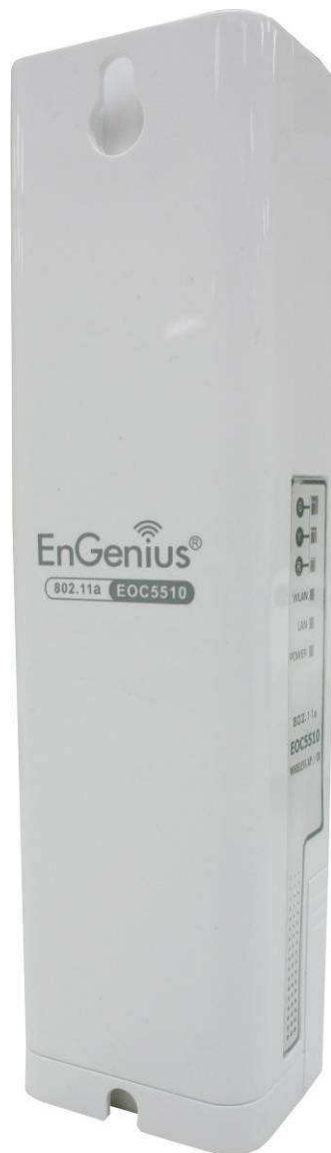


# Wireless Long Range Access Point / Client Bridge EOC5510



## User Manual

V1.0

# Table of Contents

<b>1 PRODUCT OVERVIEW .....</b>	<b>3</b>
1.1 FEATURE.....	3
1.2 BENEFITS.....	5
1.3 PACKAGE CONTENTS .....	6
1.4 SYSTEM REQUIREMENT .....	6
1.5 HARDWARE OVERVIEW .....	6
<b>2 EOC5510 MULTI-FUNCTION INSTRUCTION GUIDE.....</b>	<b>8</b>
2.1 ACCESS POINT .....	8
2.2 ACCESS POINT WITH WDS FUNCTION.....	8
2.3 CLIENT BRIDGE .....	9
2.4 WDS BRIDGE.....	9
2.5 CLIENT ROUTER .....	10
<b>3 COMPUTER SETTINGS.....</b>	<b>11</b>
3.1 ASSIGN A STATIC IP.....	11
3.2 LOGGING METHOD.....	12
<b>4 WIRELESS SETTINGS .....</b>	<b>13</b>
4.1 SWITCHING OPERATION MODE .....	13
4.2 WIRELESS SETTINGS .....	14
4.2.1 Access Point Mode -> Wireless Network.....	14
4.2.2 Client Bridge Mode -> Wireless Network.....	16
4.2.3 WDS Bridge Mode -> Wireless Network .....	17
4.2.4 Client Router Mode -> Wireless Network.....	19
4.3 WIRELESS SECURITY SETTINGS .....	20
4.3.1 WEP.....	20
4.3.2 WPA-PSK .....	21
4.3.3 WPA2-PSK .....	21
4.3.4 WPA-PSK Mixed.....	22
4.3.5 WPA .....	23
4.3.6 WPA2 .....	24
4.3.7 WPA Mixed.....	25
4.3.8 Radius Accounting.....	26
4.4 WIRELESS -> WIRELESS ADVANCED SETTINGS.....	27
4.5 WIRELESS -> WIRELESS MAC FILTER .....	29
4.6 WIRELESS -> WDS LINK SETTINGS .....	30
<b>5 LAN SETTINGS.....</b>	<b>31</b>

5.1 SYSTEM -> IP SETTINGS.....	31
5.2 SYSTEM -> SPANNING TREE SETTINGS .....	32
<b>6 ROUTER SETTINGS .....</b>	<b>33</b>
6.1 ROUTER -> WAN SETTINGS.....	33
6.1.1 WAN Settings -> Static IP .....	33
6.1.2 WAN Settings -> DHCP (Dynamic IP).....	36
6.1.3 WAN Settings -> PPPoE (Point-to-Point Protocol over Ethernet).....	38
6.1.4 WAN Settings -> PPTP (Point-to-Point Tunneling Protocol).....	40
6.2 ROUTER -> LAN SETTINGS.....	42
6.3 ROUTER -> VPN PASS THROUGH .....	43
6.4 ROUTER -> PORT FORWARDING .....	44
<b>7 INFORMATION STATUS .....</b>	<b>45</b>
7.1 STATUS -> MAIN .....	45
7.2 STATUS -> WIRELESS CLIENT LIST .....	46
7.3 STATUS -> SYSTEM LOG .....	47
7.4 STATUS -> WDS LINK STATUS .....	48
7.5 STATUS -> CONNECTION STATUS.....	48
7.6 STATUS -> DHCP CLIENT TABLE .....	49
<b>8 MANAGEMENT SETTINGS .....</b>	<b>50</b>
8.1 MANAGEMENT -> ADMINISTRATION .....	50
8.2 MANAGEMENT -> MANAGEMENT VLAN .....	51
8.3 MANAGEMENT -> SNMP SETTINGS.....	52
8.4 MANAGEMENT -> BACKUP/RESTORE SETTINGS.....	53
8.5 MANAGEMENT -> FIRMWARE UPGRADE .....	54
8.6 MANAGEMENT -> TIME SETTINGS.....	54
8.7 MANAGEMENT -> LOG.....	55
8.8 MANAGEMENT -> DIAGNOSTICS .....	56
<b>9 NETWORK CONFIGURATION EXAMPLE.....</b>	<b>58</b>
9.1 ACCESS POINT .....	58
9.2 CLIENT BRIDGE MODE .....	59
9.3 WDS BRIDGE MODE .....	59
9.4 CLIENT ROUTER .....	60
<b>APPENDIX A – FCC INTERFERENCE STATEMENT.....</b>	<b>62</b>
<b>APPENDIX B – IC INTERFERENCE STATEMENT.....</b>	<b>63</b>

## 1 Product Overview

Thank you for using EOC5510. It is a powerful, enhanced, enterprise scale product with 4+1 multi-functions Access Point, Access Point with WDS function, Client Bridge, WDS Bridge, and Client Router.

EOC5510 is easily to install almost anywhere with Power over Ethernet for quick outdoor installation. External N-type antenna provides better wireless signal quality and the antenna is upgradeable. EOC5510 uses 5G band of wireless signal to avoid interference of most digital signal such as mobile phone.

EOC5510 can manage power level control, Narrow bandwidth selection, Traffic shaping and Real-time RSSI indicator. EOC5510 is fully support of security encryption including WI-Fi Protected Access (WPA-PSK/WPA2-PSK), 64/128/152-bit WEP Encryption and IEEE 802.1x with RADIUS Accounting.

### 1.1 Feature

The following list describes the design of the EOC5510 made possible through the power and flexibility of wireless LANs:

**a) 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.

**b) 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.

**c) 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.

**d) Frequently changed environments**

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

**e) 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.

**f) Wired LAN backup**

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

**g) Training/Educational facilities**

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

---

<b>Advantage</b>	
<b>High Output Power</b>	Extended excellent Range and Coverage
<b>IEEE 802.11a Compliant</b>	Fully Interoperable with IEEE 802.11a compliant devices
<b>Detachable antenna support (N-Type)</b>	Collocate with any antenna for user's environment
<b>4+1 Multi-Function</b>	Users can use different mode in various environment
<b>Point-to-point, Point-to-multipoint Wireless Connectivity</b>	Let users transfer data between two buildings or multiple buildings
<b>Channel Bandwidth Selection</b>	Using different bandwidth to reach varied distance
<b>Support RSSI Indicator (CB mode)</b>	Users can select the best signal to connect with AP easily
<b>Power-over-Ethernet</b>	Flexible Access Point locations and cost savings. EOC5510 must uses the adapter provided in the package.
<b>Support Multi-SSID function (4 SSID) in AP mode</b>	Allow clients to access different networks through a single access point and assign different policies and functions for each SSID by manager
<b>WPA2/WPA/ WEP/ IEEE 802.1x support</b>	Fully support all types of security types.
<b>MAC address filtering in AP mode</b>	Ensures secure network connection
<b>PPPoE/PPTP function support (AP Router/CR mode)</b>	Easy to access internet via ISP service authentication
<b>SNMP Remote Configuration Management</b>	Help administrators to remotely configure or manage the Access Point easily.
<b>QoS (WMM) support</b>	Enhance user performance and density

---

## 1.2 Benefits

---

<b>Access Point Mode</b>	Use this feature to setup the access point's configuration information. It has support adjusting transmit power and channel. Client can access the network with different regulatory settings and automatically change to the local regulations.
<b>Client Bridge Mode</b>	Use this feature to connect to an Access Point and enjoy the great speed of surfing internet.
<b>WDS Bridge Mode</b>	Use this feature to link multiple APs in a network, All clients associated with any APs can communicate each other like an ad-hoc mode.
<b>Client Router Mode</b>	This feature functions completely opposite but similarly with AP Router Mode. Client Router connected to an AP wirelessly and transmit internet connection protocol through AP to access the internet.
<b>Multiple SSIDs</b>	EOC5510 supports up to 4 SSIDs on your access point. The following options can be set to each SS to each SSID: <ul style="list-style-type: none"><li>- SSID for public or private network</li><li>- Authentication is fully supported</li><li>- VLAN identifier</li><li>- Radius accounting identifier</li><li>- Profile isolation for infrastructure network</li></ul>
<b>VLAN</b>	Specify a VLAN number for each SSID to separate the services among clients.
<b>QoS</b>	Use this feature to limit the incoming or outgoing throughput.
<b>Wi-Fi Protect Access</b>	Wi-Fi Protect Access is a standard-based interoperable security enhancement that increases the level of data protection and access control for existing and future wireless LAN system. It is compatible with IEEE 802.11i standard WPA leverages TKIP and 802.1X for authenticated key management.

---

### 1.3 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- 1\* Wireless Outdoor Access Point / Client Bridge (EOC5510)
- 1\* 24V/0.6A Power Adapter
- 1\* Pole Mount
- 1\* QIG
- 1\* CD (User Manual)
- 1\* 5dBi 5GHz Dipole Antenna

Auction: 1. Using other Power Adapter than the one included with EOC5510 may cause damage of the device. 2. Screw dimension is  $\varnothing 5 \times 16$  mm for wall mount.

### 1.4 System Requirement

The following conditions are the minimum system requirement.

- A computer with an Ethernet interface and operating under Windows XP, Vista, 7 or Linux.
- Internet Browser that supports HTTP and JavaScript.

### 1.5 Hardware Overview

Hardware Specification	
MCU/RF	Atheros AR2313+AR5112
Memory	32MB SDRAM
Flash	8MB
Physical Interface	1 x 10/100 Fast Ethernet RJ-45 1 x Reset Button 1 x Antenna Switch ( Internal and External Switch ) 1 x SMA Connector
LED indicators	Power/ Status LAN (10/100Mbps) WLAN (Wireless is up) 3 x Link Quality (Client Bridge mode) <ul style="list-style-type: none"><li>• Green: Good Quality</li><li>• Yellow: Marginally Acceptable Quality</li></ul>

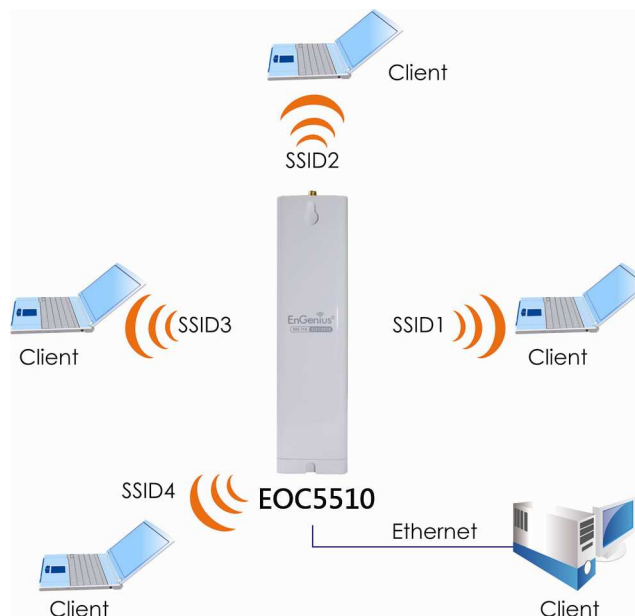
	<ul style="list-style-type: none"><li>• Red: Bad Quality</li></ul>
Power Requirements	Active Ethernet (Power over Ethernet) Proprietary PoE design Power Adapter 24V / 0.6A DC



## 2 EOC5510 Multi-Function Instruction Guide

### 2.1 Access Point

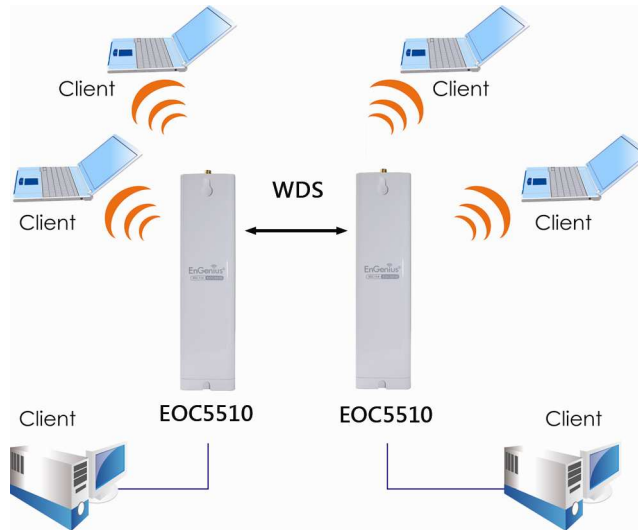
In the Access Point Mode with WDS Function, EOC5510 function like a central connection for any stations or clients that support IEEE 802.11a network. Stations and Client must configure the same SSID and Security Password to associate within the range. EOC5510 supports 4 different SSIDs to separate different clients at the same time.



### 2.2 Access Point with WDS Function

EOC5510 also supports WDS function in Access Point Mode without losing AP's capabilities. Configure others Access Point's Wireless MAC Address in both Access Point devices to enlarge the wireless area by enabling WDS Link Settings. WDS function can support up to 8 different AP's MAC addresses.

Auction: Not every Access Point device has support WDS in Access Point Mode. It is recommended using EOC5510 if you would like to use this service.



### 2.3 Client Bridge

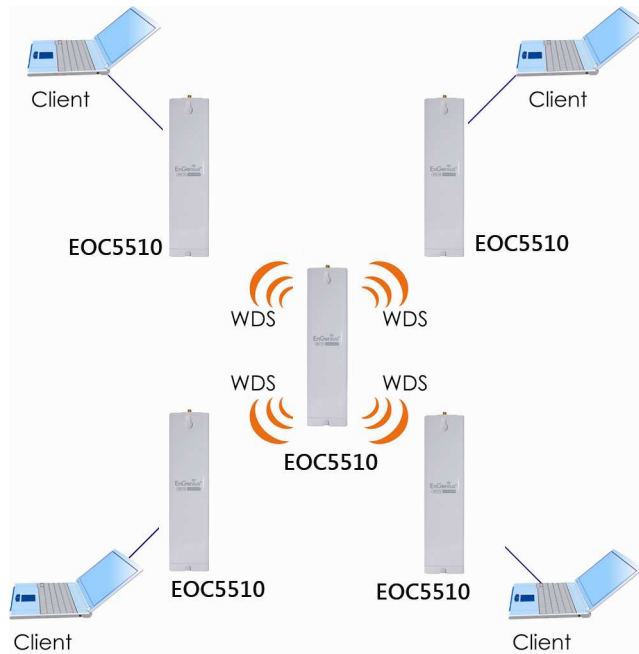
In the Client Bridge Mode, the EOC5510 function like a wireless dongle. Connected to an Access Point wirelessly and surf internet whenever you want. Using Site Survey to scan all the Access Point within the range and configure its SSID and Security Password to associate with it. Connect your station to the LAN port of the EOC5510 via Ethernet.



### 2.4 WDS Bridge

In the WDS Bridge Mode, the EOC5510 can wirelessly connect different LANs by just simply configure each other's MAC Address and Security Settings. This mode is used when two wired LANs locate in small distance and want to communicate each other. The best solution is using EOC5510 wirelessly connect two wired LANs. WDS Bridge Mode can establish 16 WDS links. The connection diagram is like a Star.

Auction: WDS Bridge Mode is not function like Access Point. APs linked by WDS are using the same frequency channel, more APs connected together may lower throughput. Please be aware to avoid loop connection, otherwise you may enable Spanning Tree Function.



## 2.5 Client Router

In the Client Router Mode, the EOC5510 has DHCP Server build inside that allows many LANs automatically generate an IP address to share the same Internet. Connect an AP/WISP Wirelessly and connect to LANs via wired. Client Router Mode is act completely opposite to the AP Router Mode.



## 3 Computer Settings

### 3.1 Assign a Static IP

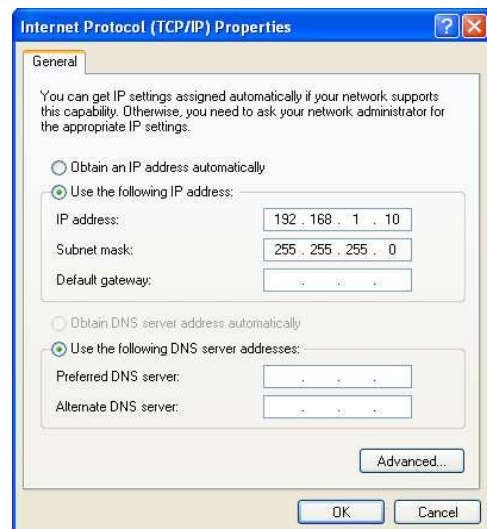
In order to configure EOC5510, please follow the instruction below:

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 and subnet mask. 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 then close LAN properties window.

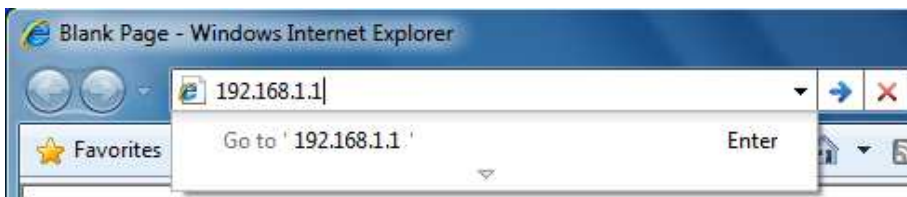


Auction: IP Address entered in the TCP/IP Properties needs to be at the same subnet of the EOC5510 IP Address. For example: EOC5510's default IP Address is **192.168.1.1** so the IP Address in the TCP/IP settings could be **192.168.1.10**.

### 3.2 Logging Method

After complete the IP settings from last section, you can now access the web-based configuration menu.

1. Open web browser



2. Enter IP **192.168.1.1** into you address filter.

Auction: If you have changed the EOC5510 LAN IP address, make sure you enter the correct IP Address.



3. After connected to the EOC5510 successfully, browser will pop out a Windows Security window. Please enter the correct **Username** and **Password**.

4. The default Username and Password are both **admin**.

Auction: If you have changed the Username and Password, please enter your own Username and Password.

## 4 Wireless Settings

### 4.1 Switching Operation Mode

The EOC5510 supports 4 different operation modes: Access Point, Client Bridge, WDS Bridge, and Client Router.

Click **System Properties** under System Section to begin.

**System Properties** Home Reset

---

Device Name	<input type="text" value="EOC5510"/> ( 1 to 32 characters )
Country/Region	<input type="text" value="United States"/>
Operation Mode	<input type="radio"/> Access Point <input checked="" type="radio"/> Client Bridge <input type="radio"/> WDS Bridge <input type="radio"/> Client Router

---

**Device Name:** Specify a name for the device, but it is not the broadcast SSID. It will be shown in SNMP management.

**Country/Region:** United States

**Operation Mode:** Select an operation mode via **Radio Button**.

Click **Apply** to save the changes.

Note: If you would like to use Access Point with WDS Function mode, please select Access Point

Mode and then enable WDS Link Settings function.

## 4.2 Wireless Settings

### 4.2.1 Access Point Mode -> Wireless Network

## Wireless Network

Home
Reset

---

<b>Wireless Mode</b>	802.11a (5GHz/54Mbps) ▾
<b>Channel / Frequency</b>	Ch48-5.24GHz ▾ <input type="checkbox"/> Auto
<b>AP Detection</b>	<input type="button" value="Scan"/>

---

Current Profiles				
SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius2	Open System/No Encryption	2	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius3	Open System/No Encryption	3	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius4	Open System/No Encryption	4	<input type="checkbox"/>	<input type="button" value="Edit"/>

---

<b>Profile (SSID)Isolation</b>	<input checked="" type="radio"/> No Isolation <input type="radio"/> Isolate all Profiles (SSIDs) from each other using VLAN (802.1Q) standard
--------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------

---

<b>Wireless Mode</b>	EOC5510 only supports 802.11a wireless band.
<b>Channel / Frequency</b>	The channel availability is based on the regulation of United States.
<b>Auto</b>	Place a <b>Check</b> to enable Auto channel selection.
<b>AP Detection</b>	AP Detection can help to select a best channel by scan nearby area.
<b>Current Profile</b>	Configure up to four different SSIDs, it can help to divide group of clients to access the network. Press <b>Edit</b> to configure the profile and place a <b>Check</b> to enable extra SSID.
<b>Profile Isolation</b>	Restricted Client to communicate with different VID by Selecting the Radio button.

Auction: EOC5510 supports 5GHz wireless network. Only the wireless client which supports 5GHz network can associate with. Please make sure your wireless client supports 5GHz wireless network.

## SSID Profile

---

### Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

### Wireless Security

Security Mode	Disabled ▼
---------------	------------

<b>SSID</b>	Specify the SSID for current profile.
<b>VLAN ID</b>	Specify the VLAN tag for current profile.
<b>Suppressed SSID</b>	Place a <b>Check</b> to hide the SSID. Client will not be able to see the broadcast SSID in Site Survey.
<b>Station Separation</b>	Select the Radio Button to allow / deny client to communicate each other.
<b>Wireless Security</b>	Please refer to the Wireless Security section.
<b>Save / Cancel</b>	Press <b>Save</b> to save the changes or <b>Cancel</b> to return previous settings.



## 4.2.2 Client Bridge Mode -> Wireless Network

### Wireless Network

[Home](#)
[Reset](#)

Wireless Mode	802.11a (5GHz/54Mbps) ▼
SSID	<p>Specify the static SSID :</p> <p>EnGenius ( 1 to 32 characters )</p> <p>Or press the button to search for any available WLAN Service.</p> <p><a href="#">Site Survey</a></p>
Prefer BSSID	<input type="checkbox"/> : : : : :
WDS Client	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

[Apply](#)
[Cancel](#)

<b>Wireless Mode</b>	EOC5510 only supports 802.11a wireless band.
<b>SSID</b>	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
<b>Site Survey</b>	Using Site Survey to scan nearby APs and then select the AP to establish the connection.
<b>Prefer BSSID</b>	Specify the MAC address if known. Prefer BSSID text box will be automatically fill in when select an AP in the Site Survey.
<b>WDS Client</b>	Place a Radio button to Enable / Disable WDS Client.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Note: Client Bridge only supports 5GHz wireless network.

### Site Survey

#### 5GHz Site Survey

📶:Infrastructure 📶:Ad\_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
-------	------	---------	--------	------	----------	--------------

[Refresh](#)

<b>Profile</b>	After Site Survey, webpage will display all nearby area's Access Point. Click the BSSID if you would like to connect with it.
<b>Wireless Security</b>	Please refer to the Wireless Security section.
<b>Refresh</b>	Press Refresh to scan again.

Auction: If the Access Point is suppressed its own SSID, SSID section will be blank, the SSID must be filled in manually.

### 4.2.3 WDS Bridge Mode -> Wireless Network

## Wireless Network

[Home](#)[Reset](#)

Wireless Mode	802.11a (5GHz/54Mbps) ▼
Channel / Frequency	Ch48-5.24GHz ▼

[Apply](#)[Cancel](#)

**Wireless Mode** EOC5510 only supports 802.11a wireless band.

**Channel / Frequency** The channel availability is based on the regulation of United States.

**Apply / Cancel** Press **Apply** to apply the changes or **Cancel** to return previous settings.

## WDS Link Settings

[Home](#)[Reset](#)

ID	MAC Address	Mode
1	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
5	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
6	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
7	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
8	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
9	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
10	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
11	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
12	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
13	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
14	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
15	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾
16	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable ▾

---

**MAC Address** Enter the Access Point's MAC address that you would like to extend the wireless area into the MAC address filter.

---

**Mode** Select Disable or Enable from the drop down list.

---

**Apply / Cancel** Press **Apply** to apply the changes or **Cancel** to return previous settings.

---

Auction: The Access Point that you would like to extend the wireless area must enter your Access Point's MAC address. Not all Access Point supports this feature.

## 4.2.4 Client Router Mode -> Wireless Network

### Wireless Network

[Home](#)
[Reset](#)

Wireless Mode	802.11a (5GHz/54Mbps) ▼
SSID	Specify the static SSID : <input type="text" value="EnGenius"/> ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Prefer BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>



<b>Wireless Mode</b>	EOC5510 only supports 802.11a wireless band.
<b>SSID</b>	Specify the SSID if known. SSID text box will be automatically fill in when select an AP in the Site Survey.
<b>Site Survey</b>	Using Site Survey to scan nearby APs and then select the AP to establish the connection.
<b>Prefer BSSID</b>	Specify the MAC address if known. Prefer BSSID text box will be automatically fill in when select an AP in the Site Survey.
<b>WDS Client</b>	Place a Radio button to Enable / Disable WDS Client.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Note: Client Bridge only supports 5GHz wireless network.

### Site Survey

#### 5GHz Site Survey

📶:Infrastructure 📶:Ad\_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
-------	------	---------	--------	------	----------	--------------

<b>Profile</b>	After Site Survey, webpage will display all nearby area's Access Point. Click the BSSID if you would like to connect with it.
<b>Wireless Security</b>	Please refer to the Wireless Security section.
<b>Refresh</b>	Press Refresh to scan again.

Auction: If the Access Point is suppressed its own SSID, SSID section will be blank, the SSID must be filled in manually.

### 4.3 Wireless Security Settings

Wireless Security Settings section will guide you to the entire Security modes configuration: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed.

We strongly recommend that uses WPA2-PSK as your security settings.

#### 4.3.1 WEP

##### Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

<b>Security Mode</b>	Select <b>WEP</b> from the drop down list to begin the configuration.
<b>Auth Type</b>	Select Auth Type in <b>Open System</b> or <b>Shared</b> .
<b>Input Type</b>	Select Input Type in <b>Hex</b> or <b>ASCII</b> .
<b>Key Length</b>	Select Key Length in 64/128/152 bit password length.
<b>Default Key</b>	Select the default index key for wireless security.
<b>Key1</b>	Specify password for security key index No.1.
<b>Key2</b>	Specify password for security key index No.2.
<b>Key3</b>	Specify password for security key index No.3.
<b>Key4</b>	Specify password for security key index No.4.

### 4.3.2 WPA-PSK

#### Wireless Security

Security Mode	WPA-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)

<b>Security Mode</b>	Select <b>WPA-PSK</b> from the drop down list to begin the configuration.
<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Passphrase</b>	Specify the security password.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.

### 4.3.3 WPA2-PSK

#### Wireless Security

Security Mode	WPA2-PSK
Encryption	Auto
Passphrase	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)

Save Cancel

<b>Security Mode</b>	Select <b>WPA2-PSK</b> from the drop down list to begin the configuration.
----------------------	----------------------------------------------------------------------------

<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Passphrase</b>	Specify the security password.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.

### 4.3.4 WPA-PSK Mixed

#### Wireless Security

<b>Security Mode</b>	WPA-PSK Mixed ▾
<b>Encryption</b>	Auto ▾
<b>Passphrase</b>	passphrase1 (8 to 63 characters) or (64 Hexadecimal characters)
<b>Group Key Update Interval</b>	3600 seconds(30~3600, 0: disabled)
<b>Group Key Update Timeout</b>	1 seconds(1~300)
<b>Pairwise Key Update Timeout</b>	1 seconds(1~300)

<b>Security Mode</b>	Select <b>WPA-PSK Mixed</b> from the drop down list to begin the configuration.
<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Passphrase</b>	Specify the security password.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.

Auction: WPA-PSK Mixed means it allow both WPA-PSK and WPA2-PSK security types to establish wireless connection.

### 4.3.5 WPA

WPA security mode is for 802.1x authentication. You must provide a **RADIUS Server** to check the permission of access the network.

#### Wireless Security

Security Mode	WPA
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable

<b>Security Mode</b>	Select <b>WPA</b> from the drop down list to begin the configuration.
<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Radius Server</b>	Specify Radius Server IP Address.
<b>Radius Port</b>	Specify Radius Port number, the default port is 1812.
<b>Radius Secret</b>	Specify Radius Secret that is given by the Radius Server.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.
<b>Radius Accounting</b>	Select <b>Enable</b> or <b>Disable</b> Radius Accounting. The detail of Radius Accounting is at next section.



### 4.3.6 WPA2

WPA2 security mode is for 802.1x authentication. You must provide a **RADIUS Server** to check the permission of access the network.

#### Wireless Security

Security Mode	WPA2
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable

<b>Security Mode</b>	Select <b>WPA2</b> from the drop down list to begin the configuration.
<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Radius Server</b>	Specify Radius Server IP Address.
<b>Radius Port</b>	Specify Radius Port number, the default port is 1812.
<b>Radius Secret</b>	Specify Radius Secret that is given by the Radius Server.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.
<b>Radius Accounting</b>	Select <b>Enable</b> or <b>Disable</b> Radius Accounting. The detail of Radius Accounting is at next section.

### 4.3.7 WPA Mixed

WPA Mixed security mode is for 802.1x authentication. You must provide a **RADIUS Server** to check the permission of access the network.

#### Wireless Security

Security Mode	WPA Mixed ▾
Encryption	Auto ▾
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Group Key Update Timeout	1 seconds(1~300)
Pairwise Key Update Timeout	1 seconds(1~300)
Radius Accounting	Disable ▾

<b>Security Mode</b>	Select <b>WPA Mixed</b> from the drop down list to begin the configuration.
<b>Encryption</b>	Select <b>Auto</b> , <b>TKIP</b> or <b>AES</b> for Encryption type.
<b>Radius Server</b>	Specify Radius Server IP Address.
<b>Radius Port</b>	Specify Radius Port number, the default port is 1812.
<b>Radius Secret</b>	Specify Radius Secret that is given by the Radius Server.
<b>Group Key Update Interval</b>	Specify Group Key Update Interval time.
<b>Group Key Update Timeout</b>	Specify Group Key Update Timeout time.
<b>Pairwise Key Update Interval</b>	Specify Pairwise Key Update Timeout time.
<b>Radius Accounting</b>	Select <b>Enable</b> or <b>Disable</b> Radius Accounting. The detail of Radius Accounting is at next section.

Auction: WPA Mixed means it allow both WPA and WPA2 security types to establish wireless connection.

### 4.3.8 Radius Accounting

**Radius Accounting** function allows you to record the statistics of user login. Your Radius Server must have the ability to support **Radius Accounting** function.

Radius Accounting	Enable ▾
Radius Accounting Server	0 . 0 . 0 . 0
Radius Accounting Port	1813
Radius Accounting Secret	secret1
Interim Accounting Interval	600 seconds(60~600)

---

<b>Radius Accounting</b>	Select <b>Enable</b> to begin configuration of Radius Accounting.
<b>Radius Accounting Server</b>	Specify Radius Accounting Server IP.
<b>Radius Accounting Port</b>	Specify Radius Accounting Server IP. The default port is 1813.
<b>Radius Accounting Secret</b>	Specify Radius Accounting Server Secret that is given by the Radius Accounting Server.
<b>Radius Accounting Interval</b>	Specify Radius Accounting Interval for updating information.

---

## 4.4 Wireless -> Wireless Advanced Settings

### Wireless Advanced Settings

[Home](#)
[Reset](#)

Data Rate	Auto ▾
Transmit Power	Auto
Antenna	Diversity ▾
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable ▾
WMM	Disable ▾
Channel Bandwidth	20MHz ▾
Distance (1-30km)	1 km

<b>Data Rate</b>	Select Data Rate from the drop down list. Data rate will affect the efficiency of the throughput. If the data rate is set to a small number, the lower through will get but it can transmit to longer distance.
<b>Transmit Power</b>	Auto
<b>Antenna</b>	Select antenna waveform from <b>Diversity, Vertical</b> or <b>Horizontal</b> .
<b>Fragment Length</b>	Specify package size during transmission. If large amount of client are accessing to the network, specify small number of the fragment length in order to avoid collision.
<b>RTS/CTS Threshold</b>	Specify Threshold package size for RTC/CTS. Using small number of the threshold will cause RTS/CTS packets to be sent more often to consuming more of the available bandwidth. In addition, if the heavy load traffic occurs, the wireless network can be recovered easily from interferences or collisions.
<b>Protection Mode</b>	Select <b>Disable</b> or <b>Enable</b> Protection Mode. If there are large amount of error occur during the transmission, please enable the protect mode otherwise protect mode should remain disable.
<b>WMM</b>	Select <b>Disable</b> or <b>Enable</b> WMM function. WMM is based on the four Access Categories: voice, video, best effort and background. WMM function is not used to guarantee transmission speed.
<b>Channel Bandwidth</b>	Select Channel Bandwidth from the drop down list. Decrease channel bandwidth may cause lower throughput but less collision.

---

<b>Distance</b>	Specify distance range between AP and Clients. Longer distance may lose high connection speed.
<b>Wireless Traffic Shaping</b>	Place a <b>Check</b> to enable Wireless Traffic Shaping function.
<b>Incoming Traffic Limit</b>	Specify the wireless transmission speed for downloading.
<b>Outgoing Traffic Limit</b>	Specify the wireless transmission speed for uploading.

---

Auction: Changing Wireless Advanced Settings may cause insufficient wireless connection quality. Please remain all settings as default unless you have acknowledged all changing that you have made.

## 4.5 Wireless -> Wireless MAC Filter

Wireless MAC Filters is used to Allow or Deny wireless clients, by their MAC addresses, accessing the Network. You can manually add a MAC address to restrict the permission to access EOC5510. The default setting is Disable Wireless MAC Filters.

**Wireless MAC Filter** [Home](#) [Reset](#)

---

ACL Mode

:  :  :  :  :  [Add](#)

#	MAC Address	
<a href="#">Apply</a>		

0.

<b>ACL Mode</b>	ACL Mode can help to deny or allow certain Client to access the network. Select Disable, Deny MAC in the list or Allow MAC in the list from the drop down list.
<b>MAC Address Filter</b>	Specify the MAC address manually.
<b>Add</b>	Press <b>Add</b> to add the MAC address in the table.
<b>Apply</b>	Press <b>Apply</b> to apply the changes.

## 4.6 Wireless -> WDS Link Settings

WDS Link Settings is used to establish a connection between Access Points but the device is not losing Access Point function. AP has WDS function can extend the wireless coverage and allow LANs to communicate each other.

### WDS Link Settings

Home

Reset

ID	MAC Address	Mode
1	: : : : :	Disable ▾
2	: : : : :	Disable ▾
3	: : : : :	Disable ▾
4	: : : : :	Disable ▾
5	: : : : :	Disable ▾
6	: : : : :	Disable ▾
7	: : : : :	Disable ▾
8	: : : : :	Disable ▾
9	: : : : :	Disable ▾
10	: : : : :	Disable ▾
11	: : : : :	Disable ▾
12	: : : : :	Disable ▾
13	: : : : :	Disable ▾
14	: : : : :	Disable ▾
15	: : : : :	Disable ▾
16	: : : : :	Disable ▾

Apply Cancel

**MAC Address** Enter the Access Point's MAC address that you would like to extend the wireless area.

**Mode** Select Disable or Enable from the drop down list.

**Apply / Cancel** Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: The Access Point that you would like to extend the wireless area must enter your Access Point's MAC address. Not all Access Point supports this feature.

## 5 LAN Settings

This section will guide you to the Local Area Network (LAN) settings

### 5.1 System -> IP Settings

This section is only available for **Non-Router Mode**. IP Settings allows you to LAN port IP address of the EOC5510.

Auction: Changing LAN IP Address will change LAN Interface IP address. Webpage will automatically redirect to the new IP address after Apply.

#### IP Settings

[Home](#)
[Reset](#)

IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address
IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0



<b>IP Network Setting</b>	Select Radio button for <b>Obtain an IP address automatically</b> or <b>Specify an IP address</b> .
<b>IP Address</b>	Specify LAN port IP address.
<b>IP Suet Mask</b>	Specify Subnet Mask.
<b>Default Gateway</b>	Specify Default Gateway
<b>Primary DNS</b>	Specify Primary DNS
<b>Secondary DNS</b>	Specify Secondary DNS
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Auction: Obtain an IP address automatically is not a DHCP server. It means automatically get IP address when device connected to a device which has DHCP server.



## 5.2 System -> Spanning Tree Settings

### Spanning Tree Settings

[Home](#)[Reset](#)

Spanning Tree Status	<input type="radio"/> On <input checked="" type="radio"/> Off
Bridge Hello Time	<input type="text" value="2"/> seconds (1-10)
Bridge Max Age	<input type="text" value="20"/> seconds (6-40)
Bridge Forward Delay	<input type="text" value="15"/> seconds (4-30)
Priority	<input type="text" value="32768"/> (0-65535)

[Apply](#)[Cancel](#)

<b>Spanning Tree Status</b>	Select the Radio button to On or Off Spanning Tree function.
<b>Bridge Hello Time</b>	Specify Bridge Hello Time in second.
<b>Bridge Max Age</b>	Specify Bridge Max Age in second.
<b>Bridge Forward Delay</b>	Specify Bridge Forward Delay in second.
<b>Priority</b>	Specify the Priority number. Smaller number has greater priority.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## **6 Router Settings**

This section is only available at **Client Router Mode**.

### **6.1 Router -> WAN Settings**

There are four different types of WAN connection: Static IP, DHCP, PPPoE and PPTP. Please contact your ISP to select the connection type.

#### **6.1.1 WAN Settings -> Static IP**

Select Static IP in WAN connection if your ISP gives all the information about IP address, Subnet Mask, Default Gateway, Primary DNS and Secondary DNS.

# WAN Settings

Home    Reset

Internet Connection Type	Static IP ▾
--------------------------	-------------

## Options

Account Name (if required)	<input type="text"/>
Domain Name (if required)	<input type="text"/>
MTU	Auto ▾ 1500

## Internet IP Address

IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
IP Subnet Mask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Gateway IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

## Domain Name Server (DNS) Address

Primary DNS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Secondary DNS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

## WAN Ping

Discard Ping on WAN	<input checked="" type="checkbox"/>
---------------------	-------------------------------------

Apply    Cancel

<b>Internet Connection Type</b>	Select <b>Static IP</b> to begin configuration of the Static IP connection.
<b>Account Name</b>	Specify Account Name that is provided by ISP.
<b>Domain Name</b>	Specify Domain Name that is provided by ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
<b>IP Address</b>	Specify WAN port IP address.
<b>IP Subnet Mask</b>	Specify WAN IP Subnet Mask.
<b>Gateway IP Address</b>	Specify WAN Gateway IP address.
<b>Primary DNS</b>	Specify Primary DNS IP.
<b>Secondary DNS</b>	Specify Secondary DNS IP.
<b>Discard Ping on WAN</b>	Place a Check to Enable or Disable ping from WAN.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Auction: If the router's MTU is set too high, packets will be fragmented downstream. If the router's

MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

## 6.1.2 WAN Settings -> DHCP (Dynamic IP)

Select DHCP as your WAN connection type to obtain your IP address automatically. You will need to enter Account Name as your hostname and DNS (Optional).

### WAN Settings

[Home](#)
[Reset](#)

Internet Connection Type DHCP ▾

#### Options

Account Name (if required)

Domain Name (if required)

MTU Auto ▾ 1500

#### Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

#### WAN Ping

Discard Ping on WAN



<b>Internet Connection Type</b>	Select <b>DHCP</b> to begin configuration of the DHCP connection.
<b>Account Name</b>	Specify Account Name that is provided by ISP.
<b>Domain Name</b>	Specify Domain Name that is provided by ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
<b>Get Automatically From ISP</b>	Select the Radio button for get the DNS automatically from DHCP server.
<b>Use These DNS Servers</b>	Select the Radio button for setup the <b>Primary DNS</b> and <b>Secondary DNS</b> servers manually.
<b>Discard Ping on WAN</b>	Place a Check to Enable or Disable ping from WAN.

---

**Apply / Cancel**

Press **Apply** to apply the changes or **Cancel** to return previous settings.

---

Auction: If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

### 6.1.3 WAN Settings -> PPPoE (Point-to-Point Protocol over Ethernet)

Select PPPoE as your WAN connection type if your ISP provides Username and Password. PPPoE is a DSL service and please remove your PPPoE software from your computer, the software is not worked in EOC5510.

#### WAN Settings

[Home](#)
[Reset](#)

Internet Connection Type

PPPoE ▼

#### Options

MTU

Auto ▼ 1492

#### PPPoE Options

Login

Password

Service Name (if required)

Connect on Demand: Max idle Time 1 Minutes

Keep Alive: Redial Period 30 Seconds

Get Automatically From ISP

Use These DNS Servers

Primary DNS

 .  .  . 

Secondary DNS

 .  .  . 

#### WAN Ping

Discard Ping on WAN




**Internet Connection Type** Select **PPPoE** to begin configuration of the PPPoE connection.

**MTU** Specify the Maximum Transmit Unit size. Suggest remain in Auto.

**Login** Specify the **Username** that is given by your ISP.

**Password** Specify the **Password** that is given by your ISP.

**Service Name** Specify the **Service Name** that is given by your ISP.

---

<b>Connect on Demand</b>	Select the Radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
<b>Keep Alive</b>	Select the Radio button to keep internet connection always on. Specify the redial period once the internet lose connection.
<b>Get Automatically From ISP</b>	Select the Radio button for get the DNS automatically from DHCP server.
<b>Use These DNS Servers</b>	Select the Radio button for setup the <b>Primary DNS</b> and <b>Secondary DNS</b> servers manually.
<b>Discard Ping on WAN</b>	Place a Check to Enable or Disable ping from WAN.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

---

Auction: If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.



## 6.1.4 WAN Settings -> PPTP (Point-to-Point Tunneling Protocol)

Select PPTP as your WAN connection type if your ISP provides information about IP Address, Subnet Mask, Default Gateway (Optional), DNS (Optional), Server IP, Username, and Password.

### WAN Settings

[Home](#)[Reset](#)

Internet Connection Type PPTP

#### Options

MTU Auto 1460

#### PPTP Options

IP Address 192 . 168 . 2 . 1

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 2 . 100

PPTP Server 0 . 0 . 0 . 0

Username

Password

Connect on Demand: Max idle Time 15 Minutes

Keep Alive: Redial Period 30 Seconds

Get Automatically From ISP

Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

#### WAN Ping

Discard Ping on WAN

**Internet Connection Type** Select **PPTP** to begin configuration of the PPTP connection.

<b>MTU</b>	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
<b>IP Address</b>	Specify WAN port IP address.
<b>IP Subnet Mask</b>	Specify WAN IP Subnet Mask.
<b>Gateway IP Address</b>	Specify WAN Gateway IP address.
<b>PPTP Server</b>	Specify PPTP Server IP address.
<b>Username</b>	Specify the <b>Username</b> that is given by your ISP.
<b>Password</b>	Specify the <b>Password</b> that is given by your ISP.
<b>Connect on Demand</b>	Select the Radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
<b>Keep Alive</b>	Select the Radio button to keep internet connection always on. Specify the redial period once the internet lose connection.
<b>Get Automatically From ISP</b>	Select the Radio button for get the DNS automatically from DHCP server.
<b>Use These DNS Servers</b>	Select the Radio button for setup the <b>Primary DNS</b> and <b>Secondary DNS</b> servers manually.
<b>Discard Ping on WAN</b>	Place a Check to Enable or Disable ping from WAN.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Auction: If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

## 6.2 Router -> LAN Settings

### LAN Settings

[Home](#)[Reset](#)

#### LAN IP Setup

IP Address	192 . 168 . 1 . 1
IP Subnet Mask	255 . 255 . 255 . 0
WINS Server IP	0 . 0 . 0 . 0

 Use Router As DHCP Server

Starting IP Address	192 . 168 . 1 . 2
Ending IP Address	192 . 168 . 1 . 254

<b>IP Address</b>	Specify LAN port IP address.
<b>IP Subnet Mask</b>	Specify LAN IP Subnet Mask.
<b>WINS Server IP</b>	Specify WINS Server IP.
<b>Use Router As DHCP Server</b>	Place a <b>Check</b> to enable DHCP server.
<b>Starting IP Address</b>	Specify DHCP server starting IP address.
<b>Ending IP Address</b>	Specify DHCP server ending IP address.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

### 6.3 Router -> VPN Pass Through

VPN Pass Through is used to allow certain protocol to be tunneled through an IP network such as PPTP and L2TP or implement secure exchange of packets at the IP Layer such as IPSec.

#### VPN Pass Through

[Home](#)[Reset](#)

- PPTP Pass Through
- L2TP Pass Through
- IPSec Pass Through

[Apply](#) [Cancel](#)

<b>PPTP Pass Through</b>	Place a <b>Check</b> to enable PPTP protocol passes through WAN.
<b>L2TP Pass Through</b>	Place a <b>Check</b> to enable L2TP protocol passes through WAN.
<b>IPSec Pass Through</b>	Place a <b>Check</b> to enable IPSec protocol passes through WAN.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## 6.4 Router -> Port Forwarding

Port Forwarding is used to allow a public service such as Web Server, Mail Server, and FTP server to be set up. For example: Set up a Web Server on your computer with port number **8080**. Visitor on the internet can access your Web Server by entering **WAN Port IP** with port number **8080**. If your WAN Port IP is 192.168.5.1, then visitor must enter **http://192.168.5.1:8080**. To find out more the well known port numbers please search the internet.

### Port Forwarding

[Home](#)
[Reset](#)

#	Name	Protocol	Start Port	End Port	Server IP Address	Enable	Modify	Delete
---	------	----------	------------	----------	-------------------	--------	--------	--------

[Add Entry](#)
[Apply](#)

#### Add Entry

Press Add Entry to add a rule of Port Forwarding.

#### Apply

Press **Apply** to apply the changes.

#### Service Name

Specify a name for current Port Forwarding rule.

#### Protocol

Select a protocol from drop down list: Both, TCP and UDP.

#### Starting Port

Specify Starting Port number.

#### Ending Port

Specify Ending Port number.

---

<b>IP Address</b>	Specify IP address.
<b>Save / Cancel</b>	Press <b>Save</b> to apply the changes or <b>Cancel</b> to return previous settings.

---

## 7 Information Status

**Status** section is on the navigation drop-down menu. You will then see three options: Main, Wireless Client List, System Log, WDS Link Status, Connection Status, and DHCP Client Table. Each option is described in detail below.

### 7.1 Status -> Main

Click on the **Main** link under the **Status** drop-down menu or click **Home** from the top-right of the webpage. The status that is displayed corresponds with the operating mode that is selected. Information such as operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless section, the frequency, channel is displayed. Since this device supports multiple-SSIDs, the details of each SSID, such as ESSID and its security settings are displayed.

## Main

---

### System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:09:0a:12
Wireless MAC Address	00:02:6f:10:0a:13
Country	N/A
Current Time	Sat Jan 1 00:16:45 UTC 2000
Firmware Version	1.0.27
Management VLAN ID	Untagged

### LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

### Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	Current Frequency:2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1
	2 N/A
	3 N/A
	4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

---

Refresh

## 7.2 Status -> Wireless Client List

Click on the **Wireless Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the EOC5510.

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

## Client List

[Home](#)[Reset](#)

#

MAC Address

RSSI(dBm)

[Refresh](#)

### 7.3 Status -> System Log

Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

## System Log

[Home](#)[Reset](#)Show log type All ▼

Local Log is disabled.

[Refresh](#)[Clear](#)



## 7.4 Status -> WDS Link Status

The WDS Link Status will only show in WDS Bridge Mode. Click on the **WDS Link Status** link under the **Status** drop-down menu. This page displays the current status of WDS link, including station ID, MAC address, status and RSSI.

### WDS Link Status

[Home](#)[Reset](#)

Station ID	MAC Address	Status	RSSI (dBm)
------------	-------------	--------	------------

[Refresh](#)

## 7.5 Status -> Connection Status

Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

## Wireless

Network Type	Client Router
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

## WAN

MAC Address	00:02:6f:75:9f:a8
Connection Type	Static IP
Connection Status	Down
IP Address	
IP Subnet Mask	0.0.0.0

Refresh

## 7.6 Status -> DHCP Client Table

Click on the **DHCP Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the EOC5510 through DHCP.

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

## DHCP Client List

Home

Reset

MAC addr	IP	Expires
----------	----	---------

Refresh

## 8 Management Settings

**Management** section is on the navigation drop-down menu. You will then see seven options: administration, management VLAN, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

### 8.1 Management -> Administration

Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured with a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.

## Administrator

Name	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
Confirm Password	<input type="password" value="•••••"/>

<b>Name</b>	Specify Username for login.
<b>Password</b>	Specify a Password for login
<b>Confirm Password</b>	Re-enter the Password for confirmation.

## Remote Access

Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Upgrade	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management Port	<input type="text" value="8080"/>

<b>Remote Management</b>	Select the Radio button to Enable or Disable Remote Management.
<b>Remote Upgrade</b>	Select the Radio button to Enable or Disable Remote Upgrade.
<b>Remote Management Port</b>	Specify the Port number for Remote Management. For example: If you specify the Port number is 8080, then you will need to enter following <code>http://&lt;IP address&gt;:8080</code> to access the web interface.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## 8.2 Management -> Management VLAN

Click on the **Management VLAN** link under the **Management** menu. This option allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN

## Management VLAN Settings

[Home](#)[Reset](#)

**Caution:** If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID

- No VLAN tag
- Specified VLAN ID   
(must be in the range 1 ~ 4095. )

[Apply](#)[Cancel](#)

### Management VLAN ID

If your network includes VLANs and if tagged packets need to pass through the Access Point, specify the VLAN ID into this field. If not, select the **No VLAN tag** radio button.

### Apply / Cancel

Press **Apply** to apply the changes or **Cancel** to return previous settings.

Auction: If you reconfigure the Management VLAN ID, you may lose connection to the EOC5510. Verify DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

## 8.3 Management -> SNMP Settings

Click on the **SNMP Settings** link under the **Management** menu. 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 Settings

Home

Reset

SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

Apply

Cancel

<b>SNMP Enable/Disable</b>	Select the Radio button to Enable or Disable SNMP function.
<b>Contact</b>	Specify the contact details of the device.
<b>Location</b>	Specify the location of the device.
<b>Community Name</b>	Specify the password for access the SNMP community for read only access.
<b>Community Name</b>	Specify the password for access the SNMP community for read and write access.
<b>Trap Destination IP Address</b>	Specify the IP address that will receive the SNMP trap.
<b>Trap Destination Community Name</b>	Specify the password of the SNMP trap community.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## 8.4 Management -> Backup/Restore Settings

Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

## Backup/Restore Settings

[Home](#)[Reset](#)

Save A Copy of Current Settings

Restore Saved Settings from A File

Revert to Factory Default Settings

---

### Save A Copy of Current Settings

Click on **Backup** to save current configured settings.

---

### Restore Saved Settings from a File

EOC5510 can restore a previous setting that has been saved. Click on Browse to select the file and Restore.

---

### Revert to Factory Default Settings

Click on Factory Default button to reset all the settings to the default values.

---

## 8.5 Management -> Firmware Upgrade

Click on the **Firmware Upgrade** link under the **Management** menu. This page is used to upgrade the firmware of the device. Make sure that downloaded the appropriate firmware from your vendor.

## Firmware Upgrade

[Home](#)[Reset](#)

Current firmware version: 1.1.24

Locate and select the upgrade file from your hard disk:

---

Auction: Upgrade process may take few minutes, please do not power off the device and it may cause the device crashed or unusable. EOC5510 will restart automatically once the upgrade is completed.

## 8.6 Management -> Time Settings

Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

## Time Settings

[Home](#)[Reset](#)

### Time

**Manually Set Date and Time**

2000 / 01 / 01 02 : 45

**Automatically Get Date and Time**

Time Zone: UTC+00:00 England

**User defined NTP Server:** 0 . 0 . 0 . 0

[Apply](#)[Cancel](#)

---

### Manually Set Date and Time

Manually setup the date and time.

---

### Automatically Get Date and Time

Specify the Time Zone from the drop down list and Place a **Check** to specify the IP address of the NTP Server manually or uses default NTP Server.

---

### Apply / Cancel

Press **Apply** to apply the changes or **Cancel** to return previous settings.

---

## 8.7 Management -> Log

Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are



triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

## Log

Home

Reset

### Syslog

Syslog	Disable ▾
Log Server IP Address	0 . 0 . 0 . 0

### Local log

Local Log	Disable ▾
-----------	-----------

Apply

Cancel

<b>Syslog</b>	Select Enable or Disable Syslog function from the drop down list.
<b>Log Server IP Address</b>	Specify the Log Server IP address.
<b>Local Log</b>	Select Enable or Disable Local Log service.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## 8.8 Management -> Diagnostics

Click on the **Diagnostics** link under the **Management** menu. This function allows you to detect

connection quality and trace the routing table to the target.

## Diagnostics

Home

Reset

### Ping Test Parameters

Target IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Ping Packet Size	64 <input type="text"/> Bytes
Number of Pings	4 <input type="text"/>

Start Ping

### Traceroute Test Parameters

Traceroute target	<input type="text"/>
-------------------	----------------------

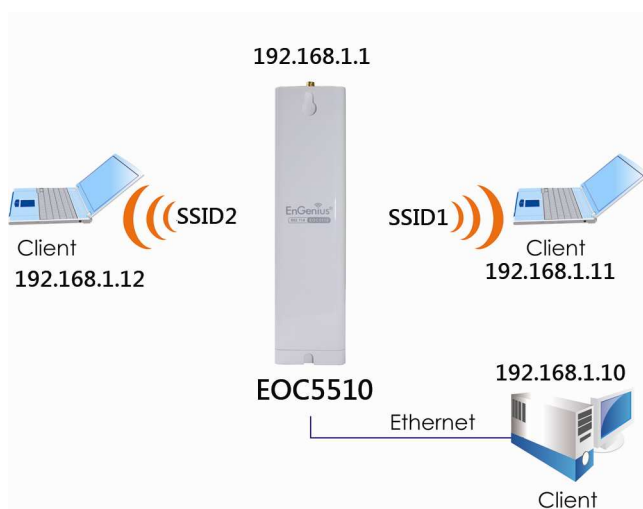
Start Traceroute

<b>Target IP</b>	Specify the IP address you would like to search.
<b>Ping Packet Size</b>	Specify the packet size of each ping.
<b>Number of Pings</b>	Specify how many times of ping.
<b>Start Ping</b>	Press Start Ping to begin.
<b>Traceroute Target</b>	Specify an IP address or Domain name you would like to trace.
<b>Start Traceroute</b>	Press Start Traceroute to begin.

## 9 Network Configuration Example

This chapter describes the role of the EOC5510 with 4 different modes. The Access Point mode's default configuration is a central unit of the wireless network or as a root device of the wired environment.

### 9.1 Access Point




---

#### **Access Point**

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.1
<b>Step2</b>	802.11a wireless network
<b>Step3</b>	Use site survey to scan channels that have been used in nearby area.
<b>Step4</b>	Select channel with less interferences.
<b>Step5</b>	Specify the SSID for your broadcast SSID and you can also configure multiple SSID at the same time.
<b>Step6</b>	Verify VLAN identifier to separate services among clients
<b>Step7</b>	Setup the authentication settings.
<b>Step8</b>	Press Apply to save all changes.

Note: For more advanced settings, please refer to the previous chapters.

---

#### **Wireless Client**

<b>Step1</b>	Select wireless mode you would like to associate with.
<b>Step2</b>	Use site survey to scan nearby Access Point and select the certain AP you would like to connect with or enter SSID manually.

---

<b>Step3</b>	Configure VLAN ID in your wireless device if available.
<b>Step4</b>	Select correct authentication type and password.

Auction: EOC5510's Access Point Mode does not provide DHCP server so the Wireless Client IP address must configure manually at the same subnet in Local Area Network.

## 9.2 Client Bridge Mode

Client Bridge Mode functions like a wireless dongle. It must connect to an Access Point/AP Router to join the network.



Please refer to the last section to check Access point's configuration.

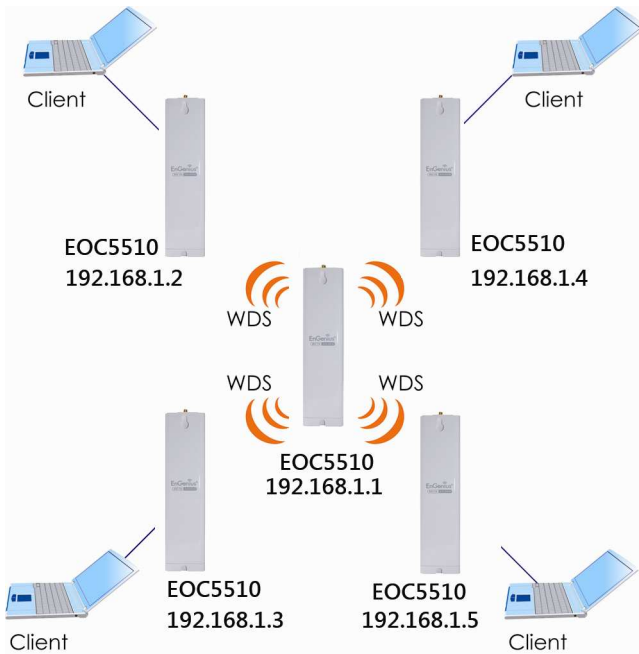
### ***Client Bridge***

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.1
<b>Step2</b>	Select <b>Operation Mode</b> to <b>Client Bridge</b> from <b>System Properties</b> .
<b>Step3</b>	802.11a (5GHz) wireless network.
<b>Step4</b>	Use site survey to scan Access Points that are available in nearby area.
<b>Step5</b>	Select the AP you would like to associate with.
<b>Step6</b>	Setup the authentication settings that match to the Access Point's setting.
<b>Step7</b>	Press Apply to process all the configurations.

Auction: Client Bridge's IP setting must match to the Access Point's subnet.

## 9.3 WDS Bridge Mode

Use this feature to link multiple APs in a network. All clients associated with any APs can communicate each other like an ad-hoc mode.




---

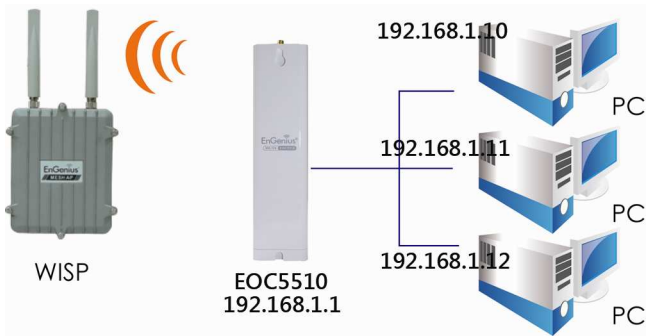
### **WDS Bridge**

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.1
<b>Step2</b>	Select <b>Operation Mode</b> to <b>WDS Bridge</b> from <b>System Properties</b> .
<b>Step3</b>	802.11a (5GHz) wireless network.
<b>Step4</b>	Select channel you would like to use.
<b>Step5</b>	Setup the authentication settings
<b>Step6</b>	Setup WDS Link Settings.
<b>Step7</b>	Specify the AP's MAC address you would like to connect with.
<b>Step8</b>	Press Apply to process all the configurations.

Auction: Each WDS bridge's device must use the same **Subnet**, **Wireless Mode**, **Wireless Channel**, and **Security Setting**.

## **9.4 Client Router**

In the Client Router Mode, the EOC5510 has DHCP Server build inside that allows many LANs automatically generate an IP address to share the same Internet. Connect an AP/WISP Wirelessly and connect to LANs via wired. Client Router Mode is act completely opposite to the AP Router Mode.



Please refer to the last section to check Access point's configuration.

### **Client Router**

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.1
<b>Step2</b>	Select <b>Operation Mode</b> to <b>Client Router</b> from <b>System Properties</b> .
<b>Step3</b>	Change your <b>Local Area Network</b> setting to <b>Obtain an IP Address Automatically</b> .
<b>Step4</b>	802.11a (5GHz) wireless network.
<b>Step5</b>	Use site survey to scan Access Points that are available in nearby area.
<b>Step6</b>	Select the AP you would like to associate with.
<b>Step7</b>	Setup the authentication settings that match to the Access Point's setting.
<b>Step8</b>	Setup your WAN connection type given by your <b>Internet Service Provider</b> from <b>WAN Settings</b> .
<b>Step9</b>	Press Apply to process all the configurations.

Auction: Client Router's IP setting must match to the Access Point's subnet.

# Appendix A – FCC Interference Statement

---

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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.

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

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:**

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

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

## Appendix B – IC Interference Statement

---

### Industry Canada statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### IMPORTANT NOTE:

#### Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

#### Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

This device has been designed to operate with an antenna having a maximum gain of 5 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.