



# User Manual

FWR9600B

---

# Contents

---

<b>About This User Guide.....</b>	<b>1</b>
Contacting FlyingVoice.....	1
Purpose .....	2
Cross references .....	2
Feedback.....	2
Declaration of Conformity.....	3
Part 15 FCC Rules .....	3
Warnings and Notes.....	4
Warnings.....	4
Notes.....	4
<b>Chapter 1 Product description.....</b>	<b>5</b>
FWR9600B.....	6
LED Indicators and Interfaces.....	7
Hardware Installation .....	10
<b>Chapter 2 Basic Settings .....</b>	<b>17</b>
Two-Level Management.....	18
Web Management Interface.....	18
Web Management Interface Details .....	20
Satus.....	20
Setting the Time Zone.....	21
Configuring an Internet Connection .....	22
Setting up Wireless Connections .....	24
Encryption.....	25
<b>Chapter 3 Web Interface.....</b>	<b>31</b>
Login.....	32
Status.....	33
Network and Security.....	34
WAN.....	34
LAN.....	39
VPN .....	40
Port Forward .....	41
DMZ.....	42
Port Setting .....	43
Routing.....	43

Advance .....	44
Wireless 2.4GHz .....	45
Wireless Security.....	48
WMM .....	51
WDS .....	51
WPS.....	52
Station Info .....	53
Advanced .....	54
Wireless 5GHz .....	56
Wireless Security.....	58
WMM .....	59
WDS .....	59
WPS.....	59
Station Info .....	59
Advanced .....	59
Security.....	77
Filtering Setting.....	77
Content Filtering .....	78
Application .....	80
Administration.....	85
Management .....	85
Firmware Upgrade .....	90
Provision .....	90
SNMP .....	92
TR-069.....	93
Diagnosis.....	94
Operating Mode.....	96
System Log .....	96
Logout .....	96
Reboot.....	97
<b>Chapter 4 IPv6 address configuration .....</b>	<b>98</b>
Introduction .....	99
IPv6 Advance.....	100
Configuring IPv6.....	100
Viewing WAN port status.....	102
IPv6 DHCP configuration for LAN/WLAN clients.....	102
LAN DHCPv6.....	103
<b>Chapter 5 Troubleshooting Guide.....</b>	<b>104</b>
Configuring PC to get IP Address automatically .....	105
Cannot connect to the Web.....	106
Forgotten Password.....	106

---

# Table

---

About This User Guide.....	1
Chapter 1 Product description .....	6
Table 1 Features at-a-glance .....	7
Table 2 LED Indicators.....	8
Table 3 Interfaces.....	9
Chapter 2 Basic Settings.....	12
Table 5 Web management interface.....	15
Table 6 Setting time zone.....	16
Table 7 Configuring an internet connection.....	17
Table 8 Wireless > Basic web page (user view) .....	19
Table 9 Wireless Security web page .....	20
Chapter 3 Web Interface .....	22
Table 12 Login details .....	23
Table 13 Status .....	24
Table 14 Internet.....	25
Table 15 DHCP.....	26
Table 16 PPPoE.....	27
Table 17 Bridge Mode.....	28
Table 18 LAN port.....	30
Table 19 VPN.....	31
Table 20 Port Forward .....	32
Table 21 Virtual Servers.....	33
Table 22 DMZ.....	33
Table 23 Port setting.....	34
Table 24 Routing .....	34
Table 25 Advance .....	35
Table 26 Basic .....	36
Table 27 Wireless security .....	39
Table 28 WiFi Security Setting.....	39
Table 29 WPA-PSK.....	40
Table 30 WPAPSKWPA2PSK .....	41
Table 31 Wireless Access Policy.....	41

Table 32 WMM .....	42
Table 33 WDS.....	42
Table 34 WPS .....	43
Table 35 Station info.....	45
Table 36 Advanced .....	45
Table 37 Basic .....	48
Table 38 Wireless security .....	50
Table 56 advance NAT .....	55
Table 57 UPnP .....	55
Table 58 IGMP .....	56
Table 62 Save Config File.....	57
Table 63 Administrator settings .....	58
Table 64 NTP settings .....	59
Table 65 Daylight Saving Time.....	60
Table 66 System log Setting .....	60
Table 67 Factory Defaults Setting .....	61
Table 68 Factory Defaults .....	61
Table 69 Firmware upgrade .....	62
Table 70 Provision .....	63
Table 71 Firmware Upgrade .....	65
Table 72 SNMP .....	65
Table 73 TR069.....	66
Table 75 Operating mode .....	69
Table 76 System log.....	69
Table 77 Logout.....	69
Chapter 4 IPv6 address configuration .....	71
Table 78 IPv6 Modes .....	72
Table 79 Enabling IPv6 .....	73
Table 80 Configuring Statefull IPv6.....	73
Table 81 Configuring Stateless IPv6 .....	74
Chapter 5 Troubleshooting Guide .....	77

# About This User Guide

---

Thank you for choosing FWR9600B wireless router with VoIP. FWR9600B includes extended functions which support, USB memory card, This design not only provide users with a conventional VoIP and routing capabilities. Users can also take FWR9600B as a FTP server, to share LAN files, pictures and other resources. Meanwhile, FWR9600B VoIP wireless router is ideally suited for small and medium enterprises (SMB) to build wireless office. FWR9600B supports IEEE802.11ac gigabit wireless LAN standard, the highest wireless speed is up to 867Mbps and it supports both 2.4GHz and 5GHz bands. For VoIP end user, 5G band can make sure less interference and the transmission quality. The more, users can enjoy greater bandwidth, and enhanced data throughput. FWR9600B is integrates Internet sharing for daily application. It can not only provides wired Internet sharing capabilities but also offers Access Point (AP) function for daily wireless communication.



This guide contains the following chapters:

- [Chapter 1 Product description](#)
- [Chapter 2 Configuring Basic Settings](#)
- [Chapter 3 Web Interface](#)
- [Chapter 4 IPv6 address configuration on WAN interface](#)
- [Chapter 5 Troubleshooting Guide](#)

## Contacting FlyingVoice

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

Sales enquiries: [sales1@flyingvoice.com](mailto:sales1@flyingvoice.com)

Support enquiries: [support@flyingvoice.com](mailto: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](mailto: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 three conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.
- The distance between user and products should be no less than 20cm
- Operations in the 5.15-5.25GHz band are restricted to indoor usage only

## CE

Manufacturer: Flyingvoice Network Technology Co., Ltd.

Address: Room 207~209, 2/F, Bldg B52#, Zhongchuang industrial park, Liuxian Avenue, Taoyuan street, Nanshan District, Shenzhen

Hereby, Flyingvoice Network Technology Co., Ltd. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU

Importers: XXXXXXXX

Address: XXXXXXXX

A copy of the declaration of conformity can be obtained with this user manual; this product is not restricted in the EU.

Hardware Version:R195W\_V1\_2

Software Version: V3.20(201901291603)

The wireless operation frequency

WIFI: 2412MHz-2472MHz, Max EIRP Power 18.95dBm

WIFI: 5180-5240MHz, Max EIRP Power 21.85dBm

WIFI: 5180-5240MHz, Max EIRP Power 21.85dBm

WIFI: 5745-5825MHz, Max EIRP Power 13.36dBm

### **Safety warning and Attentions**

If use adapter, adapter must be comply 2014/30/EU Directive

Adapter Caution: Adapter shall be installed near the equipment and shall be easily accessible.

Do not store or use your product in temperatures higher than 45°C

### **RF Exposure Statement**

The distance between user and products should be no less than 20cm

## 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:

- [FWR9600B](#)
- [LED Indicators and Interfaces](#)
- [Hardware Installation](#)
- [Voice Prompt](#)

# FWR9600B

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

Port/Model	FWR9600B
picture	
WAN	1
LAN	4
FXS	0
USB	NO
Ethernet interface	5* RJ45 10/100/1000M
WiFi	2.4G 2T2R(300Mbps) 5G 2T2R (867Mbps)
Management	Web Management, Provision:TFTP/HTTP/HTTPS, TR069, SNMP
VLAN	Support

# LED Indicators and Interfaces

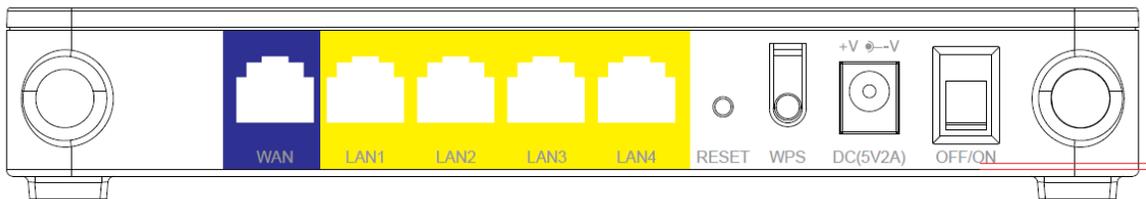
**Table 2** LED Indicators



LED	Status	Explanation
Power	on Green	System is powered on
	off	System is powered off
WAN	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
LAN ( 1-4 )	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
2.4G	on Green	Wireless access point is ready.
	Blinking Green	2.4g is connected,and there is data transmitted
	off	2.4g wifi off or system is powered off
5G	on Green	Wireless access point is ready.
	Blinking Green	5g is connected,and there is data transmitted
	off	5g wifi off or system is powered off
FXS(1-2)	on Green	Registered successfully,but no data transfer
	Blinking Green	There is data being transmitted or fxs port is registering
	off	Power is off or registered failed

**Table 3** Interfaces

FWR9600B



Interface	Description
POWER	Connector for a power adapter
RESET	Restore the factory settings button, press and hold the device after 5s to restore
WPS	Wi-Fi security settings, when mobile phones, laptops and other wireless devices to find the wireless router WiFi signal, when connected, click the WPS button on the router to complete the wireless router and wireless device encryption authentication and connection.
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices

## Hardware Installation

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

### Procedure 1 Configuring the Router

1. Connect the WAN port to the Internet your network's modem/switch/router/ADSL
2. 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 configuration or updating the device. Using other power adapters may damage the equipment and will void the manufacturer warranty.

The standard power supply is 12V, 1A, and the Operation Temperature: 0~50 Degree C

---



**Warning**

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

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

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

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

---

# Chapter 2 Basic Settings

---

This chapter covers:

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

# Two-Level Management

---

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

FWR9600B supports two-level management:

- (1) administrator mode operation: please type “admin/admin” on Username/Password and click Login button to begin configuration.
- (2) user mode operation, please type “user/user” on Username/Password and click Login button to begin configuration.

## Web Management Interface

The devices feature a web browser-based interface that may be used to configure and manage the device. See below for information

### Login in from the LAN port

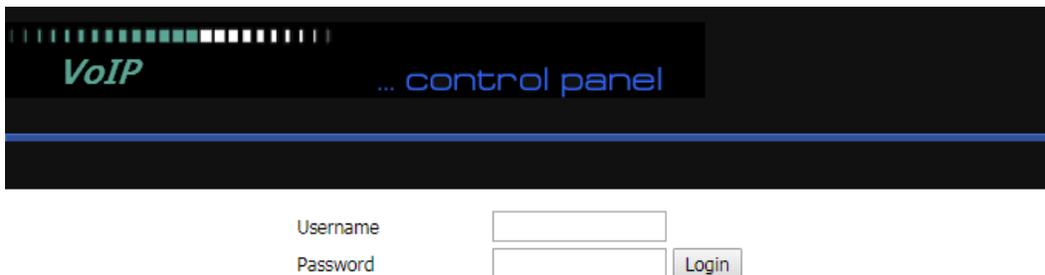
- 1.Ensure your PC is connected to the router’s LAN port correctly.



**Note**

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

- 2.Open a web browser on your PC and type “http://192.168.1.1”.
- 3.The following window appears and prompts for username , password.



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

---

**Note**



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

---

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

**Login in from the WAN port**

- 1.Ensure your PC is connected to the router’s WAN port correctly.
- 2.Obtain the IP addresses of WAN port using Voice prompt or by logging into the device web management interface via a LAN port and navigating to Network > WAN.
- 3.Open a web browser on your PC and type http://<IP address of WAN port>. The following login page will be opened to enter username and password.



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

---

**Note**



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

---

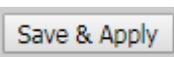
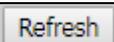
6.The web management interface automatically logs out the user after 5 minutes of inactivity.

# Web Management Interface Details

## Satus

**Table 5** Web management interface

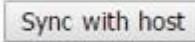


Serial number	Name	Description
Postition 1	Main navigation bar	Click this navigation bar to bring up the corresponding child navigation bar
Postition 2	navigation bar	Click the sub navigation bar to enter the configuration page
Postition 3	Product Information	Device Information Configuration Title
Postition 4	Product Information	Show product information
Postition 5	Login/Logout	main information shows the firmware version, DSP version, current time and management mode.
Postition 6	Help	help to display help information, users can get some help here
		Use this button,conifg will be saved and And take effect immediately
		After changing the parameters, you need to click this button to save. After you click Save, there is a need to restart the device.
		Click to cancel the change
		Click to restart
		Refresh current page

## Setting the Time Zone

**Table 6** Setting time zone

Time/Date Setting	
<b>NTP Settings</b>	
NTP Enable	Enable ▾
Option 42	Disable ▾
Current Time	2017 - 10 - 27 . 14 : 03 : 42
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
<b>Daylight Saving Time</b>	
Daylight Saving Time	Disable ▾

Field Name	Description
NTP Enable	Enable NTP (Network Time Protocol) to automatically retrieve time and date settings for the device
Option 42	Whether to enable Option 42
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.
Time Zone	Select the desired time zone
Primary NTP Server	Primary and secondary NTP server address for clock
Secondary NTP Server	synchronization. A valid NTP server must be reachable for full NTP
NTP Synchronization(1 - 1440min)	The synchronization period with NTP (1-1440 minutes), default is 60

## Configuring an Internet Connection

From the Network > WAN page, WAN connections may be inserted or deleted. For more information on Internet Connection setting, see Table 10below.

**Table 7** Configuring an internet connection

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate L
Advance										
<b>INTERNET</b>										
<b>WAN</b>										
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	<input type="text" value="1"/> (1-4094)									
DNS Mode	Auto ▾									
Primary DNS	<input type="text"/>									
Secondary DNS	<input type="text"/>									
DHCP										
DHCP Renew	Renew									
DHCP Vendor (Option 60)	<input type="text" value="FLYINGVOICE-G902CH"/>									
Port Bind										
<input checked="" type="checkbox"/> Port_1	<input checked="" type="checkbox"/> Port_2	<input checked="" type="checkbox"/> Port_3	<input checked="" type="checkbox"/> Port_4							
<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: LAN (local) ports can only be bound to one WAN (Internet) connection at a time!										

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	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
<b>DHCP</b>	<b>(Displayed when WAN IP Mode is set to DHCP)</b>
DHCP Renew	Refresh the DHCP IP
DHCP Vendor	Specify the DHCP Vendor field Display the vendor and product name

## Setting up Wireless Connections

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

1. Enable Wireless and Setting SSID
2. Open Wireless > Basic webpage as shown below:

**Table 8** Wireless > Basic web page (user view)

The screenshot shows the 'Basic Wireless Settings' page with the following configurations:

- Radio On/Off: Radio On
- Wireless Connection Mode: AP
- Network Mode: 11b/g/n mixed mode
- Multiple SSID: G902CH-0000B8, Enable checked, Hidden, Isolated, Max Client 16
- Multiple SSID1: Empty, Enable, Hidden, Isolated, Max Client 16
- Multiple SSID2: Empty, Enable, Hidden, Isolated, Max Client 16
- Multiple SSID3: Empty, Enable, Hidden, Isolated, Max Client 16
- broadcast (SSID): Enable selected
- AP Isolation: Disable selected
- MBSSID AP Isolation: Disable selected
- BSSID: 8C:88:2B:40:00:6C
- Frequency (Channel): Auto
- AutoChSel CH Range: 1-11 (checkboxes)
- AutoChSel Interval(sec): Empty
- HT Physical Mode: Operating Mode
- Operating Mode: Mixed Mode selected
- Channel BandWidth: 20/40 selected

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 FWR8401
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
BSSID	Basic Service Set Identifier – AP MAC Address Listing
Frquency (Channel)	Select the channel of operation for the device from the drop-down list
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
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 'Wireless Security' tab selected in a navigation menu. Below the menu is a 'Wi-Fi Security Settings' section. Under 'Select SSID', the 'SSID choice' is 'FWR9202-0C1F38' and the 'Security Mode' is 'WPA-PSK'. In the 'WPA' section, 'WPA Algorithms' are set to 'AES' (selected), with 'TKIP' and 'TKIPAES' unselected. The 'Pass Phrase' is masked with asterisks, and the 'Key Renewal Interval' is set to '3600 sec (0 ~ 86400)'. In the 'Access Policy' section, the 'Policy' is set to 'Disable'. At the bottom, there are buttons for 'Save & Apply', 'Save', 'Cancel', and 'Reboot'.

Field Name	Description
SSID Choice	Choose the SSID from the drop-down list for which security will be configured
Security Mode	<p>Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.</p> <p>Each encryption mode will launch an additional web page and ask you to offer additional configuration.</p> <p>For high security, the device can be configured for Security Mode as WPA2-PSK and WPA Algorithms as AES.</p>
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.
<b>Access Policy</b>	
Policy	<p>Disable: Access policy rules are not enforced</p> <p>Allow: Only allow the clients in the station MAC list to access Rejected: Block the clients in the station MAC list from registering</p>
Add a Station MAC	Enter the MAC address of the clients which you want to allow or reject

---

## Chapter 3 Web Interface

---

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

- [Login](#)
- [Status](#)
- [Network and Security](#)
- [Wireless](#)
- [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

---

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

**Table 13** Status

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	LAN Host	Syslog						
<b>Product Information</b>								
<b>Product Information</b>								
Product Name	G902CH							
Internet (WAN) MAC Address	00:21:F2:00:00:B9							
PC (LAN) MAC Address	00:21:F2:00:00:B8							
Hardware Version	V3.3							
Loader Version	V3.35(May 4 2017 17:41:36)							
Firmware Version	V3.20(201709081731)							
Serial Number	FLY58161000002							
<b>SIP Account Status</b>								
<b>SIP Account Status</b>								
FXS 1 SIP Account Status	Register Fail							
Primary Server	0.0.0.0							
Backup Server	0.0.0.0							

# 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	<input type="text" value="192.168.10.173"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.10.1"/>
DNS Mode	<input type="text" value="Manual"/>
Primary DNS	<input type="text" value="192.168.10.1"/>
Secondary DNS	<input type="text" value="192.168.18.1"/>

Field Name	Descripti
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	<p>Select DNS mode, options are Auto and Manual:</p> <ol style="list-style-type: none"> <li>When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS.</li> <li>When DNS mode is Manual, the user manually configures the preferred DNS and alternate DNS information</li> </ol>
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

**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-G902CH	

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.
Primary DNS Address	When DNS mode is Manual, the user should manually configure the 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	
<b>WAN</b>	
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼ <span style="float: right;">Delete Connect</span>
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"/>
<b>PPPoE</b>	
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;  <div style="text-align: right;">                     Operation Mode <input type="text" value="On Demand"/>                       On Demand Idle Time(0-60m) <input type="text" value="5"/> </div> When the mode is Manual, there are no additional settings to configure
Keep Alive Redial	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	<input type="text" value="1_MANAGEMENT_VOICE_INTERNET_R_VID"/>	<input type="button" value="Delete Connect"/>
Service	<input type="text" value="MANAGEMENT_VOICE_INTERNET"/>	
IP Protocol Version	<input type="text" value="IPv4"/>	
WAN IP Mode	<input type="text" value="Bridge"/>	
Bridge Type	<input type="text" value="IP Bridge"/>	
DHCP Service Type	<input type="text" value="Pass Through"/>	
VLAN Mode	<input type="text" value="Disable"/>	
VLAN ID	<input type="text" value="1"/> (1-4094)	

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	Descripti
<b>Bridge Type</b>	
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
<b>DHCP Service Type</b>	
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.
<b>VLAN Mode</b>	
<b>Disable</b>	The WAN interface is untagged. LAN is untagged.
<b>Enable</b>	The WAN interface is tagged. LAN is untagged.
<b>Trunk</b>	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.
<b>VLAN ID</b>	Set the VLAN ID.
<b>802.1p</b>	Set the priority of VLAN, Options are 0~7.

**Note**

Multiple WAN connections may be created with the same VLAN ID

# LAN

## LAN Port

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

**Table 18** LAN port

Status	<b>Network</b>	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Applicati		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Ra
Advance										

---

**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

DHCP Client List

DHCP Static Allotment

NO.	MAC	IP Address
Delete Selected Add Edit		

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 192.168.11.1).
Local Subnet Mask	Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24).
Local DHCP Server	Enable/Disable Local DHCP Server.

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

## VPN

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

**Table 19** VPN

The screenshot displays the router's control panel with the following elements:

- Navigation:** Status, Network (selected), Wireless, SIP Account, Phone, Administration.
- Sub-navigation:** WAN, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN (selected), Port Forward, DMZ, DDNS, Port Setting.
- Section:** VPN Settings
- Administration:**
  - VPN Enable: A dropdown menu with options: Disable (highlighted), PPTP, L2TP, OpenVPN.
  - Buttons: Save & Apply, Save, Cancel, Reboot.

Field Name	Description
VPN Enable	Enable/Disable VPN. If the VPN is enabled, user can select PPTP and L2TP mode VPN.
Initial Service IP	Enter VPN server IP address.
User Name	Enter authentication username.
Password	Enter authentication password.

## Port Forward

**Table 20** Port Forward

Status Network Wireless 2.4GHz Wireless 5GHz SIP FXS1 FXS2 Security Application Storage Adm

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

Advance

Port Forwarding

No.	Comment	IP Address	Port Range	Protocol
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Delete Selected</span> <span>Add</span> <span>Edit</span> </div>				
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <p>Port Forwarding</p> <p>Comment <input style="width: 100%;" type="text"/></p> <p>IP Address <input style="width: 100%;" type="text"/></p> <p>Port Range <input style="width: 40%;" type="text"/> - <input style="width: 40%;" type="text"/></p> <p>Protocol <span style="border: 1px solid black; padding: 2px;">TCP&amp;UDP ▼</span></p> <p><small>( The maximum rule count is 32 )</small></p> </div> <div style="width: 50%; text-align: right;"> <input style="width: 100%; height: 20px; margin-bottom: 5px;" type="text"/>  <input style="width: 100%; height: 20px; margin-bottom: 5px;" type="text"/>  <input style="width: 40%; height: 20px; margin-bottom: 5px;" type="text"/> - <input style="width: 40%; height: 20px; margin-bottom: 5px;" type="text"/>  <span style="border: 1px solid black; padding: 2px;">TCP&amp;UDP ▼</span> </div> </div>				
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Apply</span> <span>Cancel</span> </div>				

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.

**Table 21** 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	To set up a virtual server notes
IP Address	Virtual server IP address
Public Port	Public port of virtual server
Private Port	Private port of virtual servers ports
Protocol	You can select from TCP, UDP, and TCP&UDP.
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes.

## DMZ

**Table 22** DMZ

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate
Advance										
<b>Demilitarized Zone (DMZ)</b>										
<b>DMZ Setting</b>										
DMZ Enable <input type="text" value="Enable"/>										
DMZ Host IP Address <input type="text"/>										

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

## Port Setting

**Table 23** 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 24** Routing

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

## Advance

**Table 25** Advance

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate
Advance										

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 FWR8401 can provide
Mss Mode	Choose Mss Mode from Manual and Auto
Mss Value	Set the value of TCP
AntiDos-p	You can choose to enable or prohibit
IP conflict detection	Select enable if enabled, phone IP conflict will have tips or prohibit;
IP conflict Detecting Interval	Detect IP address conflicts of the time interval

# Wireless 2.4GHz

## Basic

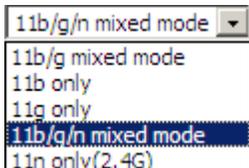
**Table 26** Basic

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

Basic Wireless Settings	
<b>Wireless Network</b>	
Radio On/Off	Radio On ▼
Wireless Connection Mode	AP ▼
Network Mode	11b/g/n mixed mode ▼
Multiple SSID	G902CH-0000B8 Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID1	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID2	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID3	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="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	8C:88:2B:40:00:6C
Frequency (Channel)	Auto ▼
AutoChSel CH Range	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11
AutoChSel Interval(sec)	<input type="text"/>
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 <input type="radio"/> Auto
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Short
Reverse Direction Grant (RDG)	<input type="radio"/> Disable <input checked="" 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
20/40 Coexistence	<input checked="" type="radio"/> Disable <input 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
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 27** Wireless security

Status	Network	<b>Wireless 2.4GHz</b>	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	<b>Wireless Security</b>	WMM	WDS	WPS	Station Info	Advanced		

---

**Wi-Fi Security Settings**

Select SSID

SSID choice: G902CH-0000B8 ▼  
 "G902CH-0000B8"  
 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
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 28** WiFi Security Setting

<b>Wi-Fi Security Settings</b>			
--------------------------------	--	--	--

---

Select SSID

SSID choice: G902CH-0000B8 ▼  
 "G902CH-0000B8"  
 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 ▼

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 29** WPA-PSK

**Wi-Fi Security Settings**

Select SSID

SSID choice	G902CH-0000B8 ▼
"G902CH-0000B8"	
Security Mode	WPA-PSK ▼
<b>WPA</b>	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	*****
Key Renewal Interval	3600 sec (0 ~ 86400)

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:

**Table 30** WPAPSKWPA2PSK

Wi-Fi Security Settings	
<b>Select SSID</b>	
SSID choice	G902CH-0000B8 ▼
"G902CH-0000B8"	
Security Mode	WPA2-PSK ▼
<b>WPA</b>	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> 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 31** Wireless Access Policy

**Access Policy**

Policy Disable ▾

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

Disable  
Allow  
Reject

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

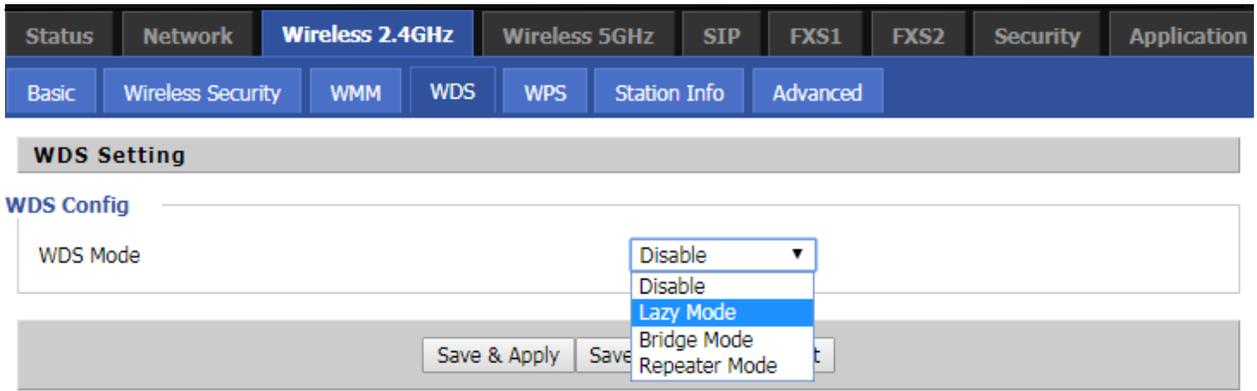
WMM (Wi-Fi Multi-Media) is the QoS certificate of Wi-Fi Alliance (WFA). This provides you to configure the parameters of wireless multimedia; WMM allows wireless communication to define a priority according to the home gateway type. To make WMM effective, the wireless clients must also support WMM.

**Table 32** WMM

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		
WMM Parameters of Access Point								
	AIFSN	CWMin	CWMax	TXOP	ACM	AckPolicy		
AC_BE	3	1 ▾	63 ▾	0	<input type="checkbox"/>	<input type="checkbox"/>		
AC_BK	7	1 ▾	102 ▾	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"/>		

## WDS

**Table 33** WDS



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

## WPS

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

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

**Table 34** WPS

Status	Network	<b>Wireless 2.4GHz</b>	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
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	G902CH-0000B8

---

**WPS Progress**

WPS Mode  PIN  PBC

---

**WPS Status**

WSC:Idle

Field Name	Description
<b>WPS Config</b>	
WPS	Enable/Disable WPS function
<b>WPS Summary</b>	
WPS Current Status	Display the current status of WPS
WPS Configured	Display the configure the status information of WPS
WPS SSID	Display WPS SSID
<b>WPS Progress</b>	
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	WPS shows status in three ways: WSC: Idle WSC: Start WSC process (begin to send messages) WSC: Success; this means clients have accessed the AP successfully
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

## Station Info

**Table 35** Station info

---

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Applicati
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

**Wireless Status**

---

**Wireless Status**

Current Channel	Channel 1
G902CH-0000B8	8C:88:2B:40:00:6C

**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

**Table 36** Advanced

---

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Applicat
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		
<b>Advanced Wireless</b>								
<b>Advanced Wireless</b>								
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			US (United States) ▾					
Support Channel			Ch1~11 ▾					
Carrier Detect			<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
<b>Wi-Fi Multimedia</b>								
WMM Capable			<input checked="" type="checkbox"/>					
Multiple SSID			<input 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					

Field Name	Description
BG Protection Mode	Select G protection mode, options are on, off and automatic.
Beacon Interval	The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.
Data Beacon Rate(DTIM)	Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive broadcast multi-cast.
Fragment Threshold	Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet is divided.
RTS Threshold	Specify the packet RTS threshold, when the packet exceeds this value, the router will send RTS to the destination site consultation
TX Power	Define the transmission power of the current AP, the greater it is, the stronger the signal is.
Short Preamble	Choose enable or disable
Short Slot	Enable/Disable short slot. By default it is enabled, it is helpful in improving the transmission rate of wireless communication.
Tx Burst	One of the features of MAC layer, it is used to improve the fairness for transmitting TCP.
Pkt_Aggregate	It is a mechanism that is used to enhance the LAN, in order to ensure that the home gateway packets are sent to the destination correctly.

---

Support Channel	Choose appropriate channel
-----------------	----------------------------

---

<b>Wi-Fi Multimedia (WMM)</b>	
-------------------------------	--

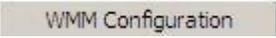
---

WMM Capable	Enable/Disable WMM.
-------------	---------------------

---

APSD Capable	Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power
--------------	-------------------------------------------------------------------------------------------------------------------------

---

WMM Parameters	Press  , the webpage will jump to the configuration page of Wi-Fi multimedia.
----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

---

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

---

# Basic

**Table 37** Basic

Basic Wireless Settings	
<b>Wireless Network</b>	
Radio On/Off	Radio On ▾
Wireless Connection Mode	AP ▾
Network Mode	11vht AC/AN/A ▾
Multiple SSID	G902CH-5G-0000B8 Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID1	<input type="text"/> Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID2	<input type="text"/> Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
Multiple SSID3	<input type="text"/> Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client <input type="text" value="16"/>
broadcast (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	8C:88:2B:40:00:6F
Frequency (Channel)	Auto ▾
AutoChSel CH Range	<input type="checkbox"/> 36 <input type="checkbox"/> 40 <input type="checkbox"/> 44 <input type="checkbox"/> 48 <input type="checkbox"/> 52 <input type="checkbox"/> 56 <input type="checkbox"/> 60 <input type="checkbox"/> 64 <input type="checkbox"/> 100 <input type="checkbox"/> 104 <input type="checkbox"/> 108 <input type="checkbox"/> 112 <input type="checkbox"/> 116 <input type="checkbox"/> 120 <input type="checkbox"/> 124 <input type="checkbox"/> 149 <input type="checkbox"/> 153 <input type="checkbox"/> 157 <input type="checkbox"/> 161
AutoChSel Interval(sec)	<input type="text"/>
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	<input type="radio"/> Long <input checked="" type="radio"/> Short
Guard Interval	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Reverse Direction Grant (RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	Auto ▾
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
20/40 Coexistence	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
HT LDPC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
VHT Option	<input checked="" type="radio"/> 20/40 <input type="radio"/> 80 <input type="radio"/> Auto
VHT Bandwidth	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VHT STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VHT Short GI	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VHT BW Signaling	<input checked="" type="radio"/> Disable <input type="radio"/> Static <input type="radio"/> Dynamic
VHT LDPC	<input type="radio"/> Disable <input checked="" 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 mode
Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed mode
Multiple 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.
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.
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  Disabled: STBC is not employed for signal transmission
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

	Enabled: Multiple frames are acknowledged together using a single Block Acknowledgement frame.
Auto Block Ack	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 38** Wireless security

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		
<b>Wi-Fi Security Settings</b>								
<b>Select SSID</b>								
SSID choice		G902CH-5G-0000B8 ▼						
"G902CH-5G-0000B8"								
Security Mode		WPA-PSK ▼						
<b>WPA</b>								
WPA Algorithms		<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES						
Pass Phrase		*****						
Key Renewal Interval		3600 sec (0 ~ 86400)						
<b>Access Policy</b>								
Policy		Disable ▼						
Add a station MAC		<input type="text"/> ( 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.
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

Select a different encryption mode, the web interface will be different, user can configure the corresponding parameters under the mode you select. Please refer to 4.4.2 section.

## **WMM**

Please refer to 4.4.3 section.

## **WDS**

Please refer to 4.4.4 section.

## **WPS**

Please refer to 4.4.5 section.

## **Station Info**

Please refer to 4.4.6 section.

## **Advanced**

Please refer to 4.4.7 section.

# Security

## Filtering Setting

**Table 54** Filtering Setting

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Admin																														
<div style="display: flex; justify-content: space-between;"> <span>Filtering Setting</span> <span>Content Filtering</span> </div>																																								
<b>Basic Settings</b>																																								
<p><b>Basic Settings</b></p> <p>Filtering <span style="float: right;">Disable ▾</span></p> <p>Default Policy <span style="float: right;">Drop ▾</span></p> <p>The packet that doesn't match any rules would be Drop</p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>																																								
<p><b>IP/Port Filter Settings</b></p> <p>Interface <span style="float: right;">LAN ▾</span></p> <p>MAC Address <span style="float: right;"><input type="text"/></span></p> <p>Dest IP Address <span style="float: right;"><input type="text"/></span></p> <p>Source IP Address <span style="float: right;"><input type="text"/></span></p> <p>Protocol <span style="float: right;">NONE ▾</span></p> <p>Dest. Port Range <span style="float: right;"><input type="text"/> - <input type="text"/></span></p> <p>Src Port Range <span style="float: right;"><input type="text"/> - <input type="text"/></span></p> <p>Action <span style="float: right;">Accept ▾</span></p> <p>Comment <span style="float: right;"><input type="text"/></span></p> <p>( The maximum rule count is 32 )</p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>																																								
<p><b>Current MAC/IP/Port Filtering Rules in the System</b></p> <table border="1"> <thead> <tr> <th>No.</th> <th>Interface</th> <th>MAC Address</th> <th>Dest IP Address</th> <th>Source IP Address</th> <th>Protocol</th> <th>Dest. Port Range</th> <th>Src Port Range</th> <th>Action</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td colspan="10" style="text-align: center;">WAN: Others would be dropped.</td> </tr> <tr> <td colspan="10" style="text-align: center;">LAN: Others would be dropped.</td> </tr> </tbody> </table> <p><input type="button" value="Delete"/> <input type="button" value="Cancel"/></p>											No.	Interface	MAC Address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Comment	WAN: Others would be dropped.										LAN: Others would be dropped.									
No.	Interface	MAC Address	Dest IP Address	Source IP Address	Protocol	Dest. Port Range	Src Port Range	Action	Comment																															
WAN: Others would be dropped.																																								
LAN: Others would be dropped.																																								

Field Name	Description
Filtering	If or not enable filter function
Default Policy	Choose to give up or accept
Mac address	Add the Mac address filtering
Dest IP address	Dest 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 55** Content Filtering

The screenshot shows the 'Security' configuration page for Content Filtering. It includes several sections:
 

- Basic Settings:** Contains 'Filtering' (set to 'Disable') and 'Default Policy' (set to 'Accept').
- Filter List Upload & Download:** Features a 'Local File' section with a file selection button and 'Upload/Download' buttons.
- Web URL Filter Settings:** Shows a table for 'Current Web URL Filters' with columns for 'No.' and 'URL', and 'Delete/Cancel' buttons.
- Add a URL Filter:** Includes a text input for 'URL' and 'Add/Cancel' buttons.

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)
<hr/> <u>Filters</u>	
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

**Table56** advance NAT

Advance Nat		UPnP	IGMP
<b>ALG</b>			
ALG Setting			
FTP	Enable ▼		
SIP	Disable ▼		
H323	Disable ▼		
PPTP	Disable ▼		
L2TP	Disable ▼		
IPSec	Disable ▼		
<input type="button" value="Save &amp; Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>			

### 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 57** UPnP

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Advance Nat		UPnP	IGMP					
<b>UPnP</b>								
UPnP Setting								
Enable UPnP	<input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Enable"/>							

### 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 58** IGMP

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

Save Config File	
Config File Upload && Download	
Local File	<input type="button" value="选择文件"/> 未选择任何文件
<input type="button" value="Upload"/> <input type="button" value="Download"/>	

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	
<b>Password Reset</b>	
User Type	Admin User ▼
New User Name	admin
New Password	<input type="text"/> (The maximum length is 25)
Confirm Password	<input type="text"/>
<b>Language</b>	
Language	English ▼
<b>VPN Access</b>	
Management Using VPN	Disable ▼
<b>Web Access</b>	
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
<b>Telnet Access</b>	
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

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

Primary NTP Server

Secondary NTP Server

NTP synchronization(1 - 1440min)

**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 style="width: 100%;" 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**

Reset to Factory Defaults	Factory Default
---------------------------	-----------------

**Description**

---

Click Factory Default to restore the residential gateway to factory settings

---

## Firmware Upgrade

**Table 69** Firmware upgrade

Status	Network	Wireless	SIP Account	Phone	Administration			
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	
<b>Firmware Management</b>								
<b>Firmware Upgrade</b>								
Local Upgrade <input type="button" value="选择文件"/> 未选择任何文件								
<input type="button" value="Upgrade"/>								

### Description

1. Choose upgrade file type from Image File and Dial Rule
2. Press "Browse.." button to browser file
3. Press  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 Account	Phone	Administration		
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)&

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

---

Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to
Profile Rule	URL of profile provision file

---

**Table 71** Firmware Upgrade

**Firmware Upgrade**

Upgrade Enable

Upgrade Error Retry Delay(sec)

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

Status Network Wireless SIP Account Phone **Administration**

Management Firmware Upgrade Scheduled Tasks Certificates Provision **SNMP** TR-069 Diagnosis

**SNMP Configuration**

**SNMP Configuration**

SNMP Service

Trap Server Address

Read Community Name

Write Community Name

Trap Community

Trap Period Interval (sec)

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

## TR-069

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

### Device Configuration using TR-069

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

**Table 73** TR069

Status	Network	Wireless	SIP Account	Phone	Administration		
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis

**TR-069 Configuration**

**ACS**

TR-069 Enable

CWMP

ACS URL

User Name

Password

Enable Periodic Inform

Periodic Inform Interval

**Connect Request**

User Name

Password

Field Name	Description
<b>ACS parameters</b>	
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
<b>Connect Request parameters</b>	
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

Management
Firmware Upgrade
Scheduled Tasks
Certificates
Provision
SNMP
TR-069
Diagnosis
Operating Mode

**Packet Trace**
Help

Tracking Interface WAN ▾

Packet Trace start stop save

**Ping Test**

Dest IP/Host Name

WAN Interface 1\_MANAGEMENT\_VOICE\_INTERNET\_R\_VID\_ ▾

Apply Cancel

**Traceroute Test**

Dest IP/Host Name

WAN Interface 1\_MANAGEMENT\_VOICE\_INTERNET\_R\_VID\_ ▾

Apply Cancel

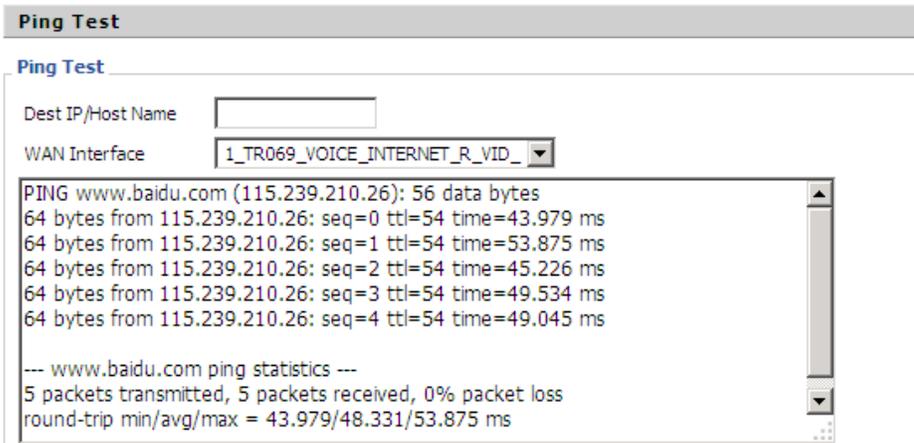
### Description

#### 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.



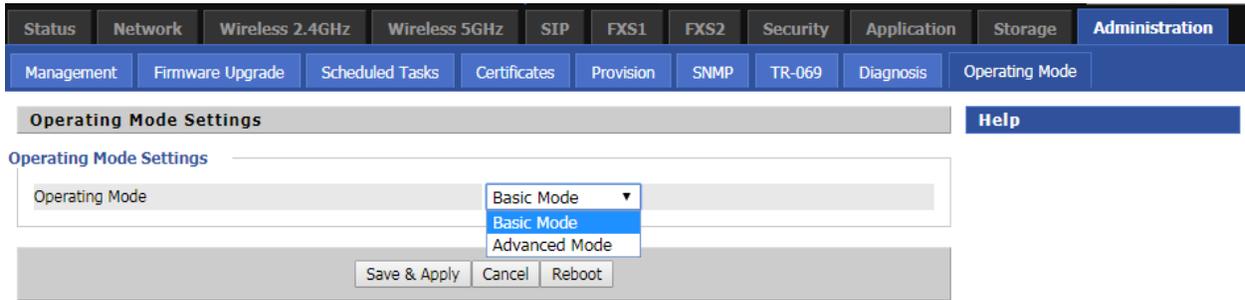
#### 3. Traceroute Test

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



# Operating Mode

**Table 75** Operating mode



### 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     DHCPv6Server[DHCPv6Server] --- Device[Device(FWR9601/FWR92)]     Device --- PC[PC]     Device --- Router[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

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	DDNS	QoS
Routing	Advance									

---

**IPv6 Advanced Settings**

IPv6 Enable Enable ▼

## Configuring IPv6

### Configuring Statefull IPv6

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

**Table 80** Configuring Statefull IPv6

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	DDNS	QoS
Routing	Advance									

---

**IPv6 WAN Setting**

IPv6 WAN Setting

Connection Type DHCPv6 ▼

DHCPv6 Address Settings Statefull ▼

Prefix Delegation Enable ▼

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

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 side 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	<b>Network</b>	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	DDNS	QoS
Routing	Advance									

<b>IPv6 LAN Setting</b>	
-------------------------	--

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

<input type="button" value="Save &amp; 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

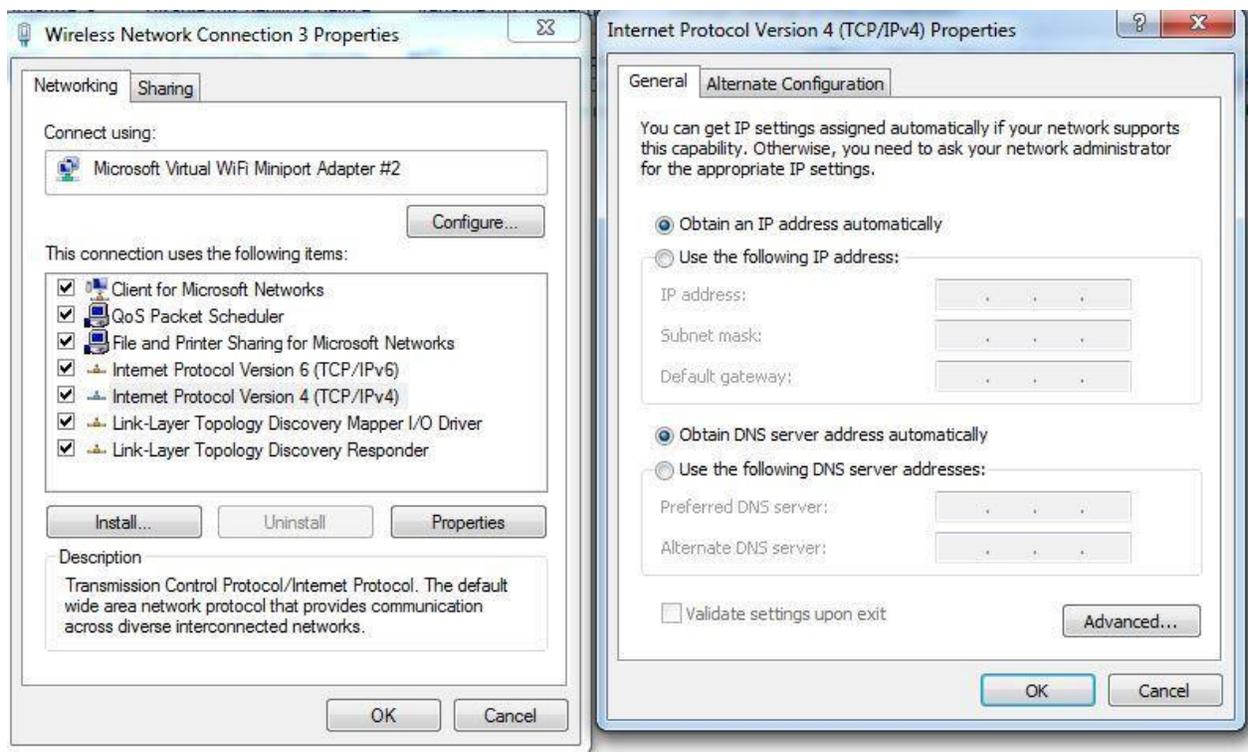
Follow the below process to set your PC to get an IP address automatically:

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.