



User Manual

FWR8102/8101/8100

Contents

| | |
|--|-----------|
| About This User Guide | 1 |
| FlyingVoice Contact Details :..... | 2 |
| Purpose..... | 3 |
| Cross references..... | 3 |
| Feedback..... | 3 |
| Declaration of Conformity..... | 4 |
| Part 15 FCC Rules..... | 4 |
| Warnings and Notes..... | 5 |
| Warnings..... | 5 |
| Notes..... | 5 |
| Chapter 1 Product description | 6 |
| FWR8100/FWR8101/FWR8102..... | 7 |
| LED Indicators and Interfaces..... | 8 |
| Interactive Voice Response Prompt..... | 14 |
| Chapter 2 Configuring Basic Settings | 19 |
| Two-Level Management..... | 20 |
| Web Management Interface..... | 20 |
| Web Management Interface Details..... | 22 |
| Setting the Time Zone..... | 23 |
| Configuring an Internet Connection..... | 24 |
| Setting up Wireless Connections..... | 26 |
| Configuring Session Initiation Protocol (SIP)..... | 29 |
| Making a Call..... | 32 |
| Chapter 3 Web Interface | 34 |
| Login..... | 35 |
| Status..... | 36 |
| Network and Security..... | 39 |
| WAN..... | 39 |
| LAN..... | 45 |
| LAN Port..... | 45 |
| Wireless..... | 57 |
| SIP..... | 70 |
| SIP Settings..... | 70 |
| FXS1..... | 78 |

Contents

- FXS2..... 88
- Security..... 89
- Application..... 92
- Administration..... 94
 - Management 94
 - Firmware Upgrade..... 99
 - Provision..... 100
 - SNMP..... 102
 - TR-069..... 103
 - Diagnosis..... 105
 - Operating Mode..... 107
 - System Log..... 108
 - Logout..... 108
 - Reboot..... 108
- Chapter 4 IPv6 address configuration..... 109**
 - Introduction..... 110
 - IPv6 Advance..... 111
 - Configuring IPv6..... 111
 - Viewing WAN port status..... 114
 - IPv6 DHCP configuration for LAN/WLAN clients..... 114
 - LAN DHCPv6..... 115
- Chapter 5 Troubleshooting Guide..... 116**
 - Configuring PC to get IP Address automatically..... 117
 - Cannot connect to the Web..... 118
 - Forgotten Password..... 118

Tables

| | |
|--|----|
| Table 1 Features at-a-glance..... | 7 |
| Table 2 LED Indicators..... | 8 |
| Table 3 Interfaces..... | 10 |
| Table 4 Interactive Voice Response Menu Setting Options..... | 14 |
| Table 5 Web management interface..... | 22 |
| Table 6 Setting time zone..... | 23 |
| Table 7 Configuring an internet connection..... | 24 |
| Table 8 Wireless > Basic web page (user view)..... | 26 |
| Table 9 Wireless Security web page..... | 28 |
| Table 10 Configuring SIP via the Web Management Interface..... | 29 |
| Table 11 Registration status..... | 31 |
| Table 12 Login details..... | 35 |
| Table 13 Status Page..... | 36 |
| Table 14 Internet..... | 39 |
| Table 15 DHCP..... | 40 |
| Table 16 PPPoE..... | 41 |
| Table 17 Bridge Mode..... | 43 |
| Table 18 LAN port..... | 45 |
| Table 19 DHCP server settings..... | 47 |
| Table 20 DHCP server, DNS and Client Lease Time..... | 48 |
| Table 21 VPN..... | 48 |
| Table 22 Port Forward..... | 49 |
| Table 23 VLAN..... | 50 |
| Table 24 DMZ..... | 51 |
| Table 25 DDNS setting..... | 51 |
| Table 26 QoS..... | 52 |
| Table 27 Port setting..... | 53 |
| Table 28 Routing..... | 54 |
| Table 29 Advance..... | 55 |
| Table 30 Eoip Tunnel..... | 56 |
| Table 31 Basic..... | 57 |
| Table 32 Wireless security..... | 60 |
| Table 33 WiFi Security Setting..... | 61 |
| Table 34 WPA-PSK..... | 62 |
| Table 35 WPAPSKWPA2PSK..... | 62 |
| Table 36 Wireless Access Policy..... | 63 |
| Table 37 WMM..... | 64 |

Tables

| | | |
|-----------|----------------------------|-----|
| Table 38 | WDS | 65 |
| Table 39 | WPS | 66 |
| Table 40 | Station info | 67 |
| Table 41 | Advanced | 68 |
| Table 42 | SIP settings | 70 |
| Table 43 | VoIP QoS | 71 |
| Table 44 | Parameters and settings | 72 |
| Table 45 | Adding one dial plan | 73 |
| Table 46 | Dial Plan | 74 |
| Table 47 | Blacklist | 75 |
| Table 48 | Call log | 76 |
| Table 49 | SIP Account - Basic | 78 |
| Table 50 | Audio configuration | 79 |
| Table 51 | Supplementary service | 80 |
| Table 52 | Advanced | 81 |
| Table 53 | Volume settings | 83 |
| Table 54 | Regional | 84 |
| Table 56 | Miscellaneous | 87 |
| Table 57 | Filtering setting | 89 |
| Table 58 | Content filtering | 90 |
| Table 60 | UPnP | 92 |
| Table 61 | IGMP | 93 |
| Table 62 | Save Config File | 94 |
| Table 63 | Administrator settings | 95 |
| Table 64 | NTP settings | 96 |
| Table 65 | Daylight Saving Time | 97 |
| Table 66 | System log Setting | 98 |
| Table 67 | Factory Defaults Setting | 98 |
| Table 68 | Factory Defaults | 99 |
| Table 69 | Firmware upgrade | 99 |
| Table 70 | Provision | 100 |
| Table 71 | Firmware Upgrade | 101 |
| Table 72 | SNMP | 102 |
| Table 73 | TR069 | 103 |
| Table 74 | Diagnosis | 105 |
| Table 75 | Operating mode | 107 |
| Table 76 | System log | 108 |
| Table 77 | Logout | 108 |
| Chapter 4 | IPv6 address configuration | 109 |
| Table 78 | IPv6 Modes | 110 |
| Table 79 | Enabling IPv6 | 111 |
| Table 80 | Configuring Statefull IPv6 | 112 |
| Table 81 | Configuring Stateless IPv6 | 113 |

About This User Guide

Thank you for choosing FWR8101/FWR8102 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 introduces and describes on how to install and configure FWR8101/FWR8102 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 FWR8101/FWR8102 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. FWR8101/FWR8102 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

FlyingVoice Contact Details :

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

Cross references

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

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

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@flyingvoice.com.

Declaration of Conformity

Part 15 FCC Rules

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Class B Digital Device or Peripheral

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



Note

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Warnings and Notes

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

Warnings

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



Warning

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

Notes

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



Notes

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




Chapter 1 Product description

This chapter covers:

- [FWR8100/FWR8101/FW8102](#)
- [LED Indicators and Interfaces](#)
- [Hardware Installation](#)
- [Voice Prompt](#)

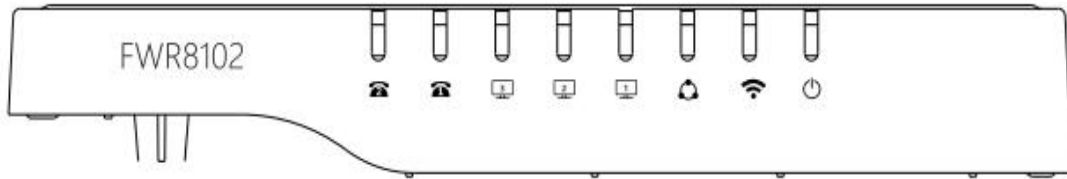
FWR8100/FWR8101/FWR8102

Table 1 Features at-a-glance

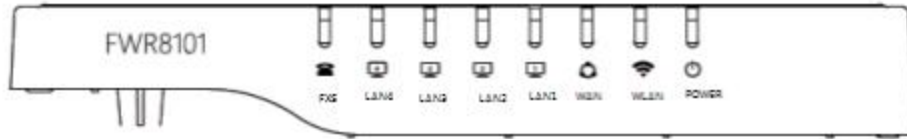
| Port/Model | FWR8100 | FWR8101 | FWR8102 |
|--------------------|---|--|---|
| picture |  |  |  |
| WAN | 1 | 1 | 1 |
| LAN | 4 | 4 | 3 |
| FXS | 0 | 1 | 2 |
| Ethernet interface | 5* RJ45 10/100M | 5* RJ45 10/100M | 4* RJ45 10/100M |
| Fax | × | T.30, T.38 Fax | |
| WiFi | 2.4G 2T2R (300Mbps) | 2.4G 2T2R(300Mbps) | 2.4G 2T2R (300Mbps) |
| Voice Code | G.711 (A-law, U-law), G.729A/B, G.723, G.722 (Wide band) | | |
| Management | Voice menu, Web Management, Provision:TFTP/HTTP/HTTPS, TR069, SNMP | | |
| VLAN | Support | | |

LED Indicators and Interfaces

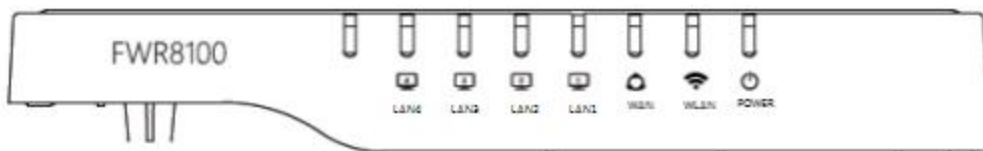
Table 2 LED Indicators



| LED | Status | Explanation |
|----------|----------------|---|
| Power | on Green | System is powered on |
| | off | System is powered off |
| WLAN | on Green | Wireless access point is ready. |
| | Blinking Green | AP is connected, and there is data transmitted |
| | off | AP wifi off or system is powered off |
| WAN | on Green | Network is connected (physical connection established), no data transmission |
| | Blinking Green | There is data being transmitted |
| | off | System is powered off or the network port is not connected to the network device. |
| LAN(1-3) | on Green | Network is connected (physical connection established), no data transmission |
| | Blinking Green | There is data being transmitted |
| | off | System is powered off or the network port is not connected to the network device. |
| FXS(1-2) | on Green | Registered successfully, but no data transfer |
| | Blinking Green | There is data being transmitted or fxs port is registering |
| | off | Power is off or registered failed |



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

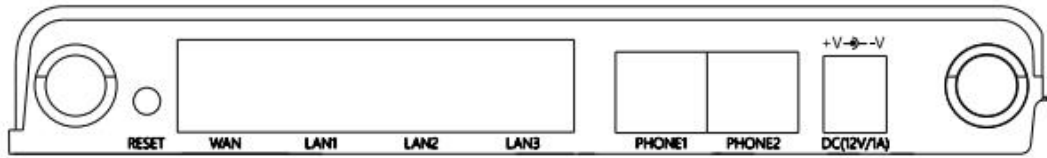


| LED | Status | Explanation |
|-------|----------------|---|
| Power | on Green | System is powered on |
| | off | System is powered off |
| WLAN | on Green | Wireless access point is ready. |
| | Blinking Green | AP is connected, and there is data transmitted |
| | off | AP wifi off or system is powered off |
| WAN | on Green | Network is connected (physical connection established), no data transmission |
| | Blinking Green | There is data being transmitted |
| | off | System is powered off or the network port is not connected to the network device. |

| | | |
|----------|----------------|---|
| LAN(1-4) | on Green | Network is connected (physical connection established), no data transmission |
| | Blinking Green | There is data being transmitted |
| | off | System is powered off or the network port is not connected to the network device. |

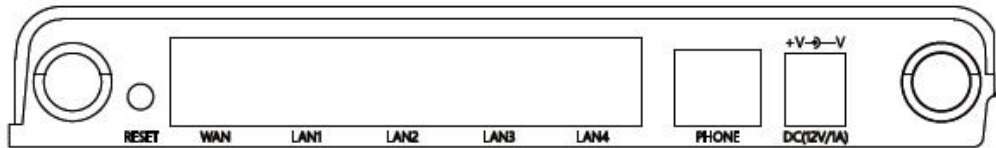
Table 3 Interfaces

FWR8102



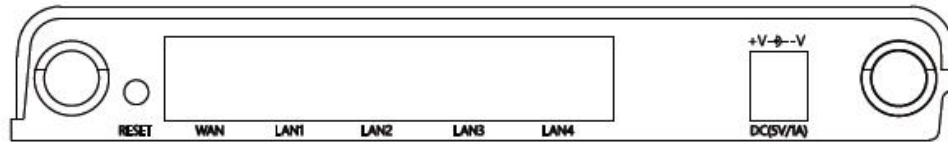
| Interface | Description |
|-----------|---|
| POWER | Connector for a power adapter |
| Phone1/2 | ATA Analog phone connector (RJ11 Interface) |
| WAN | Connector for accessing the Internet (RJ45 Interface) |
| LAN 1/2/3 | Connectors for local networked devices (RJ45 Interface) |
| RESET | Restore the factory settings button, press and hold the device for 5 sec. to restore the factory settings |

FWR8102



| Interface | Description |
|-------------|--|
| POWER | Connector for a power adapter |
| Phone | ATA Analog phone connector (RJ11 Interface) |
| WAN | Connector for accessing the Internet (RJ45 Interface) |
| LAN 1/2/3/4 | Connectors for local networked devices (RJ45 Interface) |
| RESET | Restore the factory settings button, press and hold the device for 5 sec to restore the factory settings |

FWR8100



| Interface | Description |
|-------------|--|
| POWER | Connector for a power adapter |
| WAN | Connector for accessing the Internet (RJ45 Interface) |
| LAN 1/2/3/4 | Connectors for local networked devices (RJ45 Interface) |
| RESET | Restore the factory settings button, press and hold the device for 5 sec to restore the factory settings |

Hardware Installation

Before beginning the configuration of router, please read 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 internet from modem/switch/router/ADSL to the WAN port of the equipment using an Ethernet cable.
3. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
4. Check the Power, WAN, and LAN LED to confirm network connectivity.



Warning

Please do not attempt to use unsupported power adapters and do not remove power during configuring or updating the device. Using other power adapters may damage the FWR8102 and will void the manufacturer warranty.



Warning

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

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

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

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

Interactive Voice Response Prompt

The devices may be configured by navigating the unit’s Interactive Voice Response (IVR) menu by using your analog phone and dialing a sequence of commands. Each device configuration section may be accessed by entering a certain operation code, as shown below.

Table 4 Interactive Voice Response Menu Setting Options

| Operation code | Menu Navigation |
|---------------------------------------|--|
| <p>1 WAN Port Connection Type</p> | <ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “1” , and The router reports the current WAN port connection type 3. When Prompted "Please enter password" , input password and press “#” key, to configuration WAN port connection type. The password in IVR is same as web management interface login, the user may use phone keypad to enter password directly For example: WEB login password is “admin” , so the password in IVR is “admin” . The user may “23646” to access and then configure the WAN connection port. The unit reports “Operation Successful” if the password is correct. 4. 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 …” 5. To quit, enter “*” |

| | |
|---------------------------------------|--|
| <p>2 WAN Port IP Address</p> | <ol style="list-style-type: none">1. Pick up phone and press “****” to start IVR2. Choose “2”, and The router reports current WAN Port IP Address3. Input the new WAN port IP address and press “#” key:4. Use “*” to replace “.”, for example : input 192*168*20*168 to set the new IP address 192.168.20.1685. Press # key to indicate that you have finished6. Router reports “operation successful” if user operation is ok.7. To quit, enter “**” . |
| <p>3 WAN Port Subnet Mask</p> | <ol style="list-style-type: none">1. Pick up phone and press “****” to start IVR2. Choose “3”, and router reports current WAN port subnet mask3. Input a new WAN port subnet mask and press # key:4. Use “*” to replace “.”, e.g. : enter 255*255*255*0 to set the new WAN port subnet mask 255.255.255.05. Press “#” key to indicate that you have finished6. Router reports “operation successful” if user operation is ok.7. To quit, enter “**” . |
| <p>4 Gateway</p> | <ol style="list-style-type: none">1. Pick up phone and press “****” to start IVR2. Choose “4”, and the router reports current gateway3. Input the new gateway and press “#” key:4. Use “*” to replace “.”, e.g. : input 192*168*20*1 to set the new gateway 192.168.20.1.5. Press “#” key to indicate that you have finished.6. Router reports “operation successful” if user operation is ok.7. To quit, press “**” . |

| | |
|-----------------------------|---|
| <p>5 DNS</p> | <ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “5” , and the router reports current DNS 3. Input the new DNS and press # key: 4. Use “*” to replace “.” , e.g. : input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press “#” key to indicate that you have finished. 6. Router reports “operation successful” if user operation is ok. 7. If you want to quit, press “**” . |
| <p>6 Factory Reset</p> | <ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “6” , and the router reports “Factory Reset” 3. Router Prompts "Please enter password", the method of inputting password is the same as operation 1. 4. If you want to quit, press “*” . 5. Router reports “operation successful” if password is right and then the router will be in factory default configuration. 6. Press “7” reboot to make changes effective. |
| <p>7 Reboot</p> | <ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “7”, and the router reports “Reboot” 3. Router Prompts "Please enter password", the method of inputting password is same as operation 1. 4. the router reboots if password is right . |
| <p>8 WAN Port Login</p> | <ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “8”, and the router reports “WAN Port Login” 3. Router Prompts "Please enter password", the method of inputting password is same as operation 1. 4. If user wants to quit, press “**” . |

| | |
|-----------------------------------|---|
| <p>9 WEB Access Port</p> | <ol style="list-style-type: none">1. Pick up phone and press “****” to start IVR2. Choose “9”, and the router reports “ WEB Access Port”3. Router Prompts “Please enter password”, the method of inputting password is same as operation 1.4. Router reports “operation successful” if user operation is ok.5. Router reports the current WEB Access Port6. Set the new WEB access port and press “#” key. |
| <p>0 Firmware Version</p> | <ol style="list-style-type: none">1. Pick up phone and press “****” to start IVR2. Choose “0” and the router reports the current Firmware version |



Note

1. While using Interactive Voice Response 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.

4. 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.
5. The default LAN port IP address of FWR8102 is 192.168.1.1 and this address should not be assigned to the WAN port IP address of FWR8102 in the same network segment of LAN port.
6. The password can be entered using phone keypad, the mapping table between number and letters as follows:

To Input: A, B, C, a, b, c – press '2'

To input: D, E, F, d, e, f -- press '3'

To input: G, H, I, g, h, i -- press '4'

To input: J, K, L, j, k, l -- press '5'

To input: M, N, O, m, n, o -- press '6'

To input: P, Q, R, S, p, q, r, s -- press '7'

To input: T, U, V, t, u, v -- press '8'

To input: W, X, Y, Z, w, x, y, z -- press '9'

To input all other characters in the administrator password-----press '0',

Chapter 2 Configuring Basic Settings

This chapter covers:

- [Two-Level Management](#)
- [Web Management Interface](#)
- [Configuring](#)
- [Making a Call](#)

Two-Level Management

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

FWR8102 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

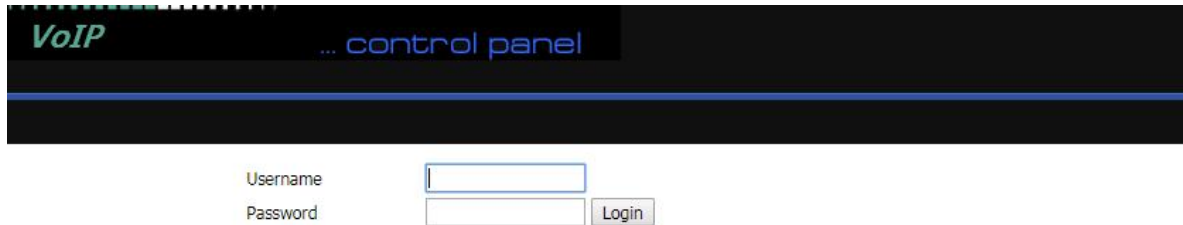
Ensure your PC is connected to the router’s LAN port correctly.



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 192.168.1.1. For detailed information, see Chapter 5 Troubleshooting Guide.

Open a web browser on your PC and type “http://192.168.1.1” . The following screen will appear that prompts for Username and Password.



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



Note

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

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

Logging in from the WAN port

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

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

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



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



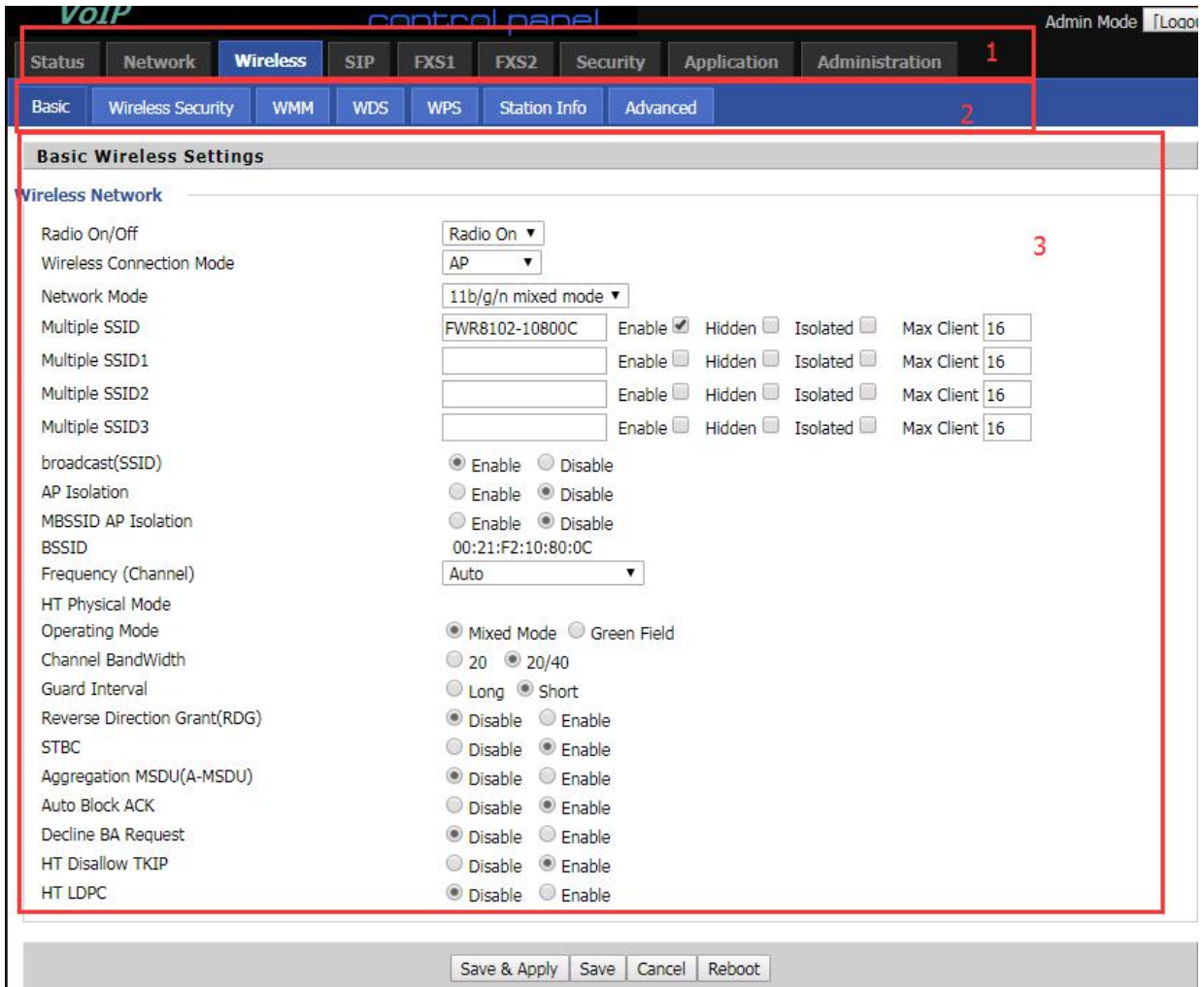
Note

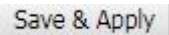
If you fail to access to the web configuration, see Chapter 6: Troubleshooting Guide for more information.




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

Web Management Interface Details

Table 5 Web management interface



| Field Name | Descripti |
|---|---|
| Top Navigation bar | Click an option in Top Navigation bar (area marked as “1”). Multiple options in the Sub-navigation bar are displayed |
| Sub-navigation bar | Click the Sub-navigation bar to choose a configuration page (area marked as “2”) |
| Parameter configuration | This area displays the current parameters for configuration (e.g. area marked as “3”) |
|  | After changing the parameters need to click this button to save&apply, modify the parameters immediately take effect. |

| | |
|---|--|
|  | 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 the device to ensure that the modification parameters take effect |
|  | To cancel the changes. |

Setting the Time Zone

Table 6 Setting time zone

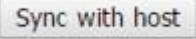
Time/Date Setting

NTP Settings

| | |
|----------------------------------|---|
| NTP Enable | Enable ▼ |
| Option 42 | Disable ▼ |
| Current Time | 2017 - 10 - 10 . 13 : 56 : 14 |
| Sync with host | <input type="button" value="Sync with host"/> |
| Time Zone | (GMT+08:00) China Coast, Hong Kong ▼ |
| Primary NTP Server | <input type="text" value="pool.ntp.org"/> |
| Secondary NTP Server | <input type="text" value="cn.pool.ntp.org"/> |
| NTP synchronization(1 - 1440min) | <input type="text" value="60"/> |

Daylight Saving Time

| | |
|----------------------|-----------|
| Daylight Saving Time | Disable ▼ |
|----------------------|-----------|

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

Configuring an Internet Connection

From the Network > WAN page, WAN connections can be configured. For more information on Internet Connection setting, see Table 10 below.

Table 7 Configuring an internet connection

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration | | |
|---------|-------------|---------------|----------|----------|------|--------------|-------------|----------------|------|-----|
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | DDNS | QoS |
| Advance | Eoip Tunnel | | | | | | | | | |

INTERNET

WAN

| | | |
|--|---|---|
| Connect Name | 1_MANAGEMENT_VOICE_INTERNET_R_VID ▾ | Delete Connect |
| Service | MANAGEMENT_VOICE_INTERNET ▾ | |
| IP Protocol Version | IPv4 ▾ | |
| WAN IP Mode | DHCP ▾ | |
| DHCP Server | <input type="text"/> | |
| MAC Address Clone | Disable ▾ | |
| NAT Enable | Enable ▾ | |
| VLAN Mode | Disable ▾ | |
| VLAN ID | 1 (1-4094) | |
| DNS Mode | Auto ▾ | |
| Primary DNS | <input type="text"/> | |
| Secondary DNS | <input type="text"/> | |
| DHCP | | |
| DHCP Renew | <input type="button" value="Renew"/> | |
| DHCP Vendor(Option 60) | FLYINGVOICE-FWR8102 | |
| Port Bind | | |
| <input checked="" type="checkbox"/> Port_1 | <input checked="" type="checkbox"/> Port_2 | <input checked="" type="checkbox"/> Port_3 |
| <input checked="" type="checkbox"/> Wireless(SSID) | <input checked="" type="checkbox"/> Wireless(SSID1) | <input checked="" type="checkbox"/> Wireless(SSID2) |
| | | <input checked="" type="checkbox"/> 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 |
|---------------------|---|
| Connect Name | Use keywords to indicate WAN port service model (the parameters are defined in Network--> multi-WAN page) |
| Service | Chose the service mode for the created connection |
| IP Protocol Version | IPv4 and IPv6 are supported |
| WAN IP Mode | Choose Internet connection mode, DHCP, PPPoE, or Bridge |
| NAT Enable | Enable or disable NAT |

VLAN ID

**Note**

Multiple WAN connections may be created with the same VLAN ID

DNS Mode

Select DNS mode, options are Auto and Manual:

When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.

When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS

Primary DNS

Enter the preferred DNS address

Secondary DNS

Enter the secondary DNS address

DHCP

(Displayed when WAN IP Mode is set to DHCP)

DHCP Renew

Refresh the DHCP IP

DHCP Vendor
(Option60)

Specify the DHCP Vendor field Display the vendor and product name

Setting up Wireless Connections

To set up the wireless connection follow the steps given below

Enable Wireless and Setting SSID

Open Wireless > Basic webpage as shown below:

Table 8 Wireless > Basic web page (user view)

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--------|-------------------|----------|-----|------|--------------|----------|-------------|----------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

Basic Wireless Settings

Wireless Network

| | | | | | |
|--------------------------|--------------------|---|---------------------------------|-----------------------------------|---------------|
| Radio On/Off | Radio On | | | | |
| Wireless Connection Mode | AP | | | | |
| Network Mode | 11b/g/n mixed mode | | | | |
| Multiple SSID | FWR8102-10800C | Enable <input checked="" type="checkbox"/> | Hidden <input type="checkbox"/> | Isolated <input type="checkbox"/> | Max Client 16 |
| Multiple SSID1 | | Enable <input type="checkbox"/> | Hidden <input type="checkbox"/> | Isolated <input type="checkbox"/> | Max Client 16 |
| Multiple SSID2 | | Enable <input type="checkbox"/> | Hidden <input type="checkbox"/> | Isolated <input type="checkbox"/> | Max Client 16 |
| Multiple SSID3 | | Enable <input type="checkbox"/> | Hidden <input type="checkbox"/> | Isolated <input type="checkbox"/> | Max Client 16 |
| broadcast(SSID) | | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | |
| AP Isolation | | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | |
| MBSSID AP Isolation | | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | |
| BSSID | 00:21:F2:10:80:0C | | | | |
| Frequency (Channel) | Auto | | | | |
| HT Physical Mode | | <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field | | | |
| Operating Mode | | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 | | | |
| Channel BandWidth | | | | | |

| Field Name | Description |
|-------------------|--|
| Radio On/Off | Select "Radio Off" to disable wireless operation Select "Radio on" to enable wireless operation Please note: "Save" required for this parameter change |
| Network Mode | Choose one network mode from the drop down list. |
| SSID | The logical name of the wireless connection (text, numbers or various special characters) |
| Multiple SSID 1-4 | Multiple SSID 1 - 4, configure up to 4 unique SSIDs |
| broadcast(SSID) | Enabled: The device SSID is broadcast at regular intervals Disabled: The device SSID is not broadcast at regular intervals, disallowing wi-fi clients from automatically connecting to the FWR8102 |

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

Encryption

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

Table 9 Wireless Security web page

The screenshot shows the 'WIFI Security Setting' page with the following fields:

- Select SSID:** SSID choice dropdown set to 'FWR8102-10800C'.
- Security Mode:** Dropdown set to 'WPA-PSK'.
- WPA Algorithms:** Radio buttons for TKIP, AES (selected), and TKIPAES.
- Pass Phrase:** Text input field with masked characters.
- Key Renewal Interval:** Text input field set to '3600' with unit 'sec' and range '(0 ~ 86400)'.
- Access policy:** Policy dropdown set to 'Disable'.
- Add a station MAC:** Text input field with a note '(The maximum rule count is 64)'.

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

Configuring Session Initiation Protocol (SIP)

SIP Accounts

FWR8102 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 via the Web Management Interface

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--|----------------------|-------------|-----|------------------------------------|-----------------------------------|----------|-------------|----------------|
| SIP Account | | Preferences | | | | | | |
| Basic | | | | | | | | |
| Basic Setup | | | | | | | | |
| Line Enable | Enable ▼ | | | Outgoing Call without Registration | Disable ▼ | | | |
| Proxy and Registration | | | | | | | | |
| Proxy Server | <input type="text"/> | | | Proxy Port | <input type="text" value="5060"/> | | | |
| Outbound Server | <input type="text"/> | | | Outbound Port | <input type="text" value="5060"/> | | | |
| Backup Outbound Server | <input type="text"/> | | | Backup Outbound Port | <input type="text" value="5060"/> | | | |
| Allow DHCP Option 120 to Override SIP Server | Disable ▼ | | | | | | | |
| Subscriber Information | | | | | | | | |
| Display Name | <input type="text"/> | | | Phone Number | <input type="text"/> | | | |
| Account | <input type="text"/> | | | Password | <input type="text"/> | | | |
| 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 | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|----------------------------|----------------------------|----------|-----|------|------|----------|-------------|----------------|
| Basic | LAN Host | Syslog | | | | | | |
| Product Information | | | | | | | | |
| Product Information | | | | | | | | |
| Product Name | FWR8102 | | | | | | | |
| Internet(WAN) MAC Address | 00:21:F2:10:80:0D | | | | | | | |
| PC(LAN) MAC Address | 00:21:F2:10:80:0C | | | | | | | |
| Hardware Version | V1.2 | | | | | | | |
| Loader Version | V3.37(May 9 2017 10:00:55) | | | | | | | |
| Firmware Version | V3.20(201705110531) | | | | | | | |
| Serial Number | 12345677856 | | | | | | | |
| SIP Account Status | | | | | | | | |
| SIP Account Status | | | | | | | | |
| FXS 1 SIP Account Status | Register Fail | | | | | | | |
| Primary Server | 0.0.0.0 | | | | | | | |
| Backup Server | 0.0.0.0 | | | | | | | |
| FXS 2 SIP Account Status | Disable | | | | | | | |
| Primary Server | 0.0.0.0 | | | | | | | |
| Backup Server | 0.0.0.0 | | | | | | | |

Procedure

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

Making a Call

Calling phone or extension numbers

To make a phone or extension number call:

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

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

Direct IP calls

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

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

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

Call Hold

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

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

Blind Transfer

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

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

A can hang up.

Attended Transfer

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

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

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

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

Conference

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

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

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

Chapter 3 Web Interface

This chapter guides users to for 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



| | |
|----------|---|
| Username | <input type="text" value="admin"/> |
| Password | <input type="password" value="....."/> <input type="button" value="Login"/> |

Procedure

1. Connect the LAN port of the router to your PC an Ethernet cable
 2. Open a web browser on your PC and type `http://192.168.1.1`.
 3. Enter Username admin and Password admin.
 4. Click Login
-

Status

Table 13 Status Page

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application |
|----------------------------|----------------------------|----------|-----|------|------|----------|-------------|
| Basic | LAN Host | Syslog | | | | | |
| Product Information | | | | | | | |
| Product Information | | | | | | | |
| Product Name | FWR8102 | | | | | | |
| Internet(WAN) MAC Address | 00:21:F2:10:80:0D | | | | | | |
| PC(LAN) MAC Address | 00:21:F2:10:80:0C | | | | | | |
| Hardware Version | V1.2 | | | | | | |
| Loader Version | V3.37(May 9 2017 10:00:55) | | | | | | |
| Firmware Version | V3.20(201705110531) | | | | | | |
| Serial Number | 123456777856 | | | | | | |
| SIP Account Status | | | | | | | |
| SIP Account Status | | | | | | | |
| FXS 1 SIP Account Status | Register Fail | | | | | | |
| Primary Server | 0.0.0.0 | | | | | | |
| Backup Server | 0.0.0.0 | | | | | | |
| FXS 2 SIP Account Status | Disable | | | | | | |
| Primary Server | 0.0.0.0 | | | | | | |
| Backup Server | 0.0.0.0 | | | | | | |
| FXS Port Status | | | | | | | |
| FXS Port Status | | | | | | | |
| FXS 1 Hook State | On | | | | | | |
| FXS 1 Port Status | Idle | | | | | | |
| FXS 2 Hook State | On | | | | | | |
| FXS 2 Port Status | Idle | | | | | | |

Network Status

Active WAN Interface

| | |
|-------------------------|---|
| Connection Type | DHCP |
| IP Address | 192.168.10.173 <input type="button" value="Renew"/> |
| Link-Local IPv6 Address | |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| Primary DNS | 192.168.10.1 |
| Secondary DNS | 192.168.18.1 |
| IPv6 PD Prefix | |
| IPv6 Domain Name | |
| IPv6 Primary DNS | |
| IPv6 Secondary DNS | |
| WAN Port Status | 100Mbps Full |

1 TR069_VOICE_INTERNET Vlan Status

| | |
|-----------------|-------------------|
| Connection Type | DHCP |
| MAC Address | 00:21:F2:10:80:0D |
| IP Address | 192.168.10.173 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| Primary DNS | 192.168.10.1 |
| Secondary DNS | 192.168.18.1 |

VPN Status

| | |
|--------------------|---------|
| VPN Type | Disable |
| Initial Service IP | |
| Virtual IP Address | |

LAN Port Status

| | |
|-------------|---------------|
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| LAN1 | Link Down |
| LAN2 | Link Down |
| LAN3 | Link Down |

Wireless Info

Wireless 2.4GHz

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

FWR8102-10800C

| | |
|------------------|-------------------|
| BSSID | 00:21:F2:10:80:0C |
| Number of Device | 0 |

System Status

System Status

| | |
|--------------|---------------------|
| Current Time | 2017-10-10 14:25:45 |
| Elapsed Time | 2 Hours, 39 Mins |

Refresh

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, MAC Clone, Port Forward and other parameters in this section of the web management interface.

WAN

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

Static IP

This configuration may be utilized when a user receives a fixed public IP address or a public subnet, namely multiple public IP addresses from the Internet providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you can assign an IP address to the WAN interface.

Table 14 Internet

| | |
|-----------------|----------------|
| Static | |
| IP Address | 192.168.10.173 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.10.1 |
| DNS Mode | Manual ▾ |
| Primary DNS | 192.168.10.1 |
| Secondary DNS | 192.168.18.1 |

| Field Name | 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: <ol style="list-style-type: none"> 1. When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user manually configures the preferred DNS and alternate DNS information |
| Primary DNS Address | The primary DNS of Internet port |
| Secondary DNS Address | The secondary DNS of Internet port |

DHCP

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

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

Table 15 DHCP

INTERNET

WAN

| | | |
|--|---|---|
| Connect Name | 1_MANAGEMENT_VOICE_INTERNET_R_VID ▾ | Delete Connect |
| Service | MANAGEMENT_VOICE_INTERNET ▾ | |
| IP Protocol Version | IPv4 ▾ | |
| WAN IP Mode | DHCP ▾ | |
| DHCP Server | <input type="text"/> | |
| MAC Address Clone | Disable ▾ | |
| NAT Enable | Enable ▾ | |
| VLAN Mode | Disable ▾ | |
| VLAN ID | 1 (1-4094) | |
| DNS Mode | Auto ▾ | |
| Primary DNS | <input type="text"/> | |
| Secondary DNS | <input type="text"/> | |
| DHCP | | |
| DHCP Renew | Renew | |
| DHCP Vendor(Option 60) | FLYINGVOICE-FWR8102 | |
| Port Bind | | |
| <input checked="" type="checkbox"/> Port_1 | <input checked="" type="checkbox"/> Port_2 | <input checked="" type="checkbox"/> Port_3 |
| <input checked="" type="checkbox"/> Wireless(SSID) | <input checked="" type="checkbox"/> Wireless(SSID1) | <input checked="" type="checkbox"/> Wireless(SSID2) |
| | | <input checked="" type="checkbox"/> Wireless(SSID3) |
| <small>Note : WAN connection can not be shared between the binding port , and finally bound port WAN connections bind operation will wash away before the other WAN connection to the port binding operation !</small> | | |

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

PPPoE

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

Table 16 PPPoE

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

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

| | |
|------------------|---------------------------------|
| Confirm Password | Enter your PPPoE password again |
|------------------|---------------------------------|

| | |
|--------------|---|
| Service Name | Enter a service name for PPPoE authentication. If it is left empty, the service name is auto detected. |
|--------------|---|

| | | | | | |
|----------------------------|--|----------------|--|----------------------------|--------------------------------|
| Operation Mode | Select the mode of operation, options are Keep Alive, On Demand and Manual: When the mode is Keep Alive, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; When the mode is On Demand, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; <table><tr><td>Operation Mode</td><td><input type="text" value="On Demand"/></td></tr><tr><td>On Demand Idle Time(0-60m)</td><td><input type="text" value="5"/></td></tr></table> | Operation Mode | <input type="text" value="On Demand"/> | On Demand Idle Time(0-60m) | <input type="text" value="5"/> |
| Operation Mode | <input type="text" value="On Demand"/> | | | | |
| On Demand Idle Time(0-60m) | <input type="text" value="5"/> | | | | |

| | |
|--------------------------|---|
| Keep Alive Redial Period | Set the interval to send Keep Alive messaging |
|--------------------------|---|

| | |
|---------------|--|
| PPPoE Account | Assign a valid user name provided by the ISP |
|---------------|--|

Bridge Mode

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

Table 17 Bridge Mode

INTERNET

WAN

Connect Name

Service

IP Protocol Version

WAN IP Mode

Bridge Type

DHCP Service Type

VLAN Mode

VLAN ID

1_MANAGEMENT_VOICE_INTERNET_R_VID ▼

MANAGEMENT_VOICE_INTERNET ▼

IPv4 ▼

Bridge ▼

IP Bridge ▼

Pass Through ▼

Disable ▼

1 (1-4094)

Delete Connect

Port Bind

Port_1 Port_2 Port_3

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

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

| Field Name | Description |
|--------------------------|---|
| Bridge Type | |
| IP Bridge | Allow all Ethernet packets to pass. PC can connect to upper network directly. |
| PPPoE Bridge | Only Allow PPPoE packets pass. PC needs PPPoE dial-up software. |
| Hardware IP Bridge | Packets pass through hardware switch with wired speed. Does not support wireless port binding |
| DHCP Service Type | |
| Pass Through | DHCP packets can be forwarded between WAN and LAN, DHCP server in gateway will not allocate IP to clients of LAN port. |
| DHCP Snooping | When gateway forwards DHCP packets form LAN to WAN it will add option82 to DHCP packet, and it will remove option82 when forwarding |

DHCP packet from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to clients of LAN port.

| | |
|---------------|---|
| Local Service | Gateway will not forward DHCP packets between LAN and WAN, it also blocks DHCP packets from the WAN port. Clients connected to the LAN port can get IP from DHCP server run in gateway. |
|---------------|---|

VLAN Mode

| | |
|---------|---|
| Disable | The WAN interface is untagged. LAN is untagged. |
|---------|---|

| | |
|--------|---|
| Enable | The WAN interface is tagged. LAN is untagged. |
|--------|---|

| | |
|-------|--|
| Trunk | Only valid in bridge mode. All ports, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN. |
|-------|--|

| | |
|---------|------------------|
| VLAN ID | Set the VLAN ID. |
|---------|------------------|



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

PC Port(LAN)

Local IP Address: 192.168.1.1

Local Subnet Mask: 255.255.255.0

Local DHCP Server: Enable

DHCP Start Address: 192.168.1.2

DHCP End Address: 192.168.1.254

DNS Mode: Auto

Primary DNS: 192.168.1.1

Secondary DNS: 192.168.10.1

Client Lease Time(0-86400s): 86400

DHCP Client List

| NO. | MAC | IP Address |
|---|-----|------------|
| <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> | | |

Add New Rule(MAX 15):

DNS Proxy: Enable

| Field Name | Description |
|-------------------|--|
| IP Address | Enter the IP address of the router on the local area network. All the IP addresses of the computers which are in the router’s LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (The default is 192.168.1.1). |
| Local Subnet Mask | Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24). |
| Local DHCP Server | 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 192.168.1.1, starting IP address can be 192.168.1.2 or greater, but should be less than the ending IP address. |
| DHCP End Address | Enter a valid IP address as an end IP address of the DHCP server. |
| DNS Mode | Select DNS mode, options are Auto and Manual: 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

| PC Port(LAN) | |
|--------------------|---|
| PC Port(LAN) | |
| Local IP Address | <input type="text" value="192.168.11.1"/> |
| Local Subnet Mask | <input type="text" value="255.255.255.0"/> |
| Local DHCP Server | <input type="text" value="Enable"/> |
| DHCP Start Address | <input type="text" value="192.168.11.2"/> |
| DHCP End Address | <input type="text" value="192.168.11.254"/> |
| DNS Mode | <input type="text" value="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 | <input type="text" value="192.168.11.1"/> |
| Secondary DNS | <input type="text" value="8.8.8.8"/> |
| Client Lease Time(0-86400s) | <input type="text" value="86400"/> |
| | <input type="button" value="DHCP Client List"/> |

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

VPN

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

Table 21 VPN

The screenshot shows the router's configuration interface. At the top, there are tabs for 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', and 'Administration'. Under the 'Network' tab, there are sub-tabs for 'WAN', 'LAN', 'IPv6 Advanced', 'IPv6 WAN', 'IPv6 LAN', 'VPN', 'Port Forward', 'DMZ', 'VLAN', and 'DDNS'. The 'VPN' sub-tab is selected. Below the sub-tabs, there are buttons for 'Advance' and 'Eoip Tunnel'. The main content area is titled 'VPN Settings' and has a sub-section for 'Administration'. In this section, there is a 'VPN Enable' dropdown menu that is currently open, showing the following options: 'Disable' (which is highlighted), 'PPTP', 'L2TP', and 'OpenVPN'. At the bottom of the page, there are buttons for 'Save', 'Cancel', and '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

Port Forwarding

| No. | Comment | IP Address | Port Range | Protocol |
|-----|---------|------------|------------|----------|
|-----|---------|------------|------------|----------|

Delete Selected Add Edit

Port Forwarding
 Comment
 IP Address
 Port Range -
 Protocol TCP&UDP ▼

(The maximum rule count is 32)

Apply Cancel

Virtual Servers

| No. | Comment | IP Address | Public Port | Private Port | Protocol |
|-----|---------|------------|-------------|--------------|----------|
|-----|---------|------------|-------------|--------------|----------|

Delete Selected Add Edit

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

(The maximum rule count 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

| VLAN Configuration | | | | |
|---------------------------------------|----------|----------|----------|----------|
| VLAN ID | Port | | | |
| | WAN | LAN1 | LAN2 | LAN3 |
| <input checked="" type="checkbox"/> 1 | UnTagged | UnSet | UnSet | UnSet |
| <input checked="" type="checkbox"/> 2 | UnSet | UnTagged | UnTagged | UnTagged |
| <input type="checkbox"/> | UnSet | UnSet | UnSet | UnSet |
| <input type="checkbox"/> | UnSet | UnSet | UnSet | UnSet |
| <input type="checkbox"/> | UnSet | UnSet | UnSet | UnSet |

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

DMZ

Table 24 DMZ

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

DDNS Setting

Table 25 DDNS setting

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

QoS

Table 26 QoS

| Name | Condition | | | | | | | | | Action | | | | | |
|------|----------------|----------------|----------|----------------|----------------|---------------|------|--------|---------|-------------|---------------|----------------|----------|------|------------|
| | Src.IP Address | Dst.IP Address | Protocol | Src.Port Range | Dst.Port Range | Physical Port | DSCP | 802.1p | VLAN ID | Remark DSCP | Remark 802.1p | Remark VLAN_ID | Priority | Drop | Rate Limit |

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

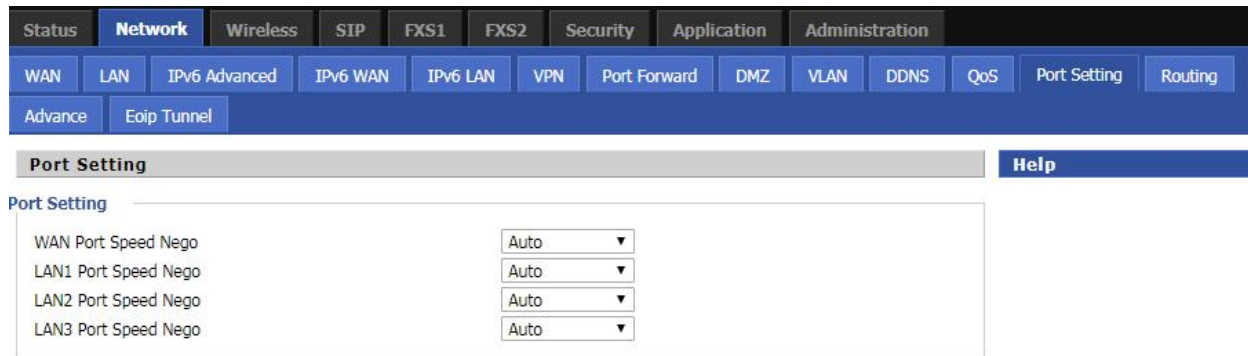


Note

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

Port Setting

Table 27 Port setting



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

Routing

Table 28 Routing

| | | | | | | | | | | | | |
|---------|----------------|---------------|----------|----------|------|--------------|-------------|----------------|------|-----|--------------|---------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration | | | | |
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | DDNS | QoS | Port Setting | Routing |
| Advance | Eoip Tunnel | | | | | | | | | | | |

Static Routing Settings

Add a routing rule

Destination:

Host/Net:

Gateway:

Interface:

Comment:

Help

You may add or remote Internet routing rules here.

Current Routing table in the system

| No. | Destination | Mask | Gateway | Flags | Metric | Interface | Comment |
|---|-------------|------|---------|-------|--------|-----------|---------|
| <input type="button" value="Delete Selected"/> <input type="button" value="Reset"/> | | | | | | | |

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

Advance

Table 29 Advance

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration | | |
|---------|-------------|---------------|----------|----------|------|--------------|-------------|----------------|------|-----|
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | DDNS | QoS |
| Advance | Voip Tunnel | | | | | | | | | |

| | |
|---|---|
| Most Nat connections(512-8192) | 4096 |
| Mss Mode | <input checked="" type="radio"/> Manual <input type="radio"/> Auto |
| Mss Value(1260-1460) | 1440 |
| AntiDos-P | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| IP conflict detection | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| IP Conflict Detecting Interval(0-3600s) | 600 |

| Field Name | Description |
|--------------------------------|--|
| Most Nat connections | The largest value which the FWR8102 can provide |
| Mss Mode | Choose Mss Mode from Manual and Auto |
| Mss Value | Set the value of TCP |
| AntiDos-p | You can choose to enable or prohibit |
| IP conflict detection | Select enable if enabled, phone IP conflict will have tips or prohibit |
| IP conflict Detecting Interval | Detect IP address conflicts of the time interval |

Eoip Tunnel

Table 30 Eoip Tunnel

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration | | |
|---------|-------------|---------------|----------|----------|------|--------------|-------------|----------------|------|-----|
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | DDNS | QoS |
| Advance | Eoip Tunnel | | | | | | | | | |

Eoip Tunnel

Eoip Tunnel

Eoip Tunnel 1 Enable Disable
 Remote IP Address

Eoip Tunnel 2 Enable Disable
 Remote IP Address

Eoip Tunnel 3 Enable Disable
 Remote IP Address

Eoip Tunnel 4 Enable Disable
 Remote IP Address

Eoip Tunnel 5 Enable Disable
 Remote IP Address

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

Wireless

Basic

Table 31 Basic

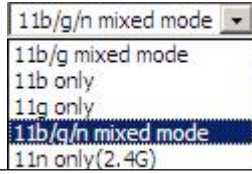
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--------|-------------------|----------|-----|------|--------------|----------|-------------|----------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

Basic Wireless Settings

Wireless Network

| | |
|------------------------------|--|
| Radio On/Off | Radio On ▼ |
| Wireless Connection Mode | AP ▼ |
| Network Mode | 11b/g/n mixed mode ▼ |
| Multiple SSID | FWR8102-10800C <input checked="" type="checkbox"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16 |
| Multiple SSID1 | <input type="text"/> <input type="checkbox"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16 |
| Multiple SSID2 | <input type="text"/> <input type="checkbox"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16 |
| Multiple SSID3 | <input type="text"/> <input type="checkbox"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16 |
| broadcast(SSID) | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| AP Isolation | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| MBSSID AP Isolation | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| BSSID | 00:21:F2:10:80:0C |
| Frequency (Channel) | Auto ▼ |
| HT Physical Mode | |
| Operating Mode | <input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field |
| Channel BandWidth | <input type="radio"/> 20 <input checked="" type="radio"/> 20/40 |
| Guard Interval | <input type="radio"/> Long <input checked="" type="radio"/> Short |
| Reverse Direction Grant(RDG) | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| STBC | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| Aggregation MSDU(A-MSDU) | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| Auto Block ACK | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| Decline BA Request | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| HT Disallow TKIP | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| HT LDPC | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |

| 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 |



| | |
|---------------------------------|---|
| SSID | It is the basic identity of wireless LAN. SSID can be any alphanumeric or a combination of special characters. It will appear in the wireless network access list. |
| Multiple SSID1~SSID3 | The device supports 4 SSIDs. |
| Hidden | After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list |
| Broadcast(SSID) | After initial State opening, the device broadcasts the SSID of the router to wireless network |
| AP Isolation | If AP isolation is enabled, the clients of the AP cannot access each other. |
| MBSSID AP Isolation | AP isolation among the devices which are not belong to this AP and along to, when the option is enabled, the devices which do not belong to this AP cannot access the devices which are within the AP |
| BSSID | A group of wireless stations and a WLAN access point (AP) consists of a basic access device (BSS), each computer in the BSS must be configured with the same BSSID, that is, the wireless AP logo |
| Frequency (Channel) | You can select Auto Select and channel 1/2/3/4/5/6/7/8/9/10/11. |
| HT Physical Mode Operating Mode | Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system |
| Channel Bandwidth | Select channel bandwidth, default is 20 MHz and 20/40 MHz. |
| Guard Interval | The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval |
| Reverse Dirction Grant (RDG) | Enabled: Devices on the WLAN are able to transmit to each other without requiring an additional contention-based request to transfer (i.e. devices are able to transmit to another device on the network during TXOP) Disabled: Devices on the WLAN must make a request for transmit when communicating with another device on the network |
| STBC | Space-time Block Code |

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

Wireless Security

Table 32 Wireless security

| | | | | | | | | |
|--------|--------------------------|-----------------|-----|------|--------------|----------|-------------|----------------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

WIFI Security Setting

Select SSID

SSID choice

"FWR8102-10800C"

Security Mode

WPA

WPA Algorithms TKIP AES TKIPAES

Pass Phrase

Key Renewal Interval sec (0 ~ 86400)

Access policy

Policy

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

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

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

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

Table 33 WiFi Security Setting

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--------|-------------------|----------|-----|------|--------------|----------|-------------|----------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

WiFi Security Setting

Select SSID

SSID choice: FWR8102-10800C ▼
 "FWR8102-10800C"
 Security Mode: OPENWEP ▼

Wire Equivalence Protection (WEP)
 Default Key: WEP Key 1 ▼

| | | | | |
|----------|-----------|-------|-------|---------|
| WEP Keys | WEP Key 1 | ***** | Hex ▼ | 64bit ▼ |
| | WEP Key 2 | ***** | Hex ▼ | 64bit ▼ |
| | WEP Key 3 | ***** | Hex ▼ | 64bit ▼ |
| | WEP Key 4 | ***** | Hex ▼ | 64bit ▼ |

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

Save & Apply Save Cancel Reboot

| 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 34 WPA-PSK

WIFI Security Setting

Select SSID

SSID choice FWR8102-10800C ▼

"FWR8102-10800C"

Security Mode WPA-PSK ▼

WPA

WPA Algorithms TKIP AES TKIPAES

Pass Phrase *****

Key Renewal Interval 3600 sec (0 ~ 86400)

Access policy

Policy Disable ▼

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

| Field Name | Description |
|----------------|--|
| WPA Algorithms | This item is used to select the encryption of wireless home gateway algorithms, options are TKIP, AES and TKIPAES. |
| Pass Phrase | Setting up WPA-PSK security password. |

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 35 WPAPSKWPA2PSK

WIFI Security Setting

Select SSID

SSID choice FWR8102-10800C ▼

"FWR8102-10800C"

Security Mode WPAPSKWPA2PSK ▼

WPA

WPA Algorithms TKIP AES TKIPAES

Pass Phrase *****

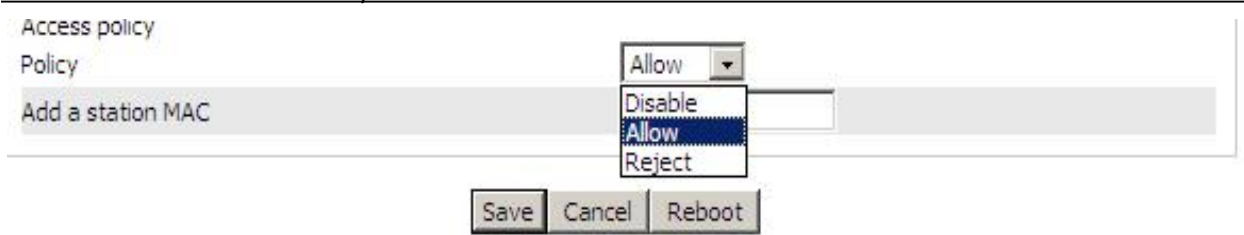
Key Renewal Interval 3600 sec (0 ~ 86400)

| 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 36 Wireless Access Policy



| Field Name | Description |
|-------------------|---|
| Access policy | Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address. |
| Policy | Disable : Prohibition: wireless access control policy. Allow: only allow the clients in the list to access. Rejected: block the clients in the list to access. |
| Add a station MAC | Enter the MAC address of the clients which you want to allow or prohibit |

Example: Prohibit the device whose wireless network card MAC address is 00:1F: D0: 62: BA:FF' s to access the wireless network, and allow other computers to access the network.Implementation: As shown, the Policy is Reject, add 00:1F: D0: 62: BA: FF to the MAC, click Save and reboot the device settings to take effect.

WMM

Table 37 WMM

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--|-------------------|----------|--------|------|--------------------------|--------------------------|-------------|----------------|
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |
| WMM Parameters of Access Point | | | | | | | | |
| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy | | |
| AC_BE | 3 | 15 ▼ | 63 ▼ | 0 | <input type="checkbox"/> | <input type="checkbox"/> | | |
| AC_BK | 7 | 15 ▼ | 1023 ▼ | 0 | <input type="checkbox"/> | <input type="checkbox"/> | | |
| AC_VI | 1 | 7 ▼ | 15 ▼ | 94 | <input type="checkbox"/> | <input type="checkbox"/> | | |
| AC_VO | 1 | 3 ▼ | 7 ▼ | 47 | <input type="checkbox"/> | <input type="checkbox"/> | | |
| <input type="button" value="Save & Apply"/> <input type="button" value="Apply"/> <input type="button" value="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 38 WDS

| | | | | | | | | |
|--------|-------------------|-----------------|------------|------|--------------|----------|-------------|---------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage |
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

| | |
|--------------------|-----------|
| WDS Setting | |
| WDS Config | |
| WDS Mode | Disable ▼ |
| Save Cancel Reboot | |

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 39 WPS

| | | | | | | | | |
|--------|-------------------|-----------------|-----|------------|--------------|----------|-------------|---------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage |
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

WPS Setting

WPS Config

WPS ▾

WPS Summary

| | |
|-----------------------|--|
| WPS Current Status | Idle |
| WPS Configured | Yes |
| WPS SSID | CAMBIUM_2.4GHz_027898 |
| WPS Auth Mode | WPA2-PSK |
| WPS Encryp Type | AES |
| WPS Default Key Index | 2 |
| WPS Key(ASCII) | 12345678 |
| AP PIN | 01619447 <input type="button" value="Generate"/> |

WPS Progress

WPS Mode PIN PBC

PIN

WPS Status

WSC:Idle

| Field Name | Description |
|-------------|--|
| WPS Setting | Enable/Disable WPS function |
| WPS Summary | Display the current status of WPS, including current state, SSSID name, authentication methods, encryption type and the PIN code of this AP. |
| Generate | Generate a new PIN code |
| Reset OOB | FWR8102 uses default security policy to allow other non- WPS users to access and apply. |

| | |
|------------|---|
| WPS Mode | <p>PIN: Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then router begins to send signals, turn on the PIN accessing method on the clients, and then it can access the wireless AP automatically.</p> <p>PBC: There are two ways to start 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.</p> |
| WPS Status | <p>WPS shows status in three ways:</p> <p>WSC: Idle</p> <p>WSC: Start WSC process (begin to send messages)</p> <p>WSC: Success; this means clients have accessed the AP successfully</p> |

Station Info

Table 40 Station info

The screenshot shows the router's web interface with the 'Wireless' tab selected. The 'Station Info' sub-tab is active. The 'Wireless Status' section shows 'Current Channel' as 'Channel 1' and 'CAMBIUM_2.4GHz_027898' as '00:04:56:02:78:98'. The 'Wireless Network' section displays a table of client statistics:

| MAC Address | Aid | PSM | MimoPS | MCS | BW | SGI | STBC |
|-------------------|-----|-----|--------|-----|-----|-----|------|
| 20:54:76:96:9B:1A | 1 | 0 | 3 | 7 | 20M | 0 | 1 |

Description

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

Advanced

Table 41 Advanced

| | | | | | | | | |
|--------|-------------------|-----------------|-----|------|--------------|-----------------|-------------|----------------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
| Basic | Wireless Security | WMM | WDS | WPS | Station Info | Advanced | | |

Advanced Wireless

Advanced Wireless

| | |
|-------------------------|---|
| BG Protection Mode | Auto ▾ |
| Beacon Interval | 100 ms (range 20 - 999, default 100) |
| Data Beacon Rate (DTIM) | 1 (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 | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Short Slot | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Tx Burst | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Pkt_Aggregate | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Country Code | US (United States) ▾ |
| Support Channel | Ch1~11 ▾ |
| Wi-Fi Multimedia | |
| WMM Capable | |
| Multiple SSID | <input checked="" type="checkbox"/> |
| Multiple SSID1 | <input type="checkbox"/> |
| Multiple SSID2 | <input type="checkbox"/> |
| Multiple SSID3 | <input type="checkbox"/> |
| APSD Capable | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| DLS Capable | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |

| Field Name | Description |
|------------------------|---|
| BG Protection Mode | Select BG protection mode, options are on, off and automatic. |
| Beacon Interval | The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network. |
| Data Beacon Rate(DTIM) | Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive broadcast multi-cast. |
| Fragment Threshold | Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet is divided. |

| | |
|--------------------------------|---|
| RTS Threshold | Specify the packet RTS threshold, when the packet exceeds this value, the router will send RTS to the destination site consultation |
| TX Power | Define the transmission power of the current AP, the greater it is, the stronger the signal is |
| Short Preamble | Choose enable or disable |
| Short Slot | Enable/Disable short slot. By default it is enabled, it is helpful in improving the transmission rate of wireless communication |
| Tx Burst | One of the features of MAC layer, it is used to improve the fairness for transmitting TCP |
| Pkt_Aggregate | It is a mechanism that is used to enhance the LAN, in order to ensure that the home gateway packets are sent to the destination correctly |
| Support Channel | Choose appropriate channel |
| Wi-Fi Multimedia (WMM) | |
| WMM Capable | Enable/Disable WMM. |
| APSD Capable | Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power |
| WMM Parameters | Press WMM Configuration , the webpage will jump to the configuration page of Wi-Fi multimedia |
| Multicast-to-Unicast Converter | Enable/Disable Multicast-to-Unicast. By default, it is Disabled |

SIP

SIP Settings

Table 42 SIP settings

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|---|-----------|----------|-------------------------|----------|------|----------|-------------|----------------|
| <div style="display: flex; justify-content: space-between;"> SIP Settings VoIP QoS Dial Rule Blacklist Call Log </div> | | | | | | | | |
| SIP Parameters | | | | | | | | |
| SIP Parameters | | | | | | | | |
| SIP T1 | 500 | ms | Max Forward | 70 | | | | |
| SIP User Agent Name | | | Max Auth | 2 | | | | |
| Reg Retry Intvl | 30 | sec | Reg Retry Long Intvl | 1200 | sec | | | |
| Mark All AVT Packets | Enable ▾ | | RFC 2543 Call Hold | Enable ▾ | | | | |
| S RTP | Disable ▾ | | S RTP Prefer Encryption | AES_CM ▾ | | | | |
| Service Type | Common ▾ | | DNS Refresh Timer | 0 | sec | | | |
| Response Status Code Handling | | | | | | | | |
| Retry Reg RSC | | | | | | | | |
| NAT Traversal | | | | | | | | |
| NAT Traversal | | | | | | | | |
| NAT Traversal | Disable ▾ | | STUN Server Address | | | | | |
| NAT Refresh Interval(sec) | 60 | | STUN Server Port | 3478 | | | | |
| <input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/> | | | | | | | | |

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

| | |
|------------------------|--|
| Mark All AVT Packets | Voice packet marking to enable this item will see the mark on the voice message when the call environment changed (such as press a key during the call) |
| RFC 2543 Call Hold | Enable the Connection Information field displays the address is 0.0.0.0 in the invite message of Hold. Disable the Connection Information field displays the device IP address in the invite message of Hold |
| SRTP | Whether to enable the call packet encryption function |
| SRTP Prefer Encryption | The preferred encryption type of calling packet (the Message body of INVITE Message) |
| Service Type | Choose the server type |
| NAT Traversal | Enable/Disable NAT Traversal FWR8102 supports STUN Traversal; if user wants to traverse NAT/Firewall, select the STUN |
| STUN Server Address | Add the correct STUN service provider IP address |
| NAT Refresh Interval | Set NAT Refresh Interval, default is 60s |
| STUN Server Port | Set STUN Server Port, default is 5060 |

VoIP QoS

Table 43 VoIP QoS

The screenshot displays the configuration page for VoIP QoS. At the top, there is a navigation bar with tabs for Status, Network, Wireless, SIP (selected), FXS1, FXS2, Security, Application, and Administration. Below this is a sub-menu for SIP settings, including SIP Settings, VoIP QoS (selected), Dial Rule, Blacklist, and Call Log. The main content area is titled 'QoS Settings' and shows 'Layer 3 QoS' configuration. Two input fields are present: 'SIP QoS(0-63)' and 'RTP QoS(0-63)', both with the value '46' entered. At the bottom of the configuration area are three buttons: 'Save', 'Cancel', and 'Reboot'.

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

SIP /RTP QoS The default value is 46, you can set a range of values is 0~63

Dial Plan

Parameters and Settings

Table 44 Parameters and settings

| Field Name | Description |
|------------|---|
| Dial Plan | Enable/Disable dial plan |
| Line | Set the line |
| Digit Map | Enter the sequence used to match input number The syntactic, please refer to the following Dial Plan Syntactic |
| Action | Choose the dial plan mode from Deny and Dial Out. Deny means router will reject the matched number, while Dial Out means router will dial out the matched number |
| Move Up | Move the dial plan up the list |
| Move Down | Move the dial plan down the list |

Adding one Dial Plan

Table 45 Adding one dial plan

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

Dial Plan Syntactic

Table 46 Dial Plan

| No. | String | Description |
|-----|-------------------------|---|
| 1 | 0 1 2 3 4 5 6 7 8 9 * # | Allowed characters |
| 2 | x | Lowercase letter “x” stands for one legal character |
| 3 | [sequence] | To match one character form sequence. For example: [0-9]: match one digit form 0 to 9 [23-5*]: match one character from 2 or 3 or 4 or 5 or * |
| 4 | x. | Match to x, xx, xxx, xxxx and so on. For example: “01” can be match to “0,”01,”011”...”011111...” and so on |
| 5 | <diald:substituted> | Replace diald with substituted. For example: <8:1650>123456: input is “85551212” , output is “16505551212” |
| 6 | x,y | Make outside dial tone after dialing “x” , stop until dialing character “y” For example: “9,1xxxxxxxxx” :the device reports dial tone after inputting “9” , stops tone until inputting “1” “9,8,010x” : make outside dial tone after inputting “9” , stop tone until inputting “0” |
| 7 | T | Set the delayed time. For example: “<9:111>T2” : The device will dial out the matched number “111” after 2 seconds. |

Blacklist

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

Table 47 Blacklist

Blacklist Upload && Download

Blacklist Upload && Download

Local File Choose File No file chosen

Upload CSV Download CSV

Blacklist

| Index | Name | Number | |
|-------|-------|--------|--------------------------|
| 1 | Rob | 12345 | <input type="checkbox"/> |
| 2 | Henry | 123456 | <input type="checkbox"/> |

Edit Add Delete Move to phonebook

Description

Click select files button to select the blacklist file and upload CSV to upload it to device; Click download CSV to save the blacklist file to your local computer.

Select one contact and click edit to change the information, click delete to delete the contact, click Move to phonebook to move the contact to phonebook.

Click Add to add one blacklist, enter the name and phone number, click OK to confirm and click cancel to cancel.

Name

Number

OK Cancel

Call Log

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

Table 48 Call log

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

Redial List

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

Answered Calls

Missed Calls

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

Missed Calls

FXS1

SIP Account

Basic

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

Table 49 SIP Account - Basic

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
|--|----------------------|-------------|-----|------------------------------------|-----------------------------------|----------|-------------|----------------|
| SIP Account | | Preferences | | | | | | |
| Basic | | | | | | | | |
| Basic Setup | | | | | | | | |
| Line Enable | Enable ▼ | | | Outgoing Call without Registration | Disable ▼ | | | |
| Proxy and Registration | | | | | | | | |
| Proxy Server | <input type="text"/> | | | Proxy Port | <input type="text" value="5060"/> | | | |
| Outbound Server | <input type="text"/> | | | Outbound Port | <input type="text" value="5060"/> | | | |
| Backup Outbound Server | <input type="text"/> | | | Backup Outbound Port | <input type="text" value="5060"/> | | | |
| Allow DHCP Option 120 to Override SIP Server | Disable ▼ | | | | | | | |
| Subscriber Information | | | | | | | | |
| Display Name | <input type="text"/> | | | Phone Number | <input type="text"/> | | | |
| Account | <input type="text"/> | | | Password | <input type="text"/> | | | |

| Field Name | Description |
|------------------------|--|
| Line Enable | Enable/Disable the line. |
| Peer To Peer | Enable/Disable PEER to PEER. If enabled, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dialed line1. |
| Proxy Server | The IP address or the domain of SIP Server |
| Outbound Server | The IP address or the domain of Outbound Server |
| Backup Outbound Server | The IP address or the domain of Backup Outbound Server |
| Proxy port | SIP Service port, default is 5060 |

| | |
|----------------------|--|
| Outbound Port | Outbound Proxy' s Service port, default is 5060 |
| Backup Outbound Port | Backup Outbound Proxy' s Service port, default is 5060 |
| Display Name | The number will be displayed on LCD |
| Phone Number | Enter telephone number provided by SIP Proxy |
| Account | Enter SIP account provided by SIP Proxy |
| Password | Enter SIP password provided by SIP Proxy |

Audio Configuration

Table 50 Audio configuration

| Audio Configuration | | | |
|--------------------------|-----------|------------------------|------------|
| Codec Setup | | | |
| Audio Codec Type 1 | G.711U ▼ | Audio Codec Type 2 | G.711A ▼ |
| Audio Codec Type 3 | G.729 ▼ | Audio Codec Type 4 | G.722 ▼ |
| Audio Codec Type 5 | G.723 ▼ | G.723 Coding Speed | 5.3k bps ▼ |
| Packet Cycle(ms) | 20ms ▼ | Silence Supp | Disable ▼ |
| Echo Cancel | Enable ▼ | Auto Gain Control | Disable ▼ |
| FAX Configuration | | | |
| FAX Mode | T.38 ▼ | ByPass Attribute Value | fax ▼ |
| T.38 CNG Detect Enable | Disable ▼ | T.38 CED Detect Enable | Enable ▼ |
| gpmid attribute Enable | Disable ▼ | T.38 Redundancy | Disable ▼ |

| | |
|-------------------|--|
| Audio Codec Type1 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type2 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type3 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type4 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |
| Audio Codec Type5 | Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723 |

| | |
|------------------------|---|
| G.723 Coding Speed | Choose the speed of G.723 from 5.3kbps and 6.3kbps |
| Packet Cycle | The RTP packet cycle time, default is 20ms |
| Silence Supp | Enable/Disable silence support |
| Echo Cancel | Enable/Disable echo cancel. By default, it is enabled |
| Auto Gain Control | Enable/Disable auto gain |
| T.38 Enable | Enable/Disable T.38 |
| T.38 Redundancy | Enable/Disable T.38 Redundancy |
| T.38 CNG Detect Enable | Enable/Disable T.38 CNG Detect |
| gpm� attribute Enable | Enable/Disable gpm� attribute. |

Supplementary Service Subscription

Table 51 Supplementary service

Supplementary Service Subscription

Supplementary Services

| | | | |
|----------------------|--------------------------------------|-----------------------|-------------------------------------|
| Call Waiting | <input type="text" value="Enable"/> | Hot Line | <input type="text"/> |
| MWI Enable | <input type="text" value="Enable"/> | Voice Mailbox Numbers | <input type="text"/> |
| MWI Subscribe Enable | <input type="text" value="Disable"/> | VMWI Serv | <input type="text" value="Enable"/> |
| DND | <input type="text" value="Disable"/> | | |

Speed Dial

| | | | |
|--------------|----------------------|--------------|----------------------|
| Speed Dial 2 | <input type="text"/> | Speed Dial 3 | <input type="text"/> |
| Speed Dial 4 | <input type="text"/> | Speed Dial 5 | <input type="text"/> |
| Speed Dial 6 | <input type="text"/> | Speed Dial 7 | <input type="text"/> |
| Speed Dial 8 | <input type="text"/> | Speed Dial 9 | <input type="text"/> |

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

| | |
|-----------------------|---|
| Voice Mailbox Numbers | Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice mail is *97 |
| VMWI Serv | Enable/Disable VMWI service |
| DND | Enable/Disable DND (do not disturb) If enable, any phone call cannot arrive at the device; default is disable |
| Speed Dial | Enter the speed dial phone numbers. Dial *74 to active speed dial function. Then press the speed dial numbers, for example, press 2, phone dials 075526099365 directly |

Advanced

Table 52 Advanced

Advanced

Advanced Setup

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

| Field Name | Description |
|-----------------------------|--|
| Domain Name Type | Enable/Disable domain name in the SIP URI. |
| Carry Port Information | Enable/Disable 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 enabled, 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 enabled, 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 | Enable/Disable OB Proxy In Dialog. |
| Reg Subscribe Enable | If enabled, subscribing will be sent after registration message, if Disabled, do not send subscription. |

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

Preferences

Volume Settings

Table 53 Volume settings

| Field Name | Description |
|--------------------|---|
| Handset Input Gain | Adjust the handset input gain from 0 to 7 |
| Handset Volume | Adjust the output gain from 0 to 7 |

Preferences

Volume Settings

Handset Input Gain Handset Volume

Regional

Table 54 Regional

Regional

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

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

Features and Call Forward

Table 55 Features and call forward

Features

| | | | |
|-------------------|--------------------------------------|--------------|--------------------------------------|
| All Forward | <input type="text" value="Disable"/> | Busy Forward | <input type="text" value="Disable"/> |
| No Answer Forward | <input type="text" value="Disable"/> | | |

Call Forward

| | | | |
|-------------------|----------------------|-------------------|---------------------------------|
| All Forward | <input type="text"/> | Busy Forward | <input type="text"/> |
| No Answer Forward | <input type="text"/> | No Answer Timeout | <input type="text" value="20"/> |

Feature Code

| | | | |
|-----------------------|--------------------------------------|---------------------|-----------------------------------|
| Hold Key Code | <input type="text" value="*77"/> | Conference Key Code | <input type="text" value="*88"/> |
| Transfer Key Code | <input type="text" value="*98"/> | IVR Key Code | <input type="text" value="****"/> |
| R Key Enable | <input type="text" value="Disable"/> | R Key Cancel Code | <input type="text" value="R1"/> |
| R Key Hold Code | <input type="text" value="R2"/> | R Key Transfer Code | <input type="text" value="R4"/> |
| R Key Conference Code | <input type="text" value="R3"/> | Speed Dial Code | <input type="text" value="*74"/> |

| Field Name | Description | |
|--------------|---------------------|--|
| Features | All Forward | Enable/Disable forward all calls |
| | Busy Forward | Enable/Disable busy forward. |
| | No Answer Forward | Enable/Disable no answer forward. |
| Call Forward | All Forward | Set the target phone number for all forward. The device will forward all calls to the phone number immediately when there is an incoming call. |
| | Busy Forward | The phone number on which the calls will be forwarded when line is busy. |
| | No Answer Forward | The phone number on which the call will be forwarded when there's no answer. |
| | No Answer Timeout | The seconds to delay before forwarding calls, if there is no answer at your phone. |
| Feature Code | Hold key code | Call hold signatures, default is *77. |
| | Conference key code | Signature of the tripartite session, default is *88. |

| | |
|-----------------------|---|
| Transfer key code | Call forwarding signatures, default is *78. |
| IVR key code | Signatures of the Interactive Voice Response 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 56 Miscellaneous

Miscellaneous

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

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

FXS2

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

Security

Filtering Setting

Table 57 Filtering setting

| Basic Settings | |
|---|---|
| Basic Settings | |
| Filtering | Disable ▾ |
| Default Policy | Drop ▾ |
| The packet that don't match with any rules would be Drop | |
| <input type="button" value="Save"/> <input type="button" value="Cancel"/> | |
| IP/Port Filter Settings | |
| Interface | LAN ▾ |
| Mac address | <input type="text"/> |
| Dest IP Address | <input type="text"/> |
| Source IP Address | <input type="text"/> |
| Protocol | NONE ▾ |
| Dest. Port Range | <input type="text"/> - <input type="text"/> |
| Src Port Range | <input type="text"/> - <input type="text"/> |
| Action | Accept ▾ |
| Comment | <input type="text"/> |
| (The maximum rule count is 32) | |
| <input type="button" value="Save"/> <input type="button" value="Cancel"/> | |

| 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 58 Content filtering

| | | | | | | | | |
|-------------------|---------|-------------------|-----|------|------|-----------------|-------------|---------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage |
| Filtering Setting | | Content Filtering | | | | | | |

Basic Settings

Basic Settings

Filtering Disable ▼

Default Policy Accept ▼

Webs URL Filter Settings

Current Webs URL Filters

| No. | URL |
|-----|-----|
| | |

Add a URL Filter

URL

Webs Host Filter Settings

Current Website Host Filters

| No. | Keyword |
|-----|---------|
| | |

Add a Host(keyword) Filter

Keyword

| 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

Table59 advance NAT

Description

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

UPnP

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

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

Table 60 UPnP

| Field Name | Description |
|-------------|-------------------------------|
| UPnP enable | Enable/Disable UPnP function. |

IGMP

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

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

Table 61 IGMP

| | | | | | | | | |
|----------------------|---------|-------------|-----|------|------|----------|--------------------|----------------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration |
| Advance Nat | UPnP | IGMP | | | | | | |
| IGMP | | | | | | | | |
| IGMP Setting | | | | | | | | |
| IGMP Proxy enable | | Enable ▾ | | | | | | |
| IGMP Snooping enable | | Enable ▾ | | | | | | |
| Save & Apply | | | | Save | | Cancel | | Reboot |

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

Administration

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

Management

Save config file

Table 62 Save Config File

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

Administrator settings

Table 63 Administrator settings

| Administrator Settings | |
|--------------------------------|---|
| Password Reset | |
| User Type | Admin User ▼ |
| New User Name | admin |
| New Password | <input type="text"/> (The maximum length is 25) |
| Confirm Password | <input type="text"/> |
| Language | |
| Language | English ▼ |
| VPN Access | |
| Management Using VPN | Disable ▼ |
| Web Access | |
| Remote Web Login | Enable ▼ |
| Local Web Port | 80 |
| Web Port | 80 |
| Web SSL Port | 443 |
| Web Idle Timeout(0 - 60min) | 5 |
| Allowed Remote IP(IP1;IP2;...) | 0.0.0.0 |
| Telnet Access | |
| Remote Telnet | Enable ▼ |
| Telnet Port | 23 |
| Allowed Remote IP(IP1;IP2;...) | 0.0.0.0 |
| HostName | FWR8102 |

| Field Name | Description |
|------------------|---|
| User type | Choose the user type from admin user and normal user and basic user |
| New User Name | You can modify the user name, set up a new user name |
| New Password | Input the new password |
| Confirm Password | Input the new password again |
| Language | Select the language for the web, the device support Chinese, English, and Spanish and so on |
| Remote Web Login | Enable/Disable remote Web login |
| Web Port | Set the port value which is used to login from Internet port and PC port, default is 80 |

| | |
|--------------------------------|--|
| Web Idle timeout | Set the Web Idle timeout time. The webpage can be logged out after Web Idle Timeout without any operation. |
| Allowed Remote IP(IP1,IP2,...) | Set the IP from which a user can login the device remotely. |
| Telnet Port | Set the port value which is used to telnet to the device. |

NTP settings

Table 64 NTP settings

Time/Date Setting

NTP Settings

NTP Enable Enable ▼

Option 42 Disable ▼

Current Time 2016 - 01 - 19 . 05 : 55 : 06

Sync with host Sync with host

NTP Settings (GMT-06:00) Central Time ▼

Primary NTP Server pool.ntp.org

Secondary NTP Server

NTP synchronization(1 - 1440min) 60

Daylight Saving Time

Daylight Saving Time Disable ▼

| Field Name | Description |
|----------------------|--|
| NTP Enable | Enable/Disable NTP |
| Option 42 | Enable/Disable DHCP option 42. This option specifies a list of the NTP servers available to the client by IP address |
| Current Time | Display current time |
| NTP Settings | Setting the Time Zone |
| Primary NTP Server | Primary NTP server's IP address or domain name |
| Secondary NTP Server | Options for NTP server's IP address or domain name |
| NTP synchronization | NTP synchronization cycle, cycle time can be 1 to 1440 minutes in any one, the default setting is 60 minutes |

Daylight Saving Time

Table 65 Daylight Saving Time

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

Procedure

Step 1. Enable Daylight Savings Time.

Step 2. Set value of offset for Daylight Savings Time

Step 3: Set starting Month/Week/Day/Hour in Start Month/Start Day of Week Last in Month/Start Day of Week/Start Hour of Day, analogously set stopping Month/Week/Day/Hour in Stop Month/Stop Day of Week Last in Month/Stop Day of Week/Stop Hour of Day.

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

System Log Setting

Table 66 System log Setting

| System Log Setting | |
|---------------------------------|----------------------|
| Syslog Setting | |
| Syslog Enable | Enable ▼ |
| Syslog Level | INFO ▼ |
| Login Syslog Enable | Enable ▼ |
| Call Syslog Enable | Enable ▼ |
| Net Syslog Enable | Enable ▼ |
| Device Management Syslog Enable | Enable ▼ |
| Device Alarm Syslog Enable | Enable ▼ |
| Kernel Syslog Enable | Enable ▼ |
| Remote Syslog Enable | Disable ▼ |
| Remote Syslog Server | <input type="text"/> |

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

Factory Defaults Setting

Table 67 Factory Defaults Setting

| Factory Defaults Setting | |
|---------------------------------|-----------|
| Factory Defaults Setting | |
| Factory Defaults Lock | Disable ▼ |

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

Factory Defaults

Table 68 Factory Defaults

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

Firmware Upgrade

Table 69 Firmware upgrade

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage |
|---|------------------|---------------|-----------|------|-------|--------------------|-------------|---------|
| Management | Firmware Upgrade | Certification | Provision | SNMP | TR069 | Cambium Network Ma | | |
| Operating Mode | | | | | | | | |
| Firmware Management | | | | | | | | |
| Firmware Upgrade | | | | | | | | |
| Upgrade Types <input type="button" value="Upgrade Software"/> ▾ | | | | | | | | |
| Local Upgrade <input type="button" value="Choose File"/> No file chosen | | | | | | | | |
| <input type="button" value="Upgrade"/> | | | | | | | | |
| Description | | | | | | | | |
| <ol style="list-style-type: none">1. Choose upgrade file type from Image File and Dial Rule2. Press “Browse..” button to browser file3. Press <input type="button" value="Upgrade"/> to start upgrading | | | | | | | | |

Provision

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

- Before testing or using TFTP, user should have tftp server and upgrading file and configuring file.
- Before testing or using HTTP, user should have http server and upgrading file and configuring file.
- Before testing or using HTTPS, user should have https server and upgrading file and configuring file and CA Certificate file (should same as https server’s) and Client Certificate file and Private key file

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

Table 70 Provision

| | | | | | | | | |
|----------------|------------------|---------------|-----------|------|-------|--------------------|-------------|---------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage |
| Management | Firmware Upgrade | Certification | Provision | SNMP | TR069 | Cambium Network Ma | | |
| Operating Mode | | | | | | | | |

Provision

Configuration Profile

| | |
|-------------------------------|-----------|
| Provision Enable | Enable ▾ |
| Resync On Reset | Enable ▾ |
| Resync Random Delay(sec) | 40 |
| Resync Periodic(sec) | 3600 |
| Resync Error Retry Delay(sec) | 3600 |
| Forced Resync Delay(sec) | 14400 |
| Resync After Upgrade | Enable ▾ |
| Resync From SIP | Disable ▾ |
| Option 66 | Enable ▾ |
| Config File Name | \$(MA) |
| User Agent | |
| Profile Rule | |

| Field Name | Description |
|------------------|------------------------------------|
| Provision Enable | Enable provision or not. |
| Resync on Reset | Enable resync after restart or not |

| | |
|-------------------------------|--|
| Resync Random Delay(sec) | Set the maximum delay for the request of synchronization file. The default is 40. |
| Resync Periodic(sec) | If the last resync was failure, The router will retry resync after the “Resync Error Retry Delay ” time, default is 3600s. |
| Resync Error Retry 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 71 Firmware Upgrade

Firmware Upgrade

Upgrade Enable Enable ▾

Upgrade Error Retry Delay(sec) 3600

Upgrade Rule

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

SNMP

Table 72 SNMP



SNMP Configuration

SNMP Configuration

| | |
|---------------------------|----------------------|
| SNMP Service | Enable ▾ |
| Trap Server Address | <input type="text"/> |
| Read Community Name | public |
| Write Community Name | private |
| Trap Community | trap |
| Trap period interval(sec) | 300 |

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

TR-069

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

Device Configuration using TR-069

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

Table 73 TR069

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

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

| | |
|--------------------------|---|
| Periodic Inform Interval | Periodic notification interval with the unit in seconds. The default value is 3600s |
|--------------------------|---|

Connect Request parameters

| | |
|-----------|--|
| User Name | The username used to connect the TR069 server to the DUT |
|-----------|--|

| | |
|----------|--|
| Password | The password used to connect the TR069 server to the DUT |
|----------|--|

Diagnosis

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

Table 74 Diagnosis

| | | | | | | | | | |
|----------------|------------------|-----------------|--------------|-----------|------|----------|-------------|-----------|-----------------------|
| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Storage | Administration |
| Management | Firmware Upgrade | Scheduled Tasks | Certificates | Provision | SNMP | TR069 | cnMaestro | Diagnosis | |
| Operating Mode | | | | | | | | | |

Packet Trace

Help

Packet Trace

Tracking Interface WAN ▼

Packet Trace

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface 1_MANAGEMENT_VOICE_INTERNET_R_VID_ ▼

...

Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface 1_MANAGEMENT_VOICE_INTERNET_R_VID_ ▼

...

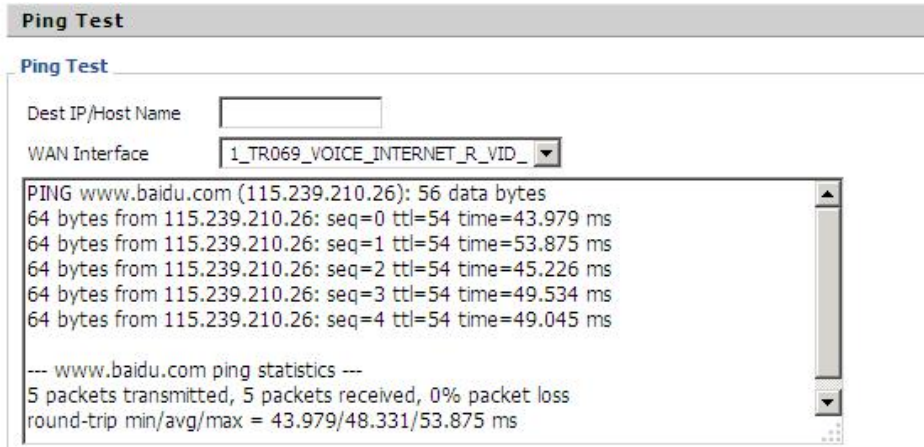
Description

1. Packet Trace

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

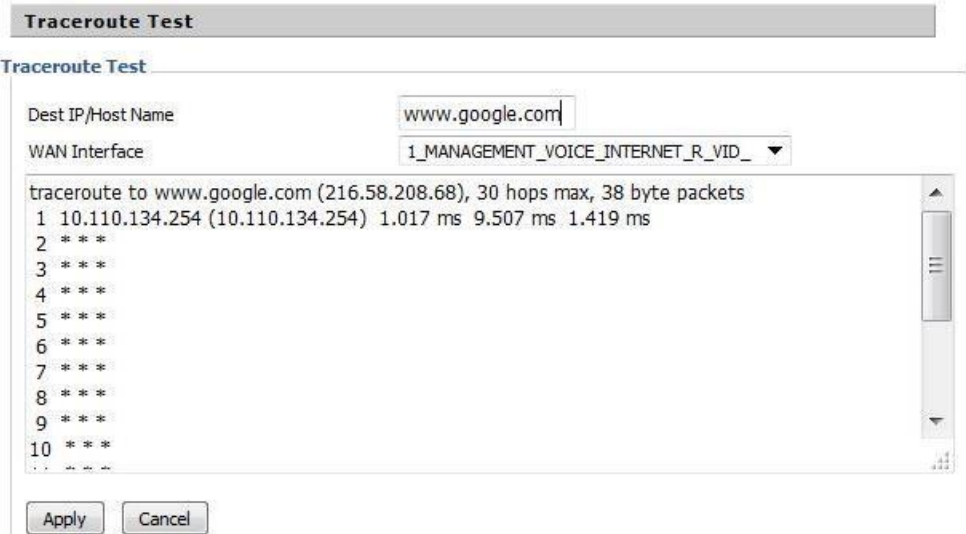
2. Ping Test

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



3. Traceroute Test

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



Operating Mode

Table 75 Operating mode

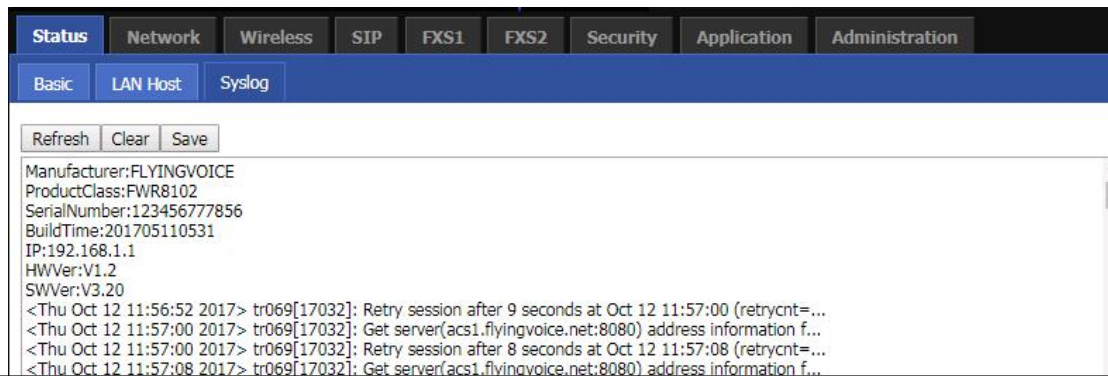
| Operating Mode Settings | | |
|-------------------------|---------------|--------|
| Operating Mode Settings | | |
| Operating Mode | Basic Mode | |
| | Basic Mode | |
| | Advanced Mode | |
| Save | Cancel | Reboot |

Description

Choose the Operation Mode as Basic Mode or Advanced Mode.

System Log

Table 76 System log

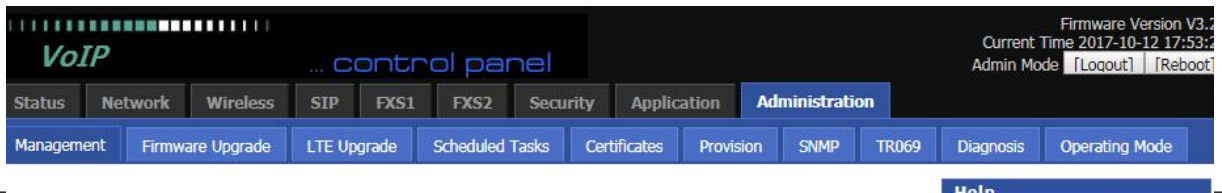


Description

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

Logout

Table 77 Logout



Description

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

Reboot

Press the  button to reboot the device.

Chapter 4 IPv6 address configuration

The router devices support IPv6 addressing. This chapter covers:

- [Introduction](#)
- [IPv6 Advance](#)
- [Configuring IPv6](#)
- [Viewing WAN port status](#)
- [IPv6 DHCP configuration for LAN/WLAN clients](#)
- [LAN DHCPv6](#)

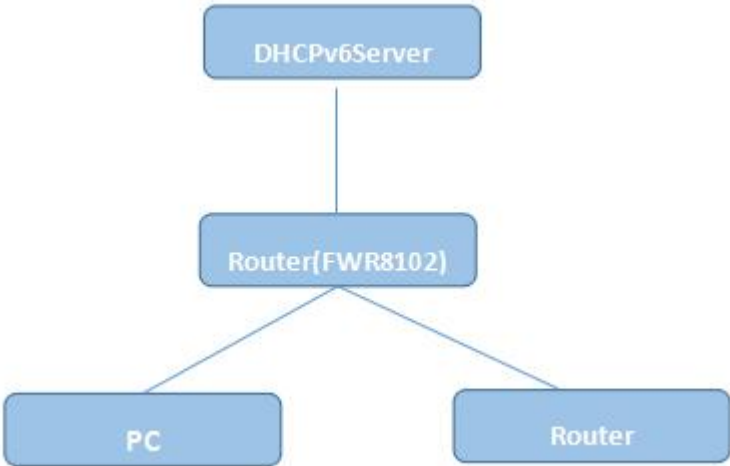
Introduction

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

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

- Stateless DHCPv6
- Statefull DHCPv6

Table 78 IPv6 Modes

| Mode | Description |
|---|--|
| Stateless | In Stateless DHCPv6 mode, the Routers devices listen for ICMPv6 Router Advertisements messages which are periodically sent out by the routers on the local link or requested by the node using a Router Advertisements solicitation message. The device derives a unique IPv6 address using prefix receives from the router and its own MAC address. |
|  <pre>graph TD; Server[DHCPv6Server] --- Router1[Router{FWR8102}]; Router1 --- PC[PC]; Router1 --- Router2[Router];</pre> | |
| Statefull | In Statefull DHCPv6 mode, the client works exactly as IPv4 DHCP, in which hosts receive both their IPv6 addresses and additional parameters from the DHCP server. |

IPv6 Advance

To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

Table 79 Enabling IPv6

The screenshot displays the 'IPv6 Advanced Settings' configuration page. The navigation menu at the top includes 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', and 'Administration'. Under the 'Network' section, 'WAN', 'LAN', 'IPv6 Advanced', 'IPv6 WAN', 'IPv6 LAN', 'VPN', 'Port Forward', 'DMZ', 'VLAN', 'DDNS', 'QoS', 'Port Setting', and 'Routing' are visible. The 'IPv6 Advanced' sub-section includes 'Advance' and 'Eoip Tunnel'. The main content area is titled 'IPv6 Advanced Settings' and features a 'Help' button. The 'IPv6 Enable' section shows a dropdown menu currently set to 'Enable'. At the bottom of the page, there are four buttons: 'Save & Apply', 'Save', 'Cancel', and 'Reboot'.

Configuring IPv6

Configuring Statefull IPv6

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

Table 80 Configuring Statefull IPv6

The screenshot shows the configuration page for IPv6 WAN settings. The navigation menu at the top includes Status, Network (selected), Wireless, SIP, FXS1, FXS2, Security, Application, and Administration. Under the Network menu, there are sub-menus for WAN, LAN, IPv6 Advanced, IPv6 WAN (selected), IPv6 LAN, VPN, Port Forward, DMZ, VLAN, DDNS, and QoS. Below the navigation, there are buttons for 'Advance' and 'Eoip Tunnel'. The main heading is 'IPv6 WAN Setting'. The configuration area contains three dropdown menus: 'Connection Type' is set to 'DHCPv6', 'DHCPv6 Address Settings' is set to 'Statefull', and 'Prefix Delegation' is set to 'Enable'. At the bottom of the configuration area, there are three buttons: 'Save', 'Cancel', and 'Reboot'.

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

Configuring Stateless IPv6

Table 81 Configuring Stateless IPv6

The screenshot displays the configuration interface for IPv6 WAN settings. The navigation bar includes 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', and 'Administration'. Under 'Network', there are sub-menus for 'WAN', 'LAN', 'IPv6 Advanced', 'IPv6 WAN', 'IPv6 LAN', 'VPN', 'Port Forward', 'DMZ', 'VLAN', 'DDNS', and 'QoS'. The 'IPv6 WAN Setting' section is highlighted, showing the following configuration options:

- Connection Type: DHCPv6
- DHCPv6 Address Settings: Stateless
- Prefix Delegation: Enable

At the bottom of the configuration area, there are three buttons: 'Save', 'Cancel', and 'Reboot'.

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

Viewing WAN port status

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

Network Status

Active WAN Interface

| | |
|-------------------------|---|
| Connection Type | DHCP |
| IP Address | 192.168.10.174 <input type="button" value="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 | |
| WAN Port Status | 100Mbps Full |

IPv6 DHCP configuration for LAN/WLAN clients

Wired and wireless clients connected to the Routers can obtain their IPv6 addresses based on how the LAN s 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:

| Status | Network | Wireless | SIP | FXS1 | FXS2 | Security | Application | Administration | | | |
|---------|-------------|---------------|----------|----------|------|--------------|-------------|----------------|------|-----|------|
| WAN | LAN | IPv6 Advanced | IPv6 WAN | IPv6 LAN | VPN | Port Forward | DMZ | VLAN | DDNS | QoS | Port |
| Advance | Eoip Tunnel | | | | | | | | | | |

| IPv6 LAN Setting | | Help |
|-------------------------|--|--------------|
| IPv6 LAN Setting | | |
| IPv6 Address | <input type="text" value="fec0::1"/> | |
| IPv6 Prefix Length | <input type="text" value="64"/> | (0-128) |
| DHCPv6 Server | | |
| DHCPv6 Status | <input type="text" value="Disable"/> | |
| DHCPv6 Mode | <input type="text" value="Stateless"/> | |
| Domain Name | <input type="text"/> | |
| Server Preference | <input type="text" value="255"/> | (0-255) |
| Primary DNS Server | <input type="text"/> | |
| Secondary DNS Server | <input type="text"/> | |
| Lease Time | <input type="text" value="86400"/> | (0-86400sec) |
| IPv6 Address Pool | <input type="text"/> - <input type="text"/> / <input type="text"/> | |
| Router Advertisement | <input type="text" value="Disable"/> | |
| Router Advertisement | <input type="text" value="30"/> | |
| Advertise Interval | (10-1800sec) | |
| RA Managed Flag | <input type="text" value="Disable"/> | |
| RA Other Flag | <input type="text" value="Enable"/> | |
| Prefix | <input type="text"/> / <input type="text"/> | |
| Prefix Lifetime | <input type="text" value="3600"/> | (0-3600sec) |

| | | | |
|---|-------------------------------------|---------------------------------------|---------------------------------------|
| <input type="button" value="Save & Apply"/> | <input type="button" value="Save"/> | <input type="button" value="Cancel"/> | <input type="button" value="Reboot"/> |
|---|-------------------------------------|---------------------------------------|---------------------------------------|

Chapter 5 Troubleshooting Guide

This chapter covers:

- [Configuring PC to get IP Address automatically](#)
- [Cannot connect to the Web GUI](#)
- [Forgotten Password](#)

Configuring PC to get IP Address automatically

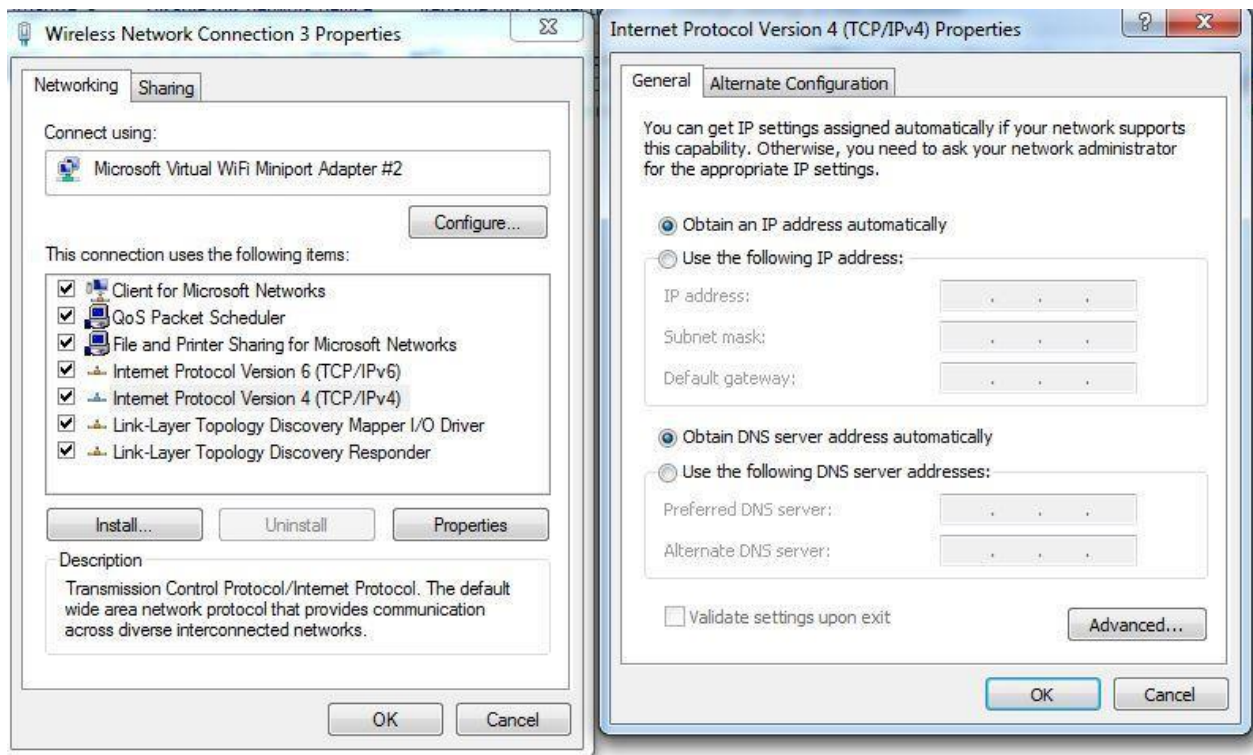
Follow the below process to set your PC to get an IP address automatically:

Step 1 : Click the “Start” button

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

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

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



Cannot connect to the Web

Solution:

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

Forgotten Password

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

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