

2.2 Wireless Security

Click **Wireless** -> **Wireless Security** to enter the Wireless Security screen. Here you can define a security key to secure your wireless network against unauthorized accesses.

The screenshot displays the Tenda Wireless Security Setup interface. The top navigation bar includes 'Wizard', 'Advanced', 'Wireless', 'QoS', 'Applications', 'Security', and 'Tools'. The left sidebar shows 'Wireless Basic Settings', 'Wireless Security' (highlighted), 'Access Control', and 'Wireless Connection Status'. The main content area is titled 'Wireless Security Setup' and contains the following fields and options:

- Select SSID:** A dropdown menu showing 'Tenda_221988'.
- Security Mode:** A dropdown menu showing 'WPA-PSK(Recommended)'.
- WPA Algorithms:** Radio buttons for 'AES(Recommended)' (selected), 'TKIP', and 'TKIP&AES'.
- Security Key:** A text input field with masked characters '.....' and a default value 'Default: 12345678'.
- WPS Settings:** Radio buttons for 'Disable' (selected) and 'Enable'. A warning message above reads: 'To configure a wireless security key, disable the WPS below!'.
- Buttons:** 'OK', 'Cancel', and 'Reset OOB'.

The **Help** section on the right provides additional information:

- WEP Key:** Must be either 5 or 13 ASCII characters or 10 or 26 Hex characters.
- WPA/WPA2-Personal:** You can enable personal (PSK) or mixed mode, but you must make sure that the wireless client also supports the selected Security mode.

Configuration Procedures:

- ① Select the wireless network (SSID) you wish to encrypt.
- ② Configure security mode, cipher type and security key.
- ③ Click **OK** to save your settings.



Knowledge Center

- 1. Open:** Wireless speed can reach up to 54Mbps if WEP - Open is selected.
- 2. Shared:** Wireless speed can reach up to 54Mbps if WEP - Shared is selected.
- 3. Default key:** Select a key to be effective for the current WEP encryption. For example, if you select Key 1, wireless clients must join your wireless network using this Key 1.
- 4. WPA-PSK:** WPA personal, support AES and TKIP cipher types.
- 5. WPA2-PSK:** WPA2 personal, support AES, TKIP and TKIP+AES cipher types.
- 6. WPA/WPA2-PSK mixed:** If selected, both WPA-PSK and WPA2-PSK secured wireless clients can join your wireless network.
- 7. AES:** If selected, wireless speed can reach up to 300Mbps.
- 8. TKIP:** If selected, wireless speed can reach up to 54Mbps.
- 9. TKIP+AES:** If selected, both AES and TKIP secured wireless clients can join your wireless network.

2.3 Wireless Access Control

Specify a list of devices to "Permit" or "Forbid" a connection to your wireless network via the devices' MAC Addresses.

Click **Wireless** -> **Wireless Access Control** to enter the configuration screen.

There are three options available: Disable, Forbid and Permit.

A. If you want to allow all wireless clients to join your wireless network, select **Disable**.

B. If you want to allow ONLY the specified wireless clients to join your wireless network, select **Permit**.

C. If you want to disallow ONLY the specified wireless clients to join your wireless network, select **Forbid**.

Wireless Access Control Application Example:

To only allow your own notebook at the MAC address of C8:3A:35:CC:34:25 to join your wireless network

The screenshot displays the Tenda wireless router's configuration interface. The top navigation bar includes 'Wizard', 'Advanced', 'Wireless', 'QoS', 'Applications', 'Security', and 'Tools'. The 'Wireless' tab is active, and the 'Access Control' option is selected in the left sidebar. The main configuration area is titled 'Access Control' and contains the following elements:

- Select SSID:** A dropdown menu showing 'Tenda_221988'.
- MAC Address Filter:** A dropdown menu showing 'Permit'.
- MAC Address Table:** A table with two columns: 'MAC Address' and 'Operate'.
 - Row 1: MAC Address 'C8 : 3A : 35 : CC : 34 : 25', Operate button 'Add'.
 - Row 2: MAC Address 'C8:3A:35:CC:34:25', Operate button 'Delete'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom center.
- Help Text:** 'Specify a list of wireless devices to "Permit" or "Forbid" a connection to your router via the devices' MAC addresses. All other devices not listed as Permitted will be Forbidden and vice versa.'

Configuration Procedures:

Select the wireless network (SSID) you wish to enable Access Control on.

① Select **Permit**.

② Enter the MAC address of the wireless device you want to restrict. Here in this example, enter C8:3A:35:CC:34:25.

- ③ Click **Add** to add the MAC address to the MAC address list.
- ④ Click **OK** to save your settings.

**Tip**

1. Up to 16 wireless MAC addresses can be configured.
2. 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.

2.4 Wireless Clients

Click **Wireless** -> **Wireless Connection Status**. Here you can see a list of wireless devices connected to the router.

NO.	MAC Address	Bandwidth
1	C8:3A:35:CA:EC:3D	40M

**Tip**

1. 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.

3 Bandwidth Control

3.1 Bandwidth Control

If there are multiple PCs behind your router competing for limited bandwidth resource, then you can use this feature to specify a reasonable amount of bandwidth for each such PC, so that no one will be over stuffed or starved to death.

**Tip**

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.

Bandwidth Control Application Example:

You share a 4M-broadband service with your neighbor (at 192.168.2.100) who always downloads a large volume of data from Internet. Your Internet surfing experience is thus affected seriously. In this case, use this feature to set limits for the volume of Internet traffic he/she can get. For example, you can equally split the bandwidth, so your neighbor can only use up to 2M Internet traffic and you can happily enjoy 2M.

Bandwidth Control

Enable Bandwidth Control Enable

IP Address 192.168.2. 100 ~ 100

Upload/Download Download

Bandwidth Range 256 ~ 256 (KByte/s)

Enable

Add To List

No.	IP Range	Destination	Bandwidth Range	Enable	Edit	Delete
1	192.168.2.100~100	Download	256~256	✓	Edit	Delete

OK Cancel

Help

The Bandwidth Control helps you to improve network performance by specifying the download/upload speed for computers.

Upload/Download: Select upload or download from the drop-down list.

Bandwidth Range: Set a upload/download bandwidth limit on specified PC(s).

Note: The maximum upload/download bandwidth should not exceed the bandwidth provided by your ISP.

Configuration Procedures:

- ① **Enable Bandwidth Control:** Check the **Enable** box to enable the Bandwidth Control feature.
- ② **IP Address:** Enter the last number of the IP address. Here in this example, enter 100 in both boxes.
- ③ **Upload/Download:** Select **Download** from the drop-down list.
- ④ **Bandwidth Range:** Set a limit to regulate download bandwidth of PCs on the LAN. Here in this example, enter 256 in both boxes.
- ⑤ **Enable:** Check to enable the current rule.
- ⑥ **Add to List:** Click to add current rule to the rule list.
- ⑦ Click **OK** to save your settings.

3.2 Traffic Statistics

Traffic Statistics meter allows you to monitor and view the volume of traffic used by LAN devices.

Click **QoS-> Traffic Statistics** to enter the Statistics screen.



Tip

If you suspect some PCs behind your router are consuming a large volume of bandwidth (downloading videos, etc) you can enable this Traffic Statistics meter feature to find out which PCs are overusing the traffic. Enabling the Traffic Statistics feature may degrade the router's performance. Do not enable it unless necessary.

IP Address	Uplink Rate (KByte/s)	Downlink Rate (KByte/s)	Sent Message	Sent Bytes (MByte)	Received Message	Received Bytes (MByte)

Configuration Procedures:

- ① Check **Enable Traffic Statistics**.
- ② Click **OK** to save your settings.



Knowledge Center

1. **IP Address:** Displays the IP addresses of the PCs that have connected to the device.
2. **Uplink Rate:** Displays the upload speed (KByte/s) of a corresponding PC.
3. **Downlink Rate:** Displays the download speed (KByte/s) of a corresponding PC.
4. **Sent Message:** The number of packets transmitted by a corresponding PC upon traffic statistics meter startup.
5. **Sent Bytes:** The number of bytes transmitted by a corresponding PC upon traffic statistics meter startup. The unit is MByte.
6. **Received Message:** The number of packets received by a corresponding PC upon traffic statistics meter startup.
7. **Received Bytes:** The number of bytes received by a corresponding PC upon traffic statistics

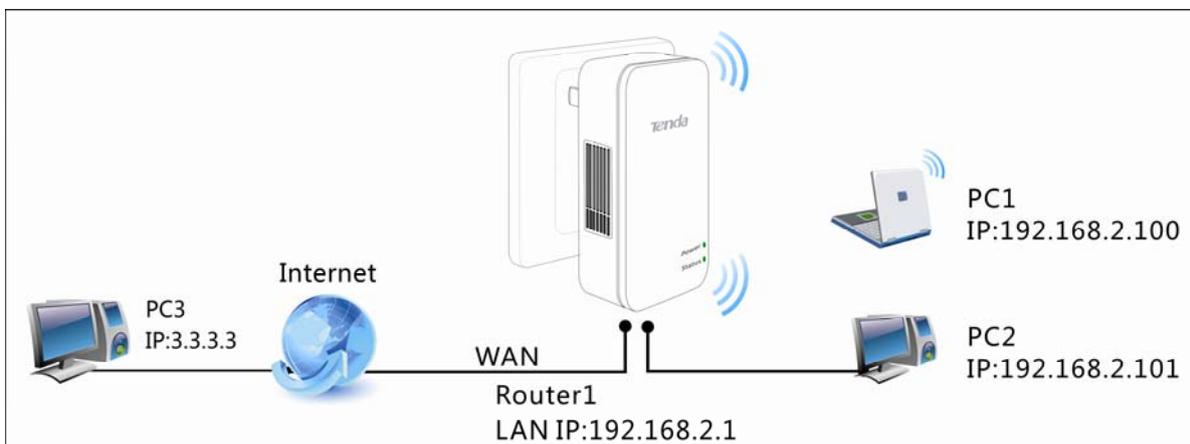
meter startup. The unit is MByte.

4 Special Applications

4.1 Port Range Forwarding

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.

Click **Applications** to enter the configuration screen.



Application Example:

As shown in the figure above, your PC at 192.168.2.100 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.



Tip

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.
-

Port Range Forwarding

Port range forwarding is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications. When you enable the port range forwarding, the communication requests from the Internet to your router's WAN port will be forwarded to the specified LAN IP address.

NO.	Start Port-End Port	LAN IP	Protocol	Enable	Delete
1.	21 - 21	192.168.2.100	TCP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
3.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
4.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
5.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
6.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
7.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Help

To forward ports to an internal host, specify a range of ports from 1~65535 (for a single port, enter the port number in both Start and End fields. Then enter the internal host's IP Address. Be sure to statically assign the host's IP Address in the Advanced > DHCP Client List section to make this function effective. Specify the protocol required for the service utilizing the port(s). Click on "Enable" and then "OK".

Start Port-End Port: Specify the WAN service ports.

Configuration Procedures:

- ① **Start Port:** Enter the starting port number for the service. Here in this example, enter 21.
End Port: Enter the ending port number for the service. Here in this example, enter 21.
- ② **LAN IP:** Enter the IP address of your local computer that will provide this service. Here in this example, enter 192.168.2.100.
- ③ **Protocol:** Specify the protocol required for the service utilizing the port(s).
- ④ Check **Enable** to activate this rule.
- ⑤ Click **OK** to save your settings.

Now, your friends only need to enter `ftp://xxx.xxx.xxx.xxx:21` in their browsers to access your FTP server. `xxx.xxx.xxx.xxx` is the router's WAN IP address. For example, if it is 172.16.102.89, your friends need to enter <ftp://202.33.56.88:21>.

4.2 DMZ Host

The DMZ (De-Militarized Zone) function disables the firewall on the router for one device for a special purpose service such as Internet gaming or video conferencing applications that are not compatible with NAT (Network Address Translation).

Click **Applications** -> **DMZ Host** to enter the DMZ Host screen.



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.
-

Configuration Procedures:

- ① **DMZ Host IP Address:** The IP Address of the device for which the router's firewall will be disabled. Be sure to statically set the IP Address of that device for this function to be consistent.
- ② **Enable:** Check to enable the DMZ host.
- ③ Click **OK** to save your settings.

**Tip**-----

1. Be sure to statically set the IP Address of the computer that serves as a DMZ host for this function to be consistent.
 2. Security softwares such as anti-virus software and OS built-in firewall, etc may affect the DMZ host feature. Disable them if DMZ host fails.
-

4.3 DDNS

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to Internet; the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember; an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS queries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained. Click **Applications -> DDNS** to enter the configuration screen.

**Tip**-----

1. To use the DDNS feature, you need to have an account with one of the Service Providers in the drop-down menu first.
 2. This router supports two DDNS service providers: dyndns and no-ip.
-

DDNS Application Example:

If your ISP gave you a dynamic (changing) public IP address, you want to access your router remotely ([6.5 Remote Web Management](#)) but you cannot predict what your router's WAN IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. It lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If you obtain the following account from your dyndns.org service provider:

- ✓ User Name: tenda
- ✓ Password: 123456

✓ Domain Name: tenda.dyndns.org.

You want to use the PC at 218.58.98.3 to remotely access this router on port number 8090.

Configuration Procedures:

- ① **DDNS Service:** Select **Enable**.
- ② **Service Provider:** Select your DDNS service provider from the drop-down menu. Here in this example, select **dyndns**.
- ③ **User Name:** Enter the DDNS user name registered with your DDNS service provider. Here in this example, enter **tenda**.
- ④ **Password:** Enter the DDNS Password registered with your DDNS service provider. Here in this example, enter **123456**.
- ⑤ **Domain Name:** Enter the DDNS domain name with your DDNS service provider. Here in this example, enter **tenda.dyndns.org**.
- ⑥ Click **OK** to save your settings.

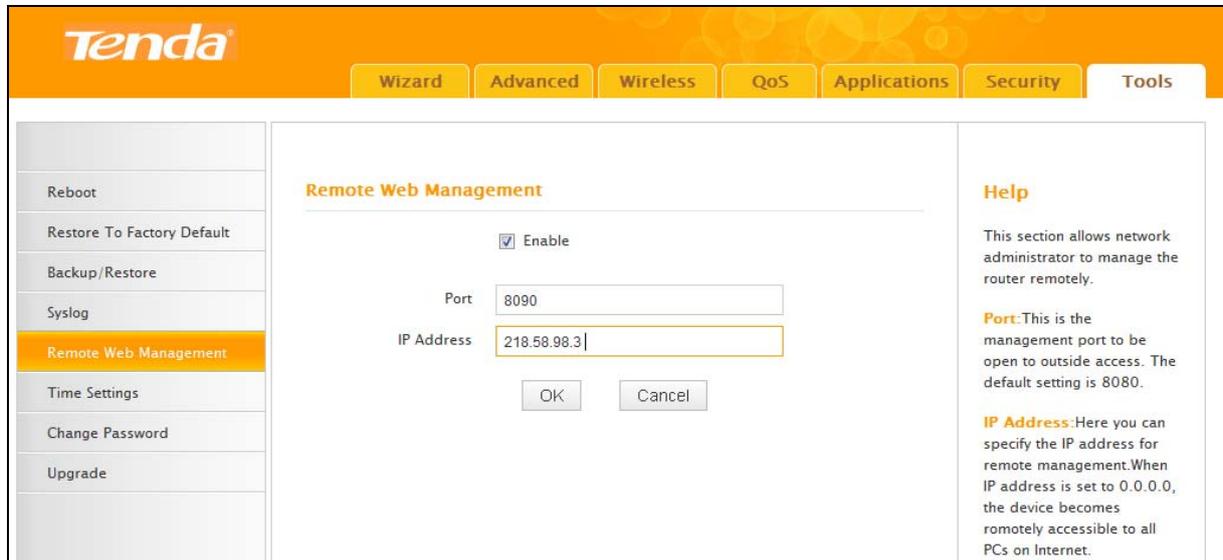
The screenshot shows the Tenda router's web interface. The top navigation bar includes 'Wizard', 'Advanced', 'Wireless', 'QoS', 'Applications', 'Security', and 'Tools'. The 'Applications' tab is selected, and the 'DDNS' sub-tab is active. The configuration fields are as follows:

DDNS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Service Provider	dyndns.org Sign up
Username	tenda
Password	123456
Domain Name	tenda.dyndns.org

Buttons: OK, Cancel

Help
DDNS (Dynamic DNS) Service allows you to assign a fixed domain name for your dynamic WAN IP address so that you can remotely access your LAN from the web. You need to have an account of any Service Providers in the drop-down menu first.
DDNS Service: Enter your Username, Password, and Domain Name (Host Name) that you registered with the DDNS service provider to enable the service for this router.

⑦ Click **Tools** -> **Remote Web Management**, enable the Remote Web Management feature, enter **8090** in the **Port** field, **218.58.98.3** in the **IP Address** field and then click **OK** to save your settings.



The screenshot shows the Tenda router's web interface. The top navigation bar includes 'Wizard', 'Advanced', 'Wireless', 'QoS', 'Applications', 'Security', and 'Tools'. The 'Tools' menu is selected, and the 'Remote Web Management' option is highlighted in the left sidebar. The main content area is titled 'Remote Web Management' and contains the following settings:

- Enable
- Port: 8090
- IP Address: 218.58.98.3

Below the input fields are 'OK' and 'Cancel' buttons. To the right of the configuration area is a 'Help' section with the following text:

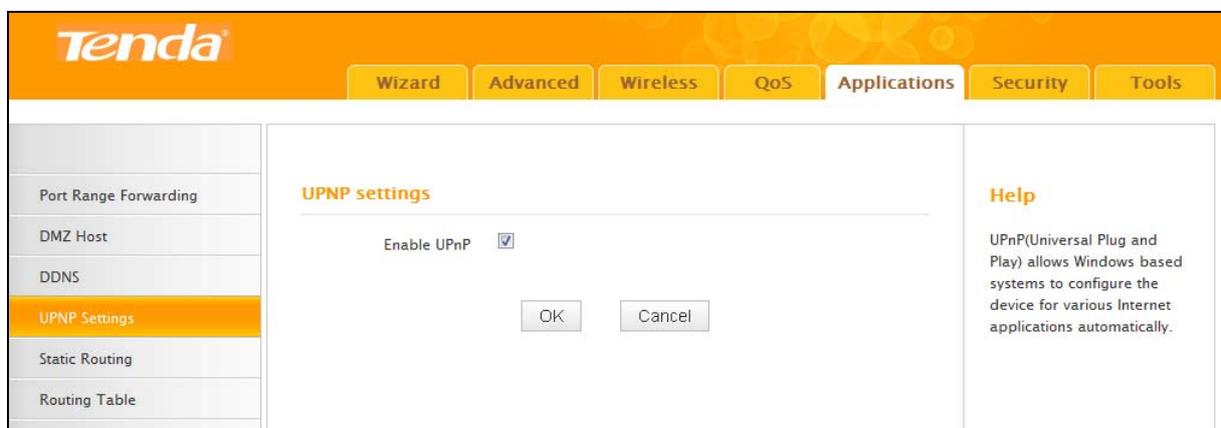
Help
This section allows network administrator to manage the router remotely.
Port: This is the management port to be open to outside access. The default setting is 8080.
IP Address: Here you can specify the IP address for remote management. When IP address is set to 0.0.0.0, the device becomes remotely accessible to all PCs on Internet.

Now you can access the router from the Internet by entering `http://tenda.dyndns.org:8090` in your browser.

4.4 UPNP

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 **Applications -> UPnP Settings** to enter the configuration screen. The UPnP feature is enabled by default.



4.5 Static Routing

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. However, when there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP domains to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing. In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically. If you want to use static routing, make sure the router's DHCP function is disabled.

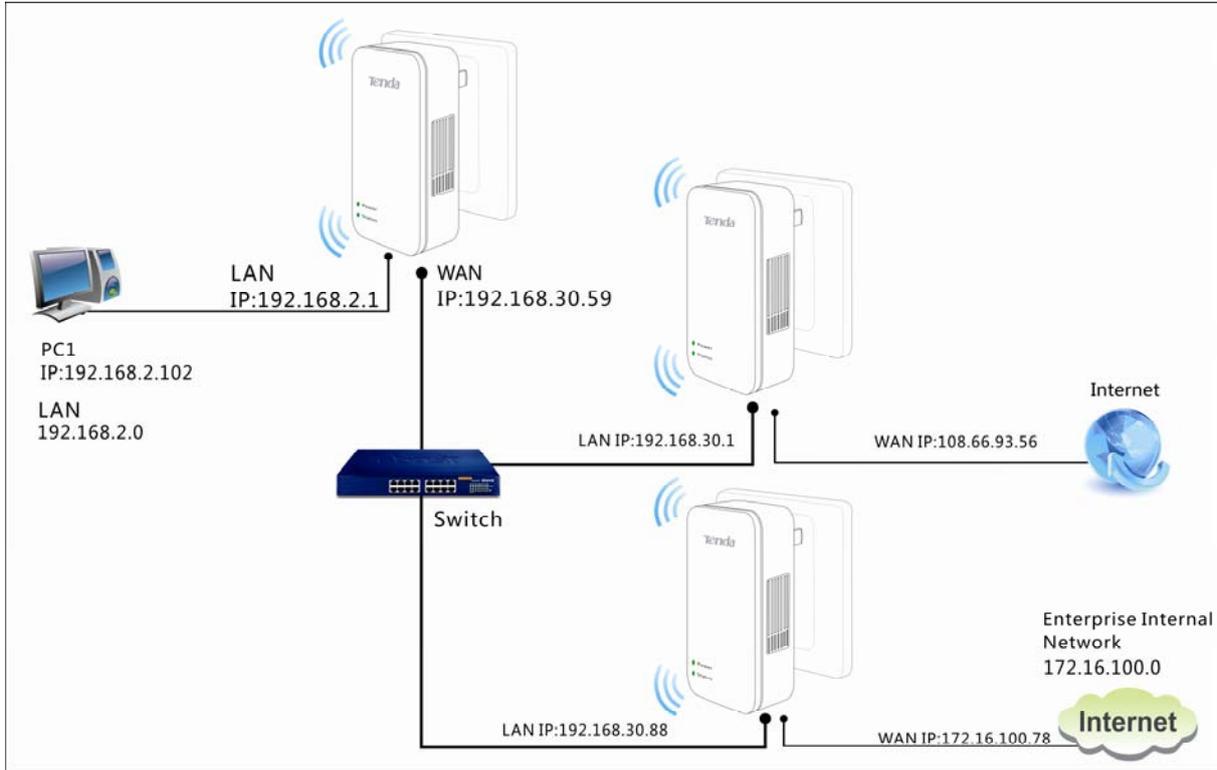
Click **Applications -> Static Routing** to enter the configuration screen.



Tip

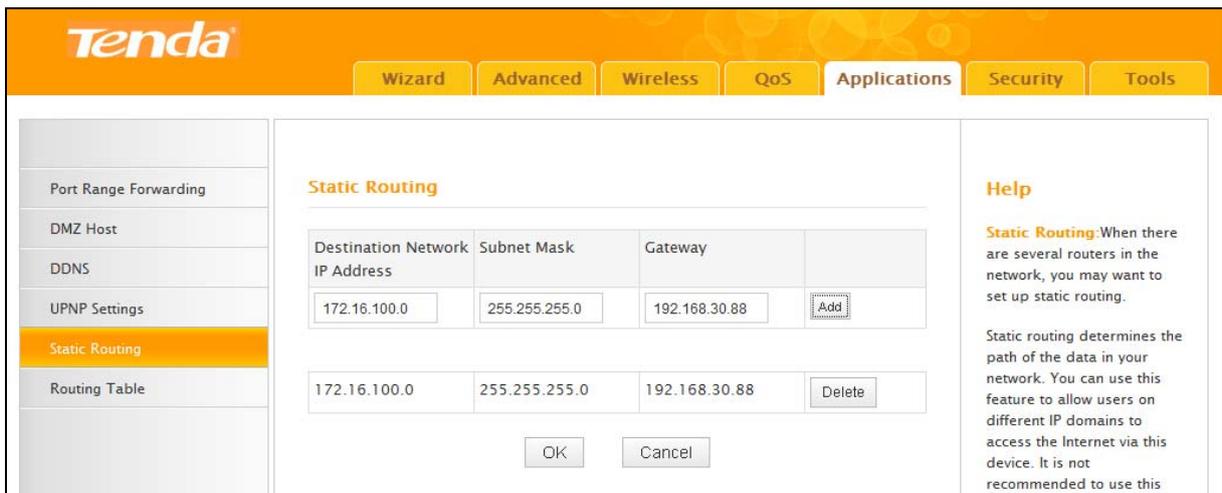
1. Gateway must be on the same IP segment as WAN or LAN segment as the router.
2. Subnet Mask must be entered 255.255.255.255 if destination IP address is a single host.

Static Route Application Example - Gateway IP address on the same IP segment as WAN IP:



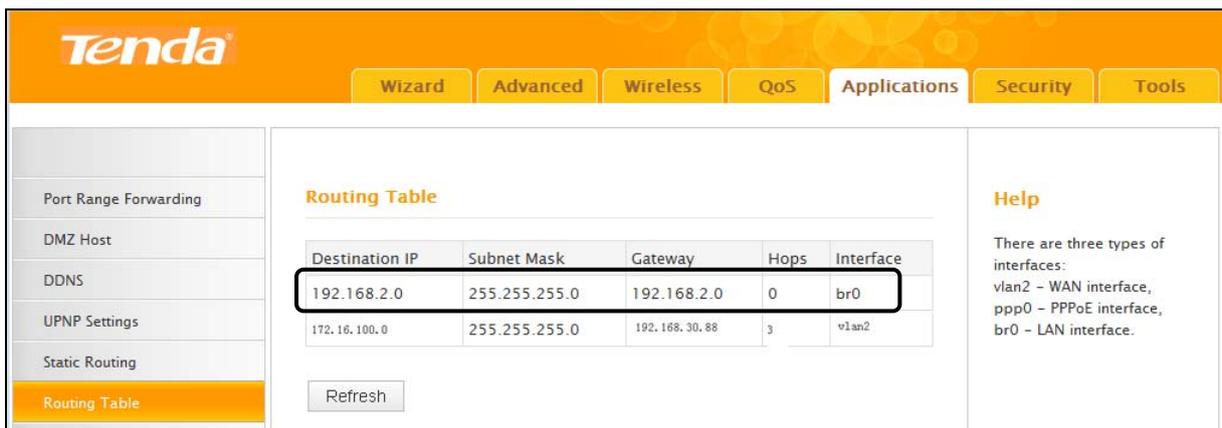
For example, your company internal network and Internet are on different IP net segment and you want PCs on your LAN to access Internet and your company internal network via the Tenda Router. You can simply configuring static routes on the Tenda Router. The figure above depicts this application scenario.

Configuration Procedures:

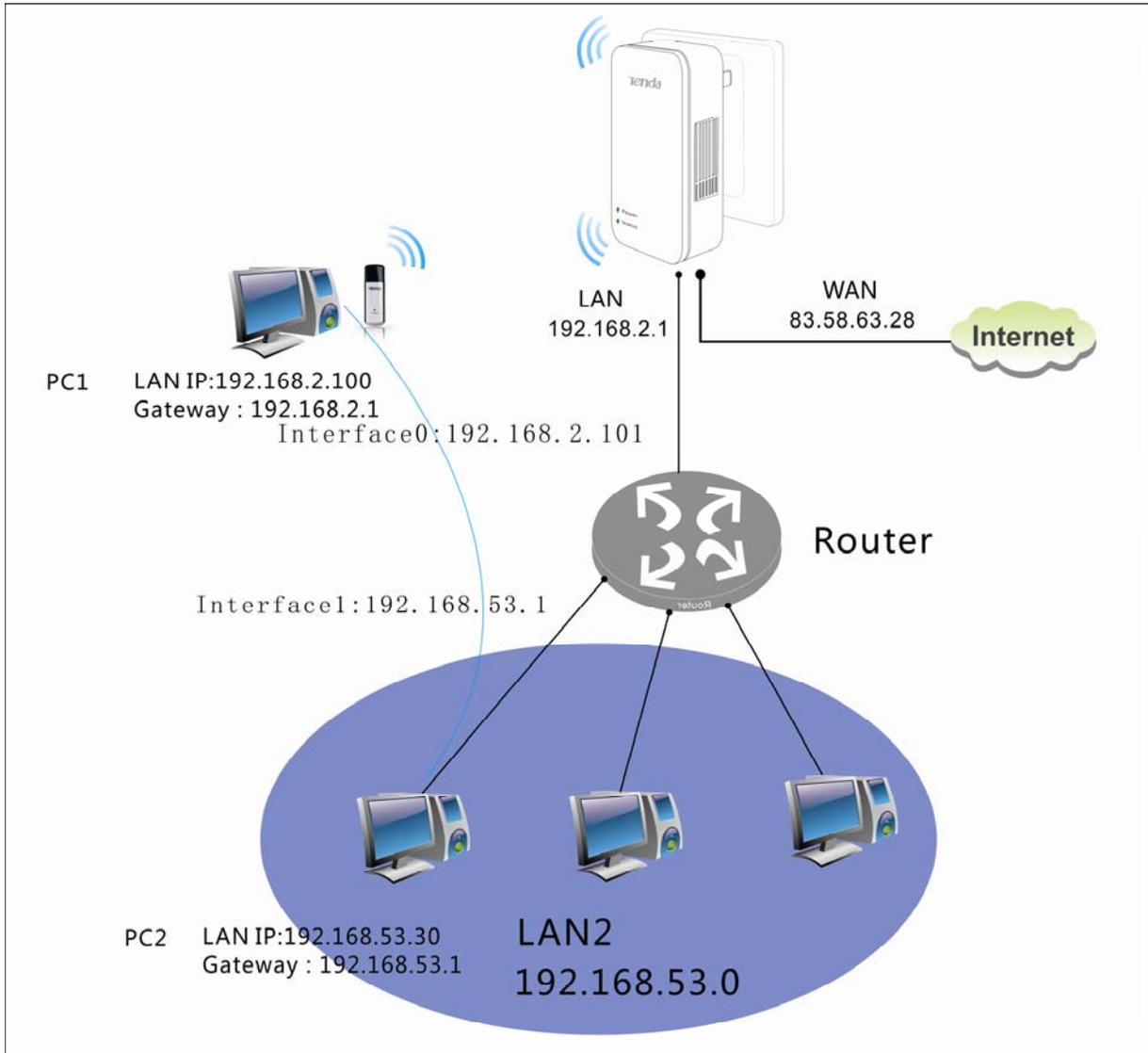


- ① **Destination Network IP Address:** The IP address of the final destination. Enter your corporate internal network address: 172.16.100.0.
- ② **Subnet Mask:** Enter the subnet mask of your corporate internal network: 255.255.255.0.
- ③ **Gateway:** Enter the gateway IP address to your corporate internal network: 192.168.30.88
- ④ Click **Add** to add a static route.
- ⑤ Click **OK** to save your settings.

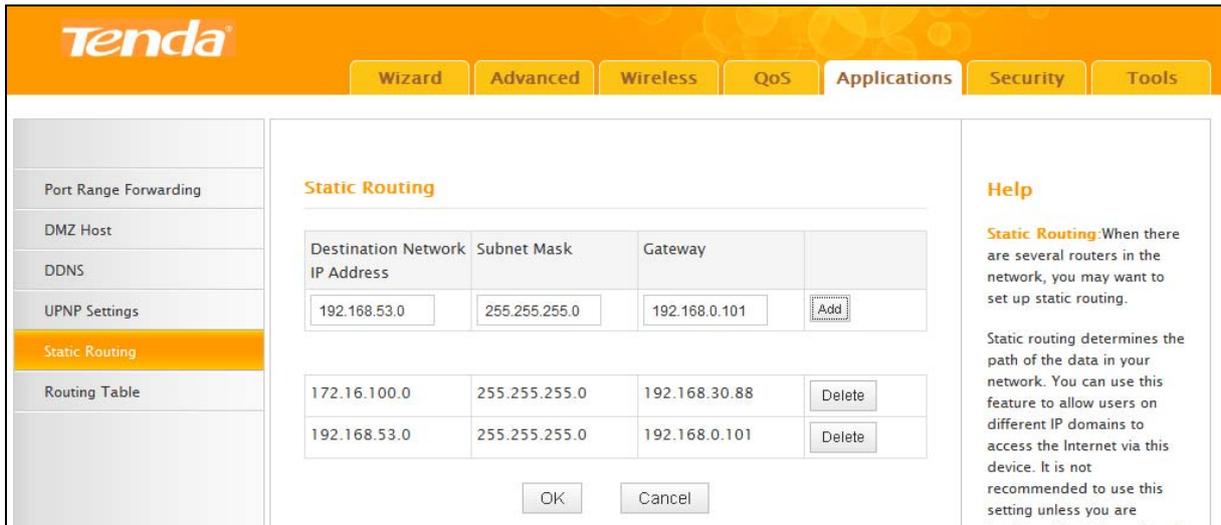
Click **Applications -> Routing Table** to view your static route entry. If it does not display, go to **Tools** to reboot your router. Enter the router's management interface. When the router successfully connects to the Internet, the following screen will display:



Static Route Application Example - Gateway IP address on the same IP segment as LAN IP:



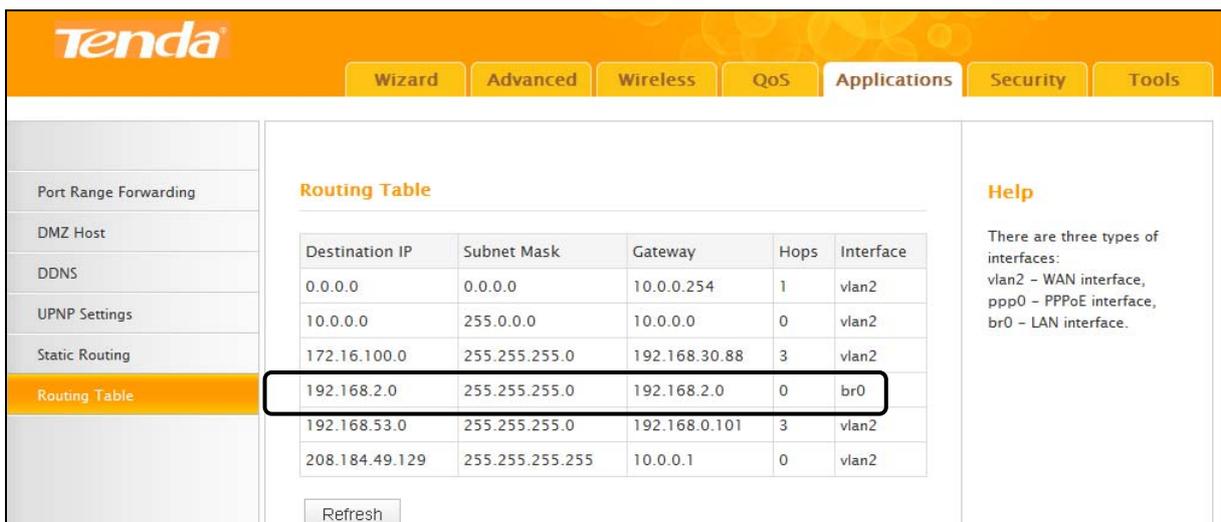
As seen in the above figure, PC2 on LAN2 connects with the Tenda Router via the Router; PC1 on LAN1 accesses Internet via the Tenda Router that performs NAT. You can configure static routes to implement mutual communication between PCs on LAN1 and LAN2.



Configuration Procedures:

- ① **Destination Network IP Address:** Enter 192.168.53.0.
- ② **Subnet Mask:** Enter 255.255.255.0.
- ③ **Gateway:** Enter 192.168.0.101.
- ④ Click **Add** to add the rule.
- ⑤ Click **OK** to save your settings.

Click **Applications** -> **Route Table** to view your static route entry. If it does not display, go to **Tools** to reboot your router. Enter the router's management interface. When the router successfully connects to the Internet, the following screen will display:



4.6 Routing Table

Click **Applications** -> **Routing Table** to view the router's route table.

Routing Table

Destination IP	Subnet Mask	Gateway	Hops	Interface
0.0.0.0	0.0.0.0	10.0.0.254	1	vlan2
10.0.0.0	255.0.0.0	10.0.0.0	0	vlan2
172.16.100.0	255.255.255.0	192.168.30.88	3	vlan2
192.168.2.0	255.255.255.0	192.168.2.0	0	br0
192.168.53.0	255.255.255.0	192.168.0.101	3	vlan2
208.184.49.129	255.255.255.255	10.0.0.1	0	vlan2

Refresh

Help

There are three types of interfaces:
 vlan2 – WAN interface,
 ppp0 – PPPoE interface,
 br0 – LAN interface.



Knowledge Center

- 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.
- Hops:** This stands for the number of routers between your network and the destination.
- Interface:** The interface between your router and the final destination.

5 Security

This router provides three security policies: MAC filter, client filter and URL filter.

- To restrict your LAN PCs to access certain websites on Internet via URL, see [URL Filter](#).
- To restrict your LAN PCs to access Internet via MAC addresses, see [MAC Filter](#).
- To restrict your LAN PCs to access certain services on Internet via their IP addresses, see [Client Filter](#).

5.1 URL Filter

This section allows you to control URL access. There are two options available: Disable and Deny.

A . Disable: Disable the URL Filter feature.

B . Deny: Disallow only the devices at specific IP addresses to access certain websites (containing specified URL characters) on Internet during the specific time period and/or

specific days of the week.

Click **Security** to enter the configuration interface.



Tip-----

1. Each rule can only include a single domain name. To filter multiple domain names, set a rule for each domain name.
2. Time/Day: If Time is set to 0:00 to 0:00 and Day is set to Sun ~ Sat, the rule will be applied 24 hrs/day.
3. If you have not set up the system time for this device, click **Tools -> Time Settings** to set up correct time and date for the rules to be effective. For more information, see [6.6 Time](#).

URL Filter Application Example:

If you want to disallow the computers (192.168.2.100~192.168.2.101) on your home network to access "YouTube" within the time period from 9 : 00 to 17 : 00 during working days: Monday ~ Friday, then do as follows:

Configuration Procedures:

- ① **Filter Mode:** Select Deny.
- ② **Select:** Select a rule ID, for example, (1).
- ③ **Description:** Briefly describe the current rule, say, yahoo, (It can only consist of numbers, letters, or underscore). This field is optional.
- ④ **Start IP/End IP:** Enter 100-101.
- ⑤ **URL Character String:** Enter the domain name you wish to filter out. Here in this example,

enter YouTube.

⑥ **Time:** Specify a time period for the current rule to take effect. Here in this example, select 9:00~17:00.

Day: Select a day, or several days of the week for the current rule to take effect. Here in this example, select Mon ~ Fri.

⑦ Click **OK** to save your settings.

5.2 MAC Filter

This section allows you to restrict specific clients to access the Internet via the devices' MAC addresses. Each PC has at least an installed network adapter with a unique MAC address. Three options are available: Disable, Forbid Only and Permit Only.

A. Disable: Disable the MAC Filter feature.

B. Forbid Only: Disallow only the devices at specific MAC addresses to access Internet during the specific time period and/or specific days of the week.

B. Permit Only: Allow only the devices at specific MAC addresses to access Internet during the specific time period and/or specific days of the week.

Click **Security -> MAC Address Filter Settings** to enter the configuration interface.



Tip

1. Time/Date: If Time is set to 0:00 to 0:00 and Day is set to Sun ~ Sat, the rule will be applied 24 hrs/day.
2. If you have not set up the system time for this device, click **Tools -> Time Settings** to set up correct time and date for the rules to be effective. For more information, see [6.6 Time](#).

MAC Filter Application Example:

Your router functions as an active DHCP server and delivers an unsecured wireless network. From time to time, you suffer from slow network speed and start to suspect unauthorized accesses to your network. You can set MAC filter rules to allow only your PC at 00:E4:A5:44:35:69 and your wireless device at 00:E4:A5:44:35:6A to access Internet via this router.

MAC Address Filter Settings

Filter Mode: Permit Only

Access Policy: (1)

Policy Name(Optional): yahoo

MAC Address: 00 : E4 : A5 : 44 : 35 : 69

Time: 0 : 0 ~ 0 : 0

Day(s): Mon ~ Fri

Enable: Clear this item: Clear

OK Cancel

Help

This section allows you to set the time specific clients can or cannot access the Internet via the devices' MAC addresses. Select a Policy from the drop-down menu and briefly describe it in the corresponding field. You can set the access restriction or permission in detail including the time period, and specific days of the week.

When Time is set to 0:0 to 0:0, the rule will be applied 24 hrs/day.

Configuration Procedures:

- ① **Filter Mode:** Select **Permit Only**.
- ② **Access Policy:** Select a rule ID, for example, (1).
- ③ **Policy Name:** Briefly describe the current rule, say, yahoo, (It can only consist of numbers, letters, or underscore). This field is optional.
- ④ **MAC Address:** Specify the MAC address of the computer that you want to restrict, 00:E4:A5:44:35:69.
- ⑤ **Time:** Keep the default of 0:00 ~ 0:00. The rule will be applied 24hrs/day.
- ⑥ **Day(s):** Select Mon ~ Fri.
- ⑦ **Enable:** Check to activate this rule.
- ⑧ Click **OK** to save your settings.
- ⑨ Repeat steps 1-7 to configure a rule for the MAC address "00:E4:A5:44:35:6A".

5.3 Client Filter

This section allows you to set the times specific clients can or cannot access services on the Internet via the devices' IP addresses and port numbers.

Click **Security -> Client Filter Settings** to enter the configuration interface. Select a Policy from the drop-down menu and briefly describe it in the corresponding field. You can set the access restriction or permission in detail including the time period, and specific days of the week. Three options are available: Disable, Forbid Only and Permit Only.

A. Disable: Disable the Filter feature.

B. Forbid Only: Disallow only the devices at specific IP addresses to access certain services on Internet during the specific time period and/or specific days of the week.

C. Permit Only: Allow only the devices at specific IP addresses to access certain services on Internet during the specific time period and/or specific days of the week.



Tip-----

1. The valid service port number range is from 1 to 65534.
2. Time/Day: If Time is set to 0:00 to 0:00 and Day is set to Sun ~ Sat, the rule will be applied 24 hrs/day.
3. If you have not set up the system time for this device, click **Tools -> Time Settings** to set up correct time and date for the rules to be effective. For more information, see [6.6 Time](#).

Client Filter Application Example:

To disallow your family member (PC IP address: 192.168.2.150) to access web pages within the time period of 8:00~18:00 from Monday to Friday

Client Filter Settings

Filter Mode: Forbid Only

Access Policy: (1)

Policy Name(Optional):

Start IP: 192.168.2.150

End IP: 192.168.2.150

Port: 80 ~ 80

Type: TCP

Time: 8 : 0 ~ 18 : 0

Day(s): Mon ~ Fri

Enable: Clear this item: Clear

OK Cancel

Help

This section allows you to set the times specific clients can or cannot access the Internet via the devices'IP addresses. Select a Policy from the drop-down menu and briefly describe it in the corresponding field. You can set the access restriction or permission in detail including the time period, and specific days of the week.

When Time is set to 0:0 to 0:0, the rule will be applied 24 hrs/day.

Configuration Procedures:

- ① **Filter Mode:** Select **Forbid Only**.
- ② **Access Policy:** Select a rule ID, for example, (1).
- ③ **Policy Name (Optional):** Briefly describe the current rule (It can only consist of numbers, letters, or underscore). This field is optional.
- ④ **Start IP:** Enter a starting IP address. Here in this example, enter 150.

- ⑤ **End IP:** Enter an ending IP address. Here in this example, enter 150.
 - ⑥ **Port:** Enter a service port number. Here in this example, enter 80.
 - ⑦ **Type:** Select a protocol for the traffic. If you are unsure, select **Both**.
 - ⑧ **Time:** Specify a time period for the current rule to take effect. Here in this example, select 8:00 ~18:00.
- Day(s):** Select a day, or several days of the week for the current rule to take effect. Here in this example, select Mon ~ Fri.
- ⑨ **Enable:** Check to enable the current rule.
 - ⑩ Click **OK** to save your settings.

6 Tools

6.1 Reboot

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



6.2 Restore to Factory Default Settings

Click **Tools -> Restore to Factory Default** to enter the configuration screen. Here you can reset the device to factory default settings.



Note-----

1. 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.
 2. Do not restore factory default settings unless the following happens:
 - You need to join a different network or unfortunately forget the login password.
 - You cannot access Internet and your ISP or our technical support asks you to reset the router.
-

The screenshot shows the Tenda web management interface. At the top, there is a navigation bar with the Tenda logo and several menu items: Wizard, Advanced, Wireless, QoS, Applications, Security, and Tools. The Tools menu is currently selected. On the left side, there is a sidebar menu with the following options: Reboot, Restore To Factory Default (highlighted), Backup/Restore, Syslog, Remote Web Management, Time Settings, Change Password, and Upgrade. The main content area is titled 'Restore To Factory Default' and contains the following text: 'Click this button to restore all settings to factory default.' Below this text is a button labeled 'Restore To Factory Default'. On the right side of the main content area, there is a 'Help' section with the following text: 'All settings will be set back to default.', 'Default Password: admin', 'Default IP Address: 192.168.2.1', and 'Default Subnet Mask: 255.255.255.0'.

The factory default settings are listed below:

- **IP Address:** 192.168.2.1
- **Subnet Mask:** 255.255.255.0.

For more factory default settings, see [2 Default Settings](#).

6.3 Back/Restore

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.

Click **Tools -> Back/Restore** to enter the configuration screen.

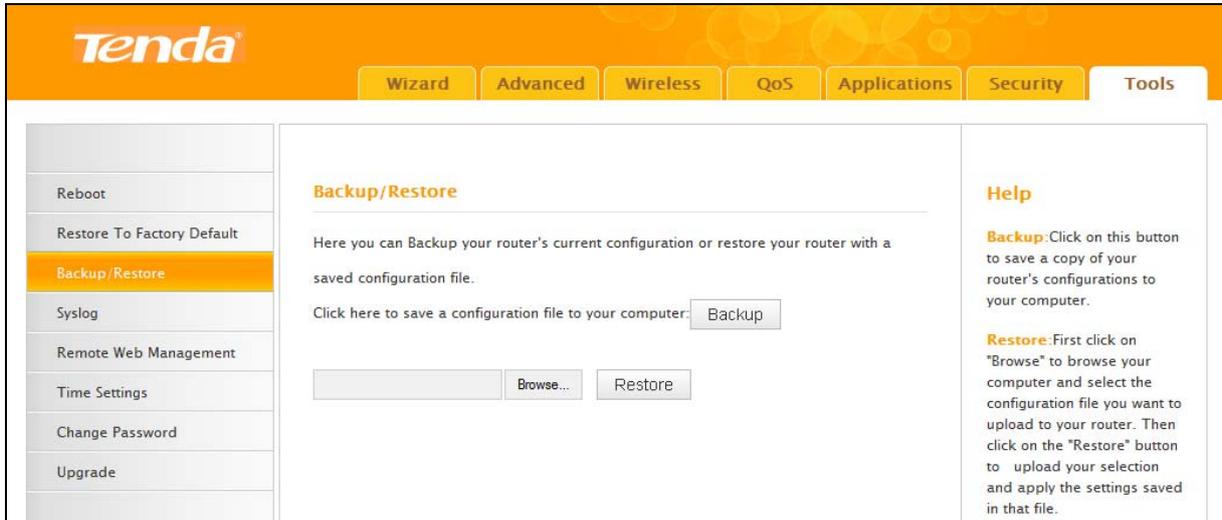


Tip

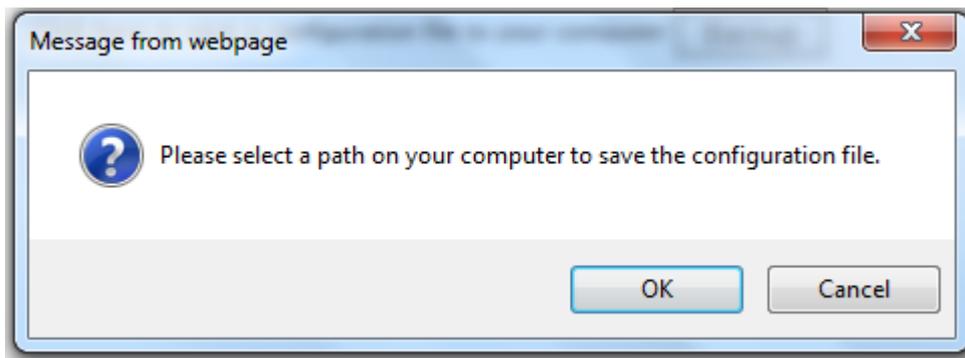
The default configuration file name is "RouterCfm.cfg". Do include the file name suffix of ".cfg" when renaming the file name to avoid problems.

To backup configurations

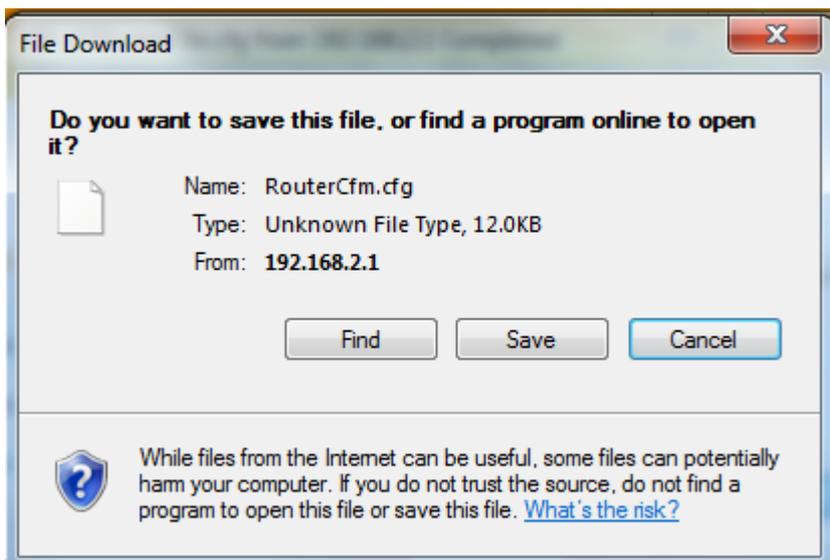
- ① Click **Backup**.



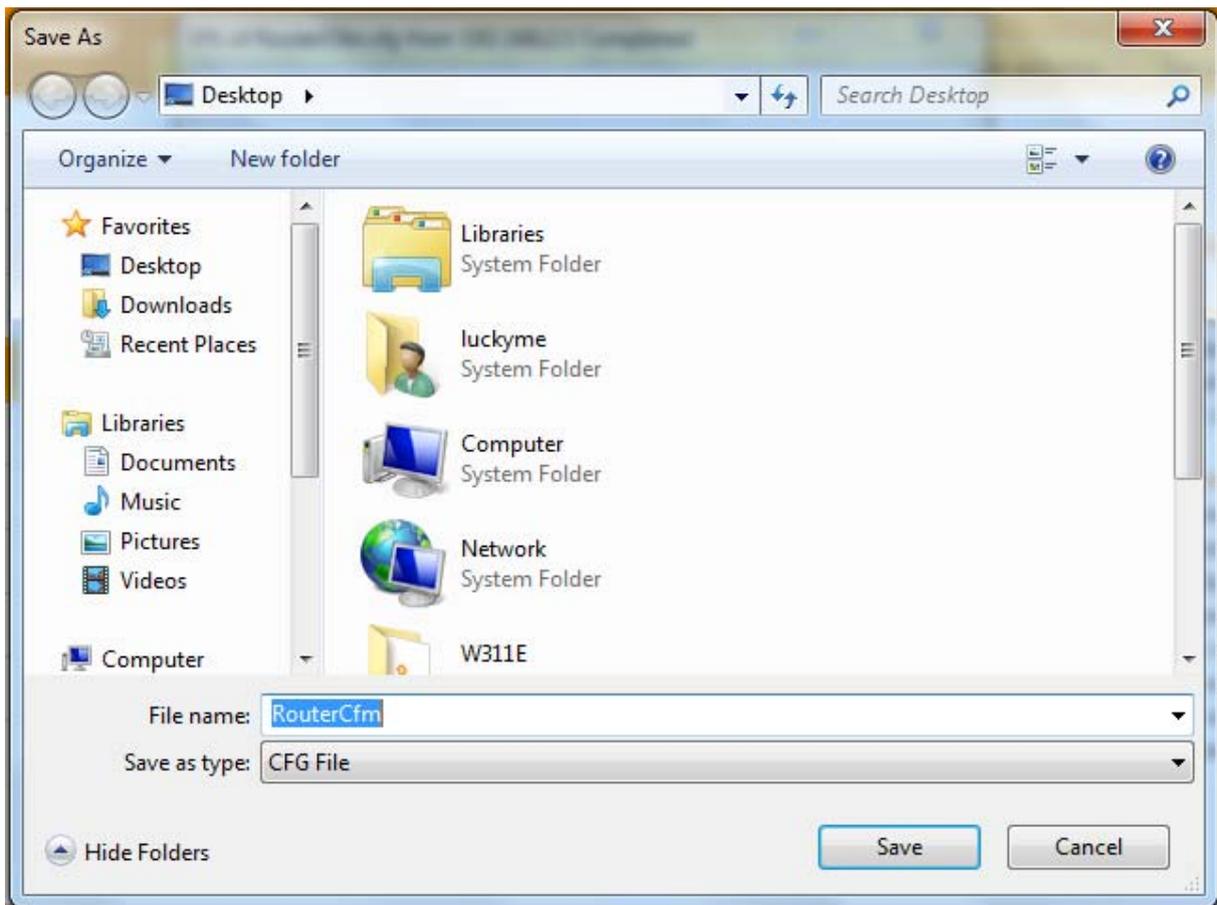
- ② Click **OK** on the appearing window.



- ③ Click **OK** on the appearing alert window.

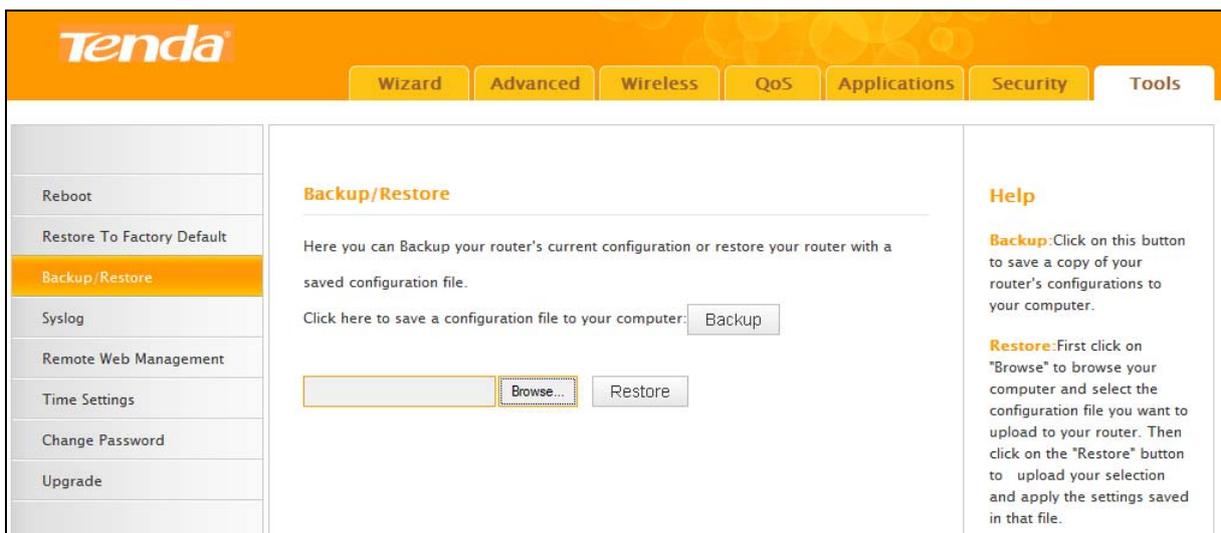


- ④ Select a local hard drive to save the file and click **Save**.

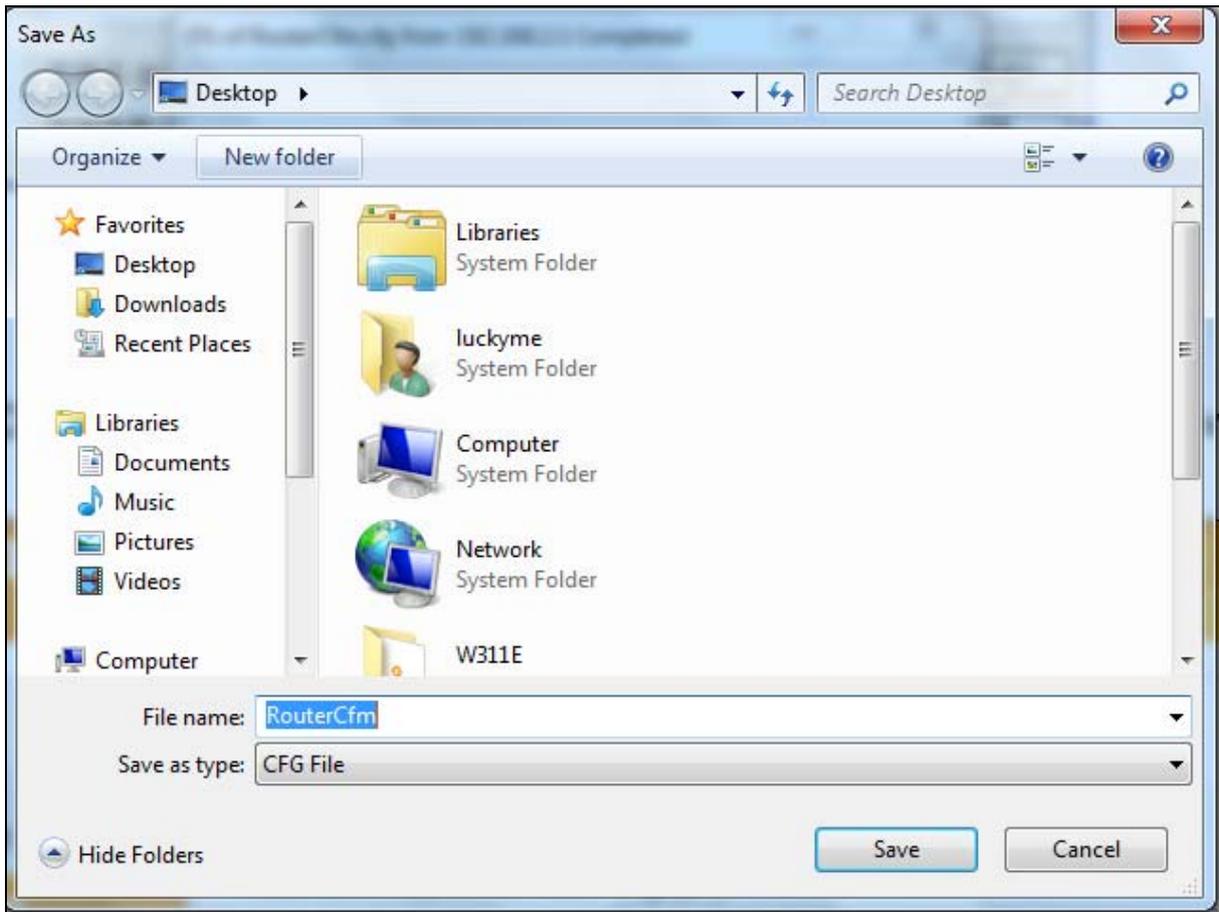


To restore configurations

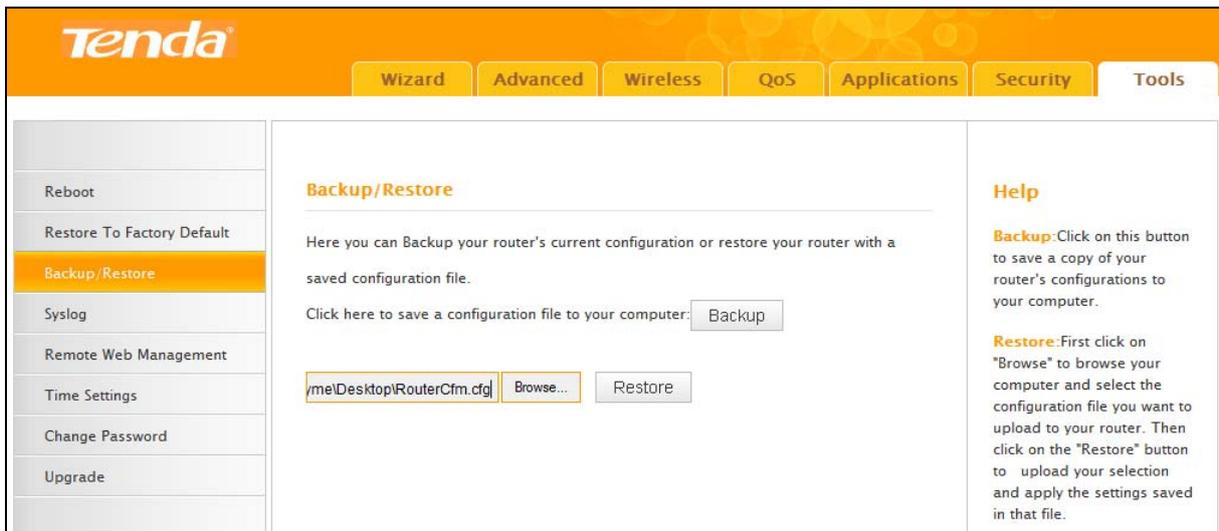
- ① Click **Browse**.



- ② Select the configuration file that is saved previously to your local hard drive and click **Open**.



- ③ Click the **Restore** button to reset your device to previous settings.



6.4 Logs

Click **Tools** -> **Syslog** to enter the logs screen. Here you can view the history of the device's actions.

Syslog			
Logs in page 1			
1	2011-04-01 00:00:00	main	System start
2	2011-04-01 00:01:27	system	interface vlan2 init
3	2011-04-01 00:01:28	system	DHCPC_DISCOVER sending
4	2011-04-01 00:01:37	system	DHCPC_DISCOVER sending
5	2011-04-01 00:01:37	system	DHCPC_DISCOVER received
6	2011-04-01 00:01:37	system	DHCPC_STATE_REQUESTING init sending

Up to 150 entries can be logged. After 150 entries, you can click **Refresh** to update the logs or click **Clear** to clear the earliest logs.

6.5 Remote Web Management

The Remote web management allows the device to be configured and managed remotely from the Internet via a web browser. Click **Tools** -> **Remote Web Management** to enter the configuration screen.



Knowledge Center-----

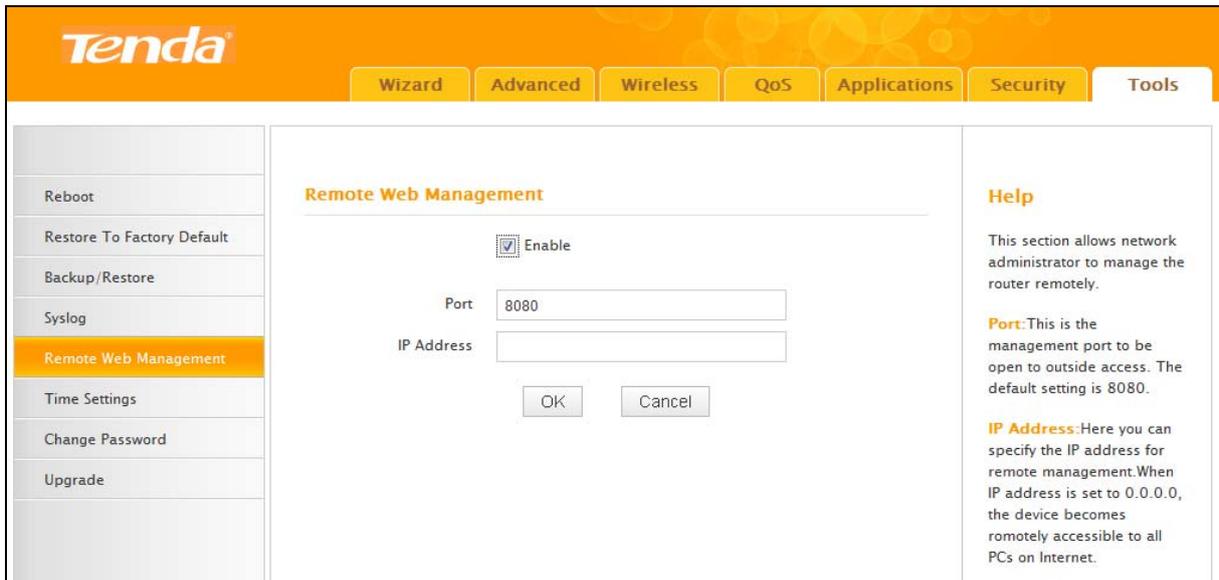
- 1. Port:** This is the management port to be open to outside access. The default setting is 8080. This can be changed.
- 2. IP Address:** Here you can specify the IP address for remote management (When set to **0.0.0.0**, the device becomes remotely accessible to all the PCs on Internet or other external networks).

Remote Web Management Application Example:

To access your router (WAN IP address: 102.33.66.88) at your home from the PC (218.88.93.33) at your office via the port number 8090

Configuration Procedures:

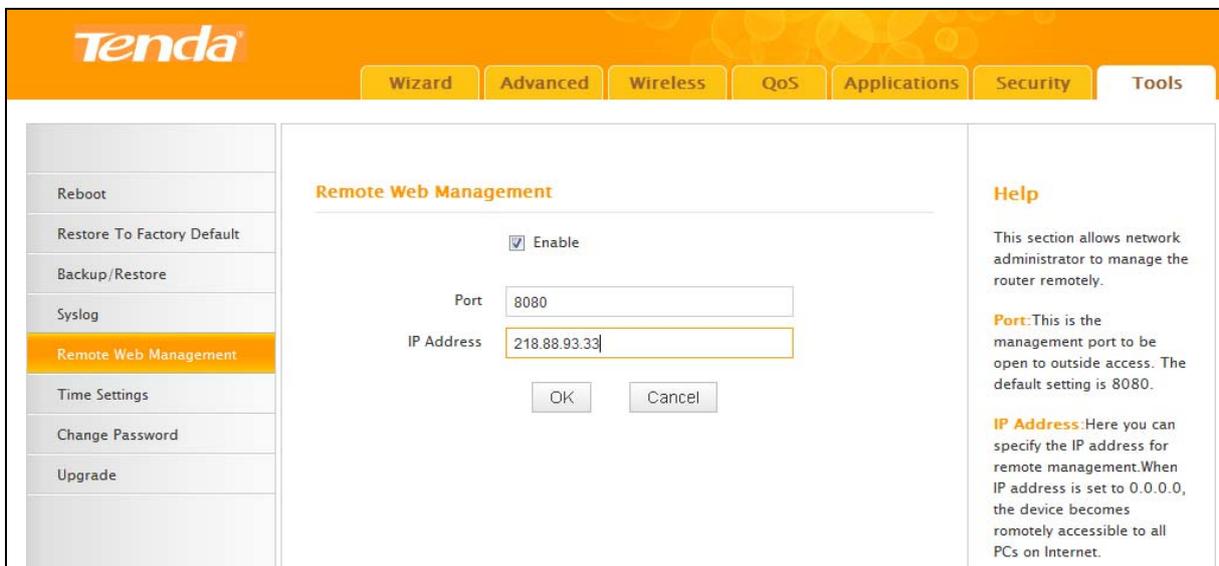
- ① **Enable:** Check to enable the remote Web management feature.



- ② **Port:** This is the management port to be open to outside access. Here in this example, enter 8090.

- ③ **IP Address:** Specify the IP address for remote management. Here in this example, enter "218.88.93.33".

- ④ Click **OK** to save your settings.



Now you can access the router at your home by simply entering `http://102.33.66.88:8090` in the web browser on the PC at your office.



Tip-----

1. For better security, customize a port number between 1025 and 65535 for the 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.
4. You must change the default login password before you can enable this feature.

6.6 Time

Click **Tools -> Time** to enter the time screen.

A. Sync with Internet time servers

Configuration Procedures:

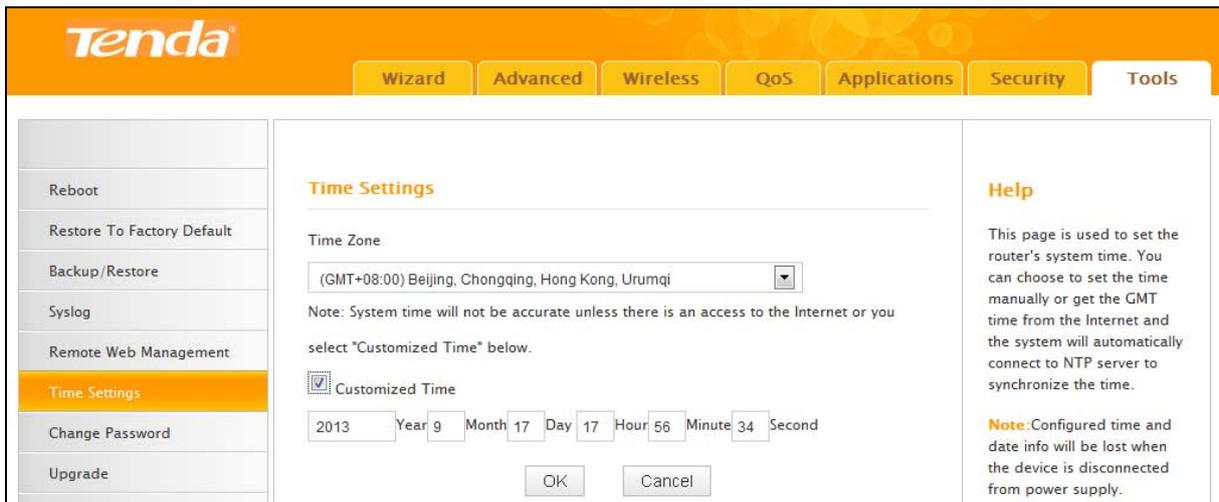
- ① Select your time zone.
- ② Click **OK** to save your settings.



Tip

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.

B. Set Time and Date Manually/Sync with Your PC



Configuration Procedures:

- ① Check **Customized Time**.
- ② Specify correct time and date.
- ③ Click **OK** to save your settings.

And then go to **Status** screen (**Advanced -> Status**) to make sure the system time is correctly updated.



6.7 Login Password

Click **Tools -> Change Password** to enter the configuration screen. It is strongly recommended that you change the factory default login password. Otherwise, anyone in your network can access this utility to change your settings.



Tip-----

1. The default login password is admin. Please change it for better security.
 2. The password can include 0-12 characters. If no character is entered (left blank), no password is set.
-

Configuration Procedures:

- ① **Old Password:** Enter the old password.
- ② **New Password:** Input a new password.
- ③ **Confirm New Password:** Re-enter the new password for confirmation.
- ④ Click **OK** to save your settings.

6.8 Firmware Upgrade

Click **Tools -> Upgrade** to enter the configuration screen. Firmware upgrade is released periodically to improve the functionality of your device and also to add new features. If you run into a problem with a specific feature of the device, log on to our website (www.tendacn.com) to download the latest firmware to update your device. If you run into a problem with a specific feature of the device, log on to our website (www.tendacn.com) to download the latest firmware to update your device.

**Note**

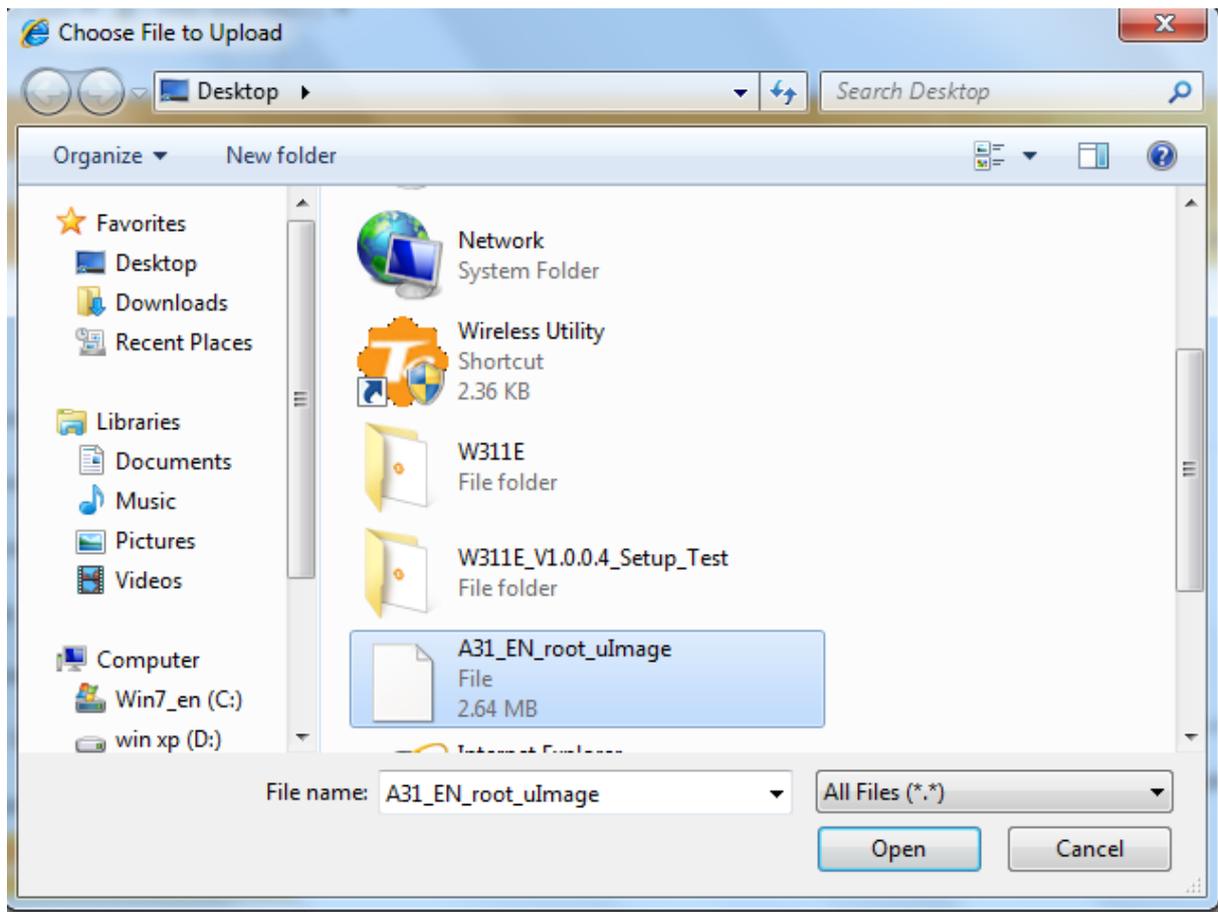
- 1 . Before you upgrade the firmware, make sure you are having a correct firmware. A wrong firmware may damage the device.
- 2 . It is advisable that you upgrade the device's firmware over a wired connection. DO NOT interrupt the power to the router when the upgrade is in process otherwise the router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

Configuration Procedures:

- ① Click **Browse**.

The screenshot displays the Tenda router's web management interface. At the top, there is an orange header with the Tenda logo and a navigation menu with tabs for Wizard, Advanced, Wireless, QoS, Applications, Security, and Tools. On the left side, there is a vertical sidebar menu with options: Reboot, Restore To Factory Default, Backup/Restore, Syslog, Remote Web Management, Time Settings, Change Password, and Upgrade (which is highlighted in orange). The main content area is titled "Upgrade" and contains the following text: "By upgrading the router's software, you'll get new features." Below this, it says "Select the firmware file:" followed by a text input field, a "Browse..." button, and an "Upgrade" button. Underneath, it displays "Current System Version: V5.07.53_en; Publishing Date: Sep 10 2013". A note follows: "Note: Do not power off the router during the upgrade and you can only use a computer that is plugged into one of the LAN ports of this router to complete the upgrade to avoid damaging the router. The router will reboot automatically after the upgrade." On the right side of the main content area, there is a "Help" section with the text: "The latest firmware can be found at www.tendacn.com. Be sure to follow the instructions carefully. Once you have downloaded the firmware file from our website and saved it to your computer, click on 'Browse' to select the file. Then click on 'Upgrade' to start the process and reboot the router."

- ② Select the upgrade file and click **Open**.



- ③ Click **Upgrade** and wait until the upgrade progress indicator bar displays 100% completed.

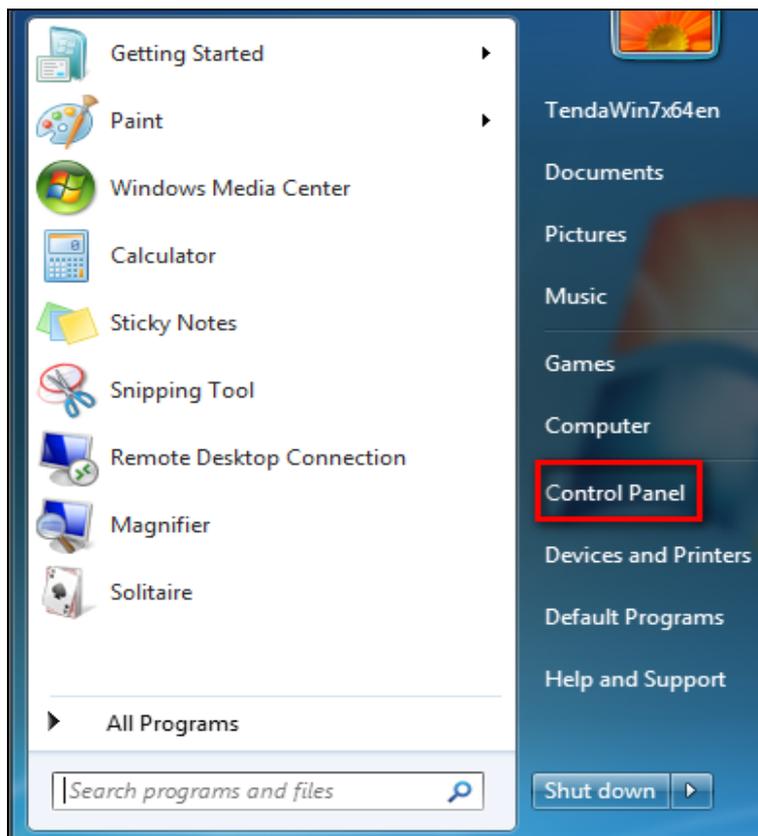
When upgrade is completed, view the **Current System Version**. It should display the firmware you load.

IV Appendix

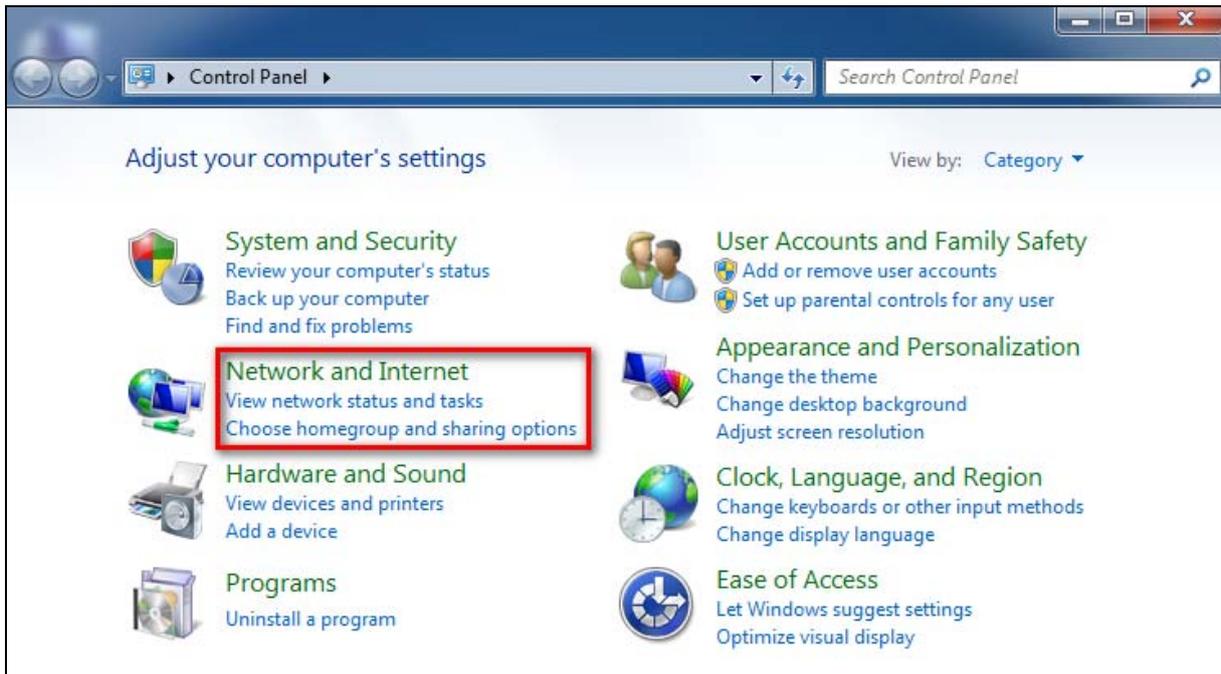
1 Configure PC TCP/IP Settings

Windows 7

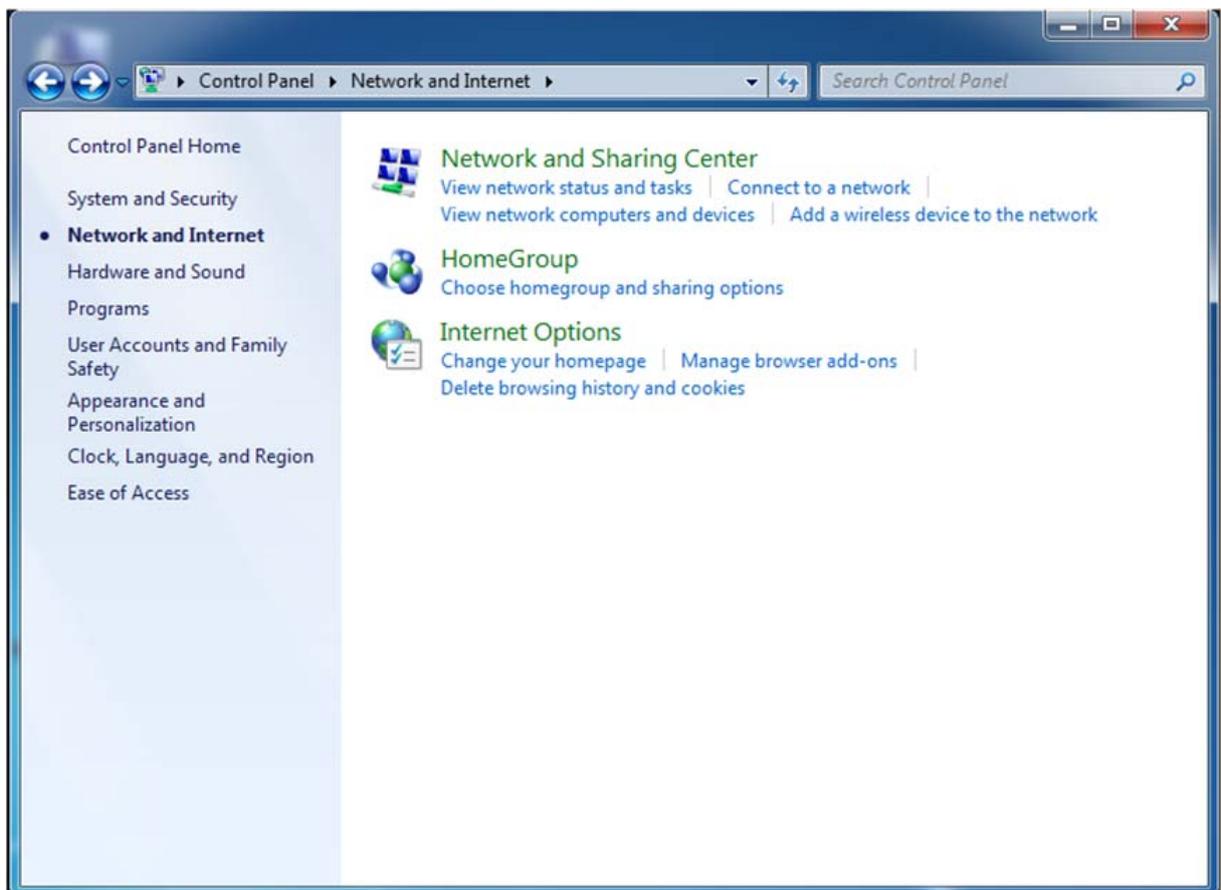
① Click **Start -> Control Panel**.



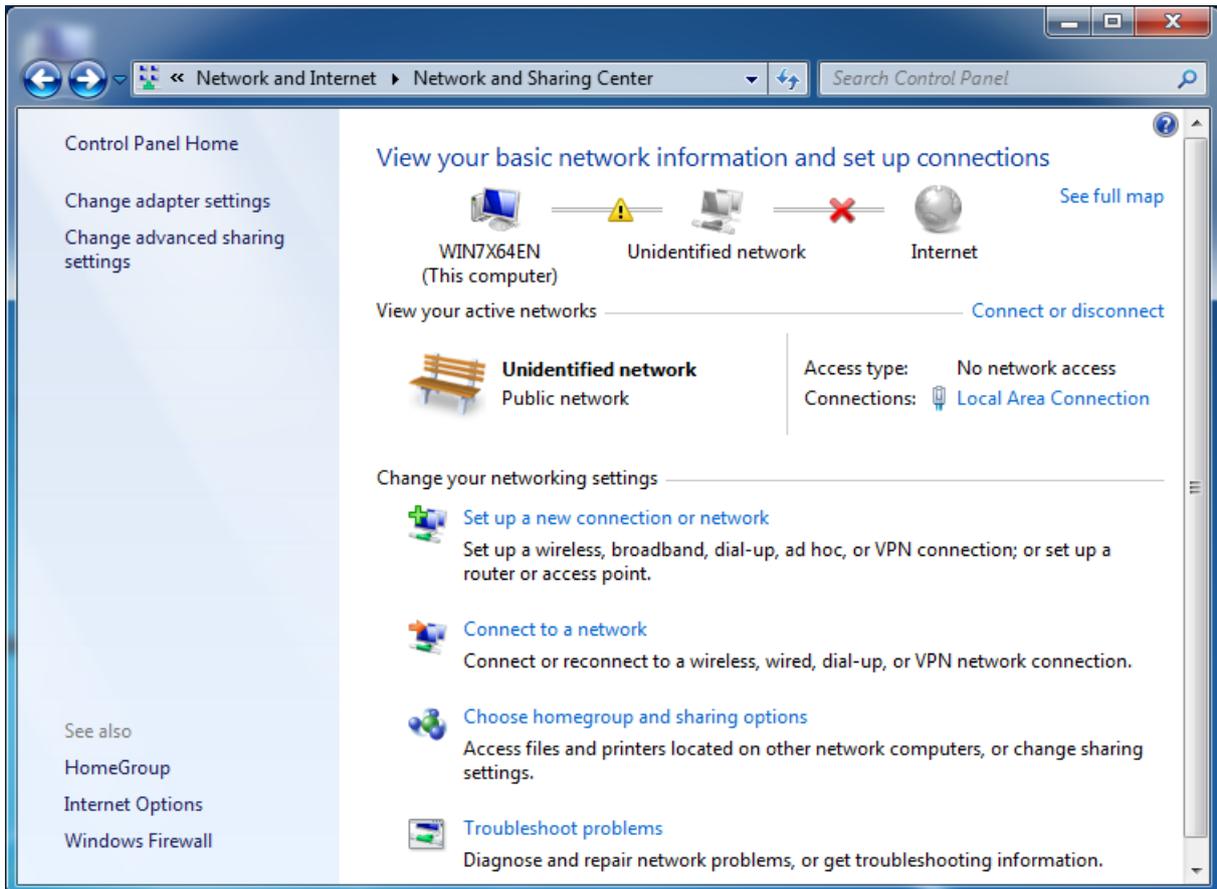
② Click **Network and Internet**.



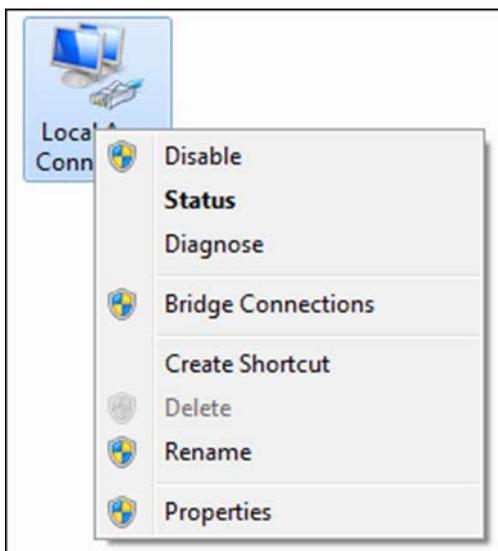
③ Click **Network and Sharing Center**.



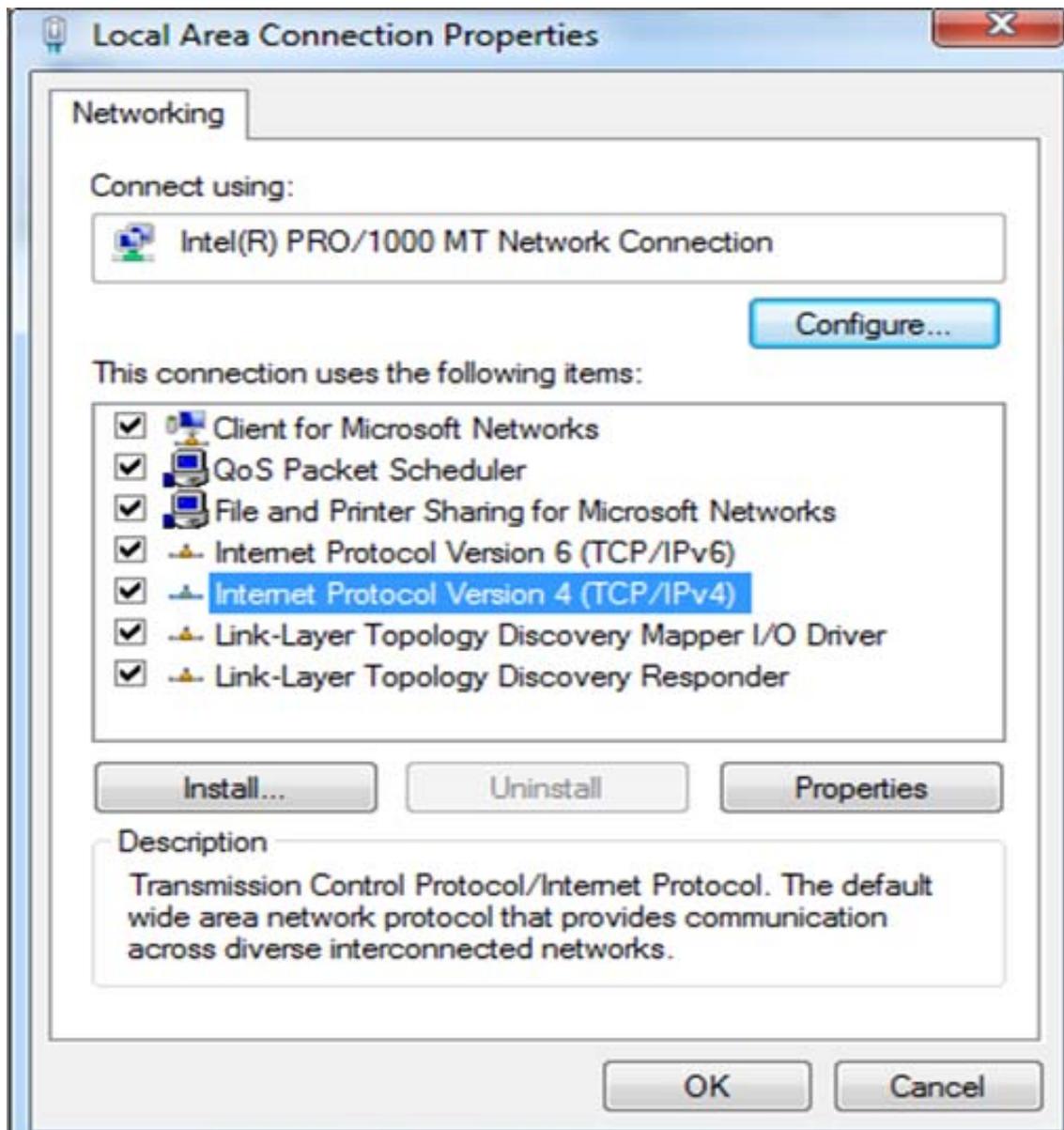
④ Click **Change adapter settings**.



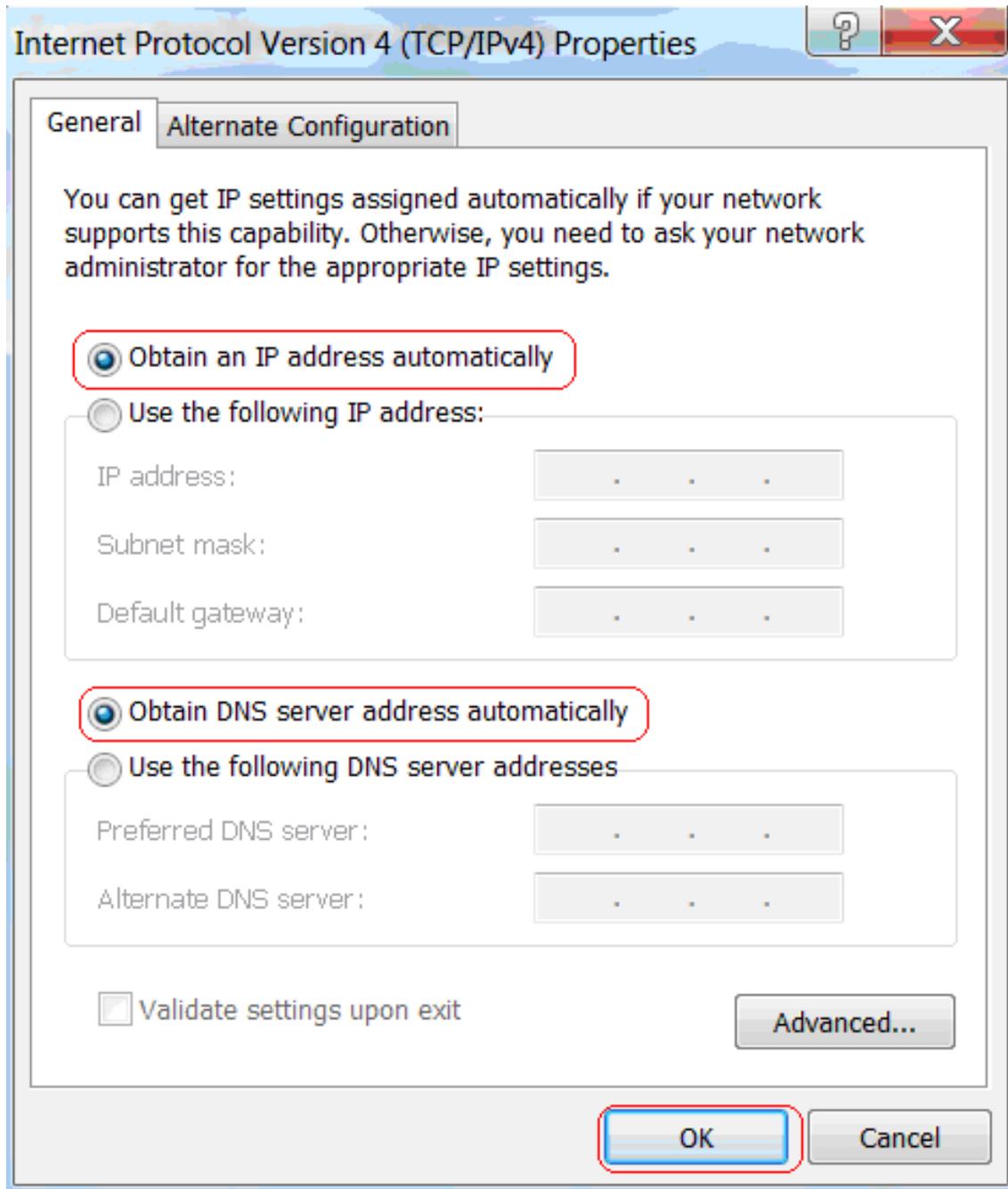
⑤ Click **Local Area Connection** and select **Properties**.



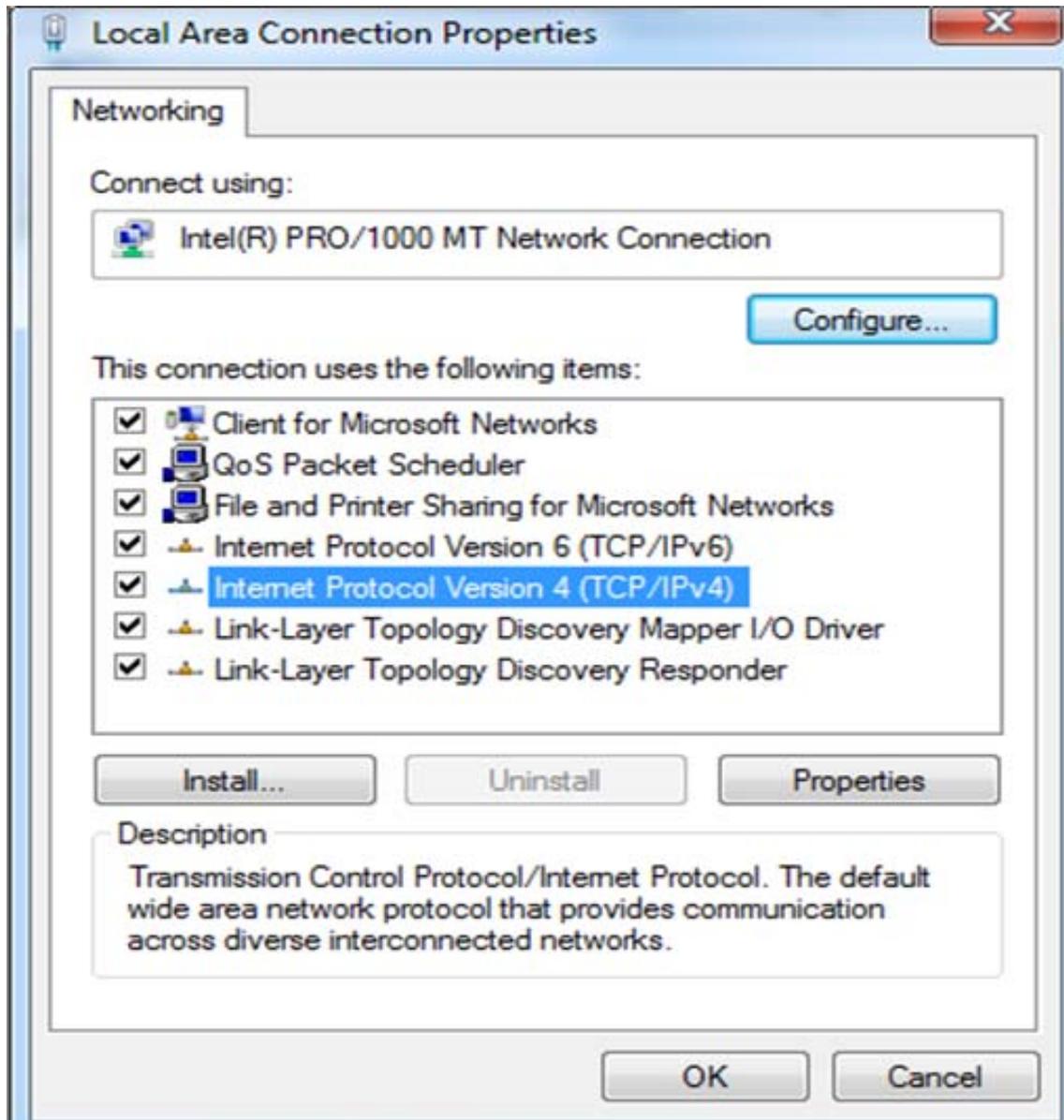
⑥ Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



- 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

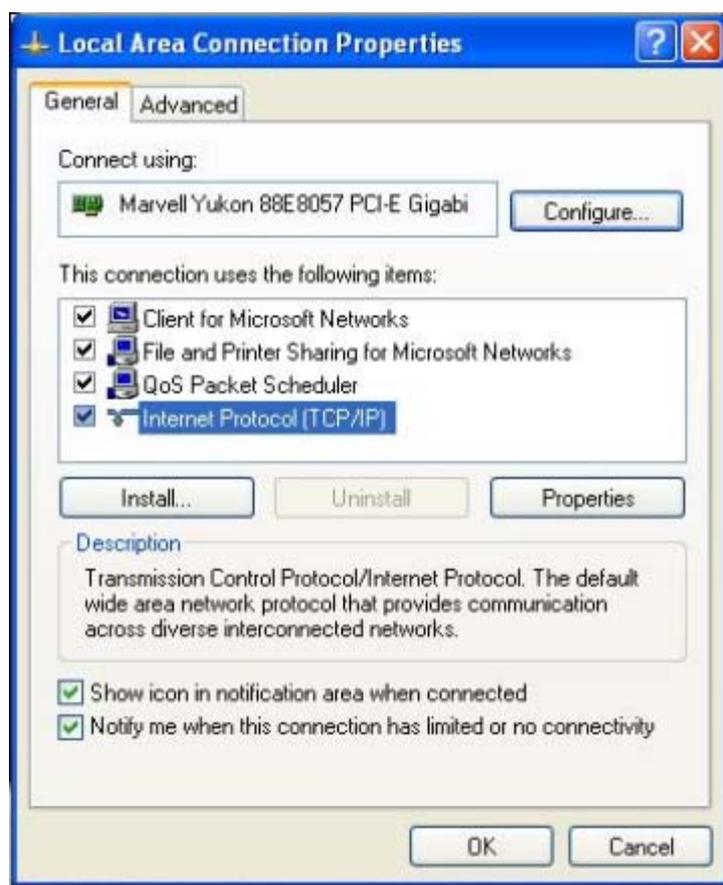
- ① Right-click **My Network Places** and select **Properties**.



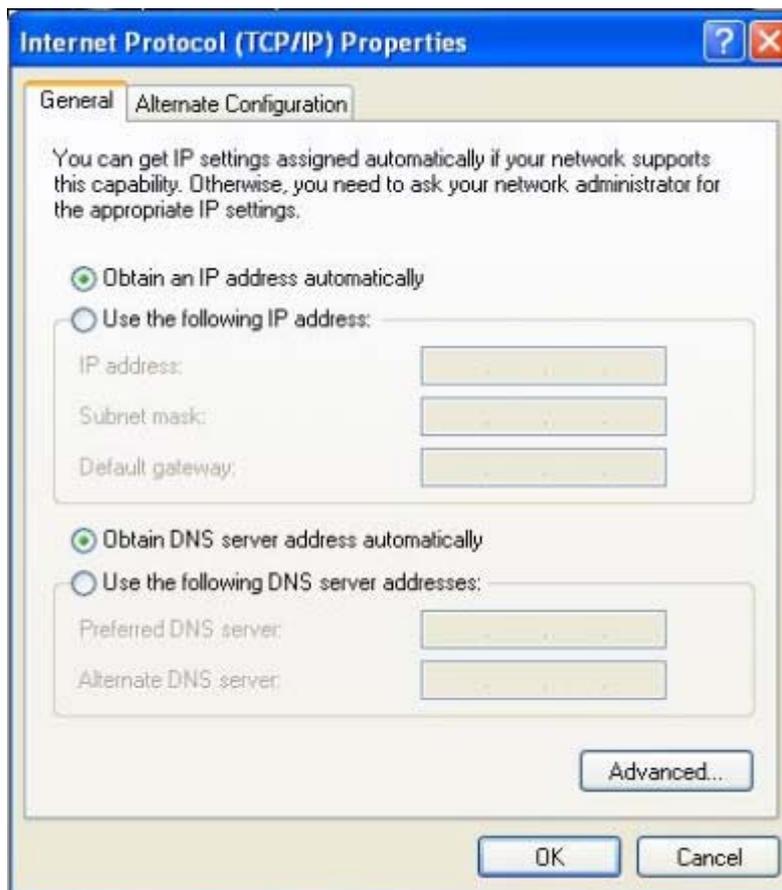
- ② Right click **Local Area Connection** and select **Properties**.



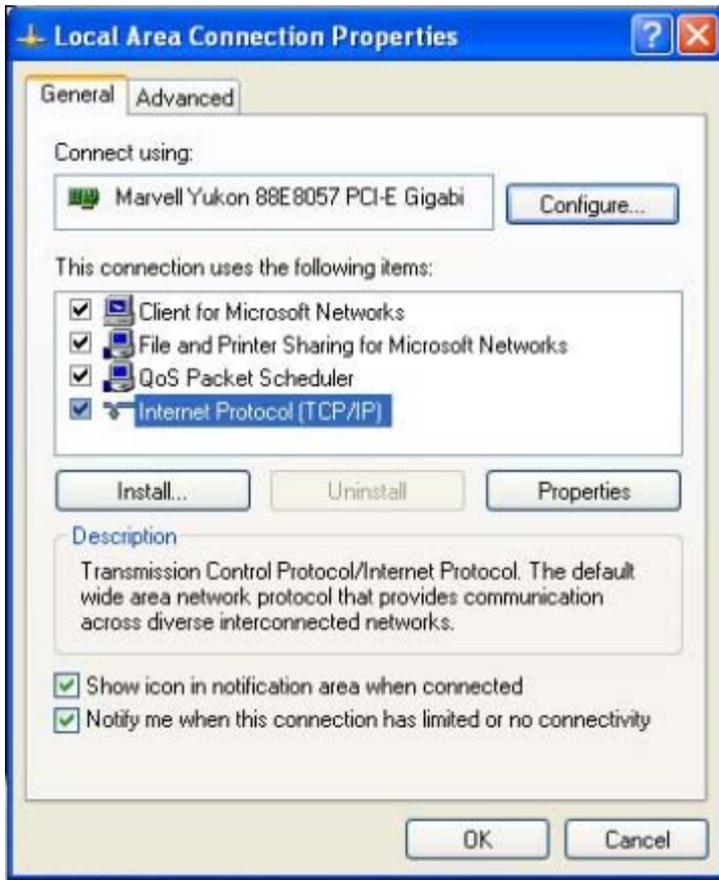
③ Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



- 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 Default Settings

Item		Default Settings
Login	IP Address	192.168.2.1
	Login Password	admin
Internet Connection Type		Hotel Mode (Dynamic IP)
WAN MAC Address		Find it on the label attached to the device
MTU		PPPoE: 1492 DHCP: 1500 Static IP: 1500
WAN Speed		Auto-negotiation
DNS		Disabled
LAN Settings	IP Address	192.168.2.1
	Subnet Mask	255.255.255.0
	DHCP Server	Enabled
	IP Pool	192.168.2.100~192.168.2.150

	System Time	By default, system automatically synchronizes with Internet time servers. Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Wireless	Wireless	Enabled
	Primary SSID (Network Name)	Tenda_XXXXXX ("XXXXXX" is the last six characters of the device's MAC address. You can find it on the label attached to the device.)
	Secondary SSID	Disabled
	Wireless Working Mode	Wireless AP
	Network Mode	11b/g/n mixed
	SSID Broadcast	Enabled
	AP Isolation	Disabled
	Channel	AutoSelect
	Channel Bandwidth	20/40
	Extension Channel	AutoSelect
	WMM Capable	Enabled
	APSD Capable	Disabled
	Security Mode	Disabled
Others	Remote Web Management	Disabled
	Bandwidth Control	Disabled
	Traffic Statistics	Disabled
	DMZ Host	Disabled
	UPnP	Enabled
	Security	Disabled

3 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.

If your problem is not covered here, please feel free to go to www.tendacn.com to find a solution or email your problems to: support@tenda.com.cn or support02@tenda.com.cn. We will be more than happy to help you out as soon as possible.

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

- Make sure the power LED on the device's front panel is on.
- Make sure Ethernet cables are connected properly.
- 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 192.168.2.2~192.168.2.254. Or you can select the "Obtain an IP address automatically" option.
- Try a different browser or delete your existing browser's cache and cookies.
- Check the IP address you entered in your browser. It should be http://192.168.2.1.
- Open your browser and click **Tools -> Internet Options -> Connections -> LAN Settings**, uncheck the **Use a proxy server for your LAN** option.
- Press the reset button on the device with a needle for 10seconds to restore factory default settings and then re-access the device.

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

Press the reset button on the device with a needle for 10seconds to restore 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 192.168.2.1.
- 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.

4 Remove Wireless Network from Your PC

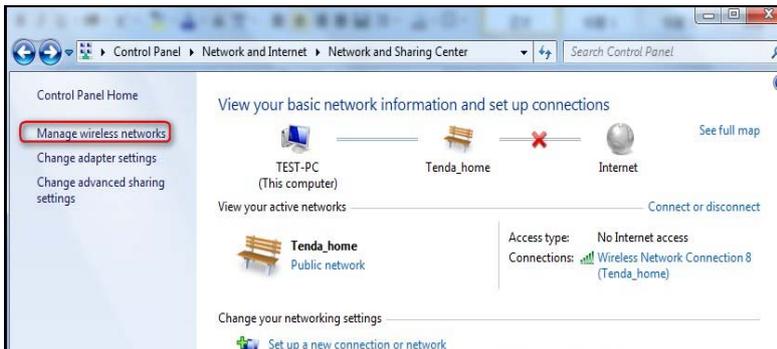
If you change wireless settings on your wireless device, you must remove them accordingly from your PC; otherwise, you may not be able to wirelessly connect to this device. Below describes how to do remove a wireless network from your PC.

Windows 7

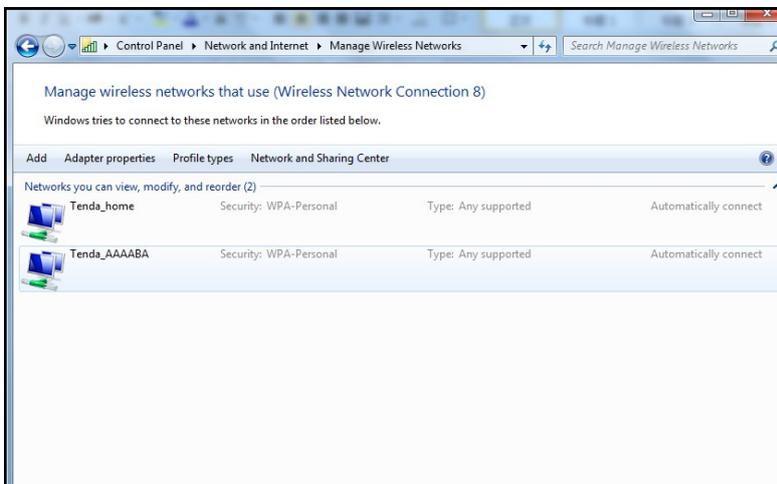
- ① Right-click the **Network** icon and select **Properties**.



- ② Select **Manage Wireless Networks**.

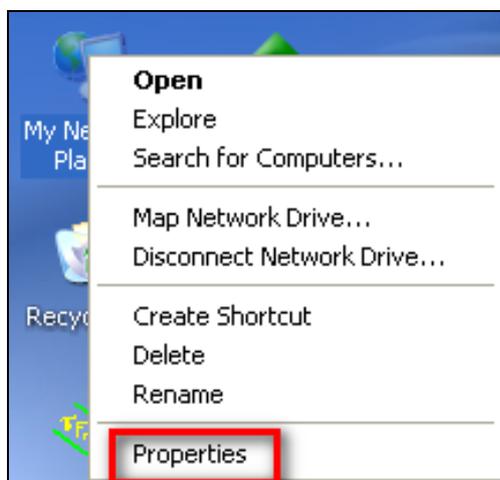


- ③ Select the wireless network and click **Remove network**.

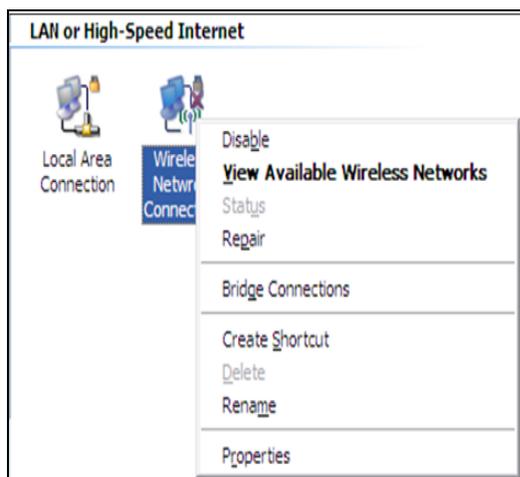


Windows XP

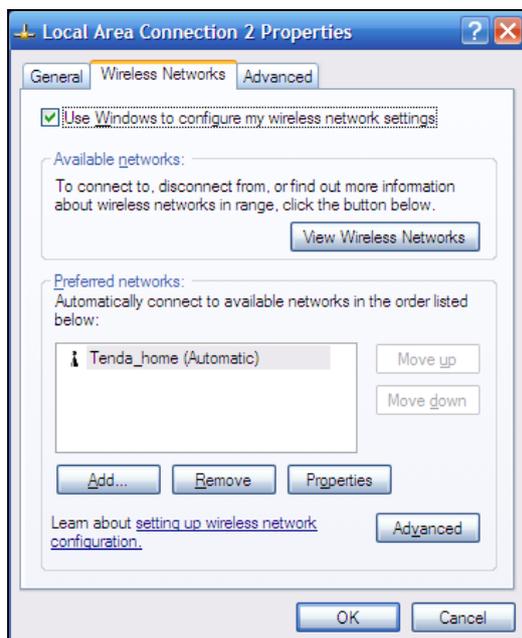
- ① Right-click **My Network Places** and select **Properties**.



- ② Right click **Wireless Network Connection** and then select **Properties**.



③ Click **Wireless Networks**, select the wireless network name under **Preferred networks** and then click the **Remove** button.



5 Safety and Emission Statement

CE Mark Warning

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 recommended to use a shielded RJ45 cable



FCC 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, 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.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

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

NCC Notice

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更設計之特性及功能。

低功率射頻電機之作用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。