



USER MANUAL

FPX9102H

Content

About This User Guide.....	1
Purpose.....	3
Cross references.....	3
Feedback.....	3
Declaration of Conformity.....	4
CE certification.....	4
Part 15 FCC Rules.....	4
Class B Digital Device or Peripheral.....	4
Operational safety requirements.....	5
Warnings and Notes.....	6
Warnings.....	6
Notes.....	6
Chapter 1 Product description.....	7
FPX9102H.....	8
LED Indicators and Interfaces.....	9
LED Indicators.....	9
Interfaces.....	10
Hardware Installation.....	11
Installation preparation.....	11
Installation steps.....	11
Chapter 2 Basic configuration.....	13
Login web page.....	13
Web Management Interface.....	14
About Password.....	15
Network Configuration.....	16
Configuring an Internet Connection.....	16
Wireless Configuration.....	17
FXO Ports.....	18
Chapter 3 Web Interface.....	20
Web Interface Structural.....	21
Web interface.....	21
Status page.....	22
Basic.....	23
LAN host.....	24
Syslog.....	24
Network page.....	24
WAN.....	25
LAN.....	28
IPv6 Advance.....	30
IPv6 WAN.....	30
IPv6 LAN.....	31
VPN.....	32

Port Forward.....	35
DMZ.....	36
QOS.....	37
Rate Limit.....	38
Port Setting.....	38
Routing.....	39
Advance.....	40
IPPBX.....	41
Basic.....	41
Wireless 2.4G.....	43
Basic.....	43
Wireless Security.....	46
Wireless 5G.....	55
Security.....	57
Filtering Setting.....	57
Content Filtering.....	58
Application.....	60
Advance NAT.....	60
UPnP.....	60
Storage.....	62
Disk Management.....	62
FTP Setting.....	63
Administration.....	64
Management.....	64
Firmware Upgrade.....	68
Scheduled Tasks.....	68
Provision.....	69
SNMP.....	72
TR-069.....	73
Diagnosis.....	74
Operating Mode.....	77
Chapter 4 Troubleshooting Guide.....	78
Configuring PC to get IP Address automatically.....	78
Cannot connect to the Web.....	79
Forgotten Password.....	79

About This User Guide

Thank you for choosing FPX9102H wireless router with VoIP. This product will allow you to make ATA call using your broadband connection, and provides Wi-Fi router function. This manual provides basic information on how to install and connect FPX9102H 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 FPX9102H 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. FPX9102H 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](#) Troubleshooting Guide

Contacting FlyingVoice

Main website: <http://www.flyingvoice.com/>

Sales enquire: sales1@flyingvoice.com

Support enquire: support@flyingvoice.com

Hotline: 010-67886296 0755-26099365

Address: Room508-509, Bldg#1, Dianshi Business Park, No.49 BadachuRd,Shijingshan
District, Beijing, China

Purpose

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

Cross references

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

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

Feedback

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

Declaration of Conformity

CE certification

This device complies with the EU Directive 2014/35 / EU and the EMC Directive 2014/30 / EU.

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.

Operational safety requirements



Warning

- Unloaded power outlets or damaged wires and plugs may cause electric shock or fire. Check the relevant power cable regularly. If its appearance has been damaged, replace it immediately.
 - Please use the power adapter provided for you. Using other power adapters can damage the device or prevent the device from working properly.
 - This product should be installed in a place with ventilation and no high temperature and no sunlight, in order to avoid overheating and failure of the product and related accessories.
 - Communication equipment should be protected against moisture and moisture and prevent water ingress. Influent water will cause the equipment to work abnormally and it is more likely to cause other hazards due to short circuit.
 - Do not place this product on an unstable support.
-

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:

- FPX9102H
- LED Indicators and Interfaces
- Hardware Installation

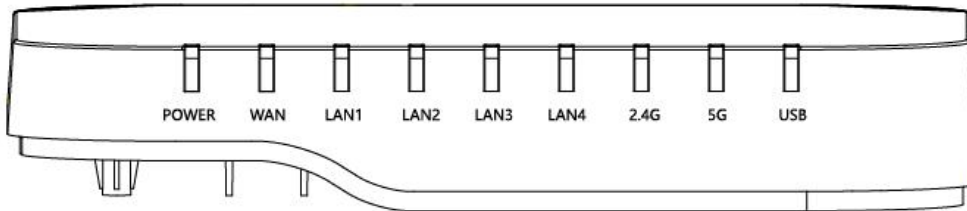
FPX9102H

Port/Model	FPX9102H
Picture	
WAN port	1
LAN port	4
FXO port	2
Ethernet interface	5* RJ45 10/100/1000M
USB interface	Yes
Speed limit NAT	Yes
FAX	T.30, T.38 Fax
WiFi	2.4G 2T2R (300Mbps),5G 2T2R (867Mbps)
Voice code	G.711 (A-law/U-law), G.729A/B, G.723,G.726
Management	Voice menu, Web Management, Provision:TFTP/HTTP/HTTPS, TR069, SNMP
Vlan	support

LED Indicators and Interfaces

LED Indicators

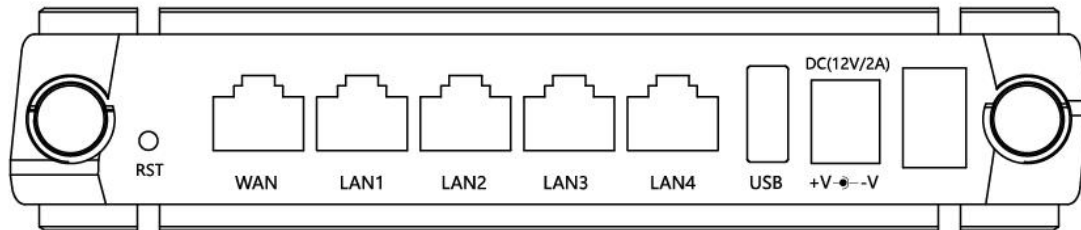
FPX9102H



LED	Status	Description
PHONE1/2	Blinking(Green)	There is transmitting data or registering
	On(Green)	Register successfully but no transmitting data
	Off	Register failure or don't register
5G	Blinking(Green)	There is transmitting data
	On(Green)	5G is work
	Off	There is no 5G
2.4G	On(Green)	2.4G is work
	Blinking(Green)	There is transmitting data
	Off	There is no 2.4G
LAN 1/2/3/4	On (Green)	The port is connected but no transmitting data
	Off	The port is disconnected.
	Blinking(Green)	It will blink while transmitting data.
WAN	Blinking(Green)	The port is connected
	Off	The port is disconnected.
	Blinking(Green)	It will blink while transmitting data.

Interfaces

FPX9102H



Interface	Description
POWER	Connector for a power adapter
PHONE1/2	Connector for a analog phone
LAN(1/2/3/4)	Connectors for local networked devices
WAN	Connector for accessing the Internet
RST	Factory reset,press 5s to restore the factory settings

Hardware Installation

Installation preparation

Before installing the equipment, check whether the items are complete and the installation conditions are met. Open the packing box of the equipment and check the contents of the box against the item list. If you find that the contents of the box do not match the list, please contact us directly. The device can be placed on a table or on a wall.



Notes

- The installation site must have the equipment and external connection conditions (such as: power cord, network cable, PC, etc.). The AC power outlet should use a single-phase three-core power socket, and ensure that the ground wire is reliably grounded.
 - The environment of the installation site must ensure adequate air flow to facilitate the heat dissipation of the equipment (appropriate operating temperature of the equipment is -10°C to 45°C).
 - The installation site should be waterproof, moisture-proof, lightning-proof and other conditions (appropriate environmental humidity of the equipment is 10% to 95%).
-

Installation steps

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

Upstream Ethernet connection

- Use RJ-11 cable to connect the phone port to the fixed phone jack;
- Connect the device's port to the modem using an Ethernet cable;
- Connect the lan port of your computer and device through RJ-45 cable;
- One end of the power cord is connected to the power connector of the device, and the other end is connected to a power outlet;

- Start the router
- Check the power, wan, and lan LEDs to ensure network connectivity.

**Warning**

Do not attempt to use an unsupported power adapter, and do not unplug the power supply while configuring or changing the device. Using other power adapters may damage the device and will void the manufacturer's warranty.

Chapter 2 Basic configuration

This chapter covers:

- [Login web page](#)
- [Network Configuration](#)
- [Wireless Configuration](#)
- [FXO port](#)

Login web page

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

(1) For administrator mode operation, please type “ admin/admin ” on Username/Password and click Login button to begin configuration, This level can configure all parameters of the operating device.

(2) For user mode operation, please type “ user/user ” on Username/Password and click Login button to begin configuration. Users at this level can browse and configure some of the phone parameters, some parameters in the SIP line that cannot be changed, such as server addresses and ports, which cannot be configured by users at this level.

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.

Open a web browser on your PC and type “ http://192.168.1.1:8080 ” . The following window appears that prompts for Username and Password.



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 and port of WAN>. The following login page will be opened to enter username and password.



The image shows a login interface for a VoIP control panel. At the top, there is a status bar with a signal strength indicator and the text "VoIP" and "... control panel". Below this, there are two input fields: "Username" with the text "admin" and "Password" with five dots. A "Login" button is positioned to the right of the password field.

About Password

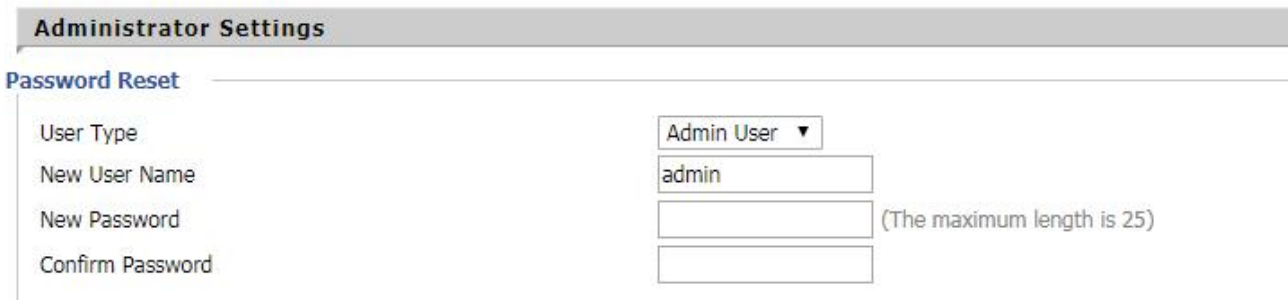
There are two types of login levels for the device: administrator level and normal user level. Different standards have different passwords.

The default administrator level login password is admin/admin

The default normal user level login password is user/user

1.Change Password

Log into the device WEB page, switch to the Manage - Manage page, find the "Reset Password" tab, select the user type, then set a new user name and password, click "Save".



The image shows a screenshot of the "Administrator Settings" page, specifically the "Password Reset" section. It contains a form with the following fields: "User Type" (a dropdown menu set to "Admin User"), "New User Name" (a text box containing "admin"), "New Password" (a text box), and "Confirm Password" (a text box). A note next to the password fields states "(The maximum length is 25)".

2.Forgot password

If the user changes the ATA page login password but forgets it, the user cannot enter the ATA configuration interface. At this time, press and hold the restore factory button for more than 5 seconds to restore the device to the factory settings and log in using the default password.

Note

If the following prompt appears:



After restoring factory default settings or uploading configuration files, click on REBOOT to ensure they are activated!

Please **reboot** the device to ensure that the changes take effect.

Network Configuration

Configuring an Internet Connection

From the Network > WAN page, WAN connections may be inserted or deleted. For more information on setting, Please refer to the following table.

The screenshot shows the WAN configuration page with the following settings:

- WAN IP Mode: DHCP
- DHCP Server: [Empty text box]
- MAC Address Clone: Disable
- LAN Connection Mode: NAT
- DNS Mode: Auto
- Primary DNS: [Empty text box]
- Secondary DNS: [Empty text box]

Field Name	Description
WAN IP Mode	You can choose which mode to use DHCP: router can get IP from DHCP server STATIC: you need setting IP manually PPPoE: need username and password for your Internet service provider
DHCP server	DHCP server IP
MAC Address Clone	If enable "MAC Address Clone" feature
LAN Connection Mode	Choose LAN port connection mode:NAT,bridge
DNS Mode	Choose DNS mode:Auto,Manual 1. When the DNS mode is Auto, the device under the LAN port will automatically obtain Primary DNS and Secondary DNS 2. When the DNS mode is Manual, the user should manually configure Primary DNS and Secondary DNS
Primary DNS	Preferred DNS for internet ports
Secondary DNS	Secondary DNS for Internet ports

Wireless Configuration

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

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administration
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

Basic Wireless Settings

Wireless Network

Radio On/Off	Radio On	1
Wireless Connection Mode	AP	2
Network Mode	11n only(2.4G)	4
Multiple SSID1	91020D6CD0	3
Multiple SSID2		
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:F2:0D:6C:D0	
FLYINGVOICE WIPO	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Frequency (Channel)	Auto	

1. Radio On/Off: please choose On,enable wireless network.
2. Wireless Connection Mode:default is AP.
3. Multiple SSID1:you can set the SSID(network name) of your wireless network here.
4. And please don't forgot "Enable" this SSID,or you will can't find the wireless

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

WIFI Security Setting

Select SSID

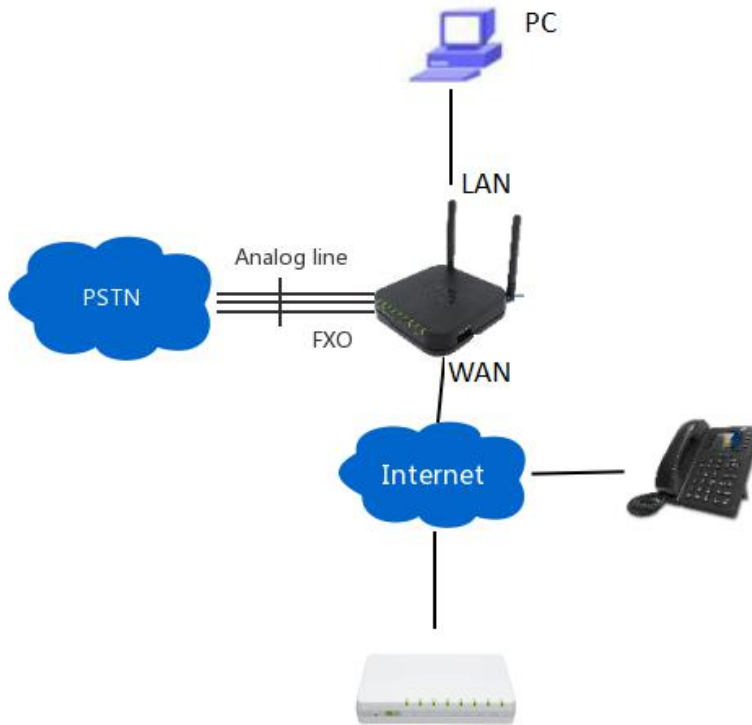
SSID choice	91020D6CD0	5
"91020D6CD0"		
Security Mode	WPA-PSK	6
WPA		
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES	7
Pass Phrase	*****	
Key Renewal Interval	3600 sec (0 ~ 86400)	
Access policy		
Policy	Disable	
Add a station MAC		(The maximum rule count is 64)

5. Need to choose which SSID you want to encrypt.
6. Choose encrypt mode.
7. Set the SSID's password,you need use this password to connect the SSID.
8. When you finished setting,must save and reboot router.
9. Wireless 5G setting:Please refer to the wireless 2.4G.

FXO Ports

To use the FXO ports, please perform the following steps:

1. Please connect FPX9102H like this picture:



2. There is simple PBX feature on FPX9102H,so you can use it to make some extension numbers in your office. There are 10 numbers by default, you can just use them, sip server ip is FPX9102H's WAN ip.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic		Users					

Register Manager					
No.	Extension	PassWord	Full Name	Client MAC	
1 <input type="checkbox"/>	600	password600	600		
2 <input type="checkbox"/>	601	password601	601		
3 <input type="checkbox"/>	602	password602	602		
4 <input type="checkbox"/>	603	password603	603		
5 <input type="checkbox"/>	604	password604	604		
6 <input type="checkbox"/>	605	password605	605		
7 <input type="checkbox"/>	606	password606	606		
8 <input type="checkbox"/>	607	password607	607		
9 <input type="checkbox"/>	608	password608	608		
10 <input type="checkbox"/>	609	password609	609		

3. Or you can add other numbers,add steps:

Delete Selected **Add** Edit

Add or Edit a User:

Extension

PassWord

Full Name

Client MAC

Apply

Cancel

Extension:extension number

Password:extension number's registertion password.

Full Name:display name

Client MAC:if you want this number bind one phone,you can input the phone's MAC address in here.

Then click "Apply" and reboot FPX9102H.

After reboot,you can use the number you add normally.

And you can check these extension numbers status in FPX9102H's web page(status page)

Chapter 3 Web Interface

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

- Web Interface Structural

- Status page

- Network page

- IPPBX

- Wireless 2.4G

- Wireless 5G

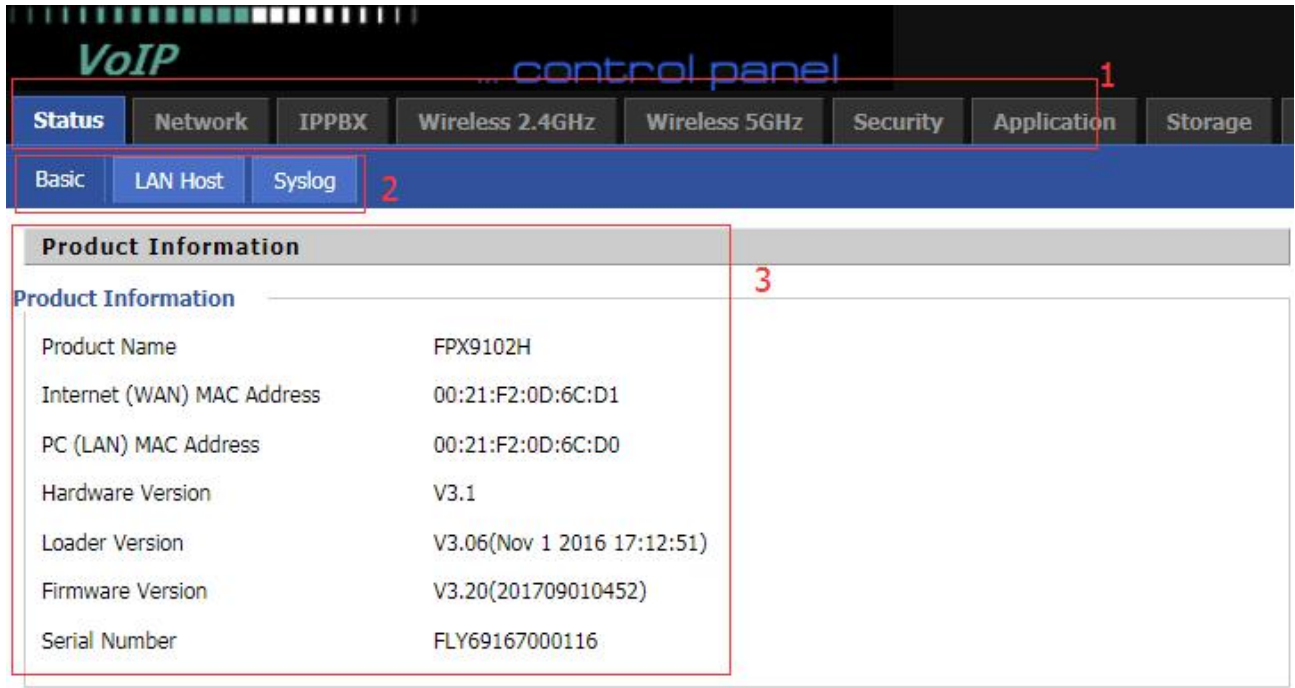
- Security

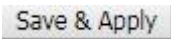

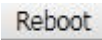
- Application

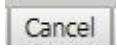
- Administration

Web Interface Structural

Web interface



Field Name	Descript
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.

Status page

Basic

The web page displays some current information about the device, including version information, network status, and wireless status.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	LAN Host	Syslog					

Product Information

Product Information

Product Name	FPX9102H
Internet(WAN) MAC Address	00:21:F2:0D:6C:D1
PC(LAN) MAC Address	00:21:F2:0D:6C:D0
Hardware Version	V3.1
Loader Version	V3.06(Nov 1 2016 17:12:51)
Firmware Version	V3.11(201611182233)
Serial Number	FLY69167000116

Line Status

Line Status

SIP Trunk 1	
SIP Trunk 2	
SIP Trunk 3	
SIP Trunk 4	
SIP Trunk 5	
SIP Trunk 6	
SIP Trunk 7	
SIP Trunk 8	
Exten1	600,Unavailable
Exten2	601,Unavailable
...	...

LAN host

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administration
Basic	LAN Host	Syslog						
LAN Host Info								
MAC Address	IP Address	Interface Type	Address Source	Expires	Host Name	Status		
IPv6 LAN Host Info								
MAC Address	IPv6 Address	Expires						
Description								

Here you can see some information about the host connected to the device LAN port

Syslog

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administr
Basic	LAN Host	Syslog						
<div style="display: flex; justify-content: space-between; margin-bottom: 5px;"> Refresh Clear Save </div> <pre> Manufacturer:FLYINGVOICE ProductClass:FPX9102H SerialNumber:FLY69167000116 BuildTime:201709010452 IP:192.168.1.1:8080 HWVer:V3.1 SWVer:V3.20 <Wed Apr 18 14:06:51 2018> kernel: Wireless: Send AUTH response (SUCCESS)... <Wed Apr 18 14:06:51 2018> kernel: Wireless: Rcv ASSOC From 00:21:f2:36:4f:27 <Wed Apr 18 14:06:51 2018> kernel: Wireless: Send ASSOC response To 00:21:f2:36:4f:27 <Wed Apr 18 14:06:57 2018> kernel: Wireless: Rcv DeAuthentication From 00:21:f2:36:4f:27 <Wed Apr 18 14:06:59 2018> kernel: Wireless: Rcv AUTH From 00:21:f2:36:4f:27 <Wed Apr 18 14:06:59 2018> kernel: Wireless: Send AUTH response (SUCCESS)... <Wed Apr 18 14:06:59 2018> kernel: Wireless: Rcv ASSOC From 00:21:f2:36:4f:27 <Wed Apr 18 14:06:59 2018> kernel: Wireless: Send ASSOC response To 00:21:f2:36:4f:27 <Wed Apr 18 14:06:59 2018> kernel: Wireless: Rcv ASSOC From 00:21:f2:36:4f:27 <Wed Apr 18 14:07:00 2018> kernel: Wireless: Send ASSOC response To 00:21:f2:36:4f:27 <Wed Apr 18 14:07:00 2018> kernel: Wireless: Rcv ASSOC From 00:21:f2:36:4f:27 <Wed Apr 18 14:07:00 2018> kernel: Wireless: Send ASSOC response To 00:21:f2:36:4f:27 <Wed Apr 18 14:07:01 2018> kernel: Wireless: Rcv DeAuthentication From 00:21:f2:36:4f:27 <Wed Apr 18 14:07:03 2018> kernel: Wireless: Rcv AUTH From 00:21:f2:36:4f:27 <Wed Apr 18 14:07:03 2018> kernel: Wireless: Send AUTH response (SUCCESS)... </pre>								
Description								

On this page, users can refresh, clear and save relevant system information by clicking the corresponding button

Network page

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

WAN

This section mainly introduces the WAN port network connection mode in the basic mode.

(1) Static IP

This configuration can be used when the user receives a fixed public IP address or public subnet, ie multiple public IP addresses, from the Internet provider. In most cases, the cable service provider will provide a fixed public IP, and the DSL service provider will provide a public subnet. If you have a public subnet, you can assign an IP address to the WAN interface.

The screenshot shows the WAN configuration page with the following settings:

- WAN IP Mode: Static
- MAC Address Clone: Disable
- LAN Connection Mode: NAT
- Static IP Address: 192.168.10.247
- 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"> 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 manually configures the

Primary DNS Address The primary DNS of Internet port

Secondary DNS Address The secondary DNS of Internet port

(2) DHCP

The DHCP server assigns a private IP address to each local client.

The DHCP function allows the FPX9102H to automatically obtain an IP address from a DHCP server. In this case, there is no need to manually assign an IP address to the client.

The screenshot shows the router's configuration interface. The top navigation bar includes tabs for Status, Network, IPPBX, Wireless 2.4GHz, Wireless 5GHz, Security, Application, and Storage. Under the Network tab, there are sub-tabs for WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN, Port Forward, DMZ, DDNS, QoS, and Rate. Below these are 'Advance' and 'L2TP' options. The main content area is titled 'INTERNET' and shows the 'WAN' configuration. The 'WAN IP Mode' is set to 'DHCP'. Other settings include 'DHCP Server' (empty), 'MAC Address Clone' (Disable), 'LAN Connection Mode' (NAT), 'DNS Mode' (Manual), 'Primary DNS' (empty), and 'Secondary DNS' (empty).

Field Name	Description
WAN IP Mode	Choose DHCP mode,default is DHCP
DHCP server	DHCP server IP
MAC Address Clone	If enable "MAC Address Clone" feature
LAN Connection Mode	Choose LAN port connection mode:NAT,bridge
DNS Mode	Choose DNS mode:Auto,Manual 1.When the DNS mode is Auto, the device under the LAN port will automatically obtain Primary DNS and Secondary DNS 2.When the DNS mode is Manual, the user should manually configure Primary DNS and Secondary DNS
Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port

(3) PPPoE

PPPoE stands for Point-to-Point Protocol over Ethernet. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a

single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection. PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage			
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	DDNS	QoS	Rat
Advance	L2TP									

INTERNET	
WAN	
WAN IP Mode	PPPoE ▼
MAC Address Clone	Disable ▼
LAN Connection Mode	NAT ▼
DNS Mode	Auto ▼
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPPoE	
PPPoE Account	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm Password	<input type="password"/>
Service Name	<input type="text"/>
	Leave empty to autodetect
Operation Mode	Keep Alive ▼
Keep Alive Redial Period (0-3600s)	<input type="text" value="5"/>

Field Name	Description
WAN IP Mode	Choose PPPoE mode
MAC Address Clone	If enable “MAC Address Clone” feature
LAN Connection Mode	Choose LAN port connection mode:NAT,bridge
DNS Mode	Choose DNS mode:Auto,Manual 1.When the DNS mode is Auto, the device under the LAN port will automatically obtain Primary DNS and Secondary DNS 2.When the DNS mode is Manual, the user should manually configure Primary DNS and Secondary DNS
Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port
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; <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 20px;"> <p>Operation Mode</p> <p>On Demand Idle Time(0-60m)</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>On Demand ▾</p> <p>5</p> </div> </div> When the mode is Manual, there are no additional settings to configure
----------------	---

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

LAN

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

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage
WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ DDNS QoS Rat
Advance L2TP

PC Port(LAN)

PC Port(LAN)

Local IP Address: 192.168.1.1

Local Subnet Mask: 255.255.255.0

Local DHCP Server: Enable

DHCP Start Address: 192.168.1.2

DHCP End Address: 192.168.1.254

DNS Mode: Auto

Primary DNS: 192.168.1.1

Secondary DNS: 192.168.10.1

Client Lease Time (0-86400s): 86400

TFTP Server IPAddr: 192.168.1.1

Boot File:

DHCP Static Allotment

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

Field Name	Description
Local 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
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.

IPv6 Advance

To enable IPv6 functionality:

- 1.Navigate to Network > IPv6 Advanced page.
- 2.Select Enable from the IPv6 Enable drop-down list.
- 3.Click Save.



IPv6 WAN

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



IPv6 WAN Setting

IPv6 WAN Setting

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

Field Name	Description
Connection Type	Select connection type:DHCPv6,STATIC IPv6,PPPoE
DHCPv6 Address Settings	Set it to statefull or Stateless mode.
Prefix Delegation	Select enable or disable

IPv6 LAN

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

To enable LAN DHCPv6 service:



IPv6 LAN Setting

IPv6 LAN Setting

IPv6 Address	<input type="text" value="fec0::1"/>
IPv6 Prefix Length	<input type="text" value="64"/> (0-128)
DHCPv6 Server	
DHCPv6 Status	Disable ▾
DHCPv6 Mode	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	
Router Advertisement	Disable ▾
Advertise Interval	<input type="text" value="30"/> (10-1800sec)
RA Managed Flag	Disable ▾
RA Other Flag	Enable ▾
Prefix	<input type="text"/> / <input type="text"/>
Prefix Lifetime	<input type="text" value="3600"/> (0-3600sec)

VPN

VPN is a technology that establishes a private network on a public network. The connection between any two nodes of the VPN network does not have the end-to-end physical link required by the traditional private network, but is structured on the network platform provided by the public network service provider, and the user data is transmitted on the logical link. Through VPN technology, users can establish private connections and transmit data between any two devices on the public network. The FPX9102H supports PPTP, L2TP, and Open VPN.

PPTP



VPN Settings

Parameters name	Description
VPN Enable	Whether to enable VPN. Select PPTP mode.
Initial Service IP	The IP address of the VPN server.
User Name	The user name required for authentication.
Password	The password required for authentication.
VPN As Default Route	Prohibited or open, the default is prohibited.
MPPE Stateful	Disable or enable MPPE Stateful.
Require MPPE	Disable or enable Require MPPE.

L2TP

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage
WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN **VPN** Port Forward DMZ DDNS QoS Rat
Advance L2TP

VPN Settings

Administration

VPN Enable L2TP ▾
 Initial Service IP
 User Name
 Password
 L2TP Tunnel Name
 L2TP Tunnel Password
 VPN As Default Route Disable ▾

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

OpenVPN:

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage
WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN **VPN** Port Forward DMZ DDNS QoS R
Advance L2TP

VPN Settings

Administration

VPN Enable OpenVPN ▾
 OpenVPN TLS Auth Disable ▾
 VPN As Default Route Disable ▾

Parameters name	Description
VPN Enable	Whether to enable VPN. Select OpenVPN mode.

OpenVPN TLS Auth	Whether OpenVPN TLS authentication is enabled
VPN As Default Route	Prohibited or open, the default is prohibited.

Port Forward

Navigation menu: Status, Network, IPPBX, Wireless 2.4GHz, Wireless 5GHz, Security, Application, Storage, Administration, WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN, Port Forward, DMZ, DDNS, QoS, Rate Limit, Port S, Advance, L2TP

Port Forwarding				
No.	Comment	IP Address	Port Range	Protocol

Port Forwarding

Comment

IP Address

Port Range -

Protocol

(The maximum rule count is 32)

Virtual Servers					
No.	Comment	IP Address	Public Port	Private Port	Protocol

Virtual Servers

Comment

IP Address

Public Port

Private Port

Protocol

(The maximum rule count is 32)

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

Comment	To set up a virtual server notes
IP Address	Virtual server IP address
Public Port	Public port of virtual server
Private Port	Private port of virtual servers ports
Protocol	You can select from TCP, UDP, and TCP&UDP
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes

DMZ

The DMZ (Demilitarized zone) is a buffer established between a non-security system and a security system to solve the problem that an external network access user cannot access an internal network server after installing a firewall. This buffer is located in the small network area between the internal network of the enterprise and the external network. In this small network area can be placed some must be open server facilities, such as corporate Web servers, FTP servers and forums. On the other hand, through such a DMZ area, the internal network is more effectively protected. Because this kind of network deployment, compared to the general firewall scheme, an additional level is added to the attacker from the external network. After the DMZ host is set in the LAN, the host will be completely exposed to the wide area network, and bidirectional unrestricted communication can be realized. Adding a client to the DMZ may bring insecurity to the local network, so do not use this item easily.

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

QoS

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage Administration

WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ DDNS **QoS** Rate Limit Port Setting Routing

Advance L2TP

QoS setting

QoS setting

Enable QoS Disable ▾

Upstream (0-102400)kbit/s

Downstream (0-102400)kbit/s

Algorithm WFQ ▾

Save Cancel

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
Delete Selected Add															

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

Rate Limit

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage Administ

WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ DDNS QoS Rate Limit

Advance L2TP

Rate Limit Setting Help

Enable Rate Limit

Port	Ingress Rate	Egress Rate
WAN	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN1	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN2	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN3	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s
LAN4	<input type="text" value="100000"/> (1-100000)kbit/s	<input type="text" value="100000"/> (1-100000)kbit/s

Port	Broadcast Storm Rate
WAN	<input type="text" value="255"/> (0-255)*64 packets/s
LAN1	<input type="text" value="255"/> (0-255)*64 packets/s
LAN2	<input type="text" value="255"/> (0-255)*64 packets/s
LAN3	<input type="text" value="255"/> (0-255)*64 packets/s
LAN4	<input type="text" value="255"/> (0-255)*64 packets/s

Description

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

Port Setting

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage Administration

WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ DDNS QoS Rate Limit Port Setting

Advance L2TP

Port Setting Help

Port Setting

WAN Port Speed Nego

LAN1 Port Speed Nego

LAN2 Port Speed Nego

LAN3 Port Speed Nego

LAN4 Port Speed Nego

Field Name	Description
WAN Port speed Nego	Auto-negotiation, options are Auto, 1000Mbps full, 100Mbps Full, 100Mbps Half, 10Mbps Full, 10Mbps Half.

LAN1~LAN3 Port Speed Auto-negotiation, options are Auto, 1000Mbps full, 100Mbps Full, 100Mbps Nego Half, 10Mbps Full, 10Mbps Half.

Routing

Status **Network** IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage Administration

WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ DDNS QoS Rate Limit Port Setting Routing

Advance L2TP

Static Routing Settings
Help

Add a routing rule

Destination

Host/Net

Host ▾

Gateway

Interface

LAN ▾

Comment

Apply
Reset

Add or remove Internet routing rules here.

Current Routing Table in the system

No.	Destination	Mask	Gateway	Flags	Metric	Interface	Comment

Delete Selected
Reset

Field Name	Description
Destination	Destination address
Host/Net	Both Host and Net selection
Gateway	Gateway IP address
Interface	LAN/INTERNET/VOICE/TR069/VPN options
Comment	Comment

Advance

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage			
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	DDNS	QoS	Rate
Advance	L2TP									

Most Nat connections (512-8192)	4096
MSS Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Auto
MSS Value (1260-1460)	1440
Anti-DoS-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 FWR9502 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

IPPBX

Click to enter the IPPBX configuration page, in this page you can configuring the FWR9502 PBX features.

Basic

The figure shows the basic configuration information related to PBX configuration :

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
--------	---------	--------------	-----------------	---------------	----------	-------------	---------

Basic

Asterisk Configuration Interface

Asterisk-GUI

Use Asterisk-GUI Configuration PBX Click here to configure the PBX

Asterisk Config File

Config File Upload & Download

Local File 选择文件 未选择任何文件

Upload Download

Welcome IVR File

Welcome IVR Upload & Download

File IVR1 ▼

Local File 选择文件 未选择任何文件 (Support only *.wav)

Upload Download

Accessible IP List

Accessible IP Setting

No.	IP Address	No.	IP Address
Delete Selected Add			
Add an Accessible IP or Network Segment or Domain Name Accessible IP / Network Segment / Domain Name 			
Apply Cancel			

Parameters name	Description
Asterisk Configuration Interface	
Use Asterisk-GUI Configuration PBX	<p>click Click here to configure the PBX button, will enter the PBX configuration interface</p>
Asterisk Cofig File	
Config File Upload & Download	can upload or download config file
Welcome IVR File	
File	<p>You can select a file in IVR1~IVR5.</p> <p>Or click on the local file to upload or download IVR, note that only upload *.wav format is supported</p>

Wireless 2.4G

Basic

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Admi
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: FLY2.4B_0D6CD0 Enable Hidden Isolated Max Client: 16

Multiple SSID1: Enable Hidden Isolated Max Client: 16

Multiple SSID2: Enable Hidden Isolated Max Client: 16

Multiple SSID3: Enable Hidden Isolated Max Client: 16

broadcast (SSID): Enable Disable

AP Isolation: Enable Disable

MBSSID AP Isolation: Enable Disable

BSSID: 00:21:F2:0D:6C:D0

Frequency (Channel): Auto ▼

AutoChSel CH Range: 1 2 3 4 5 6 7 8 9 10 11 12 13

AutoChSel Interval(sec):

HT Physical Mode

Operating Mode: Mixed Mode Green Field

Channel BandWidth: 20 20/40 Auto

Guard Interval: Long Short

Reverse Direction Grant (RDG): Disable Enable

STBC: Disable Enable

Aggregation MSDU (A-MSDU): Disable Enable

Auto Block ACK: Disable Enable

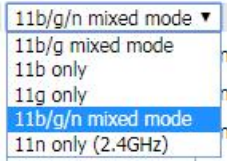
Decline BA Request: Disable Enable

HT Disallow TKIP: Disable Enable

20/40 Coexistence: Disable Enable

HT LDPC: Disable Enable

Field Name	Description
Radio on/off	Select “Radio off” to disable wireless. Select “Radio on” to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP

Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed mode 
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
Multiple SSID1~SSID3	The device supports 4 SSIDs.
Hidden	After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list
Broadcast(SSID)	After initial State opening, the device broadcasts the SSID of the router to wireless network
AP Isolation	If AP isolation is enabled, the clients of the AP cannot access each other.
MBSSID AP Isolation	AP isolation among the devices which are not belong to this AP and along to, when the option is enabled, the devices which do not belong to this AP cannot access the devices which are within the AP
BSSID	A group of wireless stations and a WLAN access point (AP) consists of a basic access device (BSS), each computer in the BSS must be configured with the same BSSID, that is, the wireless AP logo
Frequency (Channel)	You can select Auto Select and channel 1/2/3/4/5/6/7/8/9/10/11.
HT Physical Mode Operating Mode	Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system
Channel Bandwidth	Select channel bandwidth, default is 20 MHz and 20/40 MHz.
Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval

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

Wireless Security

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

Wi-Fi Security Settings

Select SSID

SSID choice:

"FLY2.4B_0D6CD0"

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:

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

Wi-Fi Security Settings

Select SSID

SSID choice:

"FLY2.4B_0D6CD0"

Security Mode:

Wire Equivalence Protection (WEP)

Default Key:

WEP Keys	WEP Key 1	<input type="text" value="*****"/>	Hex <input type="text" value="Hex"/>	64bit <input type="text" value="64bit"/>
	WEP Key 2	<input type="text" value="*****"/>	Hex <input type="text" value="Hex"/>	64bit <input type="text" value="64bit"/>
	WEP Key 3	<input type="text" value="*****"/>	Hex <input type="text" value="Hex"/>	64bit <input type="text" value="64bit"/>
	WEP Key 4	<input type="text" value="*****"/>	Hex <input type="text" value="Hex"/>	64bit <input type="text" value="64bit"/>

Access Policy

Policy:

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

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

WEP represents Wired Equivalent Privacy, which is a basic encryption method.

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

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

Wi-Fi Security Settings

Select SSID

SSID choice: FLY2.4B_0D6CD0 ▼
 "FLY2.4B_0D6CD0"
 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.
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

Wi-Fi Security Settings

Select SSID

SSID choice: FLY2.4B_0D6CD0 ▼
 "FLY2.4B_0D6CD0"
 Security Mode: WPAPSKWPA2PSK ▼

WPA

WPA Algorithms: TKIP AES TKIPAES
 Pass Phrase: *****
 Key Renewal Interval: 3600 sec (0 ~ 86400)

Access Policy

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

Field Name	Description
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
Pass Phrase	Set WPA-PSK/WPA2-PSK security code
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s



Note: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

Access Policy

Policy Disable ▾

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

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

WMM

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administration
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		
WMM Parameters of Access Point								Help
	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"/>		

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

WDS

Description

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

WPS

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

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

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	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	FLY2.4B_0D6CD0

WPS Progress

WPS Mode PIN PBC

WPS Status

WSC:Idle

Field Name	Description
WPS Config	
WPS	Enable/Disable WPS function
WPS Summary	
WPS Current Status	Display the current status of WPS
WPS Configured	Display the configure the status information of WPS
WPS SSID	Display WPS SSID
WPS Progress	

WPS Mode PIN : Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then router begins to send signals, turn on the PIN accessing method on the clients, and then it can access the wireless AP automatically.

PBC: There are two ways to start PBC mode, user can press the PBC button directly on the device, or select PBC mode on the software and apply. Users can activate WPS connection in WPS mode through these two methods, only when the clients choose PBC access, the clients can connect the AP automatically.

WPS Status WPS shows status in three ways:
 WSC: Idle
 WSC: Start WSC process (begin to send messages)
 WSC: Success; this means clients have accessed the AP successfully

Station Info

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced	

Wireless Status

Wireless Status

Current Channel	Channel 12
FLY2.4B_0D6CD0	00:21:F2:0D:6C:D0
91020D6CD0	

Wireless Network

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
-------------	-----	-----	--------	-----	----	-----	------

Description

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

Advanced

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
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)	3 (range 1 - 255, default 3)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 % (range 1 - 100, default 100)
Short Preamble	<input checked="" type="radio"/> Enable <input 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 checked="" type="radio"/> Enable <input type="radio"/> Disable
Country Code	CN (China) ▼
Support Channel	Ch1~13 ▼
Carrier Detect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
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
Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Field Name	Description
BG Protection Mode	Select G protection mode, options are on, off and automatic.
Beacon Interval	The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.
Data Beacon Rate (DTIM)	Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive
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	Multicast-to-Unicast Converter Enable/Disable Multicast-to-Unicast. By default, it is Disabled

Wireless 5G

Please refer to the [wireless 2.4G](#).

Security

Filtering Setting

Status Network IPPBX Wireless 2.4GHz Wireless 5GHz **Security** Application

Filtering Setting Content Filtering

Basic Settings

Basic Settings

Filtering Disable ▾
 Default Policy Drop ▾
 The packet that doesn't match any rules would be Drop

IP/Port Filter Settings

Interface LAN ▾
 MAC Address
 Dest IP Address
 Source IP Address
 Protocol NONE ▾
 Dest. Port Range -
 Src Port Range -
 Action Accept ▾
 Comment
 (The maximum rule count is 32)

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 ICMP

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

Status
Network
IPPBX
Wireless 2.4GHz
Wireless 5GHz
Security
Application
Storage

Filtering Setting
Content Filtering

Basic Settings

Basic Settings

Filtering Disable ▼

Default Policy Accept ▼

Filter List Upload & Download

Local File 未选择任何文件

Web URL Filter Settings

Current Web URL Filters

No.	URL

Add a URL Filter

URL

(The maximum rule count is 16)

Field Name	Description
Filtering	Enable/Disable content Filtering

Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL	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)
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

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Advance Nat	UPnP	IGMP					

ALG

ALG Setting

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

File name	Description
FTP	Enable/Disable FTP
SIP	Enable/Disable SIP
H323	Enable/Disable H323
PPTP	Enable/Disable PPTP
L2TP	Enable/Disable L2TP
IPSec	Enable/Disable

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.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Advance Nat	UPnP	IGMP					
UPnP							
UPnP Setting							
Enable UPnP	Enable ▼						
File name	Description						
UPnP	Enable/Disable UPnP						

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.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Advance Nat	UPnP	IGMP					
IGMP							
IGMP Setting							
Enable IGMP Proxy	Disable ▼						
Enable IGMP Snooping	Disable ▼						
Field Name	Description						
Enable IGMP Proxy	Enable/Disable IGMP Proxy function.						
Enable IGMP Snooping	Enable/Disable IGMP Snooping function.						

Storage

Status Network IPPBX Wireless 2.4GHz Wireless 5GHz Security Application **Storage**

Disk Management FTP Setting

Disk Management

Folder List

Directory Path	Partition
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Remove Disk"/>	

Partition Status

Partition	Path
<input type="button" value="Format"/> <input type="button" value="Reallocate"/>	

Field Name	Description
Add	Adding files to the USB storage device
Delete	Remove the USB storage device file
Remove Disk	Transfer files within a USB storage device
Format	Format the USB storage device
Re-allocate	Reset the USB storage device

Disk Management

FTP Setting

Status Network IPPBX Wireless 2.4GHz Wireless 5GHz Security Application Storage

Disk Management FTP Setting

FTP Setting

FTP Server Setup

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

Field Name	Description
FTP Server	Enable/Disable FTP server
FTP Server Name	Set the FTP server name
Anonymous Login	If or not support anonymous login
FTP Port	Set FTP server port number
Max. Sessions	Maximum number of connections
Create Directory	Enable/Disable create directory
Rename File/Directory	Enable/Disable rename file/directory
Remove File/Directory	Enable/Disable transfer of files/directories
Read File	Enable/Disable read files
Write File	Enable/Disable write files
Download Capability	Enable/Disable download capability function.
Upload Capability	Enable/Disable upload capability function

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

1) 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

2) Administrator settings

Administrator Settings

Password Reset

User Type	<input type="text" value="Admin User"/>	
New User Name	<input type="text" value="admin"/>	
New Password	<input type="text"/>	(The maximum length is 25)
Confirm Password	<input type="text"/>	

Language

Language	<input type="text" value="English"/>
----------	--------------------------------------

VPN Access

Management Using VPN	<input type="text" value="Disable"/>
----------------------	--------------------------------------

Web Access

Remote Web Login	<input type="text" value="Enable"/>
Web Port	<input type="text" value="80"/>
Web SSL Port	<input type="text" value="443"/>
Web Idle Timeout (0 - 60min)	<input type="text" value="5"/>
Allowed Remote IP (IP1;IP2;...)	<input type="text" value="0.0.0.0"/>

Telnet Access

Remote Telnet	<input type="text" value="Enable"/>
Telnet Port	<input type="text" value="23"/>
Allowed Remote IP (IP1;IP2;...)	<input type="text" value="0.0.0.0"/>
HostName	<input type="text" value="G902"/>

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
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	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.

3)NTP settings

Time/Date Setting

NTP Settings

NTP Enable	Enable ▾
Option 42	Disable ▾
Current Time	2018 - 04 - 19 . 17 : 16 : 08
Sync with host	Sync with host
Time Zone	(GMT+08:00) China Coast, Hong Kong ▾
Primary NTP Server	pool.ntp.org
Secondary NTP Server	cn.pool.ntp.org
NTP synchronization (1 - 1440min)	60

Daylight Saving Time

Daylight Saving Time	Disable ▾
----------------------	-----------

Field Name	Description
NTP Enable	Enable/Disable NTP
Option 42	Enable/Disable DHCP option 42. This option specifies a list of the NTP servers
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

4)Daylight Saving Time

Daylight Saving Time

Daylight Saving Time	Enable ▼
Offset	0 <input type="text"/> Min.
Start Month	April ▼
Start Day of Week	Sunday ▼
Start Day of Week Last in Month	First in Month ▼
Start Hour of Day	2 <input type="text"/>
Stop Month	October ▼
Stop Day of Week	Sunday ▼
Stop Day of Week Last in Month	Last in Month ▼
Stop Hour of Day	2 <input type="text"/>

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.

5)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

Remote Syslog Enable	Enable/Disable remote syslog function
Remote Syslog server	Add a remote server IP address.
Syslog Enable	Enable/Disable syslog function

6)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.

Firmware Upgrade

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	

Firmware Management

Firmware Upgrade

Local Upgrade 选择文件 未选择任何文件

Upgrade

Description

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

Scheduled Tasks

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR069	Diagnosis	Operating Mode

Scheduled Tasks

Scheduled Wifi

No.	Enable	SSID	Week Select	Open Time	Close Time
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>					

Scheduled Reboot

Scheduled Reboot: ▾

Scheduled Mode: ▾

Time: ▾ : ▾

Scheduled PPPOE

Scheduled PPPOE: ▾

Scheduled Mode: ▾

Time: ▾ : ▾

Help

Scheduled Task
This function is automatically to WIFI, REBOOT moment.

Field Name	Description
Scheduled Wi-Fi	
Enable	Enable/Disable Scheduled Wi-Fi
SSID	Choose one SSID
Scheduled Mode	Chosse Scheduled Mode
Wi-Fi Work Time	Setting Wi-Fi Work Time
Apply	After setting,you can choose “apply” or “cancel”
Scheduled Reboot	
Scheduled Reboot	Enable/Disable scheduled Reboot
Scheduled Mode	Select scheduled Mode
Time	Set the time to restart
Scheduled PPPoE	
Scheduled PPPoE	Enable/Disable scheduled PPPoE
Scheduled Mode	Select scheduled Mode
Time	Set the time to start PPPoE

Provision

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

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

- Before testing or using HTTPS, user should have https server and upgrading file and configuring file and CA Certificate file (should same as https server's) and Client Certificate file and Private key file
User can upload a CA Certificate file and Client Certificate file and Private Key file in the Security page.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis

Provision

Configuration Profile

Provision Enable	Enable ▾
Resync on Reset	Enable ▾
Resync Random Delay (sec)	40
Resync Periodic (sec)	3600
Resync Error Retry Delay (sec)	3600
Forced Resync Delay (sec)	14400
Resync after Upgrade	Enable ▾
Resync from SIP	Disable ▾
Option 66	Enable ▾
Option 67	Enable ▾
Config File Name	\$(MA)
User Agent	
Profile Rule	http://prv1.flyingvoice.net:69/config/\$(MA)?mac=\$(MA)&

Firmware Upgrade

Enable Upgrade	Enable ▾
Upgrade Error Retry Delay (sec)	3600
Upgrade 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	Set the periodic time for resync, default is 3600s.

Forced Resync Delay(sec)	If it's time to resync, but the device is busy now, in this case, the router will wait for a period time, the longest is "Forced Resync Delay", default is 14400s, when the time over, the router will forced to resync.
Resync After Upgrade	Enable firmware upgrade after resync or not. The default is Enabled.
Resync From SIP	Enable/Disable resync from SIP.
Option 66	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.
Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.
Profile Rule	URL of profile provision file
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.

Firmware Upgrade

Upgrade Enable	Enable ▾
Upgrade Error Retry Delay(sec)	3600
Upgrade Rule	<input type="text"/>

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



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.

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis

TR-069 Configuration

ACS

TR-069 Enable	Enable ▾
CWMP	Enable ▾
ACS URL	<input type="text" value="http://acs1.flyingvoice.net:8080/tr069"/>
User Name	<input type="text" value="FLY69167000116"/>
Password	<input type="password" value="....."/>
Enable Periodic Inform	Enable ▾
Periodic Inform Interval	<input type="text" value="75821"/>

Connect Request

User Name	<input type="text" value="FPX9102H"/>
Password	<input type="password" value="....."/>

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.



Packet Trace

Packet Trace

Tracking Interface:

Packet Trace:

Ping Test

Ping Test

Dest IP/Host Name:

WAN Interface:

Traceroute Test

Traceroute Test

Dest IP/Host Name:

WAN Interface:

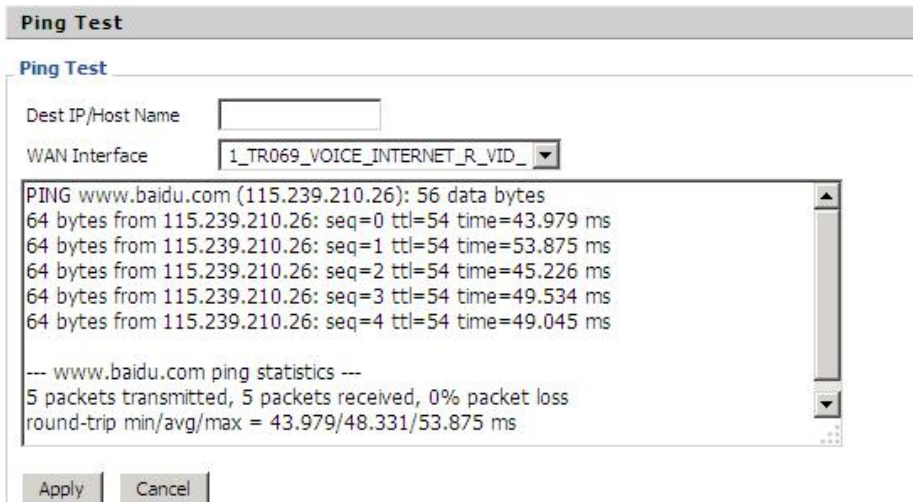
Description

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

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

Status	Network	IPPBX	Wireless 2.4GHz	Wireless 5GHz	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode
Operating Mode Settings								Help
Operating Mode Settings								
Operating Mode <input type="text" value="Advanced Mode"/>								

Description

Choose the Operation Mode as Basic Mode or Advanced Mode.

Chapter 4 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

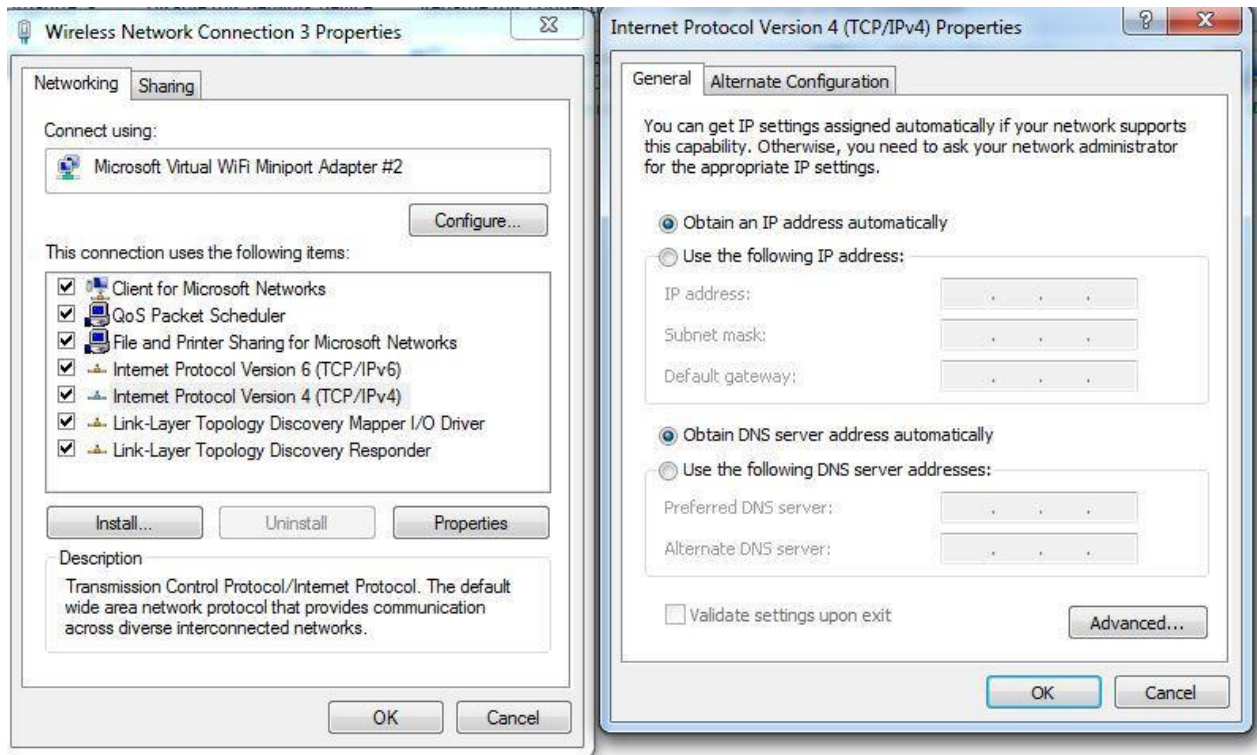
Follow the below process to set your PC to get an IP address automatically:

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.