

Wireless LAN Access Point

With WDS function

User Guide

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and

2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC 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. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

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

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

TABLE OF CONTENT

About This Guide.....	1
Purpose	1
Overview of this User's Guide.....	1
Unpacking and Setup	3
Unpacking.....	3
Setup	3
Hardware Instalation.....	5
LED Indicator	5
Rear Panel.....	6
Hardware connections.....	7
Connect to the Switch/Hub	7
Check the installation.....	7
Configuring the Wireless LAN Access Point	9
Login.....	9
Site Contents of the Access Point	10
Status.....	11
Wireless	12
TCP/IP Setting	19
Statistics	19
Upgrade Firmware	20
Save/Reload Settings	21
Password Settings	22
Technical Specifications	23

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11b Wireless LAN Access Point. This manual helps to features the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11b) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to eleven megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User's Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- ◆ One Wireless Access Point
- ◆ One external power adapter
- ◆ One CD-Rom (User's guide)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

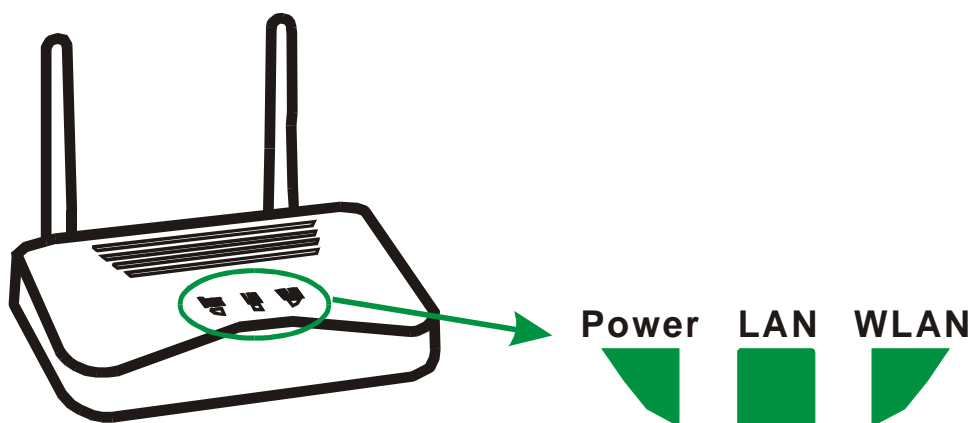
- ◆ Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, with line of sight to all of your mobile stations.
 - ◆ Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged in to the system's Ethernet switch/hub port.
 - ◆ Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
-

- ◆ Visually inspect if the Power Adaptor was fully plugged to the device power jack.

HARDWARE INSTALATION

LED Indicator

The figure below shows the LED Indicator of the Wireless LAN Access Point.



Front View

POWER

This indicator lights green when the Access Point receives power. Otherwise, it turns off.

LAN (Link/ACT)

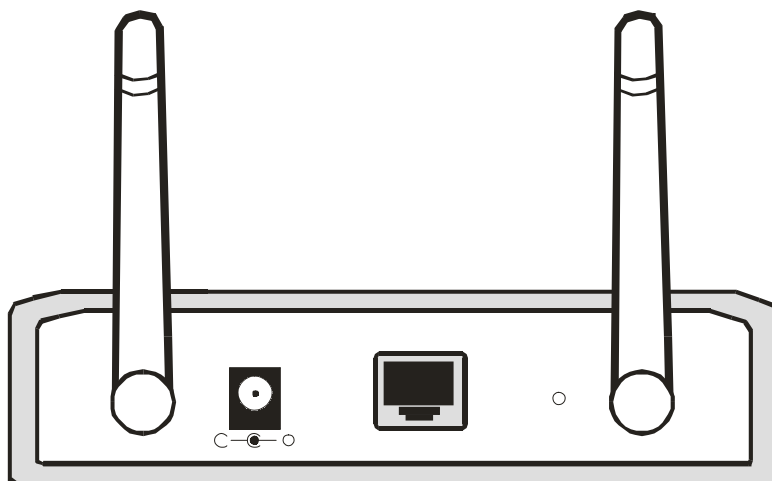
The indicator lights green when the LAN port is connected to a 100Mbps Ethernet station, the indicator blinks green while transmitting or receiving data on the 100Mbps Ethernet network.

WLAN (Link)

The indicator blinks green when the wireless station connected to the AP, the AP is always transmitting or receiving data once a wireless device is connected, otherwise, the light turns off.

Rear Panel

The figure below shows the rear panel of the Access Point



Rear Panel

Ethernet

Ethernet uplink port with auto-sensing for connecting to either 10/100Mbps Fast Ethernet connections, connect this port to switch/hub.

Reset

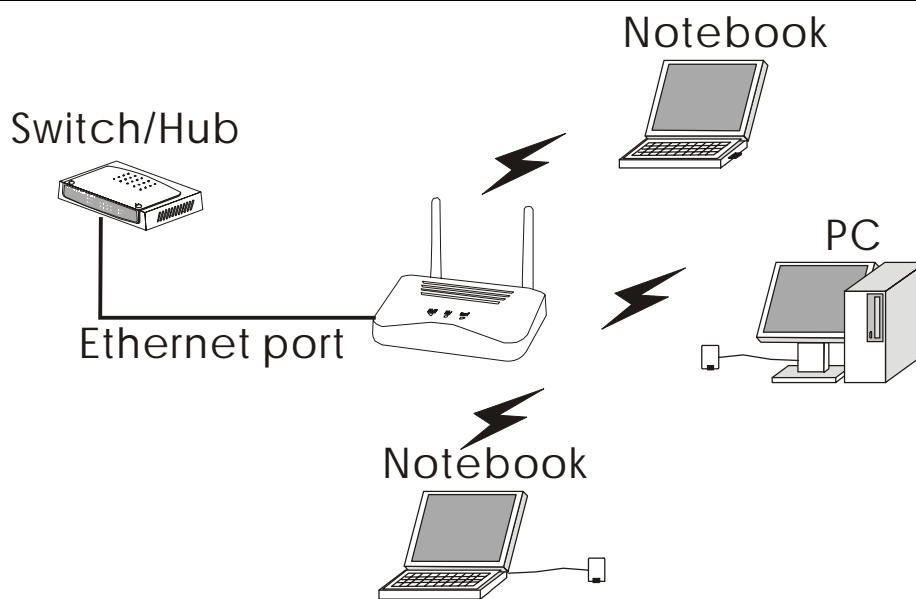
There is two function by pressing the “Reset” button, one is software reboot and the other is factory reset.

- ✓ Software Reboot: to reboot the Access Point, press the “Reset” button.
- ✓ Factory Reset: to reset the setting back to factory default setting, press the “Reset” button within 10 seconds, once you press the button, the LED of the WLAN will turn off and when the Access Point is ready, the LED will start blinking.

DC Power

Connect the AC Power Adapter to the AP’s power jack.

Hardware connections



Wireless LAN Networking

Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The control LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. If the LAN Port's Link indicator does not light up then check the RJ-45 cable if it is firmly feed to the RJ45 port, while the LAN is link up to the Switch/Hub, the LAN port's LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has a Web GUI interface for the configuration. The AP can be configured through the Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP to enable its functions.

Login

Before you configure this device, note that when the AP is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP network**. For example, when the default network address of the default IP address of the AP is **192.168.1.100**, then the manager PC should be set at 192.168.1.x (where x is a number between 1 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

Enter IP address ***http://192.168.1.100*** (the factory-default IP address setting) to the address location.

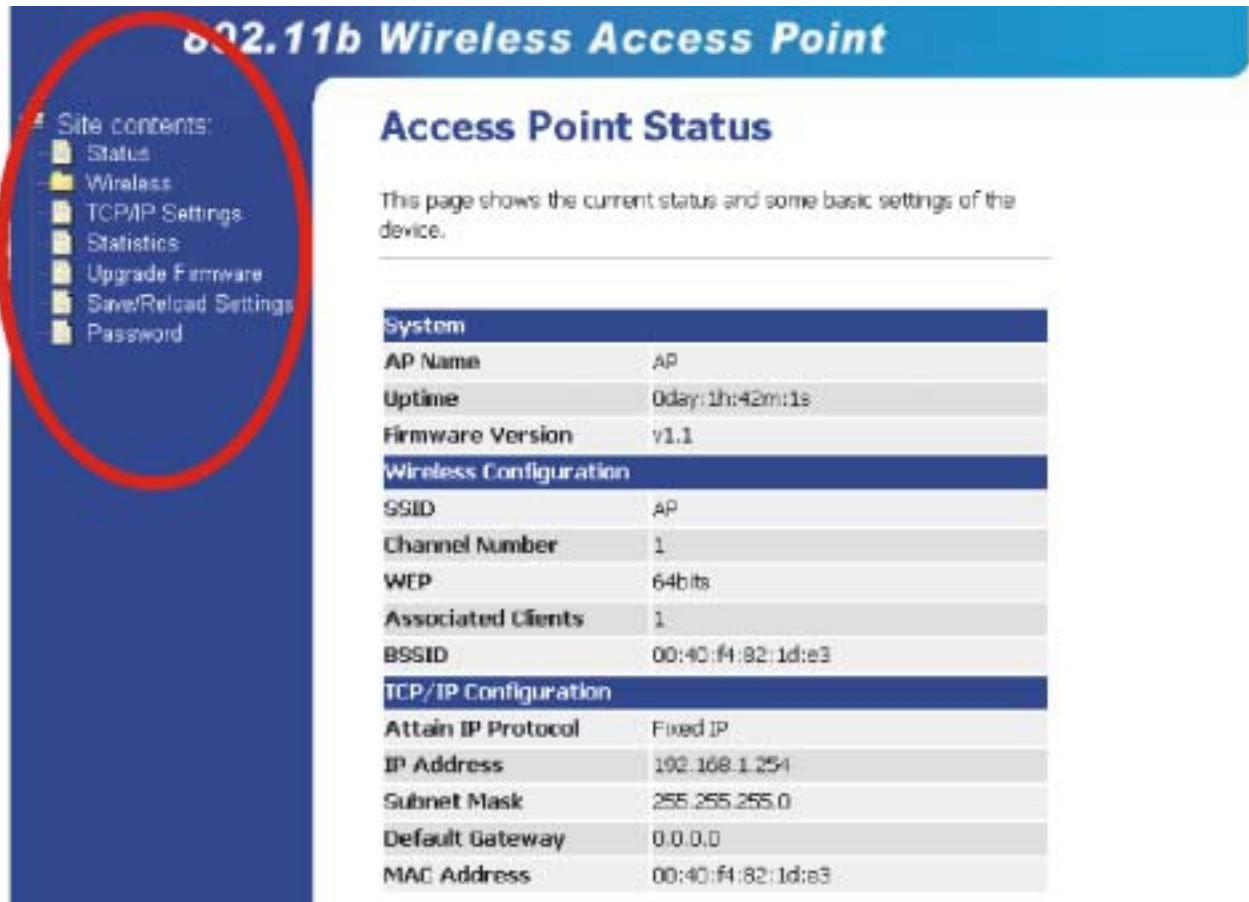


When there is a screen need to enter the Network password, it means that there is a password settle, type in the password you entered before. There is no need to enter any password when you first login the AP, the default setting is without password.



Site Contents of the Access Point

There are seven main functions included in the site contents: Status, Wireless Settings, TCP/IP Settings, Statistics, Upgrade Firmware, Save and Reload Settings and Password Settings. Point the selections in the left side of the menu screen.



802.11b Wireless Access Point

Site contents:

- Status
- Wireless
- TCP/IP Settings
- Statistics
- Upgrade Firmware
- Save/Reload Settings
- Password

Access Point Status

This page shows the current status and some basic settings of the device.

System	
AP Name	AP
Uptime	0day: 1h:42m:1s
Firmware Version	v1.1

Wireless Configuration	
SSID	AP
Channel Number	1
WEP	64bits
Associated Clients	1
BSSID	00:40:f4:82:1d:e3

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:40:f4:82:1d:e3

Status

The Status Function shows the System, Wireless Configuration and TCP/IP Configuration status and some settings of the Access Point.

Access Point Status

This page shows the current status and some basic settings of the device.

System	
AP Name	AP
Uptime	0day:21h:54m:4s
Firmware Version	v1.1
Wireless Configuration	
SSID	AP
Channel Number	1
WEP	64bits
Associated Clients	1
BSSID	00:40:f4:82:1d:e3
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:40:f4:82:1d:e3

Wireless

The Wireless Settings contain five minor settings, Basic Settings, Advanced Settings, Security, Access Control and Connection List.

I. Basic Settings

This page is to set the AP Name, SSID and Channel Number.

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

AP Name:	<input type="text" value="AP"/>
SSID:	<input type="text" value="AP"/>
Channel Number:	<input type="text" value="1"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

- ◆ **AP Name:** appoint a name for the AP.
- ◆ **SSID:** It is an ASCII string up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. The SSID value must be the same in all stations and AP in the extended WLAN.
- ◆ **Wireless Channel:** There are 14 channels available. The channels differ from country to country. Select the channel to be used.

Click “Apply Changes” after you set your AP Name, SSID and Channels to save the changes, or press “Reset” to set back to factory default setting.

II. Advanced Settings

The Advanced Settings is to set the data transferring, this is used by advanced users who knows what will effect the changes.

Wireless Advanced Settings

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

Authentication Type: Auto Open System Shared Key

Fragment Threshold: (256-2346)

RTS Threshold: (0-2347)

Beacon Interval: (20-1024 ms)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

- ◆ **Authentication Type:** to choose which authentication algorithm will be used, open system, shared key or both type.
- ◆ **Fragment Threshold:** the size at which packets will be fragmented. Choose a setting within a range of 256 to 2346 bytes.
- ◆ **RTS Threshold:** Choose a setting within a range of 0 to 2437 bytes. It is recommended limiting a long packet to prevent each station waiting too long to transmit a data.
- ◆ **Beacon Interval:** With Host AP mode, the most noticeable effect of beacon interval is latency in sending unicast packets to power saving stations and broadcast/multicast packets in general.

- ◆ **Data Rate:** to select the transfer rate from 11, 5.5, 2, 1Mbps and Auto.
- ◆ **Preamble Type:** to limit the packet size of the data to transmit. It is recommended to choose the short preamble when the link quality is bad.
- ◆ **Broadcast SSID:** to broadcast the SSID in the Wireless local area network. When the function is disable, then the wireless client can not detect the SSID while the client is surveying the site of the AP.
- ◆ **IAPP:** InterAP Protocol. A protocol being developed as the 802.11f version of the IEEE 802.11 WLAN specification, to support interoperability, mobility, handover, and coordination among APs in a WLAN. IAPP enables APs to communicate with one another.

III. Security

This function is used to protect wireless communication from eavesdropping. A secondary function of encryption is to prevent unauthorized access to a wireless network, and it can be achieved by using the Encryption function.

This AP provides two mode for Security Encrytion, WPA and WEP.

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption

methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption.

RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Wireless Security Setup

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

Encryption:

WPA Authentication Mode: WPA-RADIUS Pre-Shared Key

WPA Unicast Cipher Suite: TKIP

Pre-Shared Key Format:

Pre-Shared Key:

Use 802.1x Authentication WEP 64bits WEP 128bits

Authentication RADIUS Server: Port IP address

Password

Note: When encryption WEP is selected, you must set WEP key value.

When choose the encryption to WPA mode, you need to select some setting as follow:

- WPA Authentication Mode: select a WPA-Radius or Pre-Shared Key for the authentication mode.
- WPA Unicast Cipher Suite: select the encryption method using TKIP. TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

following range (0~F, hexadecimal), or 64bit in ASCII format, you must type 5 values in the following range (0~9, A~Z and a~z Alphanumeric). Besides, if you select 128bit in Hex format, you must type 26 values (0~F, hexadecimal), or 128bit in ASCII format, you must type 13 values in the following range (0~9, A~Z and a~z Alphanumeric).

Click on the 802.1x function to authenticate the WEP security with the wireless devices, select WEP 64bits or WEP 128bits for authentication.

IV. Access Control

Access Control function allows clients whose MAC addresses in the list will be able to connect to this Access Point. When this function is activate, there is no wireless clients will be able to connect to the Access Point unless they are listed in the Access Control list.

Wireless Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.

Enable Wireless Access Control

MAC Address: Comment:

Apply Changes

Reset

Current Access Control List:

MAC Address	Comment	Select
-------------	---------	--------

Delete Selected

Delete All

Reset

V. Connection List

This function shows the MAC Address, transmission packet counters, reception packet counters, and encrypted status for each associated wireless client.

Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
00:e0:4c:81:81:99	1	5	11	no	65

VI. WDS Setting

WDS (Wireless Distribution System) uses wireless media to communicate with other Aps, click enable WDS to configure the following setting on this page:

WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

Enable WDS

Apply Changes

Reset

Show Statistics

Add WDS AP:

MAC Address

Comment

Current WDS AP List:

MAC Address

Comment

Select

Delete Selected

Delete All

Reset

- **Add WDS AP:** set the MAC address of which AP you want to communicate with, type a name in the comment for the AP to easier the manager to monitor.
- **Current WDS AP List:** when there are AP that you set before, it will list all the AP in this field.

TCP/IP Setting

The TCP/IP Setting is to configure the parameters setting to the LAN which connects with the Access Point, you may change the setting of IP Address, Subnet Mask and Default Gateway.

Enable the function of DHCP Client to let the Access Point have an IP Address automatically assignment by the DHCP server.

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address:	<input type="text" value="192.168.1.254"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP Client:	<input type="button" value="Disabled"/>

Statistics

This screen shows the packet counters for transmission and reception on both Wireless LAN and Ethernet LAN.

Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	Sent Packets	117220
	Received Packets	60388
Ethernet LAN	Sent Packets	58896
	Received Packets	114682

Upgrade Firmware

By upgrading a new firmware for the Access Point to improve functionality and performance. Enter the path and name of the upgrade file then click the Upload button below. You will be prompted to confirm the upgrade.

Note: Do not turn off the power during uploading, it may cause the system crash.

Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

Browse...

Upload

Reset

Save/Reload Settings

This screen allows you to save the current settings, load the settings where you save before, or reset the setting back to factory default.

- ◆ **Save Setting to File:** save the current setting of the Access Point to which path and filename you want to save.
- ◆ **Load Settings from File:** load the setting where you save before, press Browse button to search the filename and press Upload button to start loading the file.
- ◆ **Reset Settings to Default:** this button will help you to bring back to factory default settings.

Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Save...

Load Settings from File:

Browse...

Upload

Reset Settings to Default:

Reset

Password Settings

This screen is used to set the password when you need to login the Access Point, type in the User Name, the New Password and Confirmed Password to access new login security.

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>

TECHNICAL SPECIFICATIONS

General	
Standards	Standard: IEEE 802.11b IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	DSSS (Direct Sequence Spread Spectrum)
Modulation:	QPSK / BPSK / CCK
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency Band:	2.4 GHz
Channel:	1 ~ 11 Channels (US, Canada, China) 1 ~ 13 Channels (Europe, Taiwan) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption
Data Transfer Rate	Fast Ethernet: 100Mbps Wireless: Up to 11Mbps (with Automatic Scale Back)
Transmission Range:	Outdoor: 100~300M Indoor: 40~100M
Network Cables	10BASET: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna:	2 x 2dBi Dipole Antenna 2 x 2dBi Reverse SMA type Dipole Antenna (optional)

Physical and Environmental

DC inputs	DC 5V /1.2 or higher current
Power Consumption	4.5W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	140 x 98 x 30 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B,