User Manual

TOTOLINK Wireless-N Router

TOTOLINK

www.totolink.net

TABLE OF CONTENTS

1. REVISION

1.1 Revision History

Version	Amendments	Revision Date
V1.0	Preliminary Document	2013-06-05
V1.1	Modify USB Storage Part	2013-08-31
V1.2	Add Schedule in Management section	2013-11-12

2. ABOUT THIS GUIDE

Thank you very much for purchasing this TOTOLINK N300RU Wireless N Router. This guide will introduce the features of this router and tell you how to connect, use and configure the router to access Internet. Please follow the instructions in this guide to avoid affecting the Router's performance by improper operation.

2.1 Navigation of the User's Guide

Product Overview. Describes the router's function, features and appearance.

Hardware Installation. Describes the hardware installation and how to setup PC.

Connecting to Internet. Tells how you can connect your PC to Internet successfully using the router.

Advanced Settings. Lists all technical functions including Network, Wireless, QoS, Firewall, USB and Management.

3. PRODUCT OVERVIEW

3.1 Introduction

N300RU is a Wireless Router with three high gain antennas and one USB2.0 port. It offers five methods to access Internet DHCP/PPPoE/Static IP/L2TP/PPTP and can deliver up to 300Mbps wireless data rate. Besides, N300RU can be used as repeater and wireless AP. So it is a high performance and cost-effective solution for home and small offices.

3.2 Features

- Complies with IEEE 802.11n/g/b standards for 2.4GHz Wireless LAN.
- Three high gain antennas enhance the wireless robustness and stability.
- Supports PPPoE, DHCP, Static IP, L2TP and PPTP broadband functions.
- Provides 64/128-bit WEP and WPA-PSK/WPA2-PSK encryptions.
- Supports IP/Port, MAC, URL filtering and Port Forwarding.
- Connects to secure network easily and fast using WPS.
- Supports three bridge modes: Repeater Bridge, Repeater WAN and WDS.
- QoS makes the bandwidth control more easily.
- Multi-SSID allows user to create multiple LANs.
- Supports IPsec, L2TP and PPTP VPN Pass-Through.
- Supports remote/local web management.
- USB2.0 port for FTP Server and Printer Server.
- Easy setup simplifies the basic settings of the router.

3.3 Panel Layout

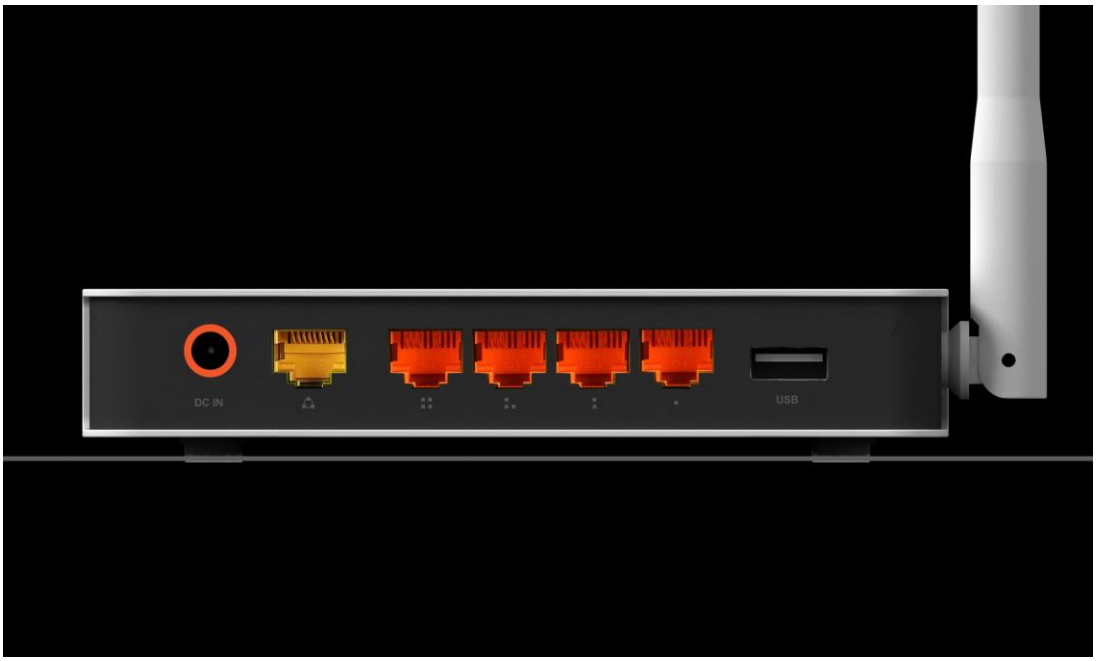
3.3.1 Front Panel

The front panel of N300RU consists of 9 LEDs, which is designed to indicate connection status.

POWER	This indicator keeps solid blue when the hub is receiving power, otherwise it is off.
CPU	This indicator keeps lighting blue when Router powered on.
USB	This indicator keeps solid blue while the USB port working.
WLAN	This indicator lights blue when the wireless function is working.
WAN	When the WAN port is connected to Internet the indicator lights blue.
	During transmitting or receiving data through the WAN port the indicator blinks blue.
1/2/3/4 LAN	When one of the LAN ports has a successful connection, the corresponding indicator lights blue.
	During transmitting or receiving data through the LAN port the indicator blinks blue.

3.3.2 Rear Panel

The figure below shows the rear panel of N300RU.

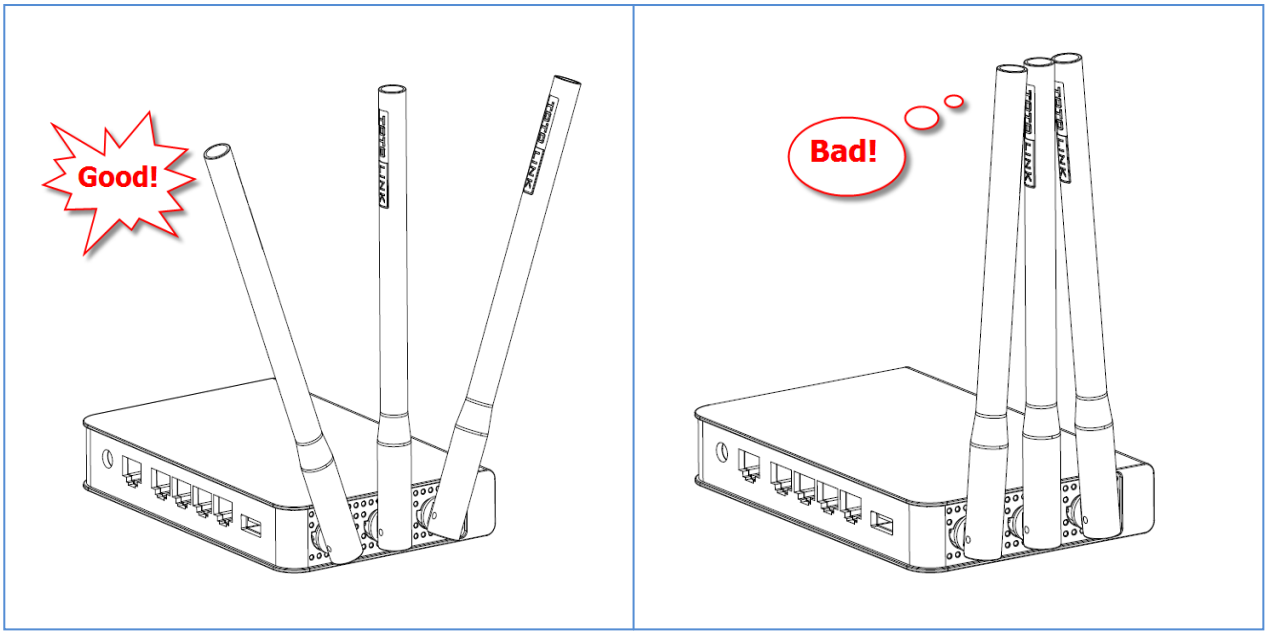


DC IN	The Power socket is used to connect power adapter.
WPS/RST	**RST:** With the router powered on, press and hold the button for about 10 seconds, the router will reboot to factory default settings.
	WPS: If you have client devices you can press this button to quickly establish secured connections between this router and client devices.
USB	This USB2.0 port is used to connect with USB devices.
WAN	This port is used to connect DSL/cable Modem, or Ethernet.
1/2/3/4 LAN	These ports connect to local PCs.

Note: *Press and hold the WPS/RST button for about 5 seconds, it is WPS working which will last for 2 minutes. For about 10 seconds, the router will reboot to default factory settings.*

3.3.3 Antenna Placement

To avoid signal interference and optimize antenna's performance, you should place the antennas at an angle against the horizontal line and let antennas not be too close to each others. We recommend you orient the antennas as the following illustration shows:



4. HARDWARE INSTALLATION

4.1 Hardware Installation

For those PCs you wish to access Internet by this router, each of them must be properly connected through UTP cables.

1. Connect your PC's LAN port to one of the router's LAN port using UTP cable.
2. Connect existing Internet cable (such as ADSL or Modem) to router's WAN port using another UTP cable.
3. Plug the Power Adapter into the router and then into an outlet.
4. Turn on your computer.
5. Check and confirm that the Power LED and LAN LED on the router are **ON**.

4.2 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 blinks 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.

4.3 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.

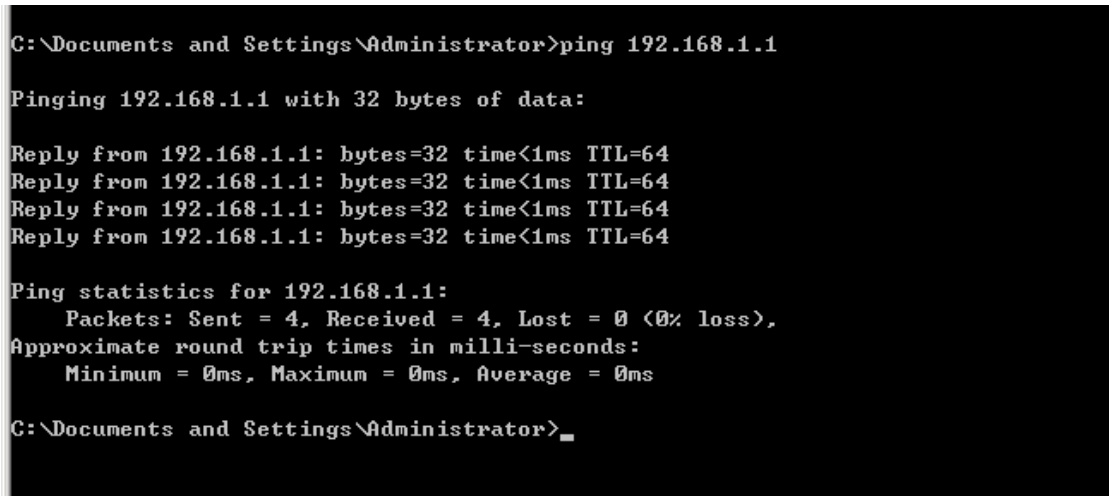
- **Configure the IP address manually**

1. Right-click **My Network Places—Properties**, then right-click **Local Area Connection—Properties**, double click **TCP/IP Protocol**.
2. Configure the network parameters manually. Set the IP address to 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).

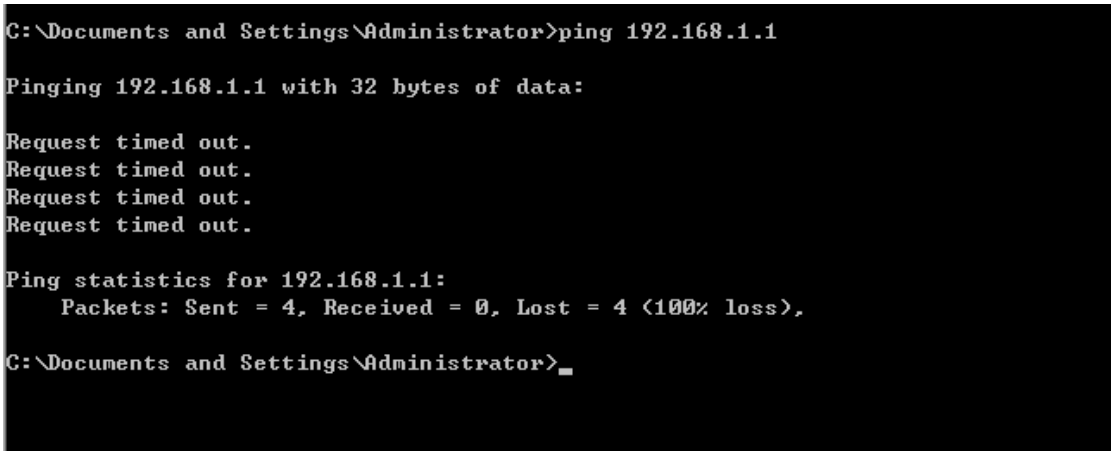
- **Obtain an IP address automatically**

Set up the TCP/IP Protocol to **Obtain an IP address automatically** mode on your 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.

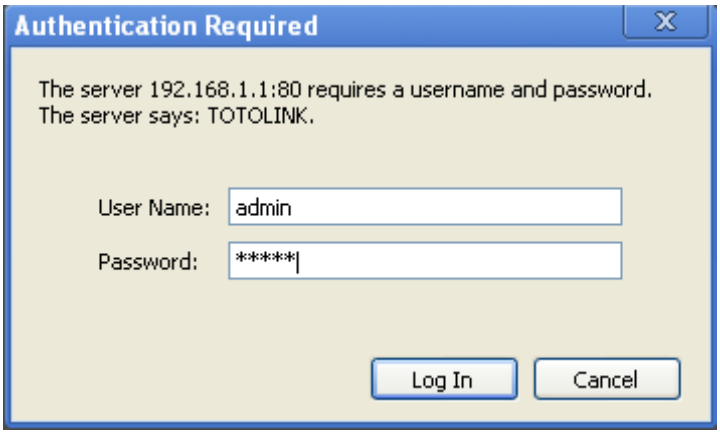
5. CONNECTING TO INTERNET

This chapter introduces how to configure the basic functions of your router to access Internet.

5.1 Accessing Web page

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 that requires you to enter valid User Name and Password:

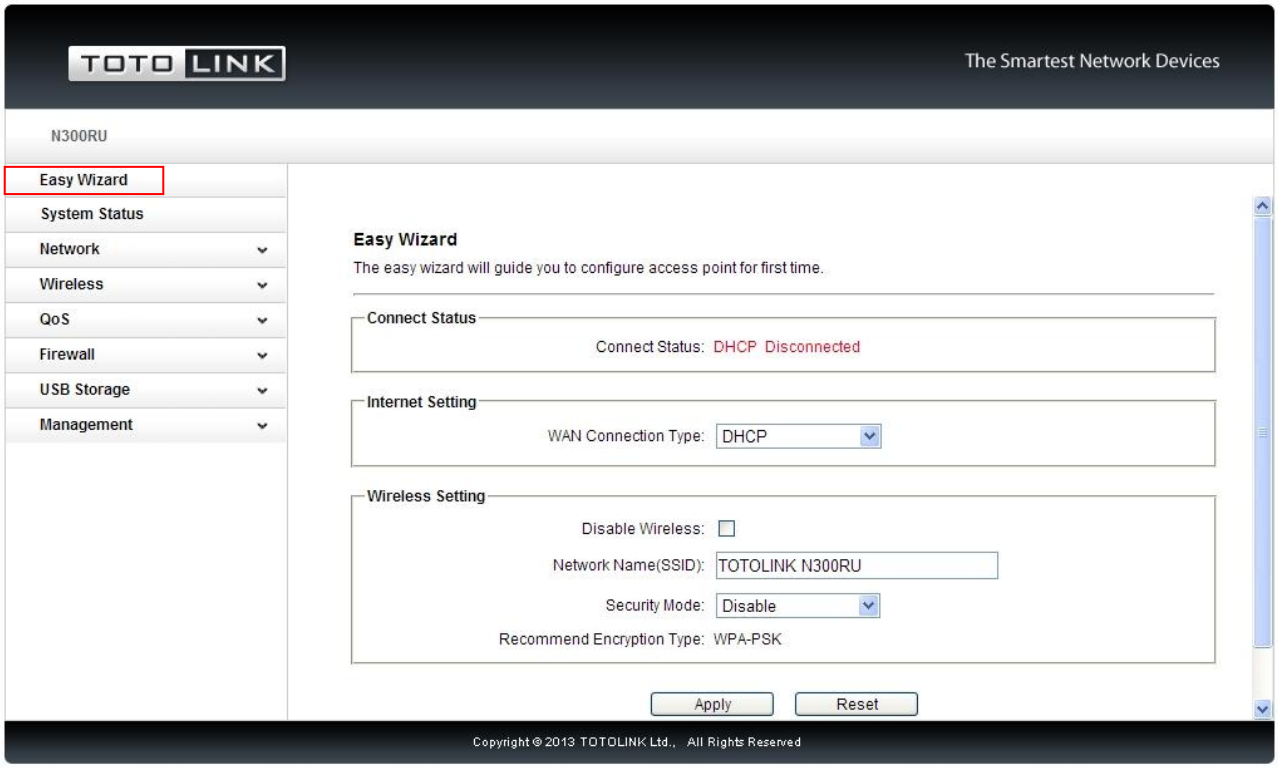


Enter **admin** for User Name and Password, both in lower case letters. Then click **Log In** button or press **Enter** key.

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.*

5.2 Easy Wizard

Now please click **Easy Wizard** on the left menu bar to quickly setup the router to access Internet. In this section, you should only enter some basic parameters about Internet setting and Wireless setting. It is ease of use that even users with less knowledge can finish the settings for network experience.

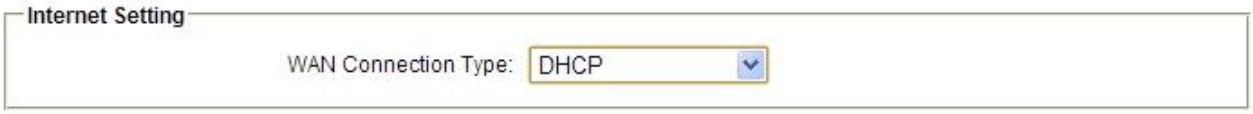


5.2.1 Internet Setting

Here you can choose one WAN connection type from the following three options.

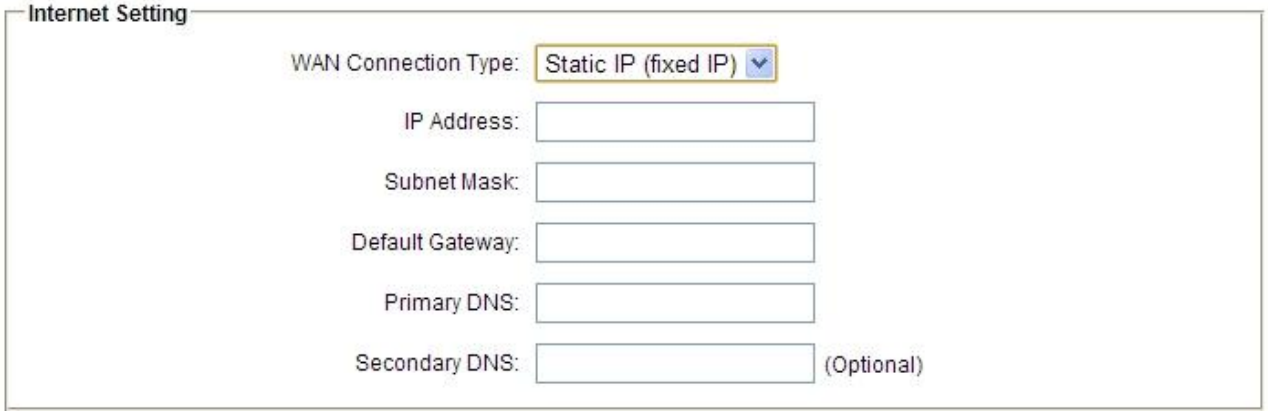
5.2.1.1 DHCP

Dynamic Host Configuration Protocol (DHCP) is a local area network protocol. If you choose this mode, you will get a dynamic IP address from your ISP automatically.



5.2.1.2 Static IP

If your ISP has provided a fixed IP that allows you to access Internet, please choose this option.



IP Address: the IP address provided by your ISP.

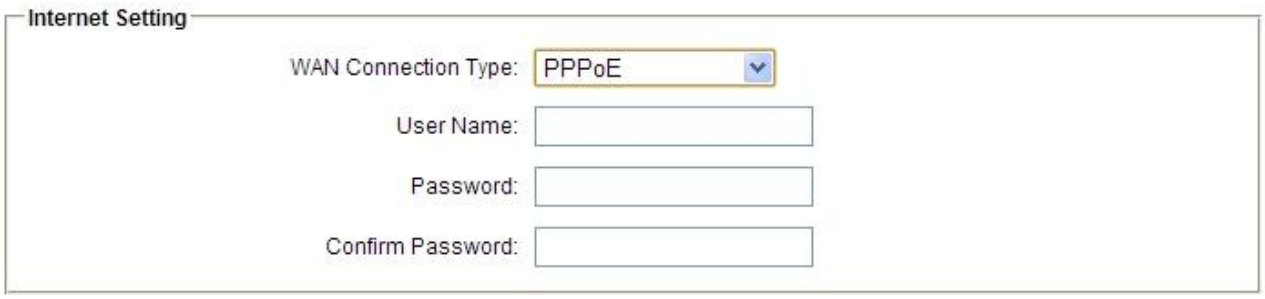
Subnet Mask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical net mask value for Class C networks. Generally it is provided by your ISP.

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. It is provided by your ISP.

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. Here you can set the Primary and Secondary DNS addresses. This is provided by your ISP.

5.2.1.3 PPPoE

If you use ADSL virtual dial-up to connect Internet, please choose this option.



User Name: a specific valid ADSL user name provided by your ISP.
Password: the corresponding valid password provided by your ISP.
Confirm Password: please enter the password one more time for confirmation.

Knowledge Extension: *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.*

5.2.2 Wireless Setting

After the Internet Setting, you can also configure the Wireless parameters.

Disable Wireless: you can choose to disable the wireless function by checking this box.
Network Name (SSID): Service Set Identifier is used to identify your 802.11 wireless LAN. By default, it is TOTOLINK N300RU.
Security Mode: Here you can choose to set no encryption or select WEP, WPA-PSK, WPA2-PSK or WPA/WPA2-PSK**.** Here we recommend you choose WPA/WPA2-PSK, and you need to set the Key (encryption key) for this wireless LAN. See below:

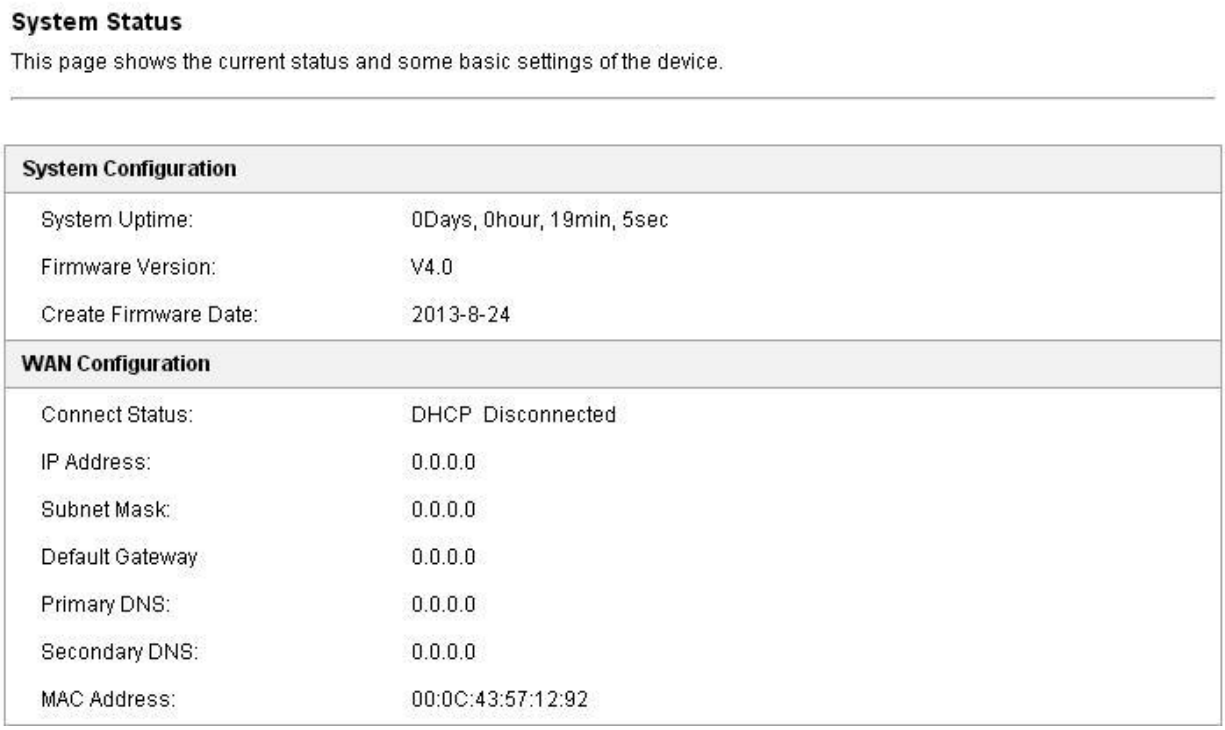
After this setting, please Click **Apply** to save the settings. Basically, you can access Internet by wired/wireless method now. If by wireless, please plug out the cable connected with your PC and the router. Enable the Wireless connection on your computer, search for the SSID you have set (here is TOTOLINK N300RU) and connect to it. If you have set encryption Key, please type in the same Key to surf Internet.

6. ADVANCED SETTINGS

This chapter allows users to configure advanced settings includes Network, Wireless, QoS, Firewall, USB and Management. Most of 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.

6.1 System Status

The System Status provides basic network settings of this router, including LAN, WAN and Wireless configuration. Also, you could get the current running firmware version or firmware related information from this presentation.



System Status

This page shows the current status and some basic settings of the device.

System Configuration	
System Uptime:	0Days, 0hour, 19min, 5sec
Firmware Version:	V4.0
Create Firmware Date:	2013-8-24
WAN Configuration	
Connect Status:	DHCP Disconnected
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0
MAC Address:	00:0C:43:57:12:92

System

System Uptime: show how long the system has run.

Firmware Version: display the current firmware version of the router.

Create Firmware Date: the date when the firmware built.

WAN Configuration

Connect Status: display the current WAN connection status.

IP Address: show the IP address of the WAN interface.

Subnet Mask: display the subnet mask of the WAN interface.

Default Gateway: display the assigned IP address of the default gateway.

Primary DNS: display the Primary DNS of the router

Secondary DNS: display the Secondary DNS of the router.

MAC Address: display the MAC address of the WAN interface.

Wireless Configuration	
Wireless Status:	WiFi OFF
SSID:	TOTOLINK N300RU
BSSID:	00:0C:43:57:12:90
Channel:	11
Network Mode:	2.4GHz (B+G+N)
Security Mode:	None
LAN Configuration	
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable
MAC Address:	00:0C:43:57:12:90

Wireless Interface Configuration

Wireless Status: shows the current wireless status.

SSID: the name of your wireless network, it is case-sensitive.

BSSID: Basic SSID.

Channel: the current Channel Number.

Network Mode: the radio's standard for operation of the router.

Security Mode: the encryption method of this router.

LAN Interface Configuration

IP Address: display the IP address of the LAN interface.

Subnet Mask: show the subnet mask address of the LAN interface.

DHCP Server: display the current status of DHCP server of the LAN interface.

MAC Address: show the MAC address of the LAN interface.

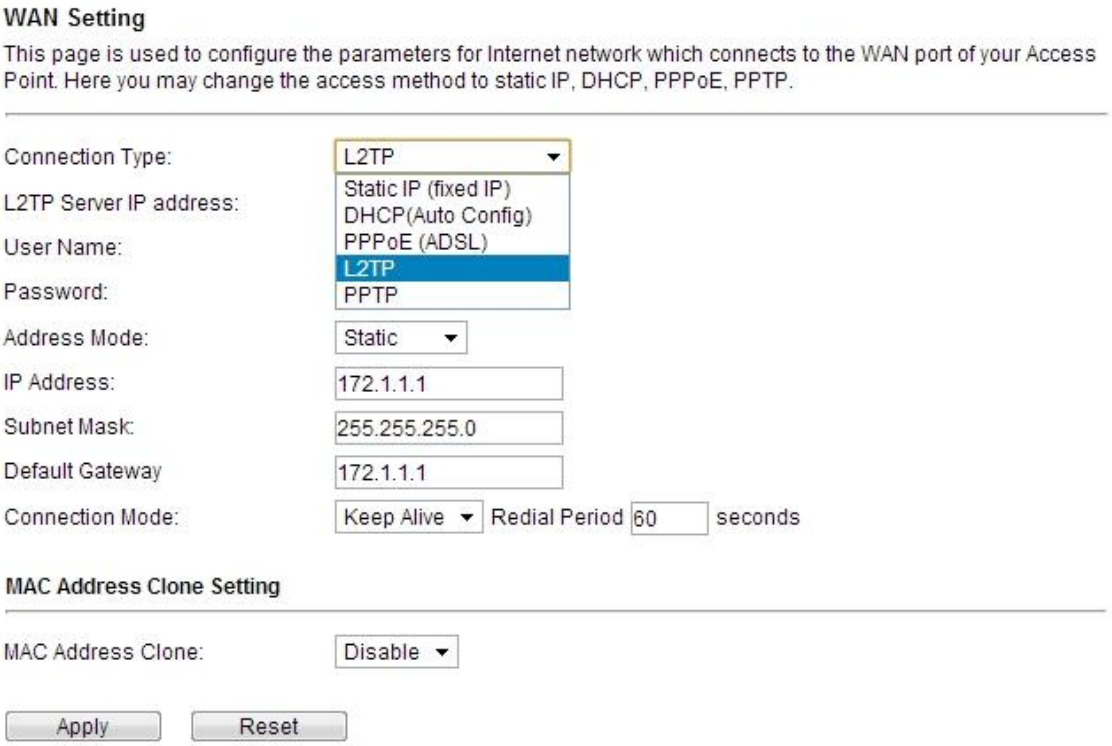
6.2 Network

This item contains settings for WAN Settings, LAN Settings, IP/MAC Banding Settings and Routing Table. Only if you set these parameters correctly, you can make sure PCs in your LAN can access Internet. Please follow the below instructions to configure.

6.2.1 WAN Setting (PPTP/L2TP)

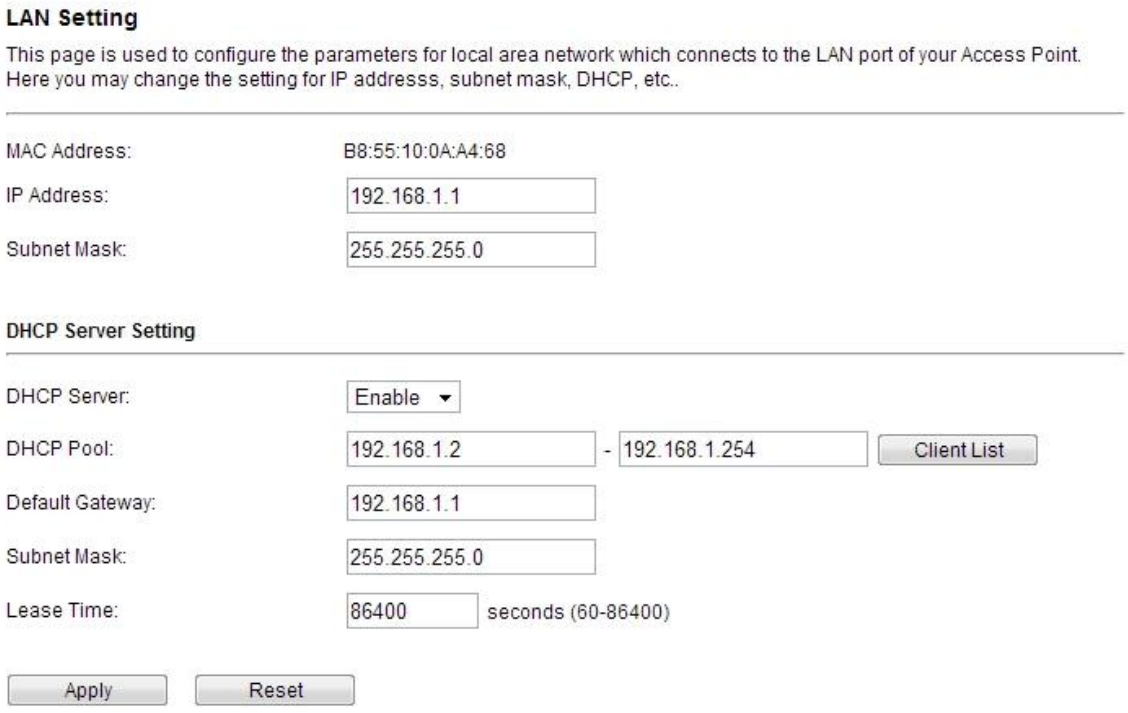
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. For PPTP and L2TP connection, your ISP must provide

below information to you.



6.2.2 LAN Setting

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP. This page allows you to configure the parameters for LAN which connects to the LAN port of your Access Point.



MAC Address: the physical address of the router.

IP Address: this is the IP address to be represented by the LAN (including WLAN) interface that is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network).

> ***Note:*** *If this IP address changed, you can log into the WEB configuration interface only using the new IP address. AND if the new IP address and the original IP address are not in the same segment, the Virtual Server and DMZ Host service will not work. If you need to enable these functions, you will have to reset this IP address.*

Subnet Mask: this is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks which support IP address range from 192.0.0.x to 223.255.255.x. Class C network netmask uses 24 bits to identify the network and 8 bits to identify the host.

DHCP Server: you can disable/enable this function. If you enable DHCP server, all the computers connected to this router will get the IP address dynamically.

DHCP Pool: the range of IP addresses that will be assigned to each PC connected with the router.

Default Gateway: this is the IP address of 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.

6.2.3 Static DHCP Setting

This page 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.

Static DHCP: you can choose to enable or disable this function from the drop-down list.

MAC Address: choose the MAC address that you want to bind.

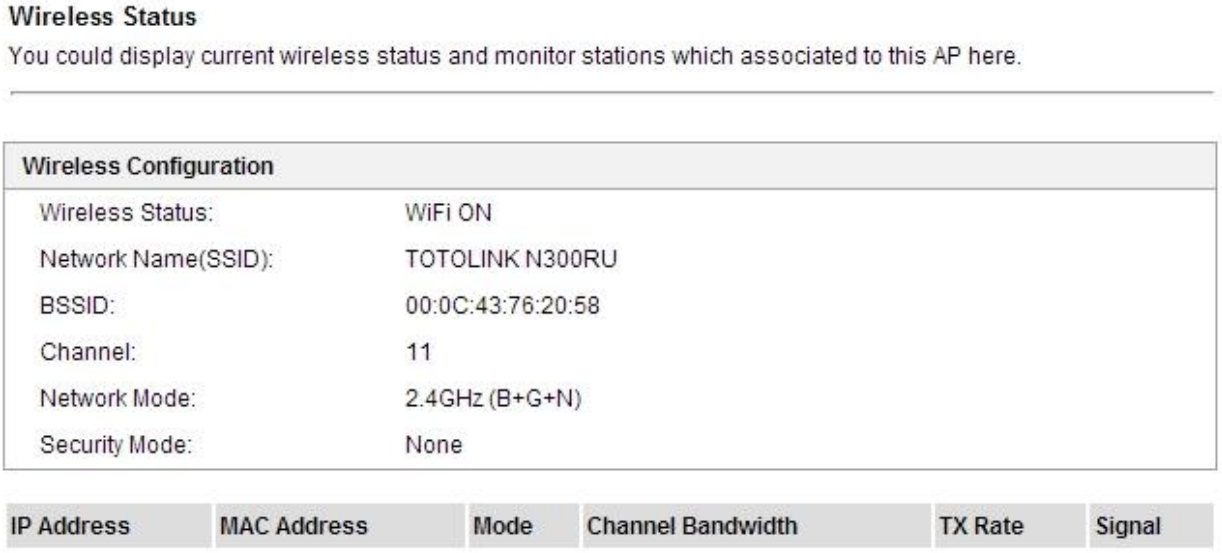
IP Address: shows the IP address of selected MAC address.

6.3 Wireless

The general wireless settings, such as 802.11 modes, SSID and data rates can be configured in this section. Also some more advanced settings can be setup here.

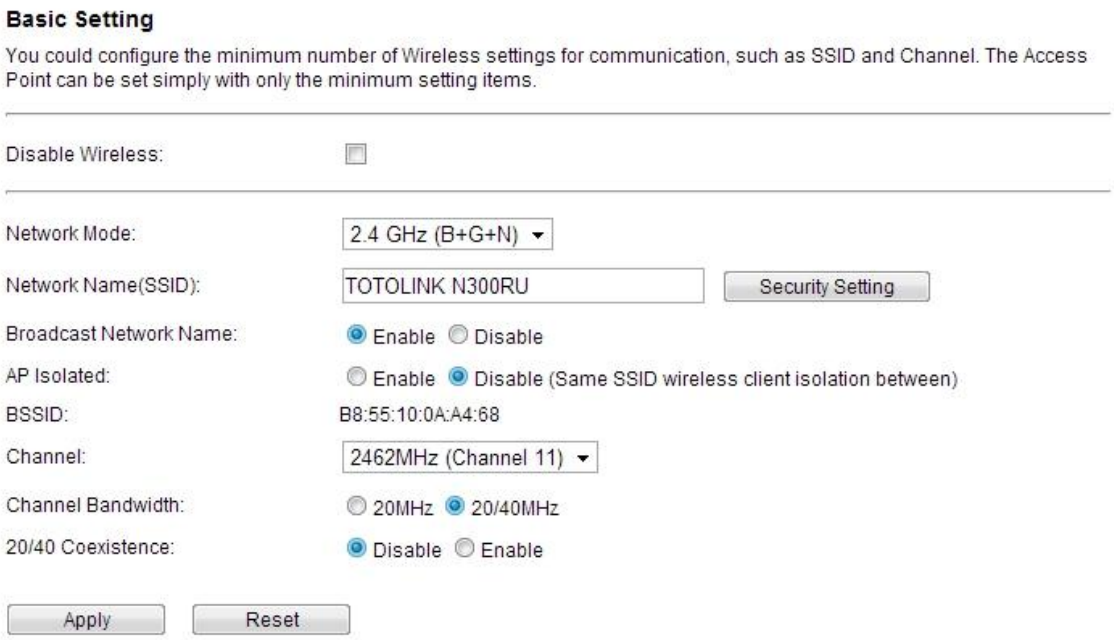
6.3.1 Wireless Status

This page displays the current Wireless Interface configuration of the router.



6.3.2 Basic Setting

On this page, you could configure the parameters for Wireless LAN clients that may connect to your Access Point.

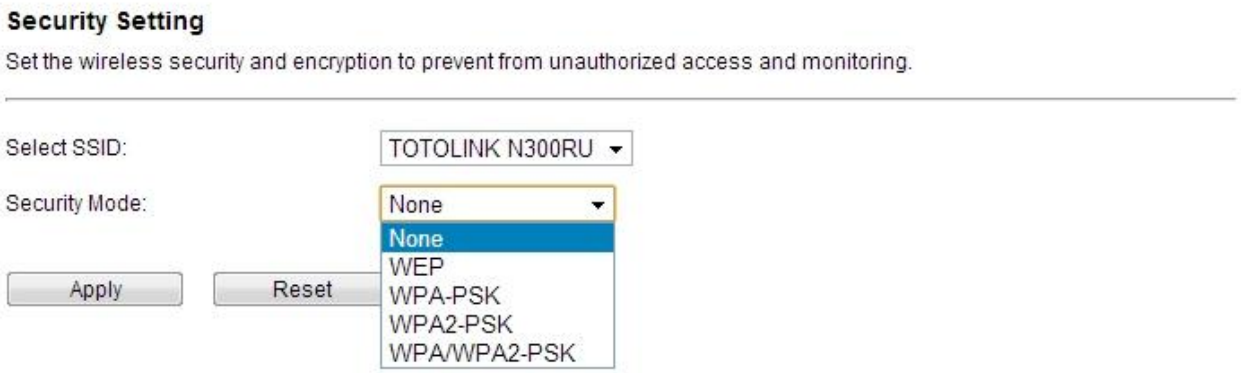


Disable Wireless: you can check this box to disable wireless function.

Network Mode: in fact, this option allows you to choose the radio standard for operation of your Router. 802.11b and 802.11g are old 2.4GHz mode, while 802.11n (2.4GHz and/or 5GHz) is the latest standard based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. Here, you can choose the last one 2.4GHz (B+G+N), this mode offers better compatibility.

Network Name (SSID): service Set Identification means the name of your wireless LAN. All the client devices within the range will receive broadcast messages from the access point advertising this SSID. You can set it by yourself and it is case-sensitive.

Security Setting



6.3.2.1 WEP

WEP (Wired Equivalent Privacy) 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.

6.3.2.2 WPA/WPA2-PSK (Recommended)

Wi-Fi Protected Access (WPA) 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. Please set one Encryption key (password) for your wireless network to prevent being occupied by others.

Broadcast Network Name: enable this function allows others to search for this router's SSID.

AP Isolated: by default, it is disabled.

Multiple AP Isolated: by default, it is disabled.

BSSID: basic SSID.

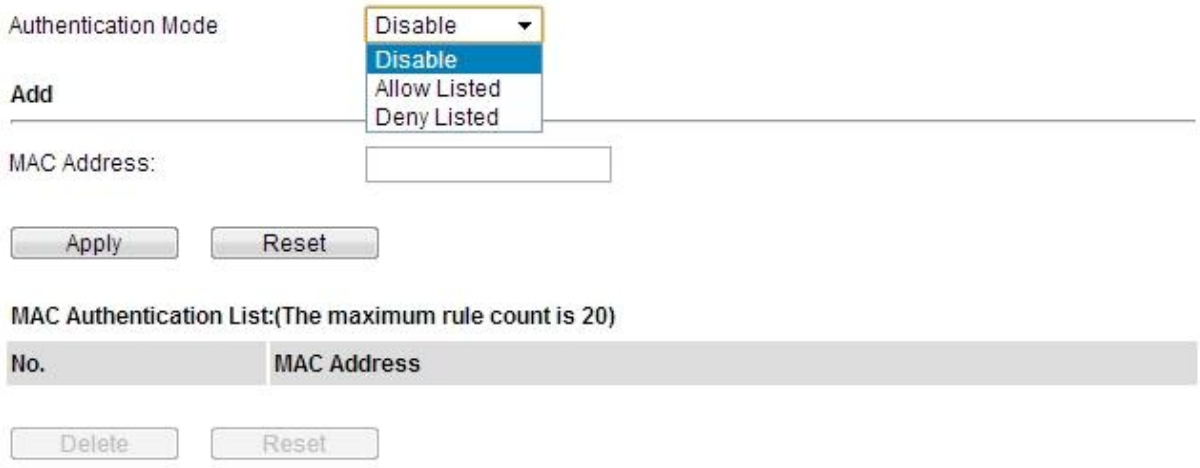
Channel: this option provides selectable channel numbers. The default value is channel 11.

Channel Bandwidth: 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.

6.3.3 MAC Authentication

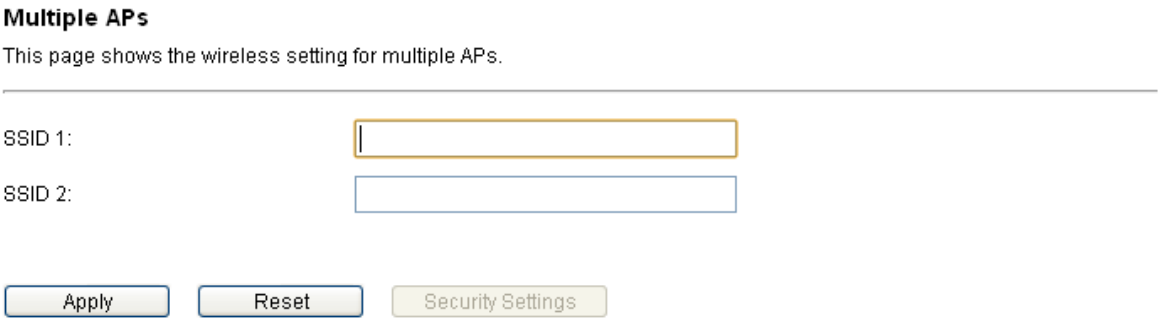


Authentication Mode: you can select to allow or deny the listed MAC address to connect to your router.

MAC Address: enter the MAC address.

6.3.4 Multiple APs

This router allows you to set other two SSIDs. You can set two different SSID with different encryptions for different clients or friends. After enter the network name, you can click Security Settings button to setup encryption for the security of your network. The security settings please refer to previous instruction.



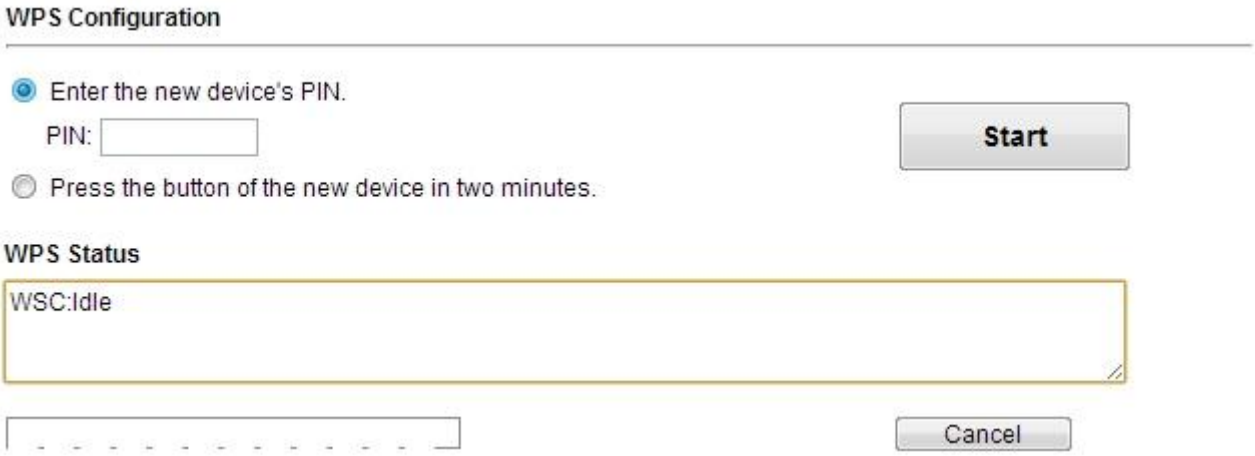
6.3.5 WPS

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.

WPS Mode: you can choose to enable/disable this function

WPS Current Status: Display related system information for WPS.

WPS Configuration



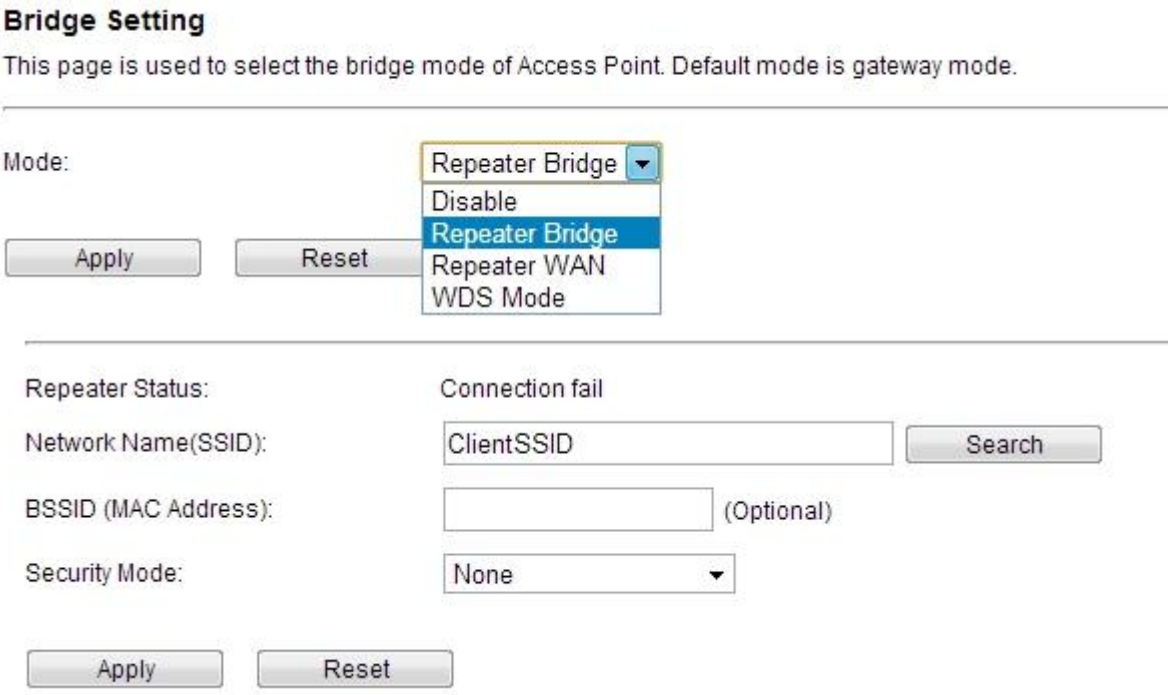
PIN: please input the PIN code specified in wireless client you wish to connect, and click **Start** button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

6.3.6 Bridge Setting

You can choose from **Repeater Bridge, Repeater WAN** and **WDS**.

6.3.6.1 Repeater Bridge

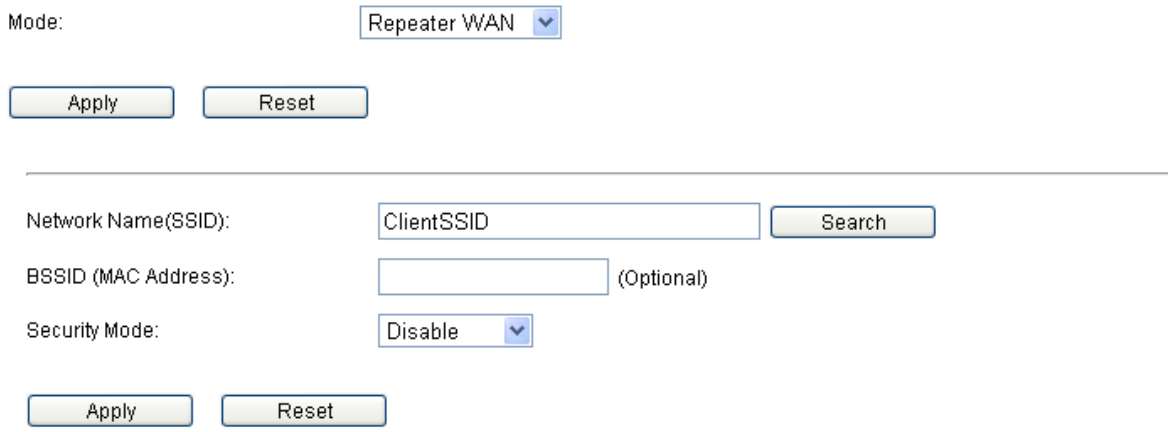
In this mode, the router is used as an AP to get other router's signal. Please search for SSID and choose one that you want this router to connect.



6.3.6.2 Repeater WAN

This mode offers the same function as Repeater Bridge, but the only setting difference is that Repeater WAN need not to stop DHCP Server. You can click **Search** to choose one

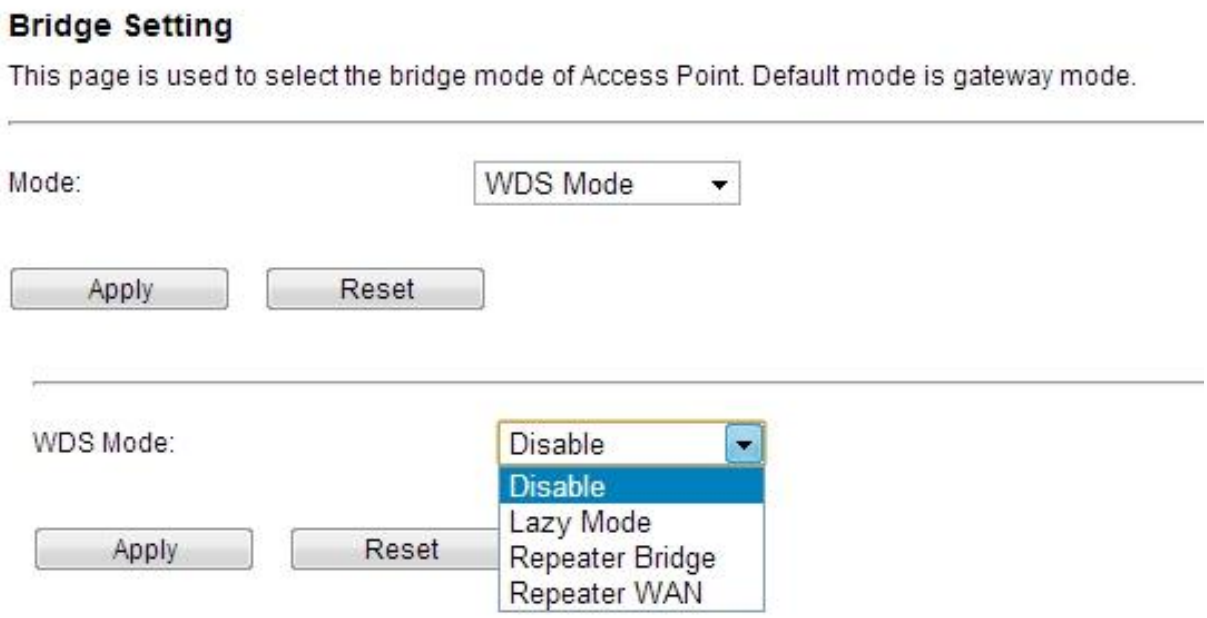
SSID to connect, then the PCs in your LAN will get IP address from the selected SSID.



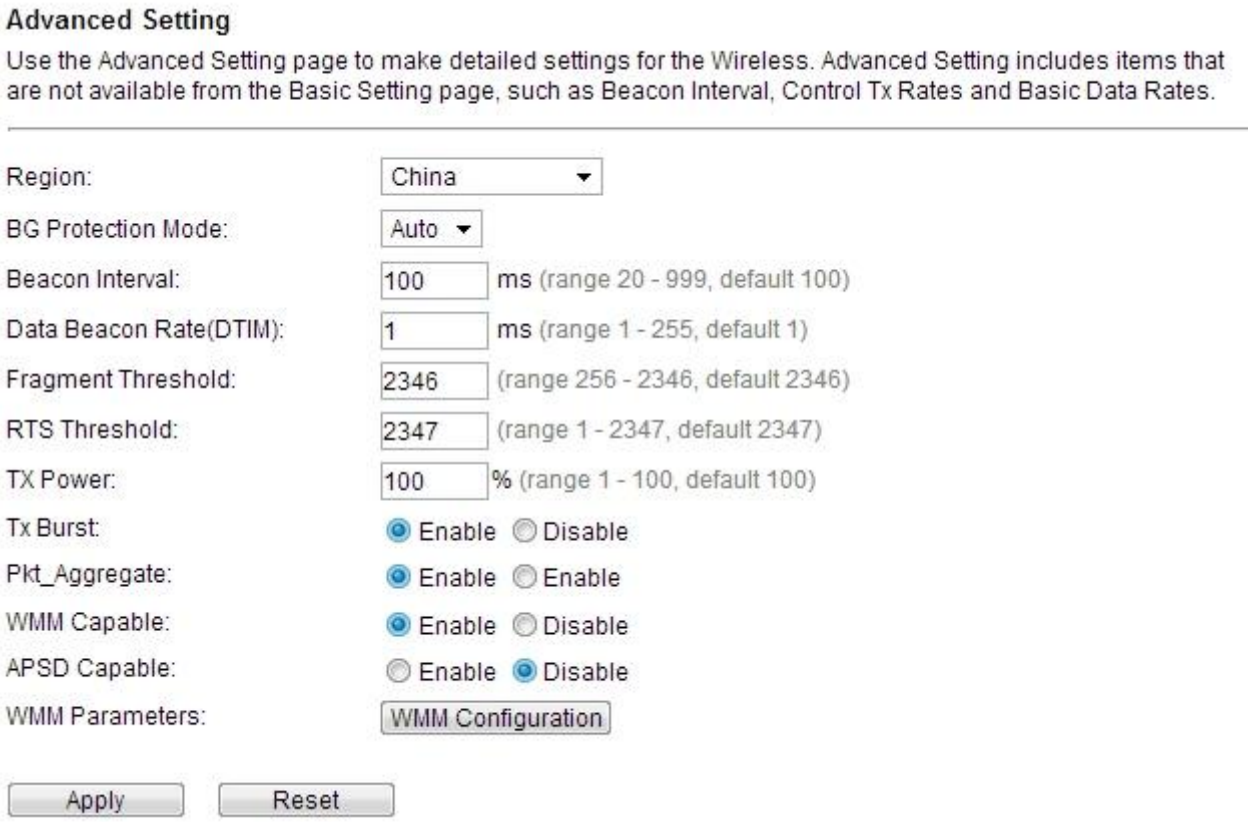
Note: *Both these two repeater methods can help you to expand the wireless coverage and allow more terminals to access Internet. But since Repeater WAN need not stop DHCP Server, all PCs' IP Addresses are assigned by the Secondary Router itself. So this method allows more PCs to access Internet than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

6.3.6.3 WDS Mode

Wireless Distribution System means connecting multiple wireless networks to one. It will use two or more wireless bandwidth Router/AP connecting with each other to expand wireless signal to longer distance. This mode is suitable for medium-size networks like school and enterprise network.



6.3.7 Advanced Setting



Region: Please choose your country.

BG Protection Mode: The default value is Auto. Just keep the value.

Beacon Interval: 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.

Data Beacon Rate: The default value is 1ms, this must be in range of 1~255.

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.

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.

TX Power: Please just keep the default.

Tx Burst: Please just keep the default.

Pkt_Aggregate: A part of the 802.11n standard. It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header. It is enabled by default.

Frames—determine the number of frames combined on the new larger frame.

Bytes—determine the size (in Bytes) of the larger frame.

WMM Capable: 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.

APSD Capable: It is disabled by default.

WMM Parameters: Click WMM Configuration to configure the parameters of this function.

6.4 QoS

Quality of Service can be also called QoS simply. Deploying QoS management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network. Since numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, we need QoS to control the bandwidth use. On this page, you could set the QoS rules.

QoS: you can choose to enable this function or not.

Total Uplink Speed: you can set the uplink speed for all LAN PCs.

Total Downlink Speed: you can set the downlink speed for all LAN PCs.

IP Address: if you choose IP address, please enter the IP address range.

Uplink Bandwidth: type in the uplink bandwidth.

Downlink Bandwidth: type in the downlink bandwidth.

Comment: describe the reason. Just few words are saved there usually.

Current QoS List: shows the detailed QoS rules you have set.

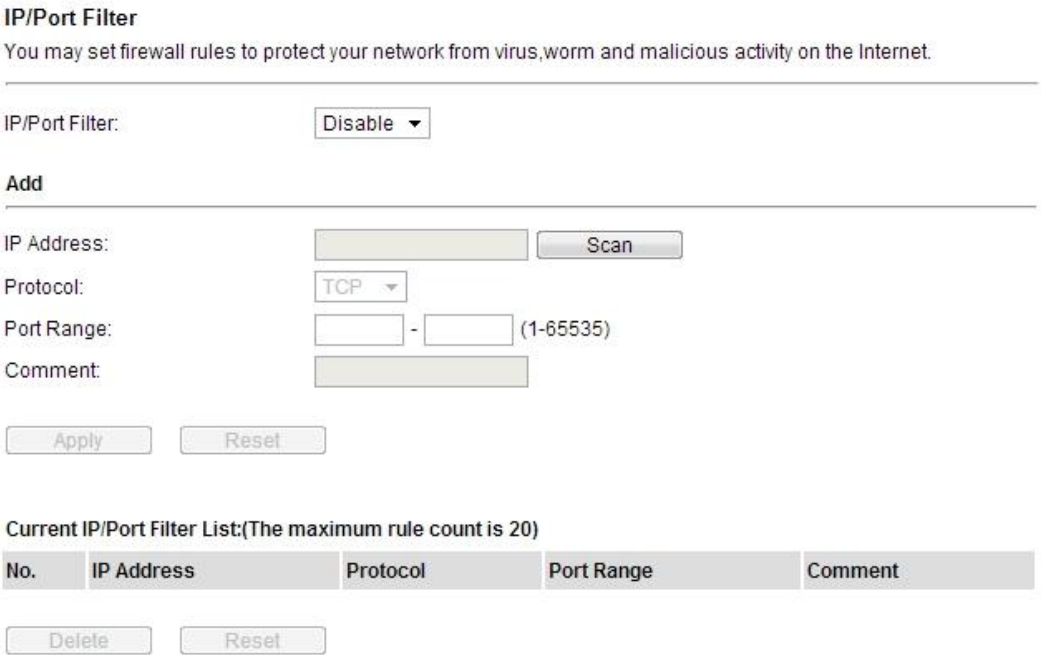
6.5 Firewall

While the broadband users require more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of this router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

6.5.1 System Firewall

On this page, you can disable of enable below firewall options.

6.5.2 IP/Port Filtering



IP/Port Filter: you can choose to disable/enable this function.

IP Address: enter the IP address that you want to filter.

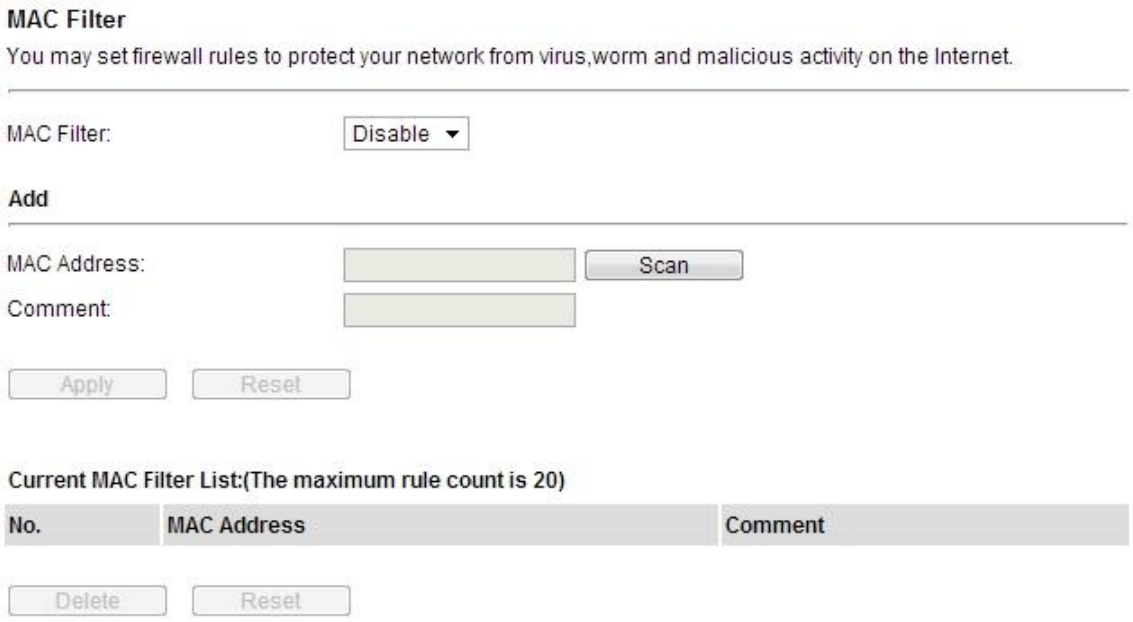
Protocol: specify the protocol which this filter rule will apply to.

Port Range: enter the Port range that you want to filter.

Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.

Current Filter Table: this table will list the detailed information about the IP and Ports that you do/don't allow to access your router.

6.5.3 MAC Filtering



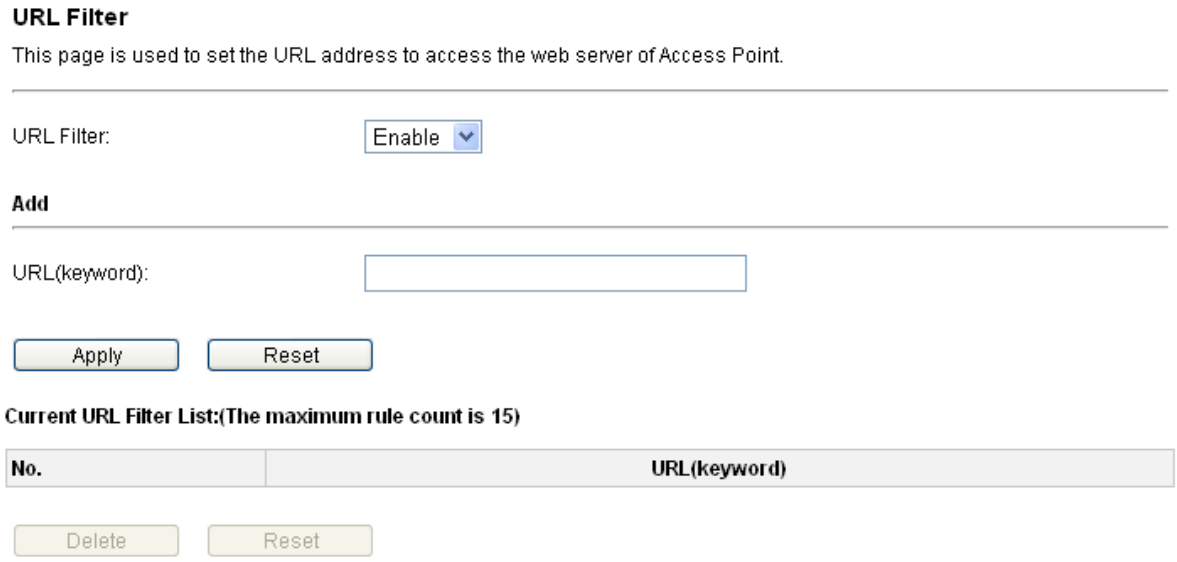
MAC Filter: you can choose to disable/enable this function.

MAC Address: enter the MAC address that you want to filter.

Comment: describe the reason why you want to filter these ports. Just few words are saved there usually.

6.5.4 URL Filtering

This page is used to deny LAN users from accessing certain sites. Block those URLs which contain keywords listed.



URL Filter: you can choose to enable or disable this function. If you enable URL filter, please provide URL keyword.

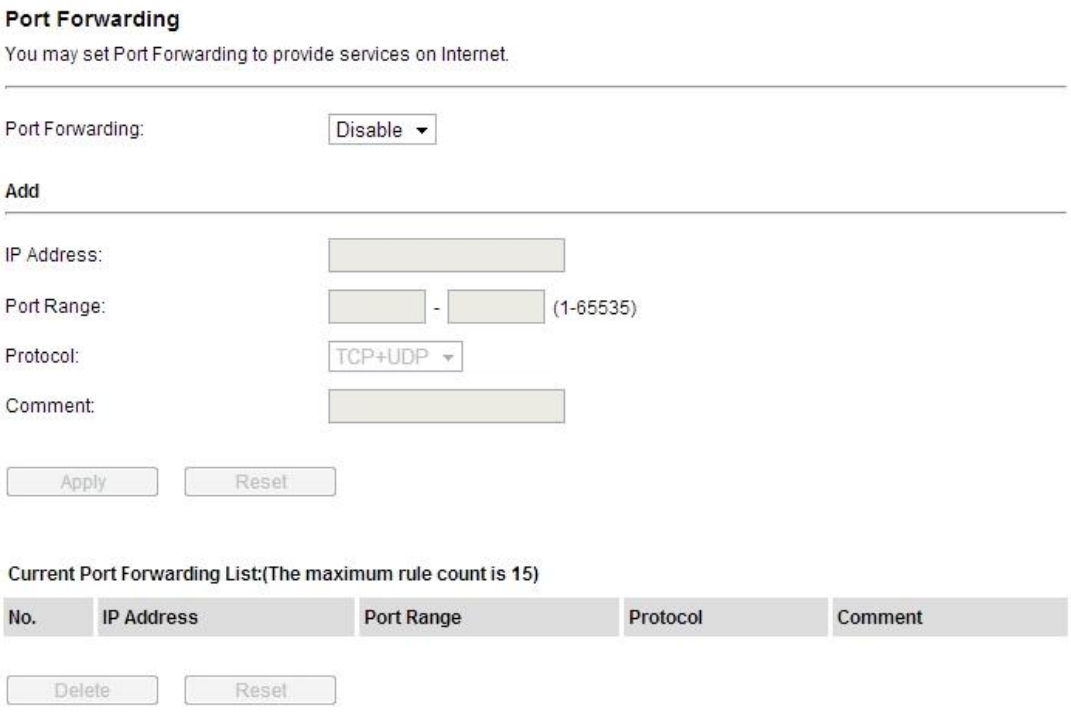
URL(keyword): enter the URLs that you don't allow LAN users to access by this router.

6.5.5 UPnP Setting

The UPnP (Universal Plug and play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows “Plug and Play” system. You can enable this function so that the router doesn’t need to work out which port need to be opened.

6.5.6 Port Forwarding

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway’s NAT firewall.



Port Forwarding: you can choose to enable or disable this function.

IP Address: enter the IP address that you want to forward.

Port Range: enter the port range that you want to forward.

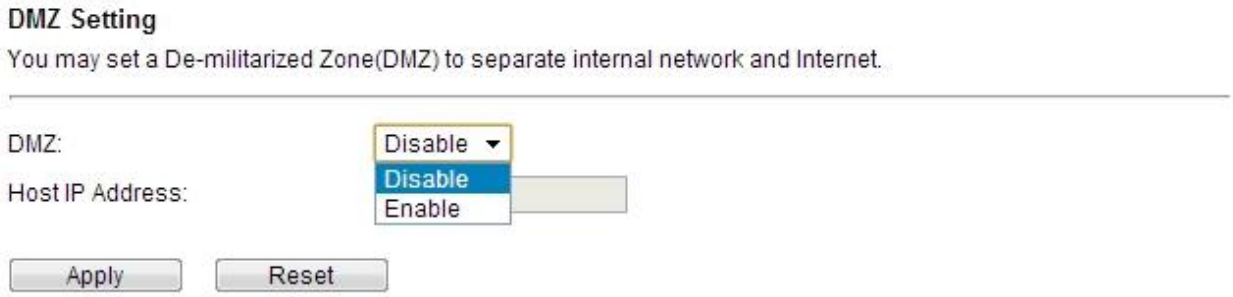
Protocol: specify the protocol which this filter rule will apply to.

Comment: describe the reason why you want to filter these MAC address. Just few words are saved there usually.

Current Port Forwarding List: this table will list the detailed information about the ports that will be forwarded.

6.5.7 DMZ Setting

DMZ means Demilitarized Zone. It can be enabled and used as a place where services can be placed such as Web Servers, Proxy Servers and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with the NAT functionality as an alternative for the Port Forwarding while makes all the ports of the host network device be visible from the external network side.



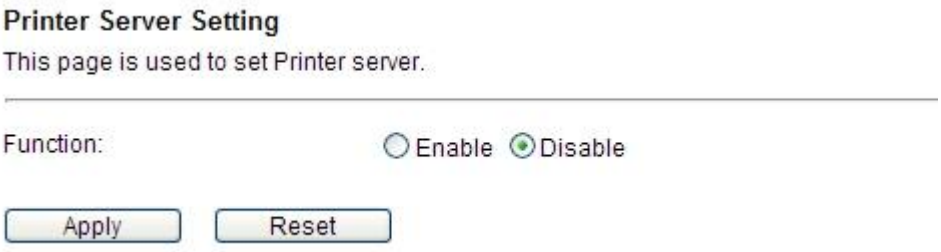
Host IP Address: type in the IP address of the DMZ host

6.6 USB Storage

With USB2.0 port, this router allows users to plug USB devices and sharing information or server service with others in LAN & Internet.

6.6.1 Printer Server

Enable Printer Server allows all users in LAN to share connected printer service.



Before you use this function, please make sure:

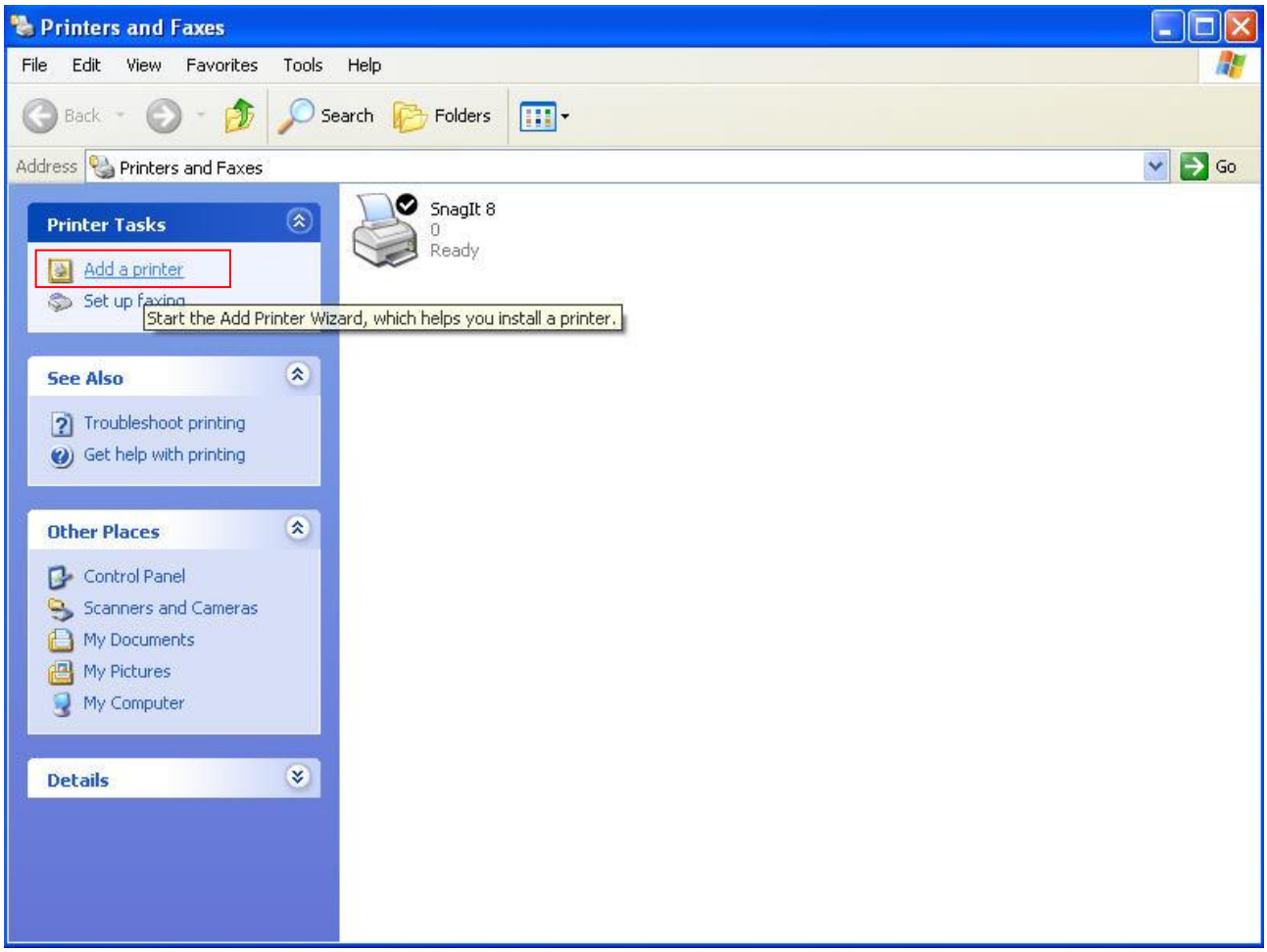
1. All the computers connected to this router have installed printer driver. If not, please install it first.
2. Your printer must be an USB printer that can be connected to the router.

If the two steps are ready, please choose **Enable** and then click **Apply** button to share the printer service connected to the USB port of router.

After enable the Printer Server and make sure you have connected your Printer with the router by the USB port. Please follow the instructions below to install Printer Driver.

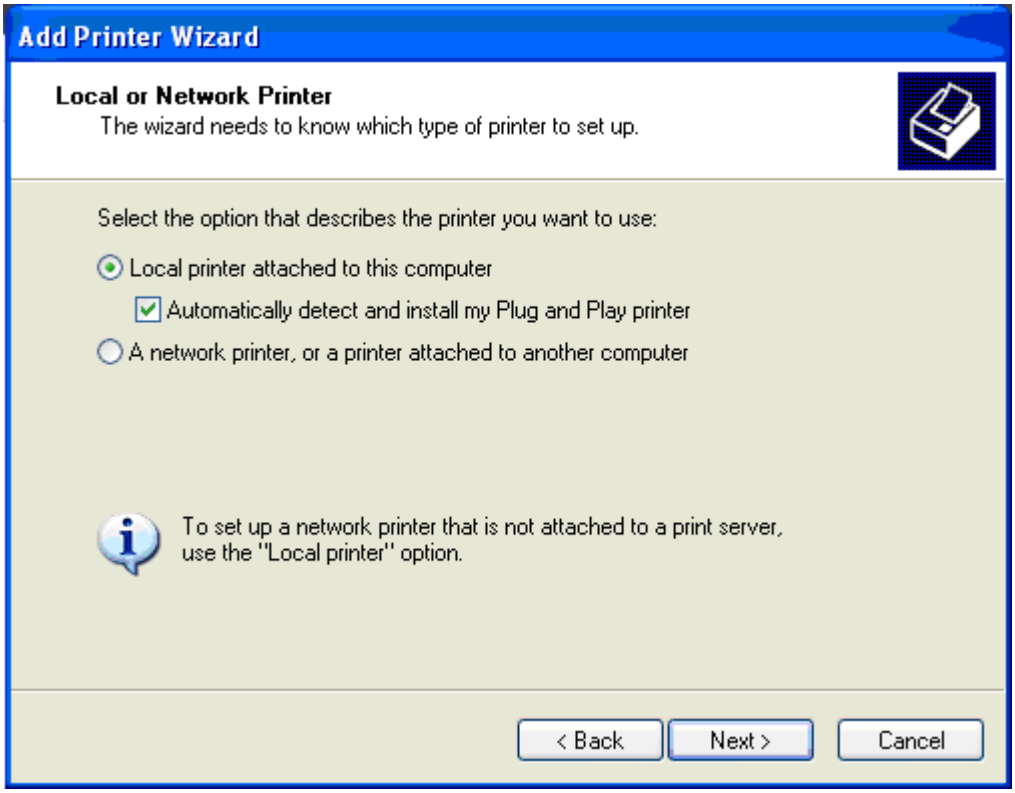
1. Click **Start—Printers and Faxes**:

2. Click **Add a printer** on the left:

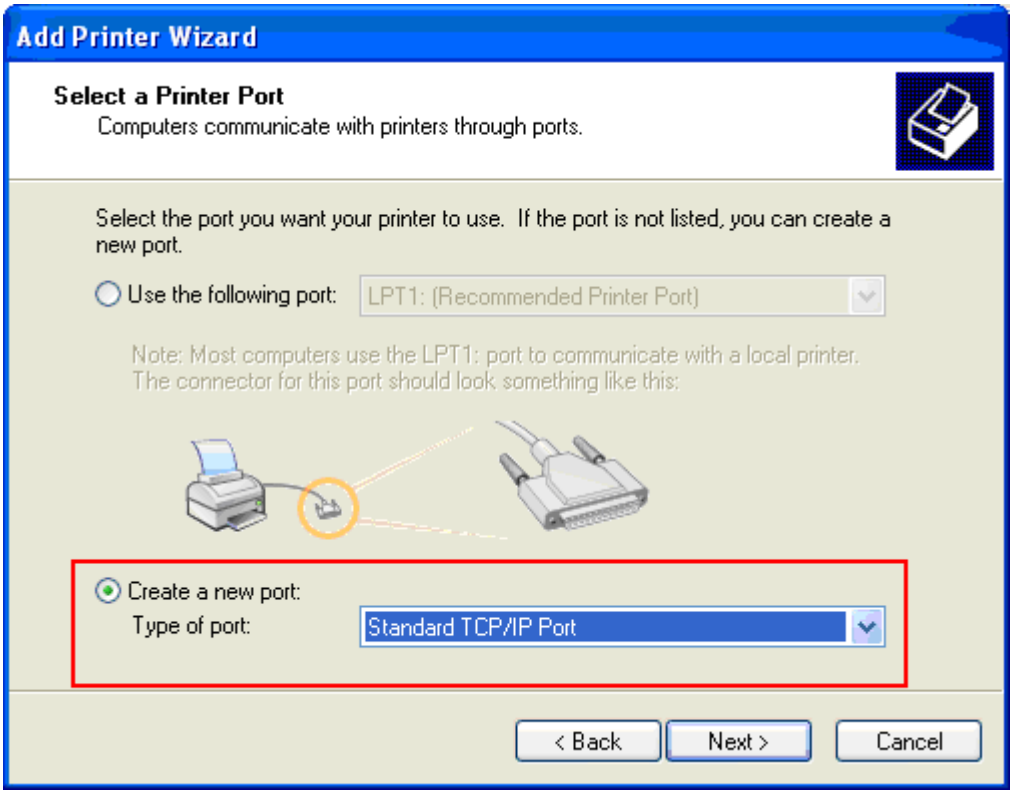


3. Click **Next** while it comes out the welcome interface as below.

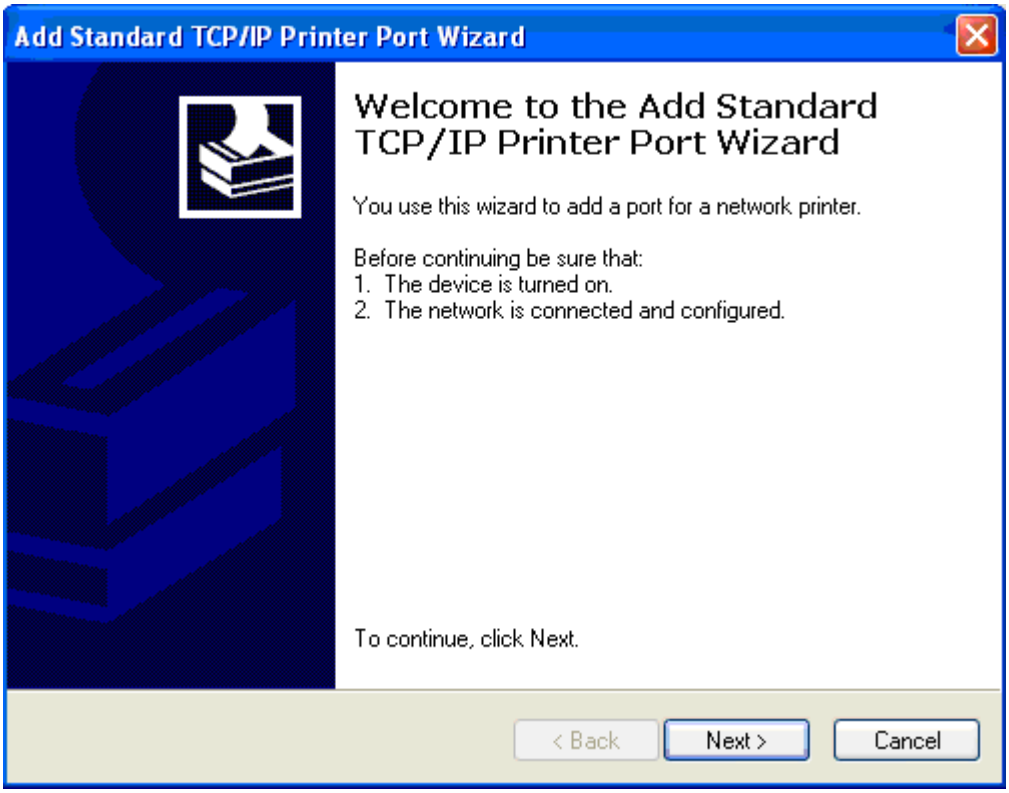
4. Choose “**Local printer attached to this computer**” and click **Next**.



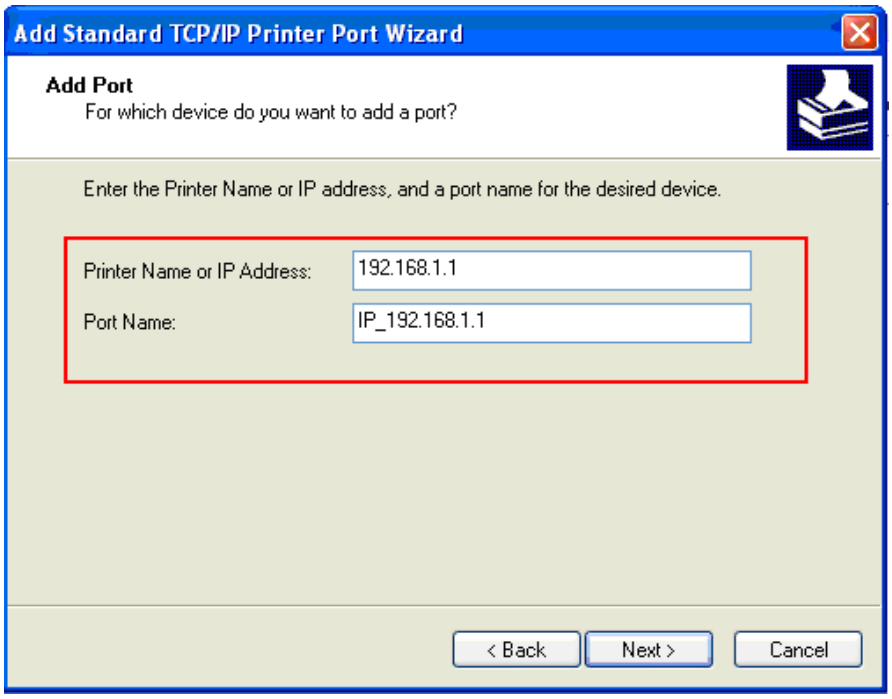
5. Select “**Create a new port**” and choose “**Standard TCP/IP Port**” for type of port. Click **Next**.



6. Please click Next on below window.



7. The most important: please type in the gateway of your wireless router, by default, it is 192.168.1.1 for TOTOLINK wireless router.



8. Now you have to select the right Printer Manufacturer and model number and install it.

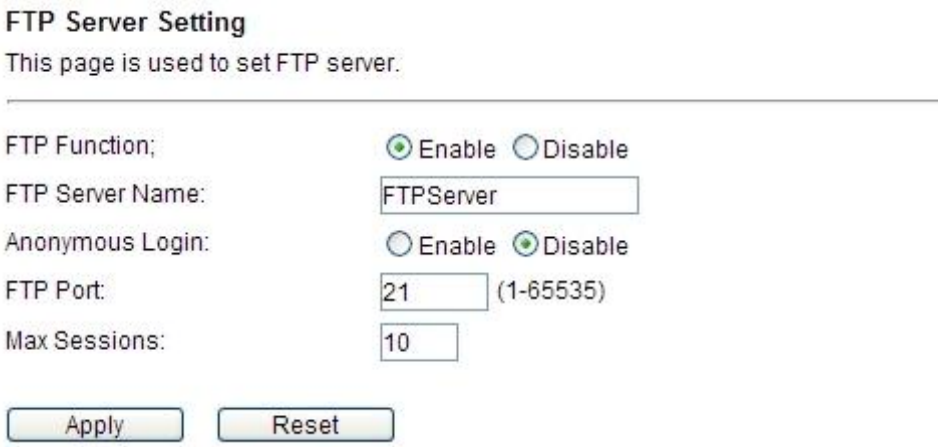
Note: Make sure the Printer has been plugged into the USB port of router, else it will show you that there isn't any printer founded.

9. After installation, you can share the USB Printer connected to your router.

If you don’t want to share your Pinter any more, just choose Disable and click Apply to save the setting.

6.6.2 FTP Server

If you enable this function, please enter the available FTP Server Name and FTP Port.



FTP Function: you can choose to enable or disable FTP Server.

FTP Server Name: Enter a name for FTP Server.

Anonymous Login: Choose Enable to login anonymously.

FTP Port: Enter the FTP Port number to use, the default is 21.

Max Sessions: The maximum number to access the FTP Server.

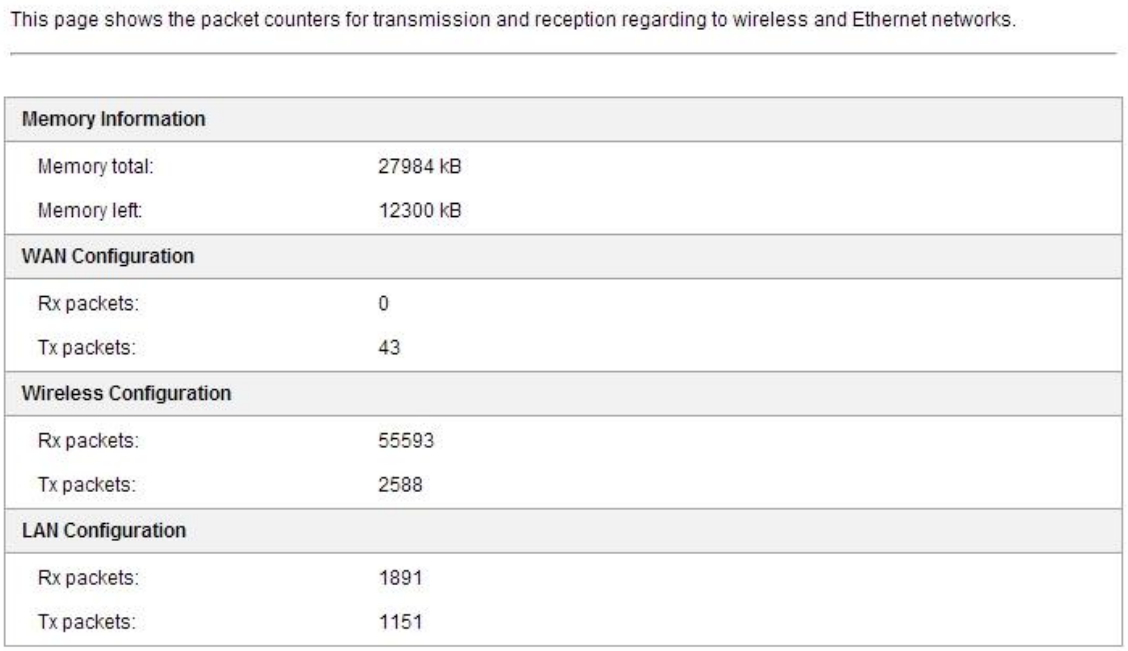
After configuration, the FTP Server can be accessed from the Internet or your local network.

6.7 Management

For system management, there are several items that you have to know the way of configuration: Traffic Statistics, DDNS Settings, NTP Settings, Remote Management, System Log, Upgrade Firmware, Save Configuration and Administrator Settings.

6.7.1 Traffic Statistics

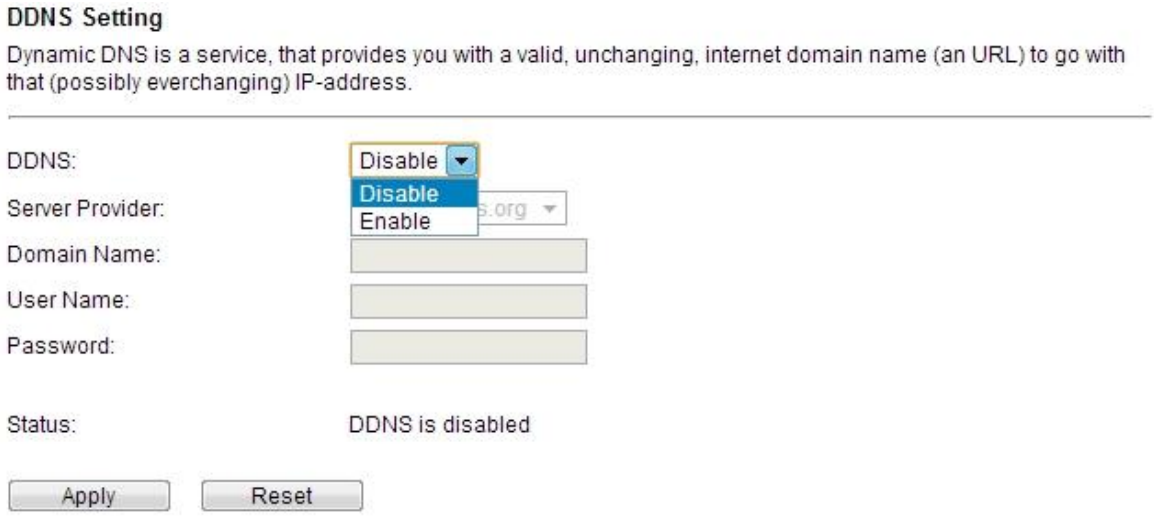
This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.



6.7.2 DDNS Setting

Dynamic Domain Name System is also called DDNS simply. The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service from the DDNS service providers. This router supports two service providers: DynDNS and NO-IP,



You could choose to enable or disable DDNS function. If you enable DDNS, you need to provide below information:

Service Provider: choose one service provider where you have applied for free DDNS service.

Domain Name: type in the host name you registered from the DDNS provider.

User Name: enter the User Name you registered from the DDNS provider.

Password: enter the Password you set for the User Name.

6.7.3 NTP Setting

This page allows you to maintain the system time by synchronizing with a public time server over the Internet.

Current Time: shows the current time based on your time zone.

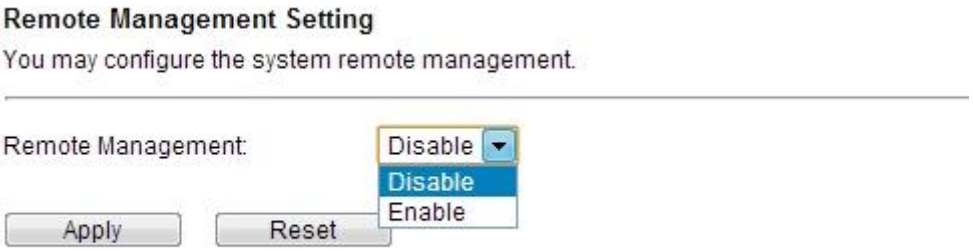
Time Zone: select the Time Zone where the router is located.

NTP Client Update: here you can enable NTP Client Update.

NTP Server: NTP means Network Time Protocol which is used to make the computer time synchronized with its server or clock source, such as Quartz and GPS. It can provide high-precision time correction and prevent harmful protocol attack by confirming encryption.

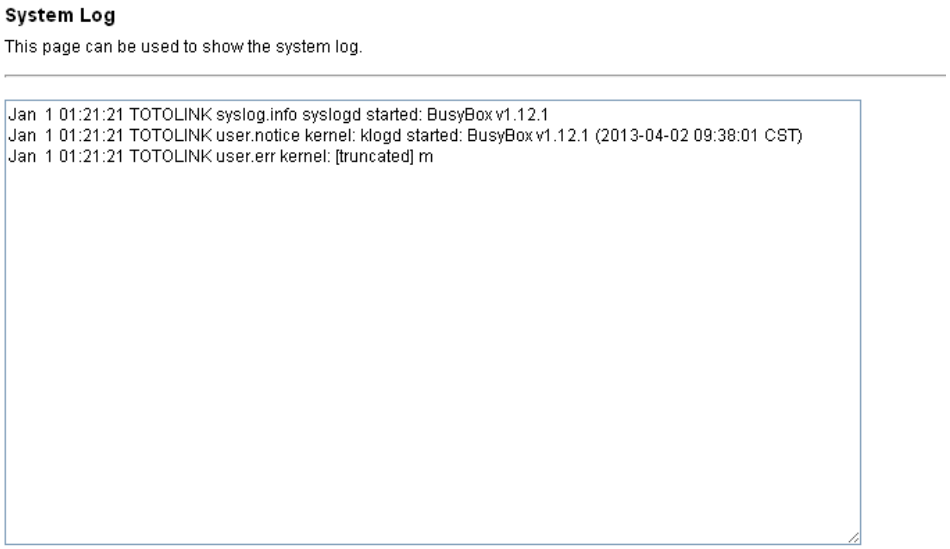
6.7.4 Remote Management Setup

You could choose to enable or disable Remote Management.



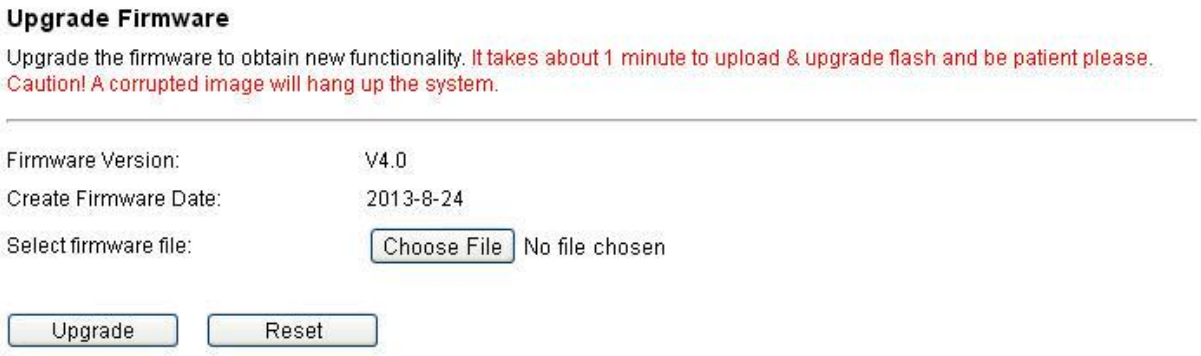
6.7.5 System Log

This page can be used to set remote log server and show the system log.



6.7.6 Upgrade Firmware

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.



Firmware Version: shows the current firmware version.

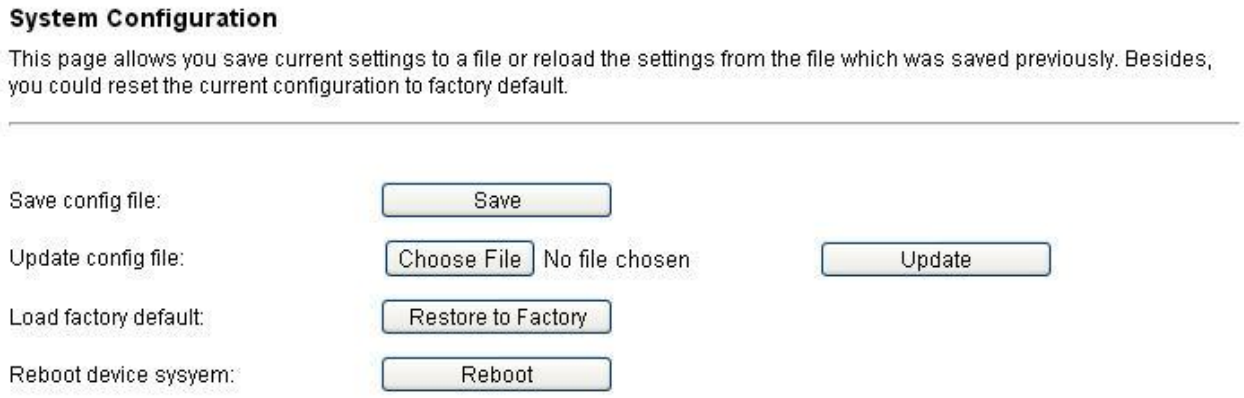
Create Firmware Date: the data this firmware version created.

Select firmware File: select the firmware version you want to upgrade on your computer.

Click **Upgrade** to upgrade the firmware version.

6.7.7 System Configuration

This page allows you to save current settings to a file or reload the settings from the file which was saved previously. Besides, you can reset the current configuration to factory default.



Save config file: click **Save** button to download the current settings of the Access Point to your computer.

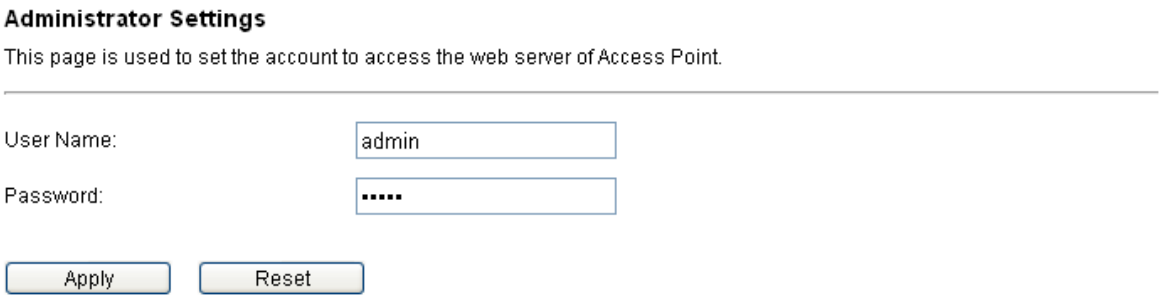
Update config file: if you want to reload the settings from the file saved before, you could click **Choose File** button to choose the right file then click **Update** button.

Load factory default: this **Restore to Factory** button is provided to allow you to restore the router settings to the default factory settings.

Reboot device System: click **Reboot** to reboot this device.

6.7.8 Administrator Setup

This page allows you to change the Administrator information to login web interface of this router.



User Name: enter the User Name you login.

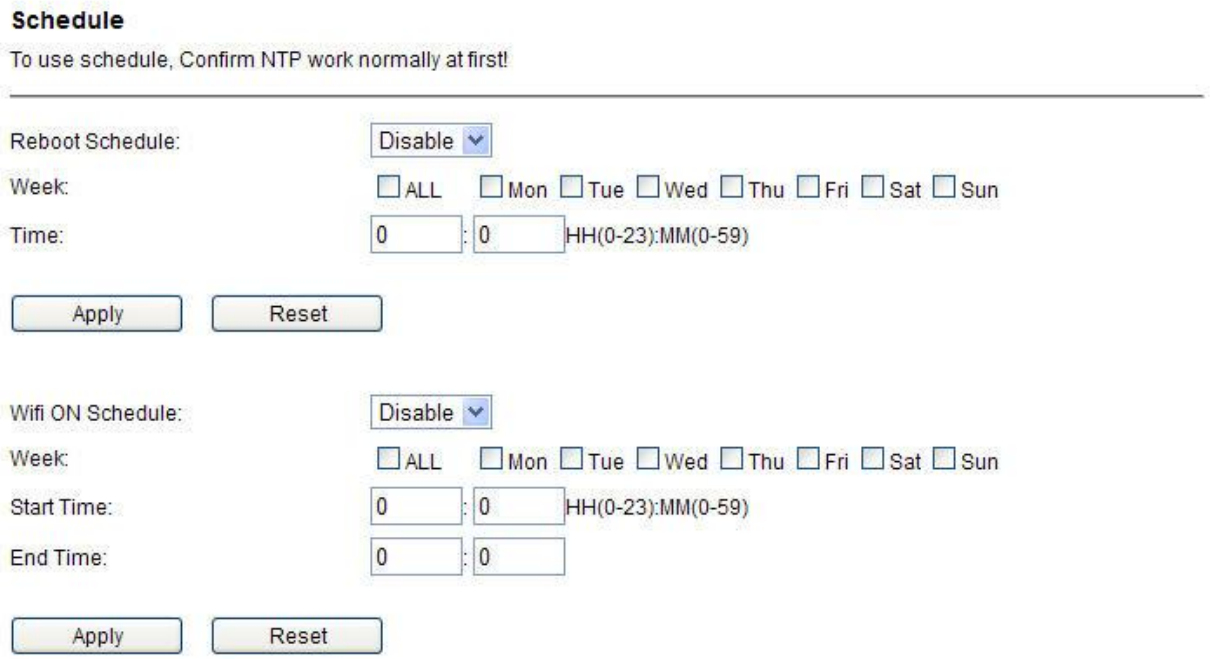
Password: new password is used for administrator authentication.

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

6.7.9 Schedule

The schedule function allows you to setup the time that the router will reboot automatically. What's more, it allows you to setup the time WiFi on and off while by the other times beyond this period WiFi will be off. It is very convenient for users who often access the Internet very

regularly.



Reboot Schedule: you can enable or disable the reboot schedule function.
Time: enter the Time Start and the router will reboot automatically by the time.
Week: select the date when the schedule function operates.
Wifi ON Schedule: you can enable or disable the reboot schedule function.
Time Start: by the time, WiFi will turn on.
Time End: by the time, WiFi will turn off.

Before you use this function, please make sure:

(1) Connect the router's WAN port to the Internet so that the router can access wide area network.
(2) Make sure that you have enabled NTP Client Update and choose the NTP Server or enter the domain name manually.