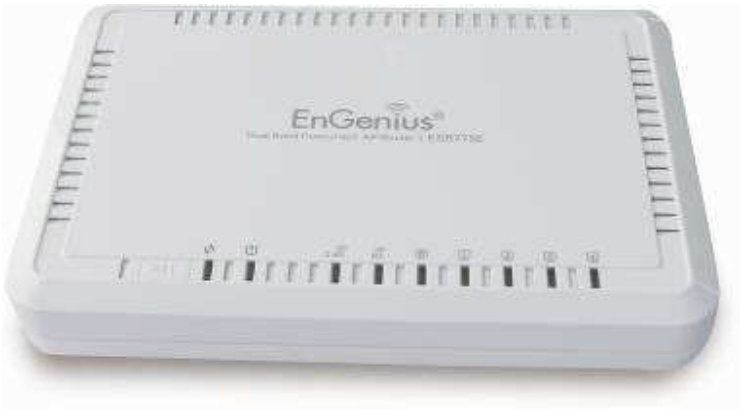
ESR7750

Dual Band Concurrent AP Router

(IEEE 802.11 a/b/g/n)



User Manual

Revision History

Version	Date	Notes
1.0	2009/1/22	Initial

Table of Content

1. INTRODUCTION 1

1.1. SUMMARY 1
1.2. KEY FEATURES 2
1.3. PACKAGE CONTENTS 3
1.4. PRODUCT LAYOUT 4

2. INSTALLATION 5

2.1. NETWORK + SYSTEM REQUIREMENTS 5
2.2. ESR7750 PLACEMENT 6
2.3. SETUP LAN & WAN 7
2.4. PC NETWORK ADAPTER SETUP (WINDOWS XP) 8
2.5. SMART WIZARD CD 10
2.6. WIZARD CONFIGURATION 12
2.7. INITIAL SETUP ESR7750 14

3. SYSTEM 16

3.1. STATUS 16
3.2. LAN 18
3.3. DHCP 19
3.4. SCHEDULE 20
3.5. EVENT LOG 21
3.6. MONITOR 22
3.7. LANGUAGE 23

4. WIZARD 24

5. INTERNET 25

5.1. STATUS 25
5.2. DYNAMIC IP 26
5.3. STATIC IP 27
5.4. POINT-TO-POINT OVER ETHERNET PROTOCOL (PPPOE) 28
5.5. POINT-TO-POINT TUNNELING PROTOCOL (PPTP) 29

6. WIRELESS 2.4G & 5G 30

6.1. BASIC 30
6.2. MODE: WDS 32
6.3. ADVANCED 32
6.4. SECURITY 34
6.5. FILTER 38
6.6. WPS (WI-FI PROTECTED SETUP) 39
6.7. CLIENT LIST 41
6.8. POLICY 42

7. FIREWALL 43

7.1. ENABLE 43
7.2. DEMILITARIZED ZONE (DMZ) 44
7.3. DENIAL OF SERVICE (DOS) 45
7.4. - MAC FILTER 46
7.5. IP FILTER 48
7.6. URL FILTER 49

8. ADVANCED 50

8.1. NETWORK ADDRESS TRANSLATION (NAT) 50
8.2. - PORT MAPPING 50
8.3. PORT FORWARDING (VIRTUAL SERVER) 52
8.4. PORT TRIGGERING (SPECIAL APPLICATIONS) 53
8.5. APPLICATION LAYER GATEWAY (ALG) 54
8.6. UPNP 55
8.7. QUALITY OF SERVICE (QOS) 55
8.8. ROUTING 58

9. TOOLS 59

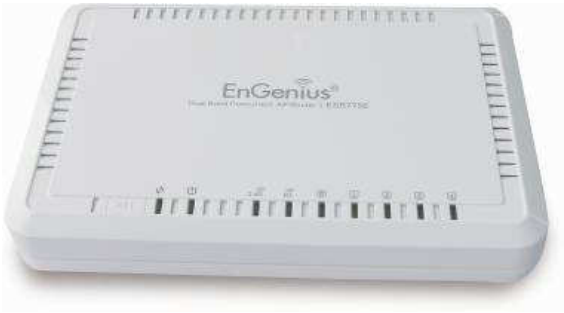
9.1. ADMIN 59
9.2. TIME 60
9.3. DDNS 61
9.4. POWER 62
9.5. DIAGNOSIS 63
9.6. FIRMWARE 64
9.7. BACK-UP 65
9.8. RESET 66

APPENDIX A – FCC INTERFERENCE STATEMENT 67

APPENDIX B – IC INTERFERENCE STATEMENT 68

1. Introduction

1.1. Summary



ESR7750 is a Dual Band Concurrent Wireless 11N Broadband Router with dual CPU that offers user unprecedented network performance. WMM support boosts streaming and multimedia intensive services. It supports 2.4Ghz band under 802.11 b/g/n mode while providing 5Ghz band to guarantee an interference-free network access.

Multiple SSID provides advance users to manage multiple users of various needs. TX power control enables flexible transmission tuning for different installation needs and prevents malicious eaves-dropping. Isolation, filter, firewall and full coverage of security standards promise a securer network environment.

Dual CPU operates work simultaneously therefore users can enjoy gaming, music or HD video on 5GHz band while web-surfing or emailing on 2.4Ghz. It also provides with built-in 4-port full-duplex 10/100 Fast Switch that allows wired ethernet for standard PC and other network devices. ESR7750 is definitely the optimal choice for both SOHO and small business entities.

1.2. Key Features

Features	Advantages
2.4Ghz & 5GhzDual Band Concurrent	**Less interference and better performance**
Incredible Data Rate up to 600Mbps**	**Heavy data payloads such as MPEG video streaming**
Multiple SSIDs	**Enhanced management among multiple users groups**
Four 10/100/1000 Mbps Fast Switch Ports (Auto-Crossover)	**Scalability, extend your network.**
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	**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**
WPS button support	**Quick WiFi Security Setup**
WMM & QoS	**Wireless QoS mechanism**

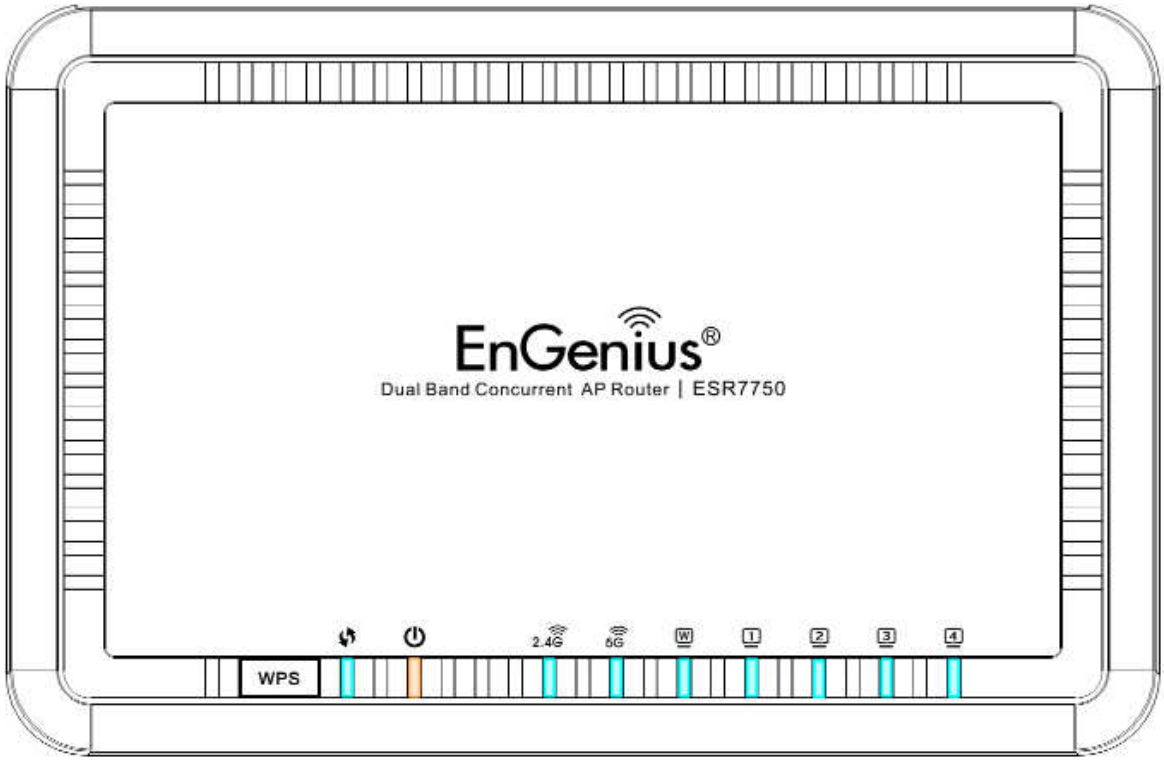
*** Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

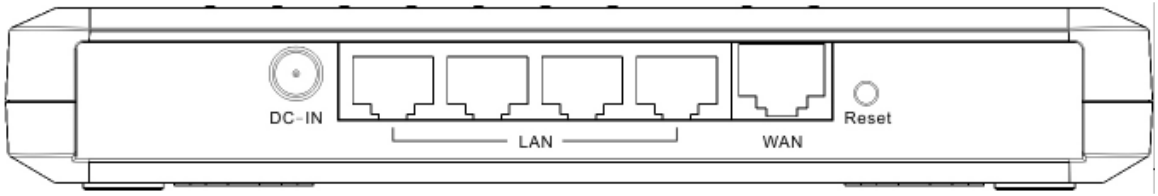
1.3. Package Contents

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 * Dual Band Concurrent AP Router (ESR7750)
- 1 * 12V/1.25 A Power Adapter
- 1 * CAT 5 UTP cable
- 1 * QIG
- 1 * CD (User Manual & Wizard)

1.4. Product Layout





Physical Interface	● WAN: 1 * 10/100 Fast Ethernet RJ-45 ● LAN: 4 * 10/100 Fast Ethernet RJ-45 ● Reset Button (5 second for reboot, 5~10 seconds for reset to factory default) ● Power Jack ● WPS push button (Wi-Fi Protected Setup)
LEDs Status	● Power/ Status ● Internet (WAN) ● LAN1~LAN4 (10/100Mbps) ● WLAN 2.4GHz ● WLAN 5GHz ● WPS

2. Installation

2.1. Network + System Requirements

To begin using the ESR7750, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System – Microsoft Windows 98SE/ME/XP/2000/VISTA
- 1 Free Ethernet port.
- WiFi card/USB dongle (802.11 a/b/g/n) – optional.
- External xDSL (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. ESR7750 Placement

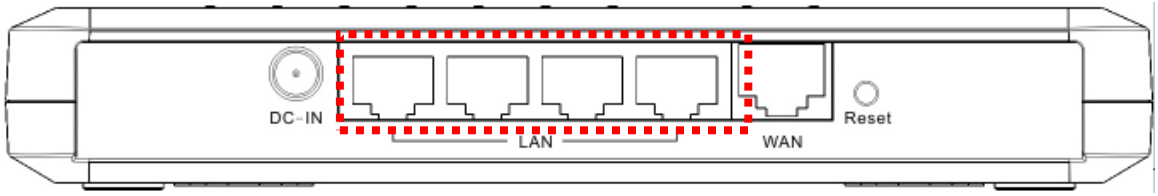
You can place ESR7750 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your device in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven.

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.

2.3. Setup LAN & WAN

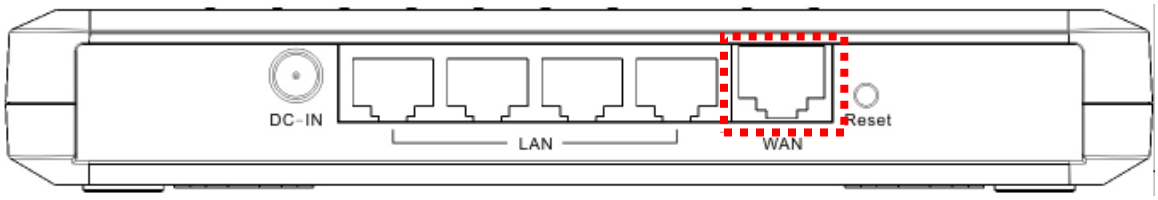
LAN connection:

Connect Ethernet cable between your PC/Notebook LAN port & one of the 4 available LAN ports on ESR7750.



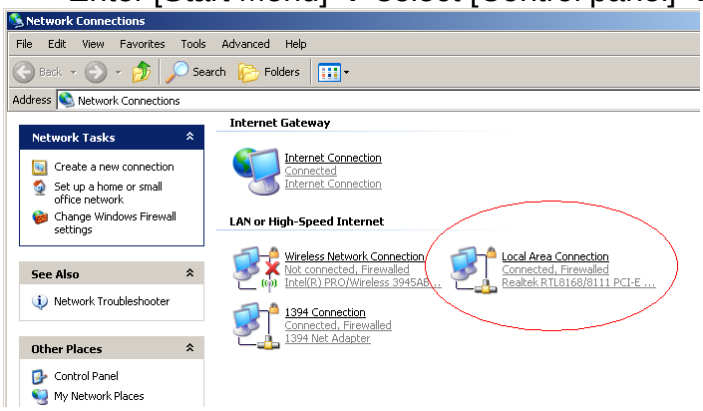
WAN connection:

Connect Ethernet cable between WAN ports of your ADSL/CABLE modem & INTERNET port of ESR7750. Make sure your ADSL/CABLE modem is working well. Contact your ISP if you have any questions.

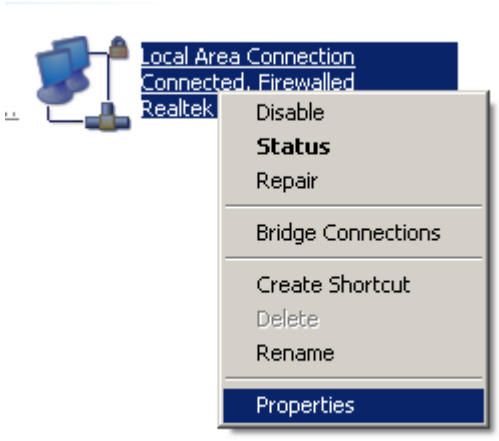


2.4. PC Network Adapter setup (Windows XP)

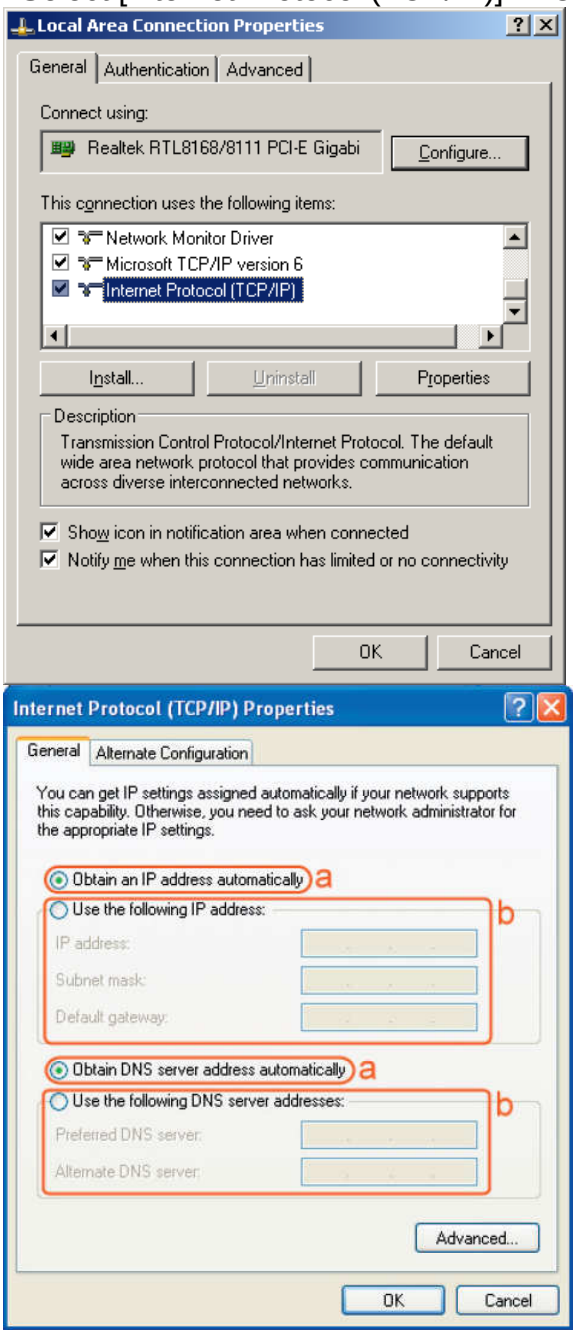
- Enter [Start Menu] → select [Control panel] → select [Network].



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



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



- Select the [General] tab.
- select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

2.5. Smart Wizard CD

Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. Then, the router 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.

Minimum Requirements

- A standard CD-ROM drive
- ADSL or cable modem should be ready for Internet connection.
- Modem must provide RJ45 port to connect with ESR7750.
- Microsoft Windows compatible PC/Notebook with UPnP enabled network adapter
- CAT 5 network cable(s), RJ45 port on PC/Notebook.

STEP 1

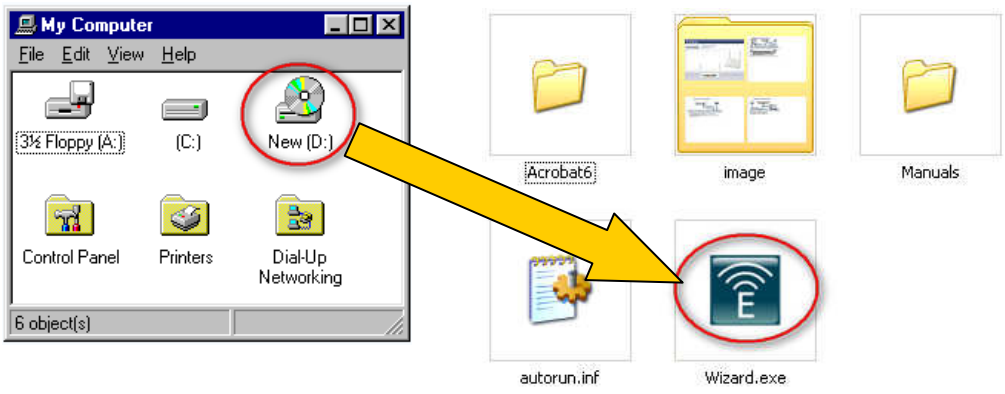
Power up the **device**.

Wait for POWER led on front panel lights up & remains stable.

STEP 2

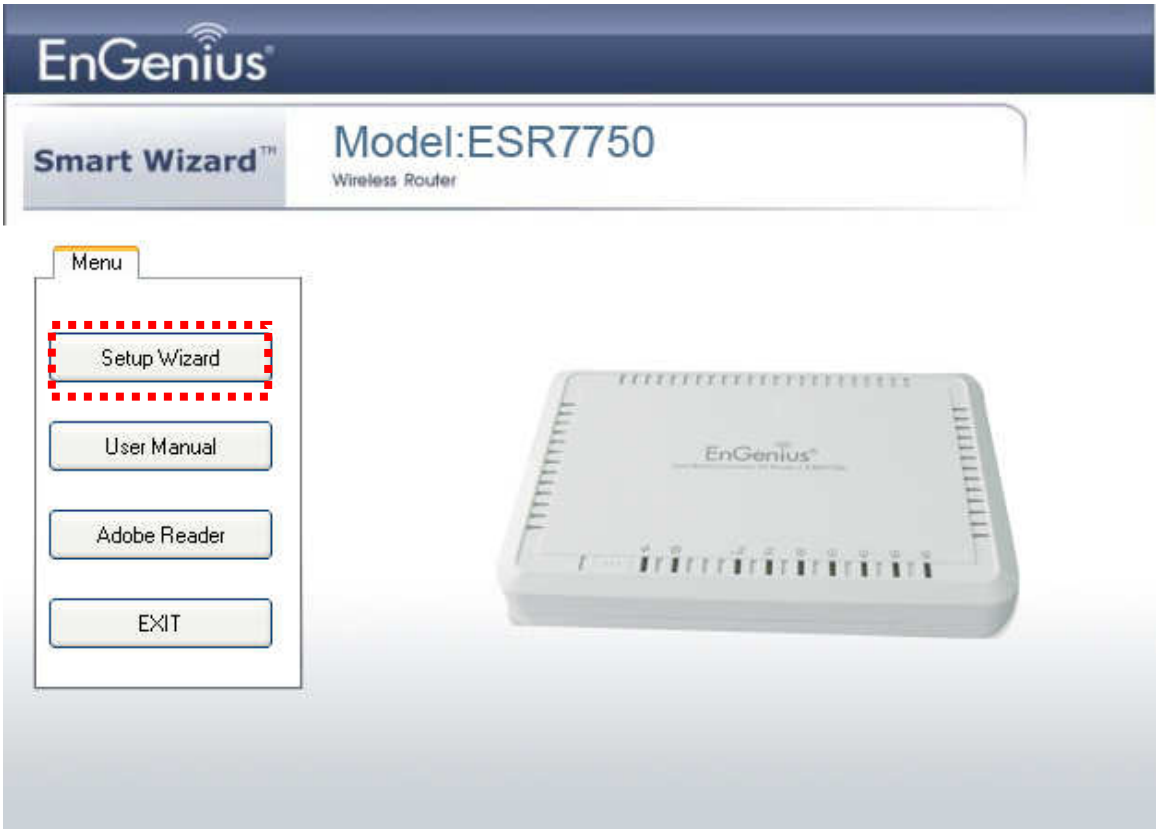
Insert **Wizard CD** into your CD-ROM drive and browse it with Windows Explorer.

Click on "**Wizard.exe**" to activate SMART WIZARD**.**

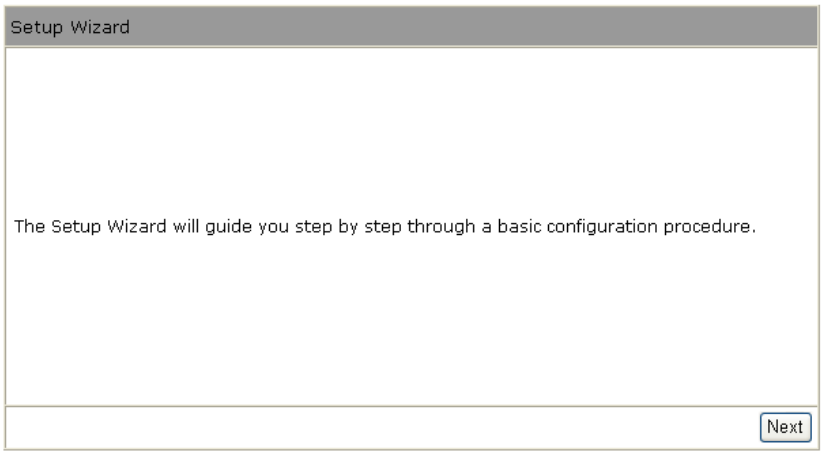


STEP 3

Click on [**Setup Wizard**] and follow the instruction given on the screen to complete the initial device configuration.

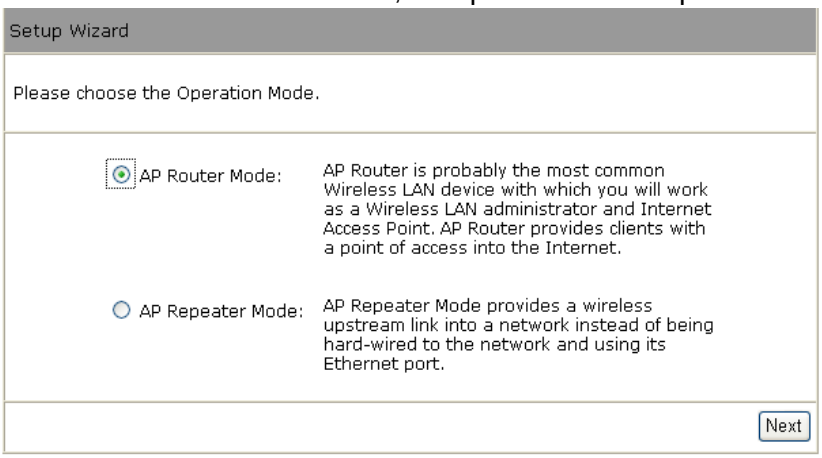

EnGenius
Smart Wizard™
Model:ESR7750
Wireless Router
Menu
Setup Wizard
User Manual
Adobe Reader
EXIT
EnGenius

2.6. Wizard Configuration



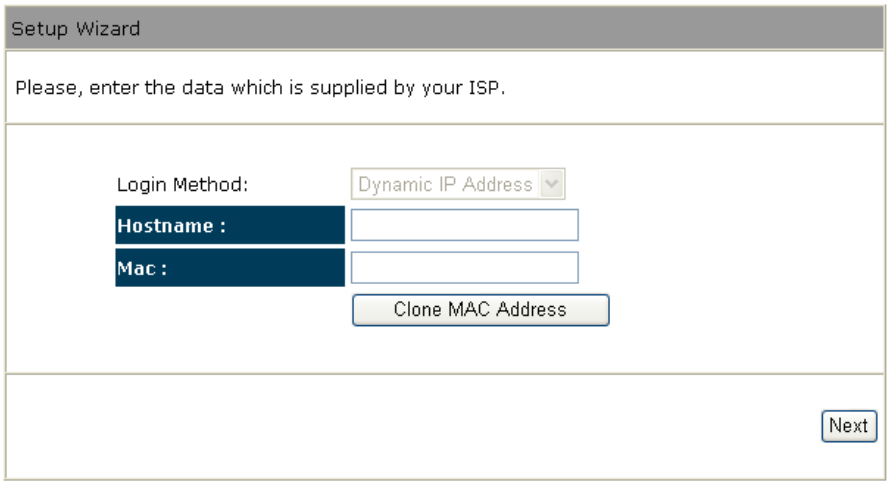
Click **<Next>** to enter mode selection.

Select the mode that ESR7750 is going to be and set its configurations. **AP Repeater mode** does not enable WAN interface, Setup Wizard will skip WAN Configuration.

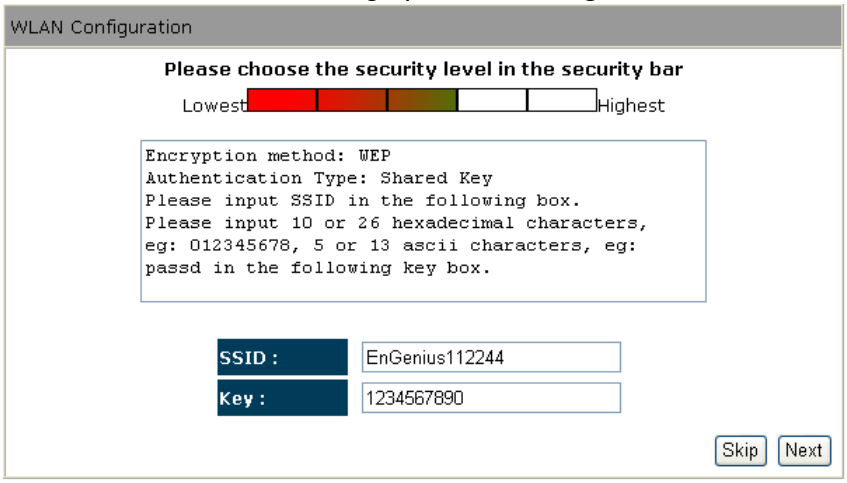


Click **<Next>** to automatically detect your **Internet Network** settings.

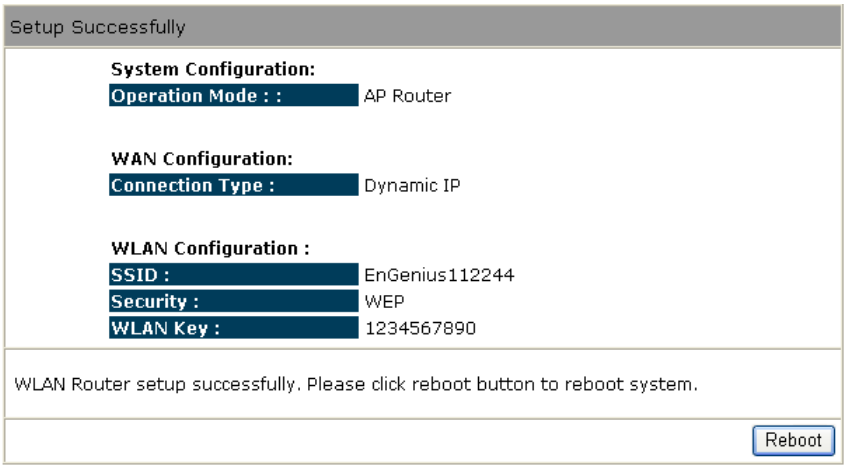
Smart Wizard has detected DHCP client. Configure the host name and MAC address of your ADSL modem. Click Next to proceed.



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>**.

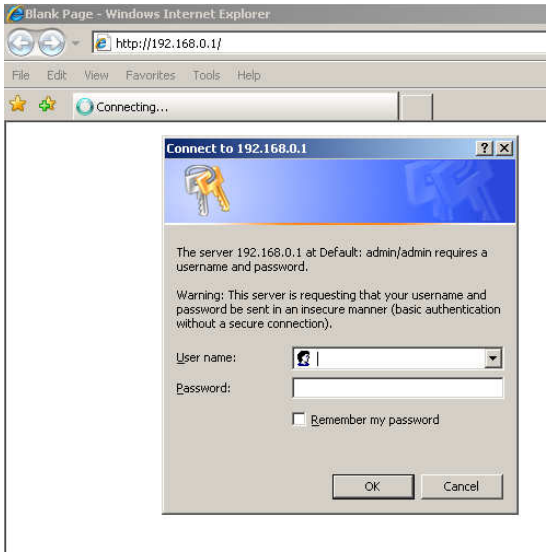
NOTE:

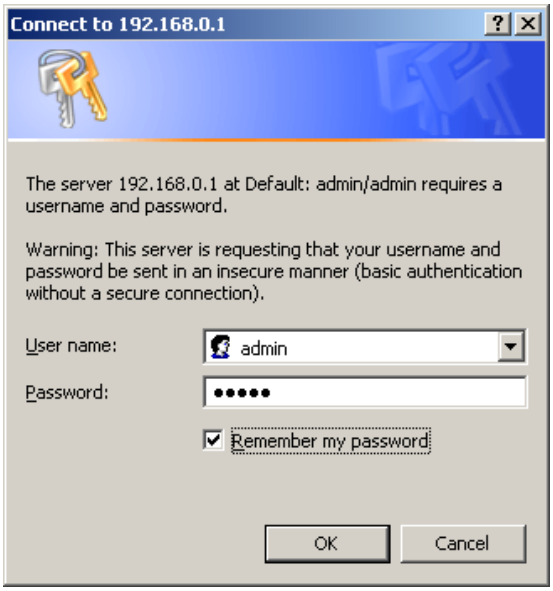
After Wireless settings are applied, you need to connect from your WLAN client with the security settings you just finished configuring. Remember the type of security & security key.

2.7. Initial Setup ESR7750

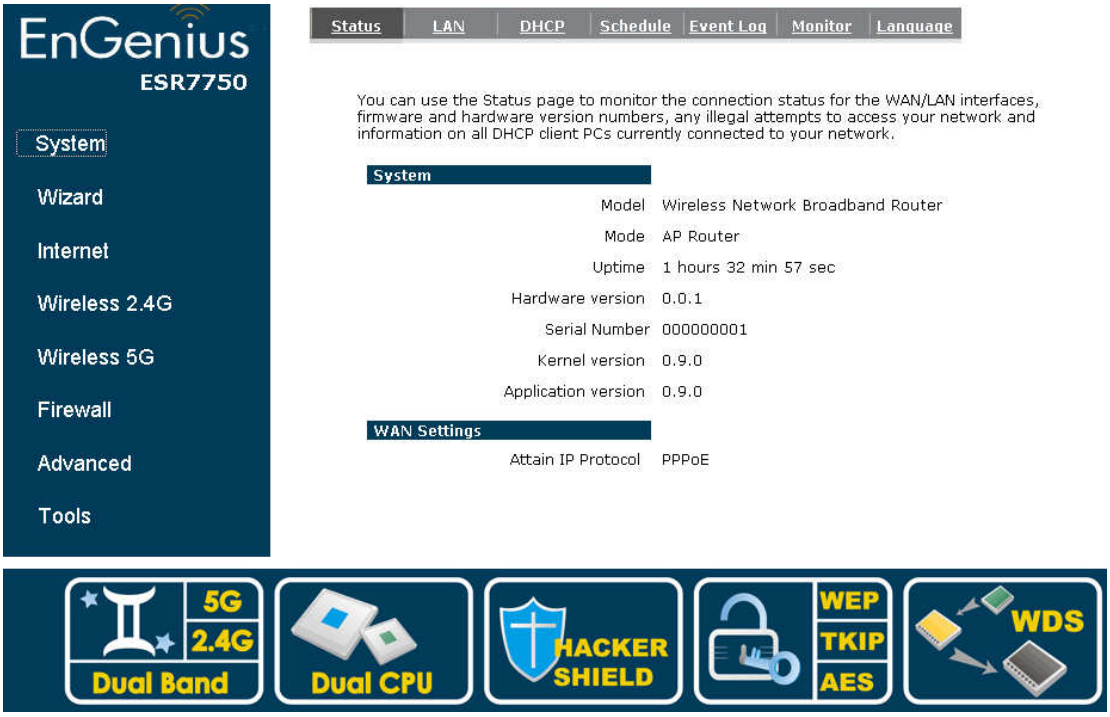
ESR7750 provides web-interface for configuration through web browser, such as Internet Explorer, Firefox or Safari.

1. Open your browser (e.g. Internet Explorer).
2. Type in http://192.168.0.1 in the address bar and press [Enter].





3. Click **<OK>** to navigate into ESR7750 configuration home page.
4. You will see the home page of ESR7750 as follows.


EnGenius
ESR7750
System
Wizard
Internet
Wireless 2.4G
Wireless 5G
Firewall
Advanced
Tools
Status
LAN
DHCP
Schedule
Event Log
Monitor
Language
You can use the Status page to monitor the connection status for the WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network and information on all DHCP client PCs currently connected to your network.
System
Model Wireless Network Broadband Router
Mode AP Router
Uptime 1 hours 32 min 57 sec
Hardware version 0.0.1
Serial Number 000000001
Kernel version 0.9.0
Application version 0.9.0
WAN Settings
Attain IP Protocol PPPoE
5G
2.4G
Dual Band
Dual CPU
HACKER
SHIELD
WEP
TKIP
AES
WDS

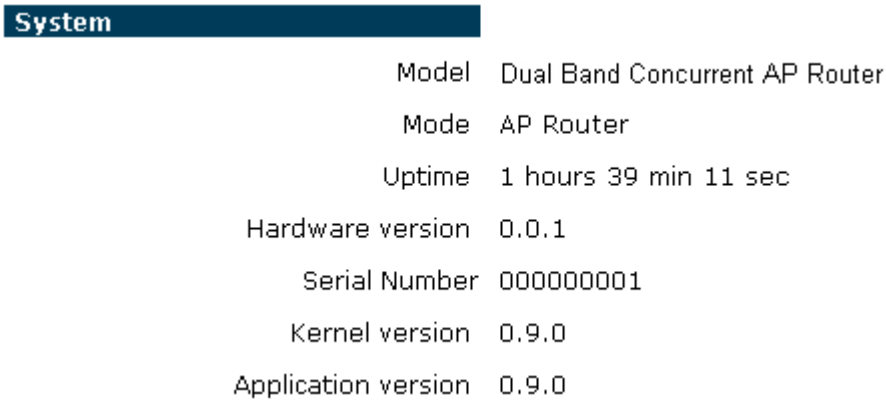
3. SYSTEM

3.1. Status

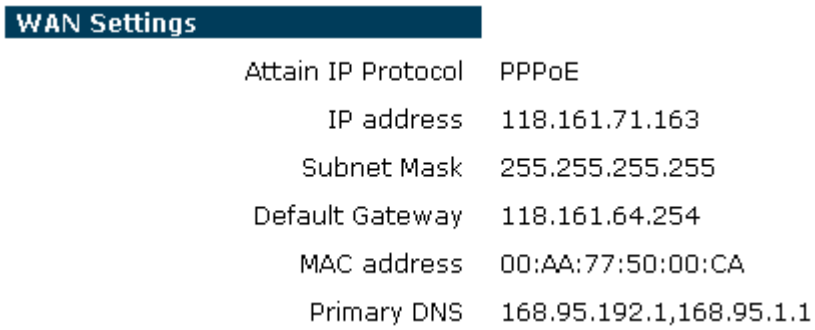
This page allows you to monitor the current status of your router. You can use the status page to quickly see if you have any updated firmware available (bug fixes, updates). You can navigate from this page with a few interesting options for reminding or skipping this page forever & so forth.

Once you click on **<OK>** button to go to the requested page, you can see the status page of the ESR7750.

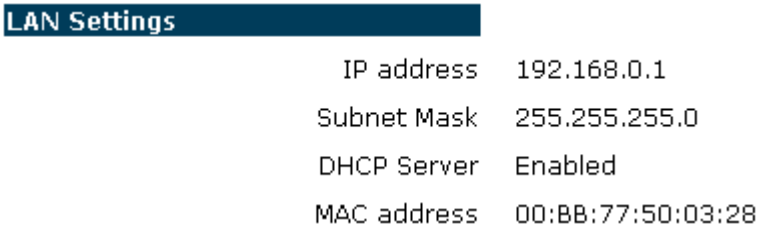
System: You can see the UP time, hardware information, serial number as well as firmware version information.



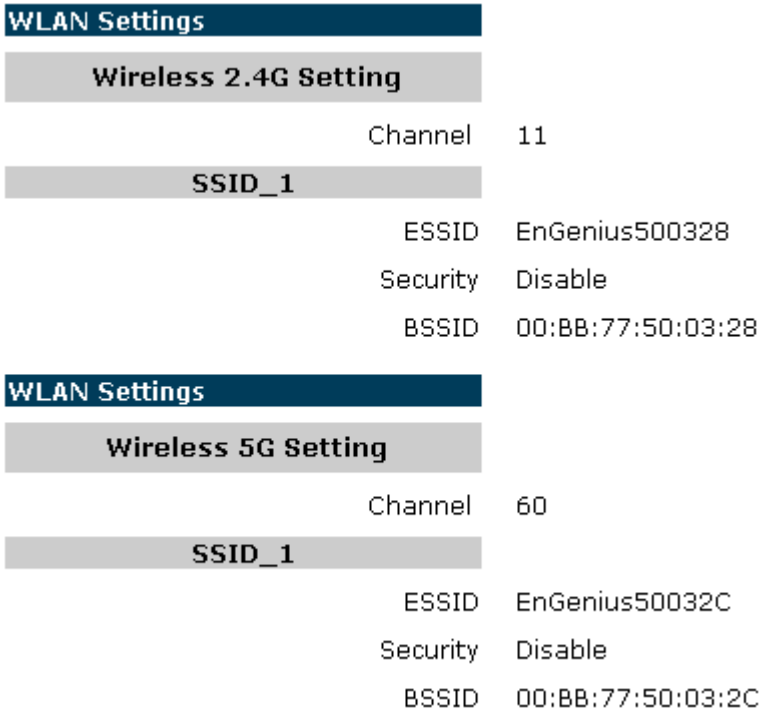
WAN Settings: This section displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **<Renew>** button to renew your WAN IP address.



LAN Settings: This section displays the Broadband router LAN port's current LAN & WLAN information. It also shows whether the DHCP Server function is enabled / disabled.



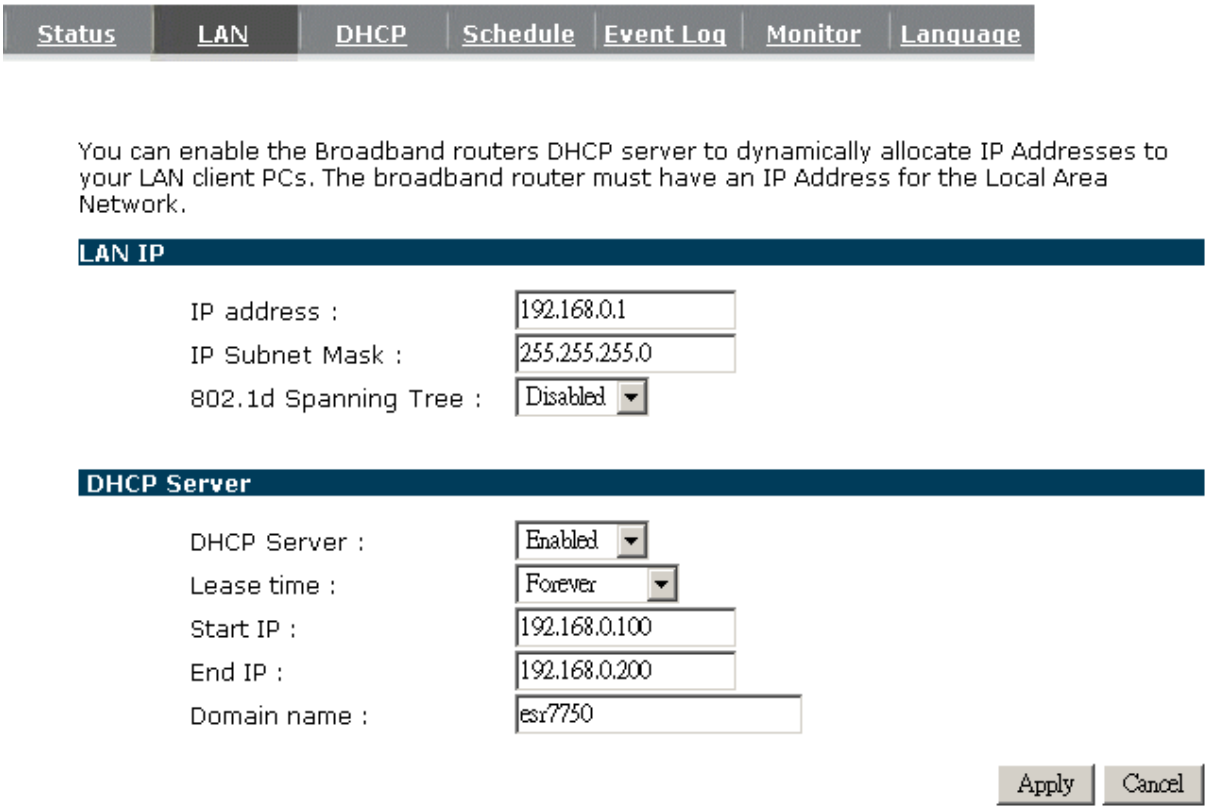
WLAN Settings: This section displays the current WLAN configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section. Wireless configuration details such as SSID, Security settings, BSSID, Channel number, mode of operation are briefly shown.



3.2. 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 router's LAN IP address (Your LAN clients default gateway IP address). 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 will enable or disable the Dynamic Pool setting..

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

Start IP: This will be the beginning of the pool of IP addresses available for client devices.

End IP: This will be the end of the pool of IP addresses available for client devices.

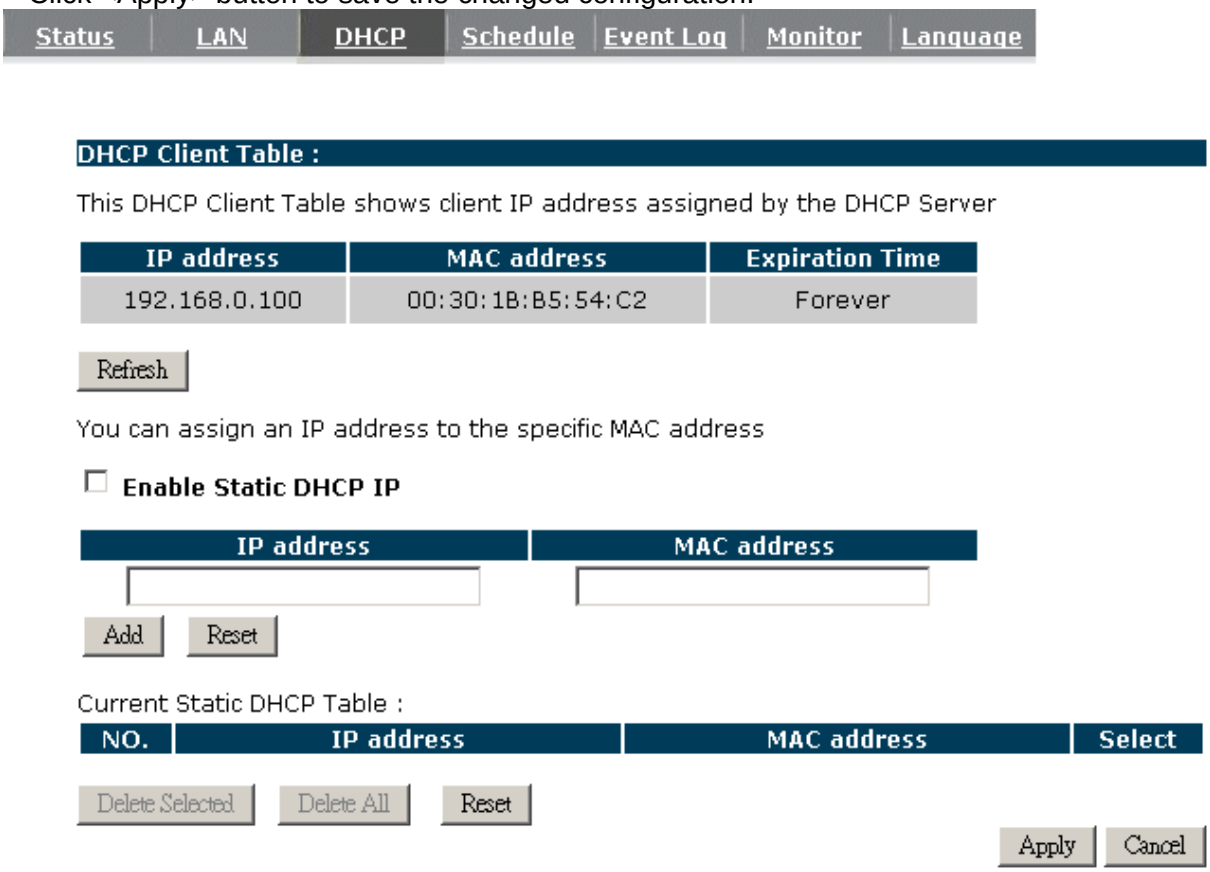
Domain name: The Domain Name for the existing or customized network.

3.3. 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.

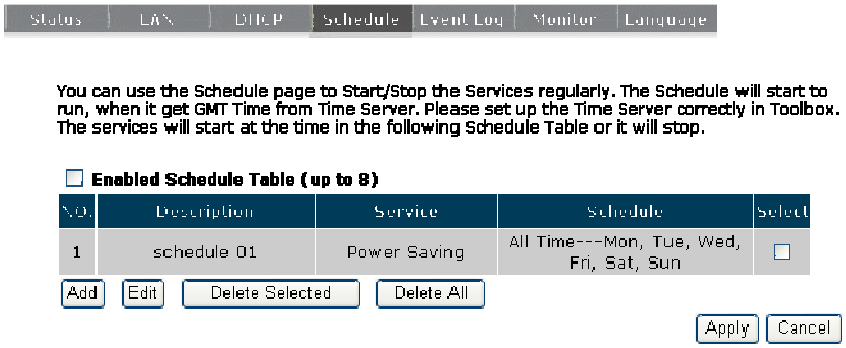
You can check “Enable Static DHCP IP“. It is possible to add more static DHCP IPs. They are listed in the table “Current Static DHCP Table“. IP address can be deleted at will from the table.

Click <Apply> button to save the changed configuration.

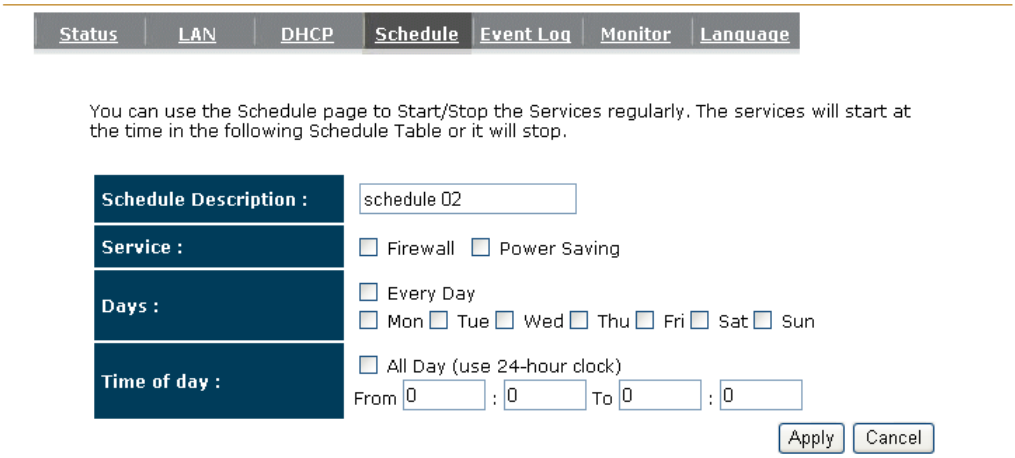


3.4. Schedule

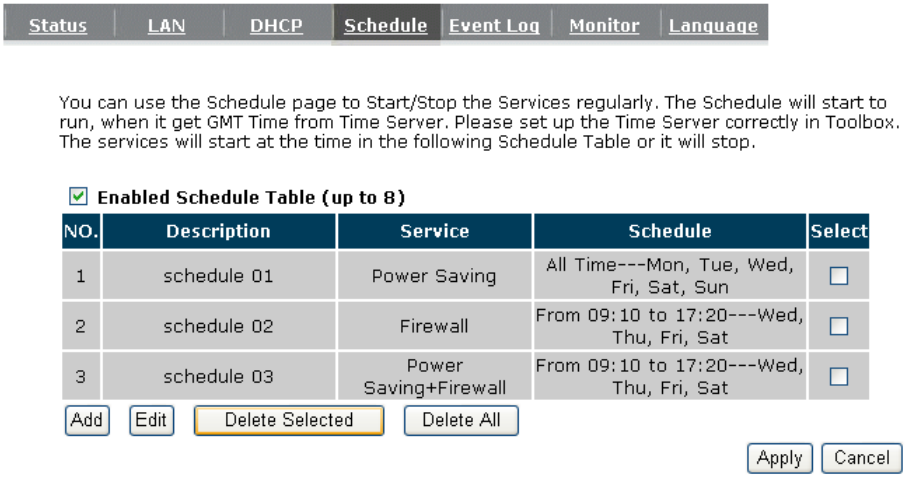
This page allows user to set up schedule function for Firewall and Power Saving.



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

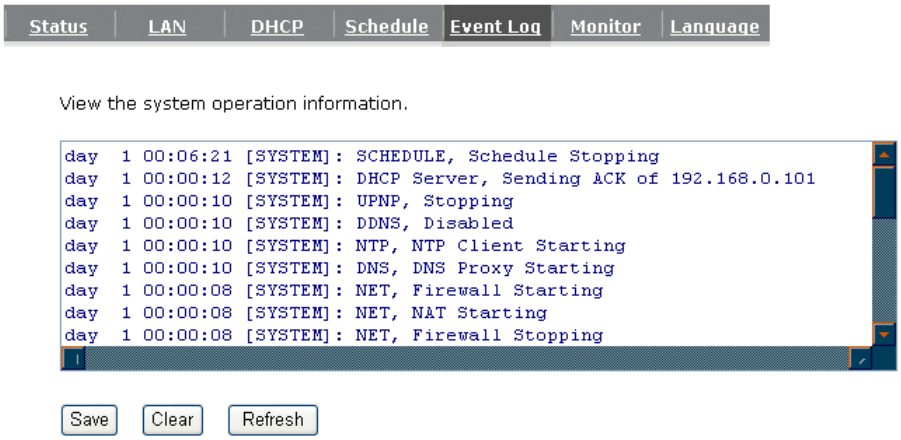


The schedule table lists the pre-schedule service-runs. You can select any of them using the check box.



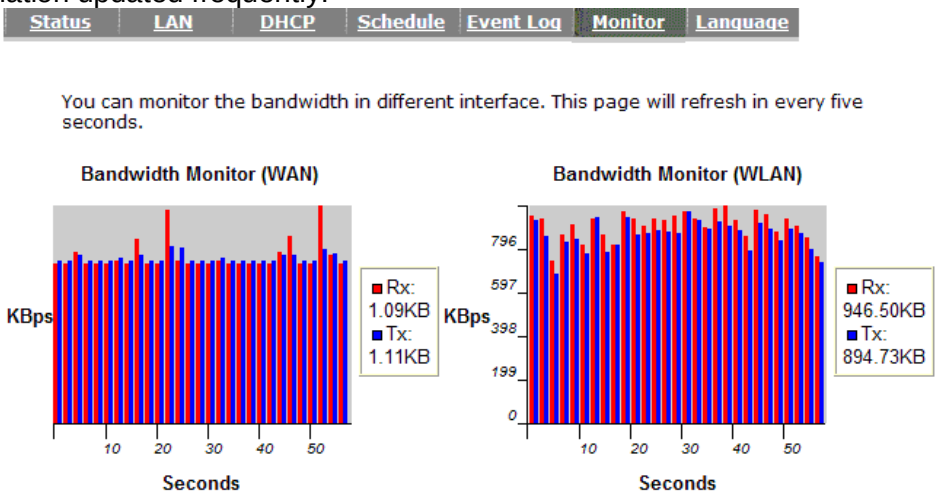
3.5. Event Log

View **operation event log**. This page shows the current system log of the Broadband 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.



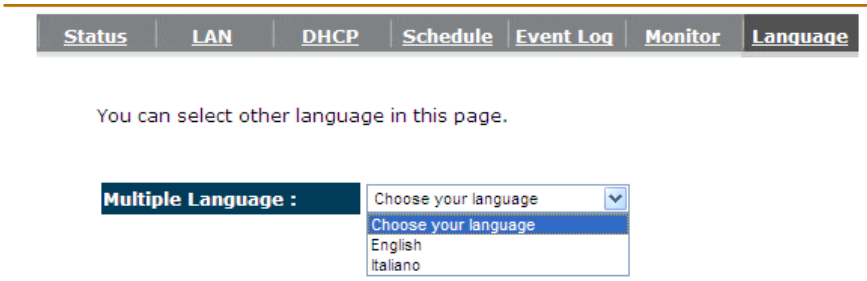
3.6. Monitor

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



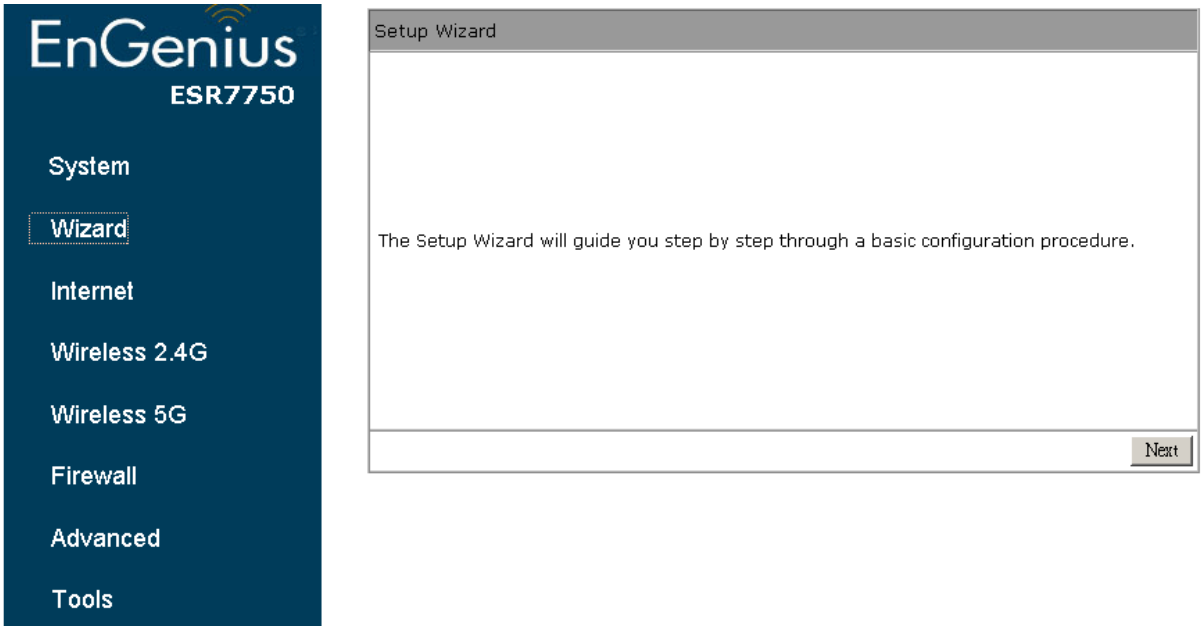
3.7. Language

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



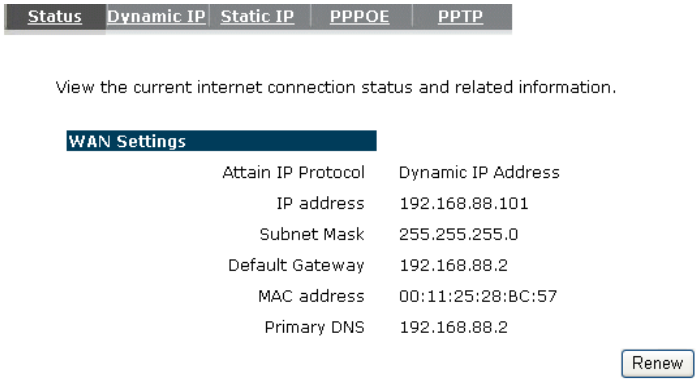
4. Wizard

Please refer to Chapter 2.6 for Wizard Configuration details



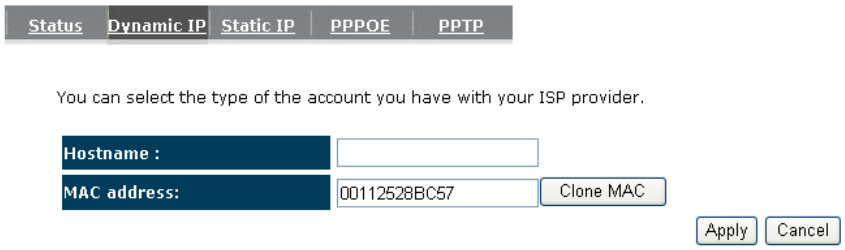
5. INTERNET
5.1. Status

This page shows the current Internet connection type and status



5.2. Dynamic IP

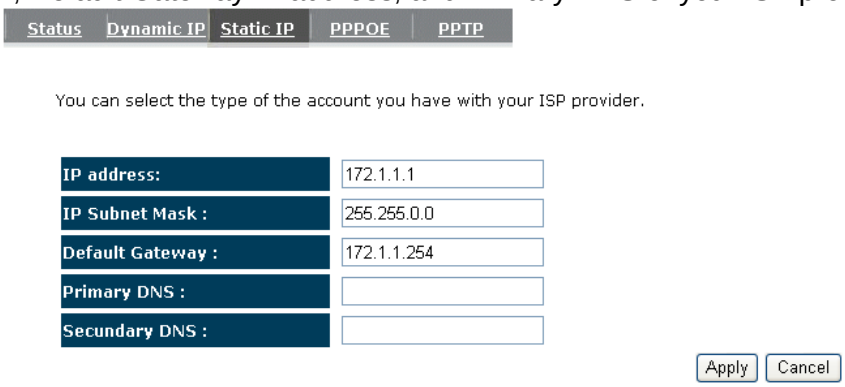
Use the MAC address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of the Ethernet card as an identifier, connect only the PC with the registered MAC address to the broadband router and click the **<Clone MAC Address>** button.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



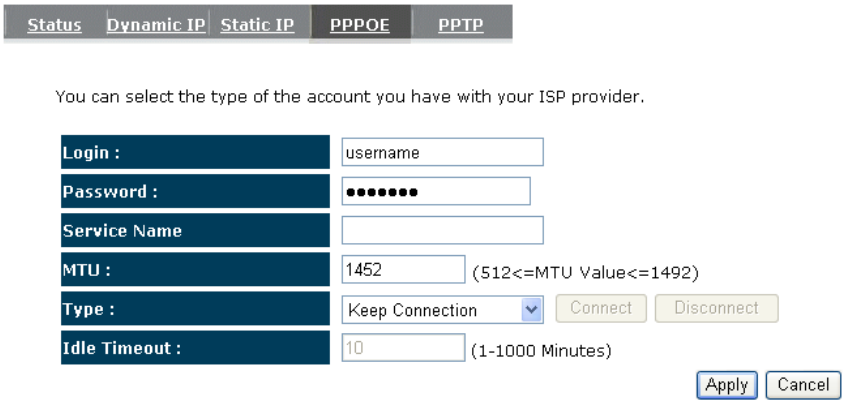
Host Name: This is optional.
MAC address: The default value is set to the WAN's physical interface of the broadband router.

5.3. 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 of your ISP provider.



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



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

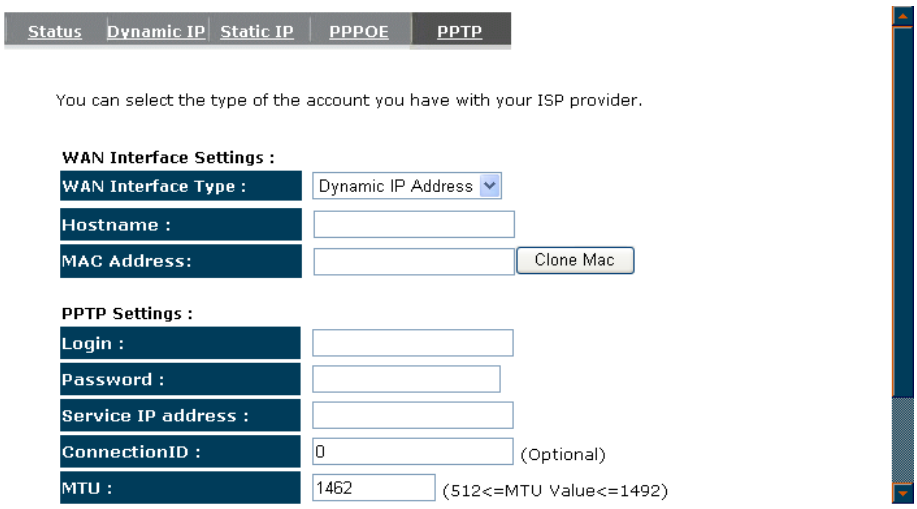
Service Name: This is normally optional.

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

Type: Enable the Auto-reconnect option to automatically re-establish the connection when an application attempts to access the Internet again.

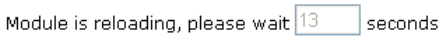
Idle Timeout: This is a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped.

5.5. 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.

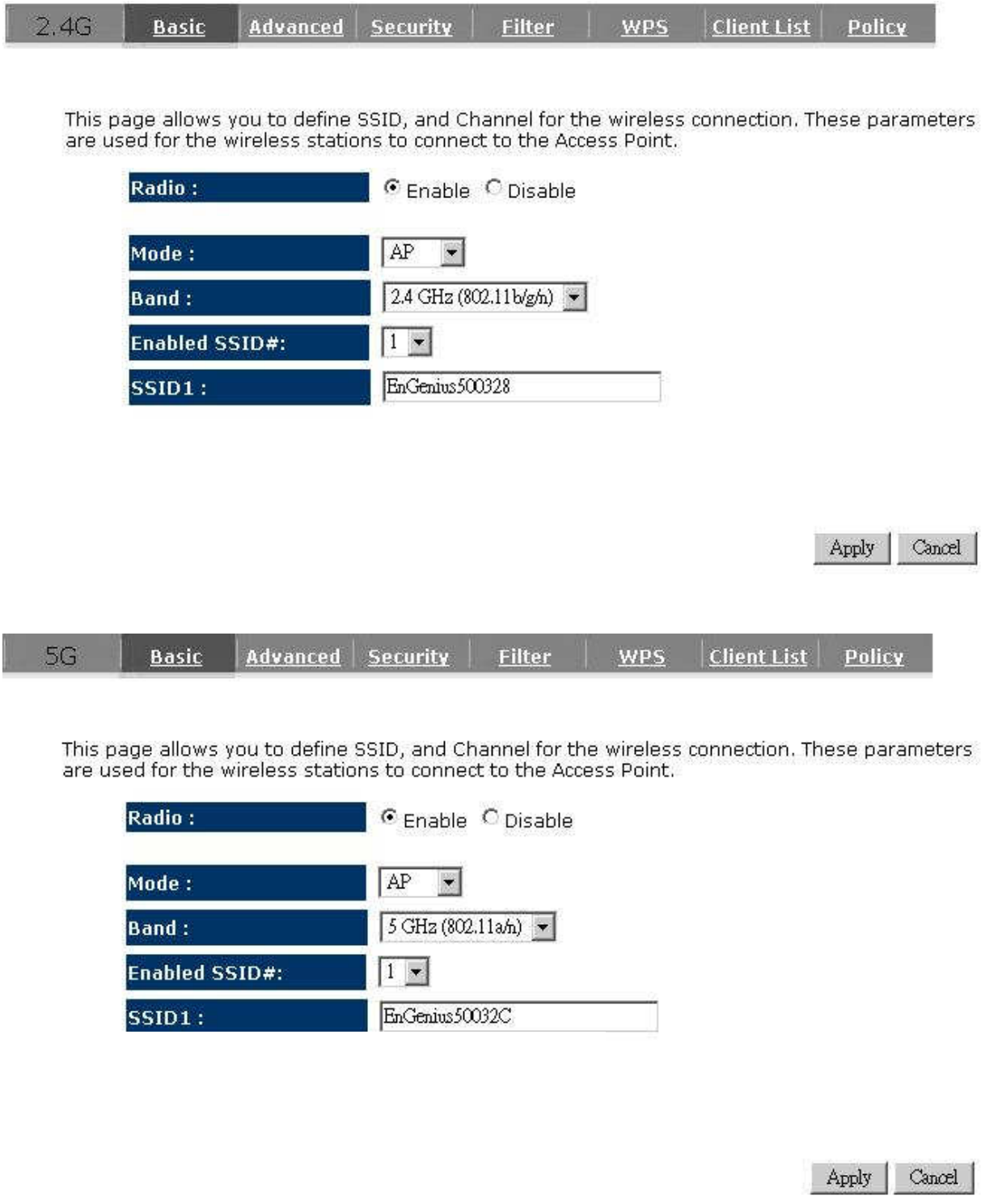
Click **<Apply>** to save configuration and connect to ISP provider.



6. WIRELESS 2.4G & 5G

ESR7750 is a dual band concurrent product, therefore two wireless radio configurations are provided. Both radios share the same features except for open band and available channels under “Basic” section.

6.1. Basic



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**, **AP route with WDS** (we will introduce this function later section), and **repeater**. 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.

- **Band 2.4G:**

  2.4 GHz(B): If all of your clients are 802.11b, select this one.
  2.4 GHz(G): If all of your clients are 802.11g, select this one.
  2.4 GHz(B/G): Either an 802.11b or an 802.11g wireless devices are in your environment.
  2.4 GHz(N): If all of your clients are 802.11n, select this one.
  2.4 GHz(B/G/N): Either 802.11b, 802.11g, or 802.11n wireless devices are in your environment.

- **Band 5G**

5 GHz (A): If all of your clients are 802.11a, select this one.
5 GHz (N): If all of your clients are 802.11n, select this one.
5 GHz (A/N): Either 802.11a or 802.11n wireless devices are in your environment.

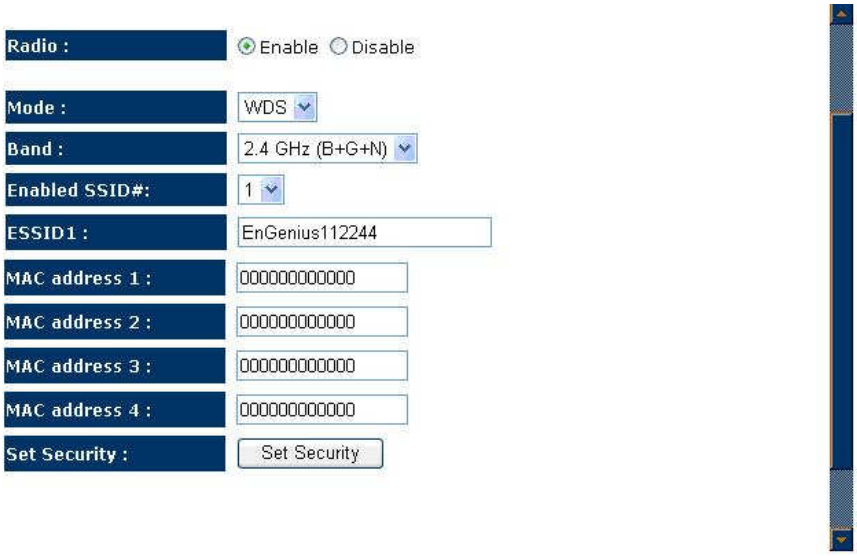
Enable ESSID: We support 4 multiple SSIDs in this device. Please select how many SSIDs you would like to use in your network environment.

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.

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.

6.2. Mode: WDS

Wireless Distribution System, a system that enables the wireless interconnection of access point, allows a wireless network to be expended using multiple access points without a wired backbone to like them. Each WDS APs need setting as same channel and encryption type.

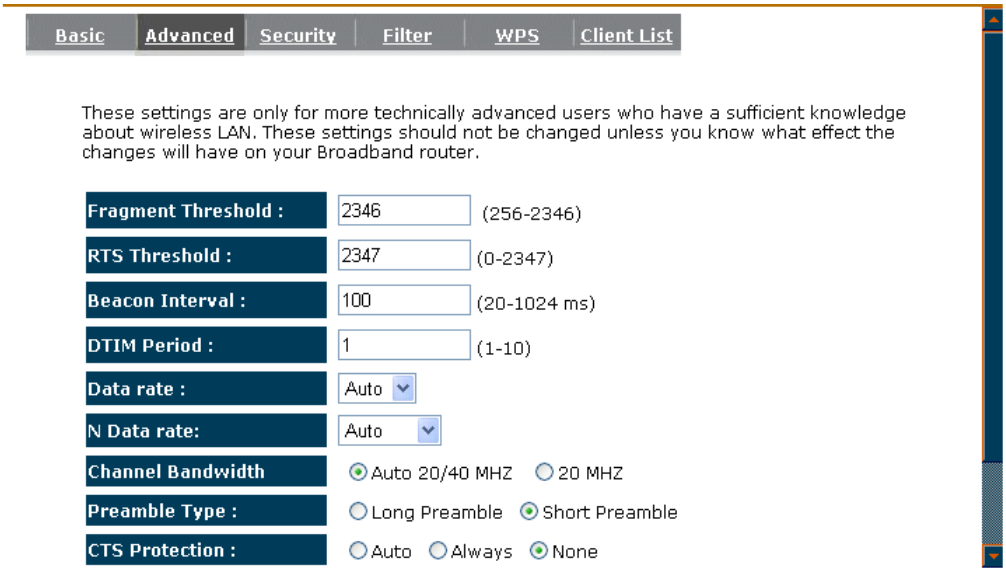


MAC address 1~4: Please enter the MAC address of the neighboring APs that participates in WDS, we support 4 devices now.

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.

6.3. Advanced

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. 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: 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 "Data Rate" 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 "Data Rate" 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.

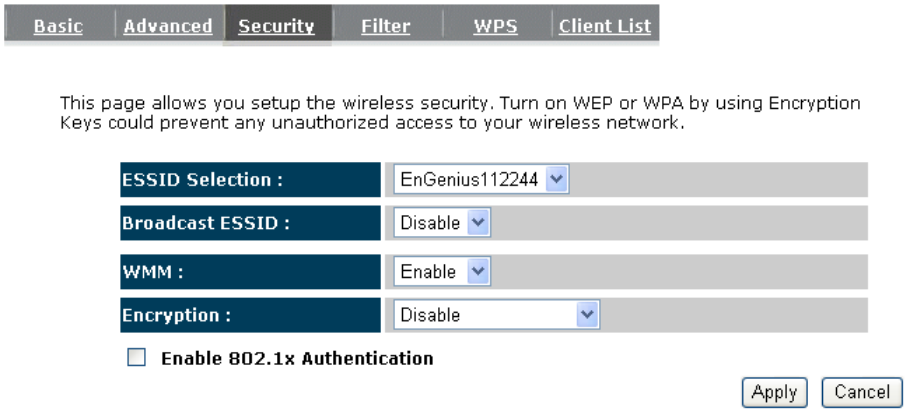
Channel Bandwidth: This is the range of frequencies that will be used.

Preamble Type: The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" 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.

6.4. 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 broadband router support multiple ESSID, you could select and set up the wanted ESSID.

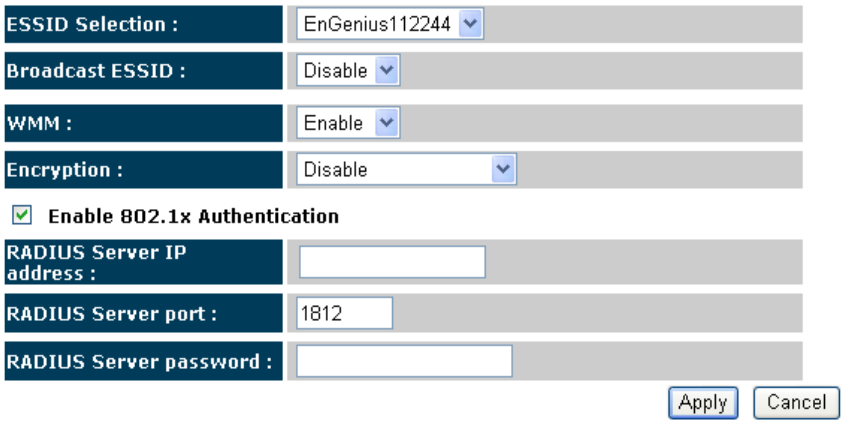
Broadcast ESSID: If you enabled “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.

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 ESR7750.

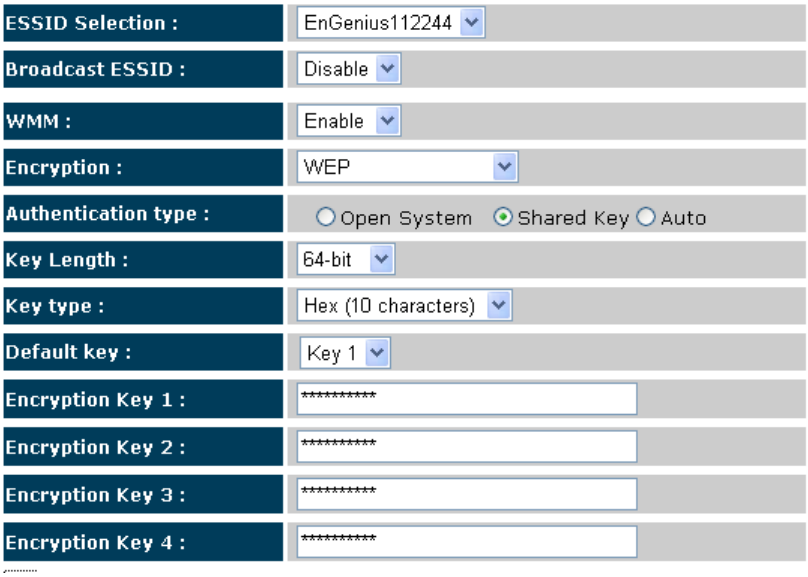
Enable 802.1x Authentication

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 the router can receive any packets encrypted by one of the four keys.



Authentication Type: There are two authentication types: **"Open System"** and **"Shared Key"**. When you select **"Open System"**, wireless stations can associate with this wireless router without WEP encryption. When you select **"Shared Key"**, you should also setup a WEP key in the **"Encryption"** page. After this has been done, make sure the wireless clients that you want to connect to the device are also setup with the same encryption key.

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.

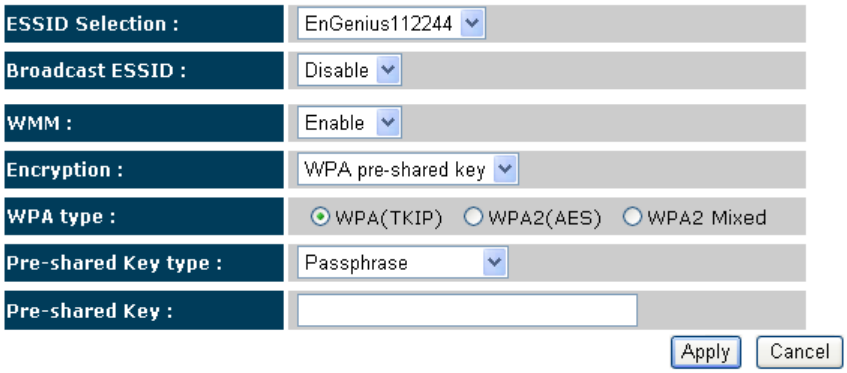
Key1 - Key4: The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys.
128-bit WEP: input 26-digit 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. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-Shared Key Encryption

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a

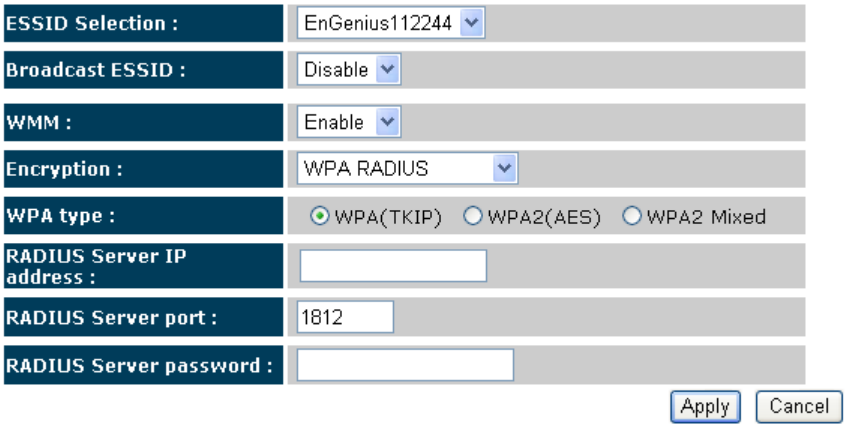
pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.



WPA-Radius Encryption

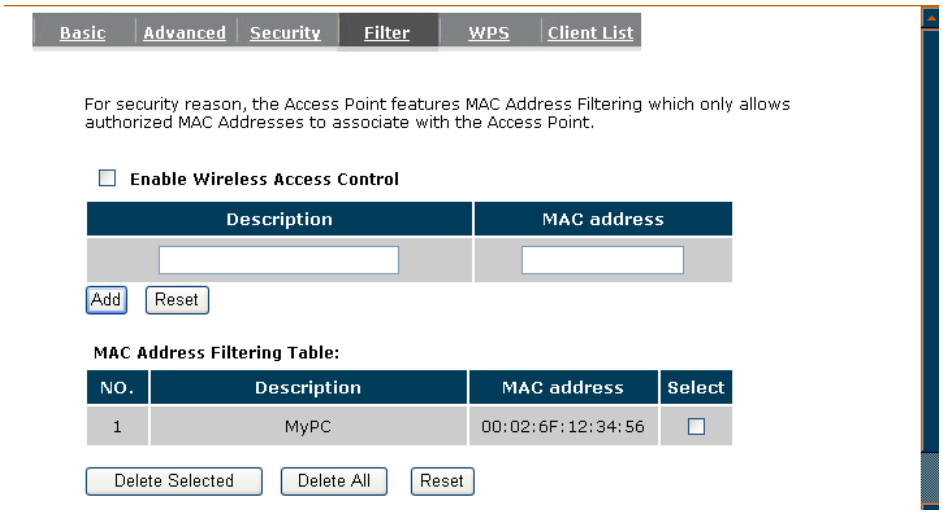
Wi-Fi Protected Access (**WPA**) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication.

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



6.5. Filter

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 "Comment" of the wireless station to be added and then click **<Add>**. The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

Remove an address from the list

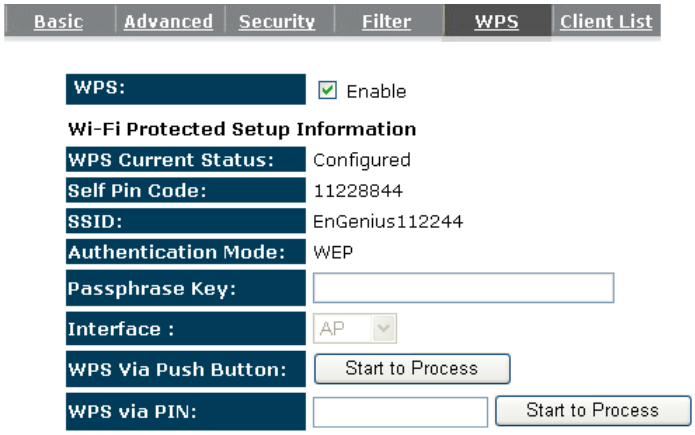
If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the **<Delete All>** button. Click **<Reset>** will clear your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

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

6.6. WPS (Wi-Fi Protected Setup)

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.

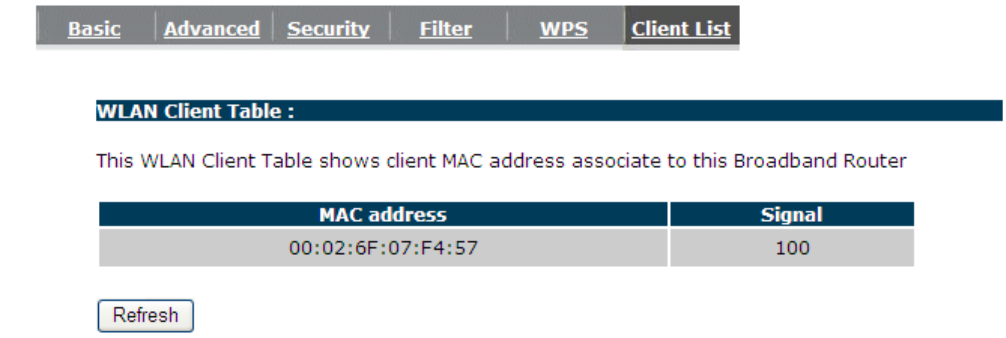
Interface: If device is set to repeater mode, you can choose **"Client"** interface to connect with other AP by using WPS, otherwise you may choose **"AP"** interface to do WPS with other clients.

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.

6.7. Client List

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



6.8. Policy

Policy provides a list of control policies. These settings define whether wireless or wired clients are able to “see” each in the LAN.

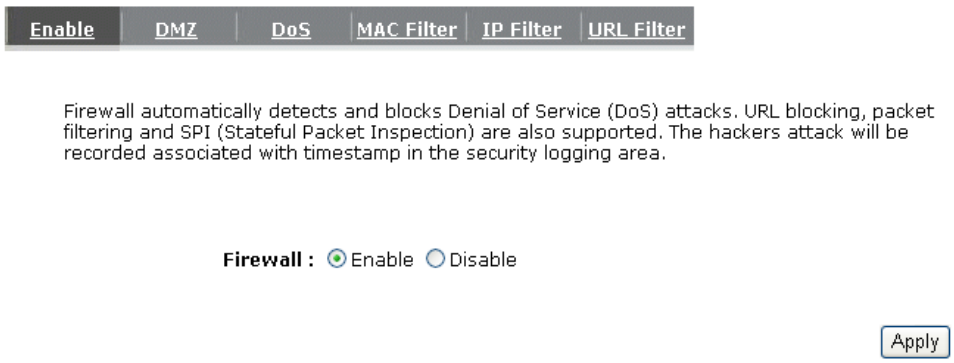
- If you are offering Internet access to your clients, please enable WAN connection.
- If you allow communication between Wireless clients please enable the second item.
- If you allow communication between Wireless client and Wired client please enable the last item.

- Disable WAN connection if you do not provide Internet access.
- Disable the items if you would like to enhance privacy between clients.

7. FIREWALL

7.1. Enable

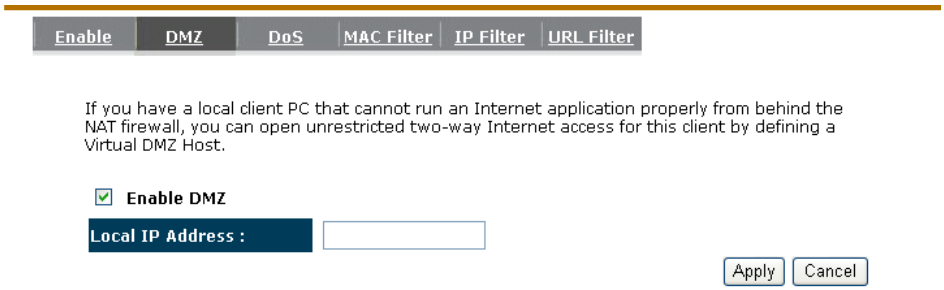
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific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



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

7.2. Demilitarized Zone (DMZ)

If you have a client PC that cannot run an Internet application (e.g. Games) properly from 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) going to your WAN IP address to a particular LAN client/server.



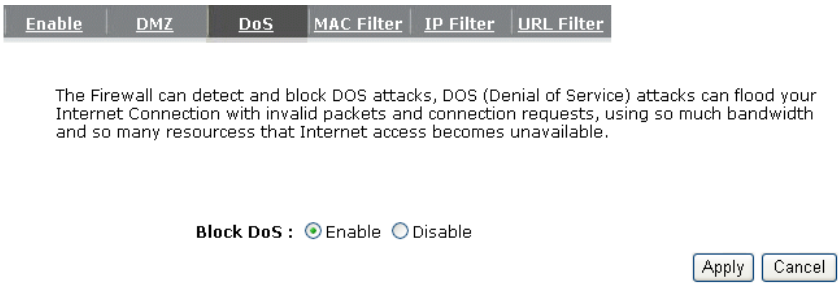
Enable DMZ: Enable/disable DMZ

LAN IP Address: Fill-in the IP address of a particular host in your LAN Network that will receive all the packets originally going to the WAN port/Public IP address above.

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

7.3. Denial of Service (DoS)

The Broadband 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.

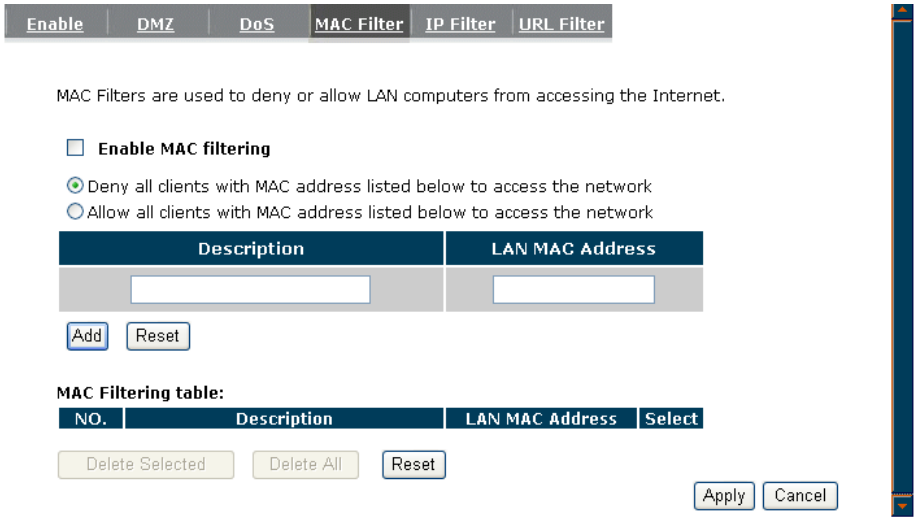
Discard Ping From WAN: The router's WAN port will not respond to any Ping requests

Port Scan: Protects the router from Port Scans.

Sync Flood: Protects the router from Sync Flood attack.

7.4. - 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. Access Control 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 "**Deny**" then all clients will be allowed to access Internet accept for the clients in the list below.

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

Add PC MAC Address

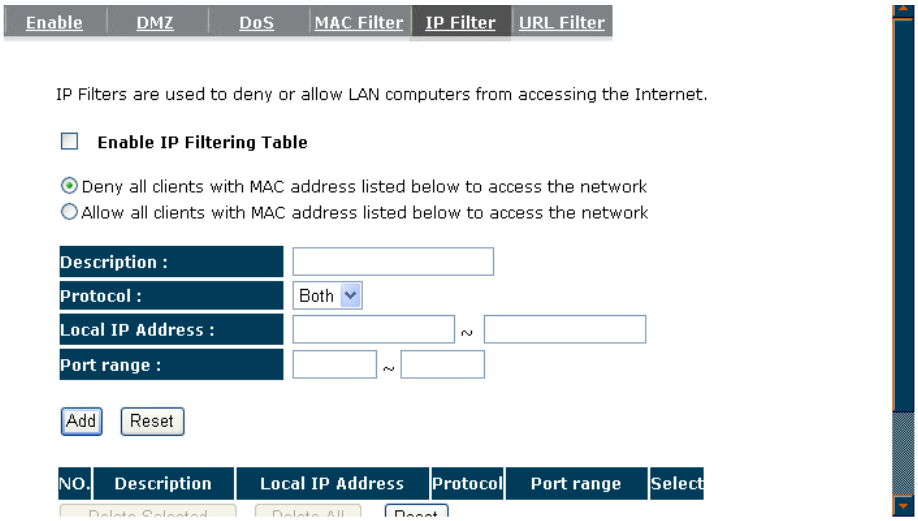
Fill in “**LAN MAC Address**” and **<Description>** of the PC that is allowed to access the Internet, and then click **<Add>**. If you find any typo before adding it and want to retype again, just click **<Reset>** and the fields will be cleared.

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.

7.5. IP Filter



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

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

Allow: If you select "**Allow**" then all clients will be denied to access Internet accept 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.

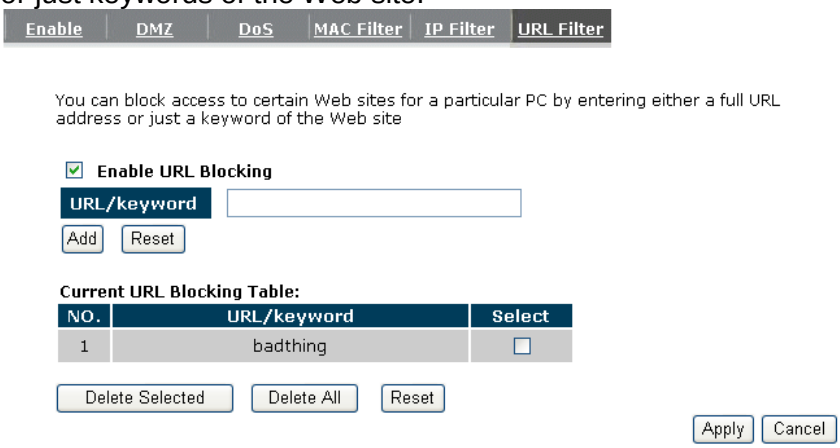
Remove PC IP Address

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.

7.6. 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 “URL/Keyword” 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>**.

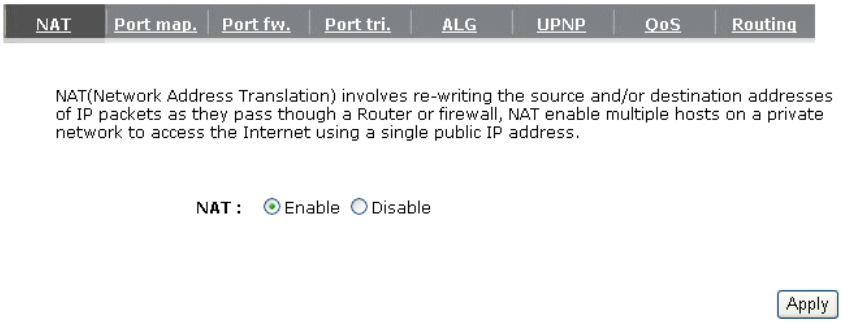
If you want remove all URL keywords from the table, click **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset**>.

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

8. Advanced

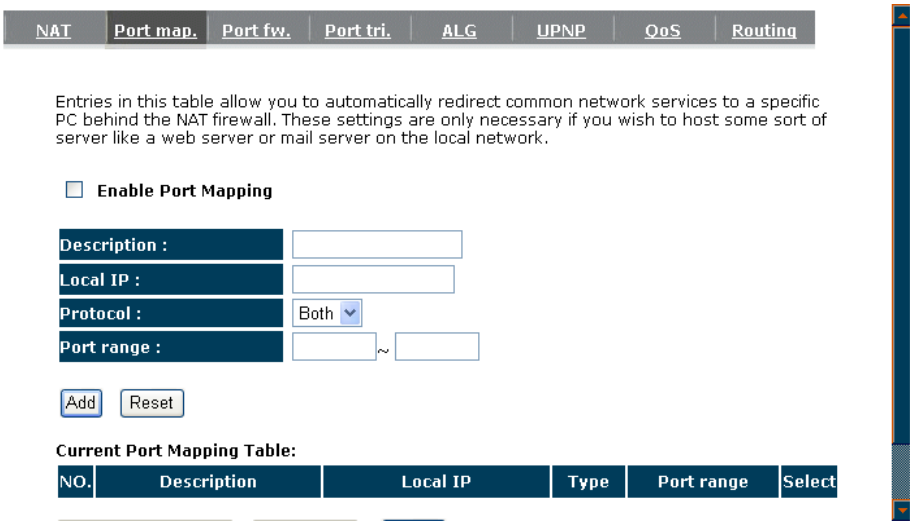
8.1. Network Address Translation (NAT)

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.



8.2. - 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.

Type: This is the protocol type to be forwarded. You can choose to forward "**TCP**" or "**UDP**" packets only, or select "**BOTH**" to forward both "**TCP**" and "**UDP**" packets.

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

Add Port Mapping

Fill in the "**Local IP**", "**Type**", "**Port Range**" 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 **<Clear>** and the fields will be cleared.

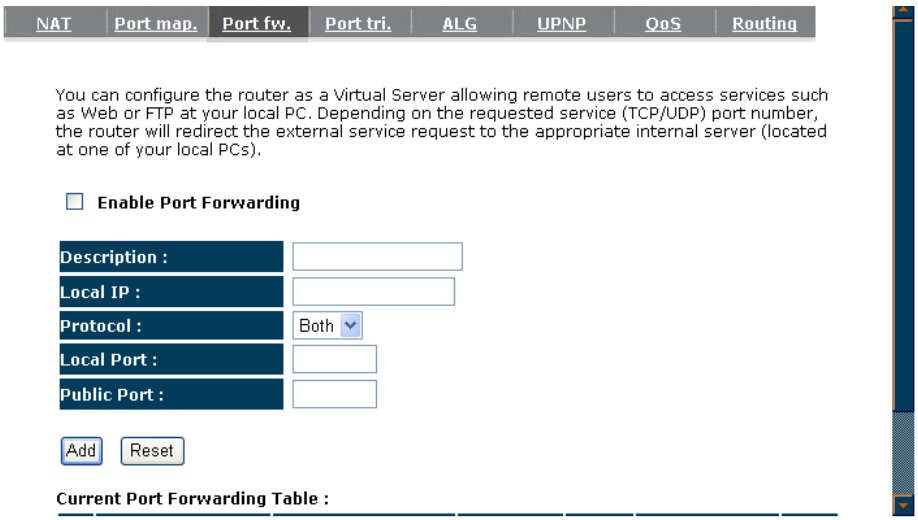
Remove Port Mapping

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.

8.3. 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 and its service port number. (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.

Type: 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**", "**Type**" 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 **<Clear>** and the fields will be cleared.

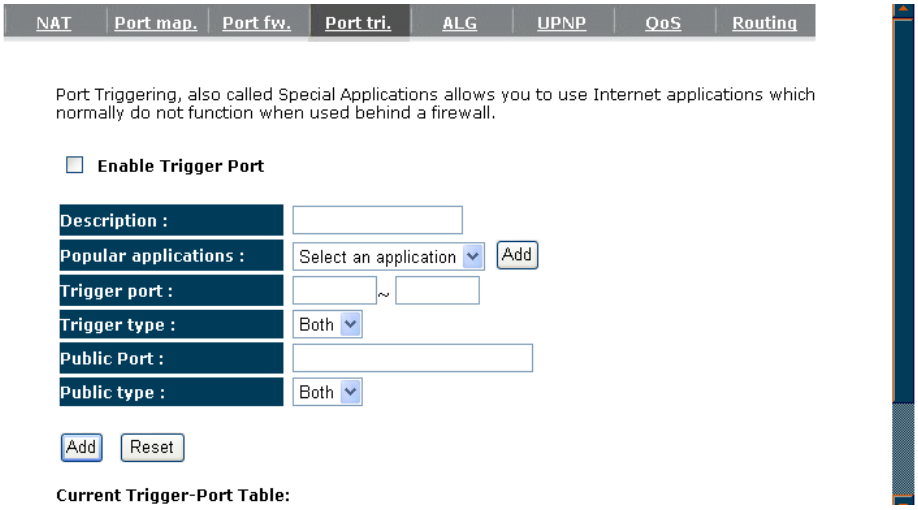
Remove Port Forwarding

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.

8.4. 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 "**TCP**", "**UDP**" or "**BOTH**".

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: "**TCP**", "**UDP**" or "**BOTH**"

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 (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

Add Port Triggering

Fill in the "**Trigger Port**", "**Trigger Type**", "**Public Port**", "**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 **<Clear>** and the fields will be cleared.

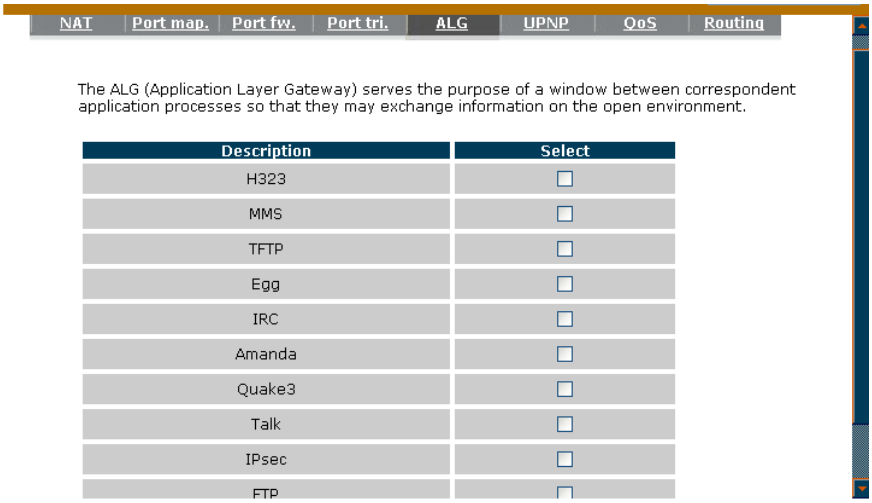
Remove Port Triggering

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.

8.5. Application Layer Gateway (ALG)

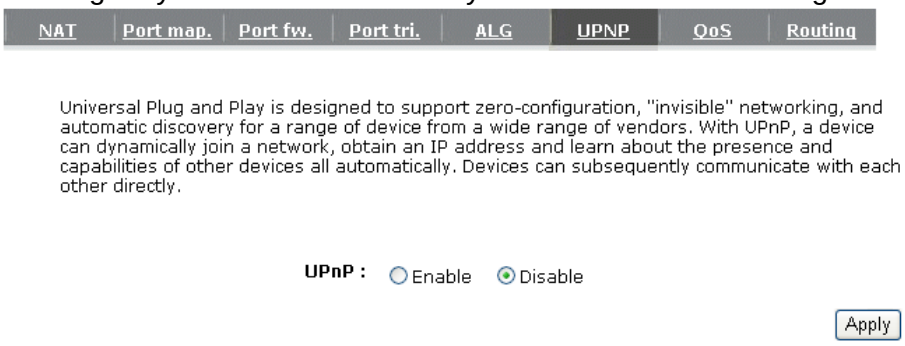
You can select applications that need **ALG** support. The router will let the selected

application to correctly pass through the NAT gateway.



8.6. 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.

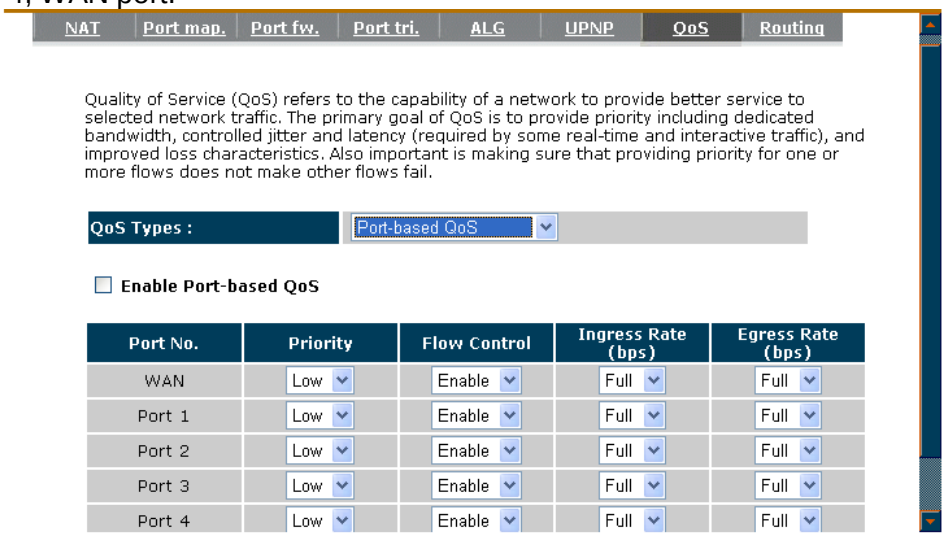
8.7. Quality of Service (QoS)

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 …etc. All the applications not specified by you are classified as rule

“Others”. The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

Port-based Qos

This is hardware port-based QoS control method. It will limit the packets throughput in LAN1~4, WAN port.



Enable Port-based QoS: Check this to enable port-based QoS functionality for the LAN/WAN port. You can also uncheck to disable.

Priority: High or Low priority level of the transmit packets.

Ingress Rate: The throughput limit of receiving packets.

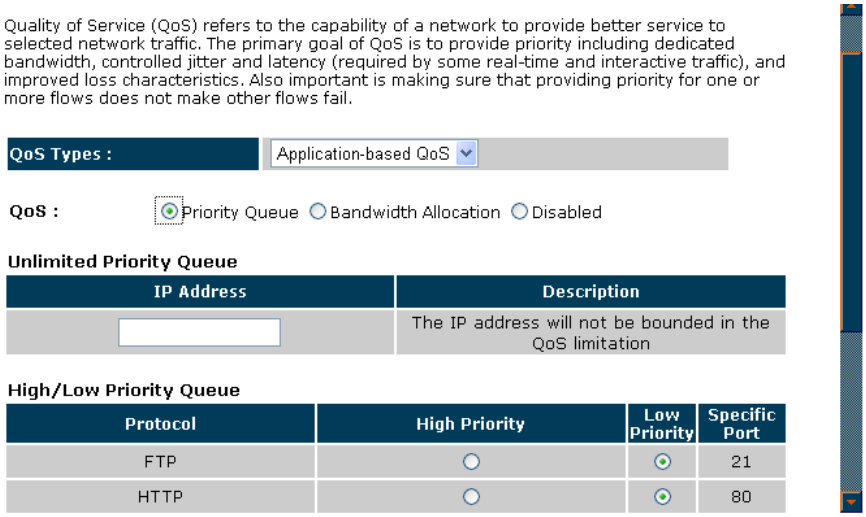
Egress Rate: The throughput limit of sending packets.

Application-based Qos

This is the application based QoS control method. You can reserve or limit the bandwidth of some LAN IP address and port number. They will guarantee the throughput in WAN connection.

Priority Queue Type:

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

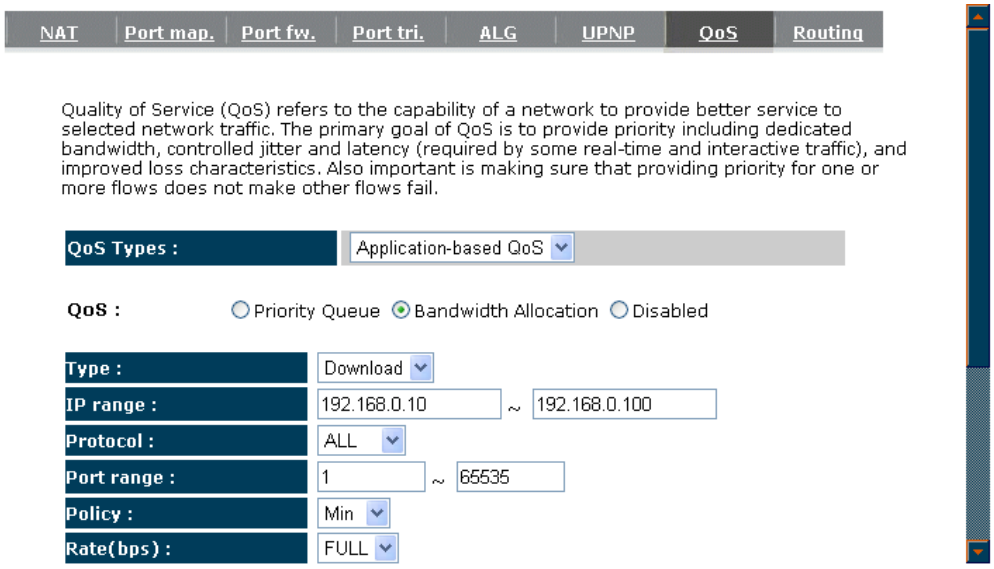


Unlimited Priority Queue: The LAN IP address will not be bounded in the QoS limitation.

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 or download.

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

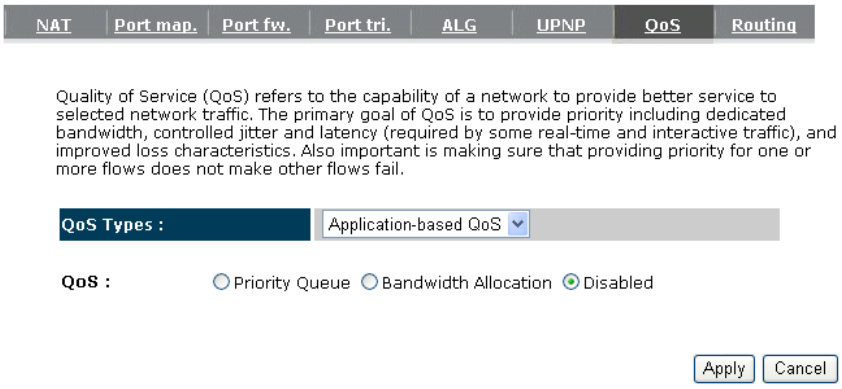
Protocol: Specify the packet type. The default ALL will put all packets in the QoS priority Queue.

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.

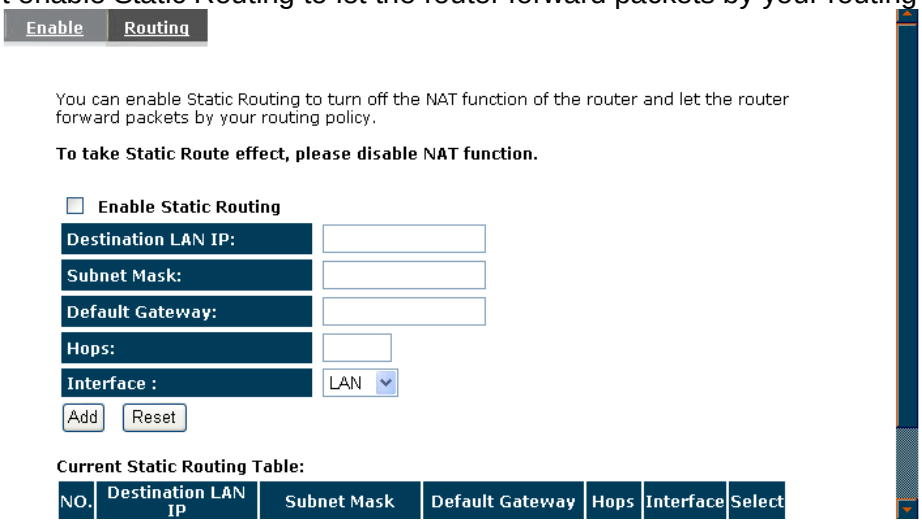
Rate: The data rate of QoS queue.

Disabled: This could turn off QoS feature.



8.8. 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.

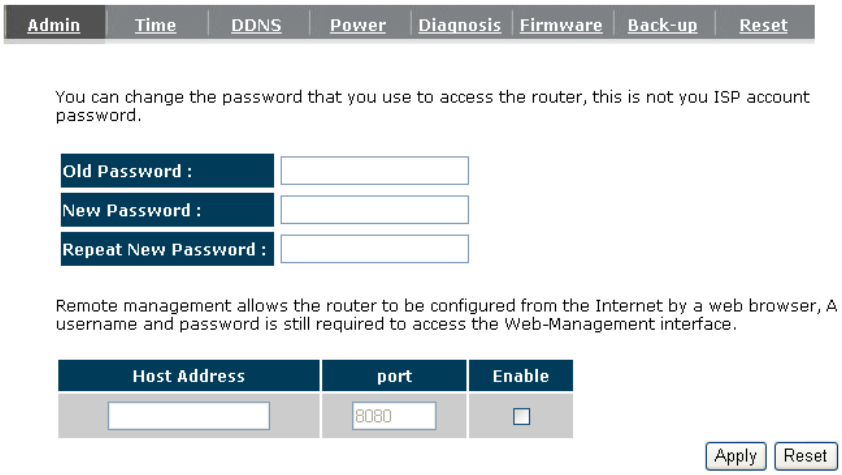
Hops: Specify the Max Hops number of static routing rule.

Interface: Specify the Interface of static routing rule.

9. TOOLS

9.1. Admin

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



Current 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 Broadband 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 Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

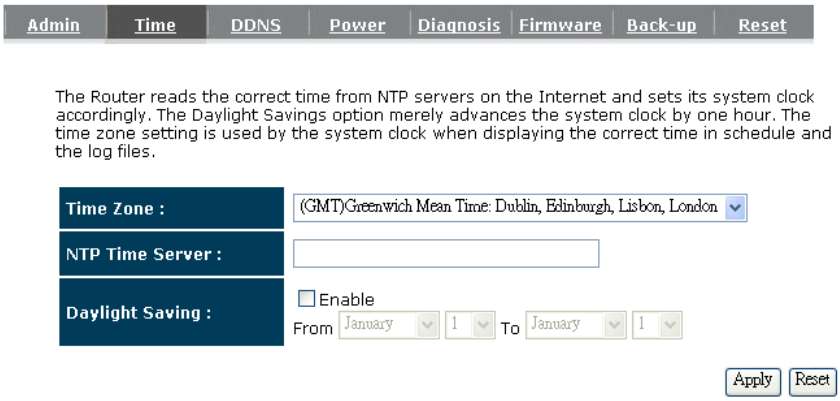
Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

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

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

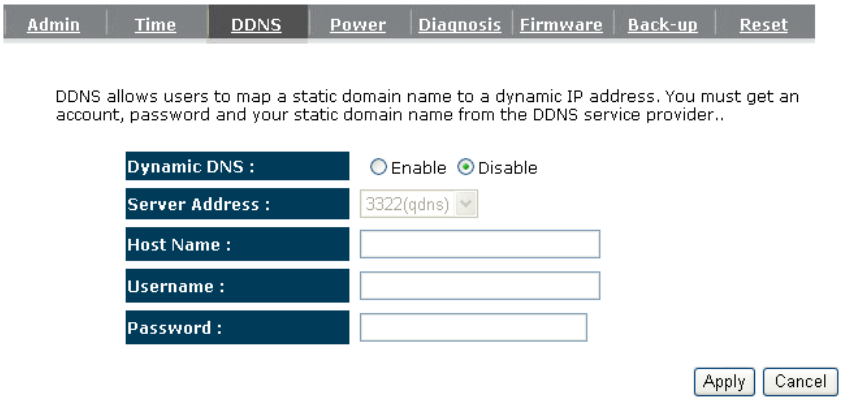
NTP Time Server: The router can set up external NTP Time Server.

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.

9.3. 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.

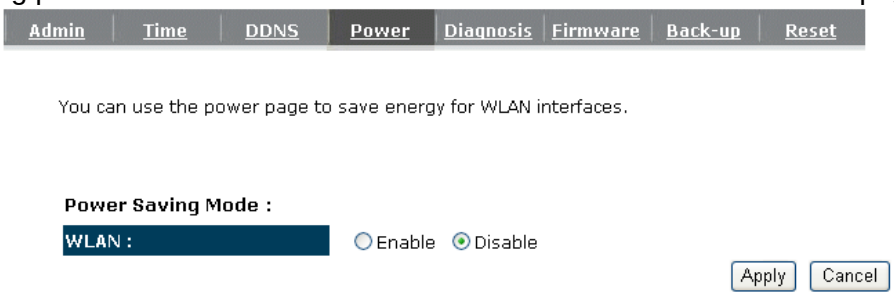
Username: The account that your DDNS service provider assigned to you.

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

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

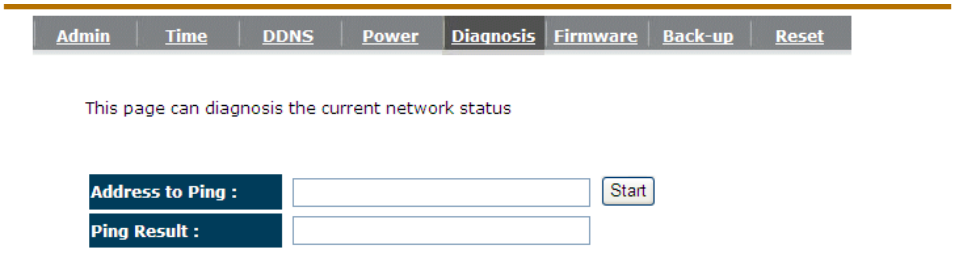
9.4. Power

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



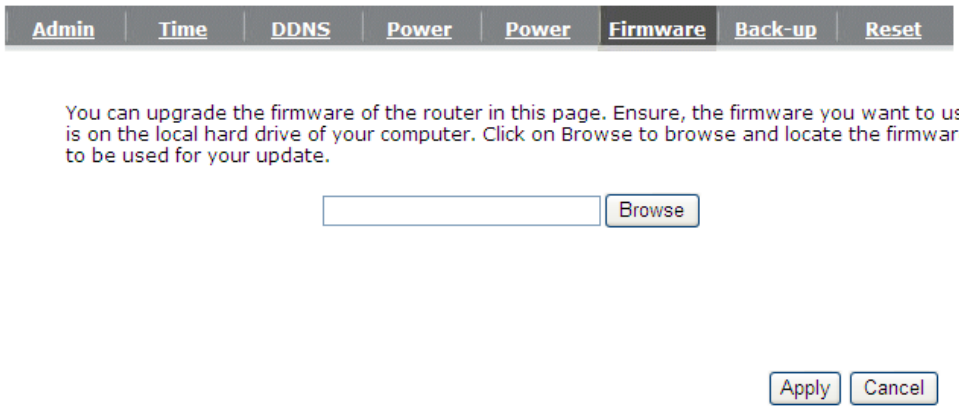
9.5. Diagnosis

This page could let you diagnosis your current network status.



9.6. Firmware

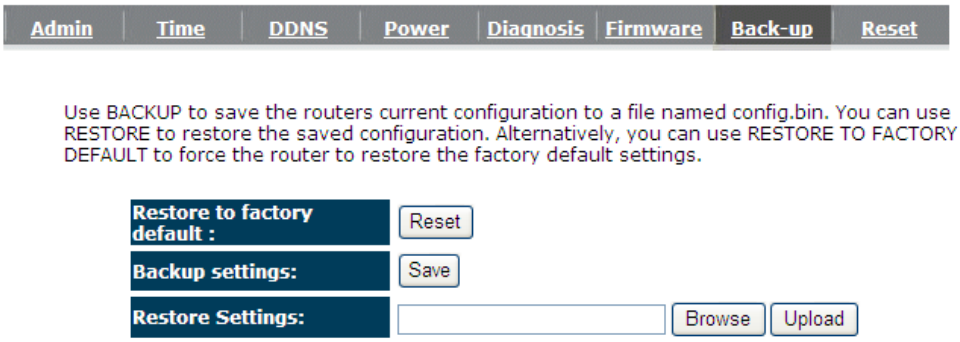
This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file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



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

9.7. Back-Up

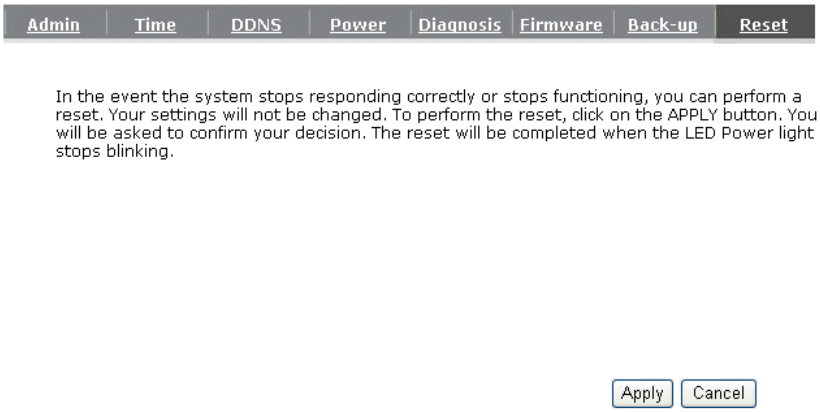
This page allows you to save the current router configurations. When you save the configurations, you also can re-load the saved configurations into the router through the **Restore Settings**. If extreme problems occur you can use the **Restore to Factory Defaults** to set all configurations to its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



Backup Settings: This can save the Broadband 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 Broadband router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the Broadband router to perform a power reset and restore the original factory settings.

9.8. Reset

You can reset the broadband 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.

For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.

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.