

**Dual Radio Concurrent AP/CB**

# **EOA7535**



## **User Manual**

**Version : 1.0**

# Table of Contents

<b>1 PRODUCT OVERVIEW .....</b>	<b>3</b>
1.1 BENEFITS.....	3
1.2 FEATURE.....	5
1.3 PACKAGE CONTENTS .....	6
1.4 SYSTEM REQUIREMENT .....	6
1.5 HARDWARE OVERVIEW .....	6
<b>2 EOA7535 MULTI-FUNCTION INSTRUCTION GUIDE .....</b>	<b>7</b>
2.1 ACCESS POINT .....	7
2.2 CLIENT BRIDGE .....	7
2.3 CLIENT ROUTER .....	8
<b>3 COMPUTER CONFIGURATION INSTRUCTION.....</b>	<b>9</b>
3.1 OBTAIN AN IP AUTOMATICALLY .....	9
3.2 LOGGING METHOD.....	10
<b>4 WIRELESS CONFIGURATION .....</b>	<b>11</b>
4.1 SWITCHING OPERATION MODE .....	11
4.1.1 <i>Separate Mode</i> .....	11
4.1.2 <i>Dual Mode</i> .....	12
4.2 WIRELESS SETTINGS .....	12
4.2.1 <i>Access Point Mode (Dual Mode)</i> .....	13
4.2.2 <i>Access Point Mode (5G)</i> .....	14
4.2.3 <i>Access Point Mode (2.4G)</i> .....	15
4.2.4 <i>Client Bridge Mode/Client Router Mode (Dual Mode)</i> .....	16
4.2.5 <i>Client Bridge Mode/Client Router Mode (5G)</i> .....	17
4.2.6 <i>Client Bridge Mode/Client Router Mode (2.4G)</i> .....	17
4.3 SITE SURVEY .....	18
4.4 AP SCAN LIST (5G / 2.4G).....	18
4.5 WIRELESS SECURITY SETTINGS .....	18
4.5.1 <i>WEP (Access Point)</i> .....	19
4.5.2 <i>WEP (Client Bridge / Client Router)</i> .....	20
4.5.3 <i>WPA pre-shared Key (Access Point)</i> .....	21
4.5.4 <i>WPA pre-shared Key (Client Bridge / Client Router)</i> .....	22
4.5.5 <i>Radius (Access Point Only)</i> .....	23
4.6 WIRELESS ADVANCED SETTINGS.....	24
4.6.1 <i>Advanced Settings (Access Point)</i> .....	24
4.6.2 <i>Advanced Settings (Client Bridge / Client Router)</i> .....	25
4.7 WIRELESS ACCESS CONTROL LIST .....	26

<b>5 LAN SETUP .....</b>	<b>26</b>
5.1 LAN SETTINGS .....	27
5.2 DHCP INFO .....	28
5.3 SNMP SETTINGS .....	29
<b>6 INTERNET SETTINGS .....</b>	<b>30</b>
6.1 DHCP (DYNAMIC IP) .....	30
6.2 STATIC IP .....	30
6.3 PPPoE (POINT-TO-POINT PROTOCOL OVER ETHERNET) .....	31
6.4 PPTP (POINT-TO-POINT TUNNELING PROTOCOL) .....	32
<b>7 INFORMATION STATUS .....</b>	<b>34</b>
7.1 STATUS .....	34
7.2 WIRELESS CLIENT LIST .....	35
7.3 SYSTEM LOG .....	35
7.4 INTERNET STATUS .....	36
<b>8 MANAGEMENT SETTINGS .....</b>	<b>37</b>
8.1 PASSWORD SETTINGS .....	37
8.2 TIME ZONE SETTINGS .....	37
8.3 DIAGNOSIS .....	38
8.4 REMOTE CONTROL .....	39
8.5 UPGRADE FIRMWARE .....	39
8.6 SAVE/RELOAD SETTINGS .....	39
<b>9 NETWORK CONFIGURATION EXAMPLE .....</b>	<b>41</b>
9.1 ACCESS POINT MODE + CLIENT BRIDGE MODE .....	41
9.2 CLIENT ROUTER MODE .....	42
<b>APPENDIX A – FCC INTERFERENCE STATEMENT .....</b>	<b>43</b>

## 1 Product Overview

Thank you for using EOA7535. EOA7535 is a dual core wireless outdoor Access Point/Client Bridge. It is a powerful, enhanced, enterprise scale product with 3 multi-functions Access Point, Client Bridge, and Client Router in both 2.4G and 5G operation mode. EOA7535 can help with reducing costs with wired internet/intranet and even constructing wireless environment.

EOA7535 is easily to install almost anywhere by wall mount. It supports Power over Ethernet for quick outdoor installation. External N-type antenna provides better wireless signal quality and the antenna is upgradeable.

EOA7535 can manage power level control, Wireless Access Control, WMM and Real-time RSSI indicator. EOA7535 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 Radius encryption.

### 1.1 Benefits

The following list describes the design of the EOA7535 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>Benefits</b>	
<b>Dual Core Wireless Network</b>	Capable of functioning both 2.4G and 5G network at the same time.
<b>High Output Power up to 28 dBm</b>	Extended excellent Range and Coverage.
<b>IEEE 802.11b/g Compliant</b>	Fully Interoperable with IEEE 802.11b/IEEE 802.11g compliant devices.
<b>IEEE 802.11a</b>	Fully Interoperable with IEEE 802.11a compliant devices.
<b>Watertight and Weatherproof</b>	Avoid water invaded and weather corroded for outdoor environment.
<b>Wall mount and mast mounting kit support</b>	Building on indoor environment easily.
<b>Internal smart antenna</b>	Diversity antenna gives better coverage of wireless signal for indoor environment.
<b>3 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>Support RSSI Indicator</b>	Access Point will show the signal quality for each client.
<b>Power-over-Ethernet</b>	Flexible Access Point locations and cost savings. EOA7535 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>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.
<b>Detachable antenna support (N-Type)</b>	Collocate with any antenna for user's environment

<b>PPPoE/PPTP function support (CR mode)</b>	Easy to access internet via ISP service authentication
--	--

## 1.2 Feature

<b>Dual Mode</b>	Use this feature to configure 2.4G and 5G at the same time. Both 2.4G and 5G are functioning in the Access Point mode and it can save much time of configuration.
<b>Separate Mode</b>	Use this feature to configure 2.4G and 5G separately. 2.4G and 5G can function with different operation modes and it gives flexible choice of the wireless network.
<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>Client Router Mode</b>	Client Router Mode has the same abilities as Client Bridge Mode but it also supports WAN type of internet connection.
<b>Multiple SSIDs</b>	EOA7535 supports up to 4 SSIDs on your access point. The following options can be set to each SSID: <ul style="list-style-type: none"> <li>- SSID for public or private network</li> <li>- Each SSID can be suppressed.</li> <li>- Authentication is fully supported</li> <li>- VLAN identifier</li> </ul>
<b>VLAN</b>	Specify a VLAN number for each SSID to separate the services among clients.
<b>WMM</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\* EnGenius Dual Concurrent Wireless Outdoor Access Point / Client Bridge (EOA7535)
- 1\* 48V/0.375A Power Adapter
- 1\* Mounting kit
- 1\* QIG
- 1\* CD (User Manual)
- 2\*Dipole Antennas

Auction: Using other Power Adapter than the one included with EOA7535 may cause damage of the device.

### 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

MCU	Atheros AR7161
RF	Atheros AR5413 (Radio1) + Atheros AR5413 (Radio2)
Memory	64MB SDRAM
Flash	8MB
Physical Interface	One 10/100 Ethernet RJ-45 One Reset Button
Power Requirements	Power over Ethernet, 48V DC IN

## 2 EOA7535 Multi-Function Instruction Guide

### 2.1 Access Point

In the Access Point Mode with WDS Function, EOA7535 function like a central connection for any stations or clients that support IEEE 802.11b/g network. Stations and Client must configure the same SSID and Security Password to associate within the range. EOA7535 supports 4 different SSIDs to separate different clients at the same time.



### 2.2 Client Bridge

In the Client Bridge Mode, the EOA7535 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 EOA7535 via Ethernet.





## 2.3 Client Router

In the Client Router Mode, the EOA7535 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.



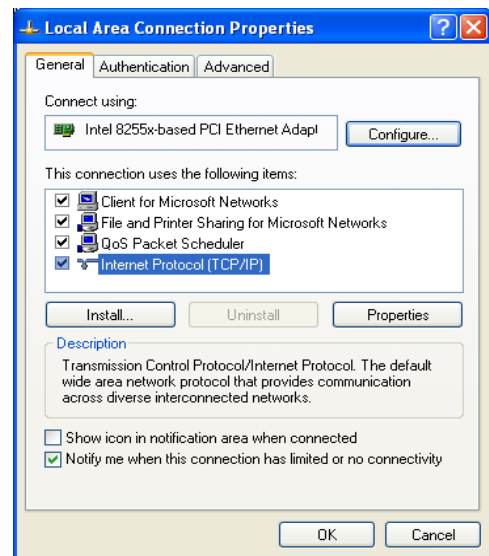
### 3 Computer Configuration Instruction

#### 3.1 Obtain an IP Automatically

In order to configure EOA7535, please follow the instruction below:

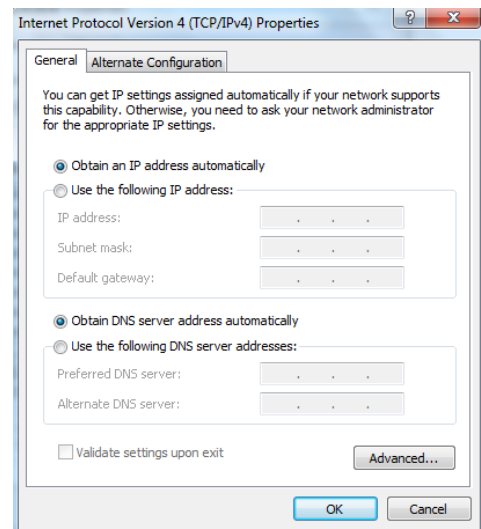
1. In the **Control Panel**, double click **Network Connections** and then double click on the connection of your **Network Interface Card (NIC)**. You will then see the following screen.

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 **Obtain an IP Address automatically** 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.

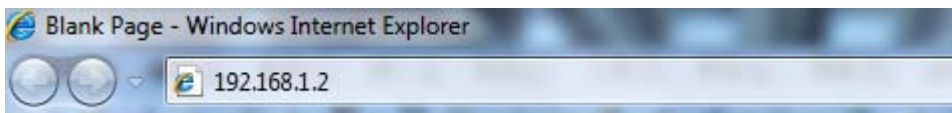


Auction: EOA7535 has provided DHCP server in the default setting. You should automatically retrieve an IP address otherwise use an IP address which is in the same subnet as the device.

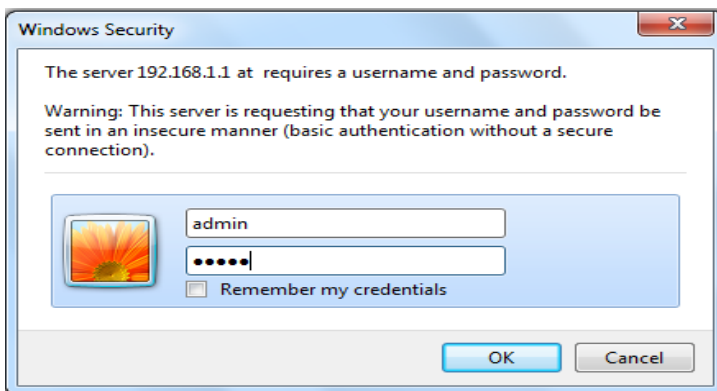
## 3.2 Logging Method

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

1. Open web browser
2. Enter IP **192.168.1.2** into you address filter.



Auction: If you have changed the EOA7535 LAN IP address, make sure you enter the correct IP Address.



3. After connected to the EOA7535 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 Password, please enter your own Password. The Username cannot be changed.

## 4 Wireless Configuration

### 4.1 Switching Operation Mode

The EOA7535 supports 3 different operation modes: Access Point, Client Bridge, and Client Router. Each mode can be used in both 2.4G and 5G wireless network at the same time or separately.

Click **Operation Mode** under Management Section to begin.

#### 4.1.1 Separate Mode

5G's and 2.4G's networks can operate separately by selecting **Separate Mode's** radio button.

Dual Mode  Separate Mode

Please choose the Operation Mode.(5G)

Access Point Mode

Client Bridge Mode

Client Router Mode

Please choose the Operation Mode.(2.4G)

Access Point Mode

Client Bridge Mode

Client Router Mode

**Operation Mode (5G):** Select which operation modes you would like to use in 5G network.

**Operation Mode (2.4G):** Select which operation modes you would like to use in 2.4G network.

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

Auction: **Client Bridge Mode** and **Client Router Mode** can not be used at the same time.

Note: If you would like to use the Access Point mode in both 5G and 2.4G network, please check next section for details.

### 4.1.2 Dual Mode

Only Access Point Mode can operate 2.4G and 5G at the same time. However, Client Bridge/Client Router can still select 2.4G and 5G network in the wireless basic settings. Please select the **Dual Mode**'s radio button to begin.

Dual Mode  Separate Mode

Please choose the Operation Mode.

Access Point Mode

Client Bridge Mode

Client Router Mode

Please Choose which Radio is Enabled.

5G Radio

2.4G Radio

**Operation Mode:** Only Access Point mode can be worked in 5G and 2.4G at the same time.

**5G / 2.4G Radio Button:** In the Access Point mode, the radio buttons will be locked because both bands can work at the same time. Select the 5G or 2.4G radio button to access the wireless network. You can still change bands in the wireless basic settings.

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

### 4.2 Wireless Settings

Configuration is under **Wireless** Section on the left-hand-side menu.

## 4.2.1 Access Point Mode (Dual Mode)

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

Radio:  Enable  Disable

Enabled SSID#: 1 ▾

ESSID1: EnGenius VID1 : 1 (1-4095)

### 5G Wireless Settings:

Band: 5 GHz (A) ▾

Channel: 44 -5.220 GHz ▾

Data Rate: Auto ▾

Auto Channel:  Enable  Disable

### 2.4G Wireless Settings:

Band: 2.4 GHz (B+G) ▾

Channel: 6 - 2.437 GHz ▾

Data Rate: Auto ▾

Auto Channel:  Enable  Disable

Apply Cancel

<b>Radio</b>	Select the radio button to enable or disable wireless function.
<b>Enable SSID#</b>	EOA7535 can support up to 4 different SSID with different VLAN tag.
<b>ESSID</b>	Specify the broadcast SSID and VLAN ID for each ESSID.
<b>5G Wireless Settings</b>	
<b>Band</b>	Standard IEEE 802.11a band.
<b>Channel</b>	Select a channel from drop down menu.
<b>Data Rate</b>	Select the data rate from drop down menu. 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>Auto Channel</b>	Select the radio button to enable auto channel function.
<b>2.4G Wireless Settings</b>	
<b>Band</b>	Standard IEEE 802.11b and 802.11g band.
<b>Channel</b>	Select a channel from drop down menu.
<b>Data Rate</b>	Select the data rate from drop down menu. 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>Auto Channel</b>	Select the radio button to enable auto channel function.

---

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

---

Auction: Both 5G and 2.4G bands are using the same SSID.

## 4.2.2 Access Point Mode (5G)

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

Radio:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Enabled SSID#:	1 ▾			
ESSID1:	EnGenius	VID1 :	1	(1-4095)

---

### 5G Wireless Settings:

Band:	5 GHz (A) ▾
Channel:	44 -5.220 GHz ▾
Data rate:	Auto ▾
Auto Channel:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

---

---

<b>Radio</b>	Select the radio button to enable or disable wireless function.
<b>Enable SSID#</b>	EOA7535 can support up to 4 different SSID with different VLAN tag.
<b>ESSID</b>	Specify the broadcast SSID and VLAN ID for each ESSID.
<b>5G Wireless Settings</b>	
<b>Band</b>	Standard IEEE 802.11a band.
<b>Channel</b>	Select a channel from drop down menu.
<b>Data Rate</b>	Select the data rate from drop down menu. 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>Auto Channel</b>	Select the radio button to enable auto channel function.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

---

Auction: If you do not have experience of data rate setting, please remain as default setting.

### 4.2.3 Access Point Mode (2.4G)

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

**Radio:**  Enable  Disable  
**Enabled SSID#:** 1 ▾  
**ESSID1:** EnGenius **VID1 :** 1 (1-4095)

---

**2.4G Wireless Settings:**  
**Band:** 2.4 GHz (B+G) ▾  
**Channel:** 6 - 2.437 GHz ▾  
**Data Rate:** Auto ▾  
**Auto Channel:**  Enable  Disable

---

<b>Radio</b>	Select the radio button to enable or disable wireless function.
<b>Enable SSID#</b>	EOA7535 can support up to 4 different SSID with different VLAN tag.
<b>ESSID</b>	Specify the broadcast SSID and VLAN ID for each ESSID.
<b>2.4G Wireless Settings</b>	
<b>Band</b>	Standard IEEE 802.11b and 802.11g band.
<b>Channel</b>	Select a channel from drop down menu.
<b>Data Rate</b>	Select the data rate from drop down menu. 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>Auto Channel</b>	Select the radio button to enable auto channel function.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Auction: If you do not have experience of data rate setting, please remain as default setting.



## 4.2.4 Client Bridge Mode/Client Router Mode (Dual Mode)

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

ESSID:	<input type="text" value="EnGenius"/>
Preferred BSSID:	<input type="text"/>

5G Wireless Setting:

Band:	<input type="text" value="5 GHz (A)"/>
-------	--

2.4G Wireless Setting:

Band:	<input type="text" value="2.4 GHz (B/G)"/>
-------	--

<b>ESSID</b>	Specify the SSID is given by Access Point if known. Otherwise, you may use <b>Site Survey</b> to scan nearby Access Point.
<b>Preferred BSSID</b>	Specify the MAC address from the Access Point that you would like to associate with.
<b>5G Wireless Setting</b>	Select the radio button to use 5G network as your default wireless network.
<b>2.4G Wireless Setting</b>	Select the radio button to use 2.4G network as your default wireless network.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Auction: EOA7535 can not operate Client Bridge in 5G and 2.4G at the same time.

Note: For more details of **Site Survey**, please refer to the Site Survey section.

## 4.2.5 Client Bridge Mode/Client Router Mode (5G)

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

ESSID:	<input type="text" value="EnGenius"/>
Preferred BSSID:	<input type="text"/>

---

5G Wireless Setting:

Band:	<input type="text" value="5 GHz (A)"/>
-------	--

---

<b>ESSID</b>	Specify the SSID is given by Access Point if known. Otherwise, you may use <b>Site Survey</b> to scan nearby Access Point.
<b>Preferred BSSID</b>	Specify the MAC address from the Access Point that you would like to associate with.
<b>5G Wireless Setting</b>	Standard IEEE 802.11a wireless band.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Note: For more details of **Site Survey**, please refer to the Site Survey section.

## 4.2.6 Client Bridge Mode/Client Router Mode (2.4G)

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

ESSID:	<input type="text" value="EnGenius"/>
Preferred BSSID:	<input type="text"/>

---

2.4G Wireless Setting:

Band:	<input type="text" value="2.4 GHz (B/G)"/>
-------	--

---

<b>ESSID</b>	Specify the SSID is given by Access Point if known. Otherwise, you may use <b>Site Survey</b> to scan nearby Access Point.
<b>Preferred BSSID</b>	Specify the MAC address from the Access Point that you would like to associate with.
<b>2.4G Wireless Setting</b>	Standard IEEE 802.11b and IEEE 802.11g wireless band.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

Note: For more details of **Site Survey**, please refer to the Site Survey section.

### 4.3 Site Survey

Use this feature to scan nearby Access Point.

No.	Select	Channel	SSID	BSSID	Encryption	Signal (dBm)
1	<input type="radio"/>	11	Jayme	00:BB:97:52:00:1C	AES	30

<b>No</b>	Numbers of Access Points have been found in the site survey.
<b>Select</b>	Select the Access Point you would like to associate with via select the radio button.
<b>Channel</b>	Access Point is currently uses which channel.
<b>SSID</b>	Access Point is broadcast the SSID.
<b>BSSID</b>	Access Point's wireless MAC address.
<b>Encryption</b>	Access Point is currently uses which security type.
<b>Signal(dBm)</b>	Signal strength from Access Point to your station.
<b>Refresh</b>	Press Refresh to rescan nearby Access Point.
<b>Connect</b>	After you selected the radio button, press Connect to process the connection.

Auction: If you select 5G as your default wireless network, you can not scan the Access Point which is operated in 2.4G band.

### 4.4 AP Scan List (5G / 2.4G)

This feature can help you to select the Access Point Channel by scan nearby Access Point status.

No.	Channel	SSID	BSSID	Encryption	Signal (dBm)
-----	---------	------	-------	------------	--------------

<b>Refresh</b>	Press Refresh to scan again.
----------------	------------------------------

### 4.5 Wireless Security Settings

Wireless Security Settings section will guide you to the entire Security modes configuration: WEP, WPA(TKIP), WPA2(AES), WPA2-Mixed, and Radius. WPA(TKIP), WPA2(AES), and WPA2-Mixed are all under **WPA pre-shared key** section.

We are strongly recommended that uses WPA2-PSK AES as your security settings.

### 4.5.1 WEP (Access Point)

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

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

<b>ESSID Selection</b>	EOA7535 supports up to 4 different SSIDs. Each SSID can be set to different authentication type.
<b>Hidden SSID</b>	Select <b>Enable</b> or <b>Disable</b> broadcast SSID.
<b>WMM</b>	Select <b>Enable</b> or <b>Disable</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>Encryption</b>	Select <b>WEP</b> from the drop down list to begin the configuration.
<b>Authentication Type</b>	Select <b>Open System</b> or <b>Shared Key</b> as your authentication type.
<b>Key Length</b>	Select Key Length in 64/128bit password length.
<b>Key Type</b>	Select Input Type in <b>Hex</b> or <b>ASCII</b> .
<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.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.

## 4.5.2 WEP (Client Bridge / Client Router)

### Security Settings

Network Name (SSID):	EnGenius
Encryption:	WEP
Key Length:	64-bit
Authentication Type:	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key
Key Type:	ASCII (5 characters)
Default Key:	Key 1
Encryption Key 1:	•••••
Encryption Key 2:	•••••
Encryption Key 3:	•••••
Encryption Key 4:	•••••

Apply

<b>Network Name (SSID)</b>	Specify the Access Point's SSID that you would like to associate with.
<b>Encryption</b>	Select <b>WEP</b> from the drop down list to begin the configuration.
<b>Authentication Type</b>	Select <b>Open System</b> or <b>Shared Key</b> as your authentication type.
<b>Key Length</b>	Select Key Length in 64/128bit password length.
<b>Key Type</b>	Select Input Type in <b>Hex</b> or <b>ASCII</b> .
<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.
<b>Apply</b>	Press <b>Apply</b> to save the changes.

### 4.5.3 WPA pre-shared Key (Access Point)

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

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

<b>ESSID Selection</b>	EOA7535 supports up to 4 different SSIDs. Each SSID can be set to different authentication type.
<b>Hidden SSID</b>	Select <b>Enable</b> or <b>Disable</b> broadcast SSID.
<b>WMM</b>	Select <b>Enable</b> or <b>Disable</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>Encryption</b>	Select <b>WPA pre-shared Key</b> from the drop down list to begin the configuration.
<b>WPA Type</b>	Select <b>WPA(TKIP)</b> , <b>WPA2(AES)</b> , or <b>WPA2 Mixed</b> as your authentication type.
<b>Pre-shared Key Type</b>	Select <b>Passphrase</b> or <b>Hex (64 characters)</b> as your key type.
<b>Pre-shared Key</b>	Specify password for security key.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.

Auction: Hex key type does not allow special characters in the password.

## 4.5.4 WPA pre-shared Key (Client Bridge / Client Router)

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

### Security Settings

Network Name (SSID):	EnGenius
Encryption:	WPA pre-shared key ▾
WPA Type:	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES)
Pre-shared Key Type:	Passphrase ▾
Pre-shared Key:	

Apply

<b>Network Name (SSID)</b>	Specify the Access Point's SSID that you would like to associate with.
<b>Encryption</b>	Select <b>WPA pre-shared key</b> from the drop down list to begin the configuration.
<b>WPA Type</b>	Select <b>WPA(TKIP)</b> , or <b>WPA2(AES)</b> as your authentication type.
<b>Pre-shared Key Type</b>	Select <b>Passphrase</b> or <b>Hex (64 characters)</b> as your key type.
<b>Pre-shared Key</b>	Specify password for security key.
<b>Apply</b>	Press <b>Apply</b> to save the changes.

Auction: Hex key type does not allow special characters in the password.

## 4.5.5 Radius (Access Point Only)

Radius authentication type is only available in Access Point Mode. Use this feature if you have Radius Server. It also supports WPA(TKIP), WPA2(AES) and WPA2 Mixed encryption types.

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

ESSID Selection:	EnGenius ▾
Hidden SSID:	Disable ▾
WMM:	Enable ▾
Encryption:	WPA RADIUS ▾
WPA Type:	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address:	<input type="text"/>
RADIUS Server port:	1812
RADIUS Server password:	<input type="text"/>

<b>ESSID Selection</b>	EOA7535 supports up to 4 different SSIDs. Each SSID can be set to different authentication type.
<b>Hidden SSID</b>	Select <b>Enable</b> or <b>Disable</b> broadcast SSID.
<b>WMM</b>	Select <b>Enable</b> or <b>Disable</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>Encryption</b>	Select <b>WPA RADIUS</b> from the drop down list to begin the configuration.
<b>WPA Type</b>	Select <b>WPA(TKIP)</b> , <b>WPA2(AES)</b> , or <b>WPA2 Mixed</b> as your encryption type.
<b>RADIUS Server IP Address</b>	Specify your Radius Server's IP address.
<b>RADIUS Server Port</b>	Specify your Radius Server Port number.
<b>RADIUS Server Password</b>	Specify the Radius Server's password that used to negotiate with Radius server authentication.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.



## 4.6 Wireless Advanced Settings

If you do not have experience with Wireless Advanced Settings, we suggest remain all settings to default. Any modifies may cause insufficient wireless connection quality.

### 4.6.1 Advanced Settings (Access Point)

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold:	<input type="text" value="2344"/>	(256-2344)
RTS Threshold:	<input type="text" value="2344"/>	(0-2345)
Beacon Interval:	<input type="text" value="100"/>	(20-1000 ms)
DTIM Period:	<input type="text" value="1"/>	(1-10)
Preamble Type:	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
Tx Power:	<input type="text" value="28dBm"/>	
Distance (1-30km):	<input type="text" value="1"/>	km
Layer2 Isolation:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

<b>Fragment Threshold</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 Threshold</b>	Specify Threshold package size for <b>Request To Send</b> (RTS). Using small number of the threshold will cause RTS 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>Beacon Interval</b>	Specify the time of Beacon Interval. Beacon is used to let wireless client scan the wireless AP is available. <b>Site Survey</b> scans the Beacon to verify which AP is in the nearby area.
<b>DTIM Period</b>	Delivery Traffic Indication Map (DTIM) is for the Power Saving purpose. Access Point sends the packet with beacon frame in the period of time. If the DTIM sets larger number, the wireless client may affect the latency throughput but save more power.
<b>Preamble Type</b>	Select the Radio button to choose Long Preamble or Short Preamble. Long Preamble can increase the capability of wireless network and wireless signal range. Short Preamble can increase the efficiency of the wireless network.
<b>Tx Power</b>	Select Tx Power to increase or decrease Transmit Power. Higher transmit power will

---

sometimes cause unable to connect to the network. On the other hand, the lower transmit power will cause client unable to connect to the device.

---

**Distance** Specify distance range between AP and Clients. Longer distance may lose high connection speed.

---

**Layer 2 Isolation** Select the Radio button to enable or disable Layer 2 Isolation. Layer 2 isolation prevents communication between wireless stations associated to different APs

---

## 4.6.2 Advanced Settings (Client Bridge / Client Router)

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold:	<input type="text" value="2344"/>	(256-2344)
RTS Threshold:	<input type="text" value="2344"/>	(0-2345)
Preamble Type:	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
802.11g Protection:	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" type="radio"/> None	
Tx Power:	<input type="text" value="28dBm"/> ▾	
Distance (1-30km):	<input type="text" value="1"/>	km

---

**Fragment Threshold** 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.

---

**RTS Threshold** Specify Threshold package size for **Request To Send** (RTS). Using small number of the threshold will cause RTS 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.

---

**Preamble Type** Select the Radio button to choose Long Preamble or Short Preamble. Long Preamble can increase the capability of wireless network and wireless signal range. Short Preamble can increase the efficiency of the wireless network.

---

**802.11g Protection** Select the Radio button to Protect types. When enable the protection mode, every time the packet is transmitted, it has to wait the CTS is received. In addition, Protection mode can prevent the collision but it will slow the wireless transmission speed.

---

**Tx Power** Select Tx Power to increase or decrease Transmit Power. Higher transmit power will sometimes cause unable to connect to the network. On the other hand, the lower transmit power will cause client unable to connect to the device.

---

**Distance** Specify distance range between AP and Clients. Longer distance may lose high connection speed.

---

## 4.7 Wireless Access Control List

Wireless Access Control List 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 EOA7535.

For security reason, the Access Point features MAC Address Filtering which deny unauthorized MAC Addresses to associate with the Access Point.

**Enable Wireless Access Control**

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

**MAC Address Filtering Table:**

No.	Description	MAC Address	Select

<b>Enable Wireless Access Control</b>	Place a <b>Check</b> to enable Wireless Access Control.
<b>Description</b>	Specify the description for the MAC address you about to add.
<b>MAC Address</b>	Specify the MAC Address.
<b>Add</b>	Press <b>Add</b> to add the MAC address.
<b>Reset</b>	Press <b>Reset</b> to cancel the condition of description and MAC Address.
<b>MAC Address Filtering Table</b>	Check all the conditions you had added.
<b>Delete Selected</b>	Place a <b>Check</b> at <b>Select</b> section, and then press <b>Delete Selected</b> to delete the option.
<b>Delete All</b>	Press <b>Delete All</b> to erase all options in the table.
<b>Reset</b>	Press <b>Reset</b> to cancel the selection.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.

## 5 LAN Setup

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

## 5.1 LAN Settings

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

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

### LAN IP

IP Address:	<input type="text" value="192.168.1.2"/>
IP Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.1.2"/>
802.1d Spanning Tree:	<input type="text" value="Disabled"/>

### DHCP Server

DHCP Server:	<input type="text" value="Enabled"/>
Lease Time:	<input type="text" value="One hour"/>
Start IP:	<input type="text" value="192.168.1.100"/>
End IP:	<input type="text" value="192.168.1.150"/>
Domain Name:	<input type="text" value="eoa7530"/>

### LAN IP

**IP Address** Specify LAN port IP address.

**IP Subnet Mask** Specify Subnet Mask.

**Default Gateway** Specify Default Gateway

**802.1d Spanning Tree** Select the drop down menu to enable or disable Spanning Tree.

### DHCP Server

**DHCP Server** Select the drop down menu to enable or disable DHCP server.

**Lease Time** Specify the expiring time of IP address given by DHCP server.

**Start IP** Specify IP Pool's first IP.

**End IP** Specify IP Pool's last IP.

**Domain Name** Specify the Domain Name of the device.

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

Auction: If you have disabled the **DHCP Server**, you must configure your PC's local IP in order to access the web-based interface. **Start IP** and **End IP** must at the same subnet.

## 5.2 DHCP Info

Click on the **DHCP Info** link under the **TCP/IP** section. This page displays the list of Clients that are associated to the EOA3630 through DHCP. You can also assign an IP address for certain MAC Address.

The **IP Address**, **MAC Address** and **Expiration Time** for each IP Address are displayed. Click on the **Refresh** button to refresh the client list.

### 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	00:23:5A:F6:74:7D	0 day 00:42:37

Refresh

You can assign an IP address to the specific MAC address

**Enable Static DHCP IP**

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

Add    Reset

### Current Static DHCP Table :

No.	IP Address	MAC Address	Select
-----	------------	-------------	--------

Delete Selected

Delete All

Reset

Apply

Cancel

<b>Enable Static DHCP IP</b>	Place a <b>Check</b> to enable <b>Static DHCP IP</b> .
<b>IP Address</b>	Specify the IP Address for the MAC address you about to add.
<b>MAC Address</b>	Specify the MAC Address.
<b>Add</b>	Press <b>Add</b> to add the MAC address.
<b>Reset</b>	Press <b>Reset</b> to cancel the condition of description and MAC Address.
<b>Current Static DHCP Table</b>	Check all the conditions you had added.
<b>Delete Selected</b>	Place a <b>Check</b> at <b>Select</b> section, and then press <b>Delete Selected</b> to delete the option.
<b>Delete All</b>	Press <b>Delete All</b> to erase all options in the table.
<b>Reset</b>	Press <b>Reset</b> to cancel the selection.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.

## 5.3 SNMP Settings

SNMP

---

SNMP Enable

SNMP Disable

---

<b>SNMP Enable</b>	Select the Radio button to enable SNMP feature.
--------------------	---

---

<b>SNMP Disable</b>	Select the Radio button to disable SNMP feature.
---------------------	--

---

<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.
-----------------------	---

---

## 6 Internet Settings

### 6.1 DHCP (Dynamic IP)

Select Dynamic IP as your WAN connection type to obtain your IP address automatically. You will need to enter Hostname

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

Hostname:

---

<b>Hostname</b>	Specify the <b>Hostname</b> is given by your Internet Service Provider.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

---

### 6.2 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.

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

IP Address:

IP Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS:

---

<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>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

---

## 6.3 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 EOA3630.

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

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

<b>Login</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>Service Name</b>	Specify the <b>Service Name</b> that is given by your ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
<b>Authentication Type</b>	Select the <b>PAP</b> , <b>CHAP</b> , or <b>Auto</b> as your encryption type from drop down menu.
<b>Type</b>	Select Connection Type from drop down menu. <b>Keep Connection:</b> Device is connected to internet automatically. <b>Automatic Connection:</b> Device is automatically connected to internet when the traffic goes through internet but it will disconnect when a period of idle time <b>Manual Connection:</b> Connect to internet manually.
<b>Idle Timeout</b>	Specify the maximum idle time for <b>Automatic Connection</b> .
<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.



## 6.4 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, Login Username, and Login Password. There are two types of PPTP connection: Dynamic IP Address and Static IP Address.

### Dynamic IP Address

#### WAN Interface Settings:

WAN Interface Type:	Dynamic IP Address ▾
Hostname:	<input type="text"/>

---

<b>WAN Interface Type</b>	Select <b>Dynamic IP Address</b> as your WAN Interface.
---------------------------	---

---

<b>Hostname</b>	Specify the <b>Hostname</b> is given by your Internet Service Provider.
-----------------	---

---

### Static IP Address

#### WAN Interface Settings:

WAN Interface Type:	Static IP Address ▾
My IP Address:	<input type="text"/>
My Subnet Mask:	<input type="text"/>
Gateway IP Address:	<input type="text"/>

---

<b>WAN Interface Type</b>	Select Static IP Address as your WAN Interface.
---------------------------	---

---

<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.
---------------------------	---------------------------------

---

**PPTP Settings:**

Login:	<input type="text"/>
Password:	<input type="text"/>
Service IP Address:	<input type="text"/>
ConnectionID:	<input type="text" value="0"/> (Optional)
MTU:	<input type="text" value="1400"/> (512<=MTU Value<=1492)
Type:	Keep Connection <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Timeout:	<input type="text" value="10"/> (1-1000 Minutes)

- Enable pptp pass through on VPN connection**
- Enable IPSec pass through on VPN connection**
- Enable L2TP pass through on VPN connection**

<b>Login</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>Service IP Address</b>	Specify the <b>Service IP Address</b> that is given by your ISP.
<b>Connection ID</b>	Specify the <b>Connection ID</b> that is given by your ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit size. Suggest remain in Auto.
<b>Type</b>	Select Connection Type from drop down menu.  <b>Keep Connection:</b> Device is connected to internet automatically. <b>Automatic Connection:</b> Device is automatically connected to internet when the traffic goes through internet but it will disconnect when a period of idle time <b>Manual Connection:</b> Connect to internet manually.
<b>Idle Timeout</b>	Specify the maximum idle time for <b>Automatic Connection</b> .
<b>Enable PPTP pass through on VPN Connection</b>	Place a Check to enable <b>PPTP pass through on VPN Connection</b> . If this feature disabled, it will cause unable to connect to internet via PPTP.
<b>Enable IPSec pass through on VPN Connection</b>	Place a Check to enable <b>IPSec pass through on VPN Connection</b> . If this feature disabled, it will cause unable to transmit IPSec Protocol.
<b>Enable L2TP pass through on VPN Connection</b>	Place a Check to enable <b>L2TP pass through on VPN Connection</b> . If this feature disabled, it will cause unable to connect to internet via L2TP.
<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.

## 7 Information Status

**Status** section is used to check the status of device information such as System up time, Firmware version, Wireless Client List, and Internet Status.

### 7.1 Status

Click on the **Status** link under the **Management** section. This page display information of the device such as Current Time, Hardware Version, Kernel Version, and Application version are displayed in the 'System' section. LAN IP address, Subnet Mask, DHCP Status, and MAC address are displayed in the 'LAN Settings' section. Access Point, Client Bridge and Client Router's basic settings are displayed in the "Wireless Information" section.

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


#### System

Current Time	Tue, Jan. 1, 2008, 12:12:38 A.M.
Hardware Version	0.80
Kernel Version	2.6
Application Version	1.1.12-11

#### LAN Settings

IP Address	192.168.1.2
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:02:6F:69:6A:99

#### 2.4GHz Wireless Information

Connect to EnGenius	fail
Channel	8
RSSI	 0%

#### 5GHz SSID\_1

ESSID	EnGenius
Security	Disable
BSSID	00:02:6F:69:6A:9B

## 7.2 Wireless Client List

Click on the **Client List** link under the **5G/2.4G Wireless** section. This page displays the list of Clients that are associated to the EOA7535.

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

### WLAN Client Table:

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

MAC Address	Signal (%)	Idle Time
No client connecting to the Router.		

## 7.3 System Log

Click on the **Log** link under the **Management** section. 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. You can **Save** your current system operation information to a text file or clear all logs.

View the system operation information.

```
day 1 00:30:27 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day 1 00:00:36 [SYSTEM]: DHCP Server, Sending ACK of 192.168.1.100
day 1 00:00:21 [SYSTEM]: TELNETD, start Telnet-cli Server
day 1 00:00:21 [SYSTEM]: HTTP, start
day 1 00:00:20 [SYSTEM]: NET, start Firewall
day 1 00:00:20 [SYSTEM]: NET, start NAT
day 1 00:00:20 [SYSTEM]: NTP, start NTP Client
day 1 00:00:17 [SYSTEM]: DNS, start DNS Proxy
day 1 00:00:17 [SYSTEM]: DHCP, start DHCP Server
```

## 7.4 Internet Status

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

View the current internet connection status and related information.

### WAN Settings

Attain IP Protocol	Dynamic IP Address
IP Address	---
Subnet Mask	---
Default Gateway	---
MAC Address	00:02:6F:69:6A:9A
Primary DNS	---
Secondary DNS	---

Renew

Note: If your internet connection type is **PPPoE** or **PPTP** with **Manual Connection**, you can connect to internet at this page.

## 8 Management Settings

**Management** section is on the navigation drop-down menu. This section can help you to manage your device and adjust system settings such as Password, Time Zone, Diagnosis, Remote Control, Upgrade Firmware, Save/Load Settings. Each option is described below.

### 8.1 Password Settings

Click on the **Password** link under the **Management** section. This option allows you to change password for the device. By default, the default password is **admin**. For security reasons it is highly recommended that you create a new password.

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

Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Repeat New Password:	<input type="text"/>

<b>Old Password</b>	Enter the current password.
<b>New Password</b>	Specify a new Password for login
<b>Repeat New Password</b>	Re-enter the new Password for confirmation.
<b>Apply / Cancel</b>	Press <b>Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

### 8.2 Time Zone Settings

Click on the **Time Zone** link under the **Management** menu. This page allows you to configure the time on the device.

The Device reads the correct time from NTP server 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 status and the log files.

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

<b>Time Zone</b>	Select your Country or Region from the drop down list.
------------------	--

<b>NTP Time Server</b>	Specify the NTP Server's Domain name or IP Address.
<b>Daylight Saving</b>	Place a <b>Check</b> to enable Daylight Saving feature. Configure the starting date and ending date.
<b>Apply / Cancel</b>	Press <b>Apply</b> to save the changes or <b>Cancel</b> to return previous settings.

### 8.3 Diagnosis

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.

This page can diagnose the current network status.

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

<b>Address to Ping</b>	Specify the IP address you would like to Ping.
<b>Start</b>	Press <b>Start</b> to begin.
<b>Count</b>	Specify numbers of time to ping.
<b>Ping Result</b>	Display Ping result.

## 8.4 Remote Control

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

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

<b>Host Address</b>	Specify the IP Address you would like to use as your remote controller.
<b>Port</b>	Specify the Port number.
<b>Enable</b>	Place a Check to enable Remote management.
<b>Apply/Reset</b>	Press <b>Apply</b> to save the changes or <b>Reset</b> to return previous settings.

## 8.5 Upgrade Firmware

Click on the **Upgrade Firmware** 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.

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

Auction: Upgrade process may take few minutes, please do not power off the device and it may cause the device crashed or unusable. EOA7535 will restart automatically once the upgrade is completed.

## 8.6 Save/Reload Settings

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



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

Restore to Factory Default:	<input type="button" value="Reset"/>
Backup Settings:	<input type="button" value="Save"/>
Restore Settings:	<input type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Upload"/>
Restart:	<input type="button" value="Restart"/>

---

<b>Restore to Factory Default Settings</b>	Click on <b>Reset</b> button to reset all the settings to the default values.
<b>Backup Settings</b>	Click on <b>Save</b> to save current configured settings.
<b>Restore Settings</b>	EOA7535 can restore a previous setting that has been saved. Click on Browse to select the file and Upload.
<b>Restart</b>	Press <b>Restart</b> to reboot the device.

---

Auction: If you choose to **Restore to Factory Default**, all the settings will be erased. It is strongly suggested to save current settings before your process.

## 9 Network Configuration Example

This chapter describes the role of the EOA7535 with three 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. Repeater mode and Mesh network mode need future configuration.

### 9.1 Access Point Mode + Client Bridge Mode




---

#### **Access Point**

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.2
<b>Step2</b>	Select 802.11b/g mixed and/or 802.11a as your wireless mode.
<b>Step3</b>	Use <b>AP Scan</b> 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.

Auction: Dual mode uses the same SSID on 5G and 2.4G wireless network.

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

---

#### **Client Bridge**

<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.2
<b>Step2</b>	Change operation mode to <b>Client Bridge</b> .

<b>Step3</b>	Select 5G or 2.4G as your wireless mode.
<b>Step4</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>Step5</b>	Select correct authentication type and then enter password.

Auction: Wireless Client IP address must configure manually at the same subnet in Local Area Network or enable DHCP server of EOA7535 to retrieve IP automatically.

## 9.2 Client Router Mode

Please refer to last section for the configuration of **Access Point**.



<b>Step1</b>	Login to the web-based configuration interface with default IP 192.168.1.2
<b>Step2</b>	Change operation mode to <b>Client Router</b> .
<b>Step3</b>	Select 5G or 2.4G as your wireless mode.
<b>Step4</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>Step5</b>	Select correct authentication type and then enter password.
<b>Step6</b>	Select your internet connection type base on your Internet Service Provider.

Note: For more details of Internet Connection Settings, Please refer to the Internet chapter.

# 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.

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 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.