Tenda®

www.tendacn.com

# User Guide

## Wireless N900 Concurrent Dual-band Gigabit 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 http://www.tendacn.com.

# Table of Contents

# Chapter 1 Product Overview

## 1.1 What it does

Thanks for purchasing Tenda Concurrent Dual Band Wireless N Gigabit Router (collectively Device).

The Tenda Concurrent Dual Band Wireless N Gigabit Router accommodates users looking for extreme wireless performance. Delivering up to 450+450Mbps wireless speed, it uses dual band technology to deliver 2.4GHz and 5GHz wireless signals simultaneously, allowing you to check email and browse the Internet using the 2.4GHz while streaming High-Definition movies and other bandwidth-intensive applications on the 5GHz band. Also, it reduces the possibility of interference from appliances and cordless phones that use the 2.4GHz band lets you enjoy IPTV. Plus, the Device provides a USB port for printing and storage sharing.

## 1.2 Features

- 2.4GHz: IEEE802.11n, IEEE802.11g, IEEE 802.11b;
  5GHz: IEEE 802.11n, IEEE 802.11a; IEEE802.3, IEEE802.3u;
- Operate in 2.4GHz and 5GHz wireless bands simultaneously
- 1 * Gigabit WAN port for Internet connection;
- 3 * Gigabit LAN ports for LAN connection;
- 1 IPTV port support IPTV service;
- Up to 450+450Mbps wireless rate;
- WDS support for extending existing wireless coverage;
- WEP and WPA&WPA2-PSK secure your wireless network against unauthorized access;
- Hidden/invisible SSID;
  MAC-based wireless access control;

- WPS one-touch encryption;
- Provides Wireless guest network feature;
- WMM streams your video and audio;
- Combines the function of a wireless AP, router, switch and firewall;
- Provides Internet connection types: Dynamic/ static IP,L2TP,PPTP ， PPPOE/ PPPOE dual access;
- 1 USB port for storage or wireless printing service sharing;
- Built-in firewall supports domain name/MAC address filter
- SNTP to synchronize local time with time servers on Internet;
- Bandwidth control;
- Supports UPnP and DDNS features;
- Provides virtual server and DMZ features;
- Syslog records router's usage status;

## 1.3 Package Contents

Unpack the box and check the following items:

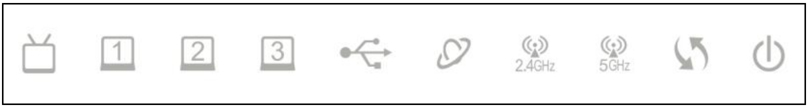
- Concurrent Dual Band Wireless N900 Gigabit Router
- Power Adapter
- Quick Install Guide
- CD-ROM

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

# Chapter 2 Hardware

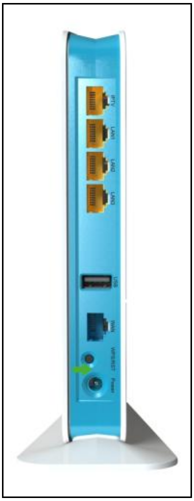
## 2.1 Panel Overview

### Front Panel:



| | |
|---|---|
| 📺 | IPTV LED: A solid light indicates corresponding IPTV port is correctly connected while a blinking light indicates it is transmitting data. |
| 3 | LAN/1/2/3 LED: A solid light indicates corresponding LAN port is correctly connected while a blinking light indicates such port is transmitting data. |
| ⭠ | USB LED: A solid light indicates the USB port is correctly connected. |
| 🌐 | WAN LED: A solid light indicates the WAN port is correctly connected while a blinking light indicates it is transmitting data. |
| 2.4GHz | 2.4G LED: A solid light indicates wireless is enabled while a blinking light indicates device is transmitting data wirelessly over 2.4G. |
| 5GHz | 5G LED: A solid light indicates wireless is enabled while a blinking light indicates Device is transmitting data wirelessly over 5GHz. |
| ⟲ | WPS LED: A blinking light indicates Device is performing WPS authentication on a client device. |
| ⏻ | Power/System LED: Blinks while system is functioning correctly. |

## Back Panel:



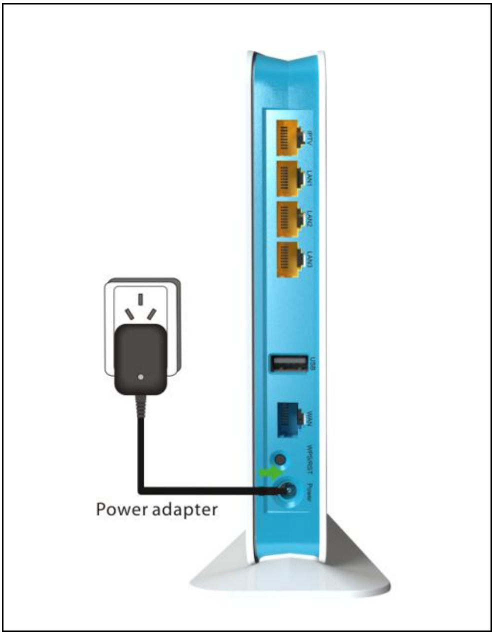
1) IPTV : IPTV port for connection to a network set-top box. However such port can function as a LAN port if IPTV STB port is not enabled;
2) LAN/1/2/3: 3 LAN ports（RJ-45）for connection to PC's NIC or uplink to a hub, switch or wireless AP;
3) WAN: Internet port （RJ-45）for connection to an Internet-enabled xDSL Modem/Cable Modem or existing Ethernet;
4) USB: USB port for connection to a USB device such as a USB printer or storage device;
5) WPS/Reset: WPS button/Reset button: Pressing it for about 1 second enables WPS encryption with a blinking WPS LED while Pressing it for about 7 seconds restores the Device to factory defaults.

## 2.2 Minimum System Requirements

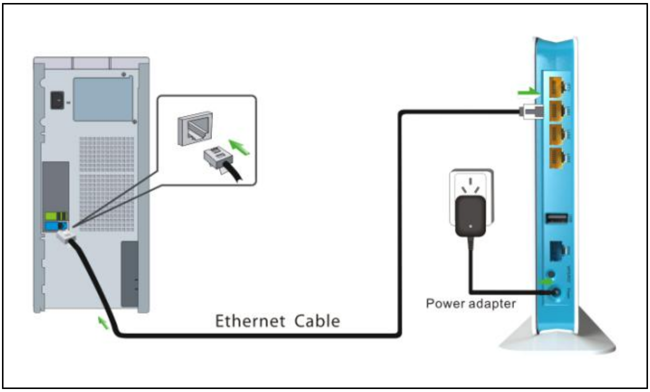
- Installed Wireless Network Adapter
- Internet Explorer 5.0 or higher
- Broadband Internet Service (through xDSL/Cable Modem/Ethernet)

## 2.3 Hardware Installation

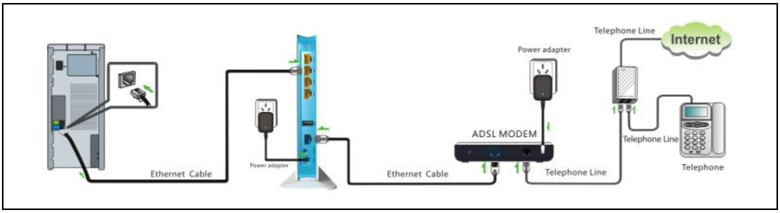
1. Connect one end of the included power adapter to the Device and plug the other end into a wall outlet nearby. (Using a power adapter with a different voltage rating than the one included with the Device will cause damage to the Device.)



2. Connect one of the LAN ports on the Device 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.

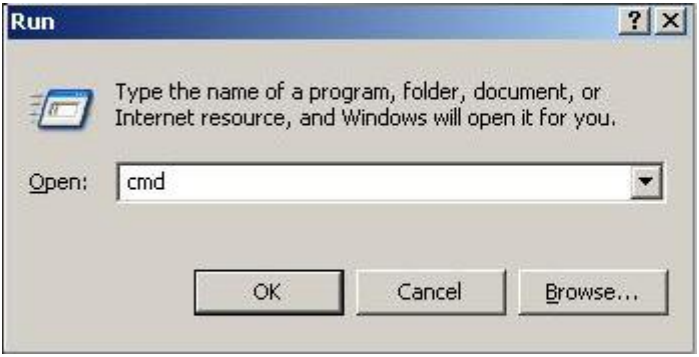


# Chapter 3 Login to Web Utility

The Device's default IP is 192.168.0.1. You can change it to accommodate your own needs. Here in this manual, we use the default IP.

Connect you PC to the Device and config your PC's TCP/IP settings following instructions in appendix 1 hereto. And then do as follows to run a Ping command to test connectivity between your PC and the Device.

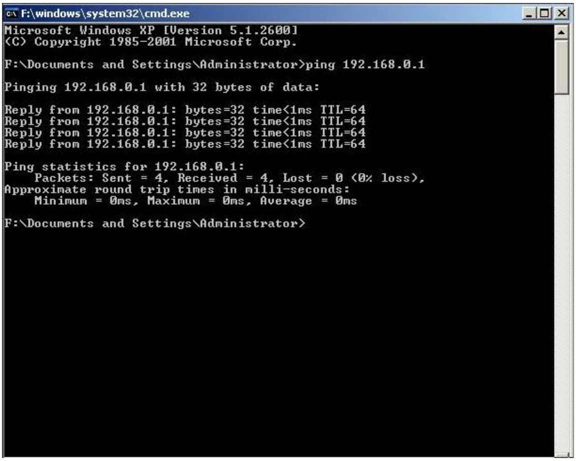
- 1. Select "Start"—"Run" and enter "cmd". Then press "Enter".



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

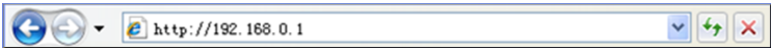
- Enter "ping 192.168.0.1" and press "Enter". If you see the following screen, it means the router is reachable on your PC. If you don't get the following screen, verify router's power supply, Ethernet cable connections and your PC's TCP/IP settings.



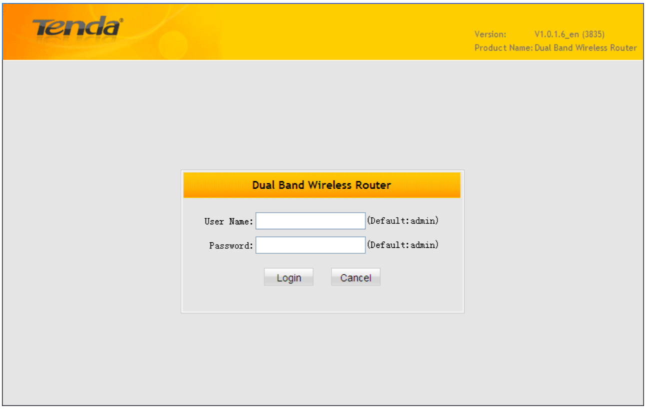
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

F:\Documents and Settings\Administrator>
```

## Login to Web Utility

Launch a web browser, in the address bar,input 192.168.0.1 and press “Enter”.



When connected to the Device successfully, you shall see the login window below. Enter user name and password in corresponding fields on window below (Default user name and password are respectively set to admin).


Version: V1.0.1.6_en (3835)
Product Name: Dual Band Wireless Router

Dual Band Wireless Router

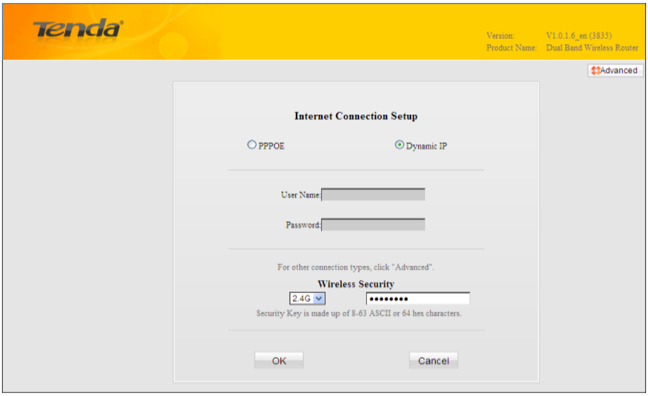
User Name: (Default:admin)

Password: (Default:admin)

⚠ **Note:**

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

You will see the following interface if you entered a correct user name and a correct password.


Version: V1.0.1.6_en (3835)
Product Name: Dual Band Wireless Router

Internet Connection Setup

○ PPPOE ● Dynamic IP

User Name:

Password:

For other connection types, click "Advanced".

Wireless Security

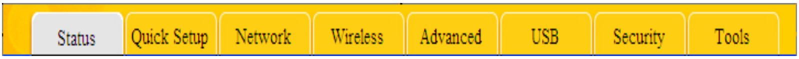
2.4G ••••••••

Security Key is made up of 8-63 ASCII or 64 hex characters.

# Chapter 4 Configurations

This chapter describes the Web based configurations for easier management of the Device. The eight tabs available on the Web interface as seen below are illustrated respectively hereunder.

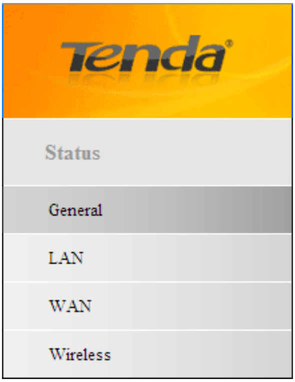
- Status
- Quick Setup
- Network
- Wireless
- Advanced
- USB
- Security
- Tools



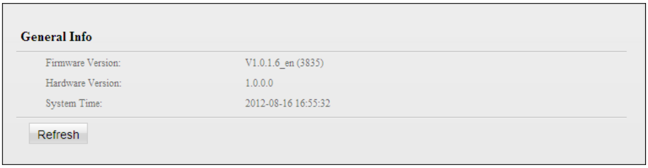
During operation, if you are not clear about a certain feature, simply read the related helpful info on the right. Below explains each feature in details.

## 4.1 Status

There are 4 subdues under the Status tab: General, LAN, WAN and Wireless, which are explained in details below.



### General:



General Info

Firmware Version: V1.0.1.6_en (3835)

Hardware Version: 1.0.0.0

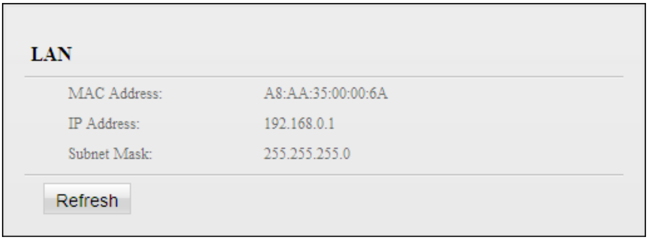
System Time: 2012-08-16 16:55:32

This section displays system time, firmware version and hardware version info.

- Firmware Version：Displays Device’s firmware version.
- Hardware Version：Displays Device’s hardware version.
- System Time: Displays Device’s current system.

## LAN:

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



LAN

MAC Address: A8:AA:35:00:00:6A

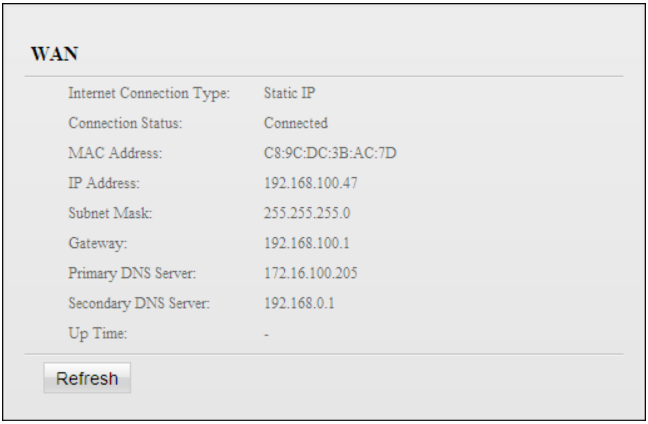
IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

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

## WAN:

This section allows you to view the router's WAN info listed below:



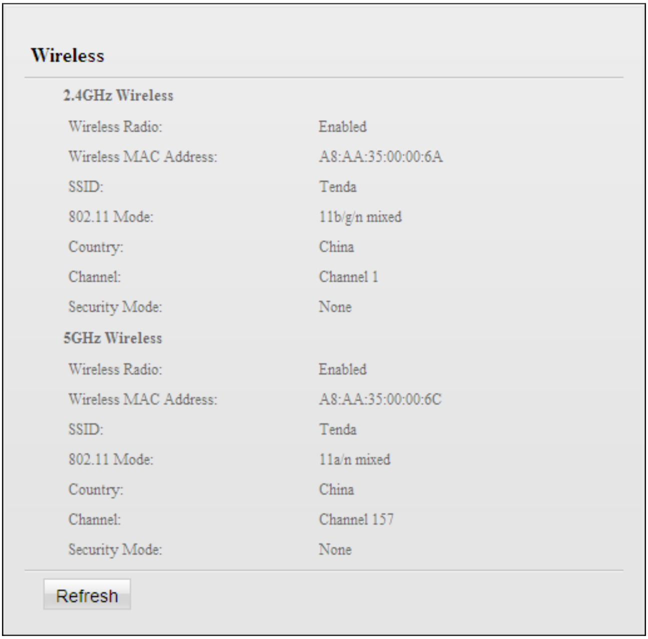
WAN

| | |
|---|---|
| Internet Connection Type: | Static IP |
| Connection Status: | Connected |
| MAC Address: | C8:9C:DC:3B:AC:7D |
| IP Address: | 192.168.100.47 |
| Subnet Mask: | 255.255.255.0 |
| Gateway: | 192.168.100.1 |
| Primary DNS Server: | 172.16.100.205 |
| Secondary DNS Server: | 192.168.0.1 |
| Up Time: | - |

- Internet Connection Type: Displays current Internet connection type.
- 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 the WAN port on the Device or the Device 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.
- MAC Address: Displays WAN MAC address.
- IP Address: Displays WAN IP address.
- Subnet Mask: Displays WAN subnet mask.
- Gateway: Displays WAN gateway address.
- Primary DNS Server: Displays primary WAN DNS address.
- Secondary DNS Server: Displays secondary WAN DNS address (if any).
- Up Time: Displays time duration indicating how long the Device has been connected to ISP.

## Wireless:

This section allows you to view the wireless info on both 2.4G and 5G bands: wireless radio status (on/off), wireless MAC address, SSID, network mode, channel and wireless security settings.



Wireless

2.4GHz Wireless

| | |
|---|---|
| Wireless Radio: | Enabled |
| Wireless MAC Address: | A8:AA:35:00:00:6A |
| SSID: | Tenda |
| 802.11 Mode: | 11b/g/n mixed |
| Country: | China |
| Channel: | Channel 1 |
| Security Mode: | None |

5GHz Wireless

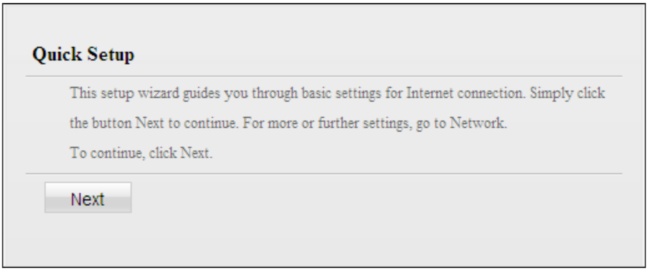
| | |
|---|---|
| Wireless Radio: | Enabled |
| Wireless MAC Address: | A8:AA:35:00:00:6C |
| SSID: | Tenda |
| 802.11 Mode: | 11a/n mixed |
| Country: | China |
| Channel: | Channel 157 |
| Security Mode: | None |

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

- Channel: Displays current channel.
- Security Mode: Displays current security Mode.

## 4.2 Quick Setup

The section instructs you to quickly configure basic settings for Internet and wireless connections.

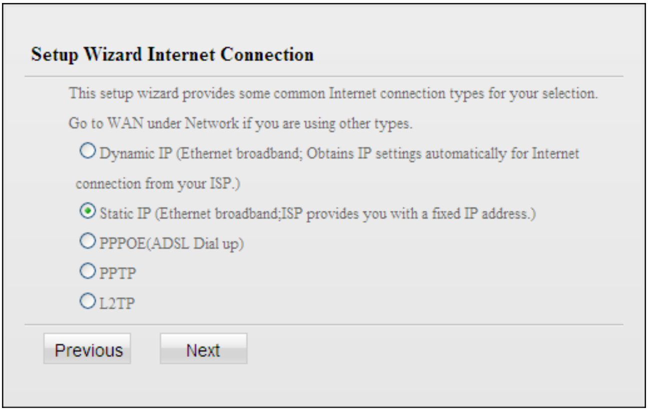


**Quick Setup**

This setup wizard guides you through basic settings for Internet connection. Simply click the button Next to continue. For more or further settings, go to Network.

To continue, click Next.

You may click Next to enter the page for selecting an Internet connection type.



**Setup Wizard Internet Connection**

This setup wizard provides some common Internet connection types for your selection. Go to WAN under Network if you are using other types.

○ Dynamic IP (Ethernet broadband; Obtains IP settings automatically for Internet connection from your ISP.)

● Static IP (Ethernet broadband;ISP provides you with a fixed IP address.)

○ PPPOE(ADSL Dial up)

○ PPTP

○ L2TP

5 types of Internet connection: Dynamic IP (DHCP), PPPoE (including PPPoE dual access), PPTP, L2TP and Static IP are available for your choice. The default type is dynamic IP.

- Dynamic.IP: Select Dynamic.IP.(DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP info and/or a user name and password.
- Static IP: Select Static IP Address if your ISP gives you all the IP info. You will need to enter the IP address, subnet mask, gateway address, and DNS address(es) in corresponding fields.
- PPPoE: Select PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection and provides you with a user name and password.
- PPTP: Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP connects a router to a VPN server.
- L2TP: Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server.

Select the type of Internet connection you have and click "Next" to config basic settings for Internet connection.

## 4.2.1 Dynamic IP

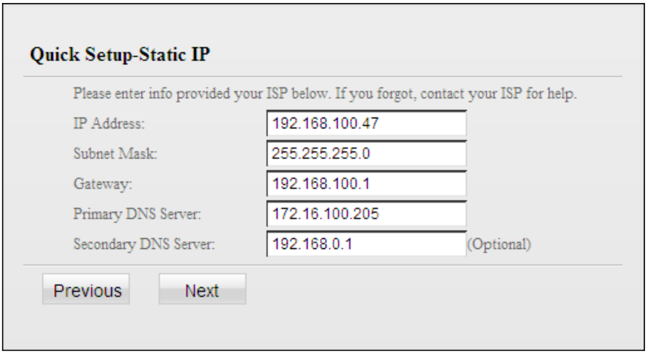
Select Dynamic.IP.(DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP info and/or a user name and password. And then simply click Next to save your settings.

⚠ **Note:**

Dynamic IP is the default Internet connection type. Skip the Quick Setup if your ISP is currently using this connection type.

## 4.2.2 Static IP

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



**Quick Setup-Static IP**

Please enter info provided your ISP below. If you forgot, contact your ISP for help.

| | |
|---|---|
| IP Address: | 192.168.100.47 |
| Subnet Mask: | 255.255.255.0 |
| Gateway: | 192.168.100.1 |
| Primary DNS Server: | 172.16.100.205 |
| Secondary DNS Server: | 192.168.0.1 (Optional) |

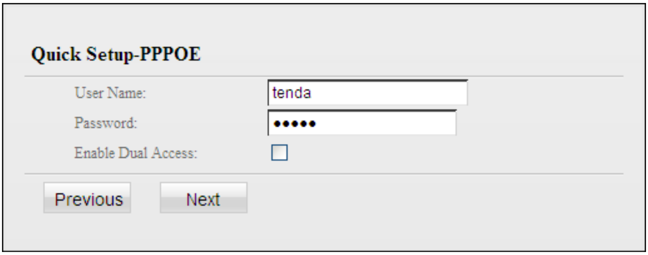
- IP Address: Enter the WAN IP address provided by your ISP. Consult your ISP if you are not clear.
- Subnet Mask: Enter WAN Subnet Mask provided by your ISP. Consult your ISP if you are not clear.
- Gateway: Enter the Gateway address provided by your ISP. Consult your ISP if you are not clear.
- Primary DNS Server: Enter the necessary DNS address provided by your ISP. Consult your ISP if you are not clear.
- Secondary DNS Server: Enter the other DNS address if your ISP provides you with 2 such addresses, and it is optional.

⚠ **Note:**

Device will not work if the dynamically obtained or manually specified WAN IP and LAN IP are on the same subnet. In case of emergency, press the "Reset" button on your device.

### 4.2.3 PPPoE

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



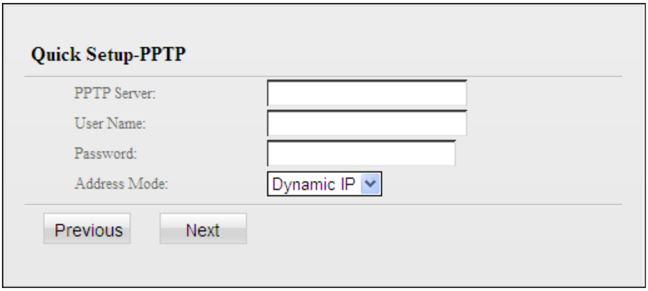
Quick Setup-PPPOE

| | |
|---|---|
| User Name: | tenda |
| Password: | ••••• |
| Enable Dual Access: | □ |

- User Name: Enter the User Name provided by your ISP. Consult your ISP if you are not clear.
- Password: Enter the password provided by your ISP. Consult your ISP if you are not clear.
- Enable Dual Access: Enable this option and configure corresponding settings if your ISP provides you with two access methods.

### 4.2.4 PPTP

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



Quick Setup-PPTP

| | |
|---|---|
| PPTP Server: | |
| User Name: | |
| Password: | |
| Address Mode: | Dynamic IP |

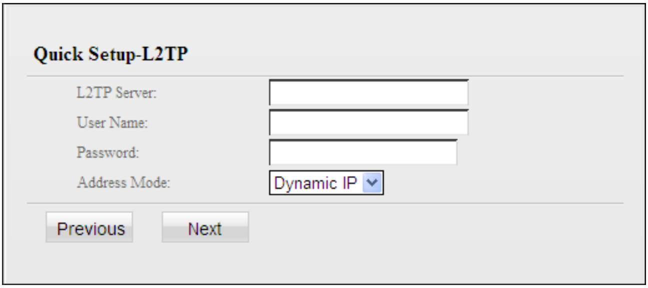
- PPTP Server: Enter the IP address of a PPTP server.
- User Name: Enter your PPTP User Name.
- Password: Enter your Password.
- Address mode: Select "Dynamic" if you don't get any IP info from your ISP, otherwise select "Static". Consult your ISP if you are not clear.

- IP Address: Enter the IP address provided by your ISP. Consult your local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- Default Gateway: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.

### 4.2.5 L2TP

Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server.

For example：A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



Quick Setup-L2TP

L2TP Server:

User Name:

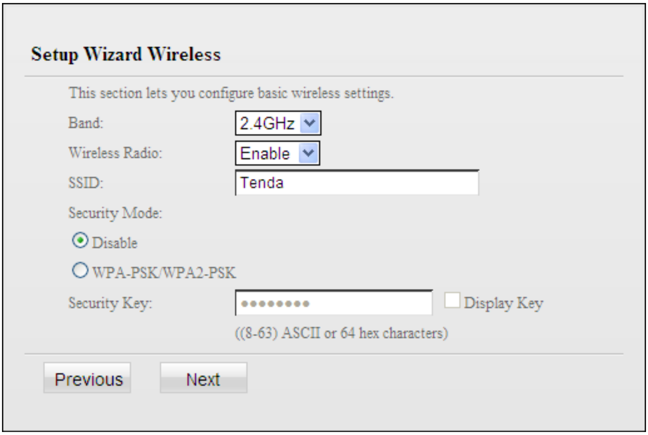
Password:

Address Mode: Dynamic IP

- L2TP Server: Enter the L2TP IP address provided by your ISP.
- User Name: Enter your L2TP User Name.
- Password: Enter your Password.

- 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 local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- Default Gateway: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.

After finishing basic settings of Internet connection, you may click "Next" to configure wireless settings.



Setup Wizard Wireless

This section lets you configure basic wireless settings.

Band: 2.4GHz

Wireless Radio: Enable

SSID: Tenda

Security Mode:

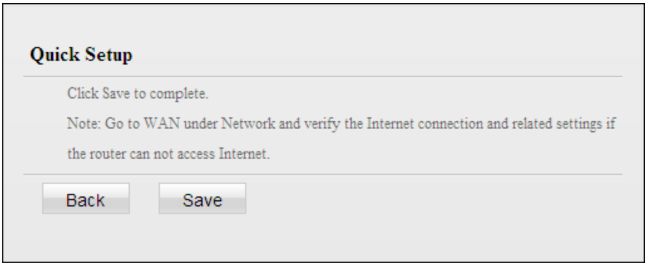
● Disable

○ WPA-PSK/WPA2-PSK

Security Key: ●●●●●●●●● □ Display Key

((8-63) ASCII or 64 hex characters)

Click Next and you will come to the end page; click "Save" there.

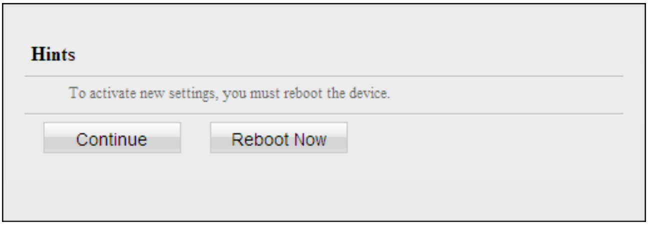


Quick Setup

Click Save to complete.

Note: Go to WAN under Network and verify the Internet connection and related settings if the router can not access Internet.

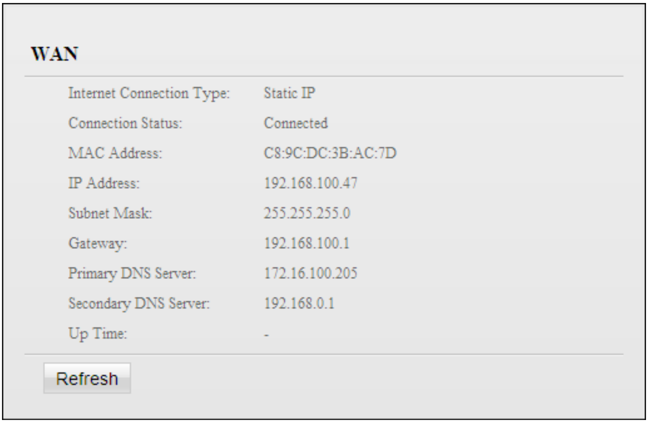
You may be asked whether to reboot the Device now if you clicked the "Save" button.



Hints

To activate new settings, you must reboot the device.

Go to Status--WAN to view the settings after reboot completed.

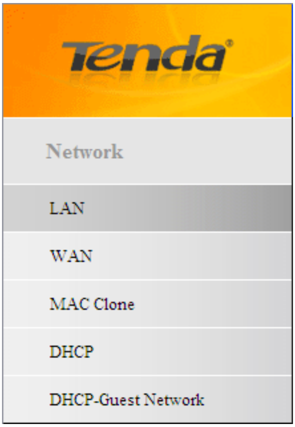


WAN

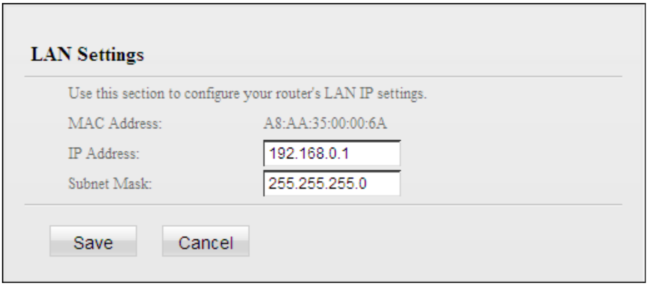
| | |
|---|---|
| Internet Connection Type: | Static IP |
| Connection Status: | Connected |
| MAC Address: | C8:9C:DC:3B:AC:7D |
| IP Address: | 192.168.100.47 |
| Subnet Mask: | 255.255.255.0 |
| Gateway: | 192.168.100.1 |
| Primary DNS Server: | 172.16.100.205 |
| Secondary DNS Server: | 192.168.0.1 |
| Up Time: | - |

## 4.3 Network

"Network" includes the following five submenus: LAN, WAN, MAC Clone, DHCP and DHCP-Guest Network. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



## 4.3.1 LAN



LAN Settings

Use this section to configure your router's LAN IP settings.

MAC Address: A8:AA:35:00:00:6A

IP Address: 192.168.0.1

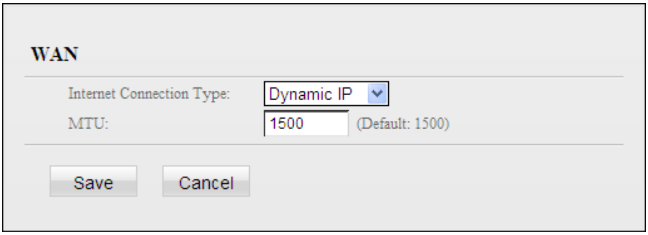
Subnet Mask: 255.255.255.0

- IP Address: Device's LAN IP. The default is 192.168.0.1. You can change it according to your need.
- Subnet Mask: Device's LAN subnet mask.

## 4.3.2 WAN

5 types of Internet connection: Dynamic IP (DHCP), PPPoE, PPTP, L2TP and Static IP are available for your choice.

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



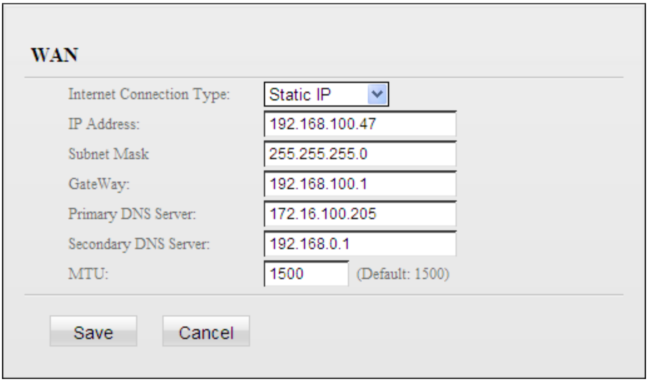
WAN

Internet Connection Type: Dynamic IP

MTU: 1500 (Default: 1500)

- Internet connection Type: Displays a list of available Internet connection types.
- MTU: Maximum Transmission Unit. The default value is1500.

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



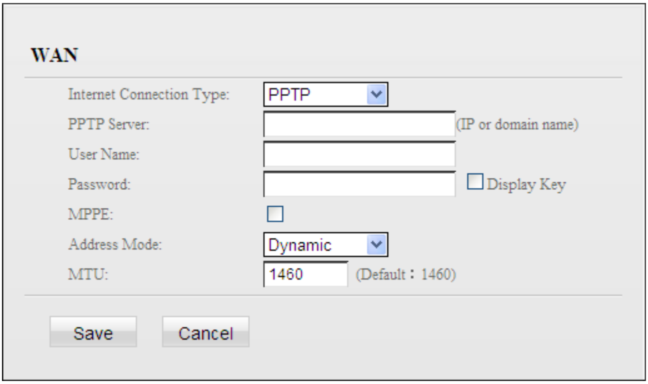
WAN

| | |
|---|---|
| Internet Connection Type: | Static IP |
| IP Address: | 192.168.100.47 |
| Subnet Mask | 255.255.255.0 |
| GateWay: | 192.168.100.1 |
| Primary DNS Server: | 172.16.100.205 |
| Secondary DNS Server: | 192.168.0.1 |
| MTU: | 1500 (Default: 1500) |

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

- MTU: Maximum Transmission Unit. The factory default is 1500.

3) PPTP: Select PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. The PPTP connects a router to a VPN server. For example : A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.



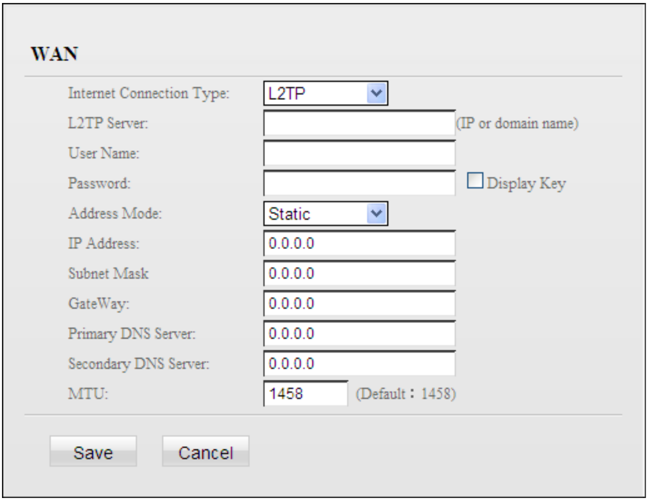
WAN

| | |
|---|---|
| Internet Connection Type: | PPTP |
| PPTP Server: | (IP or domain name) |
| User Name: | |
| Password: | □ Display Key |
| MPPE: | □ |
| Address Mode: | Dynamic |
| MTU: | 1460 (Default : 1460) |

- Internet connection Type: Displays a list of available Internet connection types.
- PPTP Server: Enter the IP address of a PPTP server.
- User Name: Enter your PPTP User Name.
- Password: Enter your Password.
- MPPE: Select whether to enable the MPPE authentication method.
- 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 local ISP if you are not clear.
- Subnet mask: Enter the subnet mask provided by your ISP. Consult your ISP if you are not clear.
- Default Gateway: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MTU: Maximum Transmission Unit. The factory default is 1460.

4) L2TP: Select L2TP (Layer 2 Tunneling Protocol) if your ISP uses an L2TP connection. The L2TP connects your router to a L2TP server. For example : A corporate branch and headquarter can use this connection type to implement mutual and secure access to each other's resources.

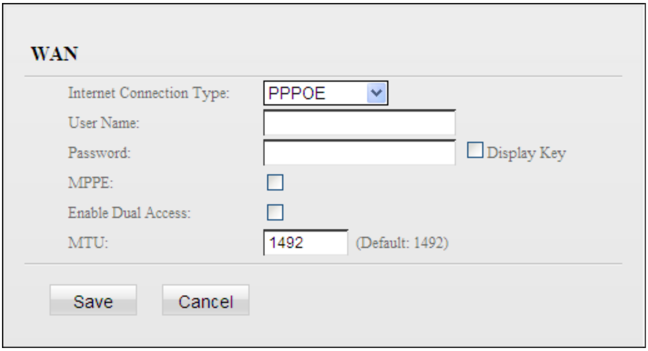


WAN

| | | |
|---|---|---|
| Internet Connection Type: | L2TP | |
| L2TP Server: | | (IP or domain name) |
| User Name: | | |
| Password: | | □ Display Key |
| Address Mode: | Static | |
| IP Address: | 0.0.0.0 | |
| Subnet Mask | 0.0.0.0 | |
| GateWay: | 0.0.0.0 | |
| Primary DNS Server: | 0.0.0.0 | |
| Secondary DNS Server: | 0.0.0.0 | |
| MTU: | 1458 | (Default：1458) |

- Internet connection Type: Displays a list of available Internet connection types.
- L2TP Server: Enter the IP address of a L2TP server.
- User Name: Enter your L2TP User Name.
- Password: Enter your Password.
- 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 local ISP if you are not clear.
- Default Gateway: Enter the gateway provided by your ISP. Consult your local ISP if you are not clear.
- Primary/Secondary DNS Server: Enter the Primary and Secondary DNS Server Addresses. Consult your local ISP if you are not clear.
- MTU: Maximum Transmission Unit. The factory default is 1458.

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



WAN

| | |
|---|---|
| Internet Connection Type: | PPPOE |
| User Name: | |
| Password: | □ Display Key |
| MPPE: | □ |
| Enable Dual Access: | □ |
| MTU: | 1492 (Default: 1492) |

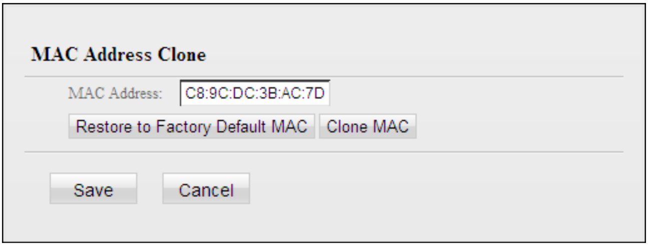
- Internet connection Type: Displays a list of available Internet connection types.
- User Name: Enter the PPPoE User Name provided by your ISP. Consult your ISP if you are not clear.
- Password: Enter the PPPoE Password provided by your ISP. Consult your ISP if you are not clear.
- MPPE: Select whether to enable the MPPE authentication method.
- Enable Dual Access: Select whether to enable Dual Access.
- MTU: Maximum Transmission Unit. The factory default is 1492.

⚠ **Note:**

It is not advisable to change the factory default MTU value unless necessary as an improper MTU value may degrade your network performance or even lead to network malfunction.

### 4.3.3 MAC Clone

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



MAC Address Clone

MAC Address: C8:9C:DC:3B:AC:7D

- MAC Address: Config Device's WAN MAC address.
- Clone MAC: Clicking this button populates the MAC address of your PC to the MAC Address field on the Device.
- Restore to Factory Default MAC: Reset Device's WAN MAC to factory default.

⚠ **Note:**

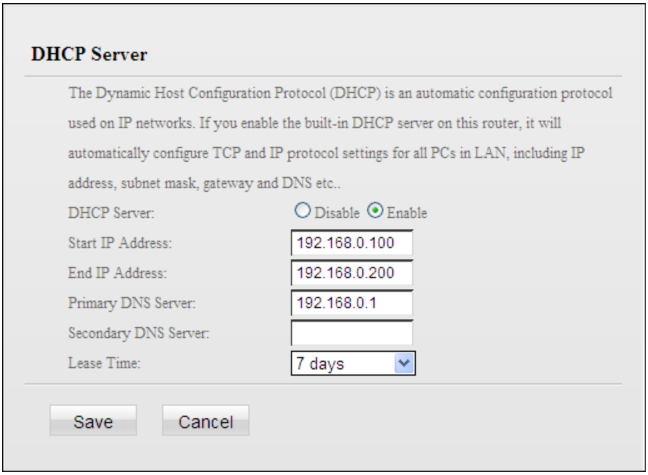
1. Normally you don't need to change the default WAN MAC value. However, some ISP may bind client PC's MAC address for Internet connection authentication. In this case, simply enter such MAC in the WAN MAC Address field or click the "Clone MAC" button. Note that the WAN MAC address in "Status" interface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

### 4.4.4 DHCP

"DHCP" includes 3 submenus: DHCP Server, Client List and Static Assignment. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.

#### DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this device, it will automatically configure TCP/IP protocol settings for all PCs in LAN, including IP address, subnet mask, gateway and DNS etc.



**DHCP Server**

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this router, it will automatically configure TCP and IP protocol settings for all PCs in LAN, including IP address, subnet mask, gateway and DNS etc..

|  |  |
|---|---|
| DHCP Server: | ○ Disable ● Enable |
| Start IP Address: | 192.168.0.100 |
| End IP Address: | 192.168.0.200 |
| Primary DNS Server: | 192.168.0.1 |
| Secondary DNS Server: | |
| Lease Time: | 7 days |

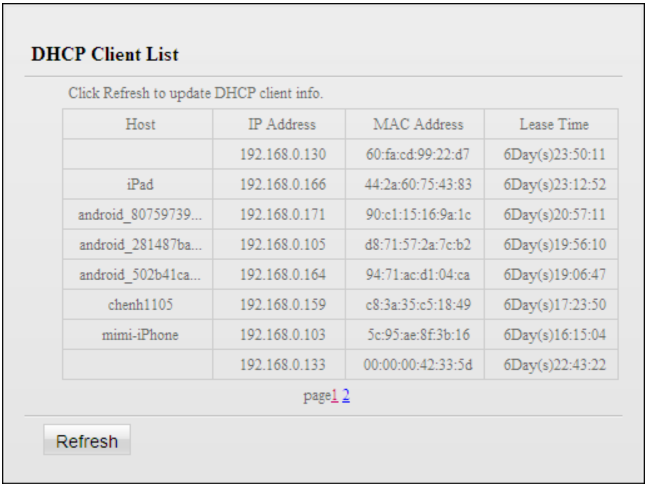
- DHCP Server: Select whether to enable or disable the Device's DHCP server feature.
- Start IP Address: Enter the starting IP address for the DHCP server's IP assignment.
- End IP Address: Enter the ending IP address for the DHCP server's IP assignment.
- Lease Time: The length of time for the IP address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

⚠ **Note:**

To apply the DHCP server settings to all PCs on your LAN, you must set all PCs to "Obtain an IP address automatically" and "Obtain DNS server address automatically" respectively.

## DHCP Client List

This section displays a DHCP dynamic client list, which includes host name, IP address, MAC address and lease time info.



DHCP Client List

Click Refresh to update DHCP client info.

| Host | IP Address | MAC Address | Lease Time |
|---|---|---|---|
|  | 192.168.0.130 | 60:fa:cd:99:22:d7 | 6Day(s)23:50:11 |
| iPad | 192.168.0.166 | 44:2a:60:75:43:83 | 6Day(s)23:12:52 |
| android_80759739... | 192.168.0.171 | 90:c1:15:16:9a:1c | 6Day(s)20:57:11 |
| android_281487ba... | 192.168.0.105 | d8:71:57:2a:7c:b2 | 6Day(s)19:56:10 |
| android_502b41ca... | 192.168.0.164 | 94:71:ac:d1:04:ca | 6Day(s)19:06:47 |
| chenh1105 | 192.168.0.159 | c8:3a:35:c5:18:49 | 6Day(s)17:23:50 |
| mimi-iPhone | 192.168.0.103 | 5c:95:ae:8f:3b:16 | 6Day(s)16:15:04 |
|  | 192.168.0.133 | 00:00:00:42:33:5d | 6Day(s)22:43:22 |

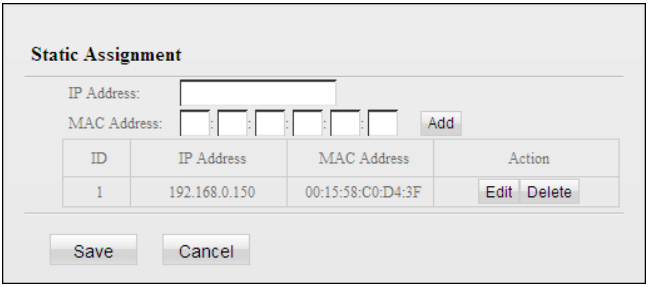
page1 2

- Host: Displays clients' host names.
- IP Address: Displays IP address(s) that client(s) obtained from the DHCP server.
- MAC Address: Displays MAC address of a given host.
- Lease Time: Remaining time for a corresponding IP address lease.

## Static Assignment

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

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



Static Assignment

IP Address:

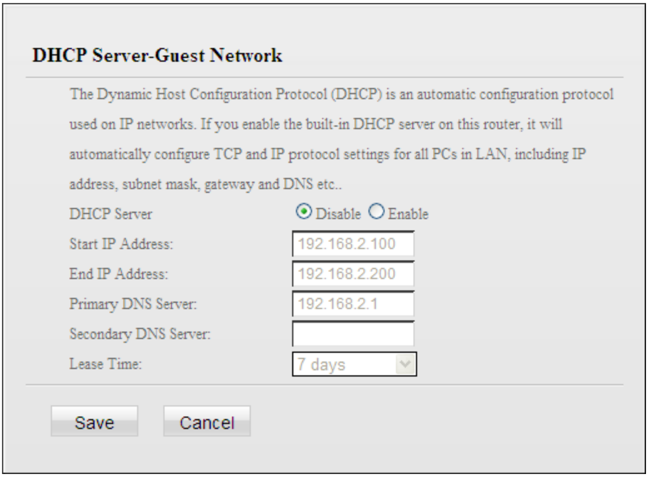
MAC Address: : : : : : Add

| ID | IP Address | MAC Address | Action |
|---|---|---|---|
| 1 | 192.168.0.150 | 00:15:58:C0:D4:3F | Edit Delete |

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

### 4.3.5 DHCP Server-Guest Network

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



**DHCP Server-Guest Network**

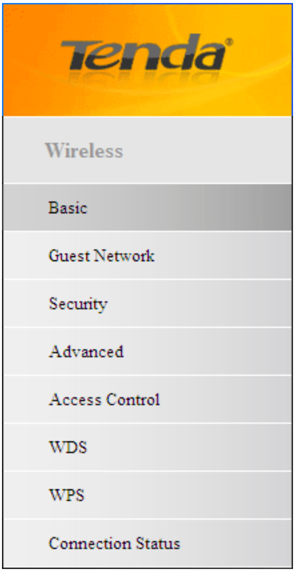
The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol used on IP networks. If you enable the built-in DHCP server on this router, it will automatically configure TCP and IP protocol settings for all PCs in LAN, including IP address, subnet mask, gateway and DNS etc..

| | |
|---|---|
| DHCP Server | ● Disable ○ Enable |
| Start IP Address: | 192.168.2.100 |
| End IP Address: | 192.168.2.200 |
| Primary DNS Server: | 192.168.2.1 |
| Secondary DNS Server: | |
| Lease Time: | 7 days |

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

## 4.4 Wireless

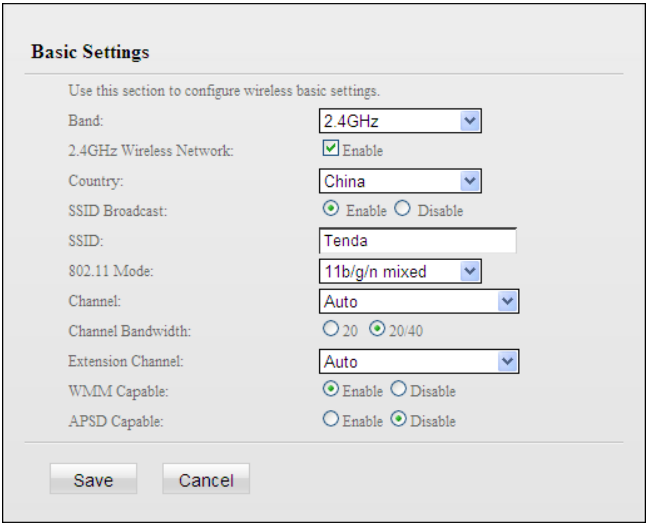
The "Wireless" tab includes 8 submenus: Basic, Guest Network, Security, Advanced, Access Control, WPS, WDS and Connection Status. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



### 4.4.1 Basic

This section allows you to manage your wireless network (2.4G or 5G). You can select your country, config wireless network name (SSID), network mode and channel settings, etc. the way you want.

## Basic Settings--2.4G



Basic Settings

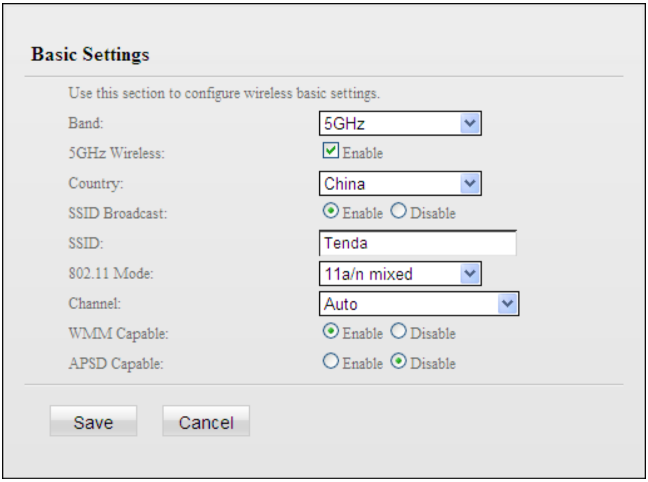
Use this section to configure wireless basic settings.

| | |
|---|---|
| Band: | 2.4GHz |
| 2.4GHz Wireless Network: | ☑ Enable |
| Country: | China |
| SSID Broadcast: | ● Enable ○ Disable |
| SSID: | Tenda |
| 802.11 Mode: | 11b/g/n mixed |
| Channel: | Auto |
| Channel Bandwidth: | ○ 20 ● 20/40 |
| Extension Channel: | Auto |
| WMM Capable: | ● Enable ○ Disable |
| APSD Capable: | ○ Enable ● Disable |

- Band: Select 2.4GHz or 5GHz.
- 2.4GHz Wireless Network: Check/uncheck to enable/disable the 2.4GHz wireless feature. If disabled, all 2.4GHz-based features will be disabled accordingly.
- Country: Select your country from the drop-down list. There are 12 options available.
- SSID Broadcast: Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. By default, it is enabled. When disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.

- SSID ：A SSID (Service Set Identifier) is the unique name of a wireless network.
- 802.11 Mode: Select a right mode according to your wireless client. The default mode is 11b/g/n mixed.
- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- Channel Bandwidth: Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select 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 ：Available only in 11b/g/n mixed mode.
- WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- ASPD Capable ：Select to enable/disable the auto power saving mode.

## Basic Settings--5G



**Basic Settings**

Use this section to configure wireless basic settings.

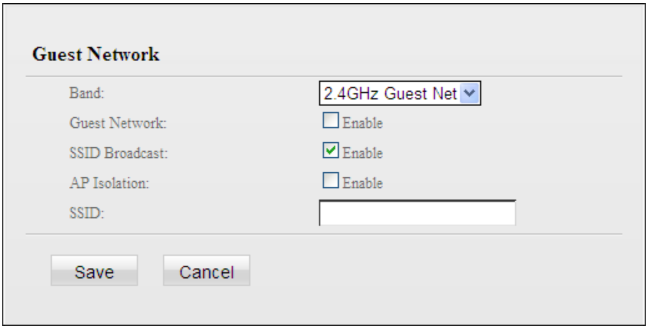
| | |
|---|---|
| Band: | 5GHz |
| 5GHz Wireless: | ☑ Enable |
| Country: | China |
| SSID Broadcast: | ● Enable ○ Disable |
| SSID: | Tenda |
| 802.11 Mode: | 11a/n mixed |
| Channel: | Auto |
| WMM Capable: | ● Enable ○ Disable |
| APSD Capable: | ○ Enable ● Disable |

- Band: Select 2.4GHz or 5GHz.
- 5GHz Wireless Network: Check/uncheck to enable/disable the 5GHz wireless feature. If disabled, all 5GHz-based features will be disabled accordingly.
- Country: Select your country from the drop-down list.
- SSID Broadcast: Select "Enable"/"Disable" to make your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. By default, it is enabled. When disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.
- SSID: A SSID (Service Set Identifier) is the unique name of a wireless network; it is configurable.
- 802.11 Mode: Select a right mode according to your wireless client. The default mode is 11a/n.

- Channel: For an optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or "Auto" to let device detect and select the best possible channel for your wireless network to operate on from the drop-down list.
- WMM-Capable: WMM is QoS for your wireless network. Enabling this option may better stream wireless multimedia data (such as video or audio).
- ASPD Capable：Select to enable/disable the auto power saving mode. By default, this option is disabled.

### 4.4.2 .Guest Network

The Guest Network feature allows guests to access Internet and other users on the guest network while disallowing them to access Device web manager, users on master network and clients behind the LAN ports. Thus the wireless master network is secured. You can find the guest network available in both 2.4G and 5G networks. Here we present you how to config such feature on 2.4GHz band, which also applies to 5GHz.



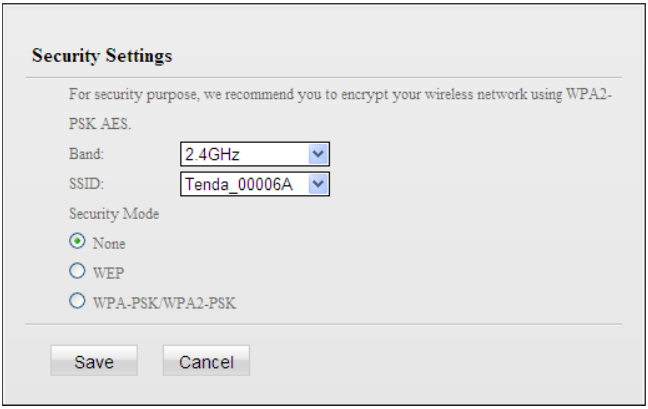
Guest Network

|  |  |
|---|---|
| Band: | 2.4GHz Guest Net |
| Guest Network: | □ Enable |
| SSID Broadcast: | ☑ Enable |
| AP Isolation: | □ Enable |
| SSID: |  |

- Band: Select 2.4GHz or 5GHz.
- Guest Network: Select to enable/disable the guest network feature.
- SSID Broadcast: Check to enable/disable the SSID feature, making your wireless network visible/ invisible to any wireless clients within coverage when they perform a scan to see what's available. By default, it is enabled. When disabled, wireless clients will have to first know this SSID and manually enter it on their devices if they want to connect to the SSID.
- AP Isolation: If enabled, clients connecting to the guest network will be mutually inaccessible.
- SSID：A SSID (Service Set Identifier) is the unique name of a wireless network.

### 4.4.3 Security

This section allows you to encrypt both 2.4GHz wireless and 5GHz wireless networks to block unauthorized accesses and malicious packet sniffing.



Security Settings

For security purpose, we recommend you to encrypt your wireless network using WPA2-PSK AES.

Band: 2.4GHz

SSID: Tenda_00006A

Security Mode

● None

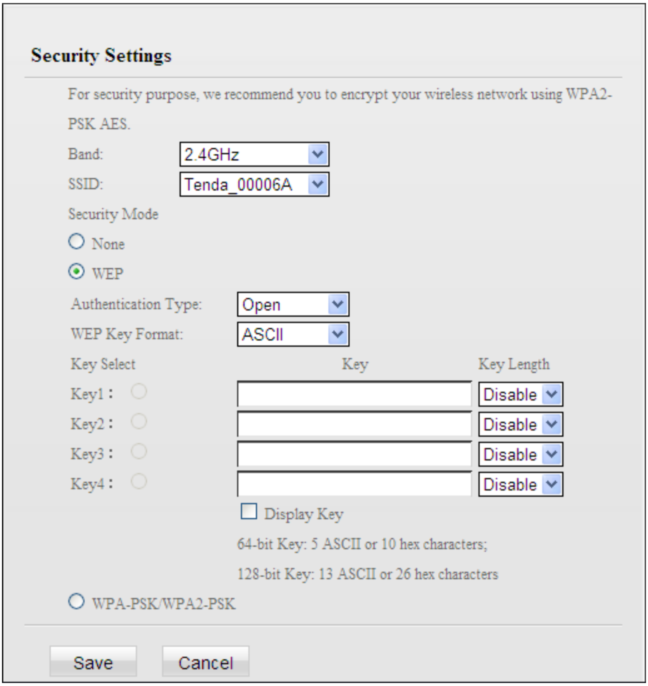
○ WEP

○ WPA-PSK/WPA2-PSK

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

## 1、 WEP

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



**Security Settings**

For security purpose, we recommend you to encrypt your wireless network using WPA2-PSK AES.

Band: 2.4GHz

SSID: Tenda_00006A

Security Mode

○ None

● WEP

Authentication Type: Open

WEP Key Format: ASCII

| Key Select | | Key | Key Length |
|---|---|---|---|
| Key1 : | ○ | | Disable |
| Key2 : | ○ | | Disable |
| Key3 : | ○ | | Disable |
| Key4 : | ○ | | Disable |

□ Display Key

64-bit Key: 5 ASCII or 10 hex characters;

128-bit Key: 13 ASCII or 26 hex characters

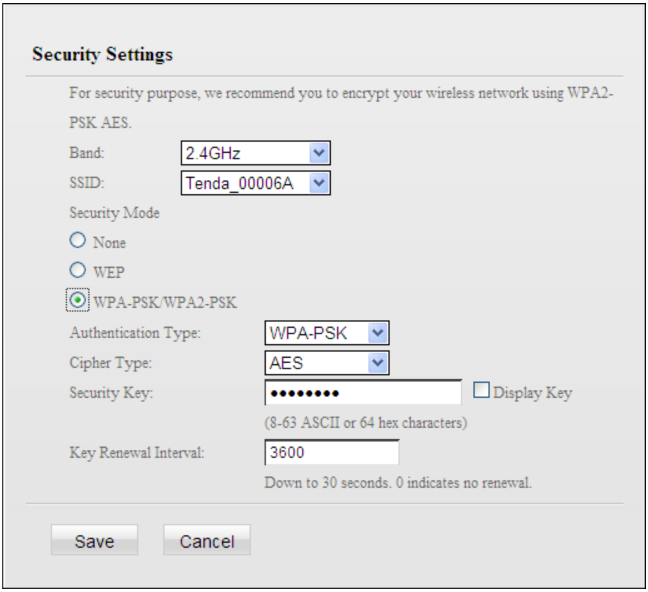
○ WPA-PSK/WPA2-PSK

➢ Authentication Type: Select "Open" or "Shared" from the drop-down list.

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

## 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. WPA adopts enhanced encryption algorithm over WEP.



Security Settings

For security purpose, we recommend you to encrypt your wireless network using WPA2-PSK AES.

Band: 2.4GHz

SSID: Tenda_00006A

Security Mode

○ None

○ WEP

● WPA-PSK/WPA2-PSK

Authentication Type: WPA-PSK

Cipher Type: AES

Security Key: ••••••••• □ Display Key

(8-63 ASCII or 64 hex characters)

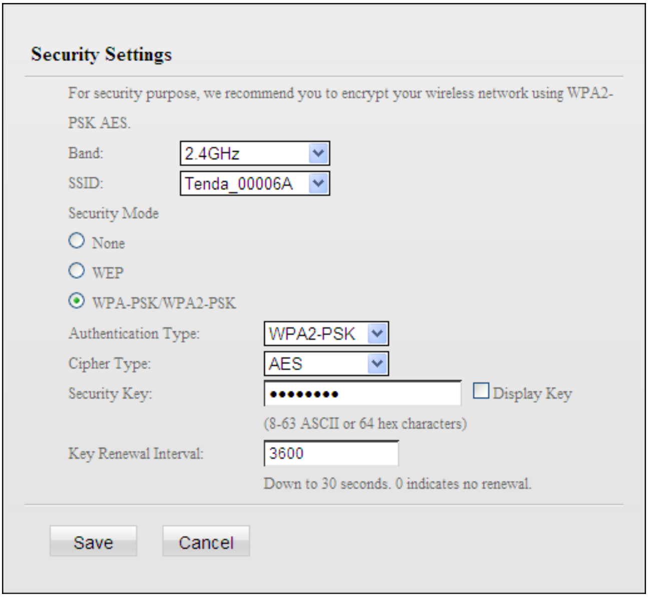
Key Renewal Interval: 3600

Down to 30 seconds. 0 indicates no renewal.

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

## 3、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.



Security Settings

For security purpose, we recommend you to encrypt your wireless network using WPA2-PSK AES.

Band: 2.4GHz

SSID: Tenda_00006A

Security Mode

○ None

○ WEP

● WPA-PSK/WPA2-PSK

Authentication Type: WPA2-PSK

Cipher Type: AES

Security Key: ••••••••• □ Display Key

(8-63 ASCII or 64 hex characters)

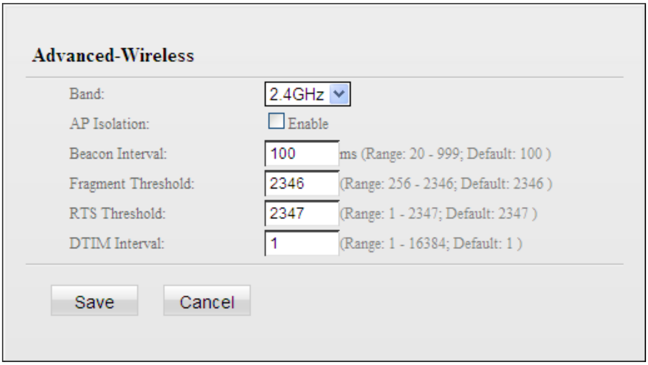
Key Renewal Interval: 3600

Down to 30 seconds. 0 indicates no renewal.

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

### 4.4.4 Advanced Settings

This section allows you to config advanced settings, including AP Isolation, Beacon interval , Fragment threshold , RTS threshold and DTIM interval, etc, for both 2.4G and 5G wireless networks.



**Advanced-Wireless**

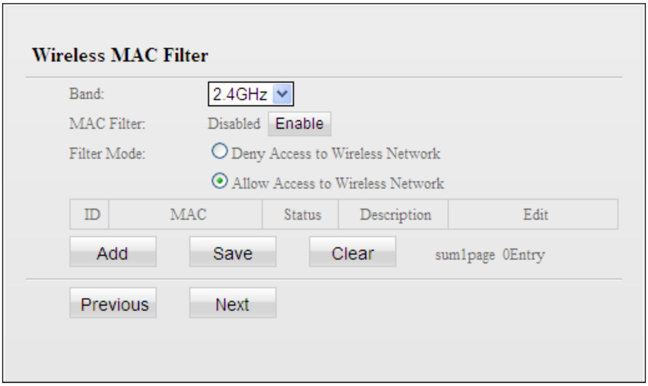
|  |  |  |
|---|---|---|
| Band: | 2.4GHz |  |
| AP Isolation: | □ Enable |  |
| Beacon Interval: | 100 | ms (Range: 20 - 999; Default: 100 ) |
| Fragment Threshold: | 2346 | (Range: 256 - 2346; Default: 2346 ) |
| RTS Threshold: | 2347 | (Range: 1 - 2347; Default: 2347 ) |
| DTIM Interval: | 1 | (Range: 1 - 16384; Default: 1 ) |

- AP Isolation: Isolates clients connecting to master SSID.
- Beacon Interval: A time interval between any 2 consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Do NOT change the default value of 100 unless necessary.
- Fragment Threshold: Specify a Fragment Threshold value. Any wireless packet exceeding the preset value will be divided into several fragments before transmission. DO NOT change the default value of 2346 unless necessary.

- RTS Threshold: If a packet exceeds such set value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. For normal SOHO, it is recommended to keep the default value unchanged; otherwise, device performance may be degraded.
- DTIM Interval: A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrives at device's buffer, the device will send DTIM (delivery traffic indication message) and DTIM interval to wake clients up for receiving these packets.

### 4.4.5 Access Control

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your 2.4G or 5G wireless network. Here we present you how to config such feature in 2.4GHz band, which also applies to 5GHz network.



Wireless MAC Filter

Band: 2.4GHz

MAC Filter: Disabled Enable

Filter Mode:
○ Deny Access to Wireless Network
● Allow Access to Wireless Network

| ID | MAC | Status | Description | Edit |
|---|---|---|---|---|

sum1page 0Entry

- Filter:

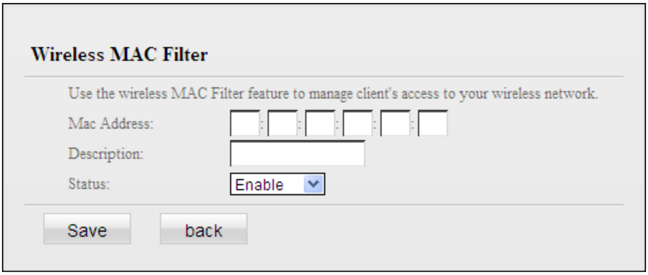
  Disabled: Indicates the MAC filter feature is disabled.
  Enabled: Indicates the MAC filter feature is enabled.
  Enable: Enable the MAC filter feature.
  Disable: Disable the MAC filter feature.

- Filter Mode:

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

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

Click Add and below screen appears:



Wireless MAC Filter

Use the wireless MAC Filter feature to manage client's access to your wireless network.

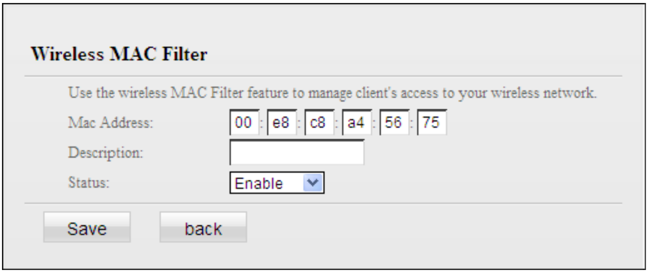
Mac Address: □:□:□:□:□:□

Description: □

Status: Enable

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

Example: 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:

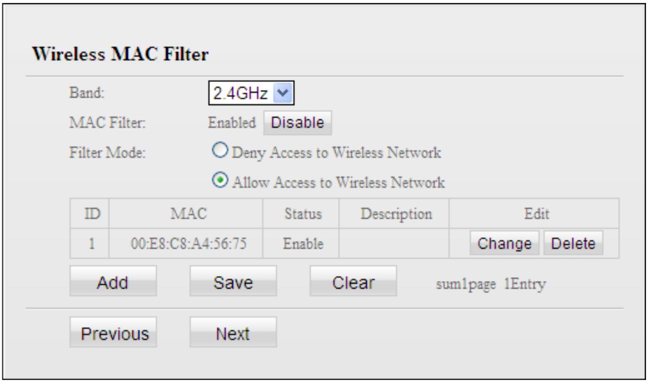


Wireless MAC Filter

Use the wireless MAC Filter feature to manage client's access to your wireless network.

|  |  |
|---|---|
| Mac Address: | 00 : e8 : c8 : a4 : 56 : 75 |
| Description: |  |
| Status: | Enable |

Click Save and the MAC address filter list will appear.



Wireless MAC Filter

Band: 2.4GHz

MAC Filter: Enabled Disable

Filter Mode: ○ Deny Access to Wireless Network

● Allow Access to Wireless Network

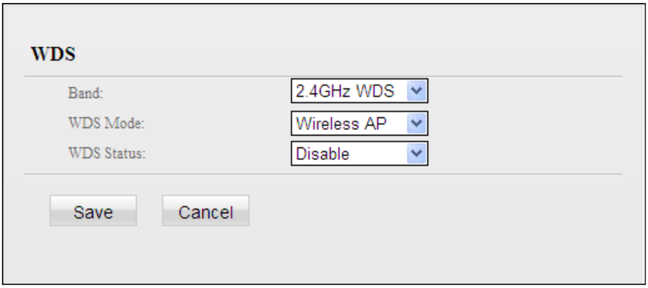
| ID | MAC | Status | Description | Edit |
|---|---|---|---|---|
| 1 | 00:E8:C8:A4:56:75 | Enable |  | Change Delete |

sum1page 1Entry

- ➢ Change: Click to edit an existing entry.
- ➢ Delete: Click to delete a corresponding entry.
- ➢ Clear: Click to delete all entries.

### 4.4.6 WDS

WDS (Wireless Distribution System) feature can be used to extend your existing 2.4G or 5G wireless network coverage. Here we present you how to config such feature in 2.4GHz, which also applies to 5GHz.


WDS

Band: 2.4GHz WDS

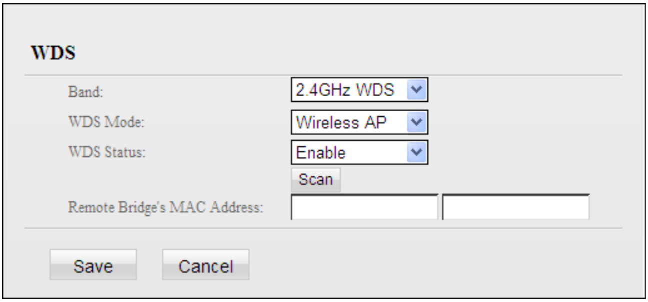
WDS Mode: Wireless AP

WDS Status: Disable

Band: Select 2.4GHz or 5GHz.
WDS Mode: Select wireless AP or wireless bridge Mode.
WDS Status: Select to enable/disable the WDS feature.

Example: To use the WDS feature on two WDS-capable devices, do as follows:

1. Select wireless bridge mode and "Enable"



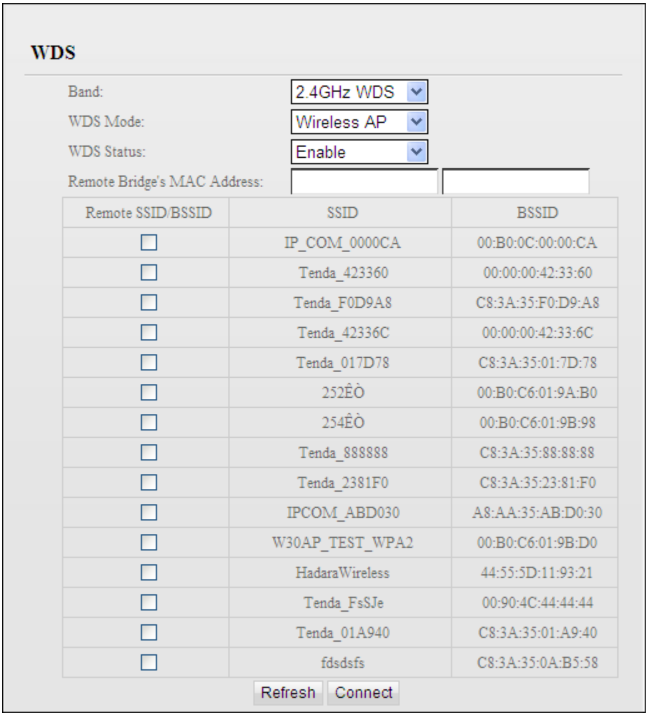
WDS

Band: 2.4GHz WDS

WDS Mode: Wireless AP

WDS Status: Enable

2. Click "Scan" to search available wireless networks (Only wireless APs operating on the same channel as the Device can be searched. To ensure that the two devices involved communicate on the same channel, set the channel on the Device to "Auto" before clicking Scan).



**WDS**

Band: 2.4GHz WDS

WDS Mode: Wireless AP

WDS Status: Enable

Remote Bridge's MAC Address:

| Remote SSID/BSSID | SSID | BSSID |
|---|---|---|
| □ | IP_COM_0000CA | 00:B0:0C:00:00:CA |
| □ | Tenda_423360 | 00:00:00:42:33:60 |
| □ | Tenda_F0D9A8 | C8:3A:35:F0:D9:A8 |
| □ | Tenda_42336C | 00:00:00:42:33:6C |
| □ | Tenda_017D78 | C8:3A:35:01:7D:78 |
| □ | 252ÊÒ | 00:B0:C6:01:9A:B0 |
| □ | 254ÊÒ | 00:B0:C6:01:9B:98 |
| □ | Tenda_888888 | C8:3A:35:88:88:88 |
| □ | Tenda_2381F0 | C8:3A:35:23:81:F0 |
| □ | IPCOM_ABD030 | A8:AA:35:AB:D0:30 |
| □ | W30AP_TEST_WPA2 | 00:B0:C6:01:9B:D0 |
| □ | HadaraWireless | 44:55:5D:11:93:21 |
| □ | Tenda_FsSJe | 00:90:4C:44:44:44 |
| □ | Tenda_01A940 | C8:3A:35:01:A9:40 |
| □ | fdsdfs | C8:3A:35:0A:B5:58 |

3. Simply check the wireless network you want to connect to. After successfully completing settings on the Device, repeat above operations on the other device. When the two devices added each other's MAC address, the WDS may be implemented successfully.

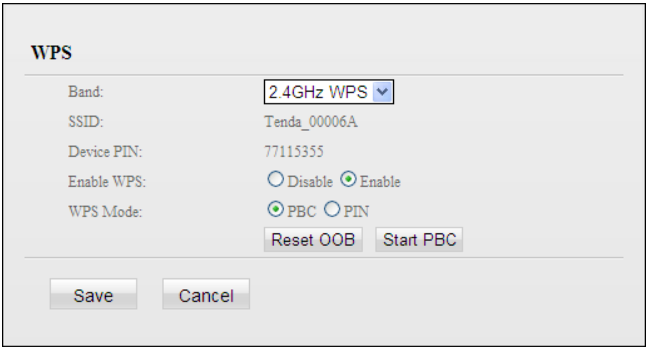
⚠ **Note:**

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.

2. Note that the the two devices involved must have different IP addresses on the same IP net segment. In addition, it is advisable to disable the DHCP server on either device.

### 4.4.7 WPS

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



WPS

Band: 2.4GHz WPS

SSID: Tenda_00006A

Device PIN: 77115355

Enable WPS: ○ Disable ● Enable

WPS Mode: ● PBC ○ PIN

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

**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 device, and the WPS LED turns off. Repeat steps mentioned above if you want to add more wireless client devices to the device.

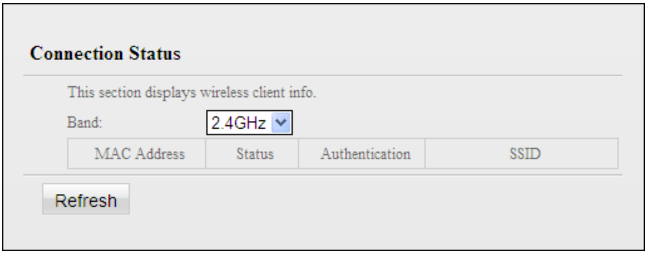
PIN: To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

⚠ **Note:**

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

### 4.4.8 Connection Status

This interface displays the information of currently connected wireless clients (if any).



Connection Status

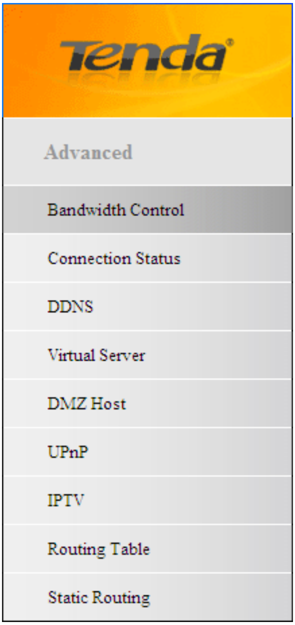
This section displays wireless client info.

Band: 2.4GHz

| MAC Address | Status | Authentication | SSID |
|---|---|---|---|

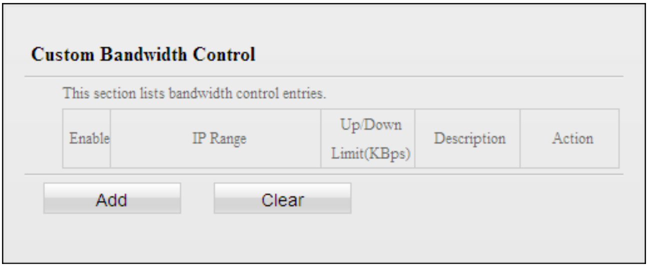
## 4.5 Advanced Applications

The “Advanced” tab includes the following 9 submenus: Bandwidth Control, Connection Status, DDNS, Virtual Server, DMZ Host, UPnP, Routing Table and Static Routing. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



## 4.5.1 Bandwidth Control

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

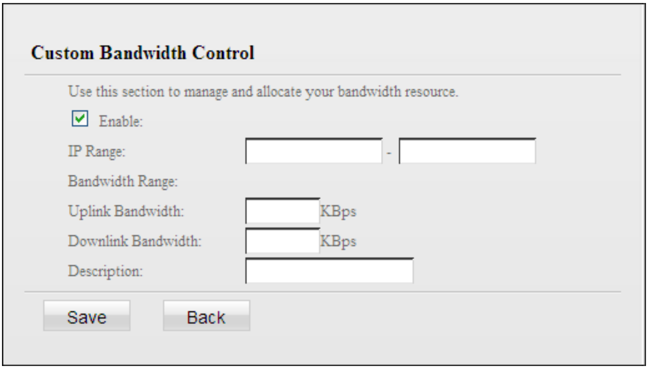


Custom Bandwidth Control

This section lists bandwidth control entries.

| Enable | IP Range | Up/Down Limit(KBps) | Description | Action |
|---|---|---|---|---|

Click "Add" to display the page below:



**Custom Bandwidth Control**

Use this section to manage and allocate your bandwidth resource.

☑ Enable:

IP Range: ____ - ____

Bandwidth Range:

Uplink Bandwidth: ____ KBps

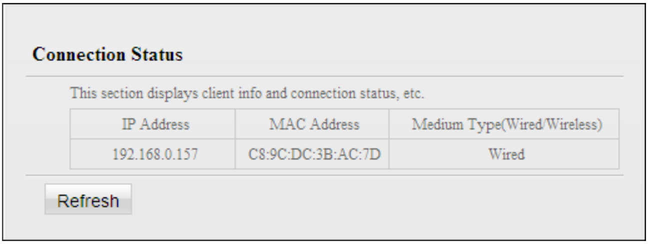
Downlink Bandwidth: ____ KBps

Description: ____

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

### 4.5.2 Connection Status

This section displays the information of clients (if any) connected to the router as seen in the screenshot.



Connection Status

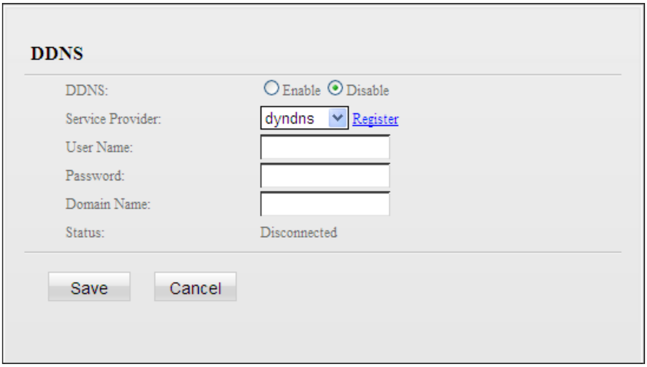
This section displays client info and connection status, etc.

| IP Address | MAC Address | Medium Type(Wired/Wireless) |
|---|---|---|
| 192.168.0.157 | C8:9C:DC:3B:AC:7D | Wired |

- IP Address: The IP address of a connected client.
- MAC Address: The MAC address of a connected client.
- Medium Type: Displays how a client is connected to the router: via a wireless or wired connection.

### 4.5.3 DDNS

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



DDNS

DDNS: ○ Enable ● Disable

Service Provider: dyndns Register

User Name:

Password:

Domain Name:

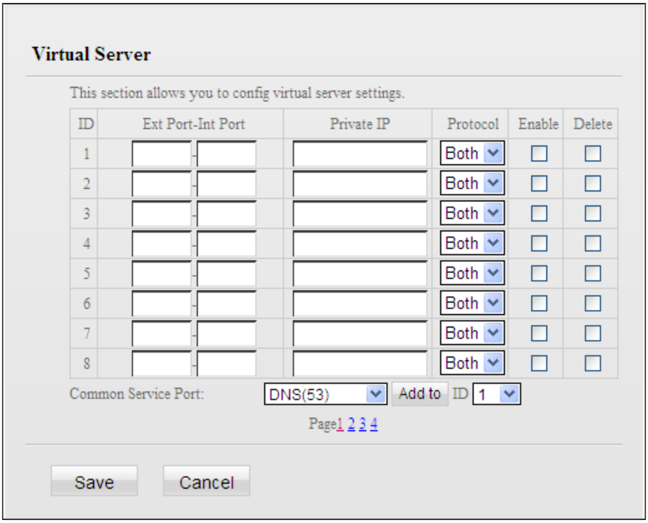
Status: Disconnected

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

Click "Save" to save your settings.

### 4.5.4 Virtual Server

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



**Virtual Server**

This section allows you to config virtual server settings.

| ID | Ext Port-Int Port | Private IP | Protocol | Enable | Delete |
|---|---|---|---|---|---|
| 1 | - | | Both | □ | □ |
| 2 | - | | Both | □ | □ |
| 3 | - | | Both | □ | □ |
| 4 | - | | Both | □ | □ |
| 5 | - | | Both | □ | □ |
| 6 | - | | Both | □ | □ |
| 7 | - | | Both | □ | □ |
| 8 | - | | Both | □ | □ |

Common Service Port: DNS(53) Add to ID 1

Page1 2 3 4

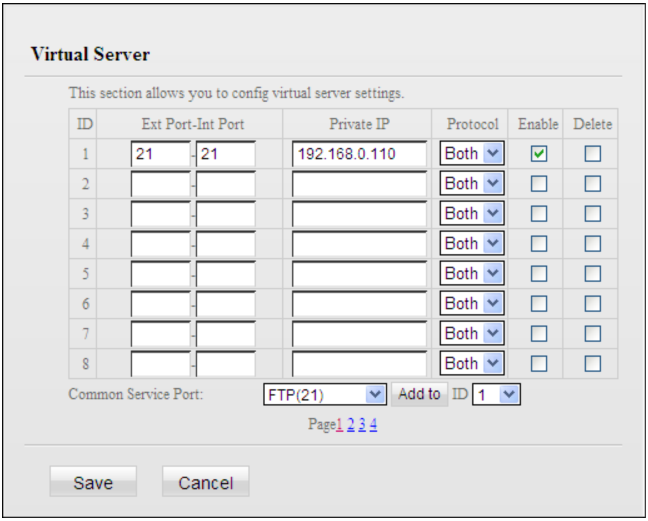
- Ext Port- Int Port: External Port- Internal Port; Enter the WAN/LAN service ports.
- Private IP: The IP address of a computer used as a server in LAN.
- Protocol: Includes TCP, UDP and Both. Select "Both" if you are not sure about which protocol to use
- Enable: The corresponding entry takes effect only if you checked this option.
- Delete: Remove a corresponding entry.

Well-Known Service Port: The "Well-Known Service Port" lists widely used protocol ports. Simply select a port, an entry ID and click the "Add to" button to 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 Virtual Server feature to let your friends access these files. Assuming that the static IP address of the FTP server (Namely, your PC) is 192.168.0.110, you 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 Ext Port and Int 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 192.168.0.110 for the "IP Address", select "TCP" and then select "Enable'.



Virtual Server

This section allows you to config virtual server settings.

| ID | Ext Port-Int Port | Private IP | Protocol | Enable | Delete |
|---|---|---|---|---|---|
| 1 | 21 - 21 | 192.168.0.110 | Both | ☑ | □ |
| 2 | - |  | Both | □ | □ |
| 3 | - |  | Both | □ | □ |
| 4 | - |  | Both | □ | □ |
| 5 | - |  | Both | □ | □ |
| 6 | - |  | Both | □ | □ |
| 7 | - |  | Both | □ | □ |
| 8 | - |  | Both | □ | □ |

Common Service Port: FTP(21) Add to ID 1

Page1 2 3 4

Save Cancel

3 Click "Save" to save your settings.

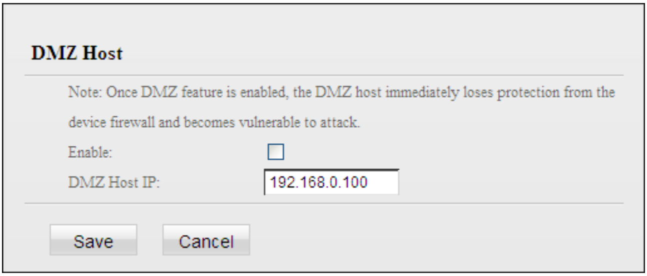
Now, your friends only need to enter ftp://xxx.xxx.xxx.xxx:21 in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the router's WAN IP address. Assuming it is 172.16.102.89, then your friends need to enter "ftp://172.16.102.89: 21" in their browsers.

⚠ **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.

### 4.5.5 DMZ Host

In some cases, a computer needs 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

Note: Once DMZ feature is enabled, the DMZ host immediately loses protection from the device firewall and becomes vulnerable to attack.

Enable: □

DMZ Host IP: 192.168.0.100

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

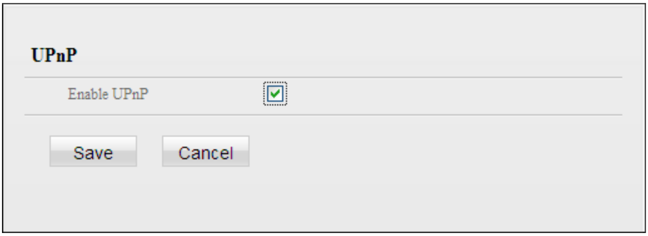
⚠ **Note:**

1. Once a PC is set to a DMZ host, it will be completely exposed to Internet, and thus may be vulnerable to attacks as related firewall settings become inoperative.

2. Users on WAN access the DMZ host through a corresponding WAN IP address.

### 4.5.6 UPnP

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



UPnP

Enable UPnP ☑

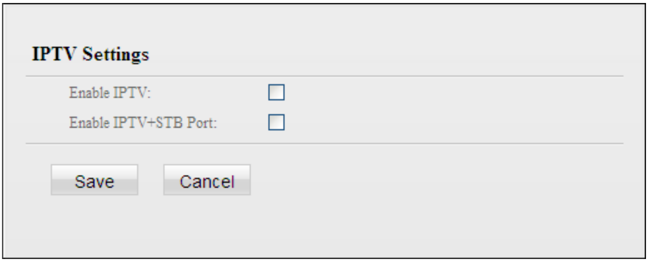
Enable UPnP: Check/uncheck to enable/disable the UPnP feature.

⚠ **Note:**

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

### 4.5.7 IPTV

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



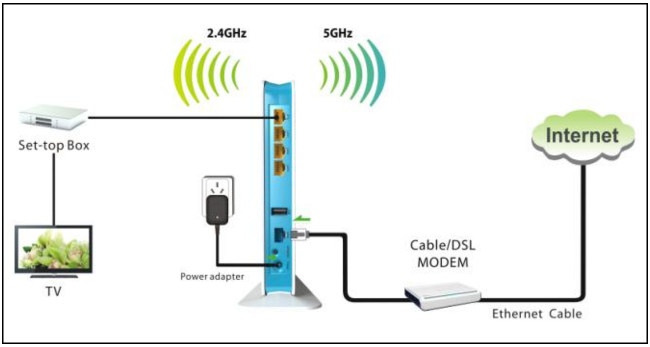
IPTV Settings

Enable IPTV: □

Enable IPTV+STB Port: □

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

See below for the network topology:

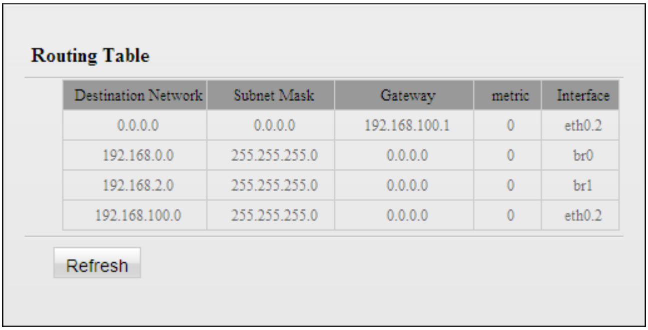


⚠ **Note:**

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

## 4.5.8 Routing Table

This section displays the routing table content.

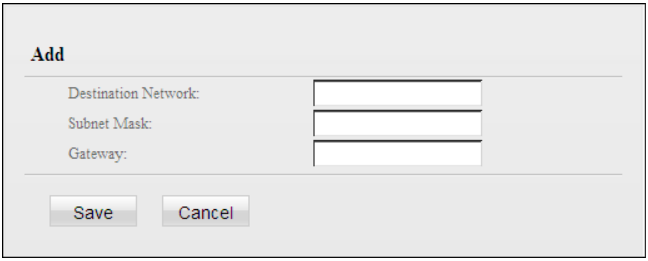


Routing Table

| Destination Network | Subnet Mask | Gateway | metric | Interface |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.100.1 | 0 | eth0.2 |
| 192.168.0.0 | 255.255.255.0 | 0.0.0.0 | 0 | br0 |
| 192.168.2.0 | 255.255.255.0 | 0.0.0.0 | 0 | br1 |
| 192.168.100.0 | 255.255.255.0 | 0.0.0.0 | 0 | eth0.2 |

## 4.5.9 Static Routing

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



Add

Destination Network:

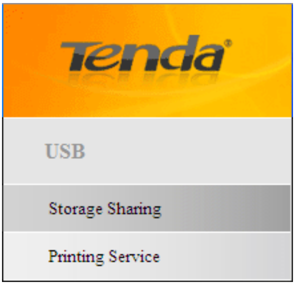
Subnet Mask:

Gateway:

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

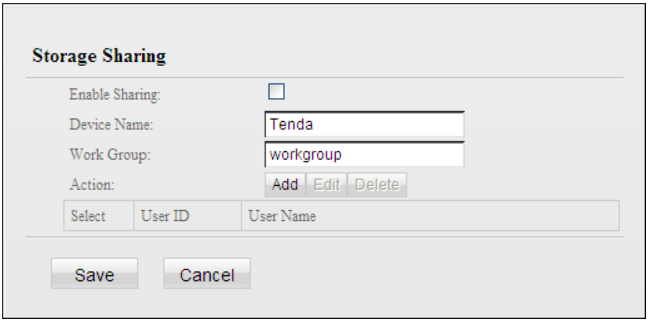
## 4.6 USB

The Router provides a USB interface for USB device connection. The "USB" tab includes two submenus: "Storage Sharing" and "Printing Service".



### 4.6.1 Storage Sharing

The storage sharing feature allows you to share files on the storage device attached to the Device.



Storage Sharing

| | |
|---|---|
| Enable Sharing: | □ |
| Device Name: | Tenda |
| Work Group: | workgroup |
| Action: | Add Edit Delete |

| Select | User ID | User Name |
|---|---|---|

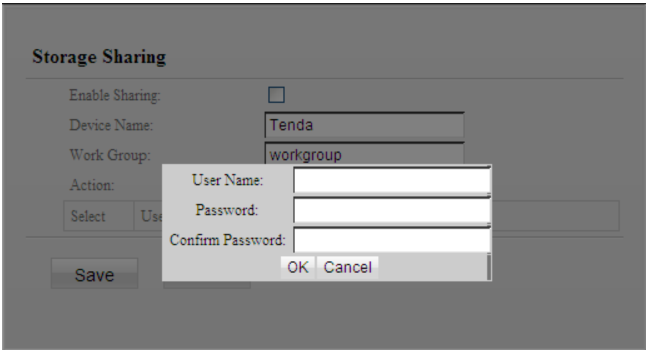
- Enable Sharing: Check/uncheck to enable/disable storage sharing feature.
- Device Name: Define a meaningful name to you for the device.
- Work Group: Define a work group name for the device.
- Add: Click to add a user account. Up to 5 accounts can be added.
- Edit: Click to edit an existing account.
- Delete: Click to delete an existing account.

## Operation Instructions:

Before sharing files on a USB storage device, you must create a user account.

1. Create account:

1). Click "Add" to display a dialogue box as seen below:



**Storage Sharing**

Enable Sharing: □

Device Name: Tenda

Work Group: workgroup

Action:

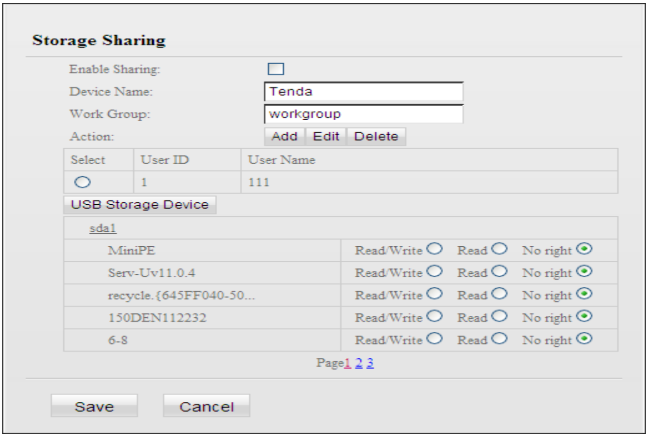
Select | Us

User Name:

Password:

Confirm Password:

2) a. Enter a user name and a password, which will be used to authenticate users trying to access the USB storage device for sharing files. b. Re-type to confirm password. Click the "OK" button and below screen will appear:



**Storage Sharing**

Enable Sharing: □

Device Name: Tenda

Work Group: workgroup

Action: Add Edit Delete

| Select | User ID | User Name |
|---|---|---|
| ○ | 1 | 111 |

USB Storage Device

sda1

| | | | |
|---|---|---|---|
| MiniPE | Read/Write ○ | Read ○ | No right ● |
| Serv-Uv11.0.4 | Read/Write ○ | Read ○ | No right ● |
| recycle.{645FF040-50... | Read/Write ○ | Read ○ | No right ● |
| 150DEN112232 | Read/Write ○ | Read ○ | No right ● |
| 6-8 | Read/Write ○ | Read ○ | No right ● |

Page1 2 3

2. Set Access Right

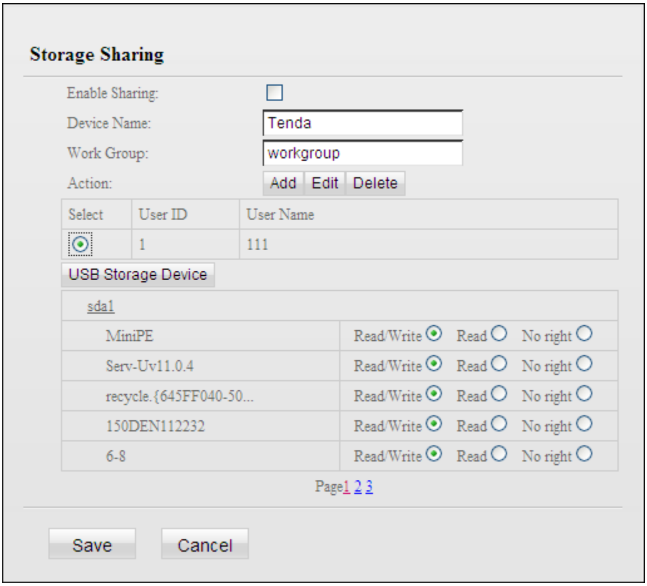
First select an account and click USB Storage Device. And then select a proper access right from below for each entry.

Read/Write ：The right to Read and Write.

Read: The right to Read.

No right: No right to share corresponding file.

Click "Save" to apply all settings.



Storage Sharing

Enable Sharing: □

Device Name: Tenda

Work Group: workgroup

Action: Add Edit Delete

| Select | User ID | User Name |
|---|---|---|
| ● | 1 | 111 |

USB Storage Device

sda1

| | | | |
|---|---|---|---|
| MiniPE | Read/Write ● | Read ○ | No right ○ |
| Serv-Uv11.0.4 | Read/Write ● | Read ○ | No right ○ |
| recycle.{645FF040-50... | Read/Write ● | Read ○ | No right ○ |
| 150DEN112232 | Read/Write ● | Read ○ | No right ○ |
| 6-8 | Read/Write ● | Read ○ | No right ○ |

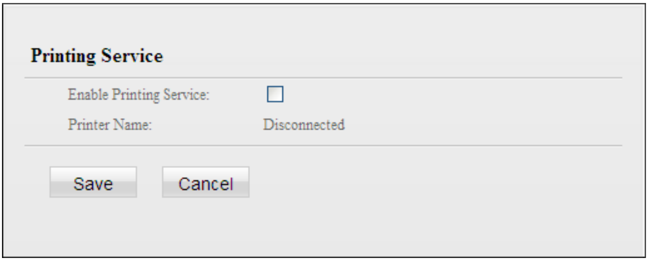
Page1 2 3

3. Access shared file

To access resources on such storage device, double click "My Computer" on your PC and enter \\192.168.0.1.

## 4.6.2 USB Printing Service

The USB printing service allows you to connect a USB printer to the device and thus all clients on your network can print anything they want on their PCs. The Router can identify a printer automatically as long as it is successfully connected.



Printing Service

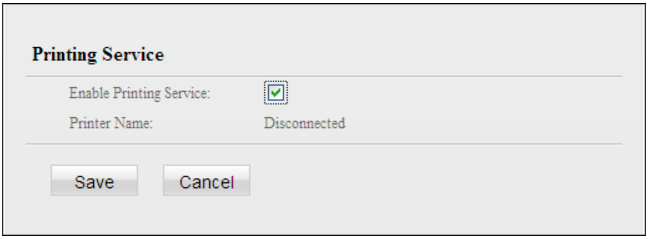
Enable Printing Service: □

Printer Name: Disconnected

- ➢ Enable Printing Service: Check/uncheck to enable/disable USB printing service.

**Operation Instructions:**

1. Correctly connect your USB printer to the USB port on the device.
2. Enable Printing Service

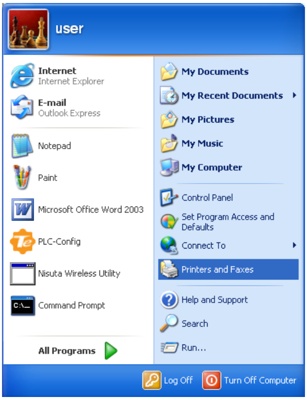


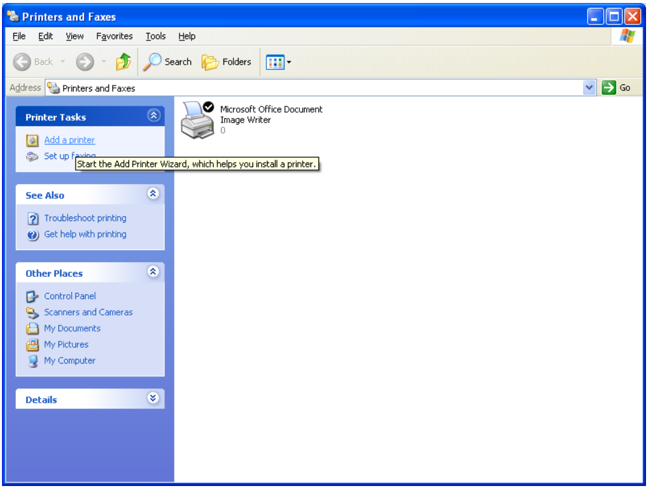
Printing Service

Enable Printing Service: ☑

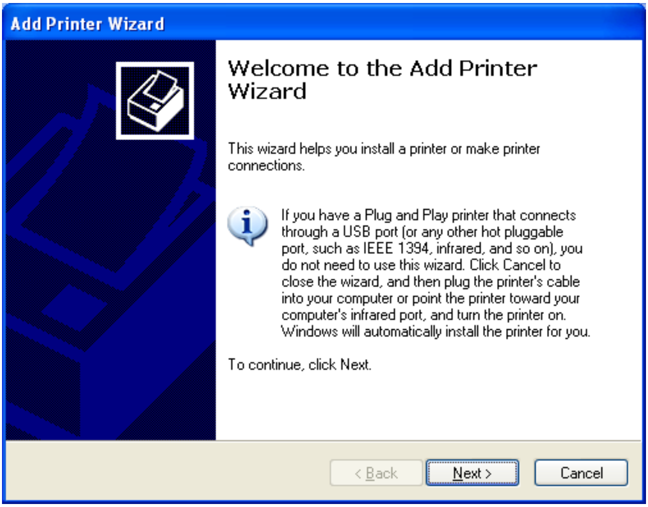
Printer Name: Disconnected

3. On your PC (connected to the device), click "Start"——"Settings"——"Printers and Faxes" and select "Add a printer" on appearing window.





4. Click "Next".



Add Printer Wizard

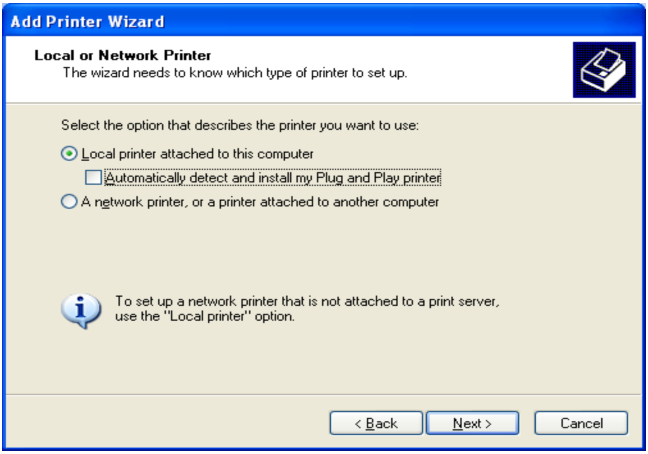
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

5. Select "Local printer attached to this computer" and click ""Next.



Add Printer Wizard

**Local or Network Printer**
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

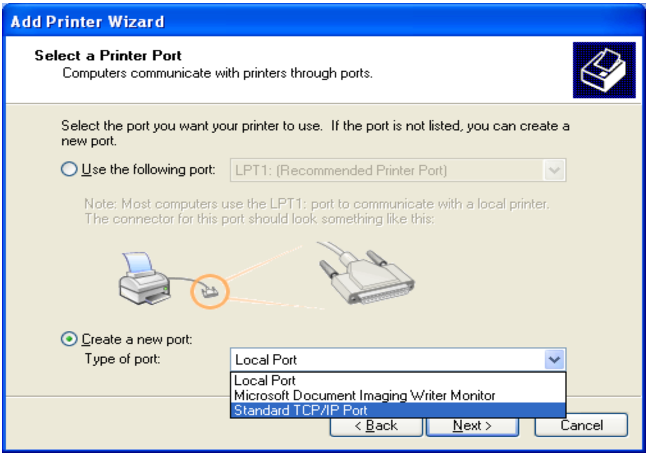
● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

6. Select "Create a new port", Type of port: "Standard TCP/IP Port" and click "Next".



Add Printer Wizard

Select a Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

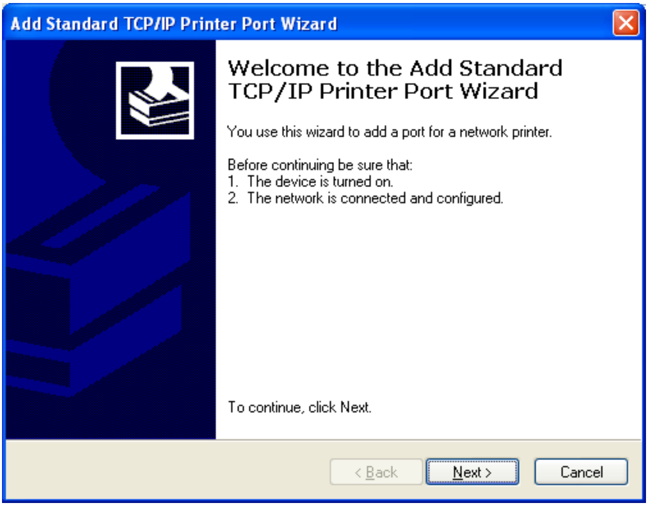
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:

Type of port: Local Port

Local Port
Microsoft Document Imaging Writer Monitor
Standard TCP/IP Port

7. Click "Next".



Add Standard TCP/IP Printer Port Wizard

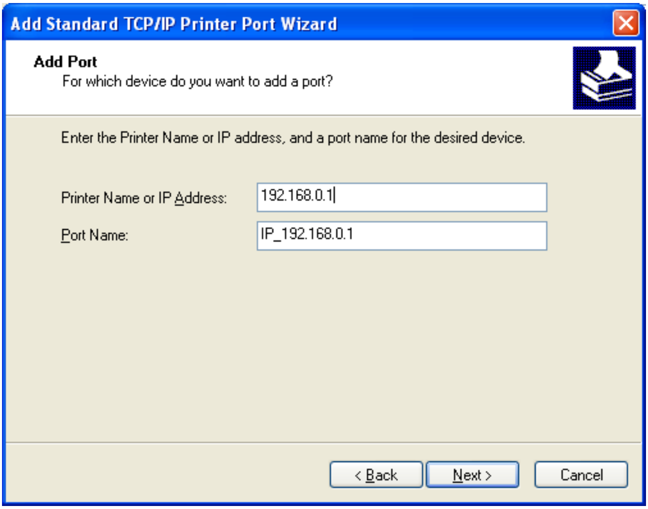
Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

8. Enter Router's LAN IP address and click "Next".



Add Standard TCP/IP Printer Port Wizard

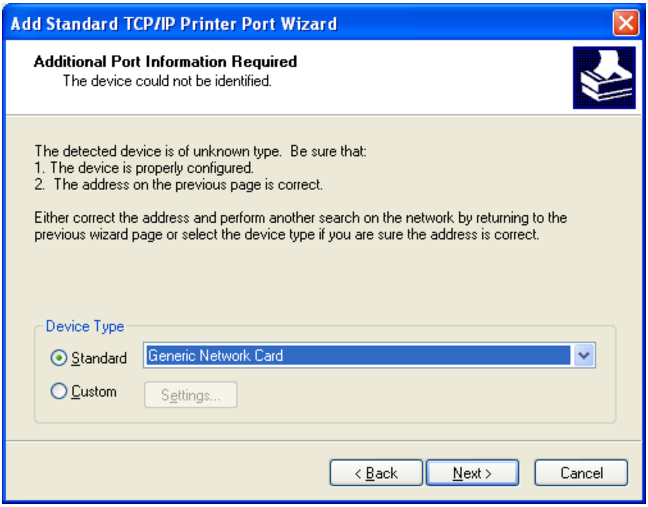
**Add Port**
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.0.1

Port Name: IP_192.168.0.1

9. Click "Standard" under Device Type and select "Generic Network Card", then click "Next".



Add Standard TCP/IP Printer Port Wizard

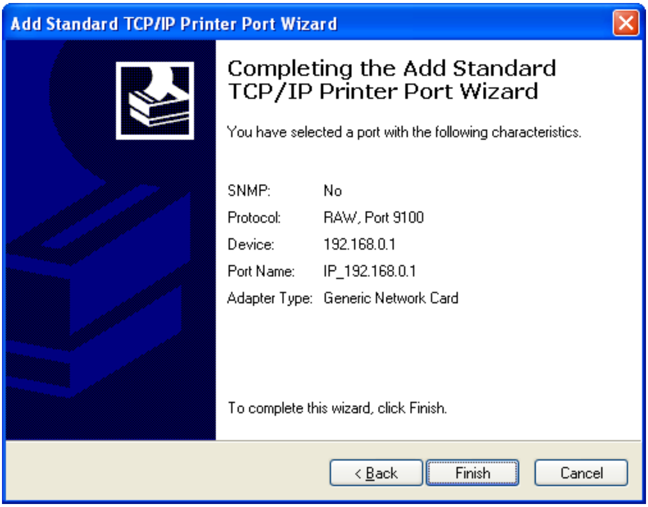
**Additional Port Information Required**
The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type
● Standard: Generic Network Card
○ Custom

10. Click "Finish".



Add Standard TCP/IP Printer Port Wizard

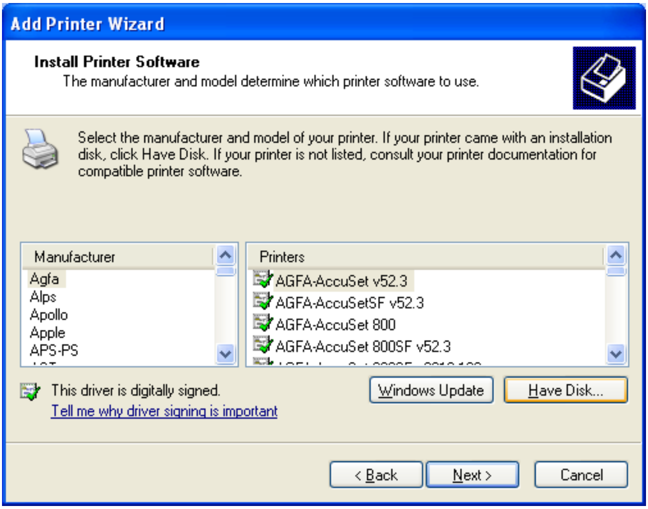
Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

| | |
|---|---|
| SNMP: | No |
| Protocol: | RAW, Port 9100 |
| Device: | 192.168.0.1 |
| Port Name: | IP_192.168.0.1 |
| Adapter Type: | Generic Network Card |

To complete this wizard, click Finish.

11. Select "Have Disk".



Add Printer Wizard

**Install Printer Software**

The manufacturer and model determine which printer software to use.

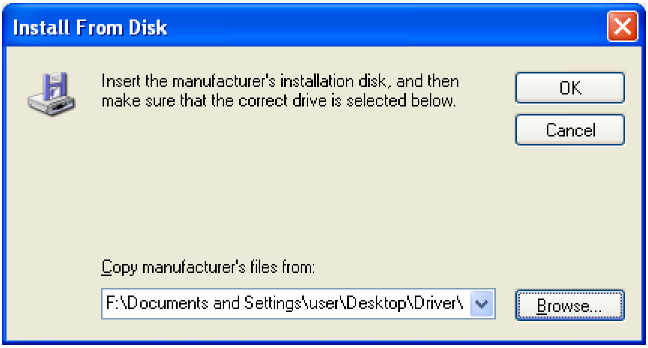
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

| Manufacturer | Printers |
|---|---|
| Agfa | AGFA-AccuSet v52.3 |
| Alps | AGFA-AccuSetSF v52.3 |
| Apollo | AGFA-AccuSet 800 |
| Apple | AGFA-AccuSet 800SF v52.3 |
| APS-PS | |

This driver is digitally signed.

Tell me why driver signing is important

12. Click “Browse”, select corresponding drive file and click “Open”. At last click “OK”.



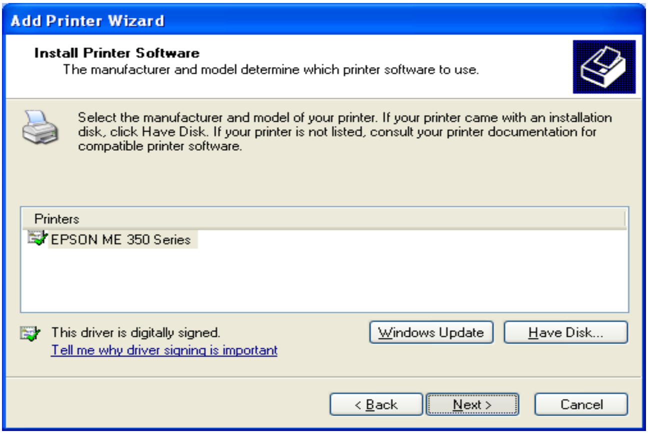
Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

F:\Documents and Settings\user\Desktop\Driver\

13. Click “Next”.



Add Printer Wizard

Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

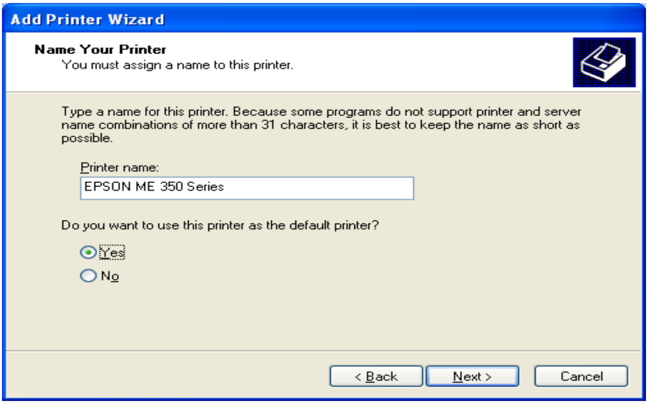
Printers

EPSON ME 350 Series

This driver is digitally signed.

Tell me why driver signing is important

14. Define a name for the printer and click "Next".



**Name Your Printer**

You must assign a name to this printer.

Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.

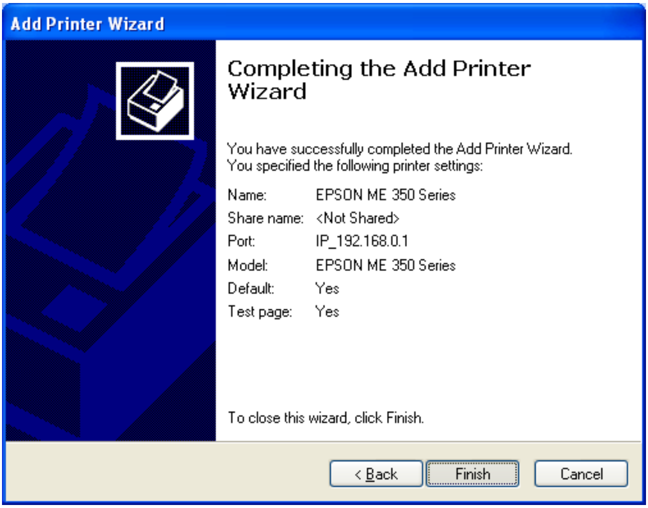
Printer name: EPSON ME 350 Series

Do you want to use this printer as the default printer?

● Yes

○ No

15. Click "Finish".



Completing the Add Printer Wizard

You have successfully completed the Add Printer Wizard. You specified the following printer settings:

Name: EPSON ME 350 Series

Share name: <Not Shared>

Port: IP_192.168.0.1

Model: EPSON ME 350 Series

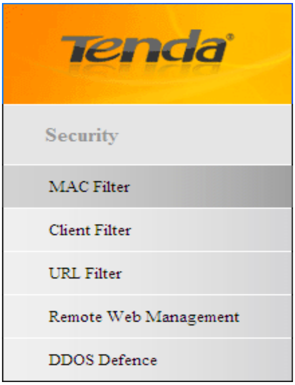
Default: Yes

Test page: Yes

To close this wizard, click Finish.

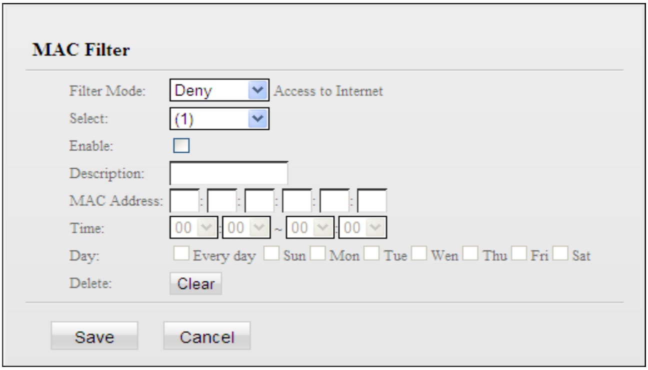
## 4.7 Security

The "Security" tab includes 5 submenus: MAC Filter, Client Filter, URL Filter, Remote Web Management and DDoS Deffence. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



### 4.7.1 MAC Filter

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



MAC Filter

Filter Mode: Deny Access to Internet

Select: (1)

Enable: □

Description:

MAC Address: : : : : :

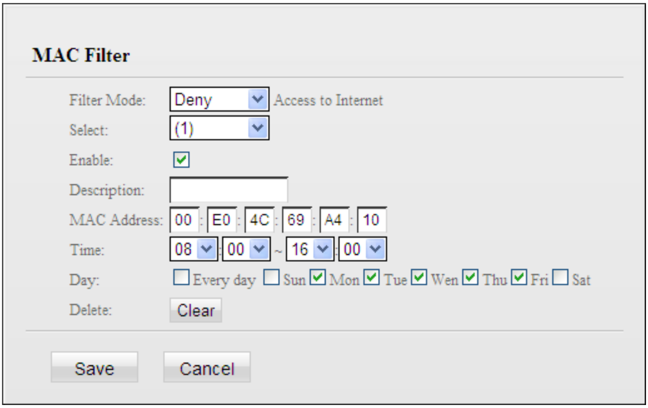
Time: 00 : 00 ~ 00 : 00

Day: □ Every day □ Sun □ Mon □ Tue □ Wen □ Thu □ Fri □ Sat

Delete: Clear

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

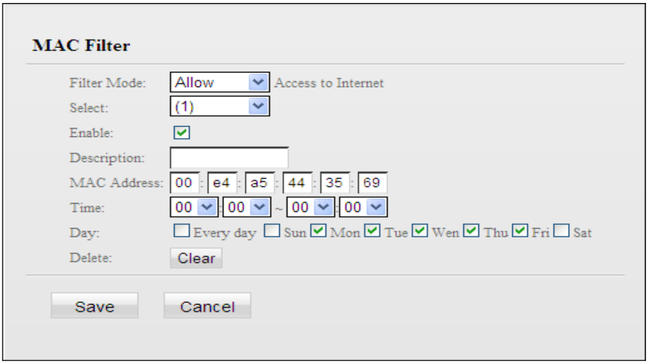
Example1: To prevent a PC at the MAC address of 00:E0:4C:69:A4:10 from accessing Internet between 8:00 and16:00 on working days: from Monday to Friday, config same settings as seen on the screenshot below on your device:



MAC Filter

| | |
|---|---|
| Filter Mode: | Deny Access to Internet |
| Select: | (1) |
| Enable: | ☑ |
| Description: | |
| MAC Address: | 00 : E0 : 4C : 69 : A4 : 10 |
| Time: | 08 : 00 ~ 16 : 00 |
| Day: | □ Every day □ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri □ Sat |
| Delete: | Clear |

Example2: To allow a PC at the MAC address of 00:E4:A5:44:35:69 to access Internet from Monday to Friday, config same settings as seen on the screenshot below on your device:



MAC Filter

Filter Mode: Allow Access to Internet

Select: (1)

Enable: ☑

Description:

MAC Address: 00 : e4 : a5 : 44 : 35 : 69

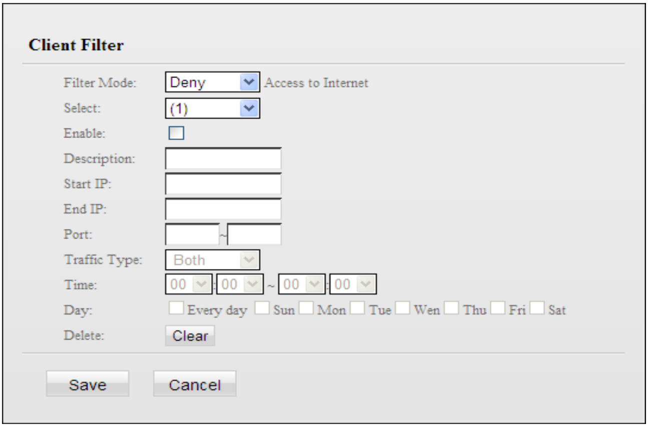
Time: 00 : 00 ~ 00 : 00

Day: □ Every day □ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri □ Sat

Delete: Clear

## 4.7.2 Client Filter

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



Client Filter

Filter Mode: Deny Access to Internet

Select: (1)

Enable: □

Description:

Start IP:

End IP:

Port: ~

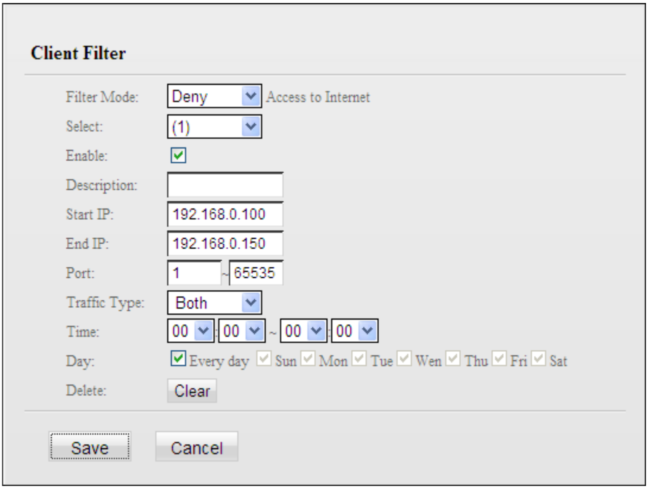
Traffic Type: Both

Time: 00 : 00 ~ 00 : 00

Day: □ Every day □ Sun □ Mon □ Tue □ Wen □ Thu □ Fri □ Sat

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

Example 1: To prohibit PCs within the IP address range of 192.168.0.100--192.168.0.150 from accessing Internet, do as follows:



Client Filter

Filter Mode: Deny Access to Internet

Select: (1)

Enable: ☑

Description:

Start IP: 192.168.0.100

End IP: 192.168.0.150

Port: 1 ~ 65535

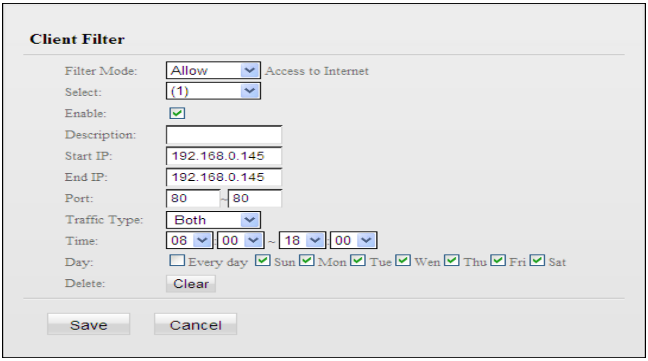
Traffic Type: Both

Time: 00 00 ~ 00 00

Day: ☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri ☑ Sat

Delete: Clear

Example 2: To allow only the PC at an IP address of 192.168. 0.145 to access Internet from 8:00 to 18：00, do as follows:



Client Filter

Filter Mode: Allow Access to Internet

Select: (1)

Enable: ☑

Description:

Start IP: 192.168.0.145

End IP: 192.168.0.145

Port: 80 ~ 80

Traffic Type: Both

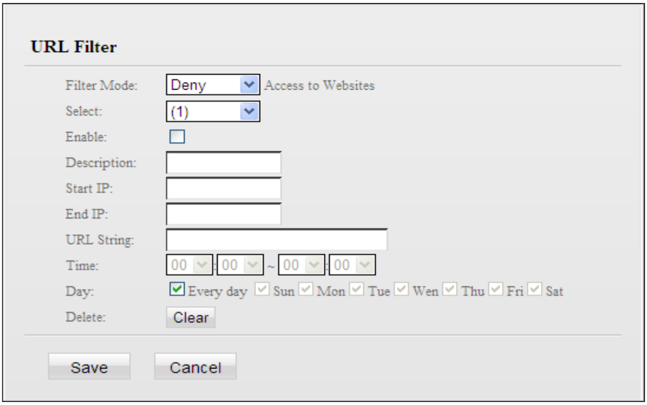
Time: 08 00 ~ 18 00

Day: □ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri ☑ Sat

Delete: Clear

### 4.7.3 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.



URL Filter

Filter Mode: Deny Access to Websites

Select: (1)

Enable: □

Description:

Start IP:

End IP:

URL String:

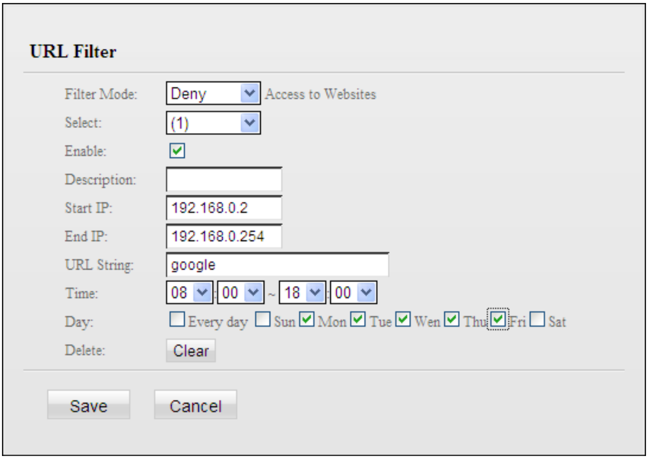
Time: 00 : 00 ~ 00 : 00

Day: ☑ Every day ☑ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri ☑ Sat

Delete: Clear

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

If you want to disallow all computers on your LAN to access google.com from 8：00 to 18：00 on working days: Monday-Friday, then do as follows:



URL Filter

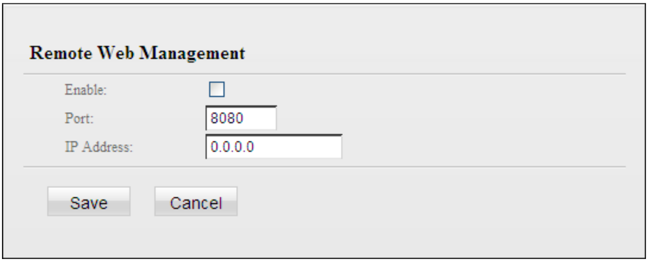
| | |
|---|---|
| Filter Mode: | Deny Access to Websites |
| Select: | (1) |
| Enable: | ☑ |
| Description: | |
| Start IP: | 192.168.0.2 |
| End IP: | 192.168.0.254 |
| URL String: | google |
| Time: | 08 : 00 ~ 18 : 00 |
| Day: | □ Every day □ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri □ Sat |
| Delete: | Clear |

⚠ **Note:**

Each entry can include up to 16 domain names, each of which must be separated with a symbol of " ".

### 4.7.4 Remote Web-based Management

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



Remote Web Management

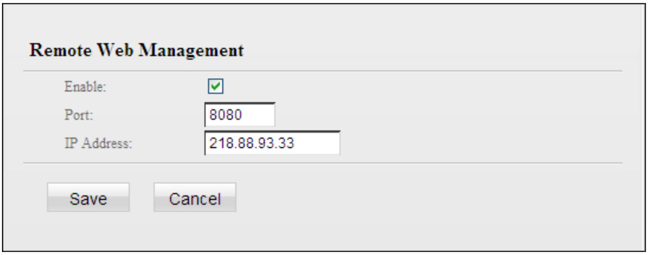
Enable: □

Port: 8080

IP Address: 0.0.0.0

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

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



Remote Web Management

Enable: ☑

Port: 8080

IP Address: 218.88.93.33

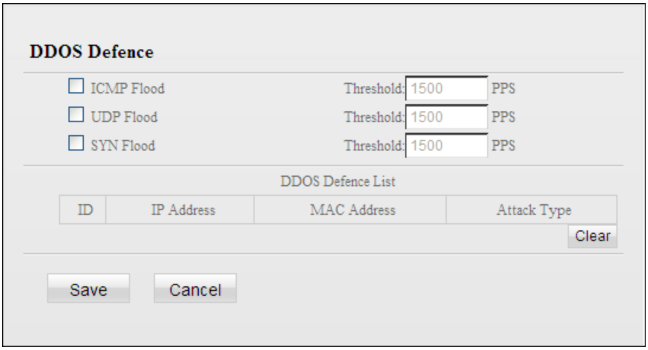
⚠ **Note:**

1. To access the Router via port 8080, enter "http://x.x.x.x:8080" where "x.x.x.x" represents the Internet IP address of the Router and 8080 is the port used for the Web-Management interface. Assuming the Router's Internet IP address is 220.135.211.56, then, simply replace the "x.x.x.x" with "220.135.211.56" (namely, http://220.135.211.56:8080).

Leaving the IP address field at "0.0.0.0" makes the router remotely accessible to all the PCs on Internet; populating it with a specific IP address such as 218.88.93.33 makes the Router only remotely accessible to the PC at the specified IP address.

### 4.7.5 DDOS Defence

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



DDOS Defence

☐ ICMP Flood Threshold: 1500 PPS

☐ UDP Flood Threshold: 1500 PPS

☐ SYN Flood Threshold: 1500 PPS

DDOS Defence List

| ID | IP Address | MAC Address | Attack Type |
|---|---|---|---|

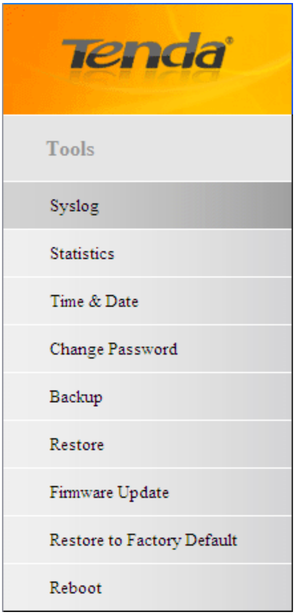
Clear

Save Cancel

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

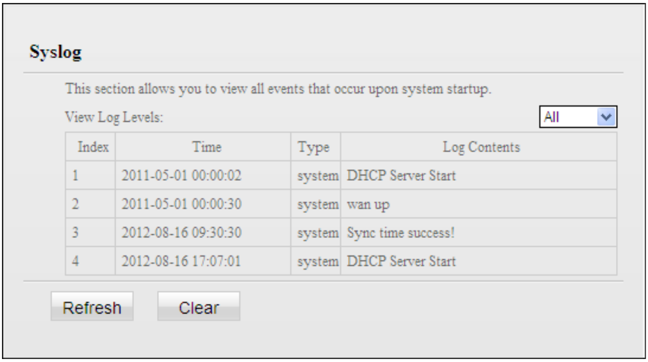
## 4.8 Tools

The "Tools" tab includes 9 submues: Syslog, Statistics, Time & Date, Change Password, Backup, Restore, Firmware Update, Restore to Factory Default and Reboot. Clicking any of them enters corresponding interface for configuration. Below explains, in details, each such feature.



## 4.8.1 Syslog

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



Syslog

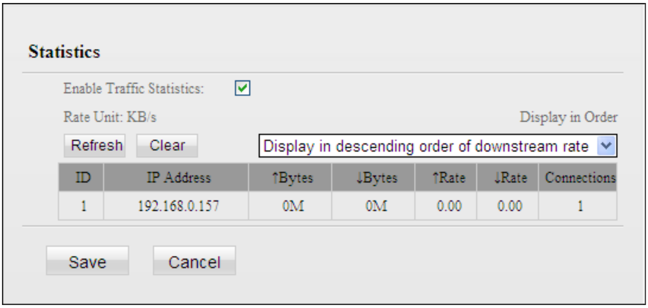
This section allows you to view all events that occur upon system startup.

View Log Levels: All

| Index | Time | Type | Log Contents |
|---|---|---|---|
| 1 | 2011-05-01 00:00:02 | system | DHCP Server Start |
| 2 | 2011-05-01 00:00:30 | system | wan up |
| 3 | 2012-08-16 09:30:30 | system | Sync time success! |
| 4 | 2012-08-16 17:07:01 | system | DHCP Server Start |

## 4. 8.2 Statistics

Statistics displays current traffic of clients on your LAN.



Statistics

Enable Traffic Statistics: ☑

Rate Unit: KB/s

Display in Order: Display in descending order of downstream rate

| ID | IP Address | ↑Bytes | ↓Bytes | ↑Rate | ↓Rate | Connections |
|---|---|---|---|---|---|---|
| 1 | 192.168.0.157 | 0M | 0M | 0.00 | 0.00 | 1 |

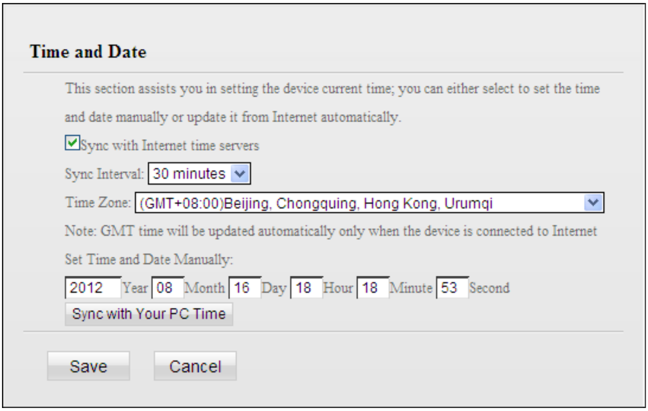
- Enable Traffic Statistics: Determine whether to enable the Traffic Statistics feature on internal users.
- Refresh: Click it to update statistic data.
- Clear: Click it to remove statistic data.

⚠ **Note:**

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

## 4.8.3.Time

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



Time and Date

This section assists you in setting the device current time; you can either select to set the time and date manually or update it from Internet automatically.

☑ Sync with Internet time servers

Sync Interval: 30 minutes

Time Zone: (GMT+08:00)Beijing, Chongquing, Hong Kong, Urumqi

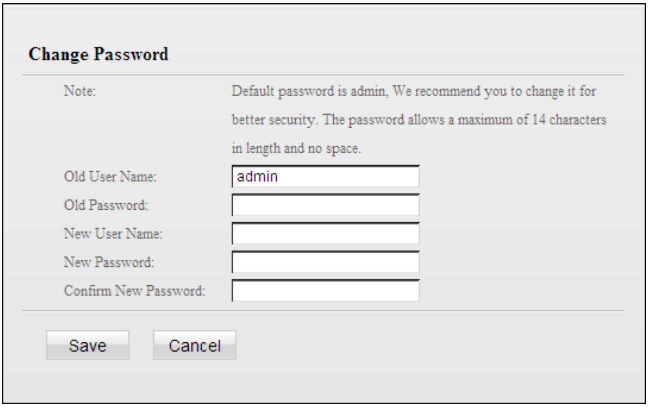
Note: GMT time will be updated automatically only when the device is connected to Internet

Set Time and Date Manually:

2012 Year 08 Month 16 Day 18 Hour 18 Minute 53 Second

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

### 4.8.4 Change Password



Change Password

|  |  |
|---|---|
| Note: | Default password is admin, We recommend you to change it for better security. The password allows a maximum of 14 characters in length and no space. |
| Old User Name: | admin |
| Old Password: |  |
| New User Name: |  |
| New Password: |  |
| Confirm New Password: |  |

- This section allows you to change login password and user name for accessing Device's Web-based management interface.
- Both login password and user name are preset to "admin" by default. To change either or both, do as follows:
  1. Enter your current user name and password in Old User Name and Old Password fields.
  2. Enter a new user name and a new password in New User Name and New Password fields.

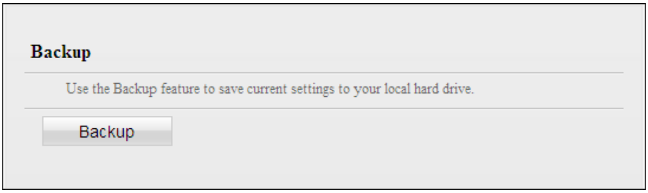
3. Click "Save”.

⚠ **Note:**

For security purpose, it is highly recommended that you change the default login password and user name.

### 4.8.5 Backup

This section allows you to backup current settings. Once you have configured the Device the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your Device in case that the Device is accidentally restored to factory default settings.



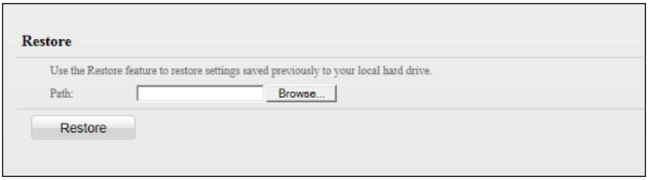
**Backup**

Use the Backup feature to save current settings to your local hard drive.

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

### 4.8.6 Restore

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



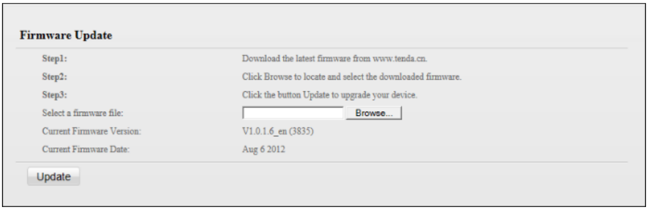
Restore

Use the Restore feature to restore settings saved previously to your local hard drive.

Path:

### 4.8.7 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.



Firmware Update

Step1: Download the latest firmware from www.tenda.cn.

Step2: Click Browse to locate and select the downloaded firmware.

Step3: Click the button Update to upgrade your device.

Select a firmware file:

Current Firmware Version: V1.0.1.6_en (3835)

Current Firmware Date: Aug 6 2012

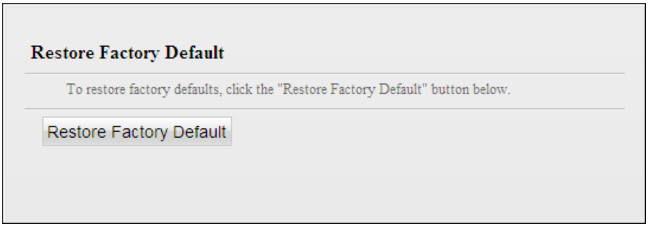
To update firmware, do as follows:

- Click "Browse” to locate and select the firmware file and "Update” to update your Device.
- Device restarts automatically when upgrade completes.

⚠ **Note:**

DO NOT power off the Device when upgrade is in process, otherwise it may be permanently damaged. When it is complete, the device will reboot automatically. The firmware upgrade takes a few minutes to complete. Please wait.

## 4.8.8 Restore to Factory Default



Restore Factory Default

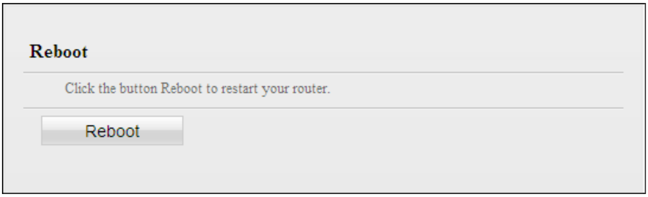
To restore factory defaults, click the "Restore Factory Default" button below.

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

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

## 4.8.9 Reboot

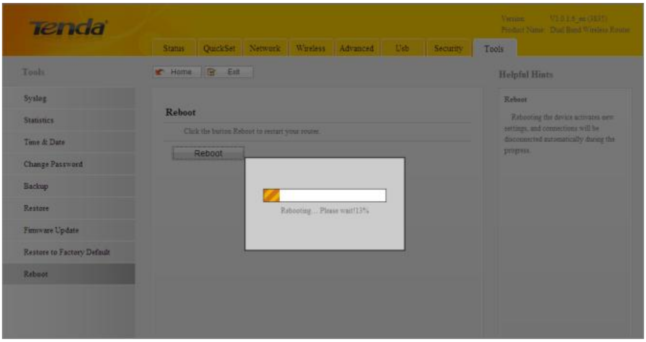
This section allows you to reboot the device.



**Reboot**

Click the button Reboot to restart your router.

To restart your device, click the "Reboot" button. Following screen will appear:



**Reboot**

Click the button Reboot to restart your router.

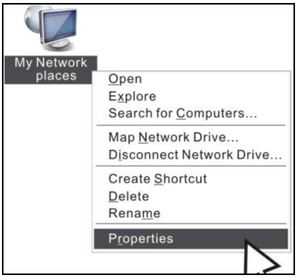
Rebooting ... Please wait!13%

Rebooting the device activates new settings, and connections will be disconnected automatically during the progress.

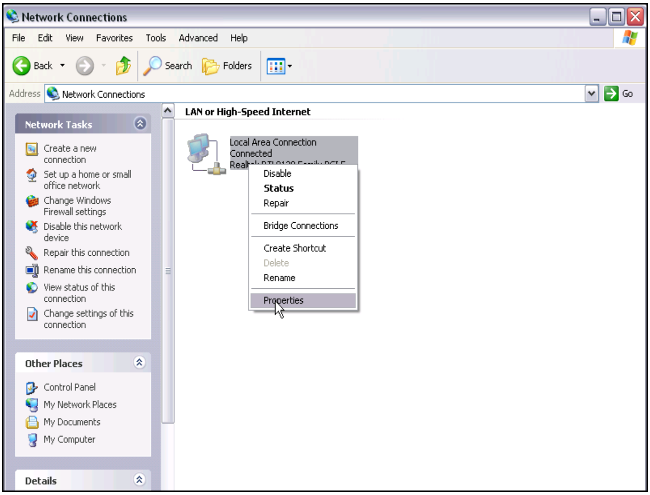
# Appendix 1 Config TCP/IP Settings

## Windows XP

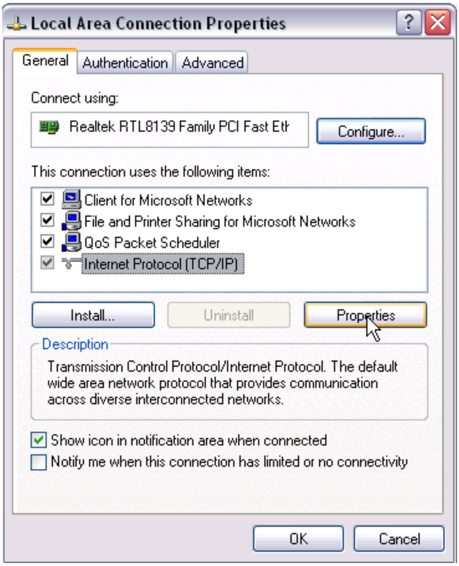
1. From the desktop, right-click My .Network .Places > Properties.



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



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



Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

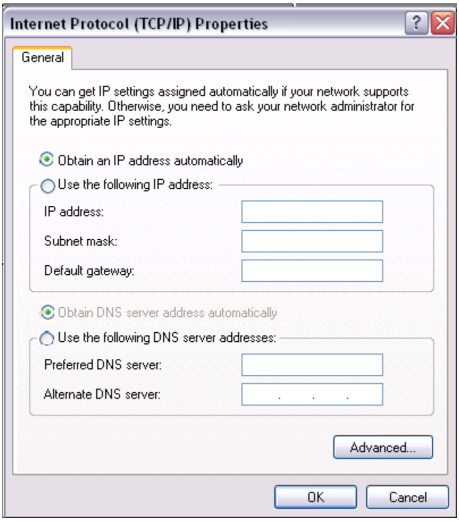
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

☐ Notify me when this connection has limited or no connectivity

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

a. "Obtain an IP address automatically"



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server: . . .

b. Use the following IP address"

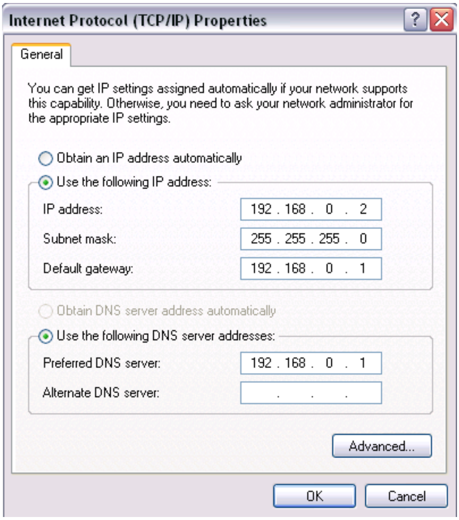
IP address: Enter 192.168.0.xxx where xxx can be any number between 2 and 254).

Subnet mask: Enter 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’s address (Or consult your ISP). The Alternate (Secondary) DNS is not needed or you may enter one from your ISP.

Click OK twice to save your settings.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

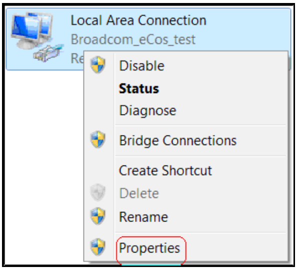
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

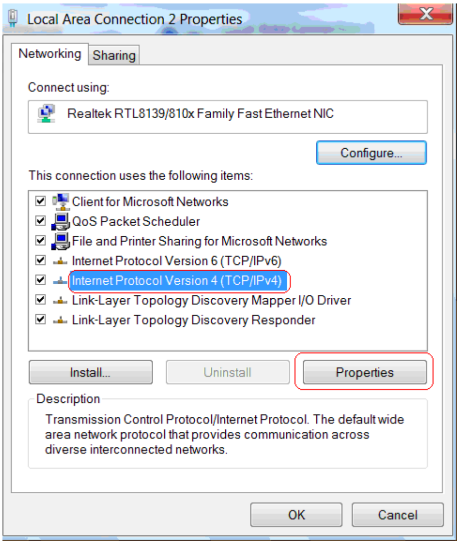
Alternate DNS server: . . .

## Windows7

- From the desktop, right-click Network > Properties.



- Click "Change adapter settings".
- Right click “Local Area Connection” and select “Properties”.
- Highlight "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".



Local Area Connection 2 Properties

Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

This connection uses the following items:

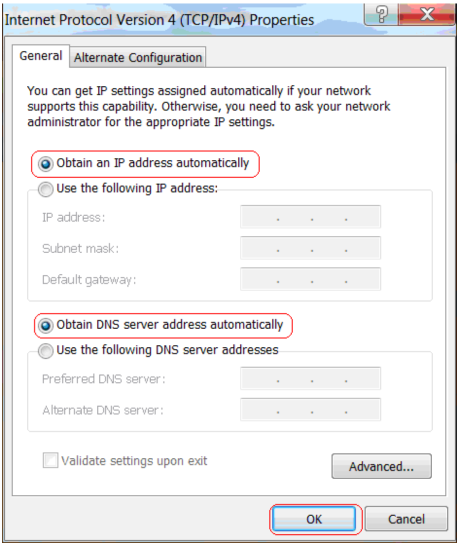
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

a. "Obtain an IP address automatically"



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

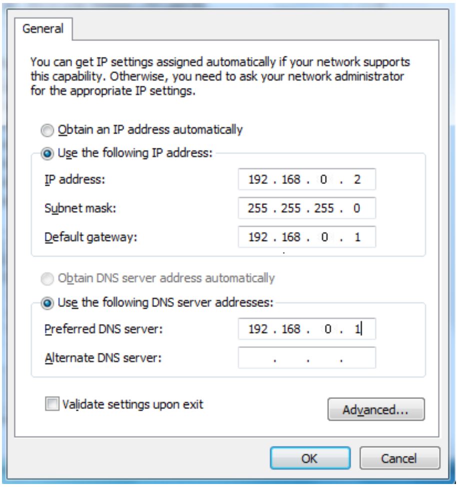
□ Validate settings upon exit

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: Enter 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 if you don't know your local DNS server address (Or consult your ISP). The Alternate (Secondary) DNS is not needed or you may enter one from your ISP.

Click OK twice to save your settings.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

In this section, we present you how to config your PC's TCP/IP settings.

Before you start, make sure your PC has an installed NIC. If not, please install one first.

## NCC Notice

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

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

5.25 ~ 5.35GHz 限室內使用 (802.11a used)

## FCC Statement

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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 Mark Warning

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.
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)."