ESR6650

3G Wireless Router
Ultra Speed

(IEEE 802.11 b/g)

User Manual

TABLE OF CONTENTS

Revision History

Version	Date	Notes
1.0	January 16, 2009	Initial

1. Introduction

1.1. Summary

Congratulations on your purchase of ESR6650 3G Wireless Router. ESR6650 is compatible with the most popular 3G standards and 802.11g & 802.11b gadgets. ESR6650 is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Switch that connects your wired-Ethernet devices together at incredible speeds.

At 150Mbps wireless transmission rate, Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple steams of data in a single wireless channel giving you seamless access to multimedia content. Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, ESR6650 encodes all wireless transmissions with WEP, WPA, and WPA2 encryption.

With inbuilt DHCP Server & powerful SPI firewall ESR6650 protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With incredible speed and QoS function, ESR6650 is ideal for media-centric applications like streaming video, gaming, and VoIP telephony to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

1.2. Key Features

Features	Advantages
3G Data Card Support	**Allows user to share 3G network among multiple users. It supports WCDMA (HSDPA), CDMA2000 and TD-SCDMA.**
Incredible Data Rate up to 150Mbps**	**Heavy data payloads such as MPEG video streaming**
IEEE 802.11b/g Compliant	**Fully Interoperable with IEEE 802.11b / IEEE 802.11g compliant devices with legacy protection**
Four 10/100 Mbps Fast Switch Ports (Auto-Crossover)	**Scalability, extend your network.**
Firewall supports, DMZ, MAC Filter, IP Filter, URL Filter, ICMP Blocking, SPI, Port Mapping, Port Forwarding, Port Trigger	**Avoids the attacks of Hackers or Viruses from Internet**
Support 802.1x Authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	**Provide mutual authentication (Client and dynamic encryption keys to enhance security**
WDS (Wireless Distribution System)	**Make wireless AP and Bridge mode simultaneously as a wireless repeater**
Multiple SSID	**Easy management of users of various groups.**

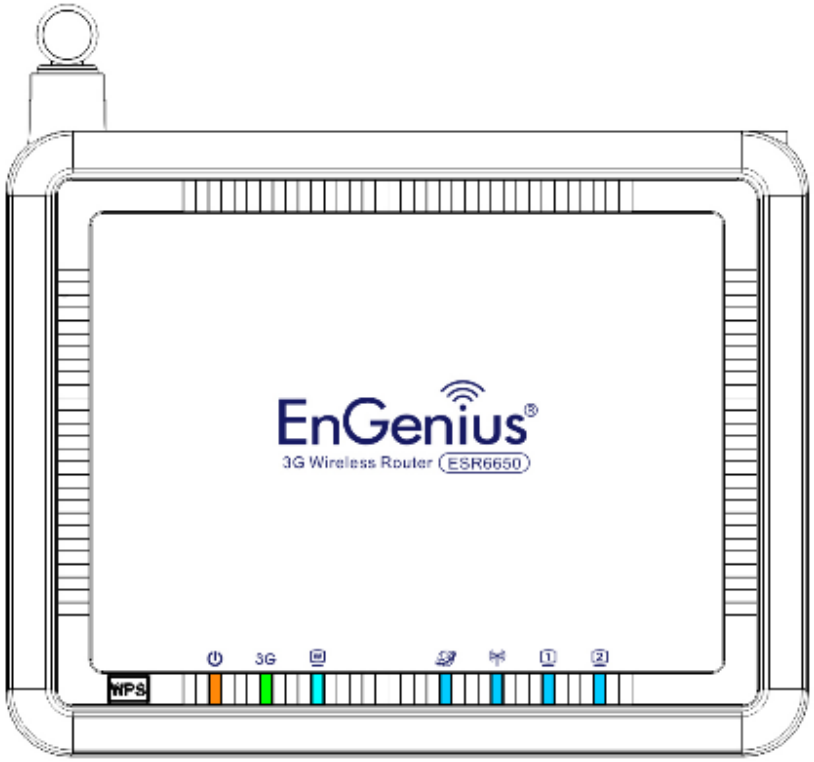
*** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

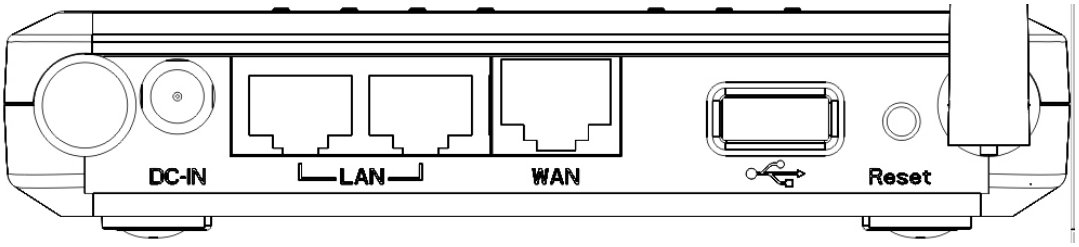
1.3. Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. SOHO Router
2. 100V or 240V Power Adapter
3. 2dBi 2.4GHz SMA Upgradable Antennas x 1 pcs
4. Quick Install Guide
5. CAT 5 UTP Cable
6. CD (User's Manual)

1.4. Product Layout





LED	Description
Power	1 (On-> red Test/reset default->blink)
3G	1 (Link-> green on, traffic->blink)
WAN	1 (Link-> blue on, traffic->blink)
Internet	1 (Link-> blue on, traffic->blink)
WLAN	1 (Link-> blue on, traffic->blink)
LAN1	1 (Link-> blue on, traffic->blink)

Interface	Description
Reset	Push this button to restart the system Press this button and hold for 10 seconds to reset to default.
WPS	Push this button once to start WPS.
DC IN	Power connector, connects to DC 12V Power Adapter
LAN1 & 2	Local Area Network (LAN) ports 1 and 2
USB	USB socket for 3G data card
WAN	WAN port for ADSL / Cable Modem

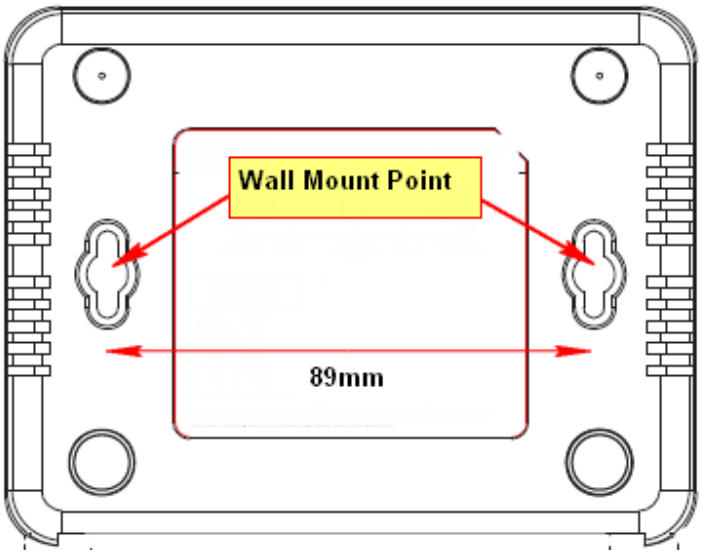
2. Installation

2.1. Network + System Requirements

To begin using the ESR6650, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System ï Microsoft Windows 98SE/ME/XP/2000/VISTA
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11b/g/n) ï optional.
- Internet
  - 3G data card or
  - ADSL or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera etc.)
- Few Ethernet compatible CAT5 cables.

2.2. Wall Mounting



You can mount the device on the wall. There are two mounting points on the bottom of the device. Please find a proper spot where two nails can be applied. The distance between the two nails is 89mm. Finally, carefully mount the device onto the wall and make sure the nails are firmly locked on the mount points.

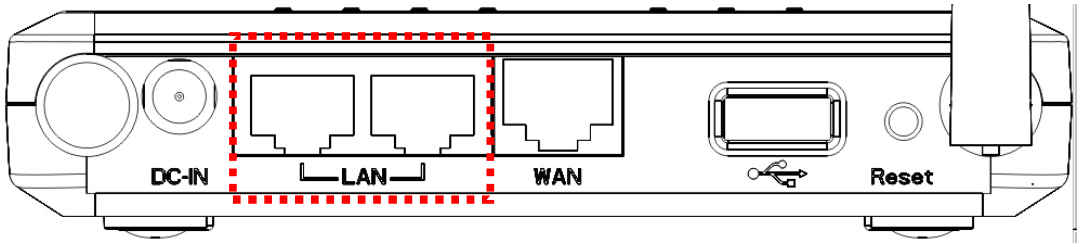
2.3. ESR6650 Placement

You can place ESR6650 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and your ADSL/Cable modem. If the antennas are not positioned correctly, performance loss can occur.

2.4. Setup LAN & 3G (WAN)

LAN connection:

Connect Ethernet cable between your PC/Notebook LAN port & one of the 2 available LAN ports on ESR6650.



3G connection:

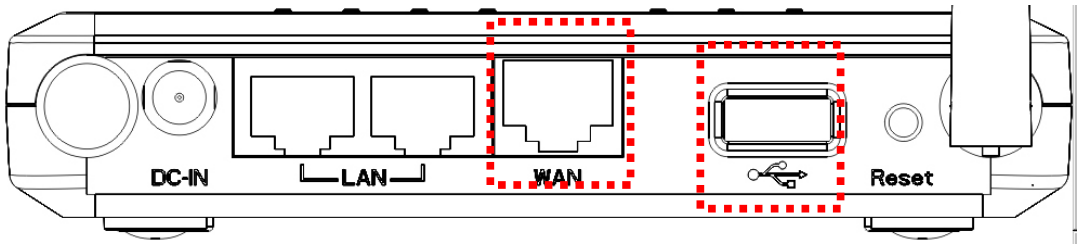
Plug-in your 3G data card into USB port if you would like to access Internet through 3G network.

Contact your ISP if you have any questions concerning the access account and password.

ADSL (Cable Modem):

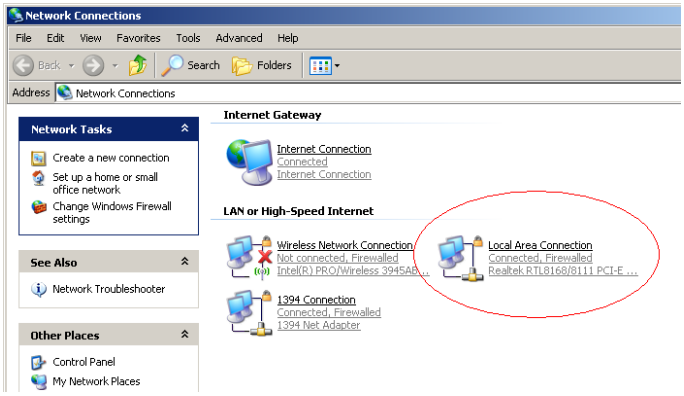
Connect Ethernet cable between WAN ports of your ADSL/CABLE modem & WAN port of ESR6650. Make sure your ADSL/CABLE modem is working well.

Contact your ISP if you have any questions concerning the access account and password.

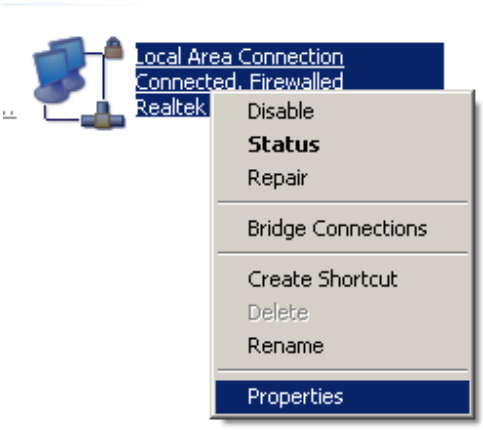


2.5. PC Network Adapter setup (*Windows XP*)

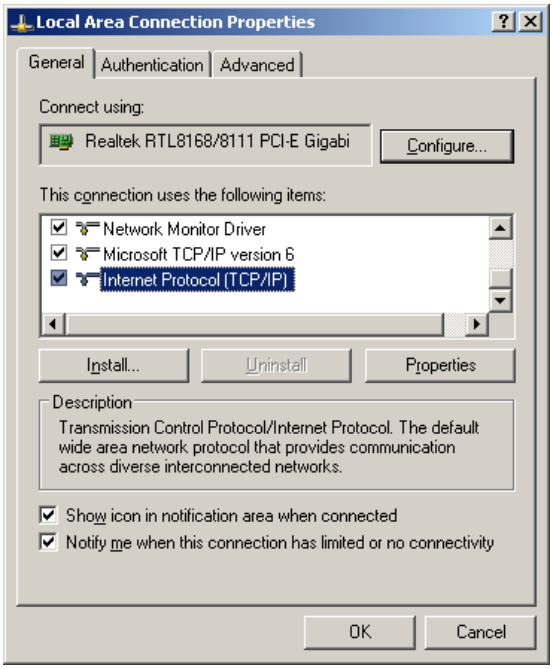
- Enter [Start Menu] → select [Control panel] → select [Network].

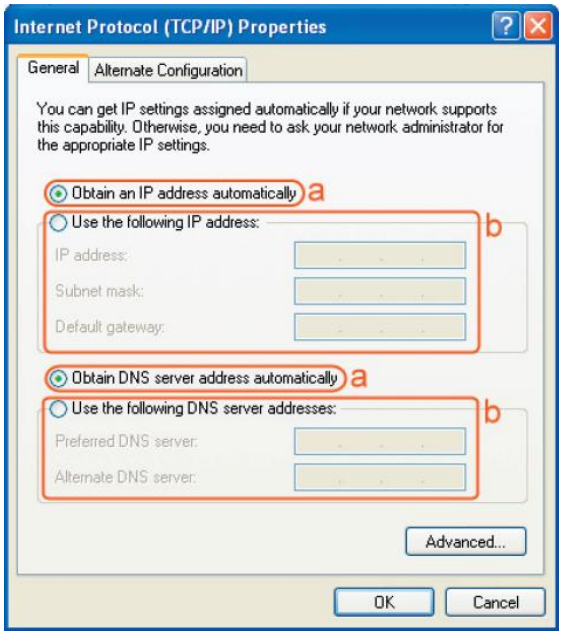


- Select [Local Area Connection]) icon=>select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].





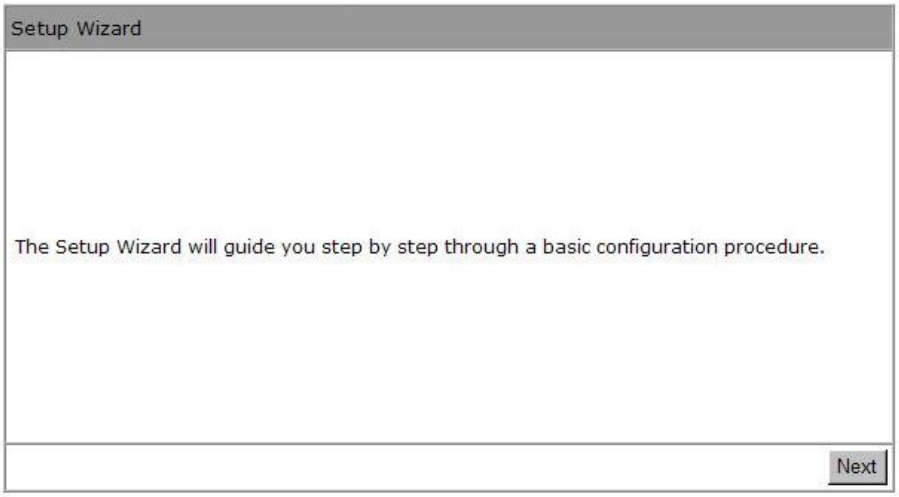
- Select the [General] tab.

ESR6650 supports [DHCP] function, please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

2.6. Bring up ESR6650

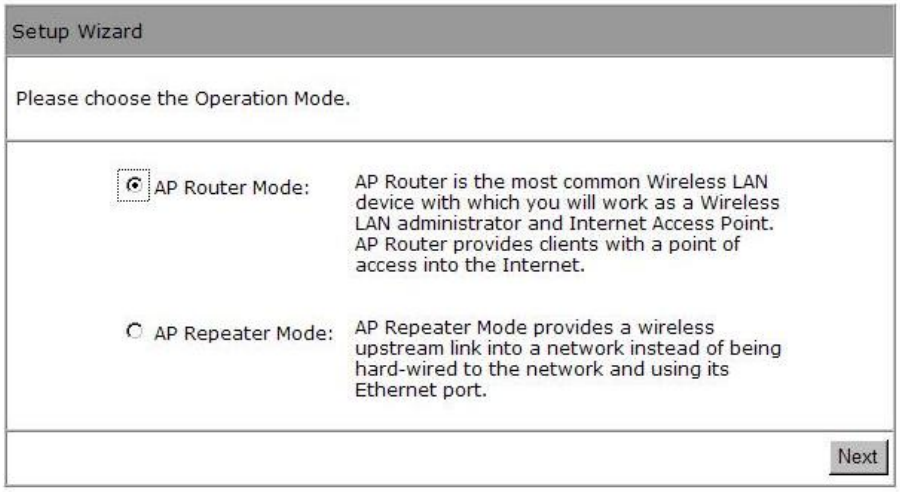
Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. Then, ESR6650 automatically enters the self-test phase. During self-test phase, Power LED will blink briefly, and then will be lit continuously to indicate that this product is in normal operation.

3. Smart Wizard



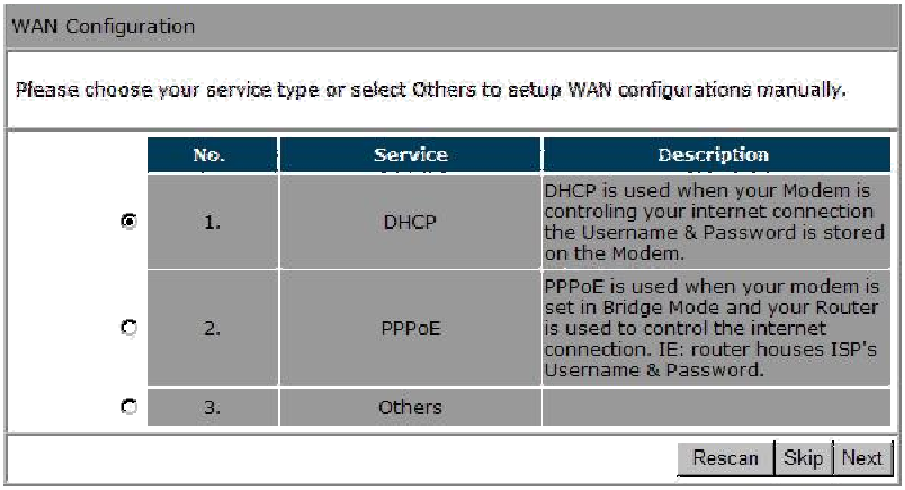
Click **<Next>** to enter mode selection.

Select the mode that ESR6650 is going to be and set its configurations. **AP Repeater mode** does not enable WAN interface, Setup Wizard will skip WAN Configuration.

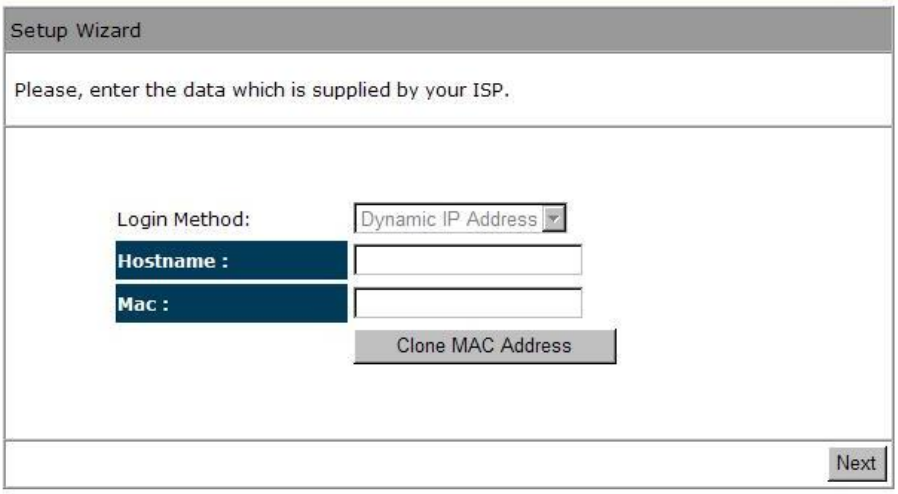


Click **<Next>** to automatically detect your **Internet Network** settings.

You could choose your service type or select Others to setup WAN configurations manually.



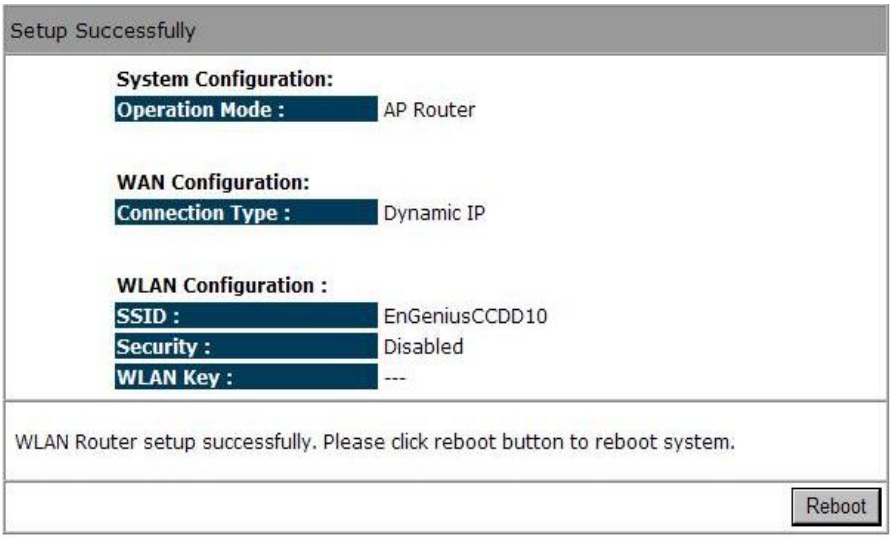
Smart Wizard has detected DHCP client. Configure the host name and MAC address of ESR6650. Click Next to proceed.



Smart Wizard has finished setting up **WAN Configuration**. Click **<Next>** to proceed.

Enter the name for your wireless network (SSID) and security key

Click **<Next>** to proceed



To apply the entire configuration, click **<Reboot>**.

NOTE:

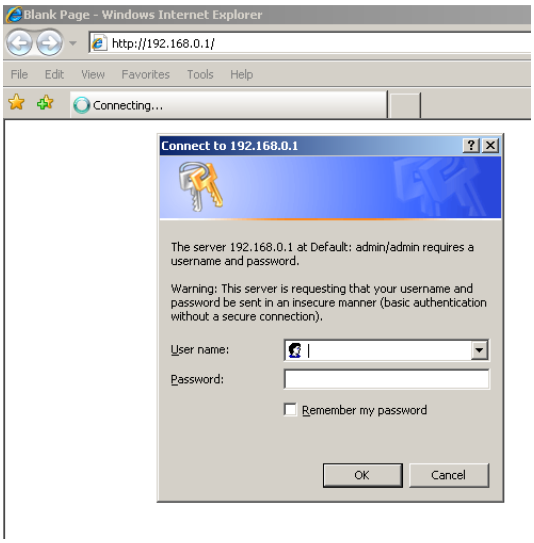
After Wireless settings are applied, you need to connect from your WLAN client with the security settings you just finished configuring. Remember the type of security & security key.

4. Initial Setup ESR6650

ESR6650 uses web-interface for configuration to be accessed through your web browser, such as Internet Explorer or Firefox.

- LOGIN Procedure

1. OPEN your browser (e.g. Internet Explorer).
2. Type **http://192.168.0.1** in address bar and hit [Enter] button on your keyboard.



3. Click **<OK>** to navigate into ESR6650 configuration home page.
4. You will see the home page of ESR6650 as follows.

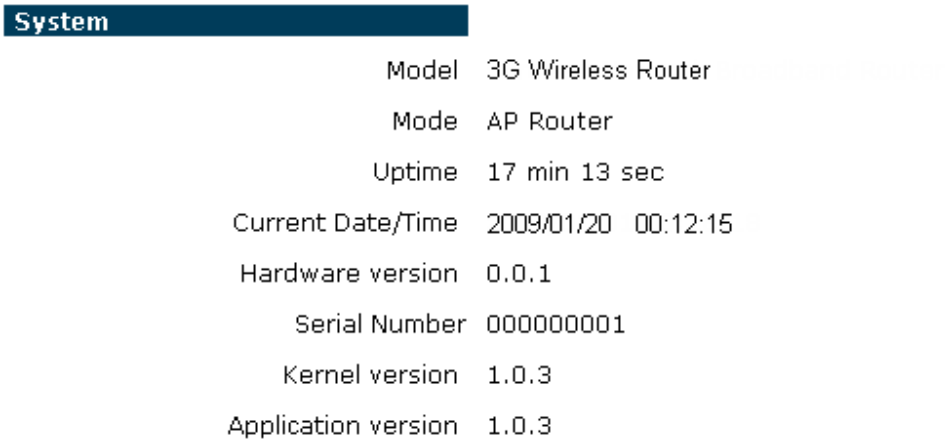
5. AP Router Mode

5.1. System

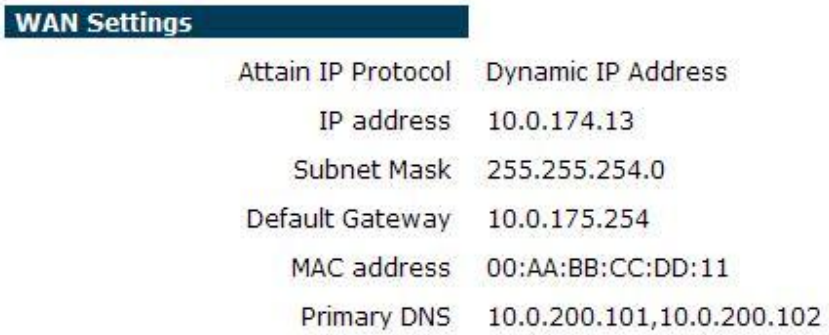
- Status

This page allows you to monitor the current status of your router.

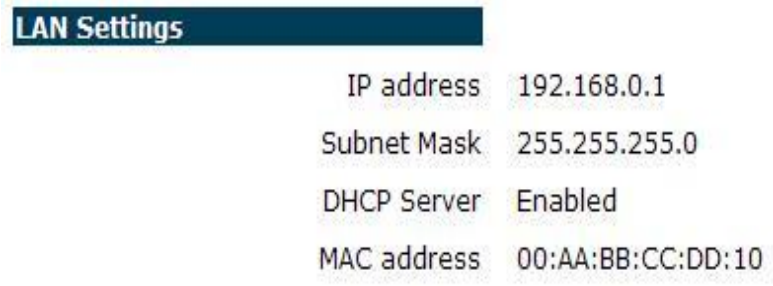
System: You can see the Uptime, hardware information, serial number as well as firmware version information.



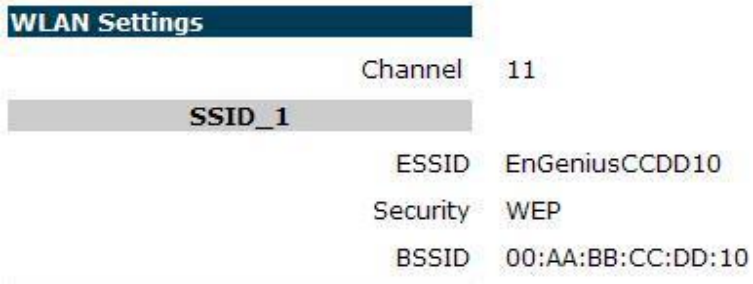
WAN Settings: This section displays whether the WAN port is connected to a Cable/DSL connection. It also displays the routerôs WAN IP address, Subnet Mask, ISP Gateway, MAC address and the Primary DNS.



LAN Settings: This section displays the Router LAN ports current information. It also shows whether the DHCP Server function is enabled / disabled.



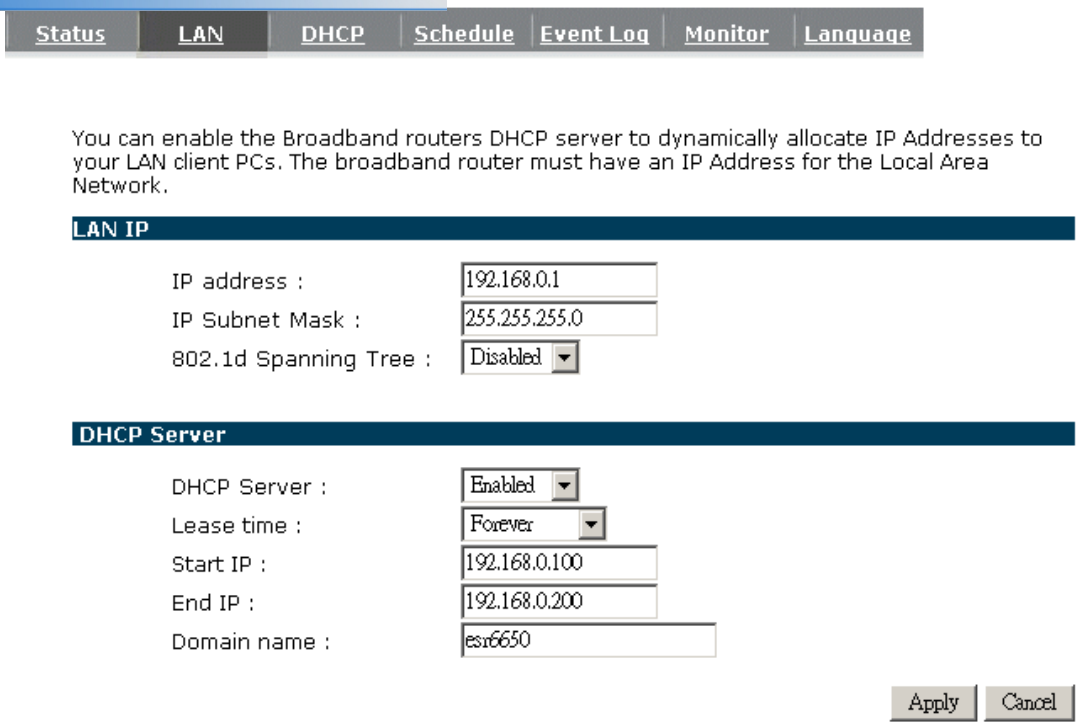
WLAN Settings: This section displays the current WLAN configuration settings. Wireless configuration details such as SSID, Security settings, BSSID, Channel number and mode of operation are briefly shown.



- LAN

The LAN Tabs reveals LAN settings which can be altered at will. If you are an entry level user, try accessing a website from your browser. If you can access website without a glitch, just do not change any of these settings.

Click **<Apply>** at the bottom of this screen to save the changed configurations.



LAN IP

IP address: 192.168.0.1. It is the routerôs LAN IP address (the ñDefault Gatewayò IP address of your LAN clients). It can be changed based on your own choice.

IP Subnet Mask: 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server

DHCP Server: This can enable or disable the Dynamic Pool setting.

Lease time: This is the lease time of each assigned IP address.

Start IP: This is the beginning of the IP pool for DHCP client hosts.

End IP:. This is the end of the IP pool for DHCP client hosts

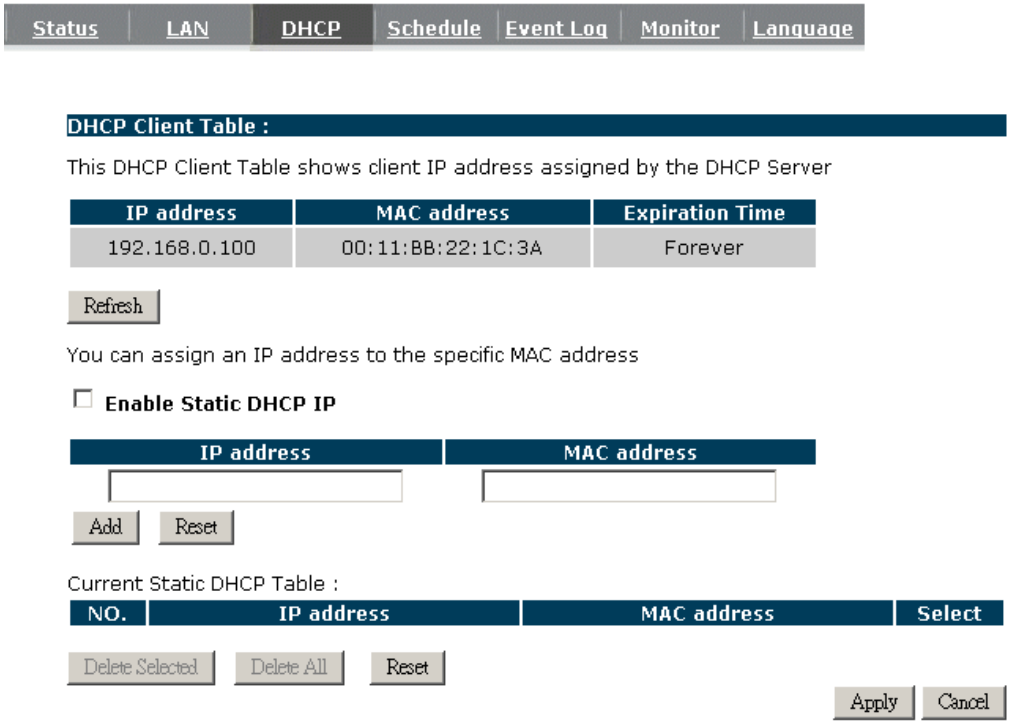
Domain name: The Domain Name for the existing or customized network.

- DHCP

View the current LAN clients which are assigned with an IP Address by the DHCP-server. This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the **<Refresh>** button to update the available information. Hit **<Refresh>** to get the updated table.

You can check ñ**Enable Static DHCP IP**ñ It is possible to add more static DHCP IPs. They are listed in the table ñ**Current Static DHCP Table**ñ IP address can be deleted at will.

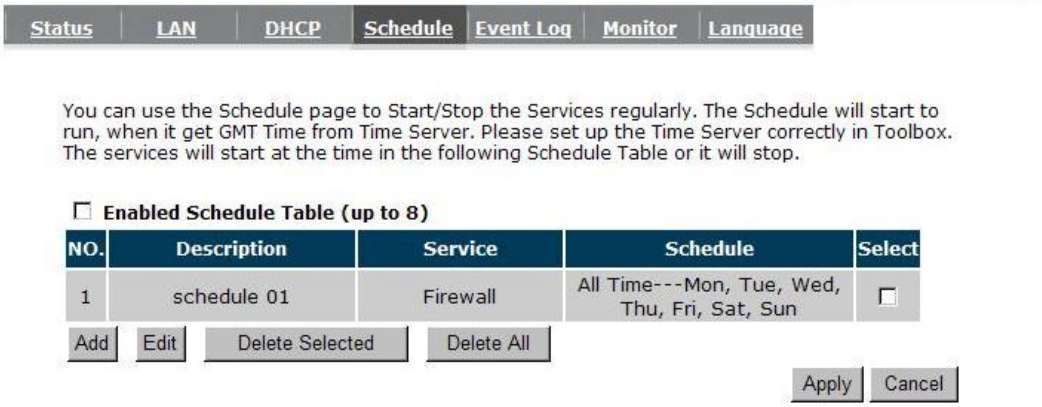
Click **<Apply>** button to save the changed configuration.



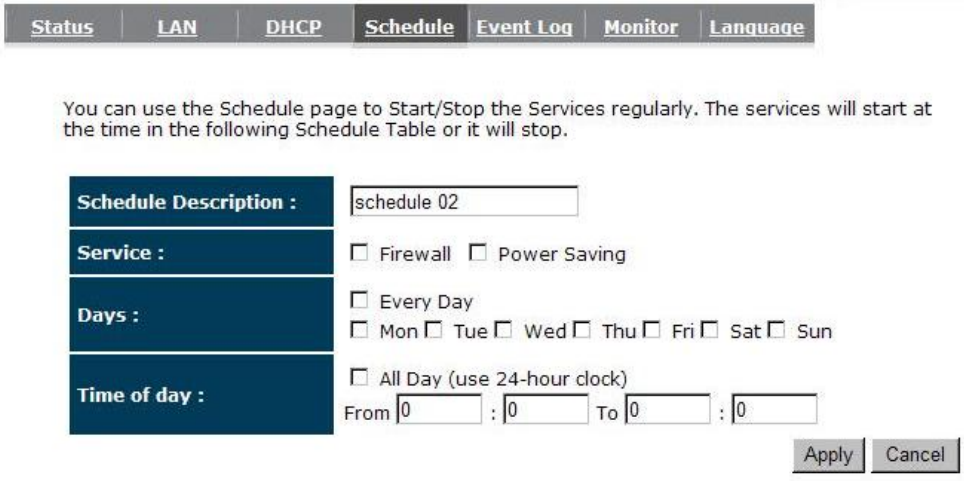
- Schedule

This page allows users to set up schedule function for Firewall and Power Saving

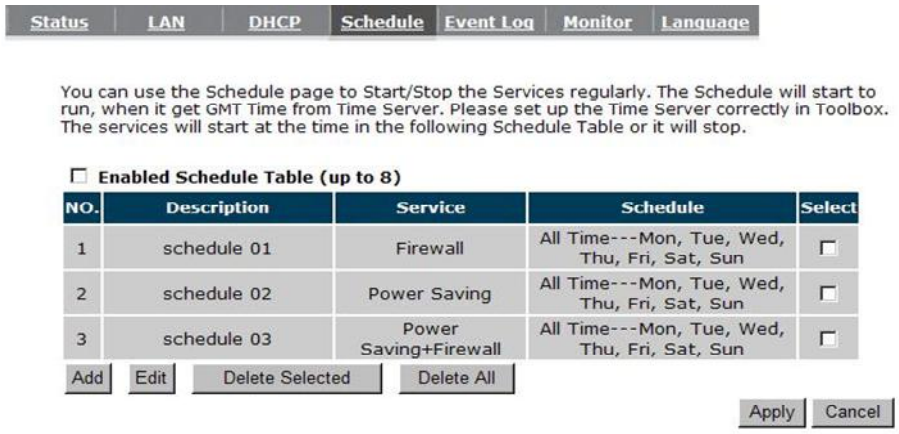
.



Edit schedule options to allow configuration of firewall and power savings services. Fill in the schedule and select type of service. Click <**Apply**> to keep the settings.

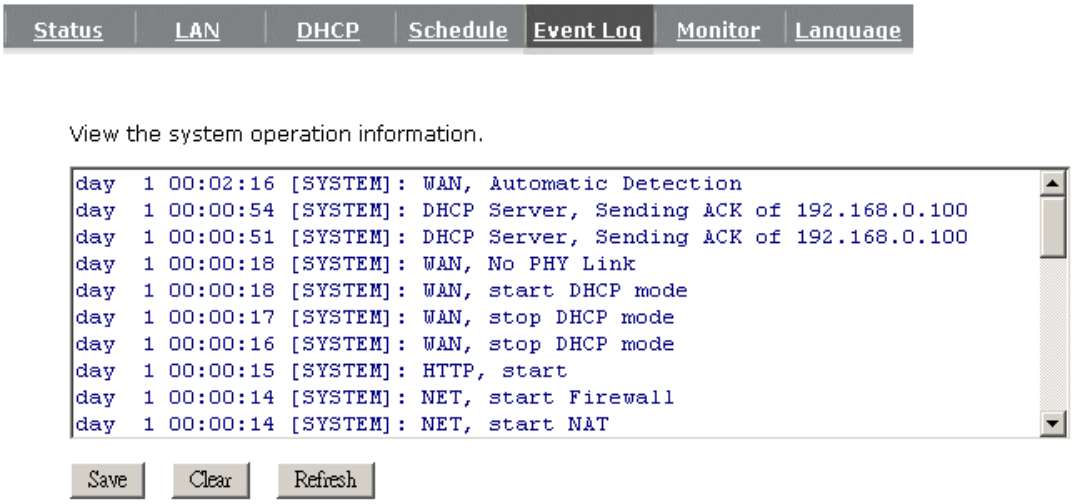


The schedule table lists the pre-schedule service-runs. You can select any of the schedule record using the check box.



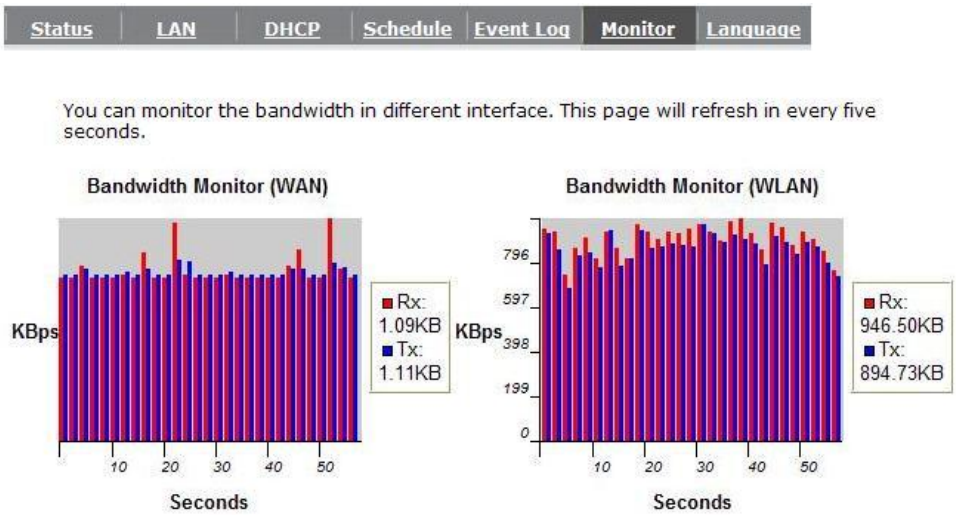
- Event Log

View **operation event log**. This page shows the current system log of the Router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will be cleared if not saved to a local file.



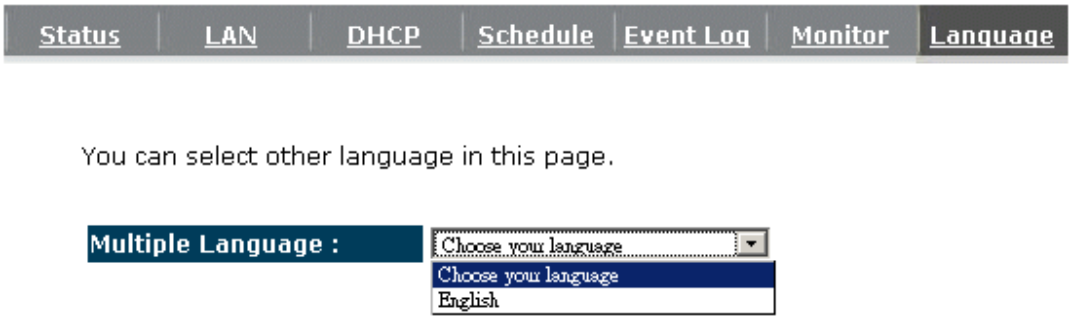
- Monitor

Show histogram for network connection on WAN, LAN & WLAN. Auto refresh keeps information updated frequently.



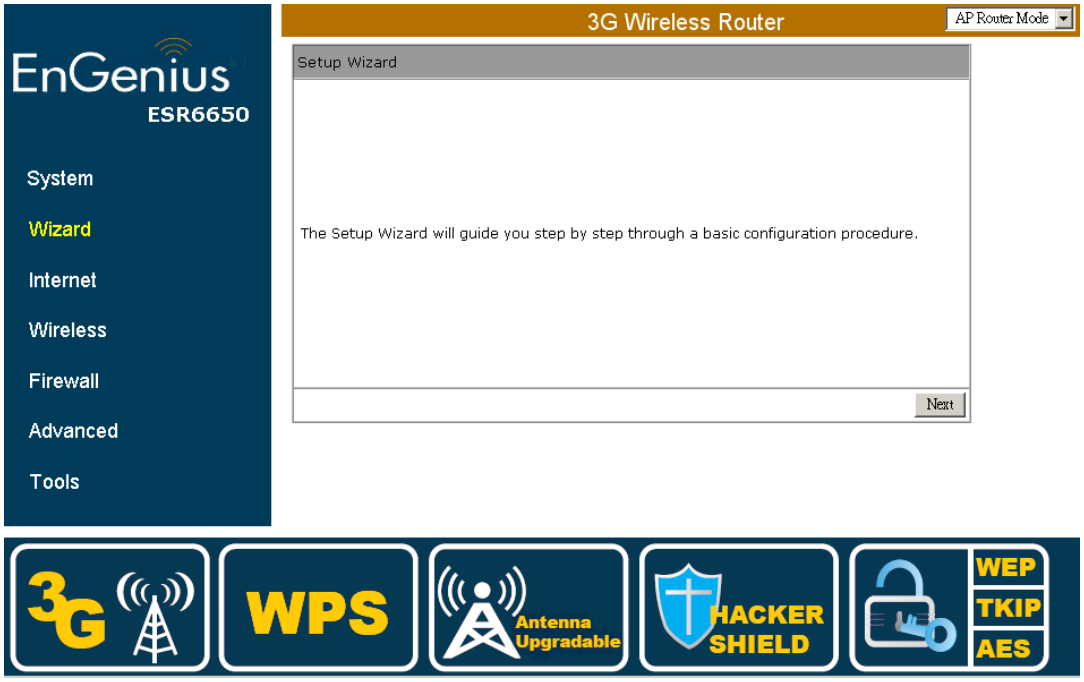
- Language

This Wireless Router support multiple language of web pages, You could select your native language here.



5.2. Wizard

Click **Wizard** to configure the Router. Setup wizard will now be displayed; check that the modem is connected and click **<Next>.** The details please refer to **Smart Wizard <Page 13>.**



5.3. INTERNET

ESR6650 supports both 3G and ADSL for Internet access. Please note that 3G (USB interface) network by default is the preferred Internet option. Therefore, in case you have both 3G and ADSL connection setup, ESR6650 will automatically use 3G for Internet access.

Please note that inserting 3G data card will switch off ADSL connection immediately. If you prefer to use ADSL for Internet access, do not insert 3G data card into the USB socket.

Your 3G data card may take more than 20 seconds to initiate and respond to ESR6650. Please be patient and pay attention to the 3G LED on the top panel. Green Light on 3G LED signifies that your 3G card is ready.

- Status

This page shows the current Internet connection type and status

View the current internet connection status and related information.

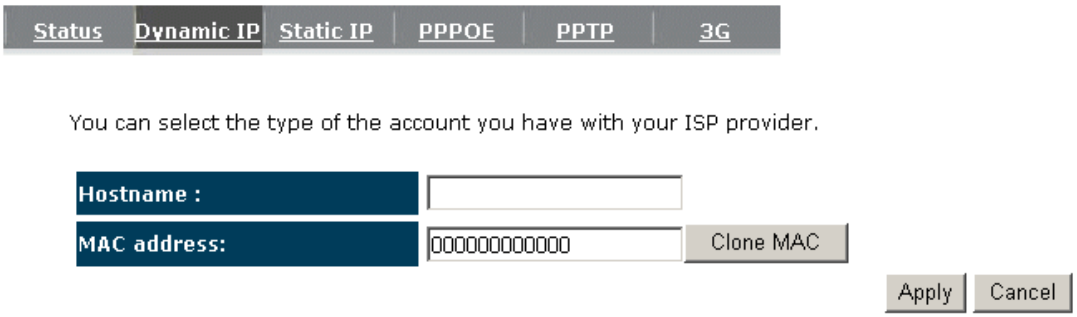
WAN Settings

Attain IP Protocol	PPPoE
IP address	118.161.71.133
Subnet Mask	255.255.255.255
Default Gateway	118.161.64.254
MAC address	00:AA:BB:CC:11:03
Primary DNS	168.95.192.1,168.95.1.1

Connect Disconnect

- Dynamic IP

Use the MAC address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of the Ethernet card as an identifier, connect only the PC with the registered MAC address to the Router and click the **<Clone MAC Address>** button. This will replace the current MAC address with the already registered Ethernet card MAC address.

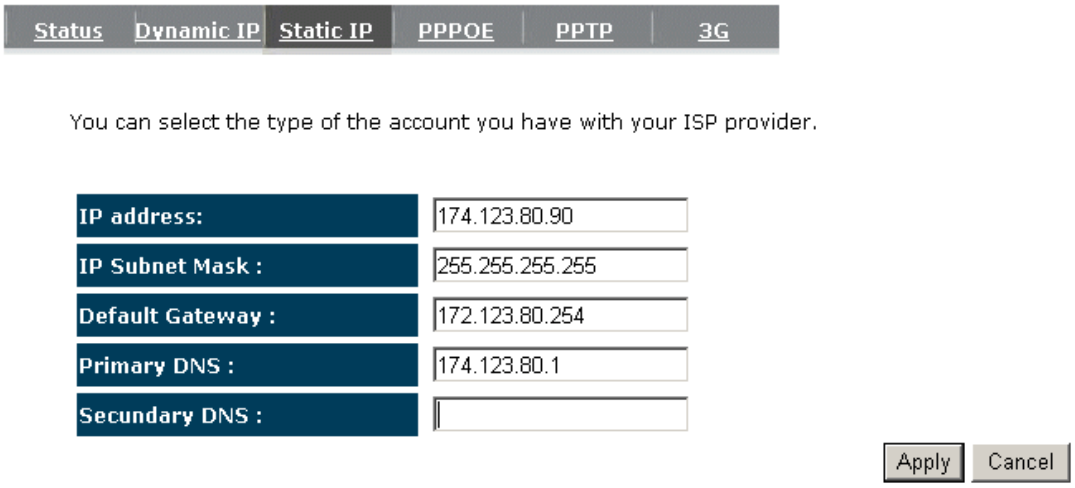


Host Name: This is optional.

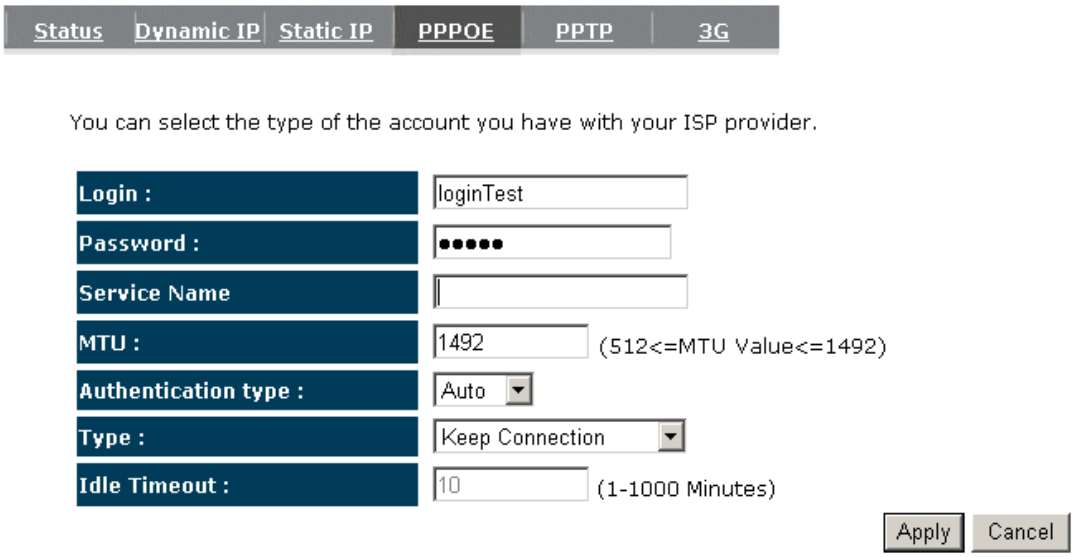
MAC address: The default value is set to the WANs physical interface of the Router.

- Static IP

If your ISP Provider has assigned a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.



- Point-to-Point over Ethernet Protocol (PPPoE)



Login / Password: Enter the PPPoE username and password assigned by your ISP Provider.

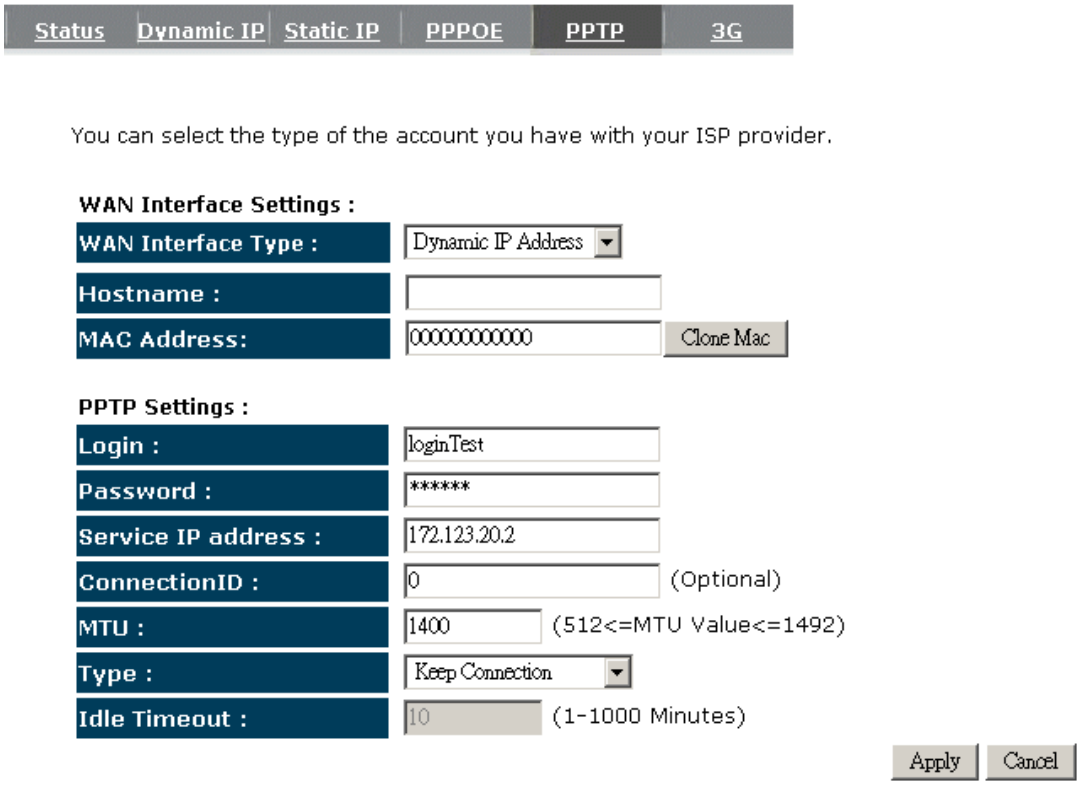
Service Name: This is normally optional.

Maximum Transmission Unit (MTU): This is the maximum size of the packets.

Type: Enable the **Automatic Connection** option to automatically re-establish the connection when an application attempts to access the Internet again.

Idle Timeout (available only under Automatic Connection): This is a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped.

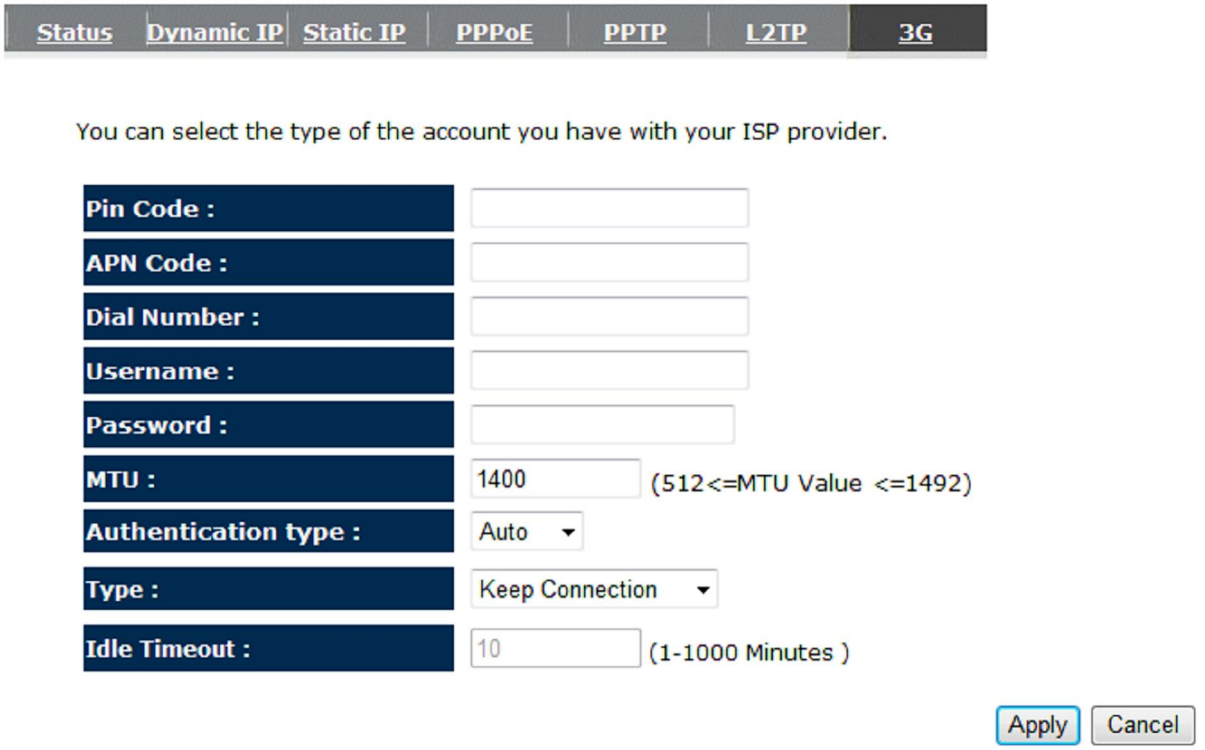
- Point-to-Point Tunneling Protocol (PPTP)



PPTP allows the secure connection over the Internet by simply dialing in a local point provided by your ISP provider. The following screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

Click **<Apply>** to save configuration and connect to ISP provider.

- 3G Network



Pin Code: Enter the Pin code required by the ISP.

APN Code: Enter APN if ISP requires it.

Dial Number: Enter phone number if ISP requires it.

User Name: Enter 3G network account / username

Password: Enter 3G network account password

MTU: Enter the MTU value if required.

Authentication Type: Select whether ISP uses PAP or CHAP authentication method.

Type:

Keep Connection: Keep connection with or without the presence of traffic.

Automatic Connection: Connect when traffic is detected.

Manual Connection: Connect only on user's demand (see status)

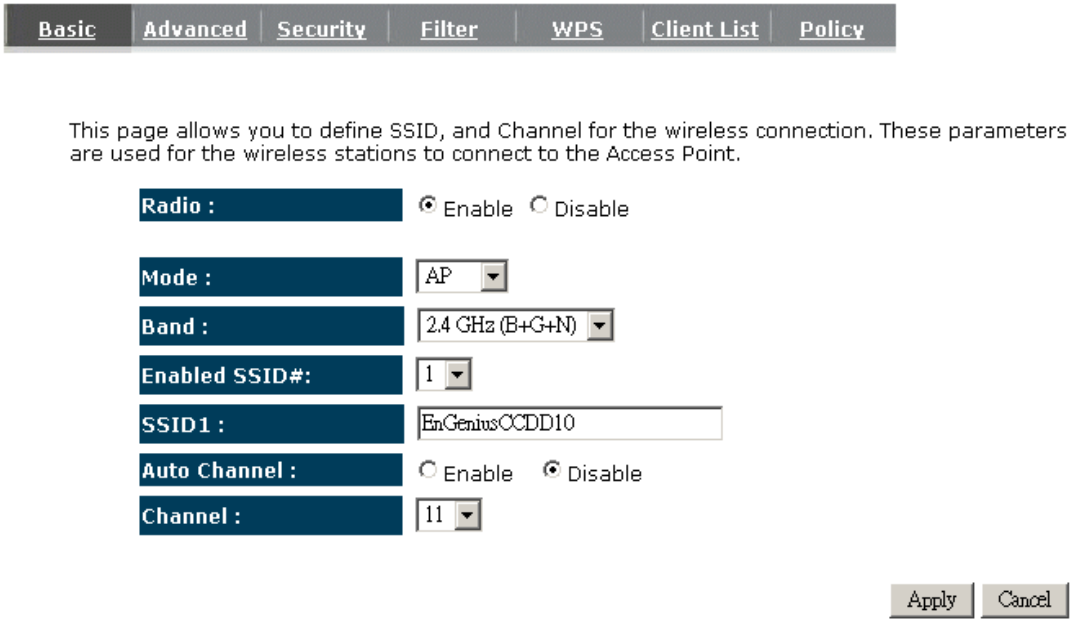
Idle Timeout: Disconnect from 3G network if there's no traffic in the specified timeout period.

Note: You may need 3G account detail and configuration pre-requisite from your local ISP.

5.4. Wireless Settings

- Basic

In basic setting page, you can set wireless Radio, Mode, Band, SSID, and Channel.



Radio: You can turn on/off wireless radio. If wireless Radio is off, you cannot associate with AP through wireless.

Mode: In this device, we support three operation modes which are **AP router** and **AP route with WDS**. If you choose AP Router Mode, you can select AP or WDS function in the drop-down menu.

Band: You can select the wireless standards running on your network environment.

2.4 GHz(B): If all your clients are 802.11b, select this one.

2.4 GHz(N): If all your clients are 802.11n, select this one.

2.4 GHz(B+G): Either 802.11b or 802.11g wireless devices are in your environment.

2.4 GHz(G): If all your clients are 802.11g, select this one.

2.4 GHz(B+G+N): Either 802.11b, 802.11g, or 802.11n wireless devices are in your environment.

Enable ESSID: We support 4 multiple SSIDs in this device. Please select how many SSIDs you would like to use in your network environment.

ESSID1~4: ESSID is the name of your wireless network. It might be a unique name to identify this wireless device in the Wireless LAN. It is case sensitive and up to 32 printable characters. You might change the default ESSID for added security.

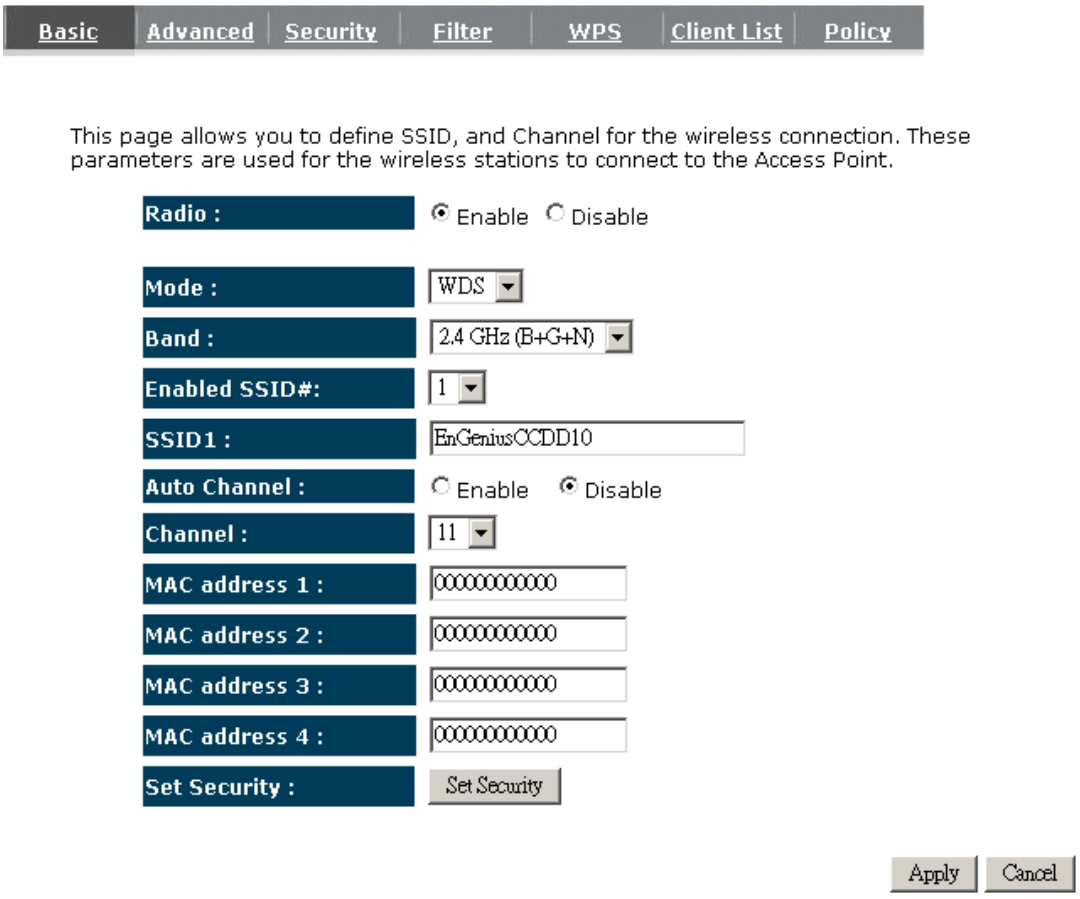
Auto Channel: Device will search all valid channels, then select a cleanest channel and change to this channel if you enable this function. Depend on this function is enabled or not, you will see different items below **Auto Channel**.

Channel: If Auto Channel is disabled, you should choose a static channel and AP will use this channel to communicate with other clients.

Check Channel Time: If Auto Channel is enabled, you can choose a period from the drop-down menu. AP will change to a clean channel periodically.

- WDS with AP Router

Wireless Distribution System, a system that enables the wireless interconnection of access point, allows a wireless network to be extended using multiple APs without a wired backbone to link them. Each WDS AP needs same channel and encryption type settings.

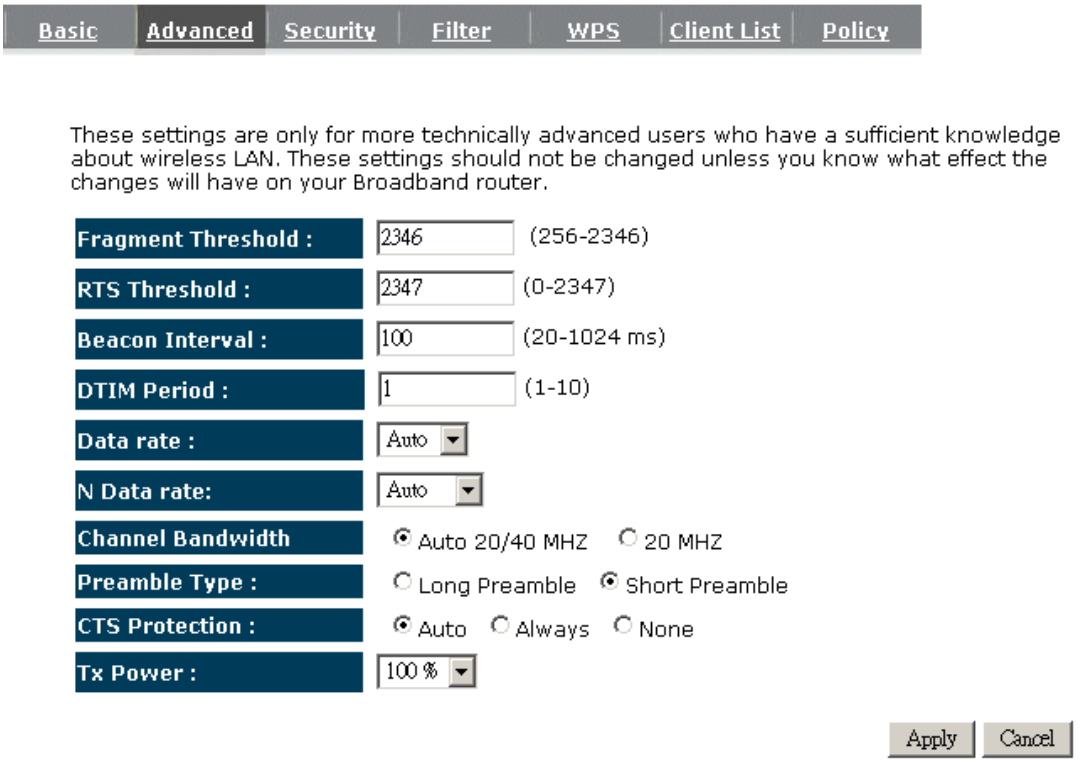


MAC address 1~4: Please enter the MAC address(es) of the neighboring APs which participate in WDS. There can be maximum of 4 devices now.

Set Security: WDS Security depends on your AP security settings. Note: it does not support **mixed mode** such as WPA-PSK/WPA2-PSK Mixed mode.

- Advanced

This tab allows you to set the advanced wireless options. You should not change these parameters unless you know what effect the changes will have on the router.



Fragment Threshold: This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold: When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval: This is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

DTIM Period: Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

Data Rate: The ñData Rateò is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate: The ñData Rateò is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth: This is the range of frequencies that will be used.

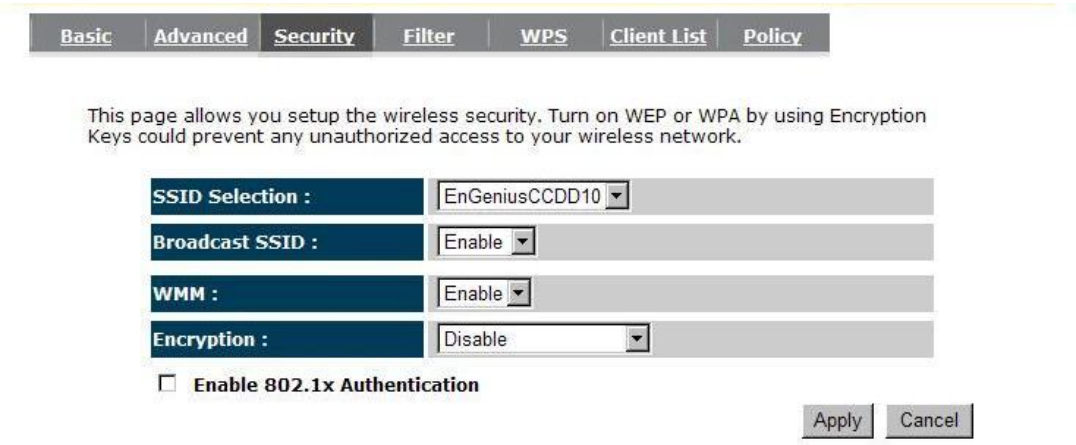
Preamble Type: The ñLong Preambleò can provide better wireless LAN compatibility while the ñShort Preambleò can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

TX Power: This can be set to a bare minimum or maximum power.

- Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.



ESSID Selection: This Router support multiple ESSID, you could select and set up the wanted ESSID.

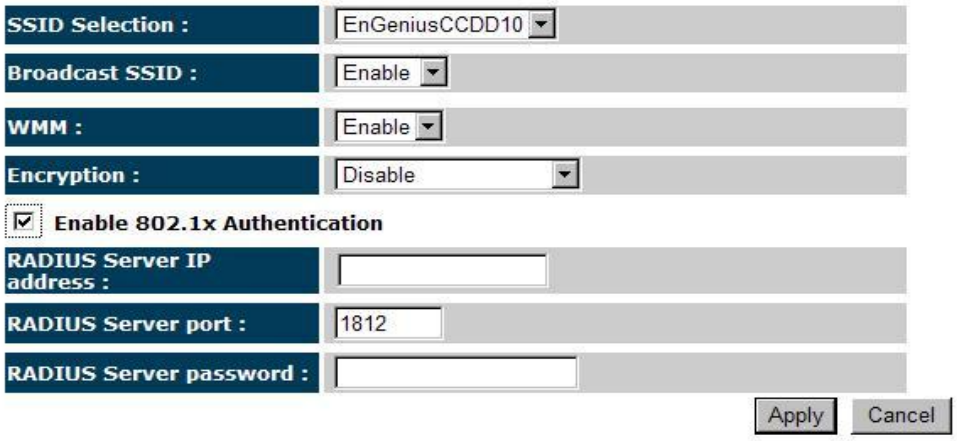
Broadcast ESSID: If you enabled ñBroadcast ESSIDò, every wireless station located within the coverage of this AP can discover this AP easily. If you are building a public wireless network, enabling this feature is recommended. Disabling ñBroadcast ESSIDò can provide better security.

WMM: Wi-Fi MultiMedia if enabled supports QoS for experiencing better audio, video and voice in applications.

Encryption: When you choose to disable encryption, it is very insecure to operate ESR6650.

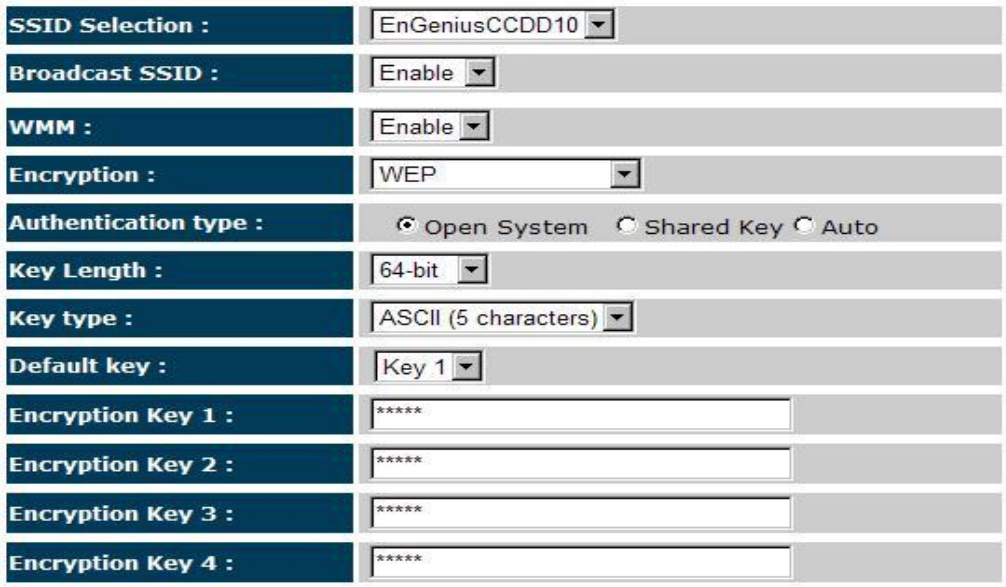
Enable 802.1x Authentication

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.



WEP Encryption

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then AP can receive any packet encrypted by one of the four keys.



Authentication Type: There are two authentication types: **"Open System"** and **"Shared Key"**. Both AP and wireless client must be configured with the same authentication type.

Key Length: You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Type: You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Default Key: It's the key used to encrypt data.

Key1 - Key4: The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device.

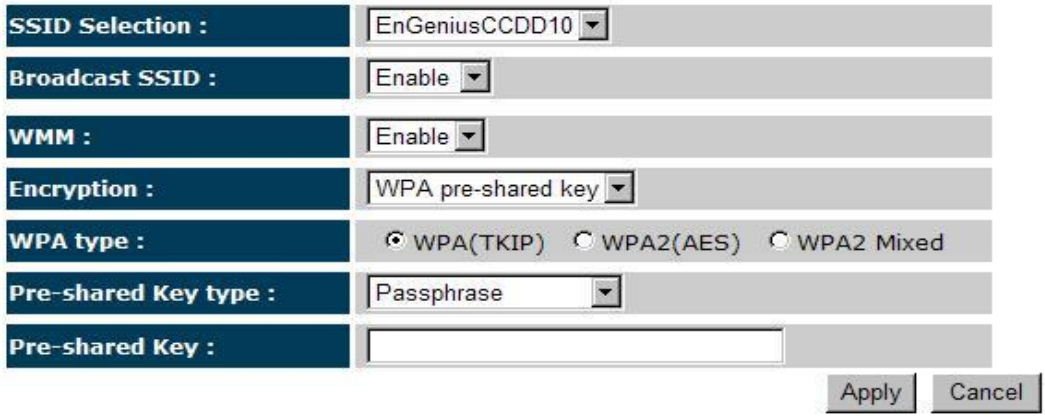
64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys.

128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click **<Apply>** at the bottom of the screen to save the above configurations.

WPA Pre-Shared Key Encryption

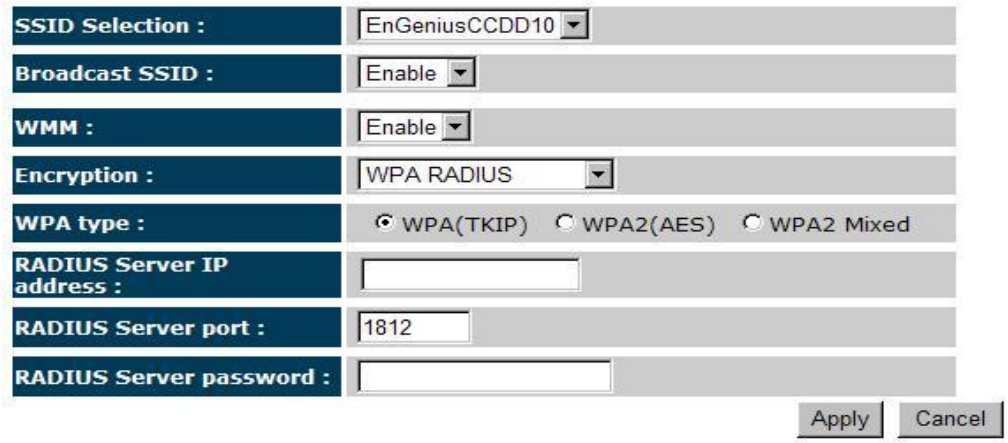
Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.



WPA-Radius Encryption

Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication.

It uses **TKIP** or CCMP (**AES**) to change the encryption key frequently. Press **<Apply>** button when you are done.



- MAC Address Filtering

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

Enable wireless access control: Enable the wireless access control function

Adding an address into the list

Enter the "MAC Address" and "Description" of the wireless station to be added and then click **<Add>**. The wireless station will now be added into the "MAC Address Filtering Table" below. If you are having any difficulties filling in the fields, just click "Reset" and both "MAC Address" and "Description" fields will be cleared.

Remove an address from the list

If you want to remove a MAC address from the "MAC Address Filtering Table", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Wi-Fi Protected Setup (WPS)

WPS is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the "Start to Process" button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

WPS: Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status: If the wireless security (encryption) function of this wireless router is properly set, you'll see a "Configured" message here. Otherwise, you'll see "**UnConfigured**".

Self Pin Code: This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID: This is the network broadcast name (SSID) of the router.

Authentication Mode: It shows the active authentication mode for the wireless connection.

Passphrase Key: It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

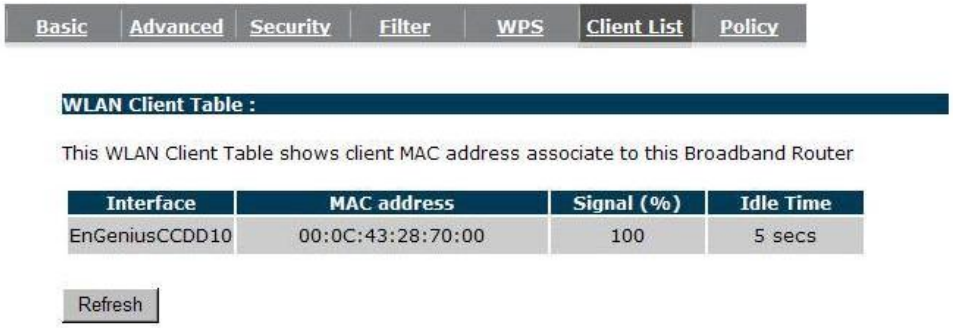
Interface: If device is set to repeater mode, you can choose **"Client"** interface to connect with other AP by using WPS, otherwise you may choose **"AP"** interface to do WPS with other clients.

WPS via Push Button: Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN: You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

- Client List

This WLAN Client Table shows the Wireless client associate to this Wireless Router.



- Policy

The Router can allow you to set up the Wireless Access Policy.

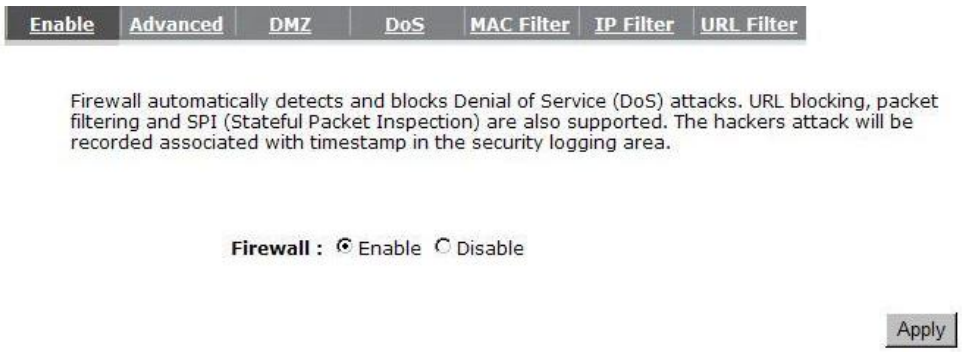
WAN Connection: Allow Wireless Client on specific SSID to access WAN port.

Communication between Wireless clients: Allow Wireless Client to communicate with other Wireless Client on specific SSID.

Communication between Wireless clients and wired clients: Allow Wireless Client to communicate with other Wireless Client on specific SSID and Wired Client on the switch. Or Wireless Client will allow to access WAN port only

5.5. Firewall Settings

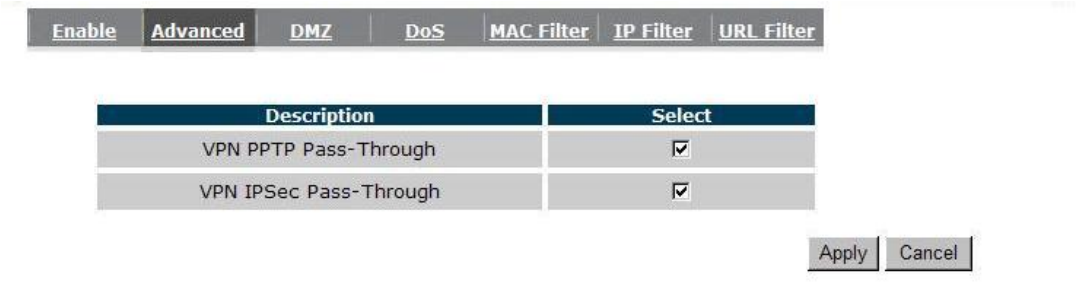
The Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).



Note: To enable the Firewall settings select Enable and click Apply

- Advanced

You can allow the VPN packets to pass through this Router.



- Demilitarized Zone (DMZ)

If you have a client PC that cannot run an Internet application (e.g. Games) properly behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all

packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) from your WAN IP address to a particular LAN client/server.

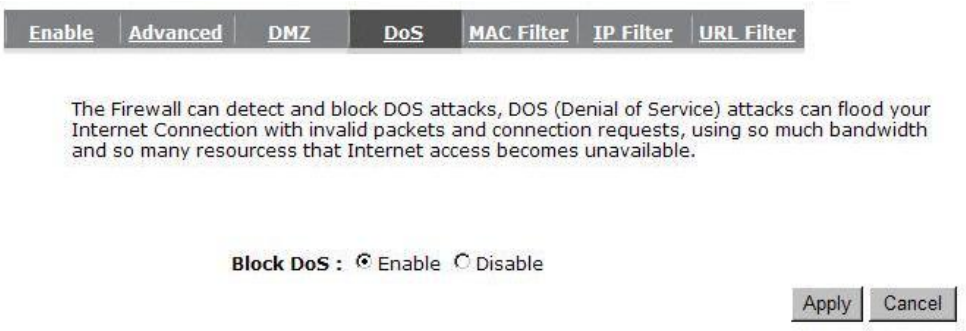
Enable DMZ: Enable/disable DMZ

LAN IP Address: Fill-in the IP address of a particular host in your LAN Network or select a PC from the list on the right that will receive all the packets originally from the WAN port/Public IP address.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- Denial of Service (DoS)

The Router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



Ping of Death: Protections from Ping of Death attack.

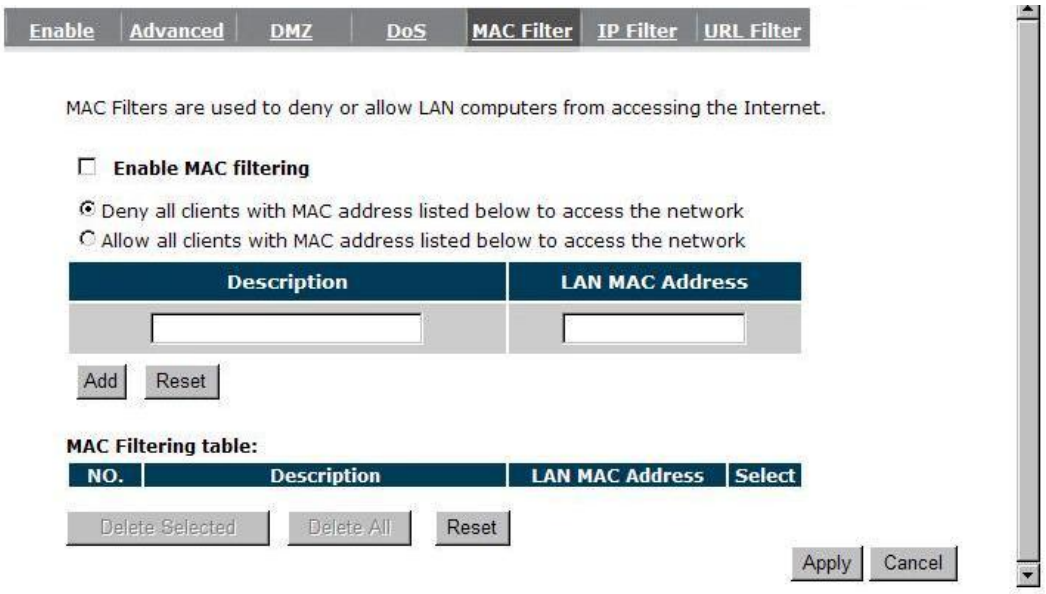
Discard Ping From WAN: The routerôs WAN port will not respond to any Ping requests

Port Scan: Protects the router from Port Scans.

Sync Flood: Protects the router from Sync Flood attack.

- MAC Filter

If you want to restrict users from accessing certain Internet applications / services (e.g. Internet websites, email, FTP etc.), and then this is the place to set that configuration. MAC Filter allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.



Enable MAC Filtering: Check to enable or disable MAC Filtering.

Deny: If you select ñ**Deny**ò then all clients will be allowed to access Internet except the clients in the list below.

Allow: If you select ñ**Allow**ò then all clients will be denied to access Internet except the PCs in the list below.

Add PC MAC Address

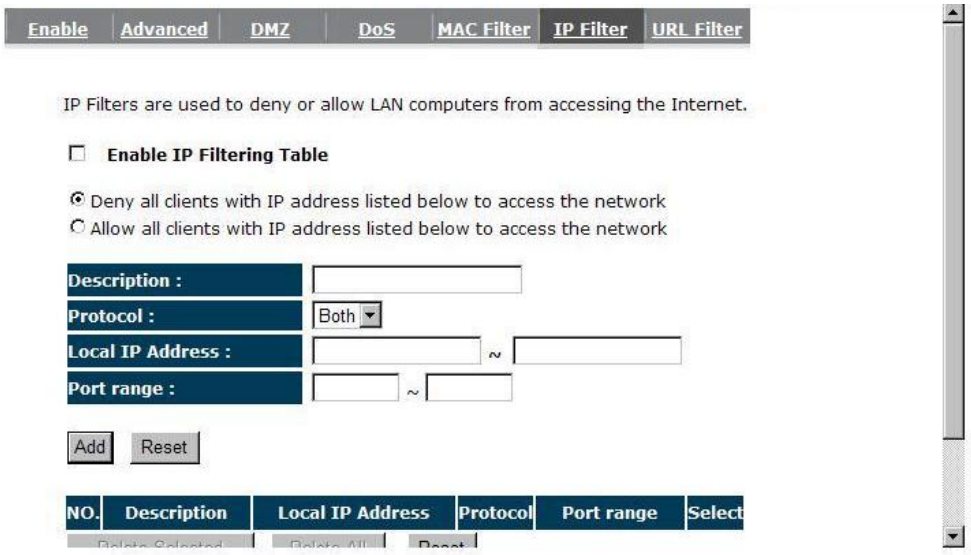
Fill in the **LAN MAC Address** and **<Description>** of the PC that is allowed / denied to access the Internet, and then click **<Add>**. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

Remove PC MAC Address

If you want to remove some PC from the "**MAC Filtering Table**", select the PC you want to remove in the table and then click **<Delete Selected>**. If you want to remove all PCs from the table, just click the **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset>**.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- IP Filter



Enable IP Filtering: Check to enable or uncheck to disable IP Filtering.

Deny: If you select ñ**Deny**ò then all clients will be allowed to access Internet except for the clients in the list below.

Allow: If you select ñ**Allow**ò then all clients will be denied to access Internet except for the PCs in the list below.

Add PC IP Address

You can click **<Add>** PC to add an access control rule for users by an IP address or IP address range.

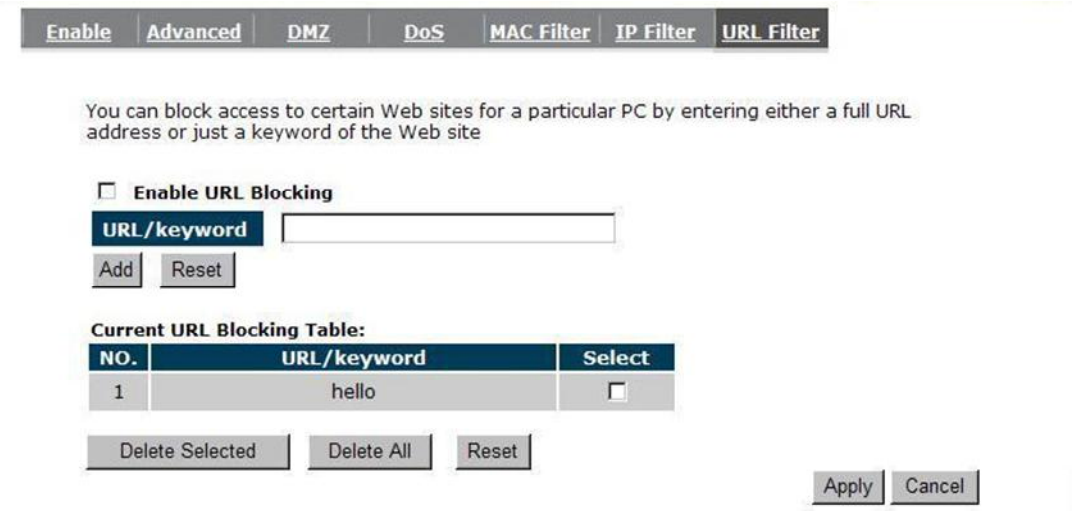
Remove PC IP Address

If you want to remove some PC IP from the **<IP Filtering Table>**, select the PC you want to remove in the table and then click **<Delete Selected>**. If you want to remove all PCs from the table, just click the **<Delete All>** button.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- URL Filter

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.



Enable URL Blocking: Enable or disable URL Blocking

Add URL Keyword

Fill in ñURL/Keywordò and then click **<Add>**. You can enter the full URL address or the keyword of the web site you want to block. If you happen to make a mistake and want to retype again, just click "Reset" and the field will be cleared.

Remove URL Keyword

If you want to remove some URL keywords from the "**Current URL Blocking Table**", select the URL keyword you want to remove in the table and then click **<Delete Selected>**.

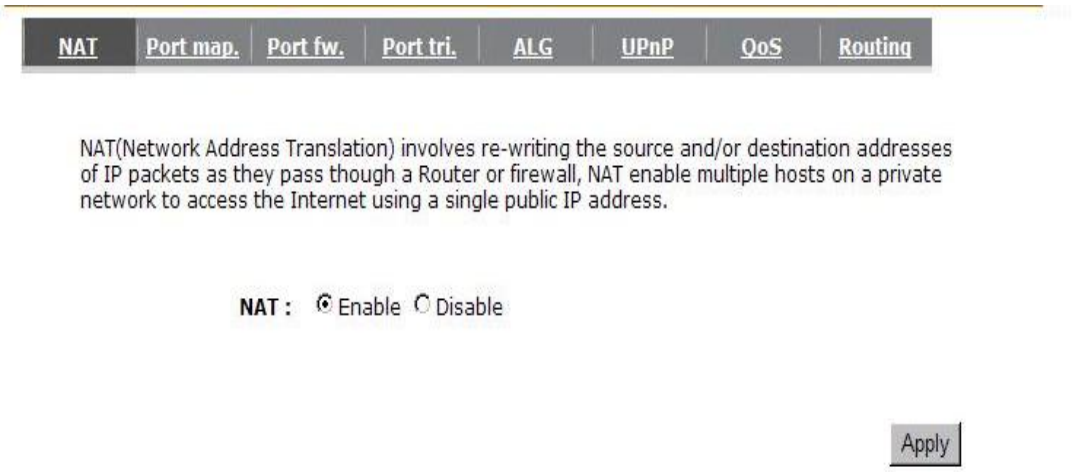
If you want remove all URL keywords from the table, click **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset**>.

Click **<Apply>** at the bottom of the screen to save the above configurations

5.6. Advanced Settings

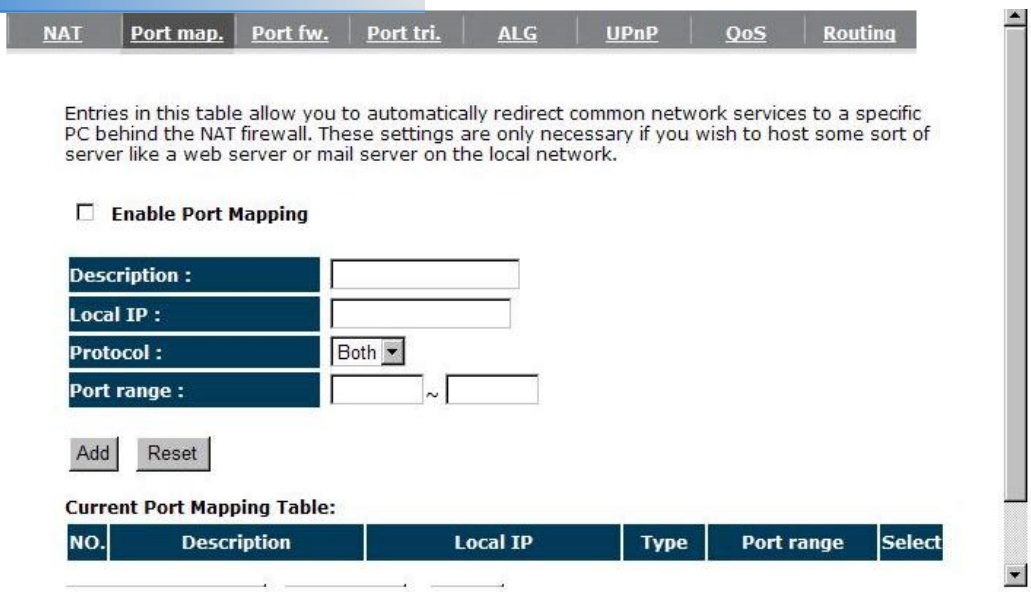
- Network Address Translation (NAT)

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.



- Port Mapping

Port Mapping allows you to re-direct a particular range of service port numbers (from the Internet / WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.



Enable Port Mapping: Enable or disable port mapping function.

Description: description of this setting.

Local IP: This is the local IP of the server behind the NAT firewall.

Protocol: This is the protocol type to be forwarded. You can choose to forward ñTCPò or ñUDPò packets only, or select ñBOTHò to forward both ñTCPò and ñUDPò packets.

Port Range: The range of ports to be forward to the private IP.

Add Port Mapping

Fill in the "**Local IP**", ñProtocolò ñPort Rangeò and "**Description**" of the setting to be added and then click "**Add**". Then this Port Mapping setting will be added into the "**Current Port Mapping Table**" below. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

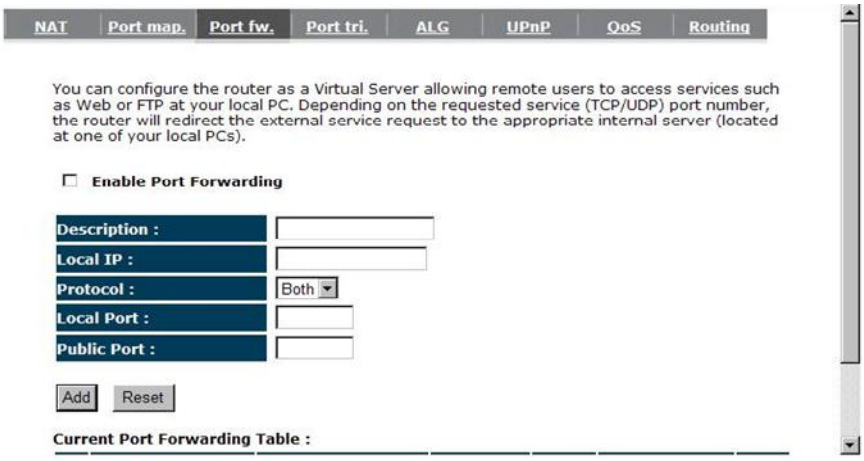
Remove Port Mapping

If you want to remove a Port Mapping setting from the "**Current Port Mapping Table**", select the Port Mapping setting that you want to remove in the table and then click **D<Delete Selected>**. If you want to remove all Port Mapping settings from the table, click **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

- Port Forwarding (Virtual Server)

Use the Port Forwarding (Virtual Server) function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address (See Glossary for an explanation on Port number).



Enable Port Forwarding: Enable or disable Port Forwarding.

Description: The description of this setting.

Local IP / Local Port: This is the LAN Client/Host IP address and Port number that the Public Port number packet will be sent to.

Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. Public Port enters the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN Network.

Public Port: Port number will be changed to Local Port when the packet enters your LAN Network.

Add Port Forwarding

Fill in the "**Description**" , "**Local IP**", "**Local Port**", "**Protocol**" and "**Public Port**" of the setting to be added and then click **<Add>** button. Then this Virtual Server setting will be added into the "**Current Port Forwarding Table**" below. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

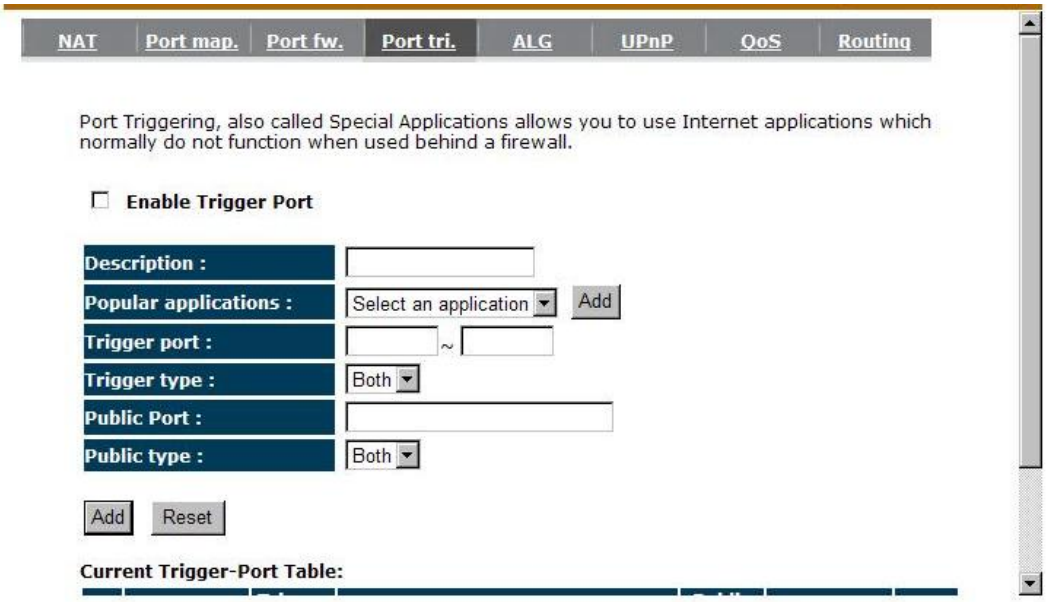
Remove Port Forwarding

If you want to remove Port Forwarding settings from the "**Current Port Forwarding Table**", select the Port Forwarding settings you want to remove in the table and then click "**Delete Selected**". If you want to remove all Port Forwarding settings from the table, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

- Port Triggering (Special Applications)

Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Enable Trigger Port: Enable or disable the Port Trigger function.

Trigger Port: This is the outgoing (Outbound) range of port numbers for this particular application.

Trigger Type: Select whether the outbound port protocol is ñ**TCP**ò ñ**UDP**òor ñ**BOTH**ò

Public Port: Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)

Public Type: Select the Inbound port protocol type: ñ**TCP**ò ñ**UDP**òor ñ**BOTH**ò

Popular Applications: This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location

(1-5) in the ñAddò selection box and then click the <Add> button. This will automatically list the Public Ports required for this popular application in the location (1-5) you specified.

Add Port Triggering

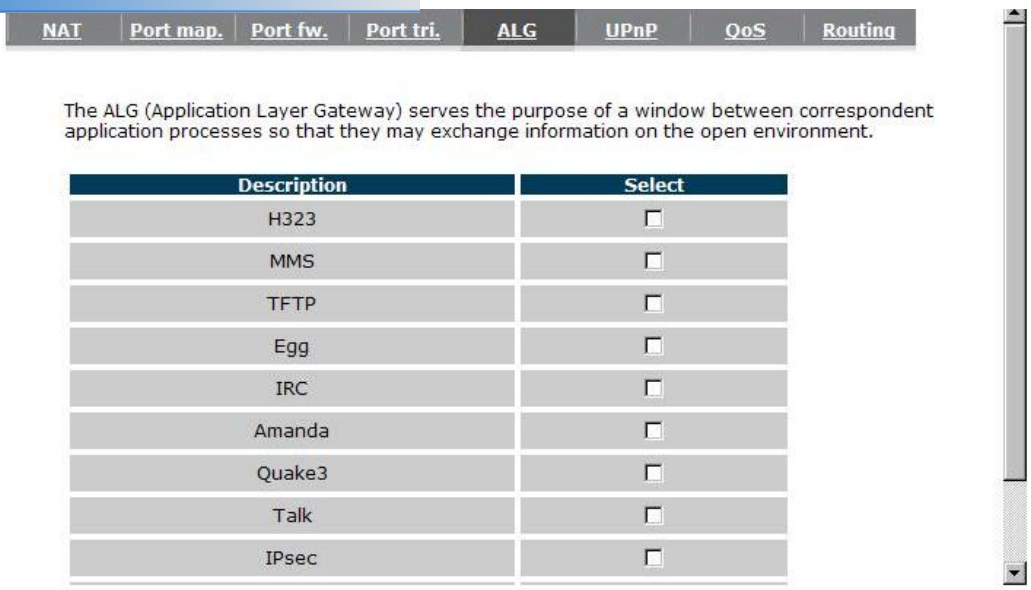
Fill in the "**Trigger Port**", "**Trigger Type**ò ñ**Public Port**ò "**Public Type**", "**Public Port**" and "**Description**" of the setting to be added and then Click **<Add>**. The Port Triggering setting will be added into the "**Current Trigger-Port Table**" below. If you happen to make a mistake, just click **<Reset>** and the fields will be cleared.

Remove Port Triggering

If you want to remove Special Application settings from the "**Current Trigger-Port Table**", select the Port Triggering settings you want to remove in the table and then click **<Delete Selected>**. If you want remove all Port Triggering settings from the table, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

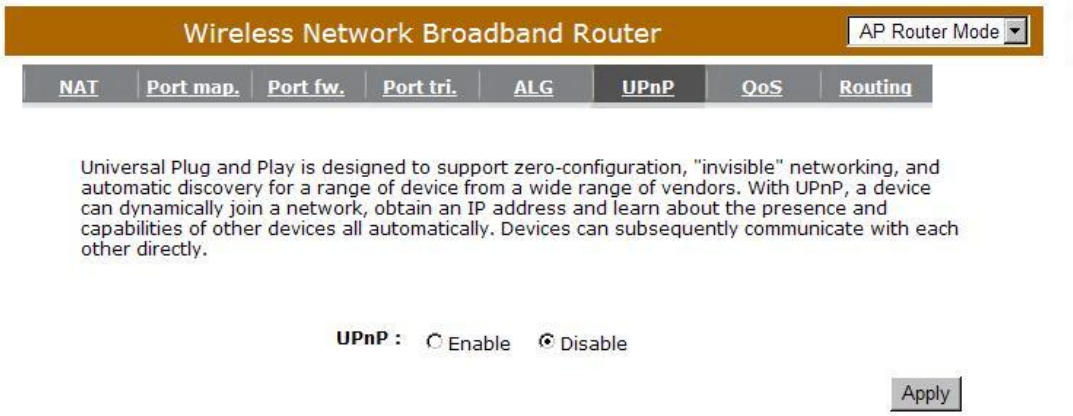
- Application Layer Gateway (ALG)

You can select applications that need **ALG** support. The router will let the selected application to correctly pass through the NAT gateway.



- UPNP

With UPnP, all PCs in you Intranet will discover this router automatically. So, you don't have to configure your PC and it can easily access the Internet through this router.



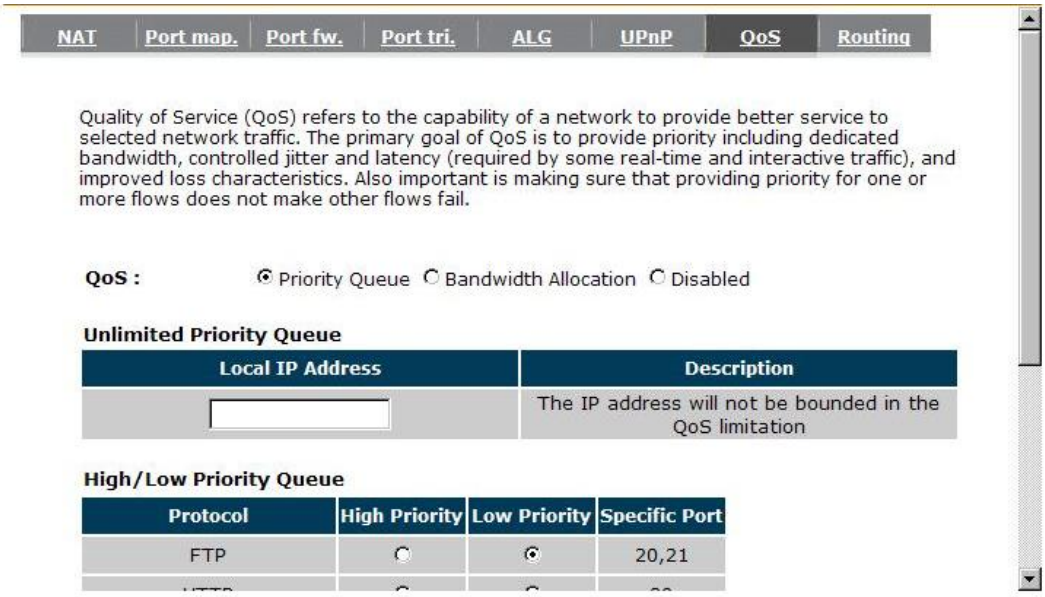
Enable/Disable UPnP: You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

- Quality of Service (QoS)

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference é etc. All the applications not specified by you are classified as rule ñOthersò

Priority Queue

This can put the packets of specific protocols in High/Low Queue. The packets in High Queue will process first.

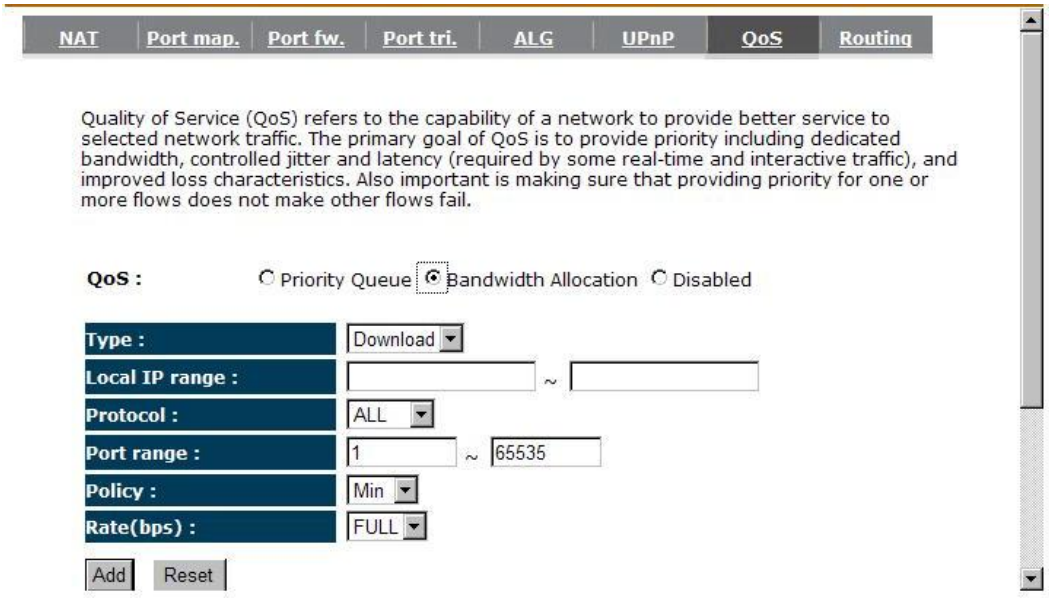


Unlimited Priority Queue: The LAN IP address will not be bounded in the QoS limitation.

High/Low Priority Queue: This can put the packets in the protocol and port range to High/Low QoS Queue.

Bandwidth Allocation:

This can reserve / limit the throughput of specific protocols and port range. You can set the upper bound and Lower bound.



Type: Specify the direction of packets. Upload, download or both.

IP range: Specify the IP address range. You could also fill one IP address

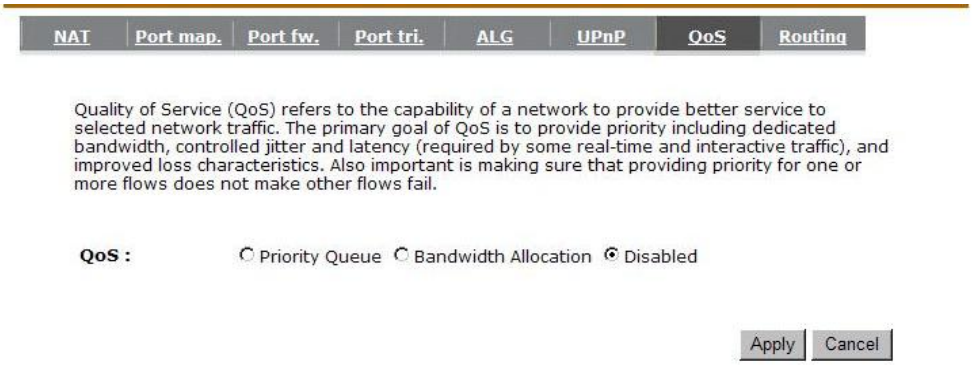
Protocol: Specify the packet type. The default ALL will put all packets in the QoS priority Queue.

Port range: Specify the Port range. You could also fill one Port.

Policy: Specify the policy the QoS, **Min** option will reserve the selected data rate in QoS queue. **Max** option will limit the selected data rate in QoS queue.

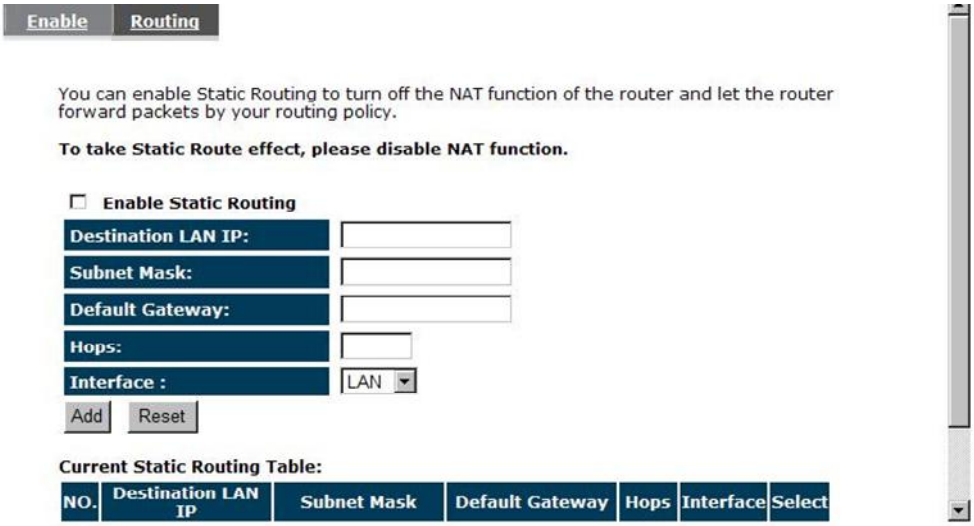
Rate: The data rate of QoS queue.

Disabled: This could turn off QoS feature.



- Routing

You can set enable Static Routing to let the router forward packets by your routing policy.



Destination LAN IP: Specify the destination LAN IP address of static routing rule.

Subnet Mask: Specify the Subnet Mask of static routing rule.

Default Gateway: Specify the default gateway of static routing rule.

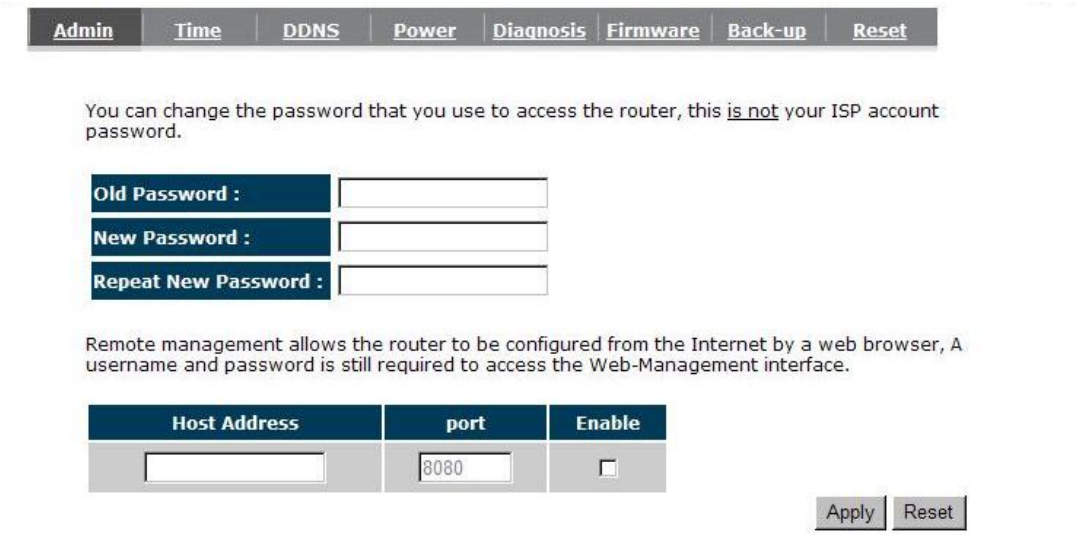
Hops: Specify the Max Hops number of static routing rule.

Interface: Specify the Interface of static routing rule.

5.7. TOOLS Settings

- Admin

You can change the password required to log into the Router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.



Old Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and type it again in **Repeat New Password** for verification purposes

Remote management

This allows you to designate a host in the Internet the ability to configure the Router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address: This is the IP address of the host in the Internet that will have management/configuration access to the Router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the routerôs web-based configuration from a remote location, providing they know the password.

Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

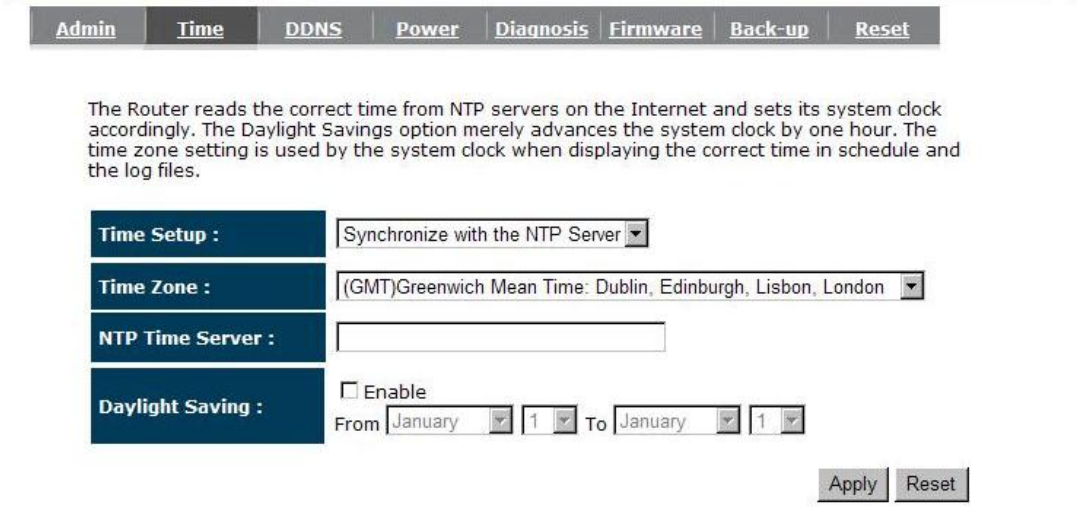
Click <**Apply**> at the bottom of the screen to save the above configurations.

- Time

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Time Setup:

Synchronize with the NTP server



Time Zone: Select the time zone of the country you are currently in. The router will set its time based on your selection.

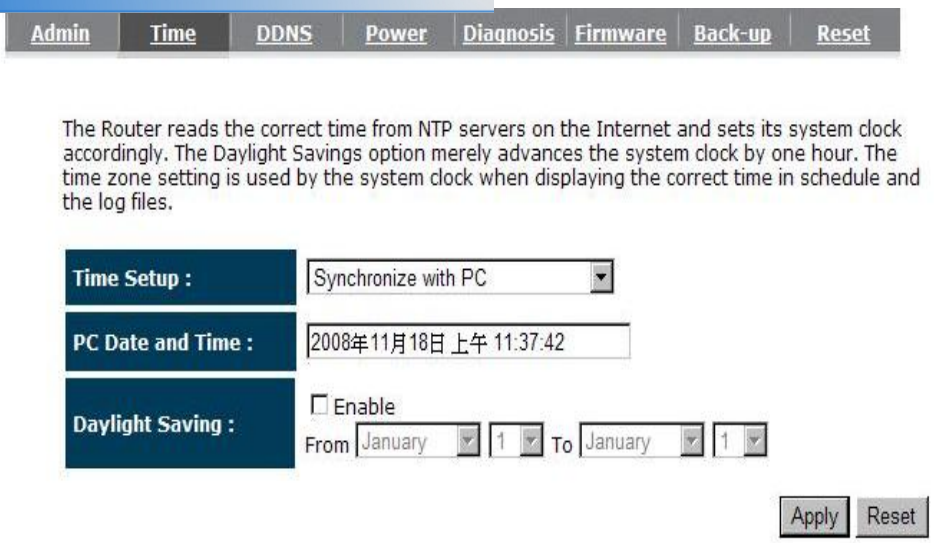
NTP Time Server: The router can set up external NTP Time Server.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Synchronize with PC

You could synchronize timer with your Local PC time.



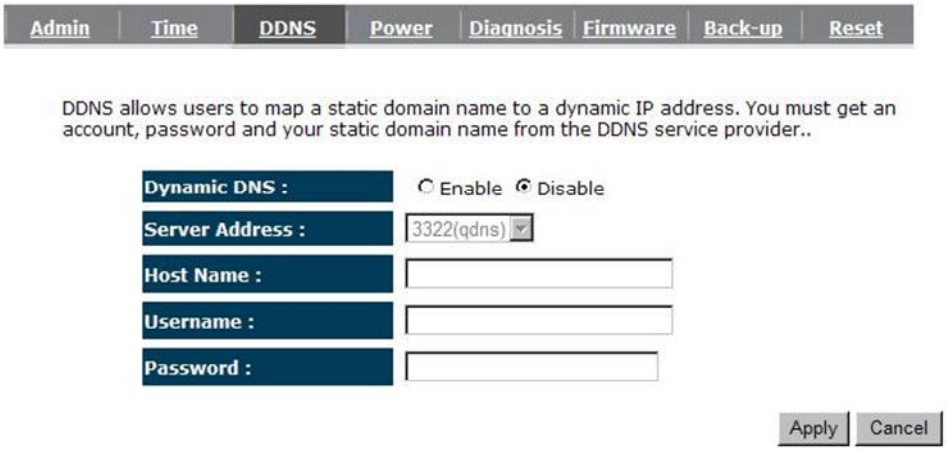
PC Date and Time: This field would display the PC date and time.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

- DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.



Enable/Disable DDNS: Enable or disable the DDNS function of this router

Server Address: Select a DDNS service provider

Host Name: Fill in your static domain name that uses DDNS.

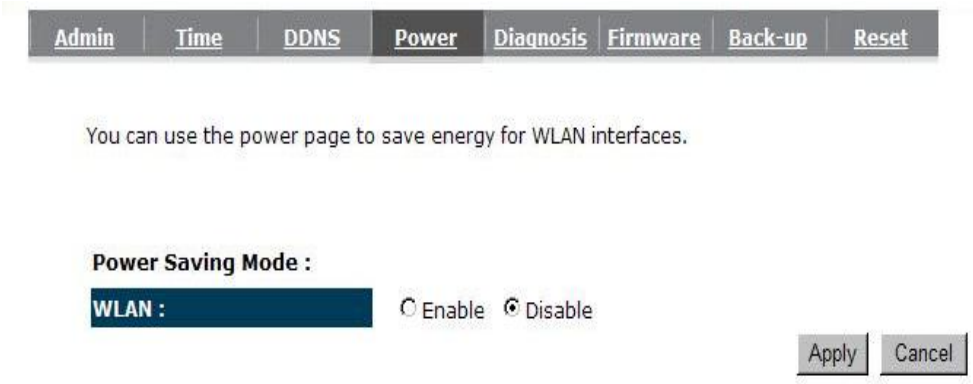
Username: The account that your DDNS service provider assigned to you.

Password: The password you set for the DDNS service account above

Click **<Apply>** at the bottom of the screen to save the above configurations.

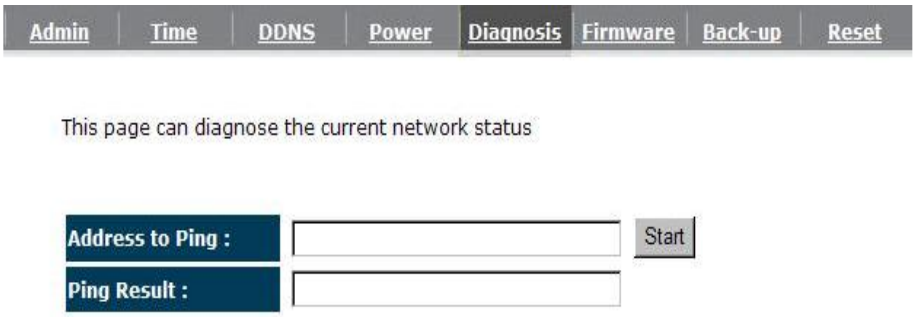
- Power

Saving power in WLAN mode can be enabled / disabled in this page.



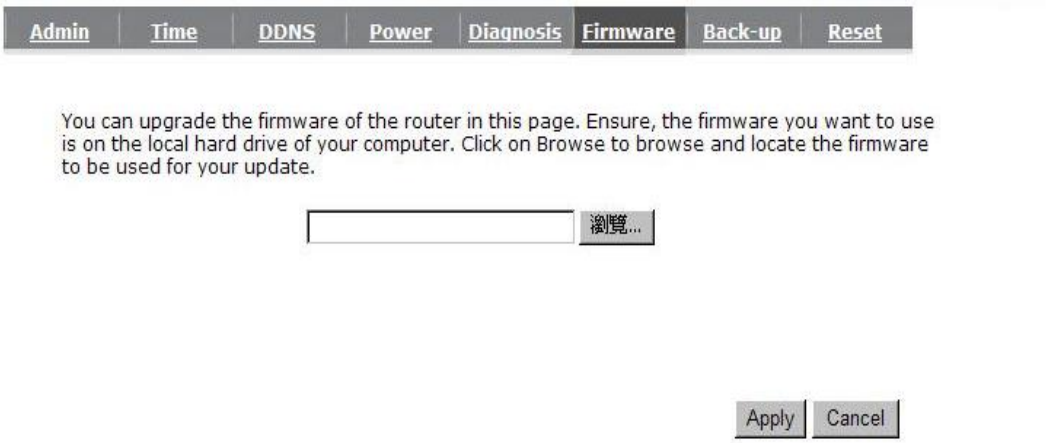
- Diagnosis

This page could let you diagnosis your current network status.



- Firmware

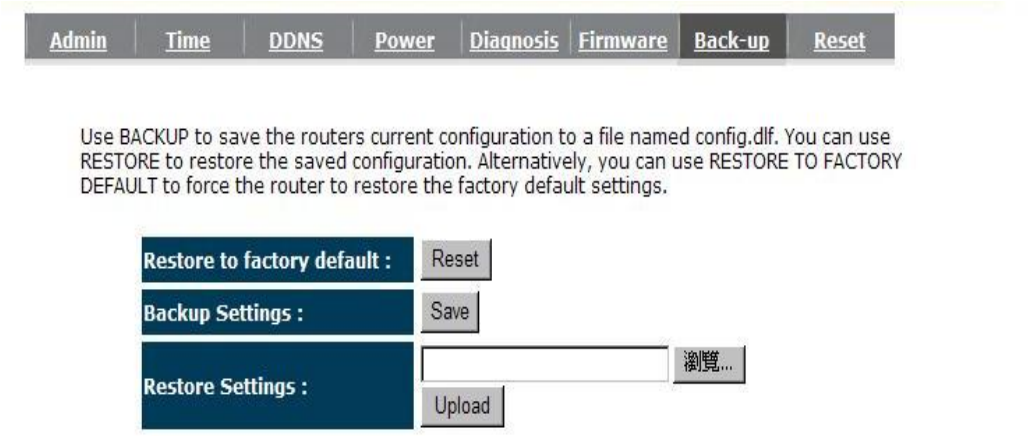
This page allows you to upgrade the routerôs firmware. To upgrade the firmware of your Router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.



Once youôve selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process

- Back-up

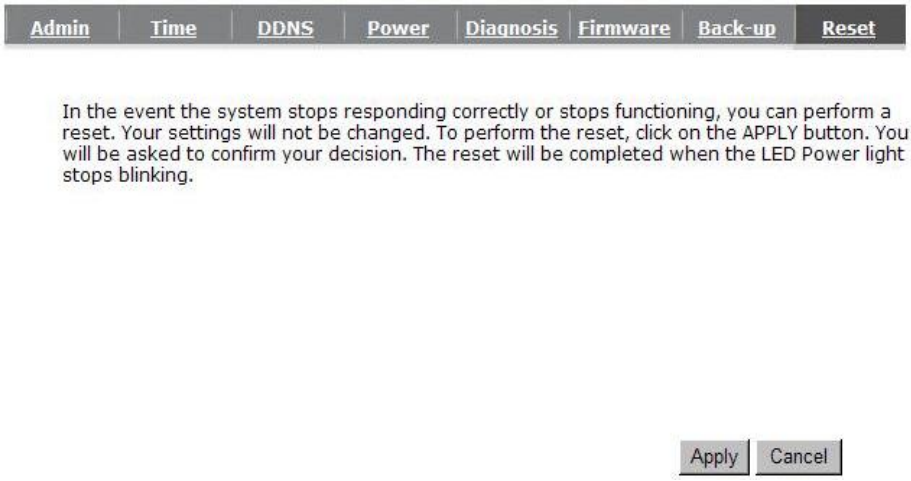
This page allows you to save the current router configurations. When you save the configurations, you also can re-load the saved configurations into the router through the **Restore Settings**. If extreme problems occur you can use the **Restore to Factory Defaults** to set all configurations to its original default settings.



Backup Settings: This can save the Router current configuration to a file named "**config.bin**" on your PC. You can also use the **<Upload>** button to restore the saved configuration to the Router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the Router to perform a power reset and restore the original factory settings.

- Reset

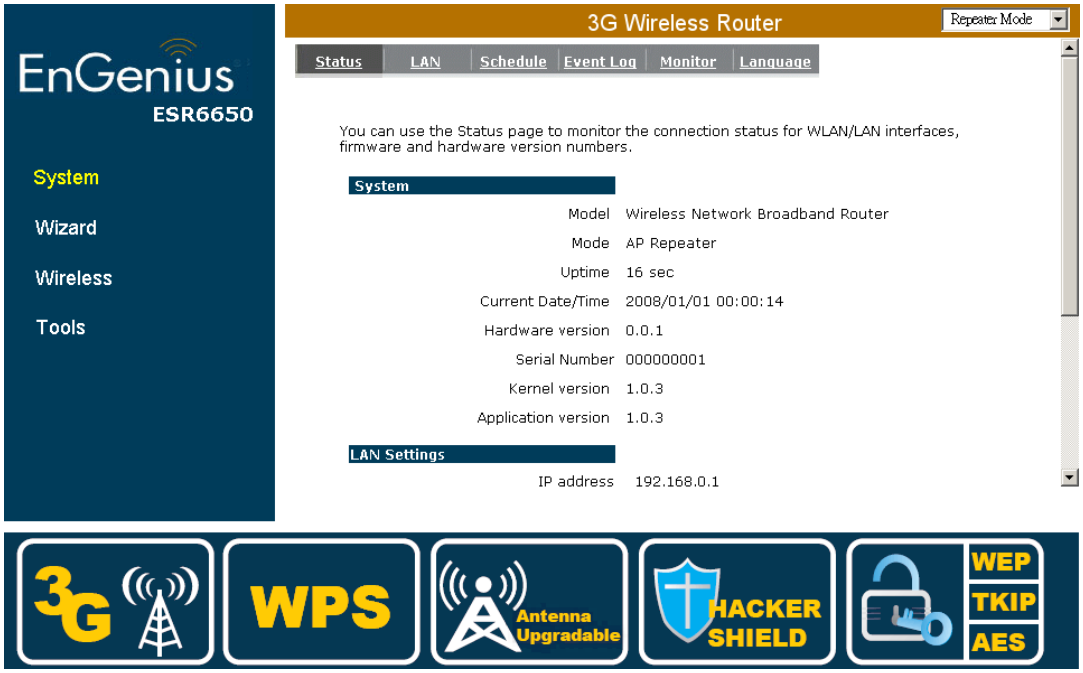
You can reset the Router when system stops responding correctly or stop functions.



6. Repeater Mode

Repeater mode has limited settings compared to the AP mode. Choose ñRepeater modeòon the top right corner of the configuration page.

System restarts and connects to the IP address http://192.168..0.1
You will see the configuration homepage under ñ**REPEATER**òmode now.



6.1. System

- Status

System status section allows you to monitor the current status of your router.

You can see the Uptime, hardware information, serial number as well as firmware version information.

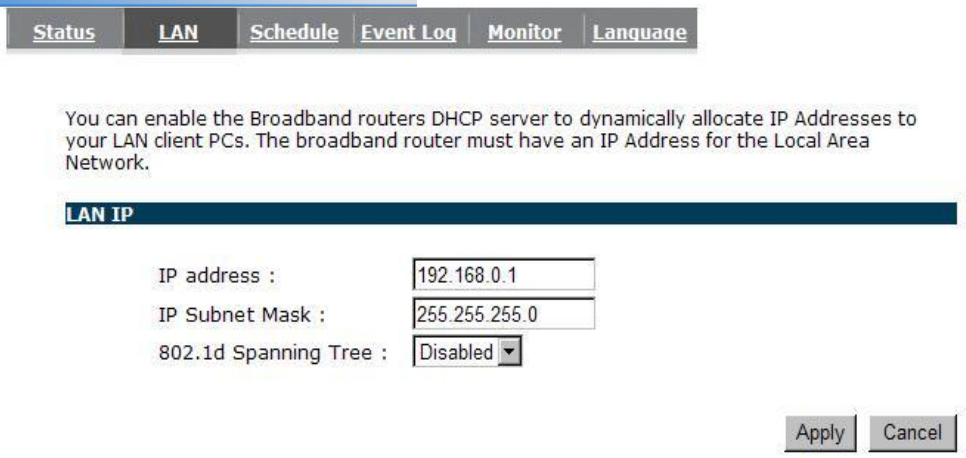
LAN Settings: This page displays the Router LAN ports current LAN & WLAN information.

WLAN Settings: Wireless configuration details such as SSID, Security settings, BSSID, Channel number, mode of operation are briefly shown.

- LAN

The LAN Tabs reveals LAN settings which can be altered at will. If you are an entry level user, try accessing a website from your browser. If you can access website without a glitch, just do not change any of these settings.

Click **<Apply>** at the bottom of this screen to save the changed configurations.



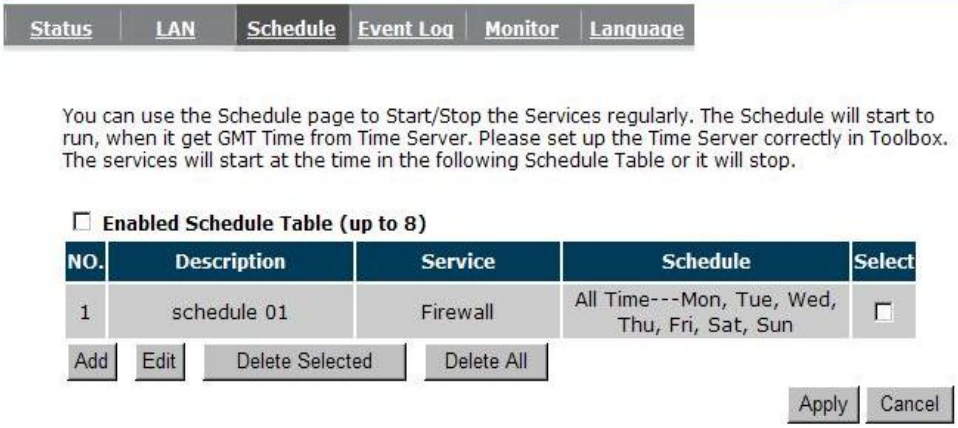
IP address: It is the routerôs LAN IP address (Your LAN clients default gateway IP address). It can be changed based on your own choice.

IP Subnet Mask: Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

- Schedule

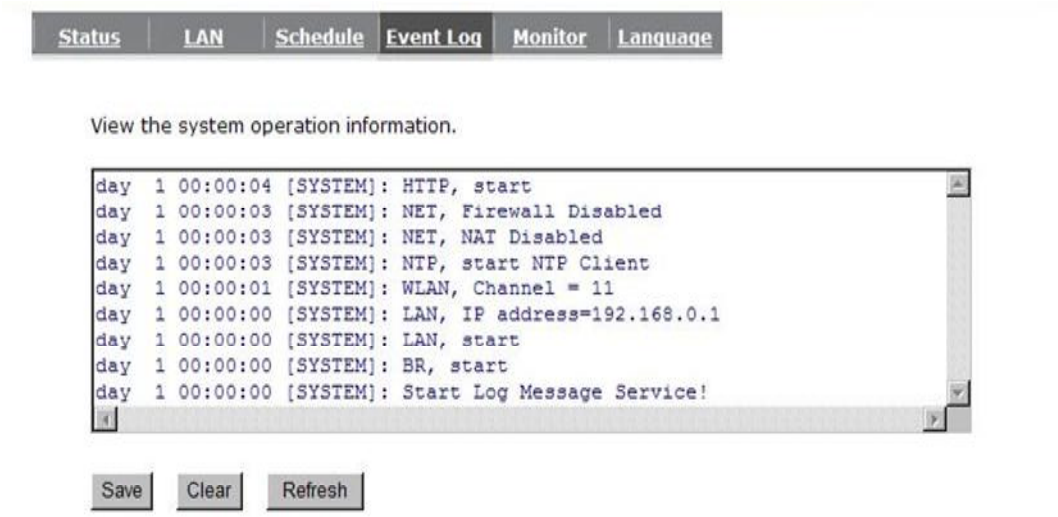
Add schedule, edit schedule options allow configuration of power savings services. Fill in the schedule and select type of service. Click **<Apply>** to implement the settings.



The schedule table lists the pre-schedule service-runs. You can select any of them using the check box.

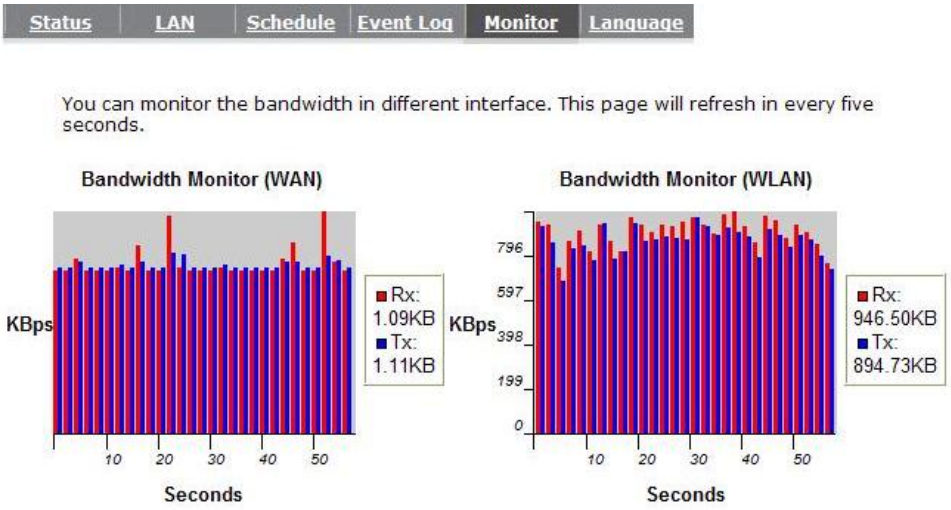
- Event Log

View operation **log of ESR6650**. This page shows the current system log of the Router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



- Monitor

Show the network packets histogram for network connection on WAN, LAN & WLAN. Auto refresh keeps information updated frequently.



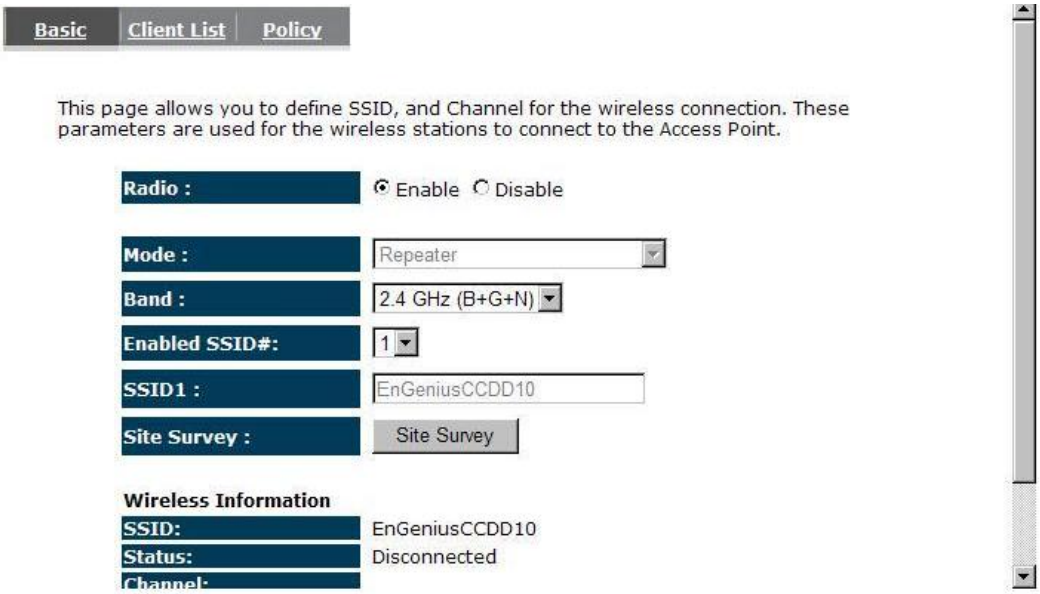
- Language

This Wireless Router support multiple language of web pages, you could select your native language here.

6.2. Wireless

-Basic

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.



Radio: Enable or Disable Wireless function

Band: Allows you to set the AP fixed at 802.11b, 802.11g or 802.11n mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.

Enable ESSID: You can specify the maximum ESSID number.

ESSID1~3: Allow you to specify ESSID of WLAN.

Site Survey: You can scan the current Wireless Access Point and connect on it.

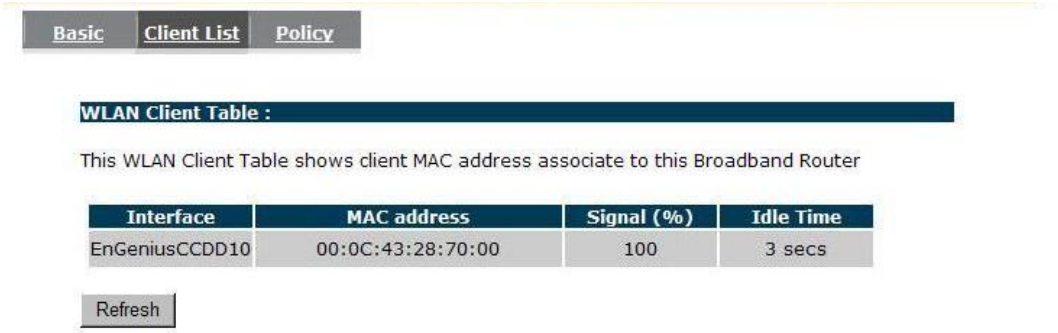
Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Auth	Signal (%)	Mode
1	○	1	ADSL_1	00:02:6f:4c:64:a0	AES	WPA2PSK	50	11b/g/n
2	○	3	ADSL_2	00:02:6f:48:0d:8b	WEP	OPEN	100	11b/g
3	○	9	ADSL_3	00:16:b6:28:07:34	NONE	OPEN	65	11b/g

Refresh Connect

-Client List

This WLAN Client Table shows the Wireless client associate to this Wireless Router.



-Policy

The Router can allow you to set up the Wireless Access Policy.

Communication between Wireless clients:

Allow Wireless Client to communicate with other Wireless Client on specific SSID.

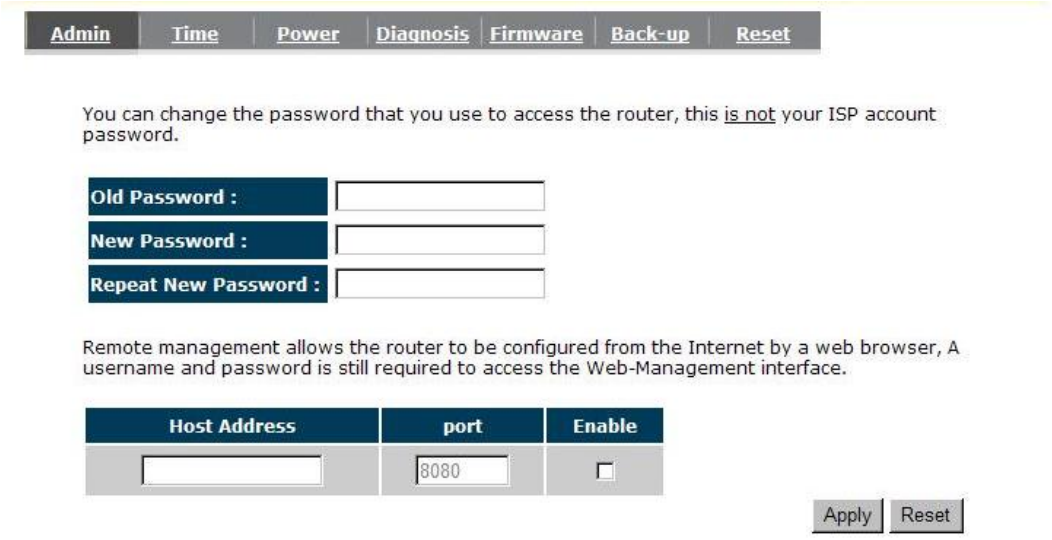
Communication between Wireless clients and wired clients:

Allow Wireless Client to communicate with other Wireless Client on specific SSID and Wired Client on the switch.

6.3. Tools

- Admin

You can change the password required to log into the Router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.



Old Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and in **Repeat New Password** for verification purposes

Click **<Apply>** at the bottom of the screen to save the above configurations

Remote management

This allows you to designate a host in the Internet the ability to configure the Router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address: This is the IP address of the host in the Internet that will have management/configuration access to the Router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the routerôs web-based configuration from a remote location, providing they know the password.

Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

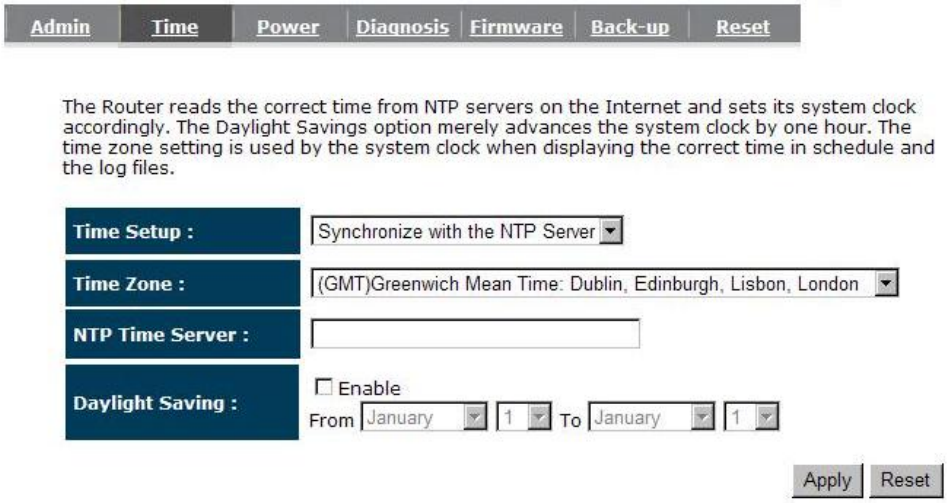
Click <**Apply**> at the bottom of the screen to save the above configurations.

- Time

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Event Log entries and Schedule settings.

Time Setup:

Synchronize with the NTP server



Time Zone: Select the time zone of the country you are currently in. The router will set its time based on your selection.

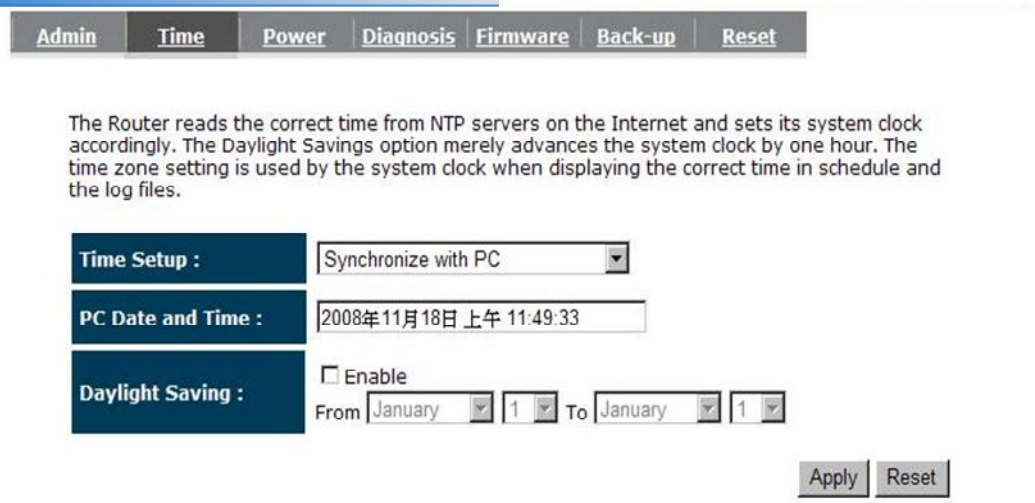
NTP Time Server: This accept local the IP Address of Local NTP Time Server Address.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click <**Apply**> at the bottom of the screen to save the above configurations

Synchronize with PC

You could synchronize timer with your Local PC time.



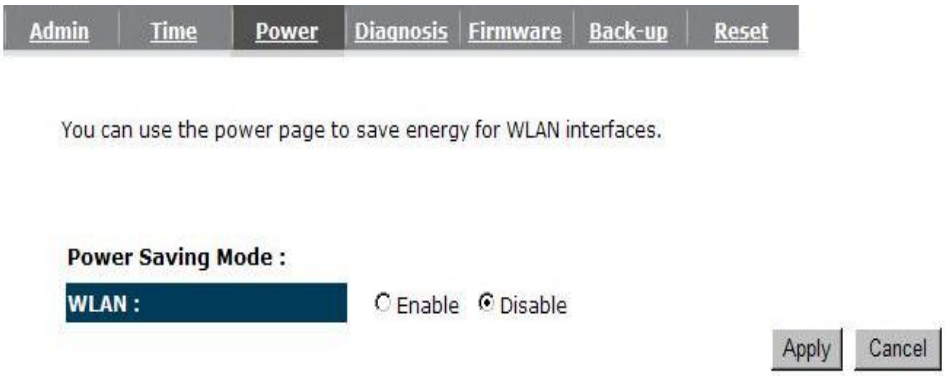
PC Date and Time: This field would display the PC date and time.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

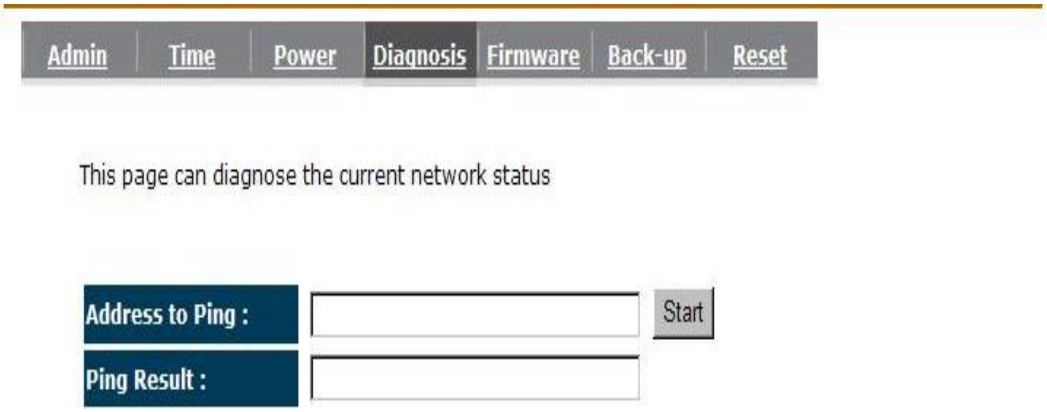
- Power

Saving power in WLAN mode can be enabled / disabled in this page.



- Diagnosis

This page could let you diagnosis your current network status.



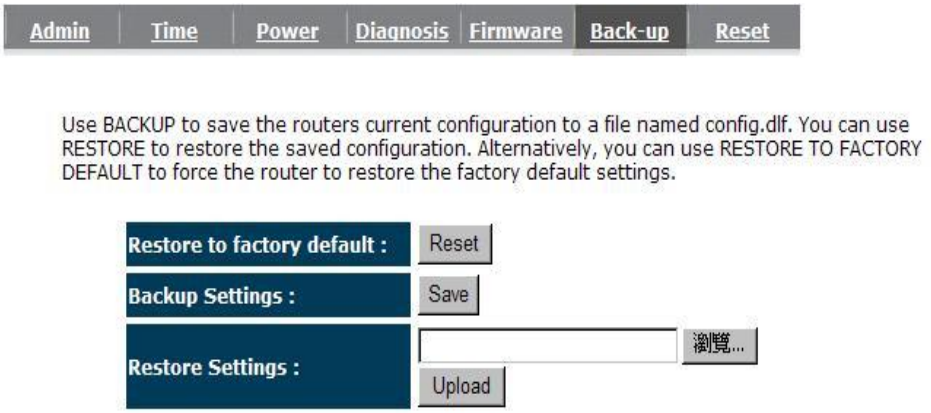
- Firmware

This page allows you to upgrade the routerôs firmware. To upgrade the firmware of your Router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process

- Back-up

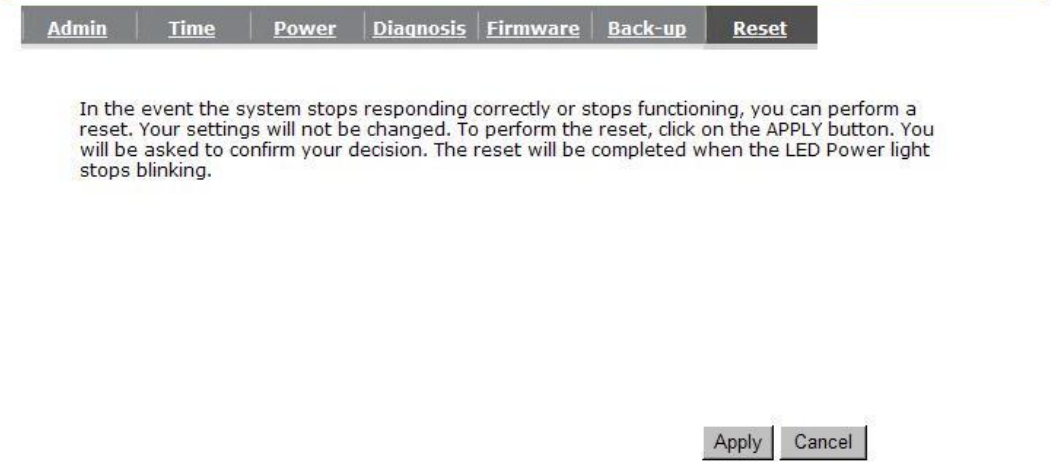
The page allows you to save (Backup) the routerûs current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the **Restore selection**. If extreme problems occur you can use the **Restore to Factory Defaults** selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



Backup Settings: This can save the Router current configuration to a file named "**config.bin**" on your PC. You can also use the **<Upload>** button to restore the saved configuration to the Router. Alternatively, you can use the "**Restore to Factory Defaults**" to force the Router to perform a power reset and restore the original factory settings.

- Reset

You can reset the Router when system stops responding correctly or stop functions.



Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

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

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 received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B – IC Interference Statement

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada 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 received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC 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.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.