

# ESR9850

## Wireless N Gigabit Router

(IEEE 802.11 b/g/n)



User Manual

# Revision History

---

<b>Version</b>	<b>Date</b>	<b>Notes</b>
1.0	2009/5/22	Initial

# Table of Content

<b>1. INTRODUCTION</b>	<b>1</b>
1.1. SUMMARY	1
1.2. KEY FEATURES	2
1.3. PACKAGE CONTENTS	3
1.4. PRODUCT LAYOUT	4
<b>2. INSTALLATION</b>	<b>5</b>
2.1. NETWORK + SYSTEM REQUIREMENTS	5
2.2. WALL MOUNTING	5
2.3. ESR9850 PLACEMENT	6
2.4. SETUP LAN & WAN	7
2.5. PC NETWORK ADAPTER SETUP (WINDOWS XP)	8
2.6. SMART WIZARD CD	10
2.7. WIZARD CONFIGURATION	12
2.8. INITIAL SETUP ESR9850	14
<b>3. SYSTEM</b>	<b>16</b>
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
<b>4. WIZARD</b>	<b>24</b>
<b>5. INTERNET</b>	<b>25</b>
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
<b>6. WIRELESS</b>	<b>30</b>
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
<b>7. FIREWALL</b>	<b>43</b>
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

<b>8.</b>	<b>ADVANCED .....</b>	<b>50</b>
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
<b>9.</b>	<b>TOOLS .....</b>	<b>59</b>
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
<b>APPENDIX A – FCC INTERFERENCE STATEMENT .....</b>		<b>67</b>
<b>APPENDIX B – IC INTERFERENCE STATEMENT .....</b>		<b>68</b>

# 1. Introduction

## 1.1. Summary



ESR9850 is a 2T2R Wireless 11N Gigabit Router that delivers up to 6x faster speeds and 3x extended coverage than 802.11g devices. ESR9850 supports home network with superior throughput and performance and unparalleled wireless range. With easy to use on the WPS function, it helps users to connect to wireless device with just one push button.

There's also a built-in 4-port full-duplex 10/100/1000 Fast Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network shares a high-speed cable or DSL Internet connection.

## 1.2. Key Features

Features	Advantages
Incredible Data Rate up to 600Mbps**	<b>Heavy data payloads such as MPEG video streaming</b>
Multiple SSIDs	<b>Enhanced management among multiple users groups</b>
Four 10/100/1000 Mbps Fast Switch Ports (Auto-Crossover)	<b>Scalability, extend your network.</b>
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	<b>Avoids the attacks of Hackers or Viruses from Internet</b>
Support 802.1x Authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	<b>Provide mutual authentication (Client and dynamic encryption keys to enhance security</b>
WDS (Wireless Distribution System)	<b>Make wireless AP and Bridge mode simultaneously as a wireless repeater</b>
WPS button support	<b>Quick WiFi Security Setup</b>
WMM & QoS	<b>Wireless QoS mechanism</b>
Best channel selection	<b>Automatic optimal channel search</b>

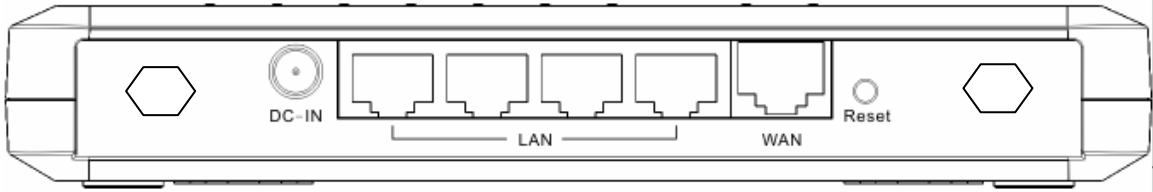
\*\* Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.

### 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 (ESR9850)
- 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	<ul style="list-style-type: none"> <li>● WAN: 1 * 10/100/1000 Fast Ethernet RJ-45</li> <li>● LAN: 4 * 10/100/1000 Fast Ethernet RJ-45</li> <li>● Reset Button (5 second for reboot, 5~10 seconds for reset to factory default )</li> <li>● Power Jack</li> <li>● WPS push button (Wi-Fi Protected Setup)</li> <li>● Antenna: SMA Connector * 2</li> </ul>
LEDs Status	<ul style="list-style-type: none"> <li>● Power/ Status</li> <li>● Internet (WAN)</li> <li>● LAN1~LAN4</li> <li>● WLAN</li> <li>● WPS</li> </ul>



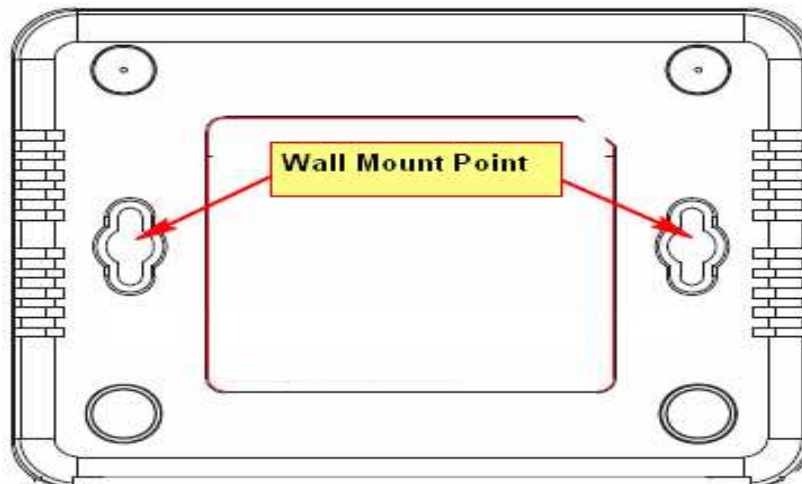
## 2. Installation

### 2.1. Network + System Requirements

To begin using the ESR9850, 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 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. 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. Finally, carefully mount the device onto the wall and make sure the nails are firmly locked on the mount points.

### **2.3. ESR9850 Placement**

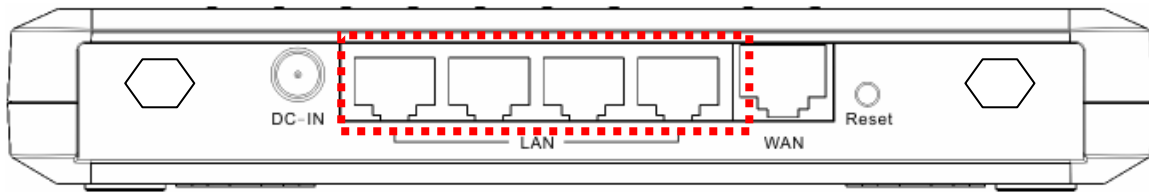
You can place ESR9850 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your device in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven.

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.

## 2.4. Setup LAN & WAN

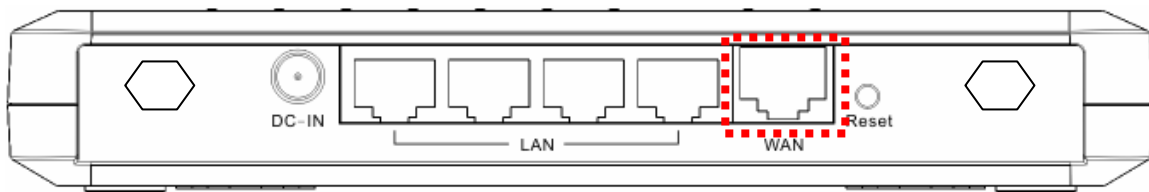
LAN connection:

Connect Ethernet cable between your PC/Notebook LAN port & one of the 4 available LAN ports on ESR9850.



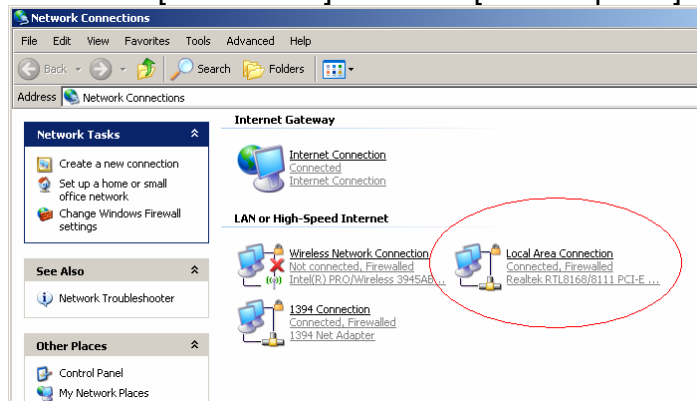
WAN connection:

Connect Ethernet cable between WAN ports of your ADSL/CABLE modem & INTERNET port of ESR9850. Make sure your ADSL/CABLE modem is working well. Contact your ISP if you have any questions.

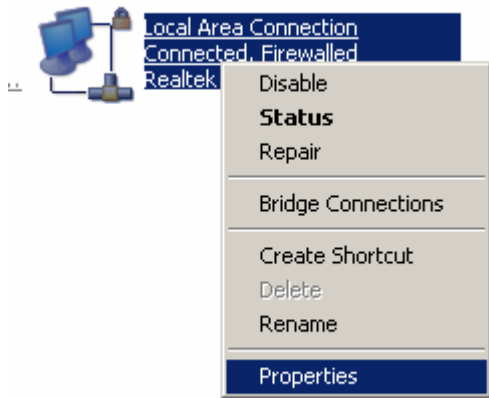


## 2.5. PC Network Adapter setup (Windows XP)

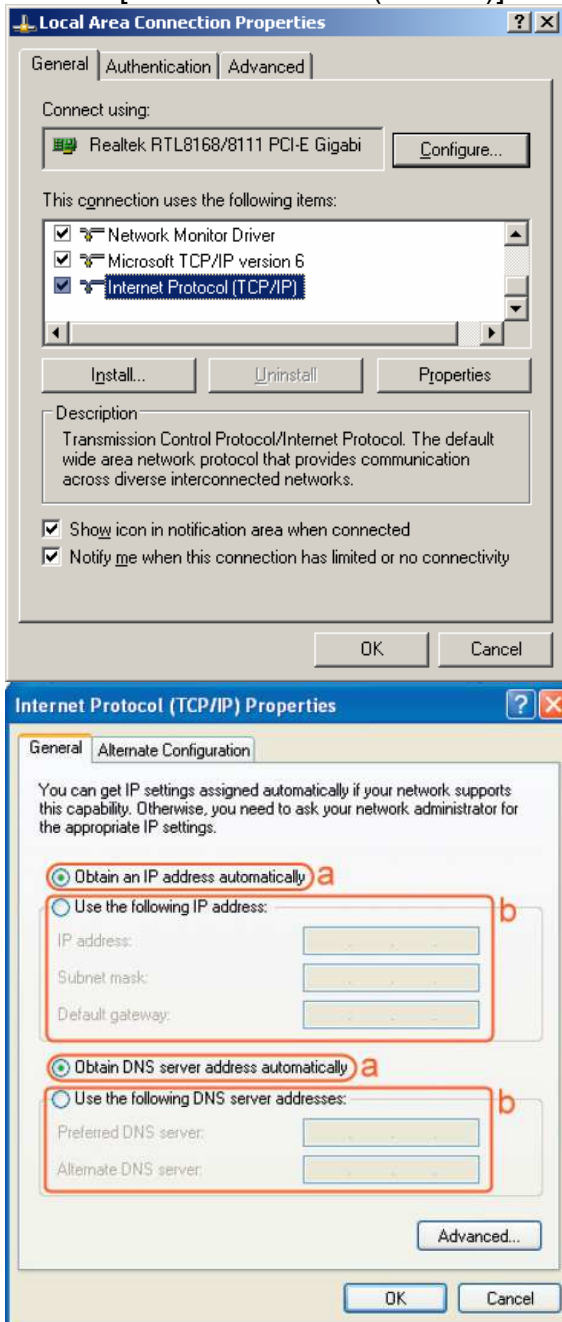
- Enter [Start Menu] → select [Control panel] → select [Network].



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



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



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

## 2.6. Smart Wizard CD

### Prerequisites:

- A standard CD-ROM drive
- ADSL / Cable Modem with RJ45 port.
- Microsoft Windows compatible PC/Notebook with Ethernet network interface.
- CAT 5 network cable(s), RJ45 port on PC/Notebook.

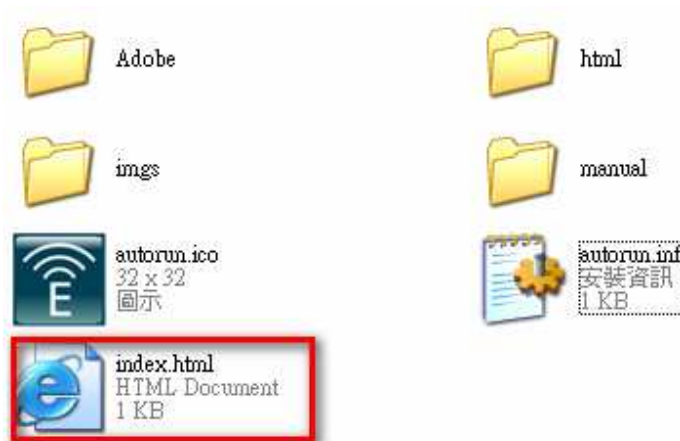
### STEP 1

Power up **ESR9850**. Please wait until WLAN starts blinking.

### STEP 2

Insert **Wizard CD** into your CD-ROM drive.

The Wizard should start in a few seconds. If Wizard does not start automatically, please browse the CD and Click on “**index.html**” to activate SMART WIZARD.



### Smart Wizard

Quick Setup

User Manual

Adobe Reader

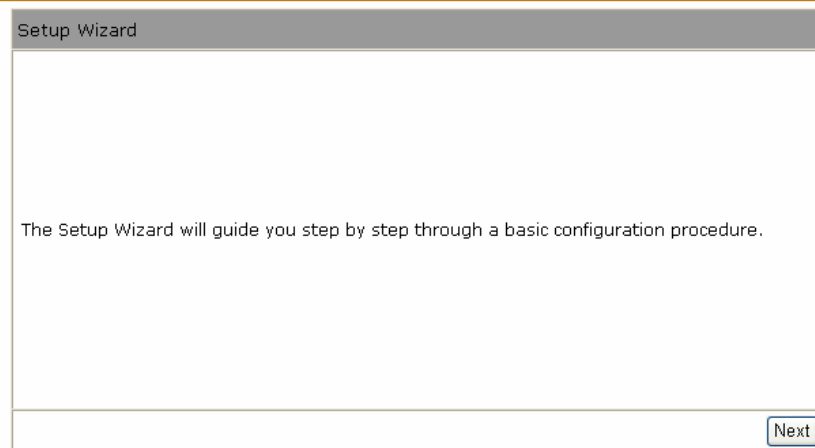
Exit



Please click on [**Quick Setup**] and follow the instructions given to complete the device initiation configuration.

Thank you for choosing **EnGenius**.

## 2.7. Wizard Configuration



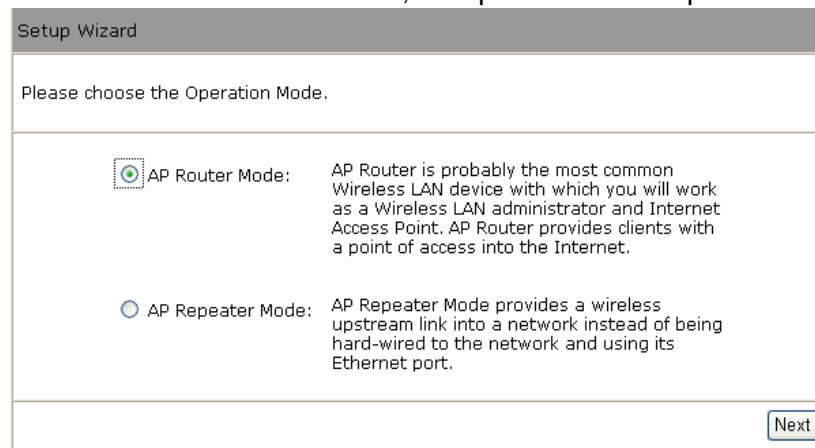
Setup Wizard

The Setup Wizard will guide you step by step through a basic configuration procedure.

Next

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

Select the mode that ESR9850 is going to be and set its configurations. **AP Repeater mode** does not enable WAN interface, Setup Wizard will skip WAN Configuration.



Setup Wizard

Please choose the Operation Mode.

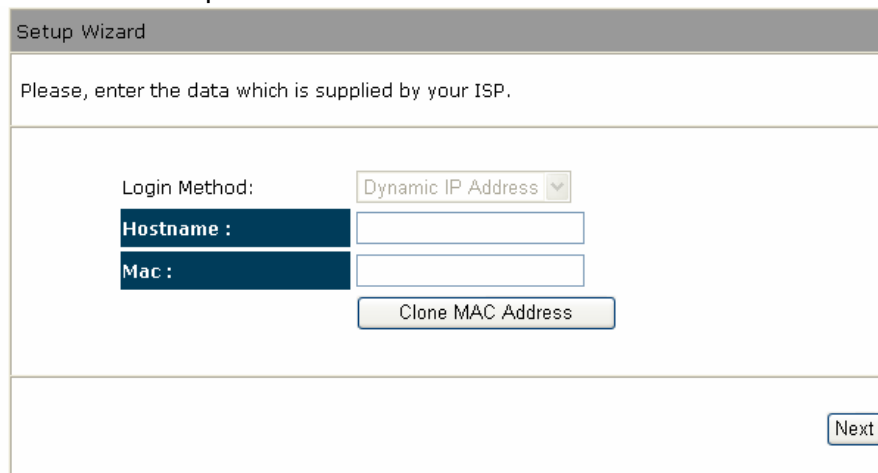
AP Router Mode: AP Router is probably the most common Wireless LAN device with which you will work as a Wireless LAN administrator and Internet Access Point. AP Router provides clients with a point of access into the Internet.

AP Repeater Mode: AP Repeater Mode provides a wireless upstream link into a network instead of being hard-wired to the network and using its Ethernet port.

Next

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.



Setup Wizard

Please, enter the data which is supplied by your ISP.

Login Method:

Hostname :

Mac :

Next



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

WLAN Configuration

Please choose the security level in the security bar

Lowest  Highest

Encryption method: WEP  
Authentication Type: Shared Key  
Please input SSID in the following box.  
Please input 10 or 26 hexadecimal characters,  
eg: 012345678, 5 or 13 ascii characters, eg:  
passd in the following key box.

SSID :

Key :

Enter the name for your wireless network (SSID) and security key  
Click **<Next>** to proceed

Setup Successfully

**System Configuration:**  
**Operation Mode :** AP Router

**WAN Configuration:**  
**Connection Type :** Dynamic IP

**WLAN Configuration :**  
**SSID :** EnGenius112244  
**Security :** WEP  
**WLAN Key :** 1234567890

WLAN Router setup successfully. Please click reboot button to reboot system.

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

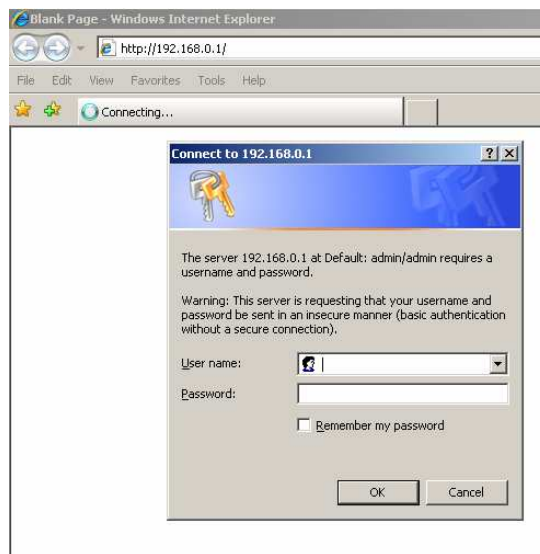
**NOTE:**

**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.**

## 2.8. Initial Setup ESR9850

ESR9850 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 ESR9850 configuration home page.
4. You will see the home page of ESR9850 as follows.

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 Gigabit Broadband Router
Mode	AP Router
Uptime	1 min 23 sec
Current Date/Time	2009/01/01 00:01:38
Hardware version	---
Serial Number	000000000
Kernel version	0.1.0
Application version	1.0.4

**WAN Settings**

Attain IP Protocol	Dynamic IP Address
IP address	---
Subnet Mask	---

## 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 ESR9850.

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

#### System

Model	Wireless Gigabit Broadband Router
Mode	AP Router
Uptime	2 min 25 sec
Current Date/Time	2009/01/01 00:02:25
Hardware version	---
Serial Number	000000000
Kernel version	0.1.0
Application version	1.0.4

**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.

#### WAN Settings

Attain IP Protocol	PPPoE
IP address	118.161.71.163
Subnet Mask	255.255.255.255
Default Gateway	118.161.64.254
MAC address	00:AA:77:50:00:CA
Primary DNS	168.95.192.1,168.95.1.1

**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.

### LAN Settings

IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC address	00:BB:77:50:03:28

**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.

### WLAN Settings

#### Wireless 2.4G Setting

Channel	11
<b>SSID_1</b>	
ESSID	EnGenius500328
Security	Disable
BSSID	00:BB:77:50:03:28

### WLAN Settings

#### Wireless 5G Setting

Channel	60
<b>SSID_1</b>	
ESSID	EnGenius50032C
Security	Disable
BSSID	00:BB:77:50:03:2C

## 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.

<a href="#">Status</a>	<a href="#">LAN</a>	<a href="#">DHCP</a>	<a href="#">Schedule</a>	<a href="#">Event Log</a>	<a href="#">Monitor</a>	<a href="#">Language</a>
------------------------	---------------------	----------------------	--------------------------	---------------------------	-------------------------	--------------------------

You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

### LAN IP

IP address :	<input type="text" value="192.168.0.1"/>
IP Subnet Mask :	<input type="text" value="255.255.255.0"/>
802.1d Spanning Tree :	<input type="text" value="Disabled"/>

### DHCP Server

DHCP Server :	<input type="text" value="Enabled"/>
Lease time :	<input type="text" value="Forever"/>
Start IP :	<input type="text" value="192.168.0.100"/>
End IP :	<input type="text" value="192.168.0.200"/>
Domain name :	<input type="text" value="esr7750"/>

### 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.

Status	LAN	<b>DHCP</b>	Schedule	Event Log	Monitor	Language
--------	-----	-------------	----------	-----------	---------	----------

#### DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server

IP address	MAC address	Expiration Time
192.168.0.100	00:30:1B:B5:54:C2	Forever

Refresh

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

IP address	MAC address
<input type="text"/>	<input type="text"/>

Add    Reset

Current Static DHCP Table :

NO.	IP address	MAC address	Select
-----	------------	-------------	--------

Delete Selected    Delete All    Reset

Apply    Cancel

### 3.4. Schedule

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



You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	All Time---Mon, Tue, Wed, Fri, Sat, Sun	<input type="checkbox"/>

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.



You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

<b>Schedule Description :</b>	<input type="text" value="schedule 02"/>
<b>Service :</b>	<input type="checkbox"/> Firewall <input type="checkbox"/> Power Saving
<b>Days :</b>	<input type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
<b>Time of day :</b>	<input type="checkbox"/> All Day (use 24-hour clock) From <input type="text" value="0"/> : <input type="text" value="0"/> To <input type="text" value="0"/> : <input type="text" value="0"/>

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



You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	All Time---Mon, Tue, Wed, Fri, Sat, Sun	<input type="checkbox"/>
2	schedule 02	Firewall	From 09:10 to 17:20---Wed, Thu, Fri, Sat	<input type="checkbox"/>
3	schedule 03	Power Saving+Firewall	From 09:10 to 17:20---Wed, Thu, Fri, Sat	<input type="checkbox"/>



### 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.



View the system operation information.

```
day 1 00:06:21 [SYSTEM]: SCHEDULE, Schedule Stopping
day 1 00:00:12 [SYSTEM]: DHCP Server, Sending ACK of 192.168.0.101
day 1 00:00:10 [SYSTEM]: UPNP, Stopping
day 1 00:00:10 [SYSTEM]: DDNS, Disabled
day 1 00:00:10 [SYSTEM]: NTP, NTP Client Starting
day 1 00:00:10 [SYSTEM]: DNS, DNS Proxy Starting
day 1 00:00:08 [SYSTEM]: NET, Firewall Starting
day 1 00:00:08 [SYSTEM]: NET, NAT Starting
day 1 00:00:08 [SYSTEM]: NET, Firewall Stopping
```

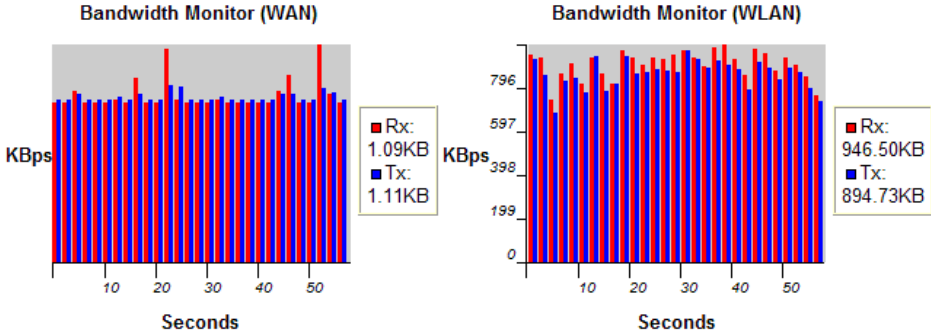


### 3.6. Monitor

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

Status	LAN	DHCP	Schedule	Event Log	Monitor	Language
--------	-----	------	----------	-----------	---------	----------

You can monitor the bandwidth in different interface. This page will refresh in every five seconds.

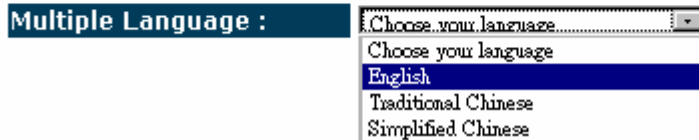


### 3.7. Language

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

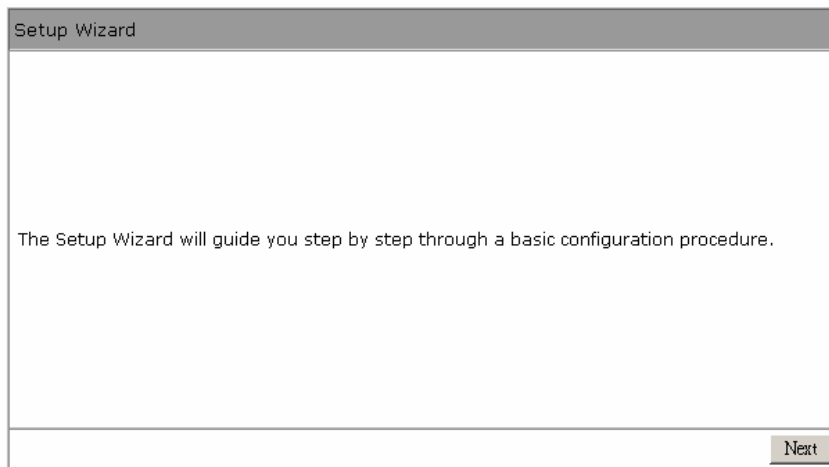


You can select other language in this page.



## 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

Status	Dynamic IP	Static IP	PPPOE	PPTP
View the current internet connection status and related information.				
<b>WAN Settings</b>				
Attain IP Protocol	Dynamic IP Address			
IP address	192.168.88.101			
Subnet Mask	255.255.255.0			
Default Gateway	192.168.88.2			
MAC address	00:11:25:28:BC:57			
Primary DNS	192.168.88.2			
<a href="#">Renew</a>				

## 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

---

Status	Dynamic IP	Static IP	PPPOE	PPTP
--------	------------	-----------	-------	------

You can select the type of the account you have with your ISP provider.

Hostname :	<input type="text"/>	
MAC address:	<input type="text" value="00112528BC57"/>	<input type="button" value="Clone MAC"/>

**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.

Status	Dynamic IP	<b>Static IP</b>	PPPOE	PPTP
--------	------------	------------------	-------	------

You can select the type of the account you have with your ISP provider.

<b>IP address:</b>	<input type="text" value="172.1.1.1"/>
<b>IP Subnet Mask :</b>	<input type="text" value="255.255.0.0"/>
<b>Default Gateway :</b>	<input type="text" value="172.1.1.254"/>
<b>Primary DNS :</b>	<input type="text"/>
<b>Secondary DNS :</b>	<input type="text"/>

Apply	Cancel
-------	--------

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

Status Dynamic IP Static IP **PPPOE** PPTP

You can select the type of the account you have with your ISP provider.

Login :	<input type="text" value="username"/>
Password :	<input type="password" value="••••••"/>
Service Name	<input type="text"/>
MTU :	<input type="text" value="1452"/> (512<=MTU Value<=1492)
Type :	<input type="button" value="Keep Connection"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Timeout :	<input type="text" value="10"/> (1-1000 Minutes)

**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)

The screenshot shows a configuration page with five tabs: Status, Dynamic IP, Static IP, PPPOE, and PPTP. The PPTP tab is selected. Below the tabs, there is a text instruction: "You can select the type of the account you have with your ISP provider." The configuration is divided into two sections: "WAN Interface Settings" and "PPTP Settings".

**WAN Interface Settings :**

- WAN Interface Type : Dynamic IP Address (dropdown menu)
- Hostname : (text input field)
- MAC Address : (text input field) with a "Clone Mac" button to its right.

**PPTP Settings :**

- Login : (text input field)
- Password : (text input field)
- Service IP address : (text input field)
- ConnectionID : 0 (text input field) with "(Optional)" to its right.
- MTU : 1462 (text input field) with "(512<=MTU Value<=1492)" to its right.

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.

Module is reloading, please wait  seconds

# 6. WIRELESS

## 6.1. Basic



This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

**Radio :**  Enable  Disable

**Mode :**

**Band :**

**Enabled SSID#:**

**SSID1 :**

**Auto Channel :**  Enable  Disable

**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**, **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.

**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.

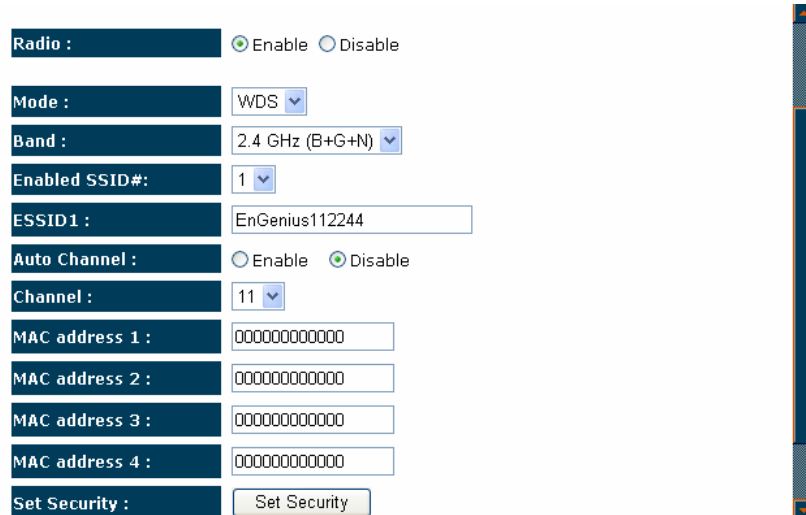
**Auto Channel:** Device will search all valid channels, then decide a most clean channel and change to this channel if you enable this function. Depend on this function enable or not, you will see different item below **Auto Channel**.

**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.

## 6.2. Mode: WDS

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



The screenshot shows the WDS configuration interface with the following settings:

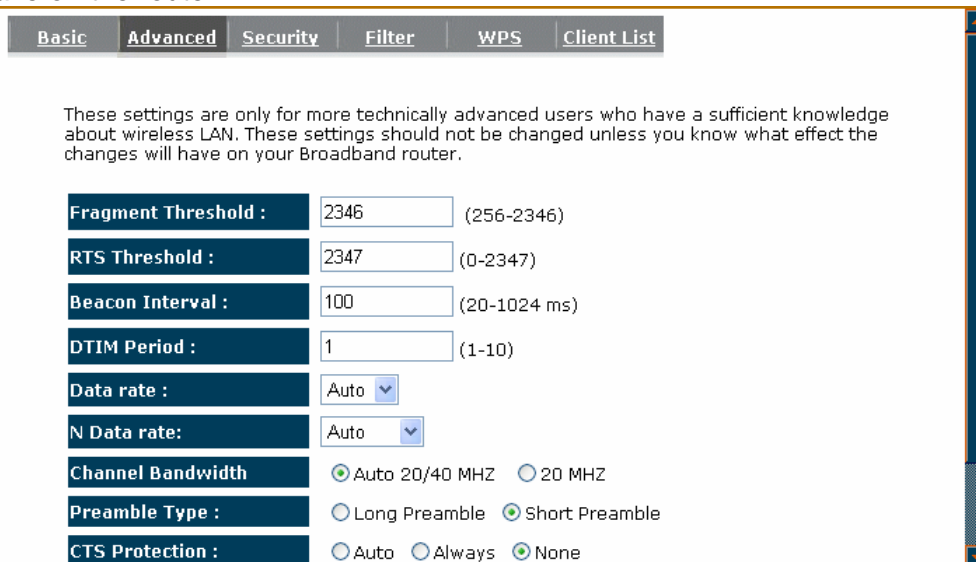
- Radio :  Enable  Disable
- Mode : WDS
- Band : 2.4 GHz (B+G+N)
- Enabled SSID# : 1
- ESSID1 : EnGenius112244
- Auto Channel :  Enable  Disable
- Channel : 11
- MAC address 1 : 000000000000
- MAC address 2 : 000000000000
- MAC address 3 : 000000000000
- MAC address 4 : 000000000000
- Set Security : Set Security

**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.



The screenshot shows the Advanced wireless settings interface with the following settings:

- Fragment Threshold : 2346 (256-2346)
- RTS Threshold : 2347 (0-2347)
- Beacon Interval : 100 (20-1024 ms)
- DTIM Period : 1 (1-10)
- Data rate : Auto
- N Data rate: Auto
- Channel Bandwidth  Auto 20/40 MHz  20 MHz
- Preamble Type :  Long Preamble  Short Preamble
- CTS Protection :  Auto  Always  None

**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.

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

## 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.

Basic	Advanced	<b>Security</b>	Filter	WPS	Client List
-------	----------	-----------------	--------	-----	-------------

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

ESSID Selection :	EnGenius112244
Broadcast ESSID :	Disable
WMM :	Enable
Encryption :	Disable

Enable 802.1x Authentication

Apply Cancel

**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 ESR9850.

### **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.

<b>ESSID Selection :</b>	EnGenius112244 ▾
<b>Broadcast ESSID :</b>	Disable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	Disable ▾
<input checked="" type="checkbox"/> <b>Enable 802.1x Authentication</b>	
<b>RADIUS Server IP address :</b>	<input type="text"/>
<b>RADIUS Server port :</b>	1812
<b>RADIUS Server password :</b>	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

## 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.

ESSID Selection :	EnGenius112244 ▾
Broadcast ESSID :	Disable ▾
WMM :	Enable ▾
Encryption :	WEP ▾
Authentication type :	<input type="radio"/> Open System <input checked="" type="radio"/> Shared Key <input type="radio"/> Auto
Key Length :	64-bit ▾
Key type :	Hex (10 characters) ▾
Default key :	Key 1 ▾
Encryption Key 1 :	*****
Encryption Key 2 :	*****
Encryption Key 3 :	*****
Encryption Key 4 :	*****

**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.

ESSID Selection :	EnGenius112244
Broadcast ESSID :	Disable
WMM :	Enable
Encryption :	WPA pre-shared key
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type :	Passphrase
Pre-shared Key :	

### 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.

ESSID Selection :	EnGenius112244
Broadcast ESSID :	Disable
WMM :	Enable
Encryption :	WPA RADIUS
WPA type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address :	
RADIUS Server port :	1812
RADIUS Server password :	

## 6.5. Filter

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

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point.

Enable Wireless Access Control

Description	MAC address
<input type="text"/>	<input type="text"/>

**MAC Address Filtering Table:**

NO.	Description	MAC address	Select
1	MyPC	00:02:6F:12:34:56	<input type="checkbox"/>

**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.

Basic	Advanced	Security	Filter	<b>WPS</b>	Client List
<b>WPS:</b>		<input checked="" type="checkbox"/> Enable			
<b>Wi-Fi Protected Setup Information</b>					
<b>WPS Current Status:</b>		Configured			
<b>Self Pin Code:</b>		11228844			
<b>SSID:</b>		EnGenius112244			
<b>Authentication Mode:</b>		WEP			
<b>Passphrase Key:</b>		<input type="text"/>			
<b>Interface :</b>		AP			
<b>WPS Via Push Button:</b>		<input type="button" value="Start to Process"/>			
<b>WPS via PIN:</b>		<input type="text"/>		<input type="button" value="Start to Process"/>	

**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.

---

Basic Advanced Security Filter WPS **Client List**

**WLAN Client Table :**

This WLAN Client Table shows client MAC address associate to this Broadband Router

MAC address	Signal
00:02:6F:07:F4:57	100

## 6.8. Policy

2.4G	Basic	Advanced	Security	Filter	WPS	Client List	<b>Policy</b>
------	-------	----------	----------	--------	-----	-------------	---------------

<b>SSID 1 Connection Control Policy</b>	
WAN Connection	Enable ▾
Communication between Wireless clients	Enable ▾
Communication between Wireless clients and Wired clients	Enable ▾

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).



Firewall automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and SPI (Stateful Packet Inspection) are also supported. The hackers attack will be recorded associated with timestamp in the security logging area.

Firewall :  Enable  Disable

Apply

**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	<b>DMZ</b>	DoS	MAC Filter	IP Filter	URL Filter
--------	------------	-----	------------	-----------	------------

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, you can open unrestricted two-way Internet access for this client by defining a Virtual DMZ Host.

**Enable DMZ**

**Local IP Address :**

**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.



The Firewall can detect and block DOS attacks, DOS (Denial of Service) attacks can flood your Internet Connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable.

Block DoS :  Enable  Disable

**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 DMZ DoS **MAC Filter** IP Filter URL Filter

MAC Filters are used to deny or allow LAN computers from accessing the Internet.

Enable MAC filtering

Deny all clients with MAC address listed below to access the network

Allow all clients with MAC address listed below to access the network

Description	LAN MAC Address
<input type="text"/>	<input type="text"/>

Add Reset

**MAC Filtering table:**

NO.	Description	LAN MAC Address	Select
-----	-------------	-----------------	--------

Delete Selected Delete All Reset

Apply Cancel

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

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

**Allow:** If you select “**Allow**” then all clients will be denied to access Internet except 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 DMZ DoS MAC Filter IP Filter URL Filter

IP Filters are used to deny or allow LAN computers from accessing the Internet.

Enable IP Filtering Table

Deny all clients with MAC address listed below to access the network  
 Allow all clients with MAC address listed below to access the network

Description :

Protocol : Both

Local IP Address :  ~

Port range :  ~

NO.	Description	Local IP Address	Protocol	Port range	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

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

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

**Allow:** If you select “**Allow**” 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.

## 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 DMZ DoS MAC Filter IP Filter **URL Filter**

You can block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site

Enable URL Blocking

URL/keyword

Add Reset

**Current URL Blocking Table:**

NO.	URL/keyword	Select
1	badthing	<input type="checkbox"/>

Delete Selected Delete All Reset

Apply Cancel

**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>**.

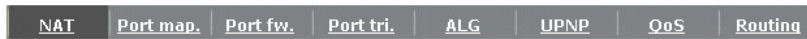
If you want remove all URL keywords from the table, click **<Delete All>** button. If you want to clear the selection and re-select again, just click **<Reset>**.

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.



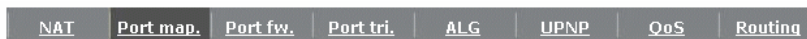
NAT(Network Address Translation) involves re-writing the source and/or destination addresses of IP packets as they pass through a Router or firewall, NAT enable multiple hosts on a private network to access the Internet using a single public IP address.

NAT :  Enable  Disable

Apply

## 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.



Entries in this table allow you to automatically redirect common network services to a specific PC behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the local network.

Enable Port Mapping

Description :   
Local IP :   
Protocol : Both   
Port range :  ~

Add Reset

Current Port Mapping Table:

NO.	Description	Local IP	Type	Port range	Select
-----	-------------	----------	------	------------	--------

**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).

NAT	Port map.	Port fw.	Port tri.	ALG	UPNP	QoS	Routing
-----	-----------	----------	-----------	-----	------	-----	---------

You can configure the router as a Virtual Server allowing remote users to access services such as Web or FTP at your local PC. Depending on the requested service (TCP/UDP) port number, the router will redirect the external service request to the appropriate internal server (located at one of your local PCs).

Enable Port Forwarding

Description :

Local IP :

Protocol : Both

Local Port :

Public Port :

Current Port Forwarding Table :



**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.

Port Triggering, also called Special Applications allows you to use Internet applications which normally do not function when used behind a firewall.

Enable Trigger Port

Description :

Popular applications :

Trigger port :  ~

Trigger type :

Public Port :

Public type :

Current Trigger-Port Table:

**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 to 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.

Description	Select
H323	<input type="checkbox"/>
MMS	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
Egg	<input type="checkbox"/>
IRC	<input type="checkbox"/>
Amanda	<input type="checkbox"/>
Quake3	<input type="checkbox"/>
Talk	<input type="checkbox"/>
IPsec	<input type="checkbox"/>
FTP	<input type="checkbox"/>

## 8.6. UPNP

With UPnP, all PCs in your 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.

UPnP :  Enable  Disable

Apply

**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.

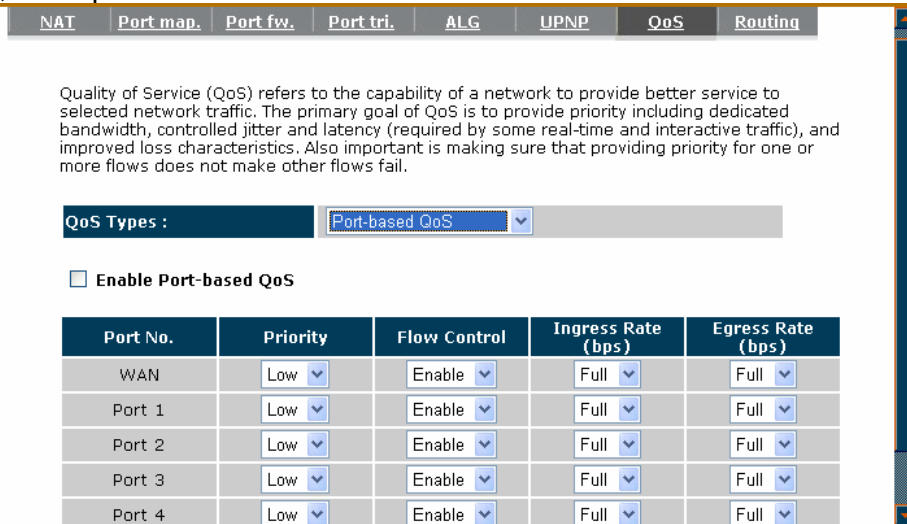
## 8.7. Quality of Service (QoS)

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.

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

**QoS Types :** Application-based QoS

**QoS :**  Priority Queue  Bandwidth Allocation  Disabled

**Unlimited Priority Queue**

IP Address	Description
<input type="text"/>	The IP address will not be bounded in the QoS limitation

**High/Low Priority Queue**

Protocol	High Priority	Low Priority	Specific Port
FTP	<input type="radio"/>	<input checked="" type="radio"/>	21
HTTP	<input type="radio"/>	<input checked="" type="radio"/>	80

**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.

NAT | Port map. | Port fw. | Port tri. | ALG | UPNP | **QoS** | Routing

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

**QoS Types :** Application-based QoS

**QoS :**  Priority Queue  Bandwidth Allocation  Disabled

**Type :** Download

**IP range :** 192.168.0.10 ~ 192.168.0.100

**Protocol :** ALL

**Port range :** 1 ~ 65535

**Policy :** Min

**Rate(bps) :** FULL

**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.

Admin	Time	DDNS	Power	Diagnosis	Firmware	Back-up	Reset
-------	------	------	-------	-----------	----------	---------	-------

You can change the password that you use to access the router, this is not you ISP account password.

Old Password :

New Password :

Repeat New Password :

Remote management allows the router to be configured from the Internet by a web browser, A username and password is still required to access the Web-Management interface.

Host Address	port	Enable
<input type="text"/>	8080	<input type="checkbox"/>

Apply Reset

**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.

Admin	Time	DDNS	Power	Diagnosis	Firmware	Back-up	Reset
-------	------	------	-------	-----------	----------	---------	-------

The Router reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
NTP Time Server :	<input type="text"/>
Daylight Saving :	<input type="checkbox"/> Enable From <input type="text" value="January"/> <input type="text" value="1"/> To <input type="text" value="January"/> <input type="text" value="1"/>

**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.

Admin	Time	<b>DDNS</b>	Power	Diagnosis	Firmware	Back-up	Reset
-------	------	-------------	-------	-----------	----------	---------	-------

DDNS allows users to map a static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service provider..

Dynamic DNS :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Address :	3322(qdns) ▼
Host Name :	<input type="text"/>
Username :	<input type="text"/>
Password :	<input type="text"/>

**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.



You can use the power page to save energy for WLAN interfaces.

### Power Saving Mode :

WLAN :

Enable  Disable

Apply

Cancel

# 9.5. Diagnosis

This page could let you diagnosis your current network status.

---

<a href="#">Admin</a>	<a href="#">Time</a>	<a href="#">DDNS</a>	<a href="#">Power</a>	<a href="#">Diagnosis</a>	<a href="#">Firmware</a>	<a href="#">Back-up</a>	<a href="#">Reset</a>
-----------------------	----------------------	----------------------	-----------------------	---------------------------	--------------------------	-------------------------	-----------------------

This page can diagnosis the current network status

<b>Address to Ping :</b>	<input type="text"/>	<input type="button" value="Start"/>
<b>Ping Result :</b>	<input type="text"/>	

## 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.



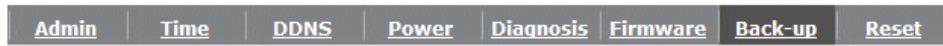
You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.

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.



Use BACKUP to save the routers current configuration to a file named config.bin. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings.

Restore to factory default :	<input type="button" value="Reset"/>
Backup settings:	<input type="button" value="Save"/>
Restore Settings:	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>

**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.



In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.



# 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.



