



User Manual FWR9402/FWR9502

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 |
| Class B Digital Device or Peripheral | 4 |
| Warnings and notes | 5 |
| Warnings | 5 |
| Notes | 5 |
| Chapter 1:Product description | 6 |
| FWR9405/FWR9502 | 7 |
| LED Indicators and Interfaces | |
| Hardware Installation | 11 |
| Voice Prompt | 13 |
| | |
| Chapter 2:Configuring Basic Settings | |
| Chapter 2:Configuring Basic Settings Two-Level Management | |
| | |
| Two-Level Management | 19 19 |
| Two-Level Management Web Management Interface | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. | 19 |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). Making a Call. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). Making a Call. Chapter 3:Web Interface. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). Making a Call. Chapter 3:Web Interface. Login. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). Making a Call. Chapter 3:Web Interface. Login. Status. | |
| Two-Level Management. Web Management Interface. Web Management Interface Details. Setting the Time Zone. Configuring an Internet Connection. Setting up Wireless Connections. Configuring Session Initiation Protocol (SIP). Making a Call. Chapter 3:Web Interface. Login. Status. Network and Security. | |
| Two-Level Management | |

| Wireless 5G | |
|---|-----|
| SIP | |
| FXS1 | |
| FXS2 | |
| Security | 87 |
| Application | |
| Storage | |
| Administration | |
| Management | |
| Firmware Upgrade | |
| Provision | |
| SNMP | |
| TR-069 | |
| Diagnosis | 106 |
| Operating Mode | |
| System Log | |
| Logout | |
| Reboot | |
| Chapter 4:IPv6 address configuration on WAN interface | 110 |
| Introduction | |
| IPv6 Advance | |
| Configuring IPv6 | |
| Viewing WAN port status | |
| IPv6 DHCP configuration for LAN/WLAN clients | 115 |
| LAN DHCPv6 | |
| Chapter 5:Troubleshooting Guide | 117 |
| Configuring PC to get IP Address automatically | |
| Cannot connect to the Web | |
| Forgotten Password | |

Tables

| Table 1 Features at-a-glance | 7 |
|---|----|
| Table 2 LED Indicators | 8 |
| Table 3 Interface | 10 |
| Table 4 Voice Menu Setting Options | 13 |
| Table 5 Web management interface | |
| Table 6 Setting time zone | |
| Table 7 Configuring an internet connection | |
| Table 8 Wireless > Basic web page (user view) | 25 |
| Table 9 Wireless Security web page | |
| Table 10 Configuring SIP the Web Management Interface | |
| Table 11 Registration status | |
| Table 12 Login details | |
| Table 13 Status Page | |
| Table 14 Internet | |
| Table 15 DHCP | 39 |
| Table 16 PPPoE | 40 |
| Table 17 Bridge Mode | |
| Table 18 LAN port | 44 |
| Table 19 DHCP server settings | 46 |
| Table 20 DHCP server, DNS and Client Lease Time | |
| Table 21 VPN | 47 |
| Table 22 Port Forward | |
| Table 23 VLAN | 49 |
| Table 24 DMZ | 50 |
| Table 25 QoS | |
| Table 26 Rate Limit | 51 |
| Table 27 Port setting | 52 |
| Table 28 Routing | 52 |
| Table 29 Advance | 53 |
| Table 30 Basic | 54 |
| Table 31 Wireless security | 57 |
| Table 32 WiFI Security Setting | 58 |

| Table 33 WPA-PSK | |
|------------------------------------|----|
| Table 34 WPAPSKWPA2PSK | |
| Table35 Wireless Access Policy | 60 |
| Table 36 WMM | 61 |
| Table 37 WDS | |
| Table 38 WPS | |
| Table 39 Station info | |
| Table 40 Advanced | |
| Table 41 SIP settings | |
| Table 42 VoIP QoS | |
| Table 43 Parameters and settings | |
| Table 44 Adding one dial plan | |
| Table 45 Dial Plan | 72 |
| Table 46 Blacklist | |
| Table 47 Call log | |
| Table 48 SIP Account -Basic | |
| Table 49 Audio configuration | 77 |
| Table 50 Supplementary service | |
| Table 51 Advanced | |
| Table 52 Volume settings | |
| Table 53 Regional | |
| Table 54 Features and call forward | |
| Table 55 Miscellaneous | |
| Table 56 Filtering setting | |
| Table 57 Content filtering | |
| Table 58 Advance NAT | |
| Table 59 UPnP | |
| Table 60 IGMP | |
| Table 61 Disk Management | |
| Table 62 FTP Setting | |
| Table 63 Smb setting | |
| Table 64 Save Config File | |
| Table 65 Administrator settings | |
| Table 66 NTP settings | |
| Table 67 Daylight Saving Time | |
| Table 68 System log Setting | |
| Table 69 Factory Defaults Setting | |
| Table 70 Factory Defaults | |
| Table 71 Firmware upgrade | |

| 101 |
|-----|
| 102 |
| 103 |
| 104 |
| 106 |
| 108 |
| 109 |
| 109 |
| 111 |
| 112 |
| 113 |
| 114 |
| |

About This User Guide

Thank you for choosing FWR9402/FWR9502 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 FWR9402/FWR9502 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 FWR9402/FWR9502 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.FWR9402/FWR9502 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

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



Warning

Changes or modifications to this unit not expressly approved by the party responsible for compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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:

- FWR9402/FWR9502
- LED Indicators and Interfaces
- Hardware Installation
- Voice Prompt

FWR9402/FWR9502

Table 1 Features at-a-glance

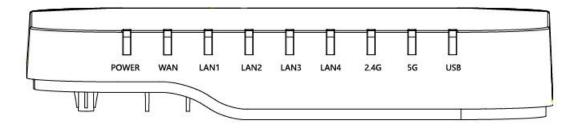
| Port/Model | FWR9402 | FWR9502 | |
|-----------------|--|--|--|
| picture | FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF | | |
| WAN | 1 | 1 | |
| LAN | 4 | 4 | |
| FXS | 2 | 2 | |
| USB | yes yes | | |
| Speed limit NAT | yes yes | | |
| Ethernet | 5* RJ45 | 5* RJ45 | |
| interface | 10/100M/1000M | 10/100M/1000M | |
| Fax | T | .30, T.38 Fax | |
| WiFi | 2.4G 2T2R (300Mbps) | 2.4G 4T4R(600Mbps) | |
| | 5G 2T2R (867Mbps) | 5G 4T4R(1700Mbps) | |
| 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 | ED Ind | licators |
|---------|--------|----------|
|---------|--------|----------|

| 4 | ۲ | ٩ | 2 | 4 | 2.4G | 50 | (3) | (3) | |
|---|---|---|---|---|------|----|-------------|-----|--|
| | | | | | | | | | |

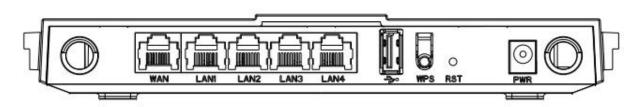
| LED | Status | Explanation |
|------------|------------------|--|
| PHONE1/2 | Blinking (Green) | Not registered |
| PHONE1/2 | On (Green) | Registered |
| | On (Green) | The port is connected with 5G |
| 5G | Off | The port is disconnected |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 2.4G |
| 2.4G | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 1000Mbps. |
| LAN1/2/3/4 | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 1000Mbps. |
| WAN | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green | Wireless access point is ready. |
| WLAN | Blinking (Green) | It will blink while wireless traffic goes through. |
| | Off | The system is not powered on or the WIFI switch is off |
| DOWER | On (Green) | The router is powered on and running normally. |
| POWER | Off | The router is powered off. |



| LED | Status | Explanation |
|------------|------------------|--|
| PHONE1/2 | Blinking (Green) | Not registered |
| PHONEI/2 | On (Green) | Registered |
| | On (Green) | The port is connected with 5G |
| 5G | Off | The port is disconnected |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 2.4G |
| 2.4G | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 1000Mbps. |
| LAN1/2/3/4 | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green) | The port is connected with 1000Mbps. |
| WAN | Off | The port is disconnected. |
| | Blinking (Green) | It will blink while transmitting data. |
| | On (Green | Wireless access point is ready. |
| WLAN | Blinking (Green) | It will blink while wireless traffic goes through. |
| | Off | The system is not powered on or the WIFI switch is off |
| POWER | On (Green) | The router is powered on and running normally. |
| POWER | Off | The router is powered off. |

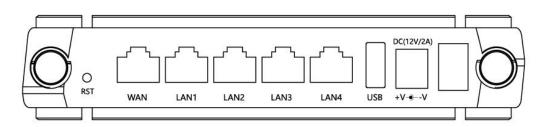
Table 3 Interfaces

FWR9502



| 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 |
| RESET | Restore the factory settings button, press and hold the device after 5s to restore the |
| | factory settings |

FWR9402



| 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 |
| 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 | Menu Navigation |
|------------|---|
| code | |
| | 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 |
| 1 | use phone keypad to enter password directly |
| (1) | For example: WEB login password is "admin", so the password in IVR is |
| WAN Port | "admin". The user may "23646" to access and then configure the WAN |
| Connection | connection port. The unit reports "Operation Successful" if the password is |
| Туре | 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 "*" |

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

| | 1. Pick up phone and press "****" to start IVR |
|---------------|--|
| | 2. Choose "5", and the router reports current DNS |
| (5) | 3. Input the new DNS and press # key: |
| DNS | 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 | 1. Pick up phone and press "****" to start IVR |
| phone port | 2. Select "2", then the device will continue to broadcast prompts the user to select |
| configuration | 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. |
| | 1. Pick up phone and press "****" to start IVR |
| | 2. Choose "6", and the router reports "Factory Reset" |
| 3 | 3. Prompt "Please enter password", the method of inputting password is the same |
| Factory Reset | as operation 1. |
| | 4. If you want to quit, press "*". |
| | 5. Prompt "operation successful" if password is right and then the router will be |
| | 1. Pick up phone and press "****" to start IVR |
| | 2. Choose "7", and the router reports "Reboot" |
| 4 | 3. Prompt "Please enter password", the method of inputting password is same as |
| Reboot | operation 1. |
| | 4. the router reboots if password is right and operation |
| | |

| | 1. Pick up phone and press "****" to start IVR |
|------------|--|
| 5 | 2. Choose "8", and the router reports "WAN Port Login" |
| WAN Port | 3. Prompt "Please enter password", the method of inputting password is same as |
| Login | operation 1. |
| | 4. If user wants to quit, press "*". |
| | 1. Pick up phone and press "****" to start IVR |
| 6 | 2. Choose "9", and the router reports "WEB Access Port" |
| WEB Access | 3. Prompt "Please enter password", the method of inputting password is same as |
| Port | operation 1. |
| | 4. Report "operation successful" if user operation is ok. |
| | 5. Report the current WEB Access Port |
| 7 | 1. Pick up phone and press "****" to start IVR |
| Firmware | 2. Choose "0" and the router reports the current Firmware version |
| 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:
- 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 FWR8102 is 192.168.11.1 and this address should not be assigned to the WAN port IP address of FWR8102 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, I -- 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.

FWR9502 supports two-level management: administrator and user. For administrator mode operation, please type "admin/admin" on Username/Password and click Login button to begin configuration. For 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.

| VoIP | CC | ontrol panel | | |
|------|----------|--------------|----|--|
| | Username | | | |
| | Password | Log | in | |

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.

| VoIP | C(| ontrol par | hel | |
|------|----------------------|------------|-------|--|
| | | | | |
| | Username Password | | Login | |

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.



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

Web Management Interface Details

Current VoIP control panel Admin M Network Wireless 2.4GHz Wireless 5GHz Security Storag Status Application WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ VLAN Rate Limit QoS Port Advance INTERNET Help VAN WAN IP Mo Static IP - Se Connect Name 1_MANAGEMENT_VOICE_INTERNET_R_VID V Delete Connect Mask and De by your ISP. MANAGEMENT_VOICE_INTERNET ▼ Service **IP Protocol Version** IPv4 ▼ DHCP - You Subnet Mask DHCP V WAN IP Mode from a DHCF DHCP Server PPPoE - Set MAC Address Clone Disable • PPPoE Passv NAT Enable Enable • VLAN Mode Disable • (1-4094) VLAN ID 1 3 DNS Mode Auto 🔻 Primary DNS Secondary DNS DHCP DHCP Renew Renew DHCP Vendor (Option 60) FLYINGVOICE-FWR9502 Port Bind Port_1 Port_2 Port_3 Port_4 ✓ Wireless (SSID) ✓ Wireless (SSID1) Wireless (SSID2) Wireless (SSID3) Note: LAN (local) ports can only be bound to one WAN (Internet) connection at a time! Save & Apply Save Cancel Reboot

| Table 5 | Web management interface |
|----------|--------------------------|
| I able 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

| Time/Date Setting | |
|----------------------------------|---|
| NTP Settings | |
| NTP Enable | Enable 🔻 |
| Option 42 | Disable 🔻 |
| Current Time | 2017 - 10 - 10 , 13 : 56 : 14 |
| Sync with host | Sync with host |
| Time Zone | (GMT+08:00) China Coast, Hong Kong 🔹 |
| Primary NTP Server | pool.ntp.org |
| Secondary NTP Server | cn.pool.ntp.org |
| NTP synchronization(1 - 1440min) | 60 |
| Daylight Saving Time | |
| Daylight Saving Time | Disable 🔻 |
| ld Name | Description |
| P Enable | Enable NTP (Network Time Protocol) to automatically retrieve time |
| | and date settings for the device |
| rrent Time | When NTP Enable is set to "Disable", manually configure the time |
| | and date via the Current Time parameter |
| c with host | Press Sync with host button to synchronize the host PC date, |
| | time and time zone |
| nary NTP Server | Primary and secondary NTP server address for clock synchronization. |
| ondary NTP Server | valid NTP server must be reachable for full NTP functionality |
| 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 |
|--|---------|-------------|-------------|------------|
|--|---------|-------------|-------------|------------|

| AN LAN IPv6 Advanced | IPv6 WAN IPv6 LAN VPN Por | t Forward DMZ VLAN QoS Rate |
|-----------------------------|----------------------------|-----------------------------|
| dvance | | |
| NTERNET | | |
| N | | |
| Connect Name | 1_MANAGEMENT_VOICE_INTERNE | T_R_VID ▼ Delete Connect |
| Service | MANAGEMENT_VOICE_INTERNET | * |
| IP Protocol Version | IPv4 ▼ | |
| WAN IP Mode | DHCP V | |
| DHCP Server | | |
| MAC Address Clone | Disable 🔻 | |
| NAT Enable | Enable 🔻 | |
| VLAN Mode | Disable 🔻 | |
| VLAN ID | 1 (1-4094) | |
| DNS Mode | Auto 🔻 | |
| Primary DNS | | |
| Secondary DNS | | |
| DHCP | | |
| DHCP Renew | Renew | |
| DHCP Vendor (Option 60) | FLYINGVOICE-FWR9502 | |
| Port Bind | | |
| Port_1 Port_2 | Port_3 | Port_4 |
| Wireless (SSID) Wireless (S | SID1) Wireless (SSID2) | Wireless (SSID3) |

Save & Apply Save Cancel Reboot

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

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 | w) |) |
|--|----|---|
|--|----|---|

| Status | Network | Vireless 2.4 | GHz | Wireless | s 5GHz | SIP | FXS1 | FXS2 | Security | Application | Storage | Adr |
|--|---------------------------|--|-------------------------------------|------------|------------|--------------------|-----------|-----------|------------|---------------|----------|-----|
| Basic | Wireless Security | WMM | WDS | WPS | Station | Info | Advanced | | | | | |
| Basic | Wireless Settin | gs | | | | | | | | | | |
| Wireless | Network | | | | | | | | | | | |
| Radio | On/Off | | | Rad | io On 🔻 | | | | | | | |
| Wirele | ss Connection Mode | | | AP | ۲ | | | | | | | |
| Netwo | rk Mode | | | 11b | /g/n mixed | d mode | • | | | | | |
| Multipl | e SSID | | | FWR | 9502-000 | 0 <mark>C</mark> 8 | Enable 🗹 | Hidden 🗐 | Isolated | Max Client 32 | | |
| Multipl | e SSID1 | | | | | | Enable 🗐 | Hidden 🗐 | Isolated 🔲 | Max Client 16 | | |
| Multipl | e SSID2 | | Enable Hidden Isolated Max Client 8 | | | | | | | | | |
| Multiple SSID3 Enable Hidden Isolated Max Client 8 | | | | | | | | | | | | |
| broadcast (SSID) Enable Disable | | | | | | | | | | | | |
| AP Iso | lation | | | © E | Enable 💿 | Disable | e | | | | | |
| MBSSI BSSID | D AP Isolation | © Enable © Disable 00:21:F2:00:00:10 | | | | | | | | | | |
| Freque | ency (Channel) | | | 243 | 7MHz (Cha | annel 6) | • | | | | | |
| 1000 | ysical Mode | | | - | | ~ | | | | | | |
| | ting Mode el BandWidth | | | | lixed Mode | 1 | een Field | | | | | |
| Field I | Name | Des | script | ion | | | | | | | | |
| | | | - | | dicabl | o wire | | oration | | | | |
| adio Oi | o/Off | Select "Radio Off" to disable wireless operation | | | | | | | | | | |
| | i)Oli | Select "Radio on" to enable wireless operation | | | | | | | | | | |
| | | Please note: "Save" required for this parameter change | | | | | | | | | | |
| etwork | Mode | Choose one network mode from the drop down list. | | | | | | | | | | |
| | | The log | gical na | ame of | the wir | eless | connec | tion (tex | t, numbe | rs or various | special | |
| SID characters) | | | | | | | | | | | | |
| Iultiple | SSID 1-4 | Multipl | le SSIE | 01-4,0 | configu | re up | to 4 uni | que SS | IDs | | | |
| | | Enable | d: The | device | SSID is | broa | dcast at | regular | intervals | Disabled: Th | e device | |
| roadca | st(SSID) | SSID is | not bi | oadcas | t at reg | gulatr | interval | s, | | | | |
| - | . , | disallov | wing v | /i-fi clie | nts fro | m aut | tomatica | Illy conn | ecting to | the FWR940 | 2 | |
| | | | - | | | | | | - | | | |

| | Enabled: Devices connected to the router are isolated from one another on virtual |
|---------------------|--|
| AP Isolation | networks |
| | Disabled: Devices connected to the router are visible on the network to each other |
| | Enabled: Devices connected to the router via one of the Multiple SSIDs are isolated |
| MBSSID AP Isolation | 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 | |
| | Mixed Mode: Packet preamble (only) is transmitted in a format compatible with |
| Operating Mode | 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 |
|-------|---|----------|----------|-----|------|
| | | | | | |

| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced |
|----------|-------------------|-----|-----|-----|--------------|----------------------------------|
| Wi-Fi | Security Setting | s | | | | |
| elect SS | ID | | | | | |
| SSID d | hoice | | | | FWR9502-0 | 000C8 • |
| "FWR9 | 502-0000C8" | | | | | |
| Securit | y Mode | | | | WPAPSKWP | A2PSK 🔻 |
| WPA | | | | | | |
| | gorithms | | | | • TKIP | AES TKIPAES |
| Pass P | nrase | | | | ****** | e |
| Key Re | newal Interval | | | | 3600 s | ec (0 ~ 86400) |
| Access | 5 Policy | | | | | |
| Policy | | | | | Disable ▼ | |
| Add a s | station MAC | | | | | (The maximum rule count is 64) |

| Field Name | Description |
|----------------------|--|
| SSID Choice | Choose the SSID from the drop-drown list for which security will be configured |
| | Select an appropriate encryption mode to improve the security and privacy of |
| Security Mode | 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. |
| | This parameter is used to select the encryption of wireless home gateway |
| WPA Algorithms | 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 | |
| | Disable: Access policy rules are not enforced |
| Policy | 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

| Status | Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application |
|------------------------|------------------------------|-----------------|---------------|---------------------------|-----------------------|------|-----------|-------------|
| SIP Acco | unt Prefere | nces | | | | | | |
| Basic | | | | | | | | |
| asic Setu | p | | | | | | | |
| Line Ena | able | Enable 🔻 | | Outgoin Registra | ig Call with ation | out | Disable 🔻 | |
| roxy and | Registration | | | | | | | |
| Proxy Se | erver | | | Proxy Po | ort | | 5060 | |
| Outbour | nd Server | | | Outbound Port 5060 | | | | |
| Backup Outbound Server | | | | Backup Outbound Port 5060 | | | | |
| | HCP Option 120 SIP Server | to Disable 🔻 | | | | | | |
| ubscribe | Information | | | | | | | |
| Display | Name | | | Phone M | Number | | | |
| Account | | | | Password | | | | |

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 Button to make changes effective.

Viewing the Registration Status

Table 11 Registration status

| Status Network Wireles | ss 2.4GHz Wireless 5GHz SIP FXS1 FXS2 Security Application | | | | | | |
|---------------------------------------|--|--|--|--|--|--|--|
| Basic LAN Host Syslog | | | | | | | |
| Product Information | | | | | | | |
| oduct Information | | | | | | | |
| Product Name | FWR9502 | | | | | | |
| Internet (WAN) MAC Address | 00:21:F2:00:00:C9 | | | | | | |
| PC (LAN) MAC Address | 00:21:F2:00:00:C8 | | | | | | |
| Hardware Version | V4.4 | | | | | | |
| Loader Version | V3.35(May 4 2017 17:41:36) | | | | | | |
| Firmware Version | V3.20(201709061037) | | | | | | |
| Serial Number FLY58161000007 | | | | | | | |
| SIP Account Status | | | | | | | |
| P Account Status | | | | | | | |
| FXS 1 SIP Account Status | Register Fail | | | | | | |
| Primary Server 0.0.0.0 | | | | | | | |
| Backup Server 0.0.0.0 | | | | | | | |
| XS 2 SIP Account Status Register Fail | | | | | | | |
| Primary Server | 0.0.0.0 | | | | | | |
| Backup Server | 0.0.0 | | | | | | |

Procedure

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

status.

Making a Call

Calling phone or extension numbers

To make a phone or extension number call:

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

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

Direct IP calls

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

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

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

Call Hold

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

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

Blind Transfer

Assume that call party A and party B are in conversation. Party A wants to Blind Transfer B to C: Party A dials "*78" to get a dial tone, then dials party C's number, and then press immediately key # (or wait for 4 seconds) to dial out.

A can hang up.

Attended Transfer

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

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

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

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

Conference

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

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

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

Chapter 3: Web Interface

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

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

Login

Table 12 Login details

| | <i>VoIP</i> C | ontrol pa | nel | |
|----|--|-------------------|----------------|--|
| | Username | admin | | |
| | Password | ***** | Login | |
| | | Proce | dure | |
| 1. | Connect the LAN port of the route | er to your PC an | Ethernet cable | |
| 2. | Open a web browser on your PC a | and type http://1 | 92.168.1.1. | |
| 3. | Enter Username admin and Password admin. | | | |
| 4. | Click Login | | | |

Status

Table 13 Status Page

| Status Network Wireles | ss 2.4GHz Wireless 5GHz SIP FXS1 FXS2 Security Application |
|----------------------------|--|
| Basic LAN Host Syslog | |
| Product Information | |
| oduct Information | |
| Product Name | FWR9502 |
| Internet (WAN) MAC Address | 00:21:F2:00:00:C9 |
| PC (LAN) MAC Address | 00:21:F2:00:00:C8 |
| Hardware Version | V4.4 |
| Loader Version | V3.35(May 4 2017 17:41:36) |
| Firmware Version | V3.20(201709061037) |
| Serial Number | FLY58161000007 |
| SIP Account Status | |
| IP Account Status | |
| FXS 1 SIP Account Status | Register Fail |
| Primary Server | 0.0.00 |
| Backup Server | 0.0.0 |
| FXS 2 SIP Account Status | Register Fail |
| Primary Server | 0.0.0.0 |
| Backup Server | 0.0.0.0 |
| FXS Port Status | |
| (S Port Status | |
| FXS 1 Hook State | On |
| FXS 1 Port Status | Idle |
| FXS 2 Hook State | On |
| FXS 2 Port Status | Idle |

| ive WAN Interface | | |
|------------------------|----------------------|--|
| Connection Type | DHCP | |
| P Address | 192.168.10.142 Renew | |
| ink-local IPv6 Address | | |
| ubnet Mask | 255.255.255.0 | |
| Default Gateway | 192.168.10.1 | |
| Primary DNS | 192.168.10.1 | |
| econdary DNS | 192.168.18.1 | |
| Pv6 PD Prefix | | |
| Pv6 Domain Name | | |
| Pv6 Primary DNS | | |
| Pv6 Secondary DNS | | |
| VAN Port Status | 100Mbps Full | |
| VAN Down Speed | 1.008KB/s | |
| VAN Up Speed | 320B/s | |
| R069_VOICE_INTERNET VI | an Status | |
| Connection Type | DHCP | |
| 1AC Address | 00:21:F2:00:00:C9 | |
| P Address | 192.168.10.142 | |
| Subnet Mask | 255.255.255.0 | |
| Default Gateway | 192.168.10.1 | |
| Primary DNS | 192.168.10.1 | |
| Secondary DNS | 192.168.18.1 | |
| Status | | |
| /PN Type | Disable | |
| nitial Service IP | | |
| /irtual IP Address | | |

| AN Port Status | | |
|-------------------------|---------------------|--|
| IP Address | 192.168.1.1 | |
| Subnet Mask | 255.255.255.0 | |
| LAN1 | Link Down | |
| LAN2 | Link Down | |
| LAN3 | 1000Mbps Full | |
| LAN4 | Link Down | |
| Wireless Info | | |
| ireless 2.4GHz | | |
| Radio On/Off | On | |
| Network Mode | 11b/g/n mixed mode | |
| Current Channel | 1 | |
| Channel Bandwidth | 40MHz | |
| ireless 5GHz | | |
| Radio On/Off | On | |
| Network Mode | 11vht AC/AN/A | |
| Current Channel | 1 | |
| Channel Bandwidth | 80/40MHz | |
| WR9502-0000C8 (2.4GHz) | | |
| BSSID | 00:21:F2:00:00:10 | |
| Number of Device | 0 | |
| WR9502-5G-0000C8 (5GHz) | | |
| BSSID | 00:0C:43:26:60:00 | |
| Number of Device | 0 | |
| System Status | | |
| ystem Status | | |
| Current Time | 2017-10-25 16:13:51 | |
| Elapsed Time | 2 Hours, 27 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

| Static | |
|-----------------------|--|
| IP Address | 192.168.10.173 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| DNS Mode | Manual 🔻 |
| Primary DNS | 192.168.10.1 |
| Secondary DNS | 192.168.18.1 |
| Field Name | 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.

| Tabl | е | 15 | DHCP |
|------|---|----|------|
| | | | |

| N | | | |
|---------------------|-----------------|-----------------------------------|------------------|
| Connect Name | | 1_MANAGEMENT_VOICE_INTERNET_R_VID | ▼ Delete Connect |
| Service | | MANAGEMENT_VOICE_INTERNET ▼ | |
| IP Protocol Version | | IPv4 ▼ | |
| WAN IP Mode | | DHCP V | |
| DHCP Server | | | |
| MAC Address Clone | | Disable 🔻 | |
| NAT Enable | | Enable 🔻 | |
| VLAN Mode | | Disable 🔻 | |
| VLAN ID | | 1 (1-4094) | |
| DNS Mode | | Auto 🔻 | |
| Primary DNS | | | |
| Secondary DNS | | | |
| DHCP | | | |
| DHCP Renew | | Renew | |
| DHCP Vendor(Option | n 60) | FLYINGVOICE-FWR8102 | |
| Port Bind | | | |
| Port_1 | Port_2 | Port_3 | |
| Wireless(SSID) | Wireless(SSID1) | Wireless(SSID2) | Wireless(SSID3) |

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

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

ΡΡΡοΕ

PPPoE stands for Point-to-Point Protocol over Ethernet. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection. PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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

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

| Confirm Password | Enter your PPPoE password again | | |
|-----------------------|--|--|--|
| Service Name | Enter a service name for PPPoE authentication. | | |
| | If it is left 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 Per | od 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.

| INTERNET | | | | | | | |
|---------------------|---------------|--|--------------------------------|--|--|--|--|
| VAN | | | | | | | |
| Connect Name | | 1_MANAGEMENT_VOICE_INTERNET_R_ | VID VID VID | | | | |
| Service | | MANAGEMENT_VOICE_INTERNET V | | | | | |
| IP Protocol Version | | IPv4 V | | | | | |
| WAN IP Mode | | Bridge 🔻 | | | | | |
| Bridge Type | | IP Bridge | | | | | |
| DHCP Service Type | | Pass Through 🔻 | | | | | |
| VLAN Mode | | Disable 🔻 | | | | | |
| VLAN ID | | 1 (1-4094) | | | | | |
| | | between the binding port , and finally bound tection to the port binding operation ! Descrip | | | | | |
| Bridge Type | | Descrip | | | | | |
| P Bridge | Allow all Eth | hernet packets to pass. PC can conn | ect to upper network directly. | | | | |
| PPoE Bridge | Only Allow | Only Allow PPPoE packets pass. PC needs PPPoE dial-up software. | | | | | |
| lardware IP Bridge | e Packets pas | s through hardware switch with wir | ed speed. Does not support | | | | |
| | wireless po | rt binding | | | | | |
| OHCP Service Type | 9 | | | | | | |
| Dece Through | | to one he ferwarded hetween MAN | | | | | |

| 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

| AN LAN IPv6 Advanced I | IPv6 WAN IPv6 LAN | VPN | Port Forward | DMZ | VLAN | QoS | Rate | | |
|------------------------------|-------------------|---------------|--------------|------|------|-----|------|--|--|
| tvance | | | | | | | | | |
| | | | | | | | | | |
| C Port(LAN) | | | | | | | | | |
| Port(LAN) | | | | | | | | | |
| ocal IP Address | | 192.168.1.1 | | | | | | | |
| .ocal Subnet Mask | | 255.255.255. | 0 | | | | | | |
| .ocal DHCP Server | | Enable 🔻 | | | | | | | |
| OHCP Start Address | 1 | 92.168.1.2 | | | | | | | |
| OHCP End Address | 1 | 192.168.1.254 | | | | | | | |
| DNS Mode | | Auto 🔻 | | | | | | | |
| Primary DNS | | 192.168.1.1 | | | | | | | |
| Secondary DNS | | 192.168.10.1 | | | | | | | |
| Client Lease Time (0-86400s) | 8 | 86400 | | | | | | | |
| | | DHCP Client | List | | | | | | |
| OHCP Static Allotment | | | | | | | | | |
| NO. | MAC | | IP Add | ress | | | | | |
| Delete Selected Add Edit | | | | | | | | | |
| ONS Proxy | F | Enable 🔻 | | | | | | | |
| DNS PIOXy | | Enable . | | | | | | | |

| Field Name | Description |
|-------------------|--|
| IP Address | Enter the IP address of the router on the local area network. All the IP addresses |
| | of the computers which are in the router's LAN must be in the same network |
| | segment with this address, and the default gateway of the computers must be |
| | this IP address. (The default is 192.168.11.1). |
| Local Subnet Mask | Enter the subnet mask to determine the size of the network (default is |
| | 255.255.255.0/24). |
| Local DHCP Server | Enable/Disable Local DHCP Server. |

| DHCP Start Address | Enter a valid IP address as a starting IP address of the DHCP server, and if the |
|--------------------|---|
| | router's LAN IP address is 192.168.11.1, starting IP address can be 192.168.11.2 |
| | or greater, but should be less than the ending IP address. |
| DHCP End Address | Enter a valid IP address as an end IP address of the DHCP server. |
| DNS Mode | Select DNS mode, options are Auto and Manual: |
| | When DNS mode is Auto, the device under LAN port will automatically obtains the |
| | preferred DNS and alternate DNS. |
| | When DNS mode is Manual, the user should manually configure the preferred |
| | DNS and alternate DNS. |
| Primary DNS | Enter the preferred DNS address. |
| Secondary DNS | Enter the secondary DNS address. |
| Client Lease Time | This option defines how long the address will be assigned to the computer within |
| | the network. In that period, the server does not assign the IP address to the other |
| | computer. |
| DNS Proxy | Enable or disable; If enabled, the device will forward the DNS request of LAN-side |
| | network to the WAN side network. |

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

| Port(LAN) | |
|--------------------|------------------------------|
| Local IP Address | 192.168.11.1 |
| Local Subnet Mask | 255.255.255.0 |
| Local DHCP Server | Enable 🔻 |
| DHCP Start Address | 192.168.11.2 |
| DHCP End Address | 192.168.11. <mark>254</mark> |
| DNS Mode | Auto 🔻 |

| 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

| Primary DNS | 192.168.11.1 |
|-----------------------------|------------------|
| Secondary DNS | 8.8.8.8 |
| Client Lease Time(0-86400s) | 86400 |
| | DHCP Client List |

| Field Name | Description |
|-------------------|--|
| | Specify the Primary DNS address provided by your ISP. If your ISP does not provide |
| Primary DNS | it, the router will automatically apply default DNS Server IP address: 202.96.134.33 |
| , | to this field. |
| | 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 |
| 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. |

VPN

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

Table 21 VPN

| Status | Netwo | ork Wir | eless 2.4GHz | Wireless 5GH | lz SIP | FXS1 | FXS2 | Security | Appl | icatior |
|----------------------|---------|-------------|--|-------------------|--------|--------------|-------|----------|------|---------|
| WAN Advance | LAN | IPv6 Advanc | ed IPv6 WAN | IPv6 LAN | VPN | Port Forward | i DMZ | VLAN | QoS | Rate |
| VPN Se Administra | ation – | | | | | | | | | |
| VPN Ena | ble | | Disable Disable PPTP L2TP OpenVPI Save of | N K Apply Save | Cancel | Reboot | | | | |

| 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

| Status Network | Wireless 2.4GH | z Wireless 5GH | z SIP | FXS1 | FXS2 | Security | Applic | ation S | torage Admi |
|-----------------------------------|------------------|----------------|------------|------------|------|------------|-----------|------------|--------------|
| WAN LAN IP | v6 Advanced IPv6 | WAN IPv6 LAN | VPN Po | rt Forward | DMZ | VLAN | QoS | Rate Limit | Port Setting |
| Advance | | | | | | | | | |
| | | | Port Forwa | rdina | | | | | |
| No. | Co | mment | IP Addre | | | Port Range | | F | Protocol |
| Delete Selected A | dd Edit | | | | | | | | |
| Port Forwarding | | | | | | | | | |
| Comment | | | | | | | | | |
| IP Address | | | _ | 1 | | | | | |
| Port Range | | | - | - | | | | | |
| Protocol (The maximum rule co | uptic 22.) | | 10 | CP&UDP V | | | | | |
| Apply Cancel | unic is 32) | | | | | | | | |
| Appry Cancer | | | | | | | | | |
| Virtual Servers | | | | | | | | | |
| No. | Comment | IP Add | ress | Public F | Port | Priv | /ate Port | | Protocol |
| Delete Selected | dd Edit | | | | | | | | |
| Virtual Servers | | | | | | | | | |
| Comment | | | | | | | | | |
| IP Address | | | | | | | | | |
| Public Port | | | | | | | | | |
| Private Port | | | | | | | | | |
| Protocol | | | T | CP&UDP V | | | | | |
| (The maximum rule co | unt is 32) | | | | | | | | |
| Apply Cancel | | | | | | | | | |

| 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

| Network | Wireless 2.4GHz | Wireless 5GHz | SIP FXS1 | FXS2 | Security A | pplication | Storage A |
|--------------|-------------------|---|---|--|--|---|--|
| AN IPv6 | Advanced IPv6 WAN | IPv6 LAN | VPN Port Forwar | d DMZ | VLAN Qo | S Rate Limi | t Port Settin |
| | | | | | | | |
| | | VLA | N Model Configuration | n | | | |
| Divide Model | Custom | • | | | | | |
| | | Port 1 | VLAN ID Configuratio | n | | | |
| WAN | LAN1 | | LAN2 | | LAN3 | | LAN4 |
| | 2 | | 2 | | 2 | | 2 |
| | | V | LAN Configuration | | | | |
| | | | P | ort | | | |
| N ID | WAN | LAN1 | L | N2 | LAN3 | 3 | LAN4 |
| | UnTagged 🔻 | UnSet | ▼ UnSet | • | UnSet | • | UnSet 🔻 |
| | UnSet 🔻 | UnTagged | ▼ UnTag | gged 🔻 | UnTagge | ed 🔻 | UnTagged 🔻 |
| | UnSet 🔻 | UnSet | ▼ UnSet | • | UnSet | • | UnSet 🔻 |
| | Divide Model | Divide Model Custom WAN LAN1 2 N ID WAN UnTagged V UnSet V | VLA Divide Model Custom ▼ Port WAN LAN1 2 N ID WAN LAN1 UnTagged ▼ UnSet UnSet UnTagged | VLAN Model Configuration Divide Model Custom ▼ Port VLAN 1D Configuration WAN LAN1 2 2 VLAN Configuration VLAN Configuration PORT N ID WAN UnTagged ▼ UnSet UnSet UnTagged ▼ | VLAN Model Configuration Divide Model Custom ▼ Port VLAN ID Configuration WAN LAN1 LAN2 2 2 2 VLAN Configuration VLAN Configuration VLAN Configuration Port N ID WAN LAN1 LAN2 UnTagged ▼ UnSet ▼ UnSet ▼ UnTagged ▼ | VLAN Model Configuration Divide Model Custom ▼ Port VLAN ID Configuration WAN LAN1 LAN2 LAN3 2 2 2 2 VLAN Configuration Port Port VLAN Configuration Port UNAN LAN3 2 2 2 2 VLAN Configuration Port N ID WAN LAN1 LAN2 LAN3 Imagged ▼ UnSet ▼ UnSet ▼ UnSet UnSet Imagged ▼ UnTagged ▼ UnTagged ▼ UnTagged ▼ UnTagged ▼ | VLAN Model Configuration Divide Model Custom ▼ Port VLAN ID Configuration WAN LAN1 LAN2 LAN3 2 2 2 2 VLAN Configuration VLAN Configuration Port NID WAN LAN1 LAN2 LAN3 UnTagged ▼ UnSet ▼ UnSet ▼ UnSet ▼ UnSet ▼ UnTagged ▼ |

| 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

| Status | Netwo | wireles | ss 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Appl | ication |
|-----------|-------------------|-------------------|----------------|----------------|----------|--------------|----------|-----------|------|---------|
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | QoS | Rate |
| DMZ Sett | litarized ting | Zone (DMZ) ess | | Er | nable 🔻 | | Get Curr | ent PC IP | | |
| eld Nan | ne | Des | Save 8 | k Apply Save | Cancel | Reboot | | | | |
| /IZ Enabl | | | ble/Disable | DMZ. | | | | | | |
| 1Z Host | IP Addres | s Ente | er the private | e IP address c | of the D | MZ host. | | | | |

QoS

Table 25 QoS

| WAN LAN Advance | IPv6 A | dvanced | IPv6 WAN | Constant of the local division of the | | | | | | | |
|--------------------|--------|----------------------|------------|---------------------------------------|-------------------------|-------------|-----------|--------------------|-----------|------------|--------|
| Advance | | | THAN WAIN | IPv6 LAN | VPN | Port Forwar | d DMZ | VLAN | QoS | Rate Limit | Port S |
| Auvance | | | | | | | | | | | |
| QoS setting | | | | | | | | | | | |
| oS setting – | | | | | | | | | | | |
| Enable QoS | | | | | | Ena | ble 🔻 | | | | |
| Upstream | | | | | | | | (0- | -102400)k | bit/s | |
| Downstream | | | | | | | | (0- | -102400)k | bit/s | |
| Algorithm | | | | | | WFC | 2 • | | | | |
| | | | | | | Save Car | icel | | | | |
| | | | | Condition | | | | | | Ac | tion |
| Name | | Dst.IP Address Pr | otocol Ran | | Physical Port Del | DSCP 80 | 02.1p VLA | Remar N ID DSCP | | | |

| 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

Rate Limit

Table 26 Port setting

| vance | | | | |
|-------------------|---------------------|-----------|--------------------|----------------------|
| ate Limit Setting | | | | н |
| ole Rate Limit | | | | |
| Enable Rate Limit | Enable 🔻 | | | |
| Port In | igress Rate | Egress Ra | ite | |
| WAN | 100000 (1-100000) |)kbit/s | 100000 (1-100000)k | bit/s |
| LAN1 | 100000 (1-100000) |)kbit/s | 100000 (1-100000)k | b <mark>i</mark> t/s |
| LAN2 | 100000 (1-100000) |)kbit/s | 100000 (1-100000)k | bit/s |
| LAN3 | 100000 (1-100000) |)kbit/s | 100000 (1-100000)k | bit/s |
| LAN4 | 100000 (1-100000) |)kbit/s | 100000 (1-100000)k | bit/s |
| Port Bi | roadcast Storm Rate | | 24 1273 44.4 | |
| WAN | 255 (0-255)*64 p | oackets/s | | |
| LAN1 | 255 (0-255)*64 p | oackets/s | | |
| LAN2 | 255 (0-255)*64 p | oackets/s | | |
| LAN3 | 255 (0-255)*64 p | oackets/s | | |
| LAN4 | 255 (0-255)*64 p | ackets/s | | |

Description

Set the port speed limit for WAN port and LAN port, select enable or disable

Port Setting

Table 27 Port setting

| WAN LAN IPv6 Advanced IPv | r6 WAN IPv6 LAN V | PN Port Forward | d DMZ | VLAN | QoS | Rate Limit | Port Setting | Routing |
|-----------------------------------|------------------------------|-----------------|----------|---------|---------|------------|--------------|---------|
| Advance | | | | A | | | | |
| Port Setting | | | | | | Hel | p | |
| ort Setting | | | | | | | | |
| WAN Port Speed Nego | Auto | • | | | | | | |
| LAN1 Port Speed Nego | Auto | * | | | | | | |
| LAN2 Port Speed Nego | Auto | | | | | | | |
| LAN3 Port Speed Nego | Auto | | | | | | | |
| LAN4 Port Speed Nego | Auto | • | | | | | | |
| | | | | | | | | |
| | | ancel Reboot | | | | | | |
| | Save & Apply Save Ca | incel Reboot | | | | | | |
| Field Name | Descriptior | | | | | | | |
| Field Name WAN Port speed Nego | |) | are Auto | o, 100N | 1 full, | 100M hal | f-duplex, 1 | 0M half |
| | Description |) | are Auto | o, 100N | 1 full, | 100M hal | f-duplex, 1 | 0M half |
| | Description Auto-negotiat | ion, options | | | | | · · | |

Routing

Table 28 Routing

| WAN LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN Port Forward | DMZ | VLAN | QoS | Rate Limit | Port Setting | Routing |
|--|--------------------|------------|-------------------------------|--------------------|----------|------|--------|-----------------|-----------------|---------------|
| dvance | | | | | - | | | | | Weinerstein U |
| Static Routin | ng Settings | | | | | | | Hel | p | |
| d a routing rule Destination Host/Net Gateway Interface Comment | e | | | st V | | | | Add or here. | remove Internet | routing rules |
| | Table in the syste | ask Ga | teway Flag Delete Selected | gs Metric Reset | Interfac | ce C | omment | | | |
| ield Nam | ie C | Descriptio | on | | | | | | | |
| | _ | | | | | | | | | |

| 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 |

IP conflict Detecting Interval

Advance

Table 29 Advance

| WAN LAN IPv6 Advan | ed IPv6 WAN IPv6 LA | N VPN | Port Forward | DMZ | VLAN | QoS | Rate |
|--|-----------------------|-------------|----------------|-----|------|-----|------|
| Advance | | | n) | | | | |
| | | 1 | | | | | 1 |
| Most Nat connections (512-819) | 2) | 4096 | | | | | |
| MSS Mode | | Manua | I 🔘 Auto | | | | |
| MSS Value (1260-1460) | | 1440 | | | | | |
| Anti-DoS-P | Enable | Disable | | | | | |
| IP Conflict Detection | Enable Disable | | | | | | |
| IP Conflict Detecting Interval(0- | 3600 <mark>s</mark>) | 600 | | | | | |
| Field Name | Description | | | | | | |
| Most Nat connections | The largest value whi | ch the FWf | R9502 can prov | ide | | | |
| Mss Mode Choose Mss Mode from Manual and Auto | | | | | | | |
| Mss Value | | | | | | | |
| AntiDos-p | You can choose to en | able or pro | hibit | | | | |
| IP conflict detection Select enable if enabled, phone IP conflict will have tips or prohibit | | | | | | bit | |

Detect IP address conflicts of the time interval

Wireless 2.4G

Basic

Table 30 Basic

| itatus Ne | etwork Wi | ireless 2.4 | GHz | Wireless | 5GHz SIF | FXS1 | FXS2 | Security | Application | Storage | Adr |
|---------------|-----------------|-------------|-----|----------|-----------------|-------------|----------|----------|---------------|---------|-----|
| lasic Wire | less Security | WMM | WDS | WPS | Station Info | Advanced | | | | | |
| Basic Wire | less Setting | s | | | | | | | | | |
| reless Netwo | ork | | | | | | | | | | |
| Radio On/Off | | | | Rad | o On 🔻 | | | | | | |
| Wireless Conr | nection Mode | | | AP | T | | | | | | |
| Network Mode | e | | | 11b | g/n mixed mod | e 🔻 | | | | | |
| Multiple SSID | | | | FWR | 9502-0000C8 | Enable 🗹 | Hidden 🗐 | Isolated | Max Client 32 | | |
| Multiple SSID | 1 | | | | | Enable 🔲 | Hidden 🗐 | Isolated | Max Client 16 | 1 | |
| Multiple SSID | 2 | | | | | Enable | Hidden 🗐 | Isolated | Max Client 8 | | |
| Multiple SSID | 3 | | | | | Enable | Hidden 🔲 | Isolated | Max Client 8 | | |
| broadcast (SS | (D) | | | | nable 🔍 Disat | | | | | | |
| AP Isolation | , | | | | nable 💿 Disat | | | | | | |
| MBSSID AP Is | olation | | | | nable 💿 Disat | | | | | | |
| BSSID | | | | 00: | 21:F2:00:00:10 | | | | | | |
| Frequency (C | hannel) | | | 243 | 7MHz (Channel (| 5) 🔻 | | | | | |
| HT Physical M | lode | | | | | | | | | | |
| Operating Mo | de | | | • M | ixed Mode 🔘 (| Green Field | | | | | |
| Channel Band | Width | | | © 2 | 0 🖲 20/40 | | | | | | |
| Guard Interva | el 🗌 | | | © ь | ong 💿 Short | | | | | | |
| Reverse Direc | tion Grant (RDC | 5) | |) D | isable 💿 Enab | le | | | | | |
| Extension Cha | annel | | | 2457 | MHz (Channel 1 | .0) 🔻 | | | | | |
| STBC | | | | O D | isable 💿 Enab | le | | | | | |
| Aggregation N | ISDU (A-MSDU) |) | | • D | isable 🔍 Enab | le | | | | | |
| Auto Block AC | K | | | OD | isable 💿 Enab | le | | | | | |
| Decline BA Re | equest | | | • D | isable 🔍 Enab | le | | | | | |
| HT Disallow T | KIP | | | O D | isable 💿 Enab | le | | | | | |
| HT LDPC | | | | () n | isable 🔍 Enab | lo i | | | | | |

| 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 | Mixed Mode: In this mode, the previous wireless card can recognize and |
| Operating | connect to the Pre-N AP, but the throughput will be affected |
| Mode | 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 |
| | Enabled: Devices on the WLAN are able to transmit to each other without |
| Reverse Dirction Grant | requiring an additional contention-based request to transfer (i.e. devices are |
| (RDG) | 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

| Status | Network | Wireless 2.4 | IGHz | Wireless | 5GHz SIP | FXS1 | FXS2 | Security | Application |
|------------------------------|-------------------|--------------|----------|----------|------------------|--------------|-----------|-----------------|-------------|
| Basic | Wireless Security | / WMM | WDS | WPS | Station Info | Advanced | | | |
| Wi-Fi | Security Setti | ngs | | | | | | | |
| Select SS | ID | | | | | | | | |
| SSID cl "FWR9: Securit | 502-0000C8" | | | | FWR9502-0 | | | | |
| WPA | | | | | | | | | |
| WPA A | gorithms | | | | ● TKIP (| AES OT | KIPAES | | |
| Pass Ph | nrase | | | | ******* | | | | |
| Key Re | newal Interval | | | | 3600 s | sec (0 ~ 864 | 00) | | |
| | Policy | | | | | | | | |
| Policy | | | | | Disable • | | | | 110 |
| Add a s | station MAC | | | | | (Tł | e maximu | m rule count is | \$ 64) |
| | | | Save | & Apply | Save Cancel | Reboot | | | |
| Field N | lame | Descr | iption | | | | | | |
| SSID Cho | pice | Choose on | e SSID f | rom SSIE |), Multiple SSI | D1, Multipl | e SSID2 a | and Multiple | e SSID3. |
| | | Select an a | ppropri | ate encr | yption mode t | o improve | the secu | rity and priv | acy of your |

Security Mode 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 Settin |
|-------------------------------|
|-------------------------------|

| Status | Network | Wireless 2.4 | 1GHz | Wireless | 5GHz | SIP | FXS1 | FXS2 | Secu | irity | Application |
|-----------|--------------------|--------------|--------|----------|---------|---------|----------|------------|----------|-----------------------|-------------|
| Basic | Wireless Securi | ty WMM | WDS | WPS | Station | Info | Advanced | | | | |
| Wi-Fi | Security Sett | ings | | | | | | | | | |
| Select SS | ID | | | | | | | | | | |
| SSID c | hoice | | | | FWF | 9502-00 | 000C8 • | | | | |
| "FWR9 | 502-0000C8" | | | | | | | | | | |
| Security | y Mode | | | | OPE | NWEP | • | | | | |
| Wire Ec | quivalence Protec | tion (WEP) | | | | | | | | | |
| Default | | | | | WEF | Key 1 | • | | | | |
| | | WEP Key 1 | | | ****** | | Hex | T | 64bit | • | |
| WED K | | WEP Ke | ey 2 | | ****** | | Hex | • | 64bit | • | |
| WEP K | WEP Keys WEP Key 3 | | ****** | | Hex | • | 64bit | • | | | |
| | | WEP Ke | ey 4 | | **** | ****** | | Hex | ۲ | 64bit | • |
| Access | Deligy | | | | | | | | | | |
| Policy | s Policy | | | | Disa | ble 🔻 | | | | | |
| | station MAC | | | | | | (Th | ne maximun | n rule c | ou <mark>nt</mark> is | 64) |

| 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

| Wi-Fi Security Settin | ngs | |
|-----------------------|--|--|
| Select SSID | | |
| SSID choice | | FWR9502-0000C8 ▼ |
| "FWR9502-0000C8" | | |
| Security Mode | | WPA-PSK T |
| WPA | | |
| WPA Algorithms | | ● TKIP ◎ AES ◎ TKIPAES |
| Pass Phrase | | ***** |
| Key Renewal Interval | | 3600 sec (0 ~ 86400) |
| Access Policy | | |
| Policy | | Disable 🔻 |
| Add a station MAC | | (The maximum rule count is 64) |
| Field Name | Description | |
| WPA Algorithms | This item is used to options are TKIP, A | o select the encryption of wireless home gateway algorithms, AES and TKIPAES. |
| Pass Phrase | Setting up WPA-PS | SK security password. |

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 34WPAPSKWPA2PSK

| Wi-Fi Security Settings | 5 | | | | |
|-------------------------|---|--|--|--|--|
| Select SSID | | | | | |
| SSID choice | FWR9502-0000C8 V | | | | |
| "FWR9502-0000C8" | | | | | |
| Security Mode | WPAPSKWPA2PSK 🔻 | | | | |
| WPA WPA Algorithms | ● TKIP ◎ AES ◎ TKIPAES | | | | |
| Pass Phrase | ***** | | | | |
| Key Renewal Interval | 3600 sec (0 ~ 86400) | | | | |
| Field Name | Description | | | | |
| WPA Algorithms | The home gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms. | | | | |
| Pass Phrase | Set WPA-PSK/WPA2-PSK security code | | | | |
| Key Renewal Interval | Set the key scheduled update cycle, default is 3600s | | | | |

WPA-PSK/WPA2-PSK WPA/WPA2 security type is actually a simplified version, which is based on the WPA shared key mode, higher security setting is also relatively simple, suitable for ordinary home users and small businesses.

Wireless Access Policy:

| Table 35 Wireless Access Policy | |
|---|--------------------|
| Access policy | |
| Policy | Allow 💌 |
| Add a station MAC | Disable Allow |
| | Reject |
| | Save Cancel Reboot |

| 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 | 0:1F: D0: 62: BA: FF to the MAC, click Save and reboot the device settings to take |
| effect. | |

WMM

Table 36 WMM

| Status | Netwo | rk W | ireless 2.4 | IGHz | Wireless | 5GHz | SIP | FXS1 | FXS2 | Security | Applicatio |
|--------|----------|----------|-------------|-------|-----------|-------------------|----------|----------|------|----------|------------|
| Basic | Wireless | Security | WMM | WDS | WPS | Station | Info | Advanced | | | |
| | | | | WM | IM Parame | eters of <i>I</i> | Access I | Point | | | |
| | | AIFSN | 1 | CWMin | | CWMax | | TXOP | A | CM | AckPolicy |
| AC_ | BE | 3 | | 15 🔻 | | 63 🔻 | | 0 | /6 | | |
| AC_ | BK | 7 | | 15 🔻 | | 1023 🔻 | | 0 | | | |
| AC | VI | 1 | | 7 🔻 | | 15 🔻 | | 94 | (| | |
| AC_ | VO | 1 | | 3 🔻 | | 7 🔹 | | 47 | 1 | | |

Save & Apply Apply Cancel

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

| Status | Network W | ireless 2.4 | IGHZ | Wireless | 5GHz | SIP | FXS | 1 | FXS2 | Security | Application |
|----------|-------------------|-------------|------|----------|---|--------|-------|-----|------|----------|-------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station | Info | Advar | ced | | | |
| WDS S | etting | | | | | | | | | | |
| DS Confi | ig | | | | | | | | | | |
| WDS Mo | ode | | | | Disa | 2000 C | • | | | | |
| | | | | | the second se | | | | | | |

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

| Status | Network | Vireless 2.4 | IGHZ | Wireless | s 5GHz | SIP | FXS1 | FXS2 | Security | Applicatio |
|-----------------|-------------------|--------------|----------|-----------|---------|-------------------------|----------|--------|----------|------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station | Info | Advanced | | | |
| WPS S | etting | | | | | | | | | |
| NPS Conf | ig | | | | | | | | | |
| WPS Er Apply | nable 🔻 | | | | | | | | | |
| NPS Sum | mary | | | | | | | | | |
| WPS CL | urrent Status | | | | Idle | | | | | |
| WPS Co | onfigured | | | | Yes | | | | | |
| WPS SS | SID | | | | FWRS | 9502- <mark>0</mark> 00 | IOC8 | | | |
| NPS Prog | ress | | | | | | | | | |
| WPS M | ode | | | | ○ p | IN 🖲 | PBC | | | |
| Apply |] | | | | | | | | | |
| NPS State | us | | | | | | | | | |
| WSC:I | dle | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | 11 | | | Cancel | | |
| - | | | | | | | | Cancer | l. | |
| ield Nam | ne D | escription | | | | | | | | |
| VPS Con | fig | | | | | | | | | |
| VPS | En | able/Disat | ole WPS | functior | า | | | | | |
| VPS Sum | imary | | | | | | | | | |
| VPS Curr | ent Status Disp | lay the cu | rrent st | atus of V | VPS | | | | | |
| | | | | | | | | | | |

Display WPS SSID 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

| Status | Network | Wireless 2. | 4GHz | Wireless | 5GHz | SIP | FXS1 | FXS2 | Security | Application |
|------------|----------------|-------------|------------|------------|---------|------|-----------------|---------------|----------|-----------------|
| Basic | Wireless Secur | ity WMM | WDS | WPS | Station | Info | Advanced | | and Ro | |
| Wirele | ss Status | | | | | | | | | |
| Wireless S | Status | | | | | | | | | |
| Current | Channel | | Channel | 1 | | | | | | |
| FWR950 | 2-0000C8 | | 00:21:F2 | 2:00:00:10 | | | | | | |
| Wirele | ss Network | | | | | | | | | |
| Wireless N | Network | | | | | | | | | |
| MAC A | idress Ai | d PSM | MIMO PS | TX Rate | TxBF | RS | Strea SI SNR | am Snd SNR | | Connect Time |

Description

This page displays information about the current registered clients' connections including operating MAC

address and operating statistics.

Advanced

Table 40 Advanced

| Basic Wireless S | ecurity WMM WDS WPS Station Info Advanced | |
|--|--|-----|
| Advanced Wire | less | |
| Advanced Wireless | | |
| BG Protection Mode | Auto 🔻 | |
| Beacon Interval | 100 ms (range 20 - 999, default 100) | |
| Data Beacon Rate (| DTIM) 3 (range 1 - 255, default 3) | |
| Fragment Threshold | 2346 (range 256 - 2346, default 2346) | |
| RTS Threshold | 2347 (range 1 - 2347, default 2347) | |
| TX Power | 100 % (range 1 - 100, default 100) | |
| Short Preamble | Enable | |
| Short Slot | Enable Disable | |
| TX Burst | Enable | |
| Pkt_Aggregate | 💿 Enable 💿 Disable | |
| Country Code | NONE | |
| Support Channel | Ch1~14 ▼ | |
| Tx Beamforming | Disable v | |
| Wi-Fi Multimedia WMM Capable Multiple SSID Multiple SSID1 Multiple SSID2 Multiple SSID3 | | |
| APSD Capable | 🔍 Enable 💿 Disable | |
| Multicast-to-Unicast | | |
| Multicast-to-Unicast | | |
| ield Name | Description | |
| G Protection Mod | e Select G protection mode, options are on, off and automatic. | |
| eacon Interval | The interval of sending a wireless beacon frame, within this range, it will send | а |
| | beacon frame for the information of the surrounding radio network. | |
| ata Beacon | Specify the interval of transmitting the indication message, it is a kind of cut d | owr |
| | | |
| ate(DTIM) | operation, and it is used for informing the next client which is going to receive | 1 |
| | broadcast multi-cast. | |
| | | |
| ragment Threshold | d Specify the fragment threshold for the packet, when the length of the packet | |

| 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 |
| | ТСР |
| 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- | Enable/Disable Multicast-to-Unicast. By default, it is Disabled |
| Unicast Converter | |

Wireless 5G

Please refer to the wireless 2.4G.

SIP

SIP Settings

Table 41 SIP settings

| Status Network Wi | reless 2.4GHz Wir | eless 5GHz | SIP | FXS1 | FXS2 | Security | Applicat |
|----------------------------|---------------------|---------------|----------|------------|----------|----------------|------------|
| SIP Settings VoIP QoS | Dial Rule Blacklist | Call Log | | | | | |
| SIP Parameters | | | | | | | |
| SIP Parameters | | | | | | | |
| SIP T1 | 500 | ms | Max | Forward | | 70 | |
| SIP User Agent Name | | | Max | Auth | | 2 | |
| Reg Retry Intvl | 30 sec | | Reg | Retry Long | Intvl | 60 | sec |
| Mark All AVT Packets | Enable 🔻 | | | 2543 Call | | Enable 🔻 | |
| SRTP | Disable 🔻 | | | Prefer En | | AES_CM ▼ | |
| Service Type | Common 🔻 | | DNS | Refresh Ti | mer | 0 | sec |
| NAT Traversal | | | | | | | |
| NAT Traversal | Disable 🔻 | _ | 220000 | Server A | | - | |
| NAT Refresh Interval (sec) | 60 | | STUP | Server P | ort | | - |
| Field Name | Description | | | | | | |
| SIP T1 | The minimum sc | ale of retran | smissio | n time | | | |
| Max Forward | SIP contains Max | Forward me | essage h | ieader fi | elds use | d to limit the | e requests |
| | for forwards | | | | | | |
| SIP Reg User Agent Name | The agent name | of SIP regist | ered us | er | | | |
| Max Auth | The maximum nu | umber of re | transmi | ssions | | | |

| Mark All AVT | Voice packet marking to enable this item will see the mark on the voice message |
|------------------------|---|
| Packets | when the call environment changed (such as press a key during the call) |
| RFC 2543 Call | Enable the Connection Information field displays the address is 0.0.0.0 in the invite |
| Hold | 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 | The preferred encryption type of calling packet (the Message body of INVITE |
| Encryption | 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 | Set NAT Refresh Interval, default is 60s |
| Interval | |
| STUN Server Port | Set STUN Server Port, default is 5060 |
| | |

VoIP QoS

Table 42 VoIP QoS

| SIP Settings | VoIP QoS | Dial Rule | Blacklist | Call Log | | | |
|----------------|----------|-----------|-----------|----------|--------|--|--|
| QoS Settin | gs | | | | | | |
| iyer 3 QoS | | | | | | | |
| SIP QoS(0-63 |) | 46 | | | | | |
| RTP QoS(0-6 | 3) | 46 | | | | | |
| 1111 (200(0 0. | -, | 10 | | | | | |
| | | | Sav | e Cancel | Reboot | | |
| | | | | | | | |

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

| Status | Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security A | pplicatio |
|------------|--------------|-----------------|--------------------|--------|--------|--------|------------|-----------|
| SIP Settir | ngs VoIP Qot | S Dial Rule | Blacklist Call Log | | | | | |
| Dial Ru | ıle | | | | | | | |
| General | 3 | | | | | | | |
| Dial Rule | e | Disable 🔻 | | | | | | |
| Unmatch | ned Policy | Accept 🔻 | | | | | | |
| | | | | | | | | |
| No. | FXS | Digit | : Мар | | Action | Move U | Move Down | n 🔳 |
| 1 | FXS 1 | N N | rb | | Deny | ~ | V | |
| 2 | FXS 1 | η | 99 | | Deny | | ~ | |
| FXS | | FXS | 1 🔻 | | | | | |
| Digit Map | | | | | | | | |
| Action | | Den | у 🔻 | | | | | |
| | | OK Cance | | | | | | |
| | | | Save Cancel | Reboot | | | | |

| 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 | |
|--------------------------------------|--|
| | |

| Dial Plan | | |
|--|---------------------------------|--------------------------|
| General Dial Plan Unmatched Policy | Disable V | |
| No. FXS | Digit Map | Action Move Up Move Down |
| FXS | FXS 1 V | |
| Digit Map | | |
| Action | Deny 🔻 | |
| | OK Cancel | |
| Description | | |
| Step 1. Enable Dial Pla | n | |
| Step 2. Click Add butto | on, and the configuration table | |
| Step 3. Fill in the value | of parameters | |
| Step 4. Press OK butto | n to end configuration | |

Dial Plan Syntactic

Table 45 Dial Plan

| No. | String | Description |
|-----|---|--|
| 1 | 0123456789*# | Allowed characters |
| 2 | X | Lowercase letter "x" stands for one legal character |
| | | To match one character form sequence. For example: |
| | [sequence] | [0-9]: match one digit form 0 to 9 |
| 3 | | [23-5*]: match one character from 2 or 3 or 4 or 5 or * |
| 4 | | Match to x, xx, xxx, xxxx and so on. |
| | х. | For example: |
| | | "01" can be match to "0","01","011""011111" and so on |
| 5 | | Replace dialed with substituted. |
| | <dialed:substituted></dialed:substituted> | For example: |
| | | <8:1650>123456: input is "85551212", output is "16505551212" |
| | | Make outside dial tone after dialing "x", stop until dialing character "y" |
| | | For example: |
| 6 | х,у | "9,1xxxxxxxxx" :the device reports dial tone after inputting "9", stops tone until inputting "1" |
| | | "9,8,010x" : make outside dial tone after inputting "9", stop tone until inputting "0" |
| | | Set the delayed time. For example: |
| 7 | Т | "<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

| And a second | pload && Dow | nioau |
|--|---------------|---------------------|
| acklist Uploa | d && Download | П |
| | | |
| Local File | Choose | File No file chosen |

| Blackli | st | | | |
|-----------|------------------------------------|------------------------------------|---------------------|------------------|
| Index | Name | Number | | |
| 1 | Rob | 12345 | | |
| 2 | Henry | 123456 | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Edit Add | Delete Move to phonebook | | |
| Descrip | tion | | | |
| Click 选 | 择文件 to select the blacklist | file and upload CSV to upload i | it to device; Click | download CSV |
| to save t | he blacklist file to your local co | omputer. | | |
| Select or | ne contact and click edit to cha | ange the information, click delete | e to delete the con | tact, 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.

| Name | Ded |
|--------|-----------|
| Number | 123589 |
| | OK Cancel |

Call Log

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

Table 47 Call log

| 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 | Γ |
| 5 | 123 | 10/28 16:20 | 00:00:13 | |
| 6 | 123 | 10/28 16:21 | 00:00:34 | Г |
| 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 | |
| x 27 | 100 | 10/00/15/07 | | - |

Redial List

| Index | NUMBER | Start Time | Duration | |
|-------|--------|---------------|----------|---|
| 1 | 22222 | 10/21 09:56 | 00:00:40 | |
| 2 | 110 | 10/21 18:14 | 00:00:03 | Γ |
| 3 | 110 | 10/21 18:15 | 00:00:07 | |
| 4 | sipp | 10/23 13:40 | 00:00:06 | Γ |
| 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 | Γ |
| | - | iologic is in | | - |

Answered Calls

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

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

| Status Network W | /ireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application |
|---|-----------------|---------------------|---------------------|---------------------|-----------|----------------|-------------|
| SIP Account Preferences | | | | | | | |
| Basic | | | | | | | |
| Basic Setup | | | | | | | |
| Line Enable | Enable • | | Outgoin Registra | g Call with tion | put | Disable 🔻 | |
| Proxy and Registration — | | | | | | | |
| Proxy Server | | | Proxy Po | ort | | 5060 | |
| Outbound Server | | | Outboun | d Port | | 5060 | |
| Backup Outbound Server | | | Backup (| Outbound P | Port | 5060 | |
| Allow DHCP Option 120 to Override SIP Server | Disable 🔻 | | | | | | |
| Subscriber Information | | | | | | | |
| Display Name | | | Phone N | lumber | | | |
| Account | | | Passwor | ď | | | |
| Field Name | Description | | | | | | |
| Line Enable | Enable/Disable | e the line. | | | | | |
| | Enable/Disable | e PEER to PEER. | | | | | |
| Peer To Peer | If enabled, SIP | -1 will not send re | egister re | equest to | SIP serv | er; but in Sta | itus/ SIP |
| | Account Statu | s webpage, Status | s is Regis | tered; lin | ies 1 can | dial out, b | ut the |
| | external line n | umber cannot dia | aled line: | 1. | | | |
| Proxy Server | The IP address | or the domain o | f SIP Ser | ver | | | |
| Outbound Server | The IP address | or the domain o | f Outbou | ind Serve | er | | |
| Backup Outbound Server | The IP address | or the domain o | f Backup | Outbour | nd Serve | r | |
| Proxy port | SIP Service po | rt, 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 Configurati | on | | |
|--------------------------|----------------------|----------------------------------|-------------------|
| Codec Setup | | | |
| Audio Codec Type 1 | G.711U 🔻 | Audio Codec Type 2 | G.711A 🔻 |
| Audio Codec Type 3 | G.729 T | Audio Codec Type 4 | G.722 T |
| Audio Codec Type 5 | G.723 T | G.723 Coding Speed | 5.3k bps 🔻 |
| Packet Cycle(ms) | 20ms 🔻 | Silence Supp | Disable 🔻 |
| Echo Cancel | Enable 🔻 | Auto Gain Control | Disable 🔻 |
| FAX Configuration | | | |
| FAX Mode | T.38 V | ByPass Attribute Value | fax 🔻 |
| T.38 CNG Detect | Disable 🔻 | T.38 CED Detect Enable | Enable 🔻 |
| gpmd attribute Enable | Disable 🔻 | T.38 Redundancy | Disable 🔻 |
| Audio Codec Type1 | Choose the audio coo | dec type from G.711U, G.711A, G. | 722, G.729, G.723 |
| Audio Codec Type2 | Choose the audio coo | dec type from G.711U, G.711A, G. | 722, G.729, G.723 |
| Audio Codec Type3 | Choose the audio coo | dec type from G.711U, G.711A, G. | 722, G.729, G.723 |
| Audio Codec Type4 | Choose the audio coo | dec type from G.711U, G.711A, G. | 722, G.729, G.723 |
| Audio Codec Type5 | Choose the audio coo | dec 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

| Supplementary Se | rvice Subscription | | | |
|------------------------|--|------------------------------------|-------------------------|--|
| Supplementary Services | s — | | | |
| Call Waiting | Enable • | Hot Line | | |
| MWI Enable | Enable 🔻 | Voice Mailbox Numbers | | |
| MWI Subscribe Enable | Disable 🔻 | VMWI Serv | Enable 🔻 | |
| DND | Disable 🔻 | | | |
| Speed Dial | | | | |
| Speed Dial 2 | | Speed Dial 3 | | |
| Speed Dial 4 | | Speed Dial 5 | | |
| Speed Dial 6 | | Speed Dial 7 | | |
| Speed Dial 8 | | Speed Dial 9 | | |
| Field Name | Description | | | |
| Call Waiting | Enable/Disable Call W | Vaiting | | |
| lot Line | Fill in the hotline num | nber,Pickup handset or press hands | -free or headset button | |
| | the device will dial ou | ut the hotline number automaticall | у | |
| VIWI Enable | Enable/Disable MWI (message waiting indicate). If the user needs to user voice | | | |
| | mail, please enable th | his feature | | |
| VIWI Subscribe Enable | Enable/Disable MWI | Subscribe | | |

| Voice Mailbox | Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice |
|---------------|--|
| Numbers | 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 |
| | |
| | Enter the speed dial phone numbers. Dial *74 to active speed dial function. |
| 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 |

Advanced

Table 51 Advanced

Advanced

| Domain Name Type | Enable 🔻 | Carry Port Information | Disable 🔻 |
|----------------------------------|-----------------------|-----------------------------------|-----------|
| Signal Port | 5060 | DTMF Type | RFC2833 • |
| RFC2833 Payload(>=96) | 101 | Register Refresh Interval(sec) | 3600 |
| RTP Port | 0 (=0 auto select) | Cancel Message Enable | Disable 🔻 |
| Session Refresh Time(sec) | 0 | Refresher | UAC 🔻 |
| Prack Enable | Disable 🔻 | SIP OPTIONS Enable | Disable 🔻 |
| Primary SER Detect Interval | 0 | Max Detect Fail Count | 3 |
| Keep-alive Interval(10-60s) | 15 | Anonymous Call | Disable • |
| Anonymous Call Block | Disable 🔻 | Proxy DNS Type | А Туре 🔻 |
| Jse OB Proxy In Dialog | Disable 🔻 | Reg Subscribe Enable | Disable 🔻 |
| Dial Prefix | | User Type | IP 🔻 |
| Hold Method | ReINVITE * | Request-URI User Check | Disable 🔻 |
| Only Recv Request From Server | Enable • | Server Address | |
| SIP Received Detection | Disable 🔻 | VPN | Disable 🔻 |
| Country Code | | Remove Country Code | Disable 🔻 |
| Caller ID Header | FROM • | | |

| 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 | Enable/Disable the only receive request from server. |
| 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 52Volume settings

| Preferences | |
|--------------------|---|
| Volume Settings | |
| Handset Input Gain | Handset Volume 5 T |
| | |
| Field Name | Description |
| | |
| Handset Input Gain | Adjust the handset input gain from 0 to 7 |

Regional

Table 53 Regional

| Regional | | | | | |
|---------------------------|--|-------------------------------------|--------------------------|--|--|
| Tone Type | China 🔻 | | | | |
| Dial Tone | | | | | |
| Busy Tone | | | | | |
| Off Hook Warning Tone | | | | | |
| Ring Back Tone | | | | | |
| Call Waiting Tone | | | | | |
| Min Jitter Delay(0-600ms) | 20 | Max Jitter Delay(20-1000ms) | 160 | | |
| Ringing Time(10-300sec) | 60 | | | | |
| Ring Waveform | Sinusoid 🔻 | Ring Voltage(40-63 Vrms) | 45 | | |
| Ring Frequency(15-30Hz) | 25 | VMWI Ring Splash Len(0.1- 10sec) | 0.5 | | |
| Flash Time Max(0.2-1sec) | 0.9 | Flash Time Min(0.1-0.5sec) | 0.1 | | |
| Field Name | Description | | | | |
| Топе Туре | Choose tone type form Chi | na, 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 | ter 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 gat | eway's jitter delay, home gatewa | ay is an adaptive jitter | | |
| | mechanism. | | | | |
| Ringing Time | How long the device will rin | ng when there is an incoming cal | Ι. | | |
| Ring Waveform | Select regional ring wavefo | rm, options are Sinusoid and Tra | pezoid, the default | | |
| | Sinusoid. | | | | |
| Ring Voltage | Set ringing voltage, the def | ault value is 70. | | | |
| Ring Frequency | Set ring frequency, the defa | ault value is 25. | | | |
| VMWI Ring Splash | Set the VMWI ring splash le | ength, default is 0.5s. | | | |
| Len(sec) | | | | | |
| Flash Time Max(sec) | Set the Max value of the de | evice's flash time, the default val | ue 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 54Features and call forward

| All Forward | Disable 🔻 | Busy Forward | Disable • |
|-------------------|-----------|--|-----------|
| No Answer Forward | Disable 🔻 | | 17 |
| all Forward | | | |
| All Forward | | Busy Forward | |
| No Answer Forward | | No Answer Timeout | 20 |
| eature Code | | | |
| Hold Key Code | *77 | Conference Key Code | *88 |
| Transfer Key Code | *98 | IVR Key Code | **** |
| R Key Enable | Disable 🔻 | R Key Cancel Code | R1 🔻 |
| it not chable | | The second s | |
| R Key Hold Code | R2 • | R Key Transfer Code | R4 🔻 |

| Field | | |
|----------|-------------------|--|
| Name | | Description |
| | All Forward | Enable/Disable forward all calls |
| Features | Busy Forward | Enable/Disable busy forward. |
| | No Answer Forward | Enable/Disable no answer forward. |
| | All Forward | Set the target phone number for all forward. |
| Call | | The device will forward all calls to the phone number immediately |
| Forward | | 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. |
| | Hold key code | Call hold signatures, default is *77. |
| Feature | Conference key | Signature of the tripartite session, default is *88. |
| Code | code | |

| 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

Escaped char enable

| Miscellaneous - | | | | |
|-------------------------------------|------------------------|---------------------------|-------------------------------------|------------|
| Codec Loop Current | 26 | Impedance Maching | US PBX,Korea,Taiwan(600) | • |
| CID Service | Enable 🔻 | CWCID Service | Disable 🔻 | |
| Caller ID Method | Bellcore 🔹 | Polarity Reversal | Disable 🔻 | |
| Dial Time Out(IDT) | 5 | Call Immediately Key | # | |
| ICMP Ping | Disable 🔻 | Escaped char enable | Disable 🔻 | |
| Bellcore Style 3- Way Conference | Disable T | | | |
| Field Name | Description | | | |
| Codec Loop Currer | nt Set off-hook loop c | urrent, default is 26. | | |
| Impedance Machi | ng Set impedance mat | ching, default is US PB | SX,Korea,Taiwan(600). | |
| CID service | Enable/Disable disp | playing caller ID; If ena | ble, caller ID is displayed when t | here is an |
| | incoming call or it v | won't be displayed. De | fault is enable. | |
| CWCID Service | Enable/Disable CW | CID. If enable, the dev | ice will display the waiting call's | caller ID, |
| | or it won't display. | Default is disable. | | |
| Dial Time Out | How long device wi | ill sound dial out tone | when device dials a number. | |
| Call Immediately K | Key Choose call immed | iately key form * or #. | | |
| ICMP Ping | Enable/Disable ICN | 1P Ping. | | |

If enable this option, home gateway will ping the SIP Server every interval

Open special character translation function; if enable, when you press the # key, it

time, otherwise, It will send "hello" empty packet to the SIP Server.

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

| Disable V Drop V |
|---------------------|
| Drop V |
| |
| |
| |
| |
| |
| |
| LAN 🔻 |
| |
| |
| |
| NONE V |
| - |
| - |
| Accept 🔻 |
| |
| |

| 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

| Filtering Setting Content Filtering | |
|-------------------------------------|------------------|
| Basic Settings | |
| Basic Settings | |
| Filtering | Disable T |
| Default Policy | Accept 🔻 |
| Save Cancel | |
| Filter List Upload & Download | |
| Local File 选择文件 未选择任何文件 | |
| Upload Download | |
| Web URL Filter Settings | |
| Current Web URL Filters | |
| No. | URL |
| | Delete Cancel |
| Add a URL Filter | |
| URL | |
| (The maximum rule count is 16) | |
| | Add Cancel |
| Web Host Filter Settings | |
| Current Website Host Filters | |
| No. | Keyword |
| | Delete Cancel |
| Add a Host (keyword) Filter | |
| Keyword | |
| (The maximum rule count is 16) | |
| | Add Cancel |

| Field Name | Description |
|--------------------------|--|
| Filtering | Enable/Disable content Filtering |
| Default Policy | The default policy is to accept or to prohibit filtering rules |
| Current Webs URL Filters | List the URL filtering rules that already existed (blacklist) |
| Delete/Cancel | You can choose to delete or cancel the existing filter rules |
| Add a URL Filter | Add URL filtering rules |
| Add/Cancel | Click adds to add one rule or click cancel |
| Current Website Host | List the keywords that already exist (blacklist) |
| Filters | |
| 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

Table 58 advance NAT

| ALG | | |
|------------|-----------|--|
| LG Setting | | |
| FTP | Enable 🔻 | |
| SIP | Disable 🔻 | |
| H323 | Disable 🔻 | |
| PPTP | Disable 🔻 | |
| L2TP | Disable 🔻 | |
| IPSec | Disable 🔻 | |

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

| UPnP | | |
|--------------------|-------------------------|--------------------|
| UPnP S UPnP ena | etting able Enable 💌 | Save Cancel Reboot |
| 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

| Status Network | Wireless | SIP FXS | 1 FXS2 | Security | Application | Administration |
|----------------------|----------|------------|------------|-------------|-------------|----------------|
| Advance Nat UPnP | IGMP | | | | | • |
| IGMP | | | | | | |
| IGMP Setting | | | | | | |
| IGMP Proxy enable | Enable 🔻 | | | | | |
| IGMP Snooping enable | Enable 🔻 | | | | | |
| | | | | | | |
| | | | | 77. | | |
| | | Save & App | ly Save Ca | ncel Reboot | | |

| 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

| Status | Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application | Storage |
|---|--|-----------------|----------------|-----------|------|------|----------|-------------|---------|
| Disk Management FTP Setting SMB Setting | | | | | | | | | |
| Disk Ma | Disk Management Help | | | | | | | | |
| Folder List | | | | | | | | | |
| Dire | ctory Path | | Pa | rtition | | | | | |
| | | | Add Delete Ren | nove Disk | | | | | |
| Partition S | tatus | | | | | | | | |
| Part | ition | Path | | | | | | | |
| | | | Format Real | locate | | | | | |
| | | | | | | | | | |
| Field Na | me | Descri | ption | | | | | | |
| Add | dd Adding files to the USB storage device | | | | | | | | |
| Delete | Delete Remove the USB storage device file | | | | | | | | |
| Remove [| Remove Disk Transfer files within a USB storage device | | | | | | | | |
| Format | Format Format the USB storage device | | | | | | | | |
| Re-alloca | Re-allocate Reset the USB storage device | | | | | | | | |

Table 62 FTP Setting

| Status Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application | Storage |
|-----------------------|-----------------|---------------|---------|---------|------|----------|-------------|---------|
| Disk Management FTF | Setting SMB Set | etting | | | | | | |
| FTP Setting | | | | | | | | Help |
| P Server Setup | | | | | | | | |
| FTP Server | | Θe | nable (| Disable | | | | |
| FTP Server Name | | FTP | | | | | | |
| Anonymous Login | | ● E | nable | Disable | | | | |
| FTP Port | | 21 | | | | | | |
| Max. Sessions | | 10 | | | | | | |
| Create Directory | | () E | nable | Disable | | | | |
| Rename File/Directory | | . E | nable | Disable | | | | |
| Remove File/Directory | | () E | nable | Disable | | | | |
| Read File | | () E | nable | Disable | | | | |
| Write File | | () E | nable (| Disable | | | | |
| Download Capability | | () E | nable | Disable | | | | |
| Upload Capability | | @ E | nable | Disable | | | | |

| 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

| Status Network | Wireless 2.4GHz | Wireless 5GHz | SIP FXS1 | FXS2 | Security | Application | Storage |
|------------------------|---------------------|-----------------|-----------------|------|----------|-------------|---------|
| Disk Management F | TP Setting SMB Sett | ing | | | | | |
| SMB Setting | | | | | | | Help |
| SAMBA Server Setup | | | | | | | |
| SAMBA Server | | © E | nable 💿 Disable | | | | |
| Workgroup | | FWR | 9502 | | | | |
| NetBIOS Name | | FileS | hare | | | | |
| Anonymous Login | | 0 E | nable 💿 Disable | | | | |
| Sharing Directory List | | | | | | | |
| Directory Name | Directory Pat | h Allow | ed Users | | | | |
| | | Add Edit | Delete | | | | |
| | | | | | | | |
| | | Apply Can | tel | | | | |
| Field Name | Descri | ption | | | | | |
| SAMBA Server | Enable/Disab | le SAMBA serv | er | | | | |
| Workgroup | Enter the wo | rking group | | | | | |
| NetBIOS Name | Network bas | ic input/output | t system nam | е | | | |
| Add | Add a shared | file | | | | | |
| Edit | Edit a shared | file | | | | | |
| Del | Delete a shar | ed file | | | | | |
| Add | Add a shared | file | | | | | |
| Edit | Edit a shared | file | | | | | |
| Del | Delete a shar | ed 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

| Save Config | File | | | |
|------------------|---------------|---------|--|--|
| onfig File Uploa | d && Download | | | |
| Local File | 选择文件 | 未选择任何文件 | | |
| Upload Dow | nload | | | |
| | | | | |

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

Administrator settings

Table 65 Administrator settings

| Administrator Settings | | | | | |
|---|----------------------|---------------------|--|--|--|
| Password Reset | | | | | |
| User Type | | Admin User 🔻 | | | |
| New User Name | | admin | | | |
| New Password | | | (The maximum length is 25) | | |
| Confirm Password | | | | | |
| Language | | | | | |
| Language | | English 🔻 | | | |
| VPN Access | | | | | |
| Management Using VPN | | Disable 🔻 | | | |
| Web Access | | | | | |
| Remote Web Login | | Enable 🔻 | | | |
| Local Web Port | | 80 | | | |
| Web Port | | 80 | | | |
| Web SSL Port | | 443 | | | |
| Web Idle Timeout(0 - 60min) | | 5 | | | |
| Allowed Remote IP(IP1;IP2;) | | 0.0.0.0 | | | |
| Telnet Access | | | | | |
| Remote Telnet | | Enable 🔻 | | | |
| Telnet Port | | 23 | | | |
| Allowed Remote IP(IP1;IP2;) | i) | 0.0.00 | | | |
| HostName | | FWR8102 | | | |
| Field Name | Description | | | | |
| User type | Choose the user typ | e from admin use | r 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 passv | vord | | | |
| confirm Password Input the new password again | | | | | |
| Language | Select the language | for the web, the c | device support Chinese, English, and Spanish | | |
| | and so on | | | | |
| Remote Web Login | Enable/Disable remo | ote Web login | | | |
| Web Port | Set the port value w | hich is used to log | gin 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 We | |
|-----------------------------|---|--|
| | 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

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

Daylight Saving Time

Disable 🔻

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

| Secondary NTP Server | Options for NTP server's IP address or domain name | |
|----------------------|--|--|
| NTP synchronization | NTP synchronization cycle, cycle time can be 1 to 1440 minutes in any one, the | |
| | default setting is 60 minutes | |

Daylight Saving Time

Table 67 Daylight Saving Time

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

Procedure

Step 1. Enable Daylight Savings Time.

Step 2. Set value of offset for Daylight Savings Time

Step 3: Set starting Month/Week/Day/Hour in Start Month/Start Day of Week Last in Month/Start Day of

Week/Start Hour of Day, analogously set stopping Month/Week/Day/Hour in Stop Month/Stop Day of Week Last in Month/Stop Day of Week/Stop Hour of Day.

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

System Log Setting

Table 68 System log Setting

| Syslog Setting | |
|---------------------------------|-----------|
| Syslog Enable | Enable 🔻 |
| Syslog Level | INFO 🔻 |
| Login Syslog Enable | Enable 🔻 |
| Call Syslog Enable | Enable 🔻 |
| Net Syslog Enable | Enable 🔻 |
| Device Management Syslog Enable | Enable 🔻 |
| Device Alarm Syslog Enable | Enable 🔻 |
| Kernel Syslog Enable | Enable 🔻 |
| Remote Syslog Enable | Disable 🔻 |
| Remote Syslog Server | |

| Field Name | Description | |
|----------------------|---|--|
| Syslog Enable | Enable/Disable syslog function | |
| Syslog Level | Select the system log, there is INFO and Debug two grades, the Debug INFO can | |
| | provide more information | |
| Remote Syslog Enable | Enable/Disable remote syslog function | |
| Remote Syslog server | Add a remote server IP address. | |
| Syslog Enable | Enable/Disable syslog function | |

Factory Defaults Setting

Table 69 Factory Defaults Setting

| ctory Defaults Setting | | |
|------------------------|-----------|--|
| Factory Defaults Lock | Disable 🔻 | |

Description

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

Factory Defaults

Table 70 Factory Defaults

Factory Defaults

Reset to Factory Defaults

Factory Default

Description

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

Firmware Upgrade

Table 71 Firmware upgrade

| Status Network Wireless 2.4GHz Wireless 5GHz SIP FXS1 FXS2 | | | | | | FXS2 | Secur | rity A | Application | | |
|--|--|---------------|-----------|----------|-------------|-------|-------------|--------|-------------|------|--------|
| Managemer | : Firmw | are Upgrade | LTE Upg | grade | Scheduled | Tasks | Certificate | es Pro | vision | SNMP | TR-069 |
| Firmwar | Manage | ment | | | | | | | | | |
| Firmware Up | grade — | | | | | | | | | | |
| Local Upgra | de [| 选择文件未过 | 先择任何文 | 件 | | | | | | | |
| | | | | | Upgrade |] | | | | | |
| Descriptio | า | | | | | | | | | | |
| 1. Choose | upgrade f | ile type fron | n Image F | File and | d Dial Rule | ē | | | | | |
| 2. Press ' | 2. Press "Browse" button to browser file | | | | | | | | | | |
| 3. Press | Upgrade | to start up | grading | | | | | | | | |

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 72 Provision

| Status Netv | work Wireless 2 | .4GHz Wi | eless 5GHz | SIP | FXS1 | FXS2 | Secu | rity / | Applicatio |
|------------------|------------------|-------------|------------|-------------|-------------|-------------|-----------|--------------------------|------------|
| Management | Firmware Upgrade | LTE Upgrade | Scheduled | l Tasks | Certificat | tes Pro | ovision | SNMP | TR-069 |
| Provision | | | | | | | | | |
| onfiguration Pro | ofile | | | | | | | | |
| Provision Enable | 9 | | Disa | able ▼ | | | | | |
| Resync on Rese | t | | Ena | ble 🔻 | | | | | |
| Resync Random | Delay (sec) | | 40 | | | | | | |
| Resync Periodic | (sec) | | 360 |) | | | | | |
| Resync Error Re | try Delay (sec) | | 3600 |) | | | | | |
| Forced Resync D | Delay (sec) | | 1440 | 00 | | | | | |
| Resync after Up | grade | | Ena | Enable 🔻 | | | | | |
| Resync from SIF | 5 | | Disa | ible 🔻 | | | | | |
| Option 66 | | | Ena | ble 🔻 | | | | | |
| Option 67 | | | Ena | ble 🔻 | | | | | |
| Config File Nam | e | | \$(M) | A) | | | | | |
| User Agent | | | | | | | | | |
| Profile Rule | | | http | ://prv1.fly | ingvoice.ne | t:69/config |)/\$(MA)? | mac= <mark>\$(</mark> M/ | A)&: |

| 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 |
|-------------------------------|--|
| Resync Periodic(sec) | default is 40. If the last resync was failure, The router will retry resync after the |
| | "Resync Error Retry Delay "time, default is 3600s. |
| Resync Error Retry Delay(rec) | Set the periodic time for resync, default is 3600s. |
| Forced Resync Delay(sec) | If it's time to resync, but 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 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 73 Firmware Upgrade

| mware Upgrade | | |
|--------------------------------|----------|--|
| Upgrade Enable | Enable 🔻 | |
| Upgrade Error Retry Delay(sec) | 3600 | |
| Upgrade Rule | | |

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

SNMP

Table 74 SNMP

| Management | Firmware Upgrade | LTE Upgrade | Scheduled Tasks | Certificates | Provision | SNMP | TR-06 | | |
|----------------------------|------------------|-------------|-----------------|--------------|-----------|------|-------|--|--|
| SNMP Conf | iguration | | | | | | | | |
| MP Configura | ation | | | | | | | | |
| SNMP Service | | | Enable • | | | | | | |
| Trap Server Address | | | 183.234.48.155 | | | | | | |
| Read Community Name | | | public | | | | | | |
| Write Commu | nity Name | | private | | | | | | |
| Trap Community | | | trap | | | | | | |
| Trap Period Interval (sec) | | | 300 | | | | | | |

Save & Apply Save Cancel Reboot

| 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

ACS username

ACS password

User Name

Password

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

| Table 75 TR069 | | | | | | | | | | | | | |
|-----------------------|---------------|--------------------|---------------|----------|--------------|-----------|------|--------|--|--|--|--|--|
| Management Fin | mware Upgrade | LTE Upgrade | Scheduled | Tasks | Certificates | Provision | SNMP | TR-069 | | | | | |
| TR-069 Configu | ration | | | | | | | | | | | | |
| ACS | | | | | | | | | | | | | |
| TR-069 Enable CWMP | | Enable T | | | | | | | | | | | |
| ACS URL | http:/ | /acs1.flyingvoice. | net:8080/tr06 | 9 | | | | | | | | | |
| User Name | | | | <u>.</u> | | | | | | | | | |
| Password | | | | •••••• | | | | | | | | | |
| Enable Periodic Info | rm Enab | Enable 🔻 | | | | | | | | | | | |
| Periodic Inform Inte | arval 3600 | 3600 | | | | | | | | | | | |
| Connect Request | | | | | | | | | | | | | |
| User Name | FWR9 | R9502 | | | | | | | | | | | |
| Password | ••••• | •••• | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | Save & Apply | y Save C | ancel | Reboot | | | | | | | | |
| | | | | | | | | | | | | | |
| Field Name | Des | cription | | | | | | | | | | | |
| ACS parameters | | | | | | | | | | | | | |
| TR069 Enable | Enable or [| Disable TR069 | | | | | | | | | | | |
| CWMP | Enable or I | Disable CWMP | | | | | | | | | | | |
| ACS URL | ACS URL ac | ldress | | | | | | | | | | | |

| 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 76 Diagnosis

| Management | Firmware Upgrade | LTE Upgrade | Scheduled Tasks | Certificates | Provision | SNMP | TR-069 | Diagnosis |
|----------------|------------------|-------------|------------------|---------------|-----------|------|--------|-----------|
| Packet Trac | ce | | | | | | | Нејр |
| Packet Trace | | | | | | | | |
| Tracking Inter | face | WAI | ▼ N | | | | | |
| Packet Trace | | sta | t stop save | | | | | |
| Ping Test | | | | | | | | |
| Ping Test | | | | | | | 12 | |
| Dest IP/Host N | Name | | | | | | | |
| WAN Interface | 9 | 1_M | ANAGEMENT_VOICE_ | INTERNET_R_VI | ID_ ▼ | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | 4 | | | |
| Apply Ca | ncel | | | | | | | |

Traceroute Test

| Dest IP/Host Name | |
|-------------------|------------------------------------|
| WAN Interface | 1_MANAGEMENT_VOICE_INTERNET_R_VID_ |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Description

1. Packet Trace

Users can use the packet trace feature to intercept packets which traverse the device. Click the Start button to start home gateway tracking and keep refreshing the page until the message trace shows to stop, click the Save button to save captured packets.

2. Ping Test

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

| Ping Test | | |
|---|--|--|
| Dest IP/Host Name | | |
| WAN Interface | 1_TR069_VOICE_INTERNET_R_VID_ | |
| | om (115.239.210.26): 56 data bytes | |
| 64 bytes from 11E | | |
| | .239.210.26: seq=0 ttl=54 time=43.979 ms | |
| 64 bytes from 115 | .239.210.26: seq=1 ttl=54 time=53.875 ms | |
| 64 bytes from 115 64 bytes from 115 | .239.210.26: seq=1 ttl=54 time=53.875 ms .239.210.26: seq=2 ttl=54 time=45.226 ms | |
| 64 bytes from 115 64 bytes from 115 64 bytes from 115 | .239.210.26: seq=1 ttl=54 time=53.875 ms .239.210.26: seq=2 ttl=54 time=45.226 ms .239.210.26: seq=3 ttl=54 time=49.534 ms | |
| 64 bytes from 115 64 bytes from 115 64 bytes from 115 | .239.210.26: seq=1 ttl=54 time=53.875 ms .239.210.26: seq=2 ttl=54 time=45.226 ms | |
| 64 bytes from 115 64 bytes from 115 64 bytes from 115 | .239.210.26: seq=1 ttl=54 time=53.875 ms .239.210.26: seq=2 ttl=54 time=45.226 ms .239.210.26: seq=3 ttl=54 time=49.534 ms .239.210.26: seq=4 ttl=54 time=49.045 ms | |
| 64 bytes from 115 64 bytes from 115 64 bytes from 115 64 bytes from 115 www.baidu.con | .239.210.26: seq=1 ttl=54 time=53.875 ms .239.210.26: seq=2 ttl=54 time=45.226 ms .239.210.26: seq=3 ttl=54 time=49.534 ms .239.210.26: seq=4 ttl=54 time=49.045 ms | |

3. Traceroute Test

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

| aceroute Test | | |
|---------------------|--|---|
| Dest IP/Host Name | www.google.com | |
| WAN Interface | 1_MANAGEMENT_VOICE_INTERNET_R_VID_ V | |
| | om (216.58.208.68), 30 hops max, 38 byte packets | |
| | 134.254) 1.017 ms 9.507 ms 1.419 ms | |
| 2 | | Ξ |
| 3 *** | | |
| 4 | | |
| 5 *** | | |
| D | | |
| 1 | | |
| 8 | | 2 |
| | | |
| 9 * * * 10 * * * | | |

Operating Mode

Table 77 Operating mode

| Operating Mode Settings | |
|-------------------------|--------------------|
| Operating Mode Settings | |
| Operating Mode | Basic Mode |
| | Basic Mode |
| | Advanced Mode |
| | Save Cancel Reboot |

Description

Choose the Operation Mode as Basic Mode or Advanced Mode.

System Log

Table 78 System log

| Status | Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application | Storage |
|---|---|-----------------|-------------------|-----|------|------|----------|-------------|---------|
| Basic | LAN Host | Syslog | | | | | | | |
| Refresh | Clear Save |] | | | | | | | |
| ProductCla SerialNuml BuildTime: IP:192.168 HWVer:V4 SWVer:V3. <wed sep<br=""><wed sep<="" td=""><th>.4 .20 6 10:40:39 2(6 10:40:39 2(</th><th>00007</th><th>ew Call from:[][]</th><th>ee</th><th></th><th></th><th></th><th></th><th>*</th></wed></wed> | .4 .20 6 10:40:39 2(6 10:40:39 2(| 00007 | ew Call from:[][] | ee | | | | | * |
| Descri | ption | | | | | | | | |

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

Logout

Π

Table 79 Logout

| Vo. | IP | | ontrol pa | nel | | | | | | Firmware Version V3.3 ime 2017-10-26 09:11:3 [Logout] [Reboot |
|----------|-------------|-----------------|---------------|-----|------|------|----------|-------------|---------|---|
| Status | Network | Wireless 2.4GHz | Wireless 5GHz | SIP | FXS1 | FXS2 | Security | Application | Storage | Administration |
| SIP Acco | unt Prefere | ences | | | | | | | Help | |
| Descri | ption | | | | | | | | | |

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

Reboot

Press the Reboot button to reboot the device.

Chapter 4: IPv6 address configuration

The router devices support IPv6 addressing. This chapter covers:

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

Introduction

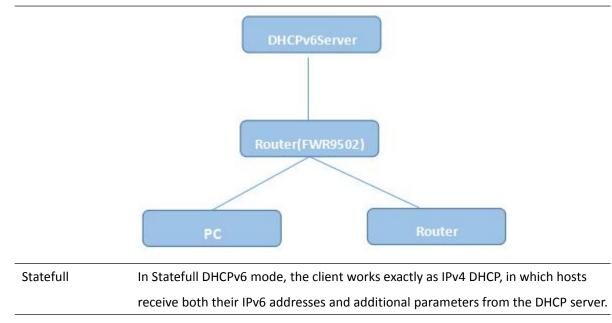
DHCPv6 protocol is used to automatically provision/configure IPv6 capable end points in a local network. In addition to acquiring an IPv6 IP address for the WAN interface and its associated LAN/WLAN clients, the devices are also capable of prefix delegation.

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

- Stateless DHCPv6
- Statefull DHCPv6

Table 80 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. |



IPv6 Advance

To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

Table 81 Enabling IPv6

| Status | Netw | ork | Wireless | 2.4GHz | Wireless 5GHz | SII | P FXS1 | FXS2 | Security | Appl | ication |
|---------------------------------|------|-------|----------|----------|-------------------|--------|-------------|-------|----------|------|---------|
| WAN | LAN | IPv6 | Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forwar | d DMZ | VLAN | QoS | Rate |
| Advance IPv6 A IPv6 Enabl | | d Set | tings | | | | | | | | |
| IPv6 Ena | able | | | Save | E & Apply Save | Cancel | Reboot | | | | |

Configuring IPv6

Configuring Statefull IPv6

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

Table 82 Configuring Statefull IPv6

| WAN LAN IPv6 Advance Advance | d IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | QoS | Rat |
|---------------------------------|-----------------|--------------|-------------------------|--------------|-----|------|-----|-----|
| IPv6 WAN Setting | | | | | | | | |
| IPv6 WAN Setting | | | | | | | | |
| Connection Type | | | DHCPv6 | • | | | | |
| DHCPv6 Address Settings | | | Statefu <mark>ll</mark> | • | | | | |
| Prefix Delegation | Į | Save Cance | Enable 🔻 | 1 | | | | |
| Field Name | Descripti | on | | | | | | |
| Connection Type | Select connec | tion type | | | | | | |
| DHCPv6 Address Settings | Set it to state | full mode. | | | | | | |
| Prefix Delegation | Select Enable | | | | | | | |

Configuring Stateless IPv6

Table 83 Configuring Stateless IPv6

| WAN LAN IPv6 Advance Advance | ad IPv6 WAN | IPv6 LAN VPN | Port Forward | DMZ | VLAN | QoS R | ate |
|---------------------------------|--------------------|----------------|--------------|-----|------|-------|-----|
| IPv6 WAN Setting | | | | | | | |
| IPv6 WAN Setting | | | | | | | 1 |
| Connection Type | | DHCPve | j 🛛 🔻 | | | | |
| DHCPv6 Address Settings | | Statele | is ▼ | | | | |
| Prefix Delegation | | Enable | T | | | | |
| | Sa | ave Cancel Ret | oot | | | | |
| Field Name | Description | n | | | | | |
| Connection Type | Select connection | on type | | | | | |
| DHCPv6 Address Settings | Set it to stateles | s mode | | | | | |
| Prefix Delegation | Select Enable | | | | | | |

Viewing WAN port status

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

| Network Status | |
|-------------------------|----------------------|
| tive WAN Interface | |
| Connection Type | DHCP |
| IP Address | 192.168.10.174 Renew |
| Link-Local IPv6 Address | |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| Primary DNS | 192.168.10.1 |
| Secondary DNS | 192.168.18.1 |
| pv6 PD Prefix | |
| pv6 Domain Name | |
| pv6 Primary DNS | |
| pv6 Secondary DNS | |
| VAN Port Status | 100Mbps Full |

IPv6 DHCP configuration for LAN/WLAN clients

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

LAN DHCPv6

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

To enable LAN DHCPv6 service:

| WAN L | AN IPv6 Advanced | IPv6 WAN IPv6 LAN | VPN Port Forward | DMZ VLAN | QoS Rate I |
|-------------|------------------|-------------------|--------------------|----------|------------|
| Advance | | 1 | 1055 - 55 - 5 1 | | |
| IPv6 LA | N Setting | | | | |
| Pv6 LAN Se | tting | | | | - |
| IPv6 Addr | ess | fec0::1 | | | |
| IPv6 Prefit | k Length | 64 | (0-128) | | |
| DHCPv6 S | erver | | | | |
| DHCPv6 S | tatus | Disable 🔻 | | | |
| DHCPv6 M | lode | Stateless • | | | |
| Domain N | ame | | | | |
| Server Pre | ference | 255 | (0-255) | | |
| Primary D | NS Server | | | | |
| Secondary | DNS Server | | | | |
| Lease Tim | e | 86400 | (0-86400sec) | | |
| IPv6 Addr | ess Pool | | - | / | |
| Router Ad | vertisement | | | ,, | - |
| Router Ad | vertisement | Disable 🔻 | | | |
| Advertise | Interval | 30 | (10-1800sec) | | |
| RA Manag | ed Flag | Disable 🔻 | | | |
| RA Other | Flag | Enable 🔻 | | | |
| Prefix | | | / | | |
| Prefix Life | time | 3600 | (0-3600sec) | | |
| | | | | | |

Chapter 5: Troubleshooting Guide

This chapter covers:

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

Configuring PC to get IP Address automatically

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

Step 1 : Click the "Start" button

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

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

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

| letworking Sharing | General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. | | | | |
|---|---|-----------|--|--|--|
| Connect using: Microsoft Virtual WiFi Miniport Adapter #2 | | | | | |
| Configure | Obtain an IP address automat | ically | | | |
| This connection uses the following items: | Use the following IP address: | | | | |
| Client for Microsoft Networks | IP address: | | | | |
| ✓ ■ QoS Packet Scheduler ✓ ■ File and Printer Sharing for Microsoft Networks | Subnet mask: | | | | |
| Internet Protocol Version 6 (TCP/IPv6) | Default gateway: | | | | |
| A Internet Protocol Version 4 (TCP/IPv4) A Link-Layer Topology Discovery Mapper I/O Driver A Link-Layer Topology Discovery Responder | Obtain DNS server address au Use the following DNS server a | | | | |
| Install Uninstall Properties | Preferred DNS server: | | | | |
| Description | Alternate DNS server: | · · · · | | | |
| Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. | Validate settings upon exit | Advanced | | | |
| | 1 | OK Cancel | | | |

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.