User Manual

TOTOLINK Wireless-N Router

TOTOLINK

www.totolink.net

Table of Contents

Copyright Statement

1. ABOUT THIS GUIDE

Thank you very much for purchasing this Wireless N Router. This guide will introduce the features of this device and tell you how to connect, use and configure the Router to connect with Internet. Please follow the instructions in this guide to avoid affecting the Router's performance by improper operation.

1.1 Overview of the User's Guide

Introduction: Describes the Wireless N Router, its appearance and features.

Hardware Installation: Describes the packaging, the hardware installation and how to set up the computer.

Connecting to Internet: Tells how to connect your computer to Internet successfully via the Router.

Advanced Settings: Lists all technical functions including Wireless, Network, NAT/Routing, Firewall, Utility, Traffic and System of the Router.

2. INTRODUCTION

2.1 Overview

This Router is a combined wired/wireless network connection device that integrates with internet-sharing router and 4-port switch. It complies with the most advanced IEEE 802.11n technology and supports multiple security methods, including wireless LAN 64/128-bit WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK encryption. Besides, IP, URL and MAC address filtering function makes it easy for user management. Also, the WPS (Wi-Fi Protected Setup) will allow you to connect to secure network simple and fast. In view of the above, it is really a high performance and cost-effective solution for home and small offices.

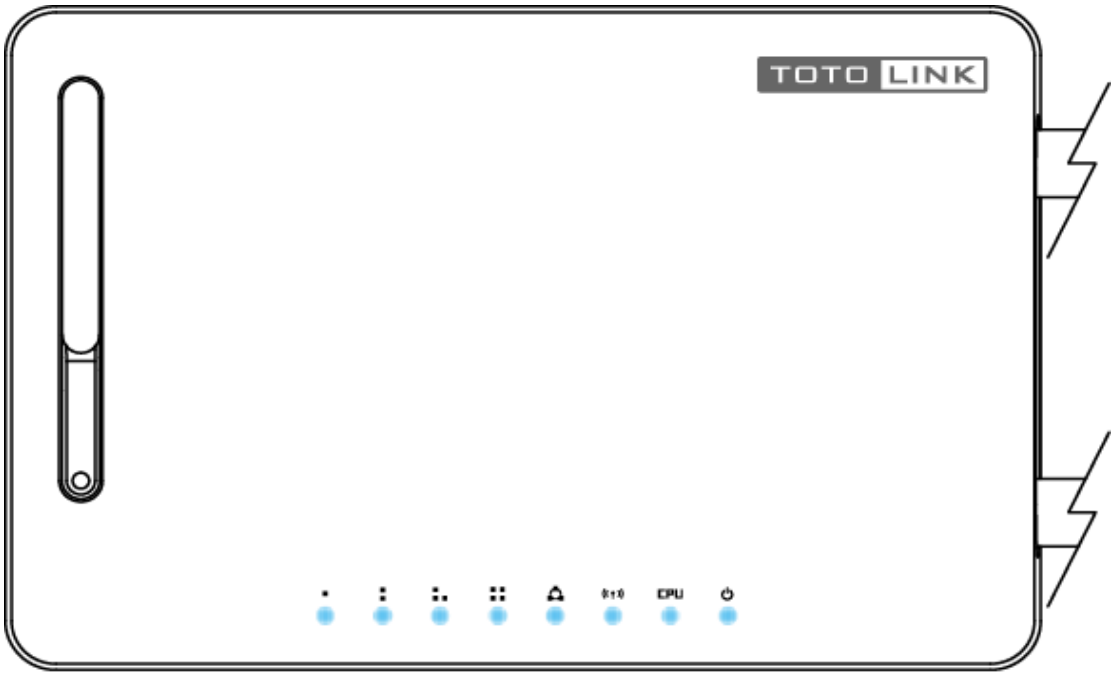
2.2 Features

- Complies with IEEE 802.11n and IEEE802.11g/b standards.
- Supports 64/128-bit WEP, WPA /WPA2 and WPA-PSK/WPA2-PSK encryption.
- Connects to secure network easily and fast using WPS.
- Supports IP/ MAC/URL filtering and Port Forwarding.
- WDS mode makes it simple for WLAN expansion.
- Supports PPPoE, DHCP and Static IP broadband functions.
- QoS function maximizes the bandwidth use.
- Supports UPnP, Static Routing and DMZ host.
- Built-in DHCP server/Client.
- Supports remote/local web management.

2.3 Panel Layout

2.3.1 Front Panel

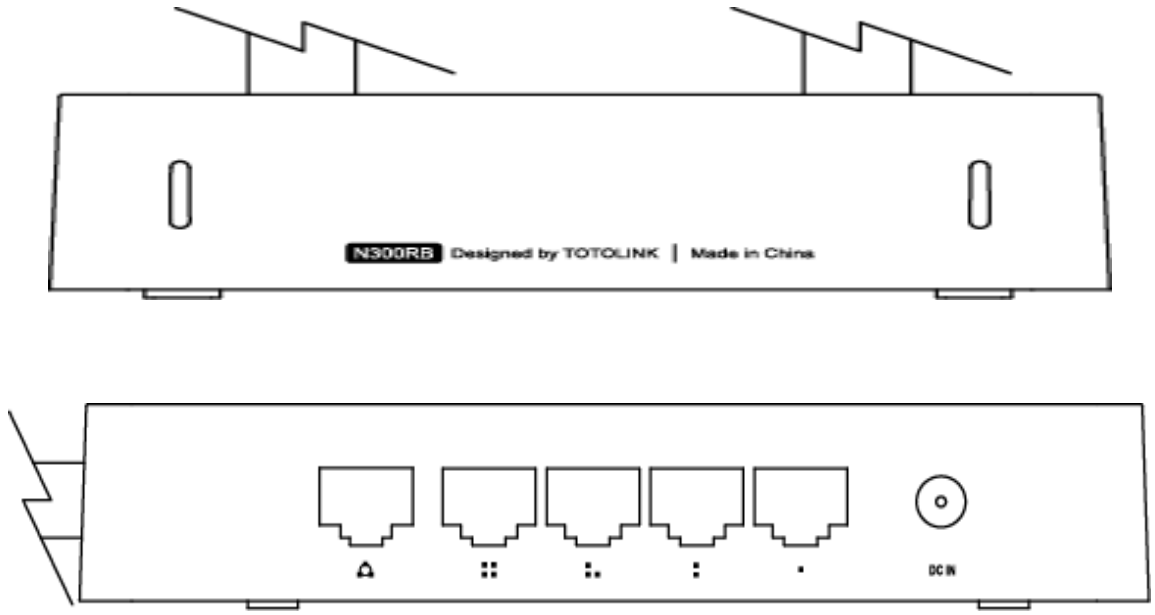
The front panel of this Wireless Router consists of 5 LEDs, which is designed to indicate connection status.



POWER	This indicator lights blue when the router is powered on, otherwise it is off.
CPU	This indicator keeps lighting when router powered on.
WLAN	This indicator lights when there are wireless devices connected and transmitting data to WLAN Router.
WAN	When the WAN port is connected successfully the indicator lights.
	During transmitting or receiving data through the WAN port the indicator blinks.
1/2/3/4 LAN	When one of the LAN ports has a successful connection, the corresponding indicator lights.
	During transmitting or receiving data through the LAN port the corresponding indicator blinks.

2.3.2 Rear Panel

The figure below shows the real panel of the Router.



DC IN	The Power socket is where you will connect the power adapter.
RST/WPS	**RST:** With the router powered on, press and hold the button until the CPU LED becomes quick-flash from slow-flash. And then release the button and wait the router to reboot to its factory default settings.
	WPS: If you have client devices you can press this button to quickly establish a router and client devices and automatically configure wireless security for your wireless network.
WAN	This port is where you will connect the DSL/cable Modem, or Ethernet.
1/2/3/4 LAN	This port connects the router to local PC.

Note: *Press and hold RST/WPS button for less than 5 seconds, the router will enable WPS function, and CPU LED indicator keeps ON. Press and hold WPS/RST button for more than 5 seconds, the router will enable RESET function, and CPU LED indicator keeps lighting.*

3. HARDWARE INSTALLATION

3.1 Hardware Installation

For those computers you wish to connect with Internet by this router, each of the computers must be properly connected with the router through provided UTP LAN Cables.

1. Connect the provided UTP LAN cable to one of the router's LAN port.
2. Connect the other end of the UTP LAN cable to your computer's LAN port.
3. Connect the second UTP LAN cable to router's WAN port.
4. Connect the other end of the UTP LAN cable to ADSL or Modem port.
5. Plug the Power Adapter into the Router and then into an outlet.
6. Turn on your computer.
7. Check and confirm that the Power LED and LAN LED on the router are **ON**.

3.2 Check the Installation

The control LEDs of the WLAN Router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, CPU, LAN, WLAN and WAN port LEDs of the WLAN Router will blink for one time indicating a normal status.
2. When the WAN Port is connected to the ADSL/Cable modem, the WAN LED will light up.
3. When the LAN Port is connected to the computer system, the LAN LED will light up.

3.3 Set up the Computer

The default IP address of the Router is 192.168.1.1, the default Subnet Mask is 255.255.255.0. Both of these parameters can be changed as you want. In this guide, we will use the default values for description.

Connect the local PC to the LAN port on the Router. There are then two ways to configure the IP address for your PC.

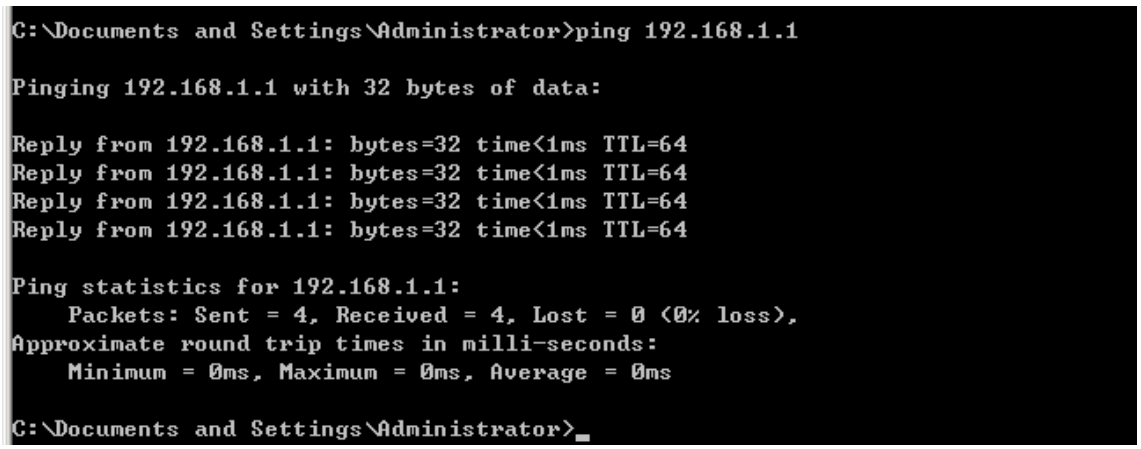
- **Configure the IP address manually**

1. Set up the TCP/IP Protocol for your PC.
2. Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" range from 2 to 254). The Subnet Mask is 255.255.255.0 and Gateway is 192.168.1.1 (Router's default IP address).

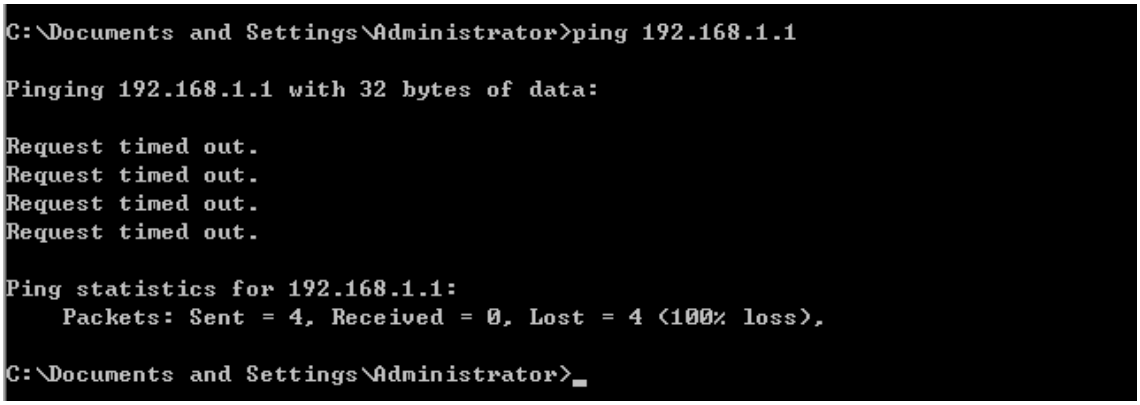
- **Obtain an IP address automatically**

1. Set up the TCP/IP Protocol in **Obtain an IP address automatically** mode on your PC.
2. Power off the Router and PC. Then turn on the Router and restart the PC. The built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the Router. Open a command prompt, and type in **ping 192.168.1.1**, then press **Enter.**



If the result displayed is similar to that shown in above figure, it means that the connection between your PC and the Router has been established.



If the result displayed is similar to that shown in the above figure, it means that your PC has not connected to the Router successfully. Please check it following below steps:

1. Is the connection between your PC and the Router correct?

If correct, the LAN port on the Router and LED on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Since the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the Gateway must be 192.168.1.1.

4. BASIC CONFIGURATION

This chapter introduces how to configure the basic functions of your Wireless N Router so that you can surf the Internet.

Web page's key functions

4.1 Login Web Interface

With a Web-based utility, for example Internet Explorer, the Wireless N Router is easy to configure and manage.

Connect to the Router by typing 192.168.1.1 in the address field of Web Browser. Then press **Enter** key.

It will show up the following page:

Click Internet Wizard  or Wireless Wizard  , it will guide you through step-by-step instructions on how to setup set up your wireless network and how to make it secure.

We will mainly introduce the Router's setting Interface in this part.

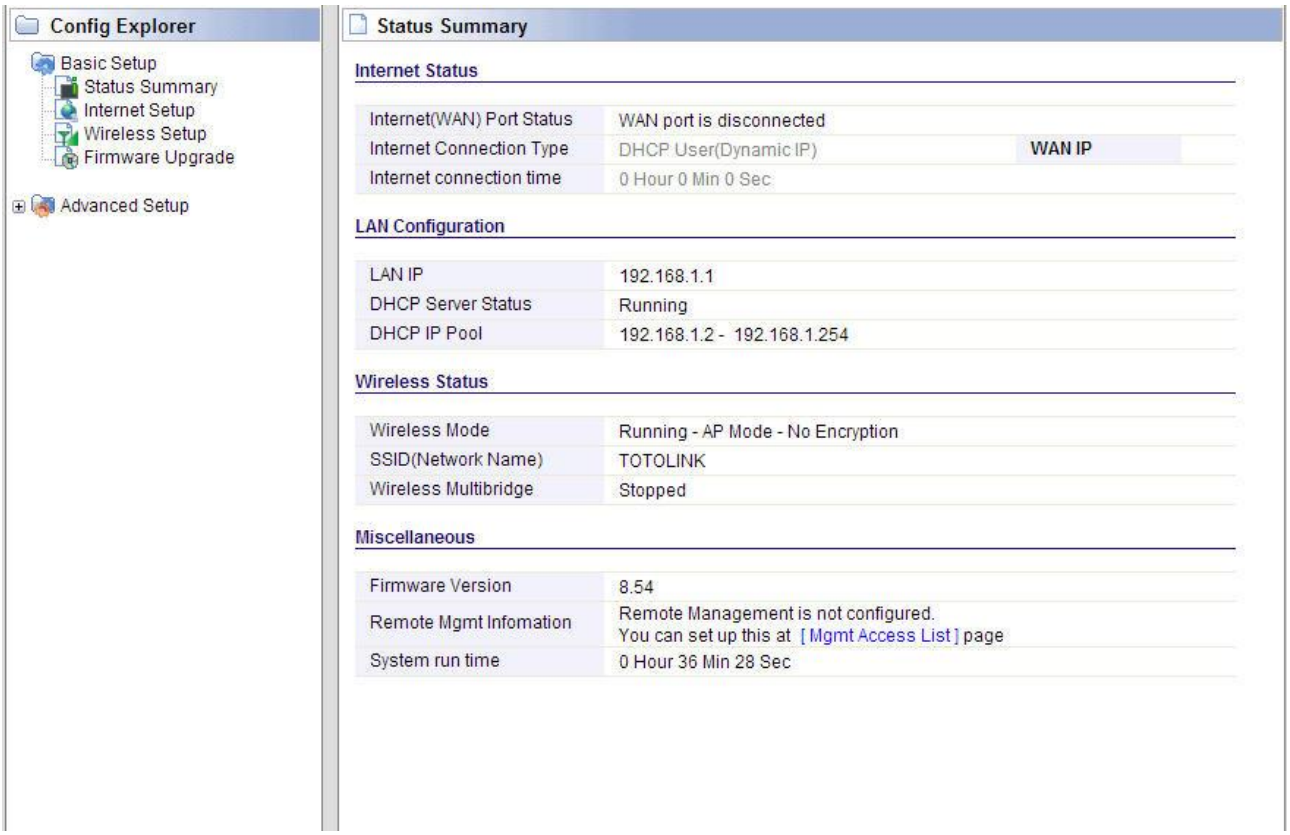
Click **Setup Tool** icon  to enter the Router's setting interface, then below window will pop up that requires you to enter valid User Name and Password.

Enter **admin** for User Name and Password, both in lower case letters. Then click **Log In**

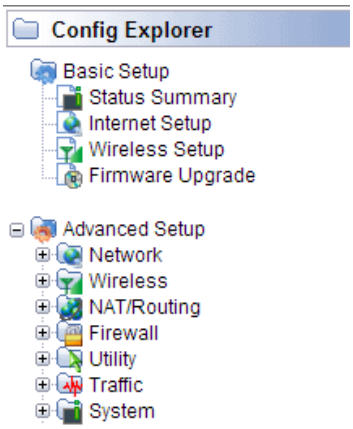
button or press **Enter** key.

> ***Note:*** *If the above screen does not prompt, it means that your web-browser has been set to using a proxy. Go to* ***Tools menu>Internet Options>Connections>LAN Settings****, in the screen that appears, cancel the* ***Using Proxy checkbox****, and click* ***OK*** *to finish it.*
> *If the User Name and Password are correct, you can configure the router using the web browser. Please click the* ***Internet Setup*** *link on the left main menu and the Internet Setup screen will appear.*

Now, you will get into the Router's configuration interface. First, you will see the Status Summary of the Router:

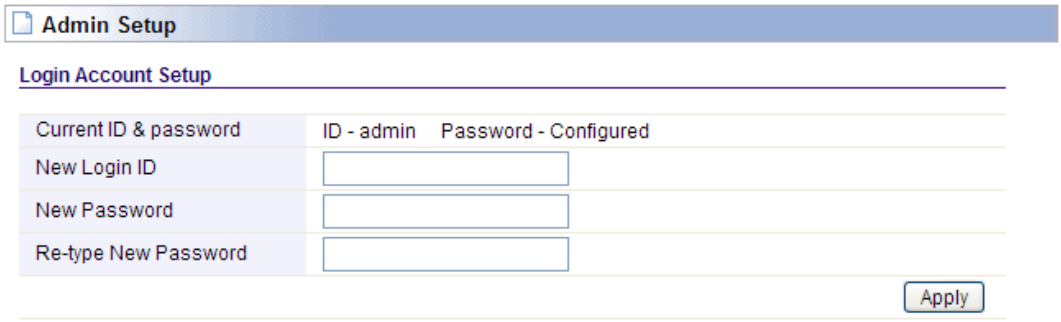


On the left, it is the guide bar:



4.2 Changing Password

Now, we recommend that you change the password to protect the security of your Router. Please go to **System—Admin Setup** change the password required to log into your Router.



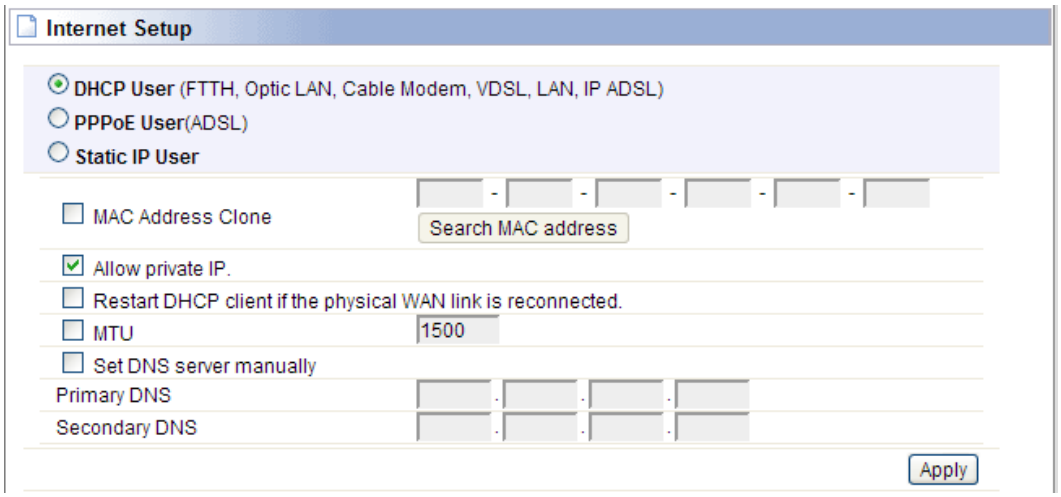
New Login ID: type in the name that you use to login the web interface of the router or change a new one.
New Password: new password is used for administrator authentication.
Re-type New Password: new password should be re-entered to verify its accuracy.

> ***Note:*** *password length is 8 characters maximum, characters after the 8th position will be truncated.*

4.3 Internet Setup

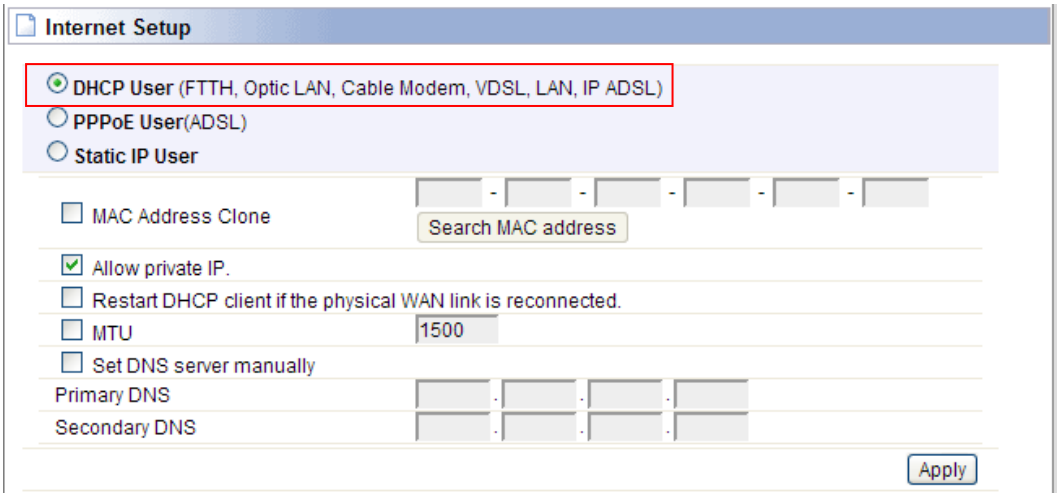
This page is used to configure the parameters for Internet Network which connects to your wireless Router WAN port. WAN access modes include DHCP, PPPoE and Static IP.

1. Click **Internet Setup**, it will show you three modes to choose:



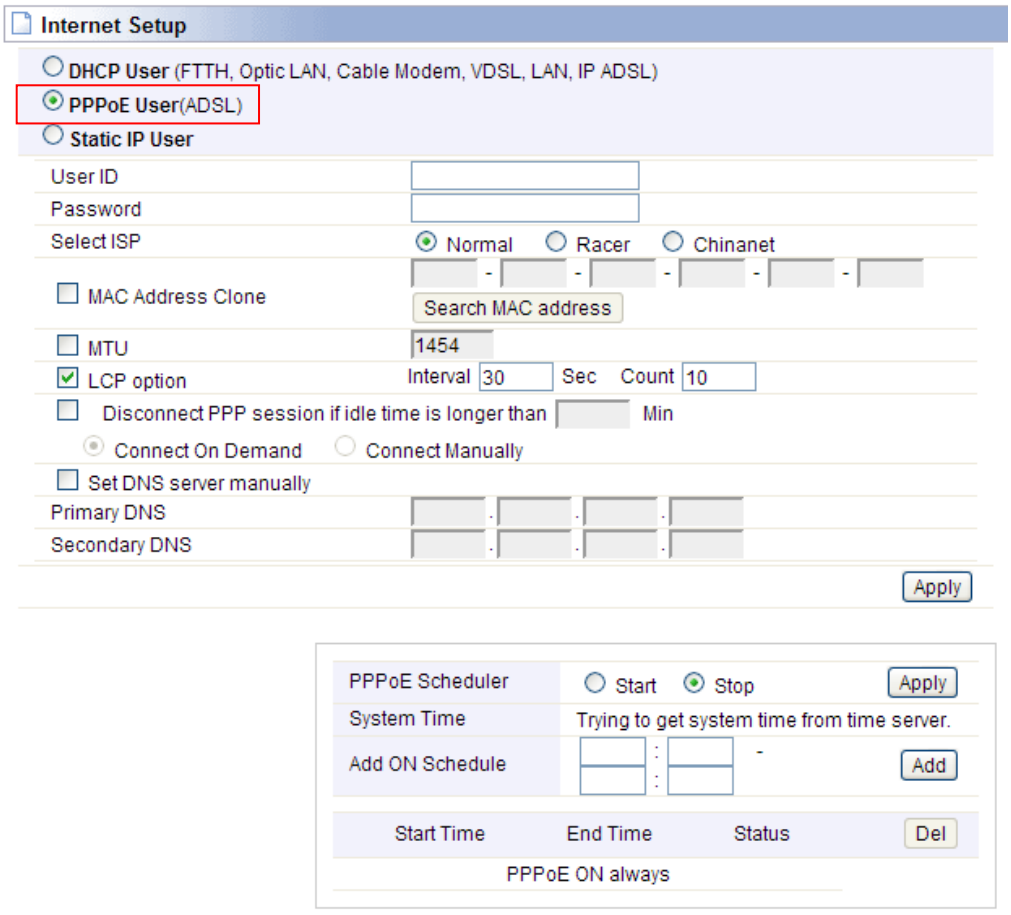
4.3.1 DHCP User

If you choose DHCP User, your computer will get dynamic IP address from your ISP (Internet Service Provider) operator automatically.



4.3.2 PPPoE User (ADSL)

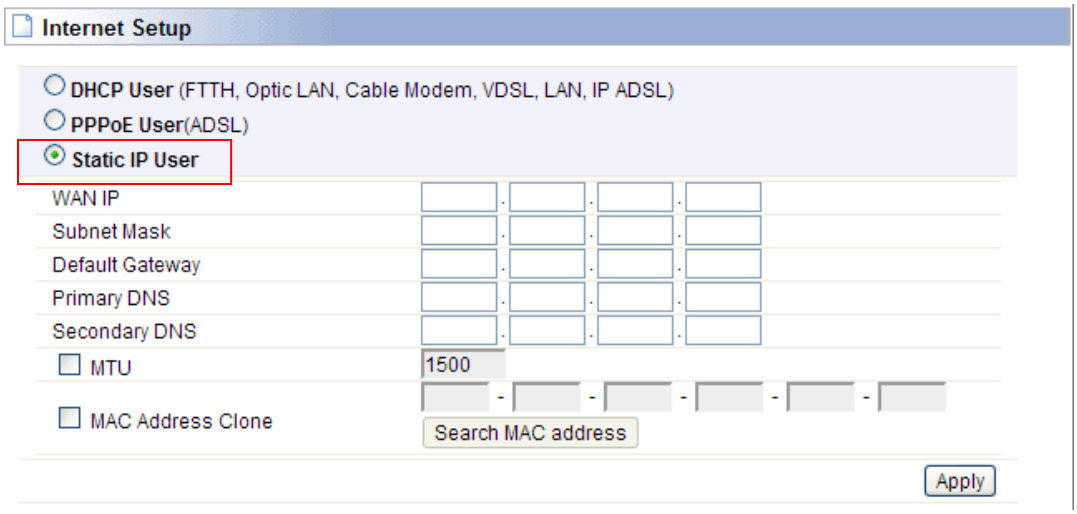
Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. It replies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as wireless device or cable modem. All the users over the Ethernet can share a common connection. If you use ADSL virtual dial-up to connect Internet, please choose this option.



User ID: a specific valid ADSL user name provided by your ISP.
Password: the corresponding valid password provided by your ISP.

4.3.3 Static IP

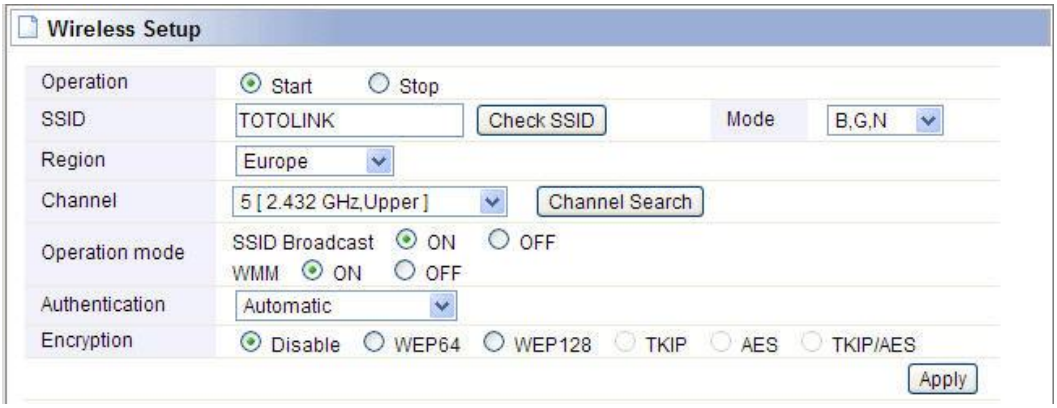
Input the IP address that provided by your ISP (Internet Service Provider). If you are not clear about this, please consult with your local ISP.



WAN IP: the IP address provided by your ISP.
Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.
Default Gateway: This is the IP address of the host router that resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The router will direct all the packets to the gateway if the destination host is not within the local network.
Primary DNS: Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. This is provided by your ISP.
After you finish the blank that required, you could click **Apply** to make it work.

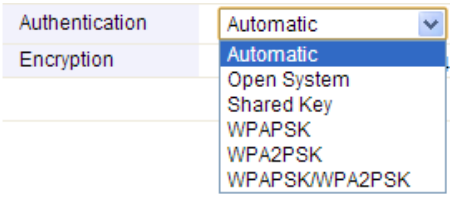
4.4 Wireless Setup

Click **Wireless Setup**, you will see below interface. This webpage shows the basic wireless parameters and wireless authentication ways.

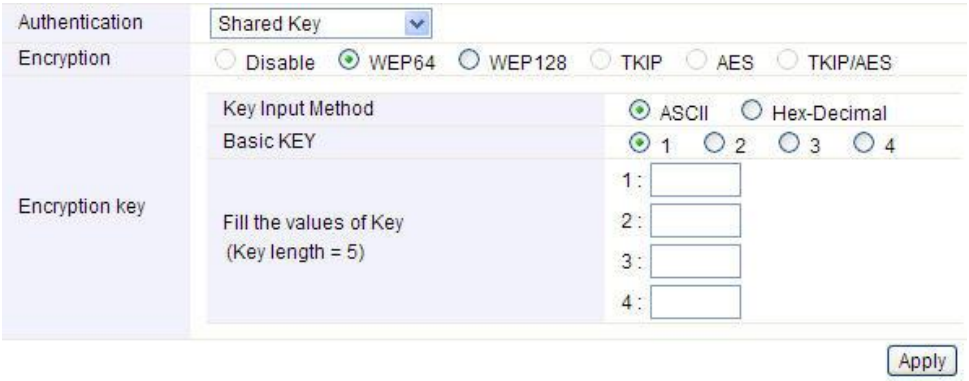


Operation: You can choose Start or Stop the wireless function.

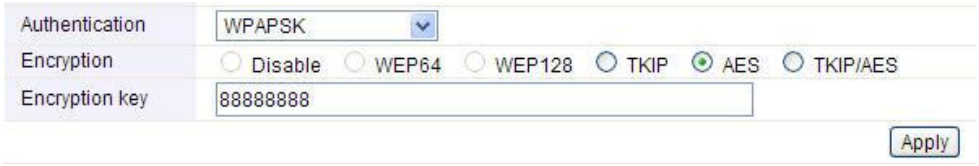
SSID: You can change the SSID for your wireless router.
Mode: If wireless connection conforms to 11g, 11b and 11n standards.
Region: Area where you are using the wireless router.
Channel: Choose the wireless channel in AP mode. If in client mode, channel option is disabled.



Encryption: You can choose Automatic, Open System, Shared Key, WPAPSK, WPA2PSK, WPAPSK/WPA2PSK.
WEP: Wired Equivalent Protocol is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encryption data being transferred over your wireless network. WEP is the oldest security algorithm, and there are few applications that can decrypt the WEP key in less than 10 minutes.



WPA: WiFi Protected Access, WPA is an intermediate solution for the security issues. It uses Temporal Key Integrity Protocol (TKIP) to replace WEP. It is the most dominating security mechanism in industry. It is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.



WPA2: means Wi-Fi Protected Access 2, it is the current most secure method of wireless security and required for 802.11n performance.

TKIP--Temporal Key Integrity Protocol is one cipher for data encryption supported by WPA. It is a compromise on strong security and possibility to use existing hardware. It still uses RC4 for the encryption like WEP, but with per-packet RC4 keys. In addition, it implements replay protection, keyed packet authentication mechanism (Michael MIC).

AES--Advanced Encryption Standard is another cipher for data encryption supported by WPA.

4.5 Firmware Upgrade

New version of firmware will be released to improve the various efficiency or to fix some bugs. This page allows you to upgrade the Access Point firmware to new version. Following the steps show below so as to realize upgrading.
Please note: DO NOT power off the device during upgrading because it may crash the system.

After finishing the settings above, you'd better restart your computer and the Router to connect to Internet successfully. Then you can enjoy the high-speed and high-stability Internet through this Router.

5. ADVANCED SETUP

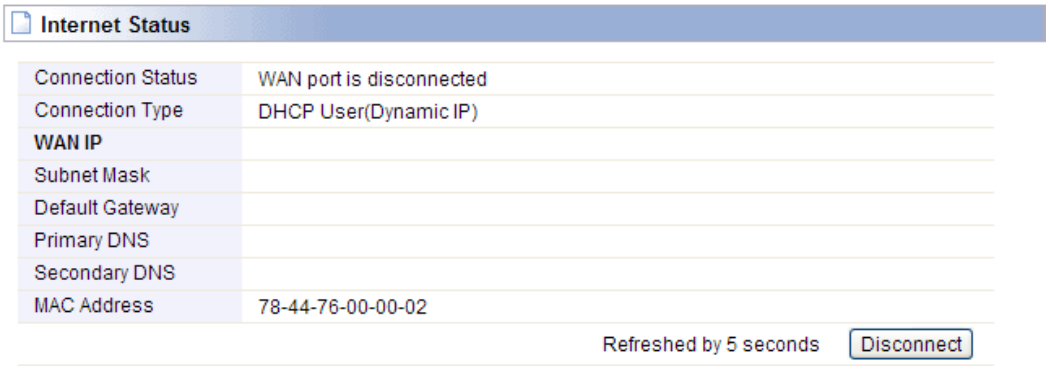
The Advanced Setup includes Network, Wireless, NAT/Routing, Firewall, Utility, Traffic and System. These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Also they should not be changed unless you know what effect the changes will have on your Wireless Router.

5.1 Network

Click the plus sign beside **Network** menu to show up all Network parameters you could set up.

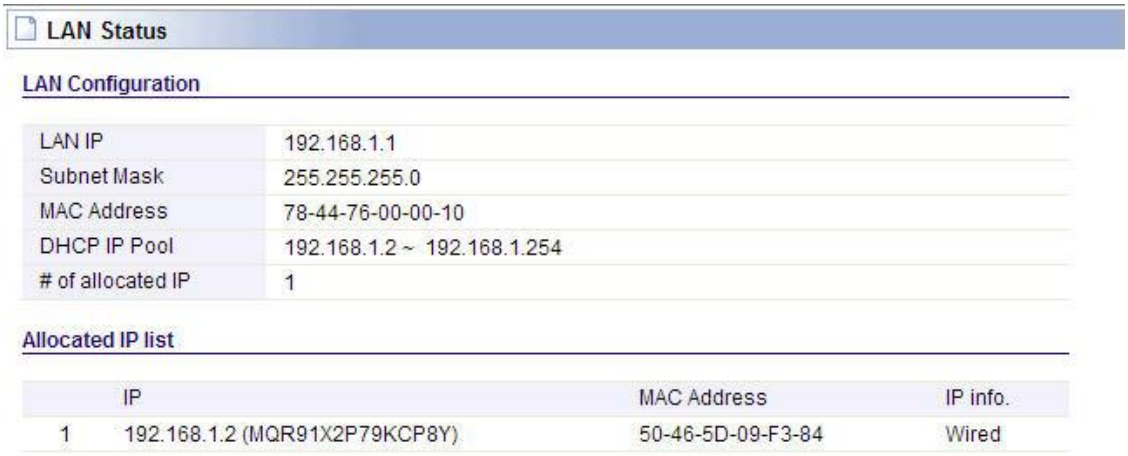
5.1.1 Internet Status

This page shows the Internet Status of this Router.



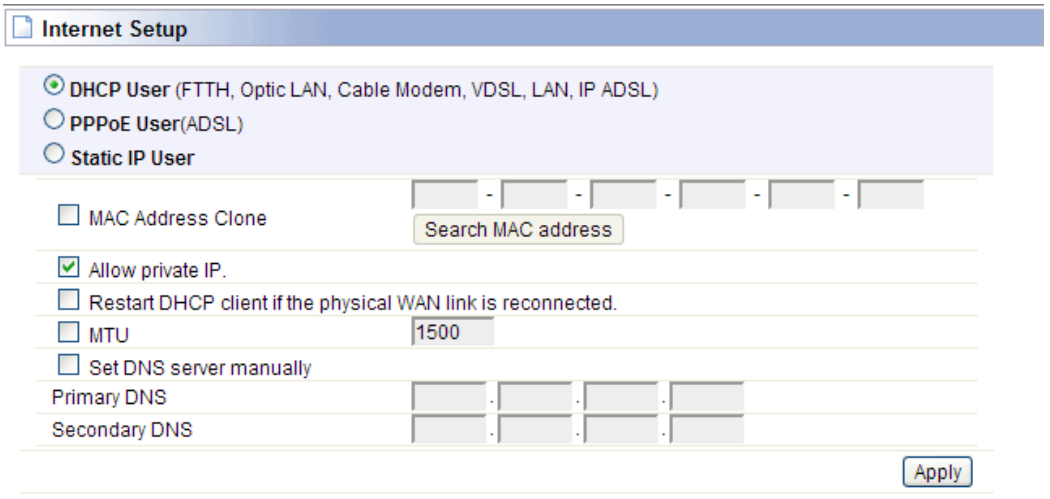
5.1.2 LAN Status

This page shows you LAN Status after your successful settings.



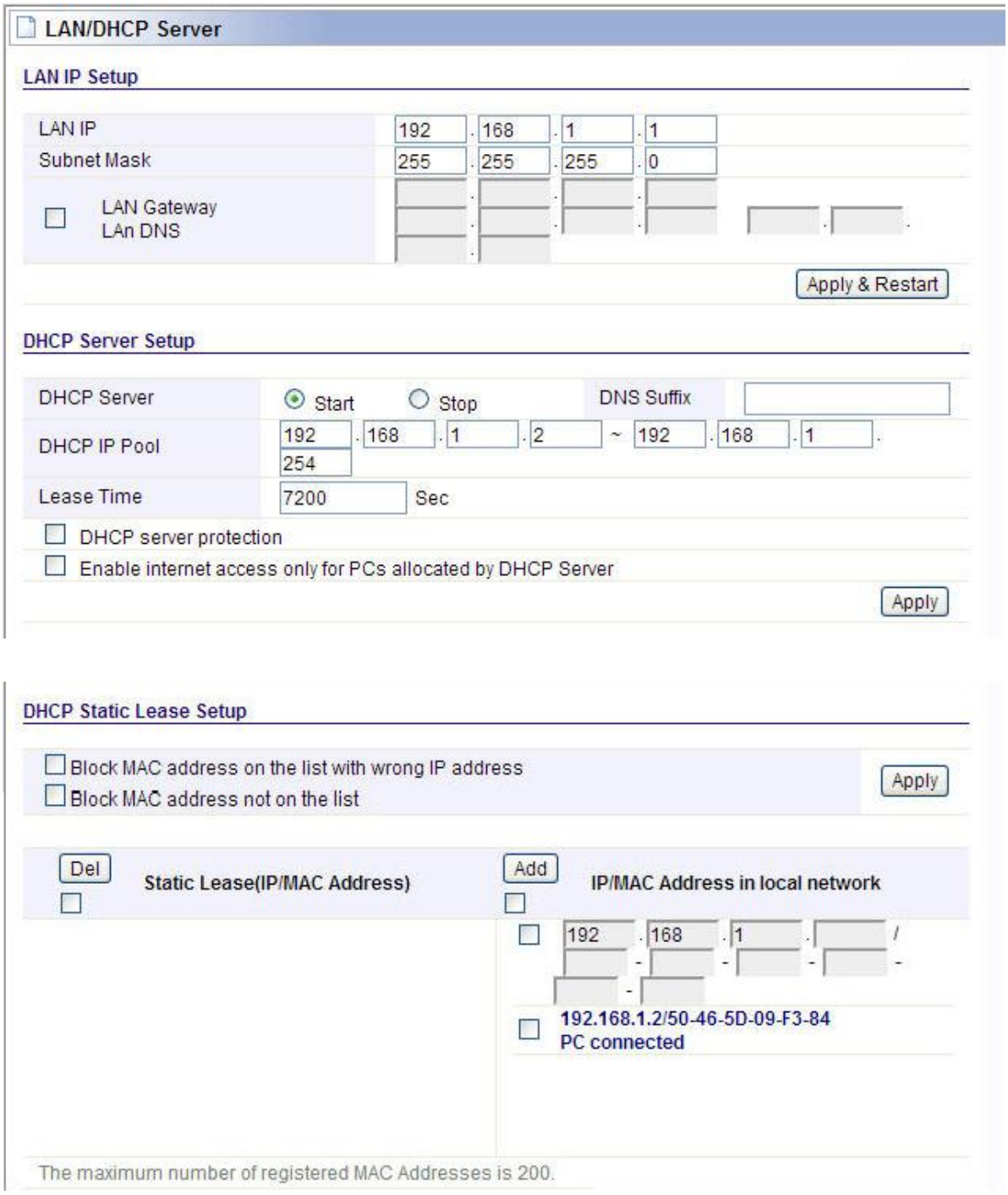
5.1.3 Internet Setup

We have discussed this setting on **4.3 Internet Setup**. You can reconfigure these settings on this page, please enter the parameters according to what your ISP provided.



5.1.4 LAN/DHCP Server

Click **LAN/DHCP Server**, you will enter the page that allows you configure the LAN port and DHCP Server. Since the LAN configuration we have discussed before, here we will tell you how to set up the DHCP Server parameters.



DHCP Server: you can choose to start or stop DHCP.
DHCP IP Pool: it is the IP range that the DHCP server will assign to every PC connected with the router.
Lease Time: the IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential

address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

Block MAC address on the list with wrong IP address: The PC'S MAC address has existed on the rule but with the wrong IP can't connect to Internet.

Block MAC address not on the list: The PC's MAC address isn't exists on the rule can't connect to Internet.

Static Lease (IP/MAC Address):

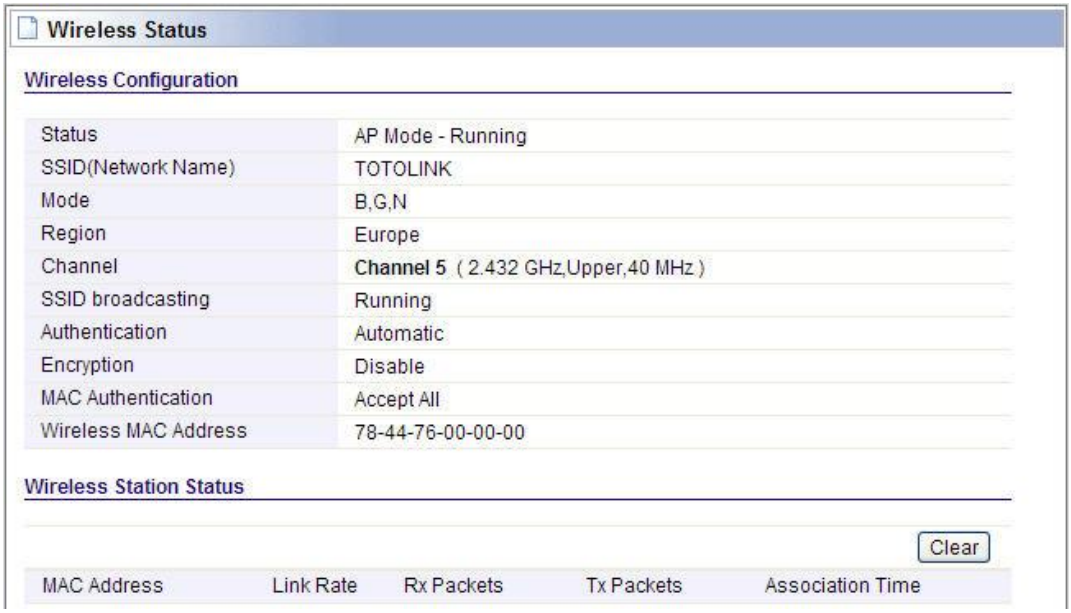
Static Lease function allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server. You can enable or disable this function.

5.2 Wireless

Next, you can set up the Wireless parameters. Click the plus sign beside **Wireless** menu to open up all wireless parameters, see below figure:

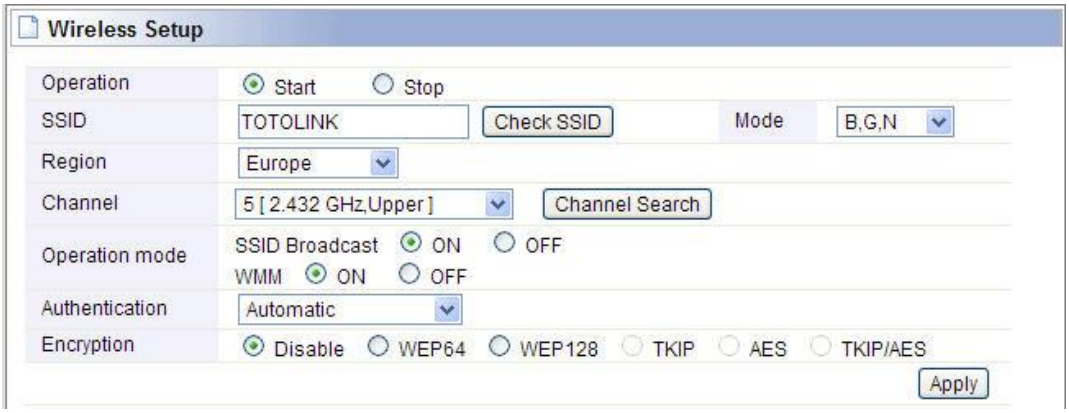
5.2.1 Wireless Status

Click **Wireless Status** menu, it will show you the current wireless status about the Router.



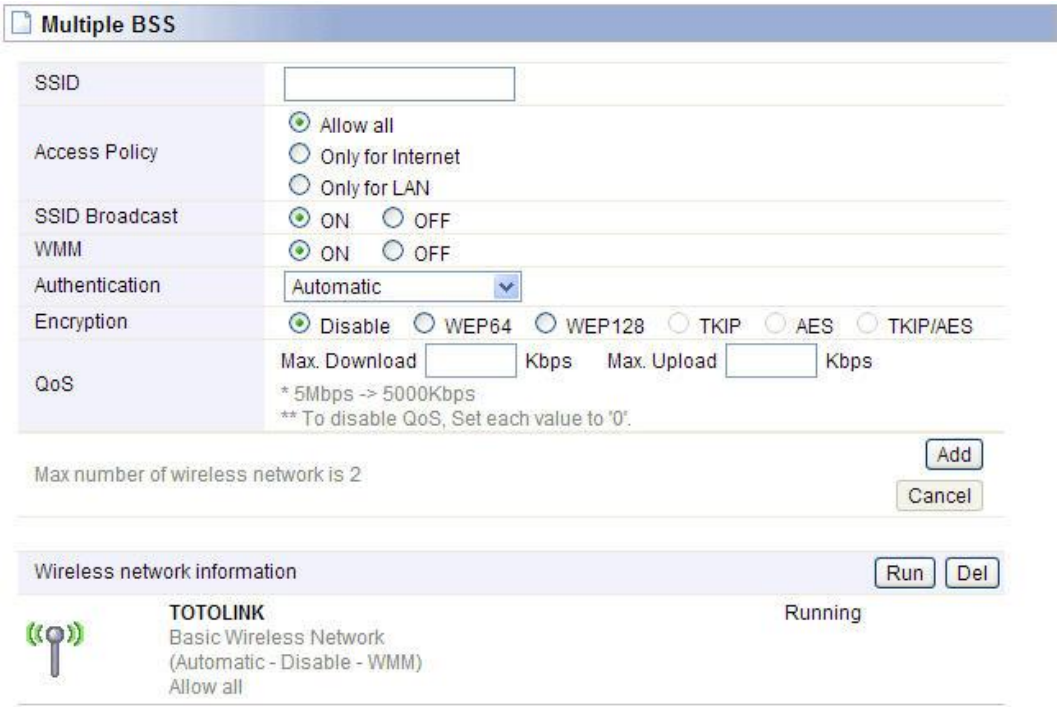
5.2.2 Wireless Setup

Click **Wireless Setup**, you will be able to configure the wireless corresponding function. We have discussed this setting on **4.4 Internet Setup**.



5.2.3 Multiple BSS

Multiple BSS function allows you to add other SSID for different needs. What's more, you can setup different encryption for different SSIDs.



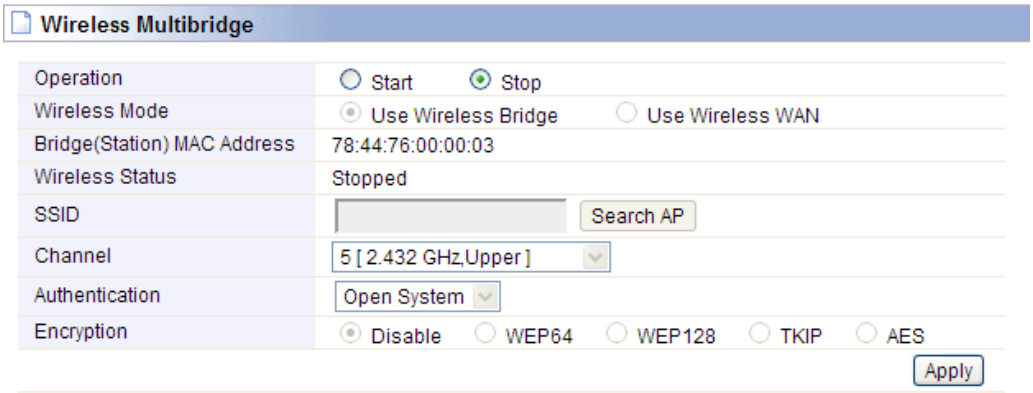
SSID: define the SSID by yourself.
Access Policy: setup the access policy as you want. Allow all, only for Internet or only for LAN according to your need.
SSID Broadcast: choose to hide or broadcast your SSID.
WMM: it is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data.

Encryption: you can choose the encryption method for WMM. Please refer to wireless security setup.

QoS: this option allows you to limit the download and upload data rate for every PCs connected with the router. So the bandwidth can be used reasonably.

5.2.4 Wireless Multibridge

When the wireless signal is too weak as the long distance, you can enable this function to extend the WiFi coverage.

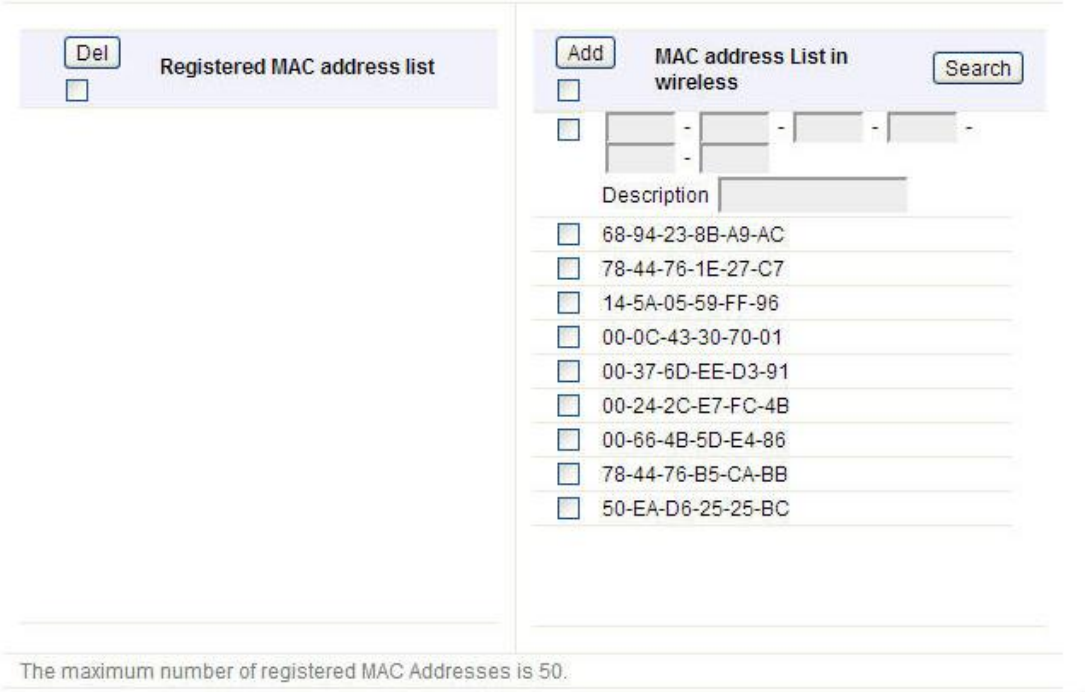


Wireless Bridge: In this mode, the router is used as an AP to get other router's signal.
Wireless WAN: The same function as **Wireless Bridge**, but the only setting difference is that Wireless WAN need not to stop the DHCP Server.
SSID: Click **Search AP**; choose the SSID of your Primary Router and then enter the encryption key of the upper AP if the encryption is enabled.

Note: *Both these two repeater methods can help you to expand the wireless coverage and allow more terminals to access Internet. But since Wireless WAN need not stop DHCP Server, all PCs' IP Addresses are assigned by the Secondary Router itself. So this method allows more PCs to access Internet than Wireless Bridge. In Wireless Bridge mode, the PCs' permissions to access Internet are decided by Primary Router which can make users to manage the LAN more easily.*

5.2.5 MAC Authentication

You can control the PC to connect the wireless Router through MAC authentication. At first, you should select the SSID of your wireless network. Then you can setup to allow all or just allow the specific PCs to connect to your wireless network.



5.2.6 WDS Setup

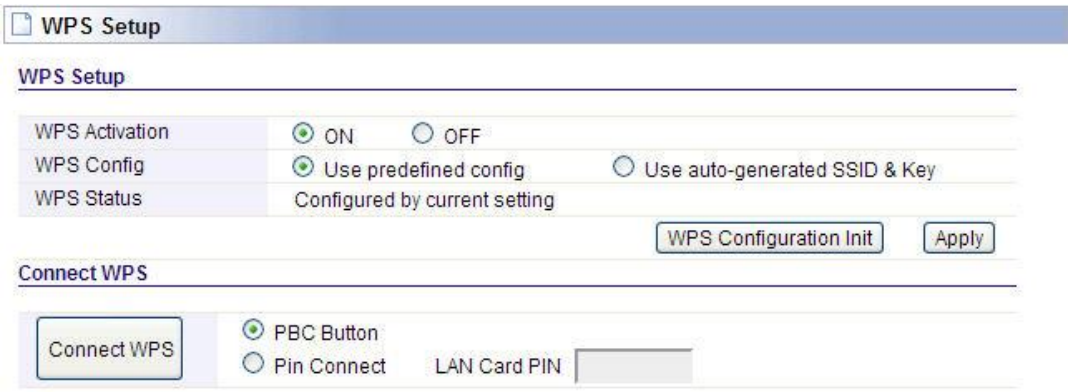
WDS means Wireless Distribution System. It is a protocol for connecting two access points wirelessly. Usually, it can be used for the following application:

1. Provide bridge traffic between two LANs though the air.
2. Extend the coverage range of a WLAN.

To meet the above requirement, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

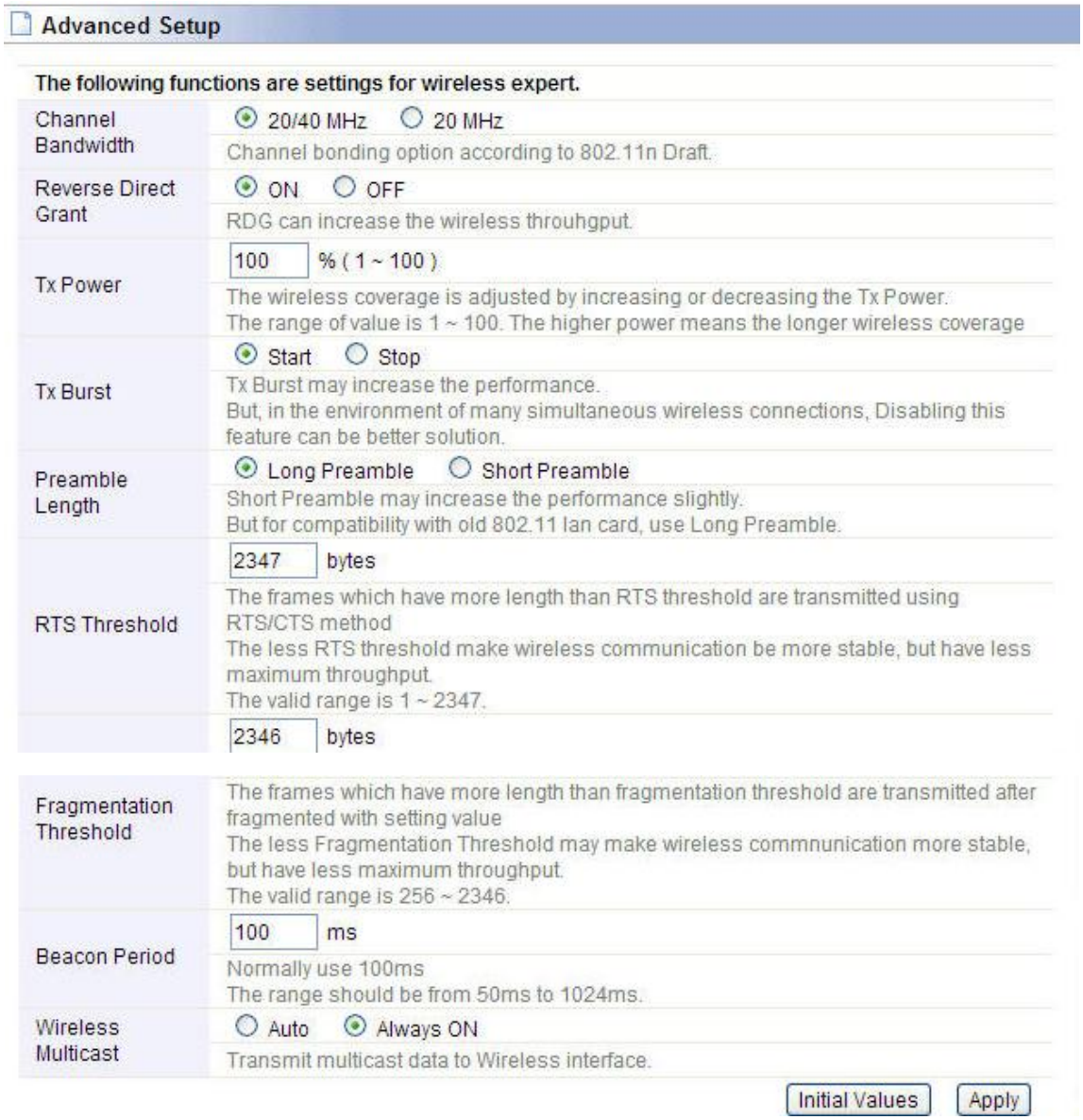
5.2.7 WPS Setup

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2. It is enabled by default.



5.2.8 Advanced Setup

Advanced Setup is for advanced parameter settings. For common users, please just keep the default configuration.



Channel Width: this is the spectral width of the radio channel. Supported wireless channel spectrum widths:

20MHz is the standard channel spectrum width.

40MHz is the channel spectrum with the width of 40MHz (selected by default).

Reverse Direct Grant: this option can increase the wireless throughput.

TX Power: please refer to the description on the page.

Rx Power: please refer to the description on the page.

Preamble Length: this option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses shot preamble with 56 bit sync filed instead of long preamble with 128 bit sync filed. However, some original 11b wireless network devices only support long preamble.

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347 bytes. The default value is 2347, which means that RTS is disabled.

RTS/CTS (Request to Send / Clear to send) are the mechanism used by the 802.11 wireless networking protocols to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

System uses Request to Send/Clear to send frames for the handshake that provide collision reduction for an access point with hidden stations. The stations are sending a RTS frame first while data is sent only after a handshake with an AP is completed. Stations respond with the CTS frame to the RTS, which provide clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all the other stations hold off the transmission and wait until the requesting station will finish transmission.

Fragment Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes. Setting the Fragment Threshold too low may result in poor network performance. The use of fragment can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However, lower values of the Fragment Threshold will result in lower throughput as well. Minor or no modifications of the Fragmentation Threshold value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

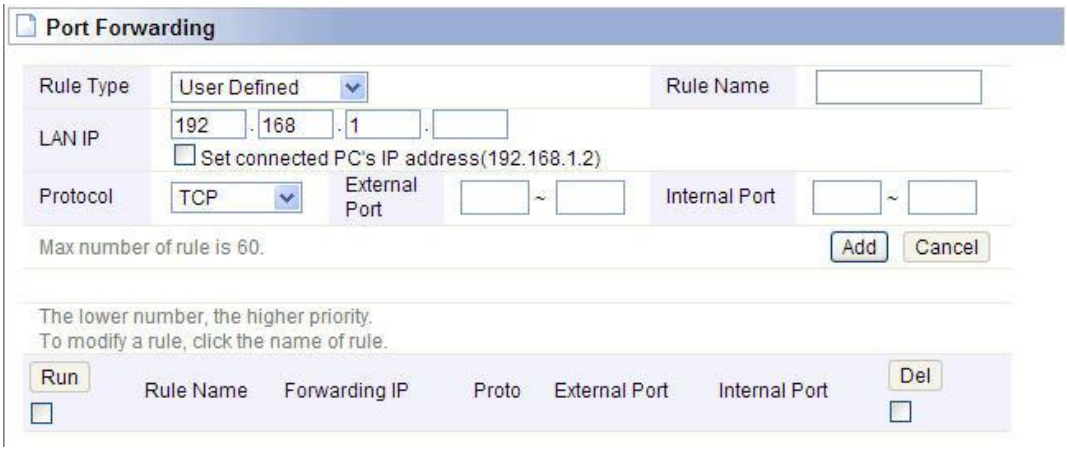
Beacon Period: By default, it is set to 100ms. Higher Beacon interval will improve the device's wireless performance and is also power-saving for client side. If this value set lower than 100ms, it will speed up the wireless client connection.

5.3 NAT/Routing

Click the plus sign beside **NAT/Routing** menu to open us all the parameters contained, see below:

5.3.1 Port Forwarding

On this page, you can redirect common network services automatically to a specific device behind the NAT firewall. This setting is only necessary when you want to host some sort of servers like a Web server or mail server on the private local network behind your Gateway's NAT firewall.



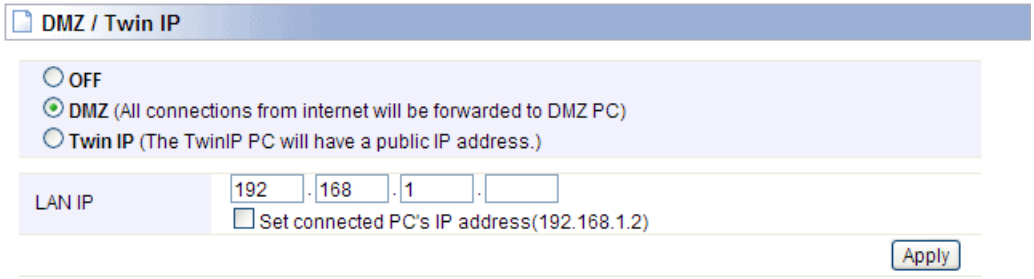
LAN IP: You can set the IP Address that you defined the rule for.

Protocol: Choose which particular protocol type should be forwarding. Here you can choose UDP/TCP.
External Port: Set the WAN range.
Internal Port: Set the LAN range.

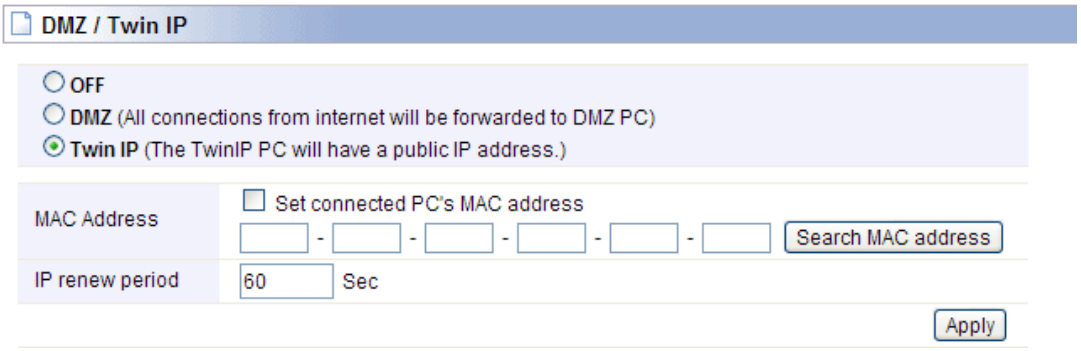
5.3.2 DMZ/Twin IP

The DMZ (Demilitarized Zone) host feature allows one local host to be exposed to the Internet for a special-purpose service such as Online Game and video conferencing. DMZ host forwards all the ports at the same time. Any PCs whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it, because its IP Address may be changed when using the DHCP function.

While you select DMZ option, you should enter the LAN IP address and click Apply to save configuration.

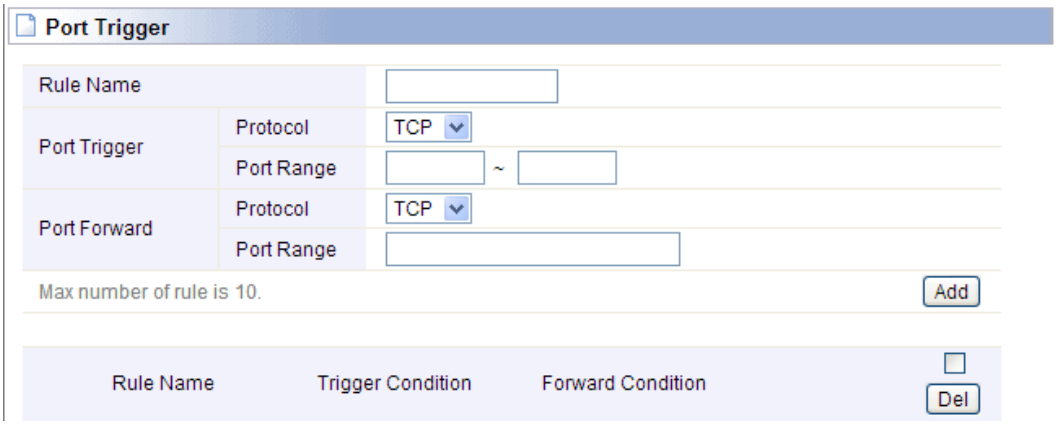


While you choose the Twin IP option, you should enter the MAC address and IP address.



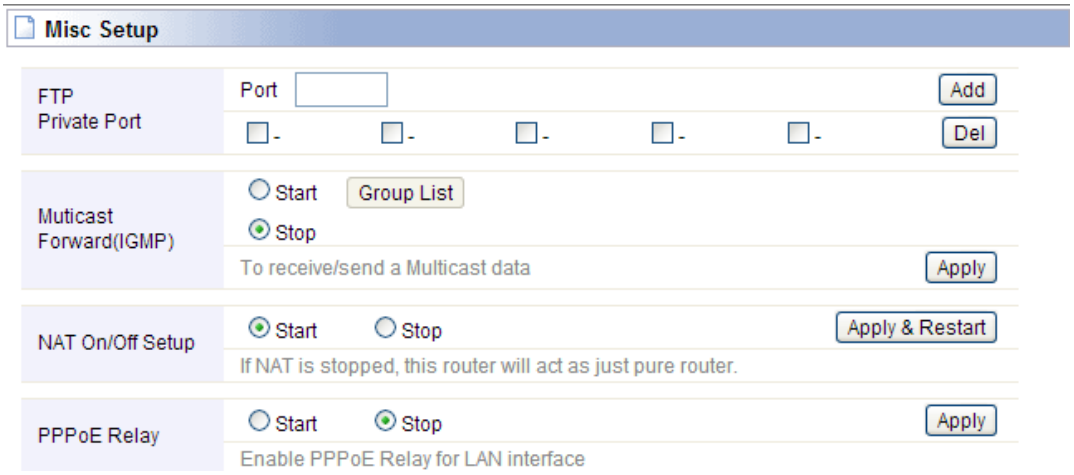
5.3.3 Port Trigger

Port Trigger is used to realize that when there comes the Outbound streaming from a specified network port (triggered port), automatically opens the gateway WAN-side interfaces specified port (forwarded port), and the streams will forward to the triggered ports. You can achieve some special purposes by this setting.



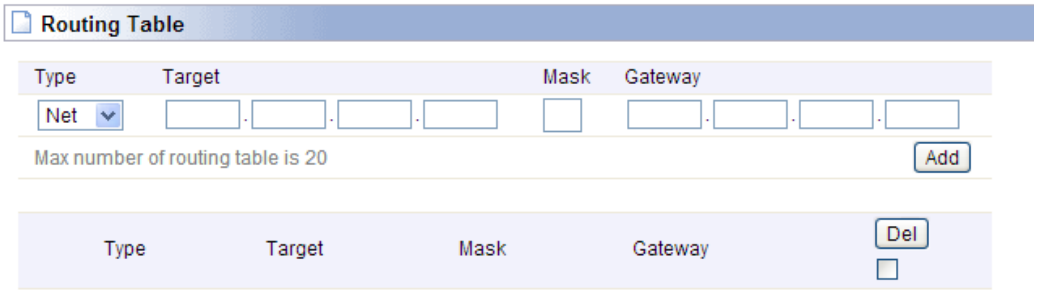
5.3.4 Misc Setup

Misc setup provides FTP Private Port, Multicast Forward and NAT on/off setup.



5.3.5 Routing Table

You can add or delete the static routing rules here.

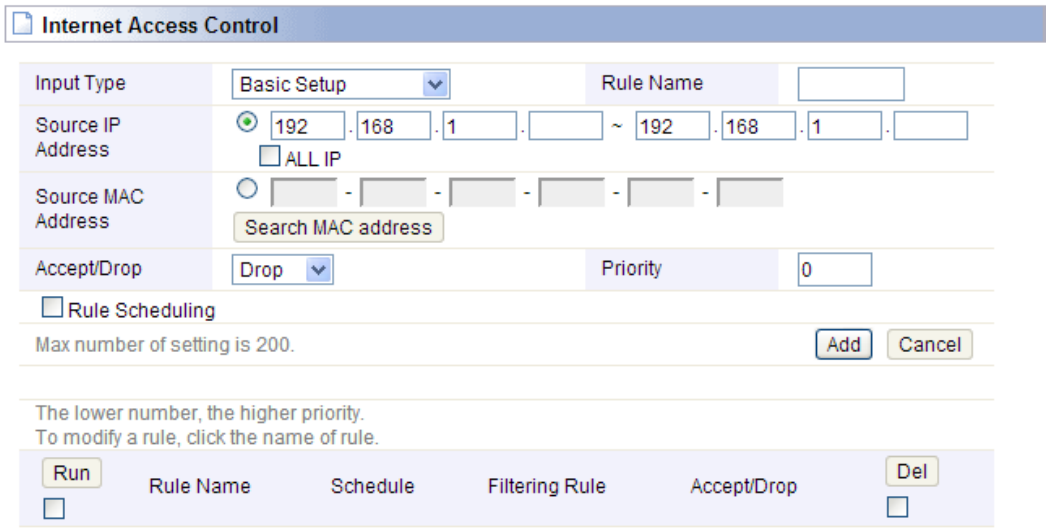


5.4 Firewall

Click the plus sign beside **Firewall** menu to show up all the parameters contained, see below:

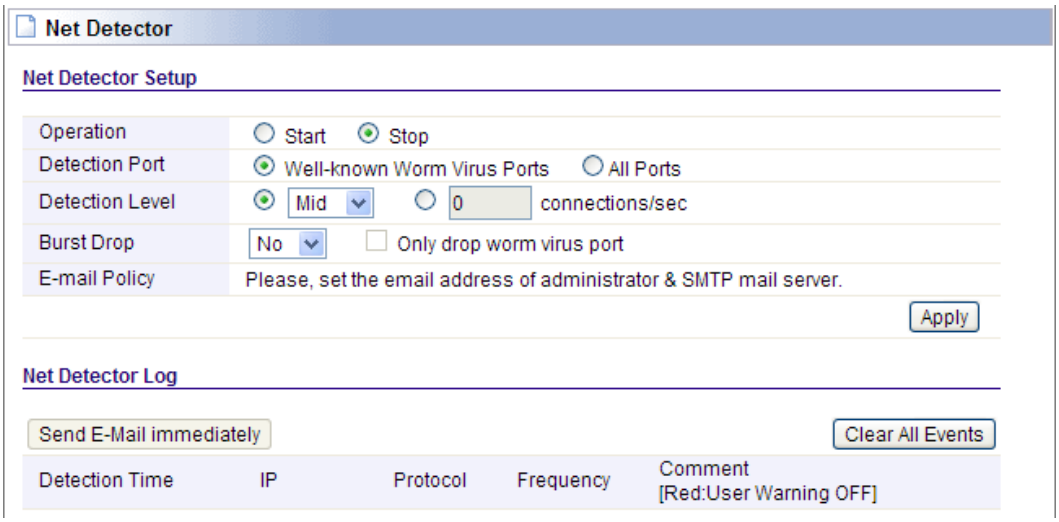
5.4.1 Internet Access Control

Internet Access Control provides multiple security protection. It can achieve MAC/Port/IP filtering, Internet access time control and other functions that enable user to control Internet access.

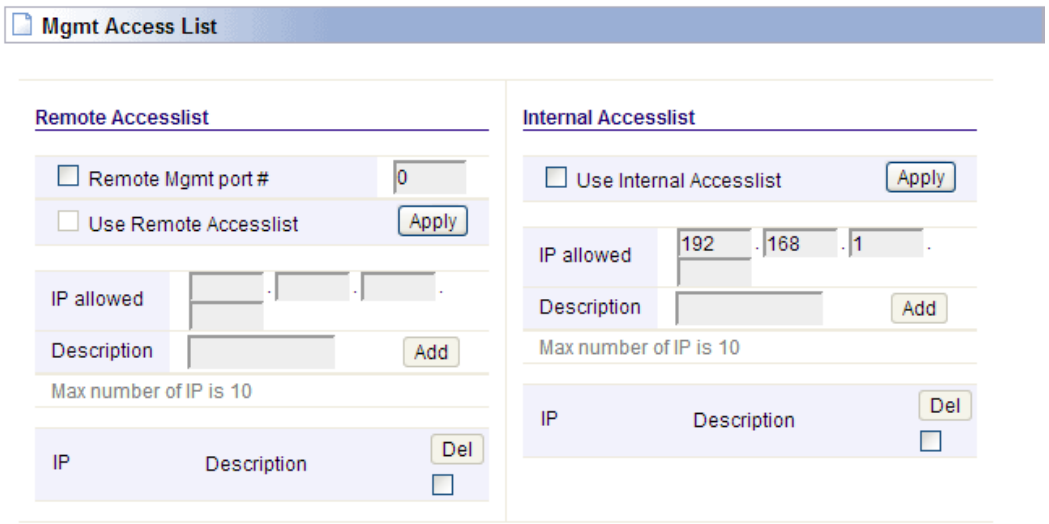


5.4.2 Net Detector

Net Detector provides some basic virus protection function that allows user to have a safer network communication.

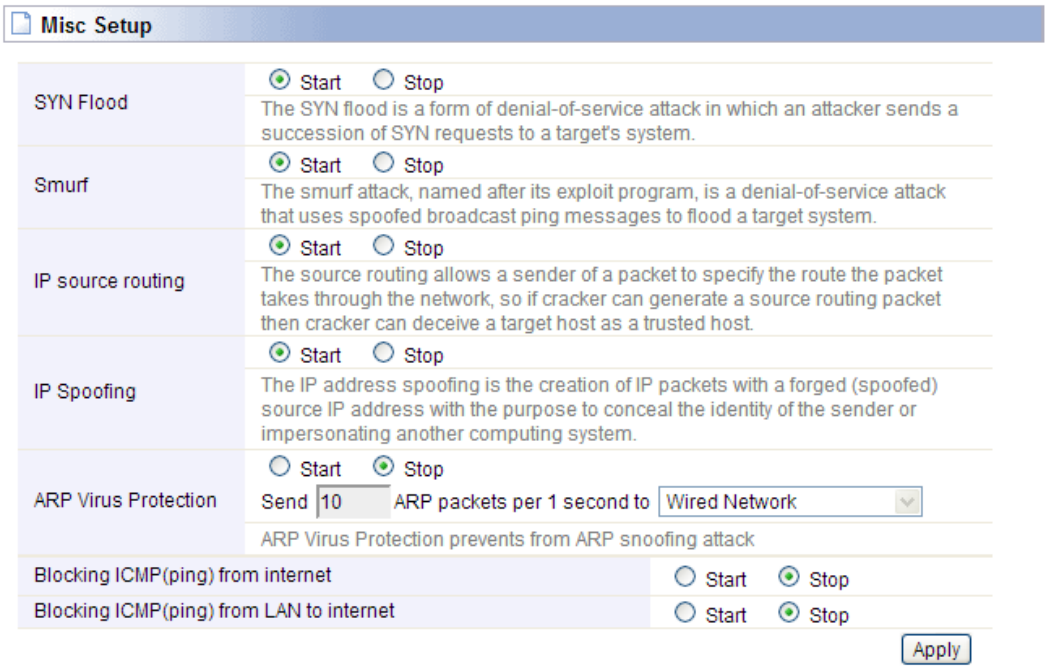


5.4.3 Mgmt Access List



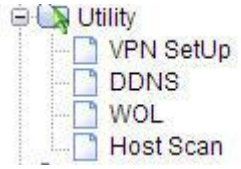
5.4.4 Misc Setup

Recommend to keep the default settings.



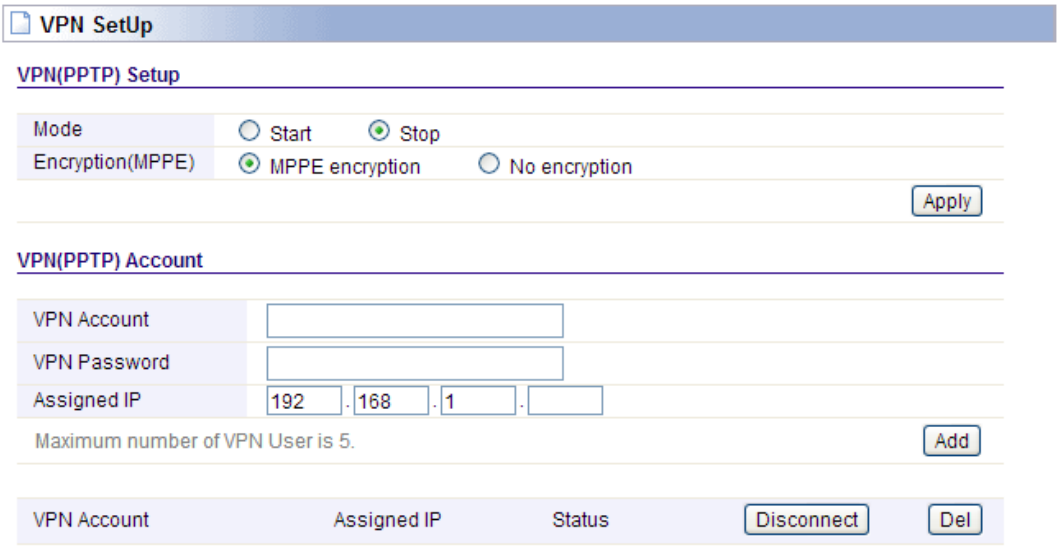
5.5 Utility

Click the plus sign beside **Utility** menu to open up all the parameters contained, please see below:



5.5.1 VPN Setup

The wireless router provides PPTP protocol VPN connection, and it supports 5 VPN users at most. Please enter the account information to connect the VPN server.



VPN (PPTP) Setup

Mode: Click Start to enable VPN server and otherwise disable.

Encryption (MPPE): MPPE encryption

Click **Apply** (this is very important, if you don't click **Apply,** the settings below will not work).

VPN (PPTP) Account

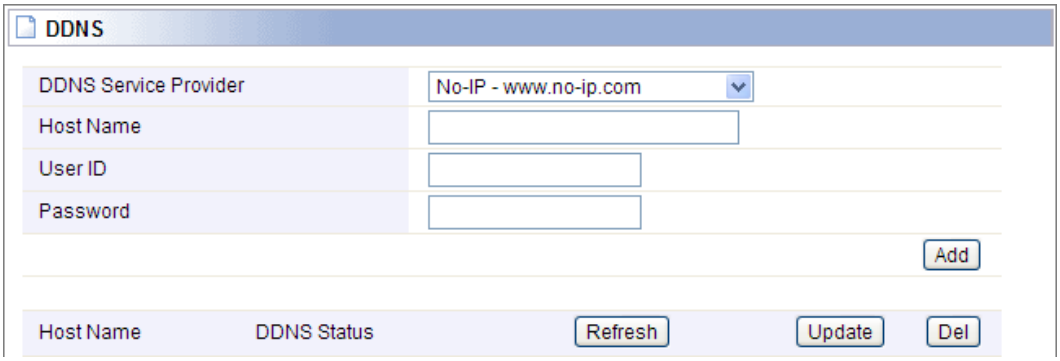
VPN Account & Password: Set the VPN account and password for verifying.

Assigned IP: This should be in the same network with your LAN IP.

Click **Add**. You can create at most 5 VPN accounts by this router. After setup, you need to provide the VPN Account, Password and your WAN IP address to anyone that needs them. The VPN Client should follow right steps to make a successful VPN connection.

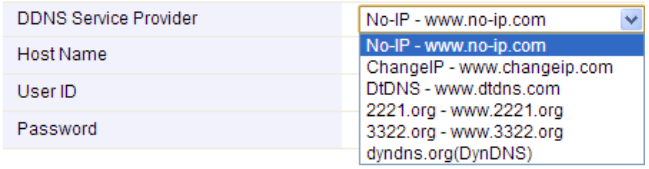
5.5.2 DDNS

DDNS (Dynamic Domain Name Server) is to achieve a fixed domain name to dynamic IP resolution. For dynamic IP address users, if there is any Internet access to their IP address, they need to show a fixed domain name to them. So their IP address will be sent to the DDNS service provider from the dynamic analysis server (3322, dyndns.org) and to update the DNS database. Then DDNS will bind the dynamic IP address to a fixed domain name. When other users on the Internet want to access this domain name, the dynamic DNS server will return the correct IP address. In this way, most users do not need to use fixed IP and can also name the fixed network system.



In order to set up DDNS, please follow the below steps:

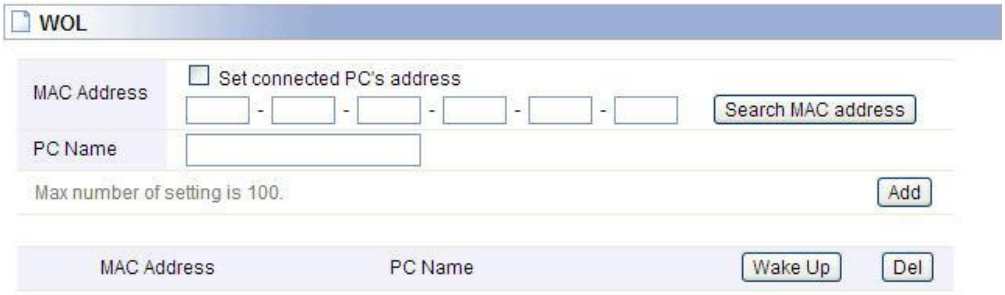
1. Choose your service provider.



2. Type in User Name for your DDNS account.
3. Type in Password for your DDNS account.
4. Host Name-the domain names are displayed here. Click **Add** to apply the modification.

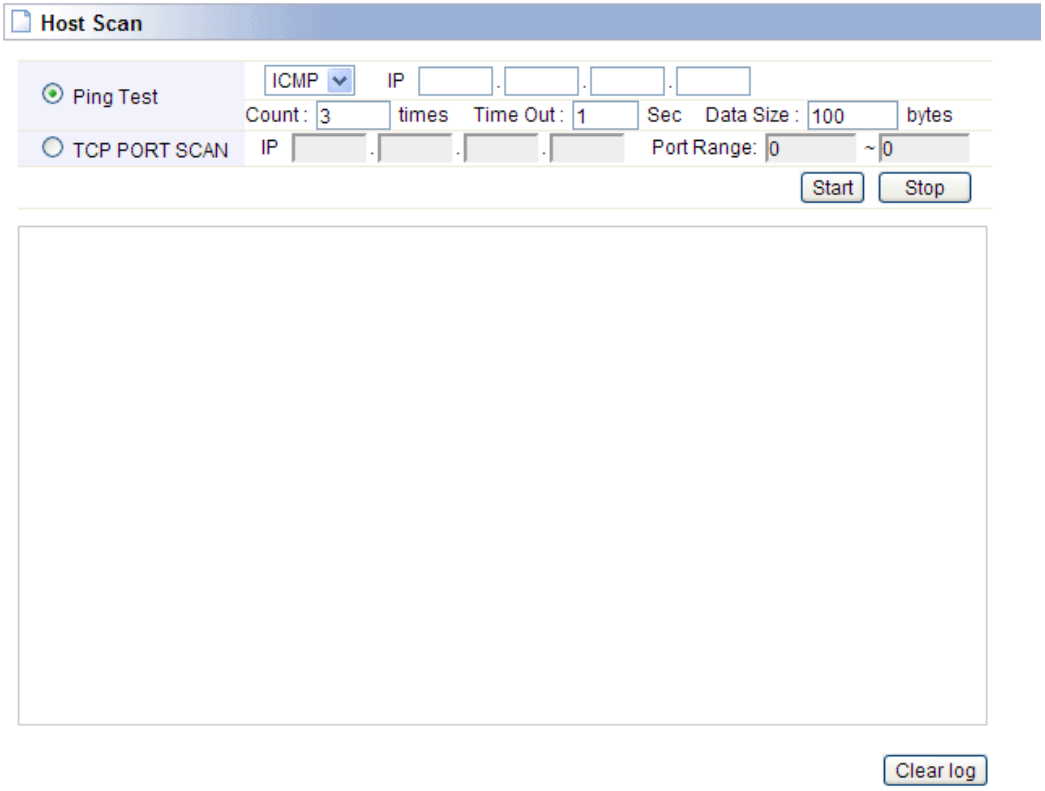
5.5.3 WOL

Users can use this Wake On Line function to start the PC remotely.



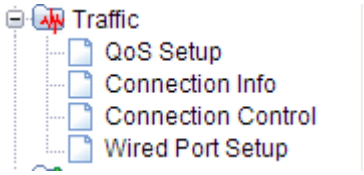
5.5.4 Host Scan

It allows user to view the working status of the PC, including status of ICMP, ARP package sending and receiving and TCP port communication information.

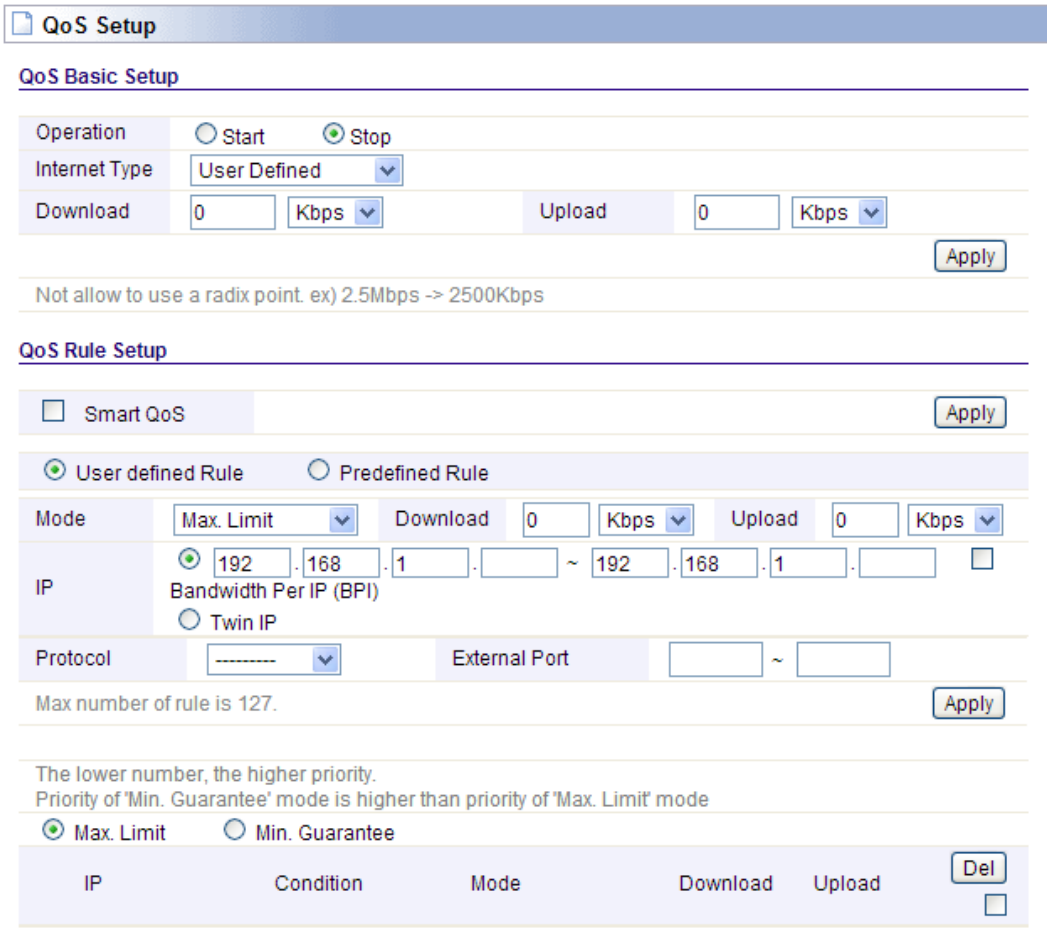


5.6 Traffic

Click the plus sign beside the Traffic menu to show up all the parameters contained, see below:



5.6.1 QoS Setup



This page is used to improve your online gaming experience by ensuring that your game traffic is prioritized over network traffic, such as FTP or Web.

Operation: You can choose to Start or Stop this function on your Router.

Internet Type: Any Internet type you want to control bandwidth.

Download/Upload: Set the bandwidth range of the Router.

QoS Rule Setup

Smart QoS: You can choose to use Smart QoS for convenient. If you select this option, you don't need to do the below settings.

Mode: You could select Max. Limit (maximum limited bandwidth) or Min. Guarantee (minimum guaranteed bandwidth).

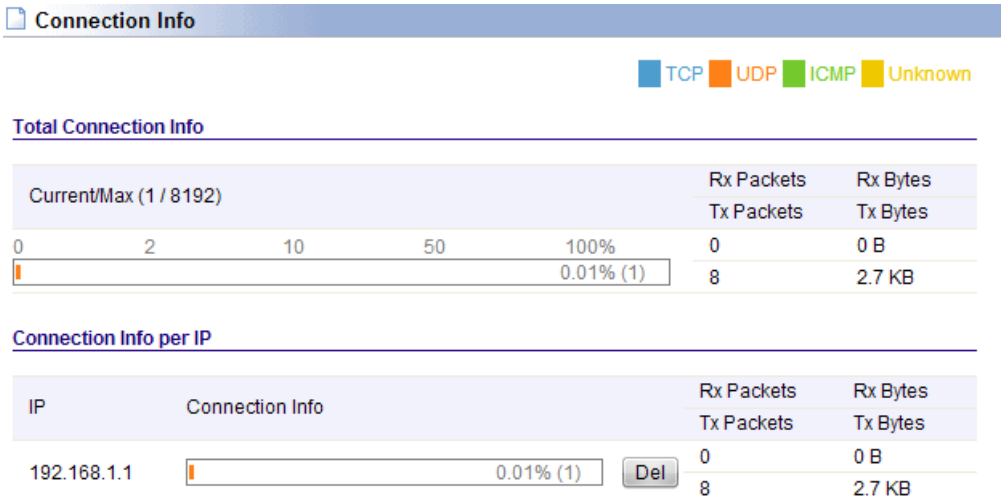
IP: You should type in the IP addresses range of PC in LAN.

Protocol: Any Protocol you want to control bandwidth.

External Port: You need to enter the range of external ports that you want to control bandwidth.

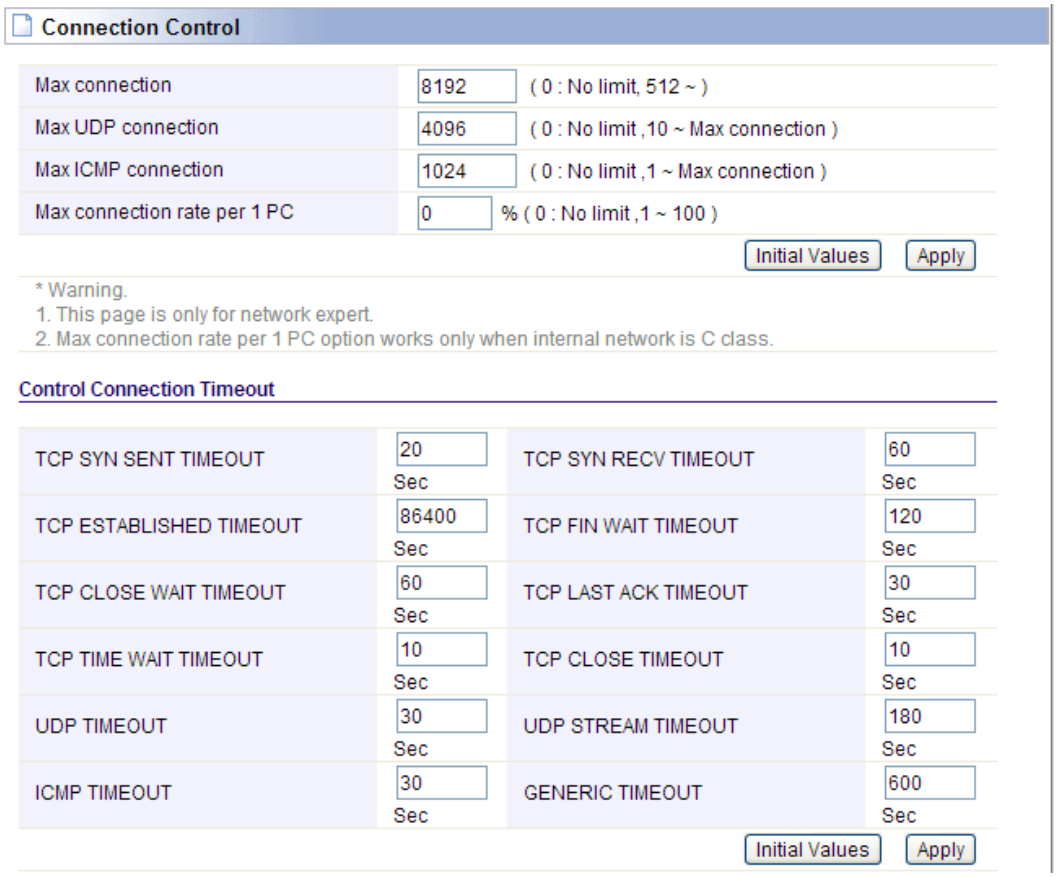
5.6.2 Connection Info

This page indicates the present connection information of the Wireless Router using graphics and data including data package sending and receiving status of each PC in connection.



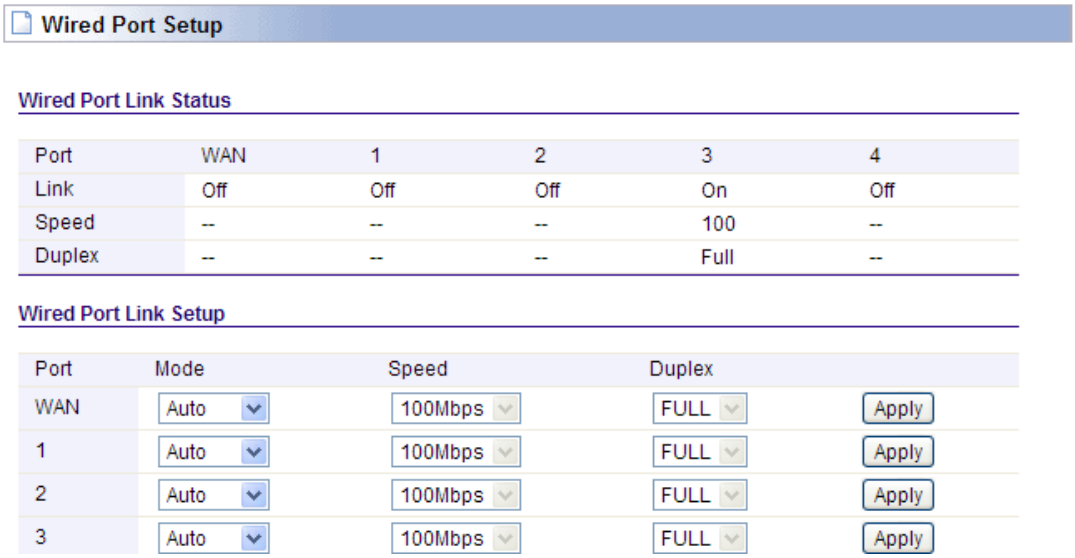
5.6.3 Connection Control

Connection Control shows the Max connection, Max UDP connection, Max ICMP connection and Max connection of each PC. These settings are only for advanced users, common users are not recommended to change them.



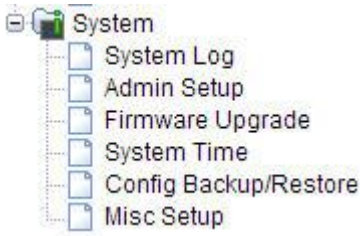
5.6.4 Wired Port Setup

This page shows the connection status of the PC connected with your router by cables.



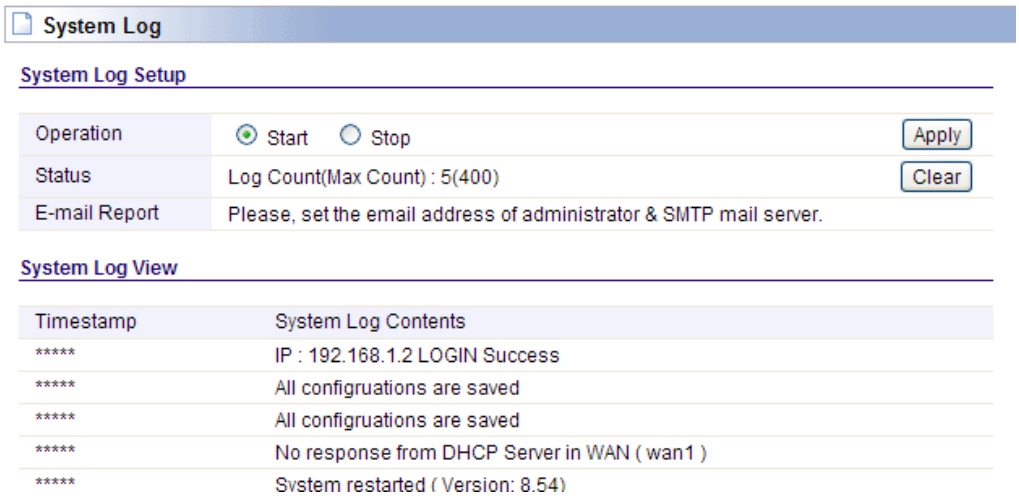
5.7 System

Click the plus sign beside the System menu to open up all the parameters contained, please see below:



5.7.1 System Log

System Log shows the working status of the wireless router, user can check the running status information here:

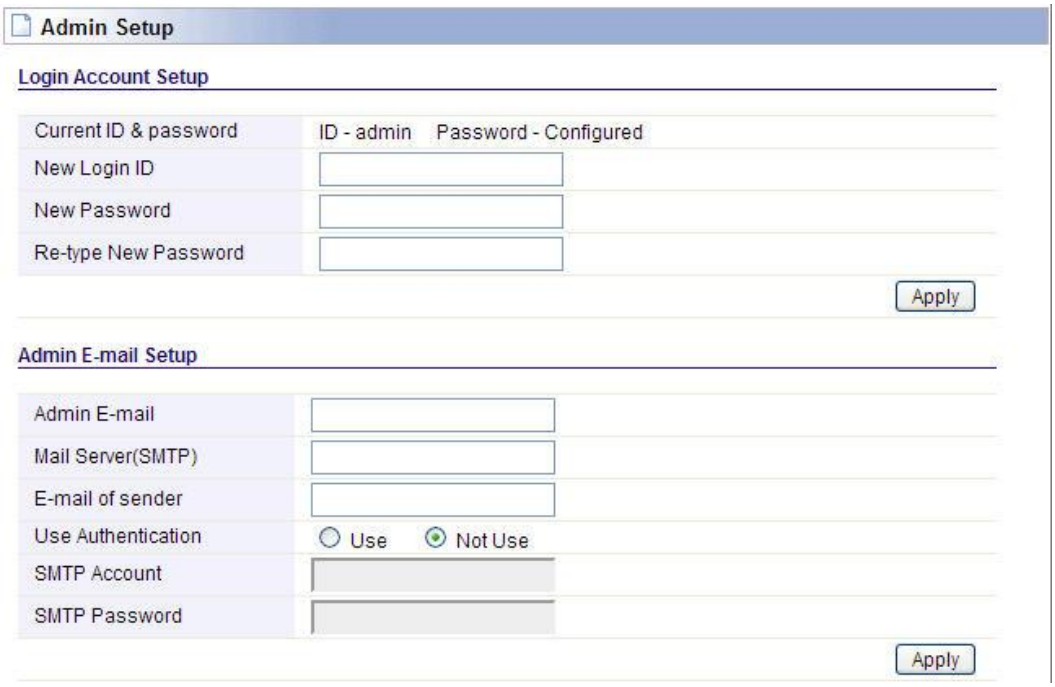


5.7.2 Admin Setup

Here you can change the login account name and password, and administrator email information.

First please input your old ID and password, then input your expected new ones. If you input your old ID and password correctly, then click **Apply** to change it.

Admin E-Mail Setup: If you want to receive IP routing log, set up Email address and SMTP server to receive it.



5.7.3 Firmware Upgrade

This page allows you to upgrade the Access Point firmware to new version. Please note: DO NOT power off the device during the upload because it may crash the system.

5.7.4 System Time

You can set the time server and time zone for your wireless Router system time.

5.7.5 Config Backup/Restore

This webpage allows you to save current settings to a file and reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

5.7.6 Misc Setup

Misc Setup provides Host name, Auto Saving, Auto Redirection, Login page setup, UPNP setup and Restart System functions.