PHICOMM

User Manual

Wireless Nano Router

M1

User Manual / V1.0

Copyright Statement

PHICOMM is the registered trademark of Shanghai Feixun Communication Co., Ltd. Other trademark or trade name mentioned herein are the trademark or registered trademark of the company. Copyright of the whole product as integration, including its accessories and software, belongs to Shanghai Feixun Communication Co., Ltd. Without the permission of Shanghai Feixun Communication Co., Ltd., individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages.

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, PHICOMM is not responsible for informing in advance. If you want to know more information about our products, please visit our website at www.phicomm.com.

CONTENTS

Chapter 1: Introduction 1

Product Overview 1

Main Features 2

Chapter 2: Operating Mode Introduction 1

Chapter 3: Installation 3

Physical Connection 3

Configure the Computer's IP Address 3

Setup Wizard 13

Chapter 4: Router Configuration 20

Basic Setting 20

Operating Mode 21

Internet Settings 21

Wireless Basic Settings 22

Wireless Security Settings 25

Running Status 27

Expert Setting 27

Network Settings 28

Wireless Settings 29

DHCP Server 32

NAT 33
Security Options 36
Access Control 38
Routing Settings 39
IP Bandwidth Control 40
IP and MAC Binding 40
System Tools 41
Logout 45

Chapter 5: Specification 46

Appendix A: Troubleshooting 47

Appendix B: Certification 48

FCC Statement 48
CE Mark Warning 49

Appendix C: Glossary 50

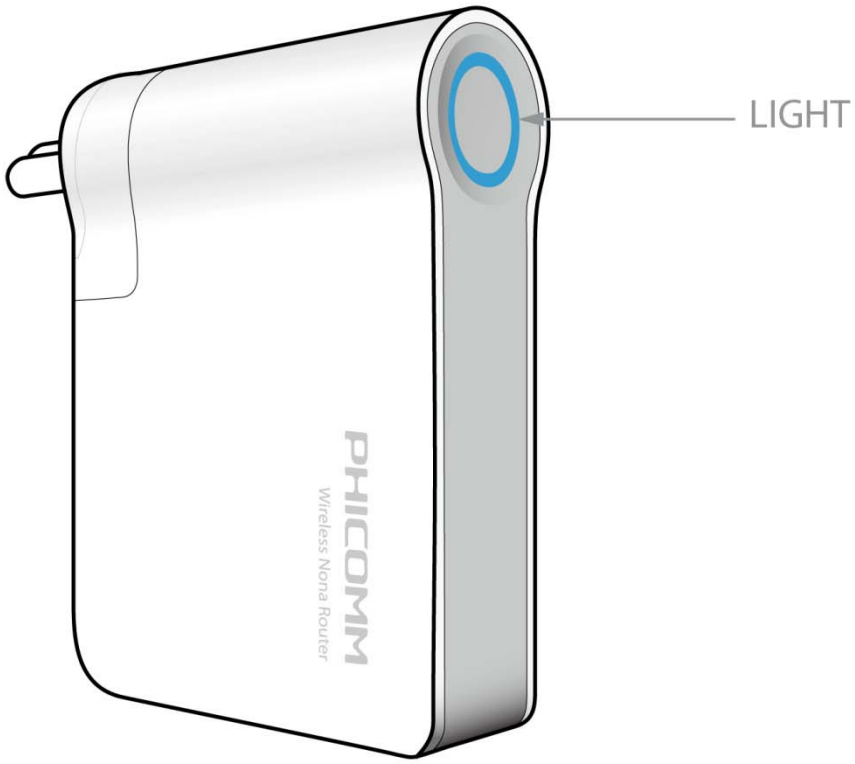
Chapter 1: Introduction

Product Overview

Thank you for choosing M1 Wireless Nano Router.

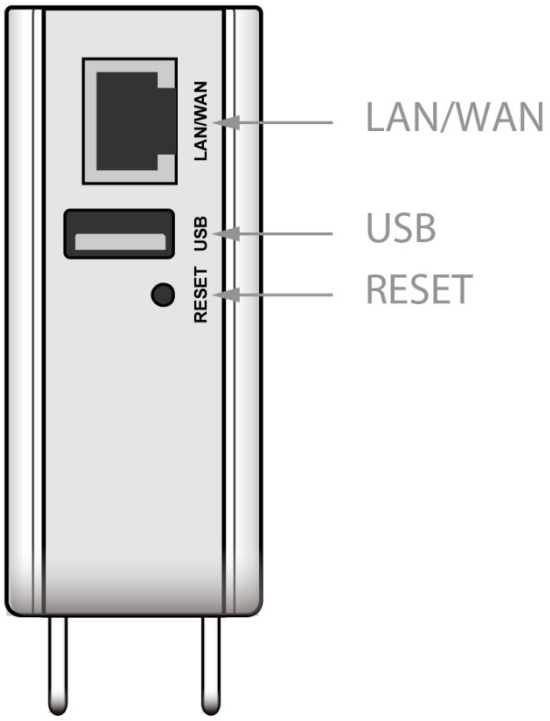
The Wireless Nano Router is an all-in-one router, ideal for creating a highly efficient mobile office or entertainment network at any time. Small enough to fit in the average pocket, the router is uniquely suited to provide robust wireless networking to travelers, students, or anyone else for work or play. It supports multiple operating modes such as AP, Router, Repeater, Bridge and Client, helping you to extend wireless range and to boost the wireless signal. You can enjoy the convenience of wireless network in home, office, hotel or any other place with this compact and portable router.

Front Panel



LED	Status	Description
SYS	On	The system is normal
	Blinking	There is a successful connection on the LAN/WAN port

Rear Panel



LAN/WAN: This Ethernet port can be used as a LAN or WAN port.

USB: Connect to your USB device.

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

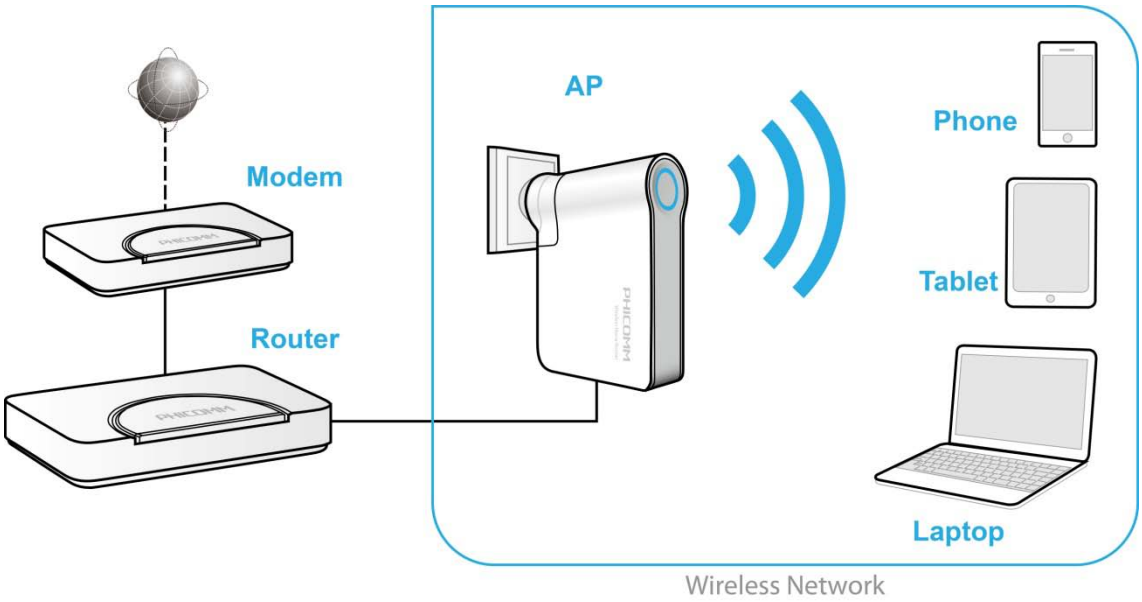
Main Features

- IEEE 802.11n, wireless speed up to 150Mbps
- Travel-sized design, lightweight, great for home or travel user
- USB port can be used for charging the Smart Phone
- Built-in firewall featured with IP, MAC , URL Filtering and ARP attack prevention to protect your PC
- Supports multiple operation modes in different environment
- Supports WEP, WPA/WPA2-Enterprise,WPA /WPA2-Personal
- Backward compatible with 802.11b/g product

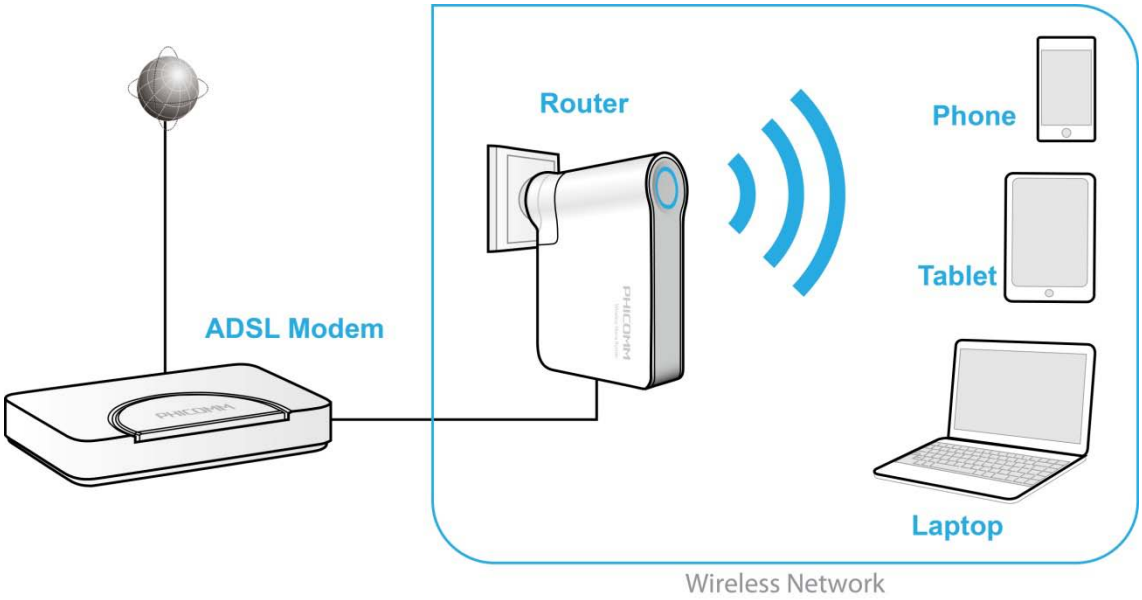
Chapter 2: Operating Mode Introduction

This Wireless Nano Router supports five operation modes: AP (Access Point), Router, Repeater, Bridge and Client. By default, the operation mode is AP.

In AP mode, it extends your existing hardwired network to your wireless clients.



In Router mode, you can connect it to your modem to access the internet.



In Repeater mode, it can extend the coverage of your root wireless router, boost the wireless signal strength.

In Bridge mode, it can wirelessly connect two or more remote LANs which also support Bridge mode together.

In Client mode, it acts as a wireless network adapter.

Chapter 3: Installation

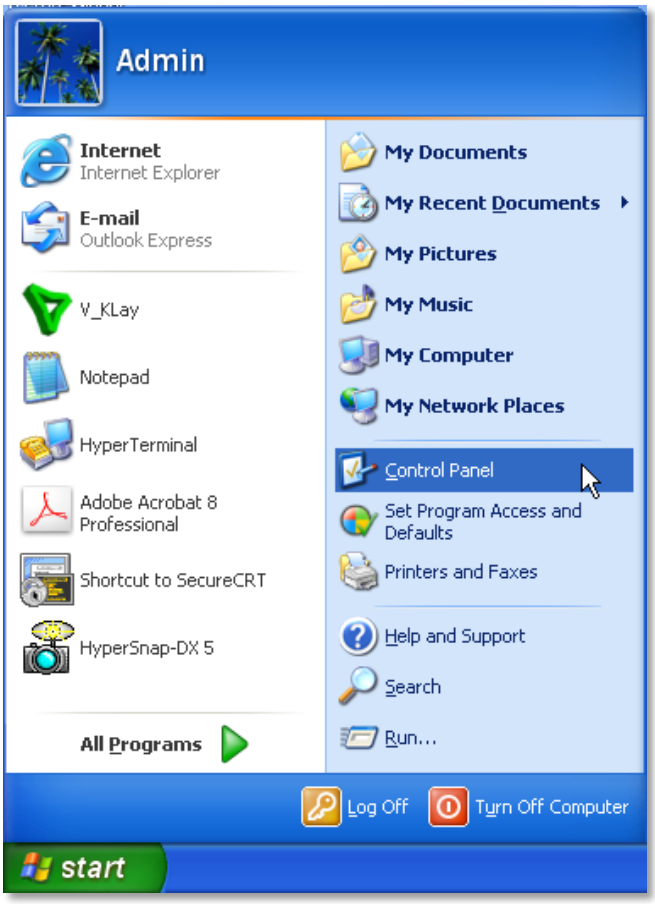
Physical Connection

Please refer to Chapter 2.

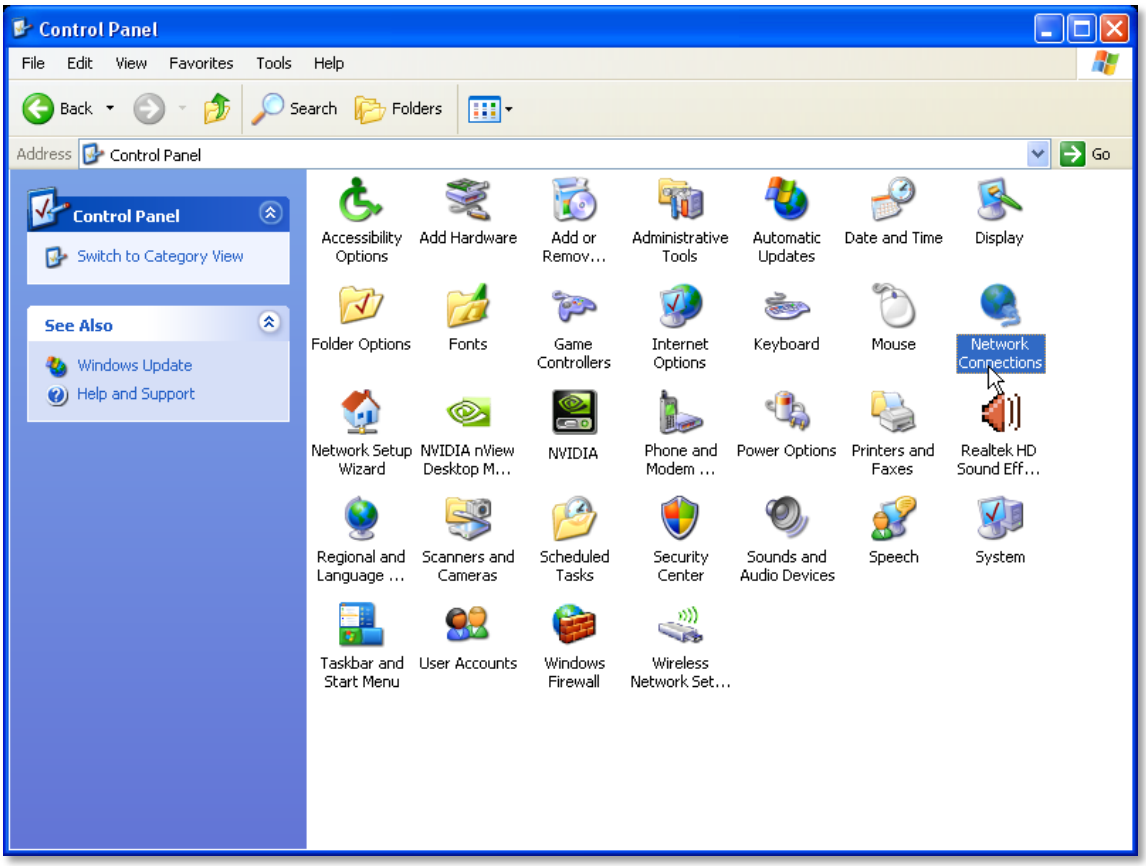
Configure the Computer's IP Address

For Windows XP/2000

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

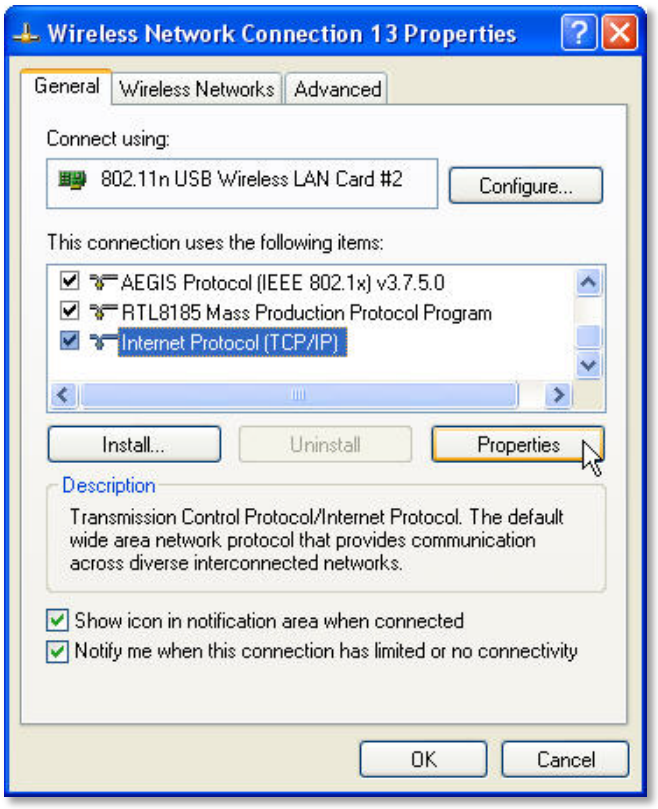


2) Select and double click **Network Connections**.

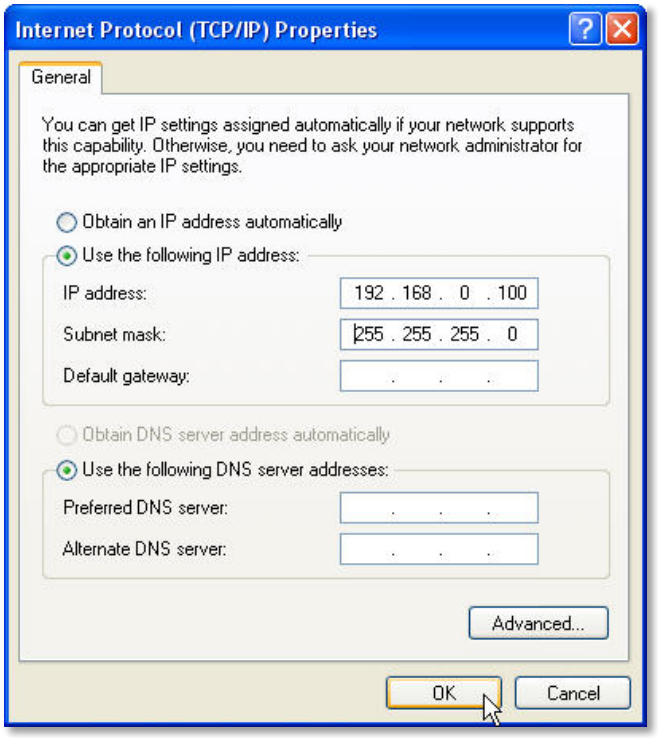


3) Right click **Wireless Network Connection** and then select **Properties**.

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

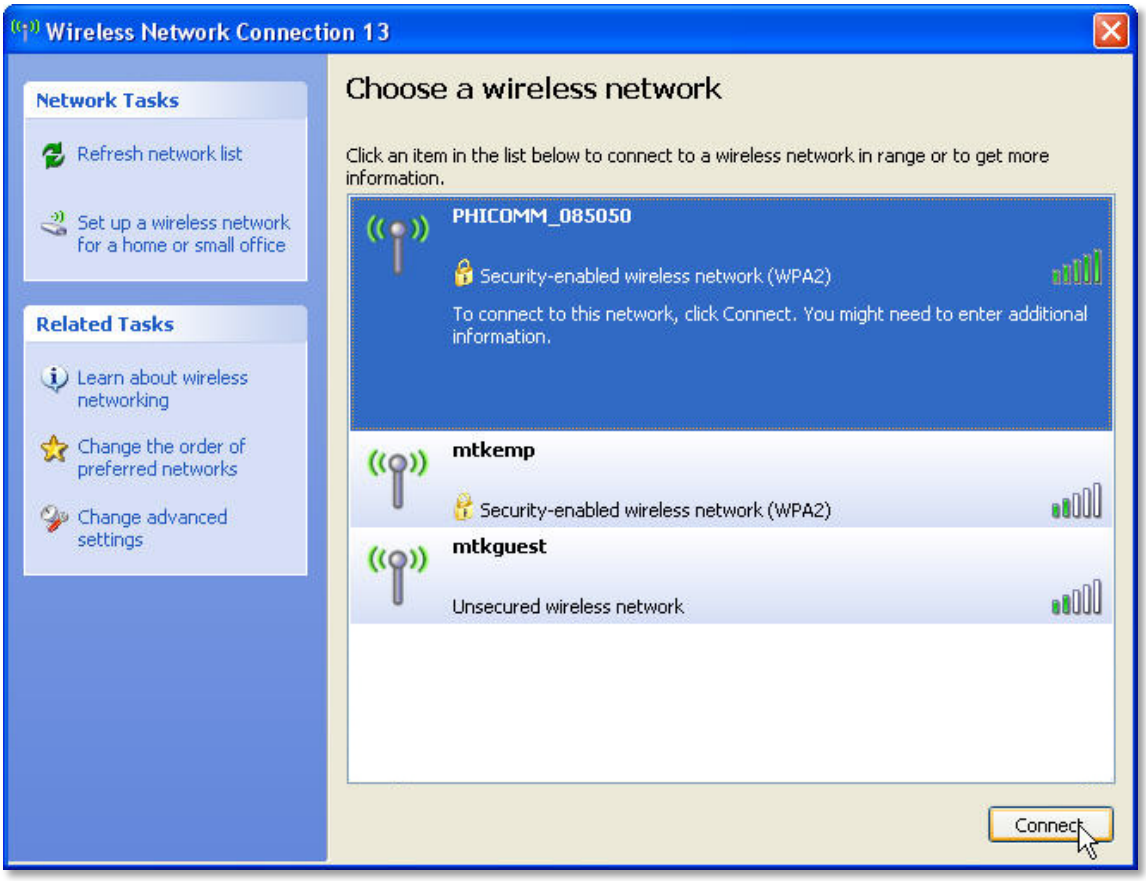


5) Select **Use the following IP address** and **Use the following DNS Server addresses**. The IP address put in 192.168.0.X (like 192.168.0.100), Subnet mask put in 255.255.255.0, Default gateway leave it blank. Then click **OK**, and then click **OK** again.

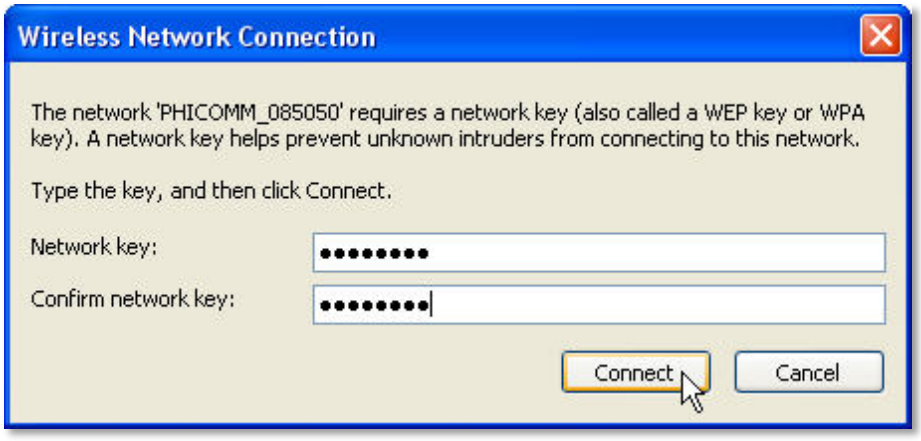


6) Right click on **Wireless Network Connection** again, choose **View Available Wireless Networks**.

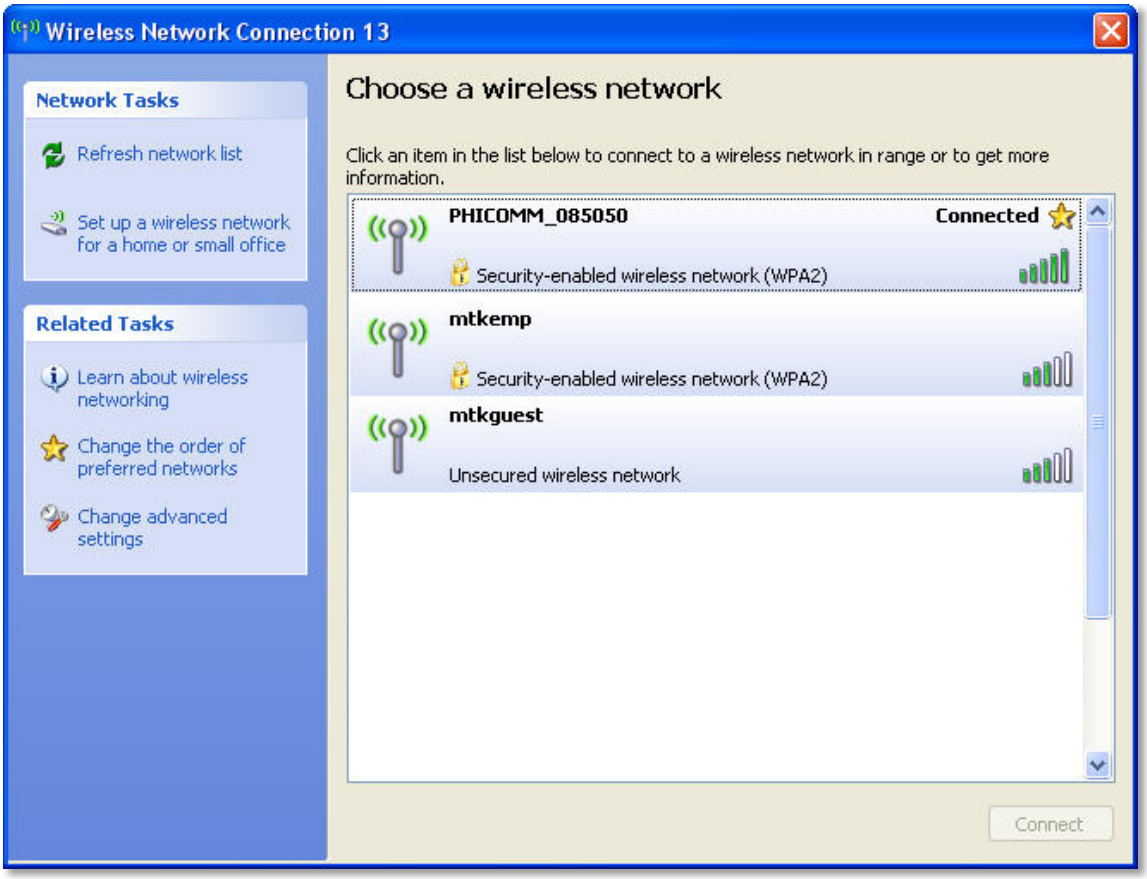
7) Click **Refresh network list**, search for PHICOMM_XXXXXX, highlight on it and then click **Connect** button.



8) You can see a windows pop up requires for a Network key, you can find the network key from the label attached on the Wireless Nano Router or the package box. Put in the network key and then click **Connect**.

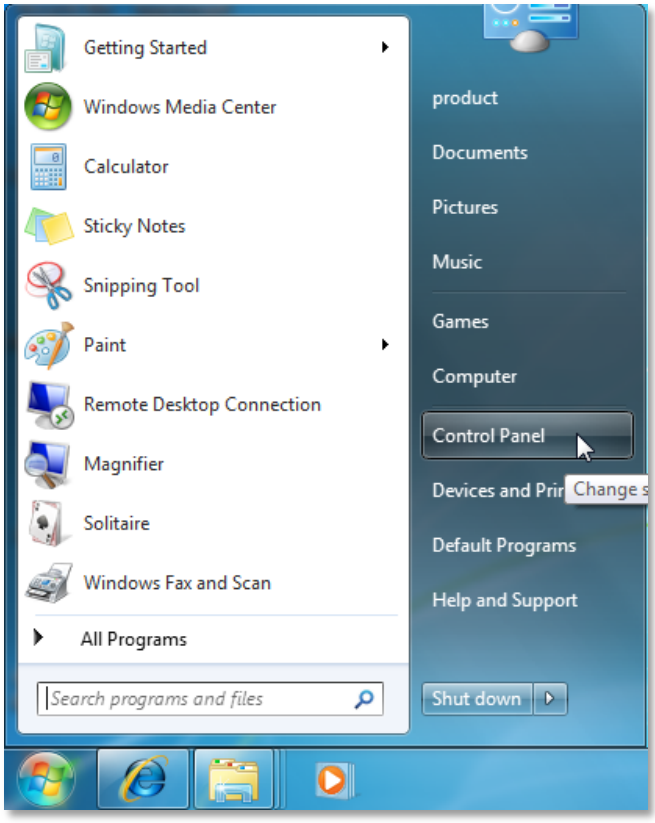


9) After you put in the correct network key, you can see it showing connected.

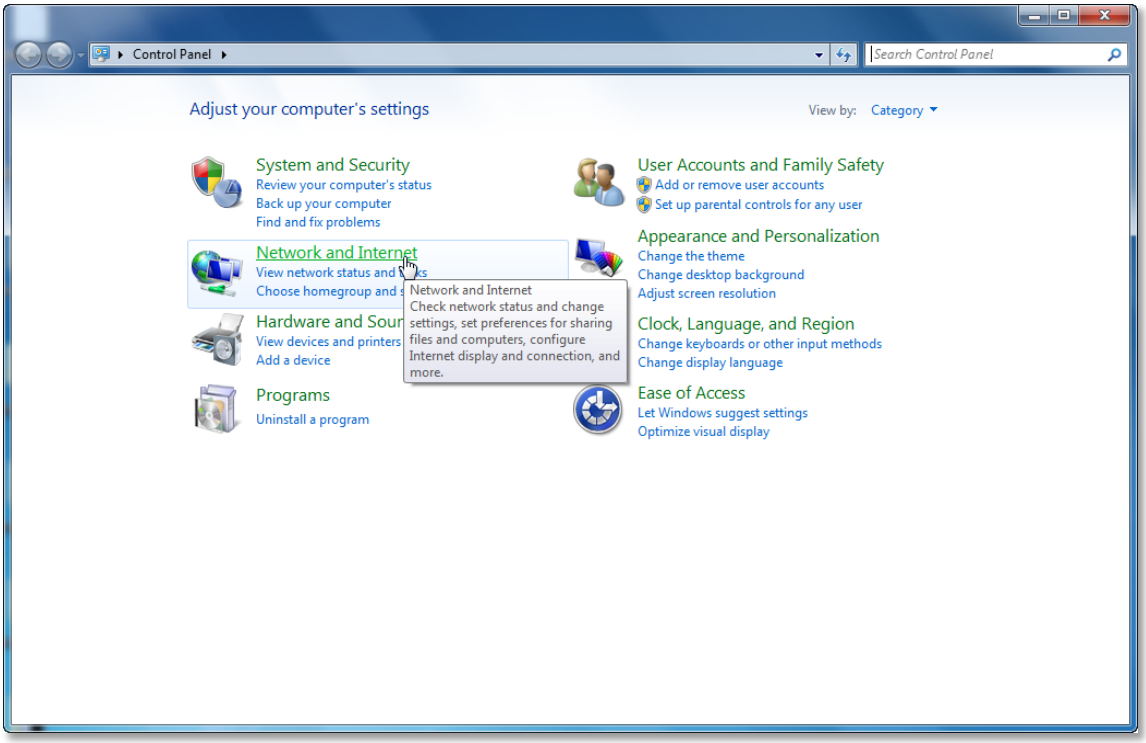


For Windows Vista/7

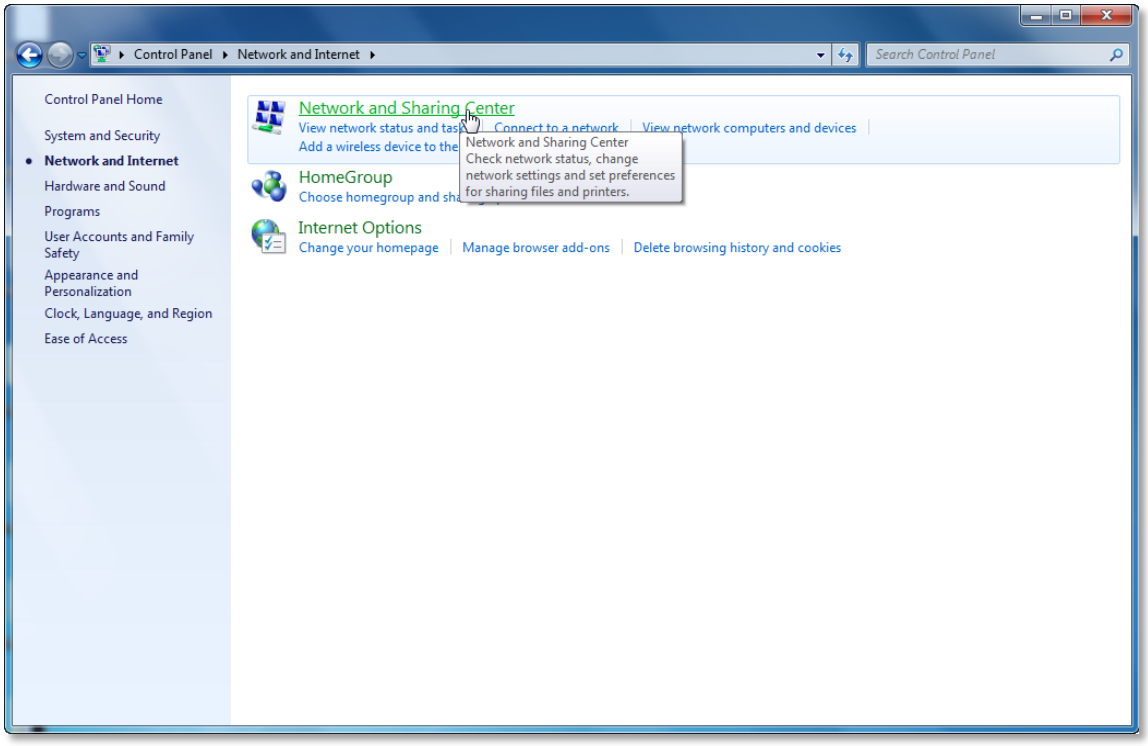
1) Click **Start**>**Control Panel**.



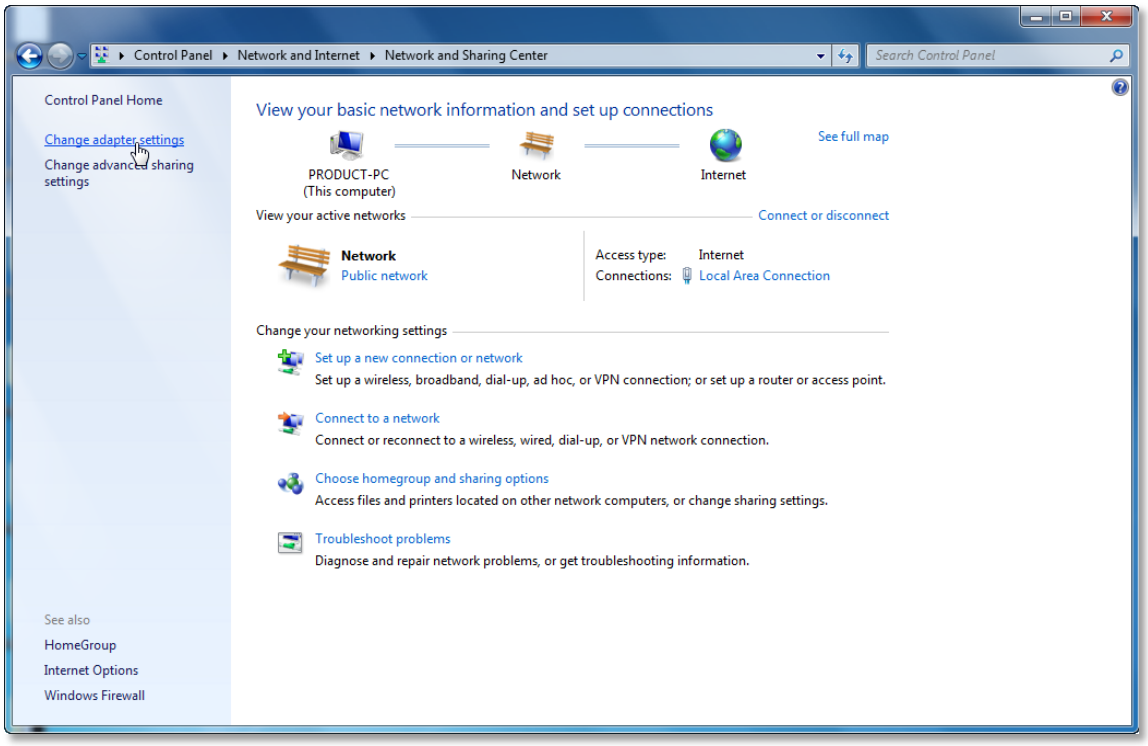
2) Click **Network and Internet**.



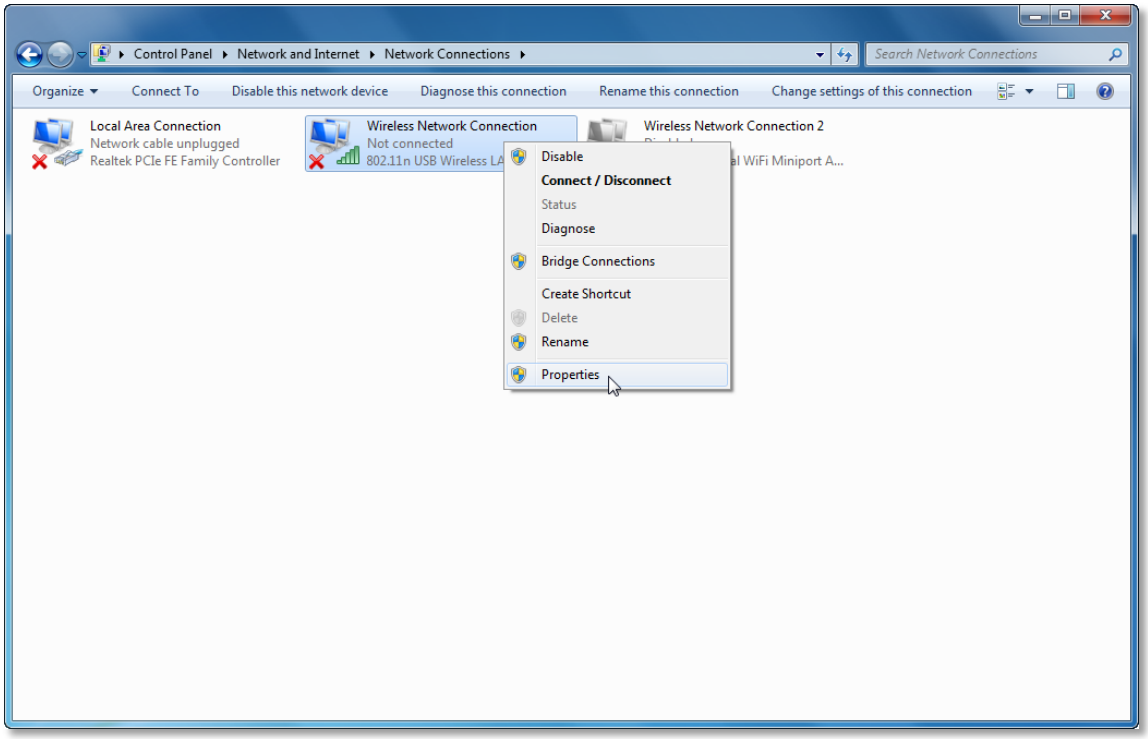
3) Click **Network and Sharing Center**.



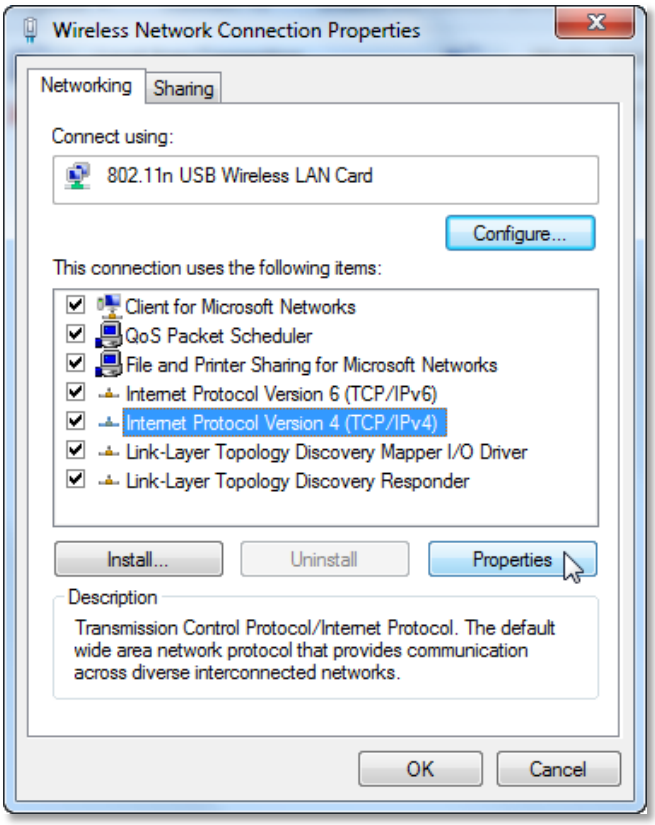
4) Go to **Change Adapter Settings** (win7)/**Manage Network Connections** (Vista).



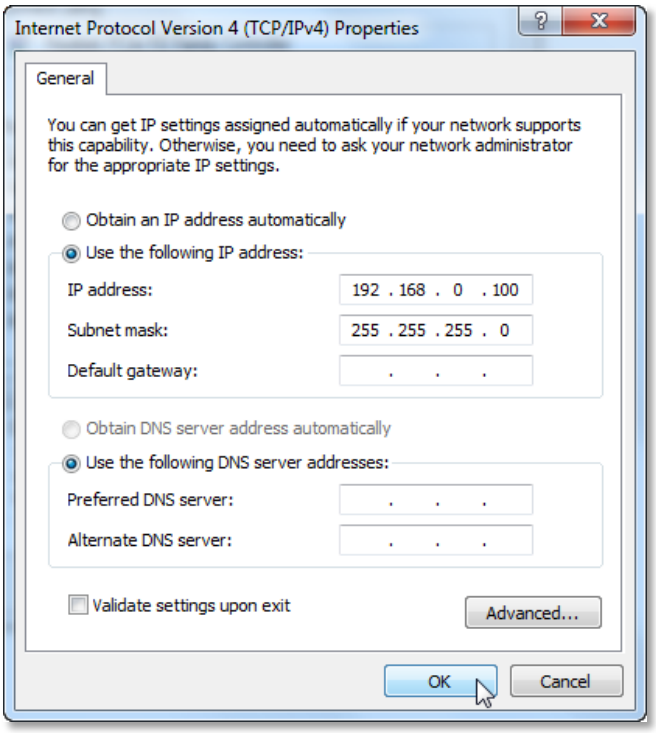
5) Right click **Wireless Network Connection**, choose **Properties**.



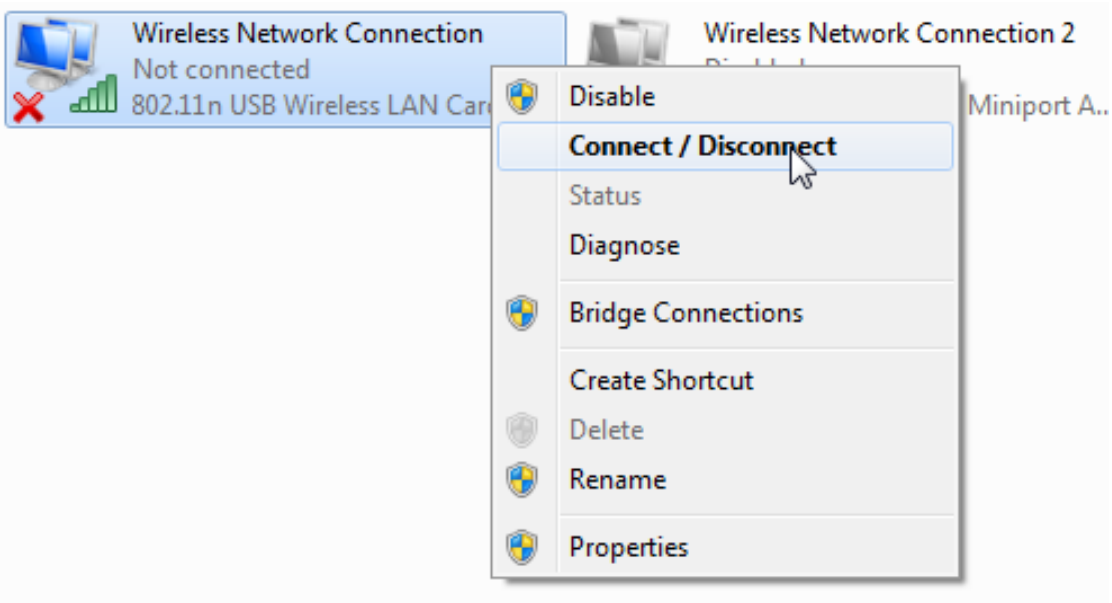
6) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



7) Select **Use the following IP address** and **Use the following DNS Server addresses**, the IP address put in 192.168.0.X (like 192.168.0.100), the Subnet mask put in 255.255.255.0, the Default gateway leave it blank, then click **OK**, and then click **OK** again.

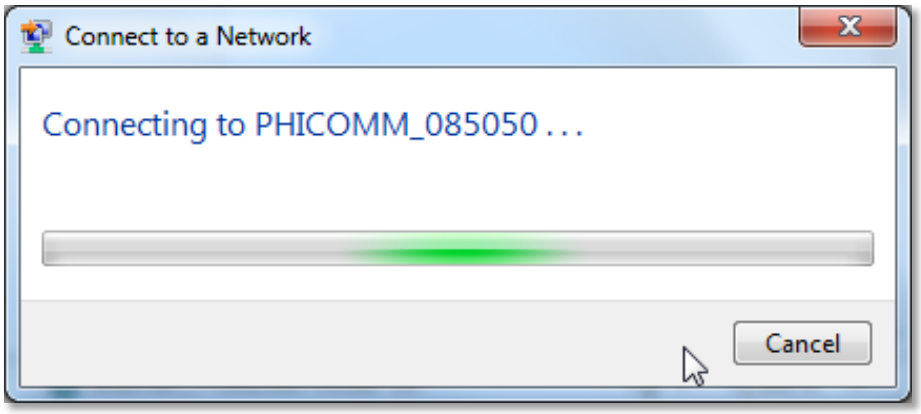


8) Right click on **Wireless Network Connection** again, choose **Connect/Disconnect**.



9) Click **Refresh network list**, search for PHICOMM_XXXXXX, highlight on it and then click **Connect** button.

10) You can see a windows pop up requires for a Network security key, you can find the key from the label attached on the Wireless Nano Router or the package box. Put in the network security key and then click **OK**.



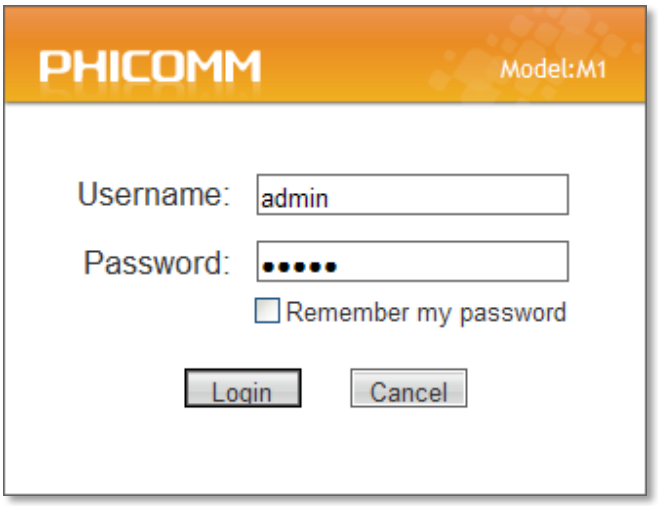
11) After you put in the correct network security key, you can see it showing connected.

Setup Wizard

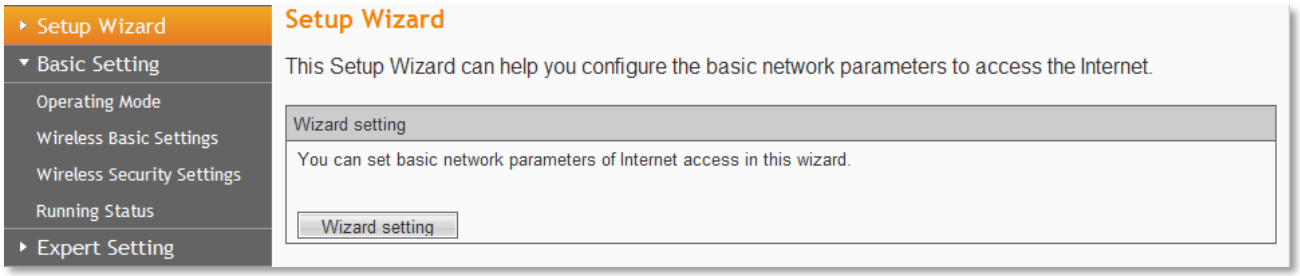
After successful installation, you can go ahead to configure the router by log in the web management page, please follow these instructions step by step:

1) Open your web browser, in the address bar, type in **192.168.0.1**

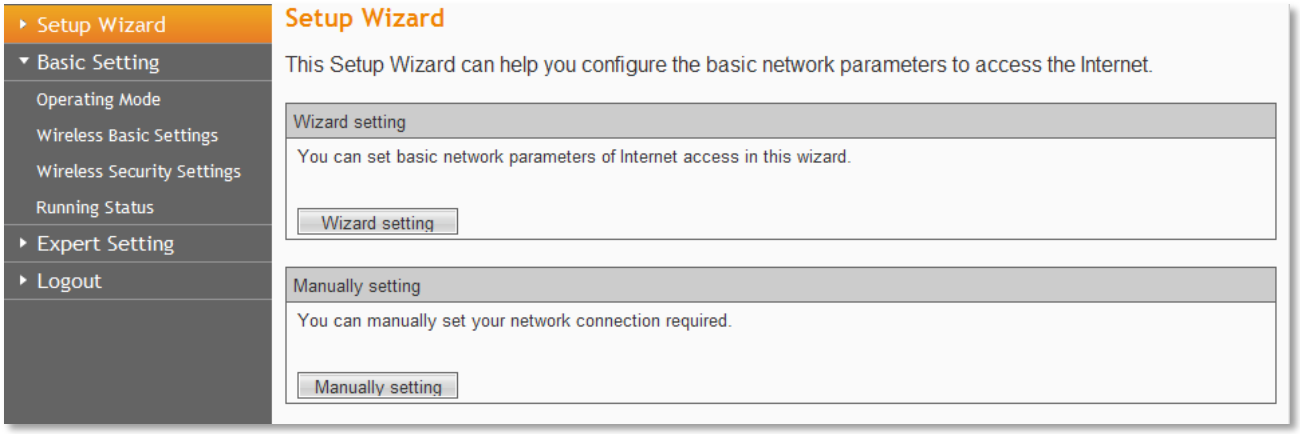
2) You are prompt to enter the Username/Password (preset as **admin**/**admin**) which you can found on the label attached to the router, click **Login**.



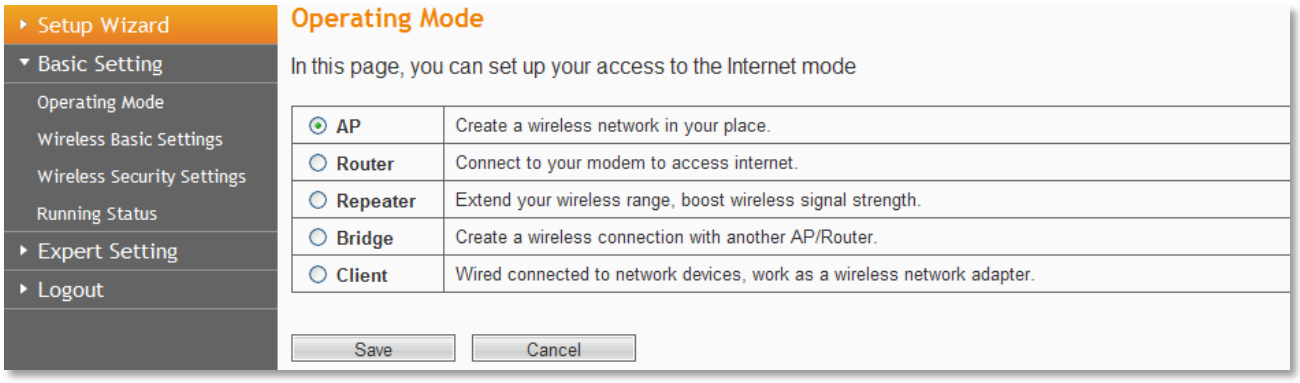
3) After successful login, you can see the web management page of the router comes up, please go to **Setup Wizard** on the left side menu.



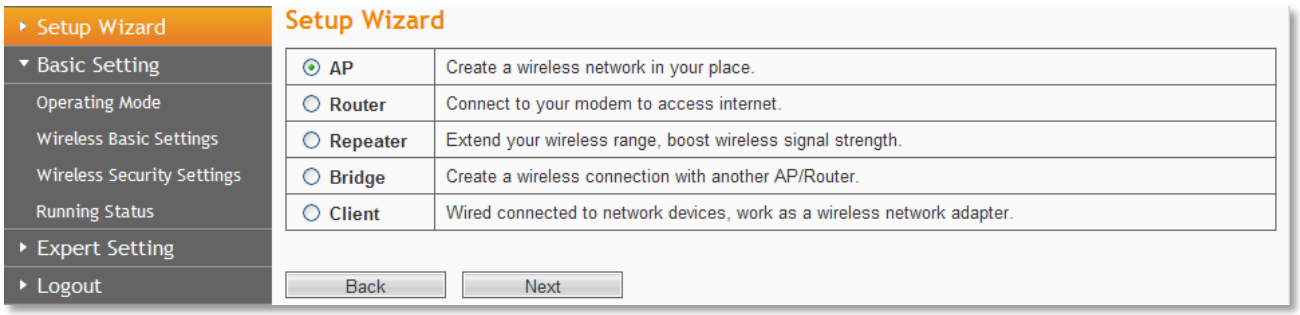
Note: If it is the first time you log in the web management page, only Wizard Setting option comes up. However, if you have changed any settings, you can see there is one more option **Manually Setting**, if you click on **Manually Setting**, you can quickly choose your operating mode and then save it.



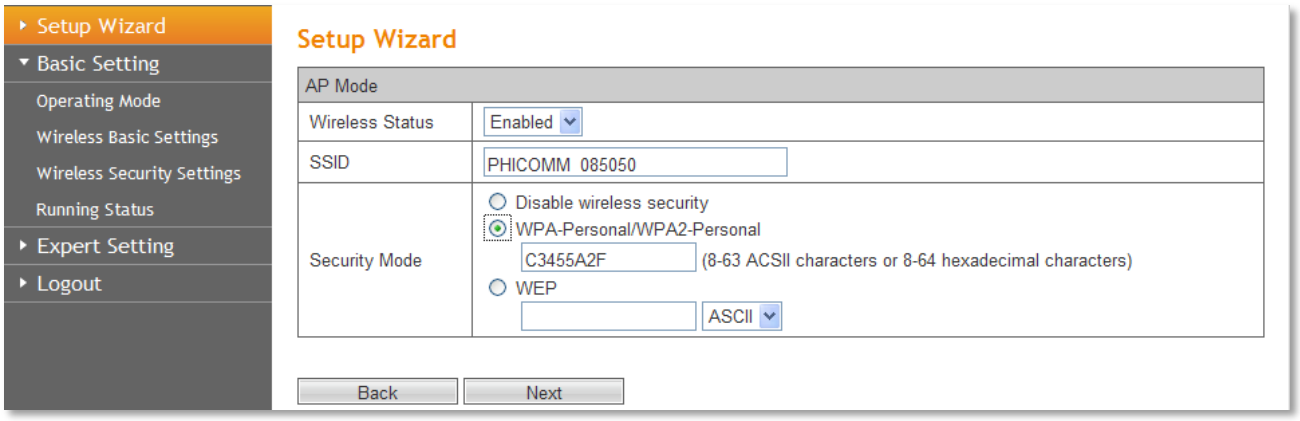
Click on **Manually Setting**.



Click on **Wizard setting.**

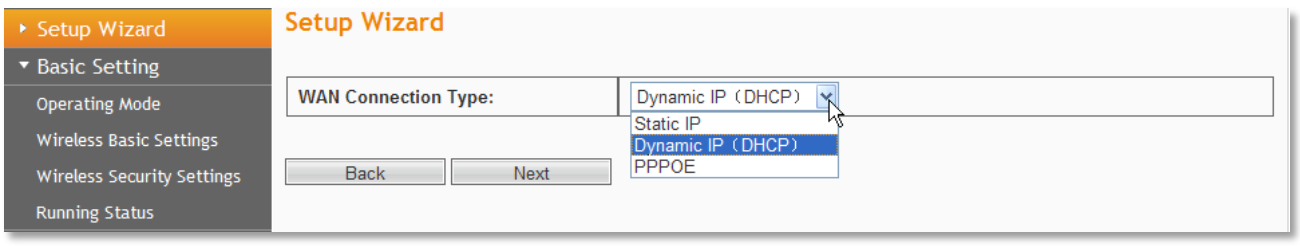


a) Choose **AP** mode.

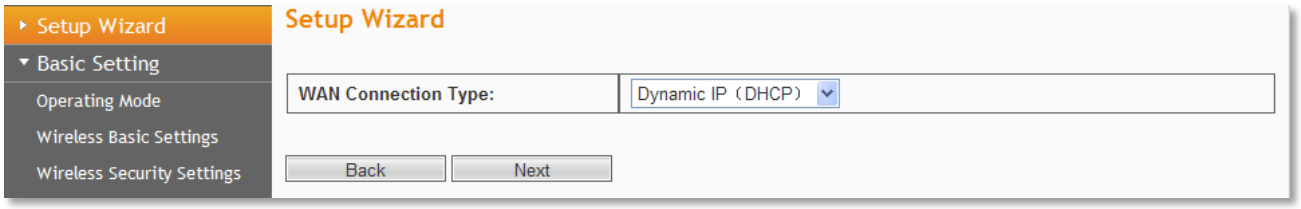


The SSID is the wireless network name of the AP, you can give it a different name, and we recommend you choose **WPA-Personal/WPA2-Personal** as your Security Mode.

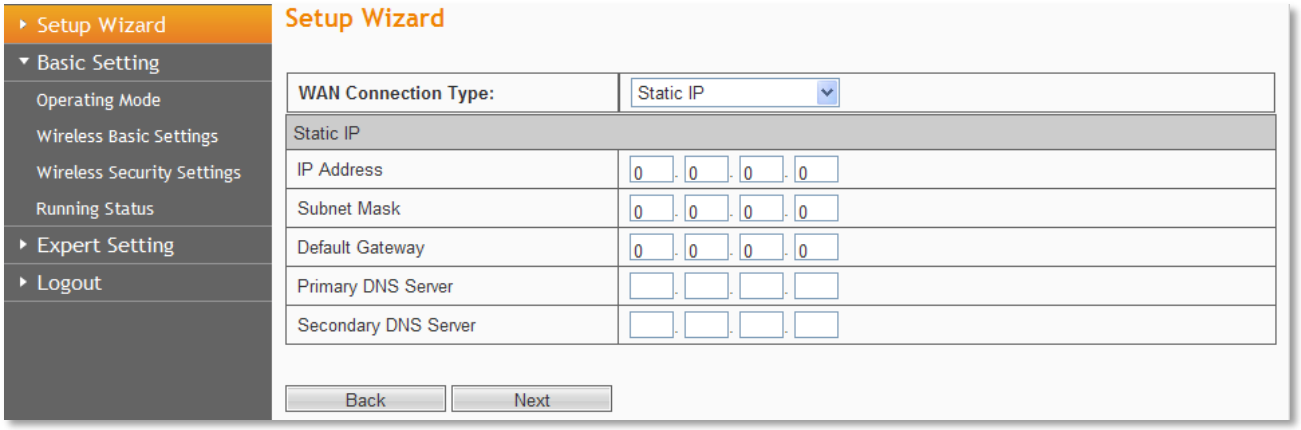
b) Choose **Router** mode.



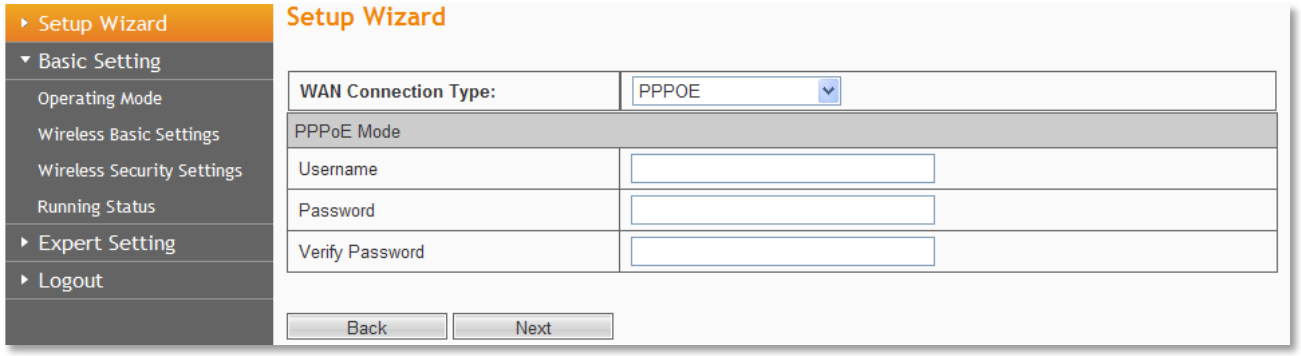
Dynamic IP(DHCP)



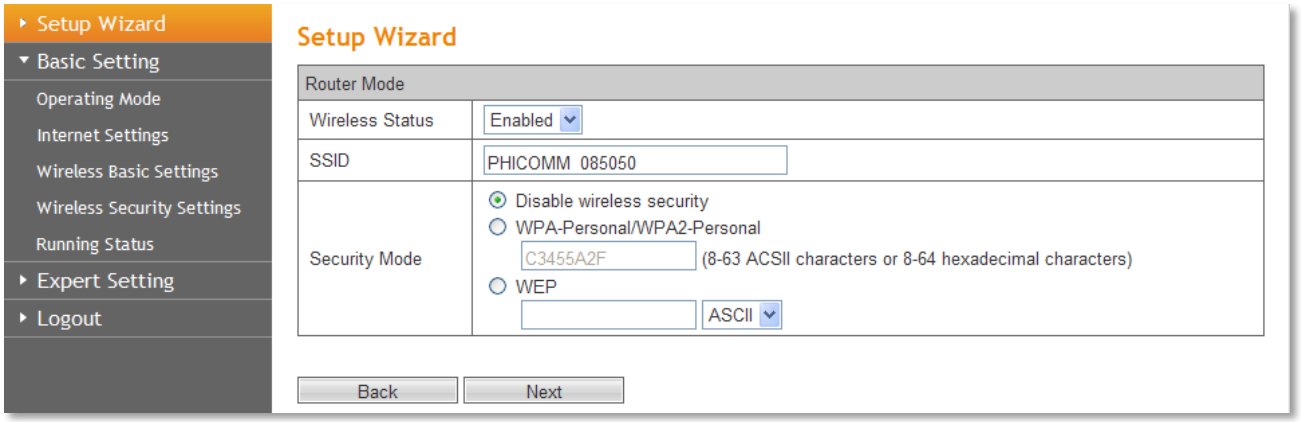
Static IP



PPPoE

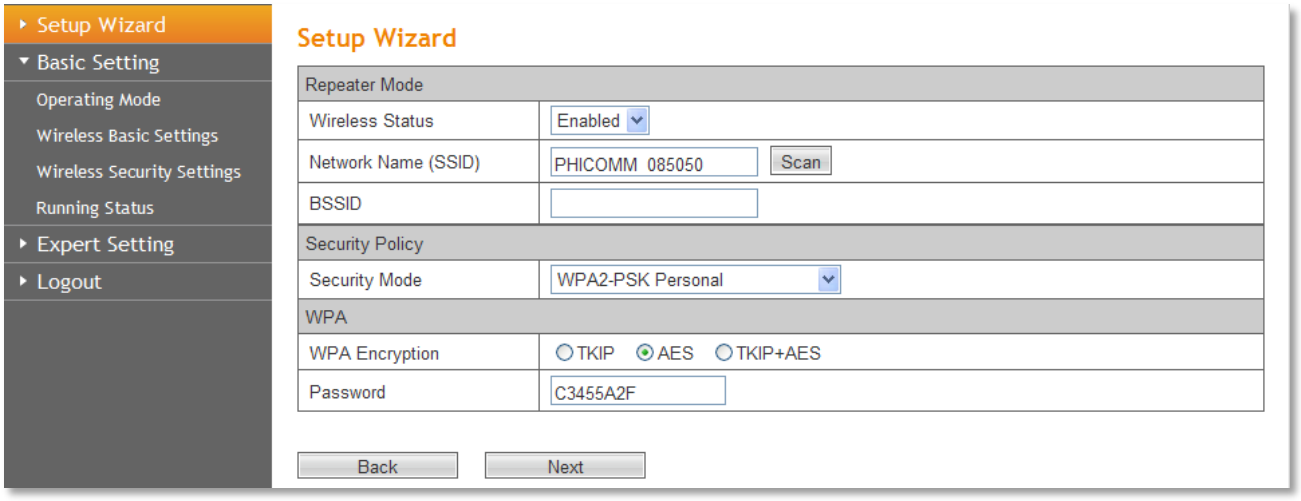


Click on **Next**.

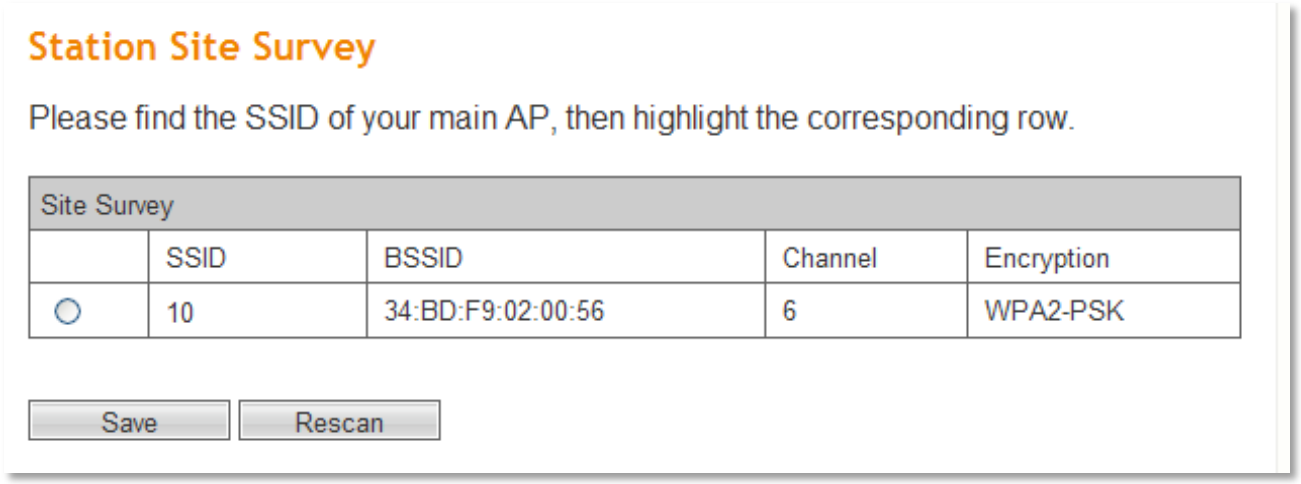


The SSID is the wireless network name of the router, you can give it a different name, and we recommend you choose **WPA-Personal/WPA2-Personal** as your Security Mode.

c) Choose **Repeater** mode.

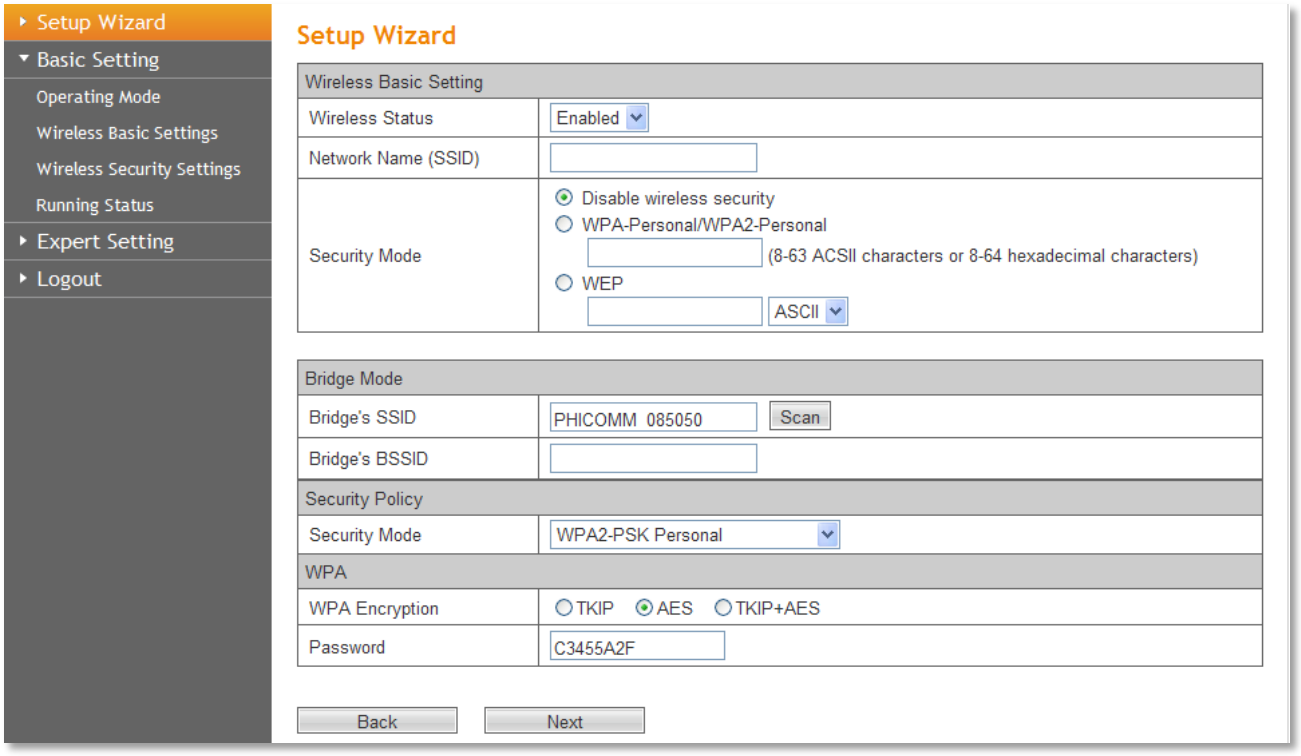


Click on **Scan** button, it will show the site list of scanning result, please find your main AP's SSID, then highlight the corresponding row, and then click **Save**.



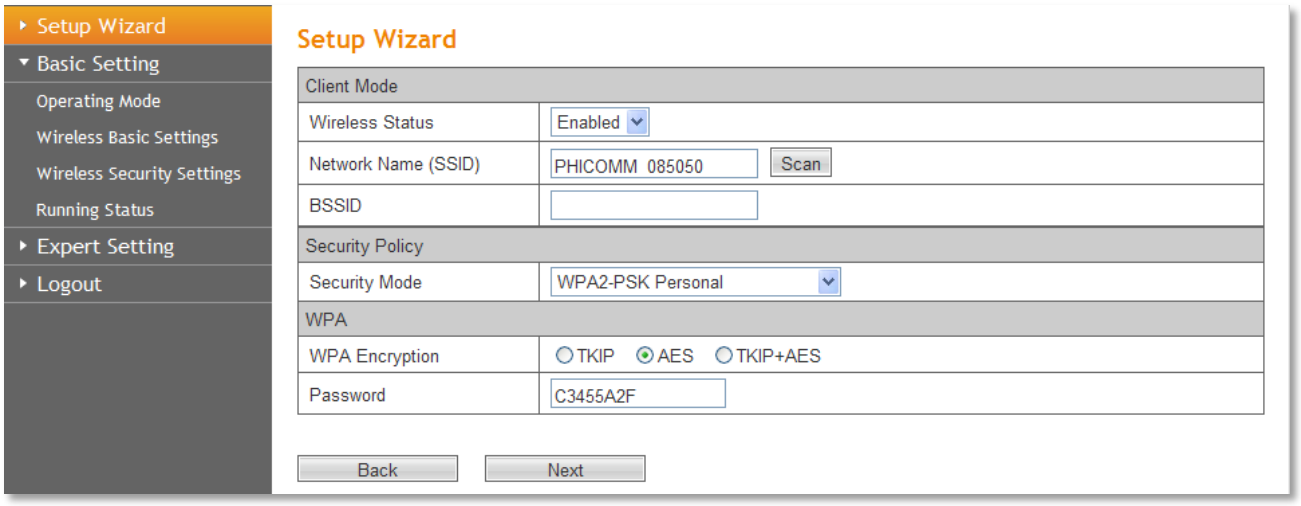
After that, the values you selected will be filled in the Network Name (SSID) and BSSID automatically. Choose the security mode and encryption type according to the wireless network you'd like to connect, and enter the password. Click **Next** to apply the settings.

d) Choose **Bridge** mode.



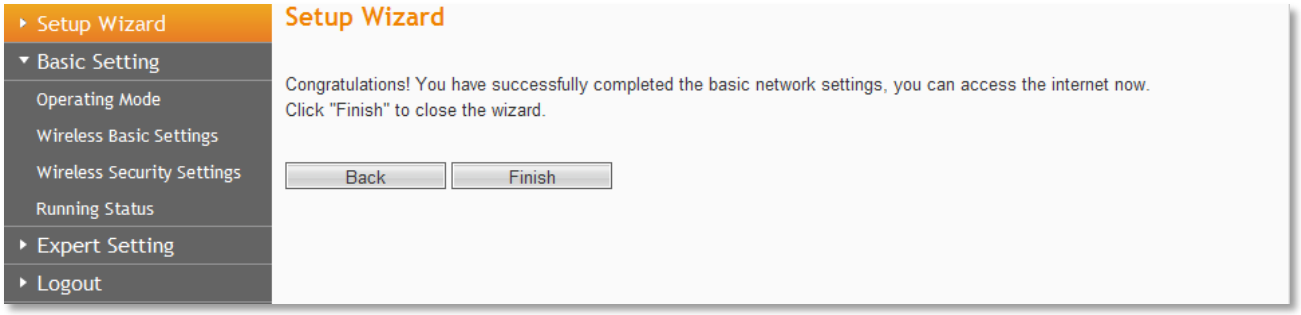
The SSID is the wireless network name of the bridge, you can give it a different name, and we recommend you choose **WPA-Personal/WPA2-Personal** as your Security Mode.

e) Choose **Client** mode.



The SSID is the wireless name of the Client, you can give it a different name, and we recommend you choose **WPA-Personal/WPA2-Personal** as your Security Mode.

Click on **Next**, and then click **Finish**.



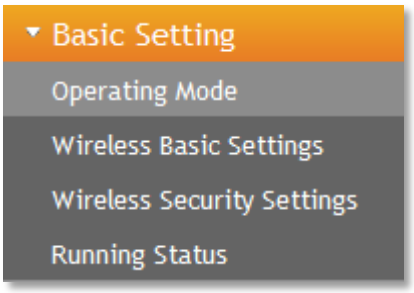
Chapter 4: Router Configuration

Basic Setting

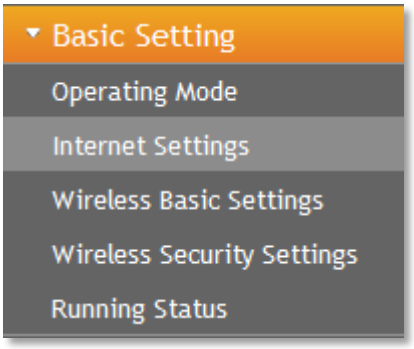
The **Basic Setting** section helps you to configure the Wireless Nano Router to access the Internet.

The submenus are different under different operating mode.

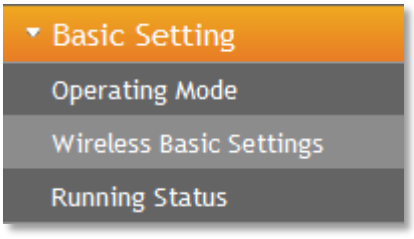
For **AP** and **Bridge** Mode:



For **Router** Mode:

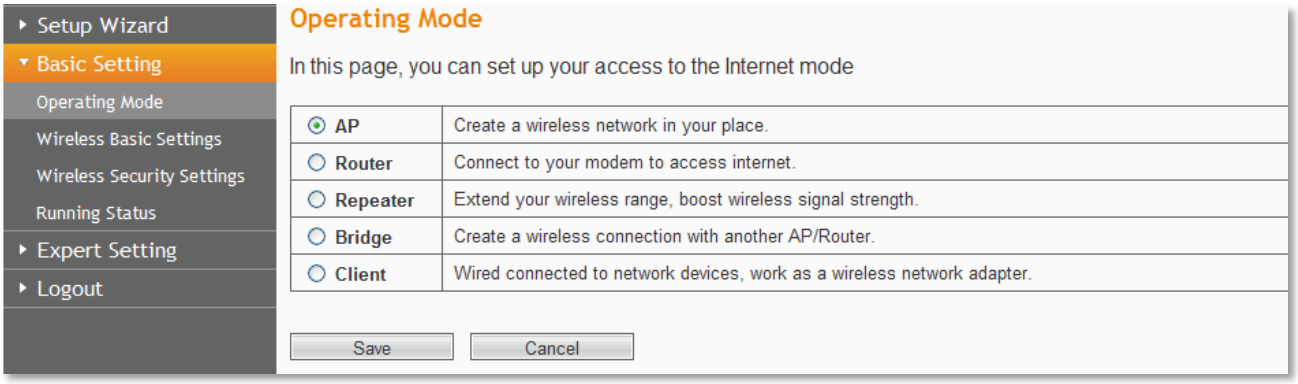


For **Repeater** and **Client** Mode:



Click any of them, you will be able to configure the corresponding function.

Operating Mode



Please choose the appropriate mode according to your requirement, it support AP, Router, Repeater, Bridge and Client mode.

AP: In this mode, the device allows wireless communication devices to connect to a wireless network by using WIFI. The Ethernet port and the wireless port both work as LAN ports.

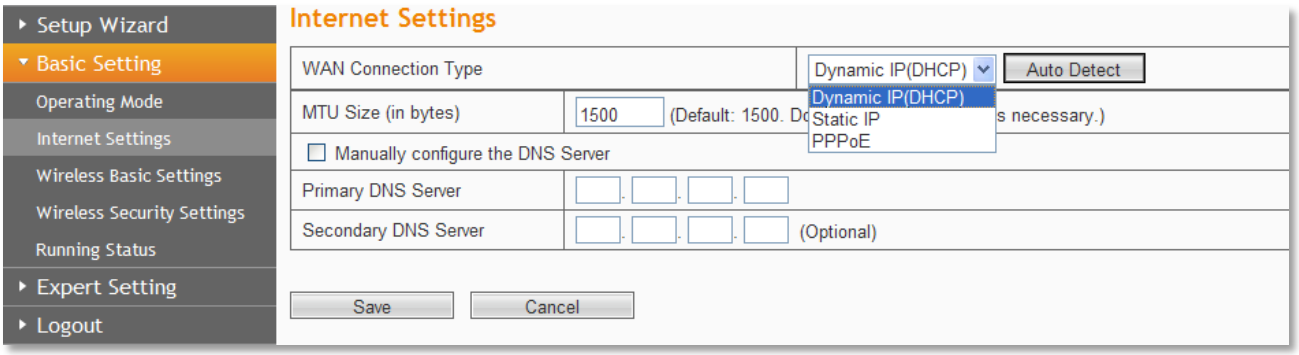
Router: In this mode, the device enables multiuser to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.

Repeater: The Repeater relays signal between its stations and the root AP for greater wireless range, it can boost wireless signal strength.

Bridge: This mode bridges the AP and another AP also in bridge mode to connect two wired LANs.

Client: In Client mode, it will act as a wireless station to enable wired host(s) to access wireless AP.

Internet Settings



This submenu only comes up under **Router** mode.

WAN Connection Type: To make sure the connection type your ISP provides, please refer to your ISP for more information.

Dynamic IP (DHCP): Connections use dynamic IP address assignment, it means your ISP is running a DHCP server.

Static IP: Connections use static IP address assignment, it means your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting.

PPPoE: Connections requires a username and a password.

MTU Size (in bytes): The default MTU (Maximum Transmission Unit) value is 1500 Bytes. Sometimes you need to modify the MTU required by your ISP.

Manually configure the DNS server: Check this one if your ISP gives you one or two DNS IP addresses. Otherwise, leave it unchecked, the DNS servers will be assigned from ISP dynamically.

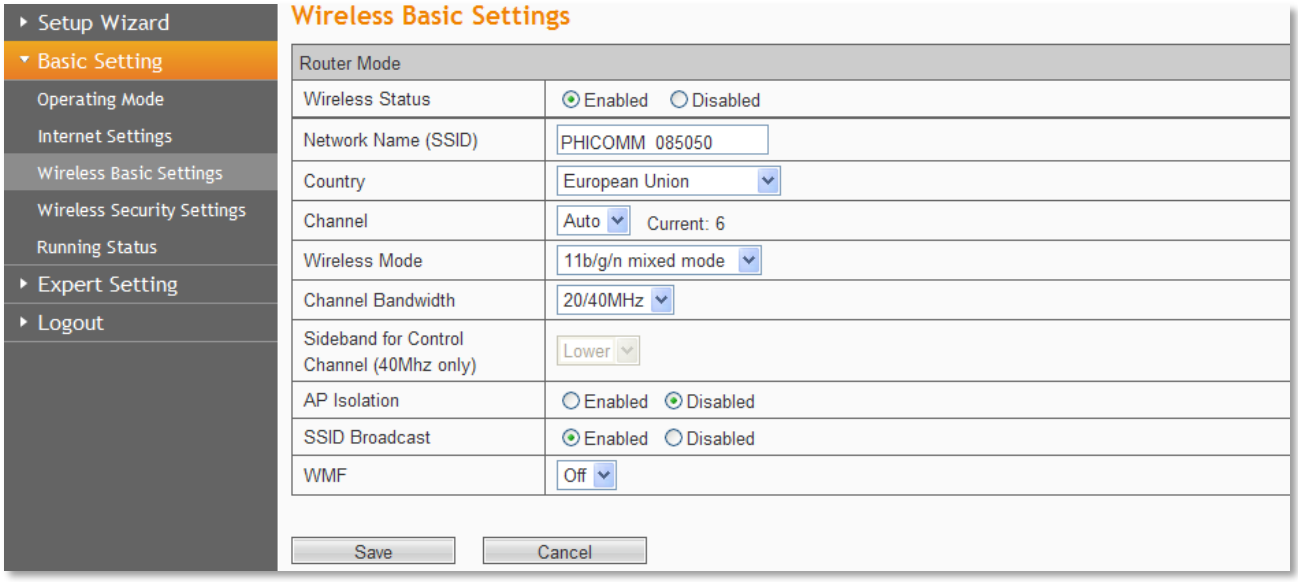
Primary DNS Server: Enter the DNS IP address in dotted-decimal notation provided by your ISP.

Secondary DNS Server: Enter another DNS IP address in dotted-decimal notation provided by your ISP.

Note: If you get Address not found error when you access a website, it is likely that your DNS servers are set up improperly. You should contact your ISP for correct DNS server addresses.

Wireless Basic Settings

a) AP and Router Mode



Wireless Status: Choose **Enable** to enable the wireless function of the router, choose **Disable** to disable the wireless function of the router.

Network Name (SSID): Enter a value of up to 32 characters. This is the wireless network name of your AP/Router; you can give it a different name which can be easier for you to remember.

Country: Select your country from the pull-down list.

Channel: The router can choose the best channel automatically in most cases. Please try to change the wireless channel if you notice interference problems with another nearby access point, or the wireless performance is not as good as you expected.

Wireless Mode: If all of the wireless devices connected with this wireless router are in the same transmission mode (e.g. 802.11b), you can choose "Only" mode (e.g. 11b only). If you have some

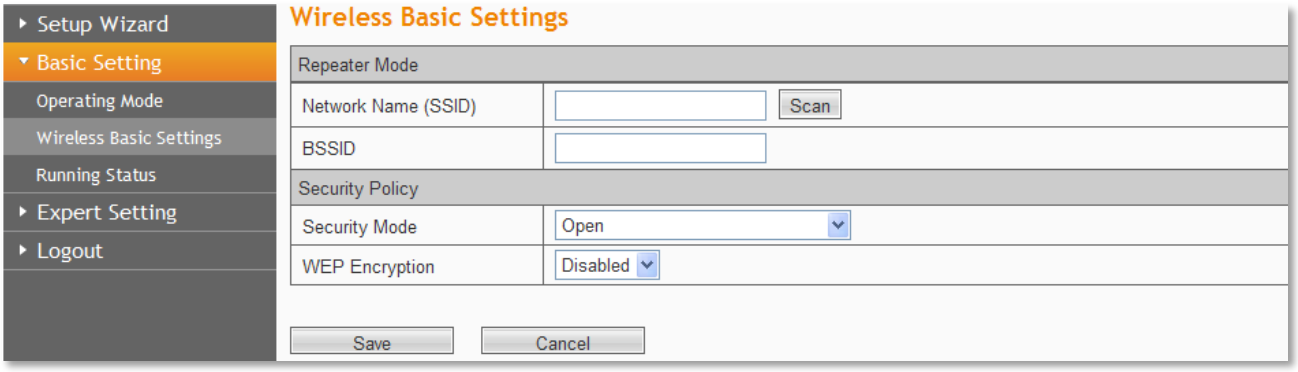
devices which use a different transmission mode, choose the appropriate "Mixed" mode.

Channel Bandwidth: The bandwidth of the wireless channel, you can select **20MHz** or **20/40MHz**.

AP Isolation: Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

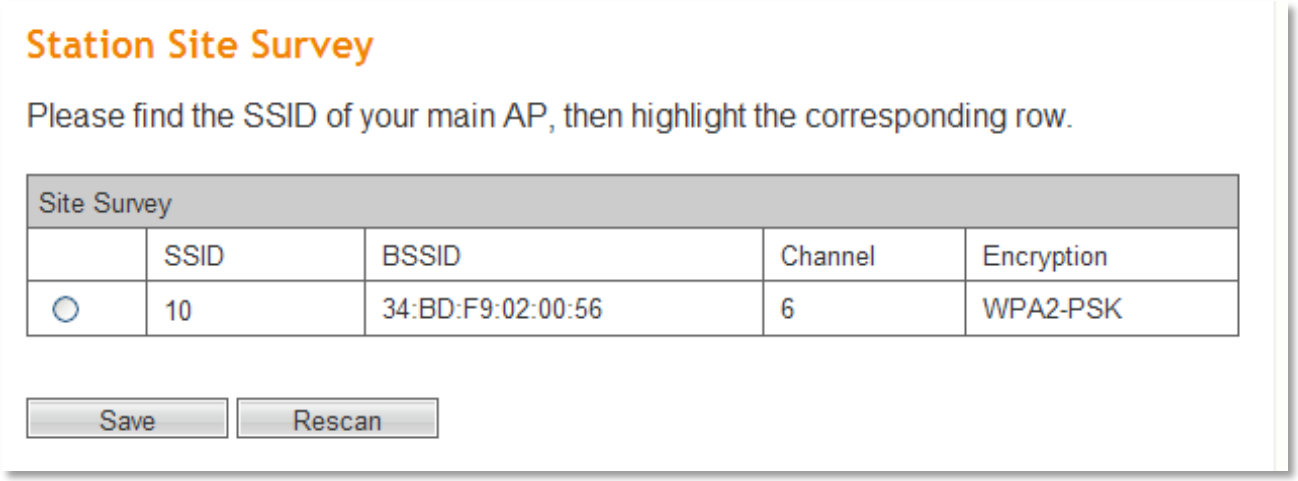
SSID Broadcast: If you choose **Enabled**, the wireless router will broadcast its name (SSID).

b) Repeater and Client Mode



Network Name (SSID): Enter a value of up to 32 characters. This is the wireless network name of your main AP.

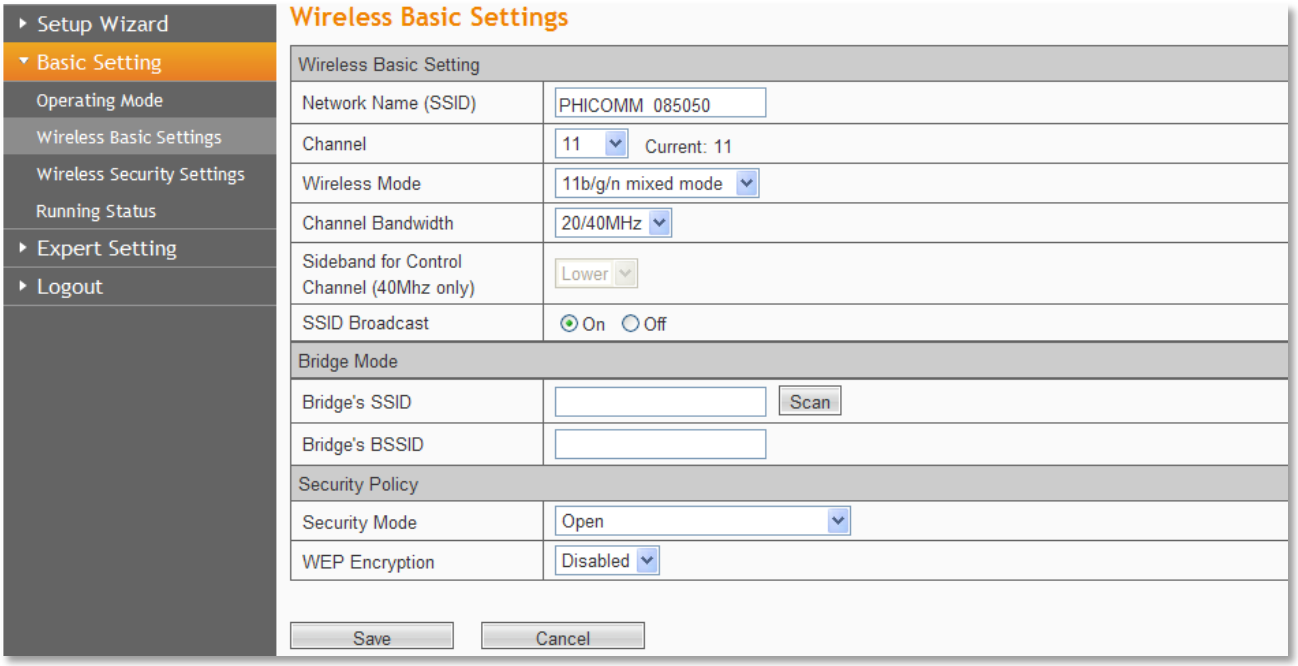
Click on **Scan** button, it will show the site list of scanning result, please find your main AP's SSID, then highlight the corresponding row, and then click **Save**.



BSSID: The physical address of your main AP.

Security Mode/Encryption Type: Choose the security mode and encryption type according to the wireless network you'd like to connect, and enter the password. Click **Next** to apply the settings.

c) Bridge mode



Network Name (SSID): Enter a value of up to 32 characters. This is the wireless network name of your main AP.

Channel: The router can choose the best channel automatically in most cases. Please try to change the wireless channel if you notice interference problems with another nearby access point, or the wireless performance is not as good as you expected.

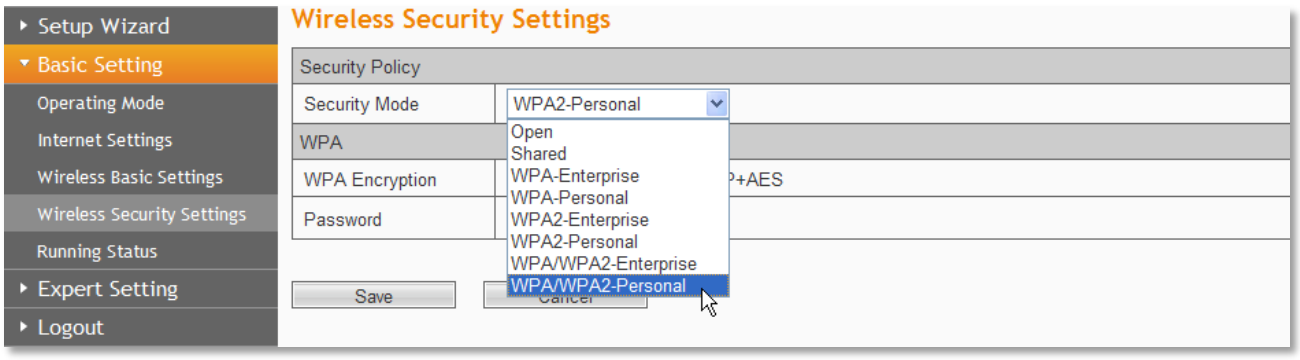
Wireless Mode: If all of the wireless devices connected with this wireless router are in the same transmission mode (e.g. 802.11b), you can choose "Only" mode (e.g. 11b only). If you have some devices which use a different transmission mode, choose the appropriate "Mixed" mode.
Channel Bandwidth: The bandwidth of the wireless channel, you can select **20MHz** or **20/40MHz**.

SSID Broadcast: If you choose Enabled, the wireless router will broadcast its name (SSID).
Bridge's SSID: The SSID of the other AP/router you want to be bridged with.

Bridge's BSSID: The physical address of the other AP/router you want to be bridged with.

Security Mode/Encryption Type: Choose the security mode and encryption type according to the wireless network you'd like to connect, and enter the password. Click **Next** to apply the settings.

Wireless Security Settings



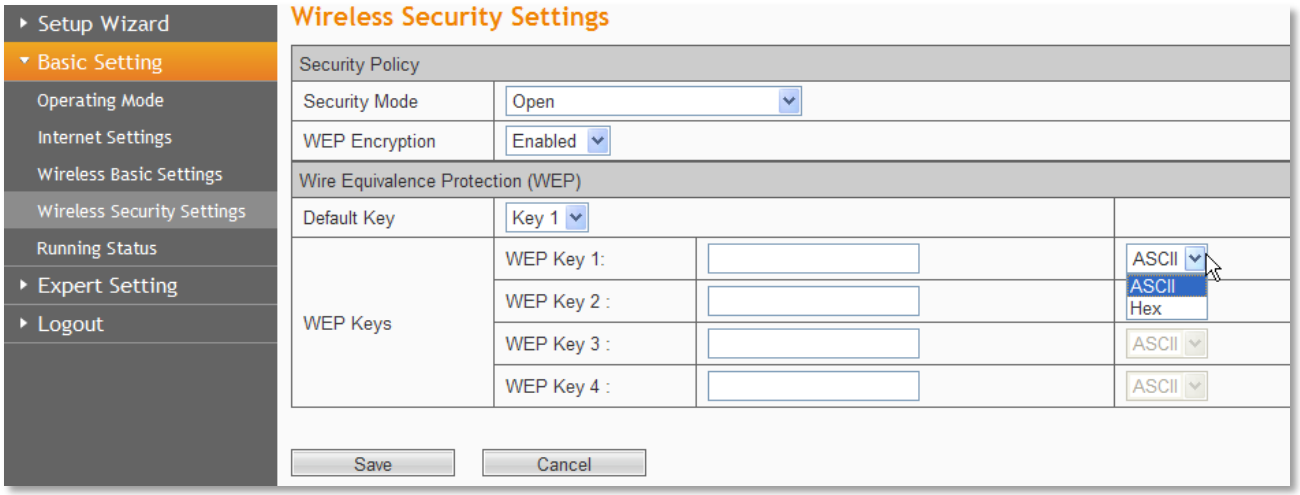
This submenu comes up under **AP**, **Bridge** and **Router** mode.

Security Mode: You can choose **Disable**, **Open**, **Shared**, **WPA-Enterprise**, **WPA2-Enterprise**, **WPA/ WPA2-Enterprise**, **WPA-Personal**, **WPA2-Personal**, **WPA/ WPA2-Personal**.

Mode 1: Security Mode > Disable

If you do not want to use wireless security, highlight on this option. That means other people can connect to your wireless network without entering any password, so it may slow down your internet speed, it's recommended strongly to choose one of the following modes to enable security.

Mode 2: Security Mode > Open/Shared



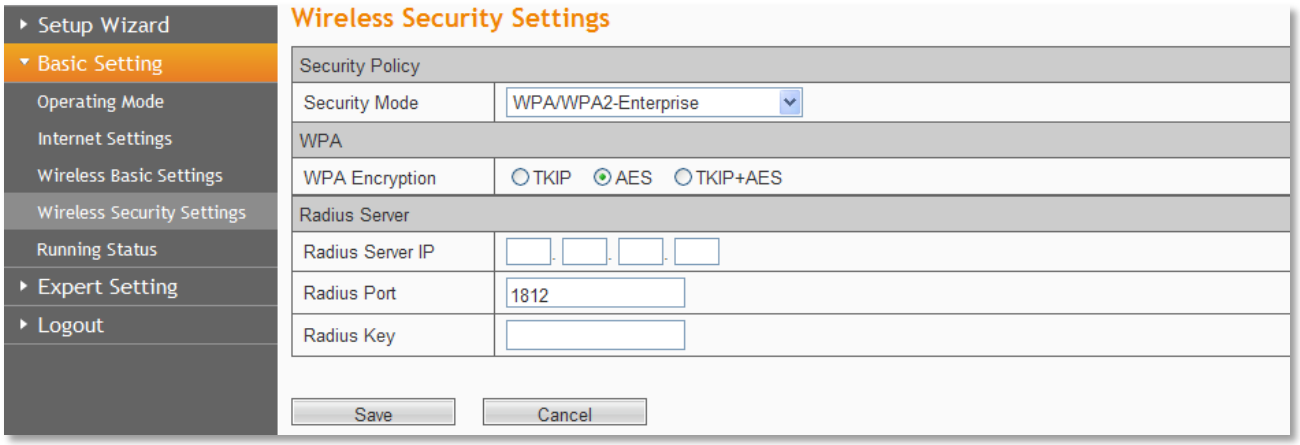
Open: Select 802.11 Open System authentications.

Shared: Select 802.11 Shared Key authentications.

You can select **ASCII** or **Hex** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hex format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters. Or enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters. Or enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

Mode 3: Security Mode > WPA-Enterprise, WPA2-Enterprise, WPA/ WPA2-Enterprise



WPA-Enterprise: Wi-Fi Protected Access, it's based on Radius Server

WPA2-Enterprise: Wi-Fi Protected Access version 2, it's based on Radius Server

WPA/ WPA2-Enterprise: Select **WPA-Enterprise** or **WPA2-Enterprise** automatically based on the wireless station's capability and request.

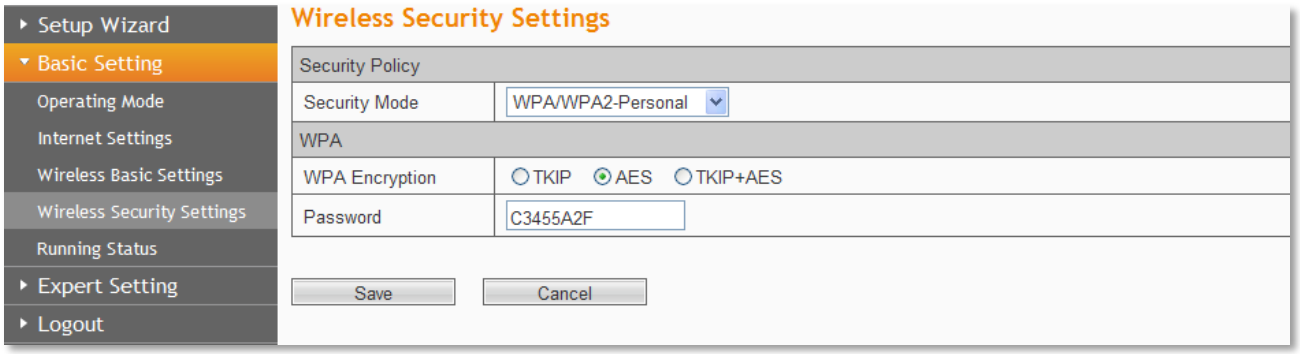
Encryption: You can select **TKIP**, **AES** or **TKIP+AES**.

Radius Server IP: The IP address of your Radius server.

Radius Port: The port your Radius server uses.

Radius Key: The Key of your Radius server.

Mode 4: Security Mode > WPA-Personal, WPA2-Personal, WPA/ WPA2-Personal



WPA-Personal: Pre-shared key of WPA.

WPA2-Personal: Pre-shared key of WPA2.

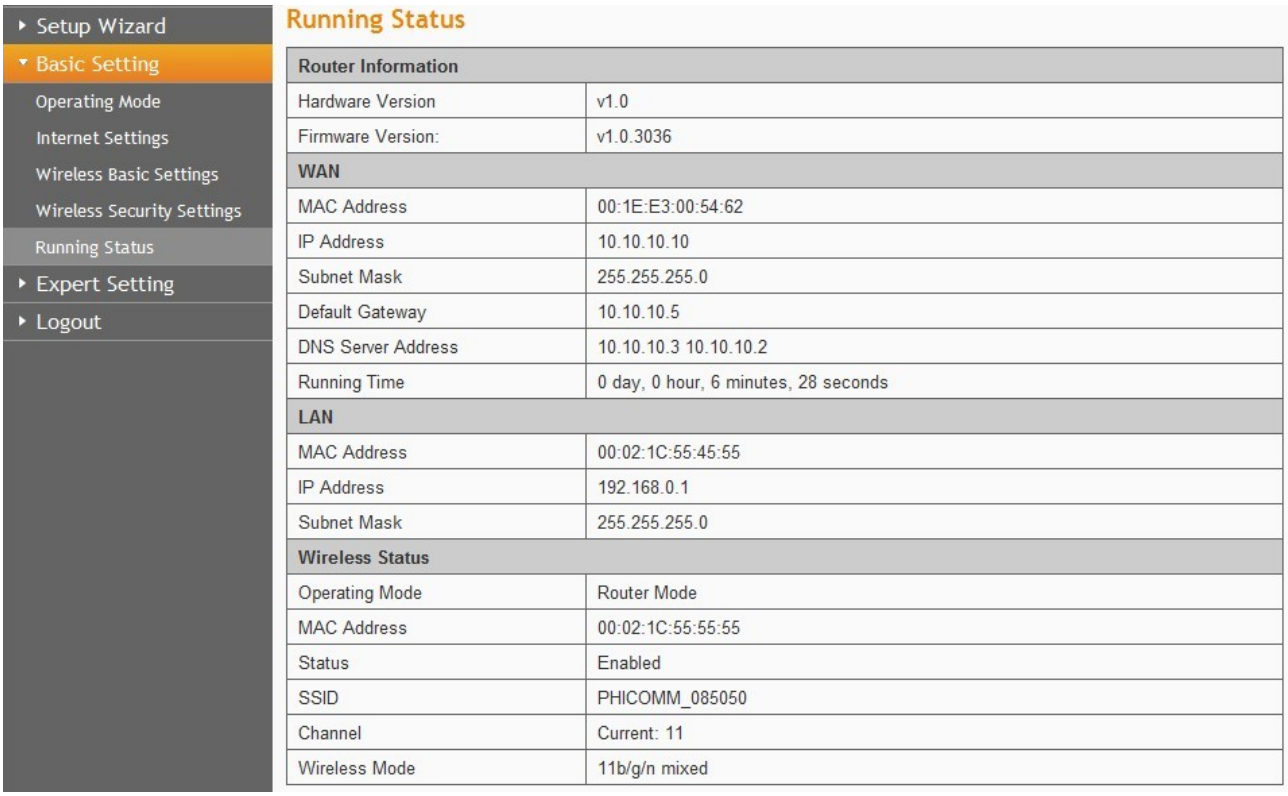
WPA/ WPA2-Personal: Select WPA-Personal or WPA2-Personal automatically based on the wireless station's capability and request.

Encryption: You can select **TKIP**, **AES** or **TKIP+AES**.

Password: The password should be between 8 and 63 characters.

Running Status

The **Running Status** page shows the current status of the Router.

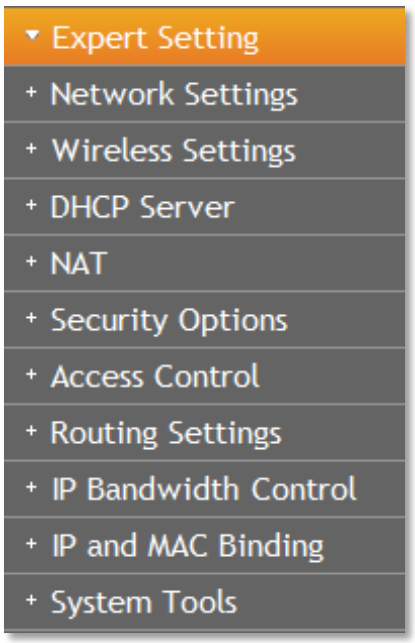


Router Information	
Hardware Version	v1.0
Firmware Version:	v1.0.3036
WAN	
MAC Address	00:1E:E3:00:54:62
IP Address	10.10.10.10
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.5
DNS Server Address	10.10.10.3 10.10.10.2
Running Time	0 day, 0 hour, 6 minutes, 28 seconds
LAN	
MAC Address	00:02:1C:55:45:55
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Wireless Status	
Operating Mode	Router Mode
MAC Address	00:02:1C:55:55:55
Status	Enabled
SSID	PHICOMM_085050
Channel	Current: 11
Wireless Mode	11b/g/n mixed

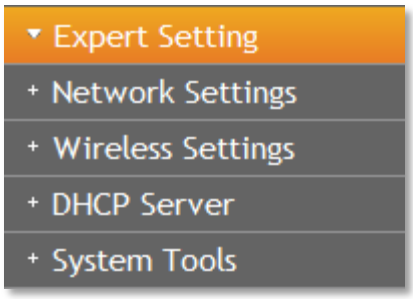
Expert Setting

The submenus are different under different operating mode.

For **Router** Mode:

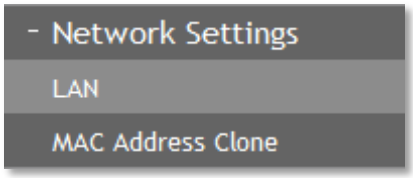


For **AP**, **Repeater**, **Bridge** and **Client** mode:

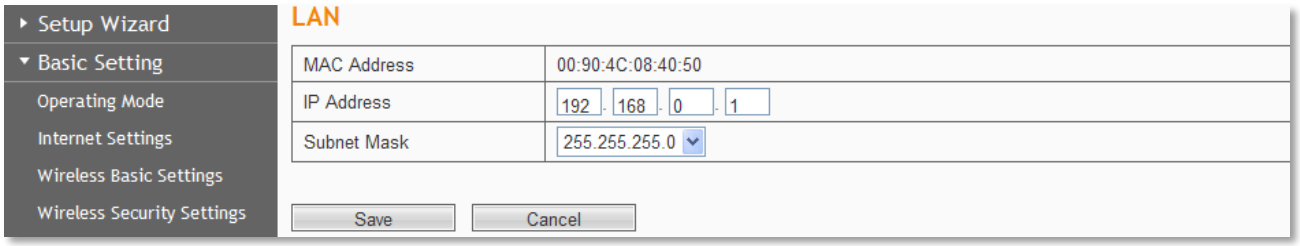


Click any of them, you will be able to configure the corresponding function.

Network Settings



LAN



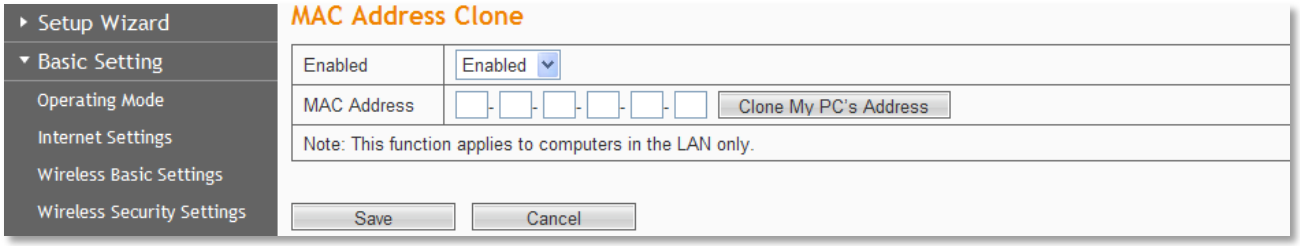
MAC Address: The physical address of the router.

IP Address: The LAN IP Address of the router.

Subnet Mask: The Subnet Mask associated with the LAN IP Address.

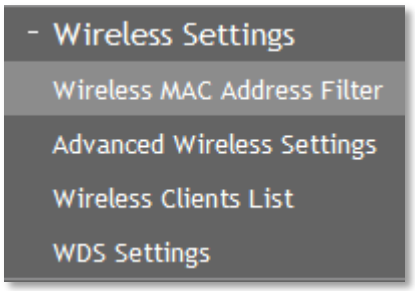
Note: If you changed the LAN IP Address of the router, please log in this web management page by the new IP address.

MAC Address Clone

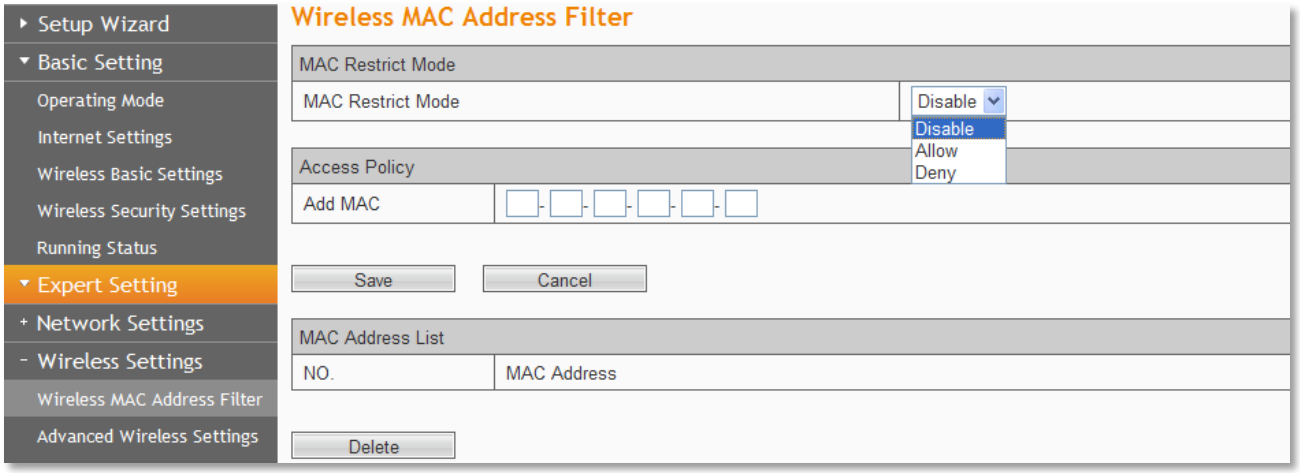


Some ISPs require you to register the MAC Address of your computer. Choose **Enabled**, and then click **Clone My PC's MAC Address**, then click **Save.**

Wireless Settings



Wireless MAC Address Filter



You can allow/deny the computers connecting to the router wirelessly by entering the MAC address with this feature.

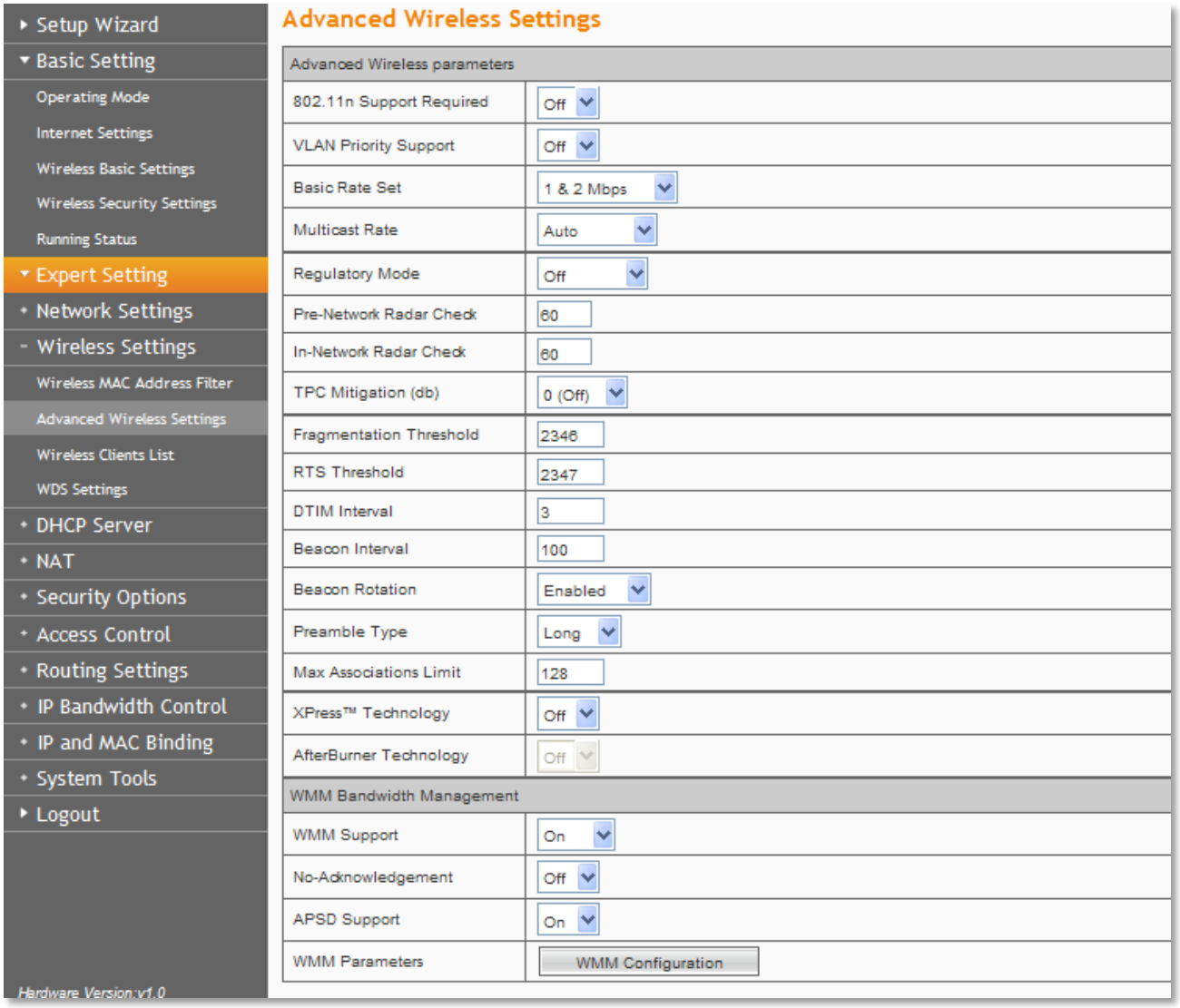
If you only want MAC address (00:0A:EB:00:07:5F) to access the Wireless Network while others cannot:

1. Choose **Allow** for the security policy.
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. Choose **Deny** for the security policy.
2. Filling MAC address 00:0A:EB:00:07:5F in and click **Save.**

Advanced Wireless Settings



This section is to configure the advanced wireless setting of the Router, 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.

Beacon Interval: The interval for sending packets of the Beacon frame. Its value range is 20-1000 in unit of ms. The default is 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.

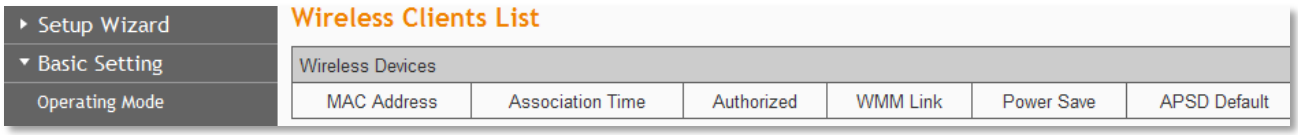
Fragment Threshold: Set the fragmentation threshold. Packets larger than the size set in this field will be fragmented. Too many data packets will lower the wireless network performance. The Fragment Threshold value should not be set too low. The default value is 2346.

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.

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

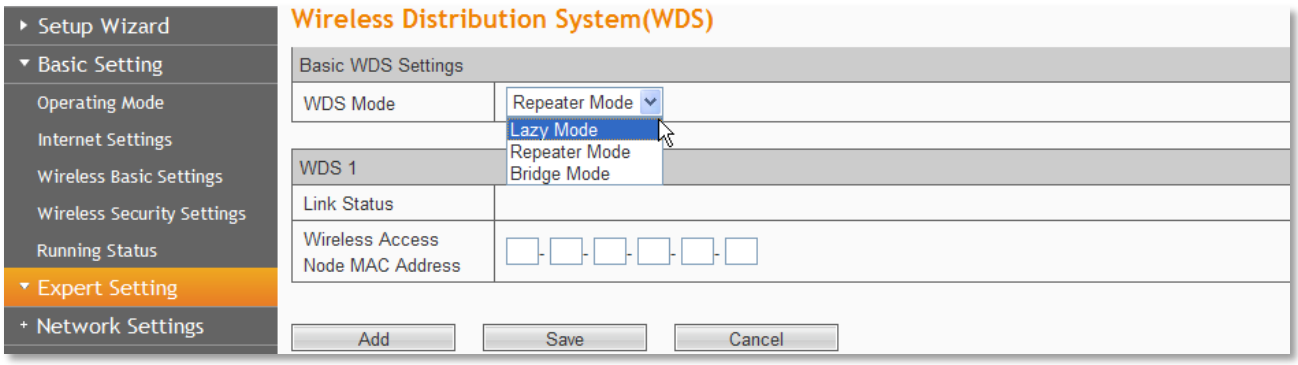
recommended to select this option.

Wireless Clients List



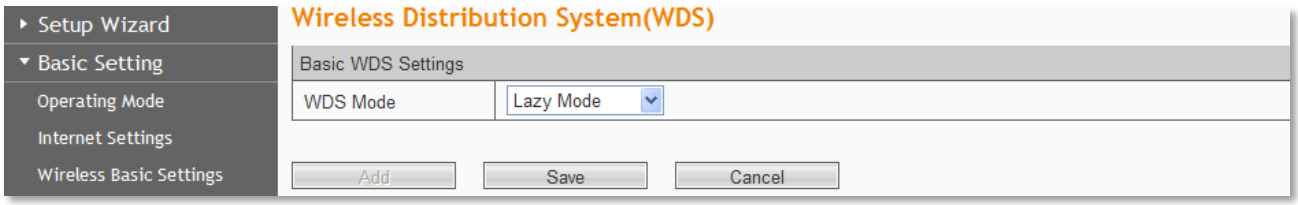
This list shows the wireless clients of the router.

WDS Settings



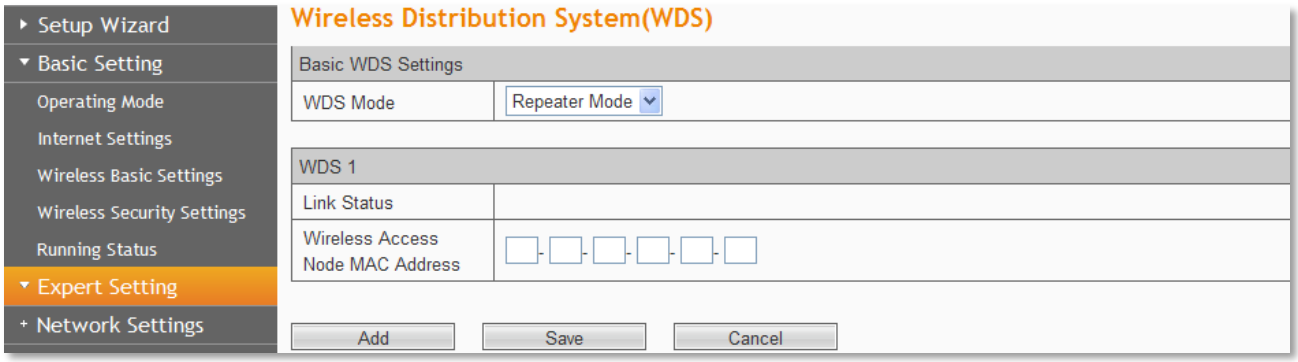
The WDS function can help you extend the wireless range; it supports **Lazy Mode**, **Repeater Mode** and **Bridge Mode.**

Lazy Mode



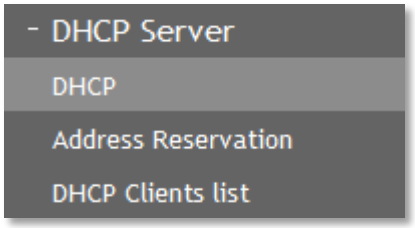
Choose **Lazy Mode**, you do not need to do any other configuration in this router, just click **Save**.

Repeater Mode and Bridge Mode

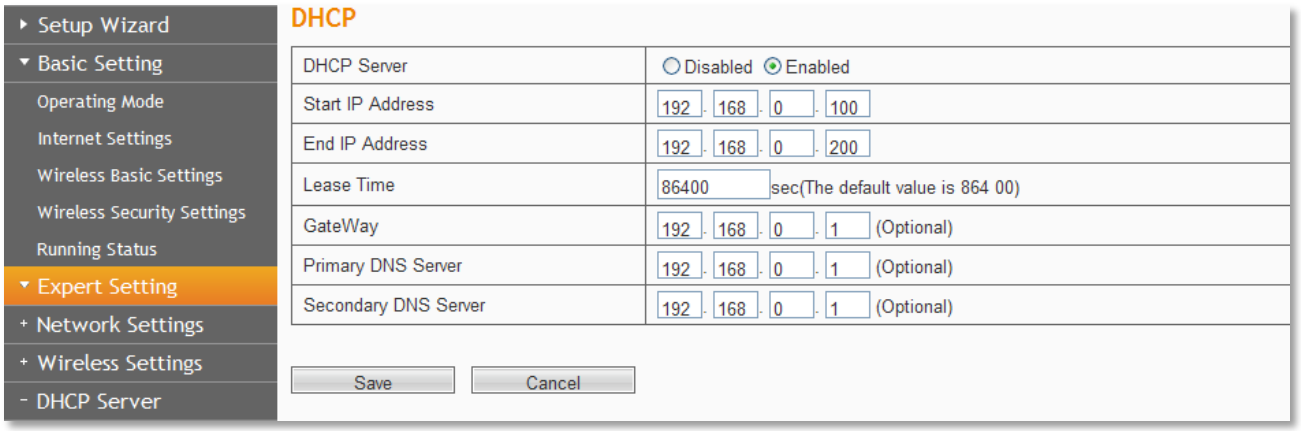


Wireless Access Node MAC Address: Input the MAC address of the other wireless router.

DHCP Server



DHCP



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

DHCP Server: If you disable the server, please make sure you have another DHCP server in your network.

Start IP Address: The first address in the IP Address pool.

End IP Address: The last address in the IP Address pool.

Lease Time: It is the time interval that server will change to use another DHCP address.

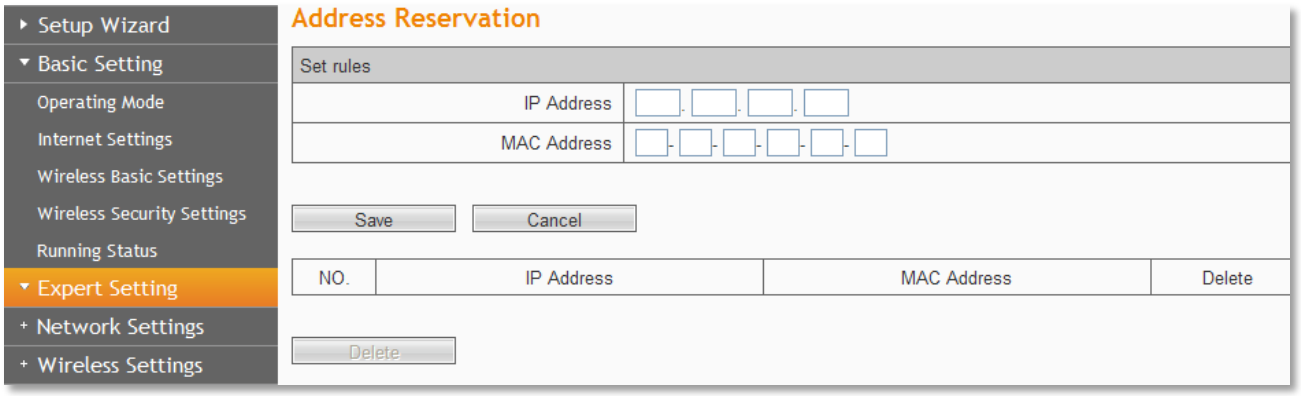
Gateway: (Optional) Suggest to input the IP Address of the LAN port of the Router.

Primary DNS Server: (Optional) Input the DNS IP address provided by your ISP. Or consult your ISP.

Secondary DNS Server: (Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Note: To use the DHCP server function of the router, please configure all computers in the LAN as Obtain an IP Address automatically mode. This function will take effect after the router rebooted.

Address Reservation

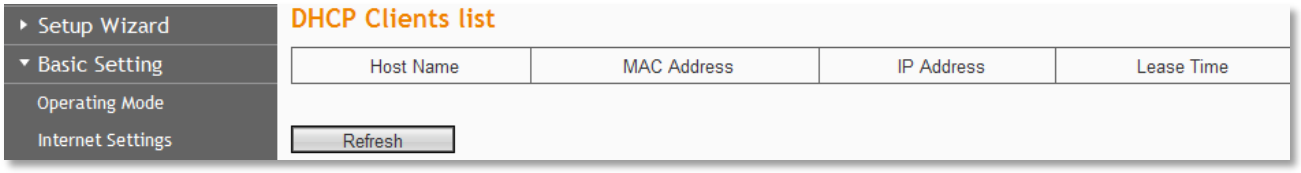


When you specify a reserved IP address for a PC in the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses could be assigned to servers that require permanent IP settings.

IP Address: The IP address that the Router reserved.

MAC Address: The MAC Address of the PC that you want to reserve for an IP address.

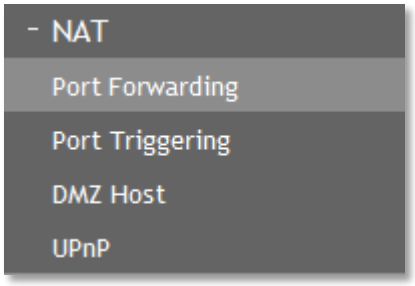
DHCP Clients list



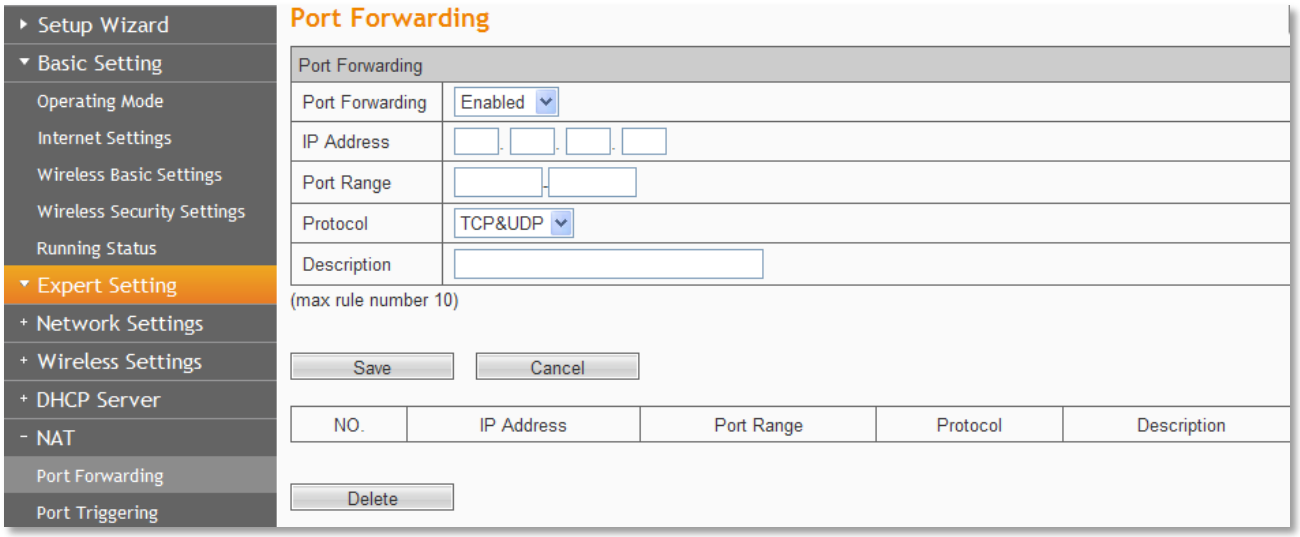
Here you can see the information of DHCP Clients.

Refresh: Click **Refresh** button to refresh the DHCP clients list.

NAT



Port Forwarding



Rule's Name: You can give this rule a name.

IP Address: The IP address of the server you want to open the port, it is like 192.168.0.X.

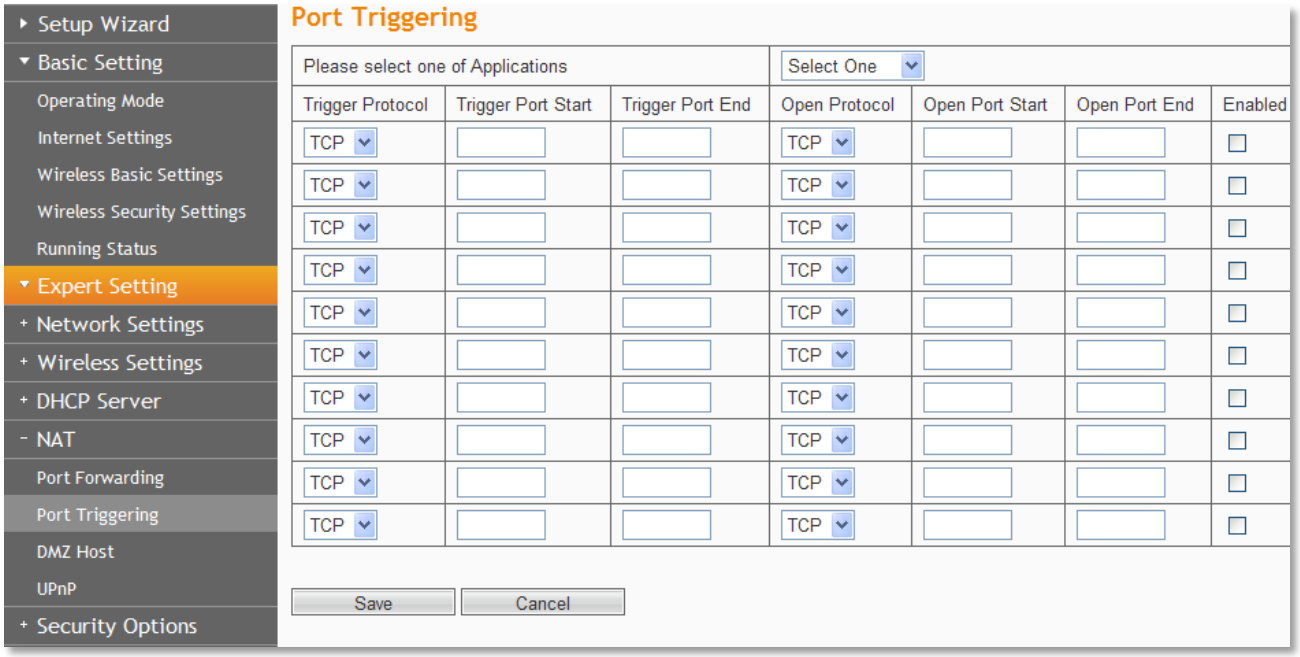
Port Range: The port range of the server you want to open the port.

Protocol: The protocol of the server.

Description: You can give it a description.

Note: Please assign a static IP address to the server.

Port Triggering



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.

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

will trigger this rule.

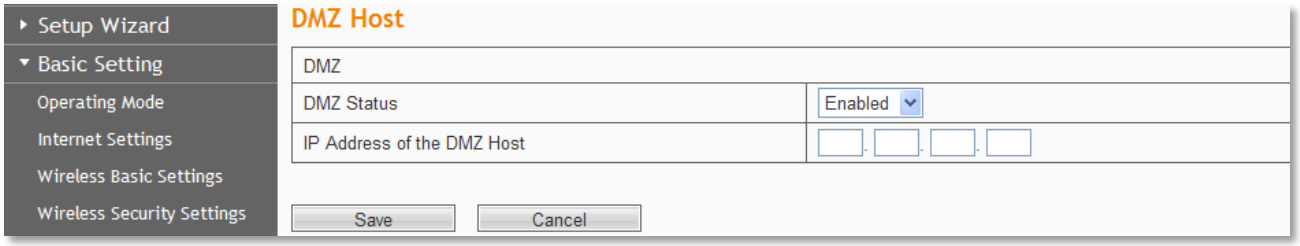
Trigger Protocol: The protocol used for Trigger Ports: **TCP**, **UDP** or **TCP/UDP**. If you are not clear about which protocol was being used, **TCP/UDP** is recommended.

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, it can be **TCP**, **UDP** or **TCP/UDP**. If you are not clear about which protocol was being used, **TCP/UDP** is recommended.

Note: Before using Port Triggering, please assign a static IP address to the designated server, and then enter this static IP address into router as the IP Address.

DMZ Host



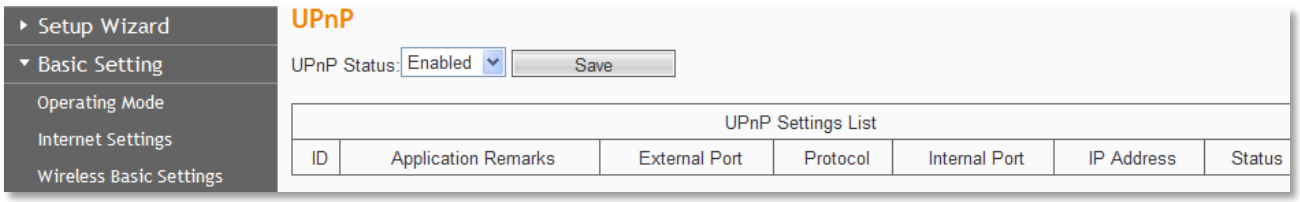
DMZ Status: Choose **Enabled** or **Disabled** to enable or disable this function.

IP Address of the DMZ Host: 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.

Note:

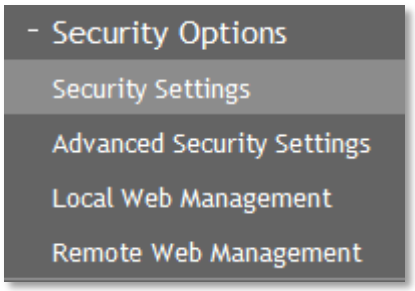
- Before using DMZ Host, you should assign a static IP address to the designated server, and then enter this static IP address into router as the **IP Address.**
- DMZ priority is higher than the Port Forwarding, if the DMZ open, all the port forwarding rules are not effective.

UPnP

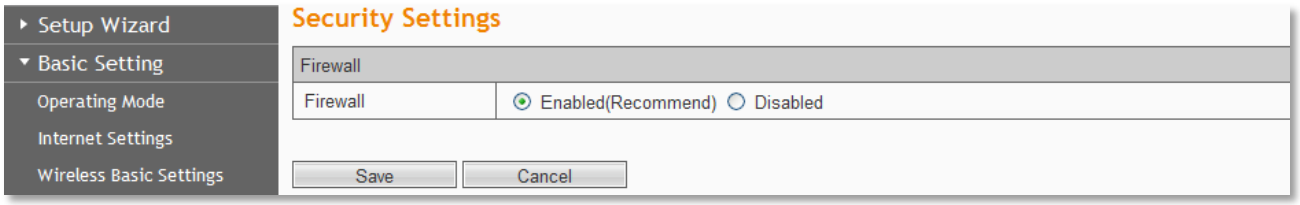


UPnP Status: Select **Enabled** or **Disabled** to enable or disable this function.

Security Options

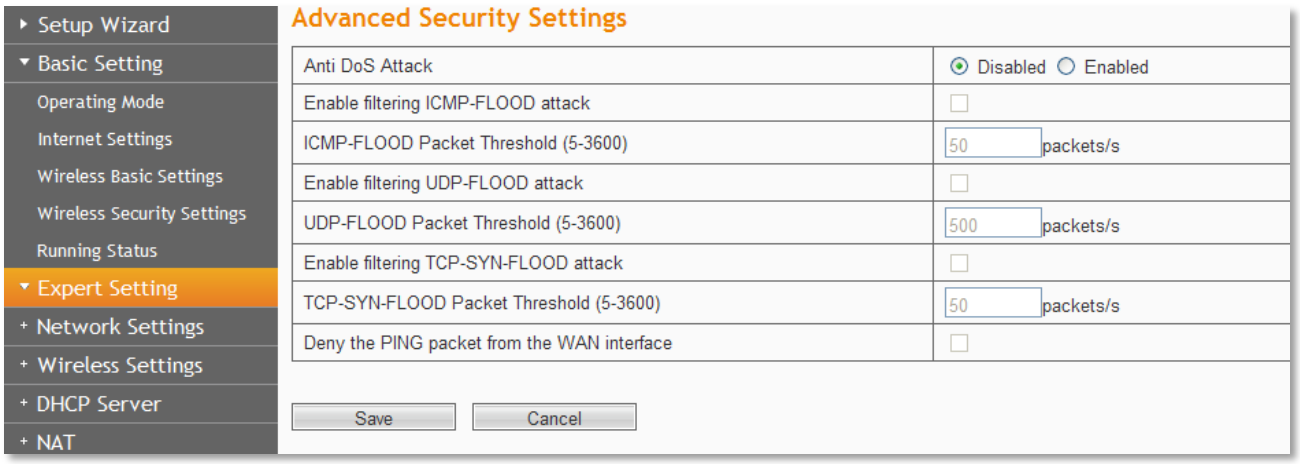


Security Settings



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

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.

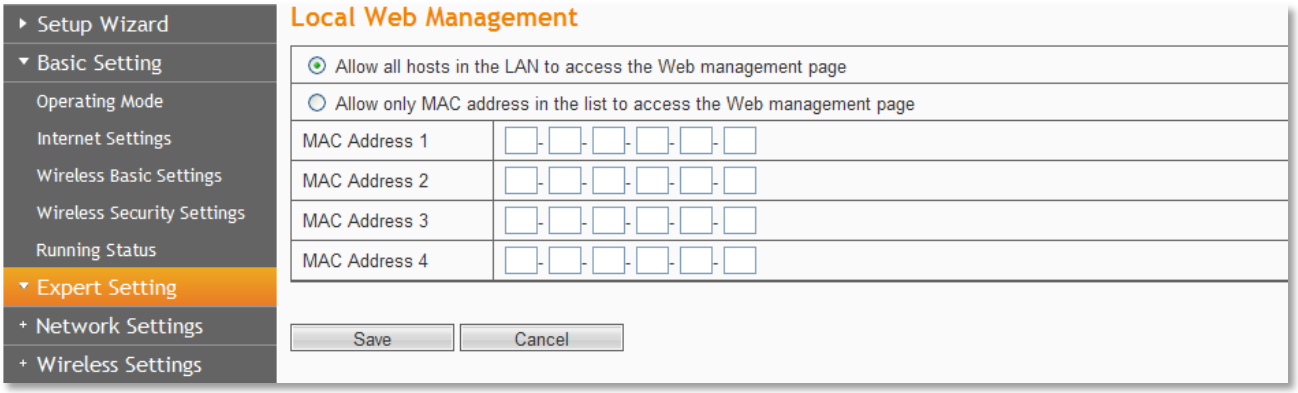
TCP-SYN-Attack Packet Threshold: If the number of TCP-SYN data packets exceeds the

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.

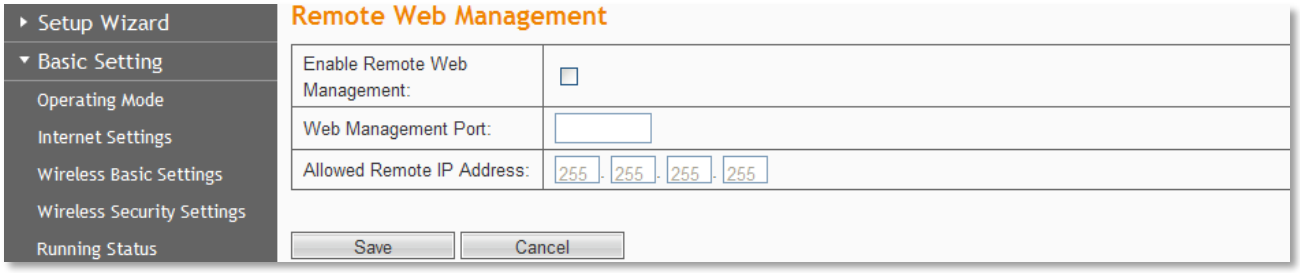
Local Web Management



By default, the router allows all computers in the LAN to log in to the router for Web management. If you select **Allow only MAC addresses in the list to access the Web management page**, and add MAC addresses to the list, only MAC addresses in the list can access the web management page of the router, while other computers in the LAN are blocked from accessing the router.

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

Remote Web Management

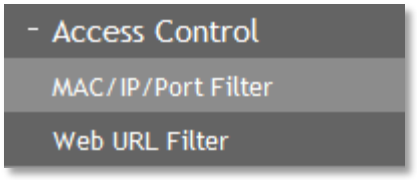


This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please highlight **Enable Remote Web Management**.

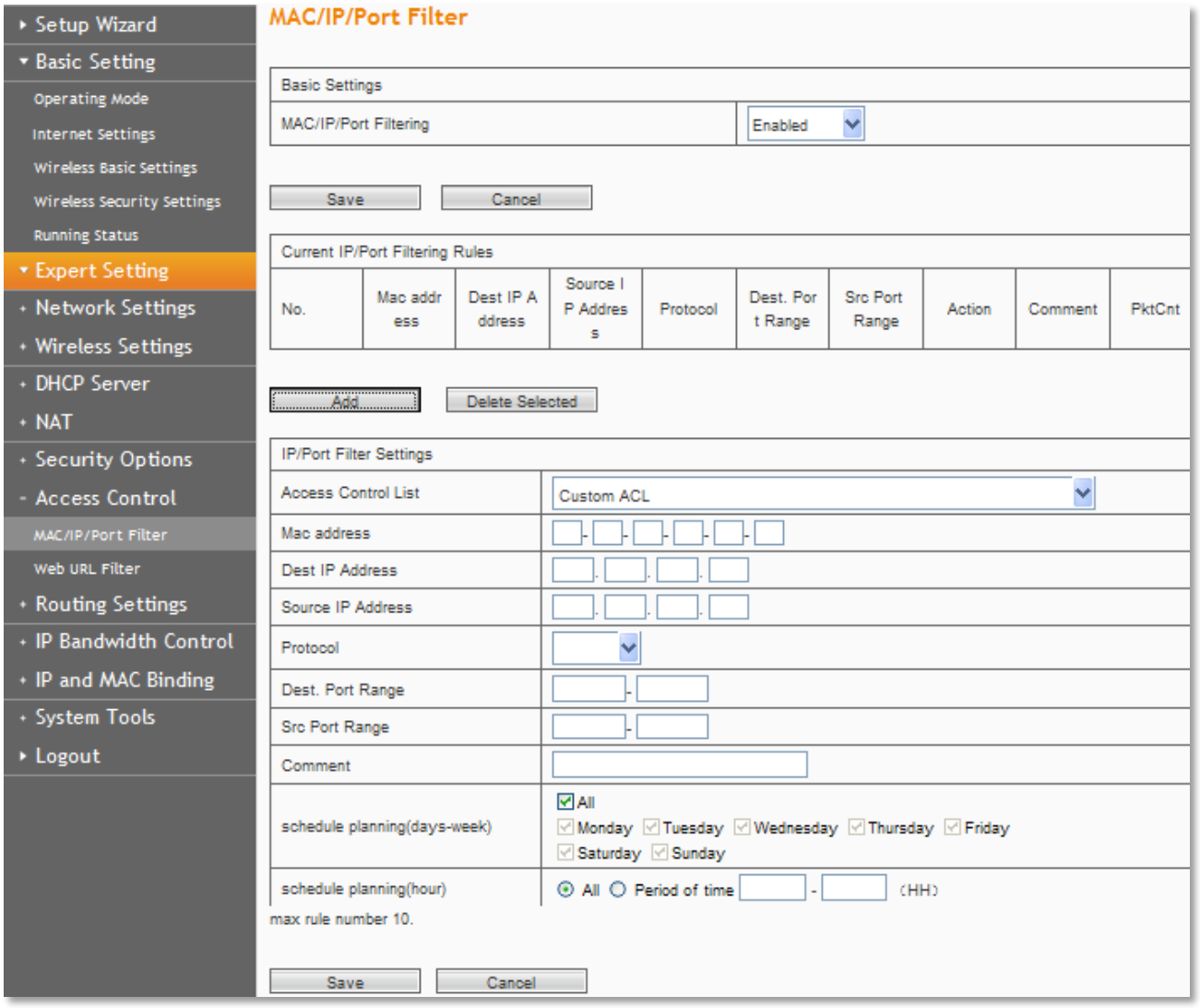
Web Management Port: The management port open to outside access the default value is 80.

Allowed Remote IP Address: Specify the range of the IP address for remote management.

Access Control



MAC/IP/Port Filter



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 Filter: Select **Enabled** or **Disabled** to enable or disable filter.

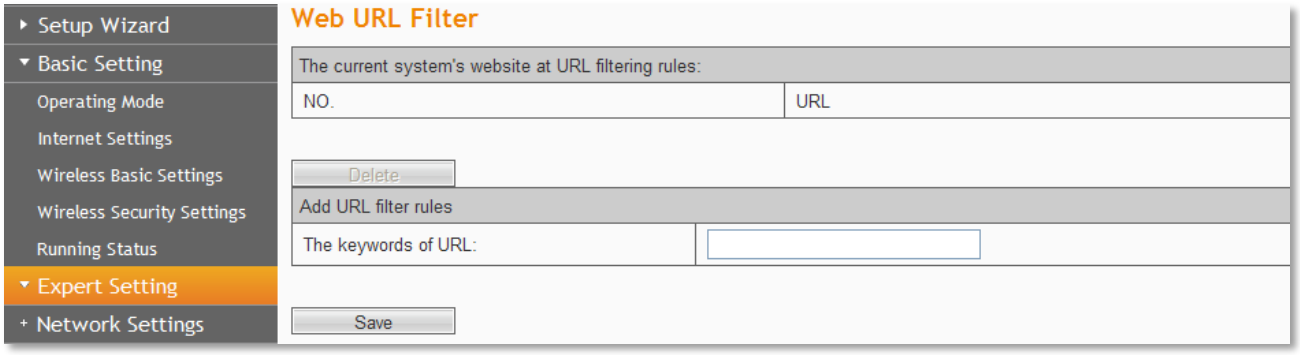
Default Policy： **Accepted** chose, all the packets and devices will be allowed to be passed normally, opposite action will be happened if **Dropped** was been chosen.

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**.

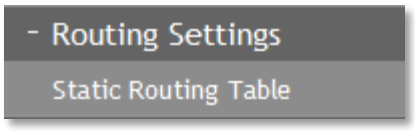
Note: Please synchronize the routers time first when selecting the timing function.

Web URL Filter

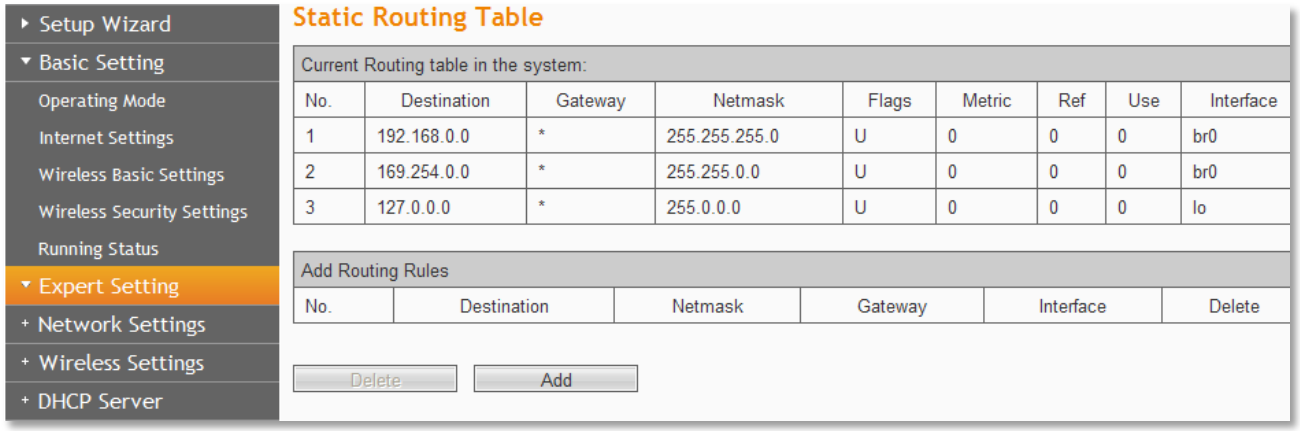


URL: Put in the URL you want to filter.

Routing Settings



Static Routing Table



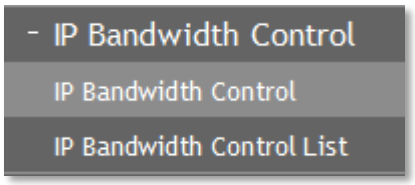
Static routes give the router information that it cannot learn automatically through other means Use the Static Routing page to add or delete a route. The max number is 10.

Destination: This is the IP address of the network or host that you want to assign to a static route.

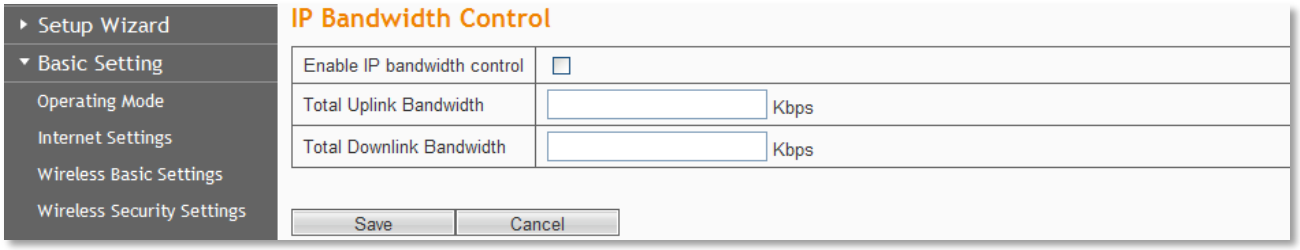
Subnet Mask: The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.

Gateway: This is the IP address of the default gateway device that allows for the contact between the Router and the network or host.

IP Bandwidth Control



IP Bandwidth Control



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.

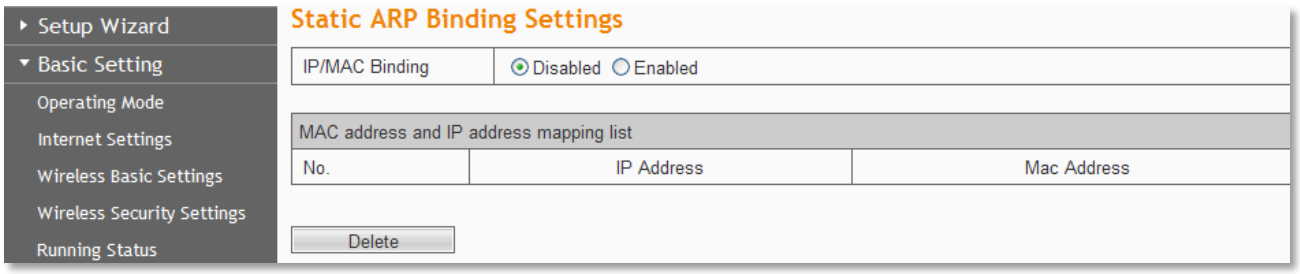
Note:

- 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 Internet Service Provider.

IP Bandwidth Control List

In this page, you can set rules of IP bandwidth control, the maximum rule is 16.

IP and MAC Binding

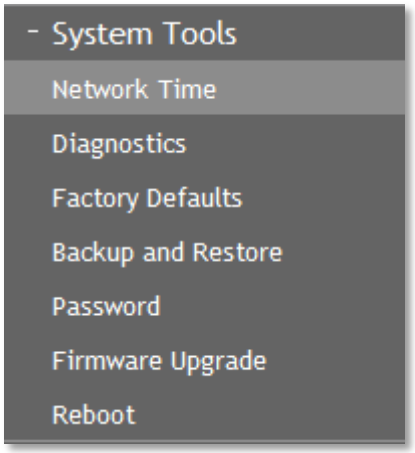


You may use the ARP binding function to control the Static ARP cache table, for preventing the ARP deception effectively.

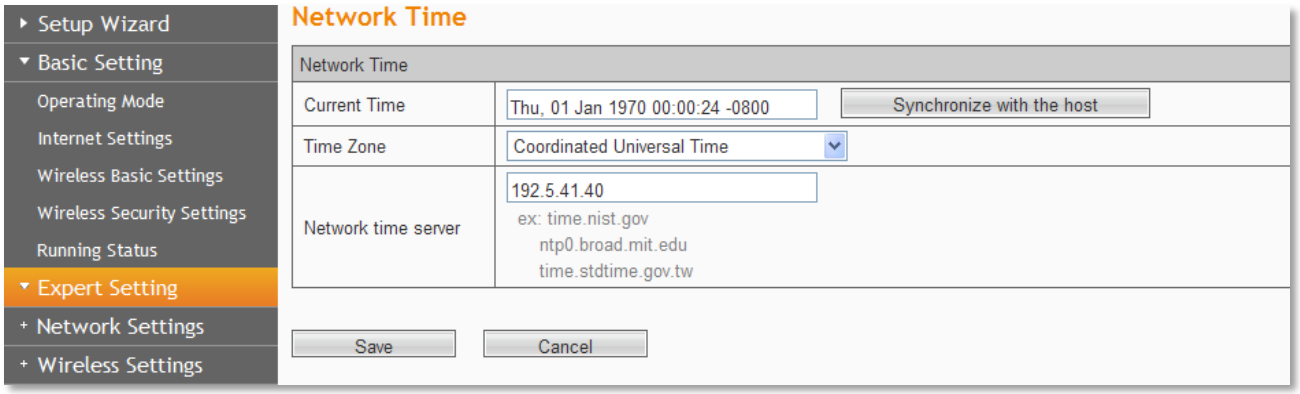
MAC Address: The MAC address of the LAN PC.

IP Address: The IP address of the LAN PC.

System Tools



Network Time



Current time: Show the current time.

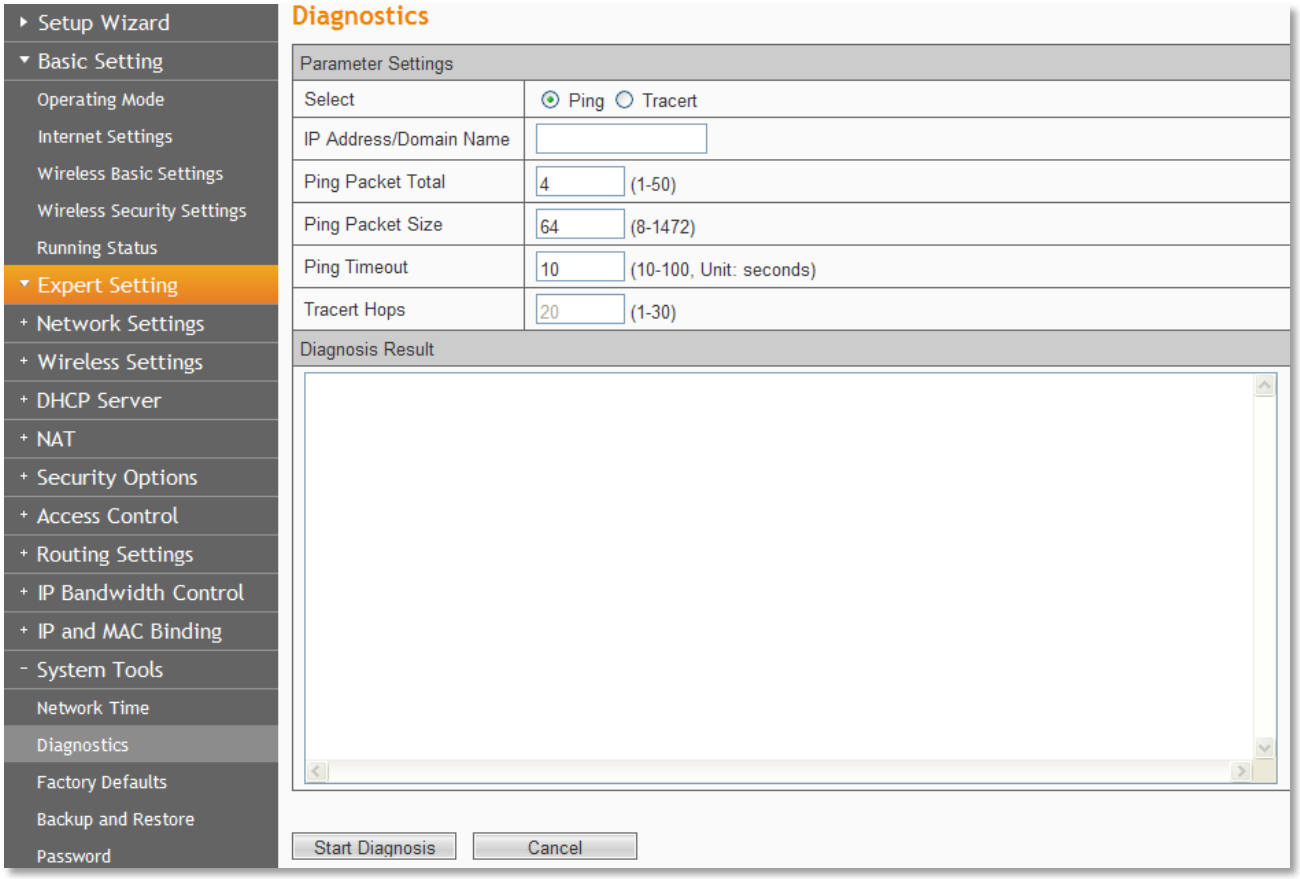
Time Zone: Select your time zone from the drop-down menu.

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.

Diagnostics



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.

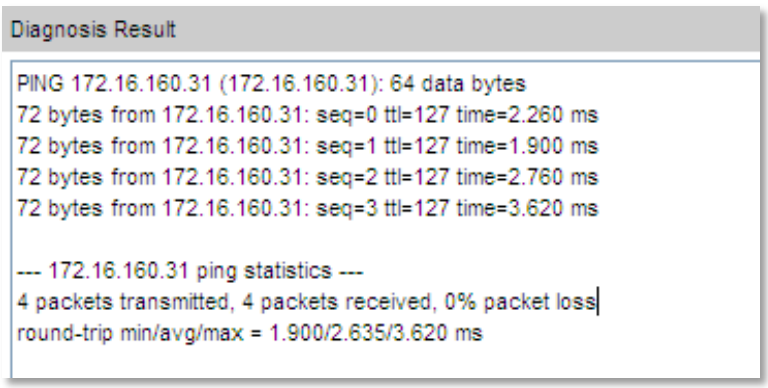
Ping Packet Size: The size of transmitted data packet when Ping operation is carried out.

Ping Timeout: The timeout time of the ping operation.

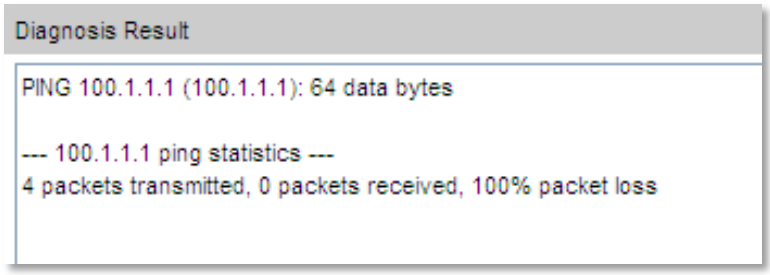
Tracert Hops: The hops of tracert.

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

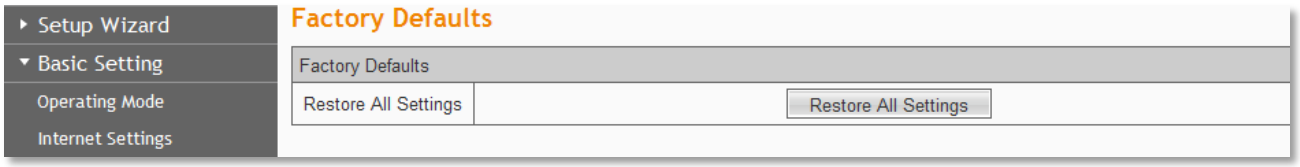
Below is a Ping diagnosis example that router has been connected to IP 172.16.160.31:



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



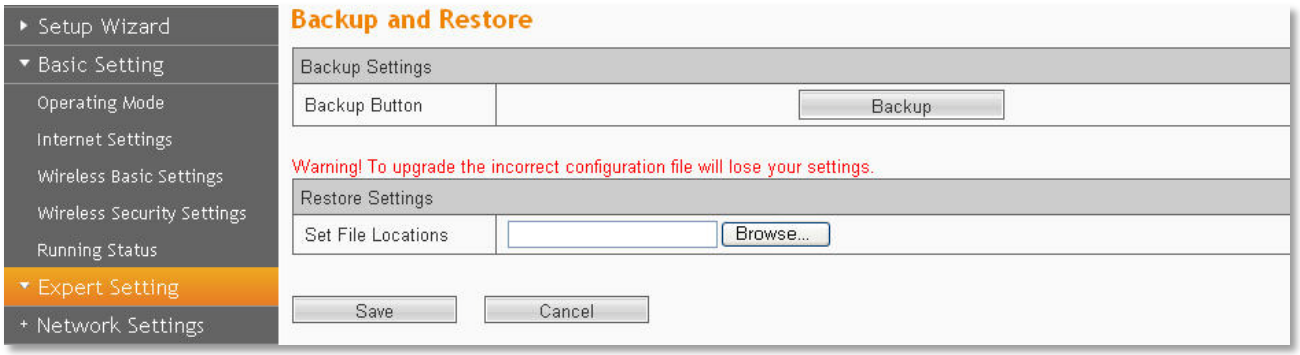
Factory Defaults



Click **Restore All Settings** button to reset all configuration settings to their default values.

Note: All changed settings will be lost when defaults are restored.

Backup and Restore



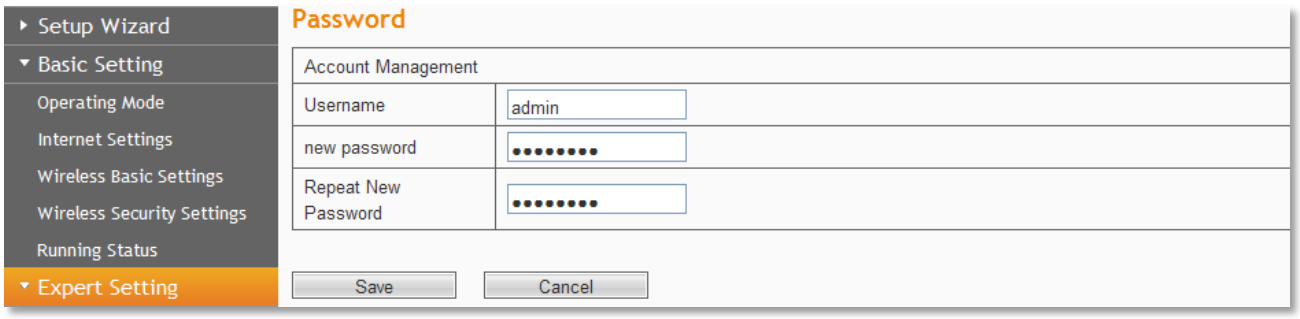
In the Backup Settings column, click **Backup** button to save all configuration settings to your local computer as a file.

To restore the Router's configuration, follow these instructions:

1) Click **Browse** button to find the configuration file which you want to restore.
2) Click **Save** button to update the configuration with the file whose path is the one you have input or selected in the blank.

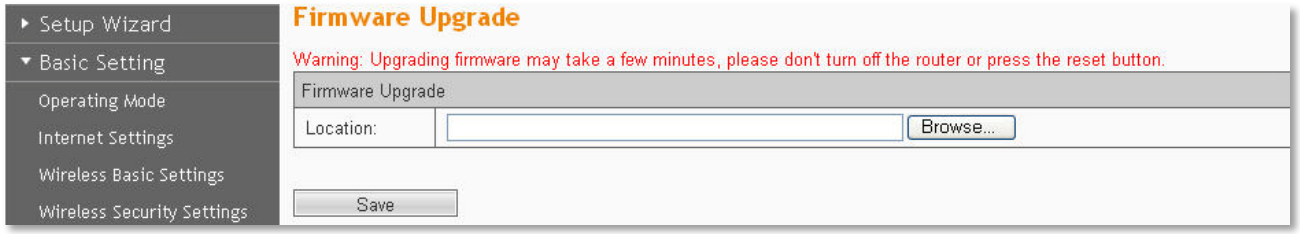
Note: Keep the power on during the process, in case of any damage.

Password



You can change the log in password for this web management page, not your ISP password or the wireless password.

Firmware Upgrade



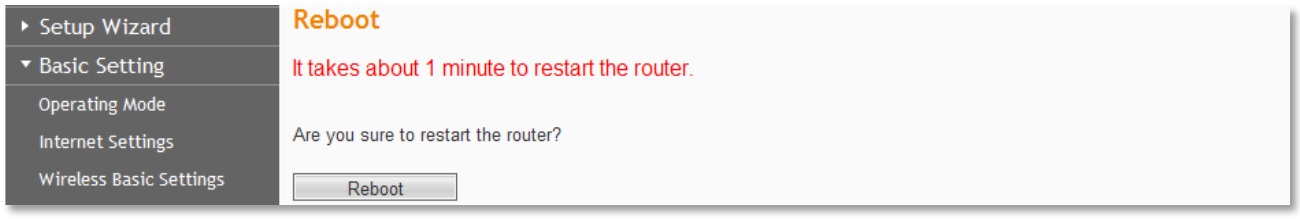
You can upgrade the router to the lasted version in this page, please download a most recent firmware upgrade file from our website. After downloading the file, you need to extract the zip file before upgrading the router. Browse for the upgrade file, then click **Upgrade** button.

Caution! Once you click **Upgrade** button, do not interrupt the process, loss of power during the upgrade could damage the Router.

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.

Reboot



Click **Reboot** button to reboot the Router.

Logout

Click to logout from the router's web management page.

Chapter 5: Specification

Wireless	
Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, CSMA/CA with ACK
Data Rate	11n: 150Mbps 11g: 54Mbps 11b: 11Mbps
Frequency Range	2.4-2.4835GHz
Wireless Transmit Power	<20dBm
Modulation Type	OFDM/CCK/16-QAM/64-QAM
Receive Sensitivity	150M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER
Operation Mode	Router, AP, Client, Bridge, Repeater
Wireless Security	64/128-bit WEP, WPA/WPA2-Enterprise, WPA/WPA2-Personal(TKIP/AES)
System Requirements	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ and Windows 7, Mac OS, Android
Hardware	
Interfaces	1 x 10/100Mbps LAN/WAN Port 1 x USB 2.0 Port
Button	Reset Button
Power Supply	100-200VAC 50/60Hz
Dimensions(W x D x H)	65mm x 92mm x 25mm
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
Certifications	CE, FCC,RoHS
Package Contents	1 x Wireless Nano Router 1 x Resource CD 1 x Ethernet Cable

* All references to speed and range are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

Appendix A: Troubleshooting

1. **How do I restore the Wireless Nano Router to factory default settings?**

   When the Wireless Nano Router is powerd on, press and hold the reset button on the rear panel for 8~10 seconds, after the light goes off, release the reset button.

2. **What can I do if I forget my password?**

- Restore the Wireless Nano Router to factory default settings. If you do not know how to do it, please refer to previous section 1.
- Use the default username and password: admin, admin.
- Reconfigure the Wireless Nano Router since you have ever reset it, it is in AP mode by default.

3. **The wireless stations cannot connect to the Wireless Nano Router.**

- Make sure the **SSID Broadcast** is enabled.
- Make sure that the wireless stations' SSID accord with the router's SSID.
- Make sure the wireless stations have the right password for encryption when the router is encrypted.
- If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

4. **I cannot login the Wireless Nano Router's web management page.**

- Check the computer's IP address, make sure the IP address is correct, for details please refer to the section of Configure the Computer's IP Address in this manual.
- Make sure you put 192.168.0.1 into the address bar, not the search bar.
- Check your web browser, make sure the Proxy server is unchecked. Take Internet Explorer as an example, go to **Tools**>**Internet Options**>**Connections**>**LAN Settings**, uncheck **Use a proxy server for your LAN**.
- If it tells you the username or password is error, and you cannot remember the new one, please reset router by pressing reset button for at least 6 seconds, and then try to login with default username and password (admin/admin).

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 equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This device and its antenna(s) must not be co-located or operation 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.

Access Point (AP): A wireless LAN transceiver or base station that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

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.

DoS (Denial of Service): A hacker attack designed to prevent your computer or network from operating or communicating.

DSL (Digital Subscriber Line): A technology that allows data to be sent or received over existing traditional phone lines.

ISP (Internet Service Provider): A company that provides access to the Internet.

MTU (Maximum Transmission Unit):The size in bytes of the largest packet that can be transmitted.

SSID: A Service Set Identification 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.

WPA (Wi-Fi Protected Access): WPA is a security technology for wireless networks that improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP. One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use. This is similar to 802.1x support and requires a RADIUS server in order to implement. The Wi-Fi Alliance will call this, WPA-Enterprise. One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short, this provides an authentication alternative to an expensive RADIUS server. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. The Wi-Fi Alliance will call this WPA-Personal.

PHICOMM

Shanghai Feixun Communication Co., Ltd.
E-mail: support@phicomm.com
Website: www.phicomm.com

Copyright © 2011 Shanghai Feixun Communication Co., Ltd. All rights reserved.