IP-COM®

# User Guide


Wireless N900 High Power
Dual Band Access Point
Model No.:**W75AP**

# Copyright Statement



# Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

# Technical Support

Website: http://www.ip-com.com.cn
Tel: (86 755) 2765 3089
Email: info@ip-com.com.cn

# Contents

# Chapter 1 Product Overview

The Wireless AP is a best-in-class 802.11n indoor access point designed specifically for wireless projects. With suspension installation and existed structure, the device saves time and costs. Versatile and powerful, the Wireless AP offers multiple security modes and supports 802.11n, which makes your data transmission safe. Plus, the provided unified management utility based on X86 allows network administrators to centrally manage IP addresses, SSID and security settings, etc. of APs on LAN, thus enabling a highly manageable and extremely robust wireless network.

## 1.1 Product Features

- Supports IEEE802.11n, IEEE802.11g, IEEE 802.11b and IEEE802.11a；
- 1000M Ethernet port for wired LAN connection;
- PoE Port for connecting to power supply with the included injector;
- One RJ-45 10/100/1000 IEEE802.3ab, IEEE802.3u, IEEE802.3 auto-sensing Gigabit port for data transmission or power supply;
- Wireless rates of up to 900Mbps (dual band);
- Unified Management allows network administrators to centrally manage APs on LAN;
- Supports IP address, wireless SSID, device name, channel, wireless security and domain diagnostics;
- WEP, WPA-PSK, WPA2-PSK and WPA-PSK/WPA2-PSK encryptions secure wireless network against unauthorized accesses;
- Can be configured to select an optimum channel for device to operate on;
- Can be configured to adjust transmitting power;
- Supports AP and WDS mode.

## 1.2 Package Contents

Please verify that the package contains the following items:

- Wireless Access Point
- Power Adapter
- PoE Injector
- 5 screws
- Ethernet Cable
- Bracket
- Install Guide

If any of the above items are incorrect, missing, or damaged, please contact your reseller for immediate replacement.

# 1.3 LEDs and Interfaces

**Side Panel:**


**Power**

**Solid:** Receiving electrical power;

**Blinking:** Functioning properly;

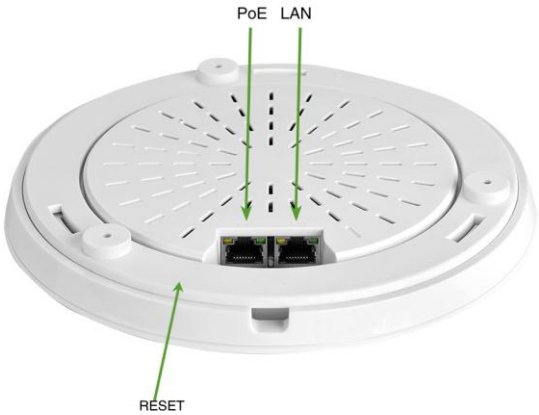
**Off:** Receiving no electrical power or LED is disabled manually.

**2.4GHz, 5GHz**

**Solid:** Wi-Fi is enabled;

**Blinking:** Transferring data;

**Back Panel:**




**RESET**

Restores the device to the factory default settings when pushed and held for 7 seconds (This button has been hidden by the bracket of this device. Before pressing this button, you should remove the bracket.).

**PoE**

PoE Port for connecting to power supply with the included injector;

**LAN**

1000M Ethernet Port for connecting to an Ethernet LAN device such as a PC or switch, etc.

# Chapter 2 Installation

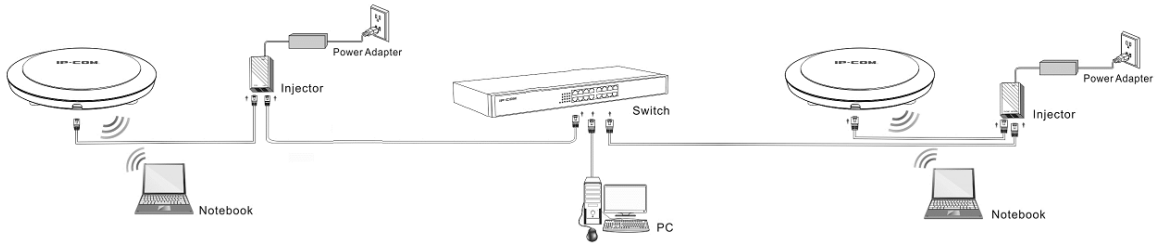
Installation procedures:

1. Connect the injector to the power adapter.
2. Connect the PoE port of the injector to the PoE port on this device with an Ethernet cable.
3. Connect the LAN port of the injector to the switch.
4. Hang the AP:

   (1) Install the bracket onto the ceiling.

   (2) Fix the AP onto the bracket.

The network topology is shown below:



# Chapter 3 Configuration Guidelines

## 3.1 IP Configuration

The default IP address of your wireless access point is 192.168.0.254. If you are using the default IP subnet, the computer you are using to connect to the device should be configured with an IP address that starts with 192.168.0.x (where x can be any number between 1~253) and a Subnet Mask of 255.255.255.0; if you have changed the subnet of the wireless access point, the computer you are using to connect must be within the same subnet. If you are not clear about this configuration, please refer to Appendix 2: Configure PC.

## 3.2 Web Login

To connect to the Wireless AP using the defaults IP address:

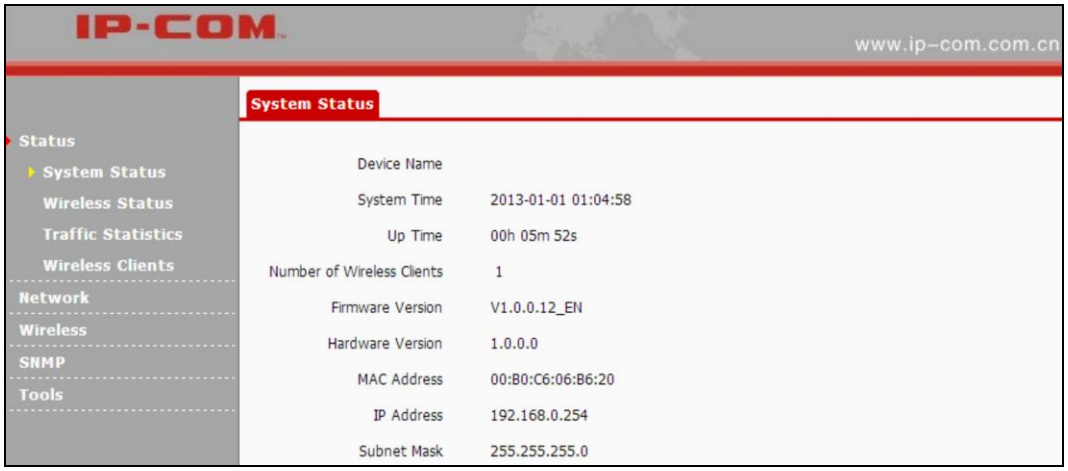
1. Open a Web browser.
2. Enter 192.168.0.254 into your browser.
3. Enter the default User Name admin and default Password admin into the login window.


4. Click **Login** and your Web browser shall automatically display the home page.

## 3.3 Status

### 3.3.1 System Status

This screen displays this device's current system status.



**1. Device Name:** Displays this device's name.

**2. System Time:** Displays system's current time.

**3. Up Time:** Displays the device's uptime.

**4. Number of Wireless Clients:** Displays the information of connected wireless clients (if any).

**5. Firmware Version:** Displays Device's current firmware version.

**6. Hardware Version:** Displays Device's current hardware version.

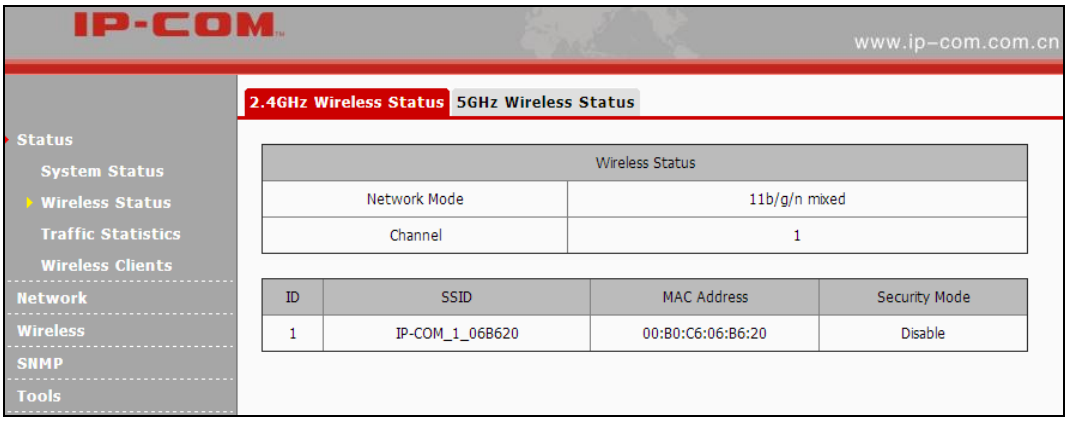
**7. MAC Address:** Displays device's LAN MAC address.

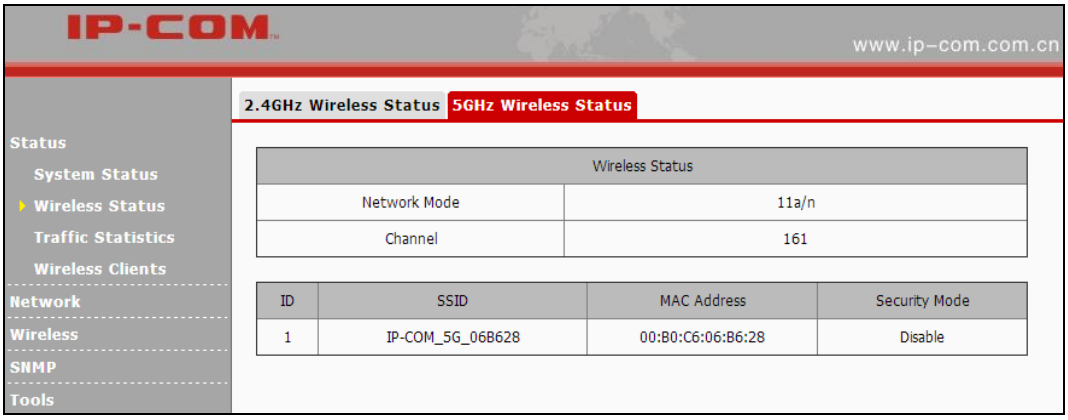
**8. IP Address:** Displays device's LAN IP address.

**9. Subnet Mask:** Displays device's subnet mask.

## 3.3.2 Wireless Status

This section displays 2.4GHz and 5GHz wireless status.




**1. Network Mode:** Displays device's current network mode.

**2. Channel:** Displays device's current channel.

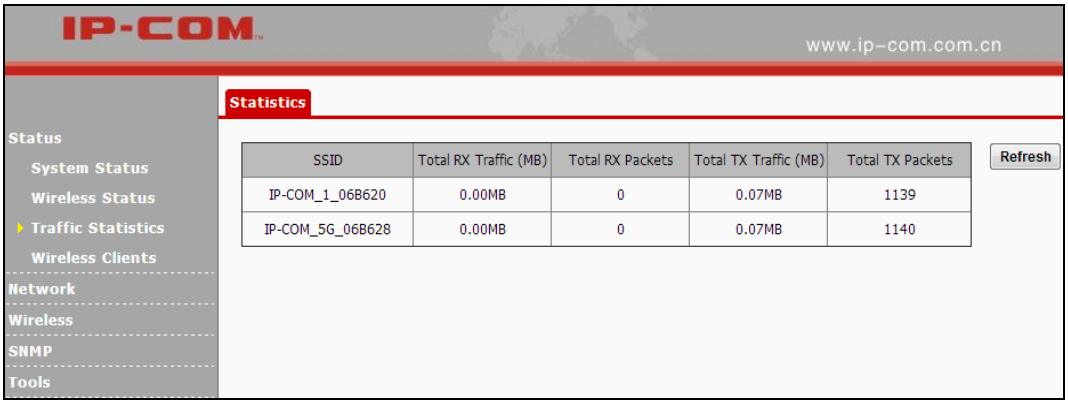
**3. SSID:** Displays device's network name.

**4. MAC Address:** Displays connected wireless client's MAC address.

**5. Security Mode:** Displays device's current security mode.

## 3.3.3 Traffic Statistics

This section displays each SSID's traffic statistics.




**1. Total RX Traffic:** Total RX bytes SSID has received.

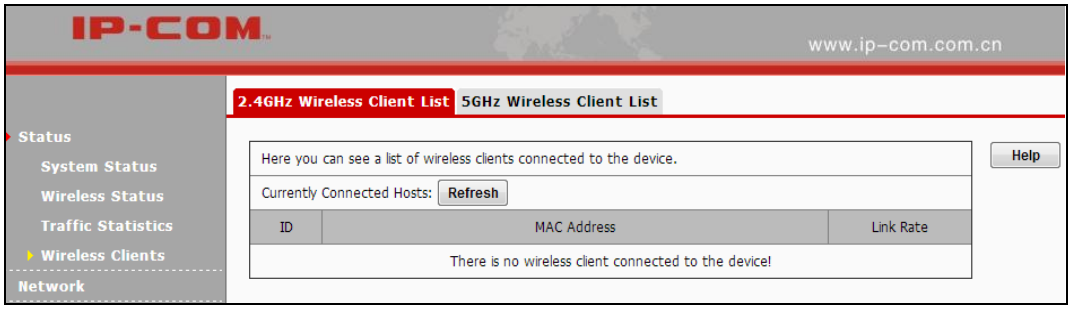
**2. Total RX Packets:** Total RX packets SSID has received.

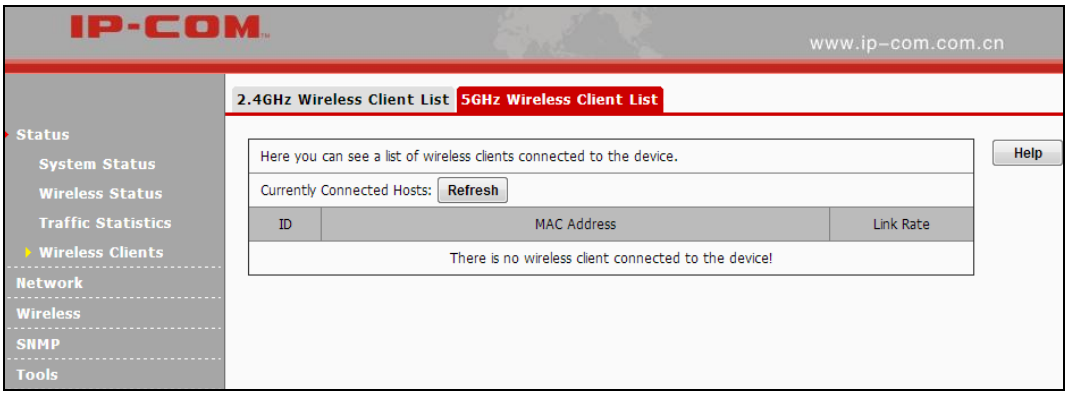
**3. Total TX Traffic:** Total TX bytes SSID has transmitted.

**4. Total TX Packets:** Total TX packets SSID has transmitted.

## 3.3.4 Wireless Clients

This section displays information of connected clients (if any). You can view 2.4GHz client list and 5GHz client list respectively here.




**1. MAC Address:** Displays connected wireless client's MAC address.

**2. Link Rate:** Displays the link speed rate between this device and the connected wireless client.

**Note** ----------

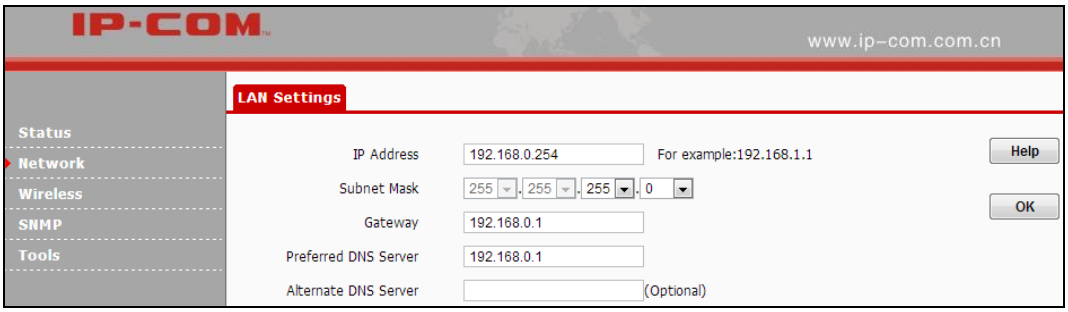
If no clients connected to this device, a prompt message will appear: There is no wireless client connected to the device.

---

# 3.4 Network

## 3.4.1 LAN Settings

Here you can configure the LAN IP address, subnet mask, gateway and DNS servers.




**Note** ----------

1. Default LAN IP: 192.168.0.254, default subnet mask: 255.255.255.0.
2. If you change this IP address, you must use the new one to re-log on to this web utility.

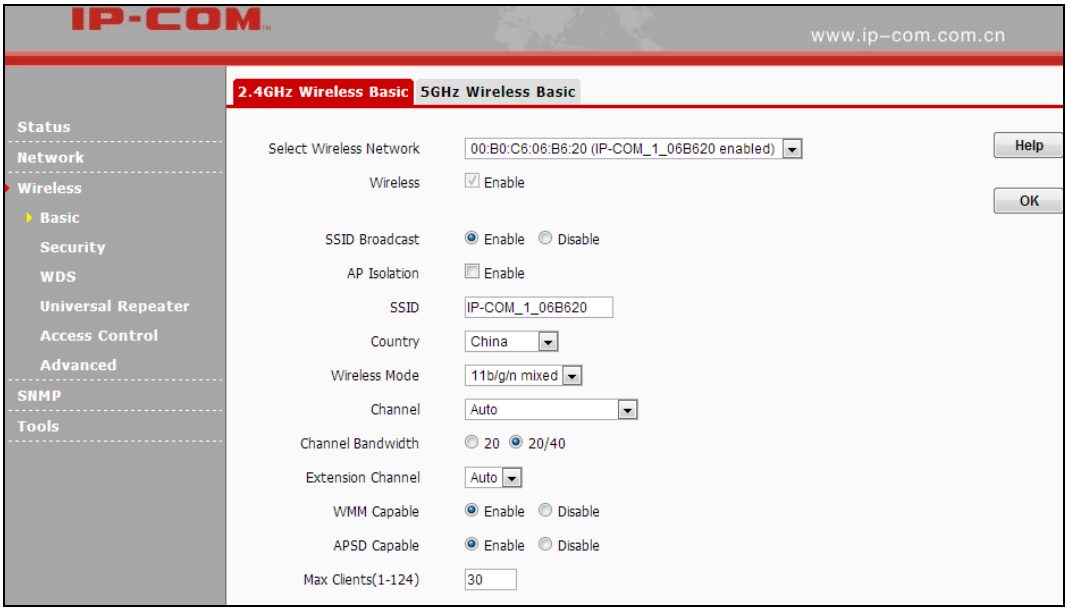
---

# 3.5 Wireless

## 3.5.1 Basic

Select 2.4GHz or 5GHz to configure basic settings.

2.4GHz Wireless Basic




**1. Select Wireless Network:** 8 SSIDs are available here.

**2. Enable:** Select it to enable wireless feature. As for 2.4GHz, only the first SSID is enabled by default and it can't be disabled. Up to 8 SSIDs can be enabled at the same time.

**3. SSID Broadcast:** This option allows you to have your network name (SSID) publicly broadcast or if you choose to disable it, the SSID will be hidden. It is enabled by default.

**4. AP Isolation:** Isolates clients connected to the same SSID.

**5. SSID:** This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.

**6. Wireless Mode:** Select a right mode according to your wireless client. The default mode of 2.4GHz is 11b/g/n mixed.

**11b mode:** Select it if you have only 11b wireless devices in your wireless network. Up to 11Mbps wireless rate is supported on this mode.

**11g mode:** Select it if you have only 11g or 11n wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

**11b/g mixed mode:** Select it if you have 11b and 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

**11b/g/n mixed mode:** Select it if you have 11b, 11g and 11n wireless devices in your wireless network. In this mode wireless connection rate is negotiated. Up to 450Mbps wireless rate is supported on this mode.

**7. Channel:** Select from 1~13 channels or Auto. The best selection is a channel that is the least used by neighboring networks.

**8. Channel Bandwidth:** Select a proper channel bandwidth to enhance wireless performance. Select 20/40M frequency width when device is operating in 11n, select 20M frequency width when device is operating in non-11n mode.

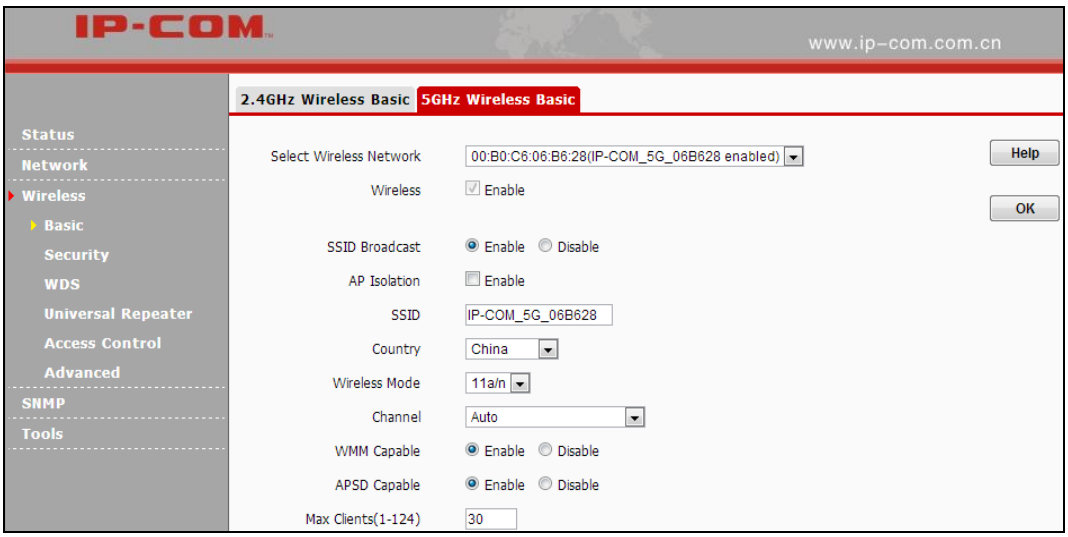
**9. Extension Channel:** This is used to enhance data throughput ability for 802.11n devices on the network.

**10. WMM-Capable:** WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

**11. ASPD Capable:** Select to enable/disable the auto power saving mode. By default, this option is disabled.

**12. Maximum Clients:** Total clients should be within 124.

**5GHz Wireless Basic**




**1. Select Wireless Network:** 8 SSIDs are available here.

**2. Enable:** Select it to enable wireless feature. As for 2.4GHz, only the first SSID is enabled by default and it can't be disabled. Up to 8 SSIDs can be enabled at the same time.

**3. SSID Broadcast:** This option allows you to have your network name (SSID) publicly broadcast or if you choose to disable it, the SSID will be hidden. It is enabled by default.

**4. AP Isolation:** Isolates clients connected to the same SSID.

**5. SSID:** This is the public name of your wireless network. Select the SSID you wish to configure from the drop-down list.

**6. Wireless Mode:** Select a right mode according to your wireless client. The default mode of 5GHz is 11a/n.

**11a mode:** Select it if you have only 11a wireless devices in your wireless network. Up to 54Mbps wireless rate is supported on this mode.

**11a/n mode:** In this mode wireless connection rate is negotiated. Up to 450Mbps wireless rate is supported on this mode.

**7. Channel:** Select 149, 153, 157, 161, 165 or Auto in 11a mode and select 149, 157 or Auto in 11a/n mode. The best selection is a channel that is the least used by neighboring networks.

**8. WMM-Capable:** WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

**9. ASPD Capable:** Select to enable/disable the auto power saving mode. By default, this option is disabled.

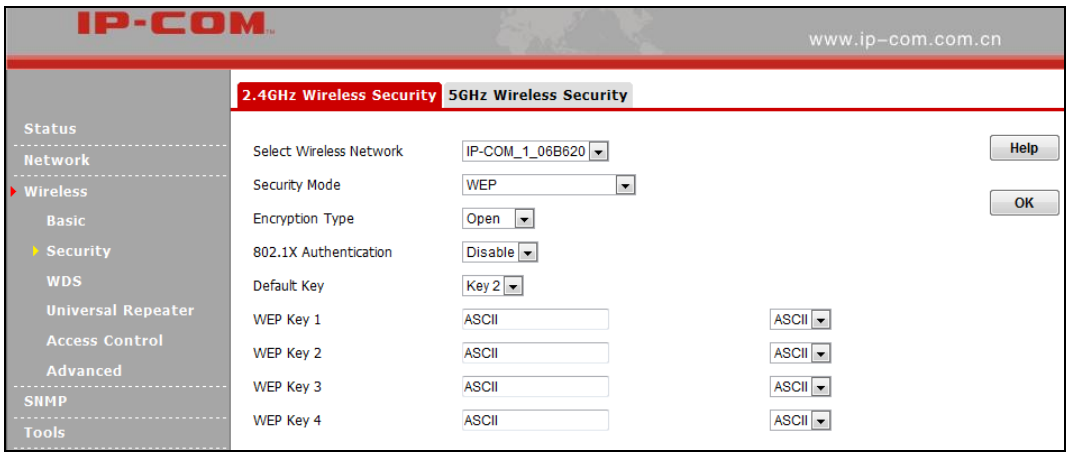
**10. Maximum Clients:** Total clients should be within 124.

## 3.5.2 Security

This section allows you to secure your wireless network. Here we introduce 4 security modes to you.


**WEP**

WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two types of encryption can be used with WEP: Open and Shared Key.




**1. Encryption Type:** Select Open or Shared from the drop-down list.

**2. WEP Key:** Select Hex or ASCII from the drop-down list. Enter 5 or 13 valid ASCII characters (0-9,a-z,A-Z,@,*,-,_ can be included) if you select ASCII or enter 10 or 26 valid Hex characters (0-9,a-f,A-F can be included) if you select Hex.

**WPA-PSK**

The WPA (Wi-Fi Protected Access) protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being tampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.

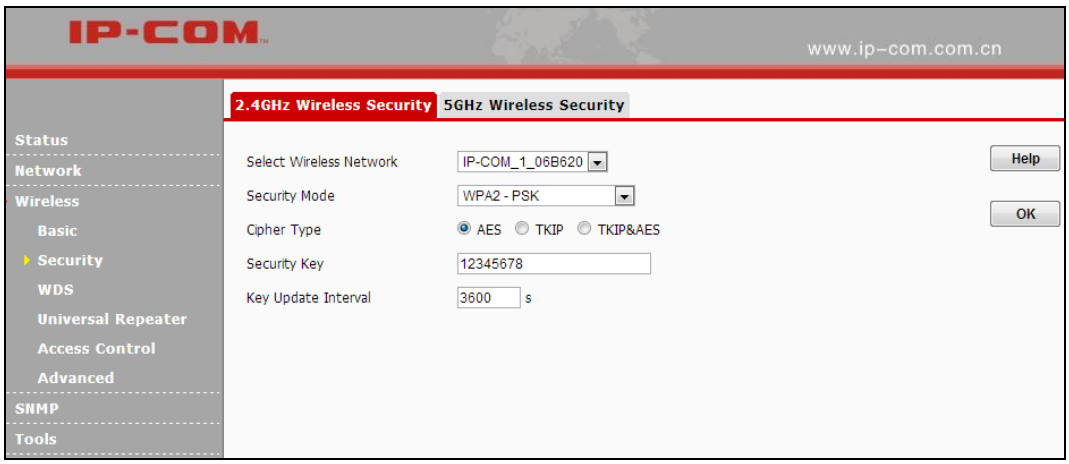

**1. Cipher Type:** Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.

**2. Security Key:** Enter a security key, which must be between 8-63 ASCII characters long.

**3. Key Update Interval:** Enter a valid time period for the key to be changed.

**WPA2-PSK**

WPA2 (Wi-Fi Protected Access version 2) is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secured than WPA and WEP.



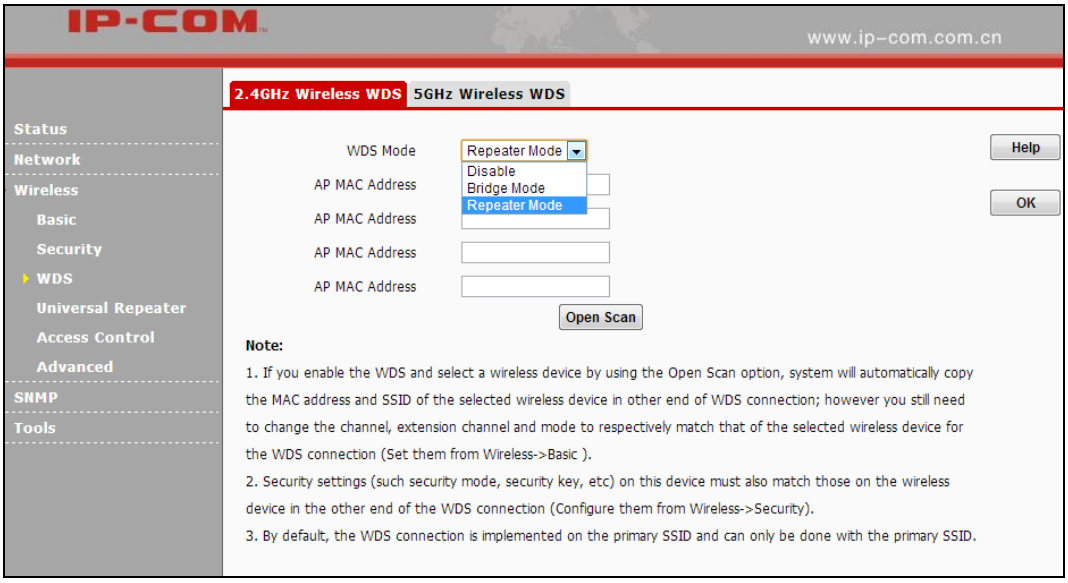

**1. Cipher Type:** Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.

**2. Security Key:** Enter a security key, which must be between 8-63 ASCII characters long.

**3. Key Update Interval:** Enter a valid time period for the key to be changed.

## 3.5.3 WDS

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. Note: The Access Points you select must support WDS.




**1. WDS Mode:** Select Disable, Repeater Mode or Bridge Mode.

**2. AP MAC Address:** Displays the remote AP's MAC address.

**For Example:**

Access Point 1 LAN IP: 192.168.0.254

Access Point 2 LAN IP: 192.168.0.253

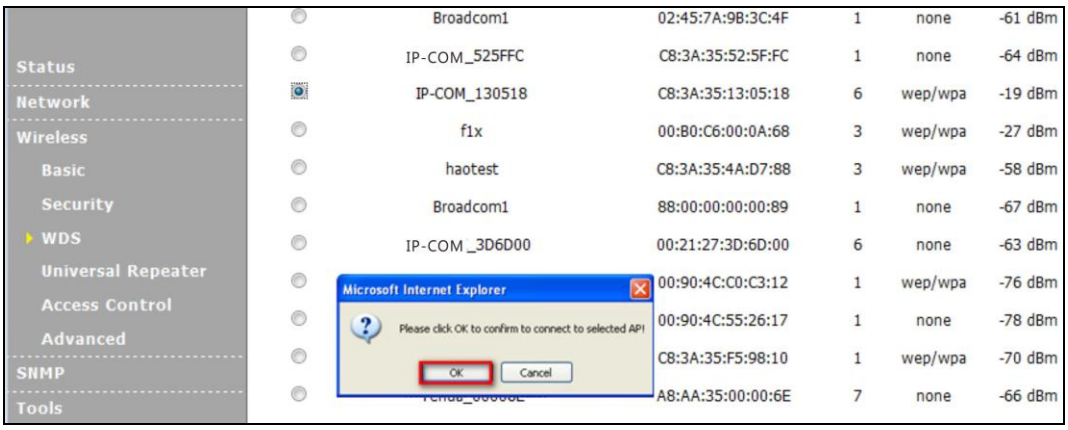
WDS Mode: Repeater Mode

Configure Access Point 1:

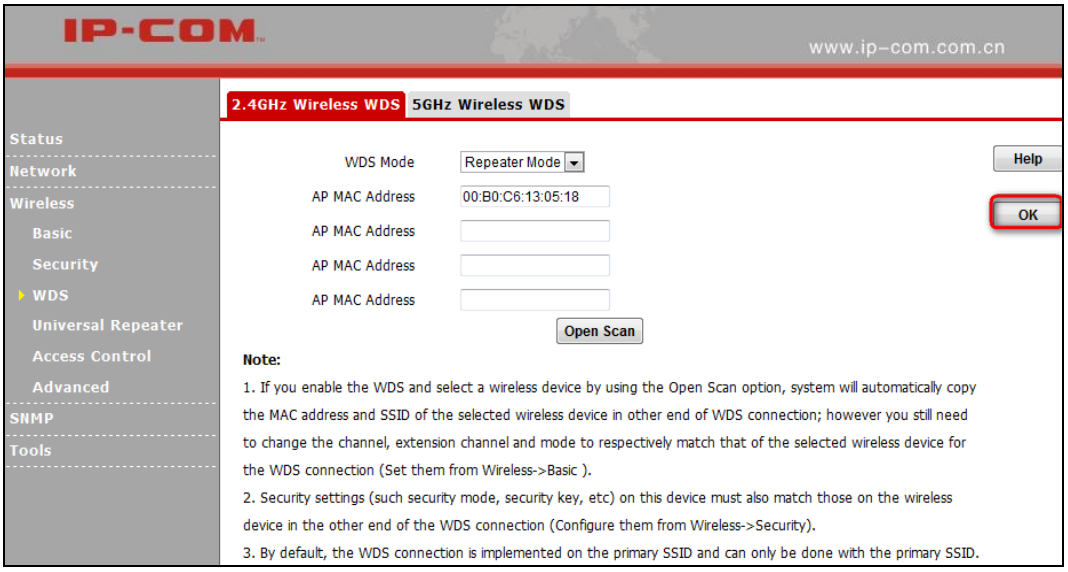
1. Enter the remote AP's MAC address and click **OK**.

2. You can also scan the remote AP.

1）Click **Open Scan** to select the remote AP and click **OK** to add the corresponding MAC address automatically.




2) Click **OK** to save your settings.




Then follow the steps mentioned above to configure the Access Point 2. After the two APs have added each other, they can be bridged successfully.

**Note** ----------

1. In WDS mode, the two APs should support WDS and you should keep their SSIDs, channels, security modes and keys the same. As for IP address, they should not be the same but on the same network segment;

2. Once the security mode has been changed, please reboot the device.

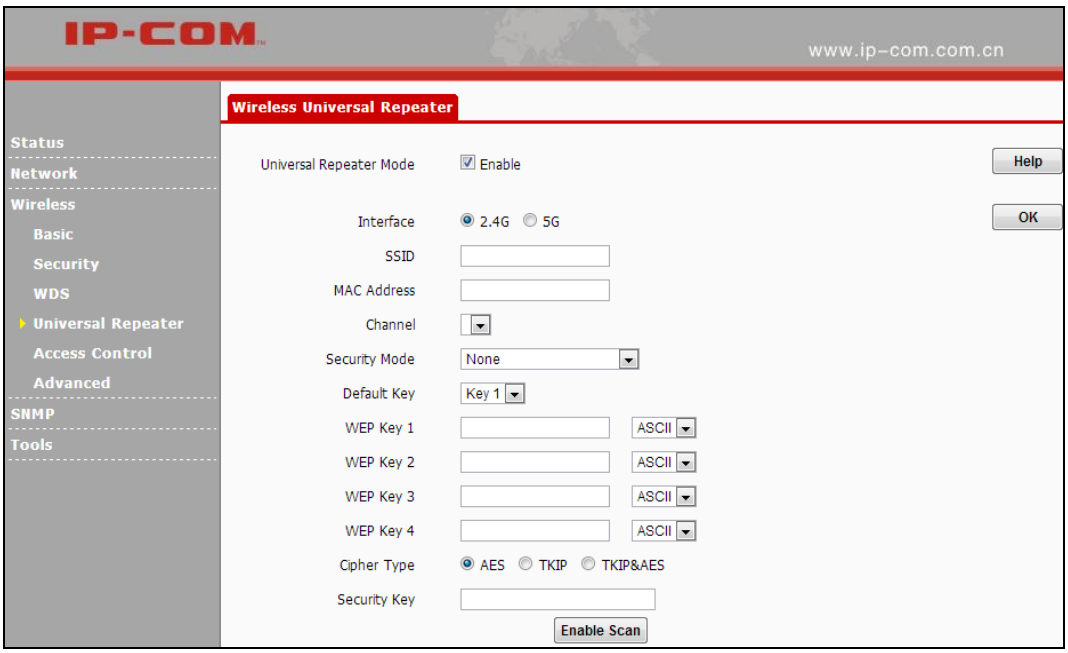
3. If one of the APs is in Bridge Mode, the remote one must be in Repeater Mode.

4. In Bridge mode, clients won't be able to access the device's primary SSID.

---

## 3.5.4 Universal Repeater

Select Universal Repeater and enable scan to automatically populate SSID and channel of the AP to connect or manually enter the AP's SSID, channel and security key.



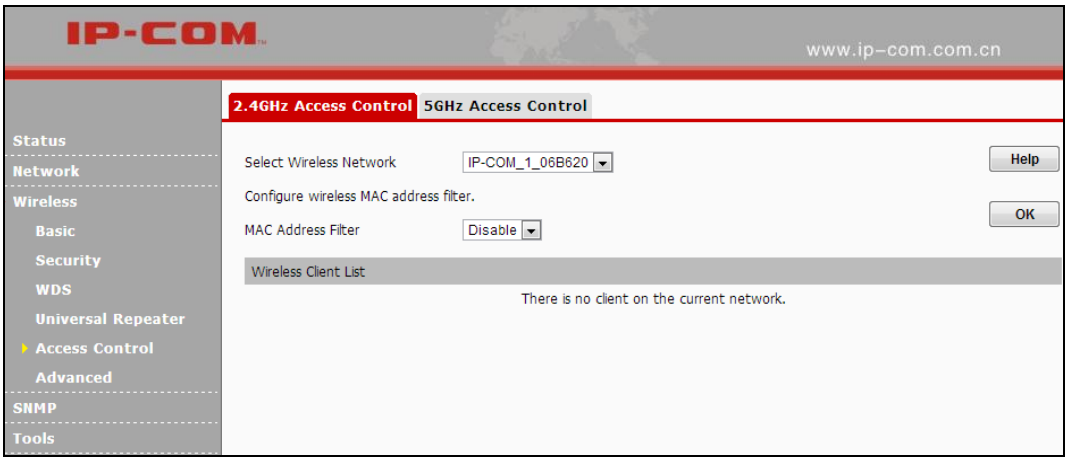

**Note** ----------

1. Enabling scan does not populate the security key, so you must still manually enter it.
2. Make sure your (local) AP, PCs connected and the remote AP to connect are on the same subnet with different IP addresses.
3. If ping requests sent from PCs connected to your local AP are properly replied by the targeted remote AP, Universal Repeater is successfully operating; if not, check your settings again.

---

## 3.5.5 Access Control

Specify a list of devices to allow or disallow a connection to your wireless network via the device's MAC addresses. To deactivate this feature, select "Disable"; to activate it, select "Allow" or "Deny" (2.4GHz/5GHz).



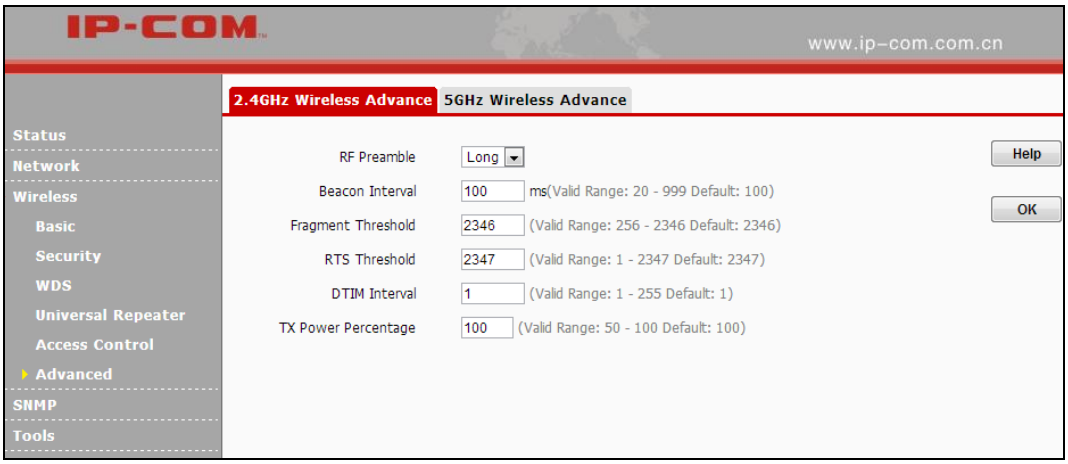

**MAC Filter Mode:** Select Allow or Deny from the drop-down list.

1. To permit a wireless device to connect to your wireless network, select **Allow**, enter its MAC address, click **Add** and then **OK**. Then only this device listed as “Allowed” will be able to connect to your wireless network; all other wireless devices will be forbidden.

2. To disallow a wireless device to connect to your wireless network, select **Deny**, enter its MAC address, click **Add** and then **OK**. Then this device listed as “Denied” will be unable to connect to your wireless network.

### 3.5.6 Advanced

This section allows you to configure advanced wireless settings (2.4GHz or 5GHz). If you are new to networking and have never configured these settings before, we recommend you to leave the default settings unchanged.




**1. RF Preamble:** This is used to synchronize frames. Do not change it unless necessary.

**2. Beacon Interval:** This is a time interval between any 2 consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Specify a valid Beacon Interval value between 20-999. The default value is 100.

**3. Fragment Threshold:** Specify a valid Fragment Threshold value between 256-2346. The default value is 2346. Any wireless packet exceeding the preset value will be divided into several fragments before transmission.

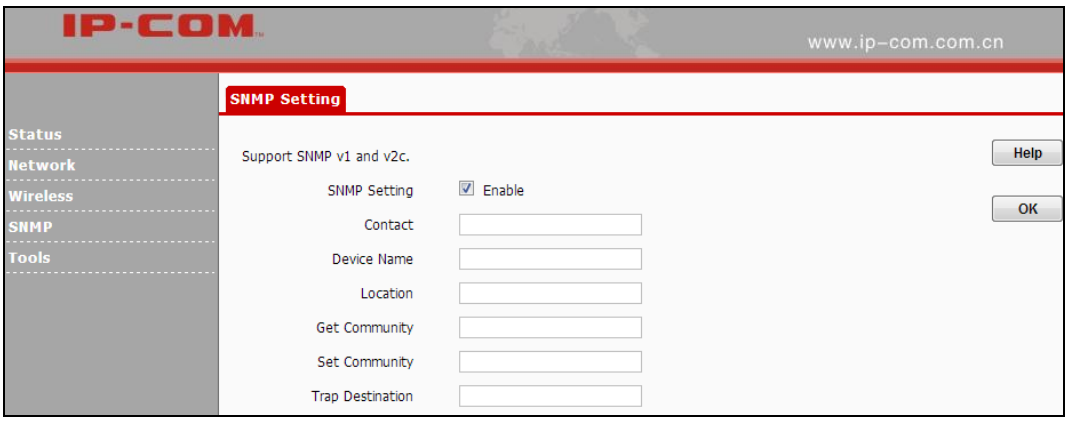
**4. RTS Threshold:** Specify a valid RTS Threshold value between 1-2347. The default is 2347. If a packet exceeds the preset value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value if there are distant clients and interference.

**5. DTIM Interval:** A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive at device’s buffer, the device will send DTIM (delivery traffic indication message) and DTIM interval to wake clients up for receiving these packets. Specify a valid value between 1-255. The default is 1.

**6. TX Power Percentage:** Control TX power . Specify a value between 50 - 100. The default is 100.

## 3.6 SNMP

The Simple Network Management Protocol (SNMP) is widely used in local area networks (LANs) for collecting information, managing, and monitoring network devices, such as servers, printers, hubs, switches, and routers. Specialized software in each SNMP capable device, known as an Agent, continuously monitors the status of the device and reports the results to the SNMP Manager software, which can then act on the report. This device supports both SNMP v1 and SNMP v2.




Click **Enable** to enable the SNMP feature.

**1. Get Community:** Specify a community for reading SNMP agent information;

**2. Set Community:** Specify a community for writing SNMP agent information.

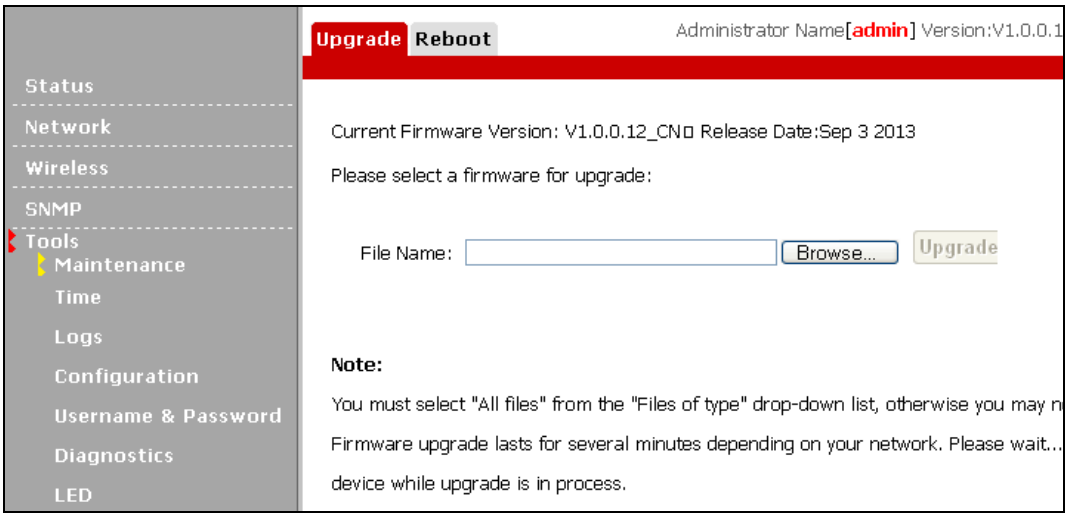
# 3.7 Tools

## 3.7.1 Maintenance

### Upgrade

Upgrade is released periodically to improve the functionality of your device or to add new features. If you run into a problem with a specific feature of the device, log on to our website (http://www.ip-com.com.cn/) to download the latest firmware to update your device.

Click **Tools > Maintenance > Upgrade** to enter the screen below:




**To upgrade device software:**

1. Open a web browser and go to **http://www.ip-com.com.cn/** to download latest firmware.
2. Unzip the compressed upgrade file (.ZIP file).
3. Click **Browse** to locate and select upgrade file on your hard disk.
4. Click **Upgrade** to upgrade device firmware.
5. When the firmware upgrade completes, your wireless access point will automatically restart.
6. Restore the AP back to factory default settings after reboot.

**Note** ----------

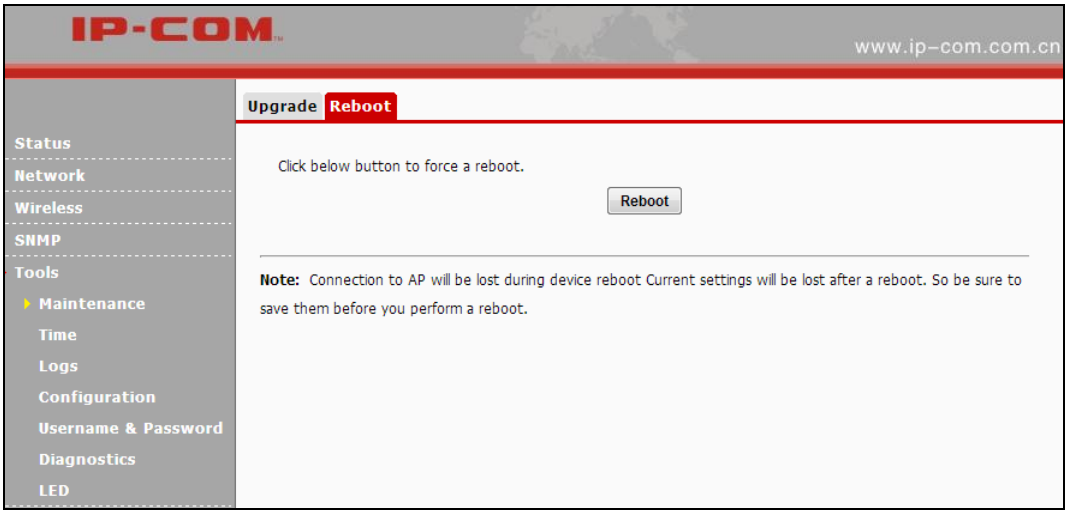
When uploading software to the Wireless AP, it is important not to disconnect the device from power supply. If the power supply is interrupted, the upload may fail, corrupt the software, and render the device inoperable. When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about several minutes.

---

**Reboot**

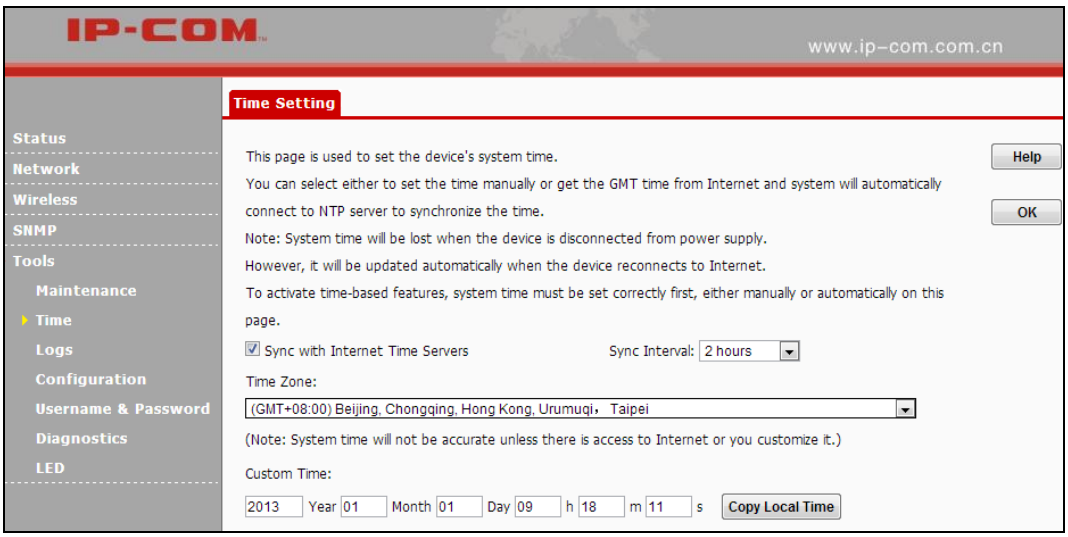
The Reboot option restarts the wireless access point using its current settings. Connections will be lost during reboot.

Click **Tools > Maintenance > Reboot** to display screen below:




## 3.7.2 Time

This page is used to set the device's system time. You can choose to set the time manually or get the GMT time from the Internet and the system will automatically connect to NTP server to synchronize the time.




**1. Sync with Internet Time Servers:** Gets the GMT time from the Internet

**2. Sync Interval:** The default sync interval is 2 hours.

**3. Time Zone:** Select your local time zone.

**4. Copy Local Time:** Copy time on your PC to the device.

**Note** ----------

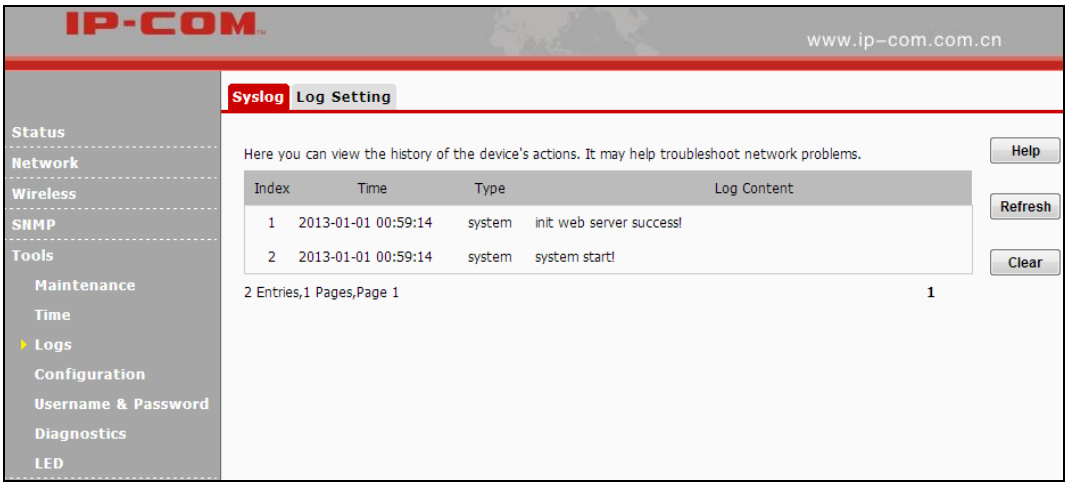
System time will be lost when the device is disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet.

---

## 3.7.3 Logs

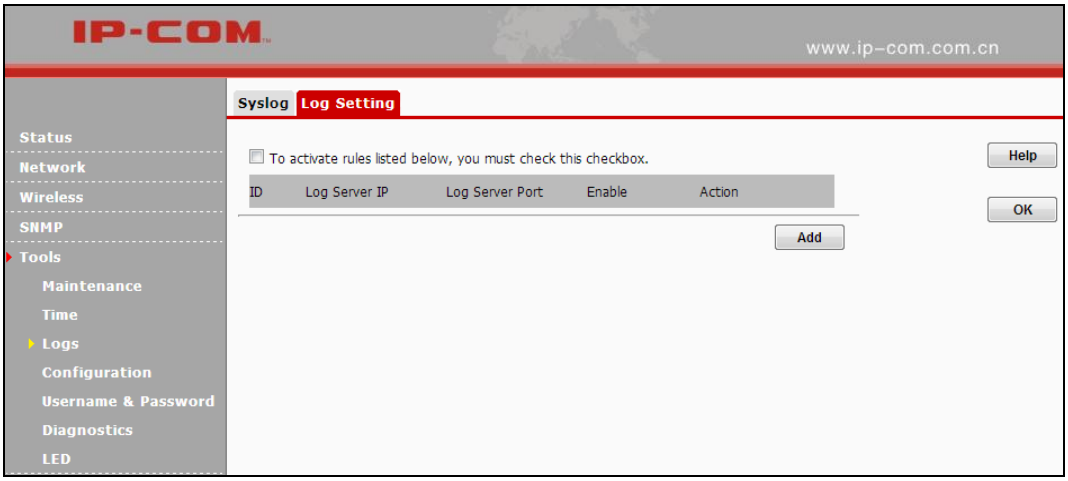
### Syslog

Here you can view the history of the device's actions. Click **Refresh** to display the latest logs and or click **Clear** to remove all logs.




### Log Setting

Here you can set up number of logs and rules of log settings. Up to 300 entries can be logged. The default is 150.




## 3.7.4 Configuration

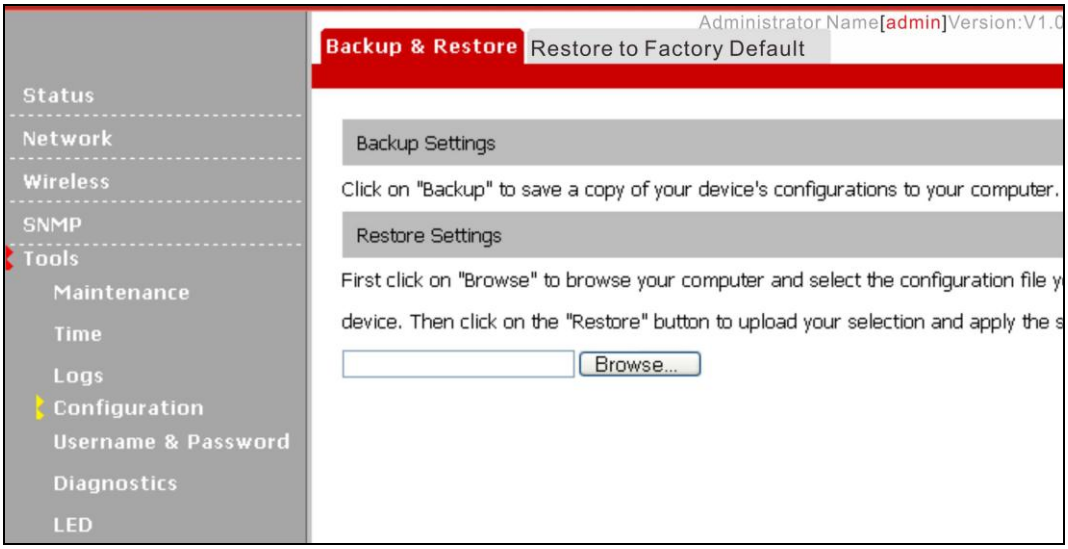
### Backup & Restore

This section allows you to save a copy of the device configurations on your local hard drive or to restore the previous configurations back to the device.

1. **Backup**: Once you have configured the device the way you want it, you can save these settings to a

configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do so, click the **Backup** button and specify a directory to save settings on your local hardware.

2. **Restore**: Click the **Browse** button to locate and select a configuration file that is saved previously on your local hard drive and then click **Restore** to restore it. Configurations will be restored after device reboot.




**Restore to Factory Default**

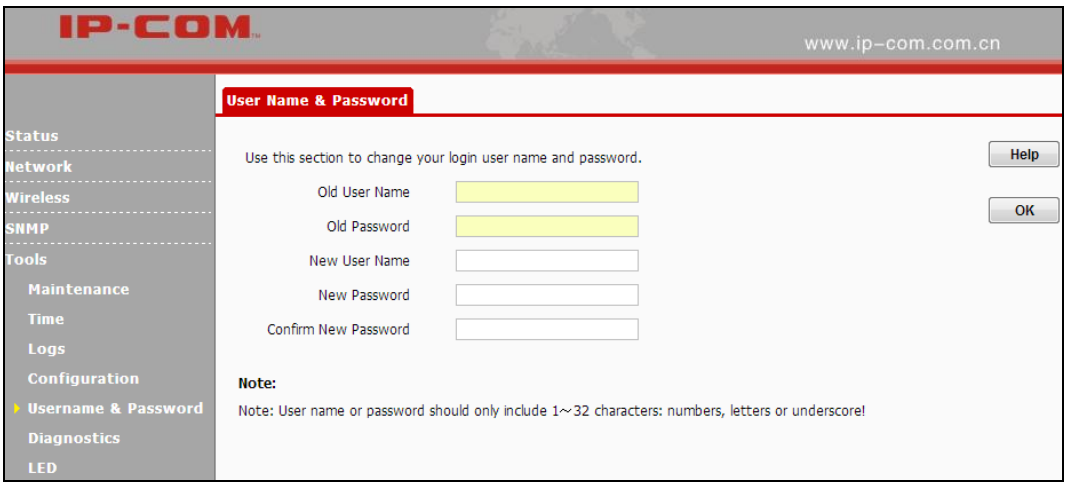
Click the **Restore to Factory Default** button to reset Device to factory default settings.


**Factory Default Settings:**

- **User Name:** admin
- **Password:** admin.
- **IP Address:** 192.168.0. 254
- **Subnet mask:** 255.255.255.0

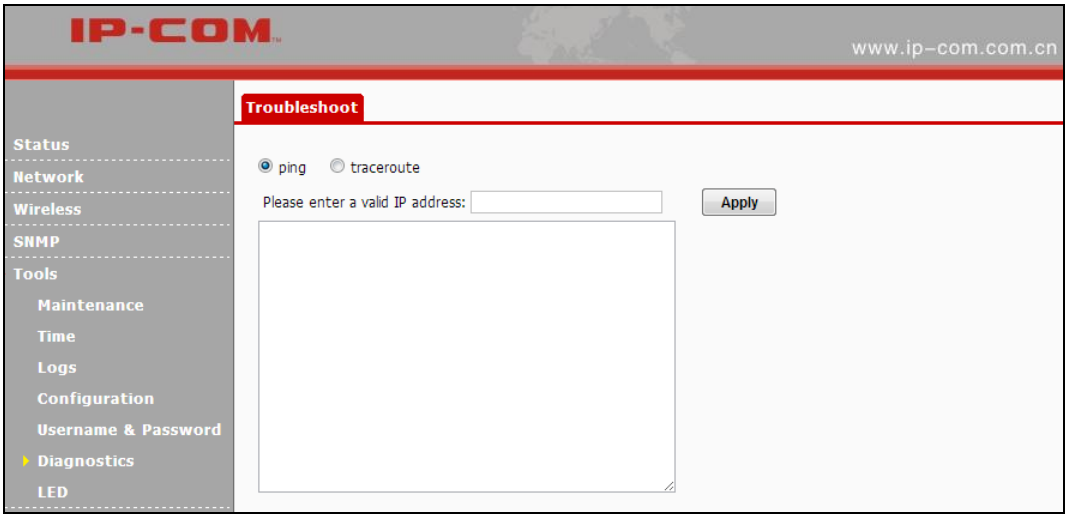
## 3.7.5 User Name & Password

Here you can change the user name and password for web login. The default username and password is admin/admin. We suggest that you change this password to a more secure password.



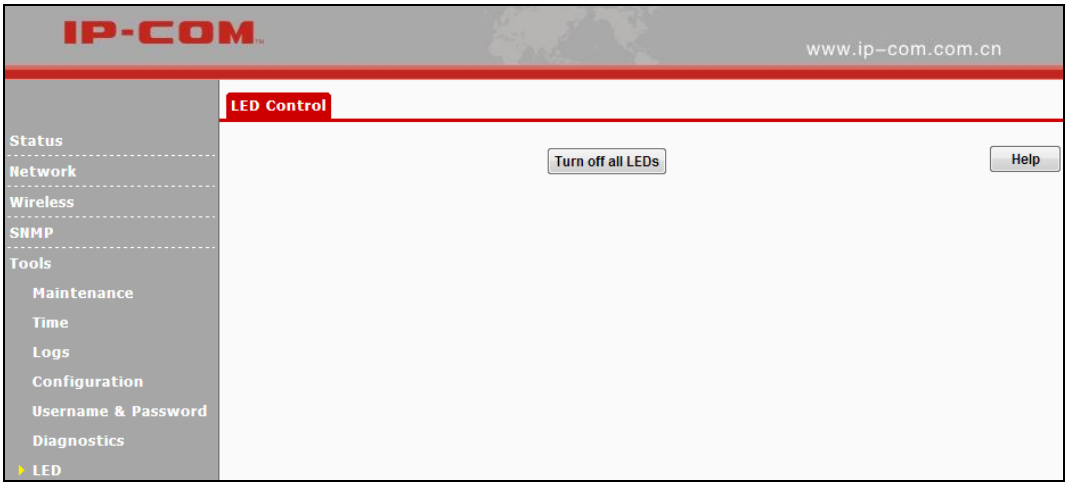

## 3.7.6 Diagnostics

You can choose Ping or traceroute to test your network connection.




## 3.7.7 LED

This section allows you to modify LED status.



# Appendix 1 Glossary

**Channel**

A communication channel, also known as channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. It is used to transfer an information signal, such as a digital bit stream, from one or more transmitters to one or more receivers. If there is only one AP in the range, select any channel you like. The default is **Auto**.

If there are several APs coexisting in the same area, it is advisable that you select a different channel for each AP to operate on, minimizing the interference between neighboring APs. For example, if 3 American- standard APs coexist in one area, you can set their channels respectively to 1, 6 and 11 to avoid mutual interference.

**SSID**

Service set identifier (SSID) is used to identify a particular 802.11 wireless LAN. It is the name of a specific wireless network. To let your wireless network adapter roam among different APs, you must set all APs' SSID to the same name.

**WEP**

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.

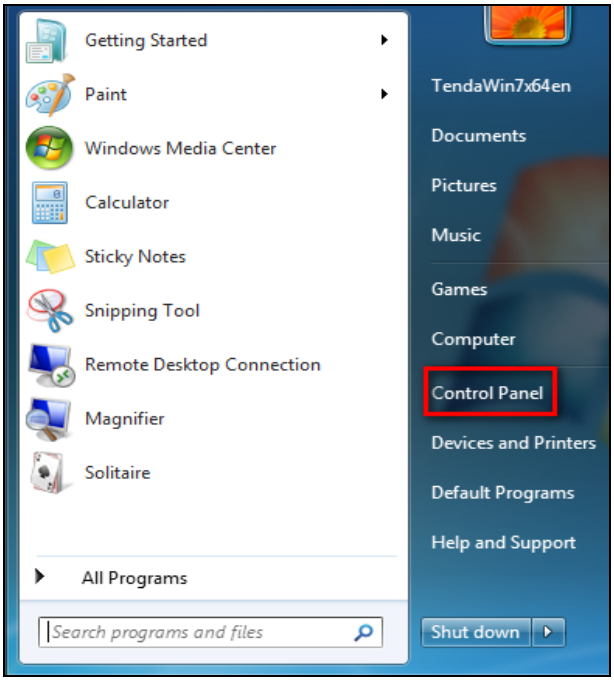
**WPA/WPA2**

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network. The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA. Currently, WPA is supported by Windows XP SP1.

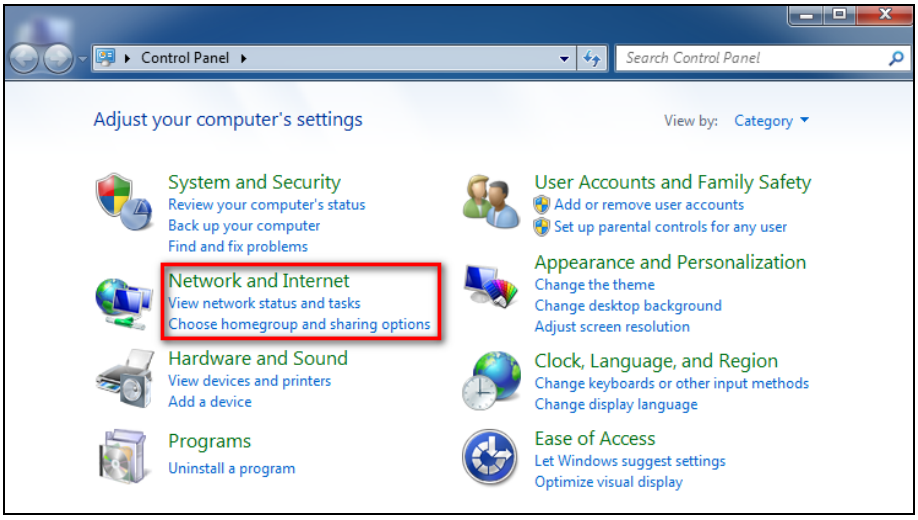
# Appendix 2 Configure PC

**WIN7 OS Configuration**

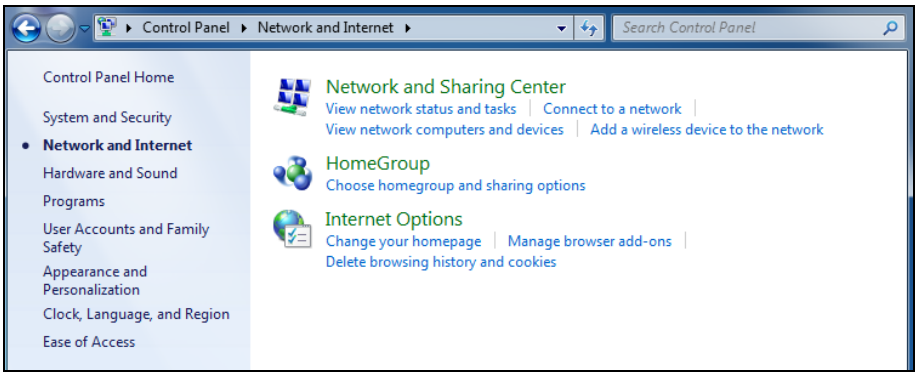
1. Click **Start > Control Panel**;



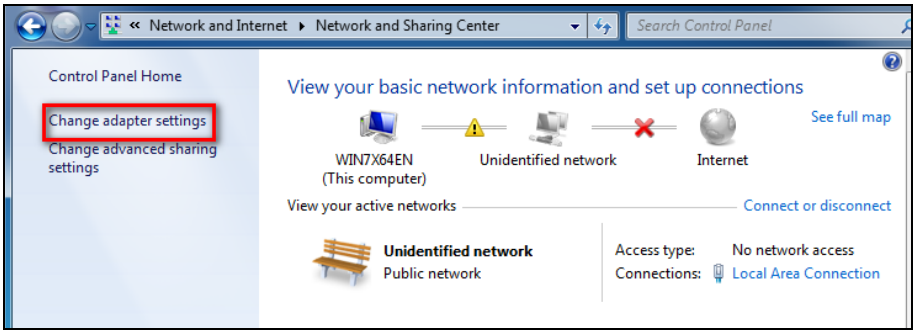

2. Enter **Control Panel** and click **Network and Internet**;



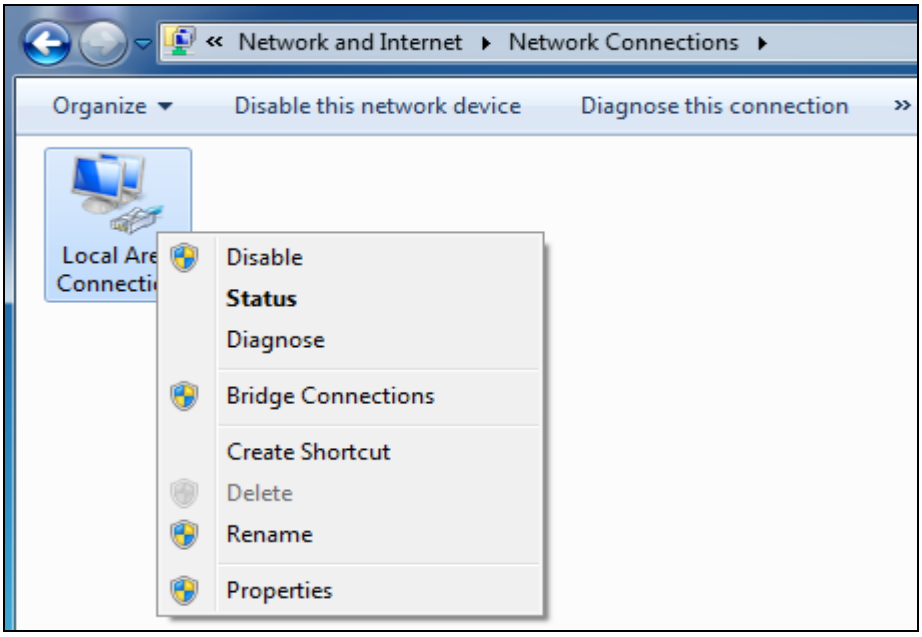

3. Click **Network and Sharing Center**;



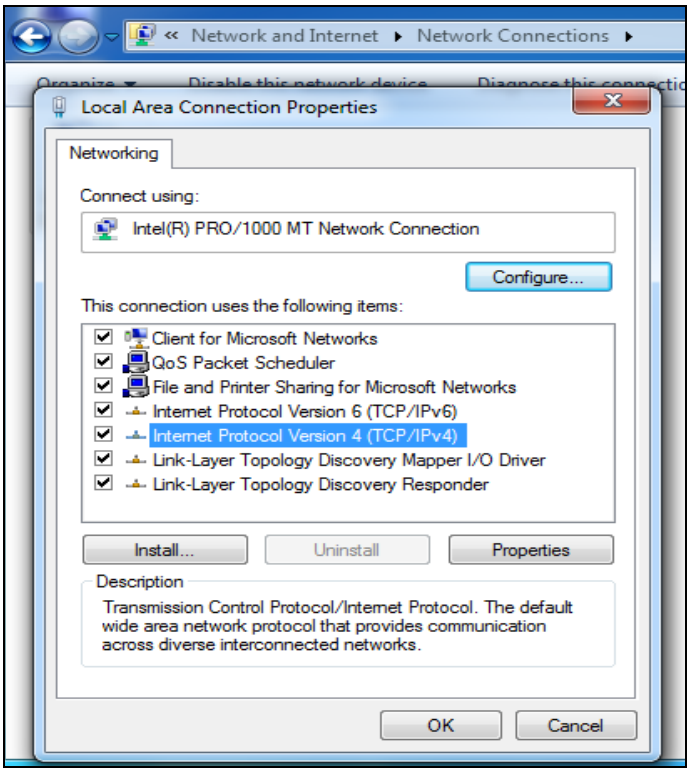
4. Click **Change adapter settings**;



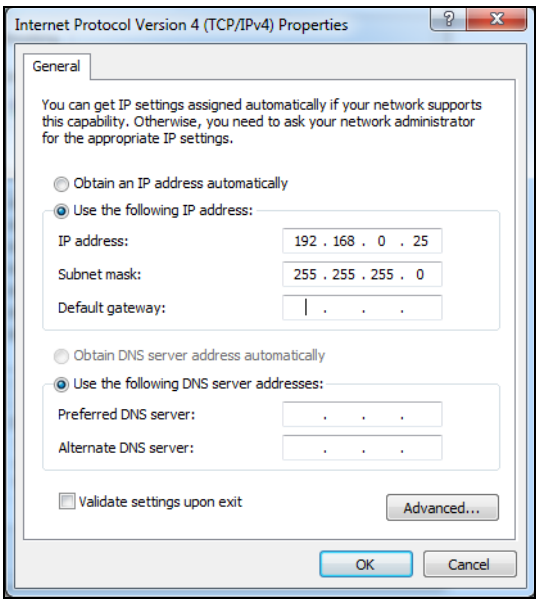

5. Right click **Local Area Connection** and select **Properties**;




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



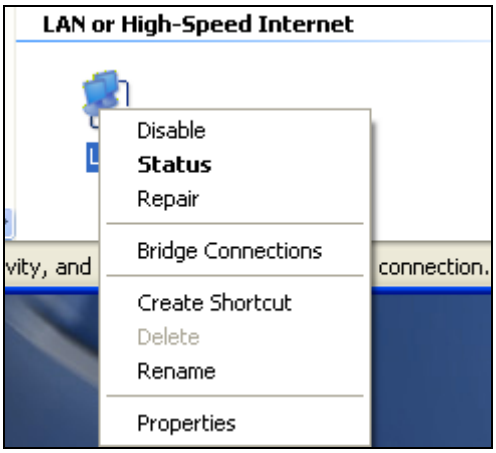
7. Select **Use the following IP address**, enter 192.168.0.X (where x can be any number between 1~253) in the IP address bar and 255.255.255.0 in the subnet mask and then click **OK** to save the configurations.



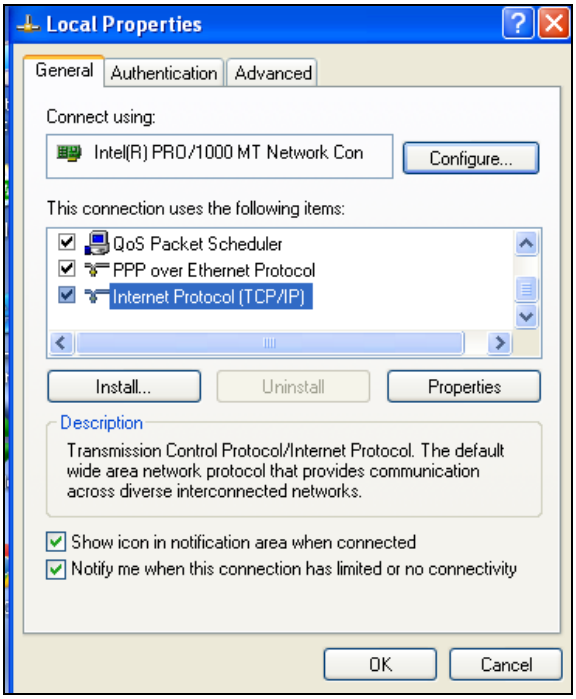

**Windows XP OS Configuration**

1. Right click **My Network Places** and select **Properties;**

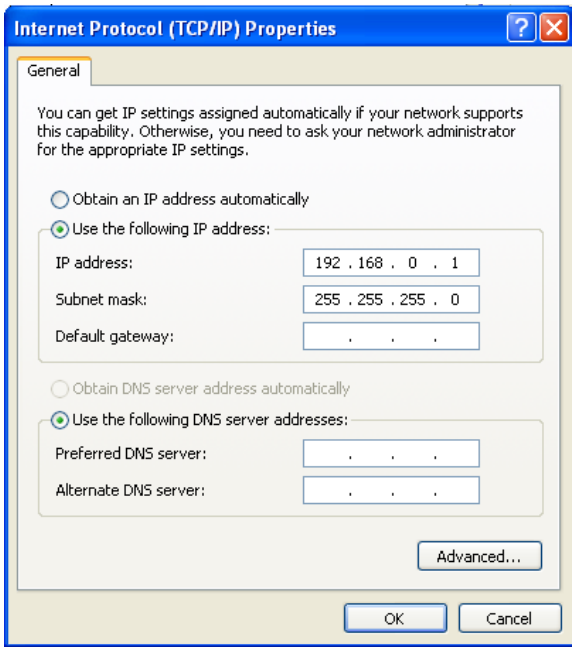

2. Right click **Local** and select **Properties**;



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




4. Select **Use the following IP address**, enter 192.168.0.X (where x can be any number between 1~253) in the IP address bar and 255.255.255.0 in the subnet mask and then click **OK** to save the configurations.



# Appendix 3 Safety and Emission Statement

**CE Mark Warning**

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

**FCC Statement**

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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.

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 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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.