

# EnGenius®

**11N Long Range Multi-Function Client Bridge / Access Point**



**ECB300**

**11 N Long Range Multi-Function Client Bridge / Access Point**

*V1.0*

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>6</b>
1.1	Features and Benefits .....	6
1.2	Package Contents .....	7
1.3	System Requirements.....	8
1.4	Applications .....	8
<b>2</b>	<b>Before you Begin.....</b>	<b>10</b>
2.1	Considerations for Wireless Installation .....	10
2.2	Computer Settings (Windows XP/Windows Vista/Windows 7) .....	11
2.3	Apple Mac X OS.....	14
2.4	Hardware Installation.....	15
<b>3</b>	<b>Configuring Your Client Bridge .....</b>	<b>17</b>
3.1	Default Settings .....	17
3.2	Web Configuration.....	18
<b>4</b>	<b>Building a Wireless Network .....</b>	<b>20</b>
4.1	Client Bridge Mode .....	20
4.2	Access Point Mode.....	21
4.3	WDS AP Mode .....	22
4.4	WDS Bridge Mode.....	23
4.5	Router Mode.....	24
4.6	Repeater Mode .....	25
<b>5</b>	<b>System.....</b>	<b>26</b>
5.1	Operation Mode.....	26
5.2	Status.....	28

5.3	DHCP .....	32
5.4	Schedule .....	34
5.5	Event Log .....	36
5.6	Monitor .....	37
<b>6</b>	<b>Wireless.....</b>	<b>38</b>
6.1	Status.....	38
6.2	Basic .....	40
6.3	Site Survey .....	44
6.4	Advanced .....	48
6.5	Security .....	52
6.6	Filter .....	58
6.7	WPS (Wi-Fi Protected Setup).....	60
6.8	Client List.....	62
6.9	VLAN.....	63
6.10	AP Profile.....	64
<b>7</b>	<b>Network.....</b>	<b>66</b>
7.1	Status.....	66
7.2	LAN.....	67
7.3	Spanning Tree .....	70
7.4	WAN (Router mode).....	71
7.4.1	Static IP Address.....	71
7.4.2	Dynamic IP Address .....	72
7.4.3	PPP over Ethernet (PPPoE).....	73
7.4.4	Point-to-Point Tunneling Protocol (PPTP).....	74
<b>8</b>	<b>Firewall.....</b>	<b>76</b>
8.1	Enable.....	76

8.2	DMZ .....	77
8.3	DoS.....	78
8.4	MAC Filter .....	79
8.5	IP Filter .....	80
8.6	URL Filter.....	82
<b>9</b>	<b>Advanced.....</b>	<b>83</b>
9.1	Network Address Translation (NAT).....	83
9.2	Port Mapping .....	84
9.3	Port Forwarding.....	85
9.4	Port Triggering.....	86
9.5	Application Layer Gateway (ALG).....	87
9.6	Universal Plug and Play (UPnP).....	88
9.7	Quality of Service (QoS).....	89
9.8	Static Routing .....	92
9.9	Dynamic Routing.....	93
9.10	Routing Table .....	94
<b>10</b>	<b>Management.....</b>	<b>95</b>
10.1	Admin.....	95
10.2	SNMP.....	97
10.3	Firmware Upgrade .....	99
10.4	Configure .....	102
10.5	Reset.....	103
<b>11</b>	<b>Tools.....</b>	<b>104</b>
11.1	Time Setting.....	104
11.2	Diagnosis.....	105
<b>12</b>	<b>Logout.....</b>	<b>106</b>

**Appendix A – FCC Interference Statement.....107**  
**Appendix B – IC Interference Statement.....108**  
**Appendix C – CE Interference Statement .....110**

## Revision History

Version	Date	Notes
1.0	Feb. 15, 2012	First Release

# 1 Introduction

The **ECB300** is a multi-function 802.11b/g/n product with 6 major multi-functions. The ECB300 is designed to operate in every working environment including enterprises.

The ECB300 is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11b/g devices. The ECB300 supports use in the home network with superior throughput, performance, and significant wireless range.

To protect data during wireless transmissions, the ECB300 encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2 encryption. The ECB300 has MAC address filtering to allow users to select differing stations to access the network. The ECB300 is an ideal product to ensure network safety for both home and enterprise environments.

## 1.1 Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300 Mbps	<b>Capable of handling heavy data payloads such as HD multimedia streaming.</b>
10/100 Fast Ethernet	<b>Support up to 100Mbps networking speed.</b>
IEEE 802.11n Draft Compliant and Backwards Compatible with 802.11b/g devices	<b>Fully compatible with IEEE 802.11b/g/n devices.</b>
Multi-Function	<b>Allowing users to select Access Point, Client Bridge, WDS AP, WDS Bridge, Router or Universal Repeater mode in various applications.</b>
Point-to-Point or Point-to-Multipoint Wireless Connectivity	<b>Allows transfer of data from building to building.</b>

Support Multiple SSID in AP mode (up to 4)	<b>Allow clients to access different networks through a single access point and assign different policies and functions for each SSID through the built in software.</b>
WPA/WPA2/IEEE 802.1x Support	<b>Powerful data security.</b>
MAC Address Filtering in AP Mode	<b>Ensure a secure network connection.</b>
User Isolation Support (AP mode)	<b>Protect the private network between client users.</b>
Power-over-Ethernet (IEEE802.3af)	<b>Flexible Access Point locations.</b>
Save User Settings	<b>Firmware upgrade does not delete user settings.</b>
SNMP Remote Configuration Management	<b>Allows remote connection to configure or manage the ECB300 easily.</b>
<b>QoS (WMM) support</b>	<b>Enhanced user performance and density.</b>

## 1.2 Package Contents

The ECB300 package contains the following items (all items must be in package to issue a refund):

- ECB300 Wireless Long Range Multi-Function Client Bridge / Access Point
- 12V/1A 100V~240V Power Adapter
- RJ-45 Ethernet Cable
- Detachable Antenna
- CD with User's Manual
- Quick Installation Guide



### 1.3 System Requirements

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

- Computer with an Ethernet interface or Wireless Network.
- Windows, Mac OS, or Linux based operating systems.
- Web-Browsing Application (example: Internet Explorer, FireFox, Safari, or other similar software)

### 1.4 Applications

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

**a) Difficult-to-Wire Environments**

There are many situations where wires cannot be laid easily or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas make the installation of a Wired LAN impossible, impractical, and/or expensive.

**b) Temporary Workgroups**

Create temporary workgroups/networks in open areas such as parks, athletic arenas, exhibition centers, temporary offices, and construction sites where one wants a temporary Wireless LAN established and easily removed.

**c) The Ability to Access Real-Time Information**

Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.

**d) Frequently Changing Environments**

Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).

**e) Small Office and Home Office (SOHO) Networks**

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

**f) Wireless Extensions to Ethernet Networks**

Extend network coverage where the network cannot reach (i.e.: There is no wired internet connection to reach certain location of the environment).

**g) Wired LAN Backup**

Implement wireless LANs to provide backup for mission-critical applications running on wired networks.

**h) Training/Educational Facilities**

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

## 2 Before you Begin

This section will guide you through the installation process. Placement of the ENGENIUS ECB300 is essential to maximize the ECB300's performance. Avoid placing the ECB300 in an enclosed space such as a closet, cabinet, or wardrobe.

### 2.1 Considerations for Wireless Installation

The operating distance of all wireless devices cannot be pre-determined due to a number of unknown obstacles in the environment that the device is deployed in. These could be the number, thickness, and location of walls, ceilings, or other objects that the ECB300's wireless signals must pass through. Here are some key guidelines to allow the ECB300 to have optimal wireless range.

- Keep the number of walls and/or ceilings between the ECB300 and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in lower signal strength.
- Building materials makes a difference. A solid metal door and/or aluminum studs may have a significant negative effect on the signal strength of the ECB300. Locate your wireless devices carefully so the signal can pass through a drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets, and/or brick can also lower your wireless signal strength.
- Interferences can also come from other electrical devices and/or appliances that generate RF noise. The most usual types are microwaves and cordless phones.

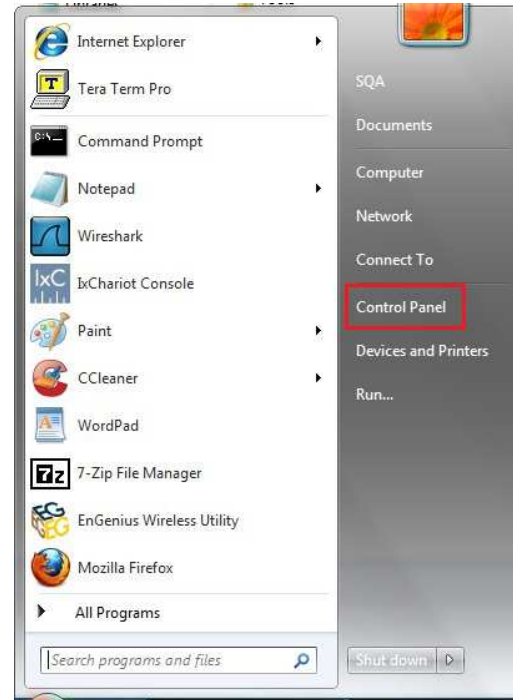
## 2.2 Computer Settings (Windows XP/Windows Vista/Windows 7)

In order to use the ECB300, you must first configure the TCP/IPv4 connection of your computer system.

- Click **Start** button and select **Control Panel**.



Windows XP

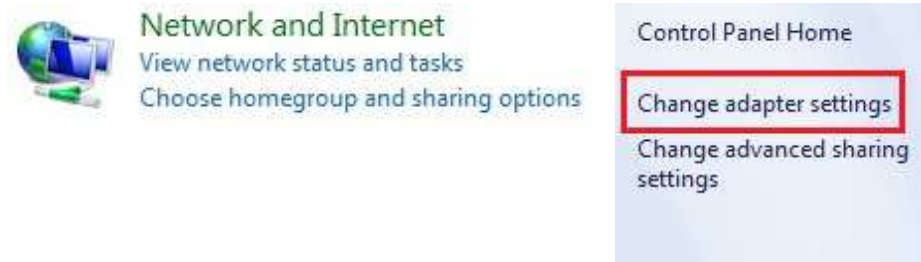


Windows Vista/Windows 7

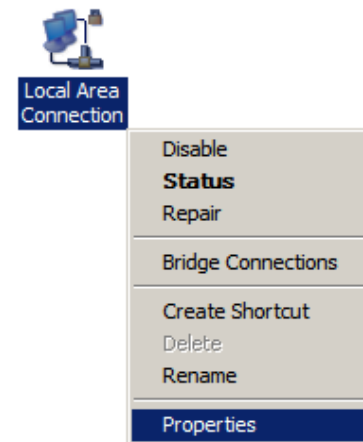
- In **Windows XP**, click **Network Connections**



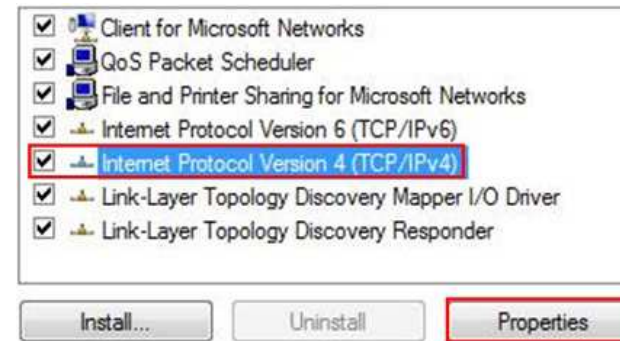
- In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet** section, then select **Change Adapter Settings**



- Right click on **Local Area Connection** and select **Properties**



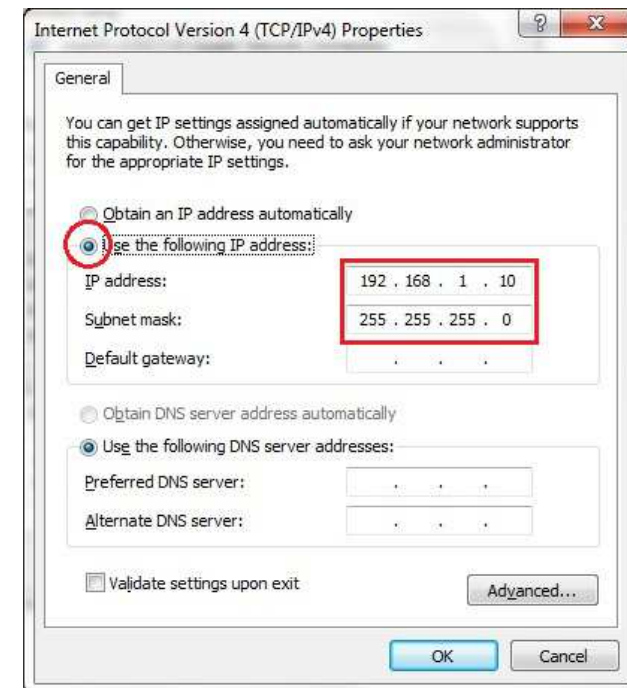
- Highlight **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**



- Select **Use the following IP address** and enter IP address and subnet mask then press **OK**.

**Note:** Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: Device IP address: 192.168.1.1  
 PC IP address: 192.168.1.2 - 192.168.1.254  
 PC subnet mask: 255.255.255.0



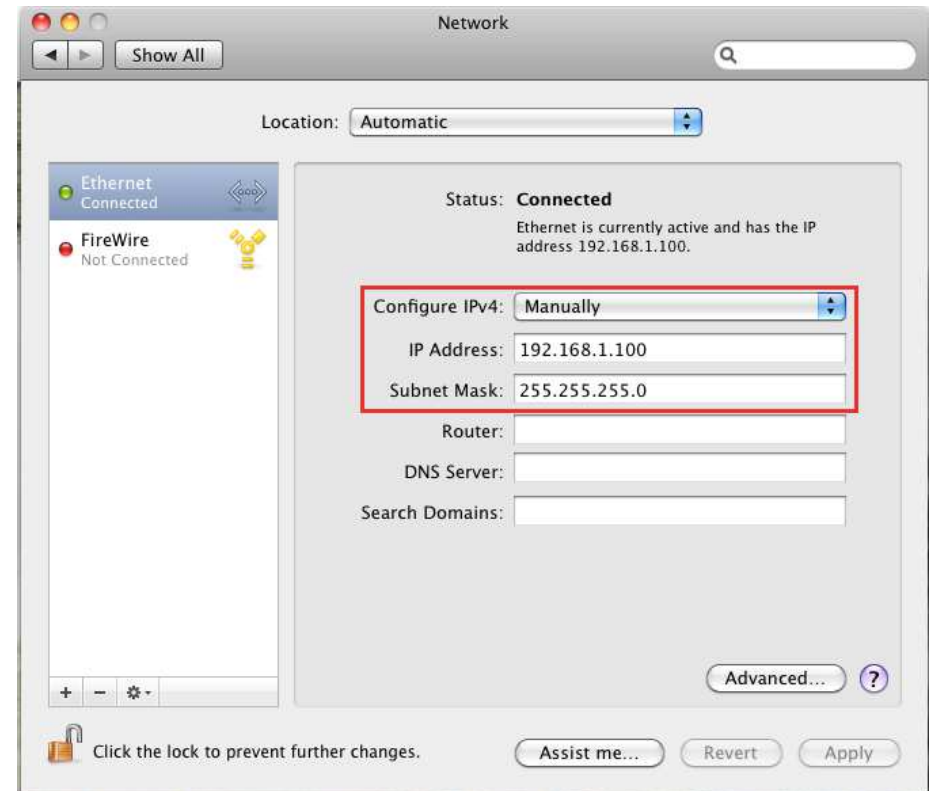
## 2.3 Apple Mac X OS

- Open the **System Preferences** (can be opened in the **Applications** folder or selecting it in the Apple Menu)
- Select **Network** in the **Internet & Network** section
- Highlight **Ethernet**
- In **Configure IPv4**, select **Manually**
- Enter IP address and subnet mask then press **OK**.

**Note:** Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: Device IP address: 192.168.1.1  
 PC IP address: 192.168.1.2 - 192.168.1.254  
 PC subnet mask: 255.255.255.0

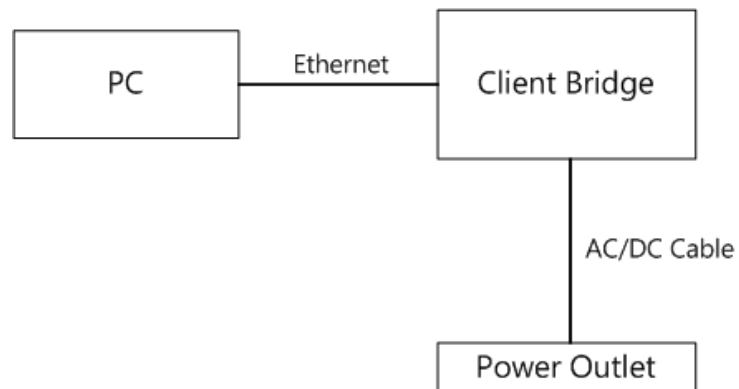
- Click **Apply** when done.



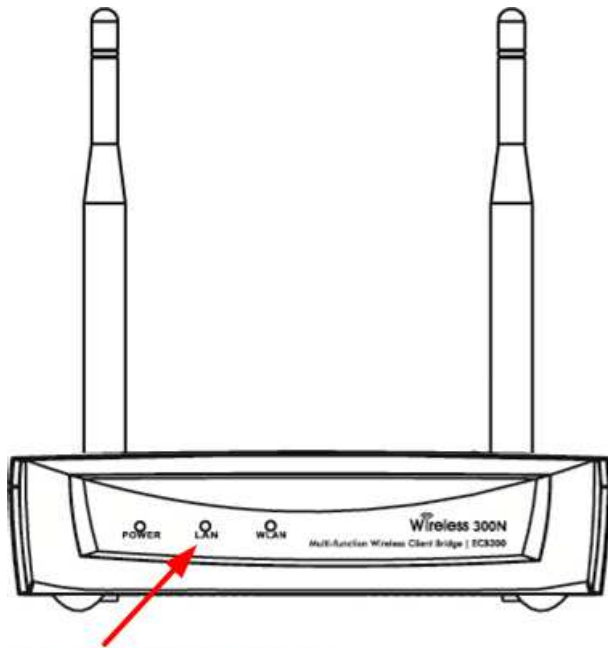
## 2.4 Hardware Installation

- 1) Ensure that the computer in use has an Ethernet Card (RJ-45 Ethernet Port). For more information, verify with our computer user manual.
- 2) Connect one end of the Category 5 Ethernet cable into RJ-45 port of the ECB300 and the other end to the RJ-45 port on the computer that will use the ECB300. Ensure that the cable is securely connected to both the ECB300 and the Computer.
- 3) Connect the Power Adaptor DC Inlet to the **DC-IN** port of the ECB300 and the Power Adaptor to the electrical out. Once both connections are secure, verify the following:
  - a) Ensure that the **Power** light is on (it will be blue).
  - b) Ensure that the **Wireless** light is on (it will be blue).
  - c) Ensure that the **LAN (Computer/ECB300 Connection)** light is on (it will be blue).
  - d) Once all three lights are on, proceed to setting up the computer.

This diagram depicts the hardware configuration.

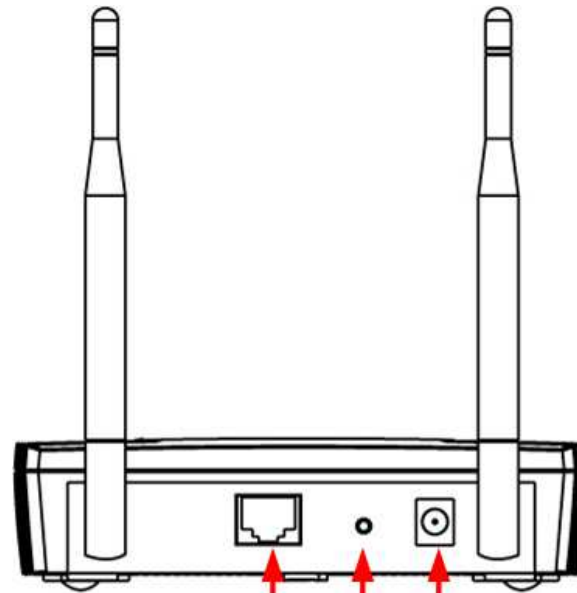






LED Lights for Wireless, Ethernet port and Power

Front Panel



Ethernet port for RJ-45 cable  
Reset Button  
DC IN for Power

Rear Panel

Front Panel	
<b>LED Lights</b>	LED lights for Wireless, Ethernet port and Power.
Rear Panel	
<b>DC IN</b>	DC IN for Power.
<b>Reset Button</b>	One click for reset the device. Press over 10 seconds for reset to factory default.
<b>Ethernet Port</b>	Ethernet port for RJ-45 cable.

## 3 Configuring Your Client Bridge

This section will show you how to configure the device using the web-based configuration interface.

### 3.1 Default Settings

Please use your Ethernet port or wireless network adapter to connect the Client Bridge.

**Default Settings**

IP Address	192.168.1.1
Username / Password	admin / admin
Operation Mode	Client Bridge

## 3.2 Web Configuration

- Open a web browser (Internet Explorer/Firefox/Safari) and enter the IP Address: **http://192.168.1.1**

**Note:** If you have changed the default LAN IP Address of the device, ensure you enter the correct IP Address.



- The default username and password are **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-base configuration page.


A login form for EnGenius. The form is titled "EnGenius" and contains two input fields: "Username:" with the value "admin" and "Password:" with five dots. Below the fields are two buttons: "Login" and "Cancel".

EnGenius

Username:

Password:

- If successful, you will be logging in and see the ECB300 User Menu

**2.4GHz Wireless-N Multi-function AP**

**Client Bridge Mode**

- System
- Wireless
- Network
- Management
- Tools
- Logout

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

System	
Operation Mode	Client Bridge
System Time	2009/01/01 00:38:27
System Up Time	38 min 34 sec
Hardware Version	0.1.0
Serial Number	201107279
Firmware version	1.0.0

WLAN Station Information	
Connection Status	Fail
Channel	---
ESSID	---
Security	---
BSSID	---

## 4 Building a Wireless Network

The ECB300 has the ability to operate in various operating modes. The ECB300 is the ideal device in which you can build your WLAN. This chapter describes how to build a WLAN around your ECB300 using the operating modes of the ECB300.

### 4.1 Client Bridge Mode

In Client Bridge Mode, the ECB300 acts as a wireless dongle that connects to an Access Point to allow a system wireless access to the network. This mode requires you to connect the Ethernet port on your PC to the ECB300 LAN port.

If you use the client bridge operating mode, use the ECB300 Site Survey feature to scan for Access Points within range.

When you find an Access Point, configure the ECB300 to use the same SSID and Security Password as the Access Point to associate with it.



## 4.2 Access Point Mode

In Access Point Mode, ECB300 behaves like a central connection for stations or clients that support IEEE 802.11b/g/n networks. The stations and clients must be configured to use the same SSID and security password to associate with the ECB300. The ECB300 supports up to four SSIDs at the same time for secure guest access.



### 4.3 WDS AP Mode

The ECB300 also supports WDS AP mode. This operating mode allows wireless connections to the ECB300 using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports four AP MAC addresses.



## 4.4 WDS Bridge Mode

In WDS Bridge Mode, the ECB300 can wirelessly connect different LANs by configuring the MAC address and security settings of each ECB300 device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to use the ECB300 to wirelessly connect two wired LANs, as shown in the following figure.

WDS Bridge Mode can establish four WDS links, creating a star-like network.



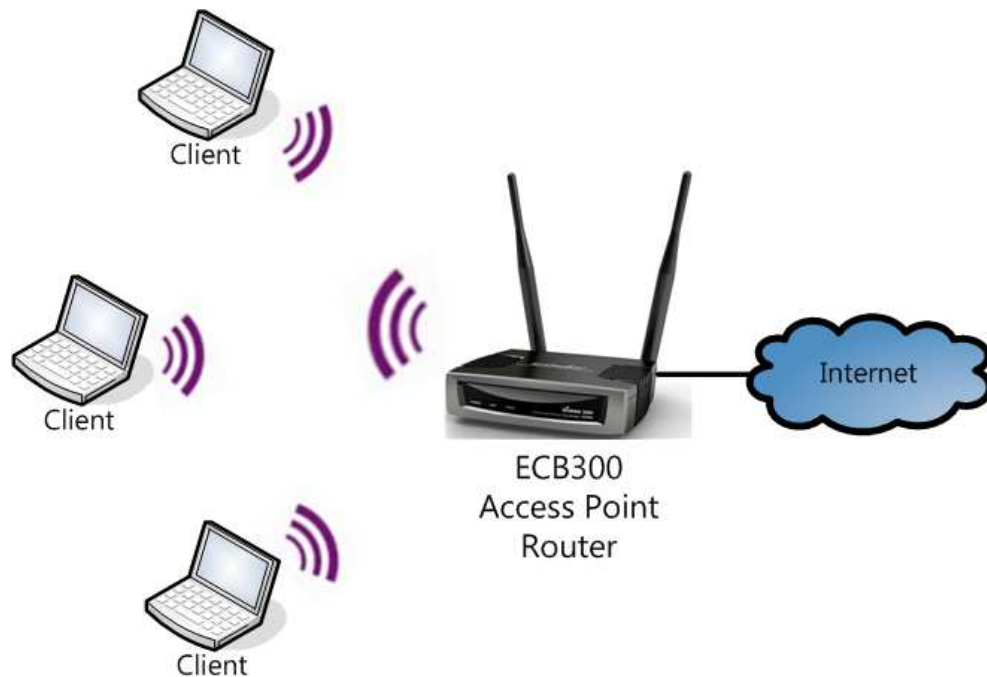
**Note:** WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. Please be aware to avoid loops in your wireless connection, otherwise enable Spanning Tree Function.



## 4.5 Router Mode

In Access Point Router Mode, ECB300 grants Internet access to multiple wireless clients. In this mode, the ECB300's internal Dynamic Host Configuration Protocol (DHCP) server automatically allocates ranges of IP addresses to each wireless client that will access the Internet through the ECB300.

This mode requires you to connect the ECB300's Ethernet port to a modem or router. And the wireless clients must be configured to use the same SSID and security password to associate with the ECB300. The ECB300 supports up to four SSIDs at the same time for secure guest access.



## 4.6 Repeater Mode

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



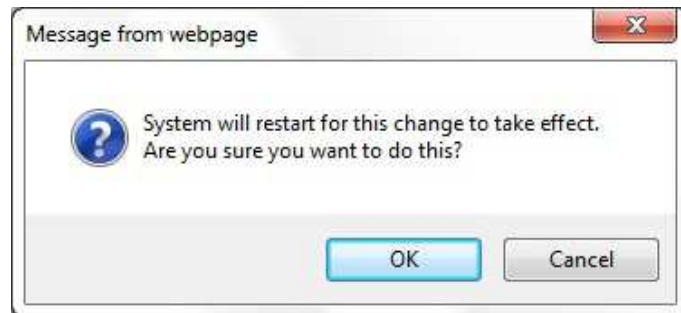
## 5 System

### 5.1 Operation Mode

Each operating mode offers different features. In order to switch the operating mode, select it from the **Operation Mode** from the **System Menu**. There are six operation modes: **Access Point**, **Client Bridge**, **WDS AP**, **WDS Bridge**, **Access Point Router** and **Universal Repeater**.



A dialog box will appear to notify you that the system will restart in order for the changes to take effect. Click on the **OK** button to continue.



The ECB300 will display how much time it will take to restart the device in the new operating mode as shown below.

System mode is changed and module is reloading, please wait  seconds.

## 5.2 Status

This page will display status of the device.

### System

Operation Mode Client Bridge  
 System Time 2009/01/01 01:01:47  
 System Up Time 1 hours 1 min 52 sec  
 Hardware Version 0.1.0  
 Serial Number 201107279  
 Firmware version 1.0.0

System	
<b>Operation Mode</b>	Displays the current mode of operation of the ECB300.
<b>System Time</b>	Displays the current time of the ECB300.
<b>System Up Time</b>	The elapsed time of operation of the ECB300.
<b>Hardware Version and Serial Number</b>	Hardware information of the ECB300.
<b>Firmware Version</b>	The current firmware version of the ECB300.

**WAN Settings**

Attain IP Protocol Dynamic IP Address  
 IP Address 192.168.7.162  
 Subnet Mask 255.255.255.0  
 Default Gateway 192.168.7.10  
 MAC Address 00:02:6F:30:0A:24  
 Primary DNS 192.168.7.10  
 Secondary DNS ---

<b>WAN Settings (Router mode)</b>	
<b>Attain IP Protocol</b>	Method used to connect to the Internet. This is your WAN connection type.
<b>IP Address</b>	The WAN IP address of the Router.
<b>Subnet Mask</b>	The WAN subnet mask of the Router.
<b>Default Gateway</b>	The default gateway of the Router.
<b>MAC Address</b>	The WAN MAC address of the Router.
<b>Primary and Secondary DNS</b>	The IP addresses of the Primary and Secondary DNS servers assigned to the WAN connection.

**WLAN Station Information**

Connection Status Fail  
 Channel ---  
 ESSID ---  
 Security ---  
 BSSID ---

<b>WLAN Station Information (Client Bridge mode)</b>	
<b>Connection Status</b>	The connection status: <b>Successful</b> or <b>Fail</b> .
<b>Channel</b>	The wireless channel in use.
<b>ESSID</b>	The SSID (Network Name) of the wireless network which ECB300 connected.
<b>Security</b>	The wireless encryption in use.
<b>BSSID</b>	The MAC address of this SSID which ECB300 connected.

**WLAN Repeater Information**

Connection Status Successful  
 Channel 8  
 ESSID EnGenius  
 Security WPA2 pre-shared key  
 BSSID 00:02:6F:30:00:25

<b>WLAN Repeater Information (Repeater mode)</b>	
<b>Connection Status</b>	The connection status: <b>Successful</b> or <b>Fail</b> .
<b>Channel</b>	The wireless channel in use.
<b>ESSID</b>	The SSID (Network Name) of the wireless network.

<b>Security</b>	Wireless encryption for this SSID.
<b>BSSID</b>	The MAC address of this SSID.

#### WLAN Settings

Channel 11

#### SSID\_1

ESSID EnGenius300024

Security Disable

BSSID 00:02:6F:30:00:24

WLAN Settings (Access Point / WDS AP / Repeater / Router mode)	
<b>Channel</b>	Displays the current Wireless Channel in use by the ECB300.
<b>ESSID</b>	The SSID (Network Name) of the wireless network (up to 4 SSIDs supported).
<b>Security</b>	Current wireless encryption for the corresponding SSID.
<b>BSSID</b>	The MAC address of the corresponding SSID.



## 5.3 DHCP

The **DHCP** option in the **System** menu displays the client IP address assigned by the DHCP Server. You can also set the IP Addresses of the connected devices manually.

**Note:** Only in Access Point / Router mode.

### DHCP Client Table :

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

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh

You can assign an IP address to the specific MAC address.

**Enable Static DHCP IP**

IP Address	MAC Address
192.168.1.100	80E3A39B703A

Add

Reset

### Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.50	00:24:E8:C7:41:0D	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server.

#### DHCP Client Table :

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

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh

DHCP Client Table	
<b>IP address</b>	Displays the IP Address of the client on the LAN.
<b>MAC address</b>	Displays the MAC Address of the client on the LAN.
<b>Expiration Time</b>	Displays the time of expiration of the IP Address of the client.
<b>Refresh</b>	Click this button to update the DHCP Client Table.

## 5.4 Schedule

The **Schedule** option of the **System** menu allows you to set a schedule when the ECB300's Wireless is active.

The **Schedule Table** will display:

- **NO.:** The entry number of the schedule.
- **Description:** The name given to the schedule.
- **Service:** Displays whether the wireless service will be activate or not during the scheduled time.
- **Schedule:** Displays when the schedule will execute.

You will also be able to **Add** new schedules (at most 10), **Edit** schedules, **Delete Selected** schedules, or **Delete All** schedules.

**Enabled Schedule Table (up to 10)**

NO.	Description	Service	Schedule	Select
1	schedule 01	Wireless Active	From 11:00 To 12:00--- Mon, Wed	<input type="checkbox"/>

After selecting **Add** or **Edit**, the following form will show up. Fill in the form to set the schedule you want.

<b>Schedule Description :</b>	<input type="text" value="schedule 01"/>
<b>Service :</b>	<input checked="" type="checkbox"/> Wireless Active
<b>Days :</b>	<input type="checkbox"/> Every Day <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
<b>Time of day :</b>	<input type="checkbox"/> All Day (use 24-hour clock) From <input type="text" value="11"/> : <input type="text" value="0"/> To <input type="text" value="12"/> : <input type="text" value="0"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Schedule	
<b>Schedule Description</b>	Assign a name to the schedule.
<b>Service</b>	The service provided for the schedule.
<b>Days</b>	Set which days the schedule will be active.
<b>Time of day</b>	Set what time of the selected days the schedule will be active.

## 5.5 Event Log

The **Event Log** of the **System** menu displays the system events and actions of the ECB300. When powered down or rebooted, the **Event Log** will be cleared.

View the system operation information.

```

day 1 00:00:07 [SYSTEM]: WLAN, start LLTD
day 1 00:00:06 [SYSTEM]: TELNETD, start Telnet-cli Server
day 1 00:00:06 [SYSTEM]: HTTPS, start
day 1 00:00:06 [SYSTEM]: HTTP, start
day 1 00:00:05 [SYSTEM]: UPnP, Start
day 1 00:00:05 [SYSTEM]: SNMP, start SNMP server
day 1 00:00:05 [SYSTEM]: SCHEDULE, Wireless Radio On
day 1 00:00:04 [SYSTEM]: NTP, start NTP Client
day 1 00:00:04 [SYSTEM]: DHCP, DHCP Server Stopping
day 1 00:00:03 [SYSTEM]: WLAN[2.4G], Channel = 11
day 1 00:00:03 [SYSTEM]: LAN, IP address=192.168.1.1
day 1 00:00:03 [SYSTEM]: LAN, start
day 1 00:00:01 [SYSTEM]: BR, start
day 1 00:00:01 [SYSTEM]: SYS, Application Version: 1.0.0
day 1 00:00:01 [SYSTEM]: Start Log Message Service!

```

Save Clear Refresh

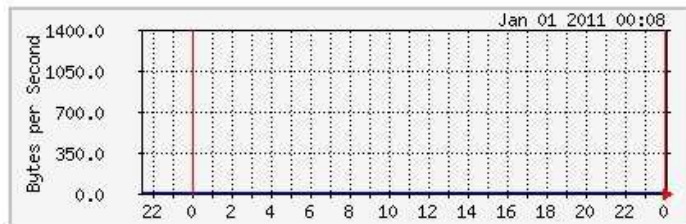
Event Log	
Save	Save the log to a .txt file.
Clear	Clear the log.
Refresh	Update the log.

## 5.6 Monitor

The **Monitor** option of the **System** menu displays 2 histogram graphs. The histograms represent the bandwidth usage of both the daily use of the Ethernet and the daily use of the WLAN. If you click on **Detail**, a new browser window will open with 4 additional histograms (6 total). In the new browser window, you will be able to view the weekly and monthly bandwidth usage for both the Ethernet and WLAN.

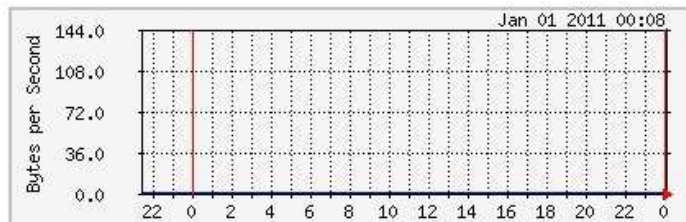
**Ethernet Daily Graph (5 Minute Average)**

[Detail](#)



	Maximum	Average	Current
<b>RX</b>	293 B/sec	293 B/sec	293 B/sec
<b>TX</b>	1365 B/sec	1365 B/sec	1365 B/sec

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



	Maximum	Average	Current
<b>RX</b>	0 B/sec	0 B/sec	0 B/sec
<b>TX</b>	144 B/sec	144 B/sec	144 B/sec

## 6 Wireless

### 6.1 Status

The **Status** of the **Wireless** menu displays the current status of the ECB300's wireless configuration.

#### Client Bridge mode:

View the current wireless connection status and related information.

##### WLAN Station Information

Connection Status	Successful
ESSID	EnGenius
Security	WPA2 pre-shared key
BSSID	00:02:6F:C7:EB:70
Channel	8
Data Rate	143 Mbps
Link Quality	100/100

#### Access Point / Router mode:

View the current wireless connection status and related information.

##### WLAN Settings

Channel 11

##### SSID\_1

ESSID	EnGenius300024
Security	Disable
BSSID	00:02:6F:30:00:24

**Repeater mode:**

View the current wireless connection status and related information.

**WLAN Repeater Information**

Connection Status	Successful
ESSID	EnGenius
Security	WPA2 pre-shared key
BSSID	00:02:6F:30:00:25
Channel	8

**WLAN Settings**

Channel	8
---------	---

**SSID\_1**

ESSID	EnGenius
Security	WPA2 pre-shared key
BSSID	00:02:6F:30:00:24



## 6.2 Basic

The **Basic** option of the **Wireless** menu displays the basic wireless options of the ECB300.

### Client Bridge:

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

Radio :  Enable  Disable

Mode :

Band :

Site Survey :

Basic (Client Bridge mode)	
<b>Radio</b>	Enable or Disable the device's wireless signal.
<b>Band</b>	Select the types of wireless clients that the device will accept.
<b>Site Survey</b>	Click on [ <b>Site Survey</b> ] to search the existing AP.

### Access Point / Router mode:

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

**Radio :**  Enable  Disable

**Mode :**

**Band :**

**Enabled SSID#:**

**ESSID1 :**

**Auto Channel:**  Enable  Disable

**Channel :**

Basic (Access Point / Router mode)	
<b>Radio</b>	Enable or Disable the ECB300's wireless signal.
<b>Mode</b>	Select between Access Point or Wireless Distribution System (WDS) modes.
<b>Band</b>	Select the types of wireless clients that the device will accept.
<b>Enable SSID#</b>	Select the number of SSID's (Wireless Network names) you would like (up to 4).
<b>SSID#</b>	Enter the name of your wireless network. You can use up to 32 characters.
<b>Auto Channel</b>	When enabled, the device will scan the wireless signals around your area and select the channel with the least interference.
<b>Channel</b>	Manually select which channel the wireless signal will use.

<b>Check Channel Time</b>	When Auto Channel is <b>Enabled</b> , you can specify the period of device will scan the wireless signals around your area.
---------------------------	---

### WDS AP / WDS Bridge mode: Wireless Distribution System (WDS)

Using a WDS to connect Access Points wirelessly extends a wired infrastructure to locations where cabling is not possible or inefficient to implement.

**Note:** Compatibility between different brands and models of Access Points is not guaranteed. It is recommended that a WDS network be created using the same Access Point models for maximum compatibility.

Also, all Access Points in the WDS network need to use the same Channel and Security settings.

*To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four access points.*

Radio :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode :	WDS ▾
Band :	2.4 GHz (B+G+N) ▾
Channel :	11 ▾
MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000
MAC Address 4 :	000000000000
WDS Data Rate :	300M ▾
Set Security :	Set Security

**Repeater mode:**

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

**Radio :**  Enable  Disable

**Mode :**

**Band :**

**Enabled SSID#:**

**ESSID1 :**

**Channel :**

**Site Survey :**

Basic (Repeater mode)	
<b>Radio</b>	Enable or Disable the device's wireless signal.
<b>Band</b>	Select the types of wireless clients that the device will accept.  <b>eg: 2.4 Ghz (B+G)</b> Only 802.11b and 11g clients will be allowed.
<b>ESSID1</b>	Enter the name of your wireless network. You can use up to 32 characters.
<b>Site Survey</b>	Click on [ <b>Site Survey</b> ] to search the existing AP.

## 6.3 Site Survey

### Client Bridge mode:

1. AP list after site survey.

#### Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	4	EAP350_test	00:02:6F:BC:07:3A	TKIPAES	WPAPSKWPA2PSK	100	/b/g/n
2	<input type="radio"/>	8	EnGenius	00:02:6F:C7:EB:70	AES	WPA2PSK	100	/b/g/n
3	<input type="radio"/>	11	ESR600H_2.4GHz_TEST	00:02:6F:C7:EB:38	NONE	OPEN	84	/b/g/n
4	<input type="radio"/>	6	SENAOWL02	00:02:6F:59:26:02	AES	WPA2PSK	100	/b/g
5	<input type="radio"/>	3	SNADSL	00:02:6F:B3:4E:F8	WEP	AUTOWEP	0	/b/g
6	<input type="radio"/>	3	SNADSL	00:02:6F:B3:4F:48	WEP	AUTOWEP	100	/b/g



2. Select an AP and click on [**Add to AP Profile**].

#### Site Survey

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	4	EAP350_test	00:02:6F:BC:07:3A	TKIPAES	WPAPSKWPA2PSK	100	/b/g/n
2	<input checked="" type="radio"/>	8	EnGenius	00:02:6F:C7:EB:70	AES	WPA2PSK	100	/b/g/n
3	<input type="radio"/>	11	ESR600H_2.4GHz_TEST	00:02:6F:C7:EB:38	NONE	OPEN	84	/b/g/n
4	<input type="radio"/>	6	SENAOWL02	00:02:6F:59:26:02	AES	WPA2PSK	100	/b/g
5	<input type="radio"/>	3	SNADSL	00:02:6F:B3:4E:F8	WEP	AUTOWEP	0	/b/g
6	<input type="radio"/>	3	SNADSL	00:02:6F:B3:4F:48	WEP	AUTOWEP	100	/b/g

3. Enter the correct security setting.

### AP Profile Settings

Network Name (SSID) :	EnGenius
Encryption :	WPA pre-shared key ▾
Authentication Type :	WPA2(AES) ▾
Pre-shared Key :	12345678

Save

4. Add AP profile successfully, click on [**Close**] to close the browser.

Add to AP Profile successfully.

Close

5. The AP profile is added in AP Profile Table.

### AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	EnGenius	00:02:6F:C7:EB:70	WPA2_PSK	AES	<input type="checkbox"/>

**Repeater mode:**

1. AP list after site survey.

**Site Survey**

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	4	EAP350_test	00:02:6F:BC:07:3A	TKIPAES	WPAPSKWPA2PSK	100	/b/g/n
2	<input type="radio"/>	8	EnGenius	00:02:6F:C7:EB:70	AES	WPA2PSK	100	/b/g/n
3	<input type="radio"/>	11	ESR600H_2.4GHz_TEST	00:02:6F:C7:EB:38	NONE	OPEN	45	/b/g/n
4	<input type="radio"/>	11	EnGenius650964_3	00:02:6F:65:09:66	NONE	OPEN	100	/b/g/n

Refresh

Connect

2. Select an AP and click on [**Connect**].

**Site Survey**

NO.	Select	Channel	SSID	BSSID	Encryption	Authentication	Signal(%)	Mode
1	<input type="radio"/>	4	EAP350_test	00:02:6F:BC:07:3A	TKIPAES	WPAPSKWPA2PSK	100	/b/g/n
2	<input checked="" type="radio"/>	8	EnGenius	00:02:6F:C7:EB:70	AES	WPA2PSK	100	/b/g/n
3	<input type="radio"/>	11	ESR600H_2.4GHz_TEST	00:02:6F:C7:EB:38	NONE	OPEN	45	/b/g/n
4	<input type="radio"/>	11	EnGenius650964_3	00:02:6F:65:09:66	NONE	OPEN	100	/b/g/n

Refresh

Connect

3. Enter the correct security setting.

**AP Profile Settings**

<b>Network Name (SSID) :</b>	<input type="text" value="EnGenius"/>
<b>Encryption :</b>	<input type="text" value="WPA pre-shared key"/>
<b>Authentication Type :</b>	<input type="text" value="WPA2(AES)"/>
<b>Pre-shared Key :</b>	<input type="text" value="12345678"/>

Save

4. Connect AP successfully, click on **[Close]** to close the browser.

**Connect to EnGenius unsuccessfully..**

Close

5. You can see the Connection Status in Status WEB page.  
View the current wireless connection status and related information.

#### WLAN Repeater Information

Connection Status	Successful
ESSID	EnGenius
Security	WPA2 pre-shared key
BSSID	00:02:6F:30:00:25
Channel	8

#### WLAN Settings

Channel 8

#### SSID\_1

ESSID	EnGenius
Security	WPA2 pre-shared key
BSSID	00:02:6F:30:00:24



## 6.4 Advanced

The **Advanced** option of the **Wireless** menu displays the advanced wireless options of the ECB300.

It is recommended that the ECB300's default settings are used unless the user has experience with advanced networking.

### Client Bridge mode:

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

<b>Fragment Threshold :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(1-2347)

Advanced (Client Bridge mode)	
<b>Fragment Threshold</b>	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
<b>RTS Threshold</b>	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.

### Access Point / WDS AP / Router / Repeater mode:

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

<b>Fragment Threshold :</b>	<input type="text" value="2346"/>	(256-2346)
<b>RTS Threshold :</b>	<input type="text" value="2347"/>	(1-2347)
<b>Beacon Interval :</b>	<input type="text" value="100"/>	(20-1024 ms)
<b>DTIM Period :</b>	<input type="text" value="1"/>	(1-255)
<b>N Data Rate:</b>	Auto ▾	
<b>Channel Bandwidth</b>	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz	
<b>Preamble Type :</b>	<input type="radio"/> Long Preamble <input checked="" type="radio"/> Short Preamble	
<b>CTS Protection :</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
<b>Tx Power :</b>	100 % ▾	

Apply Cancel

Advanced (Access Point / WDS AP / Router / Repeater mode)	
<b>Fragment Threshold</b>	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
<b>RTS Threshold</b>	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.
<b>Beacon Interval</b>	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.

<b>DTIM Period</b>	A <b>Delivery Traffic Indication Message (DTIM)</b> informs all wireless clients that the access point will be transmitting Multi-casted data.
<b>N Data Rate</b>	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
<b>Channel Bandwidth</b>	Set whether each channel uses 20Mhz or 40Mhz transmission frequency. To achieve 11n speeds, 40Mhz channels must be used.
<b>Preamble Type</b>	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, resulting in decreased compatibility, but increased performance.
<b>Tx Power</b>	Set the power output of the wireless signal.

#### WDS Bridge mode:

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

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

<b>Advanced (WDS Bridge mode)</b>	
<b>Fragment Threshold</b>	Specifies the maximum size of the packet per fragment. This function can reduce the chance of packet collision. However, when the fragment threshold is set too low, there will be increased overhead resulting in poor performance.
<b>RTS Threshold</b>	When the packet size is smaller than the RTS Threshold, the packet will be sent without an RTS/CTS handshake, which may result in incorrect transmission.
<b>N Data Rate</b>	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
<b>Channel Bandwidth</b>	Set whether each channel uses 20Mhz or 40Mhz transmission frequency. To achieve 11n speeds, 40Mhz channels must be used.
<b>Preamble Type</b>	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, resulting in decreased compatibility, but increased performance.
<b>Tx Power</b>	Set the power output of the wireless signal.

## 6.5 Security

The **Security** option in the **Wireless** menu allows you to set the wireless security settings.

**Note:** Only in Access Point / WDS AP / Router and Repeater mode.

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

ESSID Selection : EnGeniusCC3004 ▾

Separate :  SSID  STA

Broadcast ESSID : Enable ▾

WMM : Enable ▾

Encryption : Disable ▾  
 Disable  
 WEP  
 WPA pre-shared key  
 WPA RADIUS

Enable 802.1x Authentication

Apply Cancel

Security (Access Point / WDS AP / Router / Repeater mode)	
<b>SSID Selection</b>	Select the SSID that the corresponding security settings will apply to.
<b>Separate</b>	Separating the SSID from each other (or use of STA) prevents communication and data sharing between wireless stations associated with the SSIDs.
<b>Broadcast SSID</b>	If <b>Disabled</b> , the ECB300 will not broadcast the SSID. It will be invisible to the clients.
<b>WMM</b>	Wi-Fi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background. <b>Note:</b> In certain situations, WMM needs to be enabled to achieve 11n transfer speeds.

<b>Encryption</b>	<p>The encryption method to be used on the corresponding SSID. You can choose between WEP, WPA Pre-Shared Key, or WPA RADIUS.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b> - No data encryption is used.</li> <li>• <b>WEP</b> - Data is encrypted using the WEP standard. WEP is the <b>Wired Equivalent Privacy</b> security over a wireless network.</li> <li>• <b>WPA-PSK</b> - Data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. WPA-PSK is <b>Wi-Fi Protected Access</b> using a <b>Pre-Shared Key</b>. This is the equivalent of password protecting your wireless network.</li> <li>• <b>WPA2-PSK</b> - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.</li> <li>• <b>WPA-RADIUS</b> - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.</li> </ul> <p>If this option is selected:</p> <ul style="list-style-type: none"> <li>• This Access Point must have a <b>Client Login</b> on the Radius Server.</li> <li>• Each user must have a <b>User Login</b> on the Radius Server.</li> <li>• Each user's wireless client must support 802.1x and provide the login data when required.</li> <li>• All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.</li> </ul>
-------------------	--

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is then processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

**Enable 802.1x Authentication**

**RADIUS Server IP Address :**

**RADIUS Server Port :**

**RADIUS Server Shared Secret :**

802.1x Authentication	
<b>RADIUS Server IP Address</b>	The IP Address of the RADIUS Server.
<b>RADIUS Server port</b>	The port number of the RADIUS Server.
<b>RADIUS Server password</b>	The RADIUS Server password.

**WEP Encryption:**

<b>Encryption :</b>	WEP
<b>Authentication Type :</b>	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> Auto
<b>Key Length :</b>	64-bit
<b>Key Type :</b>	Hex (10 characters)
<b>Default Key :</b>	Key 1
<b>Encryption Key 1 :</b>	1234567890
<b>Encryption Key 2 :</b>	
<b>Encryption Key 3 :</b>	
<b>Encryption Key 4 :</b>	

WEP Encryption	
<b>Authentication Type</b>	Please ensure that your wireless clients use the same authentication type.
<b>Key type</b>	<b>ASCII:</b> Using characters from the ASCII standard (recommended) <b>HEX:</b> Uses hexadecimal characters.
<b>Key Length</b>	The amount of bits the WEP key will use. <ul style="list-style-type: none"> <li>• <b>64 Bit</b> - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F).</li> <li>• <b>128 Bit</b> - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).</li> </ul>
<b>Default Key</b>	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a <b>Key Value</b> for the <b>Default Key</b> .
<b>Encryption Key #</b>	Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.



**WPA Pre-Shared Key Encryption:**

<b>Encryption :</b>	WPA pre-shared key ▾
<b>WPA Type :</b>	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA2 Mixed
<b>Pre-shared Key Type :</b>	Passphrase ▾
<b>Pre-shared Key :</b>	12345678

WPA Pre-Shared Key Encryption	
<b>WPA type</b>	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings. <ul style="list-style-type: none"> <li>• <b>WPA(TKIP):</b> Uses a Pre-Shared Key with a dynamically generated key for each 128-bit packet.</li> <li>• <b>WPA2(AES):</b> Government standard of WPA2 encryption.</li> <li>• <b>WPA2 Mixed:</b> Allows the use of both WPA and WPA2 clients on the network.</li> </ul>
<b>Pre-shared Key Type</b>	Pre-Shared Key format (ASCII or Hexadecimal).
<b>Pre-shared Key</b>	Wireless clients must use the same key to associate the device to the ECB300. If using passphrase format, the Key must be from 8 to 63 characters in length.

**WPA RADIUS Encryption:**

Encryption :	WPA RADIUS
WPA Type :	<input type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input checked="" type="radio"/> WPA2 Mixed
RADIUS Server IP Address :	<input type="text"/>
RADIUS Server Port :	1812
RADIUS Server Shared Secret :	<input type="text"/>

WPA RADIUS Encryption	
<b>WPA type</b>	<p>Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.</p> <ul style="list-style-type: none"> <li>• <b>WPA(TKIP):</b> Uses a Pre-Shared Key with a dynamically generated key for each 128-bit packet.</li> <li>• <b>WPA2(AES):</b> Government standard of WPA2 encryption.</li> </ul> <p><b>WPA2 Mixed:</b> Allows the use of both WPA and WPA2 clients on the network.</p>
<b>RADIUS Server IP address</b>	Enter the IP address of the RADIUS Server.
<b>RADIUS Server Port</b>	Enter the port number used for connections to the RADIUS server.
<b>RADIUS Server password</b>	Enter the password required to connect to the RADIUS server.

## 6.6 Filter

The **Filter** option in the **Wireless** menu allows users to allow clients with specific MAC Addresses to join the SSID.

**Note:** Only in Access Point / WDS AP / Router and Repeater mode.

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

**Enable Wireless MAC Filtering**

Description	MAC Address
rule02	80A49E837BA2

Add Reset

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

NO.	Description	MAC Address	Select
1	rule01	00:21:6A:78:8E:70	<input type="checkbox"/>

Delete Selected Delete All Reset

Apply Cancel

Wireless MAC Filter (Access Point / WDS AP / Router / Repeater mode)	
<b>Enable Wireless Access Control</b>	Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
<b>Description</b>	Enter a name or description for this entry.
<b>MAC Address</b>	Enter the MAC address of the wireless client that you wish to allow connection.

<b>Add</b>	Click this button to add the entry.
<b>Reset</b>	Click this button if you have made a mistake and want to reset the MAC address and Description fields.
<b>MAC Address Filtering Table</b>	
Only clients listed in this table will be allowed access to the wireless network.	
<b>Delete Selected</b>	Delete the selected entries.
<b>Delete All</b>	Delete all entries.
<b>Reset</b>	Deselect all entries.

## 6.7 WPS (Wi-Fi Protected Setup)

The **WPS** feature in the **Wireless** menu follows the Wi-Fi Alliance WPS standard. It eases the set up of security-enabled Wi-Fi networks in homes and/or small office environments.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

**Note:** Only in Access Point / WDS AP and Router mode.

<b>WPS:</b>	<input checked="" type="checkbox"/> Enable
<b>Wi-Fi Protected Setup Information</b>	
<b>WPS Current Status:</b>	unConfigured
<b>Self Pin Code:</b>	31457644
<b>SSID:</b>	EnGenius300024
<b>Authentication Mode:</b>	Disabled
<b>Passphrase Key :</b>	<input type="text"/>
<b>WPS Via Push Button:</b>	<input type="button" value="Start to Process"/>
<b>WPS Via PIN:</b>	<input type="text"/> <input type="button" value="Start to Process"/>

Wi-Fi Protected Setup (WPS)	
<b>WPS</b>	Check to Enable the WPS feature.
Wi-Fi Protected Setup Information	
<b>WPS Current Status</b>	Shows whether the WPS function is <b>Configured</b> or <b>Un-configured</b> . Configured means that WPS has been used to authorize connection between the ECB300 and the wireless clients.

<b>SSID</b>	The SSID (network name) used when connecting using WPS.
<b>Authentication Mode</b>	Shows the encryption method used by the WPS process. This is set as the mode selected in the <b>Security</b> option in the <b>Wireless</b> menu.
<b>Passphrase Key</b>	This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.
<b>WPS Via Push Button</b>	Activate WPS using a push button.
<b>WPS Via PIN</b>	Activate WPS using the PIN code from the WPS device.

## 6.8 Client List

The **Client List** option of the **Wireless** menu shows all the wireless clients that are currently connected to the ECB300.

**Note:** Only in Access Point / WDS AP / Router and Repeater mode.

### WLAN Client Table :

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

Interface	MAC Address	Rx	Tx	Signal(%)	Connected Time	Idle Time
EnGenius300024	00:02:6F:4D:F2:1E	242.5 KBytes	245.5 KBytes	54	1 min 38 secs	0 secs
EnGenius300024	00:02:6F:11:AC:93	248.3 KBytes	242.3 KBytes	58	1 min 35 secs	0 secs

Refresh

## 6.9 VLAN

The **VLAN** option of the **Wireless** menu allows you to configure the VLAN (Virtual LAN).

**Note:** Only in Access Point mode.

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

<b>Virtual LAN :</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>SSID 1 Tag:</b>	<input type="text" value="100"/> (1~4094)
<b>LAN VLAN MGMT :</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>MGMT Tag:</b>	<input type="text" value="500"/> (1~4094)

VLAN (Access Point and WDS AP mode)	
<b>Virtual LAN</b>	Choose to Enable or Disable the VLAN feature.
<b>SSID# Tag</b>	Specify the VLAN tag for each SSID.
<b>LAN VLAN MGMT</b>	Choose to Enable or Disable the LAN VLAN MGMT feature.
<b>MGMT Tag</b>	Specify the VLAN tag for the LAN.



## 6.10 AP Profile

This page allows you to configure the profile of the Client Bridge including Security Setting exactly the same as the Access Point. You can save three AP profiles at most.

**Note:** Only in Client Bridge mode.

### AP Profile Table

NO.	SSID	MAC	Authentication	Encryption	Select
1	EnGenius	00:02:6F:C7:EB:70	WPA2_PSK	AES	<input checked="" type="checkbox"/>

AP Profile Table (Client Bridge mode)	
<b>Add / Edit</b>	Select a profile to add or edit.
<b>Move Up / Move Down</b>	Select a profile to move up or move down.
<b>Delete Selected</b>	Delete the selected entries.
<b>Delete All</b>	Delete all entries
<b>Connect</b>	Select a profile to connect.

**AP Profile Settings**

<b>Network Name (SSID) :</b>	<input type="text" value="EnGenius"/>	
<b>Encryption :</b>	<input type="text" value="Disable"/> <ul style="list-style-type: none"> <li>Disable</li> <li>WEP</li> <li style="background-color: #e0e0e0;">WPA pre-shared key</li> <li>RADIUS</li> </ul>	<input type="button" value="Save"/>

AP Profile Settings	
<b>Network Name (SSID)</b>	Enter the SSID (Network Name) of the wireless network which ERB9260 want to connect.
<b>Encryption</b>	The encryption method to be applied. You can choose from Disable, WEP, WPA pre-shared key and RADIUS. Please select the correct security type.

## 7 Network

### 7.1 Status

The **Status** option of the **Network** menu shows the current status of the ECB300's LAN and WAN (Router mode) connection.

View the current wireless connection status and related information.

#### LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	00:02:6F:30:00:24

#### WAN Settings

Attain IP Protocol	Dynamic IP Address
IP Address	192.168.7.162
Subnet Mask	255.255.255.0
Default Gateway	192.168.7.10
MAC Address	00:02:6F:30:0A:24
Primary DNS	192.168.7.10
Secondary DNS	---

Renew

## 7.2 LAN

The **LAN** option of the **Network** menu allows you to modify the device's LAN settings.

The LAN setting in Router mode:

Bridge Type :	Static IP ▾
IP Address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
DNS Type :	Static ▾
First DNS Address :	192.168.1.1
Second DNS Address :	192.168.1.1

There is additional setting **Default Gateway** in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.

Bridge Type :	Static IP ▾
IP Address :	192.168.1.1
IP Subnet Mask :	255.255.255.0
Default Gateway :	
DNS Type :	Static ▾
First DNS Address :	192.168.1.1
Second DNS Address :	192.168.1.1

LAN IP	
<b>Bridge Type</b>	Select the Bridge type of the LAN. <b>Static IP:</b> Manually specify an IP address and subnet mask for the ECB300 to use. <b>Dynamic IP:</b> The IP address is received automatically from the external DHCP server. <b>Note:</b> The option: Dynamic IP is only in Access Point and WDS AP mode.
<b>IP Address</b>	The LAN IP Address of this device.
<b>IP Subnet Mask</b>	The LAN Subnet Mask of this device.
<b>Default Gateway</b>	The Default Gateway of the device. Leave empty for default setting. <b>Note:</b> The option: Dynamic IP is only in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.
<b>DNS Type</b>	Select the DNS type of the LAN. <b>Static:</b> Manually specify the DNS of the ECB300. <b>Dynamic:</b> The DNS is received automatically from the external DNS server. <b>Note:</b> The option: Dynamic is only in Access Point and WDS AP mode.
<b>First / Second DNS Address</b>	The first / second DNS address for this device.

The **DHCP Server** feature is only available in Access Point and Router mode.

#### DHCP Server

<b>DHCP Server :</b>	Enabled ▾
<b>Lease Time :</b>	Forever ▾
<b>Start IP :</b>	192.168.1.100
<b>End IP :</b>	192.168.1.200
<b>Domain Name :</b>	ecb300
<b>First DNS Address :</b>	
<b>Second DNS Address :</b>	

<b>DHCP Server (Access Point / Router mode)</b>	
<b>DHCP Server</b>	Enable or disable DHCP feature. The DHCP Server automatically allocates IP addresses to your LAN device. Disabled as default.
<b>Lease Time</b>	The duration of the DHCP server allocates each IP address to a LAN device.
<b>Start / End IP</b>	The range of IP addresses of the DHCP server will allocate to LAN device.
<b>Domain name</b>	The domain name for this LAN network.
<b>First / Second DNS Address</b>	The first / second DNS address for this LAN network.

## 7.3 Spanning Tree

The **Spanning Tree** option of the **Network** menu allows you to set the ECB300 to use the Spanning Tree Protocol. Enabling Spanning Tree Protocol will prevent network loops in your LAN network.

**Note:** Only in Access Point / Client Bridge / WDS AP / WDS Bridge and Repeater mode.

### Spanning Tree Settings

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

Spanning Tree Settings	
<b>Spanning Tree Status</b>	Enable or disable the Spanning Tree Protocol.
<b>Bridge Hello Time</b>	The duration of the initial connection between two access points.
<b>Bridge Max Age</b>	The maximum amount of time the bridge is connected when transmitting.
<b>Bridge Forward Delay</b>	The delay between transmissions between access points.
<b>Bridge Priority</b>	The priority port of the Spanning Tree Protocol.

## 7.4 WAN (Router mode)

The WAN section allows you to manually set the WAN type connection and its related settings.

**Note:** Only in Router mode.

### 7.4.1 Static IP Address

If your ISP Provider has assigned you a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS and Secondary DNS (if available) of your ISP provider.

<b>Login Method:</b>	Static IP Address ▾
<b>IP Address:</b>	0.0.0.0
<b>IP Subnet Mask :</b>	0.0.0.0
<b>Default Gateway :</b>	0.0.0.0
<b>Primary DNS :</b>	
<b>Secondary DNS :</b>	
<b>Interface :</b>	WAN

Static IP Address	
<b>IP Address</b>	Assign an IP address Manually.
<b>IP Subnet Mask</b>	Specify an IP address's subnet mask.
<b>Default Gateway</b>	Specify the gateway of your network.
<b>Primary DNS</b>	Specify the primary DNS server's IP address.
<b>Secondary DNS</b>	Specify the second DNS server's IP address.



## 7.4.2 Dynamic IP Address

The IP Address is allocated automatically. However some ISP's will also recognize the MAC address and will reject connections if the MAC address does not match.

If your ISP has recorded the MAC address of your computer's Ethernet LAN card, please connect only the computer with the authorized MAC address, and click the **Clone MAC** button.

**Note:** This will replace the WAN MAC address to the computer MAC address. The correct MAC address is used to initiate the connection to the ISP.

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

Dynamic IP Address	
<b>Hostname</b>	This is optional. Only required if specified by ISP
<b>MAC Address</b>	The MAC Address that is used to connect to the ISP.

### 7.4.3 PPP over Ethernet (PPPoE)

This protocol is used by most DSL services worldwide.

Select this option if you have a DSL connection.

Enter the username and password provided by your ISP.

<b>Login Method:</b>	PPP over Ethernet ▾
<b>Login :</b>	<input type="text"/>
<b>Password :</b>	<input type="password"/>
<b>Service Name</b>	<input type="text"/>
<b>MTU :</b>	1492 (512<=MTU Value<=1492)
<b>Type :</b>	Keep Connection ▾
<b>Idle Timeout :</b>	10 (1-1000 Minutes)

PPP over Ethernet (PPPoE)	
<b>Login</b>	Username assigned to you by the ISP
<b>Password</b>	Password for this username.
<b>Service Name</b>	You can assign a name for this service. (Optional)
<b>MTU</b>	The maximum size of packets. Do not change unless mentioned by the ISP.
<b>Type</b>	You can choose the method that the router maintains connection with the ISP. <b>Keep Connection:</b> The device will maintain a constant connection with the ISP. <b>Automatic Connection:</b> The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. <b>Manual Connection:</b> The user will need to manually connect to the ISP by clicking the <b>Connect</b> button.
<b>Idle Timeout:</b>	When the connection type is <b>Automatic Connection</b> , when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

## 7.4.4 Point-to-Point Tunneling Protocol (PPTP)

PPTP is used by very few ISPs.

<b>Login Method :</b>	<input type="text" value="PPTP"/>
<b>WAN Interface Settings :</b>	
<b>WAN Interface Type :</b>	<input type="text" value="Dynamic IP Address"/>
<b>Hostname :</b>	<input type="text"/>
<b>MAC address:</b>	<input type="text" value="000000000000"/> <input type="button" value="Clone MAC"/> <input type="button" value="Set Default"/>
<b>PPTP Settings :</b>	
<b>Login :</b>	<input type="text"/>
<b>Password :</b>	<input type="text"/>
<b>Service IP Address :</b>	<input type="text"/>
<b>Connection ID :</b>	<input type="text" value="0"/> (Optional)
<b>MTU :</b>	<input type="text" value="1400"/> (512<=MTU Value<=1492)
<b>Type :</b>	<input type="text" value="Keep Connection"/>
<b>Idle Timeout :</b>	<input type="text" value="10"/> (1-1000 Minutes)

<b>Point-to-Point Tunneling Protocol (PPTP)</b>	
<b>WAN Interface Type</b>	Select whether the ISP is set to Static IP or will allocate Dynamic IP address.
<b>Hostname</b>	This is optional. Only required if specified by ISP
<b>MAC address</b>	The MAC Address that is used to connect to the ISP.
<b>Login</b>	Username assigned to you by the ISP
<b>Password</b>	Password for this username.
<b>Service IP Address</b>	The IP Address of the PPTP server.
<b>Connection ID</b>	This is optional. Only required if specified by ISP
<b>MTU</b>	The maximum size of packets. Do not change unless mentioned by the ISP.
<b>Type</b>	You can choose the method that the router maintains connection with the ISP. <b>Keep Connection:</b> The device will maintain a constant connection with the ISP. <b>Automatic Connection:</b> The device will only initiate connection to the ISP when there is an Internet connection request made from a LAN device. <b>Manual Connection:</b> The user will need to manually connect to the ISP by clicking the <b>Connect</b> button.
<b>Idle Timeout:</b>	When the connection type is <b>Automatic Connection</b> , when Internet traffic is idle, then the device will automatically disconnect from the ISP. Please specify the Idle time in minutes.

## 8 Firewall

The Firewall section allows you to set the access control and Firewall settings.

**Note:** Only in Router mode.

### 8.1 Enable

This page allows you to Enable / Disable the Firewall features.

If enabled Firewall service, the Denial of Service (DoS) and SPI (Stateful Packet Inspection) features will also be enabled.

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

Firewall :  Enable  Disable

Apply

## 8.2 DMZ

If enabled this feature, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the server.
- The “DMZ PC” will receive all Unknown connections and data.
- If the DMZ feature is enabled, please enter the IP address of the PC to be used as the “DMZ PC”

**Note:** The “DMZ PC” is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

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

**Enable DMZ**

**Local IP Address :**

### 8.3 DoS

Denial of Service (Denial of Service) is a type of Internet attack that sends a high amount of data to you with the intent to overload your Internet connection.

Enable the DoS firewall feature to automatically detect and block these DoS attacks.

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

Block DoS :  Enable  Disable

Apply Cancel

## 8.4 MAC Filter

You can choose whether to Deny or only Allow those computers listed in the MAC Filtering table to access the Internet.

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

**Enable MAC Filtering**

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

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

Description	LAN MAC Address
rule02	00026F11AC93

Add

Reset

**MAC Filtering table:**

NO.	Description	LAN MAC Address	Select
1	rule01	00:13:64:78:41:CE	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

MAC Filter	
<b>Enable MAC filtering</b>	Tick this box to Enable the MAC filtering feature.
<b>Deny all clients with MAC addresses listed below to access the network</b>	When selected, the computers listed in the MAC Filtering table will be <b>Denied</b> access to the Internet.
<b>Allow all clients with MAC addresses listed below to access the network</b>	When selected, only the computers listed in the MAC Filtering table will be <b>Allowed</b> access to the Internet.



## 8.5 IP Filter

You can choose whether to Deny or only Allow, computer with those IP Addresses from accessing certain Ports.

This can be used to control which Internet applications the computers can access.

You may need to have certain knowledge of what Internet ports the applications use.

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

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

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

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

<b>Description :</b>	<input type="text"/>
<b>Protocol :</b>	Both ▾
<b>Local IP Address :</b>	<input type="text"/> ~ <input type="text"/>
<b>Port Range :</b>	<input type="text"/> ~ <input type="text"/>

NO.	Description	Local IP Address	Protocol	Port Range	Select
1	rule01	192.168.1.100	BOTH	21-22	<input type="checkbox"/>

IP Filter	
<b>Enable IP filtering</b>	Tick this box to Enable the IP filtering feature.
<b>Deny all clients with IP addresses listed below to access the network</b>	When selected, the computers with IP addresses specified will be <b>Denied</b> access to the indicated Internet ports.
<b>Allow all clients with IP addresses listed below to access the network</b>	When selected, the computers with IP addresses specified will be <b>Allowed</b> access only to the indicated Internet ports.

## 8.6 URL Filter

You can deny access to certain websites by blocking keywords in the URL web address.

For example, "gamer" has been added to the URL Blocking Table. Any web address that includes "gamer" will be blocked.

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

Enable Website Blocking

Website/keyword

Add

Reset

Current Website Blocking Table:

NO.	Website/keyword	Select
1	test123	<input type="checkbox"/>

Delete Selected

Delete All

Reset

Apply

Cancel

## 9 Advanced

The **Advanced** section allows you to configure the Advanced settings of the router.

**Note:** Only in Access Point Client Router mode.

### 9.1 Network Address Translation (NAT)

This page allows you to Enable / Disable the Network Address Translation (NAT) feature. The NAT is required to share one Internet account with multiple LAN users.

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

NAT :  Enable  Disable

Apply

## 9.2 Port Mapping

Port Mapping allows you to redirect a particular range of ports to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a FTP Server that requires ports 21 to 22.

When there is a connection from the Internet on those ports, it will be redirected to the FTP Server at IP address 192.168.1.100.

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

**Enable Port Mapping**

**Description :**

**Local IP :**

**Protocol :** Both ▾

**Port Range :**  ~

**Current Port Mapping Table:**

NO.	Description	Local IP	Type	Port Range	Select
1	rule01	192.168.1.100	BOTH	21-22	<input type="checkbox"/>

Port Mapping	
<b>Enable Port Mapping</b>	Check this box to enable the Port Mapping feature.
<b>Description</b>	Enter a name or description for this entry.
<b>Local IP</b>	The local IP address of the computer the server is hosted on.
<b>Protocol</b>	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
<b>Port Range</b>	The range of ports that this feature will be applied to.

### 9.3 Port Forwarding

Port Forwarding allows you to redirect a particular public port to a computer on your LAN network. This helps you host servers behind the NAT and Firewall.

In the example below, there is a Web Server running on port 80 on the LAN.

For security reasons, the Administrator would like to provide this server to Internet connection on port 100.

Therefore when there is a connection from the Internet on port 100, it will be forwarded to the computer with the IP address 192.168.1.150 and changed to port 80.

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

**Enable Port Forwarding**

**Description :**

**Local IP :**

**Protocol :** Both ▾

**Local Port :**

**Forwarded Port :**

**Current Port Forwarding Table :**

NO.	Description	Local IP	Local Port	Type	Forwarded Port	Select
1	rule01	192.168.1.150	80	BOTH	100	<input type="checkbox"/>

Port Forwarding	
<b>Enable Port Forwarding</b>	Check this box to enable the Port Forwarding feature.
<b>Description</b>	Enter a name or description for this entry.
<b>Local IP</b>	The local IP address of the computer the server is hosted on.
<b>Protocol</b>	Select to apply the feature to TCP, UDP or Both types of packet transmissions.
<b>Local Port</b>	The port that the server is running on the local computer.
<b>Forwarded Port</b>	When a connection from the Internet is on this port, it will be forwarded to the indicated local IP address.

## 9.4 Port Triggering

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. Port Triggering will be required for these applications to work.

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

**Enable Trigger Port**

**Description :** PC-to-Phone

**Popular Applications :** PC-to-Phone

**Trigger Port :** 12053 ~

**Trigger Type :** Both

**Forwarded Port :** 12120,12122,24150-24220

**Public Type :** Both

**Current Trigger-Port Table:**

NO.	Trigger Port	Trigger Type	Forwarded Port	Public Type	Name	Select
1	28800	BOTH	2300-2400,47624	BOTH	MSN Gaming Zone	<input type="checkbox"/>

Port Triggering	
<b>Enable Port Triggering</b>	Check this box to enable the Port Trigger feature.
<b>Popular Applications</b>	This is a list of some common applications with preset settings. Select the application and click <b>Add</b> to automatically enter the settings.
<b>Trigger Port</b>	This is the outgoing (outbound) port numbers for this application.
<b>Trigger Type</b>	Select whether the application uses TCP, UDP or Both types of protocols for outbound transmissions.
<b>Forwarded Port</b>	These are the inbound (incoming) ports for this application.
<b>Public Type</b>	Select whether the application uses TCP, UDP or Both types of protocols for inbound transmissions.

## 9.5 Application Layer Gateway (ALG)

Certain applications may require the use of the ALG feature to function correctly. If you use any of the applications listed on the table below, select the feature and click Apply.

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

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

Apply Cancel



## 9.6 Universal Plug and Play (UPnP)

The UPnP function allows automatic discovery and configuration of UPnP enabled devices on your network. It also provides automatic port forwarding for supported applications to seamlessly bypass the Firewall.

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

UPnP :  Enable  Disable

Apply

## 9.7 Quality of Service (QoS)

QoS allows you to control the priority that the data is transmitted over the Internet, or to reserve a specific amount of Internet bandwidth. This is to ensure that applications get enough Internet bandwidth for a good user experience.

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

QoS :  Priority Queue  Bandwidth Allocation  Disabled

Apply Cancel

QoS	
<b>Priority Queue</b>	Sets the QoS method to Priority Queue.
<b>Bandwidth Allocation</b>	Sets the QoS method to Bandwidth Allocation.
<b>Disabled</b>	Disables the QoS feature.

**Priority Queue Method**

Bandwidth priority is set to either High or Low. The data transmissions in the High Priority queues will be processed first.

QoS :  Priority Queue  Bandwidth Allocation  Disabled

**Unlimited Priority Queue**

IP Address	Description
<input type="text"/>	The IP address will not be bounded in the QoS limitation

**High/Low Priority Queue**

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

Apply Cancel

Unlimited Priority Queue	
<b>IP Address</b>	The computer with this IP Address will not be bound by the QoS rules.
High / Low Priority Queue	
<b>Protocol</b>	The type of network protocol.
<b>High / Low Priority</b>	Sets the protocol to High or Low priority.
<b>Specific Port</b>	Each protocol uses a specific port range. Please specify the ports used by this protocol.

### Bandwidth Allocation Method

You can set the maximum amount of bandwidth a certain protocol will use at one time. Or you can set a minimum amount of bandwidth that will be guaranteed to a certain protocol.

QoS :  Priority Queue  Bandwidth Allocation  Disabled

Type : download ▾

IP range :  ~

Protocol : All ▾

Port Range : 1 ~ 65535

Policy : Min ▾

Rate(bps) : FULL ▾

**Current QoS Table:**

NO.	Type	IP range	Protocol	Port Range	Policy	Rate (bps)	Select
1	download	192.168.1.100 ~ 192.168.1.101	ALL	1 ~ 65535	Max	2M	<input type="checkbox"/>

Bandwidth Allocation	
<b>Type</b>	Set whether the QoS rules apply to transmission that are Download, Upload or Both directions.
<b>IP range</b>	Enter the IP address range of the computers that you would like the QoS rules to apply to.
<b>Protocol</b>	Select from this list of protocols to automatically set the related port numbers.
<b>Port Range</b>	Each protocol uses a specific port range. Specify the ports used by this protocol.
<b>Policy</b>	Choose whether this rule is to set a limit on the <b>Maximum</b> amount of bandwidth allocated to the specified protocol, or to set the guaranteed <b>Minimum</b> amount of bandwidth for the protocol.

## 9.8 Static Routing

If your wireless router is connected to a network with different subnets, this feature will allow the different subnets to communicate with each other.

**Note:** The NAT function needs to be disabled for the Routing feature to be enabled.

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

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

**Enable Static Routing**

**Destination LAN IP:**

**Subnet Mask:**

**Default Gateway:**

**Current Static Routing Table:**

NO.	Destination LAN IP	Subnet Mask	Default Gateway	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>				

Static Routing	
<b>Enable Static Routing</b>	Check this box to enable the Static Router feature.
<b>Destination LAN IP</b>	Enter the IP address of the destination LAN.
<b>Subnet Mask</b>	Enter the Subnet Mask of the destination LAN IP address
<b>Default Gateway</b>	Enter the IP address of the Default Gateway for this destination IP and Subnet.

## 9.9 Dynamic Routing

Dynamic routing allows routing tables in routers to change as the possible routes change. This device use RIP to support dynamic routing.

The Router supports the Routing Information Protocol (RIP). RIP allows you to set up routing information on one RIP enabled device, and have that routing information replicated to all RIP enabled devices on the network.

**Dynamic Routing**

<b>RIP Transferring:</b>	RIPv1/RIPv2 ▼
<b>RIP Receiving:</b>	RIPv1/RIPv2 ▼
<b>Password:</b>	<input type="text"/>

## 9.10 Routing Table

This page allows you to observe the current routing table.

### Current Routing Table

Destination LAN IP	Subnet Mask	Default Gateway
192.168.66.1	255.255.255.255	192.168.66.1
192.168.1.0	255.255.255.0	0.0.0.0
192.168.66.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	192.168.66.1

Refresh

## 10 Management

### 10.1 Admin

The **Admin** section of the **Management** menu allows you to change the ECB300 default password and to configure remote management (Router mode). By default, the password is: **admin**. The password can contain 0 to 12 alphanumeric characters and is case sensitive.

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"/>
Confirm password :	<input type="text"/>
Idle Timeout :	<input type="text" value="10"/> (1~10 Minutes)

Change Password	
Old Password	Enter the current password.
New Password	Enter your new password.
Confirm Password	Re-enter your new password.
Idle Timeout	Enter Administration Page timeout time (minutes).



There is additional setting **Remote Management** in Router mode.

Remote management allows the router 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" value="0.0.0.0"/>	<input type="text" value="8080"/>	<input type="checkbox"/>

Remote Management (Router mode)	
<b>Host Address</b>	You can only perform remote management from the specified IP address. Leave blank to allow any host to perform remote management.
<b>Port</b>	Enter the port number you want to accept remote management connections.
<b>Enable</b>	Tick to Enable the remote management feature.

## 10.2 SNMP

The **SNMP** section of the **Management** menu allows you to assign the contact details, location, community name, and trap settings for the Simple Network Management Protocol (SNMP). The SNMP 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 (Agents) return data stored in their Management Information Bases.

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

<b>SNMP Active</b>	Enabled ▾
<b>SNMP Version</b>	All ▾
<b>SNMP Manager IP</b>	0.0.0.0
<b>Read Community</b>	public
<b>Set Community</b>	private
<b>System Location</b>	EnGenius Technologies, Inc.
<b>System Contact</b>	SENAO Networks, Inc.
<b>Trap Active</b>	Disabled ▾
<b>Trap Manager IP</b>	192.168.1.100
<b>Trap Community</b>	public

Apply Cancel

SNMP	
<b>SNMP Active</b>	Enable or disable the SNMP feature.
<b>SNMP Version</b>	You may select the SNMP version you want to deploy. <b>All:</b> Interoperability between SNMPv1 and SNMPv2c devices. <b>v1:</b> The standard SNMP version. <b>v2c:</b> Improvement in performance and security of SNMPv1.
<b>Read Community</b>	Specify the password for access the SNMP community for read only access.
<b>Set Community</b>	Specify the password for access to the SNMP community with read/write access.
<b>System Location</b>	Specify the location of the device.
<b>System Contact</b>	Specify the contact details of the device
Trap	
<b>Trap Active</b>	Enable or disable SNMP trapping feature.
<b>Trap Manager IP</b>	Specify the IP address of the computer that will receive the SNMP traps.
<b>Trap Community</b>	Specify the password for the SNMP trap community.

## 10.3 Firmware Upgrade

The **Firmware Upgrade** section of the **Management** allows you to upgrade the ECB300's firmware.

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

### To perform the Firmware Upgrade:

1. Download the firmware version that you want to install into the ECB300 and place it in a known location.
2. Click the **Browse** button and navigate to the location of the firmware upgrade file.
3. Select the firmware upgrade file. Its name will appear in the **Upgrade File** field.
4. Click the **Apply** button to commence the firmware upgrade.

**Note:** The device is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the device will be lost.

## Emergency Upgrade

If your firmware upgrade failed, you may enter the Emergency Upgrade WEB page.

1. Enter IP address: **192.168.99.9** and enter Emergency Upgrade WEB page.



**Note:** Refer to 2.2 to configure PC/Notebook IP address to 192.168.99.8.

2. Click the **Browse** button and navigate to the location of the upgrade file and then click **Upload**.

### Emergency Web Server

File

3. Wait for 60 seconds for firmware upgrade and reboot the device.

**Updating File.....**

---

**Don't Power Down.**

Please wait for **58** seconds ...

101

4. You can access the device again.



The image shows a login dialog box for EnGenius. It has a title bar with the text "EnGenius". Below the title bar, there are two input fields: "Username:" with the text "admin" and "Password:" with five black dots. At the bottom of the dialog box, there are two buttons: "Login" and "Cancel".

## 10.4 Configure

The **Configure** option of the **Management** menu allows you to save the current device configurations. When you save the configurations, you also can re-load the saved configurations into the device through the **Restore Settings**. If extreme problems occur press the **Reset** button of the **Restore to Factory Defaults** option to set all configurations to its original default settings.

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

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

Configure	
<b>Restore to Factory Default</b>	Restores the device to factory default settings.
<b>Backup Settings</b>	Save the current configuration settings to a file.
<b>Restore Settings</b>	Restores a previously saved configuration file. Click <b>Browse</b> to select the file. Then <b>Upload</b> to load the settings.

## 10.5 Reset

In some circumstances it may be required to force the device to reboot. Click on **Apply** to reboot of the **Reset** option of the **Management** menu.

In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.

Apply



## 11 Tools

### 11.1 Time Setting

The **Time Setting** section of the **Tools** menu allows you to set the ECB300's time.

The device reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

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

Time	
<b>Time Setup</b>	Select the method you want to set the time.
<b>Time Zone</b>	Select the time zone for your current location.
<b>NTP Time Server</b>	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
<b>Daylight Savings</b>	Check whether daylight savings applies to your area.

## 11.2 Diagnosis

The **Diagnosis** section of the **Tools** menu allows you to test your network. Type in the IP Address of the device for diagnosis.

This page can diagnose the current network status.

Address to Ping :

Ping Frequency :

Diagnosis	
<b>Address to Ping</b>	Enter the IP address you like to see if a successful connection can be made.
<b>Ping Frequency</b>	Select the frequency for Ping test.
<b>Ping Result</b>	The results of the Ping test.

## 12 Logout

Click on **Logout** button to logout of the ECB300.

This page is used to logout this device.

Logout

## Appendix A – FCC Interference Statement

---

### Federal Communication Commission Interference Statement

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

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

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.

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

### **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.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

## 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. Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

### 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.

### NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

#### Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device has been designed to operate with a **diople** antenna have 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.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (**IC: 10103A-ECB300 / Model: ECB300**) has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de diopole antenne avec dBi[5]. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio (IC: 10103A-ECB300 / Modèle: ECB300) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

## Appendix C – CE Interference Statement

---

### Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:










- EN60950-1:2006 A11:2009+A1:2010+A12:2011
- Safety of Information Technology Equipment
  
- EN50385 : 2002
- Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
  
- EN 300 328 V1.7.1: 2006-10
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
  
- EN 301 489-1 V1.8.1: 2008-04
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
  
- EN 301 489-17 V2.1.1 2009-05
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

# CE 0560!

 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.



Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.