EnGenius EAP9550

11N Multi-Function AP/Repeater

Table of Content

1. Introduction 4
   - 1.1. Features and Benefits 4
   - 1.2. Package Contents 5
   - 1.3. System Requirement 5
2. Understanding the Hardware 6
   - 2.1. Hardware Installation 6
3. Modes 7
   - 3.1. Access Point 7
   - 3.2. WDS Bridge 7
   - 3.3. Universal Repeater 7
4. Web Configuration 8
   - 4.1. System 8
     - 4.1.1. Operation Mode 8
     - 4.1.2. Status 8
     - 4.1.3. DHCP 9
     - 4.1.4. Schedule 10
     - 4.1.5. Event Log 10
     - 4.1.6. Monitor 10
   - 4.2. Wireless 12
     - 4.2.1. AP 12
     - 4.2.2. WDS Bridge 22
     - 4.2.3. Universal Repeater (AP) 28
   - 4.3. Network 37
     - 4.3.1. Status 37
     - 4.3.2. LAN 37
   - 4.4. Management 39
     - 4.4.1. Admin 39
     - 4.4.2. SNMP 39
     - 4.4.3. UPnP 40
     - 4.4.4. Firmware 41
     - 4.4.5. Configure 41
     - 4.4.6. Reset 41
   - 4.5. Tools 42
     - 4.5.1. Time Setting 42
     - 4.5.2. Power Saving 43
     - 4.5.3. Diagnosis 43
     - 4.5.4. LED Control 44

4.6. Logout.....44
Appendix A – FCC Interference Statement.....45
Appendix B – IC Interference Statement.....46

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**
QoS (WMM) support	**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 EAP9550**
- **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.

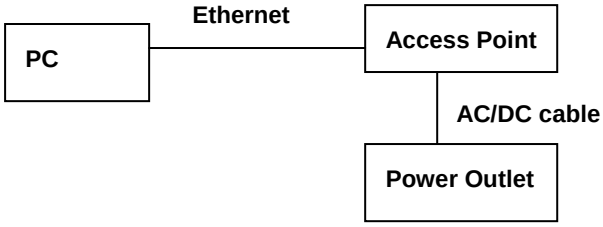
- **PC/AT compatible computer with an Ethernet interface.**
- **Operating system that supports HTTP web-browser**

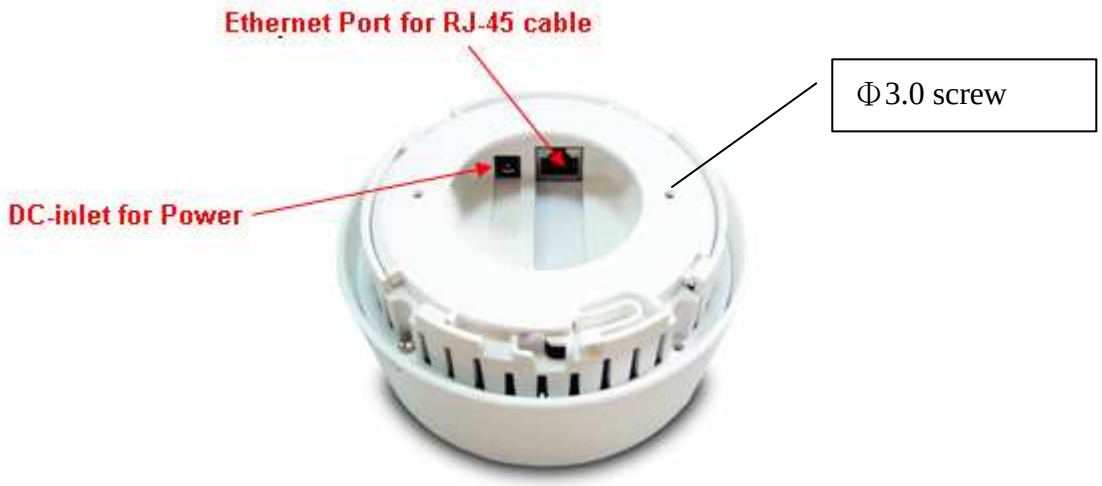
2. Understanding the Hardware

2.1. Hardware Installation

1 Place the unit in an appropriate place after conducting a site survey.
2 Plug one end of the Ethernet cable into the RJ-45 port on the rear panel of the device and another end into your PC/Notebook.
3 Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.
4 Regarding wall mount please use Φ3.0 screw for fixing.

This diagram depicts the hardware configuration





Reset Button
2~10 sec Reboot
Over 10 sec Reset to Default

3. Modes

AP/WDS/Universal Repeater

3.1. 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.

3.2. WDS Bridge

 **You can only connect to the device via Ethernet Port**

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.

3.3. 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 AP channel.

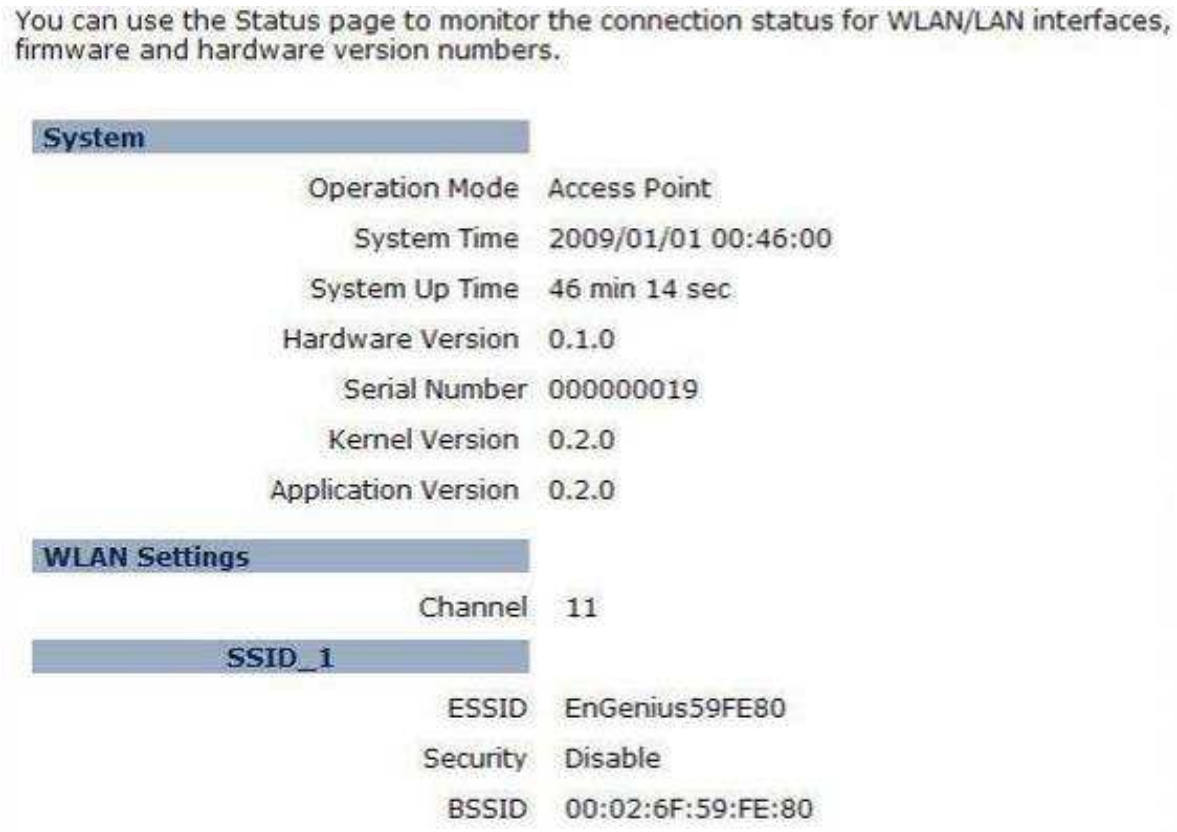
4. Web Configuration

4.1. System

4.1.1. Operation Mode

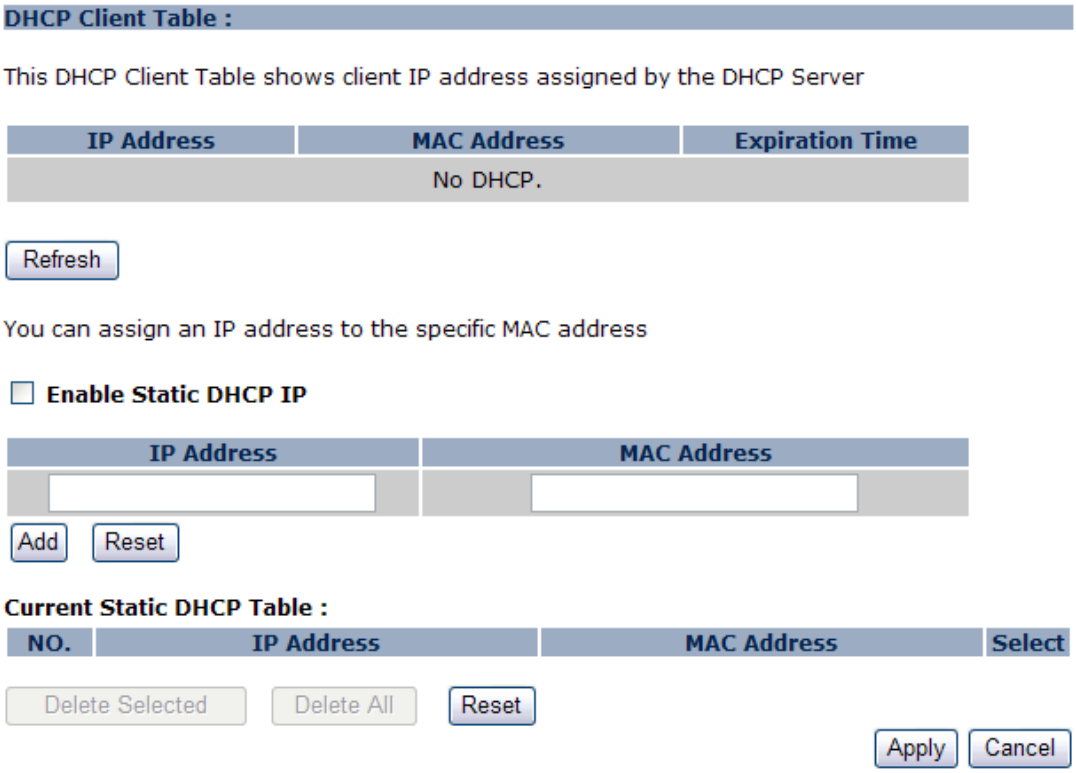
You are allowed to configure EAP9550 into different modes: AP, WDS Bridge and Universal Repeater.
Please refer to Chapter 2: Modes for operation under different modes.

4.1.2. Status

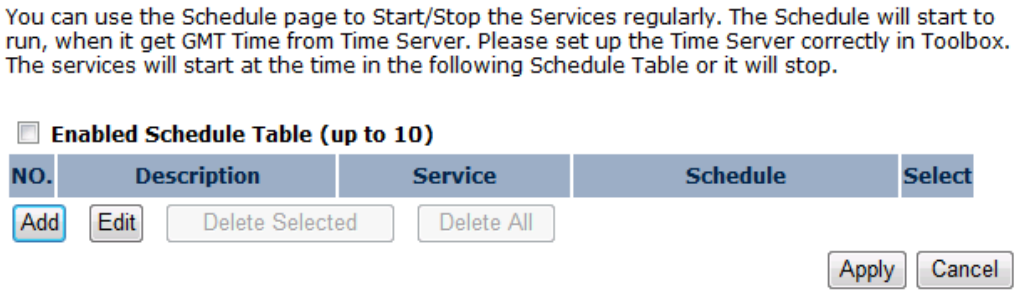


- **System: Basic information of the device.**
- **WLAN Settings: WLAN channel.**
- **SSID_1: SSID information.**

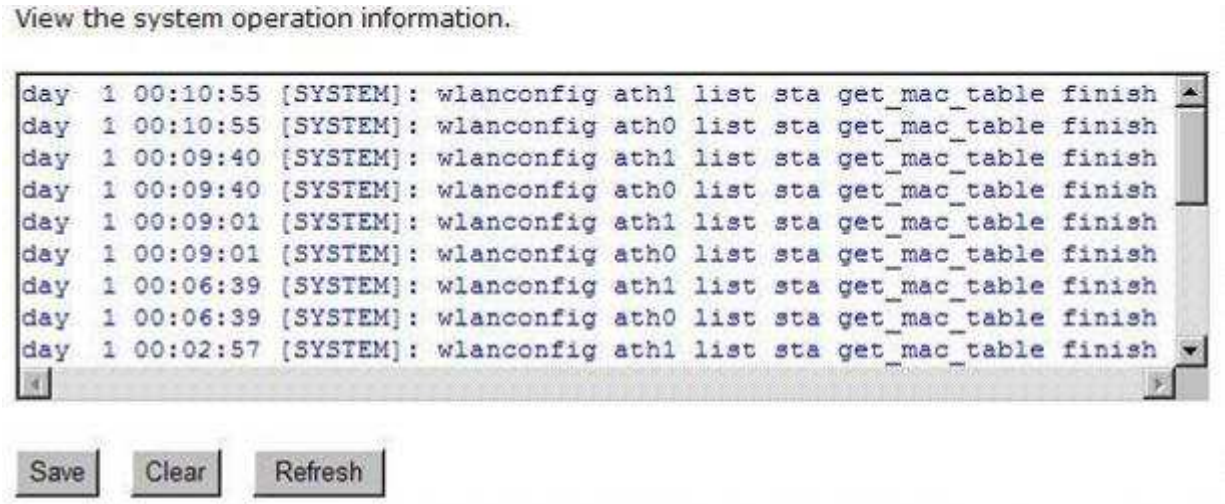
4.1.3. DHCP



4.1.4. Schedule



4.1.5. Event Log

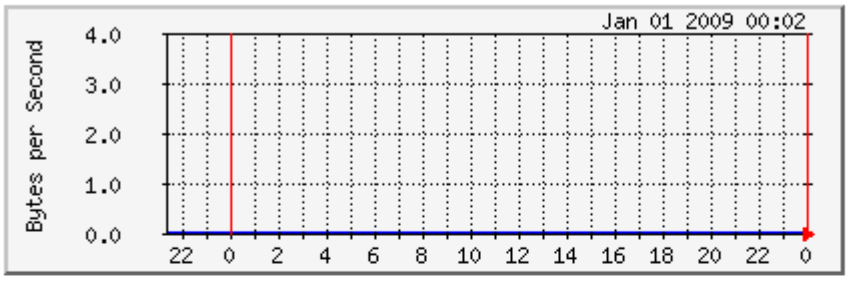


4.1.6. Monitor

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

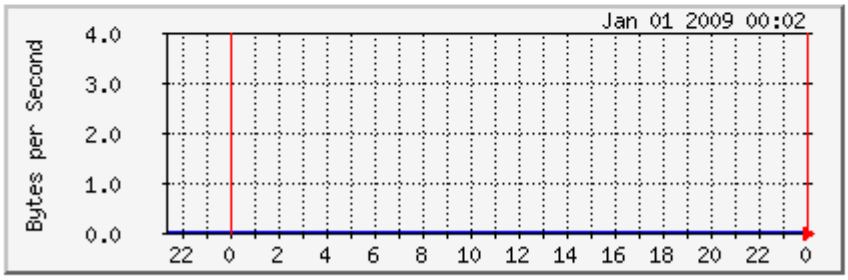
Ethernet Daily Graph (5 Minute Average)

Detail



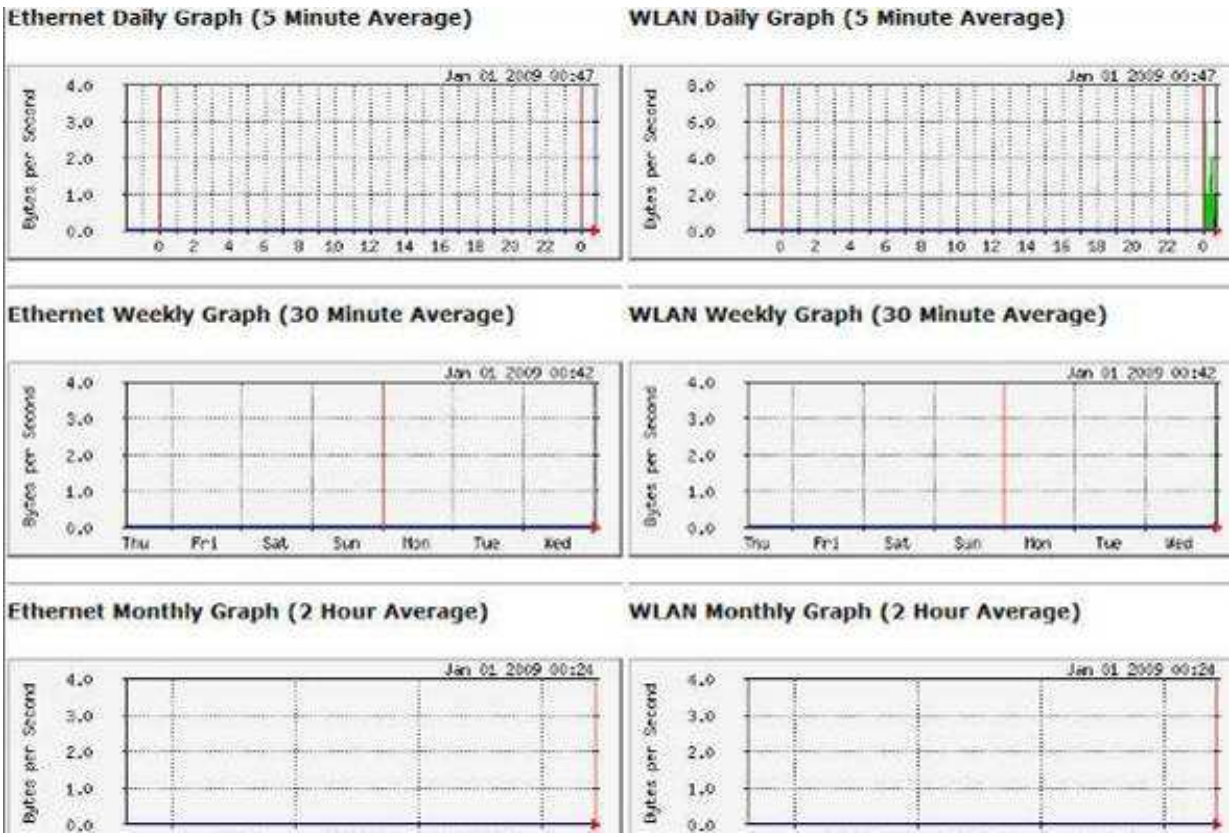
	Maximum	Average	Current
RX	0 B/sec	0 B/sec	0 B/sec
TX	0 B/sec	0 B/sec	0 B/sec

WLAN Daily Graph (5 Minute Average)



	Maximum	Average	Current
RX	0 B/sec	0 B/sec	0 B/sec
TX	0 B/sec	0 B/sec	0 B/sec

- **Detail: Click into detail to see historical record.**



4.2. Wireless

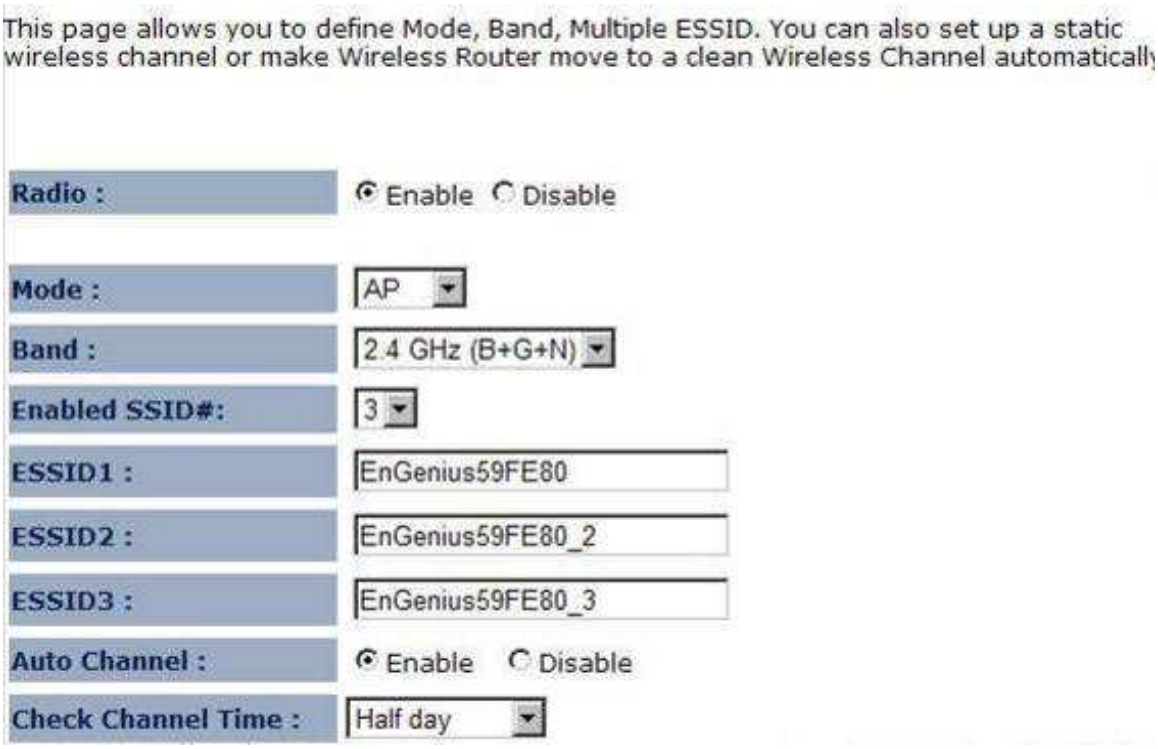
4.2.1. AP

4.2.1.1. Status

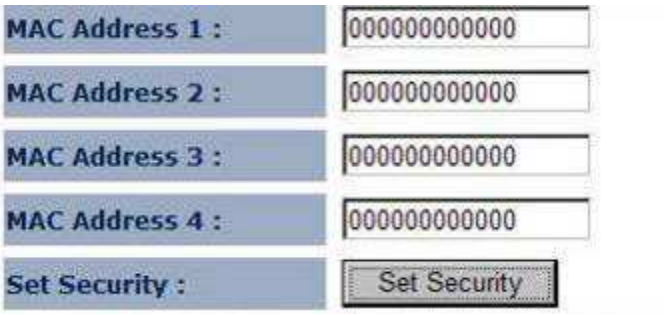
View the current internet connection status and related information.

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

4.2.1.2. Basic



- **Radio: To enable/disable wireless signal.**
- **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)**



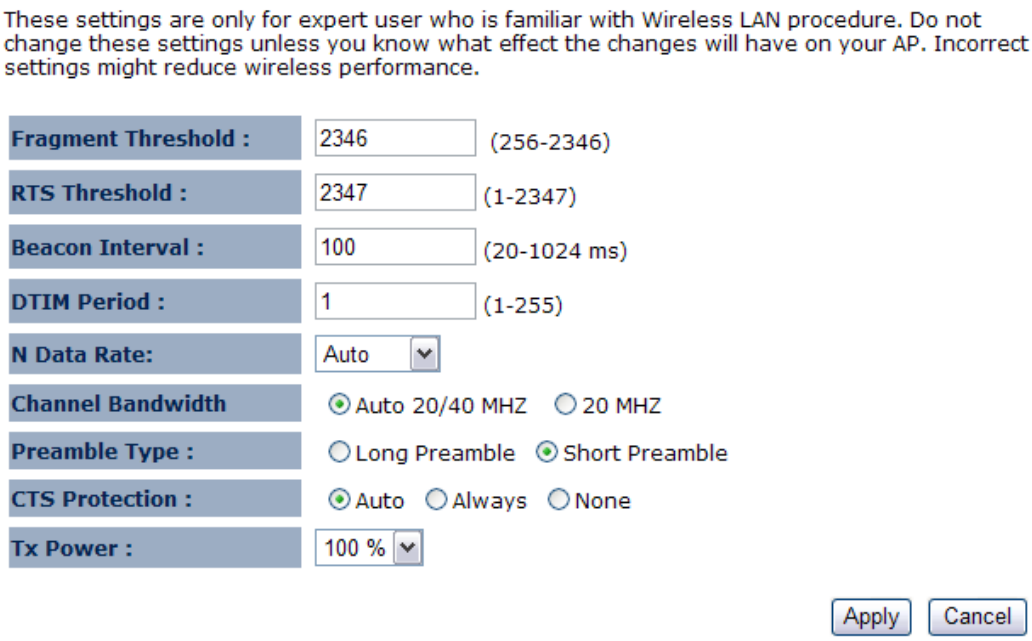
  - ✓ **AP**
  - ✓ **WDS**
- **Band: Configure the device into different wireless modes.**
  - ✓ **2.4 GHz (B)**
  - ✓ **2.4 GHz (N)**
  - ✓ **2.4 GHz (B+G)**
  - ✓ **2.4 GHz (G)**
  - ✓ **2.4 GHz (B+G+N)**
- **Enabled SSID#: The device allows you to add up to 4 unique SSID**
- **ESSID#: Description of each configured SSID**

- **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**

4.2.1.3. Advanced

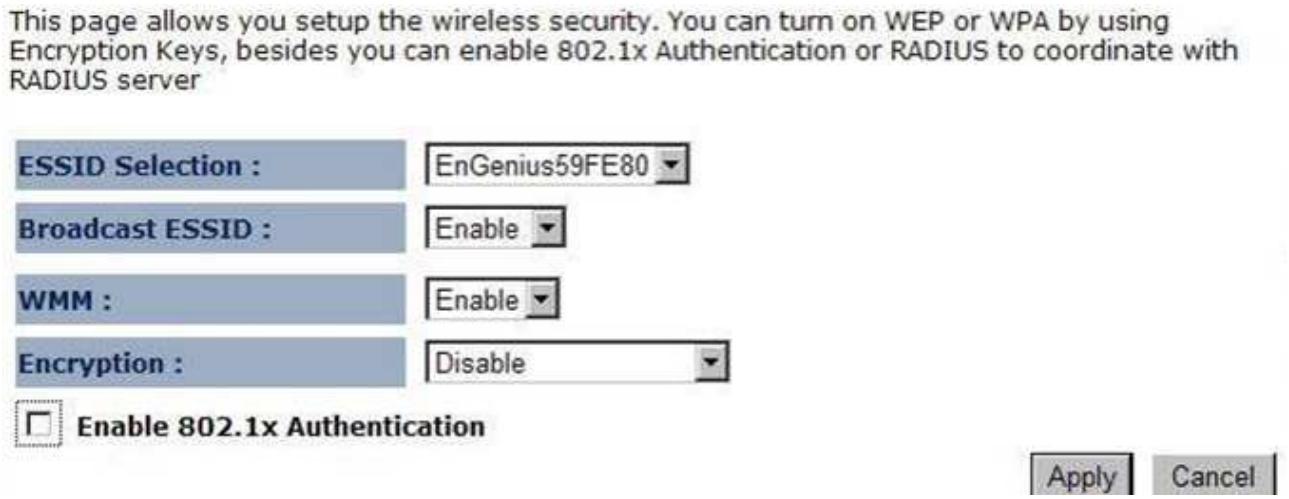


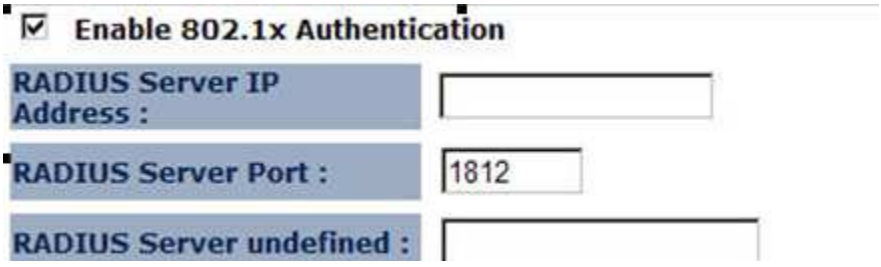
- **Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.**
- **RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in 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 255.**

- **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 (Auto 20/40MHz or 20MHz)**
- **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.**

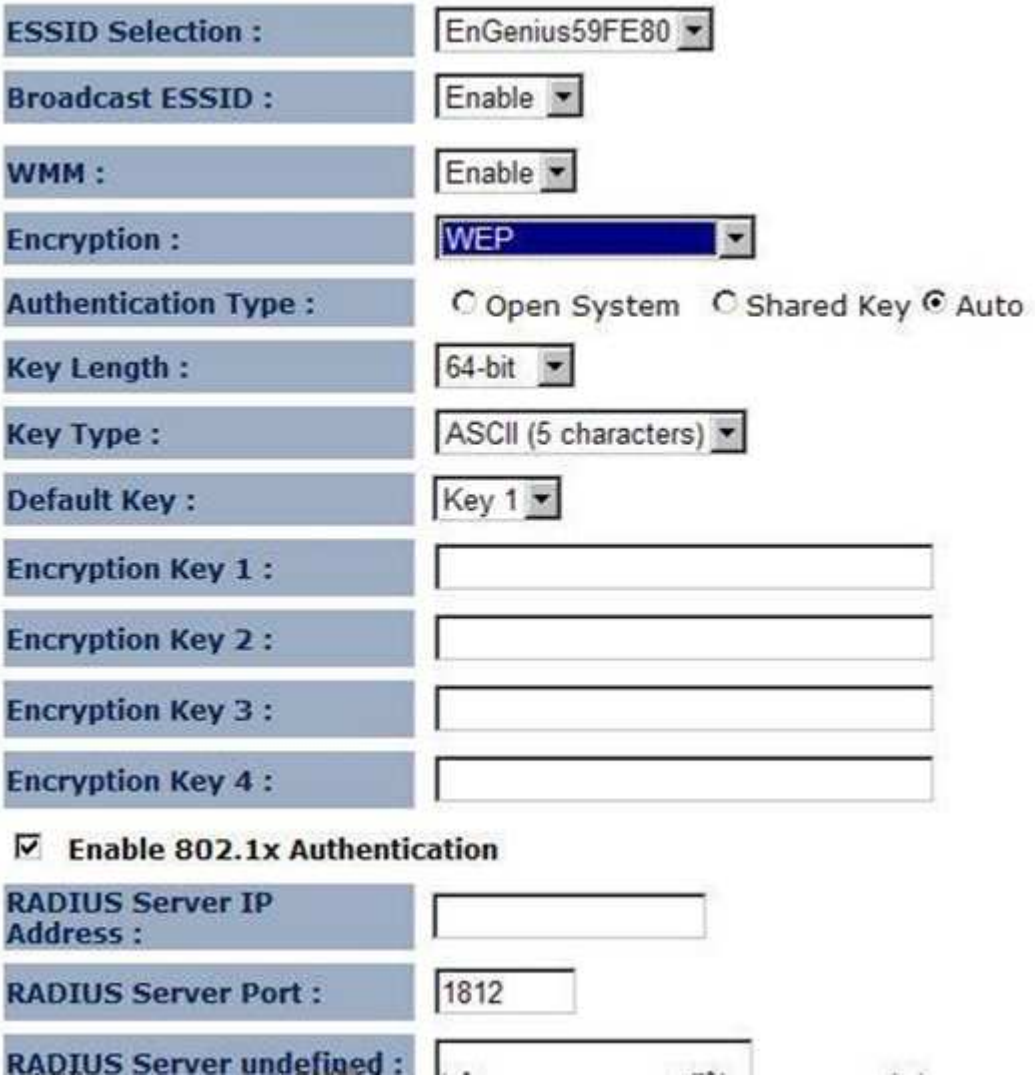
4.2.1.4. Security

➢ Encryption: Disabled





➢ Encryption: WEP

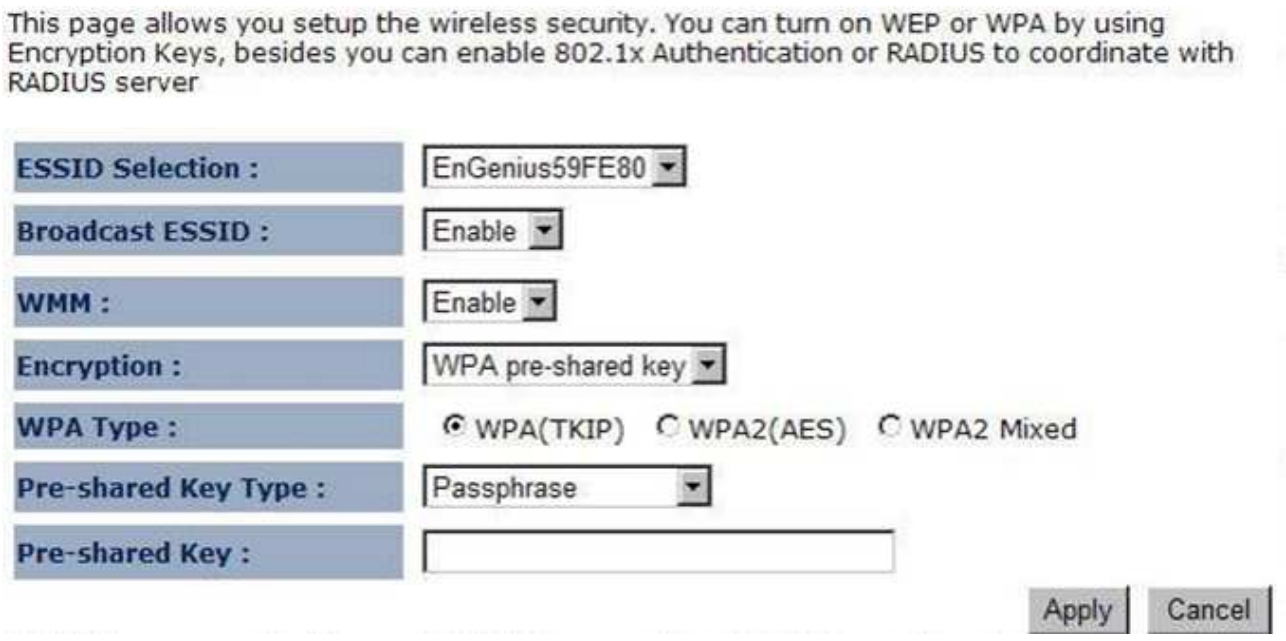


- **ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.**
- **Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option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

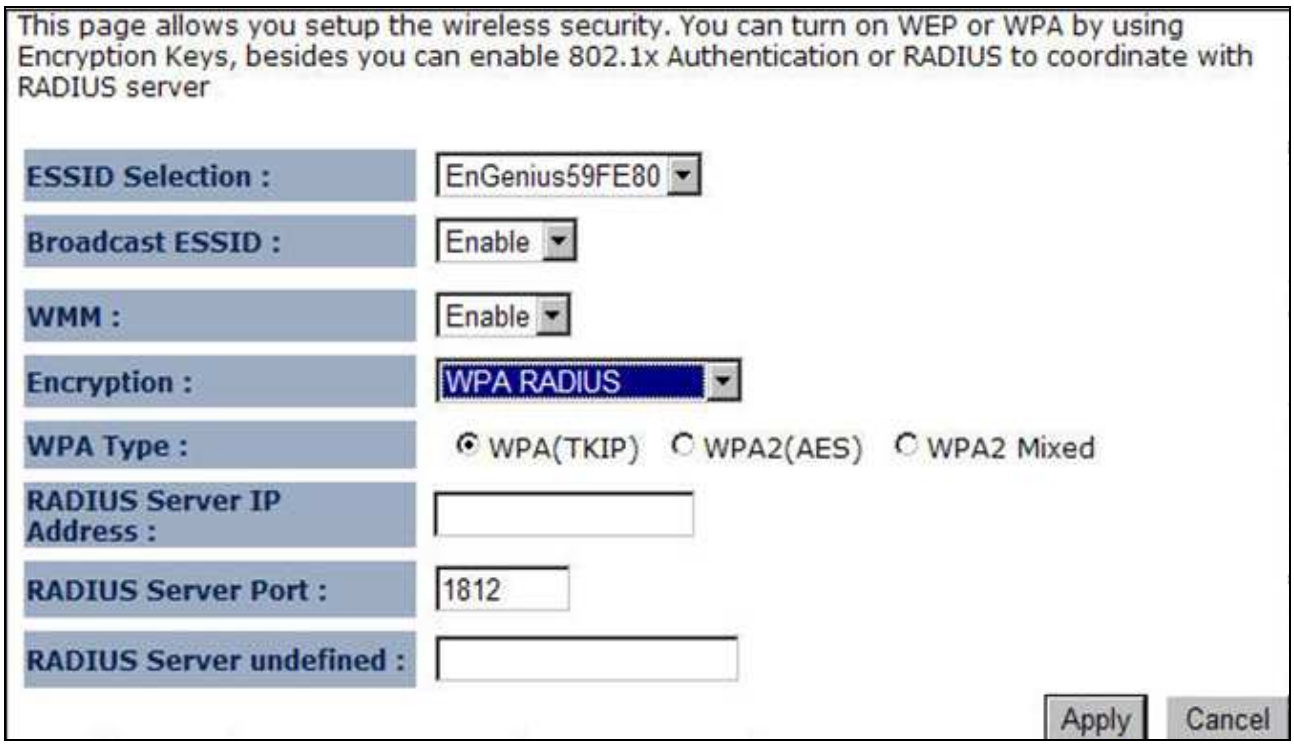
➢ Encryption: WPA pre-shared key



- **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.**

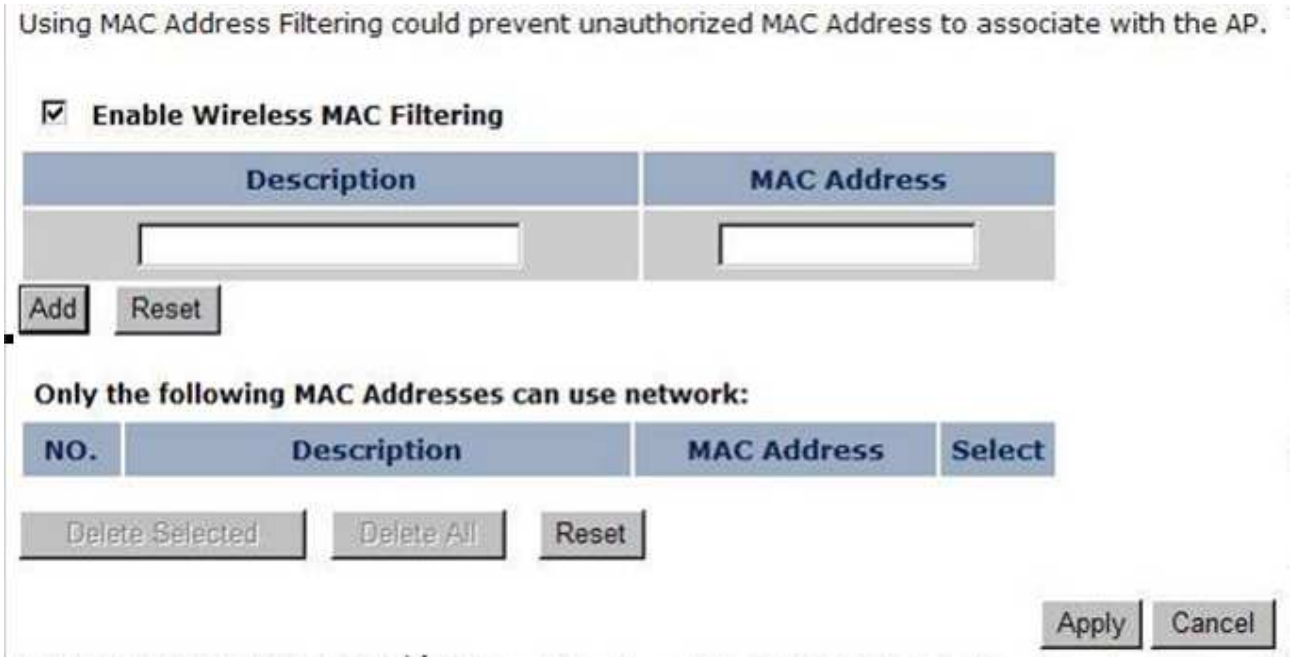
- **Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option is set to Enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When 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

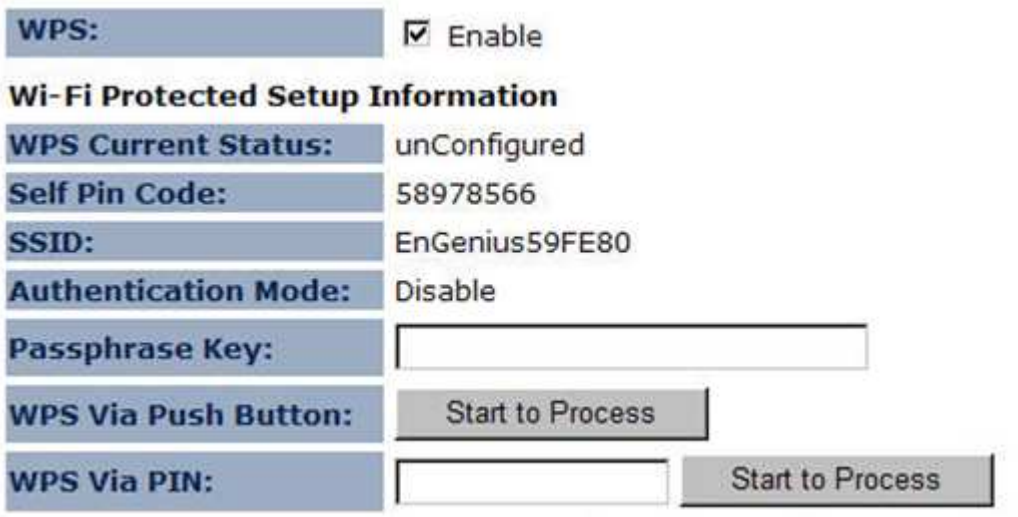


- **ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.**
- **Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option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

4.2.1.5. Filter



4.2.1.6. WPS

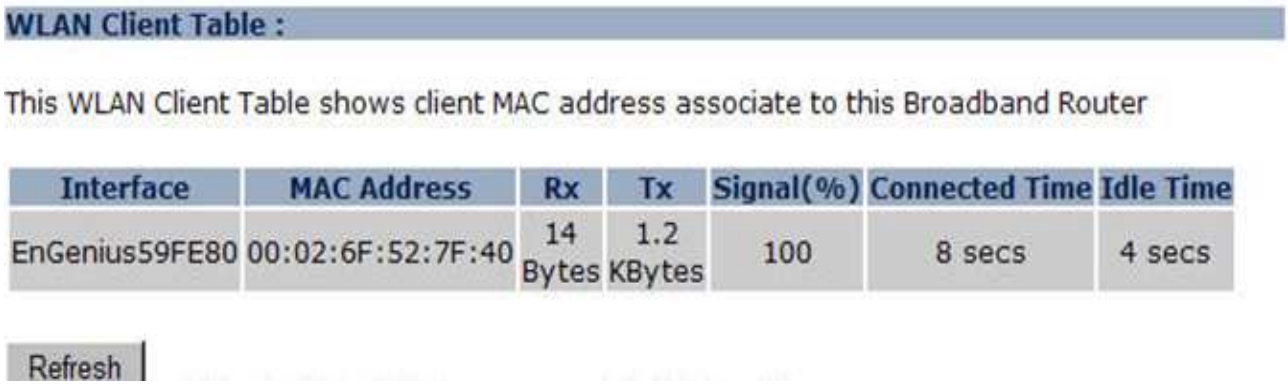


- **WPS**: Place a check in this box to enable this feature.
- **WPS Current Status:** Displays the current status of the WPS configuration.
- **Self Pin Code:** Displays the current PIN.
- **SSID:** Displays the current SSID.
- **Authentication Mode:** Displays the current authentication mode.
- **Passphrase Key:** Displays the current passphrase.
- **WPS Via Push Button:** Click on the **Start to Process** button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click on the **OK** button in the dialog box.
- **WPS via PIN:** Specify a PIN, which unique number that can be used to add the router to an existing network or to create a new network. Then click on the **Start to Process** button.

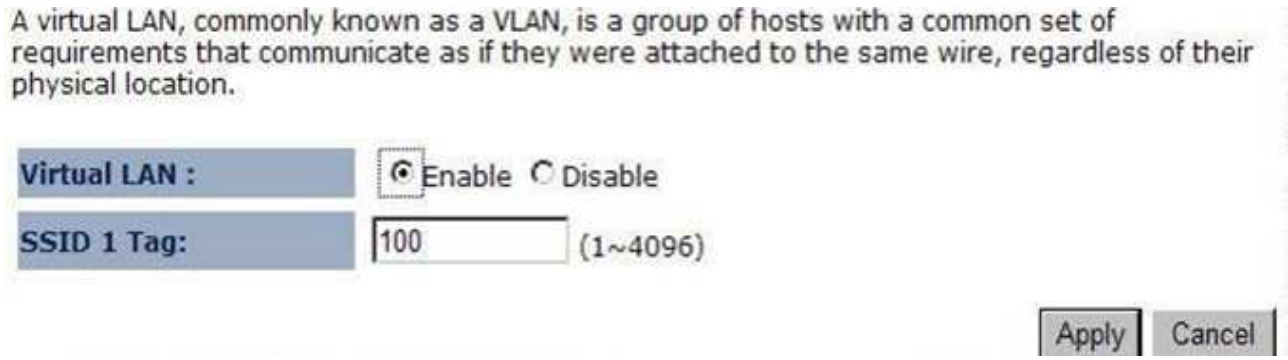
4.2.1.7. Client List

Click on the **Client List** link under the **Wireless** drop-down menu. This page displays the list of Clients that are associated to the Access Point.

The MAC address and signal strength for each client is displayed. Click on the Refresh button to **Refresh** the client list



4.2.1.8. VLAN



Only Available in AP mode

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

4.2.1.9. 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	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

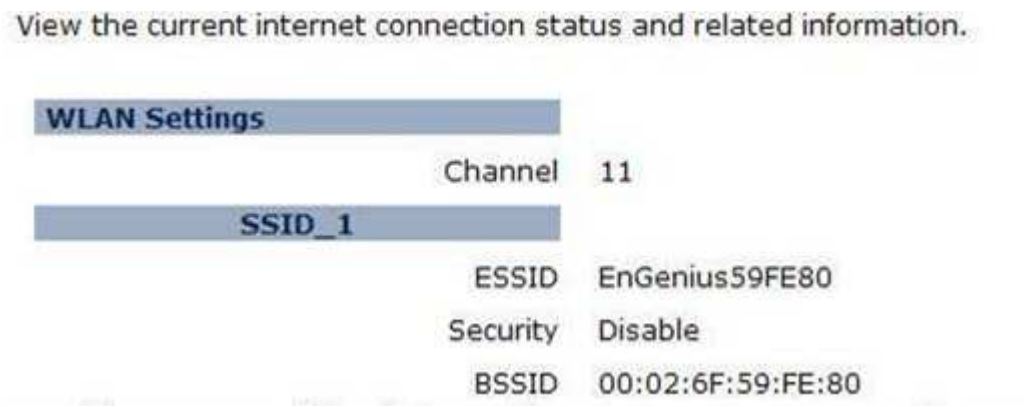
Reset to Default

Apply Cancel

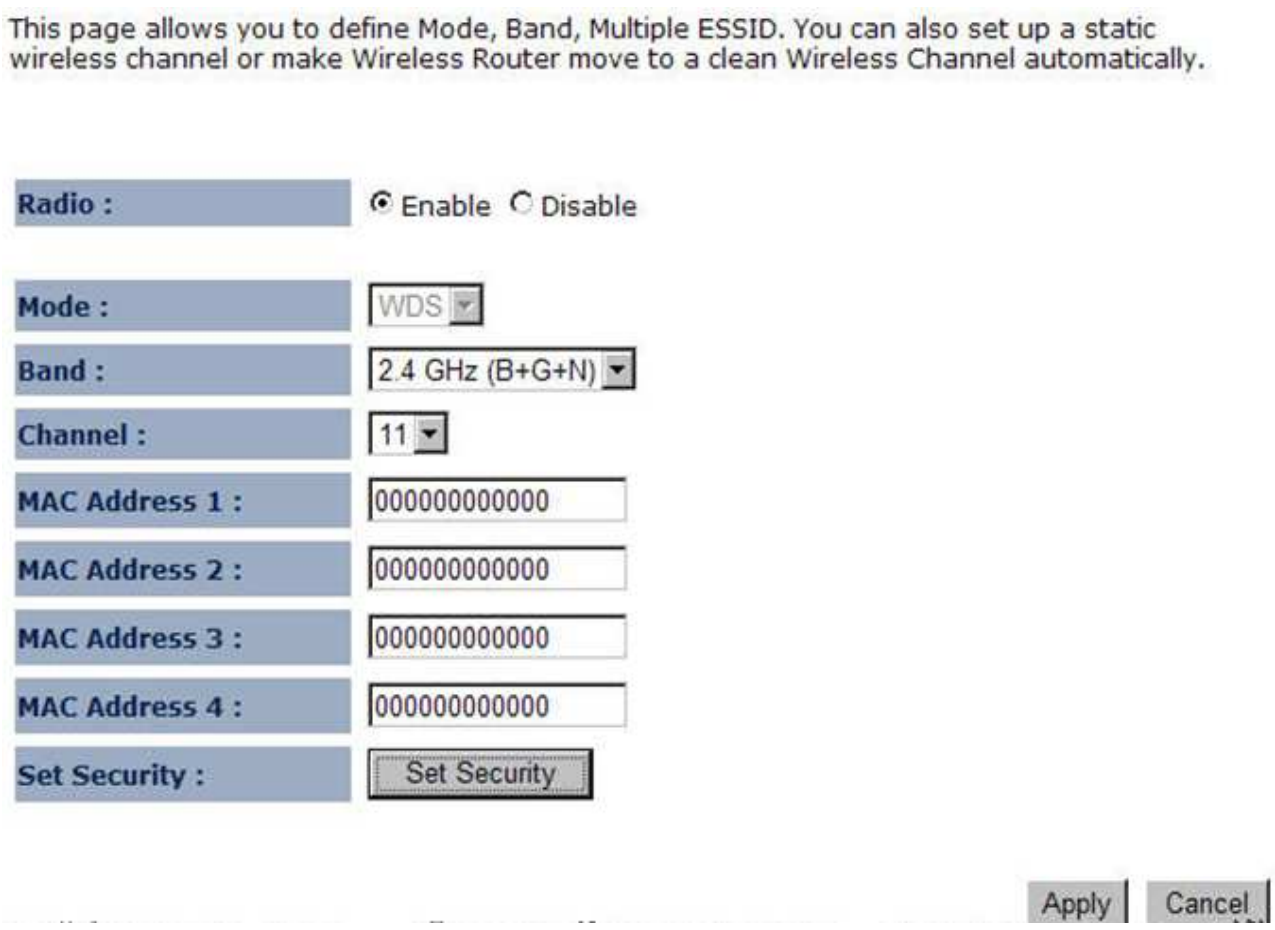
4.2.2. WDS Bridge

You can only connect to the device via Ethernet Port

4.2.2.1. Status



4.2.2.2. Basic



- **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)**

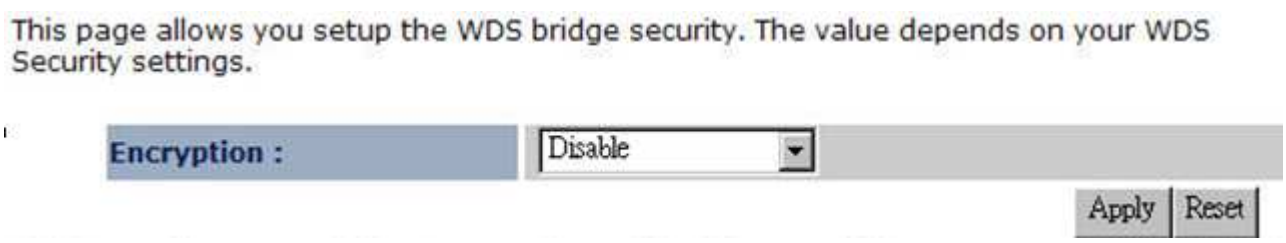
- ✓ 2.4 GHz (N)
- ✓ 2.4 GHz (B+G)
- ✓ 2.4 GHz (G)
- ✓ 2.4 GHz (B+G+N)

- **Channel: You can manually configure a channel to be used.**
- **MAC Address 1~4: To specify MAC address of other AP devices.**

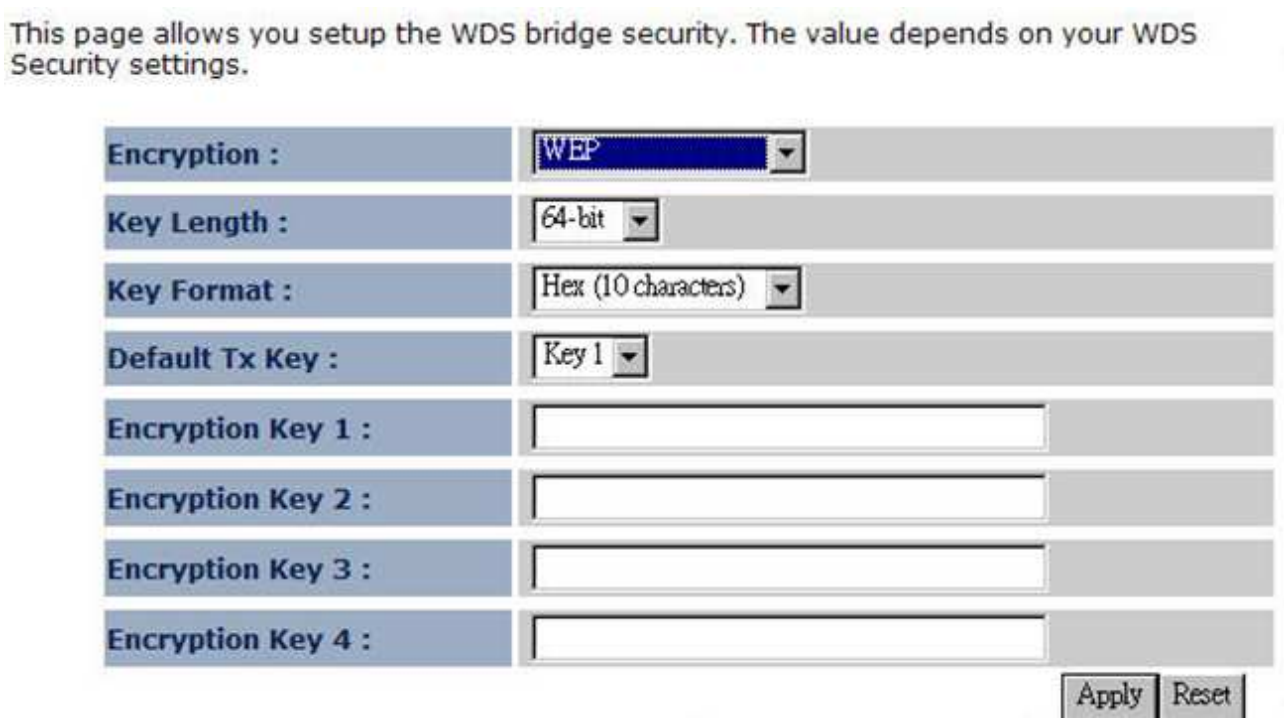
MAC address will only shows when configured in WDS mode.

- **Security: Please refer to 4.2.1.4 for encryption configuration**

➢ Security: Disabled



➢ Security: WEP

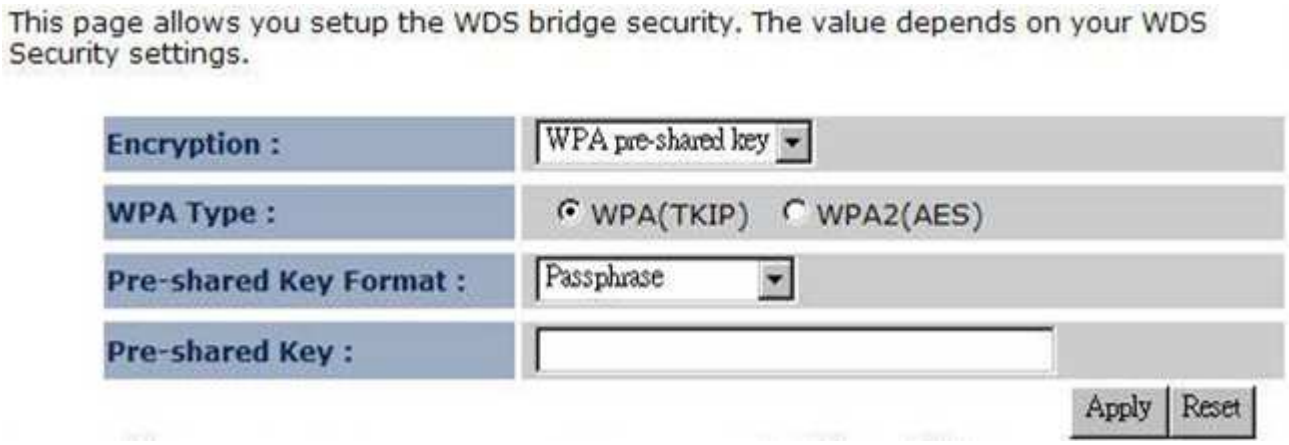


- **Key Length: Select a 64-bit or 128-bit WEP key length from the drop-down list.**
- **Key Format: Select a key type from the drop-down list. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or 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.

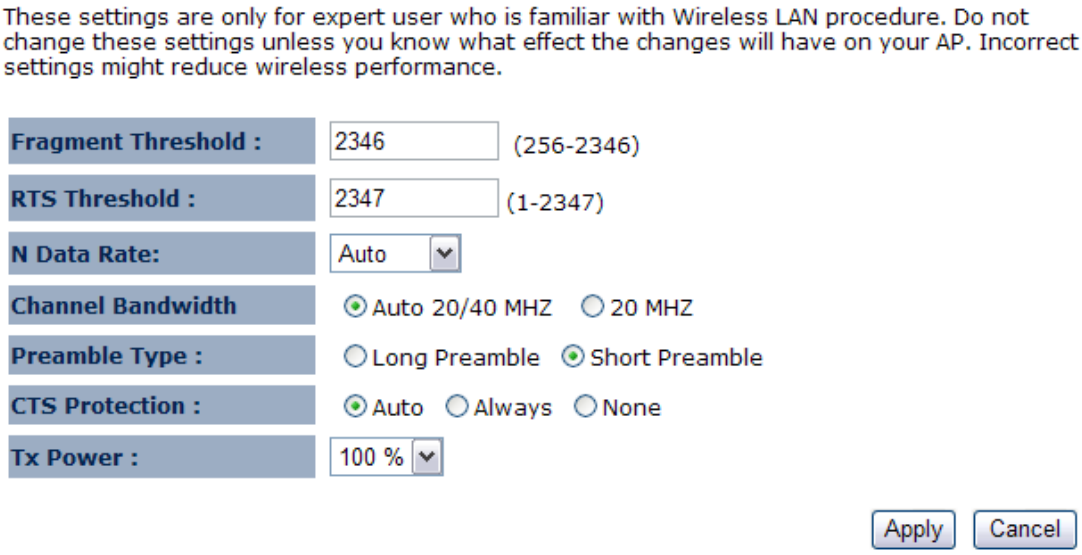
- **Default Tx Key: You may choose one of your 4 different WEP keys from below.**
- **Encryption Key 1-4: You may enter four different WEP keys.**

➢ Security: WPA pre-shared key



- **WPA Type: Select TKIP or AES. 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.**

4.2.2.3. Advanced



- **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.**
- **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. (Auto 20/40MHz or 20MHz)**
- **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.**

4.2.2.4. 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	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

Reset to Default

Apply Cancel

4.2.3. Universal Repeater (AP)

4.2.3.1. Status

View the current wireless connection status and related information.

WLAN Repeater Information	
Connection Status	Fail
ESSID	---
Security	---
BSSID	---
WLAN Settings	
Channel	6
SSID_1	
ESSID	EnGenius59FE80
Security	Disable
BSSID	00:02:6F:59:FE:80

4.2.3.2. 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.

Radio :	◉ Enable ○ Disable
Mode :	Universal Repeater
Band :	2.4 GHz (B+G+N)
Enabled SSID#:	1
ESSID1 :	EnGenius59FE80
Channel :	11
Site Survey :	Site Survey

Apply Cancel

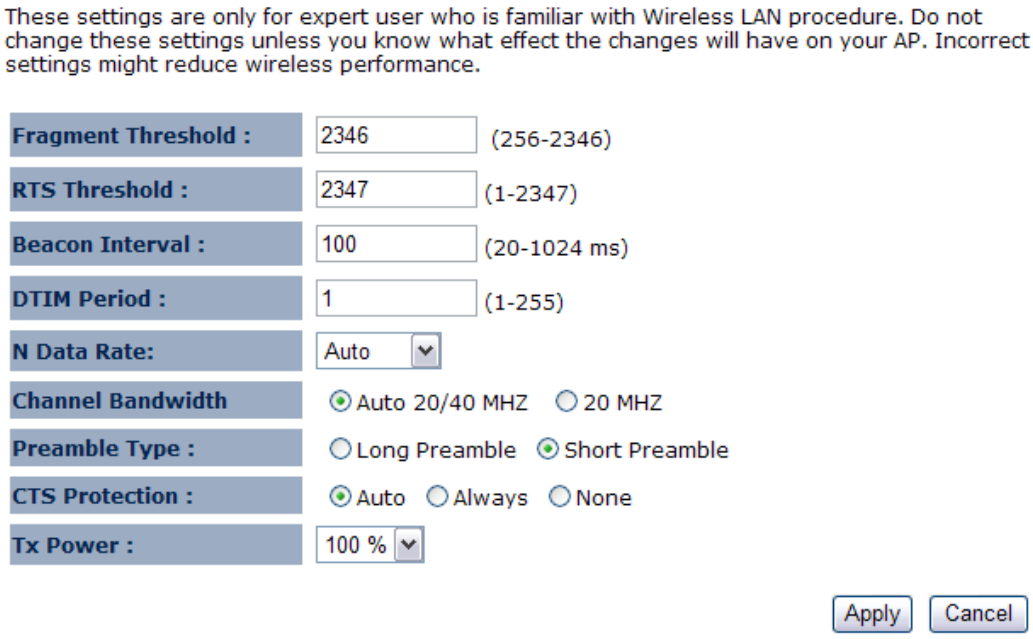
Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)
1	○	1	RD2DLINK	8E:FA:69:83:9B:88	WEP	AUTOWEP	24
2	○	1	SENAOVIP	00:02:6F:E0:02:12	NONE	OPEN	20
3	○	1	SENAOWL	00:02:6F:52:8C:D3	WEP	AUTOWEP	76
4	○	1	SENAOWL	00:02:6F:48:0D:87	WEP	AUTOWEP	65
5	○	1	SENAOWL	00:02:6F:48:0D:8B	WEP	AUTOWEP	10
6	○	1	EnGenius1	06:02:6F:E0:02:0D	NONE	OPEN	24
7	○	1	EnGenius1	00:02:6F:12:34:58	NONE	OPEN	34

- **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 have 1 unique SSID**
- **ESSID#: Description of each configured SSID**
- **Site Survey: List out all connected devices.**

4.2.3.3. Advanced

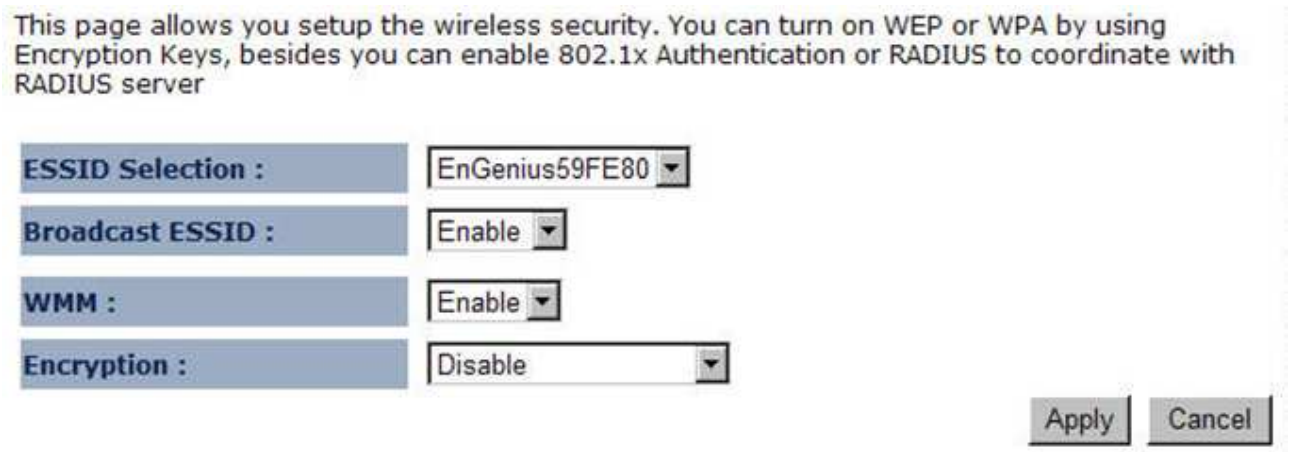


- **Fragment Threshold: Packets over the specified size will be fragmented in order to improve performance on noisy networks. Specify a value between 256 and 2346. The default value is 2346.**
- **RTS Threshold: Packets over the specified size will use the RTS/CTS mechanism to maintain performance in 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 0 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 255.**
- **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.**

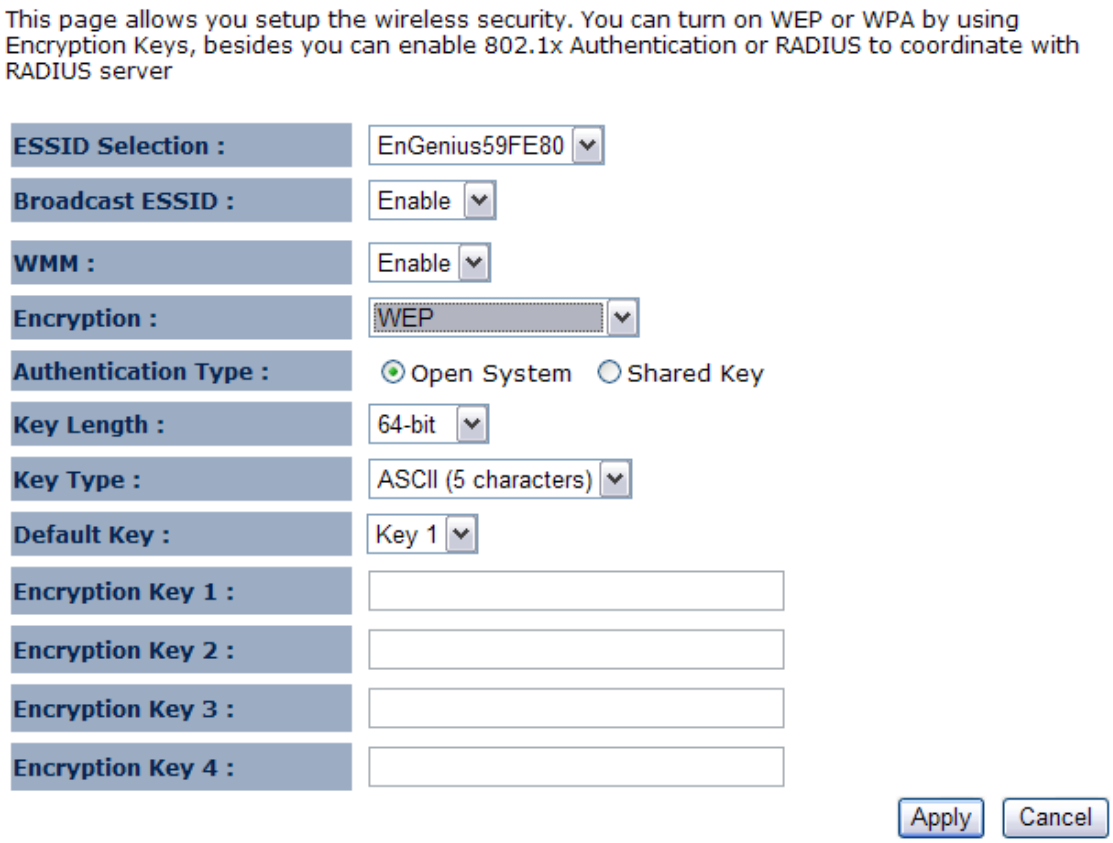
- **Preamble Type: Select a short or long preamble. For optimum performance it is recommended to also configure the client device as the same preamble type.**
- **CTS Protection: CTS (Clear to Send) can be always enabled, auto, or disabled. By enabled CTS, the Access Point and clients will wait for a 'clear' signal before transmitting. It is recommended to select auto.**

4.2.3.4. Security

➢ **Encryption: Disabled**



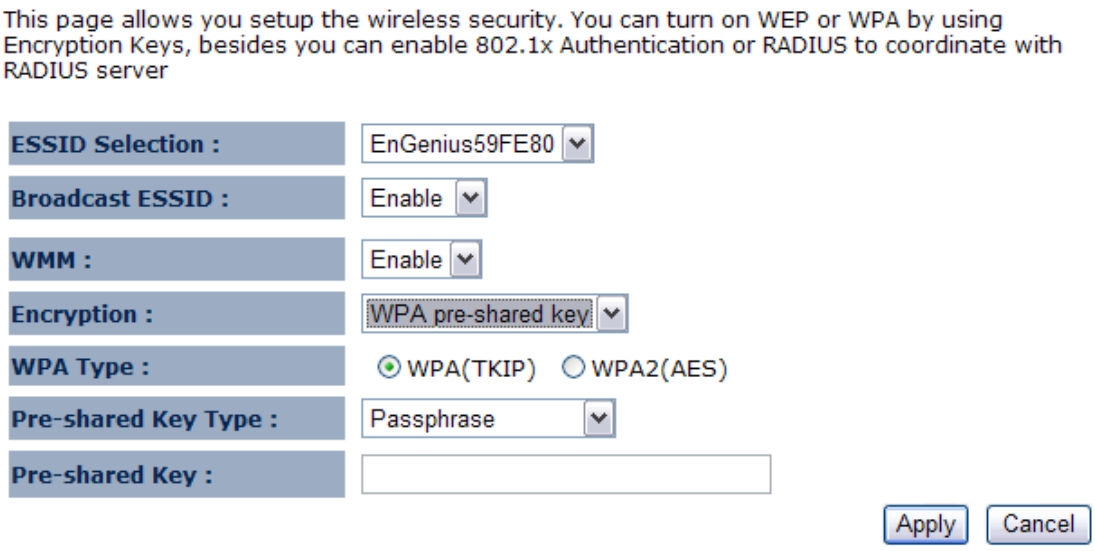
➢ **Encryption: WEP**



- **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 or Shared Key. 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

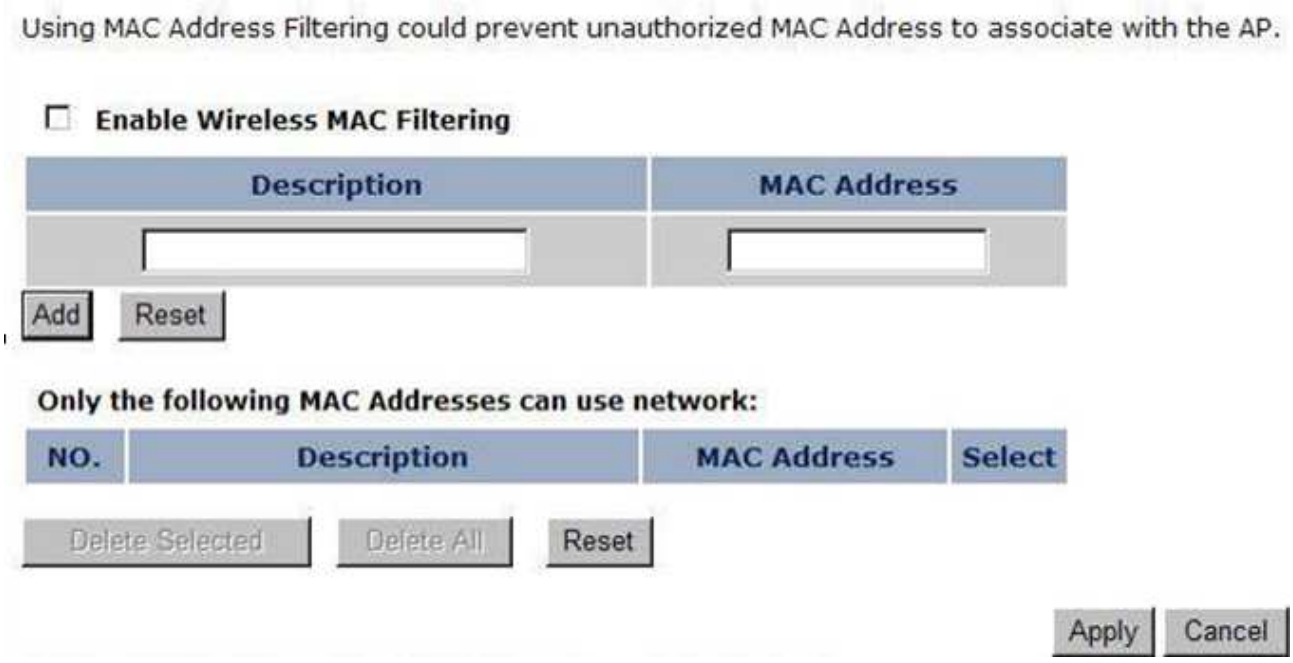


- **ESSID Selection: As this device supports multiple SSIDs, it is possible to configure a different security mode for each SSID (profile). Select an SSID from the drop-down list.**
- **Broadcast SSID: Select Enable or Disable from the drop-down list. This is the SSID broadcast feature. When this option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

4.2.3.5. Filter



4.2.3.6. WPS

- **WPS**: Place a check in this box to enable this feature.
- **WPS Current Status:** Displays the current status of the WPS configuration.
- **Self Pin Code:** Displays the current PIN.
- **SSID:** Displays the current SSID.
- **Authentication Mode:** Displays the current authentication mode.
- **Passphrase Key:** Displays the current passphrase.
- **WPS Via Push Button:** Click on the **Start to Process** button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click on the **OK** button in the dialog box.
- **WPS via PIN:** Specify a PIN, which unique number that can be used to add the router to an existing network or to create a new network. Then click on the **Start to Process** button.

4.2.3.7. Client List

Click on the **Client List** link under the **Wireless** drop-down menu. This page displays the list of Clients that are associated to the Access Point.

The MAC address and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list

WLAN Client Table :

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

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

Refresh

4.2.3.8. 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	3	15	63	0	☐	☐
AC_BK	7	15	1023	0	☐	☐
AC_VI	1	7	15	94	☐	☐
AC_VO	1	3	7	47	☐	☐

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	☐
AC_BK	7	15	1023	0	☐
AC_VI	2	7	15	94	☐
AC_VO	2	3	7	47	☐

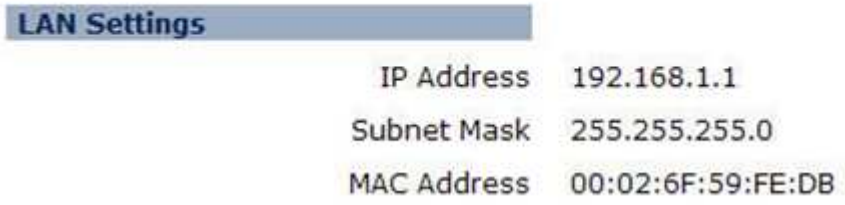
Reset to Default

Apply | Cancel

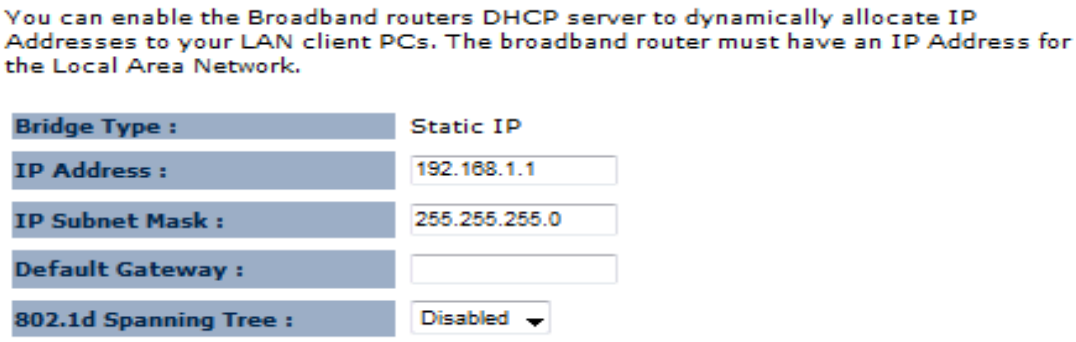
4.3. Network

4.3.1. Status

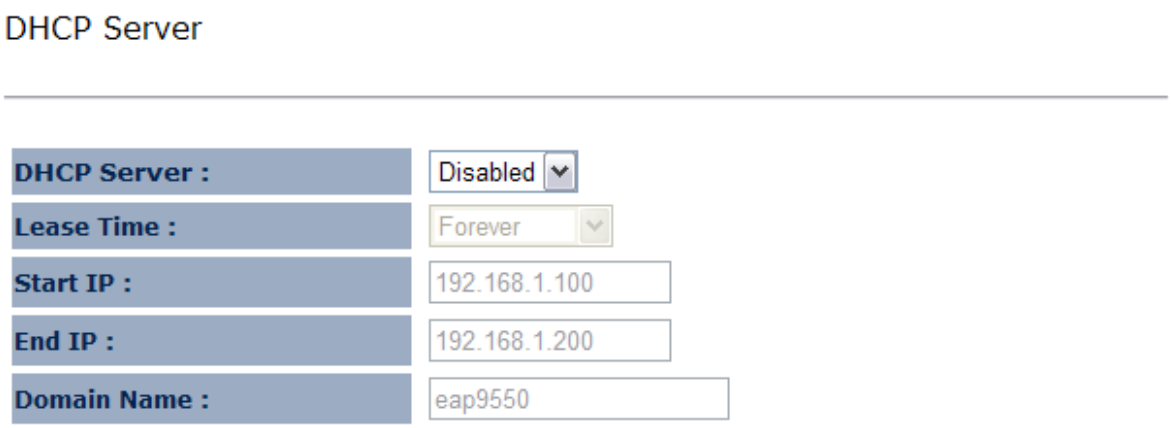
View the current internet connection status and related information.



4.3.2. LAN

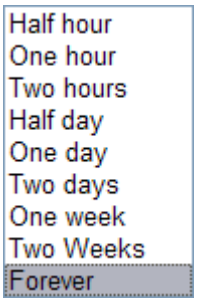


- **Bridge Type: Select Static IP or Dynamic IP from the drop-down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server.**
- **IP Address: Specify an IP address.**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



Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention.

- **DHCP server: Select Disabled or Enabled from drop-down list.**
- **Lease Time: From drop-down list user can set follows.**



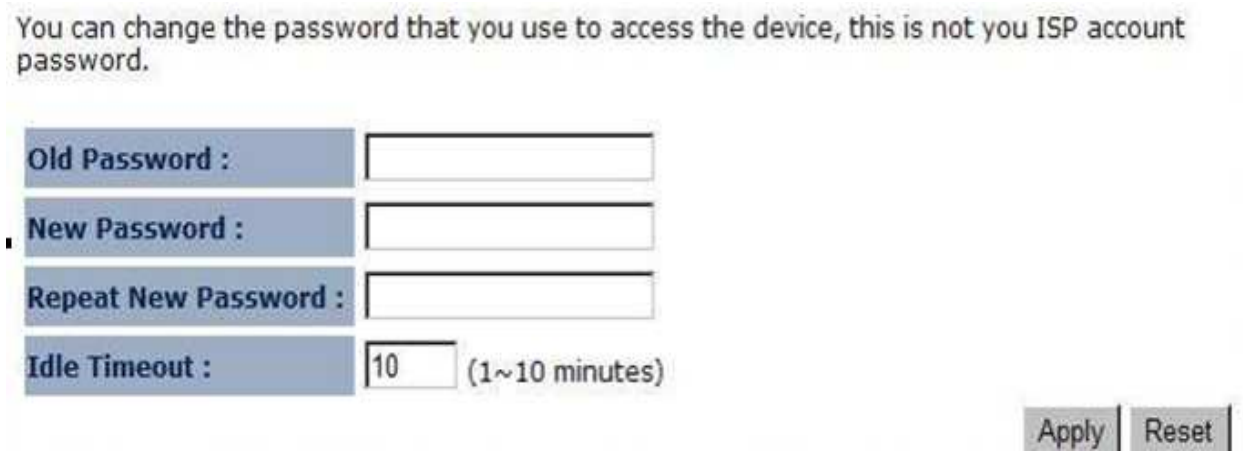
- **Start IP / End IP: Set IP range for DHCP server**
- **Domain Name: Allow user to modify Domain Name.**

Domain Name System (DNS) servers are used to translate a hostname or a domain name

4.4. Management

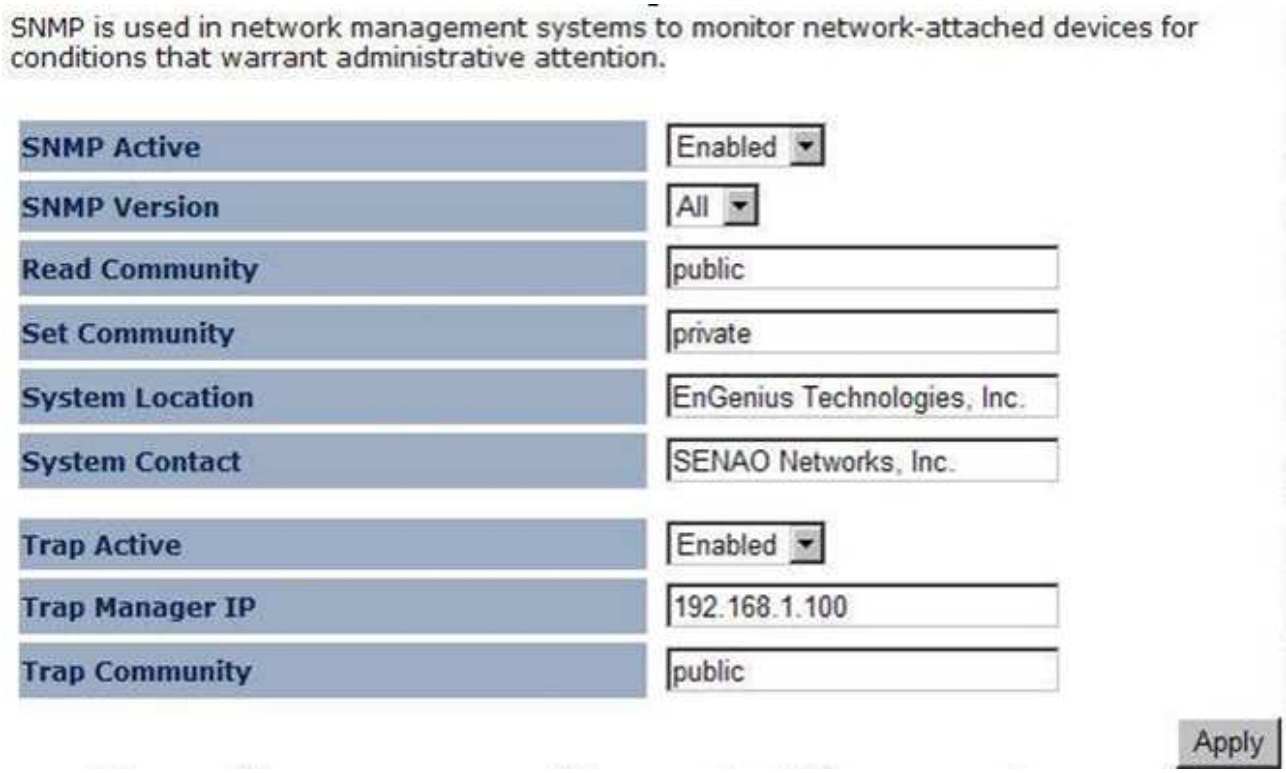
4.4.1. Admin

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



4.4.2. SNMP

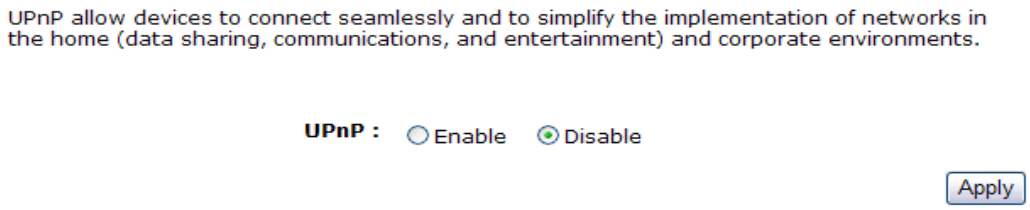
Allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages,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



- **SNMP 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.**

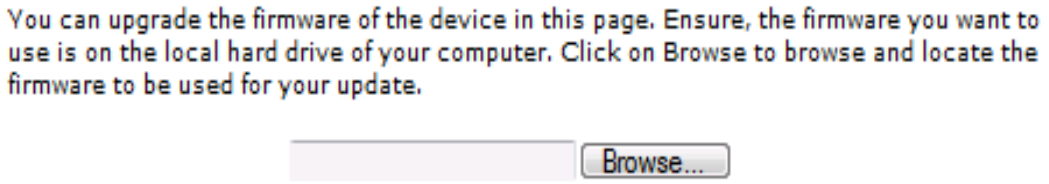
4.4.3. UPnP

Plug-and-Play



4.4.4. Firmware

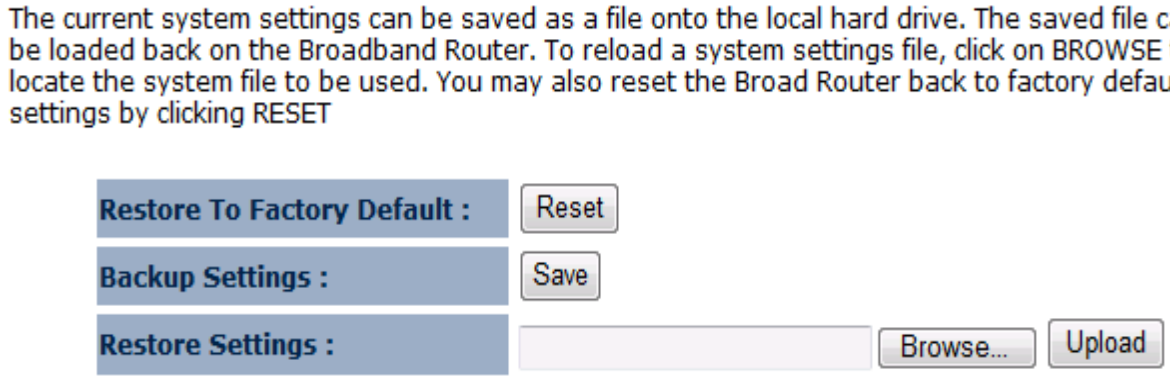
It allows you to upgrade the firmware of the device in order to improve the functionality and performance.



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.

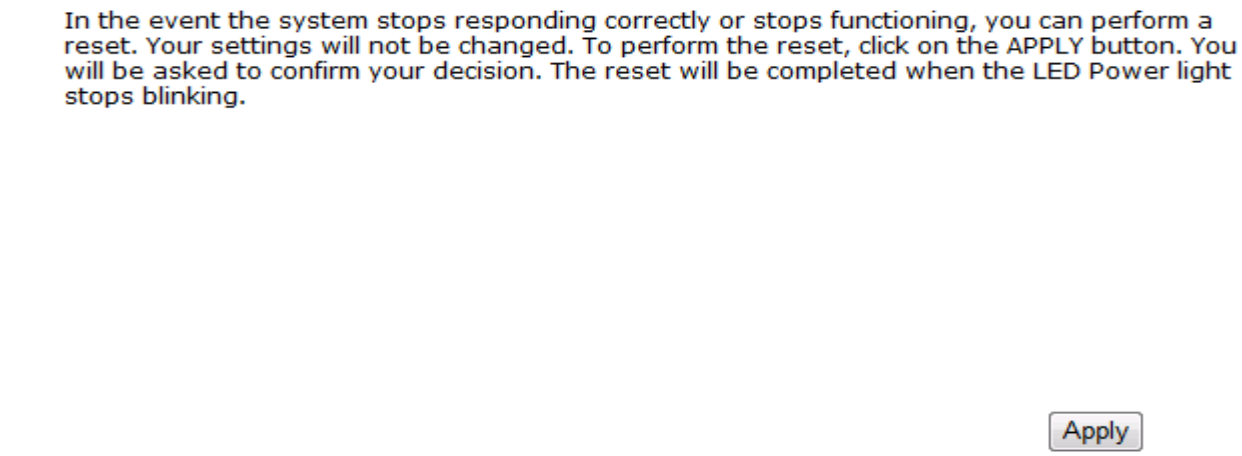
4.4.5. Configure

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



4.4.6. Reset

This will only reset you devices with current configuration unaffected.

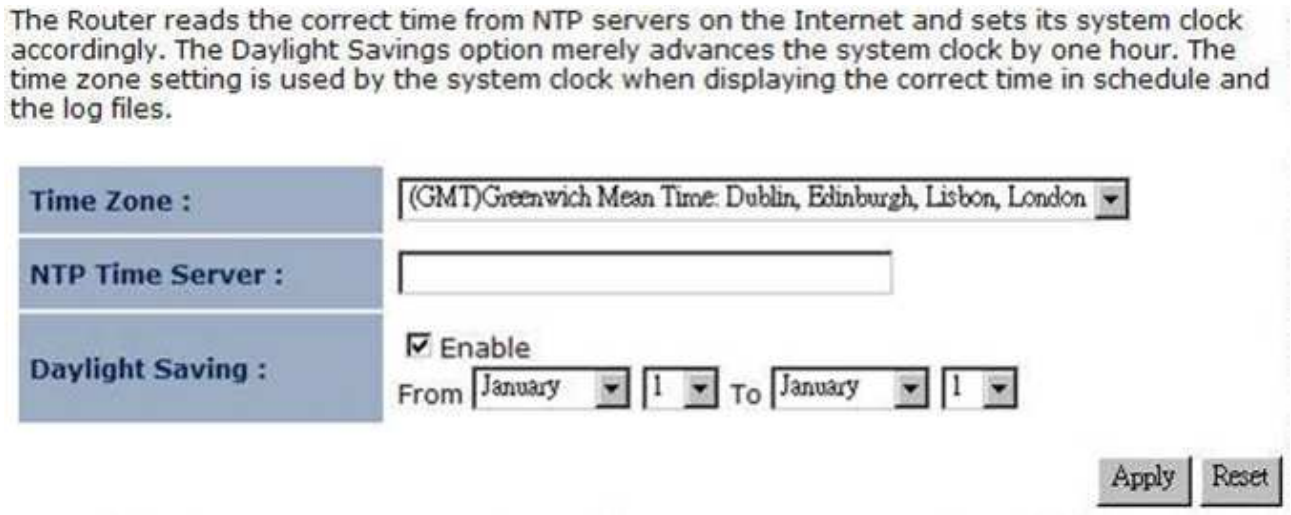


4.5. Tools

4.5.1. Time Setting

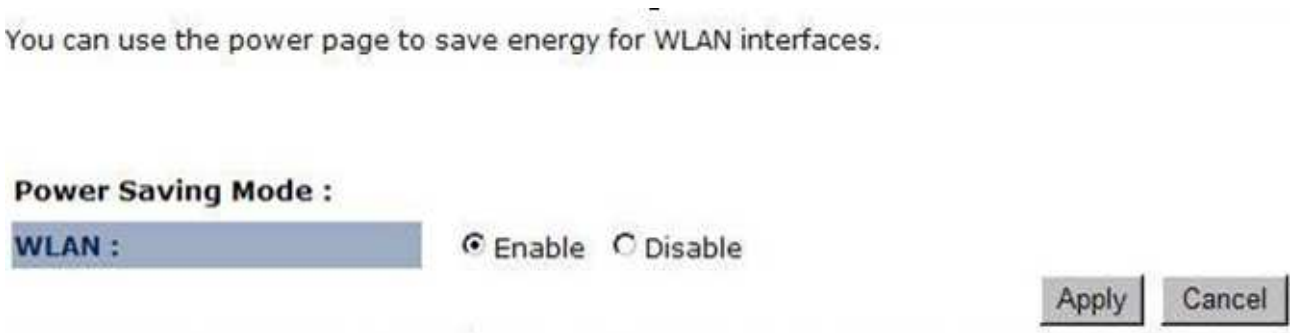
This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

If the device losses 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.



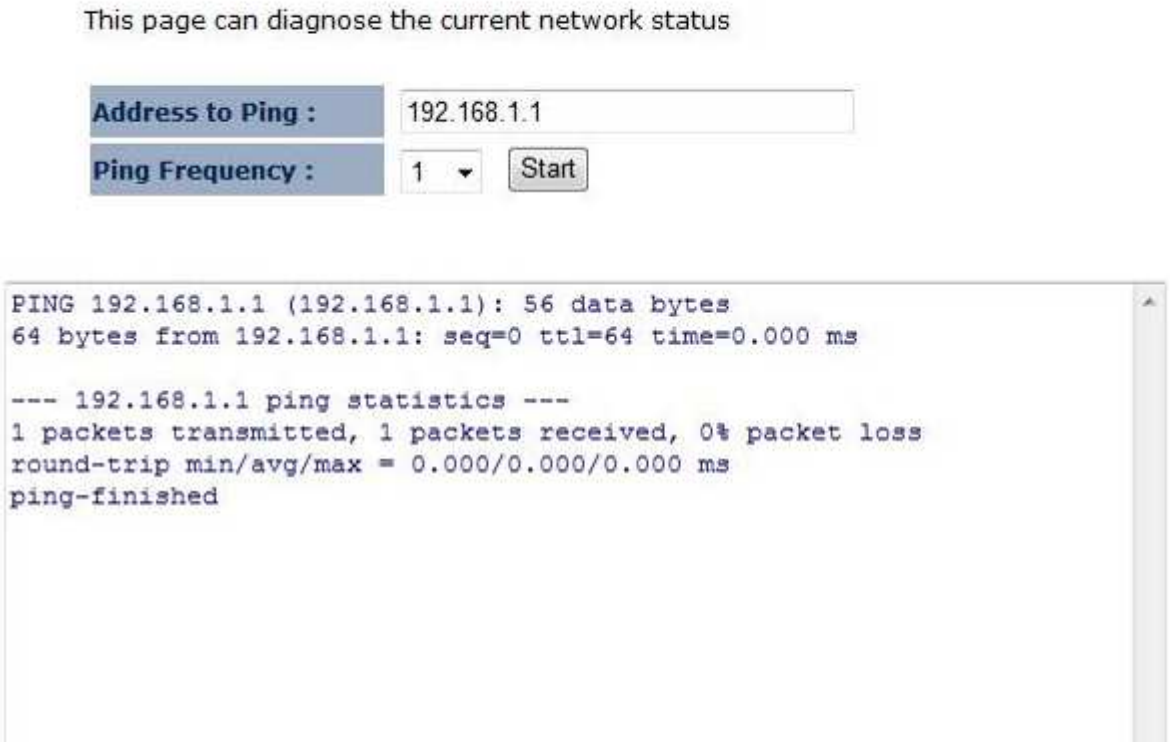
- **Time Zone: Select time zone.**
- **NTP Time Server: Specify the NTP server's IP address for time synchronization.**
- **Daylight Saving: To enable daylight savings time.**

4.5.2. Power Saving



4.5.3. Diagnosis

Check whether a network destination is reachable with ping service.



4.5.4. LED Control

You can use the LED control page to control LED on/off for Power, LAN interface and WLAN interface.

4.6. Logout

This page is used to logout this device.

Logout

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.