Wireless Router

User Manual

Version 1.0 | 7/15/2017

Table of Content

Chapter 1 Introduction

The Wireless Router is compatible with IEEE802.11n standard, which supports data rate up to 300 Mbps in 2.4 GHz band, which is also compatible with IEEE 802.11g/b wireless devices. The Wireless router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in 5-port switch and wireless AP, LAN users can share files, and playing network games all at a high speed.

The Wireless Router is designed to satisfy the small business, office and home office wireless Internet needs, it is powerful, superior performance, is easy to manage your Shared wireless broadband Internet access, the best choice for common .haring broadband Internet.

1.1 Features

- High speed data rate - up to 300Mbps.
- Support 64/128 WEP,WPA/WPA2,WPA-PSK/WPA2-PSK wireless encryption
- Support NAT,DMZ,QOS,DDNS
- Support PPPOE, Static IP, DHCP,WISP Repeater, Repeater, Client WAN connection mode
- Support DHCP server and client,
- Support VPN pass-through
- Support MAC filter, IP filter and URL filter
- Support UPNP
- Firmware upgradeable.

1.2 System Requirement

- An Ethernet-Based Cable or xDSL modem
- An Ethernet Card on PC
- TCP/IP network protocol for each PC
- RJ45 Twisted-pair
- Microsoft IE (or Firefox or Netscape)

1.3 Package Contents

Please unpack the box and check the following items:

- One 300M 11n Wireless Router
- One Power Adapter
- One User Manual

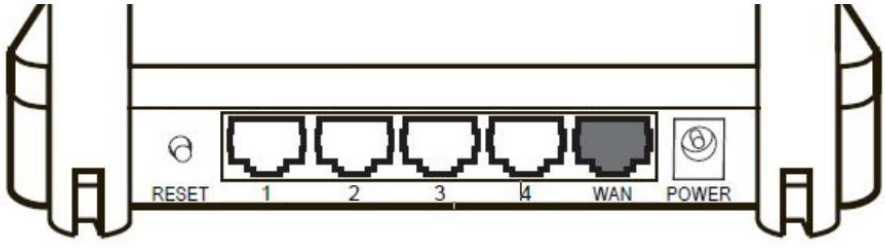
Chapter 2 Hardware Installation

2.1 LED indicators

The top panel contains LED indicators that show the status of the unit.

Name	Status	Indication
Power	Off	Power is off.
	On	Power is on.
SYS	Off	System is OK
	On	System can't work properly
WAN	Off	No device connecting with WAN port.
	On	WAN port is connecting.
LAN(1-4)	ON	LAN port is connected, but no data transmission.
	BLINK	LAN port is connected and data transmission.
2.4GHz	OFF	Wireless is disable.
	BLINK	Wireless is enable and data transmission.

2.2 Back Rear Panel

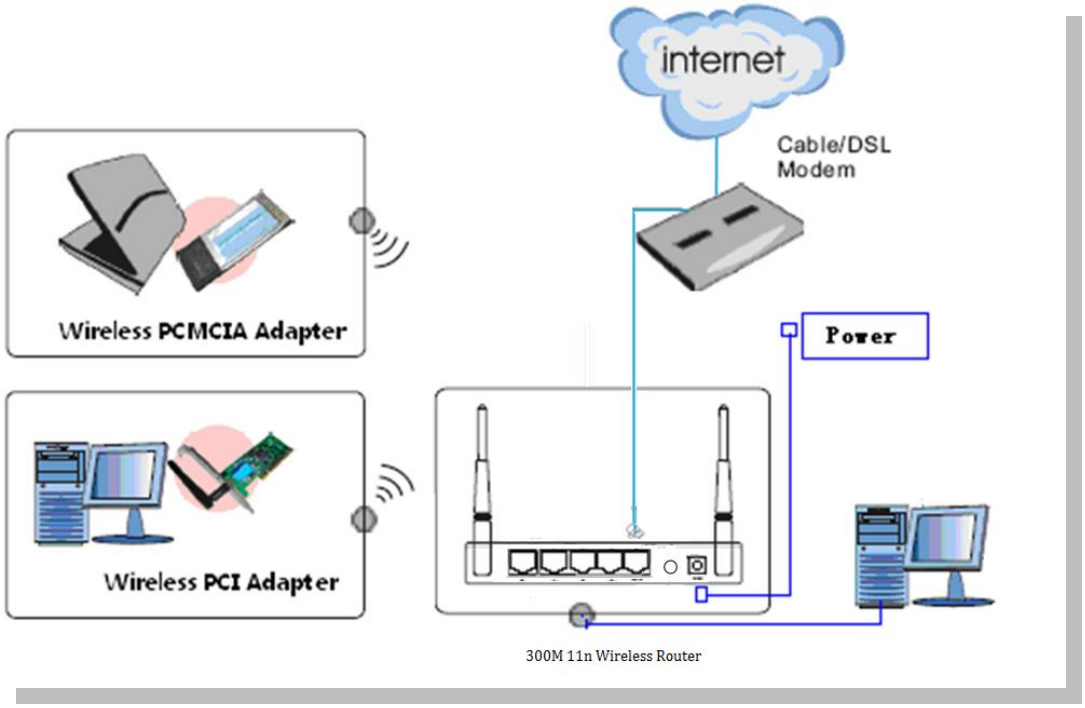


The following parts are located on the rear panel.

LAN (1,2,3,4): These four LAN ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network. If you connect this product with the Hub (or Switchboard) correctly, the router's corresponding LED and the Hub's (or the Switchboard's) must be illuminates.
Wireless antenna: To receive and transmit the wireless data.
WAN: 10/100Mbps RJ45 port. The WAN port is where you will connect Cable/xDSL Modem or other LAN.
RESET: use a pin to press and hold the button about 10 seconds, the router will restore to factory default.
POWER: The Power socket is where you will connect the power adapter. Please use the power adapter provided with this router.

2.3 Typical install

Before installing the router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.



1. Make sure all devices, including your PCs, modem, and router, are powered down.
2. Using an Ethernet network cable, connect the LAN or Ethernet network port of the cable or DSL modem to the router's WAN port.
3. Power on the cable or DSL modem, and power on the PC you wish to use to configure the router.
4. Connect the included power adapter to the router. And connect the other end of the adapter to an electrical outlet.

Chapter 3 Quick Installation Guide

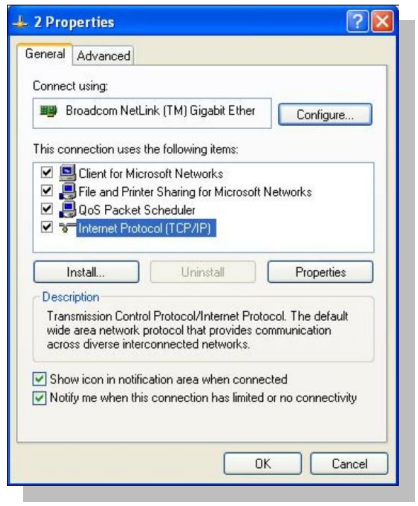
The chapter mainly presents how to enter the router's Web page and simple router settings. After you have finished the hardware installation (Please refer to chapter 2), the following steps will assist you to set the network configurations for your computer.

3.1 Set the Network Configurations

1. On your computer desktop right click **"My Network Places"** and select **"Properties"**.

2. Right click **"local Area Network Connection"** and select **"Properties"**.

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



4. Select **"Obtain an IP address automatically"** or select **"Use the following IP address(S)"**.

A. Select **"Obtain an IP address automatically"** and **"Obtain DNS server address automatically"**. Click **"OK"**.

B. **"Use the following IP address (S)"**

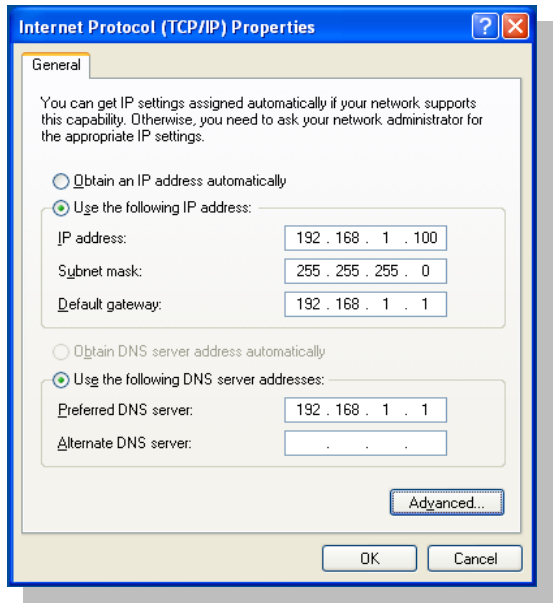
IP Address: 192.168.1.XXX: (XXX is a number from 2~254)

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

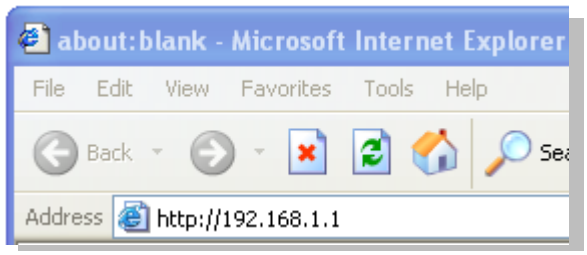
DNS Server: You need to input the DNS server address provided by you ISP. Otherwise, you can use the router's default gateway as the DNS proxy server.

Tip: If you are not sure of the DNS server address, we recommend you to select “Obtain an IP address automatically (O)” and “Obtain a DNS server address automatically”.



Click **"OK"** to save the configurations.

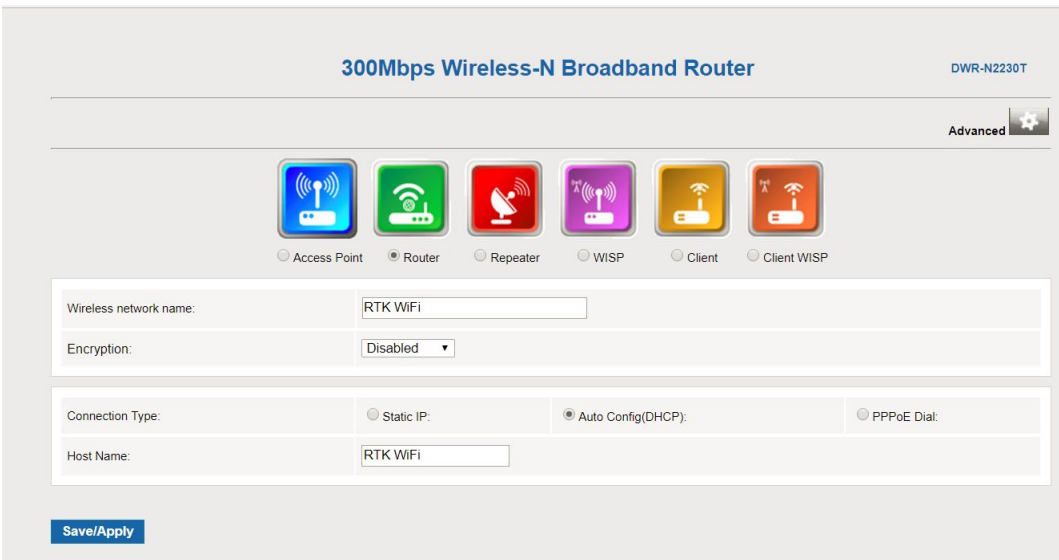
3.2 Getting Started



To access the configuration pages, open a web-browser such as Internet Explorer and enter the IP address of the router (**192.168.1.1**).

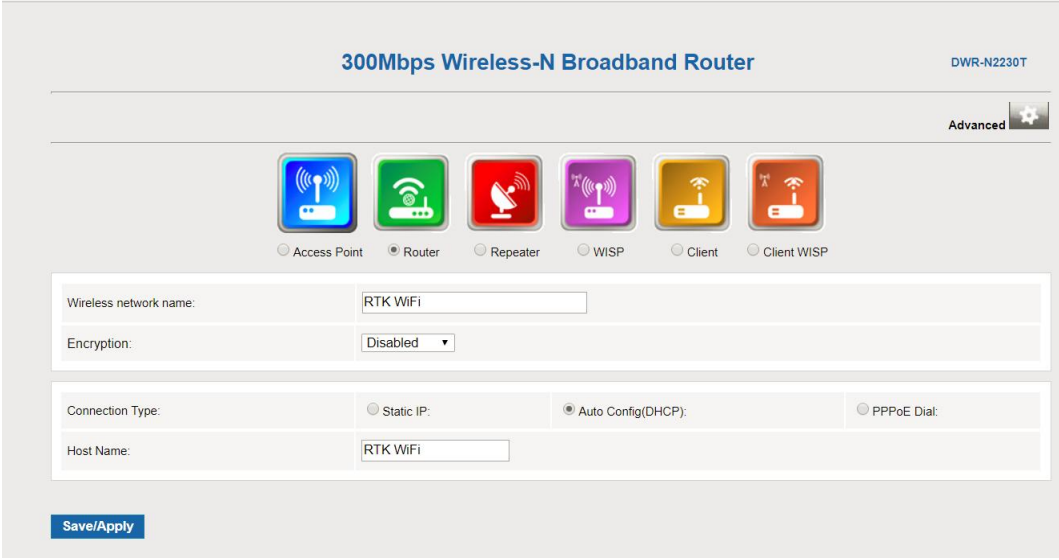
The Default User/Password: **admin**

If successful, you can see the login window, will enter setup wizard page as below:



3.3 Setup Wizard

This page will guide you to setup your router step by step in simple way. In this section, there are several modes for you to configure your router:



Please follow the steps and complete the router configuration and below are introduction of each mode:

Access Point: This mode is more used to transfer wired connection into wireless. It works like a switch. Usually, it is behind a router.

If you are in an office, hotel and places where only wired network is available, or LAN gaming party, small meeting and other situations where a temporary wireless network is needed, please use the AP Mode.

Router: Router mode can share one wired Internet connection to several clients. At that time, there will be one WAN port. It supports multiple connection types, like Dynamic IP/Static IP/PPPoE/L2TP/PPTP.

When Internet access from DSL or cable modem is available for one user but more users need to share the Internet, please use the Router Mode.

Repeater: This mode is used to extender the wireless coverage with same SSID and security.

When you have a wireless already, and there is some place can't be covered, you can consider Repeater Mode. With Repeater mode, you can have only one SSID. At that time, your wireless clients can roam in whole place.

WISP: This mode can connect to a wireless network and share the connection to its clients. The wireless is its WAN side. It can also support Dynamic IP/Static IP/PPPoE/L2TP/PPTP.

When the wireless station limits the number of clients or asks username/password to

connect, WISP Mode is what you need.

Client: In this mode, your device can connect to a wired device and works as a wireless adapter to receive wireless signal from your wireless network.

For a Smart TV, Media Player, or game console with an Ethernet port. Use the Client Mode to make your devices Wi-Fi enabled, granting them access to your wireless network.

Client WISP: In this mode, your device can connect to a wired device and works as a wireless adapter to receive wireless signal from your wireless ISP, it can also support Dynamic IP/Static IP/PPPoE/L2TP/PPTP.

For a Smart TV, Media Player, or game console with an Ethernet port. Use the Client WISP Mode to make your devices Wi-Fi enabled, granting them access to your wireless network.

How to choose internet access mode?

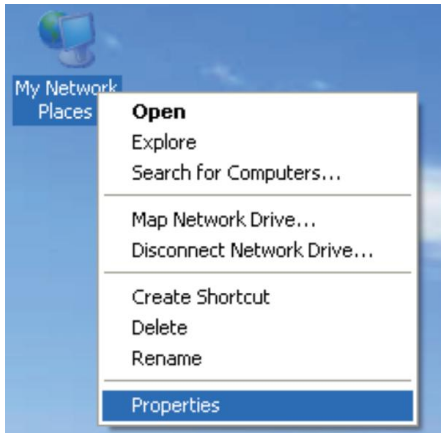
Network Parameters Provide by ISP	Internet Access Mode
Username and Password	PPPOE
Static IP address,subnet mask,gateway,DNS server	Statis IP
No need for any information from ISP, no need do any configuration on router	DHCP
Wireless connection with your ISP	WISP or Repeater

Notice: If you need more advanced functions, please click ”Advanced” to enter advanced configuration page.

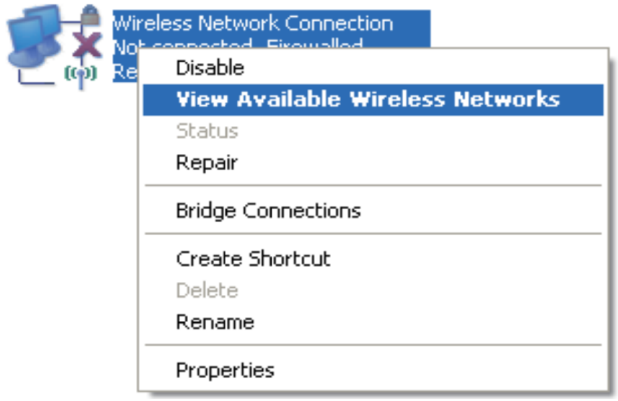
3.4 Wireless Connection

First of all please make sure your PC is installed a wireless adapter, unplug the LAN cable between PC and router, then follow below steps to configure your wireless connection:

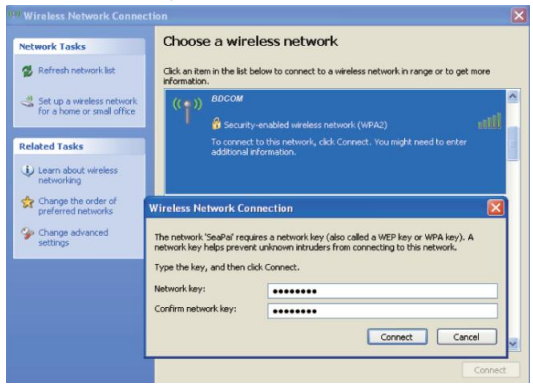
1. Right click “My Network Places”, select “Properties” on your computer desktop:



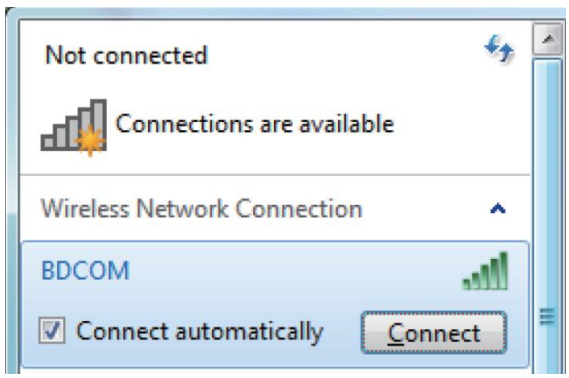
2. Open “Wireless Network Connection”, it will show “Not connected”. Right click “Wireless Network Connection”, select” View Available Wireless Networks”.



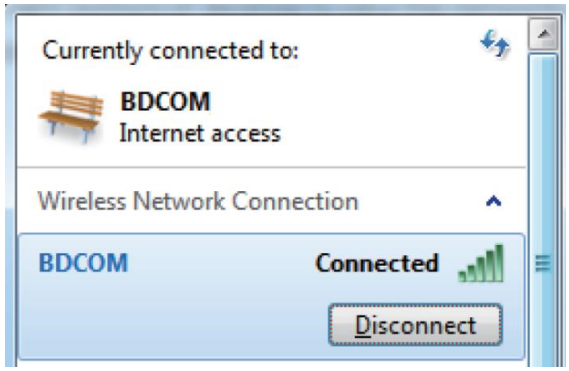
3. The right part of window shows current available wireless SSID, you can click on “refresh network list” on the left panel to renew the list. Select a specific SSID and click “Connect” or double-click the SSID ,then input the wireless password in pop-up window and click “Connect” to finish your configuration. This window won’t appear if your wireless network is not encrypted.



4. For Windows 7 or higher OS, please follow below steps:
   1) Click wireless icon on the right bottom of your computer desktop to view available network, select SSID of your router, click “Connect” or double-click it.



2) If you set wireless password on your router already, please enter password to finish your wireless connection. If you didn't set any wireless password on the router, please connect it directly.



Chapter 4 Advanced Configuration

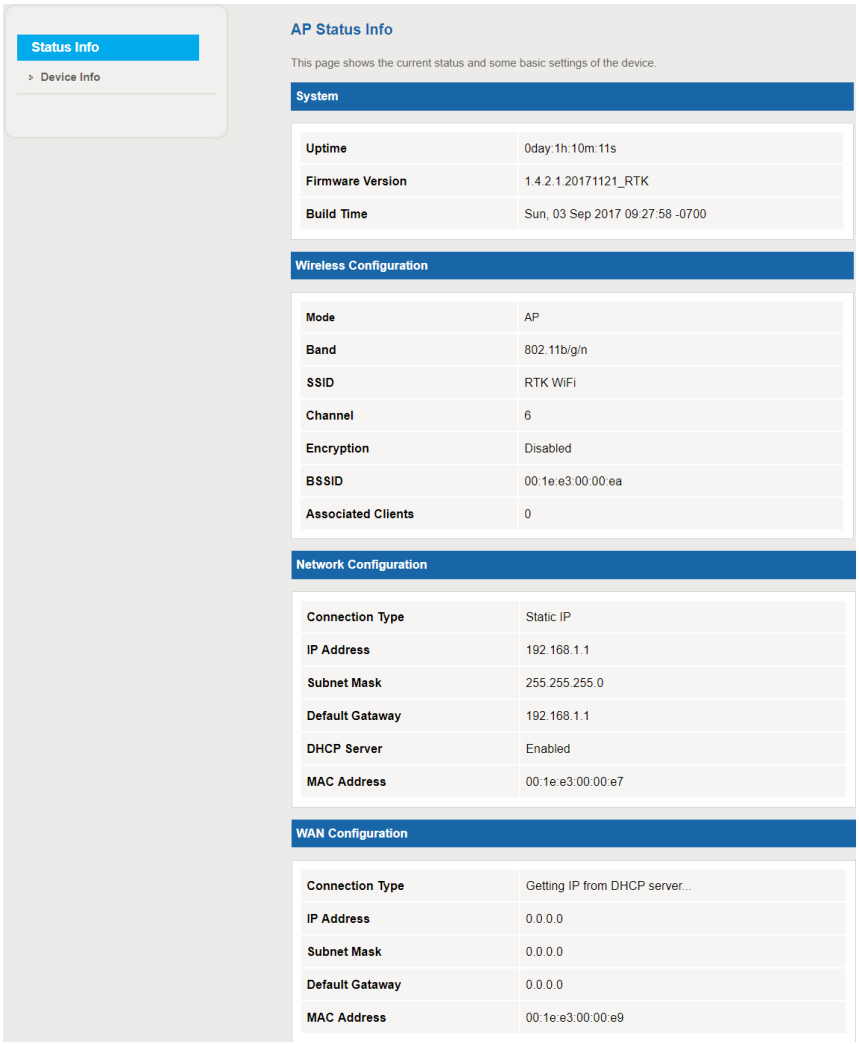
This chapter mainly introduce how to configure your router in details, there are five menus in advanced configuration page: Status, Network Setup, Advanced, Security Settings, Maintenance .Also Logout/LED/Home button will help you control router easily.

4.1 Status

The Status page provides you with a snapshot of your router's current connections and settings.

System Information section provides you with the router's firmware version and build. This is used to help our support department determine what firmware version your device is running. Wireless Configuration shows the details of the 2.4GHz wireless networks.

Network Configuration displays current configurations for local network IP address and DHCP server settings. WAN Configuration displays information from your Internet Provider.

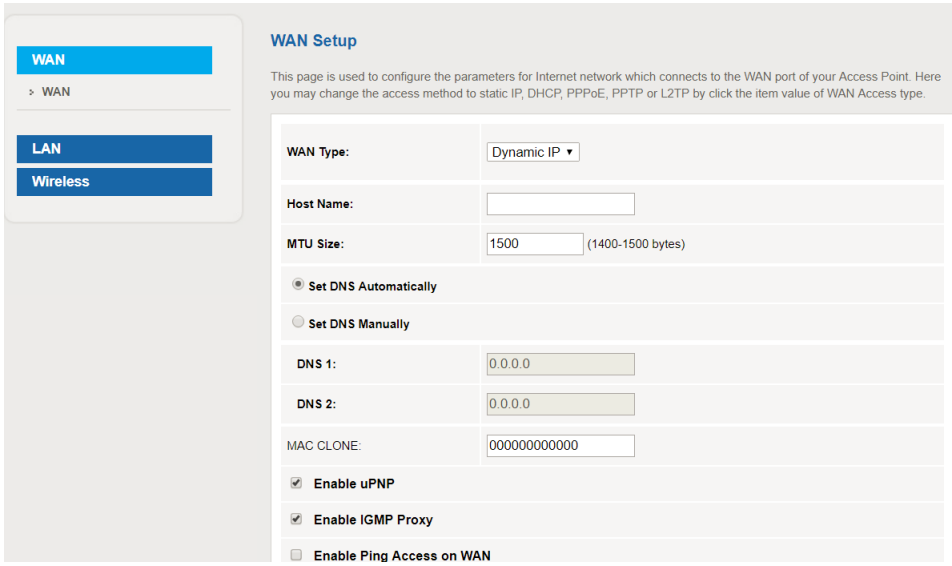


4.2 Network Setup

This page includes three sub-menus:WAN/LAN/Wireles, you can configure basic function of router in this page.

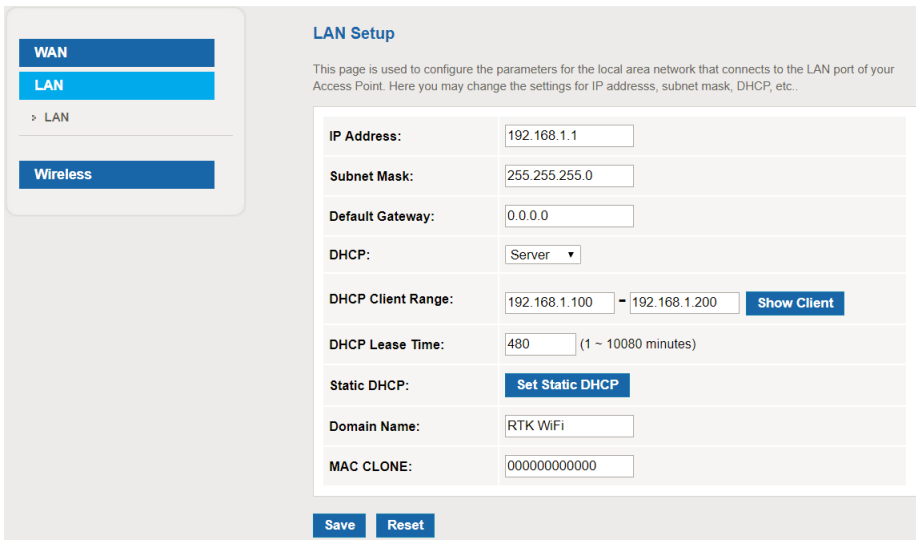
4.2.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP Client, PPPoE, PPTP or L2TP by click the item value of WAN Access type.



4.2.2 LAN

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.



IP Address: Enter the IP address of your router (**factory default: 192.168.1.1**).

Subnet Mask: An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Default Gateway: Enter the gateway IP address of your router.

DHCP: Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.

DHCP Client Range: The range of IP address the router DHCP server will assign to users and device connecting to the router.

DHCP Lease Time: The DHCP Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be “leased” this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 10080 minutes. The default value is 480 minutes.

Static DHCP: 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.

Domain Name: Input the domain name of you network.

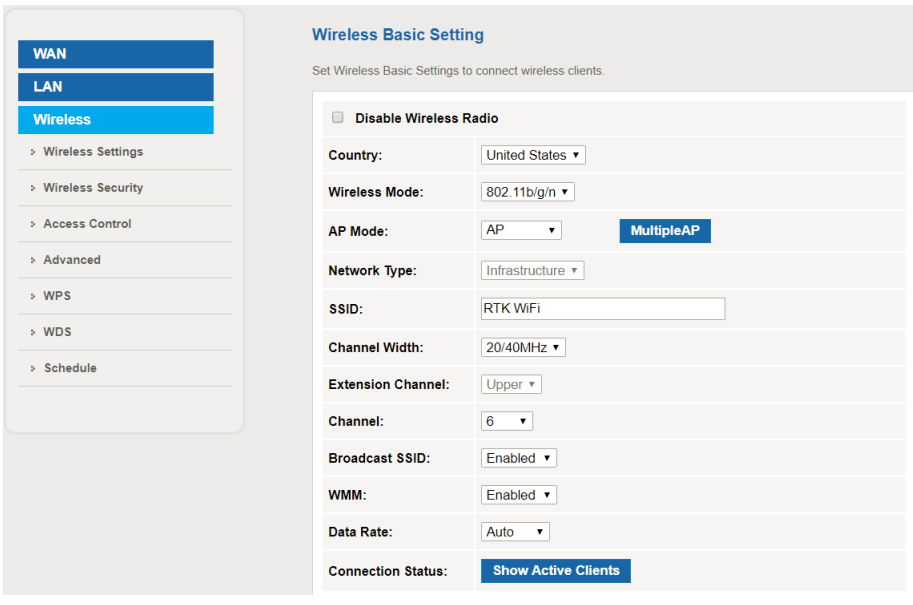
MAC CLONE: You can configure the MAC address of the LAN.

4.2.3 Wireless

There are seven submenus in Wireless page: **Wireless Settings, Wireless Security, Access Control, Advanced, WPS, WDS, Schedule** . Click any of them, and you will be able to configure the corresponding function.

1) Wireless Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

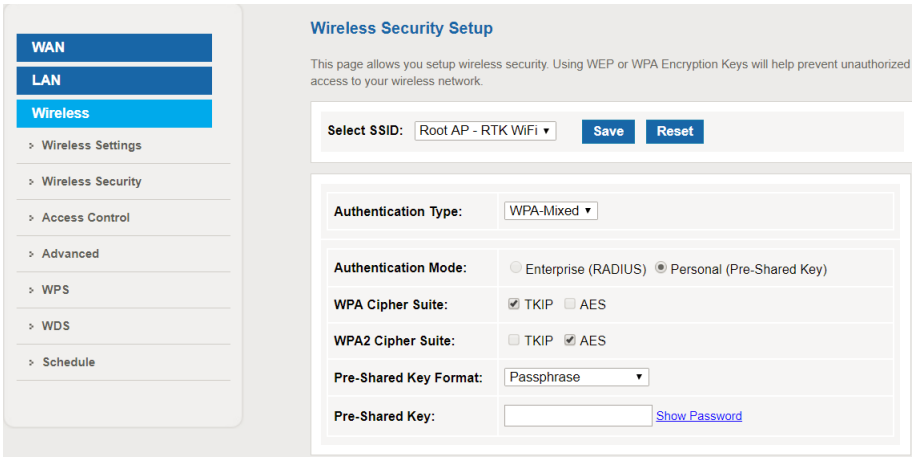


Disable Wireless Radio: Enable or disable wireless

Wireless Mode: Select one mode from the following. The default is 802.11b/g/n mode.
Mode: Support AP, Client, WDS and AP+WDS mode.
SSID: SSID (Service Set Identifier) is the unique name of the wireless network.
Channel Width: Select the channel width from the drop-down list.
Extension Channel: This relates to the channel number used for your wireless network. An upper band represents higher channels and vice versa.
Channel: Indicates the channel setting for the router.
Broadcast SSID: Select “Enable” to enable the device's SSID to be visible by wireless clients. The default is enabled.
WMM: It will enhance the data transfer performance of multimedia data when they’re being transferred over wireless network.
Data Rate: Sets the maximum wireless data rate that your network will operate on.
Connection Status: You can see the MAC Address, MAC address, transmission and reception packet counters for each associated wireless client.

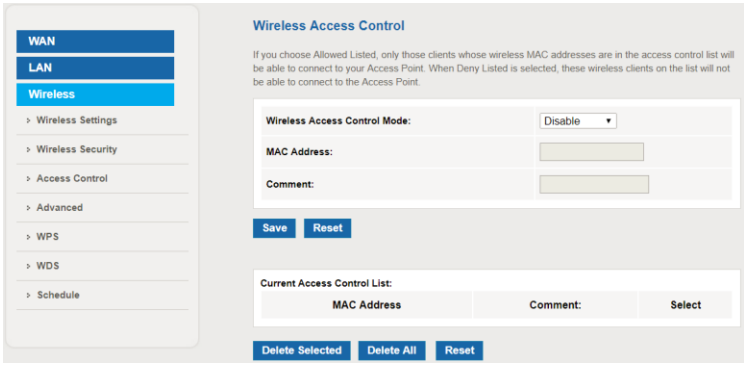
2) Wireless Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.



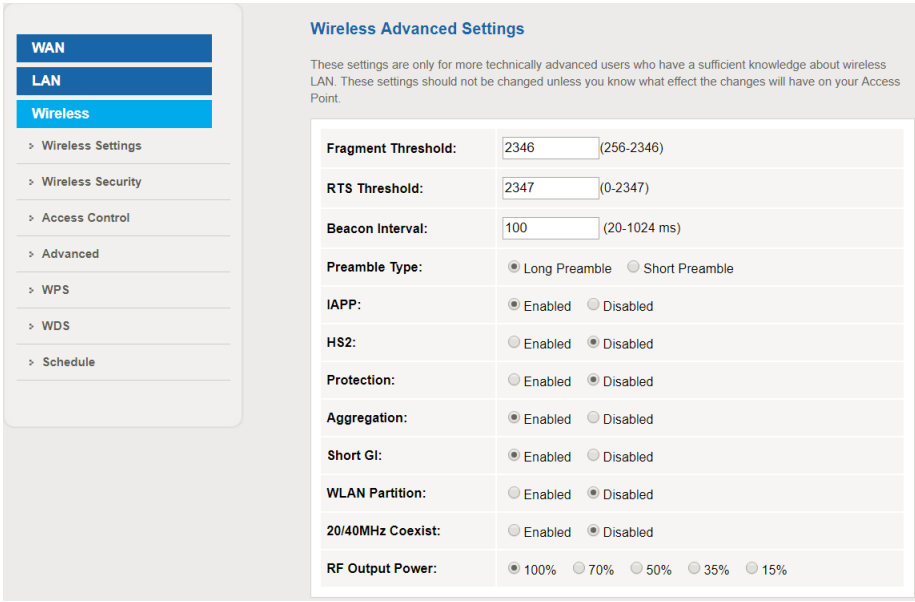
3) Access Control

This page allows you to control wireless stations accessing the router, which depend on the station’s MAC addresses.



4) Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.



Fragment Threshold: This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets.

RTS Threshold: RTS stands for “Request to Send”. This parameter controls what size data packet the frequency protocol issues to RTS packet. The default value of the attribute is 2347. It is recommended not to modify this value in SOHO environment.

Beacon Interval: Enter a value between 20-1024 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons.

Preamble Type: This configuration means that it adds some additional data header strings to help check the WiFi data transmission errors. Short Preamble Type uses shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster. Long Preamble Type uses longer data strings which allow for better error checking capability.

IAPP: Inter-Access Point Protocol.

HS2: Hot Spot 2.0 (HS 2.0), also called Wi-Fi Certified Passpoint, is a new standard for public-access Wi-Fi that enables seamless roaming among WiFi networks and between WiFi and cellular networks.

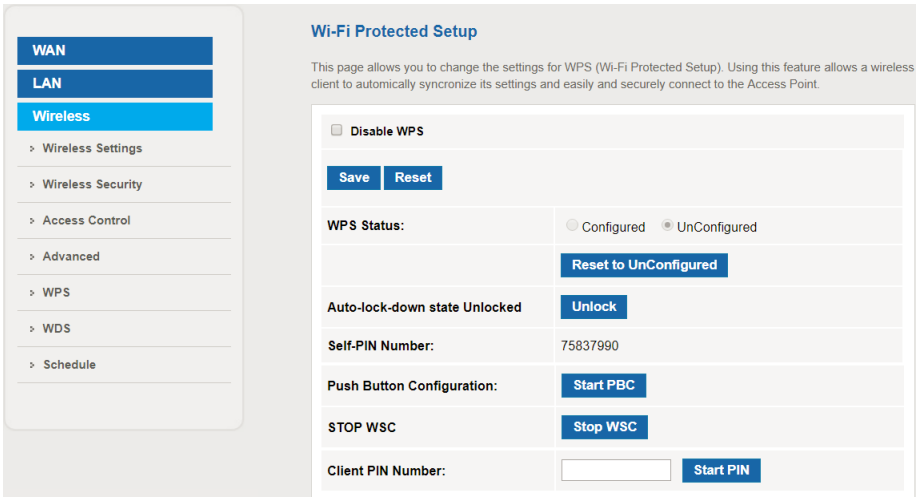
Short GI: This function is recommended for it will increase the data capacity by reducing the guard interval time.

WLAN Partition: Enabling WLAN Partition prevents associated wireless clients from communicating with each other.

RF Output Power: Here you can specify the RF output power of router.

5) WPS

WPS is designed to ease set up of security Wi-Fi networks and subsequently network management. This router supports WPS features for AP mode, AP+WDS mode, Infrastructure-Client mode, and the wireless root interface of Universal Repeater mode.



Disable WPS: Select this box and clicking “Apply” will disable WPS function. WPS is turned on by default.

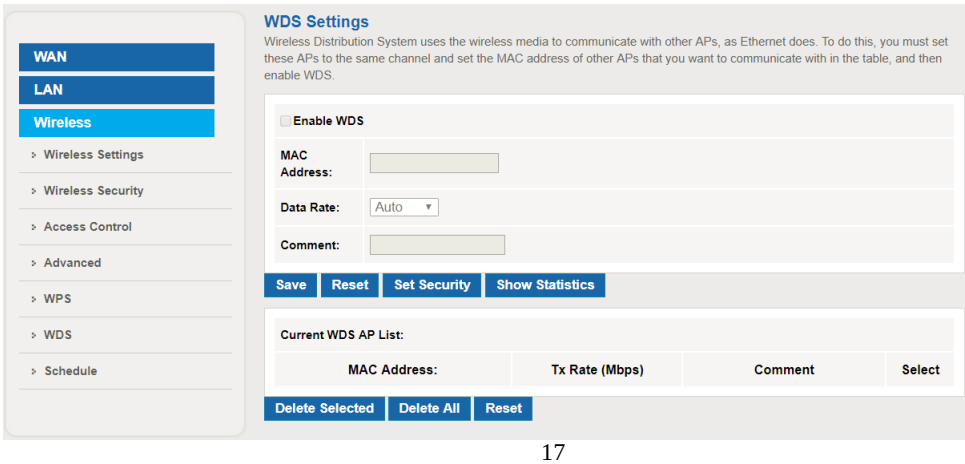
Self-PIN Number: It is AP’s PIN.

Start PBC: Clicking this button will invoke the Push Button Configuration of WPS. If one station wants to connect to the AP, it must click its PBC button in two minute. You can see the WPS LED flash this time.

Client PIN Number: The length of PIN is limited to four or eight numeric digits. If the AP and Station input the same PIN and click “Start PIN” button in two minutes, they will establish connection and setup their security key.

6) WDS

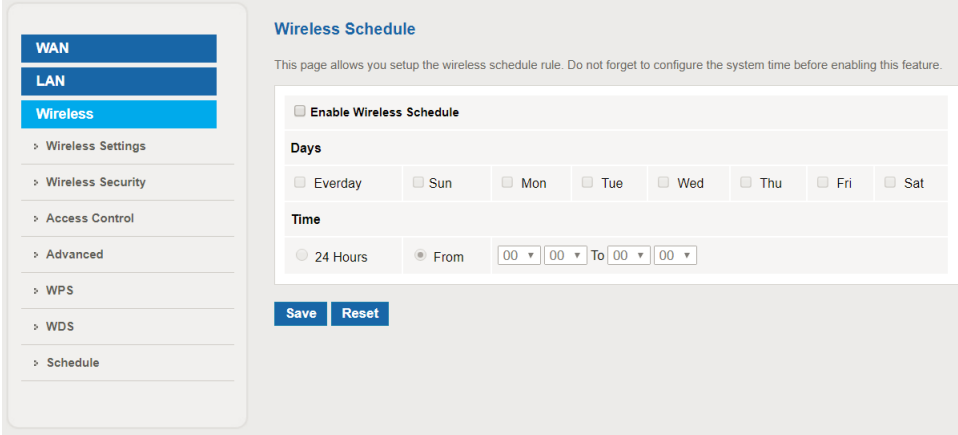
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, firstly you must set AP Mode to WDS or AP+WDS in basic setting, then enable WDS function and set another AP MAC which you want to communicate with. The WDS supports WEP and PSK security mode. Of course in order to make APs work, you have to keep them the same channel and security mode.



Enable WDS: Select this box to enable WDS function.
MAC Address: Enter the remote AP MAC address.
Data Rate: Sets the maximum wireless data rate that your network will operate on.
Comment: You can add some comment for this item.

7) Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

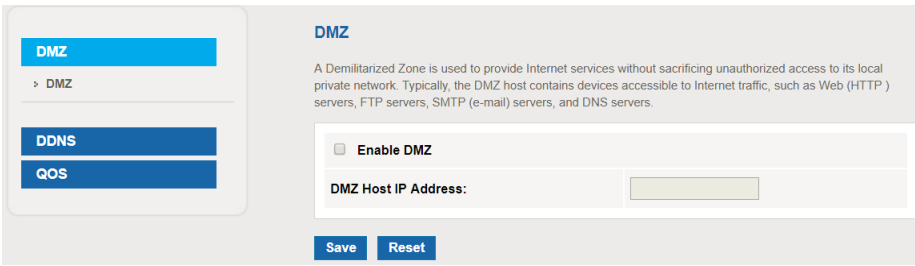


4.3 Advanced

There are three submenus under advanced menu: **DMZ, DDNS,QOS**. Click any of them, and you will be able to configure the corresponding function.

4.3.1 DMZ

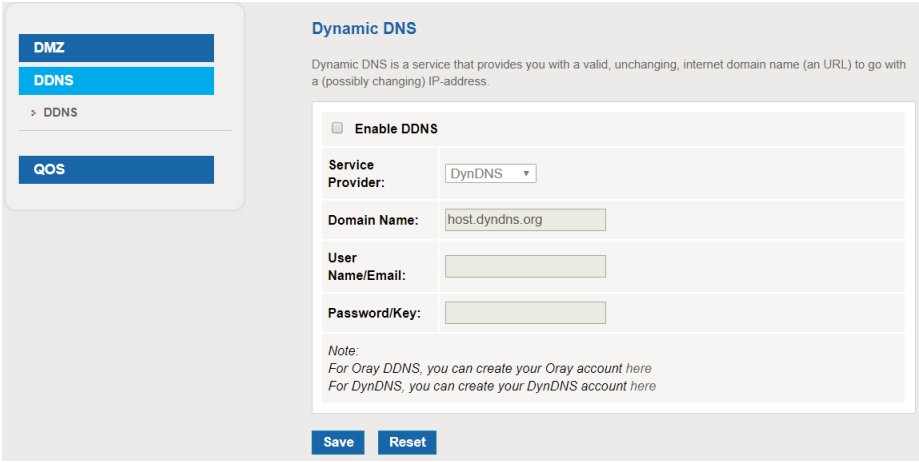
If you have a client PC that cannot run Internet application properly from behind the NAT firewall or after configuring the Port Forwarding, then you can open the client up to unrestricted two-way Internet access.



Enable DMZ: Select this box will enable DMZ function.
DMZ Host IP Address: Enter DMZ host IP Address may expose this host to a variety of security risks.

4.3.2 DDNS

Dynamic DNS is a service that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly ever changing) IP-address.

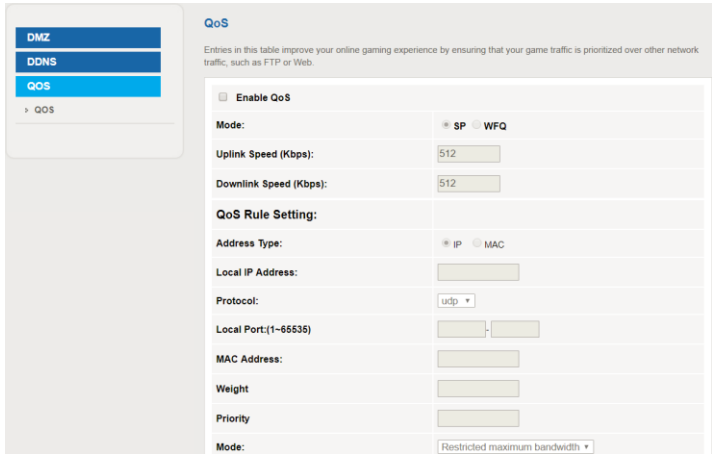


Service Provider: Select one from the drop-down menu, such as DynDNS, OrayDDNS or TZO.
Domain Name: Enter the domain name (Such as host.dyndns.org).
User Name/Email: Enter the user name or email the same as the registration name.
Password: Enter the password you set.

4.3.3 QOS

The QoS helps improve your network gaming performance by prioritizing applications. By default the bandwidth control are disabled and application priority is not classified automatically.
In order to complete this settings, please follow the steps below.

1. Enable this function.
2. Enter the total speed or choose automatic mode.
3. Enter the IP address or MAC address user want to control.
4. Specify how to control this PC with this IP address or MAC address, include Maximum or minimum bandwidth and its up/down speed.
5. Click Apply button to add this item to control table.

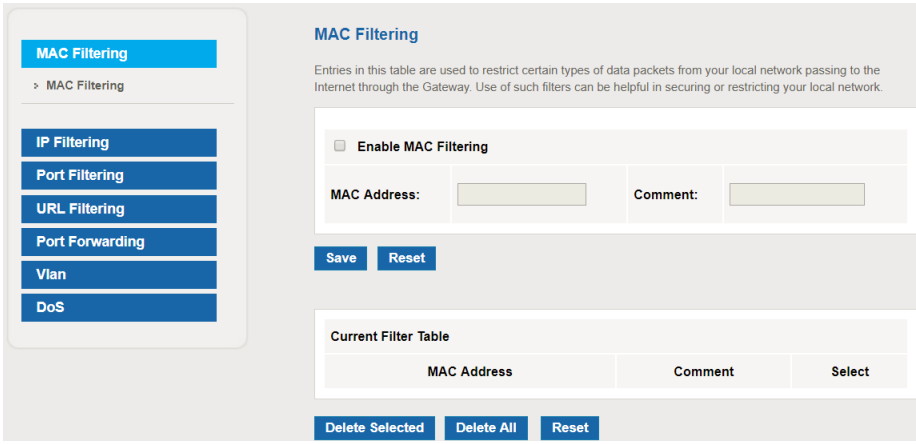


4.4 Security Settings

You can manage security function in this page, allow your router in a safe environment and make internet access limitation of clients which connected to this router.

4.4.1 MAC Filtering

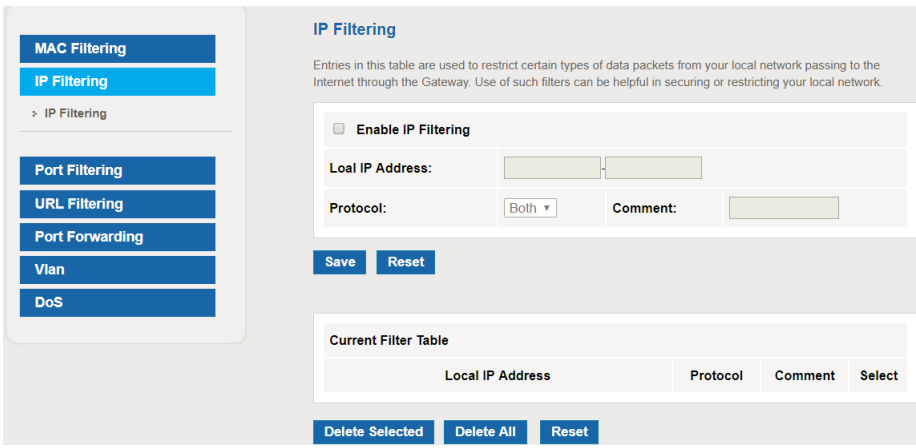
MAC Filtering allows you to deny access to specific users connecting to the network. Each networking device has a unique address called a MAC address (a 12 digit hex number).



Enable MAC Filtering: Select this box will enable MAC Filtering function.
MAC Address: The LAN device's MAC address that you want to filter.
Comment: You can add some comment for this item.
Current Filter Table: The table shows all you have configured. You can delete one or all.

4.4.2 IP Filtering

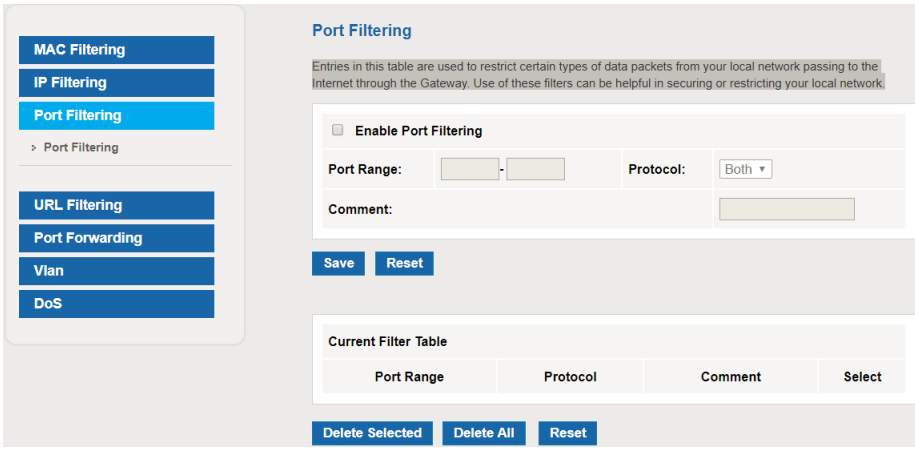
IP Filtering is used to block internet or network access to specific IP addresses on your local network. The restricted user may still be able to login to the network but will not be able to access the internet. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the user you wish to block.



Enable IP Filtering: Select this box will enable IP Filtering function.
Local IP Address: The LAN device's IP address that you want to filter.
Protocol: The protocol that you want to filter, either TCP, UDP, or Both.
Comment: You can add some comment for this item.
Current Filter Table: The table shows all you have configured. You can delete one or all.

4.4.3 Port Filtering

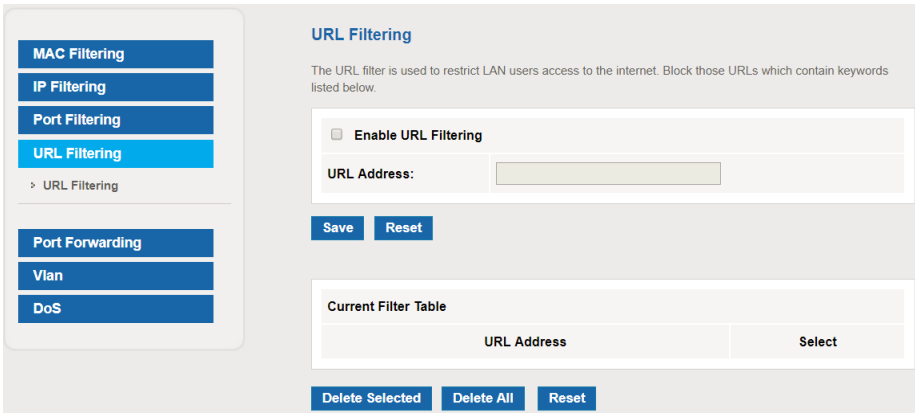
This table are used to restrict certain types of data packets from your local network passing to the Internet through the Gateway. Use of these filters can be helpful in securing or restricting your local network.



Enable Port Filtering: Select this box will enable Port Filtering function.
Port Range: The port range that you want to filter.
Comment: You can add some comment for this item.
Current Filter Table: The table shows all you have configured. You can delete one or all

4.4.4 URL Filtering

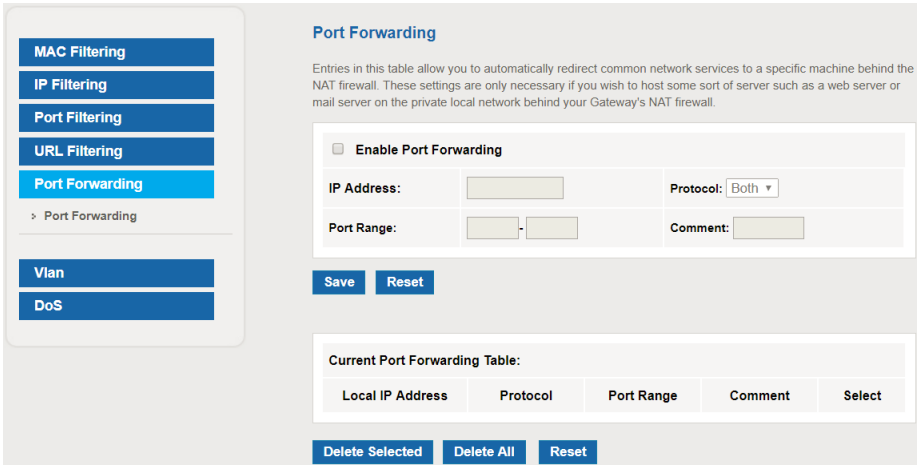
URL filtering is used to deny LAN users from accessing the internet.



Enable URL Filtering: Select this box will enable URL Filtering function.
URL Address: The URL Address that you want to filter.
Current Filter Table: The table shows all you have configured. You can delete one or all.

4.4.5 Port Forwarding

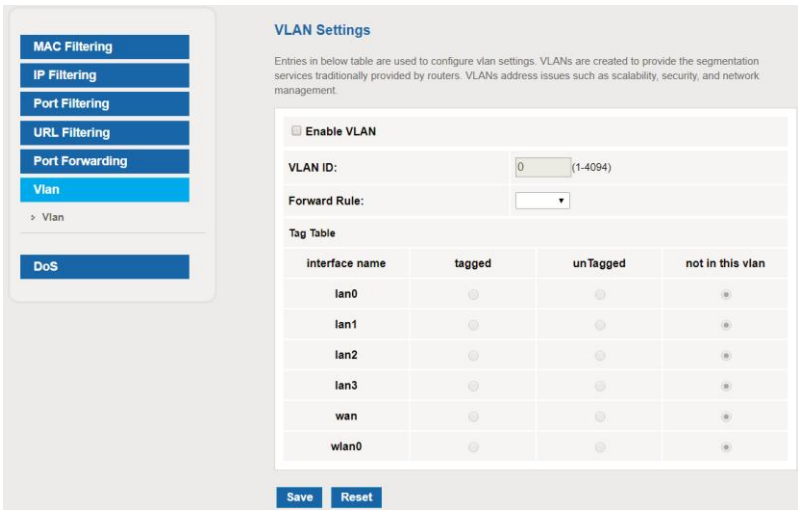
If you configure the router as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.



Enable Port Forwarding: Select this box will enable Port Forwarding function.
IP Address: That external User accesses the router will redirect to this local IP.
Protocol & Port Range: The packet with this protocol and port will be redirected to the local IP.
Comment: You can add some comment for this item.
Current Port Forwarding Table: The table shows all you have configured. You can delete one or all.

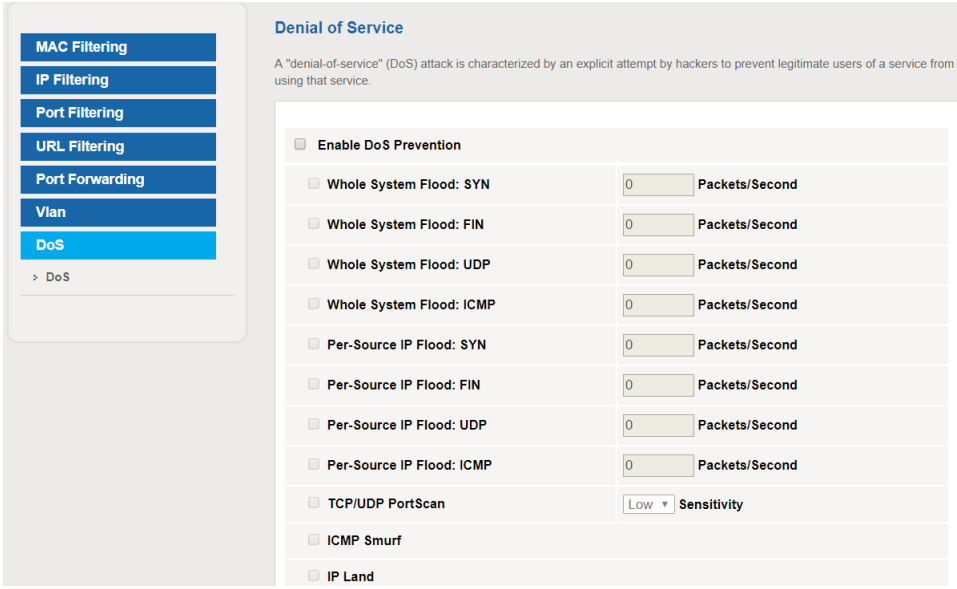
4.4.6 VLAN

VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.



4.4.7 DOS

This page used to Block DoS attack.



Enable DoS Prevention: Select this box to enable Dos Prevention.

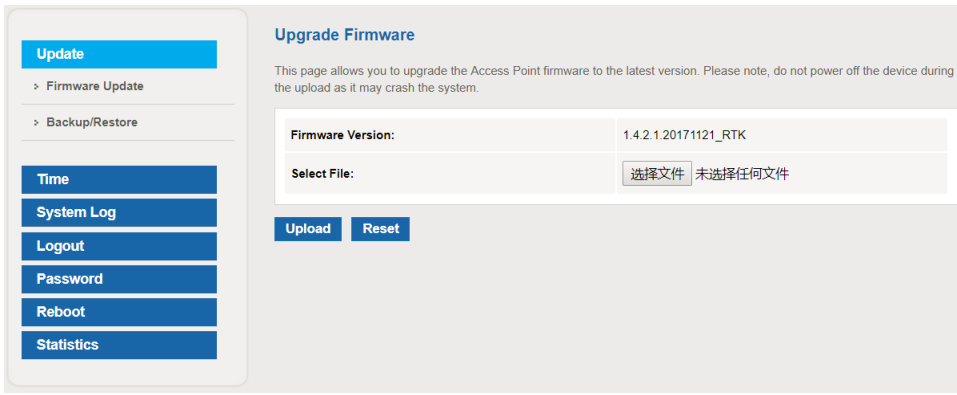
4.5 Maintenance

There are seven submenus under this menu: **Update**, **Time**, **System Log**, **Logout**, **Password, Reboot ,Statistics**. Click any of them, and you will be able to configure the corresponding function.

4.5.1 Update

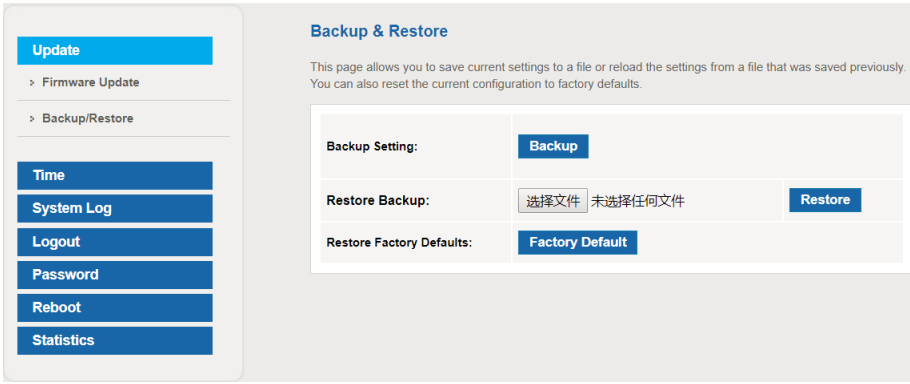
You can Upgrade, backup or restore the system configuration in this submenu

1) Firmware Update



Firmware Version: This displays current firmware version

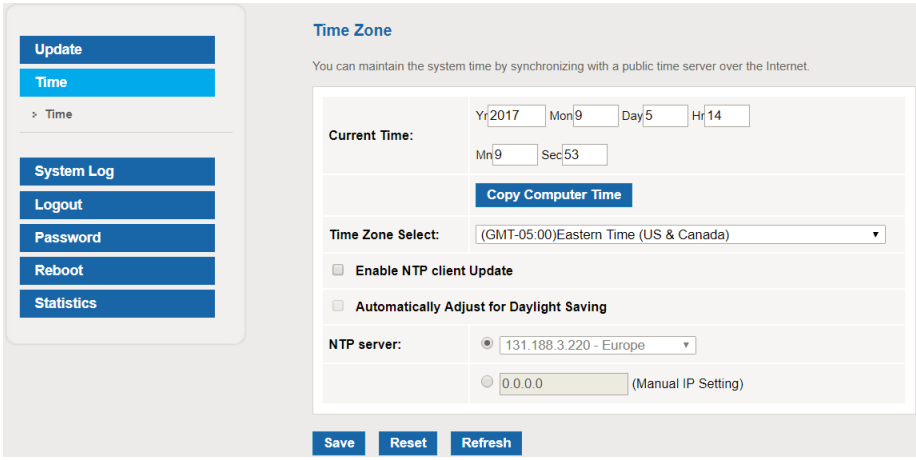
2) Backup/Restore.



Backup Settings: Get the router's settings and store it in your local computer.
Restore Backup: Restore the settings from the file you backup before from your local computer, the router will go to the former settings.
Restore Factory Defaults: Restore the system settings to factory default.

4.5.2 Time

You can maintain the system time by synchronizing with a public time server over the Internet.

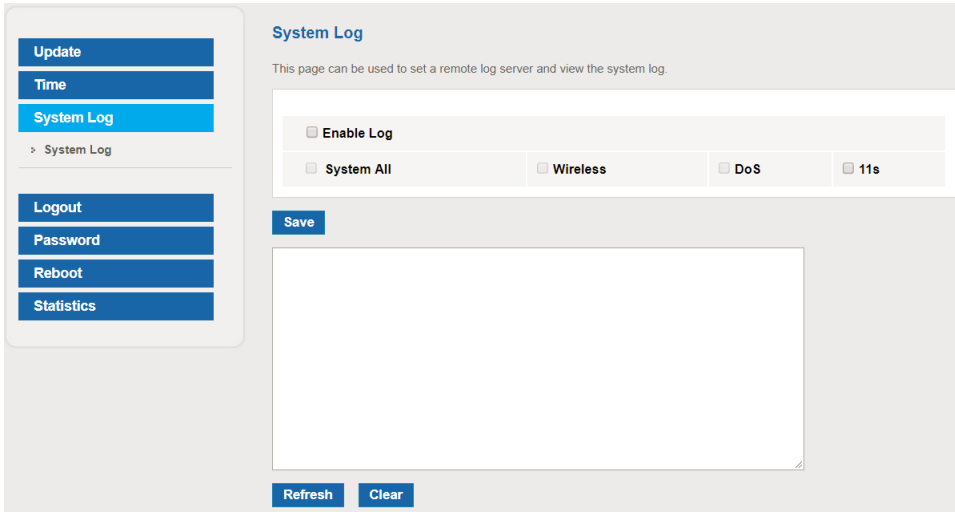


Copy Computer Time: Enter your PC's current time into the above blanks.
Time Zone select: Select your local time zone from this pull down list.
Enable NTP client Update: Select this box to connect NTP Server and synchronize internet time.
NTP Server: Select the NTP Server, then the router will get the time form the NTP Server preferentially.

4.5.3 System Log

The System Log is useful for viewing the activity and history of your router. The System Log is also used by Amped Wireless technicians to help troubleshoot your router when needed. It is recommended that you enable logs in the event that troubleshooting is required. Click the **"Refresh"** to update the log. Click **"Clear"** to clear all shown

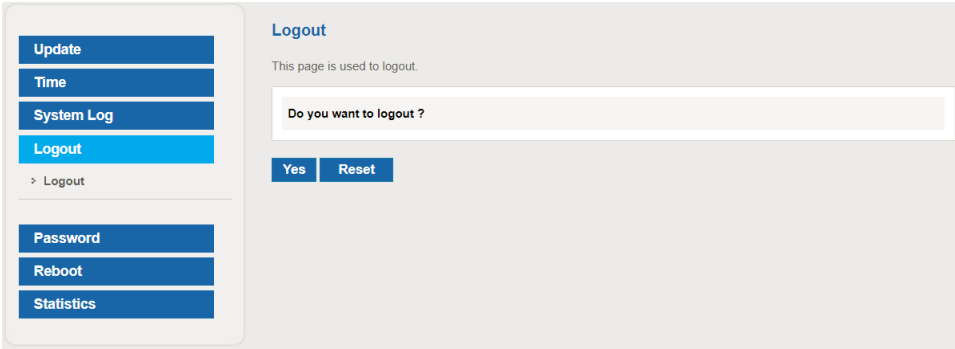
information.



Enable Log: Select this box to enable Log.

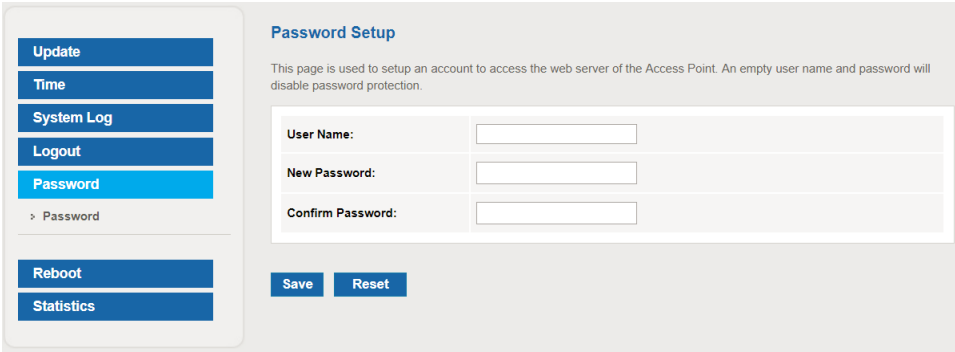
4.5.4 Logout

Choose **"Logout"**, and you will be back to the login screen.



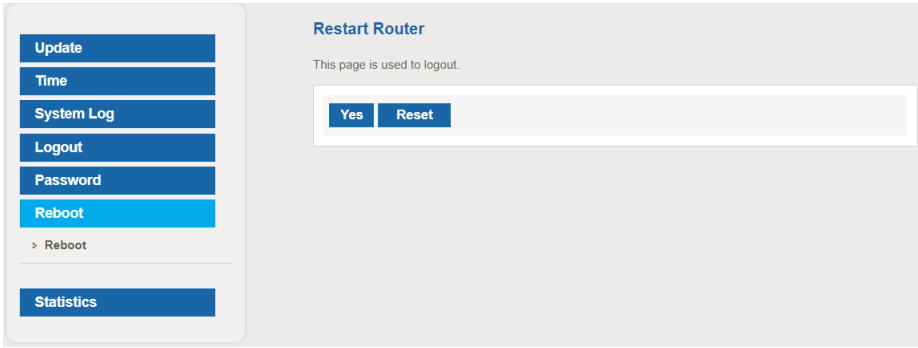
4.5.5 Password

To ensure the router's security, you will be asked for your password when you access the router's Web-based Utility. The default user name and password is **"admin"**.
This page will allow you to modify the User name and passwords.



4.5.6 Reboot

You can restart your router in this page.



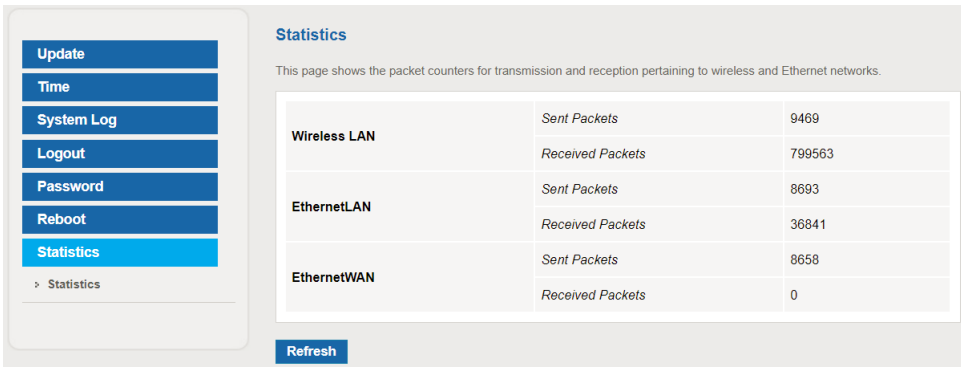
4.5.7 Statistics

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

The Wireless LAN connection statistics shows all data activity for both the 5.0GHz wireless networks.

The Ethernet LAN connection statistics shows all data activity for all users physically connected to the wired ports on the router.

The Ethernet WAN connection statistics shows the data activity for all upload and download data over your Internet connection.



Specification

Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u.
Interface Type	LAN: 4 x 10/100M RJ45 Ports(Auto MDI/MDIX) WAN: 1 x 10/100M RJ45Port(Auto MDI/MDIX) One Reset
Frequency range	2.4~2.48GHz
Radio Data Rate	11n: 300/270/243/216/162/130/108/65/13/6.5Mbps 11g: 54/48/36/24/18/12/9/6M 11b: 11/5.5/2/1M
Demodulation Mode	BPSK,QPSK,CCK and OFDM(BPSK/QPSK/16QAM/64QAM)
RF Power	21.33dBm(Max)
Antennas	2 *External 5dBi Omni Directional Antenna
Power	12V/1A
LEDs	Power, SYS,WAN,LAN(1,2,3,4), WLAN
Dimensions (W x D x H)	160x 87 x 30 (mm)
Environment	Operating Temperature： -5℃~45℃ Storage Temperature： -40~70℃ Operating Humidity： 10%~90% non-condensing Storage humidity： 5%~95% non-condensing

FCC Warning:

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.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void our authority to operate this equipment. This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference, and (2) this device must accept any interference

2) Received, including interference that may cause undesired operation.

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