

## A5s User Guide

### Copyright Statement

**Tenda**<sup>®</sup> is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without prior expressed written permission from Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, reproduce, or translate it into other languages.

All photos and product specifications mentioned in this manual are for references only. Upgrades of software and hardware may occur; Tenda reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes. If you would like to know more about our product information, please visit our website at [www.tendacn.com](http://www.tendacn.com).

---

**Table of Contents**

Copyright Statement .....	1
Table of Contents.....	2
<b>Chapter 1 Product Overview .....</b>	<b>1</b>
1.1 Features .....	1
1.2 Package Content .....	2
1.3 Panel Overview .....	2
<b>Chapter 2 Hardware Install.....</b>	<b>5</b>
2.1 Hardware Install.....	5
2.1.1 Connect device to a power source.....	6
2.1.2 Network Connection .....	6
<b>Chapter 3 Mode Overview.....</b>	<b>9</b>
3.1 Hotel Mode (Dynamic IP).....	9
3.2 Residence Mode (PPPoE) .....	10
3.3 WISP Mode .....	10

---

Chapter 4 Web Utility Login.....	12
4.1 Connect to Device Wirelessly.....	12
4.2 Login to Web Utility .....	15
 Chapter 5 Mode Toggle & Popup Windows .....	16
5.1 Mode Auto-switch .....	16
5.2 Smart Popup Windows .....	17
 Chapter 6 Mode Setup.....	19
6.1 Hotel Mode (Dynamic IP) Setup.....	19
6.2 Residence Mode (PPPoE) Setup .....	20
6.3 WISP Mode Setup .....	24
 Chapter 7 Network Setup .....	30
7.1 LAN Setup.....	30
7.2 WAN Settings .....	30
7.3 WAN Speed .....	32
7.4 WAN MAC Clone .....	33
7.5 DNS Server .....	34

---

Chapter 8 Wireless Settings.....	35
8.1 Wireless-Basic .....	35
8.2 Wireless-Security .....	37
8.3 Wireless Access Control .....	40
8.4 Connection Status .....	41
Chapter9 DHCP .....	43
9.1 DHCP Settings .....	43
9.2 DHCP Client List &Reservation .....	44
Chapter 10 Virtual Server .....	46
10.1 Port Forwarding .....	46
10.2 DMZ Host .....	47
10.3 UPNP .....	48
Chapter 11 Security .....	49
11.1 Client Filter .....	50
11.2 MAC Filter .....	52
11.3 URL Filter.....	55

---

11.4 Remote Web-based Management .....	58
Chapter 12 Routing Settings .....	60
12.1 Routing Table .....	60
Chapter 13 Bandwidth Control .....	61
13.1 Bandwidth Control .....	61
Chapter 14 Tools .....	62
14.1 Time & Date .....	62
14.2 DDNS .....	64
14.3 Back/Restore .....	65
14.4. Restore to Factory Default Settings .....	67
14.5 Firmware Update .....	68
14.6 Reboot .....	69
14.7 Change Password .....	69
14.8.1 Logs .....	70
Appendix 1 Set PC to“Obtain an IP address automatically” .....	70

---

Appendix 2. How to connect to an encrypted wireless network .....	74
Appendix 3: Glossary .....	77
Appendix 4 FAQs.....	79
Appendix 5 EMC Statement.....	84

## Chapter 1 Product Overview

Thanks for purchasing this Tenda A5s Designed for those who travel, the Tenda A5s is not only a fashionable and ultra-compact router, it is also a smart router that can auto-detect your Internet connection type and intelligently switch between Hotel Mode (Dynamic IP) and Residence Mode (PPPoE).

### 1.1 Features

- Compliant with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3 and IEEE 802.3u standards
- Based on 802.11n technology, equipped with a high-performance antenna, the device delivers wireless speed of up to 150Mbps
- Triple modes: Hotel Mode, Residence Mode and WISP Mode to provide you with flexibility and freedom to connect to Internet
- Provides encryption methods of 64-/128-bit WEP, WPA and WPA2, etc to secure your wireless network

- 1\* 10/100M LAN/WAN interchangeable port
- Provides Internet connection types: Dynamic/ static IP; can be connected to an xDSL/Cable MODEM
- Local/remote web based management
- Wireless Roaming technology to ensure high-efficiency wireless connectivity
- Hidden/invisible SSID;  
MAC-based wireless access control;
- Logs to record device's usage status;
- Supports UPnP and DDNS features;
- Allow/disallow specified PCs on LAN to access Internet
- Provides virtual server and DMZ features;
- Internal firewall to block potential attacks from hackers.

## **1.2 Package Content**

Unpack the box and check the following items:

- A5s
  - Quick Install Guide
- If any of the above items are incorrect, missing, or damaged, please contact your Tenda reseller for immediate replacement.

## **1.3 Panel Overview**

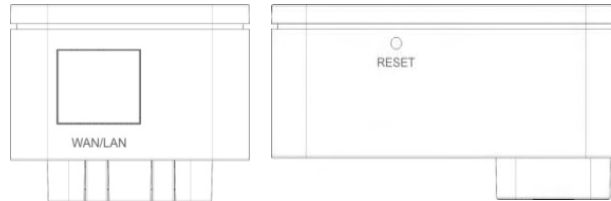




LED Overview:

LED	Status	Description	
Power LED	A green and solid light	Device has electrical power	
Status LED	Hotel Mode	A green and blinking light	Device is currently operating in hotel mode and WAN port is NOT properly connected
		A green and solid light	Device is currently operating in hotel mode and WAN port is connected
	Residence Mode	A dark blue and blinking light	Device is currently operating in Residence Mode and WAN port is NOT properly connected

		A dark blue and solid light	Device is currently operating in Residence Mode and WAN port is connected
	WISP Mode	A light blue and blinking light	Device is currently operating in WISP Mode and is not connected to a wireless hotspot
		A light blue and solid light	Device is currently operating in WISP Mode and is connected to a wireless hotspot



- Reset: Pressing it for about 7 seconds restores the Device to factory defaults.
- LAN/WAN Interface: The device provides 1\* 10/100M LAN/WAN interchangeable interface, which functions as a) a WAN interface for connection to an Internet-enabled DSL

modem or other uplink network device when operating in Residence Mode or Hotel Mode; and b) a LAN interface for connection with a PC or an Ethernet switch when operating in WISP Mode.

## **Chapter 2 Hardware Install**

### **2.1 Hardware Install**

Before you start configuring the device, follow below steps to install device. For optimum wireless performance, it is advisable to

place the device in the center of the coverage.

**2.1.1 Connect device to a power source**

Simply plug the device into a electrical outlet nearby.



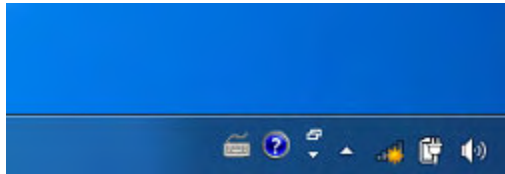
**2.1.2 Network Connection**

A. For first time use, you must connect to the device wirelessly (Find device's default SSID from the label on the back of the device; by default, device's wireless is unencrypted.). For network topology, see below:



To configure wireless network adapter, do as follows:

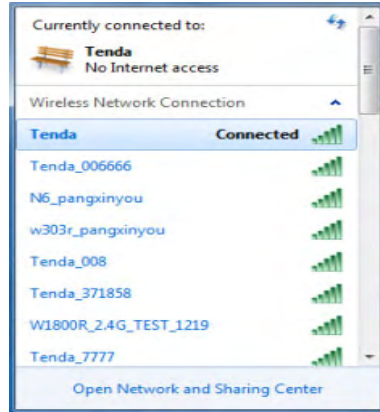
- a. Right-click the "📶" icon from the bottom right corner of your desktop.



- b. Select the desired wireless network and click "Connect".
  - c. Enter the customized security key (if any) or simply click "Connect" as there is no preset security key by default.
- Note: Select "Connect to the network without settings it up" if you are asked to provide a PIN code during connection.



d. When you see “Connected” displayed next to the wireless network you selected, it means you have connected to the wireless network successfully. (Note: To access Internet, below settings must be configured)



## Chapter 3 Mode Overview

The device provides modes of Hotel, Residence and WISP to meet different network environments. By default, the device can automatically detect your Internet connection type and switch between Hotel mode and Residence mode. You can also disable it if you don't want the device to auto-switch between the two modes. However you must select and setup the WISP mode manually if you want to use it.

### **3.1 Hotel Mode (Dynamic IP)**

The device operates in Hotel Mode (also known as Dynamic IP or DHCP) by default. In this mode, the device functions as a wireless router to obtain an IP address and DNS server automatically from your ISP. Simply connect to it wirelessly and multiple users can share the Internet connection concurrently. No configuration needed! Simply connect the device to the broadband Interface in a hotel room with an Ethernet cable and your PC to the device wirelessly. That is all it! In case you have encrypted the wireless with a customized security key, you will be asked to provide it when attempting to connect to device wirelessly. Simply enter it there. See below for typical network topology:



### 3.2 Residence Mode (PPPoE)

In this mode, the device functions as a wireless broadband router, dialing up for Internet connection and delivering Internet access sharing to multiple wireless clients. For typical network topology, see below:

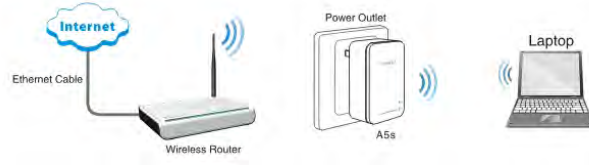


### 3.3 WISP Mode

In this mode, the device functions as a Wireless range extender to relay an existing wifi hotspot and its RJ45 port functions as a LAN port. Simply uplink the device wirelessly to an existing Internet-enabled hotspot/AP, and clients can share Internet access by connecting to the device wirelessly or using an Ethernet cable.

For typical network topology, see below:





## Chapter 4 Web Utility Login

This chapter mainly presents how to log in to device's web utility.

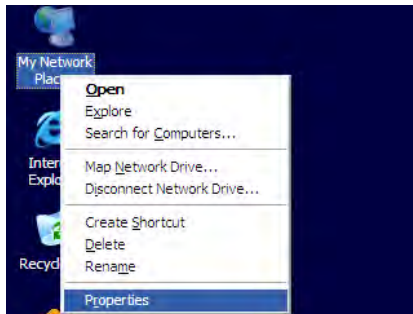
### 4.1 Connect to Device Wirelessly

**IMPORTANT:** For first-time use, you must use the wireless network adapter on your PC to connect to the device wirelessly instead of using an Ethernet cable as the device is preset to Hotel Mode (which means the Ethernet port on the device functions as a WAN port) by default.

4.1.1 Setup Wireless Connection (Windows XP is used in below illustration. For setup methods in Windows 7, see sections hereunder)

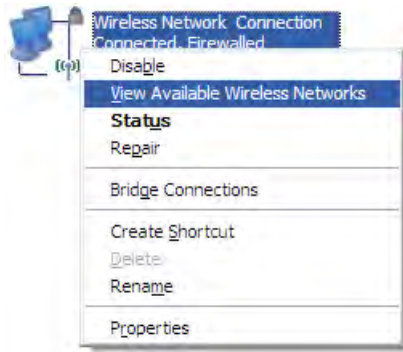
If you are using Windows XP, do as follows:

- a、 Right click My Network Places and select Properties.

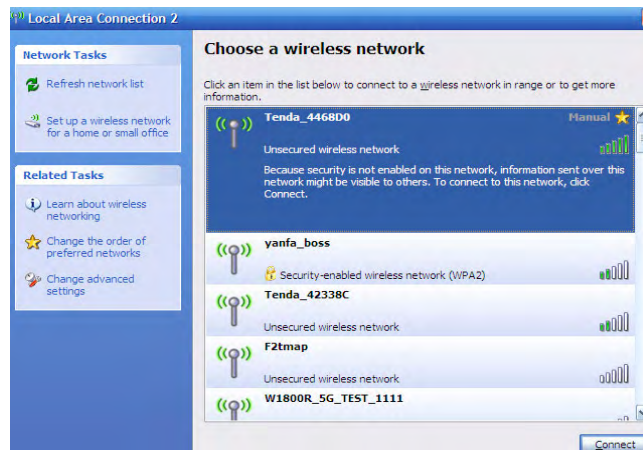


- b、 Click "Wireless Network Connection" and select "View

Available Wireless Networks".

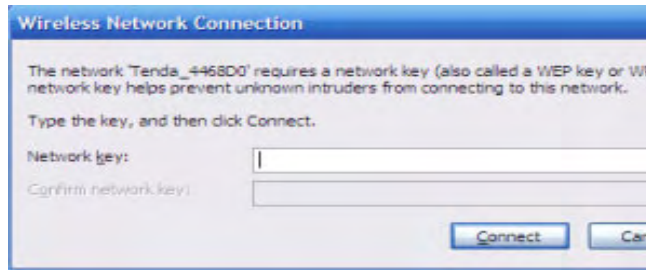


c. Select the desired wireless network and click "Connect".



d. Enter the customized security key twice (If any) or simply click


"Connect" as there is no preset security key by default.



e. When you see "Connected" displayed next to the wireless network you selected, it means you have connected to the wireless network successfully. (Note: To access Internet, below settings must be configured)

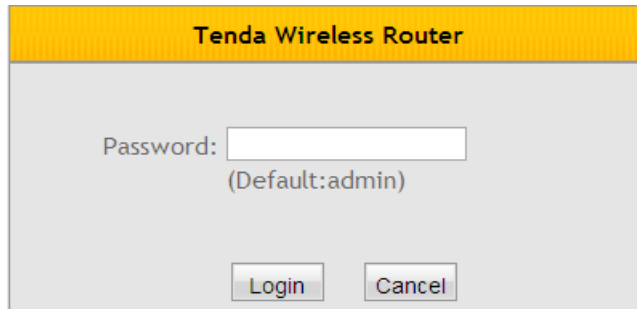


## 4.2 Login to Web Utility

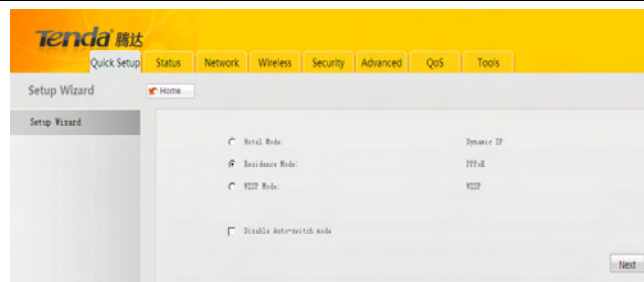
4.2.1 Launch a web browser, (say, IE ), input "http : //192.168.2.1" and press Enter. (In case of Internet connection failure, this screen will open automatically, whatever is entered in the web browser)



4.2.2 Enter "admin" in Password field and then click Login. (Note: Password is case-sensitive.)

A screenshot of the Tenda Wireless Router login page. The page has a yellow header with the text "Tenda Wireless Router". Below the header is a grey background with a "Password:" label followed by a text input field. Below the input field, the text "(Default:admin)" is displayed. At the bottom of the page, there are two buttons: "Login" and "Cancel".

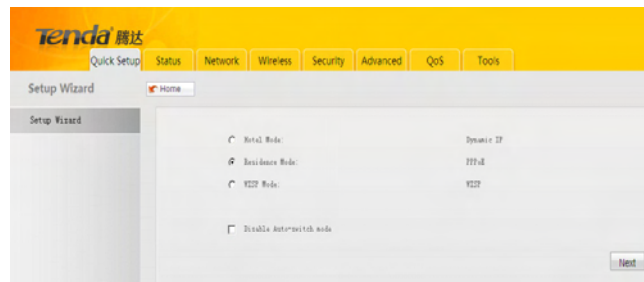
4.2.3 You will see below screen if you entered a correct password.



## Chapter 5 Mode Toggle & Popup Windows

### 5.1 Mode Auto-switch

By default, the device can automatically detect your Internet connection type and switch between Hotel Mode (Dynamic IP) and Residence Mode (PPPoE). You can also disable this feature manually if you don't need it. However if you want to use WISP mode you need to select and setup it manually



When in hotel, simply connect the device to the broadband interface there and then to an electrical outlet nearby. The device will detect and switch to Hotel Mode automatically. No need for extra operation! When back at home, simply connect the device to an Internet-enabled DSL modem or Ethernet network and then to an electrical outlet nearby. The device will detect and switch to Residence Mode automatically. If operating in Residence Mode for the first time, it will prompt you to finish the settings required for your Internet connection. Simply follow the onscreen instructions. After you set up the device the way just mentioned, it will auto-switch between the Hotel Mode and Residence Mode depending on the detected network environment. No need to repeat operations.

## 5.2 Smart Popup Windows

In event of an unencrypted wireless network, a dialog window will pop up, prompting you to secure your wireless network with a custom security key. Select "Unencrypted" and "Never ask me

again" if you don't want to encrypt it, otherwise you will see this window every time you start the device. (Tips: For security purpose, it is highly advisable that you encrypt your wireless network.)



When operating in Residence Mode for the first time, system will pop up a dialog window, prompting you to enter a user name and a password required for PPPoE Internet connection. The pop up window is as below:



**Current Internet Connection Type: Residence Mode**  
**(PPPoE)**

*Please provide the user name and password info:*

PPPOE User Name

PPPOE Password

## Chapter 6 Mode Setup

### 6.1 Hotel Mode (Dynamic IP) Setup

No need for configurations in this mode! The device is wirelessly accessible to all wireless clients within coverage. (For connection diagram, see section 2.1.1)

Connect device as below:



Normally, Internet access in hotels is DHCP/dynamic IP, which means devices connecting to hotel network can obtain IP address automatically. So, simply connect the device to the broadband interface in hotel, and Internet access shall be shared by multiple wireless clients. Note that you must set these PCs to "Obtain an IP address automatically" and "Obtain DNS server address automatically" (For details, see appendix 1).

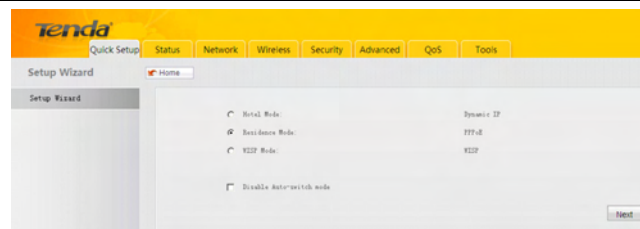
Note: In this mode, the device's RJ45 port functions as a WAN port for Internet connection. When activated, clients can only connect to the device wirelessly.

## 6.2 Residence Mode (PPPoE) Setup

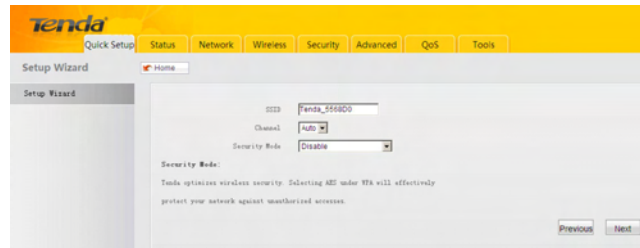
Residence Mode: Also known as ADSL dial-up or PPPoE connection type. Upon detecting this connection type, device switches to the Residence Mode automatically.

To set up it manually, do as follows:

1. Simply select "Residence Mode" and click "Next".



2. And you will enter the interface for configuring basic wireless settings.



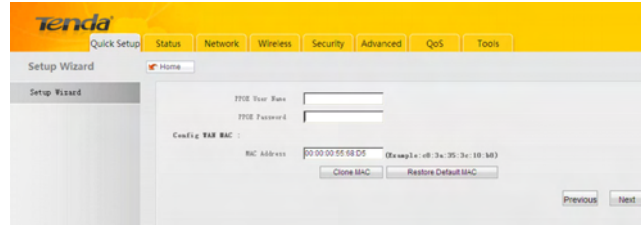
- SSID: A SSID (Service Set Identifier) is the unique name of a wireless network. To connect to the device wirelessly, you must know its SSID.
- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or “Auto” to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.

You can select WEP, WPA-PSK or WPA2-PSK encryption

method to secure your wireless network. Note down the self-defined security key for future use. You must provide it for wireless connections later.

It is advisable that you select the WPA-PSK>AES encryption method for better security. Simply enter 8-63 alphanumeric characters or other symbols in the Security Key field. For detailed configurations, see sections hereunder. Click "Next" to continue when finishing above settings.

3. You shall come to the Internet connection setup interface.



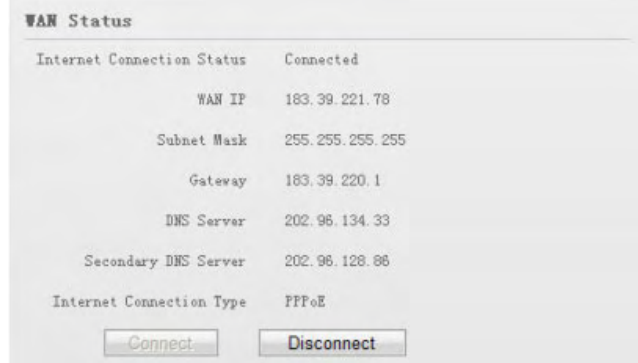
Enter the user name and password provided by your ISP in corresponding fields. Contact your ISP if you forget or are not clear. Click "Next" to continue when finishing above settings.

For example: Assuming that your ISP provides you with a user name: pppoe\_user and a password: pppoe\_passwd, then simply enter them in corresponding fields as seen on the screenshot.

The screenshot shows a configuration page for WAN MAC address. It includes fields for 'PPPOE User Name' (pppoe\_user), 'PPPOE Password' (pppoe\_passwd), and 'WAN MAC Address' (00:00:00:00:00:00). Below the MAC address field are buttons for 'Clone MAC' and 'Restore Default MAC'. At the bottom right are 'Previous' and 'Next' navigation buttons.

- Configure device's WAN MAC address (Optional).  
Normally you don't need to change device's default WAN MAC address. However, some ISPs may bind client PC's MAC address for Internet connection authentication. In this case, simply enter the bound MAC in the WAN MAC Address field or click "Copy My PC's MAC" to populate the field automatically. (Config above settings using the PC whose MAC address is bound with your ISP.)
- WAN MAC Address: Config Device's WAN MAC address.
- Copy My PC's MAC: Click to copy your PC's MAC address to device's WAN MAC address field.
- Restore to Factory Default MAC: Reset Device's WAN MAC to factory default.

After device reboot, go to Status to check the WAN (Internet) connection status. If you see below info there, congratulations, you can enjoy surfing now.



The screenshot shows the WAN Status page with the following configuration details:

WAN Status	
Internet Connection Status	Connected
WAN IP	183.39.221.78
Subnet Mask	255.255.255.255
Gateway	183.39.220.1
DNS Server	202.96.134.33
Secondary DNS Server	202.96.128.86
Internet Connection Type	PPPoE

At the bottom of the table are two buttons: **Connect** and **Disconnect**.

For methods of configuring more and featured functionalities, read sections hereunder.

4. Click Finish and reboot device to activate new settings.

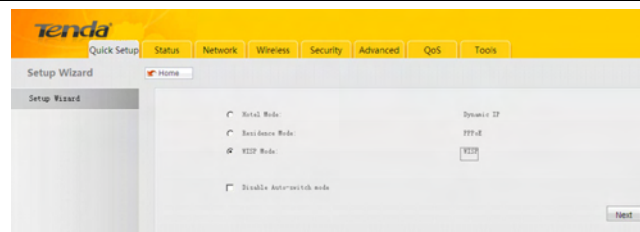


Note: In this mode, the device's RJ45 port functions as a WAN port for Internet connection. When activated, clients can only connect to the device wirelessly.

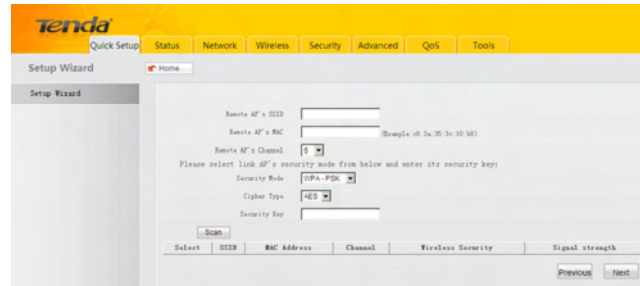
### 6.3 WISP Mode Setup

To amplify uplink device's wireless signal (extend wireless coverage), select this mode manually.

1. Select "WISP Mode" and then click "Next".



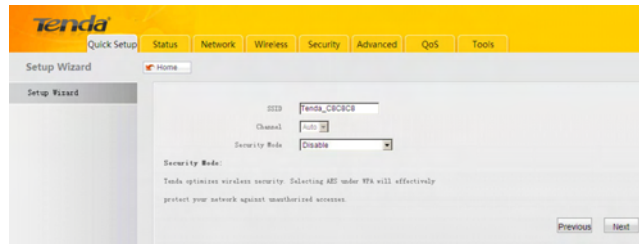
2. You shall now come to the WISP mode setup screen.



- **SSID:** A SSID (Service Set Identifier) is the unique name of a wireless network. Enter the SSID of your WISP's AP that you are going to connect to.
- **MAC Address:** Enter the WISP's MAC address that you are going to connect to. Wireless MAC address is also known as BSSID.
- **Channel:** Select the channel which your WISP's AP (to which the device is going to connect) is currently operating on.
- **Security Mode:** Config the same security settings (including security key) as set on your WISP's AP on your device. For details, see Wireless > Security section.

For convenience purpose, it is advisable to use the “Open Scan” option to search and select the link partner to add certain settings to the device automatically. Click "Next" to continue when finishing above settings.

3. And you will enter the interface for configuring basic wireless settings.



- SSID: A SSID (Service Set Identifier) is the unique name of a wireless network. To connect to the device wirelessly, you must know its SSID.
- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or “Auto” to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list. (Channel change unsupported here)

You can select WEP, WPA-PSK or WPA2-PSK encryption method to secure your wireless network. Note down the self-defined security key for future use. You must provide it for wireless connections later.

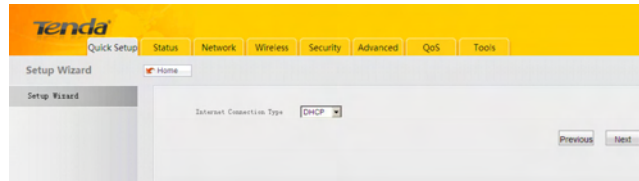
It is advisable that you select the WPA-PSK>AES encryption



method for better security. Simply enter 8-63 alphanumeric characters or other symbols in the Security Key field. For detailed configurations, see sections hereunder.

Click "Next" to continue when finishing above settings.

4. You shall now enter the Internet connection setup screen.



➤ DHCP

This is the default Internet connection type. No configurations are required for this connection. Simply select Dynamic IP and click Next if your ISP is using this connection.

➤ Static IP

If your ISP offers you static IP Internet connection type, select "Static IP" from corresponding drop-down menu, enter IP address, subnet mask, Primary DNS and secondary DNS (optional) info provided by your ISP in corresponding fields. Click "Next" to continue when finishing above settings.

Internet Connection Type: **Static IP**

IP Address: 192.168.100.100

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.100.1

Primary DNS Address: 202.96.134.33

Secondary DNS Address: 202.96.134.133 (Optional)

MTU: 1500 (Default is 1500.)

Save Cancel

➤ **PPPoE**

Select PPPoE, if your ISP is using a PPPoE connection, enter the PPPoE user name and password provided by your ISP in corresponding fields. Contact your ISP for help if you are not clear about or unfortunately forget this info. Click "Next" to continue when finishing above settings.

For example: Assuming that your ISP provides you with a user name: pppoe\_user and a password: pppoe\_passwd, then simply enter them in corresponding fields as seen on the screenshot.

PPPoE User Name: pppoe\_user

PPPoE Password: pppoe\_passwd

Config WAN MAC:

MAC Address: 00:00:00:55:58:08 (Example: 08:3a:35:3e:10:88)

Clone MAC Restore Default MAC

Previous Next

After device reboot, go to Status to check the WAN (Internet) connection status. If you see below info there, congratulations, you can enjoy surfing now.

WAN Status	
Internet Connection Status	Connected
WAN IP	183.39.221.78
Subnet Mask	255.255.255.255
Gateway	183.39.220.1
DNS Server	202.96.134.33
Secondary DNS Server	202.96.128.86
Internet Connection Type	PPPoE
<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>	

For methods of configuring more and featured functionalities, read sections hereunder.

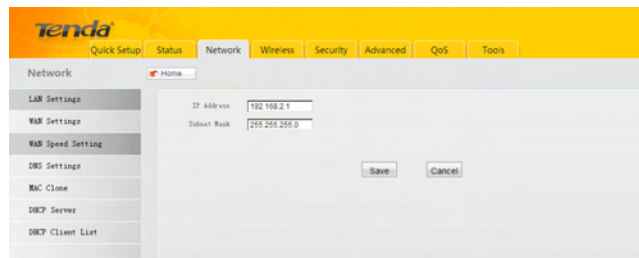
Note: It is strongly recommended not to change the channel settings when using this mode, as improper change may cause connection failure. Click Finish and reboot device to activate new settings

Important: The device must share identical channel, security (including security key), extension channel (if any) settings with the link partner to achieve successful connection in this mode.

## Chapter 7 Network Setup

### 7.1 LAN Setup

This section allows you to config the TCP/IP settings for the device's LAN interface.



IP Address: Device's LAN IP address, 192.168.2.1 by default. You can change it according to your needs; just remember to use the new one to log on to the device's web utility if you changed it.

Subnet Mask: Device's LAN subnet mask, 255.255.255.0 by default.

Note: If you change the device's LAN IP address, you must use the new one to log on to the web-based configuration utility.

### 7.2 WAN Settings

WAN setup is only available in WISP Mode and Wireless Router Mode.

## PPPoE

- Internet connection Type: Displays the current Internet connection type.
- User Name: Enter the User Name provided by your ISP.
- Password: Enter the password provided by your ISP.
- MTU: Maximum Transmission Unit. DO NOT change it from the factory default of 1480 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled; in this case, try 1450, 1400, etc.
- Service Name: Description of PPPoE connection. Leave blank unless otherwise required.
- Server Name: Description of server. Leave blank unless otherwise required.

**Static IP**

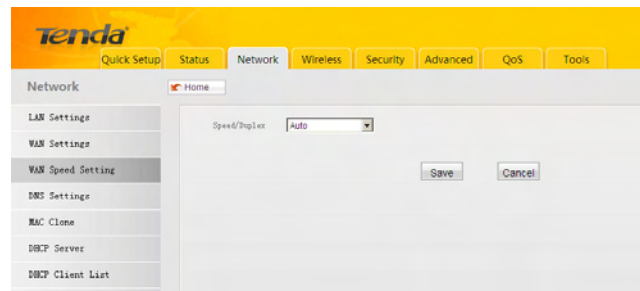
The screenshot shows the Tenda web interface with the 'Network' tab selected. On the left, there is a sidebar menu with options: LAN Settings, WAN Settings (highlighted), WAN Speed Setting, DNS Settings, MAC Clone, DHCP Server, and DHCP Client List. The main content area is titled 'Network' and contains a 'Home' link. Below this, the 'Internet Connection Type' is set to 'Static IP'. There are input fields for 'IP Address', 'Subnet Mask', 'Gateway IP Address', 'Primary DNS Address', and 'Secondary DNS Address'. The 'Secondary DNS Address' field has '(Optional)' next to it. At the bottom, there is an 'MTU' field set to '1500 (Default is 1500)'. 'Save' and 'Cancel' buttons are located at the bottom right of the form.

If your ISP assigns a fixed IP address to you, then select Static IP, and enter the IP address, subnet mask, primary DNS and secondary DNS (optional) info provided by your ISP in corresponding fields.

- IP Address: Enter the WAN IP address provided by your ISP. Consult your ISP if you are not clear.
- Subnet Mask: Enter WAN Subnet Mask provided by your ISP. The default is 255.255.255.0.
- Gateway: Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.
- Primary DNS Server: Enter the DNS address provided by your ISP.
- Secondary DNS Server: Enter the other DNS address if your ISP provides 2 such addresses (optional).

### 7.3 WAN Speed

This section lets you setup a proper speed/duplex for device's WAN port.



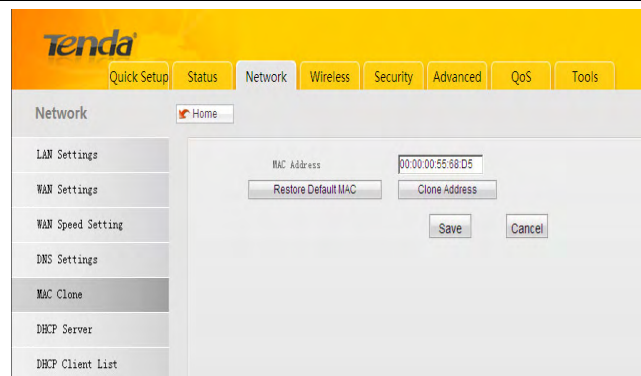
Select auto (auto-negotiation), 10M half duplex, 10M full duplex, 100M half duplex or 100M full duplex depending on your network environment.

The WAN port speed/duplex mode must match that of the link port to achieve successful communication; otherwise, the WAN port may not function properly. So, if you are not sure about the link port's speed/duplex mode, please select "Auto".

Try to change the WAN speed/duplex to 10M full duplex if the WAN connection status alternates between "Connecting" and "Disconnected".

#### **7.4 WAN MAC Clone**

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



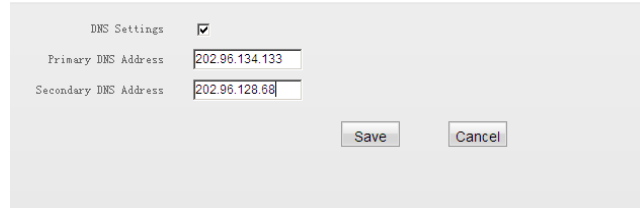
Normally you don't need to change device's default WAN MAC address. However, some ISPs may bind client PC's MAC address for Internet connection authentication. In this case, simply enter the bound MAC in the WAN MAC Address field or click "Copy My PC's MAC" to populate the field automatically. (Config above settings using the PC whose MAC address is bound with your ISP.)

- WAN MAC Address: Config Device's WAN MAC address.
- Copy My PC's MAC: Click to copy your PC's MAC address to device's WAN MAC address field.
- Restore to Factory Default MAC: Reset Device's WAN MAC to factory default.

## 7.5 DNS Server

DNS is short for Domain Name System or Domain Name Service. It resolves catchy domain names into corresponding IP addresses





The screenshot shows a web-based configuration interface for DNS settings. At the top left, it says "DNS Settings" with a checked checkbox. Below this, there are two input fields: "Primary DNS Address" containing the value "202.96.134.133" and "Secondary DNS Address" containing the value "202.96.128.68". At the bottom right of the form area, there are two buttons: "Save" and "Cancel".

- DNS: Check/uncheck to enable/disable the DNS server feature.
- Primary DNS Server: Enter the DNS address provided by your ISP.
- Secondary DNS Server: Enter the other DNS address if your ISP provides 2 such addresses (optional).

## Chapter 8 Wireless Settings

### 8.1 Wireless-Basic

- **802.11 Mode:** Select a right mode according to your wireless client.
  - 11b mode: Select it if you have only Wireless-B clients in your wireless network.
  - 11g mode: Select it if you have only Wireless-G clients in your wireless network.
  - 11b/g mixed mode: Select it if you have only Wireless-B and Wireless-G clients in your wireless network.
  - 11b/g/n mixed mode: Select it if you have Wireless-B, Wireless-G and Wireless-N clients in your wireless network.
- **SSID:** A SSID (Service Set Identifier) is the unique name of a wireless network. This option is configurable.
- **BSSID:** A BSSID, in IEEE 802.11 wireless network, is the MAC address of a wireless AP.
- **SSID Broadcast:** Select “Enable”/“Disable” to make your wireless network visible/ invisible to any wireless clients

within coverage when they perform a scan to see what's available. When disabled, this SSID becomes invisible to any wireless clients within the coverage. Manually enter the SSID if you want to connect to it.

- **Channel:** For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- **Channel Bandwidth:** Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select 40M frequency band; when there are only non-11n wireless clients, select 20M frequency band mode; when the wireless network mode is 11n mode, please select 20/40 frequency band to boost its throughput.
- **Extension Channel:** Available only in 11b/g/n mixed mode. It is used to ensure N speed for 802.11n devices on the network.

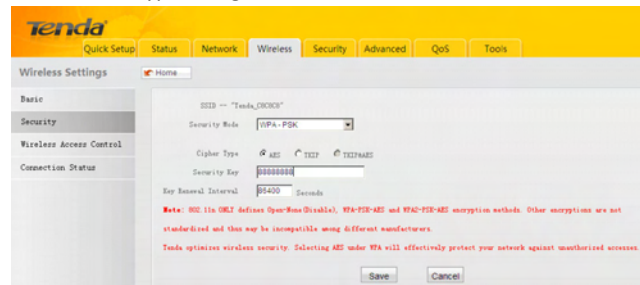
## 8.2 Wireless-Security

This section allows you to encrypt your wireless network to block unauthorized accesses and malicious packet sniffing with WEP, WPA and WPA2. For better security, it is advisable to use the WPA-AES encryption.

### 8.2.1 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 hampered with. Only authorized network users can access the wireless network. WPA adopts enhanced encryption algorithm over WEP.



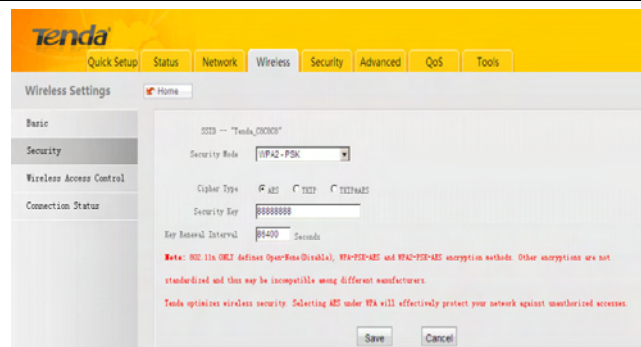
Cipher Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol).

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

Key Renewal Interval: Specify a valid time interval for the key to be updated.

### 8.2.2 WPA2-PSK

The later WPA2 protocol (Wi-Fi Protected Access version 2) 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.



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

### 8.2.3 Mixed WEP

WEP is intended to provide data confidentiality comparable to that of a traditional wired network.

Wireless Settings

Basic

Security

Wireless Access Control

Connection Status

SSID -- "Tenda\_001000"

Security Mode: Mixed WEP

Default Key: Key 1

WEP Key 1: 12345 ASCII

WEP Key 2: 12345 ASCII

WEP Key 3: 12345 ASCII

WEP Key 4: 12345 ASCII

Note: IEEE 802.11a (G/L) defines Open Mode (Disable), WEP-TKIP-48bit and WPA2-TKIP-48bit encryption methods. Other encryptions are not standardized and thus may be incompatible among different manufacturers.  
Tenda optimizes wireless security. Selecting AES under WPA will effectively protect your network against unauthorized accesses.

Save Cancel

- **Security Mode:** Select a proper security mode from the drop-down menu. Here we select Mixed WEP.
- **WEP Key:** Select ASCII or Hex.
- **Note:** Enter 5 or 13 ASCII characters (Invalid characters like / " and ', etc are not allowed) if you select ASCII or enter 10 or 26 HEX characters if you select Hex. Note that you must enter the key content in the corresponding format selected.
- **Default Key:** Select a key from the preset keys 1-4 for current use.

### 8.3 Wireless Access Control

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



- **MAC Filter:** "Allow Access to Wireless Network" only allows PCs at specified MAC addresses (in the list) to connect to your wireless network; Deny Access to Wireless Network: Block only PCs at specified MAC addresses from connecting to your wireless network.
- **MAC Address:** Enter the MAC address of a wireless client which you want to allow or disallow to connect your wireless network. Add: Click to add the MAC address.
- **MAC Address List:** Displays added MAC address entries. You can add new entries or delete existing entries according to your needs.

## 8.4 Connection Status

This section displays the info of connected wireless clients including MAC addresses and frequency width, etc.

This section displays info of connected clients.

Currently Connected Clients:

ID	MAC Address	Bandwidth
1	C8:3A:35:C6:E3:E5	40M

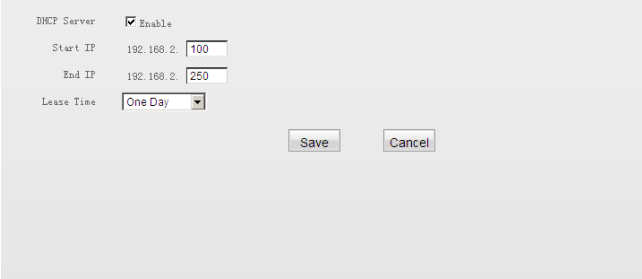
- **MAC Address:** Displays MAC addresses of wireless clients connected to the Device.
- **Bandwidth:** Displays channel bandwidth used by currently connected hosts (wireless clients).



## Chapter9 DHCP

### 9.1 DHCP Settings

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 TCP/IP protocol settings for all DHCP-Client-enabled PCs in your LAN (Namely, PCs are set to "Obtain an IP address automatically" and "Obtain DNS server address automatically"), including IP address, subnet mask, gateway and DNS etc, eliminating the need for manual intervention.



DHCP Server  Enable

Start IP 192.168.2. 100

End IP 192.168.2. 250

Lease Time One Day

Save Cancel

- **DHCP Server-Enable:** Check or uncheck the box to enable or disable the device's DHCP server feature.
- **Start IP:** Enter the starting IP address for the DHCP server's IP assignment.
- **End IP:** Enter the ending IP address for the DHCP server's IP assignment.

- **Lease Time:** The length of time for the IP address lease. Configuring a proper lease time improves the efficiency for the DHCP server to reclaim disused IP addresses.
- **For example:** If the lease time is set to one hour, then the DHCP server will reclaim disused IP addresses every hour.

## 9.2 DHCP Client List & Reservation

DHCP Client List displays information of devices that have obtained IP addresses from the device's DHCP Server. If you would like some devices on your network to always have the same IP addresses, you can use this feature and manually add a static DHCP Reservation entry for each such device. And then a registered MAC will get a correspondingly reserved IP address while an unregistered MAC will be assigned with an unused IP address.

ID	IP Address	MAC Address	Delete
----	------------	-------------	--------

Host Name	IP Address	MAC Address	Lease Time
Test-20120918	192.168.2.100	08:3A:35:C6:E3:85	23:16:41

- **Host name:** Displays name of a given host (DHCP client). IP Address: Enter the IP address for static DHCP reservation.
- **MAC Address:** Enter the MAC address of a computer to always receive the same IP address (the IP you just specified).

- **Lease Time:** Displays remaining time for a corresponding IP address lease.

## Chapter 10 Virtual Server

The virtual server feature is only available in WISP Mode and Wireless Router Mode.

### 10.1 Port Forwarding

Port Forwarding allows you to open a range of WAN service ports and redirect all traffic received through such ports to a LAN server at a designated IP address. It allows remote computers, such as PCs from Internet, to access web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications on a private local area network (LAN).

ID	Start Port-End Port	Private IP	Protocol	Enable	Delete
0.	23-80	192.168.2.10	TCP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.		192.168.2.	TCP	<input 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"/>
8.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>
9.		192.168.2.	TCP	<input type="checkbox"/>	<input type="checkbox"/>

Wall-known Service Port:  DNS(S3)  ID:

- **Start/End Port:** Enter the number or range of port(s) used by the server or Internet applications.
- **Private 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:** Click to remove a corresponding entry/rule.

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 populate the selected port to the corresponding fields of the selected entry. In case that you don't find the port you need, enter it manually.

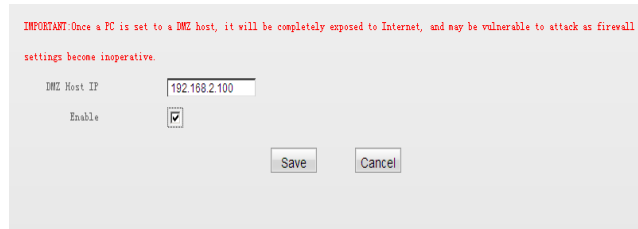
- **Add to:** Click to add a selected Well-Known Service Port to Port fields of the entry you selected.
- **For example:** A LAN PC at 192.68.2.10 hosts WEB service on Port 80 and provides Telnet service on Port 23. To make such services accessible to Internet users, config as shown on the screenshot above.

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

## 10.2 DMZ Host

In some cases such as playing Internet games or holding video conferences, you may need to have your computer completely exposed to external networks for implementation of a bidirectional communication. To do so, set it as a DMZ host. Note that you

should assign a static IP address to the PC designated as a DMZ host (DHCP Server> DHCP Client List> DHCP Reservation) before using the feature.



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

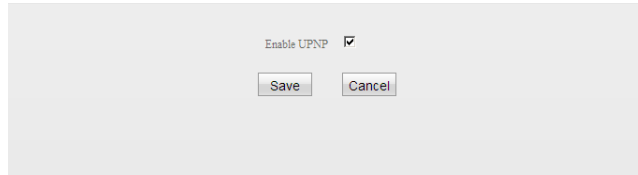
For example: To set a PC at 192.168.2.10 to a DMZ host for intercommunication with another host on the Internet, config the same settings as shown on the screenshot on the device.

**Note:** Once enabled, the DMZ host loses protection from device's firewall and becomes vulnerable to attacks.

### 10.3 UPNP

Note: UPnP (Universal Plug and Play) works in Windows XP, Windows ME or later (NOTE: Operational system needs to be integrated with or installed with Directx 9.0) or in an environment with installed application software that supports UPnP. It allows a network device to discover and connect to other devices on the network. With this feature enabled, hosts in LAN can request the

device to perform special port forwarding so as to enable external hosts to access resources on internal hosts.



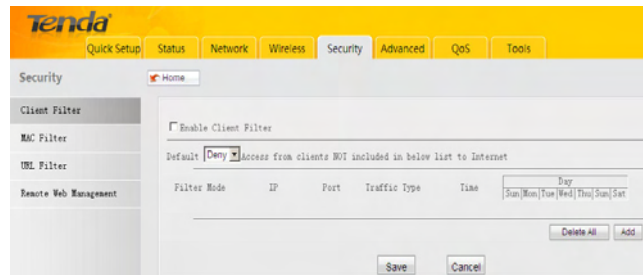
**Enable UPnP:** Check/uncheck to enable/disable the UPnP feature.

## Chapter 11 Security

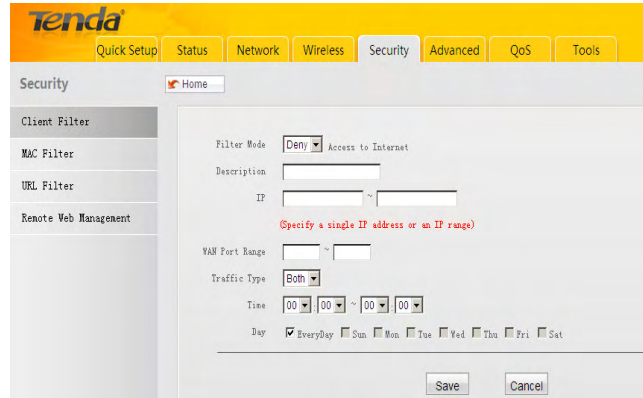
The Security feature is only available in WISP Mode and Wireless Router Mode.

### 11.1 Client Filter

To better manage PCs in LAN, you may use the Client Filter functionality to allow or disallow PCs within a specified range of IP addresses to access Internet.



Click "Add" to enter page below:



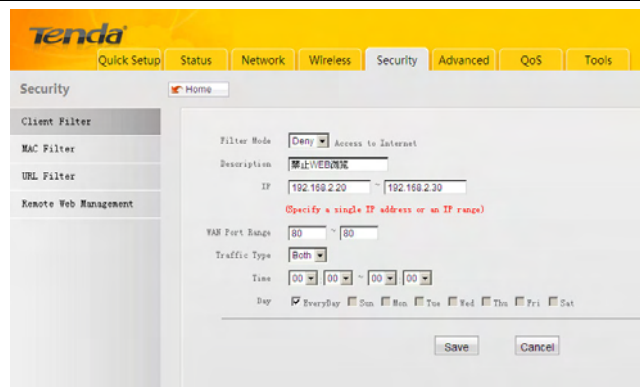
Filter Mode: Select Deny or Allow according to your own needs.



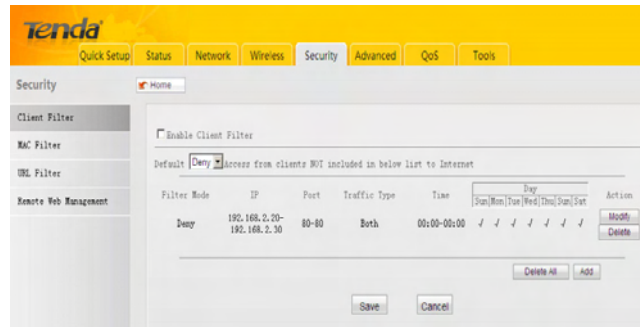
Deny Access to Internet: Disallow specified packets to pass through the device; other packets are processed according to default mode.

Allow Access to Internet: Allow specified packets to pass through the device; other packets are processed according to default mode.

- **Description:** Briefly describe the current entry/rule.
- **IP Address:** Specify a single IP address or an IP range of PCs for current rule to apply to.
- **WAN Port Range:** Specify a single port or a range of ports by entering an identical port NO or two different port NOs in both boxes respectively. Allowed port NO ranges from 1 to 65535.
- **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.
- **Example:** To prohibit PCs within the IP address range of 192.168.2.20-192.168.2.30 from accessing Internet from 8:00 to 18: 00 during working days (Monday-Friday), do as follows:



Click “Save” and you will find such entry in the List below.

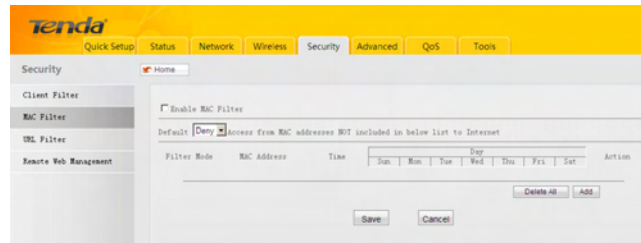


Select Allow from the Default Mode drop-down list and check Enable Client Filter feature.

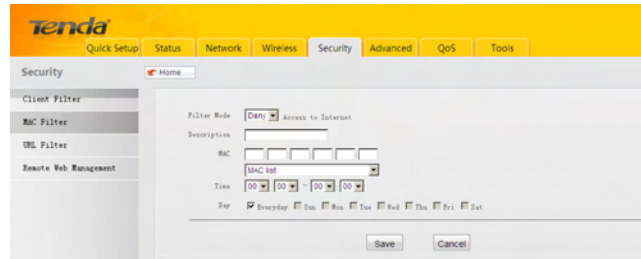
### 11.2 MAC Filter

To better manage computers in your LAN network, you can

use the MAC Filter feature to allow or disallow specified PCs to access Internet.



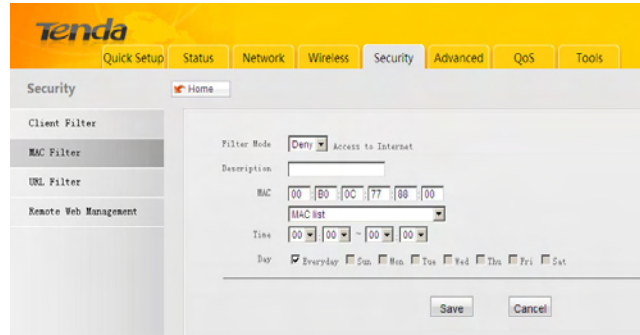
Click “Add” to enter page below:

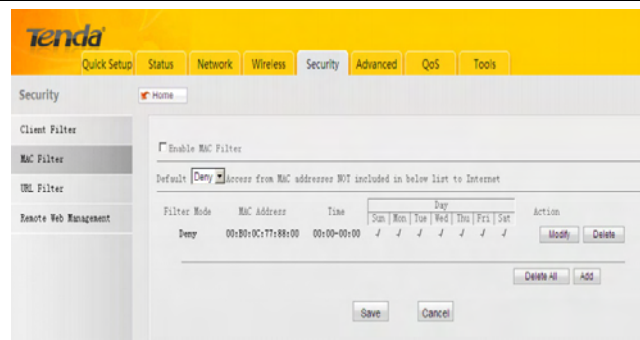


- **Filter Mode:** Select Deny or Allow according to your own needs.
  - Deny Access to Internet:** Disallow specified packets to pass through the device; other packets are processed according to default mode.
  - Allow Access to Internet:** Allow specified packets to pass through the device; other packets are processed according to default mode.
- **Description:** Simply describe current rule/rule.

- **MAC Address:** Enter the PC's MAC address that you want to filter out or select it from the MAC list.
- **Time:** Select a time range for current rule to take effect.
- **Day:** Select a day or several days for current rule to take effect.

Example: To prevent a PC at the MAC address of 00:B0:0C:77:88:00 from accessing Internet from 8:00 to 18:00 daily without restricting it during other time period, config the same settings as shown on the screenshot below on your device:

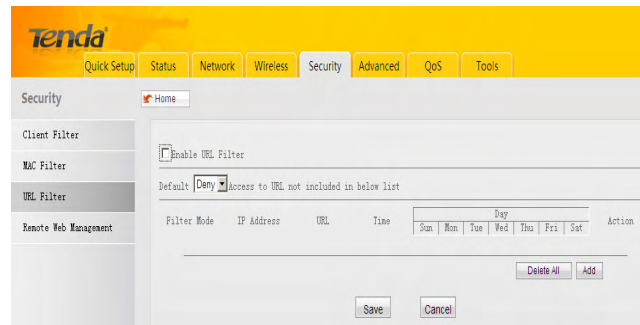




Click “Save”, select “Allow” from the “Default” drop-down list and check the “Enable MAC Filter” feature.

### 11.3 URL Filter

To better regulate LAN PCs, you may use the Website Filter (also known as URL Filter) functionality to allow or disallow such PCs to access certain websites within a specified time period.



Click “Add” to enter page below:

- Filter Mode: Select Deny or Allow according to your own needs.

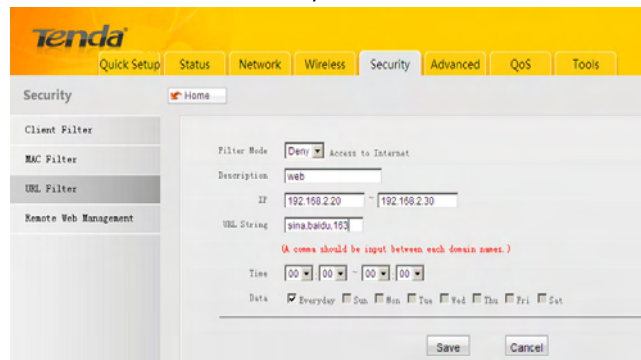
Deny Access to Internet: Disallow specified packets to pass through the device; other packets are processed according to default mode.

Allow Access to Internet: Allow specified packets to pass through the device; other packets are processed according to default mode.

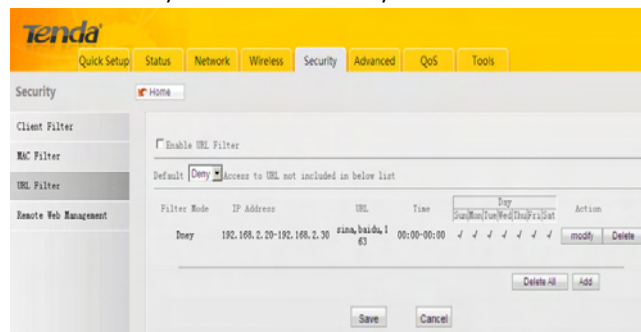
- **Description:** Briefly describe a current entry/rule.
- **IP Address:** Specify a single IP address or an IP range of PCs for current rule to apply to.
- **URL String:** Enter domain names or a part of a domain name to be filtered out.
- **Time:** Specify a time range for current entry to take effect.
- **Day:** Select a day or several days for current entry to take effect.

For example: If you want to disallow only PCs within the IP

range of 192.168.2.20~192.168.2.30 on your LAN to access only "yahoo.com" from 8: 00 to 18: 00 during working days (Monday-Friday) while not restricting other PCs, then config same settings as shown on below screenshot on your device:



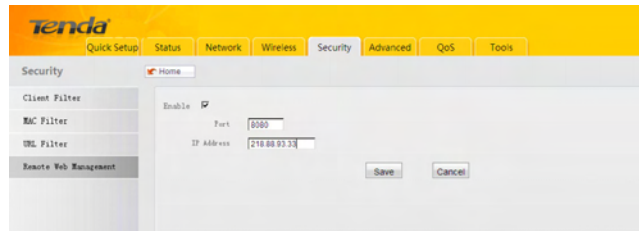
Click "Save" and you will find such entry in the List below.



Select Allow from the Default Mode drop-down list and check Enable U R L Filter (Also known as website filter on some

## 11.4 Remote Web-based Management

The Remote Web Management feature allows the Router to be managed from the Internet via a web browser.



- **Enable:** Select whether to enable the Remote Web-based Management feature.
- **Port:** Remote admin port; the port used by trusted hosts from Internet or other external networks to access and manage the Router remotely.
- **IP Address:** Enter the trusted IP address of a PC from Internet or other external networks which you want to authorize to manage your router remotely.

Note: To access the device via port 8080, enter "http://x.x.x.x:8080" where "x.x.x.x" represents the the device's Internet IP address and 8080 is the remote admin port. Assuming the device'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).



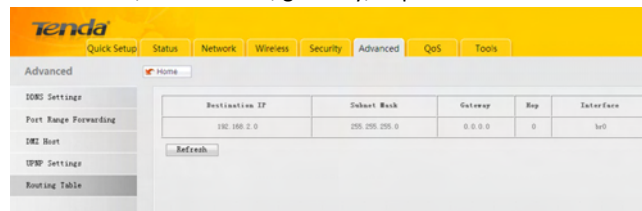
Leaving the IP address field at "0.0.0.0" makes the device remotely accessible to all the PCs on Internet or other external networks; populating it with a specific IP address, say, 218.88.93.33, makes the device only remotely accessible to the PC at the specified IP address.

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

## Chapter 12 Routing Settings

### 12.1 Routing Table

This page displays the device core routing table which lists destination IP, subnet mask, gateway, hop count and interface.



Destination IP	Subnet Mask	Gateway	Hop	Interface
192.168.2.0	255.255.255.0	0.0.0.0	0	lan

The principal task for a router is to look for an optimal transfer path for each data packet passing through it, and transfer it to the specified destination. So, it's essential for a router to select an optimal path, i.e. routing algorithm. To complete this work, the router stores and maintains related data of various transfer paths, i.e. establishing a routing table, for future route selection.

## Chapter 13 Bandwidth Control

Use this section to manage bandwidth allocation to devices on your LAN.

### 13.1 Bandwidth Control

Enable the bandwidth control feature and you will see below screen.

The screenshot shows the Tenda router's web interface for configuring bandwidth control. The main navigation bar includes 'Quick Setup', 'Status', 'Network', 'Wireless', 'Security', 'Advanced', 'QoS', and 'Tools'. The 'Bandwidth Control' page is displayed, featuring a 'Home' button and a 'Bandwidth Control' section. This section includes a 'Bandwidth Control' checkbox (checked), an 'IP Address' field (containing '100.100.2'), 'Upload Limit' and 'Download Limit' fields (both with 'KB/s (Max Traffic)' units), and an 'Enable' checkbox (unchecked). Below these fields is an 'Add to List' button. At the bottom, there is a table with columns: IP, IP Range, Uplink, Downlink, Enable, Edit, and Delete. Below the table are 'Save' and 'Cancel' buttons.

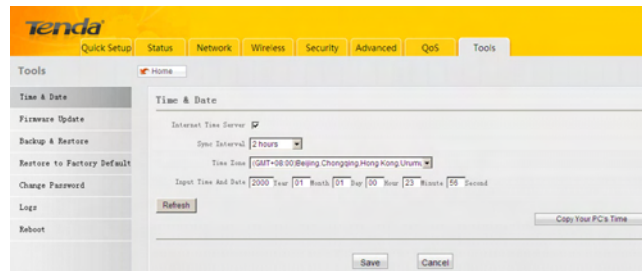
- IP Address: Enter an Identical IP or two different IPs in both boxes to specify only a single IP address or an IP range.
- Upload Limit: Max total upload bandwidth for a specified PC or a range of PCs.
- Download Limit: Max total download bandwidth for a specified PC or a range of PCs.
- Enable: The corresponding entry takes effect only if you checked this option.
- Edit: Click to edit an existing entry/rule.

- Delete: Click to remove a corresponding entry/rule.

## Chapter 14 Tools

### 14.1 Time & Date

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 Device is connected to Internet. You can also configure the system time manually.

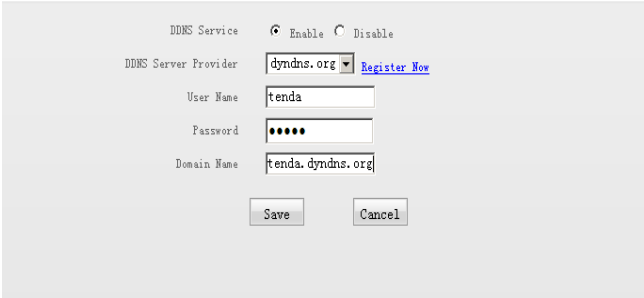


- Internet time servers: Time and date will be updated automatically from Internet if enabled.
- Sync Interval: Specify a time length for device to update its time and date info from Internet periodically. The default is 2 hours.
- Time Zone: Select your current time zone.
- Copy Your PC's Time: Click it to copy your PC's time to the device.

Note: Configured time and date info loses when the device is 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.

## 14.2 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; 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.



DDNS Service  Enable  Disable

DDNS Server Provider  [Register Now](#)

User Name

Password

Domain Name

- Service Provider: Select your DDNS service provider from the

drop-down menu.

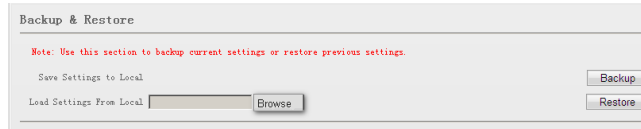
- User Name: Enter the DDNS user name registered with your DDNS service provider.
- Password: Enter the DDNS Password registered with your DDNS service provider.
- Domain Name: Enter the DDNS domain name with your DDNS service provider.
- For example: If you have registered a DDNS service in dyndns.org and are allocated with tenda, 123456, tenda.dyndns.info respectively as username, password and domain name for a web server on your PC at 192.168.2.10:

User Name	tenda
Password	123456
Domain Name	tenda.dyndns.org

Then configure port settings on port range forwarding interface and enter this information on the above DDNS interface. Others can access your web server by simply entering http://tenda.dyndns.info in their browser address bar.

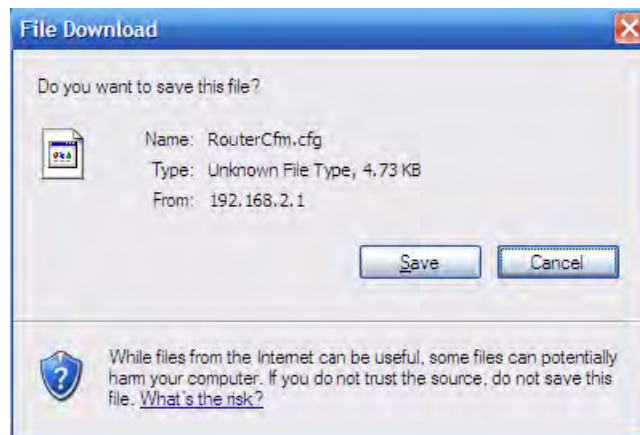
### 14.3 Back/Restore

This section allows you to backup current settings or to restore previous settings configured on the Device.



To backup settings:

Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do so, click the "Backup" button and specify a directory to save settings on your local hardware.

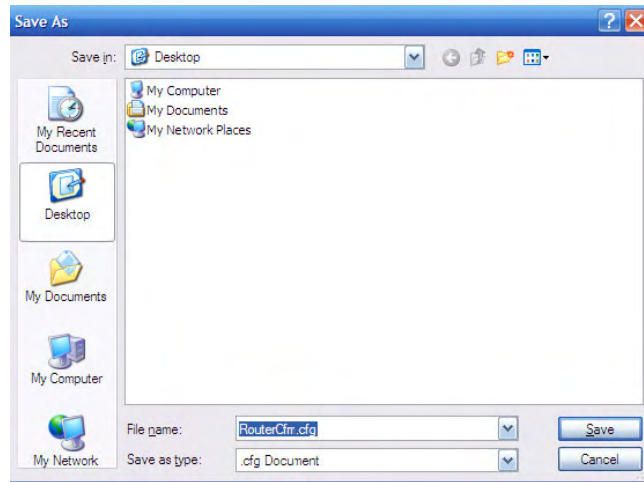


Click Save to save the configuration file.

To restore settings:

Click the "Browse" button to locate and select a configuration file that is saved previously to your local hard drive.





Click the "Restore" button to reset your device to previous settings.



#### 14.4. Restore to Factory Default Settings

Click this button to reset the device to factory default values.

### Restore to Factory Default

To restore factory defaults, click the "Restore to Factory Default" button below.

#### Factory Default Settings:

- Password: admin
- IP Address: 192.168.2.1
- Subnet mask: Enter 255.255.255.0.

Note: To activate your settings, you need to reboot the device after you reset it.

## 14.5 Firmware Update

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](http://www.tendacn.com)) to download the latest firmware to update your device.

### Firmware Update

Use this section to update your router's software for better functionality or new features.

Select Firmware File

Current System Version: V3.02.08; Release Date: Dec 7 2012

**Note: Do not power off the router while upgrading otherwise it may be permanently damaged.**

- Browse: Click to locate and select the firmware.
- Update: Click to start update. Device will restart

automatically when update completes.

**NOTE:** Do not disconnect the device from the management PC (the PC you use to configure the device) or power supply during update; otherwise, it may be permanently damaged.

## 14.6 Reboot

This section allows you to reboot the device. New settings will be activated after reboot. And WAN connection will be disconnected during reboot.

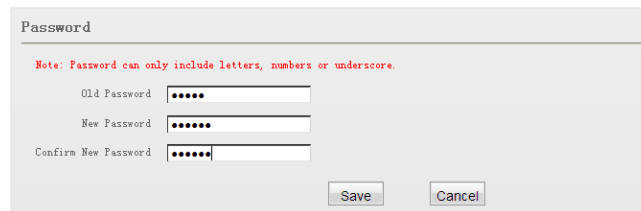


The screenshot shows a web interface titled "Reboot". Below the title, there is a line of text: "Click the button below to restart your router." Below this text is a single button labeled "Reboot".

Reboot: Click to restart the device.

## 14.7 Change Password

This section allows you to change login password for accessing device's Web-based interface.



The screenshot shows a web interface titled "Password". Below the title, there is a red note: "Note: Password can only include letters, numbers or underscore." Below the note are three input fields: "Old Password", "New Password", and "Confirm New Password". Each field contains six black dots. At the bottom right of the form are two buttons: "Save" and "Cancel".

Old Password: Enter the old password.

New Password: Enter a new password.

Confirm New Password: Re-enter the new password for confirmation.

Save: Click to save your new password.

Caution: For security purpose, it is highly recommended that you change Device's default login user name and password.

### 14.8.1 Logs

The Logs option allows you to view all events that occur upon system startup. Up to 150 entries of logs can be recorded.

Index	Time	User	Message
5	2012-12-20 15:23:54	system	start DHCP service success
4	2012-12-20 15:23:54	system	enable dhcp service success
3	2012-12-20 15:23:54	system	enable dhcp service success
2	2012-12-20 15:23:41	root	start setup program
1	2009-01-01 00:00:04	system	ip address interface success

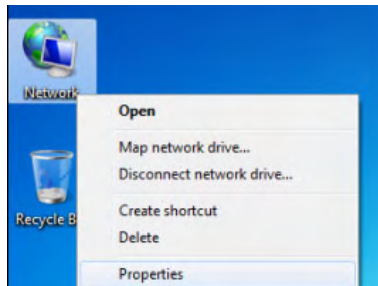
- Refresh: Click to update current logs.
- Clear: Click to remove all logs.

## Appendix 1 Set PC to“Obtain an IP address automatically”

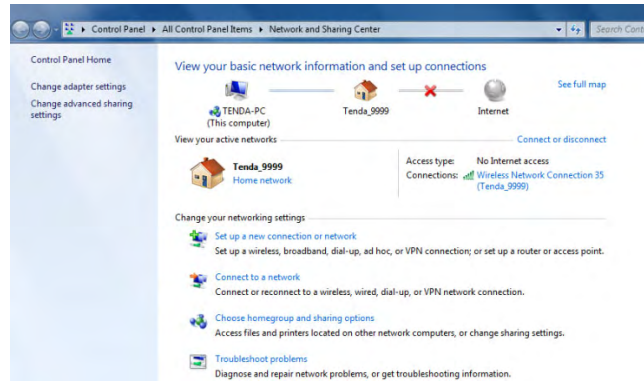
The DHCP server feature is enabled on the device by default. Simply set your PC to “Obtain an IP address

automatically”(enable DHCP client on your PC)and your PC will be able to access Internet via the device.Follow below steps:

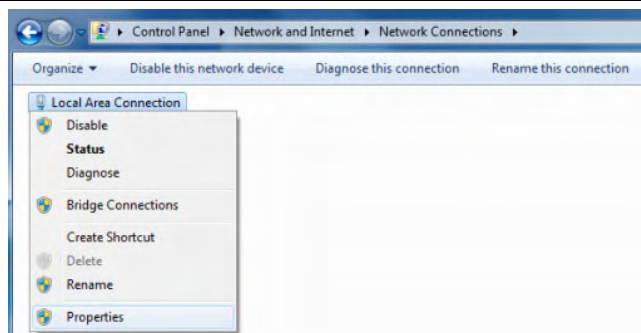
Here we take Windows 7 OS as an example for illustration. From the desktop, right-click Network > Properties.



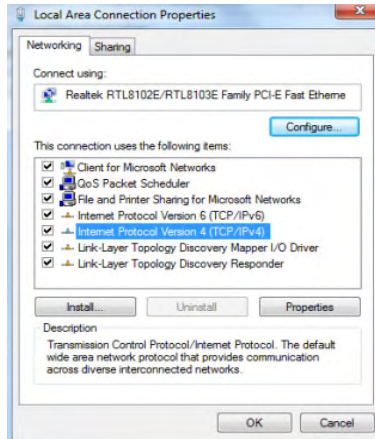
Left click "Change adapter settings".



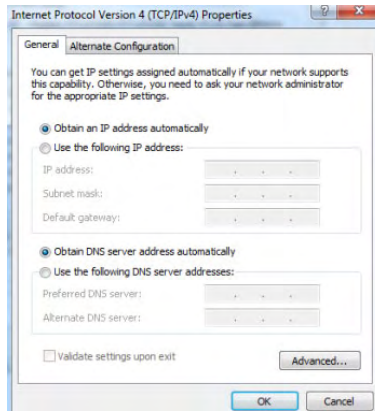
Right click Local Area Connection(or Wireless Network Connection if you are connecting to the device wirelessly)and select Properties.



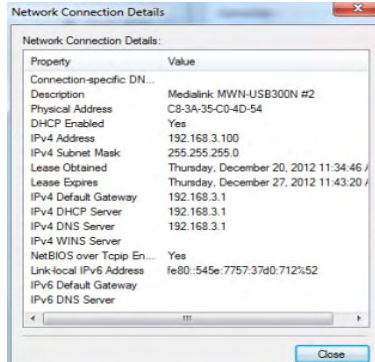
Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".



Select "Obtain an IP address automatically".



Right click Local Area Connection and select Status>Details to check whether your PC has obtained an IP address successfully.



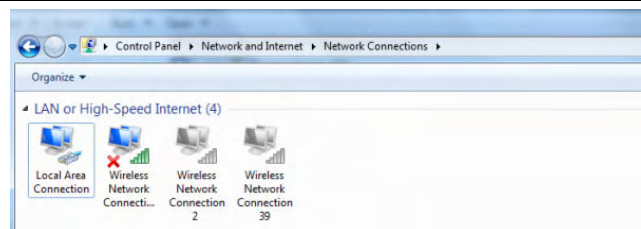
## **Appendix 2. How to connect to an encrypted wireless network**

How should I config my network adapter to successfully connect to an encrypted wireless network? (Below explains how to connect to a WPA-encrypted wireless network in Windows 7 OS)

To connect to an encrypted wireless network, you must provide a valid security key. To configure wireless network adapter, do as follows:

1. Right click "Network", select "Properties", and then left click "Change adapter settings". As seen below, Wireless Network Connection displays "Not Connected".





2. Right click the Wireless Network Connection and select “Connect/Disconnect”. All searched wireless networks shall be displayed in below screen. If you don't see the SSID of Tenda, click Refresh.

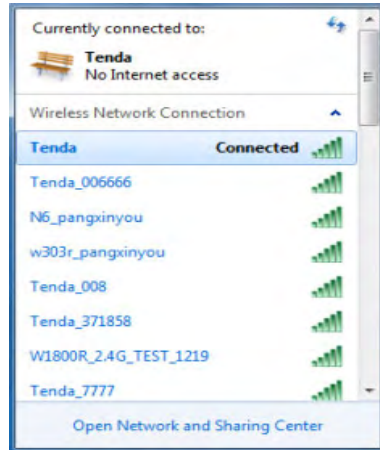


3. Double click or select the SSID entitled “Tenda\_xxxxxx” (wherexxxxxx represents the last 6 characters in the device MAC address) and click “Connect”. Enter the security key on appearing

window (Note that security key is case-sensitive. Here we assume it is tendatenda) and click “OK”.



4. As seen below, display of “Connected” next to “Tenda\_xxxxxx” indicates a successful connection.



## Appendix 3: 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.

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks with the intention to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use. WEP uses the stream cipher RC4 for confidentiality,[5] and the CRC-32 checksum for integrity. Standard 64-bit WEP uses a 40-bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. The extended 128-bit WEP protocol uses a 104-bit key size (WEP-104). A 152-bit WEP is available from some vendors. Static WEP encryption allows to include 4 WEP Keys while dynamic WEP encryption changes WEP key dynamically.

#### **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

## Appendix 4 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 go to our website of [www.tendacn.com](http://www.tendacn.com) or e-mail to [support@tenda.cn](mailto:support@tenda.cn) for help.

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

1) 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.

2) In Wireless Router Mode, you must use a wireless network adapter to connect to the device, as the only Ethernet port works as a WAN port for Internet connection; while in Wireless AP, Universal Repeater Mode and Client Mode, you must specify an IP address (192.168.2.2 ~ 192.168.2.254) on your PC to connect to the device.

3) Click "Start" -- "Run", enter "cmd" and then "ping 192.168.2.1" on appearing CLI to diagnose whether your PC has

connected to the device or not. If ping succeeds, then check whether the Proxy Server feature is enabled on your browser. If enabled, disable it immediately. 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 "ping192.168.2.1" again.

4) 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?**

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?**

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

2) The default IP address of the device is 192.168.2.1; 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. My computer can neither log in to the device nor access Internet, and there is a yellow triangle with an exclamation mark shown in the network adapter icon on the right bottom corner of my computer desktop; how am I supposed to deal with it?**

This problem occurs because your network card has not been assigned with an IP address. If your computer is set to obtain an IP

address automatically, please ensure that the router's DHCP function is enabled. DHCP can automatically assign an IP address to your computer. If there is no DHCP server available on your network, please set a static IP address and fill in gateway and DNS, otherwise you cannot access Internet.

**5. Q: I cannot access Internet and send/receive emails; what should I do?**

This problem mainly happens to users using ADSL dialup or dynamic IP Internet connection types. In this case, go to "WAN Settings" to change the MTU value from default 1480 to 1450 or 1400, etc.

**6. I am using Dynamic IP Internet connection type. How should I config the device for Internet access?**

a. Enter the device web utility, select "Dynamic IP" on Quick Setup section and click "Save".

b. If your ISP requires a specified MAC address for Internet connection authentication, then go to MAC Clone and change the device WAN MAC address to that MAC address and click "Save".

**7. 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 for Web server is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: Click “Advanced” and select “Port Range Forwarding” (Also known as Port Ranging) on the Router’s web interface.

Step 3: Input the start service port (also known as External Port on some devices) NO, say, 80.

Step 4: Input the end service port (also known as Internal Port on some devices) NO, say, 80.

Step 5: Input the internal server’s IP address. For example, assuming that your Web server’s IP address is 192.168. 2.10, then simply input it.

Step 6: Select a communication protocol used by your internal host: TCP, UDP or ICMP and enable the rule.

Step 7: 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
NetMeeting	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



**8. Q: I cannot access Internet in WISP Mode; what should I do?**

a. Make sure your wireless network adapter is functioning correctly on your PC and wireless signal is strong enough. If there are too many available wireless networks, it is advisable to use 802.11 b/g mode for less interference.

b. Make sure you entered correct SSID and MAC address of the link partner on the device. It is advisable to use the “Open scan” option.

c. Make sure the device WAN IP and LAN IP addresses are not on the same IP net segment. If so, change the device LAN IP. The device's IP address is set to 192.168.2.1 to avoid IP conflict with other devices. Generally, you don't need to change it.

d. Make sure antenna on the device is not detached.

If you still are unable to access Internet after you tried all the above steps, contact our technical staff for help.

Website: [www.tendacn.com](http://www.tendacn.com)

Technical Support: [support@tenda.com.cn](mailto:support@tenda.com.cn)

**Shenzhen Tenda Technology Co., Ltd**

## Appendix 5 EMC 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.

### 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.



### 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.

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.

#### 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、加大功率或變更原設計之特性及功能。

低功率射頻電機之使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，指依電信法規定作業之無線電通信。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。