

11N Multi-Function Access Point

EAP350

11N Multi-Function Access Point

V1.0



Table of Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 4 |
| 1.1 | Features and Benefits | 4 |
| 1.2 | Package Contents..... | 5 |
| 1.3 | System Requirements..... | 6 |
| 1.4 | Applications | 6 |
| 2 | Before you Begin | 8 |
| 2.1 | Considerations for Wireless Installation | 8 |
| 2.2 | Computer Settings (Windows XP/Windows 7) | 9 |
| 2.3 | Apple Mac X OS..... | 12 |
| 2.4 | Hardware Installation..... | 13 |
| 3 | Configuring Your Access Point | 15 |
| 3.1 | Default Settings..... | 15 |
| 3.2 | Web Configuration..... | 16 |
| 4 | Status..... | 18 |
| 4.1 | Save/Reload | 18 |
| 4.2 | Main | 19 |
| 4.3 | Wireless Client List..... | 21 |
| 4.4 | System Log..... | 22 |
| 5 | System..... | 23 |
| 5.1 | Operation Mode | 23 |
| 5.2 | IP Settings..... | 24 |
| 5.3 | Spanning Tree Setting..... | 25 |
| 6 | Wireless..... | 27 |

| | | |
|----------|--|-----------|
| 6.1 | Wireless Network..... | 27 |
| 6.2 | Wireless Security..... | 30 |
| 6.3 | Wireless MAC Filter | 34 |
| 6.4 | Wireless Advanced | 35 |
| 6.5 | WPS (Wi-Fi Protected Setup)..... | 37 |
| 6.6 | WDS Link Settings | 39 |
| 7 | Management | 41 |
| 7.1 | Administration..... | 41 |
| 7.2 | Management VLAN..... | 42 |
| 7.3 | SNMP | 43 |
| 7.4 | Backup/Restore..... | 45 |
| 7.5 | Firmware Upgrade..... | 46 |
| 7.6 | Time Setting | 47 |
| 7.7 | Log..... | 48 |
| 7.8 | Diagnosis | 49 |
| 7.9 | LED Control | 50 |
| 7.10 | Logout..... | 51 |
| 7.11 | Reset | 52 |
| 8 | Building a Wireless Network | 53 |
| 8.1 | Access Point Mode..... | 53 |
| 8.2 | Access Point Mode with WDS Function (WDS AP mode)..... | 54 |
| 8.3 | WDS Bridge Mode..... | 55 |
| | Appendix A – FCC Interference Statement | 56 |

Revision History

| Version | Date | Notes |
|----------------|-------------|---------------|
| 1.0 | 2011/07/28 | First Release |

1 Introduction

EAP350 is a multi-functioned 11n product with 3 major multi-functions, is designed to operate in every working environment for enterprises.

EAP350 is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11b/g devices. EAP350 supports home network with superior throughput, performance and unparalleled wireless range.

To protect data during wireless transmissions, EAP350 encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2. Its MAC address filter allows users to select stations with access to connect network. In addition, the function of user isolation protects private network between client users. EAP350 thus is the best product to ensure network safety for enterprises.

1.1 Features and Benefits

| Features | Benefits |
|---|---|
| High Speed Data Rate Up to 300Mbps | Capable of handling heavy data payloads such as MPEG video streaming. |
| 10/100/1000 Fast Ethernet | Support up to 1Gbps networking speed. |
| IEEE 802.11n draft Compliant and backward compatible with 802.11b/g | Fully compatible with IEEE 802.11b/g/n devices. |
| Multi-Function, 3 functions | Allowing users to select AP, WDS AP or WDS Bridge mode in various applications. |
| Point-to-point, Point-to-multipoint Wireless Connectivity | Allowing to transfer data from buildings to buildings. |

| | |
|---|--|
| Support Multi-SSID function (4 SSID) in AP mode | Allowing clients to access different networks through a single access point and to assign different policies and functions for each SSID by manager. |
| WPA2/WPA/ IEEE 802.1x support | Powerful data security. |
| MAC address filtering in AP mode | Ensuring secure network connection. |
| User isolation support (AP mode) | Protecting the private network between client users. |
| Power-over-Ethernet (IEEE802.3af) | Flexible Access Point locations and saving cost. |
| Keep personal setting | Keeping the latest setting when firmware upgrade. |
| SNMP Remote Configuration Management | Helping administrators to remotely configure or manage the Access Point easily. |
| QoS (WMM) support | Enhancing user performance and density. |

1.2 Package Contents

The package contains the following items. In case of return, please keep the original box set, and the complete box set must be included for full refund.

- EAP350
- 12V/1A 100V~240V Power Adapter
- RJ-45 Ethernet LAN Cable
- CD-ROM with User's Manual
- Quick 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, Mac OS or Linux based operating systems
- Internet Explorer or Firefox or Safari Web-Browser Software

1.4 Applications

The 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. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**

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

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

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

d) **Frequently changed environments**

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

e) 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

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

g) Wired LAN backup

Network managers 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 EAP350 is very important to avoid poor signal reception and performance. Avoid placing the device in enclosed spaces 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. These could be the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through. Here are some key guidelines to ensure that you have the optimal wireless range.

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

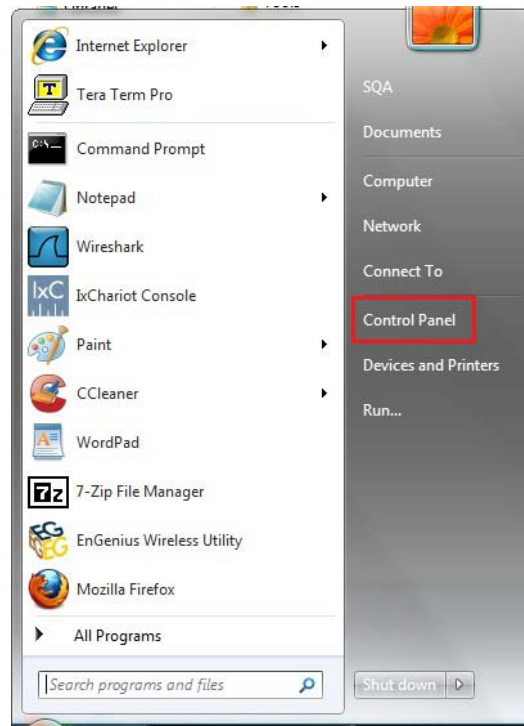
2.2 Computer Settings (Windows XP/Windows 7)

This device can be configured as an Access Point, WDS AP or WDS Bridge. The default IP address of the device is **192.168.1.1** (In Access Point Mode as default). In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

- Click Start button and open Control Panel.



Windows XP



Windows 7

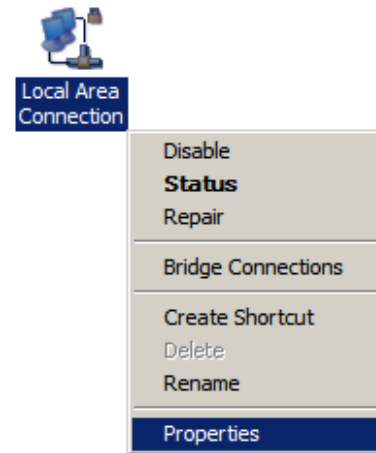
- Windows XP, click [Network Connection]



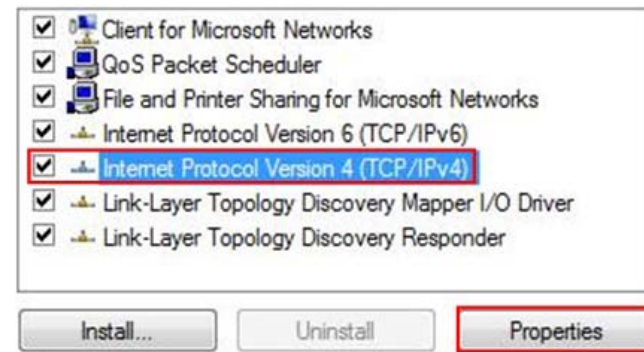
- Windows 7, click [View Network Status and Tasks] then [Change adapter settings]



- Right click on [Local Area Connection] and select [Properties].



- Select "**Internet Protocol (TCP/IP)**" and click [Properties]



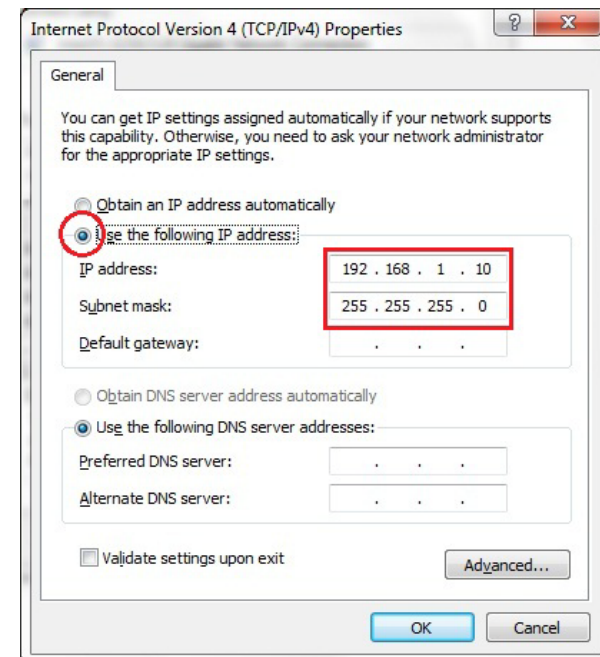
- Select "**Use the following IP address**" and enter IP address and subnet mask then click [OK].

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

For example: Device IP address: 192.168.1.1

PC IP address: 192.168.1.10

PC subnet mask: 255.255.255.0

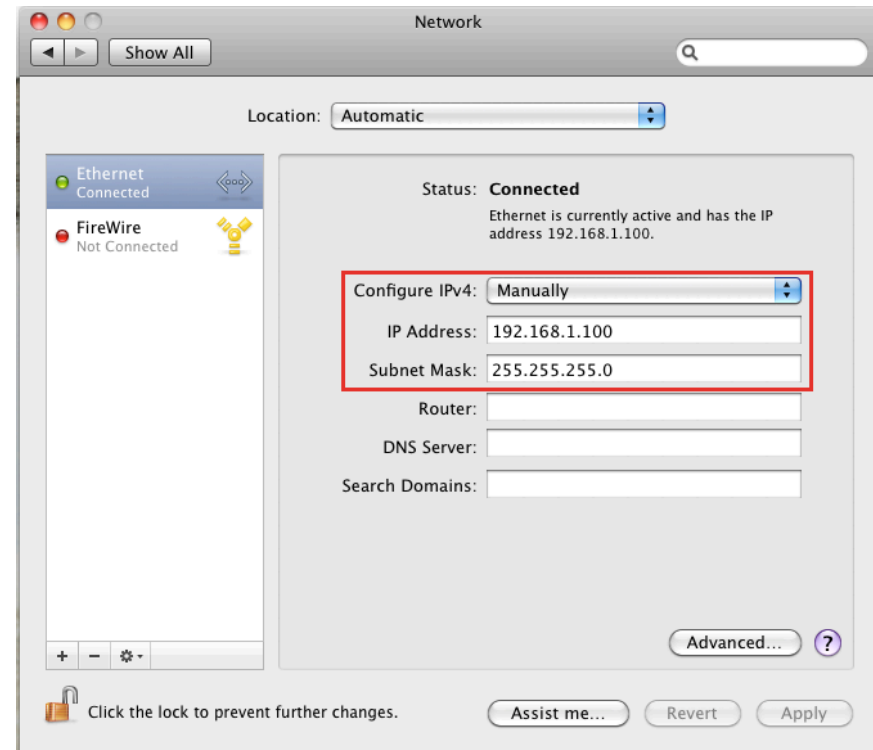


2.3 Apple Mac X OS

- Go to **System Preferences > Network**



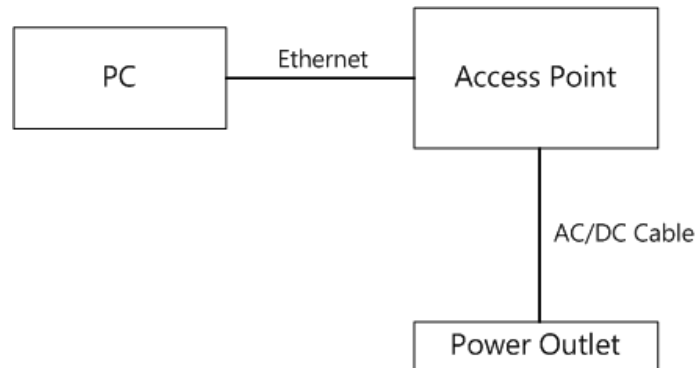
- Under Network setting, select "**Manually**" and enter IP address and subnet mask.
- Click **Apply** when done.



2.4 Hardware Installation

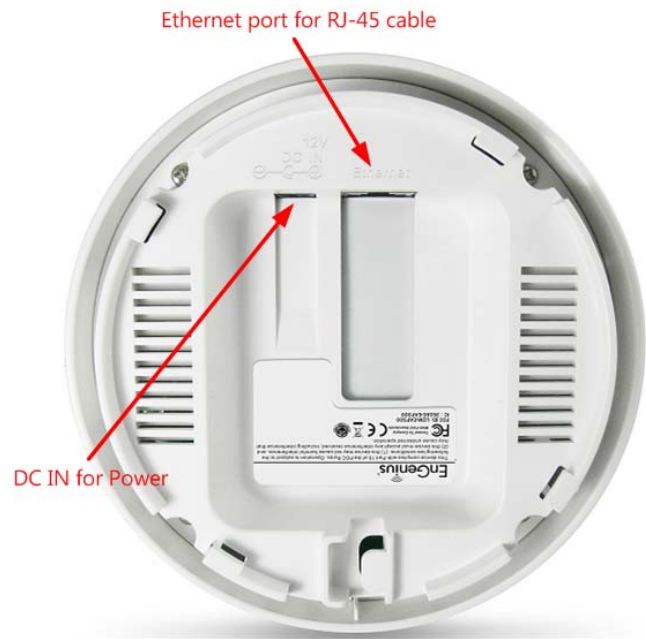
1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Ethernet port of the device and another end into your PC/Notebook.
3. Insert the DC-inlet of the power adapter into the port labeled "DC-IN" and the other end into the power socket on the wall.

This diagram depicts the hardware configuration.





Front Panel



Rear Panel

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

3 Configuring Your Access Point

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 Access Point.

Default Settings

| | |
|---------------------|----------------|
| IP Address | 192.168.1.1 |
| Username / Password | admin / admin |
| Operation Mode | Access Point |
| Wireless SSID | EnGeniusxxxxxx |
| Wireless Security | None |

Note: xxxxxx represented in the wireless SSID above is the last 6 characters of your device MAC Address. This can be found on the device body label and is unique for each device.

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 title is "EnGenius". Below the title, there are two input fields: "Username:" with the text "admin" and "Password:" with five dots. Below the input fields are two buttons: "Login" and "Reset".

- You will see the following webpage if login successfully.

The screenshot displays the EnGenius Wireless Access Point web interface. The top navigation bar includes the EnGenius logo and the title "Wireless Access Point". A left sidebar menu is titled "Access Point" and contains sections for Status, System, Wireless, and Management. The main content area is titled "Main" and includes "Home" and "Reset" buttons. The interface is divided into three main sections: System Information, LAN Settings, and Current Wireless Settings, each presented as a table.

System Information

| | |
|---------------------------|------------------------------|
| Device Name | EAP350 |
| Ethernet Main MAC Address | 00:02:6F:BE:EF:06 |
| Wireless MAC Address | 00:02:6F:BE:EF:06 |
| Country | N/A |
| Current Time | Wed Jul 27 06:56:02 UTC 2011 |
| Firmware Version | 1.0.4 |
| Management VLAN ID | Untagged |

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 | Access Point |
| Wireless Mode | IEEE 802.11b/g/n Mixed |
| Channel Bandwidth | 20-40 MHz |
| Frequency/Channel | 2.462 GHz (Channel 11) |
| Profile Isolation | No |
| Profile Settings (SSID/Security/VID) | 1 EnGeniusBEEF06/None/1 |
| | 2 N/A |
| | 3 N/A |

4 Status

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

4.1 Save/Reload

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

Save/Reload

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

Unsaved changes list

```
-network.1.ifname
-network.4.ifname
-network.3.ifname
-network.2.ifname
wireless.cfg0de25d.WLANWpaAccEnable=0
wireless.cfg036f4e.wps_configured=1
wireless.cfg036f4e.key=12345678
wireless.cfg036f4e.encryption=psk-mixed tkip+aes
wireless.cfg036f4e.WLANWpaRadiusAccSrvIP=...
wireless.cfg036f4e.hidden=0
wireless.cfg036f4e.server=...
-wireless.cfg0bb08c.WLANWDSPeer
```

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

4.2 Main

Clicking the **Main** link under the **Status** menu or clicking **Home** at the top-right of the Web Configurator shows 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.

System Information

| | |
|---------------------------|------------------------------|
| Device Name | EAP350 |
| Ethernet Main MAC Address | 00:02:6F:BE:EF:06 |
| Wireless MAC Address | 00:02:6F:BE:EF:06 |
| Country | N/A |
| Current Time | Wed Jul 27 06:56:02 UTC 2011 |
| Firmware Version | 1.0.4 |
| Management VLAN ID | Untagged |

- The **LAN Settings** section shows Local Area Network setting 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 **Current Wireless Settings** section shows wireless information such as operating mode, frequency and channel. Since the EAP350 supports multiple-SSIDs, information about each SSID, such as its ESSID and security settings, are displayed.

Current Wireless Settings

| | |
|---|-------------------------|
| Operation Mode | Access Point |
| Wireless Mode | IEEE 802.11b/g/n Mixed |
| Channel Bandwidth | 20-40 MHz |
| Frequency/Channel | 2.462 GHz (Channel 11) |
| Profile Isolation | No |
| Profile Settings (SSID/Security/VID) | 1 EnGeniusBEEF06/None/1 |
| | 2 N/A |
| | 3 N/A |
| | 4 N/A |
| Spanning Tree Protocol | Disabled |
| Distance | 1 Km |

4.3 Wireless Client List

Clicking the **Wireless Client List** link under the **Status** menu displays the list of clients associated to the EAP350, along with the MAC addresses and signal strength for each client. Clicking the [**Refresh**] button updates (refreshes) the client list.

Note: Only in Access Point and WDS AP 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](#)

4.4 System Log

The EAP350 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.

Home
Reset

Show log type
All

```

Jun 27 12:00:03 EAP350 user.notice root: starting ntpclient
Jun 27 12:00:02 EAP350 user.notice root: starting ntpclient
Jun 27 12:00:01 EAP350 cron.err crond[1103]: USER root pid 1501 cmd . /etc/notplug.d/iface/20-ntp
Jun 27 11:56:40 EAP350 user.warn kernel: jffs2_build_filesystem(): erasing all blocks after the er
Jun 27 11:56:40 EAP350 user.info kernel: mini_fo: using storage directory: /jffs
Jun 27 11:56:40 EAP350 user.info kernel: mini_fo: using base directory: /
Jun 27 11:56:34 EAP350 user.warn kernel: jffs2_scan_eraseblock(): End of filesystem marker found e
Jun 27 11:56:34 EAP350 user.warn kernel: jffs2_build_filesystem(): unlocking the mtd device... do
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: using local addresses only for domain lan
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: using local addresses only for domain lan
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: started, version 2.52 cachesize 150
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: reading /tmp/resolv.conf.auto
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: read /etc/hosts - 1 addresses
Jun 27 11:56:31 EAP350 daemon.info dnsmasq[1221]: compile time options: IPv6 GNU-getopt no-DBus no
Jun 27 11:56:27 EAP350 cron.err crond[1103]: crond (busybox 1.15.3) started, log level 5
Jun 27 11:56:26 EAP350 user.warn kernel: start running
Jun 27 11:56:26 EAP350 user.warn kernel: osif_vap_init :vap up
Jun 27 11:56:26 EAP350 user.info kernel: device ath0 entered promiscuous mode
Jun 27 11:56:26 EAP350 user.info kernel: br-lan: topology change detected, propagating
Jun 27 11:56:26 EAP350 user.info kernel: br-lan: port 2(ath0) entering learning state
Jun 27 11:56:26 EAP350 user.info kernel: br-lan: port 2(ath0) entering forwarding state
Jun 27 11:56:25 EAP350 user.warn kernel: osif_acs_start_bss :vap up

```

Refresh
Clear

| System Log | |
|----------------|-----------------|
| Refresh | Update the log. |
| Clear | Clear the log. |

5 System

5.1 Operation Mode

The EAP350 supports three operating modes: Access Point, WDS Access Point and WDS Bridge.

System Properties

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

System Properties

| | |
|----------------|---|
| Device Name | EAP350 (1 to 32 characters) |
| Country/Region | Please Select a Country Code ▼ |
| Operation Mode | <input type="radio"/> Access Point <input checked="" type="radio"/> WDS <input checked="" type="radio"/> Access Point <input type="radio"/> Bridge |

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

| System Properties | |
|------------------------|---|
| Device Name | 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. |
| Country/Region | Select a Country/Region to conform to local regulations. |
| Operation Mode | Use the radio button to select an operating mode. |
| Accept / Cancel | Click [Accept] to confirm the changes or [Cancel] to cancel and return previous settings. |

5.2 IP Settings

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

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 | |
|--------------------------------|---|
| IP Network Setting | 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. |
| IP Address | The IP Address of this device. |
| IP Subnet Mask | The IP Subnet Mask of this device. |
| Default Gateway | The Default Gateway of this device. Leave it blank if you are unsure of this setting. |
| Primary / Secondary DNS | The primary / secondary DNS address for this device. |

5.3 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.

Spanning Tree Settings

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

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

| Spanning Tree | |
|-----------------------------|---|
| Spanning Tree Status | Enable or disable the Spanning Tree function. |
| Bridge Hello Time | Specify Bridge Hello Time, in seconds. This value determines how often the device sends hello packets to communicate information about the topology throughout the entire Bridged Local Area Network. |
| Bridge Max Age | 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. |
| Bridge Forward Delay | 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 looks at some traffic before participating. |

| | |
|------------------------|---|
| Priority | Specify the Priority number. Smaller number has greater priority. |
| Accept / Cancel | Click [Accept] to confirm the changes or [Cancel] to cancel and return previous settings. |

6 Wireless

6.1 Wireless Network

This page shows the current status of the device's Wireless settings.

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 | Scan |

Current Profiles

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

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

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

| Wireless Network | |
|----------------------------|---|
| Wireless Mode | Wireless mode supports 802.11b/g/n mixed mode. |
| Channel HT Mode | The default channel bandwidth is 20/40MHz. The larger the channel, the better the transmission quality and speed. |
| Extension Channel | Select upper or lower channel. Your selection may affect the Auto channel function. |
| Channel / Frequency | Select the channel and frequency appropriate for your country's regulation. |
| Auto | Check this option to enable auto-channel selection. |
| AP Detection | AP Detection can select the best channel to use by scanning nearby areas for Access Points. |
| Current Profile | Configure up to four different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click [Edit] to configure the profile and check whether you want to enable extra SSID. |
| Profile Isolation | Restricted client to communicate with different VID by selecting the radio button. |
| Accept / Cancel | Click [Accept] to confirm the changes or [Cancel] 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 | |
|---------------------------|---|
| SSID | Specify the SSID for the current profile. |
| VLAN ID | Specify the VLAN tag for the current profile. |
| Suppressed SSID | Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey. |
| Station Separation | Click the appropriate radio button to allow or prevent communication between client devices. |
| Wireless Security | See the Wireless Security section. |
| Save / Cancel | Click [Save] to accept the changes or [Cancel] to cancel and return previous settings. |

6.2 Wireless Security

The Wireless Security section lets you configure the EAP350's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you use WPA2-PSK.

Note: Only in Access Point and WDS AP mode.

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 Open System or Shared Key . |
| Input type | ASCII: regular text (recommended) HEX: 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 the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key . |
| Encryption Key # | 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 | |
|--|---|
| Encryption | Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings. |
| Passphrase | 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. |
| Group Key Update Interval | Specify how often, in seconds, the group key changes. |

WPA Encryption:**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 | |
|----------------------------------|--|
| Encryption | Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings. |
| Radius Server | Enter the IP address of the Radius Server |
| Radius Port | Enter the port number used for connections to the Radius server. |
| Radius Secret | Enter the secret required to connect to the Radius server. |
| Group Key Update Interval | 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 change from 802.11n to 802.11g.

6.3 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 EAP350. The default setting is Disable Wireless MAC Filter.

Note: Only in Access Point and WDS AP 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 | Delete |

Accept

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

6.4 Wireless Advanced

This page allows you to configure wireless advance settings. It is recommended the default settings are used unless the user has experience with these functions.

Wireless Advanced Settings

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

| | |
|------------------------------|---|
| Data Rate | Auto ▾ |
| Transmit Power | 17 dBm ▾ |
| RTS/CTS Threshold (1 - 2346) | 2346 bytes |
| Distance (1-30km) | 1 km |
| Short GI: | Enable ▾ |
| 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](#)

| Wireless Advanced | |
|---------------------------------|---|
| Data Rate | Select a data rate from the drop-down list. The data rate affects throughput. If you select a low data rate value, for example, the throughput is reduced but the transmission distance increases. |
| Transmit Power | Set the power output of the wireless signal. |
| RTS/CTS Threshold | Specify the threshold package size for RTC/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth. |
| Distance | Specify the distance between Access Points and clients. Longer distances may drop high-speed connections. |
| Short GI | Sets the time that the receiver waits for RF reflections to settle out before sampling data. Using a short (400ns) guard interval can increase throughput, but can also increase error rate in some installations due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation. |
| Aggregation | Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes. |
| Wireless Traffic Shaping | Check this option to enable wireless traffic shaping. Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service. |
| Incoming Traffic Limit | Specify the wireless transmission speed used for downloading. |
| Outgoing Traffic Limit | Specify the wireless transmission speed used for uploading. |
| Accept / Cancel | Click [Accept] to confirm the changes or [Cancel] to cancel and return previous settings. |

6.5 WPS (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 in Access Point and WDS AP mode.

WPS Setting

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

WPS

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

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

| Wi-Fi Protected Setup (WPS) | |
|------------------------------------|--|
| WPS | Select Enable or Disable the WPS feature. |
| WPS Current Status | Shows whether the WPS function is Configured or unConfigured . Configured means that WPS has been used to authorize connection between the device and wireless clients. |
| Self Pin Code | The PIN code of this device. |
| SSID | The SSID (wireless network name) used when connecting using WPS. |
| Authentication Mode | Shows the encryption method used by the WPS process. |
| Passphrase Key | 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. |
| WPS Via Push Button | Click this button to initialize WPS feature using the push button method. |
| WPS Via PIN | Enter the PIN code of the wireless device and click this button to initialize WPS feature using the PIN method. |

6.6 WDS Link Settings

Using WDS (Wireless Distribution System) to connect Access Point wirelessly, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

Note that compatibility between different brands and models is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note that 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 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 ▾ |

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

7 Management

7.1 Administration

This page allows you to change the system password and to configure remote management. By default, the user name is **admin** and the password is: **admin**.

Password can contain 0 to 12 alphanumeric characters and are case sensitive.

Login Setting

| | |
|------------------|-------|
| Name | admin |
| Password | |
| Confirm Password | |

| Change Password | |
|----------------------------|--|
| Name | Enter a new username for logging in to the Web Configurator. |
| Password | Enter a new password for logging in to the Web Configurator. |
| Confirm Password | Re-enter the new password for confirmation. |
| Save/Apply / Cancel | Click Save/Apply to apply the changes or Cancel to return previous settings. |

7.2 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 that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Management VLAN Settings

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

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

| | |
|--------------------|---|
| Management VLAN ID | <input checked="" type="radio"/> No VLAN tag <input type="radio"/> Specified VLAN ID <input type="text"/> (must be in the range 1 ~ 4094.) |
|--------------------|---|

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

| Management VLAN | |
|---------------------------|--|
| Management VLAN ID | If your network includes VLANs and if tagged packets need to pass through the Access Point, enter the VLAN ID. Otherwise, click 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 EAP350. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the EAP350 using the new IP address.
2. Clicking **Accept** does not apply the changes. To apply them, use Status > Save/Load (see section 4.1).

7.3 SNMP

This page allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP 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) | public <input type="text"/> |
| Community Name (Read/Write) | private <input type="text"/> |
| Trap Destination Address | <input type="text"/> |
| Trap Destination Community Name | <input type="text"/> |

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

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

7.4 Backup/Restore

This page 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 Saved Settings from A File]**. If extreme problems occur you can use the **[Revert to Factory Default Settings]** to set all configurations to its 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 | |
|---|--|
| Save A Copy of Current Settings | Click [Backup] to save the current configured settings. |
| Restore Saved Settings from A File | To restore settings that have been previously backed up, click [Browse] , select the file, and click [Restore] . |
| Revert to Factory Default Settings | Click [Factory Default] button to restore the EAP350 to its factory default settings. |

7.5 Firmware Upgrade

This page allows you to upgrade the device's firmware.

The screenshot shows a web interface for a firmware upgrade. At the top left, the title "Firmware Upgrade" is displayed in a large, bold, dark blue font. To the right of the title are two buttons: "Home" and "Reset", both in a light blue box with dark text. Below the title bar, a horizontal line separates the header from the main content. The main content area has a light blue background. It starts with the text "Current firmware version: 1.0.3" in a dark blue font. Below this is the instruction "Locate and select the upgrade file from your hard disk:" in a dark blue font. Underneath the instruction is a text input field, currently empty, followed by a "Browse..." button. At the bottom of the main content area, there is an "Upload" button.

To perform the Firmware Upgrade:

1. Click the [**Browse**] button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name 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.

7.6 Time Setting

This page allows you to set the system time.

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

Manually Set Date and Time

Manually specify the date and time.

Automatically Get Date and Time

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.

7.7 Log

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

Log

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

Syslog

| | |
|-----------------------|---|
| Syslog | Disable ▾ |
| Log Server IP Address | <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> |

Local log

| | |
|-----------|----------|
| Local Log | Enable ▾ |
|-----------|----------|

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

Log

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

7.8 Diagnosis

This page allows you to ascertain connection quality and trace the routing table to the target.

Diagnostics

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

Ping Test Parameters

| | |
|---|----------------------|
| Target IP | <input type="text"/> |
| Ping Packet Size | 64 Bytes |
| Number of Pings | 4 |
| <input type="button" value="Start Ping"/> | |

Traceroute Test Parameters

| | |
|---|----------------------|
| Traceroute target | <input type="text"/> |
| <input type="button" value="Start Traceroute"/> | |

| Diagnosis | |
|--------------------------|---|
| Target IP | Enter the IP address you would like to search. |
| Ping Packet Size | Enter the packet size of each ping. |
| Number of Pings | Enter the number of times you want to ping. |
| Start Ping | Click [Start Ping] to begin pinging. |
| Traceroute Target | Enter an IP address or domain name you want to trace. |
| Start Traceroute | Click [Start Traceroute] to begin the trace route operation. |

7.9 LED Control

This page allows you to control LED on/off for Power, LAN interface and WLAN interface.

LED Control

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

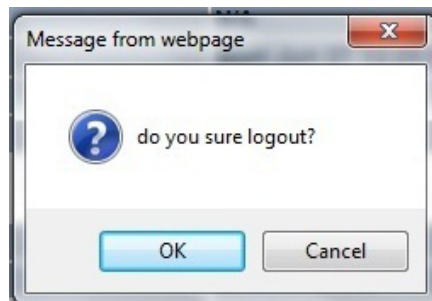
LED Control

| | |
|-----------|---|
| 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](#)

7.10 Logout

Click [**Logout**] in **Management** menu to logout.



7.11 Reset

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

Reset

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

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](#)

8 Building a Wireless Network

With its ability to operate in various operating modes, your EAP350 is the ideal device around which you can build your WLAN. This appendix describes how to build a WLAN around your EAP350 using the device's operating modes.

8.1 Access Point Mode

In Access Point Mode, EAP350 behaves like a central connection for stations or clients that support IEEE 802.11b/g/n networks. Stations and clients must be configured to use the same SSID and security password to associate with the EAP350. The EAP350 supports four SSIDs at the same time for secure guest access.



8.2 Access Point Mode with WDS Function (WDS AP mode)

The EAP350 also supports WDS AP mode. This operating mode allows wireless connections to the EAP350 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.



8.3 WDS Bridge Mode

In WDS Bridge Mode, the EAP350 can wirelessly connect different LANs by configuring the MAC address and security settings of each EAP350 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 EAP350 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 is unlike 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 loop in your wireless connection, otherwise enable Spanning Tree Function.

Appendix A – FCC Interference Statement

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

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