User Guide

www.tendacn.com

Wireless N300 High Power Router

Copyright Statement

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 http://www.tendacn.com

Table of Contents

CHAPTER 1 PRODUCT OVERVIEW **3**

1.1 PACKAGE CONTENT 3
1.2 PANEL OVERVIEW 4

CHAPTER 2 INSTALLATION **6**

CHAPTER 3 INTERNET CONNECTION SETUP **7**

3.1 CONFIG TCP/IP SETTINGS ON YOUR PC 7
3.2 WEB LOGIN 12
3.3 QUICK INTERNET CONNECTION SETUP 12
3.4 QUICK ENCRYPTION 14

CHAPTER 4 ADVANCED SETTINGS **15**

4.1 STATUS 15
4.2 WAN SETTINGS 17
4.3 LAN SETTINGS 22
4.4 MAC CLONE 22
4.5 DNS SETTINGS 23
4.6 BANDWIDTH CONTROL 24
4.7 TRAFFIC STATISTICS 27
4.8 WAN SPEED 28

CHAPTER 5 WIRELESS SETTINGS **29**

5.1 WIRELESS BASIC SETTINGS 29
5.2 WIRELESS SECURITY 30
5.2.1 WPS 30
5.2.2 WEP 31
5.2.3 WPA-PSK 32
5.2.4 WPA2-PSK 33
5.2.5 Mixed WPA/WPA2-PSK 33
5.3 WIRELESS EXTENDER 34
5.3.1 Universal Repeater Mode 34
5.3.2 WISP Client Mode 34
5.3.3 WDS 37
5.4 ACCESS CONTROL 39
5.5 CONNECTION STATUS 41

CHAPTER 6 DHCP **42**

6.1 DHCP SETTINGS 42
6.2 DHCP CLIENT LIST 43

CHAPTER 7 VIRTUAL SERVER **44**

7.1 PORT RANGE FORWARDING 44
7.2 DMZ HOST 46
7.3 UPNP 47

CHAPTER 8 PARENTAL CONTROL **48**

8.1 CLIENT FILTER 48
8.2 MAC FILTER 50
8.3 URL FILTER 52
8.4 REMOTE WEB-BASED MANAGEMENT 53

CHAPTER 9 ROUTING SETTINGS **55**

9.1 ROUTING TABLE 55
9.2 STATIC ROUTING 55

CHAPTER 10 SYSTEM TOOLS **57**

10.1 TIME SETTINGS 57
10.2 DDNS 57
10.3 BACKUP/RESTORE 59

10.4 RESTORE TO FACTORY DEFAULT SETTINGS 59
10.5 FIRMWARE UPDATE 60
10.6 REBOOT 60
10.7 CHANGE PASSWORD 61
10.8 SYSTEM LOGS 61
APPENDIX 1 GLOSSARY 62
APPENDIX 2 PRODUCT FEATURES 63
APPENDIX 3 TROUBLESHOOTING 64

Chapter 1 Product Overview

Thanks for purchasing this Tenda router .

The Tenda W3002R Wireless N300 High Power Router is a802.11n wireless router. You just need simply connect the W3002R to a cable or DSL modem and Internet access sharing will be reachable to multiple computers, game consoles, and media players over an up to 300Mbps WLAN that is secured with WPA and WPA2 encryption methods. Plus, it provides WISP client mode to let you access Internet wirelessly and WDS to extend your wireless coverage. With high power, the Tenda W3002R is ideal for large homes or offices.

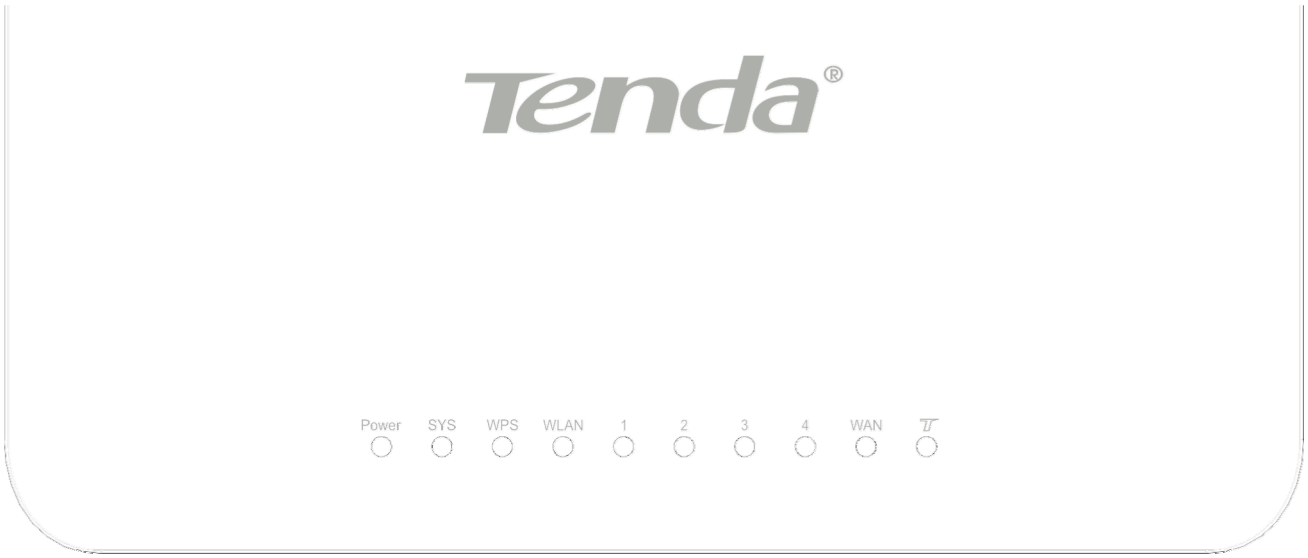
1.1 Package Content

Unpack the box and verify the following items:

- W3002R
- Power Adapter;
- Resource CD
- Two undetachable 5dbi antenna
- Ethernet Cable
- Quick Installation Guide

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

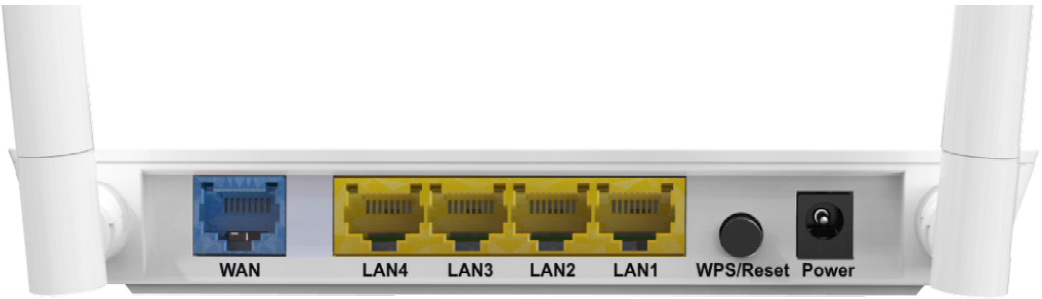
1.2 Panel Overview



LED Overview:

LED Indicator	Status	Description
POWER	On	The router is powerd on
WPS	Flashing	The router is performing WPS authentication with wireless client
	On	WPS is enabled
SYS	Flashing	The router is working properly
WLAN	On	The wireless function is enabled
	Flashing	the router is transmitting data wirelessly
WAN LAN(1-4)	On	Devices connect to the corresponding port properly but no data transmitted or received
	Flashing	Sending or Receiving data over corresponding port

Back Panel:



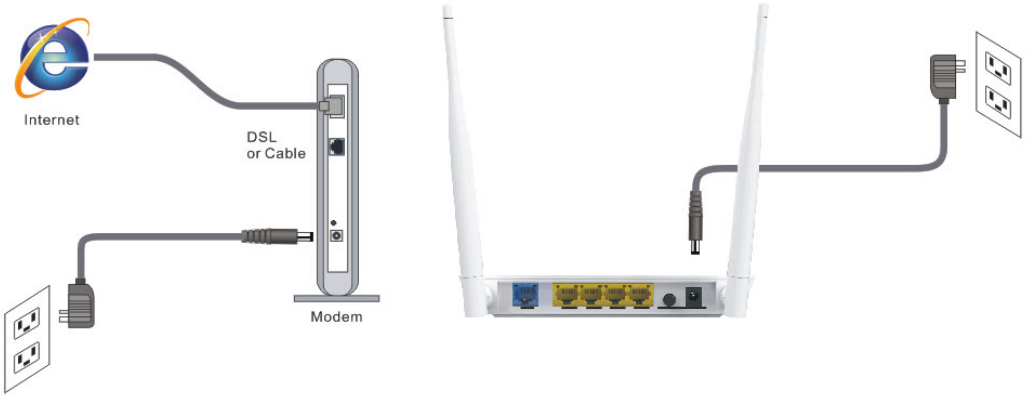
Interface/button overview:

Interface /Button	Description
POWER	Power receptacle. Note: Using a power supply with a different voltage rating than the one included the package may damage the router.
WAN	The Internet port for connection to the cable or the DSL modem or direct ISP service via an Ethernet cable.
LAN(1/2/3/4)	Connect Ethernet devices such as computers, switches, and hubs.
RESET/WPS	Press and hold the button for 7 seconds to restore the router to its original factory default settings or for about 1 second to enable the WPS functionality.

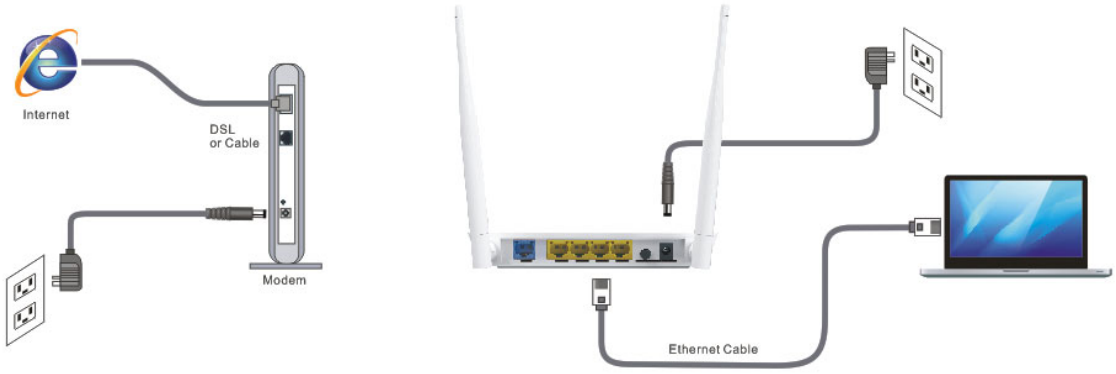
Chapter 2 Installation

This manual takes the Tenda W3002R as an example to demonstrate whole installation process, which applies to other products alike.

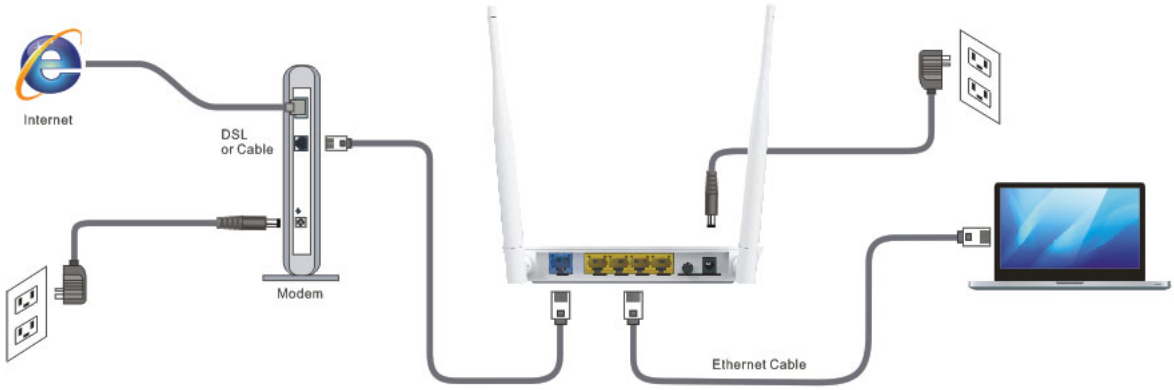
1. Connect one end of the included power adapter to the Device and plug the other end into a wall outlet nearby. (Using a power adapter with a different voltage rating than the one included the package may damage to the router.)



2. Connect one of the LAN ports on the Router to the NIC port on your PC using an Ethernet cable.



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



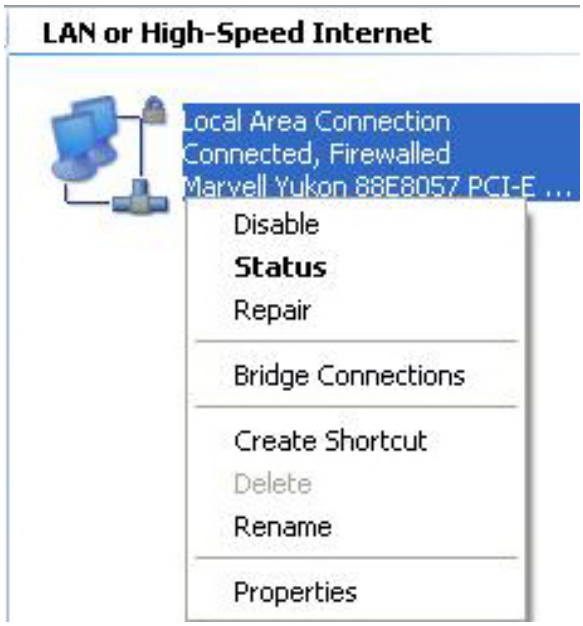
Chapter 3 Internet Connection Setup

3.1 Config TCP/IP settings on your PC

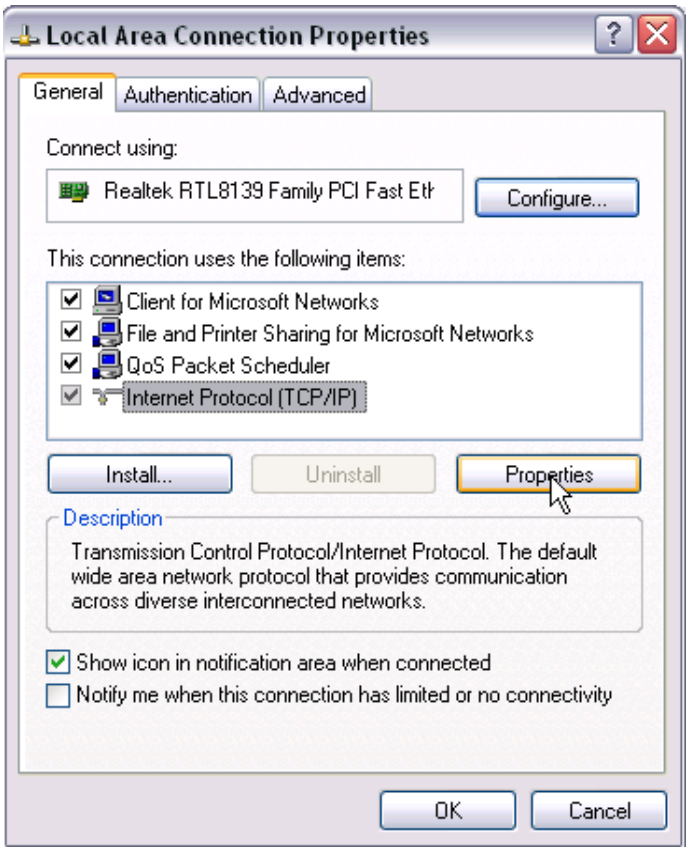
If you are using Windows XP,do as follows:

1. From the desktop, right-click My Network Places > Properties.

2. Right-click on the Local .Area Connection and select Properties.

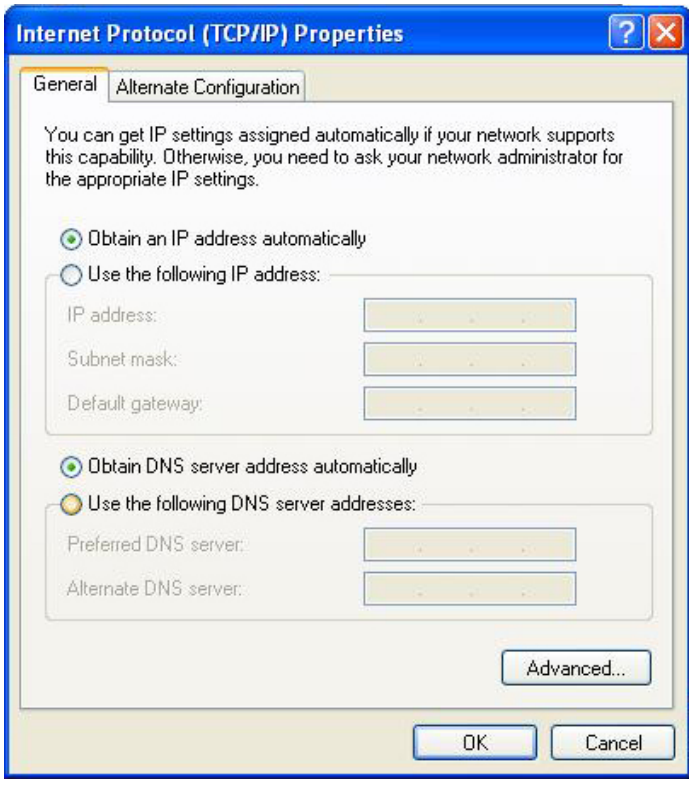


3. Select Internet Protocol (TCP/IP) and click Properties.



4. Select "Obtain an IP address automatically" or "Use the following IP address".

a. "Obtain an IP address automatically"



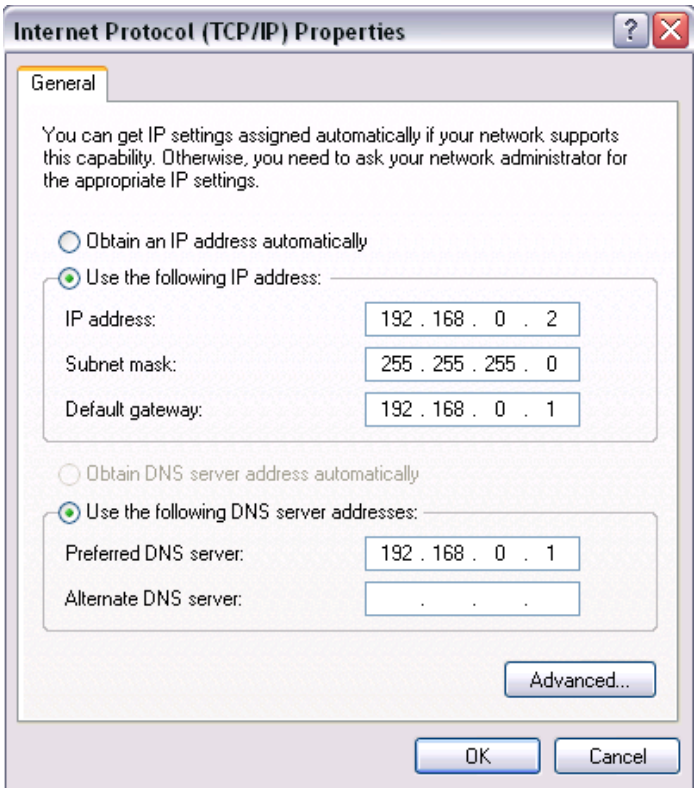
b. Use the following IP address"

IP address: Enter 192.168.0.xxx where xxx can be any number between 2 and 254).

Subnet mask: 255.255.255.0.

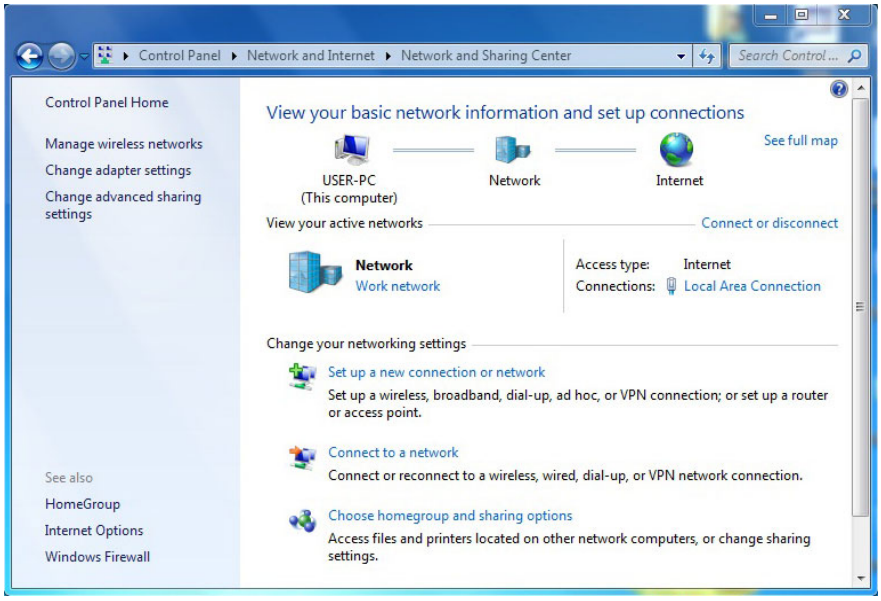
Default gateway: Enter 192.168.0.1.

Preferred DNS server: Set Preferred (Primary) DNS the same as the LAN IP address of your Device (192.168.0.1) if you don't know your local DNS server address (Or consult your ISP). The Alternate (Secondary) DNS is optional. Click **OK** twice to save your settings.

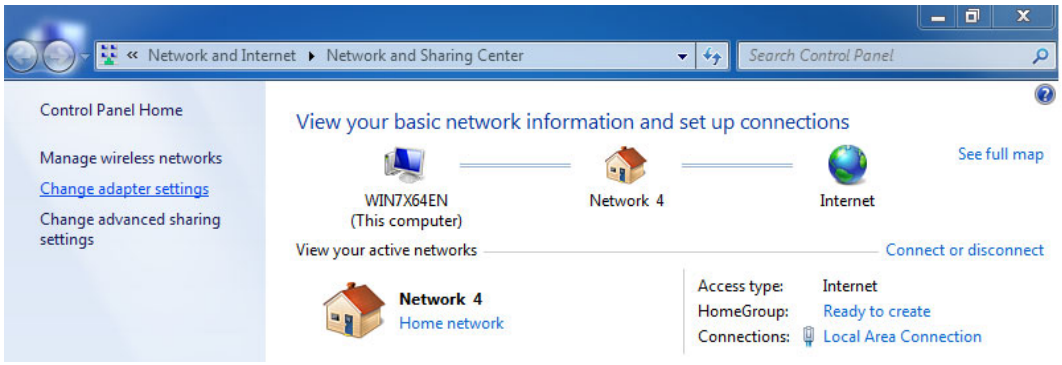


If you are using Windows 7, do as follows:

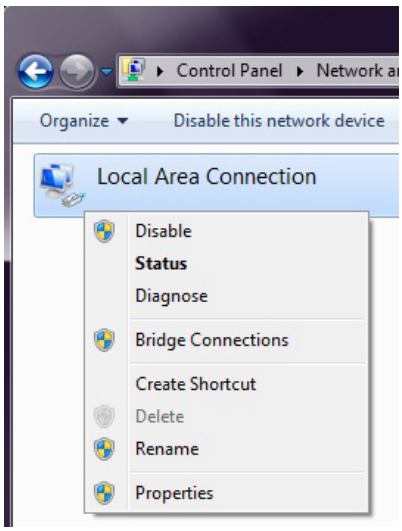
1. Click on Start > Control Panel > Network and Internet > Network and Sharing Center.



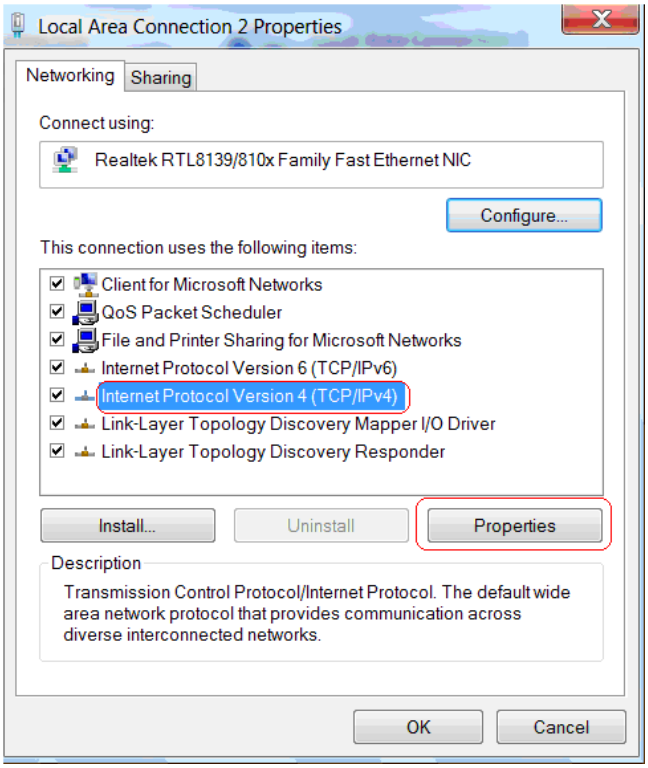
2. Click "Change adapter settings".



3. Right-click on the Local Area Connection and select Properties.

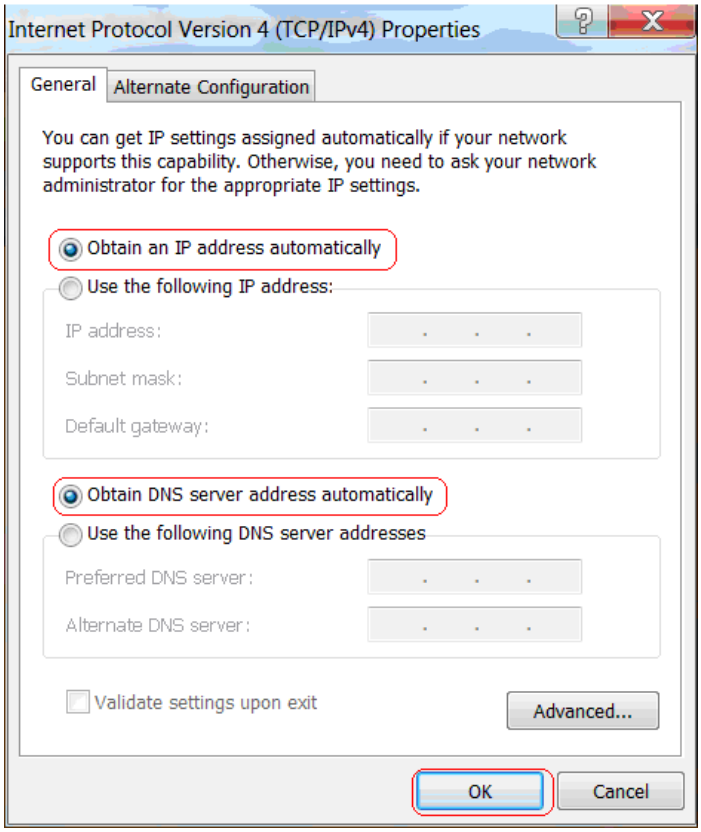


4. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).

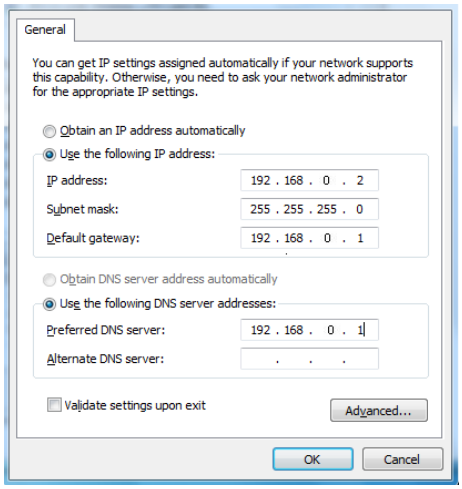


5. Select "Obtain an IP address automatically" or "Use the following IP address".

a. "Obtain an IP address automatically"



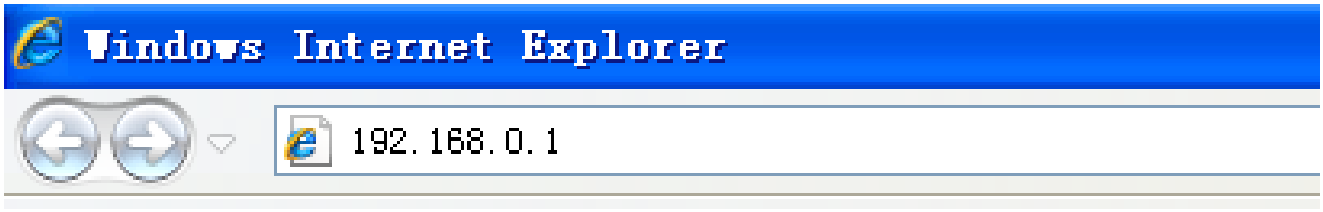
b. "Use the following IP address"



IP address: Enter 192.168.0.xxx where xxx can be any number between 2 and 254).
Subnet mask: 255.255.255.0.
Default gateway: Enter 192.168.0.1.
Preferred DNS server: Set Preferred (Primary) DNS the same as the LAN IP address of your Device (192.168.0.1) if you don't know your local DNS server address (Or consult your ISP). The Alternate (Secondary) DNS is optional. Click OK twice to save your settings.

3.2 Web Login

1. Open a web browser(IE, Firefox, Safari etc), type 192.168.0.1 in the address bar and press "Enter". Then you can login to the router's web management.



3.3 Quick Internet Connection Setup

2 common Internet connection types are available on the home page: PPPoE and DHCP.

DHCP: Select DHCP (Dynamic IP) if you are online immediately when your computer connects to the ADSL/Cable modem directly, and then configure a security key to secure your wireless network.

PPPoE: Select PPPoE (Point to Point Protocol over Ethernet) if you used to connect to the Internet Using a Broadband Connection that requires a username and password. Enter the user name and password provided by your ISP and configure a security key to secure your wireless network.

⚠ Note:

DHCP is the default Internet connection type. If you need other connection types, please go to Chapter 4-> WAN settings.

3.4 Quick Encryption

Secure your wireless network either by configuring a security key on the home page, which is quicker and simpler, or going to wireless security page where you can customize security mode and Encryption type in addition to a security key (For the latter, see section 5.2).

NOTE: Wireless network is not encrypted by factory default and thus insecure! Please secure it with custom encryption.

To secure your wireless network quick and simple on the home page.

Simply define a custom security key. Security mode and Encryption type here is preset to WPA-PSK and AES respectively by default. If you don't customize a security key, then "12345678" is populated automatically by default as a security key as seen below after you submit your settings:

Chapter 4 Advanced Settings

4.1 Status

Here you can view WAN status and system status.

WAN Status	
Connection Status	Connected
Connection Type	Dynamic IP
WAN IP	10.10.10.10
Subnet Mask	255.255.255.0
Gateway	10.10.10.1
Prefered DNS Server	11.11.11.12
Alternate DNS Server	12.12.12.12
Connection Time	00:00:29

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

Disconnected: Indicates that the Ethernet cable from your ISP side is not correctly connected to device's WAN port or the router 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 the router has been connected to your ISP.

Connection Type: Displays current Internet connection type.

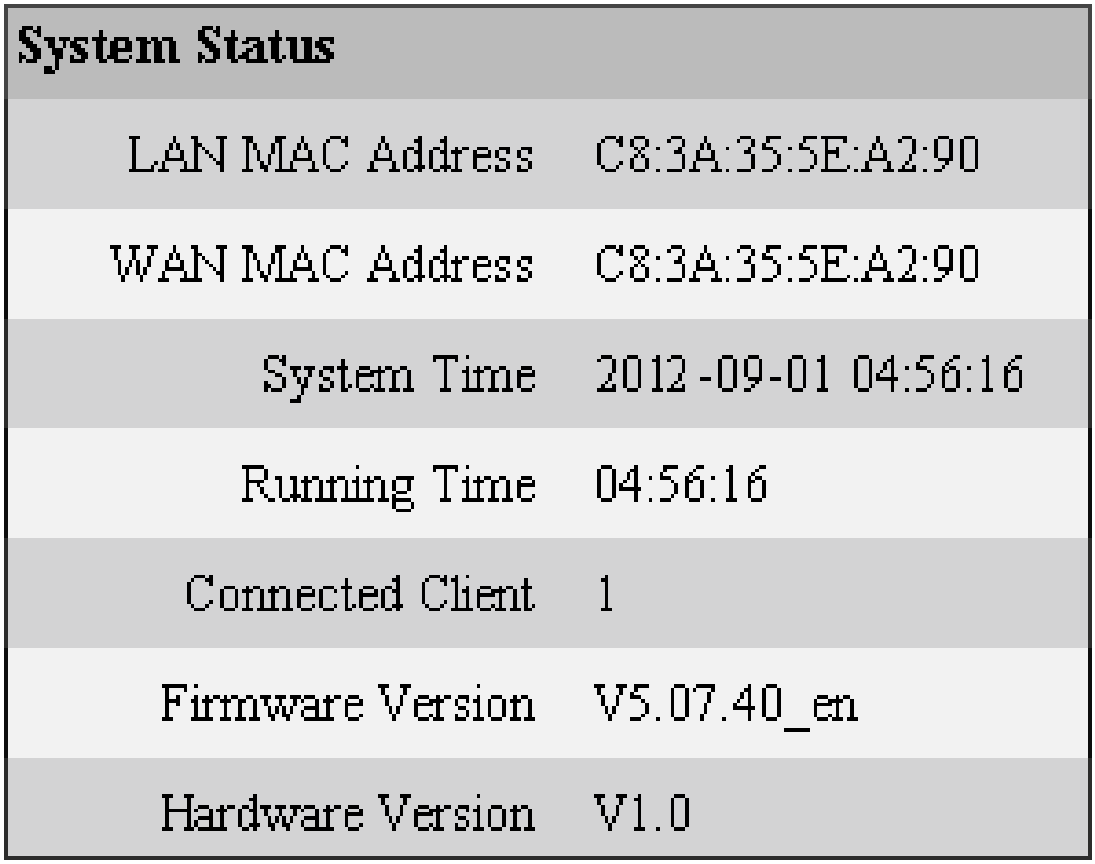
WAN IP: Displays the IP address of WAN port that provided by your ISP.

Subnet Mask: Displays WAN subnet mask provided by your ISP.

Gateway: Displays WAN gateway address.

Preferred DNS Server: Displays the preferred DNS Server address.

Alternate DNS Server: Displays the alternate DNS Server address .

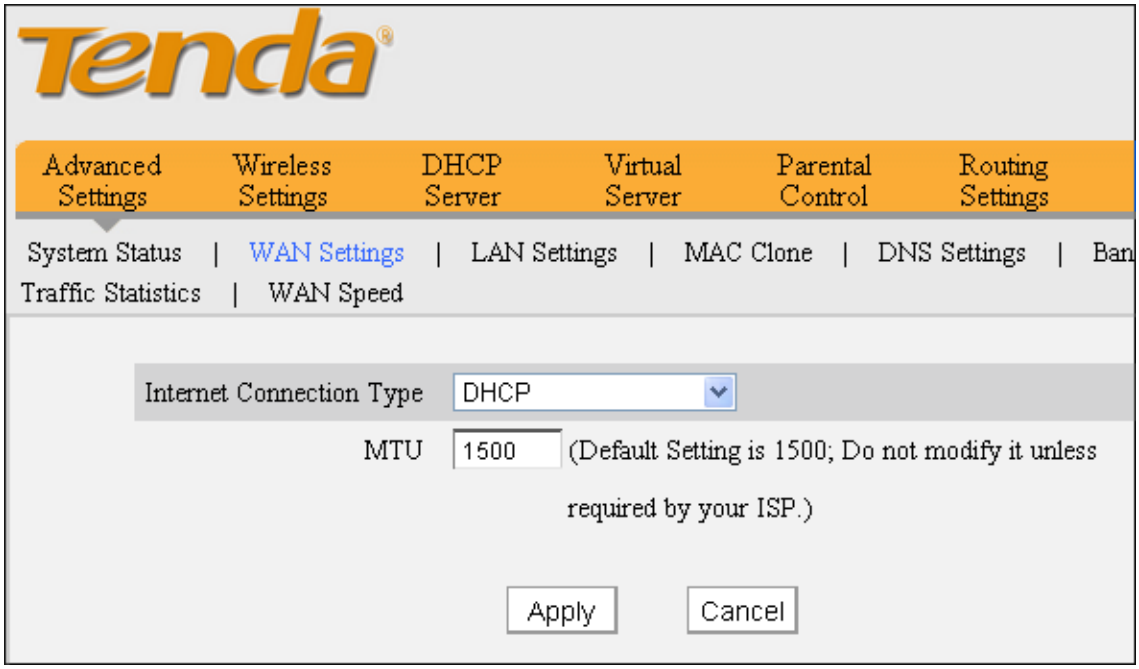


LAN MAC Address: Displays router's MAC address of LAN interface.
WAN MAC Address: Displays router's MAC address of WAN interface.
System Time: Displays router system time either customized or update with NTP server.
Connected Client: Displays the number of client devices.
Firmware Version: Displays router's current firmware version.
Hardware Version: Displays router's current hardware version.

4.2 WAN Settings

DHCP (Dynamic IP)

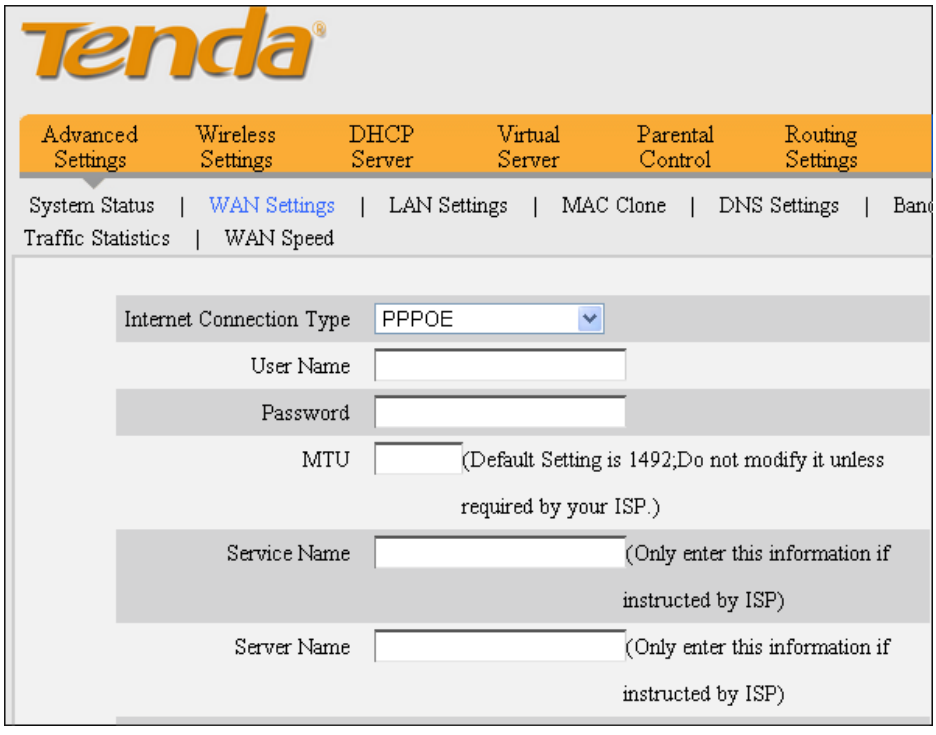
DHCP (Dynamic IP): Select this option to let router obtain IP settings automatically from your ISP if you are online immediately when your computer connect to the ADSL/Cable modem directly.



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.

PPPoE

Use this option if you used to connect to the Internet Using a Broadband Connection that requires a username and password



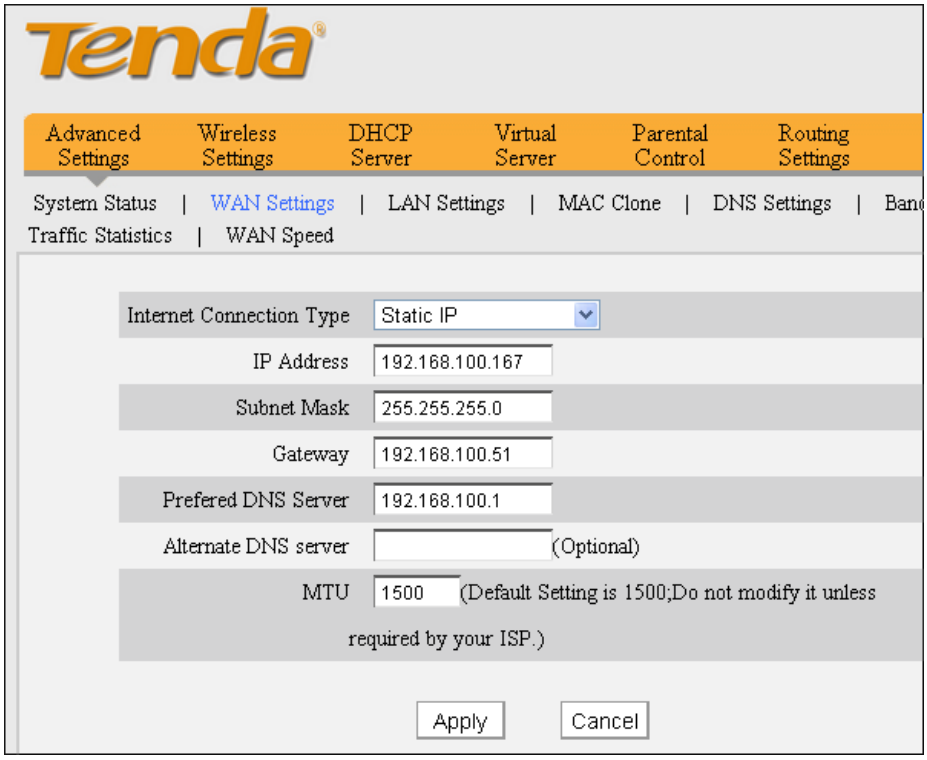
Internet connection Type: Displays the current Internet connection type.
User Name: Enter the PPPoE User Name provided by your ISP.
Password: Enter the PPPoE password provided by your ISP.
MTU: Maximum Transmission Unit. DO NOT change it from the factory default of 1492 unless necessary. You may need 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.
Connect Automatically: Connect automatically to Internet upon system startup or connection failure.
Connect Manually: Require users to manually connect to Internet upon system startup or connection failure.
Connect on Demand: Connect automatically to Internet only when there is data being transferred.
Connect during Specified Time Period: Connect automatically to Internet during a specified time length.

⚠ **Note:**

Before you can use the "Connect during Specified Time" feature, you must configure system time (System Tools> Time) .

Static IP

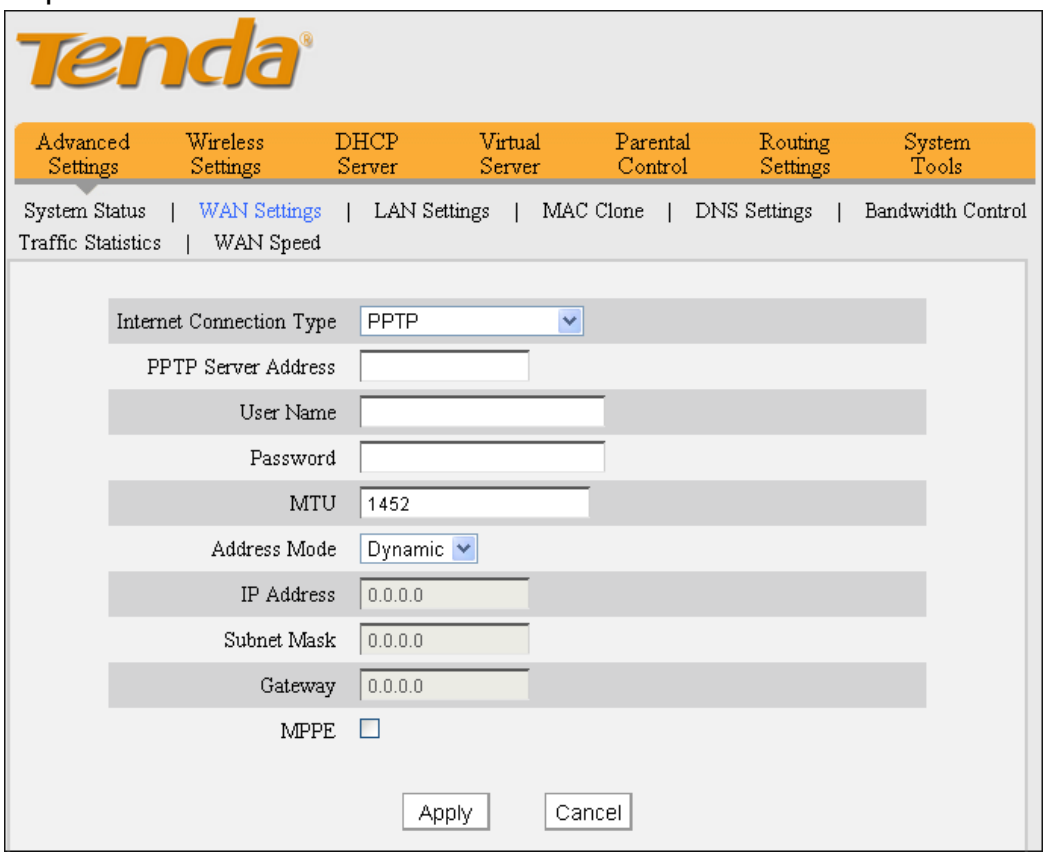
If your ISP provide the details IP address, Subnet Mask,Gateway,Preferred DNS Server address,Alternate DNS Server address ,please select “Static IP" as Internet Connection Type, enter IP address, subnet mask, Gateway,Preferred DNS Server address and Alternated DNS Server address (optional) info provided by your ISP in corresponding fields.



Internet connection Type: Displays the current Internet connection type.
IP Address: Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
Subnet mask: Enter the subnet mask provided by your ISP.
Gateway: Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.
Preferred DNS Server: Enter the DNS address provided by your ISP.
Alternate DNS Server: Enter the other DNS address if your ISP provides(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; in this case, try 1450, 1400, etc.

PPTP

PPTP: Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP requires. The PPTP allows you to connect to PPTP VPN server from ISP or headquarter. For example : A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.

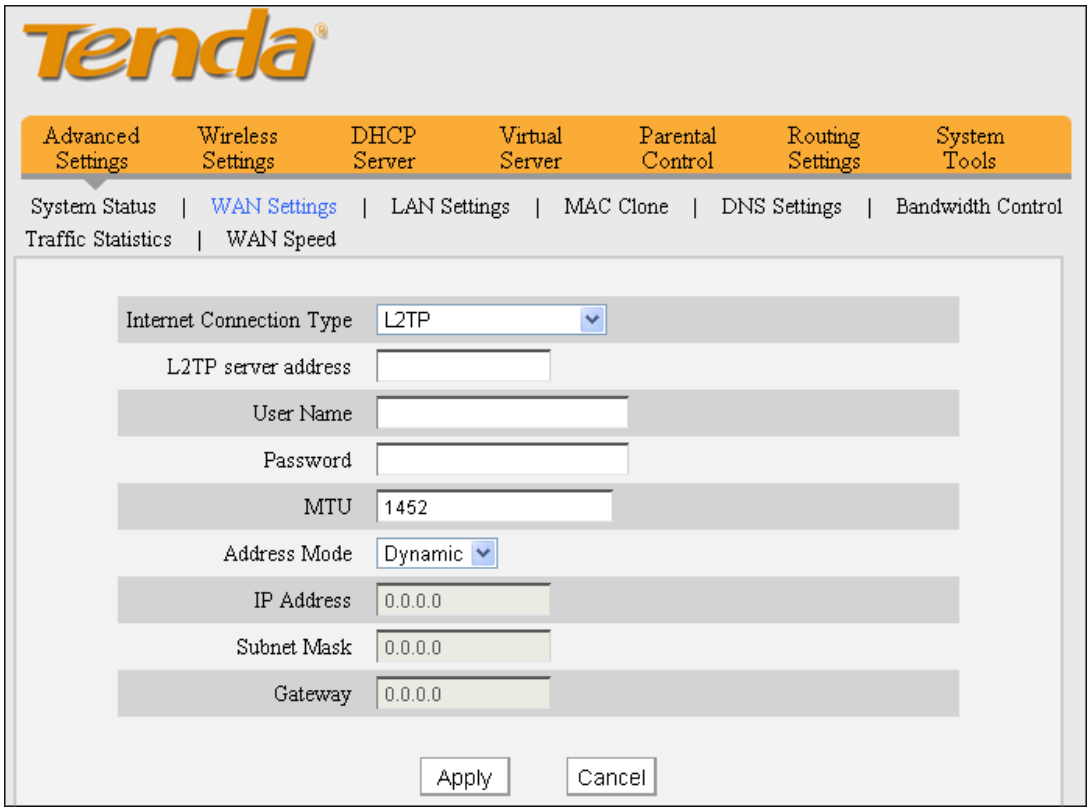


Internet connection Type: Displays the current Internet connection type.
PPTP Server Address: Enter the IP address of domain name of a PPTP server.
User Name: Enter the PPTP User Name provided by your ISP.
Password: Enter your Password.
MTU: Maximum Transmission Unit. DO NOT change it from the factory default of 1452 unless necessary.

Address Mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
IP Address: Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
Subnet mask: Enter the subnet mask provided by your ISP.
Gateway: Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.

L2TP

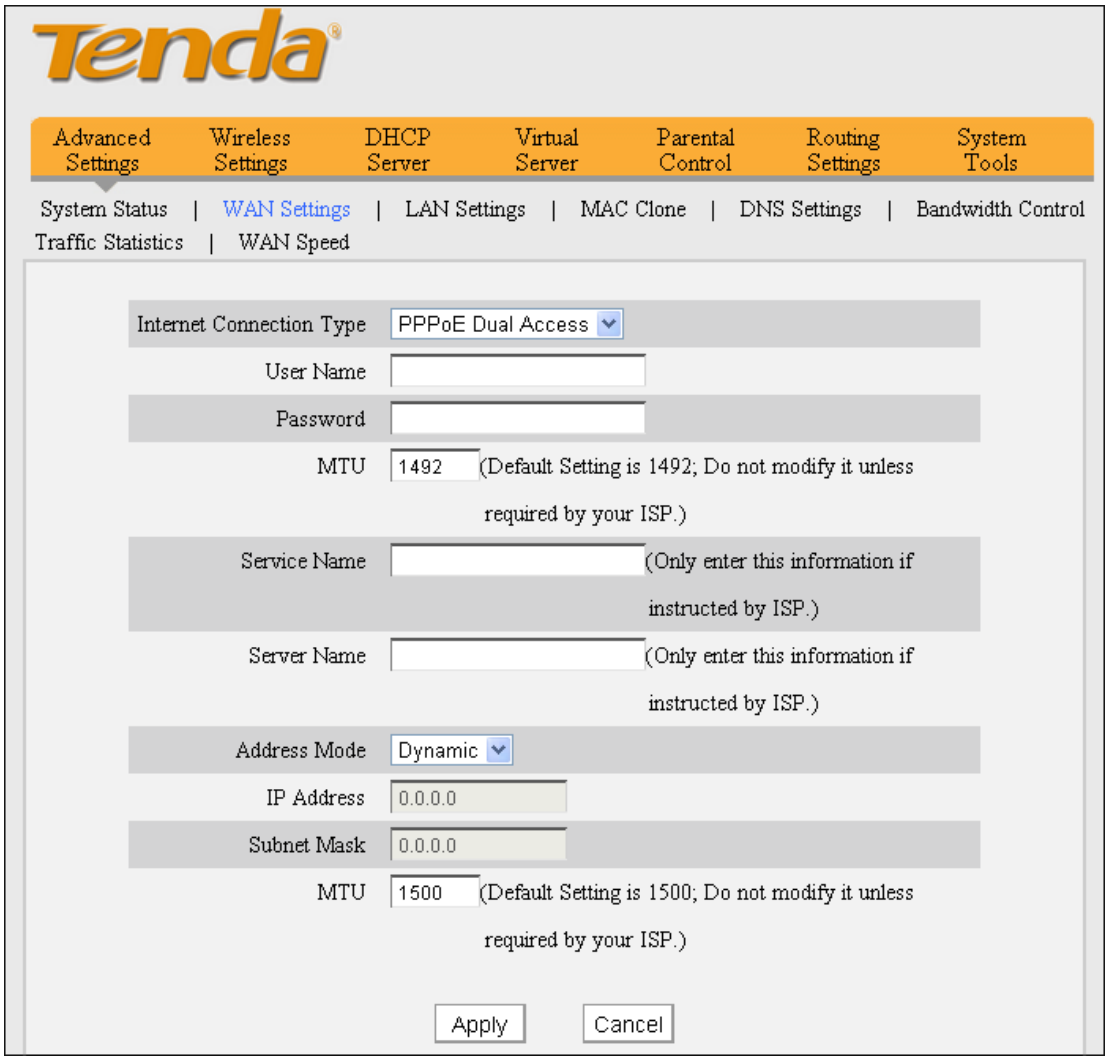
Select L2TP (Layer 2 Tunneling Protocol) if your ISP requires. The L2TP allow you connect to L2TP VPN server from ISP or headquarter. For example : A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



Internet connection Type: Displays the current Internet connection type.
L2TP Server Address: Enter the IP address or domain name of a L2TP server.
User Name: Enter the L2TP User Name provided by your ISP.
Password: Enter your Password.
MTU: Maximum Transmission Unit. DO NOT change it from the factory default of 1452 unless necessary..
Address Mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.
IP Address: Enter the IP address provided by your ISP. Consult your ISP if you are not clear.
Subnet mask: Enter the subnet mask provided by your ISP.
Gateway: Enter the WAN Gateway provided by your ISP. Consult your ISP if you are not clear.

PPPoE Dual Access

(only supported in special Areas e.g.Russia.)



Internet connection Type: Displays a list of available Internet Connection types.

Username: Enter the PPPOE account provided by your ISP.

Password: Enter the PPPOE password provided by your ISP.

Address Mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static".

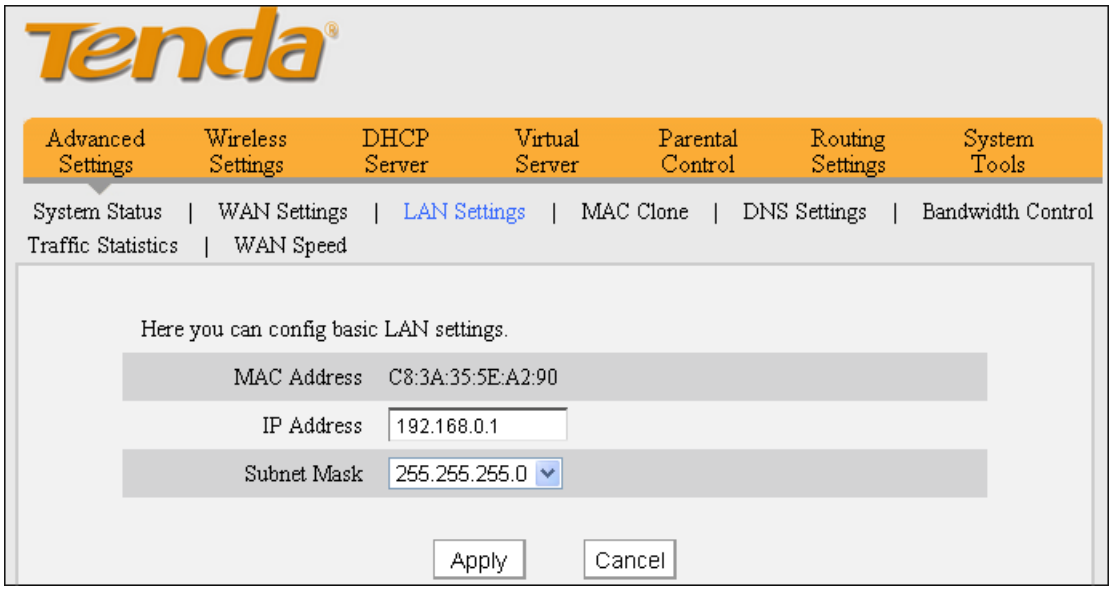
IP Address: The IP address provided by your ISP. Inquire your local ISP if you are not clear.

Subnet mask: The subnet mask provided by your ISP.

MTU: Maximum Transmission Unit. The default value is 1492.

4.3 LAN Settings

Click Advanced Settings-> LAN Settings to enter below screen.



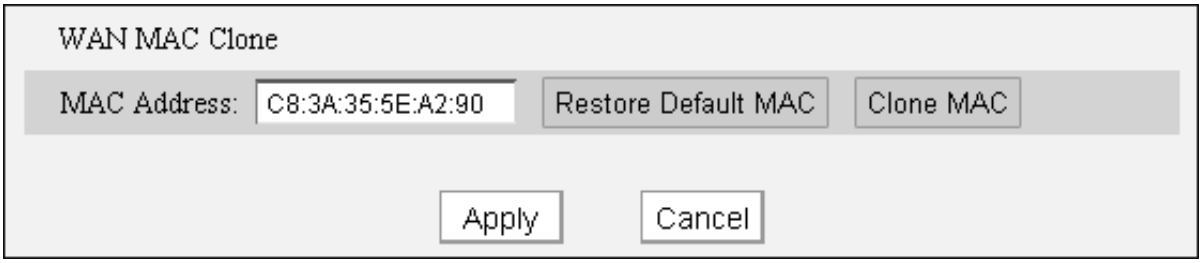
MAC Address: Displays MAC address of LAN interface, which is NOT changeable.
IP Address: Router's LAN IP address. The default is 192.168.0.1. You can change it according to your need.
Subnet Mask: Device's LAN subnet mask, 255.255.255.0 by default.

⚠ **Note:**

If you change the device's LAN IP address, please renew the IP information of the computer that connect to the router to login to the web management page.

4.4 MAC Clone

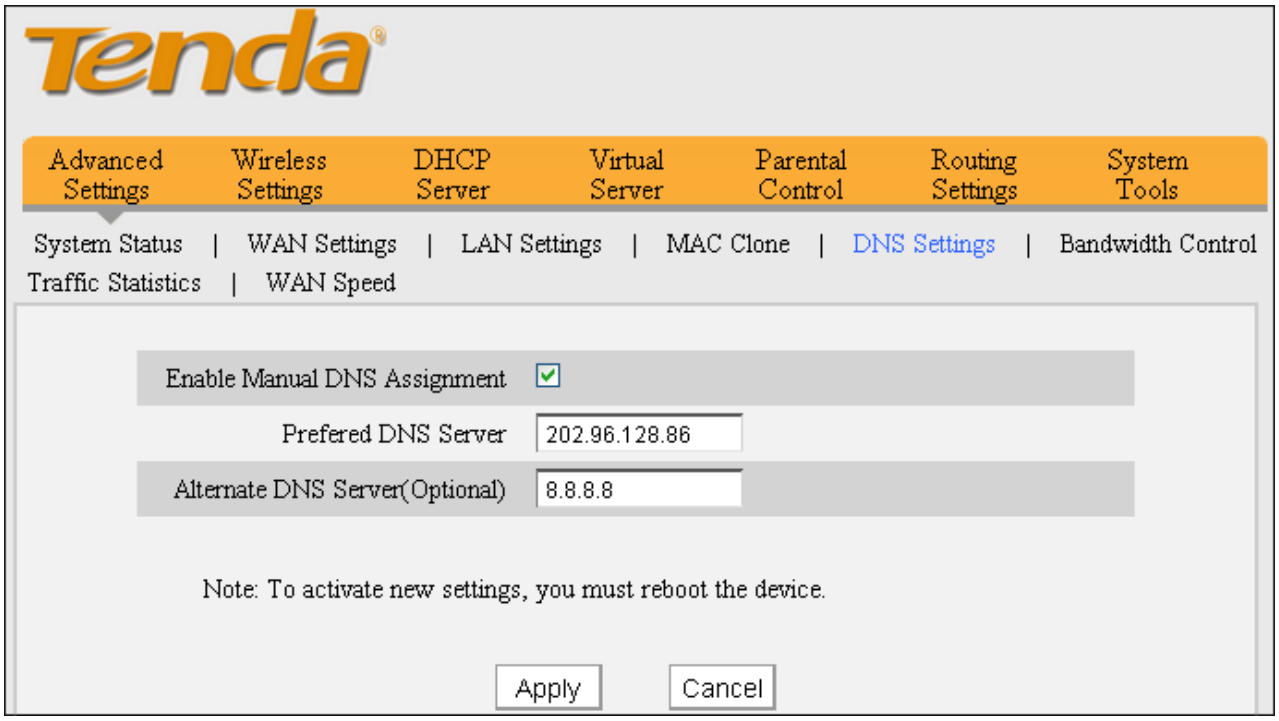
This section allows you to configure MAC address of router's WAN interface. Normally you don't need to change the default WAN MAC value. However, some ISP may bind client PC's MAC address for Internet connection authentication. In this case, simply enter such MAC in the WAN MAC Address field or use the MAC clone function.



MAC Address: The MAC address of router's WAN interface.
Clone MAC: Click this button to clone your PC's MAC address to the router's WAN interface.
Restore to Factory Default MAC: Reset router's WAN interface's MAC to factory default.

4.5 DNS Settings

DNS is short for Domain Name System or Domain Name Service.



Enable Manual DNS Assignment: Check to activate DNS settings.

Preferred DNS Server : Enter the Preferred DNS Server address provided by your ISP.

Alternate DNS Server (Optional)**:** Enter the Alternate DNS Server address if your ISP provides(optional).

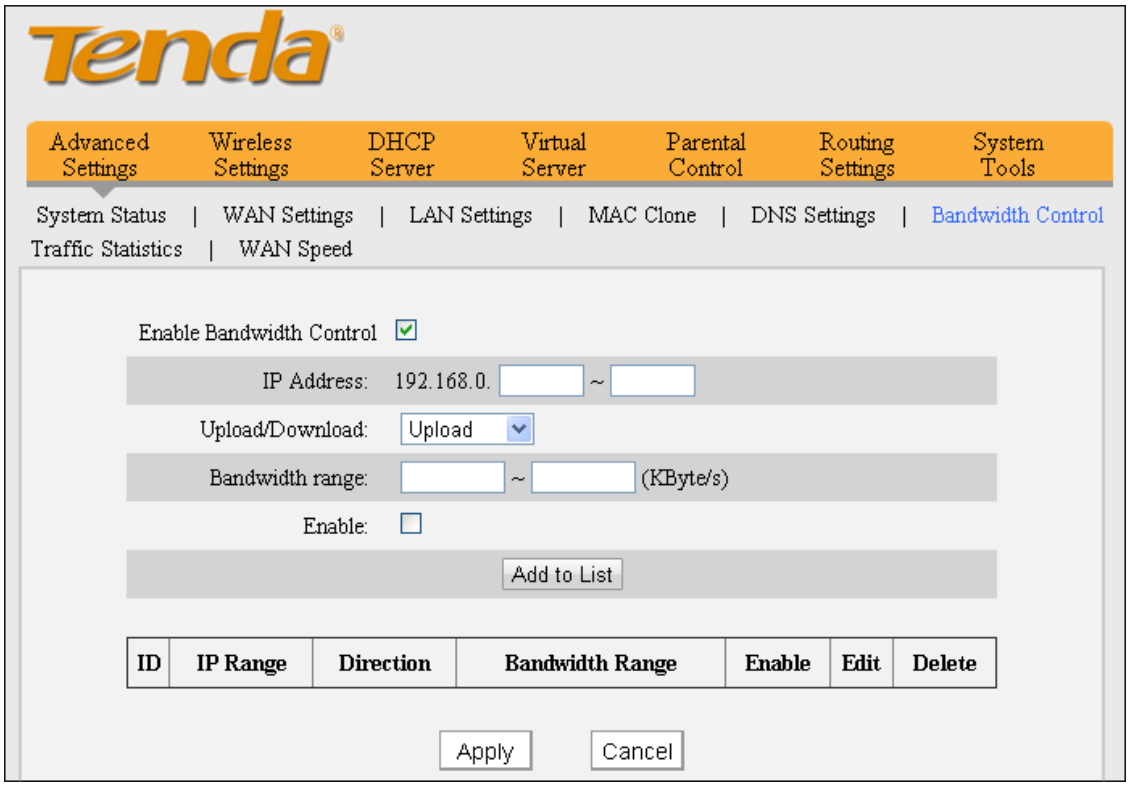
⚠ **Note:**

The websites can't display if DNS server address is wrong.

Do remember to restart the device to activate new settings when they completed.

4.6 Bandwidth Control

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



Enable Bandwidth Control: Check or uncheck the box to enable or disable the bandwidth control feature. This option is disabled by default.

IP Address: Enter the same IP or two different IP addresses in both boxes to specify a single IP address or an IP range to which the current bandwidth control rule will apply.

Upload/Download: Select to control bandwidth over data upload or download traffic.

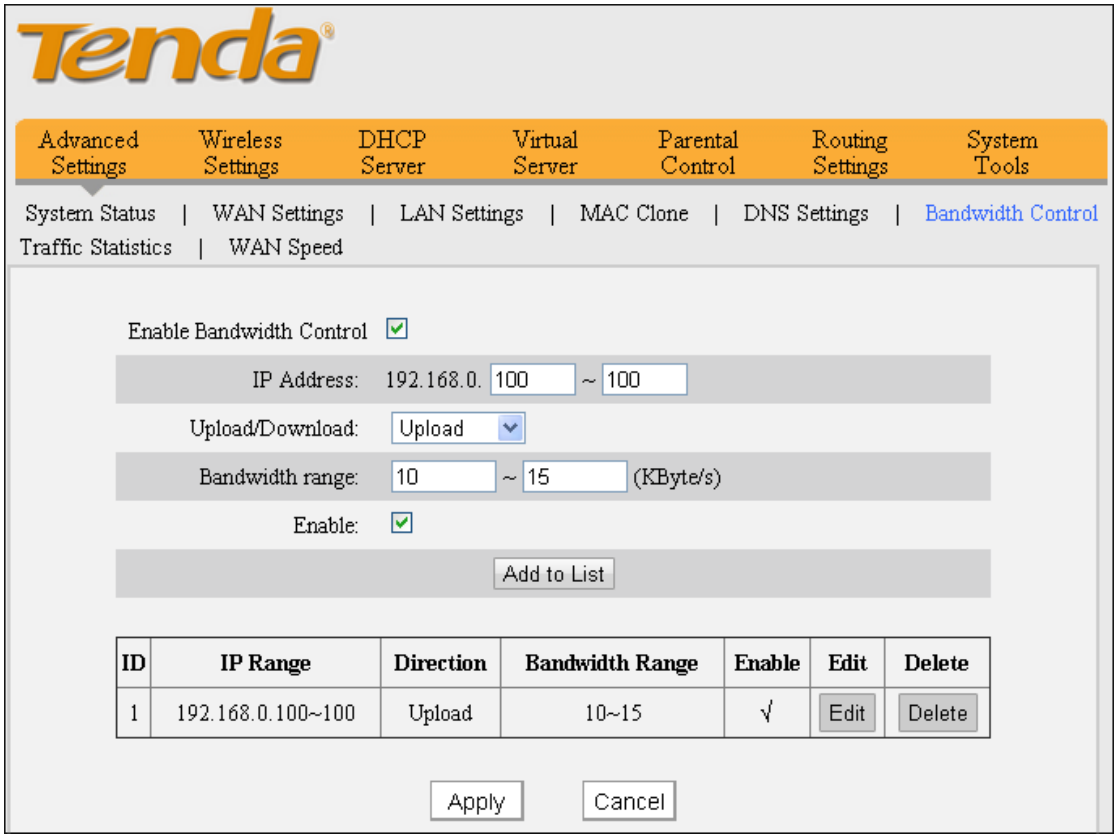
Bandwidth Range: Set a upload/download bandwidth limit on PCs within a specified IP range. Note that maximum upload/download bandwidth should not exceed your router's WAN bandwidth limit. (Consult your ISP if you are not clear.)

Enable: Check/uncheck to enable/disable current entry. When disabled, corresponding entry will not take effect though existing in fact.

Add to List: Click to add current bandwidth control rule to the rule list.

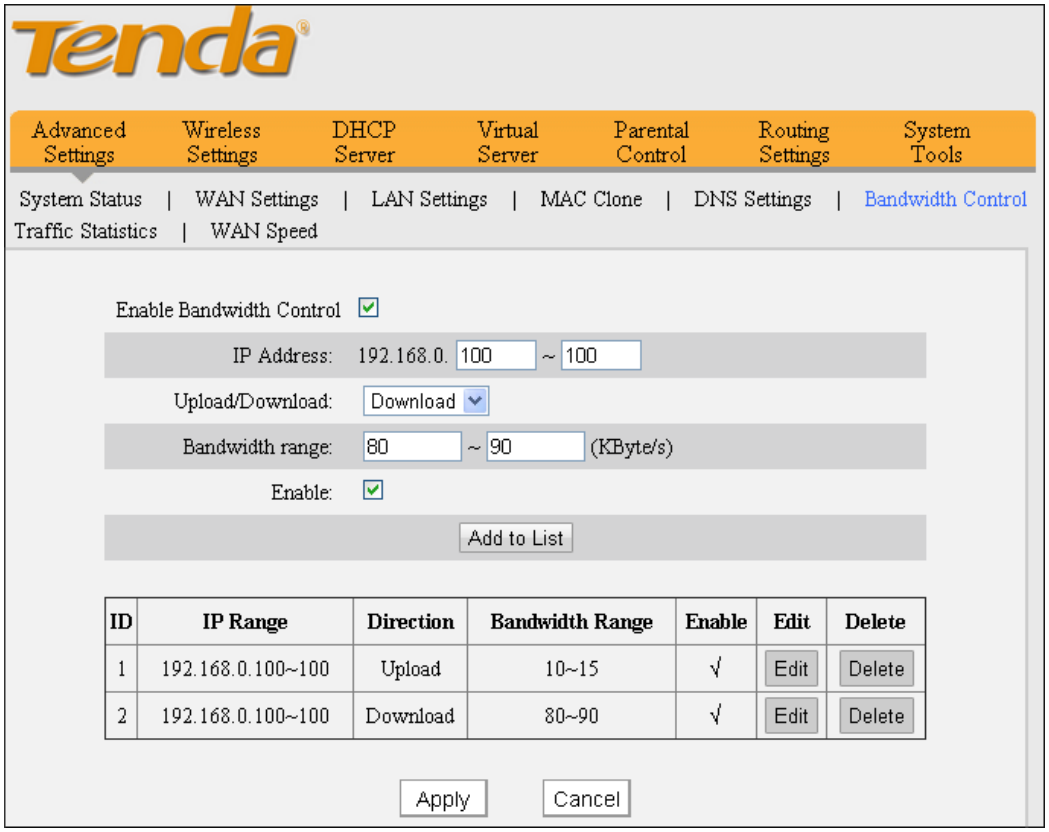
For a 2M broadband service, you may download and upload data at speeds up to 2Mbps (256KByte/) and 512kbps (64KByte/s) in theory respectively.

Example 1: To let the PC at the IP address of 192.168.0.100 to upload data at speeds of 10-15KByte/s and download data at speeds of 80-90KByte/s.
To add an upload bandwidth control rule, do as follows:

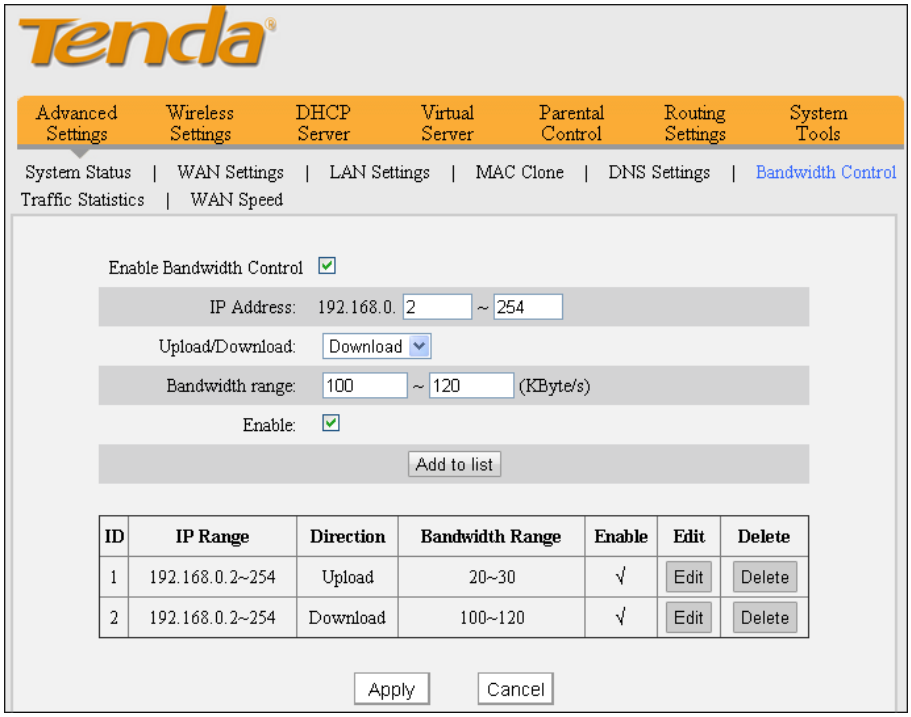


1. Input "192.168.0.100" in corresponding IP Address fields.
2. Select Upload.
3. Enter "10" and "15" in corresponding bandwidth fields.
4. Check "Enable".
5. Click "Add to List".
6. Click Apply.

And then add a download bandwidth control rule as seen below.

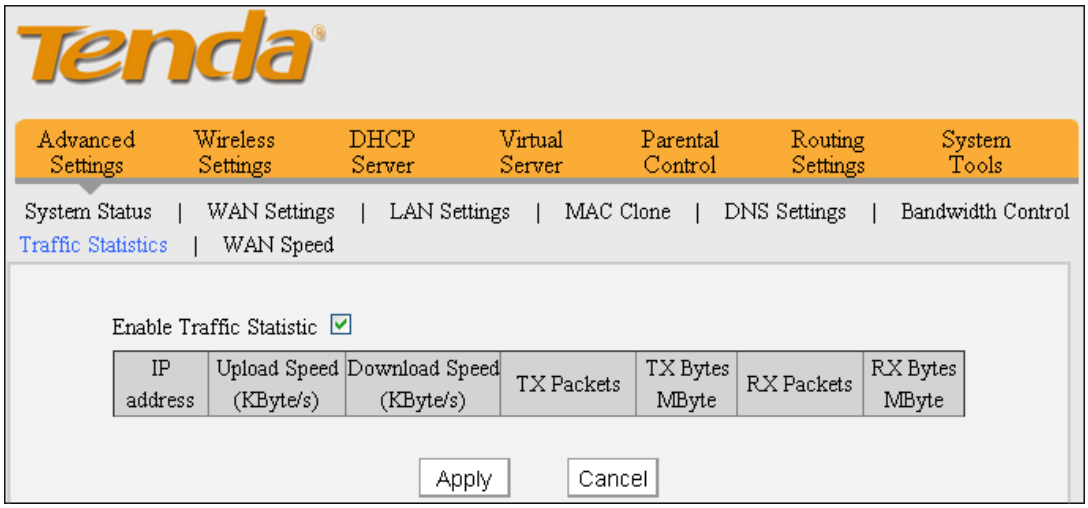


Example 2: To let PCs within the IP address range of 192.168.0.2-192.168.0.254 to upload data at speeds of 20-30KByte/s and download data at speeds of 100-120KByte/s, follow instructions above.



4.7 Traffic Statistics

Traffic Statistics allows you to see at a glance how much traffic each device in your network is using.



Enable Traffic Statistics: Check/uncheck the box to enable/disable the Traffic Statistics feature. To see at a glance how much traffic each device in your network is using, enable this option. However usually, disabling it may boost your network performance. This option is disabled by default. However, once enabled the page refreshes every five minutes.

IP Address: Displays the IP address of a corresponding PC.

Upload Speed: Displays the upload speed (KByte/s) of a corresponding PC.

Download Speed: Displays the download speed (KByte/s) of a corresponding PC.

TX Packets: Displays the number of packets sent by a corresponding PC via the device since Statistics is enabled.

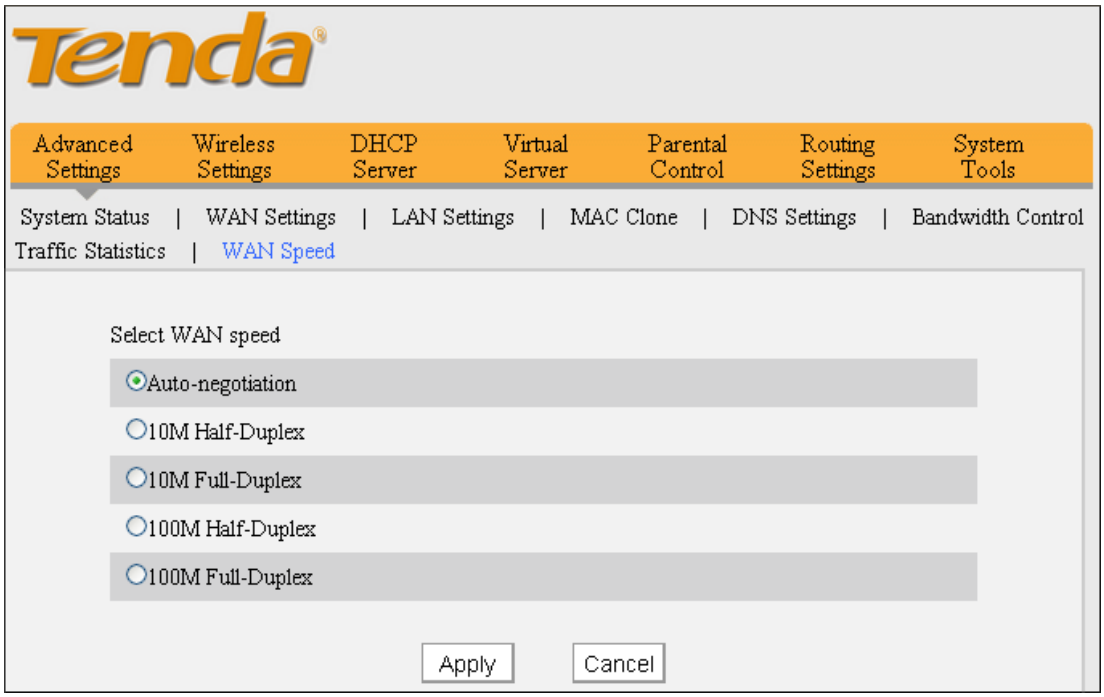
TX Bytes: Displays the number of Bytes sent by a corresponding PC via the device since Statistics is enabled. The unit is MByte.

RX Packets: Displays the number of packets received by a corresponding PC via the device since Statistics is enabled.

RX Bytes: Displays the number of Bytes received by a corresponding PC via the device since Statistics is enabled. The unit is MByte.

4.8 WAN Speed

Here you can set the speed for WAN port. It is advisable to keep the default "Auto" setting to get the best speed.

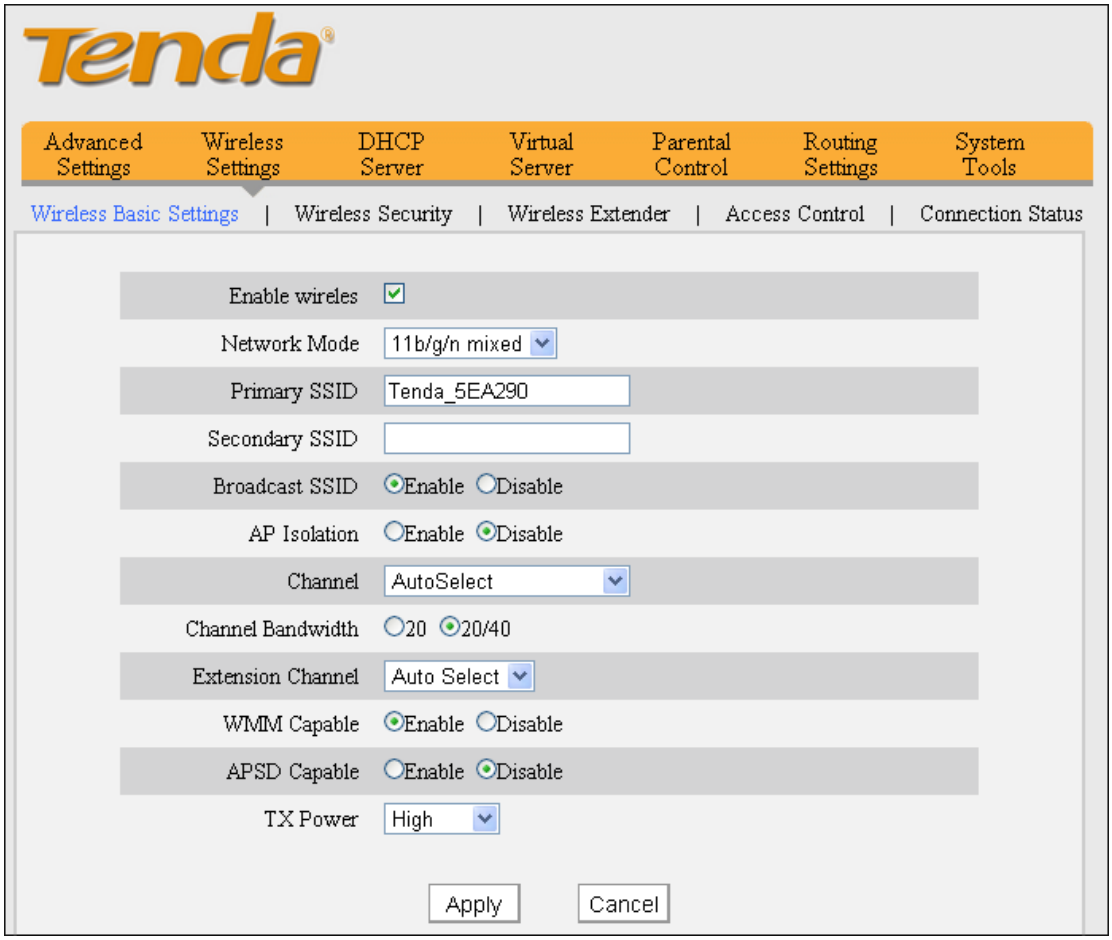


⚠ **Note:**

Aging and the length of Ethernet cable may reduce its transmission capability. In this case select 10M Full Duplex or the mode specified by the ISP from the Speed/Duplex drop-down list to improve performance.

Chapter 5 Wireless Settings

5.1 Wireless Basic Settings



Enable Wireless: Check/uncheck to enable/disable the 2.4GHz wireless feature. If disabled, all wireless-based features will be disabled accordingly.

Network Mode: Select a right mode according to your wireless client devices. The default mode is 11b/g/n mixed.

11b mode: Select it if you have only 11b wireless devices in your wireless network.

11g mode: Select it if you have only 11g wireless devices in your wireless network.

11b/g mixed mode: Select it if you have 11b and 11g wireless devices in your wireless network.

11b/g/n mixed mode: Select it if you have 11b, 11g and 11n wireless devices in your wireless network.

Primary SSID: A SSID (Service Set Identifier) is the public name of a wireless network. This option is configurable and can't be empty.

Secondary SSID: This is alternate public name of a wireless network. This option is configurable and can be empty.

SSID Broadcast: This option is enabled By default. 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, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.

AP Isolation: Disabled by default. When enabled, wireless clients can't share file or communicate with the wireless client connect to the same SSID.

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 20/40M frequency band; when there are only non-11n wireless clients, select 20M frequency band mode.

Extension Channel: Available only in 11b/g/n mixed mode. It is used to ensure N speed for 802.11n devices on the network.

WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data such as video or audio (recommended).

ASPD Capable: Select to enable/disable the auto power saving mode. By default, this option is disabled.

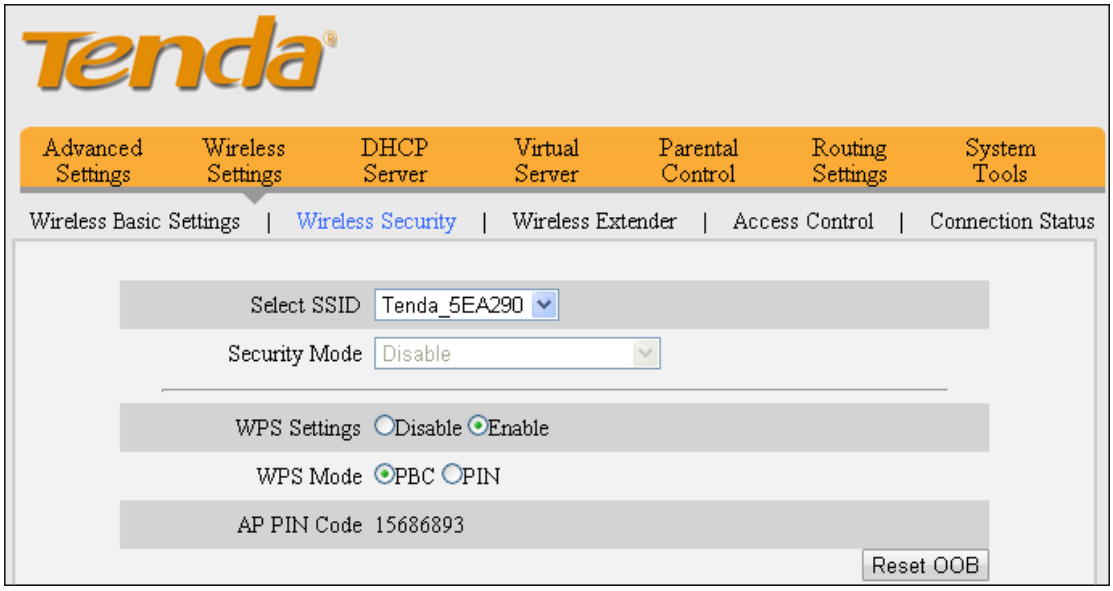
TX Power: Select a proper power level (High, Medium, Low) for optimal performance.

5.2 Wireless Security

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

5.2.1 WPS

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



WPS: Select to enable/disable the WPS feature. This option is disabled by default.

WPS Mode: Select PBC (Push-Button Configuration) or PIN.

PBC: To use the PBC option, select it and click "Save"; Then press the WPS button on router's back panel for about one second while enabling WPS >PBC on the intended wireless client simultaneously.

Operation Instructions:

PBC: If you find the WPS LED blinking for 2 minutes after you press the hardware WPS button on the device for 1 second, it means that PBC encryption method is successfully enabled. And an authentication will be performed between your router and the WPS/PBC-enabled wireless client device during this time; if it succeeds, the wireless client device connects to your router, and the WPS LED displays a solid light. Repeat steps mentioned above if you want to add more wireless client devices to the device.

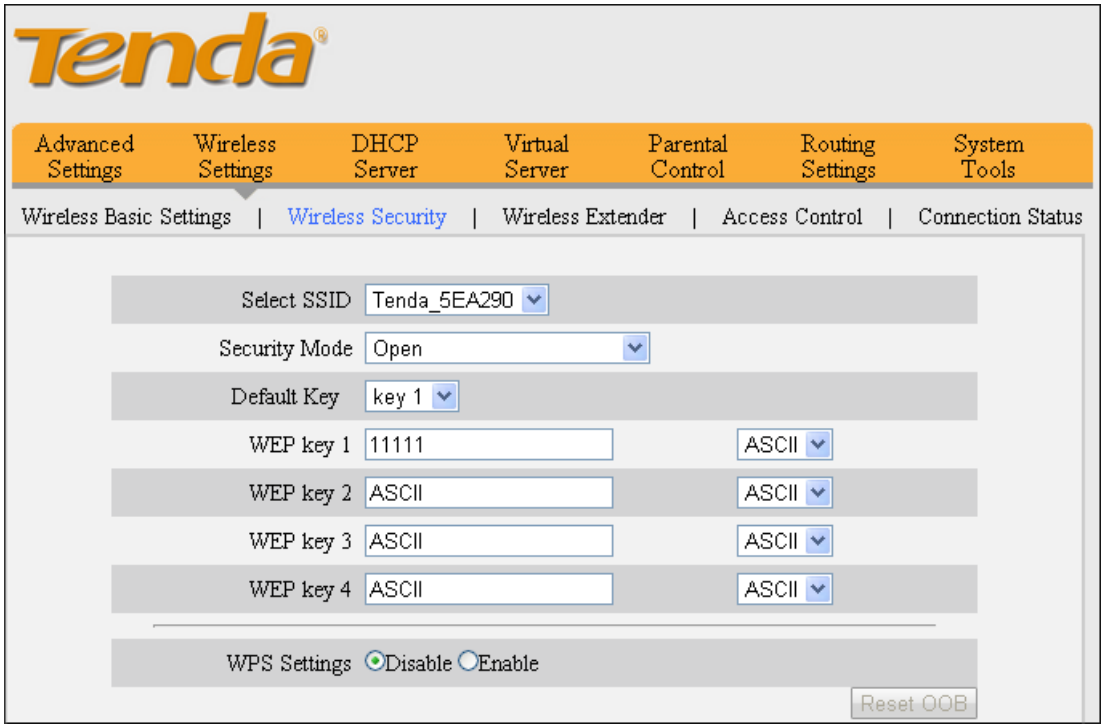
PIN: To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

Reset OOB: Wireless module will be reset if clicked.

⚠ **Note:To use the WPS security, the wireless client must be also WPS-capable.**

5.2.2 WEP

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

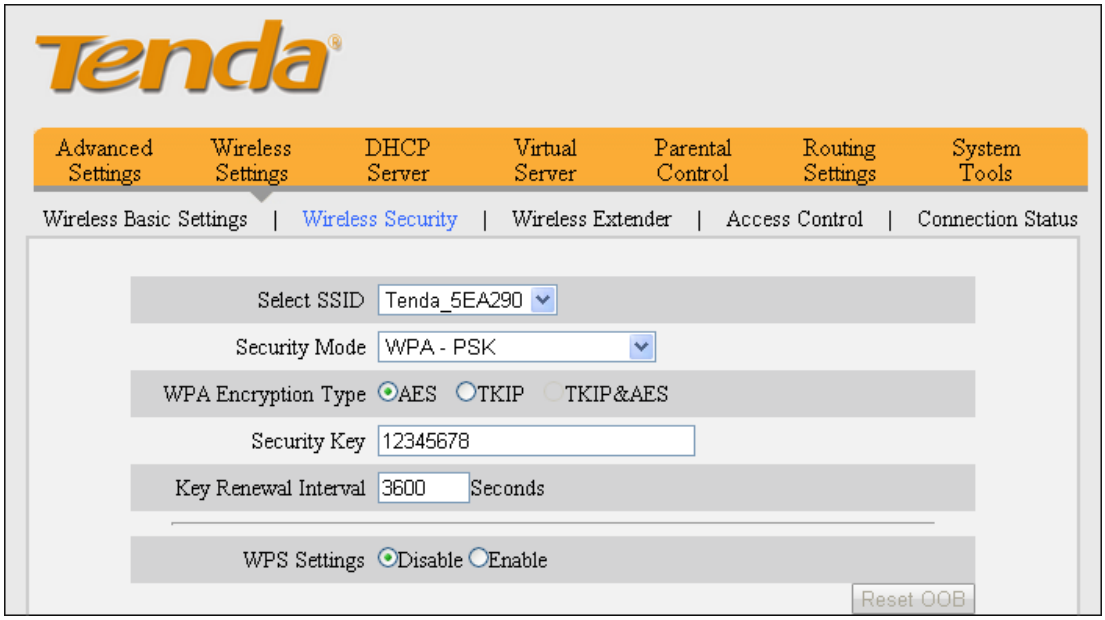


Security Mode: Select a proper security mode from the drop-down list.

Default Key: Select a key from the preset keys 1-4 for current use.

5.2.3 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.



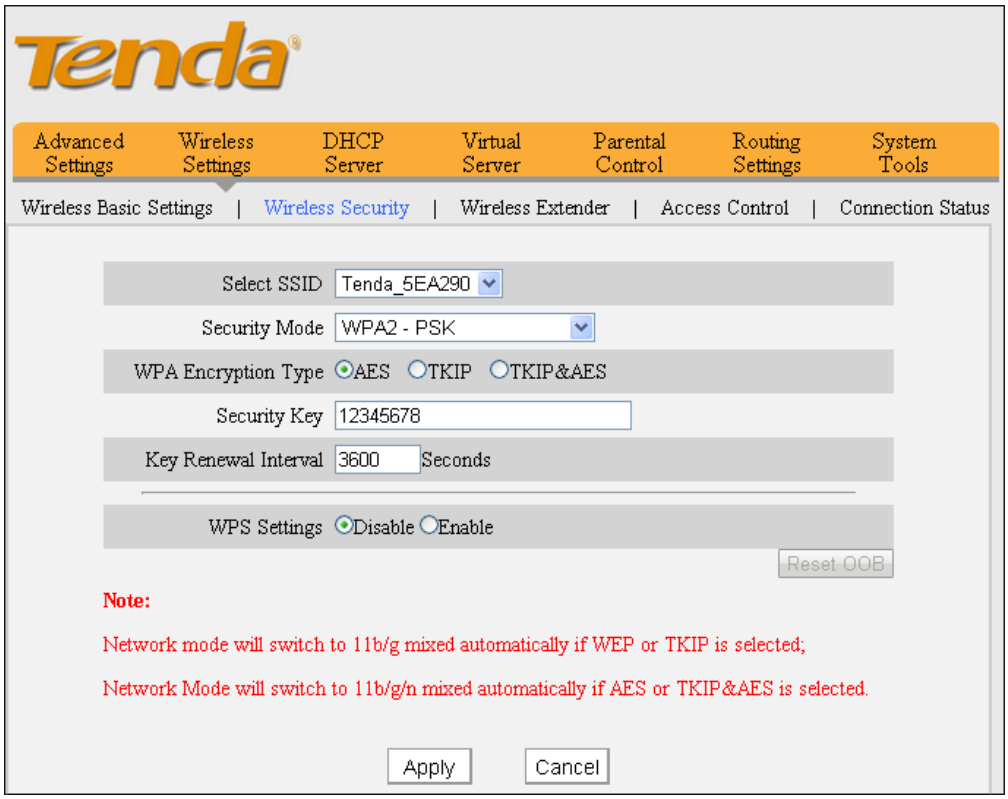
WPA Encryption Type: Select AES (advanced encryption standard) or TKIP (temporary key integrity protocol).

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.

5.2.4 WPA2-PSK

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



WPA Encryption Type: Select one encryption 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.

5.2.5 Mixed WPA/WPA2-PSK

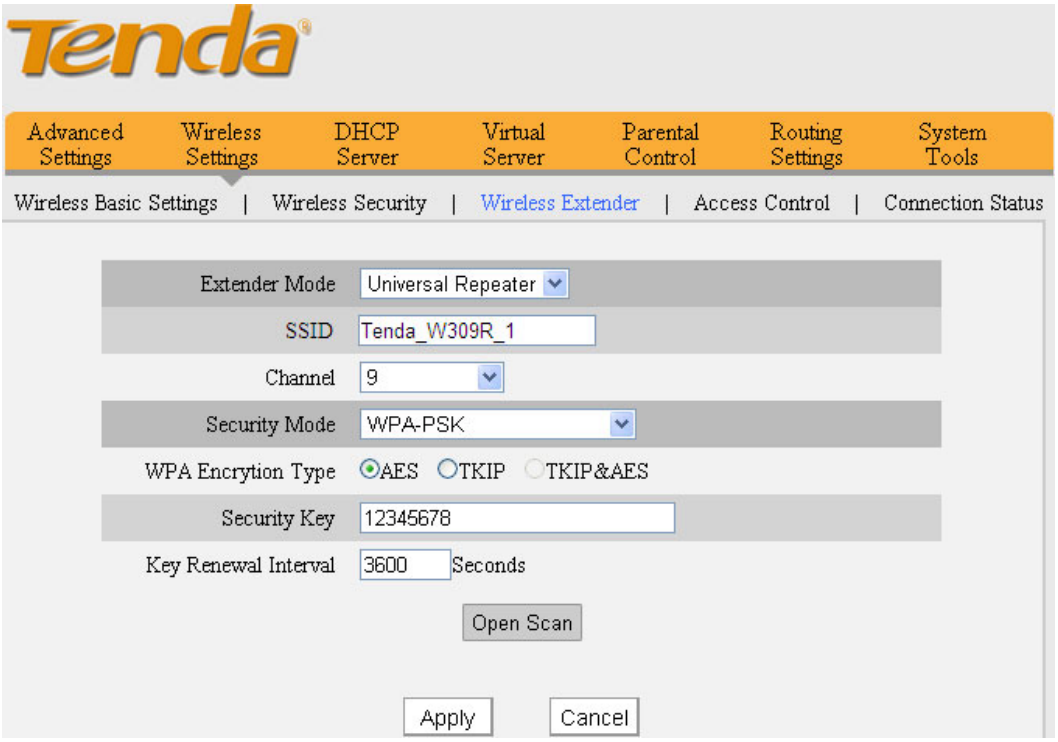
The mixed WPA/WPA2-PSK security mode includes WPA-PSK and WPA2-PSK. To use this mode, follow instructions on WPA2-PSK section.

5.3 Wireless Extender

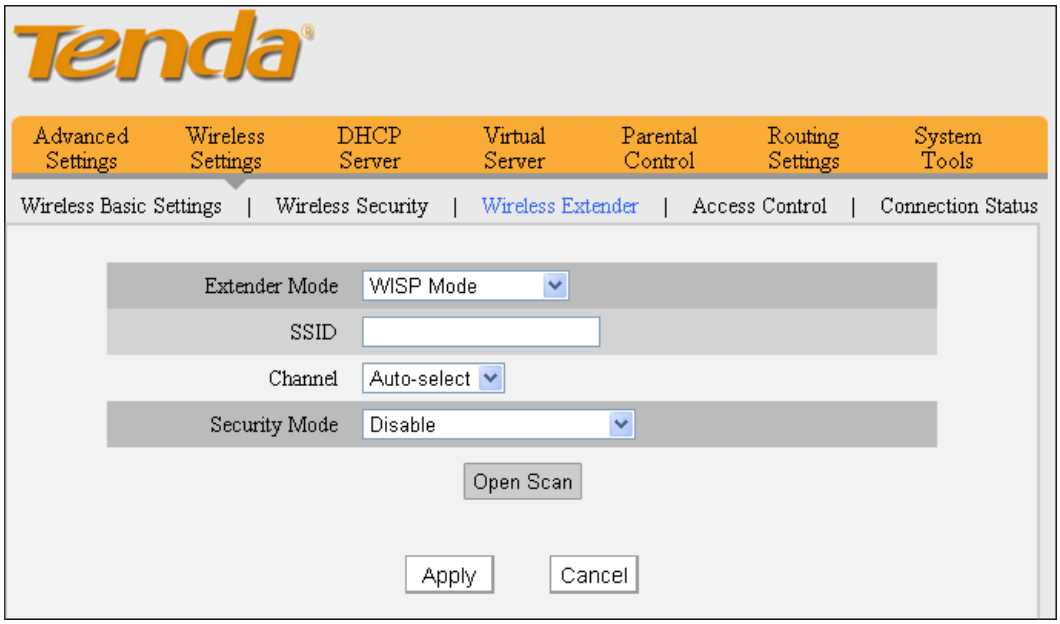
Here you can expand your wireless coverage with the following modes: Universal Repeater, WISP Client (Wireless WAN) and WDS.

5.3.1 Universal Repeater Mode

Universal Repeater: In this mode, the device will relay data to an associated root AP and AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. (The Universal Repeater mode differs from the WDS in terms that it requires only a one-way connection authentication.)



5.3.2 WISP Client Mode



SSID: The wireless name of the uplink wireless device.

Channel: The channel used by uplink wireless device.

Security Mode: The security mode and key used for connection to the uplink wireless device.

Open Scan: Click to search available wireless networks. Take two W3002R as

example to illustrate how to implement the WISP client feature.

Set the uplink device as below:

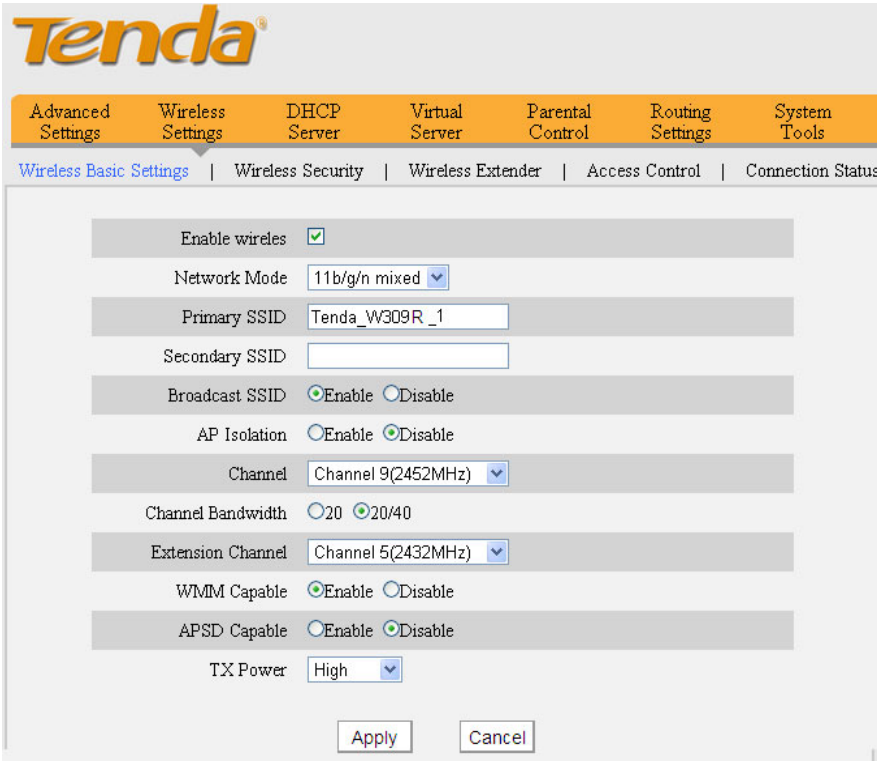
SSID: Tenda_W309R_1,

Chanel: 9

Security Mode: WPA-PSK

Security Key: 12345678

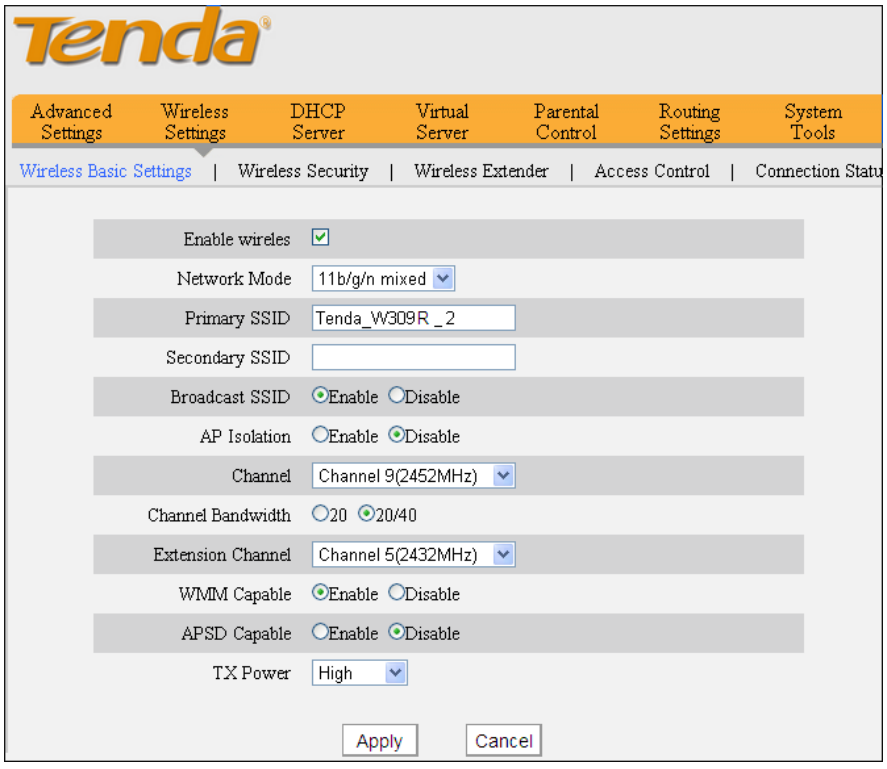
LAN IP address: 192.168.10.1.



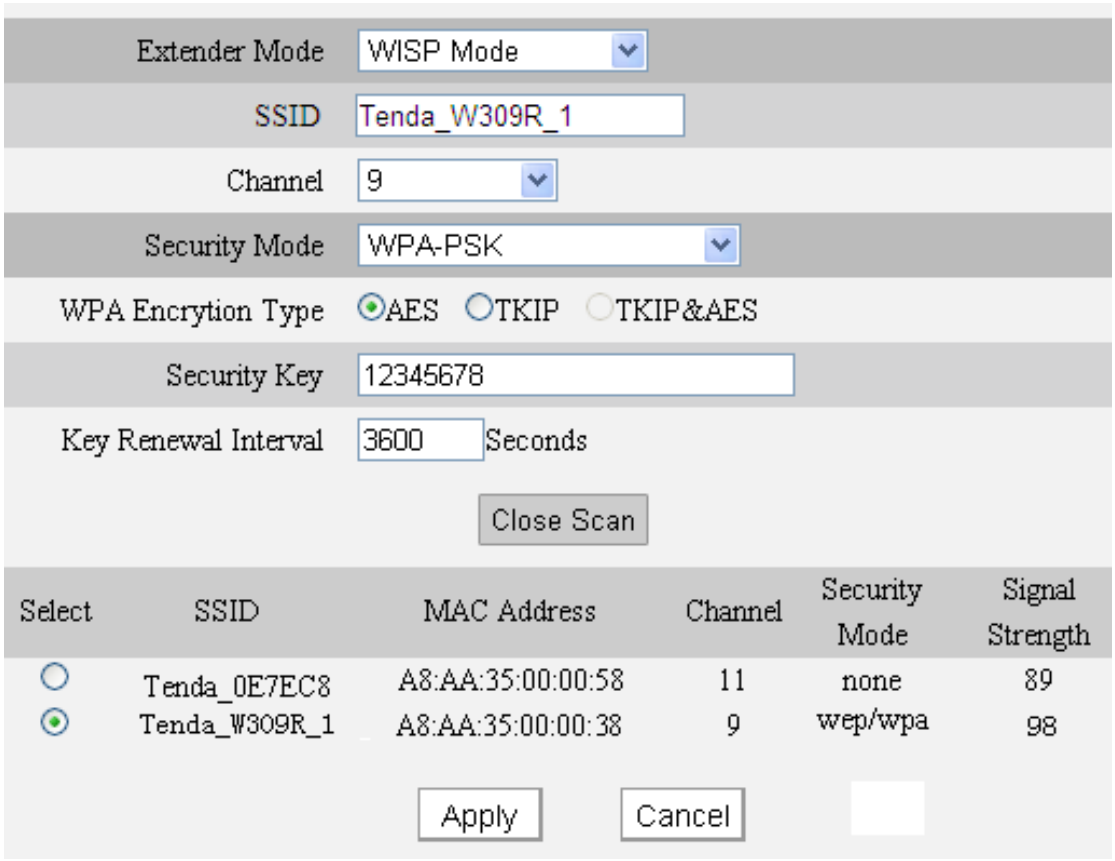
Set the Second W3002R as below:

SSID: Tenda_W309R_2,

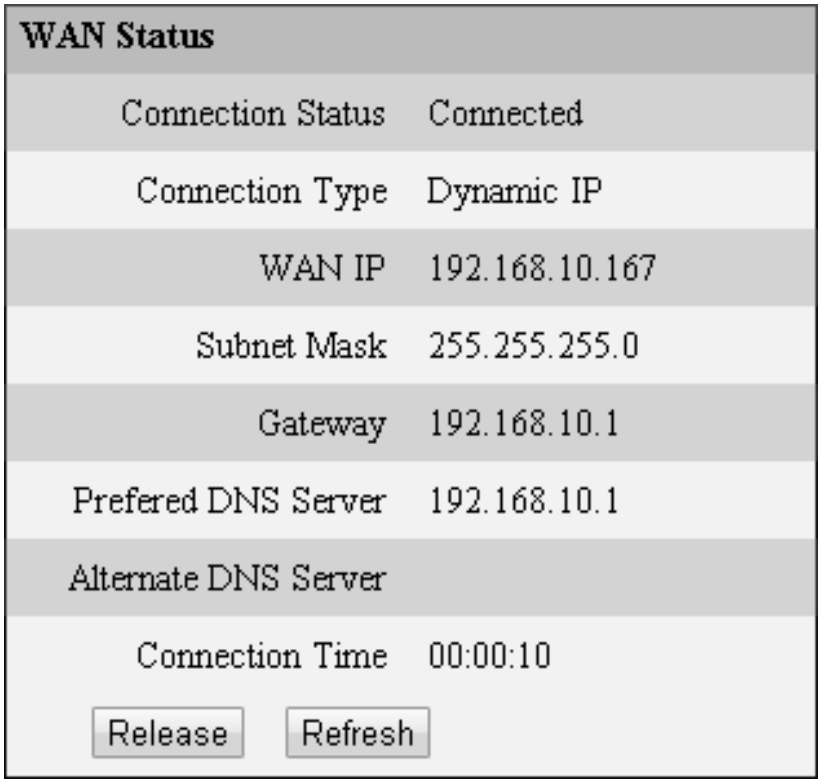
Chanel: 9



Scan the first W3002R's wireless signal (Tenda_W309R_1) on the second W3002R (WISP client device) or manually enter (Tenda_W309R_1).



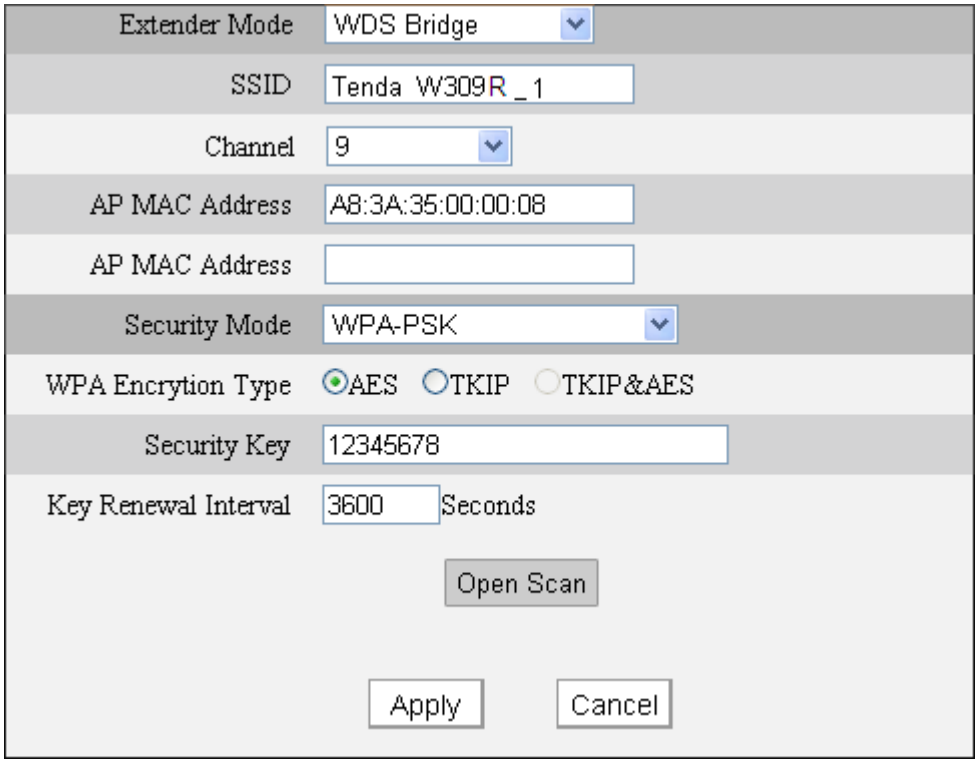
After finish the setting, you can check the ip address of the router's WAN port through view system status.



5.3.3 WDS

WDS Bridge Mode: wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.

Note: Both wireless Access Points MUST support WDS.



Extender Mode: Select a proper extender mode to use.

SSID: Enter the wireless network name of the wireless device you want to connect.

Channel: The channel on which the link partner device is currently operating.

AP MAC Address: Enter the MAC address of the wireless device you want to connect.

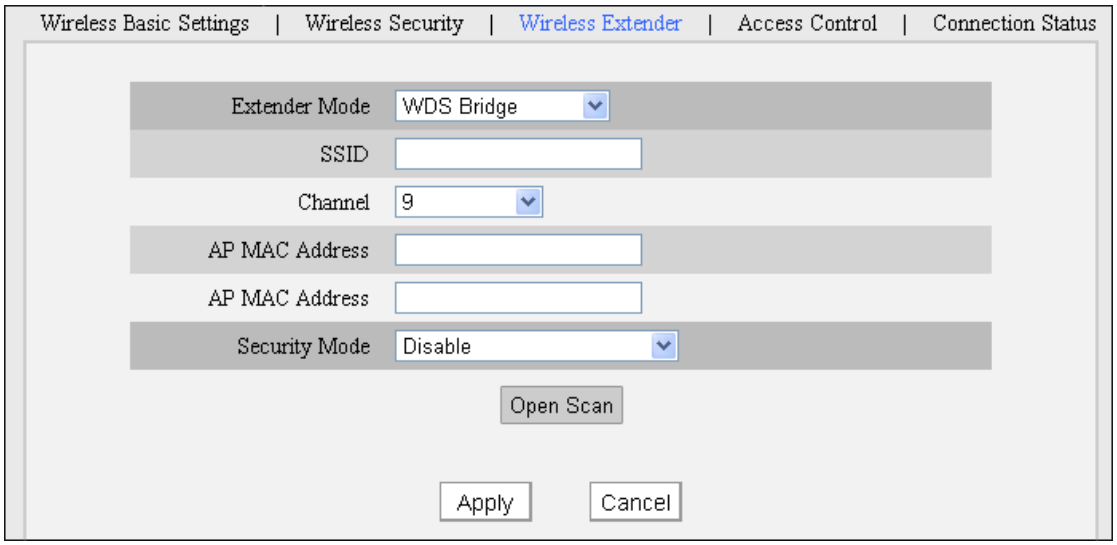
Security Mode: Select a security mode for the connection.

WPA Encryption Type: Select a proper encryption type.

Security Key: Enter a correct security key.

Take two W3002R as example to illustrate WDS implementation.

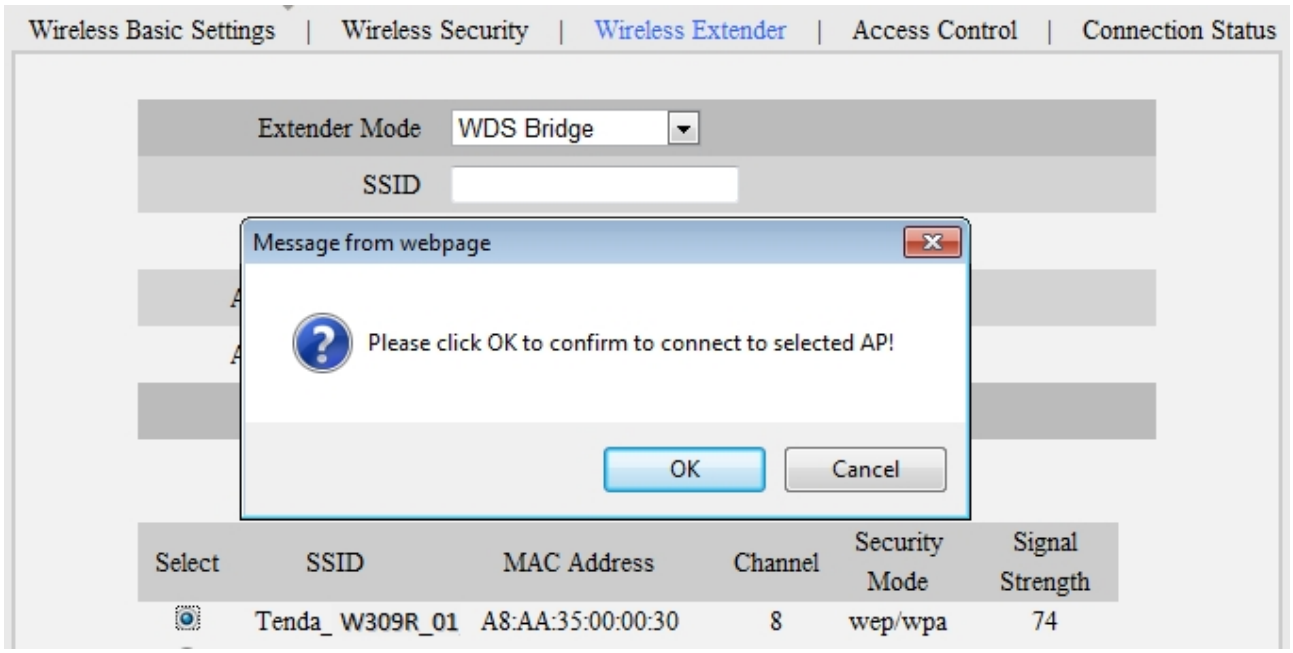
Choose WDS Bridge on both W3002R as seen below:



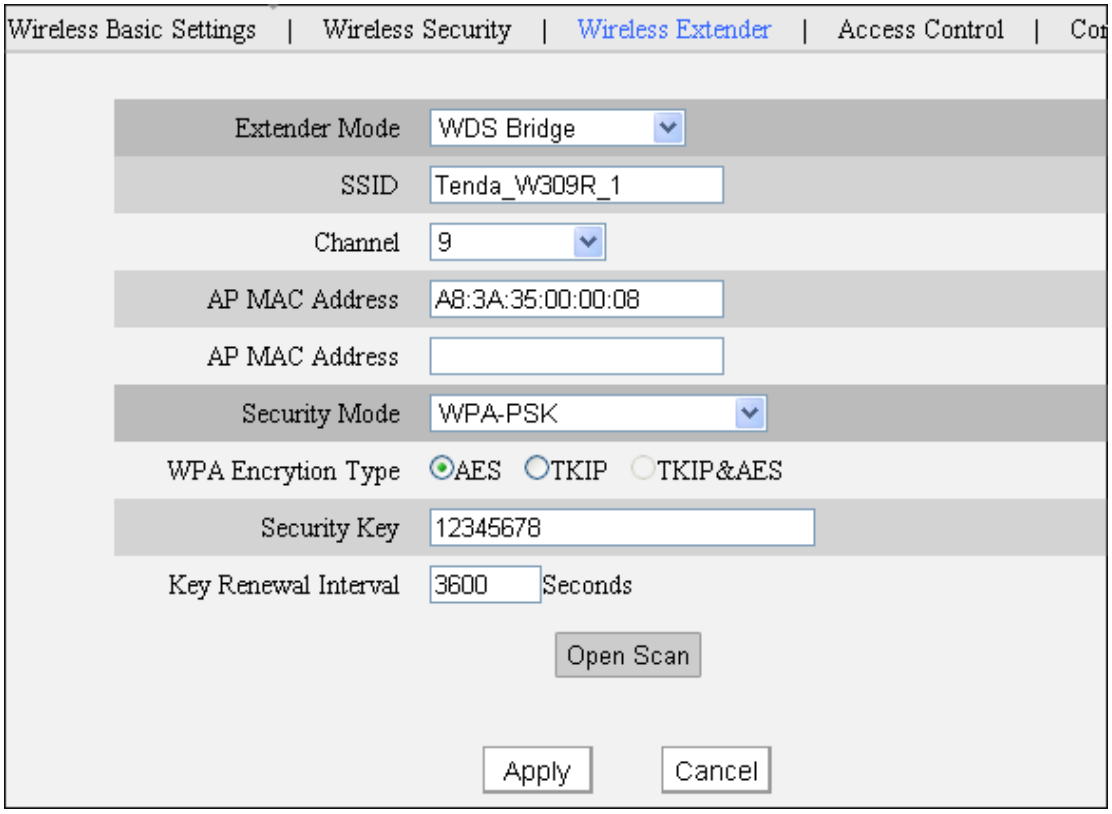
1 Directly enter the MAC address and SSID of the link partner if you already know them and then configure proper security settings.

2 Use the Open Scan button.

1) Click "Open Scan", select the desired wireless network and click OK. The MAC will then be added automatically.



2) Click OK as seen below.



Configure the same settings on the other W3002R the same way above.

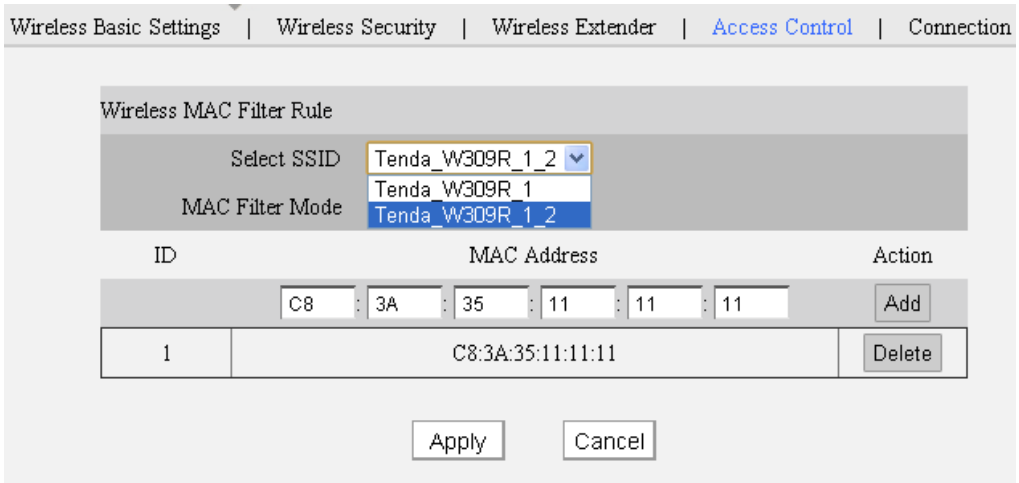
Both wireless devices involved must be entered each other's MAC address for successful WDS connection.

⚠ **Note:**

1. WDS feature can only be implemented between 2 WDS-capable wireless devices. Plus, SSID, channel, security settings and security key must be exactly the same on both such devices.

5.4 Access Control

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



Select SSID: Select primary SSID or secondary SSID for your filter rules to apply.

MAC Filter Mode: "Permit Only" only allows PCs at specified MAC addresses (in the list) to connect to your wireless network; Forbid Only: Only PCs at specified MAC addresses list can't connect to your wireless network.

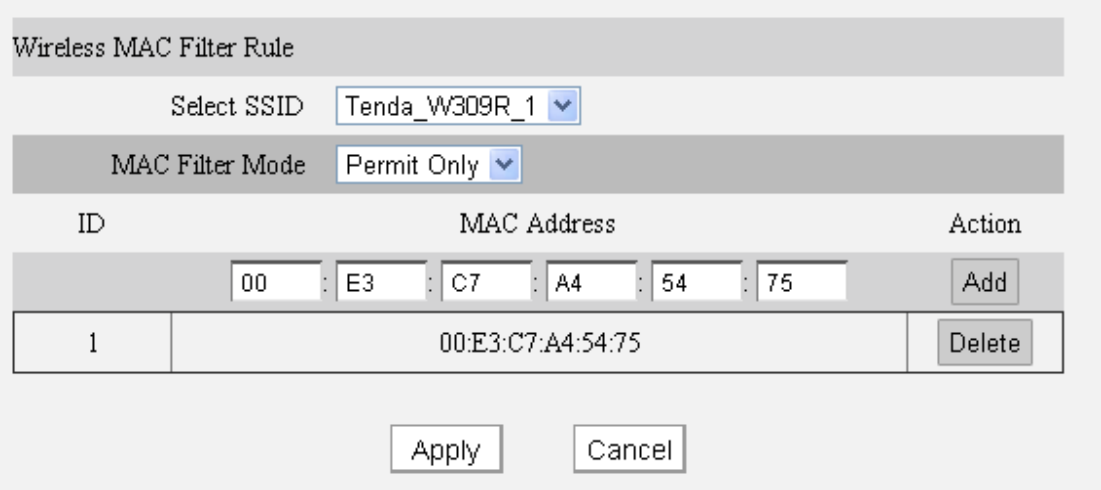
MAC Address: Enter the MAC address of a wireless client which you want to permit or forbid to connect your wireless network.

Add: Click to add the MAC address.

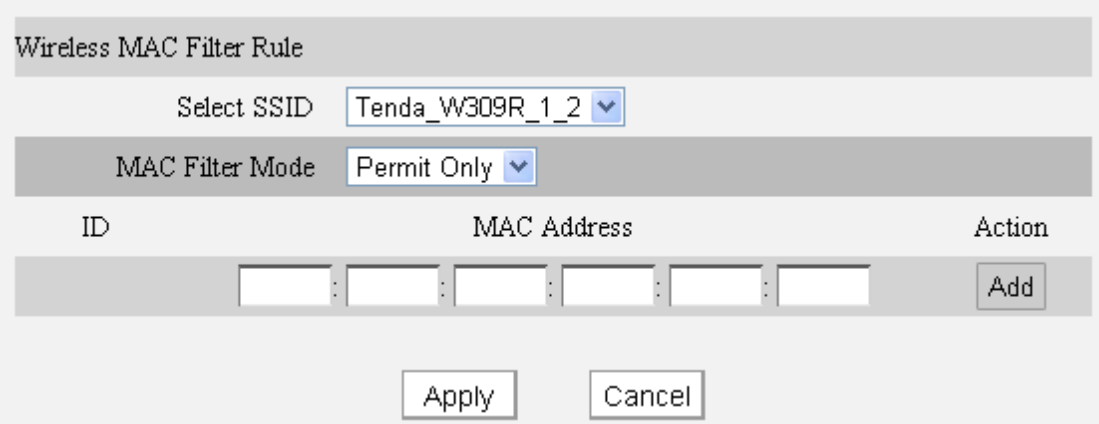
MAC Address List: Displays added MAC address entries. You can add new entries or delete existing entries according to your needs.

Example: To permit only a PC at the MAC address of 00:e3:c7:a4:54:75 to connect to your wireless network via the primary SSID, do as follows:

A) For the primary SSID: Tenda_W3002R_1, configure settings as seen on the screenshot below:

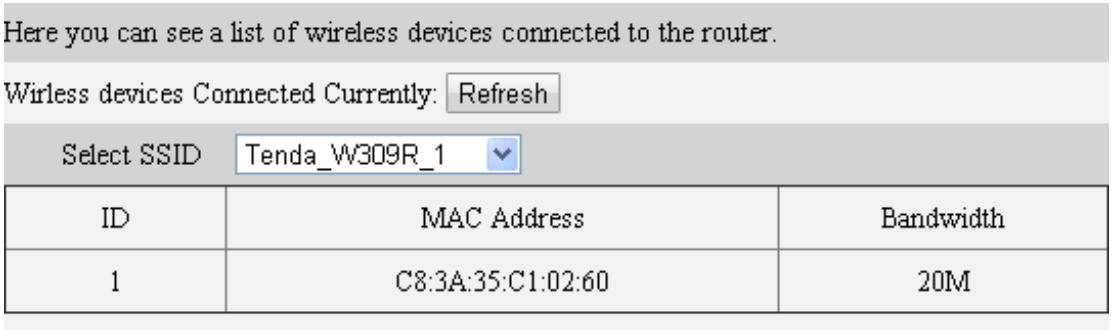


B) For the secondary SSID: Tenda_W309R_1_2, configure settings as seen on the screenshot below:



5.5 Connection Status

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



Select SSID: Select the SSID you want to view.

MAC Address: Displays MAC addresses of wireless clients connected to the router.

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

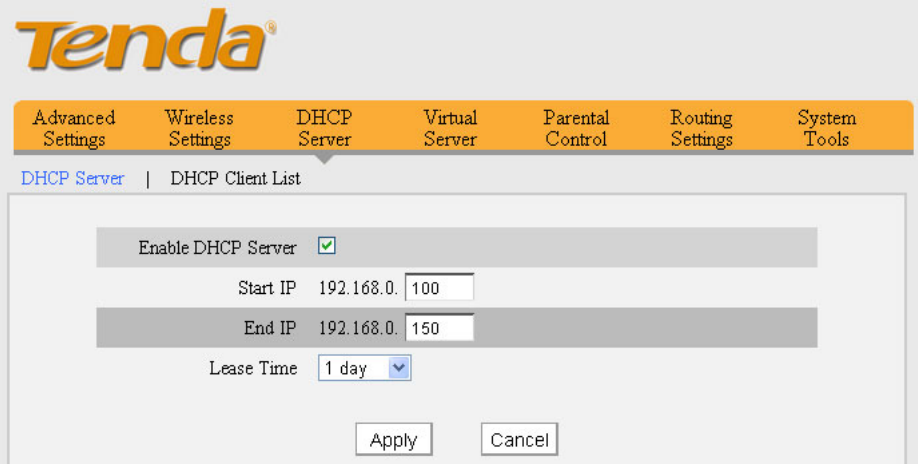
⚠ **Note:**

The bandwidth here refers to the channel bandwidth instead of wireless connection rate.

Chapter 6 DHCP

6.1 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 the device, it will automatically configure the TCP/IP settings for all your LAN computers (including IP address, subnet mask, gateway and DNS etc), eliminating the need of manual intervention. Just be sure to set all computers on your LAN to be DHCP clients by selecting "Obtain an IP Address Automatically" respectively on each such PC. When turned on, these PCs will IP information from the DHCP server.



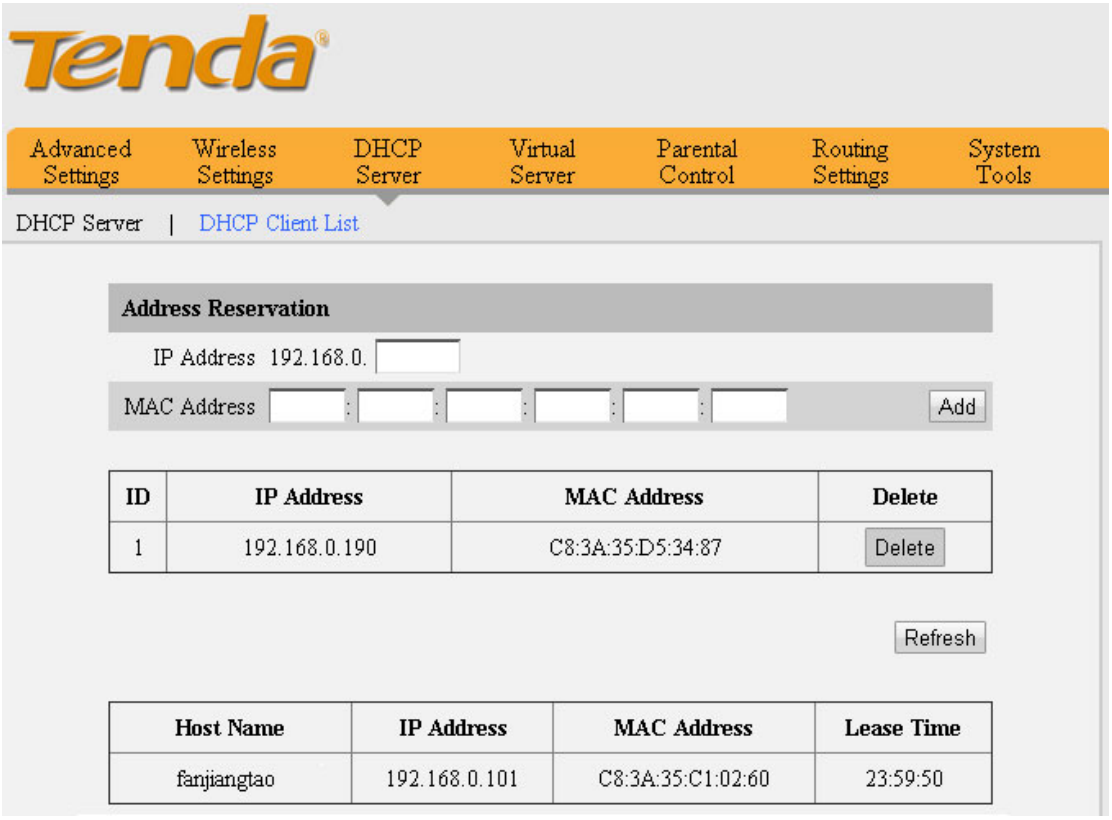
Enable DHCP Server: Check or uncheck the box to enable or disable the device's DHCP server feature.

Start/End IP: Enter the starting/ending IP address for the DHCP server's IP assignment.

Lease Time: The length of time for the IP address lease.

6.2 DHCP Client List

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 get the same IP addresses always, you can use this feature and manually add a static DHCP Reservation entry for each such device.



IP Address: Enter the IP address for static DHCP reservation.

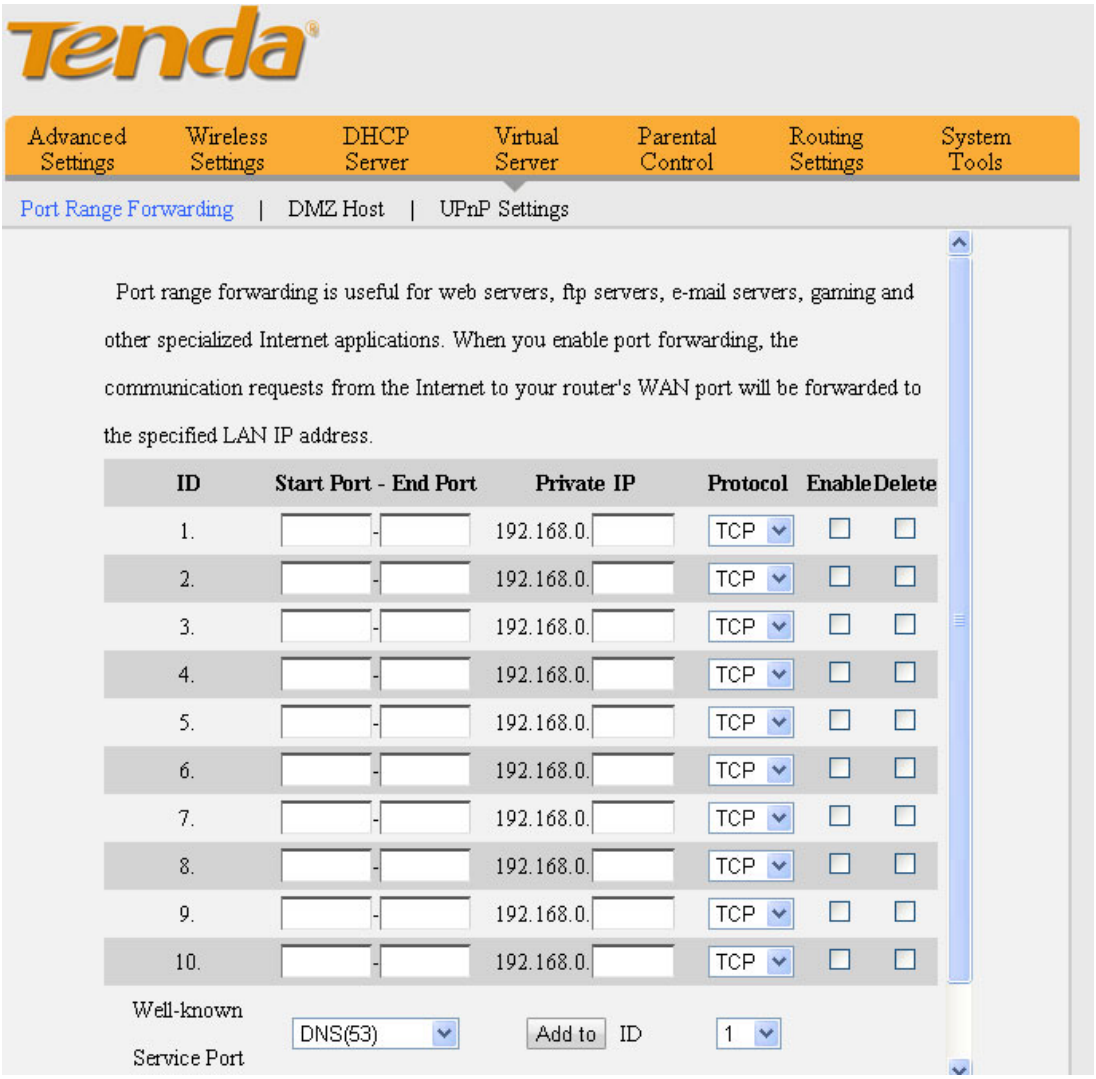
MAC Address: Enter the MAC address of a computer to always receive the same IP address (the IP you just specified).

Host Name: Displays host name of the PC that get IP address from the DHCP server.

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

Chapter 7 Virtual Server

7.1 Port Range Forwarding



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.

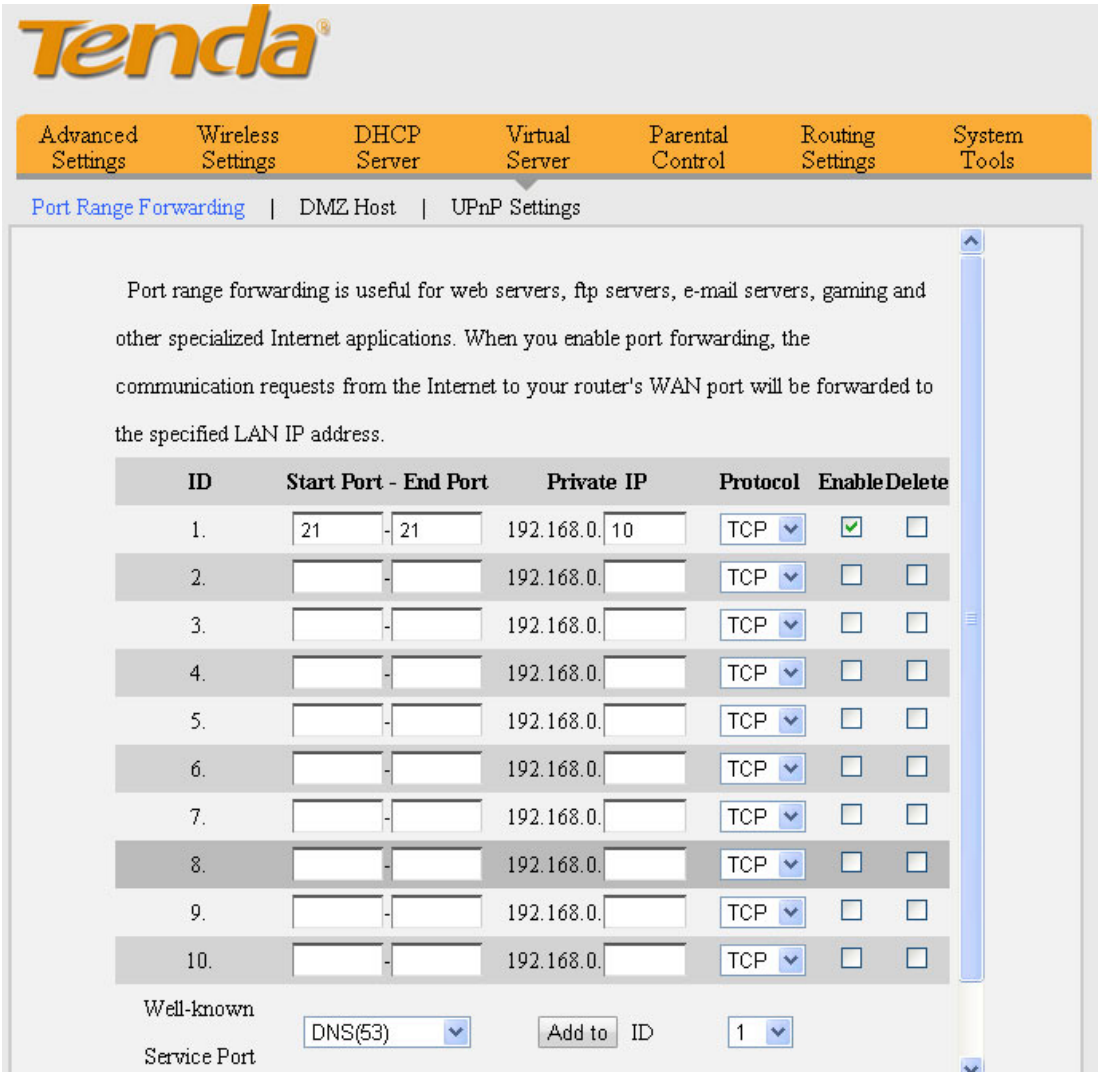
Delete: Click to remove a corresponding entry/rule.

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.

Example: You want to share some large files with your friends who are not in your LAN; however it is not convenient to transfer such large files across network. 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. Assuming that the static IP address of the FTP server (Namely, your PC) is 192.168.0.10, you want your friends to access this FTP server on the default port of 21 using the TCP protocol, then do as follows:

1． Enter 21 in both Start Port and End Port fields or select FTP from "Well-known Service Port" and an entry ID, 21 will be automatically populated to corresponding fields of the selected entry.

2． Enter 192.168.0.10 in the private field, select "TCP" and then select "Enable'.



3． Save your settings.

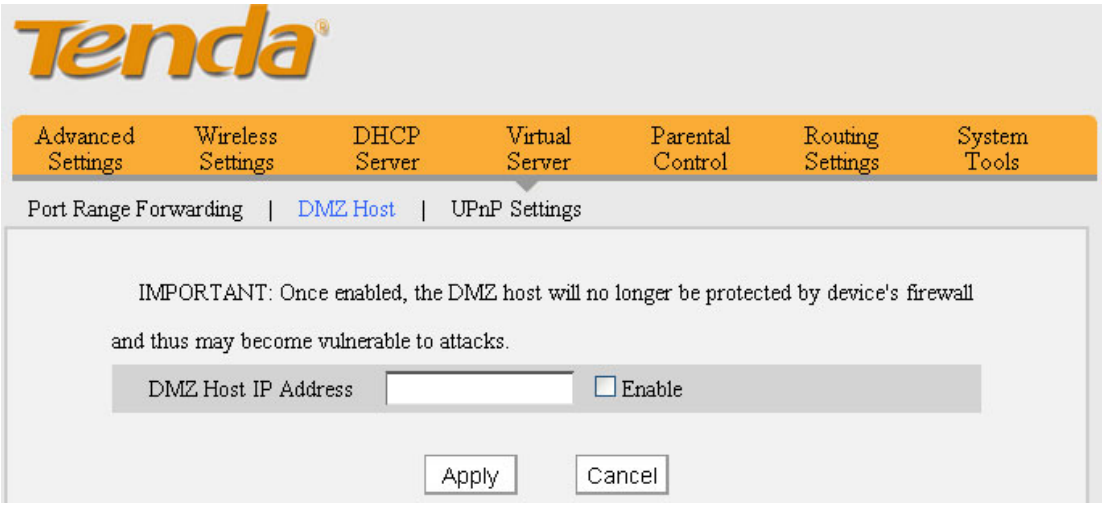
Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the router's WAN IP address. Assuming it is 172.16.102.89, then your friends need to enter "ftp://172.16.102.89: 21" in their browsers.

⚠ **Note:**

If you include port 80 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.

7.2 DMZ Host

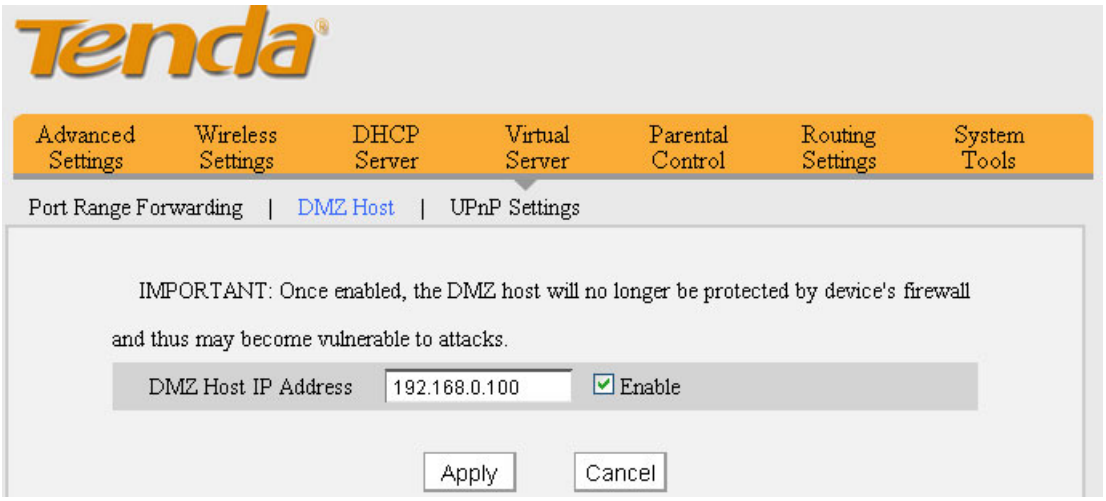
In some cases such as playing Internet games or holding video conferences, you may need to have your computer completely exposed to external networks for implementation of a bidirectional communication. To do so, set it as a DMZ host. Note that you should assign a static (fixed) IP address to the PC designated as a DMZ host (DHCP Server> DHCP Client List> DHCP Reservation (also known as Static Assignment on some products)) before using the feature. Enter the static IP address of the PC on your LAN which you want to set as a DMZ host. Enabling DMZ host may expose your local network to potential attacks. So it is advisable to use it with caution.



DMZ Host IP Address: Enter the IP address of computer on your LAN which you want to set to be DMZ host.

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

For example: To set a PC at 192.168.0.100 to a DMZ host for intercommunication with another host on the Internet, configure the same settings as shown on the screenshot on the device.

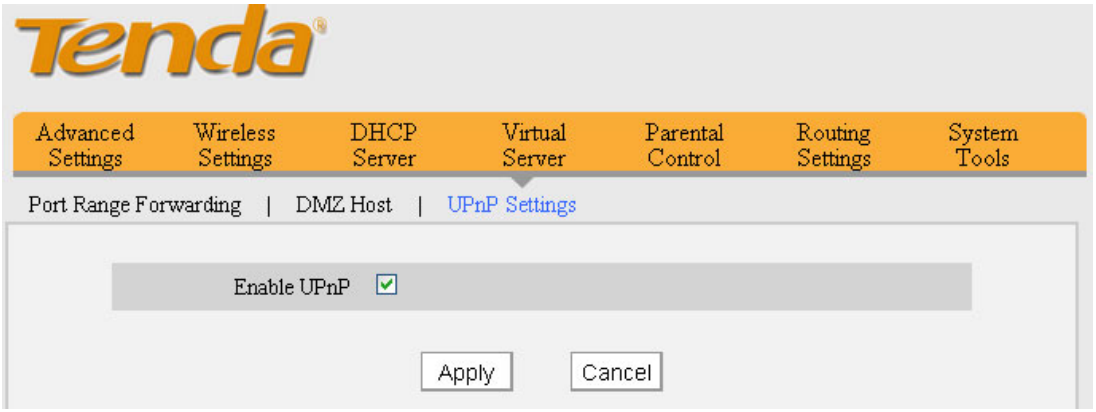


⚠ **Note:**

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

7.3 UPNP

The Universal Plug and Play (UPnP) feature allows network devices, such as computers from Internet, to access resources on local host or devices as needed. UPnP-enabled devices can be discovered automatically by the UPnP service application on the LAN.



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

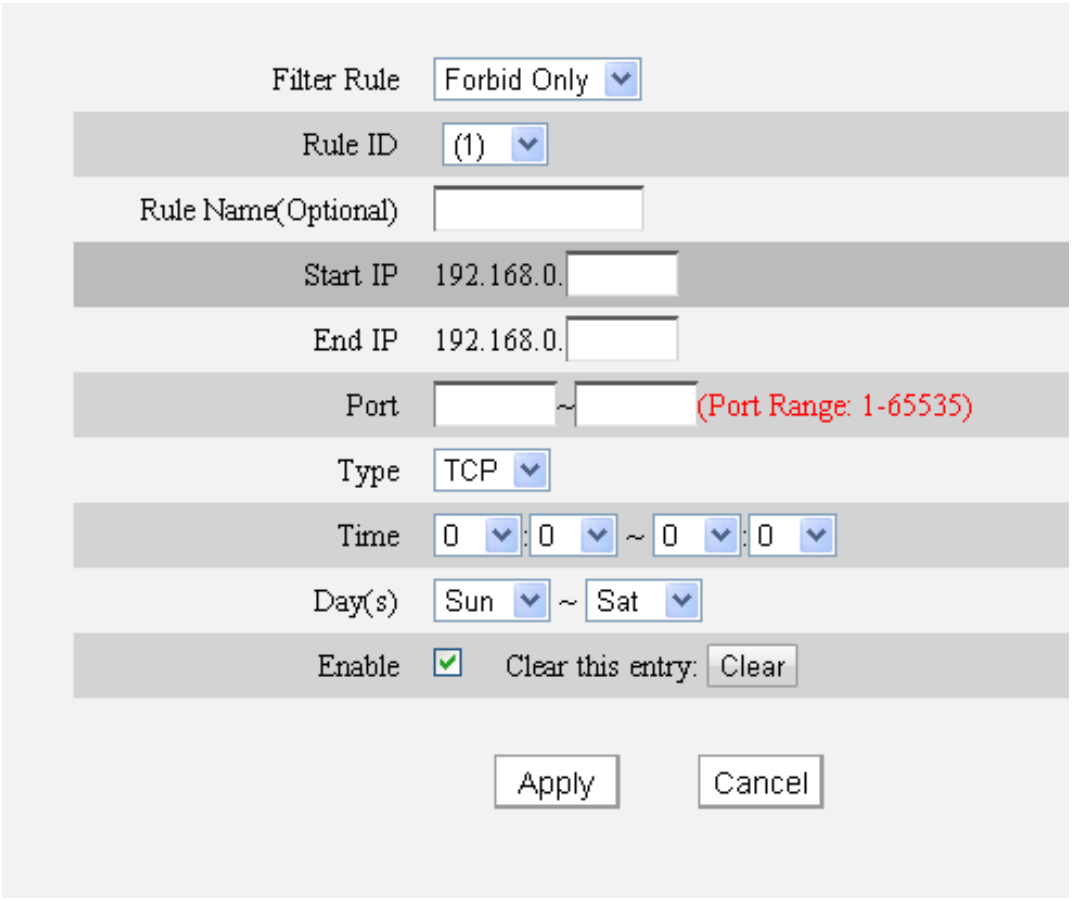
⚠ **Note:**

Note: UPnP works in Windows XP, Windows ME or later (NOTE: Operating system needs to be integrated with or installed with Directx 9.0) or in an environment with installed application software that supports UPnP.

Chapter 8 Parental Control

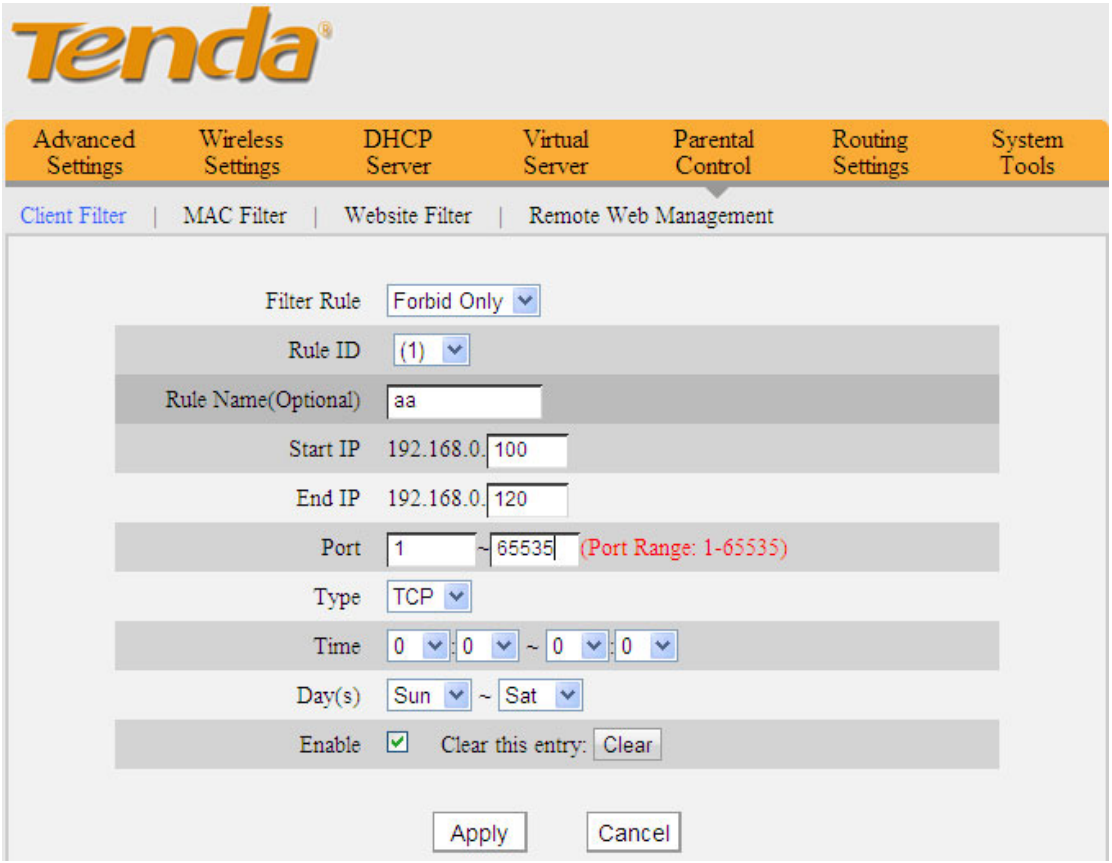
8.1 Client Filter

To better manage PCs in LAN, you can limit the time to access internet through the Client Filter.

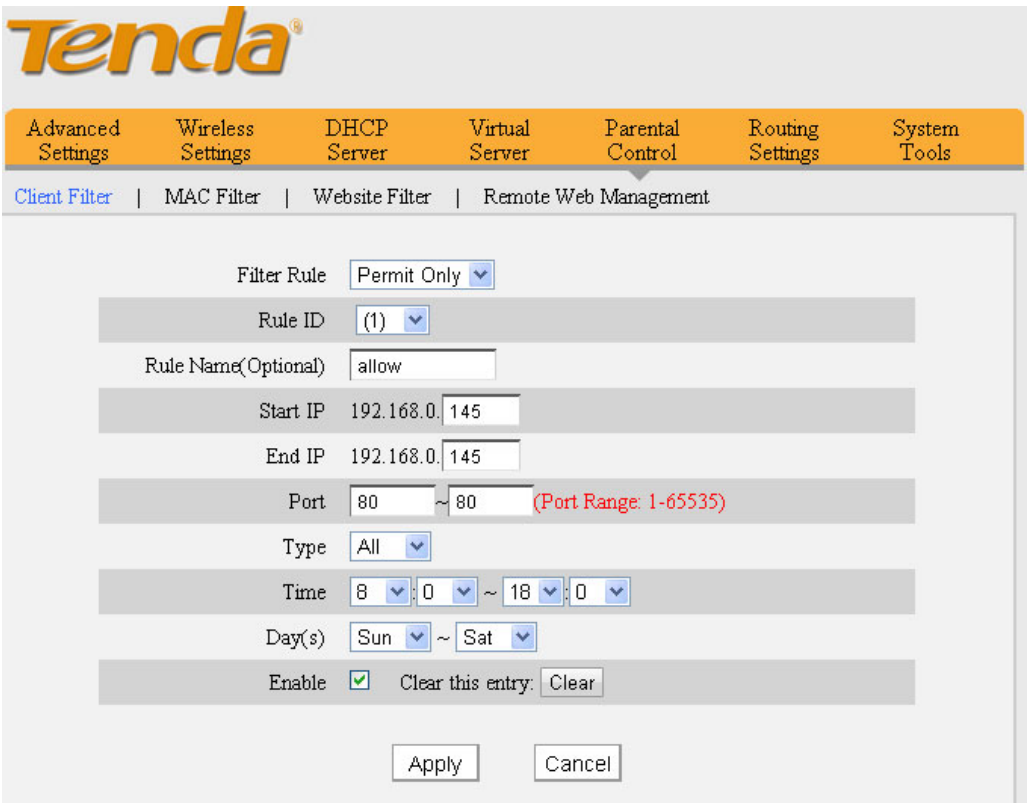


Filter Rule: Select Forbid Only or Permit Only.
Rule ID: Select a rule ID from the drop-down list.
Rule Name: Briefly describe the current entry/rule.
Start IP/End IP: Enter the same IP address or 2 different IP addresses in both boxes to specify a single PC or a range of PCs for current rule to apply to.
Port: Enter TCP/UDP protocol port number (s); it can be a range of ports or a single port.
Type (Protocol): 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 a current rule to take effect.
Enable: Check to enable or uncheck to disable a corresponding filter rule.

Example 1: If you want prohibit PCs within the IP address range of 192.168.0.100--192.168.0.120 access Internet, do as follows:

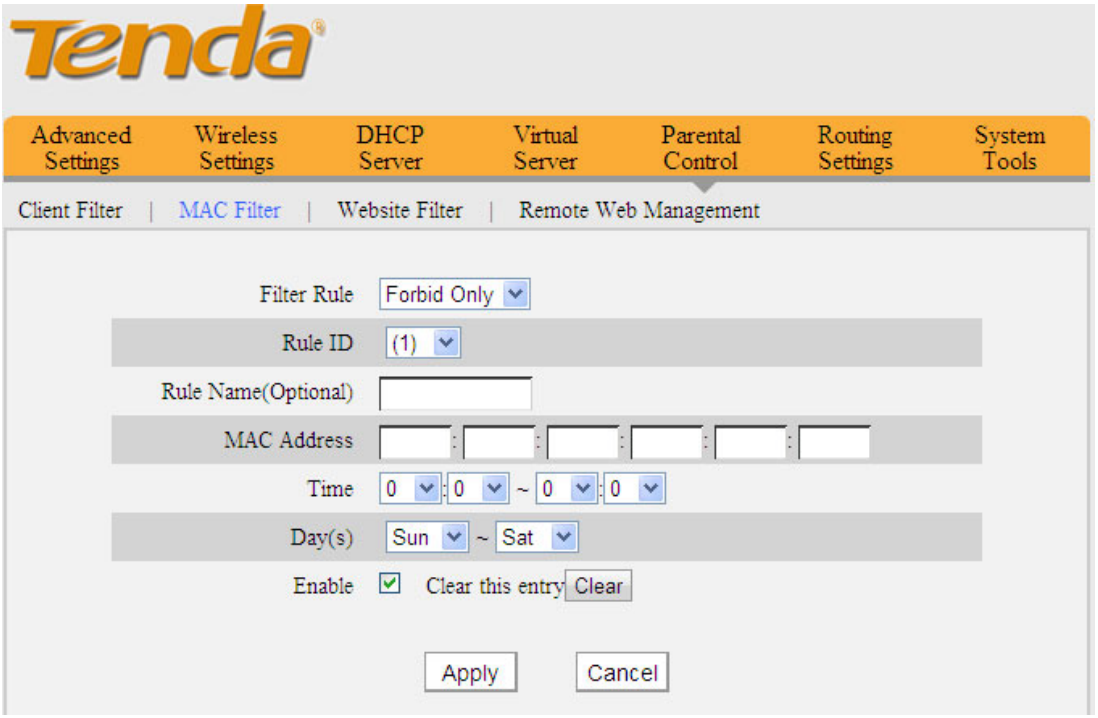


Example 2: if you want the pc with the IP address 192.168. 0.145 only can browse web pages from 8:00 to 18 : 00, do as follows:



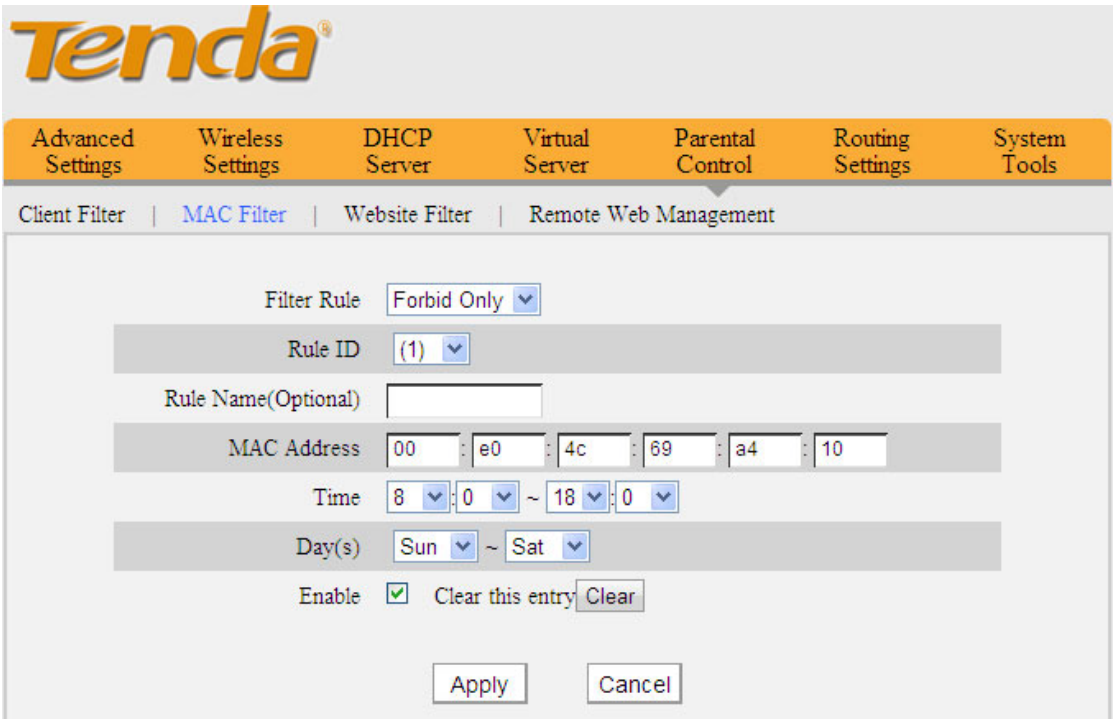
8.2 MAC Filter

To better manage PCs in LAN, you can limit the time to access the internet through MAC Filter.

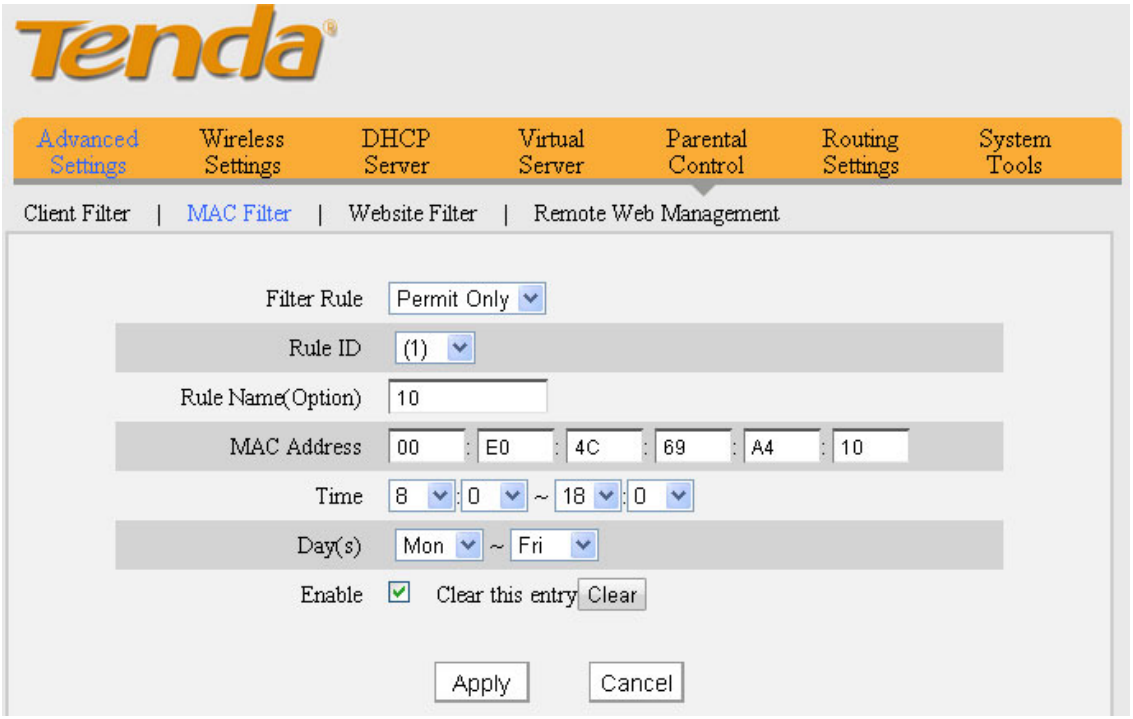


Filter Rule: Select Forbid Only or Permit Only.
Rule ID: Select a rule ID from the drop-down list.
Rule Name: Briefly describe the current entry/rule.
MAC Address: Specify a MAC address for a corresponding MAC filter rule to apply to.
Time: Specify a time period for a current rule to take effect.
Day: Select a day or several days for a current rule to take effect.
Enable: Check to enable or uncheck to disable a corresponding filter rule .

Example1: If you want to prohibit a PC with the MAC address 00:E0:4C:69:A4:10 to access Internet between 8:00 and18:00.

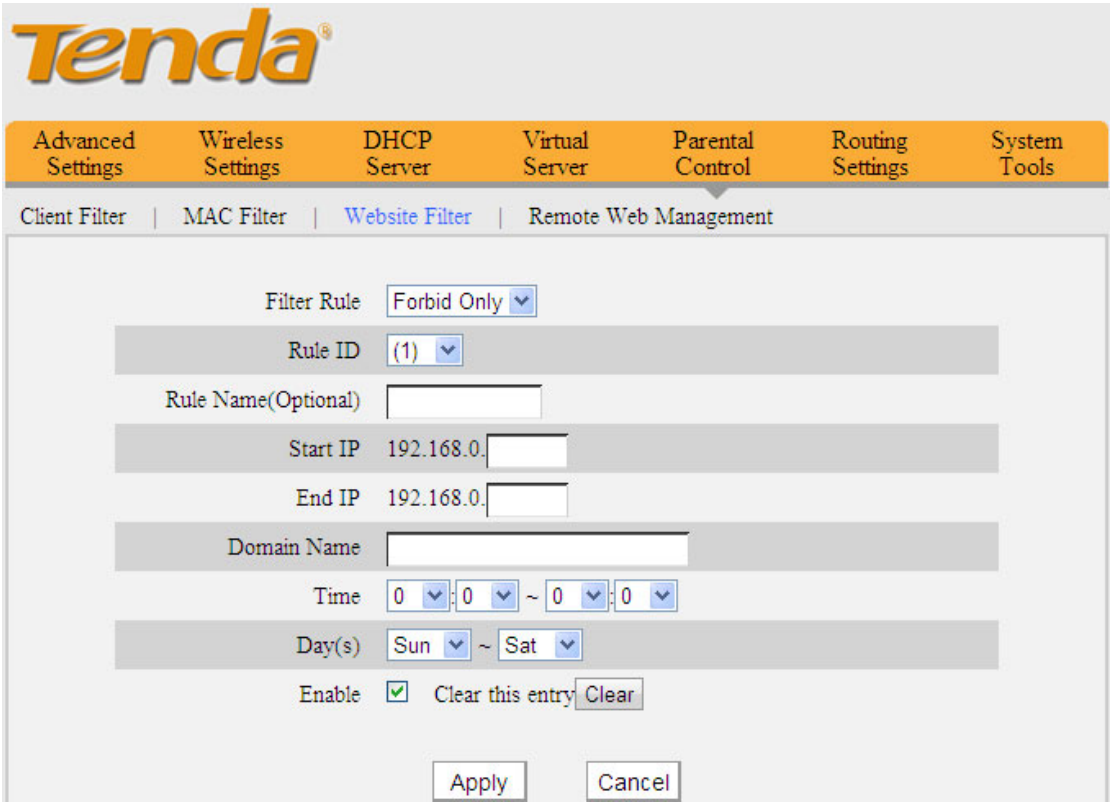


Example2: if you want PC with the MAC address 00:E0:4C:69:A4:10 can access Internet between 8:00 and18:00 only from Monday to Friday.



8.3 URL Filter

To better control LAN PCs, you can use the URL filter functionality to allow or disallow such PC to access certain websites within a specified time range.



Filter Rule: Select Forbid Only.

Rule ID: Select a rule ID from the drop-down list.

Rule Name: Briefly describe the current entry/rule.

Start IP/End IP: Enter the same IP address or 2 different IP addresses in both boxes to specify a single PC or a range of PCs for current rule to apply to.

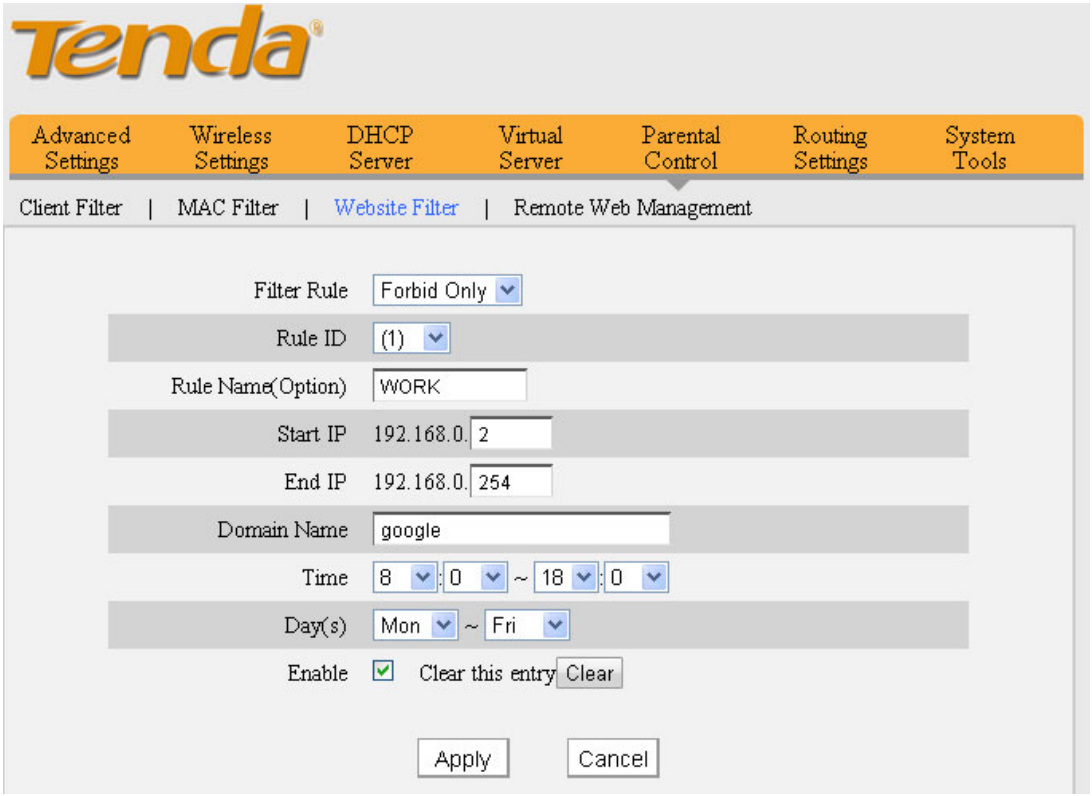
Domain Name: Enter full domain name or keyword of a domain name to be filtered out.

Time: Specify a time period for a current rule to take effect.

Day(s): Select a day or several days for a current rule to take effect.

Enable: Check to enable or uncheck to disable a corresponding filter rule.

Example: If you want to forbid the computers on your LAN to access “www.google.com” from 8 : 00 to 18 : 00 during working days: Monday- Friday, then do as follows:

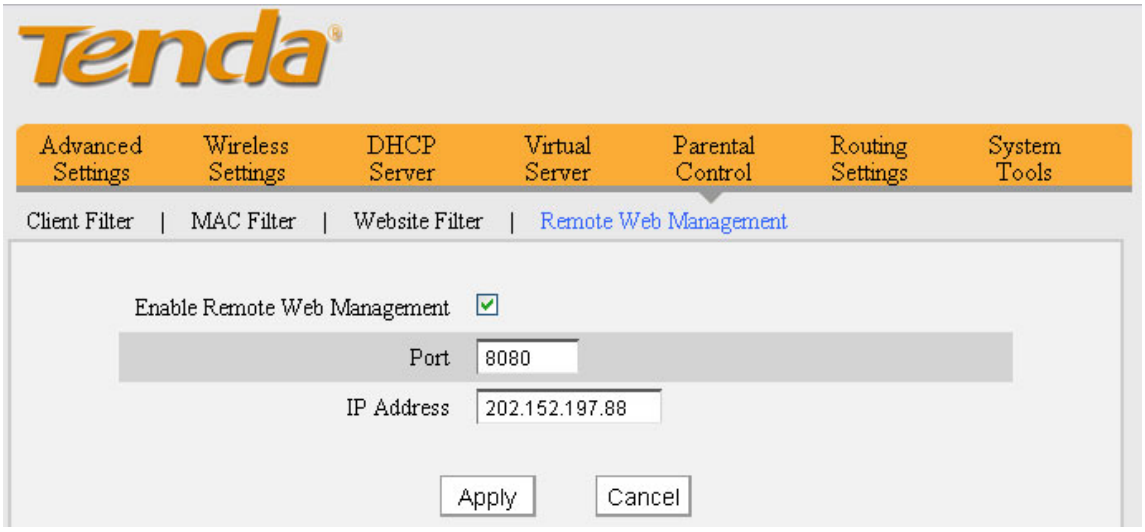


⚠ **Note:**

Each rule can only include one domain name. Simply add more rules accordingly, if you want to filter multiple domain names.

8.4 Remote Web-based Management

The Remote management allows the Router to be configured from the Internet by a web browser.



Enable Remote Web Management: Select it to enable the Remote Web Management feature, then you can access the router from Internet.

Port: the management port to be open to outside access.

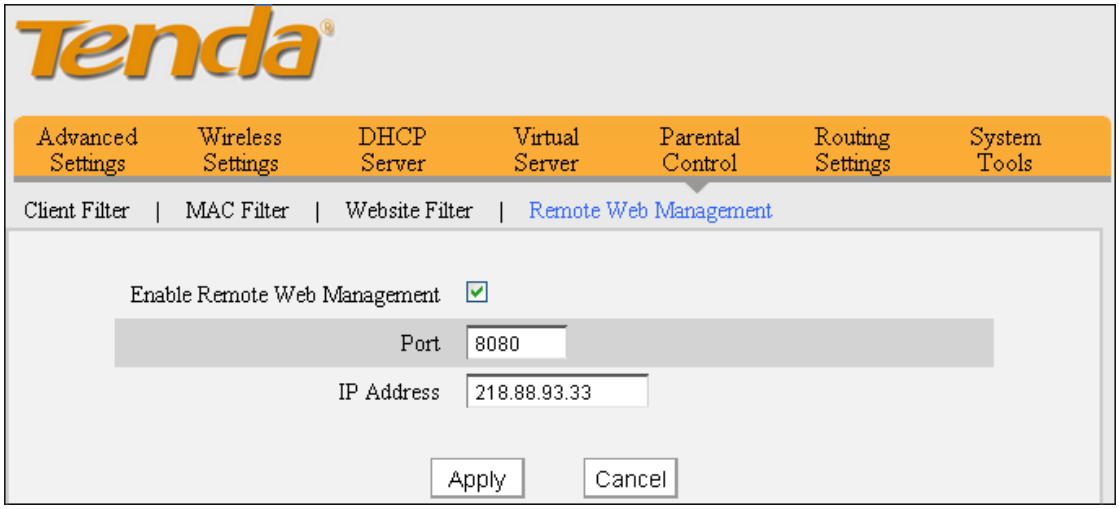
IP Address: Enter a trusted IP address of a PC from Internet or other external networks which you want to authorize to manage your router remotely via a web browser.

⚠ **Note:**

1. To access the device via port 8080, enter "http://x.x.x.x:8080" where "x.x.x.x" represents the router's WAN 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).

2. 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.

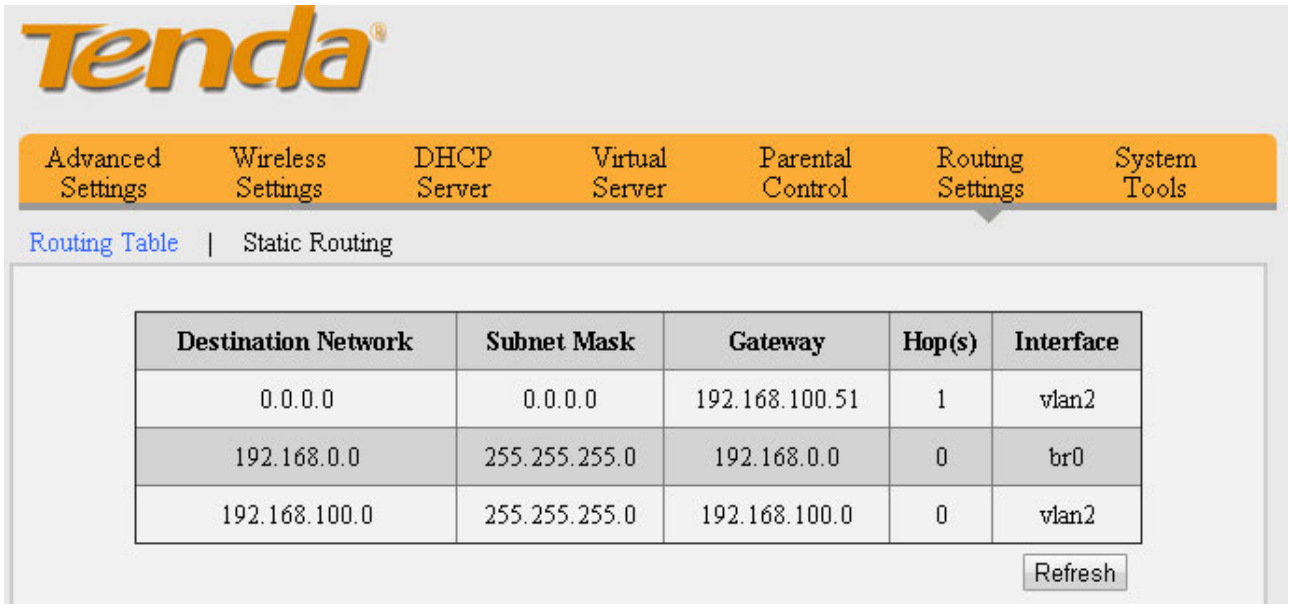
For example: If you want to allow only the PC at the IP address of 218.88.93.33 from Internet to access Device's web-based utility via port: 8080, then configure the same settings as shown on the screenshot above on the device.



Chapter 9 Routing Settings

9.1 Routing Table

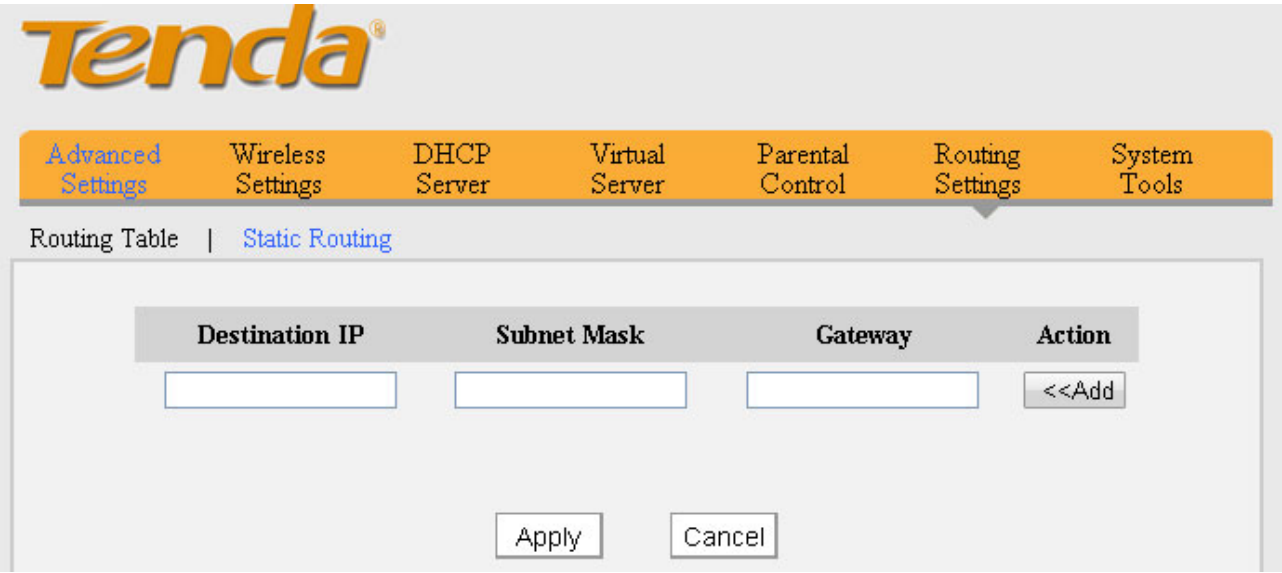
This page displays the router's routing table which lists destination IP, subnet mask, gateway, hop count and interface.



The principal task for a router is to look for an optimal transfer path for data forwarding, and transfer it to the specified destination. 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.

9.2 Static Routing

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



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

⚠ **Note:**

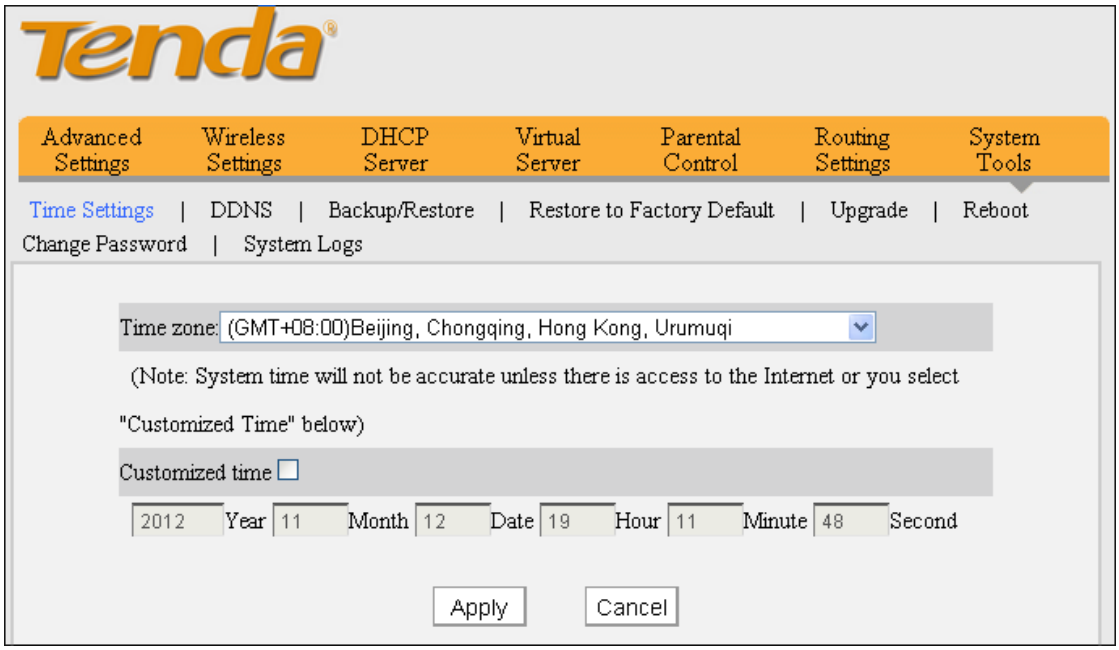
1. Gateway must be on the same IP net segment as device's LAN/WAN IP address.
2. Subnet Mask must be entered 255.255.255.255 if destination IP address is a host.
3. Subnet Mask must be entered accordingly if destination IP address represents an IP network segment. It must correspond to the specified IP address.

For example: Destination IP: 10.0.0.0 , Subnet Mask: 255.0.0.0.

Chapter 10 System Tools

10.1 Time Settings

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

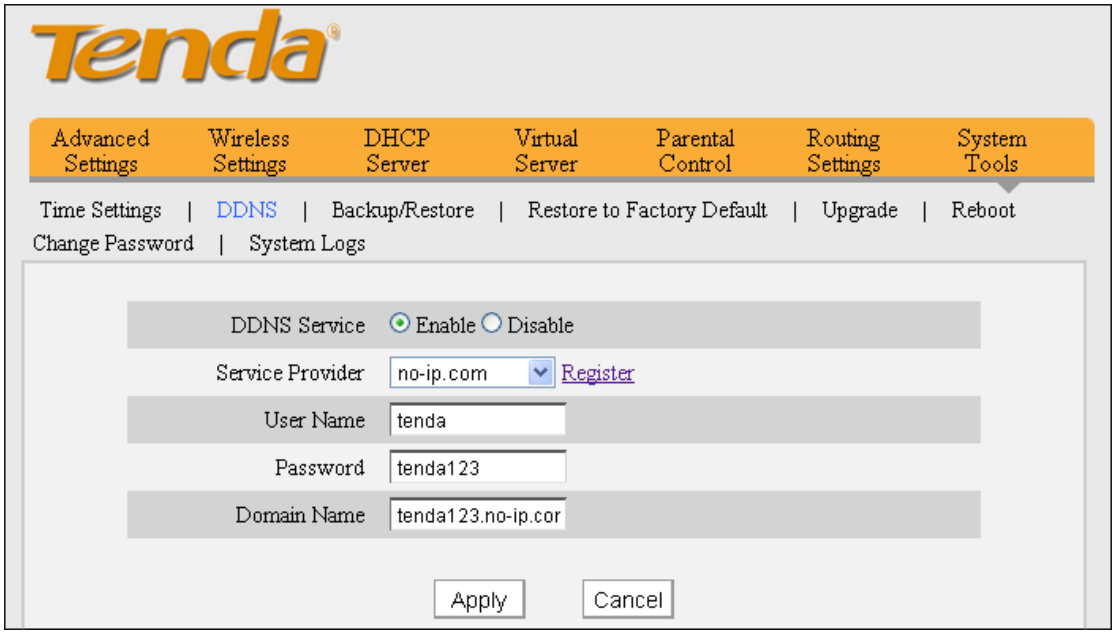


⚠ **Note:**

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.

10.2 DDNS

DDNS (Dynamic DNS) Service allows you to assign a fixed domain name for your dynamic WAN IP Address so that you can remotely access your LAN from the web.



Service Provider: Select your DDNS service provider from the drop-down menu.

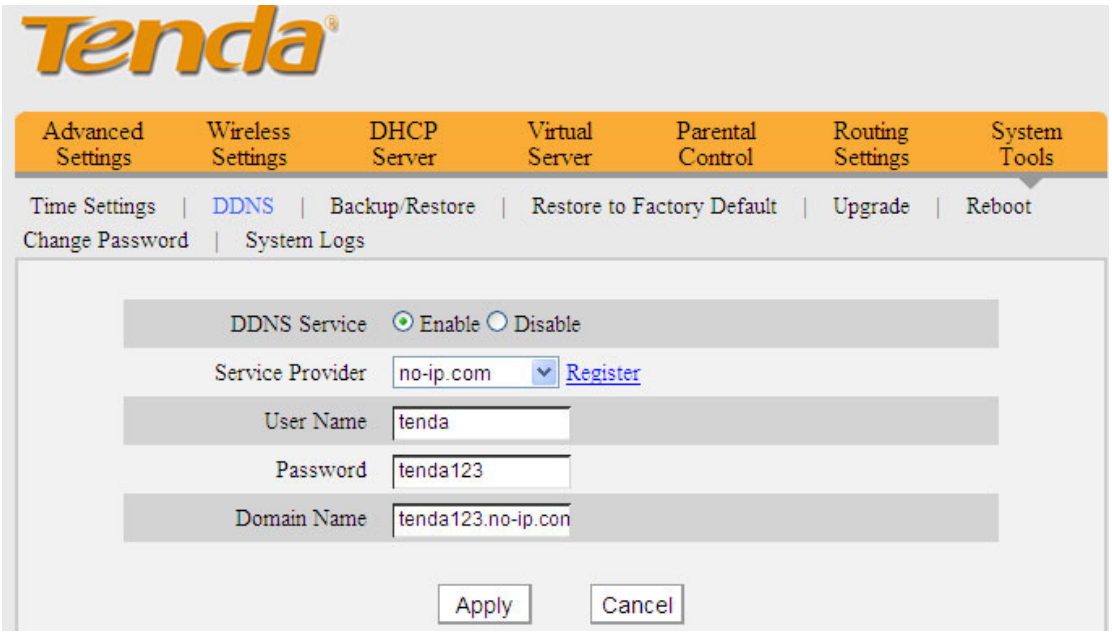
User Name: Enter the DDNS user name registered with your DDNS service provider.

Password: Enter the DDNS Password registered with your DDNS service provider.

Domain Name: Enter the DDNS domain name you register.

For example: If you have registered a domain name from no-ip.com for a web server on the host at 192.168.0.10 and get below info:

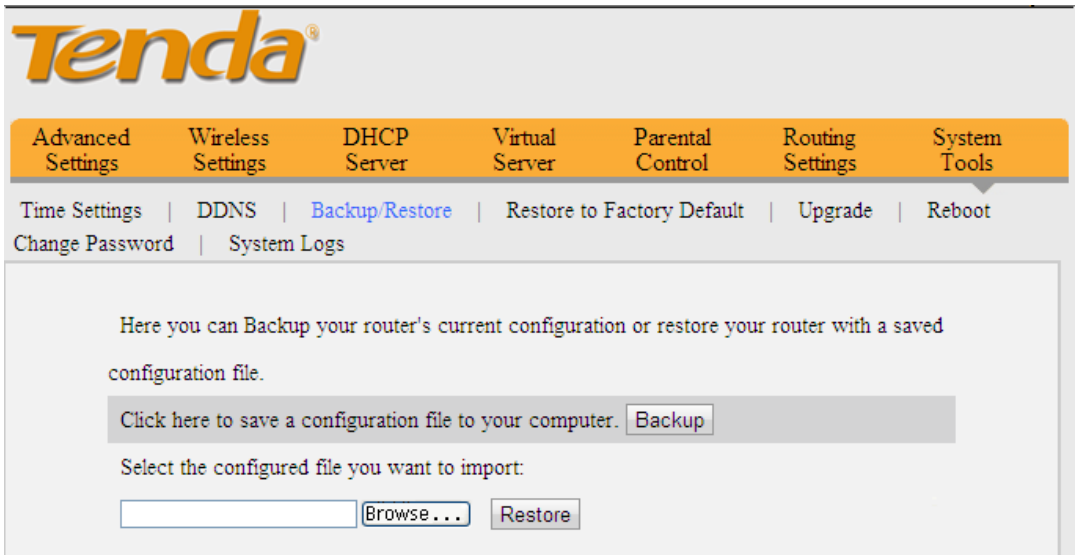
User Name	tenda
Password	tenda123
Domain Name	tenda123.no-ip.com



Configure necessary settings on port forwarding interface and enter the information provided by your DDNS service provider on the DDNS screen. Others can access your web server by simply entering http://tenda123.no-ip.com in their browser address bar.

10.3 Backup/Restore

This section allows you to backup the router settings or restore the settings you saved to the router.

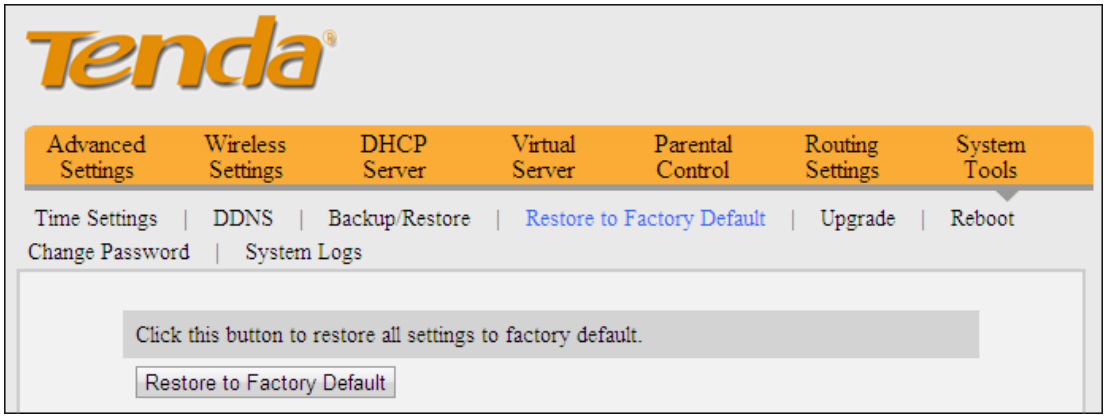


Backup: Once you have configured the device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your device in case that the device is restored to factory default settings. To do so, click the “Backup” button and specify a directory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

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

10.4 Restore to Factory Default Settings

Click the "Restore to Factory Default" button to reset Device to factory default settings.



Factory Default Settings:

Password: There is no preset password by default.

IP Address: 192.168.0.1

Subnet mask: 255.255.255.0.

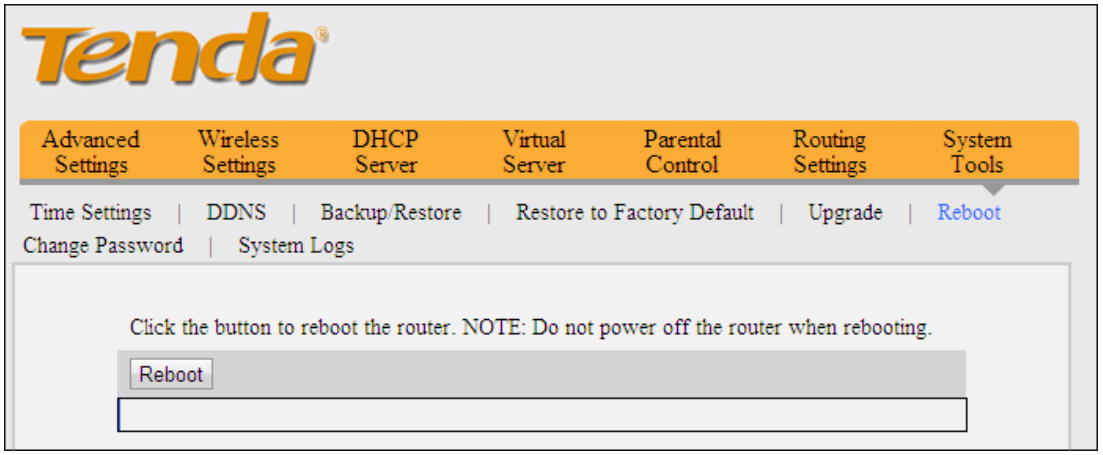
10.5 Firmware Update

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) to download the latest firmware to update your device. If you run into a problem with a specific feature of the device, log on to our website (www.tendacn.com) to download the latest firmware to update your device.

1. Click "Browse" to locate and select the firmware.
2. Upgrade: Click to start upgrading. Device will restart automatically after finish upgrading.

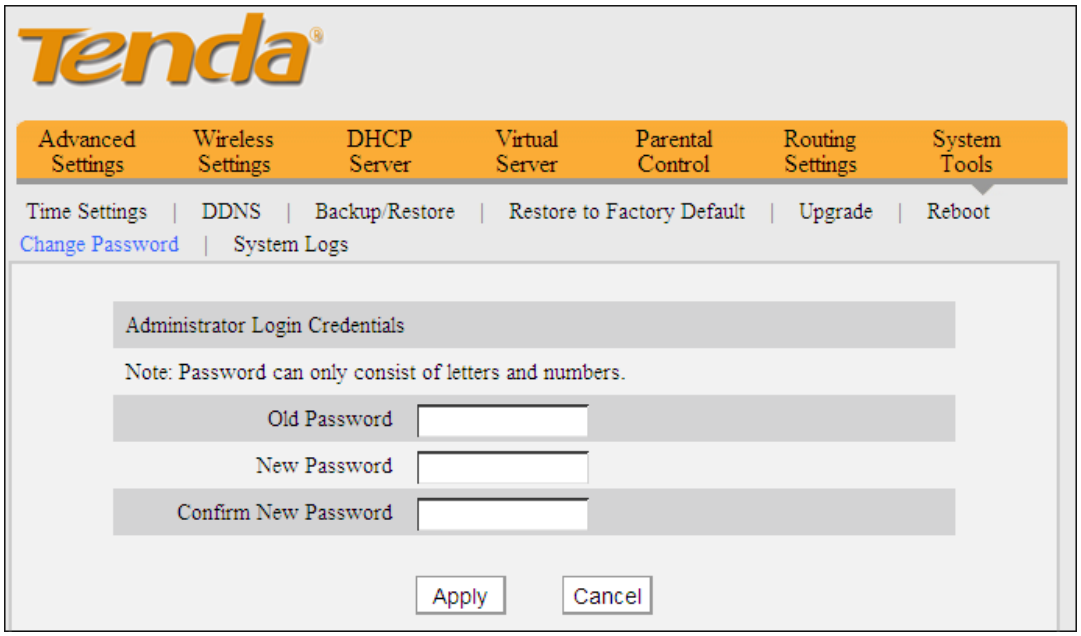
10.6 Reboot

Reboot the device to activate your settings. WAN connection will be disconnected during reboot.



10.7 Change Password

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

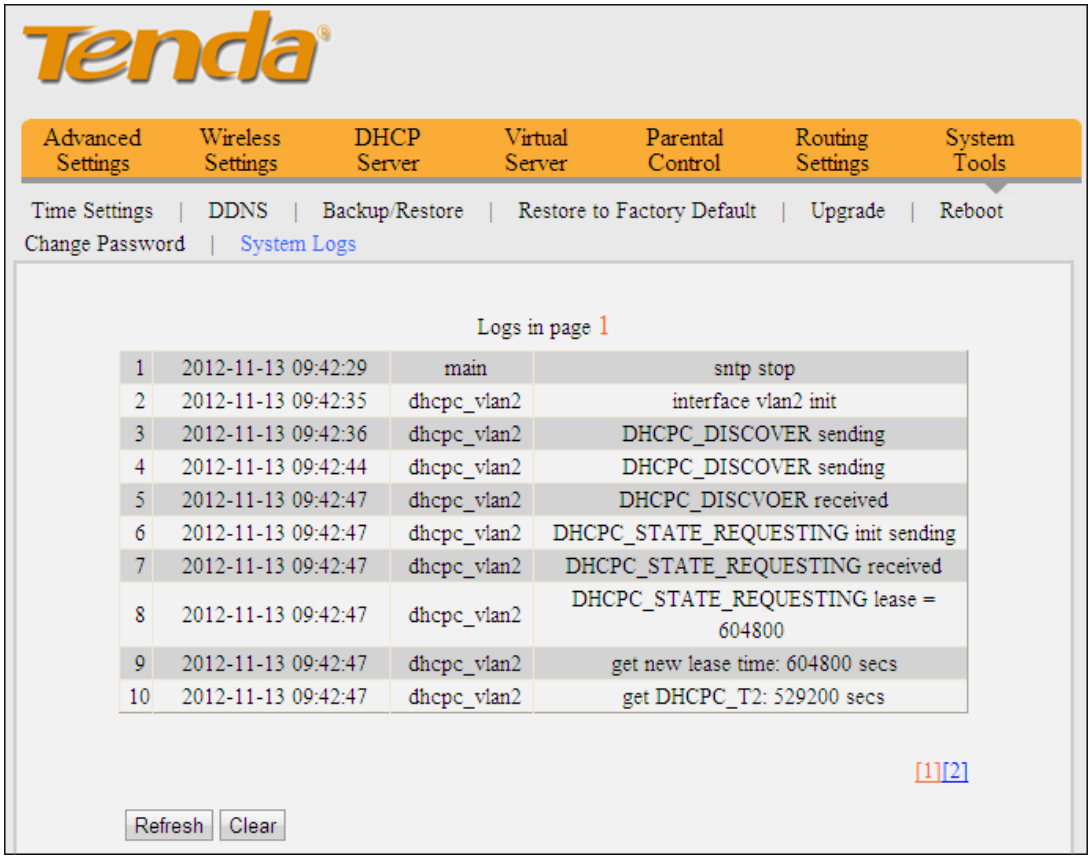


Click OK to submit your new password.

Note: For security purpose, it is highly recommended that you change Device's default login password.

10.8 System Logs

The System Logs option allows you to view all events that occur upon system startup



Refresh: Click to update current logs.

Clear: Click to remove all logs.

Appendix 1 Glossary

Channel

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

SSID

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

WPA/WPA2

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

The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA. Currently, WPA is supported by Windows XP SP1.

Appendix 2 Product Features

- Compliant with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3 and IEEE 802.3u standards
- High gain omni-directional antenna delivers more powerful signal and extends coverage to farther distance
- Up to 150+300Mbps wireless rate;
- 1 10/100M WAN port for Internet connection;
- 4 10/100M Ethernet ports for LAN connection;
- Auto MDI/MDIX on each port
- Provides Internet connection types: Dynamic/ static IP; can be connected to an xDSL/Cable MODEM
- Combines the function of a wireless AP, router, 4-port switch and firewall;
- WPA, WPA2 and WPA&WPA2, etc to secure your wireless network
- Simple and quick to secure a WiFi connection at a push of the WPS button;
- Multiple operating modes: WISP Client, universal repeater, WDS (available only on some products)
- Provides primary SSID and secondary SSID
- Hidden/invisible SSID;
  MAC-based wireless access control;
- WMM streams your video and audio;
- SNTP to synchronize local time with Internet time servers;
- Supports UPnP and DDNS features;
- WDS support for extending existing wireless coverage;
- Provides virtual server and DMZ features;
- Provides logs to record device's usage status;

Appendix 3 Troubleshooting

This section provides solutions to problems that may occur during installation and operation of the device. Read the following if you are running into problems. If your problem is not covered here, please feel free to go to www.tendacn.com to find a solution or email your problems to support@tenda.com.cn orsupport02@tenda.com.cn. We will be more than happy to help you out as soon as possible.

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

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

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.

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

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?

A: Reset your device by pressing the Reset button for over 7 seconds. Note: All settings will be deleted and restored to factory defaults once you pressed the Reset button.

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

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

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

This problem mainly happens to users who use the PPPoE or Dynamic IP Internet connection type. You need to change the MTU size (1492 by default). In this case, go to "WAN Settings" to change the MTU value from default 1480 to 1450 or 1400, etc.

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

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

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

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

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

Click Enable and save your settings.

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

Server	Protocol	Service Port
Web Server	TCP	80
FTP Server	TCP	21
Telnet	TCP	23
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
SMTP	TCP	25
POP3	TCP	110

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1)The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.(2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable

CE

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

"The product can be used without restrictions in the following countries: all EU member states except France and Norway.

The product can be used with limitations in the following countries: France (for indoor use only) and Norway (20 km in the center of Ny-Ĺlesund)."