FLYINGVOICE
VoIP & VoWLAN Solutions


# User Manual

FTA1101

# Contents

# Table

# About This User Guide

FTA1101, which has one FXS port , one LAN port and one WAN port, is one of the most popular VoIP ATAs researched and produced by FlyingVoice. This product can not only provide one SIP lines for users to make calls, but also it is a wire-speed NAT router, make you enjoy easy network atmosphere. What's more, FTA1101 support T.38 real time FAX and T.30 FAX with G.711.FTA1101 is a stand-alone device, which requires no PC to make Internet calls. This ATA 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.The Flyingvoice powerful VoIP Wireless Router FTA1101, Users can also take FTA1101 as a FTP server, to share LAN files, pictures and other resources. Meanwhile, 1 FXS port can be well adapted to small and micro enterprises, FXS can work for telephone or for Fax, no need to add additional equipment. FTA1101 VoIP wireless router is ideally suited for small and medium enterprises (SMB) to build wireless office.The FTA1101 is based on SIP V2.0 and 802.11n standard and compatibility with most service providers. It features 1phone port telephone ports, 2 10M/100M Ethernet ports which brings great convenience when deploying VoIP network.


This guide contains the following chapters:

- Chapter 1: Product description
- Chapter 2: Configuring Basic Settings
- Chapter 3: Web Interface 1
- Chapter 4: IPv6 address configuration on WAN interface
- 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:

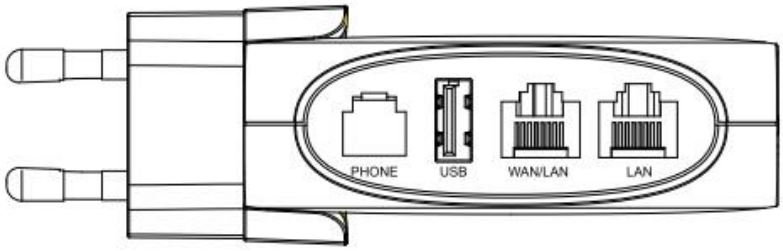
# FTA1101

**Table 1** Features at-a-glance

| Port/Model | FTA1101 |
|---|---|
| picture |  |
| WAN | 1 |
| LAN | 1 |
| FXS | 1 |
| Ethernet interface | 2* RJ45 10/100M |
| Fax | T.30, T.38 Fax |
| Wire-speed NAT | Support |
| 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** FTA1101 Interfaces




| Interface | Description |
|---|---|
| PHONE | Analog phone connector |
| USB | Connect USB |
| WAN | Connector for accessing the Internet |
| LAN | Connectors for local networked devices |

# 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 FTA1101and will void the manufacturer warranty.

**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.

# Chapter 2 IVR Voice Prompt

This chapter contains:

# Voice Gateway Configuration Method (IVR)

The device can be configured in two ways, as follows:

(1) Use IVR (Interactive Voice Response)

(2) the use of web pages

This chapter mainly introduces how to configure the voice gateway through IVR.

## Start IVR

Users follow these steps to achieve IVR:

(1) Go off-hook and press the "****" key to start the IVR. Then the user will hear the voice prompt "1 WAN port configuration...".

(2) According to different options, press any digit between 0 and 9, the device will broadcast the corresponding content, the numbers 0 to 9 represent the details as shown in the chart below.

(3) After each setting will play "Please input option, 1 WAN port configuration...".

Note

Before using IVR,please confirm analog phone is connected with ATA correctly.

## IVR Description

The following chart lists the IVR requirements and a detailed description:

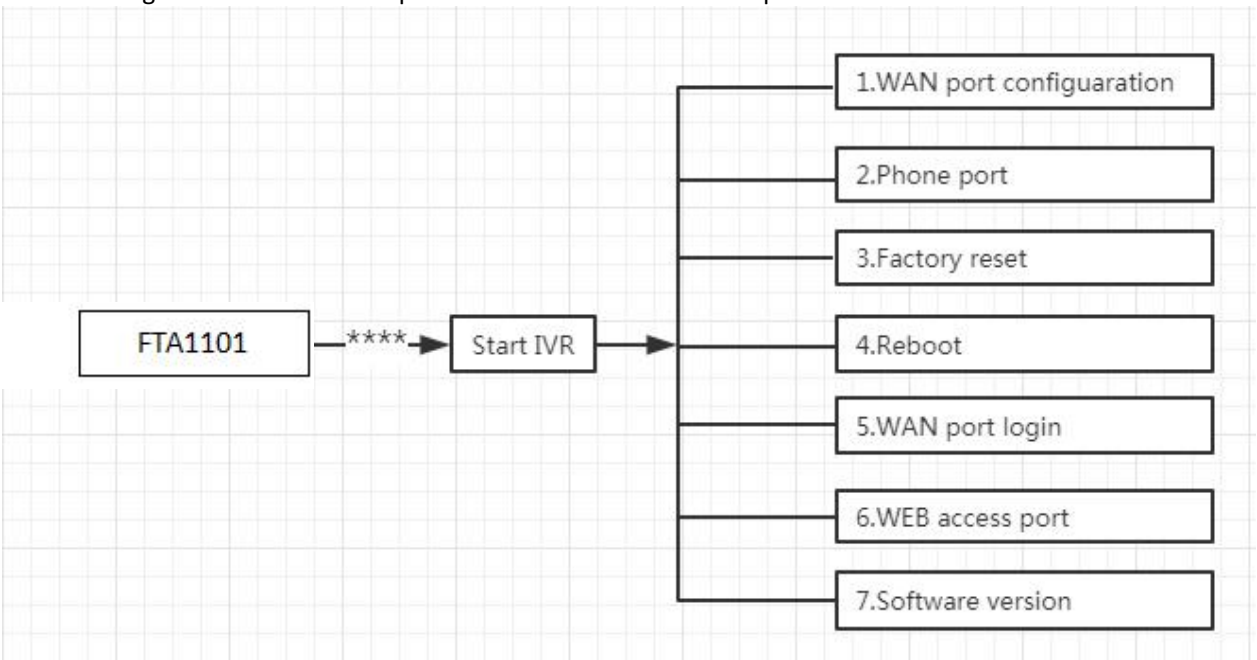


**Table 3** IVR Menu Setting Options

| Operation code | Menu |
|---|---|
| 1<br>Network port configuration<br>(1)WAN Port Configuration | 1. Pick up phone and press “****” to start IVR<br>2. Select "1", then the device will continue to broadcast to remind users to choose 1.WAN port connection type; 2.WAN port IP address; 3. WAN subnet mask; 4. Gateway; 5. DNS<br>3. Choose “1”, and The router reports the current WAN port connection type2)<br>4. Prompt "Please enter password”, user needs to input password and press “#” key, if user wants to configuration WAN port connection type.<br>The password in IVR is same as web management interface login, the user may use phone keypad to enter password directly<br>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.<br>5. Prompt "Please enter password”, user needs to input password and press “#” key if user wants to configuration WAN port connection type.<br>6. Choose the new WAN port connection type (1) DHCP or (2) Static<br>The unit reports “Operation Successful” if the changes are successful. The router returns to the prompt “please enter your option …”<br>7. To quit, enter “*” |

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

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

| | |
|---|---|
| 5<br>WAN Port Login | 1. Pick up phone and press “****” to start IVR<br>2. Choose “5”, and the router reports “WAN Port Login”<br>3. Prompt "Please enter password", the method of inputting password is same as operation 1.<br>4. If user wants to quit, press “*”. |
| 6<br>WEB Access Port | 1. Pick up phone and press “****” to start IVR<br>2. Choose “6”, and the router reports “ WEB Access Port”<br>3. Prompt “Please enter password”, the method of inputting password is same as operation 1.<br>4. Report “operation successful” if user operation is ok. |
| 7<br>Firmware Version | 1. Pick up phone and press “****” to start IVR<br>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 FTA1101 is connected.

7.The default LAN port IP address of FTA1101 is 192.168.11.1 and this address should not be assigned to the WAN port IP address of FTA1101 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 3 Basic Settings

This chapter covers:

# Web Page

## About Password

Our device supports two levels of management: administrators and users.

(1) Administrator mode can browse and set all configuration parameters.

(2) User mode can set all configuration parameters except SIP1that some parameters can not be changed, such as server address and port.

- Default user with administrator mode： Username: admin, Password: admin
- Default user with user mode: Username: admin, Password: user

## URL Format

FTA1101 has a built-in web server in response to HTTP get / post requests. Users can use a web browser, such as Microsoft's IE, to log in to the FTA1101 page and configure the FTA1101.

### LAN port Login

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

**Note**

You may either set up your PC to get an IP dynamically from the router or set up the IP address of the PC to be the same subnet as the default IP address of router is 192.168.1.1. For detailed information, see Chapter 5: Troubleshooting Guide.

2.Open a web browser on your PC and input “http://192.168.1.1”.

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


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

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

**Note**

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

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

### WAN port Login

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

2.Obtain the IP addresses of WAN port using Voice prompt or by logging into the device web management interface via a LAN port and navigating to Network > WAN.

3.Open a web browser on your PC and input http://<IP address of WAN port>. The following login page will be opened to enter username and password.


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

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

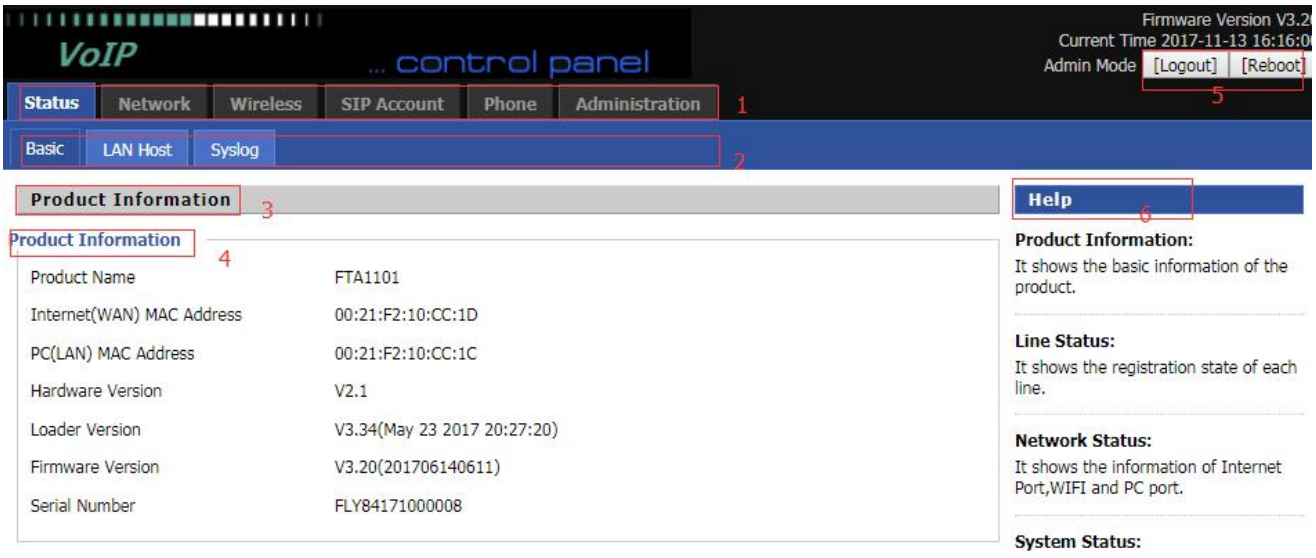
**Note**

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

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

# WEB Interface Introduction

**Table 4** WEB Interface Introduction

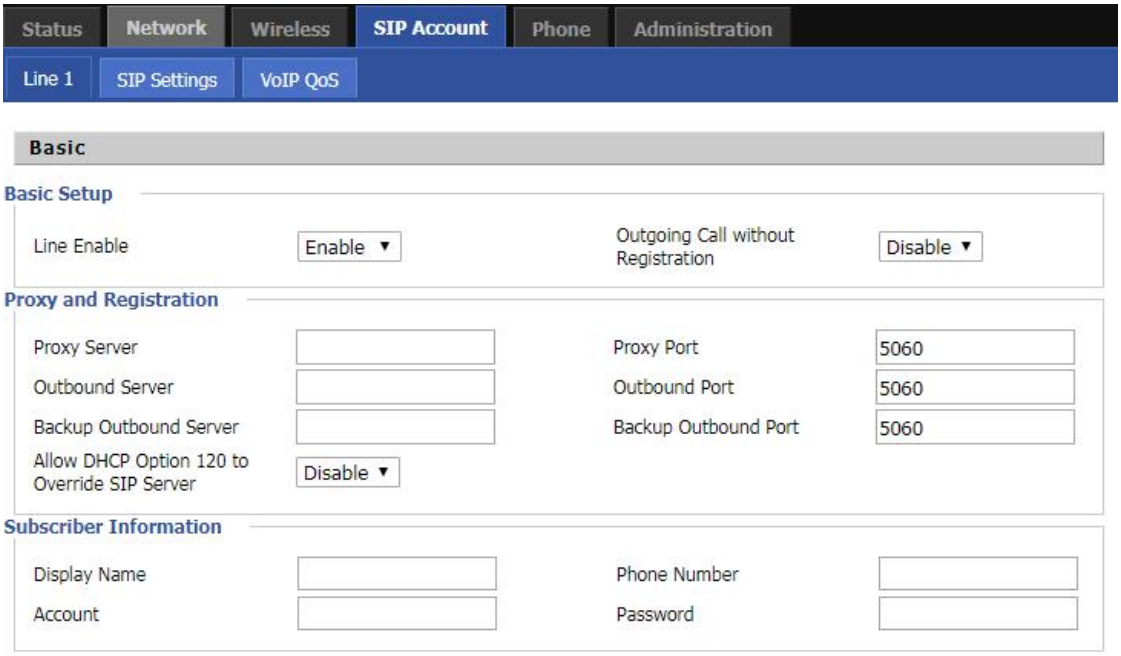



| Serial number | Name | Description |
|---|---|---|
| Postition 1 | navigation bar | Click navigation bar, many sub-navigation bar will appear in the place 2 |
| Postition 2 | sub-navigation bar | Click sub-navigation bar to enter to configuration page |
| Postition 3 | configuration title | The configuration title |
| Postition 4 | configuration bars | The configuration bars |
| Postition 5 | main information | Display the firmware version, DSP version, Current Time, and user can change login level (mode) to return to login page by press blue Switch button. |
| Postition 6 | Help | Display the main information for configuration; user can get help from it directly. |
| | Save & Apply | Use this button,conifg will be saved |
| | Save | After changing the parameters, you need to click this button to save. After you click Save, there is a need to restart the device. |
| | Cancel | Click to cancel the change |
| | Reboot | Click to restart |
| | Refresh | Refresh current page |

# SIP Account configuration

FTA1101 have 1 Line to make SIP (Session Initiation Protocol) calls. Before registering, the device user should have a SIP account configured by the system administrator or provider. See the section below for more information.

**Table 5** Config SIP the Web Management Interface




**Steps:**

Step 1. The account enable is set to "On" and the line can be used after opening.

Step 2. The registration server fills in the IP address of the SIP server.

Step 3. Display Name Fill in the content is the name of the number displayed on the LCD.

Step 4. The registration account is filled with the account provided by the SIP server.

Step 5. The name of the authentication is the SIP account provided by the SIP server.

Step 6. The password is filled with the password provided by the SIP server registration account.

Step 7. When you are finished, click the Save button at the bottom of the page to make the configuration take effect.

Step 8. Check the registration of the corresponding line on the display / web status page.

**Notes**

**Step 3-9 is to fill in the required content, other parameters fill in the required**

## Procedure

To view the SIP account status of device, open the **Status** web page and view the value of registration status.

# Basic Function

## Calling phone or extension numbers

To make a phone or extension number call:

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

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

## Direct IP calls

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

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

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

## Call Hold

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

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

## Call transfer

### 1.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.

### 2.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.

e

l

# Chapter 4 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
- Phone
- Security
- Application
- Administration
- Management
- System Log
- Logout
- Reboot

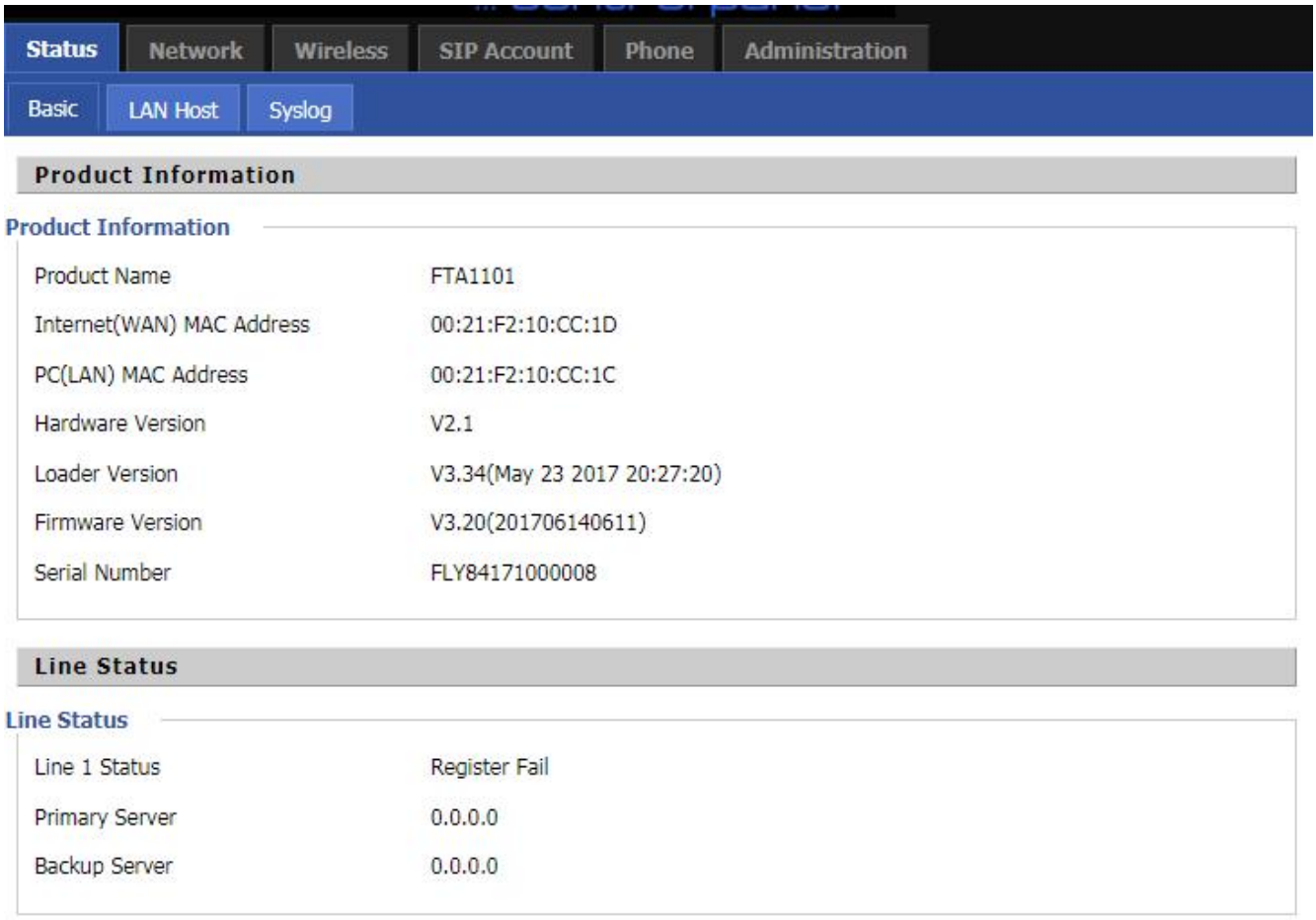
# Login

**Table 6** 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

This webpage shows the status information about the Product, Network, 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, MAC Clone, Port Forward and other parameters in this section of the web management interface.

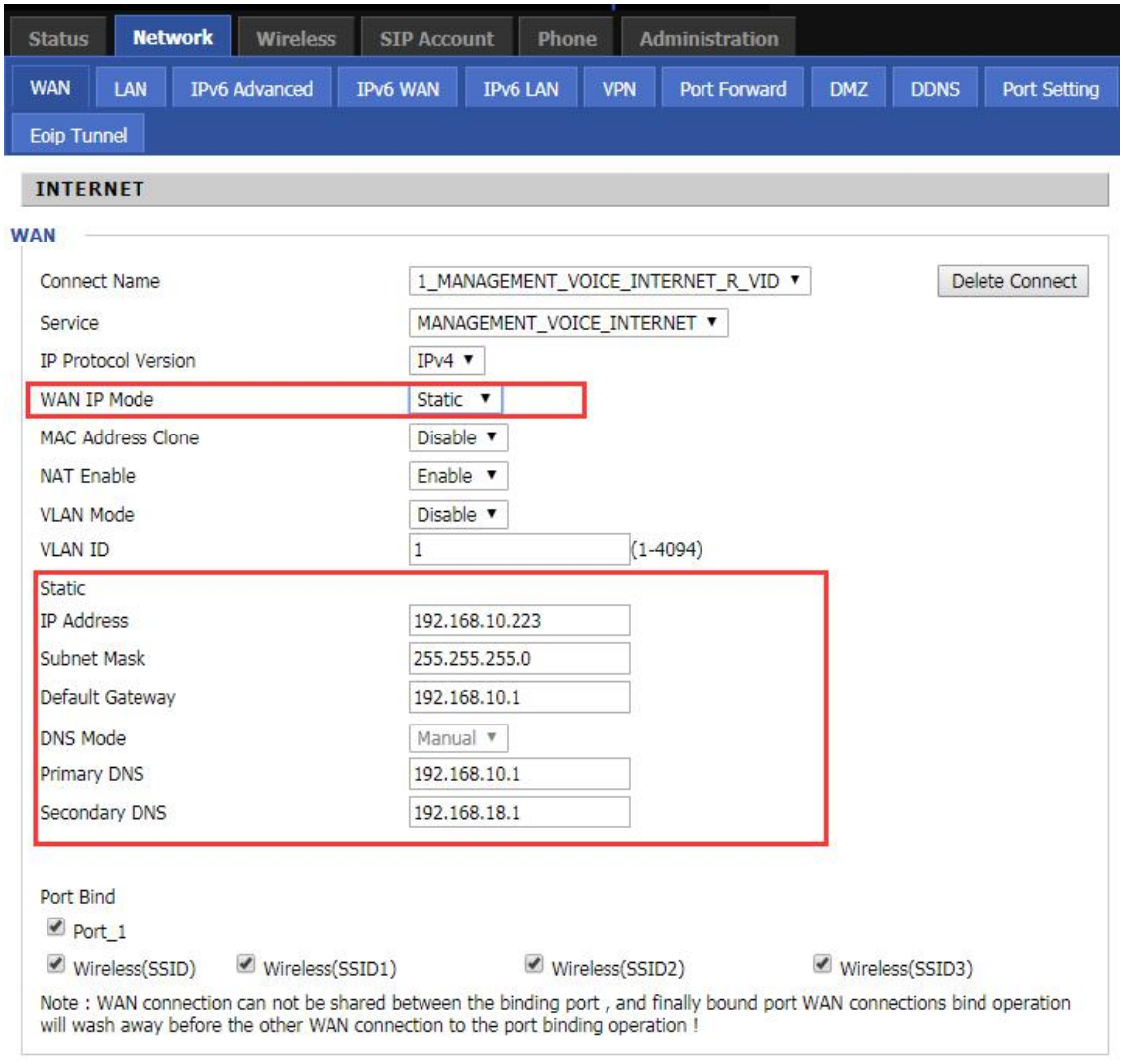
## WAN

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

### 1.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 7** Internet



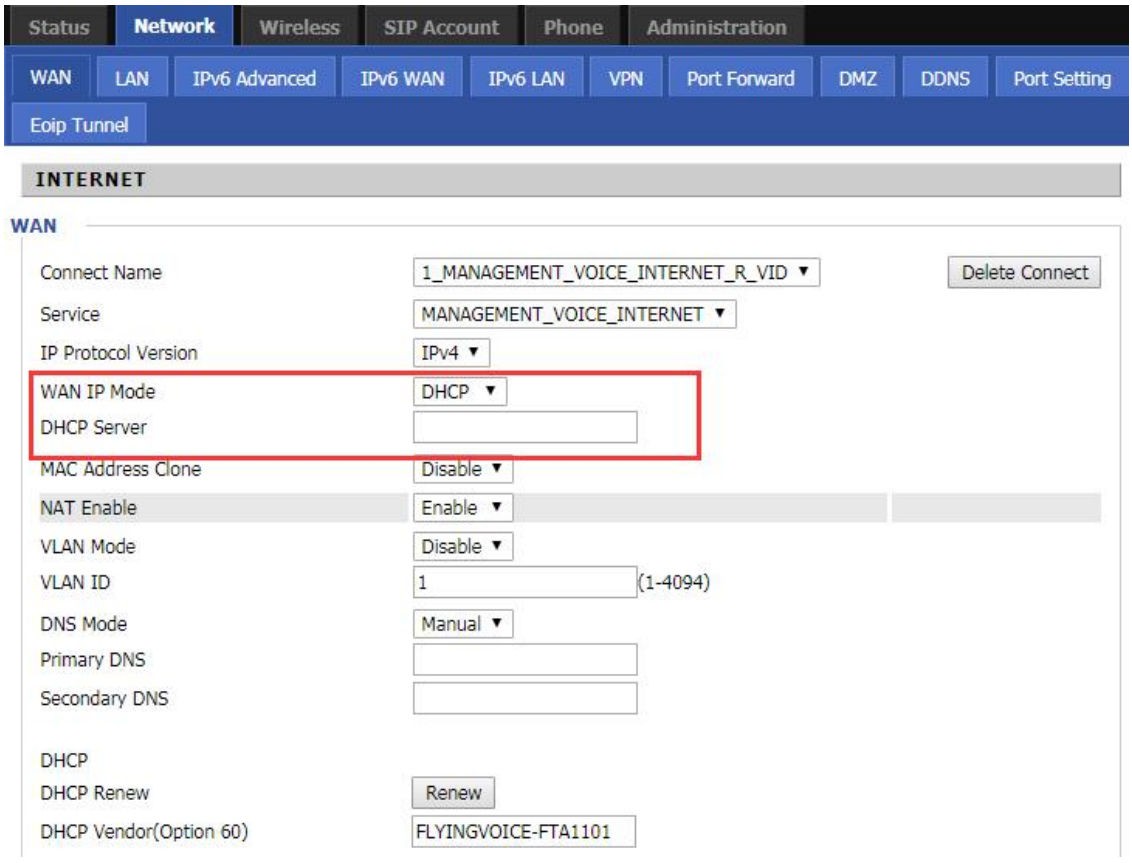
| Field Name | Descriptio |
|---|---|
| IP Address | The IP address of Internet port |
| Subnet Mask | The subnet mask of Internet port |
| Default Gateway | The default gateway of Internet port |
| DNS Mode | Select DNS mode, options are Auto and Manual:<br>1. When DNS mode is Auto, the device under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

## 2.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 8** DHCP



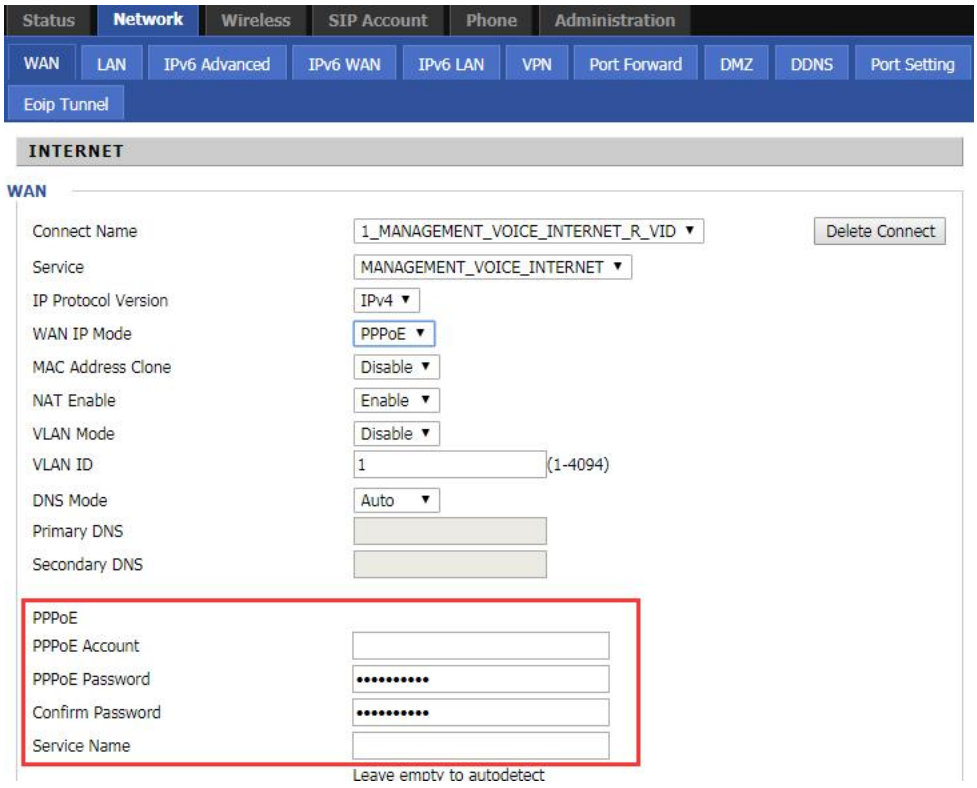
| Field Name | Description |
|---|---|
| DNS Mode | Select DNS mode, options are Auto and Manual:<br>When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS.<br>When DNS mode is Manual, the user should manually configure the preferred DNS and alternate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

### 3.PPPoE

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

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

**Table 9** PPPoE

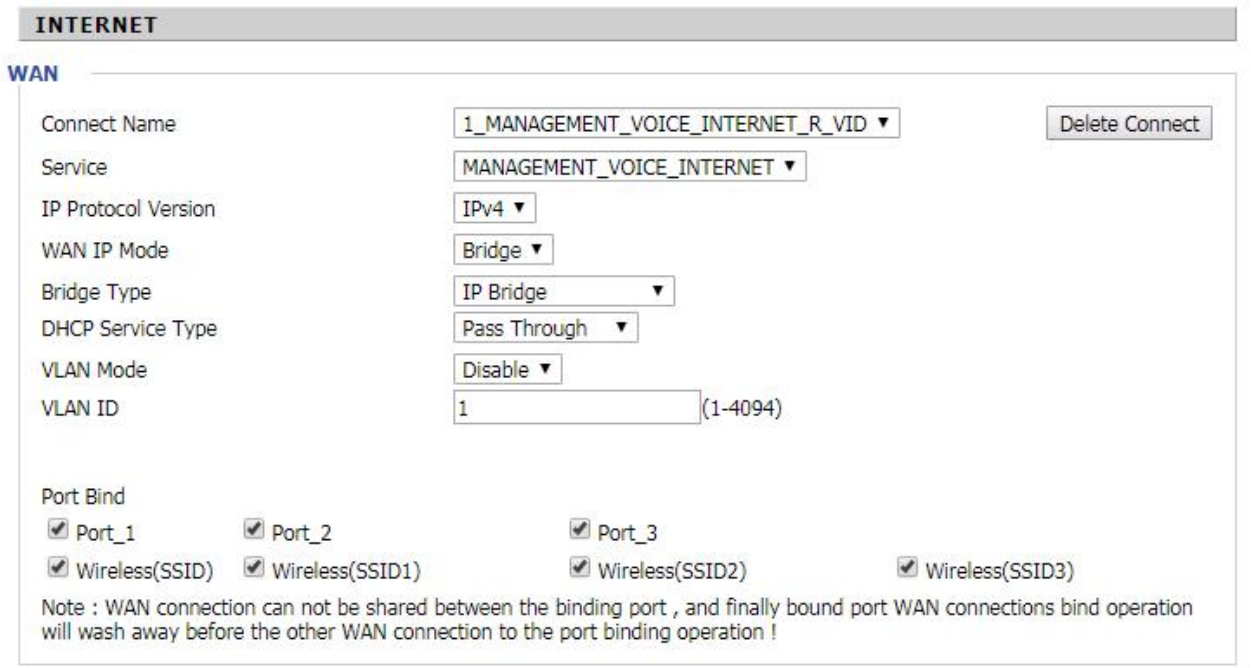


| Field Name | Descri |
|---|---|
| PPPoE Account | Enter a valid user name provided by the ISP |
| PPPoE Password | Enter a valid password provided by the ISP. The password can contain special characters and allowed special characters are $, +, *, #, @ and ! For example, the password can be entered as #net123@IT!$+*. |
| Confirm Password | Enter your PPPoE password again |
| Service Name | Enter a service name for PPPoE authentication.<br>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:<br>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; |
| Keep Alive Redial Period | Set the interval to send Keep Alive messaging |
| PPPoE Account | Assign a valid user name provided by the ISP |

## 4.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 10** Bridge Mode



| Field Name | Descripti |
|---|---|
| **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** | Select 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** | Enable or disable the VLAN mode. |
| **Disable** | The WAN interface is untagged. LAN is untagged. |
| **Enable** | The WAN interface is tagged. LAN is untagged. |
| **Trunk** | Only valid in bridge mode. All ports, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN. |
| **VLAN ID** | Set the VLAN ID. |
| **802.1p** | Set the priority of VLAN, Options are 0~7. |

**Note**

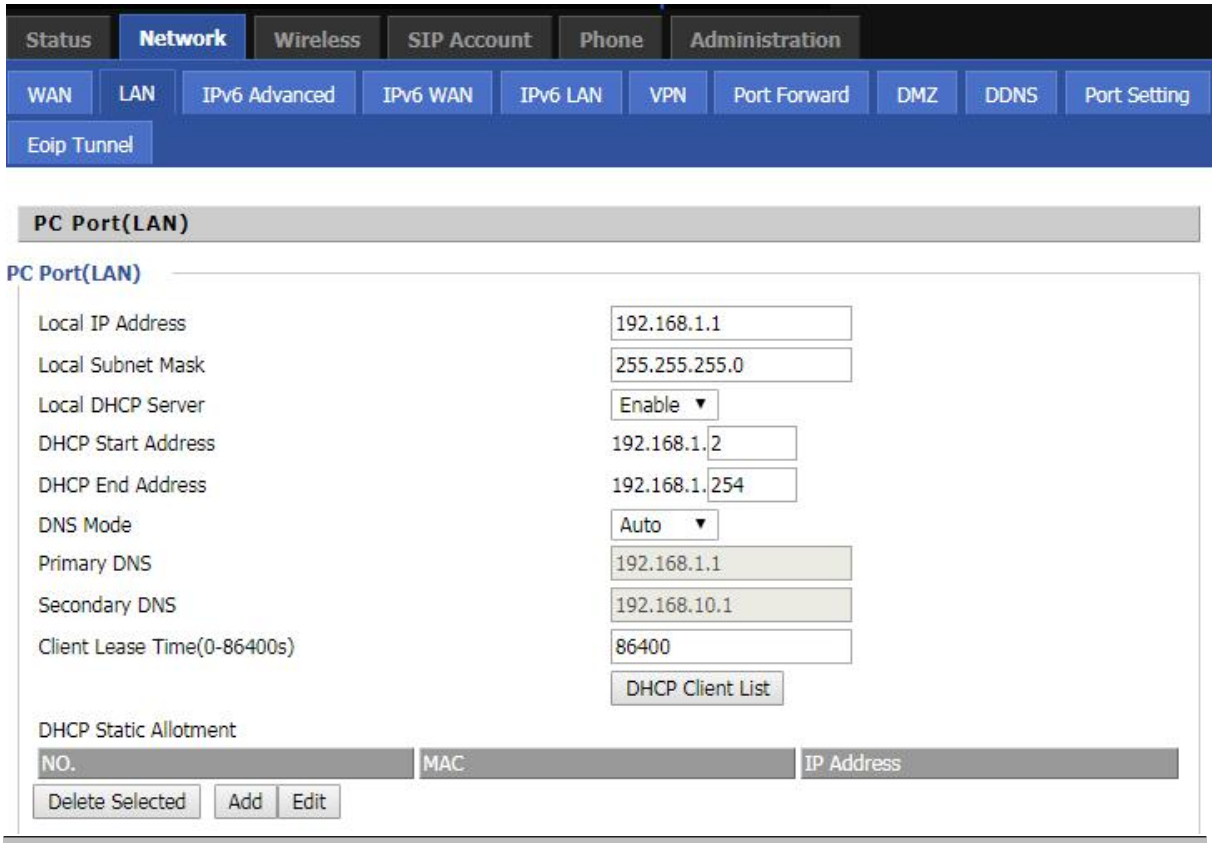
Multiple WAN connections may be created with the same VLAN ID

# LAN

## LAN Port

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

**Table 11** LAN port



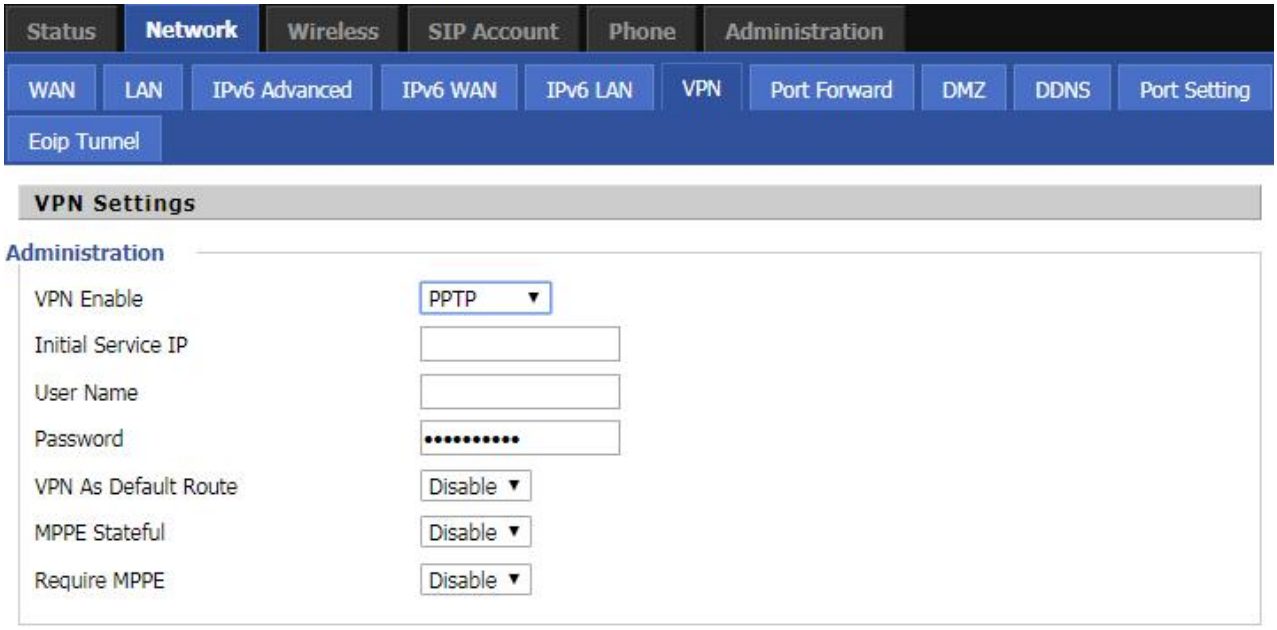

| Field Name | Description |
|---|---|
| IP Address | Enter the IP address of the router on the local area network. All the IP addresses of the computers which are in the router's LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (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:<br>When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.<br>When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS. |
| Primary DNS | Enter the preferred DNS address. |
| Secondary DNS | Enter the secondary DNS address. |
| Client Lease Time | This option defines how long the address will be assigned to the computer within the network. In that period, the server does not assign the IP address to the other computer. |
| DNS Proxy | Enable or disable; If enabled, the device will forward the DNS request of LAN-side network to the WAN side network. |

# VPN

VPN is a technology that builds a private network on a public network. The connection between any two nodes of the VPN network does not have the end-to-end physical link required by the traditional private network, but rather the network platform provided by the public network service provider, and the user data is transmitted in the logical link. With VPN technology, you can establish private connections and transfer data between any two devices on the public network.

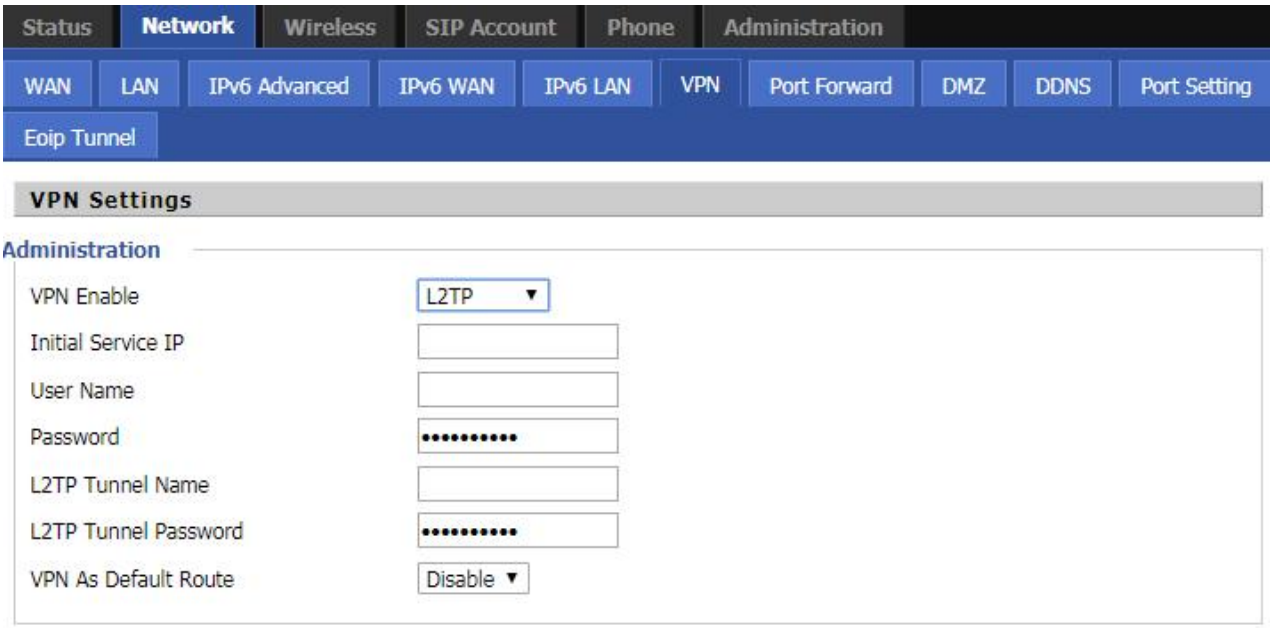
**Table 12** PPTP




| Parameters name | Description |
|---|---|
| VPN Enable | Whether to enable VPN.<br>Select PPTP mode. |

| | |
|---|---|
| Initial Service IP | The IP address of the VPN server. |
| User Name | The user name required for authentication. |
| Password | The password required for authentication. |
| VPN As Default Route | Prohibited or open, the default is prohibited. |
| MPPE Stateful | Enable or Disable MPPE Stateful. |
| Require MPPE | Enable or Disable Require MPPE. |

**Table 13** L2TP



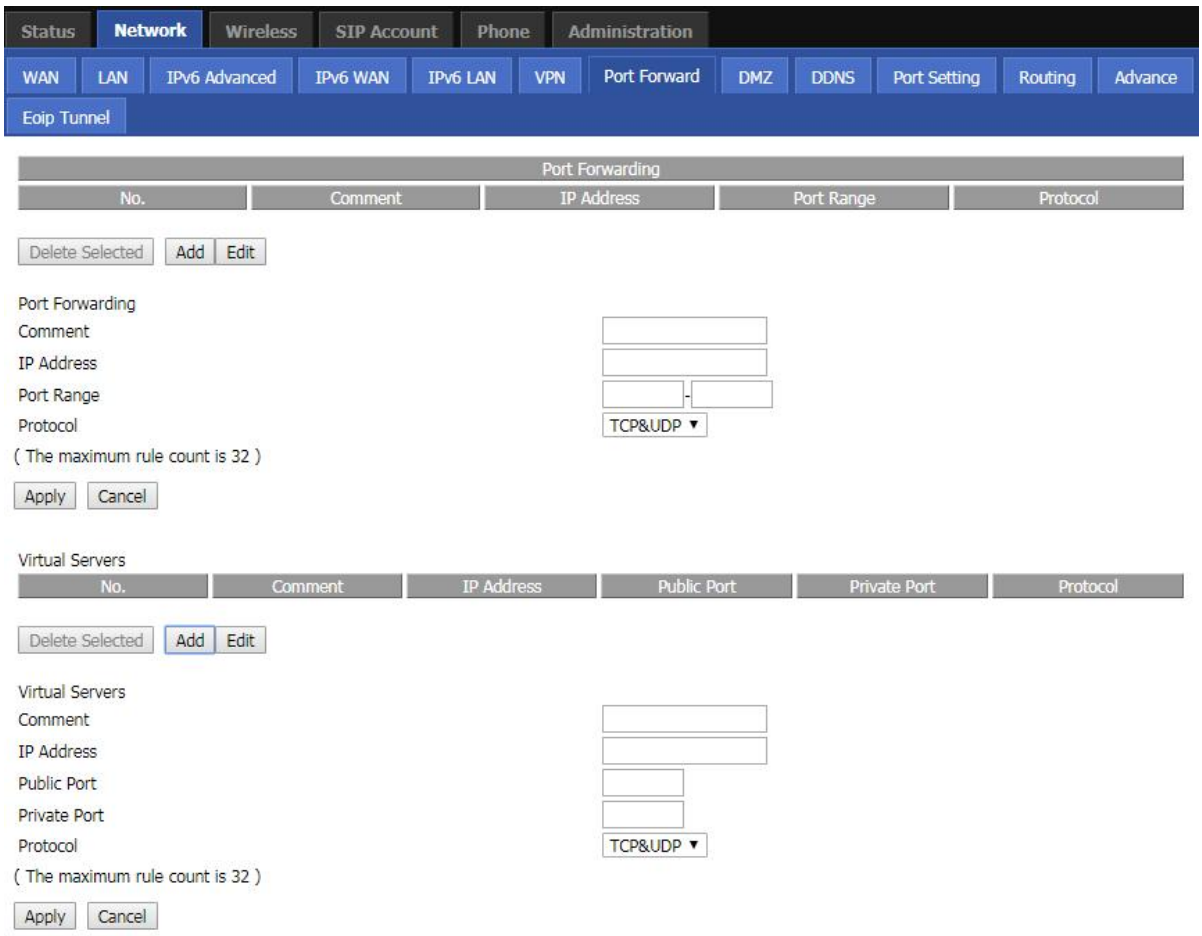

| Parameters name | Description |
|---|---|
| VPN Enable | Whether to enable VPN.<br>Select PPTP mode. |
| Initial Service IP | The IP address of the VPN server. |
| User Name | The user name required for authentication. |
| Password | The password required for authentication. |
| L2TP Tunnel Name | L2TP Tunnel Name |
| L2TP Tunnel Password | L2TP Tunnel Password |
| VPN As Default Route | Prohibited or open, the default is prohibited. |

**Table 14** OpenVPN


| Parameters name | Description |
|---|---|
| VPN Enable | Whether to enable VPN.<br>Select OpenVPN mode. |
| OpenVPN TLS Auth | Whether OpenVPN TLS authentication is enabled |
| VPN As Default Route | Prohibited or open, the default is prohibited. |

# Port Forward

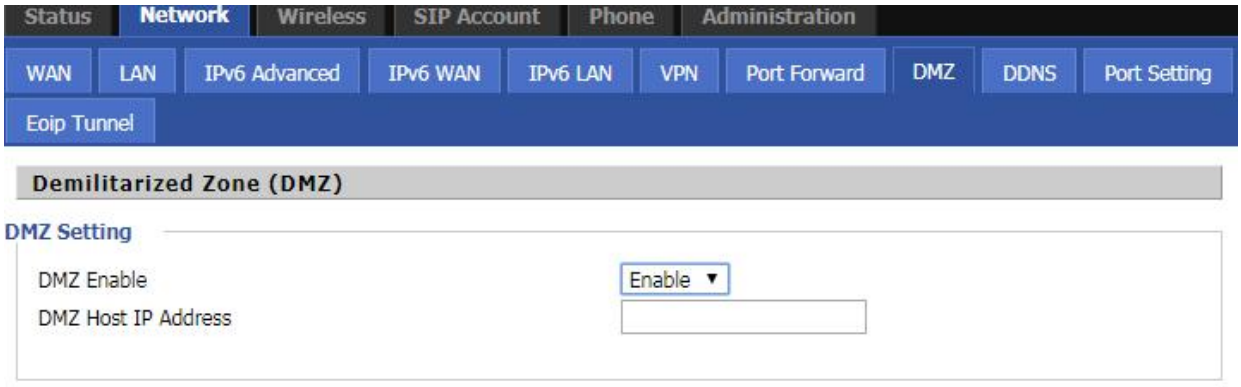
**Table 15** Port Forward



| 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 |

# DMZ

**Table 16** DMZ




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

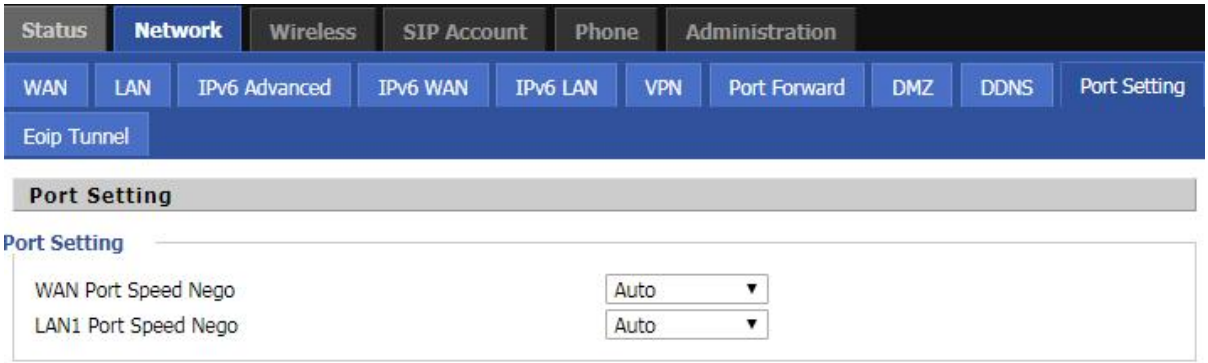
# DDNS

**Table 17** DDNS


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

# Port Setting

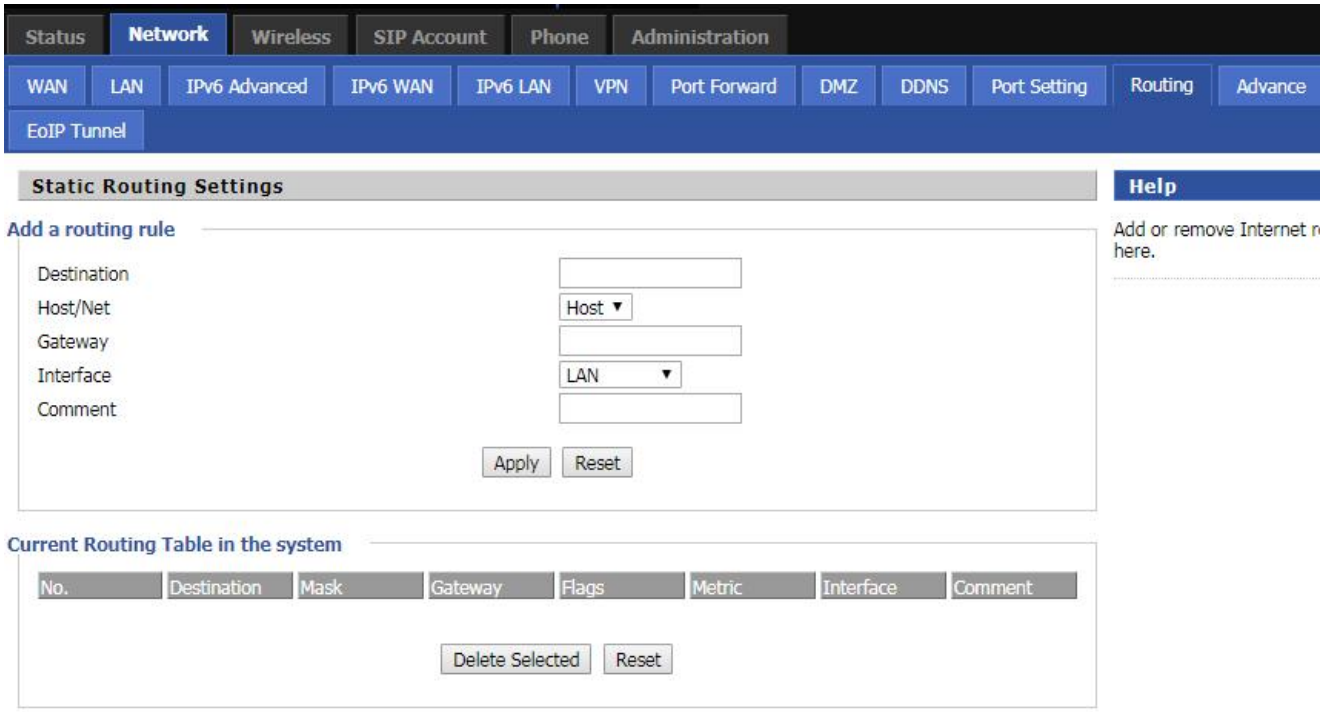
**Table 18** Port setting




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

# Routing

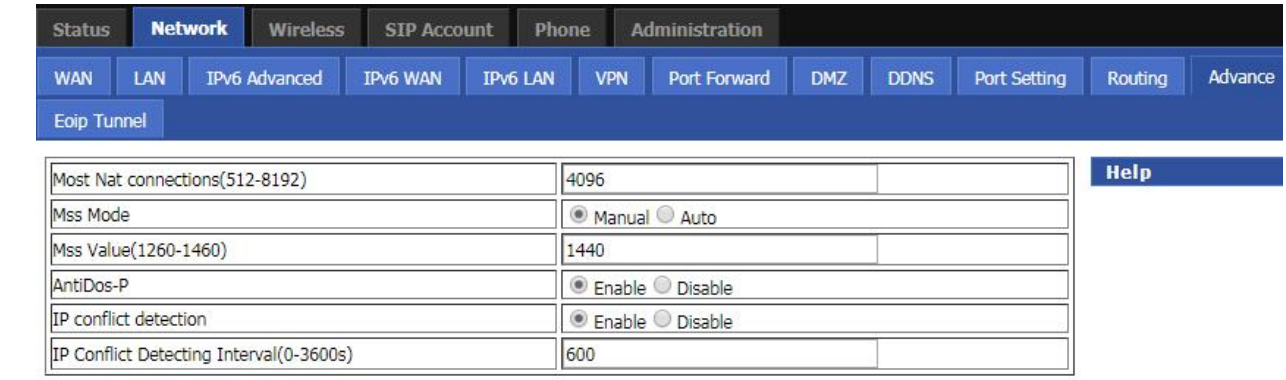
**Table 19** Routing




| 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

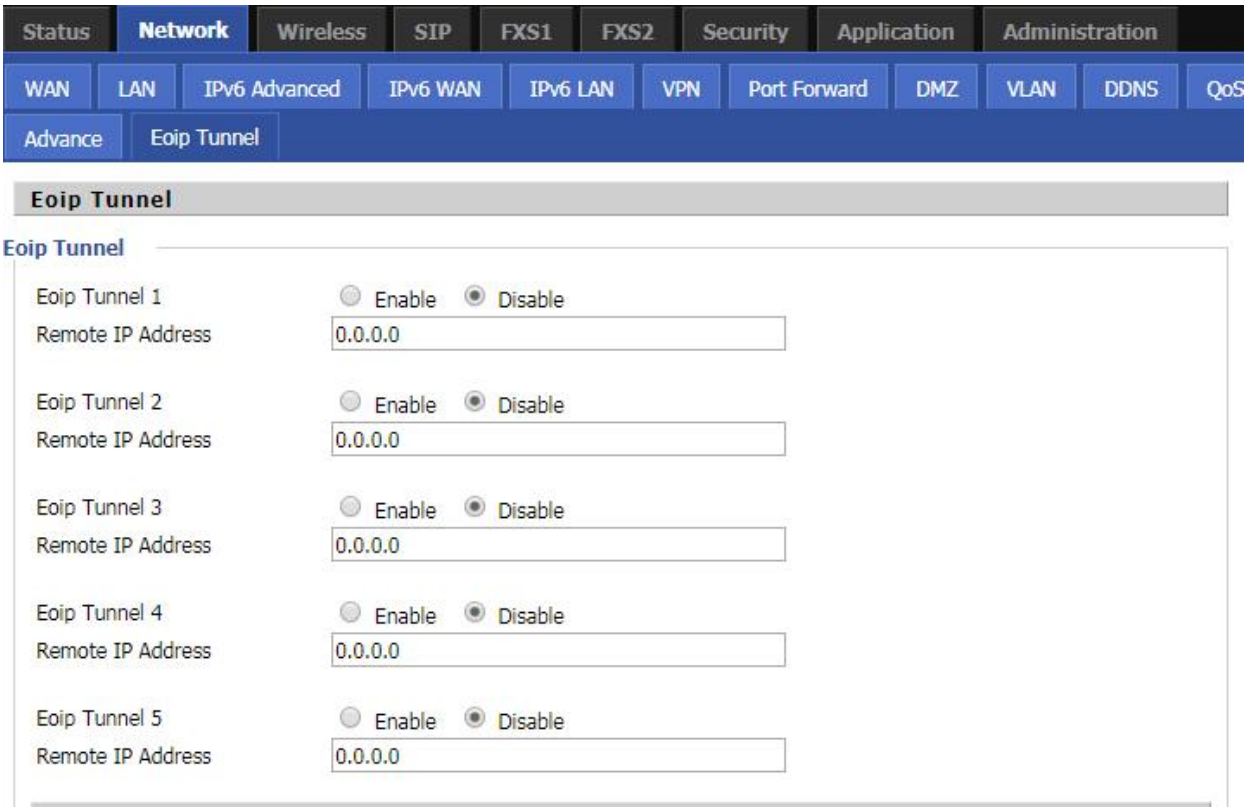
**Table 20** Advance



| Field Name | Description |
|---|---|
| Most Nat connections | The largest value which the FWR8401 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 |

# Eoip Tunnel

**Table 21** Eoip Tunnel

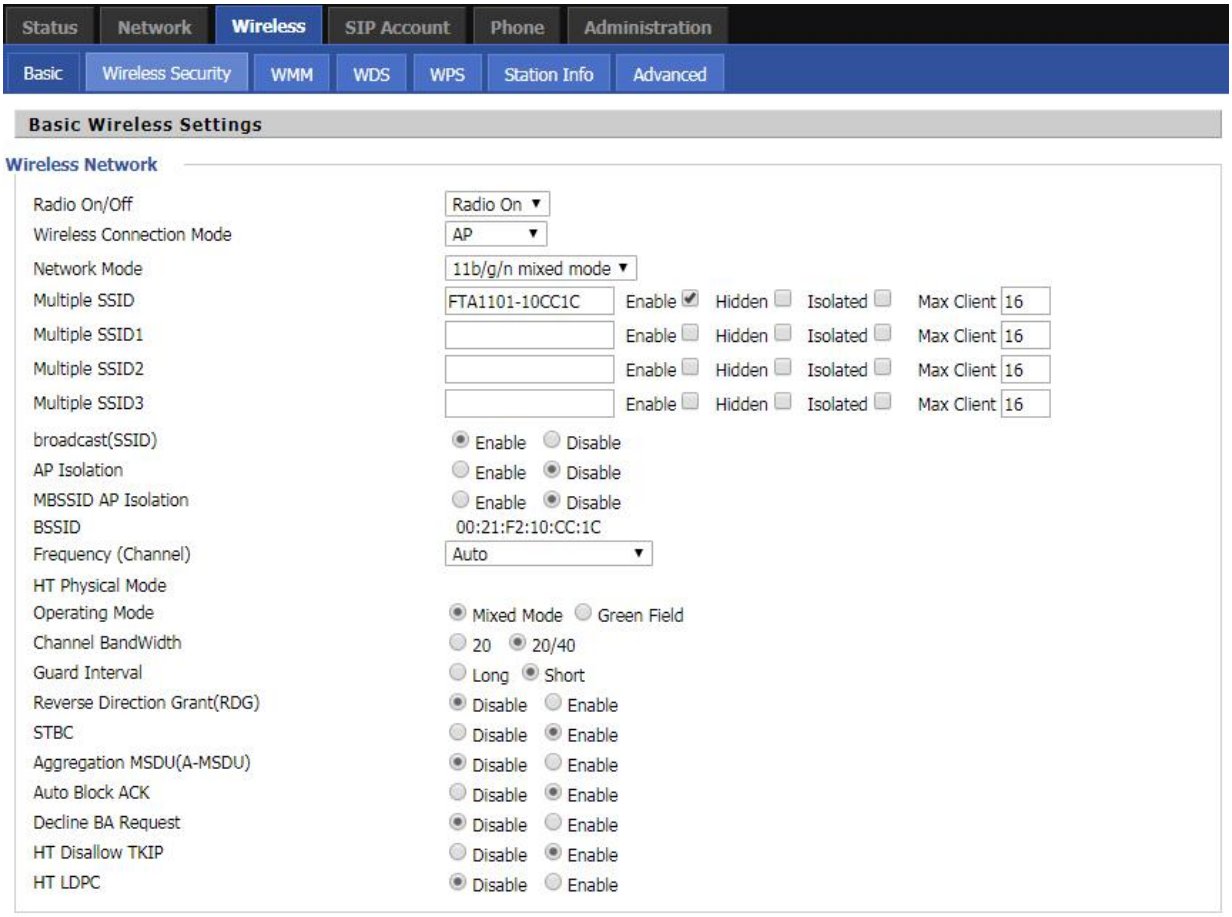



| Field Name | Description |
|---|---|
| Eoip Tunnel 1-5 | Choose to enable or disable the tunnel |
| Remote Address | Input requires a remote IP address |

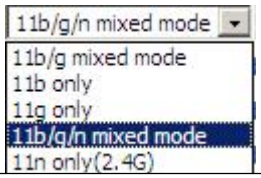
# Wireless configuration

## Basic

**Table 22** Basic



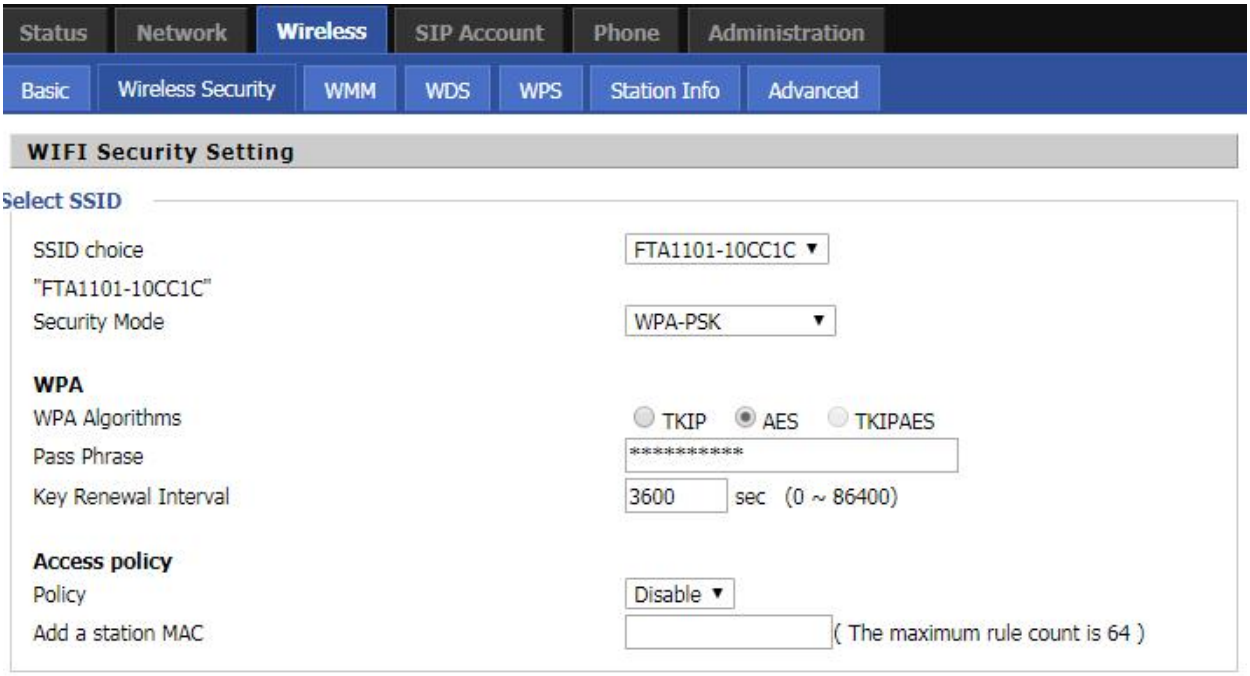

| Field Name | Description |
|---|---|
| Radio on/off | Select “Radio off” to disable wireless.<br>Select “Radio on” to enable wireless. |
| Wireless connection mode | According to the wireless client type, select one of these modes. Default is AP |
| Network Mode | Choose one network mode from the drop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

| | |
|---|---|
| |  |
| 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<br>Operating<br>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<br>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)<br>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<br>Disabled: No frame aggregation is employed at the router |
| Auto Block Ack | Enabled: Multiple frames are acknowledged together using a single Block Acknowledgement frame.<br>Disabled: Auto block acknowledgement is not used by the device – use this configuration when low throughput/connectivity issues are experienced by |
| Decline BA Request | Enabled: Disallow block acknowledgement requests from devices Disabled: Allow block acknowledgement requests from devices |
| HT Disallow TKIP | Enabled: Disallow the use of Temporal Key Integrity Protocol for connected devices<br>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<br>Disabled: Disable Low-Density Parity Check mechanism |

# Wireless Security

**Table 23** Wireless security

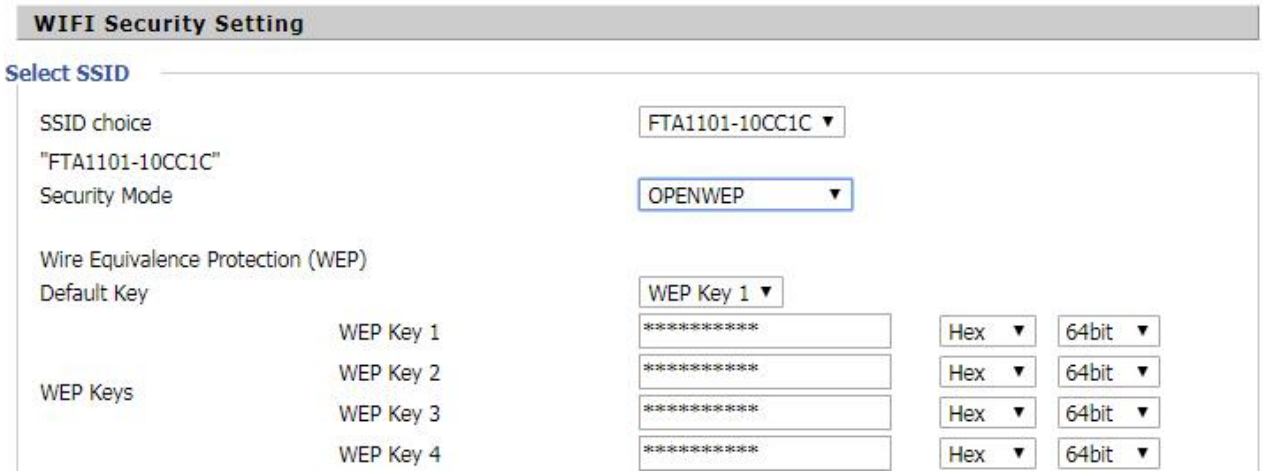



| Field Name | Description |
|---|---|
| SSID Choice | Choose one SSID from SSID, Multiple SSID1, Multiple SSID2 and Multiple SSID3. |
| Security Mode | Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.Each encryption mode will bring out different 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 24** WiFI Security Setting

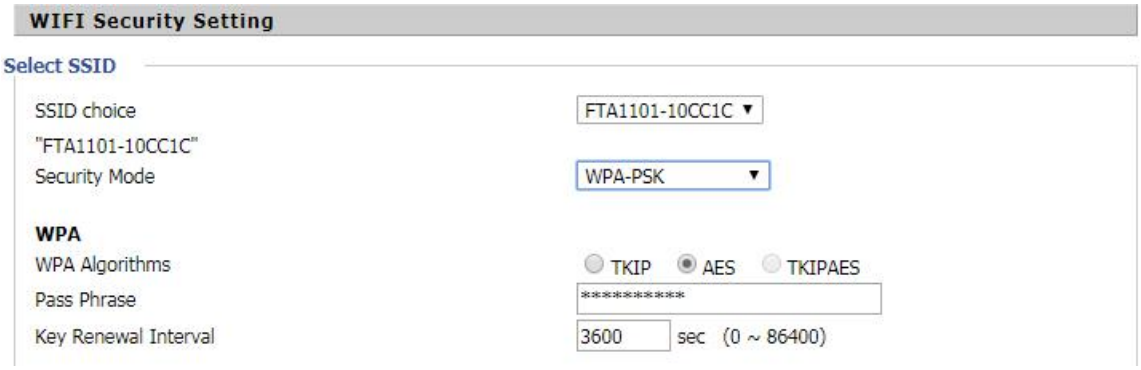



| Field Name | Description |
|---|---|

| | |
|---|---|
| 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 25** WPA-PSK

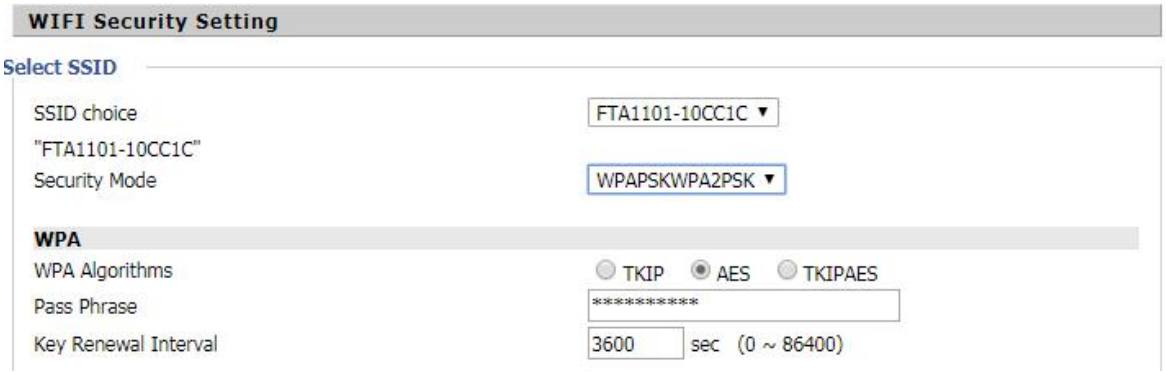



| Field Name | Description |
|---|---|
| WPA Algorithms | This item is used to select the encryption of wireless home gateway algorithms, options are TKIP, AES and TKIPAES. |
| Pass Phrase | Setting up WPA-PSK security password. |
| Key Renewal Interval | Set the key scheduled update cycle, default is 3600s. |

**W**

**PAPSKWPA2PSK** manner is consistent with WPA2PSK settings:

**Table 26** WPAPSKWPA2PSK



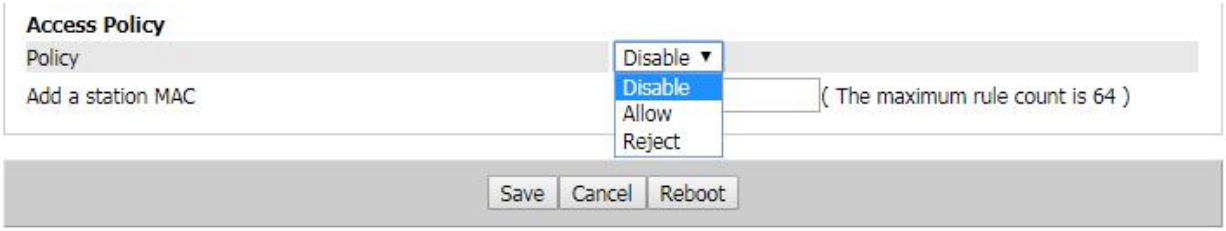

| Field Name | Description |
|---|---|
| WPA Algorithms | The home gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms. |
| Pass Phrase | Set WPA-PSK/WPA2-PSK security code |

| | |
|---|---|
| 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:

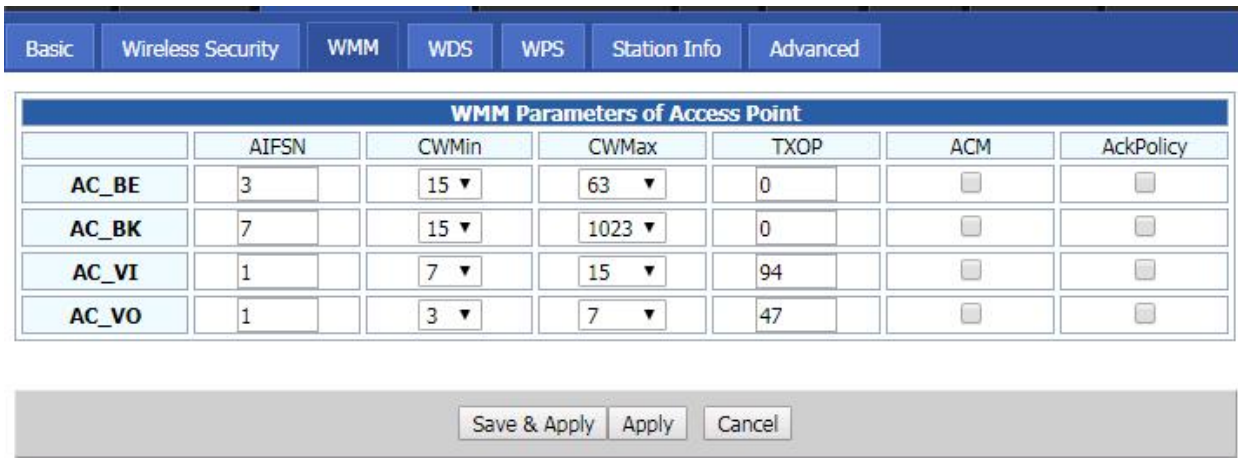
**Table 35** Wireless Access Policy




| 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.<br>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

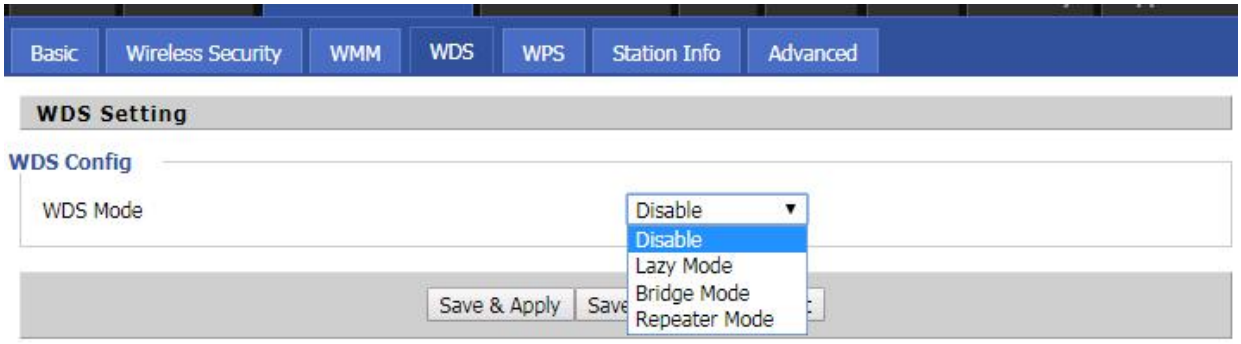



## Description

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

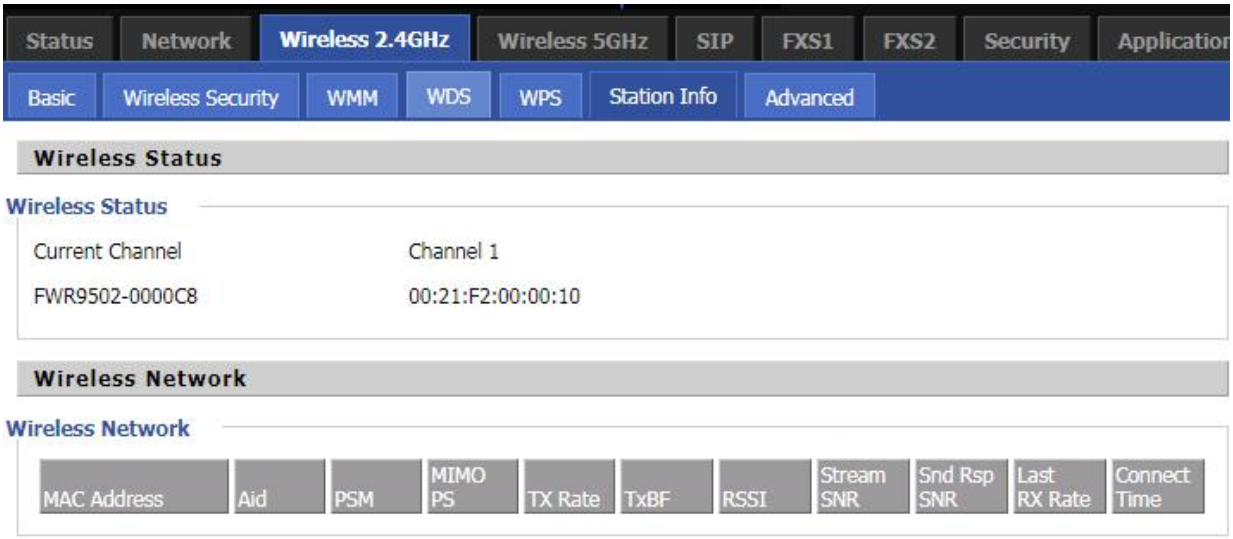
**Table 37** WDS




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

# Station Info

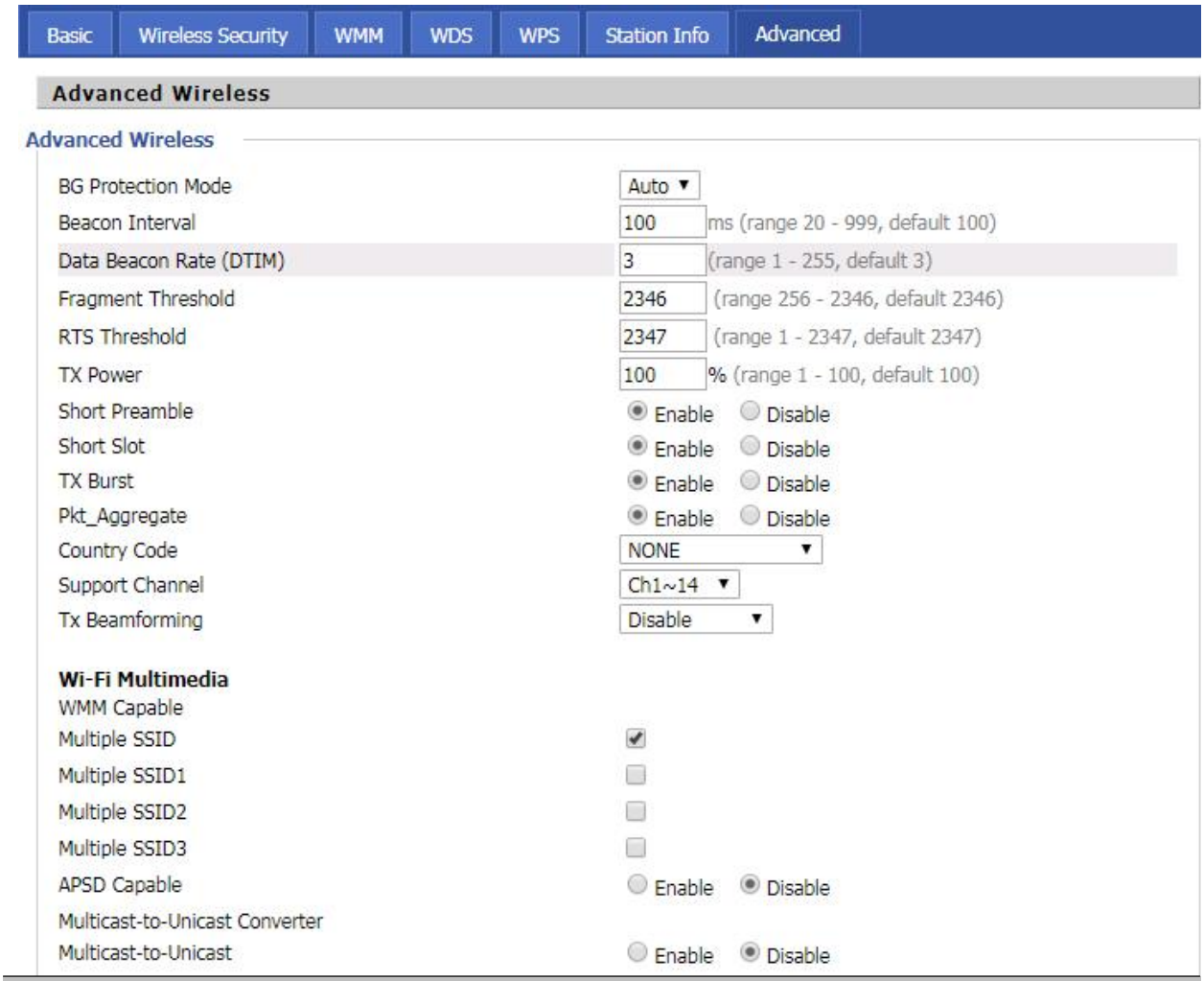
**Table 39** Station info



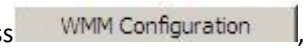

| Description |
|---|
| This page displays information about the current registered clients' connections including operating MAC address and operating statistics. |

# 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  , 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 |

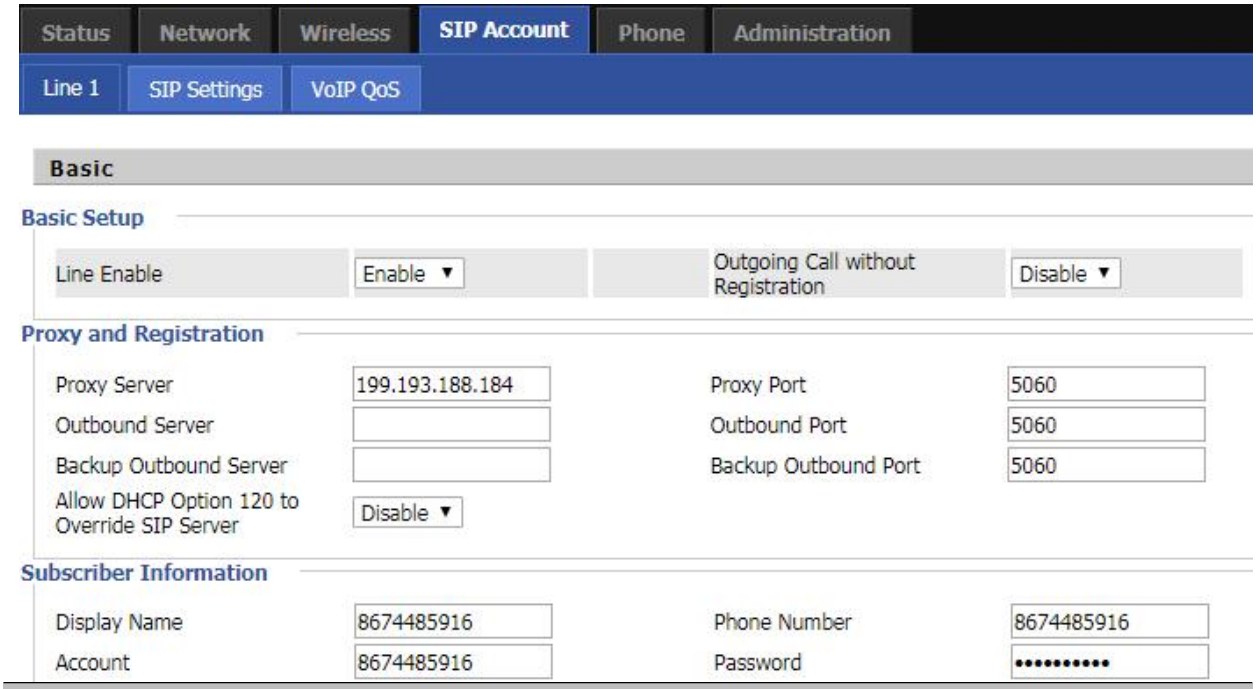
# SIP Account

## SIP Account

### Basic

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

**Table 30** Line

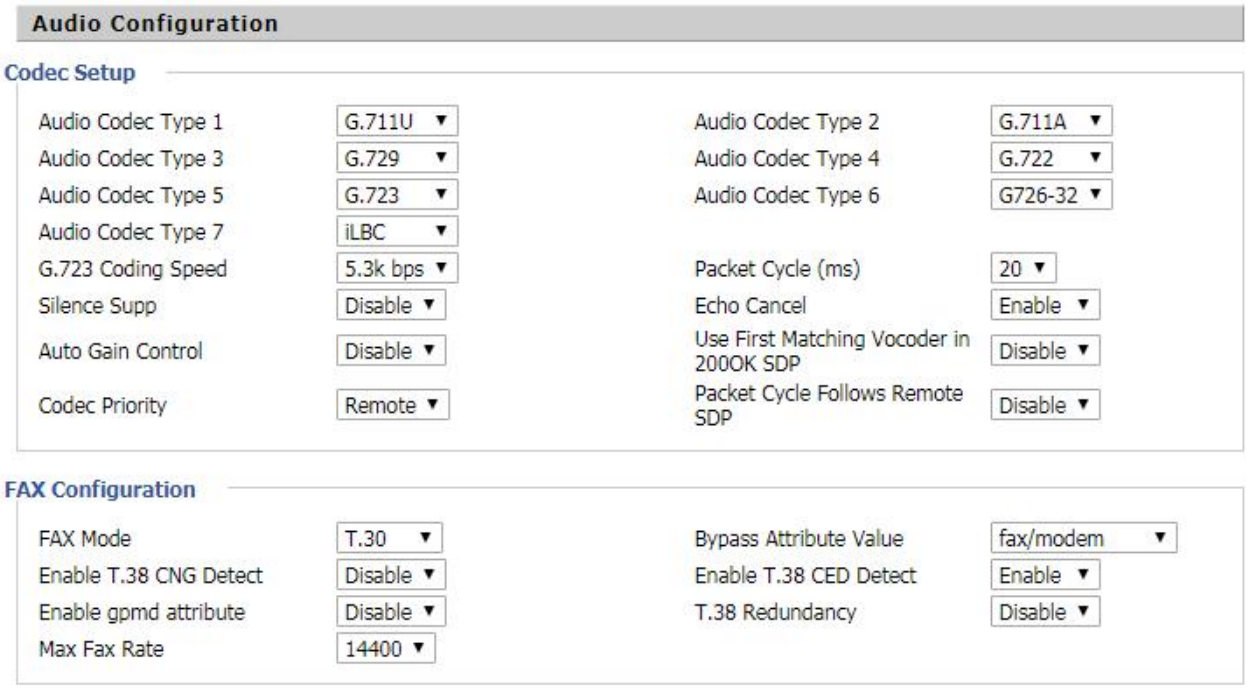



| Field Name | Description |
|---|---|
| Line Enable | Enable/Disable the line. |
| Outgoing Call without Registration | Enable/Disable Outgoing Call without Registration<br>If enabled, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; 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 31** Audio configuration

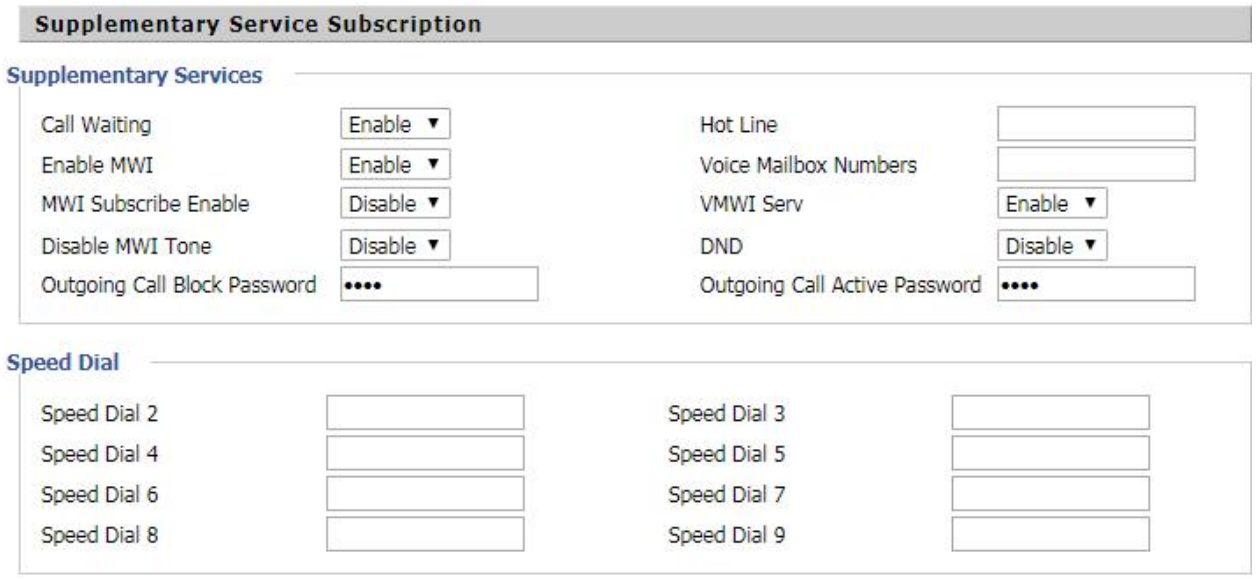



| Field Name | Description |
|---|---|
| Audio Codec Type1 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type2 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type3 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type4 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type5 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| G.723 Coding Speed | Choose the speed of G.723 from 5.3kbps and 6.3kbps |
| Packet Cycle | The RTP packet cycle time, default is 20ms |
| Silence Supp | 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

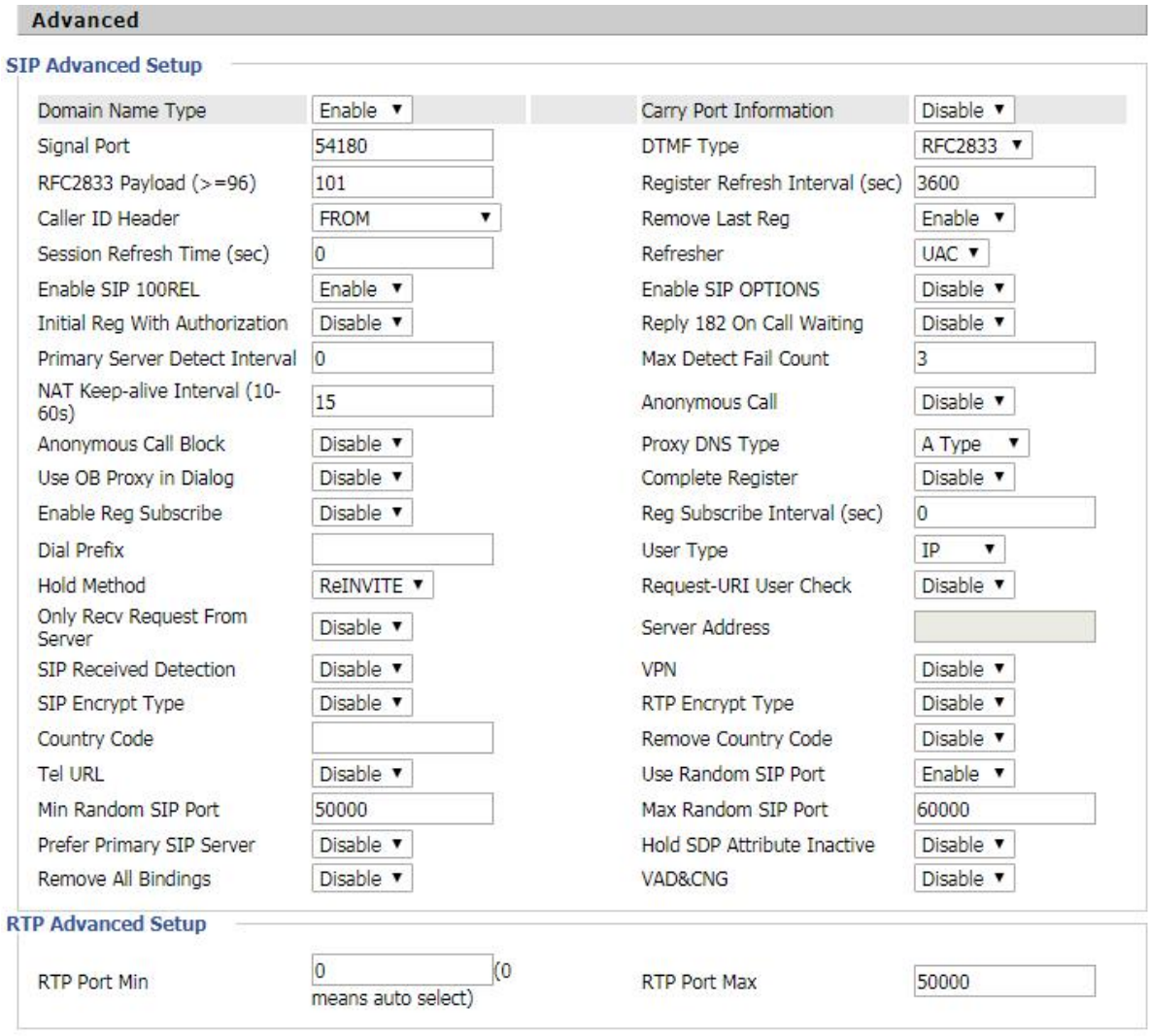
**Table 32** Supplementary service




| 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) |
| 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

**Table33** Advanced



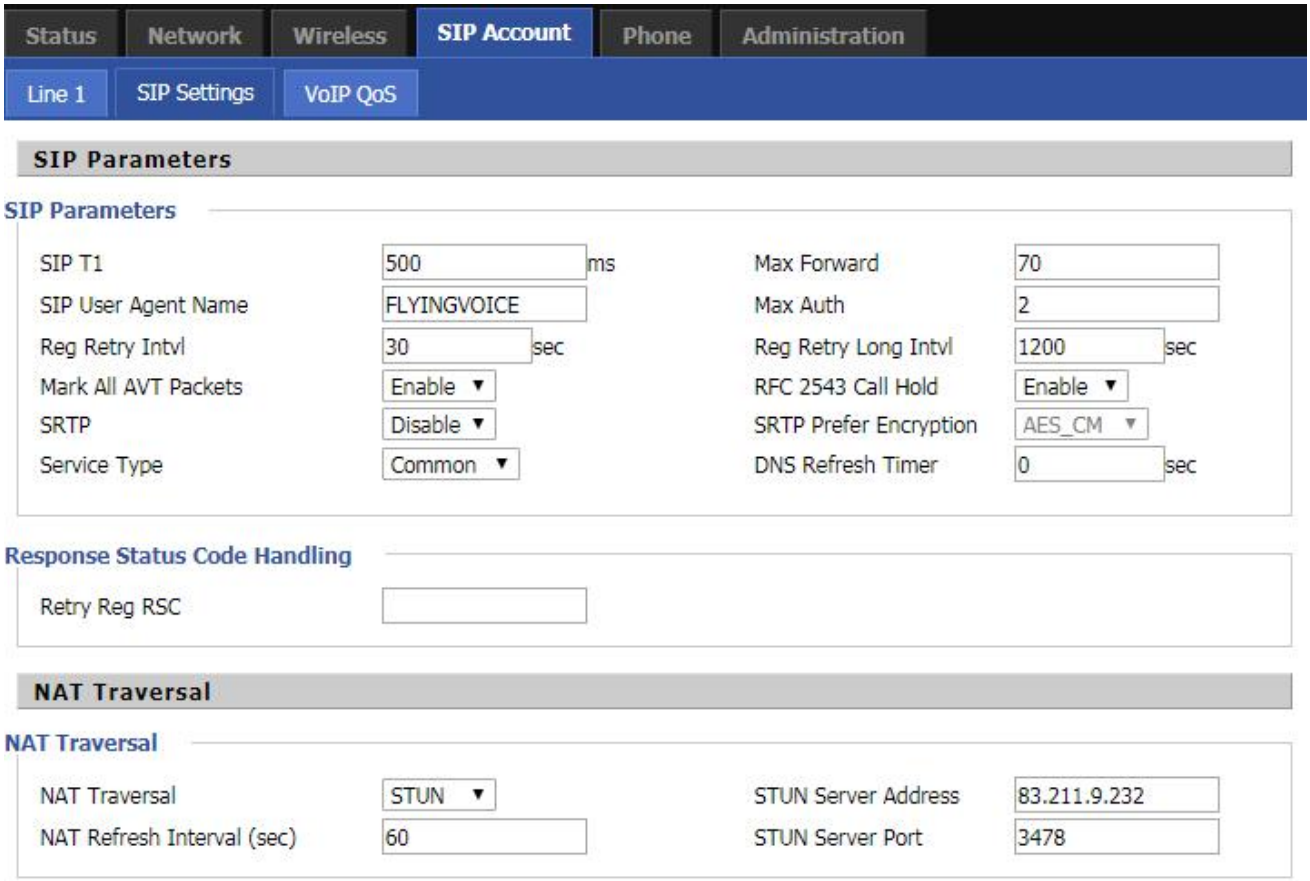

| Parameter name | Description |
|---|---|
| Domain Name Type | Whether to enable domain name recognition in SIP URIs |
| Carry Port Information | Whether to carry the SIP URI port information |
| Signal Port | The local port number of the SIP protocol |
| DTMF Type | Select the second way of dialing, optional items are In-band, RFC2833 and SIP Info. |
| RFC2833 Payload(>=96) | The user can use the default settings |
| Register Refresh Interval(sec) | The time interval between two normal registration messages. The user can use the default settings. |
| Caller ID Header | When enabled, an unregistered message will be sent before the registration is disabled, and no unregistered messages will be sent before registration; should be set according to the different server requirements |

| | |
|---|---|
| Remove Last Reg | Whether to remove the last registration message |
| Session Refresh Time(sec) | The interval between two sessions, the user can use the default settings |
| Refresher | Select Refresh from UAC and UAS |
| SIP 100REL Enable | If this option is enabled, the IP phone will send SIP-OPTION to the server instead of sending Hello messages on a regular basis. The interval for sending is the parameter set for the "NAT Hold Interval" parameter. |
| SIP OPTIONS Enable | Whether to open the SIP OPTION function |
| Initial Reg With Authorization | Whether to carry the certification information when registering |
| Reply 182 On Call Waiting | Whether or not to send 182 when the call is waiting |
| NAT Keep-alive Interval(10-60s) | The time interval for sending empty packets |
| Anonymous Call | Whether anonymous calls are enabled |
| Anonymous Call Block | Whether to enable anonymous call blocking |
| Proxy DNS Type | Set the DNS server type, the optional items are Type A, DNS SRV, and Auto |
| Use OB Proxy In Dialog | Whether the OB agent is used in the conversation |
| Complete Register | Whether to enable full registration |
| Reg Subscribe Enable | When enabled, the subscription message is sent after the registration message; the subscription message is not sent when disabled |
| Reg Subscribe Interval(sec) | Enable or disable the Reg Subscribe Interval |
| Dial Prefix | Dial before prefix |
| User Type | Whether the end user is IP or Phone |
| Hold Method | Call hold is REINVITE or INFO |
| Request-URI User Check | Whether to allow the user to check |
| Only Recv Request From Server | If enabled, will only accept requests from the server, do not accept other requests |
| Server Address | SIP server address |
| SIP Received Detection | Whether to allow SIP receive detection |
| VPN | Whether to enable VPN |
| SIP Encrypt Type | Whether to allow SIP message encryption |
| RTP Encrypt Type | Whether to allow RTP message encryption |
| Country Code | Country code |
| Remove Country Code | Whether to allow the removal of national codes |
| Tel URL | Whether to open the Tel URL |

| | |
|---|---|
| Use Random SIP Port | Whether to use the minimum random port |
| Min Random SIP Port | SIP minimum random port |
| Max Random SIP Port | SIP maximum random port |
| Prefer Primary SIP Server | Whether to enable the preferred primary server |
| Hold SDP Attribute Inactive | Whether to enable the call to keep the inactive attribute |
| RTP Port Min | RTP minimum port |
| RTP Port Max | RTP's maximum port |

# SIP Settings

**Table 23** SIP Settings

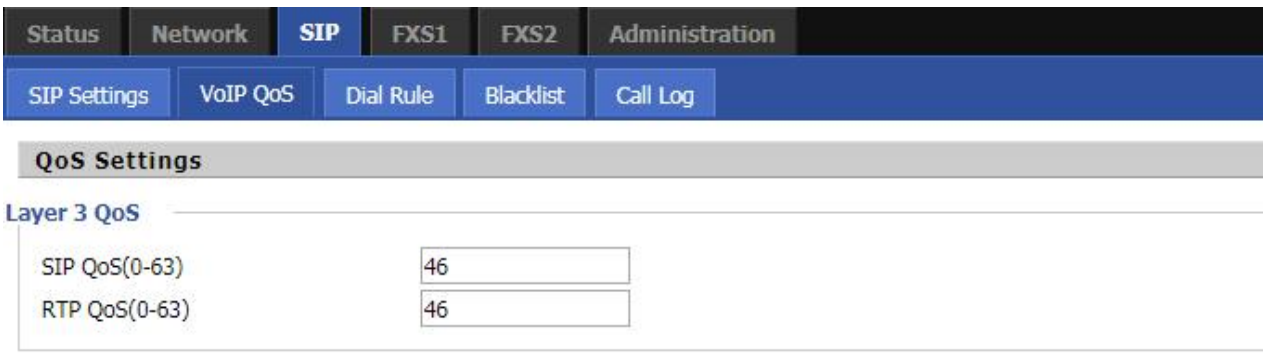



| Parameters name | Description |
|---|---|
| **SIP Parameters** | |
| SIP T1 | The default value is 500 |
| SIP User Agent Name | Enter the SIP User Agent header field |
| Max Forward | Modify the maximum hop value, the default is 70 |
| Max Auth | Change the number of authentication failures, the default value is 2 |

| | |
|---|---|
| Reg Retry Intvl | Registration failed again registration interval, default is 30 |
| Reg Retry Long Intvl | Registration failed Register again for the long interval Default 1200 |
| Mark All AVT Packets | The default enable is on |
| RFC 2543 Call Hold | The default enable is on |
| SRTP | The default is disabled |
| SRTP Prefer Encryption | Support for AES_CM and ARIA_CM |
| Service Type | Default general |
| DNS Refresh Timer | Modify the DNS refresh time, the default value of 0 |
| Transport | The transmission type defaults to UDP |
| **NAT Traversal** | |
| NAT Traversal | Whether to enable NAT mode, or select STUN to penetrate |
| STUN Server Address | STUN server IP address |
| NAT Refresh Interval(sec) | Refresh interval |
| STUN Server Port | STUN port, the default is 3478 |

## VoIP QoS

**Table 24** VoIP QoS



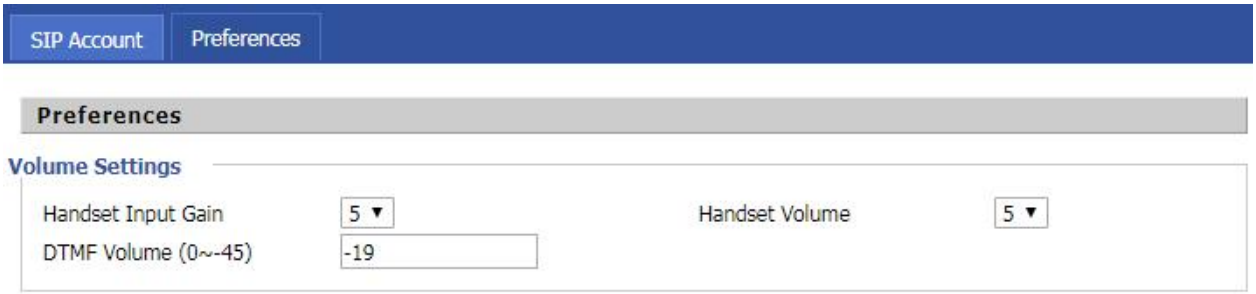

| Parameters name | Description |
|---|---|
| SIP QoS(0-63) | Defaults to 46,you can set a range of values is 0~63 |
| RTP QoS(0-63) | Defaults to 46,you can set a range of values is 0~63 |

# Phone

## Preferences

### Preferences

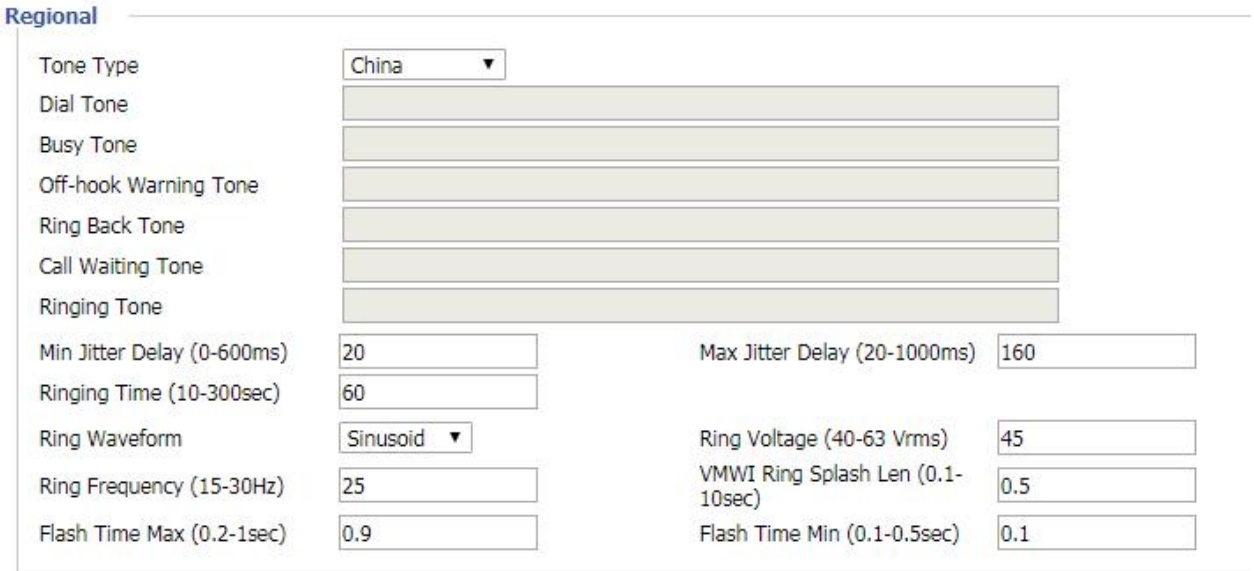
**Table 34** Preferences




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

### Regional

**Table 35** Regional

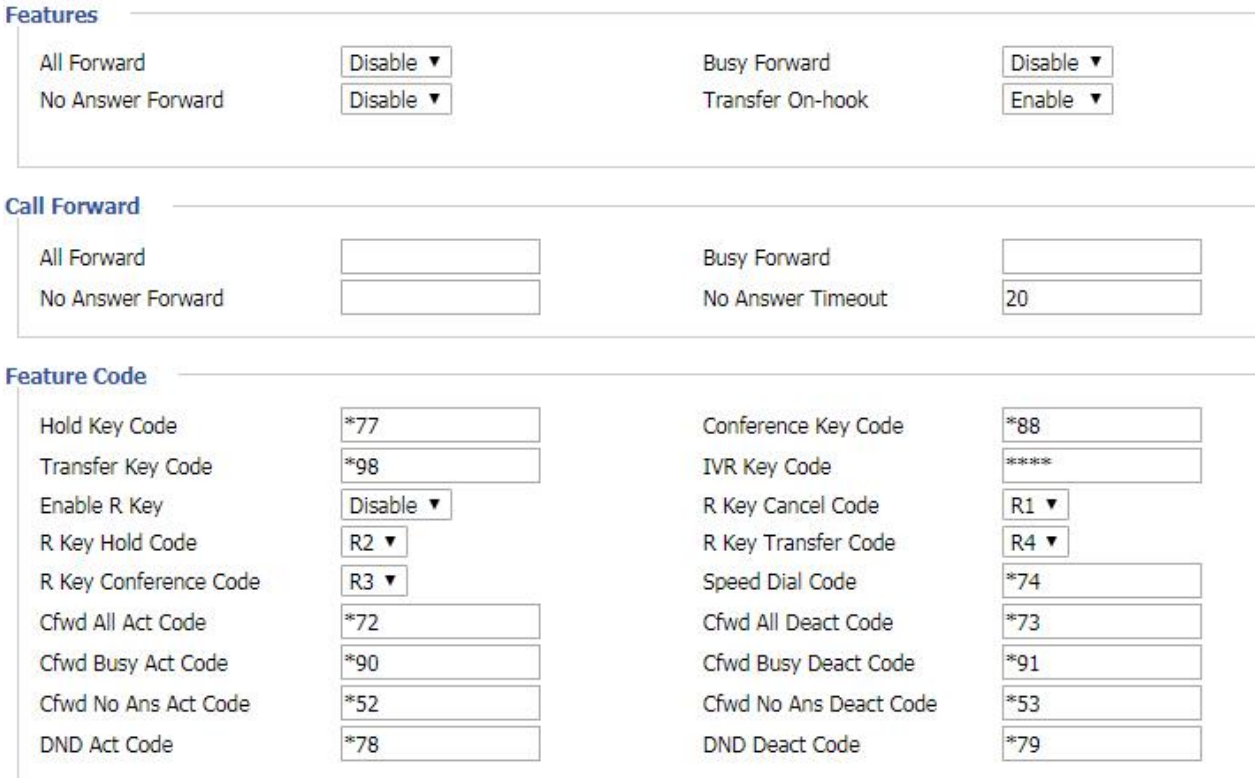



| | |
|---|---|
| Dial Tone | Dial Tone |
| Busy Tone | Busy Tone |
| Off Hook Warning | Off Hook warning tone |

| | |
|---|---|
| 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 FTA1101 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

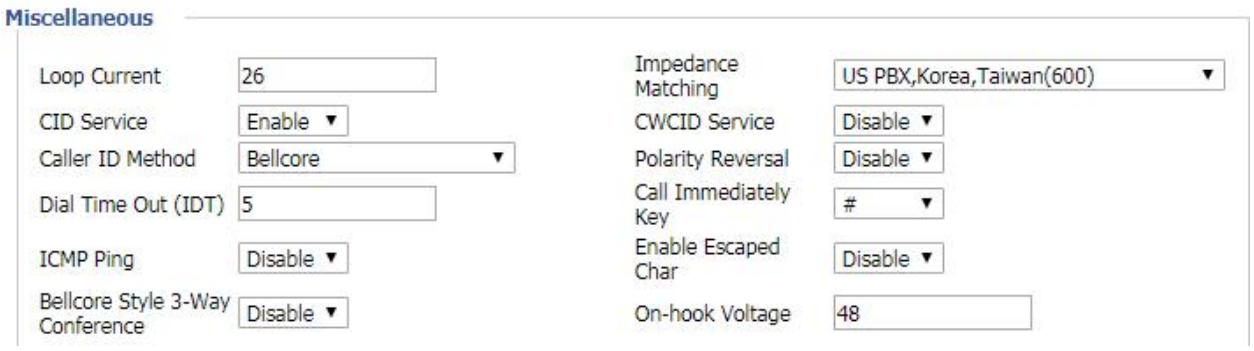
**Table 36** Features and call forward



| 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 code | Signature of the tripartite session, default is *88. |
| | Transfer key code | Call forwarding signatures, default is *98. |
| | IVR key code | Signatures of the voice menu, default is ****. |
| | R key enable | Enable/Disable R key way call features. |
| | R key cancel code | Set the R key cancel code, option are ranged from R1 to R9, default value is R1. |
| | R key hold code | Set the R key hold code, options are ranged from R1 to R9, default value is R2. |
| | R key transfer code | Set the R key transfer code, options are ranged from R1 to R9, default value is R4. |
| | R key conference code | Set the R key conference code, options are ranged from R1 to R9, default value is R3. |
| | R Key Reject 2nd Call Code | Set the R key Reject 2nd Call code, options are ranged from R1 to R9, default value is R0. |
| | Speed Dial Code | Speed dial code, default is *74. |

## Miscellaneous

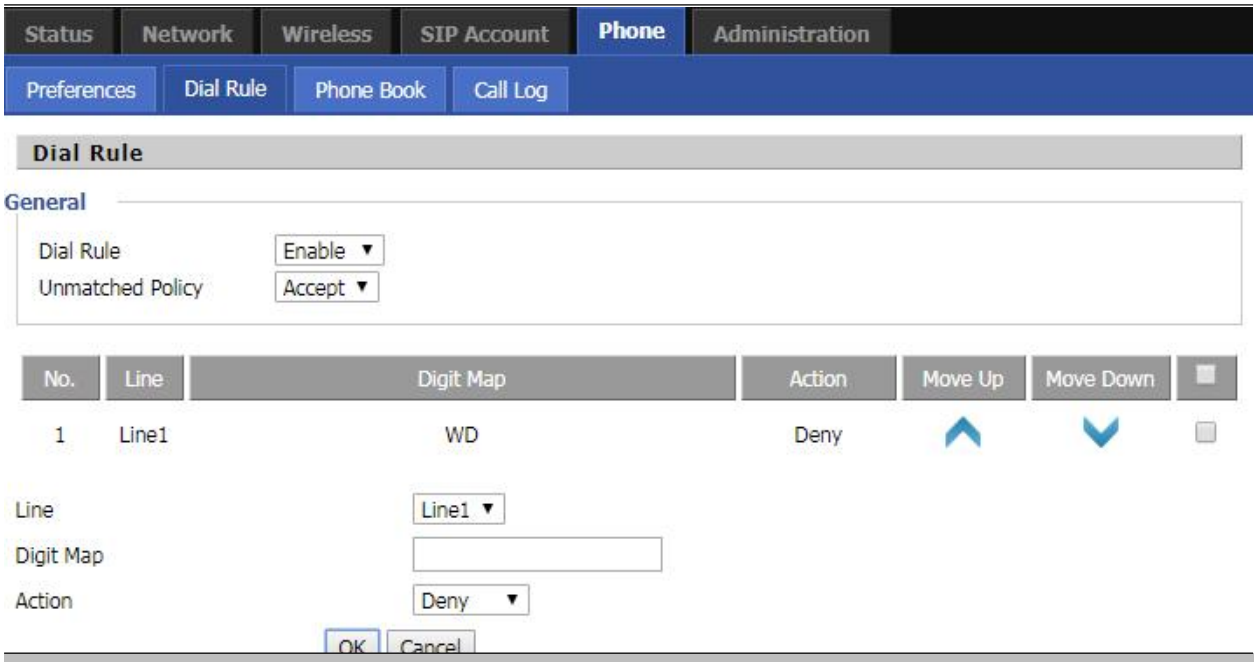
**Table 37** Miscellaneous




| 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.<br>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 # |

# Dial Rule

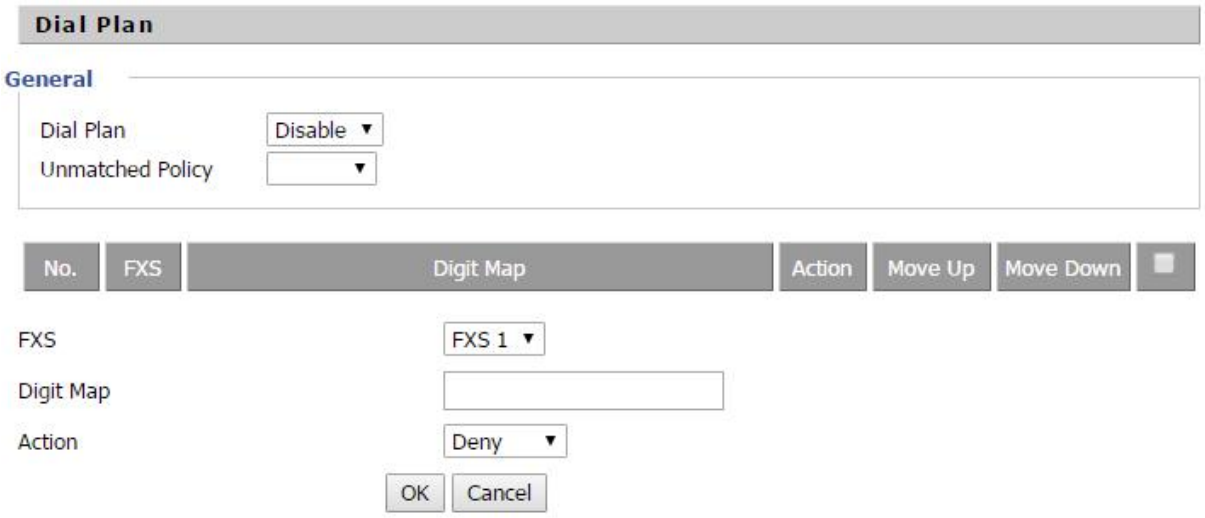
**Table 25** Dial Plan




| Field Name | Description |
|---|---|
| Dial Plan | Enable/Disable dial plan. |
| Line | Set the line. |
| Digit Map | Enter the sequence used to match input number<br>The syntactic, please refer to the following Dial Plan Syntactic. |
| Action | Choose the dial plan mode from Deny and Dial Out.<br>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 26** 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 40** Dial Plan Syntactic

| No. | String | Description |
|---|---|---|
| 1 | 0 1 2 3 4 5 6 7 8 9 * # | Allowed characters |
| 2 | x | Lowercase letter x stands for one legal character |
| 3 | [sequence] | To match one character form sequence. For example:<br>[0-9]: match one digit form 0 to 9<br>[23-5*]: match one character from 2 or 3 or 4 or 5 or *<br>$x^0$ $x^1$ $x^2$ $x^3$ $x^n$ |
| 4 | x. | Match to , , , …...<br>For example:<br>“01.”:can match ”0”, “01”, “011”, ”0111”, ……..,” 01111…” |

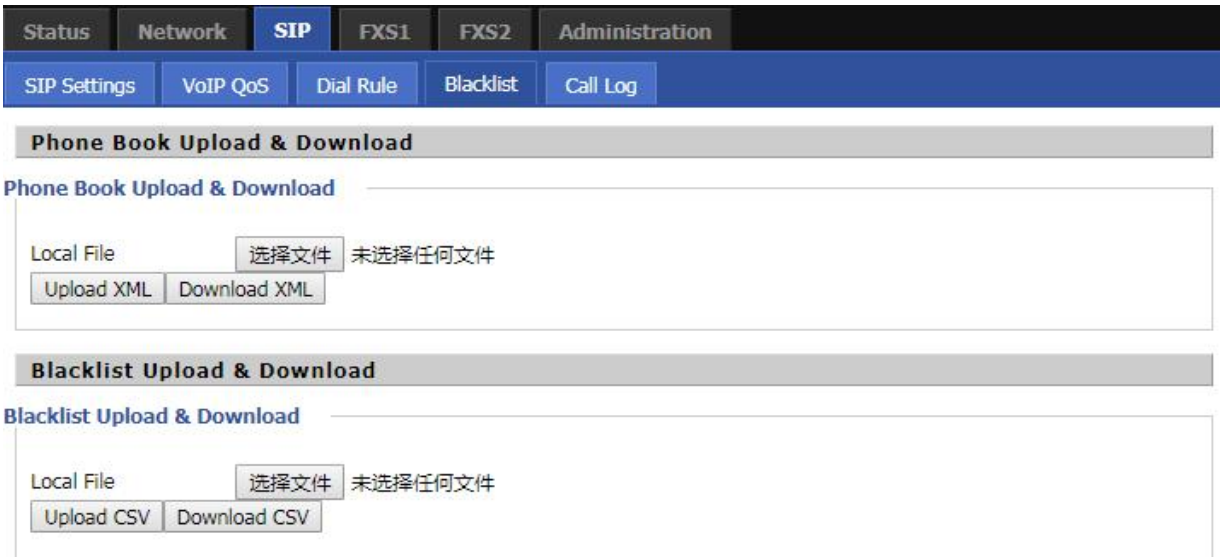
| | | |
|---|---|---|
| 5 | <dialed:substituted> | Replace dialed with substituted. For example：<br><8:1650>123456：input is “85551212”, output is “16505551212” |
| 6 | x,y | Make outside dial tone after dialing “x”, stop until dialing character “y”<br>For example：<br>“9,1xxxxxxxxx”:the device reports dial tone after inputting “9”, stops tone until inputting “1”<br>“9,8,010x”: make outside dial tone after inputting “9”, stop tone until inputting “0” |
| 7 | T | Set the delayed time. For example:<br>“<9:111>T2”: The device will dial out the matched number “111” after 2 seconds. |

# Blacklist

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

## Upload or download Phonebook/blacklist file

**Table 28** Blacklist




Steps:

1.Click 选择文件 ,select a locally stored phonebook.

2.There will be a tips after select successfully.

3.Click Upload XML, begin upload.

4.Click Download XML ,begin download

# Call Log

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

**Table 29** Call log

Redial Calls

**Redial List**

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

Answered Calls

**Answered Calls**

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

Missed Calls

**Missed Calls**

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

# 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

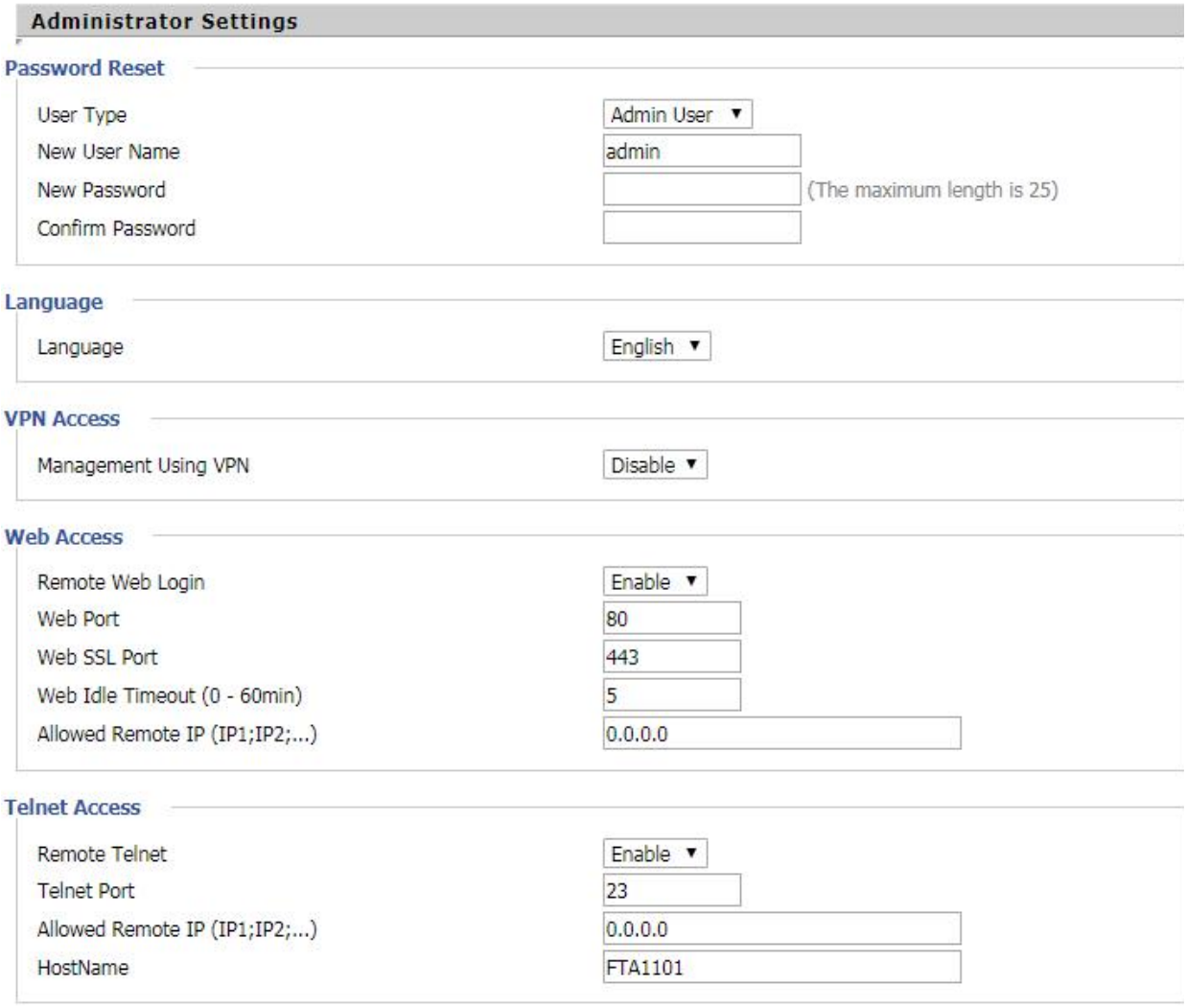
### Save config file

**Table 38** 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 39** Administrator settings

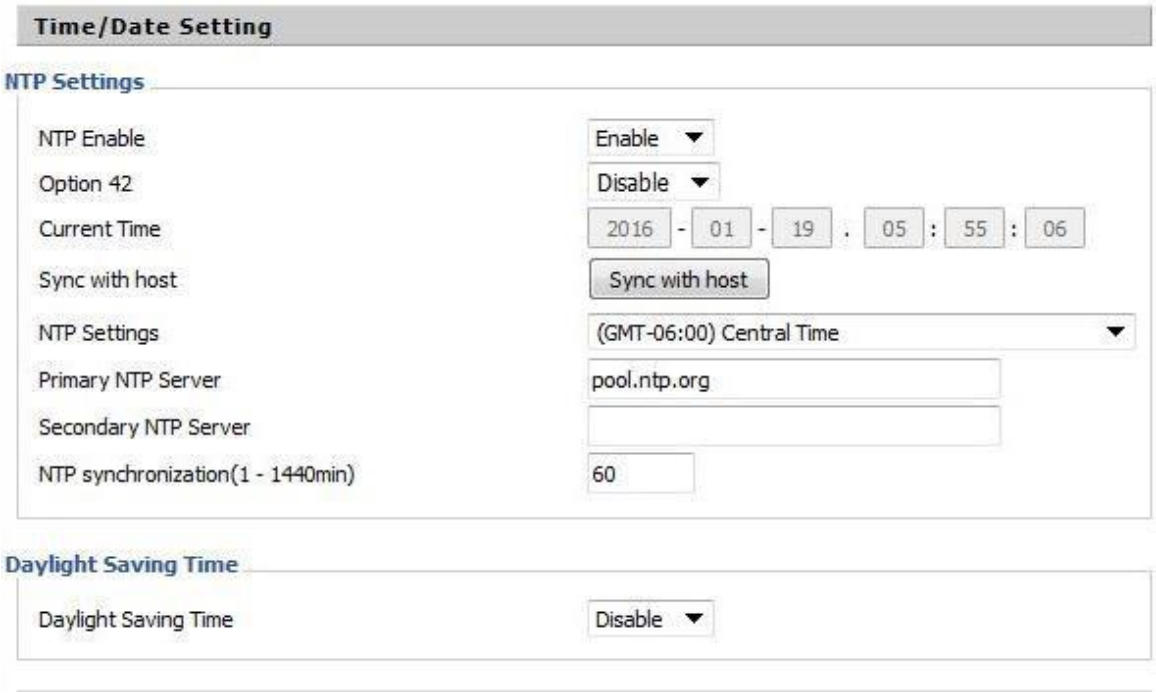



| Field Name | Description |
|---|---|
| User type | Choose the user type from admin user and normal user and basic user |
| New User Name | You can modify the user name, set up a new user name |
| New Password | Input the new password |
| Confirm Password | Input the new password again |
| Language | 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

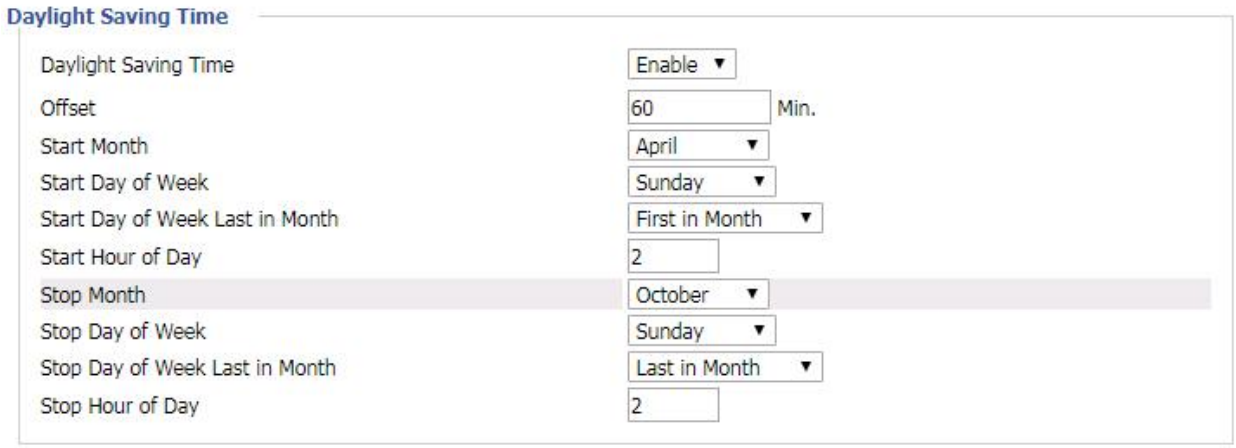
**Table 40** NTP settings




| 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 41** Daylight Saving Time




**Procedure**

Step 1. Enable Daylight Savings Time.

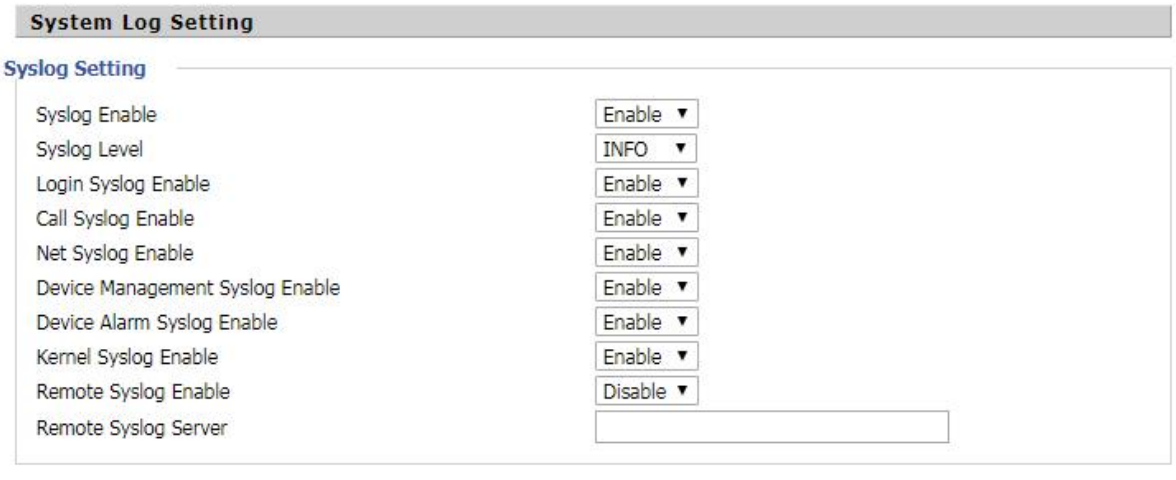
Step 2. Set value of offset for Daylight Savings Time

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 60** 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 |

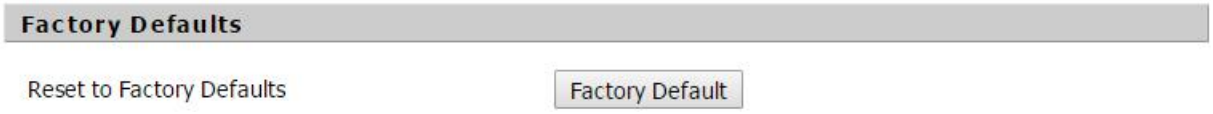
# Factory Defaults Setting

**Table 43** Factory Defaults Setting


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

# Factory Defaults

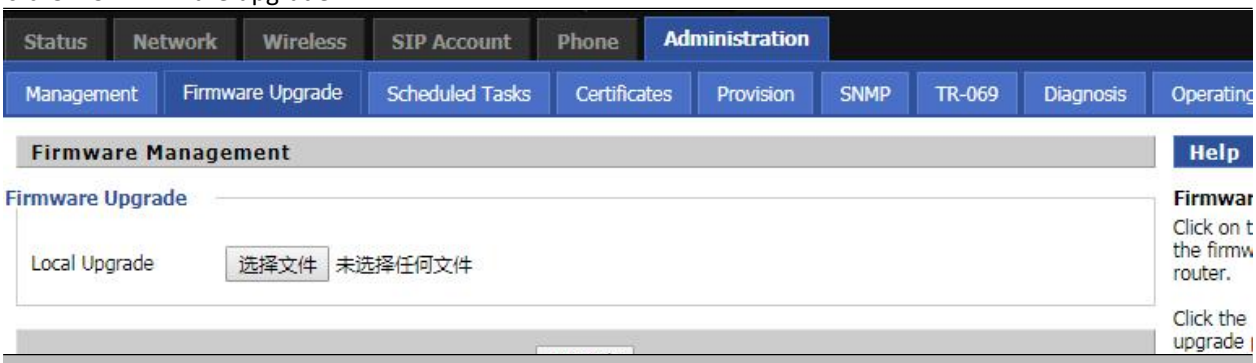
**Table 44** Factory Defaults




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

# Firmware Upgrade

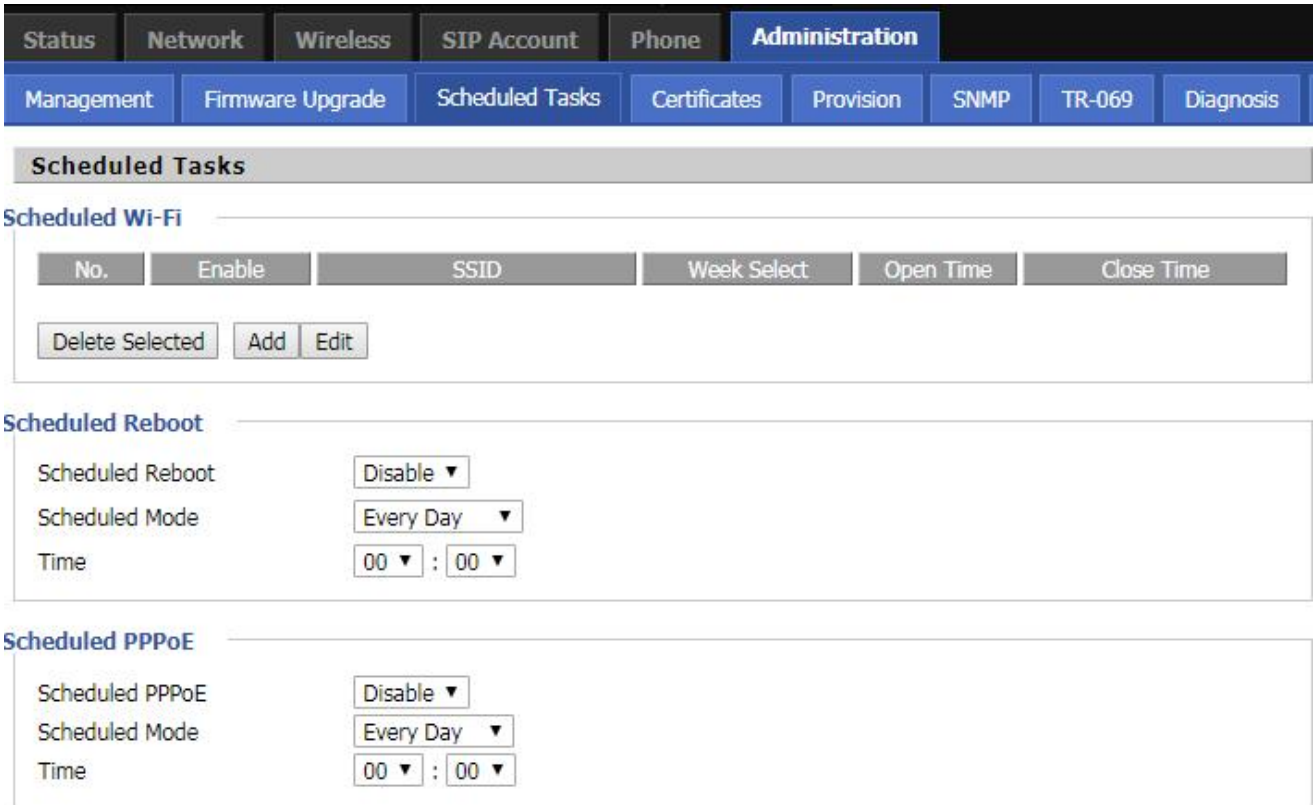
**Table 45** Firmware upgrade




| 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 |

# Scheduled Tasks

**Table 46** Scheduled Tasks




| Field Name | Description |
|---|---|
| **Scheduled Reboot** | |

| | |
|---|---|
| Scheduled Reboot | Enable/Disable scheduled Reboot |
| Scheduled Mode | Select scheduled Mode |
| Time | Set the time to restart |
| **Scheduled PPPoE** | |
| Scheduled PPPoE | Enable/Disable scheduled PPPoE |
| Scheduled Mode | Select scheduled Mode |
| Time | Set the time to start PPPoE |

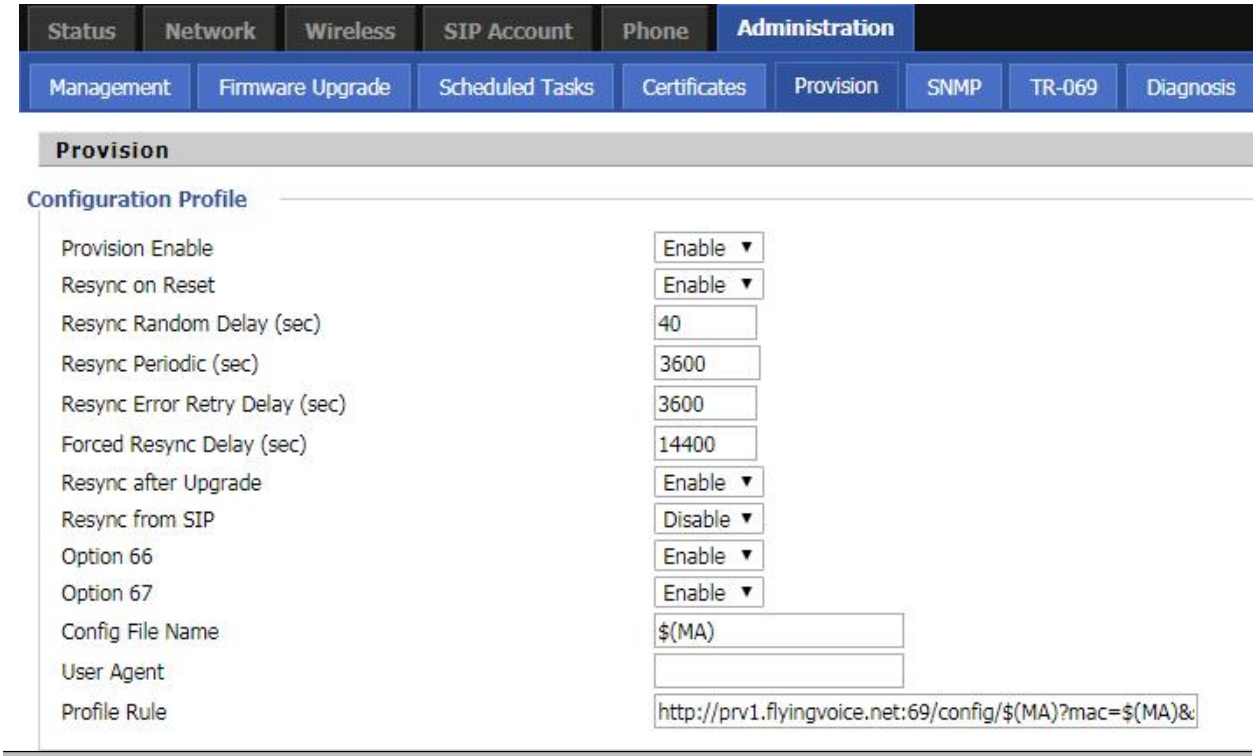
# Provision

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.

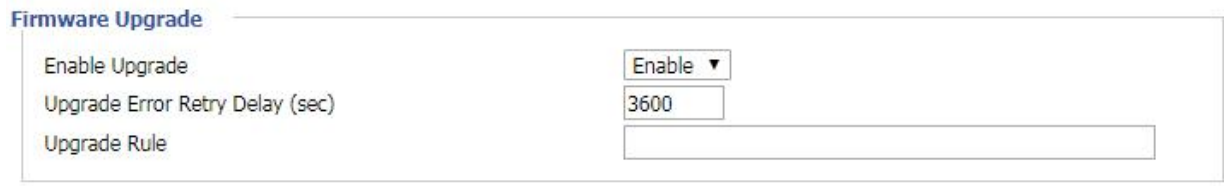
**Table 47** Provision




| Field Name | Description |
|---|---|
| Provision Enable | Enable provision or not. |

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

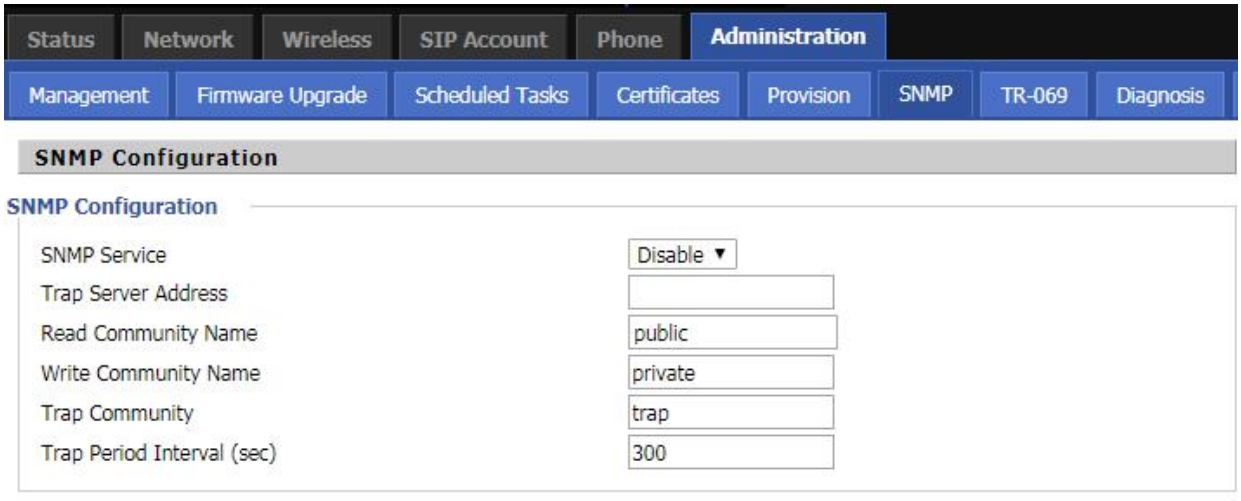
**Table 48** Firmware Upgrade




| 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 49** 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 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 |

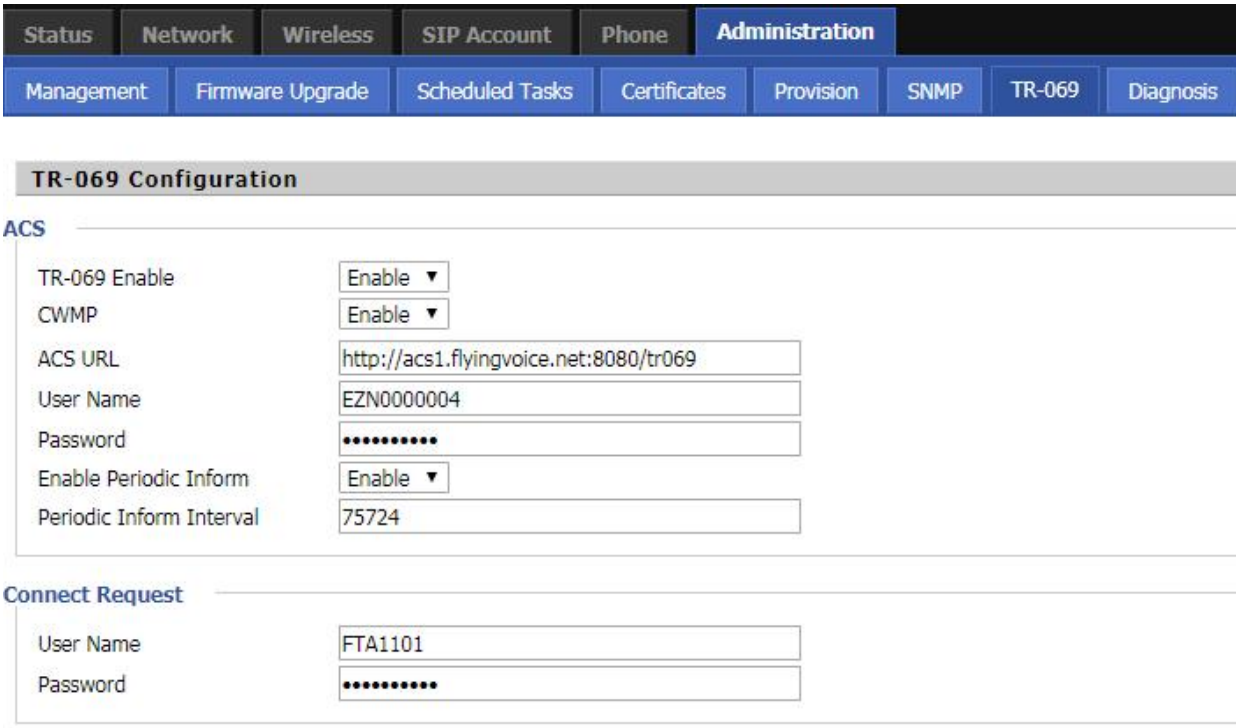
# TR-069

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 67** TR069



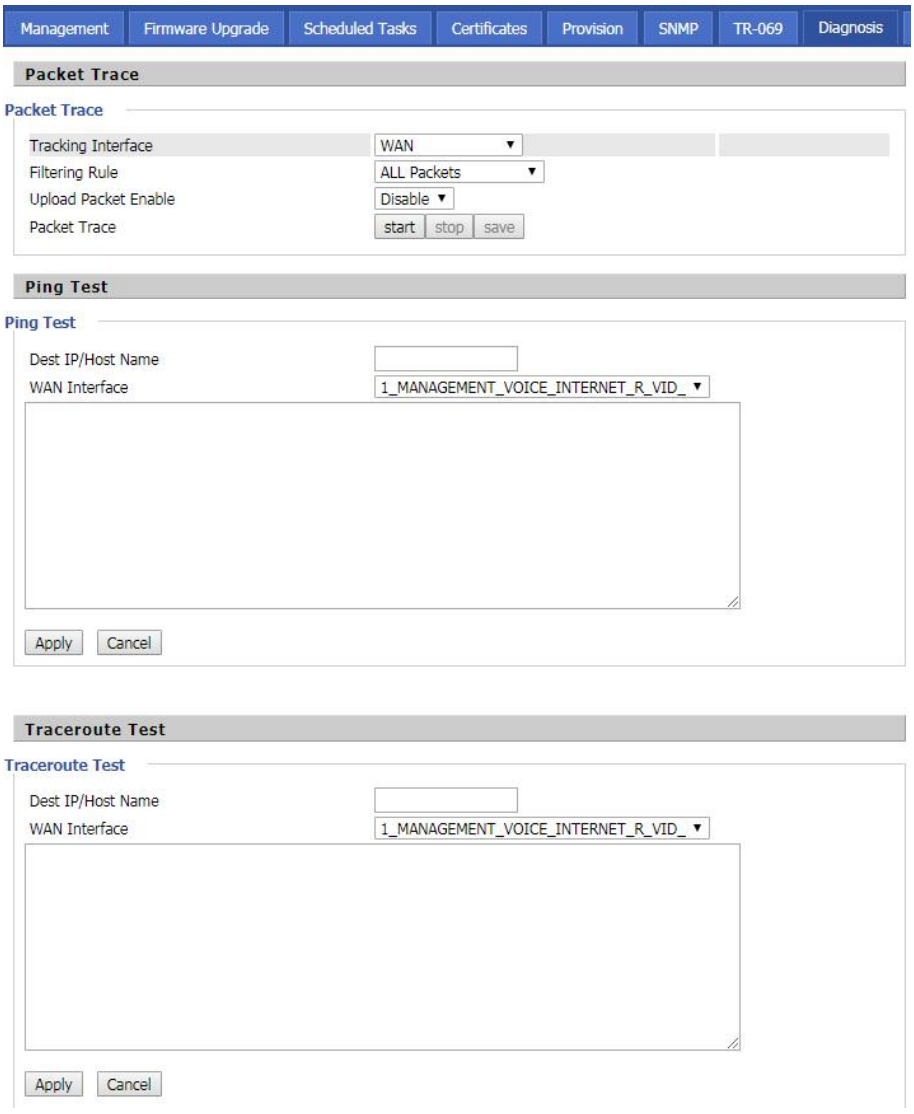

| Field Name | Description |
|---|---|
| **ACS parameters** | |

| | |
|---|---|
| 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 the function of periodic inform or not. By default it is Enabled |
| Periodic Inform | 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 51** Diagnosis



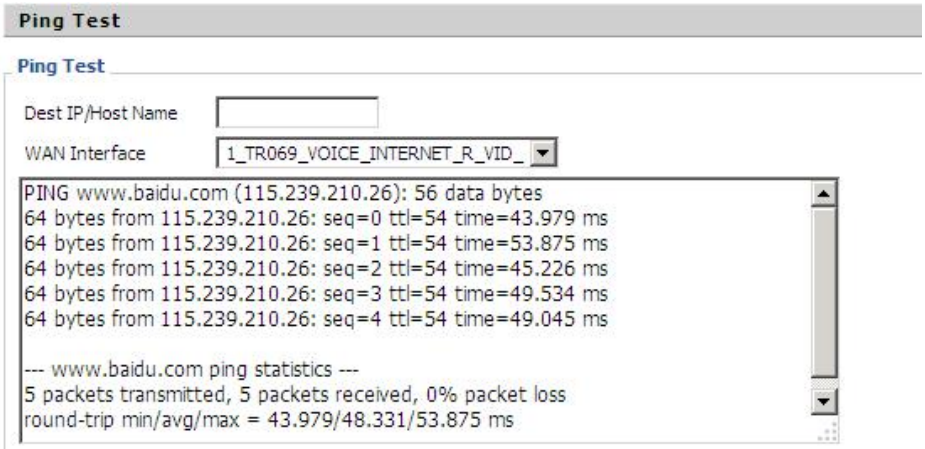
## Description

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.

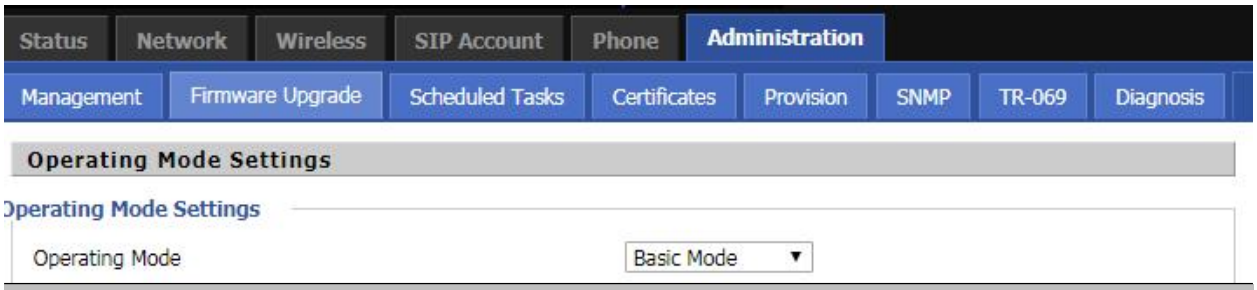



3. Traceroute Test

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

# Operating Mode

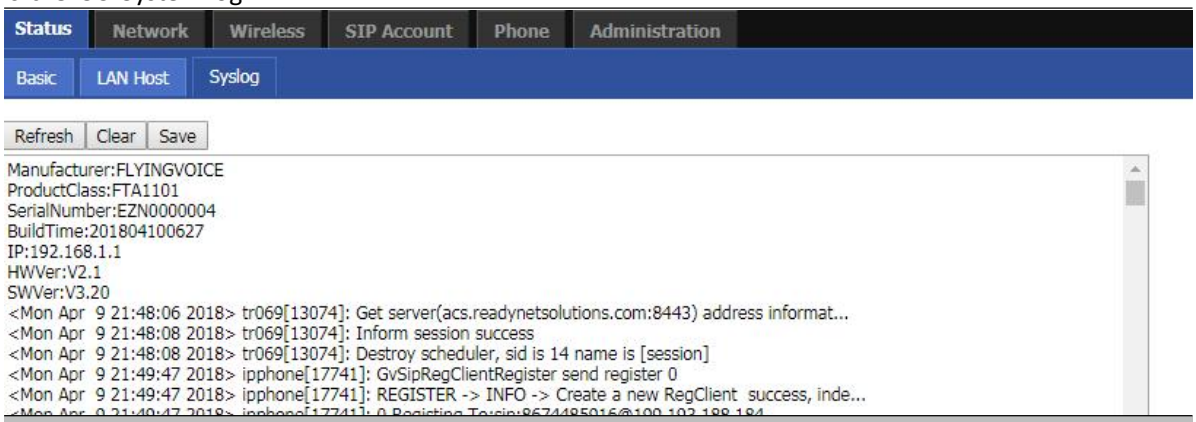
**Table 52** Operating mode




| Description |
|---|
| Choose the Operation Mode as Basic Mode or Advanced Mode |

# System Log

**Table 53** System log




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

# Logout

**Table 54** Logout


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

# Reboot

Press the  button to reboot the device.

# Chapter 5 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

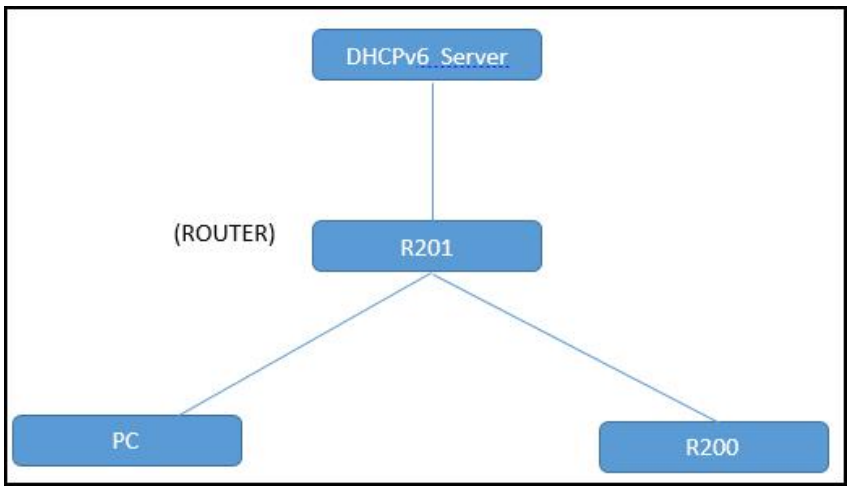
# Introduction

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 55** IPv6 Modes

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

# IPv6 Advance

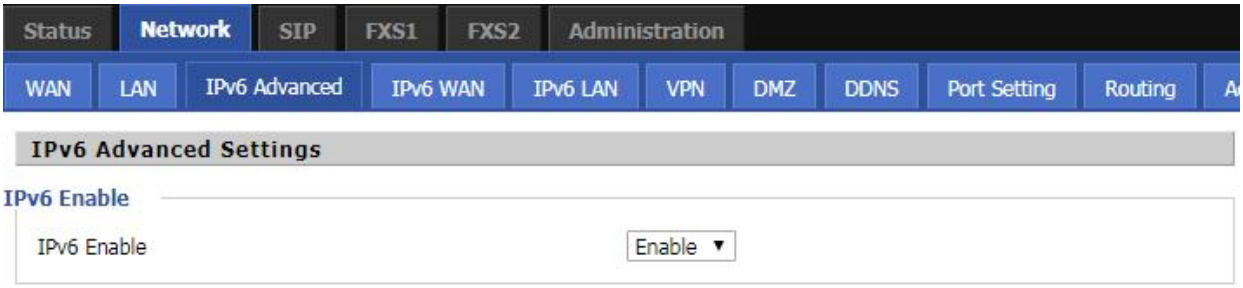
To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

**Table 56** Enabling IPv6




# Configuring IPv6

## Configuring Statefull IPv6

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

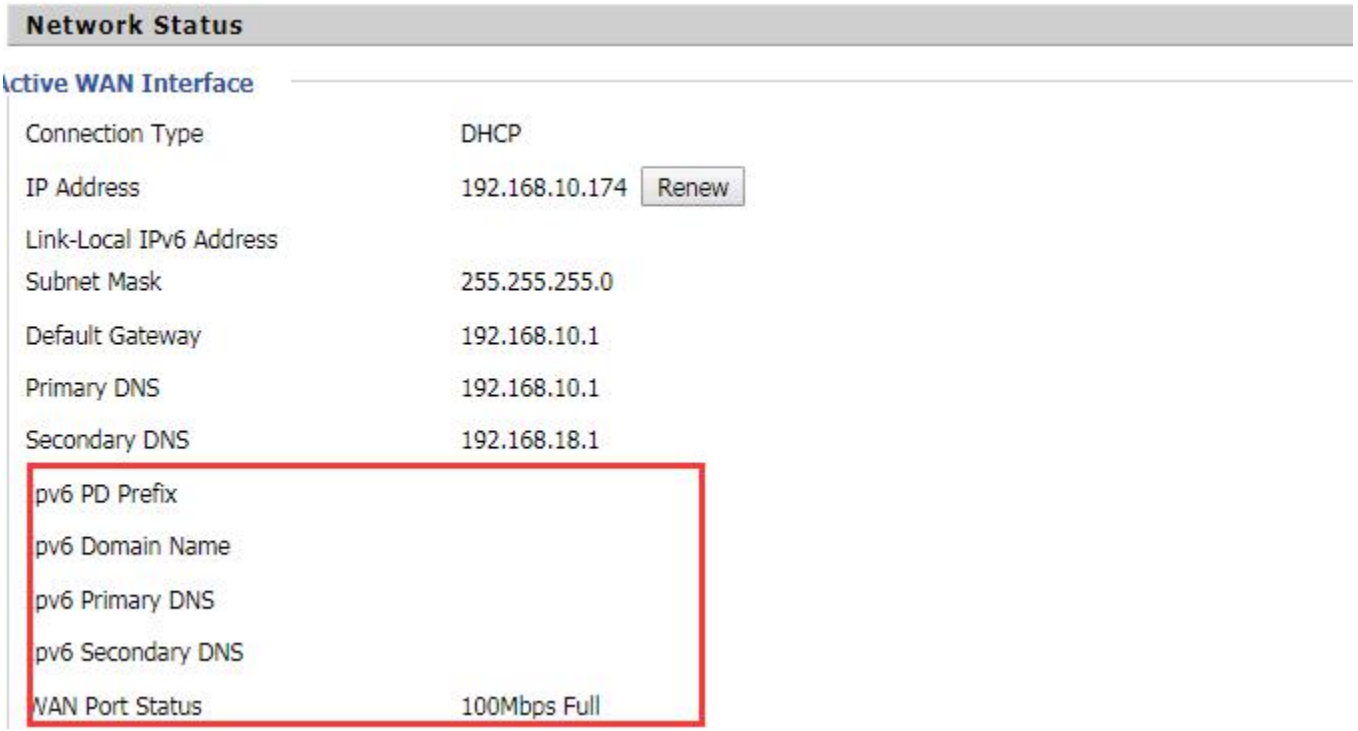
**Table 57** Configuring Statefull IPv6


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

# Viewing WAN port status

To view the status of WAN port:

Navigate to Status page.

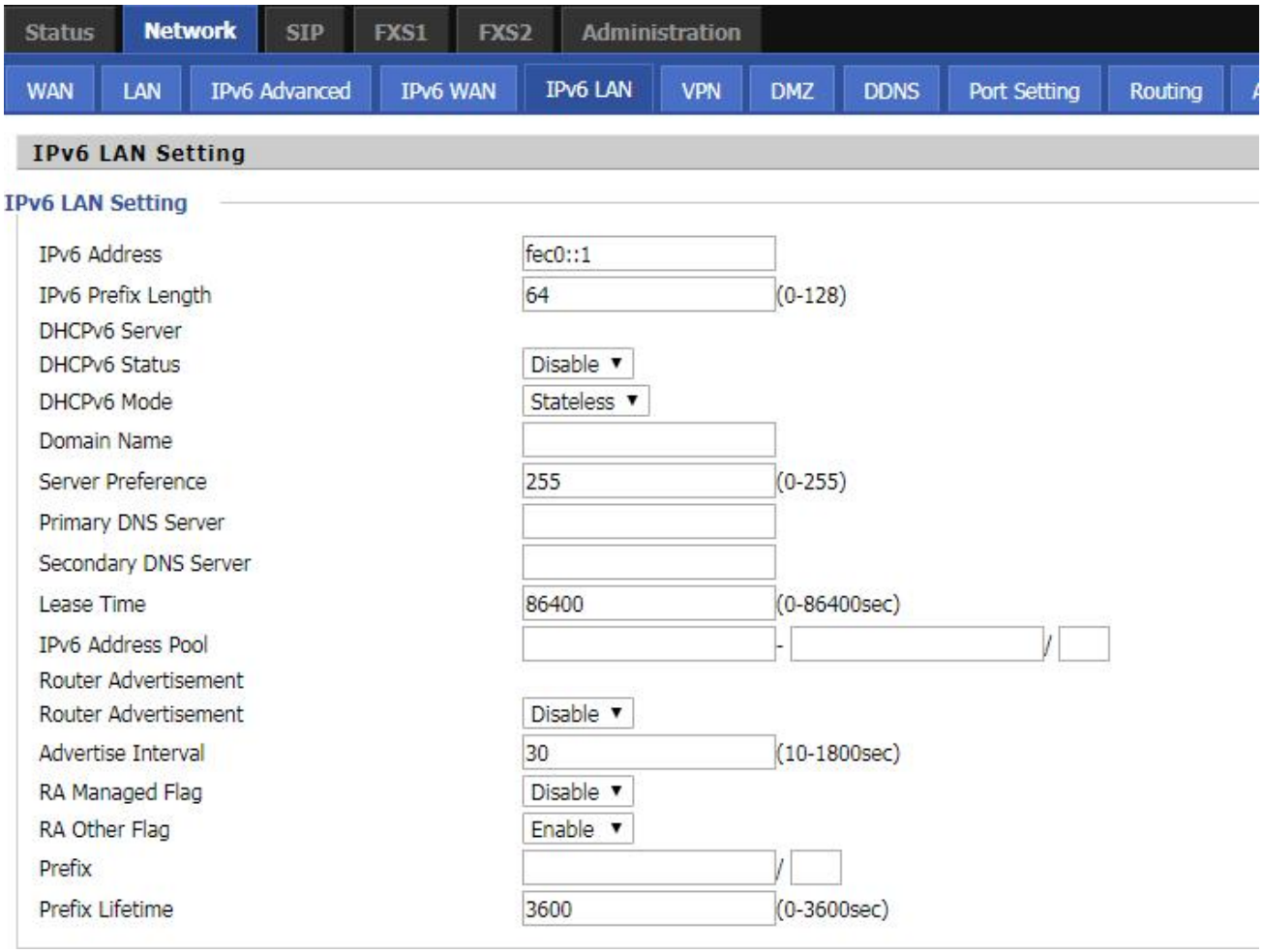



# IPv6 DHCP configuration for LAN/WLAN clients

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.

, 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 6 Troubleshooting Guide

This chapter covers:

# Configuring PC to get IP Address automatically

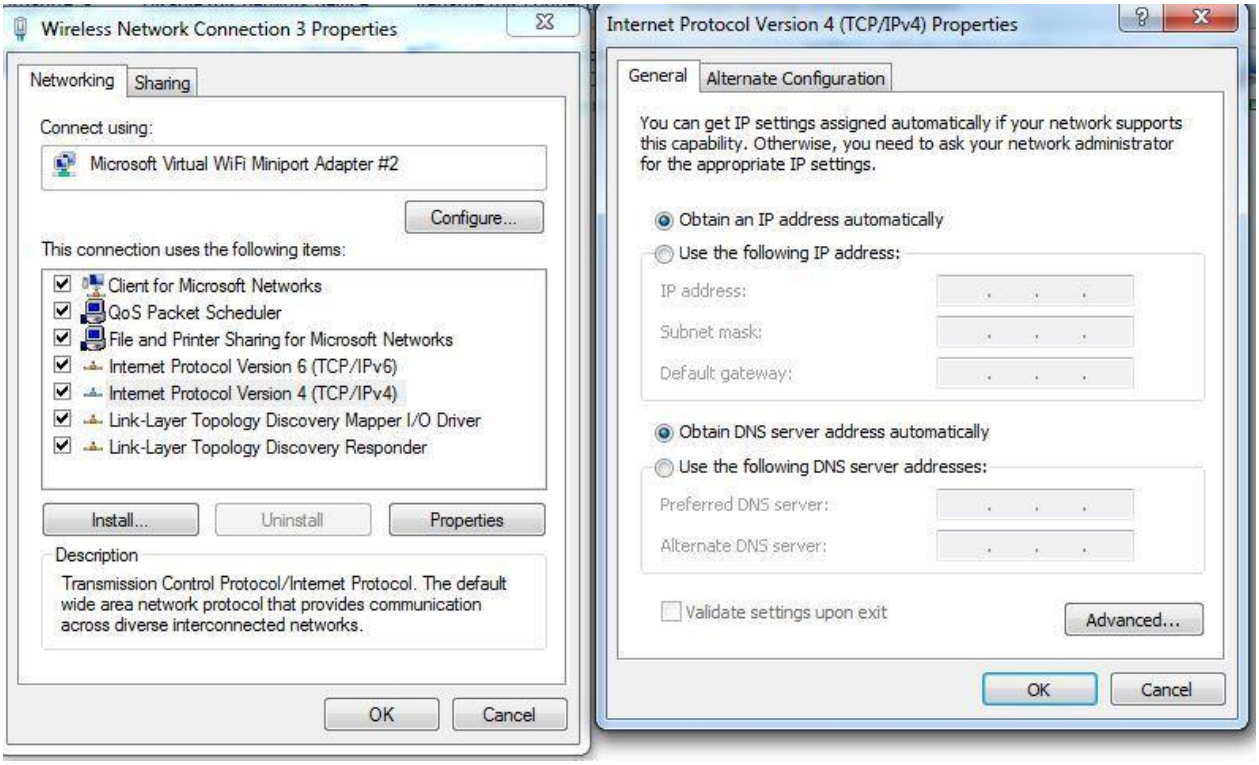
Follow the below process to set your PC to get an IP address automatically:

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.