Tenda®

V1.0

User Guide

www.tenda.cn

A5

150Mbps Wireless N Travel Router

Copyright Statement

Tenda® 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.tenda.cn.

CONTENTS

COPYRIGHT STATEMENT 1

CHAPTER 1 PRODUCT OVERVIEW 4

1.1 DESCRIPTION 4
1.2 PACKAGE CONTENTS 4
1.3 PANEL OVERVIEW 4
1.4 MINIMUM SYSTEM REQUIREMENTS 5
1.5 OPERATION ENVIROMENT REQUIREMENTS 6

CHAPTER 2 INSTALLATION 7

2.1 HARDWARE INSTALLATION 7
2.1.1 WIRED WAN CONNECTION 7
2.1.2 WIRELESS WAN CONNECTION 8
2.2 CONFIGURE YOUR PC TO CONNECT TO A5 WIRELESSLY 9
2.2.1 IN WINDOWS XP 9
2.2.2 IN WINDOWS 7 12
2.3 QUICK INTERNET CONNECTION SETUP 17
2.3.1 WIRED INTERNET CONNECTION SETUP 17
2.3.2 WIRELESS INTERNET CONNECTION (WISP) SETUP 19
2.4 QUICK WIRELESS SECURITY SETUP 21

CHAPTER 3 CONFIGURATION 22

3.1 ADVANCED SETTINGS 22
3.1.1 SYSTEM STATUS 22
3.1.2 WAN SETTINGS 23
3.1.3 LAN SETTINGS 28
3.1.4 MAC ADDRESS CLONE 29
3.1.5 DNS SETTINGS 30
3.1.6 WAN MEDIUM TYPE 31
3.1.7 BANDWIDTH CONTROL 32
3.1.8 STATISTICS 35
3.2 WIRELESS SETTINGS 36
3.2.1 BASIC SETTINGS 36
3.2.2 WIRELESS SECURITY 38
3.2.3 MAC-BASED WIRELESS ACCESS CONTROL 40

3.2.4 CONNECTION STATUS 41
3.3 DHCP 42
3.3.1DHCP 42
3.3.2 DHCP CLIENTS 43
3.4 VIRTUAL SERVER 45
3.4.1 PORT RANGE FORWARDING 45
3.4.2 DMZ SETTINGS 47
3.4.3 UPNP SETTINGS 48
3.5 SECURITY SETTINGS 48
3.5.1 CLIENT FILTER 49
3.5.2 MAC ADDRESS FILTER 51
3.5.3 URL FILTER 52
3.5.4 REMOTE WEB-BASED MANAGEMENT 54
3.6 ROUTING SETTINGS 55
3.6.1 ROUTING TABLE 55
3.6.2 STATIC ROUTING 56
3.7 TOOLS 57
3.7.1 TIME SETTINGS 57
3.7.2 DDNS 58
3.7.3 BACKUP/RESTORE SETTINGS 58
3.7.4 RESTORE TO FACTORY DEFAULT SETTINGS 61
3.7.5 FIRMWARE UPGRADE 61
3.7.6 REBOOT 62
3.7.7 CHANGE PASSWORD 63
3.7.8 SYSLOG 64
3.7.9 LOGOUT 64

APPENDIX 1 FEATURES 65

APPENDIX 2 SECURITY STATEMENT 66

Chapter 1 Product Overview

1.1 Description

The Tenda 150Mbps Travel Wireless Router (A5) allows you to create an instant wireless network when you are at hotel, job site or wherever you need one. Just plug it into an electrical outlet, connect to your DSL or cable modem, an existing Ethernet network or a wireless hotspot from ISP (WISP), up to 10 users at a time can surf, chat, play wirelessly and more using PC, Mac, iPad, iPhone or other WiFi-enabled devices. Plus, the A5 supports wired and wireless WAN connections.

1.2 Package Contents

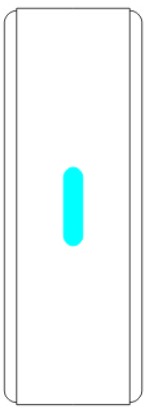
Please unpack the box and check the following items:

- A5 150Mbps Travel Wireless Router
- Quick Installation Guide

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

1.3 Panel Overview

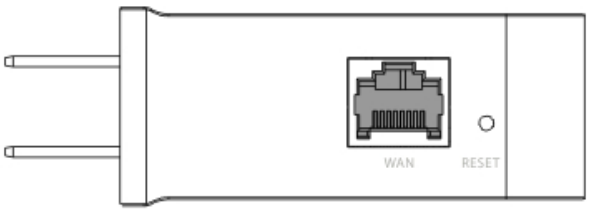
LED overview:



The router has only one LED.

It displays a solid light upon and during router's startup, which indicates the router is correctly powered and system is starting, and thereafter, a flashing light.

Port/Button Overview：



Port/Button Description:

Port/Button	Description
WAN	WAN port: Internet port for connection to a DSL/cable Modem or community broadband via an Ethernet cable or ISP's WIFI hotspot.
Reset	Pressing this button for 7 seconds restores the router to factory default settings.

Note: The RJ45 port functions as a WAN port when you are using a wired WAN connection and a LAN port when you are using a wireless WAN (WISP) connection.

1.4 Minimum System Requirements

Computer with:

- ✓ 128M or larger memory
- ✓ Windows 98/2000/XP/Vista/WIN7/MAC OS
- ✓ A installed 802.11b/g/n 2.4GHz network adapter
- ✓ Internet broadband service, Ethernet access or WIFI hotspot
- ✓ Microsoft Internet Explorer 5.5, Firefox 1.0 or higher

1.5 Operation Environment Requirements

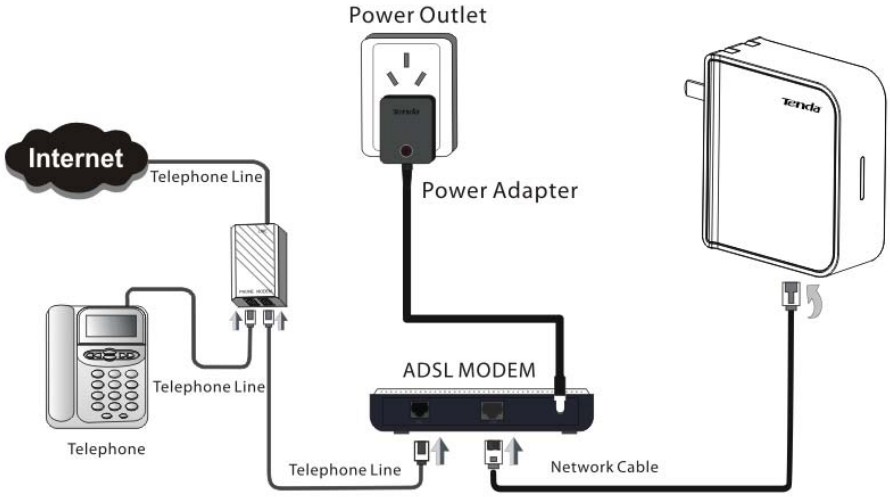
- ✓ The device operates correctly only with a specified voltage rating; otherwise it may be damaged.
- ✓ Keep it away from heat source.
- ✓ Keep it away from electrical appliances (such as a microwave oven) to avoid electromagnetic interference.
- ✓ Disconnect the device's power supply in presence of thunder or storm.

Chapter 2 Installation

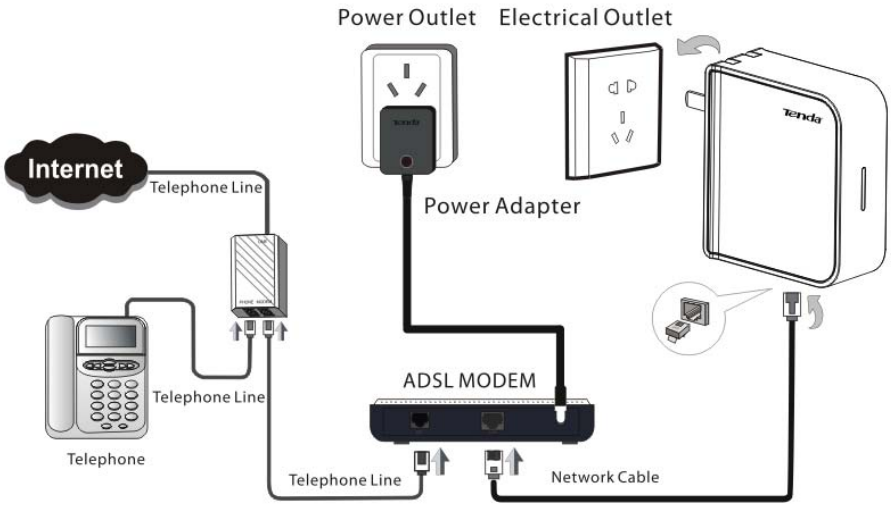
2.1 Hardware Installation

2.1.1 Wired WAN Connection

1. Connect your ADSL/Cable modem to the WAN port on A5 using an Ethernet cable.



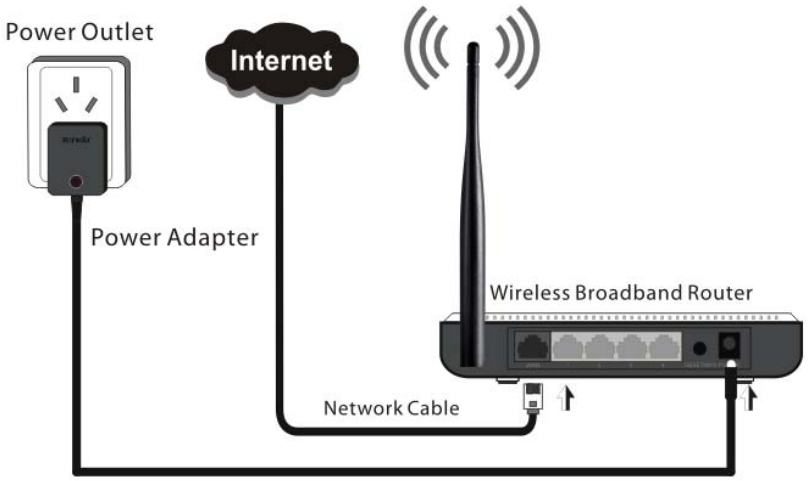
2. Plug A5 into a power outlet nearby.



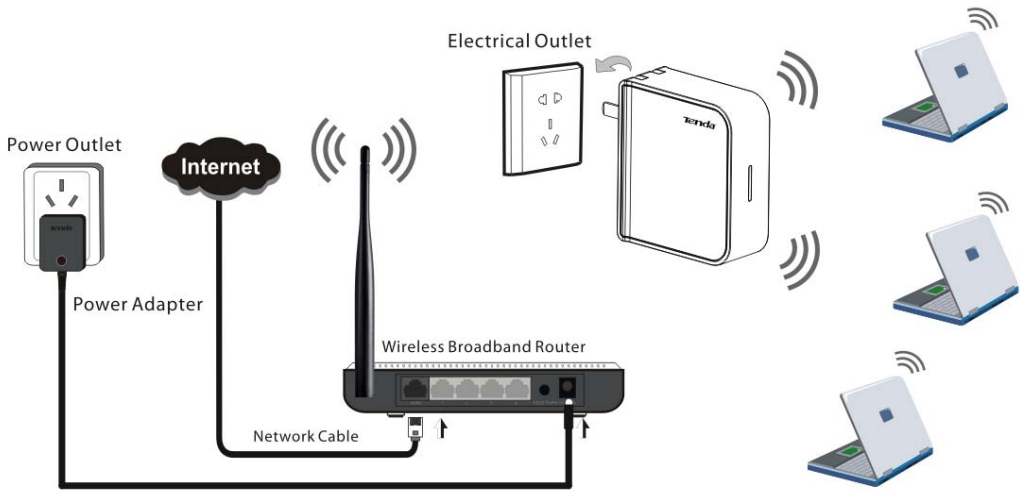
2.1.2 Wireless WAN Connection

With the unique wireless WAN feature enabled, the A5 can work both as a wireless client for connection to a WIFI hotspot or an Internet-service-enabled wireless router and as a wireless AP to extend wireless signal to your reachable distance. Here we explain it using the Tenda W316R, a wireless broadband router.

1. Connect W316R to Internet.



2. Plug A5 into a power outlet nearby.



2.2 Configure Your PC to Connect to A5 Wirelessly

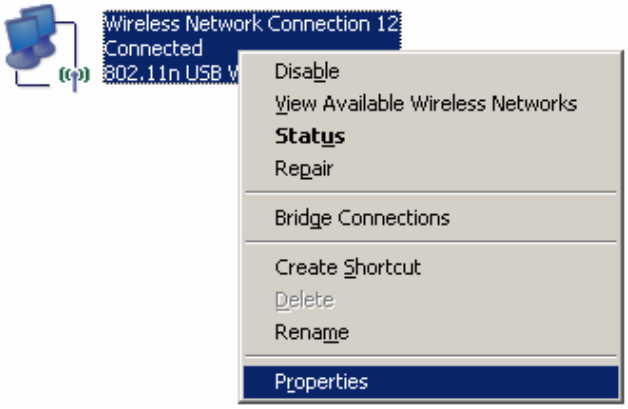
By default, the RJ45 port is used as a WAN port, so you can only connect to A5 via a wireless connection. The wireless security feature is disabled by default. So there is no need to enter a security key for first-time connection to A5.

To configure your PC to connect to A5 wirelessly, Windows XP users refer to section 2.2.1 and Windows 7 users skip to section 2.2.2.

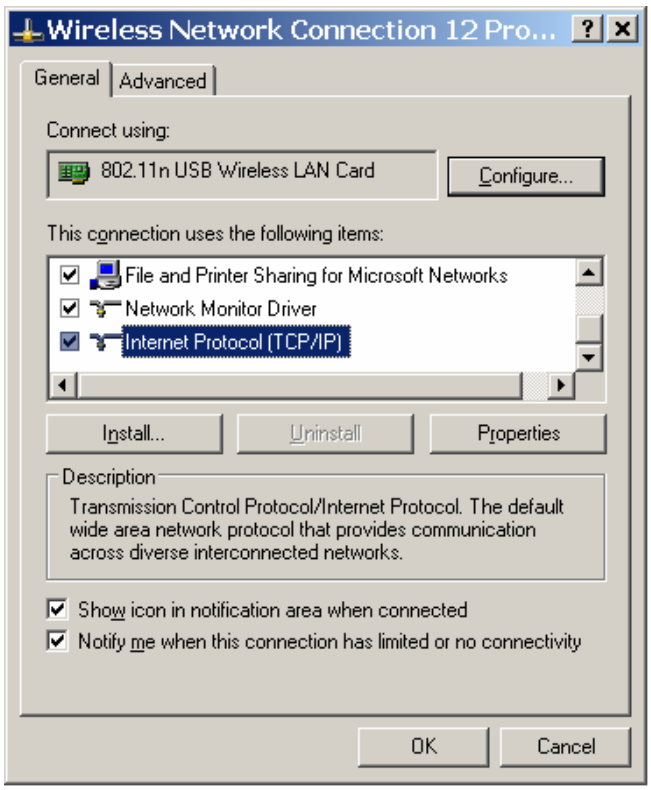
2.2.1 In Windows XP

Step1. Right click “My Network Places” and select “Properties”.

Step2. Right click “Wireless Network Connection” and select “Properties”.

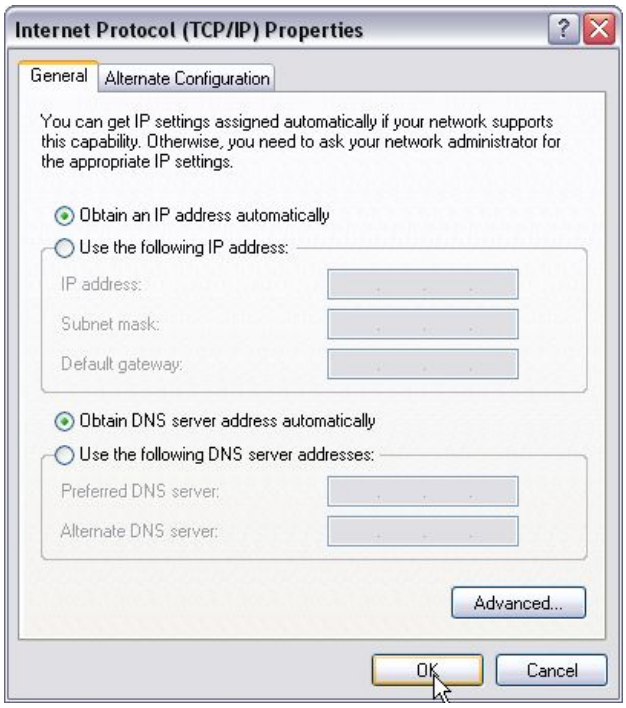


Step3. Select “Internet Protocol (TCP/IPv4)” and then click “Properties”.



Step4. There are 2 ways to configure your PC’s IP address in this TCP/Ipv4.

A. The first one is “Obtain an IP address automatically” as below:



In the IP Address field, Input: 192.168.2.XXX (XXX stands for any value from 2 to 254) and in the Subnet Mask field, input: 255.255.255.0.

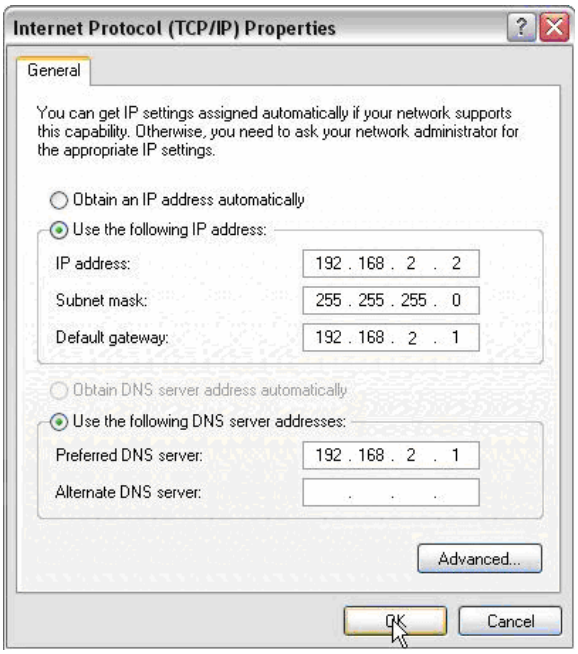
For example:

IP Address: 192.168.2.100

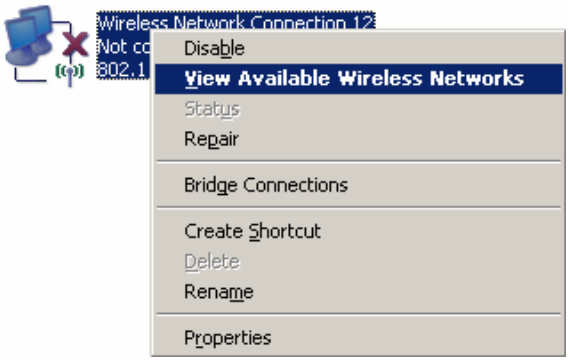
Subnet Mask: 255.255.255.0

DNS Server: you can either enter your local DNS server addresses (Consult your ISP if you are not clear.) or use the device as a proxy DNS server.

After you finish all settings, click “OK” to submit and click the “OK” button for properties on Local Area Connection interface to save them.

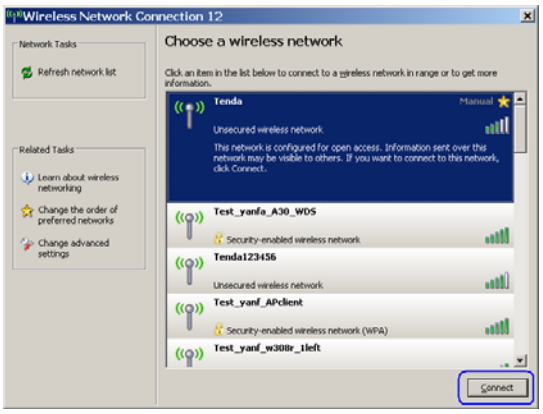


Step5. Right click “Wireless Network Connection” and select select “View Available Wireless Networks”.

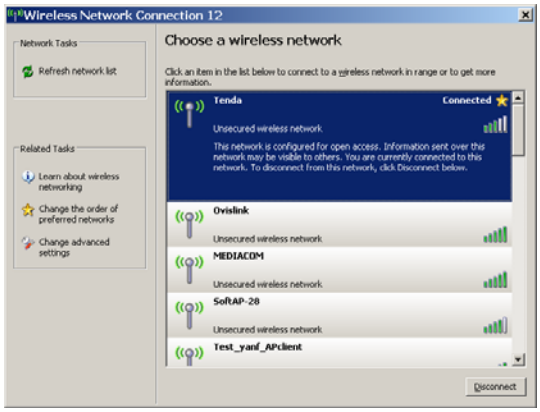


Step6. Select A5's SSID (wireless network name) and click "Connect".

Note: A5's default SSID is Tenda_XXXXXX (XXXXXX stands for the last 6 characters in A5's MAC address).

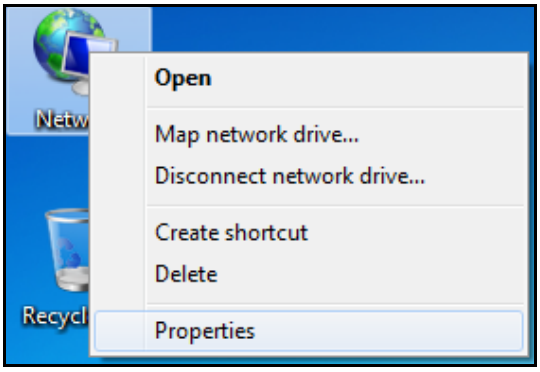


Step7. When you see "Connected" displayed next to A5's SSID, you have successfully connected to A5 wirelessly.

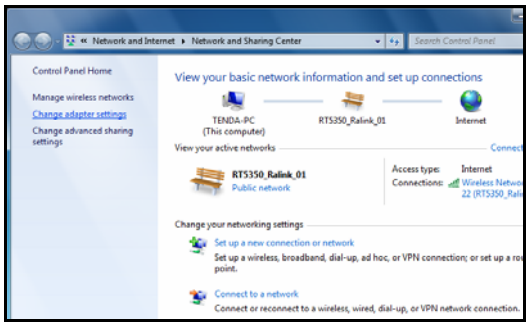


2.2.2 In Windows 7

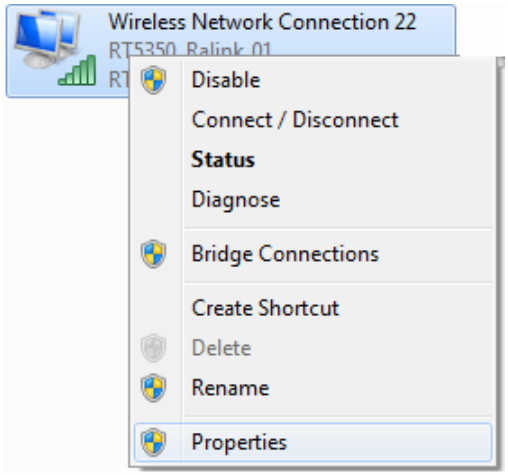
Step1. Right click "Network" icon on your computer desktop and select "Properties".



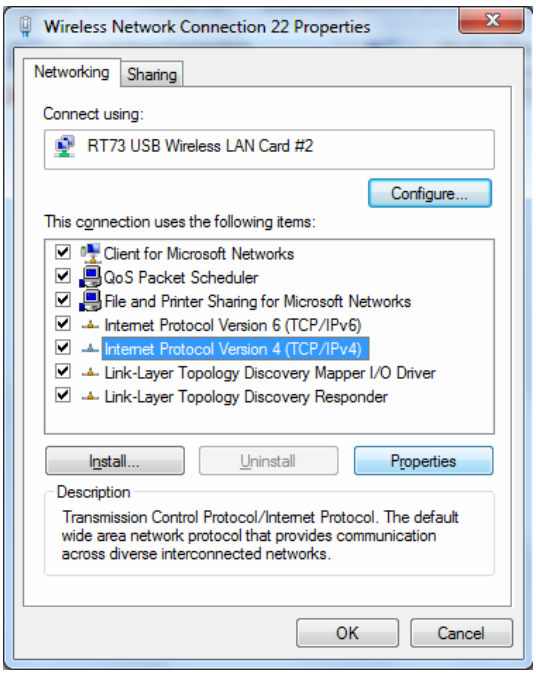
Step2. Click “Change adapter settings” on the appearing window.



Step3. Select “Wireless Network Connection” and select “Properties” in the following window.

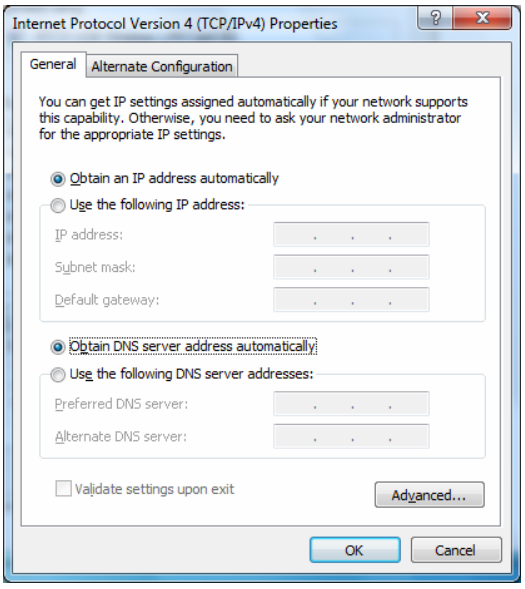


Step4. Select” Internet Protocol Version 4(TCP/IPv4)"and then click “Properties” in the appearing window.

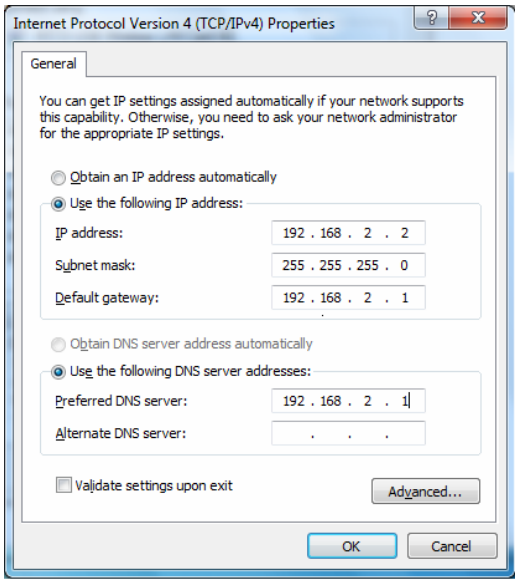


Step5. There are 2 ways to configure your PC's IP address in this TCP/Ipv4.

A. The first one is "Obtain an IP address automatically" as below:



B. The second one is "Use the following IP address" as below:



In the IP Address field, Input: 192.168.2.XXX (XXX stands for any value from 2 to 254) and in the Subnet Mask field, input: 255.255.255.0

For example:

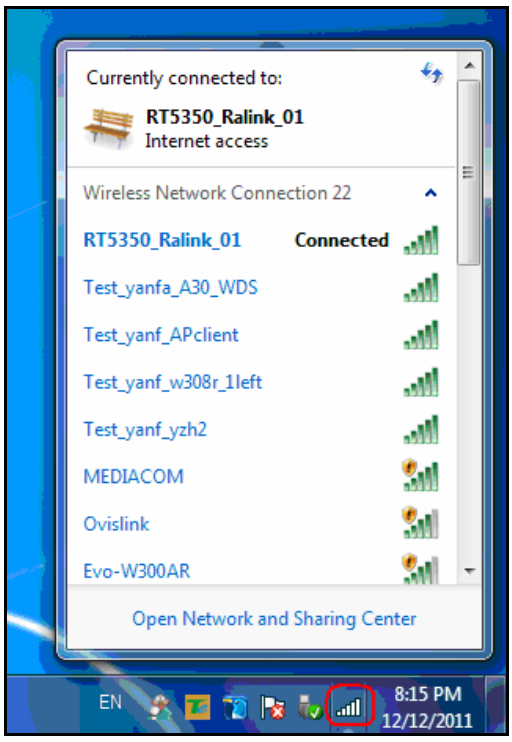
IP Address: 192.168.2.100

Subnet Mask: 255.255.255.0

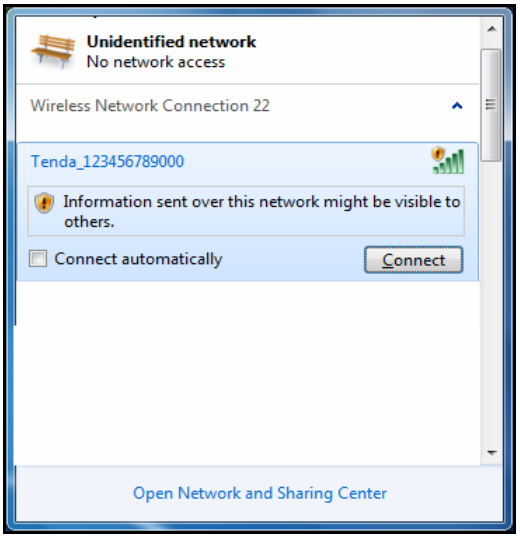
DNS Server: you can either enter your local DNS server addresses (Consult your ISP if you are not clear.) or use the device as a proxy DNS server.

After you finish all settings, click “OK” to submit and click the “OK” button for properties on Local Area Connection interface to save them.

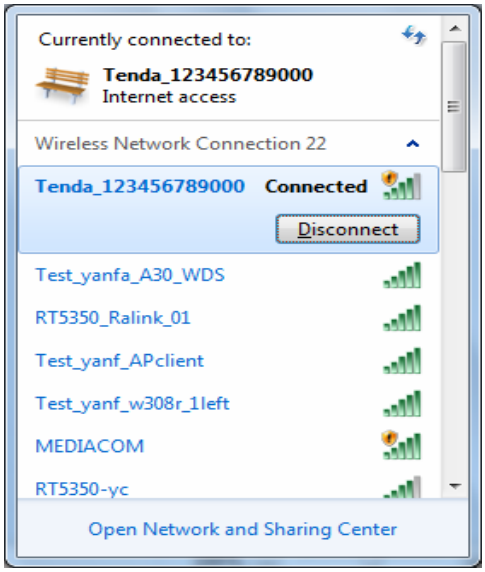
Step6. Click Network icon and then “Network and Internet Sharing Center”.



Step7. Select A5's SSID (wireless network name) and click "Connect".



Step8. When you see "Connected" displayed next to A5's SSID, you have successfully connected to A5 wirelessly.

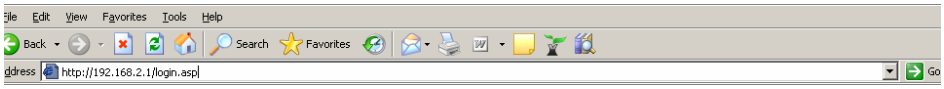


2.3 Quick Internet Connection Setup

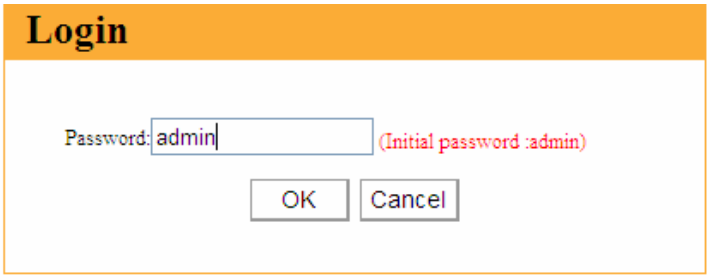
This section instructs you to setup Internet connection quickly. If you are trying to connect to your ISP via an Ethernet cable, refer to section 2.3.1 below for assistance; if you are trying a wireless Internet connection, skip to section 2.3.2.

2.3.1 Wired Internet Connection Setup

Step1. Open a web browser, enter http://192.168.2.1 in the address bar and then press “Enter”.



Step2. Input the default Password “admin” and click “OK” on the login window.



Step3. You will be redirected to the quick Internet connection setup screen below:

There are 2 Internet connection types on this screen: ADSL dialup (PPPoE) and Dynamic IP (DHCP).

PPPoE

Select PPPoE, if your ISP are using a PPPoE connection and enter PPPoE user name and password provided by your ISP. To secure your wireless network, you are recommended to setup a wireless security key on this interface. Then click the OK button to save your settings.

Dynamic IP

Keep this default option if your ISP does not give you any IP information or account information. You don’t need to configure any settings for this connection. However for the sake of security, we recommend you to setup a wireless security key on this

interface to protect your wireless network from undesired access.

Then click the OK button to save your settings.

⚠Note:

- Contact your ISP if you are not clear about the PPPoE user name and password.
- Skip to Chapter3 > WAN Settings, if you are using an Internet connection type other than the above- mentioned.

2.3.2 Wireless Internet Connection (WISP) Setup

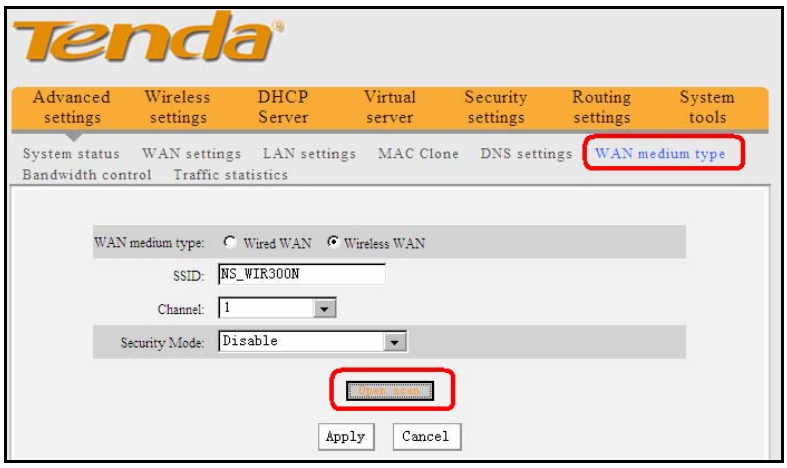
To set up your wireless WAN connection, do as follows:

Step1. Follow steps 1-3 on section 2.3.1 to enter the quick Internet setup interface.

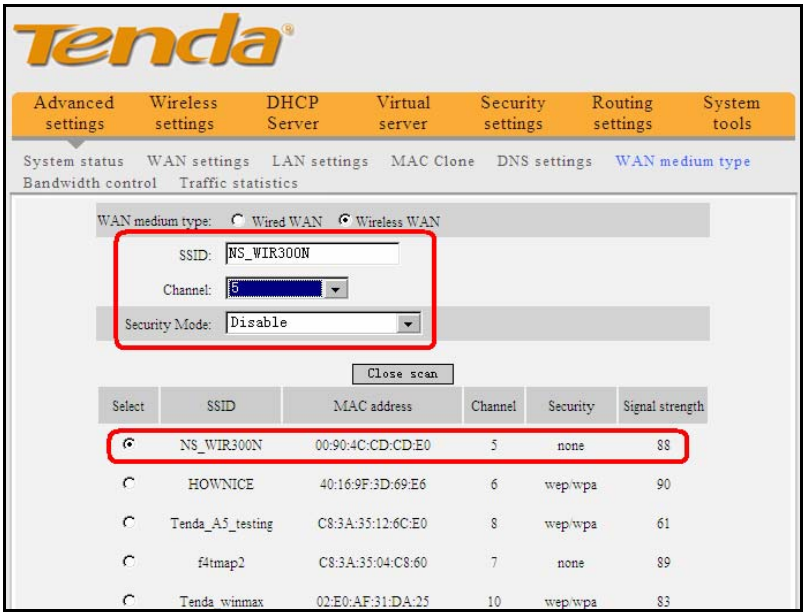
Step2. On the quick Internet setup interface, click “Advanced Settings” to enter WAN media setting interface.

Step3. Click “Open Scan” on the WAN Medium Type interface to

display all wireless networks within the range and select the one you want to connect to (your ISP's). System will populate the SSID and Channel fields automatically.



Step4. Configure wireless security settings if required (Select a security mode, cipher type and enter a security key; all of these settings must be exactly the same as your wireless ISP's. If you are not clear, contact your ISP for assistance).

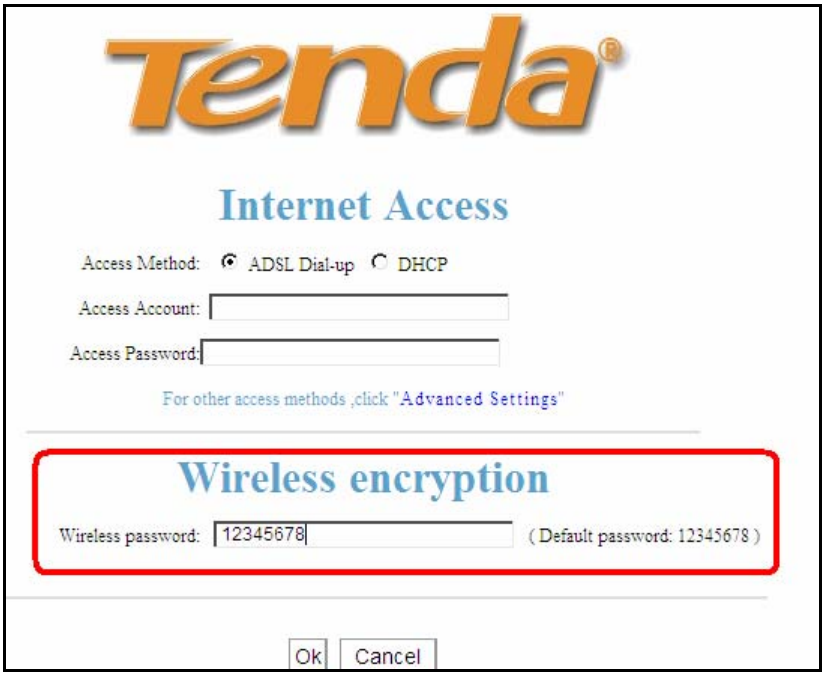


Step5. Enter WAN Settings interface and select your Internet connection type (For example, select Dynamic IP if your wireless ISP does not provide you any IP information.).

2.4 Quick Wireless Security Setup

There are 2 ways of setting up A5's wireless security: set it up on the Quick Internet Connection Setup interface below or set it up on the Wireless Security Interface under Wireless Settings menu. Here we only present the former, for the latter, please refer to section 5.2 hereof.

By default, A5 is preset to WPA-PSK and AES. The security key allows 8 characters only. Enter your key on the interface below to secure your wireless network.

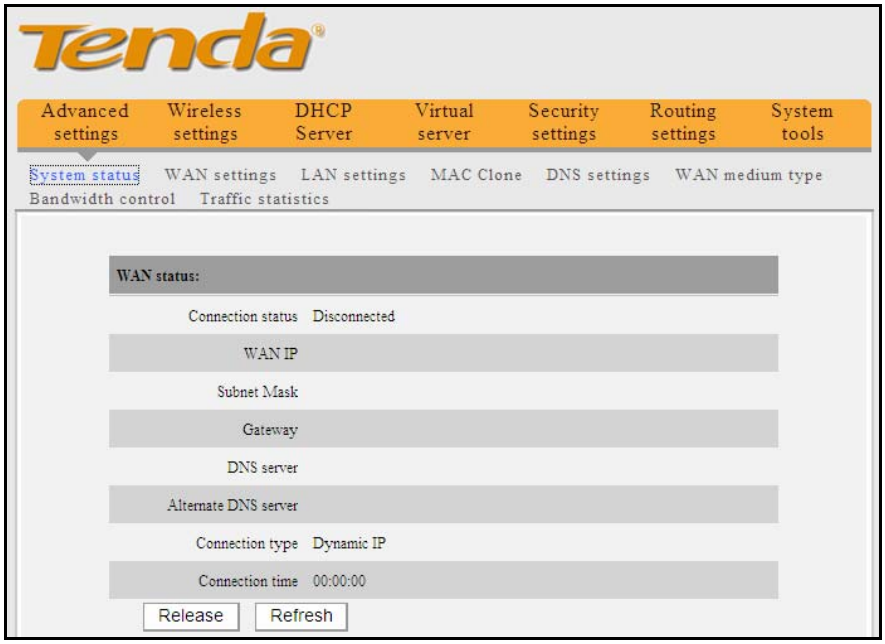


Chapter 3 Configuration

3.1 Advanced Settings

3.1.1 System Status

This section allows you to view WAN information and device information.



Connection Status: Displays WAN connection status: Disconnected, Connecting and Connected.

Disconnected: Indicates that the Ethernet cable from your ISP side is not / not correctly connected to the WAN port on A5 or A5 is not logically connected to your ISP.

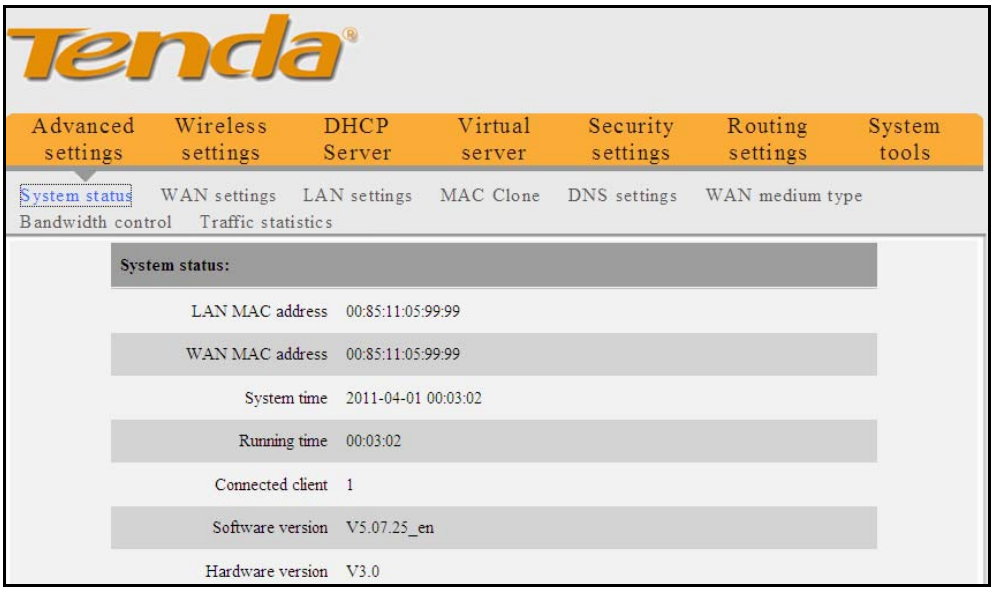
Connecting: Indicates that the WAN port is correctly connected and is requesting an IP address from your ISP.

Connected: Indicates that A5 has been connected to your ISP.

- **WAN IP**：Displays WAN IP address.
- **Subnet Mask:** Displays WAN subnet mask.
- **Gateway:** Displays WAN gateway address.
- **Primary DNS:** Displays WAN primary DNS address.
- **Secondary DNS:** Displays WAN secondary DNS address.

- Displays current Internet connection type.

System Status:



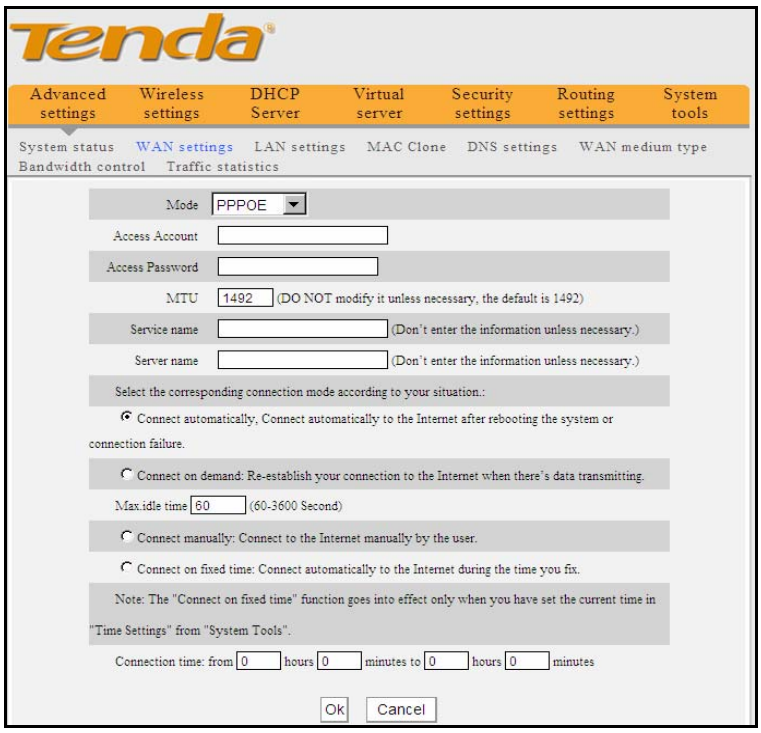
- **LAN MAC Address:** Displays router's LAN MAC address.
- **WAN MAC Address:** Displays router's WAN MAC address.
- **System Time:** Displays the time when system is updated.
- **Connected client**：Displays the number of connected computers (which obtains IP addresses from the device' DHCP server).
- **Software Version**：Displays router's firmware version.
- **Hardware Version:** Displays router's hardware version.

3.1.2 WAN Settings

There are **5** Internet connection types available for your selection: PPPoE, Static IP，Dynamic IP，PPTP and **L2TP**. Select your Internet connection type and follow corresponding instructions below:

PPPoE

Select PPPoE, if your ISP are using a PPPoE connection and provide you with PPPoE user name and password information.



- **Mode:** Displays current Internet connection type.
- **Access Account:** Enter the user name provided by your ISP.
- **Access Password:** Enter the password provided by your ISP.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1492 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 necessary.
- **Server Name:** Description of server. Leave blank unless necessary.
- **Connect Automatically:** Connects automatically to the Internet upon device startup or disconnection from the Internet.
- **Connect Manually:** Users need to connect the device to

Internet manually upon disconnection from the Internet.

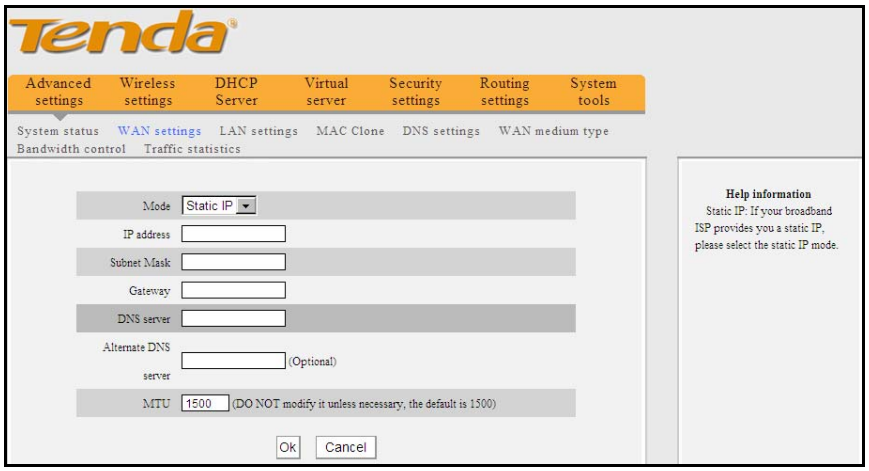
- **Connect on Demand:** Connects to Internet automatically upon traffic present.
- **Connect on Fixed Time:** Connects to Internet automatically within the specified time length.

⚠Note:

To activate the “Connect on Fixed Time" feature, you must first configure current time on the "Time Settings” screen under "System Tools" menu.

Static IP

If your ISP offer you static IP Internet connection type, select “Static IP" from Mode drop-down menu and then enter IP address, subnet mask, Primary DNS and secondary DNS information provided by your ISP into corresponding fields.

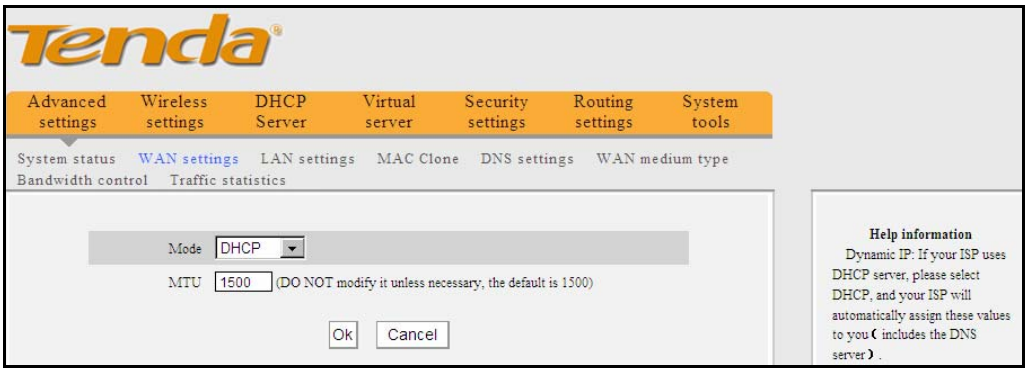


- **Mode:** Displays the current Internet connection type.
- **IP Address:** Enter the WAN IP address provided by your ISP. Inquire your ISP if you are not clear.
- **Subnet Mask:** Enter WAN Subnet Mask provided by your ISP. The default is 255.255.255.0.

- **Gateway:** Enter the WAN Gateway provided by your ISP.
- **DNS Server:** Enter the necessary DNS address provided by your ISP.
- **Alternate DNS Server:** Enter the secondary DNS address if your ISP provides, and it is optional.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1500 unless necessary. You may need to change it for optimal performance with some specific websites or application software that cannot be opened or enabled.

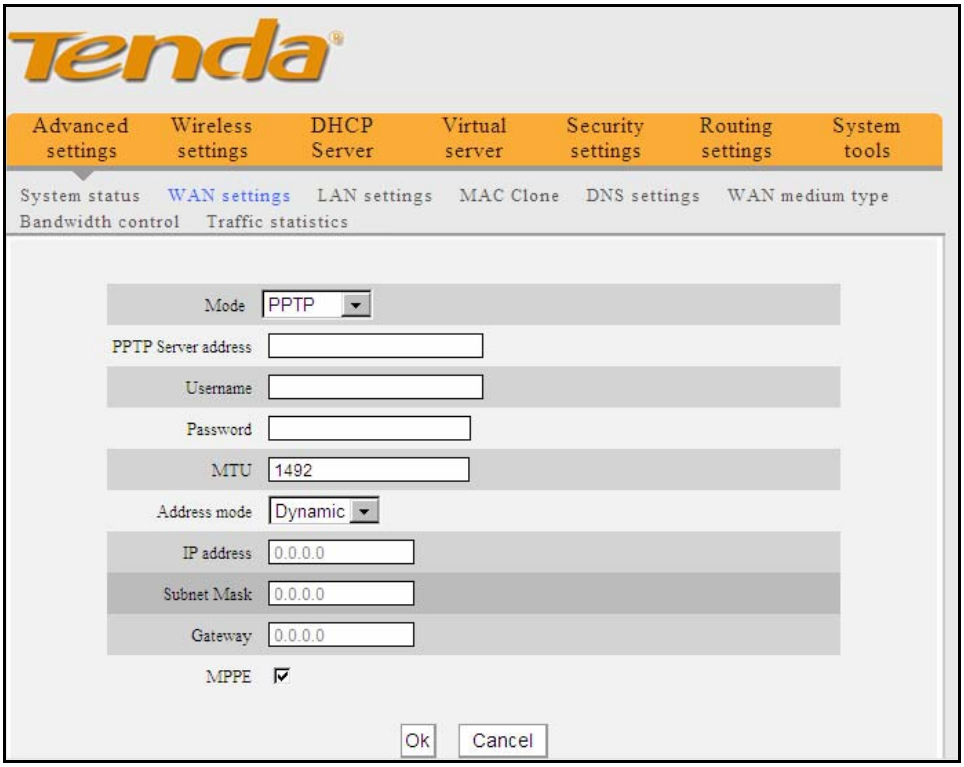
Dynamic IP (DHCP)

Select this option if your ISP does not give you any IP information or account information. You don't need to configure any settings for this connection.



- **Mode:** Displays the current Internet connection type.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1500 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.

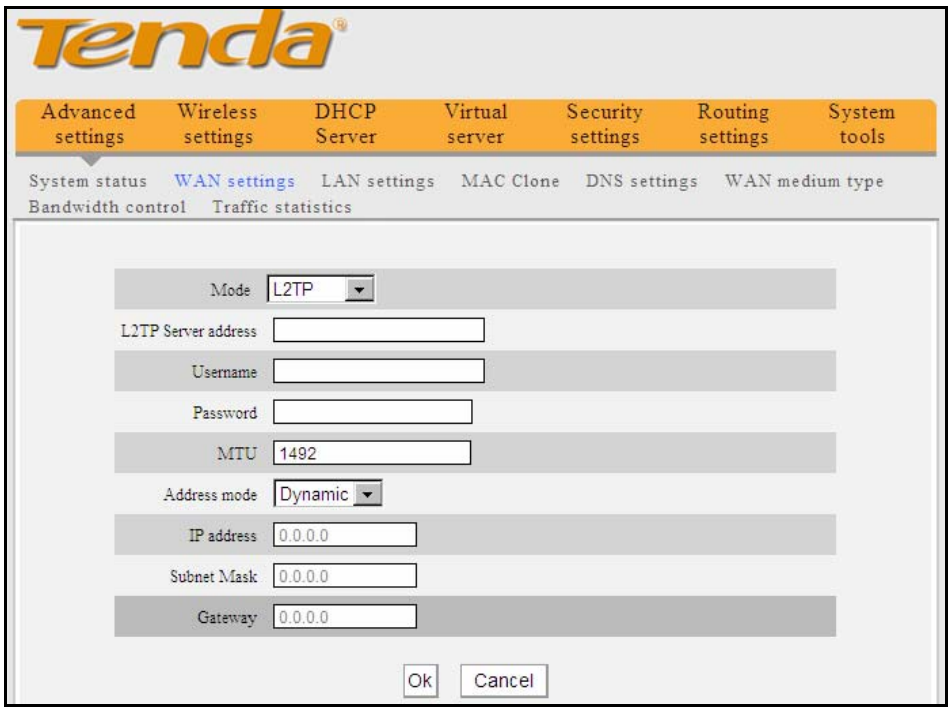
PPTP



- **Mode:** Displays the current Internet connection type.
- **PPTP server address:** Enter the IP address of a PPTP server.
- **Username/Password:** Enter Username/Password specified by the PPTP server.
- **MTU:** Maximum Transmission Unit. DO NOT change it from the factory default of 1492 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.
- **Address mode:** Select “Dynamic” if you don’t get any IP information from the PPTP server, otherwise select “Static”.
- **IP address:** Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).
- **Subnet mask:** Enter the subnet mask provided by your ISP, normally, 255.255.255.0 (Static IP address mode only).
- **Gateway:** Enter the gateway provided by your ISP (Static IP

address mode only). Inquire your local ISP if you are not clear.

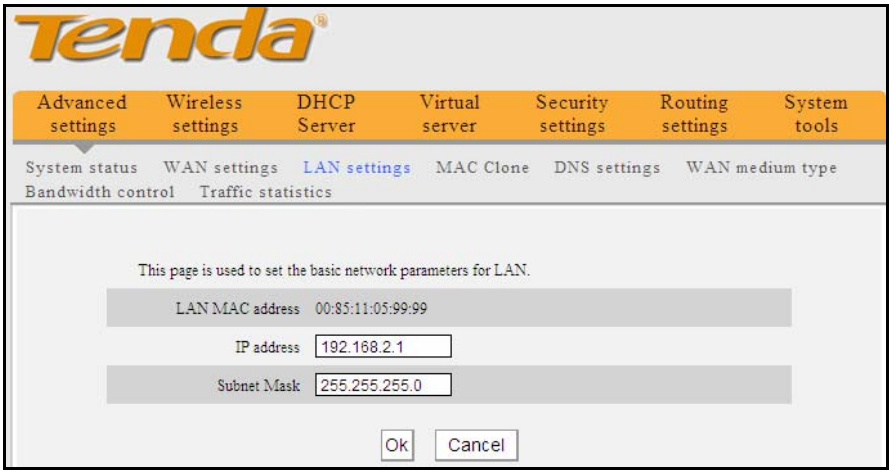
L2TP



- **Mode:** Displays the current Internet connection type.
- **L2TP server address:** Enter the IP address of a L2TP server.
- **Username/Password:** Enter Username/Password specified by the PPTP server.
- **Address mode:** Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).
- **IP address:** Enter the IP address information provided by your ISP (PPTP server). Inquire your local ISP if you are not clear (Static IP address mode only).
- **Subnet mask:** Enter the subnet mask provided by your ISP, normally, 255.255.255.0 (Static IP address mode only).
- **Gateway:** Enter the gateway provided by your ISP (Static IP address mode only). Inquire your local ISP if you are not clear.

3.1.3 LAN Settings

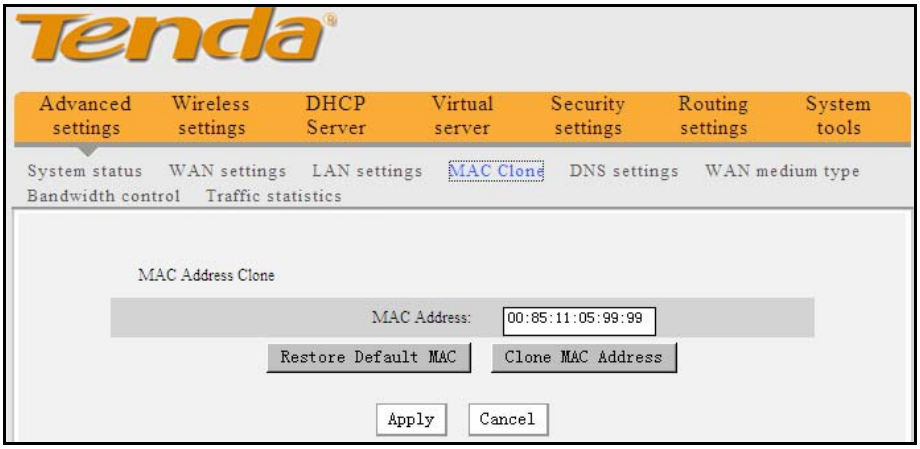
Click “Advanced Settings”----“LAN Settings” to enter the interface below.



- **LAN MAC Address:** Displays the router’s LAN MAC address, which cannot be changed.
- **IP Address:** The default LAN IP address for this router is 192.168.2.1. You can change it according to your need.
- **Subnet Mask:** Enter the Router’s LAN subnet mask. The default value is 255.255.255.0.

3.1.4 MAC Address Clone

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



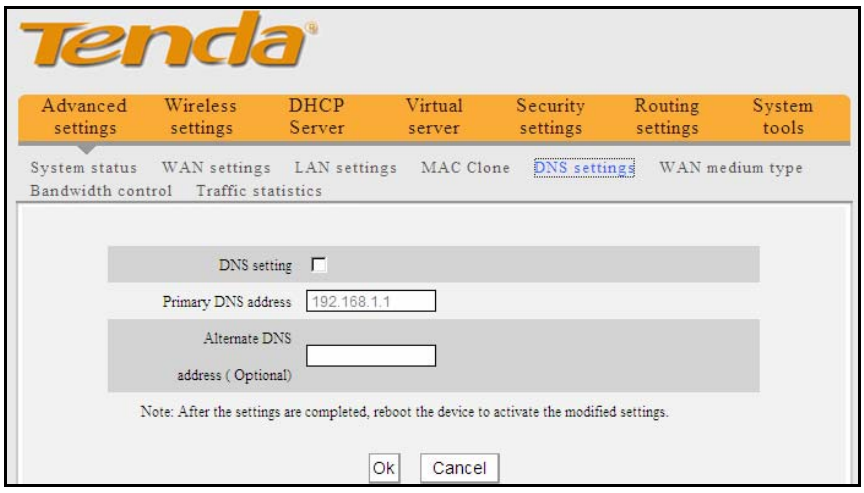
Some ISP may require binding an accepted MAC address for communication. If the bound MAC address differs from your router’s predefined WAN MAC address, then you need to replace

the router's WAN MAC with the bound MAC for achieving valid communication with your ISP.

- **Clone MAC Address**: Clicking this button changes router's WAN MAC address from default to the MAC address of the PC you are currently on. Don't use this button unless your PC's MAC address is the one bound by your ISP.
- **Restore Default MAC:** Restores router's WAN MAC to default settings.

3.1.5 DNS Settings

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It functions just as the "phone book" for the Internet by translating human-friendly domain names into numerical identifiers of IP addresses for the purpose of locating and addressing these devices worldwide.



- **DNS Setting:** Check the box to enable DNS settings.
- **Primary DNS address:** Enter the DNS server address provided by your ISP.
- **Alternate DNS Address:** Enter the secondary DNS address

if your ISP offers you 2 DNS addresses (Optional).

⚠**Note:**

1. Wrong DNS server addresses will lead to failure in accessing websites.

2. To activate the new settings, reboot the device.

3.1.6 WAN Medium Type

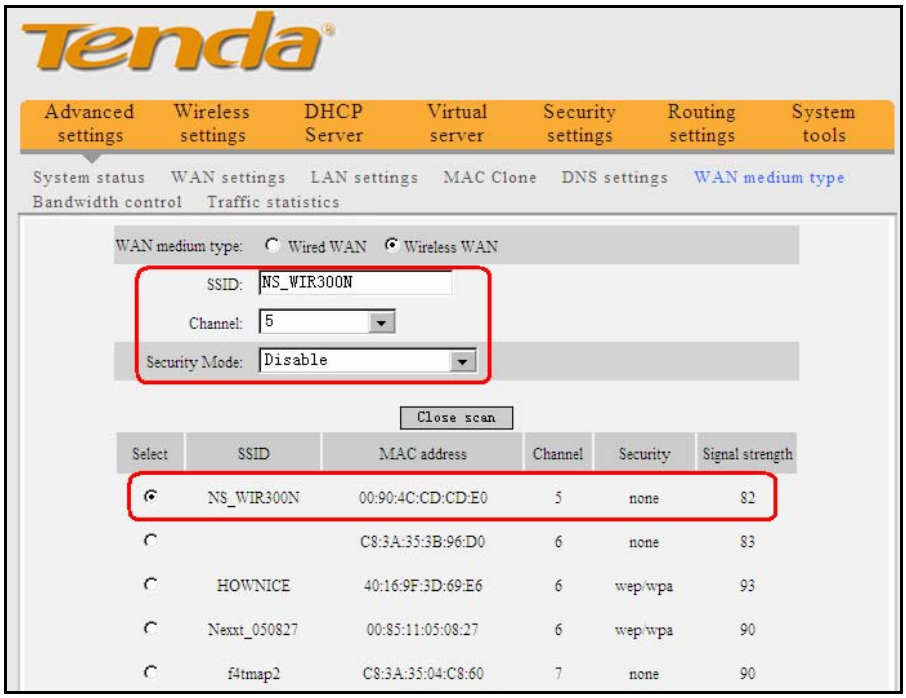
The A5 supports 2 types of WAN media: wired WAN (via Ethernet cable) and wireless WAN (WISP). By default, it is preset to wired WAN.

- **Wired WAN:** Select this mode if you are using an Ethernet cable from your ISP to connect to the router's WAN port.
- **Wireless WAN:** Use this mode if your ISP provides you wireless Internet connection service or you want to amplify wireless signal.
- **SSID：** SSID (Service Set Identifier). Enter your ISP's SSID. You can also enable "Open Scan" to obtain a list of available ISP SSIDs and then select your ISP's SSID to let system populate the SSID field automatically.
- **Channel:** Select a channel that corresponds to the ISP's SSID you select. You can view it in a scanned SSID list if you

enable the “Scan” function.

- **Security Mode:** Configure the same settings on your router as those on your ISP’s side for wireless security.

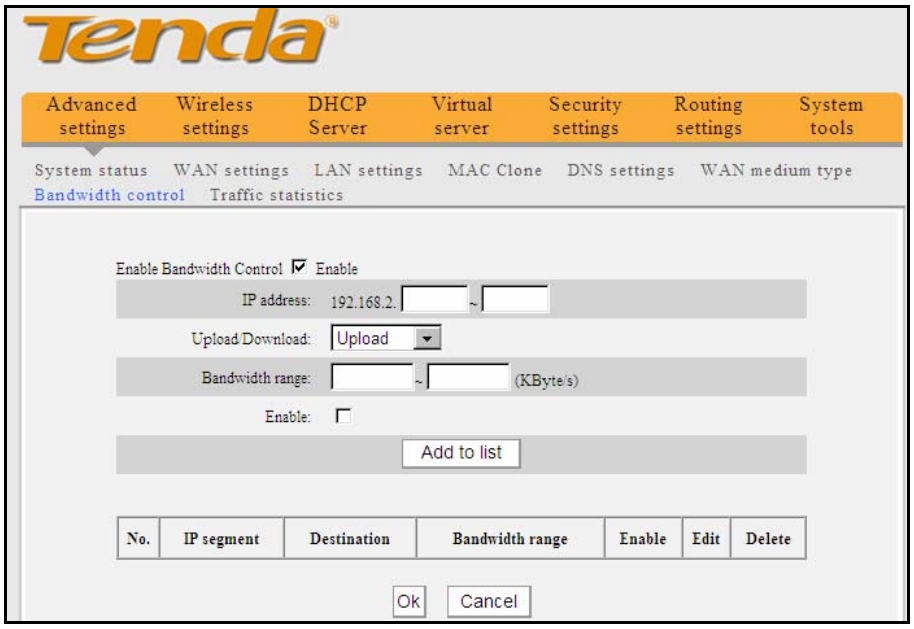
For example: If your ISP’s SSID is “NS_WIR300N” and channel is 1, then enter “NS_WIR300N” in the SSID box and select 1 from the channel drop-down menu; or you can let system automatically populate the SSID field and select the right channel by selecting your ISP’s SSID from the scan list provided that you enabled the “Open Scan” function on the interface below. You must configure the same settings on your router as those on your ISP’s side for wireless security to achieve successful connection. Save the settings on this interface and go to WAN Settings to select your Internet connection type (for example, if your ISP is using a dynamic IP connection on its wireless device, then you need to select DHCP/Dynamic IP.).



3.1.7 Bandwidth Control

Bandwidth control can be used to simultaneously regulate

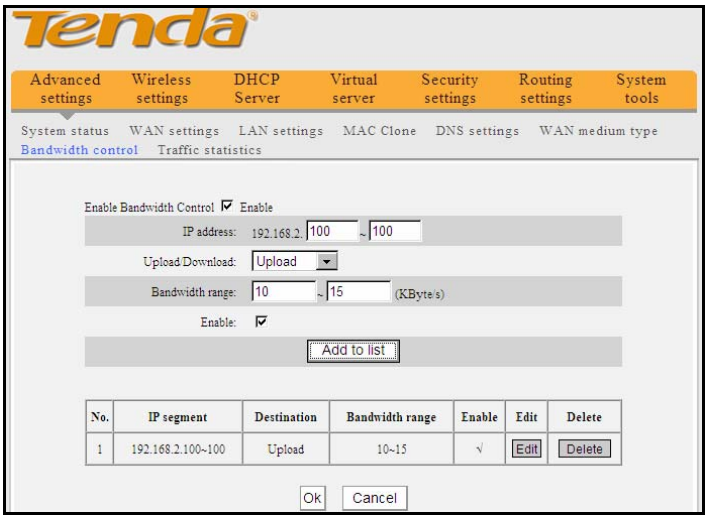
traffic of up to 254 computers on your LAN network. You can regulate a group of PCs' traffic by specifying a range of IP addresses.



- **Enable Bandwidth Control**：Check the box to enable bandwidth control.
- **IP Address**：Enter an IP address (same number in both boxes) or a range of IP addresses (different numbers in two boxes) of the PCs whose traffic you want to regulate.
- **Upload /Download**：**You can** select either to limit Uplink or Downlink Bandwidth of PCs within a specified IP range.
- **Bandwidth Range**：Maximum and minimum data flow which is permitted to be uploaded/downloaded by computers within a specified IP range. Unit is Kbytes/s. (For WAN bandwidth range, consult your ISP.)
- **Enable:** Check the box to enable edit. Leaving it unchecked means disabling the function.
- **Add to List:** Click it to add currently edited bandwidth control rule to the list when finishing.

1. For example: Suppose that you have a 2M WAN connection, then maximum download and upload rates in theory will be 2Mbps=256KByte/s and 512kbps=64KByte/s. And you want the PC at the IP address of 192.168.2.100 to have 10-15KByte/s upload and 80-90KByte/s download rates. Then follow instructions below:

First, add an upload rule as shown in the figure below:



Step1. Enter 192.168.2.100 in IP address boxes.

Step2. Select Upload from the corresponding drop-down menu.

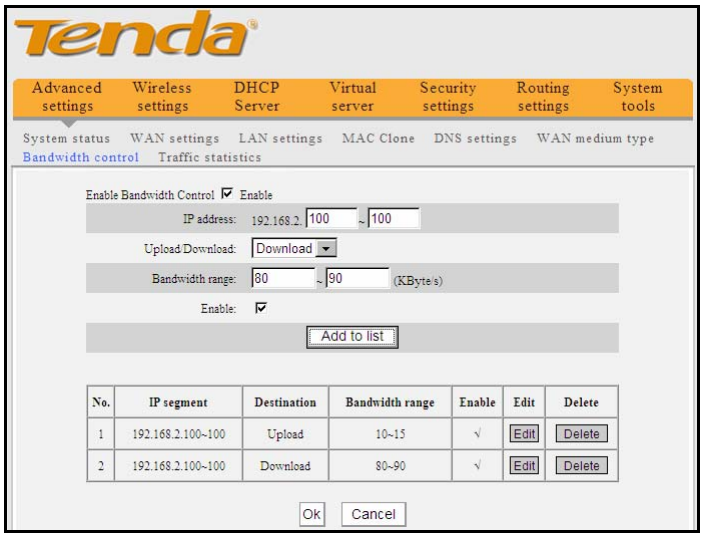
Step3. Enter 10~15 in bandwidth range box

Step4. Check the “Enable” box.

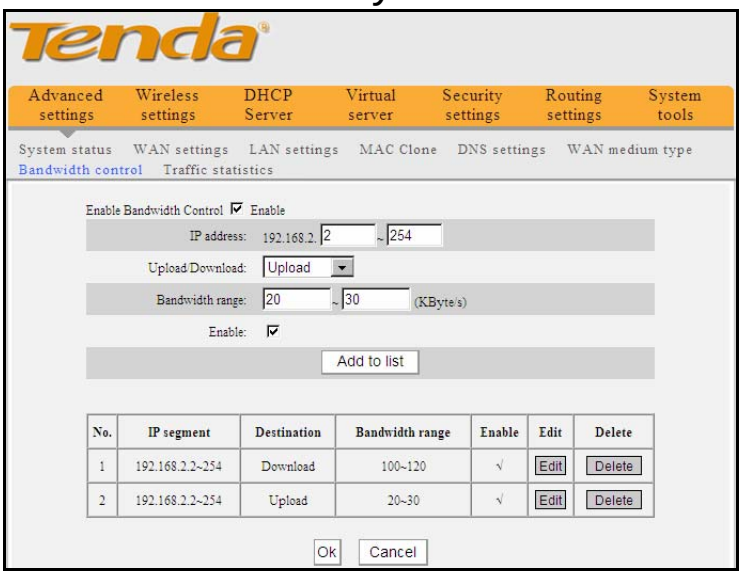
Step5. Click “Add to List”.

Step6. Click “OK” to finish settings.

Then, follow steps above to add a download rule.

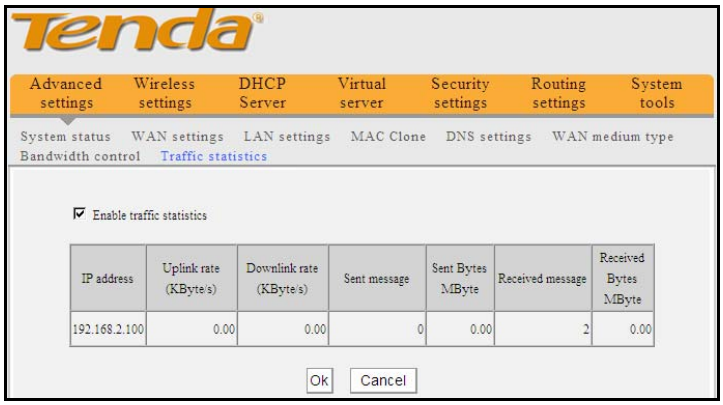


2. For example, supposing that you want PCs within the IP range of 192.168.2.2--192.168.2.254 to have 100-120KByte/s download rate and 20-30KByte/s upload rate, then repeat same settings shown on the below interface on your router:



3.1.8 Statistics

Statistics dynamically displays bandwidth usage by PCs on your LAN.

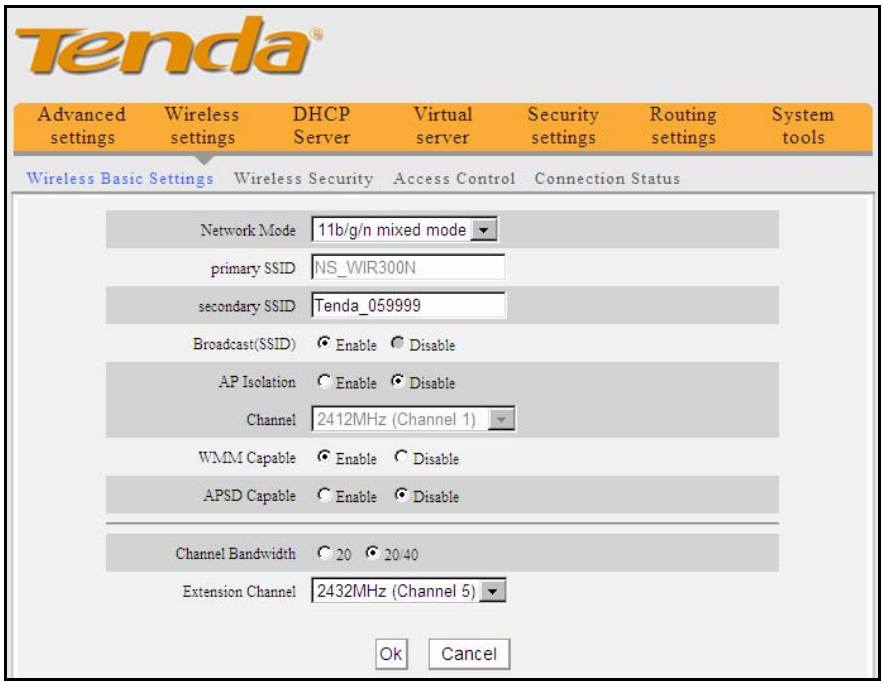


- **Enable Traffic** Statistics**:** Check the box to gather bandwidth usage by PCs on your LAN. It is disabled by default. Disabling this option may boost router's packet handling capacity. When enabled, system will dynamically renew statistics information every 5 minutes.
- **IP Address:** Displays IP address information of a corresponding statistics item.

- **Uplink Rate:** Displays the amount of packets transmitted per second in KByte/s.
- **Downlink Rate:** Displays the amount of packets received per second in KByte/s.
- **Sent Message (TX Packets):** Displays the total amount of packets transmitted by a corresponding IP address through the router.
- **Sent Bytes:** Displays the total amount of bytes transmitted by a corresponding IP address through the router. The unit is MByte.
- **Received Message (RX Packets):** Displays the total amount of packets received by a corresponding IP address from the router.
- **Recieved Bytes:** Displays the total amount of bytes received by a corresponding IP address from the router. The unit is MByte.

3.2 Wireless Settings

3.2.1 Basic Settings



- **Network Mode:** Select a right mode according to your wireless client. The default mode is 11b/g/n mixed.
- **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.
- **Broadcast (SSID):** Select “Disable” to hide your SSID. With this option disabled, no wireless clients will be able to see your wireless network when they perform a scan to see what’s available. If they want to connect to your router, they will have to first know this SSID and then manually enter it on their devices. By default, this option is enabled.
- **Channel:** The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. From the drop-down list，you can select a most effective channel, which ranges from 1 to 11. You can also select “Auto Select” to let system detect and choose one that best fits your network.
- **WMM-Capable**：Enabling this option may boost transmission capacity of wireless multimedia data (such as online video play).
- **ASPD Capable**：Auto power saving mode, disabled by default.
- **Channel Bandwidth:** Select a proper channel bandwidth to

enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 20/40M 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.

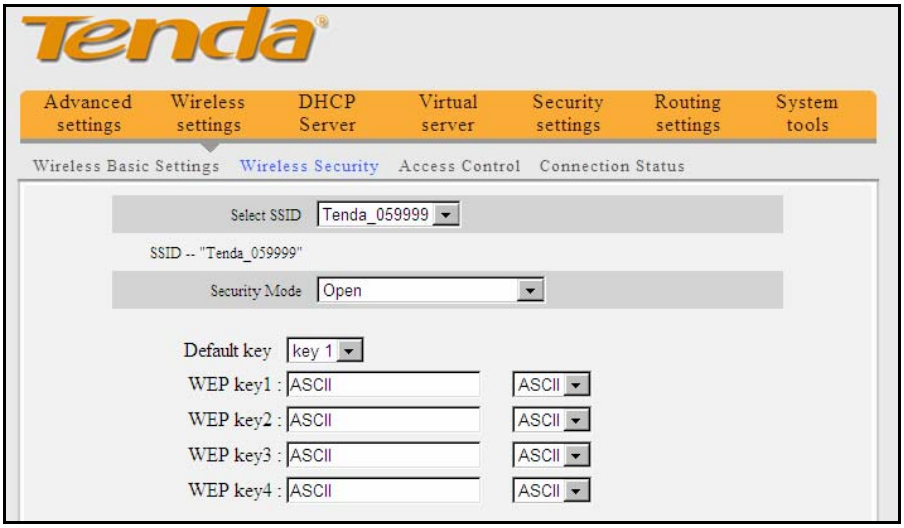
- **Extension Channel**：Indicates the working network frequency range for 11n mode.

3.2.2 Wireless Security

This section allows you to configure wireless encryption to block unauthorized access to your wireless network and prevent malicious packet sniffing. You have 3 ways to encrypt your data: WEP, WPA-PSK and WPA2-PSK.

1. WEP (Wired Equivalent Privacy)

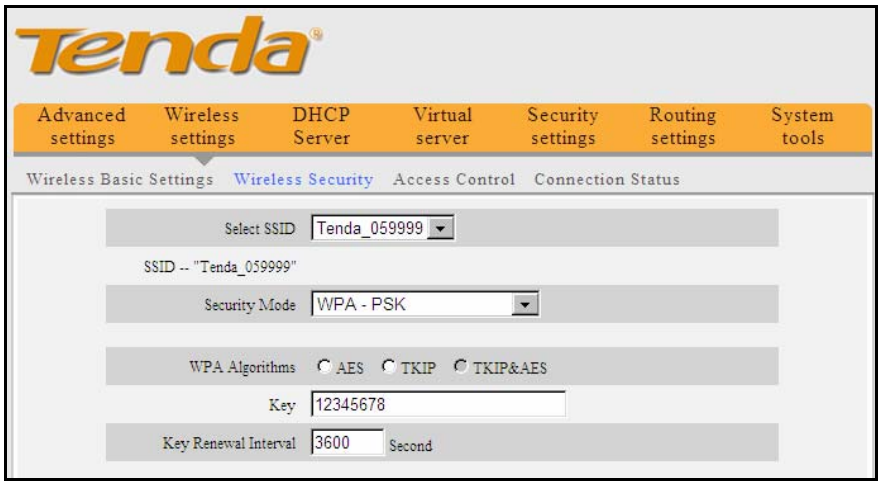
WEP is intended to provide data confidentiality comparable to that of a traditional wired network. Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.



- **Select SSID:** Select a SSID that you want to encrypt. Both SSIDs can be encrypted respectively.
- **Security Mode:** Select a proper mode from the drop-down menu.
- **Default Key:** Select one key from the 4 preset keys.

2、 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.



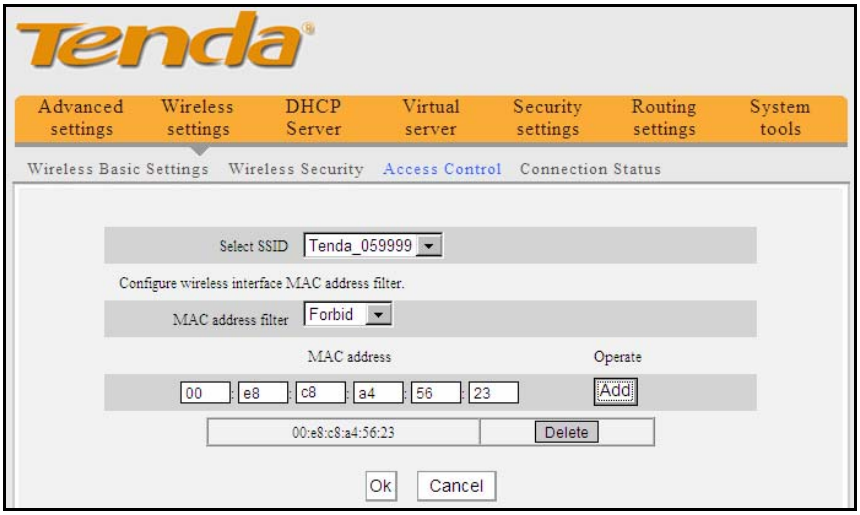
- **Security Mode:** Select a proper mode that is also supported by your wireless clients.
- **WPA Algorithms:** Select either AES (advanced encryption standard) or TKIP (temporary key integrity protocol) type.
- **Key:** Enter a security key，which must be between 8-63 ASCII characters.
- **Key Renewal Interval:** Set a valid period for the security key.

3、WPA2-PSK

3.2 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.

3.2.3 MAC-based 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 Address Filter:** “Permit” means to permit PCs at specified MAC addresses to connect to your wireless network while “Forbid” means to block PCs at specified MAC addresses from connecting to your wireless network.
- **MAC Address：** Enter the MAC addresses of a wireless client and click “Add”.
- **MAC Address List:** Displays the MAC addresses added by you. You can delete any entry by clicking on the “Delete” button next to it.

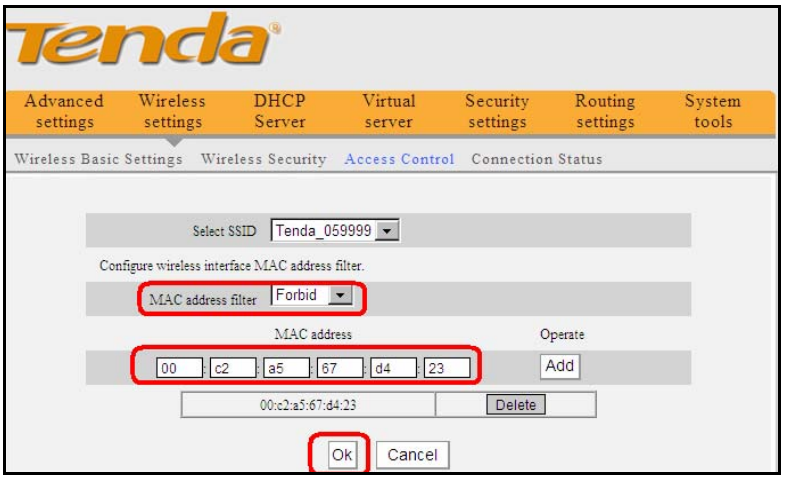
Example 1:

To allow only a PC at the MAC address of 00:e8:c8:a4:56:75 to connect to your wireless network, do as follows:

Step1. Select “Permit” from MAC Address Filter drop-down menu.
Step2. Enter 00:e8:c8:a4:56:75 in the MAC address box.
Step3. Click the “OK” button to save your settings and you can add more MAC addresses, if you like, simply repeating the above steps.

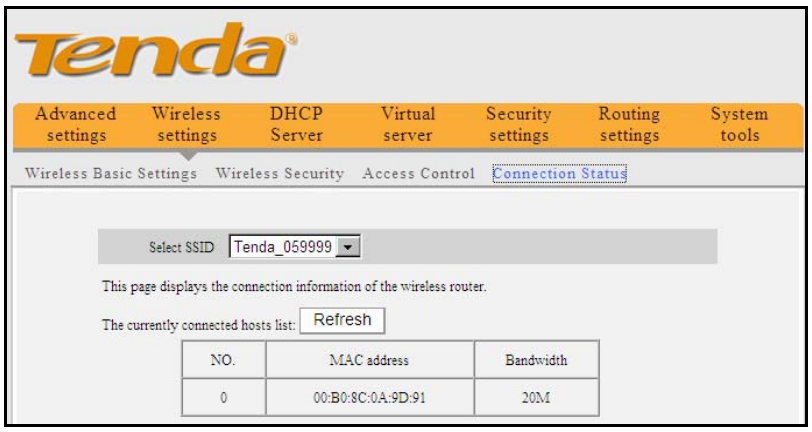
Example 2:

To prohibit only a PC at the MAC address of 00:c2:a5:67:d4:23 from connecting to your wireless network, do as follows:



3.2.4 Connection Status

This interface displays the information of currently connected wireless clients including MAC addresses and bandwidth.



MAC Address: Displays the MAC addresses of the PCs that have been wirelessly connected to your router.

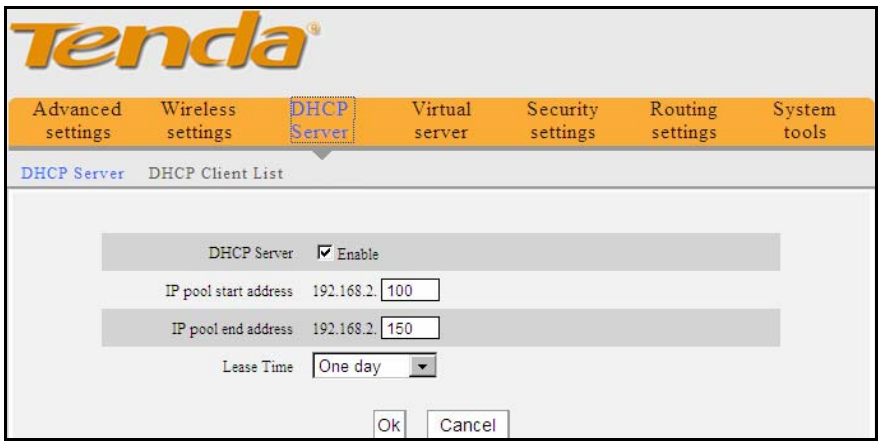
Bandwidth: Displays the channel channel bandwidth used by the currently connected hosts (connected wireless clients).

Note:"Bandwidth" refers to the wireless channel bandwidth instead of wireless connection rate.

3.3 DHCP

3.3.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on A5, it will automatically configure the parameters of TCP/IP protocol for all your LAN computers (including IP address, subnet mask, gateway and DNS etc), eliminating the need for manual intervention. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically”. When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the A5.



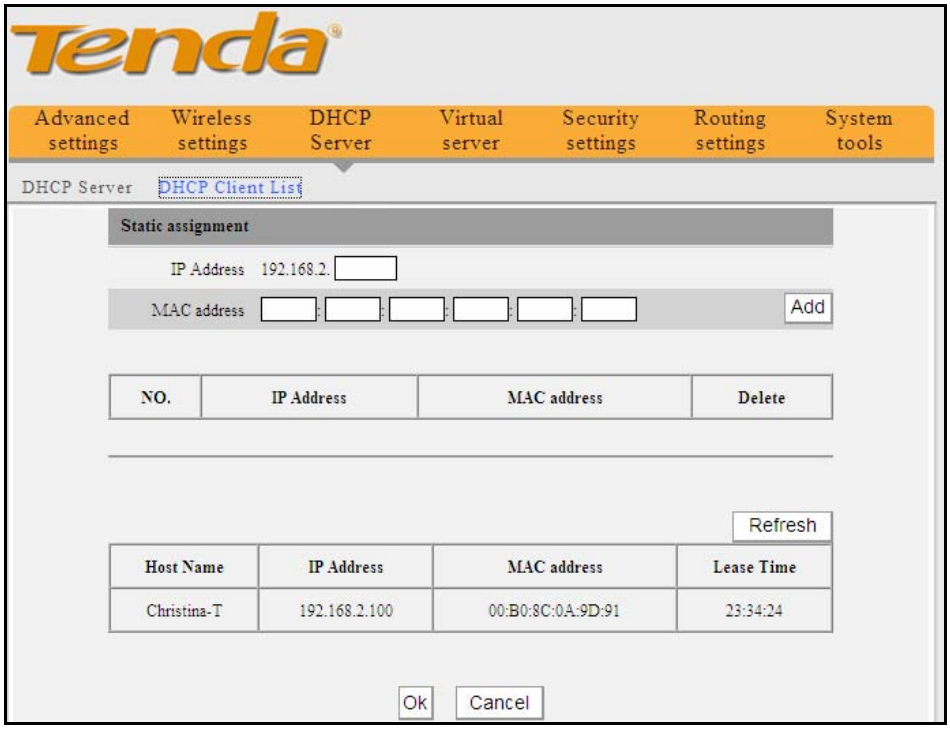
- **DHCP Server:** Check or uncheck the box to Enable or disable the device's DHCP server feature.
- **IP pool start address:** Enter the starting IP address for the DHCP server's IP assignment.
- **IP pool end address:** Enter the ending IP address for the DHCP server's IP assignment.
- **Lease Time:** 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.

3.3.2 DHCP Clients

This section not only displays a DHCP dynamic client list but also includes a configurable Static DHCP assignment feature.

The DHCP client list displays the obtained IP addresses from A5's built-in DHCP server, MAC addresses, host names and lease time. If you would like some devices on your network to always have fixed IP addresses, you can manually add a static DHCP assignment entry for each such device. You can manually add an IP address and a MAC address and check the IP-MAC Binding option, and then whenever a host with this MAC address connects to the router, it will always get the same IP address (the one you

just added). According to the connected computer's MAC address, the router checks relevant entries in its DHCP reservation list and decides what IP address to assign to this host (an unused IP from DHCP IP address pool, or a reserved one): If it fails in finding a reserved IP address bound to the PC with this MAC address in the list, it will immediately assign an unused IP from its DHCP IP address pool; and if such IP is found, it will be assigned to this host so as to ensure that host with a DHCP reservation always get this fixed reserved IP address. Once a host registers DHCP reservation to have a fixed IP address bound to its MAC address, it can not use a different IP address except this one to connect to the router for Internet access. Thus, due to DHCP reservation, a host is prevented from escaping monitoring by changing its IP address.



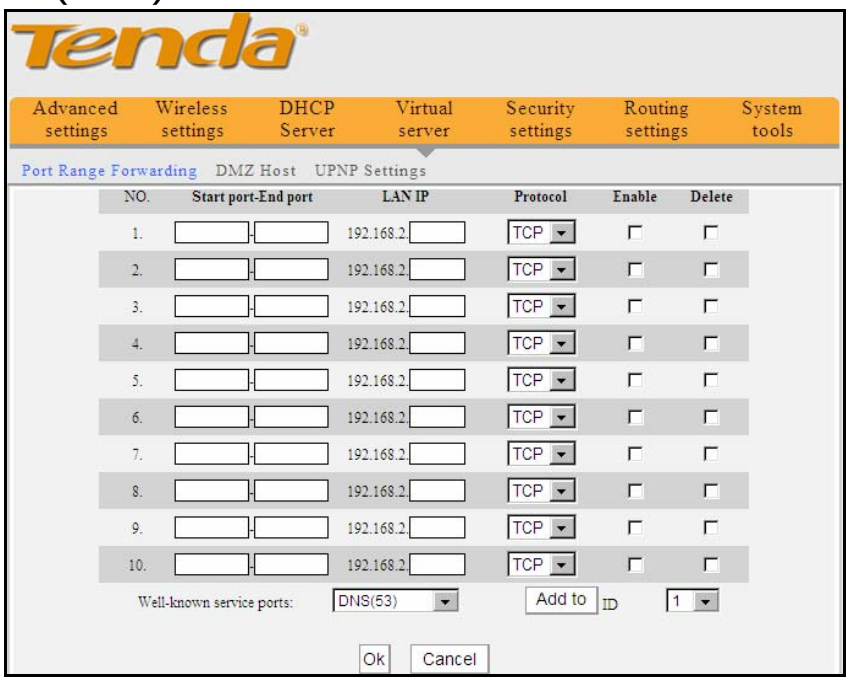
- **IP Address:** Enter the IP address which needs static binding.
- **MAC Address:** Enter the MAC address of the computer you want to bind.

- **Host name:** It displays the name of the bound computer.
- **Lease Time:** The remaining time for the corresponding IP address lease.

3.4 Virtual Server

3.4.1 Port Range Forwarding

Port Range forwarding feature allows you to open a single or a range of WAN service ports and redirect all traffic received through these ports to a LAN server with a designated IP address. It allows remote computers, such as computers on the Internet, to connect to a specific computer or service within a private local area network (LAN).



- **Start/End Port:** Enter the service port range provided by the mapped host in internal network.
- **LAN IP:** The IP address of the computer which is used as a server in LAN.
- **Protocol:** Includes TCP, UDP and Both. Select “Both” when

you are not sure about which protocol to use.

- **Enable:** Check the “Enable” option to activate the corresponding rule next to it.
- **Delete:** Check the “Delete” option to delete the corresponding rule next to it.
- **Well-Known Service Ports:** The “Well-Known Service Port” provides commonly used protocol ports. Select one from them and then click the “Add to” button to automatically add selected port to the Start Port-End Port fields of the corresponding rule ID. You can also manually add the ports which are not included in the “Well-Known Service Port”.
- **Add to:** Add a selected Well-Known Service Port to the Start Port-End Port boxes of the rule you select.

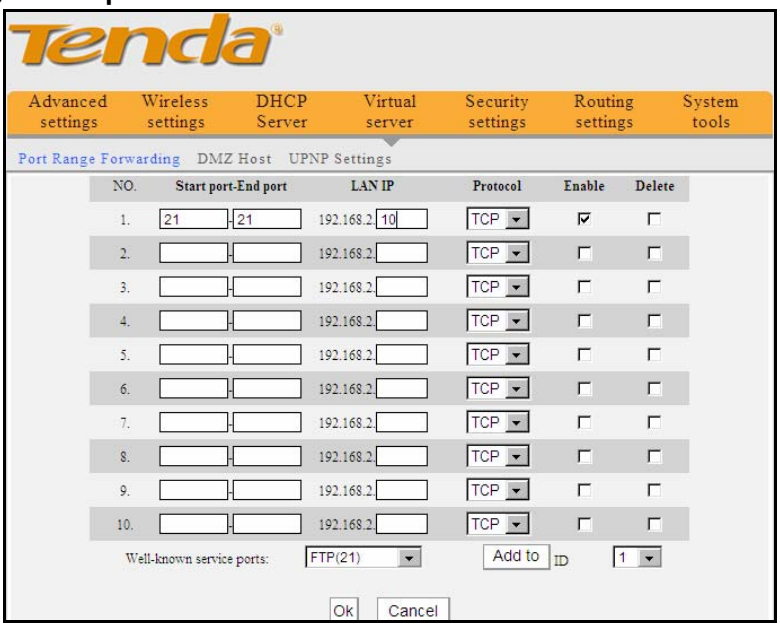
For example:

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. Then, you can set up your own PC as a FTP server and use the port range forwarding feature to let your friends access these files. Provided that the static IP address of the FTP server (Namely, your PC) is 192.168.2.10 and you want your friends to access this FTP server through default port 21 and TCP protocol, then you can follow the steps below for configurations.

1. Enter 21 for both the start and end port in ID 1, or select "FTP" from “Well-Known Service Port” and port 21 will be added automatically to ID 1.

2. Enter 192.168.2.10 for the "IP Address", select "TCP" and then select "Enable'.

3. The configured parameters are shown in the screen below.

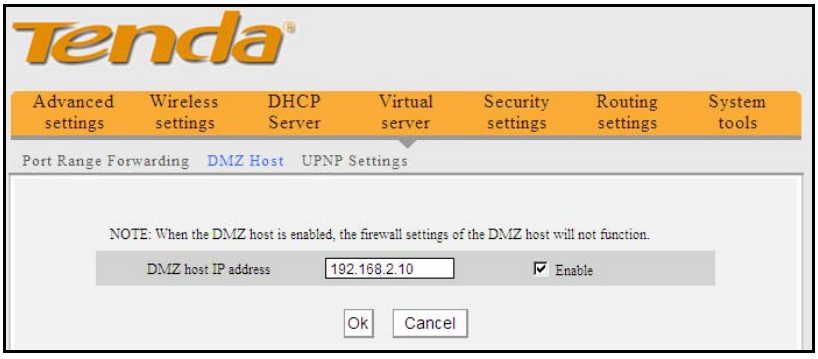


4. Click "OK".

Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the device's WAN IP address. For example, if it is 172.16.102.89, then your friends only need to enter "ftp://172.16.102.89：21" in address fields of their respective browsers.

3.4.2 DMZ Settings

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



➢ **DMZ Host IP Address:** Enter the IP address of a LAN

computer which you want to set to a DMZ host.

- **Enable:** Check/uncheck to enable/disable the DMZ host.

For example:

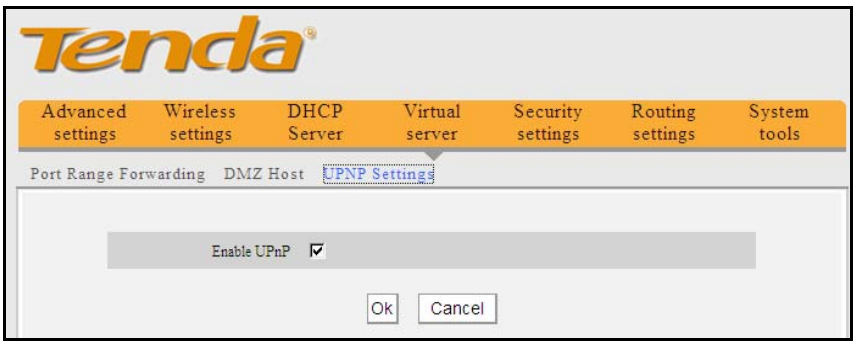
You can set a LAN computer at the IP address of 192.168.2.10 as a DMZ Host to intercommunicate with another host on the Internet.

NOTE:

If you set a PC to a DMZ host, it will be completely exposed to extranet and gains no more protection from the device firewall.

3.4.3 UPnP Settings

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



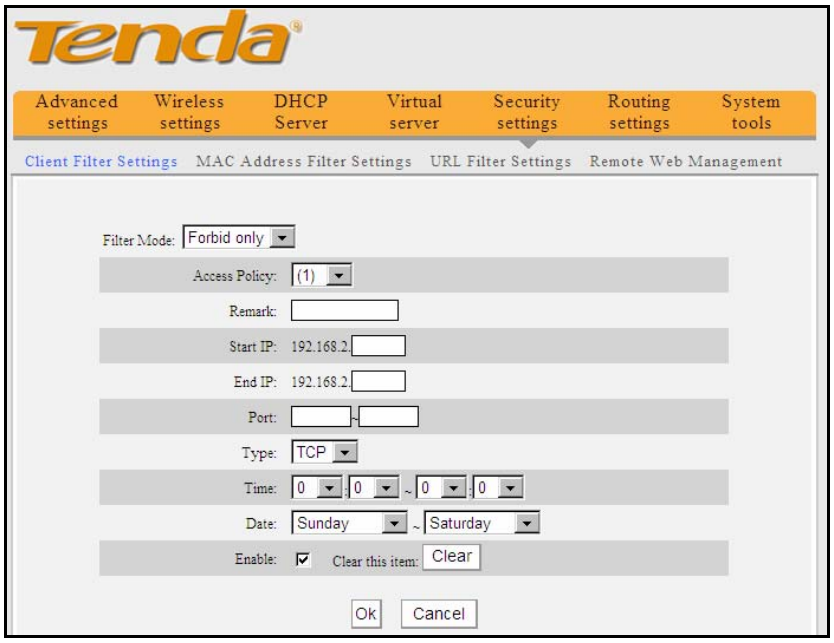
- **Enable UPnP:** Check/uncheck to enable/disable the UPnP.

Note: UPnP works in Windows XP, Windows ME or later operational systems (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.

3.5 Security Settings

3.5.1 Client Filter

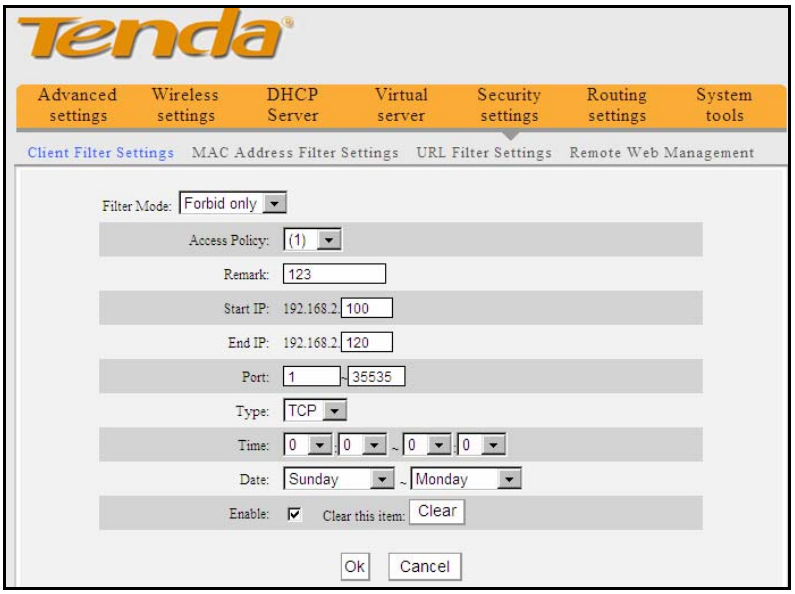
To better manage the computers in LAN, you can regulate LAN computers' access to some ports on Internet through using Client Filter functionality.



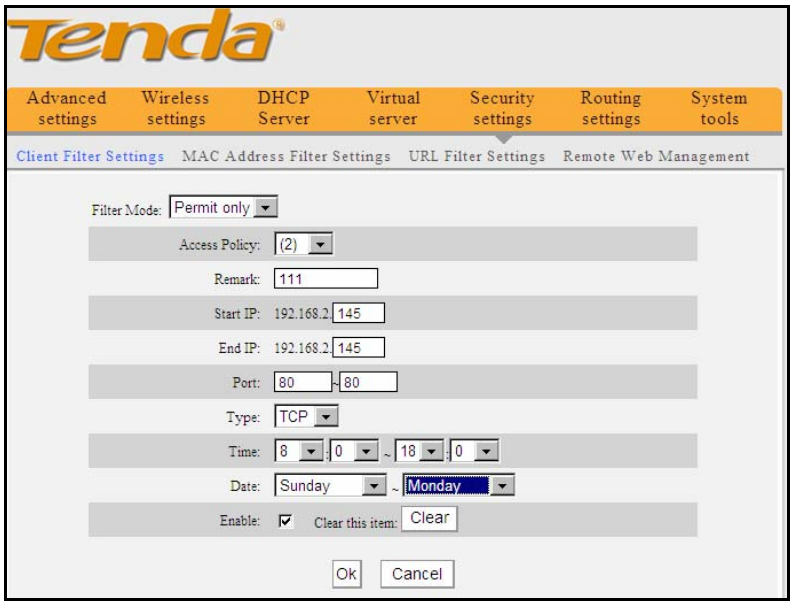
- **Filter Mode:** Select Disable, Forbid only or Permit only according to your own needs.
- **Access Policy:** Select a number (indicating a filter rule) from the drop-down menu.
- **Remark:** Enter a meaningful name to you for a new filter rule.
- **Start /End IP Address:** Enter a starting/ending IP address.
- **Port:** Enter TCP/UDP protocol port; it can be a port range.
- **Type:** Select a protocol or protocols for the traffic (TCP/UDP/Both).
- **Time:** Select a time range for the rule to take effect.
- **Day:** Select a day or several days for the rule to take effect.
- **Enable:** Check to enable or uncheck to disable a corresponding filter rule （allow/disallow matched packets to

pass through router）.

Example 1: To prohibit PCs within the IP address range of 192.168.2.100--192.168.2.120 from accessing Internet, do as follows:

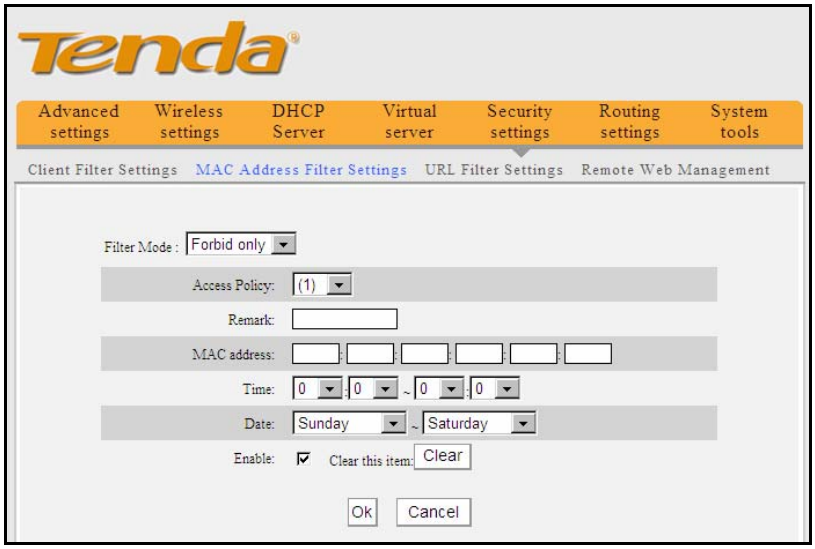


Example 2: To allow only the computer at an IP address of 192.168.2. 145 to access Internet from 8:00 to 18：00 without restricting other computers in LAN, do as follows:



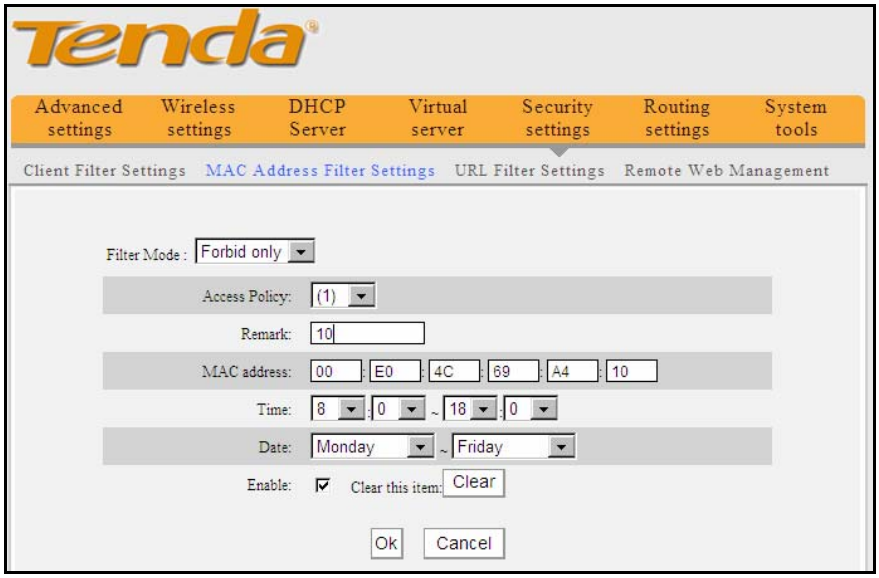
3.5.2 MAC Address Filter

To better manage the computers in LAN, you can use the MAC Address Filter function to control the computer's access to Internet.

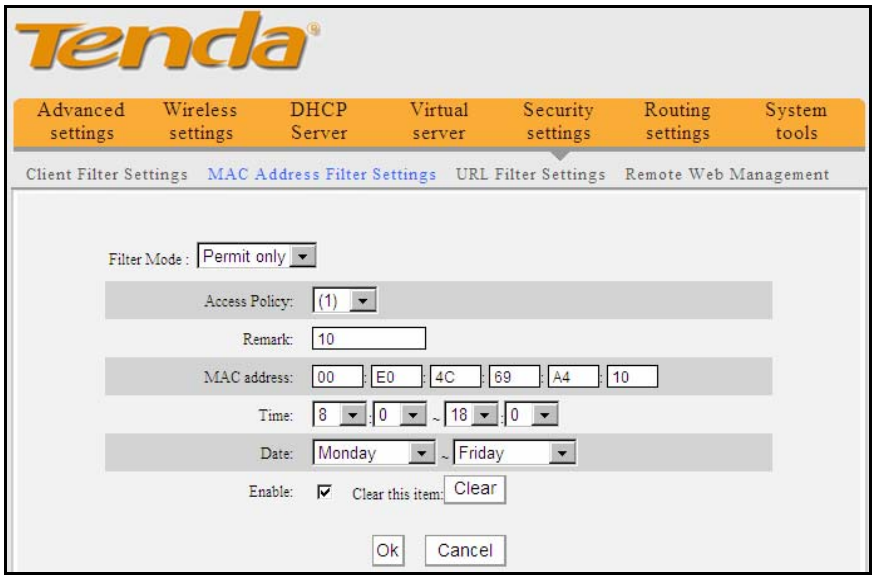


- **Filter Mode:** Select Disable, Forbid only or Permit only according to your own needs.
- **Access Policy:** Select a number (indicating a filter rule) from the drop-down menu.
- **Remark:** Enter a meaningful name to you for a new filter rule.
- **MAC address:** Enter the computer's MAC address that you want to filter out in the MAC address field.
- **Time:** Select a time range for the new MAC address filter rule to take effect.
- **Day:** select a day or several days for the new MAC address filter rule to take effect.
- **Enable:** Check to enable or uncheck to disable a corresponding filter rule （allow/disallow matched packets to pass through router）.
- **OK:** Click "OK" to activate new settings.

Example1: To prevent a PC at the MAC address of 00:E0:4C:69:A4:10 from accessing Internet within the time range of 8:00-18：00 from Monday to Friday do as follows:



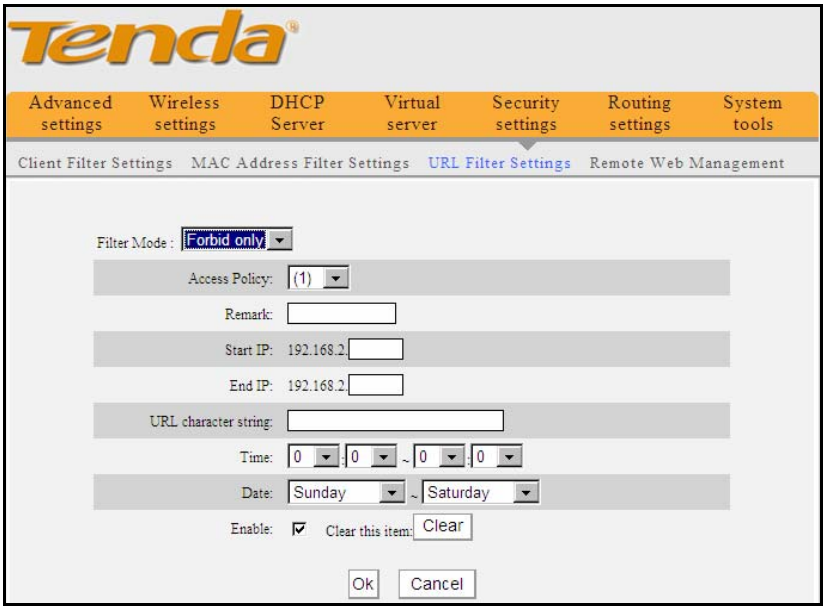
Example1: To allow only the PC at a MAC address of 00:E4:A5:44:35:69 to access Internet from Monday to Friday, do as follows:



3.5.3 URL Filter

To better control the LAN computers' access to websites, you can use URL filtering to deny their access to certain websites

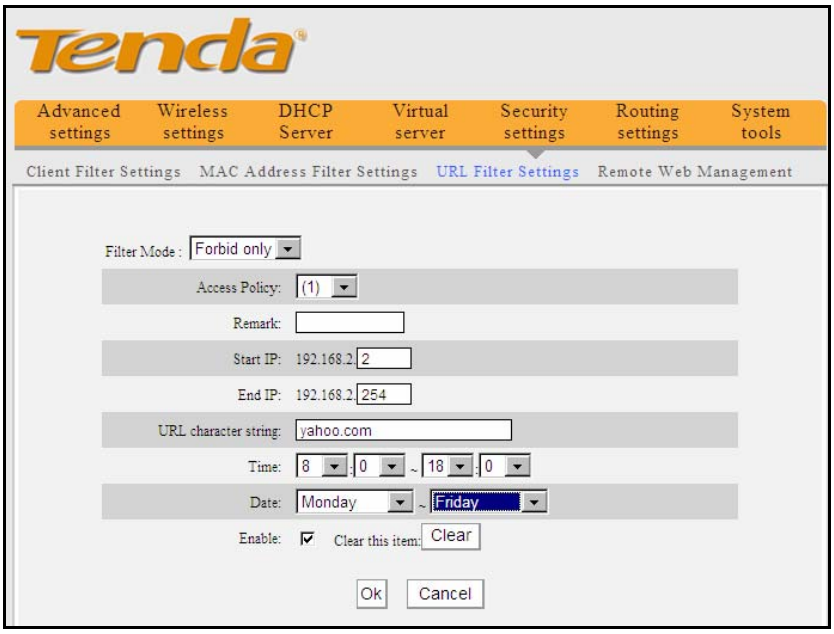
within a specified time range.



- **Filter Mode:** Select Disable or Forbid only according to your own needs.
- **Access Policy:** Select a number (indicating a filter rule) from the drop-down menu.
- **Remark:** Enter a meaningful name to you for a new filter rule.
- **Start/End IP Address:** Enter the starting/ending IP address.
- **URL character string:** Enter domain names or a part of a domain name that needs to be filtered.
- **Time:** Select a time range for the new URL filter rule to take effect.
- **Day:** select a day or several days for the new MAC address filter rule to take effect.
- **Enable:** Check to enable or uncheck to disable a corresponding filter rule （allow/disallow matched packets to pass through router）.
- **OK:** Click “OK” to activate the settings.

For example:

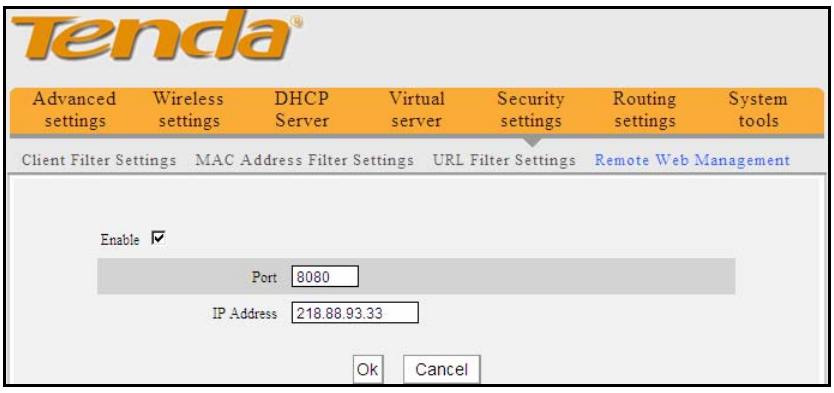
If you want to disallow all computers on your LAN to access “yahoo.com” at the time range of 8：00-18：00 from Monday to Friday, then do as follow:



⚠ **Note:** *Each URL character string entry can corresponde to only a domain name. So you need to set multiple rules if you want to filter out multiple domain names.*

3.5.4 Remote Web-based Management

The Remote Web-based Management feature allows users to configure your router from Internet via a web browser.



- **Enable:** Check or uncheck to enable or disable the remote web-based management feature.
- **Port:** Enter a port number for remote web-based management.
- **IP Address:** Enter the IP address of a PC on Internet authorized to access and manage your router's web-based utility remotely.

For example: If you want to allow a PC at the IP address of 218.88.93.33 to access your router's web-based utility from Internet via port: 8080, you need to configure same settings shown in the diagram above on your router. And what this IP user needs to do is to simply launch a browser and enter http: //220.135.211.56:8080 (provided that your router's WAN IP address is 220.135.211.56).

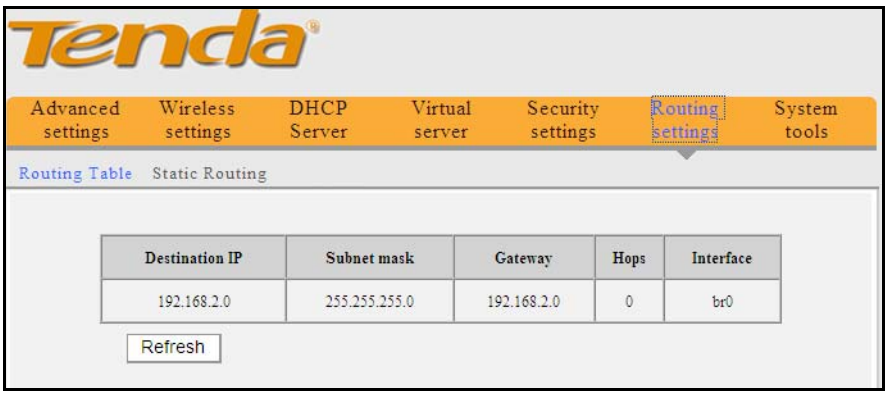
⚠ **Note:**

If you enter 0.0.0.0 in the IP address box, then all PCs on Internet can access your router's Web-based utility to view or change your settings remotely once you enable the remote Web-based management feature.

3.6 Routing Settings

3.6.1 Routing Table

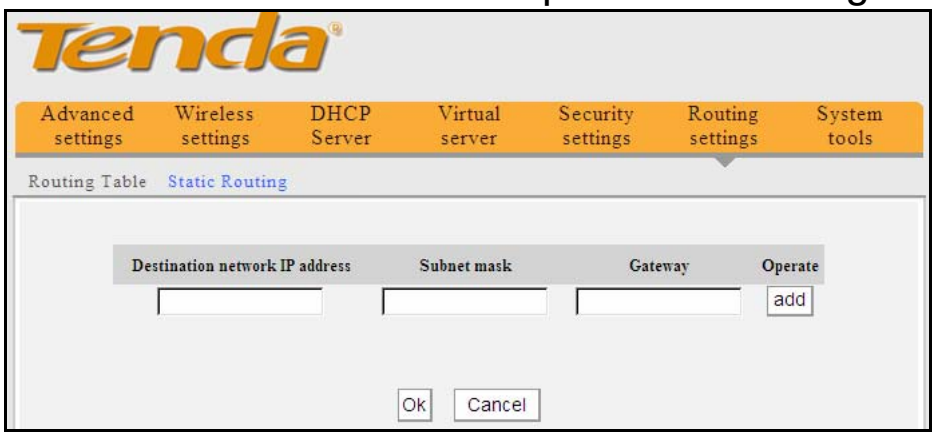
This page displays the router's core routing table which lists destination IP address, subnet mask, gateway, hop count and interface.



The main duty 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 the router to select an optimal path, i.e. routing algorithm. To complete this work, the router stores the related information of various transfer paths, i.e. establishing a routing table, for future route selection.

3.6.2 Static Routing

You can use this section to set up router's routing feature.



- **Destination Network IP Address:** Enter a destination IP address or subnet.
- **Subnet Mask:** Enter a Subnet Mask that corresponds to destination IP address or subnet you entered.
- **Gateway: Next-hop IP address.**

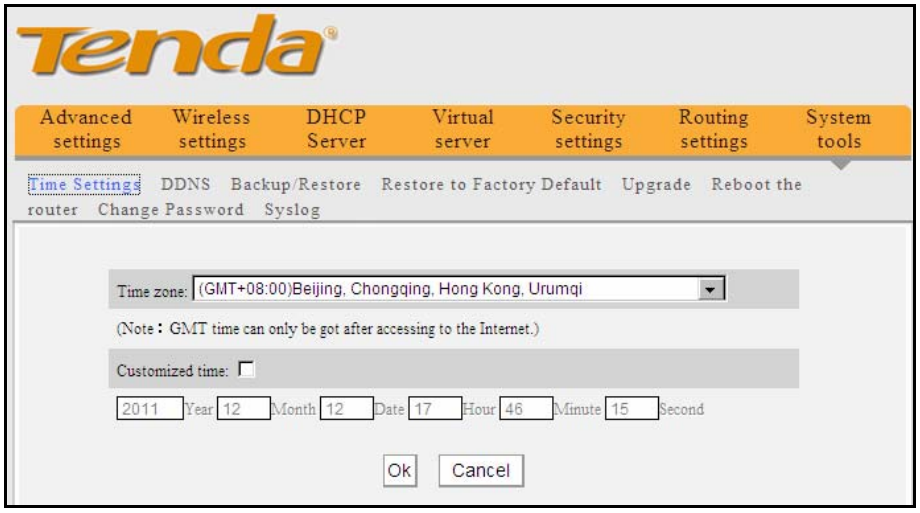
1. Gateway IP address must be on the same subnet with LAN/WAN IP address.

2. If Destination IP address box is entered with a single IP address, then corresponding subnet mask must be set to 255.255.255.255.
3. If Destination IP address box is entered with an IP subnet, then corresponding subnet mask must be set to 255.0.0.0.

3.7 Tools

3.7.1 Time Settings

This section assists you in setting the device's system time; you can either select to set the time and date manually or automatically obtain the GMT time from Internet.



⚠NOTE*:*

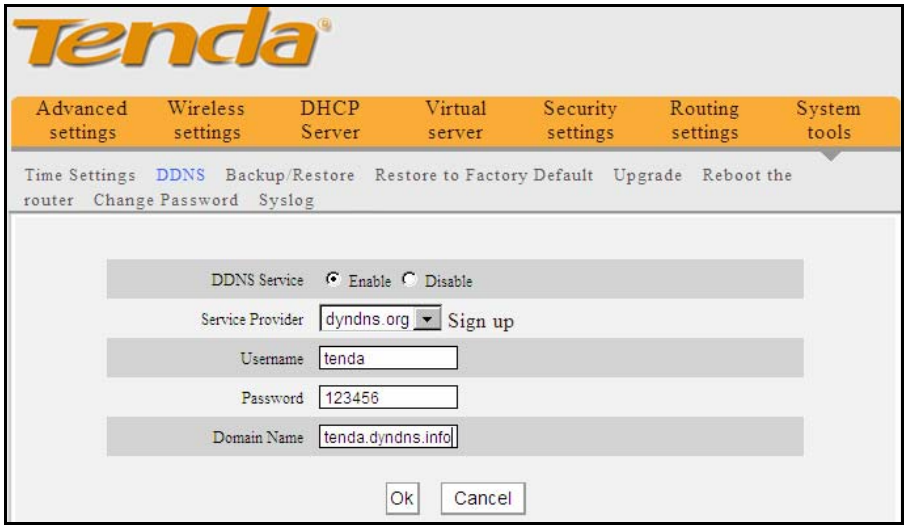
The configured time information loses once the router is powered off. But it obtains the GMT time automatically when you connect it to the Internet. Features/functions based on time (e.g. security settings) take effect only after Time and Date settings are configured manually or updated automatically from Internet.

3.7.2 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 hostname 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 hostname 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.



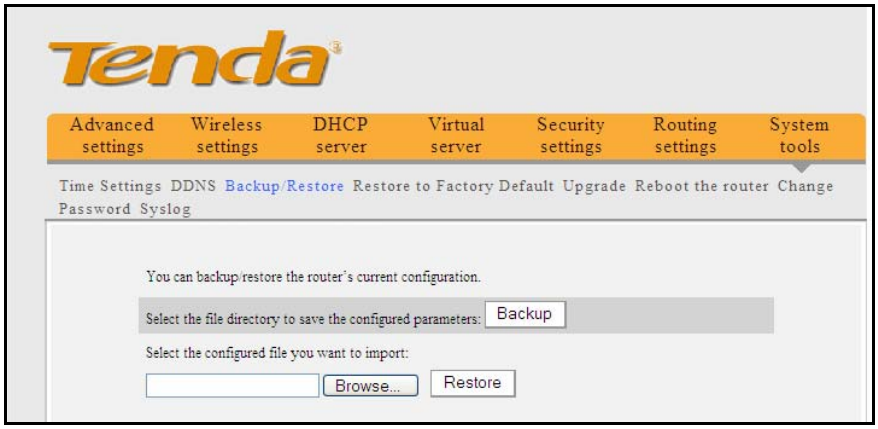
- **DDNS Service:** Click Enable or Disable radio button to enable/disable the DDNS feature.

- **Service Provider:** Select your DDNS service provider from the drop-down menu.
- **Username:** Enter the DDNS username provided by your DDNS service provider.
- **Password:** Enter the DDNS password provided by your DDNS service provider.
- **Domain Name:** Enter the DDNS domain name distributed by 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, then configure port settings on port range forwarding interface under virtual server menu 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's address bar.

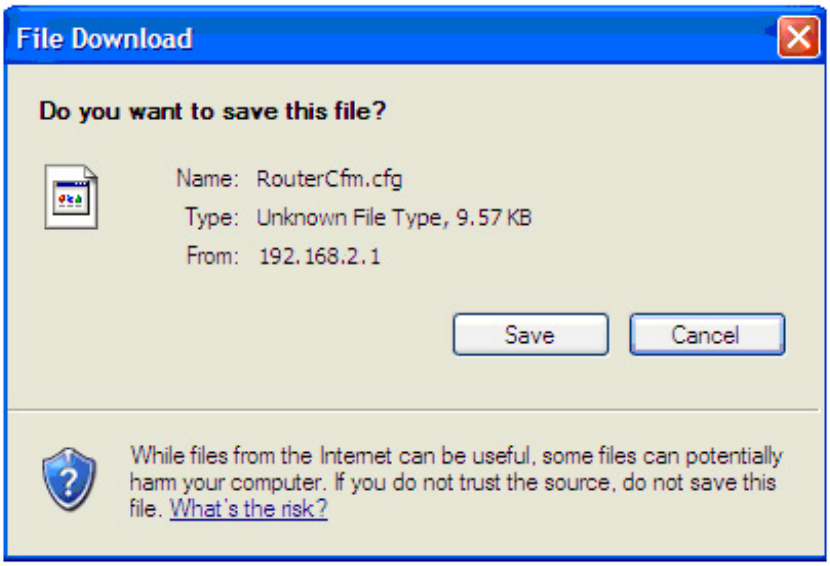
3.7.3 Backup/Restore Settings

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



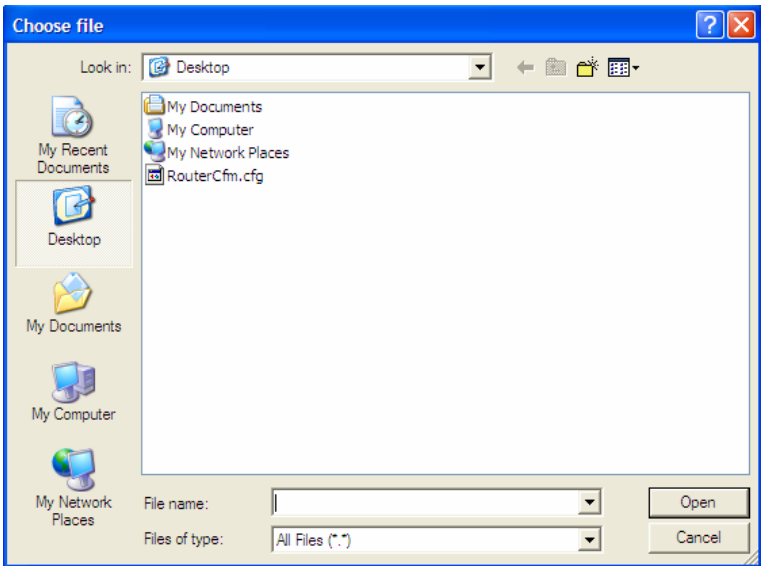
Backup Settings: Once you have configured the router the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your router in

case that the router is restored to factory default settings. To do this, click the “Backup” button next to where it says “Select the file directory to save the configured parameters” on the screen above.



And then，click the “Save” button on the appearing screen above to store it under the selected path.

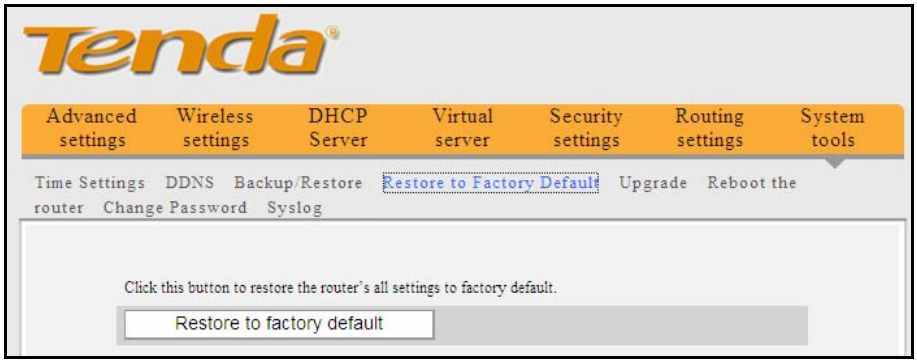
Restore Settings: Click the "Browse" button to locate and select a configuration file that is saved previously to your local hard drive.



And then click the "Restore" button to reset your router to previous settings.'

3.7.4 Restore to Factory Default Settings

To restore all settings to the device's factory default values, click the "Restore to Factory Default" button on the interface below:



Factory Default Settings:

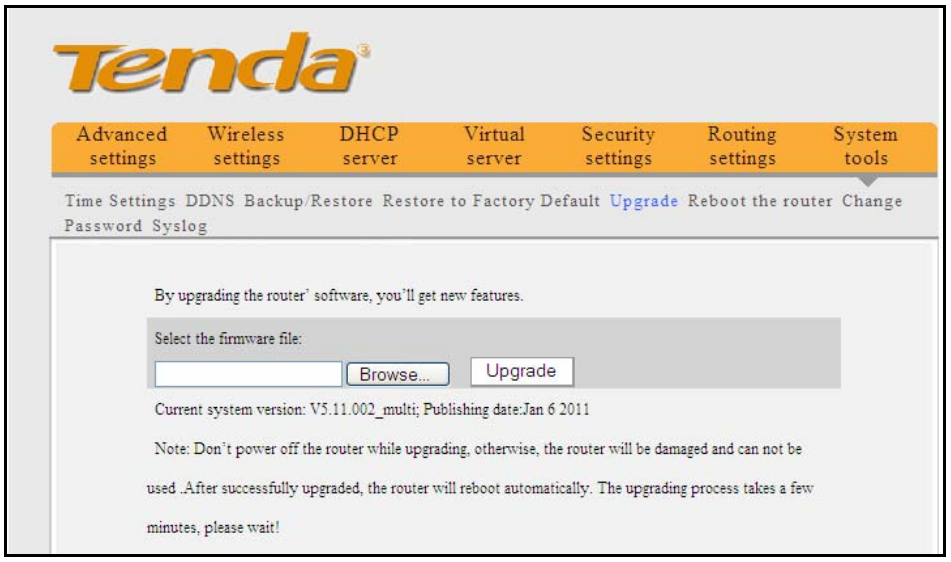
- **Password:** admin
- **IP Address:** 192.168.2.1
- **Subnet Mask:** 255.255.255.0

⚠**Note:** To activate your configurations, reboot the device after you reset the router.

3.7.5 Firmware Upgrade

Firmware upgrade is released periodically to improve the functionality of your router and also to add new features. If you run into a problem with a specific feature of the router, log on to our

website（www.tenda.cn）to download the latest firmware to update your router.

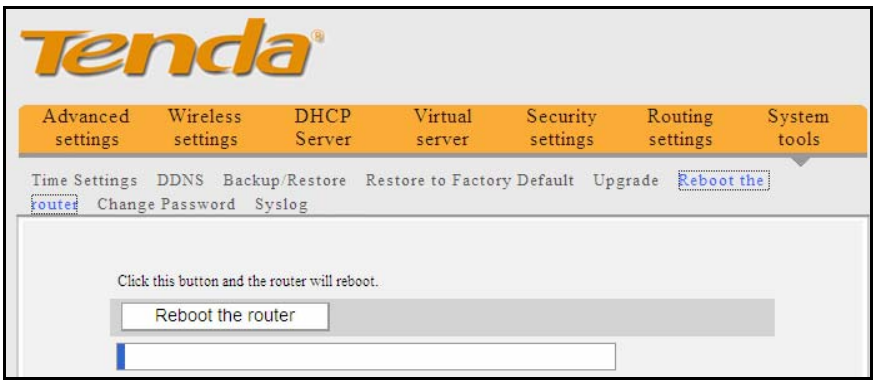


- **Browse:** Click this button to select an upgrade file.
- **Upgrade:** Click this button to start an upgrading process. After the upgrade is completed, the Router will reboot automatically.

  NOTE: Do not disconnect the router from your management PC (the PC you use to configure the router) or power off the router during the upgrade process; otherwise, it may be permanently damaged. The router will restart automatically when the upgrade process, which takes several minutes, completes.

3.7.6 Reboot

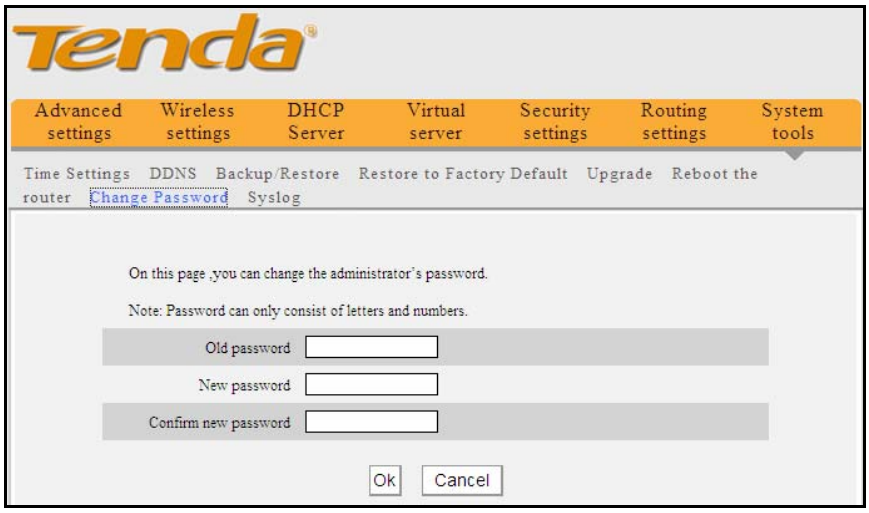
By Rebooting the device，new settings can be brought into effect. And WAN connection will be cut automatically during this process.



➢ **Reboot:** Click this button to reboot the device.

3.7.7 Change Password

On the screen below, you can change the password for login to the device's Web-based interface.



➢ **Old Password:** Enter the old password.

➢ **New Password:** Enter a new password.

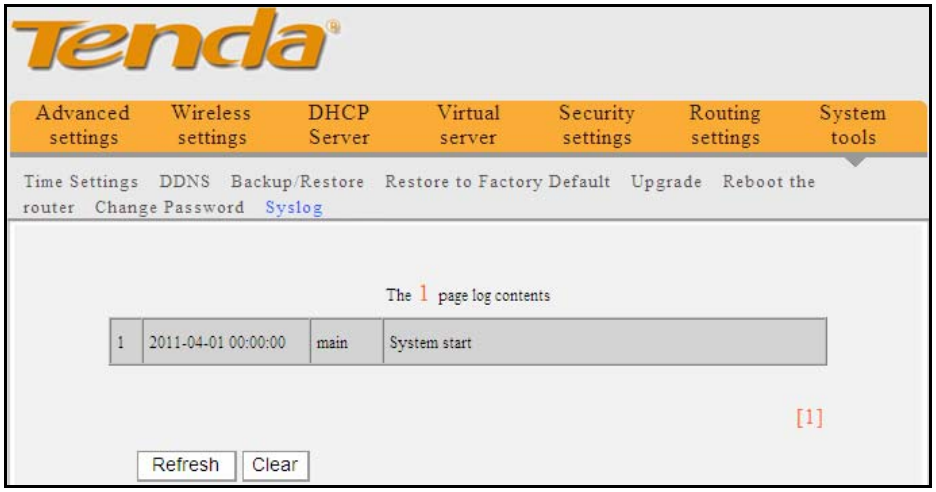
➢ **Confirm new Password:** Re-enter the new password for confirmation.

If you enter a correct old password, then clicking the "OK" button saves your new password.

NOTE: For the sake of security, it is highly recommended that you change default login password and user name.

3.7.8 SysLog

The Syslog option allows you to view all events that occur upon system startup and check whether there is attack on your network.



- **Refresh:** Click this button to update the log.
- **Clear:** Click this button to clear the log record.

3.7.9 Logout

After you have finished all settings, click the Logout tab to exit the utility.

Appendix 1 Features

- Compliant or compatible with 802.11n, 802.11g, 802.11b, 802.3, 802.3u
- Delivers wireless speed up to 150Mbps
- 1*10/100Mbps auto-negotiation LAN/WAN port
- Can be connected to a xDSL/Cable MODEM or community broadband (Dynamic/static IP internet connection type)
- Supports WEP, WPA-PSK, WPA2-PSK and WPA&WPA2-PSK security modes
- WISP feature to connect to ISP's wireless hot spot.
- Supports hidden SSID and MAC-based access control features
- Support WMM to stream your video and audio
- Supports SNTP, UPnP, DDNS, virtual server and DMZ
- Provides syslog to record all events occurring upon system startup

Appendix 2 Security Statement

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference

to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment. (Example- use only shielded interface cables when connecting to computer or peripheral devices).

"The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter."

FCC 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 the minimum distance of 20 cm. Operation is subject to the following two conditions:

1) This device may not cause interference, and

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

Caution!

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user authority to operate the equipment.

Eu Declaration or Declaration of Conformity

Hereby, SHENZHEN TENDA TECHNOLOGY CO.,LTD, declares that this wireless router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.