

# EAP 9550

## 11N Multi-Function AP/Repeater



# Table of Content

1.	Introduction.....	3
1.1.	Features and Benefits.....	3
1.2.	Package Contents.....	4
1.3.	System Requirement.....	4
2.	Modes.....	5
2.1.	Access Point.....	5
2.2.	WDS Bridge.....	5
2.3.	Universal Repeater.....	5
3.	Web Configuration.....	6
3.1.	System.....	6
3.1.1.	Operation Mode.....	6
3.1.2.	Status.....	7
3.1.3.	Schedule.....	7
3.1.4.	Event Log.....	8
3.1.5.	Monitor.....	8
3.2.	Wireless.....	10
3.2.1.	AP.....	10
3.2.2.	WDS Bridge.....	20
3.2.3.	Universal Repeater (AP).....	26
3.3.	Network.....	33
3.3.1.	Status.....	33
3.3.2.	LAN.....	34
3.4.	Management.....	34
3.4.1.	Admin.....	34
3.4.2.	SNMP.....	35
3.4.3.	Firmware.....	36
3.4.4.	Configure.....	36
3.4.5.	Reset.....	36
3.5.	Tools.....	37
3.5.1.	Time Setting.....	37
3.5.2.	Power Saving.....	38
3.5.3.	Diagnosis.....	38
3.5.4.	LED Control.....	39
3.6.	Logout.....	39
	Appendix A ó SPECIFICATIONS.....	40
	Appendix B ó FCC INTERFERENCE STATEMENT.....	41
	Appendix C ó IC Interference Statement.....	42

# 1.Introduction

**EAP9550** is a powerful and multi-functioned 11n Access Point and it can act three modes AP/WDS/Universal Repeater. Smoke detector appearance will minimize visibility. So this model can work properly at Hotel or public area. EAP9550 is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11g devices. Product's RF performance is finely tuned so it will bring best wireless signal for each client. EAP9550 supports home network with superior throughput, performance and unparalleled wireless range. To protect data during wireless transmissions, EAP9550 encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2. Its MAC address filter allows users to select stations with access to connect network. EAP9550 thus is the best product to ensure network quality for hotspots.

## 1.1. Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	Capable of handling heavy data payloads such as MPEG video streaming
IEEE 802.11n draft Compliant and backward compatible with 802.11b/g	Fully compatible with IEEE 802.11b/g/n devices
Multi-modes selectable	Allowing users to select AP/WDS/Universal Repeater mode in various application
Point-to-point, Point-to-multipoint Wireless Connectivity	Allowing to transfer data from buildings to buildings
WDS (Wireless Distributed System)	Making wireless AP and Bridge mode simultaneously as a wireless repeater
Universal Repeater	The easiest way to your wireless network's coverage
Support Multi-SSID function (4 SSID) in AP mode	Allowing clients to access different networks through a single access point and to assign different policies and functions for each SSID by manager
WPA2/WPA	Powerful data security
MAC address filtering in AP mode	Ensuring secure network connection
User isolation support (AP mode)	Protecting the private network between client users.
Power-over-Ethernet (IEEE802.3af)	Flexible Access Point locations and saving cost
Keep personal setting	Keeping the latest setting when firmware upgrade
SNMP Remote Configuration Management	Helping administrators to remotely configure or manage the Access Point easily
<b>QoS (WMM) support</b>	Enhancing user performance and density

## 1.2. Package Contents

The package contains the following items. In case of return, please keep the original box set, and the complete box set must be included for full refund.

- 1 EAP 9550
- 1 12V/1A 100V~240V Power Adapter
- 1 CD-ROM with User's Manual
- 1 Quick Guide

## 1.3. System Requirement

The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

## 2. Modes

AP/WDS/Repeater

### 2.1. Access Point

In AP (Access Point) mode, your device acts as a communication hub for users with a wireless device to connect to a wired LAN/WAN.

### 2.2. WDS Bridge



You can only connect to the device via Wireless Client

WDS (Wireless Distribution System) allows AP to communicate with one another wirelessly. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks.

### 2.3. Universal Repeater

Repeater is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances and through areas with high levels of electromagnetic interference (EMI).

Universal Repeater (AP) mode on one radio channel is usually configured along with Universal Repeater (STA) mode on another radio channel.

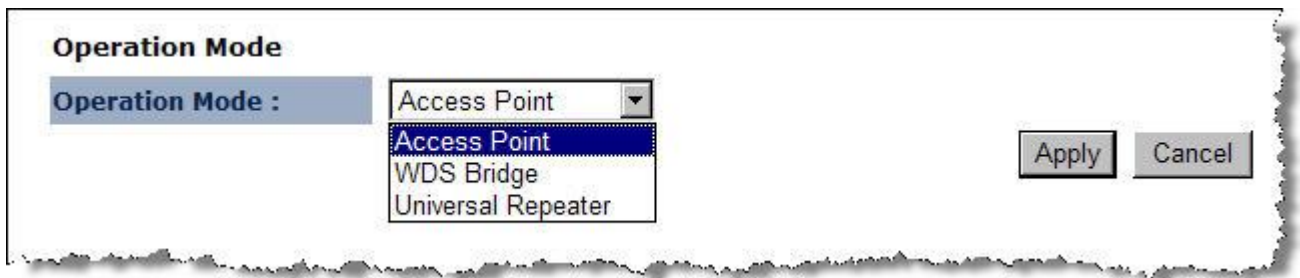
# 3. Web Configuration

## 3.1. System

### 3.1.1. Operation Mode

You are allowed to configure EAP 9550 into different modes: AP, WDS Bridge and Universal Repeater.

Please refer to [Chapter 2: Modes](#) for operation under different modes.



**Operation Mode**

Operation Mode :

- Access Point
- WDS Bridge
- Universal Repeater

### 3.1.2. Status

You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.

**System**

Operation Mode	Access Point
System Time	2009/01/01 00:46:00
System Up Time	46 min 14 sec
Hardware Version	0.1.0
Serial Number	000000019
Kernel Version	0.2.0
Application Version	0.2.0

**WLAN Settings**

Channel	11
---------	----

**SSID\_1**

ESSID	EnGenius59FE80
Security	Disable
BSSID	00:02:6F:59:FE:80

- System: Basic information of the device.
- WLAN Settings: WLAN channel.
- SSID\_1: SSID information.

### 3.1.3. Schedule

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
-----	-------------	---------	----------	--------

### 3.1.4. Event Log

View the system operation information.

day	1	00:10:55	[SYSTEM]: wlanconfig	ath1	list	sta	get_mac_table	finish
day	1	00:10:55	[SYSTEM]: wlanconfig	ath0	list	sta	get_mac_table	finish
day	1	00:09:40	[SYSTEM]: wlanconfig	ath1	list	sta	get_mac_table	finish
day	1	00:09:40	[SYSTEM]: wlanconfig	ath0	list	sta	get_mac_table	finish
day	1	00:09:01	[SYSTEM]: wlanconfig	ath1	list	sta	get_mac_table	finish
day	1	00:09:01	[SYSTEM]: wlanconfig	ath0	list	sta	get_mac_table	finish
day	1	00:06:39	[SYSTEM]: wlanconfig	ath1	list	sta	get_mac_table	finish
day	1	00:06:39	[SYSTEM]: wlanconfig	ath0	list	sta	get_mac_table	finish
day	1	00:02:57	[SYSTEM]: wlanconfig	ath1	list	sta	get_mac_table	finish

Save Clear Refresh

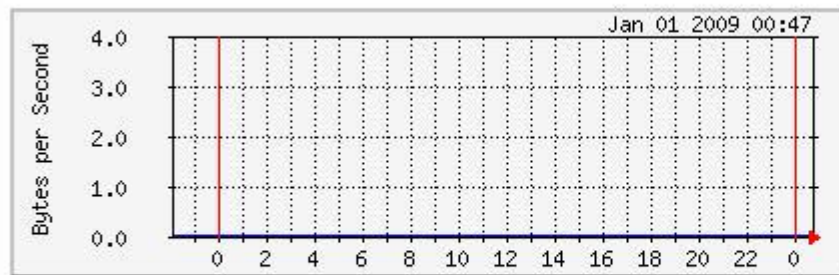
### 3.1.5. Monitor

The device will record the router transmission status in a time span.



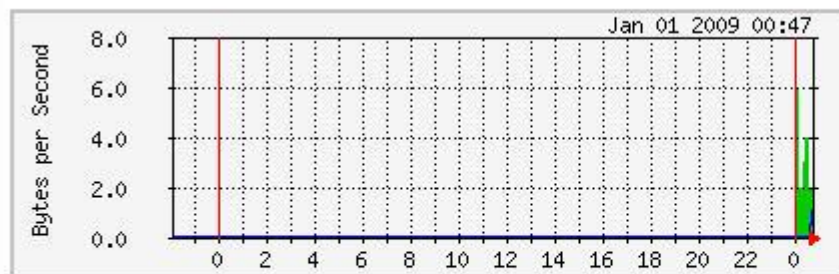
### Ethernet Daily Graph (5 Minute Average)

Detail



	Maxmun	Average	Current
<b>RX</b>	0 B/sec	0 B/sec	0 B/sec
<b>TX</b>	0 B/sec	0 B/sec	0 B/sec

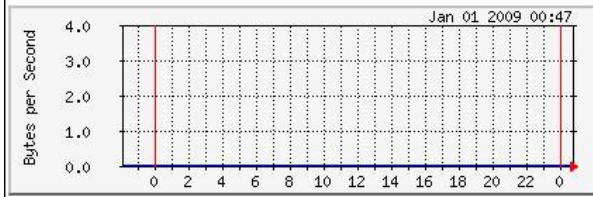
### WLAN Daily Graph (5 Minute Average)



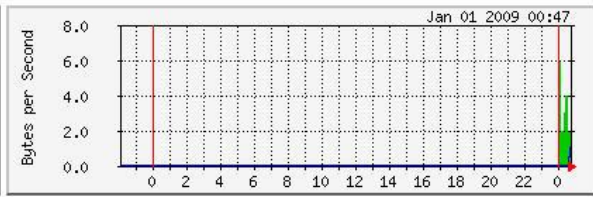
	Maxmun	Average	Current
<b>RX</b>	6 B/sec	2 B/sec	2 B/sec
<b>TX</b>	1 B/sec	0 B/sec	0 B/sec

- Detail: Click into detail to see historical record.

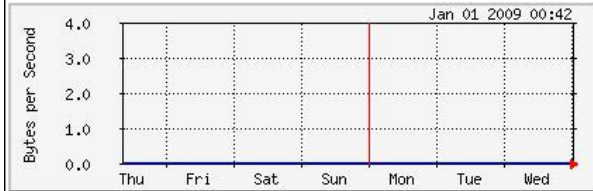
**Ethernet Daily Graph (5 Minute Average)**



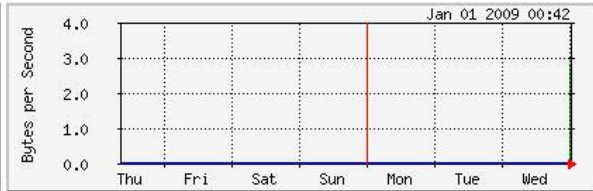
**WLAN Daily Graph (5 Minute Average)**



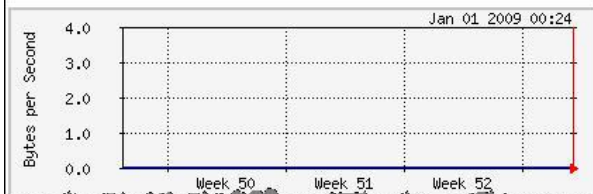
**Ethernet Weekly Graph (30 Minute Average)**



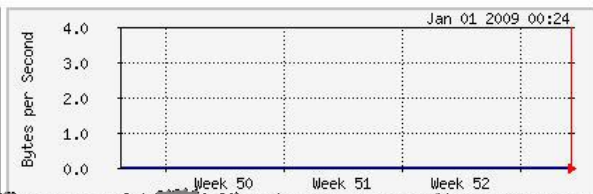
**WLAN Weekly Graph (30 Minute Average)**



**Ethernet Monthly Graph (2 Hour Average)**



**WLAN Monthly Graph (2 Hour Average)**



## 3.2. Wireless

### 3.2.1. AP

#### 3.2.1.1. Status

View the current internet connection status and related information.

<b>WLAN Settings</b>	
Channel	11
<b>SSID_1</b>	
ESSID	EnGenius59FE80
Security	Disable
BSSID	00:02:6F:59:FE:80

## 3.2.1.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

<b>Radio :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Mode :</b>	AP
<b>Band :</b>	2.4 GHz (B+G+N)
<b>Enabled SSID#:</b>	3
<b>ESSID1 :</b>	EnGenius59FE80
<b>ESSID2 :</b>	EnGenius59FE80_2
<b>ESSID3 :</b>	EnGenius59FE80_3
<b>Auto Channel :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Check Channel Time :</b>	Half day

- **Radio:** To enable/disable radio frequency.
- **Mode:** Define AP in different modes. When in AP mode, the device works as regular AP, or WDS mode to interlink with other AP devices You are allowed to set MAC address and encryption algorithm (Please refer to [4.2.1.4](#) for encryption configuration)

<b>MAC Address 1 :</b>	000000000000
<b>MAC Address 2 :</b>	000000000000
<b>MAC Address 3 :</b>	000000000000
<b>MAC Address 4 :</b>	000000000000
<b>Set Security :</b>	Set Security

- ✓ **AP**
- ✓ **WDS**
- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (B)**
  - ✓ **2.4 GHz (N)**
  - ✓ **2.4 GHz (B+G)**
  - ✓ **2.4 GHz (G)**
  - ✓ **2.4 GHz (B+G+N)**

- **Enabled SSID#:** The device allows you to add up to 4 unique SSID
- **ESSID#:** Description of each configured SSID
- **Auto Channel:** To enable/disable devices auto-detect channel used
- **Check Channel Time (Channel):** When Auto Channel is enabled; you can configure the channel detection interval. When Auto Channel is disabled; you can manually configure a channel to be used.
- **MAC Address 1~4:** To specify MAC address of other AP devices.



MAC address will only shows when configured in WDS AP mode.

- **Security:** Please refer to [4.2.1.4](#) for encryption configuration

### 3.2.1.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

<b>Fragment Threshold :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(0-2347)
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(20-1024 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-10)
<b>Data Rate :</b>	<input type="text" value="Auto"/>	
<b>N Data Rate:</b>	<input type="text" value="Auto"/>	
<b>Channel Bandwidth</b>	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
<b>Tx Power :</b>	<input type="text" value="100 %"/>	

- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.
- **Beacon Interval:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 24 and 1024. The default value is set to 100 milliseconds.

- **DTIM Period:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.
- **Data rate:** You may select a data rate from the drop-down list, however, it is recommended to select **auto**. This is also known as auto-fallback.
- **N Data Rate:** You may select N data rate from the drop-down list, however, it is recommended to select **auto**.
- **Channel Bandwidth:** Select channel bandwidth.
- **Preamble Type:** Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.
- **CTS Protection:** CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a clear signal before transmitting. It is recommended to select **auto**.
- **Tx Power:** You may control the transmit output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.

### 3.2.1.4. Security

#### ➤ Encryption: Disabled

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

<b>ESSID Selection :</b>	EnGenius59FE80 ▼
<b>Broadcast ESSID :</b>	Enable ▼
<b>WMM :</b>	Enable ▼
<b>Encryption :</b>	Disable ▼
<input type="checkbox"/> <b>Enable 802.1x Authentication</b>	

**Enable 802.1x Authentication**

<b>RADIUS Server IP Address :</b>	<input type="text"/>
<b>RADIUS Server Port :</b>	1812
<b>RADIUS Server undefined :</b>	<input type="text"/>

## ➤ Encryption: WEP

ESSID Selection :	EnGenius59FE80 ▼
Broadcast ESSID :	Enable ▼
WMM :	Enable ▼
Encryption :	WEP ▼
Authentication Type :	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length :	64-bit ▼
Key Type :	ASCII (5 characters) ▼
Default Key :	Key 1 ▼
Encryption Key 1 :	<input type="text"/>
Encryption Key 2 :	<input type="text"/>
Encryption Key 3 :	<input type="text"/>
Encryption Key 4 :	<input type="text"/>
<input checked="" type="checkbox"/> Enable 802.1x Authentication	
RADIUS Server IP Address :	<input type="text"/>
RADIUS Server Port :	1812
RADIUS Server undefined :	<input type="text"/>

- **ESSID Selection:** As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.
- **Broadcast SSID:** Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **WMM:** Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.
- **Encryption:** Select **WEP** from the drop-down list.
- **Authentication Type:** Select **Open System**, **Shared Key**, or **auto**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device

attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

- **Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **Key Type:** Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.
- **Default Key:** You may choose one of your 4 different WEP keys from below.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- **Enable 802.1x Authentication:** Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

## ➤ Encryption: WPA pre-shared key

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

<b>ESSID Selection :</b>	EnGenius59FE80 ▾
<b>Broadcast ESSID :</b>	Enable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	WPA pre-shared key ▾
<b>WPA Type :</b>	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
<b>Pre-shared Key Type :</b>	Passphrase ▾
<b>Pre-shared Key :</b>	<input type="text"/>

- **ESSID Selection:** As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.
- **Broadcast SSID:** Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the

range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **WMM:** Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.
- **Encryption:** Select **WPA pre-shared key** from the drop-down list.
- **WPA Type:** Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
- **Pre-shared Key Type:** The Key Type can be **passphrase** or **Hex** format.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

## ➤ Encryption: WPA RADIUS

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server.

ESSID Selection :	EnGenius59FE80 ▾
Broadcast ESSID :	Enable ▾
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 :	<input type="text"/>
RADIUS Server Port :	1812 <input type="text"/>
RADIUS Server undefined :	<input type="text"/>

Apply Cancel

- **ESSID Selection:** As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.
- **Broadcast SSID:** Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the



range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **WMM:** Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.
- **Encryption:** Select **WPA RADIUS** from the drop-down list.
- **WPA Type:** Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
- **RADIUS Server IP Address:** Specify the IP address of the RADIUS server.
- **RADIUS Server Port:** Specify the port number of the RADIUS server, the default port is 1812.
- **RADIUS Server Password:** Specify the pass-phrase that is matched on the RADIUS Server.

### 3.2.1.5. Filter

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

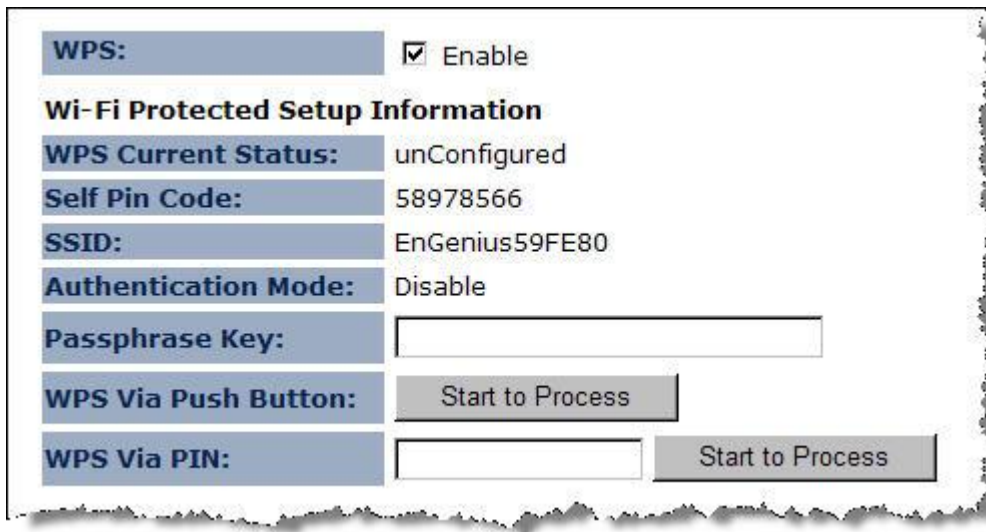
**Enable Wireless MAC Filtering**

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

**Only the following MAC Addresses can use network:**

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

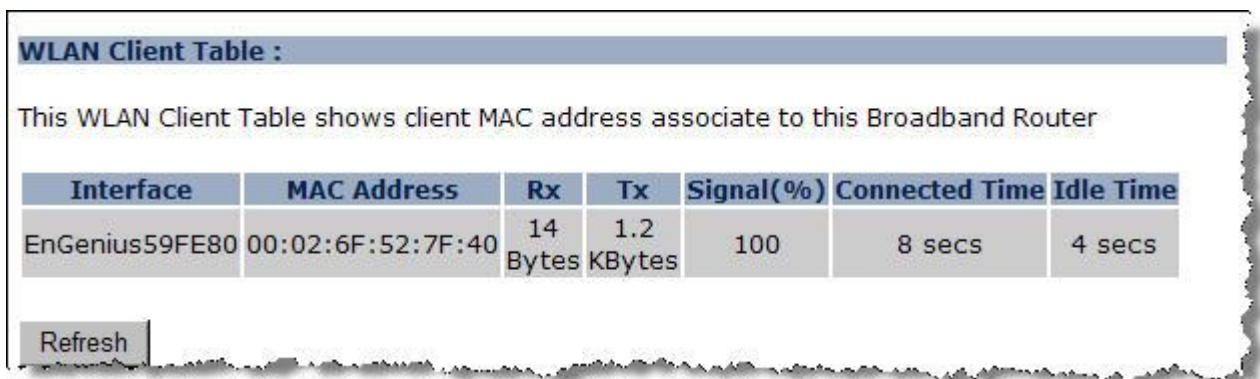
### 3.2.1.6. WPS



The screenshot shows a configuration page for WPS (Wi-Fi Protected Setup). At the top, there is a checkbox labeled 'WPS:' which is checked and labeled 'Enable'. Below this is a section titled 'Wi-Fi Protected Setup Information'. It contains several fields: 'WPS Current Status:' with the value 'unConfigured', 'Self Pin Code:' with the value '58978566', 'SSID:' with the value 'EnGenius59FE80', and 'Authentication Mode:' with the value 'Disable'. There are two input fields for 'Passphrase Key:'. At the bottom, there are two buttons labeled 'Start to Process' for 'WPS Via Push Button:' and 'WPS Via PIN:'.

- **WPS Current Status:**
- **Self Pin Code:**
- **SSID:**
- **Authentication Mode:**
- **Passphrase Key:**
- **WPS Via Push Button:**
- **WPS Via PIN:**

### 3.2.1.7. Client List



The screenshot shows a table titled 'WLAN Client Table :'. Below the title, there is a text description: 'This WLAN Client Table shows client MAC address associate to this Broadband Router'. The table has seven columns: 'Interface', 'MAC Address', 'Rx', 'Tx', 'Signal(%)', 'Connected Time', and 'Idle Time'. There is one data row for the interface 'EnGenius59FE80' with MAC address '00:02:6F:52:7F:40', showing 14 Bytes of Rx, 1.2 KBytes of Tx, 100% signal, 8 secs connected, and 4 secs idle. A 'Refresh' button is located at the bottom left of the table area.

Interface	MAC Address	Rx	Tx	Signal(%)	Connected Time	Idle Time
EnGenius59FE80	00:02:6F:52:7F:40	14 Bytes	1.2 KBytes	100	8 secs	4 secs

### 3.2.1.8. VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

**Virtual LAN :**  Enable  Disable

**SSID 1 Tag:**  (1~4096)

Apply Cancel

 Only Available in AP mode

- **Virtual LAN:** Choose to Enable or Disable the VLAN features.
- **SSID1 Tag:** Specify the VLAN tag.

### 3.2.1.9. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Reset to Default

Apply Cancel

## 3.2.2. WDS Bridge



You can only connect to the device via Wireless Client

### 3.2.2.1. Status

View the current internet connection status and related information.

<b>WLAN Settings</b>	
Channel	11
<b>SSID_1</b>	
ESSID	EnGenius59FE80
Security	Disable
BSSID	00:02:6F:59:FE:80


### 3.2.2.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

<b>Radio :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Mode :</b>	WDS
<b>Band :</b>	2.4 GHz (B+G+N)
<b>Channel :</b>	11
<b>MAC Address 1 :</b>	000000000000
<b>MAC Address 2 :</b>	000000000000
<b>MAC Address 3 :</b>	000000000000
<b>MAC Address 4 :</b>	000000000000
<b>Set Security :</b>	Set Security

Apply Cancel

- **Radio:** To enable/disable radio frequency.

- **Mode:** WDS mode allows you to interlink with other AP devices. Setting MAC address and encryption algorithm (Please refer to [4.2.1.4](#) for encryption configuration)
  - **Band:** Configure the device into different wireless modes.
    - ✓ **2.4 GHz (B)**
    - ✓ **2.4 GHz (N)**
    - ✓ **2.4 GHz (B+G)**
    - ✓ **2.4 GHz (G)**
    - ✓ **2.4 GHz (B+G+N)**
  - **Enabled SSID#:** The device allows you to add up to 4 unique SSID
  - **ESSID#:** Description of each configured SSID
  - **Channel:** You can manually configure a channel to be used.
  - **MAC Address 1~4:** To specify MAC address of other AP devices.
-  MAC address will only shows when configured in WDS AP mode.
- **Security:** Please refer to [4.2.1.4](#) for encryption configuration

## ➤ Security: Disabled

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

<b>Encryption :</b>	Disable	<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
---------------------	---------	--------------------------------------	--------------------------------------

## ➤ Security: WEP

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	<input type="text"/>
Encryption Key 2 :	<input type="text"/>
Encryption Key 3 :	<input type="text"/>
Encryption Key 4 :	<input type="text"/>

Apply Reset

- **Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **Key Format:** Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.
- **Default Tx Key:** You may choose one of your 4 different WEP keys from below.
- **Encryption Key 1-4:** You may enter four different WEP keys.

## ➤ Security: WPS pre-shared key

This page allows you setup the WDS bridge security. The value depends on your WDS Security settings.

Encryption :	WPA pre-shared key
WPA Type :	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES)
Pre-shared Key Format :	Passphrase
Pre-shared Key :	<input type="text"/>

Apply Reset

- **WPA Type:** Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
- **Pre-shared Key Type:** The Key Type can be **passphrase** or **Hex** format.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

### 3.2.2.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

<b>Fragment Threshold :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(0-2347)
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(20-1024 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-10)
<b>Data Rate :</b>	<input type="text" value="Auto"/>	
<b>N Data Rate:</b>	<input type="text" value="Auto"/>	
<b>Channel Bandwidth</b>	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
<b>Tx Power :</b>	<input type="text" value="100 %"/>	

- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.

- **Beacon Interval:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.
- **DTIM Period:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.
- **Data rate:** You may select a data rate from the drop-down list, however, it is recommended to select **auto**. This is also known as auto-fallback.
- **N Data Rate:** You may select N data rate from the drop-down list, however, it is recommended to select **auto**.
- **Channel Bandwidth:** Select channel bandwidth.
- **Preamble Type:** Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.
- **CTS Protection:** CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a clear signal before transmitting. It is recommended to select **auto**.
- **Tx Power:** You may control the transmit output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.



### 3.2.2.4. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Reset to Default

Apply

Cancel

## 3.2.3. Universal Repeater (AP)

### 3.2.3.1. Status

View the current internet connection status and related information.

WLAN AP Client Information	
Connection Status	Fail
ESSID	---
Security	---
BSSID	---

WLAN Settings	
Channel	6

SSID_1	
ESSID	EnGenius59FE80
Security	Disable
BSSID	00:02:6F:59:FE:80

### 3.2.3.2. Basic

This page allows you to define Mode, Band, Multiple ESSID. You can also set up a static wireless channel or make Wireless Router move to a clean Wireless Channel automatically.

<b>Radio :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Mode :</b>	Universal Repeater ▾
<b>Band :</b>	2.4 GHz (B+G+N) ▾
<b>Enabled SSID#:</b>	1 ▾
<b>ESSID1 :</b>	EnGenius59FE80
<b>Channel :</b>	11 ▾
<b>Site Survey :</b>	Site Survey

Site Survey								
NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	6	CHOU	00:19:CB:56:AA:B2	WEP	AUTOWEP	100	11b/g

Refresh    Connect

- **Radio:** To enable/disable radio frequency.
- **Mode:** Universal Repeater
- **Band:** Configure the device into different wireless modes.
  - ✓ 2.4 GHz (B)
  - ✓ 2.4 GHz (N)
  - ✓ 2.4 GHz (B+G)
  - ✓ 2.4 GHz (G)
  - ✓ 2.4 GHz (B+G+N)
- **Enabled SSID#:** The device allows you to add up to 4 unique SSID
- **ESSID#:** Description of each configured SSID
- **Channel:** You can manually configure a channel to be used.
- **Site Survey:** List out all connected devices.

### 3.2.3.3. Advanced

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

<b>Fragment Threshold :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(0-2347)
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(20-1024 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-10)
<b>Data Rate :</b>	Auto ▾	
<b>N Data Rate:</b>	Auto ▾	
<b>Channel Bandwidth</b>	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
<b>Tx Power :</b>	100 % ▾	

- **Fragment Threshold:** Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance. Specify a value between 0 and 2347. The default value is 2347.
- **Beacon Interval:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Interval value between 25 and 1000. The default value is set to 100 milliseconds.
- **DTIM Period:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Period value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 10.
- **Data rate:** You may select a data rate from the drop-down list, however, it is recommended to select **auto**. This is also known as auto-fallback.
- **Preamble Type:** Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.
- **CTS Protection:** CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a clear signal before transmitting. It is recommended to select **auto**.
- **Tx Power:** You may control the transmit output power of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.

### 3.2.3.4. Security

#### ➤ Encryption: Disabled

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

<b>ESSID Selection :</b>	EnGenius59FE80 ▾
<b>Broadcast ESSID :</b>	Enable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	Disable ▾

## ➤ Encryption: WEP

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius59FE80 ▾
Broadcast ESSID :	Enable ▾
WMM :	Enable ▾
Encryption :	WEP ▾
Authentication Type :	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
Key Length :	64-bit ▾
Key Type :	ASCII (5 characters) ▾
Default Key :	Key 1 ▾
Encryption Key 1 :	<input type="text"/>
Encryption Key 2 :	<input type="text"/>
Encryption Key 3 :	<input type="text"/>
Encryption Key 4 :	<input type="text"/>

- **ESSID Selection:** As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.
- **Broadcast SSID:** Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **WMM:** Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.
- **Encryption:** Select **WEP** from the drop-down list.
- **Authentication Type:** Select **Open System**, **Shared Key**, or **auto**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly,

the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

- **Key Length:** Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **Key Type:** Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in **HEX** (hexadecimal - using characters 0-9, A-F) or **ASCII** (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.
- **Default Key:** You may choose one of your 4 different WEP keys from below.
- **Encryption Key 1-4:** You may enter four different WEP keys.
- **Enable 802.1x Authentication:** Place a check in this box if you would like to use RADIUS authentication. This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. You will then be required to specify the RADIUS Server's IP address, port, and password.

## ➤ Encryption: WPA pre-shared key

This page allows you setup the wireless security. You can turn on WEP or WPA by using Encryption Keys, besides you can enable 802.1x Authentication or RADIUS to coordinate with RADIUS server

ESSID Selection :	EnGenius59FE80 ▾
Broadcast ESSID :	Enable ▾
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 :	<input type="text"/>

- **ESSID Selection:** As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.
- **Broadcast SSID:** Select **Enable** or **Disable** from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **WMM:** Choose to **Enable** or **Disable** WMM. This is the Quality of Service (QoS) feature for prioritizing voice and video applications. This option can be further configured in **WMM** under the **Wireless** drop-down menu.
- **Encryption:** Select **WPA pre-shared key** from the drop-down list.
- **WPA Type:** Select TKIP, AES, or WPA2 Mixed. The encryption algorithm used to secure the data communication. **TKIP** (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. **AES** (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.
- **Pre-shared Key Type:** The Key Type can be **passphrase** or **Hex** format.
- **Pre-Shared Key:** The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

### 3.2.3.5. Filter

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

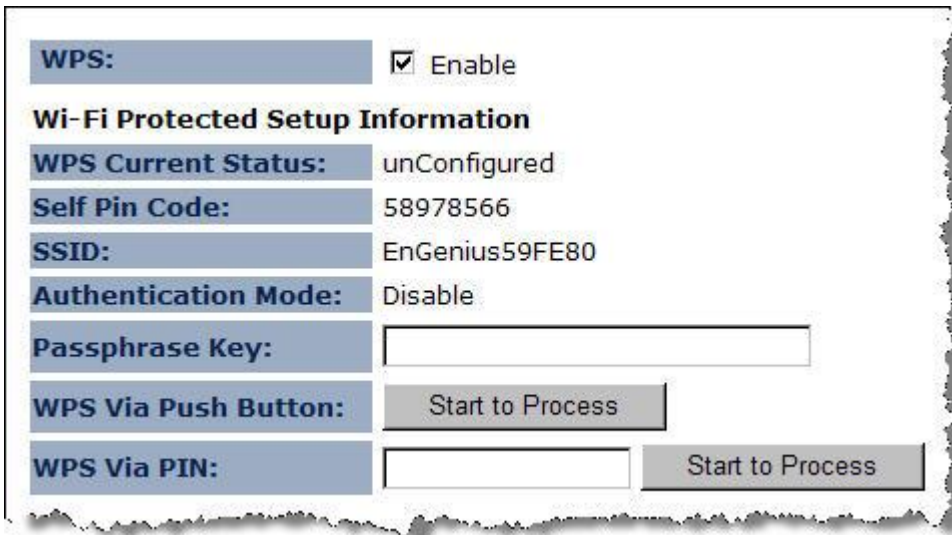
**Enable Wireless MAC Filtering**

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

**Only the following MAC Addresses can use network:**

NO.	Description	MAC Address	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

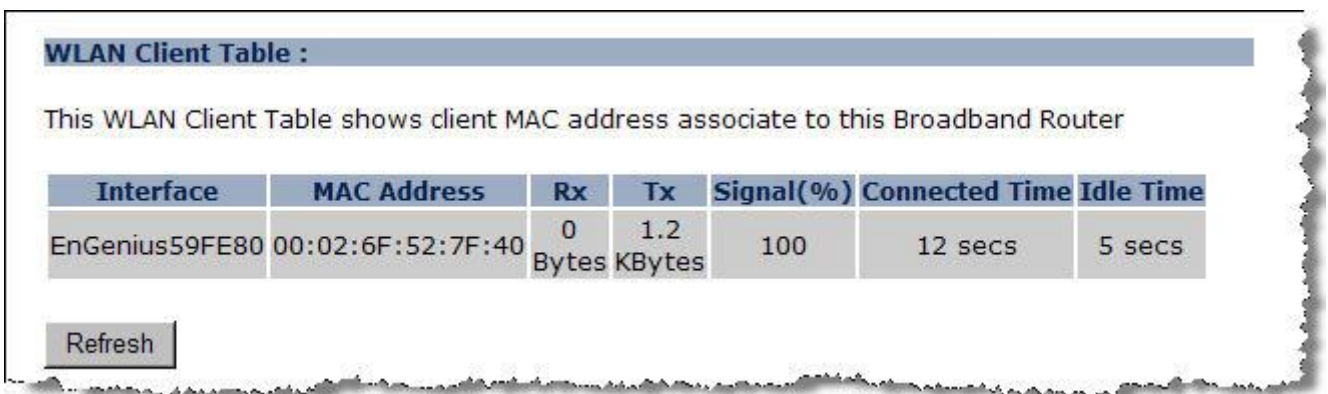
### 3.2.3.6. WPS



The screenshot shows a configuration page for WPS (Wi-Fi Protected Setup). At the top, there is a 'WPS:' section with a checked 'Enable' checkbox. Below this is the 'Wi-Fi Protected Setup Information' section. It contains several fields: 'WPS Current Status' is 'unConfigured', 'Self Pin Code' is '58978566', 'SSID' is 'EnGenius59FE80', and 'Authentication Mode' is 'Disable'. There are three input fields: 'Passphrase Key', 'WPS Via Push Button', and 'WPS Via PIN'. The 'WPS Via Push Button' and 'WPS Via PIN' fields each have a 'Start to Process' button next to them.

- **WPS Current Status:**
- **Self Pin Code:**
- **SSID:**
- **Authentication Mode:**
- **Passphrase Key:**
- **WPS Via Push Button:**
- **WPS Via PIN:**

### 3.2.3.7. Client List



The screenshot shows a 'WLAN Client Table' with a header bar. Below the header, there is a text description: 'This WLAN Client Table shows client MAC address associate to this Broadband Router'. The table has seven columns: 'Interface', 'MAC Address', 'Rx', 'Tx', 'Signal(%)', 'Connected Time', and 'Idle Time'. There is one data row for the interface 'EnGenius59FE80'. Below the table is a 'Refresh' button.

Interface	MAC Address	Rx	Tx	Signal(%)	Connected Time	Idle Time
EnGenius59FE80	00:02:6F:52:7F:40	0 Bytes	1.2 KBytes	100	12 secs	5 secs



### 3.2.3.8. WMM

WMM technology maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>

Reset to Default

Apply

Cancel

## 3.3. Network

### 3.3.1. Status

View the current internet connection status and related information.

#### LAN Settings

IP Address 192.168.1.1  
Subnet Mask 255.255.255.0  
MAC Address 00:02:6F:59:FE:DB

## 3.3.2. LAN

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.

<b>Bridge Type :</b>	Static IP ▾
<b>IP Address :</b>	192.168.1.1
<b>IP Subnet Mask :</b>	255.255.255.0
<b>Default Gateway :</b>	
<b>802.1d Spanning Tree :</b>	Enabled ▾

- **Bridge Type:** Select Static IP or Dynamic IP from the drop-down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server.
- **IP Address:** Specify an IP address.
- **IP Subnet Mask:** Specify a subnet mask for the IP address.
- **802.1d Spanning Tree:** Select Enable or Disable from the drop-down list. Enabling spanning tree will avoid redundant data loops.

## 3.4. Management

### 3.4.1. Admin

Change current login password of the device. It is recommended to change the default password for security reasons.

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

<b>Old Password :</b>	<input type="text"/>
<b>New Password :</b>	<input type="text"/>
<b>Repeat New Password :</b>	<input type="text"/>
<b>Idle Timeout :</b>	<input type="text" value="10"/> (1~10 minutes)

### 3.4.2. SNMP

Allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

<b>SNMP Active</b>	Enabled ▾
<b>SNMP Version</b>	All ▾
<b>Read Community</b>	public
<b>Set Community</b>	private
<b>System Location</b>	EnGenius Technologies, Inc.
<b>System Contact</b>	SENAO Networks, Inc.
<b>Trap Active</b>	Enabled ▾
<b>Trap Manager IP</b>	192.168.1.100
<b>Trap Community</b>	public

- **SNMP Active:** Choose to **enable** or **disable** the SNMP feature.
- **SNMP Version:** You may select a specific version or select **All** from the drop-down list.
- **Read Community Name:** Specify the password for access the SNMP community for read only access.
- **Set Community Name:** Specify the password for access to the SNMP community with read/write access.

- **System Location:** Specify the location of the device.
- **System Contact:** Specify the contact details of the device.
- **Trap Active:** Choose to **enable** or **disable** the SNMP trapping feature. .
- **Trap Manager IP:** Specify the password for the SNMP trap community.
- **Trap Community:** Specify the name of SNMP trap community.

### 3.4.3. Firmware

Allows you to upgrade the firmware of the device in order to improve the functionality and performance.

You can upgrade the firmware of the device 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.



Ensure that you have downloaded the appropriate firmware from the vendor's website.

Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded with wireless interface.

### 3.4.4. Configure

This allows you to restore to factory default setting or backup/restore your current setting.

The current system settings can be saved as a file onto the local hard drive. The saved file can be loaded back on the Broadband Router. To reload a system settings file, click on BROWSE to locate the system file to be used. You may also reset the Broad Router back to factory default settings by clicking RESET

<b>Restore To Factory Default :</b>	<input type="button" value="Reset"/>
<b>Backup Settings :</b>	<input type="button" value="Save"/>
<b>Restore Settings :</b>	<input style="width: 150px; height: 20px;" type="text"/> <input type="button" value="瀏覽..."/>
	<input type="button" value="Upload"/>

### 3.4.5. Reset

This will only reset you devices with current configuration unaffected.

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.

Apply Cancel

## 3.5. Tools

### 3.5.1. Time Setting

This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.



If the device loses power for any reason, it will not be able to keep its clock running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.

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 :**

**Daylight Saving :**

Enable  
From   To

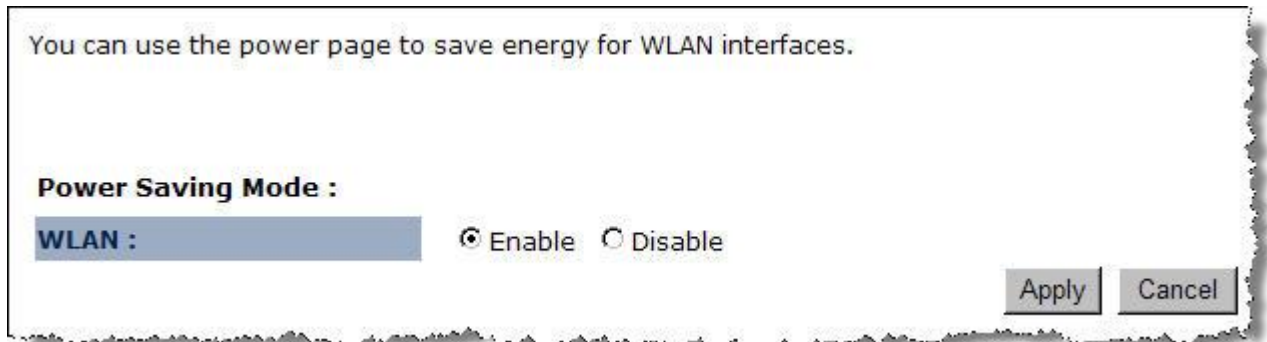
Apply Reset

- **Time Zone:** Select time zone.

- **NTP Time Server:** Specify the NTP server's IP address for time synchronization.
- **Daylight Saving:** To enable daylight savings time.

## 3.5.2. Power Saving

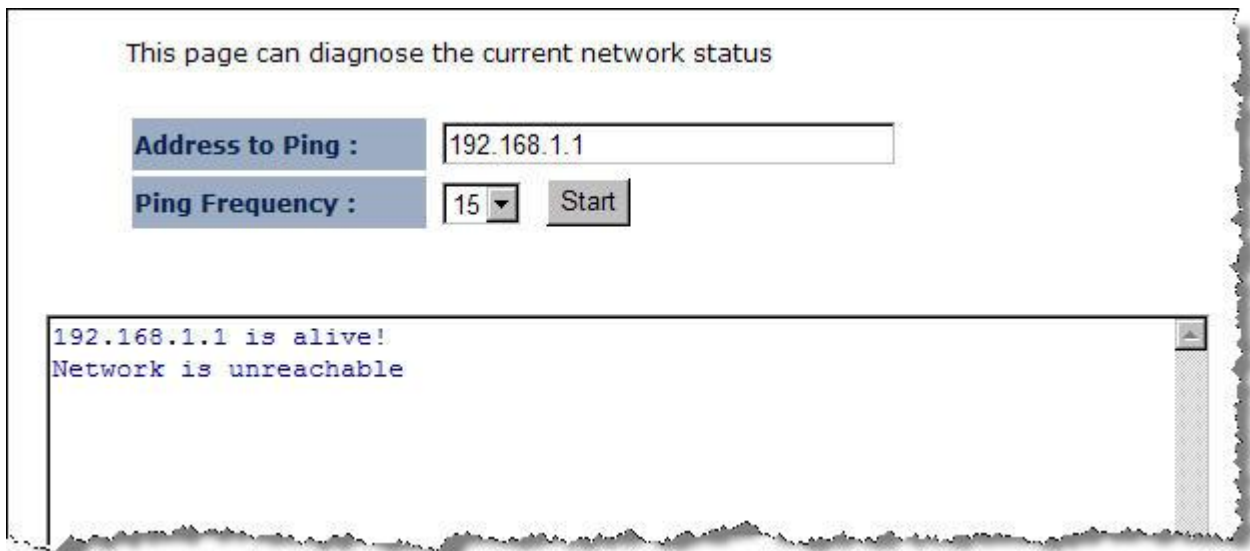
DDNS allows you to create a hostname that points to your dynamic IP or static IP address or URL. The device allows you redirecting the traffic to a specific DDNS provider for dynamic domain name routing.



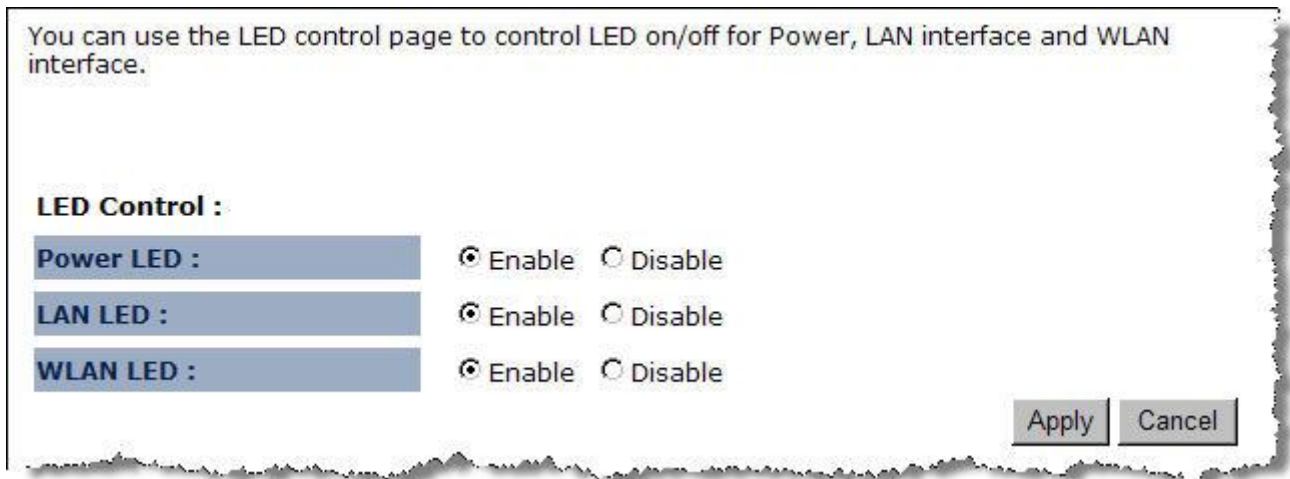
- **Dynamic DNS:** To enable/disable the DDNS service
- **Server Address:** List of DDNS Service providers
  - ✓ 3322
  - ✓ DHS
  - ✓ DynDNS
  - ✓ ZoneEdit
  - ✓ CyberGate
- **Host Name:** Host name to be redirected
- **Username:** User name for DDNS Service providers
- **Password:** Password for DDNS Service providers

## 3.5.3. Diagnosis

Check whether a network destination is reachable with ping service.



### 3.5.4. LED Control



### 3.6. Logout

# Appendix A – SPECIFICATIONS

Frequency Band	2.400~2.484 GHz
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation Technology	- OFDM: BPSK, QPSK, 16-QAM, 64-QAM - DBPSK, DQPSK, CCK
Operating Channels	11 for North America, 14 for Japan, 13 for Europe
Receive Sensitivity (Typical)	- IEEE802.11n MCS8 @ -90dBm MCS15 @ -70dBm - IEEE802.11g 6Mbps@ -92dBm 54Mbps@ -72dBm - IEEE802.11b 1Mbps@ -93dBm 11Mbps@ -89dBm
Available transmit power	- IEEE802.11n/g 18dBm@6~9 Mbps / MCS9 16dBm@12~18 Mbps / MCS11 14dBm@24~36 Mbps / MCS13 13dBm@48~54 Mbps / MCS15 - IEEE802.11b 17.5dBm@1, 11Mbps
Antenna *3	Directional internal antenna TNC type; Peak Gain = 5dBi



# Appendix B – 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 C – 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.