Tenda

User Guide

www.tendacn.com

Wireless N450 Home Router

Copyright Statement

Contents

Chapter 1 Product Overview

1 Package Contents

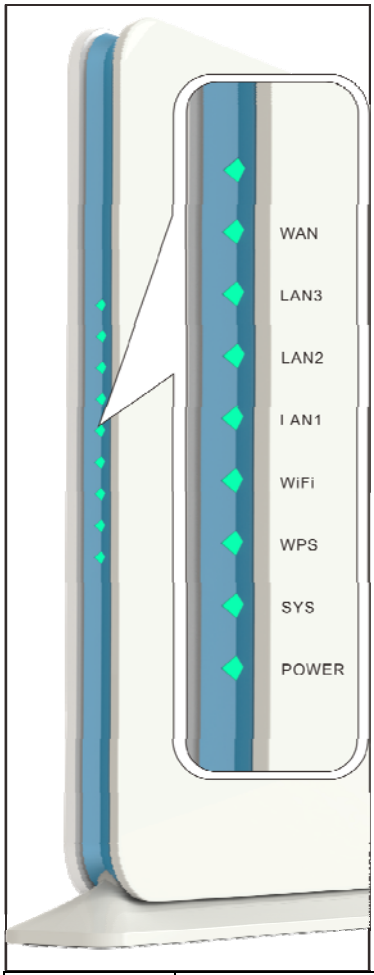
Please verify that the package contains the following items:

- Wireless Router
- Power Adapter
- Installation Guide
- Ethernet Cable
- Resource CD

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

2 Getting to Know Your Router

Front LED Overview



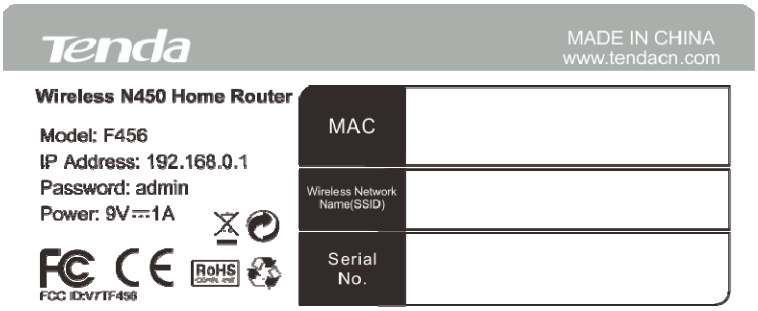
LED	Status	Description
WAN	Solid	WAN port connected correctly
	Blinking	WAN port is transmitting data
	Off	WAN port connected incorrectly
LAN (1/2/3)	Solid	LAN port connected correctly
	Blinking	LAN port is transmitting data
	Off	LAN port connected incorrectly

LAN 1/ IPTV	Solid	IPTV port is correctly connected
	Blinking	IPTV port is transmitting data
	Off	IPTV port is incorrectly connected
WiFi	Solid	WiFi is enabled
	Blinking	Transmitting data
	Off	WiFi is disabled
WPS	Blinking	Device is performing WPS authentication on a client device
	Off	WPS is disabled or WPS authentication finished
SYS	Blinking	Indicates the system is functioning correctly
	Solid/Off	Indicates the system is functioning incorrectly
POWER	Solid	Indicates a proper connection to power supply
	Off	Indicates an improper connection to power supply

Back Panel

- **POWER:** The power adapter is connected and you can use the provided adapter to supply power.
- **WPS/RST:** WPS button/Reset button: Pressing it for about 3 second enables WPS encryption with a blinking WPS LED while pressing it for about 7 seconds restores the router to its factory default setting.
- **WiFi:** WiFi button, pressing it disables wireless. WiFi is enabled by default.
- **LAN/1/2/3:** 3 LAN ports (RJ-45) for connection to PC's NIC or uplink to a hub, switch or wireless AP.
- **LAN 1/IPTV:** IPTV port for connection to a network set-top box. However, this port can also function as a LAN port if the IPTV STB option is not enabled.
- **WAN:** Internet port (RJ-45) for connection to an Internet-enabled DSL Modem/Cable Modem or existing Ethernet.

Label



You can acquire the following information from Label:

- **Model:** Displays the product model.
- **IP Address:** The default IP is 192.168.0.1.
- **Password:** The default password is admin.
- **MAC:** Displays the device's default MAC address.
- **Wireless Network Name(SSID):** Displays the device's default SSID name.

3 Position Your Router

For best performance, please place your router:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- Accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, PCs, the base of a cordless phone, or a 2.4-GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Chapter 2 Installation and Quick Setup Guide

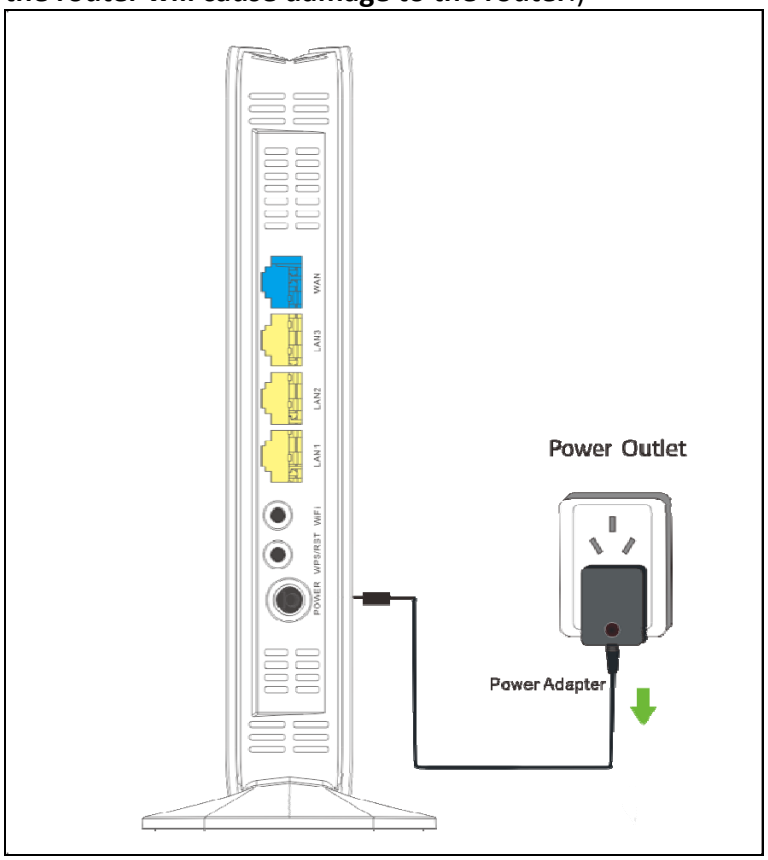
1 Preparation

Before connecting Ethernet cables, please verify the following items:

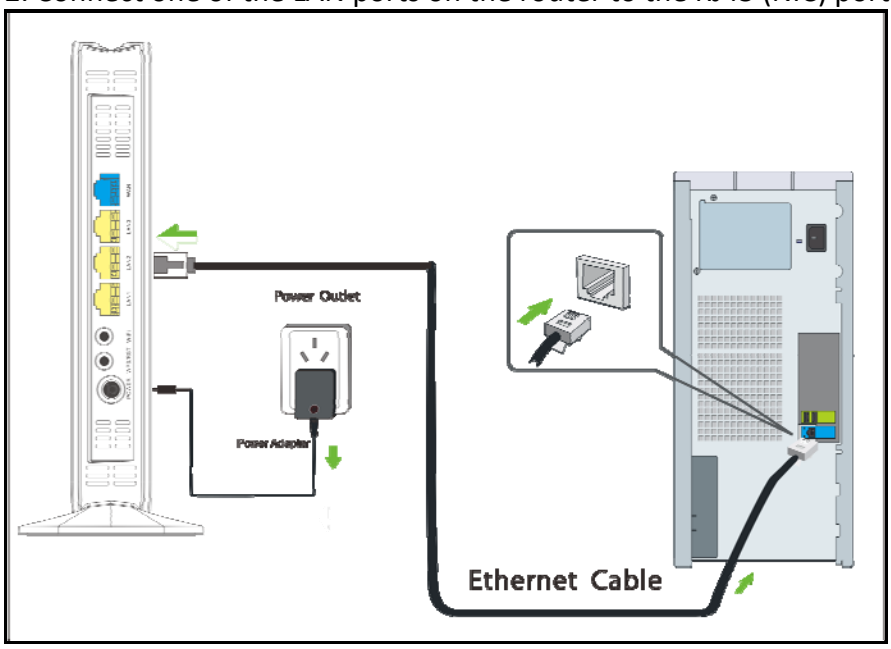
Item	Description
Wireless Router	Used with the provided power supply
PC	Installed with IE8 or other better web browsers.
Ethernet Cable	Used for linking the PC to the router
Broadband Service	Provided by ISP
Internet Connection Type	● If you connect to the Internet using a broadband connection that requires a username and a password provided by your ISP, please select PPPoE; ● If you can access Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem, please select Dynamic IP.

2 Hardware Installation

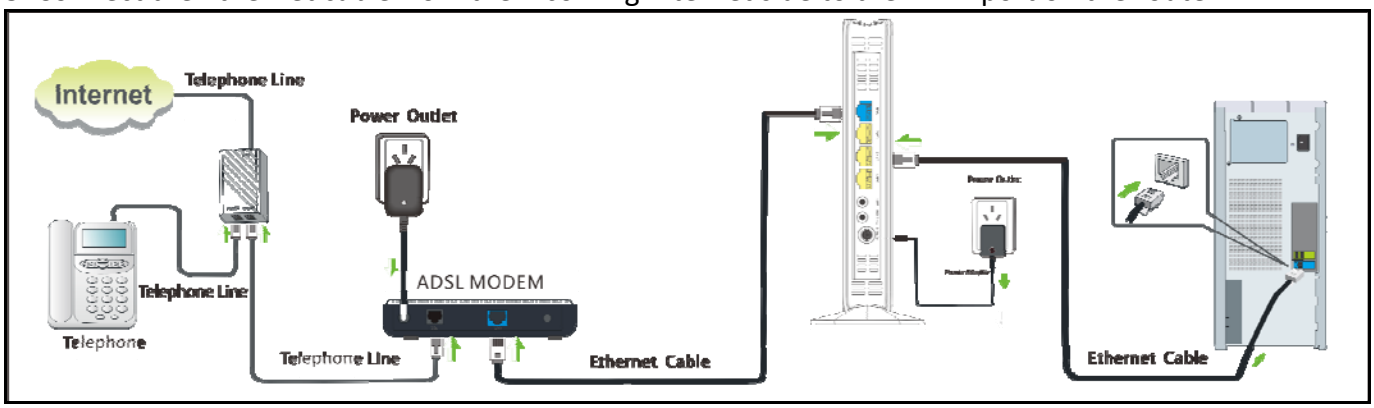
1. Connect one end of the included power adapter to the router and plug the other end into a surge protected power strip. (**Using a power adapter with a different voltage rating than the one included with the router will cause damage to the router**.)



2. Connect one of the LAN ports on the router to the RJ45 (NIC) port on your PC using an Ethernet cable.



3. Connect the Ethernet cable from the incoming Internet side to the WAN port on the router.



3 Internet Connection Setup

Configure PC

Configure your PC obtain IP address automatically. If you are not clear about this, please refer to Appendix 1 Configure PC.

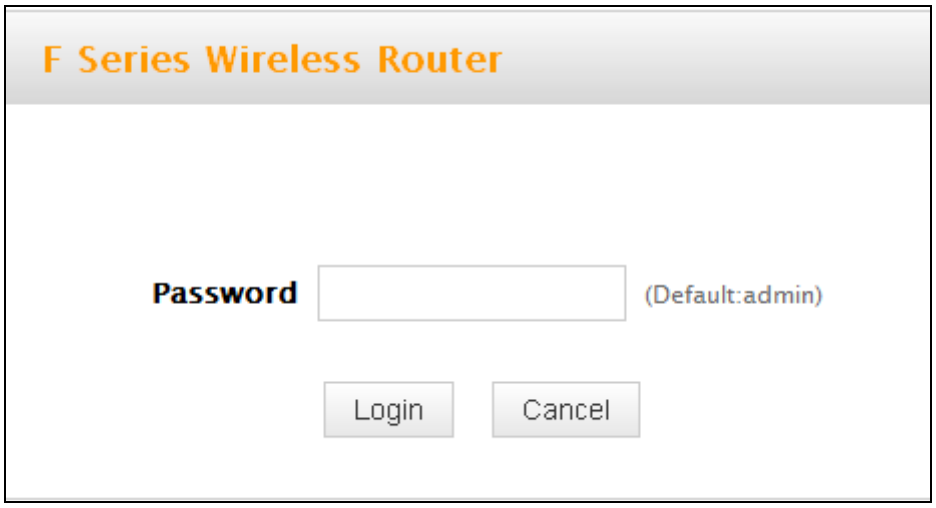
Configure Router

Login to Web Utility

1. Launch a web browser, such as IE Web browser;

2. In the address bar, input 192.168.0.1 and press Enter;

3. Enter a password in the corresponding field as shown in the window below (the default password is set to “admin”).

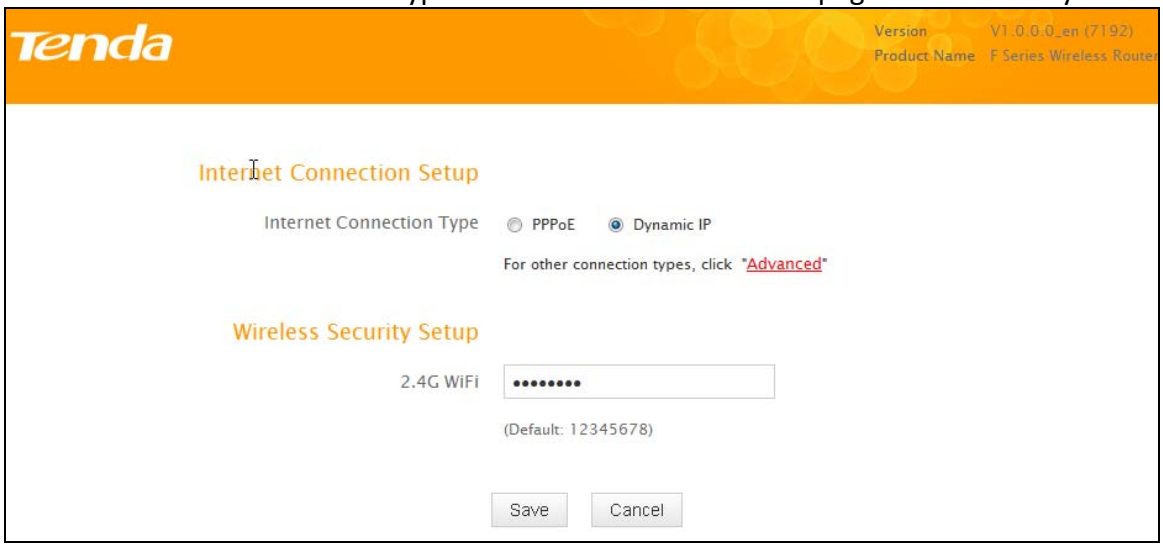


Note

For security purpose, please change the default password after you have logged in to the web utility.

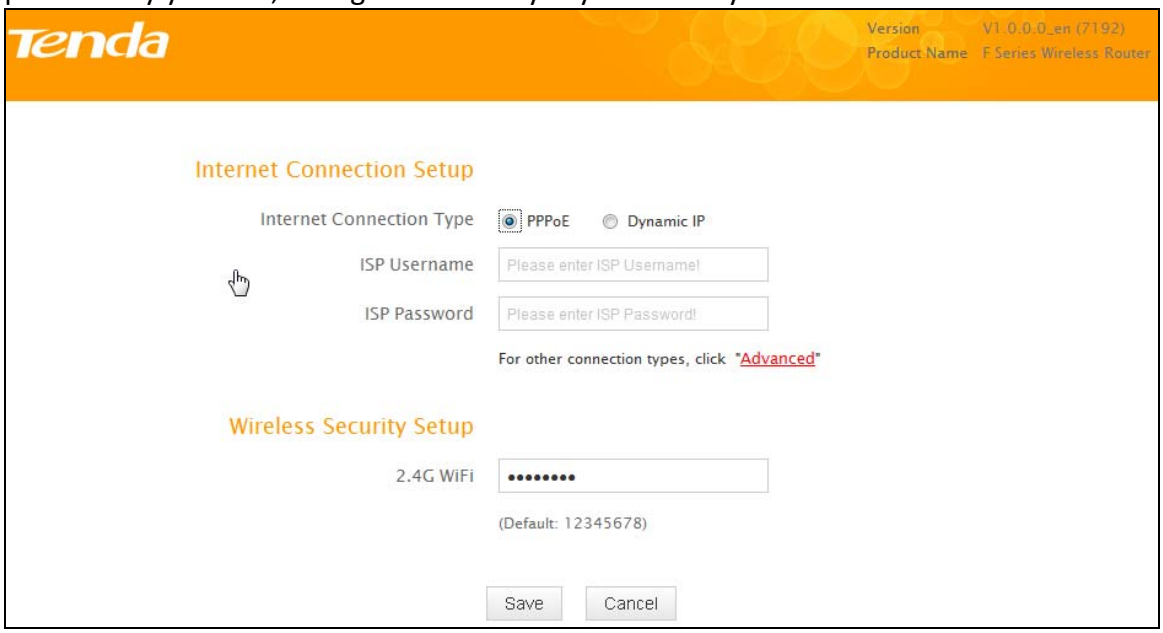
Internet Connection Setup

Common Internet connection types are available on the home page: PPPoE and Dynamic IP.



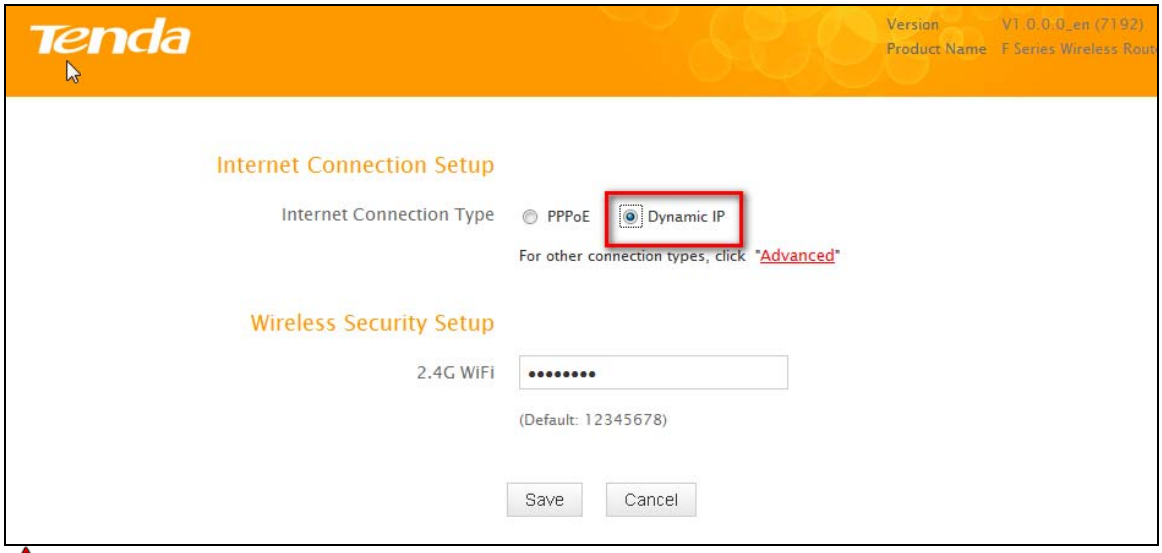
PPPoE

Select PPPoE (Point to Point Protocol over Ethernet) if you used to connect to the Internet using a broadband connection that requires a username and a password. Enter the user name and password provided by your ISP; configure a security key to secure your wireless network and then click OK.



Dynamic IP

Select DHCP (Dynamic IP) if you can access Internet as soon as your computer directly connects to an Internet-enabled ADSL/Cable modem; configure a security key (8-63 characters) to secure your wireless network and then click OK.



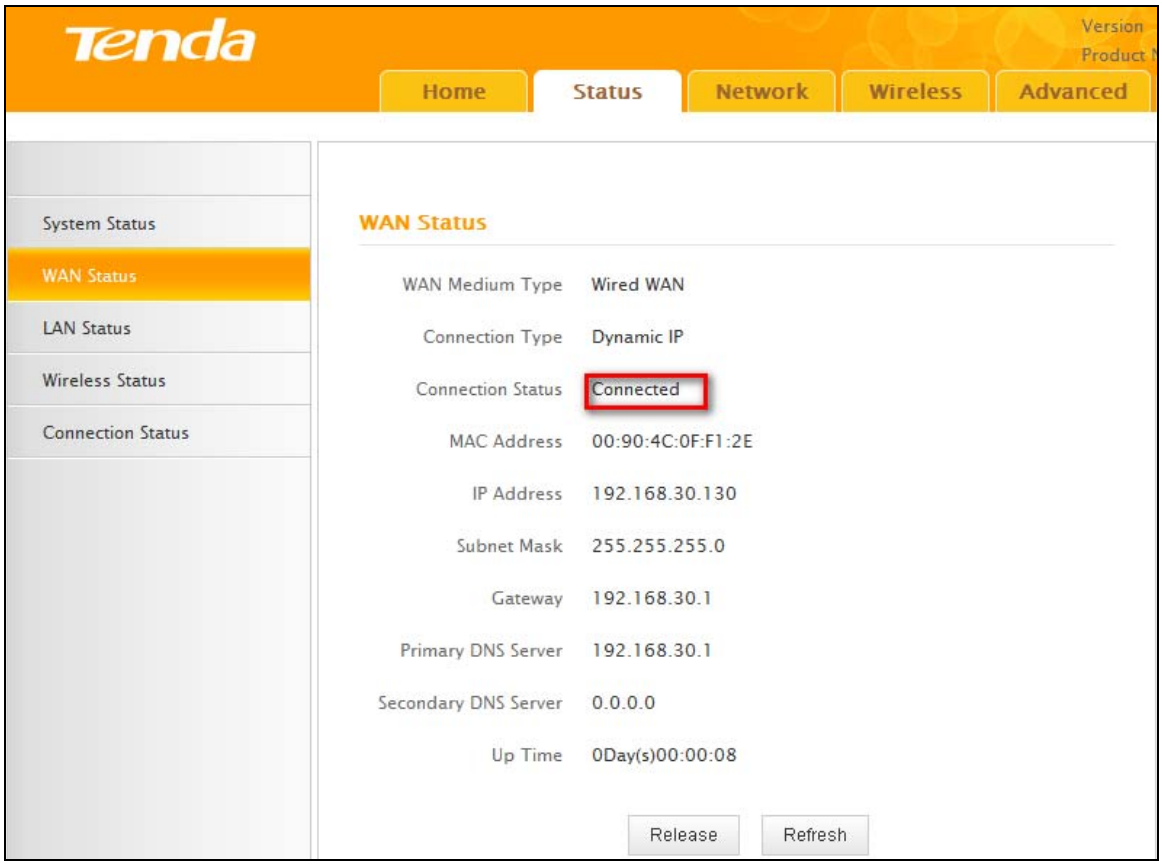
Note

1. DHCP is the default Internet connection type;
2. If you are not sure about your PPPoE username and password, contact your Internet service provider (ISP) for help. For other Internet connection types, please go to section 2.2: WAN.

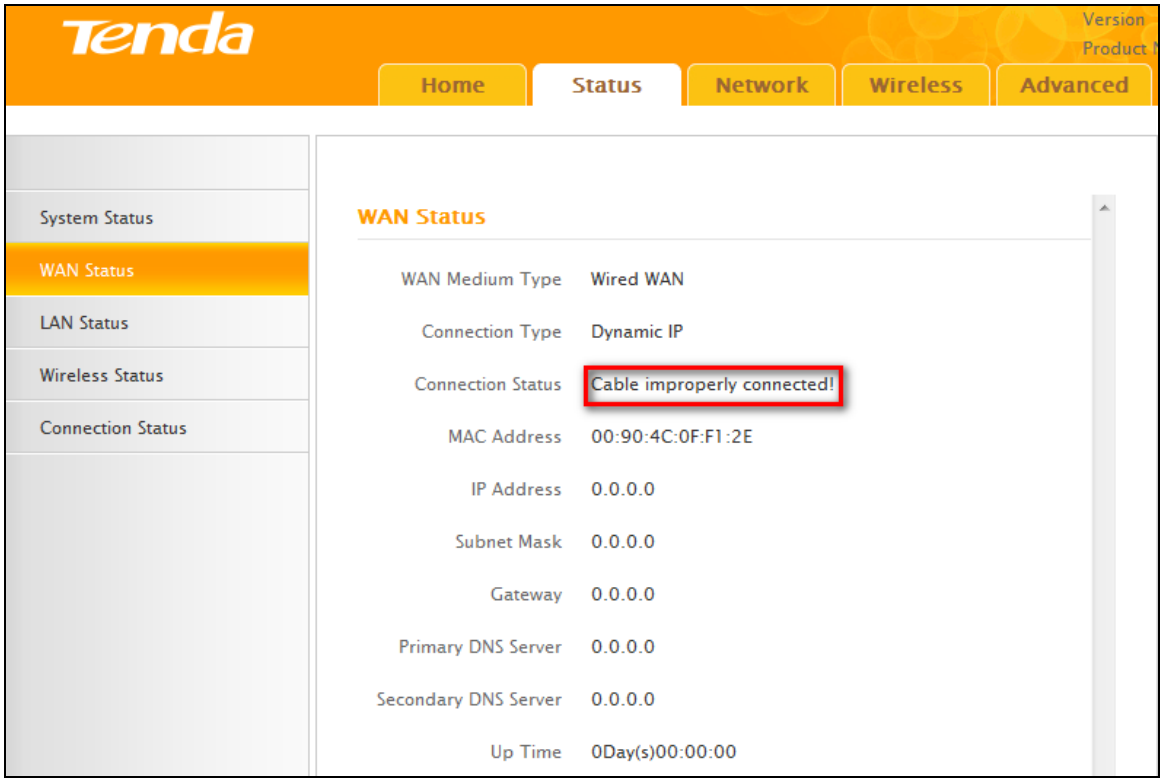
4 Verify Internet Connection Settings

System automatically skips to the status page when you finish all needed settings on the home page. Here you can see the system status and WAN connection status of the device.

1. If you find **Connected** and a WAN IP address displayed there (as shown below), you have got a wired internet access now.



2. If connection status displays **Cable improperly connected** and there is no WAN IP address displayed (as seen below), connection between the Internet-enabled modem and your device may have failed. Please double check or re-connect all involved devices and cables properly and then refresh the page. If nothing is wrong, **Connecting** or **Connected** will be displayed.



3. If **Connecting** is displayed and no WAN IP address is seen, try refreshing the page five times. And if it still displays **Connecting** try steps below:

1). Contact your ISP for assistance.

2). Read the connection diagnostic info on WAN status.

Note

The following diagnostic info will be displayed on particular occasions for your reference:

1). You have connected to Internet successfully.

2). You might have entered a wrong user name and/or a wrong password. Please contact your ISP for the correct user name and password and enter them again.

3). Ethernet cable is not connected or not properly connected to the WAN port on the device. Please reconnect it properly.

4). No response is received from your ISP. Please verify that you can access Internet when you directly connect your PC to an Internet-enabled modem. If not, contact your local ISP for help.

5 Connect to Device Wirelessly

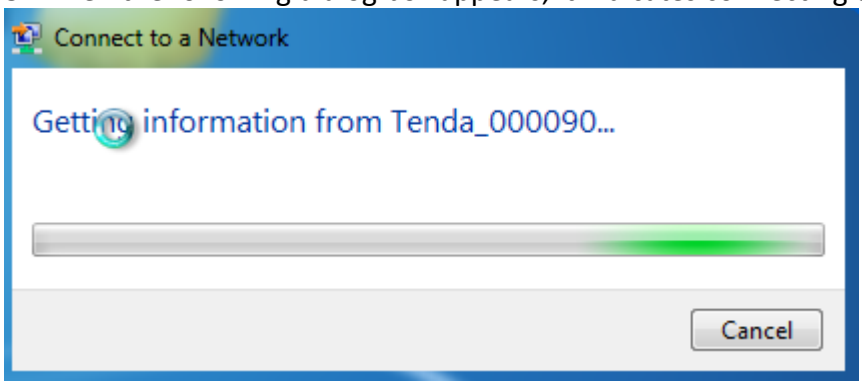
Having finished above settings, you can search the device's wireless network (SSID) from your wireless devices (notebook, iPad, iPhone, etc) and enter a security key to connect to it wirelessly. Desktop computers should be equipped with wireless network cards.

WIN7 OS

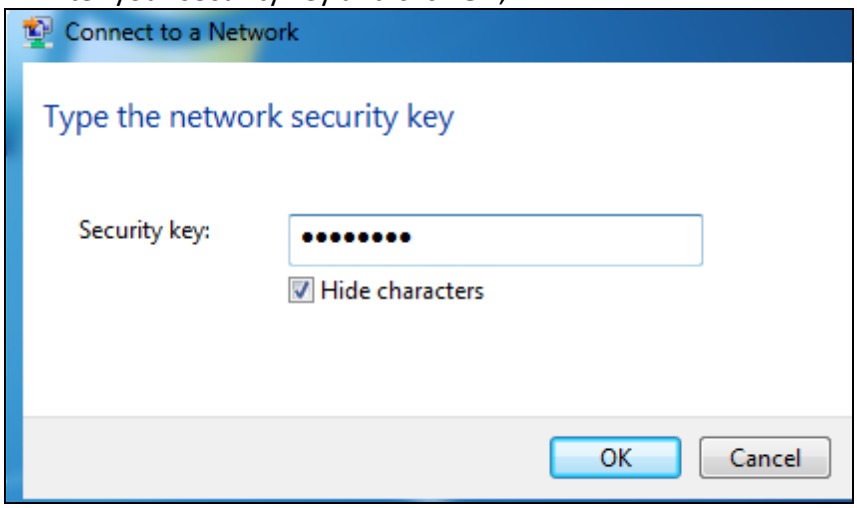
1. Click on the icon  at the bottom of the right corner on your desktop;

2. Select the network you wish to connect, such as Tenda-000090;

3. When the following dialog box appears, it indicates connecting to the network;



4. Enter your security key and click **OK**;



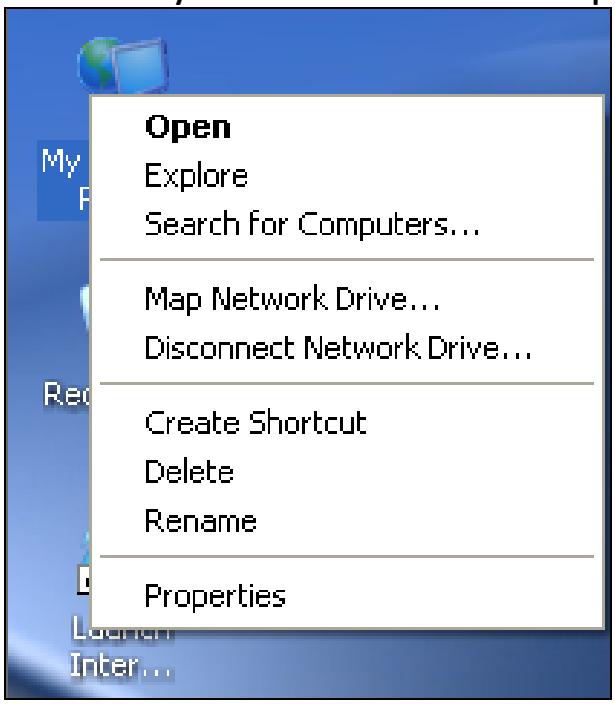
5. When displaying Connected, you have connected to network successfully.

Tips ----------

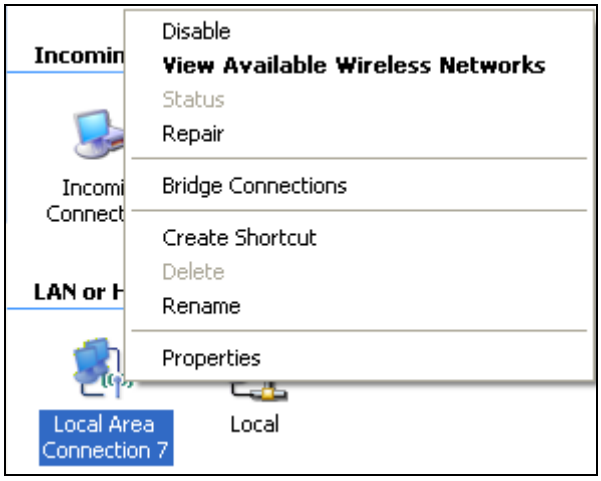
If you cannot find the icon  at the bottom of the right corner on your desktop, please refer to Appendix 2 Join a Wireless Connection>Win7 OS.

Windows XP OS

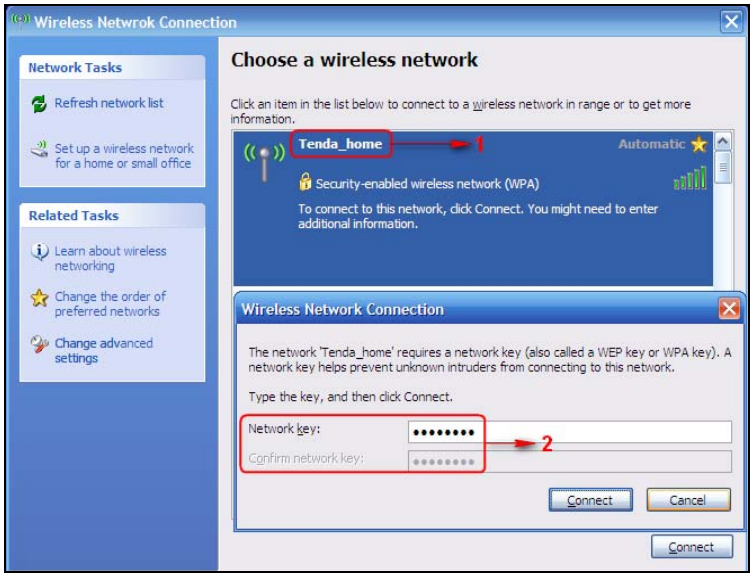
1. Click on **My Network Places** and select **Properties**;



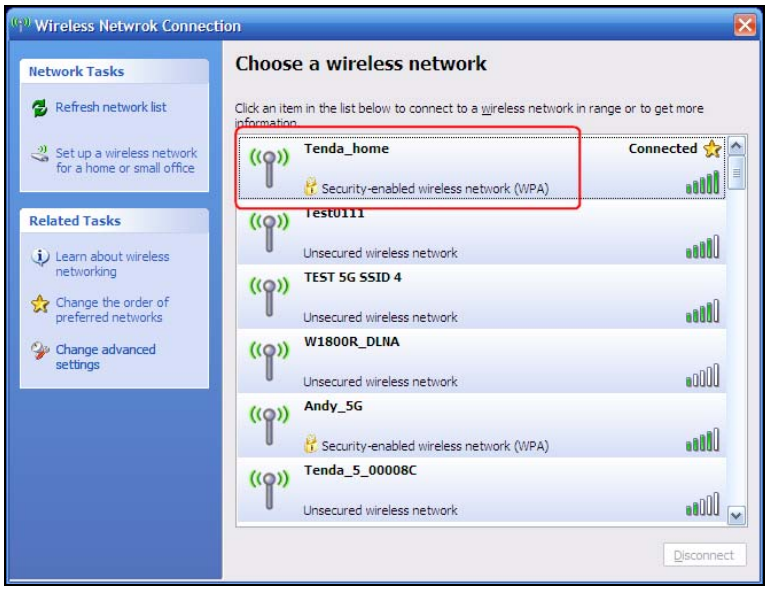
2. Click **Local Area Connection** and select **View Available Wireless Networks;**



3. Select the SSID you wish to connect, such as Tenda_home, click **Connect**, enter the security key and then click **OK**;



4. You can access Internet via the device when **Connected** appears next to the wireless network name you selected.



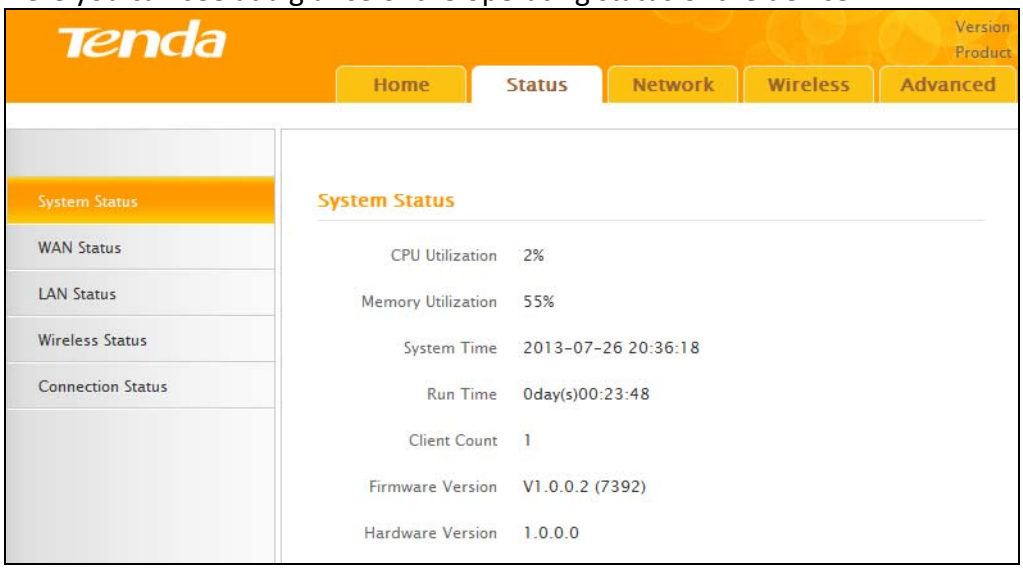
Chapter 3 Configurations

This chapter describes the Web based configurations for easier management of your router. During the configuration operation, if you are not clear about a certain feature, simply read the related helpful info below.

1 Status

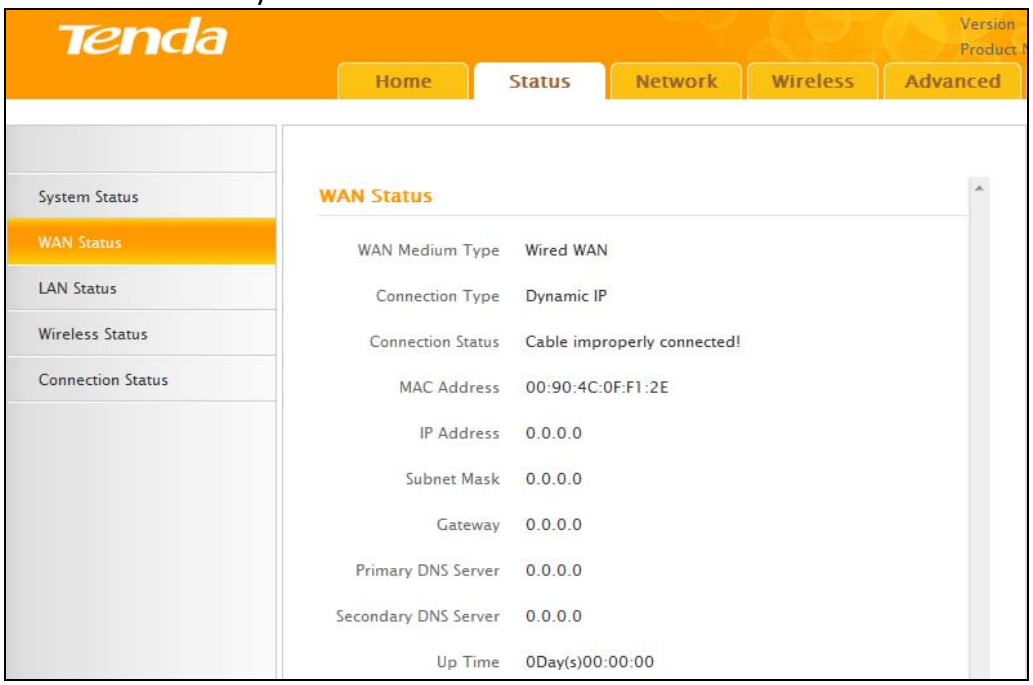
1.1 System Status

Here you can see at a glance of the operating status of the device.



1.2 WAN Status

This section allows you to view the router's WAN information as noted below:

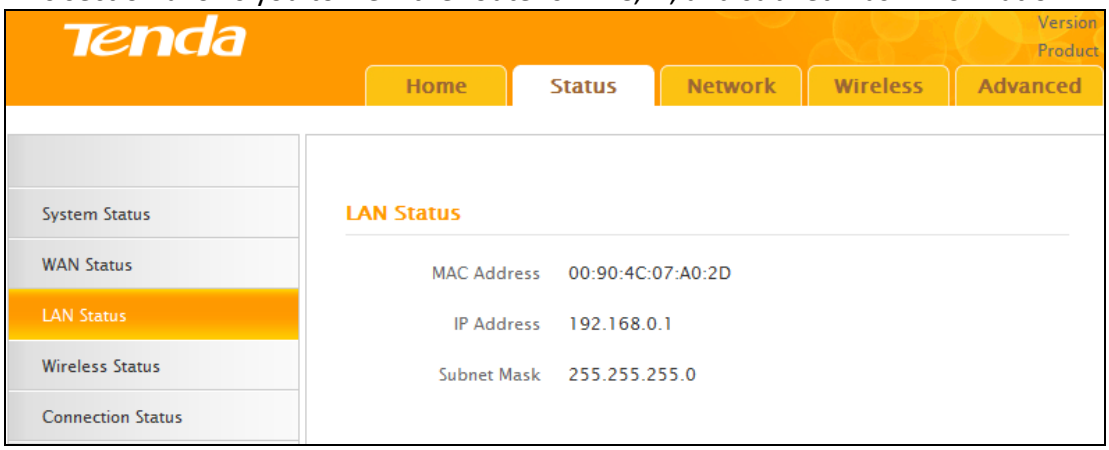


- Connection Type: Displays the current Internet connection type.
- Connection Status: Displays the WAN connection status: Disconnected, Connecting, or Connected.
- MAC Address: Displays the WAN MAC address.
- IP Address: Displays the WAN IP address.
- Subnet Mask: Displays the WAN subnet mask.
- Gateway: Displays the WAN gateway address.
- Primary DNS Server: Displays the primary WAN DNS address.

- Secondary DNS Server: Displays the secondary WAN DNS address (if any).
- Up Time: Displays the time duration indicating how long the router has been connected to the ISP.

1.3 LAN Status

This section allows you to view the router's MAC, IP, and subnet mask information.



- MAC Address: Displays the router's LAN MAC address.
- IP Address：Displays the current LAN IP address.
- Subnet Mask: Displays the current LAN subnet mask.

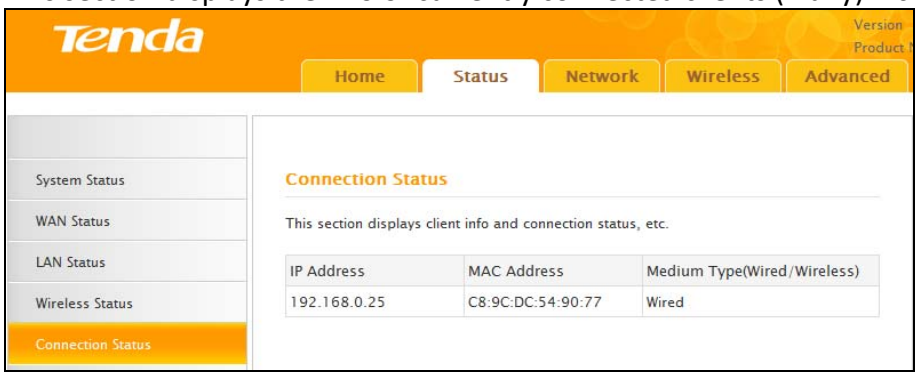
1.4 Wireless Status

This section allows you to view the wireless information of 2.4Ghz band.

- Wireless Radio: Displays whether wireless is enabled or not.
- Wireless MAC address: Displays the MAC address of the router's wireless interface.
- SSID: Displays the current SSID.
- 802.11 Mode: Displays the currently active network mode.
- Country: Displays the current country selection.
- Channel: Displays the current channel.
- Security Mode: Displays the current security Mode.

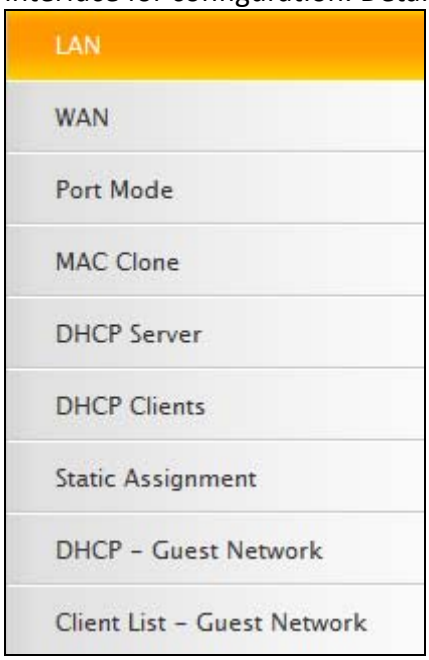
1.5 Connection Status

This section displays the info of currently connected clients (if any) including IP and MAC addresses, etc.



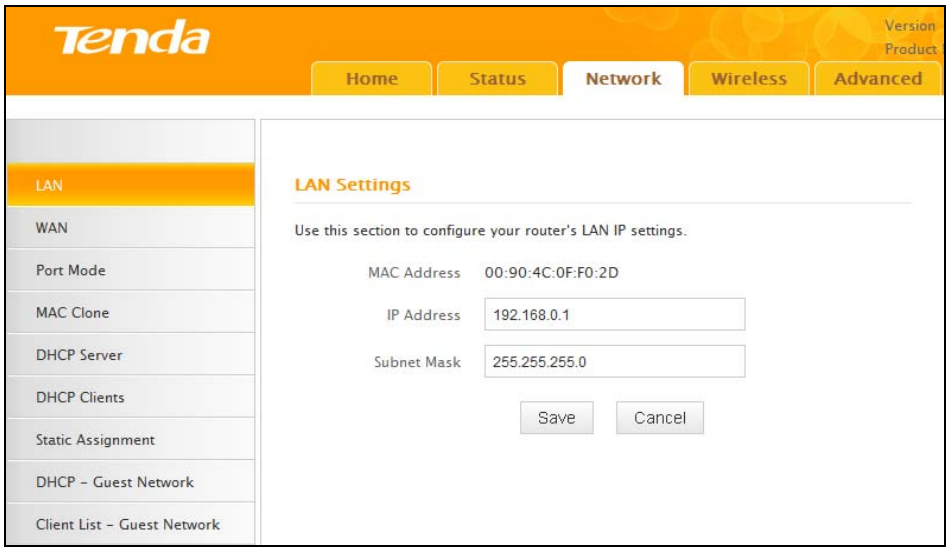
2 Network

Network menu includes the following nine submenus. Clicking any of them enters the corresponding interface for configuration. Details are explained below:



2.1 LAN

This section allows you to configure your router's LAN IP settings.



- IP Address: The router's LAN IP. The default is 192.168.0.1 and you can change it according to your needs.
- Subnet Mask: Router's LAN subnet mask. The default is 255.255.255.0.

Note

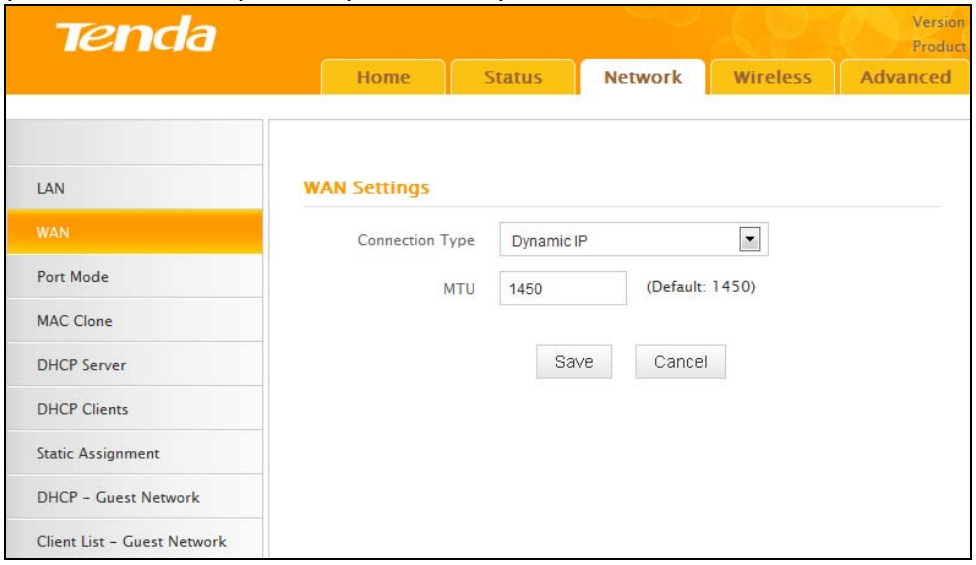
If you change the LAN IP address, you must use the new one to log on to the web utility.

2.2 WAN

There are three types of Internet connection: Dynamic IP (DHCP), Static IP, and PPPoE(including dual access).

Dynamic IP

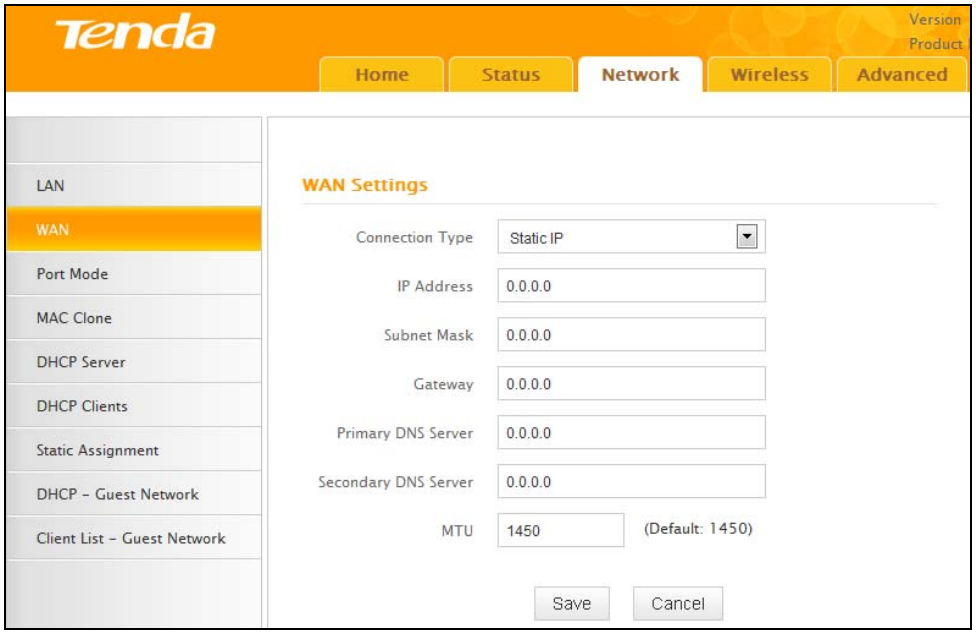
Select Dynamic IP (DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not provide you with any IP information.



- Connection Type: Displays a list of available Internet connection types.
- MTU: Maximum Transmission Unit. The default value is 1450.

Static IP

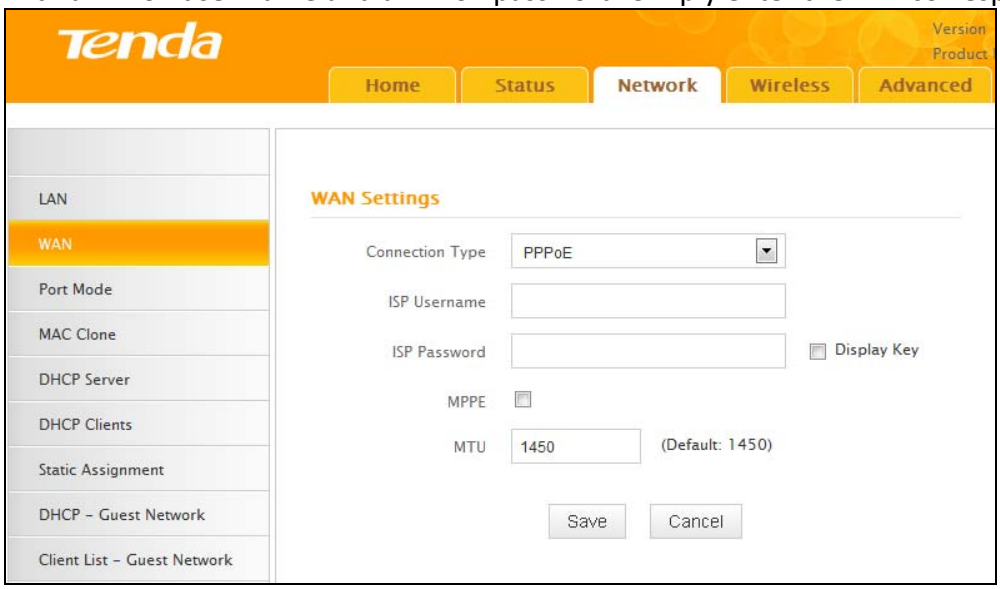
Select Static IP Address if your ISP provides all the connection information. You will need to enter the provided IP address, subnet mask, gateway address, and DNS address(es) in the corresponding fields.



- Connection Type: Displays a list of available Internet connection types.
- IP Address: Enter the IP address provided by your ISP. Consult your local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- Gateway: Enter the gateway address provided by your ISP. Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MTU: Maximum Transmission Unit. The factory default is 1450.

PPPoE

Select PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection and provides you with a PPPoE user name and a PPPoE password. Simply enter them in corresponding fields.



- Connection Type: Displays a list of available Internet connection types.
- ISP User Name: Enter the PPPoE User Name provided by your ISP. Consult your ISP if you are not clear.
- ISP Password: Enter the PPPoE Password provided by your ISP. Consult your ISP if you are not clear.
- MPPE: Select whether to enable the MPPE authentication method.
- Enable Dual Access: Select whether to enable Dual Access.
- MTU: Maximum Transmission Unit. The factory default is 1450.

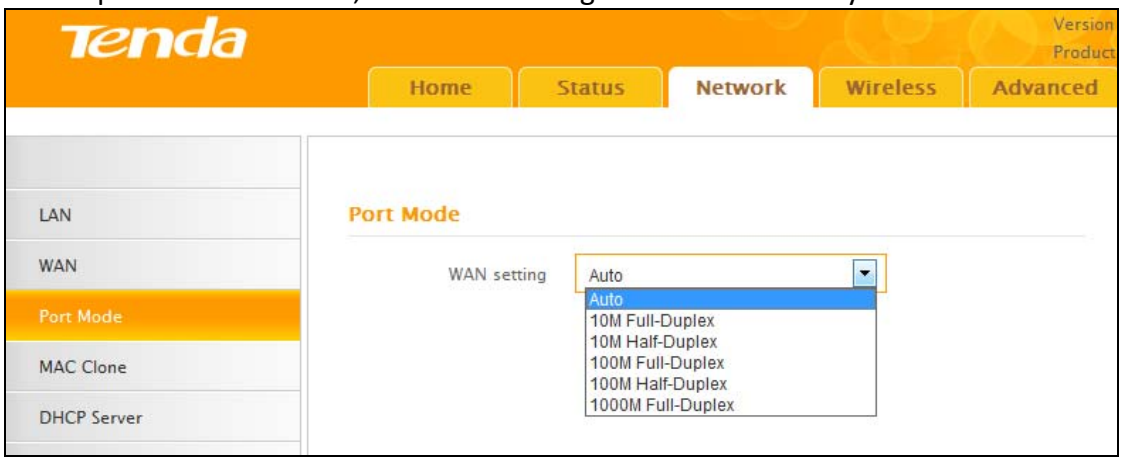
Tips ----------

1. It is not advisable to change the factory default MTU value unless necessary, an improper MTU value may

degrade your network performance or even lead to network malfunction.
2. If you want to active new settings you've changed, you must reboot the device.

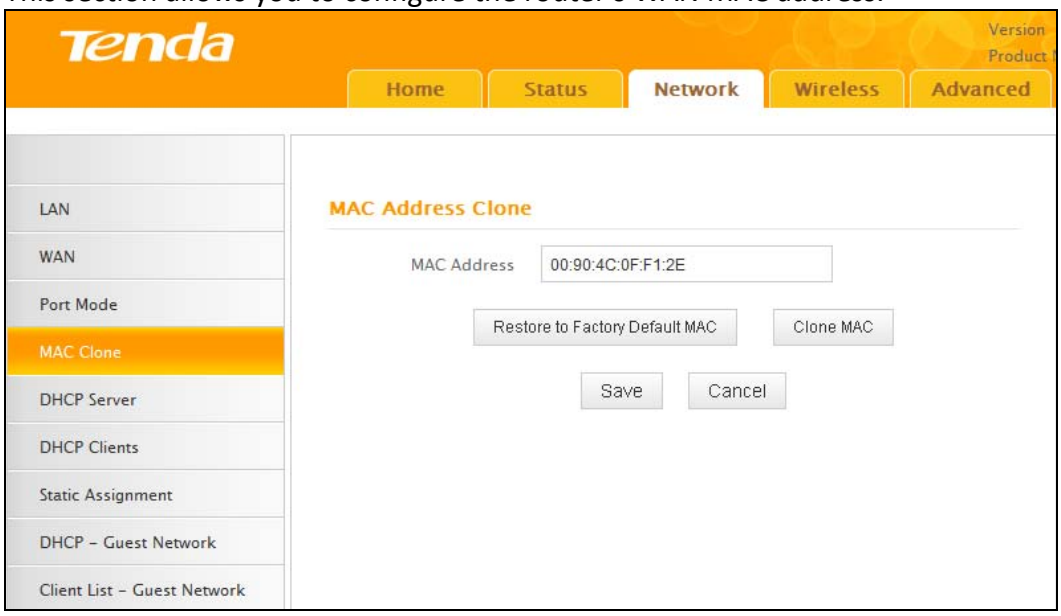
2.3 Port Mode

Mode includes auto,10M Half-Duplex,10M Full-Duplex,100M Half-Duplex,100M Full-Duplex,1000M Full-Duplex. Default is auto, and do not change it unless necessary.



2.4 MAC Clone

This section allows you to configure the router's WAN MAC address.



- MAC Address: Configure the router's WAN MAC address.
- Restore to Factory Default MAC: Reset the router's WAN MAC to factory default.
- Clone MAC: Clicking this button copies the MAC address of your PC to the MAC Address field in the router.

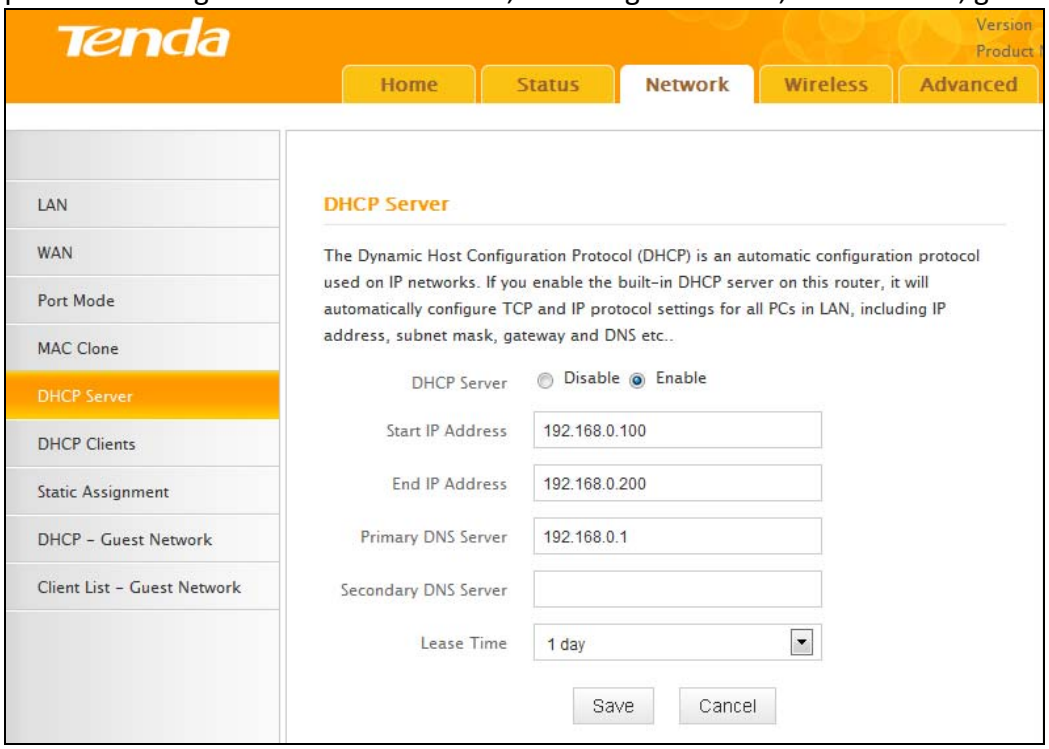
Note

1. Normally you don't need to change the default WAN MAC value. However, some ISP's may require the client PC's MAC address for Internet connection authentication. In this case, simply enter the MAC address in the WAN MAC Address field or click the **Clone MAC** button. Note that the WAN MAC address in the **Status** interface will be updated accordingly once you have changed it.
2. Remember to reboot the router to activate the new WAN MAC. DO NOT use the **Clone MAC** feature unless required by your ISP.
3. Only the MAC addresses of the PCs on the LAN can be cloned to the router.

2.5 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP

networks. If you enable the built-in DHCP server on this device, it will automatically configure the TCP/IP protocol settings for all PC's in the LAN, including IP address, subnet mask, gateway, and DNS.



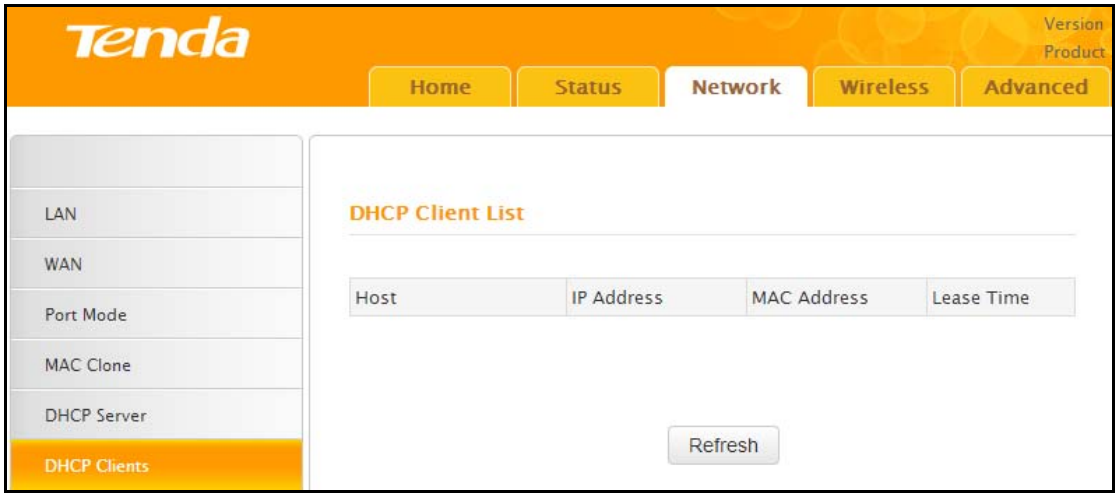
- DHCP Server: Select whether to enable or disable the router's DHCP server feature.
- Start IP Address: Enter the starting IP address for the DHCP server's IP assignment.
- End IP Address: Enter the ending IP address for the DHCP server's IP assignment.
- Lease Time: The length of time for the IP address lease.

Tips ----------

1. The device has enabled the DHCP server by default and it is not advisable to disable it unless necessary.
2. To apply the DHCP server settings to all PC's on your LAN, you must set all PC's to "Obtain an IP address automatically" and "Obtain DNS server address automatically".

2.6 DHCP Clients

This list displays the DHCP dynamic client list, which includes host name, IP address, MAC address, and lease time information.



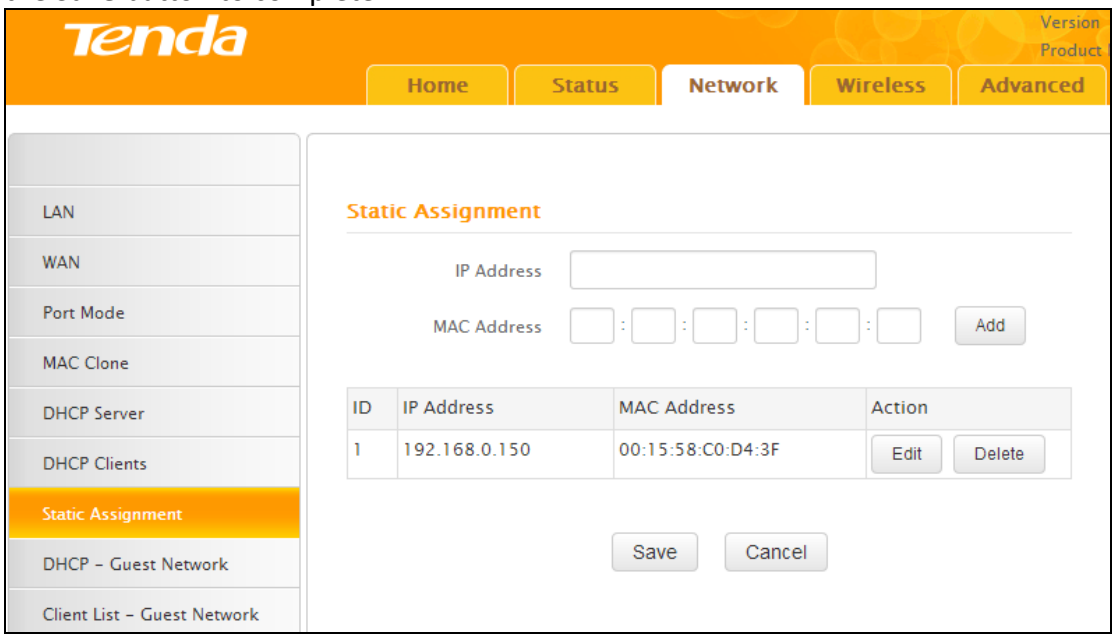
- Host: Displays clients' host names.
- IP Address: Displays IP addresses that clients obtained from the DHCP server.
- MAC Address: Displays the MAC address of a given host.

- Lease Time: Remaining time for a corresponding IP address lease.

2.7 Static Assignment

If you would like some devices on your network to always have fixed IP addresses, you can use this feature and manually add a static DHCP assignment entry for each device.

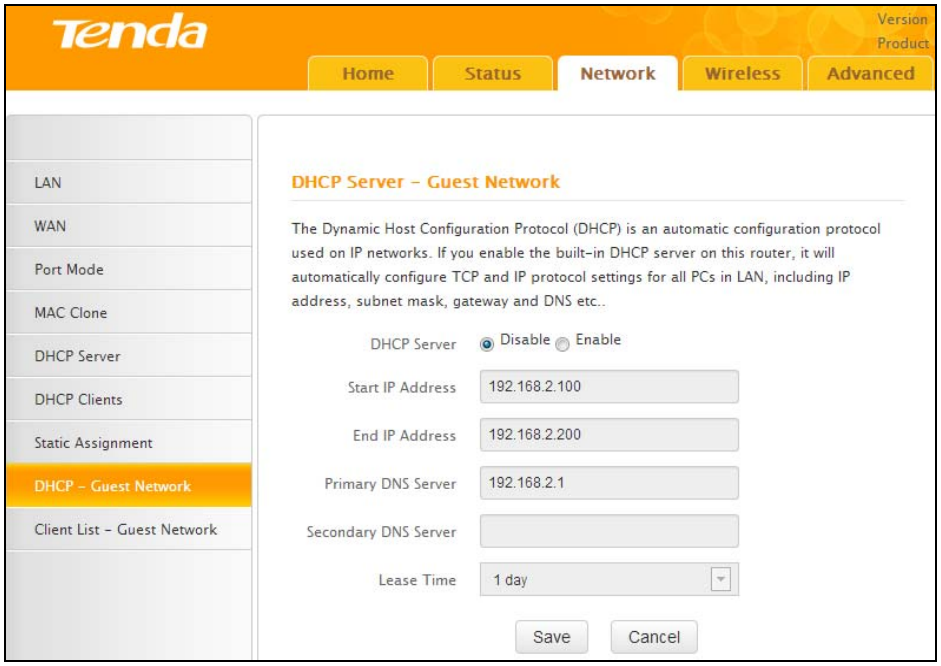
For example: To have a PC at the MAC address of 00:15:58:c0:d4:3f always receive the same IP address of 192.168.0.150, simply enter the IP and MAC addresses in the corresponding fields and click **Add** and then the **Save** button to complete.



- IP Address: Enter the IP address for static DHCP assignment.
- MAC Address: Enter the MAC address of a computer to always receive the same IP address you specify.
- Add: Click it to add a new IP-MAC static assignment entry to list.
- Edit: Click it to change an existing entry.
- Delete: Click to remove an existing entry.

2.8 DHCP-Guest Network

If you enable the built-in DHCP server for the Guest Network on the router it will automatically configure the TCP/IP protocol settings for all PC's on the Guest Network, including IP address, subnet mask, gateway, and DNS.



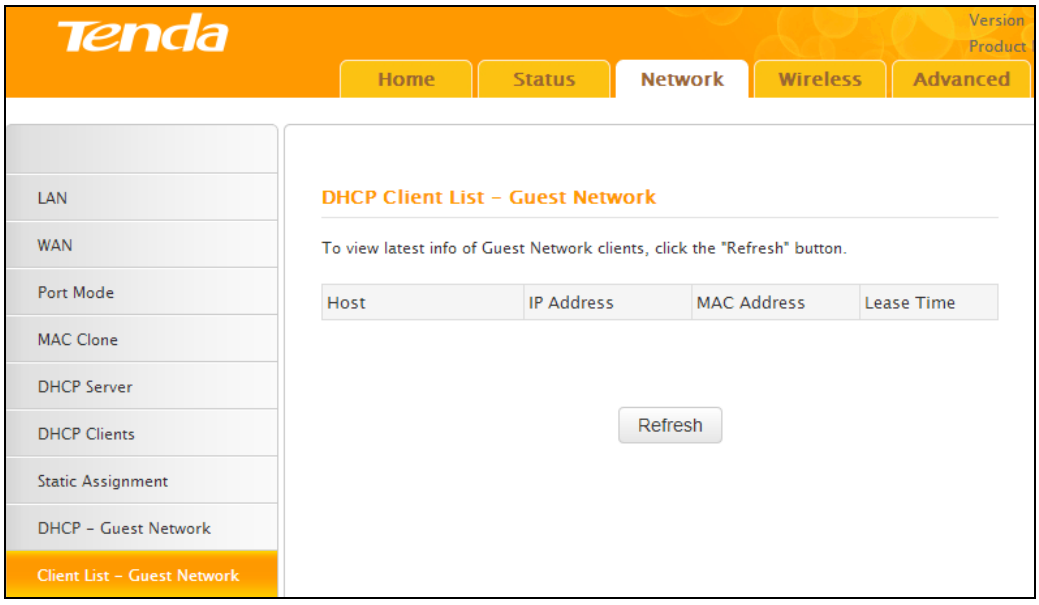
- DHCP Server: Select whether to enable or disable the router's DHCP server feature.
- Start IP Address: Enter the starting IP address for the DHCP server's IP assignment.
- End IP Address: Enter the ending IP address for the DHCP server's IP assignment.
- Lease Time: The length of time for the IP address lease.

Tips ----------

The IP address configured in DHCP-guest network should not be in the same network segment as that of DHCP server's.

2.9 Client List-Guest Network

This list displays the DHCP dynamic client list, which includes host name, IP address, MAC address, and lease time information.

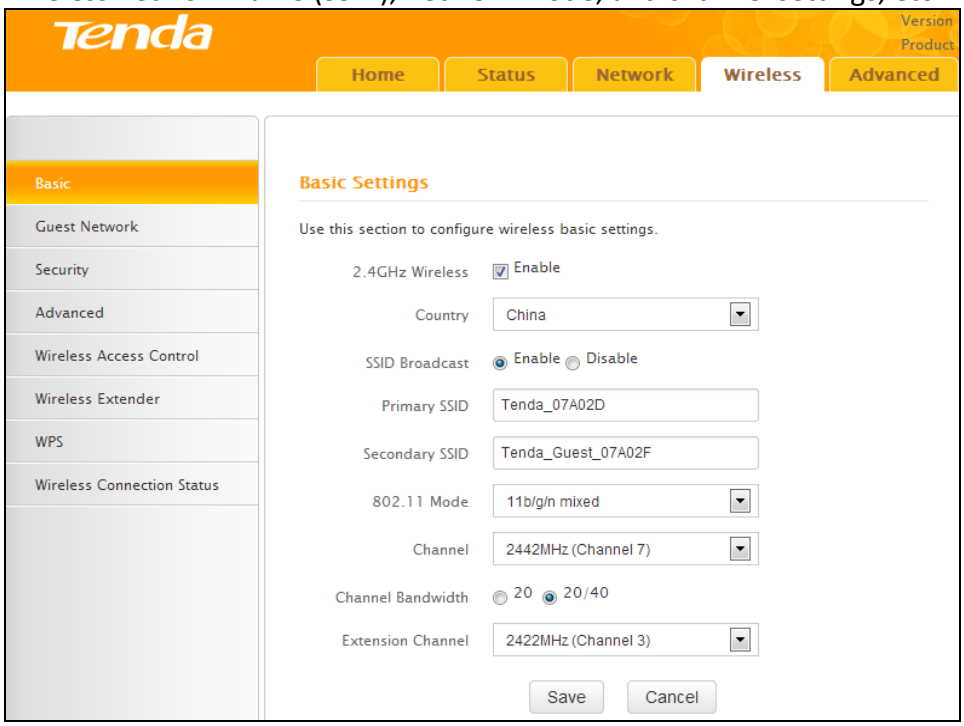


3 Wireless

The **Wireless** tab includes 8 submenus: Basic, Guest Network, Security, Advanced, Wireless Access Control, Wireless Extender, WPS, and Connection Status. Clicking any of them enters the corresponding interface for configuration. Details are explained below:

3.1 Basic

This section allows you to manage your wireless network. You can select your country, configure the wireless network name (SSID), network mode, and channel settings, etc.



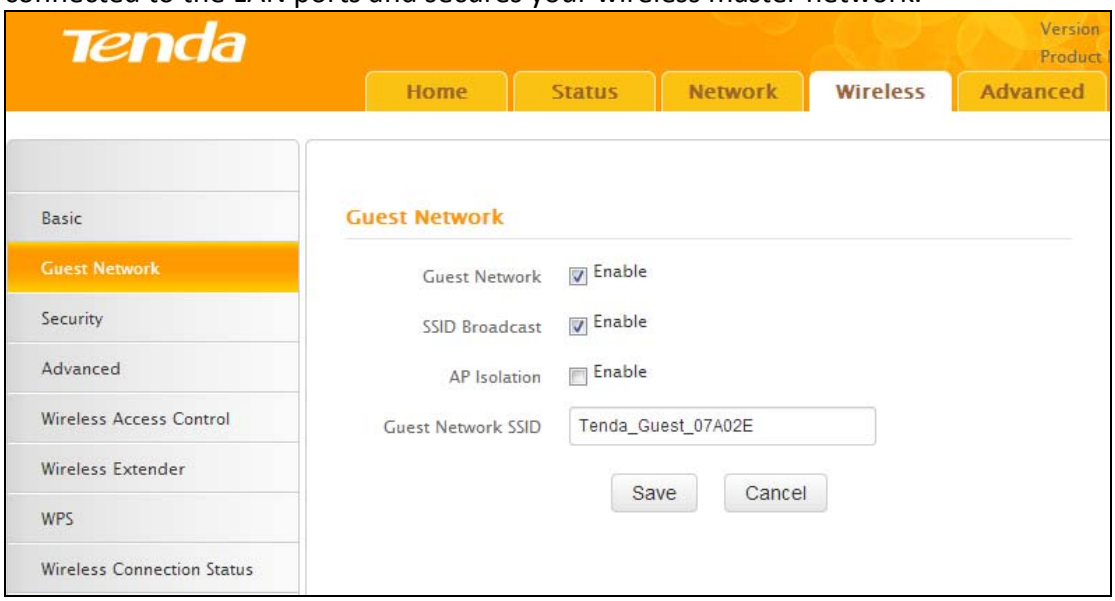
- 2.4GHz Wireless Network: Check/uncheck to enable/disable the 2.4GHz wireless feature. If disabled, all 2.4GHz-based features will be disabled accordingly.
- Country: Select your country from the drop-down list. There are 12 options available.
- SSID Broadcast: Select Enable/Disable to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to available networks. By default, it is enabled. When disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.
- SSID ：Service Set Identifier, is the unique name of a wireless network.
- 802.11 Mode: Select a correct mode according to your wireless clients. The default mode is 11b/g/n mixed.
- Channel: For optimal wireless performance, you may select the least used channel. It is advisable that

you select an unused channel from the drop down list, or “Auto” to let the router detect and select the best possible channel for your wireless network to operate on.

- Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. When there only 11n or a mix of 11b/g/n wireless clients, please select the 802.11n mode of 20/40M frequency band, but when there are only non-11n wireless clients, select the 20M frequency band mode
- Extension Channel：Available only in 11b/g/n mixed mode.

3.2 Guest Network

The Guest Network feature allows guests to access the Internet and other users on the guest network, while disallowing them to access the router’s web manager, users on the master network, and clients connected to the LAN ports and secures your wireless master network.



- Guest Network: Select to enable/disable the guest network feature.
- SSID Broadcast: Check to enable/disable the SSID feature, making your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to available networks. By default, it is enabled, but when disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.
- AP Isolation: If enabled, clients connecting to the guest network will be mutually inaccessible.
- Guest Network SSID：Service Set Identifier, is the configured unique name of the guest network.

Note

AP Isolation is disabled by default. If enabled, clients connecting to the guest network will be mutually inaccessible.

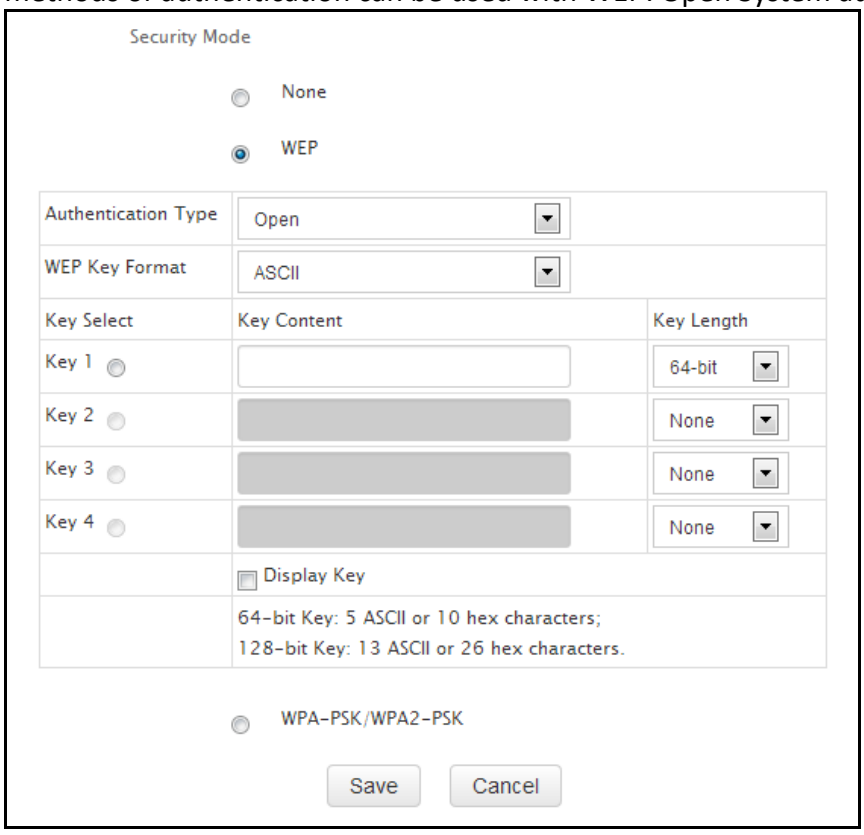
3.3 Security

This section allows you to encrypt your wireless network to block unauthorized accesses and malicious packet sniffing.

Three security modes are available: None, WEP, and WPA-PSK/WPA2-PSK.

WEP

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

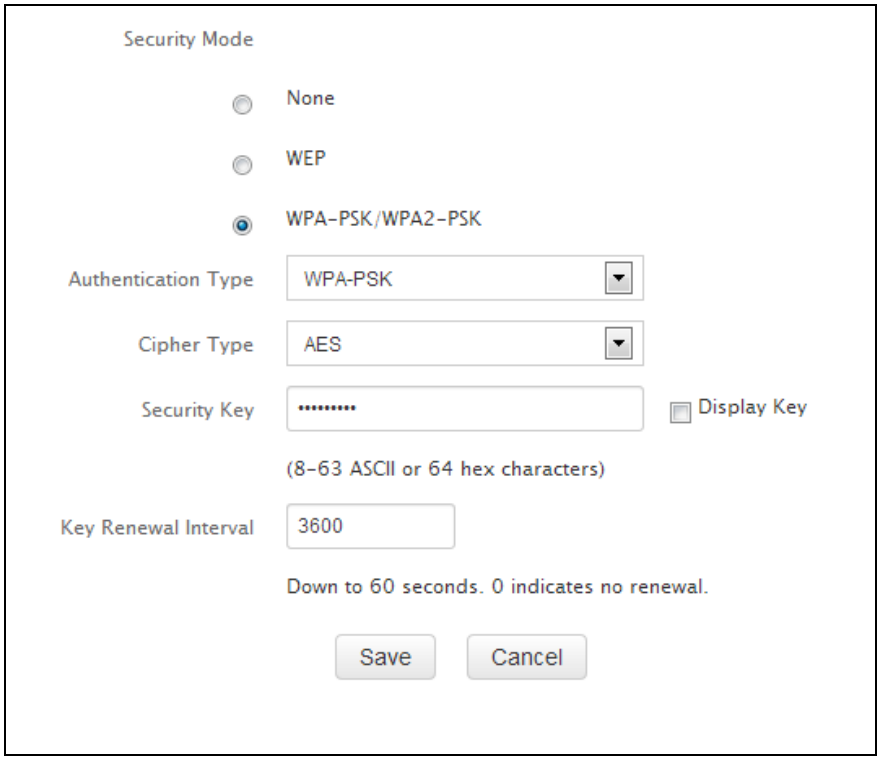


authentication.

- Authentication Type: Select Open or Shared from the drop-down list.
- WEP Key Format: Select Hex or ASCII from the drop-down list.
- Key Select: Select a key from the preset keys 1-4 for current use.

WPA-PSK

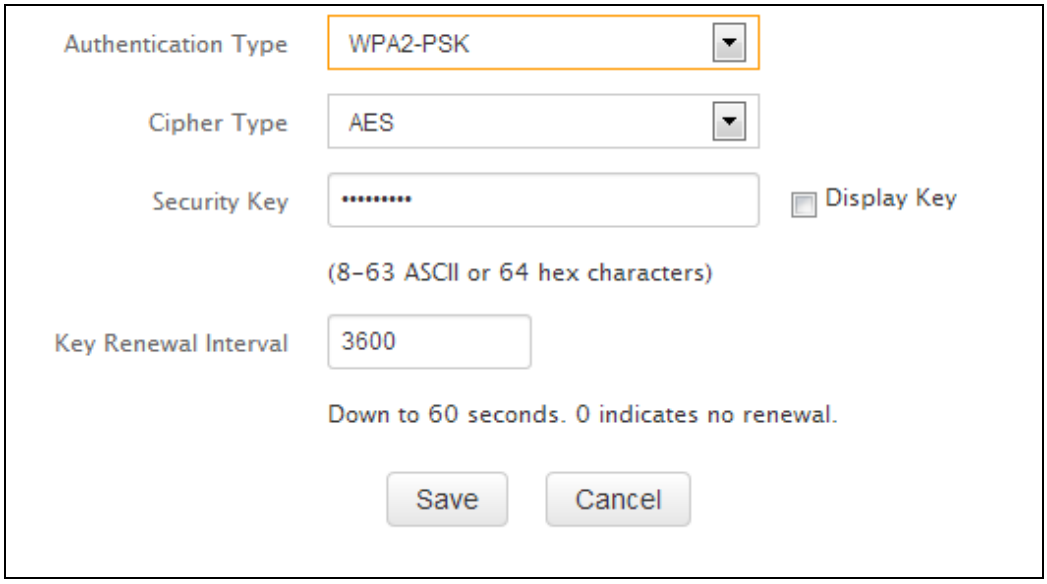
The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature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



- Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- Key Renewal Interval: Enter a valid time period for the key to be changed.

WPA2-PSK

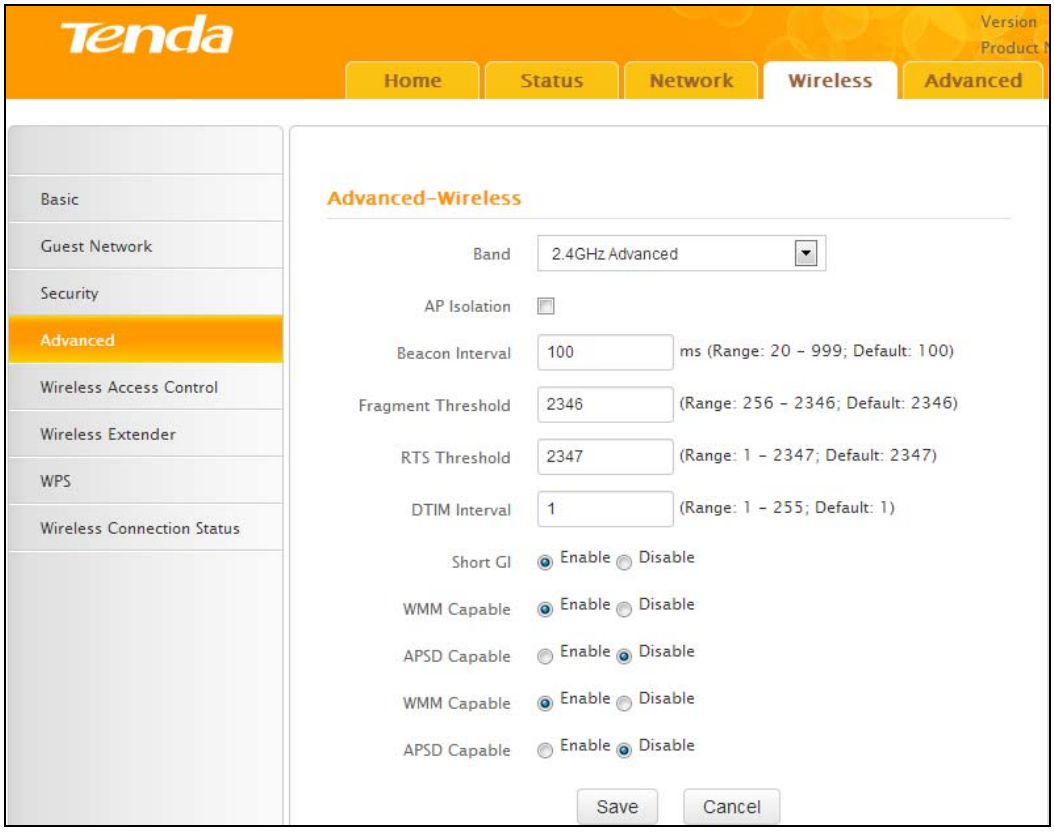
WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP. It is more secured than WPA and WEP.



- Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol) &AES.
- Security Key: Enter a security key, which must be between 8-63 ASCII characters long.
- Key Renewal Interval: Enter a valid time period for the key to be changed.

3.4 Advanced

This section allows you to configure advanced settings, including AP Isolation, Beacon interval，Fragment threshold, RTS threshold, and DTIM interval, etc.



- AP Isolation: Isolates clients connecting to the master SSID.
- Beacon Interval: A time interval between any two consecutive Beacon packets sent by an Access Point to synchronize a wireless network. DO NOT change the default value of 100 unless necessary.
- Fragment Threshold: Specify a Fragment Threshold value. Any wireless packet exceeding the preset value will be divided into several fragments before transmission. DO NOT change the default value of 2346 unless necessary.
- RTS Threshold: If a packet exceeds such set value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. For normal SOHO, it is recommended to keep the default value unchanged, otherwise, the router performance may be degraded.
- DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive in the router's buffer, the router will send DTIM (delivery traffic indication message) and DTIM interval to alert clients of the receiving packets.
- WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- ASPD Capable：Select to enable/disable the auto power saving mode.

3.5 Wireless Access Control

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless network.

- Filter Mode:

Deny Access to Wireless Network: Blocks only devices at specified MAC addresses from connecting to your wireless network.

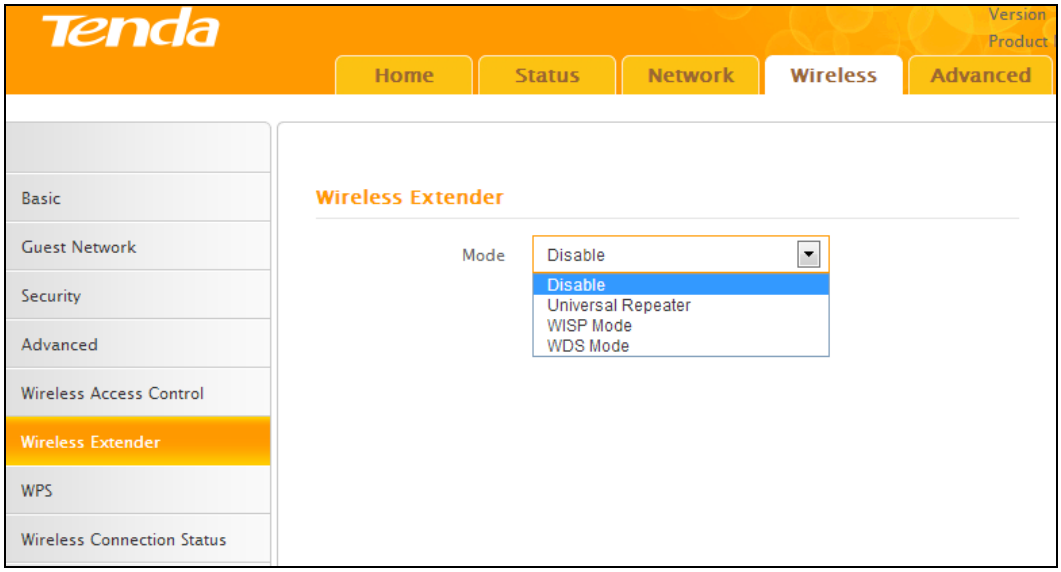
Allow Access to Wireless Network: Allow only devices at specified MAC addresses to connect to your wireless network.

Click **Add** and the screen below will open:

- MAC Address: Enter the MAC address of a wireless client.
- Description: Briefly describe the new entry.
- Status: Select Enable/Disable to enable/disable a corresponding entry.

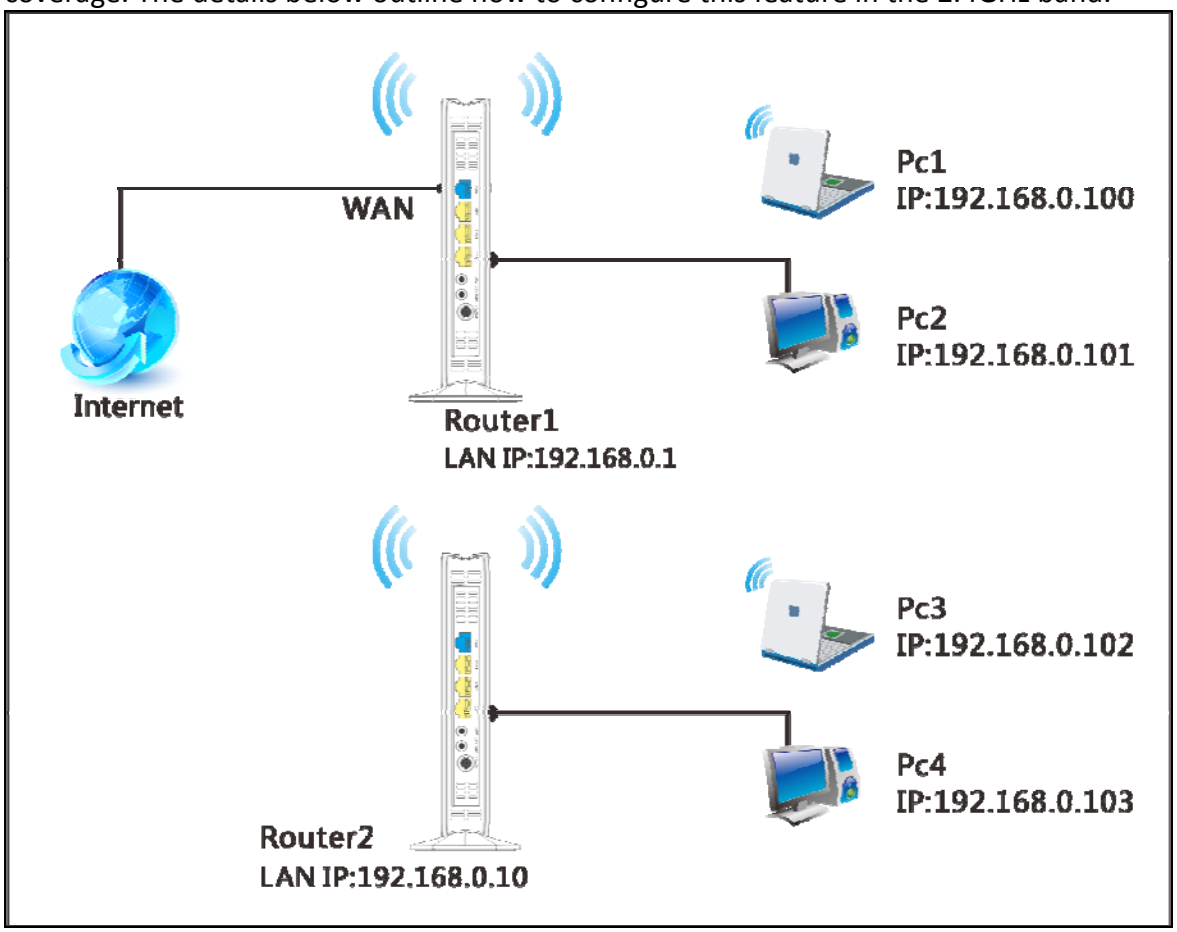
3.6 Wireless Extender

Here you can set the Bridge mode (Universal Repeater, WISP, WDS) to extend wireless coverage.



WDS

WDS (Wireless Distribution System), this feature can be used to extend your existing 2.4Ghz network coverage. The details below outline how to configure this feature in the 2.4GHz band.

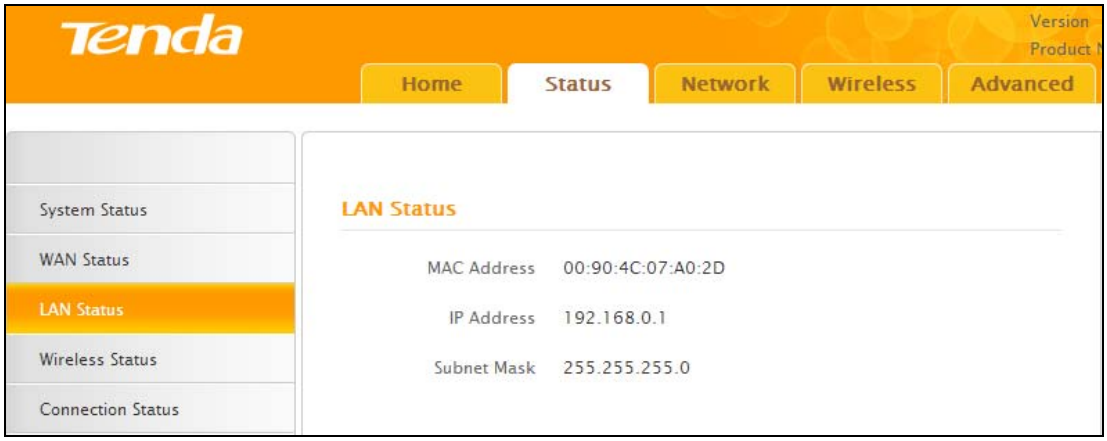


For example:

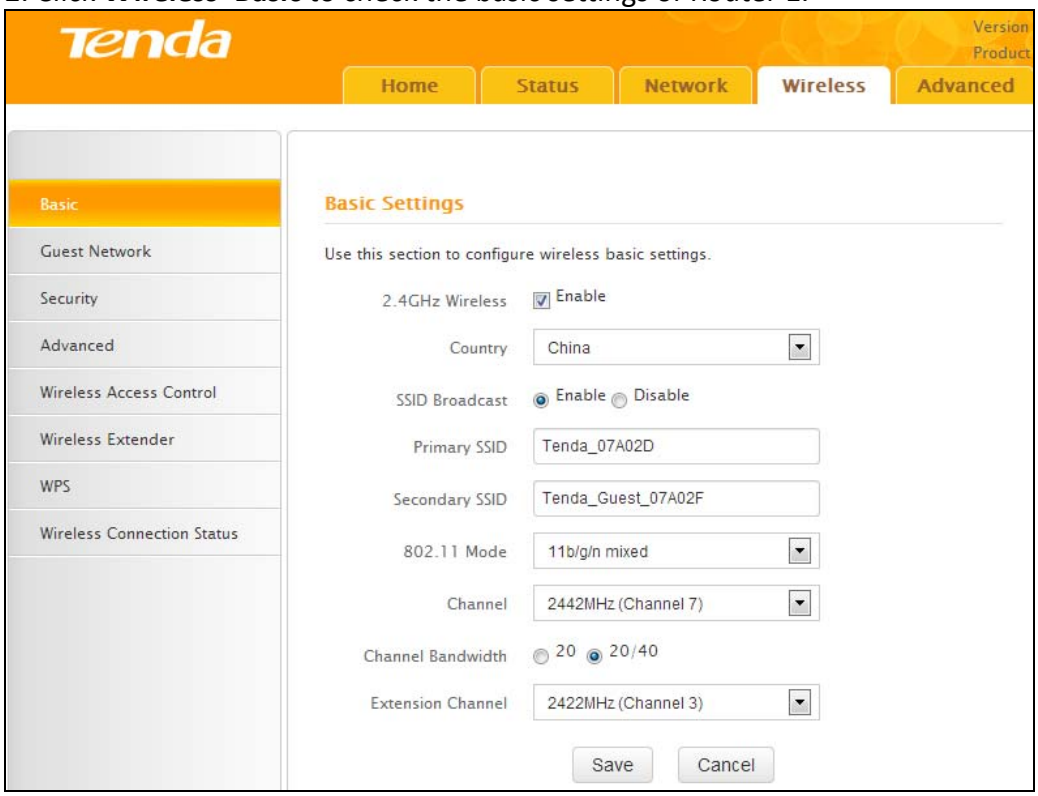
As seen in the figure above, PC1 and PC2 access Internet via a wireless connection to Router 1. While PC3 and PC4 are too far to directly connect to Router 1 for Internet access. Now you can use the WDS bridge feature to let PC3 and PC4 access Internet.

Before you get started:

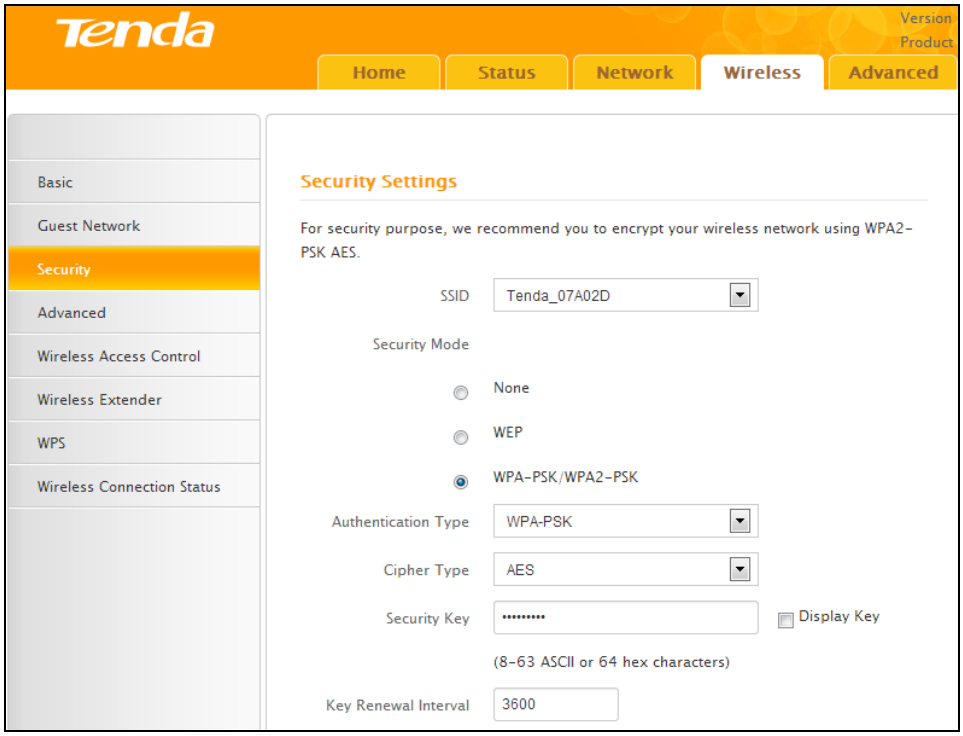
1. View and note down the wireless security settings: security mode, cipher type, security key, etc. on Router 1; Click **Status**>**LAN Status** and check the IP address.



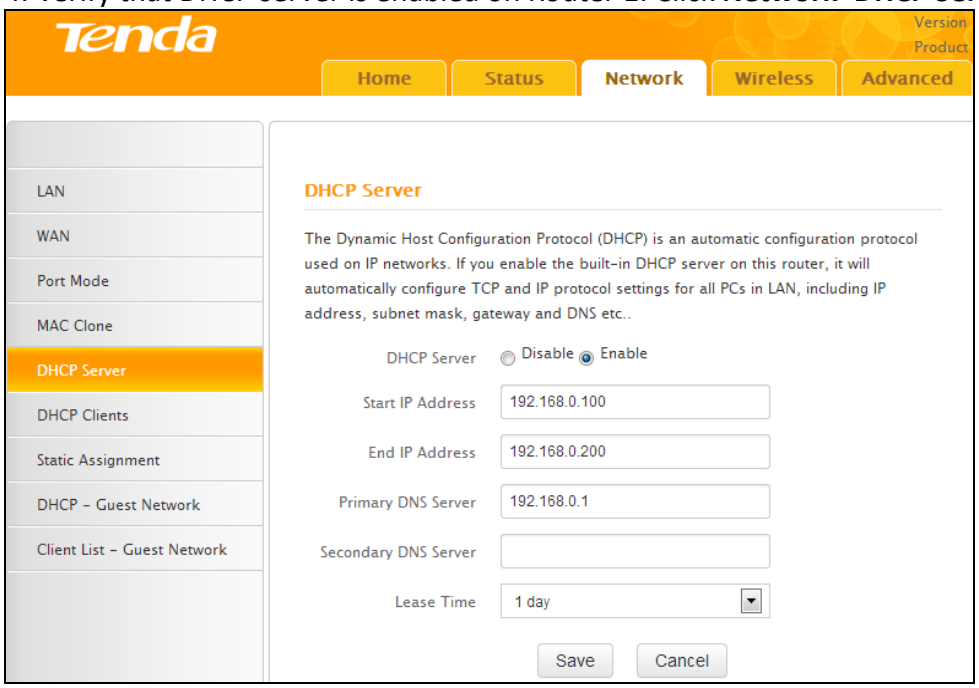
2. Click **Wireless**>**Basic** to check the basic settings of Router 1.



3. Click **Wireless**>**Security** to check wireless security settings of Router 1.



4. Verify that DHCP server is enabled on Router 1: Click **Network>DHCP Server**.



5. Set the LAN IP address of Router 2 to a different address yet on the same net segment as Router 1.

As shown below:

Router 1:

LAN IP: 192.168.0.1;

Subnet Mask: 255.255.255.0;

Router 2:

LAN IP：192.168.0.10;

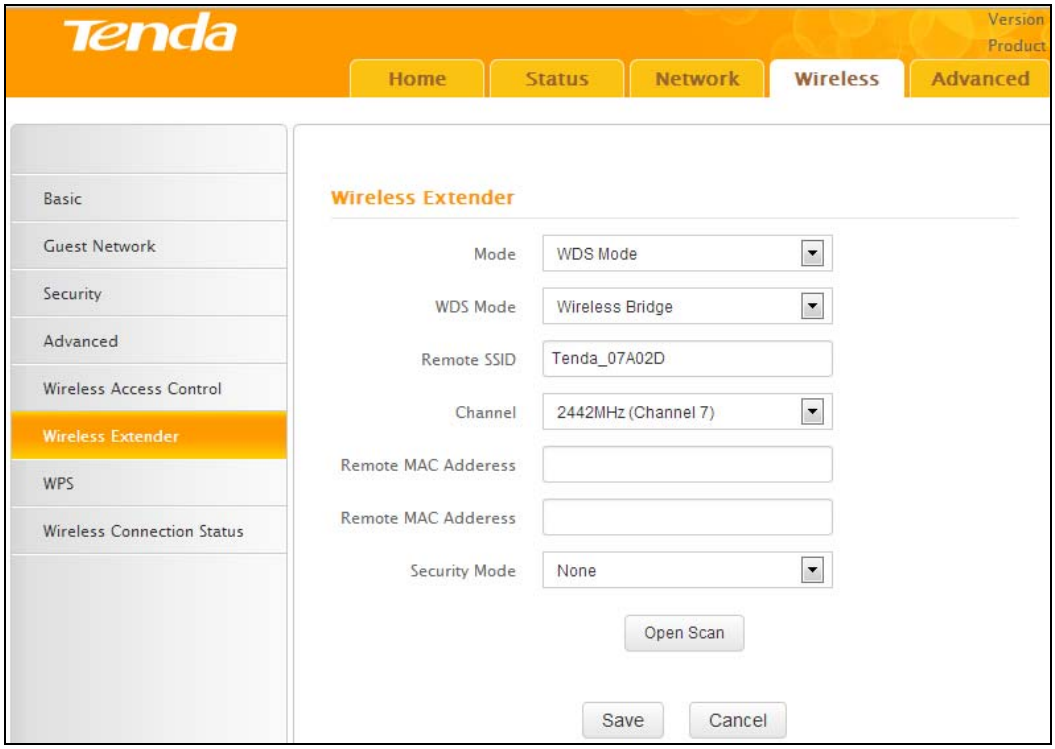
Subnet Mask: 255.255.255.0;

Then do as follows:

1. Configure Router 2:

1) Wireless Working Mode: Select WDS Bridge Mode.

2) Click **Open Scan** to search for Router 1.



3) Select the wireless network to connect and click **OK**.

4) Verify that the SSID, channel, and AP MAC address on the page match those of the added wireless network. If not, manually correct them.

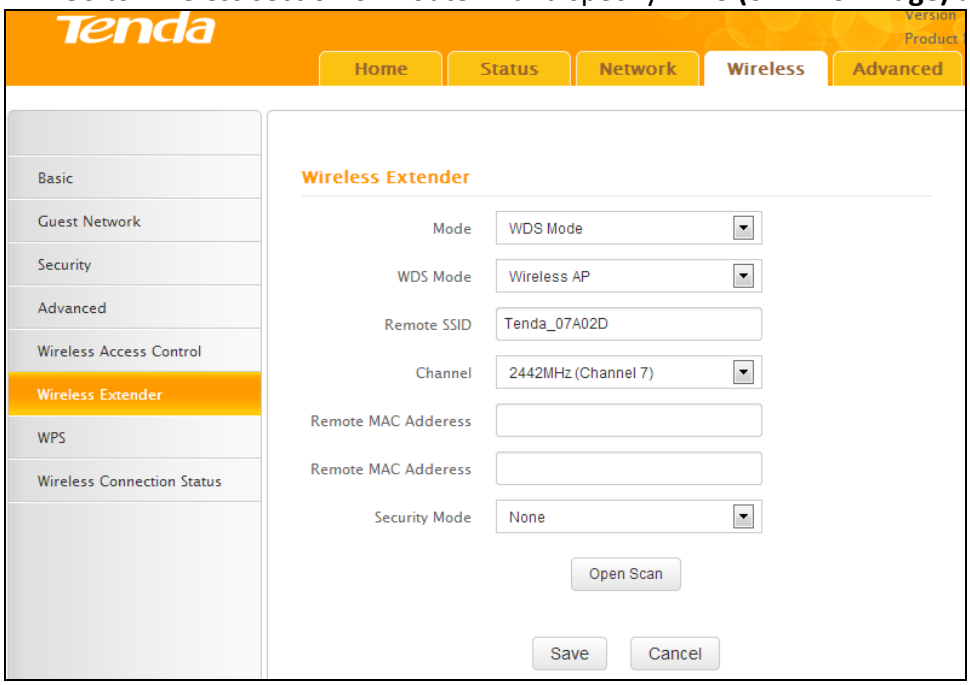
5) Close **Scan** and click **Save** to save your settings.

6) Go to Wireless Security page and set the wireless security settings exactly as they are on the link partner (Router 1).

7) Go to **DHCP Server** to disable the DHCP on Router 2. Now you have finished all settings on Router 2 required for WDS.

2. Configure Router 1:

1. Go to wireless section on Router 1 and specify **WDS (**or **WDS Bridge)** as its wireless working mode.



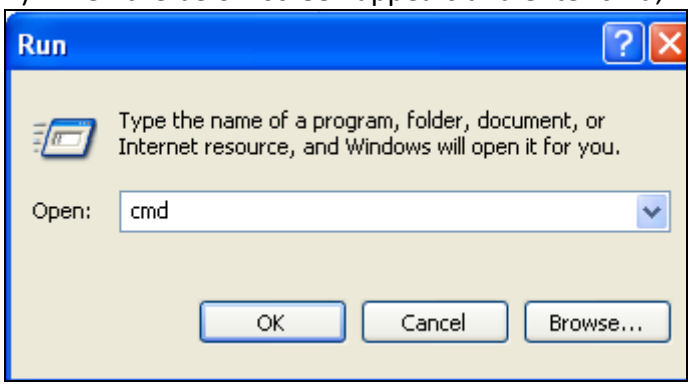
2. Manually enter Router 2's MAC address (Also, you can use the **Open Scan** option as mentioned above) and click **Save** to finish your settings.


Wireless Extender
Mode
WDS Mode
WDS Mode
Wireless AP
Remote SSID
Tenda_000090
Channel
2442MHz (Channel 7)
Remote MAC Adderess
C8:3A:35:00:00:90
Remote MAC Adderess
Security Mode
WPA-PSK/WPA2-PSK
Authentication Type
WPA2-PSK
Cipher Type
AES
Security Key
Display Key
(8-63 ASCII or 64 hex characters)
Close Scan

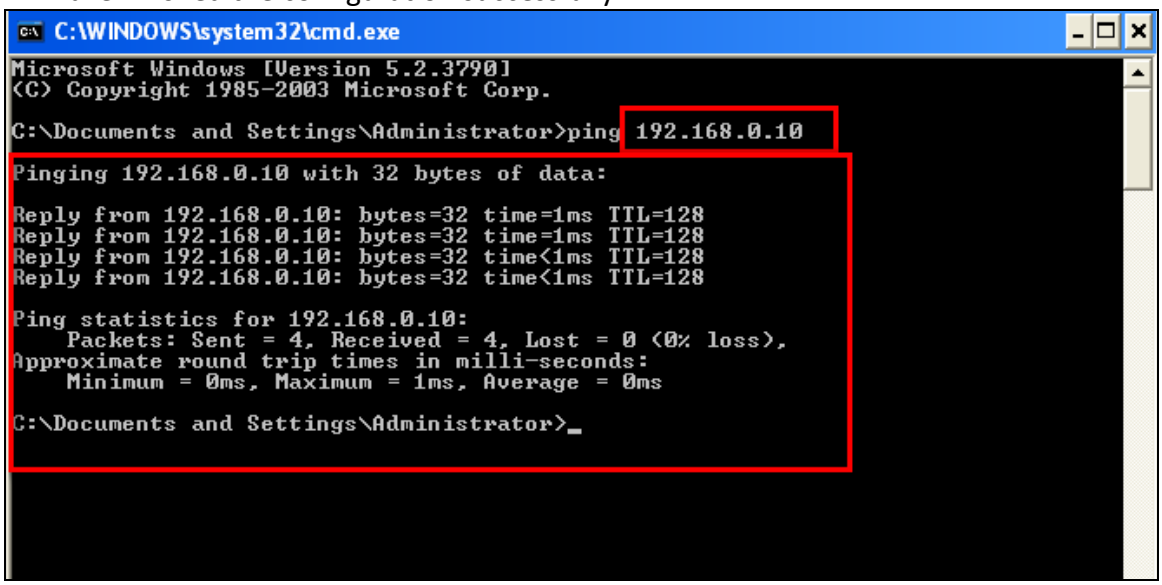
After the above configurations, you can verify the connection by pinging Router 2's IP. Steps are as follows (Take Windows XP OS for example):

1) Click **Start** >**Run**;

2) Then the below screen appears and enter cmd;



3) Input ping 192.168.0.10 in the screen and press Enter. If the folllowing screen appears, it indicates you have finished the configuration successfully.



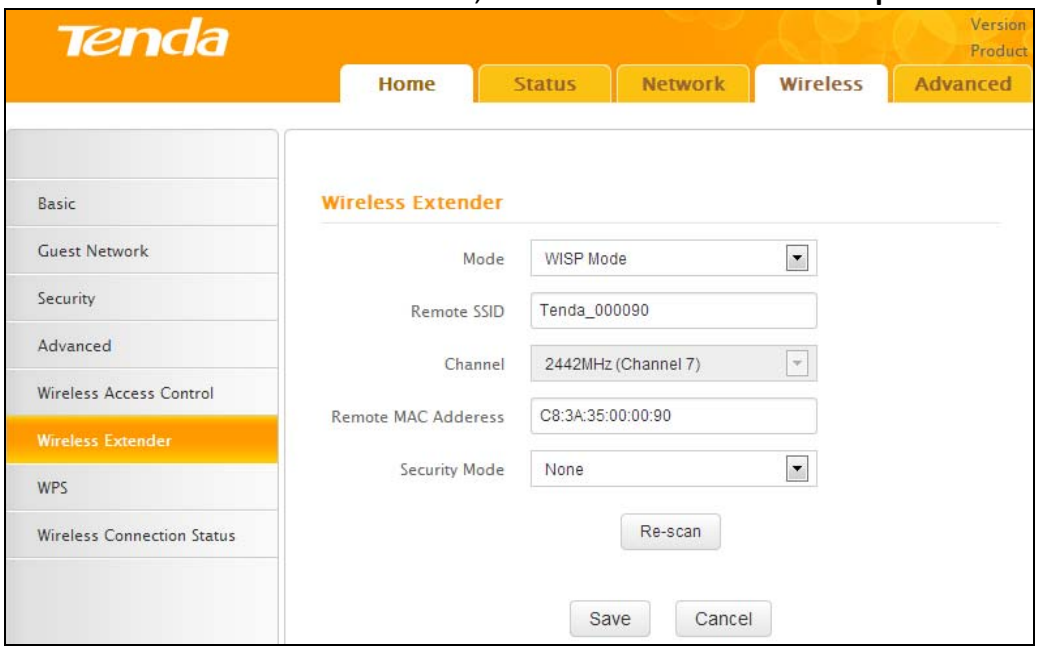
Note

1. WDS feature can only be implemented between 2 WDS-capable wireless devices. Additionally, the SSID, channel, security settings, and security key must be exactly the same on both such devices.
2. Note that the two devices involved must have different IP addresses on the same IP net segment. In addition, it is advisable to disable the DHCP server on either device.

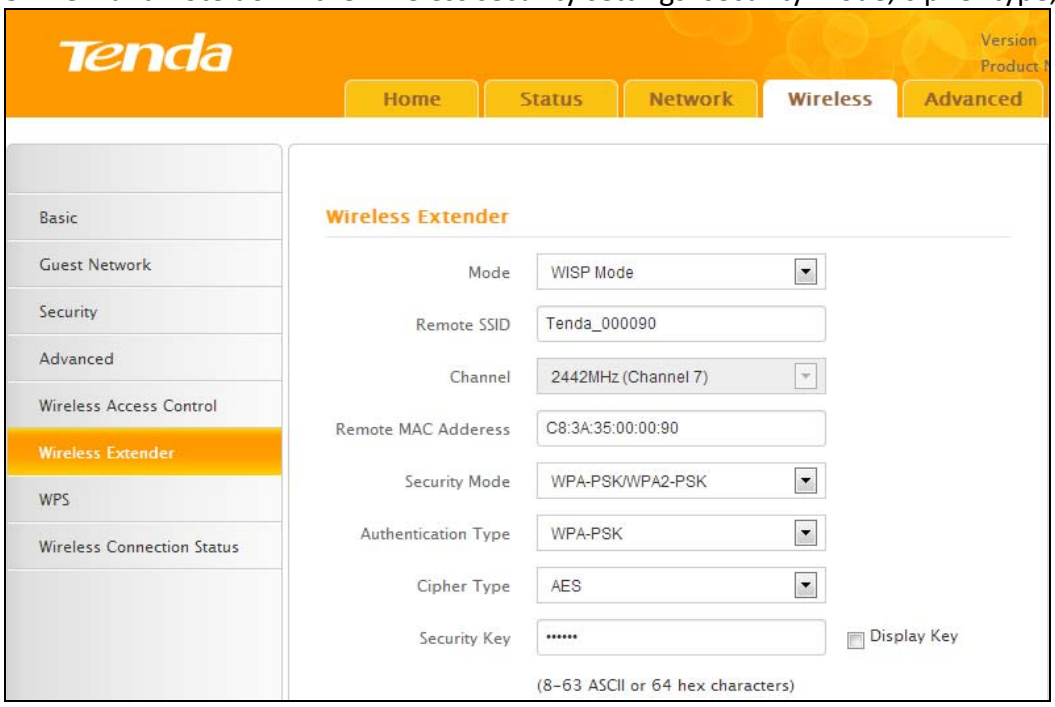
WISP Mode

If your router acquires Internet access from a wireless Access Point, please select WISP mode. Specific steps are as follows:

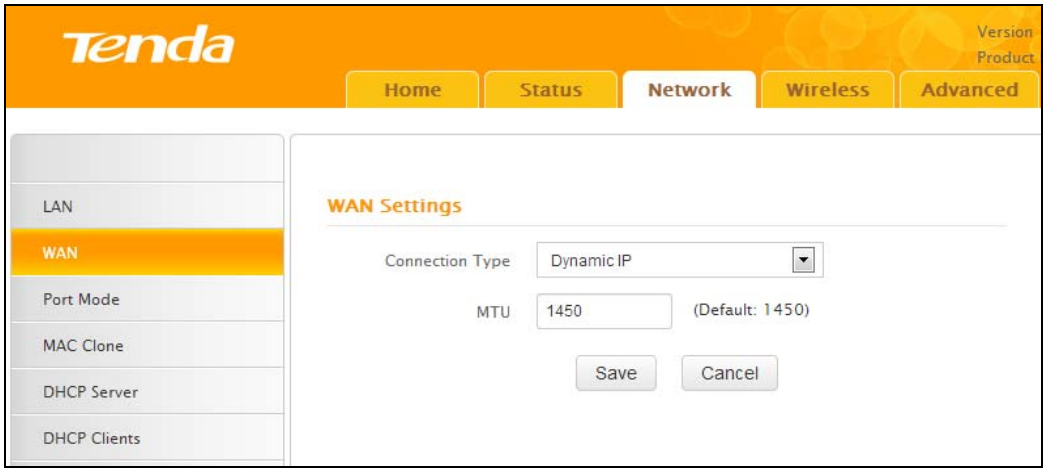
1. Click **Wireless**>**Wireless Extender**, select **WISP mode** and click **Open Scan**.



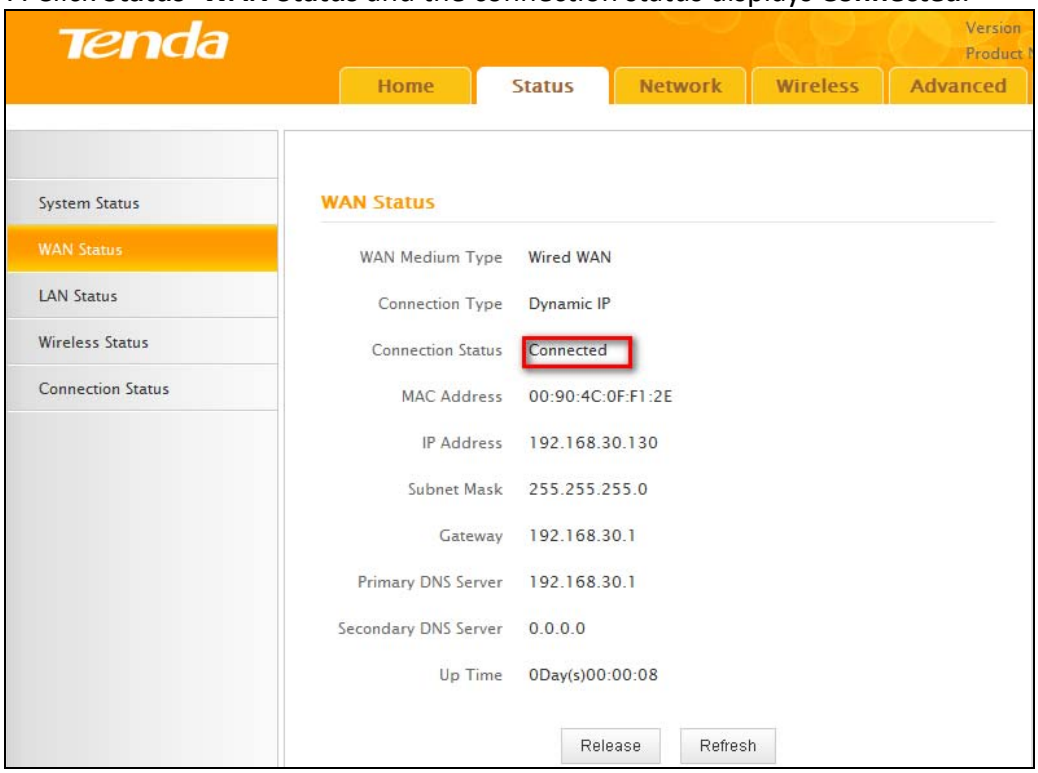
2. Click **Open Scan**, select the AP you wish to connect and click **OK**.
3. View and note down the wireless security settings: security mode, cipher type, security key.



4. Click **Close Scan** and **Save**.
5. Save the settings and the router will reboot automatically.
6. Internet Connection Setup: Click **Network**>**WAN**, select Connection Setup, such as DHCP, and click **Save**.



7. Click **Status**>**WAN Status** and the connection status displays **Connected**.



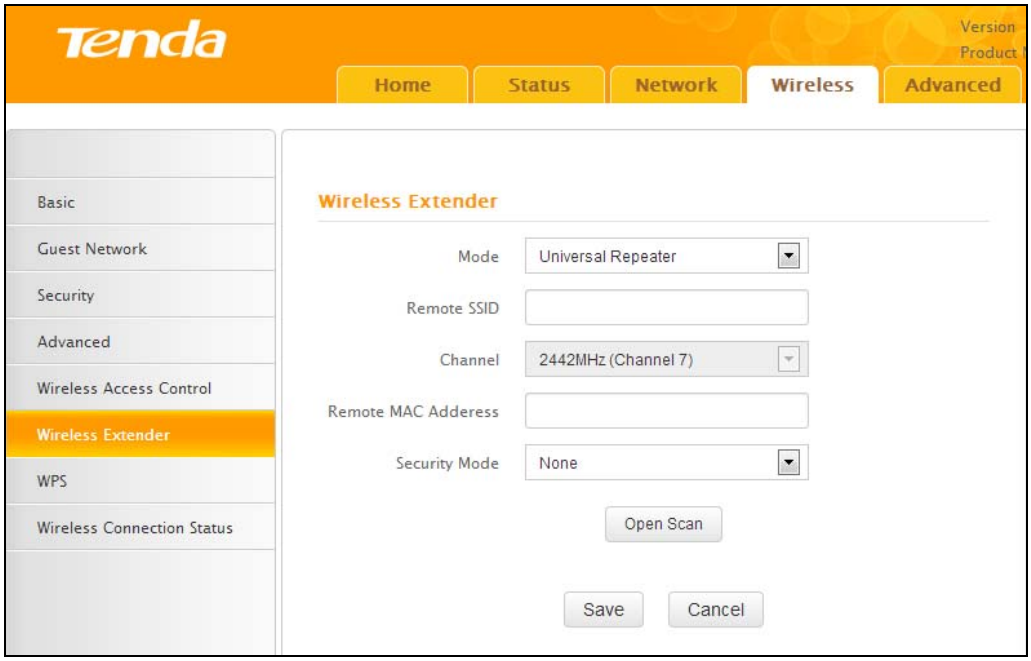
Note

1. When the settings finished, remember to enter **Connection Setup** to set up Internet connection.
2. Verify that the SSID, channel, and security mode on the page match those of the added wireless network. If not, manually correct them.
3. For the normal wireless connection between two routers, do not change this router's SSID settings, including SSID, channel, security mode and security key.

Universal Repeater

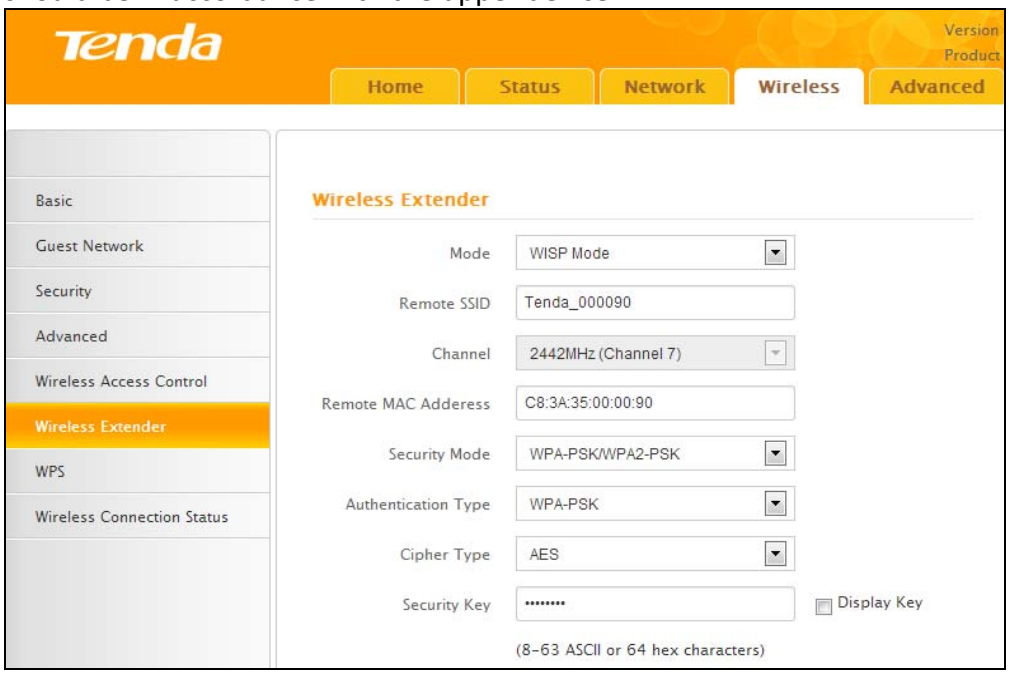
In this mode, the router will relay data to an associated root AP and AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Steps are shown as below:

1. Click **Wireless**>**Wireless Extender**, select **Universal Repeater** in the extender mode and click **Open Scan**.



2. Click **Open Scan**, select the AP you wish to connect and click **OK**.

3. View and note down the wireless security settings: security mode, cipher type, security key, etc., which should be in accordance with the upper device.

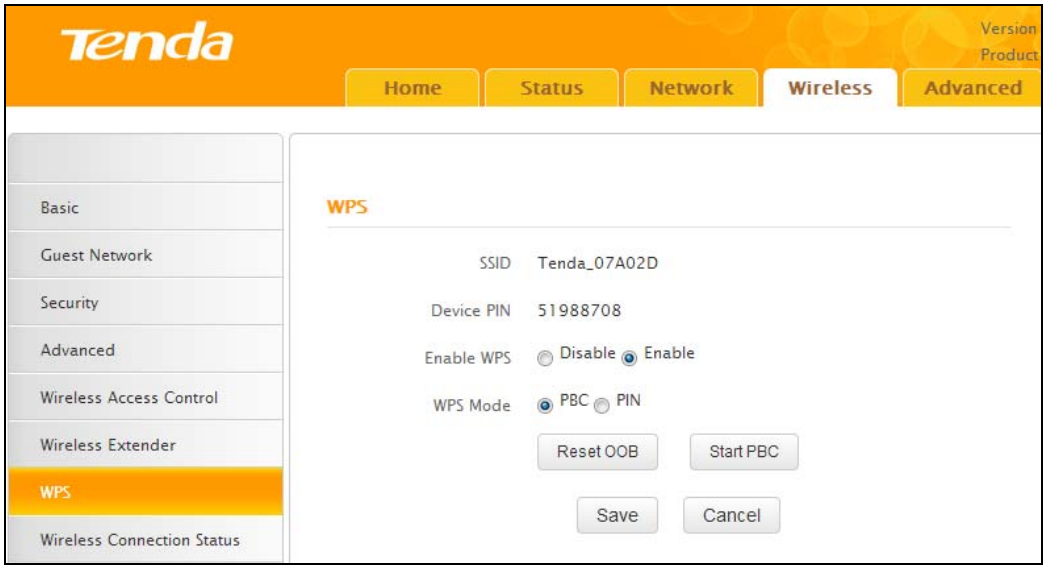


4. Click **Close Scan** and **OK**.

5. Save the settings and the router will restart automatically.

3.7 WPS

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a secure wireless home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. Simply enter a PIN code or press the software PBC button or hardware WPS button (if equipped) and a secure wireless connection can be established.



- Enable WPS: Select to enable/disable the WPS encryption.
- WPS Mode: Select PBC (Push-Button Configuration) or PIN.
- Reset OOB: When selected, the WPS LED turns off and the WPS function will be disabled automatically. The WPS server on the router enters idle mode and will not respond to any client's WPS connection request.

Operation Instructions:

PBC: The WPS LED will blink for 2 minutes after you press the hardware WPS button on the router for 1 second, and means that the PBC encryption method is successfully enabled. An authentication routine will be performed between your router and the WPS/PBC enabled wireless client device during this time, if it succeeds, the wireless client device will connect to your router and the WPS LED will turn off. Repeat the steps above if you want to add more wireless client devices to the router.

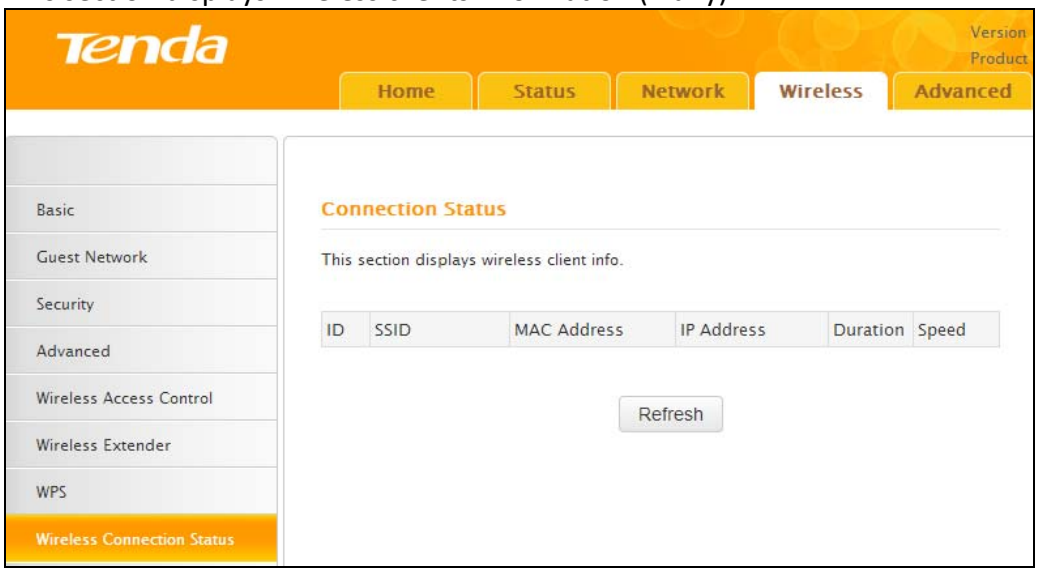
PIN: To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your router while using the same PIN code on the client side for this connection.

Note

To use the WPS encryption, the wireless adapter must be WPS-capable.

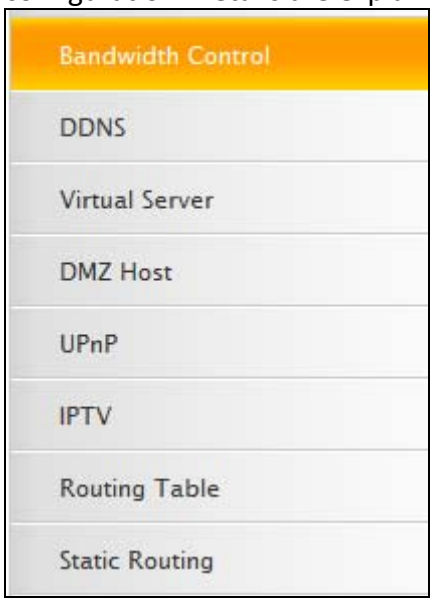
3.8 Connection Status

This section displays wireless clients information (if any).



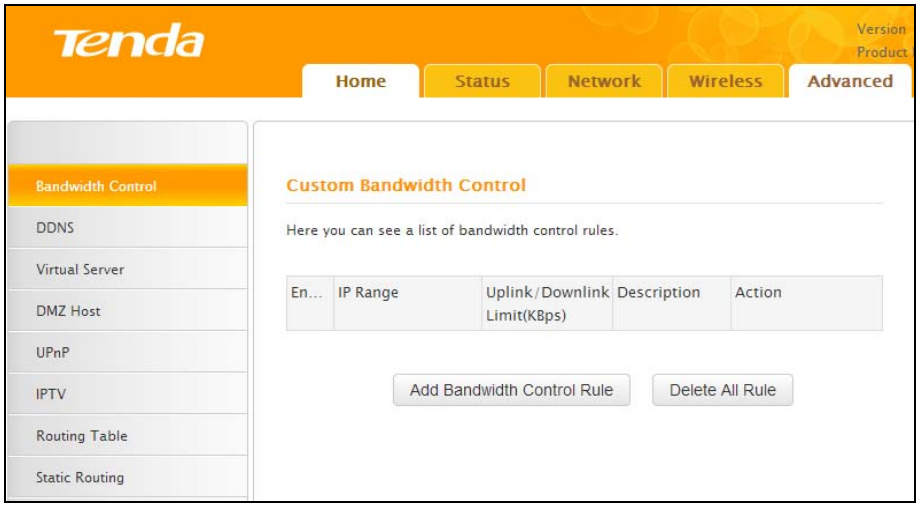
4 Advanced Applications

The **Advanced** tab includes the following 8 submenus: Bandwidth Control, DDNS, Virtual Server, DMZ Host, UPnP, IPTV, Routing Table, and Static Routing. Clicking any of them enters the corresponding interface for configuration. Details are explained below:



4.1 Bandwidth Control

To better manage bandwidth allocation and optimize network performance, use the Bandwidth Control feature.

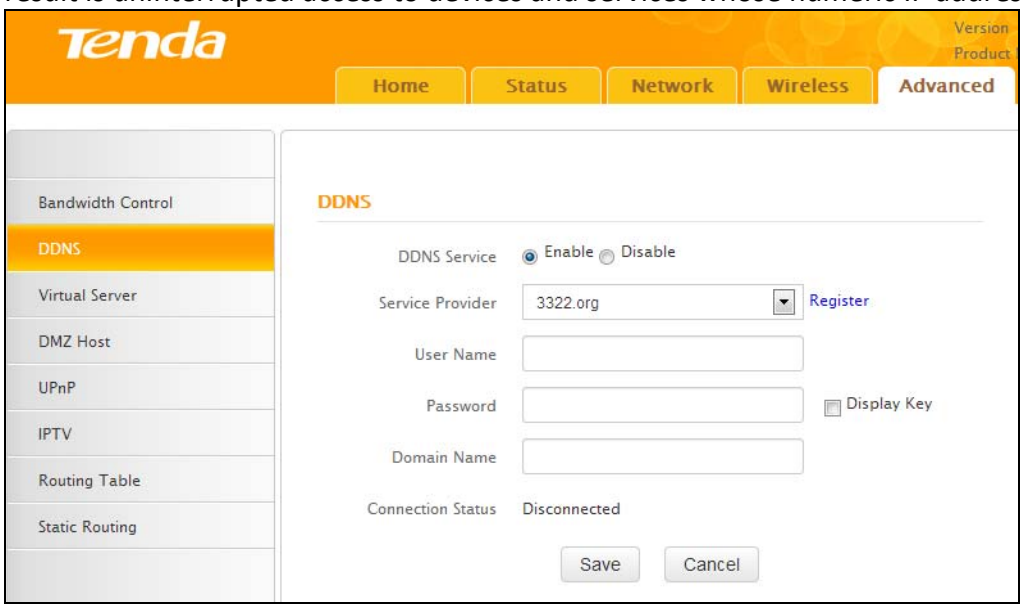


Click **Add Bandwidth Control Rule** and the screen below will open.

- Enable: Check/uncheck to enable/disable current entry. When disabled, corresponding entry will not take effect.
- IP Range: Enter a single IP or an IP range.
- Uplink Bandwidth: Max uplink traffic.
- Downlink Bandwidth : Max downlink traffic.
- Description: Briefly describe the current entry.

4.2 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 and 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 it 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. The result is uninterrupted access to devices and services whose numeric IP address may change is maintained.

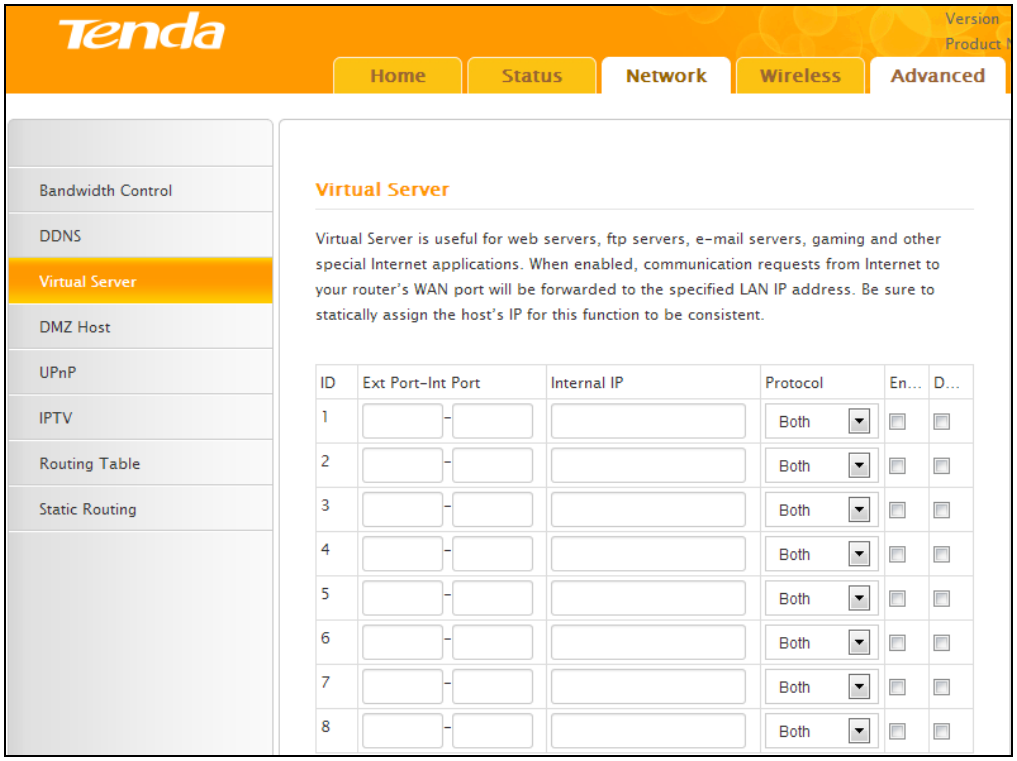


- Service Provider: Select your DDNS service provider from the drop-down menu.
- User Name: Enter the DDNS user name registered with your DDNS service provider.
- Password: Enter the DDNS Password registered with your DDNS service provider.
- Domain Name: Enter the DDNS domain name with your DDNS service provider.
- Connection Status: Displays current status of connection with the DDNS server.

Click **Save** to save your settings.

4.3 Virtual Server

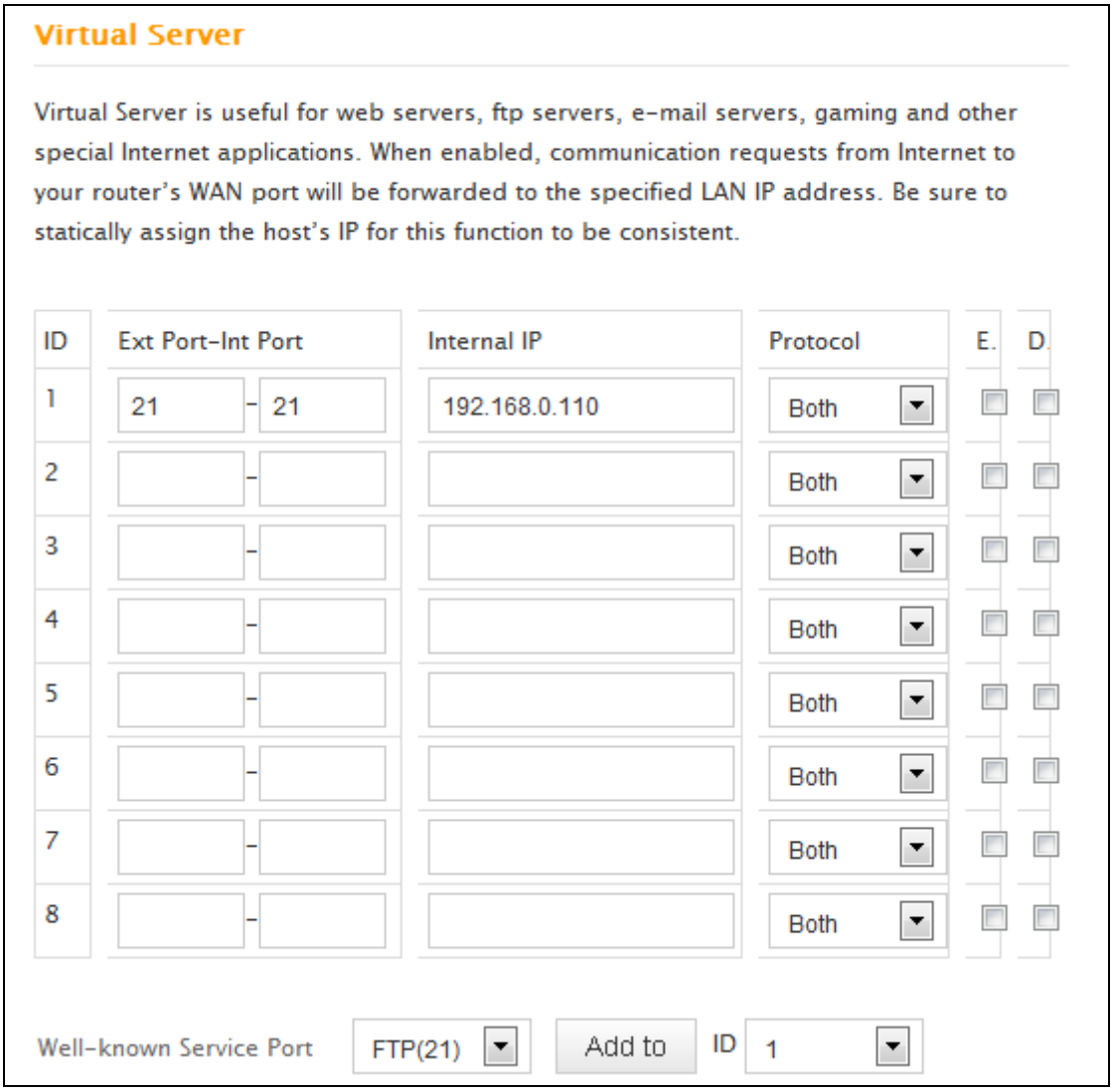
The Virtual Server feature grants Internet users access to services on your LAN. It is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a WAN port on your router for redirection to an internal LAN IP Address.



- Ext Port - Int Port: External Port - Internal Port, enter the WAN/LAN service ports.
- Internal IP: The IP address of a computer used as a server in LAN.
- Protocol: Includes TCP, UDP, and Both. Select “Both” if you are not sure about which protocol to use
- Enable: The corresponding entry takes effect only if you checked this option.
- Delete: Remove a corresponding entry
- Well-known Service Port: The well-known Service Port lists widely used protocol ports. Simply select a port, an entry ID, and click the "Add to" button to transfer the selected port to the corresponding fields of the selected entry. In case you cannot find the port you will need to enter it manually.

Example: You want to share some large files with your friends who are not in your LAN, however, it is not convenient to transfer such large files across the network. You can set up your own PC as a FTP server and use the Virtual Server feature to let your friends access these files. Assuming that the static IP address of the FTP server (Namely, your PC) is 192.168.0.110, you will want your friends to access this FTP server on the default port of 21 using the TCP protocol, details are explained below:

1. Enter 21 in both Ext Port and Int Port fields or select FTP from **Well-known Service Port** and an entry ID 21 will be automatically transferred to the corresponding fields of the selected entry.
2. Enter 192.168.0.110 for the IP Address, select TCP and then select **Enable**.



3. Click **Save** to save your settings.

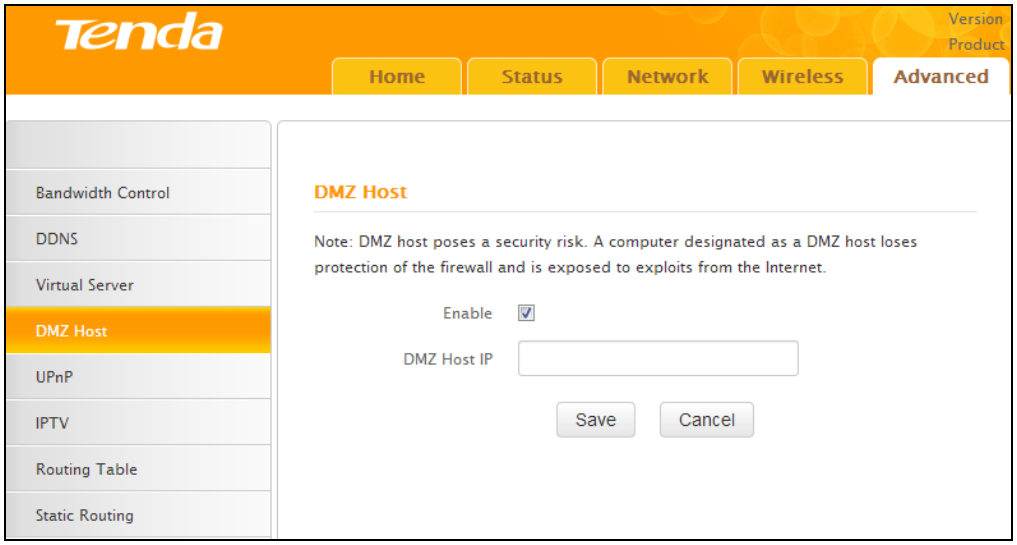
Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx, Assuming the router's WAN IP address is 172.16.102.89, then your friends need to enter "ftp://172.16.102.89: 21" in their browsers.

Note

If you include port 80 in this section, you must set the port for remote (web-based) management to a different number other than 80, such as 8080, otherwise the virtual server feature may not take effect.

4.4 DMZ Host

In some cases, a computer may need to be completely exposed to the Internet for implementation of a 2-way communication. To do so, we will set it as a DMZ host.



- Enable: Check/uncheck to enable/disable the DMZ host feature.
- DMZ Host IP: Enter the IP address of a computer on your LAN which you want to set as a DMZ host. The DMZ host should be connected to a LAN port on the router.

Note

1. Once a PC is set to a DMZ host, it will be completely exposed to Internet, and thus may be vulnerable to attacks as related firewall settings become inoperative.
2. Users on the WAN can access the DMZ host through a corresponding WAN IP address.

4.5 UPnP

UPnP (Universal Plug and Play) allows a network device to discover and connect to other devices on the network. With this feature enabled, hosts in the LAN can request the device to perform special port forwarding so as to enable external hosts to access resources on internal hosts.

- Enable UPnP: Check/uncheck to enable/disable the UPnP feature.

Note

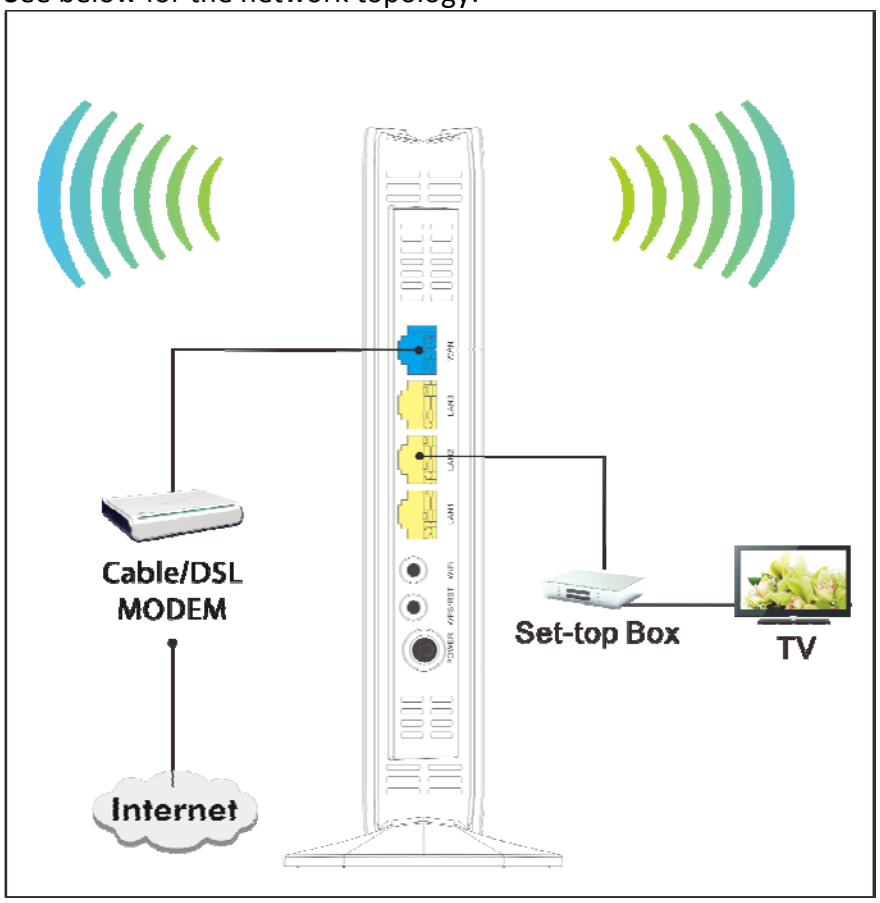
UPnP works in Windows ME, Windows XP, or later, or in an environment with installed application software that supports UPnP. Operational systems needs to be integrated with or installed with Directx 9.0.

4.6 IPTV

The IPTV feature makes it possible to enjoy online videos on your TV set via a set-top box while surfing the Internet concurrently without mutual interference.

- Enable IPTV: Check/uncheck to enable/disable the IPTV feature.
- Enable IPTV STB Port: Check/uncheck to enable/disable the IPTV-specific port.

See below for the network topology:



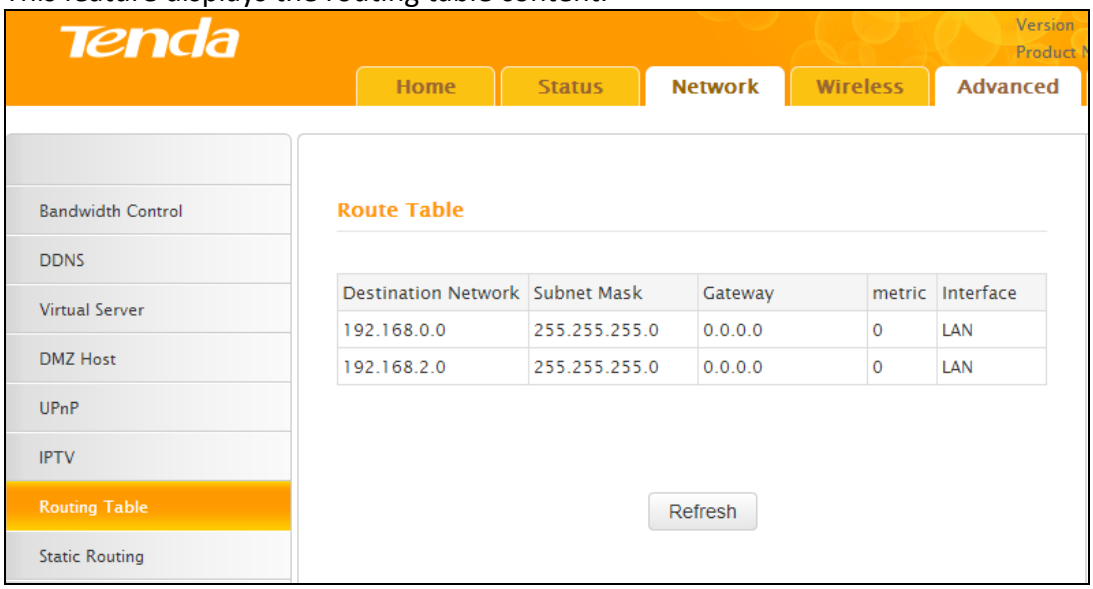
Note

1. If you enabled both options mentioned above, then note below: (a). Set IPTV set-top box's connection type to DHCP/dynamic IP or static IP (IMPORTANT: Note that the set-top box's IP address should be on the same IP net segment as the router's LAN IP.) if the set-top box is connected to any port of LAN ports 1-3. (b). Select the dialup mode provided by your ISP if the set-top box is connected to the IPTV-specific port.
2. After the IPTV port is set for IPTV purpose the PC that connects to such port will not be able to obtain an IP address or access Internet. Consider this situation before configuring this feature. Additionally, LAN ports1-3 can only be used as LAN ports to connect PCs instead of an IPTV set-top box.

3. The IPTV feature is currently not supported on WLAN.

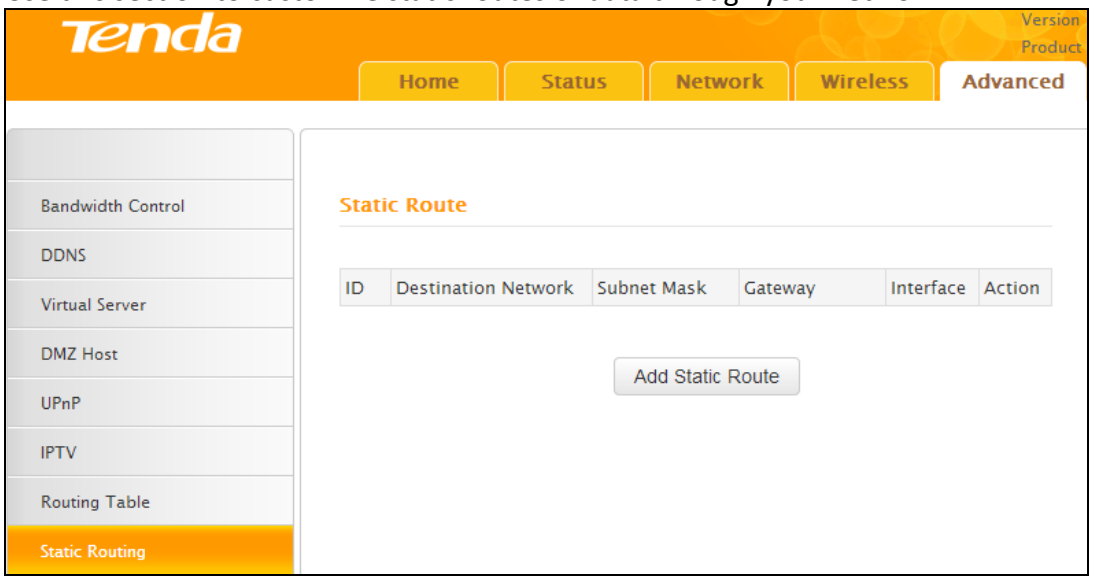
4.7 Routing Table

This feature displays the routing table content.

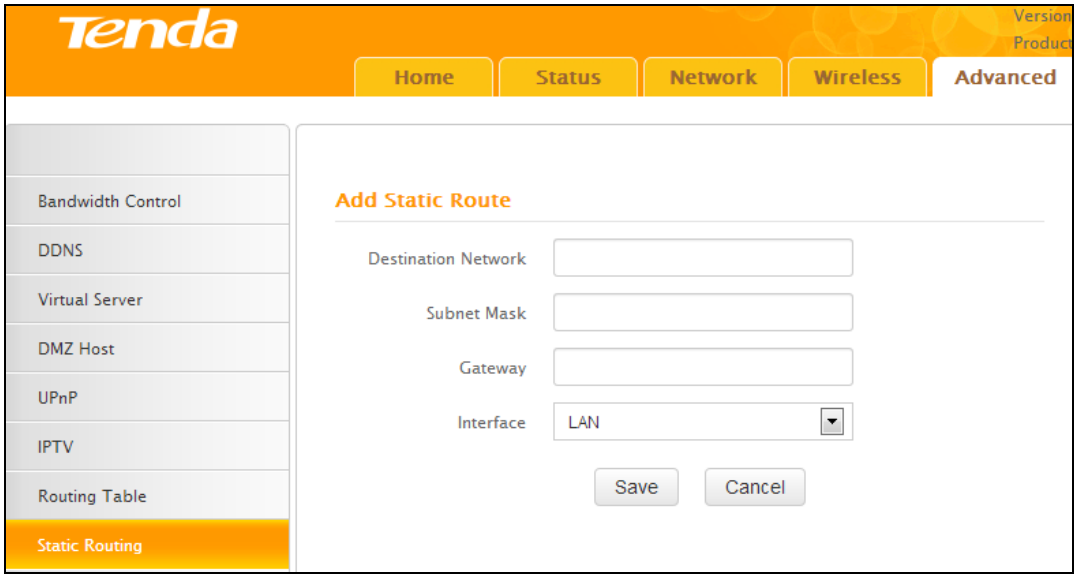


4.8 Static Routing

Use this section to customize static routes of data through your network.



Click **Add Static Route** and here comes the screen below:



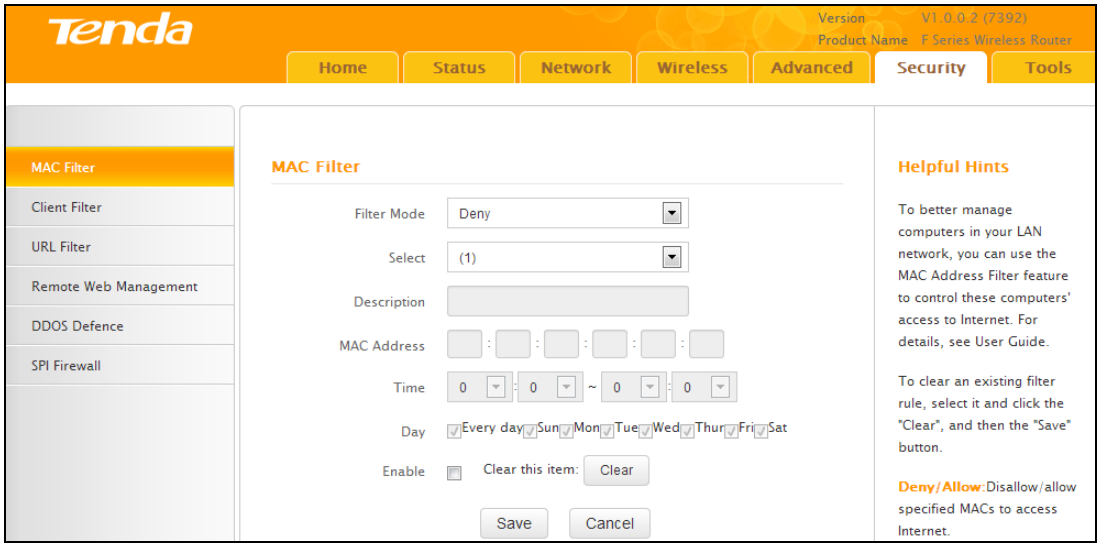
- Destination Network: The IP address of a destination network.
- Subnet Mask: The Subnet Mask that corresponds to the specified destination IP address.
- Gateway: The IP address for next hop.

5 Security

The **Security** tab includes 6 submenus: MAC Filter, Client Filter, URL Filter, Remote Web Management, DDoS Defence and SPI Firewall. Clicking any of them enters the corresponding interface for configuration. Details are explained below:

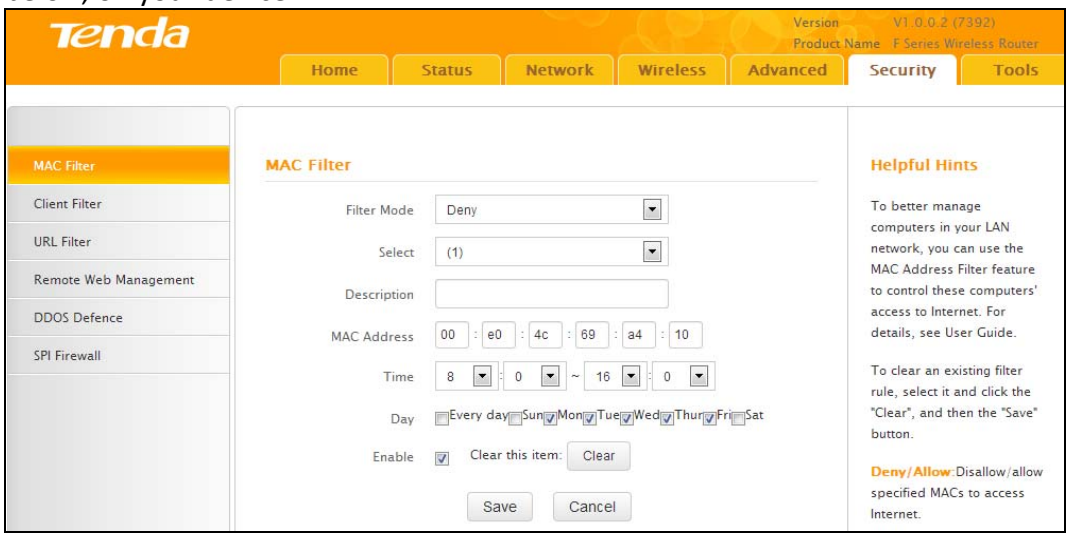
5.1 MAC Filter

To better manage devices in the LAN, you may use the MAC Address Filter function to allow/disallow such devices to access the Internet.



- Filter Mode:
- Disable: Disable the MAC Filter feature.
- Deny Access to Internet: Disallow only specified devices to access Internet, other devices are not restricted.
- Allow Access to Internet: Allow only specified devices to access Internet, other devices are denied.
- Select: Select an ID for the current entry.
- Description: Briefly describe current entry.
- MAC: Specify the MAC address of the computer that you want to restrict.
- Time: Specify a time range for current entry to take effect.
- Day: select a day, or several days, for the entry to take effect.
- Enable: Select to enable/disable corresponding entry.

Example: To prevent a PC at the MAC address of 00:E0:4C:69:A4:10 from accessing Internet between 8:00 and16:00 on working days: from Monday to Friday, configure the same settings as shown in the screen below, on your device:

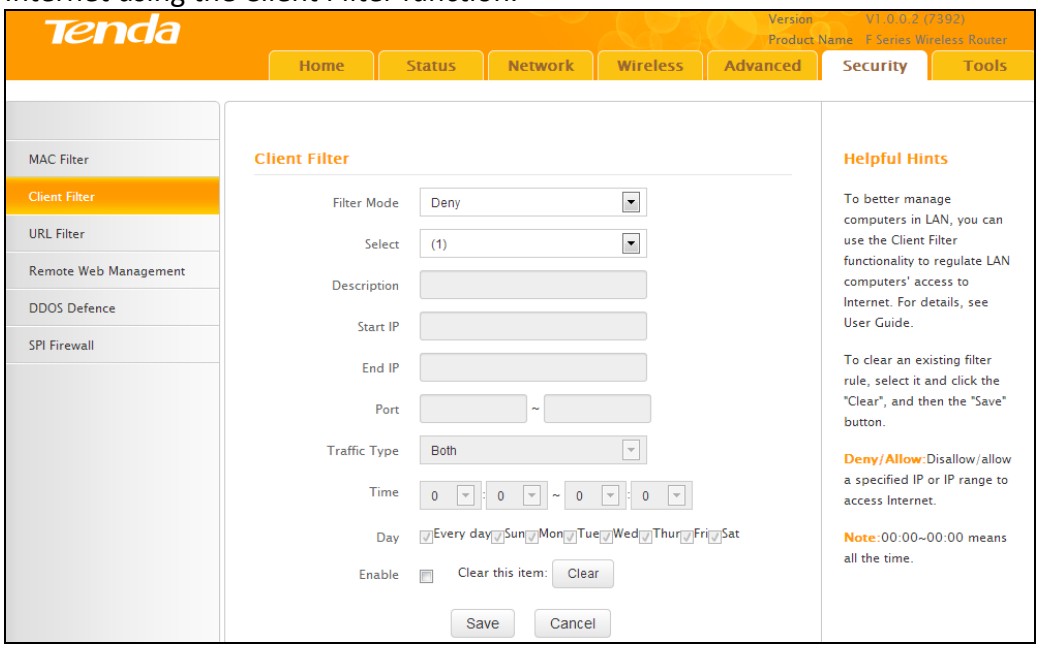


Tips ----------

1. Maximum 10 entries can be configured in MAC Filter.
2. After saving your configurations, for correct time, please go to **Tools**>**Time** to configure your router's system time.

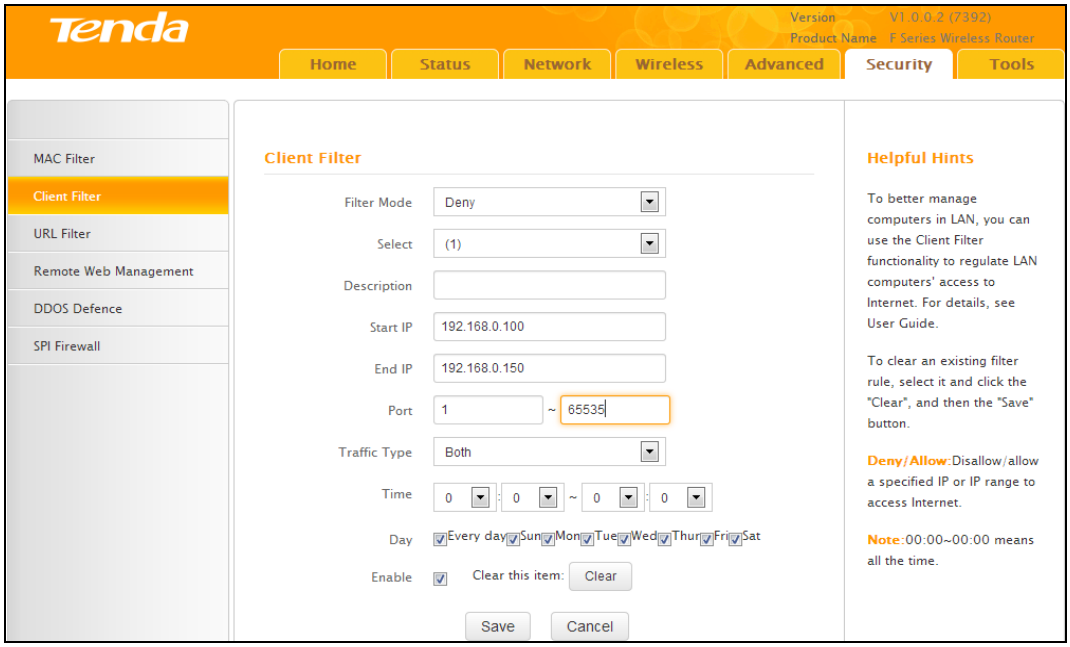
5.2 Client Filter

To better manage devices in the LAN, you can allow or disallow the devices to access certain ports on the Internet using the Client Filter function.



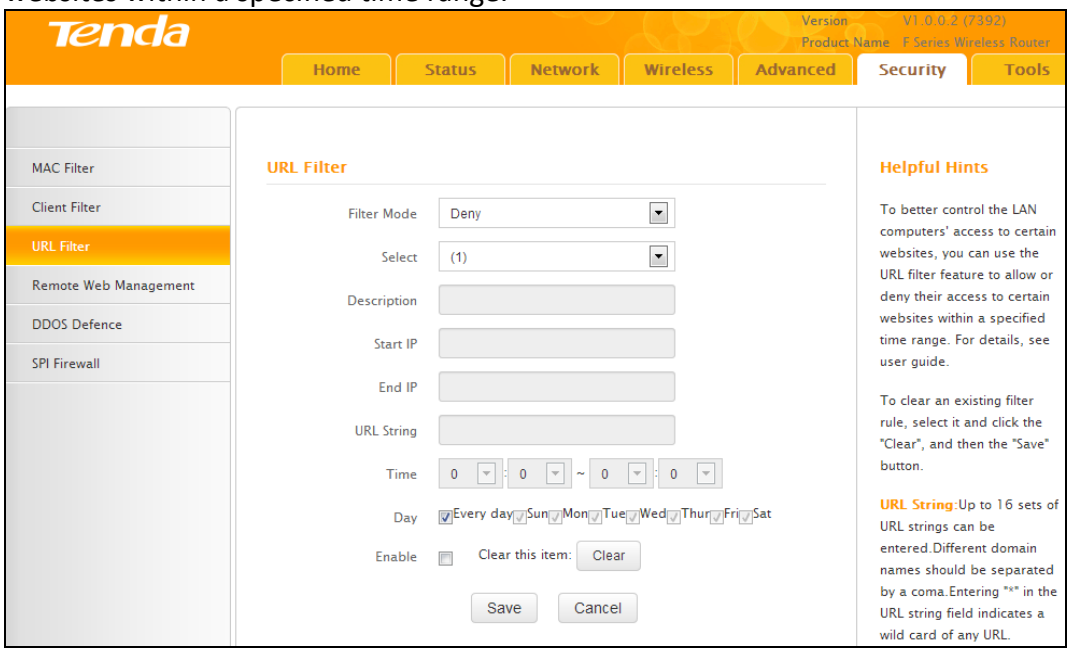
- Filter Mode: Select Deny or Allow.
- Select: Select an ID for the current entry.
- Description: Briefly describe the current entry.
- Start IP: Enter a starting IP address.
- End IP: Enter an ending IP address.
- Port: Enter TCP/UDP protocol port number, it can be a single port or a range of ports.
- Traffic Type: Select a protocol or protocols for the traffic (TCP/UDP/Both).
- Time: Specify a time range for current entry to take effect.
- Day: select a day or several days for current entry to take effect.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched addresses to pass through router).

Example: To prohibit PCs within the IP address range of 192.168.0.100--192.168.0.150 from accessing the Internet, use the following example:



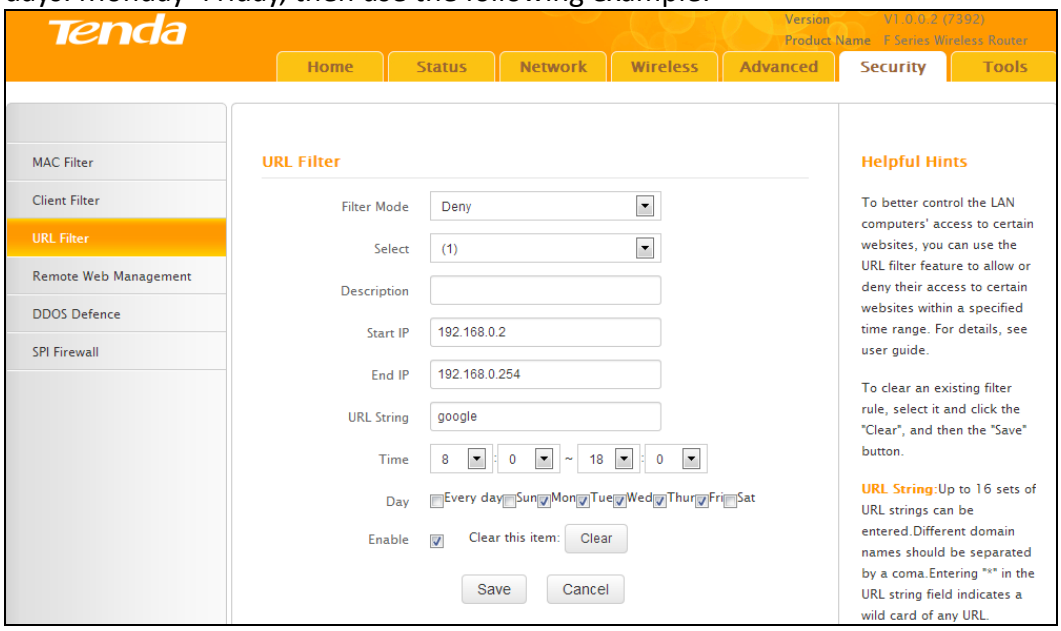
5.3 URL Filter

To better control LAN devices, you can use the URL filter function to allow or disallow PC's to access certain websites within a specified time range.



- Filter Mode: Select Deny or Allow.
- Select: Select an ID for current entry.
- Enable: Check to enable or uncheck to disable a corresponding filter rule (allow/disallow matched addresses to pass through router).
- Description: Briefly describe the current entry.
- Start IP: Enter a starting IP address.
- Start IP: Enter a starting IP address.
- URL String: Enter domain names or a part of a domain name to be filtered out.
- Time: Specify a time range for current entry to take effect.
- Day: select a day or several days for current entry to take effect.

If you want to disallow all computers on your LAN to access Google.com from 8:00 to 18:00 on working days: Monday- Friday, then use the following example:

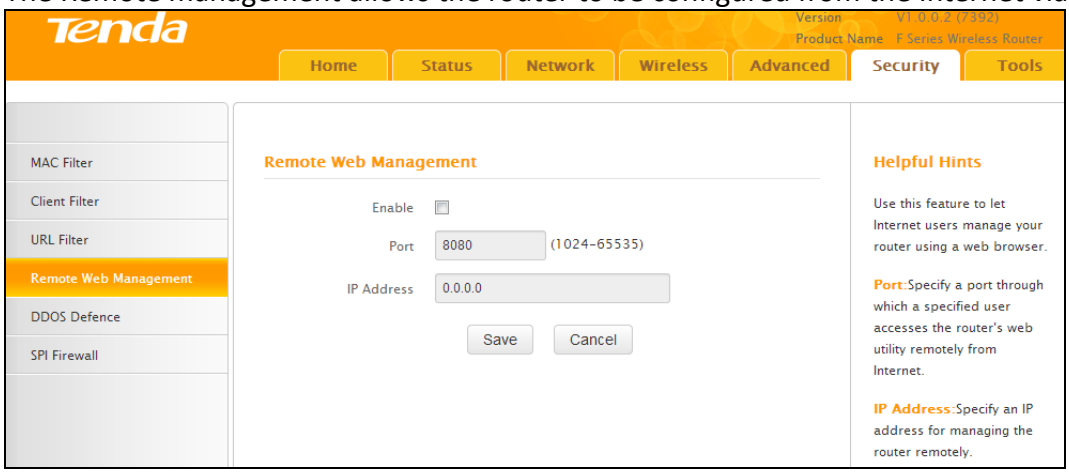


Note

Each entry can include up to 16 domain names, each of which must be separated with the quotation symbols " ".

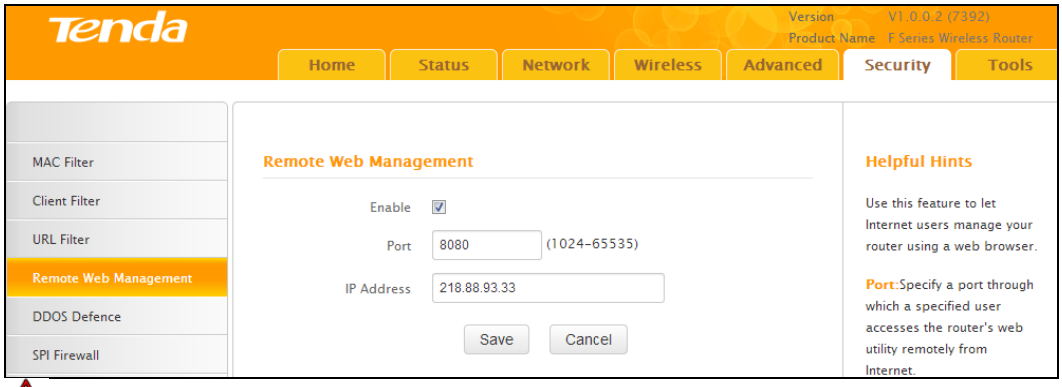
5.4 Remote Web Management

The Remote management allows the router to be configured from the Internet via a web browser.



- Enable: Select to enable the Remote Web-based Management feature.
- Port: Remote admin port is the port number used to access the router from Internet.
- IP Address: Enter the IP address of the PC on the Internet authorized to manage your router remotely.

For example: If you want to allow only the PC at the IP address of 218.88.93.33 from the Internet to access the router's web-based utility via port 8080, then configure the same settings as shown below on your router.



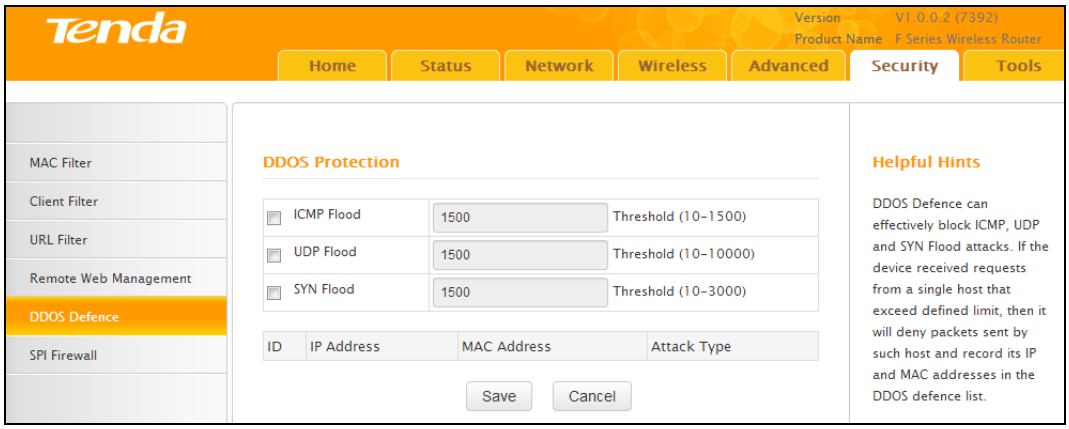
Note

1. The default port is 8080. Do not change it.
2. To access the router via port 8080, enter "http://x.x.x.x:8080" where "x.x.x.x" represents the Internet IP address of the router and 8080 is the port used for the Web-Management interface. Assuming the router's Internet IP address is 220.135.211.56, then simply replace the "x.x.x.x" with "220.135.211.56" (namely, http://220.135.211.56:8080).

Leaving the IP address field at "0.0.0.0" makes the router remotely accessible to all the PCs on the Internet. Entering a specific IP address, such as 218.88.93.33, makes the router only remotely accessible to the PC at the specified IP address.

5.5 DDOS Defence

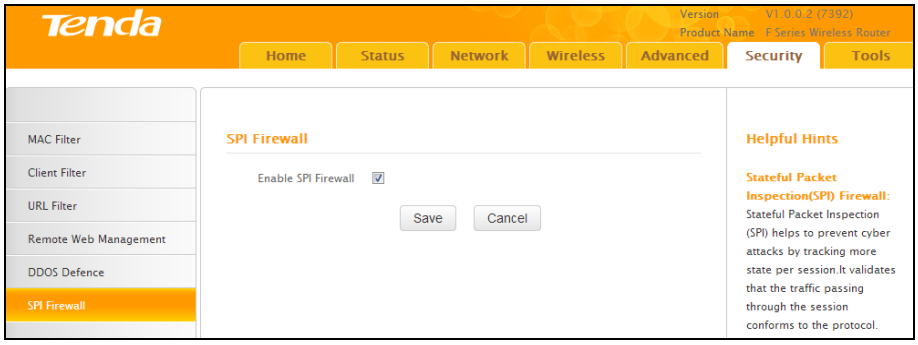
The DDOS Defence feature effectively blocks ICMP, UDP, and SYN flooding attacks. When the number of ICMP, UDP, or SYN packets received exceeds the defined threshold, the router will record its IP and MAC addresses in the "DDOS Defence List".



- ICMP Flood: If an IP receives the number of ICMP request packets that exceeds the defined limit continuously from the same sender within one second, then such IP is considered to encounter an ICMP Flood attack.
- UDP Flood：If an IP receives, on an identical port, UDP packets exceeding the defined limit continuously from the same sender within a second, then the port is suffering a UDP Flood attack.
- SYN Flood: If an IP receives, on an identical port, TCP SYN packets exceeding defined limit continuously from the same sender within a second, then the port is suffering a SYN Flood attack.

5.6 SPI Firewall

Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.



Tips ----------

Once SPI enabled, DMZ and remote web management will be invalid.

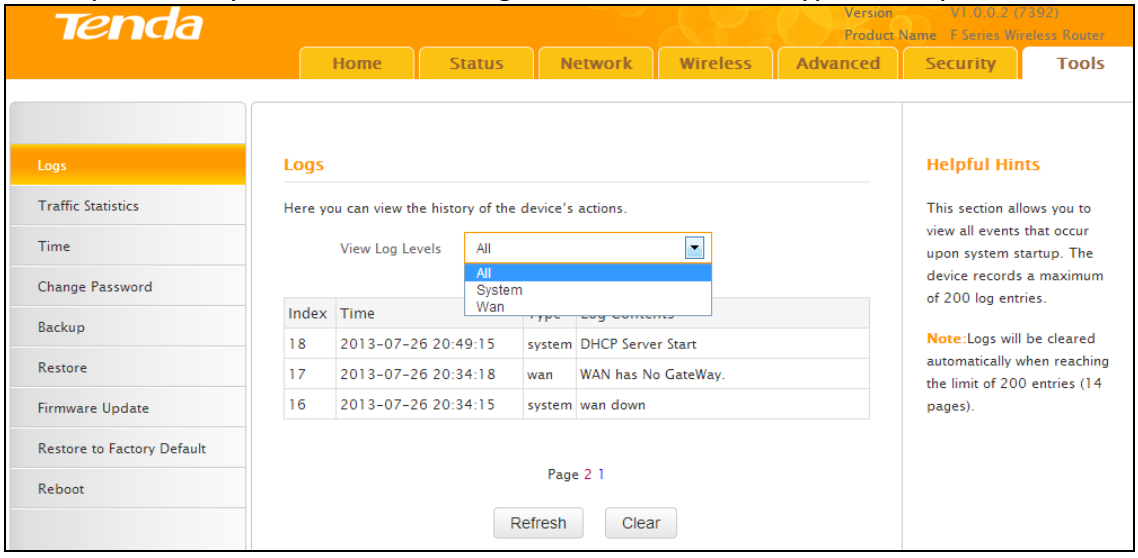
---

6 Tools

The "Tools" tab includes 9 submenus: Logs, Traffic Statistics, Time, Change Password, Backup, Restore, Firmware Update, Restore to Factory Default, and Reboot. Clicking any of them enters the corresponding interface for configuration. Details are explained below:

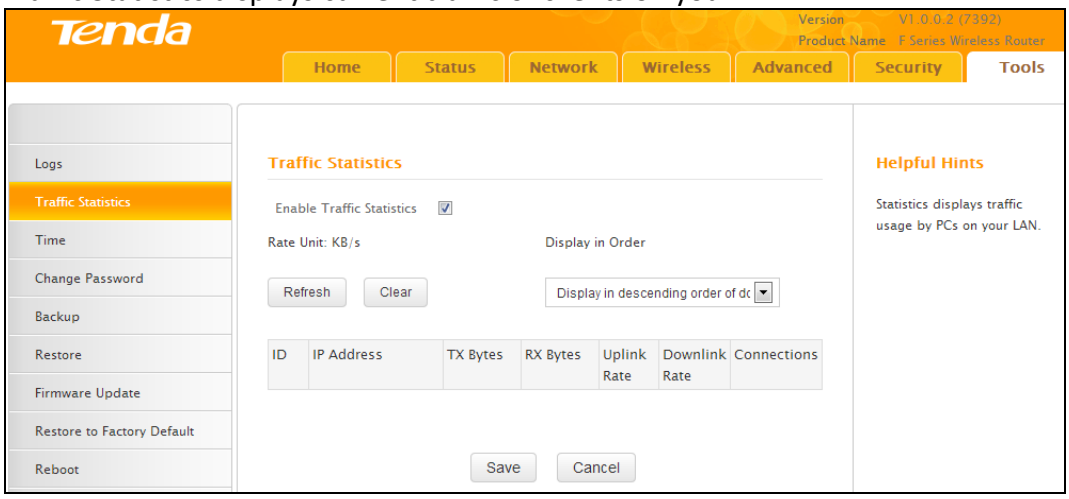
6.1 Logs

The Syslog option allows you to view all events that occur on system startup and checks whether there is an attack present in your network. The logs are classified into 3 types: All, System, and WAN.



6.2 Traffic Statistics

Traffic Statistics displays current traffic of clients on your LAN.



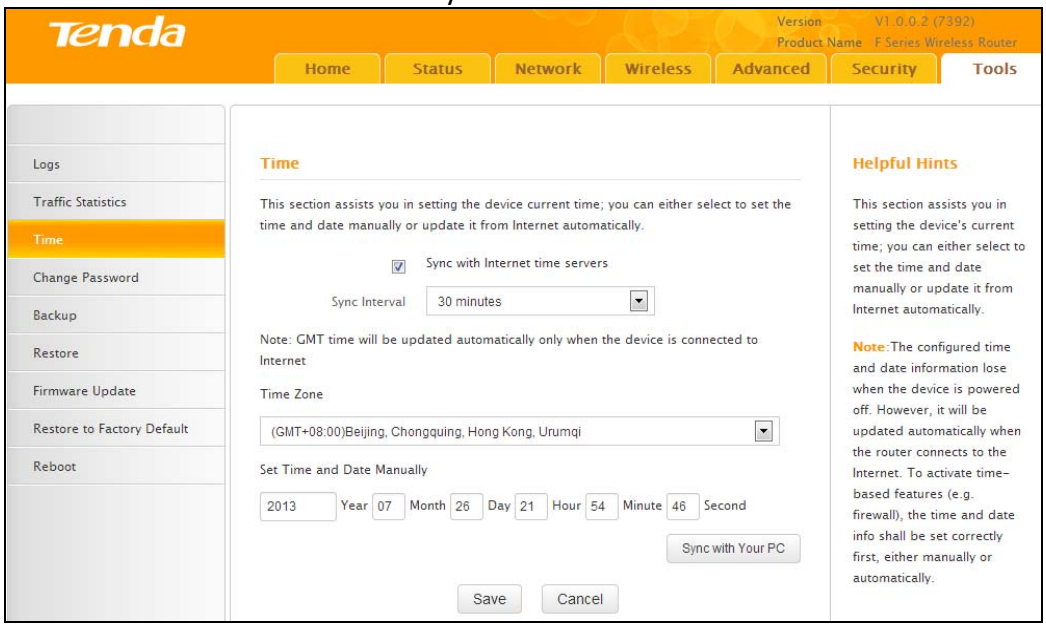
- Enable Traffic Statistics: Determine whether to enable the Traffic Statistics feature on internal users.
- Refresh: Click it to update statistic data.
- Clear: Click it to remove statistic data.

Note

Enabling the Traffic Statistics feature may degrade the router's performance. Do not enable it unless necessary.

6.3 Time

This section lets you configure, update, and maintain the correct time on the internal system clock. You can either select to set the time and date manually or automatically obtain the GMT time from Internet. Note that the GMT time is obtained only when the router is connected to the Internet.

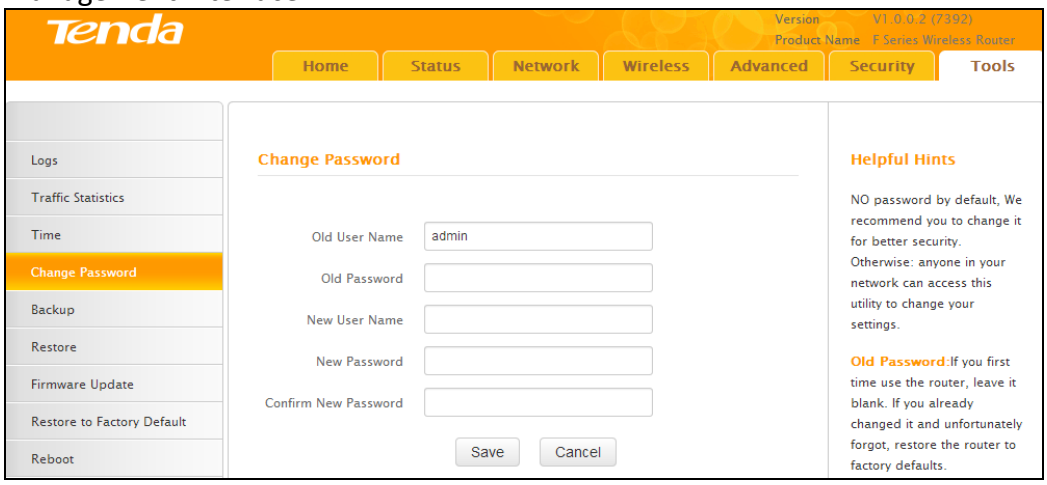


- Sync with Internet time servers: Time and date will be updated automatically from the Internet.
- Sync Interval: Specify a time interval for periodic update of time and date information from the Internet.
- Time Zone: Select your current time zone.
- Sync with Your PC: Click it to copy your PC's time to the router.

6.4 Change Password

This section allows you to change login password and user name for accessing the router's Web-based

management interface.



Both login password and user name are preset to “admin” by default. To change either or both, do the following:

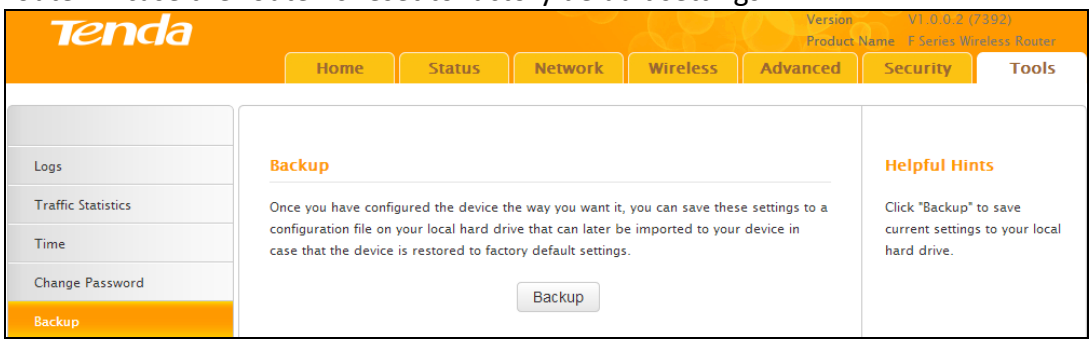
1. Enter your current user name and password in **Old User Name** and **Old Password fields**.
2. Enter a new user name and a new password in **New User Name** and **New Password** fields.
3. Click **Save**.

Note

For security purpose, it is highly recommended that you change the default login password and user name as part of the initial configuration of your router.

6.5 Backup

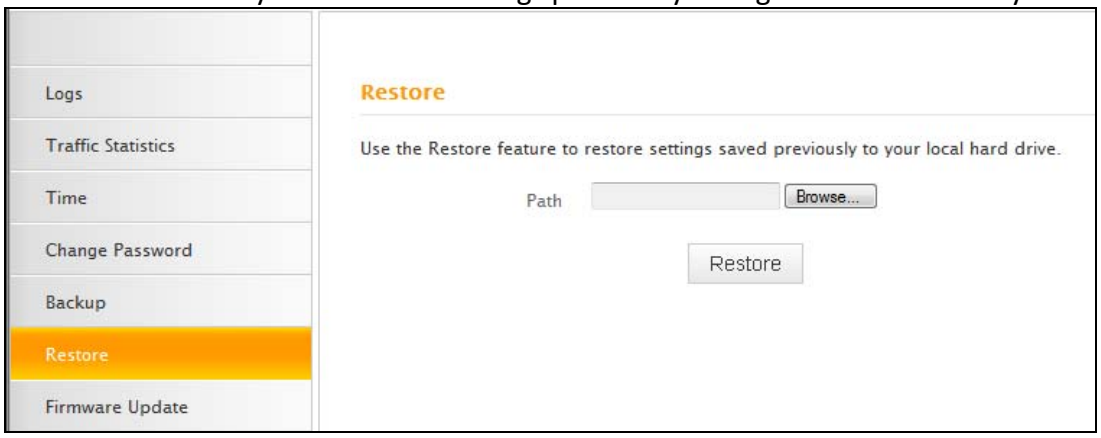
This feature allows you to backup current settings. Once you have configured the router, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to your router in case the router is reset to factory default settings.



- Backup: To backup settings, click the Backup button and specify a directory to save settings to your local hardware.

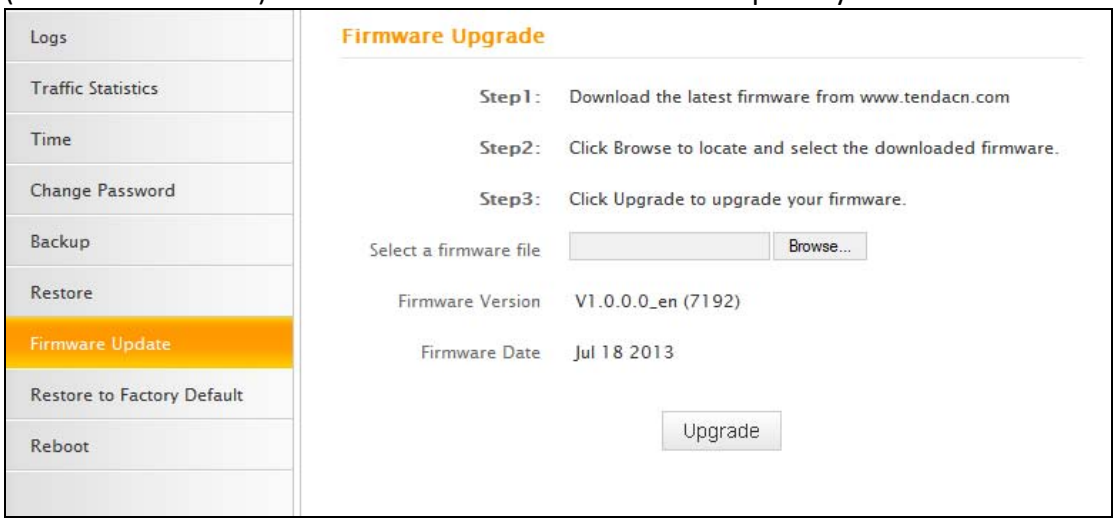
6.6 Restore

This section allows you to restore settings previously configured and saved to your local hard drive.



6.7 Firmware Update

Firmware upgrade is released periodically to improve the functionality of your router, and also to add any new features. If you run into a problem with a specific feature of the router you could log on to our website (www.tendacn.com) to download the latest firmware to update your device.



To update firmware, do the following:

1. Click **Browse** to locate and select the firmware file and **Upgrade** to update your router.
2. Device restarts automatically when the upgrade process is completed.

Note

DO NOT power off the router when the upgrade is in process otherwise the router may be permanently damaged. When the upgrade is completed, the router will automatically reboot. The firmware upgrade may take a few minutes to complete so please wait for the process to finish.

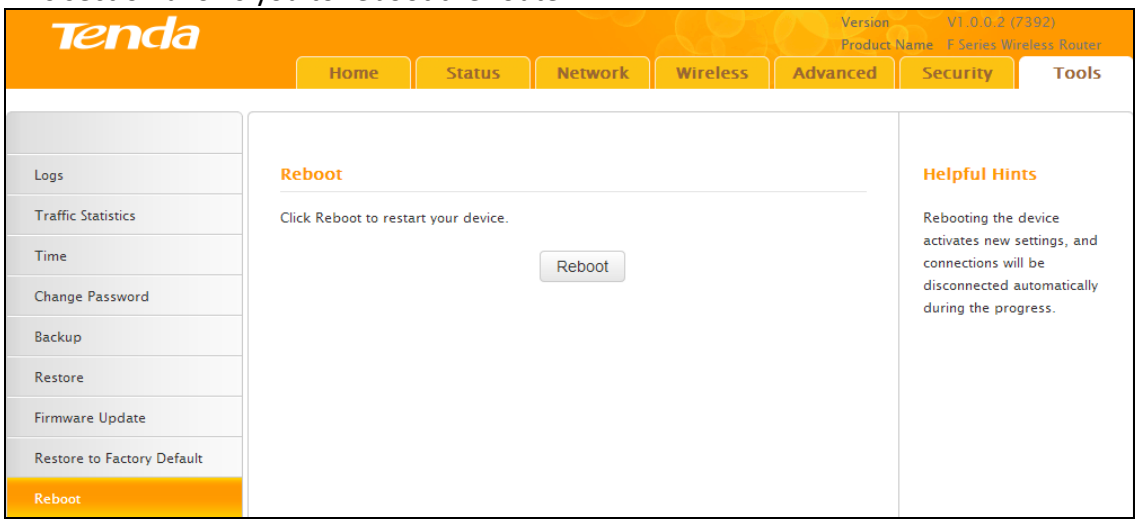
6.8 Restore to Factory Default

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

- Default IP Address: 192.168.0.1
- Default Subnet Mask: 255.255.255.0
- Default User Name: admin
- Default Password: admin

6.9 Reboot

This section allows you to reboot the router.

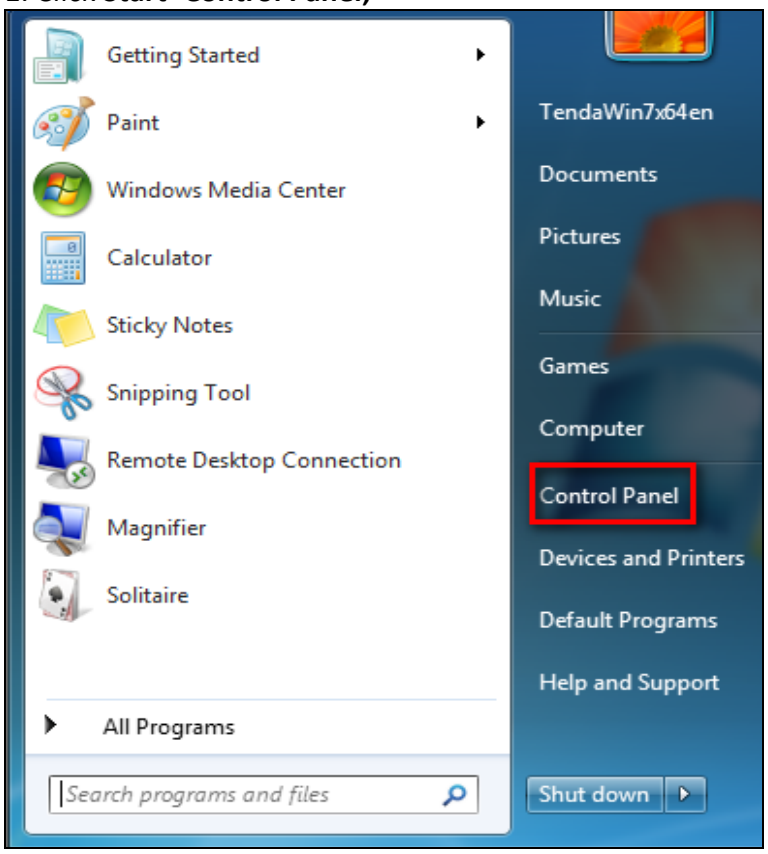


Appendix 1 Configure PC

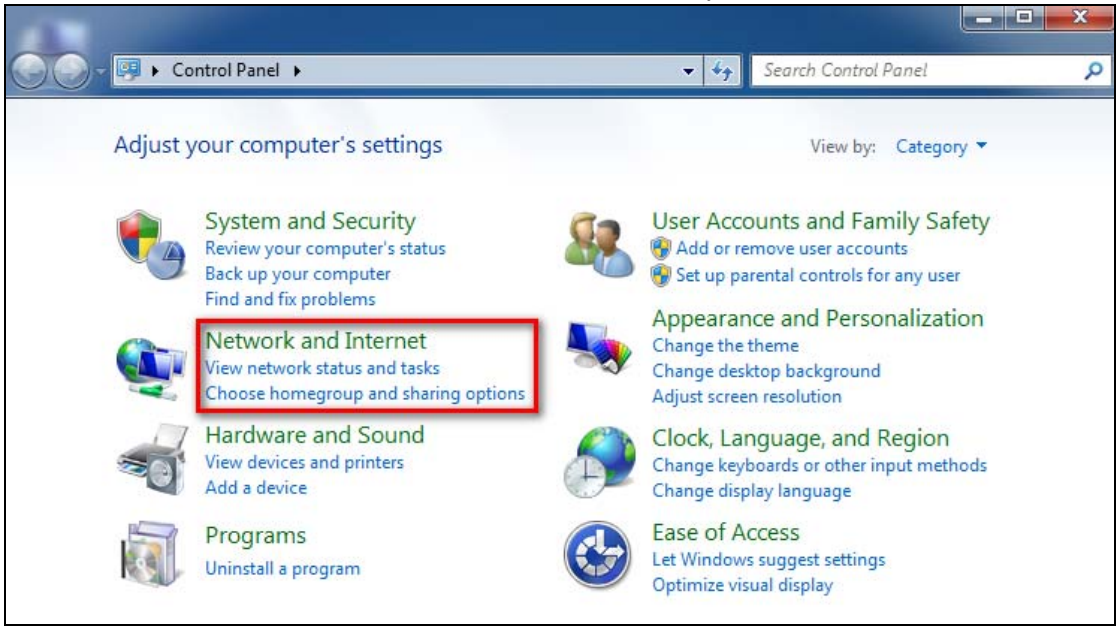
In this section we explain how to configure your PC's TCP/IP settings.

WIN7 OS

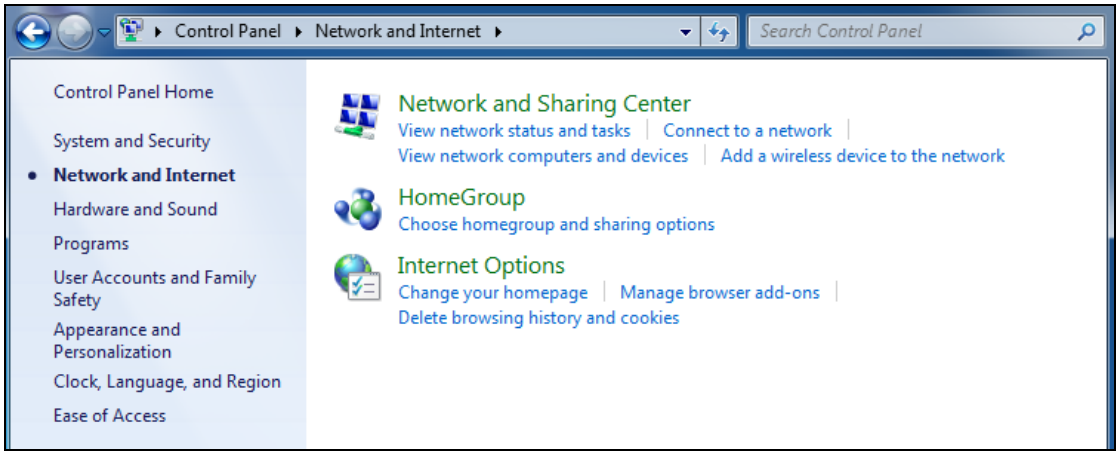
1. Click **Start>Control Panel;**



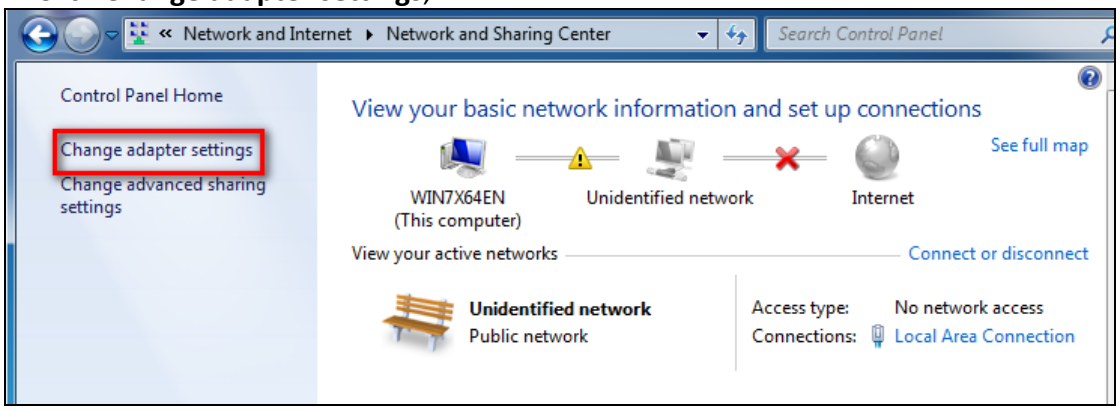
2. Enter **Control Panel** and click **Network and Internet;**



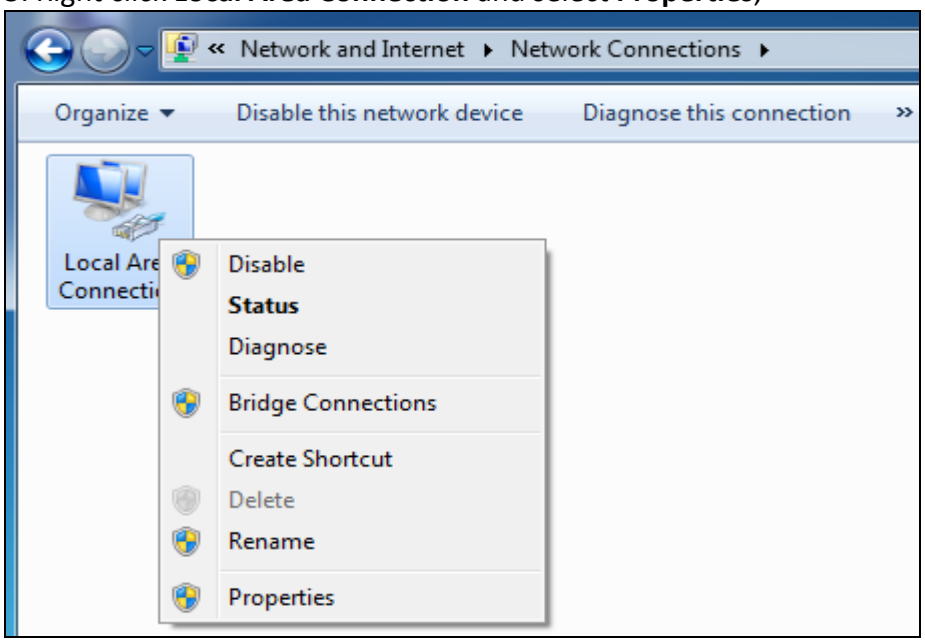
3. Click **Network and Sharing Center**;



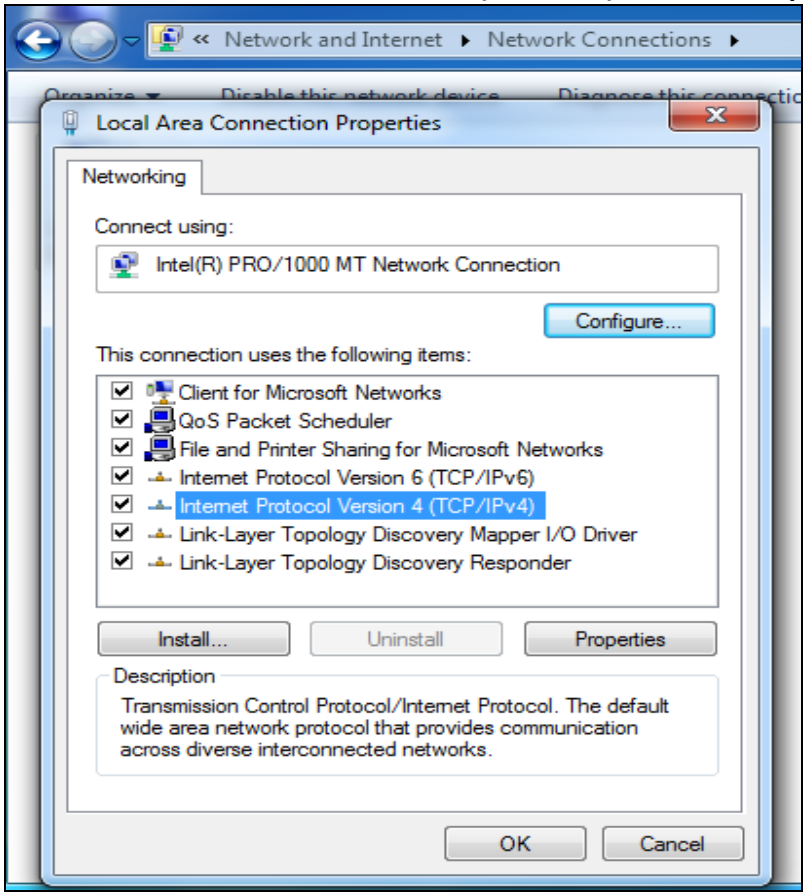
4. Click **Change adapter settings**;



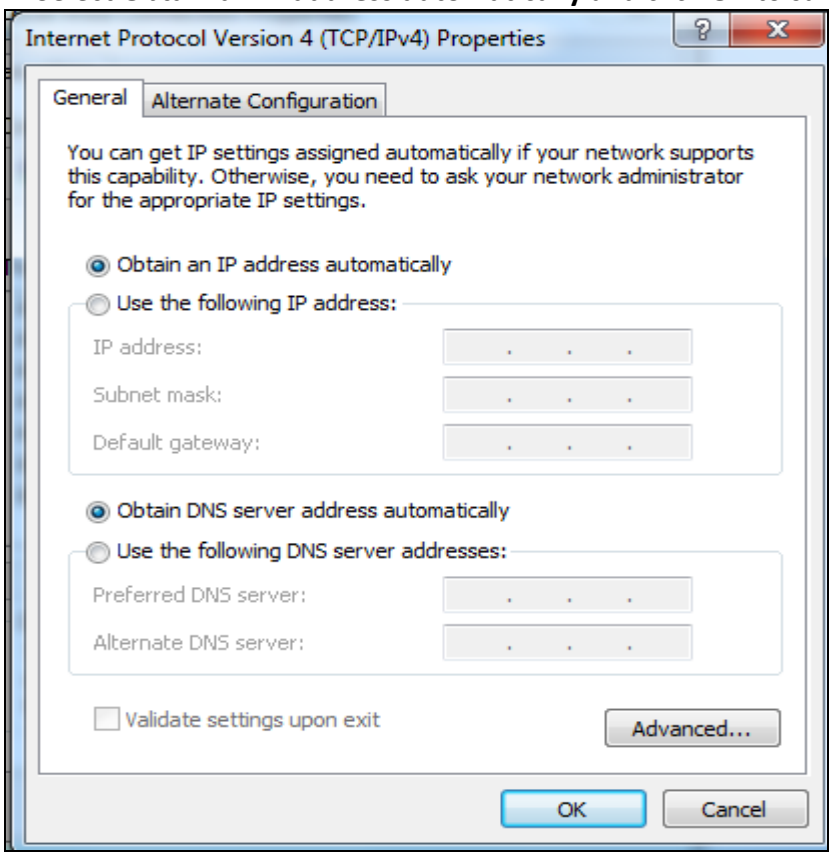
5. Right click **Local Area Connection** and select **Properties**;



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



7. Select **Obtain an IP address automatically** and click **OK** to save the configurations.

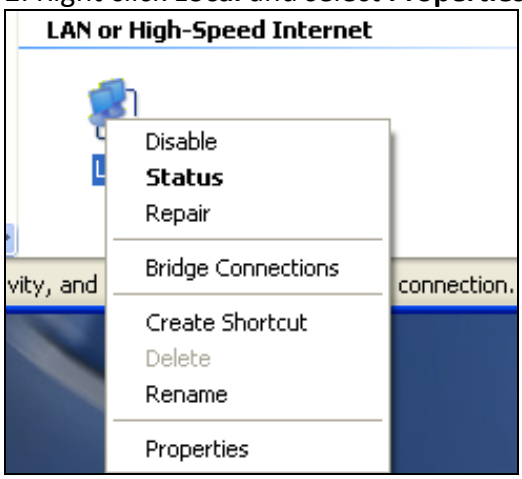


Back to Configure Router

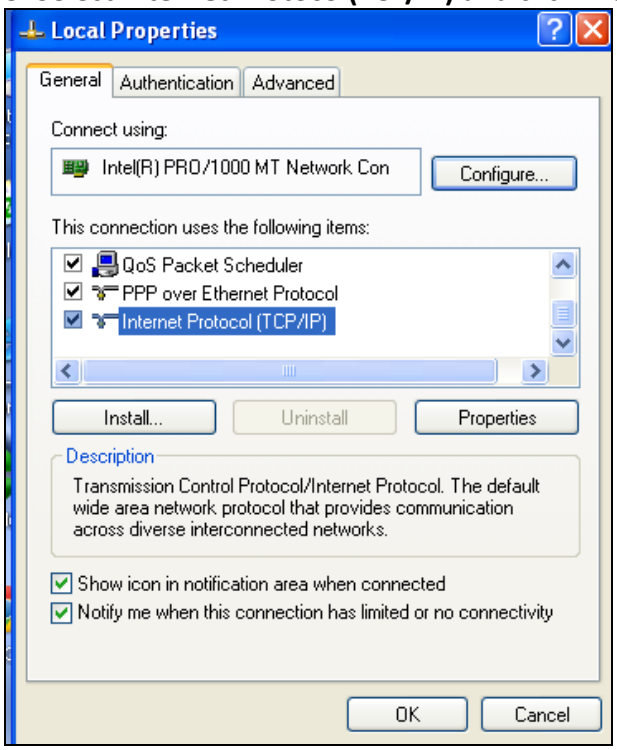
Windows XP OS

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

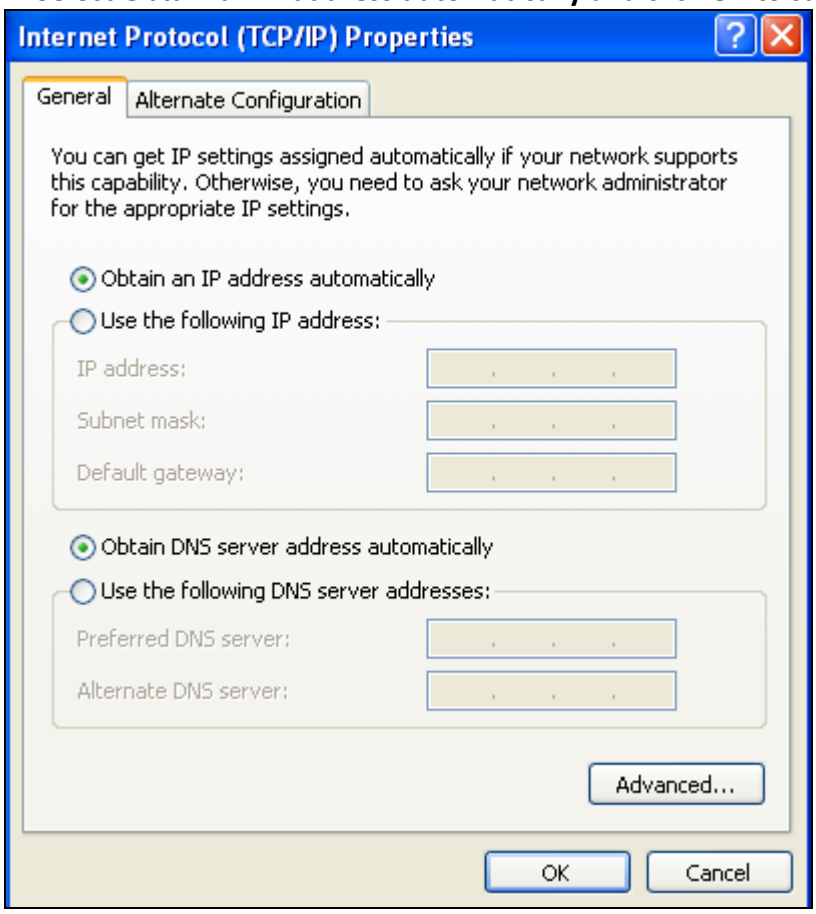
2. Right click **Local** and select **Properties**;



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



4. Select **Obtain an IP address automatically** and click **OK** to save the settings.



Back to Configure Router

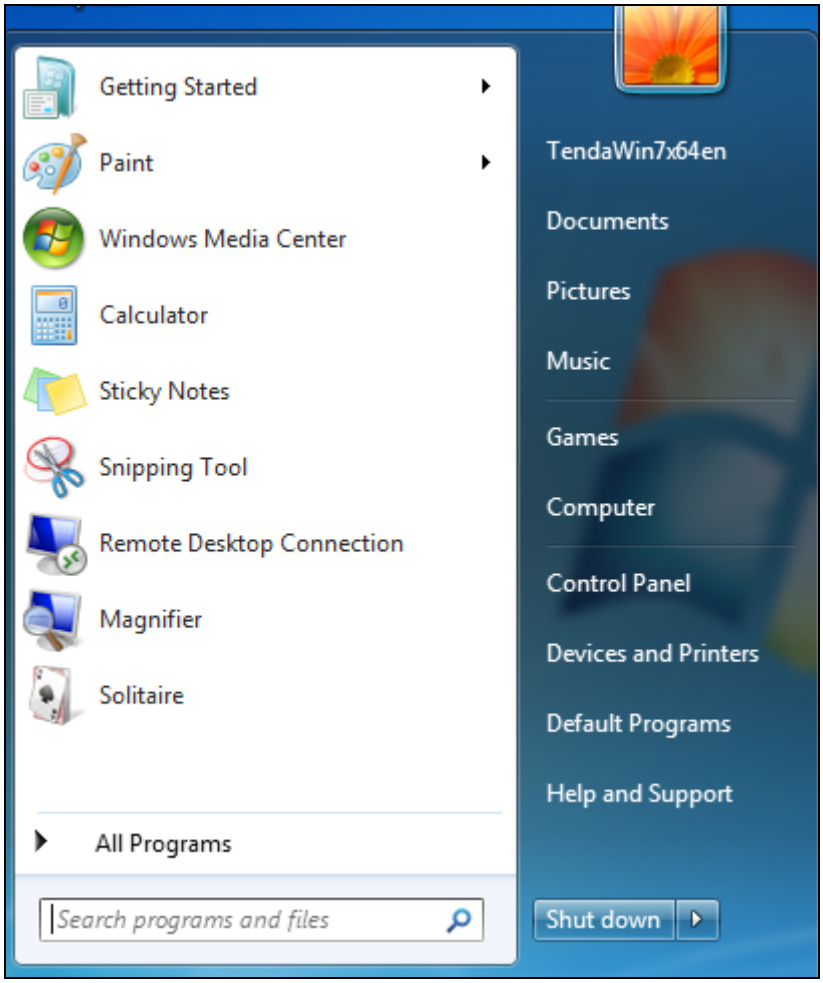
Appendix 2 Join a Wireless Connection

Note

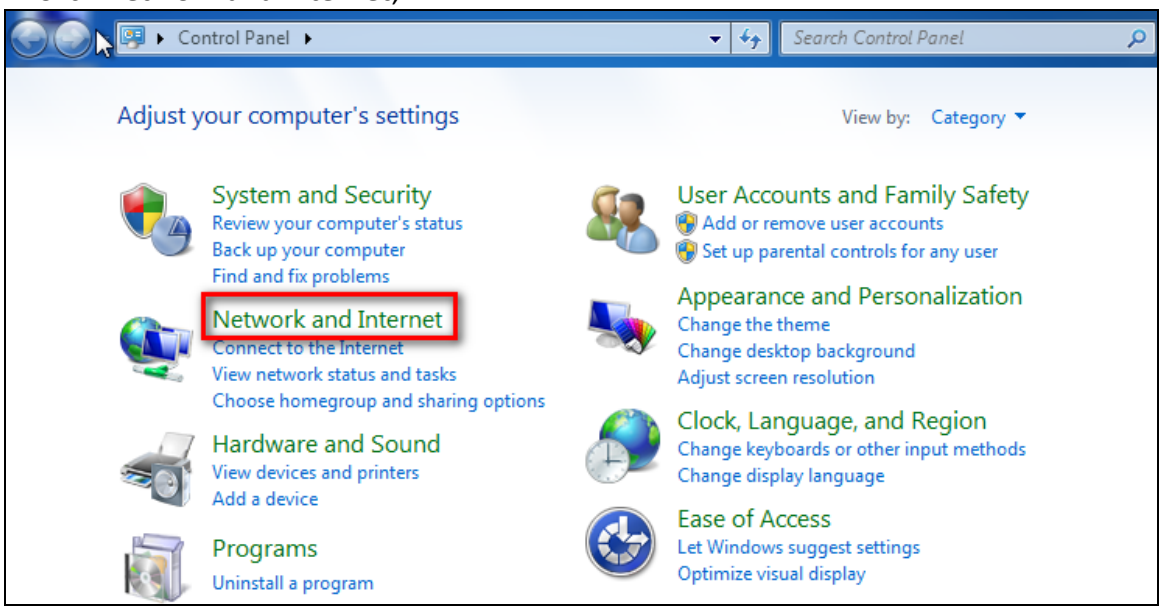
For wireless connection, desktop computers need to be equipped with wireless network cards first.

Win7 OS

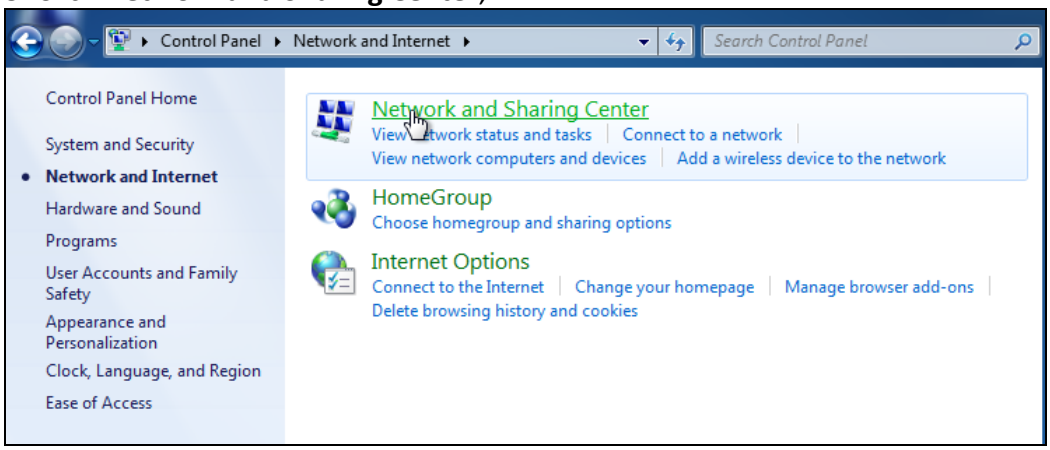
1. Click **Start>Control Panel**;



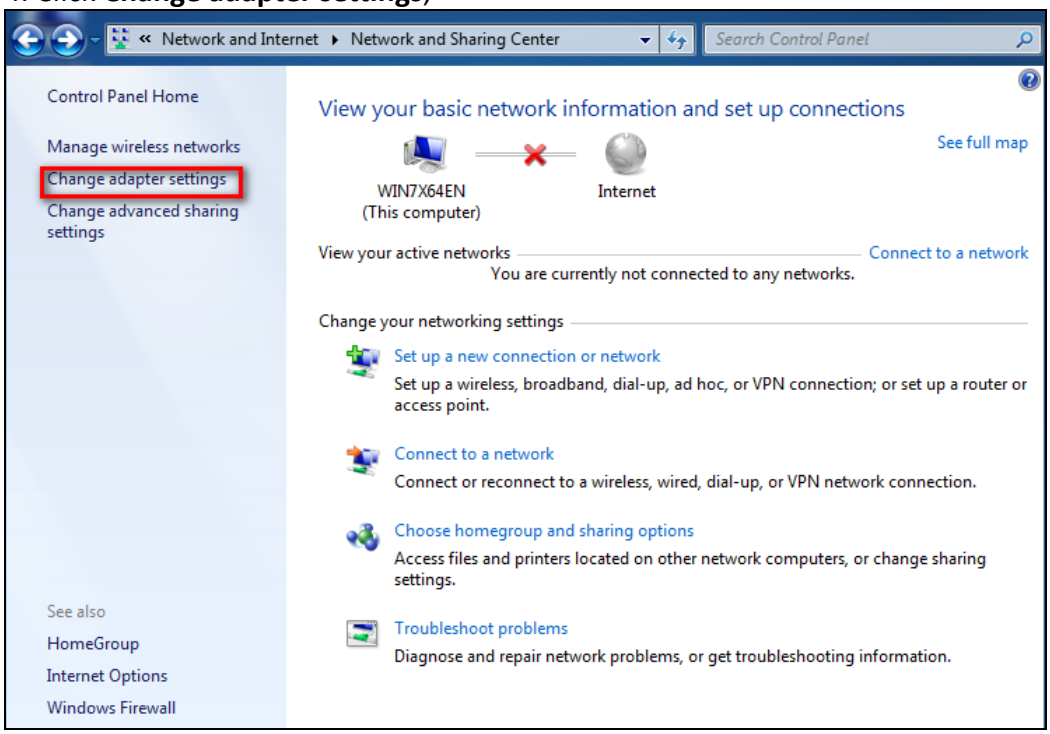
2. Click **Network and Internet**;



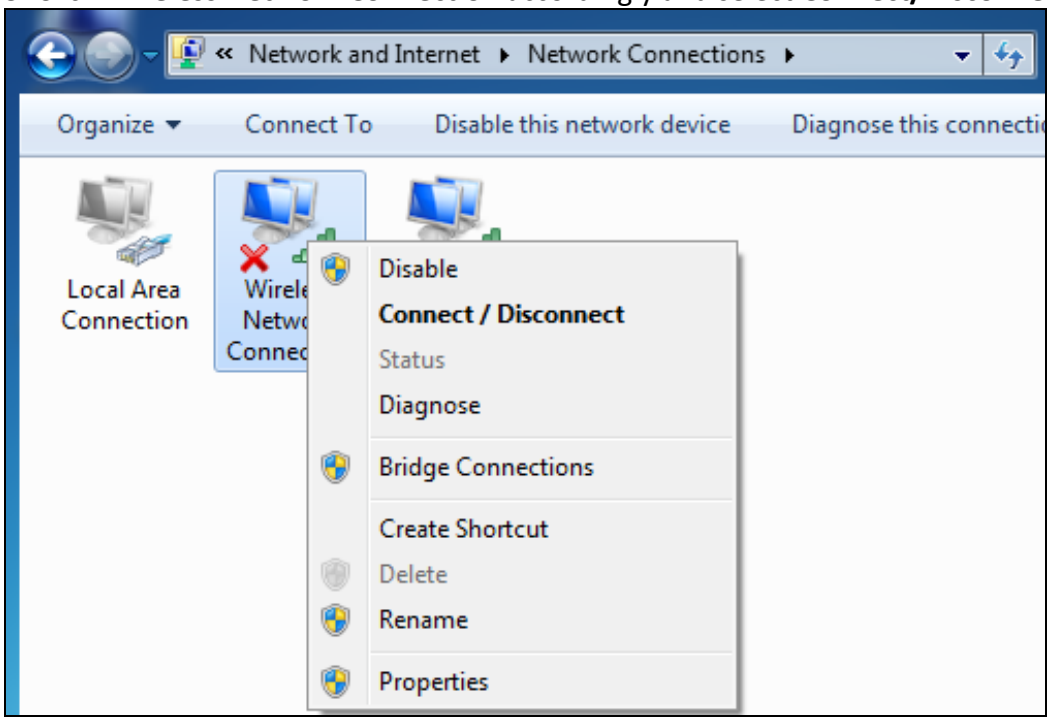
3. Click **Network and Sharing Center**;



4. Click **Change adapter settings**;

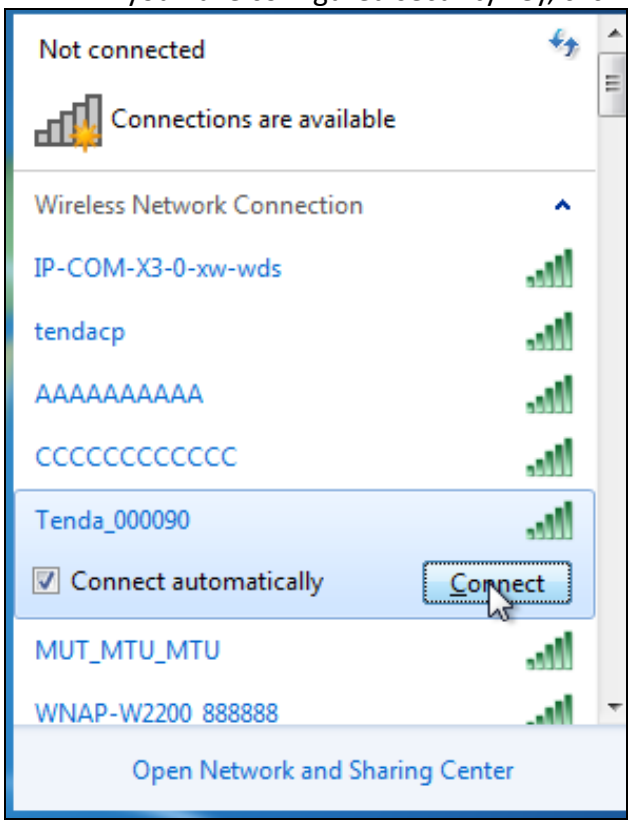


5. Click **Wireless Network Connection** accordingly and select **Connect/Disconnect**;

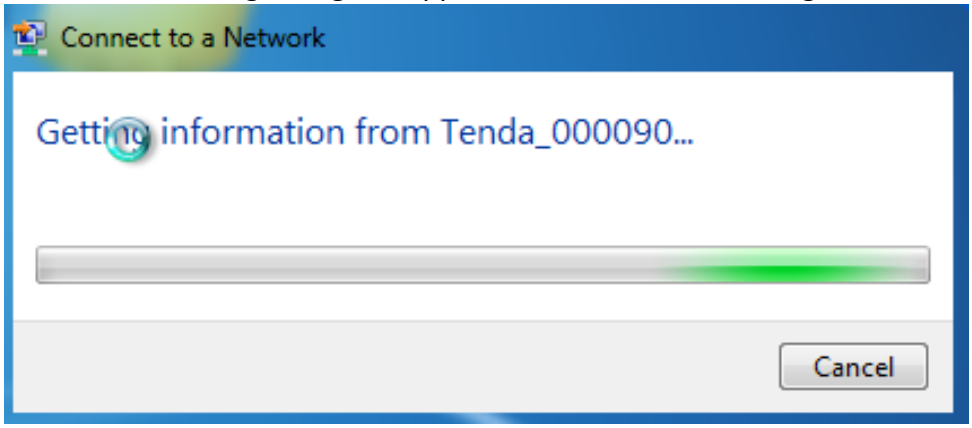


6. Select the network you wish to connect, such as Tenda-000090; According to different cipher types, here goes two situations:

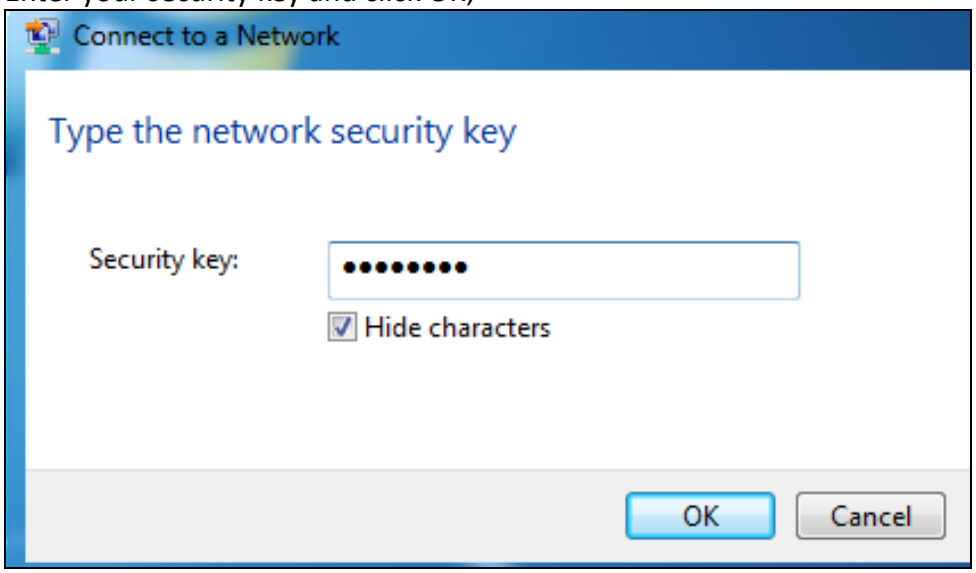
A. If you have configured security key, click **Connect**;



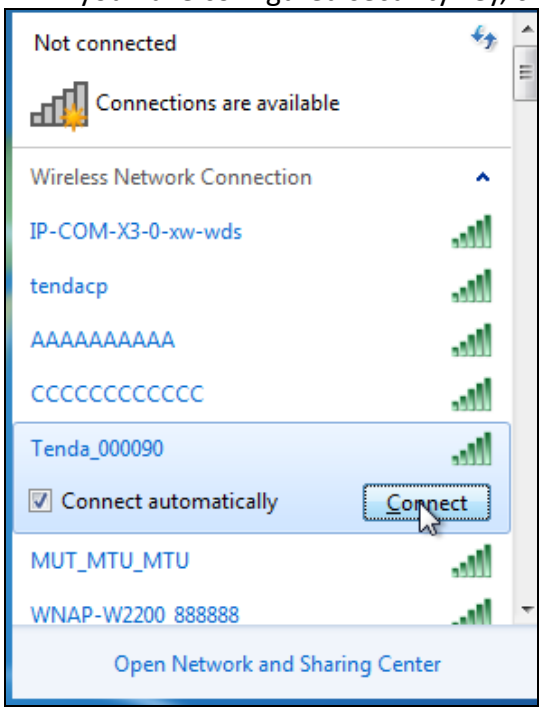
When the following dialog box appears, it indicates connecting to the network;



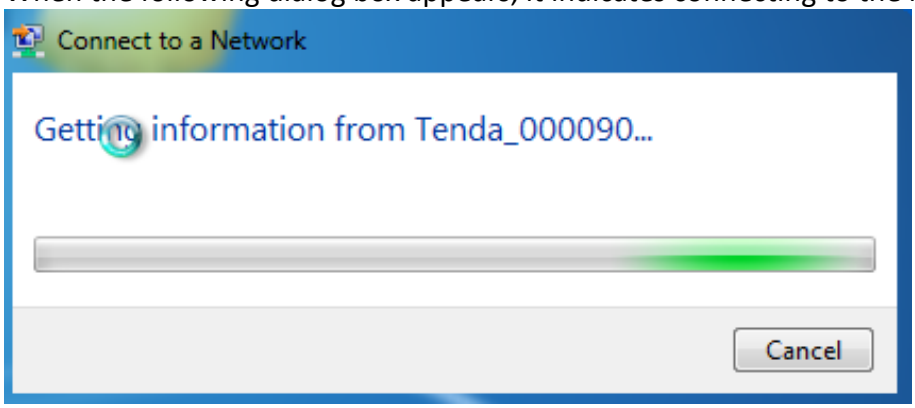
Enter your security key and click OK;



B. If you have configured security key, click **Connect**;



When the following dialog box appears, it indicates connecting to the network;



7. When displaying Connected, you have connected to network successfully.

Appendix 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 entered the device's LAN IP address in the web browser but cannot access the utility. What should I do?

a.Check whether device is functioning correctly. The SYS LED should blink a few seconds after device is powered up. If it does not light up, then some internal faults may have occurred.

b.Verify physical connectivity by checking whether a corresponding port's link LED lights up. If not, try a different cable. Note that an illuminated light does NOT ALWAYS indicate successful connectivity.

c. Run the "ping 192.168.0.1" command. If you get replies from 192.168.0.1, open your browser and verify that Proxy server is disabled. In case that ping fails, press and hold the "RESET" button on your device for 7 seconds to restore factory default settings, and then run "ping192.168.0.1" again.

d. Contact our technical support for help if the problem still exists after you tried all the above.

2. Q: What should I do if I forget the login password to my device?

A: Reset your device by pressing the Reset button for over 7 seconds.

Note

All settings will be deleted and restored to factory defaults once you pressed the Reset button.

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

a.Check if there are other DHCP servers present in your LAN. If there are other DHCP servers except your router, disable them immediately.

b.The default IP address of the device is 192.168.0.1; make sure this address is not used by another PC or device. In case that two computers or devices share the same IP addresses, change either to a different address.

4.Q: I cannot access Internet and send/receive emails; 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 (1492 by default). In this case, go to "WAN Settings" to change the MTU value from default 1480 to 1450 or 1400, etc.

5. Q: How do I share resources on my computer with users on Internet through the device?

To let Internet users access internal servers on your LAN such as e-mail server, Web, FTP, via the device, use the "Virtual Server" feature. To do so, follow steps below:

Step 1: Create your internal server, make sure the LAN users can access these servers and you need to know related service ports, for example, port number for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Enter Port Forwarding (also called Port Range Forwarding on some products) screen from device web UI.

Step 3: Complete the Start Port (also called External/Ext Port on some products) and End Port (also known as Internal Port on some products) fields, say, 80-80.

Step 4: Input the internal server's IP address. For example, assuming that your Web server's IP address is 192.168. 0.10, then simply input it.

Step 5: Select a proper protocol type: TCP, UDP, or Both depending on which protocol(s) your internal host is using.

Step 6: Click Enable and save your settings.

For your reference, we collected a list of some well-known service ports as follows:

Server	Protocol	Service Port
Web Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
Net Meeting	TCP	1503、1720
MSN Messenger	TCP/UDP	File Send:6891-6900(TCP) Voice:1863, 6901(TCP) Voice:1863, 5190(UDP)
PPTP VPN	TCP	1723
Iphone5.0	TCP	22555
SMTP	TCP	25
POP3	TCP	110

Appendix 4 Glossary

Channel

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

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

SSID

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

WPA/WPA2

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

IEEE 802.1X Authentication

IEEE 802.1X Authentication is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.IEEE 802.1X defines the encapsulation of EAP over LAN or EAPOL. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e. client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name / password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

PPPOE

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Integrated PPP protocol implements authentication, encryption, and compression functions that traditional Ethernet cannot provide and can also be used in the cable modem and digital subscriber line (DSL) and Ethernet that provide access service to the users. Essentially, it is a protocol that allows to establish a point-to-point tunnel between two Ethernet interfaces within an Ethernet broadcast domain.

DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.

WDS

A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. All base stations in a wireless distribution system must be configured to use the same radio channel, method of encryption (none, WEP, or WPA) and the same encryption keys. They may be configured to different service set identifiers. WDS also requires every base station to be configured to forward to others in the system. WDS may also be considered a repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).WDS may be incompatible between different products (even occasionally from the same vendor) since it is not certified by the Wi-Fi Alliance. WDS may provide two modes of wireless AP-to-AP connectivity:
Wireless bridging, in which WDS APs communicate only with each other and don't allow wireless clients or stations (STA) to access them.
Wireless repeating, in which APs communicate with each other and with wireless STAs.

DMZ

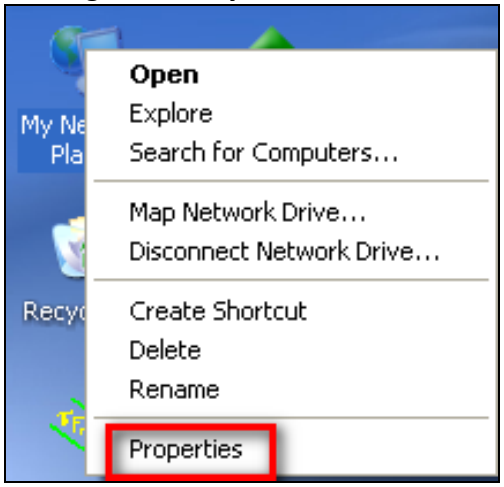
In computer security, a DMZ (sometimes referred to as a perimeter networking) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, although communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. Any services such as Web servers, Mail servers, FTP servers and VoIP servers, etc. that are being provided to users on the external network can be placed in the DMZ.

Appendix 5 Remove Wireless Network from Your PC

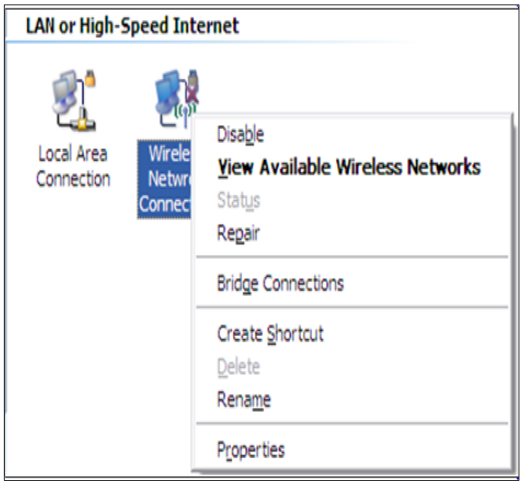
If you change wireless settings on your wireless device, you must remove them accordingly your PC; otherwise, you may not be able to wirelessly connect to the device. Below describes how to do remove a wireless network from your PC.

Windows XP OS

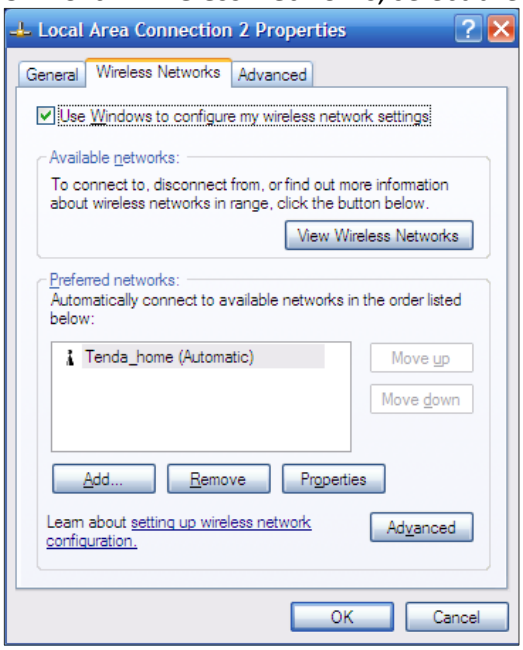
1. Right click **My Network Places** and select **Properties**.



2. Click **Wireless Network Connection** and then select **Properties**.

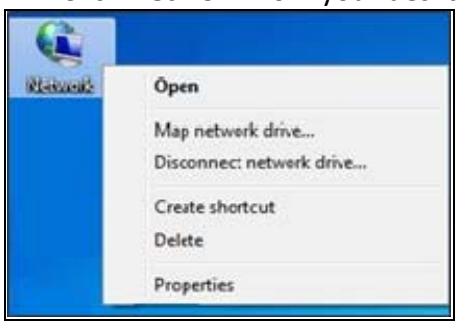


3. Click **Wireless Networks**, select the item under **Preferred networks** and then click the **Remove** button.

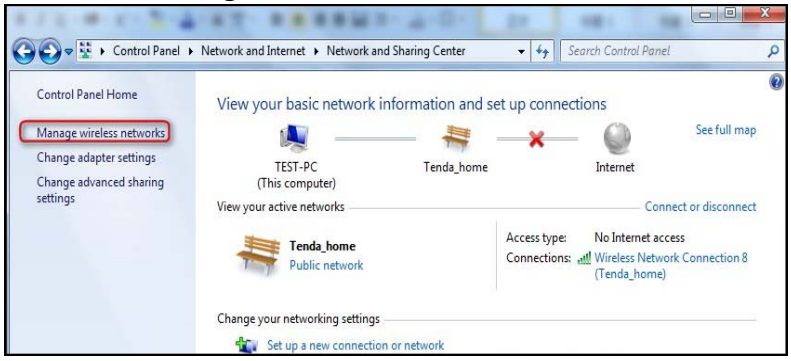


Windows 7 OS

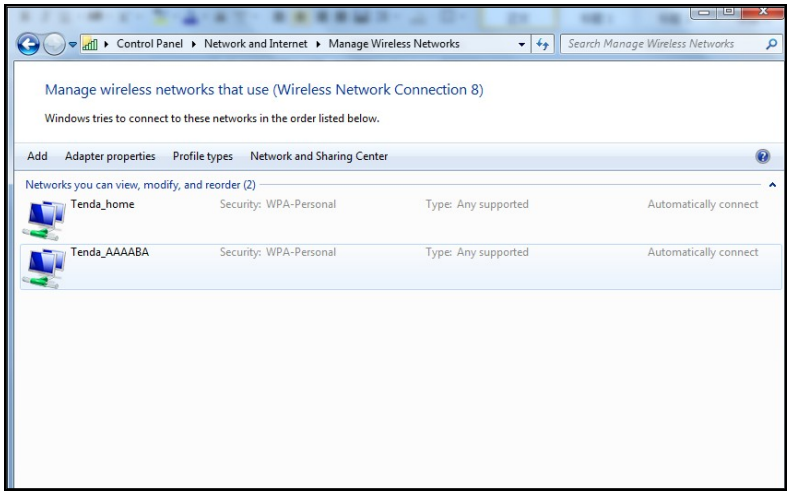
1. Click **Network** from your desktop and select **Properties**.



2. Select **Manage Wireless Networks**.



3. Click the wireless connection and select **Remove network**.



Appendix 6 Safety

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