FEIXUN

300Mbps Wireless N Router

FWR-734N

User Manual

V1.0

Copyright Statement

All the photos and product specifications mentioned in this manual are for references only, as the upgrading of software and hardware, there will be changes. And if there are changes, Feixun is not responsible for informing in advance. If you want to know more about our products information, please visit our website at www.feixun.com.cn

CONTENTS

Introduction

▪ Product Overview

Thank you for choosing FWR-734N Wireless-N Router.

FWR-734N 300Mbps Wireless N Router is an all-in-one router, ideal for home and SOHO users to share broadband Internet connection over the wired and wireless network. With the speed of up to 300Mbps, it can provide users with extraordinary smooth internet surfing, internet phone calling, on-line gaming, and HD video streaming. Moreover, by adopting built-in Omni-directional antennas and MIMO technology, FWR-734N could greatly increases the wireless range & sensitivity, which enables you to receive wireless signals in the farthest corner of your home or office. And you can quickly setup the security at a simple push of the “WPS” (Wi-Fi Protected Setup) button on the fashionable designed router, preventing your device from potential internet attacks.

Front Panel

Power LED
The Power LED lights up when the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, the LED flashes. When the diagnostic is complete, the LED is continuously lit.

WLAN LED
The Wireless LED lights up when the wireless feature is enabled. It flashes when the Router sends or receives data over the wireless network.

Wi-Fi Protected Setup (WPS) LED
If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use the Wi-Fi Protected Setup button to automatically configure wireless security for your wireless network. To use Wi-Fi Protected Setup, refer to the section of Wi-Fi Protected Setup.

WAN LED
The Internet LED lights up when there is a connection made through the Internet port. It flashes to indicate network activity over the Internet port.

LED (1-4)
These LEDs are corresponding with the LAN ports on the rear panel. The LED is continuously lit when the Router is connected to a device through that port. It flashes to indicate network activity over that port.

LED	Status	Description
Power	On	Power is on
	Off	Power is off
WLAN	On	Wireless network is switched on
	Off	Wireless LAN is disabled
	Blink	Data is transmitting
WPS	Off	WPS function is disabled
	Blink	A wireless device is connecting to the network by WPS function. This process will last in the first 2 minutes
	On	A wireless device has been successfully connected to the network by WPS function
WAN	On	Internet is connected
	Off	Internet is unconnected
	Blink	Data is transmitting
LAN (Port 1-4)	On	LAN port is connected
	Off	LAN port is unconnected
	Blink	Data is transmitting

Rear Panel

Reset
Long press and hold the button for 8 seconds, the Router will reboot to its factory default settings.

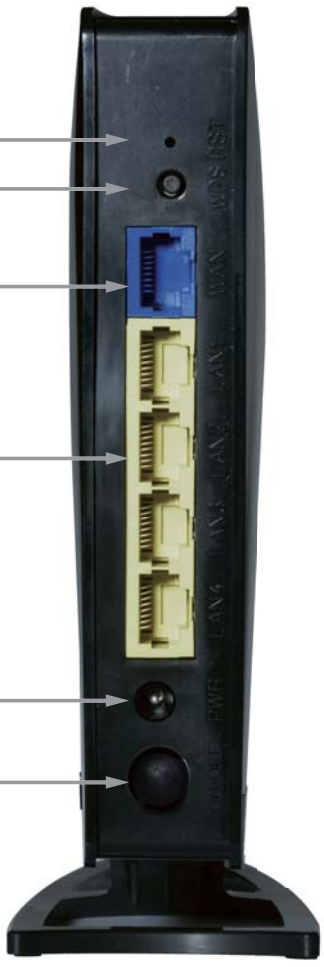
WPS
Press the button and the WPS LED in front panel flashing, WPS function is enabled.

WAN
Using an Ethernet cable (also called a network or Internet cable), the Internet port connects the Router to your Internet connection, which is typically a cable or Digital Subscriber Line (DSL) modem.

LAN (1-4)
Using Ethernet cables, these Ethernet ports (4, 3, 2, 1) connect the Router to computers and other Ethernet network devices on your wired network.

Power
The Power port connects to the included power adapter.

ON/OFF
The power on/off button.

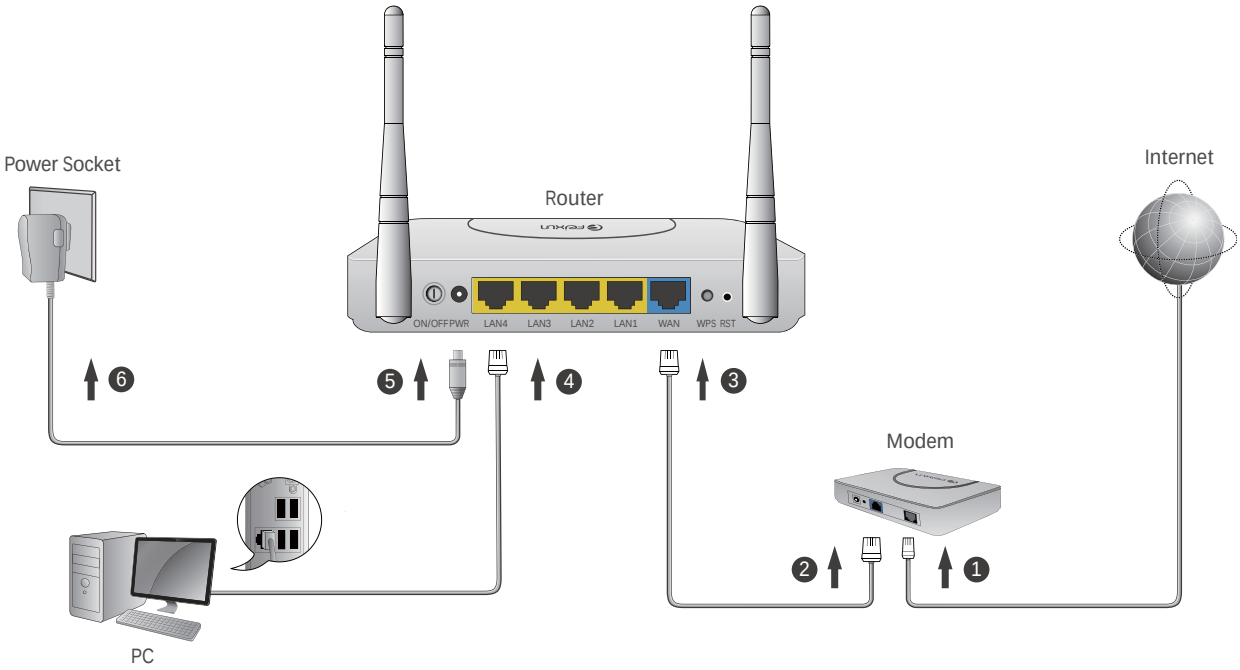


▪ Main Features

- 4 LAN ports and 1 WAN port
- Wireless N speed up to 300Mbps, ideal for internet surfing, on-line gaming and HD video streaming
- MIMO technology greatly increases the wireless range, sensitivity and stability
- Multi-SSID allows users to create multiple networks, and distributes access privilege of each network
- QoS controls the reasonable allocation of bandwidth to achieve optimum utilization, ensuring reliable Internet connection
- Quick wireless security setup by simply pressing the WPS button
- WDS wireless bridge provides seamless bridging to expand your wireless network
- Built-in firewall featured with IP, MAC, URL filtering and ARP attack prevention to protect your PC
- Backward compatible with 802.11b/g product
- Setup wizard simplifies installation and configuration

Installation

▪ Physical Connection



⚠ **Note:**

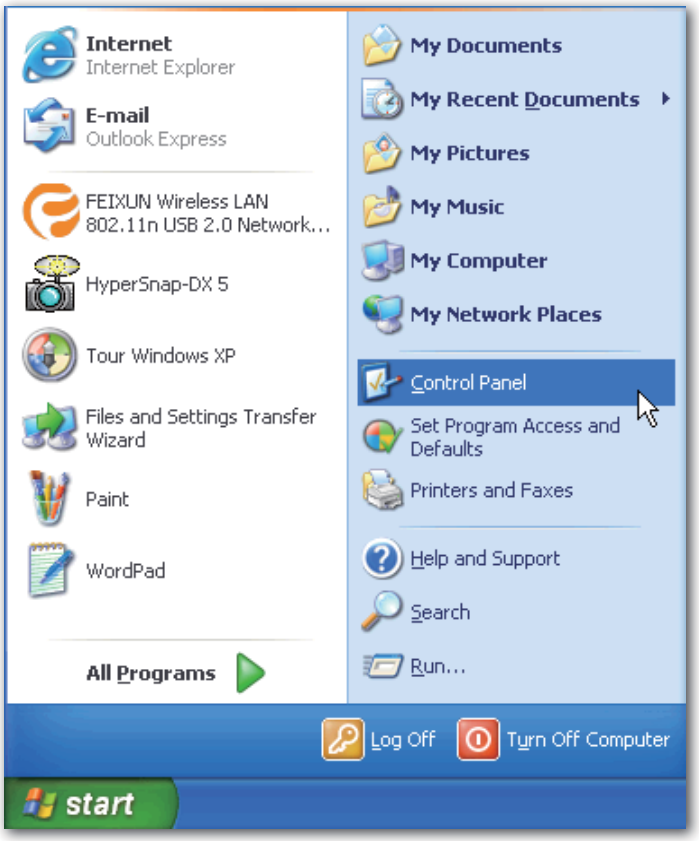
- Actual product may be different as the picture, but the installation will be the same.
- Please use the included power adapter. Use of a different power adapter could cause damage and void the warranty for this product.
- Please ensure the Power, LAN and WAN lights are ON when the installation finished successfully.

▪ Configure the Computers IP Address

After connecting your PC to the router, you need to configure your PCs IP address.

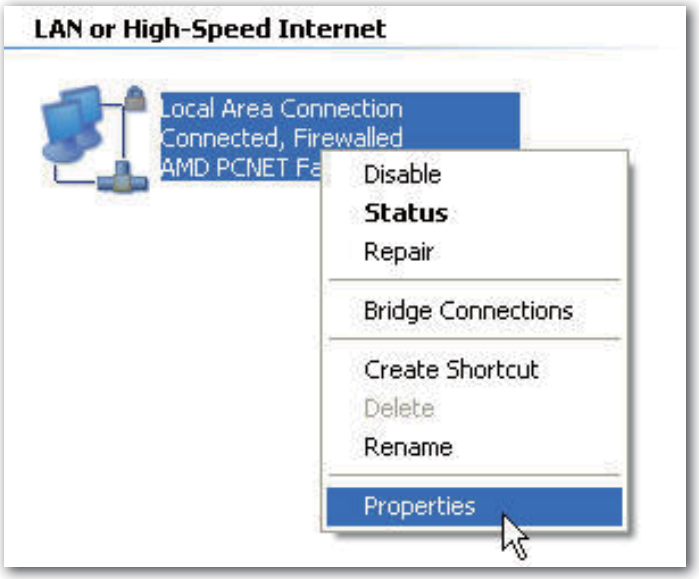
For Windows XP/2000

1. Click **Start>Control Panel**.

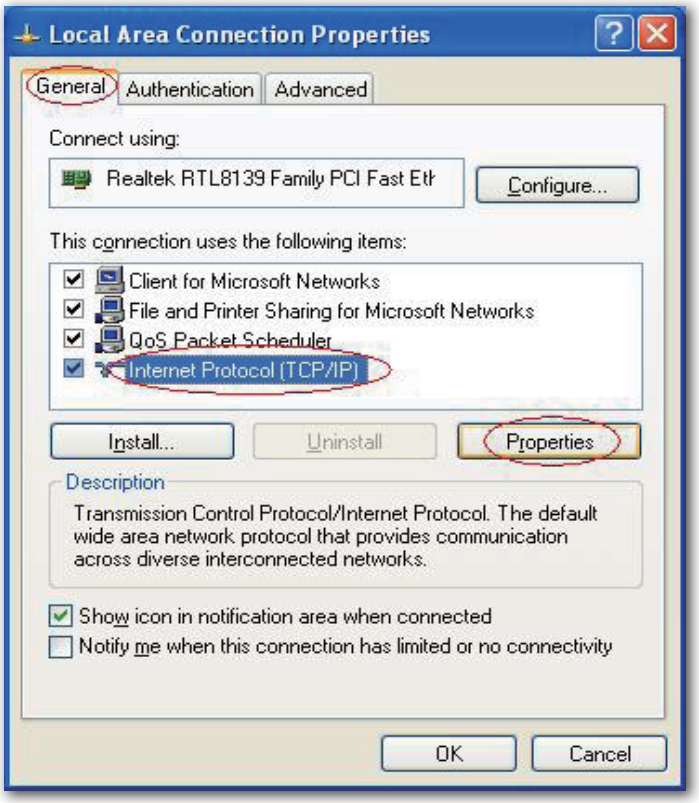


2. Select and double click **Network Connection**.

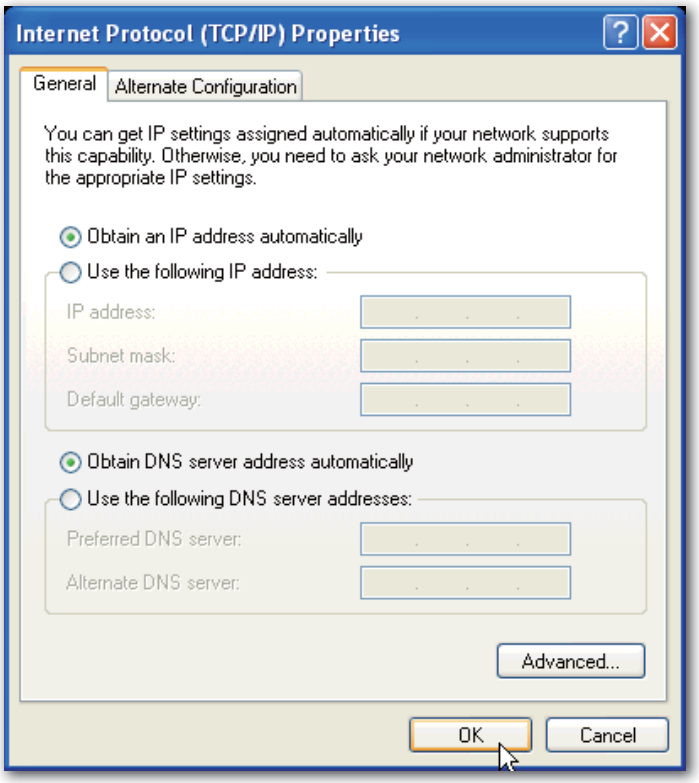
3. Right click **Local Area Connection** and then select **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.



For Windows Vista/7

1. Click **Start>Control Panel**.
2. Click View **network status and tasks** and then click **Manage network connection**

(**Change adapter settings** for Windows 7).

3. Right click **Local Area Connection** and then click **Properties**.
4. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

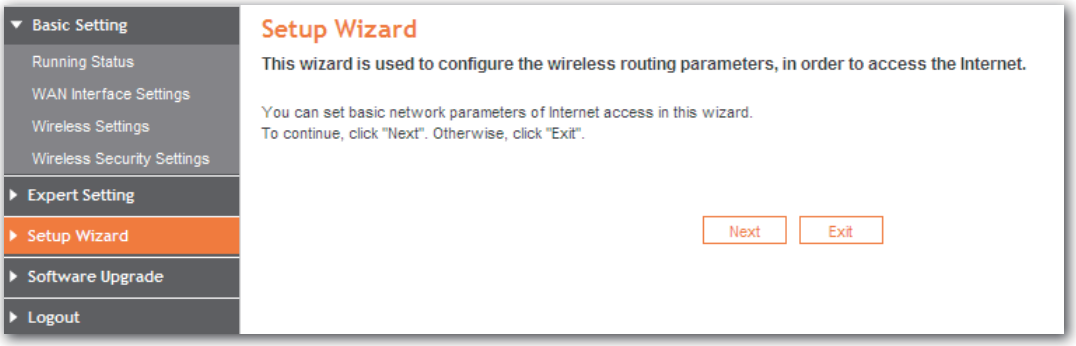
▪ Setup Wizard

After successful installation, now you can go ahead with connecting to the internet, the operations are as following:

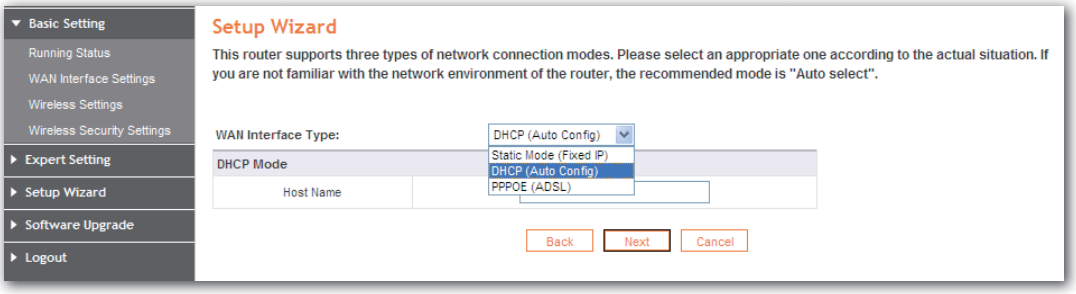
1. Open your web browser and enter 192.168.0.1.

2. You are prompt to enter the Username/Password (preset as admin/admin) which you can found on the label at the bottom of your router, and then click **Login**.

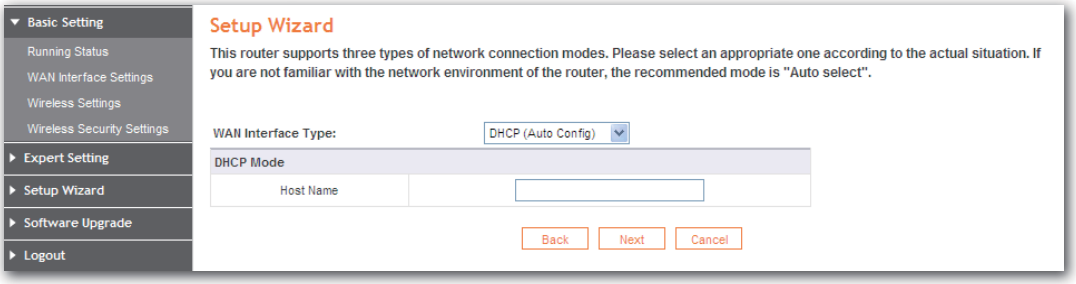
3. After a successful login, the following page will appear. Click **Next**.



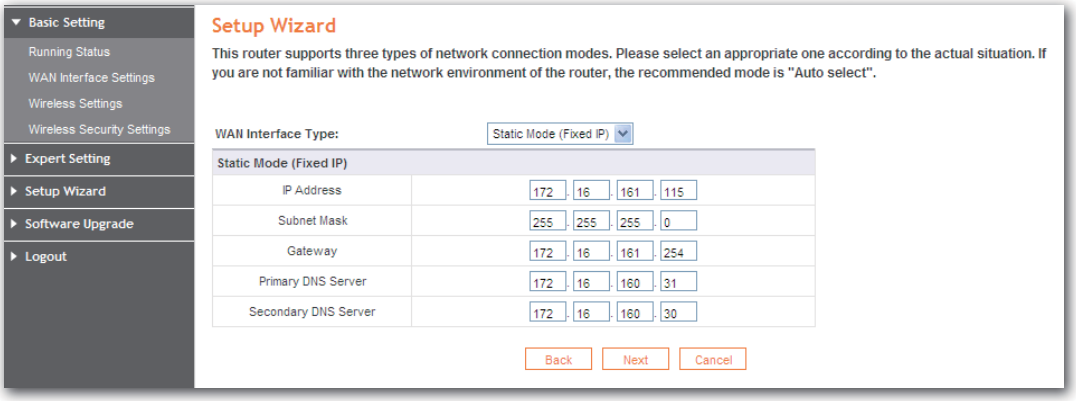
4. You are prompted to select your WAN interface type, there are three types available: **DHCP**, **Static IP** and **PPPoE**.



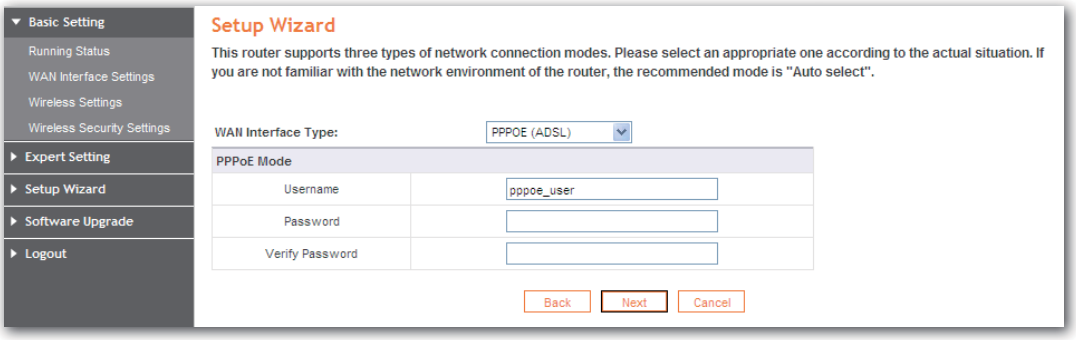
a. Select **Dynamic IP (DHCP)** if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services. Router will obtain IP address information automatically. In this case, no need to input anything but click **Next**.



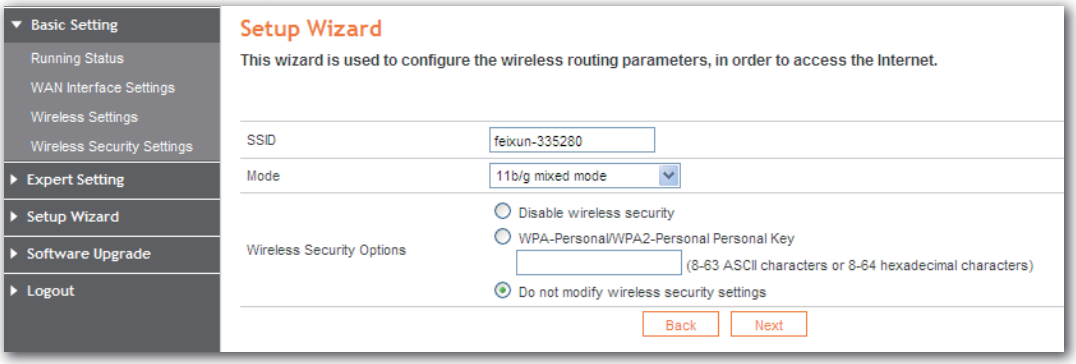
b. Select **Static IP** if all the internet ports IP information is provided to you by your ISP, you will need to enter in the IP address, subnet mask, gateway address and DNS address, and then click **Next**.



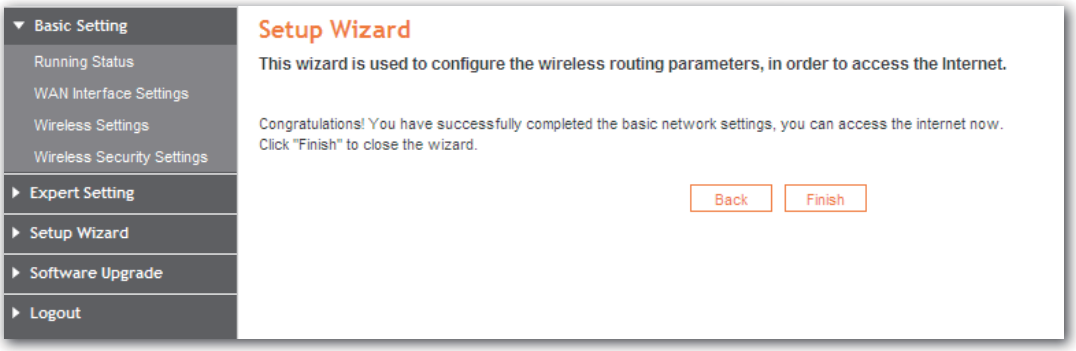
c. PPPoE is typically used for DSL services. Select **PPPoE** and fill the Username and Password information provided by your ISP, and then click **Next**.



5. In this page, please set the Wireless Network Name (SSID), Mode, Wireless Security, click **Next**.

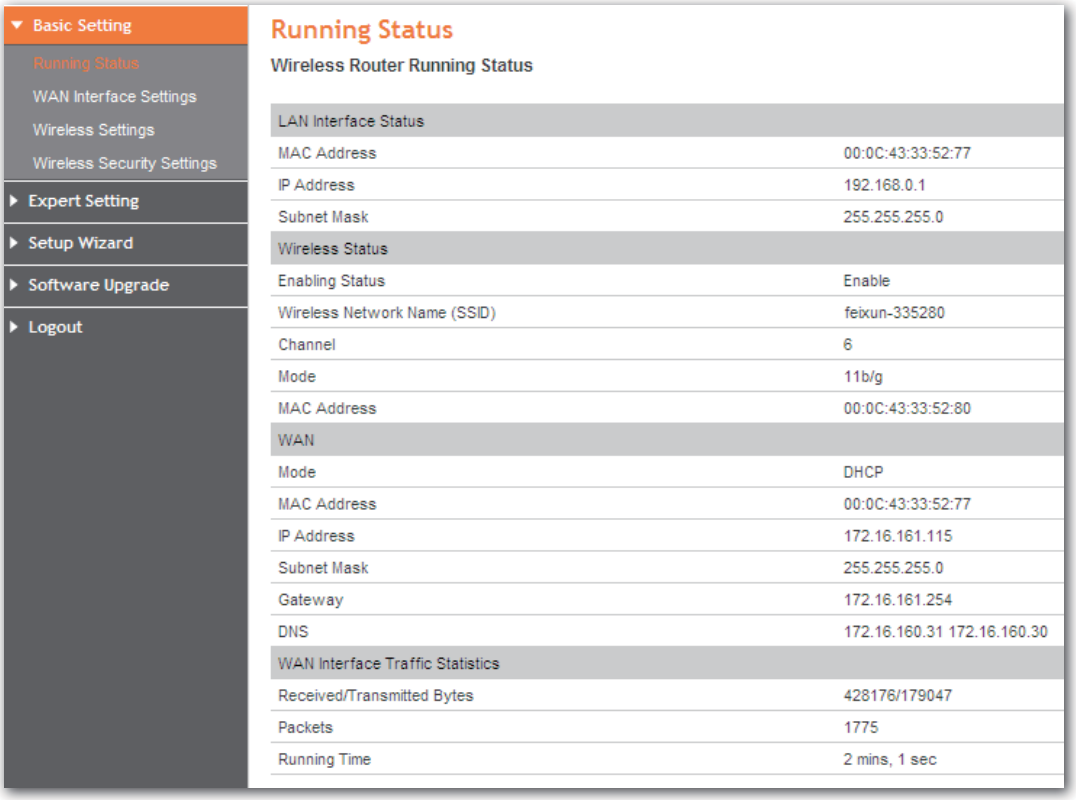


6. Click **Finish**, you would successfully access to the internet.



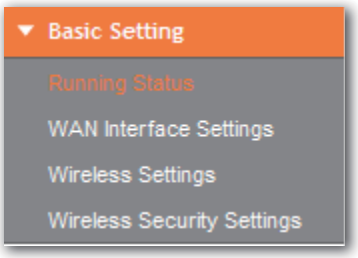
Router Configuration

You will see the five main menus on the left of the web-based utility. On the right, there are the corresponding explanations and instructions. The Status page provides the current status information about the Router. All information is read-only.

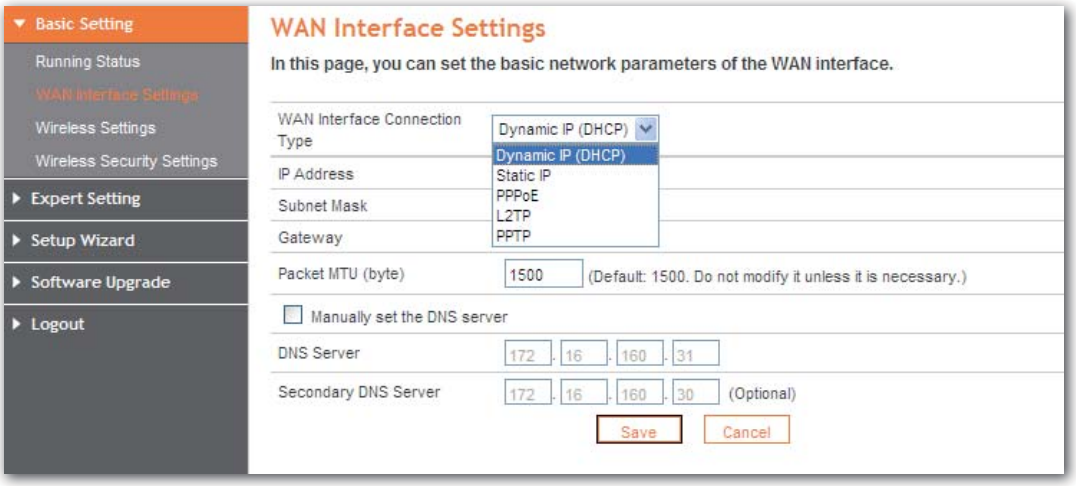


▪ Basic Setting

The basic setting section configures the Router to your Internet connection. Most of this information can be obtained through your Internet Service Provider (ISP).



WAN Interface Settings



WAN Interface Connection Type:

Dynamic IP: Obtain the IP address automatically assigned by the DHCP server from the ISP.

Static IP: Have a static IP address provided by the ISP.

PPPoE: Access the Internet by virtual ADSL dialup.

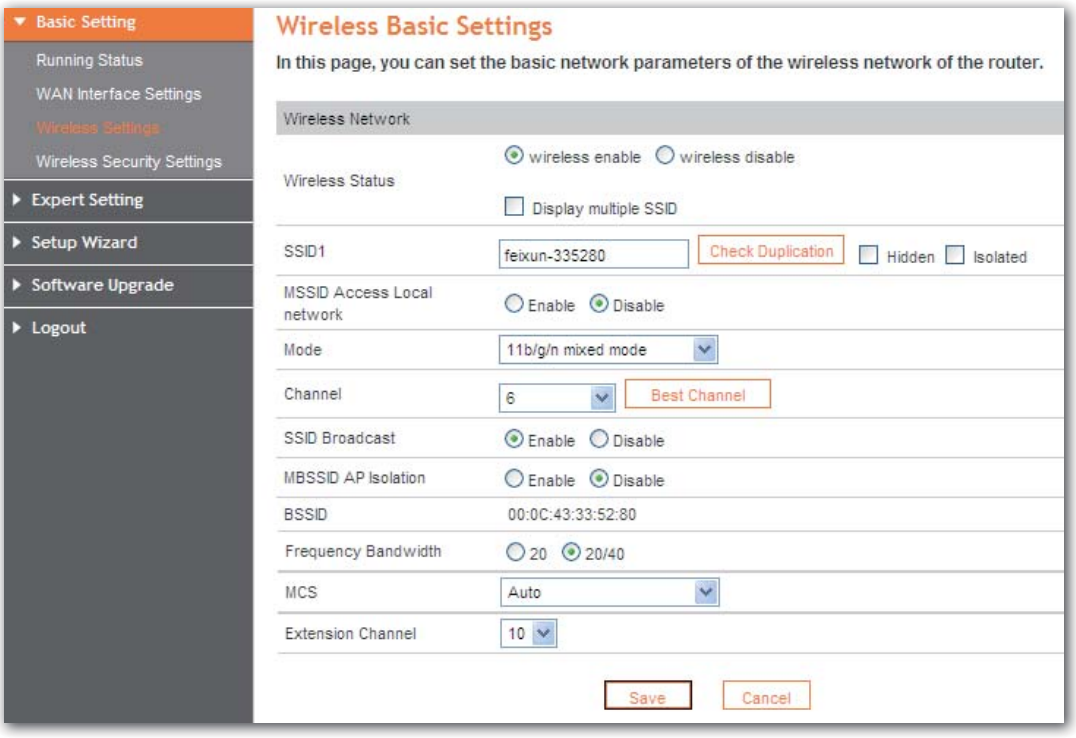
L2TP: Layer 2 Tunneling Protocol (L2TP) is a service applies to connections in Israel only.

PPTP: Point-to-Point Tunneling Protocol (PPTP) is a service applies to connections in Europe only.

Select the connection type according to the information provided by your Internet Service Provider (ISP), and fill in the information accordingly.

Wireless Settings

The basic settings for wireless networking are set on this screen. In this page, you can set the basic network parameters of the wireless network of the router.



Wireless Status: If you do not have any other wireless devices in your network, select **Wireless Disabled**.

Wireless Network Name (SSID): The name of routers wireless network. The wireless work station must keep the same SSID name with the APs for connections. By select **Hidden** or Isolated, the device can open or close to search available APs.

Mode: From this drop-down menu, you can select the wireless standards running on your network:

- **11b/g/n-Mixed:** If you have only Wireless-G Wireless-N and Wireless-B devices in your network, select **11b/g/n-Mixed**.
- **11b/g-Mixed:** If you have only Wireless-G and Wireless-B devices in your network, select 11b/g-Mixed.
- **Wireless-G Only:** If you have only Wireless-G devices, select **Wireless-G Only**.
- **Wireless-B Only:** If you have only Wireless-B devices, select **Wireless-B Only**.

Channel: You can use the channel same as the AP. By enabling Open Scanning button to find out the available APs channel.

SSID Broadcast: Select enable to enable the devices SSID to be visible by wireless clients.

BSSID: It is a 48-bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP.

Frequency Bandwidth: Select wireless work frequency 20M or 20/40M.

Save: Click the **Save** button to save your setting.

Wireless Security Settings

The wireless security settings configure the security of your wireless network(s). Six wireless security modes, WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise and RADIUS, are supported. If you do not want to use wireless security, select **Disable** from the drop-down menu.

WIRELESS NETWORK NAME (SSID): Select SSID to be configured security. The device

supports to configure different security classes between the main SSID and the subordinate SSID.

Security Mode: There are several different security modes; you can choose one from disable, open, share, WEPAUTO, WPA-PSK WPA2-PSK, and WPA-PSK/WPA2-PSK etc..

The operations of each security mode are as following:

- **Mode 1: Security Mode > Disable**

  If you do not want to use wireless security, check this radio button.

- **Mode 2: Security Mode > Open/Share/ WEPAUTO**

  It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as show in Figure 4-18. You can choose the type for the WEP security on the pull-down list. You can select **Shared Key** or **Open System** authentication type automatically based on the wireless stations capability and request.

  Default Key: Select a valid encryption key.

  WEP Key 1, 2, 3, 4: Enter the WEP key here. Please note that the key should be in accordance with the key format and be valid. The key should be **ASCII Characters** or **Hexadecimal Digits**.

  ⚠ **Note:** If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as the Authentication Type.

- **Mode 3: Security Mode>WPA-Personal/WPA2-Personal**

  WPA PSK (Wi-Fi Protected Access): A Wi-Fi standard is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorized wireless device.

  WPA Algorithms: Select one encryption type, AES or TKIP. (AES is stronger than TKIP)

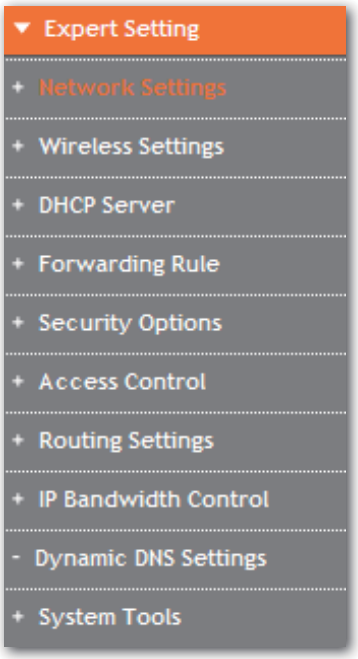
  Pass Phrase: Default as 12345678, please enter a new key (8-63 ASCII characters).

  Key Renewal Interval: It is to tell how often the Router changes key. The default time is 3600s; do not change it unless it is necessary.

  ⚠ **Note:** To improve security level, do not set the keyword with words that can be found in a dictionary or too easy to remember.

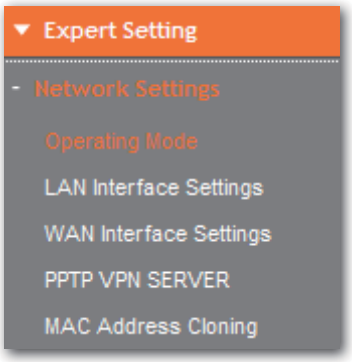
▪ Expert Setting

Expert Setting enables users to realize many advanced funtions of the router. Under this menu, there are ten submenus as follow:



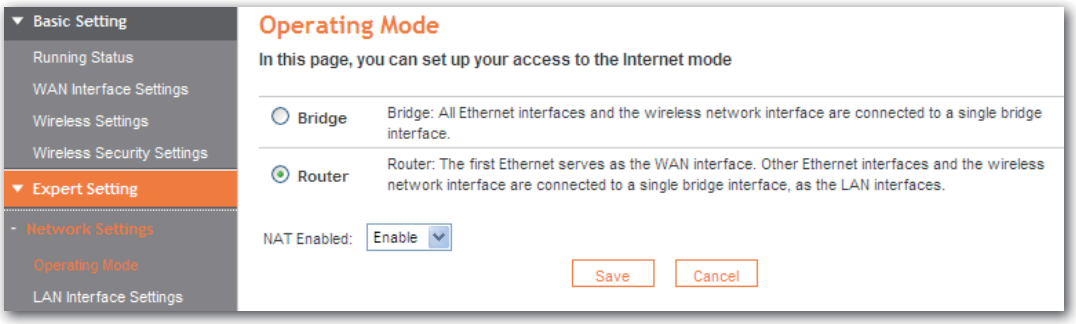
Network Settings

There are five submenus under the Network Setting menu as shown below. Click any of them, and you will be able to configure the corresponding function.

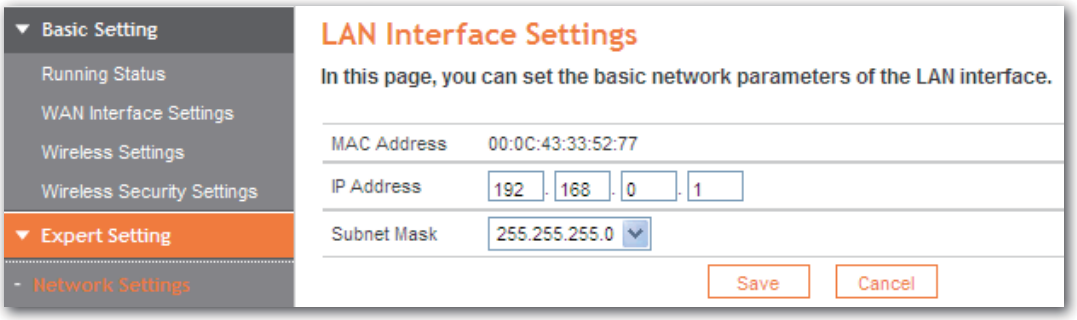


- **Operating Mode**

This page is used to set the operating mode of the device. Please choose Bridge mode or router mode according to your requirement; When the NAT is enabled, it can provide the transfer of internal / external networks addresses for the LAN and wireless networks. You can choose the mode for the router on the pull-down list.



- **LAN Interface Settings**



MAC Address: The Routers physical MAC address as seen on your local network, which is unchangeable.

IP Address: The Routers LAN IP Address (not your PCs IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.0.1 is the default value.

Subnet Mask: It's shown the Routers subnet mask for measurement of the network size. 255.255.255.0 is the default value.

Save: Click the **Save** button to save your setting.

⚠ **Note:**

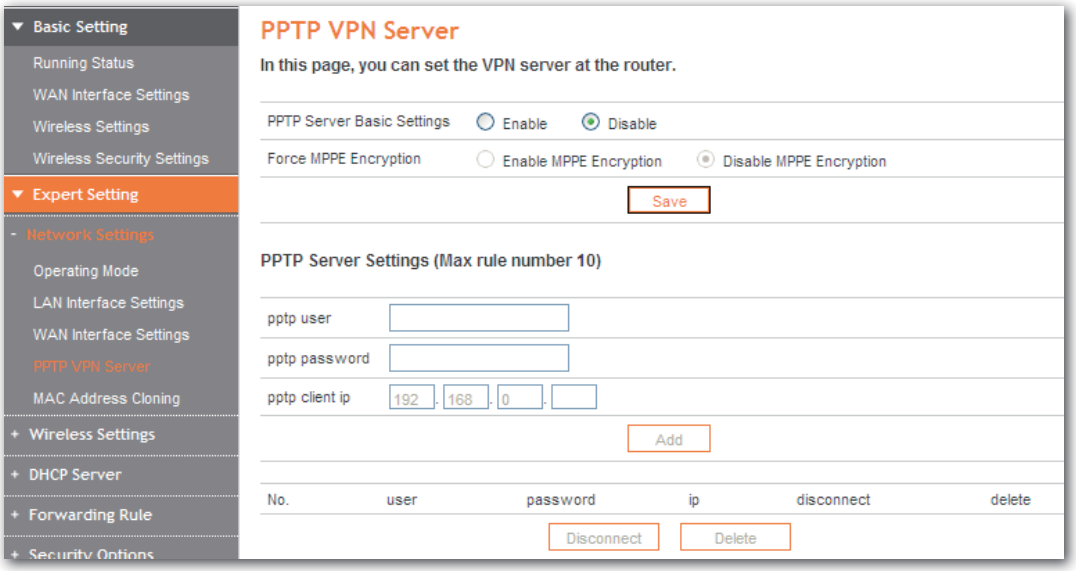
- If the LAN IP Address changes, you must use the new IP address to log in to the router, in order to access the Web configuration page.
- If the new LAN IP address is in a different network segment from the original LAN IP address, the dynamic IP service of the router is automatically switched to work in the network segment of the new LAN IP address. To apply virtual server, DMZ host and DHCP Static Address Allocation, please perform the settings again.

- **WAN Interface Settings**

Please refer to **Basic Setting** > **WAN Interface Settings**.

- **PPTP VPN Server**

A PPTP Server (Point-To-Point Tunneling Protocol) allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office, etc. This way you can use the services provided in your office at the comfort of your home.



PPTP Server Basic Settings: Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default as **Enabled**.

Force MPPE Encryption: Keep the default as **Enabled**.

PPTP user: Enter PPTP username provided by your ISP.

PPTP password: Enter PPTP password provided by your ISP.

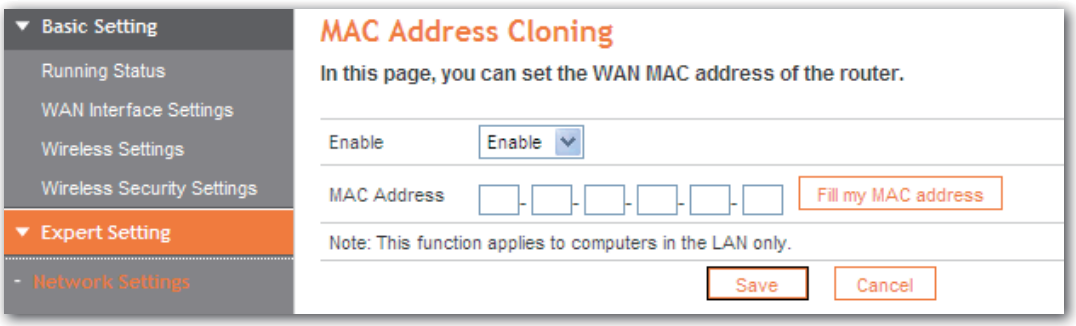
PPTP client IP: Enter the PPTP client IP address.

Click the **Add** button to save your setting.

- **MAC Address Cloning**

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require you to register a MAC address in order to access the Internet. If you were using cable modem, you were suggested to clone the current registered MAC address to the router. This page was designed to realize this function.

⚠ **Note:** To enable this function, you would to ensure the computer connecting to the router is the main computer, and the computer links to the router by cable.



Disable/Enable: To have the MAC address cloned, select **Enable**.

MAC Address: The MAC address to be registered with your Internet service provider.

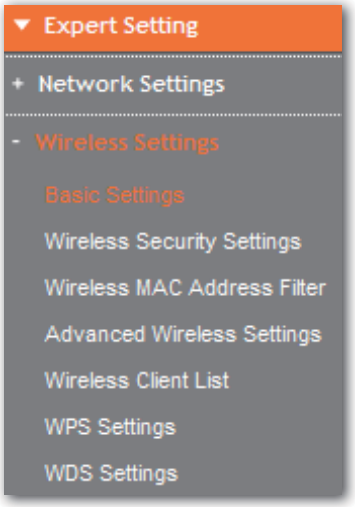
Fill my MAC address: Click this button, system will clone the registered MAC address

from your computer and auto fill in the blanks.

Save: Click the **Save** button to save your setting.

Wireless Settings

There are seven submenus under the wireless menu. Click any of them, you will be able to configure the corresponding function.



- **Basic Settings**

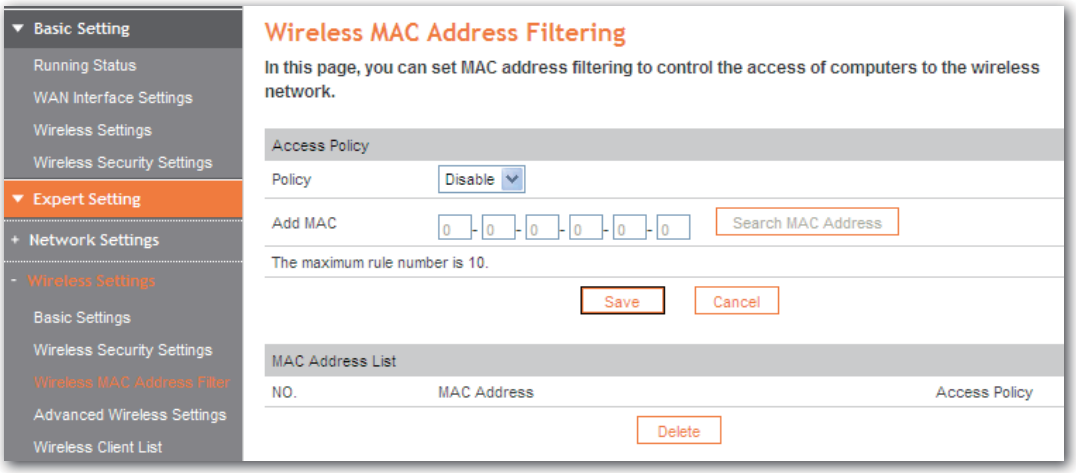
  Please refer to section of **Basic setting** > **wireless setting**.

- **Wireless Security Settings**

  Please refer to section of **Basic setting** > **Wireless Security Setting**.

- **Wireless MAC Address Filtering**

  MAC Address: MAC addresses involved in the wireless host access control.



Example:

If you only want MAC address (00:0A:EB:00:07:5F) to access the wireless network while others cannot:

1. The security policy chooses to allow.

2. Fill MAC address 00:0A:EB:00:07:5F in and click **Save**.

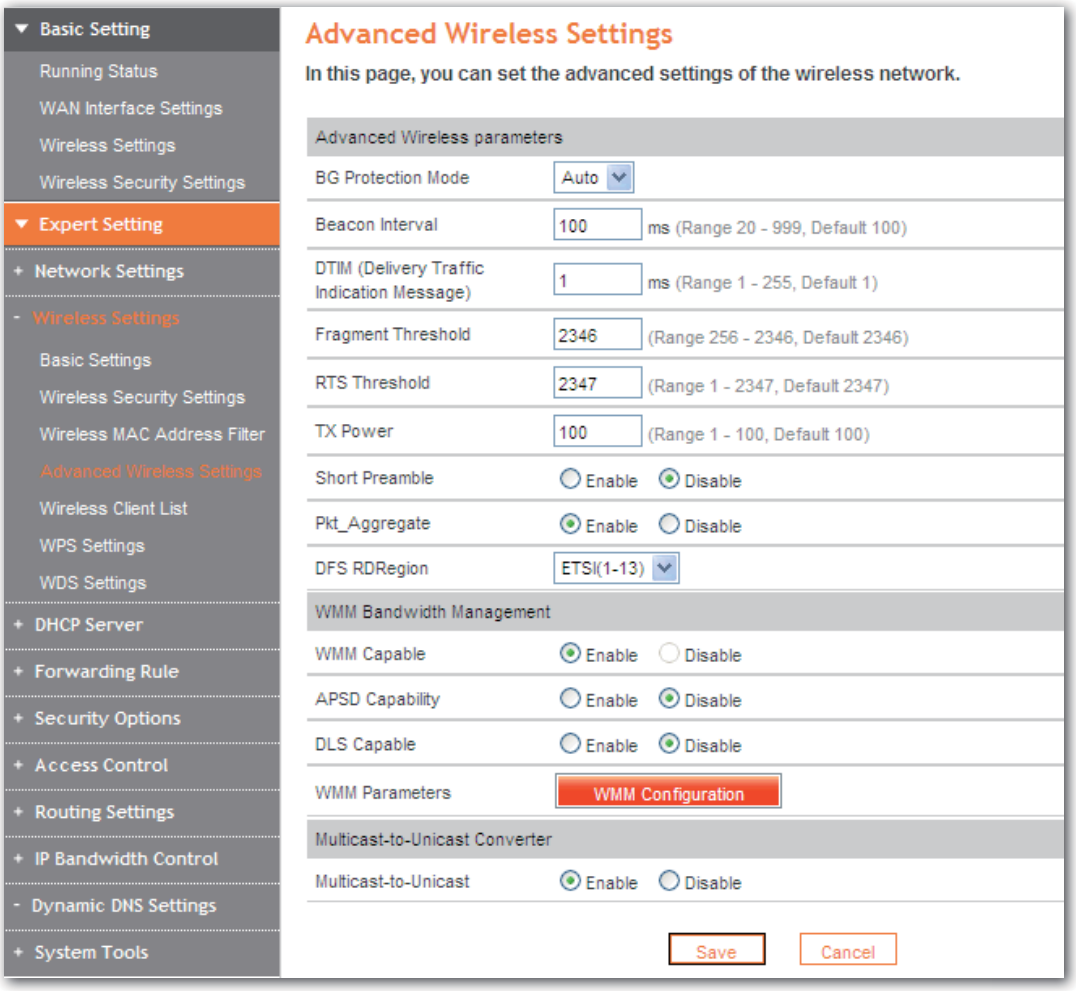
If you want MAC address (00:0A:EB:00:07:5F) cannot access the wireless network while others can:

1. The security policy chooses to refuse.
2. Filling MAC address 00:0A:EB:00:07:5F in and click **Save**.

In the MAC Address list, click **Remove** to delete the MAC addresses selected.

- **Advanced Wireless Settings**

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, Beacon Period and DTIM Interval.



BG protection Mode: Auto by default. You can select **On** or **Off**.

Beacon Interval: The interval for sending packets of the Beacon frame. Its value range is 20.1000ms, default as 100.

DTIM Interval: It indicates the interval of the delivery traffic indication message (DTIM). The value range is between 1 and 255 milliseconds. The default value is 1.

Fragment Threshold: Set the fragmentation threshold. Packets larger than the size set

in this field will be fragmented. Too many data packets will lower the wireless network performance. The Fragment Threshold value should not be set too low. The default value is 2346.

RTS Threshold: Set the RTS (Request to send threshold) threshold. When 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. The default value is 2347.

TX Power: You can set the output power of wireless radio. Unless you are using this wireless router in a really big space, you may not have to set output power to 100%. This will enhance security (malicious/unknown users in distance will not be able to reach your wireless router).

Enable WMM: If you select it, the router will process the packets with the priority first. You are recommended to select this option.

APSD Capable: It is used for auto power-saved service. The default is **Disabled**.

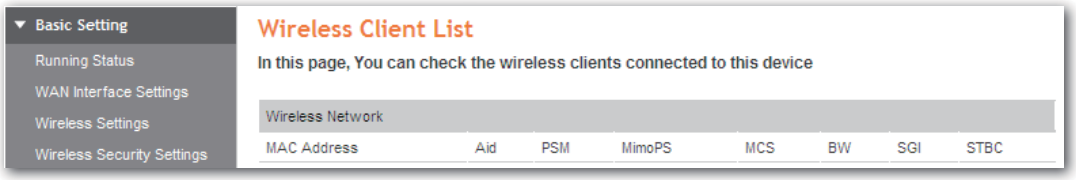
MAC Address List: The added MAC addresses are listed here. Click the **Delete** button to delete the filter management for this MAC address.

Save: Click the **Save** button to save your Log.

⚠ **Note:** If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

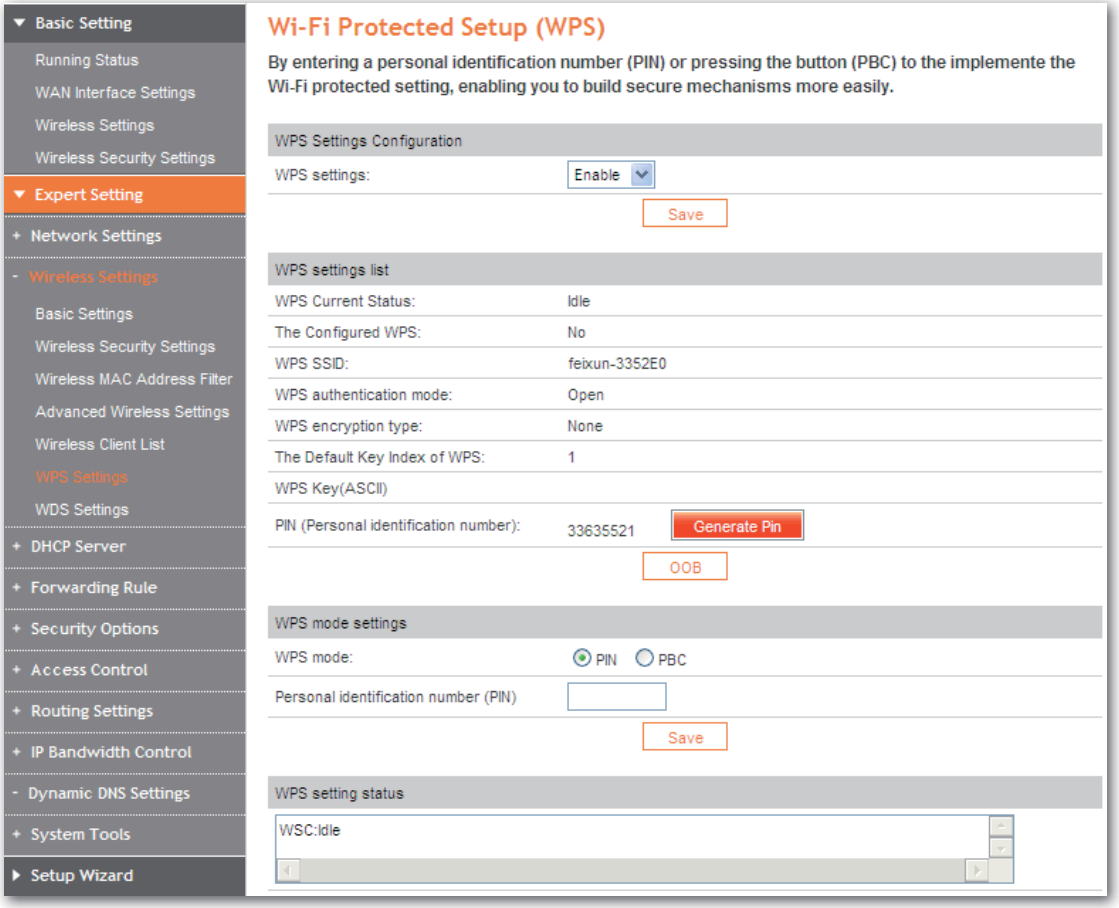
- **Wireless Client List**

Show wireless clients access to the wireless net.



- **WPS Settings**

In this page, you can configure the WPS settings, which can make your client automatically synchronize with the AP setting within several minutes and establish the connection.



WPS (Wi-Fi Protected Setting): Easy and quick to establish the connection between wireless network client and Router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

WPS Mode: Supports two ways to configure WPS settings: PBC (Push-Button Configuration) and PIN code.

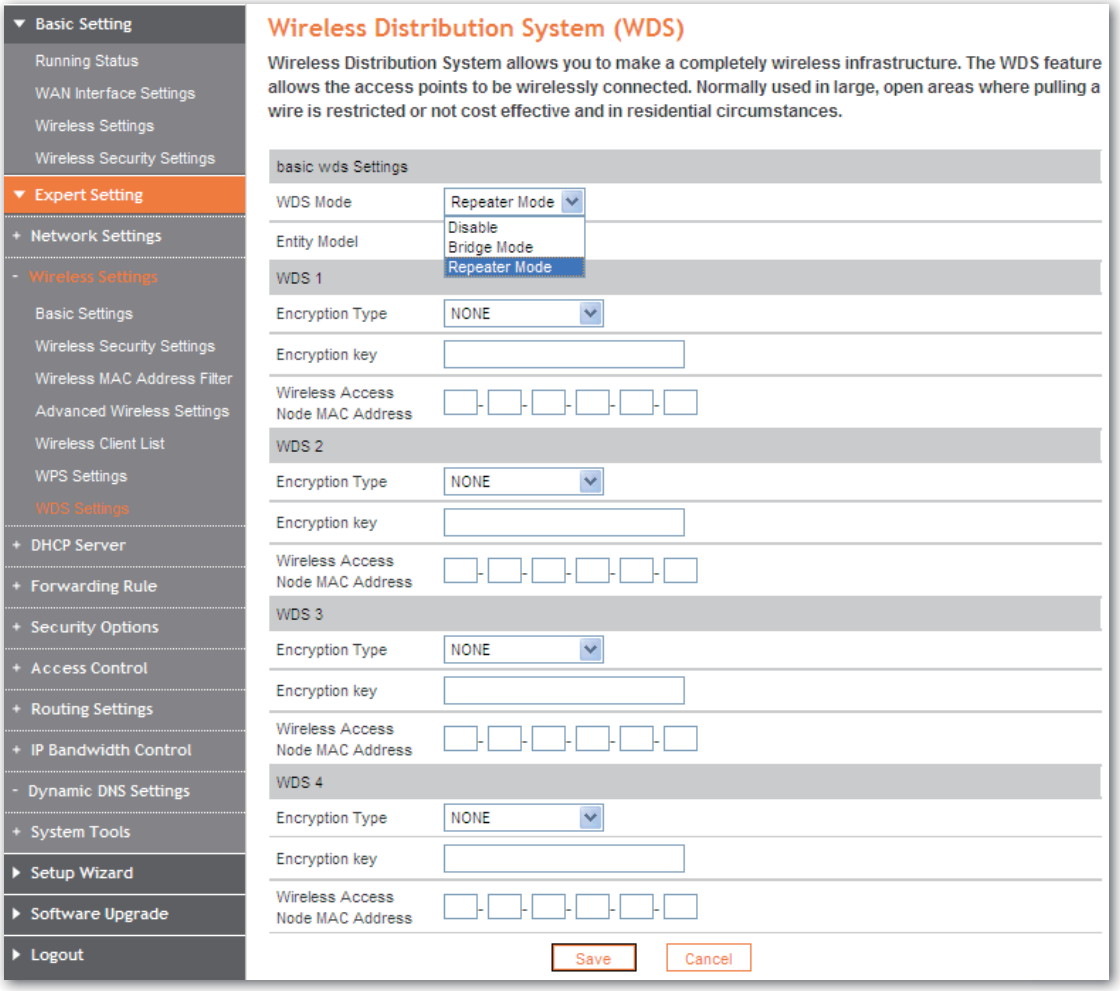
PBC: Select the **PBC** button or press the WPS button on the panel of the Router. (Press WPS button and WPS LED will blink, which means the WPS function is enabled. During the blinking time, press the WPS button on another network device, WPS LED light will become solid when the connection succeeds.)

PIN: If this option is enabled, you need to enter a wireless clients PIN code in the blank and keep the same code in the client.

Save: Click the **Save** button to save your setting.

- **WDS Settings**

In this page, you can configure the function of WDS, supporting Repeater mode, Bridge mode and Lazy mode. You'd better use the same router in order to optimize the performance.



WDS Mode: In this mode, you can expand the scope of network by combining up to four other access points together, and every access point can still accept wireless clients.

Bridge Mode: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Routers AP MAC address table or select one from the scanning table. At the same time, the connecting device should be in Lazy, Repeater or Bridge mode.

Repeater Mode: You can select the mode to extend the distance between the two WLAN devices. Functioning as a WDS repeater, the W306R connects to both a client card as an AP and to another AP. In typical repeater applications, APs connecting to other APs equipped with WDS functionality must also support WDS. In this mode, you need to add the MAC address of the connecting device into the Routers AP MAC address table and the connecting client should be in Lazy, Repeater or client mode.

Encryption Type: You can select WEP 64bits mode, WEP 128bits mode TKIP mode, AES mode for security here.

Encryption key: Enter the key, the key format according to encryption you selected.

Wireless Access Node MAC Address: Input the MAC address of another wireless router.

⚠ **Note:** Two wireless routers must use the same band, channel number, and security

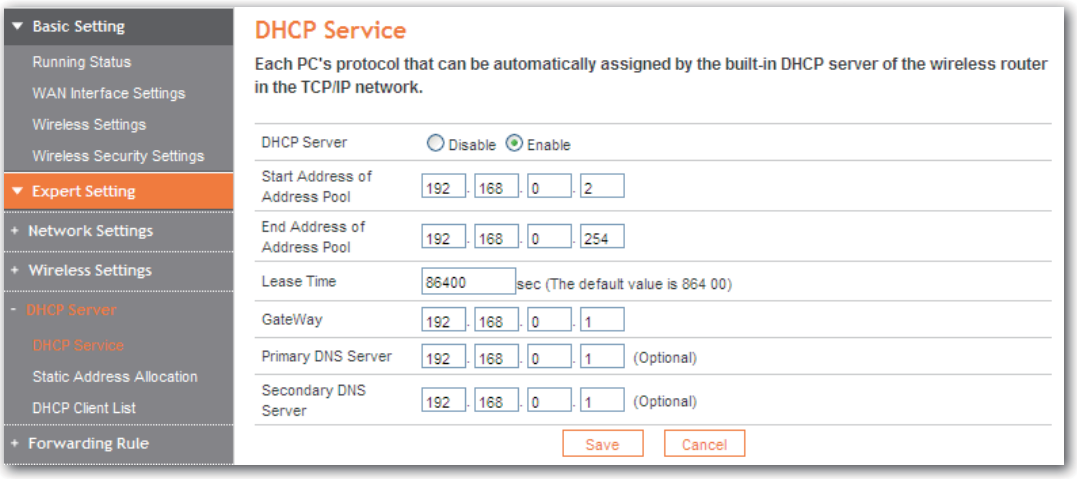
setting.

DHCP Server

The TCP/IP protocol settings include the information of the IP address, subnet mask, gateway, and DNS server. Properly configuring the TCP/IP protocol for all computers in the LAN is not easy. Fortunately, the DHCP server provides this function.

- **DHCP Service**

If you enable DHCP server of the router, the DHCP server automatically configures the TCP/IP protocol for each computer in the LAN.



Start Address of Address Pool: The first IP address that is automatically assigned by the DHCP server.

End Address of Address Pool: The last IP address that is automatically assigned by the DHCP server.

Lease Time: The time length of the corresponding IP address lease.

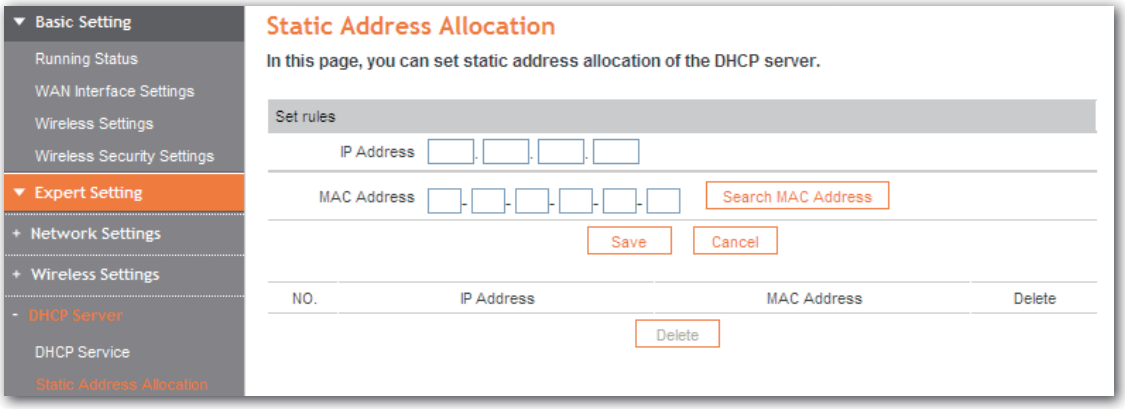
Gateway: You can enter the LAN IP address of the router. The default is 192.168.0.1. It is optional.

Primary DNS Server: Enter the information of the DNS server provided by the ISP. You can consult your ISP. It is optional.

Secondary DNS Server: If the ISP provides you two DNS servers, you can enter the IP address of the other DNS server in this field. It is optional.

Save: Click the **Save** button to save your setting.

- **Static Address Allocation**

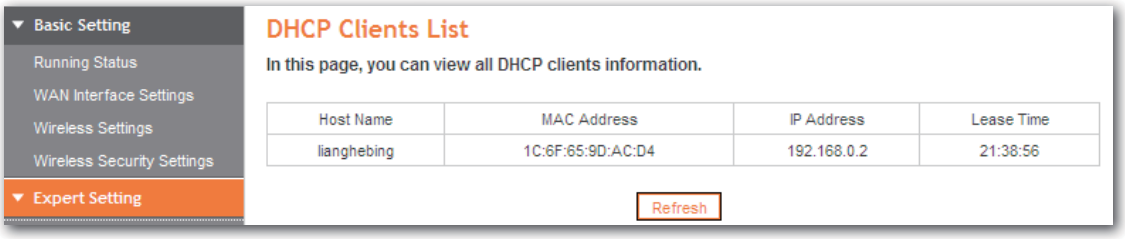


IP Address: Enter one IP address for the computer on the LAN network.

MAC Address: Enter the MAC address of the computer you want to assign the above IP address. Click **Add** to add the entry in the list.

Save: Click the **Save** button to save your setting.

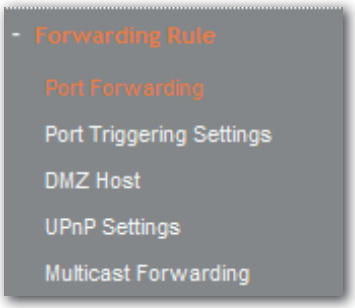
- **DHCP Client List**



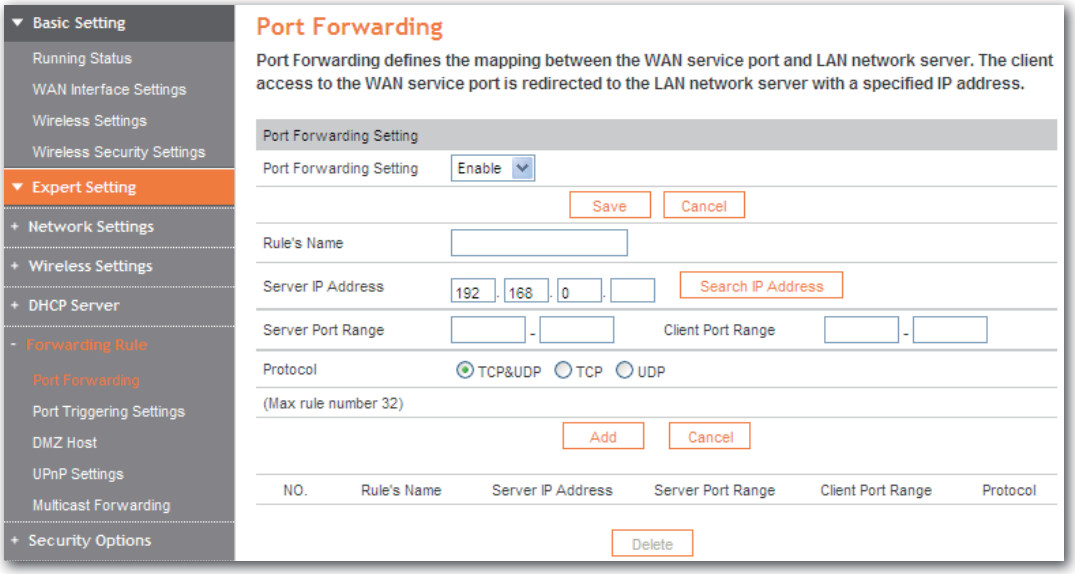
Refresh: Click to refresh the DHCP client list.

Forwarding Rule

There are four submenus under the Forwarding menu, **Port Forwarding**, **Port Triggering Setting**, **DMZ Host** and **UPnP Settings**. Click any of them, and you will be able to configure the corresponding function.



- **Port Forwarding**



Disable/Enable: To realize the function of port forwarding, select **Enable**.

Rules Name: Enter the Rules Name.

Server IP Address: Enter the IP address of the server that should receive these requests. Details please refer to the note below.

Server Port Rang: The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).

Client Port Rang: The numbers of client Ports. You can type a client port or a range of client ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).

Protocol: Select the protocol (TCP/UDP/Both) for the application.

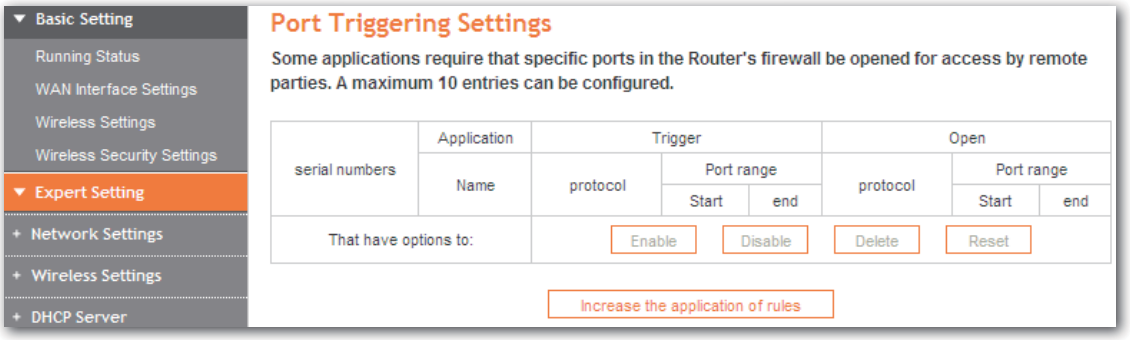
Save: Click the **Save** button to save your setting.

⚠ **Note:**

- Before using port forwarding, you should assign a static IP address to the designated server, and then enter this static IP address into router as the Server IP Address.
- Please ensure the SPI Firewall was closed before setting the port triggering. You could check the SPI Firewall settings at Expert SettingSecurity OptionsSecurity Settings.

- **Port Triggering Settings**

Choose menu **Forwarding** > **Port Triggering**, you can view and add port triggering in the screen as shown below. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.



Application Name: Describe the name of the application that being set.

Start/End Trigger Port: The port for outgoing traffic. An outgoing connection using this port will trigger this rule.

Trigger Protocol: The protocol used for Trigger Ports, TCP, UDP, or **TCP/UDP**. If you are not clear about which protocol was being used, **TCP/UDP** is recommended.

Open Port: The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule.

Open Port Protocol: The protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **TCP/UDP**. If you are not clear about which protocol was being used, **TCP/UDP** is recommended.

To modify an existing entry:

Enable: Select the number of application and click the **Enable** button to make it enabled.

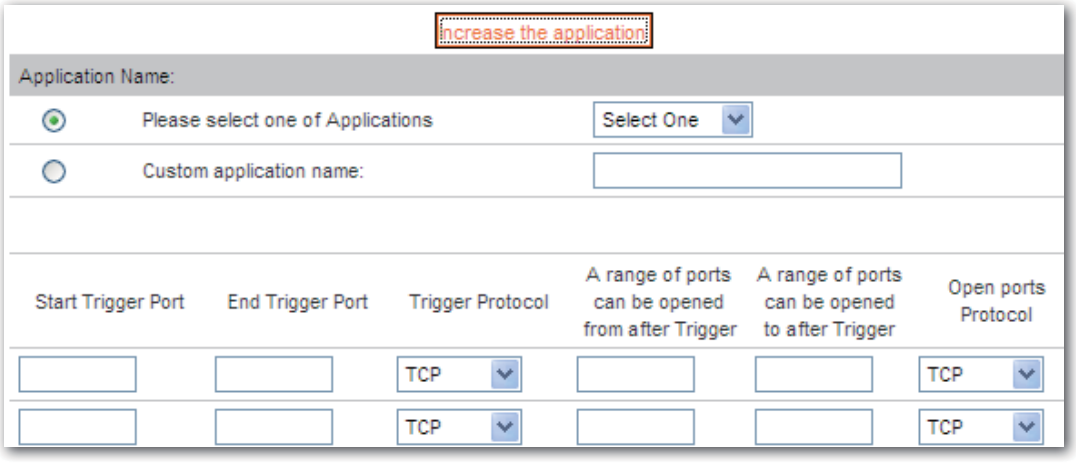
Disable: Select the number of application and click the **Disabled** button to make it disabled.

Delete: Select the number of application and click the **Delete** button.

Reset: Select the number of application and click the **Reset** button.

To add a new rule, follow the steps below:

Click **Increase the application of rules** button, the following screen appear:



Please select one of the applications: There are few common applications available such as Dailpad, MSN gaming, PC Phone etc. the blank will be automatically filled once been chosen.

Custom application name: If the application you want to add is not included, enter the blank manually.

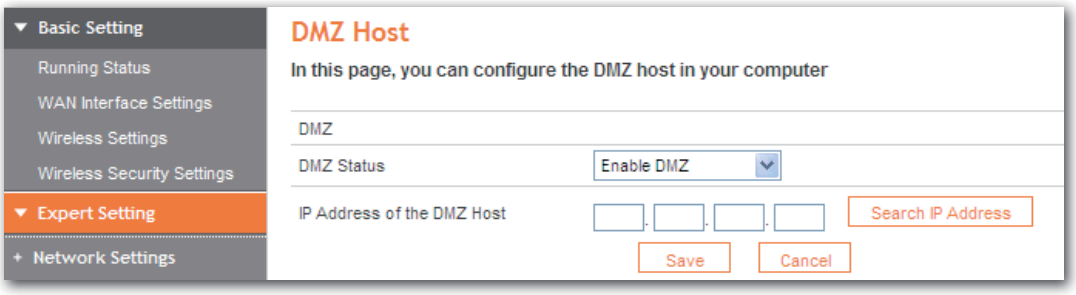
Save: Click the **Save** button to save your setting.

⚠ **Note:**

- Before using port forwarding, you should assign a static IP address to the designated server, and then enter this static IP address into router as the **Server IP Address**.
- Please ensure the SPI Firewall was closed before setting the port triggering. You could check the SPI Firewall settings at Expert Setting > Security Options > Security Settings.

- **DMZ Host**

DMZ Host forwards all the ports at the same time to one PC.



DMZ Status: Click the checkbox to choose disable or enable DMZ.

IP Address of DMZ Host: Click **Search IP Address** to clone the IP address of the computer you want to expose.

Save: Click the **Save** button to save your setting.

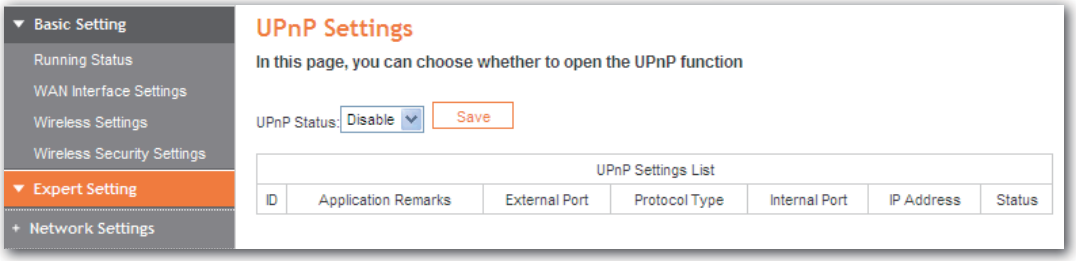
To set a DMZ host, do as follows:

1. Enter the IP address of the computer in the LAN that you want to set to a DMZ host in the DMZ Host IP Address field.
2. Select Enabled.
3. Click Save to complete the settings.

⚠ **Note:**

- Before using DMZ Host, you should assign a static IP address to the designated server, and then enter this static IP address into router as the Server IP Address.
- DMZ priority is higher than the Port Forwarding, if the DMZ open, all the port forwarding rules are not effective.

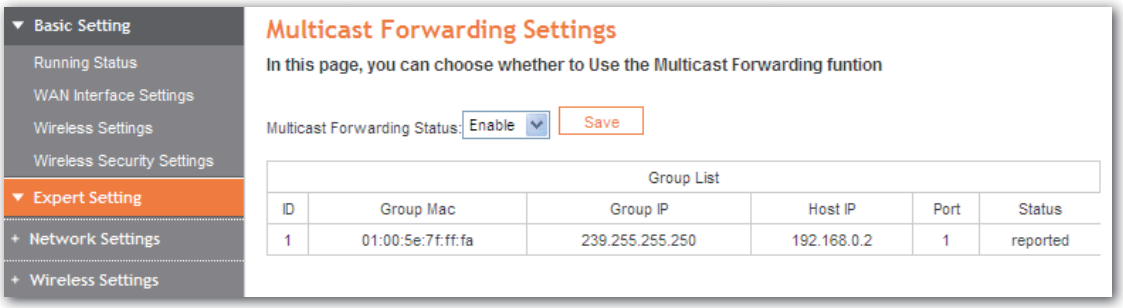
- **UPnP Settings**



UPnP: Click the checkbox to **Enable** or **Disable** the UPnP.

Save: Click the **Save** button to save your setting.

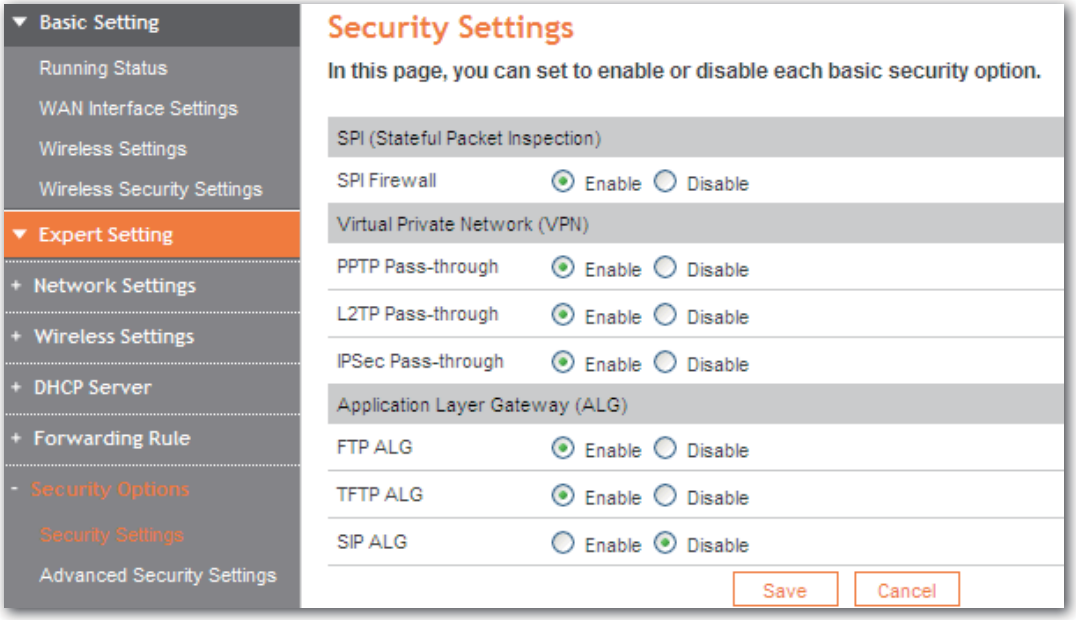
- **Multicast Forwarding Settings**



Security Options

There are four submenus under the Security Options menu: **Security Settings**, **Advanced Security Settings**, **LAN Web Management** and **Remote Web Management**. Click any of them, and you will be able to configure the corresponding function.

- **Security Settings**

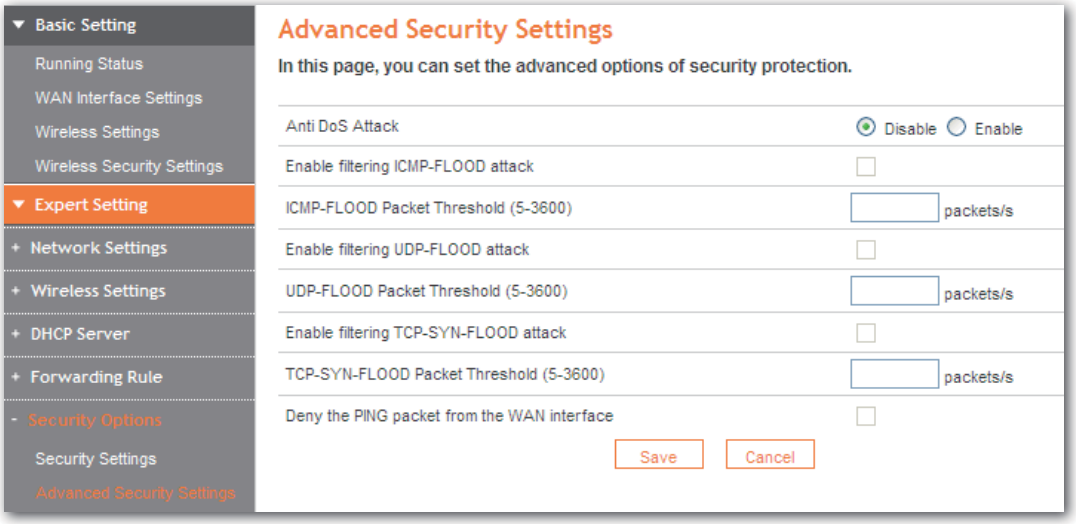


Stateful Packet Inspection (SPI): When the SPI firewall is enabled, the system refuses all requests from the Internet. Only packets that belong to connections that respond requests from the LAN and for which status database is created can pass the firewall and access to the LAN. By default, the SPI is enabled. To expose all hosts in the LAN to the Internet, you can disable SPI.

Virtual Private Network (VPN): VPN provides a safe communication method among remote computers through WAN. If a host in the LAN wants to connect to the remote VPN network through the router by using the VPN protocol, such as PPTP, L2TP, or IPSec, you need to enable the corresponding VPN pass through.

Application Layer Gateway (ALG): ALG supports that some protocols at the application layer that adopt the control/data mode, such as FTP, TFTP, and H323, help to translate network addresses and ports at the NAT gateway. You are recommended to enable this option. The Common Service Port drop-down list contains some common service ports. You can select one and click Add to add the service port to the virtual server list.

- **Advanced Security Settings**



Anti DoS Attack: Check to enable it for attack prevention.

IGMP-Flood Packet Threshold: If the number of ICMP data packets exceeds the threshold, the defense measures act immediately.

Enable filtering UDP-FLOOD attack: Select it if you want to protect against UDP-FLOOD attacks.

UDP-Flood Packet Threshold: If the number of UDP data packets exceeds the threshold, the defense measures act immediately.

Enable filtering TCP-SYN-FLOOD attack: Select it if you want 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.

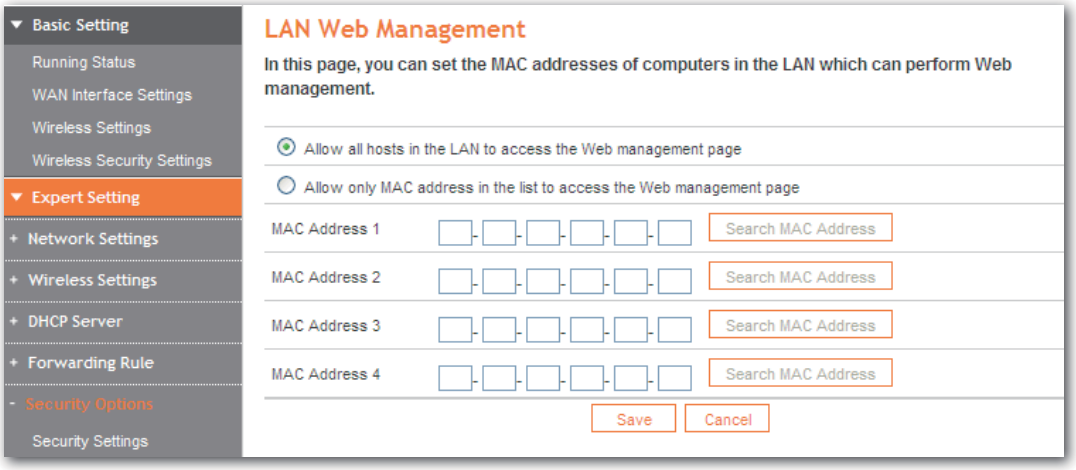
Block the PING packets from the WAN interface: If you select this option, the PC in the WAN cannot send the PING packets to the router.

Block the PING packets from the LAN: If you select this option, the PC in the LAN cannot send the PING packets to the WAN.

Save: Click the **Save** button to save your setting.

- **LAN Web Management**

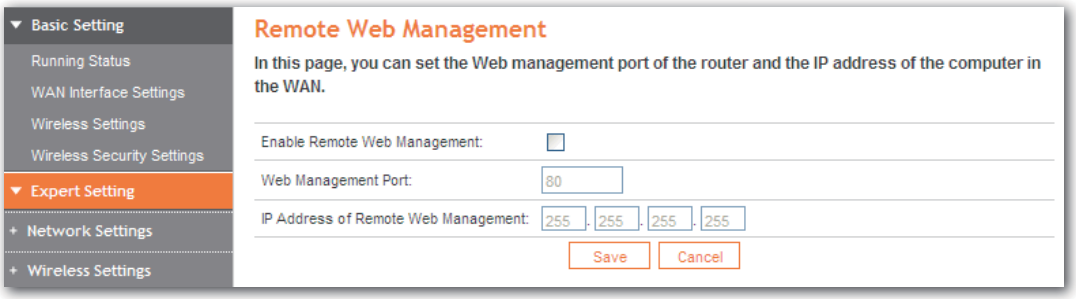
The alternative to remote web management, it is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default, so you can enter the specific MAC address of the LAN computer.



MAC Address 1/2/3/4: Enter the MAC addresses of LAN computers.

Save: Click the **Save** button to save your setting.

- **Remote Web Management**



This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the **Enable Remote Web Management**.

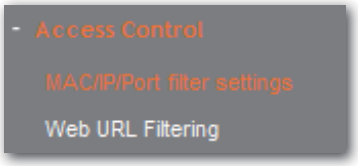
Web Management Port: The management port open to outside access the default value is 80.

IP Address of Remote Web Management: Specify the range of the WAN IP address for remote management.

Save: Click the **Save** button to save your setting.

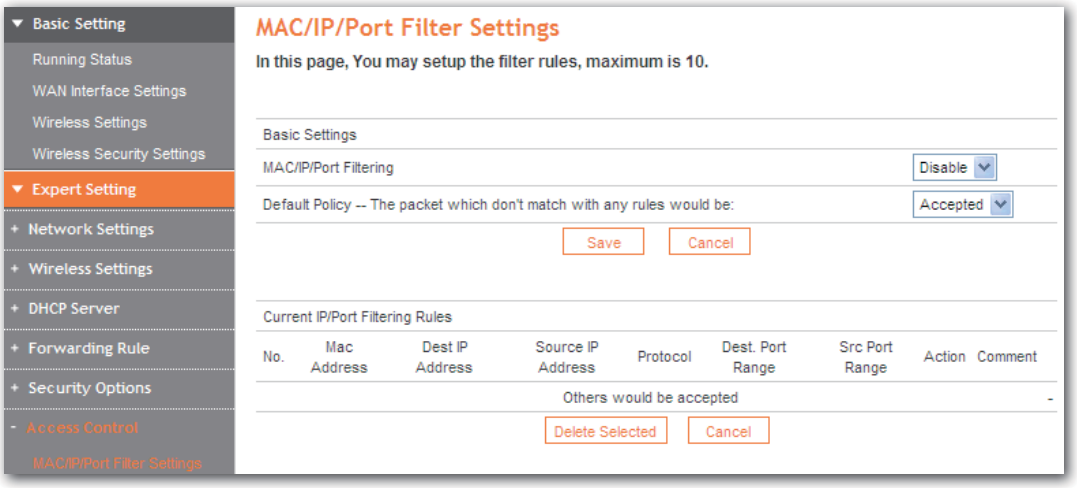
Access Control

There are two submenus under the Access Control menu. Click any of them, and you will be able to configure the corresponding function.



- **MAC/IP/Port Filter Settings**

This page is used to enable the firewall filtering function, select the filtering service or manually set the parameters that need to be filtered, such as MAC address, IP address and Port. You must set at least one filtering condition. You may also set multiple conditions or all the conditions.



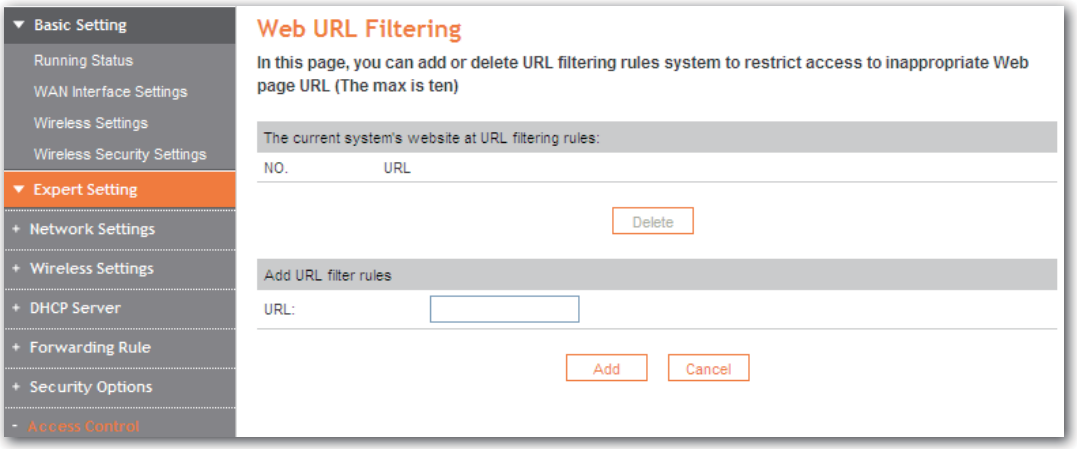
MAC/IP/Port Filtering: Select **Enabled** or **Disabled** to enable or disable filtering.

Default Policy: Accepted chose, all the packets and devices will be allowed to be passed normally, opposite action will be happened if **Dropped** was been chosen.

Current IP/Port Filtering Rules: All the existing rules will be listed below, any needed of rules deleting, please select the rules, and then click **Delete Selected**.

⚠ **Note:** Please synchronize the routers time first when selecting the timing function.

- **Web URL Filtering**

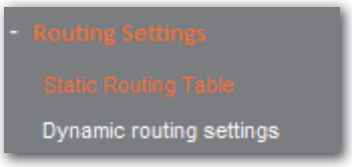


Web URL Filter: Check to enable URL filter.

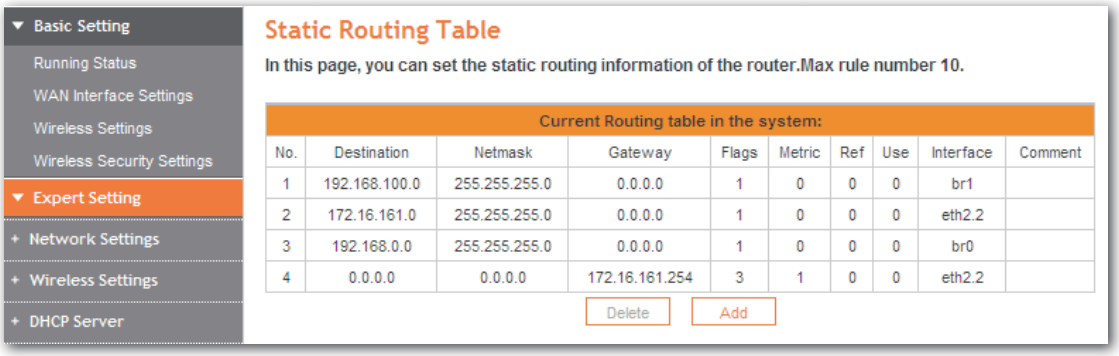
Save: Click the **Save** button to save your setting.

Routing Settings

There are two submenus under the Routing Setting menu. Click any of them, and you will be able to configure the corresponding function.

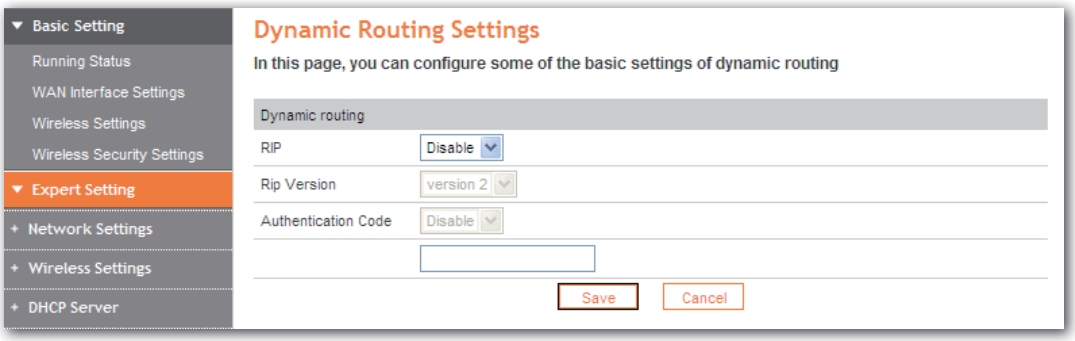


- **Static Routing Table**



The main duty for router is to look for a best path for every data frame, and transfer this data frame to destination. So, it is essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.

- **Dynamic Routing Settings**



RIP: The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. Choose **Enable** dynamic routing need to be activated.

Rip Version: Choose the version of RIP.

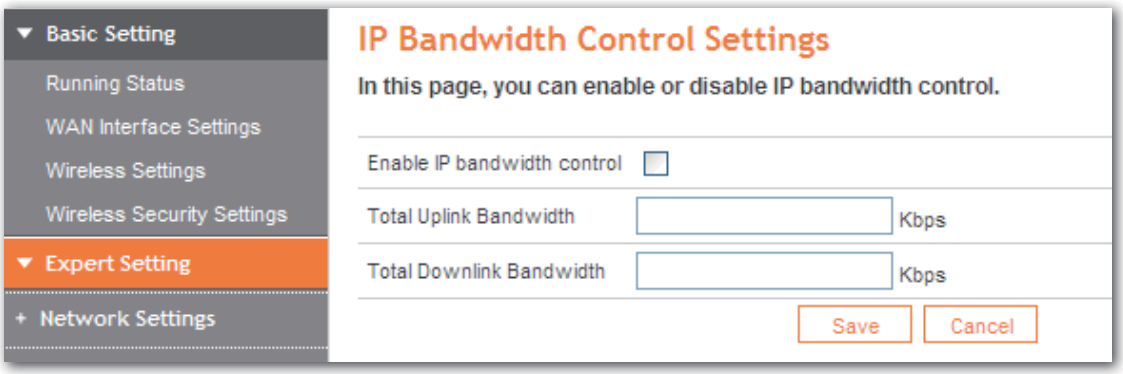
Authentication Code: Choose the encrypt method used between routers.

Save: Click the **Save** button to save your setting.

IP Bandwidth Control

There are two submenus under the IP Bandwidth Control menu. Click any of them, and you will be able to configure the corresponding function.

- **IP Bandwidth Control Settings**



Enable IP bandwidth control: If you select it, the bandwidth control rule takes effect.

Total Uplink Bandwidth: The rate of uploading through the WAN interface.

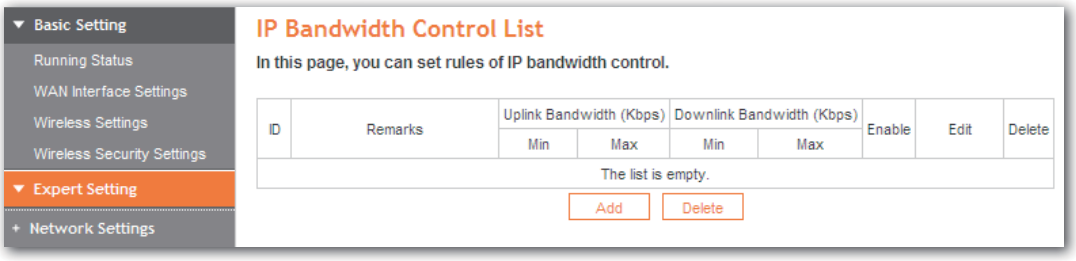
Total Downlink Bandwidth: The rate of downloading through the WAN interface.

Save: Click the Save button to save your setting.

⚠ **Note:**

- The 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, consult your broadband provider.
- After finishing the settings, click the Save button to apply the settings.

- **IP Bandwidth Control List**



Enable IP bandwidth control: If you select it, the bandwidth control rule takes effect.

Total Uplink Bandwidth: The rate of uploading through the WAN interface.

Total Downlink Bandwidth: The rate of downloading through the WAN interface.

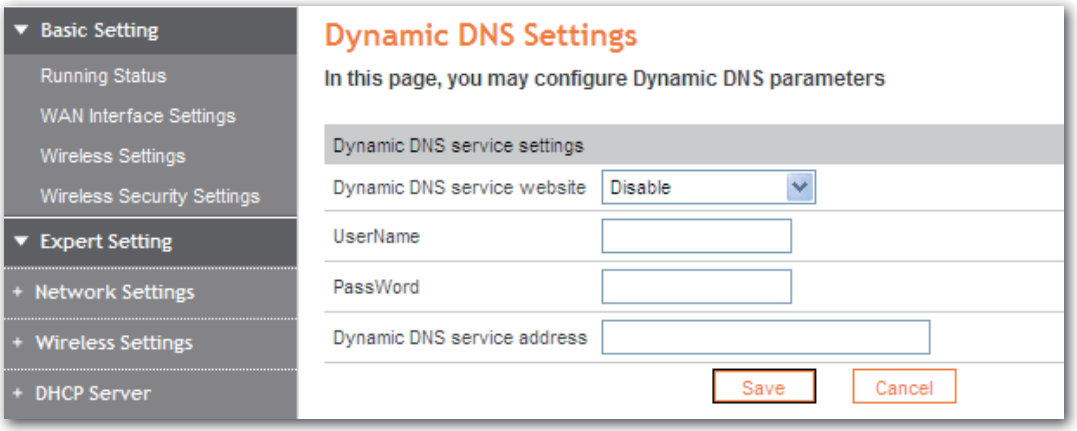
Bandwidth setting: The min. rate can be zero, the sum of all items min. rate should be

≤ the master bandwidth. The max rate must > 0. If the max rate is larger than the master bandwidth, the rule will use master bandwidth instead.

Save: Click the **Save** button to save your setting.

Dynamic DNS Settings

The **DDNS (Dynamic Domain Name System)** is supported in this router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select Enable and a DDNS service provider to sign up.



Dynamic DNS service website (DDNS): Select to **enable** or **disable** the DDNS service.

Username: Enter the username the same as the registration name.

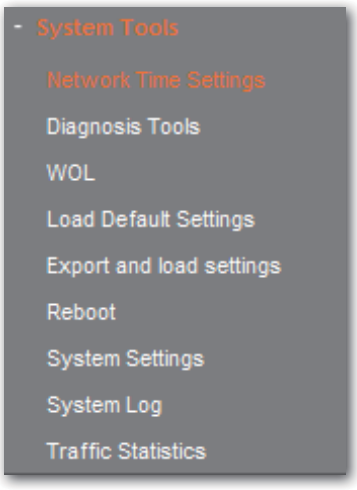
Password: Enter the password you set.

Dynamic DNS service address: Enter the DDNS service address.

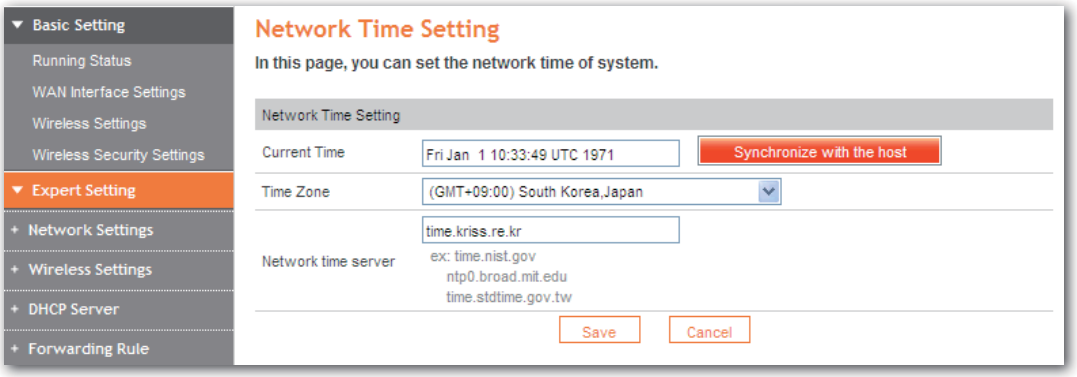
Save: Click the **Save** button to save your setting.

System Tools

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.



- **Network Time Settings**



Current time: Show the current time.

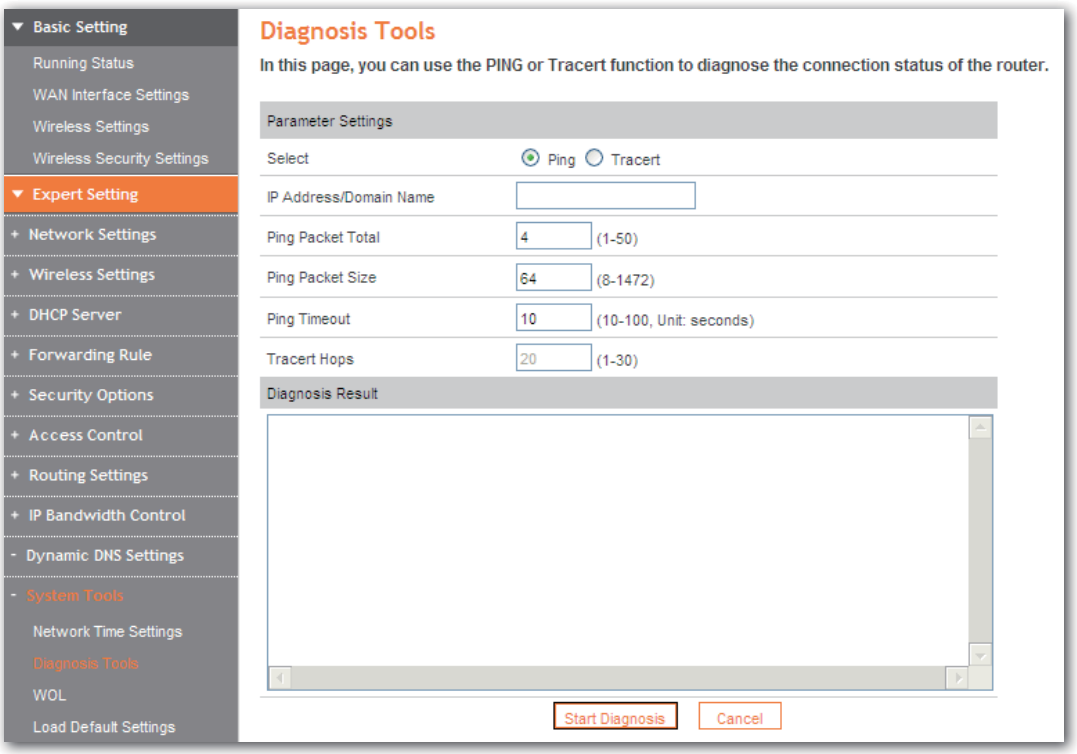
Time Zone: Select your time zone from the drop-down menu.

Network time server: To set NTP server.

Save: Click the Save button to save your setting.

⚠ **Note:** The system will Synchronous with the Network Time Server every hour after saving, and it will affect the WAN dial-up on demand.

- **Diagnosis Tools**



Select: Select **Ping** or **Tracert**.

IP Address/Domain Name: The destination IP address or domain name.

Ping Packet Total: The number of transmitted data packet when Ping operation is carried out.

Ping Packet Size: The size of transmitted data packet when Ping operation is carried

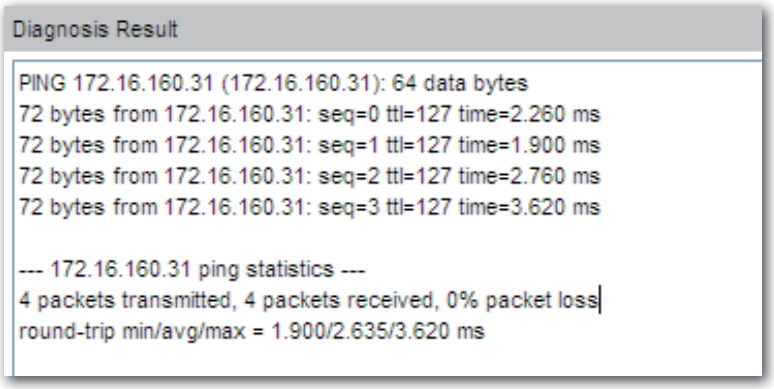
out.

Ping Timeout: The timeout time of the ping operation.

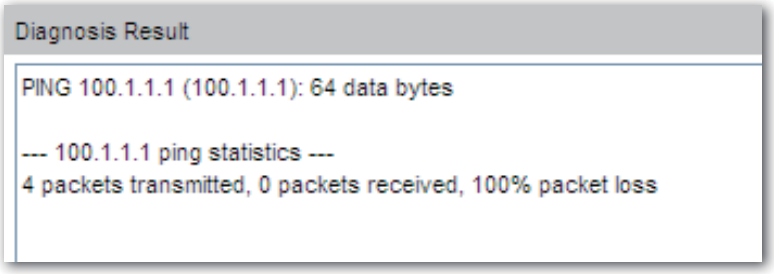
Tracert Hops: The hops of tracert.

Click **Start Diagnosis** button, the selected ping or tracert testing will be started.

Below is a Ping diagnosis example that router has been connected to IP 172.16.160.31:

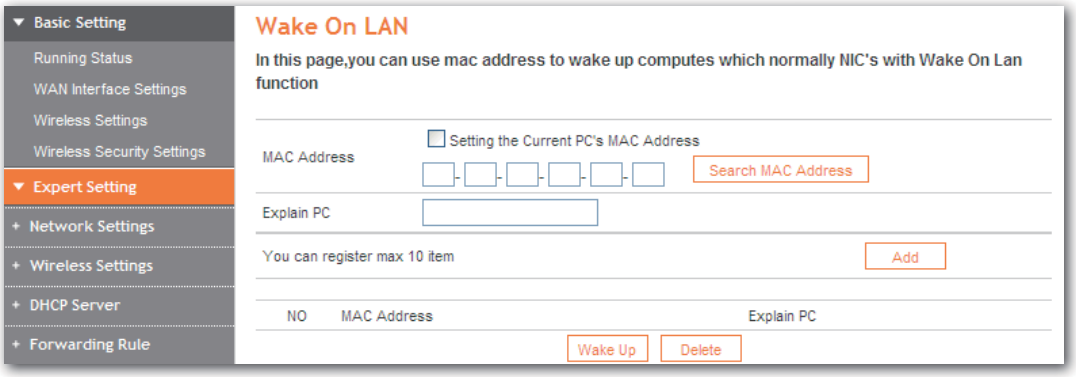


Below is a Ping diagnosis example that router has failed to connect to IP 100.1.1.1:



- **Wake On LAN**

WOL broadcasts so called Magic Packet Frames across a network to wake up hardware that understands such packets. These are normally NICs with Wake On LAN function.



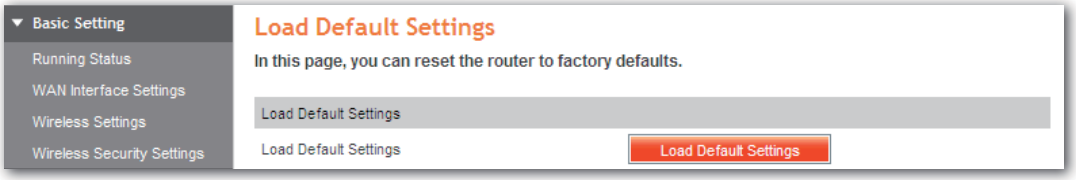
MAC Address: Increase a MAC address to wake the computer on.

Explain PC: Description about the computer.

Add: Click the **Add** button to finish, and the computer will display in the list.

Select one or more computers in the list, and click the **Wake Up** button, these computers will be waked up.

- **Load Default Settings**



Load Default Settings: Click this button to restore to factory default settings.

User Name: admin

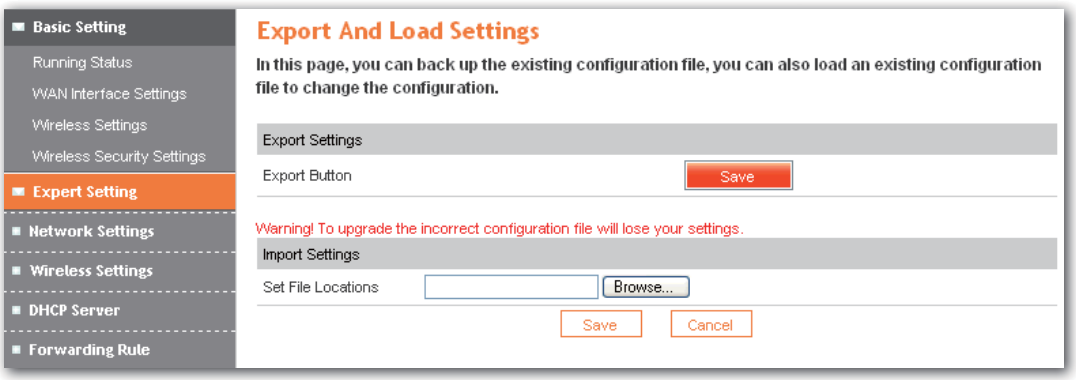
Password: admin

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

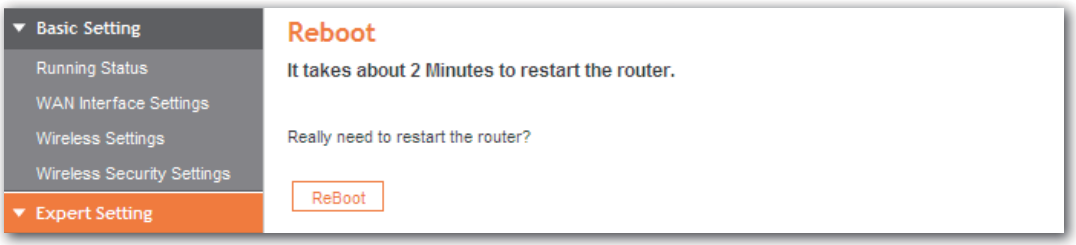
⚠ **Note:** After restoring to default settings, please restart the device, then the default settings can go into effect.

- **Export and Load Settings**



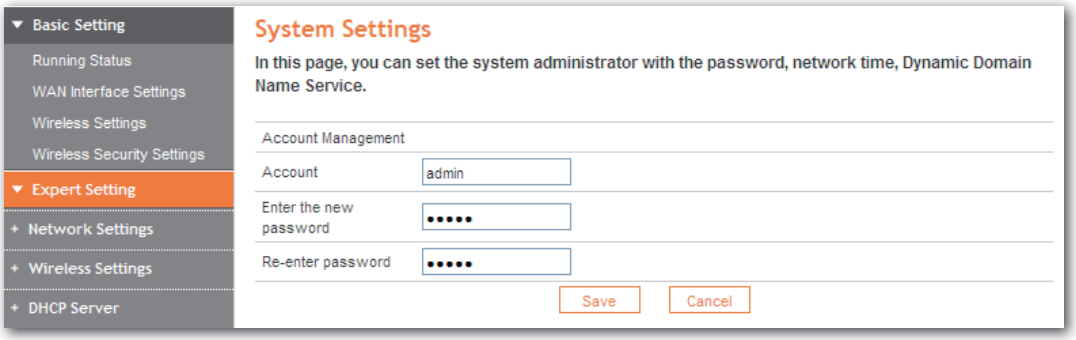
- **Reboot**

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.



Reboot the router: Click this button to reboot the device.

- **System Settings**



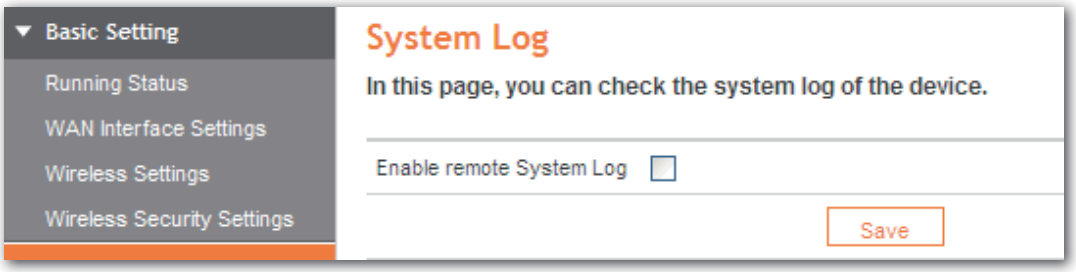
Account: Enter the username you set.

Enter the new Password: Enter the password you set.

Re-enter password: Re-enter the password you set.

- **System Log**

The section is to view the system log. Click the **Refresh** to update the log. Click **Clear** to clear all the shown information. If the log is over 150 records, it will clear them automatically.



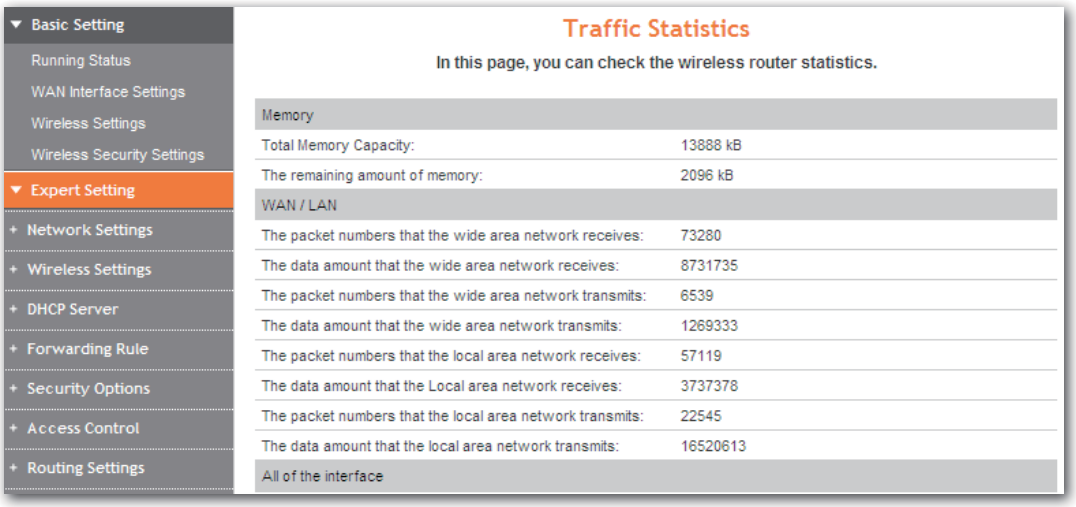
Enable remote System Log: Check the radio button to enable remote System Log.

Save: Click the **Save** button to save your Log.

Clean: Click the **Clear** button to clear all shown information.

- **Traffic Statistics**

This page used to display the current system memory usage, WLAN, LAN and WAN networks to send and receive data packets to the number.

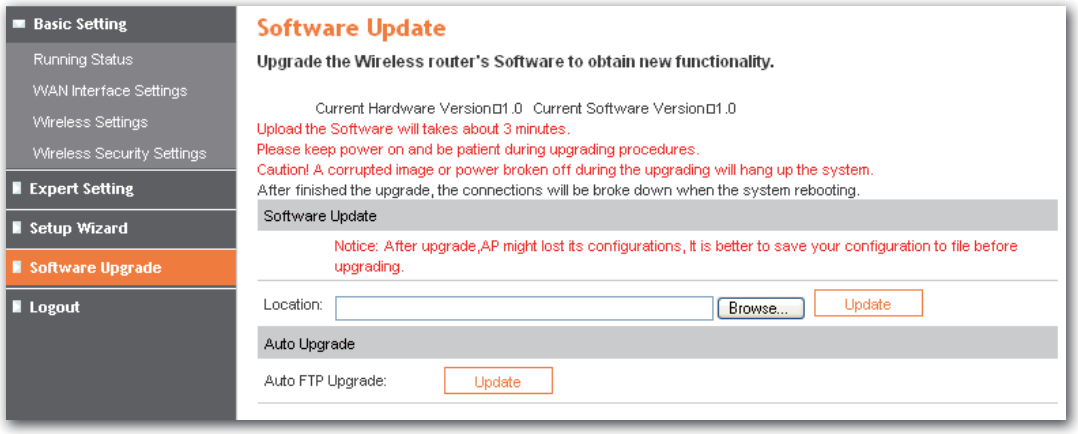


▪ Setup Wizard

Please find the section of **Setup Wizard**.

▪ Software Upgrade

Software Update



You can choose to upgrade manually by:

1. Click the **Browse** button to browse the directory where you download the software upgrade files.
2. Click **Update** button to start upgrade.

Or you can choose to upgrade automatically by click the **Update** button, the router will download and upgrade automatically from FTP server.

Router will auto reboot when the upgrade finished.

⚠ **Note:**

- Router might be changed to factory default settings after upgrade, please backup in advance.
- During the updating, please do not turn off the power.
- Please make sure the software version is matching with the existing hardware.

▪ Logout

Click to logout from the router configuration web.

Specification

Wireless	
Standard	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, CSMA/CA with ACK
Wireless Signal Rate	11n: 300Mbps 11g: 54Mbps 11b: 11Mbps
Frequency Range	2.4-2.4835GHz
Wireless Transmit Power	< 20dBm
Modulation Type	OFDM/CCK/16-QAM/64-QAM
Receiver Sensitivity	300M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER
Security	64/128-bit WEP, WPA/WPA2-Enterprise, WPA /WPA2-Personal (TKIP/AES)
Support Operating System	Microsoft® Windows® 98SE, NT, 2000, XP, Vista and Windows 7
Hardware	
Connection	4 x 10/100Mbps LAN ports 1 x 10/100Mbps WAN port Power connector
Button	Power button WPS button Reset button
Power Supply	12VDC, 0.5A
Dimension (W x D x H)	150 x 144 x 28mm
Package	
Contents	1× Wireless N Router 1× Power Adapter 1× CD-ROM 1× Quick Installation Guide 1× RJ-45 Ethernet Cable
Others	
Operating Temperature	0°C~40°C (32°F~104°F)
Storage Temperature	-40°C~70°C (-40°F~158°F)
Relative Humidity	10% ~ 90%, non-condensing
Storage Humidity	5% ~ 95%, non-condensing
Certification	FCC, CE, RoHS

Appendix A: Troubleshooting

1. **Feixun Setup cannot find my Router.**

   If Feixun Setup is not able to communicate with your Router during installation, please check the following items.

   - Ensure that the Router is on. The front-panel light should be on.
   - Make sure the computer is connected to the routers LAN port via cable.
   - Make sure the routers WAN port is connected to DSL modem via cable.
   - There may be firewall software on your computer preventing an outgoing connection. You may choose to temporarily disable this software before attempting setup.
   - Unplug the Routers power supply for 10 seconds, then plug it back in.

2. **The DSL telephone line does not fit into the Routers Internet port.**

   The Router does not replace your modem. You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer. Follow the QIG to install your router.

3. **I cannot enter into the routers web page or cannot login.**

   - Check if the computer is connected to the router.
   - Configure your computers IP address, details please refer to the section of Configure the Computers IP Address in this manual.
   - If you cannot login because of forgetting username and password, please reset router by pressing reset button for 5 seconds, and then login with default username and password (admin/admin).

4. **The computer cannot connect to the Internet.**

   - Make sure that the Power LED, WAN LED, and Wireless LED are on; the LAN LED you connected is on or blinking.
   - Make sure the DSL/cable modem is connect to the Router correctly.
   - Make sure to enter correct password. If you have forgotten the password, please reset the router by pressing reset button.
   - Reconnect all of the devices on your network if you still cannot link to the Internet.

5. **The computer cannot connect to the network wirelessly.**

   At first, please make sure you could log on the Internet successfully by cable (detailed operations please refer to Question 3), and then do the followings to check the wireless connection:

   - If you are far from the Router, you might try moving closer to see if you might have been out of range.

- Search available networks and choose your network. If your network SSID is not listed in, please connect to Router via a network cable, visit 192.168.0.1 and ensures the Broadcast SSID is enabled. This setting can be found on the Wireless Settings page.
- Make sure the wireless network name or SSID is the same on both the computer and the Router.
- If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router.

6. **I've installed this new Router and some of my network clients (computers, game consoles etc.) are unable to connect.**

   Your new Router came pre-configured with a network name and no password. All clients must use this network name to connect wirelessly to your Router. You will need to find the network settings on your client, and select the network name from the list of available networks to join the wireless network. Details please refer to your client (computer, game consoles etc.).

Appendix B: Certification

▪ FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution

- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

▪ CE Mark Warning

Marking with the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

⚠ **Note:** Please don't use the product outdoors in France.

Appendix C: Glossary

- **802.11b:** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g:** Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System):** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol):** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone):** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System):** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name:** A descriptive name for an address or group of addresses on the Internet.
- **DSL (Digital Subscriber Line):** A technology allowing data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider):** A company that can provide access to the Internet.
- **MTU (Maximum Transmission Unit):** The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation):** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet):** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID (Service Set Identification):** It is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy):** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi:** A trade name for the 802.11b wireless networking standard, given by the Wireless

Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

- **WLAN (Wireless Local Area Network):** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Appendix D: Technical Support

Please contact Feixun technical support through Feixun website:

www.feixun.com.cn

Support via E-mail:
support@feixun.com.cn

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. FWR-734N)
- Hardware version (e.g. Ver.: A1.0)
- Serial number (S/N)

All these information can be found on the label at the bottom of your product.

www.feixun.com.cn

Shanghai Feixun Communication Co., Ltd.