

# WR1201

## 1200M Wireless Router

### User Guide





---

## FCC STATEMENT

**Warning:** Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**Note:** 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 RF Radiation Exposure Statement:

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
- 2) this device must accept any interference received, including interference that may cause undesired operation.

"FCC RF Radiation Exposure Statement Caution: To maintain compliance with the FCC's RF exposure guidelines, place the product at least 20cm from nearby persons."



---

## FCC ID : 2AHVHWR1201

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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

## CE Mark Warning

**CE0359**

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. This device complies with EU 1999/5/EC.

### 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 recom

## DECLARATION OF CONFORMITY

Hereby, [**Shenzhen MTC Co., LTD**], declares that this [**1200M Wireless Router**] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The declaration of conformity may be consult at

Import / manufacture Name:

Import / manufacture Address:

## ADAPTER INFORMATION

MOSO SWITCHING ADAPTER

Model:MSP-C15001C12.0-18A-US

Input:100~240V 50/60Hz 0.6A Max.

Output:DC 12V-1.5A

---

## Important Safety Instructions

1. Don't disassemble the product, or make repairs yourself. If you need service, please contact us.
2. Do not operate this product near water.
3. Do not place or operate this product near a radiator or a heat register.
4. Do not expose this product to dampness, dust or corrosive liquids.
5. Do not connect this product or disconnect it from a socket during a lightning or a thunderstorm.
6. Do not block the ventilation slots of this product, for insufficient airflow may harm it.
7. When plugging this product into a socket, make sure that the electrical socket is not damaged, and that there is no gas leakage.
8. Place the connecting cables properly so that people won't stumble or walk on it.
9. This product should be operated from the type of power indicated on the marking label. If you are not sure of the type of power available, consult the qualified technician.
10. Unplug this product from the mains and refer the product to qualified service personnel for the following conditions:

If liquid has been spilled on the product

If the product has been exposed to rain or water

11. The Operating temperature is 0°C~40°C(32°F~104°F). The Storage temperature is -40°C~70°C (-40°F~158°F).

---

## CONTENTS

Important Safety Instructions.....	4
Chapter 1 Product Overview .....	8
1.1 Introduction .....	8
1.2 LED Indicator .....	8
1.3 Physical Interfaces.....	9
Chapter 2 Connecting Mechanism.....	10
2.1 Preparation.....	10
2.2 Hardware Connection .....	11
2.3 Configure PC TCP/IP Settings.....	11
Chapter 3 Log in to the Router.....	15
3.1 Log in.....	15
3.2 Web Page.....	16
3.3 Web page Introduce to Layouts.....	17
3.4Commonly used Web page elements Introductions.....	18
Chapter 4 Features & Configurations.....	19
4.1 System Status .....	19
4.1.1 System Status.....	19
4.1.2 WAN Status .....	20
4.1.3 LAN Status.....	21
4.1.4 Wireless Status .....	21
4.2 Network Settings.....	23
4.2.1 LAN Setting.....	23
4.2.2 WAN Setting .....	24
4.2.3 MAC Address Clone .....	27
4.3 WLAN Settings.....	29
4.3.1 Basic Settings .....	29

---

4.3.2 Security Settings.....	31
4.3.3 Advanced Settings.....	34
4.3.4 WPS Settings.....	35
4.3.5 Access Control.....	36
4.3.6 Connection Status .....	38
4.4 USB Setting.....	38
4.4.1 Device Sharing .....	38
4.4.2 Media Server.....	39
4.4.3 Print Server .....	40
4.4.4 User Accounts.....	40
4.5 IPTV Settings .....	41
4.6 DHCP Server.....	41
4.6.1 DHCP Server.....	41
4.6.2 DHCP List & Binding.....	43
4.7 Virtual Server.....	44
4.7.1 Port Range.....	45
4.7.2 DMZ Settings .....	46
4.7.3 uPnP Settings .....	47
4.8 Security Settings .....	48
4.4.1 Client Filter.....	48
4.4.2 URL Filter.....	50
4.4.3 MAC Filter.....	51
4.4.4 Prevent.....	52
4.4.5 Remote WEB .....	52
4.4.6 WAN Ping.....	54
4.9 Routing Settings.....	55
4.10 Traffic Control .....	55
4.11 System Tools .....	57
4.11.1 Time Settings .....	57



---

4.11.2 DDNS .....	58
4.11.3 Backup & Restore .....	59
4.11.4 Firmware Update .....	60
4.11.5 Restore to Factory .....	61
4.11.6 Reboot.....	62
4.11.7 Change Password.....	63
4.11.8 System Logs .....	63
Appendix.....	65
1 Configure PC TCP/IP Settings.....	65
Windows 7 .....	65
Windows XP.....	71
2 FAQs .....	75
3 Factory Default Settings.....	76

---

## Chapter 1 Product Overview

### 1.1 Introduction

WR1201 1200M Wireless Router supports simultaneous 2.4GHz and 5GHz connections for 1200Mbps of total available bandwidth, supports for DHCP, PPPOE, static IP three modes to Internet. You can set up wireless password and Internet filler function. The router also support for USB function, you can save data in USB disk or read data from it.

- Complies with IEEE 802.11a/an/ac and 802.11b/g/n.
- Provide one USB3.0 port supporting file sharing and print server.
- Provide internally installed TF card function.
- Provide WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Support access control.
- Support firmware upgrade.
- Support Client Filer, MAC Filer, URL Filer.
- Support remote web management
- Support DDNS, port forwarding, DMZ Host, UPNP.
- Use built-in antenna.

### 1.2 LED Indicator

The LED indicator displays information about the device's status.

LEDs	Names	Status	Indications
	System LED	Blinking	The router is booting or upgrading.
		Solid	The router has booted.
		Off	Power is off or the router is not booted.
2.4G	2.4G LED	Blinking	2.4G wireless is on and have data transferred.

		Off	2.4G wireless is disabled.
5.0G	5G LED	Blinking	The 5G wireless is on and have data transferred.
		Off	The 5G wireless is disabled.
	Internet LED	Solid	The Internet port is connected but inaccessible.
		Blinking	The Internet port is connected and accessible.
		Off	The Internet port isn't connected.
	Ethernet LED	Off	There is device(s) connected to the Ethernet (1/2/3/4) port(s).
		Blinking	No any device is connected to the Ethernet (1/2/3/4) port.
	WPS LED	Blinking	WPS button on the router is pressed, and the router is trying to connect a wireless device to its network via WPS.
		Solid	The connection via WPS is successful.
		Off	The connection via WPS fails.
	USB LED	Off	No device is connected to the USB port.
		Solid	The device is connected to the USB port.

### 1.3 Physical Interfaces

There are physical interfaces on this router

Item	Description
Supply hub	A Supply hub connected to power socket with power adapter (output 12V, 1.5A).
WAN Port	A port connected Internet with reticle.
LAN Port	Ports (1, 2, 3, 4) connected your computer.
WPS/RST Button	Press the button to connect another router through the WPS Press the button more than 10 seconds, the device will restore to its factory default.
USB Port	The USB port connects to a USB storage device or a USB printer.

## Chapter 2 Connecting Mechanism

### 2.1 Preparation

Before you start the installation process, you need to prepare the following:

Item	Description
Router	Find it in your package.
Power adapter	Find it in your package.
PC	Should have a installed IE8 or higher browser.
Gather ISP Information	<p>DHCP, PPPOE or Static IP Internet Connection Type:</p> <ol style="list-style-type: none"><li>1. Ethernet Cable from the incoming Internet side: This is provided by your ISP</li><li>2. ISP Information: Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it</li></ol> <p>If your ISP uses a PPPOE Internet connection, you will need ISP login name and password</p> <ul style="list-style-type: none"><li>● If you use a DHCP Internet connection, no information is needed</li><li>● If your ISP gives you a fixed or static IP address for Internet connection, you will need to gather the following information:</li></ul> <ol style="list-style-type: none"><li>1) IP Address</li><li>2) Subnet Mask</li><li>3) Gateway</li><li>4) DNS Server</li><li>5) Alternate DNS Server (Optional)</li></ol>
	<p>WISP Internet Access:</p> <ol style="list-style-type: none"><li>1. Remote AP's SSID, MAC address, security mode, cipher type and security key</li><li>2. Internet connection information provided by the remote AP</li><li>3. Ethernet Cable: This can be found in the product package. You will need it</li></ol>



to connect your PC to this device

## 2.2 Hardware Connection



### Note

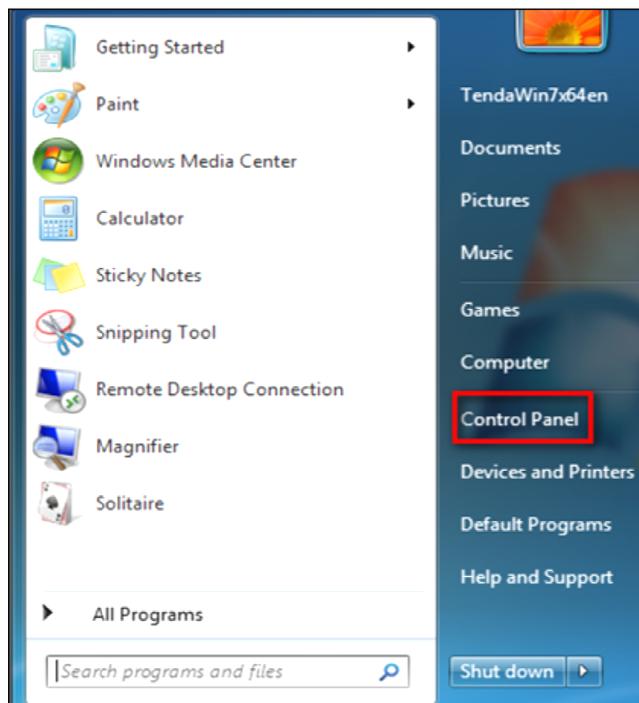
Before connecting, please make sure that you can surf the internet in your computer to use the reticle provided by ISP.

- 
- ① Please connect reticle what you ever connected to the computer with the router's WAN port.
  - ② Use another reticle to connect your computer Ethernet port with the router's any LAN port.
  - ③ Connect the router's power adapter. And the hardware connection is finished.
- 

## 2.3 Configure PC TCP/IP Settings

Before you log in to the router, please make sure your computer set to "Obtain an IP address automatically" and "Obtain DNS server address automatically" from the device.

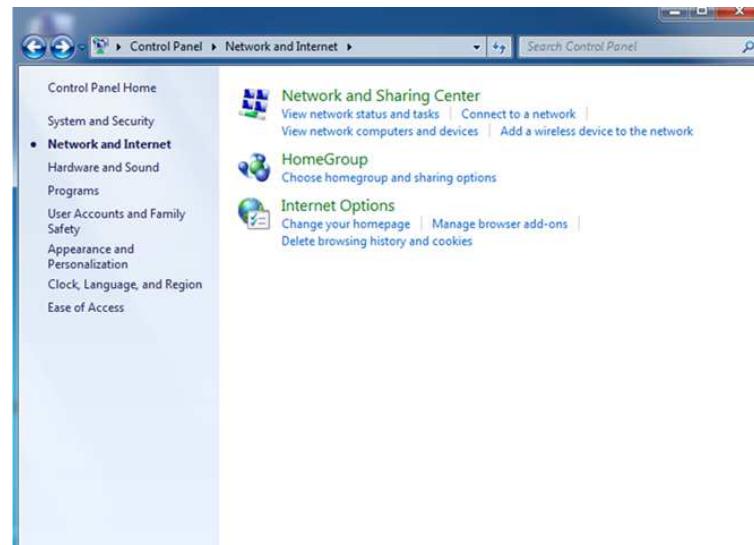
- ① Click **Start -> Control Panel**.



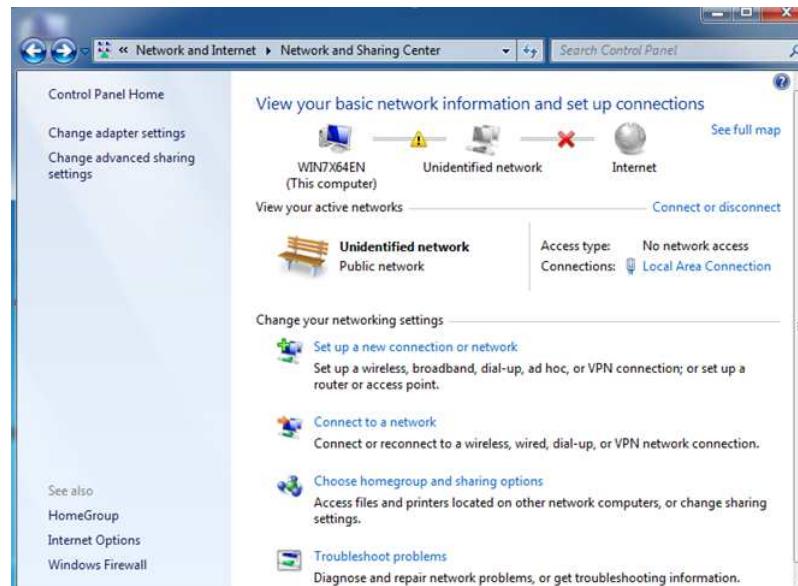
**② Click Network and Internet.**



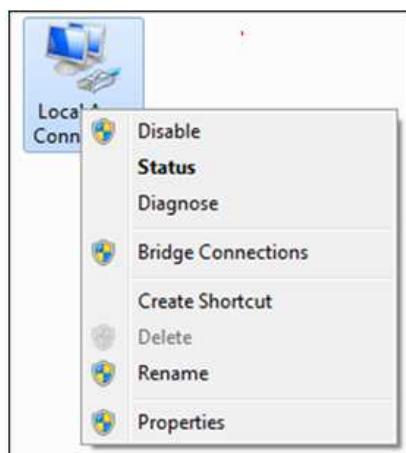
**③ Click Network and Sharing Center.**



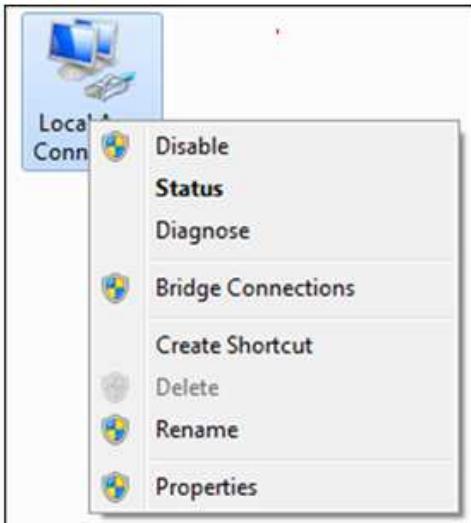
④ Click **Change adapter settings**.



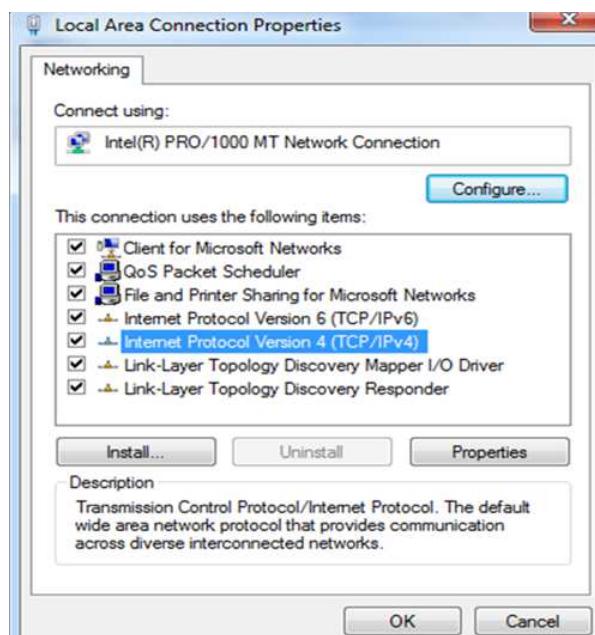
⑤ Click **Local Area Connection** and select **Properties**.



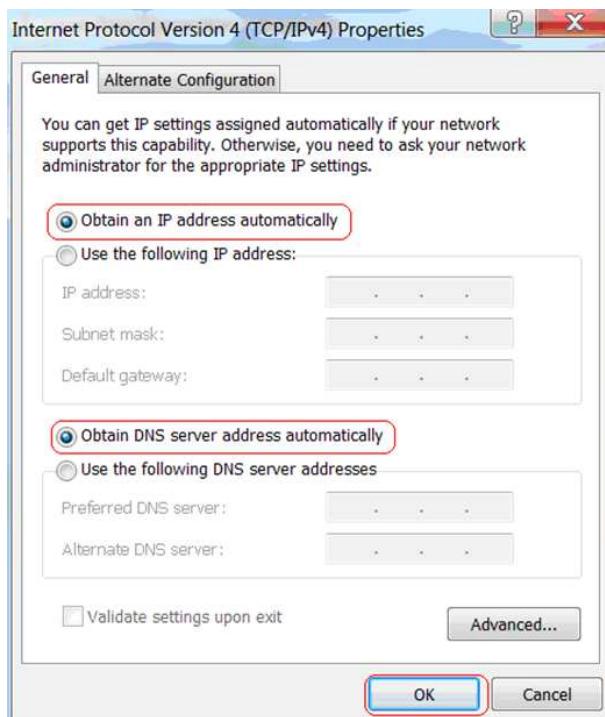
⑥ Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



- ⑦ Select Obtain an IP address automatically and click OK



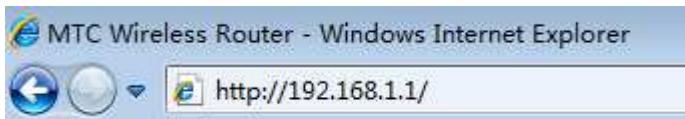
- ⑧ Click OK on the Local Area Connection Properties window to save your settings



## Chapter 3 Log in to the Router

### 3.1 Log in

To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter <http://192.168.1.1> in your browser's address bar. Press "Enter".



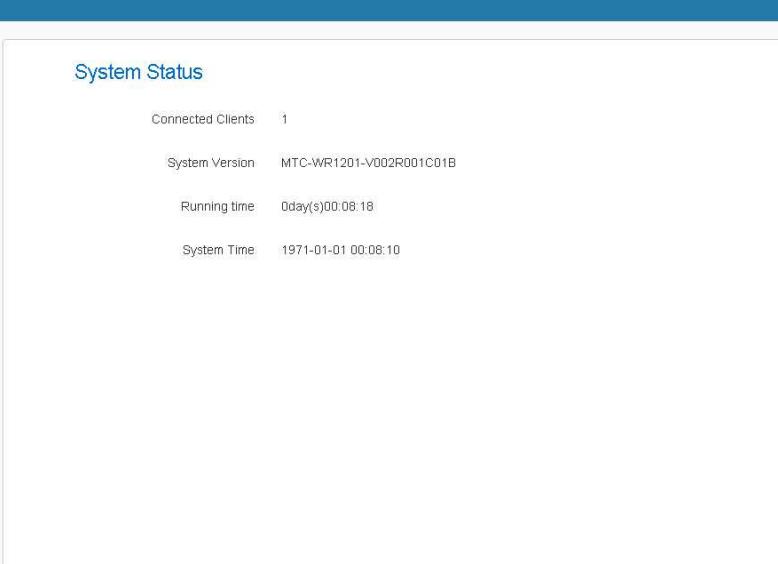
The system will automatically display the login page, please enter the correct password (default password is admin). Click the "Sign in" button or press "Enter".



The image shows a sign-in page with a blue header containing the AMTC logo. The main content area has a white background with a light gray border. It features a title "Please sign in" at the top, followed by a dropdown menu set to "English". Below it is a text input field with a lock icon and the placeholder "admin". At the bottom is a large blue "Sign in" button.

## 3.2 Web Page

After clicking the “Sign in” ,the system will display the router Web page. You can view and modify settings here



The image shows the router's web interface. The left sidebar has a blue header and contains a vertical list of navigation items: System Status, WAN Status, LAN Status, Wireless Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, and System Tools. The main content area has a white background and displays the "System Status" section. It includes five data rows: "Connected Clients" (1), "System Version" (MTC-WR1201-V002R001C01B), "Running time" (0day(s)00:08:18), "System Time" (1971-01-01 00:08:10), and a "Help" section. The "Help" section defines "Running time" as the total time the router is turned on and "System Version" as the firmware version.

System Status	
Connected Clients	1
System Version	MTC-WR1201-V002R001C01B
Running time	0day(s)00:08:18
System Time	1971-01-01 00:08:10

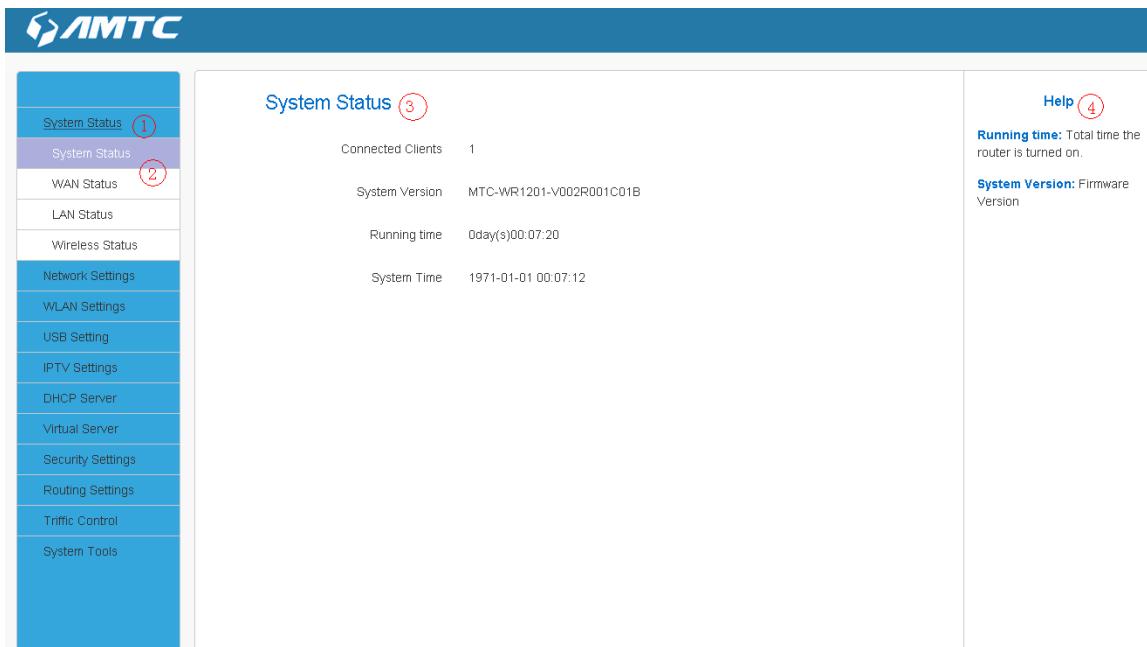
**Help**

**Running time:** Total time the router is turned on.

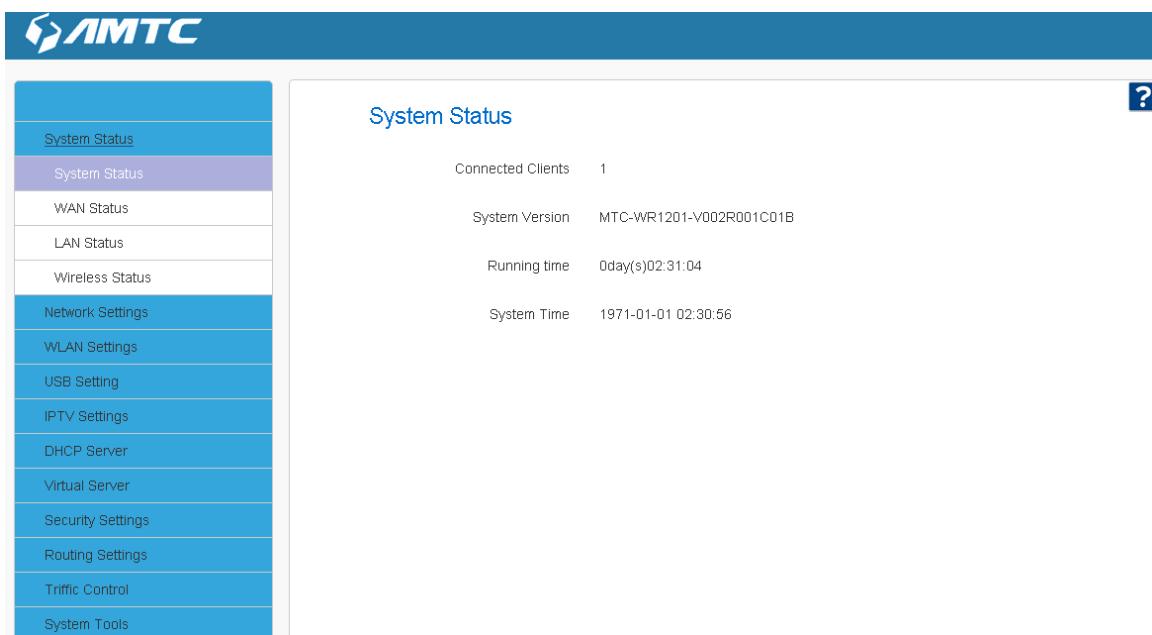
**System Version:** Firmware Version

### 3.3 Web page Introduce to Layouts

The Web page consist of Primary & secondary navigation, configuration area and help information area.



NO	Name	Introductions
①	Primary navigation	The navigation bar organize function menu of Web page in the form of a navigation tree. The user can easily select function menu in the navigation bar. The results will display in the configuration area.
②	secondary navigation	
③	configuration area	The user can configure and view settings here.
④	help information area	Show help information of the current page.



System Status

Connected Clients 1

System Version MTC-WR1201-V002R001C01B

Running time 0day(s)02:31:04

System Time 1971-01-01 02:30:56

**Note**

Change the resolution of the screen the help information may become “?” as above shown, if you want to refer the help information please click the symbol.

### 3.4 Commonly used Web page elements Introductions

Common elements	Introductions
Release	To release the WAN IP address information.
Renew	To obtain the WAN IP address information again.
Save	To save the current configuration page.
Cancel	To cancel the current configuration page.
Add	To add settings to the list
Delete	To delete the corresponding rules.
Refresh	To refresh the current page display content.



## Chapter 4 Features & Configurations

### 4.1 System Status

Click “**System Status**”, enter the system status web page, in this page you can see the “**SystemStatus**”, “**WAN Status**”, “**LAN Status**”, “**Wireless Status**”.

#### 4.1.1 System Status

This page displays Connected Clients, System Version, Running Time, System Time.

The screenshot shows the 'System Status' page. On the left is a vertical navigation menu with the following items:

- System Status
- System Status (selected)
- WAN Status
- LAN Status
- Wireless Status
- Network Settings
- WLAN Settings
- USB Setting
- IPTV Settings
- DHCP Server
- Virtual Server
- Security Settings
- Routing Settings
- Traffic Control
- System Tools

The main content area is titled 'System Status' and contains the following information:

Connected Clients	1
System Version	MTC-WR1201-V002R001C01B
Running time	0day(s)02:35:10
System Time	1971-01-01 02:35:02

On the right side, there is a 'Help' section with two entries:

- Running time:** Total time the router is turned on.
- System Version:** Firmware Version

#### Parameters Specification:

- **Connection Clients:** displays the number of DHCP clients.
- **System Version:** Firmware Version.
- **Running Time:** Displays the time duration indicating how long the router has been up since startup. Up time is recounted and renewed upon poweroff.
- **System Time:** Current system time on this device. The device automatically synchronizes the system time with Internet time servers.



#### Tips

- Running time is total time the router is turned on



## 4.1.2 WAN Status

The screenshot shows the 'Network Status' section of the router's configuration interface. On the left, a sidebar lists various settings: System Status, WAN Status (selected), LAN Status, Wireless Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, and System Tools. The main content area displays the following information:

Parameter	Value
Connection Type	Static IP
Connection Status	Connected
WAN MAC Address	BC:88:2B:B0:02:5E
WAN IP	172.16.87.170
Subnet Mask	255.255.255.0
Gateway	172.16.87.254
Primary DNS Server	172.16.9.3
Secondary DNS Server	
Connection Duration	0day(s)02:37:14

On the right side, there is a 'Help' section with three entries:

- Connection Type:** Displays the current access mode of WAN port.
- Connection Duration:** Access method for dynamic IP or PPPoE server and router and ISP connection is properly timed.
- WAN MAC Address:** MAC address of your ISP's router to see.

### Parameters Specification:

- **Connection Type:** It displays the current access mode of WAN port.
- **Connection Status:** The network connection status.
- **WAN MAC Address:** MAC address of your ISP's router to see.
- **WAN IP:** IP address obtained from ISP.
- **Subnet Mask:** Obtained from ISP.
- **Gateway:** Obtained from ISP.
- **Primary DNS Server:** Obtained from ISP.
- **Secondary DNS Server:** Obtained from ISP.
- **Connection Duration:** Access method for dynamic IP or PPPoE server and router and ISP connection is properly timed.



### Tips

**WAN IP/Subnet Mask/Gateway/Primary DNS Server/Secondary DNS Server:** This type of information appears only if the router successfully connects to Internet via a PPPoE or DHCP (dynamic IP) connection. However if you connect the router to Internet with static IP settings provided by your ISP, these fields will display the settings you entered whether the router successfully connects to the Internet or not.

If nothing appears in the secondary DNS server field, there is no available secondary DNS server



### 4.1.3 LAN Status

LAN Status	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
LAN MAC Address	8C:88:2B:B0:02:5D

**Help**  
**DHCP Server:** If the router as a DHCP server, here shown as enabled. Otherwise disabled.

#### Parameters Specification:

- **IP Address:** The Router's LAN IP Address (not your PC's IP address).
- **Subnet Mask:** The Router's LAN subnet mask.
- **DHCP Server:** the status of DHCP server.
- **LAN MAC Address:** The router's [physical address](#).



#### Tips

- The default IP address is 192.168.1.1.
- The default Subnet mask value is 255.255.255.0
- If the router as a DHCP server, here shown as enabled. Otherwise disabled

### 4.1.4 Wireless Status

This page shows the information of 2.4G Wireless and 5G Wireless.



AMTC

System Status	SSID Name	MTC_B0025C
WAN Status	BSSID	8C:88:2B:B0:02:5C
LAN Status	Channel	6
Wireless Status	Security Mode	Mixed WPA/WPA2 - Personal
Network Settings	SSID Name	MTC_B0025F_5G
WLAN Settings	BSSID	8C:88:2B:B0:02:5F
USB Setting	Channel	149
IPTV Settings	Security Mode	Mixed WPA/WPA2 - Personal
DHCP Server		
Virtual Server		
Security Settings		
Routing Settings		
Traffic Control		
System Tools		

### Parameters Specification:

- **SSID Name:** The name of Wireless.
- **BSSID:** The MAC Address of Wireless.
- **Channel:** The Channel of Wireless.
- **Security Mode:** Encryption schemes.



### Tips

- The default SSID of 2.4G is **MTC\_XXXXXX**, and SSID of 5G is **MTC\_XXXXXX\_5G**, where XXXXXX is the last six characters in the device's MAC address. You can find it on the label attached on the bottom of the device.
- **Default channel is AutoSelect.**



### Knowledge Expansion

- **AutoSelect:** Under the "AutoSelect" the wireless signal will choice the user number is the least channel to improve the efficiency of the signal, it works for most cases.
- If you choice other mode, the channel will not change all the time not matter the channel is good or bad.



## 4.2 Network Settings

To Click “**Network Settings**” enter the Network setup web page, in this page you can set “**LAN Settings**”, “**WAN Settings**”, “**MAC Address Clone**”.

### 4.2.1 LAN Setting

This page is to configure the basic parameters for LAN ports. This IP address is to be used to access the device’s settings through a web browser. Be sure to make a note of any changes you apply to this page

#### Set Steps:

- ① Click “**Network Settings**”.
- ② Select“**LAN Settings**”.
- ③ Enter **IP Address**, **Subnet Mask**.
- ④ Click “**Save**” and wait for the router reboot automatically.

**LAN Settings**

MAC Address: BC:88:2B:B0:02:5D

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

**Help**

This is to configure the basic parameters for LAN ports.

**MAC Address:** The device's MAC address as seen on your local network.

**IP Address:** The device's IP address as seen on your local network(192.168.1.1 by default).

**Subnet Mask:** It is shown the device's subnet mask here (255.255.255.0 by default.)

#### Parameters Specification:

- **MAC Address:** It displays the Router’s LAN MAC address.
- **IP Address:** It displays the Router’s LAN IP address.
- **Subnet Mask:** it displays the Router’s LAN subnet mask.



#### Tips

1. Default IP address and subnet mask are respectively 192.168.1.1 and 255.255.255.0.

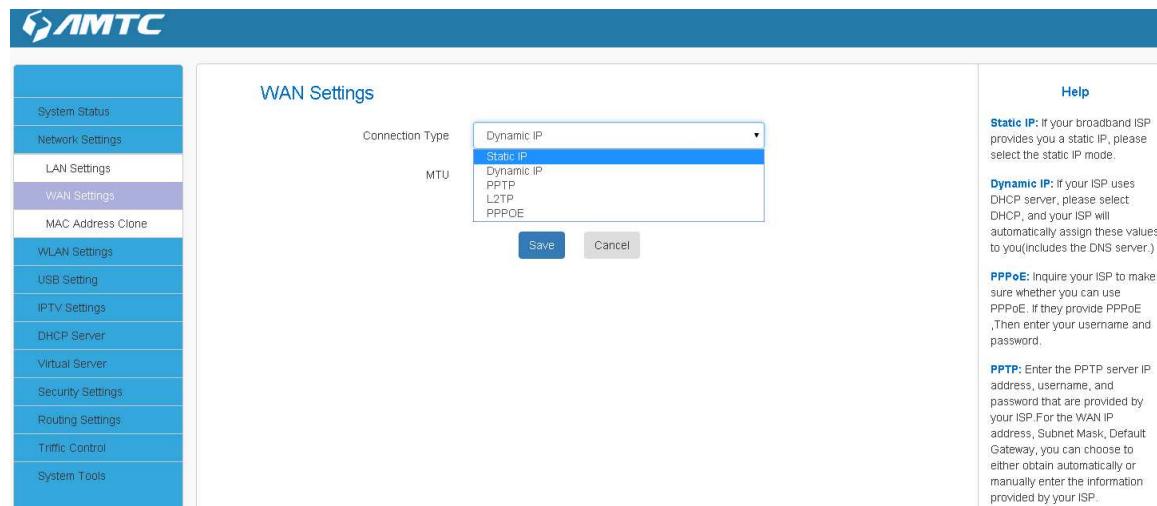
2. Be sure to make a note of any changes you apply to this page. If you change the LAN IP address of the router, you have to open a new connection to the new IP address and log in again. Also, you have to set the default gateway addresses of all LAN PCs to this new IP address.
3. The router's LAN IP address and WAN IP address cannot be on the same IP segment. If not, the router will not be able to access Internet.

#### 4.2.2 WAN Setting

Plug Internet cable to WR1201 WAN port.

##### Set Steps:

- ① Enter the web and Select“Network Settings”.
- ② Click the“WAN Settings”.



##### Parameters Specification:

➤ **Connection Type:**It displays the routers mode.

##### 1、Configuration the Internet access

Support Static IP mode、Dynamic IP(DHCP)、PPOE.

WAN Connection Type	Instruction
Static IP mode	If your ISP provides you with an Ethernet cable from the incoming Internet side IP information (IP address, subnet mask, gateway IP address, DNS server address), your ISP



	uses a static IP connection.
Dynamic IP	If your ISP provides you with an Ethernet cable from the incoming Internet side but no ISP login account or IP information, your ISP uses a DHCP connection.
PPOE	If your ISP provides you with an Ethernet cable from the incoming Internet side and ISP login account, your ISP uses a PPOE connection.

### 1.1> Static IP mode

#### Set Steps:

- ① Click “Network Settings”.
- ② Select “WAN Settings”.
- ③ Select Connection Type “Static IP”.
- ④ Enter IP, Subnet Mask, Gateway, MTU, DNS
- ⑤ Click “Save” to confirm.

The screenshot shows the 'WAN Settings' configuration page. The left sidebar has a blue header and lists various network settings. The 'WAN Settings' option is highlighted in purple. The main area is titled 'WAN Settings'. It contains fields for Connection Type (set to 'Static IP'), IP Address, Subnet Mask, Gateway, Primary DNS Server, Secondary DNS Server, and MTU. Below these fields are 'Save' and 'Cancel' buttons. To the right of the form is a 'Help' section with detailed explanations for each connection type: Static IP, Dynamic IP, PPPoE, and PPTP.

#### Parameters Specification:

- **Connection Type:** Select Static IP.
- **IP Address/Subnet Mask/WAN subnet mask/Gateway/Primary DNS Server/Secondary DNS Server:** Enter the ISP information you gathered in Getting Prepared.
- Click **Save** to save your settings.



#### Tips

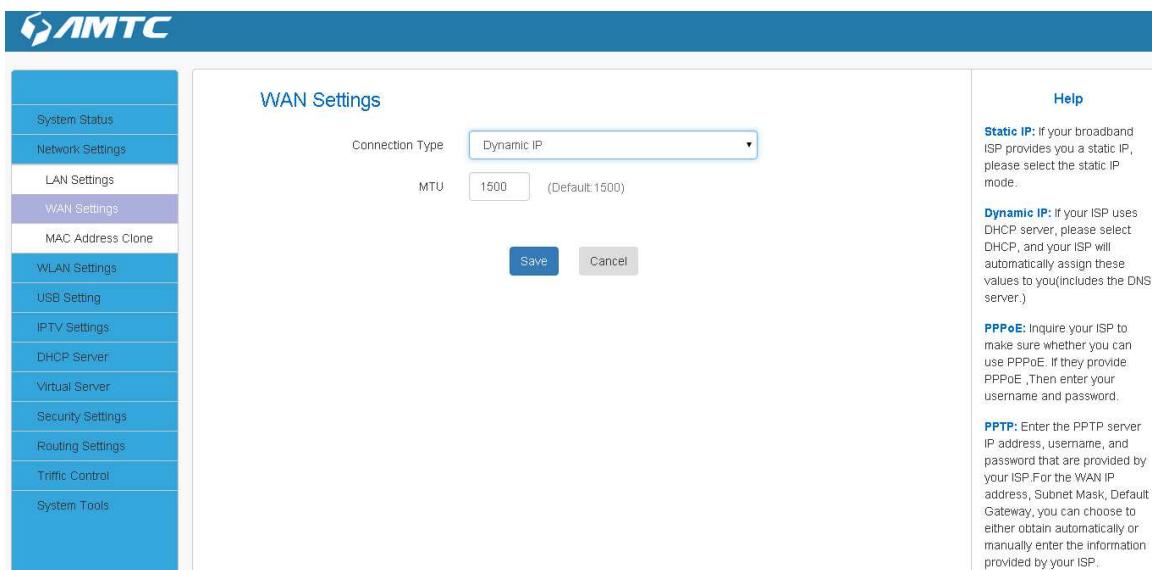


- MTU better to choose the default values.
- 

## 1.2>Dynamic IP mode.

### Set Steps:

- ① Click “**Network Settings**”.
- ② Select“**WAN Settings**”.
- ③ Select Connection Type “**Dynamic IP**”.
- ④ Click“**Save**” to confirm.



### Tips

---

- MTU better to choose the default values.
- 

## 1.3>PPOE

### Set Steps:

- ① Click “**Network Settings**”.
- ② Select “**WAN Settings**”.
- ③ Select Connection Type “**PPOE**”.
- ④ Enter the ISP login **UserName**, the ISP login **Password**.
- ⑤ Click“**Save**” to confirm.
- ⑥ Click “System Status”--->“WAN Status” to confirm



### Knowledge Expansion

- **MTU:** Maximum Transmission Unit. It is the size of the largest data packet that can be sent over the network. The default value is 1500.

The common MTU sizes and applications are listed in the table below.

MTU	Application
1500	Typical for connections that do not use PPPoE or VPN.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1436	Used in PPTP environments or with VPN.



### Note

- A wrong/improper MTU value may cause Internet communication problems. For example, you may be unable to access certain websites, frames within websites, secure login pages, or FTP or POP servers.
- Do not modify it unless necessary, but if a specific website or web application software cannot open or be enabled, you can try to change the MTU value to 1500, 1400.

### 4.2.3 MAC Address Clone



Some ISPs (Internet Service Providers) require end-user's MAC address to access their network. This feature copies your current PC's MAC address to the router.

### Set Steps:

- ① Click “**Network Settings**”.
- ② Click “**MAC Address Clone**”.
- ③ You can set this page from three methods:

#### 1、To Restore to Factory Default MAC

- 1> Click “Restore to factory Default MAC”
- 2> Click **Save** to save your settings.

#### 2、To clone the MAC address of the computer that you are now using to the router:

- 1> Click **Clone My PC's MAC Address**.
- 2> Click **Save** to save your settings.

#### 3、To manually enter the MAC address allowed by your ISP:

- 1> Enter the MAC address allowed by your ISP.
- 2> Click **Save** to save your settings.

The screenshot shows the 'MAC Address Clone' configuration page. The left sidebar menu is visible with 'MAC Address Clone' highlighted. The main form has a 'MAC Address' field set to '8C:88:2B:80:02:5E'. It includes two buttons: 'Restore to Factory Default MAC' and 'Clone MAC'. At the bottom are 'Save' and 'Cancel' buttons. To the right, a 'Help' section provides information about MAC address cloning and defines terms like 'MAC Address', 'Restore Default MAC', and 'Clone MAC'.

### Parameters Specification:

- **MAC Address:** The computer or broadband modem authorized by your ISP.



### Knowledge Expansion

1. **Restore toFactory Default MAC:** Reset the router's WAN MAC to factory default.
2. **Clone MAC:** Clicking this button copies the MAC address of the computer that you are now

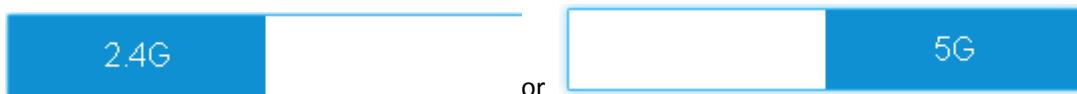
---

using to the router. Also, you can manually enter the MAC address that you want to use. You have to use the computer whose MAC address is allowed by your ISP

### 4.3 WLAN Settings

Click “**WLAN Settings**” enter the configure page , here you can configure “**Base Settings**”, “**Security Settings**”, “**Advanced Settings**”, “**WPS Settings**”, “**Access Control**”, “**Connection Status**”.

The Wireless includes two working frequency band: 2.4GHz and 5GHz. You coule change it by clicking button



#### Knowledge Center

2.4GHz and 5GHz is the router working frequency. They use different protocol: 2.4G use 802.11g and 5G use 802.11a. 2.4G band and household appliances are using the same frequency band. 5G band use few. So 5G has strong anti-jamming capability.

---

#### 4.3.1 Basic Settings

Here you can configure the basic wireless settings of the router

##### Set Steps:

- ① Click“**WLAN Settings**”.
- ② Select “**Basic Settings**”.
- ③ Wireless **Enable**.
- ④ Select Network Mode
- ⑤ Enter **SSID name** (Default name is **i3005\_XXXXXX**).
- ⑥ Select“**Channel**”.
- ⑦ Select “**Channel BandWidth**”.

### Parameters Specification:

- **Wireless:** wireless “Enable” or “Disable”.
- **SSID:** It is the unique name of the wireless network and can be modified.
- **Broadcast (SSID):** Select “Enable” to enable the router’ SSID to be scanned by wireless devices. The default is enabled. If you disable it, the wireless devices must know the SSID for communication.
- **BSSID:** This is the MAC address of the device's wireless interface.
- **Channel:** The currently used channel by the router. Select an effective channel of the wireless network. The default is AutoSelect.
- **Channel Bandwidth:** Select an appropriate channel bandwidth to enhance the wireless performance. Select 20/40M when the network has 11b/g/n to promote its throughput



#### Note

- The wireless Enable.
- The SSID must be entered.



#### Tips

1. The default SSID of 2.4G is **MTC\_XXXXXX**, and SSID of 5G is **MTC\_XXXXXX\_5G** , where XXXXXX is the last six characters in the device's MAC address. You can find it on the label

---

attached on the bottom of the device.

2. If you are not an advanced user, it is advisable to only change the SSID (name of the network) and channel and leave other items unchanged.
- 



### Knowledge Expansion

---

**Network Mode (802.11 Mode):** Select a correct mode according to your wireless clients.

- **11b:** This network mode delivers wireless speed up to 11Mbps and is only compatible with 11b wireless clients.
  - **11g:** This network mode delivers wireless speed up to 54Mbps and is only compatible with 11g wireless clients.
  - **11b/g mixed:** This network mode delivers wireless speed up to 54Mbps and is compatible with 11b/g wireless clients.
  - **11b/g/n mixed:** This network mode delivers wireless speed up to 300Mbps and is compatible with 11b/g/n wireless clients
- 

### 4.3.2 Security Settings

With the wireless security function, you can prevent others from connecting to your wireless network and using the network resources without your consent. Meanwhile, you can also block illegal users from intercepting or intruding your wireless network

#### Set Steps:

- ① Click “**Network Settings**”.
- ② Select “**Security Settings**”.
- ③ Select“**Security Mode**”.
- ④ Click “**Apply**” to use you settings and click “**Save**” to save your settings.



AMTC

System Status  
Network Settings  
WLAN Settings  
Basic Settings  
**Security Settings**  
Advanced Settings  
WPS Settings  
Access Control  
Connection Status  
USB Setting  
IPTV Settings  
DHCP Server  
Virtual Server  
Security Settings  
Routing Settings  
Traffic Control  
System Tools

Security Settings

Band Switch: 2.4G

SSID Name: MTC\_B0025C

Security Mode:

- Disable
- WPA - Personal
- WPA2 - Personal
- Mixed WPA/WPA2 - Personal

Help

**WPA/WPA2-Personal:** You can enable personal or mix mode, but you must make sure that the wireless client also supports the selected encryption method.

➤ **Security mode:**WPA – Personal、WPA2 – Personal、Mixed WPA/WPA2 – Personal.

Security mode	Instruction
Disable	Not open this function
WPA – Personal	Support AES and TKIP cipher types
WPA2 – Personal	Support AES, TKIP and TKIP+AES cipher types
Mixed WPA/WPA2 – Personal	Both WPA-Personal and WPA2-Personal secured wireless clients can join your wireless network.



**Note**

- **WPA/WPA2-Personal:** You can enable personal or mix mode, but you must make sure that the wireless client also supports the selected encryption method.

Security Settings

System Status
Network Settings
WLAN Settings
Basic Settings
Security Settings
Advanced Settings
WPS Settings
Access Control
Connection Status
USB Setting
IPTV Settings
DHCP Server
Virtual Server
Security Settings
Routing Settings
Traffic Control
System Tools

Band Switch: 2.4G

SSID Name: MTC\_B0025C

Security Mode: Mixed WPAWPA2 - Personal

WPA Algorithms:  AES  TKIP  TKIP&AES

Pass Phrase: 12345678

Key Renewal Interval: 3600 Second

Save Cancel

Help  
**WPAWPA2-Personal:** You can enable personal or mix mode, but you must make sure that the wireless client also supports the selected encryption method.

### Parameters Specification:

- **WPA Algorithms:** Wi-Fi Protected Access Algorithms.
- **Pass Phrase:** The default is 12345678.



### Knowledge Expansion

1. **WEP:** (Wired Equivalent Privacy) is the wireless transmission of data between two devices for encryption, to prevent illegal users wiretapping or invade the wireless network.
2. **AES:** (Advanced encryption standard) is an iterative, symmetric key group password. If selected, wireless speed can reach up to 300Mbps.
3. **TKIP:** (Temporal Key Integrity Protocol) Responsible for handling the wireless encryption part of security issues, TKIP is in WEP password outermost layer of the existing "shell". If selected, wireless speed can reach up to 54Mbps.
4. **TKIP+AES:** If Selected, both AES and TKIP secured wireless clients can join your wireless network.
5. **Key Renewal Interval:** Enter a valid time period for the key to be changed.



### Tips

- Recommended that you choice "WPA-Personal" + "AES" mode , make sure the wireless efficiency and ensure the security of wireless network. Meanwhile, avoid some kind of

---

wireless network card does not support security mode, cause cannot connect the wireless network.

---

### **Backup Configuration Procedures:**

- ① Configure security mode, cipher type and security key.
- ② Click **Save** to save your settings.



### **Knowledge Center**

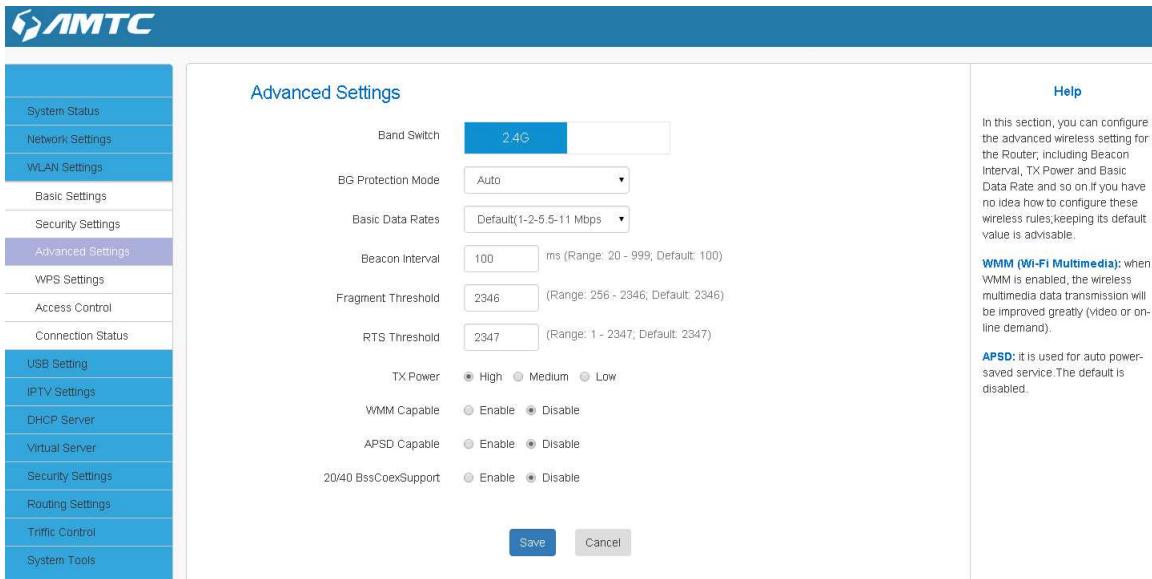
---

1. **WEP:** WEP is intended to provide data confidentiality comparable to that of a traditional wired network.
  2. **Open:** Wireless speed can reach up to 54Mbps if WEP - Open is selected.
  3. **Shared:** Wireless speed can reach up to 54Mbps if WEP - Shared is selected.
  4. **Mixed WEP:** Compatible with both Open and Shared. Clients can connect to your wireless network either using Open or Shared
  5. **Default Key:** Select a key to be effective for the current WEP encryption. For example, if you select Key 2, wireless clients must join your wireless network using this Key 2.
  6. **WPA-PSK:** WPA personal, support AES and TKIP cipher types.
  7. **WPA2-PSK:** WPA2 personal, support AES, TKIP and TKIP+AES cipher types.
  8. **Mixed WPA/WPA2-PSK:** If selected, both WPA-PSK and WPA2-PSK secured wireless clients can join your wireless network.
  9. **AES:** If selected, wireless speed can reach up to 300Mbps.
  10. **TKIP:** If selected, wireless speed can reach up to 54Mbps.
  11. **TKIP+AES:** If selected, both AES and TKIP secured wireless clients can join your wireless network.
  12. **Key Renewal Interval:** Enter a valid time period for the key to be changed.
- 

### **4.3.3 Advanced Settings**

You can configure the advanced wireless setting for the Router; including Beacon Interval, TX

Power and Basic Data Rate and so on.



**Advanced Settings**

Band Switch: 2.4G

BG Protection Mode: Auto

Basic Data Rates: Default(1-2-5.5-11 Mbps)

Beacon Interval: 100 ms (Range: 20 - 999; Default: 100)

Fragment Threshold: 2348 (Range: 256 - 2346; Default: 2346)

RTS Threshold: 2347 (Range: 1 - 2347; Default: 2347)

TX Power:  High  Medium  Low

WMM Capable:  Enable  Disable

APSD Capable:  Enable  Disable

20/40 BssCoexSupport:  Enable  Disable

**Help**

In this section, you can configure the advanced wireless setting for the Router, including Beacon Interval, TX Power and Basic Data Rate and so on. If you have no idea how to configure these wireless rules, keeping its default value is advisable.

**WMM (Wi-Fi Multimedia):** when WMM is enabled, the wireless multimedia data transmission will be improved greatly (video or online demand).

**APSD:** it is used for auto power-saved service. The default is disabled.

#### 4.3.4 WPS Settings

**Set Steps:**

- ① Click “**WLAN Settings**”.
- ② Select “**WPS Settings**”.



#### Knowledge Expansion

WPS provides you with two main functions:

- if your wireless network unencrypted, WPS can quickly encryption your wireless network.
- If your wireless network encrypted, WPS can make you quickly connect your encrypted wireless network.



### Parameters Specification:

The WPS provides below methods:

- **PBC:**Using routers and physical or logical button on a wireless device to connect WPS.

You have below methods to connect WPS:

#### 1、Using the router WPS button on the rear panel for the PBC connection

- ① Click “Enable”
- ② Click “Save”
- ③ Hold the router on the rear panel of the WPS button for 3 seconds, then let go
- ④ The router's WPS led flashes two minutes, During this time, In the wireless client devices use the WPS/PBC connect to your wireless signal



#### Knowledge Expansion

##### resetOOB:

- The router wireless SSID, safe mode resumed to not configured mode. Make the WPS reset the SSID, Encryption and password, after the completion of the reset, the router's SSID is factory default, safe mode is unencrypted.

#### 4.3.5 Access Control

Wireless access control is actually based on the MAC address to permit or forbid specified clients to access the wireless network



## Set Steps:

- ① Click “WLAN Settings”.
- ② Select “Access Control”.

The screenshot shows the 'Wireless Access Control' configuration page. On the left, a vertical menu lists various settings: System Status, Network Settings, WLAN Settings (selected), Basic Settings, Security Settings, Advanced Settings, WPS Settings, Access Control (selected), Connection Status, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, and System Tools. The main panel title is 'Wireless Access Control'. It features a 'Band Switch' dropdown set to '2.4G' and a 'MAC Address Filter' dropdown set to 'Off'. Below these are 'Save' and 'Cancel' buttons. To the right, a 'Help' section provides a brief description of how MAC address filtering works based on the wireless adapter's MAC address.

## Parameters Specification:

- The Wireless Access Control is based on the MAC address of the wireless adapter to determine whether it communicates with the Router or not;
1. Select “Off” to allow all wireless clients to join your wireless network.
  2. Select “Allow” allow ONLY the specified wireless clients to join your wireless network.
  3. Select “Block” disallow ONLY the specified wireless clients to join your wireless network.

## Wireless Access Control Application Example:

To only allow your own notebook at the MAC address of 00:12:35:EC:DF:25 to join your wireless network

## Set Steps:

- ① Select **Allow**.
- ② Enter the MAC address of the wireless device you want to restrict. Here in this example, enter 00:12:35:EC:DF:25.
- ③ Click **Add** to add the MAC address to the MAC address list.
- ④ Click **Save** to save your settings.



### Tips

- Up to 10 wireless MAC addresses can be configured
- If you don't want to configure the complex wireless security settings and want to disallow others to join your wireless network, you can configure a wireless access control rule to allow only your own wireless device

## 4.3.6 Connection Status

This page shows the current wireless access list

Click “Refresh” to update.



The screenshot shows a web-based management interface for a router. The left sidebar has a blue header and contains the following menu items: System Status, Network Settings, WLAN Settings (which is highlighted in purple), Basic Settings, Security Settings, Advanced Settings, WPS Settings, Access Control, Connection Status (which is also highlighted in purple), USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, and System Tools. The main content area has a white header titled "Wireless Connection Status" with the sub-instruction "The Current Wireless Access List". It includes a "Refresh" button. Below the header is a table with three columns: NO., MAC, and Bandwidth. To the right of the table is a "Help" section with two entries: "MAC Address: Shows the connecting PC's MAC address." and "Bandwidth: The width of channel frequency.".



### Tips

- The bandwidth here refers to the channel bandwidth instead of wireless connection rate.
- You can know whether there are unauthorized accesses to your wireless network by viewing the wireless client list.

## 4.4 USB Setting

### 4.4.1 Device Sharing

You could configure the USB drive connected to the Router.



- [System Status](#)
- [Network Settings](#)
- [WLAN Settings](#)
- [USB Setting](#)
- [Device Sharing](#)
- [Media Server](#)
- [Print Server](#)
- [User Accounts](#)

- [IPTV Settings](#)
- [DHCP Server](#)
- [Virtual Server](#)
- [Security Settings](#)
- [Routing Settings](#)
- [Traffic Control](#)
- [System Tools](#)

## Device Scan

Device
Scan

Device Scan results will appear here.

[Help](#)

Click “Scan” button , wait a minute , you could see the USB drive connected to the Router.

AMTC

### Device Scan

Device
Scan

All Disk

/media/sda1
Share
Delete

**Help**

Configure the USB drive connected to the Router. In this section, you may view the Device Settings like Volume, Capacity, Used Space and Sharing Status.

**Volume:** The volume name of the storage drive.

**Capacity:** The storage capacity of the storage drive.

**Used Space:** The used space of the storage drive.

**Sharing Status:** Indicates the shared or non-shared status of the volume. When the volume is shared, you can click the Disable button to stop sharing the volume; but when volume is non-shared, you can click the Enable button to share the volume.

You can click the “**Share**” or “**Delete**” to enable or disable sharing the volume.

#### **4.4.2 Media Server**

You can configure media server on this page. You could enable this server to share the media information in USB driver. And other user in this local area network could see these information your shared.



Media Server

DLNA  Enable

Save Cancel

Help

You can configure media server on this page.

#### 4.4.3 Print Server

You could connect a network printer to the router and **Enable** the **Print Server**. The other user in this local area network could use the printer.

Print Server

Print Server  Enable

Printer Name Printer\_mtc

Save Cancel

Help

**Print Server:** Indicates the current Enable/Disable status of the Print Server.

**Printer Name:** Name of printer connected to the router.

#### 4.4.4 User Accounts

You could add user in your USB Server. And other user could use this user name and password to login in the USB Server



AMTC

USB Access control

ID	Username	Password	Action
1			<input type="button" value="Delete"/>
1	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

**Help**  
You can specify the user name and password for Storage Sharing and FTP Server users on this page.

**User Name:** Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 32 characters in length.

**Password:** Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 32 characters in length. For security purposes, the password for each user account is not displayed.

## 4.5 IPTV Settings

If you enable this function, you could connect a set-top box to the router to use.

AMTC

IPTV

IPTV  Enable

**Help**  
**IPTV:** Select to enable the IPTV feature.  
**Mode:** If your ISP is not listed and no other parameters are required, you can simply select Bridge mode. Select Custom if your ISP is not listed but provides the necessary parameters, including Internet/Phone/IPTV VLAN IDs and Priority.  
**IGMP Proxy:** Select the IGMP (Internet Group Management Protocol) Proxy version, either V2 or V3, according to your ISP.

## 4.6 DHCP Server

Click “**DHCP Server**” enter the Virtual Server configure page ,here you can set “**DHCP Server**”, “**DHCP List & Binding**”.

### 4.6.1 DHCP Server

**Set Steps:**



- 
- ① Click “DHCP Server”.
  - ② Select “DHCP Server”.

DHCP Server

DHCP Server  Enable

Start IP Address 192.168.1.100

End IP Address 192.168.1.200

Lease Time One day

Save Cancel

**Help**

DHCP (Dynamic Host Configuration Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating obtain an IP Address. Automatically?So specifying the starting and ending address of the IP Address pool is needed. The lease time is the length of the IP address lease.

#### Parameters Specification:

- **DHCP Server:** Select whether enable or disable the DHCP server feature.
- **Start IP Address and End IP Address:** You can specify the starting and ending address of the IP address pool here. These addresses should be part of the same IP address subnet as the router’s LAN IP address.
- Enter the Lease Time



#### Knowledge Expansion

- **DHCP** (Dynamic Host Configuration Protocol) assigns an IP address to each device on the LAN/private network.
- When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool specified in this screen to the requesting device as long as the device is set to “Obtain an IP Address Automatically”.
- If you disable this feature, you have to manually configure the TCP/IP settings for all PCs on your LAN to access Internet.
- **Lease Time:** is the length of the IP address lease before it is refreshed.



#### Tips



By default, the router functions as a DHCP server. Do not disable the DHCP server feature unless you want to manually configure the TCP/IP settings for all PCs on your LAN.

1. Lease time will be renewed automatically upon expiry. No additional configurations are needed.
2. If you are not an advanced user, the default DHCP server settings are recommended.

In order to use the function of the router's DHCP server, LAN in the computer's TCP/IP protocol must be set to "automatically obtain IP".

#### 4.6.2 DHCP List & Binding

##### Set Steps:

- ① Click "DHCP Server".
- ② Select "DHCP List& Binding".

NO.	IP Address	MAC Address	IP-MAC bind	Delete
LZG-PC	192.168.1.100	50:7B:9D:13:8B:93	23:24:59	

##### Parameters Specification:

- Enter the IP Address and MAC Address
- Click "Add" add to the DHCP list
- Click "Refresh" to update the related DHCP client information.



##### Tips

- You can know whether there are unauthorized accesses by viewing the client list.
- Also, you can 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.



### Static Assignment Application Example:

To have a PC at the MAC address of 44:37:E6:4F:37:3B always receive the same IP address of 192.168.1.200

NO.	IP Address	MAC Address	IP-MAC bind	Delete
1	192.168.1.200	50:7B:9D:12:41:69	<input checked="" type="checkbox"/>	<button>Delete</button>

#### Parameters Specification:

- Enter the last number of the IP address you want to reserve, for example, 200.
- Enter the MAC address of 50:7B:9D:12:41:69
- Click “Add”.
- Click “Save” to save your settings.



#### Tips

1. If the IP address you have reserved for your PC is currently used by another client, then you will not be able to obtain a new IP address from the device's DHCP server, instead, you must manually specify a different IP address for your PC to access Internet.
2. For PCs that has already obtained IP addresses, you may need to perform the Repair action to activate the configured static IP addresses

## 4.7 Virtual Server

Click “Virtual Server” enter the Virtual Server configure page ,here you can set “Port Range”, “DMZ Settings”, “uPnP Settings”.

---

#### 4.7.1 Port Range

You want to share resources on your PC with your friends who are not in your LAN. But, by default, the router's firewall blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You can use the Port Forwarding feature to create exceptions to this rule so that your friends can access these files from external networks.

When accessing your PC from Internet, type "protocol://xxx.xxx.xxx.xxx:port number" into your browser's address or location field. The protocol and port are the ones used by the service and "xxx.xxx.xxx.xxx" is the WAN IP address of your router. For example, a FTP server uses the ftp protocol and 21 (standard port number).

##### **Set Steps:**

- ① Click "Virtual Server".
- ② Select "Port Range".

##### **Application Example:**

As shown in the figure above, your PC at **192.168.2.10** connects to the router and runs a FTP server on port number 21. Your friends want to access this FTP server on your PC from external network.



##### Tips -----

To successfully implement the port forwarding feature, note below:

1. Make sure your WAN IP address (Internet IP address) is a public IP address. Private IP addresses are not routed on the Internet.
  2. Make sure you enter correct service port numbers.
  3. To ensure that your server computer always has the same IP address, assign a static IP address to your PC.
  4. Operating System built-in firewall and some anti-virus programs may block other PCs from accessing resources on your PC. So it is advisable to disable them before using this feature.
-

ID	Start Port-End Port	To IP Address	Protocol	Enable	Delete
1.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
2.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.1.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Well-known Service Port: DNS(53) Add to: 1

Save Cancel

### Parameters Specification:

- Start/End Port: Enter the start/end port number which ranges the External ports used to set the server or Internet applications. Here in this example, enter 21.
- IP Address: Enter the IP address of the PC where you want to set the applications. Here in this example, enter 192.168.1.100.
- Protocol: Specify the protocol required for the service utilizing the port(s). Select the protocol (TCP/UDP/Both) for the application.
- “**Enable**” to apply this function, “Delete” cancel this host configure.
- Click ‘**Save**’ to save your settings.

If your WAN IP address is 192.168.1.100 when accessing your FTP server from external network, your friends only need to enter <ftp://192.168.1.100:21> in their browsers.

## 4.7.2 DMZ Settings

### Set Steps:

- ① Click “Virtual Server”.
- ② Select “DMZ Settings”.
- ③ Select “Enable”
- ④ Add DMZ Host IP which is the LAN IP
- ⑤ Click “Save” to confirm.



### Tips

- The DMZ Settings screen allows one local computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing.
- DMZ hosting forwards all the ports at the same time to one PC.



### Note

1. DMZ host poses a security risk. A computer configured as the DMZ host loses much of the protection of the firewall and becomes vulnerable to attacks from external networks.
2. Hackers may use the DMZ host computer to attack other computers on your network

### 4.7.3 uPnP Settings

The Universal Plug and Play (UPnP) feature allows network devices, such as computers from Internet, to access resources on local host or devices as needed. UPnP-enabled devices can be discovered automatically by the UPnP service application on the LAN. If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you may need to enable Universal Plug and Play (UPnP) for better experience.

Click **Virtual Server -> uPnP Settings** to enter the UPnP page. The UPnP feature is enabled by default.



The screenshot shows the AMTC web-based management interface. The left sidebar contains a navigation menu with the following items: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Port Range, DMZ Settings, UPnP Settings (which is highlighted in purple), Security Settings, Routing Settings, Traffic Control, and System Tools. The main content area is titled "UPnP" and contains a single configuration item: "UPnP" followed by an enable/disable checkbox which is checked and labeled "Enable". Below the checkbox are two buttons: "Save" (blue) and "Cancel" (gray). To the right of the main content area is a vertical help panel titled "Help" which provides a brief description of the UPnP feature.

## 4.8 Security Settings

Click “**Security Settings**” enter the Security configure page ,here you can set “**Client Filler**”,“**URL Filter**”, “**MAC Filler**”, “**Prevent**”, “**Remote WEB**”, “**WAN Ping**”.

### 4.4.1 Client Filter

This section allows you to set the times specific clients can or cannot access the Internet via the devices' assigned IP addresses and service port. Click **Security Settings ->Client Filter** to enter the configuration page.



**Client Filter**

**Filter Settings**  Enable

Access Policy:

Enable:  Clear this item:

Policy Name:

Start IP: 192.168.1.

End IP: 192.168.1.

Port:  -

Type:

Time:   ~

Day:  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Help**

This section is to set client filtering access. If you want to enable this function, please activate the checkbox. Select one policy from the drop-down menu and enter a policy name in the field. Of course, you can set the access restriction in details (e.g. the fixed IP range, times and days).

Note: When times is 0:0~0:0, it express 24 hours.

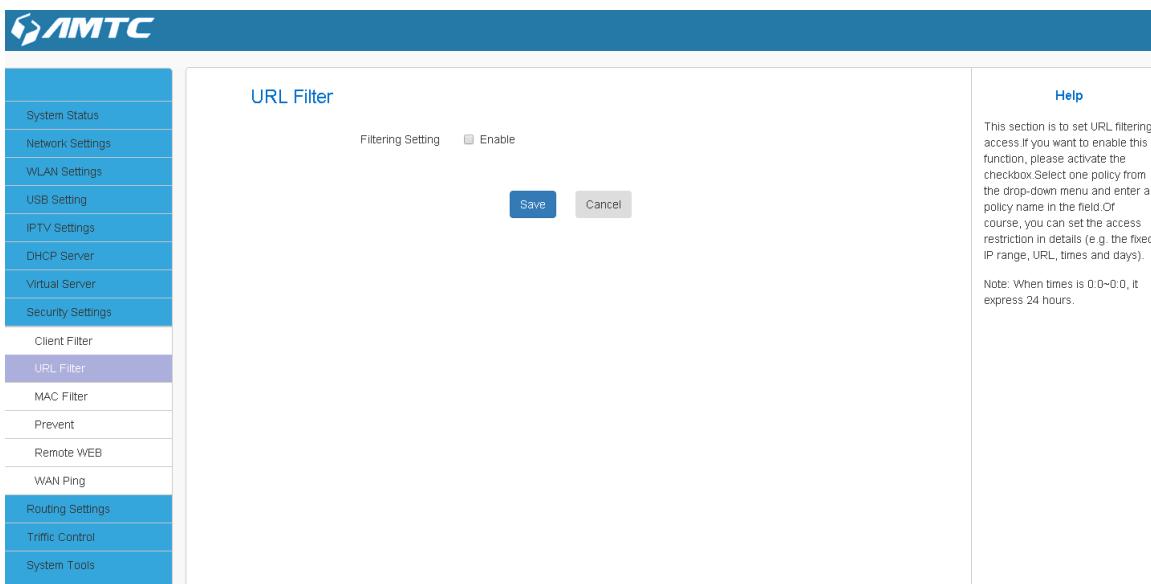
#### 4.4.2 URL Filter

This section is to set URL filtering access. If you want to enable this function, please activate the checkbox. Select one policy from the drop-down menu and enter a policy name in the field. Of course, you can set the access restriction in details (e.g. the fixed IP range, URL, times and days).

Note: When time is 0:0~0:0, it express 24 hours.

##### Set Steps:

- ① Click “**Security Settings**”.
- ② Select “**URL Filter**”.



##### URL Filter Application Example:

To prevent your home PC (192.168.1.100) from accessing “YouTube” from 8:00 to 18:00 during working days: Monday- Friday.

##### Set Steps:

- ① Enter a Policy Name
- ② Enter the Start IP and End IP here for example:192.168.1.100
- ③ Enter part of or the entire domain name of the web site you wish to restrict. Separate different domain names or domain name key words with a comma, for example, "YouTube, Hollywood.com"
- ④ Select time and day
- ⑤ Click “**Save**” to save your settings.

**Help**

This section is to set URL filtering access if you want to enable this function, please activate the checkbox. Select one policy from the drop-down menu and enter a policy name in the field. Of course, you can set the access restriction in details (e.g. the fixed IP range, URL, times and days).

Note: When times is 0:0~0:0, it express 24 hours.



### Tips

1. Different URL strings must be separated with a comma. To match all websites, use \* (asterisk)
2. Up to 10 filter rules can be configured.
3. If you have not set up the system time for this device, click **System Tools -> Time Settings** to set up correct time and date for the rules to be effective

### 4.4.3 MAC Filter

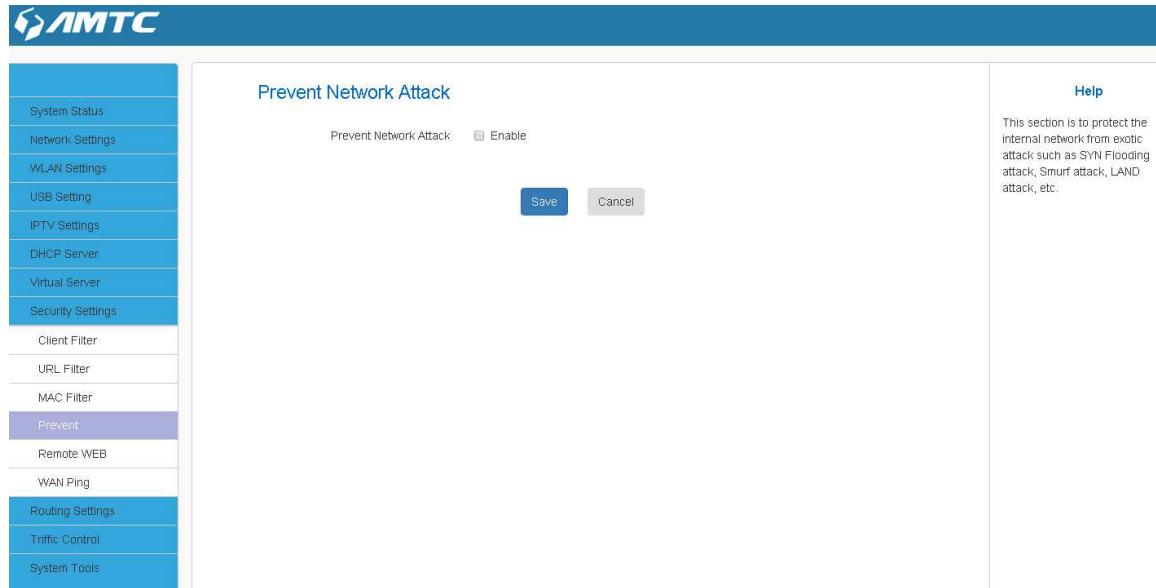
**Help**

This section is to set MAC address filtering access. If you want to enable this function, please activate the checkbox. Select one policy from the drop-down menu and enter a policy name in the field. Of course, you can set the access restriction in details (e.g. the fixed MAC address, times and days).

Note: When times is 0:0~0:0, it express 24 hours.

#### 4.4.4 Prevent

This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc



#### 4.4.5 Remote WEB

This section is to allow the network administrator to manage the router remotely. If you want to access the router remotely, please select “**Enable**”.

##### **Set Steps:**

- ① Click “**Security Settings**”.
- ② Select “**Remote WEB**”.
- ③ Enter the Port
- ④ Click “**Save**” to confirm.

The screenshot shows the AMTC router's web-based management interface. On the left, there's a vertical sidebar with a blue header containing the AMTC logo. Below the logo, the sidebar lists several menu items: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Client Filter, URL Filter, MAC Filter, Prevent (which is highlighted with a purple background), Remote WEB, WAN Ping, Routing Settings, Traffic Control, and System Tools. The main content area has a white background and a title 'Prevent Network Attack'. It contains a single input field with the label 'Prevent Network Attack' followed by a checked checkbox labeled 'Enable'. At the bottom of this panel are two buttons: a blue 'Save' button and a grey 'Cancel' button. To the right of the main content area is a vertical sidebar with a blue header labeled 'Help'. The help text explains that this section is used to protect the internal network from exotic attacks like SYN Flooding, Smurf attack, LAND attack, etc.

### Parameters Specification:

- **Port:** The management port to be open to outside access.



#### Tips

1. For better security, configure a port number (between 1025-65535) as remote web management interface, do not use the number of any common service port (1-1024).
2. Make sure your WAN IP address (Internet IP address) is a public IP address. Private IP addresses are not routed on the Internet.
3. It is unsafe to make your router remotely accessible to all PCs on external network. For better security, we suggest that only enter the IP address of the PC for remote management

### Remote Web Management Application Example:

To access your router (WAN IP address: 172.16.87.160) at your home from the PC (210.16.87.154) at your office via the port number 6060.

#### Set Steps:

- ① Management “**Enable**”.
- ② Enter the Port: 6060.
- ③ Click “**Save**” to save your settings.

In the PC 210.16.87.154 Type “<http://172.16.87.160:6060>” into your browser’s address or location field and you can access the router at your home remotely.

**Remote Web Management**

Management  Enable

Port  (1024-65535)

**Help**

This section is to allow the network administrator to manage the router remotely. If you want to access the router remotely, please select "Enable".

**Port:** The management port to be open to outside access. The default value is 8080.

## Knowledge Expansion

**1. Port:** This is the management port to be open to outside access. The default setting is 8080.

This can be changed

### 4.4.6 WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system would prevent the ping test from WAN.

**WAN Ping**

Ignore the Ping from WAN  Enable

**Help**

The ping test is to check the status of your internet connection. When disabling the test, the system would prevent the ping test from WAN.

#### Set Steps:

- ① Select the “Expert Setting”

---

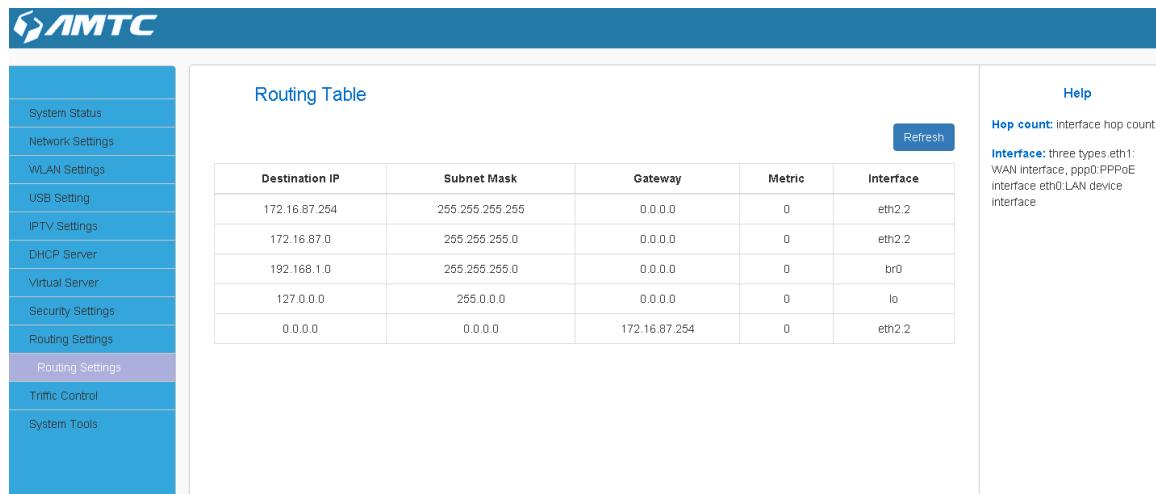
② Select the “WAN Ping”

③ Select the “Enable”

## 4.9 Routing Settings

In this page you can view the routing table information.

Click “Refresh” to update



Destination IP	Subnet Mask	Gateway	Metric	Interface
172.16.87.254	255.255.255.255	0.0.0.0	0	eth2.2
172.16.87.0	255.255.255.0	0.0.0.0	0	eth2.2
192.168.1.0	255.255.255.0	0.0.0.0	0	br0
127.0.0.0	255.0.0.0	0.0.0.0	0	lo
0.0.0.0	0.0.0.0	172.16.87.254	0	eth2.2

- **Destination IP:** The IP address of the final destination. “0.0.0.0” indicates any network segment.
- **Subnet Mask:** The subnet mask for the specified destination.
- **Gateway:** This is the next router on the same LAN segment as the router to reach.
- **Interface:** The interface between your router and the final destination.

## 4.10 Traffic Control

Traffic control is used to limit communication speed in the LAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.

**Traffic Control Settings**

Traffic Control  Enable

Save Cancel

**Help**

Traffic control is used to limit communication speed in the LAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.

**Interface:** to limit the uploading and downloading bandwidth in WAN port.

**Bandwidth Range:** to specify the uploading/downloading Min/Max traffic speed (kByte/s), which can not exceed the WAN speed.



1. 1M=128KByte/s.

2. The volume of uplink traffic/downlink traffic should not be larger than that allowed on your router's WAN (Internet) port. You can ask your ISP to provide the volume of Internet traffic.
3. The bandwidth for ADSL/DSL line usually refers to the download bandwidth

### Bandwidth Control Application Example:

You share a 4M-broadband service with your neighbor (at 192.168.1.102). He always downloads a large volume of data from Internet, which sharply frustrates your Internet surfing experience; you can use this feature to set limits for the volume of Internet traffic he can get. For example, you can split the 4M into two, so your neighbor can only use up to 2M Internet traffic and you can enjoy 2M.

**Traffic Control Settings**

Traffic Control  Enable

IP Range 192.168.1.102 ~

Up/Down Up

Bandwidth Range 128 ~ 128 (kByte/s)

Apply

Add Num IP Up/Down BW Range Apply Edit Del Save Cancel

**Help**

Traffic control is used to limit communication speed in the LAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.

**Interface:** to limit the uploading and downloading bandwidth in WAN port.

**Bandwidth Range:** to specify the uploading/downloading Min/Max traffic speed (kByte/s), which can not exceed the WAN speed.

### Set Steps:

- ① **Enable Traffic Control:** Check the **Enable** box to enable the Traffic Control feature.

- 
- ② **IP Range:** Enter the last number of the IP address. Here in this example, enter 101 in both boxes.
  - ③ **Up:** Set a limit to regulate upload bandwidth of PCs on the LAN. Here in this example, enter 32 in first boxes, and 256 in second box.
  - ④ **Down:** Set a limit to regulate download bandwidth of PCs on the LAN.
  - ⑤ **Apply:** Check to enable the current rule.
  - ⑥ **Add:** Click to add current rule to the rule list.
  - ⑦ Click **Save** to save your settings.

## 4.11 System Tools

Click “**SystemTools**” enter the configure page ,here you can set “**TimeSettings**”, “**DDNS**”, “**Backup/Restore**”, “**Restore to Factory**”, “**firmware Upgrade**”, “**Reboot**”, “**Change Password**”, “**System Log**”.

### 4.11.1 Time Settings

Click **System Tools -> Time Settings** to enter the time page.



#### Tips

Configured time and date info will be lost if the device gets disconnected from power supply. However, it will be updated automatically when the device reconnects to Internet. To activate time-based features (e.g. firewall), the time and date info shall be set correctly first, either manually or automatically

---

**Time Settings**

Note: GMT time will be updated automatically only when the device is connected to Internet

System Time: 1971-01-01 01:37:14

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Customized time:  Enable

**Help**

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

### Set Steps:

- ① Click “**System Tools**”.
  - ② Select “**Time Settings**”.
  - ③ The time will synchronize with the internet automatically in the default situation
  - ④ Select Time Zone
  - ⑤ If you can enter the time and date manually or click “**Sync with your PC**”, synchronize automatically.
  - ⑥ Click **Save** to save you settings.
- **Synchronize with your PC:** Specify a time interval for periodic update of time and date information from your host.

### 4.11.2 DDNS

The screenshot shows the 'DDNS' configuration page. On the left, a sidebar menu lists various settings: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, System Tools, Time Settings, DNS (selected), Backup/Restore, Restore to Factory, Firmware Upgrade, Reboot, Change Password, and System Log. The main content area has a title 'DDNS' and a sub-section 'DDNS Service' with a checkbox labeled 'Enable'. Below this are two buttons: 'Save' (blue) and 'Cancel' (grey). To the right, a 'Help' section provides a detailed explanation of what DDNS is and how to activate it.

### 4.11.3 Backup & Restore

#### Set Steps:

- ① Click “System Tools”.
- ② Select “Restore to Factory”.

The screenshot shows the 'Backup/Restore' configuration page. The sidebar menu is identical to the previous one, with 'DNS' selected. The main content area has a title 'Backup/Restore' and a note: 'The device provides backup/restore settings, so you need set a directory to keep these parameters.' It features a 'Backup' button and a 'Please choose restore file' input field containing '选择文件 未选择任何文件'. To the right, a 'Help' section defines the 'Backup' and 'Restore' buttons.

#### Parameters Specification:

- This “Restore” button is to reset all configurations to the default values. It means the Range

---

Extender will lose all the settings you have set. So please note down the related settings if necessary.

- **Default Password:** admin
- **Subnet Mask:**255.255.255.0
- **Default IP:**192.168.1.1



#### Note

- If you enable this option, all current settings will be deleted and be restored to factory default values. You will have to reconfigure Internet connection settings and wireless settings.
- Do not restore factory default settings unless the following happens:
  - 1> You need to join a different network or unfortunately forget the login password.
  - 2>You cannot access Internet and your ISP or our technical support asks you to reset the router.

---

#### 4.11.4 Firmware Update

The router provides the firmware upgrade by clicking the "Upgrade" after browsing for the firmware upgrade packet. After the upgrade is completed, the router will reboot automatically.

The screenshot shows the router's configuration interface. The left sidebar has a blue header with the AMTC logo and a list of settings: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, System Tools, Time Settings, DDNS, Backup/Restore, Restore to Factory, **Firmware Upgrade** (which is selected and highlighted in purple), Reboot, Change Password, and System Log. The main content area has a blue header "Firmware Upgrade". It says "Select the firmware version:" and has a file input field with placeholder text "选择文件 未选择任何文件". Below it is a large blue "Upgrade" button. At the bottom, it shows "The current firmware version MTC-WR1201-V002R001C01B-Apr 6 2016". To the right, there is a "Help" section with text about the upgrade process and a note that the router will reboot automatically after completion.

#### Set Steps:

- ① Click "**System Tools**"

- 
- ② Select “**FirmwareUpgrade**”
  - ③ Click “**Browse**”, select the upgrade file
  - ④ Click “**Upgrade**”, and wait for it to complete.



#### Note

- 1. Before you upgrade the firmware, make sure you are having a correct firmware. A wrong firmware may damage the device.
  - 2. It is advisable that you upgrade the device's firmware over a wired connection. DO NOT interrupt the power to the router when the upgrade is in process otherwise the router may be permanently damaged.
- 

### 4.11.5 Restore to Factory

#### Set Steps:

- ① Click “**System Tools**”.
- ② Select “**Restore to Factory**”.

The screenshot shows the AMTC web configuration interface. The top navigation bar has the AMTC logo. On the left, there is a vertical sidebar menu with the following items: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, System Tools, Time Settings, DDNS, Backup/Restore, **Restore to Factory** (which is highlighted in purple), Firmware Upgrade, Reboot, Change Password, and System Log. The main content area has a title "Restore to Factory" and a sub-instruction "Restore to Factory Default Settings.". Below this is a blue "Restore" button. To the right of the main content area is a "Help" section containing the following text:  
This button is to reset all configurations to the default values. It means the router will lose all the settings you have set. So please note down the related settings if necessary.  
**Default password:** admin  
**Default IP:** 192.168.1.1  
**Default subnet mask:** 255.255.255.0

#### Parameters Specification:

- This “**Restore**” button is to reset all configurations to the default values. It means the Range

---

Extender will lose all the settings you have set. So please note down the related settings if necessary.

- **Default Password:** admin
- **Subnet Mask:** 255.255.255.0
- **Default IP:** 192.168.1.1



#### Note

- If you enable this option, all current settings will be deleted and be restored to factory default values. You will have to reconfigure Internet connection settings and wireless settings.
- Do not restore factory default settings unless the following happens:
  - 1>You need to join a different network or unfortunately forget the login password.
  - 2>You cannot access Internet and your ISP or our technical support asks you to reset the router.

---

#### 4.11.6 Reboot

When a certain feature does not take effect or the device fails to function correctly, try rebooting the device.

The screenshot shows the AMTC web configuration interface. The left sidebar has a blue header 'AMTC' and a list of navigation items. The 'System Tools' section is expanded, showing 'Restore to Factory' as the selected item, indicated by a purple background. Other items in this section include 'Firmware Upgrade', 'Reboot', 'Change Password', and 'System Log'. The main content area has a title 'Restore to Factory' and a sub-instruction 'Restore to Factory Default Settings.' Below this is a large blue 'Restore' button. To the right of the main content is a 'Help' panel containing information about the restore function, default settings, and a note about losing user settings. It also lists the default password (admin), default IP (192.168.1.1), and default subnet mask (255.255.255.0).

- Rebooting the Wifi Router is to make the settings configured go into effect or to set the Range Extender again if setting failure happens.

#### 4.11.7 Change Password

You can change the password by this function

The screenshot shows the AMTC web interface. The left sidebar contains a navigation menu with the following items: System Status, Network Settings, WLAN Settings, USB Setting, IPTV Settings, DHCP Server, Virtual Server, Security Settings, Routing Settings, Traffic Control, System Tools, Time Settings, DDNS, Backup/Restore, Restore to Factory, Firmware Upgrade, Reboot, Change Password (which is highlighted in purple), and System Log. The main content area is titled "Change Password" and contains three input fields: "Old Password", "New Password", and "Confirm New Password". Below the fields are two buttons: "Save" (blue) and "Cancel" (gray). To the right of the main content is a "Help" section with the following text:  
Default password is admin, We recommend you to change it for better security. Otherwise, anyone in your network can access this utility to change your settings.  
**Old Password:** If you first time use the router, enter admin. If you already changed it and unfortunately forgot, restore the router to factory defaults.  
**New Password:** Input a new password. It MUST only consist of 3-32 characters without any space.  
**Confirm New Password:** Re-enter the new password.

#### Set Steps:

- ① Click “**System Tools**”
- ② Select “**Change Password**”
- ③ Enter “**Old Password**”“**New Password**”and“**Confirm New Password**”
- ④ Click “**Save**” to save you settings.



#### Tips

- The default login password is admin.
- The valid password must be between 3~12 characters and only include letters, numbers and underscore

#### 4.11.8 System Logs

The section is to view the system log. Click the “**Refresh**” to update the log.

Click the “**Clear**” to clear the screen.

The screenshot shows the AMTC web-based management interface. At the top left is the AMTC logo. On the left side is a vertical navigation menu with the following items:

- System Status
- Network Settings
- WLAN Settings
- USB Setting
- IPTV Settings
- DHCP Server
- Virtual Server
- Security Settings
- Routing Settings
- Traffic Control
- System Tools
- Time Settings
- DDNS
- Backup/Restore
- Restore to Factory
- Firmware Upgrade
- Reboot
- Change Password

The "System Tools" item is highlighted with a purple background. Below the menu, the main content area has a title "System Log". It includes a search bar with fields for "Time" (1), "Date" (1970-01-01 00:00:08), "Protocol" (http), and "Content" (web service start OK!). There are "Refresh" and "Clear" buttons. A red bracket [1] points to the first log entry. To the right of the log table is a "Help" section with the following text:

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

## Set Steps:

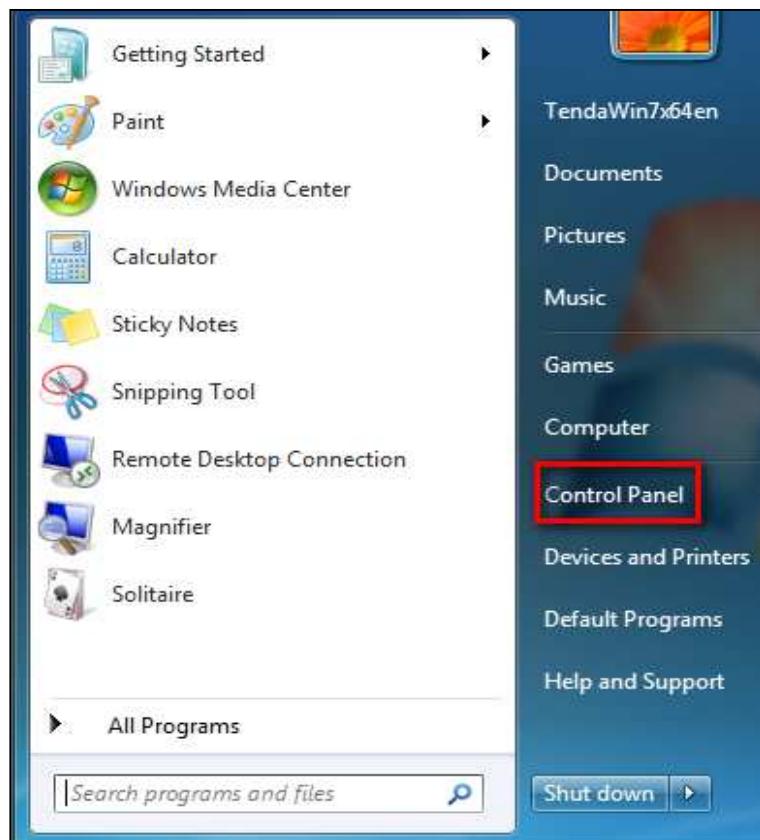
- ① Click "**System Tools**"
- ② Select "**System Log**"
- ③ Click "**Refresh**" can update the information
- ④ Click "**Clear**" to clear the screen

## Appendix

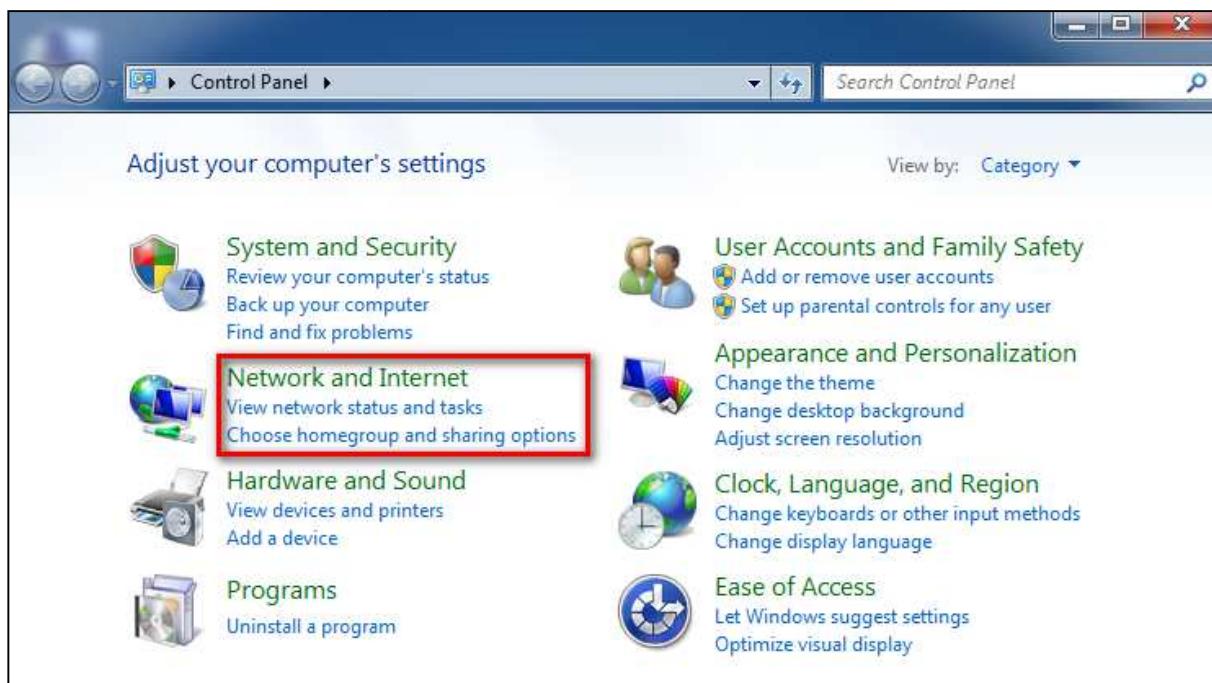
### 1 Configure PC TCP/IP Settings

#### Windows 7

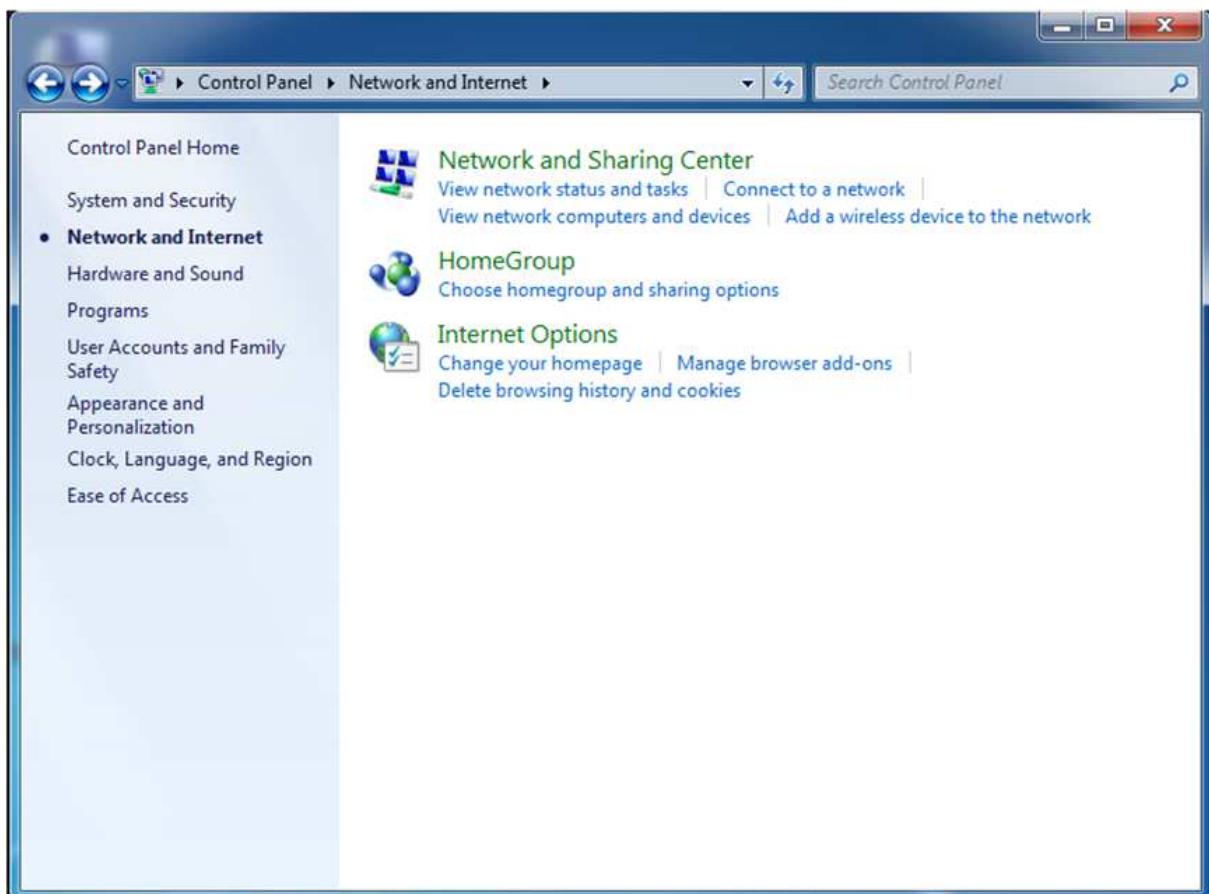
① Click Start -> Control Panel.



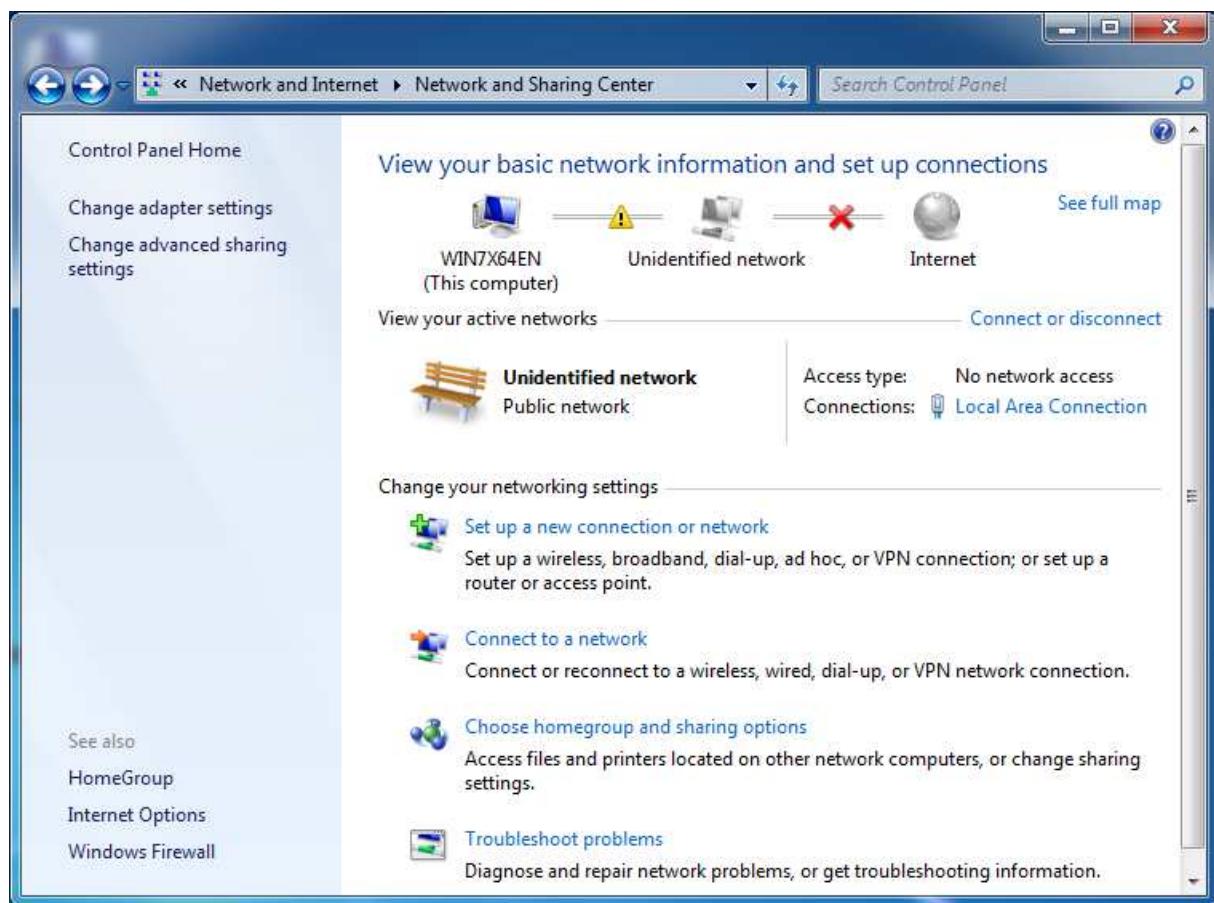
② Click **Network and Internet**.



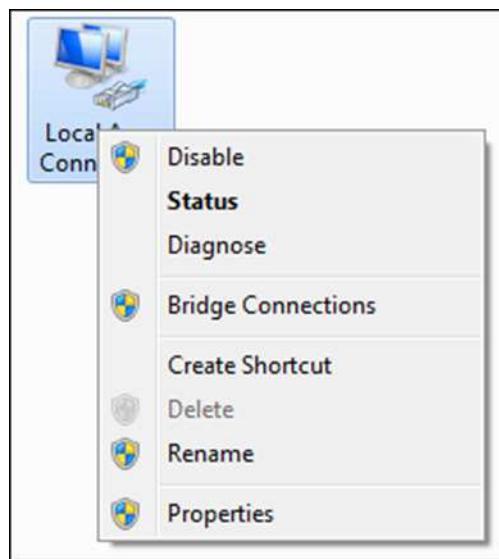
③ Click **Network and Sharing Center**.



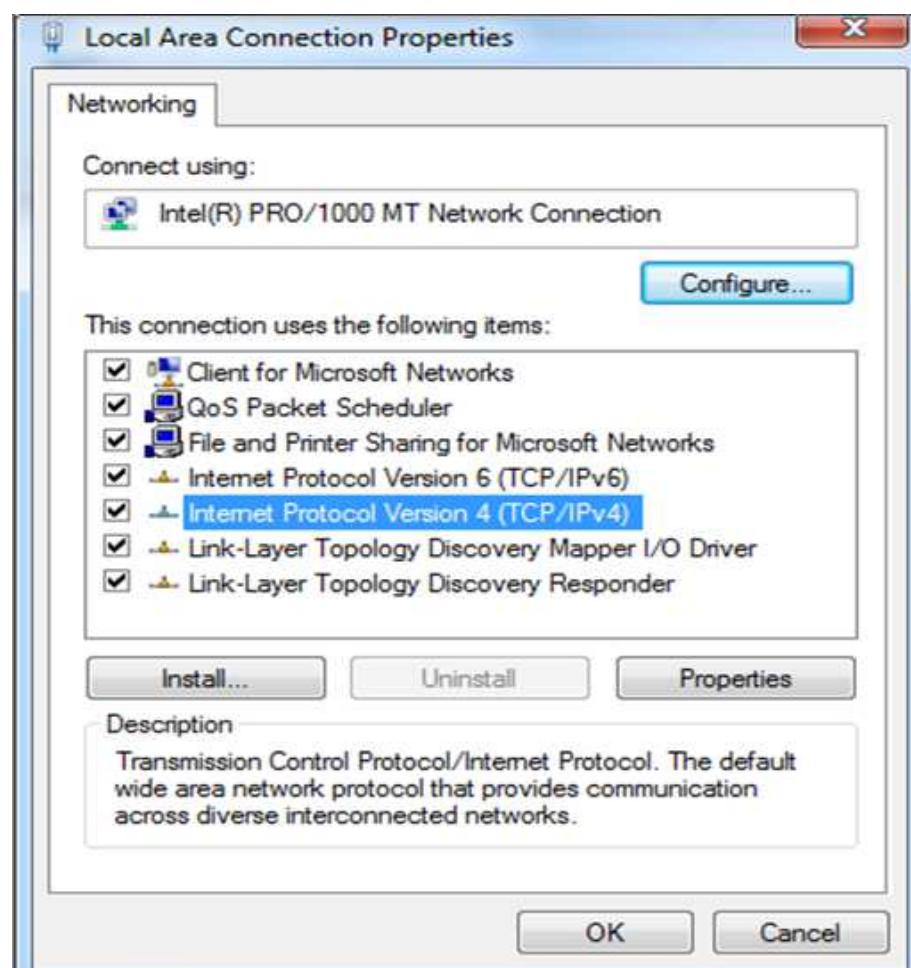
④ Click **Change adapter settings**.



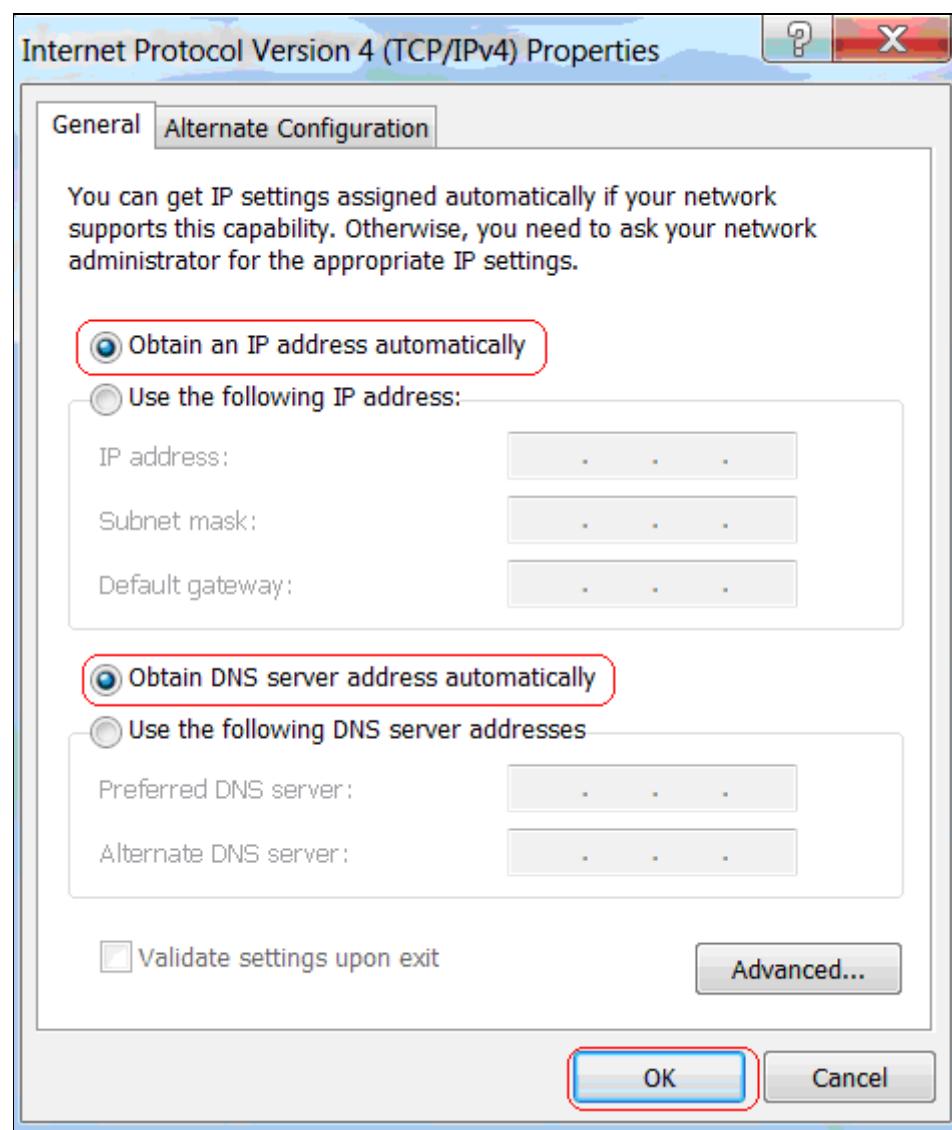
⑤ Click **Local Area Connection** and select **Properties**.



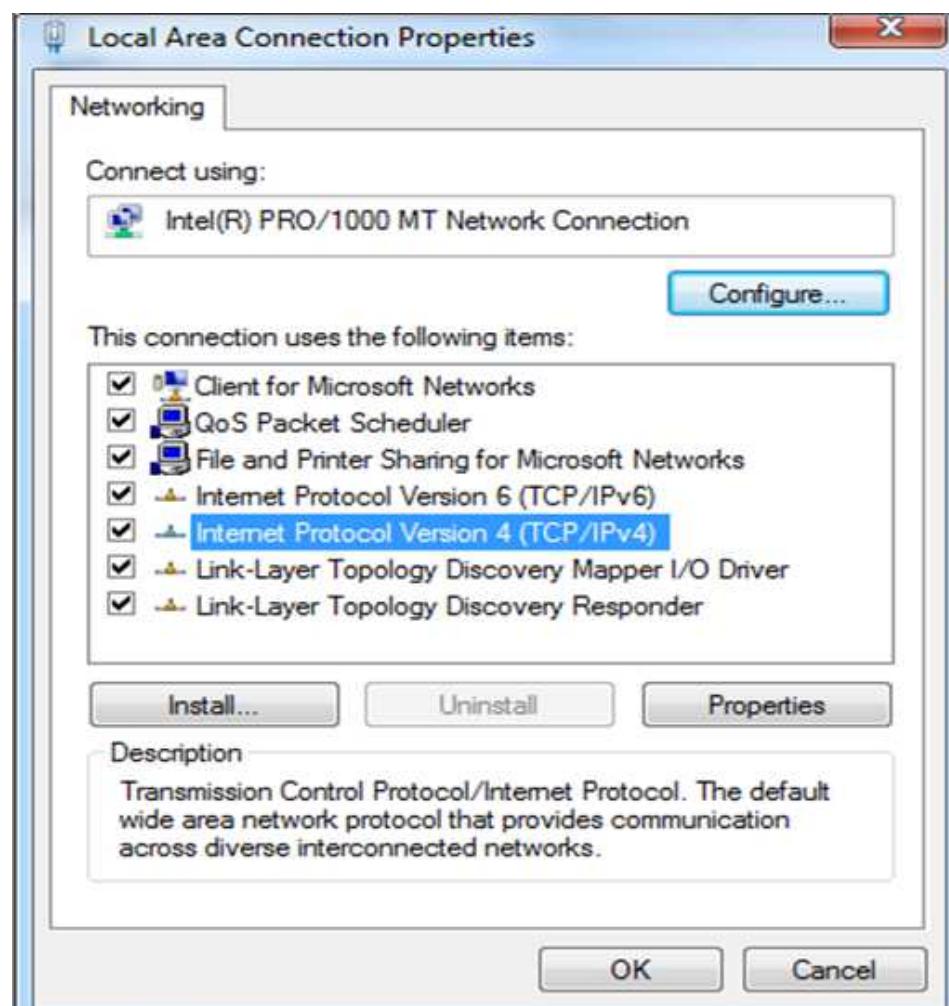
⑥ Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



⑦ Select **Obtain an IP address automatically** and click **OK**.



⑧ Click **OK** on the **Local Area Connection Properties** window to save your settings.



## Windows XP

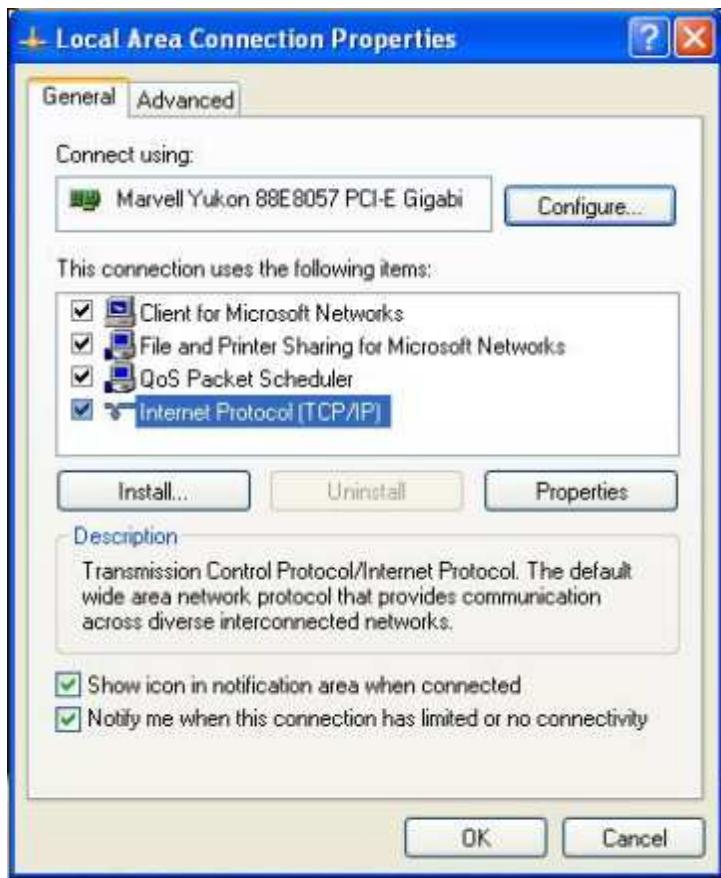
- ① Right-click **My Network Places** and select **Properties**.



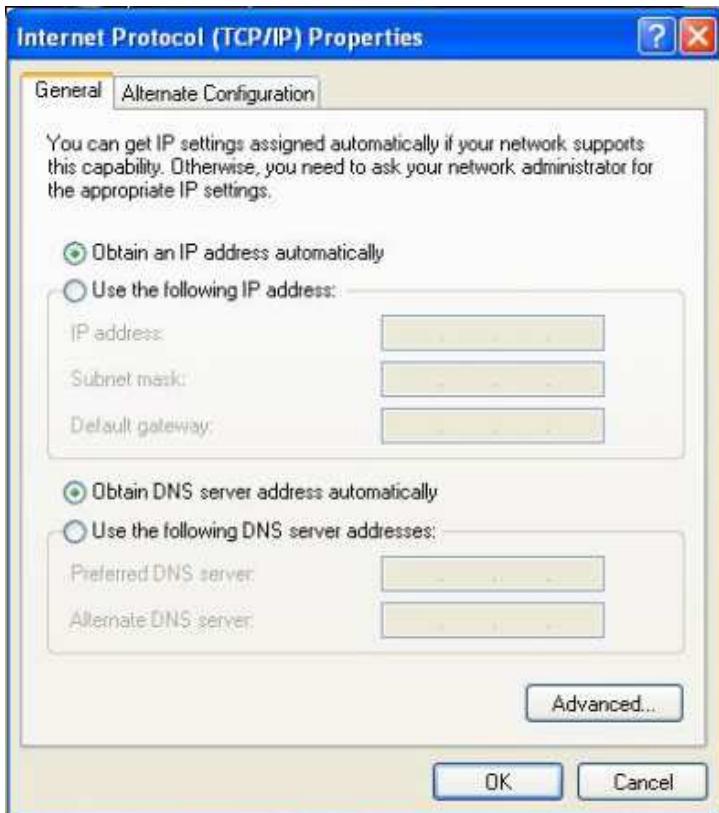
- ② Right click **Local Area Connection** and select **Properties**.



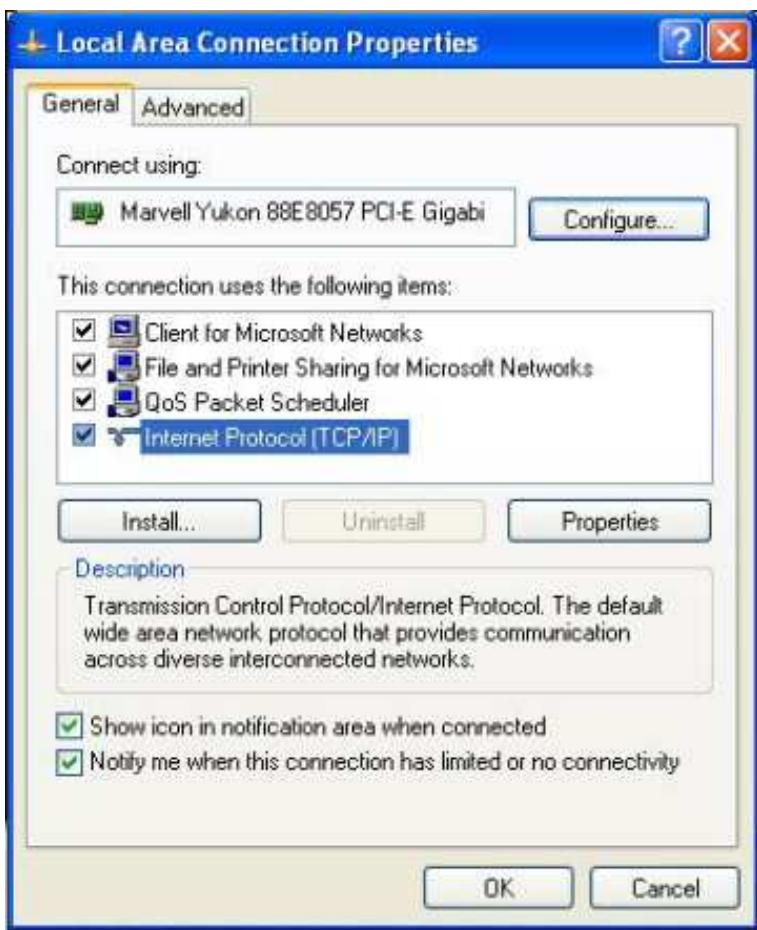
- ③ Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



- ④ Select **Obtain an IP address automatically** and click **OK**.



- ⑤ Click **OK** on the **Local Area Connection Properties** window to save your settings.



---

## **2 FAQs**

This section provides solutions to problems that may occur during installation and operation of the device. Read the following if you are running into problems.

### **1. Q: I cannot access the device's management interface. What should I do?**

- Make sure the System LED on the device's front panel is on.
- Make sure all cables are correctly connected and the corresponding LAN LED on the device is on.
- Verify that your PC's TCP/IP settings are configured correctly. If you select the "Use the following IP address" option, set your PC's IP address to any IP address between 192.168.1.2~192.168.1.254. Or you can select the "Obtain an IP address automatically" option.
- Delete your browser cache and cookies or use a new browser. Make sure you enter 192.168.1.1 in the address bar.
- Press the WPS/RST button for about 10 seconds to restore your device to factory default settings. Then log to your device again.

### **2. Q: I changed the login password and unfortunately forgot it. What should I do?**

Press the WPS/RST button for over 10 seconds to restore your device to factory default settings.

### **3. Q: My computer shows an IP address conflict error after having connected to the device. What should I do?**

- Make sure there are no other DHCP servers on your LAN or other DHCP servers are disabled.
- Make sure the device's LAN IP is not used by other devices on your LAN. The device's default LAN IP address is 192.168.1.1.
- Make sure the statically assigned IP addresses to the PCs on LAN are not used by others PCs.

### **4. Q: I have problems connecting to Internet/Secure websites do not open or**

---

### **displays only part of a web page. What should I do?**

This problem mainly happens to users who use the PPPOE or Dynamic IP Internet connection type. You need to change the MTU size. Try changing the MTU to 1450 or 1400. If this does not help, gradually reduce the MTU from the maximum value until the problem disappears.

## **3 Factory Default Settings**

The table below lists the factory default settings of your device.

<b>Item</b>	<b>Default Settings</b>	
Router Login	Login IP Address	192.168.1.1
	Login User Name	admin
	Login Password	admin
Network Settings	Internet Connection Type	Mode Auto-switch Enabled
	MTU	1492 (PPPOE) 1500 (DHCP/ Static IP)
	WAN Speed	Auto
	DNS	Disable
LAN Settings (LAN)	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	DHCP Server	Enabled
	IP Pool	192.168.1.100~192.168.1.200
	Time Zone	(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi
2.4G Wireless	Wireless	Enabled
	SSID	MTC_XXXXXX (where XXXXXX is the last six characters in the device's MAC address)
	802.11 Mode	11b/g/n mixed Mode

	SSID Broadcast	Enabled
	Channel	2437MHz(Channel 6)
	Channel Bandwidth	20/40
	Extension Channel	2417MHz(Channel 2)
	Wireless Security	Disabled
	Wireless Access Control	Disabled
5.0G Wireless	Country	America
	Wireless	Enabled
	SSID	MTC_XXXXXX (where XXXXXX is the last six characters in the device's MAC address)
	802.11 Mode	11a/an/ac mode
	SSID Broadcast	Enabled
	Channel	5745MHz(Channel 149)
	Channel Bandwidth	40
	WMM Capable	Enable
	APSD Capable	Disabled
	Wireless Security	Disabled
	Wireless Access Control	Disabled
	Remote Web Management	Disabled
Others	Bandwidth Control	Disabled
	DMZ Host	Disabled
	UPnP	Enable
	Internet Access Management	Disabled