PHICOMM

User Manual

150Mbps Wireless N Access Point

FWA-600ND

User Manual / V2.0

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

LED and Button Descriptions 1

Main Features 3

Chapter 2: Operation Mode Introduction 4

Chapter 3: Hardware Installation 6

Physical Connection 6

Configure Your Computer 6

Login 14

Chapter 4: Software Configuration 16

Running Status 16

Running Status 17

Wireless Basic Settings 17

Wireless Security Settings 22

LAN 23

Wireless Settings 24

Wireless Basic Settings 24

Wireless Security Settings 24

Wireless MAC Address Filter 24

Advanced Wireless Settings 25
Wireless Clients List 26
WPS Settings 26
DHCP Server 27
DHCP 27
Address Reservation 28
DHCP Client List 28
System Tools 29
Factory Defaults 29
Backup and Restore 29
Password 30
System Log 30
Traffic Statistics 31
Firmware Upgrade 31
Reboot 32
Logout 32
Chapter5: PoE (Power over Ethernet) 33
Hardware Overview of PoE 33
Installation with PoE Injector 33
Chapter6: Specification 34
Appendix A: Troubleshooting 35

Appendix B: Certification 36

FCC Statement 36

CE Mark Warning 37

Appendix C: Glossary..... 38

Chapter 1: Introduction

Product Overview

Thank you for choosing FWA-600ND 150Mbps Wireless N Access Point. It is dedicated to Small Office/Home Office (SOHO) wireless network solutions. It allows for greater range and mobility within your wireless network while allowing you to connect the wireless devices to a wired environment. Increased mobility and the absence of cable will be beneficial for your network. With IEEE 802.11n wireless technology, your device can transmit wireless data at the rate of up to 150Mbps. With multiple protection measures including SSID broadcast control and advanced firewall protections, the product delivers complete data privacy. Wireless security type of WPA/WPA2-Enterprise as well as WPA/WPA2-Personal ensures transmission safety. Supporting a simple web-based setup wizard for installation and management, even novice users can easily configure it with the help of this manual.

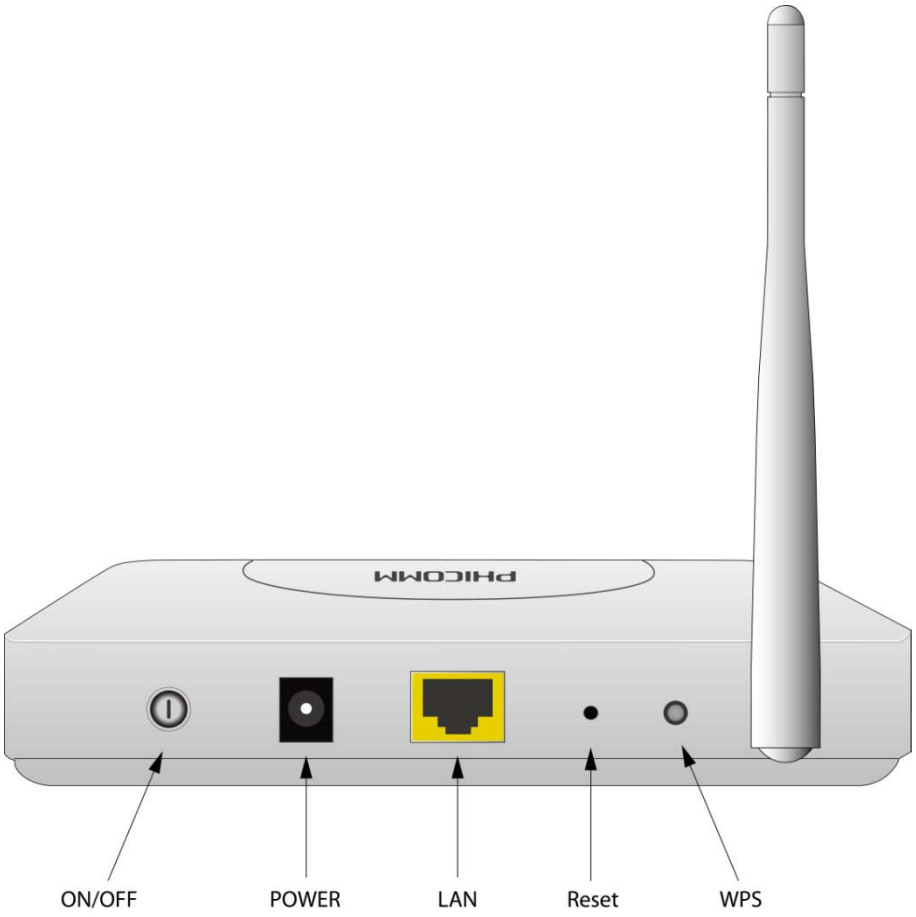
LED and Button Descriptions

Front Panel

The front panel of the wireless Access Point includes 4 LED indicators, as explained in table below:

LED	Status	Indication
POWER	On	Power is on
	Off	Power is off
LAN	On	There is a successful connection on the LAN port
	Off	There is no connection on the LAN port
	Blinking	Data is being transferred over the LAN port
WLAN	On	The wireless function is enabled
	Off	The wireless function is disabled
	Blinking	Sending or receiving data over wireless network
WPS	On	A wireless device is successfully connected to the network by WPS function
	Off	WPS function is deactivated
	Blinking	A wireless device is connecting to the network by WPS function

Rear Panel



The rear panel of the wireless Access Point includes 1 power ON/OFF switch, 1 power connector, 1 LAN port, 1 Reset button, 1 WPS button and 1 antenna, as explained in table below:

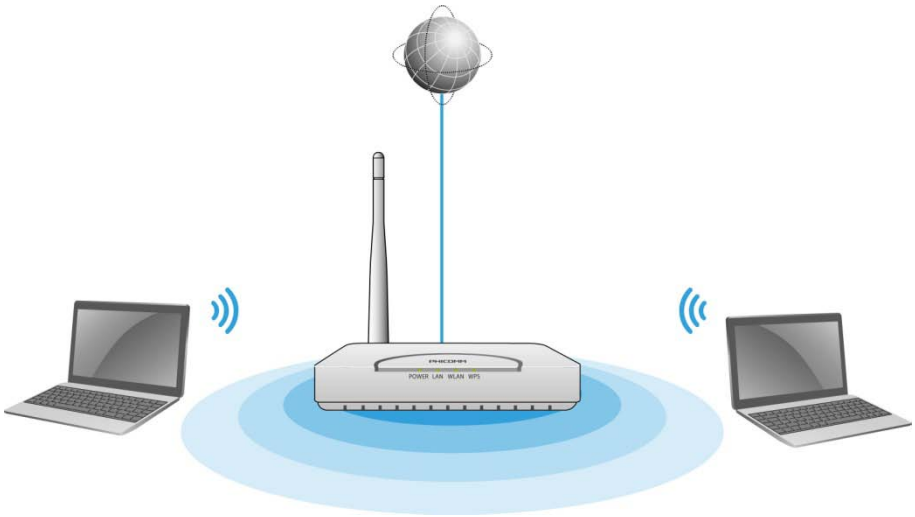
Interface/Button	Function
ON/OFF	Used to power on or power off the wireless Access Point
PWR	Connect with a power adapter
LAN	Connect to your network devices
Reset	Used to restore the product to factory default settings
WPS	Used to create a secured wireless network automatically by pressing the WPS button

Main Features

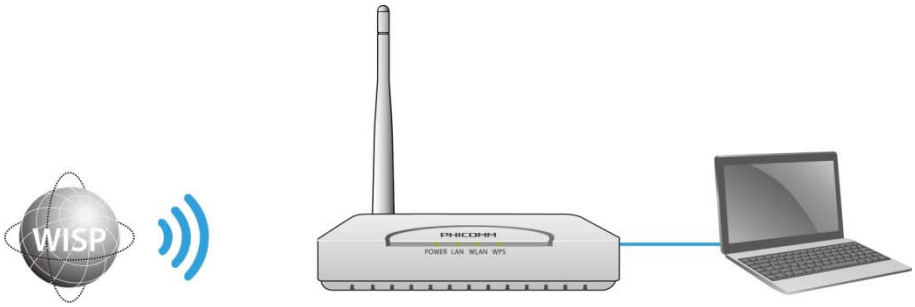
- Complies with IEEE 802.11n to provide a wireless data rate of up to 150Mbps
- Supports 1 RJ45 LAN port which also allows Power over Ethernet (PoE)
- Provides multiple encryption security Types including: 64/128-bit WEP, WPA/WPA2-personal
- Easily setup a WPA2 encrypted secure connection at a push of the WPS button
- Wireless MAC address filtering allows you to control the access rights of the wireless clients according to the MAC addresses
- Supports built-in DHCP server
- Supports operation modes including: AP, Client, Bridge, Bridge with AP, and Repeater
- Supports Multiple SSID
- Firmware upgrade allows you to update the firmware to the latest version through the configuration page
- External detachable antenna allows better alignment and stronger antenna upgrade

Chapter 2: Operation Mode Introduction

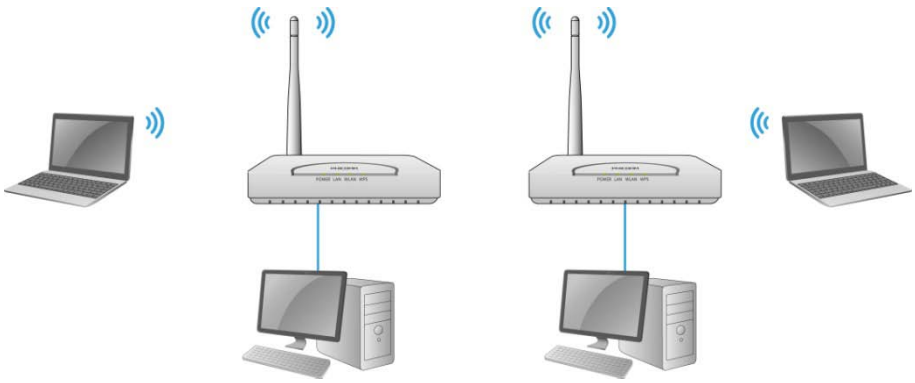
The Wireless Access Point supports five operation modes: **AP (Access Point)**, **Client**, **Bridge**, **Bridge with AP** and **Repeater**. By default, the operation mode is AP.
In AP mode, it extends your existing hardwired network to your wireless clients.



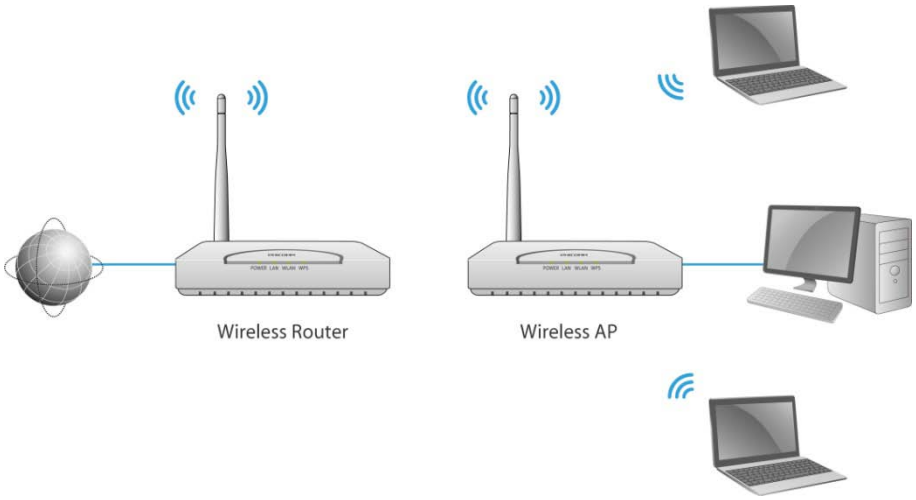
In Client mode, it acts as a wireless network adapter.



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



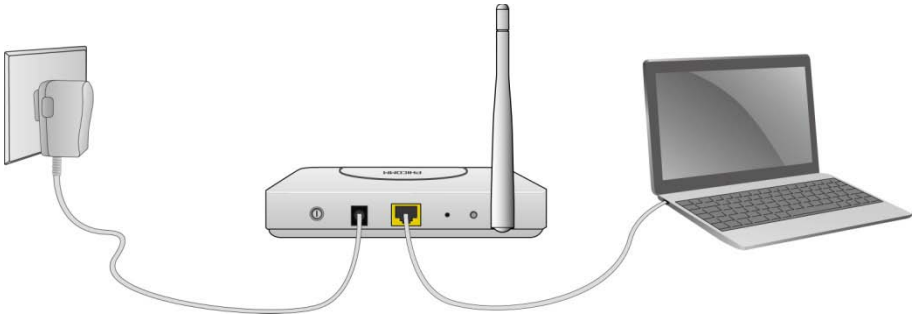
In Repeater mode, it can extend the coverage of your root wireless router, boost the wireless signal strength.



Chapter 3: Hardware Installation

Physical Connection

Before installing the device, please make sure that the broadband service provided by your ISP is available. Connect your computer to the Wireless Access Point with an Ethernet cable when trying to configure it.

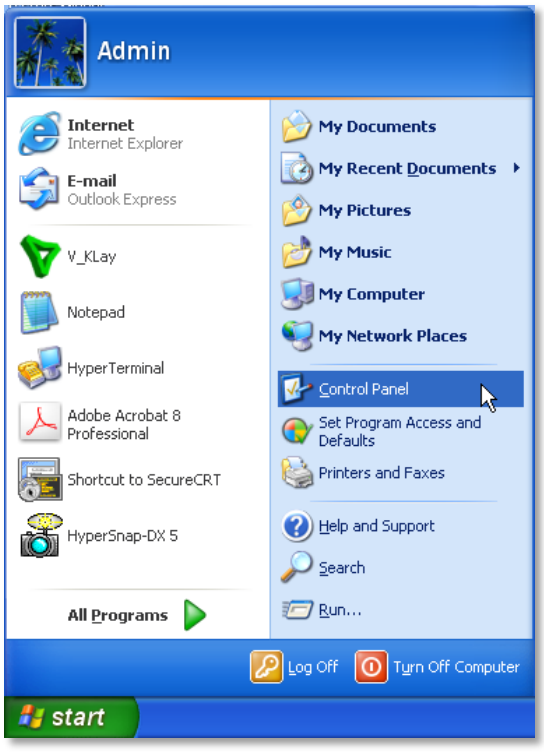


Configure Your Computer

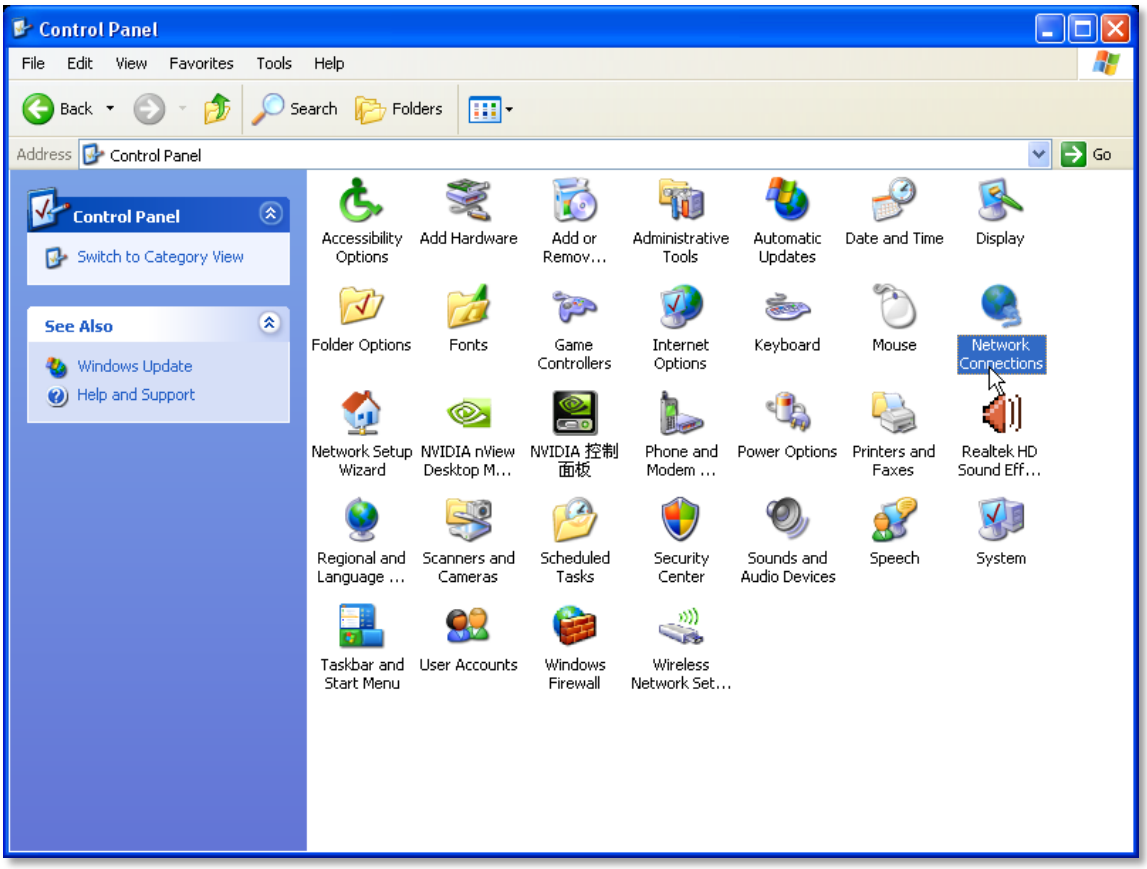
By default, the DHCP server of FWA-600ND is enabled. It can assign an IP address to your computer automatically. So we suggest you set your computer to obtain IP address automatically after the physical connection.

For Windows XP/2000

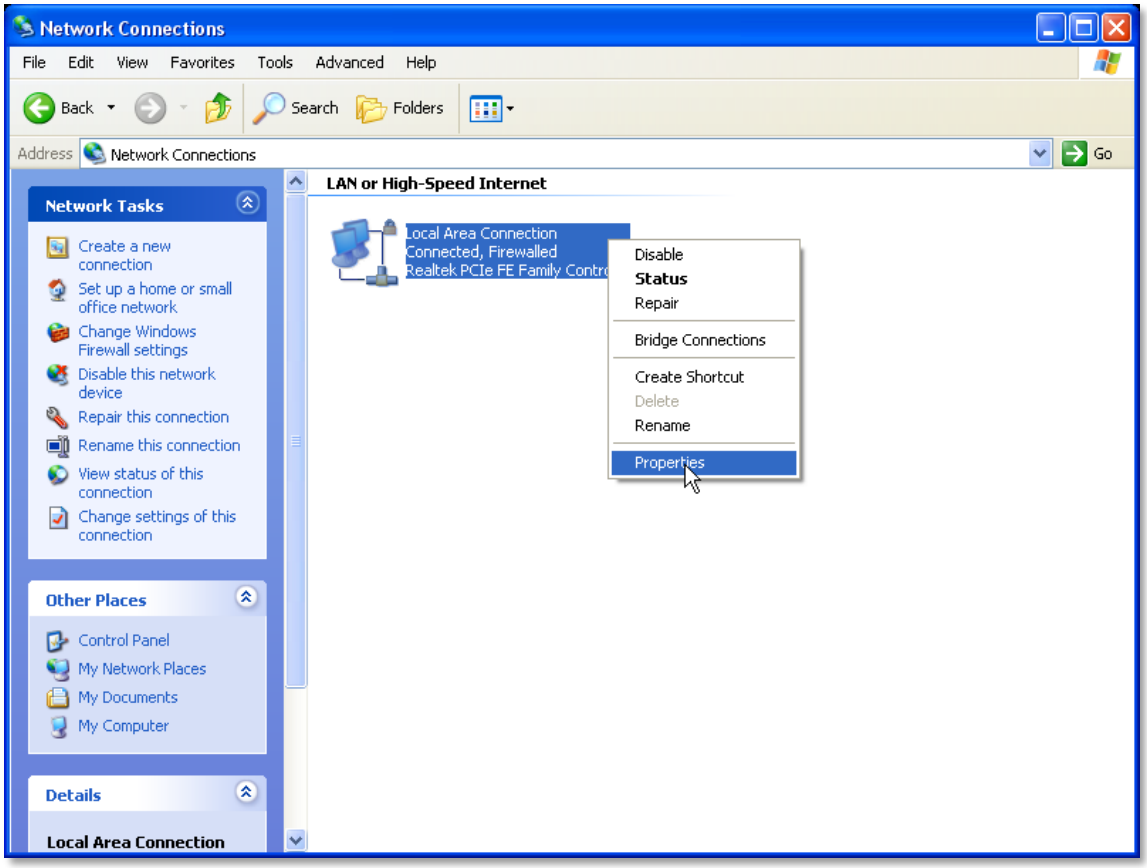
1) Click **Start** > **Control Panel**.



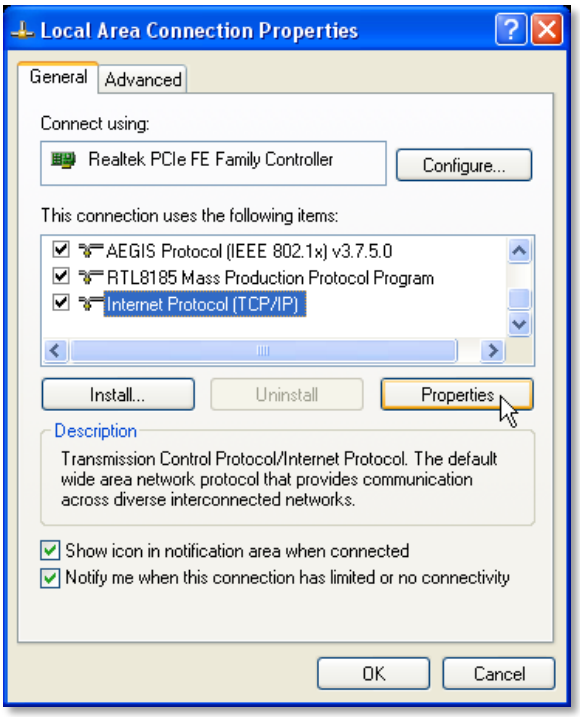
2) Select and double click **Network Connections**.



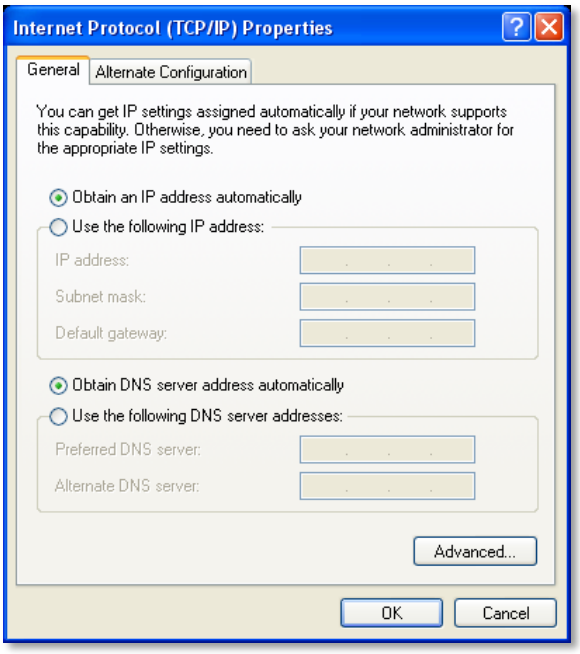
3) Right click **Local Area Connection** and then select **Properties**.



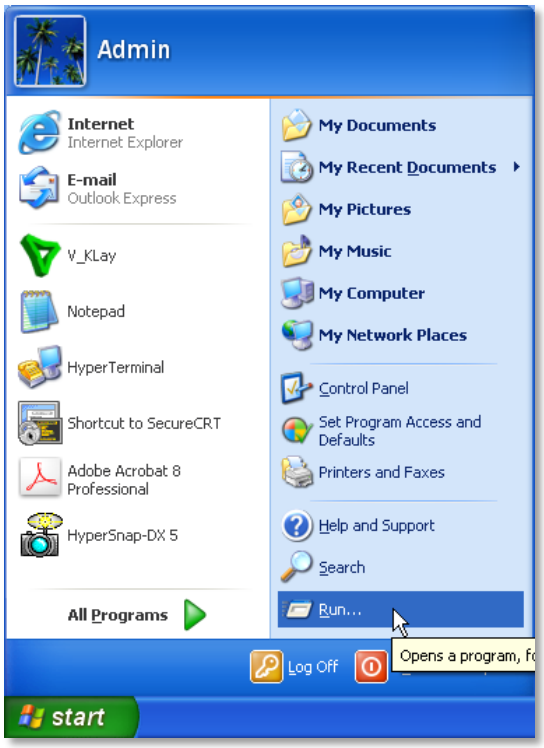
4) Select **Internet Protocol (TCP/IP)** and click **Properties.**

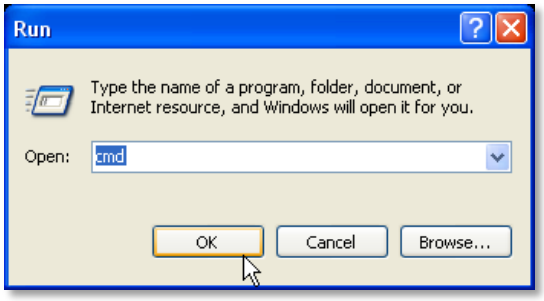


5) Select **Obtain an IP address automatically** and **Obtain DNS server address automatically.** Then click **OK.**



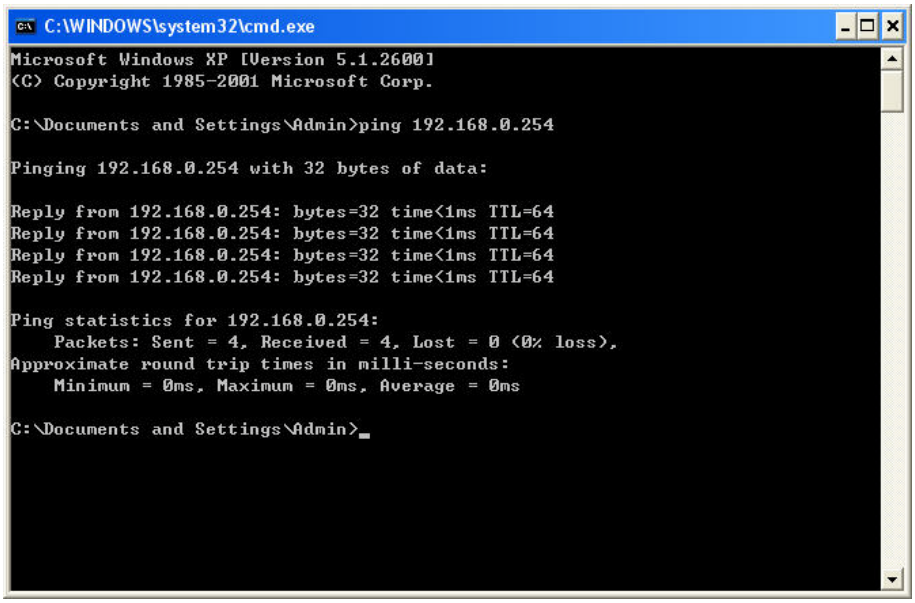
6) Run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **Run** tab, type **cmd** in the field.





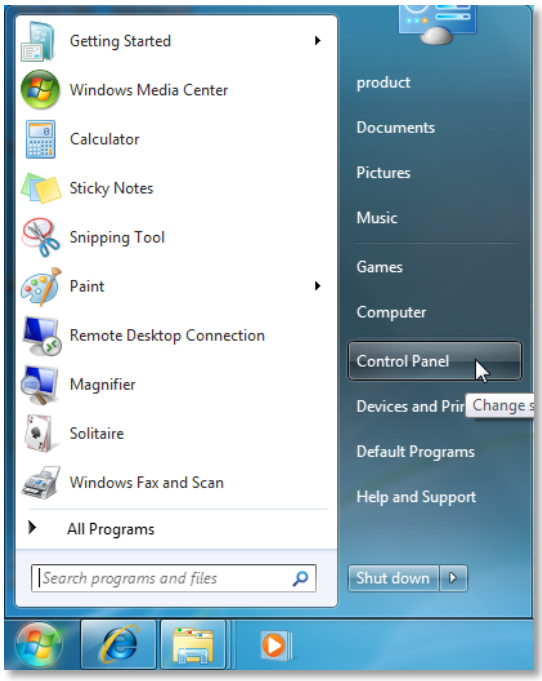
7) Then type **ping 192.168.0.254** on the next screen, press Enter.

If you can receive reply from that IP address that means you has succeeded.

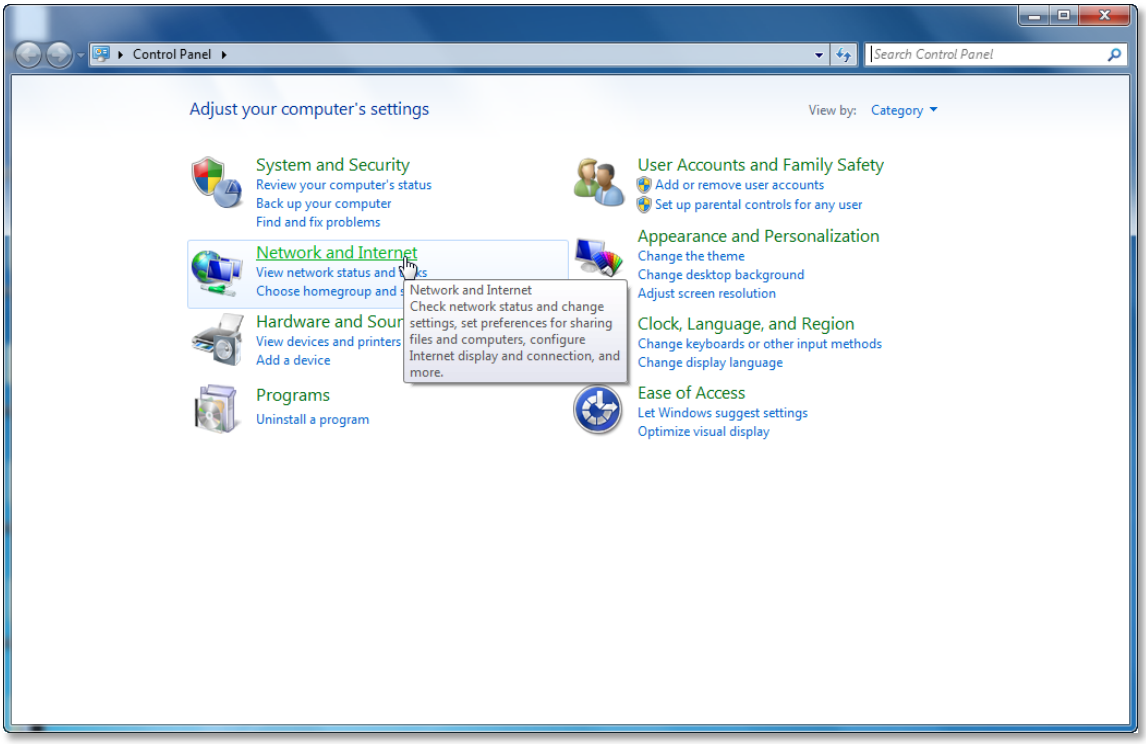


For Windows Vista/7

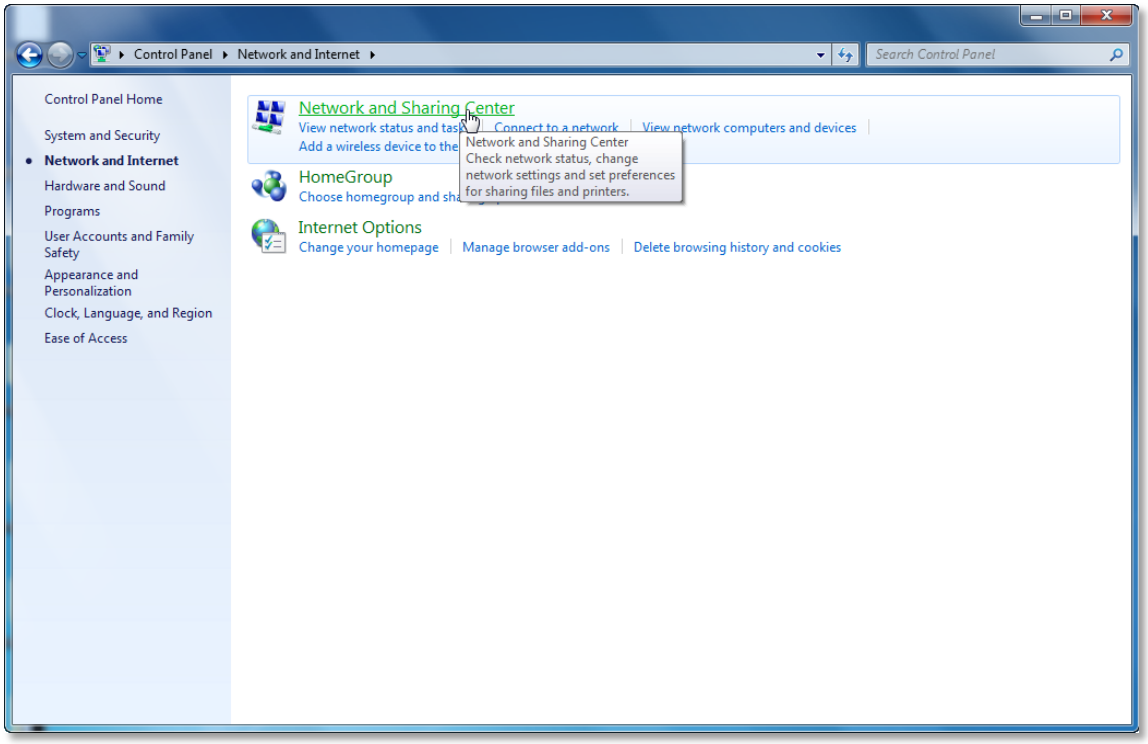
1) Click **Start**>**Control Panel**.



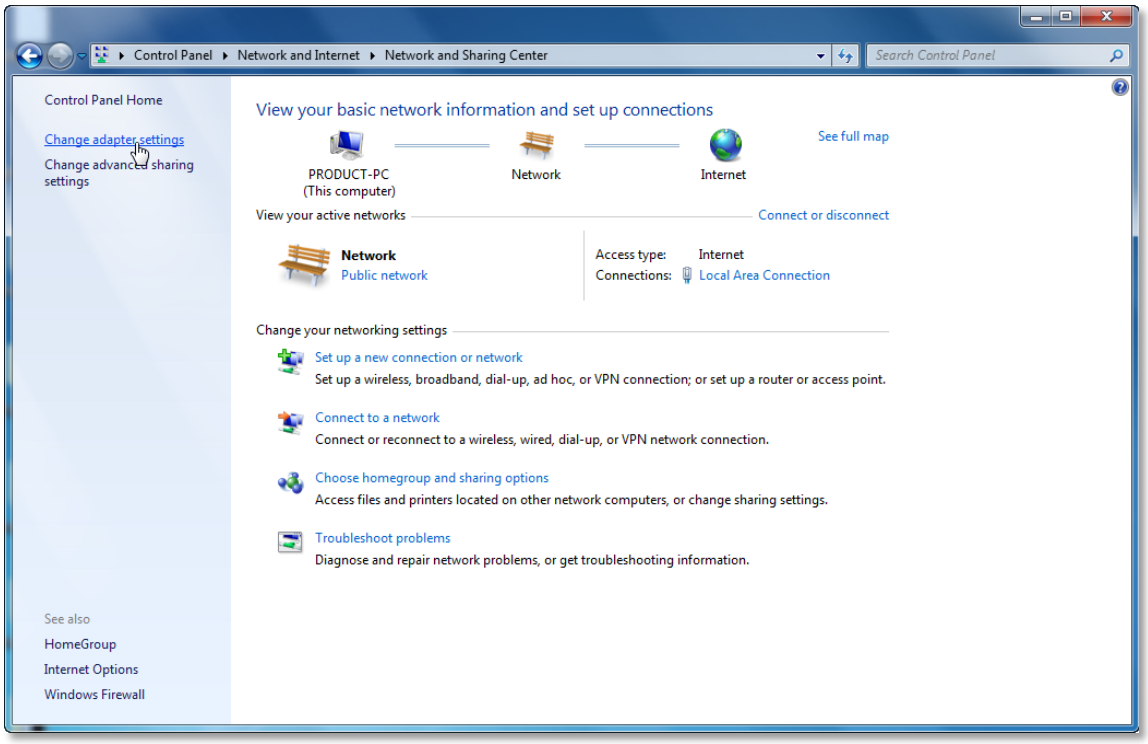
2) Click **Network and Internet**.



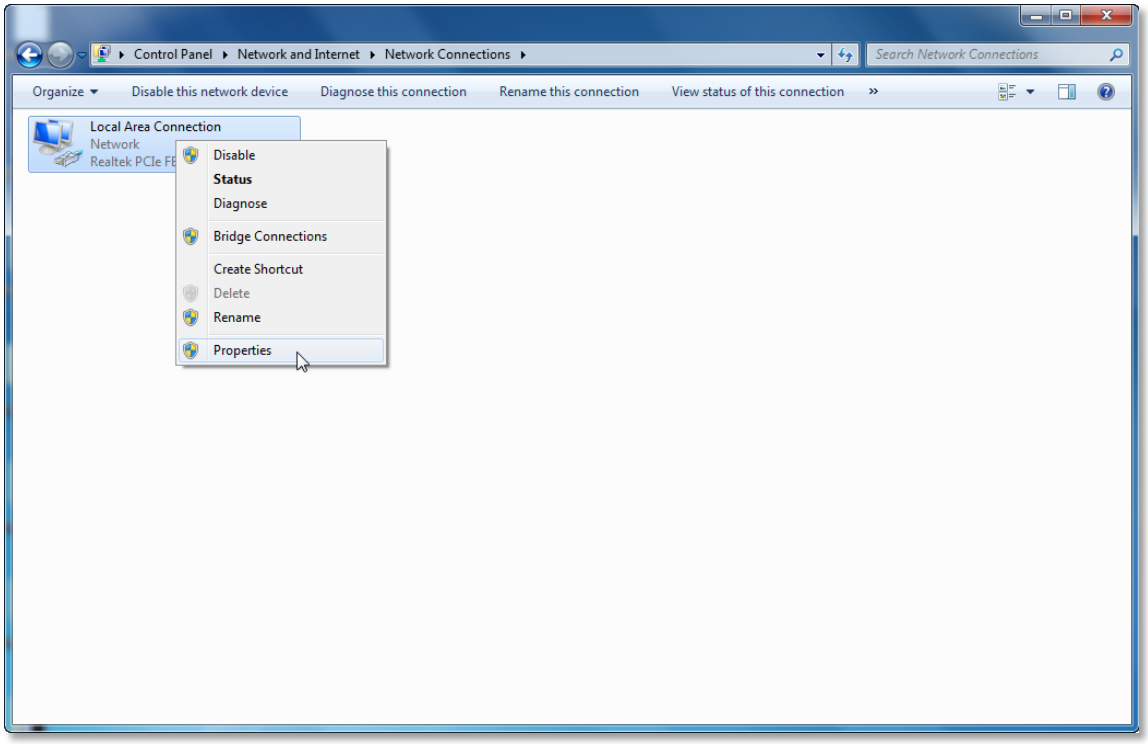
3) Click **Network and Sharing Center**.



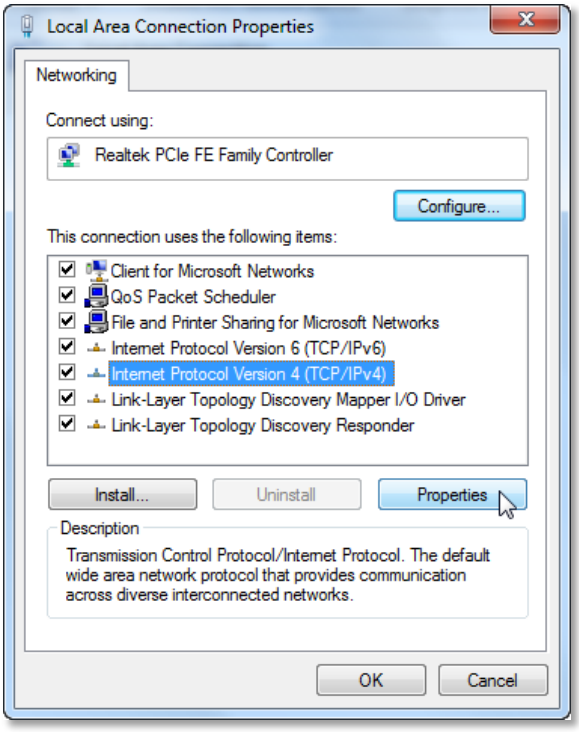
4) Go to **Change Adapter Settings** (win7)/**Manage Network Connections** (Vista).



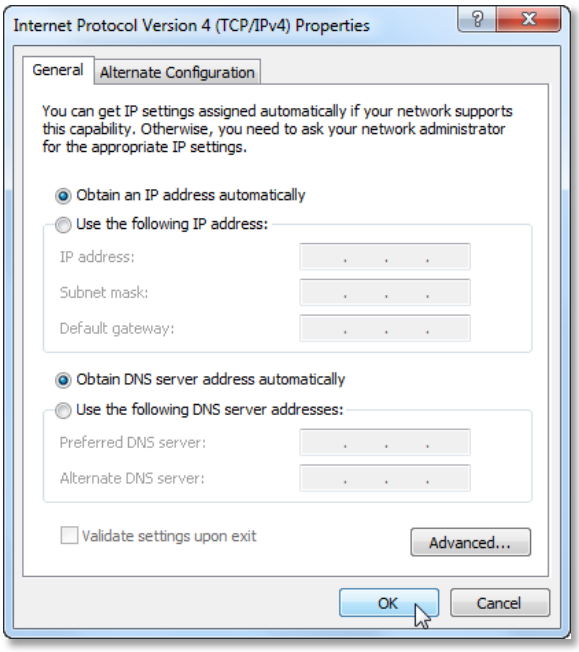
5) Right click **Local Area Connection**, choose **Properties**.



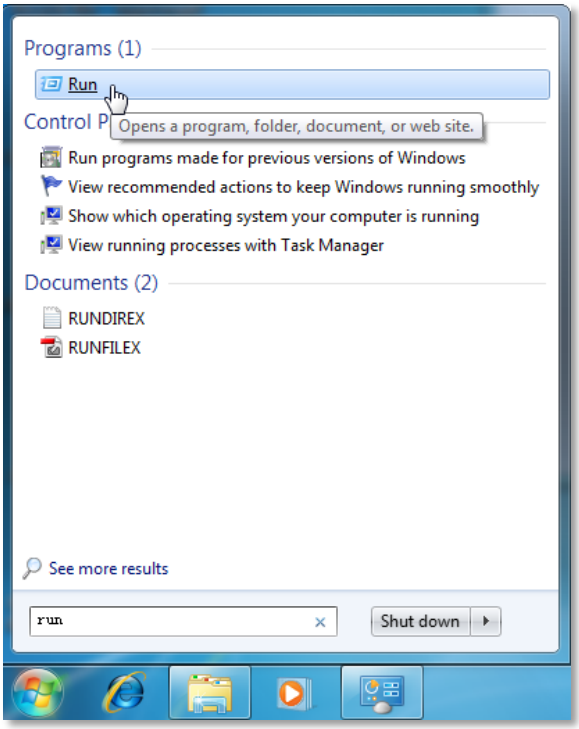
6) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

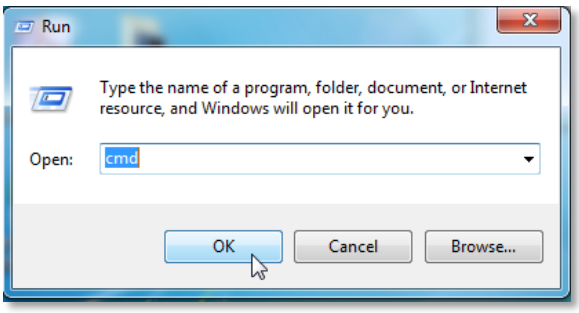


7) Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Then click **OK**.

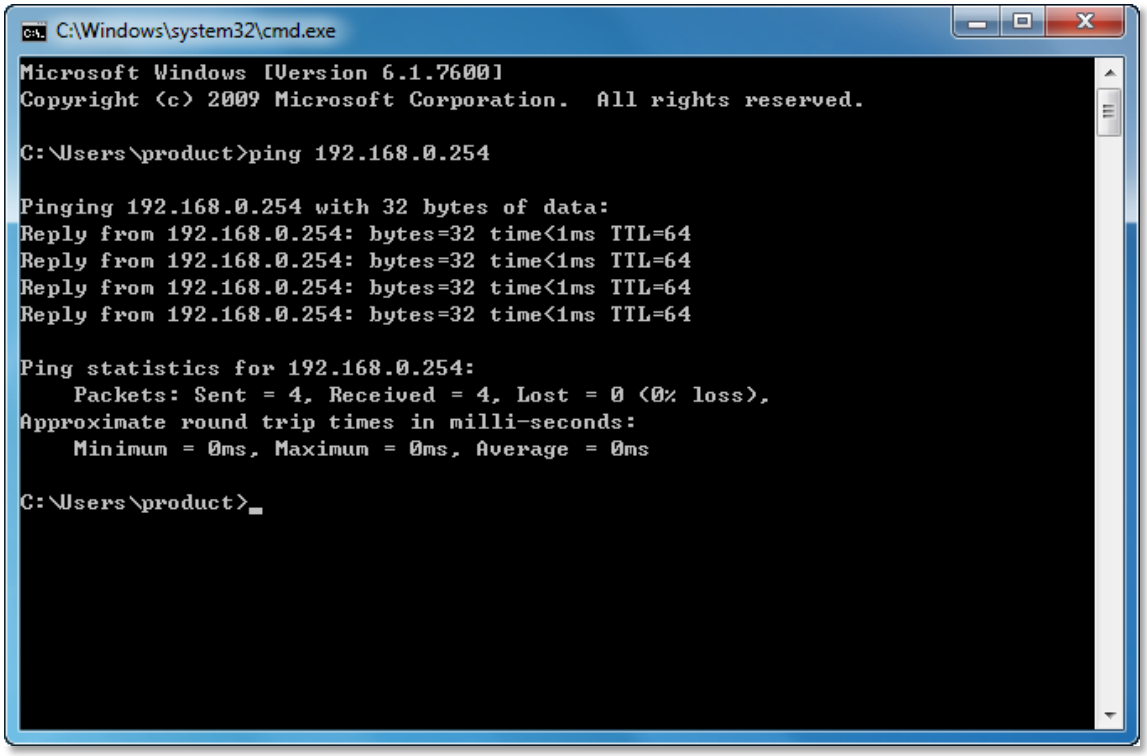


8) Run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **Run** tab, type **cmd** in the field,





9) Then type **ping 192.168.0.254** on the next screen, press **Enter**. If you can receive reply from that IP address, that means you have succeeded.



Login

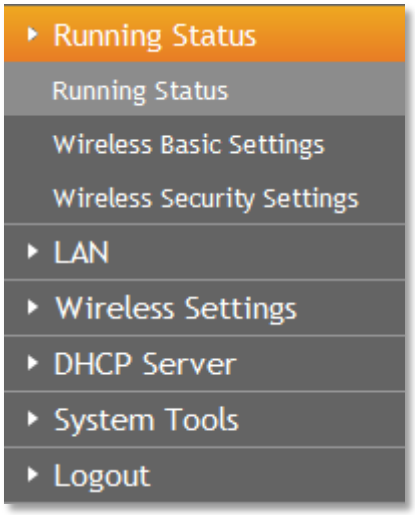
Now we can login to the Web-based Setup Wizard to do advanced configuration.

Step 1: Open your web browser, type the default IP address **192.168.0.254** in the address bar, press enter.

Step 2: Enter the default Username **admin** and Password **admin**.

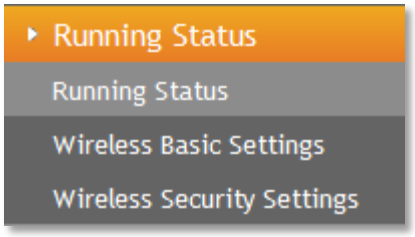
Chapter 4: Software Configuration

After the successful login, you can configure and manage the device. There are six main menus on the left side of the web management page: **Running Status**, **LAN**, **Wireless Settings**, **DHCP Server**, **System Tools** and **Logout**. Submenus will be available after clicking one of these main menus. On the right of the web management page you can see the detailed explanations and instructions for the corresponding page.

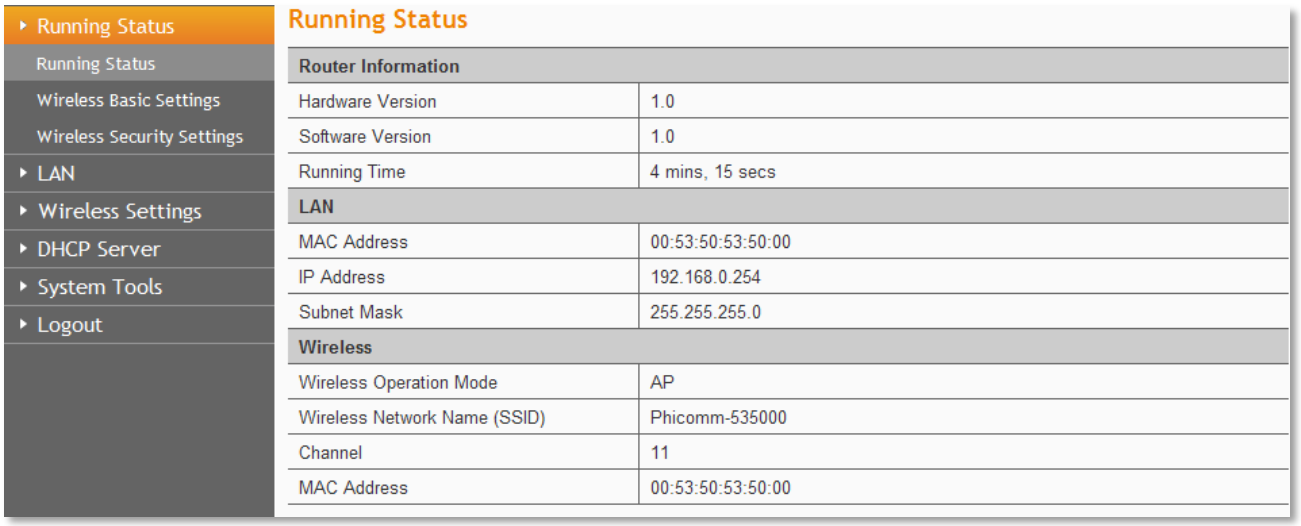


Running Status

Running Status includes three submenus: **Running Status**, **Wireless Basic Settings** and **Wireless Security Settings**. Click any of them, you will be able to configure the corresponding function.

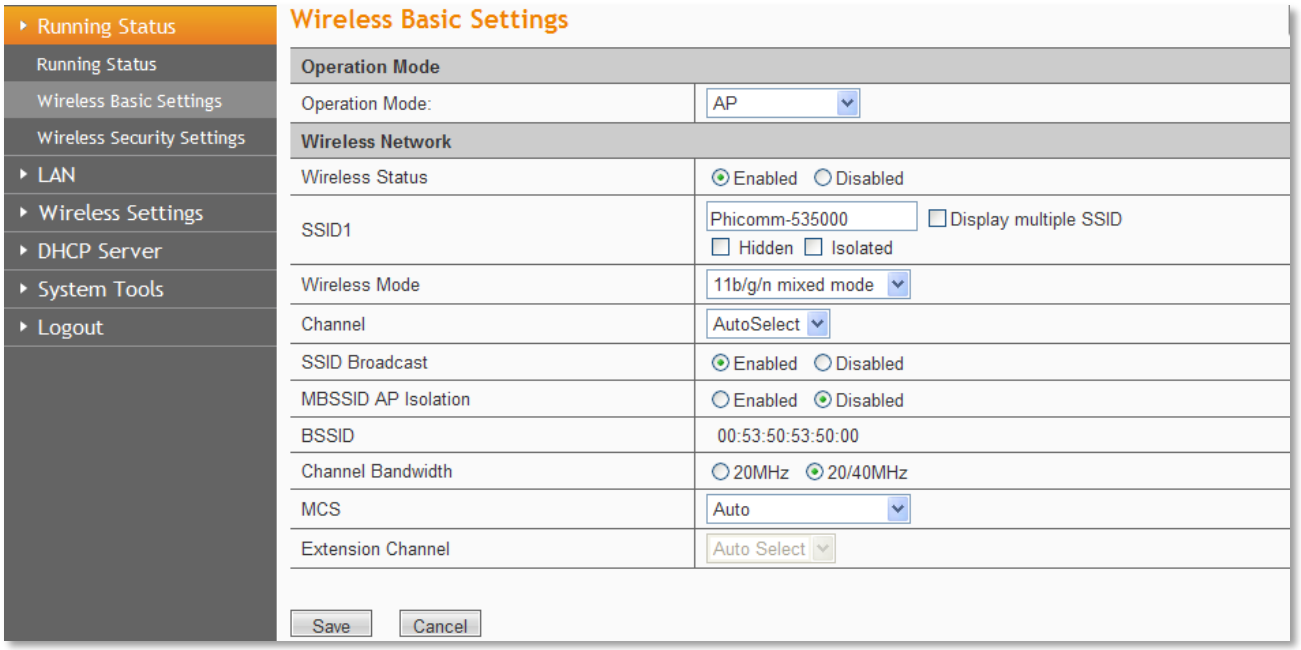


Running Status



Running Status page shows the current status of the wireless access point.

Wireless Basic Settings



a) AP Mode

By default, the operation mode is AP.

Operation Mode: It displays the current operation mode. Choose the operation mode in the drop-down list, the corresponding configuration page will pop up.

Note: Since the DHCP server of your original router is enabled and it assigns IP addresses to you computers automatically so you have to disable the DHCP service on the wireless Access Point after the settings.

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

wireless function.

SSID1: The wireless network name of AP, you can change it to whatever you want.

Display multiple SSID: It supports up to 4 SSIDs. If you enable other SSIDs and tick the Isolated radio button then computers that connected to different SSIDs become logically separated.

Hidden: Select it to disable SSID broadcast. We do not suggest you tick it.

Isolated: Get different SSIDs become logically separated.

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: 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.

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

MBSSID AP Isolation: Leave it as disable.

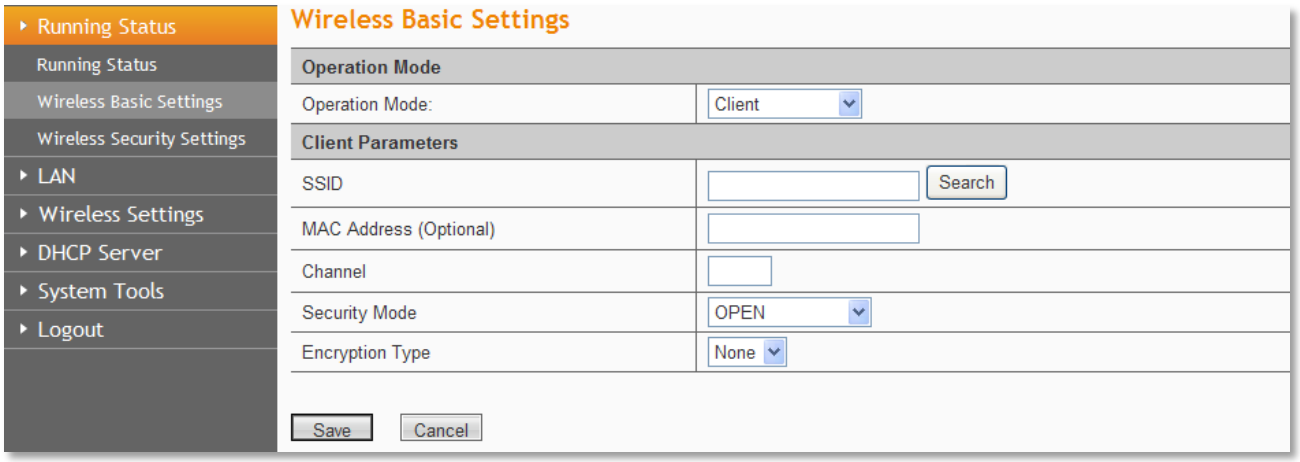
BSSID: The physical address of the AP.

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

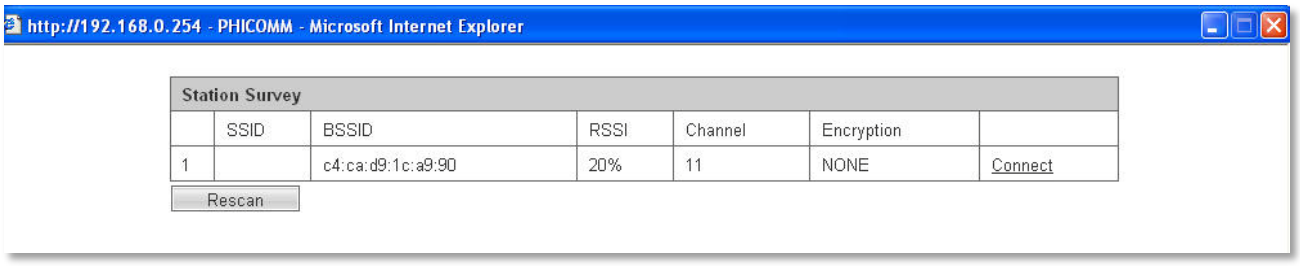
MCS: You can leave it as Auto.

Extension Channel: There is assistant channel if frequency bandwidth 20/40 is chosen.

b) Client Mode



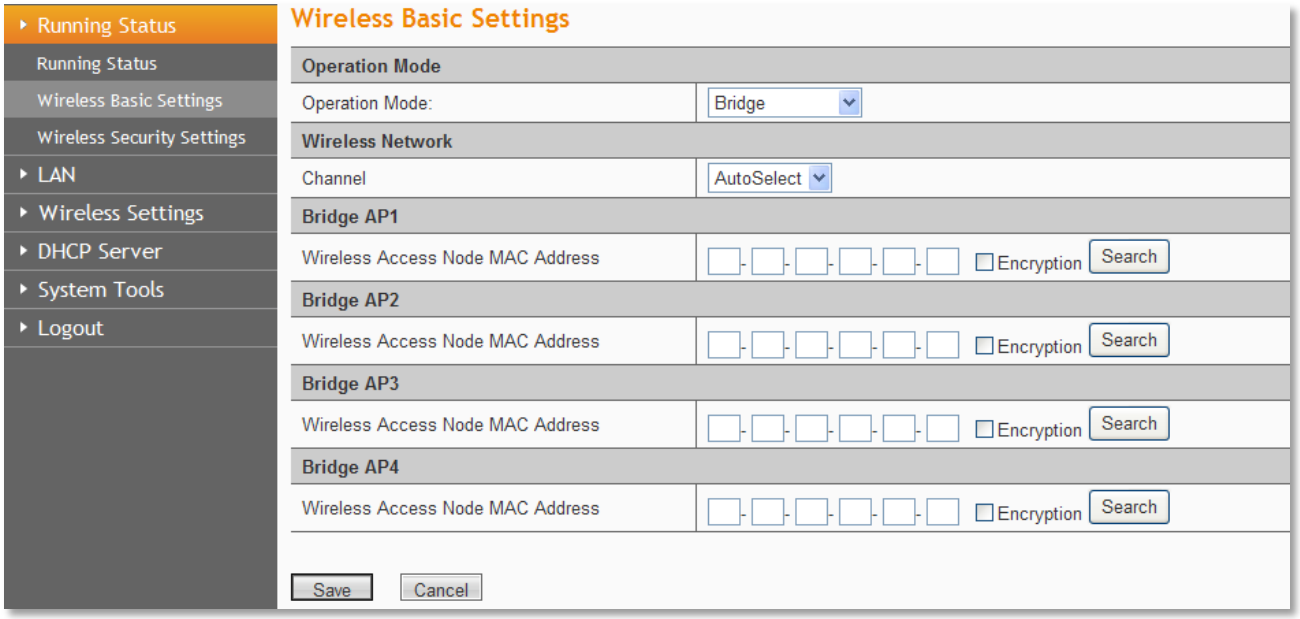
SSID/MAC Address: Please click **Search** then a **Station Survey** page will pop up. Choose your wireless network of your main AP/Router and click **Connect** button. After that you can see that the SSID and MAC Address of your main AP/Router appeared in the box automatically.



Security Mode: You can choose **open**, **shared**, **WPA-Personal**, **WPA2-Personal**. Please make sure it matches with the settings in your main AP/Router.

Encryption Type: You can choose WEP, TKIP, and AES. Please make sure it matches with the settings in your main AP/Router.

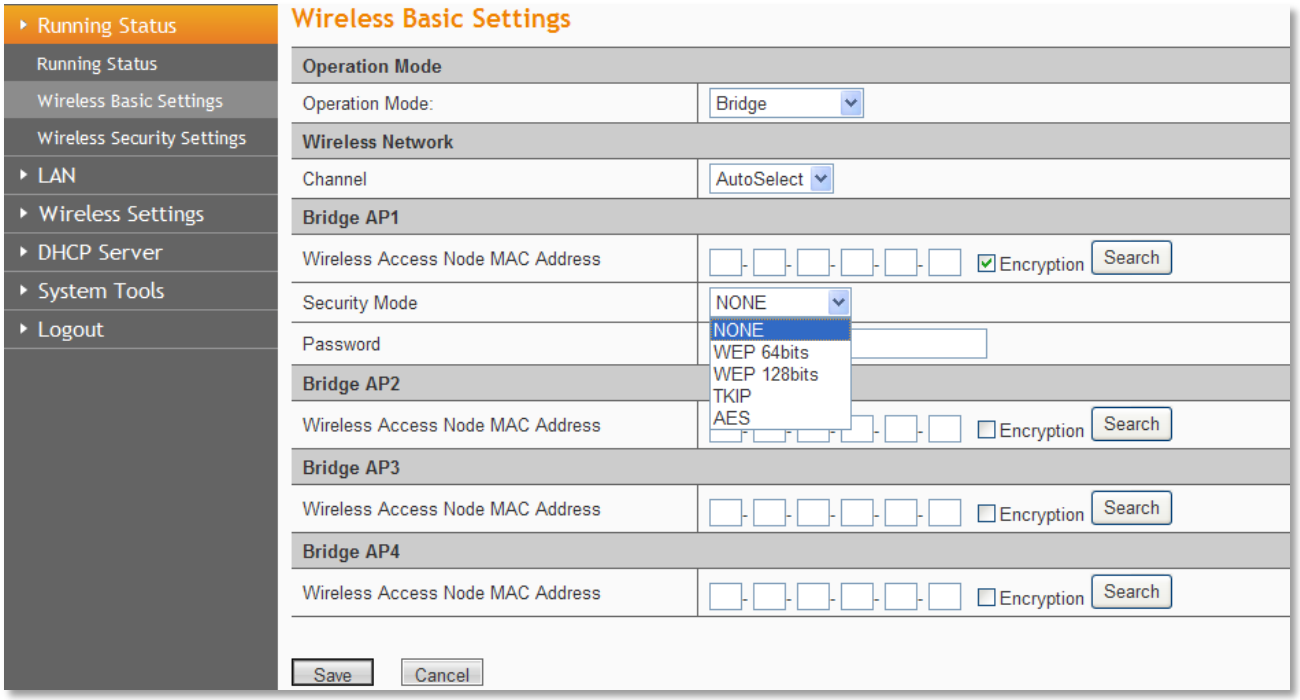
c) Bridge Mode



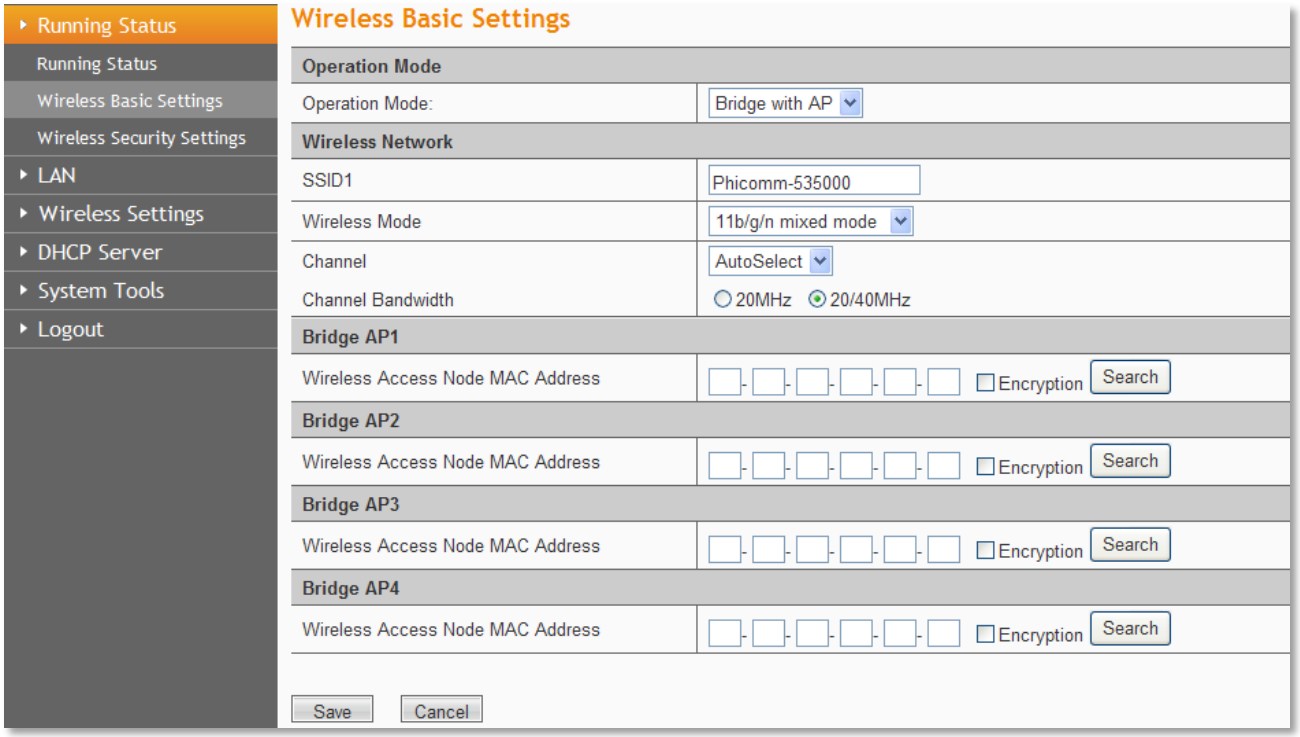
Wireless Access Node MAC Address: Click search then the Site Survey page pops up.

Choose the wireless network which you'd like to bridge, then click **Connect**. The Wireless Access Node Mac Address will be filled in automatically.

Encryption: Tick encryption, then a new page including encryption type and encryption key pops up. Choose the correct encryption type and enter the key according to the original wireless network.



d) Bridge with AP Mode



SSID1: Show the wireless network name, you can change it to whatever you want.

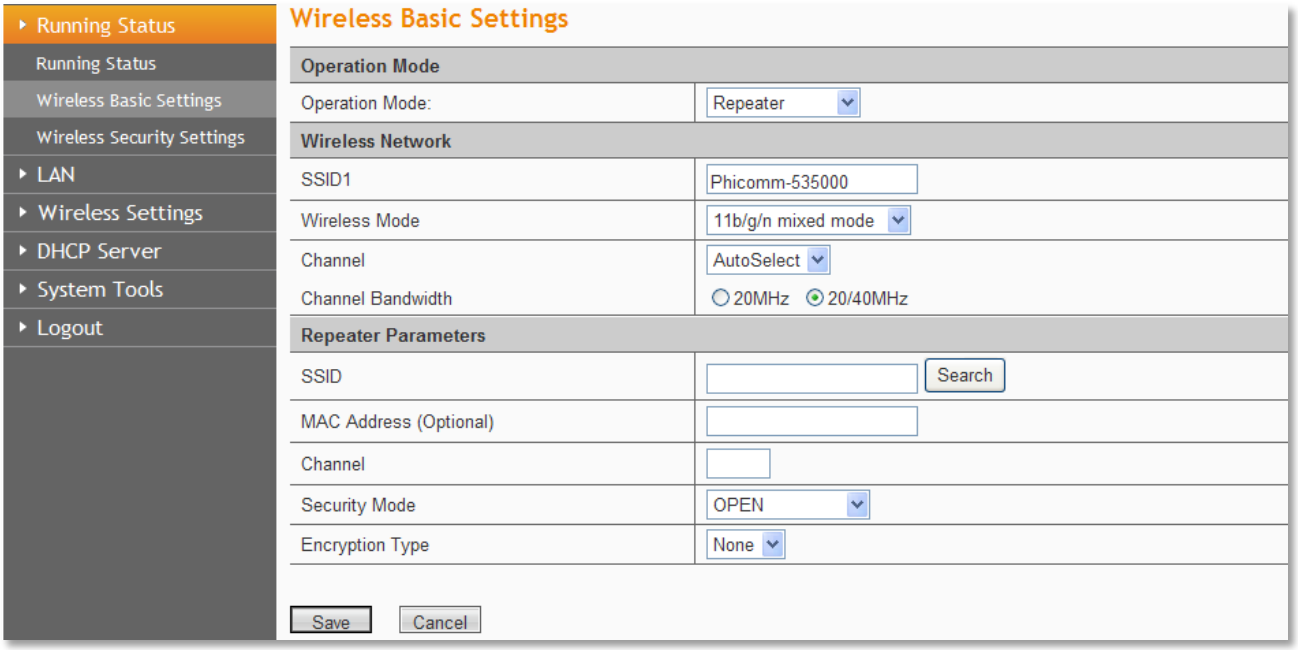
Wireless Mode: If all of the wireless devices connected with this wireless router are in the same transmission mode (e.g. 802.11b), you can choose "Only" mode (e.g. 11b only). If you have some devices which use a different transmission mode, choose the appropriate "Mixed" mode.

Channel: 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.

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

Wireless Access Node Mac Address: The following operations are the same as setting it as Bridge. Click **Search** then the **Site Survey** page pops up. Choose the wireless network which you'd like to bridge, then click **Connect**.

e) Repeater Mode



SSID1: If you configured it as a repeater successfully, the SSID1 would be the same with your main AP/Router.

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: If you configured it as a repeater successfully, the channel would be the same with your main AP/Router.

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

SSID: Click **Search**, the **Site Survey** page will pop up, please connect to the wireless network name of your main AP/Router.

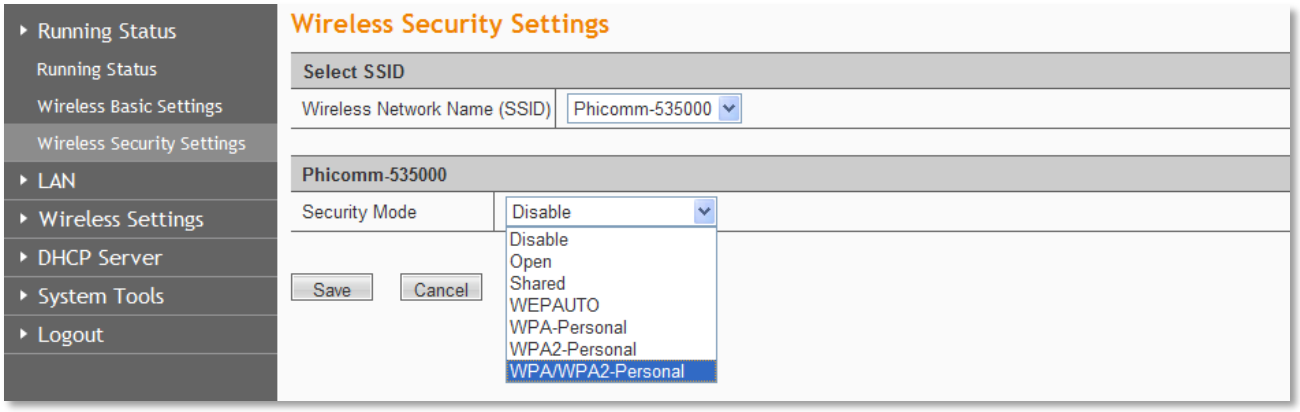
MAC Address: The Mac Address will be automatically put in after the above operations.

Channel: The channel will pop up automatically. It is the same as the wireless channel of your main AP/Router.

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.

Note: If you have no idea about the wireless network, security mode or encryption type please login to the configuration page of your main AP/Router to check the information.

Wireless Security Settings



Wireless Network Name (SSID): Show the current wireless network name.

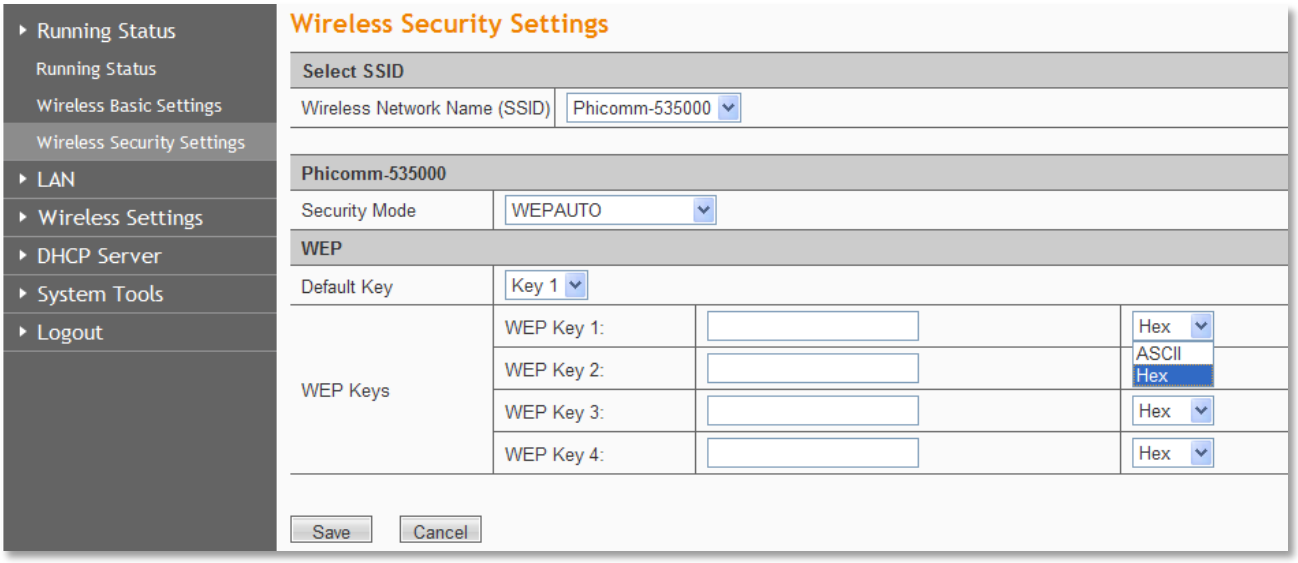
Security Mode:

You can choose **Disable**, **Open**, **Shared**, **WEPAUTO**, **WPA-Personal**, **WPA2-Personal**, **WPA-Personal/ 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/ WEPAUTO



Open System: Select 802.11 Open System authentications.

Shared Key: Select 802.11 Shared Key authentications.

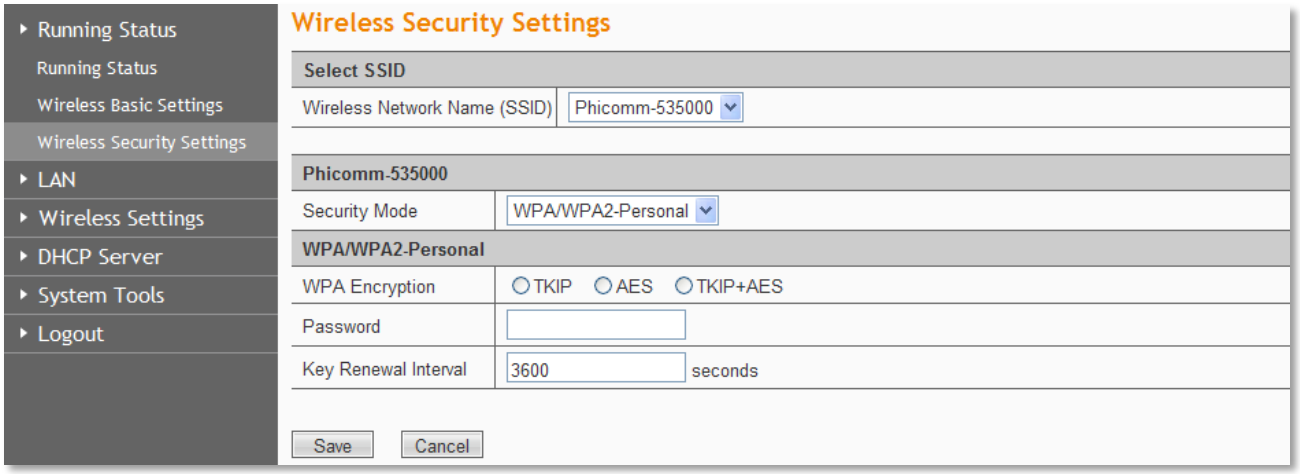
WEPAUTO: Select Shared Key or Open System authentication type automatically based on the

wireless station's capability and request.

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-Personal, WPA2-Personal, WPA- Personal/ WPA2-Personal



WPA-Personal: Pre-shared key of WPA.

WPA2-Personal: Pre-shared key of WPA2.

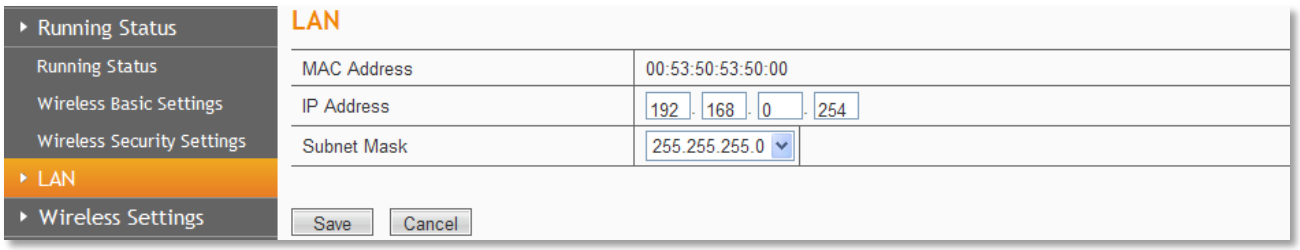
WPA- Personal/ WPA2-Personal: Select WPA-Personal or WPA2-Personal automatically based on the wireless station's capability and request.

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

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

Note: You can set different wireless security for each SSID if you have enabled multiple SSIDs.

LAN



MAC Address: The physical address of the router.

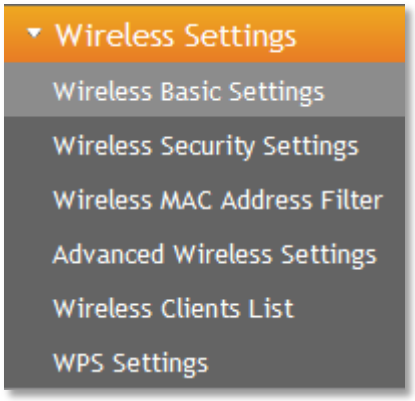
IP Address: The LAN IP Address of the router.

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.

Wireless Settings

Wireless Settings includes six submenus: **Wireless Basic Settings**, **Wireless Security Settings**, **Wireless MAC Address Filter**, **Advanced Wireless Settings**, **Wireless Clients List** and **WPS Settings**. Click any of them, you will be able to configure the corresponding function.



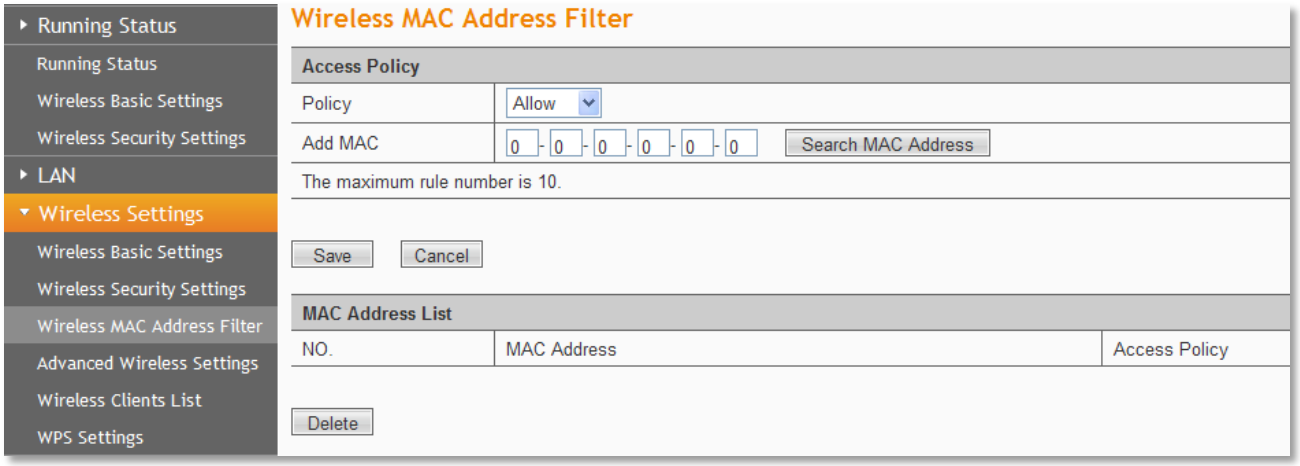
Wireless Basic Settings

Please refer to introduction in Running Status (page 17).

Wireless Security Settings

Please refer to introduction in Running Status (page 22).

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.

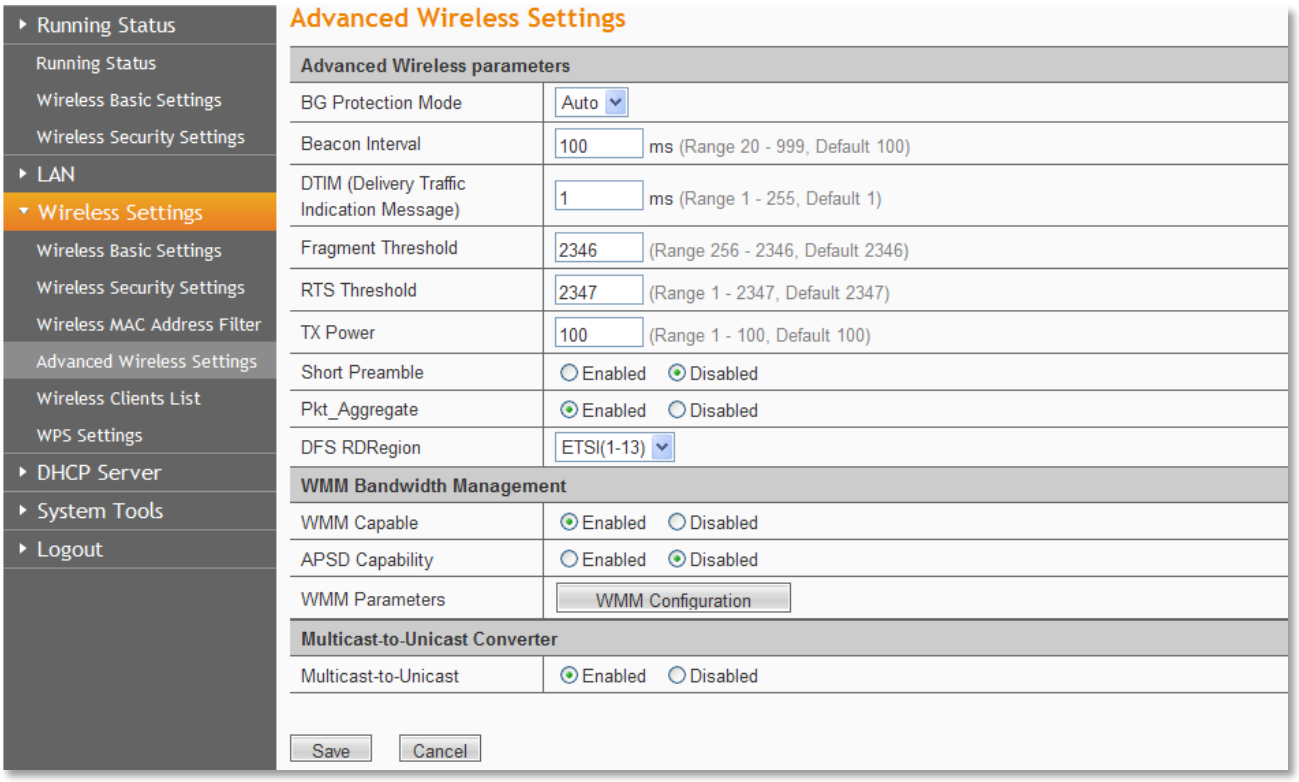
2: Fill MAC address 00:0A:EB:00:07:5F in and click **Save**.

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

1: Choose **Reject** 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.

BG Protection Mode: Leave it as Auto.

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

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

RTS Threshold: Set the RTS (Request to send threshold.) threshold. When the packet size is larger than the preset RTS size, the wireless router will send a RTS to the destination station to start a negotiation. The default value is 2347.

TX Power: Wireless transmission power. You can choose from 1 to 100.

Short Preamble: Leave it as enable.

Pkt_Aggregate: Leave it as disable.

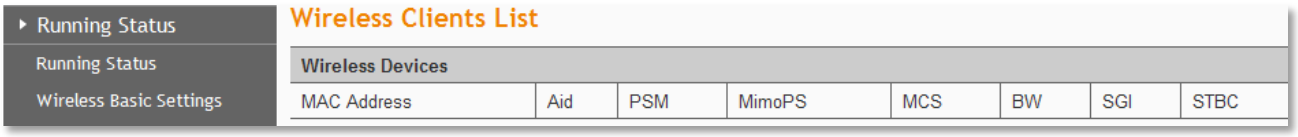
DFS RD Region: Choose the region for the wireless network.

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

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

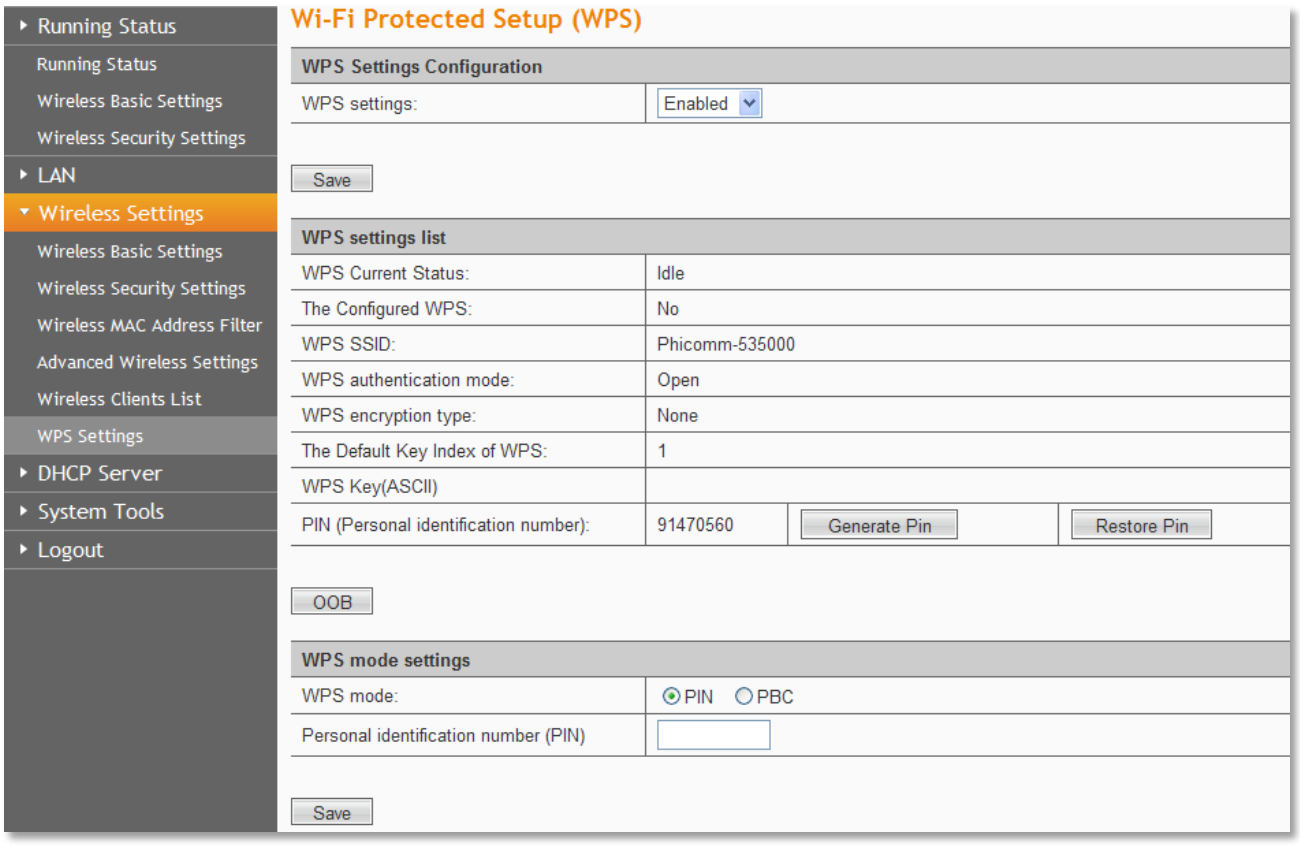
Multicast-to-Unicast: Leave it as enable.

Wireless Clients List



You can check the wireless clients of the access point in this page.

WPS Settings



The WPS function can help you add a new device to the network quickly. If the client device supports Wi-Fi Protected Setup and is equipped with a WPS button, you can add it to the network by pressing the WPS button on the device and then press the button on the router

within two minutes. The status LED on the router will light green for five minutes if the device has been successfully added to the network; If your client asks for the Router's PIN number, enter the router's PIN number into your client device; If your client device has a WIFI Protected Setup PIN number, enter that number in the PIN box.

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

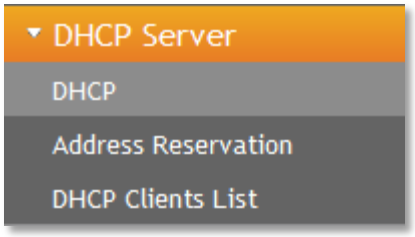
WPS Mode: Supports two ways to configure WPS settings: PBC (Push-Button Configuration) and PIN code.

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

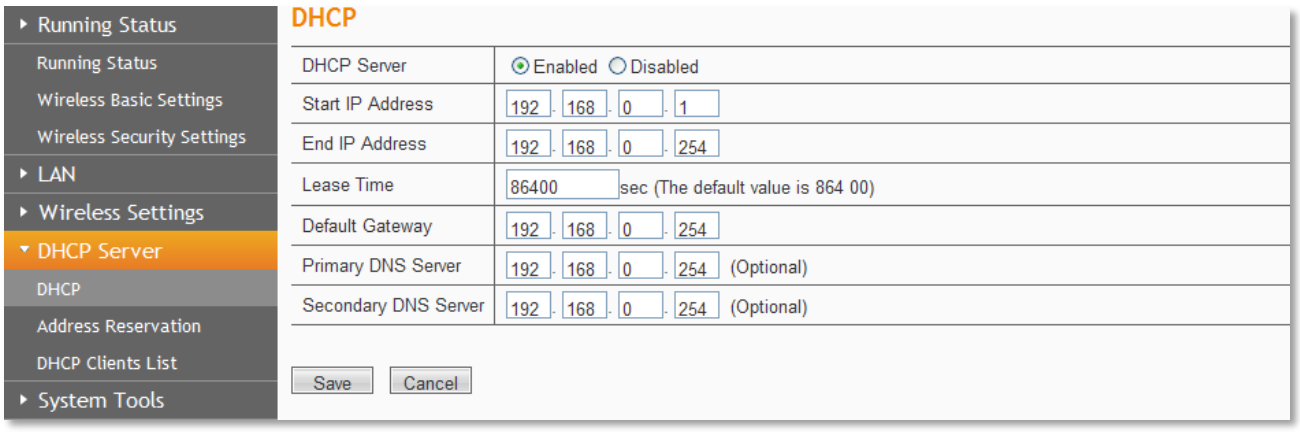
PIN: If this option is enabled, you need to enter a wireless clients PIN code in the blank and keep the same code in the client.

DHCP Server

There are three submenus under the DHCP menu: **DHCP**, **Address Reservation** and **DHCP Clients List**. Click any of them, and you will be able to configure the corresponding function.



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.

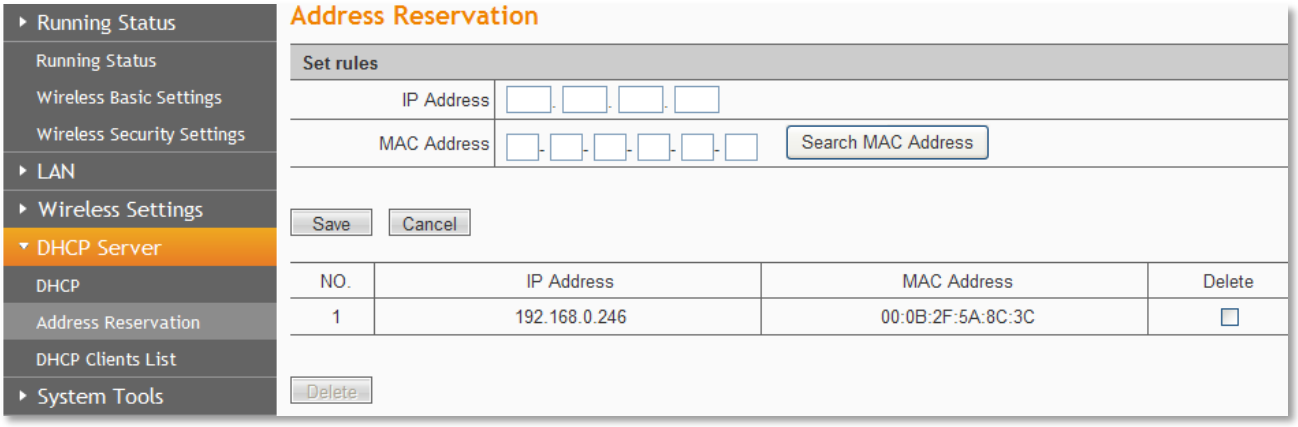
Default Gateway: (Optional) Suggest to input the IP Address of the LAN port of the Router.

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



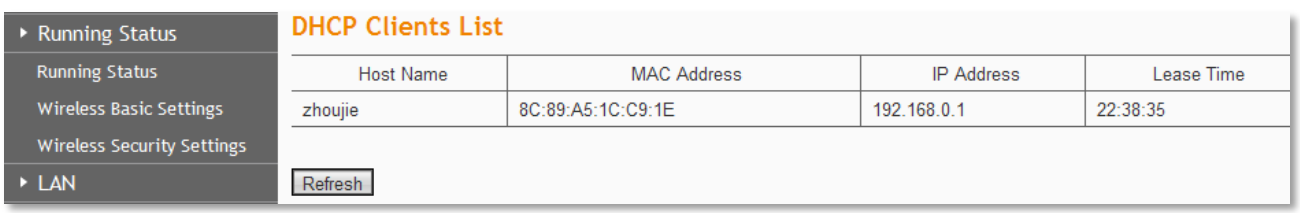
When you specify a reserved IP address for a PC in the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses could be assigned to servers that require permanent IP settings.

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.

Note: This function takes effect only when the DHCP service is enabled.

DHCP Client List

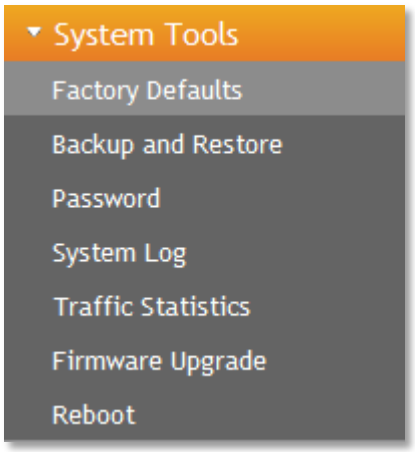


Here you can see the information of DHCP Clients.

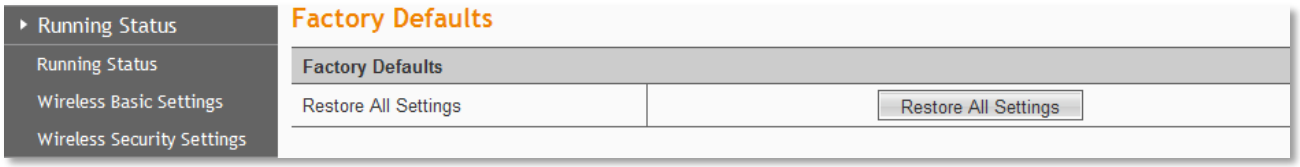
Refresh: Click **Refresh** button to refresh the DHCP clients list.

System Tools

There are seven submenus under the System Tools: **Factory Defaults**, **Backup and Restore**, **Password**, **System Log**, **Traffic Statistics**, **Firmware Upgrade** and **Reboot**. Click any of them, and you will be able to configure the corresponding function.



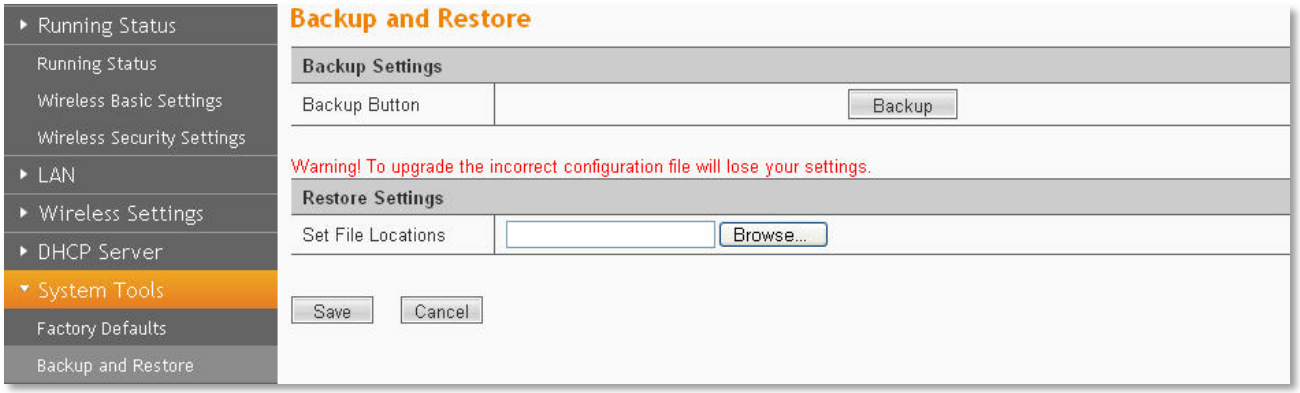
Factory Defaults



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

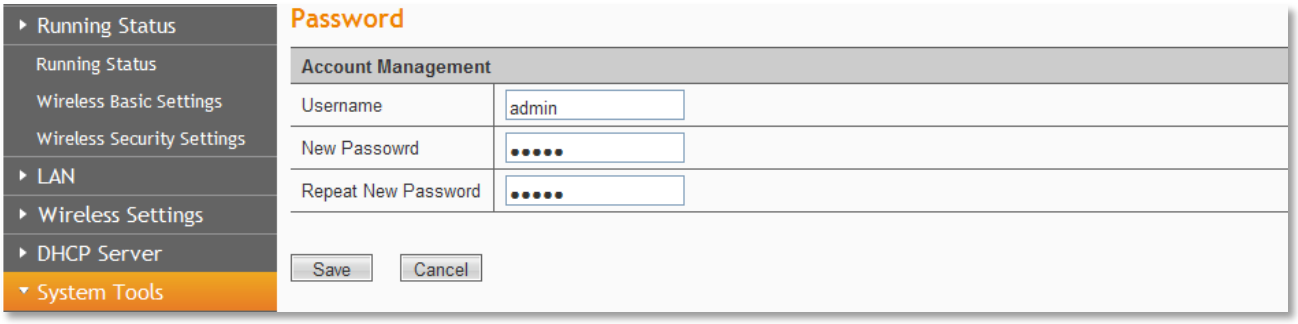
To restore the Router's configuration, follow these instructions:

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.

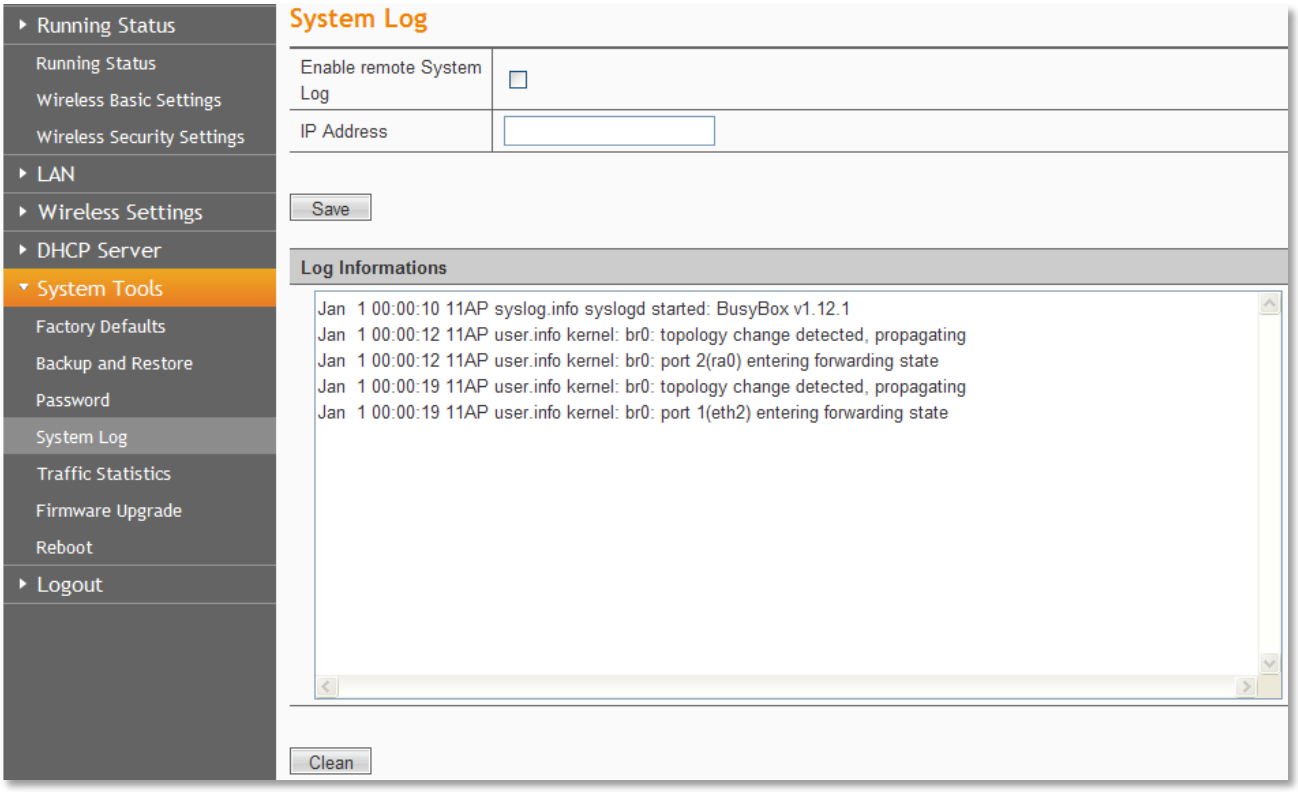
Note: Keep the power on during the process, in case of any damage.

Password



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

System Log



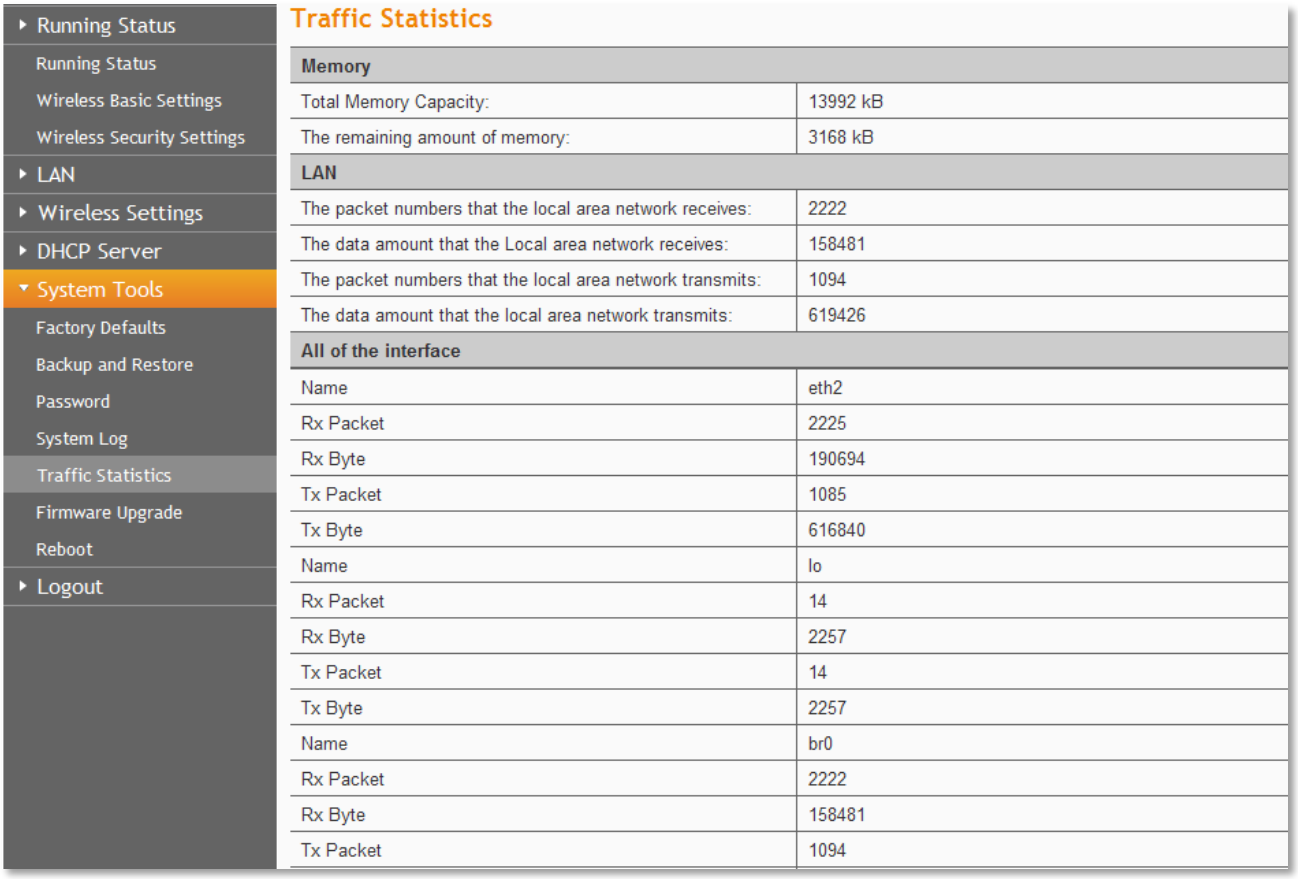
The system log is a detailed record of the websites that users on your network have accessed or attempted to access. You can enable remote System Log function to view the log in remote place.

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

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

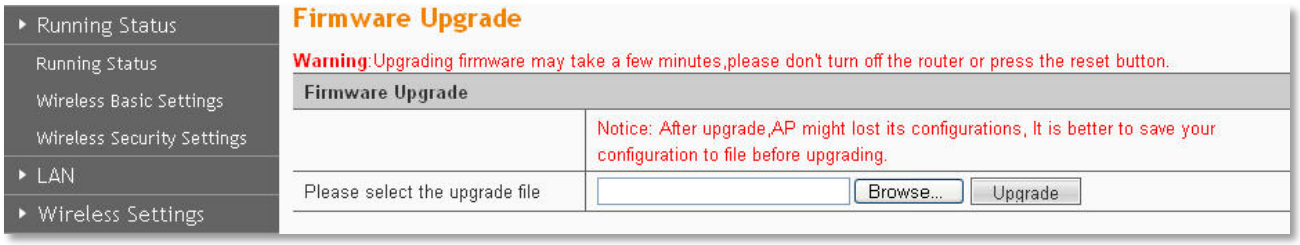
Clean: Click **Clean** button to clear all shown information.

Traffic Statistics



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

Firmware Upgrade



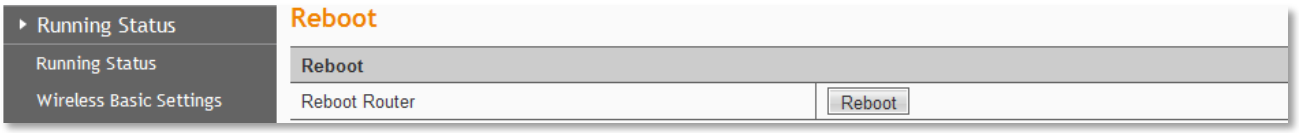
You can upgrade the router to the lasted version in this page, please download a most recent firmware upgrade file from our website. After downloading the file, you need to extract the zip file before upgrading the router. Browse for the upgrade file, then click **Upgrade** button.

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.

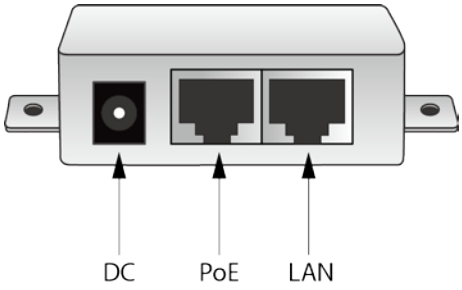
Logout

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

Chapter5: PoE (Power over Ethernet)

Equipped with Power Injector, the Access Point can be placed at any position regardless of the location of the Power Adapter (within a certain distance range).

Hardware Overview of PoE



DC: Connect to the provided power adapter.

PoE: Connect to the LAN port of AP.

LAN: Connect to the Ethernet device with CAT5 Ethernet cable to transmit data.

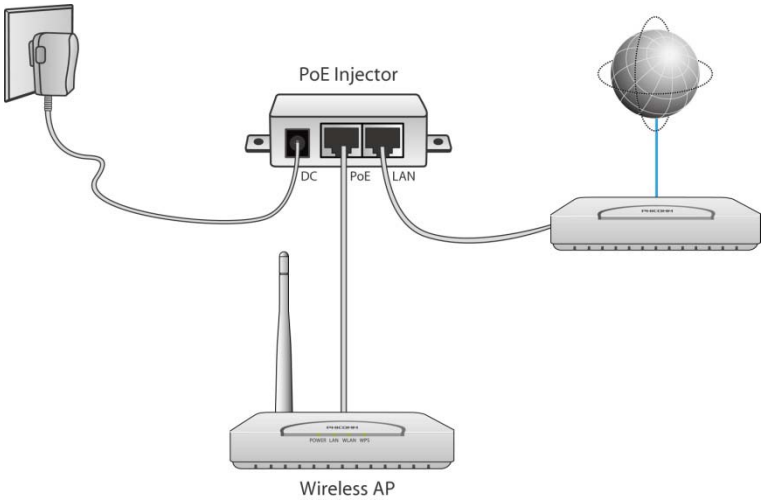
Installation with PoE Injector

1. Turn off all your network devices, including the Switch, power injector and the AP.

2. Connect your Modem Router to the LAN port on the power injector with an Ethernet cable.

3. Plug the provided power adapter into the DC jack on the power injector, and the other end to a standard electrical wall socket.

4. Connect your AP to the PoE (LAN) port on the power injector with an Ethernet cable.



Note: Provided with the power of DC 5V/1A, the cable between PoE port of passive PoE Injector and the LAN port on Access Point is not more than 30m long, and all cables connected to the passive PoE Injector should be no more than 100m long.

Chapter6: 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
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, NetWare®, UNIX® or Linux
Hardware	
Interface	1 x 10/100Mbps LAN port with passive PoE supported
Buttons	ON/OFF Button, WPS Button, Reset Button
Antenna	1 x3dBi Detachable Omni-directional Antenna
Power Supply	DC 12V 0.5A
Dimensions(W x D x H)	165mm x 106mm x 26.5mm
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, RoHS
Package Contents	1 x Wireless N Access Point 1 x Power Adapter 1 x Resource CD 1 x Quick Installation Guide 1 x Ethernet Cable 1 x Passive PoE Injector

*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 Access Point to factory default settings?**

   When the Wireless Access Point is powered on, press and hold the reset button on the rear panel for 8~10 seconds, after all the lights start flashing, release it.

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

- Restore the wireless Access Point to factory default settings. If you do not know how to do it, please refer to the answer for question 1.
- Use the default username and password: admin, admin.
- Reconfigure the wireless Access Point since you have ever reset it.

3. **I cannot login the 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 Computers IP Address in this manual.
- Make sure you put 192.168.0.254 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.