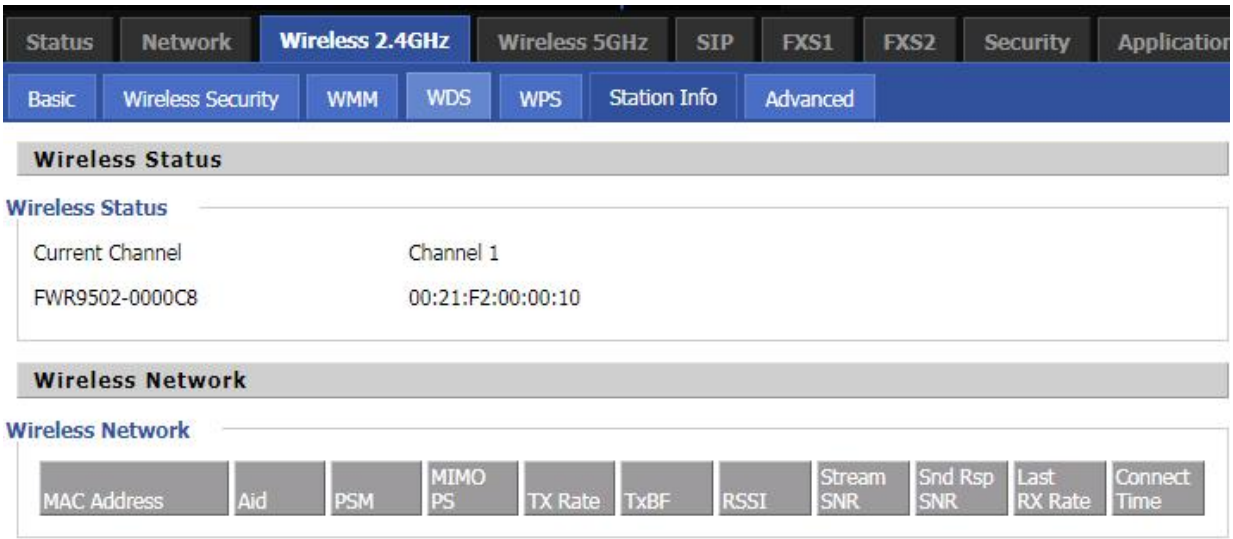


Field Name	Description
WPS Config	
WPS	Enable/Disable WPS function
WPS Summary	
WPS Current Status	Display the current status of WPS
WPS Configured	Display the configure the status information of WPS
WPS SSID	Display WPS SSID
WPS Progress	
WPS Mode	PIN：Enter the PIN code of the wireless device which 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

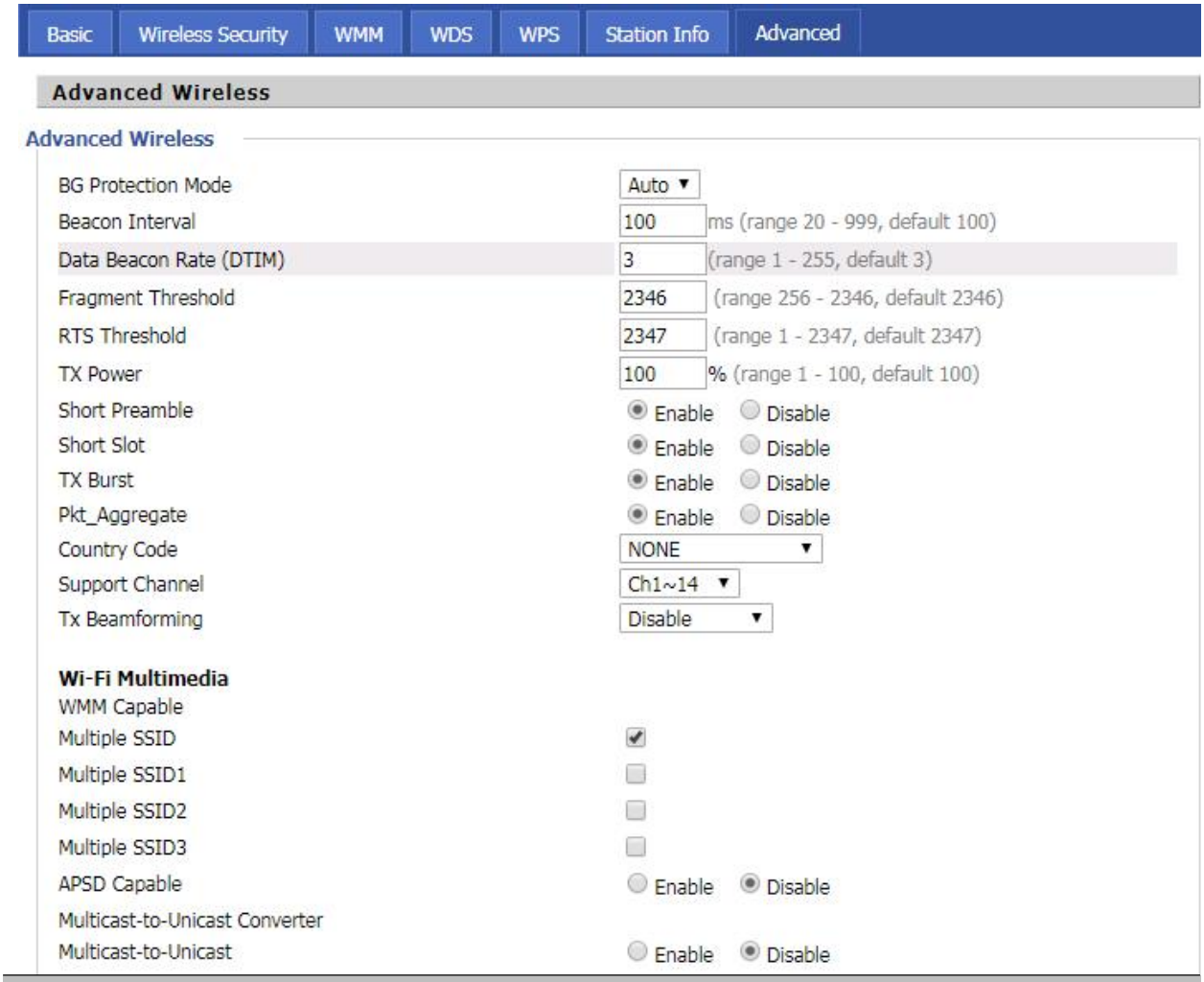
Table 39 Station info



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

Advanced

Table 40 Advanced



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 WMM Configuration, 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

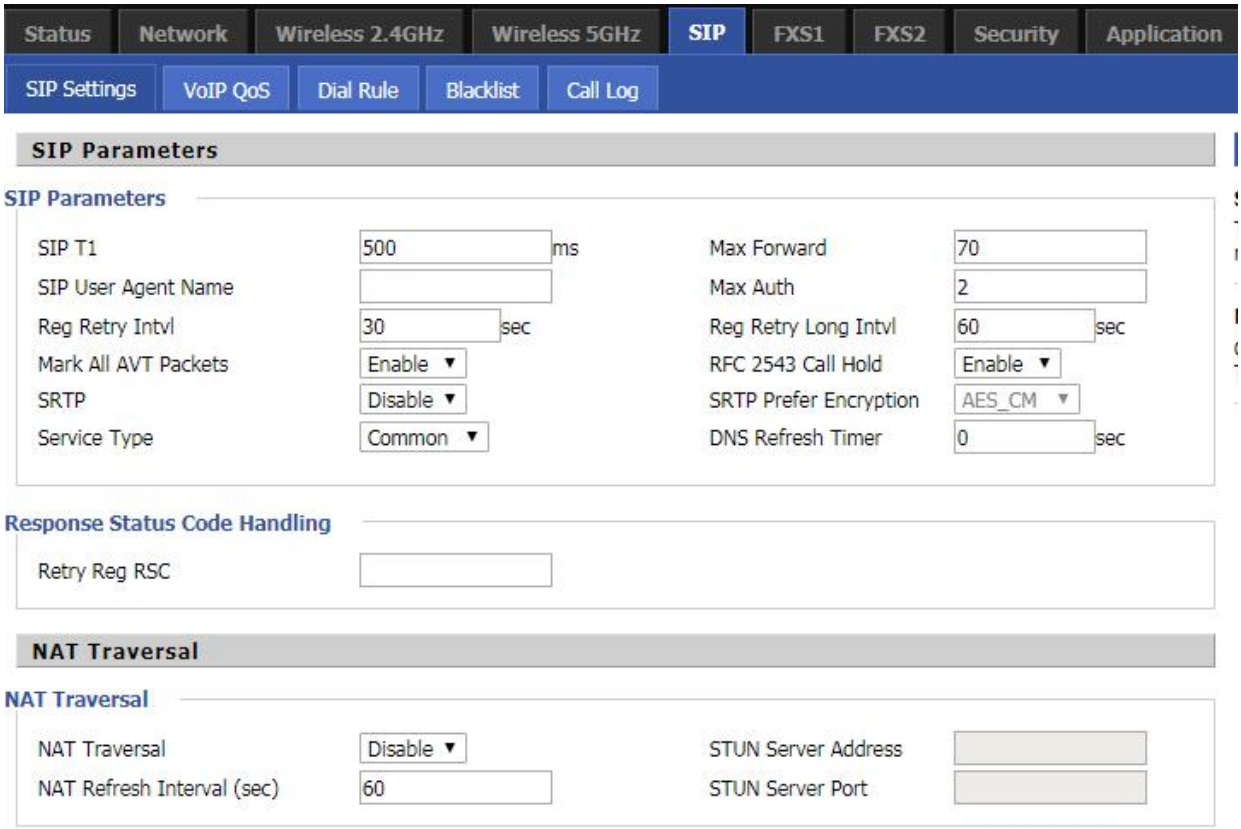
Wireless 5G

Please refer to the wireless 2.4G.

SIP

SIP Settings

Table 41 SIP settings

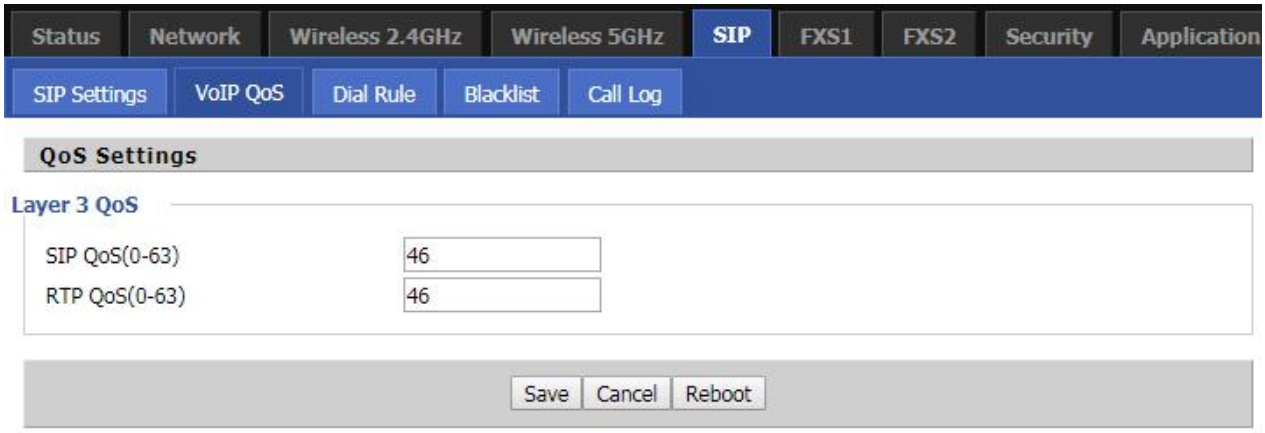


Field Name	Description
SIP T1	The minimum scale of retransmission time
Max Forward	SIP contains Max Forward message header fields used to limit the requests for forwards
SIP Reg User Agent Name	The agent name of SIP registered user
Max Auth	The maximum number of retransmissions

Mark All AVT Packets	Voice packet marking to enable this item will see the mark on the voice message when the call environment changed (such as press a key during the call)
RFC 2543 Call Hold	Enable the Connection Information field displays the address is 0.0.0.0 in the invite message of Hold.Disable the Connection Information field displays the device IP address in the invite message of Hold
SRTP	Whether to enable the call packet encryption function
SRTP Prefer Encryption	The preferred encryption type of calling packet (the Message body of INVITE Message)
Service Type	Choose the server type
NAT Traversal	Enable/Disable NAT Traversal FWR9502 supports STUN Traversal; if user wants to traverse NAT/Firewall, select the STUN
STUN Server Address	Add the correct STUN service provider IP address
NAT Refresh Interval	Set NAT Refresh Interval, default is 60s
STUN Server Port	Set STUN Server Port, default is 5060

VoIP QoS

Table 42 VoIP QoS

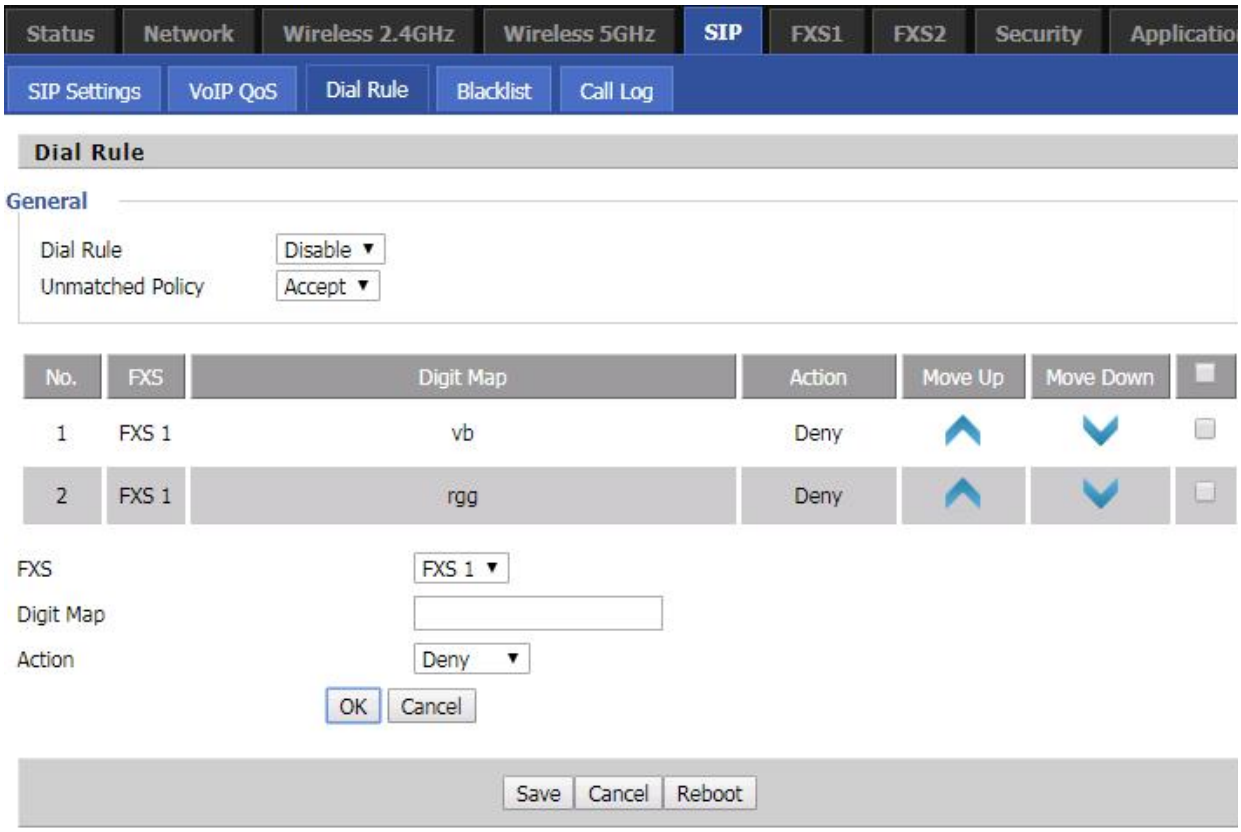


Field Name	Description
SIP /RTP QoS	The default value is 0,you can set a range of values is 0~63

Dial Plan

Parameters and Settings

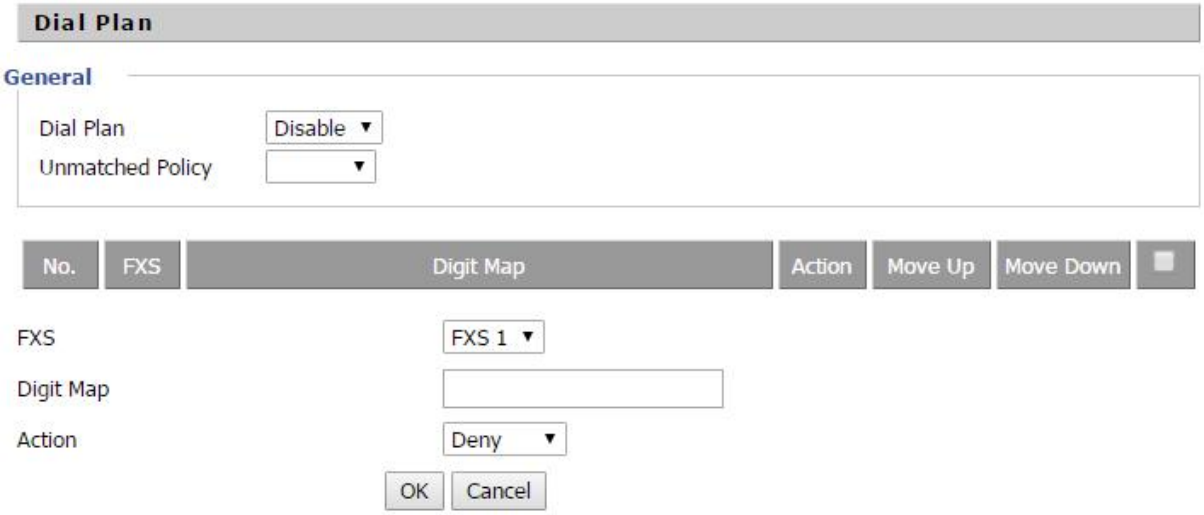
Table 43 Parameters and settings



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 44 Adding one dial plan



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

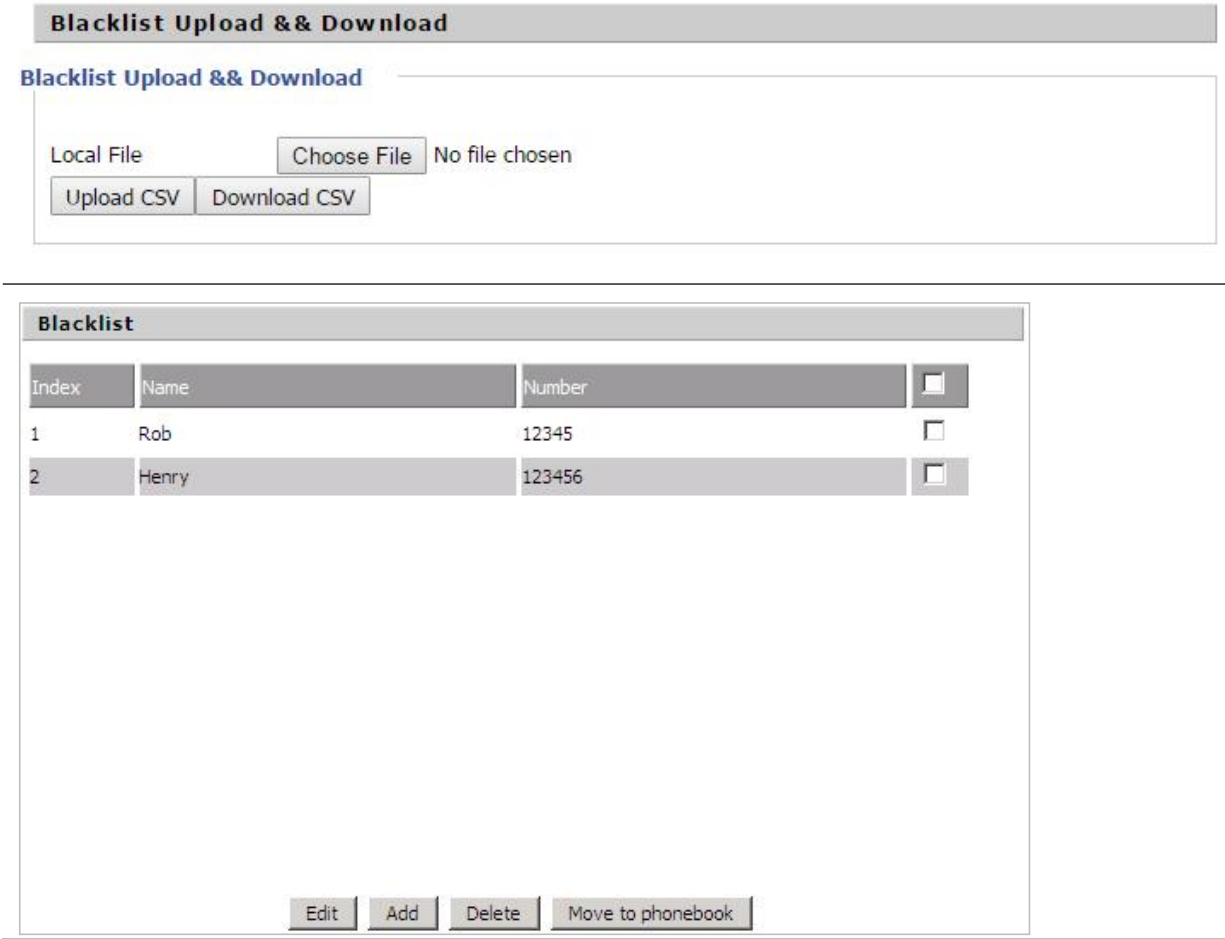
Table 45 Dial Plan

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 46 Blacklist



Description
Click 选择文件 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 47 Call log

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	

Redial List

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	

Answered 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	☐

Missed Calls

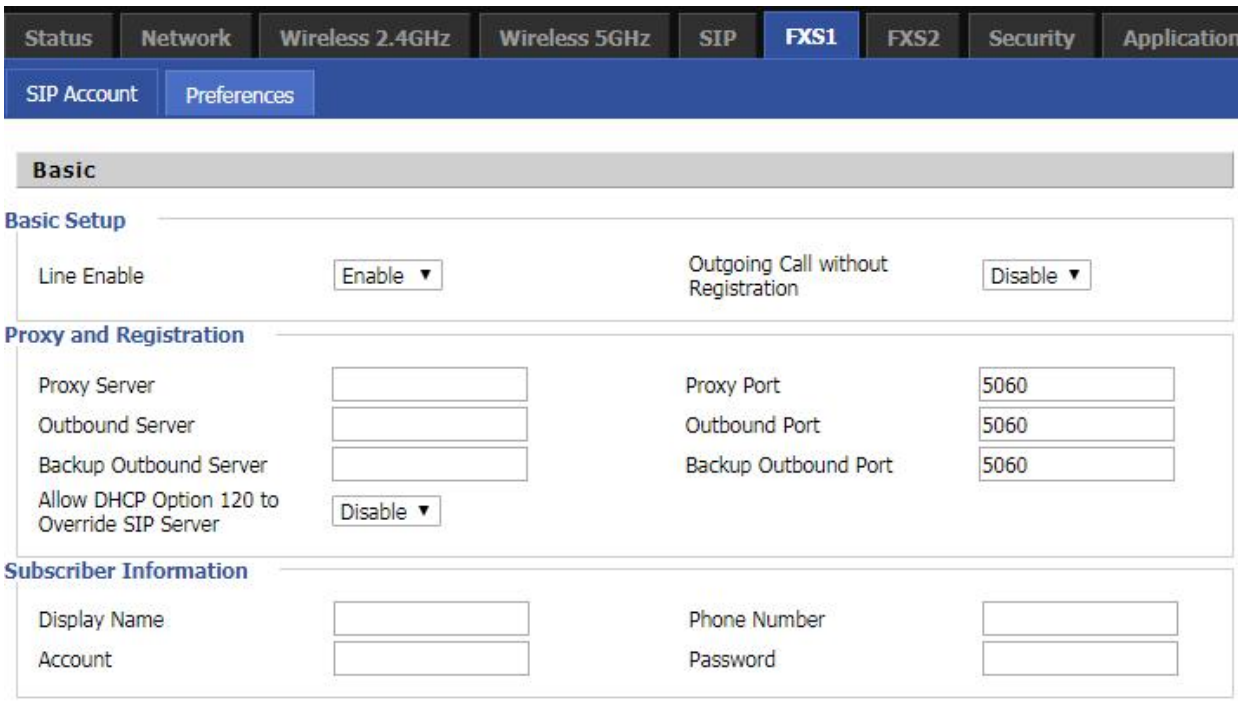
FXS1

SIP Account

Basic

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

Table 48 SIP Account - Basic

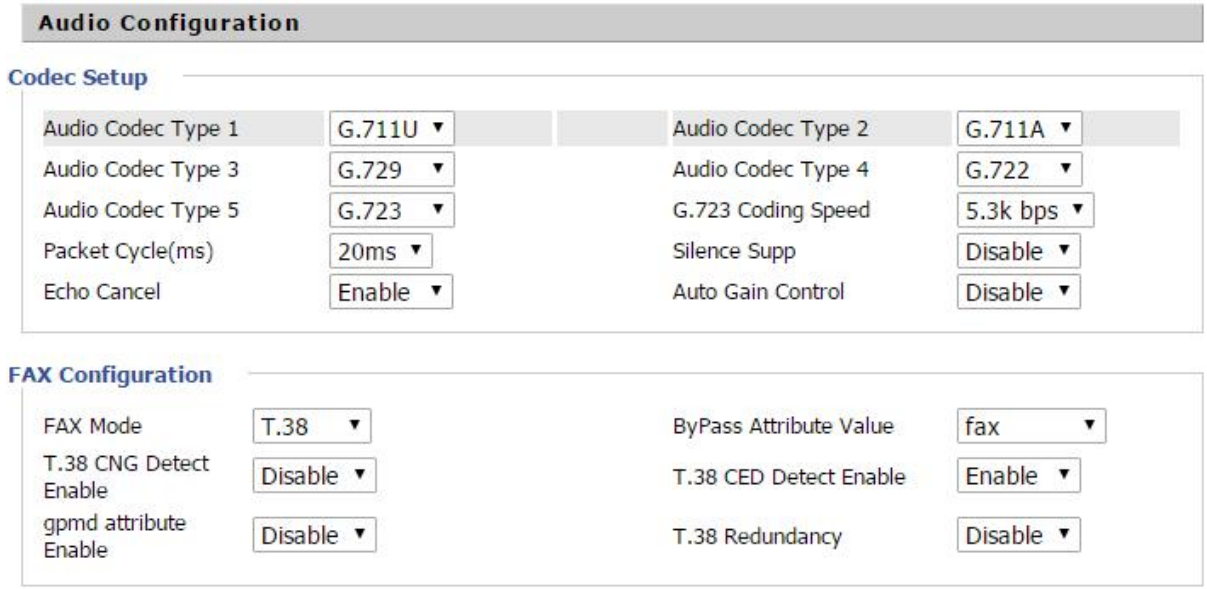


Field Name	Description
Line Enable	Enable/Disable the line.
Peer To Peer	Enable/Disable PEER to PEER. If enabled, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dialed line1.
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 49 Audio configuration

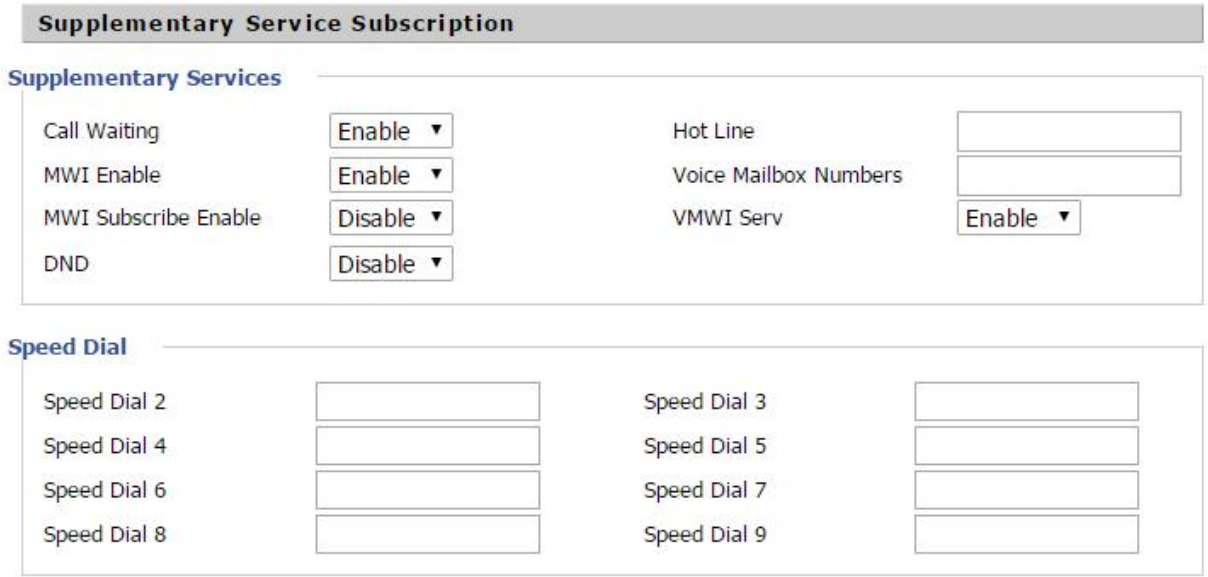


Audio Codec Type1	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type2	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type3	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type4	Choose the audio codec 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 50 Supplementary service

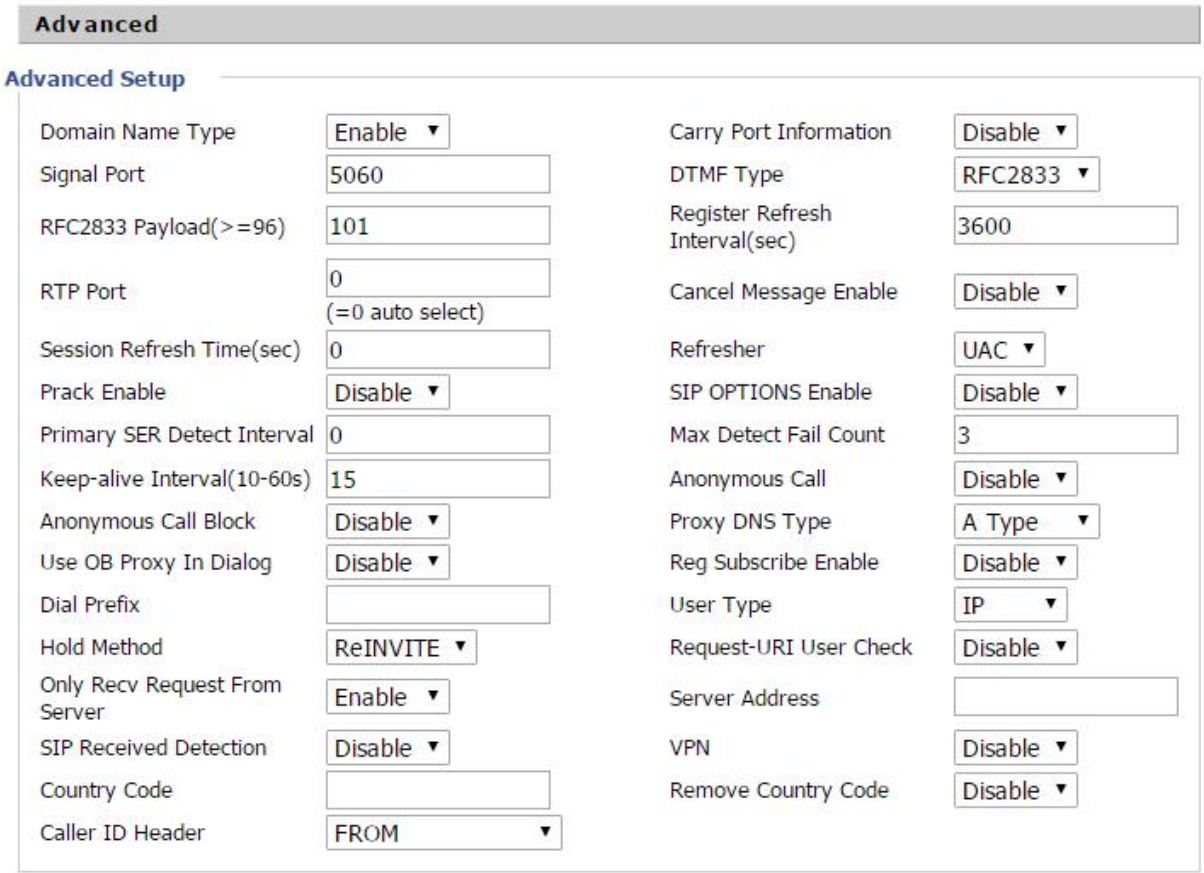


Field Name	Description
Call Waiting	Enable/Disable Call Waiting
Hot Line	Fill in the hotline number,Pickup handset or press hands-free or headset button, the device will dial out the hotline number automatically
MWI Enable	Enable/Disable MWI (message waiting indicate). If the user needs to user voice 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 51 Advanced



Field Name	Description
Domain Name Type	If or not use domain name in the SIP URI.
Carry Port Information	If or not carry port information in the SIP URI.
Signal Port	The local port of SIP protocol, default is 5060.
DTMF Type	Choose the DTMF type from Inbound, RFC2833 and SIP INFO.
RFC2833Payload(>=96)	User can use the default setting.
Register Refresh Interval	The interval between two normal Register messages. You can use the default setting.
RTP Port	Set the port to send RTP. The device will select one idle port for RTP if you set “0”; otherwise use the value which user sets.
Cancel Message Enable	When you set enable, an unregistered message will be sent before registration, while you set disable, unregistered message will not be sent before registration. You should set the option for different Proxy.
Session Refresh Time(sec)	Time interval between two sessions, you can use the default settings.
Refresher	Choose refresher from UAC and UAS.
Prack Enable	Enable/Disable prack.
SIP OPTIONS Enable	When you set enable, the device will send SIP-OPTION to the server, instead of sending periodic Hello message. The sending interval is Keep- alive interval.
Primary SER Detect Interval	Test interval of the primary server, the default value is 0, it represents disable.
Max Detect Fail Count	Interval of detection of the primary server fail; the default value is 3, it means that if detect 3 times fail; the device will no longer detect the primary server.
Keep-alive Interval(10-60s)	The interval that the device will send an empty packet to proxy.
Anonymous Call	Enable/Disable anonymous call.
Anonymous Call Block	Enable/Disable anonymous call block.
Proxy DNS Type	Set the DNS server type, choose from A type and DNS SRV.
Use OB Proxy In Dialog	If or not use OB Proxy In Dialog.
Reg Subscribe Enable	If enable, subscribing will be sent after registration message, if not enable, do not send subscription.

Dial Prefix	The number will be added before your telephone number when making calls.
User Type	Choose the User Type from IP and Phone.
Hold Method	Choose the Hold Method from ReINVITE and INFO.
Request-URI User Check	Enable/Disable the user request URI check.
Only Recv request from server	Enable/Disable the only receive request from server.
Server Address	The IP address of SIP server.
SIP Received Detection	Enable/Disable SIP Received Detection, if enable, use it to confirm the public network address of the device.

Preferences

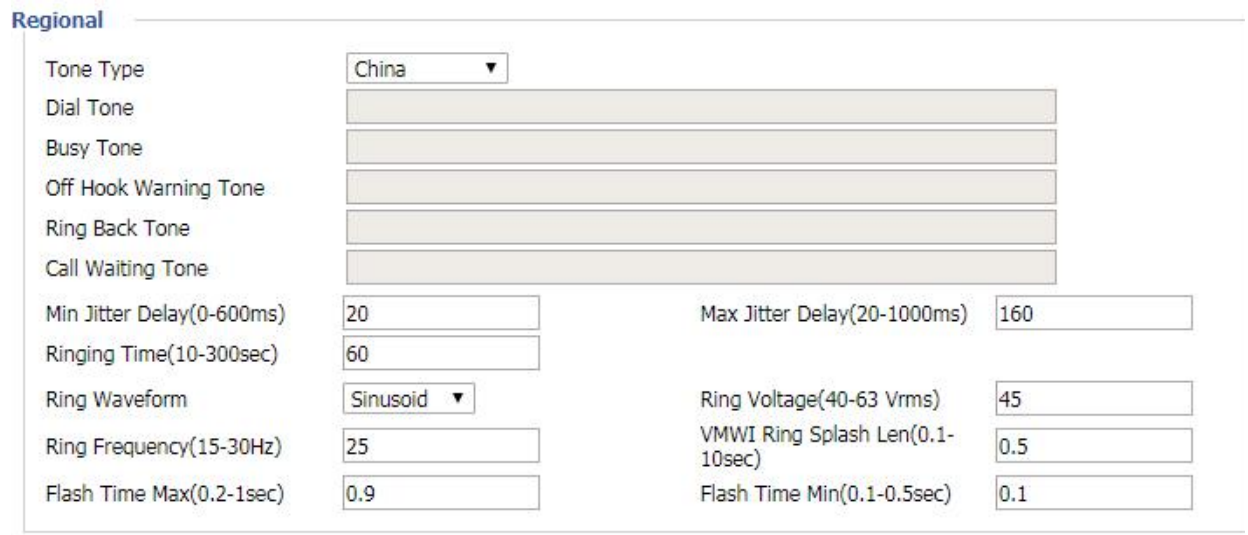
Volume Settings

Table 52 Volume settings

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

Regional

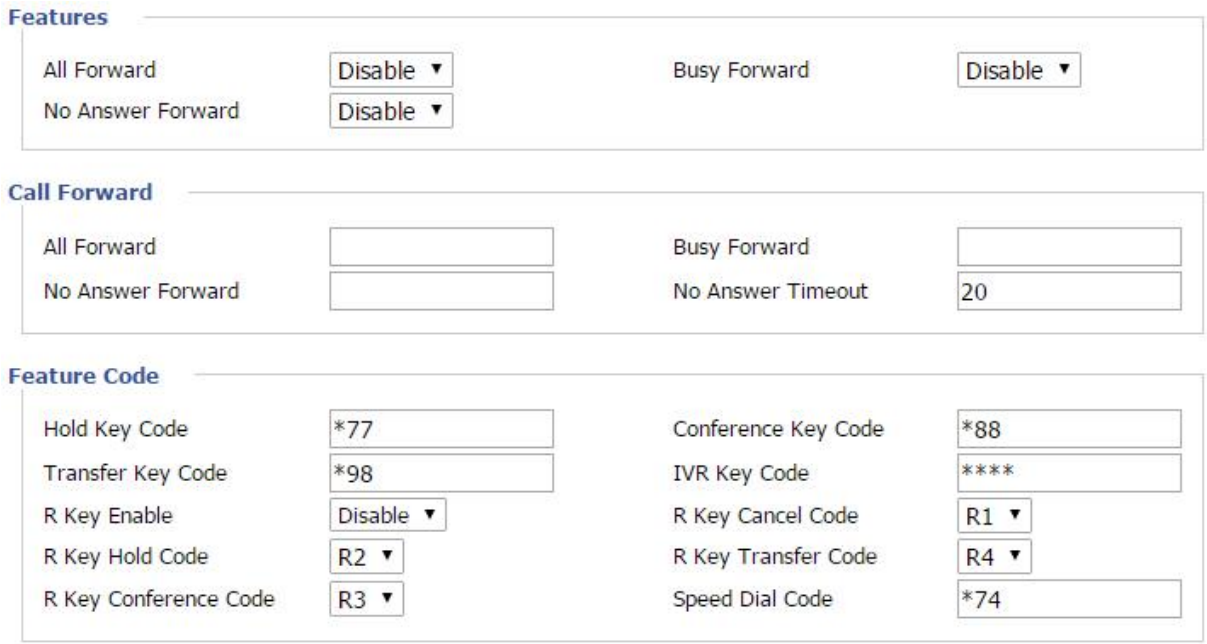
Table 53 Regional



Field Name	Description
Tone Type	Choose tone type form China, US, Hong Kong and so on
Dial Tone	Dial Tone
Busy Tone	Busy Tone
Off Hook Warning Tone	Off Hook warning tone
Ring Back Tone	Ring back tone
Call Waiting Tone	Call waiting tone
Min Jitter Delay	The Min value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Max Jitter Delay	The Max value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Ringing Time	How long the device 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 54 Features and call forward

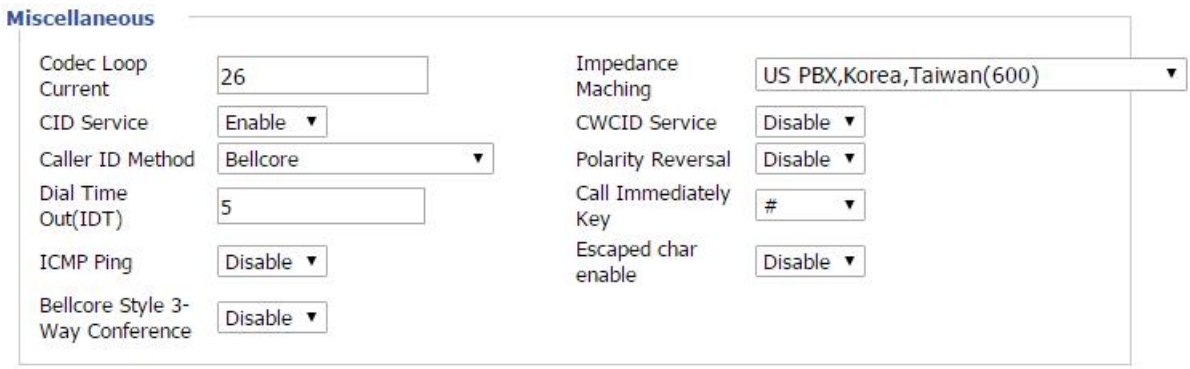


Field Name		Description
Features	All Forward	Enable/Disable forward all calls
	Busy Forward	Enable/Disable busy forward.
	No Answer Forward	Enable/Disable no answer forward.
Call Forward	All Forward	Set the target phone number for all forward. The device will forward all calls to the phone number immediately 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.
	Speed Dial Code	Speed dial code, default is *74.

Miscellaneous

Table 55 Miscellaneous



Field Name	Description
Codec Loop Current	Set off-hook loop current, default is 26.
Impedance Maching	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 #.

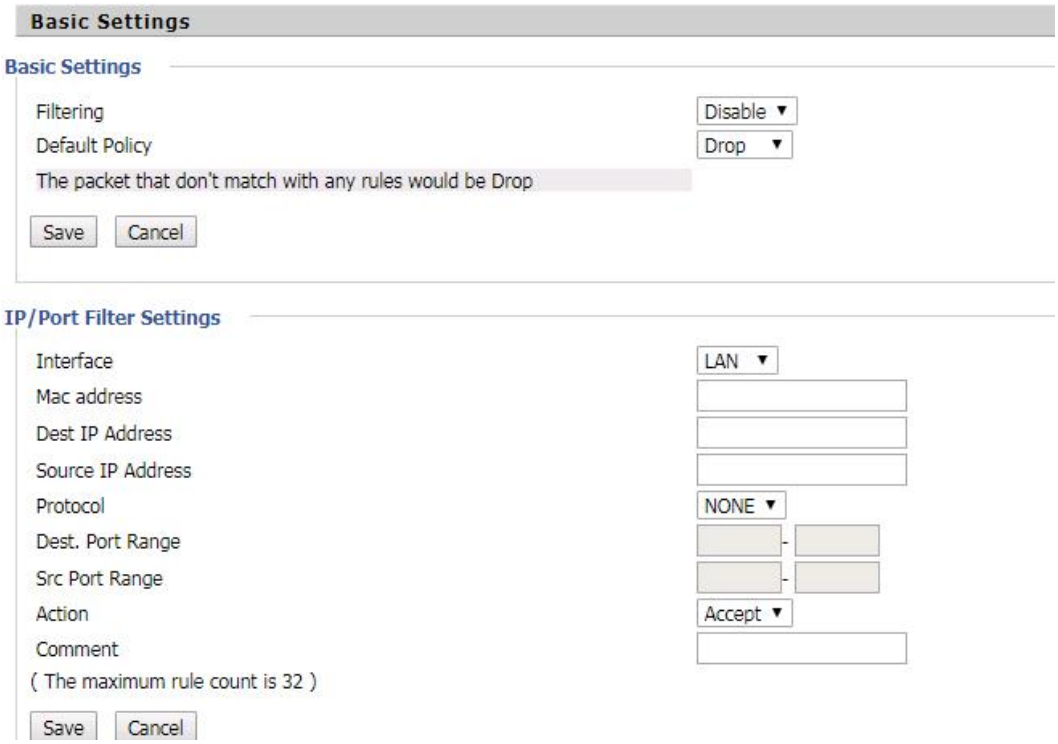
FXS2

The settings of FXS2 are the same as FXS1. See FXS1 on page 74.

Security

Filtering Setting

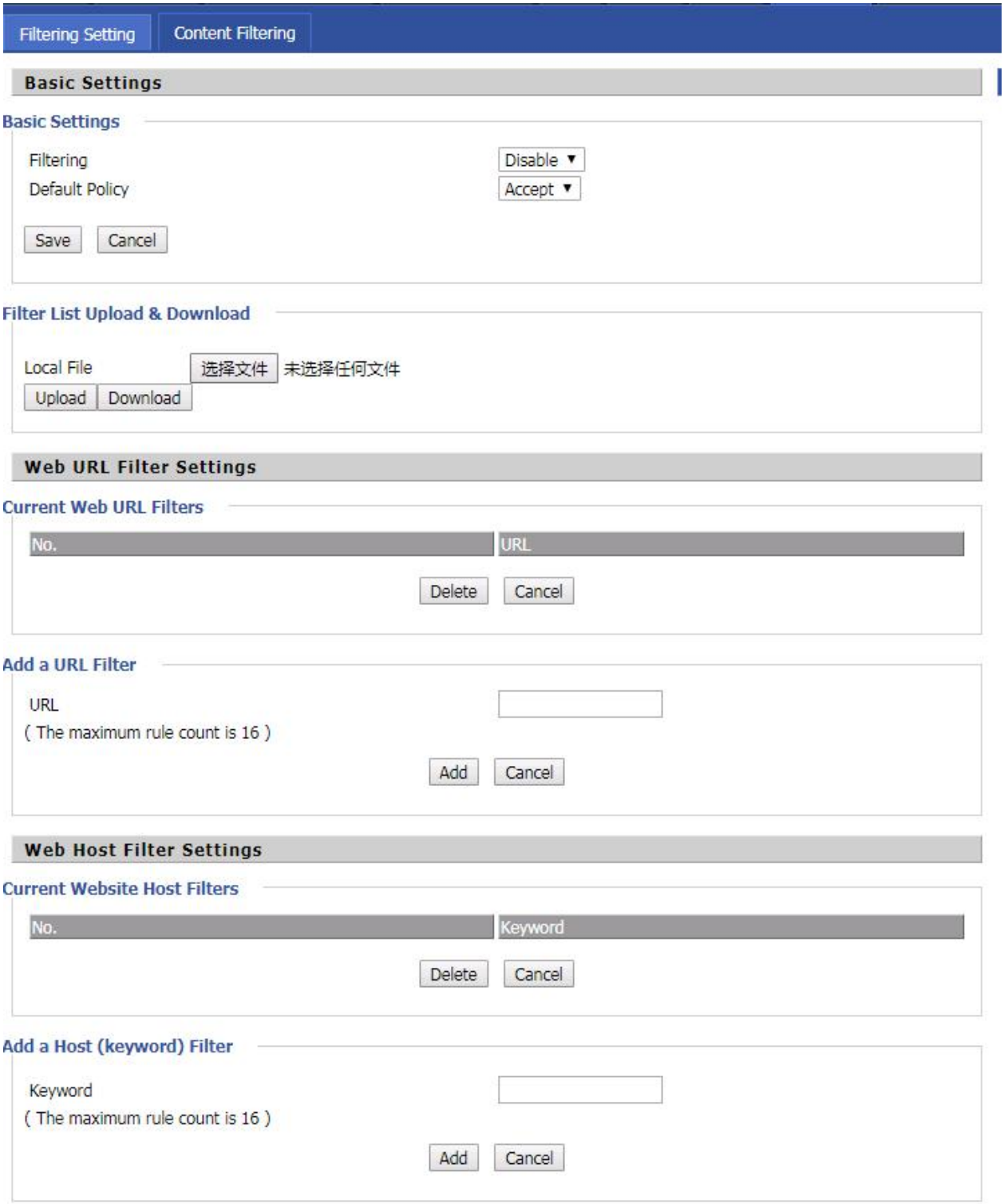
Table 56 Filtering setting



Field Name	Description
Filtering	Enable/Disable filter function
Default Policy	Choose to drop or accept filtered MAC addresses
Mac address	Add the Mac address filtering
Dest IP address	Destination 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 57 Content filtering

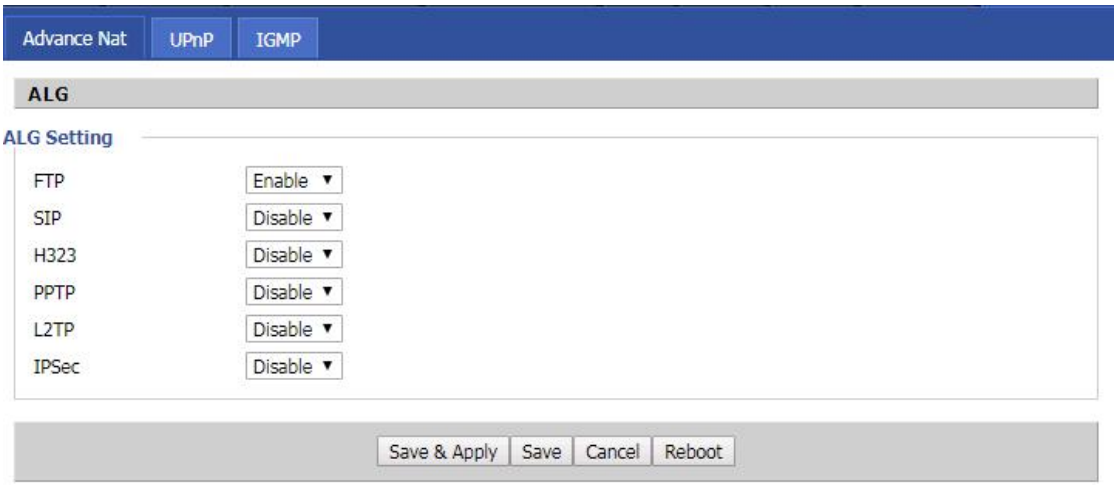


Field Name	Description
Filtering	Enable/Disable content Filtering
Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL Filters	List the URL filtering rules that already existed (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules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

Table58 advance NAT



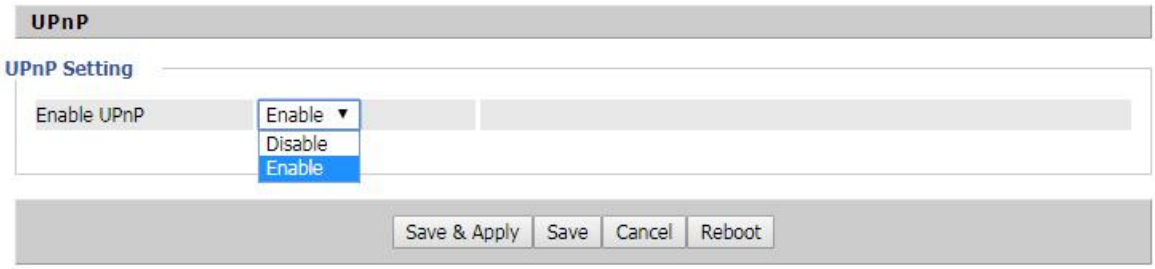
Description
Enable/Disable these function(FTP/SIP/H323/PPTP/L2TP/IPSec).

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 59 UPnP



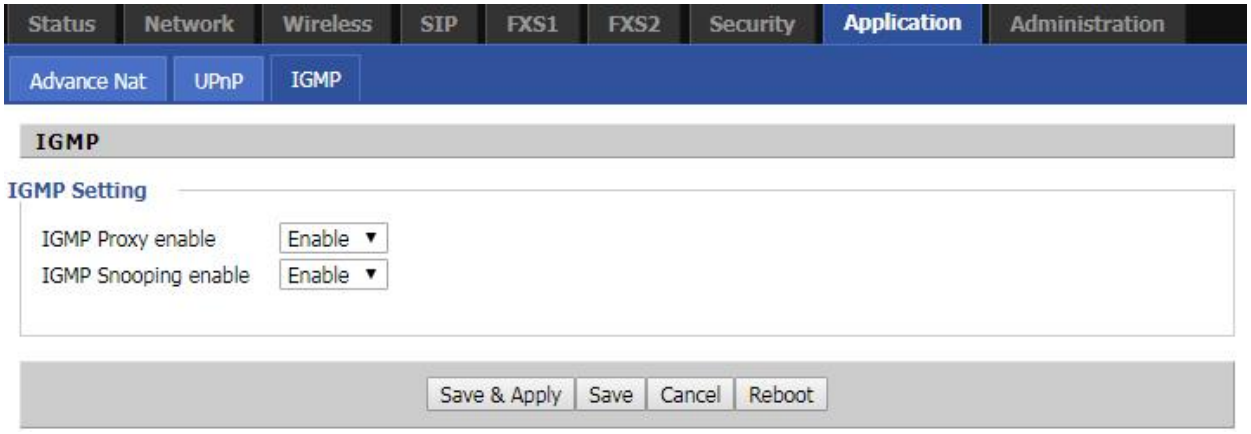
Field Name	Description
UPnP enable	Enable/Disable UPnP function.

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 60 IGMP



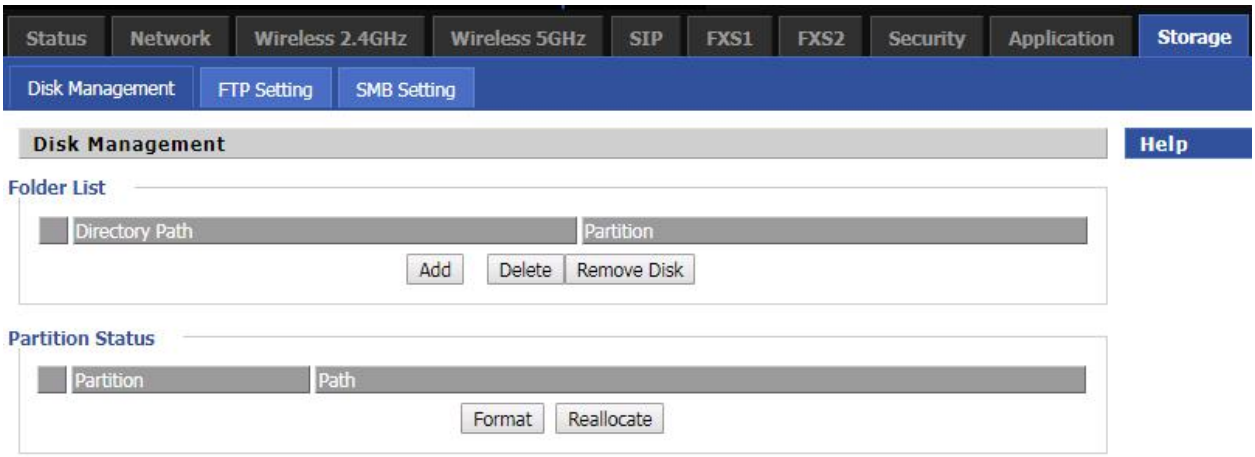
Field Name	Description
IGMP Proxy enable	Enable/Disable IGMP Proxy function.
IGMP Snooping enable enable	Enable/Disable IGMP Snooping function.

Storage

Disk Management

This page is used to manage the USB storage device.

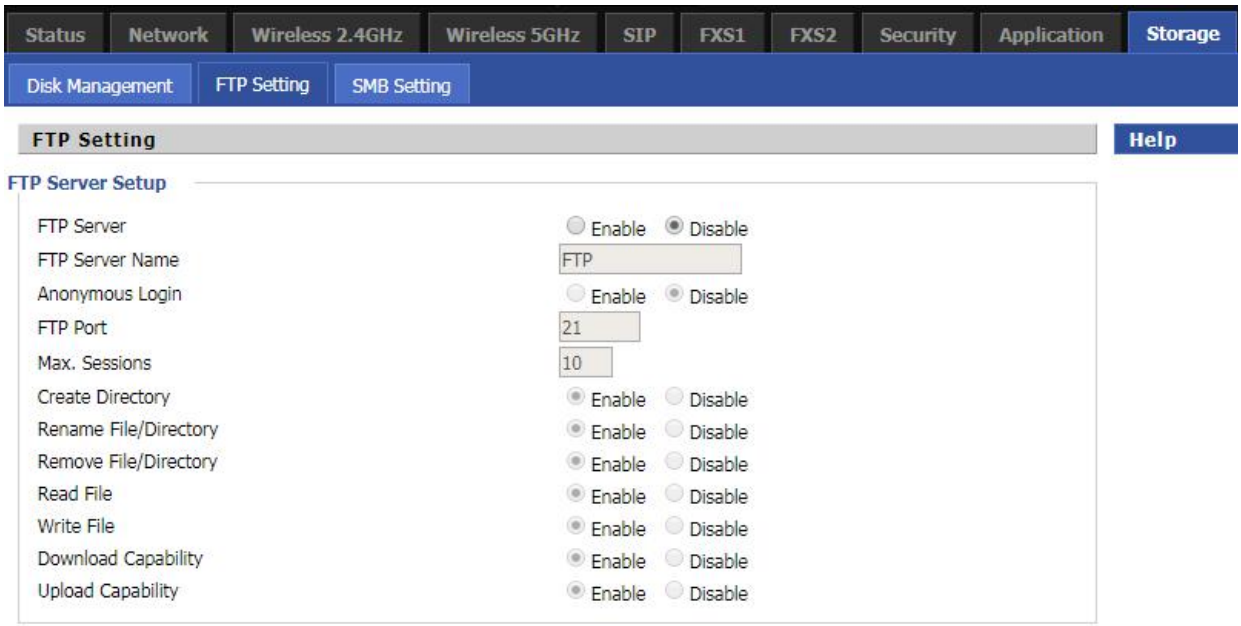
Table 61 Disk Management



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	Reset the USB storage device

FTP Setting

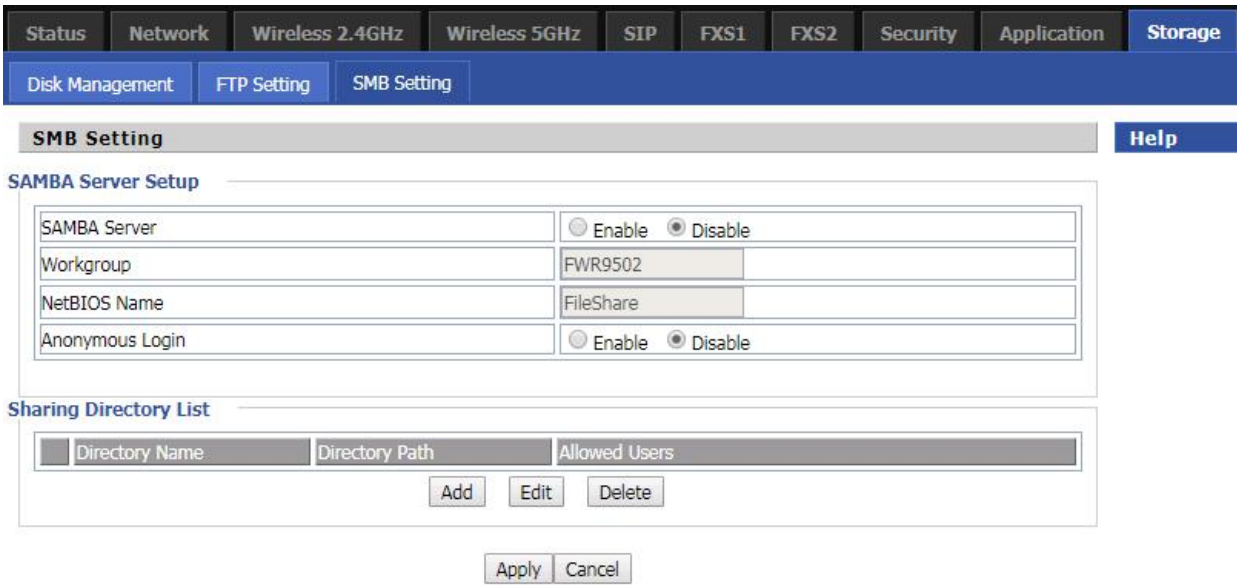
Table 62 FTP Setting



Field Name	Description
FTP Server	Enable/Disable 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	Enable/Disable create directory
Rename File/Directory	Enable/Disable rename file/directory
Remove File/Directory	Enable/Disable transfer of files/directories
Read File	Enable/Disable read files
Write File	Enable/Disable write files
Download Capability	Enable/Disable download capability function.
Upload Capability	Enable/Disable upload capability function

Smb Setting

Table 63 Smb setting



Field Name	Description
SAMBA Server	Enable/Disable SAMBA server
Workgroup	Enter 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
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

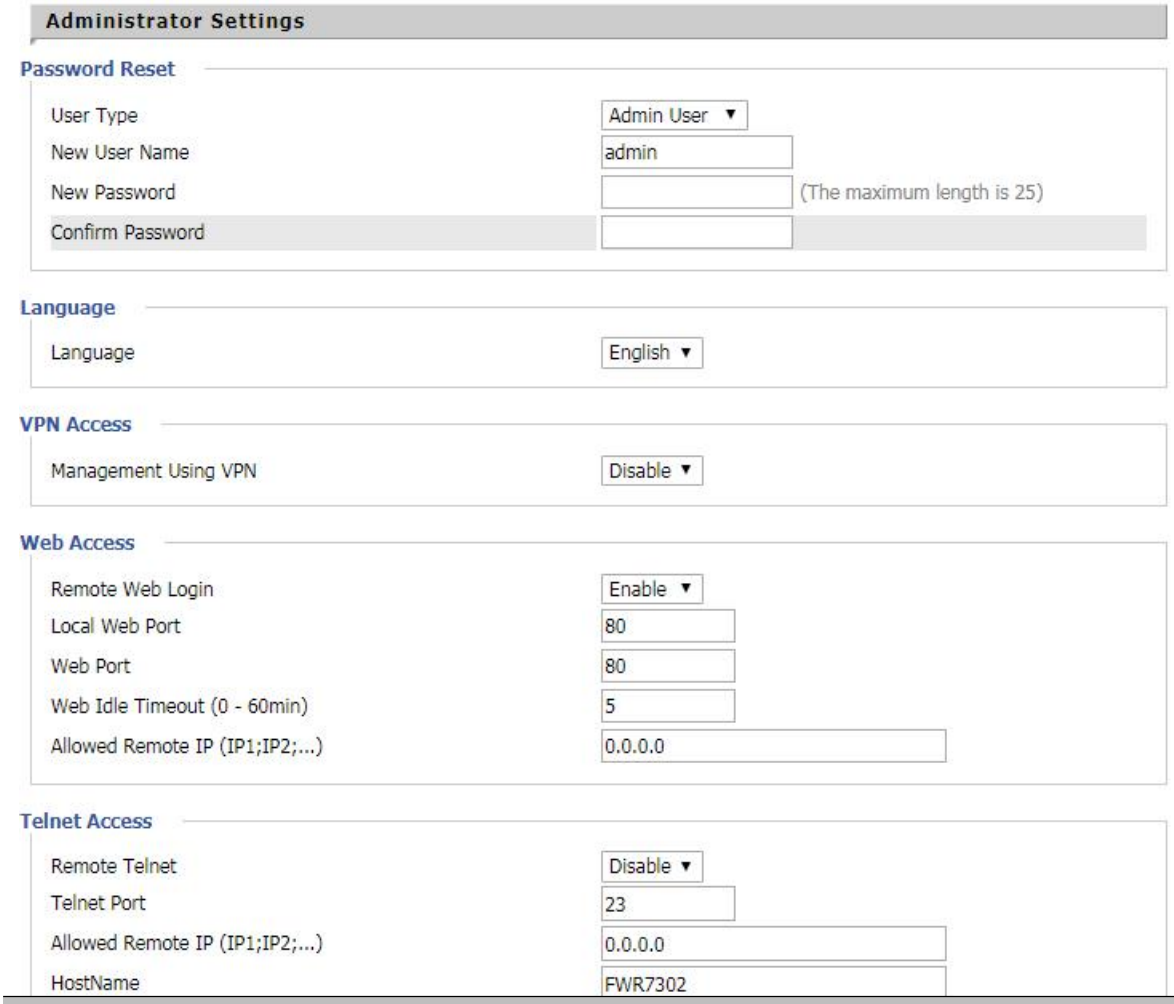
Save config file

Table 64 Save Config File

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

Administrator settings

Table 65 Administrator settings

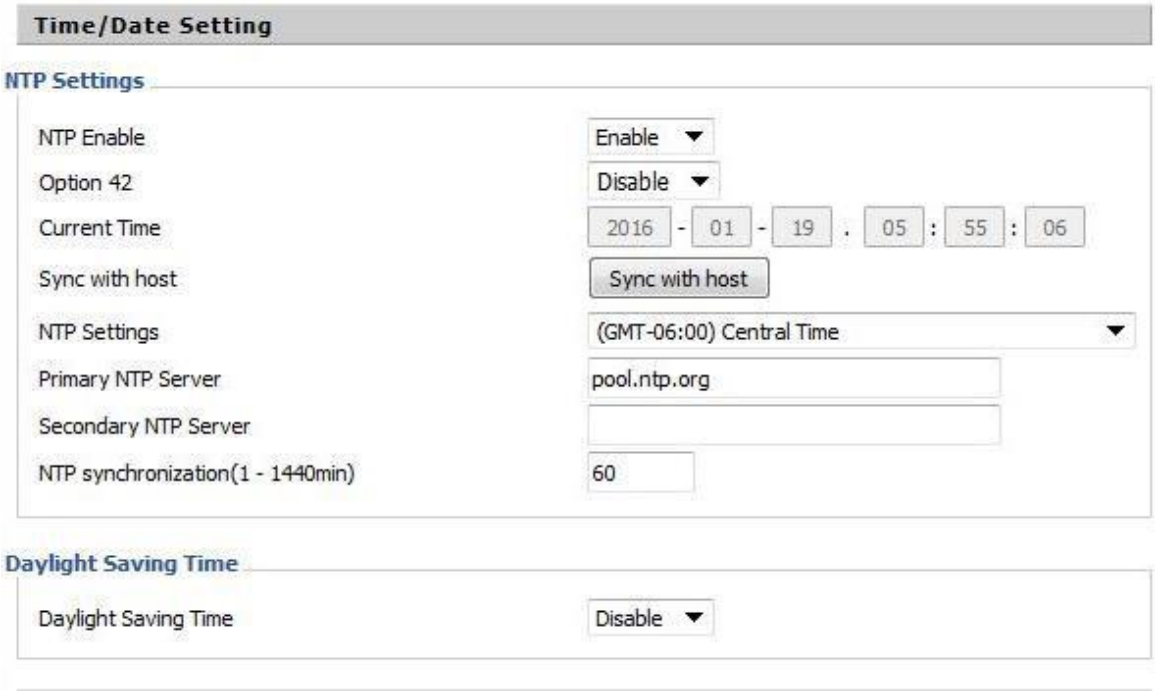


Field Name	Description
User type	Choose the user type from admin user and normal user and basic user
New User Name	You can modify the user name, set up a new user name
New Password	Input the new password
Confirm Password	Input the new password again
Language	Select the language for the web, the device support Chinese, English, and Spanish and so on
Remote Web Login	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 66 NTP settings

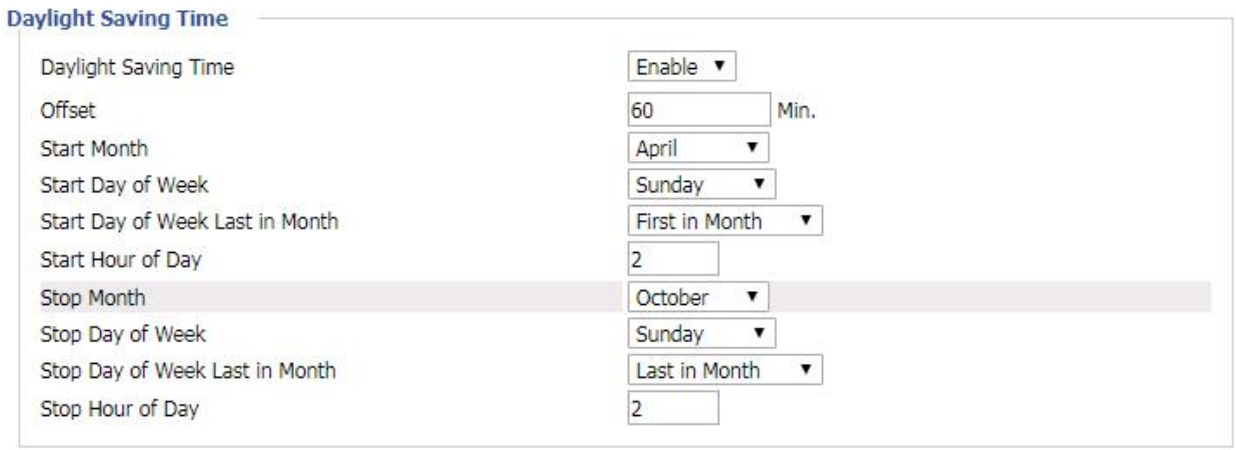


Field Name	Description
NTP Enable	Enable/Disable NTP
Option 42	Enable/Disable DHCP option 42. This option specifies a list of the NTP servers available to the client by IP address
Current Time	Display current time
NTP Settings	Setting the Time Zone
Primary NTP Server	Primary NTP server's IP address or 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 67 Daylight Saving Time



Procedure

Step 1. Enable Daylight Savings Time.

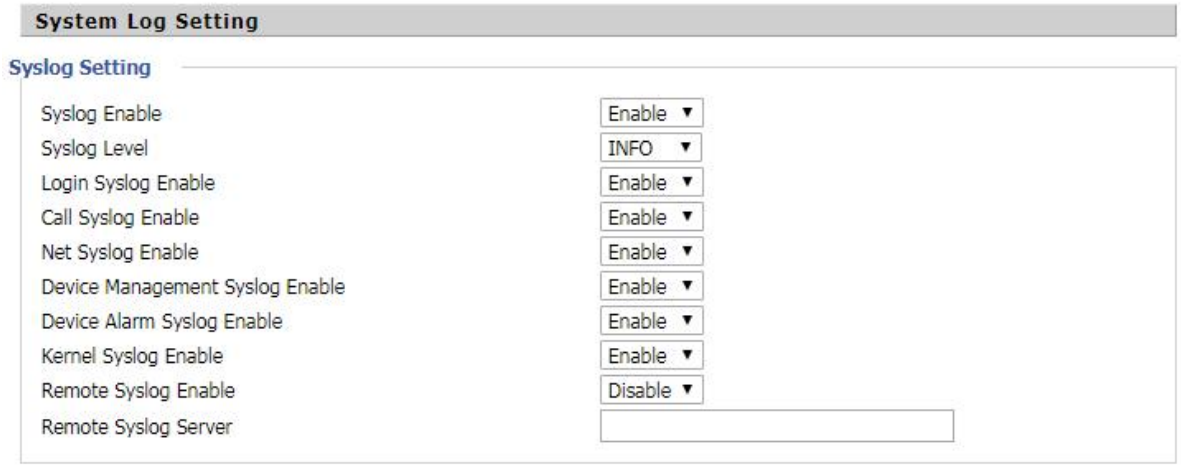
Step 2. Set value of offset for Daylight Savings Time

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 68 System log Setting



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 69 Factory Defaults Setting

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

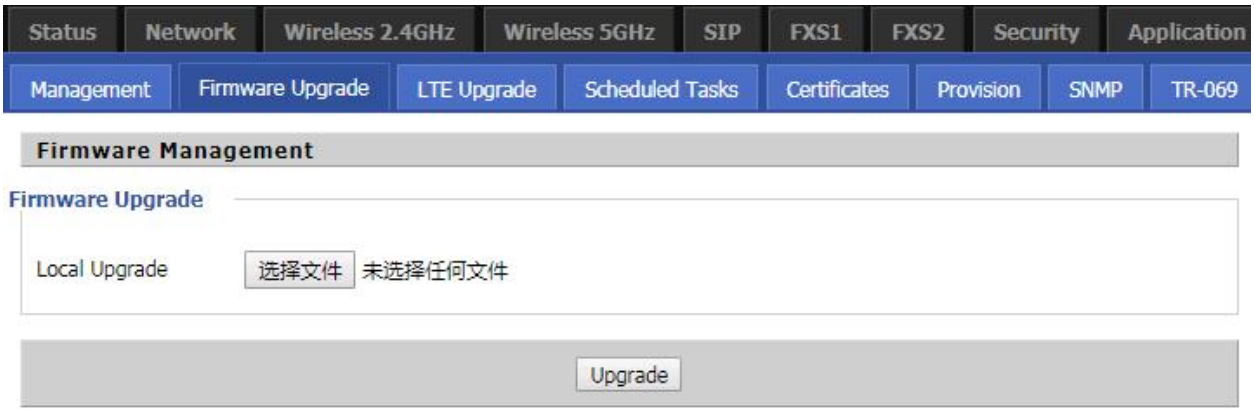
Factory Defaults

Table 70 Factory Defaults

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

Firmware Upgrade

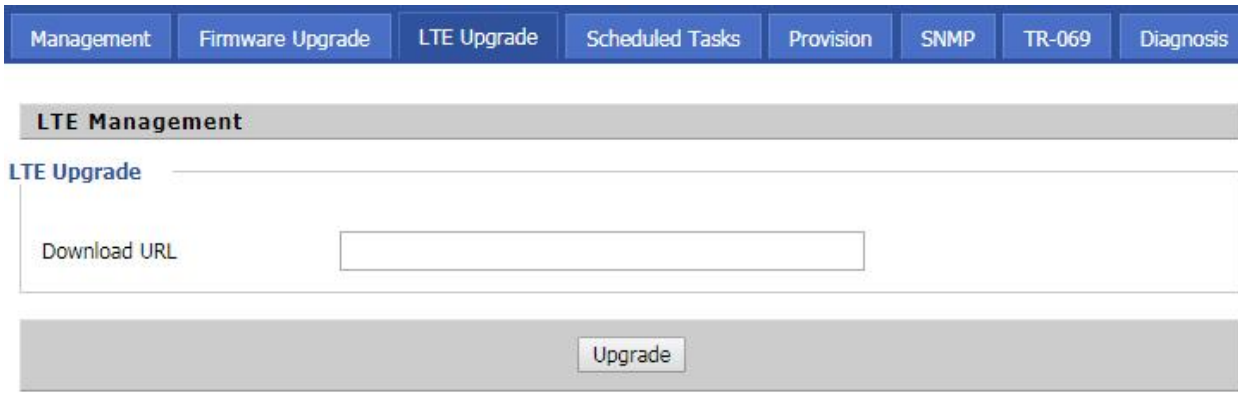
Table 71 Firmware upgrade



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

LTE Upgrade

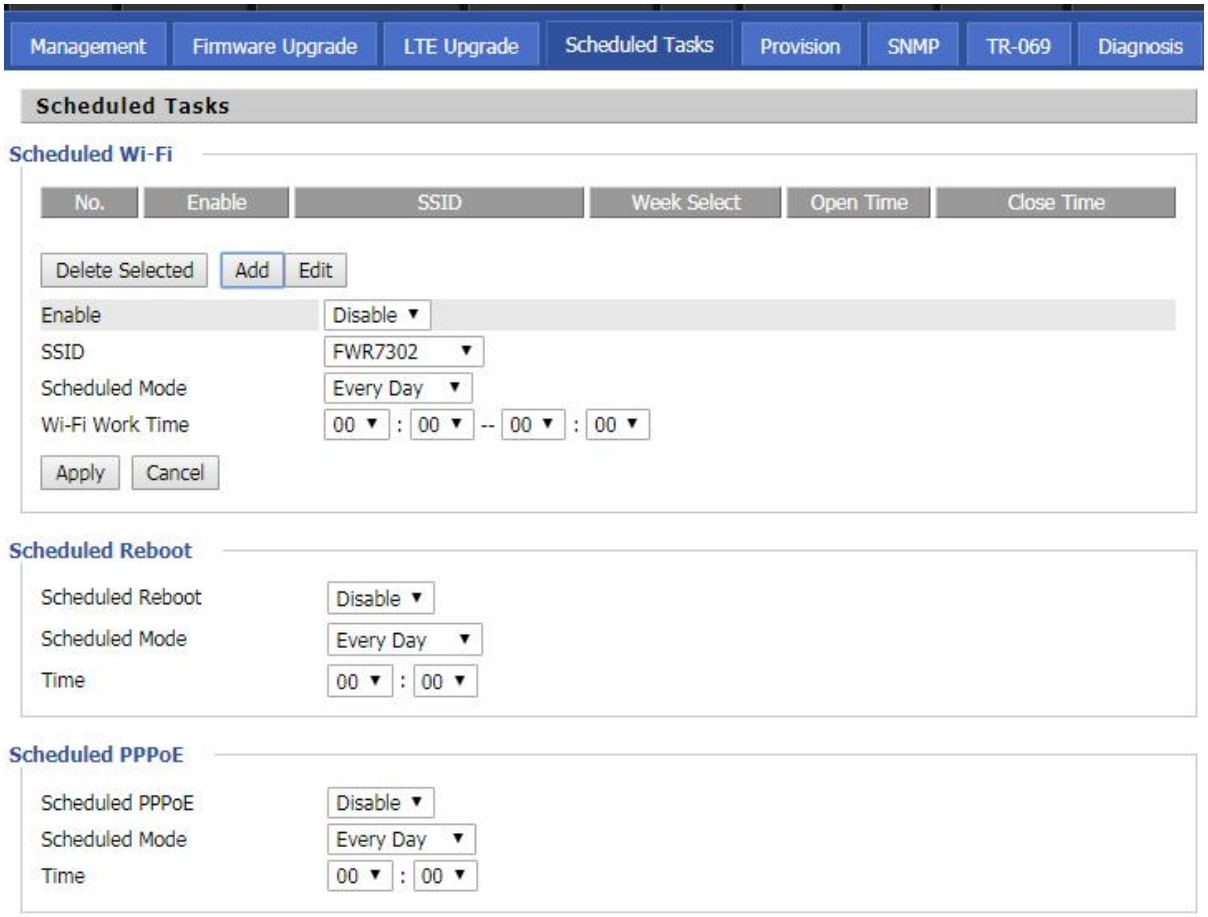
Table 72 LTE upgrade



Description
You can fill in LTE download URL, upgrade LTE

Scheduled Tasks

Table 73 Scheduled Tasks



Field Name	Description
Scheduled Wi-Fi	
Enable	Enable / Disable Timed WIFI
SSID	This is not optional
Scheduled Mode	Choose work mode, weekly / days
Wi-Fi work time	Set the WIFI duty cycle
Apply and Cancel	After modifying the parameters, select Apply, or Cancel
Scheduled Reboot	
Scheduled Reboot	Enable / disable scheduled reboot
Scheduled Mode	Choose work mode every day / week
Time	Set the time for scheduled reboot
Scheduled PPPoE	
Scheduled PPPoE	Enable / disable restart PPPoE
Scheduled Mode	Choose work mode every day / week
Time	Set the time for scheduled PPPoE

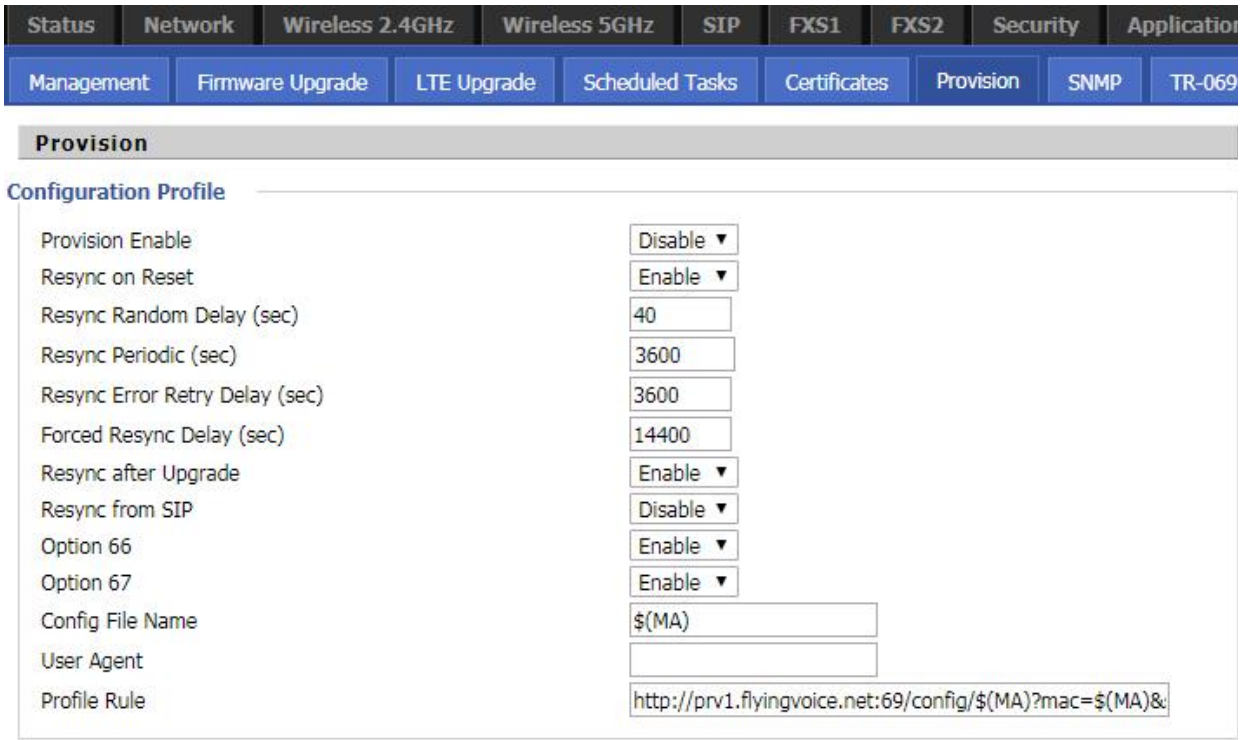
Provision

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 74 Provision



Field Name	Description
Provision Enable	Enable provision or not.
Resync on Reset	Enable resync after restart or not
Resync Random Delay(sec)	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 Retry Delay” time, default is 3600s.
Resync Error Retry	Set the periodic time for resync, default is 3600s.
Forced Resync Delay(sec)	If it’s time to resync, but the device is busy now, in this case,the router will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over, the router will forced to resync.
Resync After Upgrade	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 realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.

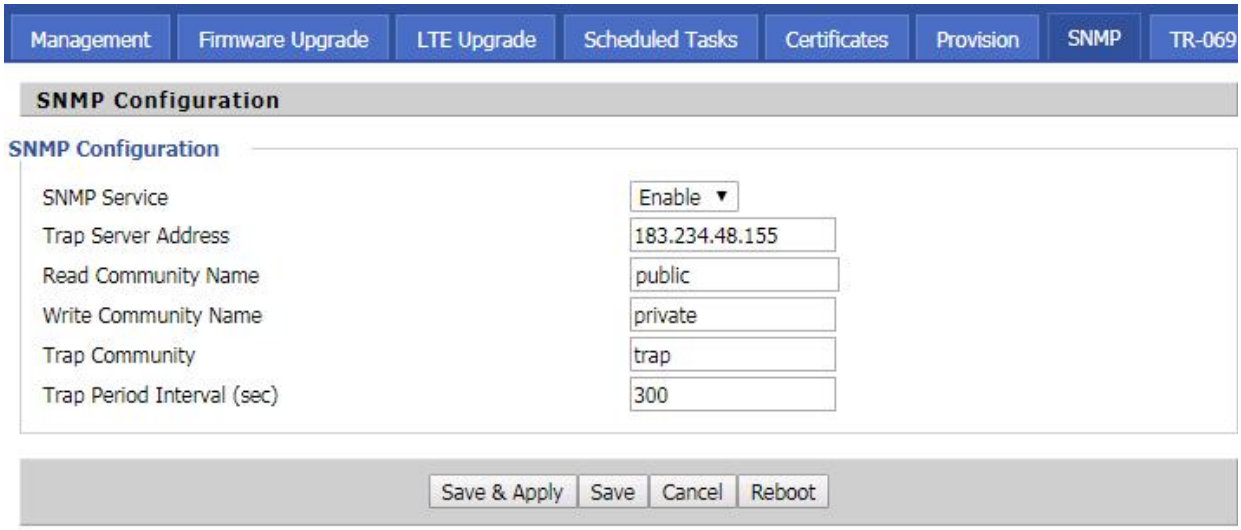
Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.
Profile Rule	URL of profile provision file Note that the specified file path is relative to the TFTP server’s virtual root directory.

Table 75 Firmware Upgrade

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 76 SNMP



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 via 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

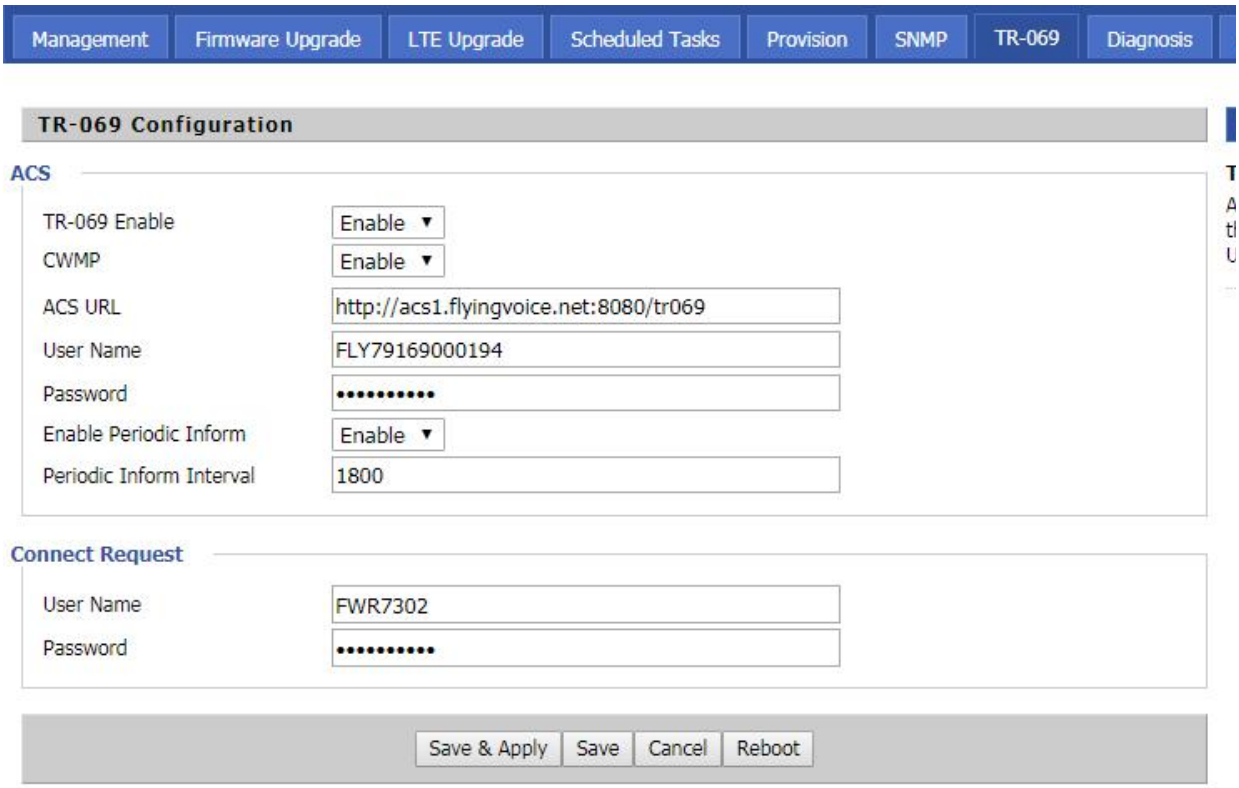
TR-069

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 77 TR069



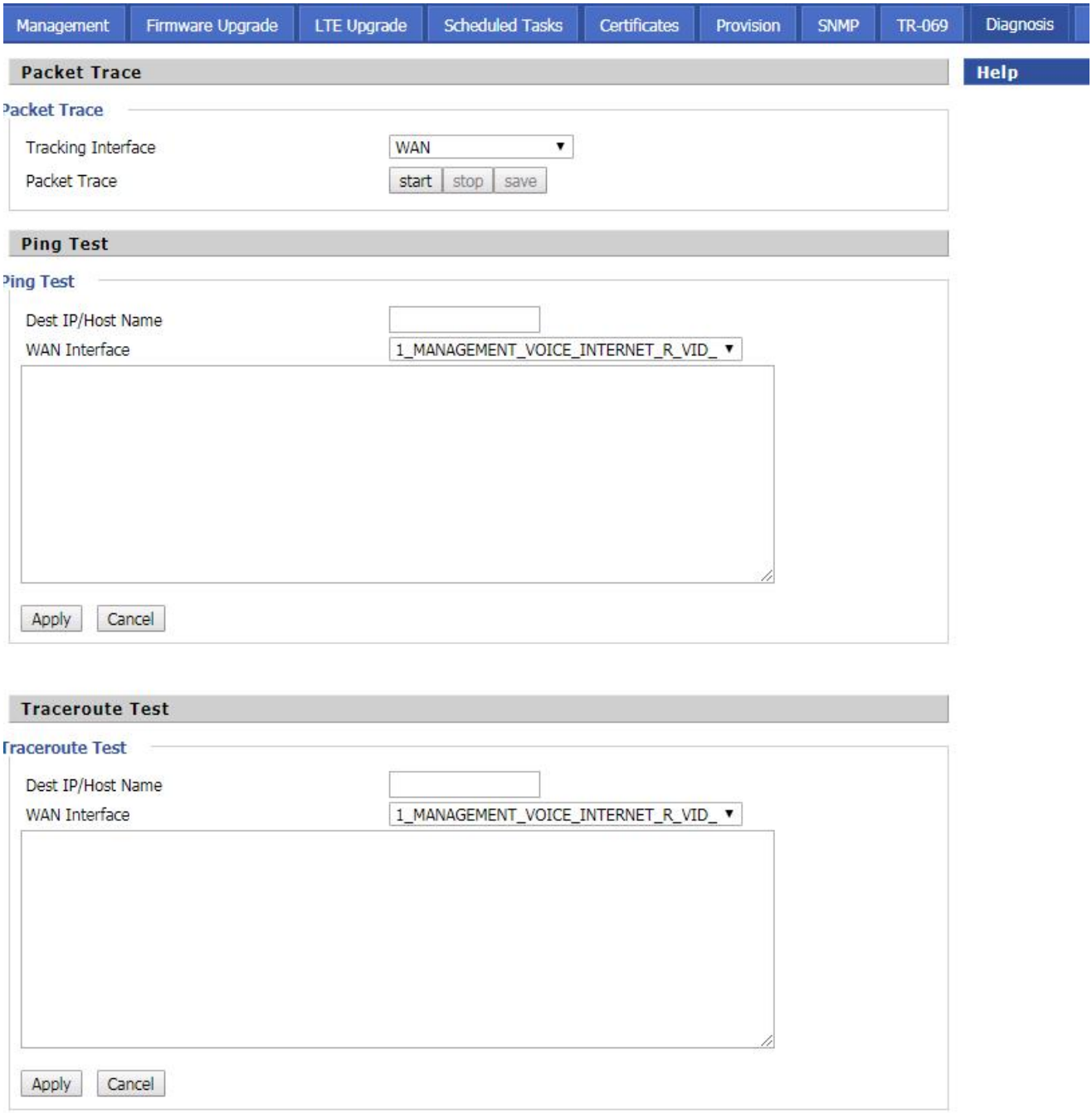
Field Name	Description
ACS parameters	
TR069 Enable	Enable or Disable TR069
CWMP	Enable or Disable CWMP
ACS URL	ACS URL address
User Name	ACS username
Password	ACS password

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 78 Diagnosis



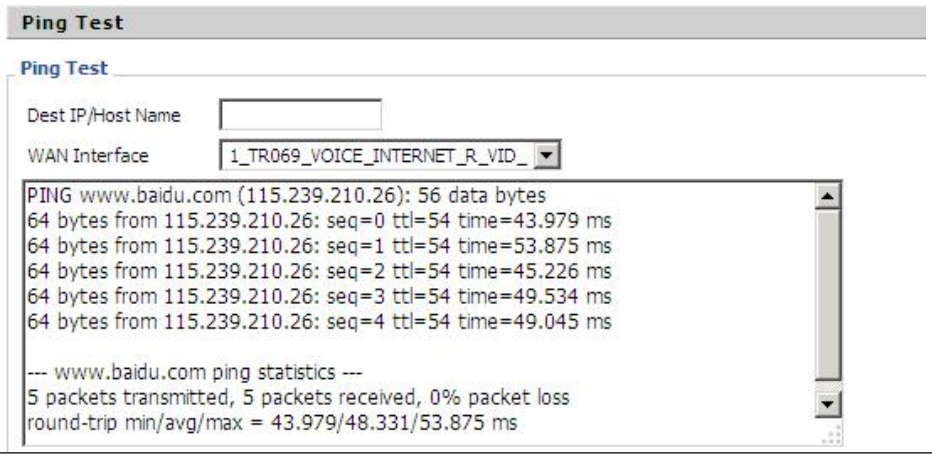
Description

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.

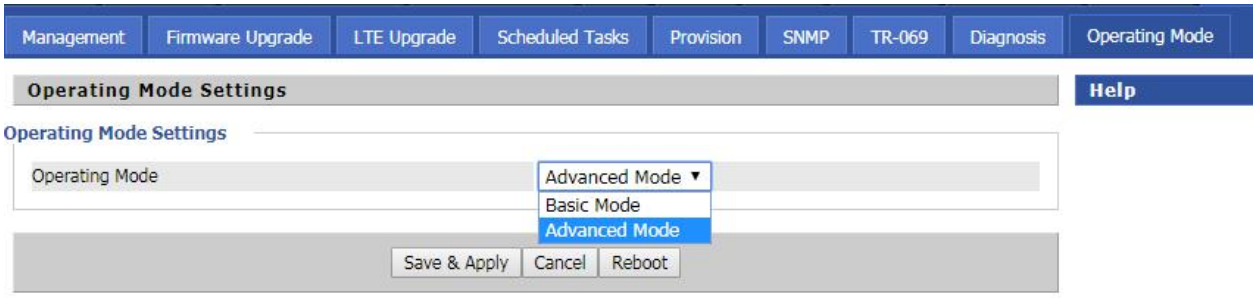


3. Traceroute Test

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

Operating Mode

Table 79 Operating mode



Description
Choose the Operation Mode as Basic Mode or Advanced Mode.

System Log

Table 80 System log

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

Logout

Table 81 Logout

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

Reboot

Press the

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

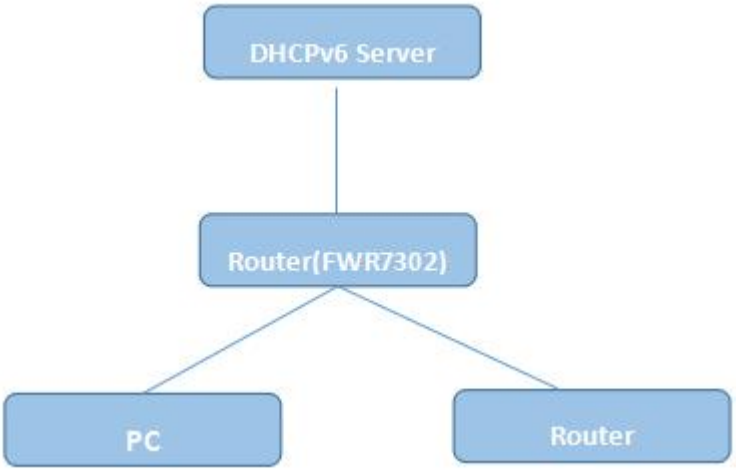
Introduction

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 82 I Pv6 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

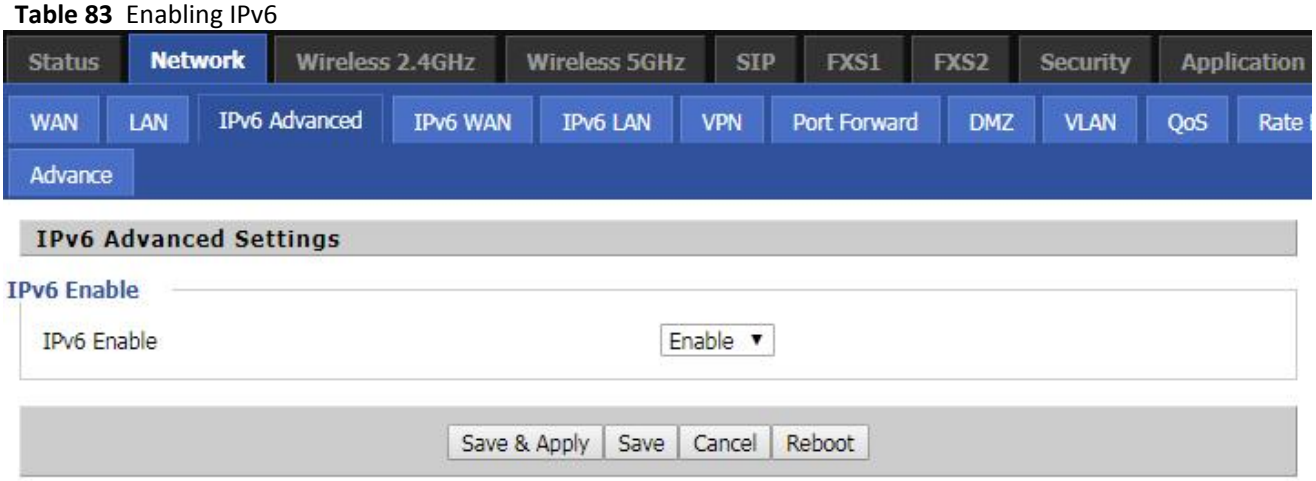
To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

Table 83 Enabling IPv6

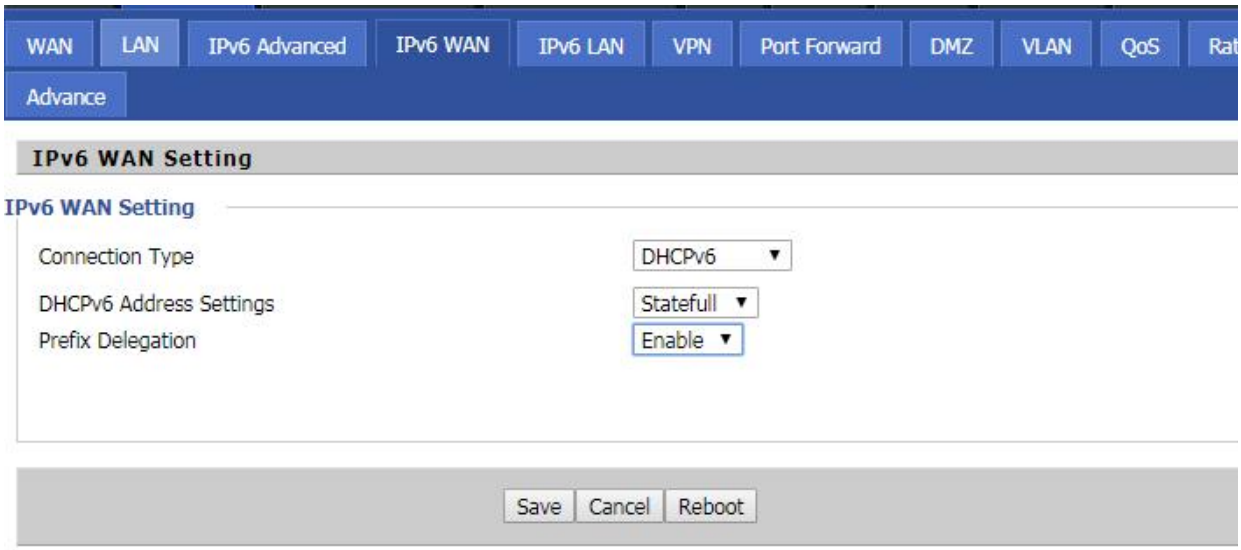


Configuring IPv6

Configuring Statefull IPv6

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

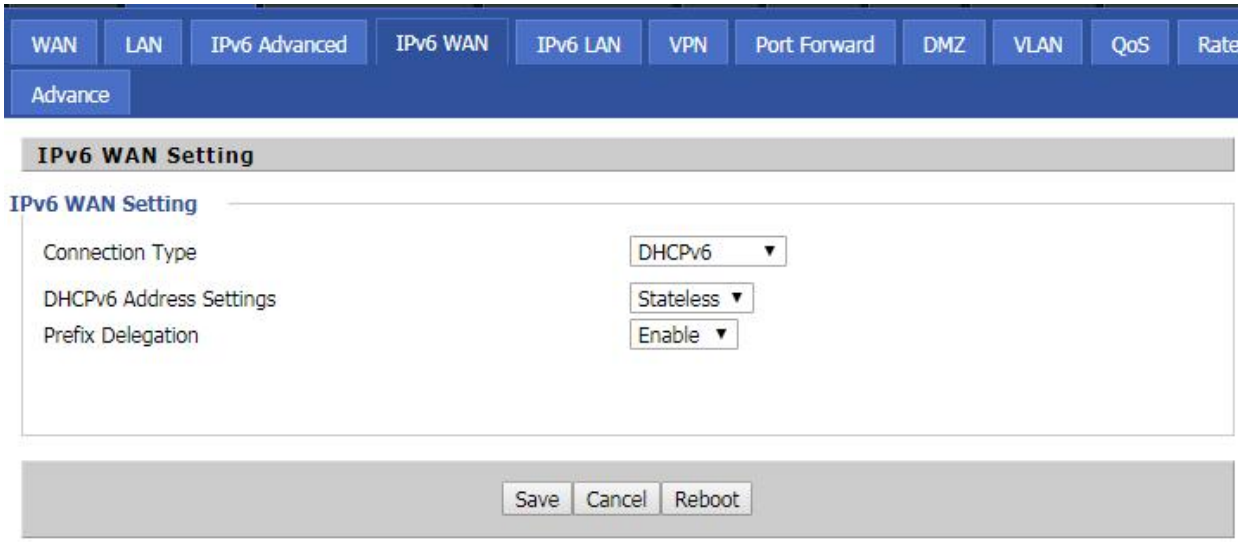
Table 84 Configuring Statefull IPv6



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

Configuring Stateless IPv6

Table 85 Configuring Stateless IPv6

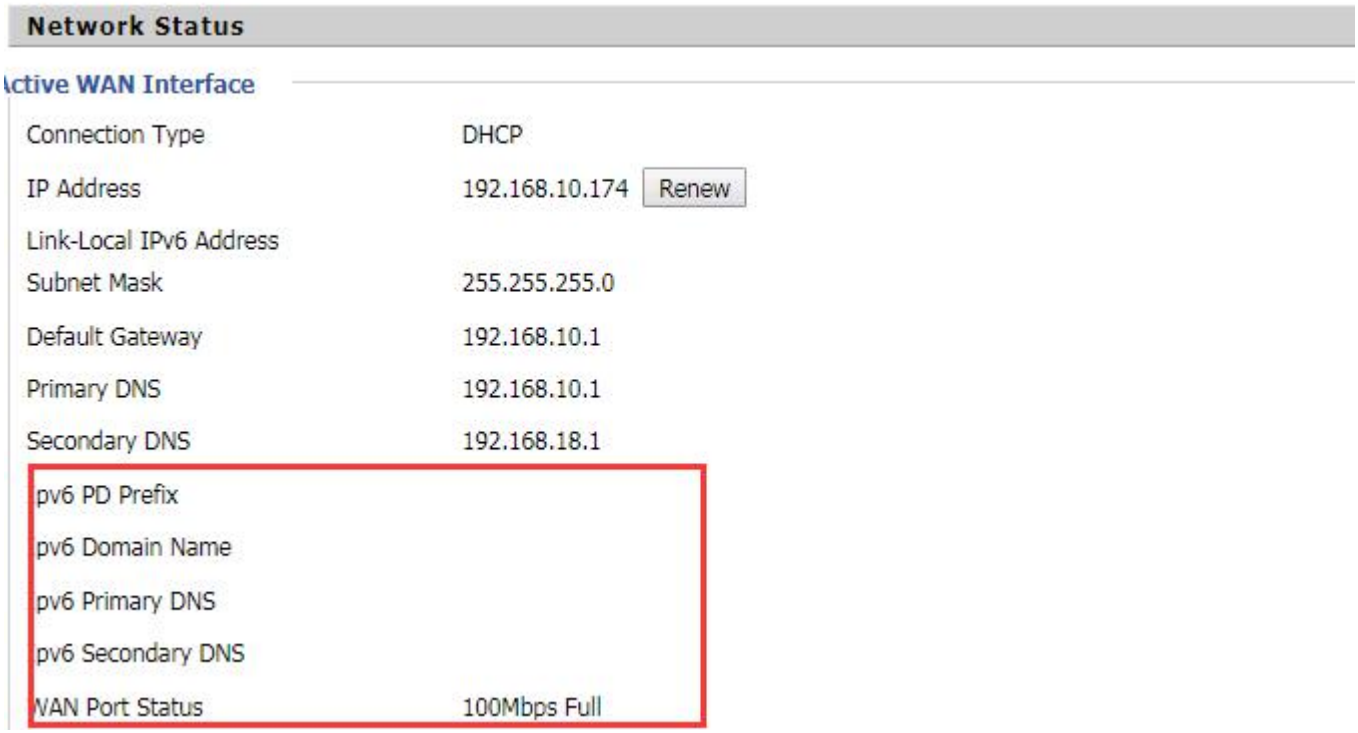


Field Name	Description
Connection Type	Select connection type
DHCPv6 Address Settings	Set it to stateless mode
Prefix Delegation	Select Enable

Viewing WAN port status

To view the status of WAN port:

Navigate to Status page.



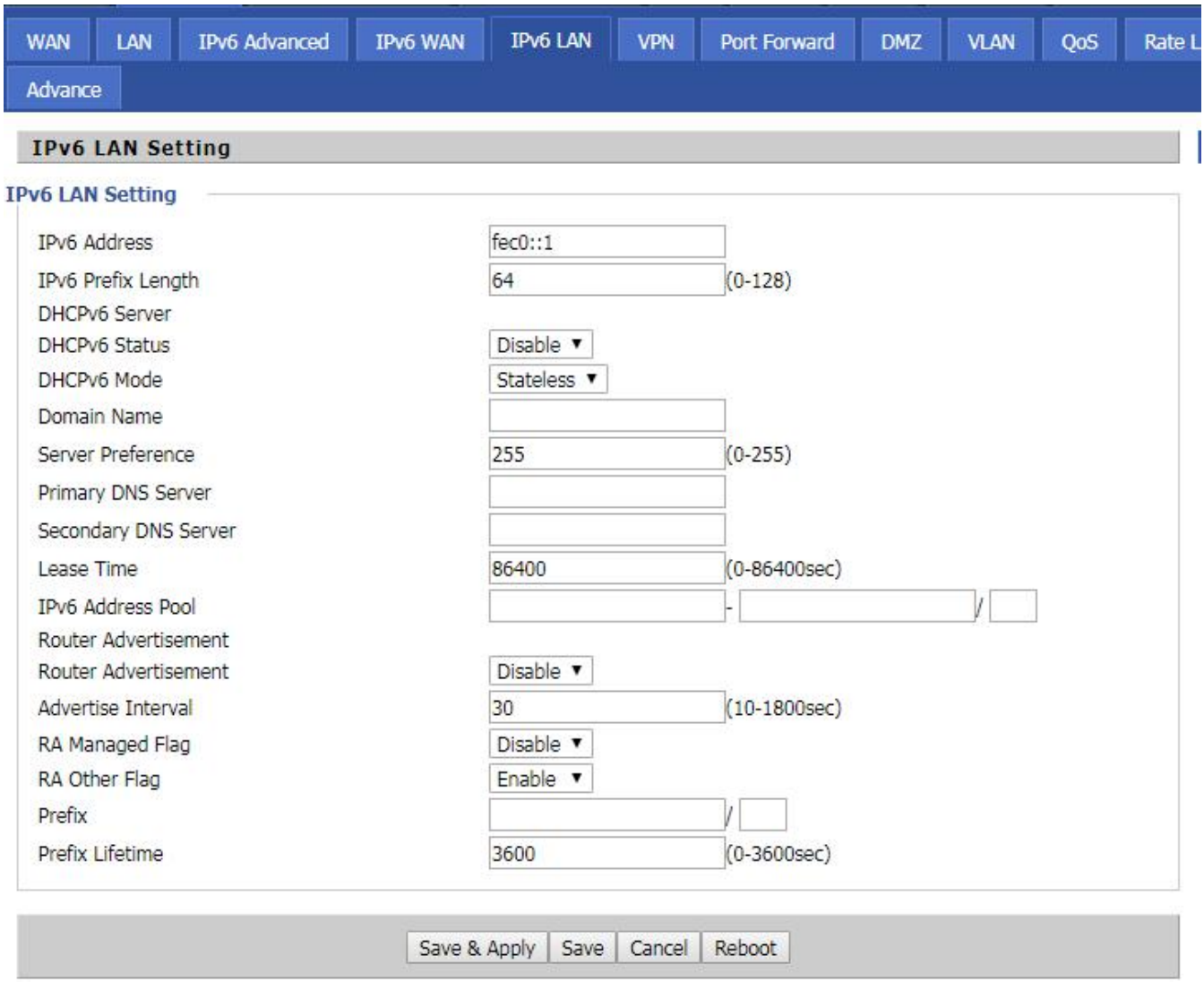
IPv6 DHCP configuration for LAN/WLAN clients

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:



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

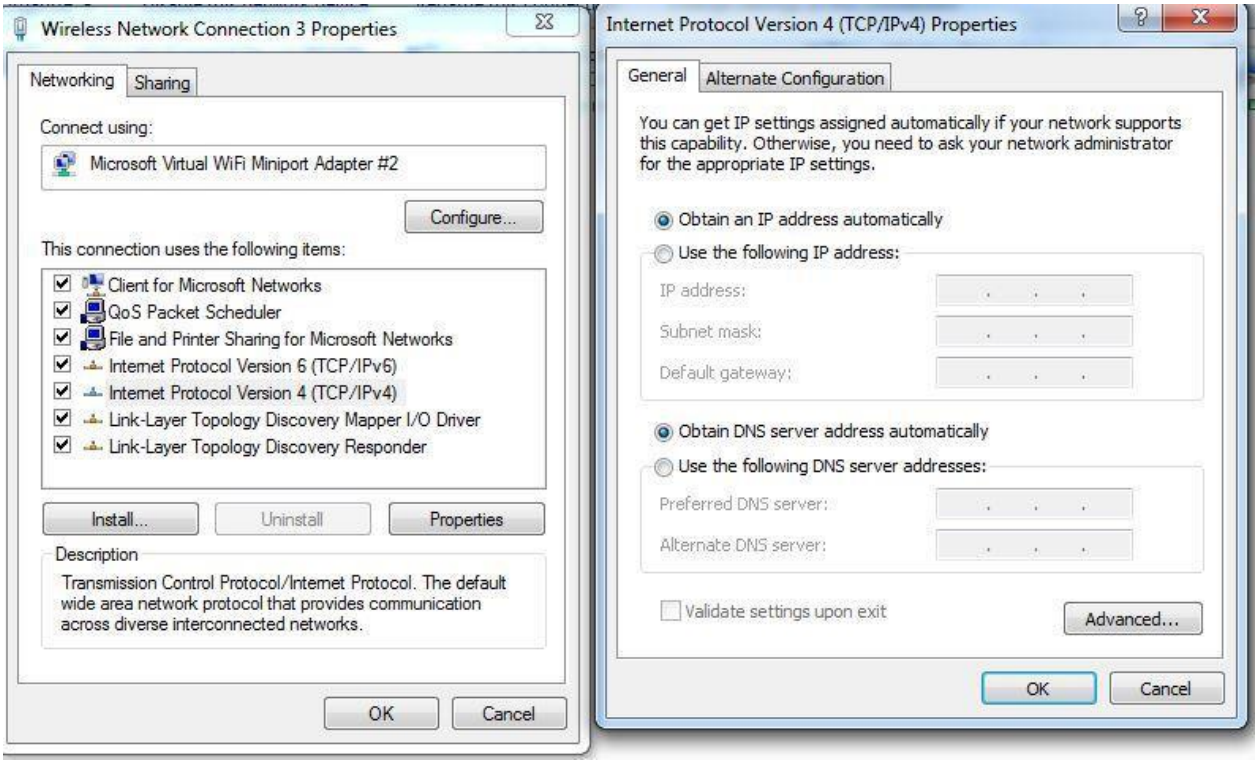
Follow the below process to set your PC to get an IP address automatically:

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”.



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 Google
- 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.