

# EnGenius™

## EOR7550

### Dual Radio Multi-Function Repeater

### User's Manual

V1.0



# Table of Content

1.	Introduction .....	1
1.1.	Features.....	1
1.2.	Package Contents .....	2
1.3.	System Requirement .....	2
1.4.	Applications.....	2
2.	Modes .....	5
2.1.	AP .....	5
2.2.	Client Bridge .....	6
2.3.	Client Router .....	6
2.4.	WDS Bridge .....	6
2.5.	WDS Repeater .....	6
2.6.	Universal Repeater (AP) .....	6
3.	Understanding the Hardware.....	7
3.1.	Hardware Installation.....	7
3.2.	IP Address Configuration.....	7
4.	Web Configuration .....	8
4.1.	System .....	8
4.1.1.	Operation Mode.....	8
4.1.2.	Status.....	9
4.1.3.	DHCP .....	10
4.1.4.	Schedule .....	10
4.1.5.	Event Log .....	11
4.1.6.	Monitor .....	12
4.2.	Wireless.....	13
4.2.1.	AP .....	13
4.2.2.	Client Bridge .....	23
4.2.3.	Client Router .....	27
4.2.4.	WDS Bridge .....	30
4.2.5.	WDS Repeater .....	33
4.2.6.	Universal Repeater (AP) .....	36
4.2.7.	Universal Repeater (STA).....	44
4.3.	Network.....	47
4.3.1.	Status.....	47
4.3.2.	LAN .....	47
4.3.3.	WAN .....	48
4.4.	Firewall.....	49

4.4.1.	Enable.....	49
4.4.2.	DMZ.....	49
4.4.3.	DoS .....	49
4.4.4.	MAC Filter .....	50
4.4.5.	IP Filter .....	50
4.4.6.	URL Filter.....	51
4.5.	Advanced.....	52
4.5.1.	NAT .....	52
4.5.2.	Port Mapping .....	52
4.5.3.	Port Forwarding .....	53
4.5.4.	Port Triggering.....	54
4.5.5.	ALG .....	55
4.5.6.	UPnP.....	55
4.5.7.	QoS.....	56
4.5.8.	Static Routing .....	58
4.5.9.	Dynamic Routing.....	59
4.5.10.	Routing Table.....	59
4.6.	Management.....	60
4.6.1.	Admin .....	60
4.6.2.	SNMP.....	60
4.6.3.	Firmware .....	61
4.6.4.	Configure.....	62
4.6.5.	Reset.....	62
4.7.	Tools .....	64
4.7.1.	Time Setting .....	64
4.7.2.	DDNS .....	64
4.7.3.	Diagnosis .....	65
4.8.	Logout .....	67
Appendix A – SPECIFICATIONS .....		68
Appendix B – FCC INTERFERENCE STATEMENT .....		72

## Revision History

---

Version	Date	Notes
1.0	January, 08, 2009	Initial Version

---

# 1. Introduction

EOR7550 equips with two powerful independent RF interfaces which support 802.11a/b/g and 802.11b/g/n. With certified IP-65 protection, it is designed to deliver high reliability under harsh outdoor environment.

Built-in advanced multi-functions provide flexibility in constructing scalable WiFi networks for all possible applications. With two individual interfaces, each can be configured into 6 different modes with maximum of 18 combinations. With 802.11n support, EOR7550 offers bandwidth up to 300Mbps to accommodate heavy traffic services such as multimedia streaming. Establishing backbone network using 802.11a ensures stability and reduces interference while 802.11b/g offers great compatibility to all wireless clients.

EOR7550 provides wide-range of authentication and encryption standards (including WEP, WPA, WPA2, TKIP/AES and IEEE 802.1X) to enforce maximum security. Furthermore, friendly security management user interface reduces configuration complexity. EOR7550 is a true carrier-grade product which is guaranteed to fulfill any business proposals.

## 1.1. Features

### Wireless

- **Dual Radio** Two radio for independent backhaul(a/b/g, Radio1) and local access(b/g/n, Radio2).
- **High Data Rate** High speed physical transmitting rate up to 300Mbps with 11n, support large payload such as MPEG video streaming
- **Multifunction application** Defining each radio configuration for different application
- **Wireless Distributed System (WDS)** Supporting WDS to bridge repeater

### Networking

- **Public wireless solution** An AP interface that is especially useful in public areas such as hotspots and enterprise
- **Bandwidth Selection** Provides 5MHz/ 10MHz/ 20MHz for 802.11a/b/g and 20MHz/ 40MHz for 802.11n
- **Signal Strength** Display 0%~100% to show the signal condition for more convenient installation and setup.
- **QoS(WMM)** Enhance performance and density

### Security

- **802.11i** WPA, WPA2
- **802.1x** EAP-TLS/TTLS, IEEE 802.1x Supplicant support in CB mode
- **MAC address functions** MAC address access control list, MAC address filter
- **Multiple SSID** 4 BSSID supported. Primary(1<sup>st</sup>) BSSID for normal setting follow this router's main default setting for security setting. Each SSID can set itself wireless or WAN

access setting.

## Management

- **Firmware Upgrade** Upgrading firmware via web browser, setting are reserved after upgrade
- **Reset & Backup** Reset to factory default. User can export all setting into a file via WEB
- **MIB** MIB I, MIB II(RFC1213) and private MIB
- **SNMP** V1, V2c

## 1.2. Package Contents

- 1 x Dual Radio Multi-Function Repeater (EOR7550)
- 1 x PoE injector with Power Adapter
- 1 x Wall Mounting kit
- 1 x 1.8m Grounding Cable
- 1 x CD with User's Manual
- 1 x QIG

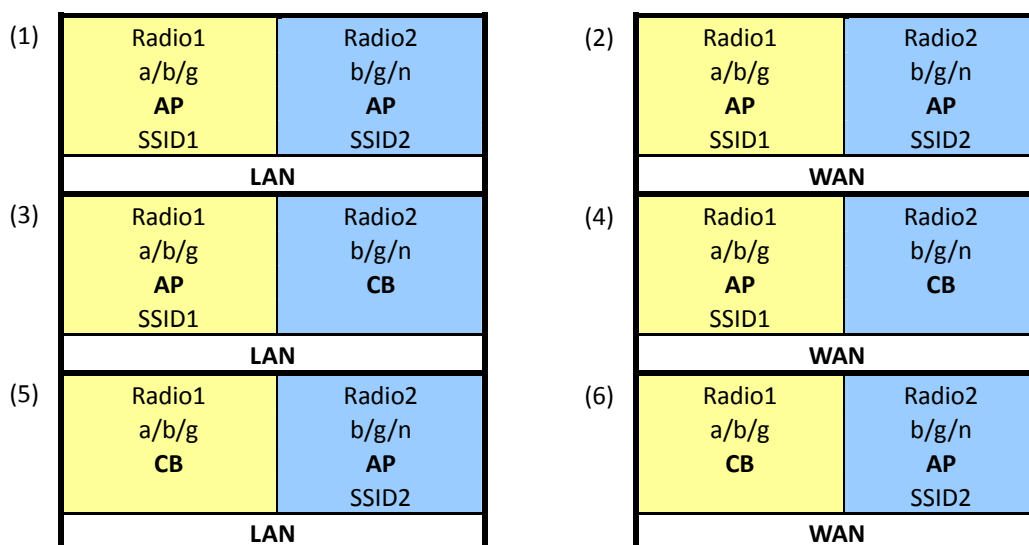
## 1.3. System Requirement

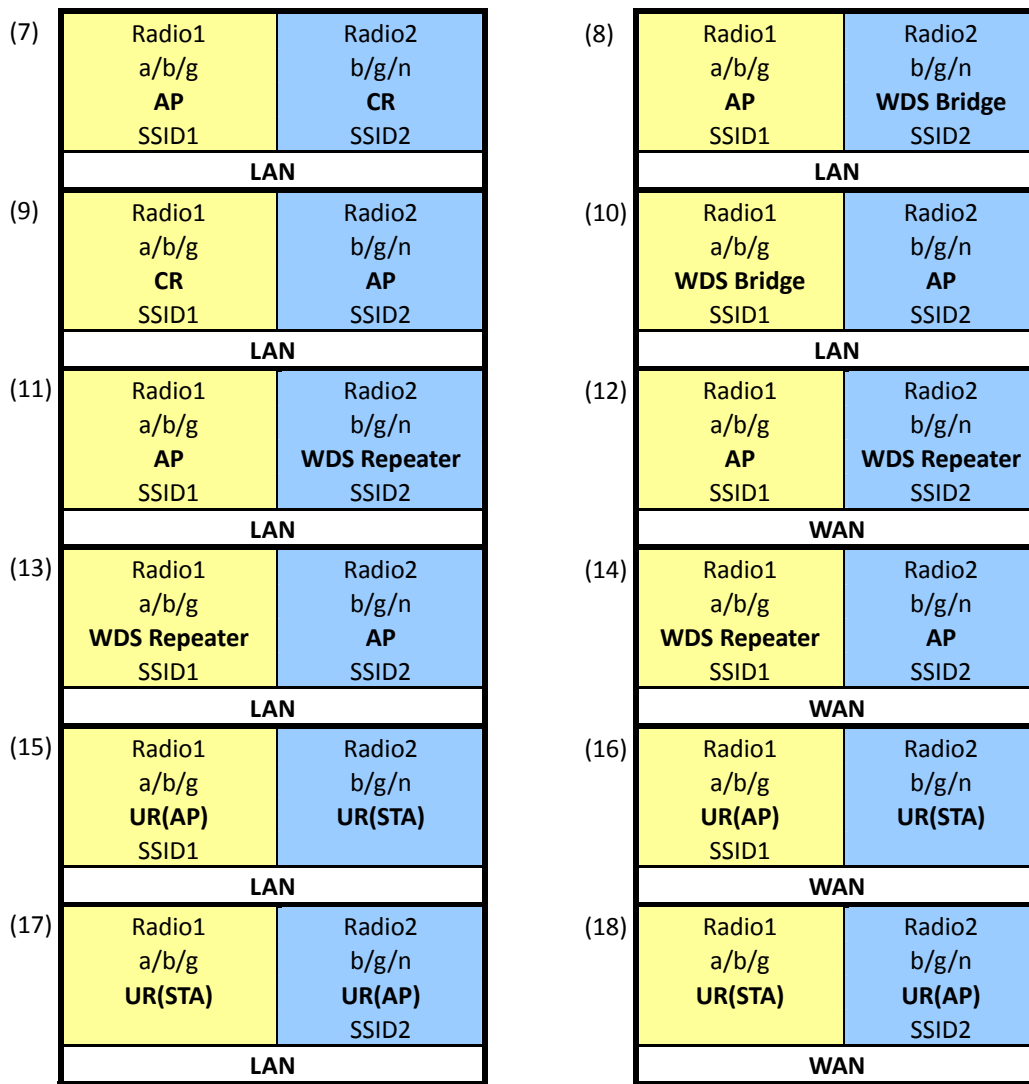
The following are the minimum system requirements in order configure the device.

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

## 1.4. Applications

EOR7550 provides 18 operation modes for different applications in different environment.





EOR7550 are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

#### **Difficult-to-wire environments**

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

- **Temporary workgroups**

Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

- **The ability to access real-time information**

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

- **Frequently changed environments**

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

- **Small Office and Home Office (SOHO) networks**

SOHO users need a cost-effective, easy and quick installation of a small network.

- **Wireless extensions to Ethernet networks**

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

- **Wired LAN backup**

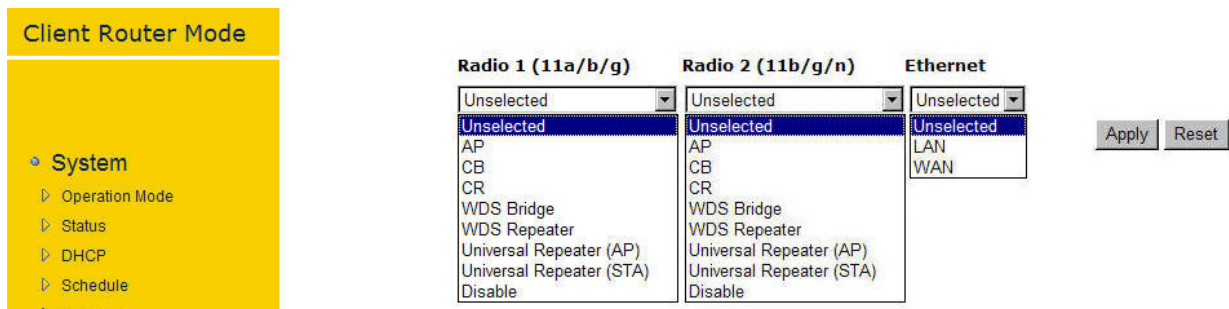
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

- **Training/Educational facilities**

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.



## 2. Modes



EOR7550 provides 2 separate radio channels for wider service area. Each of these 2 radio channels can be configured as different function mode separately. The device allows you to configure into different modes for different purposes in your network infrastructure. Each of these modes will have different setting. You are allowed to configure your radio channel freely with the following combination.

EOR7550 Concurrent Modes	Radio1(11a/b/g)							
	Radio2(11b/g/n)	AP	CB	CR	WDS Bridge	WDS Repeater	UR(AP)	UR(STA)
AP	<input type="radio"/> (LAN/WAN)	<input type="radio"/> (LAN/WAN)	<input type="radio"/> (LAN)	<input type="radio"/> (LAN)	<input type="radio"/> (LAN/WAN)	X	X	<input type="radio"/> (LAN/WAN)
CB	<input type="radio"/> (LAN/WAN)	X	X	X	X	X	X	<input type="radio"/> (LAN/WAN)
CR	<input type="radio"/> (LAN)	X	X	X	X	X	X	<input type="radio"/> (LAN)
WDS Bridge	<input type="radio"/> (LAN)	X	X	X	X	X	X	<input type="radio"/> (LAN)
WDS Repeater	<input type="radio"/> (LAN/WAN)	X	X	X	X	X	X	<input type="radio"/> (LAN/WAN)
UR(AP)	X	X	X	X	X	X	<input type="radio"/> (LAN/WAN)	X
UR(STA)	X	X	X	X	X	<input type="radio"/> (LAN/WAN)	X	X
Disable	<input type="radio"/> (LAN/WAN)	<input type="radio"/> (LAN/WAN)	<input type="radio"/> (LAN)	<input type="radio"/> (LAN)	<input type="radio"/> (LAN/WAN)	X	X	X

### 2.1. AP

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

## 2.2. Client Bridge

When in Client Bridge, EOR7550 will associate with nearby AP and sees the network device combination as a standard mobile unit (MU). The access point then forms a wireless bridge between the wired LAN and clients through EOR7550.

## 2.3. Client Router

As Client Bridge mode, this allows your device to function as Client Bridge and Router as well. The device connection map can refer to 2.2 Client Bridge.

## 2.4. WDS Bridge

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.

## 2.5. WDS Repeater

WDS (Wireless Distribution System) Repeater is not only an extended device, but also provides a wireless application for other wireless clients.

## 2.6. Universal Repeater (AP)

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.

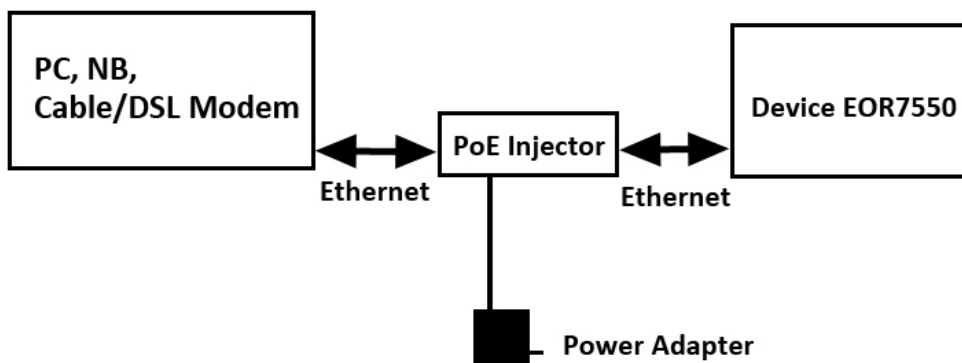
## 2.7. Universal Repeater (STA)

Universal Repeater (STA) mode allows your device to operate as a client. This is usually configured with Universal Repeater (AP) on another channel.

# 3.Understanding the Hardware

## 3.1. Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Network port of the PoE injector and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to AP/Bridge port of the PoE injector and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the 48V port of the PoE injector and the other end into the power socket on the wall.
5. This diagram depicts the hardware configuration



## 3.2. IP Address Configuration

The default IP address of the device is 192.168.1.2. In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.
2. Select Internet Protocol (TCP/IP) and then click on the Properties button. This will allow you to configure the TCP/IP settings of your PC/Notebook.
3. Select Use the following IP Address radio button and then enter the IP address (192.168.1.21) and subnet mask (255.255.255.0). Ensure that the IP address and subnet mask are on the same subnet as the device.
4. Click on the OK button to close this window, and once again to close LAN properties window.

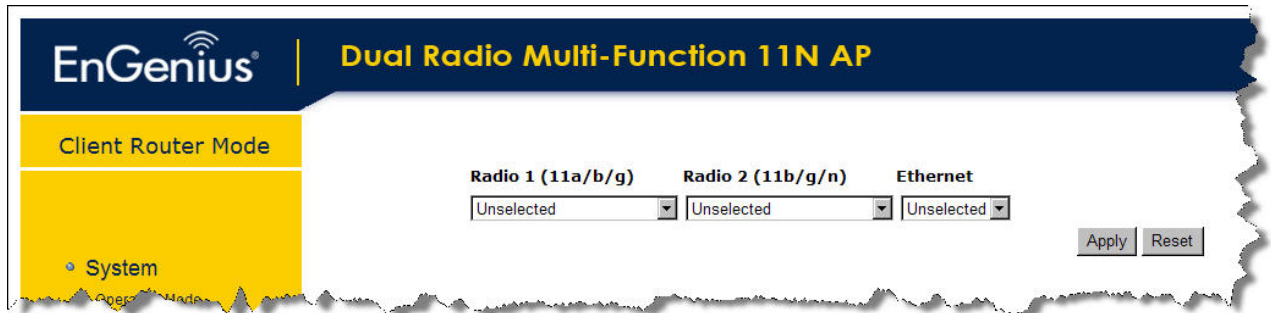
# 4. Web Configuration

## 4.1. System

### 4.1.1. Operation Mode

You are allowed to configure your device into different modes for different purposes (Please see [Chapter 2](#)).

1. To start configuration, press Reset to purge the default setting.
2. All 3 drop down fields will be reset for new configuration.
3. Refers to table in [Chapter 2](#) for further configuration.



## 4.1.2. Status

#### Access Point Mode

- System
  - ▷ Operation Mode
  - ▷ **Status**
  - ▷ Schedule
  - ▷ Event Log
  - ▷ Monitor
- Wireless
- Network
- Management
- Tools
- ▷ Logout

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	2008/01/01 00:22:09
System Up Time	14 min 36 sec
Hardware version	1.0.0
Serial Number	08B259984
Kernel version	1.0.6
Application version	1.0.6

#### LAN Settings

IP address	192.168.1.1
Subnet Mask	255.255.255.0
MAC address	00:02:6F:55:47:01

#### WLAN Settings

##### Radio 1 Settings

Channel 11

##### SSID\_1

ESSID EnGenius5545F4\_1  
Security Disable  
BSSID 00:02:6F:55:45:F4

##### Radio 2 Settings

Channel 11

##### SSID\_1

ESSID EnGenius554644\_1  
Security Disable  
BSSID 00:02:6F:55:46:44

### 4.1.3. DHCP

#### DHCP Client Table :

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

IP address	MAC address	Expiration Time
192.168.1.100	00:22:43:24:B8:5E	Forever

Refresh

You can assign an IP address to the specific MAC address

Enable Static DHCP IP

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

Add

Reset

#### Current Static DHCP Table :

NO.	IP address	MAC address	Select
1	192.168.1.3	00:00:00:00:00:00	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel



DHCP Configuration Menu only shows when device is in Client Router mode.

### 4.1.4. 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 10)

NO.	Description	Service	Schedule	Select
1	schedule 01	Power Saving	From 01:01 to 02:02---Mon, Tue, Wed	<input type="checkbox"/>

Add

Edit

Delete Selected

Delete All

Apply

Cancel

## 4.1.5. Event Log

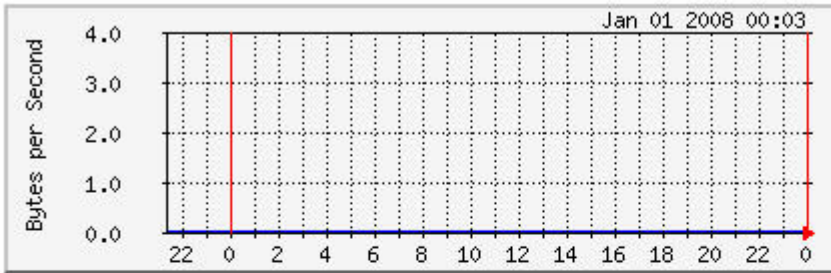
View the system operation information.

```
day 1 00:03:30 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day 1 00:03:27 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day 1 00:03:27 [SYSTEM]: DHCP Server, Sending OFFER of 192.168.1.100
day 1 00:01:53 [SYSTEM]: NET, start Firewall
day 1 00:01:53 [SYSTEM]: NET, start NAT
day 1 00:01:53 [SYSTEM]: NET, stop Firewall
day 1 00:01:53 [SYSTEM]: NET, stop NAT
day 1 00:01:53 [SYSTEM]: NTP, start NTP Client
day 1 00:01:53 [SYSTEM]: DHCP, start DHCP Server
day 1 00:01:53 [SYSTEM]: DHCP, DHCP Server Stopping
day 1 00:01:52 [SYSTEM]: LAN, IP address=192.168.1.2
day 1 00:01:52 [SYSTEM]: LAN, start
day 1 00:01:52 [SYSTEM]: LAN, Stopping
day 1 00:01:36 [SYSTEM]: NET, start Firewall
day 1 00:01:36 [SYSTEM]: NET, start NAT
day 1 00:01:36 [SYSTEM]: NET, stop Firewall
day 1 00:01:36 [SYSTEM]: NET, stop NAT
day 1 00:01:36 [SYSTEM]: NTP, start NTP Client
day 1 00:01:36 [SYSTEM]: DHCP, start DHCP Server
day 1 00:01:36 [SYSTEM]: DHCP, DHCP Server Stopping
day 1 00:01:36 [SYSTEM]: LAN, IP address=192.168.1.2
day 1 00:01:36 [SYSTEM]: LAN, start
day 1 00:01:36 [SYSTEM]: LAN, Stopping
```

## 4.1.6. Monitor

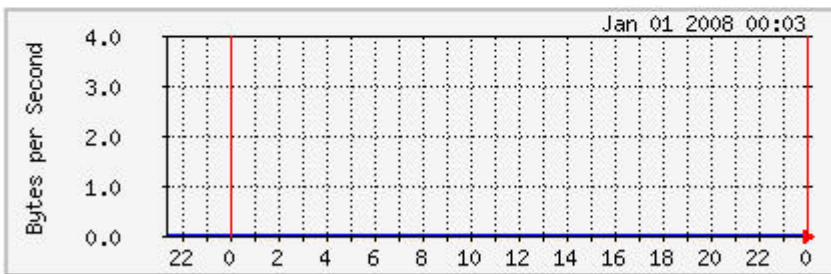
### Ethernet Daily Graph (5 Minute Average)

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

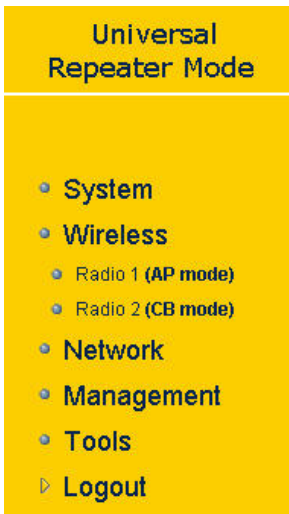
### WLAN Daily Graph (5 Minute Average)



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



## 4.2. Wireless



EOR7550 provides 2 separate Radio Channel which allows you configuring your device into different separate modes. Each Radio Channel can be configured separately with different configuration menu.

### 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	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

## 4.2.1.2. 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>Band :</b>	2.4 GHz (802.11b/g) ▼
<b>Enabled SSID#:</b>	1 ▼
<b>ESSID1 :</b>	EnGenius5545F4_1
<b>Channel :</b>	11 2.462 GHz ▼

- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (802.11b/g)**
  - ✓ **5 GHz (802.11a)**
  - ✓ **2.4 GHz (802.11b)**
  - ✓ **2.4 GHz (802.11g)**
- **Enabled SSID#:** The device allows you to add up to 4 unique SSID
- **ESSID#:** Description of each configured SSID
- **Channel:** Channel selection. This will vary based on selected Band.

### 4.2.1.3. 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="2346"/>	(0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/>	(21~191 us) to <input type="text" value="4200"/> meters
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(25-1000 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-10)
<b>Data rate :</b>	<input type="text" value="Auto"/>	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" 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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

#### 4.2.1.4. 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

ESSID Selection :	EnGenius5545F4_1 ▼
Broadcast ESSID :	Enable ▼
WMM :	Enable ▼
Encryption :	Disable ▼

Enable 802.1x Authentication

Apply Cancel

## ➤ 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 :	EnGenius5545F4_1
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 type="checkbox"/> Enable 802.1x Authentication	
<input type="button" value="Apply"/> <input type="button" value="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 **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>	EnGenius5545F4_1
<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

<b>ESSID Selection :</b>	EnGenius5545F4_1 ▾
<b>Broadcast ESSID :</b>	Enable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	WPA RADIUS ▾
<b>WPA type :</b>	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
<b>RADIUS Server IP address :</b>	<input type="text"/>
<b>RADIUS Server port :</b>	1812
<b>RADIUS Server Shared Secret :</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 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

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"/>
<input type="button" value="Add"/>	<input type="button" value="Reset"/>

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

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	<input type="checkbox"/>



## 4.2.1.6. Client List

### WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

## 4.2.1.7. 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.

## 4.2.1.8. 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"/>

## 4.2.1.9. Power Saving

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

**Power Saving Mode :**

**WLAN :**

Enable  Disable



Only Available for Radio 2

## 4.2.2. Client Bridge

### 4.2.2.1. Status

View the current internet connection status and related information.

WLAN AP Client Information	
Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	54 Mbps
Link Quality	85/100
Signal Level	-60 dBm
Noise Level	-87 dBm

### 4.2.2.2. 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>Band :</b>	2.4 GHz (802.11b/g/n) ▼
<b>Site Survey :</b>	<input type="button" value="Site Survey"/>

- **Radio:** To enable/disable radio channel
- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (802.11b/g)**
  - ✓ **5 GHz (802.11a)**
  - ✓ **2.4 GHz (802.11b)**
  - ✓ **2.4 GHz (802.11g)**

## ➤ Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

### Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

### 4.2.2.3. 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>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	

- **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 Period:** Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 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 a data rate for 802.11n 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.

#### 4.2.2.4. AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point.

##### AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	<input type="checkbox"/>
2	EnGenius	00:00:00:00:00:00	NONE	Open System	<input type="checkbox"/>

## 4.2.2.5. 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

## 4.2.3. Client Router

### 4.2.3.1. Status

View the current internet connection status and related information.

#### WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

### 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.

<b>Band :</b>	2.4 GHz (802.11b/g) ▼
<b>Site Survey :</b>	Site Survey

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (802.11b/g)**
  - ✓ **5 GHz (802.11a)**
  - ✓ **2.4 GHz (802.11b)**
  - ✓ **2.4 GHz (802.11g)**

## ➤ Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

### Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh

Add to AP Profile

### 4.2.3.3. 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="2346"/>	(0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/>	(21~191 us) to <input type="text" value="4200"/> meters
<b>Data rate :</b>	<input type="text" value="Auto"/>	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	

Apply

Cancel

- **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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

#### 4.2.3.4. AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point.

##### AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	<input type="checkbox"/>
2	EnGenius	00:00:00:00:00:00	NONE	Open System	<input type="checkbox"/>

#### 4.2.3.5. 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"/>

## 4.2.4. WDS Bridge



You can only connect to the device via Wireless Client

### 4.2.4.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

### 4.2.4.2. 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.

Band :	<input type="text" value="2.4 GHz (802.11b/g)"/>
Channel :	<input type="text" value="11 2.462 GHz"/>
MAC address 1 :	<input type="text" value="000000000000"/>
MAC address 2 :	<input type="text" value="000000000000"/>
MAC address 3 :	<input type="text" value="000000000000"/>
MAC address 4 :	<input type="text" value="000000000000"/>
Set Security :	<input type="button" value="Set Security"/>

- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (802.11b/g)**
  - ✓ **5 GHz (802.11a)**
  - ✓ **2.4 GHz (802.11b)**

✓ **2.4 GHz (802.11g)**

- **Channel:** Channel selection. This will vary based on selected Band.
- **MAC address 1~4:** Specify up to 4 MAC address of the device.
- **Set Security:** Wireless security mode setting.

## ➤ Security: Disabled

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

<b>Encryption :</b>	Disable ▾	Apply	Reset
---------------------	-----------	-------	-------

## ➤ Security: WEP

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

<b>Encryption :</b>	WEP ▾	Apply	Reset
<b>Key Length :</b>	64-bit ▾		
<b>Key Format :</b>	ASCII (5 characters) ▾		
<b>Default Tx Key :</b>	Key 1 ▾		
<b>Encryption Key 1 :</b>	<input type="text"/>		
<b>Encryption Key 2 :</b>	<input type="text"/>		
<b>Encryption Key 3 :</b>	<input type="text"/>		
<b>Encryption Key 4 :</b>	<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.

### 4.2.4.3. 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="2346"/> (0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/> (21~191 us) to <input type="text" value="4200"/> meters
<b>Beacon Interval :</b>	<input type="text" value="100"/> (25-1000 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/> (1-10)
<b>Data rate :</b>	<input type="text" value="Auto"/>
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble
<b>CTS Protection :</b>	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" 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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

## 4.2.5. WDS Repeater

### 4.2.5.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

### 4.2.5.2. 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>Band :</b>	2.4 GHz (802.11b/g) ▼
<b>Channel :</b>	11 2.462 GHz ▼
<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

- **Band:** Configure the device into different wireless modes.
  - ✓ 2.4 GHz (802.11b/g)
  - ✓ 5 GHz (802.11a)
  - ✓ 2.4 GHz (802.11b)
  - ✓ 2.4 GHz (802.11g)
- **Channel:** Channel selection. This will vary based on selected Band.
- **MAC address 1~4:** Specify up to 4 MAC address of the device.
- **Set Security:** Wireless security mode setting.

## ➤ Security: Disabled

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

<b>Encryption :</b>	Disable ▾	Apply   Reset
---------------------	-----------	---------------

## ➤ Security: WEP

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

<b>Encryption :</b>	WEP ▾	
<b>Key Length :</b>	64-bit ▾	
<b>Key Format :</b>	ASCII (5 characters) ▾	
<b>Default Tx Key :</b>	Key 1 ▾	
<b>Encryption Key 1 :</b>	<input type="text"/>	
<b>Encryption Key 2 :</b>	<input type="text"/>	
<b>Encryption Key 3 :</b>	<input type="text"/>	
<b>Encryption Key 4 :</b>	<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.

### 4.2.5.3. 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="2346"/> (0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/> (21~191 us) to <input type="text" value="4200"/> meters
<b>Beacon Interval :</b>	<input type="text" value="100"/> (25-1000 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/> (1-10)
<b>Data rate :</b>	<input type="text" value="Auto"/>
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble
<b>CTS Protection :</b>	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" 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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

## 4.2.6. Universal Repeater (AP)

### 4.2.6.1. Status

View the current internet connection status and related information.

WLAN Settings	
Channel	11
<b>SSID_1</b>	
ESSID	EnGenius5545F4_1
Security	Disable
BSSID	00:02:6F:55:45:F4

### 4.2.6.2. 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>Band :</b>	2.4 GHz (802.11b/g) ▼
<b>Enabled SSID#:</b>	1 ▼
<b>ESSID1 :</b>	EnGenius5545F4_1
<b>Channel :</b>	11 2.462 GHz ▼

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - ✓ 2.4 GHz (802.11b/g)
  - ✓ 5 GHz (802.11a)



- ✓ 2.4 GHz (802.11b)
- ✓ 2.4 GHz (802.11g)
- **Enabled SSID#:** The device allows you to add up to 4 unique SSID
- **ESSID#:** Description of each configured SSID

**Channel:** Channel selection. This will vary based on selected Band.

### 4.2.6.3. 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="2346"/>	(0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/>	(21~191 us) to <input type="text" value="4200"/> meters
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(25-1000 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-10)
<b>Data rate :</b>	<input type="text" value="Auto"/>	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" 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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

#### 4.2.6.4. 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>	EnGenius5545F4_1 ▾
<b>Broadcast ESSID :</b>	Enable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	Disable ▾

**Enable 802.1x Authentication**

Apply Cancel

## ➤ 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

<b>ESSID Selection :</b>	EnGenius5545F4_1 ▼
<b>Broadcast ESSID :</b>	Enable ▼
<b>WMM :</b>	Enable ▼
<b>Encryption :</b>	WEP ▼
<b>Authentication type :</b>	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
<b>Key Length :</b>	64-bit ▼
<b>Key type :</b>	ASCII (5 characters) ▼
<b>Default key :</b>	Key 1 ▼
<b>Encryption Key 1 :</b>	<input type="text"/>
<b>Encryption Key 2 :</b>	<input type="text"/>
<b>Encryption Key 3 :</b>	<input type="text"/>
<b>Encryption Key 4 :</b>	<input type="text"/>
<input type="checkbox"/> <b>Enable 802.1x Authentication</b>	
<input type="button" value="Apply"/> <input type="button" value="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 **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 :	EnGenius5545F4_1
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 :	

- **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

<b>ESSID Selection :</b>	EnGenius5545F4_1 ▾
<b>Broadcast ESSID :</b>	Enable ▾
<b>WMM :</b>	Enable ▾
<b>Encryption :</b>	WPA RADIUS ▾
<b>WPA type :</b>	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
<b>RADIUS Server IP address :</b>	<input type="text"/>
<b>RADIUS Server port :</b>	1812
<b>RADIUS Server Shared Secret :</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 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.

#### 4.2.6.5. 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"/>

Add    Reset

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

NO.	Description	MAC address	Select
1	CHOU	00:11:22:33:44:55	<input type="checkbox"/>

Delete Selected    Delete All    Reset

Apply    Cancel

## 4.2.6.6. Client List

### WLAN Client Table :

This WLAN Client Table shows client MAC address associated to this device.

Interface	MAC address	Signal(%)	Idle Time
No WLAN client is connected to the device.			

Refresh

## 4.2.6.7. 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

## 4.2.7. Universal Repeater (STA)

### 4.2.7.1. Status

View the current internet connection status and related information.

#### WLAN AP Client Information

Connection Status	Successful
ESSID	CHOU
Security	WEP
BSSID	00:19:CB:56:AA:B2
Channel	11
Frequency	2.462 GHz
Data Rate	36 Mbps
Link Quality	25/94
Signal Level	-68 dBm
Noise Level	-93 dBm

### 4.2.7.2. 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>Band :</b>	2.4 GHz (802.11b/g) ▼
<b>Site Survey :</b>	Site Survey

Apply Cancel

- **Band:** Configure the device into different wireless modes.
  - ✓ **2.4 GHz (802.11b/g)**
  - ✓ **5 GHz (802.11a)**
  - ✓ **2.4 GHz (802.11b)**
  - ✓ **2.4 GHz (802.11g)**



## ➤ Site Survey

Click on the Site Survey button to view a list of Access Points in the area. The Site Survey page displays information about devices within the 802.11b/g/n frequency. Information such as channel, SSID, BSSID, encryption, authentication, signal strength, and operating mode are displayed. Select the desired device and then click on the Add to AP Profile button.

### Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	11	CHOU	00:19:CB:56:AA:B2	WEP	OPEN	86	11b/g

Refresh

Add to AP Profile

### 4.2.7.3. 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="2346"/>	(0-2347)
<b>ACK Timeout</b>	<input type="text" value="49"/>	(21~191 us) to <input type="text" value="4200"/> meters
<b>Data rate :</b>	<input type="text" value="Auto"/>	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	

Apply

Cancel

- **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.
- **ACK Timeout:** The wait time for an ACK signal to time out.
- **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.

#### 4.2.7.4. AP Profile

##### AP Profile Table

NO.	SSID	MAC	Encryption	Authentication	Select
1	CHOU	00:19:CB:56:AA:B2	WEP	Open System	<input type="checkbox"/>
2	EnGenius	00:00:00:00:00:00	NONE	Open System	<input type="checkbox"/>

#### 4.2.7.5. 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"/>

## 4.3. Network

### 4.3.1. 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:55:47:01

### 4.3.2. LAN

You can enable the DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The device 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>802.1d Spanning Tree :</b>	Disabled ▾

Apply Cancel

- **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.

### 4.3.3. WAN

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

<b>Login Method:</b>	<input type="text" value="Dynamic IP Address"/>		
<b>Hostname :</b>	<input type="text"/>		
<b>MAC address:</b>	<input type="text" value="000000000000"/>	<input type="button" value="Clone MAC"/>	<input type="button" value="Set Default"/>
<b>Interface :</b>	<input type="text" value="WAN"/>		



Only shows when device is in WAN Interface

- **Login Method:** Configure different connection methods with WAN.
  - ✓ **Static IP Address**
  - ✓ **Dynamic IP Address**
  - ✓ **PPP over Ethernet**
  - ✓ **PPTP**
- **Hostname:** Specify the host name of your services
- **MAC address:** Specify MAC address over WAN
- **Interface:** WAN

## 4.4. Firewall



Only shows when device is in AP or CR modes with WAN Interface enabled.

### 4.4.1. Enable

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

Firewall :  Enable  Disable

Apply

### 4.4.2. DMZ

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

Enable DMZ

Local IP Address :

192.168.1.200

Apply

Cancel

### 4.4.3. DoS

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

Block DoS :  Enable  Disable

Apply

Cancel

## 4.4.4. MAC Filter

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

**Enable MAC filtering**

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

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

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

MAC Filtering table:

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

## 4.4.5. IP Filter

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

**Enable IP Filtering Table (up to 20 computers)**

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

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

<b>Description :</b>	<input type="text"/>
<b>Protocol :</b>	<input type="text" value="Both"/>
<b>Local IP Address :</b>	<input type="text"/> ~ <input type="text"/>
<b>Remote port range :</b>	<input type="text"/> ~ <input type="text"/>

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

- **Description:** Description of IP Filtering item
- **Protocol:** Type of Protocols
  - ✓ Both
  - ✓ TCP
  - ✓ UDP
- **Local IP Address:** Local IP address range
- **Remote port range:** Remote port number range

## 4.4.6. URL Filter

You can limit access to certain sites on the Internet. The URL filter will check each Web Site access. If the address , or part of the address, is included in the block site list, access will be denied. To filter a specific site, enter the Website for that site. For example, to stop your users from browsing a site called www.badsite.com, enter www.badsite.com or badsite.com in Website block fields.

**Enable URL Blocking**

URL/keyword

Add

Reset

**Current URL Blocking Table:**

NO.	URL/keyword	Select
-----	-------------	--------

Delete Selected

Delete All

Reset

Apply

Cancel

## 4.5. Advanced

### 4.5.1. NAT

This allows you to enable/disable NAT service of the device.

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

NAT :  Enable  Disable

Apply

### 4.5.2. Port Mapping

Port Mapping allows you to redirect common network services to a specific Client PC behind the NAT firewall.

Enable Port Mapping

Description :	<input type="text"/>
Local IP :	<input type="text"/>
Protocol :	Both <input type="button" value="v"/>
Remote port range :	<input type="text"/> ~ <input type="text"/>

Add

Current Port Mapping Table:

NO.	Description	Local IP	Type	Remote port range	Select
1	Test	192.168.1.123	BOTH	10-8888	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

- **Description:** Description of Port Mapping item.
- **Local IP:** Source IP to be mapped.



- **Protocol:** Protocol type.
  - ✓ Both
  - ✓ TCP
  - ✓ UDP
- **Remote Port Range:** Source Port number to be mapped.

### 4.5.3. Port Forwarding

Port Forwarding, also called Virtual Server. Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it..

**Enable Port Forwarding**

<b>Description :</b>	<input type="text"/>
<b>Local IP :</b>	<input type="text"/>
<b>Protocol :</b>	Both ▼
<b>Local Port :</b>	<input type="text"/>
<b>Forwarded Port :</b>	<input type="text"/>

**Current Port Forwarding Table :**

NO.	Description	Local IP	Local Port	Type	Forwarded Port	Select
1	Test	192.168.1.124	10	BOTH	20	<input type="checkbox"/>

- **Description:** Description of Port Forwarding item.
- **Local IP:** Source IP to be forwarded.
- **Protocol:** Protocol type
  - ✓ Both
  - ✓ TCP
  - ✓ UDP
- **Local Port:** Source Port Number to be forwarded.
- **Forwarded Port:** Destination Port Number forwarding to.

## 4.5.4. Port Triggering

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

**Enable Trigger Port**

<b>Description :</b>	<input type="text"/>
<b>Popular applications :</b>	Select an application <input type="button" value="Add"/>
<b>Trigger port :</b>	<input type="text"/> ~ <input type="text"/>
<b>Trigger type :</b>	Both <input type="button" value="v"/>
<b>Forwarded Port :</b>	<input type="text"/>
<b>Public type :</b>	Both <input type="button" value="v"/>

**Current Trigger-Port Table:**

NO.	Trigger port	Trigger type	Forwarded Port	Public type	Name	Select
1	7175	BOTH	51200-51201,51210	BOTH	Dialpad	<input type="checkbox"/>
2	28800	BOTH	2300-2400,47624	BOTH	MSN Gaming Zone	<input type="checkbox"/>
3	10-100	BOTH	20	BOTH	Test	<input type="checkbox"/>

## 4.5.5. ALG

The ALG (Application Layer Gateway) serves the purpose of a window between correspondent application processes so that they may exchange information on the open environment.

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

Apply Cancel

## 4.5.6. UPnP

UPnP allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and corporate environments.

UPnP :  Enable  Disable

Apply

## 4.5.7. QoS

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

QoS :  Priority Queue  Bandwidth Allocation  Disabled

Apply Cancel

### ➤ Priority Queue

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

QoS :  Priority Queue  Bandwidth Allocation  Disabled

#### Unlimited Priority Queue

IP Address	Description
192.168.1.123	The IP address will not be bounded in the QoS limitation

#### High/Low Priority Queue

Protocol	High Priority	Low Priority	Specific Port
FTP	<input type="radio"/>	<input checked="" type="radio"/>	20,21
HTTP	<input type="radio"/>	<input checked="" type="radio"/>	80
TELNET	<input type="radio"/>	<input checked="" type="radio"/>	23
SMTP	<input type="radio"/>	<input checked="" type="radio"/>	25
POP3	<input type="radio"/>	<input checked="" type="radio"/>	110
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>
Name: <input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="0"/>

Apply Cancel

## ➤ Bandwidth Allocation

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

**QoS :**       Priority Queue    Bandwidth Allocation    Disabled

<b>Type :</b>	Download ▾
<b>Local IP range :</b>	<input type="text"/> ~ <input type="text"/>
<b>Protocol :</b>	ALL ▾
<b>Remote port range :</b>	<input type="text"/> 1 ~ <input type="text"/> 65535
<b>Policy :</b>	Min ▾
<b>Rate(bps) :</b>	FULL ▾

### Current QoS Table:

NO.	Type	Local IP range	Protocol	Remote port range	Policy	Rate (bps)	Select
1	Download	192.168.1.100 ~ 192.168.1.110	ALL	1 ~ 65535	Min	FULL	<input type="checkbox"/>

- **Type:** Type of traffics to be monitored.
  - ✓ **Download**
  - ✓ **Upload**
  - ✓ **Both**
- **Local IP range:** Destination IP Range.
- **Protocol:** Protocol type to be monitored.
  - ✓ **All**
  - ✓ **TCP**
  - ✓ **UDP**
  - ✓ **SMTP**
  - ✓ **HTTP**
  - ✓ **POP3**

- ✓ FTP
- **Remote port range:** Source Port Number range
- **Policy:** The policy rules for QoS service.
  - ✓ Min
  - ✓ Max
- **Rate(bps):**
  - ✓ FULL
  - ✓ 32M
  - ✓ 13M
  - ✓ 8M
  - ✓ 4M
  - ✓ 2M
  - ✓ 1M
  - ✓ 512K
  - ✓ 256K
  - ✓ 128K

## 4.5.8. Static Routing

You can enable Static Routing to turn off the NAT function of the router and let the router forward packets by your routing policy.

**To take Static Route effect, please disable NAT function.**

**Enable Static Routing**

**Destination LAN IP:**

**Subnet Mask:**

**Default Gateway:**

**Current Static Routing Table:**

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Select
1	192.168.1.130	255.255.255.0	192.168.1.130	<input type="checkbox"/>

- **Destination LAN IP:** Destination IP address
- **Subnet Mask:** Destination subnet mask
- **Default Gateway:** Destination default gateway

## 4.5.9. Dynamic Routing

RIP allows you to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

**Dynamic Routing**

**RIP Transferring:**

RIPv1/RIPv2 ▼

**RIP Receiving:**

RIPv1/RIPv2 ▼

**Password:**

Apply

Cancel

## 4.5.10. Routing Table

Providing an overview of current Routing table.

### Current Routing Table

Destination LAN IP	Subnet Mask	Default Gateway
192.168.1.0	255.255.255.0	0.0.0.0

Refresh

## 4.6. Management

### 4.6.1. 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 your 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)

### 4.6.2. 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.

### 4.6.3. 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.

## 4.6.4. 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 device. 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

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

## 4.6.5. 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.



## 4.7. Tools

### 4.7.1. 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 device 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.

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

### 4.7.2. DDNS

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 providers for dynamic domain name routing.

The most common use for DDNS is in allowing an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. This makes it possible for other sites on the Internet to establish connections to the machine without needing to track the IP address themselves.

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

- **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

### 4.7.3. Diagnosis

Check whether a network destination is reachable with ping service.

This page can diagnose the current network status

<b>Address to Ping :</b>	<input type="text" value="192.168.1.2"/>
<b>Ping Count :</b>	<input type="text" value="1"/> <input type="button" value="Start"/>

```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: seq=0 ttl=64 time=0.000 ms

--- 192.168.1.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
ping-finished
```

## 4.8. Logout

Logout will let user leave the GUI.

# Appendix A – SPECIFICATIONS

Hardware Specification	
MCU	Ralink RT2880
RF	Atheros AR5414 (Radio1) + Ralink RT2820 (Radio2)
Memory	32MB SDRAM
Flash	8MB
Physical Interface	One 10/100 Fast Ethernet RJ-45 One Reset Button
Power Requirements	Power over Ethernet, 48V DC/0.375A
Regulation Certifications	FCC Part 15/UL, ETSI 300/328/CE

RF Specification																										
Frequency Band	<b>802.11a</b> 4.92 ~ 5.08 GHz 5.15 ~ 5.35GHz, 5.47 ~ 5.725GHz, 5.725~5.825GHz  <b>802.11b/g/n</b> U.S., Europe and Japan product covering 2.400 to 2.484 GHz, programmable for different country regulations																									
Modulation Technology	OFDM = BPSK, QPSK, 16-QAM, 64-QAM DSSS = DBPSK, DQPSK, CCK																									
Operating Channels	<b>802.11a</b> US/Canada:12 non-overlapping channel (5.15~5.35GHz, 5.725~5.825GHz) Europe:19 non-overlapping channel (5.15~5.35GHz, 5.47~5.825GHz) Japan:4 non-overlapping channel (5.15~5.25GHz) China:5 non-overlapping channel (5.725~5.85GHz)  <b>802.11b/g</b> 11 for North America, 14 for Japan, 13 for Europe																									
Receive Sensitivity (Typical)	<b>802.11a</b> -92dBm @ 6Mbps, -73dBm @ 54Mbps	<b>802.11g</b> -94 dBm @ 6Mbps, -74 dBm @ 54Mbps	<b>802.11b</b> -97 dBm @ 1Mbps -92 dBm @ 11Mbps	<b>802.11n</b> -91 dBm @ MCS8 -74 dBm @ MCS15																						
Available transmit power	<b>Radio 1 (WLAN1)</b> <table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">FCC</th> <th colspan="2">ETSI</th> </tr> <tr> <th>Frequency</th> <th>Power</th> <th>Frequency</th> <th>Power</th> </tr> </thead> <tbody> <tr> <td rowspan="4" style="text-align: center;">5.150~5.350 GHz IEEE802.11a</td> <td>27dBm@6~24Mbps</td> <td rowspan="4" style="text-align: center;">5.150~5.350 GHz IEEE802.11a</td> <td>27dBm@6~24Mbps</td> </tr> <tr> <td>25dBm@36Mbps</td> <td>25dBm@36Mbps</td> </tr> <tr> <td>23dBm@48Mbps</td> <td>23dBm@48Mbps</td> </tr> <tr> <td>21dBm@54Mbps</td> <td>21dBm@54Mbps</td> </tr> <tr> <td style="text-align: center;">5.470~5.725 GHz</td> <td>27dBm@6~24Mbps</td> <td style="text-align: center;">5.470~5.725 GHz</td> <td>27dBm@6~24Mbps</td> </tr> </tbody> </table>				FCC		ETSI		Frequency	Power	Frequency	Power	5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps	5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps	25dBm@36Mbps	25dBm@36Mbps	23dBm@48Mbps	23dBm@48Mbps	21dBm@54Mbps	21dBm@54Mbps	5.470~5.725 GHz	27dBm@6~24Mbps	5.470~5.725 GHz	27dBm@6~24Mbps
FCC		ETSI																								
Frequency	Power	Frequency	Power																							
5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps	5.150~5.350 GHz IEEE802.11a	27dBm@6~24Mbps																							
	25dBm@36Mbps		25dBm@36Mbps																							
	23dBm@48Mbps		23dBm@48Mbps																							
	21dBm@54Mbps		21dBm@54Mbps																							
5.470~5.725 GHz	27dBm@6~24Mbps	5.470~5.725 GHz	27dBm@6~24Mbps																							



	IEEE802.11a	25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	IEEE802.11a	25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
	5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps	5.725~5.825 GHz IEEE802.11a	27dBm@6~24Mbps 25dBm@36Mbps 23dBm@48Mbps 21dBm@54Mbps
	2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps	2.412~2.462 GHz IEEE802.11g	27dBm@6~24Mbps 25dBm@36Mbps 24dBm@48Mbps 23dBm@54Mbps
	2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps	2.412~2.462 GHz IEEE802.11b	28dBm@1~11Mbps
<b>Radio 2 (WLAN2)</b>				
	FCC		ETSI	
	Frequency	Power	Frequency	Power
	2.412~2.462 GHz IEEE802.11g/n	19dBm@6~24Mbps 18dBm@36Mbps 17dBm@48Mbps 16dBm@54Mbps	2.412~2.472 GHz IEEE802.11g/n	19dBm@6~9Mbps 18dBm@12~18Mbps 17dBm@24~36Mbps 16dBm@48~54Mbps
	2.412~2.462 GHz IEEE802.11b	18dBm@1~11Mbps	2.412~2.472 GHz IEEE802.11b	18dBm@1~11Mbps
<b>Antenna</b>	<b>2 x N type connector for 802.11a and 802.11b/g</b> <b>1 x Simulated Omni Antenna (2.4GHz) for 802.11b/g/n</b>			

<b>Software Features</b>	
General	
Topology	Infrastructure
Protocol / Standard	IEEE 802.3 (Ethernet) IEEE 802.3u (Fast Ethernet) IEEE 802.11a (5GHz WLAN) IEEE 802.11b/g (2.4GHz WLAN) RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 1034, 1035 DNS RFC 1058 RIP RFC 1305 NTP RFC 1541 / 2131 / 3046 DHCP client / Server RFC 2068 / 2616 HTTP RFC 2516 PPPoE

	RFC 2865,2866 RADIUS																																																																																										
Operation Mode	<b>18 modes</b> <table border="1" style="margin-top: 10px;"> <thead> <tr> <th>EOR7550</th> <th colspan="8">Radio1(11a/b/g)</th> </tr> <tr> <th>Radio2 (11b/g/n)</th> <th>AP</th> <th>CB</th> <th>CR</th> <th>WDS Bridge</th> <th>WDS Repeater</th> <th>UR(AP)</th> <th>UR(STA)</th> <th>Disable</th> </tr> </thead> <tbody> <tr> <td>AP</td> <td>O (LAN/WAN)</td> <td>O (LAN/WAN)</td> <td>O (LAN)</td> <td>O (LAN)</td> <td>O (LAN/WAN)</td> <td>X</td> <td>X</td> <td>O (LAN/WAN)</td> </tr> <tr> <td>CB</td> <td>O (LAN/WAN)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN/WAN)</td> </tr> <tr> <td>CR</td> <td>O (LAN)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN)</td> </tr> <tr> <td>WDS Bridge</td> <td>O (LAN)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN)</td> </tr> <tr> <td>WDS Repeater</td> <td>O (LAN/WAN)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN/WAN)</td> </tr> <tr> <td>UR(AP)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN/WAN)</td> <td>X</td> </tr> <tr> <td>UR(STA)</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>O (LAN/WAN)</td> <td>X</td> <td>X</td> </tr> <tr> <td>Disable</td> <td>O (LAN/WAN)</td> <td>O (LAN/WAN)</td> <td>O (LAN)</td> <td>O (LAN)</td> <td>O (LAN/WAN)</td> <td>X</td> <td>X</td> <td>X</td> </tr> </tbody> </table>	EOR7550	Radio1(11a/b/g)								Radio2 (11b/g/n)	AP	CB	CR	WDS Bridge	WDS Repeater	UR(AP)	UR(STA)	Disable	AP	O (LAN/WAN)	O (LAN/WAN)	O (LAN)	O (LAN)	O (LAN/WAN)	X	X	O (LAN/WAN)	CB	O (LAN/WAN)	X	X	X	X	X	X	O (LAN/WAN)	CR	O (LAN)	X	X	X	X	X	X	O (LAN)	WDS Bridge	O (LAN)	X	X	X	X	X	X	O (LAN)	WDS Repeater	O (LAN/WAN)	X	X	X	X	X	X	O (LAN/WAN)	UR(AP)	X	X	X	X	X	X	O (LAN/WAN)	X	UR(STA)	X	X	X	X	X	O (LAN/WAN)	X	X	Disable	O (LAN/WAN)	O (LAN/WAN)	O (LAN)	O (LAN)	O (LAN/WAN)	X	X	X
EOR7550	Radio1(11a/b/g)																																																																																										
Radio2 (11b/g/n)	AP	CB	CR	WDS Bridge	WDS Repeater	UR(AP)	UR(STA)	Disable																																																																																			
AP	O (LAN/WAN)	O (LAN/WAN)	O (LAN)	O (LAN)	O (LAN/WAN)	X	X	O (LAN/WAN)																																																																																			
CB	O (LAN/WAN)	X	X	X	X	X	X	O (LAN/WAN)																																																																																			
CR	O (LAN)	X	X	X	X	X	X	O (LAN)																																																																																			
WDS Bridge	O (LAN)	X	X	X	X	X	X	O (LAN)																																																																																			
WDS Repeater	O (LAN/WAN)	X	X	X	X	X	X	O (LAN/WAN)																																																																																			
UR(AP)	X	X	X	X	X	X	O (LAN/WAN)	X																																																																																			
UR(STA)	X	X	X	X	X	O (LAN/WAN)	X	X																																																																																			
Disable	O (LAN/WAN)	O (LAN/WAN)	O (LAN)	O (LAN)	O (LAN/WAN)	X	X	X																																																																																			
LAN	DHCP Server DHCP Client																																																																																										
Wireless	<p>- Auto Channel Selection (Setting varies by Regular Domains)</p> <p>- Transmission Rate</p> <p>11 a/b/g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 in Mbps</p> <p>11n :</p> <table border="1" style="margin-top: 10px;"> <thead> <tr> <th rowspan="2">MCS Index</th> <th colspan="2">Guard Interval 800ns</th> <th colspan="2">Guard Interval 400ns</th> </tr> <tr> <th>20 MHz</th> <th>40 MHz</th> <th>20 MHz</th> <th>40 MHz</th> </tr> </thead> <tbody> <tr><td>0</td><td>6.5</td><td>13.5</td><td>7.2</td><td>15</td></tr> <tr><td>1</td><td>13</td><td>27</td><td>14.4</td><td>30</td></tr> <tr><td>2</td><td>19.5</td><td>40.5</td><td>21.7</td><td>45</td></tr> <tr><td>3</td><td>26</td><td>54</td><td>28.9</td><td>60</td></tr> <tr><td>4</td><td>39</td><td>81</td><td>43.3</td><td>90</td></tr> <tr><td>5</td><td>52</td><td>108</td><td>57.8</td><td>120</td></tr> <tr><td>6</td><td>58.5</td><td>121.5</td><td>65</td><td>135</td></tr> <tr><td>7</td><td>65</td><td>135</td><td>72.2</td><td>157.5</td></tr> <tr><td>8</td><td>13</td><td>27</td><td>14.4</td><td>30</td></tr> <tr><td>9</td><td>26</td><td>54</td><td>28.9</td><td>60</td></tr> <tr><td>10</td><td>39</td><td>81</td><td>43.3</td><td>90</td></tr> <tr><td>11</td><td>52</td><td>108</td><td>57.8</td><td>120</td></tr> <tr><td>12</td><td>78</td><td>162</td><td>86.7</td><td>180</td></tr> <tr><td>13</td><td>104</td><td>216</td><td>115.6</td><td>240</td></tr> </tbody> </table>	MCS Index	Guard Interval 800ns		Guard Interval 400ns		20 MHz	40 MHz	20 MHz	40 MHz	0	6.5	13.5	7.2	15	1	13	27	14.4	30	2	19.5	40.5	21.7	45	3	26	54	28.9	60	4	39	81	43.3	90	5	52	108	57.8	120	6	58.5	121.5	65	135	7	65	135	72.2	157.5	8	13	27	14.4	30	9	26	54	28.9	60	10	39	81	43.3	90	11	52	108	57.8	120	12	78	162	86.7	180	13	104	216	115.6	240											
MCS Index	Guard Interval 800ns		Guard Interval 400ns																																																																																								
	20 MHz	40 MHz	20 MHz	40 MHz																																																																																							
0	6.5	13.5	7.2	15																																																																																							
1	13	27	14.4	30																																																																																							
2	19.5	40.5	21.7	45																																																																																							
3	26	54	28.9	60																																																																																							
4	39	81	43.3	90																																																																																							
5	52	108	57.8	120																																																																																							
6	58.5	121.5	65	135																																																																																							
7	65	135	72.2	157.5																																																																																							
8	13	27	14.4	30																																																																																							
9	26	54	28.9	60																																																																																							
10	39	81	43.3	90																																																																																							
11	52	108	57.8	120																																																																																							
12	78	162	86.7	180																																																																																							
13	104	216	115.6	240																																																																																							

	<table border="1"> <tr> <td>14</td> <td>117</td> <td>243</td> <td>130</td> <td>270</td> </tr> <tr> <td>15</td> <td>130</td> <td>270</td> <td>144.4</td> <td>300</td> </tr> </table>	14	117	243	130	270	15	130	270	144.4	300
14	117	243	130	270							
15	130	270	144.4	300							
	<ul style="list-style-type: none"> <li>- Distance Control (802.1x Ack timeout) for Radio2</li> <li>- Signal Strength indication using LEDs</li> <li>- Bandwidth Selection</li> </ul>										
Security	<p>Authentication:</p> <ul style="list-style-type: none"> <li>- 802.11i (WPA, WPA2)</li> <li>- 802.1x (including EAP-TLS/TTLS)</li> </ul> <p>IEEE 802.1x Supplicant support in CB mode</p> <p>Encryption: Open, WEP-64/128, TKIP, AES</p> <p>MAC address access control list</p> <p>MSSID Support in client access mode</p> <p>Hide SSID in beacons</p> <p>User isolation</p> <p>MAC address Filtering</p> <p>NAT in Client Router mode</p> <p>Multiple SSID (4 SSID)</p>										
QoS	WMM										
Management											
Configuration	Web-based configuration (HTTP)/Telnet										
Firmware Upgrade	<p>Upgrade firmware via web browser</p> <p>Fix latest setting parameter when firmware upgrading</p>										
Administrator Setting	Administrator password can be changed										
System monitoring	Status in hand , useful statistic and Event log										
Reset Setting	Reset to factory default and reboot										
MIB	MIB I , MIB II(RFC1213) and Private MIB										
SNMP	V1 , V2c										
Backup	Save all setting and condition to a file by web										

# 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.

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.

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.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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

