User Guide

www.tenda.cn

W311R/W311R+

Wireless-N Broadband Router

Copyright Statement

Contents

Chapter 1 Product Introduction

Thank you for purchasing the Tenda W311R/W311R+11N Wireless Broadband Router!

The W311R/W311R+ utilizes the latest IEEE802.11n standard with its wireless transmitting distance over 6 times and transmitting rate over 3 times that of ordinary 802.11g products. It is backwards compatible with 802.11b/g standards and includes router, wireless AP, 4-port switch, and firewall all in one. WMM is supported to allow you to enjoy in audio and streaming video and on-line games.

It supports WDS (Wireless Distribution System) function for wirelessly bridging multiple wireless broadband routers as well as repeating and amplifying signals to extend the wireless network coverage area. Meanwhile, it allows two ways of WPS encryption: PBC and PIN modes, and enables you to close broadcast SSID manually. Besides, client, MAC address and Website filtering are supported to protect your network against malicious attack.

Its bandwidth control function can efficiently distribute downloading rates for each online member. In addition, the Setup Wizard included in the software CD makes installation and access to the Internet, fast and easy, even for the non-savvy users.

1.1 Product Features

- Includes router, wireless access point, four-port switch and firewall all in one
- "Setup Wizard" in the configuration CD enables you to configure the router and let it access to the Internet without entering the router's management interface
- Complies with the latest IEEE802.11n standard and is downwards compatible with IEEE802.11 b/g standards
- coverage distance 6 times father than 802.11g standard and reduces the dead spots in the coverage area
- Supports transmitting rate over 3 times that of wireless G-products
- Supports 64/128-bit WEP, WPA, WPA2, WPA&WPA2 encryption methods and security modes
- Supports RTS/CTS protocol and data partitioning function
- Provides one 10/100Mbps auto-negotiation Ethernet WAN port to connect to the Wide Area Network
- Provides four 10/100Mbps auto-negotiation Ethernet LAN ports to connect to the Local Area Network
- Supports xDSL/Cable MODEM, static and dynamic

IP in community broadband networking

- Supports MAC address/ client/ URL filtering (Max.10 entries for each)
- Supports remote Web management and simple Web upgrading method
- Supports wireless Roaming technology for high-efficient wireless connections
- Supports hidden SSID function and MAC address-based access control (up to14 entries).
- Supports Auto MDI/MDIX
- Provides syslog to record the running status of the router
- Supports 802.11b/802.11g auto-negotiation and manual mode
- Supports UPnP and DDNS
- Supports Firefox1.0, IE5.5 or higher
- Supports LAN access control to the Internet
- Supports SNTP
- Supports virtual server, DMZ host
- Supports WDS to extend wireless network
- Supports bandwidth control function
- Supports IP-MAC address binding (up to 32 entries)
- Detachable antenna(only for W311R+)

1.2 Package Contents

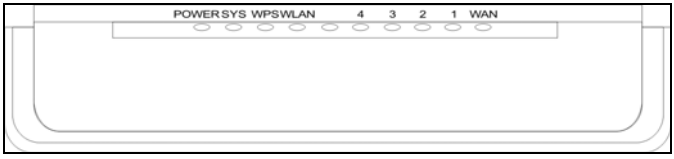
Please verify the following items after you open the package:

- One W311R/W311R+ Wireless Broadband Router
- One Quick Installation Guide
- One Power Adapter
- One Software CD
- One External Antenna(only for W311R+)

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

1.3 LED Indicators and Port Description

Panel and LED indicators show:



LED indicator description on front panel :(from L to R)

POWER LED

Continuously lit green to indicate the router is on and has power.

SYS LED

Flashes green to indicate the router is operating correctly.

WPS LED

Flashes to indicate the device is communicating with the client in WPS mode.

WLAN LED

Wireless signal indicator, flashes green to indicate the wireless function is enabled.

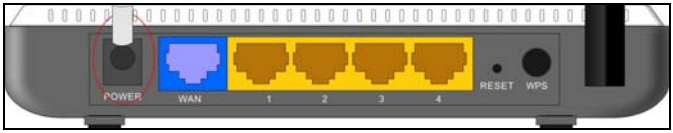
LAN (4,3,2,1) LEDs

Wired local network indicators are continuously lit green when the router's LAN port is connected to an Ethernet device; flashing green indicates the device is transmitting and/or receiving data.

WAN LED

Wide Area Network indicator is continuously lit green to indicate the router's WAN port is connected to an Ethernet device; flashing green indicates the port is transmitting and/or receiving data packets.

Back panel port show



Back panel port description (from L to R)

POWER

The jack is for power adapter connection. Please use the included standard power adapter.

WAN

One 100Mbps Ethernet port that can be connected to Ethernet devices such as MODEM, Switch, Router, etc.. Usually it is used to connect DSL MODEM or Cable MODEM, or ISP network cable for connecting to the Internet.

LAN (1, 2, 3, 4)

Four 100Mbps Ethernet ports that can be connected to an Ethernet switch, Ethernet router, or NIC card. Mostly they are used to connect to computers, Ethernet switches, etc.

RESET

The system reset button. Press and hold this button for 7 seconds and all of the settings will be deleted and router settings will be restored to factory default.

WPS

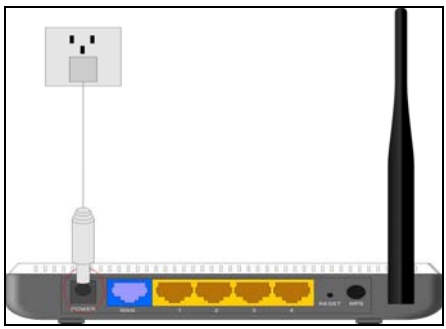
Press and hold the WPS button for 1 second and the WPS feature will be enabled. The WPS LED will flash when communicating in this mode.

Chapter 2 Product Installation

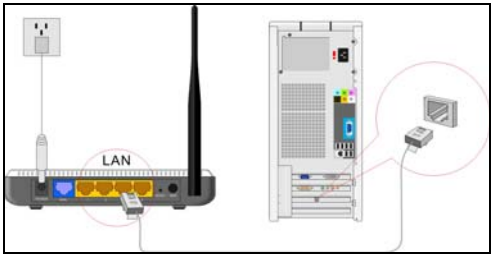
2.1 Hardware Installation

Before you configure the Router, please follow the steps below to connect other devices. For better wireless performance, please place the device in the middle of the wireless coverage area.

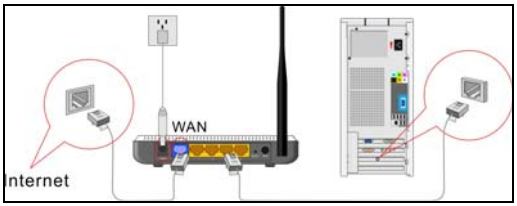
1. Please use only the included power adapter to power your router. (NOTE: Use of an unmatched power adapter could cause damage to this product).



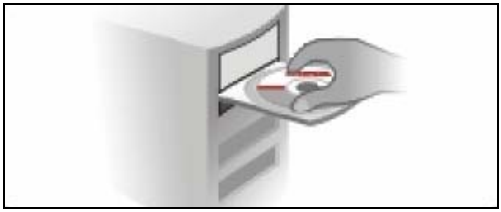
2. Please connect the router's LAN port to your computer with an Ethernet cable as shown below.



3. Please connect your broadband line provided by your ISP to the router's WAN port.

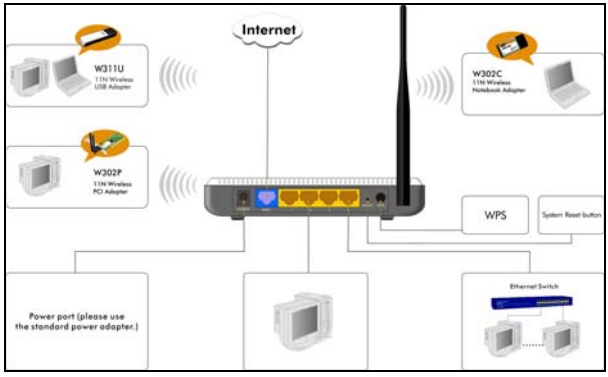


4. Insert the included software CD into the CD drive of your computer. After the software automatically initiates, double click the "**Setup**" icon and follow the instructions to complete the installation. You can also enter the router's Web-based Utility to complete the configuration (For more details please refer to Chapter 3).



2.2 Network Application Topology

Usually, a wireless LAN network is positioned in an area where each access point is set up in a dedicated location to ensure optimum wireless coverage and consistent communication service. Generally speaking, it is in the center of the area to reduce “dead spots”.



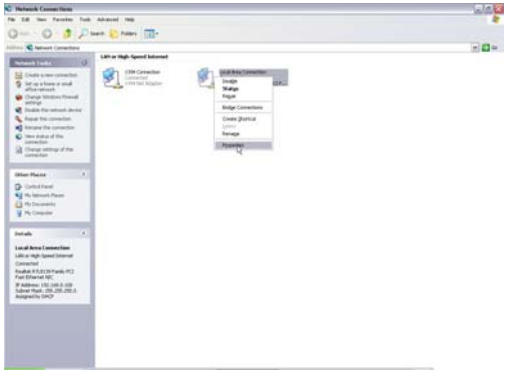
Chapter 3 How to Log in to the Router

This chapter explains how to enter the router's Web-based Utility. After you have finished wired connection to this router (refer to chapter 2 for connection method), the following steps will assist you in setting the network configurations for your computer.

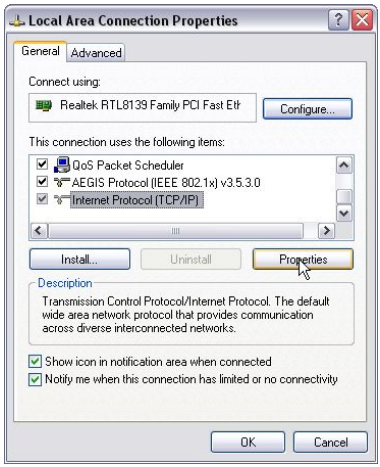
3.1 How to Set the Network Configurations

1. Right click "**My Network Places**" on your computer desktop and select "**Properties**".

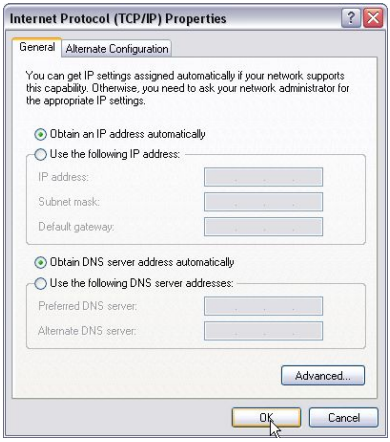
2. Right click "**Local Area Connection**" and select "**Properties**".



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

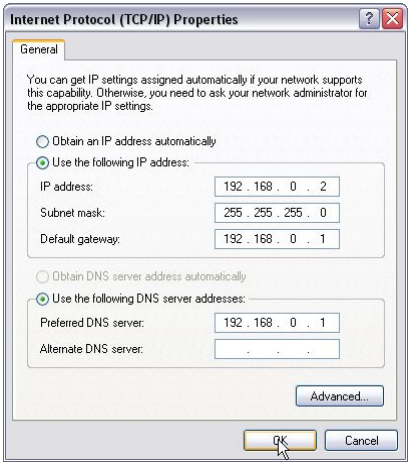


4. Select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**". Click "**OK**" to save the configurations.



Or select "**Use the following IP address**" and enter the IP address, Subnet mask, Default gateway as follows:

- **IP Address:** 192.168.0.XXX: (XXX is a number from 2~254)
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.0.1
- **DNS server:** You should input the DNS server address provided by your ISP. Otherwise, you can use the router as the DNS proxy server. Click "OK" to save the configurations.



3.2 Log in to the Router

1. To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter http://192.168.0.1. Press "**Enter**".

2. Type "**admin**" in both "**User Name**" and "**Password**" fields. Click "**OK**".

3. If you enter the correct user name and password, you will come to the router's homepage interface as is shown below.

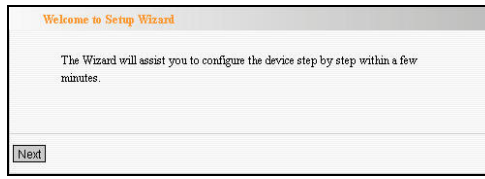
Chapter 4 Quick Setup Guide

This chapter mainly deals with how to access the Internet quickly.

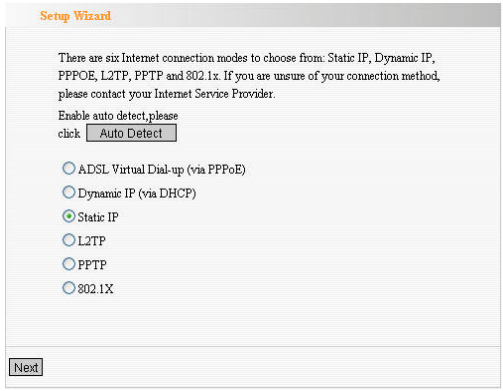
Click "**Next**" after you enter the router's configuration interface and select the current access way provided by your ISP to finish the basic settings for Internet access. Please follow the steps below to complete the configuration.

4.1 Setup Wizard

1. This wizard will assist you to configure the device step by step within a few minutes. Click "**Next**"



2. This router supports common Internet connection modes .In this section we will introduce to you how to configure the five commonest connection modes. Please select the Internet connection mode you are using. If you are not sure about the mode, you can click "Auto Detect" button for confirmation.



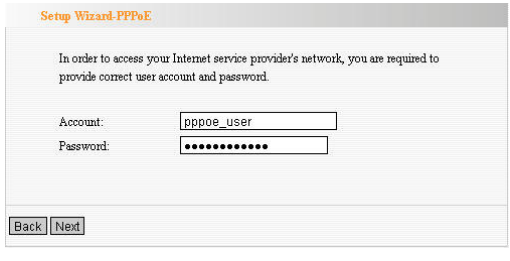
ADSL Virtual Dial-up (Via PPPoE)

Enter the Account and Password provided by your ISP, and click "**Next**". If you have forgotten or are not sure about them, please inquire your ISP.

For example:

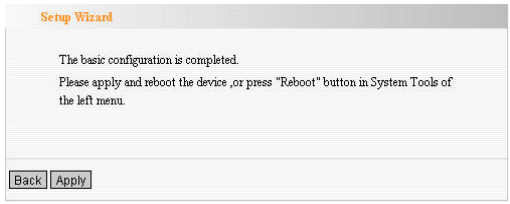
- **Account:** pppoe_user
- **Password:** 123456

Please input the parameters as the screen shows below.



Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means every time you access the Internet, you will get a different IP. You don't need to enter the parameters information as the other two modes. Click "**Next**" to enter the screen below and click **"Apply**" to finish the settings.



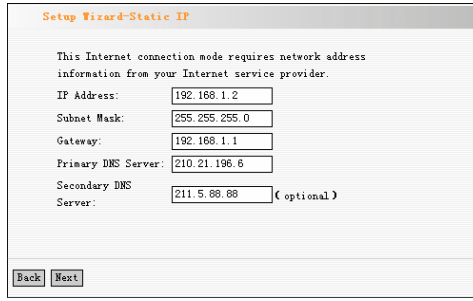
Static IP

In this screen, enter the parameters provided by your ISP or network administrator in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click "**Next**".

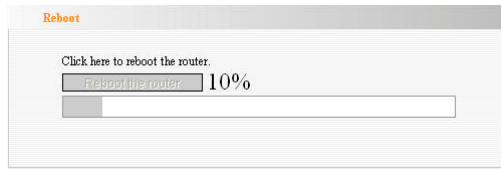
For example:

ISP provides the TCP/IP parameters as follows:

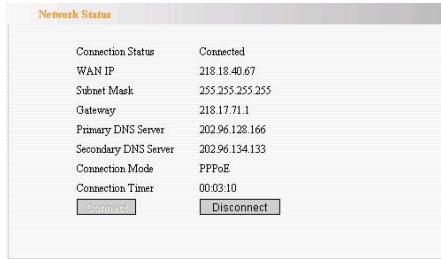
- **IP Address**: 192.168.1.2
- **Subnet Mask**: 255.255.255.0
- **Gateway**: 192.168.1.1
- **Primary DNS Server**: 210.21.196.6
- **Secondary DNS Server**: 211.5.88.88



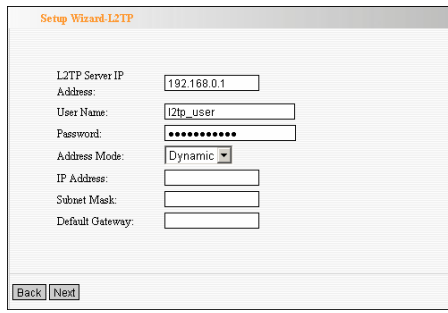
Click "**Next**" to enter the next screen and click "**Apply**" to complete the setup wizard. The Router will record the settings you made. To activate the settings, it is recommended that you select "**Reboot the Router**" from "**System Tool**" in the left menu.



After rebooting, click the "***System Status***" in the left menu of the Web-based Utility to view the current network and system information. If the "**Connection Status**" shows "**Connected**", congratulations! You have completed the router's basic settings and you can now have access to the Internet. If you want to configure more functions, please refer to the subsequent chapters.



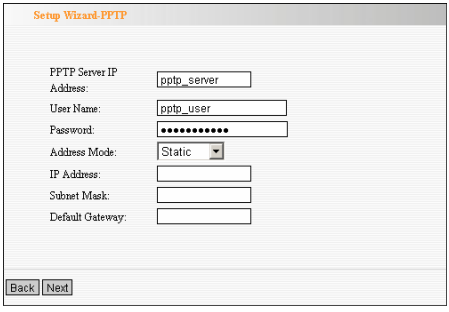
L2TP



- **L2TP server:** The IP address or domain name of the destination server and it is used to specify the destination address which needs for L2TP connection.
- **User name/Password:** Used to validate identity when connecting to the L2TP server.
- **Address Mode:** Set the router's IP address mode, you can select either "Dynamic" or "Static". If your ISP doesn't provide the IP address, please select "Dynamic".

All the above parameters are provided by ISP.

PPTP

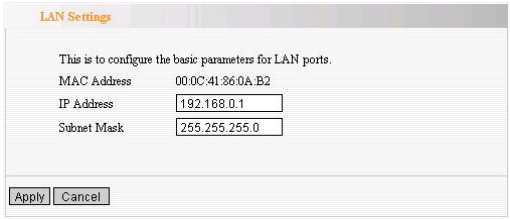


For PPTP connection configuration, please refer to the L2TP connection method.

Chapter 5 Advanced Settings

5.1 LAN Settings

This section is to configure the basic TCP/IP parameters of LAN ports.



- **MAC Address:** The Router's LAN MAC address, which is unchangeable.
- **IP Address:** The Router's LAN IP address (not your PC's IP address).The default value is 192.168.0.1; you can change it when necessary.
- **Subnet Mask:** The Router's LAN subnet mask. The default value is 255.255.255.0

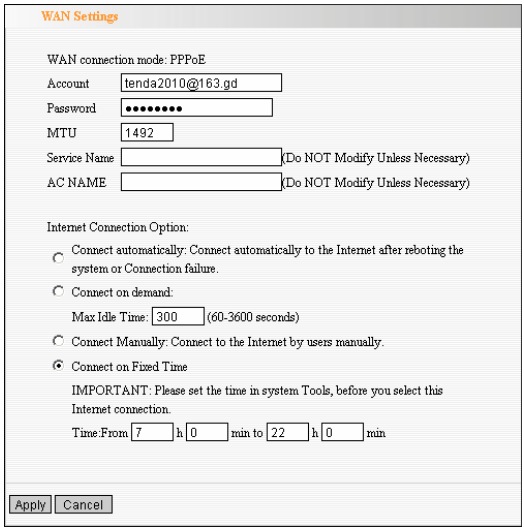
NOTE:

Once you modify the IP address, you need to remember it for next time you log in to the web-based utility.

5.2 WAN Settings

If you want to modify the related settings after you select the ISP connection mode in "**Setup Wizard**" menu, here you can modify and configure the settings in details.

Virtual Dial-up (PPPoE)



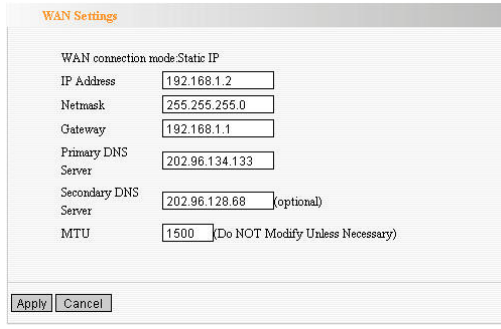
- **Connection Mode:** Show your current connection mode.
- **Account:** Enter the account provided by your ISP.
- **Password:** Enter the password provided by your ISP.
- **MTU:** Maximum Transmission Unit. It is the size of the largest data packet that can be sent over the network. The default value is 1492. Do NOT modify it unless necessary, but if a specific website or web application software cannot open or be enabled, you can try to change the MTU value to 1450, 1400, etc.

- **Service Name:** The connection name for current PPPOE, enter it if necessary, otherwise, leave it blank.
- **AC Name:** The service name, enter it if necessary, otherwise, leave it blank.
- **Connect Automatically:** Connect automatically to the Internet after rebooting the system or connection failure.
- **Connect on Demand:** Re-establish your connection to the Internet after the specific time (Max Idle Time). Zero means you are connected to the Internet all times. Otherwise, enter the minutes to be elapsed before you are disconnected from the Internet.
- **Connect Manually:** Connect to the Internet by users manually.
- **Connect on Fixed Time:** Connect to the Internet during the time you fix automatically.

NOTE:

The "**Connect on Fixed Time**" goes into effect only when you have set the current time in "**Time Settings**" from "**System Tools**".

Static IP

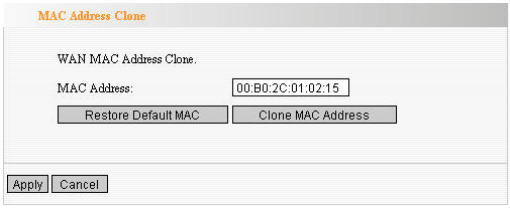


If Static IP connection mode is chosen, you can modify the following parameters.

- **IP Address:** Enter the WAN IP address provided by your ISP. If you are not clear, please inquire your local ISP.
- **Subnet Mask:** Enter the WAN Subnet Mask provided by your ISP. Generally it is 255.255.255.0。
- **Gateway:** Enter the Gateway provided by your ISP. If you are not clear, please inquire your local ISP.
- **Primary DNS Server:** Enter the necessary DNS server provided by your ISP.
- **Secondary DNS Server:** Enter the second DNS address if your ISP provides, which is optional.

5.3 MAC Address Clone

This screen is to set the router's WAN MAC address.



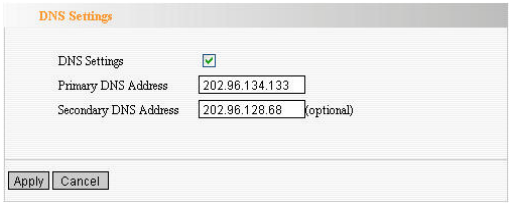
Some ISPs may bind the MAC addresses of the users' computers to let them access their network.

This feature copies the MAC address of the bound computer to the WAN MAC address field of the Router.

- **MAC Address:** To set the router's WAN MAC address. Here it displays the router's WAN MAC address.
- **Clone MAC Address:** To copy your PC's MAC address and set it as the router's WAN MAC address.
- **Restore Default MAC Address:** Restore router's WAN MAC address to factory default.

5.4 DNS Settings

DNS stands for Domain Name System (or Service). The server that implements domain name service is called DNS server, which is used to respond to the domain name service inquiry.



- **DNS Settings:** Select to enable the DNS server. The Router's DHCP server will answer the client's request and distribute the DNS server address.
- **Primary DNS Address:** Enter the necessary address provided by your ISP.
- **Secondary DNS Address:** Enter the second DNS address if your ISP provides, which is optional.

NOTE:

After the settings are completed, reboot the device to activate the modified settings.

Chapter 6 WLAN Settings

6.1 Basic Settings

- **Enable Wireless:** Select to enable the Router's wireless features; deselect to disable it and all functions related with wireless are disabled.
- **Network Mode**: Select one mode from the drop-down menu.

11b mode：Select it if you have only Wireless-B clients in your network.

11g mode：Select it if you have only Wireless-G clients in your network.

11b/g mixed mode: Select it if you have only

Wireless-B and Wireless-G clients in your network.

11b/g/n mixed mode: Select it if you have Wireless-B, Wireless-G and Wireless-N clients in your network.

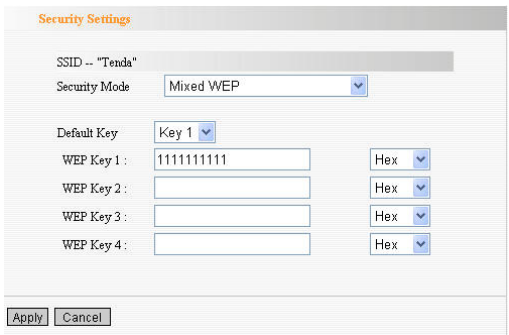
- **SSID:** SSID (Service Set Identifier) is the unique name of the wireless network. It must be entered but you can modify it.
- **Broadcast (SSID):** Select "**Enable**" to enable the router' SSID to be scannable by wireless devices. The default is enabled. If you disable it, the wireless devices must know the SSID for communication.
- **BSSID**: Basic Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.
- **Channel:** The currently used channel by the router. Select an effective channel (from 1 to 13\Auto) of the wireless network.
- **Extension Channel:** To confirm the network's frequency range in 11n mode.
- **Channel bandwidth:** Select an appropriate channel bandwidth to enhance the wireless performance. Select 20/40M when the network has 11b/g and 11n wireless clients. Select 20M when the network has only non-11n wireless clients. Select 20/40M to promote its throughput when the wireless network is in 11n mode.

6.2 Wireless Security Settings

This section is for wireless security settings. The three commonest encryption methods are introduced: Mixed WEP, WPA-personal, and WPA2-personal.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy) is an encryption method which encrypts the data wirelessly transferred between two devices to prevent unauthorized users from intercepting or invading the wireless network. WEP security, based on RC4 data encryption technology, provides data confidentiality, integrity, and authentication for wireless communication.



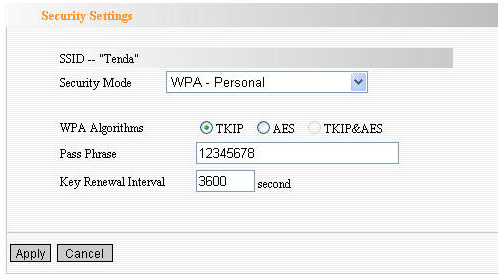
- **Security Mode:** Select the corresponding security mode from the drop-down menu.
- **WEP Key1~4:** Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13

ASCII characters. Illegal characters such as "/" is not allowed). Or 10/26 hex characters.

- **Default Key:** Select one key from the four preset keys as the current effective one.

6.2.2 WPA- Personal

WPA is a standard and interoperable WLAN enhanced security solution which greatly strengthens data protection and access control ability for the existing and future WLAN system. WPA originates from IEEE802.11i standard, and is backwards compatible with it. WPA guarantees to protect WLAN users' data and only the authorized network users can have access to WLAN. The encryption Algorithm it adopts is better than WEP for it can change the keys dynamically on every authorized wireless device.



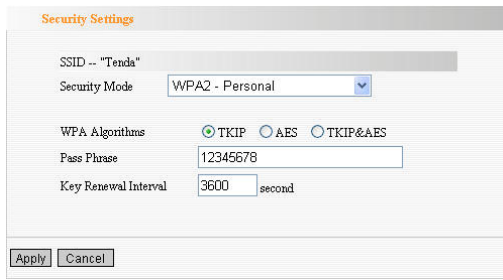
- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption

Standard].

- **Pass Phrase:** Enter the pass phrase that consists of 8-63 ASCII characters.
- **Key Renewal Interval:** Set the key's renewal period, which tells the device how often it should change the dynamic encryption keys.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access). It does not only adopt TKIP encryption but also the new encryption mode----AES.

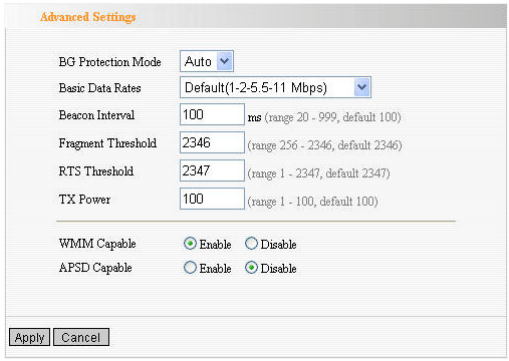


- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard].
- **Pass Phrase:** Enter the pass phrase that consists of 8-63 ASCII characters.

- **Key Renewal Interval:** Set the key's renewal period, which tells the device how often it should change the dynamic encryption keys.

6.3 Advanced Settings

This section is to configure the advanced wireless settings of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, etc.

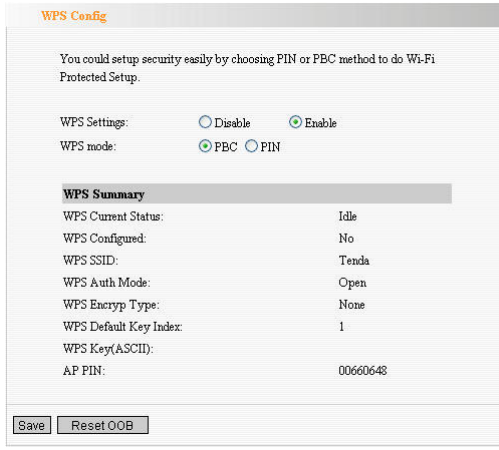


- **BG protection Mode:** Auto by default. It is for relatively slower 11b/g wireless clients to connect to 11n wireless network smoothly in a complicated wireless area.
- **Basic Data Rates:** For different requirements, you can select one of the suitable Basic Data Rates. The default value is 1-2-5.5-11Mbps. Modification to this value is not recommended.

- **Beacon Interval:** Set the beacon interval for AP. Generally, the smaller the interval is, the faster wireless clients connect; the bigger it is, the higher efficiency wireless network data transmission will achieve. Default value is 100. Modification to this value is not recommended.
- **Fragment Threshold:** The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if it is bigger than the threshold setting. The default size is 2346 bytes. Modification to this value is not recommended.
- **RTS Threshold:** RTS stands for "Request to Send". When the data is bigger than the preset value, use CTS/RTS mechanism to reduce the collision possibility. It is recommended not to modify this value in SOHO environment lest it should affect AP's performance.
- **TX Power:** Set the output power of the wireless radio. The default value is 100.
- **WMM Capable:** Enable it to enhance the transfer performance of the wirelessly transferred multimedia data (such as video or online playing).We recommend enabling this option if you are not familiar with WMM.
- **APSD Capable:** It is used for auto power-saved service. The default is disabled.

6.4 WPS Settings

WPS (Wi-Fi Protected Setting) makes it quick and easy to establish a secure connection between the wireless network clients and the router. The users only need to enter a PIN code or press WPS button on the back panel to configure it without manually selecting an encryption method or secret keys. In the "**WLAN settings**" menu, click "**WPS settings**" to enter the next screen.



- **WPS settings**: To enable or disable WPS function. The default is "**Enable".**
- **WPS mode:** Provide two ways: PBC (Push-Button Configuration) and PIN code.
- **PBC:** Select the PBC and click **Save,** or press and hold the WPS button on the back panel of the device for about one second. The WPS LED indicator will be flashing for 2 minutes, which

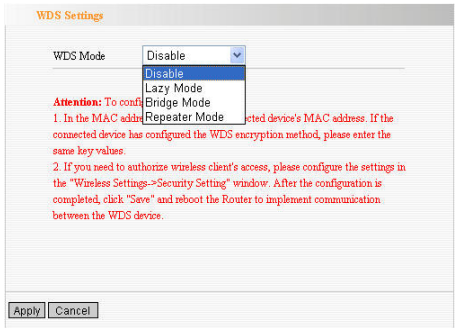
means the WPS is enabled. During this time (flashing WPS LED), you can enable another device to implement the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. To add more clients, repeat the above steps. At present, the WPS supports up to 32 clients access.)

- **PIN:** If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the WPS client.
- **WPS Summary:** Show the current state of Wi-Fi protected setting, including authentication mode, encryption type, default key and other information.
- **WPS Current Status:** Idle means WPS is in an idle state. Start MSC process means the process has been started and is waiting for being connected. Configured means the negotiation between server and clients is successful.
- **WPS Configured:** "**Yes**" means WPS feature is enabled and goes into effect. "**No**" means it is not used. Usually when the AP-security has been enabled, here it will display "**No**".
- **WPS SSID:** Show the SSID set by WPS.
- **WPS Auth. Mode:** The authentication mode used by WPS, generally WPA/WPA2-personal mode.
- **WPS Encrypt Type:** The encryption type used by WPS, generally AES/TKIP.
- **WPS key:** The effective key generated by AP automatically.

- **AP PIN (KEY):** The PIN code used by default.
- **Reset OOB:** Press this button, the WPS client will be in an idle state, and the WPS indicator will turn off. AP will not respond to the WPS client's connection request and will set the security mode as Open-None mode.

6.5 WDS Settings

WDS (Wireless Distribution System) is used to expand wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.



- **Lazy Mode:** In this mode, the connected device can be either in Bridge mode or Repeater mode. Enter this router's BSSID to establish the connection.
- **Bridge Mode:** In this mode, you need to add the Wireless MAC address of the connected device into the Router's AP MAC address table or select one from the scanning table. Click" Apply" and two

wired networks are wirelessly connected.

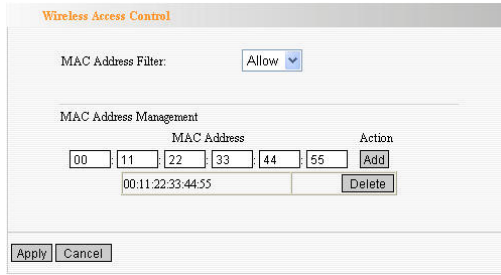
- **Repeater Mode:** In this mode, you must add the MAC address of the connected device into the AP MAC address table either manually or by scanning to enlarge and extend the wireless radio coverage.
- **Encrypt Type:** Select one from WEP, TKIP, AES for security here.
- **Pass phrase:** Enter the encrypted key for wireless devices.
- **AP MAC:** Input the MAC address of another (opposing) wireless router you want to connect.

NOTE:

It is recommended that two wireless routers keep the same bandwidth, channel, and security settings. Apply the settings and reboot the Router to activate it.

6.6 Wireless Access Control

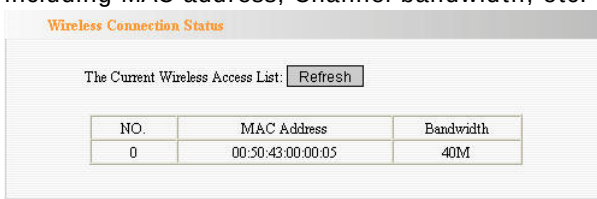
Wireless access control is actually based on the MAC address management to allow or block specific clients to access the wireless network.



- **MAC Address Filter:** "**Allow**" indicates to permit the clients in the list to access the wireless network, "**Block**" indicates forbid the clients in the list to access the wireless network
- **MAC Address Management:** Input the MAC addresses of the wireless clients to implement the filter policy. Click "**Add**" to finish the MAC add operation.
- **MAC Address list:** Show the added MAC addresses. You can add or delete them.

6.7 Connection Status

This screen shows wireless client's connection status, including MAC address, Channel bandwidth, etc.

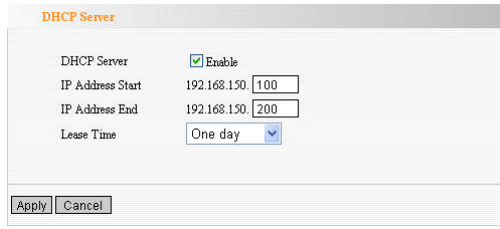


- **MAC Address:** Shows the MAC addresses of the hosts connected to the Router.
- **Bandwidth:** Shows current bandwidth of the connected hosts (wireless clients).

Chapter 7 DHCP Server

7.1 DHCP Settings

DHCP (Dynamic Host Control Protocol) is used to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating "Obtain an IP Address Automatically". So specifying the starting and ending address of the IP Address pool is needed.



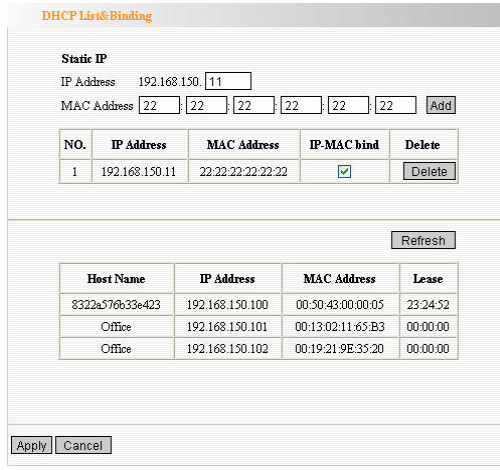
- **DHCP Server:** Check the **Enable** box to enable DHCP server.
- **IP Address Start/End:** Enter the range of IP addresses for DHCP server distribution.
- **Lease Time:** The length of the IP address lease. Set an appropriate lease time to improve DHCP server's efficiency in reclaiming the invalid IP addresses.

For example:

If the lease time is an hour, then DHCP server will reclaim the invalid IP address each hour.

7.2 DHCP List and Binding

DHCP client list displays user computer' IP address, MAC address, host name and other information which are assigned by the DHCP server. You can manually enter the IP and MAC address and convert them to static allocation. According to the connected computer's MAC address, the router will look up the related items from the table and assign the appropriate IP address to the computer. Failing to find the corresponding static binding entry, it will assign an unused IP address to this computer from the DHCP pool. If the IP address and MAC address of one computer have been bound, and they do not match, then the computer will be unable to access Internet via the router. (Binding it prevents the client changing IP address and to evade the monitoring device)

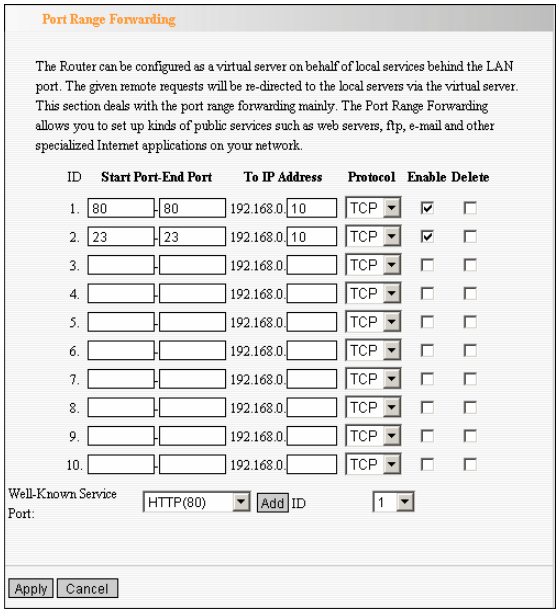


- **IP Address:** Enter the IP address which needs static binding.
- **MAC Address:** Enter the MAC address of the computer you want to bind. Click "**Add**" to add the entry in the list.
- **Host Name:** It displays the name of the bound computer.
- **Lease Time:** The left time length of the corresponding IP address lease.

Chapter 8 Virtual Server

8.1 Port Range Forwarding

Port range forwarding sets up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications. When users send these types of access requests to your network via the Internet, the router will forward those requests to the LAN servers which are specified by IP addresses.



- **Start/End Port:** Enter the start/end port number

which ranges the External ports used to set the server or Internet applications.

- **IP Address:** Enter the IP address of the PC which you want to set as the server.
- **Protocol:** Select the protocol (TCP/UDP/Both) for the application. If you are not clear about the protocol you are using, you can select “Both”.
- **Enable:** Click the **Enable** checkbox to bring the set rule into effect.
- **Delete:** Clear all settings of this item.
- **Well-Known Service Port:** The well-known protocol ports are listed in the drop-down menu.Select one and select a sequence number in the ID drop-down menu and then click “Add”,this port will be added automatically to the ID list. For other well known service ports that are not listed, you can manually add them to the list.
- **Add:** Add the selected well-known port to the policy ID.

For example:

The server at IP address of 192.168.0.10 provides port 80 for WEB service and port 23 for Telnet service. If you want clients in the Internet to visit that server, you need to set it as above.

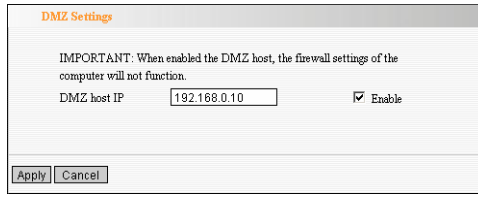
NOTE:

If you set the service port of the virtual server as 80,

you must set the Web management port on Remote Web Management screen to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.2 DMZ Settings

The DMZ Settings screen allows one local computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.



- **DMZ Host IP Address:** The IP address of the LAN computer you want to set as DMZ host.
- **Enable:** Check to enable the DMZ host.

For example:

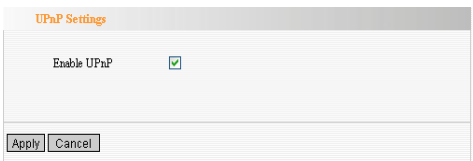
Set the computer at IP address of 192.168.0.10 as DMZ host to connect another host in the Internet for

intercommunication.

NOTE: When the DMZ host is enabled, the firewall settings of the DMZ host will not function.

8.3 UPNP Settings

It supports the latest Universal Plug and Play device drivers. This function goes into effect under Windows XP or Windows ME (NOTE: the system should integrate or have installed the Directx 9.0) or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, the internal host can request the router to process some special port switching so as to enable the external host to visit the resources of the internal host.

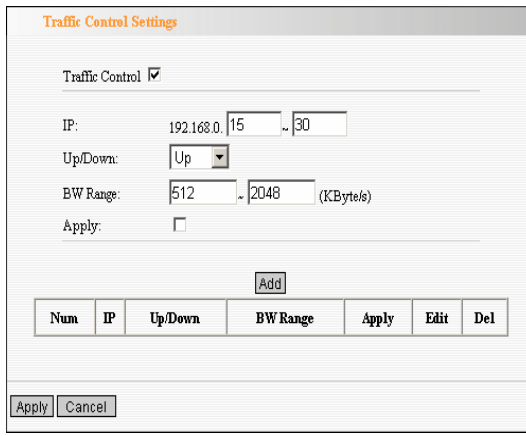


- **Enable UPnP:** Click the checkbox to enable the UPnP.

Chapter 9 Traffic Control

9.1 Traffic Control

Traffic control is used to limit the communication traffic of LAN computers' accessing the Internet. It can support limitation rules up to 20 entries and simultaneously control maximum of 254 PCs' traffic. In addition, IP address range configuration is supported.



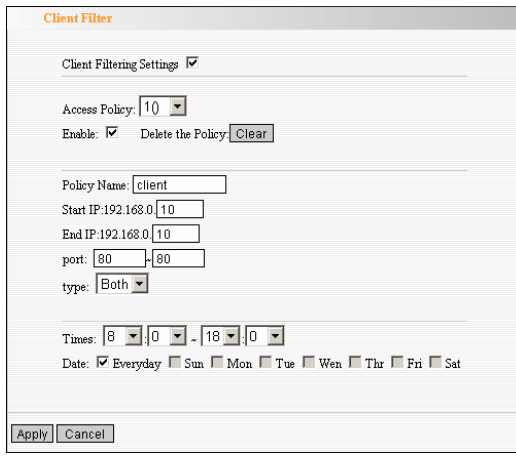
- **Enable Traffic Control:** To enable or disable the internal IP bandwidth control. The default is disabled.
- **IP Address:** The IP address range of the hosts whose traffic has been controlled. It can be a single IP address or IP address range.

- **Uploading/Downloading:** To specify the traffic heading way for the selected IP addresses: uploading or downloading.
- **Bandwidth Range:** The maximum and minimum uploading/downloading data traffic of the hosts in specified IP range. The unit is KByte/s. The uplink of uploading and downloading can not exceed the WAN port bandwidth limitation range.
- **Apply:** To enable the current edited rule. Otherwise, the rule will not go into effect.
- **Add:** After you edit the rule, click the "**add to list**" button to add the current rule to rule list.
- **Apply:** Click "**Save**" to activate the current rule.
- **Cancel:** Click "**Cancel**" to drop all settings saved last time.

Chapter 10 Security Settings

10.1 Client Filter Settings

To manage the online access of all computers in the network, you can enable client filter to control LAN computers' access to some ports of the Internet。



- **Client Filter:** Check to enable client filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** To enable/disable the access policy (forbid the packets matched with the access policy to pass through the router.
- **Policy Name:** Enter a name for the access policy selected.

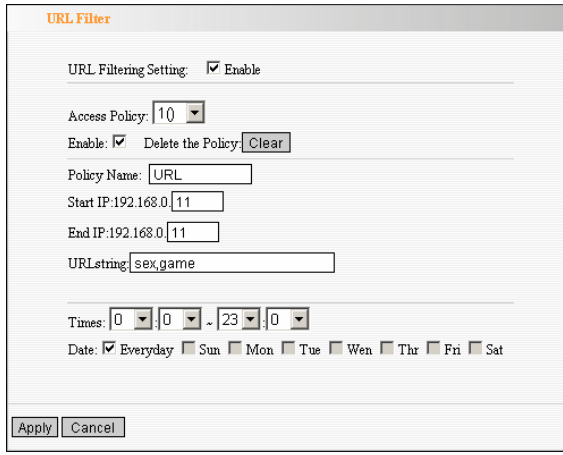
- **IP Start/End:** Enter the starting/ending IP address.
- **Port:** Enter the controlled TCP/UDP protocol port. You can specify a port or port range.
- **Protocol:** Select one protocol (TCP/UDP/Both) from the drop-down menu.
- **Times:** Select the time range of client filter.
- **Date:** Select the day(s) to run the access policy.

For example:

If you don't want the designated computer at the IP address of 192.168.0.10 to visit website from 8:00 to 18:00 everyday without restriction to other computers in LAN, you need to set it as above.

10.2 URL Filter Settings

To better control the LAN computers' access to the websites; you can use URL filtering to forbid their access to certain websites at a specified time.



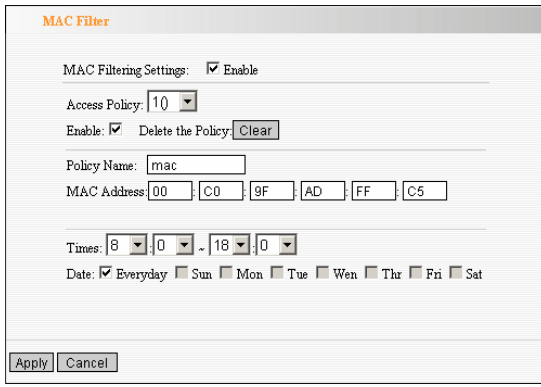
- **URL Filter:** Check to enable URL filter.
- **Access Policy:** Select one number from the drop-down menu.
- **Enable:** To enable/disable the access policy (forbid the packets matched with the access policy to pass through the router).
- **Policy Name:** Enter a name for the access policy selected.
- **Start/End IP:** Enter the starting/ending IP address.
- **URL Strings:** Specify the text strings or keywords needed to be filtered. If any part of the URL contains these strings or words, the web page will not be accessible and displayed.
- **Times:** Select the time range of URL filter.
- **Date:** Select the day(s) to run the access policy.
- **Save:** Click **Save** to activate the configuration.

For example:

If you don't want the computer at the IP address of 192.168.0.11 to visit the website containing the character strings of "**sex**" and "**game**", you need to set the packet filtering list as the above diagram(Notice: different strings need to be separated by a comma.).

10.3 MAC Address Filter

In order to manage the computers in LAN better, you could limit the computer's access to Internet by MAC Address Filter.



- **MAC Address Filter:** Check to enable MAC address filter.
- **Access Policy:** Select one number from the drop-down menu.

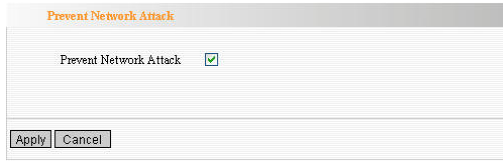
- **Enable:** To enable/disable the access policy (forbid the packets matched with the access policy to pass through the router).
- **Policy Name:** Enter a name for the access policy selected.
- **MAC Address:** Enter the MAC address you want to run the access policy.
- **Times:** Select the time range of MAC address filter.
- **Date:** Select the day(s) to run the access policy.
- **Apply:** Click to make the settings go into effect.

For example:

If you want to forbid the host with MAC address 00:C0:9F:AD:FF:C5 to access the Internet at 8:00-18:00 without restriction to other computers in LAN, you need to set it as noted in the above diagram.

10.4 Prevent Network Attack

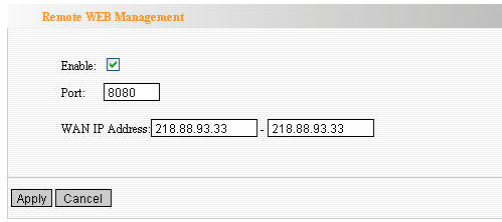
This section instructs how to protect the internal network from exotic attacks such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once the unknown attack is detected, the router will restrict its bandwidth automatically. The attacker's IP address can be found in the "System Log".



- **Prevent Network Attack:** Check to enable.

10.5 Remote Web Management

This section instructs how to allow the network administrator to manage the Router remotely. If you want to access the Router from outside of the local network, please select the “Enable”.



- **Enable:** Check to enable remote web management.
- **Port:** The management port open to outside access. The default value is 80.
- **WAN IP Address:** Specify the range of the WAN IP address for remote management.

NOTE:

1. If you want to log in the device’s Web-based Utility via port 8080, you need to use the format of

WAN IP address: port (for example http：//220.135.211.56:8080) to implement remote login.

2. If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 218.88.93.33-218.88.93.35, then only the computers at the IP addresses of 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the Router to implement remote web management.

For example:

If you want to configure the computer at the IP address of 218.88.93.33 to access the router's web management interface via port 8080, please set the parameters as above.

10.6 WAN Ping

The ping test is to check the status of your Internet connection. When disabling the test, the system will ignore the ping test from WAN, namely it will not respond to ping request from WAN port. But LAN computers can ping pass.

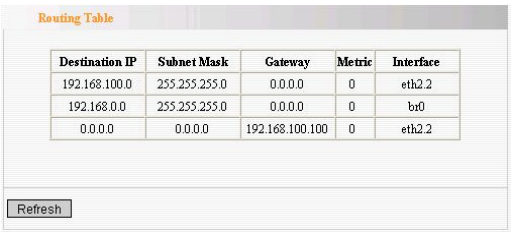
- **Ignore Ping from WAN:**

  Check to ignore the ping request and give no reply.

Chapter 11 Routing Settings

11.1 Routing Table

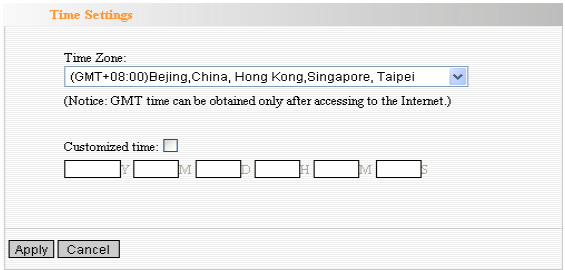
The main duty for a router is to look for a best path for every data packet, and transfer this data packet to a destination station. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to fulfill this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.



Chapter 12 System Tools

12.1 Time Settings

This section is to configure the router's system time. You can set it manually or obtain the GMT time from the Internet.



- **Time Zone:** Select the time zone where you are operating the Router from the drop-down menu.
- **Customized time:** Enter the time you wish to configure.

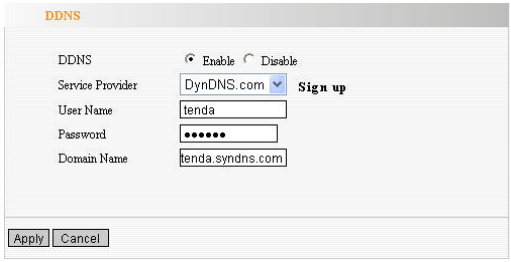
NOTE:

When the Router is powered off, the time settings will be lost. The router will obtain the GMT time automatically when you next time access the Internet. Only after you connect to the Internet and obtain the GMT time or set the time on this screen, can the time settings in other functions

(e.g. security settings) take effect.

12.2 DDNS

The DDNS (Dynamic Domain Name System) is supported in this Router. It is used to assign a fixed host and domain name to a dynamic Internet IP address. Every time you access the Internet, the dynamic domain name software installed on your host will tell the ISP'S host server its dynamic IP address by sending messages. And the server software is responsible for providing DNS service and implementing dynamic domain name resolution.



➢ **Main Features:**

1. Mostly, your ISP provides a dynamic IP address and the DDNS is used to capture the changeable IP address and match to the fixed domain. Then users can have access to the Internet to communicate with others outside the network.

2. DDNS can help you to establish a virtual host in

your home or company.

- **DDNS:** Click the radio button to enable or disable the DDNS service.
- **Service Provider:** Select one from the drop-down menu and press "**Sign up**" for registration.
- **User Name:** Enter the user name the same as the registration name.
- **Password:** Enter the password you set.
- **Domain Name:** Enter the effective registered domain name

For example:

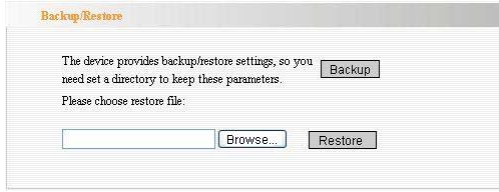
Establish a Web server in the local host 192.168.0.10 and register in 3322.org as follows:

User name	Tenda
Password	123456
Domain Name	tenda.3322.org

After mapping the port in the virtual server, and setting account information in DDNS server, you can then access the web page by entering http://tenda.3322.org in the address field.

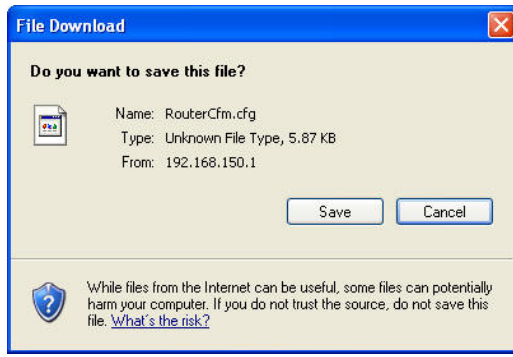
12.3 Backup/Restore Settings

On this screen, you can back up the router's current settings or restore previous settings.



➢ **Backup Setting:**

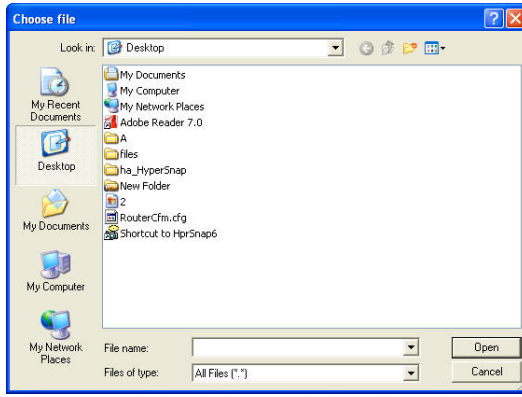
Click the **Backup** button to back up the Router's settings and select a path to save them.



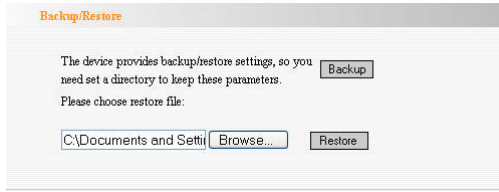
Click the "**Save"** button to save the configuration files.

➢ **Restore Setting:**

Click the "**Browse"** button to select the backup files.

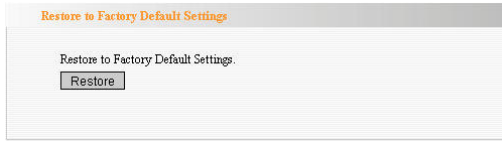


Click the "**Restore**" button to restore previous settings.



12.4 Restore to Factory Default Settings

This screen allows you to restore all settings to the factory default values.



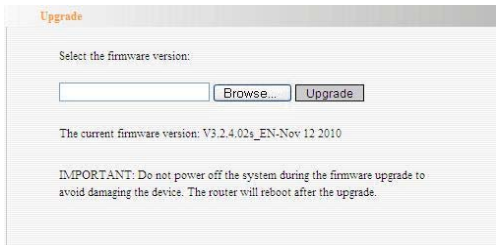
- **Restore:** Click this button to restore to default settings.
- **Factory Default Settings:**
  User Name: admin
  Password: admin
  IP Address: 192.168.0.1
  Subnet Mask: 255.255.255.0

NOTE:

After restoring to default settings, please restart the router to make the default settings effective.

12.5 Upgrade Firmware

By upgrading the router's firmware, you'll get better firmware version and appreciated routing function. Before upgrading, download the Router's firmware upgrade file from our website, www.tenda.cn.

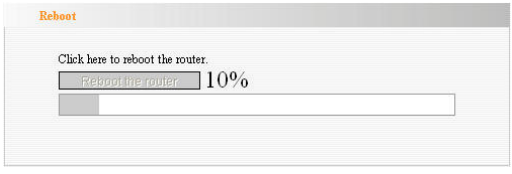


- **Browse:** Click this button to select the upgrade file.

- **Upgrade:** Click this button to start the upgrading process. After the upgrade is completed, the router will reboot automatically.

12.6 Reboot the Router

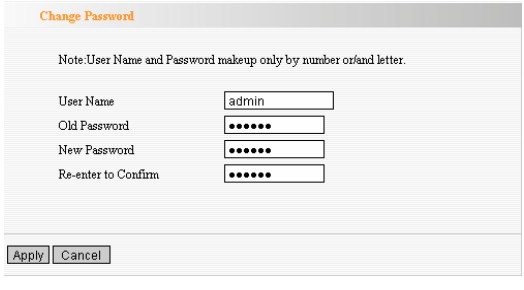
Reboot the router to make the configuration effective. The router will cut its WAN connection automatically after rebooting.



Reboot the router: Click this button to reboot the router.

12.7 Password Change

This section is to set a new user name and password to better secure your router and network.



- **User Name:** Enter a new user name for the device.

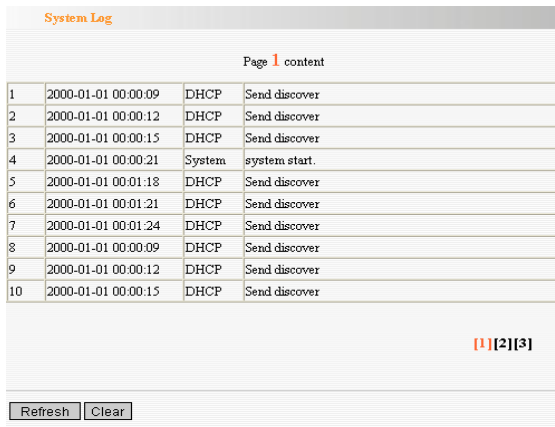
- **Old Password:** Enter the old password.
- **New Password:** Enter a new password.
- **Re-enter to Confirm:** Re-enter to confirm the new password.

NOTE:

It is highly recommended that you change the initial user name and password to secure the router and your network.

12.8 Syslog

The section is to view the system log. You can view various conditions appearing after system start, and also check whether there's an attack in the network. The log can record at most 150 entries.



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

12.9 Logout

After you have finished configuring the settings, go to the logout screen and click **"Yes"** to logout from the Web-based Utility.

Appendix 1 Glossary

Channel:

An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID:

SSID (Service Set Identifier) is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP:

Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the

same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it is NOT recommended using.

WPA/WPA2 Encryption:

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

802,1x authentication

Static WEP key is difficult to manage for when you change the key, you will have to inform all others, and if

the key is disclosed in one of the places, the key can no longer provide security. Besides, there's severe security loophole about static WEP encryption. The WEP key can be decrypted after one person receives a specific amount of data via wireless intercepting. 802,1x is initially used for wired Ethernet authentication access to prevent illegal users from accessing the network. Later, it is found that 802.1x can better solve the wireless network security problem. EAP-TLS of the 802.1x successfully achieves the two-way authentication between users and networks, i.e. can prevent illegal users from accessing the network and can also prevent users from accessing the illegal AP. 802.1x utilizes dynamic WEP encryption to protect the WEP key from being decrypted. To solve the publishing problem for digital certification, people make some changes to TLS authentication and TTLS and EAP come into exist, which enable you to access the network by using the traditional way of authentication: username and password.

Appendix 2 FAQ

This section provides some solutions to the problems which may occur during the router's installation or usage. The instructions below may help you deal with the problems. If your problem is not in the list, please log into our website www.tenda.cn or send an E-mail to support@tenda.cn, and we will reply to you at the earliest time.

1. Cannot log in to the Web-based Utility of the router after you enter the IP address in the address field?

Step 1: Check if the router is working correctly, after the device is powered on for a few seconds, the SYS indicator on the front panel should light up. If it is not, please contact us.

Step 2: Check the network cables are connected correctly and the corresponding LED indicator lights up. Sometimes, the indicator lights up, but it does not mean it is functioning.

Step 3: Run "Ping" command and check if it can ping the Router's LAN IP address 192.168.0.1 (open "Command Prompt" and type "Ping 192.168.0.1" and then enter). If it is OK, please make sure your browser does not access the Internet by proxy server. If the ping fails, you can press the "RESET" button for 7 seconds to

restore to default settings. And then repeat the ping operation. If it still does not work, please contact us.

2. Forgot the login password and cannot enter the Web-based Utility. What can I do?

Press the “RESET” button for 7 seconds to restore the Router to default settings.

3. The computer connected with the Router shows IP address conflict. What can I do?

Check if there are other DHCP servers in the LAN and if there are then disable them. The default IP address of the router is 192.168.0.1 please maker sure the address is not being used by any other device. If there are two computers with the same IP address, please change one of them.

4. I cannot use E-mail and access the Internet. What can I do?

Sometimes happens with ADSL connection and Dynamic IP users. You may need to modify the default MTU value (1492). Please open the “WAN Setting” and modify the MTU value with the recommended value as 1450 or 1400.

5. How to configure and access the Internet via Dynamic IP?

In Setup Wizard of the Web-based Utility, select

"Dynamic IP" connection type and click "**Save**" to activate it.

6.How to share my computer's resource with other users in Internet?

If you want Internet users to access the internal server via the router such as: e-mail server, Web, FTP. You can configure the "**Virtual Server**".

Step 1: create your internal server, make sure the LAN users can access these servers and know related service port. For example, Web server's port is 80; FTP is 21; SMTP is 25 and POP3 is 110.

Step 2: In the router's web click "**Virtual Server**" and select "**Port Range Forwarding**".

Step 3: Input the service port provided by the router (i.e. the external port) for mapping the internal and external network, for example, 80-80.

Step 4: input the internal Web service port, for example, 80-80.

Step 5: Input the internal server's IP address. For example, if your Web server's IP address is 192.168.0.10, please input it.

Step 6: select the communication protocol used by your internal host: TCP, UDP, Both.

Step 7: click "**Apply**" to activate the settings.

The following table lists some well-known applications and their respective service ports:

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

Appendix 3 Regulatory Information

EU Declaration or Declaration of Conformity

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

FCC Statement

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

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and

receiver.

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

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

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with the minimum distance of 20 cm. Operation is subject to the following two conditions:

1) This device may not cause interference, and

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

Caution!

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