PHICOMM

((· YOUR PORTAL TO SMART LIFE ·))

FIR151B/300B/302B/303B

Wireless Router

User Manual

Contents

LEGAL INFORMATION ABOUT INTELLECTUAL PROPERTY

All company, product and service names mentioned herein are trademarks, registered trademarks or service marks of their respective owners. Shanghai Feixun Communication Co., Ltd. reserves the right to revise the content of this document at any time without prior notice. No part of this document may be reproduced or transmitted in any form or by any means, electronical or mechanical, including photo-copying, recording or storing in a retrieval system, or translated into any language in any form without prior written permission of Shanghai Feixun Communication Co., Ltd.

DISCLAIMER

Any pre-installed software or data provided as a bundle to this device is subject to the applicable law under the responsibility of the issuing software / service provider. The hardware manufacturer cannot be held liable for any breach, malfunction or other occurrence raised by using this third-party software. Only the issuing providers can lawfully be held responsible. Shanghai Feixun Communication Co., Ltd. does not own the intellectual property of the third-party software and applications that are delivered with this product. Therefore, Shanghai Feixun Communication Co., Ltd. will not provide any warranty of any kind for these third-party software and applications. Neither will Shanghai Feixun Communication Co., Ltd. provide support to customers who use these third-party software and applications nor be responsilbe or liable for the functions of these third-party software and applications. Third-party software and applications services may be interrupted or terminated at any time. Shanghai Feixun Communication Co., Ltd. does not guarantee that any content or service would be maintained for any period during its availability. Third-party service providers provide content and services through network or transmission tools outside of the control of Shanghai Feixun Communication Co., Ltd. to the greatest extent permitted by applicable law, it is explicitly stated that Shanghai Feixun Communication Co., Ltd. shall not compensate or be liable for services provided by third-party service providers or the interruption or termination of third-party contents or services. Shanghai Feixun Communication Co., Ltd. Shall be not responsible for the legality, quality or any other aspects of any software installed on this product, or for any uploaded or downloadad third-party works, such as texts, images, videos or software. Customers shall bear the risk for any and all effects including incompatibility between the software and this product, which result from installing software or uploading or downloading the third-party works.

LIMITATION OF DAMAGES

To the maximum extent permitted by applicable law, in no event shall Shanghai Feixun Communication Co., Ltd. be liable for any special incidental, indirect or consequential damages or lost profits, business, revenue, data, goodwill or anticipated savings. The maximum liability (this limitaion shall not apply to liability for personal injury to the extent applicable law prohibits such a limitation) of Shanghai Feixun Communication Co., Ltd. arising from the use of the product described in this document shall be limited to the amount paid by customers for the purchase of this product.

IMPORTANT HEALTH INFORMATION AND SAFETY PRECAUTIONS

When using this product, the safety precautions below must be taken to avoid possible legal liabilities and damages. Retain and follow all product safety and operating instructions. Observe all warnings in the operating instructions on the product.
To reduce the risk of bodily injury, electric shock, fire and damage to the equipment, observes the following precautions.

SAFETY PRECAUTIONS FOR PROPER INSTALLATION

CAUTION: Connecting to a weaker inappropriate charger can result in an electric shock to your device.

SAFETY PRECAUTIONS FOR PROPER SUPPLY UNIT

Use the correct power source!
This product can only be charged with matching standard external power source appointed by Shanghai Feixun Communication Co., Ltd.
Shanghai Feixun Communication Co., Ltd. is not liable for any device breakdown or safety accident arising from the use of unauthorized external power source.

PRECAUTION OF HEARING LOSS

GENERAL WARNING: **To prevent possible hearing damage, do not listen at high volume levels for long periods.**

Permanent hearing loss may occur if the receiver, headphones, speakerphone or earpieces are used at high volume. Use only compatible receivers, headphones, speakerphones or earpieces with your device. Turn on the audio and check the volume before inserting anything in your ear. You can adapt over time to a higher volume of sound that may sound normal but can be damaging to your hearing. If you experience ringing in your ears or muffled speech, stop listening and check your hearing. The louder the volume, the less time is required before your hearing could be affected.

Hearing experts suggest that to protect your hearing:

- Limit the amount of time you use receiver, headphones, speakerphone or earpieces at high volume.
- Avoid turning up the volume to block out noisy surroundings.
- Turn the volume down if you cannot hear people speaking near you.

SAFETY PRECAUTION FOR DIRECT SUNLIGHT

Keep this product away from excessive moisture and extreme temperatures. The device is designed to be operated in temperatures between 0°C and 40°C. Low- or high-temperature conditions might cause the device to temporarily stop working properly. Do not leave the product in a vehicle or in places where the temperature may exceed 70°C (window sill or behind glass). Avoid dramatic changes in temperature or humidity when using the device as condensation may form on or within the device.

When you are using the device, it is normal for the device to get warm. The exterior of the device functions as a cooling surface that transfers heat from inside the unit to the cooler air outside.

ENVIRONMENT RESTRICTIONS

Do not use this product in gas stations, fuel depots, chemical plants or where blasting operations are in process, or in potentially explosive atmospheres such as below deck on boats, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as grain, dust or metal powders. Please be aware that sparks in such areas could cause an explosion or fire resulting in bodily injury or even death.

EXPLOSIVE ATMOSPHERES

In any area with a potentially explosive atmosphere or where flammable materials exist, the product should be turned off and the user should obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Users are advised not to use the equipment at refueling areas such as service or gas stations, and are reminded of the need to observe restrictions on the use or radio equipment in fuel depots, chemical plants or where blasting operations are in progress. Areas with a potentially explosive atmosphere are often, but not always, clearly marked. These include fueling areas, below deck on boats, fuel or chemical transfer or storage facilities, and areas where the air contains chemicals or particles, such as dust or metal powders.

SAFETY PRECAUTIONS FOR RADIO FREQUENCY EXPOSURE

- Avoid using your device near metal structures (e. g. the steel frame of a building).
- Avoid using the device near strong electromagnetic sources, such as microwave ovens, sound speakers, TV and radio.
- Use only original manufacturer-approved accessories.
- Use of non-original manufacturer-approved accessories may violate your local RF exposure guidelines and should be avoided.

INTERFERENCES WITH MEDICAL EQUIPMENT FUNCTIONS

This product may cause medical equipment to malfunction. The use of this device is forbidden in most hospitals and medical clinics.

If you use any other personal medical device, consult the manufacturer of your device to determine if they are adequately shielded from external RF energy.

HEARING AID DEVICES

Some devices may interfere with some hearing aid devices. In the event of such interference, you may want to consult your service provider, or call customer service line to discuss alternatives.

NON-IONIZING RADIATION

Your device has external antennas. This product should be operated in its normal-use position to ensure the radiative performance and safety of the interference. Users are advised that for satisfactory operation of the equipment and for the safety of personnel, it is recommended that no part of the human body be allowed to come too close to the antenna during operation of the equipment.

Use only the supplied antennas. Use of unauthorized or modified antennas may impair transfer quality and damage the device, causing loss of performance and SAR levels exceeding the recommended limits as well as result in noncompliance with local regulatory requirements in your country.

To assure optimal device performance and ensure human exposure to RF energy is within the guidelines set forth in the relevant standards, always use your device only its normal-use position. Contact with the antennas may impair quality and cause your device to operate at a higher power level than needed. Avoiding contact with the antenna area when the device is in use optimizes the antenna performance.

GENERAL PRECAUTIONS

AVOID APPLYING EXCESSIVE PRESSURE TO THE DEVICE

Do not apply excessive pressure on the device to prevent damaging them.

DEVICE IS GETTING WARM AFTER PROLONGED USE

When using your device for prolonged periods the device may become warm. In most cases this condition is normal and therefore should not be interpreted as a problem with the device.

HEED SERVICE MARKING

Except as explained in the user manual, do not repair any product yourself. Service needed on components inside the device should be done by an authorized service outlet or provider.

PHICOMM is entitled to use new or reconditioned replacements parts or boards for repairs under warranty, provided they have the same functionality as the parts to be replaced.

DAMAGE REQUIRING SERVICE

Unplug the device from the electrical outlet and refer servicing to an authorized service center or provider under the following conditions:

- Liquid has been spilled or an object has fallen onto the product.
- The product has to been exposed to rain or water.
- There are noticeable signs of overheating.
- The product does not operate normally when you follow the operating instructions.

AVOID HOT AREAS

The product should be placed away from heat sources such as radiators, heat registers, stoves, or other products (including amplifiers) that products heat.

AVOID HOT AREAS

Never use the product in a wet location.

AVOID USING YOUR DEVICE AFTER A DRAMATIC CHANGE IN TEMPERATURE

When you move your device between environments with very different temperature and/or humidity ranges, condensation may form on or within the device. To avoid damaging the device, allow sufficient time for the moisture to evaporate before using the device.

NOTICE: When taking the device from low-temperature conditions into a warmer environment or from high-temperature conditions into a cooler environment, allow the device to acclimate to room temperature before turning on power.

AVOID PUSHING OBJECTS INTO THE DEVICE

Never push objects of any kind into cabinet slots or other openings in the product. Slots and openings are provided for ventilation. These openings must not be blocked or covered.

MOUNTING ACCESSORIES

Do not use the product on an unstable table, cart, tripod or bracket. Any mounting of the product should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.

AVOID UNSTABLE MOUNTING

Do not place the product with an unstable base.

USE PRODUCT WITH APPROVED EQUIPMENT

This product should be used only with personal computers and options identified as suitable for use with your equipment.

CLEANING

Unplug the product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning, but NEVER use water to clean the device.

The device has been provided with special treatments featuring that it could dispose dirt and sweat on its surface. The device itself does not have a stain-resistant function. In case of smudginess and dyeing, please wipe it with clean damp sponge immediately. Please keep the device dry when necessary.

PACEMAKER

The device may cause disturbance to pacemakers. Please keep the device a proper distance of least 5 centimeters away from pacemakers.

If you need detailed information about other active implantable medical devices, please consult your doctor to ensure the magnetic interference of such active implantable medical devices.

CAUTION

Update your operating system with caution.

- Improper operation or unforeseen external factors may cause an operating system update fails; the device will not work properly. If such a situation occurs, you need to send the unit in for repair.
- An unofficial operating system can cause security risks. Please install only official updates provided by Phicomm, if not you will void the warranty and a repair is chargeable.

SW-Update

- During the update process all user data will be erased. Please backup your data before.

Package contents

Please check the package content before the installation of the router:
1x Wireless Router
1x power supply unit
1x RJ45 cable
1x quick start guide
GPL license and CE declaration

Summary of changes

Issue	Issue date	Remarks
1	September 2014	Initial release

1. About the user manual

This user manual includes a complete overview of the configuration and functions of PHICOMM routers of the FIR series.

1.1 Structure of the user manual

The document is structured as follows:

Chapter	Title	Subject
1	About the user manual	Basic description of document content, definition of symbols and conventions
2	Introduction	Description of basic functions
3	Hardware connections	Description of the way connecting the router with other hardware
4	Wireless router configurations	Description of the router configuration
5	Troubleshooting	FAQs and solutions
6	Technical support – contact us	

1.2 Used symbols and fonts

The following symbols are used in the user manual:

DANGER! WARNING!
May result in personal injury

Note
Useful additional information

The following editorial conventions are used in the manual:

Convention	Explanation
Bold	Field names / button names are written in bold Example: click menu **View**
Italic	Commands, screen output, file names and paths are written in *Italic*. Example: Input *192.168.0.1* in **IP address** text box.
<...>	<...> keyboard or actual names are represented in angle brackets Example: Click <Ctrl> + <Alt> + <Delete> to open the task manager.
>	Used for menu sequence Example: Click **File > Print** to print.

1.3 standard compliances (CE, FCC)

Declaration of Conformity

For CE marking in the EU (European Union)

Shanghai Feixun Communication Co., Ltd.

No.3666, Sixian Rd., Songjiang District, Shanghai, P.R.China

We declare under our sole responsibility that our products

Product Name: Wireless Router

Model: FIR151B, FIR300B, FIR302B, FIR303B

to which this declaration relates are in conformity with the following normative European and international standards:

Safety

- ✓ EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
- ✓ EN 62311:2008

EMC

- ✓ EN 301 489-1 V1.9.2(2011-09)
- ✓ EN 301 489-17 V2.2.1(2012-09)
- ✓ EN 55022:2010
- ✓ EN 61000-3-2:2006+A1:2009+A2:2009
- ✓ EN 61000-3-3:2008
- ✓ EN 55024:2010

Radio Spectrum

- ✓ EN 300 328 V1.7.1(2006-10)

By conformance with the standards referenced our products follow the provisions of the directives listed below.

- ✓ R&TTE Directive 1999/5/EC
- ✓ EMC Directive 2004/108/EC
- ✓ Low Voltage Directive 2006/95/EC

Date: July 8, 2014

Jie Hu

Manager for Product Certification

FCC STATEMENT

This device has been tested and complies with Part 15 of the FCC Rules for Class B. These regulations are intended to protect against adverse effects of device operation in a home environment.

The operation of a device under FCC regulations Part 15 is subject to the following two conditions:

- The device may not cause harmful interference.
- This device must accept any interference, including all those that cause undesirable behavior.

This router generates and uses radio signals and therefore may interfere with radio communications if not installed. However, there can be no guarantee that interference will not occur. If a communication fault can occur, which can be tested by simply switching off and on the device, you should perform the following actions:

- Realign antennas
- Increase distance of the router to radio or television
- Use router with a different circuit than the radio or TV operate
- Contact dealer or manufacturer

Any use not expressly approved by PHICOMM changes to the device will invalidate the guarantee.

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This router and its antenna / antennas must not be operated in the immediate vicinity of other radio wave emitting devices / antennas. The antennas used for this router must be at least 20 cm away from people.

2. Introduction

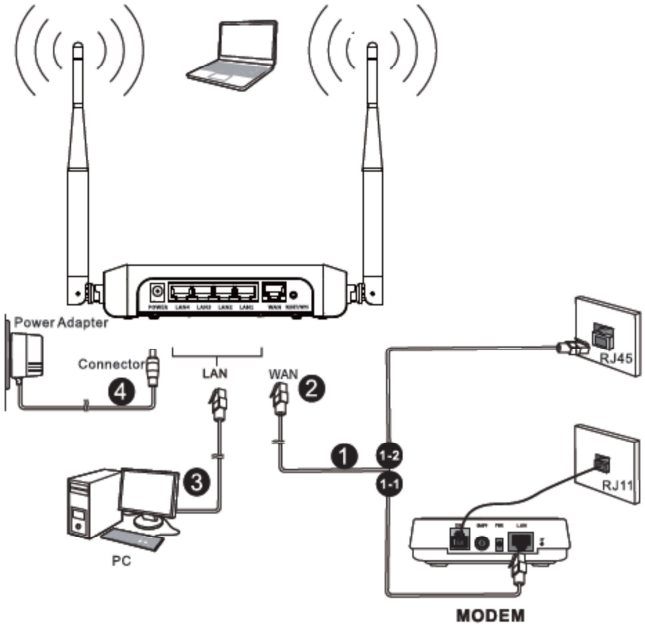
The routers of the FIR series are all-in-one router for home and SOHO users to share broadband internet connection over a wired or a wireless network.
The speed of up to 300 Mbps (FIR151B up to 150 Mbps) provides users with extraordinary smooth internet surfing, internet phone calling and online gaming.
By adopting external Omni-directional antenna(s), the product greatly increases the wireless range and sensitivity, which enables to receive wireless signals in any corner of your home or your office.

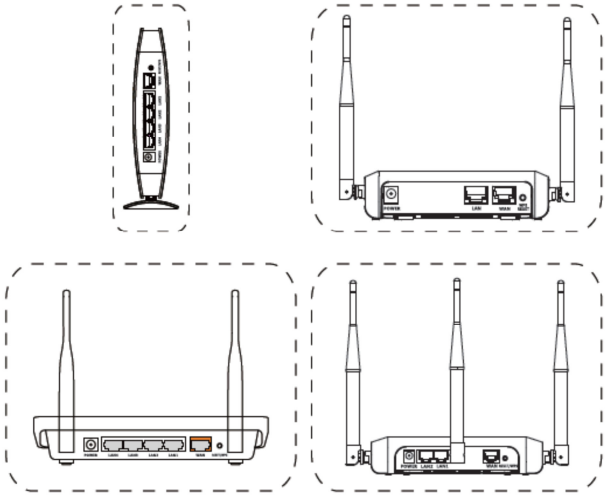
The routers of the FIR series support the following features:

- speed up to 300 Mbps (FIR151B up to 150Mbps)
- backward compatible with 802.11b/g products
- health and power saving allows parents or administrators to establish restricted access policies for children or staff
- WPS button allows easy ON/OFF of the internet connection
- bandwidth control allows administrators to control the bandwidth for each PC

3. Hardware connections

To establish a connection using a modem, please follow the steps 1-1 to 4 of the chart below.
If you use an Ethernet cable, please connect RJ with the WAN port directly (steps 1-2 to 4)





Note

The connections might vary by models**.**

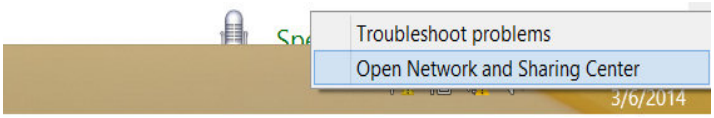
4. Wireless router configurations

This section gives instructions of the procedures that must be performed to enable the wireless router.
After completion of the third point the router is connected with the internet. Please select the corresponding internet connection on your PC and click **connect**.

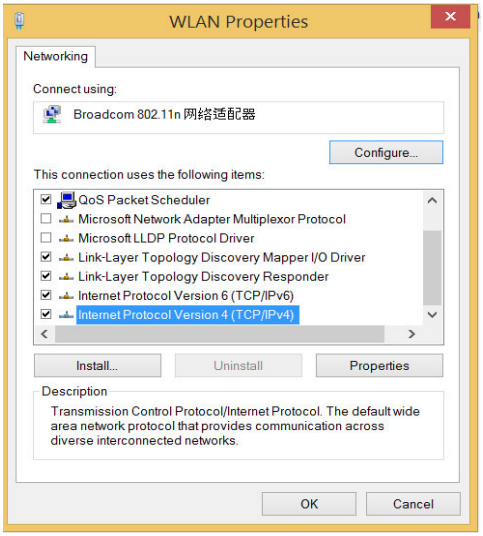
4.1 TCP/IP settings

The IP address has to be obtained automatically before starting the configuration of the router. Please follow these steps:

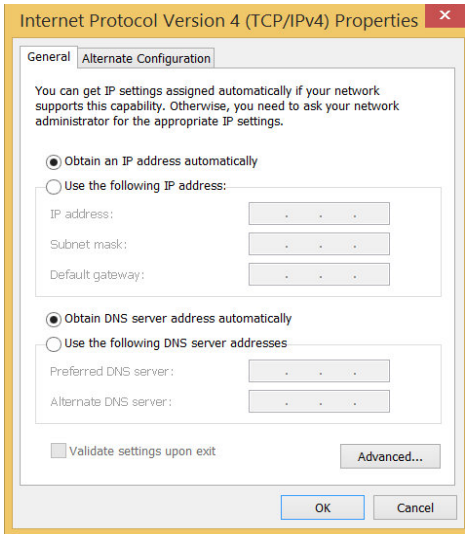
1. With the right mouse button please click on the right bottom corner. Click **Open Network and Sharing Center** and select **Change adapter settings** on the upper left of the screen.



2. Select network connection type and open the **Properties**. In the **Properties** window please double click **Internet Protocol Version 4 (TCP/IPv4)**.

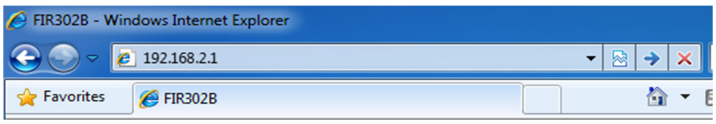


3. Select both **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to confirm the configuration.

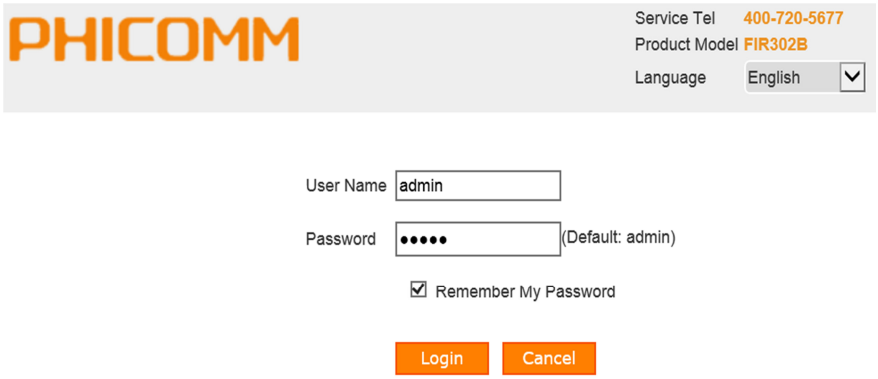


4.2 Router configurations

Open the web browser and enter *192.168.2.1* in the address bar.



Enter **Username** and **Password** (preset as *admin/admin*). You can find this information also at the bottom of the label on your router. Select the languages on the right side. Then click the **Login** button.

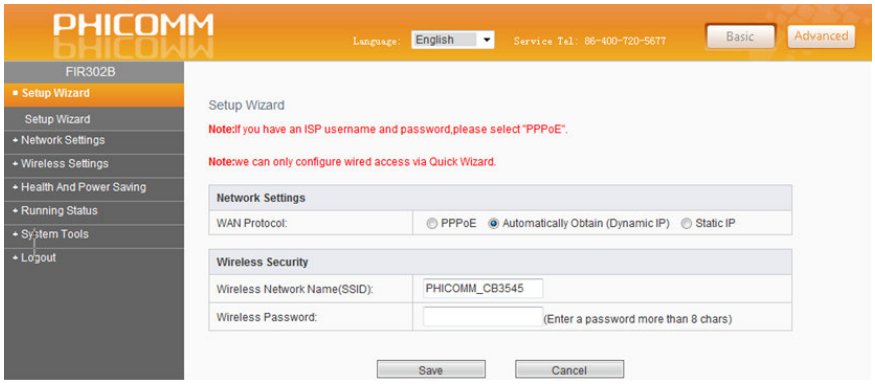


After successful login, you will see the page of the Setup Wizard. Enter the needed settings or click **Cancel** to leave this page (to see the web management page).
You can find the **Setup Wizard** in menu on the left. A small **HELP** button is on the right side to provide comprehensive instructions.

To confirm the settings on all pages please click **Save**. By clicking **Cancel** you always will return to the former page.

4.2.1 Setup Wizard

The setup wizard simplifies installation and configuration steps.



Menu item	Explanation
Network Settings	
WAN protocol	**PPPoE** PPPoE is typically used for DSL services. Select PPPoE and type in the **Username** and **Password** provided by your internet service provider. Then click the **Save** button. **Dynamic IP (automatically obtain)** Select **Automatically obtain (Dynamic IP)** if internet service provider does not provide any IP to use. This option is commonly used for cable modem services. Router will obtain IP address information automatically. Click **Save** button. **Static IP address** Select **Static IP** if internet service provider provides the static IP address, subnet mask, default gateway and DNS server address. Type in those information and click the **Save** button.
Wireless Security	
Wireless network name (SSID)	Define SSID to any other name you prefer or keep it unchanged.

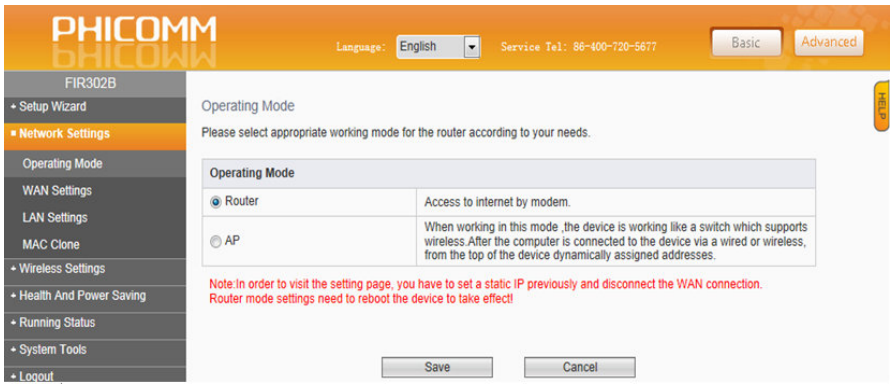
Menu item	Explanation
Wireless password	Set a wireless password (more than 8 characters) to prevent others from accessing your network without permission.

Note

The SSID should be changed and no longer match with the name specified by the manufacturer. Please create an anonymous one as possible SSID, which does not allow any conclusions about the location of the router.

4.2.2 Network Settings

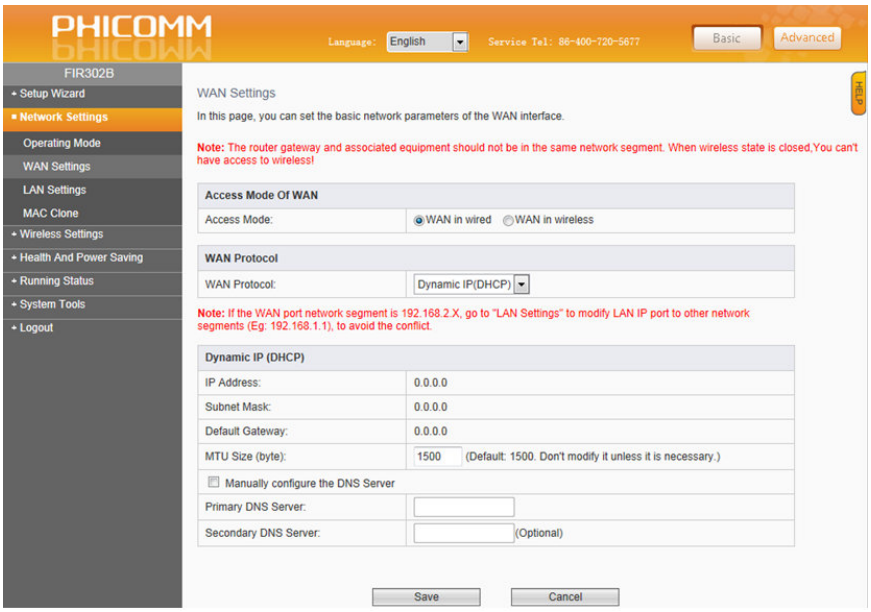
Operating mode



Select **Router** or **AP** button for operation mode.

Menu item	Explanation
Router	This is the default and the most commonly used wireless operating mode. The router connects wired or wireless with the network / internet.
AP	The router acts as a central connection point, which wireless clients can connect to.

WAN settings

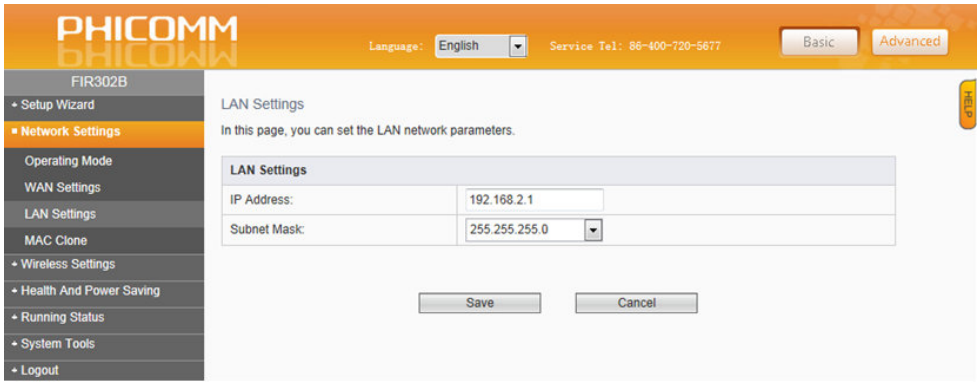


Select **Access Mode Of WAN** and **WAN Protocol** on **WAN Settings page**. If your internet service provider is running on a DHCP server, select **Dynamic IP** as connection type. The router will automatically get IP parameters from your internet service provider.

Note

If the WAN port network segment is 192.168.2.X, go to **LAN Settings** page to modify LAN IP port to other network segments (for example 192.168.2.1) to avoid conflicts.

LAN Settings

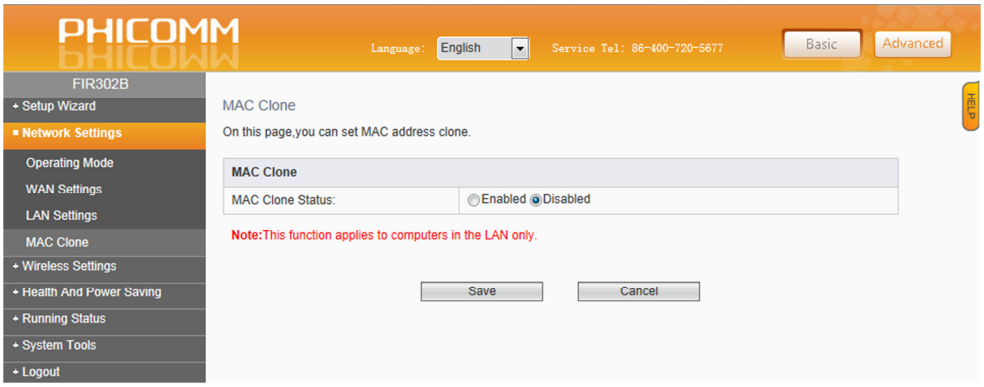


Menu item	Explanation
IP address	Enter LAN IP address of the router.
Subnet Mask	Enter the subnet mask associated with the LAN IP address.

Note

If you change the LAN IP address of the router, log in the web management page with the new IP address.

MAC Clone



Some internet service providers require the registration of your computer's MAC address. If you want to clone the MAC address select **Enabled**.

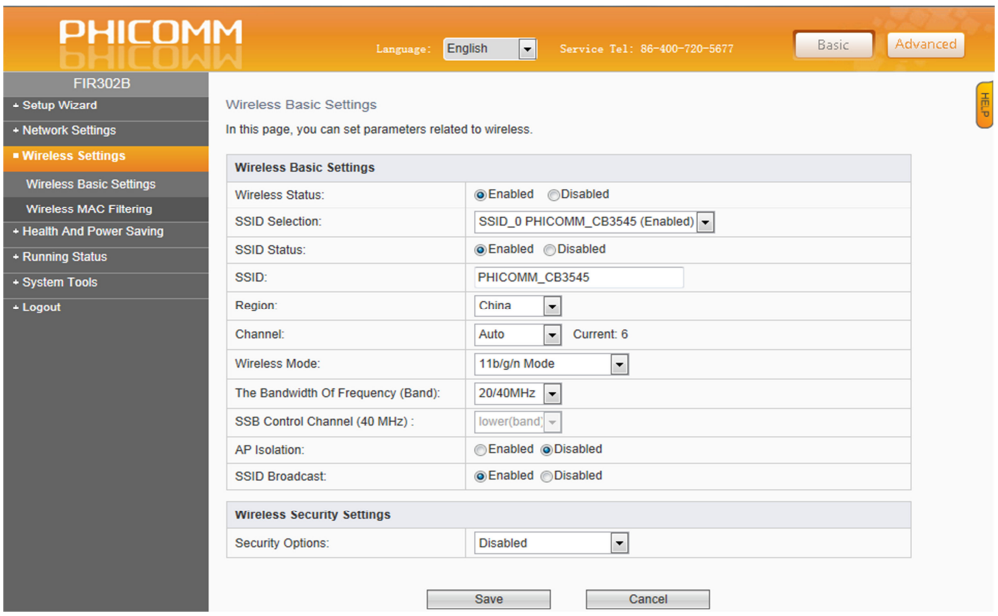
4.2.3 Wireless Settings

There are two submenus under the **Wireless Settings** menu:

- Wireless Basic Settings
- Wireless MAC Filtering

Click any of them to configure the corresponding function.

Wireless Basic Settings



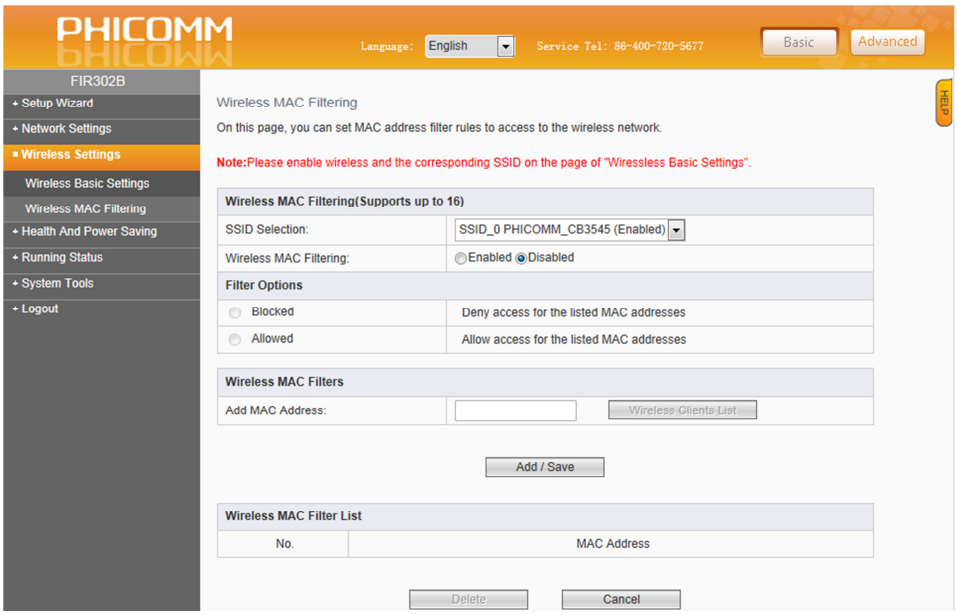
Menu item	Explanation
Wireless Basic Settings	
Wireless Status	Select **Enabled** or **Disabled** to control the wireless function of the router.
SSID	Name of the wireless network
Wireless Mode	If all wireless devices connected with the wireless router are in the same transmission mode (for example 802.22b), select **11b Mode**. If the devices use different transmission modes, select **11b/g/n Mode**.
SSID Broadcast	If you choose **Enabled**, the wireless router will broadcast the SSID name.

Menu item	Explanation
Wireless Security Settings	
Security Options	Disabled
	WEP: Wired Equivalent Privacy
	WPA-PSK: Pre-Shared Key of WPA
	WPA2-PSK: Pre-Shared Key of WPA2
	WPA/WPA2-PSK: automatically based on the wireless stations' capacity and request

Note

The security modes are different in the kind of encryption.
WEP encryption provides the least protection while WPA2-PSK is to overcome the most difficult and therefore offers the best protection.

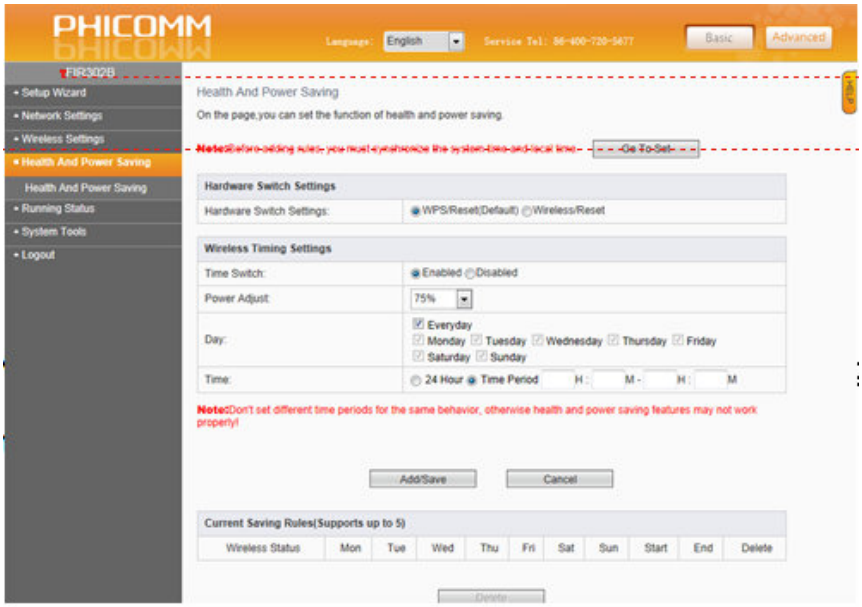
Wireless MAC Filtering



Enter the MAC address. Set to block or allow the PC(s) to connect with the wireless router. To set MAC addresses proceed as follows:

1. Select **Enabled** under **Wireless MAC Filtering**.
2. Select **Blocked** or **Allowed** under Filter Options.
3. Fill *00:0A:EB:00:07:5F* in **Add MAC Address**.
4. Click **Add/Save** button.

4.2.4 Health and Power Saving



Set to turn on/off the wireless router according to your actual needs (for example rest times or limit surfing time for children). You can also turn off the power of the wireless router to save power and protect the environment at the same time.

Note
In order the router is working properly, the router time must be synchronized with the internet time.

If the router time is different from the internet time, proceed as follows to synchronize: Click **Set at once** > **synchronize with PC**

Now you can configure the time settings:

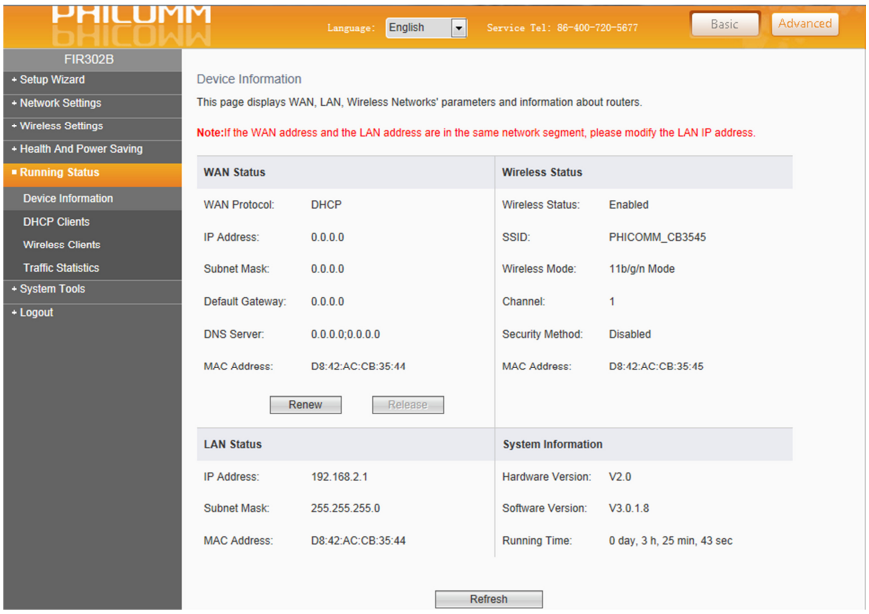
1. Select **WIFI/Reset Combination** under **Hardware Switch Settings**.
2. Select **Enabled** (default) under **Time Switch** and adjust the RF power in **Power Adjust** according to your demand.

Note
It will impact the performance and the coverage of the wireless.

3. Set time **in Time Settings (day, week)** and **Time Settings (hour)** separately.

4.2.5 Running status

Device Information

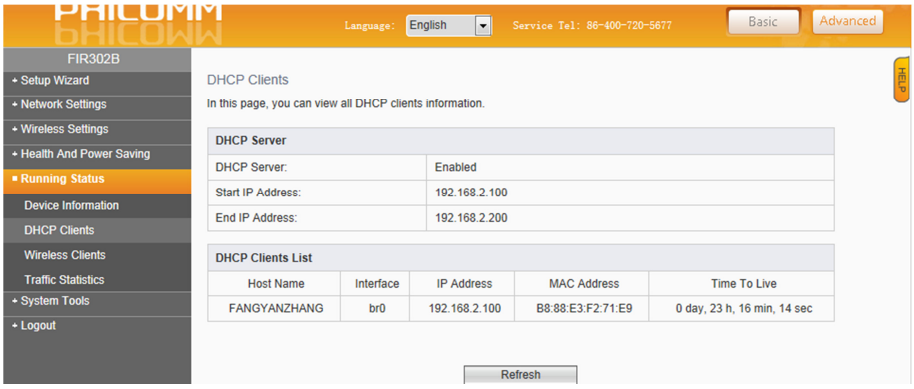


This page displays WAN, LAN, Wireless network's parameters and information about the router.

There are IP addresses, subnet masks, default gateways, SSID, hardware- and software-versions etc.

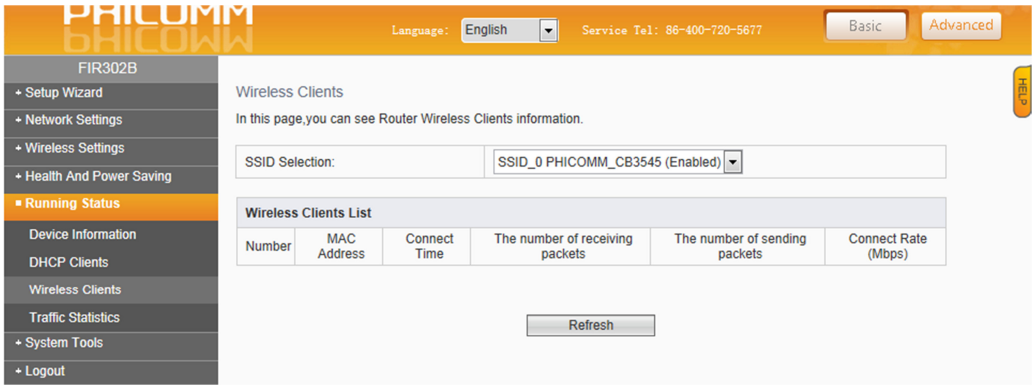
Press **Refresh** button to refresh the **Device Information** list.

DHCP Clients



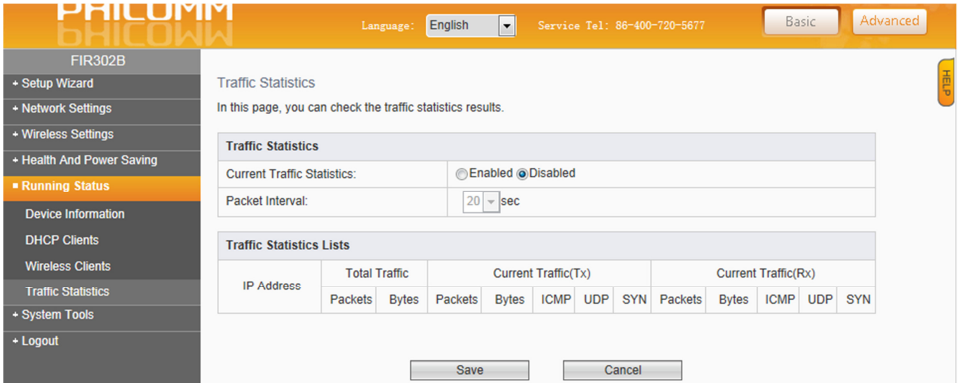
Menu item	Explanation
DHCP Clients	
DHCP-Server	DHCP server configures the TCP/IP protocol for each PC in the LAN automatically.
Start IP address	1st address in the IP address pool
End IP address	Last address in the IP address pool
DHCP Clients List	
Refresh	Click the button to refresh the DHCP clients list

Wireless Clients



Click **Refresh** button to check the wireless clients.

Traffic Statistics

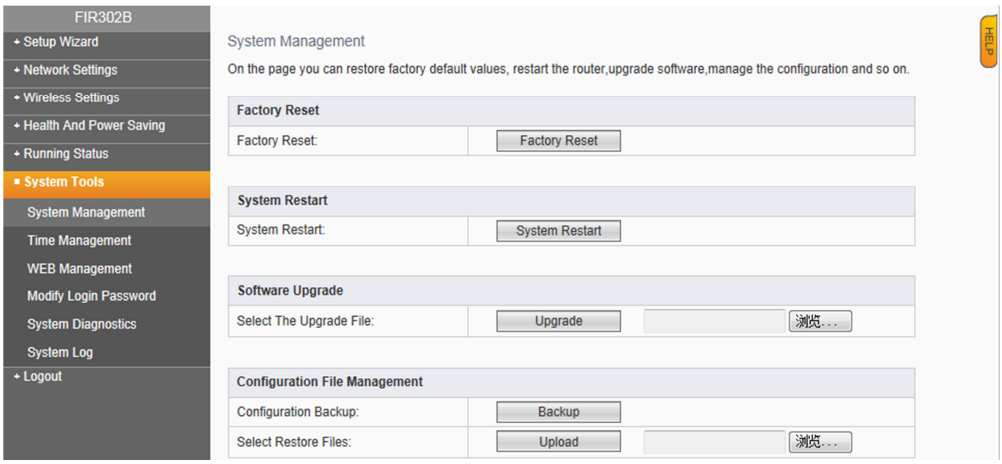


Check the traffic statistic results and the packet intervals.

4.2.6 System Tools

Check out different administration tools: **System Management**, **Time Management**, **WEB Management**, **Modify Login Password**, **System Diagnostics** and **System Log**.

System Management

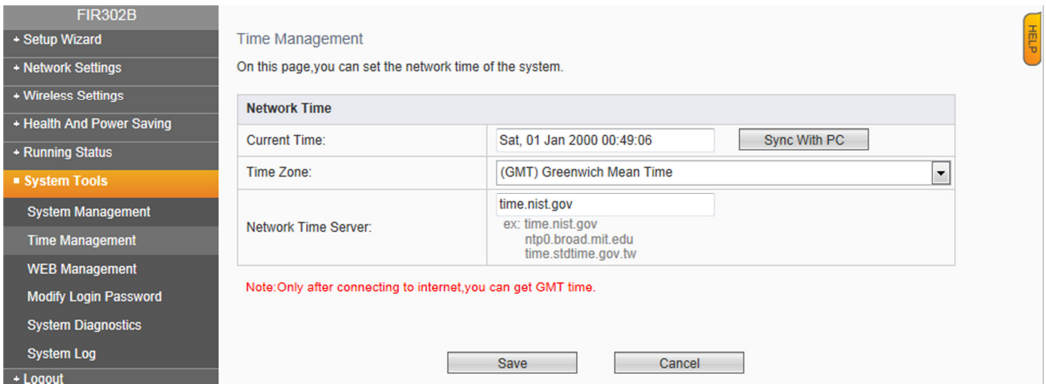


Menu item	Explanation
Factory Reset	Restore factory default values
System Restart	Restart the router
Software Upgrade	Update software
Configuration File Management	Backup and restore the configuration

Note

All user settings will be deleted when factory reset is enabled.

Time Management

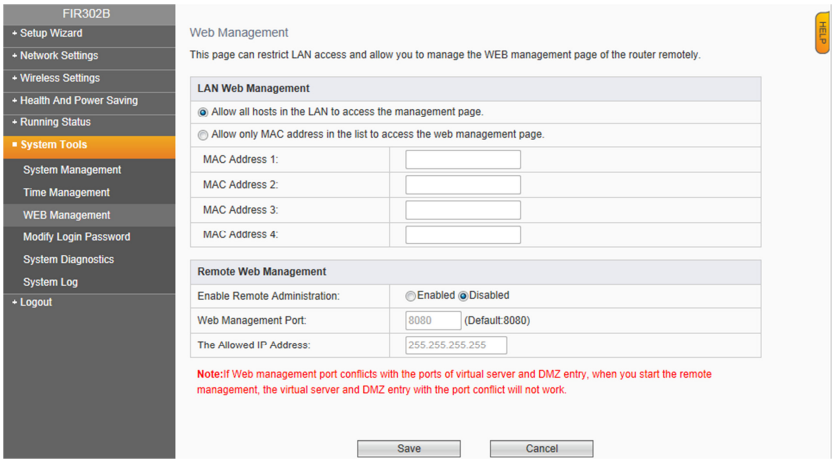


Set the network time of your system or click **Sync with PC** to synchronize with the computer.

Note

You can get GMT time after connecting with the internet.

Web Management

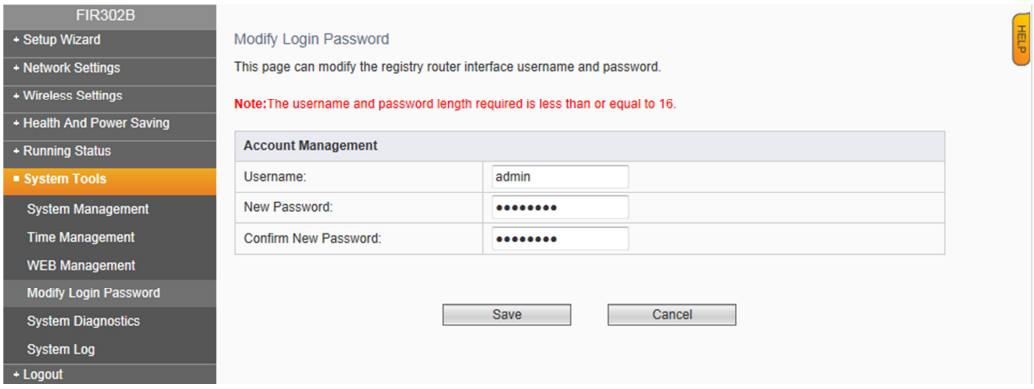


Menu item	Explanation
LAN Web Management	Restricts LAN access and only allows MAC addresses in the list to access the Web Management page
Remote Web Management	Allows the remote management of the router

Note

If the web management port conflicts with the ports of virtual server and DMZ entry, when you start the remote management, the virtual server and DMZ entry will not work.

Modify Login Password

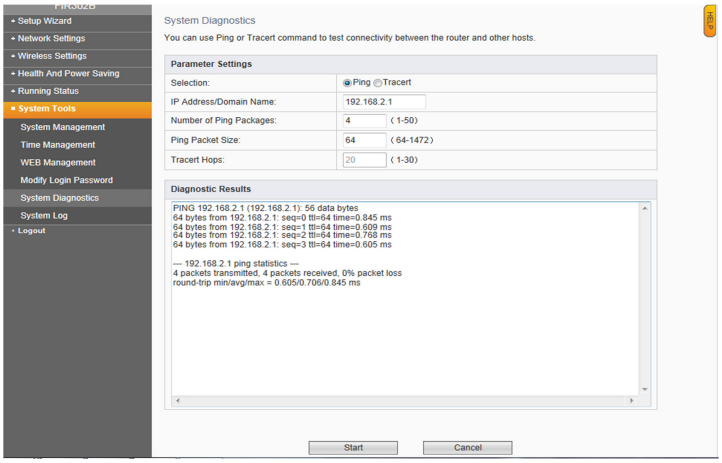


Manage the details of your account and modify username and password.

Note

Username and password lengths are less than or equal to 16 characters.

System Diagnostics

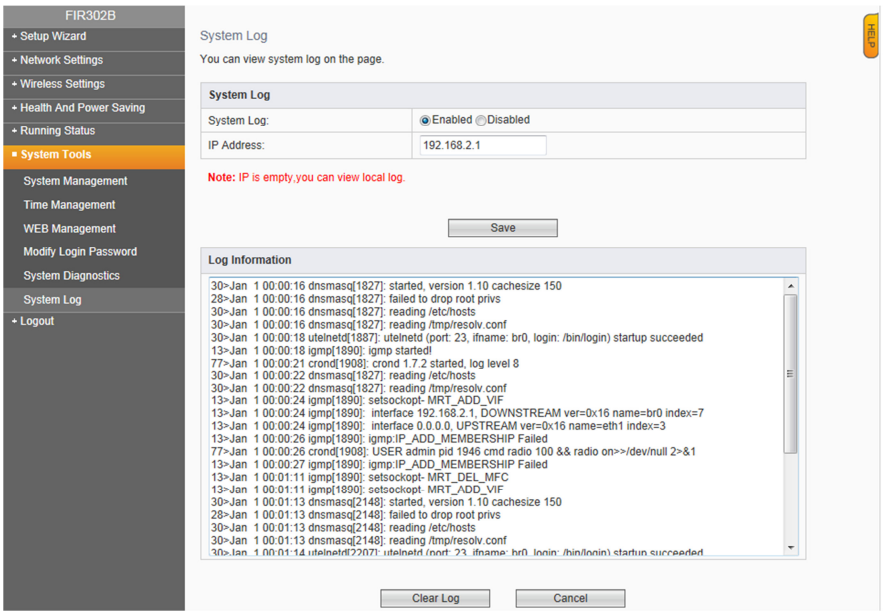


Ping or Tracert commands to test connectivity between router and other hosts. Please proceed as follows:

- Select **Ping**.
- Enter **IP Address** / **Domain Name**.
- Enter **Number of Ping Packages**, **Ping Packet Size** and **Tracert Hops**.
- Click **Start**.

You will see the results in **Diagnostic Results**.

System Log



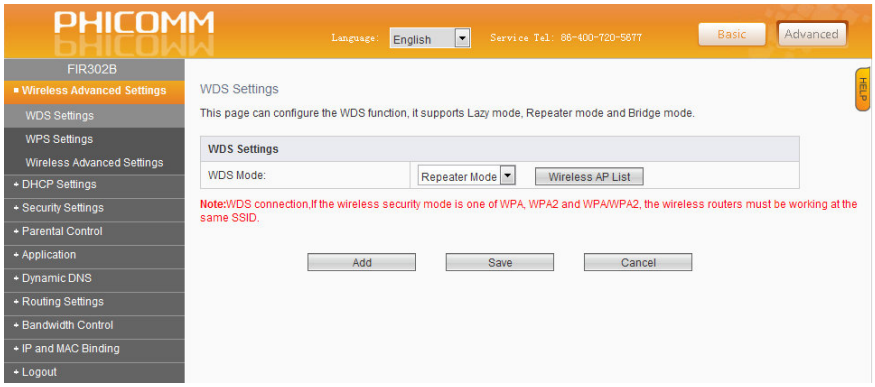
If you want to set more detailed settings, select **Advanced** beside the **Basic** button at the top of the screen.

4.2.7 Wireless Advanced Settings

There are **WDS Settings**, **WPS Settings** and **Wireless Advanced Settings**.

WDS Settings

The WDS function can help you to extend the wireless range. It supports Lazy Mode, Repeater Mode und Bridge Mode.



Menu item	Explanation
WDS Mode	
Lazy Mode	In this mode no further configurations are needed. Click **Save** and the connecting client should be in **Repeater Mode** or **Bridge Mode**.
Bridge Mode	In this mode you can connect two or more wired devices wirelessly. You need to add the wireless MAC address of the connected device into the routers AP MAC address table or select one from the scanning table. At the same time the connected device should be in **Lazy**, **Repeater** or **Bridge Mode**.
Repeater Mode	You can select this mode to extend the distance between two WLAN devices. It operates as WDS repeater and connects to both – client card as AP and another AP. In typical repeater applications APs with WDS function connect to other APs, which have to support WDS too. In this mode you need to add the MAC address of the connected device into the routers AP MAC address table. The connected client should be in **Lazy**, **Repeater** or **Bridge Mode**.

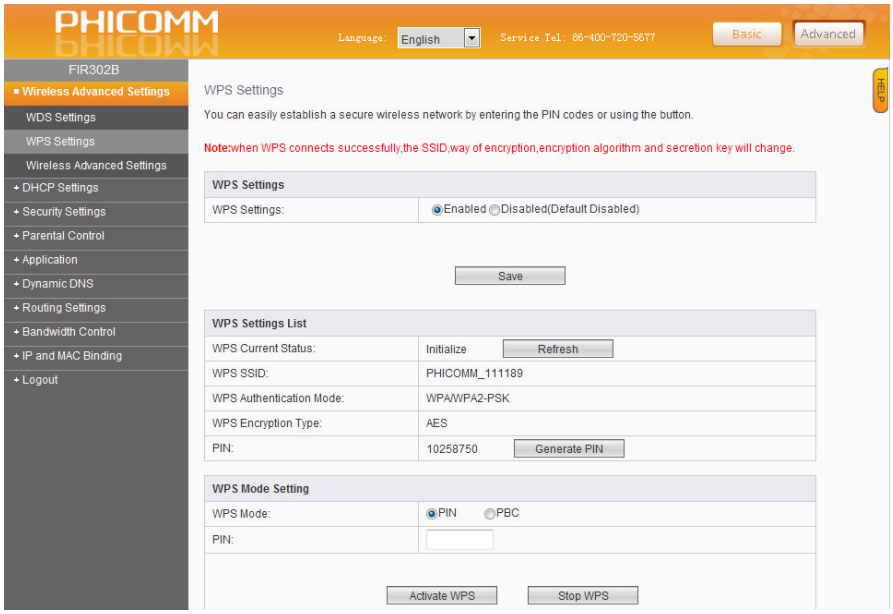
Input the MAC address of the other wireless router in **MAC address of the wireless access point**.

Note

Two wireless routers must use the same channel, encryption type and encryption key. If the wireless security mode is one of WPA, WPA2 and WPA/WPA2, the wireless routers must work with the same SSID.

WPS settings

The WPS function can help to add a new device to the network quickly. If the client device supports WPS and is equipped with a WPS button, you can add it to the network by pressing the WPS button on the device and then press the button of the router two minutes. The status LED on the router becomes green after five minutes, if the device has been added to the network successfully. If your client asks for the router's PIN number, enter this PIN number into your client device. If your client device has a WPS Settings PIN number, enter that number into the PIN box.



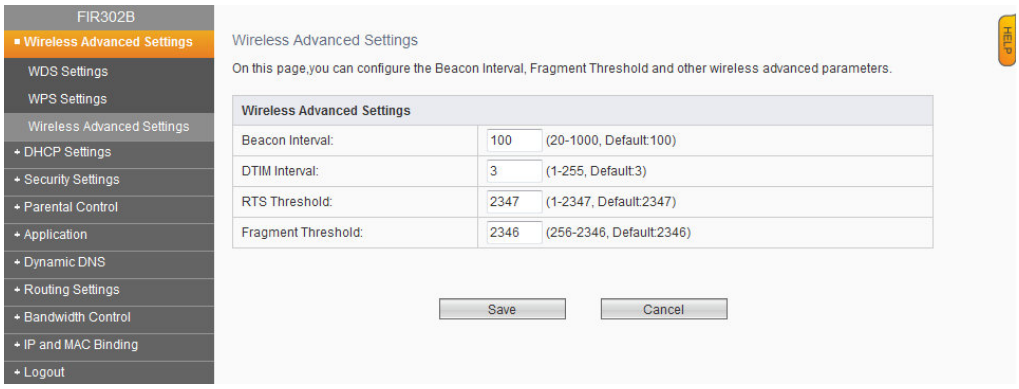
Menu item	Explanation
WPS Settings	
WPS (WiFi Protected Settings)	Establish easy and quick a connection between router and client device through encrypted contents. The users only enter the PIN code to configure.

Menu item	Explanation
WPS Mode	Supports two ways of configuration: PBC (Push-Button-Configuration) PIN Code
PBC (Push-Button-Configuration)	Select PBC button or press the WPS button on the panel of your router (press WPS button on the router and press the WPS button on another network device within two minutes).
PIN	Enable this option, you need to enter a wireless clients PIN code in the blank field and keep the same code in the client.

Wireless Advanced Settings

This section is to configure the advanced wireless settings of the router.

If you are not familiar with the setting items on this page, it is strongly recommended to keep the provided default values; otherwise it may result in poor wireless network performance!



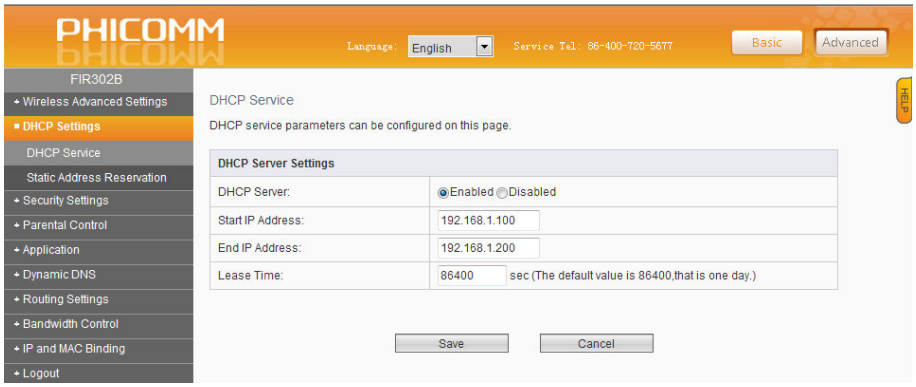
Menu item	Explanation
Wireless Advanced Settings	
Beacon Interval	Interval for sending packets of the beacon frame (value range 20 – 1000 ms, default = 100 ms)
DTIM Interval	Interval for Delivery Traffic Indication Message (DTIM) – value range 1 - 255 ms, default = 1ms
RTS Threshold	If the packet size is larger than the preset RTS size, the wireless router will send a RTS to the destination station to start a negotiation (default = 2347).
Fragment Threshold	Sets the fragment threshold. Packets larger than the size

Menu item	Explanation
	set in this field will be fragmented. Too many data packets will degrade the wireless network performance. The fragment threshold value should not be set too low (default = 2346).

DHCP Settings

DHCP Service

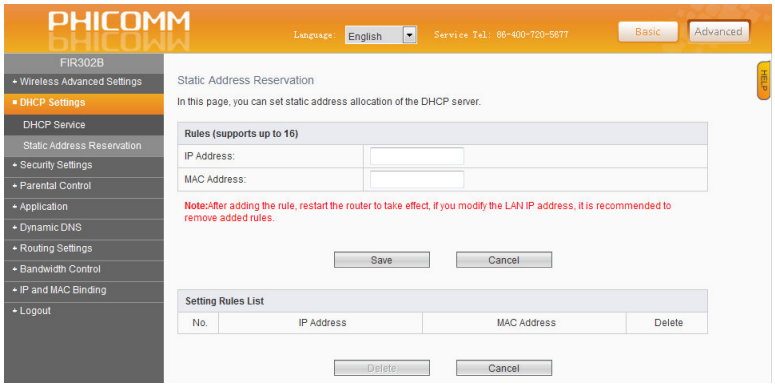
If you enable the DHCP server of the router, the DHCP server will configure the TCP/IP protocol for each PC in the LAN automatically.



Menu item	Explanation
DHCP Server Settings	
DHCP Server	If you disable this server, please make sure that another DHCP server is enabled in your network.
Start IP Address	1st address in your IP address pool
End IP Address	Last address in your IP address pool
Lease Time	This is the time interval, after the server uses a different DHCP address.

Static Address Reservation

When you specify a reserved IP address for a PC in the LAN, the PC will always receive the same IP address each time accessing the DHCP server. Reserved IP addresses could be assigned to servers that require permanent IP settings.



Menu item	Explanation
Rules (supports up to 16)	
IP address	IP address, reserved for routers
MAC address	MAC address of the PC for which you want to reserve an IP address

4.2.8 Security Settings

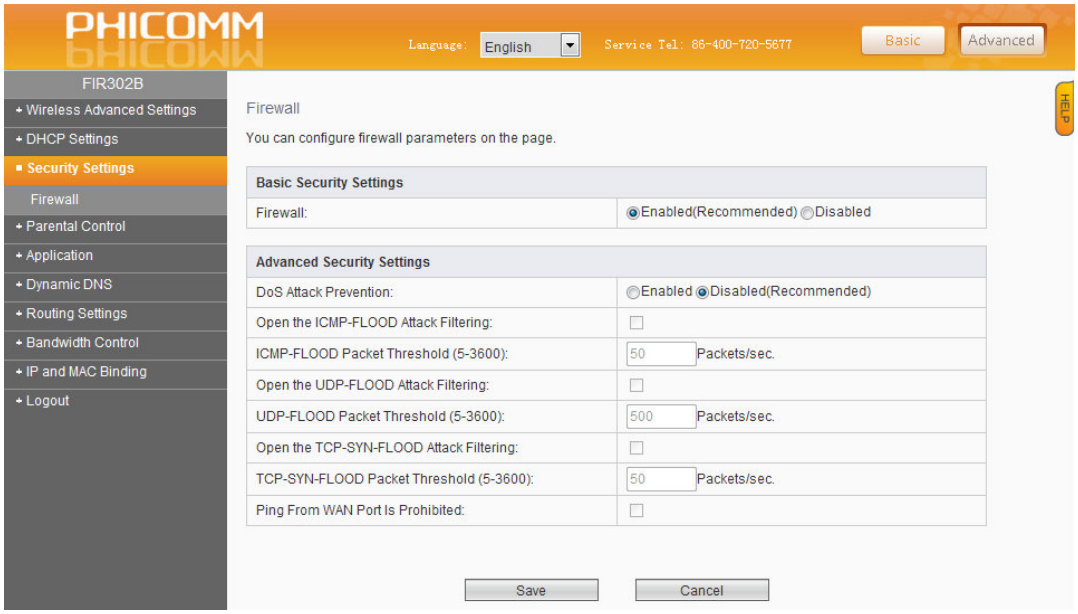
Click **Firewall** to configure.

Firewall

Select **Enabled** or **Disabled** to enable or disable the firewall.

If the firewall is enabled, the system refuses all requests from the internet. Only packets from the LAN which are belonging to defined connections and for which the status database is created can pass the firewall and can have access to the LAN.

By default the firewall is enabled. To expose all hosts in the LAN to the internet you can disable the firewall.



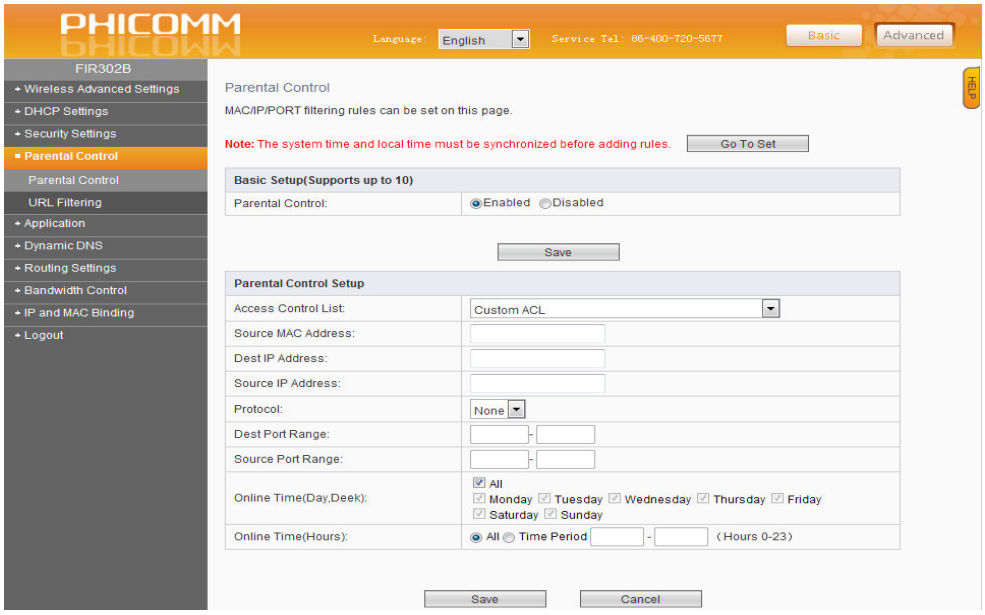
Menu item	Explanation
Advanced Security Settings	
DoS Attack Prevention	Enable for attack prevention.
Open the ICMP-Flood Attack Filtering	Select to protect against ICMP-FLOOD attacks.
ICMP-Flood Packet Threshold	If the number of ICMP data packets exceeds the threshold, the defense measures act immediately.
Open the UDP-Flood Attack Filtering	Select to protect against UDP-FLOOD attacks.

Menu item	Explanation
UDP-Flood Packet Threshold	If the number of UDP data packets exceeds the threshold, the defense measures act immediately.
Open TCP-SYN-FLOOD Attack Filtering	Select to protect against TCP-SYN-FLOOD attacks.
TCP-SYN-Attack Packet Threshold	If the number of TCP-SYN data packets exceeds the threshold, the defense measures act immediately.
Ping from WAN Port is prohibited:	If you select this option, the PC in the WAN cannot send the Ping packets to the router.

4.2.9 Parental Control

Parental Control

This page is used to enable the firewall filtering function. You can select the blocking service or set the parameters (MAC address, IP address and ports), which need to be blocked, manually. You must set at least one filtering condition. You may also set multiple conditions or all conditions.

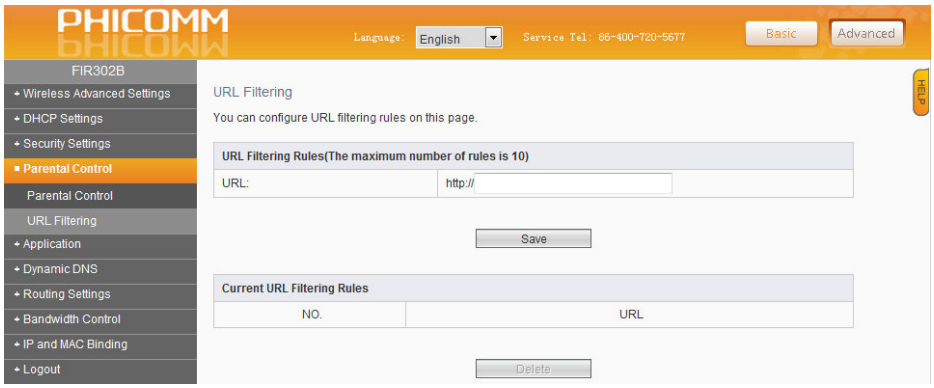


Note

Please synchronize the router's time first, if selecting the timing function.

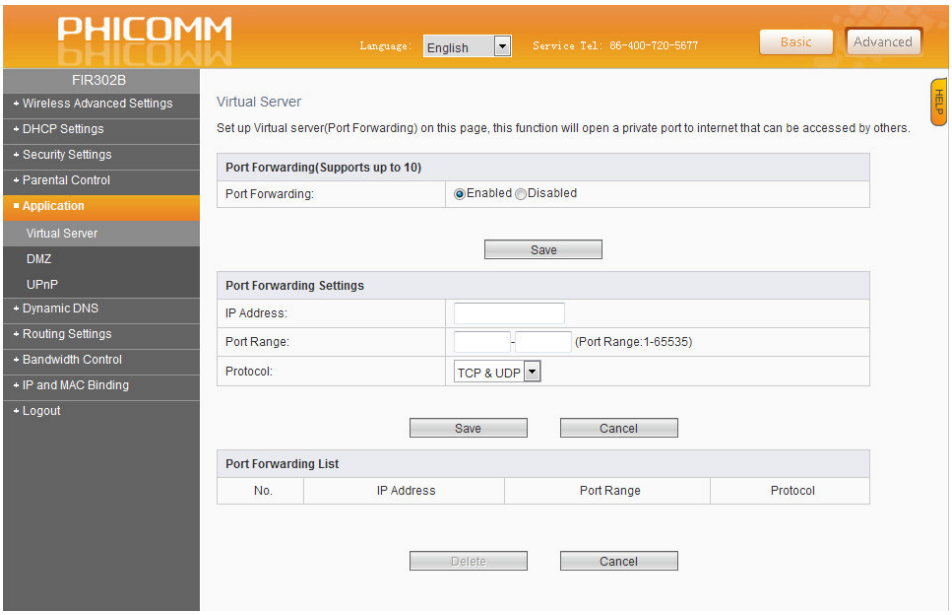
URL Filtering

Enter the URL address you want to filter in the URL box.



4.2.10 Application

Virtual Server



Select **Enabled** under **Port Forwarding** function to open a private port to internet that can be accessed by others.

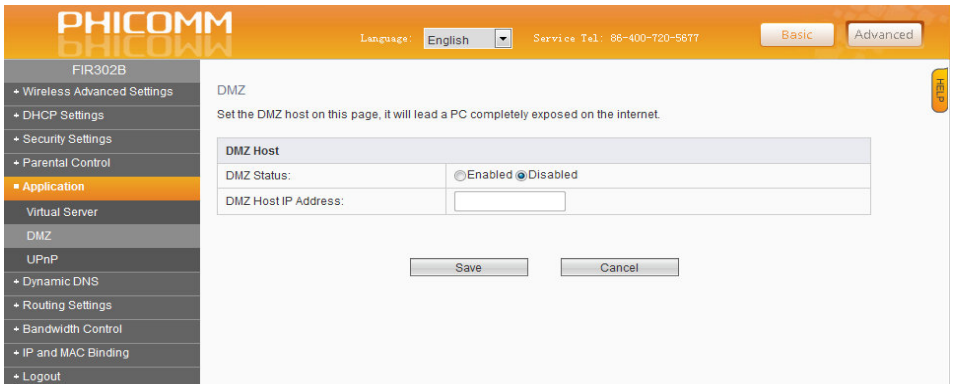
Menu item	Explanation
Port Forwarding Settings	
IP address	IP address of the server you want to open the port, for example 192.168.2.X
Port Range	Port range of the server you want to open.
Protocol	Protocol of the server.

Note

Please assign a static IP address to the server.

DMZ

Please select **Enabled** under **DMZ Host**.



Menu item	Explanation
DMZ Host	
DMZ Status	Select **Enabled** or **Disabled.**
DMZ-Host IP address	Enter the IP address of the PC in the LAN that you want to set.

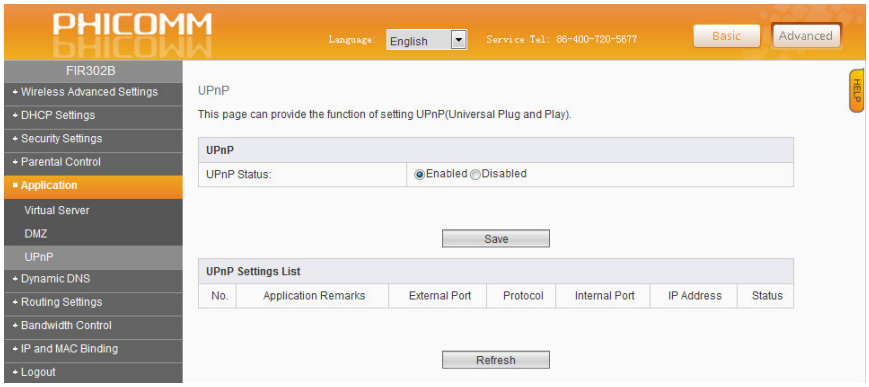
Note

Before using the DMZ host, you should assign a static IP address to the designated server. Then enter this static IP address into the router as its IP address.

DMZ priority is higher than the port forwarding. If the DMZ is open, all port forwarding rules are not effective.

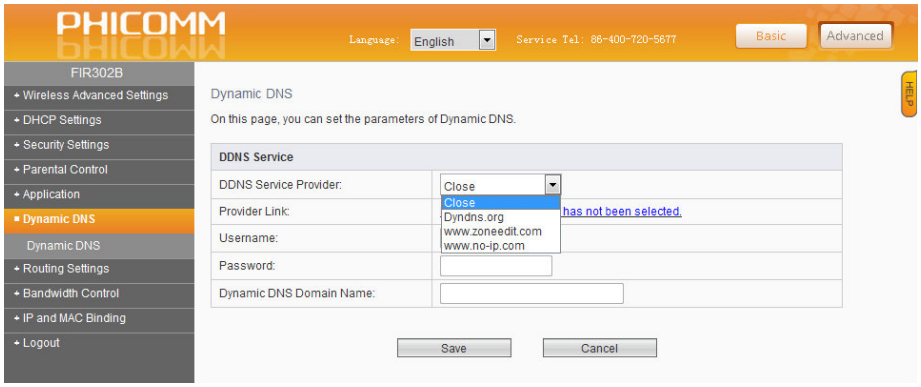
UPnP

Select **Enabled** or **Disabled**.

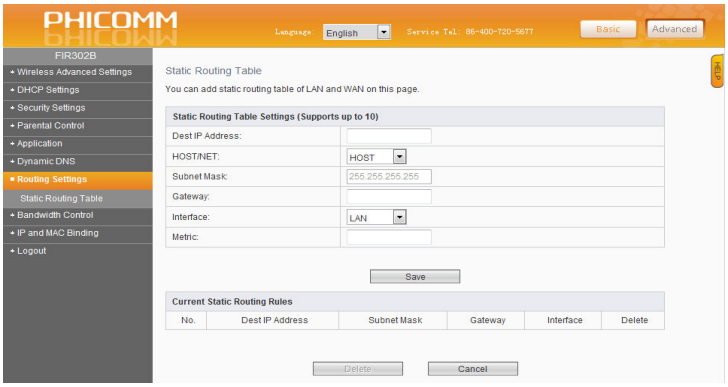


4.2.11 Dynamic DNS

The dynamic DNS allows assigning a fixed host and domain name to a dynamic internet IP address. If you want to use this feature, please register at a DDNS service provider for this service (e. g. www.no-ip.com). After registration please select your service provider and enter **Username**, **Password** and **Dynamic DNS Domain Name**.



4.2.12 Routing Settings

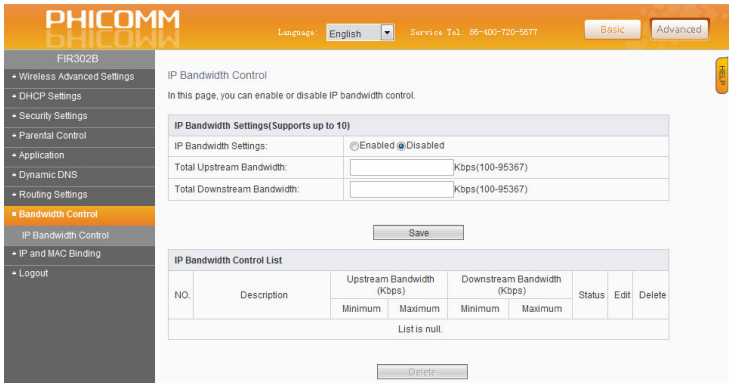


Static Routing Table

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing protocol to forward traffic.

Menu item	Explanation
Static Routing Table Settings (support up to 10)	
Destination IP address	IP address of the network or host that you want to assign to a static route
Subnet Mask	The subnet mask determines which portion of an IP address is the network portion and which portion is the host portion.
Gateway	This is the IP address of the default gateway device that allows the contact between router and network or host.

4.2.13 Bandwidth Control



IP Bandwidth Control

Menu item	Explanation
IP Bandwidth Settings	
IP Bandwidth Settings	Select **Enabled** or **Disabled.**
Total Upstream Bandwidth	Rate of uploading through WAN interface
Total Downstream Bandwidth	Rate of downloading through WAN interface

Note

Bandwidth conversion: 1 Mbps = 1024 Kbps

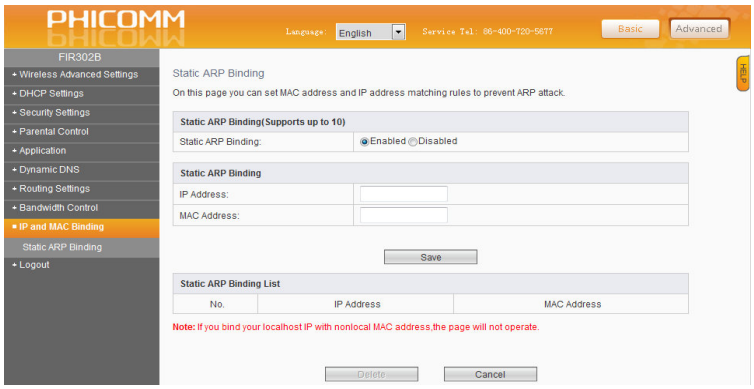
Select the type of the broadband line and the bandwidth according to the actual situation. If you are not sure about the information, please consult your broadband provider.

After finishing the settings, click the **Save** button to apply the settings.

4.2.14 IP and MAC Binding

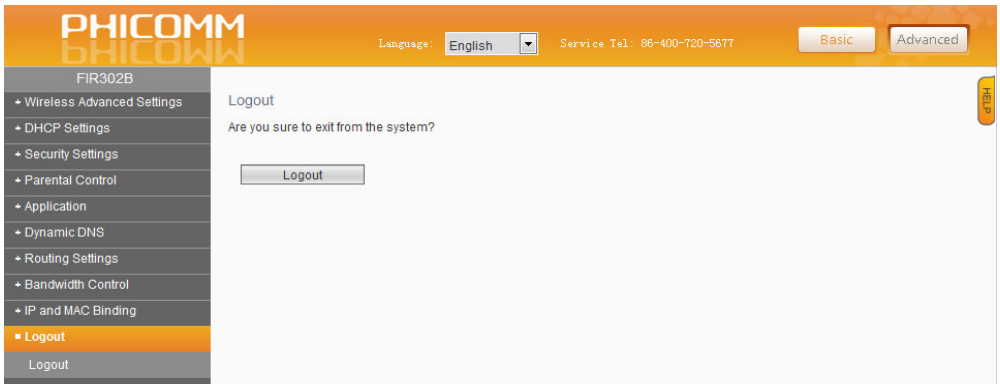
Static ARP Binding

You may use the ARP binding function to control the static ARP cache table for preventing the ARP deception effectively.



Menu item	Explanation
Static ARP Binding	
IP address	IP address of the LAN PC
MAC address	MAC address of the LAN PC

4.2.15 Logout



Click **Logout** to exit from the router's configuration page.

5. Troubleshooting

Why I cannot open the management page?

- Turn off browser's proxy settings.
- Make sure that your network card has been set to obtaining an IP automatically.
- Make sure that your LAN and wireless LED is on and all cables are connected correctly.

I forgot my network name or encryption keys!

- Try to set up a wired connection and configure the wireless encryption again.
- Press the Reset button of the router longer than 5 seconds.

Why I cannot access the internet via LAN adapter?

- Move the router closer to the wireless client.
- Check whether the wireless adapter is connected to the correct wireless router.
- Check whether the wireless channel conforms to the channels available in your country / area.
- Retry using another Ethernet cable.
- Check if all cables are connected correctly.

Factory default settings

Item	Default
Basic settings	
Username	admin
Password	admin
IP address	192.168.2.1
Subnet mask	255.255.255.0
Wireless	
SSID	Phicomm_16AE03
Wireless security	Disabled
Wireless MAC address filtering	Disabled
DHCP	
DHCP server	Enabled
Start IP address	192.168.2.100
End IP address	192.168.2.200

6. Technical support – contact us

Shanghai Feixun Communication Co., Ltd.
Phone: +86 21 67754400
Email Sales: info@phicomm.com
Email Support: service@phicomm.com.cn

Phicomm Europe GmbH
Phone: +49 89 66056720
Email Sales: info-eu@phicomm.com
Email Support: support-de@phicomm.com

For detailed product information and Downloads (software, user manuals and certificates) please visit our website:

www.phicomm.com/de for Germany
www.phicomm.com/eu for Europe
www.phicomm.com Phicomm Global