

Wireless LAN Device Series

Multi-Mode AP

AP-G250 User's Manual

Version. 1.4.3b (2007.09.14)

TABLE OF CONTENTS

NOTICE	3
PREFACE	5
CH 1. AP-G250 INSTALLATION	6
PACKING LIST	6
BACK PANEL CONNECTIONS	6
HARDWARE INSTALLATION	7
CH 2. FIRST TIME CONFIGURATION	7
BEFORE START TO CONFIGURE	7
KNOWING THE NETWORK APPLICATION	8
BASIC SETTINGS	28
ADVANCED SETTINGS	31
CONFIGURING WIRELESS SECURITY	34
CONFIGURING AS WLAN CLIENT ADAPTER	37
QUICK START TO CONFIGURE	37
MAC CLONE FOR SINGLE ETHERNET CLIENT	39
EXTEND THE REMOTE AP (BSS).....	40
CH 3. CONFIGURING WDS	42
WDS NETWORK TOPOLOGY	42
WDS APPLICATION.....	44
CH 4. ADVANCED CONFIGURATIONS	46
CONFIGURING LAN TO WAN FIREWALL	46
PORT FILTERING	46
IP FILTERING	47
MAC FILTERING.....	48
NAT (NETWORK ADDRESS TRANSLATION).....	49
CONFIGURING PORT FORWARDING (VIRTUAL SERVER).....	50
MULTIPLE SERVERS BEHIND NAT EXAMPLE:	50
CONFIGURING DMZ	51
CONFIGURING VPN	52
CONFIGURING WAN INTERFACE.....	54
STATIC IP.....	54
DHCP CLIENT (DYNAMIC IP).....	55
PPPoE.....	56
PPTP	57
CONFIGURING CLONE MAC ADDRESS	59

CONFIGURING DHCP SERVER	61
BANDWIDTH CONTROL.....	62
QoS (QUALITY OF SERVICE).....	62
STATIC ROUTE SETUP	66
DYNAMIC ROUTE SETUP	67
VPN PASS-THROUGH.....	68
USING CLI MENU.....	68
THE SYSTEM MANAGEMENT	70
SNMP AGENT	70
MISCELLANEOUS SETTINGS.....	73
PING WATCHDOG	74
AIMING TOOL	75
CONNECTING PROFILE.....	76
CONFIGURATION DATA BACKUP & RESTORE	77
AUTO DISCOVERY TOOL.....	78

Notice

FCC Warning

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the 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.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC 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 or more 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 RF 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. For product available in the USA/Canada market, only channel 1~11 can be operated.

Selection of other channels is not possible. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Shielded interface cables must be used in order to comply with emission limits.

CE Statement

Hereby, ZINWELL, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

This device will be sold in the following EEA countries : Austria, Italy, Belgium, Liechtenstein, Denmark, Luxembourg, Finland, Netherlands, France, Norway, Germany, Portugal, Greece, Spain, Iceland, Sweden, Ireland, United Kingdom, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Slovakia, Poland, Slovenia, Bulgaria, Romania.

Preface

This guide is for the networking professional who installs and manages the Zinwell AP-G250 product hereafter referred to as the “device”. To use this guide, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of wireless local area networks.

Ch 1. AP-G250 Installation

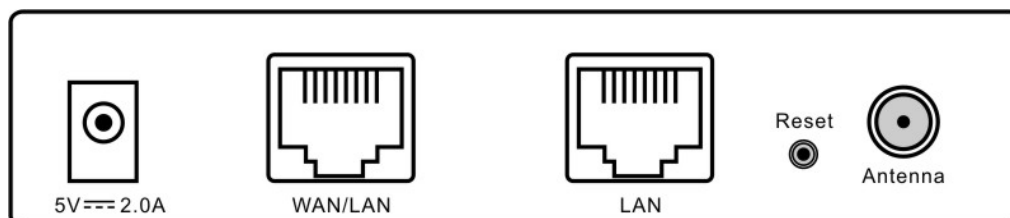
Packing List

Before you start to install the device, make sure the package contains the following items :

- AP-G250 Multi-Mode AP unit * 1
- Power Adapter * 1
- RJ-45 Cable * 1



Back panel connections



From Left to Right:

DC jack: ZW-220 can use power source in DC jack. Please supply the power in 5V and 2A

WAN/LAN: This port could be WAN or LAN port depending on the

configuration. It will be WAN port in router mode and LAN port in bridge mode.

LAN: This port is always LAN in ZW-220. In Bridge mode, it bridges to WLAN and “WAN/LAN” port. In Router mode, it bridges to WLAN only, In WISP mode, it bridges to “WAN/LAN” port only.

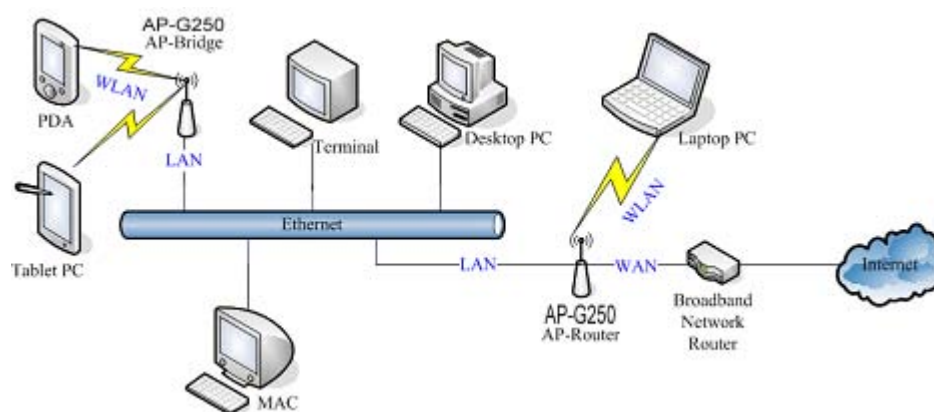
Reset: Press Reset button to revert it to factory default.

Antenna: This SMA Reverse allows the user to connect antenna or RF cable. At least connect an antenna to help ZW-220 to send and receive RF signal.

ZW-220 integrates LNA/PA (Low Noise Amplifier) module and has at least 3dB RF sensitivity better than the regular WLAN products.

Hardware Installation

Once you check off everything from the package, you can start to install the device. You can use the wall mount hole on the bottom of the device to mount the device on the wall, or just put the device on the desktop. The administrator can refer to the figure below while constructing your WLAN environment.



Ch 2. First Time Configuration

Before Start to Configure

There are two ways to configure the device, one is through web-browser, and the other is through Secure Shell CLI interface. To access the configuration interfaces, make sure you are using a computer connected to

the same network as the device. The default IP address of the device is 192.168.2.254, and the subnet-mask is 255.255.255.0.

The device has three operation modes (Router/Bridge/WISP). In bridge mode, also known as AP Client, you can access the device by WLAN (Wireless Local Area Network) and both wired LAN ports. And in router/WISP modes, the device can be accessed by WLAN, LAN and WAN. The default IP addresses for the device are 192.168.2.254 (for LAN), 172.1.1.1(for WAN), so you need to make sure the IP address of your PC is in the same subnet as the device, such as 192.168.2.X (for LAN), 172.1.1.X (for WAN).

Please note that the DHCP server inside the device is default to up and running. Do not have multiple DHCP servers in your network environment, otherwise it will cause abnormal situation.

We also provide an auto-discovery tool which is for finding out the IP of the device. In case, you've forgot the IP of the device or the IP of the device has been changed, you can use the tool to find out the IP of the device even your PC is not in the same subnet as the device is.

Knowing the Network Application

The device can act as the following roles, and it supports WDS (Wireless Distribution System) function.

- Access Point
- WDS mode
- Bridge/Router
- WISP
- AP Client

The device provides 3 different operation modes and the wireless radio of device can act as AP/Client/WDS. The operation mode is about the communication mechanism between the wired Ethernet NIC and wireless NIC, the following is the types of operation mode.

Router

The wired Ethernet (WAN) port is used to connect with ADSL/Cable modem and the wireless NIC is used for your private WLAN. The other wired Ethernet (LAN) port bridges to the private WLAN. The NAT is existed

between WAN and WLAN/LAN and all the wireless and wired clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is static IP. You can access the web server of device through the default WAN IP address 172.1.1.1 and modify the setting base on your ISP requirement.

Bridge

The two wired Ethernet ports and wireless NIC are bridged together. Once the mode is selected, all the WAN related functions will be disabled.

WISP (Wireless ISP)

This mode can let you access the AP of your wireless ISP and share the same public IP address from your ISP to the PCs connecting with both the wired Ethernet ports of the device. To use this mode, first you must set the wireless radio to be client mode connecting to the AP of your ISP as the WAN connection and then you can configure the WAN IP configuration to meet your ISP requirement.

The wireless radio of the device acts as the following roles.

AP (Access Point)

The wireless radio of device serves as communications “hub” for wireless clients and provides a connection to a wired LAN.

AP Client

This mode provides the capability to connect with the other AP using infrastructure/Ad-hoc networking types. With bridge operation mode, you can directly connect one of the wired Ethernet port to your PC and the device becomes a wireless adapter. And with WISP operation mode, you can connect one of the wired Ethernet port to a hub/switch and all the PCs connecting with hub/switch can share the same public IP address from your ISP.

WDS (Wireless Distribution System)

This mode combines up to 8 AP to a single wireless network; the device forwards the packets to another AP with WDS function. When this mode is selected, all the wireless clients can't survey and connect to the device. The device only allows the WDS connection.

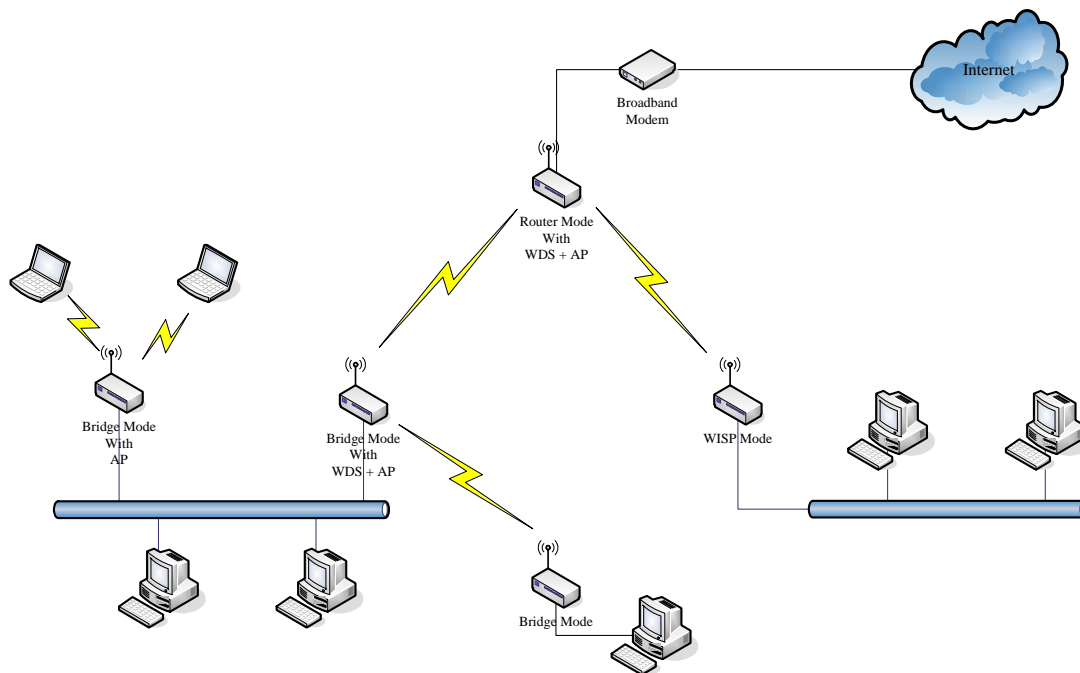
WDS+AP

This mode combines WDS plus AP modes, it not only allows WDS connections but also the wireless clients can survey and connect to the device.

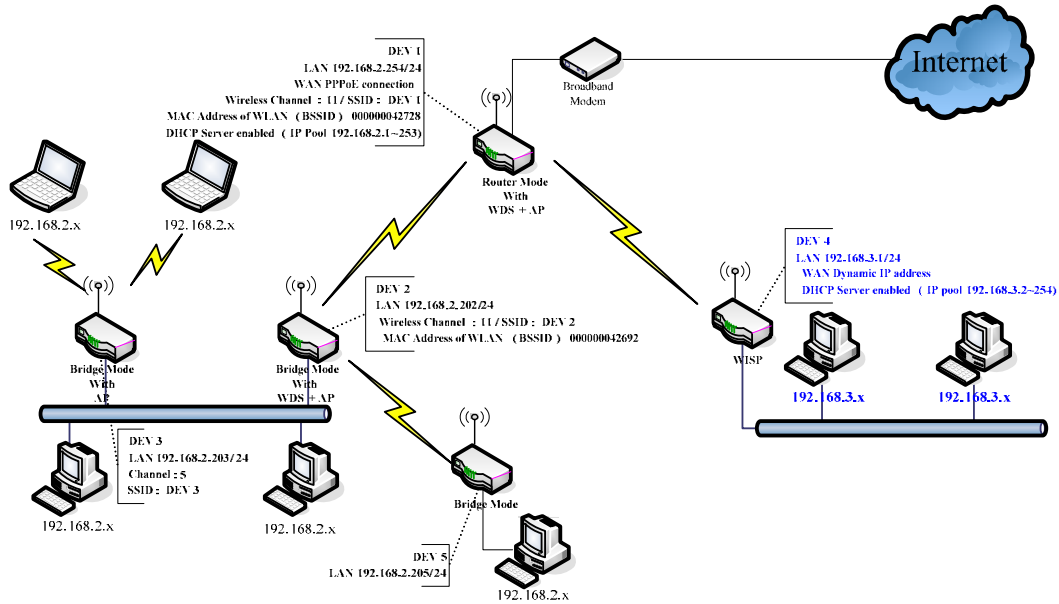
The following table shows the supporting combination of operation and wireless radio modes.

	<i>Bridge</i>	<i>Router</i>	<i>WISP</i>
AP	V	V	X
WDS	V	V	X
Client	V	X	V
AP+WDS	V	V	X

Hereafter are some topologies of network application for your reference.



Examples of Configuration



This example demonstrates how to set up a network with different device configurations. There are 2 DHCP servers (DEV1/DEV4) in the network to control the IP configuration of 2 domains (192.168.2.x/192.168.3.x). Once the setting is done, all the PCs can visit Internet through DEV1.

We assume all the devices keep the factory default setting. To make sure that user can continuing press the rest button for more than 5 seconds to restore the factory default setting.

The following descriptions show the steps to configure DEV1 to DEV5.

Configure DEV1:

1. Connect the ADSL modem to Ethernet port of device using Ethernet cable.
2. Access the web server (<http://192.168.2.254>) of device from the wireless station.
3. Use Wizard page to setup device.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

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 Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

4. Press “Next>>” button then set the “Operation Mode” to “Router” mode.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or Static IP. 172.1.1.1 is the default Static IP address for WAN port
- Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or Static IP.

Cancel <<Back Next>>

5. Press “Next>>” button then disable “Time Zone” function.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

NTP server : 192.5.41.41 - North America

Cancel <<Back Next>>

6. Press “Next>>” button then set the IP address of LAN interface.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.

IP Address: 192.168.2.254

Subnet Mask: 255.255.255.0

Cancel <<Back Next>>

7. Press “Next>>” button then select the “PPPoE” for “WAN Access Type” and fill in the “User Name” and “Password” fields.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name: 87043609@hinet.net

Password: ●●●●●●●●

Cancel <<Back Next>>

- Press “Next>>” button then select the “AP+WDS” for “mode” and change the SSID to “DEV1”.

- Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

- Wait for refreshing web page.

- Use “WDS Settings” page to configure WDS.

12. Enable WDS function and add the BSSID of DEV2 to “Current WDS AP List”.

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
00:00:00:04:26:92	DEV2	<input type="checkbox"/>

13. Since we access the device by wireless connection, it may temporarily disconnect when applying the WDS setting. After re-connecting to the device, use the “Status” page to check the settings.

System

Uptime 0day:0h:20m:6s

Free Memory 10776 kB

Firmware Version 1.4.0c 20060914

Webpage Version 1.4.0c 20060914

Wireless Configuration

Mode AP+WDS - Router

Band 2.4 GHz (B+G)

SSID DEV1

Channel Number 11

Encryption Disabled(AP), Disabled(WDS)

BSSID 00:00:00:04:27:28

Associated Clients 0

Power(OFDm/G) 100mW

Power(CCK/B) 250mW

TCP/IP Configuration

Attain IP Protocol Fixed IP

IP Address 192.168.2.254

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.254

DHCP Server Enabled

MAC Address 00:00:00:04:27:28

WAN Configuration

Attain IP Protocol PPPoE Connected

IP Address 218.168.146.93

Subnet Mask 255.255.255.0

Default Gateway 218.168.146.254

MAC Address 00:00:00:04:27:29

Configure DEV2:

1. Access the web server (<http://192.168.2.254>) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp -d” then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

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 Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Next>>

3. Press “Next>>” button then set the “Operation Mode” to “Bridge” mode.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP. 172.1.1.1 is the default Static IP address for WAN port
- Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. You must set the wireless to client mode and connect to the ISP AP. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP.

Cancel <<Back Next>>

4. Press “Next>>” button then disable “Time Zone” function.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada);Tijuana

NTP server : 192.541.41 - North America

Cancel <<Back Next>>

5. Press “Next>>” button then set the IP address of LAN interface.

The screenshot shows the '3. LAN Interface Setup' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '3. LAN Interface Setup' and a descriptive paragraph: 'This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.' Below this are two input fields: 'IP Address:' with the value '192.168.2.202' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

6. Press “Next>>” button then select the “AP+WDS” for “mode” and change the SSID to “DEV2”.

The screenshot shows the '5. Wireless Basic Settings' page. The 'Site contents' sidebar is identical to the previous page. The main content area has a title '5. Wireless Basic Settings' and a descriptive paragraph: 'This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.' Below this are several configuration fields: 'Band:' set to '2.4 GHz (B+G)', 'Mode:' set to 'AP+WDS', 'Network Type:' set to 'Infrastructure', and 'SSID:' set to 'DEV2'. There is also a 'Channel Number:' field set to '11' and an unchecked checkbox labeled 'Enable Mac Clone (Single Ethernet Client)'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

7. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

The screenshot shows the '6. Wireless Security Setup' page. The 'Site contents' sidebar is identical to the previous pages. The main content area has a title '6. Wireless Security Setup' and a descriptive paragraph: '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.' Below this is an 'Encryption:' dropdown menu set to 'None'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Finished'.

8. Wait for refreshing web page.

The screenshot shows a confirmation page. The 'Site contents' sidebar is identical to the previous pages. The main content area has a title 'Change setting successfully!' followed by the text: 'Please wait a while for refreshing webpage.' and 'If IP address was modified, you have to re-connect the WebServer with the new address.'

- Access the web server by new IP address "192.168.2.202" then use "LAN Interface" page to disable DHCP Server.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address:
Subnet Mask:
Default Gateway:
DHCP:
DHCP Client Range: -
802.1d Spanning Tree:
Clone MAC Address:
MTU Size:

- Wait for refreshing web page.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

- Use "WDS Settings" page to configure WDS.

Site contents:

- Wizard
- Operation Mode
- Wireless
 - Basic Settings
 - Advanced Settings
 - Security
 - Access Control
 - WDS settings
 - Site Survey
 - Connecting Profile
- TCP/IP
- Firewall
- Management
- Reboot

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
<input type="text"/>	<input type="text"/>

Current WDS AP List:

MAC Address	Comment	Select
<input type="text"/>	<input type="text"/>	<input type="button" value="Delete Selected"/>

12. Enable WDS function and add the BSSID of DEV1 to “Current WDS AP List”.

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
00:00:00:04:27:28	DEV1	<input type="checkbox"/>

13. Use the “Status” page to check the settings.

System

Uptime	0day:0h:39m:6s
Free Memory	10992 kB
Firmware Version	1.4.0c 20060914
Webpage Version	1.4.0c 20060914

Wireless Configuration

Mode	AP+WDS - Bridge
Band	2.4 GHz (B+G)
SSID	DEV2
Channel Number	11
Encryption	Disabled(AP), Disabled(WDS)
BSSID	00:00:00:04:26:92
Associated Clients	0
Power(OFDM/G)	100mW
Power(CCK/B)	250mW

TCP/IP Configuration

Attain IP Protocol	Fixed IP
IP Address	192.168.2.202
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:00:00:04:26:92

Configure DEV3:

1. Access the web server (http://192.168.2.254) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you not able to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp -d” then you can access the web server of device using the default IP address.

2. Use “LAN Interface” page to set the IP address of LAN interface and disable DHCP server.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
 - Route
- Firewall
- Management
- Reboot

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address:

Subnet Mask:

Default Gateway:

DHCP:

DHCP Client Range: -

802.1d Spanning Tree:

Clone MAC Address:

MTU Size:

3. Wait for refreshing web page.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
 - Route
- Firewall
- Management
- Reboot

Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

- Access the web server by new IP address “192.168.2.203” then use “Basic Settings” page to change SSID and CHANNEL.

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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: DEV3

Channel Number: 5 Show Active Clients

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode

Extended SSID:

(once selected and applied, extended SSID and channel number will be updated)

SSID	BSSID	Channel	Type	Encrypt	RSSI	Quality
Refresh						

Apply Changes Reset

- Use the “Status” page to check the settings.

System

Uptime	0day, 2h, 33m, 18s
Free Memory	11352 KB
Firmware Version	1.4.0c.20060914
Webpage Version	1.4.0c.20060914

Wireless Configuration

Mode	AP - Bridge
Band	2.4 GHz (B+G)
SSID	AP-G250
Channel Number	11
Encryption	Disabled
BSSID	00:00:00:04:28:29
Associated Clients	0
Power(OFDM/G)	100mW
Power(CCK/B)	250mW

TCP/IP Configuration

Attain IP Protocol	Fixed IP
IP Address	192.168.2.203
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:00:00:04:28:29

Configure DEV4:

1. Access the web server (<http://192.168.2.254>) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp -d” then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

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 Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Next>>

3. Press “Next>>” button then set the “Operation Mode” to “Wireless ISP” mode.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Router: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP. 172.1.1.1 is the default Static IP address for WAN port

Bridge: In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Wireless ISP: In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. **You must set the wireless to client mode and connect to the ISP AP.** The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP.

Cancel <<Back Next>>

4. Press “Next>>” button then disable “Time Zone” function.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

NTP server : 192.5.41.41 - North America

Cancel <<Back Next>>

5. Press “Next>>” button then set the IP address of LAN interface.

The screenshot shows the '3. LAN Interface Setup' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '3. LAN Interface Setup' and a description: 'This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.' Below the description are two input fields: 'IP Address:' with the value '192.168.3.1' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

6. Press “Next>>” button then select the “DHCP Client” for “WAN Access Type”.

The screenshot shows the '4. WAN Interface Setup' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '4. WAN Interface Setup' and a description: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.' Below the description is a dropdown menu for 'WAN Access Type:' with 'DHCP Client' selected. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

7. Press “Next>>” button then select the “Client” for “mode” and change the SSID to “DEV4”.

The screenshot shows the '5. Wireless Basic Settings' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '5. Wireless Basic Settings' and a description: 'This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.' Below the description are several fields: 'Band:' with a dropdown set to '2.4 GHz (B+G)', 'Mode:' with a dropdown set to 'Client', 'Network Type:' with a dropdown set to 'Infrastructure', 'SSID:' with a text box containing 'DEV4', and 'Channel Number:' with a dropdown set to '11'. There is also an unchecked checkbox labeled 'Enable Mac Clone (Single Ethernet Client)'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

8. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

The screenshot shows the '6. Wireless Security Setup' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '6. Wireless Security Setup' and a description: '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.' Below the description is a dropdown menu for 'Encryption:' with 'None' selected. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Finished'.

9. Wait for refreshing web page.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

10. Change the IP address of your PC to 192.168.3.x then access the web server by the new IP address “192.168.3.1” and use “Status” page check the setting.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
 - Status
 - QoS
 - Bandwidth Control
 - SNMP
 - Statistics
 - DDNS
 - Time Zone
 - Log
 - Miscellaneous
 - Upgrade Firmware
 - Save/Reload Setting
 - Password
 - Reboot

System

- Uptime: 0day:2h:56m:36s
- Free Memory: 10896 kB
- Firmware Version: 1.4.0c 20060914
- Webpage Version: 1.4.0c 20060914

Wireless Configuration

- Mode: Infrastructure Client - Router
- Band: 2.4 GHz (B+G)
- SSID: DEV4
- Channel Number: 5
- Encryption: Disabled
- BSSID: 00:00:00:00:00:00
- State: Scanning
- RSSI: 0

TCP/IP Configuration

- Attain IP Protocol: Fixed IP
- IP Address: 192.168.3.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.3.1
- DHCP Server: Enabled
- MAC Address: 00:00:00:05:12:13

WAN Configuration

- Attain IP Protocol: Getting IP from DHCP server...
- IP Address: 0.0.0.0
- Subnet Mask: 0.0.0.0
- Default Gateway: 0.0.0.0
- MAC Address: 00:00:00:05:12:14

11. If the “State” of “Wireless Configuration” is not “Connected” or you want to refresh the “RSSI”, please use “Site Survey” page to re-connect a AP.

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	Rate	RSSI	Quality	Select	Auto
DEV4	00:00:00:04:27:28	11 (B+G)	AP	no	67 (-49 dbm)	96	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	00:02:14:00:80:18	1 (B+G)	AP	no	61 (-53 dbm)	85	<input type="checkbox"/>	<input type="checkbox"/>
AIR802	00:05:9e:0046:69	11 (B)	AP	no	40 (-70 dbm)	90	<input type="checkbox"/>	<input type="checkbox"/>
AIR802-1F	00:05:9e:0060:ed	1 (B+G)	AP	yes	36 (-68 dbm)	92	<input type="checkbox"/>	<input type="checkbox"/>
AIR802-2F	00:05:9e:0060:3d	11 (B+G)	AP	yes	29 (-72 dbm)	85	<input type="checkbox"/>	<input type="checkbox"/>
RTL8185-Default	00:00:00:aa:bb:00	7 (B+G)	AP	no	24 (-75 dbm)	68	<input type="checkbox"/>	<input type="checkbox"/>
Auto...	00:05:9e:11:19:67	6 (B+G)	AP	no	12 (-82 dbm)	34	<input type="checkbox"/>	<input type="checkbox"/>

Refresh Auto Refresh **Connect** Auto

Configure DEV5:

1. Access the web server (<http://192.168.2.254>) of device from the Ethernet port.

Caution

If you configure multiple devices in the same PC, since the devices have the same default IP address but different MAC addresses, it may cause you unable to access the web server of device. If the situation happens, please try to clean the ARP table of your PC by DOS command “arp -d” then you can access the web server of device using the default IP address.

2. Use Wizard page to setup device.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

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 Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Next>>

3. Press “Next>>” button then set the “Operation Mode” to “Wireless ISP” mode.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

- Router:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs connected with WLAN share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP. 172.1.1.1 is the default Static IP address for WAN port
- Bridge:** In this mode, the ethernet port and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, the wireless client will connect to ISP access point. The NAT is enabled and PCs connecting with the ethernet port share the same IP to ISP through wireless LAN. **You must set the wireless to client mode** and connect to the ISP AP. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP.

Cancel <<Back Next>>

4. Press “Next>>” button then disable “Time Zone” function.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
- Reboot

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

NTP server : 192.5.41.41 - North America

Cancel <<Back Next>>

5. Press “Next>>” button then set the IP address of LAN interface.

The screenshot shows the '3. LAN Interface Setup' page. On the left is a 'Site contents' sidebar with a tree view containing: Wizard, Operation Mode, Wireless, TCP/IP, Firewall, Management, and Reboot. The main content area has a title '3. LAN Interface Setup' and a descriptive paragraph: 'This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask. The DHCP Server will be up and running, please make sure there is no another DHCP Server in your network when the device is in Bridge/Client Modes.' Below this are two input fields: 'IP Address:' with the value '192.168.2.205' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

6. Press “Next>>” button then select the “Client” for “mode” and change the SSID to “DEV5”.

The screenshot shows the '5. Wireless Basic Settings' page. The 'Site contents' sidebar is identical to the previous page. The main content area has a title '5. Wireless Basic Settings' and a descriptive paragraph: 'This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. If you want to use Wireless ISP mode, please choose the Client Mode.' Below this are several configuration fields: 'Band:' set to '2.4 GHz (B+G)', 'Mode:' set to 'Client', 'Network Type:' set to 'Infrastructure', and 'SSID:' set to 'DEV5'. There is also a 'Channel Number:' field set to '11' and an unchecked checkbox labeled 'Enable Mac Clone (Single Ethernet Client)'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Next>>'.

7. Press “Next>>” button then select “None” for “Encryption” then press “Finished” button.

The screenshot shows the '6. Wireless Security Setup' page. The 'Site contents' sidebar is identical to the previous pages. The main content area has a title '6. Wireless Security Setup' and a descriptive paragraph: '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.' Below this is an 'Encryption:' dropdown menu currently set to 'None'. At the bottom right are three buttons: 'Cancel', '<<Back', and 'Finished'.

8. Wait for refreshing web page.

The screenshot shows a confirmation message. The 'Site contents' sidebar is identical to the previous pages. The main content area has a title 'Change setting successfully!' followed by the text: 'Please wait a while for refreshing webpage.' and 'If IP address was modified, you have to re-connect the WebServer with the new address.'

- Access the web server by the new IP address “192.168.2.205” and use “LAN Interface” page to disable DHCP Server.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the device. Here you may change the setting for IP Address, Subnet Mask, DHCP, etc..

IP Address:
Subnet Mask:
Default Gateway:
DHCP:
DHCP Client Range: -
802.1d Spanning Tree:
Clone MAC Address:
MTU Size:

- Wait for refreshing webpage.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
 - LAN Interface
 - WAN Interface
- Route
- Firewall
- Management
- Reboot

Change setting successfully!

Please wait a while for refreshing webpage.

If IP address was modified, you have to re-connect the WebServer with the new address.

- Use “State” page to check setting.

Site contents:

- Wizard
- Operation Mode
- Wireless
- TCP/IP
- Firewall
- Management
 - Status
 - QoS
 - Bandwidth Control
 - SNMP
 - Statistics
 - DDNS
 - Time Zone
 - Log
 - Miscellaneous
 - Upgrade Firmware
 - Save/Reload Setting
 - Password
 - Reboot

System	
Uptime	0day:3h:15m:1s
Free Memory	11184 kB
Firmware Version	1.4.0c 20060914
Webpage Version	1.4.0c 20060914
Wireless Configuration	
Mode	Infrastructure Client - Bridge
Band	2.4 GHz (B+G)
SSID	DEV5
Channel Number	2
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
RSSI	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.205
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:00:00:04:22:21

12. If the “State” of “Wireless Configuration” is not “Connected” or you want to refresh the “RSSI “, please use “Site Survey” page to re-connect a AP.

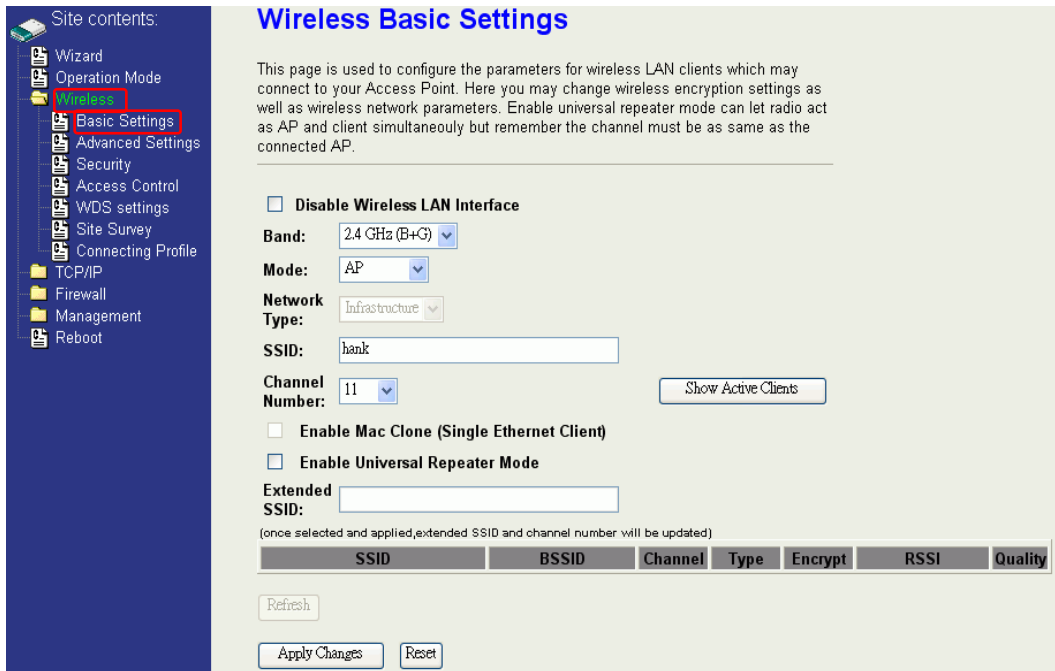
Wireless Site Survey

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

SSID	BSSID	Channel	Type	Encrypt	RSSI	Quality	Select	Act
D572	00:00:00:04:26:90	11 (B+G)	AP	no	61 (-53 dbm)	15	<input type="radio"/>	<input type="button" value="Refresh"/>
	00:0e:14:00:80:18	1 (B+G)	AP	no	60 (-54 dbm)	15	<input type="radio"/>	<input type="button" value="Refresh"/>
AIR802-2F	00:05:9e:80:b1:e3	1 (B+G)	AP	yes	41 (-65 dbm)	90	<input type="radio"/>	<input type="button" value="Refresh"/>
AIR802	00:05:9e:80:46:69	11 (B)	AP	no	40 (-70 dbm)	93	<input type="radio"/>	<input type="button" value="Refresh"/>
AIR802-3F	00:05:9e:80:b1:fd	11 (B+G)	AP	yes	29 (-72 dbm)	78	<input type="radio"/>	<input type="button" value="Refresh"/>
RTL116-default	00:00:00:aa:bb:cc	7 (B+G)	AP	no	26 (-74 dbm)	89	<input type="radio"/>	<input type="button" value="Refresh"/>
Auto.	00:05:9e:11:b9:67	6 (B+G)	AP	no	13 (-82 dbm)	67	<input type="radio"/>	<input type="button" value="Refresh"/>

Refresh Auto Refresh **Connect** Acting

Basic Settings



Disable Wireless LAN Interface

Disable the wireless interface of device

Band:

The device supports 2.4GHz(B), 2.4GHz(G) and 2.4GHz(B+G) mixed modes.

Mode:

The radio of device supports different modes as following:

1. AP

The radio of device acts as an Access Point to serves all wireless clients to join a wireless local network.

2. Client

Support Infrastructure and Ad-hoc network types to act as a wireless adapter.

3. WDS

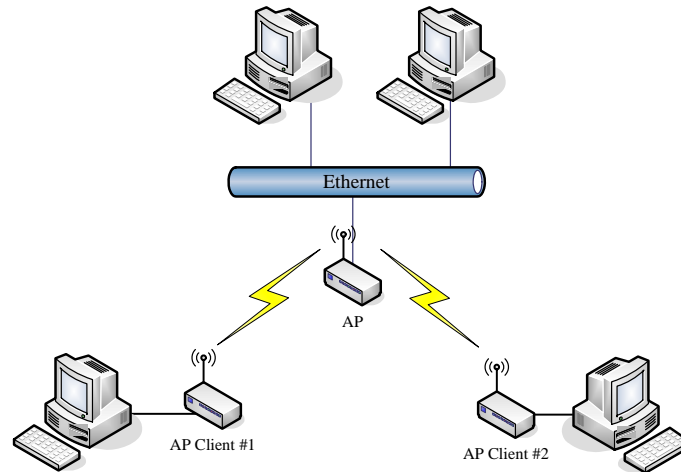
Wireless Distribution System, this mode joins to a WDS network which combines up to 8 WDS-AP, only devices with WDS function supported can connect to it, all the wireless clients can't survey and connect the device when the mode is selected.

4. AP+WDS

Support both AP and WDS functions, the wireless clients and devices with WDS function supported can survey and connect to it.

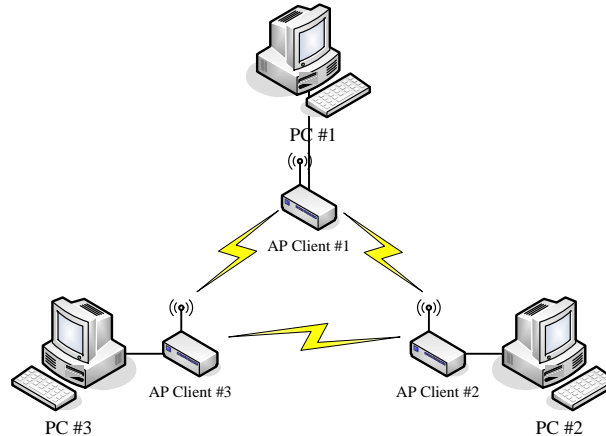
- **Infrastructure:**

This type requires the presence of 802.11b/g Access Point. All communication is done via the Access Point.



- **Ad Hoc:**

This type provides a peer-to-peer communication between wireless stations. All the communication is done from Client to Client without any Access Point involved. Ad Hoc networking must use the same SSID and channel for establishing the wireless connection.



In client mode, the device can't support the Router mode function including Firewall and WAN settings.

SSID:

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access point/bridges on a network or sub-network can use the same SSID. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID.

Channel Number

The following table is the available frequencies (in MHz) for the 2.4-GHz radio:

Channel No.	Frequency	Country Domain
1	2412	Americas, EMEA, Japan, and China
2	2417	Americas, EMEA, Japan, and China
3	2422	Americas, EMEA, Japan, Israel, and China
4	2427	Americas, EMEA, Japan, Israel, and China
5	2432	Americas, EMEA, Japan, Israel, and China
6	2437	Americas, EMEA, Japan, Israel, and China
7	2442	Americas, EMEA, Japan, Israel, and China
8	2447	Americas, EMEA, Japan, Israel, and China
9	2452	Americas, EMEA, Japan, Israel, and China
10	2457	Americas, EMEA, Japan, and China
11	2462	Americas, EMEA, Japan, and China
12	2467	EMEA and Japan
13	2472	EMEA and Japan
14	2484	Japan only

EMEA (Europe, the Middle East and Africa).

When set to “Auto”, the device will find the least-congested channel for use.

Associated Client

Show the information of active wireless client stations that connected to the device.

Advanced Settings

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your device. The default setting is optimized for the normal operation. For specific application, setting configuration will required highly attention to reach optimistic condition.

Note :

Any unreasonable value change to default setting will reduce the throughput of the device.

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)

ACK Timing: (0-255 * 4 us)

Client Expired Time: (101-40000000 sec)

MTU Size: (100-1500)

Data Rate:

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

802.11g Protection: Enabled Disabled

Block WLAN Relay: Enabled Disabled

Turbo Mode: Enabled Disabled (auto)

Aggregation Mode: Enabled Disabled

Tx Burst Mode: Enabled Disabled

Transmit Power(OFDM)

Transmit Power(CCK)

Authentication Type

The device supports two Authentication Types “Open system” and “Shared Key”. When you select “Share Key”, you need to setup “WEP” key in “Security” page (See the next section). The default setting is “Auto”. The wireless client can associate with the device by using one of the two types.

Fragment Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. This function will help you to improve the network performance.

RTS Threshold

The RTS threshold determines the packet size at which the radio issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the device, or in areas where the clients are far apart and can detect only the device and not each other. You can enter a setting ranging from 0 to 2347 bytes.

Beacon Interval

The beacon interval is the amount of time between access point beacons in mini-seconds. The default beacon interval is 100.

ACK Timing

Acknowledgement Timing, is the amount of time that device wait client's response. This concept is related to EIFS (Extended Inter-Frame Space). The EIFS interval shall begin while the device is idle after detection of the erroneous frame. The EIFS is defined to provide enough time for another device to acknowledge what was, to this device, an incorrectly received frame before this device commences transmission. The default setting of ACK timing is 0. You may need to change this value due to the environment or distance.

Client Expired Time

The client expired time determines time interval the client need to re-associate with the device while client is idle. The default client expired time is 300 sec.

MTU Size

Maximum Transmission Unit, the default MTU size is 1500. The MTU setting controls the maximum Ethernet packet size your PC will send. Why a limit? Because although larger packets can be constructed and sent, your ISP and Internet backbone routers and equipment will fragment any larger than their limit, then these parts are re-assembled by the target equipment before reading. This fragmentation and re-assembly is not optimal. You may need to change the MTU for optimal performance of your wireless LAN traffic.

Data Rate

The standard IEEE 802.11b/11g supports 1, 2, 5.5, 11 / 6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates. You can choose the rate that the device uses for data transmission. The default value is "auto". The device will use the highest possible selected transmission rate.

Broadcast SSID

Broadcasting the SSID will let your wireless clients find the device automatically. If you are building a public Wireless Network, disable this function can provide better security. Every wireless stations located within the coverage of the device must connect this device by manually configure the

SSID in your client settings.

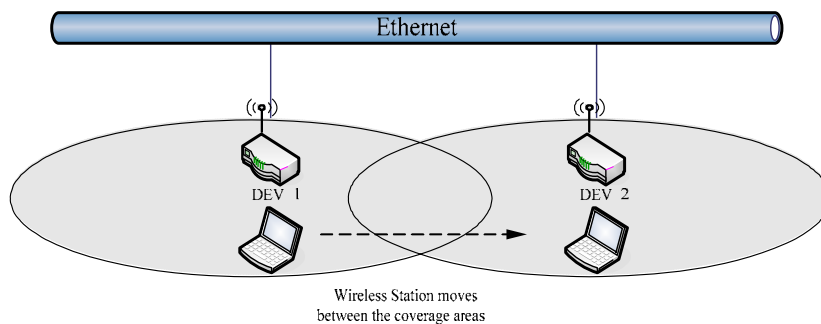
IAPP (Inter-Access Point Protocol)

This function will let Wireless Stations roam among a network environment with multiple devices. Wireless Stations are able to switch from one device to another as they move between the coverage areas. Users can have more wireless working range. An example is as the following figure.

You should comply with the following instructions to roam among the wireless coverage areas.

Note : For implementing the roaming function, the setting **MUST** comply the following two items.

- All the devices must be in the same subnet network and the SSID must be the same.
 - If you use the 802.1x authentication, you need to have the user profile in these devices for the roaming station.
-



Block WLAN Relay (Isolate Client)

The device supports isolation function. If you are building a public Wireless Network, enable this function can provide better security. The device will block packets between wireless clients (relay). All the wireless clients connected to the device can't see each other.

Transmit Power

The default transmit power of this device is 24dBm for CCK (802.11b) and 20dBm for OFDM (802.11g). In case of decrease the wireless distance and coverage of this device, turn down the power level for CCK and OFDM. For CCK, 4 levels are available to turn down the power from default 24dBm to 23, 22, 21, 20dBm. For OFDM, 3 levels are available to turn down the power from default 20dBm to 19, 18, 17dBm.

If you want to restore the wireless distance and coverage of the device, select a higher level or the default level of transmit power.

Configuring Wireless Security

This device provides complete wireless security function include WEP, 802.1x, WPA-TKIP, WPA2-AES and WPA2-Mixed in different mode (see the Security Support Table).

The default security setting of the encryption function is disabled. Choose your preferred security setting depending on what security function you need.

Site contents:

- Wizard
- Operation Mode
- Wireless**
- Basic Settings
- Advanced Settings
- Security
- Access Control
- WDS settings
- Site Survey
- Connecting Profile
- TCP/IP
- Firewall
- Management
- Reboot

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.

Authentication Type: Open System Shared Key Auto

Encryption:

Use 802.1x Authentication WEP 64bits WEP 128bits

Enable MAC Authentication

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

Pre-Shared Key Format:

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server: Port IP address Password

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

WEP Encryption Setting

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be as same as each client in your wireless network. For more secure data transmission, you can change encryption type to “WEP” and click the “Set WEP Key” button to open the “Wireless WEP Key setup” page.

Encryption:

Use 802.1x Authentication WEP 64bits WEP 128bits

Enable MAC Authentication

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

Pre-Shared Key Format:

Pre-Shared Key:

Enable Pre-Authentication

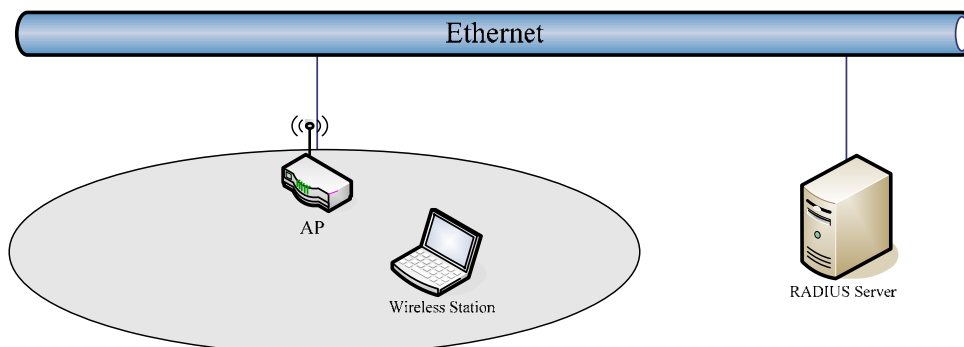
Authentication RADIUS Server: Port IP address Password

When you decide to use the WEP encryption to secure your WLAN, please refer to the following setting of the WEP encryption:

- 64-bit WEP Encryption : 64-bit WEP keys are as same as the encryption method of 40-bit WEP. You can input 10 hexadecimal digits (0~9, a~f or A~F) or 5 ACSII chars.
- 128-bit WEP Encryption : 128-bit WEP keys are as same as the encryption method of 104-bit WEP. You can input 26 hexadecimal digits (0~9, a~f or A~F) or 10 ACSII chars.
- The Default Tx Key field decides which of the four keys you want to use in your WLAN environment.

WEP Encryption with 802.1x Setting

The device supports external RADIUS Server that can secure networks against unauthorized access. If you use the WEP encryption, you can also use the RADIUS server to check the admission of the users. By this way every user must use a valid account before accessing the Wireless LAN and requires a RADIUS or other authentication server on the network. An example is shown as following.



You should choose WEP 64 or 128 bit encryption to fit with your network environment first. Then add user accounts and the target device to the RADIUS server. In the device , you need to specify the IP address、 Password (Shared Secret) and Port number of the target RADIUS server.

Encryption:

Use 802.1x Authentication WEP 64bits WEP 128bits

Enable MAC Authentication

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

Pre-Shared Key Format:

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server: Port IP address Password

WPA Encryption Setting

WPA feature provides a high level of assurance for end-users and administrators that their data will remain private and access to their network restricted to authorized users. You can choose the WPA encryption and select the Authentication Mode.

WPA Authentication Mode

This device supports two WPA modes. For personal user, you can use the Pre-shared Key to enhance your security setting. This mode requires only an access point and client station that supports WPA-PSK. For Enterprise, authentication is achieved via WPA RADIUS Server. You need a RADIUS or other authentication server on the network.

- **Enterprise (RADIUS):**

When WPA Authentication mode is Enterprise (RADIUS), you have to add user accounts and the target device to the RADIUS Server. In the device , you need to specify the IP address, Password (Shared Secret) and Port number of the target RADIUS server.

- **Pre-Share Key:**

This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8~63 ACSII chars. When Key format is Hex, the key value should have 64 hexadecimal digits (0~9, a~f or A~F).

Configuring as WLAN Client Adapter

This device can be configured as a wireless Ethernet adapter. In this mode, the device can connect to the other wireless stations (Ad-Hoc network type) or Access Point (Infrastructure network type) and you don't need to install any driver.

Quick start to configure

Step 1. In "Basic Settings" page, change the Mode to "Client" mode. And key in the SSID of the AP you want to connect then press "Apply Changes" button to apply the change.

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. Enable universal repeater mode can let radio act as AP and client simultaneously but remember the channel must be as same as the connected AP.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

3 Mode: Client

Network Type: Infrastructure

4 SSID: Target-AP-SSID

Channel Number: 11 [Show Active Clients](#)

Enable Mac Clone (Single Ethernet Client)

Enable Universal Repeater Mode

Extended SSID:

(once selected and applied, extended SSID and channel number will be updated)

SSID	BSSID	Channel	Type	Encrypt	RSSI	Quality
------	-------	---------	------	---------	------	---------

[Refresh](#)

5 [Apply Changes](#) [Reset](#)

Step 2. Check the state of connection in "Status" web page

System

Uptime 0day:0h:14m:2s

Free Memory 11912 kB

Firmware Version 1.4.0c 20060914

Webpage Version 1.4.0c 20060914

Wireless Configuration

Mode Infrastructure Client - Bridge

Band 2.4 GHz (B+G)

SSID Target-AP-SSID

Channel Number 11

Encryption Disabled

BSSID 00:00:00:00:00:00

5 State Scanning

RSSI 0

TCP/IP Configuration

Attain IP Protocol Fixed IP

IP Address 192.168.2.205

Subnet Mask 255.255.255.0

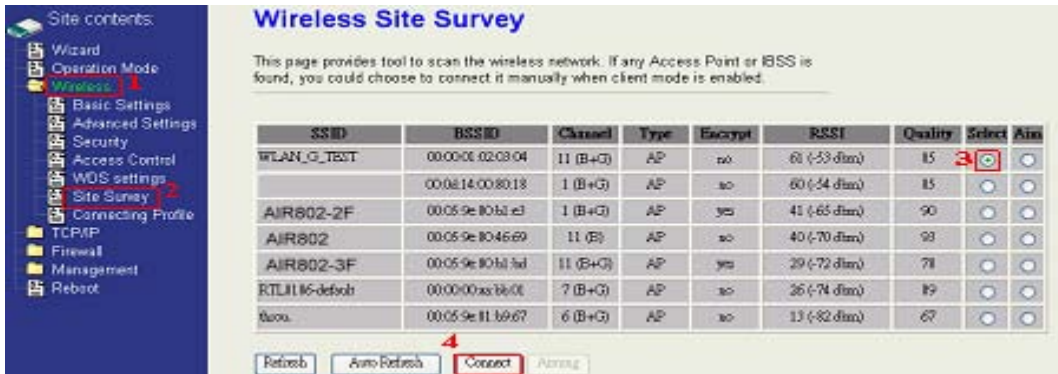
Default Gateway 0.0.0.0

DHCP Server Disabled

MAC Address 00:00:00:04:22:21

The alternative way to configure as following:

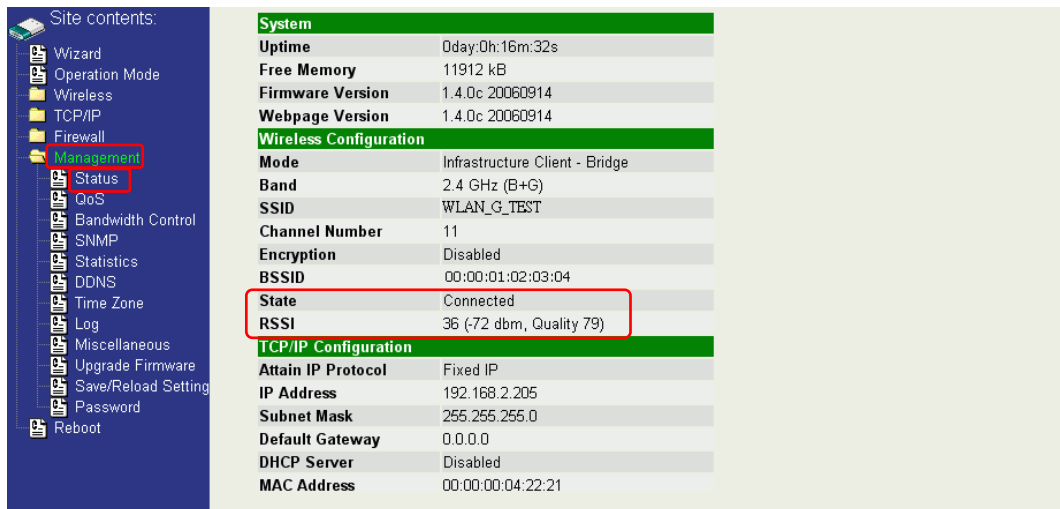
Step 1. In “Wireless Site Survey” page, select one of the SSIDs you want to connect and then press “Connect” button to establish the link.



Step 2. If the linking is established successfully. It will show the message “Connect successfully”. Then press “OK”.



Step 3. Then you can check the linking information in “Status” page.



Note :

If the available network requires authentication and data encryption, you need to setup the authentication and encryption before step1 and all the settings must be as same as the Access Point or Station. About the detail authentication and data encryption settings, please refer the security section.

Authentication Type

In client mode, the device also supports two Authentication Types “Open system” and “Shared Key”. Although the default setting is “Auto”, not every Access Points can support “Auto” mode. If the authentication type on the Access Point is knew by user, we suggest to set the authentication type as same as the Access Point.

Data Encryption

In client mode, the device supports WEP and WPA Personal/Enterprise except WPA2 mixed mode data encryption. About the detail data encryption settings, please refer the security section.

MAC Clone for Single Ethernet Client

Enable/Disable Mac Clone (Single Ethernet Client) in Wireless-Basic Settings page determines whether the Ethernet Client use it's own MAC address or AP-Client's MAC address to transmit data. Enable MAC Clone, the single Ethernet client can use its own MAC address. Disable MAC Clone, the single Ethernet client must to use AP-Client's MAC address.

While you use this device act as AP-Client and only one host connect to this device via Ethernet, you need to check this option in this page, otherwise the other device can't recognize your host behind AP-Client. If you use hub/switch connect multi-device to this AP-Client, you should uncheck this option.