



**WLA-500AP**

*WISP Client Router Mode*

# User's Manual



## **Copyright Statement**

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the prior writing of the publisher.

Windows 95/98/Me and Windows 2000 are trademarks of Microsoft Corp.

Pentium is trademark of Intel.

All copyright is reserved.

---

# TABLE OF CONTENT

<b>INTRODUCING THE WISP CLIENT ROUTER MODE .....</b>	<b>3</b>
OVERVIEW OF THE WLA-5000AP .....	4
WISP CLIENT ROUTER MODE APPLICATIONS.....	4
<i>Accessing the Internet .....</i>	<i>4</i>
<i>Accessing Servers from the Public Network.....</i>	<i>5</i>
A SECURITY OVERVIEW .....	5
WLA-5000AP FEATURES .....	5
SETTING UP THE DEVICE .....	6
<b>INSTALLING THE WLA-5000AP .....</b>	<b>7</b>
WHAT'S IN THE BOX?.....	7
A PHYSICAL LOOK AT THE BACK PANEL .....	8
A PHYSICAL LOOK AT THE FRONT PANEL .....	9
CONNECTING THE CABLES .....	10
HIGH LEVEL CONFIGURATION STEPS REQUIRED FOR THE WLA-5000AP .....	10
SETTING UP A WINDOWS PC OR WIRELESS CLIENT AS DHCP CLIENTS.....	10
CONFIGURING A PC RUNNING MS-WINDOWS 95/98/ME: .....	11
CONFIGURING A PC RUNNING MS-WINDOWS XP/2000: .....	11
CONFIRMING YOUR PC'S IP CONFIGURATION:.....	11
CONNECTING MORE DEVICES THROUGH A HUB TO THE WLA-5000AP .....	12
<b>BASIC CONFIGURATION OF THE WLA-5000AP .....</b>	<b>13</b>
<b>LOGGING ON</b> .....	14
SETUP WIZARD .....	14
<i>Set up your Local Time Zone and Date/Time .....</i>	<i>15</i>
<i>Configure the ISP profile .....</i>	<i>15</i>
<i>Device IP Settings .....</i>	<i>19</i>
<i>Configure Your Wireless LAN Connection .....</i>	<i>20</i>
<i>Finish Setup Wizard and Save Your Settings.....</i>	<i>23</i>
<b>ADVANCED SETTINGS.....</b>	<b>25</b>
PASSWORD SETTINGS .....	26
SYSTEM MANAGEMENT .....	27
SNMP SETTINGS .....	29
DHCP SERVER SETTINGS .....	31
MULTIPLE DMZ .....	33
VIRTUAL SERVER SETTINGS .....	34
<b>SPECIAL APPLICATIONS</b> .....	35
IP FILTERING SETTINGS .....	36
IP ROUTING SETTINGS .....	38
WIRELESS SETTINGS.....	39
DYNAMIC DNS SETTINGS .....	40
<b>MANAGING YOUR WLA-5000AP.....</b>	<b>42</b>
HOW TO VIEW THE DEVICE STATUS .....	42
HOW TO VIEW THE SYSTEM LOG.....	43
DHCP CLIENT TABLE .....	44
BRIDGE TABLE .....	44
RADIO TABLE.....	45
UPGRADING FIRMWARE.....	46
HOW TO SAVE OR RESTORE CONFIGURATION CHANGES .....	48
HOW TO RESTORE THE SYSTEM SETTINGS TO THE FACTORY DEFAULTS .....	49
<b>HOW TO REBOOT YOUR WLA-5000AP</b> .....	50
<b>WHAT IF YOU FORGOT THE PASSWORD?</b> .....	51
<b>SPECIFICATION .....</b>	<b>52</b>



## Chapter

# 1

## Introducing the WISP Client Router Mode

This manual gives a basic introduction to WISP Client Router Mode. It provides information to configure the WLA-5000AP to operate in common applications such as connecting to the Internet.

We'll describe how to use your web browser to configure the WLA-5000AP and to perform various management functions, e.g. upgrading the software, or viewing the system log, a task that can be useful in ongoing operations.

This manual consists of the following chapters and appendixes:

**Chapter One**, *Introduction*, summarizes features and capabilities of the WLA-5000AP.

**Chapter Two**, *Installing the WLA-5000AP*, gives steps you should follow to install the WLA-5000AP and configure your PCs.

**Chapter Three**, *Configuring the WLA-5000AP*, describes how to log in to the Web Manager, the browser screen, and steps needed to configure your WLA-5000AP for specific applications. It gives easy-to-follow instructions for quick Internet access and provides a guide to basic WLA-5000AP configuration.

**Chapter Four**, *Advanced Configuration*, provides information on advanced router configuration.

**Chapter Five**, *Managing your WLA-5000AP*, explains other management features of the WLA-5000AP.

## Overview of the WLA-5000AP



The WISP Client Router mode that sits between your local Ethernet network and a remote network (e.g., the Internet). The WLA-5000AP contains a 10/100Mbps Ethernet switch for connection to PCs on your local wired network, and two wireless interfaces for connection to your local wireless network: one supports 802.11a, another can be configured to support either both 802.11b and 802.11g or 802.11g only (both radios support a data rate of up to 54 Mbps).

Data comes into the WLA-5000AP from the local wired and wireless LAN and then is “routed” to the Internet, and vice versa.

## *WISP Client Router mode Applications*

### ACCESSING THE INTERNET

The most common use of the WISP Client Router mode is to provide shared Internet access to allow everyone on your LAN to surf the web and send/receive emails or files. The WISP Client Router mode can automatically acquire a public IP address when connecting to the Internet. In turn, it will

---

automatically assign IP addresses to PCs (requesting DHCP client devices) on your LAN - you don't have to apply for and assign IP addresses to PCs on your network.

## ACCESSING SERVERS FROM THE PUBLIC NETWORK

If you want special servers to be accessible to remote users across the Internet (e.g., an e-mail server, an FTP server, or a web server), you can configure the WLA-5000AP to *proxy* the service using its (public) IP address. It means a remote user can access the server by using the WLA-5000AP's IP address. Upon receiving a request, the WLA-5000AP will re-direct the request to the actual server on your local network.

## A Security Overview

More and more people are concerned about protecting your local network from the Internet. The WLA-5000AP provides several ways to keep your network secure:

- Devices on your wired or wireless network are assigned private IP addresses; therefore remote users from the Internet cannot see nor access them.
- The WLA-5000AP implements IP packet filtering with SPI (Stateful Packet Inspection) capabilities, which you can use to selectively filter (discard) packets to/from the Internet.
- You can selectively restrict management from remote devices.

To address the growing security concern in a wireless LAN environment, different levels of security can also be enabled in the WLA-5000AP, including:

- To disable SSID broadcast so to restrict association to only client stations that are already pre-configured with correct SSIDs
- To enable WEP (Wireless Encryption Protocol) encryption to implement privacy of your data
- To enable WPA (WiFi Protected Access) to assure authorized access as well as to implement privacy of your data. WPA comes with PSK (Pre-Shared Key) for SOHO users.

## WLA-5000AP Features

- High performance 11 Mbps (802.11b) or 54Mbps (802.11a/g) data rate
  - Wi-Fi, WPA certificated interoperability
  - Web-based, SNMP v1/v2, Telnet management
  - WPA with Pre-Shared Key Support
  - WPA with TKIP Support
  - WPA with Advanced Encryption Standard (AES) support
  - 152-bit WEP support (Atheros Proprietary)
  - S/W (station/receiver based) DMZ support
  - VPN pass through support
  - Advanced NAT/Firewall features
  - Special applications support including MSN Messenger6.0, Netmeeting... etc
  - 802.1d Spanning Tree Protocol support
  - RoHS complied
-

## *Setting Up the device*

A local PC on either the wired or wireless LAN network can manage the WLA-5000AP. To do this, the WLA-5000AP must have an IP address, which can be statically configured, or is dynamically obtained from a DHCP server on the LAN.



## Chapter

# 2

## Installing the WLA-5000AP

This section describes the installation procedure for your WLA-5000AP. It starts with a summary of the content of the package you have purchased, followed by steps of how to connect and power up your WLA-5000AP. Finally, it describes how to configure a Windows PC to communicate with your WLA-5000AP.

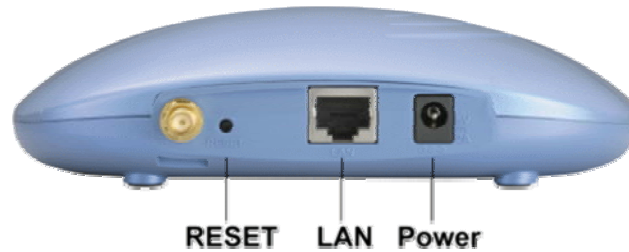
### *What's in the Box?*

The WLA-5000AP package comes with the following items:

- One WLA-5000AP
- One 5V DC/2A power adapter with a barrel connector
- One CD contains WLA-5000AP User' Guide

## *A physical look at the back panel*

The following illustration shows the rear panel of WLA-5000AP.



- (1) 1 RJ-45 10/100 Switch connectors for connecting to PCs and workstations or connecting external Ethernet hub, or switch with auto-sensing.
  - (2) 1 DC 5V/2A power connector for connecting through a DC power adapter (included as part of the product) to the wall power outlet.
  - (3) 1 Reset button to restore the device back to the factory settings.
-

## *A physical look at the front panel*

The LEDs on the front of the WLA-5000AP reflect the operational status of the unit.



## WLA-5000AP LED Description

Label	LAN	WAN	11g (WLAN)	11a (WLAN)	Power
<b>Steady Green</b>	Link is active	Link is active	Link is active	Link is active	System boot-up OK
<b>OFF</b>	No LAN connection	No connection	Radio off	Radio off	No Power
<b>Flashing Green</b>	XMT/RCV Data	XMT/RCV Data	XMT/RCV Data	XMT/RCV Data	Under boot-up

## *Connecting the Cables*

Follow these steps to install your WLA-5000AP:

- Step 1.** Connect ADSL/Cable modem to the Wireless Router WAN port using CAT5 UTP LAN cable.
- Step 2.** Connect a PC/Workstation to one of the LAN ports of the Wireless Router.
- Step 3.** Connect one end of the DC adapter to the Wireless Router and plug the other end into an electrical outlet.

## *High Level Configuration Steps Required for the WLA-5000AP*

This section describes configuration required for the WLA-5000AP before it can work properly in your network.

Normally, devices on both LANs (except for servers) are configured to obtain their IP addresses automatically. Depending on whether there is a separate DHCP server available in your LAN environment network, thus to determine if you need to enable the built-in DHCP server in the Wireless Router. The following configuration step assumes that the router's built-in DHCP server will be used.

Additionally, since you need to perform various configuration changes to the WLA-5000AP, including the SSID, Channel number, the WEP key, etc., it is necessary to associate a fixed IP address with the WLA-5000AP, which is why the WLA-5000AP will be shipped with a factory default private IP address of 192.168.1.1 (and a network mask of 255.255.255.0).

## *Setting up a Windows PC or wireless client as DHCP clients*

The following will give detailed steps of how to configure a PC or a wireless client to “obtain IP addresses automatically”. For other types of configuration, please refer to the corresponding user manual.

For the case of using a LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the WLA-5000AP either directly or through an external LAN switch, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

---

For the case of using a wireless client, the client must also have a wireless interface installed properly, be physically within the radio range of the WLA-5000AP, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

### *Configuring a PC running MS-Windows 95/98/Me:*

1. Click the Start Button, and select Settings.
2. Click the Control Panel. The Win95/98/Me Control Panel will appear.
3. Open the Network setup window by double-clicking the Network icon.
4. Check your list of Network items. If TCP/IP is already installed, proceed to step 5. Otherwise:  
(You may need your Windows CD to complete the installation of TCP/IP.)
  - Click the ADD button.
  - In the Network Component Type dialog box, select Protocol.
  - In the Select Network Protocol dialog box, select Microsoft.
  - In the Network Protocols area of the same dialog box, select TCP/IP and click OK.
5. With TCP/IP installed, select TCP/IP from the list of Network Components.
6. In the TCP/IP window, check each of the tabs and verify the following settings:
  - Bindings: Select Client for Microsoft Networks and Files and printer sharing for Microsoft Networks
  - Gateway: All fields are blank.
  - DNS Configuration: Select Disable DNS.
  - WINS Configuration: Select Use DHCP for WINS Resolution.
  - IP address: Select the Obtain IP address automatically radio button.
7. Reboot the PC.

### *Configuring a PC running MS-Windows XP/2000:*

1. Click the Start button, and choose Control Panel (in Classic View).
2. In the Control Panel, double-click Network Connections.
3. Double-click Local Area Connection.
4. In the LAN Area Connection Status window, select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

### *Confirming your PC's IP Configuration:*

There are two tools useful for finding out a computer's IP address and default gateway:

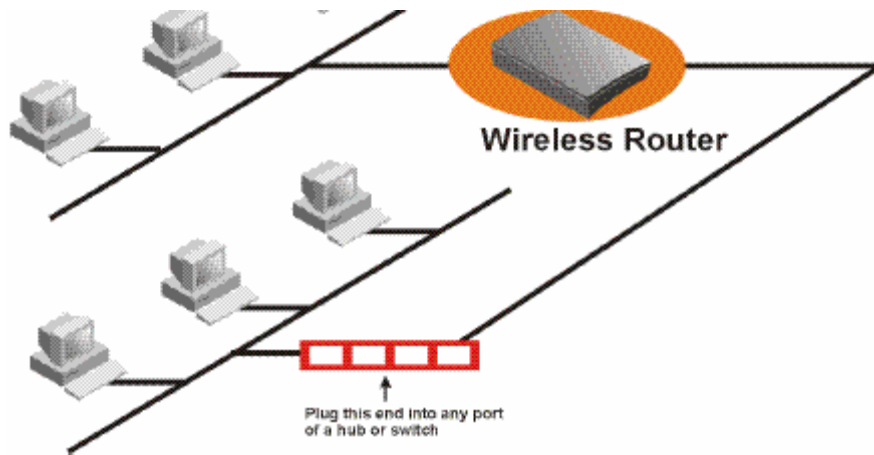
WINIPCFG (for Windows 95/98/Me) Select the Start button, and choose Run. Type winipcfg, and a window will appear listing the IP configuration. You can also type winipcfg in the MS-DOS prompt.

---

The procedure required to set a static IP address is not too much different from the procedure required to set to “obtain IP addresses dynamically” - except that instead of selecting “obtain IP addresses dynamically”, you should specify the IP address explicitly.

### *Connecting More Devices Through A Hub To The WLA-5000AP*

The Wireless Router provides four LAN ports to allow up to four PCs or Workstations to be connected to it directly. If you want to connect more devices, you can connect an external hub or switch to any of the LAN ports using a LAN cable.



## Chapter

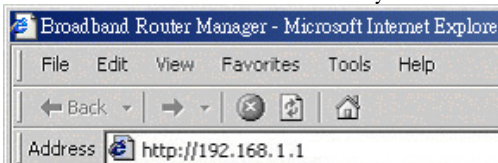
# 3

## Basic Configuration of the WLA-5000AP

This section contains basic configuration procedure for the WLA-5000AP. It also describes how to set up the **WISP Client Router mode** for Internet Access operation, and how to set up the LAN configuration.

The WLA-5000AP is designed so that all basic configuration may be easily invoked through the a standard Web browser such as Internet Explorer. Currently only the Internet Explorer 6.0 (or above) is supported.

To access the WLA-5000AP's management interface for the first time, enter the default IP address of the WLA-5000AP in your Web browser <http://192.168.1.1/>.



**Note:** The IP address of your PC must be in the same IP subnet as the WLA-5000AP. It is preferred that you configure the PC to obtain an IP address automatically from the WLA-5000AP.

The **Home Page** of the WLA-5000AP screen will appear, with its main menu displayed on the screen, showing the following top-level choices: Setup Wizard, Device Status, System Tools, Advanced Settings, and Help. Selecting any will allow you to navigate to other configuration menus.

## Logging On



When you attempt to access a configuration screen from the browser menu, an administrator login screen will appear, prompting you to enter your password to log on. Once you are logged in, you will not be asked to log in again unless your “session” expires such as due to inactivity timeout.

If you are logging in for the first time after you received your WLA-5000AP you should use the factory default password, “**airlive**” to log in. (You should change it as soon as after you log in.)

Characters you type (as your password) will be echoed back as a string of asterisks (“\*”) for security reasons. After you enter the password, clicking the **LOG ON** button will begin the password verification process and, if successful, your configuration session can begin.

**Note:** Should there be no settings or access on the web management screen, system will logout automatically in 10 minutes.

## Setup Wizard

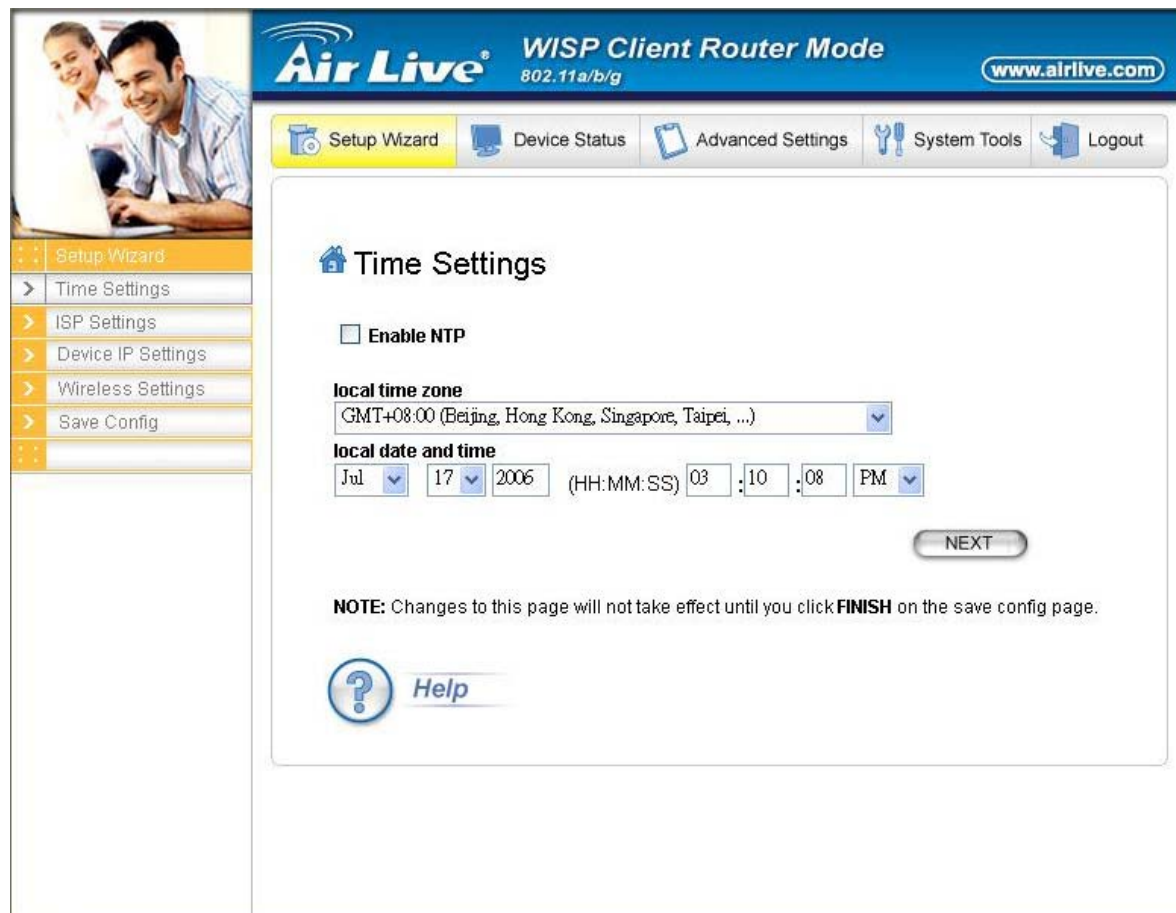
The Setup Wizard will guide you through a series of configuration screens to set up the basic configuration of your WLA-5000AP. At the end of the Setup Wizard screens, you should press the “**FINISH**” button, and all your configuration modifications will take effect.

---



## SET UP YOUR LOCAL TIME ZONE AND DATE/TIME

After logging in, the **Time Settings** page appears. The router time will first be set to the local time of the PC (on which the browser is running). If this time is not correct, modify the appropriate fields as necessary, and then click “NEXT”.



The screenshot shows the 'Time Settings' page in the Air Live WISP Client Router Mode. The page has a blue header with the 'Air Live' logo, 'WISP Client Router Mode', and '802.11a/b/g'. A navigation bar includes 'Setup Wizard', 'Device Status', 'Advanced Settings', 'System Tools', and 'Logout'. On the left, a sidebar lists 'Setup Wizard', 'Time Settings', 'ISP Settings', 'Device IP Settings', 'Wireless Settings', and 'Save Config'. The main content area is titled 'Time Settings' and contains an 'Enable NTP' checkbox, a 'local time zone' dropdown menu set to 'GMT+08:00 (Beijing, Hong Kong, Singapore, Taipei, ...)', and a 'local date and time' section with fields for month (Jul), day (17), year (2006), time (03:10:08 PM), and a 'NEXT' button. A note states: 'NOTE: Changes to this page will not take effect until you click FINISH on the save config page.' A 'Help' link is also present.

## CONFIGURE THE ISP PROFILE

In the following configuration screen, as with the usual convention, radio buttons are used to make a selection when only one out of multiple mutually exclusive choices can be selected, while square check boxes can be used to select multiple non-mutually-exclusive choices.

When configuring the device for Internet access, decide which one of the following multiple choices to select (through radio buttons):

1. You can use a **static IP address** provided by your ISP to connect to the Internet. In this case, you need to configure the following information:
    - **IP Address Assigned by Your ISP:** the IP address of the WAN interface of your router.
    - **IP Subnet Mask:** the IP subnet mask of the WAN interface of your router.
    - **ISP Gateway IP Address:** the IP address of your ISP's Gateway.
    - **DNS IP Address:** the IP address of the DNS server.
-

2. You use the user name and password assigned by your ISP to connect to the Internet (required for the underlying **PPPoE** protocol). In this case, you need to configure the following information:
    - **User Name:** the username of your ISP account.
    - **Password:** the password of your ISP account.
    - **Service Name:** the service name of your ISP account
    - **Connection Type:** There are 3 options for this option.
      - Always on: the connection is always on no matter there is traffic or not. If the connection is lost (e.g. the PPPoE server is down or the ADSL/Cable line is disconnected), the connection will be brought up right after the connection is recovered.
      - Demand Dialing: the connection will be brought up only when there is traffic. That is, it requires an outgoing packet to trigger the connection.
      - Manual: Users have to bring up and take down the connection manually.
    - **MTU/MRU:** This is to set the values of MTU (Maximum Transmit Unit) and MRU (Maximum Receive Unit) that is used between the 802.11 a/g Router and the ISP device at the other side. Users are not encouraged to change these values unless you know what you are doing.
    - **Session Type:** There are 3 options for this setting.
      - Normal: This option only supports one PPPoE session.
      - Unnumbered Link: This option can let your LAN be a public IP subnet. That is, PC's on the LAN can be configured with public IP addresses provided by your ISP. You can put your own servers on the LAN, and then people on the Internet can access these servers. The source IP address of the traffic from these PC's to the Internet is not modified (i.e. NAT is not applied) either. If you still want to keep a private LAN, you can check the **Maintain Private LAN** setting and enter the **IP Address** and **IP Subnet Mask** of your private LAN. If you do not keep a private LAN, the "Device IP Settings" menu at the left side will disappear.
  3. You use **DHCP** to connect to the Internet (most likely through a cable modem connection). In this case, your ISP **may** require you to configure the Host Computer Name:
    - **Host Name:** The Host Name provided by your ISP.
  4. You use **PPTP** to connect to the Internet. In this case, your ISP requires you to configure PPTP's tunnel IP address, the username, and password. In this case, configure the static IP address as in the above and then configure the following information:
    - **PPTP Local IP Address:** the IP address on the local side of the PPTP tunnel provided by your ISP.
    - **PPTP IP Netmask:** the Netmask on the local side of the PPTP tunnel provided by your ISP.
    - **PPTP Remote IP Address:** the IP address of the remote side of the PPTP tunnel provided by your ISP.
-

- **User Name:** the username of your ISP account.
- **Password:** the password of your ISP account.
- **Idle time:** The Idle Timeout is the number of seconds of "inactivity" before the PPTP connection is taken down.

Its value should be between 0 to 60 minutes, with 5 (minutes) being the default value, and 0 meaning the connection will never time out.

5. **Cloned MAC Address:** Some ISPs expect a PC to be connected to their service, and use the MAC address of this PC's LAN card for identification purposes. By checking the following "**Cloned MAC address**" square check box, your WLA-5000AP allows a MAC address to be configured and "cloned" in the router to simulate a PC.

If the device is a PC based on WIN 95/98/Me, you can run **winipcfg** to find out the MAC Address of its LAN card. If the device is a PC based on WIN 2000/NT/XP, you need to run "**ipconfig/all**" to find out the MAC address of its LAN card.

---



Setup Wizard



Device Status



Advanced Settings



System Tools



Logout

- Setup Wizard
- Time Settings
- ISP Settings
- Device IP Settings
- Wireless Settings
- Save Config

## ISP Settings

- ☐ If your ISP has assigned you a **static IP** address, select this button and enter the information below:

IP Address Assigned by Your ISP:

IP Subnet Mask:

ISP Gateway IP Address:

DNS IP Address:

- ☐ If your ISP already provides you with **PPPoE** authentication information, select this button and enter the information below:

User Name:

Password:

Service name:

Connection Type:

## DEVICE IP SETTINGS

The **Device IP setting** screen allows you to configure the IP address and subnet mask of your WLA-5000AP: you can configure a static IP address and a subnet mask, or configure it to obtain an IP address and a subnet mask automatically from a DHCP server on the local network.

The screenshot shows the 'Device IP Settings' page in the Air Live WISP Client Router Mode. The page has a blue header with the 'Air Live' logo, 'WISP Client Router Mode', and '802.11a/b/g'. A navigation bar includes 'Setup Wizard', 'Device Status', 'Advanced Settings', 'System Tools', and 'Logout'. A left sidebar lists menu items: 'Setup Wizard', 'Time Settings', 'ISP Settings', 'Device IP Settings' (highlighted), 'Wireless Settings', and 'Save Config'. The main content area is titled 'Device IP Settings' and contains the following text: 'You can select one of the following two approaches to assign an IP address to this device.' There are two radio button options: 'Assign static IP to this device.' (selected) and 'Use the DHCP client protocol to automatically get the IP address for this device.' Below the first option are input fields for 'IP Address' (192, 168, 1, 1) and 'IP Subnet Mask' (255, 255, 255, 0). Below the second option is a note: 'Selecting this option will disable your DHCP server automatically.' At the bottom of the main area are 'BACK' and 'NEXT' buttons. A 'NOTE' states: 'Changes to this page will not take effect until you click FINISH on the save config page.' A 'Help' link with a question mark icon is also present.

If you choose to assign a static IP address manually, check the button that says, “**Assign static IP to this device**” and then fill in the following fields

**IP Address** and **IP Subnet Mask**: These values default to 192.168.1.1 and 255.255.255.0, respectively.

This IP address can be modified if necessary, to either a different address in this same subnet or to an address in a different subnet.

When you modify it, if the DHCP server function of your WLA-5000AP is enabled, the pool of IP addresses it will use for assignment purposes will also be automatically adjusted accordingly. For example, if the default IP address is used, the IP address pool for assignment consists of addresses from 192.168.1.2 to 192.168.1.254. However, please do not change the default IP address unless you know exactly what you want to achieve.

Then you should press **Next** to get to the next screen.

If you choose to use an external DHCP Server to automatically assign an IP address to your WLA-5000AP check the button that says, “**Use the DHCP protocol to automatically get the IP address for this device**”, and then press **Next** to the next screen.

When an IP address is *dynamically* assigned to the router, its value can change depending on the IP address assignment policy used by the DHCP server in the network. Since you need to use an IP address to control and manage your WLA-5000AP, without the knowledge of its IP address, in order to access it, you will need to use UPnP (Universal Plug and Play) or other management tools that do not depend on a fixed IP address.

It is strongly recommended that you select the manual static IP address.

## CONFIGURE YOUR WIRELESS LAN CONNECTION

In the following configuration screen, you can configure wireless related parameters of your WLA-5000AP:

**Network Name (SSID):** The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the wireless network. Several Routers on a network can have the same SSID. The SSID can be up to 32 characters long. This SSID is used for both radios (i.e. 802.11a and 802.11 b/g).

**Disable SSID Broadcasting:** An access point periodically broadcasts its SSID, along with other information, which allows client stations to learn its existence while searching for Routers in the wireless network. Select **Disable** if you do not want the device to broadcast the SSID.

**Regulatory Domain:** This place shows the regulatory domain where the device is running. This field cannot be changed by regulation.

**WLAN standard for Radio 1/2:** Here you can set the configuration for each radio.

**Mode:** For the radio 1, you can select it to run the **802.11a** protocol.

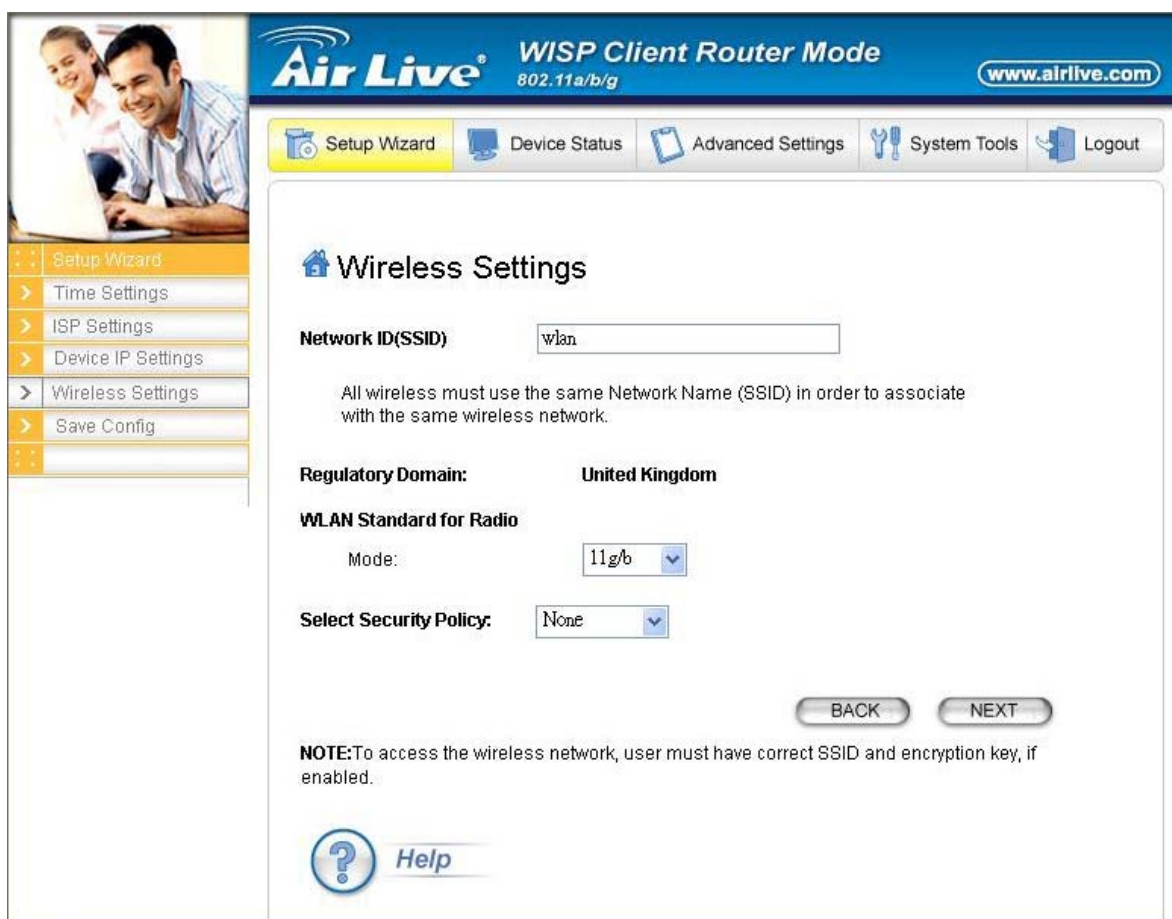
For the radio 2, you can select it to run the **802.11g only** protocol or the **802.11b/g** (mix mode) – allowing both 802.11b and 802.11g to co-exist.

**Channel:** Select the channel from the available list to match your network settings. All devices in the wireless network must use the same channel and share the total bandwidth available.

**Note:** The available channels are different from country to country and for different WLAN mode.

**Security Policy:** You can select different security policy to provide association authentication and/or data encryption.

---



The image shows a screenshot of the Air Live WISP Client Router Mode Setup Wizard. The interface has a blue header with the 'Air Live' logo, 'WISP Client Router Mode', '802.11a/b/g', and the website 'www.airlive.com'. Below the header is a navigation bar with icons for 'Setup Wizard', 'Device Status', 'Advanced Settings', 'System Tools', and 'Logout'. On the left is a sidebar menu with options: 'Setup Wizard', 'Time Settings', 'ISP Settings', 'Device IP Settings', 'Wireless Settings' (which is highlighted), 'Save Config', and a 'Help' link at the bottom. The main content area is titled 'Wireless Settings'. It contains a 'Network ID (SSID)' field with 'wlan' entered. Below this is a note: 'All wireless must use the same Network Name (SSID) in order to associate with the same wireless network.' There is a 'Regulatory Domain' dropdown set to 'United Kingdom'. Below that is a 'WLAN Standard for Radio' section with a 'Mode' dropdown set to '11g/b'. There is also a 'Select Security Policy' dropdown set to 'None'. At the bottom right of the form are 'BACK' and 'NEXT' buttons. A 'NOTE' states: 'To access the wireless network, user must have correct SSID and encryption key, if enabled.' A 'Help' icon is located at the bottom left of the main content area.

## WEP

You can use WEP encryption to protect your data when you are transmitting data in the wireless network. There are 3 types of keys: 64 (**WEP64**), 128 (**WEP128**), and 152 (**WEP152**) bits. You can configure up to 4 keys using either **ASCII** or **Hexadecimal** format.

**Key Settings:** For WEP64 and WEP128, you can enter a “Passphrase” (a key of up to 32 alphanumeric characters), choose 64-bit, and press the **Generate** button to generate four WEP64 keys in the entries below, or choose 128-bit, and press the **Generate** button to generate one WEP128 key in the first entry.

Alternatively, and for WEP152, you can manually configure each of them.

When you manually configure a key, the length for a WEP64 key must be equal to 5, for a WEP128 key it must be equal to 13, and for a WEP152 key it must be equal to 16. Once you enable the WEP function, please make sure that exactly the same WEP key is configured in both the Wireless Router and client stations.

You can define a key using ASCII or hex characters. A WEP128 ASCII key looks like "An ASCII key!" (13 characters), while a WEP64 hex key looks like "44-12-24-A8-B2" (5 bytes) and "11-22-33-44-55-66-77-88-99-00-A3-BB-2C" as WEP128 hex key. Each set of hexadecimal numbers should be separated by “-”(dash).

**Key Index:** You have to specify which of the four keys will be active.

Please note that some Wireless Client Cards allow hexadecimal characters only.

Select Security Policy:
WEP

**Encryption**  
 Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.

Passphrase
for
☒ 64 bit
☐ 128 bit

GENERATE

**Select one of the WEP keys for the wireless network:**  

Encrypt data transmitting with WEP Key 1

WEP Key 1

WEP64-ASCII

WEP Key 2

WEP64-ASCII

WEP Key 3

WEP64-ASCII

WEP Key 4

WEP64-ASCII

WEP64-ASCII

WEP64-Hex

WEP128-ASCII

WEP128-Hex

WEP152-ASCII

WEP152-Hex

BACK

NEXT

**NOTE:** To access the wireless network, you must have correct SSID and encryption key, if enabled.

## WPA-PSK

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.

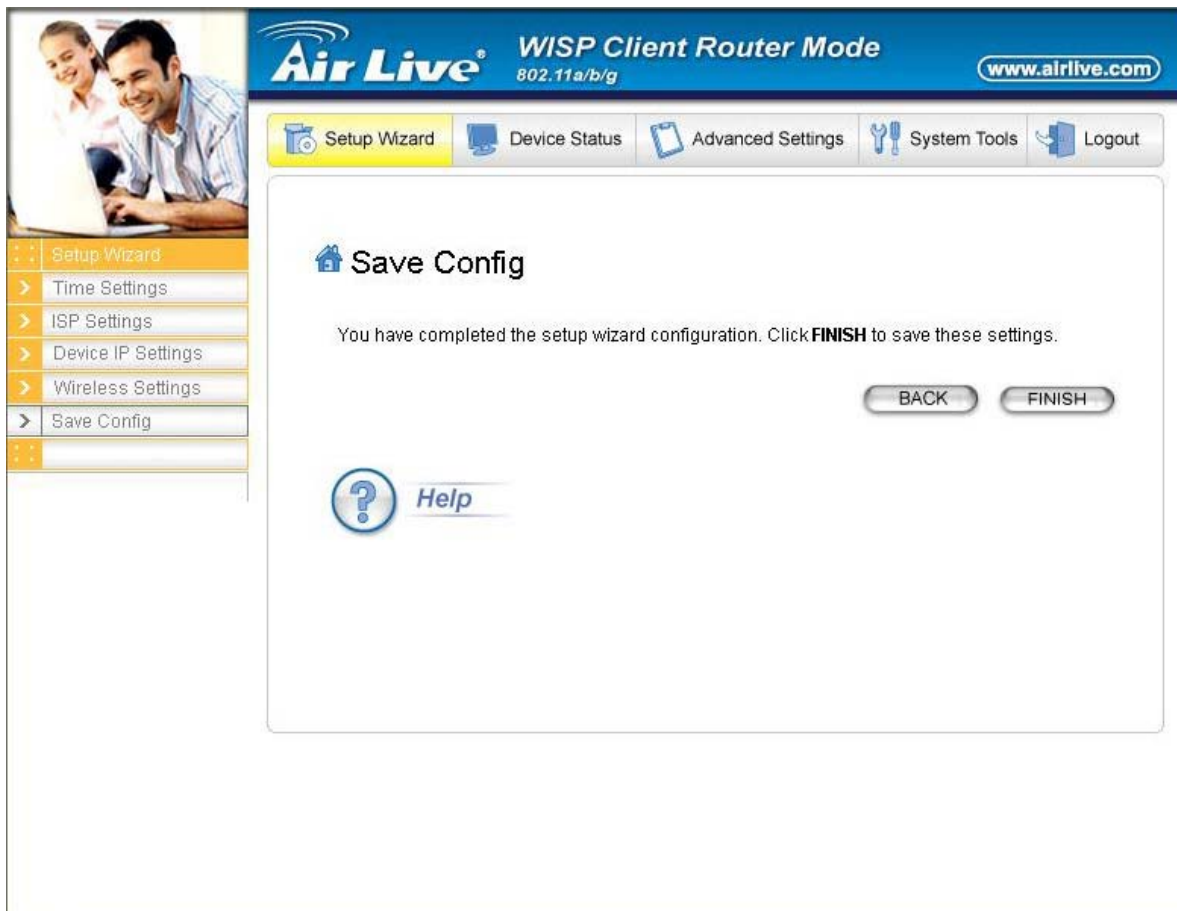
## WPA2-PSK

WPA2 is an improvement on the WPA-PSK standard, and is simply using a shared password for access to the network..



## FINISH SETUP WIZARD AND SAVE YOUR SETTINGS

After stepping through the Wizard's pages, you can press the **FINISH** button for your modification to take effect. This will also cause your new settings to be saved into your system permanently.



Alternatively, you can also click the “BACK” button to go back to previous configuration screens for more changes.



**Note:** If you change the router’s IP address to a different IP network address space, as soon as you click on **FINISH** you will no longer be able to communicate with your WLA-5000AP. You need to change your IP address and then re-boot your computer in order to resume the communication.

## Chapter

# 4

## Advanced Settings

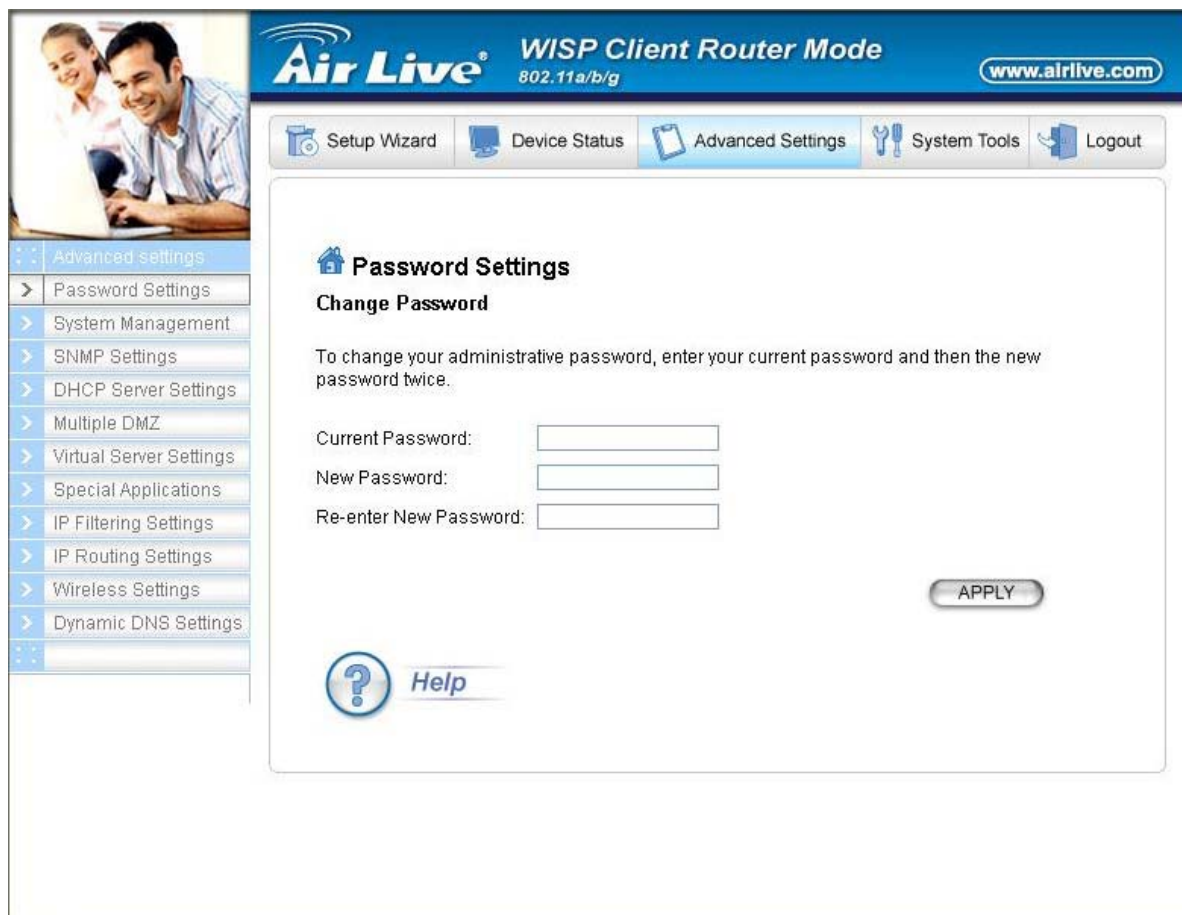
This section contains advanced setting procedures for the WLA-5000AP. It describes modifications that normally you may not need for basic system operation. One exception is changing your password: it is highly recommended that you change the default factory setting as soon as you start to use your WLA-5000AP

## Password Settings

Your WLA-5000AP comes with a default factory password of “**airlive**”. After you start using the AP, you should change the default password.

To change the password, press the **Password Settings** button to enter the **Password Settings** screen, enter the current password followed by the new password twice. The entered characters will appear as asterisks.

If you forgot the password, the only way to recover it is to return the device to its default state as shipped from the factory. To restore the password to the default password, please refer to the section, "What if I forgot the Password?" in the user manual.



The screenshot displays the web interface of an Air Live WISP Client Router. The top header features the "Air Live" logo, the text "WISP Client Router Mode 802.11a/b/g", and the website "www.airlive.com". A navigation bar includes links for "Setup Wizard", "Device Status", "Advanced Settings", "System Tools", and "Logout". On the left, a sidebar menu lists various settings categories, with "Advanced settings" expanded to show "Password Settings", "System Management", "SNMP Settings", "DHCP Server Settings", "Multiple DMZ", "Virtual Server Settings", "Special Applications", "IP Filtering Settings", "IP Routing Settings", "Wireless Settings", and "Dynamic DNS Settings". The main content area is titled "Password Settings" and "Change Password". It provides instructions: "To change your administrative password, enter your current password and then the new password twice." Below this are three input fields labeled "Current Password:", "New Password:", and "Re-enter New Password:". An "APPLY" button is located to the right of these fields. At the bottom left of the main area is a "Help" link with a question mark icon.

## System Management

Clicking the **System Management** button allows system related parameters to be configured for the WLA-5000AP.

**Remote Management:** The remote management feature allows you to manage your WLA-5000AP remotely through the use of an HTTP browser.

The system allows you to (1) **allow remote management from all WAN IP addresses**, to (2) **allow remote management from up to two WAN IP addresses**, or to (3) **disallow remote management from any WAN IP addresses**.

**System Administration:** The router allows you to designate special port numbers other than the standard 80 for **http** for remote management. It also allows you to specify the duration of idle time (inactivity) before a web browser session times out. The default time-out value is 10 minutes.

**UPnP:** The router's Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover the router and automatically show an icon in the task bar on the screen. You can double-click the icon to access the router directly (without having to specify its IP address).

**Disable Ping:** "Ping" is a utility for testing the connectivity. Response to a ping can be disabled, such as when you do not want the router to be accessed (e.g., attacked) from the Internet.

**Syslog:** Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the WLA-5000AP encounters an error or warning condition (e.g., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the **Enable Syslog** box, configure the IP address of a PC where a Syslog daemon is running in the background. When doing so, the WLA-5000AP will send logged events over the network to the PC for future viewing.

**Syslog server IP address:** The IP address of the PC where the Syslog daemon is running.

---



Setup Wizard



Device Status



Advanced Settings



System Tools



Logout

- Advanced settings
- Password Settings
- System Management**
- SNMP Settings
- DHCP Server Settings
- Multiple DMZ
- Virtual Server Settings
- Special Applications
- IP Filtering Settings
- IP Routing Settings
- Wireless Settings
- Dynamic DNS Settings

## System Management

### Remote Management

- ☐ Allow management from all remote IP addresses
- ☐ Allow remote management for only 2 WAN IP addresses

Remote management IP address 1:

Remote management IP address 2:

- ☒ Deny remote management from all WAN IP addresses

### System Administration

HTTP Port No.:  timeout:  minutes

### UPnP

- ☒ Enable UPnP

### Disable Ping

- ☒ Disable ping from Internet

## SNMP Settings

This screen allows you to configure SNMP parameters including the system name, the location and contact information. Additionally, you can configure the WLA-5000AP to send SNMP Traps to remote SNMP management stations. Traps are unsolicited alert messages that WLA-5000AP sends to remote management stations.

The screenshot shows the 'SNMP Settings' page in the Air Live WISP Client Router Mode. The page has a blue header with the 'Air Live' logo, 'WISP Client Router Mode', '802.11a/b/g', and the website 'www.airlive.com'. A navigation bar includes 'Setup Wizard', 'Device Status', 'Advanced Settings', 'System Tools', and 'Logout'. A left sidebar lists various settings categories, with 'SNMP Settings' highlighted. The main content area is titled 'SNMP Settings' and contains the following sections:

- Enable SNMP:** A checkbox labeled 'Enable SNMP' is checked.
- Assign system information:** Three input fields are provided: 'System Name' (containing 'AirRDRA-81'), 'System Location' (containing 'Input System Location'), and 'System Contact' (containing 'Input Contact Person').
- Assign the SNMP community string:** Two input fields are provided: 'Community String For Read' (containing 'public') and 'Community String For Write' (containing 'private').
- Assign a specific name and IP address for your SNMP trap manager:** Two input fields are provided: 'Name' and 'IP Address'.

An 'APPLY' button is located at the bottom right of the main content area.

**System Name:** A name that you assign to your WLA-5000AP. It is an alphanumeric string of up to 30 characters.

**System Location:** Description of where your WLA-5000AP is physically located. It is an alphanumeric string of up to 60 characters.

**System Contact:** Contact information for the system administrator responsible for managing your WLA-5000AP. It is an alphanumeric string of up to 60 characters.

**Community String For Read:** If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.

**Community String For Write:** For read-write operation, you need to configure a write “community string”.

A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

You can define trap managers in the system.

You can add a trap manager by entering a **name**, an **IP address**, followed by pressing the **ADD** button.

You can delete a trap manager by selecting the corresponding entry and press the **DELETE SELECTED** button.

You enable a trap manager by checking the **Enable** box in the corresponding entry or disable the trap manager by un-checking the **Enable** box.

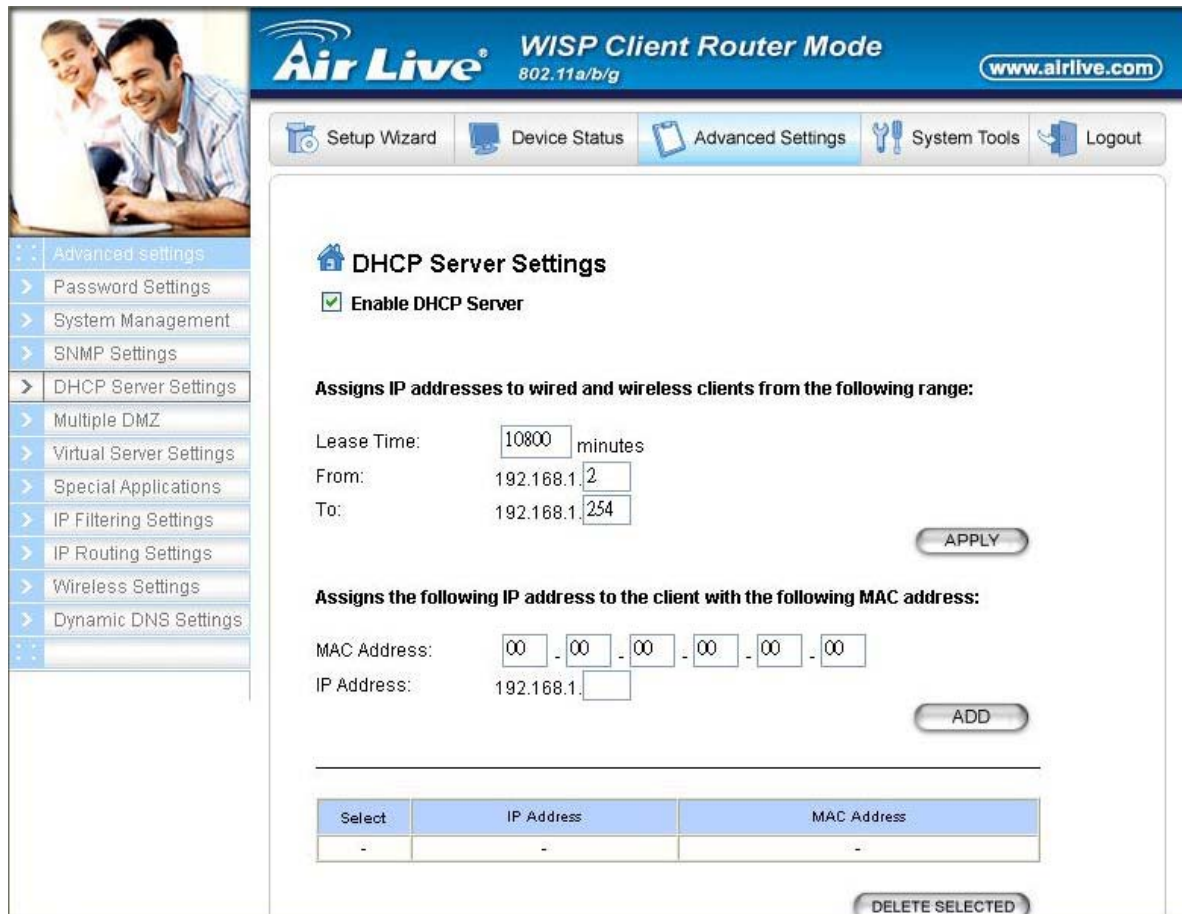
---



## DHCP Server Settings

The DHCP server option allows the WLA-5000AP to assign IP addresses to DHCP client devices on your wired or wireless LAN to obtain IP addresses automatically.

If you want the Router to act as a DHCP server and assign private IP addresses to requesting DHCP clients on the LAN, you need to check the **Enable DHCP Server** box.



The screenshot shows the 'Air Live' WISP Client Router Mode interface. The top navigation bar includes 'Setup Wizard', 'Device Status', 'Advanced Settings' (selected), 'System Tools', and 'Logout'. A left sidebar lists various settings, with 'DHCP Server Settings' highlighted. The main content area is titled 'DHCP Server Settings' and features a checked 'Enable DHCP Server' option. Below this, it states 'Assigns IP addresses to wired and wireless clients from the following range:' and provides input fields for 'Lease Time' (10800 minutes), 'From' (192.168.1.2), and 'To' (192.168.1.254), followed by an 'APPLY' button. The next section, 'Assigns the following IP address to the client with the following MAC address:', includes fields for 'MAC Address' (00-00-00-00-00-00) and 'IP Address' (192.168.1.), with an 'ADD' button. At the bottom, a table with columns 'Select', 'IP Address', and 'MAC Address' is shown, containing a single row with dashes. A 'DELETE SELECTED' button is located at the bottom right.

**Air Live® WISP Client Router Mode** 802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status **Advanced Settings** System Tools Logout

Advanced settings  
Password Settings  
System Management  
SNMP Settings  
**DHCP Server Settings**  
Multiple DMZ  
Virtual Server Settings  
Special Applications  
IP Filtering Settings  
IP Routing Settings  
Wireless Settings  
Dynamic DNS Settings

**DHCP Server Settings**

☒ **Enable DHCP Server**

**Assigns IP addresses to wired and wireless clients from the following range:**

Lease Time: 10800 minutes  
From: 192.168.1.2  
To: 192.168.1.254 **APPLY**

**Assigns the following IP address to the client with the following MAC address:**

MAC Address: 00 - 00 - 00 - 00 - 00 - 00  
IP Address: 192.168.1. **ADD**

Select	IP Address	MAC Address
-	-	-

**DELETE SELECTED**

You can select one of the following two ways to assign IP addresses:

**Assigns IP addresses to wired or wireless clients from the following range:**

When IP addresses are assigned to a requesting DHCP client, after the “**lease time**”, the client is expected to renew the lease. Its default value is 10080 minutes.

The **from** and **to** range of IP addresses to be assigned to requesting DHCP clients can be configured manually, with the default being 2 to 254.

After you enter the information, you should press **APPLY**.

**Assigns the following IP address to the client with the following MAC address:**

You can also specify the **IP address** to be assigned to a device with a pre-configured **MAC address**.

You can add such a mapping by entering a MAC address, and the IP address to be assigned, followed by pressing the **ADD** button. Up to 20 mappings can be added.

You can delete a mapping by **selecting** the corresponding entry and press the **DELETE SELECTED** button.

**DHCP Table:** Press this button will cause the screen to jump to DHCP client table page.

## Multiple DMZ

The router supports multiple software DMZ ports, and they are implemented through software.

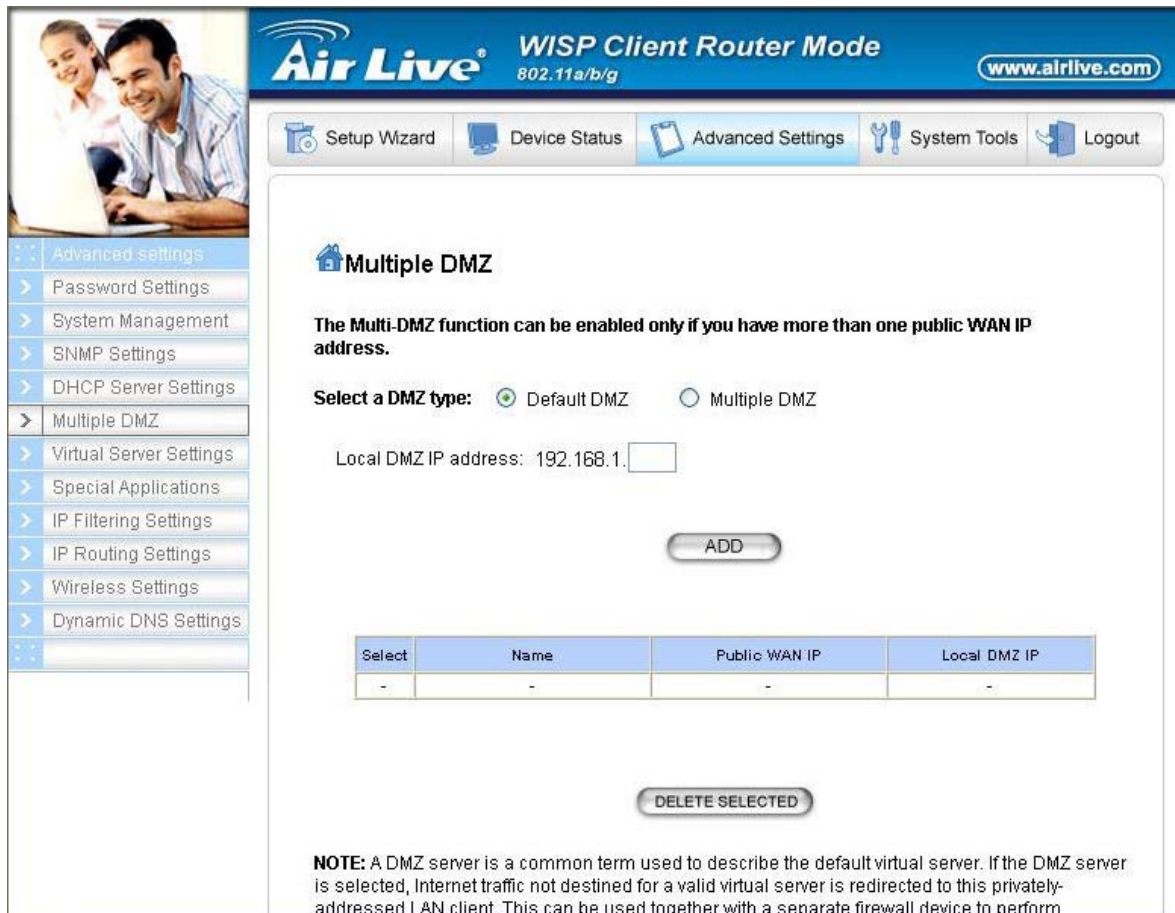
When the router receives incoming data from the Internet, it will search through an internal address translation table to perform address translation function. If a match can be found, the data will be forwarded to the corresponding device in your local LAN, otherwise the data will be dropped or forwarded to the default DMZ if it is configured.

An additional feature is to allow devices with WAN IP addresses to be used by the Internet users to access private devices in your local LAN. In this case, you need to configure the mapping between the WAN IP address and the private IP address.

To add the default DMZ, you need to select “**Default DMZ**” and enter the **local DMZ IP address**, followed by pressing the **ADD** button.

To add a device for multiple DMZ, first select “**Multiple DMZ**”, add a mnemonic name, a **public WAN IP address**, and the **local DMZ IP** address on the LAN, followed by pressing the **ADD** button.

You can delete a DMZ entry by selecting the corresponding entry and press the **DELETE SELECTED** button.



The screenshot shows the web interface of an Air Live WISP Client Router. The top navigation bar includes links for Setup Wizard, Device Status, Advanced Settings (which is highlighted), System Tools, and Logout. A sidebar on the left lists various configuration options, with 'Multiple DMZ' selected. The main content area is titled 'Multiple DMZ' and contains the following elements:

- A warning message: "The Multi-DMZ function can be enabled only if you have more than one public WAN IP address."
- DMZ type selection: Two radio buttons are present, 'Default DMZ' (selected) and 'Multiple DMZ'.
- Local DMZ IP address: A text input field containing '192.168.1.' followed by an empty box for the last octet.
- An 'ADD' button.
- A table with four columns: 'Select', 'Name', 'Public WAN IP', and 'Local DMZ IP'. The table currently contains one row with dashes in all four columns.
- A 'DELETE SELECTED' button.
- A note at the bottom: "NOTE: A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately-addressed LAN client. This can be used together with a separate firewall device to perform".

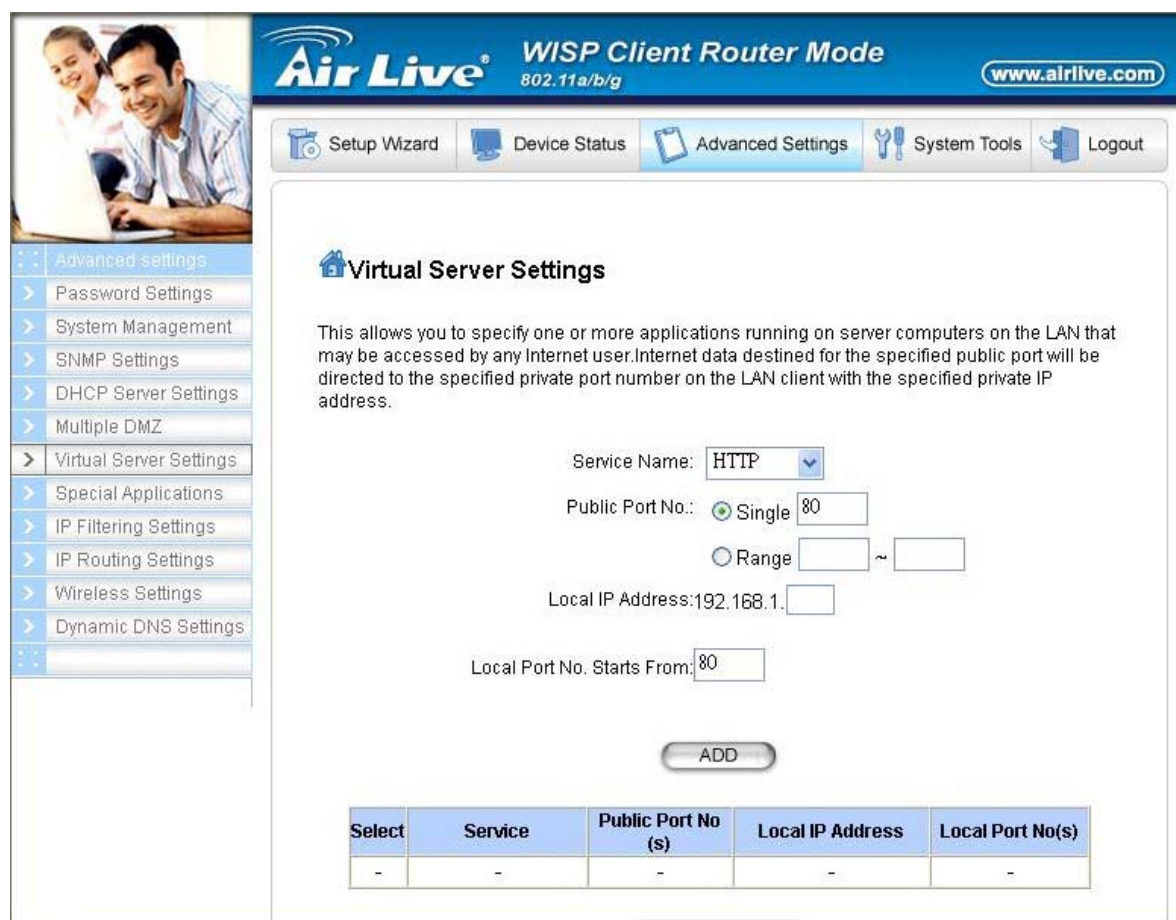
## Virtual Server Settings

A Virtual Server is a server built on a single or a cluster of real servers. A DMZ server is a term commonly used to describe the default Virtual Server - the router will redirect all traffic from the Internet without a valid port address mapping to this device. An HTTP server with a private IP address on the LAN allows access from the Internet by mapping a special port to the HTTP server. In this case, the HTTP service will be mapped to a special port of the Router.

You can add a virtual server mapping by (1) selecting the **service name** (such as HTTP, FTP, TELNET, SMTP, POP3, CUSTOM), (2) enter the **public port number** to be used (either a **single** port number or a **range**), (3) enter the **local IP address** of the server on your LAN, (4) enter its **local port number** to map to (either a single port number or the starting port number of a range), (5) followed by pressing the **ADD** button.

You can delete a mapping by **selecting** the corresponding entry and press the **DELETE SELECTED** button.

**Note:** Virtual Server Setting and IP Filtering may affect with each other.



**Air Live** WISP Client Router Mode  
802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status Advanced Settings System Tools Logout

Advanced settings  
Password Settings  
System Management  
SNMP Settings  
DHCP Server Settings  
Multiple DMZ  
Virtual Server Settings  
Special Applications  
IP Filtering Settings  
IP Routing Settings  
Wireless Settings  
Dynamic DNS Settings

### Virtual Server Settings

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

Service Name: HTTP

Public Port No.: ☒ Single 80 ☐ Range ~

Local IP Address: 192.168.1.

Local Port No. Starts From: 80

ADD

Select	Service	Public Port No (s)	Local IP Address	Local Port No(s)
-	-	-	-	-

## Special Applications

Special applications such as some Internet games are getting to be increasingly popular. These applications usually work in the following manner:

A client can start an Internet game by first registering with a game server on the Internet. Other clients can, using the corresponding protocol, join the game by checking with the server and deciding if to join the game. A client can "leave" the game at any time.

If the initiating client is behind your router, you need to add the application by performing the following configuration:

**Select an application:** Select an application that you want to add to the supported list. You should choose "Other" if your application is not explicitly shown in the list.

**Name:** You can provide a mnemonic name.

**Trigger Port:** You need to specify, based on instructions provided by your application's user manual, the (UDP/TCP) port number in the router that the initiating client uses to start an Internet game.

**Trigger Type:** Select UDP, TCP, or both for the trigger port.

**Opened ports:** You need to specify the port numbers in the router that joining clients can use to communicate with the initiating client, again based on instructions provided by your application user manual.

**Public Type:** Select UDP, TCP, or both for the Opened ports.

After you finish the above, you press the **ADD** button to add an entry to the table.

You can delete an entry by **selecting** the corresponding entry and press the **DELETE SELECTED** button.

---

**Air Live® WISP Client Router Mode**  
802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status Advanced Settings System Tools Logout

**Special Applications**

Some Internet applications such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through. Before you set up special application, please see your applications' help for such information.

Select an Application: -- select one --

Name:

Trigger Ports:

Trigger Protocol: BOTH

Opened Ports:

Opened Protocol: BOTH

ADD

Select	Name	Trigger Port	Trigger Protocol	Opened Ports	Opened Protocol
-	-	-	-	-	-

## IP Filtering Settings

Three mutually exclusive rules can be defined to forward/filter IP packets based on their IP address and/or port numbers.

- **Disable IP filtering:** If this is selected, the IP filtering feature is disabled. No IP filtering will be performed.
- **GRANT IP access:** When this is elected, packets received from/transmitted to WAN with specified (source or destination) IP addresses will be allowed/forwarded.
- **DENY IP access:** Packets received from/transmitted to WAN with the specified IP addresses will be denied/filtered.

Once a choice is made, the choice applies to all filtering rules.

To define/add an IP filtering rule, enter the following information

- **Name:** The name of the filter
- **IP Protocol:** TCP or UDP

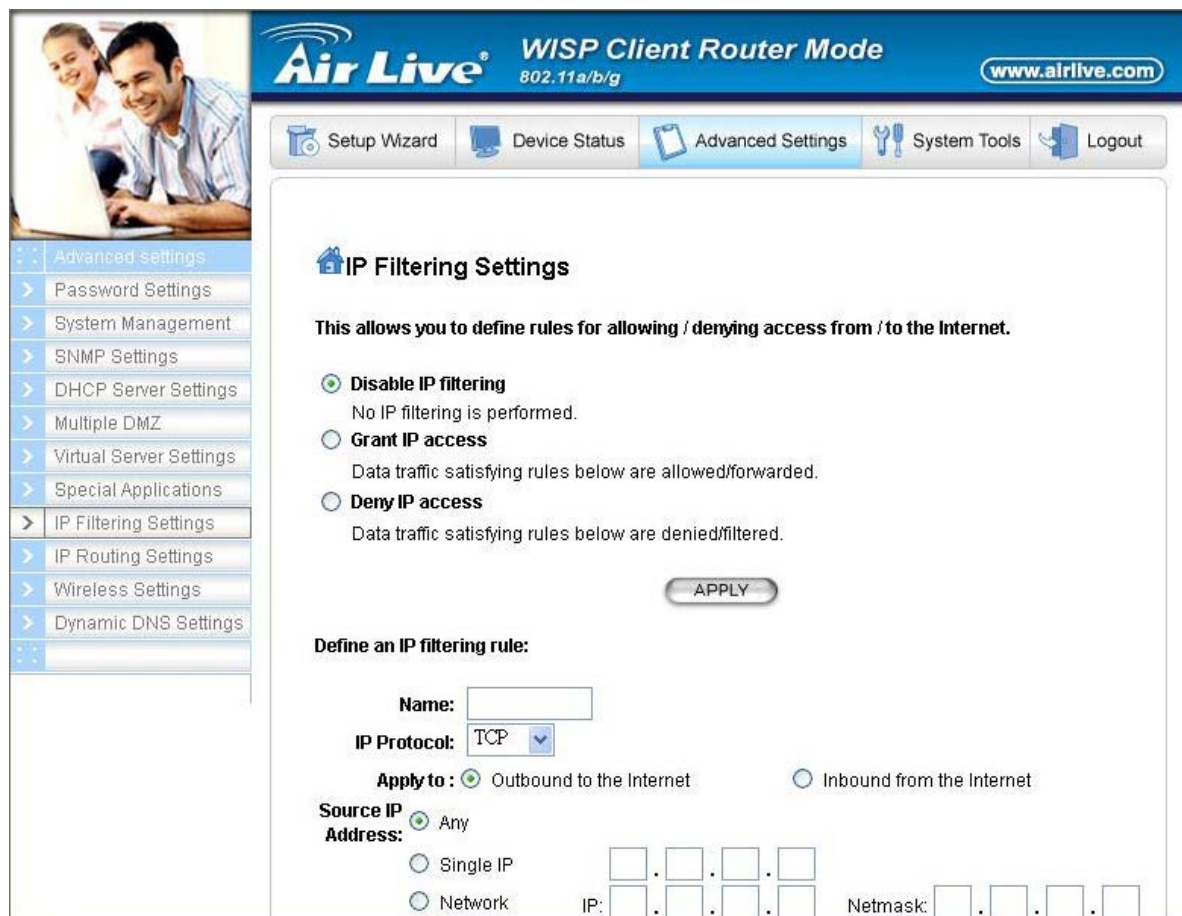


- **Apply to:** You need to select whether the filtering rule should apply to packets outbound for the Internet or inbound from the Internet.
- **Source IP address:** you can select **Any**, **Single IP**, or a **Network** (of source IP addresses).
- **Source Port:** you can select **Any**, **Single**, or a **Range** of port numbers.
- **Destination IP address:** **Any**, **Single IP**, or a **Network** (of destination IP addresses).
- **Destination Port:** you can select **Any**, **Single**, or a **Range** of port numbers.

After you finish the above, you press the **ADD** button to add the entry to the table. There are up to 32 IP filtering rules could be configured.

You can delete an entry by selecting the corresponding entry and press the **DELETE SELECTED** button.

Please Note that IP filtering is a sophisticated feature that can severely impact your Router operation. Please be sure that you fully understand it before you use this feature. If you make any mistakes, it can produce dramatic and potentially undesirable results.



The screenshot shows the web interface of an Air Live WISP Client Router. The top header includes the 'Air Live' logo, 'WISP Client Router Mode', the version '802.11a/b/g', and the website 'www.airlive.com'. A navigation bar contains links for 'Setup Wizard', 'Device Status', 'Advanced Settings' (which is highlighted), 'System Tools', and 'Logout'. On the left, a sidebar menu lists various settings: 'Advanced settings', 'Password Settings', 'System Management', 'SNMP Settings', 'DHCP Server Settings', 'Multiple DMZ', 'Virtual Server Settings', 'Special Applications', 'IP Filtering Settings' (which is selected), 'IP Routing Settings', 'Wireless Settings', and 'Dynamic DNS Settings'. The main content area is titled 'IP Filtering Settings' and includes a description: 'This allows you to define rules for allowing / denying access from / to the Internet.' There are three radio button options: 'Disable IP filtering' (selected), 'Grant IP access', and 'Deny IP access'. Below these are descriptions for each. An 'APPLY' button is present. The 'Define an IP filtering rule:' section contains a 'Name' text box, an 'IP Protocol' dropdown menu set to 'TCP', and an 'Apply to' section with two radio buttons: 'Outbound to the Internet' (selected) and 'Inbound from the Internet'. The 'Source IP Address' section has three radio buttons: 'Any' (selected), 'Single IP', and 'Network'. Below these are IP address input fields: a single IP field for 'Single IP' and IP/Netmask fields for 'Network'.

## *IP Routing Settings*

**Dynamic Routing:** enable gateway to exchange the routing table dynamically through LAN port. Currently you can choose to use RIPv1 or RIPv2 with Send enabled (active mode) or disabled (passive mode).

**Static Routing:** If you have routers on your LAN or WAN, you can configure static routes on the a/g Router to route network traffic to a specific, predefined destination. The WLA-5000AP routes packets based only on the packet's destination not on the source of a packet.

Static Routes are configured when network traffic is directed to a specific destination on the network whether it is the LAN or WAN. For instance, you can configure the WLA-5000AP to route traffic destined to a particular network to a specific router on the LAN or WAN using the following steps:

1. Enter the IP address of the destination network in the Destination Network field.
2. Enter the subnet in the Subnet Mask field.
3. Enter the IP address of the specific router in the Gateway IP Address field.
4. Select LAN or WAN, where is the specific router is, from the Interface menu.
6. Click Add.

**IP Routing Table:** The Routing Table shows a list of destinations that the IP software maintains on each host and router. The destination network IP address, subnet mask, gateway address, and the corresponding interface are displayed.

**Note:** The WLA-5000AP can support up to 128 static route entries.

---



**Air Live® WISP Client Router Mode**  
802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status Advanced Settings System Tools Logout

**IP Routing Settings**

**Dynamic Routing**

Select the routing protocol scheme used for the router's LAN port.

☒ Disable  
☐ RIP

APPLY

**Static Routing**

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

Destination IP Address:  0  0  0  0  
Subnet Mask:  0  0  0  0  
☒ Gateway IP Address:  0  0  0  0  
☐ Interface:  lan

## Wireless Settings

You can use this screen to configure various parameters of your WLA-5000AP.

**Beacon Interval:** The WLA-5000AP broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted - in time unit of milliseconds. Its default value is 100; a valid value should be between 20 and 1000.

**RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than the specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 0 and 2347 bytes, with a default value of 2347. A value of zero activates the RTS/CTS handshake before every transmission. It is recommended that this value does not deviate from the default too much.

**Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, the frame will be fragmented before transmission. The threshold should have a value of 256-2346 bytes, with a default value of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

**DTIM Interval:** The WLA-5000AP buffers packets for stations that operate in the power-saving mode. A Delivery Traffic Indication Message (DTIM) contains information on which power-conserving stations have packets waiting to be received. The DTIM interval specifies how often beacon frames should contain DTIMs. It should have a value between 1 and 255, with a default value of **3**.

**Air Live® WISP Client Router Mode**  
802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status Advanced Settings System Tools Logout

**Wireless Settings**

RTS Threshold :  bytes (range: 0-2347, default 2347)

Fragmentation :  bytes (range: 256-2346, default 2346)

Transmit Power :  dBm (range: 0-20, default 20)

AckTimeOut (11a):  (range: 10-255, default 25)

AckTimeOut (Turbo-11a):  (range: 10-255, default 22)

AckTimeOut (11g):  (range: 10-255, default 48)

AckTimeOut (Turbo-11g):  (range: 10-255, default 22)

## Dynamic DNS Settings

Some people advertise the IP addresses of their routers so that Internet users can access these routers (which is actually to access virtual servers behind these routers) using these IP addresses. However, for those routers that are assigned dynamic IP addresses from the ISP, this approach requires additional work (since the addresses assigned are not always the same).

The WLA-5000AP implements the dynamic DNS feature so that each time it is booted, it will re-register its domain-name-to-IP-address mapping with the dynamic DNS server you use (currently only DynDNS.org is supported), the service provider that provides domain name to IP address mapping. This is so that you can advertise your router by providing your domain name, while Internet users can access the router using the domain name, not the router's IP address.

To activate this feature, you need to check the “**Enable Dynamic DNS Client using DynDNS.org**” box first, and then configure the following parameters:

**Hostname:** the hostname (domain name) registered with DynDNS.org by you.

**Username:** the username required to log in to the domain name server maintained by DynDNS.org.

**Password:** the password required to log in to the domain name server maintained by DynDNS.org.



WISP Client Router Mode  
802.11a/b/g

[www.airlive.com](http://www.airlive.com)



Setup Wizard



Device Status



Advanced Settings



System Tools



Logout

- Advanced settings
- > Password Settings
- > System Management
- > SNMP Settings
- > DHCP Server Settings
- > Multiple DMZ
- > Virtual Server Settings
- > Special Applications
- > IP Filtering Settings
- > IP Routing Settings
- > Wireless Settings
- > Dynamic DNS Settings



## Dynamic DNS Settings

☐ Enable Dynamic DNS Client using [DymDNS.org](http://DymDNS.org)

Hostname:

Username:

Password:

APPLY



Help

## Chapter

# 5

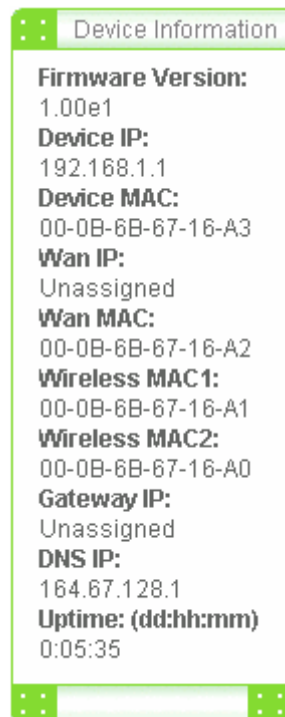
## Managing your WLA-5000AP

This Chapter covers other management aspects of your WLA-5000AP:

- How to view the device status
- How to view the system log
- How to upgrade your WLA-5000AP firmware
- How to save or restore configuration changes
- How to reboot your WLA-5000AP
- What if you forgot the password

### *How to View the device Status*

You can monitor the system status and get general device information from the **Device Information** screen:



## How to View the System Log

The WLA-5000AP maintains a system log that you can use to track events that have occurred in the system. Such event messages can sometimes be helpful in determining the cause of a problem that you may have encountered.

You can select System Log on the left to view log events recorded in the system. The System Log entries are shown in the main screen along with the log level, the severity level of messages that are being displayed (a low number such as 2 means critical), and the uptime, the amount of time since the WLA-5000AP was last reset. The maximum number of entries is 128. If there are more than 128 entries, older entries will be deleted.

The screenshot displays the web interface of an Air Live WISP Client Router. The top navigation bar includes links for Setup Wizard, Device Status (highlighted), Advanced Settings, System Tools, and Logout. On the left sidebar, the System Log is selected under the Device Status section. The main content area shows the System Log with a Log Level of 3 (err). The log entries are as follows:

Time	Event
Jan 1 00:00:19	AirRDRA-81 csp: Link Up on interface [lan]
Jan 1 00:00:45	AirRDRA-81 http: Login into the system
Jan 1 00:00:57	AirRDRA-81 csp: Link Up on interface [isp]

Below the log entries is a Help button. On the left sidebar, the Device Information section shows the following details:

- Firmware Version: 1.00e05
- Device IP: 192.168.1.1
- Device MAC: 00-4F-69-50-00-0D
- Wan IP: 172.16.30.146
- Wan MAC: 00-4F-69-50-00-0B
- Uptime: (dd:hh:mm) 0:00:06

## DHCP Client Table

The DHCP client table lists current DHCP clients connected with its host name, IP address, MAC address, expiration time, and entry type.

The screenshot displays the Air Live WISP Client Router Mode web interface. The top navigation bar includes links for Setup Wizard, Device Status (highlighted), Advanced Settings, System Tools, and Logout. The left sidebar contains a menu with options like Device Status, System Log, DHCP Client Table (selected), Bridge Table, Radio Table, and Site Survey. Below the menu is a 'Device Information' box showing details such as Firmware Version, Device IP, Device MAC, Wan IP, Wan MAC, and Uptime.

### DHCP Client Table

**DHCP Server Information :**

DHCP Status :	Enabled	Lease Time :	10800 minutes
Primary DNS :	192.168.1.1	Secondary DNS :	0.0.0.0
Default Gateway :	192.168.1.1		

**DHCP Client List :**


Host Name	IP Address	MAC Address	Expiration Time	Entry Type	Network Type
-	-	-	-	-	-

At the bottom of the DHCP Client List section, there is a 'Help' button with a question mark icon and a '>> DHCP Server' button.

## Bridge Table







The bridge table shows all MAC entries learned from the wired LAN interface, wireless clients, and WDS peers.





**WISP Client Router Mode**  
 802.11a/b/g


[www.airlive.com](#)

[Setup Wizard](#)
[Device Status](#)
[Advanced Settings](#)
[System Tools](#)
[Logout](#)


 Device Status
  System Log
  DHCP Client Table
  Bridge Table
  Radio Table
  Site Survey

 Device Information

**Firmware Version:**  
1.00e05  
**Device IP:**  
192.168.1.1  
**Device MAC:**  
00-4F-69-50-00-0D  
**Wan IP:**  
172.16.30.146  
**Wan MAC:**  
00-4F-69-50-00-0B  
**Uptime: (dd:hh:mm)**  
0:00:07

 **Bridge Table**

MAC Address	Interface
00-00-e2-49-8b-f2	eth0
00-4f-69-50-00-0d	eth0(local)

 [Help](#)

## Radio Table

The radio table shows the information of each radio, including the current mode, channel, number of clients associated, number of packets transmitted and received, and number of errors happened.

**Air Live® WISP Client Router Mode**  
802.11a/b/g [www.airlive.com](http://www.airlive.com)

Setup Wizard Device Status Advanced Settings System Tools Logout

**Radio Table**

Radio Name	Mode	Op Channel	Assoc. Clients	Tx Pkts	Rx Pkts	Error
radio1		11	1	9	306	4780

**Device Information**

Firmware Version: 1.00e05  
 Device IP: 192.168.1.1  
 Device MAC: 00-4F-69-50-00-0D  
 Wan IP: 172.16.30.146  
 Wan MAC: 00-4F-69-50-00-0B  
 Uptime: (dd:hh:mm) 0:00:07

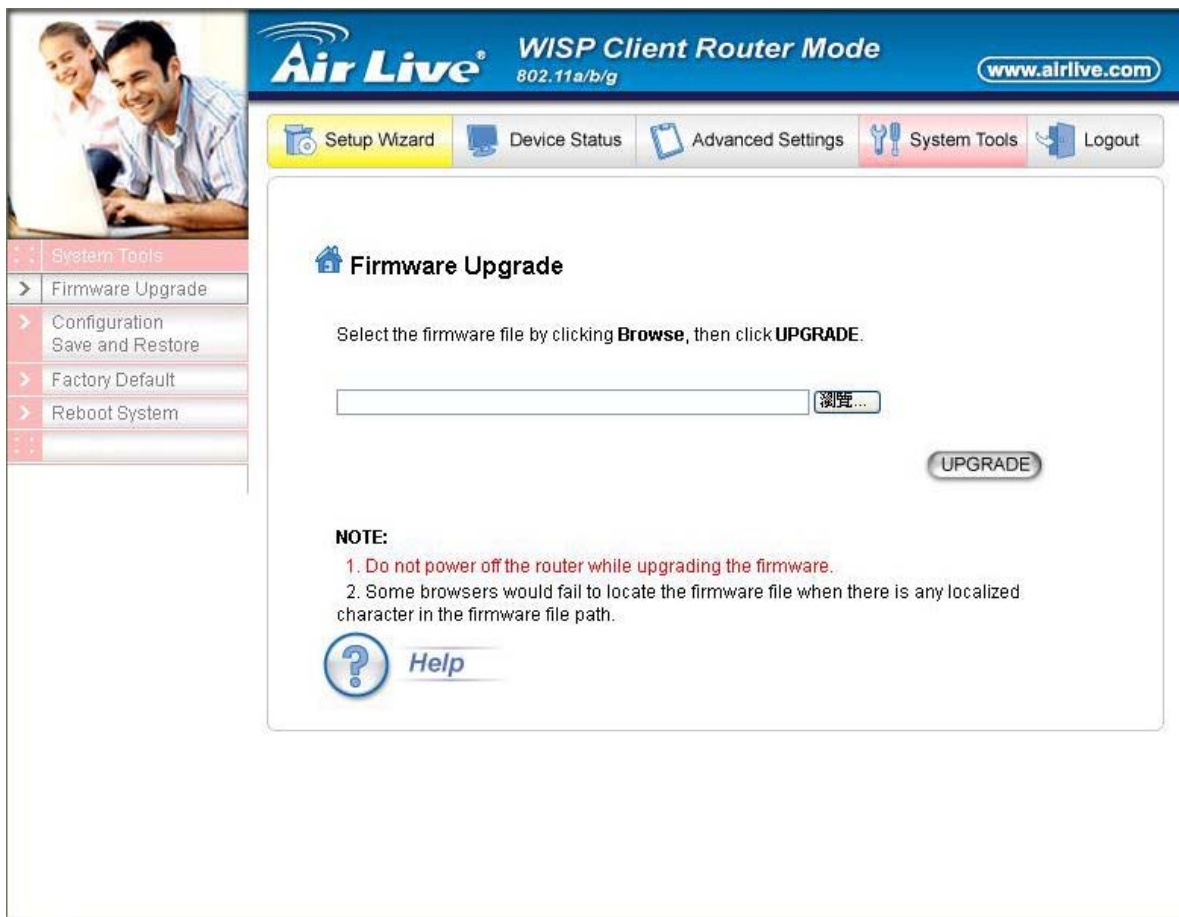
**Help**

## Upgrading Firmware

You can upgrade your WLA-5000AP's firmware (the software that controls your WLA-5000AP's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems you have encountered when using the current version. System upgrade can be performed through the System Upgrade option as follows:

**Step 1** Select **System Tools**, then **Firmware Upgrade** from the menu and the following screen displays:





**Step 2:** To update the WLA-5000AP firmware, first download the firmware from the distributor's web site to your local disk. Then from the above screen enter the path and filename of the firmware (or click **Browse** to select the path and filename of the firmware). Next, Click the **Upgrade** button.

The new firmware will begin loading to your WLA-5000AP. After a message appears telling you that the operation is complete, you need to reset the system to have the new firmware take effect.



---

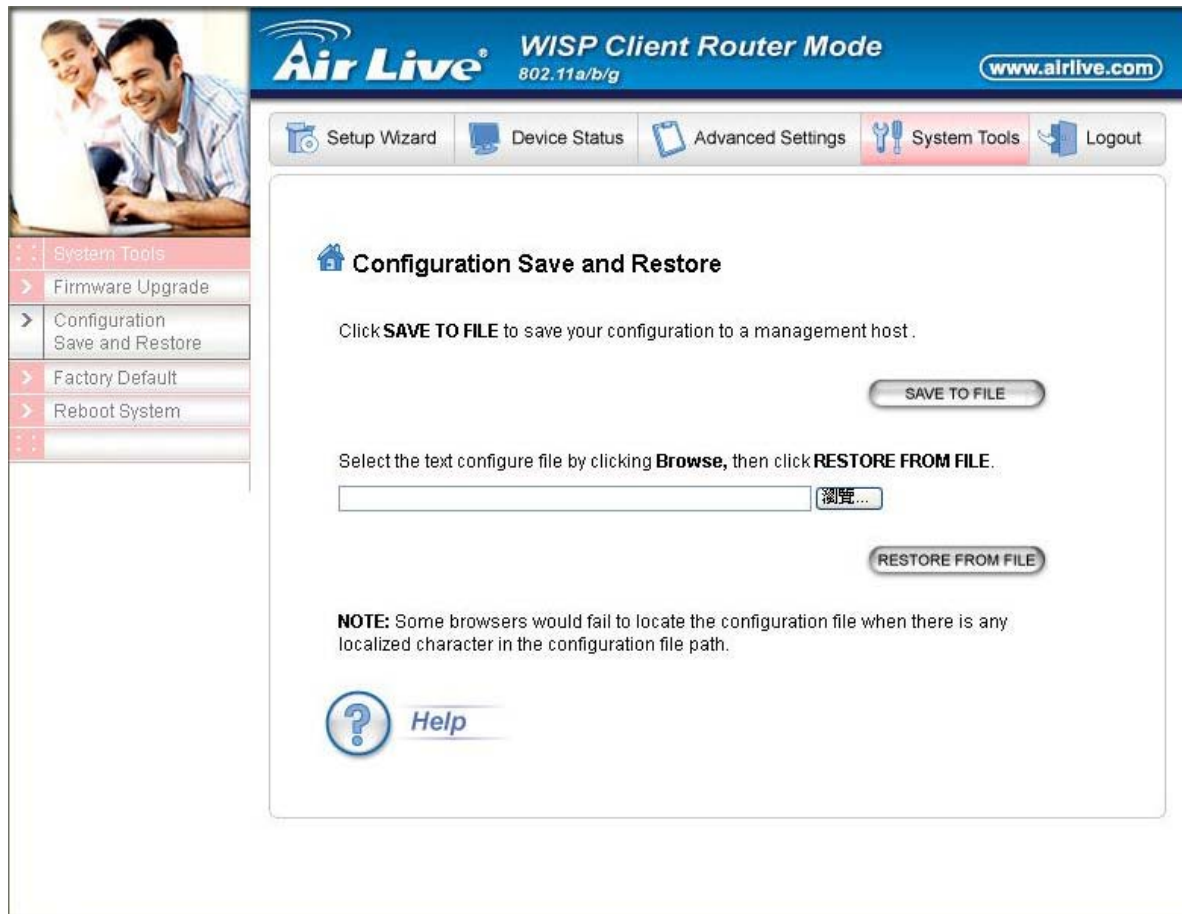
**Note:** It is recommended that you do not upgrade your WLA-5000AP if you are happy with its operation.

---

## How to Save or Restore Configuration Changes

You can save system configuration settings to a file, and later download it back to the WLA-5000AP system by following the steps below.

**Step 1** Select **Configuration Save and Restore** from the **System Tools** menu and the following screen displays:



The screenshot shows the Air Live WISP Client Router Mode web interface. The top header includes the Air Live logo, the text "WISP Client Router Mode 802.11a/b/g", and the website "www.airlive.com". A navigation bar contains links for Setup Wizard, Device Status, Advanced Settings, System Tools (highlighted), and Logout. On the left, a sidebar menu lists System Tools, Firmware Upgrade, Configuration Save and Restore (highlighted), Factory Default, and Reboot System. The main content area is titled "Configuration Save and Restore" and contains the following instructions and controls:

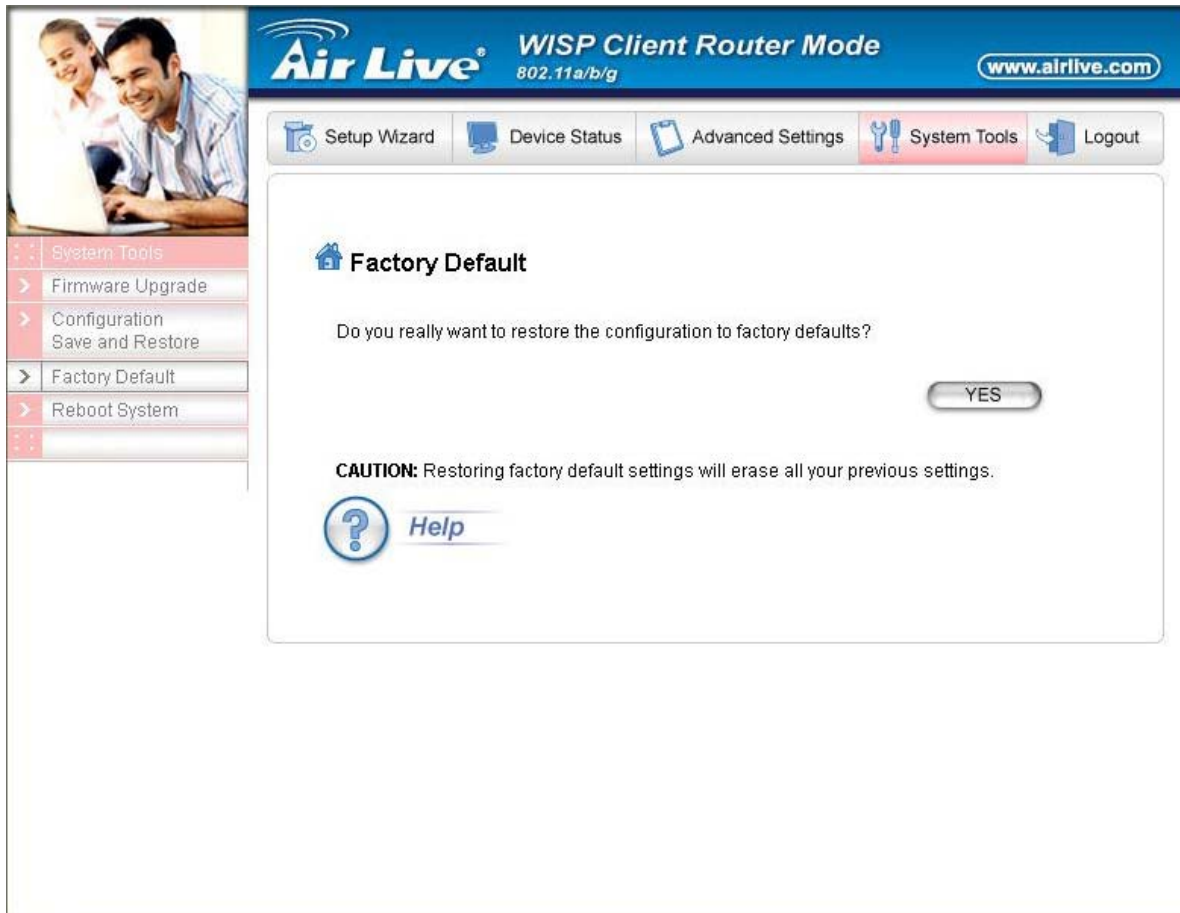
- Click **SAVE TO FILE** to save your configuration to a management host.
- Select the text configure file by clicking **Browse**, then click **RESTORE FROM FILE**.
- A text input field for the file path is shown with a "浏览..." (Browse...) button next to it.
- A **RESTORE FROM FILE** button is located below the input field.
- A **NOTE** states: "Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path."
- A **Help** link with a question mark icon is at the bottom left.

**Step 2** Click **SAVE TO FILE** and then select a local file to save to, or click **RESTORE FROM FILE** and then select a local file to upload.

## How to Restore the System Settings to the Factory Defaults

You can restore the system settings to the factory defaults.

**Step 1** Select **Factory Default** from the **System Tools** menu and the following screen displays:

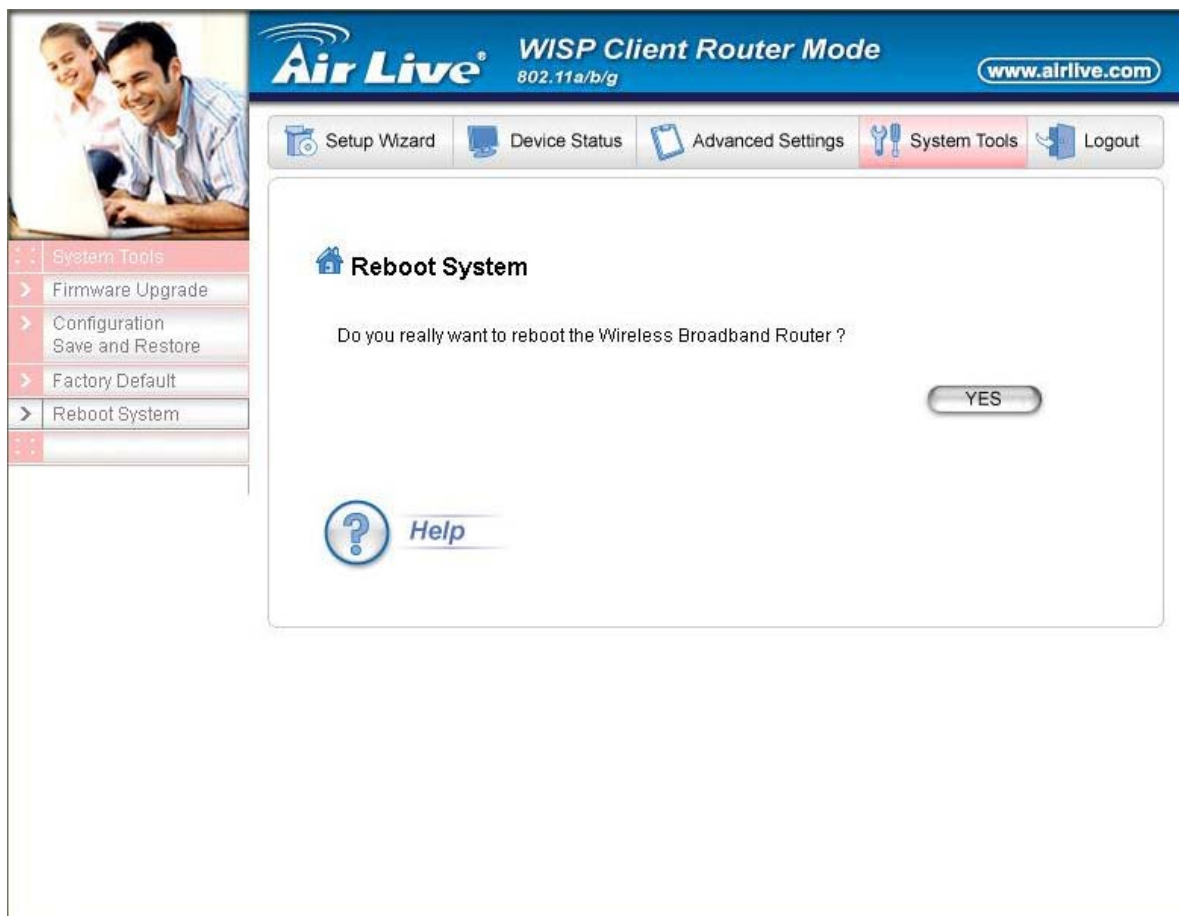


**Step 2** Click **YES** to restore the system configurations to the factory defaults, and the system will re-boot automatically.

## How to Reboot your WLA-5000AP

You can reset your WLA-5000AP from the Brower. To reset it:

**Step 1** Select **Reboot System** from the **System Tools** menu, the following screen shows:



**Step 2** Click **YES** to reset the WLA-5000AP.



---

**Note:** Resetting the WLA-5000AP disconnects any active clients, and therefore will disrupt any current data traffic.

---

## ***What if you Forgot the Password?***

If you forgot the password, the only way to recover is to clear the device configuration and return the unit to its original state as shipped from the factory. You can do this by pressing the hardware “re-store” button on the device for “**2 seconds**”. Please note that this will require you to re-enter all of your configuration data.

## Specification

<b>Product Name</b>	IEEE 802.11a/g Wireless LAN AP (WISP Client Router mode)
<b>OS</b>	Linux® 2.4.18 kernel
<b>Standard</b>	<ul style="list-style-type: none"> <li>• IEEE 802.11a</li> <li>• IEEE 802.11b</li> <li>• IEEE 802.11g</li> <li>• IEEE 802.1x</li> <li>• IEEE 802.3u</li> </ul>
<b>WLAN Network Architecture Type</b>	<ul style="list-style-type: none"> <li>• Infrastructure</li> <li>• Bridge Mode (WDS)</li> </ul>
<b>Wireless Transfer Data Rate for IEEE 802.11a Draft Standard</b>	IEEE 802.11a Standard: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps with auto fallback
<b>Wireless Transfer Data Rate for IEEE 802.11g Draft Standard</b>	IEEE 802.11g Standard: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps with auto fallback
<b>Wireless Transfer Data Rate for IEEE 802.11b</b>	11, 5.5, 2 & 1 Mbps with auto fallback
<b>Physical Specification</b>	<ul style="list-style-type: none"> <li>• External Power Adapter with DC5v/2A Input</li> <li>• Dimension: 164.3(L) x 170(W) x 36.5(H) mm</li> <li>• Desktop Installation</li> <li>• Wall/Ceiling Mountable</li> </ul>
<b>Hardware &amp; Antenna</b>	<ul style="list-style-type: none"> <li>• 3 x RJ45 (4x 10/100 Mbps Ethernet Switch Auto MDI/MDI-X) for LAN ports</li> <li>• 1 x RJ45 for WAN</li> <li>• 1 x RJ45 for DMZ</li> <li>• 1 x Reset Button</li> <li>• 2x External Antenna</li> <li>• 9 x LED: 1 x Power; 1 x Diag; 1 x WLAN; 1 x WAN (LINK/ACT); 4 x LAN (LINK/ACT); 1 x DMZ (LINK/ACT)</li> </ul>
<b>DHCP Server</b>	<ul style="list-style-type: none"> <li>• Build-in DHCP server</li> <li>• Support static DHCP assignment</li> </ul>
<b>Security, VPN Support</b>	<ul style="list-style-type: none"> <li>• IP Sec, L2TP, PPTP pass through</li> </ul>
<b>NAT &amp; Firewall</b>	<ul style="list-style-type: none"> <li>• Support special applications including H323, NetMeeting, internet gaming</li> <li>• Default private receiver (Software DMZ)</li> <li>• Virtual server</li> <li>• IP Filtering</li> </ul>
<b>IP Routing</b>	<ul style="list-style-type: none"> <li>• Rip v1 &amp; v2</li> <li>• Static and default route</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>• Web-Based Management Tool</li> <li>• UPnP</li> <li>• SNMP V1 &amp; V2</li> <li>• MIB: Ethernet, MIB II, 802.11</li> <li>• Command line interface with Telenet</li> <li>• Upload &amp; download test-based configuration file vis HTTP browser</li> <li>• Firmware upgrade via HTTP browser</li> <li>• SysLog</li> </ul>
<b>DNS</b>	<ul style="list-style-type: none"> <li>• DNS relay &amp; Dynamic DNS</li> </ul>
<b>WAN Encapsulation</b>	<ul style="list-style-type: none"> <li>• Static IP</li> <li>• DHCP client; PPPoE client</li> <li>• PPTP client</li> </ul>
<b>IP Address Assignment</b>	<ul style="list-style-type: none"> <li>• DHCP Client</li> <li>• Static IP Address</li> </ul>
<b>Environmental Specification</b>	<ul style="list-style-type: none"> <li>• Operation Temperature: 0<sup>0</sup> ~40<sup>0</sup> C.</li> <li>• Storage Temperature: -20<sup>0</sup> ~ 65<sup>0</sup> C</li> <li>• Operating Humidity: 10% ~90% (without Condensation)</li> </ul>
<b>EMC Certification</b>	<ul style="list-style-type: none"> <li>• CE</li> </ul>
<b>Certificate</b>	<ul style="list-style-type: none"> <li>• Wi-Fi Class 5 GHz 802.11a, Wi-Fi Class 2.4 GHz 802.11g (Planning)</li> </ul>