



**11N Long Range Multi-Function Gigabit CB / AP**



**ECB350**

**11N Long Range Multi-Function Gigabit CB / AP**

*V1.0*

4Gon [www.4Gon.co.uk](http://www.4Gon.co.uk) [info@4gon.co.uk](mailto:info@4gon.co.uk) Tel: +44 (0)1245 808295 Fax: +44 (0)1245 808299

## Table of Contents

---

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
1.1	Features and Benefits .....	5
1.2	Package Contents .....	6
1.3	System Requirements.....	7
1.4	Applications.....	7
<b>2</b>	<b>Before you Begin .....</b>	<b>9</b>
2.1	Considerations for Wireless Installation .....	9
2.2	Computer Settings (Windows XP/Windows 7) .....	10
2.3	Apple Mac X OS.....	13
2.4	Hardware Installation .....	14
<b>3</b>	<b>Configuring Your Client Bridge .....</b>	<b>16</b>
3.1	Default Settings .....	16
3.2	Web Configuration.....	17
<b>4</b>	<b>Building a Wireless Network .....</b>	<b>19</b>
4.1	Client Bridge Mode .....	19
4.2	Client Router Mode.....	20
4.3	Access Point Mode .....	21
4.4	Access Point Router Mode .....	22
4.5	WDS AP / WDS Station Mode.....	23
4.6	WDS Bridge Mode.....	24
4.7	Repeater mode .....	25
<b>5</b>	<b>Status .....</b>	<b>26</b>
5.1	Save/Reload.....	26
5.2	Main.....	27

5.3	Connection Status.....	29
5.4	Wireless Client List.....	30
5.5	System Log .....	31
<b>6</b>	<b>System .....</b>	<b>32</b>
6.1	Operation Mode.....	32
6.2	IP Settings .....	33
6.3	Spanning Tree Setting.....	34
<b>7</b>	<b>Router .....</b>	<b>36</b>
7.1	WAN Settings .....	36
7.1.1	Static IP .....	36
7.1.2	DHCP .....	39
7.1.3	PPPoE .....	41
7.1.4	PPTP .....	43
7.2	LAN Settings.....	45
7.3	VPN Pass Through .....	46
7.4	Port Forwarding .....	47
7.5	Port Triggering .....	49
7.6	DMZ.....	51
7.7	MAC Filter.....	52
7.8	IP Filter.....	53
7.9	URL Filter .....	55
<b>8</b>	<b>Wireless .....</b>	<b>56</b>
8.1	Wireless Network .....	56
8.2	Wireless Security .....	60
8.3	Site Survey .....	63
8.4	Wireless MAC Filter .....	67
8.5	Wireless Advanced .....	68

8.6	WPS (Wi-Fi Protected Setup).....	70
8.7	WDS Link Settings.....	72
<b>9</b>	<b>Management.....</b>	<b>74</b>
9.1	Administration.....	74
9.2	Management VLAN.....	75
9.3	SNMP Settings .....	76
9.4	Backup/Restore.....	78
9.5	Firmware Upgrade .....	79
9.6	Time Setting .....	80
9.7	Log .....	81
9.8	Diagnostics .....	82
9.9	LED Control.....	83
9.10	Logout .....	84
9.11	Reset.....	85
	<b>Appendix A – FCC Interference Statement .....</b>	<b>86</b>
	<b>Appendix B – IC Interference Statement .....</b>	<b>87</b>
	<b>Appendix C – CE Interference Statement.....</b>	<b>89</b>

## Revision History

Version	Date	Notes
1.0	2012/02/22	First Release

# 1 Introduction

The **ECB350** is a multi-function 802.11b/g/n product with 8 major multi-functions. The ECB350 is designed to operate in every working environment including enterprises.

The ECB350 is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11b/g devices. The ECB350 supports use in the home network with superior throughput, performance, and significant wireless range.

To protect data during wireless transmissions, the ECB350 encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2 encryption. The ECB350 has MAC address filtering to allow users to select differing stations to access the network. The ECB350 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>
10/100/1000 Fast Ethernet	<b>Support up to 1000Mbps 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, WDS Station, Universal Repeater, Router or Client Router 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 ECB350 easily.</b>
<b>QoS (WMM) support</b>	<b>Enhanced user performance and density.</b>

## 1.2 Package Contents

The ECB350 package contains the following items (all items must be in package to issue a refund):

- ECB350 Wireless Long Range Multi-Function CB / AP
- 12V/1A 100V~240V Power Adapter
- RJ-45 Ethernet LAN Cable
- CD-ROM with User's Manual
- Quick User 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 function
- Windows OS (XP, Vista, 7), Mac OS, or Linux based operating systems
- Web-Browsing Application (i.e.: 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 or 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 ECB350 is essential to maximize the ECB350's performance. Avoid placing the ECB350 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 ECB350's wireless signals must pass through. Here are some key guidelines to allow the ECB350 to have optimal wireless range.

- Keep the number of walls and/or ceilings between the ECB350 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 ECB350. 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 your other electrical devices and/or appliances that generate RF noise. The most usual types are microwaves, or cordless phones.

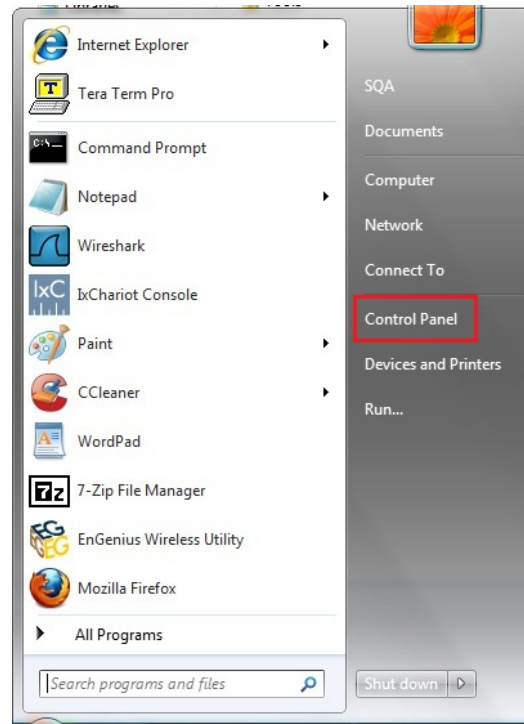
## 2.2 Computer Settings (Windows XP/Windows 7)

In order to use the ECB350, you must first configure the TCP/IPv4 connection of your computer system.

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



Windows XP

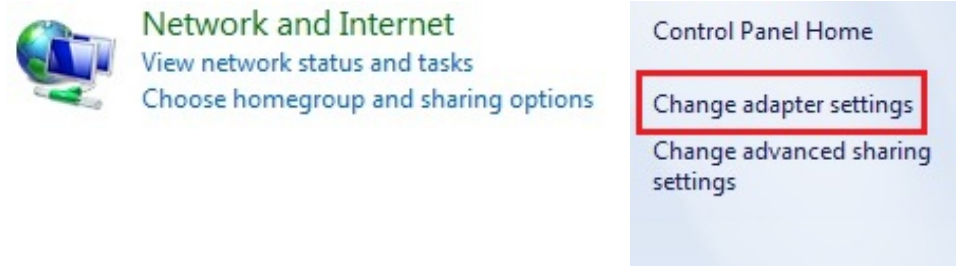


Windows 7

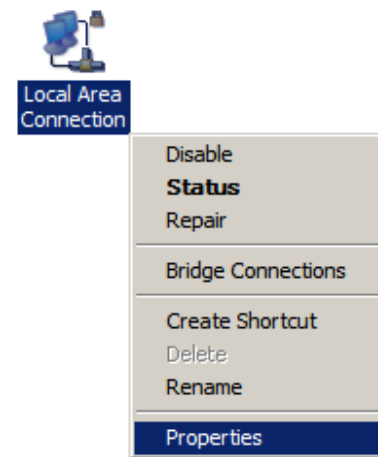
- In **Windows XP**, click **Network Connections**



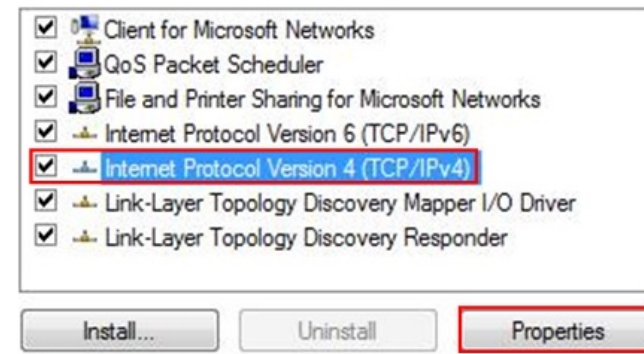
- In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet** section, then select **Change adapter settings**



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



- Select "**Internet Protocol Version 4 (TCP/IPv4)**" and then select **Properties**



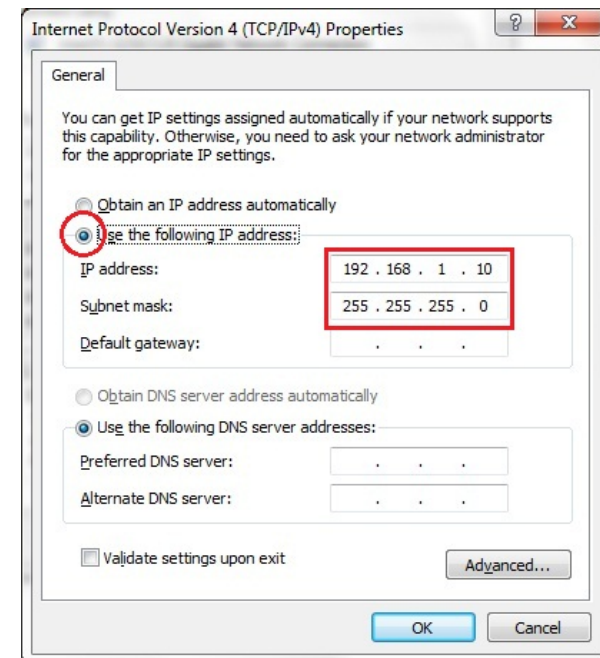
- Select **Use the following IP address** and enter an IP address that is different from the ECB350 and subnet mask then click **OK**.

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

For example: ECB350 IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

PC subnet mask: 255.255.255.0



## 2.3 Apple Mac X OS

- Go to **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 an IP address that is different from the ECB350 and subnet mask then press **OK**

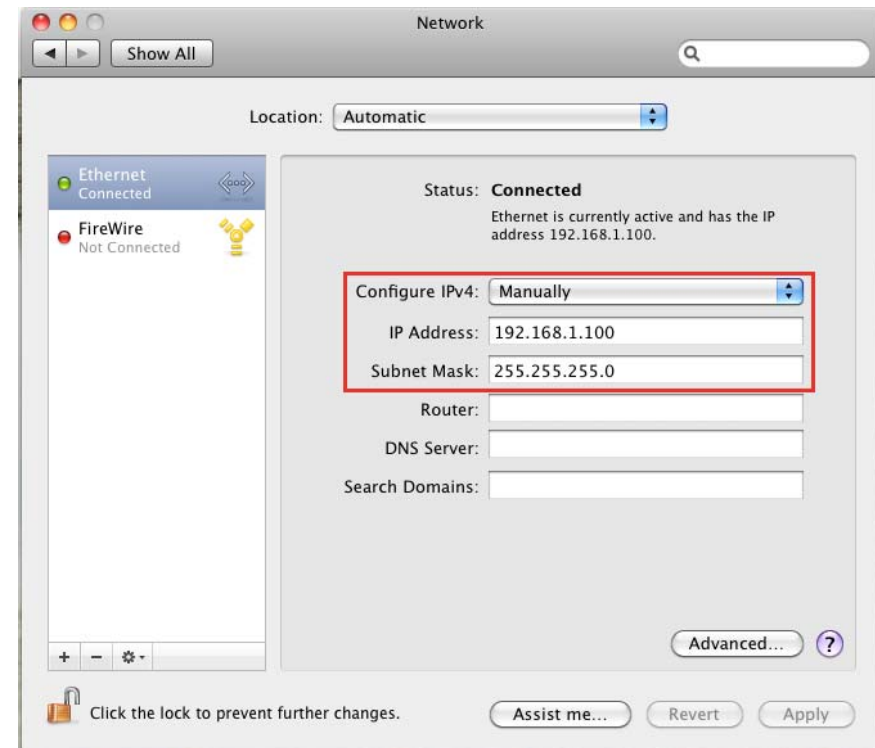
**Note:** Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: ECB350 IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

PC subnet mask: 255.255.255.0

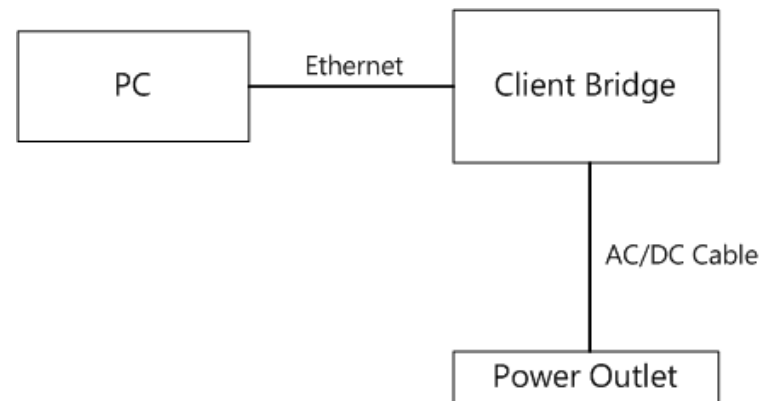
- Click **Apply** when done.

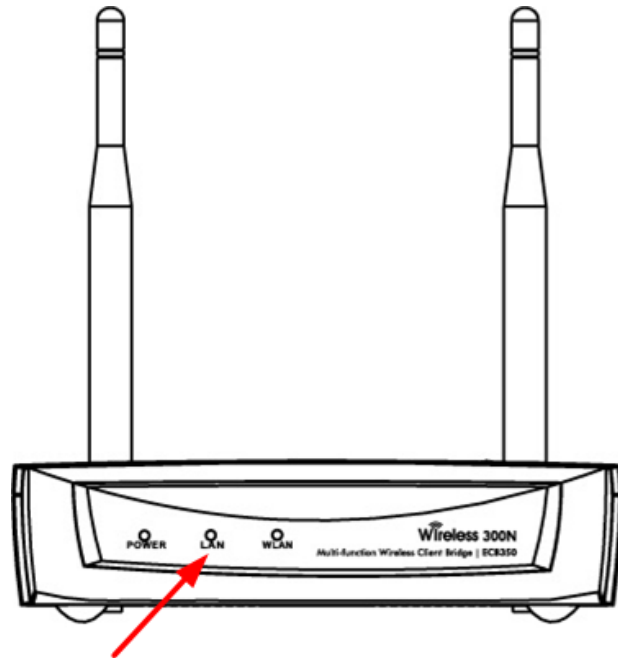


## 2.4 Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller (RJ-45 Ethernet Port). For more information, verify with your computer user manual.
2. Connect one end of the Category 5 Ethernet cable into the RJ-45 port of the ECB350 and the other end to the RJ-45 port of the computer that will use the ECB350. Ensure that the cable is securely connected to both the ECB350 and the Computer.
3. Connect the Power Adaptor DC Inlet to the DC-IN port of the ECB350 and the Power Adaptor to the electrical outlet. Once both connections are secure, verify the following:
  - a) Ensure that the **POWER** light is on (it will be green).
  - b) Ensure that the **WLAN** light is on (it will be green).
  - c) Ensure that the **LAN (Computer/ECB350 Connection)** light is on (it will be green).
  - d) Once all three lights are on, proceed to setting up the computer.

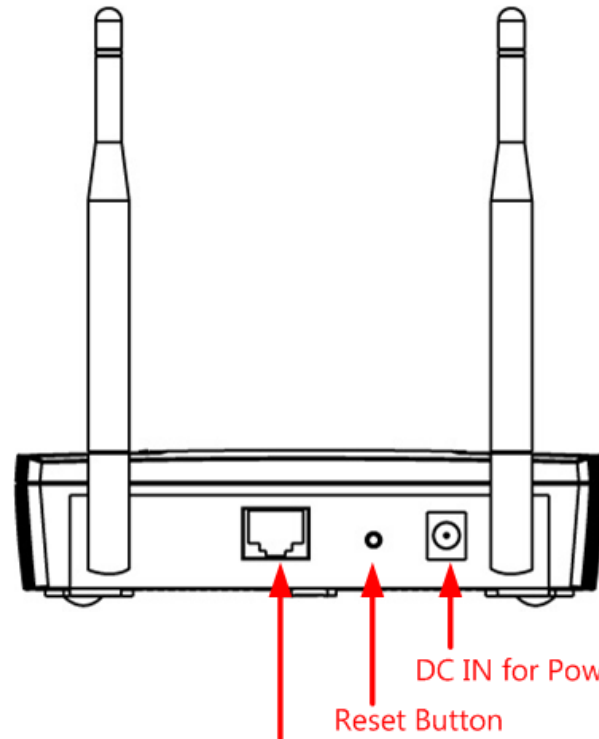
This diagram depicts the hardware configuration.





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.

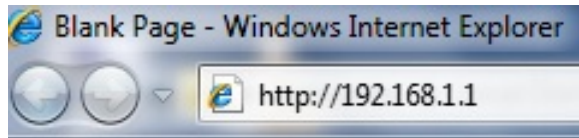
**Default Settings**

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 Access Point, 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 screenshot of the EnGenius login page. The page has a light gray background with a rounded rectangular border. At the top center, the text "EnGenius" is displayed. Below it, there are two input fields: "Username:" with the text "admin" entered, and "Password:" with five dots representing a masked password. At the bottom, there are two buttons: "Login" and "Reset".

- If successful, you will be logging in and see the ECB350 User Menu.


**Wireless Access Point/Client Bridge**

### Client Bridge

- Status**
  - Save/Reload:0
  - Main
  - Connection Status
  - System Log
- System**
  - Operation Mode
  - IP Settings
  - Spanning Tree Settings
- Wireless**
  - Wireless Network
  - Wireless Advanced Settings
- Management**
  - Administration
  - SNMP Settings
  - Backup/Restore Settings
  - Firmware Upgrade
  - Time Settings
  - Log
  - Diagnostics
  - Led Control
  - Logout

**Main**

HomeReset

**System Information**

Device Name	ECB350
Ethernet Main MAC Address	00:03:7F:BE:F0:05
Current Time	Mon Aug 15 05:25:38 UTC 2011
Firmware Version	1.0.4

**LAN Settings**

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

**Current Wireless Settings**

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g/n Mixed
Channel Bandwidth	20/40 MHz
Frequency/Channel	2.422 GHz (Channel 3)
Wireless Network Name (SSID)	AP SSID
Security	None
Spanning Tree Protocol	Disabled
Distance	1 Km

## 4 Building a Wireless Network

The ECB350 has the ability to operate in various operating modes. The ECB350 is the ideal device in which you can build your WLAN. This chapter describes how to build a WLAN around your ECB350 using the operating modes of the ECB350.

### 4.1 Client Bridge Mode

In Client Bridge Mode, the ECB350 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 ECB350 LAN port.

If you use the client bridge operating mode, use the ECB350 Site Survey feature to scan for Access Points within range. When you find an Access Point, configure the ECB350 to use the same SSID and Security Password as the Access Point to associate with it.



## 4.2 Client Router Mode

In the Client Router Mode, the ECB350 grants Internet access to multiple LANs. In this mode, the ECB350's internal Dynamic Host Configuration Protocol (DHCP) server automatically allocates ranges of IP addresses to each LAN that will access the Internet through the ECB350.

This mode requires you to connect the ECB350 wirelessly to an Access Point or Wireless Router and then connect the LANs to the ECB350 using a wired connection.



### 4.3 Access Point Mode

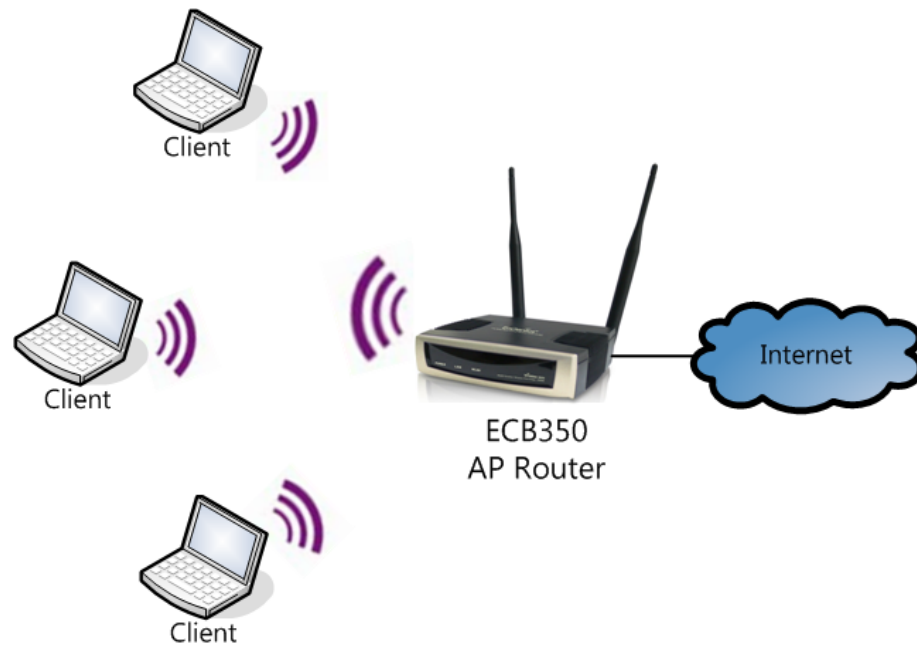
In Access Point Mode, ECB350 behaves like a central connection for stations or clients that support IEEE 802.11b/g/n networks. The stations and clients must be configured to use the same SSID and security password to associate with the ECB350. The ECB350 supports up to four SSIDs at the same time for secure guest access.



## 4.4 Access Point Router Mode

In Access Point Router Mode, ECB350 grants Internet access to multiple wireless clients. In this mode, the ECB350'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 ECB350.

This mode requires you to connect the ECB350'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 ECB350. The ECB350 supports up to four SSIDs at the same time for secure guest access.



## 4.5 WDS AP / WDS Station Mode

The ECB350 also supports WDS AP mode. This operating mode allows wireless connections to the ECB350 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.



**Note:** WDS Station Mode does not support Access Point feature.



## 4.6 WDS Bridge Mode

In WDS Bridge Mode, the ECB350 can wirelessly connect different LANs by configuring the MAC address and security settings of each ECB350 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 ECB350 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.

## 4.7 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 Status

The **Status** section contains the following options: **Main**, **Wireless Client List**, and **System Log**.

The following sections describe these options.

### 5.1 Save/Reload

This page lets you save and apply the settings shown under **Unsaved changes list**, or cancel the unsaved changes and revert them to the previous settings that were in effect.

**Save/Reload**

HomeReset

**Unsaved changes list**

```
wireless.cfg03378f.ssid=EnGenius
wireless.cfg03378f.encryption=psk2 aes
wireless.cfg03378f.key=12345678
wireless.cfg03378f.bssid=00:02:6F:10:10:14
wireless.cfg03378f.WDScompatibleMTEK=0
wireless.cfg03378f.PreferBSSIDEnable=0
wireless.wifi0.channel=1
```

Save & ApplyRevert

## 5.2 Main

Clicking the **Main** link under the **Status** menu or clicking **Home** at the top-right of the ECB350 Page shows the status information about the current operating mode.

- The **System Information** section shows general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID (**Note:** VLAN ID is only applicable in Access Point or WDS AP mode).

### System Information

Device Name	ECB350
Ethernet Main MAC Address	00:03:7F:BE:F0:05
Current Time	Mon Aug 15 04:48:57 UTC 2011
Firmware Version	1.0.4
Management VLAN ID	Untagged

- The **LAN Settings** section shows the Local Area Network settings such as the LAN IP Address, Subnet Mask, and DNS Address.

### LAN Settings

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

- The **WAN Settings** section shows WAN setting such as the MAC Address, Connection Type, Connection Status, IP Address, Subnet Mask, and DNS Address.

**Note:** WAN Settings is only in Client Router and Router mode.

#### WAN Settings

MAC Address	00:03:7F:BE:F0:05
Connection Type	Static IP
Connection Status	Down
IP Address	
IP Subnet Mask	255.255.255.0
Primary DNS	0.0.0.0
Secondary DNS	

- The **Current Wireless Settings** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the ECB350 supports multiple-SSIDs, information about each SSID, the ESSID and security settings, are displayed (**Note:** Profile Settings is only applicable in Access Point, WDS AP, or Router mode).

#### Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g/n Mixed
Channel Bandwidth	20-40 MHz
Frequency/Channel	2.437 GHz (Channel 6)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGeniusBEF005/None/1
	2 N/A
	3 N/A
	4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

## 5.3 Connection Status

Click on the **Connection Status** link under the **Status** menu. This page displays the current status of the Network, including Network Type, SSID, BSSID, Connection Status, Wireless Mode, Current Channel, Security, Data Rate, Noise Level, and Signal Strength.

**Note:** Only applicable in Client Bridge, Client Router, WDS Station, and Repeater mode.

### Connection Status

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

Network Type	Client Bridge
SSID	EnGenius
BSSID	00:02:6F:10:10:14
Connection Status	Associated
Wireless Mode	IEEE 802.11b/g/n Mixed
Current Channel	2.427 GHz(Channel 4 )
Security	WPA2-PSK AES
Tx Data Rates(Mbps)	52 Mbps
Current noise level	-95 dBm
Signal strength	-41 dBm

[Refresh](#)

## 5.4 Wireless Client List

Clicking the **Wireless Client List** link under the **Status** menu displays the list of clients associated to the ECB350, along with the MAC addresses and signal strength for each client. Clicking **Refresh** updates the client list.

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

Client List			Home	Reset
SSID:#	MAC Address	RSSI(dBm)		
SSID1:#1	00:02:6f:47:65:ca	-40		
SSID1:#2	00:02:6f:4d:f2:1e	-36		
SSID1:#3	00:02:6f:11:ac:93	-38		
			Refresh	

## 5.5 System Log

The ECB350 automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **System Log** link under the **Status** menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

**System Log**

Home
Reset

---

Show log type

All

```

Aug 15 04:55:03 ECB350 user.notice root: starting ntpclient
Aug 15 04:55:01 ECB350 cron.err crond[1059]: USER root pid 2191 cmd . /etc/hotplug.d/iface/20-ntpcli
Aug 15 04:50:03 ECB350 user.notice root: starting ntpclient
Aug 15 04:50:01 ECB350 cron.err crond[1059]: USER root pid 1928 cmd . /etc/hotplug.d/iface/20-ntpcli
Aug 15 04:45:40 ECB350 user.notice root: starting ntpclient
Aug 15 04:45:32 ECB350 daemon.crit dnsmasq[1177]: bad command line options: inconsistent DHCP range
Aug 15 04:45:32 ECB350 daemon.crit dnsmasq[1177]: FAILED to start up
Aug 15 04:45:27 ECB350 cron.err crond[1059]: crond (busybox 1.15.3) started, log level 5
Aug 15 04:45:26 ECB350 user.warn kernel: osif_vap_init : wait for connection SM start failed
Aug 15 04:45:26 ECB350 user.info kernel: device ath0 entered promiscuous mode
Aug 15 04:45:26 ECB350 user.info kernel: br-lan: topology change detected, propagating
Aug 15 04:45:26 ECB350 user.info kernel: br-lan: port 2(ath0) entering learning state
Aug 15 04:45:26 ECB350 user.info kernel: br-lan: port 2(ath0) entering forwarding state
Aug 15 04:45:23 ECB350 user.warn kernel: start running
Aug 15 04:45:22 ECB350 user.warn kernel: set SIOC80211NWID, 8 characters
Aug 15 04:45:22 ECB350 user.warn kernel: ieee80211_ioctl_setparam parameter 0x35 is not supported
Aug 15 04:45:22 ECB350 user.warn kernel: ieee80211_ioctl_setparam parameter 0x21 is not supported
Aug 15 04:45:21 ECB350 user.notice root: ATH-LSDK:loaddriver
Aug 15 04:45:21 ECB350 user.err kernel: VAP device ath0 created
Aug 15 04:45:20 ECB350 user.warn kernel: ath_get_caps[3741] rx chainmask mismatch actual 3 sc_chainm
Aug 15 04:45:20 ECB350 user.warn kernel: ath_get_caps[3716] tx chainmask mismatch actual 3 sc_chainm
Aug 15 04:45:20 ECB350 user.info kernel: wifi0: Atheros 9280: mem=0x10000000, irq=48 hw_base=0xb0000

```

Refresh
Clear

System Log	
<b>Refresh</b>	Update the log.
<b>Clear</b>	Clear the log.



## 6 System

### 6.1 Operation Mode

The ECB350 supports 8 operating modes: Access Point, Client Bridge, WDS AP, WDS Bridge, WDS Station, Universal Repeater, Router, and Client Router.

#### System Properties

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

##### System Properties

Device Name	ECB350 ( 1 to 32 characters )
Country/Region	Please Select a Country Code ▼
Operation Mode	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input checked="" type="radio"/> WDS <ul style="list-style-type: none"> <li><input checked="" type="radio"/> Access Point</li> <li><input type="radio"/> Bridge</li> <li><input type="radio"/> Station</li> <li><input type="radio"/> Access Point Router</li> <li><input type="radio"/> Client Router</li> <li><input type="radio"/> Repeater</li> </ul>

[Save & Apply](#)
[Cancel](#)

#### System Properties

<b>Device Name</b>	Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.
<b>Country/Region</b>	Select a Country/Region to conform to local regulations.
<b>Operation Mode</b>	Use the radio button to select an operating mode.
<b>Save &amp; Apply / Cancel</b>	Click <b>Save &amp; Apply</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 6.2 IP Settings

This page allows you to modify the device's IP settings.

**Note:** Only applicable in Access Point, Client Bridge, WDS AP, WDS Bridge, WDS Station, and Repeater mode.

### IP Settings

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

#### System Information

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

[Accept](#)
[Cancel](#)

IP Settings	
<b>IP Network Setting</b>	Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.
<b>IP Address</b>	The IP Address of this device.
<b>IP Subnet Mask</b>	The IP Subnet Mask of this device.
<b>Default Gateway</b>	The Default Gateway of this device. Leave it blank if you are unsure of this setting.
<b>Primary / Secondary DNS</b>	The primary / secondary DNS address for this device.

## 6.3 Spanning Tree Setting

This page allows you to modify the Spanning Tree settings. Enabling Spanning Tree protocol will prevent network loops in your LAN network.

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

### Spanning Tree Settings

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

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

[Accept](#)
[Cancel](#)

Spanning Tree	
<b>Spanning Tree Status</b>	Enable or disable the Spanning Tree function.
<b>Bridge Hello Time</b>	Specify Bridge Hello Time, in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.
<b>Bridge Max Age</b>	Specify Bridge Max Age, in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be dead.
<b>Bridge Forward Delay</b>	Specify Bridge Forward Delay, in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided

	so that when a new bridge comes onto a busy network, it analyzes data traffic before participating.
<b>Priority</b>	Specify the Priority Number. A smaller number has greater priority.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7 Router

This section is only applicable for **AP Router Mode** or **Client Router Mode**.

### 7.1 WAN Settings

There are four types of WAN connections: Static IP, DHCP, PPPoE, and PPTP. Please contact your ISP to find out which settings you should choose.

#### 7.1.1 Static IP

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.

## WAN Settings

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

Internet Connection Type

Static IP ▾

### Options

Account Name (if required)

Domain Name (if required)

MTU

Auto ▾ 1500 ( 576 - 1500 )

### Internet IP Address

IP Address

 .  .  . 

IP Subnet Mask

 .  .  . 

Gateway IP Address

 .  .  . 

### Domain Name Server (DNS) Address

Primary DNS

 .  .  . 

Secondary DNS

 .  .  . 

### WAN Ping

Discard Ping on WAN

☒[Accept](#)[Cancel](#)

Static IP	
<b>Internet Connection Type</b>	Select Static IP to begin configuration of the Static IP connection.
<b>Account Name</b>	Enter the account name provided by your ISP.
<b>Domain Name</b>	Enter the domain name provided by your ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit (MTU) size. It is recommended that you accept the default setting of <b>Auto</b> . Otherwise, packets will be fragmented downstream if the MTU is set too high or too low, which impacts network performance. In extreme cases, an MTU setting that is too low can prevent the ECB350 from establishing some connections.
<b>IP Address</b>	Assign an IP address Manually.
<b>IP Subnet Mask</b>	Specify an IP address's subnet mask.
<b>Gateway IP Address</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.
<b>Discard Ping on WAN</b>	Check to Enable to recognize pings on the ECB350 WAN interface or Disable to block pings on the ECB350 WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

**Note:** Clicking **Accept** does not apply the changes. To apply them, use **Status > Save/Load** (see section 4.1).

## 7.1.2 DHCP

Select DHCP as your WAN connection type to obtain an IP address automatically. You will need to enter the account name as your hostname and, optionally, enter DNS information.

### WAN Settings

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

Internet Connection Type

DHCP ▾

#### Options

Account Name (if required)

Domain Name (if required)

MTU

Auto ▾

1500

( 576 - 1500 )

#### Domain Name Server (DNS) Address

☒ Get Automatically From ISP

☐ Use These DNS Servers

Primary DNS

0 . 0 . 0 . 0

Secondary DNS

0 . 0 . 0 . 0

#### WAN Ping

Discard Ping on WAN

☒

[Accept](#)

[Cancel](#)



DHCP	
<b>Internet Connection Type</b>	Select <b>DHCP</b> to begin configuration of the DHCP connection.
<b>Account Name</b>	Enter the account name provided by your ISP.
<b>Domain Name</b>	Enter the domain name provided by your ISP.
<b>MTU</b>	Specify the Maximum Transmit Unit (MTU) size. It is recommended that you accept the default setting of <b>Auto</b> . Otherwise, packets will be fragmented downstream if the MTU is set too high or too low, which impacts network performance. In extreme cases, an MTU setting that is too low can prevent the ECB350 from establishing some connections.
<b>Get Automatically From ISP</b>	Click this radio button to obtain the DNS automatically from the DHCP server.
<b>Use These DNS Servers</b>	Click the radio button to set up the Primary DNS and Secondary DNS servers manually.
<b>Discard Ping on WAN</b>	Check to Enable to recognize pings on the ECB350 WAN interface or Disable to block pings on the ECB350 WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides extra security from hackers.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

### 7.1.3 PPPoE

Select Point-to-Point Protocol over Ethernet (PPPoE) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This selection is typically used for DSL services. Remove your PPPoE software from your computer, as it is not needed and will not work with your ECB350.

WAN Settings		Home	Reset
Internet Connection Type	PPPoE ▼		
Options			
MTU	Auto ▼ 1492 ( 576 - 1492 )		
PPPoE Options			
Login	<input type="text"/>		
Password	<input type="password"/>		
Service Name (if required)	<input type="text"/>		
<input type="radio"/> Connect on Demand: Max idle Time 1 <input type="text"/> Minutes <input checked="" type="radio"/> Keep Alive: Redial Period 30 <input type="text"/> Seconds			
Domain Name Server (DNS) Address			
<input checked="" type="radio"/> Get Automatically From ISP <input type="radio"/> Use These DNS Servers			
Primary DNS	0 <input type="text"/> . 0 <input type="text"/> . 0 <input type="text"/> . 0 <input type="text"/>		
Secondary DNS	0 <input type="text"/> . 0 <input type="text"/> . 0 <input type="text"/> . 0 <input type="text"/>		
WAN Ping			
Discard Ping on WAN	<input checked="" type="checkbox"/>		
<input type="button" value="Accept"/> <input type="button" value="Cancel"/>			

<b>PPPoE</b>	
<b>Internet Connection Type</b>	Select <b>PPPoE</b> to begin configuration of the PPPoE connection.
<b>MTU</b>	Specify the Maximum Transmit Unit (MTU) size. It is recommended you accept the default setting of <b>Auto</b> . Otherwise, packets will be fragmented downstream if the MTU is set too high or too low, which impacts network performance. In extreme cases, an MTU setting that is too low can prevent the ECB350 from establishing some connections.
<b>Login</b>	Enter the Username provided by your ISP.
<b>Password</b>	Enter the Password provided by your ISP.
<b>Service Name</b>	Enter the Service Name provided by your ISP.
<b>Connect on Demand</b>	Select the radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
<b>Keep Alive</b>	Select whether to keep the Internet connection always on, or enter a redial period once the internet lose connection.
<b>Get Automatically From ISP</b>	Click this radio button to obtain the DNS automatically from the DHCP server.
<b>Use These DNS Servers</b>	Click the radio button to set up the Primary DNS and Secondary DNS servers manually.
<b>Discard Ping on WAN</b>	Check to Enable to recognize pings on the ECB350 WAN interface or Disable to block pings on the ECB350 WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.1.4 PPTP

Select PPTP as your WAN connection type if your Internet Service Provider (ISP) uses a Point-to-Point Tunneling Protocol (PPTP) connection. You will need to provide the IP address, Subnet Mask, Default Gateway (Optional), DNS (Optional), Server IP, Username, and Password provided by your ISP.

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

---

**WAN Settings**

Internet Connection Type: PPTP

Options

MTU: Auto 1400 ( 1200 - 1400 )

PPTP Options

IP Address	192	.	168	.	10	.	1
Subnet Mask	255	.	255	.	255	.	0
Default Gateway	0	.	0	.	0	.	0
PPTP Server	0	.	0	.	0	.	0
Username							
Password							

☐ Connect on Demand: Max idle Time 15 Minutes  
☒ Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

☒ Get Automatically From ISP  
☐ Use These DNS Servers

Primary DNS	0	.	0	.	0	.	0
Secondary DNS	0	.	0	.	0	.	0

WAN Ping

Discard Ping on WAN ☒

[Accept](#)
[Cancel](#)

<b>PPTP</b>	
<b>Internet Connection Type</b>	Select <b>PPTP</b> to begin configuration of the PPTP connection.
<b>MTU</b>	Specify the Maximum Transmit Unit (MTU) size. It is recommended that you accept the default setting of <b>Auto</b> . Otherwise, packets will be fragmented downstream if the MTU is set too high or too low, which impacts network performance. In extreme cases, an MTU setting that is too low can prevent the ECB350 from establishing some connections.
<b>IP Address</b>	Enter the WAN port IP address.
<b>Subnet Mask</b>	Enter the WAN IP subnet mask.
<b>Default Gateway</b>	Enter the WAN gateway IP address.
<b>PPTP Server</b>	Enter the IP address of the PPTP server.
<b>Username</b>	Enter the Username provided by your ISP.
<b>Password</b>	Enter the Password provided by your ISP.
<b>Service Name</b>	Enter the Service Name provided by your ISP.
<b>Connect on Demand</b>	Select the radio button to specify the maximum idle time. Internet connection will disconnect when it reach the maximum idle time, but it will automatically connect when user tries to access the network.
<b>Keep Alive</b>	Select whether to keep the Internet connection always on, or enter a redial period once the internet loses connection.
<b>Get Automatically From ISP</b>	Click this radio button to obtain the DNS automatically from the DHCP server.
<b>Use These DNS Servers</b>	Click the radio button to set up the Primary DNS and Secondary DNS servers manually.
<b>Discard Ping on WAN</b>	Check to Enable to recognize pings on the ECB350 WAN interface or Disable to block pings on the ECB350 WAN interface. Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.2 LAN Settings

This page allows you to modify the device's LAN settings.

### LAN Settings

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

#### LAN IP Setup

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

☒ Use Router As DHCP Server

Starting IP Address	192	.	168	.	1	.	100
Ending IP Address	192	.	168	.	1	.	200
WINS Server IP	0	.	0	.	0	.	0



LAN Settings	
<b>IP Address</b>	The LAN IP Address of this device.
<b>IP Subnet Mask</b>	The LAN Subnet Mask of this device.
<b>Use Router As DHCP Server</b>	Check this option to enable the Internal DHCP server.
<b>Starting /Ending IP Address</b>	The range of IP addresses of the DHCP server will allocate to LAN device.
<b>WINS Server IP</b>	Enter the IP address of the WINS server.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.3 VPN Pass Through

The VPN Passthrough allows a secure virtual private network (VPN) connection between two computers. Enabling the options on this page opens a VPN port and enables connections to pass through the ECB350 without interruption.

### VPN Pass Through

[Home](#)[Reset](#)☒ PPTP Pass Through☒ L2TP Pass Through☒ IPSec Pass Through[Accept](#)[Cancel](#)

## 7.4 Port Forwarding

Port forwarding can be used to open a port or range of ports to a device on your network. Using port forwarding, you can set up public services on your network. When users from the Internet make certain requests on your network, the ECB350 can forward those requests to computers equipped to handle the requests. For example, if you set the port number 80 (HTTP) to be forwarded to IP address 192.168.1.150, all HTTP requests from outside users are forwarded to 192.168.1.150.

Home Reset

---

**Port Forwarding**
Enable ▾

Service Name

Protocol
Both ▾

Starting Port

(1~65535)

Ending Port

(1~65535)

IP Address

Add Cancel

**Port Forwarding Table**

#	Name	Protocol	Start Port	End Port	Server IP Address	Select
1	rule01	both	20	21	192.168.1.100	<input type="checkbox"/>

Delete Selected Delete All Reset

Accept Cancel



Port Forwarding	
<b>Port Forwarding</b>	Enables or disables the Port Forwarding feature.
<b>Service Name</b>	Enter a name or description to help you identify this entry.
<b>Protocol</b>	Select a protocol for the application. Choices are <b>Both</b> , <b>TCP</b> , and <b>UDP</b> .
<b>Start / End Port</b>	The port range that the server is running on the local computer.
<b>IP Address</b>	The local IP address of the computer the server is hosted on.
<b>Add / Cancel</b>	Click <b>Add</b> to add port forwarding rule or <b>Cancel</b> to discard the settings
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.5 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 device's firewall. Port Triggering will be required for these applications to work.

### Port Triggering

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

Port Trigger	Enable ▾
Service Name	rule02
Trigger Port	2000 ~ 2020 (1~65535)
Trigger Type	Both ▾
Forwarded Port	2000 (1~65535)
Public Type	Both ▾
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

Port Trigger Table

#	Trigger Port	Trigger Type	Forwarded Port	Public Type	Name	Select
1	1000 ~ 1010	both	1000-1010	both	rule01	<input type="checkbox"/>
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>						

Port Triggering	
<b>Port Triggering</b>	Enables or disables the Port Triggering feature.
<b>Service Name</b>	Enter a name or description to help you identify this entry.
<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.
<b>Add / Cancel</b>	Click <b>Add</b> to add port forwarding rule or <b>Cancel</b> to discard the settings
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.6 DMZ

If you have a computer that cannot run Internet applications properly from behind the ECB350, you can allow the computer to have unrestricted Internet access. Enter the IP address of that computer as a Demilitarized Zone (DMZ) host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks, so use this option as a last resort.

Home
Reset

---

DMZ Hosting	Disable ▾
DMZ Address	<input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/> <input style="width: 40px;" type="text" value="0"/>

Accept
Cancel

DMZ	
<b>DMZ Hosting</b>	Enables or disables the DMZ function.
<b>DMZ Address</b>	Enter an IP Address of the computer that will have unlimited Internet access.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 7.7 MAC Filter

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

**MAC Filter**
Home
Reset

---

MAC Filter
Enable ▾

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

Service Name
rule02

LAN MAC Address
00 : 02 : 6F : 83 : 93 : DA

Add
Cancel

MAC Filter Table

#	Name	MAC Address	Select
1	rule01	00:02:6F:11:99:EE	<input type="checkbox"/>

Delete Selected
Delete All
Reset

Accept
Cancel

MAC Filter	
<b>MAC Filter</b>	Enables or disables the MAC Filter function.
<b>Deny all clients with MAC addresses listed below to access the network</b>	When selected, the computers listed in the MAC Filter Table will be <b>Denied</b> to access 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 Filter table will be <b>Allowed</b> to access the Internet.

## 7.8 IP Filter

You can choose whether to Deny or Allow only devices with those IP Addresses listed on the IP Filter Table from accessing certain ports. This can be used to control which Internet applications the computers can access.

**Note:** You will need to have knowledge of which Internet port numbers each application uses.

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

---

IP Filter

Enable ▾

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

Service Name

rule02

Protocol

Both ▾

Local IP Address

192.168.1.200 ~

Port Range

80 ~ (1~65535)

Add

Cancel

IP Filter Table

#	Name	Local IP Address	Protocol	Port Range	Select
1	rule01	192.168.1.150 - 192.168.1.151	both	20 - 21	<input type="checkbox"/>

Delete Selected

Delete All

Reset

IP Filter	
IP Filter	Enables or disables the IP Filter function.
Deny all clients with IP addresses listed below to access the network	When selected, the computers listed in the IP Filter table will be <b>Denied</b> to access the Internet.
Allow all clients with IP addresses listed below to access the network	When selected, only the computers listed in the IP Filter table will be <b>Allowed</b> to access the Internet.

## 7.9 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 Filter Table. Any web address that includes "gamer" will be blocked.

**URL Filter**

HomeReset

URL Filter

Enable ▾

Website / Keyword

test123

Add

Cancel

**URL Filter Table**

#	Website / Keyword	Select
1	gamer	<input type="checkbox"/>

Delete Selected

Delete All

Reset



## 8 Wireless

### 8.1 Wireless Network

This page displays the current status of the Wireless settings of the ECB350.

**Access Point / WDS AP / Router mode:**

#### Wireless Network

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

Wireless Mode	802.11 B/G/N Mixed ▾
Channel HT Mode	20/40MHz ▾
Extension Channel	Lower Channel ▾
Channel / Frequency	Ch5-2.432GHz ▾ <input checked="" type="checkbox"/> Auto
AP Detection	<a href="#">Scan</a>

#### Current Profiles

SSID	Security	VID	Enable	Edit
EnGeniusBEEF06	None	1	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
EnGeniusBEEF06_2	None	2	<input type="checkbox"/>	<a href="#">Edit</a>
EnGeniusBEEF06_3	None	3	<input type="checkbox"/>	<a href="#">Edit</a>
EnGeniusBEEF06_4	None	4	<input type="checkbox"/>	<a href="#">Edit</a>

Profile (SSID) Isolation	<input checked="" type="radio"/> No Isolation <input type="radio"/> Isolate all Profiles (SSIDs) from each other using VLAN (802.1Q) standard <b>CAUTION:</b> No Management VLAN ID Packet only allow on Primary Ethernet Port.
--------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[Accept](#)
[Cancel](#)

<b>Wireless Network (Access Point / WDS AP / Router mode)</b>	
<b>Wireless Mode</b>	Wireless mode supports 802.11b/g/n mixed mode.
<b>Channel HT Mode</b>	The default channel bandwidth is 20/40MHz. The larger the channel, the better the transmission quality and speed.
<b>Extension Channel</b>	Select upper or lower channel. Your selection may affect the Auto channel function.
<b>Channel / Frequency</b>	Select the channel and frequency appropriate for your country's regulation.
<b>Auto</b>	Check this option to enable auto-channel selection.
<b>AP Detection</b>	AP Detection can select the best channel to use by scanning nearby areas for Access Points.
<b>Current Profile</b>	Configure up to four different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click <b>Edit</b> to configure the profile and check whether you want to enable extra SSID.
<b>Profile Isolation</b>	Restricted client to communicate with different VID by selecting the radio button.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## SSID Profile

### SSID Profile

#### Wireless Setting

SSID	EnGeniusBEEF06	(1 to 32 characters)
VLAN ID	1	(1~4094)
Suppressed SSID	<input type="checkbox"/>	
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

#### Wireless Security

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



SSID Profile	
<b>SSID</b>	Specify the SSID for the current profile.
<b>VLAN ID</b>	Specify the VLAN tag for the current profile.
<b>Suppressed SSID</b>	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
<b>Station Separation</b>	Click the appropriate radio button to allow or prevent communication between client devices.
<b>Wireless Security</b>	See the Wireless Security section.
<b>Save / Cancel</b>	Click <b>Save</b> to accept the changes or <b>Cancel</b> to cancel and return previous settings.

## Client Bridge / Client Router / WDS Station / Repeater mode:

### Wireless Network

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

Wireless Mode	802.11 B/G/N Mixed ▼
SSID	Specify the static SSID : AP SSID <input type="text"/> ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Preferred BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

### Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

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



<b>Wireless Mode</b>	Wireless mode supports 802.11b/g/n mixed mode.
<b>SSID</b>	The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the <b>Site Survey</b> .
<b>Site Survey</b>	Click on <b>Site Survey</b> to search the existing Access Points.
<b>Preferred BSSID</b>	Specify the BSSID (Access Point's MAC Address).
<b>Wireless Security</b>	The encryption is using. It must the same as Access Point's encryption.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 8.2 Wireless Security

The Wireless Security section lets you configure the ECB350's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you use WPA2-PSK.

### WEP Encryption:

#### Wireless Security

Security Mode	WEP ▾
Auth Type	Open System ▾
Input Type	Hex ▾
Key Length	40/64-bit (10 hex digits or 5 ASCII char) ▾

Default Key	1 ▾
Key1	1234567890
Key2	
Key3	
Key4	

WEP Encryption	
Auth Type	Select <b>Open System</b> or <b>Shared Key</b> .
Input type	<b>ASCII:</b> Regular Text (recommended) <b>HEX:</b> Hexadecimal Numbers (For advanced users)
Key Length	Select the desired option and ensure the wireless clients use the same setting. Choices are 64, 128, 152-bit password lengths.
Default Key	Select the key you wish to be 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-PSK (WPA Pre-Shared Key) Encryption:

#### Wireless Security

Security Mode	WPA-PSK Mixed ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

WPA-PSK (WPA Pre-Shared Key) Encryption	
<b>Encryption</b>	Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.
<b>Passphrase</b>	Wireless clients must use the same key to associate the device. If using passphrase format, the Key must be from 8 to 63 characters in length.
<b>Group Key Update Interval</b>	Specify how often, in seconds, the group key changes.

### WPA Encryption: Only in Access Point / WDS AP / Router mode

#### Wireless Security

Security Mode	WPA Mixed ▾
Encryption	Both(TKIP+AES) ▾
Radius Server	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Radius Port	1812 <input type="text"/>
Radius Secret	<input type="text"/>
Group Key Update Interval	3600 <input type="text"/> seconds(30~3600, 0: disabled)

WPA Encryption	
<b>Encryption</b>	Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.
<b>Radius Server</b>	Enter the IP address of the Radius Server.
<b>Radius Port</b>	Enter the port number used for connections to the Radius server.
<b>Radius Secret</b>	Enter the secret required to connect to the Radius server.
<b>Group Key Update Interval</b>	Specify how often, in seconds, the group key changes.

**Note:** 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

## 8.3 Site Survey

Use this feature to scan nearby Access Points.

**Note:** Only applicable in Client Bridge, Client Router, or Repeater modes.

1. Click **Site Survey**.

Wireless Network		Home	Reset
Wireless Mode	802.11 B/G/N Mixed ▼		
SSID	<div>Specify the static SSID : AP SSID <input type="text"/> ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <div>Site Survey</div></div>		
Preferred BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>		
Wireless Security			
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.			
Security Mode	Disabled ▼		
<div>Accept</div> <div>Cancel</div>			



## 2. Scanning the nearby Access Points

## Scanning













Please wait...

## 3. The ECB350 will list the available access points after site survey.

### Site Survey

#### 2GHz Site Survey

:Infrastructure :Ad\_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:02:6F:B9:3A:30	SQA-ADSL	1	-66 dBm	11g/n	WPA2-PSK	
00:0C:F6:54:A9:79		6	-72 dBm	11g/n	WPA2-PSK	
00:02:6F:9C:3D:84	EnGenius9C3D84	11	-85 dBm	11b/g	WPA-PSK	
00:03:7F:BE:F2:25	ADDA_TEST	11	-84 dBm	11g/n	WPA/WPA2-PSK	
00:03:7F:BE:F0:C0	EAP350- antennatesting	11	-52 dBm	11g/n	WPA2-PSK	
00:02:6F:10:10:14	EnGenius	4	-38 dBm	11g/n	WPA2-PSK	
00:02:6F:51:F9:38	EnGenius51F938	11	-79 dBm	11g/n	none	
00:02:6F:B3:4F:38	SENAOWL	1	-83 dBm	11g/n	WEP	
00:02:6F:6D:0B:EF	yenger	4	-83 dBm	11b/g	WEP	
06:03:7F:BE:F1:1D	EnGenius2	6	-89 dBm	11g/n	none	
00:1B:11:62:71:C3	dlink	2	-90 dBm	11g/n	none	
00:40:05:C7:49:4C	default	6	-90 dBm	11b	none	















Refresh

Site Survey (Client Bridge / Client Router / Repeater mode)	
<b>BSSID</b>	Access Point's wireless MAC address.
<b>SSID</b>	SSID that the Access Point is broadcasting.
<b>Channel</b>	Channel that the Access Point is using.
<b>Signal Level (dBm)</b>	Signal strength from the Access Point to your station.
<b>Type</b>	The band that the Access Point is using.
<b>Security</b>	Encryption method that the Access Point is using to secure data over the WLAN.
<b>Refresh</b>	Click <b>Refresh</b> to rescan nearby Access Point.

4. Select an Access Point and click that Access Point's BSSID.

#### Site Survey

##### 2GHz Site Survey

						 :Infrastructure  :Ad_hoc
BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:02:6F:B9:3A:30	SQA-ADSL	1	-66 dBm	11g/n	WPA2-PSK	
00:0C:F6:54:A9:79		6	-72 dBm	11g/n	WPA2-PSK	
00:02:6F:9C:3D:84	EnGenius9C3D84	11	-85 dBm	11b/g	WPA-PSK	
00:03:7F:BE:F2:25	ADDA_TEST	11	-84 dBm	11g/n	WPA/WPA2-PSK	
00:03:7F:BE:F0:C0	EAP350- antennatesting	11	-52 dBm	11g/n	WPA2-PSK	
00:02:6F:10:10:14	EnGenius	4	-38 dBm	11g/n	WPA2-PSK	
00:02:6F:51:F9:38	EnGenius51F938	11	-79 dBm	11g/n	none	
00:02:6F:B3:4F:38	SENAOWL	1	-83 dBm	11g/n	WEP	
00:02:6F:6D:0B:EF	yenger	4	-83 dBm	11b/g	WEP	
06:03:7F:BE:F1:1D	EnGenius2	6	-89 dBm	11g/n	none	
00:1B:11:62:71:C3	dlink	2	-90 dBm	11g/n	none	
00:40:05:C7:49:4C	default	6	-90 dBm	11b	none	

Refresh

5. Enter the correct security setting.

## Wireless Network

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

Wireless Mode	802.11 B/G/N Mixed ▾
SSID	<p>Specify the static SSID : EnGenius ( 1 to 32 characters ) Or press the button to search for any available WLAN Service.</p> <p>Site Survey</p>
Preferred BSSID	<input type="checkbox"/> 00 : 02 : 6F : 10 : 10 : 14

## Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK ▾
Encryption	AES ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)

[Accept](#)[Cancel](#)

## 8.4 Wireless MAC Filter

Wireless MAC Filters are used to allow or deny network access to wireless clients according to their MAC addresses. You can manually add a MAC address to restrict the permission to access ECB350. The default setting is **Disable Wireless MAC Filter**.

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

**Wireless MAC Filter**
Home
Reset

---

ACL Mode Disabled

00 : 02 : 6f : 00 : 35 : 01

Add

#	MAC Address	
1	00:02:6F:00:35:04	<span>Delete</span>

Accept

Wireless Filter (Access Point / WDS AP / Router mode)	
<b>ACL Mode</b>	Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. Choices are: <b>Disabled</b> , <b>Deny MAC in the list</b> , or <b>Allow MAC in the list</b> .
<b>MAC Address</b>	Enter the MAC address of the wireless client.
<b>Add</b>	Click <b>Add</b> to add the MAC address to the <b>MAC Address</b> table.
<b>Delete</b>	Delete the selected entries.
<b>Apply</b>	Click Apply to apply the changes.

## 8.5 Wireless Advanced

This page allows you to configure wireless advance settings. It is recommended that the default settings are used unless the user has experience with more advanced networking features.

### Wireless Advanced Settings

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

Data Rate	Auto ▾
Transmit Power	17 dBm ▾
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	1 km
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)

### Wireless Traffic Shaping

Enable Traffic Shaping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Incoming Traffic Limit	1000 kbit/s
Outgoing Traffic Limit	2000 kbit/s

[Accept](#)[Cancel](#)

<b>Wireless Advanced</b>	
<b>Data Rate</b>	Select a data rate from the drop-down list. The data rate affects throughput of data in the ECB350. The lower the data rate, the throughput will be lower, but so will the transmission distance.
<b>Transmit Power</b>	Set the power output of the wireless signal.
<b>RTS/CTS Threshold</b>	Specify the threshold package size for RTC/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth.
<b>Distance</b>	Specify the distance between Access Points and clients. Longer distances may drop high-speed connections.
<b>Aggregation</b>	Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes.
<b>Wireless Traffic Shaping</b>	Check this option to enable wireless traffic shaping. Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.
<b>Incoming Traffic Limit</b>	Specify the wireless transmission speed used for downloading.
<b>Outgoing Traffic Limit</b>	Specify the wireless transmission speed used for uploading.
<b>Accept / Cancel</b>	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 8.6 WPS (Wi-Fi Protected Setup)

Wi-Fi Protected Setup (WPS) feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

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 applicable in Access Point, WDS AP, and Router mode.

### WPS Setting

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

#### WPS

WPS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
WPS current status	Configured	<a href="#">Release Configuration</a>
Self Pin Code	45998621	
SSID	EnGeniusBEEF06	
Authentication Mode	WPA-PSK Mixed TKIP/AES	
Passphrase Key	12345678	
WPS Via Push Button	<a href="#">Start to Process</a>	
WPS Via Pin	<input type="text"/>	<a href="#">Start to Process</a>

[Accept](#)
[Cancel](#)

<b>Wi-Fi Protected Setup (WPS)</b>	
<b>WPS</b>	Select to Enable or Disable the WPS feature.
<b>WPS Current Status</b>	Shows whether the WPS function is <b>Configured</b> or <b>unConfigured</b> .  When it is Configured, the WPS has been used to authorize connection between the device and wireless clients.
<b>Self Pin Code</b>	The PIN code of this device.
<b>SSID</b>	The SSID (wireless network name) used when connecting using WPS.
<b>Authentication Mode</b>	Shows the encryption method used by the WPS process.
<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>	Click this button to initialize WPS feature using the push button method.
<b>WPS via PIN</b>	Enter the PIN code of the wireless device and click this button to initialize WPS feature using the PIN method.



## 8.7 WDS Link Settings

Using WDS (Wireless Distribution System) will allow you to connect to Access Points wirelessly. Doing so will extend the 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 the WDS network be created using the same models for maximum compatibility.

Also note: All Access Points in the WDS network needs 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.*

**Note:** Only applicable in WDS AP and WDS Bridge mode.

### WDS Link Settings

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

**Caution:** NAWDS was enabled, you need assign Wifi Channel manually later.

ID	MAC Address	Mode
1	00 : 02 : 6F : 11 : 22 : 33	Enable ▼
2	:  :  :  :  :	Disable ▼
3	:  :  :  :  :	Disable ▼
4	:  :  :  :  :	Disable ▼

[Accept](#)
[Cancel](#)

WDS Link Settings	
MAC Address	Enter the Access Point's MAC address to which you want to extend the wireless area.
Mode	Select <b>Disable</b> or <b>Enable</b> from the drop-down list.
Accept / Cancel	Click <b>Accept</b> to confirm the changes or <b>Cancel</b> to cancel and return previous settings.

## 9 Management

### 9.1 Administration

This page allows you to change the ECB350 password as well as configure the device by remote access. By default, the username is **admin** and the password is: **admin**. The password can contain 0 to 12 alphanumeric characters and is case sensitive.

**Note:** Remote Access is only applicable in AP Router and Client Router mode.

#### Login Setting

New Name	admin
New Password	
Confirm Password	
<input type="button" value="Save/Apply"/> <input type="button" value="Cancel"/> <input type="button" value="logout"/>	

#### Remote Access

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

Change Password	
<b>Name</b>	Enter a new username for logging in to the New Name entry box.
<b>Password</b>	Enter a new password for logging in to the Password entry box.
<b>Confirm Password</b>	Re-enter the new password in the Confirm Password entry box for confirmation.
<b>Save/Apply / Cancel</b>	Click <b>Save/Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.
Remote Access (only applicable in AP Router and Client Router mode)	
<b>Remote Management</b>	Enable or Disable remote management.
<b>Remote Upgrade</b>	Specify whether the firmware of the ECB350 can be upgraded remotely.
<b>Remote Management Port</b>	If remote management is enabled, enter the port number to be used for remote management. Example: If you specify the port number to <b>8080</b> , enter <b>http://&lt;IP address&gt;:8080</b> to access the ECB350.

## 9.2 Management VLAN

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

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

### Management VLAN Settings

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

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

Management VLAN ID

- ☒ No VLAN tag  
☐ Specified VLAN ID   
 (must be in the range 1 ~ 4094. )

[Accept](#)
[Cancel](#)

#### Management VLAN (Only applicable in Access Point mode)

##### Management VLAN ID

If your network includes VLANs, you can specify a VLAN ID for packets pass through the Access Point with a tag. Otherwise, select **No VLAN tag**.

##### Accept / Cancel

Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

**Note:**

1. If you reconfigure the Management VLAN ID, you may lose your connection to the ECB350. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the ECB350 using the new IP address.
2. Clicking **Accept** does not apply the changes. To apply them, use Status > Save/Load (see section 4.1).

## 9.3 SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This is a networking management protocol used to monitor network attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) return the data stored in their Management Information Bases.

### SNMP Settings

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

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

[Save/Apply](#)
[Cancel](#)

SNMP	
<b>SNMP Enable/Disable</b>	Enable or Disable SNMP feature.
<b>Contact</b>	Specify the contact details of the device
<b>Location</b>	Specify the location of the device.
<b>Community Name (Read Only)</b>	Specify the password for the SNMP community for read only access.

<b>Community Name (Read/Write)</b>	Specify the password for the SNMP community with read/write access.
<b>Trap</b>	
<b>Trap Destination Address</b>	Specify the IP address of the computer that will receive the SNMP traps.
<b>Trap Destination Community Name</b>	Specify the password for the SNMP trap community.

## 9.4 Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you also can reload the saved configurations into the device through the **Restore Saved Settings from A File** section. If extreme problems occur, or if the you have set the ECB350 wrongly, you can use the **Factory Default** button in the **Revert to Factory Default Settings** section to restore all the configurations of the ECB350 to the original default settings.

**Backup/Restore Settings**
Home
Reset

---

Save A Copy of Current Settings
Backup

Restore Saved Settings from A File
Browse...
Restore

Revert to Factory Default Settings
Factory Default

---

Backup/Restore	
<b>Save A Copy of Current Settings</b>	Click <b>Backup</b> to save the current configured settings.
<b>Restore Saved Settings from A File</b>	To restore settings that have been previously backed up, click <b>Browse</b> , select the file, and click <b>Restore</b> .
<b>Revert to Factory Default Settings</b>	Click <b>Factory Default</b> button to restore the ECB350 to its factory default settings.

## 9.5 Firmware Upgrade

This page allows you to upgrade the firmware of the ECB350.

**Firmware Upgrade**

HomeReset

---

Current firmware version: 1.0.4

Locate and select the upgrade file from your hard disk:

Browse...

---

Upload

### To perform the Firmware Upgrade:

1. Click the **Browse** button and navigate the OS File System to the location of the upgrade file.
2. Select the upgrade file. The name of the file will appear in the *Upgrade File* field.
3. Click the **Upload** 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.



## 9.6 Time Setting

This page allows you to set the internal clock of the ECB350.

### Time Settings

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

#### Time

☐ **Manually Set Date and Time**

2011 / 06 / 27 13 : 26

☒ **Automatically Get Date and Time**

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

☐ User defined NTP Server: 209.81.9.7

[Save/Apply](#)
[Cancel](#)

Time	
<b>Manually Set Date and Time</b>	Manually specify the date and time.
<b>Automatically Get Date and Time</b>	Select a time zone from the drop-down list and check whether you want to enter the IP address of an NTP server or use the default NTP server to get have the internal clock set automatically.

## 9.7 Log

This page allows you to setup Syslog and local log functions of the ECB350.

### Log

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

#### Syslog

Syslog

Disable ▾

Log Server IP Address

.  .  .

#### Local log

Local Log

Enable ▾

Save/Apply

Cancel

Log	
<b>Syslog</b>	Enable or disable the syslog function.
<b>Log Server IP Address</b>	Enter the IP address of the log server.
<b>Local Log</b>	Enable or disable the local log service.
<b>Save/Apply / Cancel</b>	Click <b>Save/Apply</b> to apply the changes or <b>Cancel</b> to return previous settings.

## 9.8 Diagnostics

This page allows you to analyze the connection quality of the ECB350 and trace the routing table to a target in the network.

### Diagnostics

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

#### Ping Test Parameters

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

[Start Ping](#)

#### Traceroute Test Parameters

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

[Start Traceroute](#)

### Diagnosis

<b>Target IP</b>	Enter the IP address you would like to search.
<b>Ping Packet Size</b>	Enter the packet size of each ping.
<b>Number of Pings</b>	Enter the number of times you want to ping.
<b>Start Ping</b>	Click <b>Start Ping</b> to begin pinging target device (via IP).
<b>Traceroute Target</b>	Enter an IP address or domain name you want to trace.
<b>Start Traceroute</b>	Click <b>Start Traceroute</b> to begin the trace route operation.

## 9.9 LED Control

This page allows you to control LED for Power, LAN interface and WLAN interface of the ECB350.

### LED Control

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

#### LED Control

Power LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
LAN LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
WLAN LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF

[Save/Apply](#)[Cancel](#)

## 9.10 Logout

Click **Logout** in the **Management** menu to logout of the ECB350 interface.



## 9.11 Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reboot the Device** to reboot the ECB350.

**Reset**

HomeReset

---

The System Settings section allows you to reboot the device, or restore the device to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules you have created.

System Commands

Reboot the Device

Restore to Factory Defaults

---

## 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 **diopole** antenna have a maximum gain of **[5]** dB. 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-ECB350 / Model: ECB350**) 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 dB [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-ECB350 / Modèle: ECB350) 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
- 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> deklaruoją, 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.