

User's Manual

Version: 1.0

Wireless 802.11g Multi-mode AP

Trademarks

Copyright ©2005

Contents are subject to change without notice.

All trademarks belong to their respective proprietors.

Copyright Statement

THIS DOCUMENT CONTAINS OF PROPRIETARY TECHNICAL INFORMATION THAT IS THE PROPERTY OF THIS COMPANY. AND NO PART OF THIS DOCUMENTATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRICAL OR MECHANICAL, BY PHOTOCOPYING, RECORDING, OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF THIS COMPANY.

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.

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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

Table of Contents

REVISION HISTORYI

TERMINOLOGY II

1 INTRODUCTION..... 1

 1.1 PACKAGE CONTENTS 1

 1.2 PRODUCT SPECIFICATIONS 1

 1.3 PRODUCT FEATURES 2

 1.4 UPPER PANEL DESCRIPTION 3

 1.5 REAR PANEL DESCRIPTION..... 4

2 INSTALLATION 5

 2.1 HARDWARE INSTALLATION 5

 2.2 SOFTWARE INSTALLATION..... 5

3 SOFTWARE CONFIGURATION 6

 3.1 PREPARE YOUR PC TO CONFIGURE THE WLAN ACCESS POINT 6

 3.2 CONNECT TO THE WLAN ACCESS POINT 8

 3.3 MANAGEMENT AND CONFIGURATION ON THE WLAN ACCESS POINT 8

 3.3.1 Status..... 8

 3.3.2 Setup Wizard..... 9

 I LAN Interface Setup 10

 II Wireless Basic Settings..... 11

 III Wireless Security Setup 12

 3.3.3 Wireless - Basic Settings..... 12

 3.3.4 Wireless - Advanced Settings 14

 3.3.5 Wireless - Security Setup 15

 I WEP Key Setup 17

 3.3.6 Wireless - Access Control 18

 3.3.7 WDS Settings..... 20

 I WDS Security Setup 21

 II WDS AP Table 21

 3.3.8 Site Survey 22

 3.3.9 TCP/IP Settings..... 23

3.3.10 Log 25

3.3.11 Statistics 26

3.3.12 Upgrade Firmware 27

3.3.13 Save/ Reload Settings 27

3.3.14 Password Setup 28

3.3.15 Logout 29

4 FREQUENTLY ASKED QUESTIONS (FAQ)..... 30

4.1 WHAT AND HOW TO FIND MY PC’S IP AND MAC ADDRESS? 30

4.2 WHAT IS WIRELESS LAN? 30

4.3 WHAT ARE ISM BANDS? 30

4.4 HOW DOES WIRELESS NETWORKING WORK? 30

4.5 WHAT IS BSSID? 31

4.6 WHAT IS ESSID? 31

4.7 WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE? 32

4.8 WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS? 32

4.9 WHAT IS WEP? 32

4.10 WHAT IS FRAGMENT THRESHOLD? 32

4.11 WHAT IS RTS (REQUEST TO SEND) THRESHOLD? 33

4.12 WHAT IS BEACON INTERVAL? 33

4.13 WHAT IS PREAMBLE TYPE? 34

4.14 WHAT IS SSID BROADCAST? 34

4.15 WHAT IS WI-FI PROTECTED ACCESS (WPA)? 34

4.16 WHAT IS WPA2? 35

4.17 WHAT IS 802.1X AUTHENTICATION? 35

4.18 WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)? 35

4.19 WHAT IS ADVANCED ENCRYPTION STANDARD (AES)? 35

4.20 WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)? 35

4.21 WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)? 36

4.22 WHAT IS CLONE MAC ADDRESS? 36

Revision History

| DATE | REVISION OF USER'S MANUAL | FIRMWARE |
|-------------|----------------------------------|-----------------|
| 2006/5/19 | First release (Version 1.0) | a1.4.0 |

Terminology

| | |
|---------|--|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| AP | Access Point |
| CCK | Complementary Code Keying |
| CSMA/CA | Carrier Sense Multiple Access/ Collision Avoidance |
| CSMA/CD | Carrier Sense Multiple Access/ Collision Detection |
| DHCP | Dynamic Host Configuration Protocol |
| DSSS | Direct Sequence Spread Spectrum |
| EAP | Extensible Authentication Protocol |
| ESP | Encapsulating Security Payload |
| FCC | Federal Communications Commission |
| IEEE | Institute of Electrical and Electronic Engineers |
| IP | Internet Protocol |
| ISM | Industrial, Scientific and Medical |
| LAN | Local Area Network |
| MAC | Media Access Control |
| NT | Network Termination |
| PSD | Power Spectral Density |
| RF | Radio Frequency |
| SNR | Signal to Noise Ratio |
| SSID | Service Set Identification |
| TCP | Transmission Control Protocol |
| TFTP | Trivial File Transfer Protocol |
| TKIP | Temporal Key Integrity Protocol |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy |
| WLAN | Wireless Local Area Network |
| WPA | Wi-Fi Protected Access |

1 Introduction

The Wireless LAN Access Point is an affordable IEEE 802.11b/g wireless LAN Access Point solution; setting SOHO and enterprise standard for high performance, secure, manageable and reliable WLAN.

This document describes the steps required for the initial IP address assign and other WLAN router configuration. The description includes the implementation of the above steps.

1.1 Package contents

The package of the WLAN Access Point includes the following items,

- ✓ The WLAN Access Point
- ✓ The AC to DC power adapter
- ✓ The Documentation CD
- ✓ 1.8M RJ-45 Cable Line

1.2 Product Specifications

| | |
|-----------------------|---|
| Product Name | Wireless 802.11g Multi-mode AP |
| Standard | 802.11b/g(Wireless), 802.3(10BaseT), 802.3u(100BaseT) |
| Data Transfer Rate | 54Mbps(Wireless), 100Mbps(Ethernet) |
| Modulation Method | CCK(802.11b), OFDM(802.11g) |
| Frequency Band | 2.4GHz – 2.497GJz ISM Band, DSSS |
| RF Output Power | CCK< 17 dBm, OFDM< 13.5 dBm |
| Receiver Sensitivity | 802.11b -80 dBm@8%, 802.11g -68 dBm@5% |
| Operation Range | 30 to 280 meters (depend on surrounding) |
| Antenna | External Antenna |
| LED | Power, Active (WLAN/Ethernet) |
| Security | 64 bit/ 128 bit WEP, WPA, WPA2 |
| LAN interface | One 10/100BaseT with RJ45 connector |
| Power Consumption | 7.5V DC Power Adapter |
| Operating Temperature | 0 ~ 50°C ambient temperature |
| Storage Temperature | -20 ~ 70°C ambient temperature |
| Humidity | 5 to 90 % maximum (non-condensing) |
| Dimension | 118 x 75 x 25 mm |

1.3 Product Features

- Complies with IEEE 802.11b/g standard for 2.4GHz Wireless LAN.
- Supports AP/Client/WDS/AP+WDS modes on wireless interfaces.
- Supports 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Support Wi-Fi Protected Access Authentication with Radius and Pre-Shared Key mode.
- Supports Inter-Access Point Protocol (IAPP).
- Supports Wireless Distribution System (WDS).
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client auto IP address assignment from ISP.
- Supports clone MAC address function.
- Supports WEB based management and configuration.
- Supports Log table and remote Log service.
- Support Setup Wizard mode.

1.4 Upper Panel Description

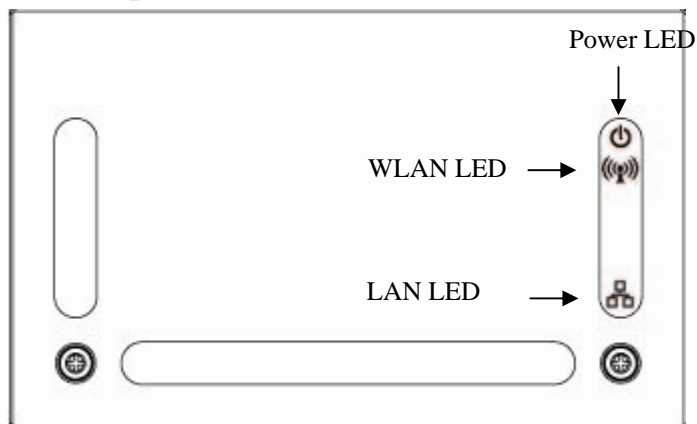


Figure 1 –WLAN Access Point Upper Panel

| LED Indicator | State | Description |
|-------------------|----------|---|
| 1. Power LED | On | The WLAN Access Point is powered on. |
| | Off | The WLAN Access Point is powered off. |
| 2. WLAN LED | Flashing | Data is transmitting or receiving on the antenna. |
| | Off | No data is transmitting or receiving on the antenna. |
| 3. LAN LED ACT | Flashing | Data is transmitting or receiving on the LAN interface. |
| | On | Port linked. |
| | Off | No link. |

1.5 Rear Panel Description

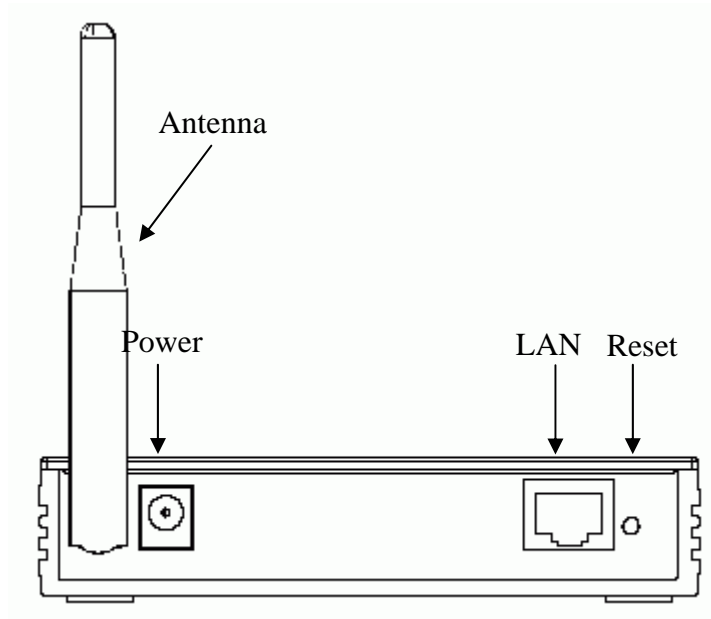


Figure 2 – WLAN Access Point Rear Panel

| Interfaces | Description |
|-----------------------------|---|
| 1. Antenna (Fixed / SMA) | The Wireless LAN Antenna. |
| 2. Power | The power jack allows an external DC +7.5 V power supply connection. The external AC to DC adaptor provide adaptive power requirement to the WLAN Access Point. |
| 3. LAN | The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively. |
| 4. Reset | Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults. |

2 Installation

2.1 Hardware Installation

Step 1: Place the Wireless LAN Access Point to the best optimum transmission location.

The best transmission location for your WLAN Access Point is usually at the geographic center of your wireless network, with line of sign to all of your mobile stations.

Step 2: Connect the WLAN Access Point to your wired network. Connect the Ethernet LAN interface of WLAN Access Point by category 5 Ethernet cable to your switch/ hub/ xDSL modem or cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the WLAN Access Point. Use only the AC/DC power adapter supplied with the WLAN Access Point; it may occur damage by using a different type of power adapter.

The hardware installation finished.

2.2 Software Installation

- There are no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 3 for software configuration.

Notice: It will take about 55 seconds to complete the boot up sequence after powered on the WLAN Access Point; Power LED will be active, and after that the WLAN Activity LED will be flashing to show the WLAN interface is enabled and working now.

3 Software configuration

There are web based management and configuration functions allowing you to have the jobs done easily.

The WLAN Access Point is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: **192.168.1.254**

Default IP subnet mask: **255.255.255.0**

WEB login User Name: *<empty>*

WEB login Password: *<empty>*

3.1 Prepare your PC to configure the WLAN Access Point

For OS of Microsoft Windows 95/ 98/ Me:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
Note: Windows Me users may not see the Network control panel. If so, *select View all Control Panel options* on the left side of the window
2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear.
3. Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
5. Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
7. Select *Specify an IP address* and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK and reboot your PC after completes the IP parameters setting.

For OS of Microsoft Windows 2000, XP:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control*

- Panel* window will appear.
2. Move mouse and double-click the right button on *Network and Dial-up Connections* icon. Move mouse and double-click the *Local Area Connection* icon. The *Local Area Connection* window will appear. Click *Properties* button in the *Local Area Connection* window.
 3. Check the installed list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
 4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
 5. Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
 6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
 7. Select *Specify an IP address* and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
 8. Click OK to completes the IP parameters setting.

For OS of Microsoft Windows NT:

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Move mouse and double-click the right button on *Network* icon. The *Network* window will appear. Click *Protocol* tab from the *Network* window.
3. Check the installed list of *Network Protocol* window. If TCP/IP is not installed, click the *Add* button to install it; otherwise go to step 6.
4. Select *Protocol* in the *Network Component Type* dialog box and click *Add* button.
5. Select *TCP/IP* in *Microsoft* of *Select Network Protocol* dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to *Network* dialog box after the TCP/IP installation.
6. Select *TCP/IP* and click the *properties* button on the *Network* dialog box.
7. Select *Specify an IP address* and type in values as following example.
 - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
 - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

3.2 Connect to the WLAN Access Point

Open a WEB browser, i.e. Microsoft Internet Explore, then enter 192.168.1.254 on the URL to connect the WLAN Access Point.

3.3 Management and configuration on the WLAN Access Point

3.3.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, and Ethernet LAN configuration information.

Access Point Status

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

| System | |
|---------------------------|-------------------|
| Uptime | 0day:2h:10m:34s |
| Firmware Version | a1.4.0 |
| Wireless Configuration | |
| Mode | AP |
| Band | 2.4 GHz (B+G) |
| SSID | MyWLAN |
| Channel Number | 11 |
| Encryption | Disabled |
| BSSID | 00:0e:8e:7d:3a:bf |
| Associated Clients | 8 |
| TCP/IP Configuration | |
| Attain IP Protocol | Fixed IP |
| IP Address | 192.168.1.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.254 |
| MAC Address | 00:0e:8e:7d:3a:bf |

Screen snapshot – Status

| Item | Description |
|------------------|--|
| System | |
| Uptime | It shows the duration since WLAN Access Point is powered on. |
| Firmware version | It shows the firmware version of WLAN Access Point. |

| Wireless configuration | |
|------------------------|--|
| Mode | It shows wireless operation mode |
| Band | It shows the current wireless operating frequency. |
| SSID | It shows the SSID of this WLAN Access Point. The SSID is the unique name of WLAN Access Point and shared among its service area, so all devices attempts to join the same wireless network can identify it. |
| Channel Number | It shows the wireless channel connected currently. |
| Encryption | It shows the status of encryption function. |
| Associated Clients | It shows the number of connected clients (or stations, PCs). |
| BSSID | It shows the BSSID address of the WLAN Access Point. BSSID is a six-byte address. |
| Associated Clients | It shows total numbers of WLAN clients connected, |
| TCP/IP Configuration | |
| Attain IP Protocol | It shows how the WLAN Access Point gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server. |
| IP Address | It shows the IP address of WAN interface of WLAN Access Point. |
| Subnet Mask | It shows the IP subnet mask of LAN interface of WLAN Access Point. |
| Default Gateway | It shows the default gateway setting for outgoing data packets. |
| MAC Address | It shows the MAC address of WLAN Access Point. |

3.3.2 Setup Wizard

This page guides you to configure wireless Access Point for first time

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Setup LAN Interface
2. Wireless LAN Setting
3. Wireless Security Setting

Next>>

Screen snapshot – Setup Wizard

I LAN Interface Setup

This page is used to configure local area network IP address and subnet mask

1. 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:

Subnet Mask:

Cancel

<<Back

Next>>

Screen snapshot – LAN Interface Setup

II Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone(Single Ethernet Client)

2. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band: 2.4 GHz (B+G) ▼

Mode: AP ▼

Network Type: Infrastructure ▼

SSID: MyWLAN

Channel Number: 11 ▼

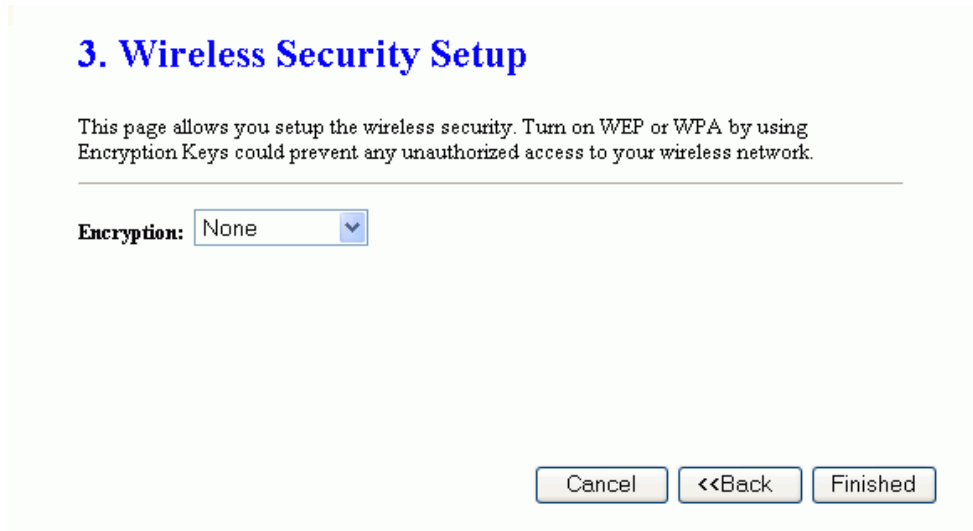
Enable Mac Clone (Single Ethernet Client)

Cancel <<Back Next>>

Screen snapshot – Wireless Basic Settings

III Wireless Security Setup

This page is used to configure wireless security



3. 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:

Cancel <<Back Finished

Screen snapshot – Wireless Security Setup

3.3.3 Wireless - Basic Settings

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

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.

Disable Wireless LAN Interface

Band:

Mode:

Network Type:

SSID:

Channel Number:

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

Screen snapshot – Wireless Basic Settings

| Item | Description |
|--------------------------------|---|
| Disable Wireless LAN Interface | Click on to disable the wireless LAN data transmission. |
| Band | Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(B+G) |
| Mode | Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode. |
| Site Survey | The Site Survey button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. Refer to 3.3.9 Site Survey . |
| SSID | It is the wireless network name. The SSID can be 32 bytes long. |
| Channel Number | Select the wireless communication channel from pull-down menu. |
| Associated Clients | Click the Show Active Clients button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet and transmission-rate for |

| | |
|---|---|
| | each associated wireless client. |
| Enable Mac Clone (Single Ethernet Client) | Take Laptop NIC MAC address as wireless client MAC address. [Client Mode only] |
| Enable Universal Repeater Mode | Click to enable Universal Repeater Mode |
| SSID of Extended Interface | Assign SSID when enables Universal Repeater Mode. |
| Apply Changes | Click the Apply Changes button to complete the new configuration setting. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

3.3.4 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 WLAN Access Point.

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: Open System Shared Key Auto

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

802.11g Protection: Enabled Disabled

RF Output Power: 100% 50% 25% 10% 5%

Turbo Mode: Auto Always Off

Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

Screen snapshot – Wireless Advanced Settings

| Item | Description |
|---------------------|---|
| Authentication Type | Click to select the authentication type in <i>Open System</i> , <i>Shared Key</i> or <i>Auto</i> selection. |
| Fragment Threshold | Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to 4.10 What is Fragment Threshold? |
| RTS Threshold | Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to 4.11 What is RTS(Request To Send) Threshold? |
| Beacon Interval | Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to 4.12 What is Beacon Interval? |
| Data Rate | Select the transmission data rate from pull-down menu. Data rate can be auto-select, 11M, 5.5M, 2M or 1Mbps. |
| Preamble Type | Click to select the <i>Long Preamble</i> or <i>Short Preamble</i> support on the wireless data packet transmission. Refer to 4.13 What is Preamble Type? |
| Broadcast SSID | Click to enable or disable the SSID broadcast function. Refer to 4.14 What is SSID Broadcast? |
| IAPP | Click to enable or disable the IAPP function. Refer to 4.20 What is Inter-Access Point Protocol(IAPP)? |
| 802.11g Protection | Protect 802.11b user. |
| RF Output Power | To adjust transmission power level. |
| Turbo Mode | Click to enable/disable turbo mode. (<i>Only apply to WLAN IC of Realtek</i>). |
| Apply Changes | Click the <i>Apply Changes</i> button to complete the new configuration setting. |
| Reset | Click the <i>Reset</i> button to abort change and recover the previous configuration setting. |

3.3.5 Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.

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: None Set WEP Key

Use 802.1x Authentication WEP 64bits WEP 128bits

WPA Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)

WPA Cipher Suite: TKIP AES

WPA2 Cipher Suite: TKIP AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

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

Apply Changes Reset

Screen snapshot – Wireless Security Setup

| Item | Description |
|---------------------------|--|
| Encryption | Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA(TKIP), WPA2 or WPA2 Mixed Refer to 4.9 What is WEP? 4.15 What is Wi-Fi Protected Access (WPA)? 4.16 What is WPA2(AES)? 4.17 What is 802.1X Authentication? 4.18 What is Temporal Key Integrity Protocol (TKIP)? 4.19 What is Advanced Encryption Standard (AES)? |
| Use 802.1x Authentication | While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function. Refer to 4.16 What is 802.1x Authentication? |
| WPA Authentication Mode | While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to 4.15 What is Wi-Fi Protected Access (WPA)? |
| WPA Cipher Suite | Enable TKIP or AES. Depends on which encryption you |

| | |
|------------------------------|--|
| | set. |
| WPA2 Cipher Suite | Enable TKIP or AES. Depends on which encryption you set. |
| Pre-Shared Key Format | While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only] |
| Pre-Shared Key | Fill in the key value. [WPA, Personal(Pre-Shared Key) only] |
| Enable Pre-Authentication | Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only] |
| Authentication RADIUS Server | Set the IP address, port and login password information of authentication RADIUS sever. |
| Apply Changes | Click the Apply Changes button to complete the new configuration setting. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

I WEP Key Setup

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, and select ASCII or Hex as the format of input value.

Key Length:

Key Format:

Default Tx Key:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

Screen snapshot – WEP Key Setup

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|------------------|---|
| Key Length | Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit). |
| Key Format | Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code. |
| Default Tx Key | Set the default secret key for WEP security function. Value can be chose between 1 and 4. |
| Encryption Key 1 | Secret key 1 of WEP security encryption function. |
| Encryption Key 2 | Secret key 2 of WEP security encryption function. |
| Encryption Key 3 | Secret key 3 of WEP security encryption function. |
| Encryption Key 4 | Secret key 4 of WEP security encryption function. |
| Apply Changes | Click the Apply Changes button to complete the new configuration setting. |
| Close | Click to close this WEP Key setup window. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

WEP encryption key (secret key) length:

| | Length | 64-bit | 128-bit |
|--------|--------|----------------------|----------------------|
| Format | | | |
| | ASCII | 5 characters | 13 characters |
| | HEX | 10 hexadecimal codes | 26 hexadecimal codes |

3.3.6 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.

Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Allow Listed ▼

MAC Address: Comment:

Apply Changes
Reset

Current Access Control List:

| MAC Address | Comment | Select |
|-------------------|---------|--------------------------|
| 00:02:72:81:86:01 | ST-1 | <input type="checkbox"/> |
| 00:00:55:66:66:50 | ST-2 | <input type="checkbox"/> |

Delete Selected
Delete All
Reset

Screen snapshot – Wireless Access Control

| Item | Description |
|------------------------------|--|
| Wireless Access Control Mode | Click the <i>Disabled</i> , <i>Allow Listed</i> or <i>Deny Listed</i> of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN Access Point. |
| MAC Address | Fill in the MAC address of client to register this WLAN Access Point access capability. |
| Comment | Fill in the comment tag for the registered client. |
| Apply Changes | Click the <i>Apply Changes</i> button to register the client to new configuration setting. |
| Reset | Click the <i>Reset</i> button to abort change and recover the previous configuration setting. |
| Current Access Control List | It shows the registered clients that are allowed to link to this WLAN Access Point. |
| Delete Selected | Click to delete the selected clients that will be access right removed from this WLAN Access Point. |
| Delete All | Click to delete all the registered clients from the access allowed list. |
| Reset | Click the <i>Reset</i> button to abort change and recover the |

previous configuration setting.

3.3.7 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 AP that you want to communicate with in the table and then enable the WDS.

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

Add WDS AP: MAC Address Comment

Current WDS AP List:

| MAC Address | Comment | Select |
|-------------------|---------|--------------------------|
| 00:02:72:81:86:0a | AP-1 | <input type="checkbox"/> |
| 00:02:72:81:86:0b | AP-2 | <input type="checkbox"/> |

Screen snapshot – WDS Setup

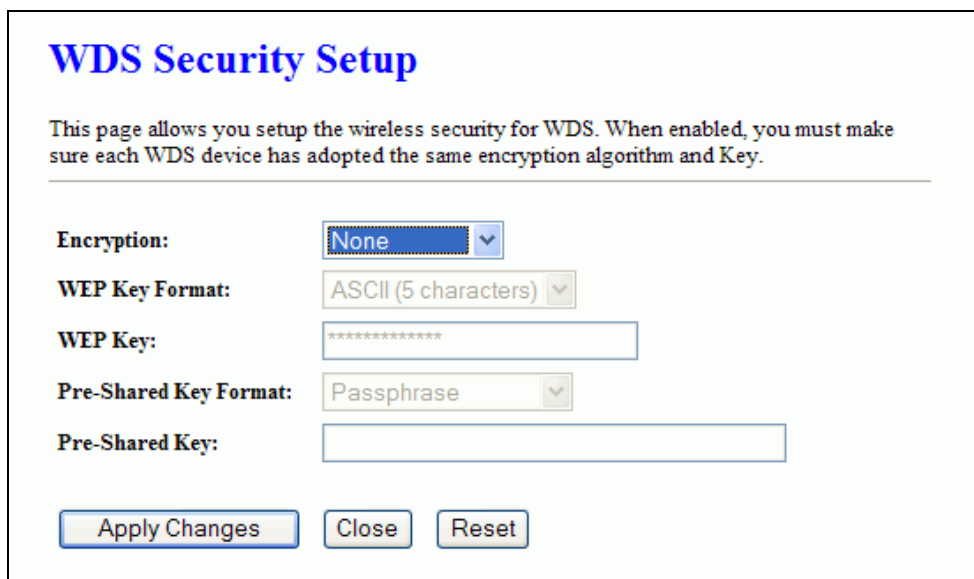
| Item | Description |
|---------------|---|
| Enable WDS | Click the check box to enable wireless distribution system. Refer to 4.21 What is Wireless Distribution System (WDS)? |
| MAC Address | Fill in the MAC address of AP to register the wireless distribution system access capability. |
| Comment | Fill in the comment tag for the registered AP. |
| Apply Changes | Click the Apply Changes button to register the AP to new configuration setting. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |
| Set Security | Click button to configure wireless security like |

| | |
|-----------------|--|
| | WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES) or None |
| Show Statistics | It shows the TX, RX packets, rate statistics |
| Delete Selected | Click to delete the selected clients that will be removed from the wireless distribution system. |
| Delete All | Click to delete all the registered APs from the wireless distribution system allowed list. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

I WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs. Refer to [3.3.6 Wireless Security Setup](#).



Screen snapshot – WDS Security Setup

II WDS AP Table

This page is used to show WDS statistics

WDS AP Table

This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.

| MAC Address | Tx Packets | Tx Errors | Rx Packets | Tx Rate (Mbps) |
|-------------------|------------|-----------|------------|----------------|
| 00:02:72:81:86:0a | 22 | 0 | 0 | 1 |
| 00:02:72:81:86:0b | 22 | 14 | 0 | 1 |

Refresh Close

Screen snapshot – WDS AP Table

| Item | Description |
|----------------|---|
| MAC Address | It shows the MAC Address within WDS. |
| Tx Packets | It shows the statistic count of sent packets on the wireless LAN interface. |
| Tx Errors | It shows the statistic count of error sent packets on the Wireless LAN interface. |
| Rx Packets | It shows the statistic count of received packets on the wireless LAN interface. |
| Tx Rare (Mbps) | It shows the wireless link rate within WDS. |
| Refresh | Click to refresh the statistic counters on the screen. |
| Close | Click to close the current window. |

3.3.8 Site Survey

This page is used to view or configure other APs near yours.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|----------------|-------------------|----------|--------|---------|--------|-----------------------|
| MyWLAN | 00:02:72:00:81:86 | 11 (B+G) | AP | no | 90 | <input type="radio"/> |
| linux-wlan | 00:02:72:f1:02:ad | 6 (B) | AP | no | 76 | <input type="radio"/> |
| RTL8186-VPN-GW | 00:e0:4c:81:86:23 | 11 (B+G) | AP | no | 66 | <input type="radio"/> |
| Sales | 00:02:72:04:68:92 | 11 (B) | AP | yes | 53 | <input type="radio"/> |
| Tekomn_Office | 00:02:72:00:93:fb | 9 (B) | AP | yes | 35 | <input type="radio"/> |
| alex | d6:4c:fc:0d:2a:d4 | 1 (B) | Ad hoc | no | 32 | <input type="radio"/> |
| MyWLAN | 00:02:72:85:15:99 | 11 (B+G) | AP | no | 32 | <input type="radio"/> |

Screen snapshot – Wireless Site Survey

| Item | Description |
|---------|---|
| SSID | It shows the SSID of AP. |
| BSSID | It shows BSSID of AP. |
| Channel | It show the current channel of AP occupied. |
| Type | It show which type AP acts. |
| Encrypt | It shows the encryption status. |
| Signal | It shows the power level of current AP. |
| Select | Click to select AP or client you'd like to connect. |
| Refresh | Click the Refresh button to re-scan site survey on the screen. |
| Connect | Click the Connect button to establish connection. |

3.3.9 TCP/IP Settings

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

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:
Subnet Mask:
Default Gateway:
DHCP: ▼
DHCP Client Range: -
DNS Server:
Domain Name:
802.1d Spanning Tree: ▼
Clone MAC Address:

Screen snapshot – LAN Interface Setup

| Item | Description |
|-------------------|--|
| IP Address | Fill in the IP address of LAN interfaces of this WLAN Access Point. |
| Subnet Mask | Fill in the subnet mask of LAN interfaces of this WLAN Access Point. |
| Default Gateway | Fill in the default gateway for LAN interfaces out going data packets. |
| DHCP | Click to select <i>Disabled</i> , <i>Client</i> or <i>Server</i> in different operation mode of wireless Access Point. |
| DHCP Client Range | Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range. |
| Show Client | Click to open the <i>Active DHCP Client Table</i> window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only] |
| DNS Server | Manual setup DNS server IP address. |

| | |
|----------------------|--|
| Domain Name | Assign Domain Name and dispatch to DHCP clients. It is optional field. |
| 802.1d Spanning Tree | Select to enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu. |
| Clone MAC Address | Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address? |
| Apply Changes | Click the Apply Changes button to complete the new configuration setting. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

3.3.10 Log

This page is used to configure the remote log server and shown the current log.

System Log

This page can be used to set remote log server and show the system log.

Enable Log
 system all *wireless*
 Enable Remote Log **Log Server IP Address:**

```

Oday 03:43:58 wlan0: A wireless client is associated - 00:90:4B:0A:AA:C8
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A expired STA is resumed - 00:04:23:69:A0:3B
Oday 03:43:58 wlan0: A wireless client is associated - 00:E0:4C:81:87:05
Oday 03:43:58 wlan0: A STA is expired - 00:E0:4C:81:87:05
Oday 03:43:58 wlan0: A expired STA is resumed - 00:E0:4C:81:87:05
    
```

Screen snapshot – Log

| Item | Description |
|----------------------|--|
| Enable Log | Click the checkbox to enable log. |
| <i>System all</i> | Show all log of wireless Access Point. |
| <i>Wireless only</i> | Only show wireless log. |

| | |
|------------------------------|---|
| Enable Remote Log | Click the checkbox to enable remote log service. |
| Log Server IP Address | Input the remote log IP address |
| Apply Changes | Click the Apply Changes button to save above settings. |
| Refresh | Click the refresh the log shown on the screen. |
| Clear | Clear log display screen |

3.3.11 Statistics

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

Statistics

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

| | | |
|---------------------|-------------------------|-------|
| Wireless LAN | <i>Sent Packets</i> | 490 |
| | <i>Received Packets</i> | 40434 |
| Ethernet LAN | <i>Sent Packets</i> | 2551 |
| | <i>Received Packets</i> | 5418 |

Screen snapshot – Statistics

| Item | Description |
|--|---|
| Wireless LAN <i>Sent Packets</i> | It shows the statistic count of sent packets on the wireless LAN interface. |
| Wireless LAN <i>Received Packets</i> | It shows the statistic count of received packets on the wireless LAN interface. |
| Ethernet LAN <i>Sent Packets</i> | It shows the statistic count of sent packets on the Ethernet LAN interface. |
| Ethernet LAN <i>Received Packets</i> | It shows the statistic count of received packets on the Ethernet LAN interface. |
| Refresh | Click the refresh the statistic counters on the screen. |

3.3.12 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.

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:

Screen snapshot – Management - Upgrade Firmware

| Item | Description |
|-------------|--|
| Select File | Click the Browse button to select the new version of web firmware image file. |
| Upload | Click the Upload button to update the selected web firmware image to the WLAN Access Point. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

3.3.13 Save/ Reload Settings

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

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:

Load Settings from File:

Reset Settings to Default:

Screen snapshot – Management - Save/Reload Settings

| Item | Description |
|---------------------------|---|
| Save Settings to File | Click the Save button to download the configuration parameters to your personal computer. |
| Load Settings from File | Click the Browse button to select the configuration files then click the Upload button to update the selected configuration to the WLAN Access Point. |
| Reset Settings to Default | Click the Reset button to reset the configuration parameter to factory defaults. |

3.3.14 Password Setup

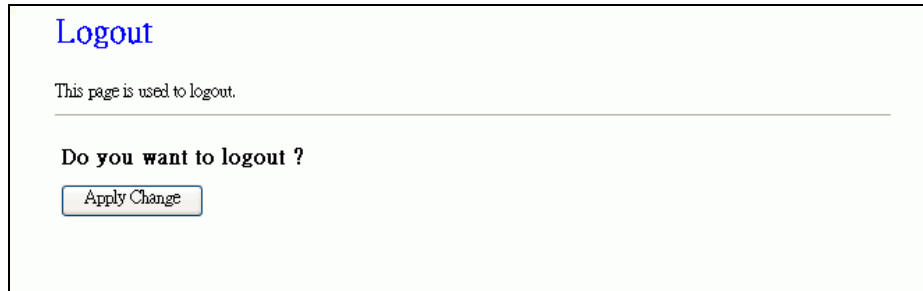
This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Screen snapshot – Management - Password Setup

| Item | Description |
|--------------------|--|
| User Name | Fill in the user name for web management login control. |
| New Password | Fill in the password for web management login control. |
| Confirmed Password | Because the password input is invisible, so please fill in the password again for confirmation purpose. |
| Apply Changes | Clear the User Name and Password fields to empty, means to apply no web management login control. Click the Apply Changes button to complete the new configuration setting. |
| Reset | Click the Reset button to abort change and recover the previous configuration setting. |

3.3.15 Logout

This page is used to logout web management page. This item will be activated next time you login after you define user account and password.



The screenshot shows a web page titled "Logout" in blue text. Below the title, it says "This page is used to logout." followed by a horizontal line. Underneath the line, the text "Do you want to logout ?" is displayed. At the bottom of the page, there is a button labeled "Apply Change".

Screen snapshot – Logout



The screenshot shows a dialog box with the text "Change setting successfully!" at the top. Below the text, there is a button labeled "OK".

Screen snapshot – Logout - OK

| Item | Description |
|--------------|--|
| Apply Change | Click the <i>Apply Change</i> button, Then click <i>OK</i> button to logout. |

4 Frequently Asked Questions (FAQ)

4.1 What and how to find my PC's IP and MAC address?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- ✓ Open the Command program in the Microsoft Windows.
 - ✓ Type in *ipconfig /all* then press the *Enter* button.
- Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

4.2 What is Wireless LAN?

A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

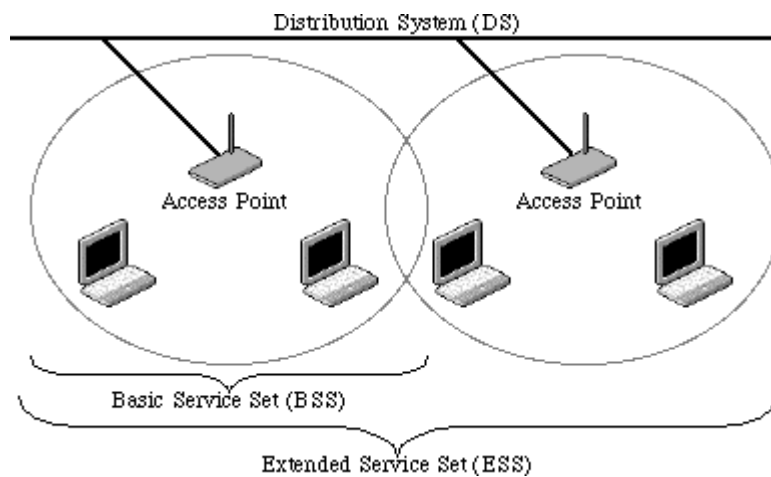
4.3 What are ISM bands?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

4.4 How does wireless networking work?

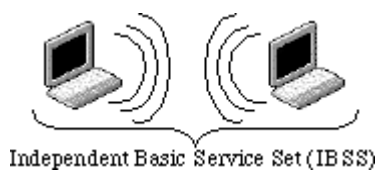
The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access

to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

4.5 What is BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

4.6 What is ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

4.7 What are potential factors that may causes interference?

Factors of interference:

- Obstacles: walls, ceilings, furniture... etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- ✓ Minimizing the number of walls and ceilings.
- ✓ Position the WLAN antenna for best reception.
- ✓ Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, ... etc.
- ✓ Add additional WLAN Access Points if necessary.

4.8 What are the Open System and Shared Key authentications?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

4.9 What is WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

4.10 What is Fragment Threshold?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several

fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

4.11 What is RTS (Request To Send) Threshold?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

4.12 What is Beacon Interval?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling

stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

4.13 What is Preamble Type?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

4.14 What is SSID Broadcast?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

4.15 What is Wi-Fi Protected Access (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an

authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

4.16 What is WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

4.17 What is 802.1x Authentication?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

4.18 What is Temporal Key Integrity Protocol (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

4.19 What is Advanced Encryption Standard (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

4.20 What is Inter-Access Point Protocol (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

4.21 What is Wireless Distribution System (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

4.22 What is Clone MAC Address?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.

Since that all the clients will communicate outside world through the WLAN Access Point, so have the cloned MAC address set on the WLAN Access Point will solve the issue.