Contents

Introduction ..... *- 3 -*

Section one Product Overview ..... *- 4 -*

1.1 Product Features ..... **- 4 -**

1.2 Specification ..... **- 4 -**

Section Two Hardware Installation ..... *- 6 -*

2.1 Panel layout ..... **- 6 -**

2.1.1 Front panel ..... - 6 -

2.1.2 Rear panel ..... - 7 -

2.2 System Requirements ..... **- 7 -**

2.3 Installation Environment ..... **- 7 -**

2.4 Hardware Installation Steps ..... **- 7 -**

Section Three Quick Installation Guide ..... *- 8 -*

3.1 TCP/IP configuration ..... **- 8 -**

3.2 Quick Setup wizard ..... **- 9 -**

3.3 Operation mode ..... **- 15 -**

Section four Configuration Guide ..... *- 16 -*

4.1 Login ..... **- 16 -**

4.2 Wireless Setting ..... **- 16 -**

4.2.1 Wireless Status ..... - 16 -

4.2.2 Wireless Basic settings ..... - 17 -

4.2.3 Repeater settings ..... - 17 -

4.2.4 Virtual AP settings ..... - 18 -

4.2.5 WDS Settings ..... - 18 -

4.2.6 Advanced Settings ..... - 19 -

4.2.7 Access Control ..... - 19 -

4.2.8 WPS Settings ..... - 20 -

4.3 TCP/IP Setting ..... **- 21 -**

4.3.1 LAN Status ..... - 21 -

4.3.2 WAN Status ..... - 21 -

4.3.3 LAN Interface Setup ..... - 22 -

4.3.4 WAN Interface Setup ..... - 22 -

4.4 Firewall ..... - 23 -
4.4.1 IP/Port Filtering ..... - 23 -
4.4.2 MAC Filtering ..... - 23 -
4.4.3 Port Forwarding ..... - 24 -
4.4.4 URL Filtering ..... - 25 -
4.4.5 DMZ ..... - 25 -
4.5 Management ..... - 26 -
4.5.1 QOS ..... - 26 -
4.5.2 DDNS Setting ..... - 26 -
4.5.3 Time Zone Setting ..... - 27 -
4.5.4 Denial of Service ..... - 28 -
4.5.5 Log ..... - 28 -
4.5.6 Upgrade Firmware ..... - 29 -
4.5.7 Save/Reload settings ..... - 29 -
4.5.8 Password setup ..... - 29 -

Introduction

Thank you for purchasing the 11N Wireless Broadband Router. This user guide will assist you with the installation procedure.

WR353ND router is a hybrid design product which combines Ethernet technology and wireless access into a single stand-alone unit. The device allows you to take advantages of both mobility and fast connection. All PCs whenever on wireless LAN or Ethernet LAN can share files, printers and other network resources. Moreover, all users can share single account of Internet access by having this device connect to a DSL/Cable modem.

It complies with IEEE 802.11n (Draft 2.0) standards, supports up to 150Mbps (1Tx-1Rx) wireless connection speed, adopting MIMO technology to ensure a good performance, stability and coverage to bring you an enjoyable new experience. It's wireless data transmission rate can be 3 times better and coverage 4 times better than a normal 802.11g/b router. It is a high performance and cost-effective solution for Home and Small office.

The router provides multiple security protection, which can protect the wireless access security effectively. It is easy to install and configure with user friendly interface. For better application of the router functions, please read this user manual carefully.

Package List

Open the box carefully, check the contents listed below:

- Wireless Broadband Router
- Power adapter
- User Manual
- UTP Lan Cable
- 2x 5dBi antenna
- CD

Note: If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the Wireless Router for assistance

Section one Product Overview

1.1 Product Features

- Complies with IEEE 802.11n, 802.11g, 802.11b standard for 2.4GHz Wireless LAN
- 1 10/100M WAN RJ45 port, 4 10/100M LAN RJ45 ports
- Supports Auto MDI/MDIX
- Supports Wireless Roaming, can move among different AP and no break
- Provides 64/128 bit WEP, WPA and WPA2 authentication and TKIP/AES encryption security
- Supports wireless Relay/Bridging/WDS/WDS+AP mode, WPS Settings .
- Provides wireless LAN ACL (Access Control List) filtering
- Built-in NAT and DHCP server supporting dynamic IP address distributing
- Supports Virtual Server, Special Application, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT
- Supports UPnP, Dynamic DNS, Static Routing,
- Supports Flow Statistics
- Firmware upgrade, and configuration file backup and restore
- Supports Remote and Web management

1.2 Specification

Standard	IEEE802.11n current draft、IEEE 802.11g、IEEE 802.11b IEEE 802.3、IEEE 802.3u、IEEE 802.3x
Protocol	CSMA/CA、CSMA/CD、TCP/IP、ICMP、NAT、PPPoE、 DHCP、PPTP、UDP、NAT、DNS、DDNS、VPN
Port LAN	4*100BaseTX (Auto MDI/MDIX)
Port WAN	1*100BaseTX (Auto MDI/MDIX)
RF Frequency	2.4~2.4835GHz
Data Rate	11n: 150/135/121.5/108/81/54/40.5/27/13.5Mbps 130/117/104/78/52/39/26/13Mbps 72/65/58.5/52/39/26/19.5/13/6.5Mbps 11g: 54/48/36/24/18/12/9/6Mbps 11b: 11/5.5/2/1Mbps
Receive Sensitivity	135M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Channels	1-11 (North America) 1-13 (General Europe) 1-14 (Japan)
Transmission Technology	BPSK, QPSK, CCK and OFDM (BPSK/QPSK/16-QAM/ 64-QAM)
Antenna Type	2*2.4GHz Dipole Antenna（1TX*1RX）
Operation Mode	Standard Access Point; Wireless WAN mode (Client Mode Wireless), WDS, WPS

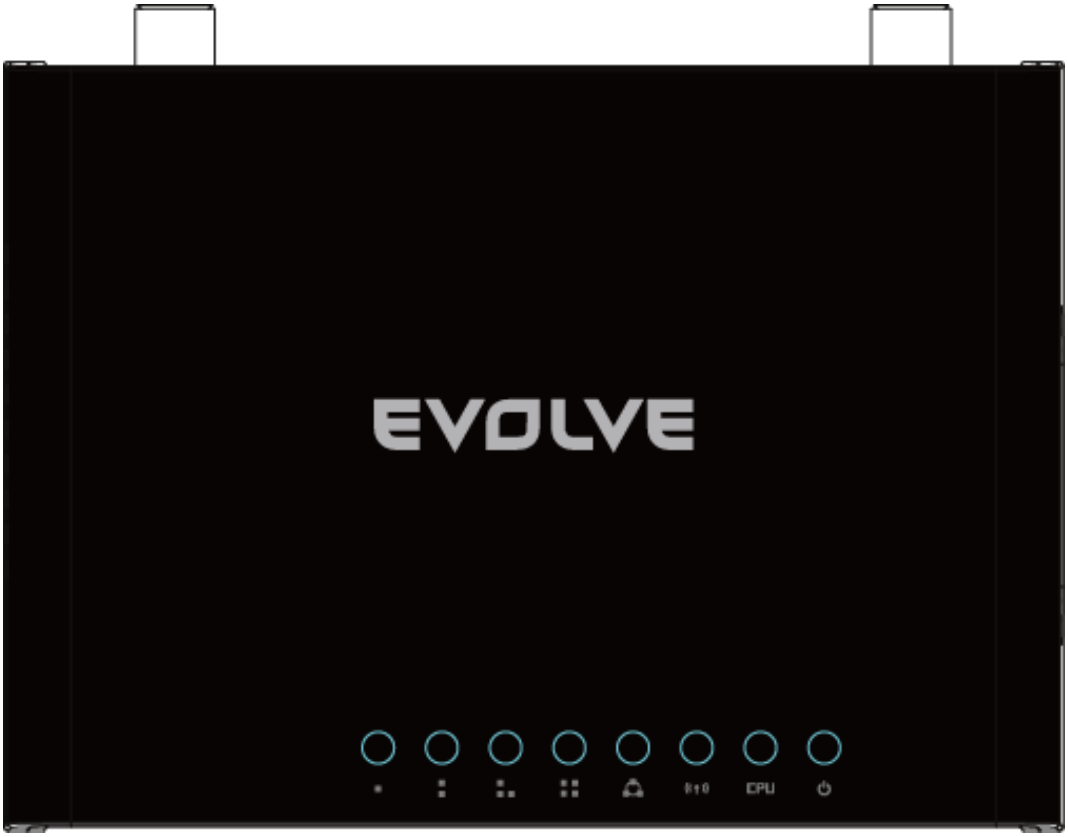
Wireless Security	SSID Enable/Disable; MAC Address, IP and URL Filter ; 64/128/152-bit WEP Encryption WPA/WPA2/WPA-PSK/WPA2-PSK (AES/TKIP) Encryption
RF power	11g:14-16dbm 11b:17-19dbm 11n:13-15dbm
Chipset	RTL8196BU+8191RE
LED	1*Power, 1*CPU Status,1*Wireless, 1*WAN, 4*LAN
Management	Local/Remote Web-based configuration
Operating Temperature	0 ~ 55°C
Storage	-20 ~ 65°C
Humidity	5 ~ 95% non-condensing
External Power Adapter	Input 100V~240V Output DC5V 1A;

Section Two Hardware Installation

2.1 Panel layout

2.1.1 Front panel

The front panel of the 11N Wireless Router consists of several LED indicators, which is designed to indicate connections.



LED indicators:

Led Name	Action	Description
Power	off	no power
	on	power on
CPU	off	the router has a hardware error
	flashing	the router is working properly
WLAN	off	wireless function is disabled
	flashing	wireless function is enabled
WAN /LAN1 、2、3、4	off	there is no device connected to the corresponding port
	on	there is a device connected to the corresponding port
	flashing	there is an active device connected to the corresponding port

2.1.2 Rear panel

2.2 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (you do not need it if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft IE 5.0 or later, Netscape Navigator 6.0 or later

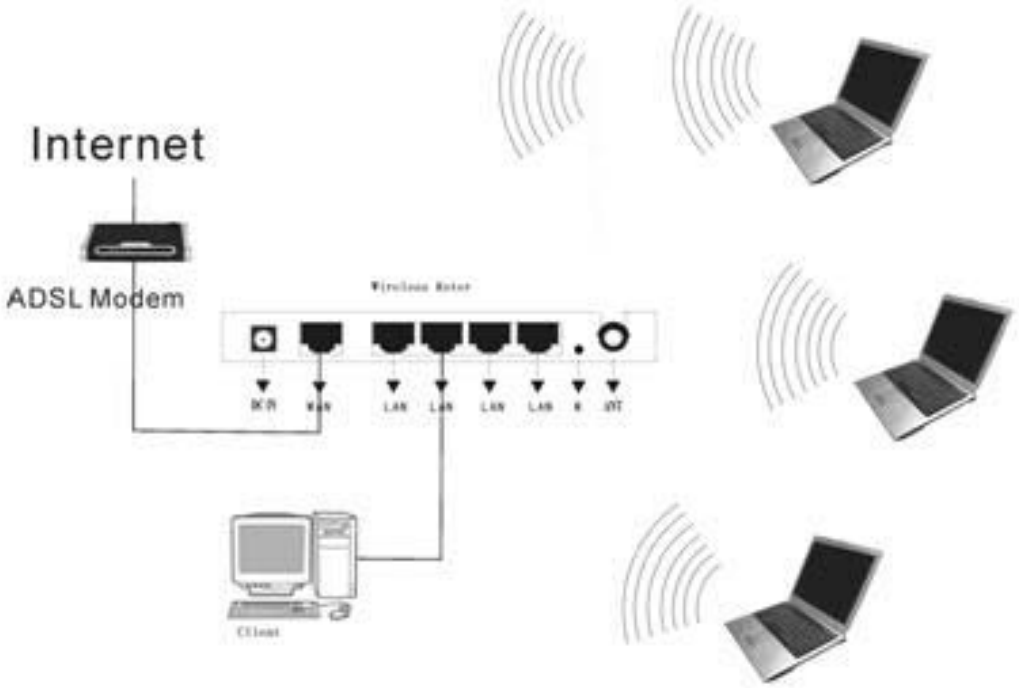
2.3 Installation Environment

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0□~40□
- Operating Humidity: 5%~90%RH, Non-condensing

2.4 Hardware Installation Steps

Before you install the router, you should connect your PC to the Internet through your 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.

- Power off your PC(s), Cable/DSL modem, and the router.
- Locate an optimum location for the router. The best place is usually near the center of the area in which your PC(s) will wirelessly connect. The place must accord with the Installation Environment Requirements.
- Adjust the direction of the antenna. Normally, upright is a good direction.
- Connect the PC(s) and each Switch/Hub on your LAN to the LAN Ports on the router.
- Connect the DSL/Cable Modem to the WAN port on the router.
- Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
- Power on your PC(s) and Cable/DSL modem.



Section Three Quick Installation Guide

After connecting the 11N Wireless Router into your network, you should configure it. This chapter describes how to configure the basic functions of your 11N Wireless Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configured.

3.1 TCP/IP configuration

The default IP address of the Wireless Router is 192.168.1.1, and the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

Connect the local PC to the LAN ports on the router. There are then two means to configure the IP address for your PC.

- **Configure the IP address manually**

1. Set up the TCP/IP Protocol for your PC(s).

2. Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1(The router's default IP address)

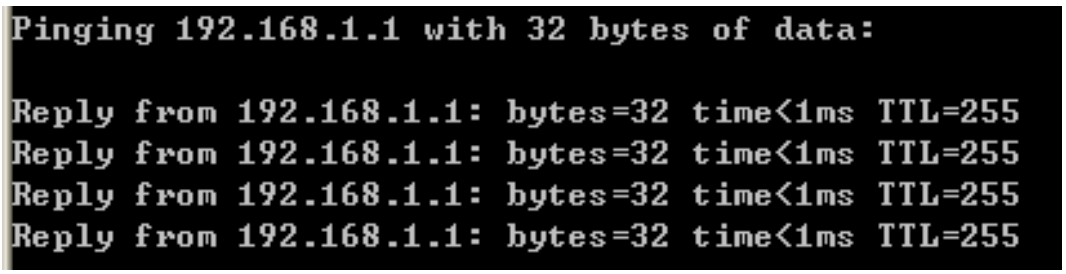
- **Obtain an IP address automatically**

1. Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC(s)

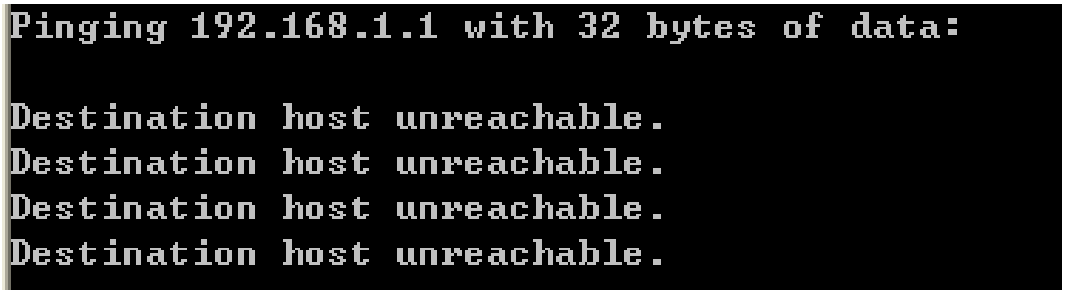
2. Power off the router and PC(s). Then turn on the router, and restart the PC(s). The built-in DHCP server will assign IP addresses for the PC(s).

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC(s) and the router.

Open a command prompt, and type ping **192.168.1.1**, then press **Enter.**



If the result displayed is similar to that shown in the top of figure, the connection between your PC and the router has been established.



If the result displayed is similar to that shown in the top of figure, it means that your PC has not connected to the router. Please check it following these steps:

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

Notice: The 1/2/3/4 LEDs of LAN port on the router and LEDs on your PC's adapter should be lit

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

Notice: If 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

3.2 Quick Setup wizard

With a Web-based (Internet Explorer or Netscape® Navigator) utility, the 11N 150bps Wireless Router is easy to configure and manage. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

Connect to the router by typing *http://192.168.1.1* in the address field of web browser.

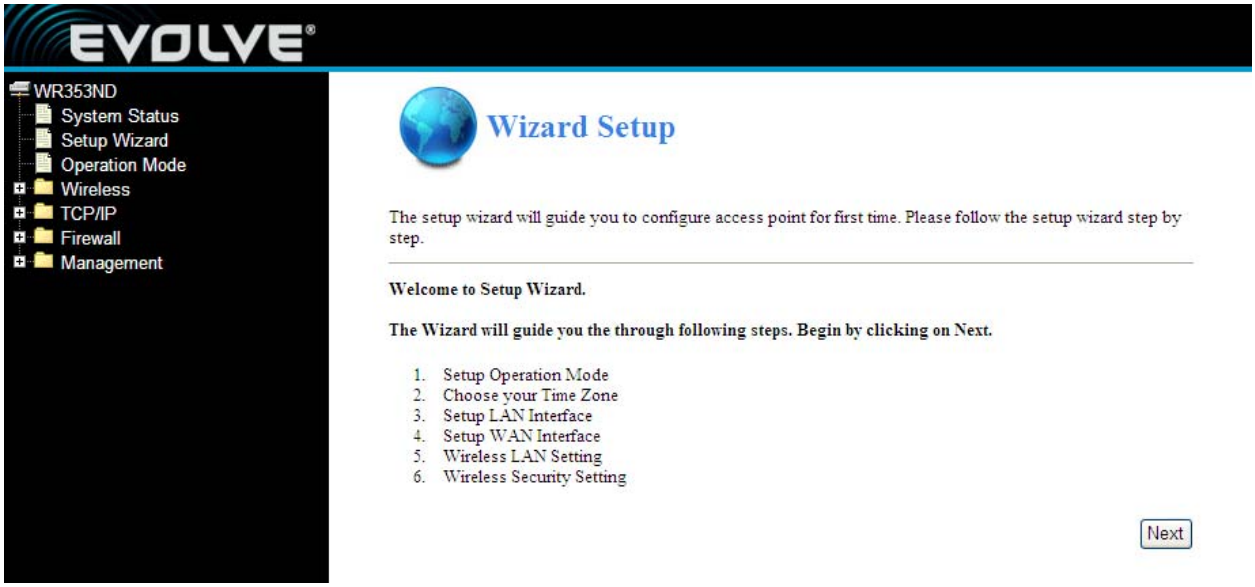
After a moment, a login window will appear similar to that shown in Figure. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

NOTE:

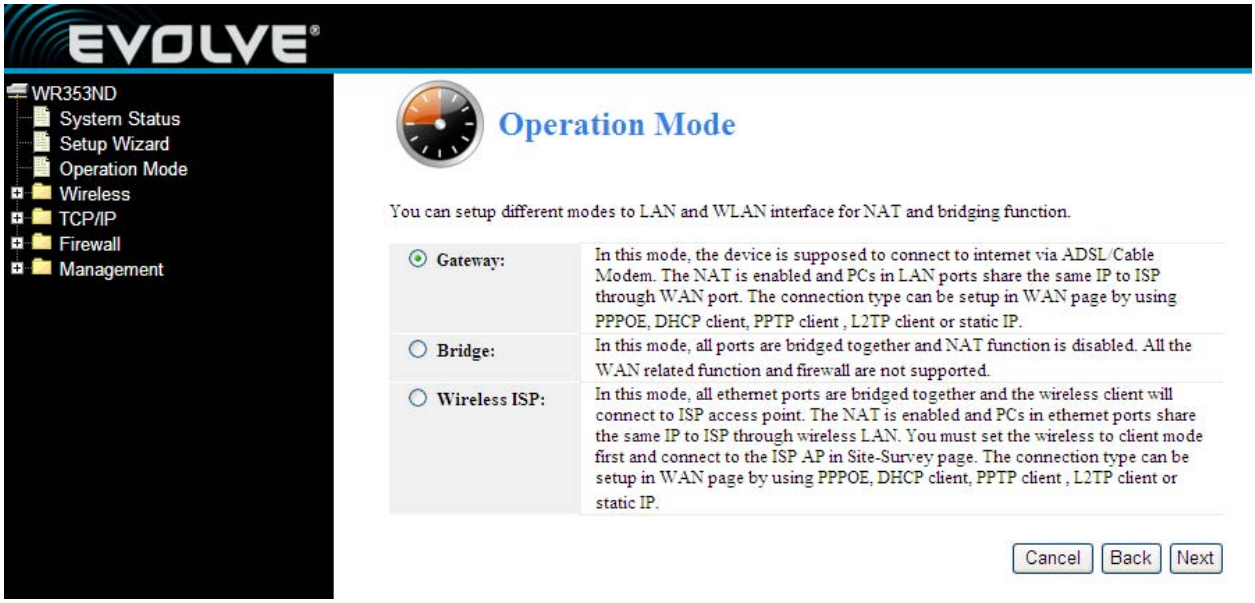
If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

If the User Name and Password are correct, you can configure the router using the web browser. Please click the Setup Wizard link on the left of the main menu and the Setup Wizard screen will appear.

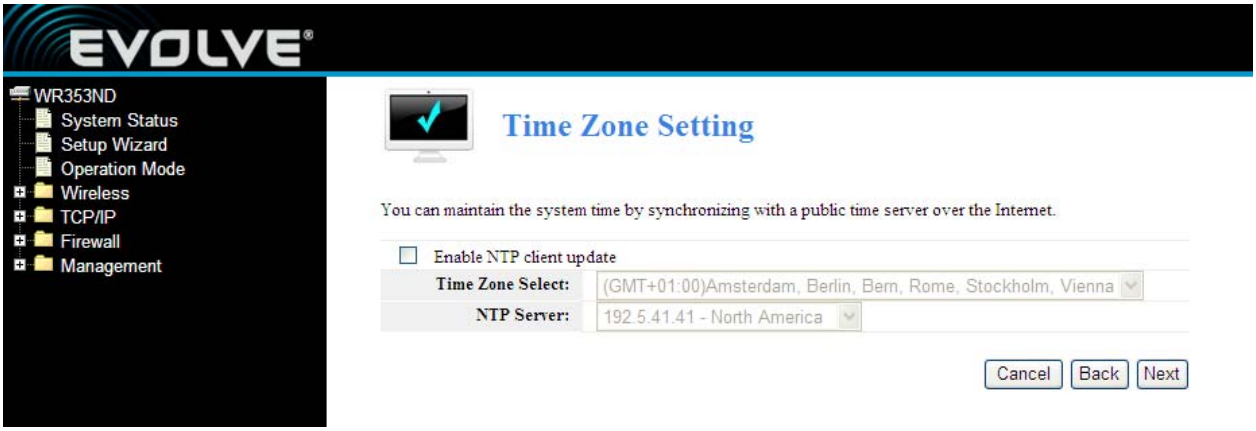
Click **Setup Wizard**, the **Setup Wizard** will appear.



The router supports three modes: gateway, bridge, wireless ISP. You can setup different modes to LAN and WLAN interface for NAT and bridging function.



Click **next**, **Time Zone Setting** will appear. You can select the time zone what you need.

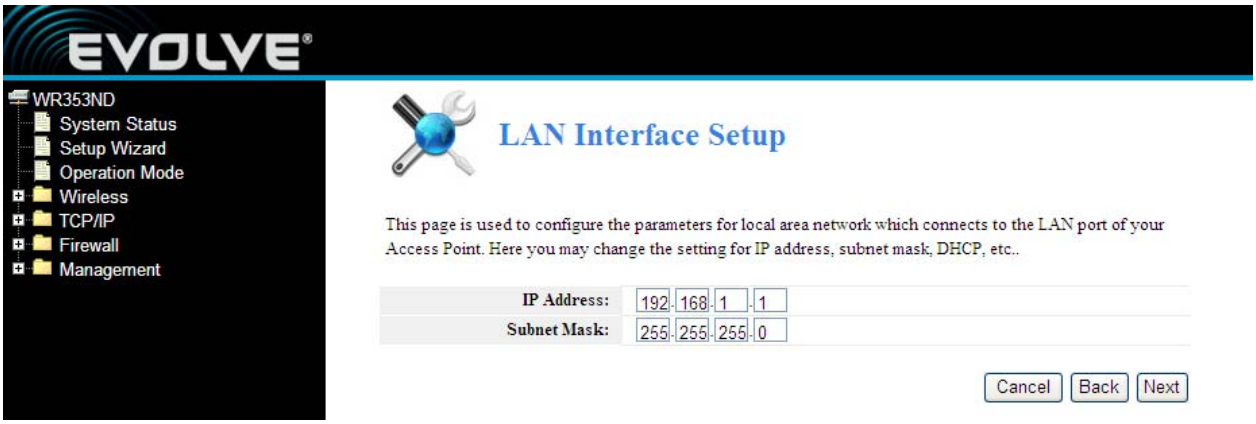


Click **next**, **LAN Interface setup** will appear. In this page, you can set IP address, Subnet Mask.

IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).

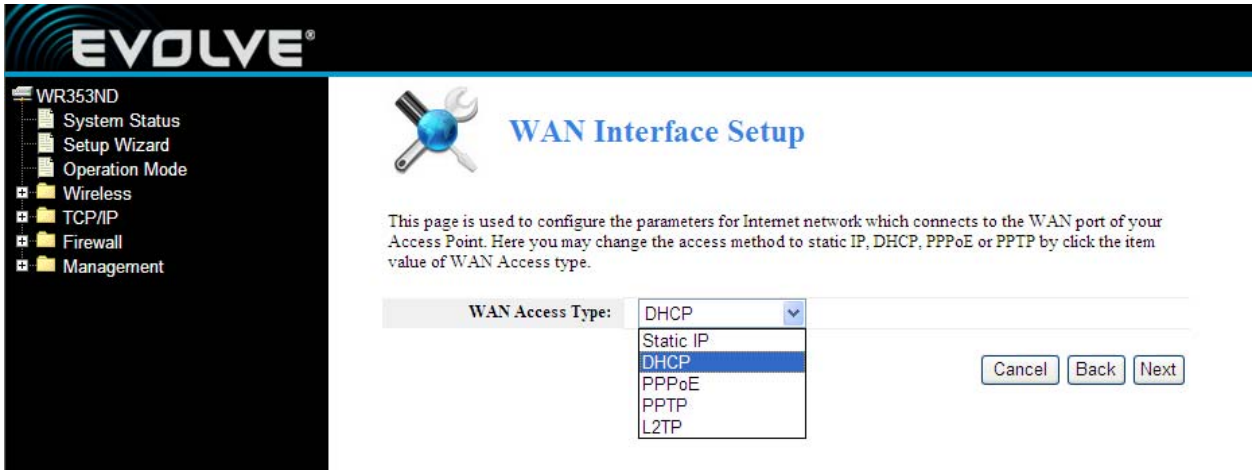
Subnet Mask - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Notice: All PCs' Subnet Mask is the same with router in you LAN.

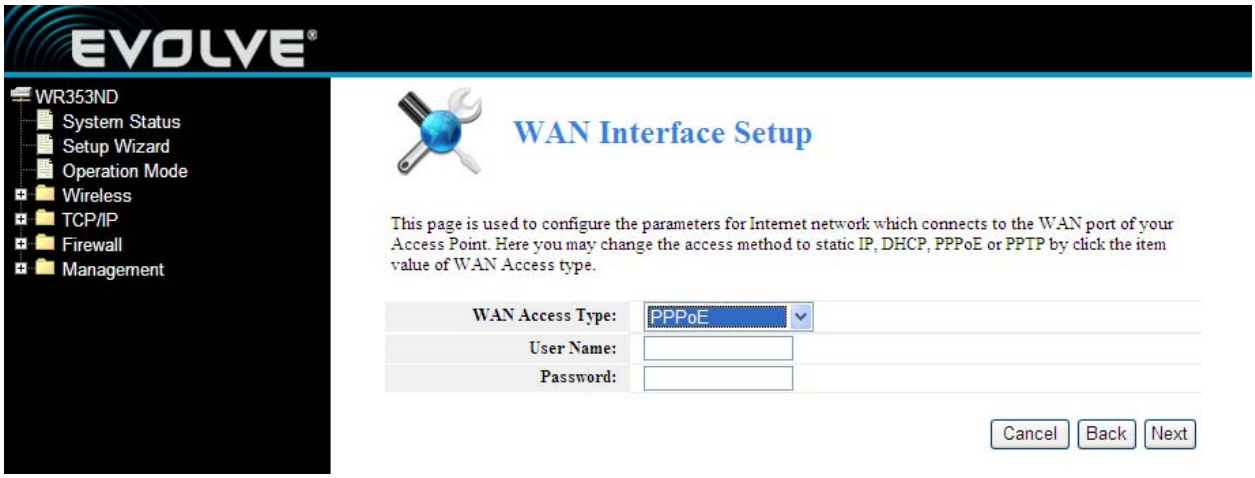


Click **next**, **WAN Interface Setup** will appear. In this page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.

WAN Access Type: Here you can select the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.



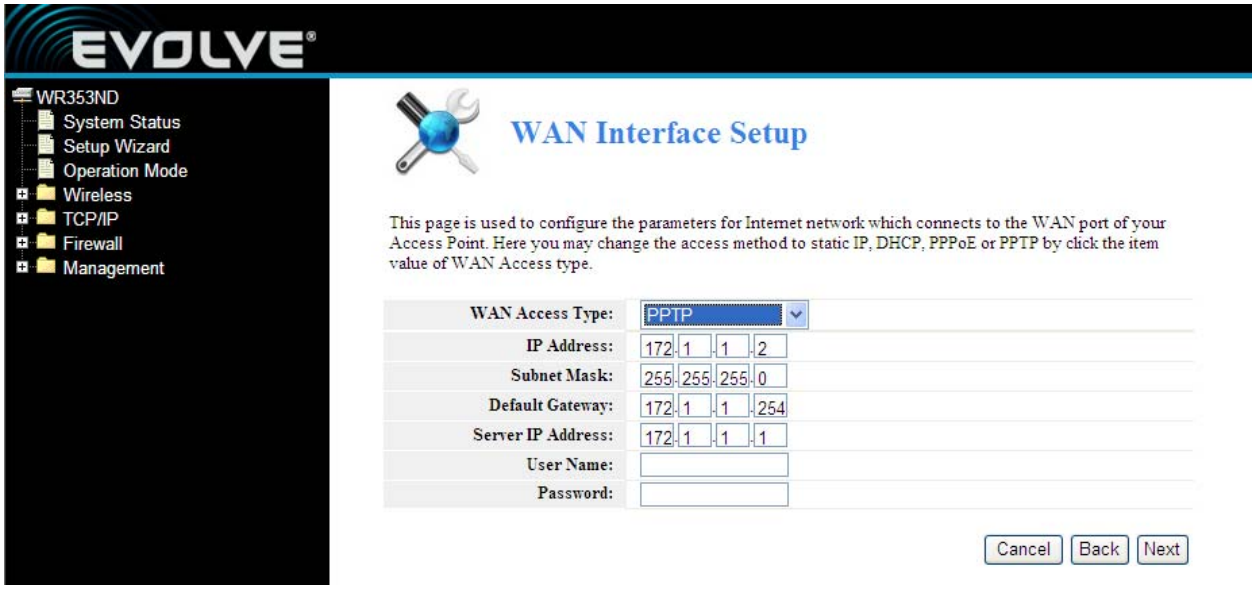
If you choose "**PPPoE**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.



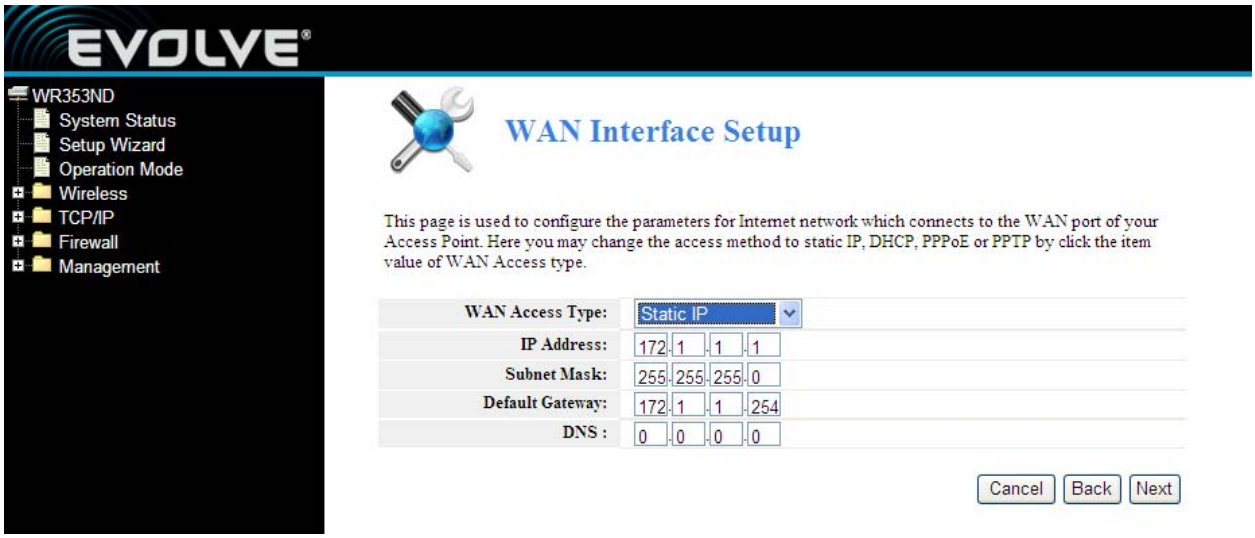
User Name and **Password -** Enter the **User Name** and **Password** provided by your ISP.

If you choose " **DHCP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose "**PPTP**", the Static IP settings page will appear, shown in the figure.



You can get IP Address Subnet Mask, server IP Address, User Name and Password from your ISP. If you Choose "**Static IP**", the Static IP settings page will appear, shown in figure.



Notice: The IP parameters should have been provided by your ISP.

IP Address - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.

Subnet Mask - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0

Default Gateway - Enter the gateway into the box if required.

DNS - Enter the DNS Server IP address into the boxes if required.

Click **next**, **Wireless Basic Setting** will appear.

【This page is used to configure these parameters】

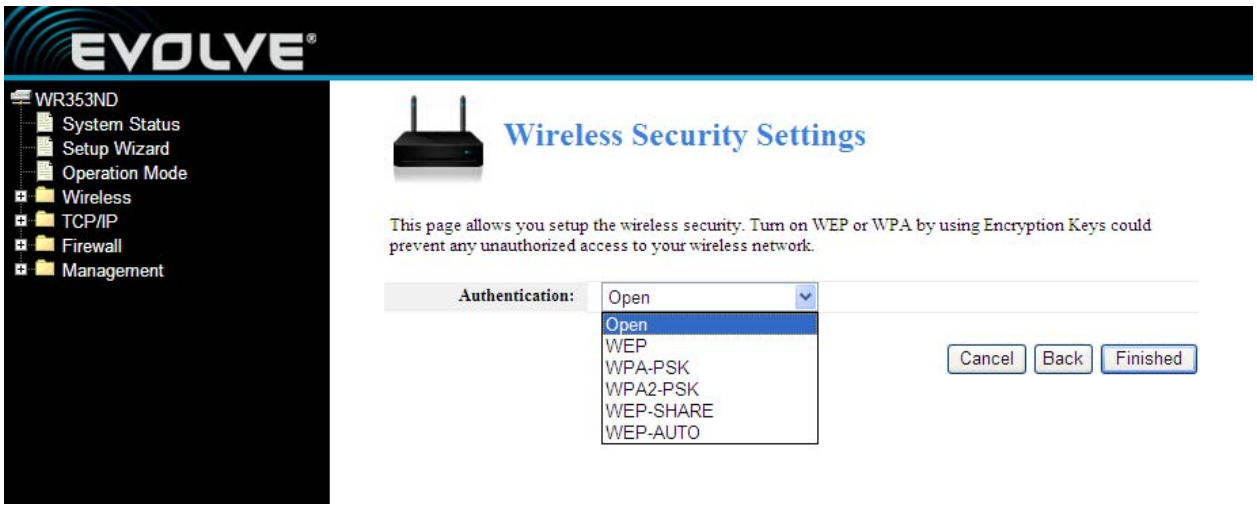
Band - Indicates the current mode 2.4GHz(B+G+N) , 2.4GHz(G+B), 2.4GHz(B)

Mode- Default is AP, you can select Infrastructure Client or AP

SSID - Enter a value of up to 32 characters. The default SSID is WR353ND, but it is recommended strongly that you change your networks name (SSID) to a different value.

Channel –This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you meet interference problems with another nearby access point.

Click **next**, **Wirelss Security Settings** will appear. This page allows you to setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network. You can select Open, WEP, WPA-PSK, WPA2-PSK.



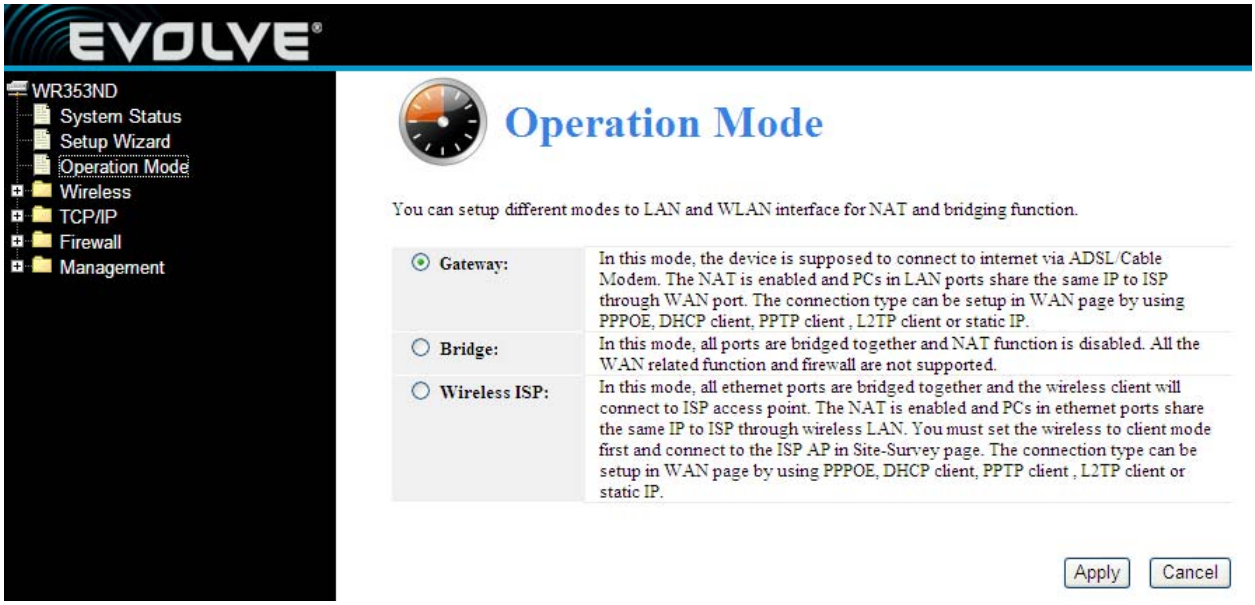
Click **Finished** to finish the configuration

Notice: If you change the parameters of wireless, The router will reboot automatically.

WPA-psk： Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode

WPA2-psk： (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access).

3.3 Operation mode



Gateway : (default) In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

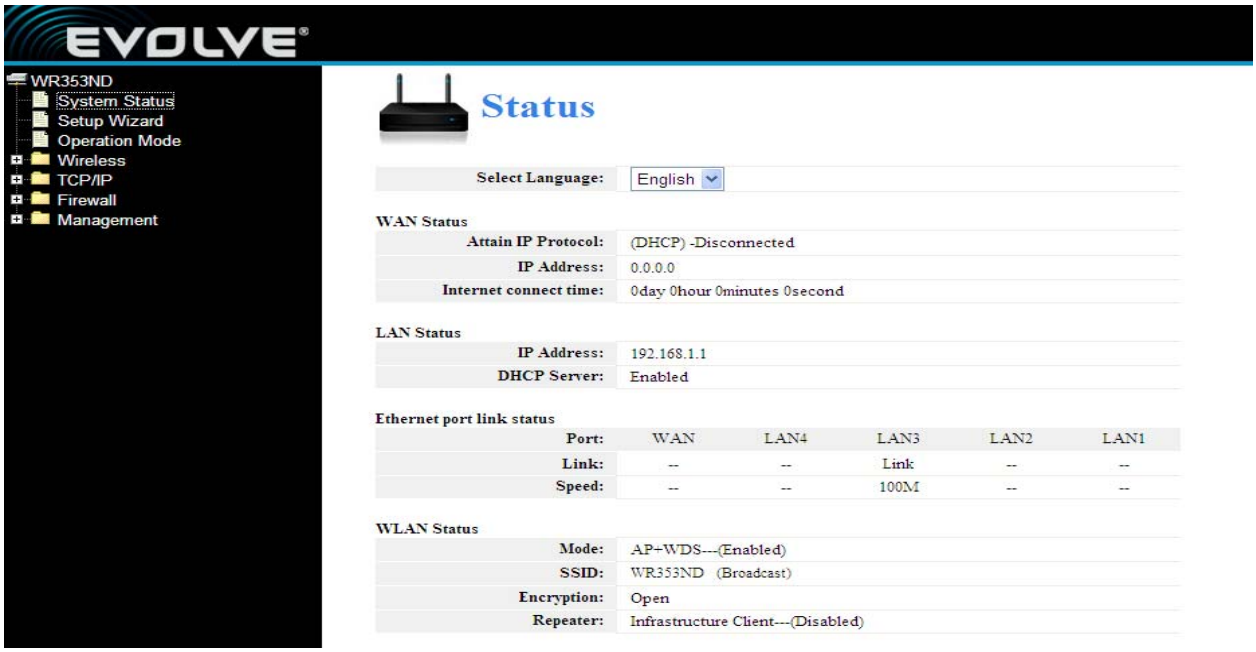
Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP..

Section four Configuration Guide

4.1 Login

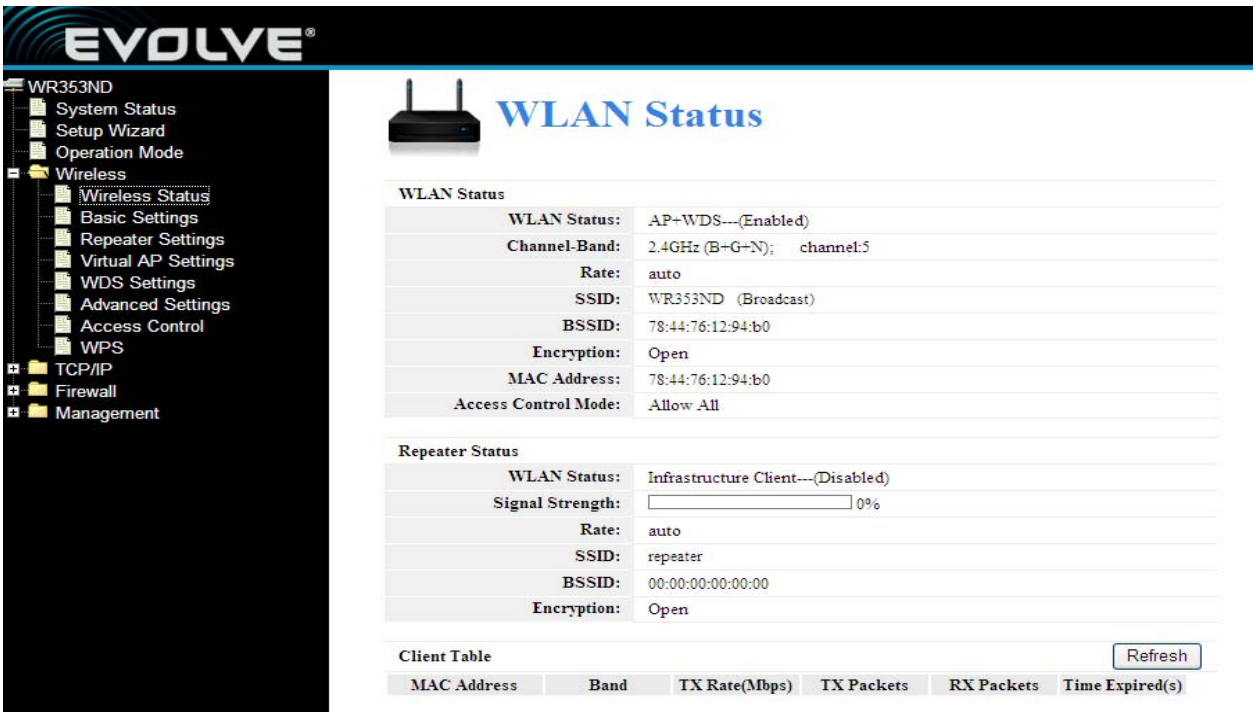
After you login successful, Browser will show administrator WEB. on the left is contents. it contains: Wireless setting, WAN Settings, LAN Settings, Network Security, System Services, Management, Status Show ect..



4.2 Wireless Setting

It contains Wireless Basic settings, Repeater settings, Virtual AP settings, WDS Settings, Advanced Settings, Access Control and WPS

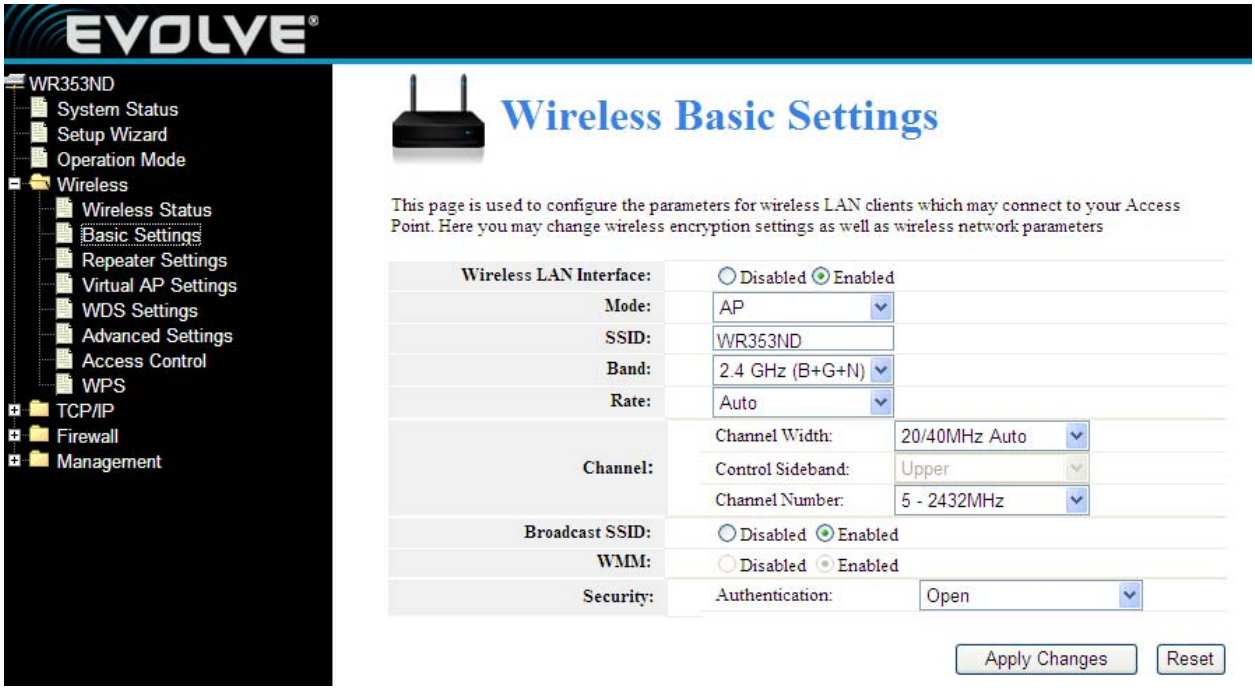
4.2.1 Wireless Status



This page shows the current status and some basic settings of the device. you can check system Information, Repeater Interface Information, WLAN Interface Information.

4.2.2 Wireless Basic 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.



WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window

Security： From the drop-down menu select the corresponding security encryption modes.

WEP ： Set the WEP key with the format of ASCII and Hex. You can enter ASCII code (5 or 13 ASCII characters. Illegal character as “/” is not allowed.) Or 10/26 hex characters..

4.2.3 Repeater settings

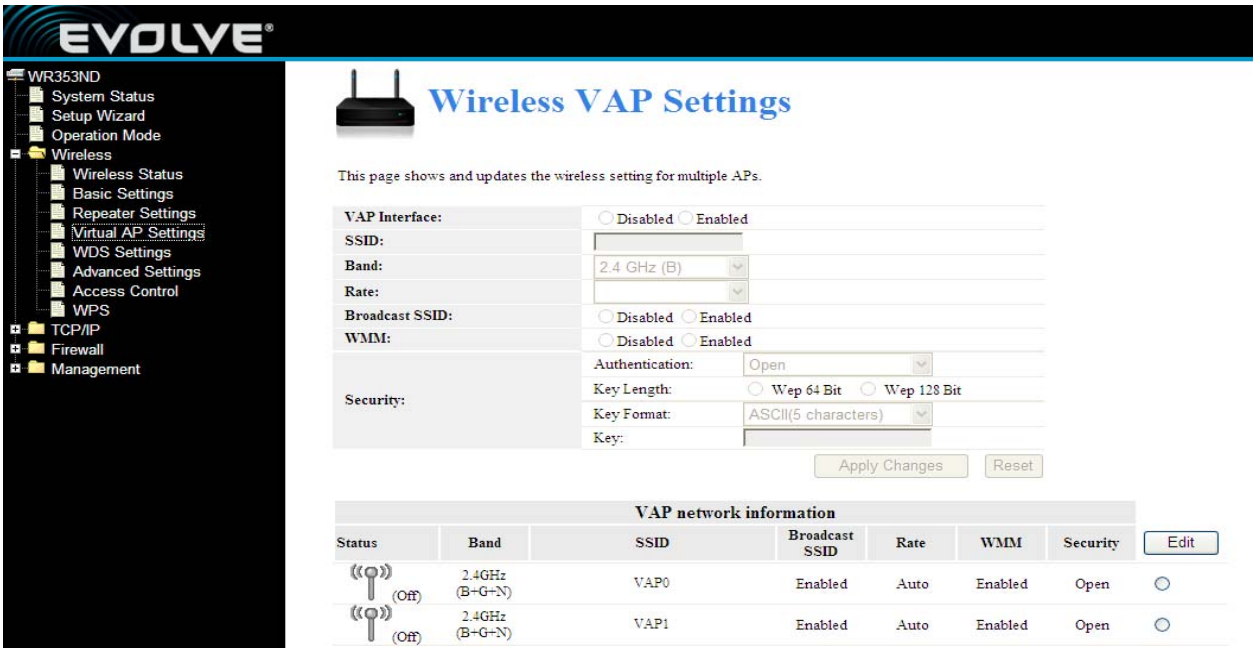
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Mode: Default is AP

SSID: Enter a value of up to 32 characters. The same name (SSID) must be signed to all wireless devices in your network. The default SSID is repeater, but it is recommended strongly that you change your networks name (SSID) to a different value.

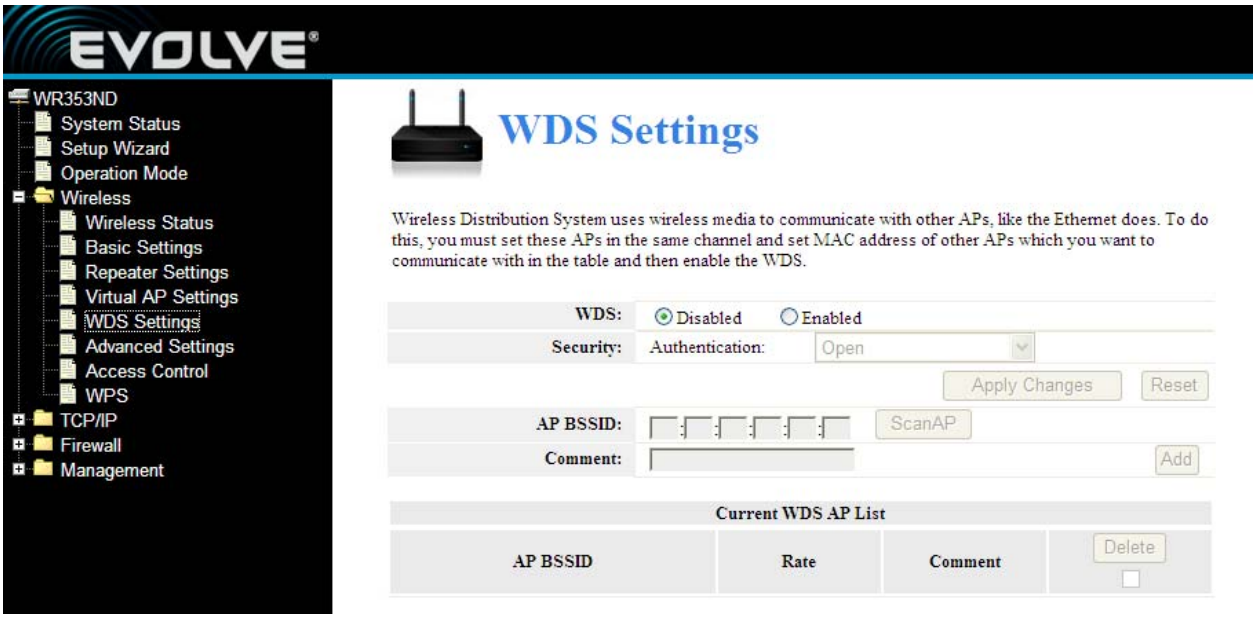
Channel: This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

4.2.4 Virtual AP settings



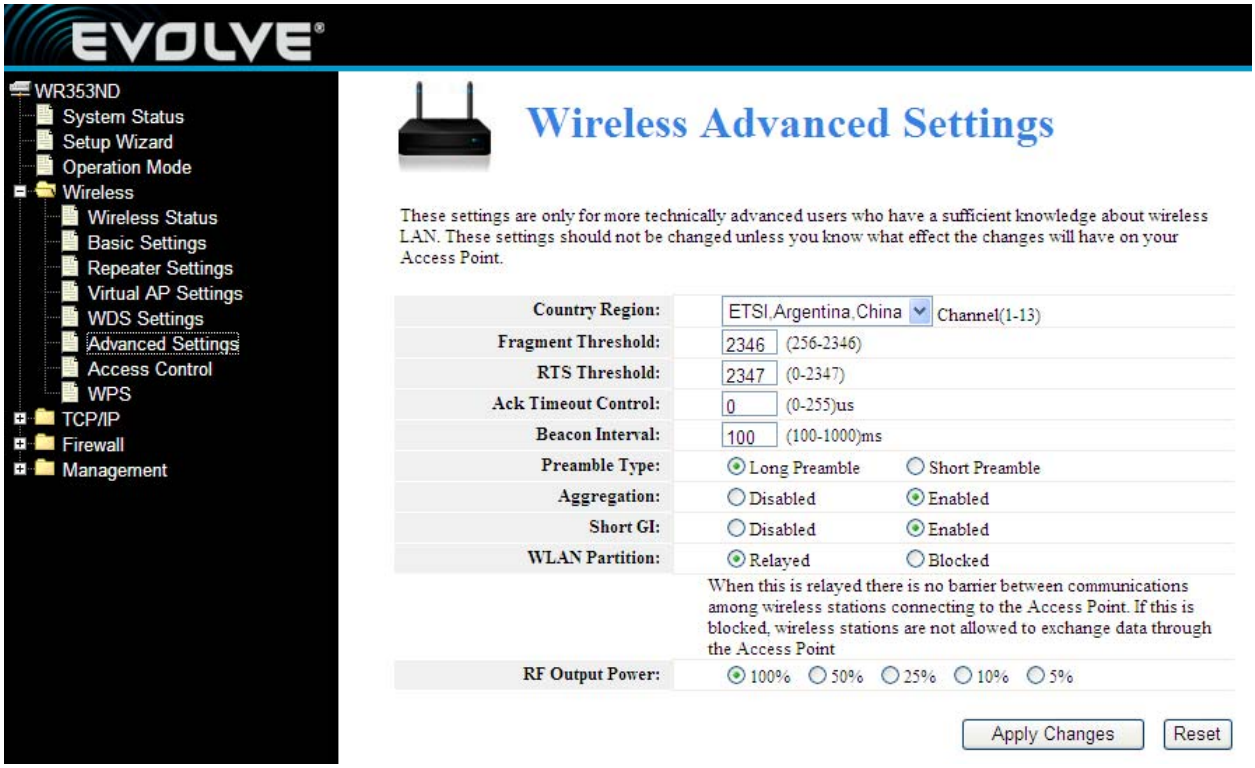
This page shows and updates the wireless setting for multiple Aps

4.2.5 WDS Settings



Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, 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.

4.2.6 Advanced Settings



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.

4.2.7 Access Control

If you choose 'Allow Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

4.2.8 WPS Settings

WPS (Wi-Fi Protected Setting) can easily and quickly establish the connection between the wireless network clients and the device through an encrypted way. The users only enter PIN code or press RST/WPS button on the panel to configure it. In the “Wireless settings” menu, click “WPS settings” to enter the next screen.

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

WPS ： To enable or disable WPS function. The default is “disable”.

Self –PIN Number: The effective key generated by AP automatically.

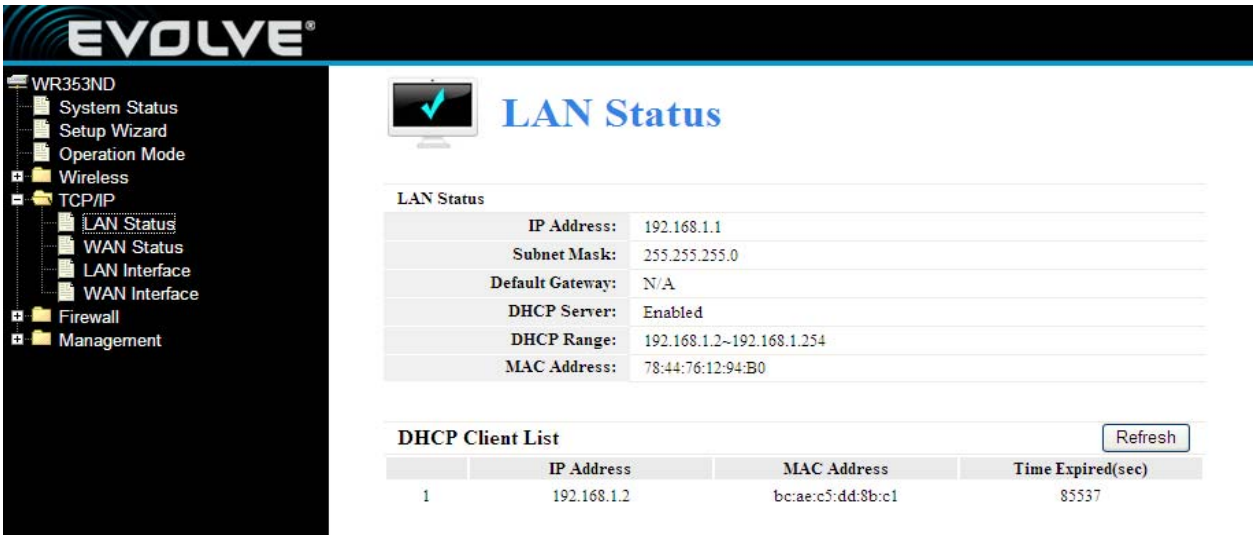
Push-Button Configuration： Provide two ways: PBC (Push-Button Configuration) and PIN code.

PBC： Select the PBC or press the RST/WPS button on the front panel of the device for about one second (Press the button for about one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. Two minutes later, the WPS indicator will be off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports up to 32 clients access.)

Client PIN Number： If this option is enabled, you need to enter a wireless client’s PIN code in the field and keep the same code in the WPS client.

4.3 TCP/IP Setting

4.3.1 LAN Status



This page shows the current status and some basic settings of the device. you can check system Information, LAN Interface Information

MAC Address - the physical address of the router, as seen from the LAN. The value can't be changed.

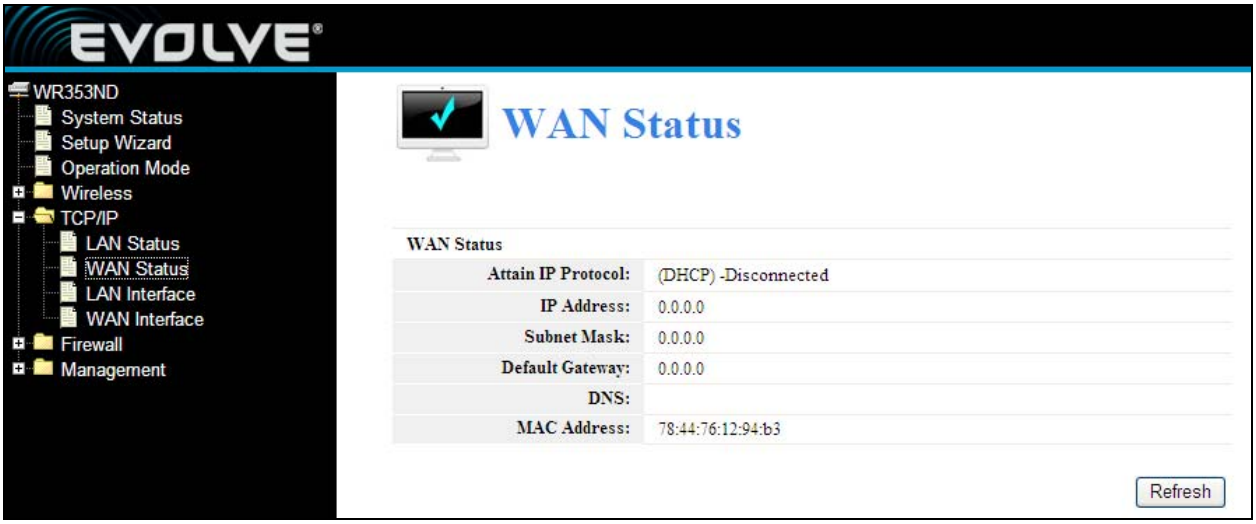
IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).

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

DHCP: You can select None, Client, Serve. The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.

DHCP Client Range: This field specifies the first of the addresses in the IP address pool.

4.3.2 WAN Status



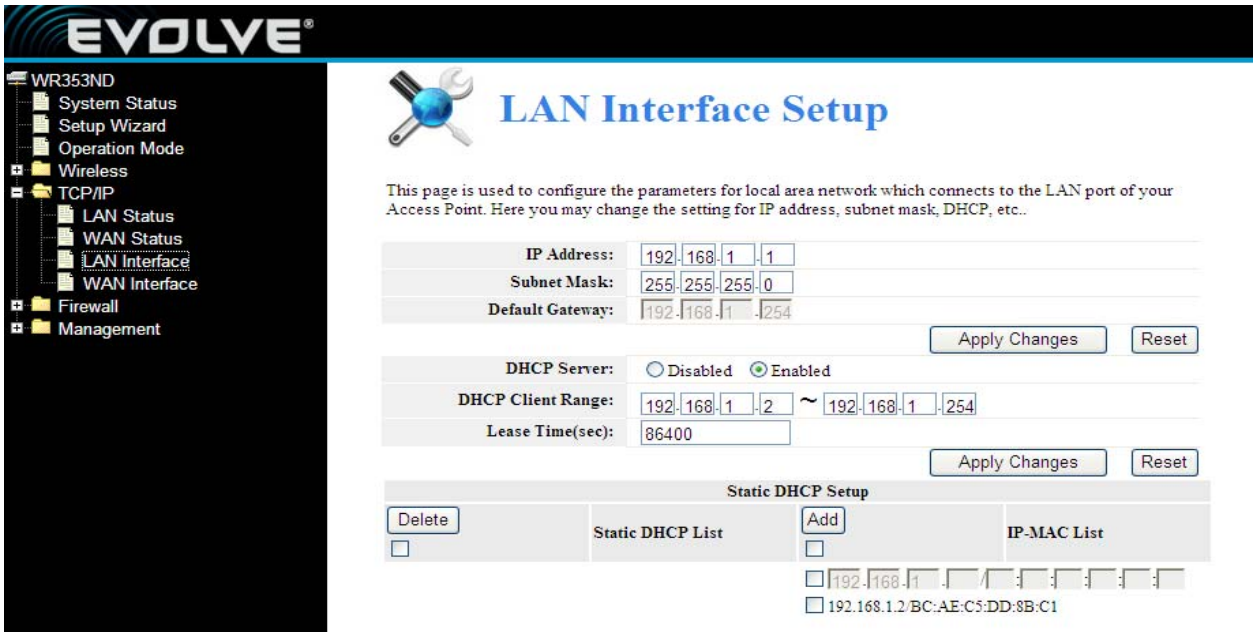
This page shows the current status and some basic settings of the device. you can check system Information, WAN Interface Information.

MAC Address - the physical address of the router, as seen from the LAN. The value can't be changed.

IP Address - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).

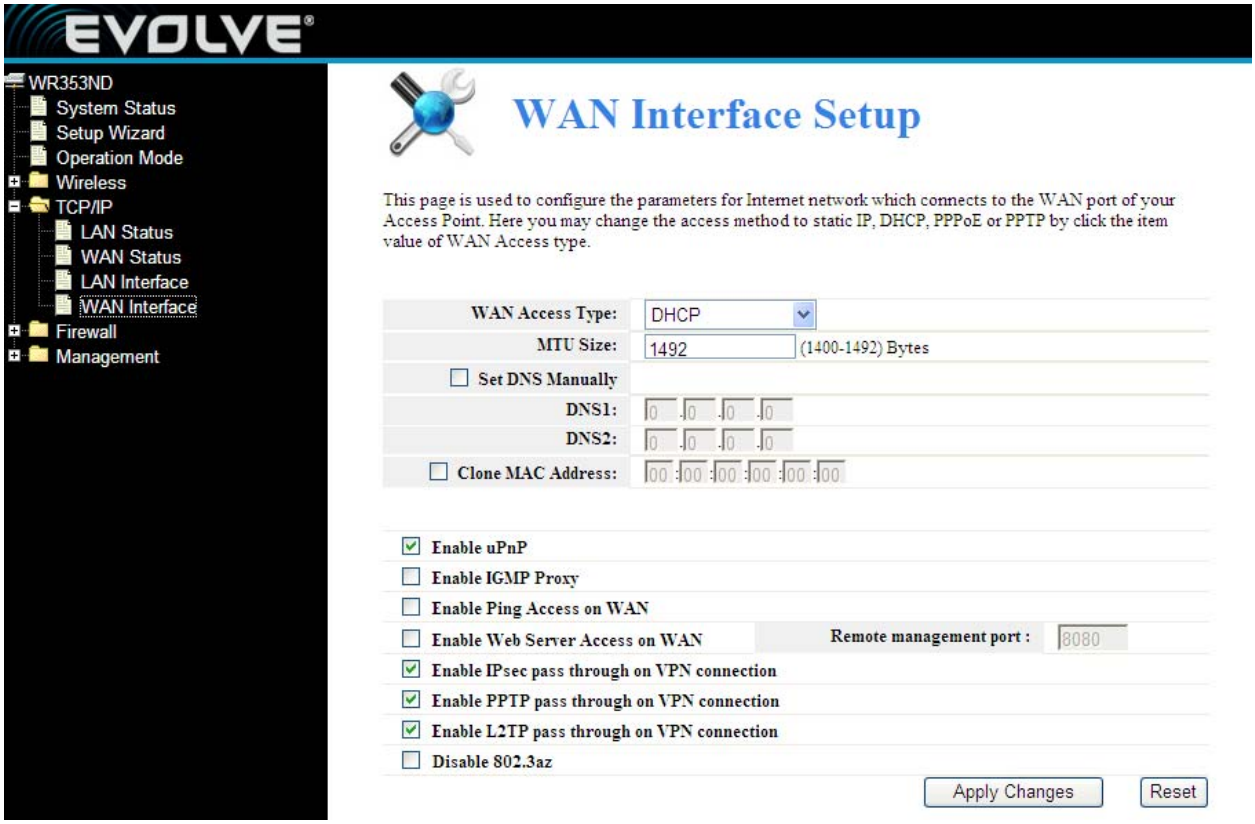
Subnet Mask- An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

4.3.3 LAN Interface Setup



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.

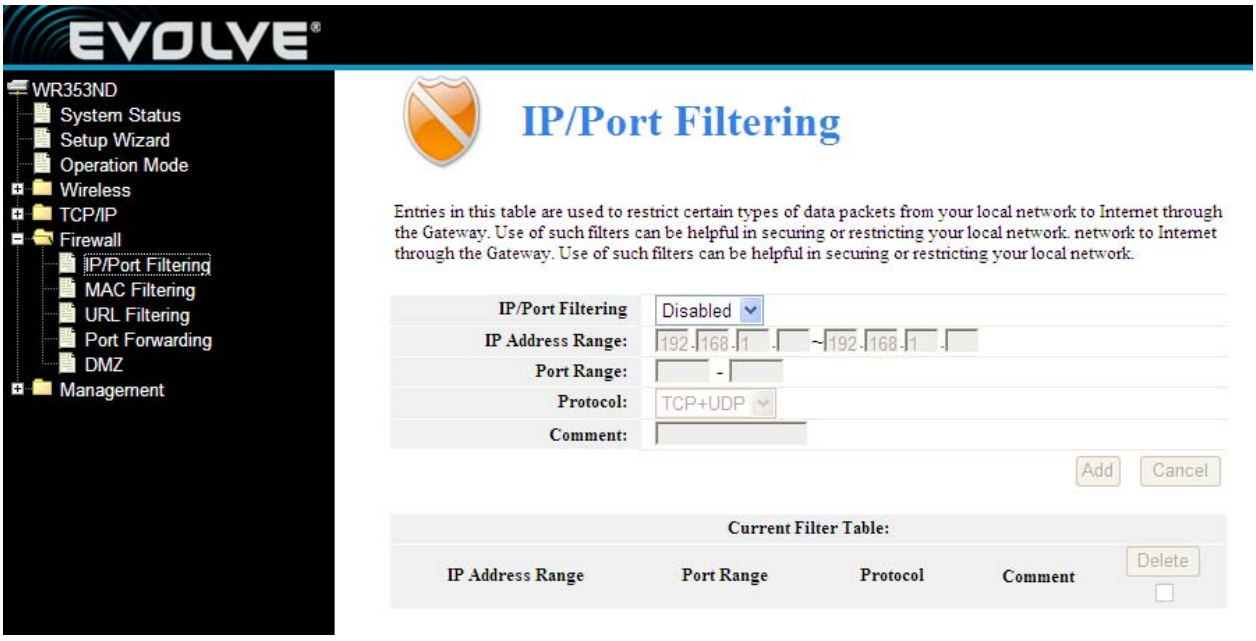
4.3.4 WAN Interface Setup



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

4.4 Firewall

4.4.1 IP/Port Filtering



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

IP/Port filtering: If you choose 'White list', only those clients whose IP addresses are in the list will be able to connect to your Access Point. When 'Blacklist' is selected, these IP Addresses on the list will not be able to connect the Access Point.

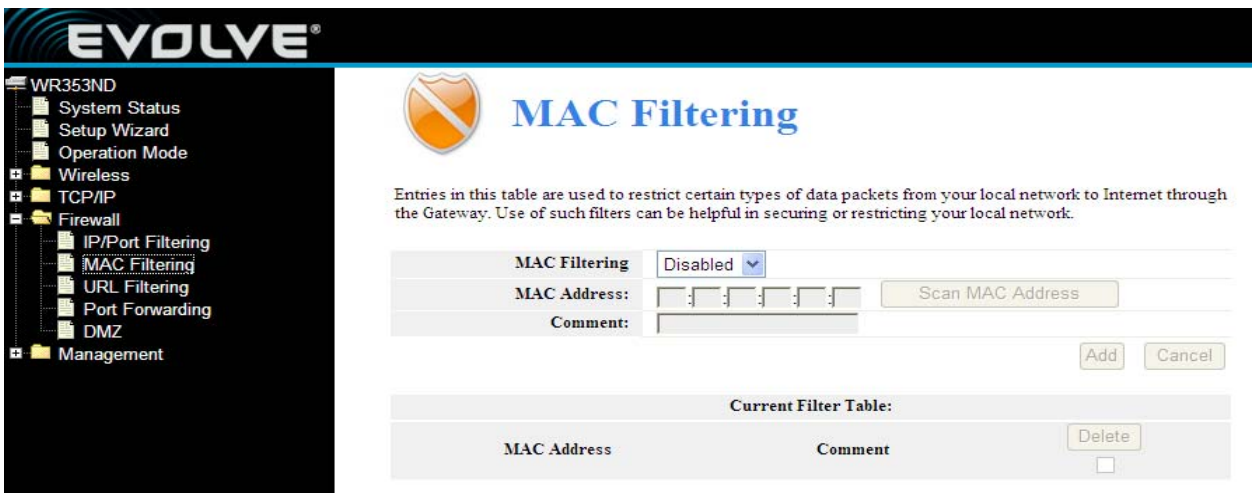
IP Address Range: input the IP address range for the rule

Port range: input the filter port, for example 20-220

Protocol: you can select both TCP and UDP

Current filter table: The list of port filter.

4.4.2 MAC Filtering



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

MAC Filtering: If you choose 'White list', only those clients whose MAC addresses are in the list will be able to connect to your Access Point. When 'Blacklist' is selected, these MAC Addresses on the list will not be able to connect the Access Point.

MAC Address: type the MAC Address, for example: 00:E0:4C:3F:2D:C5.

Current Filter table: The list of MAC filter.

4.4.3 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. 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: select it to Enable

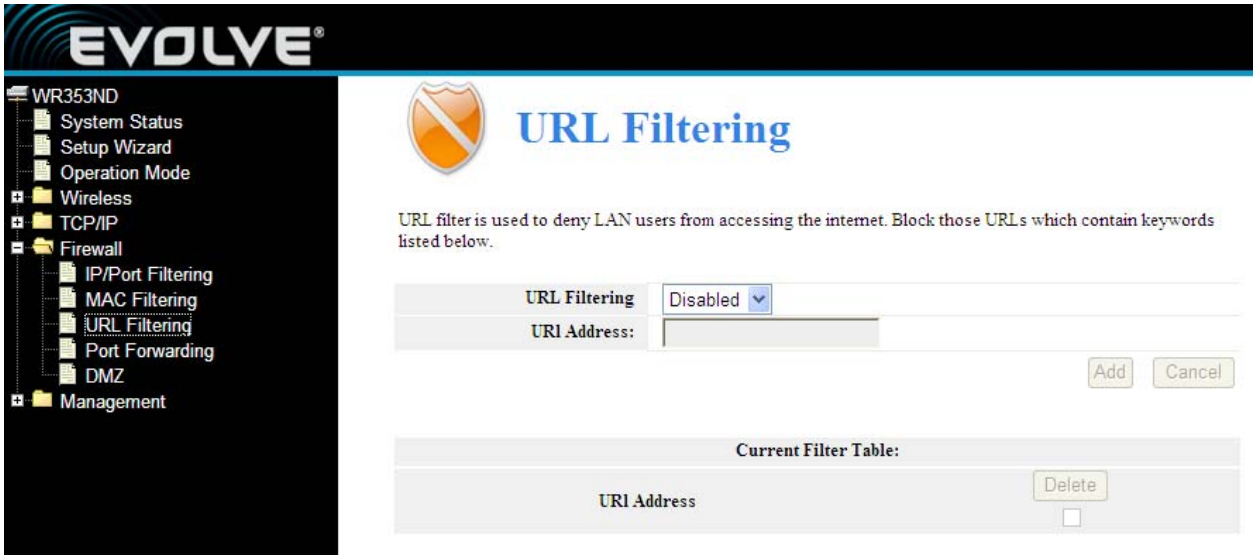
IP Address: The IP Address of the PC running the service application

Protocol - The protocol used for this application, either **TCP**, **UDP**, or **both** (all protocols supported by the router).

Port Range- The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).

Current Port Forward Table: port forward services already list.

4.4.4 URL Filtering

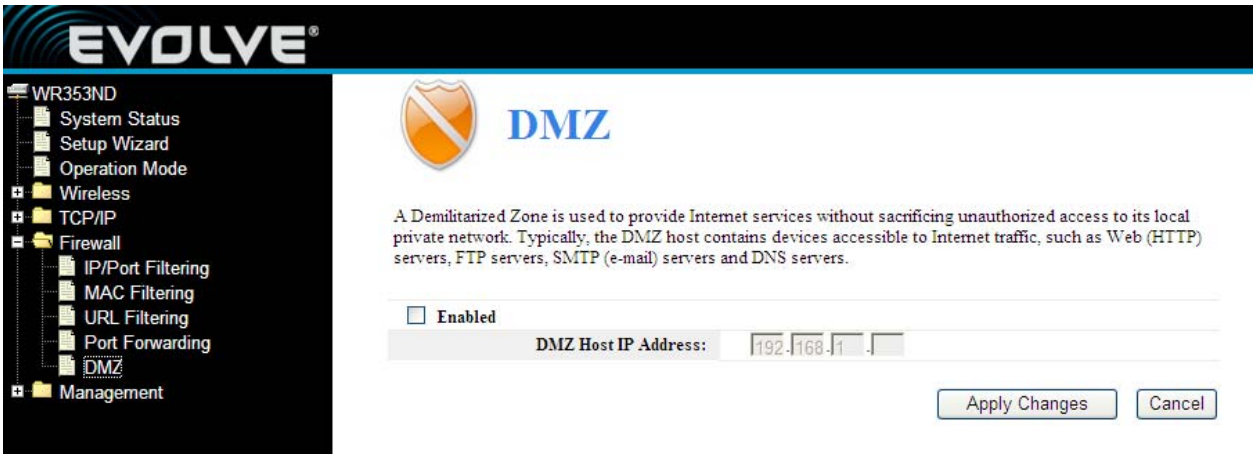


URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

URL Filtering : If you choose 'White list', only those URL Addresses are in the list will be able to connect to your Access Point. When 'Blacklist' is selected, these URL Addresses on the list will not be able to connect the Access Point.

URL Address: Input the URL address for the rule, Click apply changes.

4.4.5 DMZ



The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC 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 change when using the DHCP function.

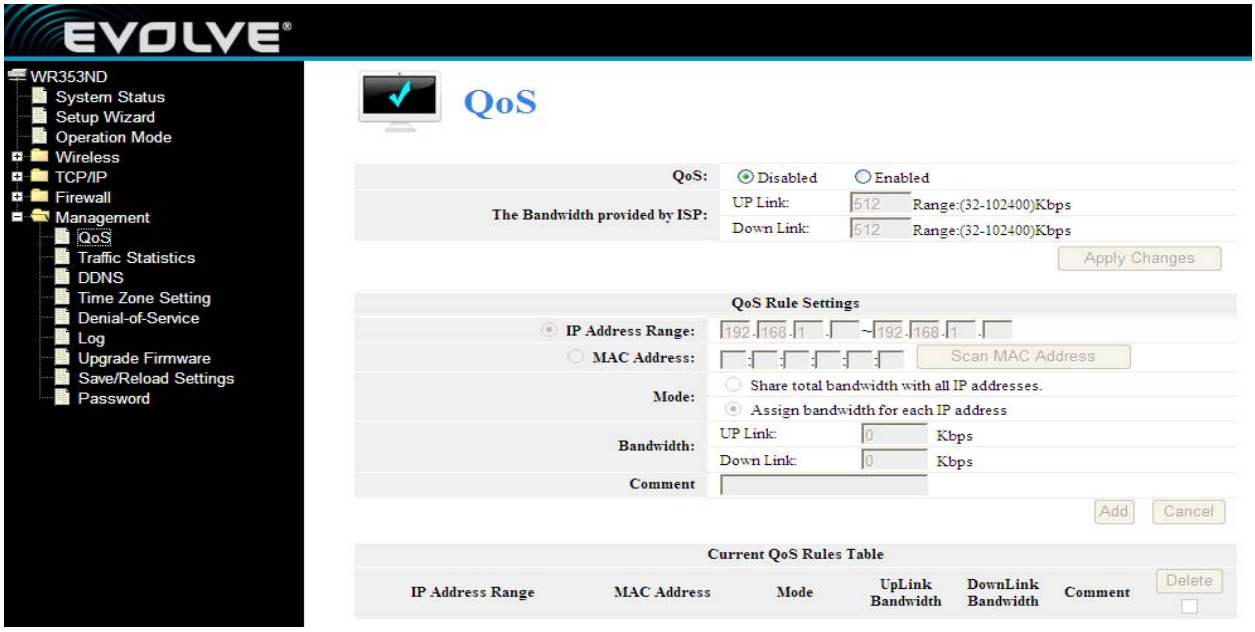
DMZ Enable: Select it, DMZ can be edit..

DMZ Host IP Address: input IP Address. for example 192.168.1.34.

Click **apply changes**, complete set DMZ.

4.5 Management

4.5.1 QOS



Notice: If you add any QoS rules, the DoS function will have no effect.

This page is used to help users configure the parameters of QoS.

The Maximum Bandwidth provided by ISP----Indicate the network max bandwidth for up and down data stream

Direction----Direction of data stream, Up stream means data go out the LAN, Downstream means go in the LAN

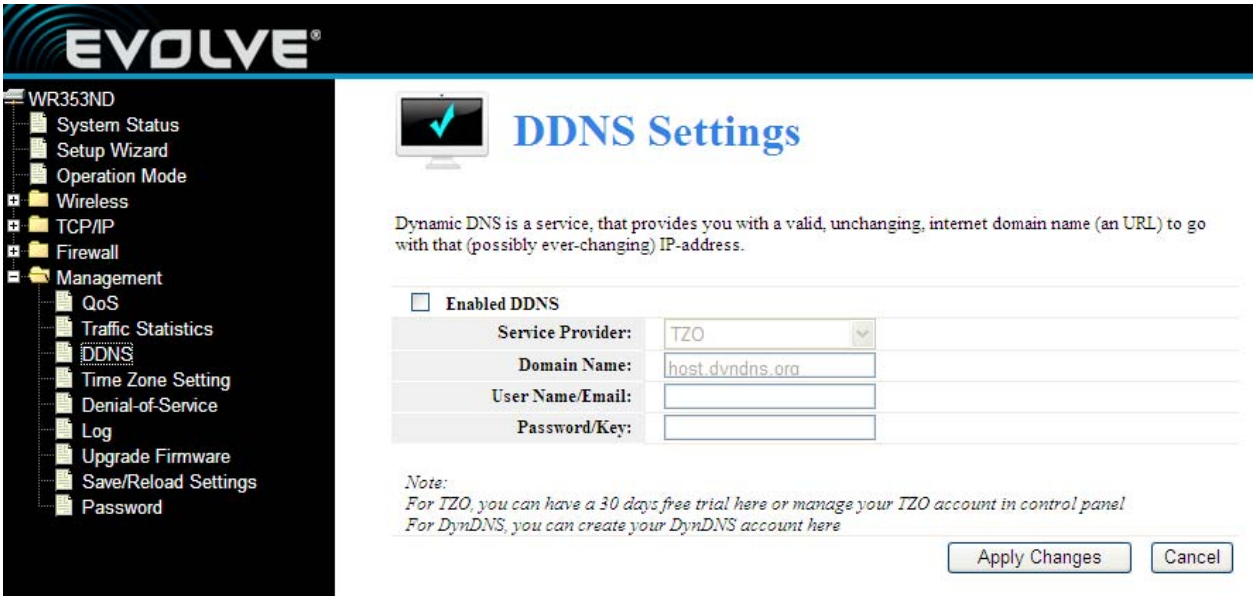
IP Address Range----The IP address of the PC in LAN

Mini. Rate & Max. Rate----The minimum & maximum rate you assign to the IP

Bandwidth sharing----The way to share bandwidth

Enable----Enable or disable this rule

4.5.2 DDNS Setting

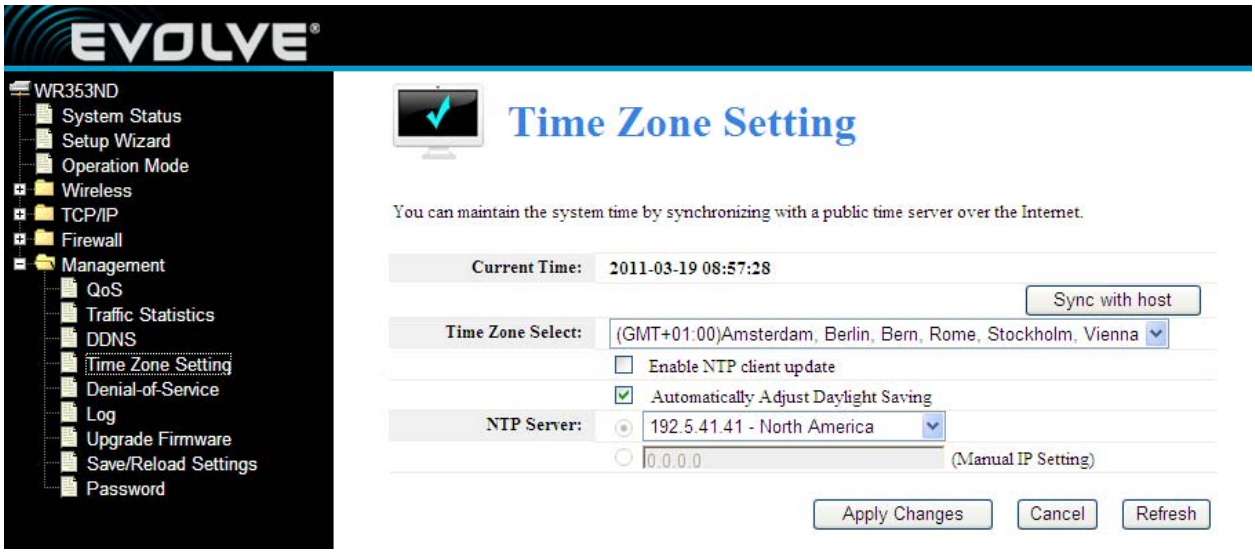


Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly ever changing) IP-address. DDNS. lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.DynDNS.org or www.TZO.com. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

1. Type your **Service Provider.**
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. **Domain Name -** the domain names are displayed here. Click **Apply Changes** to logout the DDNS service.

4.5.3 Time Zone Setting



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

Current time: type the date and time.

Time Zone Select: Select your local time zone from this pull down list.

Enable NTP client update: select it, you can get the time from **NTP.**

NTP server: select a server from list.

Click the Apply changes get the time from Internet if you have connected to Internet.

4.5.4 Denial of Service

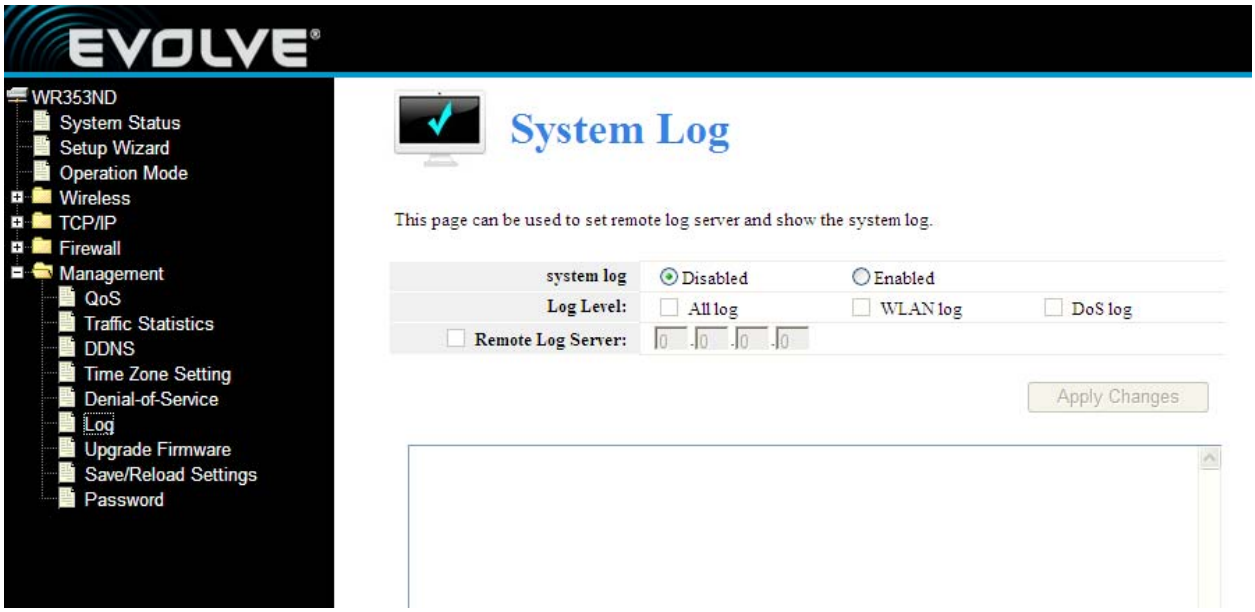
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DoS Prevention: select it, you can modify DOS Prevention.

Enable Source IP Blocking: you can input source IP Blocking time

Click apply changes, DoS take effect.

4.5.5 Log



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

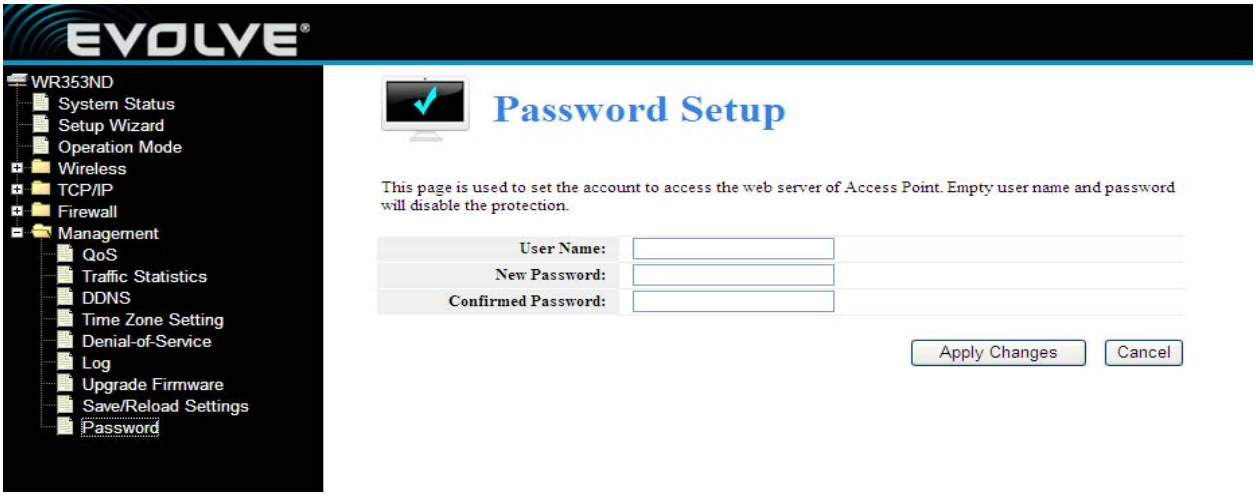
4.5.6 Upgrade Firmware

This page allows you 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

4.5.7 Save/Reload settings

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

4.5.8 Password setup



This page is used to set the account to access the web server of Access Point.