

# Portable Router

## User Manual

Portable Router .....	1
Chapter1 Introductions .....	3
1.1 Introductions .....	4
1.2 Features .....	4
1.3 Specifications .....	4
Chapter2 Quick Start Guide .....	5
Chapter3 Software installation .....	12
3.1 Basic Settings .....	12
3.1.1 WAN Settings .....	12
3.1.2 MAC Clone .....	14
3.1.3 LAN Settings .....	16
3.2 Wireless Settings .....	16
3.2.1 Basic Settings .....	16
3.2.2 Wireless Encryption .....	17
3.2.3 Advanced Settings .....	19
3.2.4 MAC Filter .....	20
3.2.5 WPS Settings .....	21
3.2.6 Wireless Client List .....	21
3.3 HCP Server .....	21
3.3.1 DHCP Server .....	21
3.3.2 DHCP Allocation List .....	22
3.4 Security Settings .....	23
3.4.1 Firewall Settings .....	23
3.4.2 Access Control List .....	23
3.4.3 MAC Filter .....	27
3.4.4 Domain Filter .....	29
3.4.5 IP & MAC Binding .....	30
3.4.6 Remote WEB Management .....	31
3.4.7 Advanced Security Settings .....	32
3.5 Advanced Settings .....	33
3.5.1 DDNS .....	33
3.5.2 WDS .....	34
3.5.3 UPnP Settings .....	35
3.5.4 Virtual Server .....	35
3.5.5 DMZ Settings .....	37
3.5.6 Special Application .....	38
3.6 System Tools .....	39
3.6.1 Time Settings .....	39
3.6.2 Password Modify .....	39
3.6.3 Backup & Restore .....	40
3.6.4 Firmware Upgrade .....	41
3.6.5 Reboot .....	41
3.6.6 Factory Defaults .....	41
3.7 System Status .....	42

3.7.1 Running Status .....	42
3.7.2 Traffic Statistics.....	错误！未定义书签。
3.7.3 Client List.....	43
3.7.4 Syslog.....	43
Help.....	44

# Chapter1 Introductions

## 1.1 Introductions

This Portable Router, it set of router, firewall, wired and wireless network connection functions, it is designed to meet high-speed Internet access needs of the small business, office and home wireless connection.

## 1.2 Features

- ▶ Compliant with IEEE802.3, IEEE802.3u, IEEE802.b/g/n standards.
- ▶ Supports USB power supply.
- ▶ Supported protocols: TCP, UDP, IP, ARP, ICMP, DHCP, PPPoE, DNS, PAP/CHAP.
- ▶ Supports PPPoE (DSL and Cable modem), dynamic IP, static IP broadband access.
- ▶ Supports IP Filtering, Domain Filtering, MAC Filtering, block QQ and MSN by settings.
- ▶ Supports Virtual Server, Special Application, UPnP, DMZ host ideal for creating a personal website within your LAN.
- ▶ Supports 64-bit and 128-bit WEP encryption, WPA-PSK/WPA2-PSK (TKIP/AES) standard.
- ▶ DC 5V, 2A power supply, and with a 1500mAH high-capacity Li-ion battery, can be recharged several times.
- ▶ Supports firmware upgrade, easy local or remote management via HTTP, TELNET.

## 1.3 Specifications

Protocols		IEEE802.11b/g/n, IEEE802.3, IEEE802.3u, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE,
Ports	WAN/LAN (Micro USB to RJ45)	This is one 10/100M RJ45 Auto-Negotiation port, can configurable as WAN or LAN via firmware.
Antenna	Frequency	2.4~2.462GHz
		IEEE802.11n:150Mbps (maximum) IEEE 802.11g: 54/48/36/24/18/12/9/6(Auto-Negotiation)

		IEEE 802.11b : 11/5.5/2/1M(Auto-Negotiation)
Channel	1~14	
Spread Spectrum	DSSS(Direct Sequence Spread Spectrum)	
Data Modulation	DBPSK, DQPSK, CCK and OFDM(BPSK/QPSK/16-QAM/64-QAM)	
Transmission Rate	As far as 50 meters indoors	
Antenna	Internal Antenna	
Dimension	85x48x10(mm)	
Operating Environments	Operating Temperature:0°C~40°C;Operating Humidity 10%~90% No-condensing. Storage Temperature:-40°C~70°C ; Storage Humidity 5%~90% No-condensing	
Power Supply	DC 5V/2A, USB	

## Chapter2 Quick Start Guide

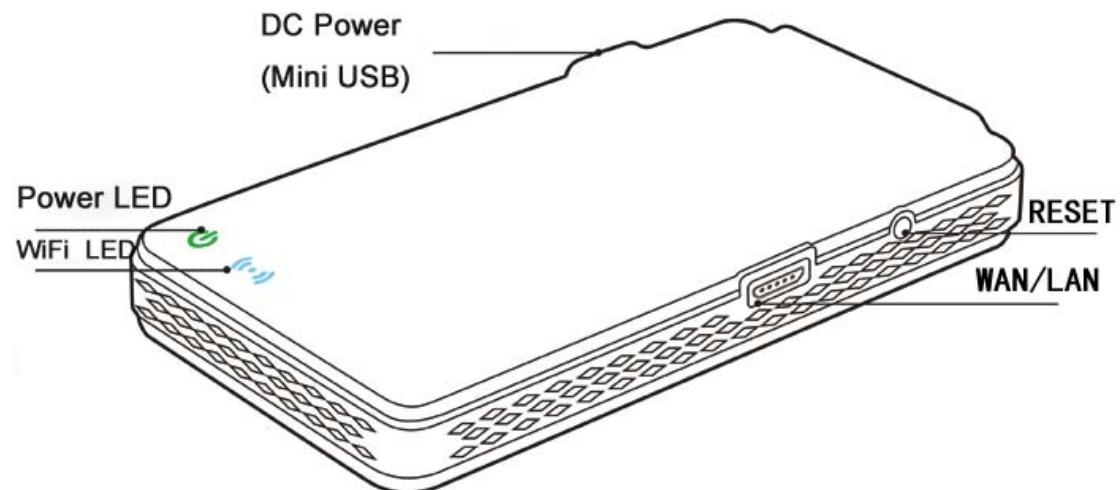
### Packages

The following items should found in your package:

- Portable Router
- Battery
- USB Charging Cable
- RJ45 Cable Connector
- Quick Start Guide,
- Warranty card.

If any of above items are damaged or missing, please contact with your distributor.

## Panel Description



## Functions

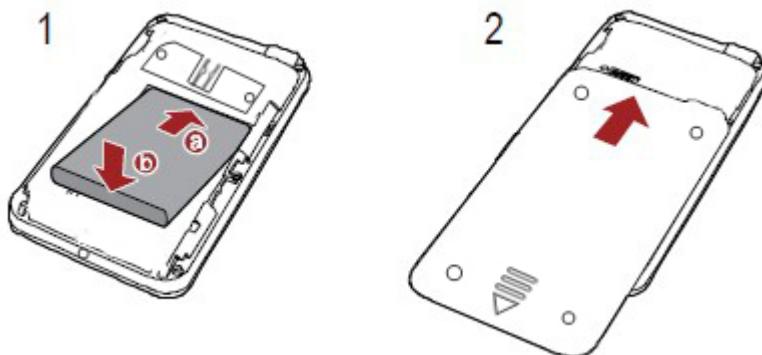
Name	Description
DC Power	Mini USB interface, power and charge Portable router
USB	Standard USB2.0 port, used to connect the modem
ON/OFF	Power Switch, used to turn on /turn off router
RESET	With the Router powered on, use a pin to press and hold the RESET button (about 5 seconds) until the WiFi LED off.
WAN/LAN	MICRO USB port, is where you will connect LAN or xDSL/cable Modem, or Hotel network, can configured as WAN/LAN.

## LED

LEDs	Status	Description
Power LED	Green in flashing	Powered by battery, fully charged
	Red	Powered by USB or low power
	Amber	battery is charging
WiFi LED	Blue	WiFi is available
	Blue in flashing	WiFi is transmission data

## Install battery

According to following page to install battery, Note installation direction of the battery

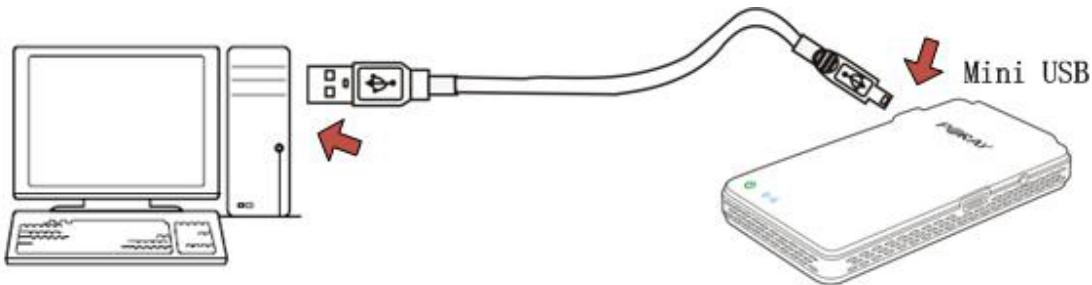


## Start Router

Turn on the power switch, the router will boot automatically, when started, Power LED turn to Green and flashing, WiFi LED turn to Bule and flashing.

## Charging the Router

The router can powered by battery, also can powered by USB directly, put one end of the USB charging cable into computer's USB port, put another end of USB charing cable into Rouer's DC power, as bellow:

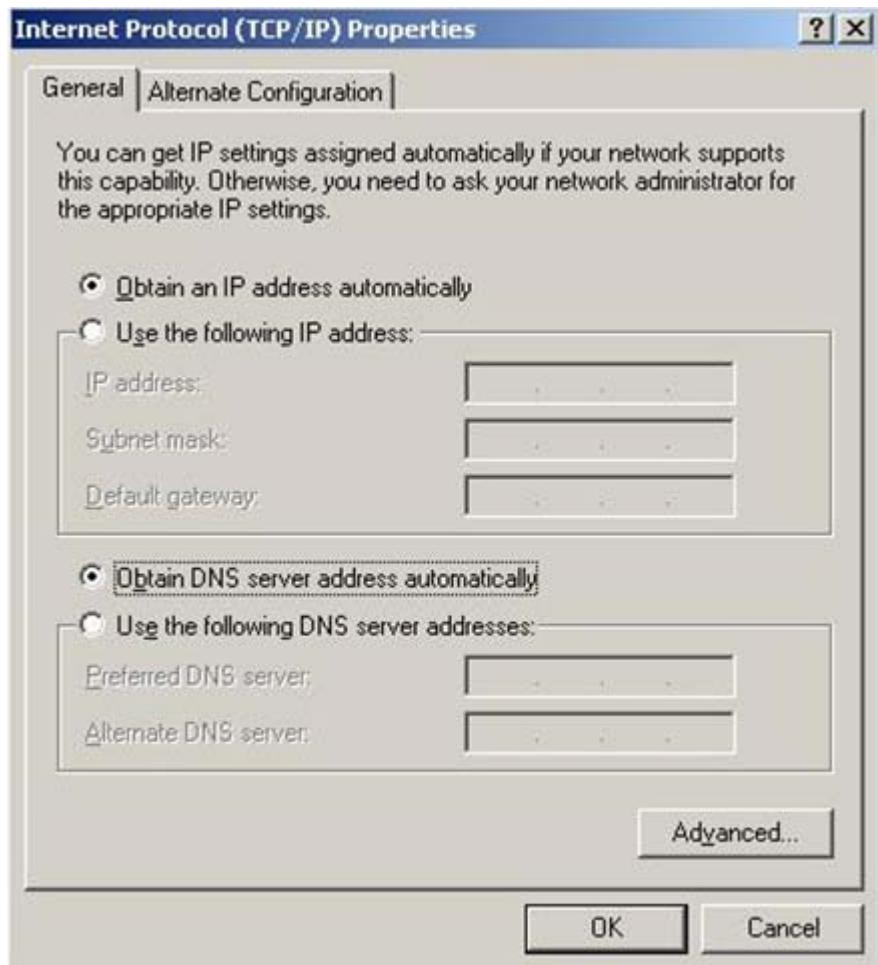


**Attention:** Be sure to use original accessories, when charging, note the location of the router charging port, plug the wrong charger interface or using non-original parts cause damage to the router will not fall free warranty!

## Configure the Router

[Windows XP]

Choose **Start > Control Panel**, double-click **Network Connections**, right-click **Local Area Connection**, choose **Property**, double-click **Internet Protocol (TCP/IP)**, select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then your computer can obtain IP address and DNS from the router automatically.



## Access Router's WEB

Open a web-browser and type in the default address <http://192.168.100.1> in the address field of the browser, after a moment, a login windows will appear, shown as below, click OK button to login in Router's default page.



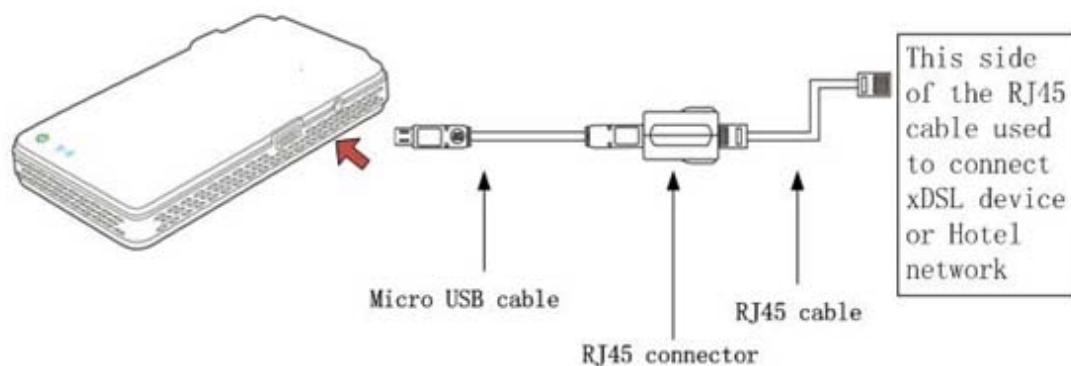
## Parameters settings

the router support Static IP, Dynamic IP, PPPoE, click “Basic Settings” on the left side of WEB page, so you should first choose Router’s operating mode.

### 1. PPPoE

Most DSL provides PPPoE (Point-to Point Protocol over Ethernet) to establish Internet connection for end-users, to setup the router, you need to enable PPPoE on the router’s web-based setup page, choose “PPPoE” mode, enter Username and Password provided by your ISP, the fields are case sensitive, click OK to save settings.

Return to **System Status >Running Status**, check PPPoE says “connected”, if it’s connected, the PPPoE connection is active, you should able to access Internet via xDSL, click “disconnect” button to disconnect current Internet connection.



## 2. Static IP

When you have the fixed IP parameters given by your ISP, please choose "Static IP", the Static IP settings page will appear, parameters needed to input including IP Address, Subnet Mask, Default Gateway, MTU, Primary DNS, Secondary DNS, if you don't know these parameters, please contact with your ISP.

## 3. Dynamic IP

Most of the hotels and the hotel's network providing a dynamic IP broadband service, On dynamic IP mode, the Router's WAN/LAN port is configured as WAN port, click "Basic settings> WAN Settings", select Dynamic IP mode, then click save button, retrun to "System Status > Running Status", if the IP Address parameters is displayed here, that shows the Router has obtained the IP Address form other network successfully.

System Status > Running Status			
WAN Status			
DHCP	Connected	Release	Refresh
IP address	192.168.0.109		
Subnet Mask	255.255.255.0		
Default Gateway	192.168.0.1		
Primary DNS Server	192.168.0.1		
Secondary DNS Server			
DHCP Lease Time	01:59:57		
MAC Address	00:1E:23:03:0D:37		
Online Time	00:00:01		
Current System Time	05/09/2011 Mon 09:29:38		
firmware version	V3.05-2011Apr8		
WLAN Status			
Mode	802.11b/g/n		
SSID	3G ROUTER		
Channel	3		
MAC Address	00:1E:23:03:0D:38		
LAN Status			
IP address	192.168.100.1		
Subnet Mask	255.255.255.0		
DHCP Server	enable		
MAC Address	00:1E:23:03:0D:36		
			Refresh

# Chapter3 Software installation

## 3.1 Basic Settings

### 3.1.1 WAN Settings

#### 1. Static IP

If your ISP provides a static or fixed IP address, Subnet Mask, Default Gateway and DNS setting, please select **Static IP**, the Static IP settings page will appear, parameters needed to input including IP Address, Subnet Mask, Default Gateway, MTU, Primary DNS, secondary DNS, if you don't know these parameters, please contact with your ISP in local.

**Basic Settings > WAN Settings**

Wan Settings	
<input checked="" type="radio"/> Static IP Address	
<input type="radio"/> Dynamic IP Address	
<input type="radio"/> PPPoE	
<input type="radio"/> 3G Dial-up	
<b>Parameters Settings</b>	
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MTU	1500 (576~1500)
<b>DNS Address</b>	
Primary DNS	0.0.0.0 (optional)
Secondary DNS	0.0.0.0 (optional)
<b>Save</b> <b>Cancel</b>	

- IP Address: Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask: Enter the subnet mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- Default Gateway: (Optional) Enter the gateway IP Address in dotted-decimal notation provided by your ISP.
- MTU: The normal MTU (maximum transmission Unit) value for most Ethernet networks is 1500 Bytes, it is not recommended that you change the default MTU size unless required by your ISP.

- Primary and Secondary DNS: (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

## 2. Dynamic IP

If your ISP provides the DHCP service, please choose Dynamic IP connection, the router will automatically get IP parameters from your ISP, as follows:

**Basic Settings > WAN Settings**

<b>Wan Settings</b>	
<input type="radio"/> Static IP Address	
<input checked="" type="radio"/> Dynamic IP Address	
<input type="radio"/> PPPoE	
<input type="radio"/> 3G Dial-up	
<hr/>	
<b>Parameters Settings</b>	
MTU	<input type="text" value="1500"/> (576~1500)
Host Name	<input type="text"/>
<hr/>	
<b>DNS Address</b>	
Primary DNS	<input type="text" value="0.0.0.0"/> (optional)
Secondary DNS	<input type="text" value="0.0.0.0"/> (optional)
<hr/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- MTU: the normal MTU (maximum transmission Unit) value for most Ethernet networks is 1500 Bytes, it is not recommended that you change the default MTU size unless required by your ISP.
- Host Name: (optional) usually leaving this field blank will work.
- Primary/Secondary DNS: (Optional) Enter one or two DNS addresses in dotted decimal notation provided by your ISP.

## 3. PPPoE

Most xDSL provides PPPoE (Point-to Point Protocol over Ethernet) to establish Internet connections for end-users, to setup the Portable router, you need to enable PPPoE on the router's web-based setup page.

**Basic Settings > WAN Settings**

**Wan Settings**

Static IP Address  
 Dynamic IP Address  
 PPPoE  
 3G Dial-up

---

**Parameters Settings**

Username	<input type="text" value="username"/>
Password	<input type="password" value="*****"/>
MTU(Maximum Transmission Unit)	<input type="text" value="1492"/> (546~1492)
Service Name	<input type="text"/>

---

**DNS Address**

Primary DNS	<input type="text" value="202.96.128.86"/> (optional)
Secondary DNS	<input type="text" value="220.192.32.103"/> (optional)

**Save** **Cancel**

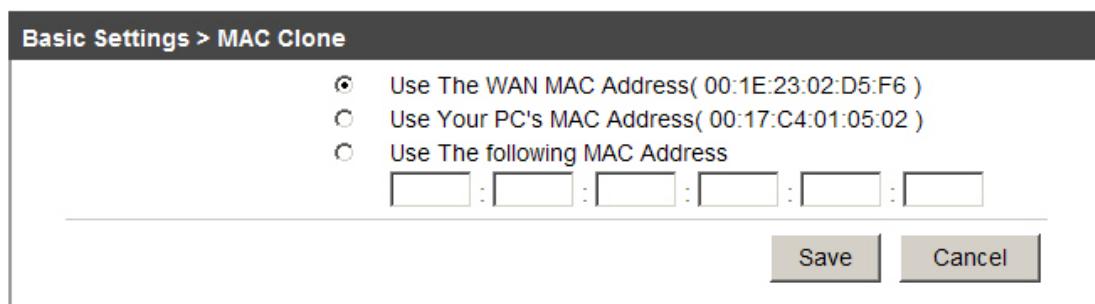
- Username: Enter the username provided by ISP, this field is case-sensitive.
- Password: Enter the password provided by ISP, this field is case-sensitive.
- MTU: the normal MTU (maximum transmission Unit) value for most Ethernet network is 1500 Bytes, it is not recommended that you change the default MTU size unless required by your ISP.
- Service Name: The service name should not be configured unless you are sure it is necessary for your ISP, in most cases, leaving these fields blank will work.
- Primary/Secondary DNS: If your ISP does not automatically assign IP address during login, please fill in the DNS address to the field.



Attention: the router only has only one Ethernet port, once it is used to xDSL (PPPoE ), then the LAN funtion is not available, only WiFi function is available.

### 3.1.2 MAC Clone

Choose **Basic settings > MAC Clone**, you can configure the MAC address of the WAN on the screen below:



- Use the WAN MAC Address: this is default option, it displays current MAC address of the WAN port.
- Use your PC's MAC Address: this field displays the MAC address of the PC that is managing the Router, If your ISP requires you to register the MAC address, please choose this option, click **Save** button to save settings, then the MAC address of WAN port changed to your PC's MAC address.
- Use the Following MAC Address: some ISP requires binding MAC address, only special MAC address can access to network, so you should enter the MAC address provided by ISP in this field, click **Save** button, then the MAC of WAN port address changed to this MAC address.

### 3.1.3 LAN Settings

Choose **Basic Settings > LAN Settings**, you can configure LAN parameters, you can also modify these parameters according to your need, you may not access the router's WEB page when you modified the LAN IP address, don't worry, you can modify your PC's IP address as same subnet as gateway.

Basic Settings > LAN Settings

LAN IP address	192.168.100.1
Subnet Mask	255.255.255.0

Save Cancel

- LAN IP Address: Enter the IP address of your router (factory default:192.168.100.1).
- Subnet Mask: An address code that determines the size of the network, normally use 255.255.255.0 as the subnet mask.

Note:

1. If you change the IP address of LAN, you must use new IP address to login the router.
2. If the LAN IP address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

## 3.2 Wireless Settings

### 3.2.1 Basic Settings

Choose **Wireless Settings > Basic Settings**, here you can configure basic wireless parameters.

Wireless Settings > Basic Settings

Mode	802.11b/g/n mixed
SSID	3G ROUTER
Channel	3
Hide SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Save Cancel

- Mode: This field determines the wireless mode which the Router works on, there are five options, the default value is 802.11b/g/n.

- 802.11b only-the Router works on 802.11b only.
- 802.11g only-the Router works on 802.11g only.
- 802.11b/g mixed-the Router works on 802.11b/g.
- 802.11g/n mixed-the Router works on 802.11g/n.
- 802.11b/g/n mixed-the Router works on 802.11b/g/n.

➤ SSID: (Service Set Identification), must be assigned to all wireless devices in your network, the default SSID is set to “Portable ROUTER”, you can change it to another.

➤ Channel: This field determines which operating frequency will be used, the default channel is set to 3. it is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

➤ Hide SSID: When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router, if you select the Hide SSID, the Portable Router will not broadcast its name (SSID) on the air.

### 3.2.2 Wireless Encryption

Choose **Wireless Settings > Wireless Encryption**, you can configure the security settings of your wireless network. there are five wireless security modes supported by the router: Disable, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK, Open system, Auto.

**Wireless Settings > Wireless Encryption**

**Encryption**

Tips: For your wireless network security, we strongly recommend using WPA-PSK or WPA2-PSK encryption.

Security Mode	Disable
Save Cancel	

➤ **Disable:** if you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.

➤ **WPA-PSK/WPA2-PSK:** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

**Wireless Settings > Wireless Encryption**

**Encryption**

Tips: For your wireless network security, we strongly recommend using WPA-PSK or WPA2-PSK encryption.

Security Mode	<input type="button" value="WPA-PSK"/>
WPA Encryption	
WPA Encryption Algorithm	<input type="radio"/> Auto <input checked="" type="radio"/> TKIP <input type="radio"/> AES
Group Key Update Period	<input type="text" value="3600"/>
PSK Password	<input type="text"/> (8-bit or 64-bit digits or characters)

- Security Mode: Select WPA-PSK.
- WPA Encryption Algorithm: When WPA-PSK is set as the Authentication type, you can select either Auto, or TKIP or AES as WPA Encryption.
- Group Key Update Period: Default value is 3600 seconds, 0 second means don't update.
- PSK Password: Enter PSK password, you can enter ASCII characters between 8-63 Hexadecimal 64 characters.

➤ **WEP Auto:** It is based on the IEEE 802.11 standard.

**Wireless Settings > Wireless Encryption**

**Encryption**

Tips: For your wireless network security, we strongly recommend using WPA-PSK or WPA2-PSK encryption.

Security Mode	<input type="button" value="WEP Auto"/>
WEP Encryption	
Key Length	<input type="button" value="64-bit"/>
Key Format	<input type="button" value="Hex"/>
Default Key ID	<input type="button" value="Key 1"/>
Key1	<input type="text" value="*****"/>
Key2	<input type="text" value="*****"/>
Key3	<input type="text" value="*****"/>
Key4	<input type="text" value="*****"/>

- Security Mode: WEP Auto means the router will auto select between **Open System** and **Share Key** authentication type based on the wireless station's capability and request.
- Key Length: You can select the WEP key length.
- Key Format: ASCII and Hexadecimal formats are provided, ASCII format stands for any combination of keyboard characters in the specified length; Hexadecimal format

stands for any combination of hexadecimal digits(0-9, a-f, A-F) in the specified length.

- Default Key ID: Index number, default is **Key1**.
- Key1-Key4-Respectively, corresponding to the key areas of the input.

### 3.2.3 Advanced Settings

Choose **Wireless Settings > Advanced Settings** menu, you can configure the advanced settings of your wireless network, the page as follows:

**Wireless Settings > Advanced Settings**

BG Protection Mode	<input type="button" value="Auto"/>	
Fragment Threshold	<input type="text" value="2346"/>	(range 256-2346, default 2346)
RTS Threshold	<input type="text" value="2347"/>	(range 1-2347, default 2347)
Beacon Interval	<input type="text" value="100"/>	ms(range 20-999, default 100)
DTIM(DTIM)	<input type="text" value="1"/>	ms(range 1-255, default 1)
Tx Power	<input type="text" value="100"/>	(range 1-100, default 100)

- BG Protection Mode: There are **on, off or Auto**.
- Fragment Threshold: This value is the maximum size determining whether packets will be fragmented, setting the Fragmentation Threshold too low may result in poor network performance since excessive packets.2346 is the default setting and is recommended.
- RTS: Threshold-Here you can specify the RTS(Request to Send)threshold if the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.
- Beacon: Enter a value between 20 and 999 for Beacon Interval here, the beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- DTIM: This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next windows for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value, you can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM interval is the same as Beacon Interval.

- RF Power: Indicates the Power capacity of broadcasting the SSID, the greater the value, the stronger the signal the default value is 100 (maximum).

### 3.2.4 MAC Filter

This function is used to control the wireless clients access the Internet via wireless MAC address. The page as follows:

- Filter Mode: There are three options: Disable, Only Allow, Only Deny, default value is **Disable**, Disable shows that the MAC filtering function is invalid.
- Only Allow - Those wireless MAC clients already added to the list can access the Internet.
- Only Deny - Those wireless MAC clients already added to the list can not access the Internet.
- MAC Address: The wireless station's MAC address that you want to filter.
- User Name: A simple description of the wireless station.

For example: If you desire the wireless station with MAC address 00:03:25:5A:19:CE, (username is Gateway) is able to access the router, but other wireless stations cannot access the router, do as follows:

1. Select “Only Allow” in **Filter Mode** box.
2. Enter MAC Address in **Client MAC Address** box
3. Enter “Gateway” in **Notes** box.
4. Click the **Add To List** button to add the entry.

5. Click the **Save** button to save the entry.

### 3.2.5 WPS Settings

Wireless Settings > WPS Settings

WPS Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Router's PIN	1858471
WPS Mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN code	<input type="text"/>
<b>Add New Device</b>	
<b>Save</b> <b>Cancel</b>	

- WPS Status: Enable or disable WPS function.
- Router's PIN: The router's default PIN code
- WPS Modem: this fields have two parameters: PIN and PBC.
- PIN Code: Enter PIN code manually.

### 3.2.6 Wireless Client List

Select **Wireless Settings > Wireless Client List**, you can see current wireless clients connected to the router, the page as follows:

Wireless Settings > Wireless Clients List

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:17:C4:01:05:02	1	0	0	7	20M	0	0

**Refresh**

## 3.3 DHCP Server

### 3.3.1 DHCP Server

Select **DHCP Server**, you can configure DHCP (Dynamic Host Configuration Protocol)

Server on this page, the router is set up by default as a DHCP server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN.

DHCP Server > DHCP Server

DHCP Server  Disable  Enable

Start IP Address: 192.168.100.100

End IP Address: 192.168.100.150

Address Lease Time: 3600

Default Domain: wan

Primary DNS address: 202.96.128.86

Secondary DNS address: 220.192.32.103

Save Cancel

- **DHCP Server:** Enable or Disable the DHCP server function, if you disable the server, you must have another DHCP server within your network or else you must manually configure the computer IP address.
- **Start IP Address:** This field specifies the first of the addressed in the IP address pool.192.168.100.100 is the default start address.
- **End IP Address:** This field specifies the last of the addressed in the IP address pool.192.168.100.150 is the default end address.
- **Address Lease Time:** The amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be leased this dynamic IP address, the default value is 3600 minutes.
- **Default Domain:** (optional) Enter the domain name of your network.
- **Primary / Secondary DNS -** Enter the DNS address provided by your ISP(optional).

### 3.3.2 DHCP Allocation List

This page displays “Assigned IP”, “Client Name”, “MAC Address” assigned by your DHCP Server, the page as follows:

DHCP Server > DHCP Allocation Table

IP Address	Host Name	MAC Address
192.168.100.100	fae	00:17:C4:01:05:02

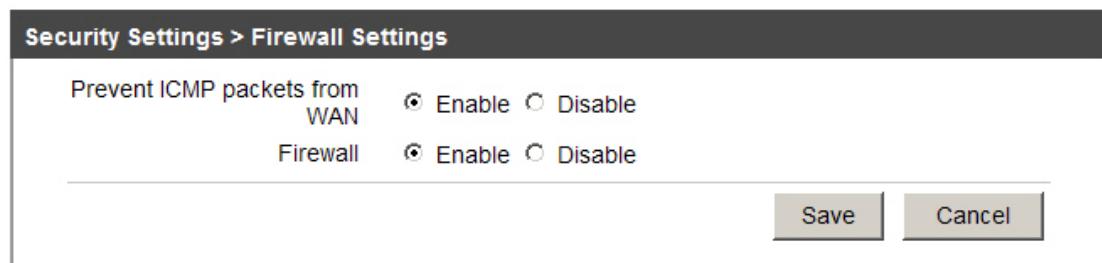
Refresh

From above page, we can see that only one client obtained a IP address from DHCP Server.

## 3.4 Security Settings

### 3.4.1 Firewall Settings

Select **Security Settings > Firewall Settings**, you can configure the firewall settings.



**Security Settings > Firewall Settings**

Prevent ICMP packets from WAN  Enable  Disable

Firewall  Enable  Disable

**Save** **Cancel**

- To prevent the ICMP packets from WAN: When enable this option, PING packets from Internet can not arrive the Router.
- Firewall Status: This is Master switch of the Firewall, When the master firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

### 3.4.2 Access Control List

You can configure the IP address filtering rule in this page, the ACL settings allows you to control the Internet access of some specific users based on their IP addresses:

**Security Settings > Access Control List**

Enable : <input type="checkbox"/>	
Source IP address: 192.168. <input type="text"/> . <input type="text"/> ~ <input type="text"/> . <input type="text"/>	
Target IP address: <input type="text"/> /24 (blank means all IP address.)	
Protocol: <input type="button" value="TCP"/>	
Target Port: <input checked="" type="radio"/> Port Range <input type="text"/> ~ <input type="text"/> <input type="button" value="Please choose"/>	
<input type="radio"/> Special application <input type="checkbox"/> QQ <input type="checkbox"/> MSN	
Day: <input checked="" type="radio"/> Every day <input type="radio"/> Date of work(Monday To Friday)	
Time(24 hours): <input type="text"/> : <input type="text"/> To <input type="text"/> : <input type="text"/>	
Deny or Pass: <input type="button" value="Deny"/>	
<input type="button" value="Add To List"/>	
<div style="border: 1px solid black; height: 150px; width: 100%;"></div>	
<input type="button" value="Delete This Entry"/>	<input type="button" value="Delete ALL"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Enable: Enable or disable the entry.
- Source IP Address: This is the LAN IP address or the range of LAN IP address in dotted-decimal notation format. For example: 192.168.100.20 - 192.168.100.30. keep the field blank, which means all LAN IP addresses are controlled by the rule.
- Target IP Address: This is the WAN IP address or the range of WAN IP addresses in dotted-decimal notation format. For example: 219.134.134.12 to 219.134.134.56. Keep this field blank, which means that all WAN IP addresses are controlled by the rule. The Default Subnet Mask of single IP is /32; If you want to control a range of IP address, you can use the VLSM (variable-length subnet mask) method to carry out, if there are 30 consecutive IP addresses starting with 219.134.132.128, we only need fill in the field with 219.134.132.128/27, it means a range of IP address from 219.134.132.128 to 219.134.132.159, remove a network address and a broadcast address, Just still have 30 IP addresses available. As for the relationship between VLSM and IP Address, please refer to the relevant books.
- Protocol: This indicates which protocol is used, TCP, UDP, or TCP/UDP.
- Target Port: This is the WAN port or a range of WAN ports. For example: 25-110.
- Special Applications: This is use to Deny QQ and MSN when you want to full control of QQ, the TCP/UDP protocol must to be selected.
- Days: This is the date or a range of date for the entry to take effect. For example,

Working Days (Monday to Friday), it means that the entry will take effect from Monday to Friday.

- Time (24 Hours): This is the time or a range of time for the entry to take effect .For example, 18:00-23:00, it means that the entry will take effect from 18:00 to 23:00.
- Deny or Pass: This field displays the action that the Router takes to deal with the traffic, **Pass** means that the Router allows the traffic through the Router, **Deny** means that the router rejects the traffic through the router.

Note: Before adding an IP address filtering entry, you should enable the Firewall and the ACL Filter function first.

### To add or modify an IP address filter entry.

#### Example 1

Make the PCs with IP addresses 192.168.100.2 to 192.168.100.10 unable to visit the website of IP address 219.134.132.128 during the time of 8:30 to 18:00 in working days, while other PCs have no limit, you can configure the rules as follows:

1. Enable **IP Address Filtering** function.
2. Enter “192.168.100.2 to 192.168.100.10 “ in Source IP Address field.
3. Enter “219.134.132.128” in Target IP Address field, and select /32.
4. Select **TCP** protocol.
5. Target Port is set to “80-80”
6. Time is set to “8:30 to 18:00” in working days.
7. Block or Pass is set to **Block**
8. Click the **Add To List** button to add the entry.
9. Click the **Save** button to save the entry.

**Security Settings > Access Control List**

Enable :

Source IP address: 192.168.100.2 ~ 192.168.100.10

Target IP address: 219.134.132.128 /32 (blank means all IP address.)

Protocol: TCP

Target Port:  Port Range  
 80 ~  80  Please choose

Special application  
 QQ  MSN

Day:  Every day  Date of work(Monday To Friday)

Time(24 hours):  08 :  30 To  18 :  00

Deny or Pass:  Deny

100.2~100.10 => 219.134.132.128/32 => TCP => 80~80(port) => Every day 08:30~18:00

### Other configurations for the entries:

Click the **Update This entry** to update the entry.

Click the **Delete This Entry** button to delete the entry you selected.

Click the **Delete ALL Entry** button to delete all the entries.

Click the **Add New Entry** button to add a new entry.

### Example 2

Deny to access QQ by the IP address 192.168.100.2~192.168.100.10 on your local network during the time of 8:30~18:00, the settings as follows:

**Security Settings > Access Control List**

Enable :

Source IP address: 192.168.100.2 ~ 192.168.100.10

Target IP address:  /24 (blank means all IP address.)

Protocol:

Target Port:  Port Range  
 ~  Please choose

Special application  
 QQ  MSN

Day:  Every day  Date of work(Monday To Friday)

Time(24 hours):  08 :  30 To  18 :  00

Deny or Pass:

100.2~100.10 => All => TCP/UDP QQ(Apply) => Date of work 08:30~18:00 => Deny

### 3.4.3 MAC Filter

You can configure the MAC Address filtering rule in the next page, the MAC Address feature allows you to control access to the Internet by users on your local network based on their MAC addresses:

**Security Settings > MAC Filter**

MAC Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Filter Mode	<input checked="" type="radio"/> Only Deny <input type="radio"/> Only Allow
<b>MAC List Management</b>	
MAC address	<input type="text"/> : <input type="text"/>
Username	<input type="text"/>
enable	<input type="checkbox"/>
<b>Add To List</b>	
<b>Delete This Entry</b>   <b>Delete ALL</b>	

**Save** | **Cancel**

- MAC Filter: Enable or Disable MAC filtering function.
- MAC Filter Mode: Only Deny means can not access to Internet, Only Allow means can access to Internet.
- MAC Address: This is the PC's MAC address which is controlled by the rule, its format is xx:xx:xx:xx:xx:xx (X is any hexadecimal digit), like this: 00:12:34:43:32:22.
- Username: This is the description about the PC, For example: Lucky's PC.
- Enable: The status of this entry either enabled or disabled.

### To add/modify a MAC filter entry:

#### For example:

If you want to Deny the PCs with MAC Address 00:14:78:12:23:34 to access the Internet, you can configure as follows:

1. Enable the "MAC Filter".
2. Specify the MAC Address Mode as "Only Deny".
3. Enter the appropriate MAC Address and Username, and then choose the "enable" status.
4. Click the **Add To List** button to add the entry.
5. Click the **Save** button to save the entry.

#### Other configurations for the entries:

Click the **Update This Entry** button to update the entry (you must select the entry first).

Click the **Delete This Entry** button to delete the entry.

Click the **Delete All Entry** button to delete all the entries.

### 3.4.4 Domain Filter

The Domain Filter feature allows you to control access to certain websites on the internet by specifying their domains or key words, the page as follows:

The screenshot shows a web-based configuration interface for a domain filter. At the top, a header bar reads "Security Settings > Domain Filter". Below this, a "Mode" section contains three radio buttons: "Disable" (selected), "Only Allow", and "Only Deny". A "Domain Name Address" input field is followed by an "Add To List" button. A large rectangular area below the input field is a list box for domain entries. At the bottom of the list box are two buttons: "Delete This Entry" and "Delete All Entry". At the very bottom of the interface are "Save" and "Cancel" buttons.

- Mode: This field have three options: **Disable, Only Allow, Only Deny**.
- Domain Address: Type the domain or key word as desired in the field. For example: [www.sohu.com](http://www.sohu.com), [.net](http://.net) and so on.

#### For example:

If you want to allow the PCs on your LAN from accessing websites [www.qq.com](http://www.qq.com), [www.sohu.com](http://www.sohu.com), do as follows:

1. Specify the Mode as **Only Allow**.
2. Enter a domain name in the **Domain Address** box.
3. Repeat above step to add another domain name.
4. Click the **Add To List** button to add the entry.
5. Click the **Save** button to save the entry.

**Security Settings > Domain Filter**

Mode  Disable  Only Allow  Only Deny

Domain Name Address

**Other configurations for the entries:**

Click the **Update This Entry** button to update the entry (you must select the entry first).

Click the **Delete This Entry** button to delete the entry.

Click the **Delete All Entry** button to delete all the entries.

### 3.4.5 IP & MAC Binding

IP & MAC Binding is useful for controlling access of specific computers in the LAN, for bound IP address, can allow or deny to modify it's IP address; for unbound MAC address, can allow or deny to pass.

**Security Settings > IP&MAC binding**

IP&MAC binding	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP address has been bound	<input checked="" type="radio"/> allow to modify IP Address <input type="radio"/> Deny to modify IP Address
IP Address has not been bound	<input checked="" type="radio"/> Allow to pass <input type="radio"/> Deny to pass
MAC address	<input type="text"/>
IP address	192.168. <input type="text"/> . <input type="text"/>
Username	<input type="text"/>
Enable	<input type="checkbox"/>
<input type="button" value="Add to List"/> <input type="button" value="View new IP"/> <input type="button" value="Bulk import"/>	
<input type="button" value="Delete This Entry"/> <input type="button" value="Delete All Entry"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- IP & MAC Binding: The status of this entry either enabled or disabled.
- IP address has been bound: Allow or Deny to modify bound IP address, if enable deny to modify IP, that means some computers can not access the Router if this IP address has not in the binding list.
- IP address has not been bound: Allow or Deny to pass for those unbound IP address, if you choose **Deny To Pass**, some MAC addresses that not added to list can not access the Router.
- MAC Address: The MAC address of the controlled computer in the LAN.
- IP Address: The assigned IP address of the controlled computer in the LAN.
- Username: given a description for this computer
- Enable: Enable this rule.

### 3.4.6 Remote WEB Management

This feature allows you to manage your router from a remote location via the Internet, WEB management port used to access the router, this router's default remote access web port number is 8080, choose a number between 1025 and 65535, but do not use the number of any common service port.



**For example:**

If your router's WAN address is 121.34.12.34, and the port number you used is 8080, please enter <http://121.34.12.34:8080> in your browser, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web-based utility.

### 3.4.7 Advanced Security Settings

Using this function, you can protect the Router from being attacked by TCP / UDP / ICMP Flood.

**Security Settings > Advanced Security Settings**

Port Block		Port Range
NO	Status	
1	<input checked="" type="checkbox"/> Enable	135 -- 139
2	<input checked="" type="checkbox"/> Enable	445 -- 445
3	<input type="checkbox"/> Enable	--
4	<input type="checkbox"/> Enable	--
5	<input type="checkbox"/> Enable	--
6	<input type="checkbox"/> Enable	--

**DDoS**

<input checked="" type="checkbox"/> Enable TCP/UDP/ICMP Flood Attack	Threshold <input type="text" value="150"/>
<input checked="" type="checkbox"/> Enable ARP Attack	Packets/S
	Interval <input type="text" value="1S"/>

**Save** **Cancel**

- Port Block: If the target port already existing in the range of the list, these packets will be discarded.
- DDOS: DDOS(Distribution Denial Of Service), The default value is 150 packet/s when the current TCP/UDP/ICMP Flood packets numbers is beyond the set value, the Router will startup the blocking function immediately, when the ARP attacks time less 1s, the Router will startup the blocking function immediately to protect ARP Table.

## 3.5 Advanced Settings

### 3.5.1 DDNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name(named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. This router built-in three DDNS client, there are 3322.org, dydns.org and tzo.org.

**Advanced Settings > DDNS**

Service Provider	<input type="button" value="Disable"/>
Username	<input type="text"/>
Password	<input type="text"/>
Domain Name	<input type="text"/>
WAN IP Address	0.0.0.0
DDNS Status	Disconnected

Before using this feature, you need to sign up for DDNS service provider to set up for DDNS.

1. Select one Service Provider from pull down list.
2. Type the Username for your DDNS account.
3. Type the Password for your DDNS account.
4. Type the Domain Name that you registered with your DDNS Service Provider.
5. Click the “Save” button to login to the DDNS service, if you connected to DDNS server, the DDNS Status is set to “Connect successful”.

### 3.5.2 WDS

WDS is a wireless interconnection system via multiple wireless access points in IEEE 802.11 network. It allows to extend the wireless network through multiple access points. Rather than before, the wireless access point connects through cable. WDS has three modes: Lazy Mode, Bridge Mode, Repeater Mode.

**Advanced Settings > WDS**

WDS Mode	<input type="button" value="Disable"/>
Phy Mode	<input type="button" value="GREENFIELD"/>
Encryption Type	<input type="button" value="NONE"/>
Encryption Key	<input type="text"/>
AP1 MAC Address	<input type="text"/>
AP2 MAC Address	<input type="text"/>
AP3 MAC Address	<input type="text"/>
AP4 MAC Address	<input type="text"/>

- WDS Mode: Supports Lazy Mode, Bridge Mode, Repeater Mode.
- Lazy Mode-Lazy mode do not need to fill in each other's BSSID, The AP's WDS connections as passive connection, only need to fill out the other side of the AP's BSSID.
- Bridge Mode-Bridge Mode need to fill in each other's BSSID, local AP's SSID was Shield, As a SSID extension form of the Repeater Mode, Repeater Mode also need to fill in each other's BSSID, Local AP as a core, other AP just as extension form of repeater mode.
- Repeater Mode- Repeater Mode need to fill in each other's BSSID, local AP as core, other APs is a extension from of Repeat Mode.
- Phy Mode: There are four options: GREENFILED, CCK, OFDM, HTMIX.
- Encryption Type: This is used to set encryption key for two sides in WDS connection
- Key: Enter the password.
- AP MAC (MAC1-MAC4): Enter the MAC address of connected device.

### 3.5.3 UPnP Settings

The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



UPnP can be enabled or disabled by clicking the **Enable** or **Disable** option, as allowing this may present a risk to security, this feature is disabled by default.

### 3.5.4 Virtual Server

Virtual server can be used for setting up public services on your LAN, such as DNS, E-mail and FTP, a virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP, any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

Advanced Settings > Virtual Server

Preset Settings	-- Please choose --
Service Name	<input type="text"/>
Service Port	<input type="text"/> -- <input type="text"/>
Internal Server IP	192.168.100. <input type="text"/>
<input type="button" value="Add To List"/>	
<input type="button" value="Delete This Entry"/>	<input type="button" value="Delete All Entry"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Preset Settings: You can select the service want to use from the Preset Settings list, if it does not have the service that you want to use, type the number of the service port or service port range in the **service port** box.
- Service Name: This is a description for the service.
- Service Port: 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).
- IP Address- The IP address of the PC providing the service application.

### To setup a virtual server entry:

1. Enter a Service Name in “Service Name” box.
2. Select the service you want to use from the Preset Settings list, if the Preset Settings list does not have the service that you want to use, type the number of the service port or services port range in the “Service Port” box.
3. Type the IP Address of the computer in the “IP Address” box.
4. Click “Add To List” to add the entry.
5. Click “Save” to save the settings.

### To modify or delete an existing entry:

1. Select the entry you want to modify.
2. If you want to delete the entry, click the “Delete This Entry” button.
3. Modify the information.
4. Click the “Update This Entry” button to update the entry.
5. Click the “Save” button to save the entry.

**Advanced Settings > Virtual Server**

Preset Settings	FTP (port: 21)
Service Name	FTP
Service Port	21
Internal Server IP	192.168.100.10
<b>Add To List</b>	
192.168.100.10 => 21-21 => FTP	
<a href="#">Delete This Entry</a> <a href="#">Delete All Entry</a> <a href="#">Add New Entry</a>	
<a href="#">Save</a> <a href="#">Cancel</a>	

**Note:**

If your computer or server has more than one type of available service, please select another service, and enter the same IP address for that computer or server.

### 3.5.5 DMZ Settings

The DMZ host feature allows one local host to be exposed to the internet for a special-purpose service such as Internet gaming or video conferencing, DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change, when using the DHCP function, the page as follows:

**Advanced Settings > DMZ Settings**

<input checked="" type="radio"/> Disable	
<input type="radio"/> Enable	
DMZ host IP address	0.0.0.0
<a href="#">Save</a> <a href="#">Cancel</a>	

**To assign a computer to be a DMZ server**

1. Enable the DMZ function
2. Enter the local DMZ host IP address in the **DMZ host IP address** box.
3. Click the **Save** button to save the settings.

Note: After you set the DMZ host, the firewall related to the host will not work.

### 3.5.6 Special Application

Some applications require multiple connections, like Internet games, Videoconferencing, these applications can not work with a pure NAT router, port Triggering is used for some of these applications that can work with an NAT router, the page as follows:

Advanced Settings > Special Application

Name	<input type="text"/>
Trigger port	<input type="text"/> -- <input type="text"/>
Forward Port	<input type="text"/>
Enable	<input type="checkbox"/>
<input type="button" value="Add To List"/>	
<input type="button" value="Delete This Entry"/> <input type="button" value="Delete All Entry"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Name: Enter a description for the rule.
- Trigger Port: The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- Forward Port: The port 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. You can enter group of ports must be set apart with “ , ” For example: 2000-3000, 4340-4360 and so on..
- Enable: The status of this entry either enabled or disabled.

#### To add a new rule:

1. Enter the Name for the entry.
2. Enter a port number or a ports range used for Trigger Port.
3. Enter the port number or a ports range used by the remote system when it responds to the PC's request.
4. Click **Add To List** button to add the entry.

5. Click the **Save** button to save the settings.

#### **To modify or delete an existing entry:**

1. Select the entry you want to modify.
2. If you want to delete the entry, click the **Delete This Entry** button.
3. Modify the information.
4. Click the **Update This Entry** button to update the entry.
5. Click the **Save** button to save the settings.

#### Note:

1. When the trigger connection is released, the according opening ports will be closed.
2. Each rule allowed to be used only by one host on LAN synchronous, the trigger connection of other hosts on LAN will be refused.
3. Incoming Port cannot overlap each other.

## **3.6 System Tools**

### **3.6.1 Time Settings**

You can configure the time on the following screen:



System Tools > Time Settings

Time Server: time.windows.com

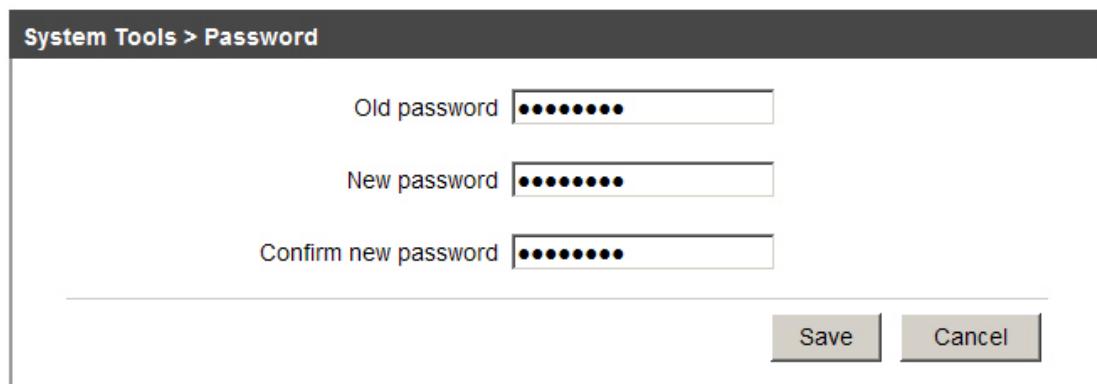
Time Zone: (GMT +08:00) Beijing

Save Cancel

- Time Server: you can select time server from this pull down list, the default value is time.windows.com.
- Time Zone: Select your local time zone from this pull down list

### **3.6.2 Password Modify**

You can change the factory default password of the Router in the next screen:

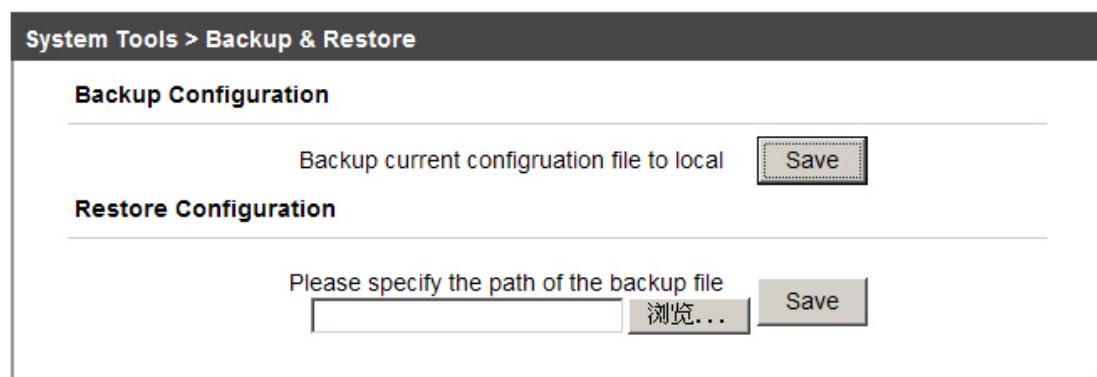


- Old Password: Factory default password, the default is admin
- New Password: You can enter a new password for the Router, the new password must be at least 5 characters in length.
- Confirm New Password: Re-enter new password for the Router.

When finished above settings, click the **Save** button to take effect. It is recommended strongly that you should change the factory default password of the router, because all users who try to access the router's Web-based utility will be prompted for the router's default user name and password.

### 3.6.3 Backup & Restore

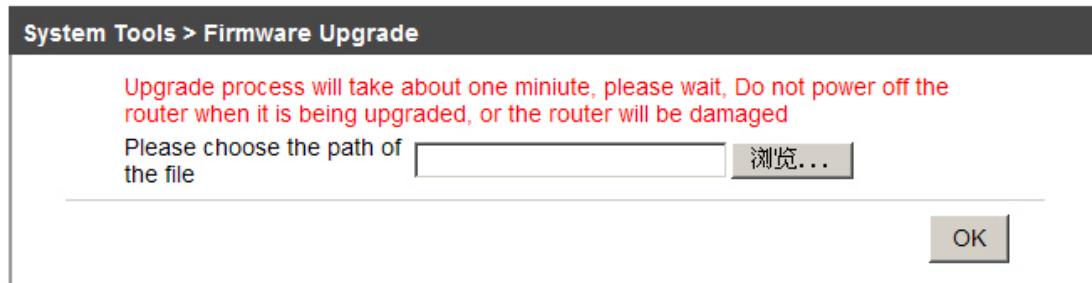
You can save the current configuration of the router as a backup file and restore this configurations when the router reset.



- Backup: click the **Save** button to save all configuration settings as a backup file in your local computer.
- Restore: Click the **Browse** button to locate the update file for the device, or enter the exact path to the setting file in the text box.

### 3.6.4 Firmware Upgrade

Using this function, router can achieve more stable function via firmware upgrade, during the upgrade process, do not turn off the power, or it may be damaged!



To upgrade the router's firmware, do as follows:

1. Download the firmware first.
2. open the router 's WEB page, click **System Tools > Firmware Upgrade**, click **Browse** button to locate the upgrade file.
3. Click **OK** to start to upgrade.

### 3.6.5 Reboot

click System Tools> Reboot, you can reboot the router.



### 3.6.6 Factory Defaults

Click the **Factory Defaults** button, you can restore the configurations of the Router to factory defaults, any settings you have saved will be lost when the default settings are restored. The default parameters are:

Default User name: admin

Default Password: admin

Default IP Address: 192.168.100.1

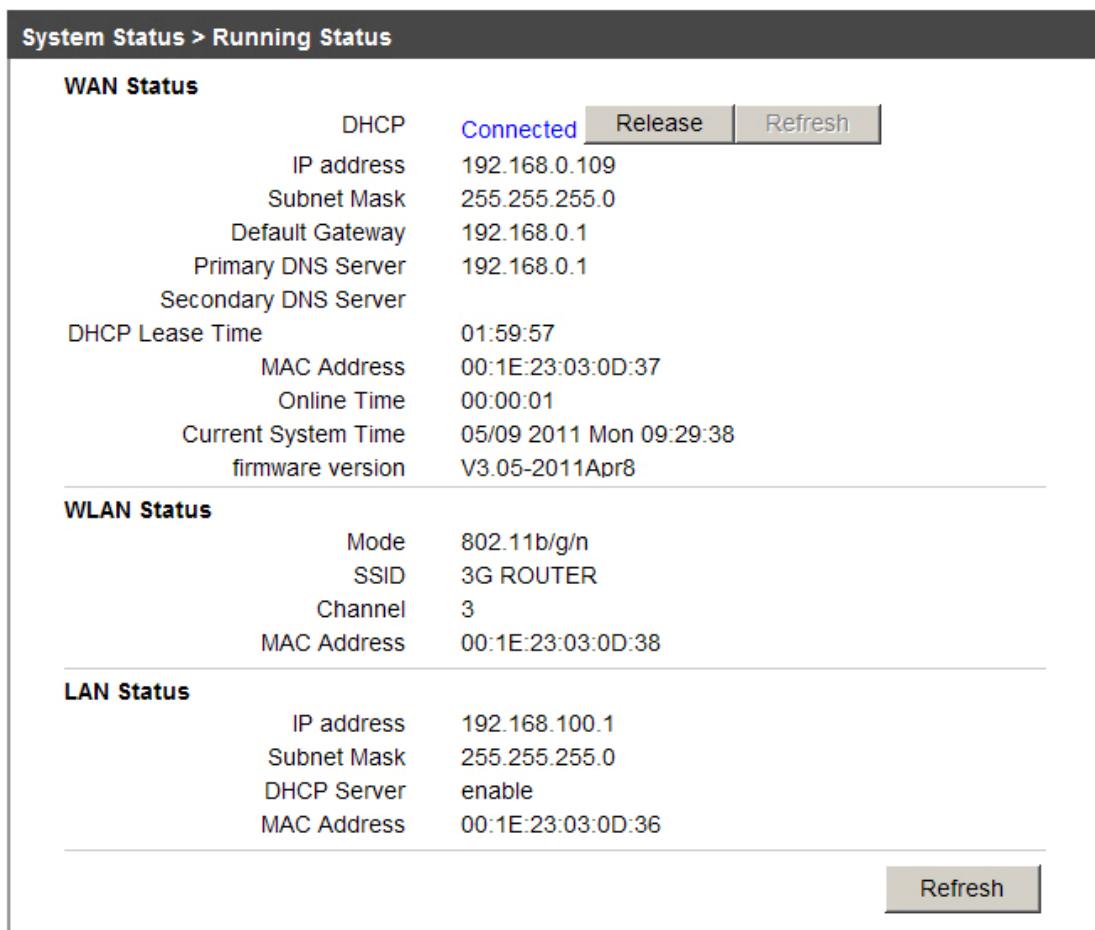
Default Subnet Mask:255.255.255.0



## 3.7 System Status

### 3.7.1 Running Status

The **Running Status** page provides the current status information about the router. All information is read-only, the following page displays parameters, WLAN status, LAN status:



### 3.7.2 Client List

Client List displays users connected to the Router, the information include IP Address, MAC Address, Host Name, the page as follows:

System Status > Client List

Setup		
IP address	MAC address	Host Name
192.168.100.100	00:17:C4:01:05:02	

**Refresh**

### 3.7.3 Syslog

You can view the logs of the Router on this page, the router can keep logs of all traffic, you can query the logs to find what happened to the router.

System Status > System Log

```

[192.168.100.1 00:00:25] pppd[743]: pppd 2.4.2 started by (unknown),
uid 0
[192.168.100.1 00:00:26] chat[745]: timeout set to 20 seconds
[192.168.100.1 00:00:26] chat[745]: abort on (BUSY)
[192.168.100.1 00:00:26] chat[745]: abort on (ERROR)
[192.168.100.1 00:00:26] chat[745]: report (CONNECT)
[192.168.100.1 00:00:26] chat[745]: abort on (NO CARRIER)
[192.168.100.1 00:00:26] chat[745]: abort on (VOICE)
[192.168.100.1 00:00:26] chat[745]: abort on (NO DIALTONE)
[192.168.100.1 00:00:26] chat[745]: send (ATDT#777'M)
[192.168.100.1 00:00:26] chat[745]: timeout set to 30 seconds
[192.168.100.1 00:00:26] chat[745]: expect (CONNECT)
[192.168.100.1 00:00:27] chat[745]: ^M
[192.168.100.1 00:00:27] chat[745]: CONNECT
[192.168.100.1 00:00:27] chat[745]: -- got it
[192.168.100.1 00:00:27] chat[745]: send (c'M)
[192.168.100.1 00:00:27] pppd[743]: Serial connection established.
[192.168.100.1 00:00:27] pppd[743]: using channel 1
[192.168.100.1 00:00:27] pppd[743]: Using interface ppp0
[192.168.100.1 00:00:27] pppd[743]: Connect: ppp0 <-> /dev/ttyUSB0

```

**Refresh**

## Help

From the Help menu, you can quickly get the function description information about this router.

### ***FCC Notice***

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.

NOTE 1: 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.

NOTE 2: The manufacturer is not responsible for any changes or modifications not expressly approved by the manufacturer for compliance, such modifications could void the user's authority to operate the equipment.