Air Live®
Powered by OvisLink Corp.

AIR3G

Wireless-N PoE 3G Router

User's Manual

Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

FCC Statement

Federal Communication Commission Interference Statement This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

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

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

FCC Caution

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

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

Bluetooth © 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction 1

1.1 Overview 1

1.2 Firmware Upgrade and Tech Support 2

1.3 Features 2

1.4 Operation Modes 3

1.4.1 3G Router Mode 3
1.4.2 AP mode 4
1.4.3 Client Mode 4
1.4.4 WDS Bridge Mode 5
1.4.5 WDS Repeater Mode 5

1.5 Hotspot Authentication 6

2. Installing the Air3G 8

2.1 Before You Start 8

2.2 Package Content 8

2.3 Knowing your Air3G 9

2.4 Hardware Installation 10

2.4.1 Passive PoE Installation 11
2.4.2 Wall Mount Installation 12

2.5 LED Table 13

2.6 Restore Settings to Default 13

3. Configuring the Air3G 14

3.1 Important Information 14

3.2 Prepare your PC 14

3.3 Introduction to Web Management 15

3.3.1 Getting into Web Management 15
3.3.2 Web Menu Structure 16

3.4 Configuration Wizard 17

3.5 Change Operation Mode 19

3.6 Change Regulatory Domain 20

3.7 WPS (WiFi Protected Setup) 20

3.7.1 AP and 3G Router Modes 21
3.7.2 Client Mode 23

4. Configuration: 3G Router Mode 25

4.1 Application for 3G Router Mode 25

4.2 Internet Setting Menu 26

4.2.1 Setup Wizard 26
4.2.2 WAN Setting 28
4.2.3 Hotspot 31
4.2.4 Virtual Server 31
4.2.5 DMZ 32
4.2.6 URL Filtering 33
4.2.7 MAC Filtering 33
4.2.8 IP Filtering 34
4.2.9 DDNS 34
4.2.10 Static Route 35

4.3 Hotspot Authentication 35

4.4 Connection Auto Backup Function 37

4.5 Wireless Settings Menu 38

4.5.1 Regulatory Domain 39
4.5.2 Multiple SSID 39
4.5.3 Channel 40
4.5.4 Wireless Security 40
4.5.5 Access Control 41
4.5.6 Bandwidth Control 42
4.5.7 Associated Client 43
4.5.8 Advanced Settings 43
4.5.9 WMM Settings 45
4.5.10 WDS Settings (Repeater) 48
4.5.11 WPS Settings 49

5. System Configuration and Status Menu 51

5.1 Menu Structure 51

5.2 LAN Interface Setup 52

5.2.1 DHCP Settings 52
5.2.2 Add DHCP Static Lease Client 53

5.3 Time Settings 53

5.4 Password Settings 54

5.5 Power Saving (Green AP) 54

5.6 Firmware Upgrade 55

5.7 Configuration Save and Restore 56

5.8 Factory Default 56

5.9 Status Menu 56
5.9.1 Device Information 56
5.9.2 Statistic 57
5.9.3 Client Table 57
5.9.4 LOG 58
6. AP Mode 59
6.1 Application for AP Mode 59
6.2 Wireless Settings 59
6.2.1 Regulatory Domain 60
6.2.2 Multiple SSID 60
6.2.3 Channel 61
6.2.4 Wireless Security 61
6.2.5 Access Control 62
6.2.6 Associated Client 63
6.2.7 Advanced Settings 63
6.2.8 WMM Settings 65
6.2.9 WDS Settings (Repeater) 68
6.2.10 WPS Settings 69
7. Client Mode 71
7.1 Application for Client Mode 71
7.2 Wireless Settings 71
7.2.1 Regulatory Domain 72
7.2.2 Profile Setting 72
7.2.3 Site Survey 73
7.2.4 Advance Settings 74
7.2.5 WPS Settings 75
8. WDS Bridge Mode 78
8.1 Application for WDS Bridge Mode 78
8.2 Wireless Settings 78
8.2.1 Regulatory Domain 79
8.2.2 Advance Setup 79
8.2.3 WDS Settings 81
9. Emergency Firmware Recovery 83
10. Frequent Asked Questions 85
11. Specifications 87
11.1 Hardware Features 87
11.1.1 General Hardware Feature 87
11.1.2 Power Supply 87
11.1.3 Dimension and Weight 87

11.2 Radio Specifications.....88
11.2.1 Frequency Band.....88
11.2.2 Rate and Modulation.....88
11.2.3 TX Output Power.....88
11.2.4 Receiver Sensitivity.....89
11.2.5 Supported WLAN Mode.....89
11.3 Software Features.....89
12. Wireless Network Glossary.....91

1 Introduction

1.1 Overview

The Air3G is a wireless multi-function router based on 150Mbps wireless-b/g/n 2.4GHz radio technologies. Users can share a wireless 3G/3.5G USB modem or xDSL cable modem internet connection at high speed. It also provides to 4 operation modes to satisfy different application environments. In addition, it features passive PoE port for installations in places that have no nearby access to electricity. Please take notice of the following features:

- This product does not come with 3G modem. It works with your 3G USB dongle. For latest 3G USB dongle support list, please visit our website at www.airlive.com and type “Air3G” on the product search.

- The Air3G is not just a 3G sharing router. It can also share other broadband connections from xDSL modem, ADSL modem, or Cable modem.
- The Air3G can support 12V on its passive PoE port. You will need to purchase a passive PoE Injector (PoE-1P) separately. For more information, please read section 2.4.1.
- The maximum output power for Air3G is about 1watt(30dBm). However, it is limited to 20dBm in EU and 23dBm in the U.S. for compliance with regulations. Nevertheless, unlike normal 11n routers that typically provide less than 15dBm output power in 11n mode, the Air3G can provides up to 19dBm(EU) and 22dBm(FCC) in 11n mode. It means greater coverage in 11n mode. Despite of Air3G’s capability, we strongly recommend that you use as little power as possible to reduce interference and conserve energy.

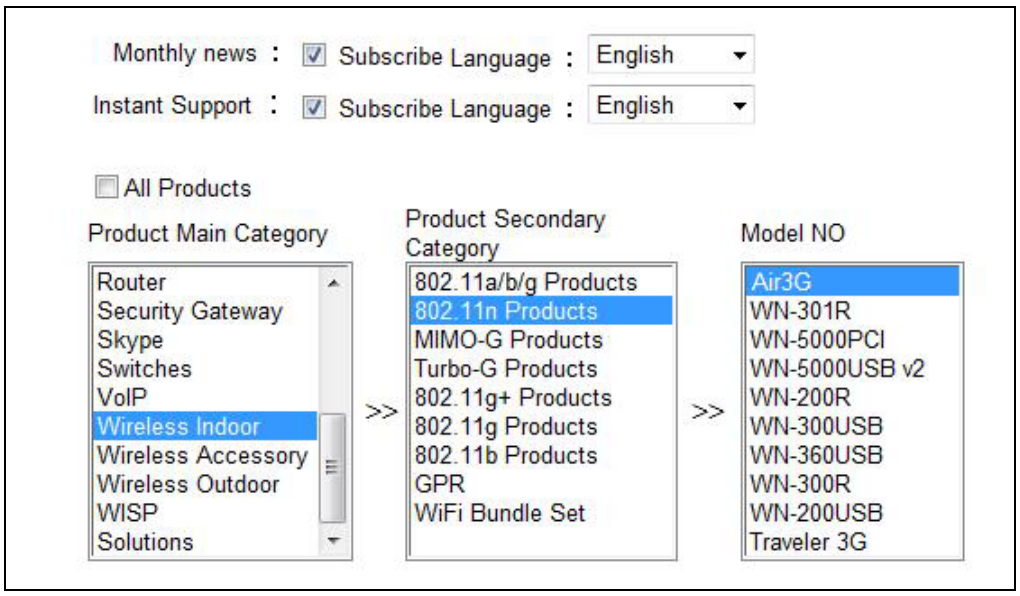
If you encounter any technical issues, we strongly recommend you read through Chapter 10: Frequent Asked Questions. The answers you need are very likely to be there.

1.2 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for Air3G. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the "Newsletter Instant Support System" on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



1.3 Features

- Wireless-N 3G Router
- Up to 30dBm Output Power (20dBm in EU, 23 dBm in the U.S.)
- Work with 3G/3.5G/UMTS/EVDO/HSDPA USB Dongle
- 1 x USB 2.0 Port
- 7 LED indicators
- Hotspot authentication function
- 150Mbps 1T1R Wireless-b/g/n standard

- 12V Passive POE Port
- WAN port for ADSL/Cable Modem support
- WAN/3G Connection Auto-Backup
- 3G Router, AP, Client, Bridge, Repeater modes
- Bandwidth Control
- 8MB Flash, 32MB SDRAM
- Green AP energy saving function
- Wall Mount Screw Holes
- Emergency firmware recovery mode

1.4 Operation Modes

The Air3G can perform as a multi-function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the Air3G to perform.

The Air3G can be configured to operate in the following wireless operation modes:

Air3G Wireless Operation Mode			
Wireless Mode	**Radio**	**WAN**	**Application**
3G Router	AP	3G only	3G Internet Sharing
		WAN only	xDSL/Cable Broadband Sharing
		3G with WAN backup	3G as primary connection, Broadband as backup connection
		WAN with 3G backup	Broadband as primary connection, 3G as backup connection.
AP	AP	none	Hotspot only or extend distance of another WDS AP/Router
Client	Client	none	Connect to AP Router
WDS Bridge	WDS	none	Create a backbone connection
WDS Repeater	AP + WDS	N/A	Extend the wireless signal. WDS Repeater setting is inside the “Wireless Settings” of 3G Router mode and AP Mode.

1.4.1 3G Router Mode

In this mode, you can share your 3G Internet connection and/or broadband connection. If you do not have a 3G USB dongle, you can still share your ADSL modem, xDSL mdoem, or Cable Modem connections. If you have both 3G and Broadband, you can use both for connection backup.

1.4.2 AP mode

When operating in the Access Point mode, the Air3G becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through Air3G. This type of network is known as “Infrastructure network”. Other Air3G or 802.11 b/g/n devices can connect to AP mode through Client Mode.

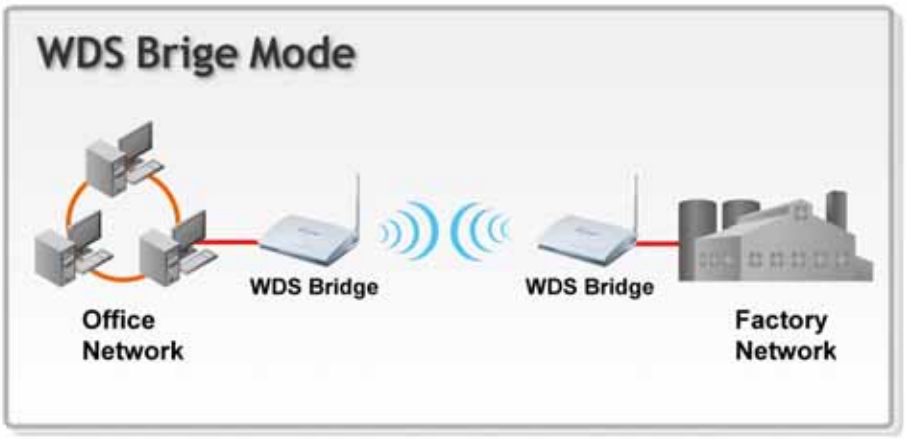
1.4.3 Client Mode

The Air3G acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of Air3G to get network access.

1.4.4 WDS Bridge Mode

This mode is best used when you want to connect LAN networks together wirelessly (for example, between office and warehouse). WDS Bridge using WPA-PSK or WPA2-PSK encryptions might be limited to devices using the same wireless chipset.

WDS Bridge works by entering remote Bridge's wireless MAC address on the WDS table. You can find the MAC address on the bottom label of the Air3G.

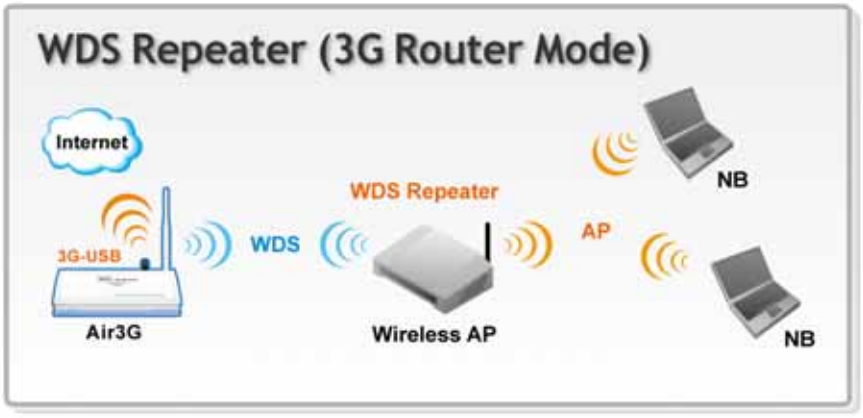


1.4.5 WDS Repeater Mode

The purpose of repeater is to extend the wireless signal of the remote AP/Router. ***In Air3G, the AP mode and the 3G Router mode also turn ito "WDS Repeater mode." You can find the WDS settings in the "Wireless Settings" page.*** Both sides must support WDS connection to work.

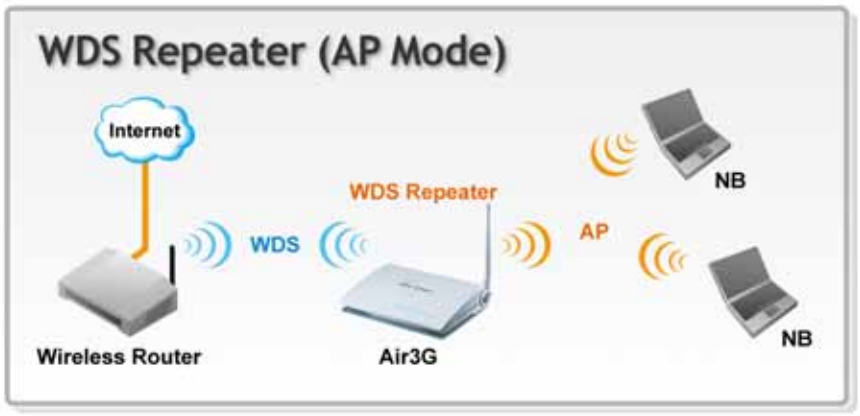
WDS Repeater in 3G Router Mode

The WDS Repeater function in 3G Router mode is to allow the remote AP to extend the wireless signal of Air3G. Please see the diagram below:



WDS Repeater in AP Mode

The WDS Repeater function in AP mode is to extend the wireless signal of remote AP. Please see the diagram below for details:



For information on how to configuration WDS Repeater, please go to section 4.6 or section 6.3.

1.5 Hotspot Authentication

The Air3G features basic Hotspot Authentication function. Hotspot authentication enables the administrator to manage Internet Access by username and password. ***The hotspot authentication function for Air3G is only suitable for small scale hotspot service like in the coffee shop. For larger installation, it is recommended to use a dedicated hotspot gateway like the AirLive WIAS-1200G***. For configuration procedures, please go to section 4.3.

Hotspot
Authentication!
Air Live
Air3G
Wireless-N PoE 3G Router
www.airlive.com
User Name:
Password:
Login
Internet
3G-USB
NB
Air3G

2 Installing the Air3G

This section describes the hardware features and the hardware installation procedure for the Air3G. For software configuration, please go to chapter 3 for more details.

2.1 Before You Start

It is important to read through this section before you install the Air3G

- This product does not come with 3G modem. It works with your 3G USB dongle. For latest 3G USB dongle support list, please visit our website at www.airlive.com
- The LAN1 port also work as the passive POE port
- The passive PoE DC Injector is optional; it is not included with the package. Please use a 12V passive POE system with Air3G's passive POE port. Do not use 802.3af 48V system or PoE switch with this device.
- When you use Passive PoE with 3G USB installed, it is recommend to use a power adapter of 12Vdc at 1.25A or greater.
- To protect the Air3G USB port from damage, please turn off the power when plugging in or pulling out USB device from the USB port.

2.2 Package Content

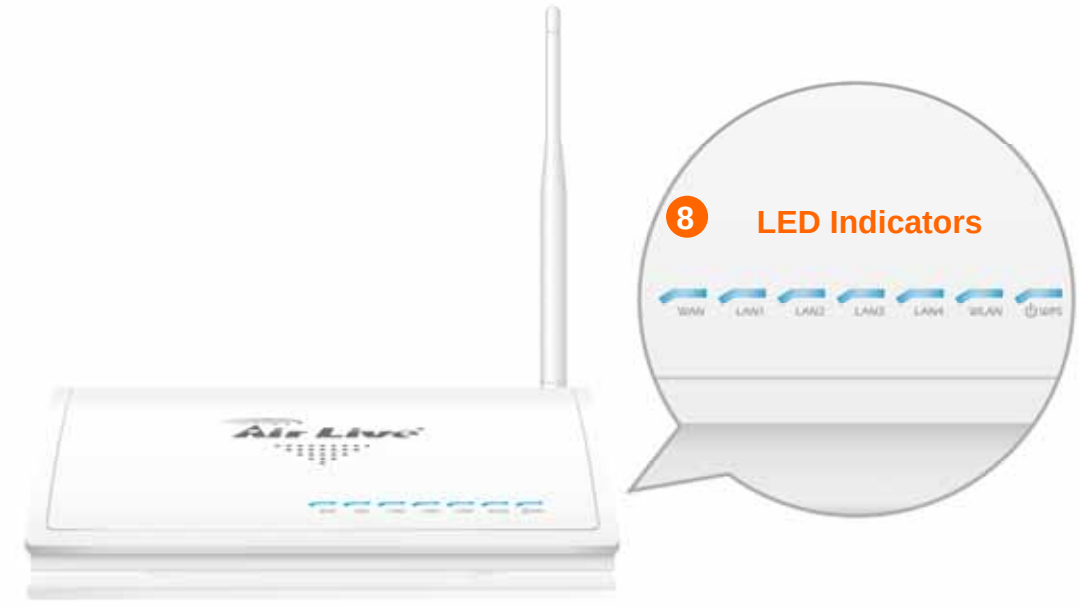
The Air3G package contains the following items:

- One Air3G main unit
- One 12V 1A DC power adapter
- 1 x Antenna
- User's Guide CD
- Quick Start Guide

2.3 Knowing your Air3G

Below are descriptions and diagrams of the product:

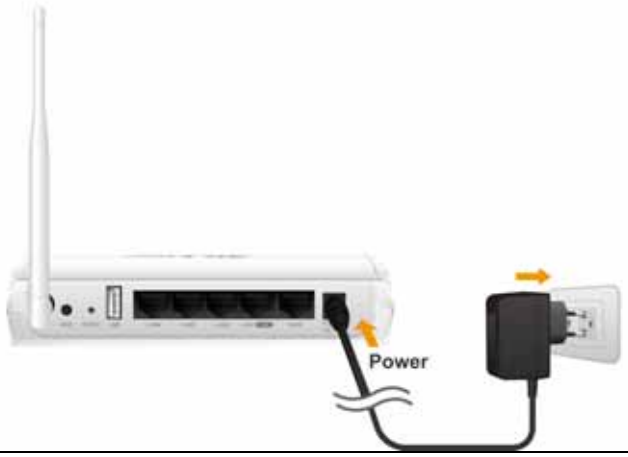
1. Antenna Connector
2. Power Adapter Connector
3. WAN Port
4. LAN Ports (LAN1 for Passive PoE Port)
5. Reset Button
6. WPS Button
7. USB Port (For 3G Dongle Use)



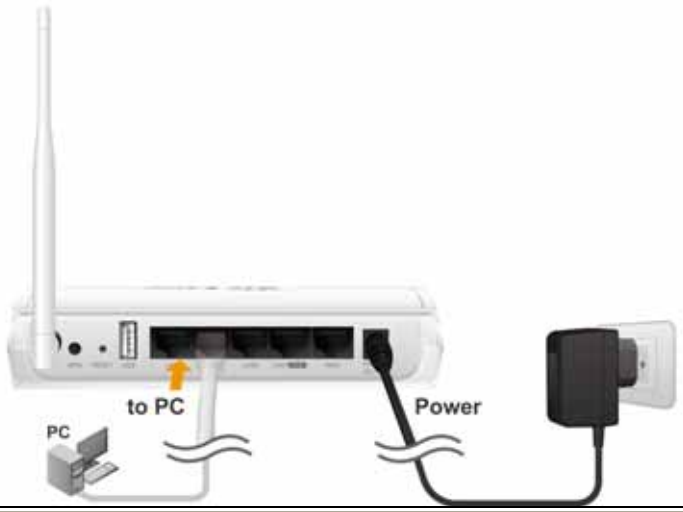
2.4 Hardware Installation

.1. Please install the antennas by turning clock wise into the RF antenna connectors

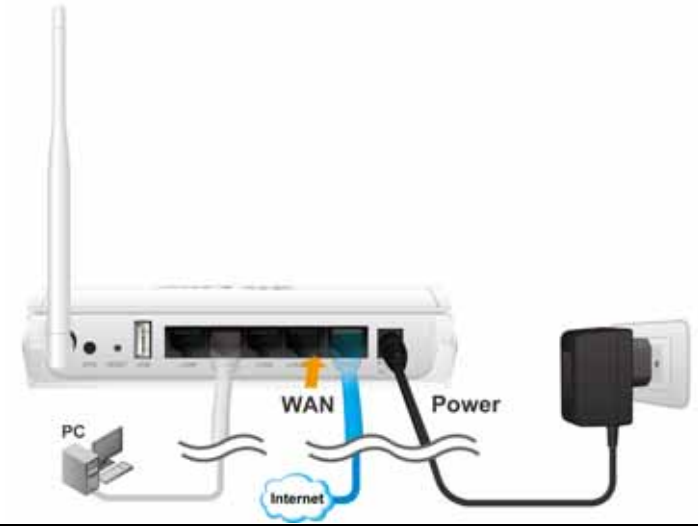
2. Now connect the power adapter to the Air3G



3. Connect the Ethernet cable to one of the LAN port and the other end to your PC.

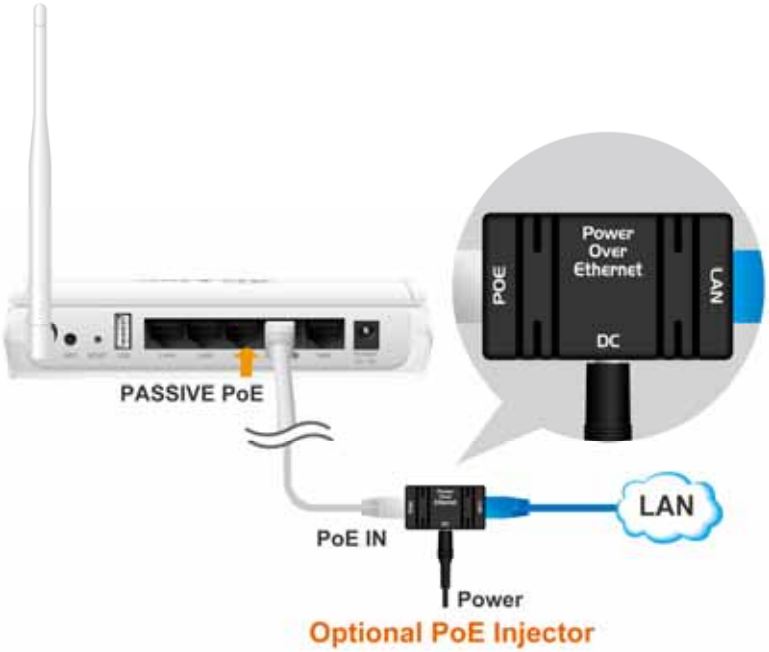


4. If you have broadband connection, please connect the Internet cable to “WAN port”.



2.4.1 Passive PoE Installation

If you want to supply the power by using Passive PoE, please follow the installation diagram below. Please note that the passive DC Injector is not included with Air3G, it needs to be purchased separately (AirLive Model: PoE-1P). Air3G uses 12V passive PoE system. it is recommend to use a power adapter of 12Vdc at 1.25A or greater if you have the USB dongle installed.



2.4.2 Wall Mount Installation

1. The holes for the wall mount screw are on the underside of the case. Please measure the distance between the holes. Then install 2 screws in the desire location with the measured distance apart from each other. Please do not screw all the way in, leave some space for mounting with the Air3G

2. Now please hang the Air3G on those 2 screws.

2.5 LED Table

This section describes the LED behavior of Air3G. You can find the LED on the top side of the Air3G.

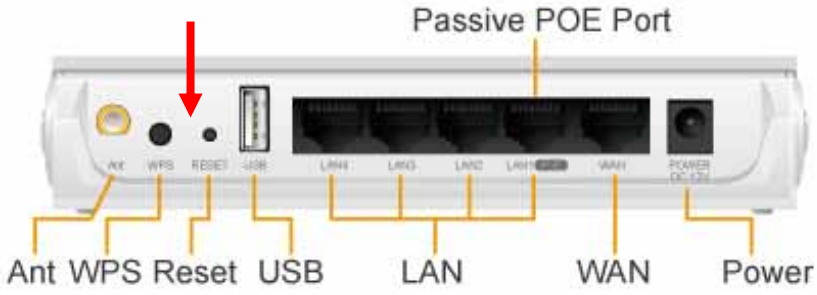
WPS (Power)
- Steady Blue – Normal Operation
- Slow Flashing: WPS Surveying
- OFF – No Power

WLAN
- Slow Flashing : Radio is active
- Fast Flashing: Transmitting Data
- OFF: Radio Disabled

LAN1 ~4, WAN
- Steady Blue : Link established
- Fast Flashing: Transmitting Data
- OFF: No Link

2.6 Restore Settings to Default

If you have forgotten your Air3G's IP address or password, you can restore your Air3G to the default settings by pressing on the "reset button" for more than 10 seconds. You might need a pen or pencil for this operation. The reset button is inside the bottom case. Please see diagram below for details.



3 Configuring the Air3G

The Air3G offers web browser (http) as management interface. In this chapter, we will explain Air3G's management interface and how to get into them.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the password and SSID are case sensitive.

- ❑ The default IP address is: 192.168.1.254 Subnet Mask: 255.255.255.0
- ❑ The default Account is "admin"
- ❑ The default Password is "airlive"
- ❑ The default SSID is "airlive"
- ❑ The default wireless mode is : 3G Router mode
- ❑ Please remember to "Apply Change" for settings to be saved and take effect.
- ❑ Please remember to "Reboot" the device after all settings are changed.
- ❑ The Emergency Firmware Recovery only works when you connect to LAN1~4
- ❑ By Default, the DHCP server is turned on in 3G Router mode. The other modes' DHCP servers are turned off. Therefore, if you switch from 3G Router mode to other modes, please remember to configure your PC's IP address manually.
- ❑ The default regulatory domain is "ETSI" for Europe. If you are not living in EU countries, you might wish to change the regulatory domain. However, please do not choose regulatory domain that does not apply to your country. Using wrong regulatory domain might be illegal.

.

3.2 Prepare your PC

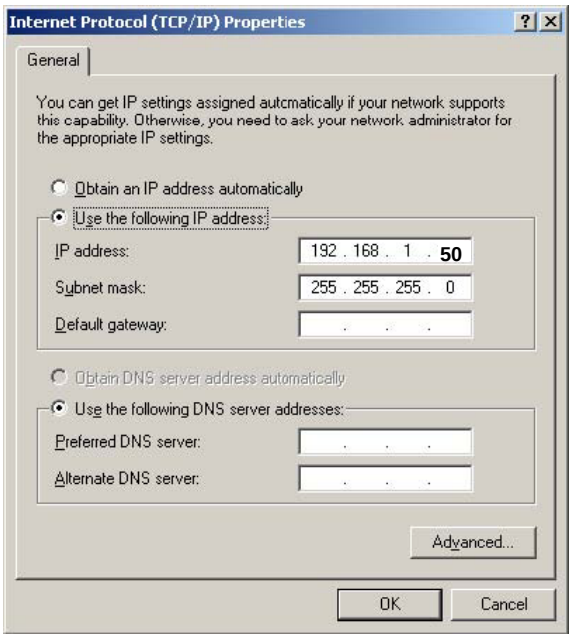
The Air3G can be managed remotely by a PC through either the wired or wireless network. The default IP address of the Air3G is **192.168.1.254** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.1` to 192.168.1.253.

To prepare your PC for management with the Air3G, please do the following:

1. Connect your PC directly to the LAN port on the DC Injector of Air3G

2. Set your PC's IP address to "Obtain an IP address Automatically". The Air3G should provide your PC an valid IP address.

3. If you want to set your PC's IP address manually, please set to 192.168.1.50 (or other address in the same subnet)



You are ready now to configure the Air3G using your PC.

3.3 Introduction to Web Management

The Air3G can be configured using the Web management interfaces by simply typing its IP address in the web browser. Most functions of Air3G can be accessed by it.

If you are placing the Air3G behind router or firewall, you might need to open the port 80 at virtual server on your firewall/router. This procedure is not necessary in most cases unless there is a router/firewall between your PC and Air3G.

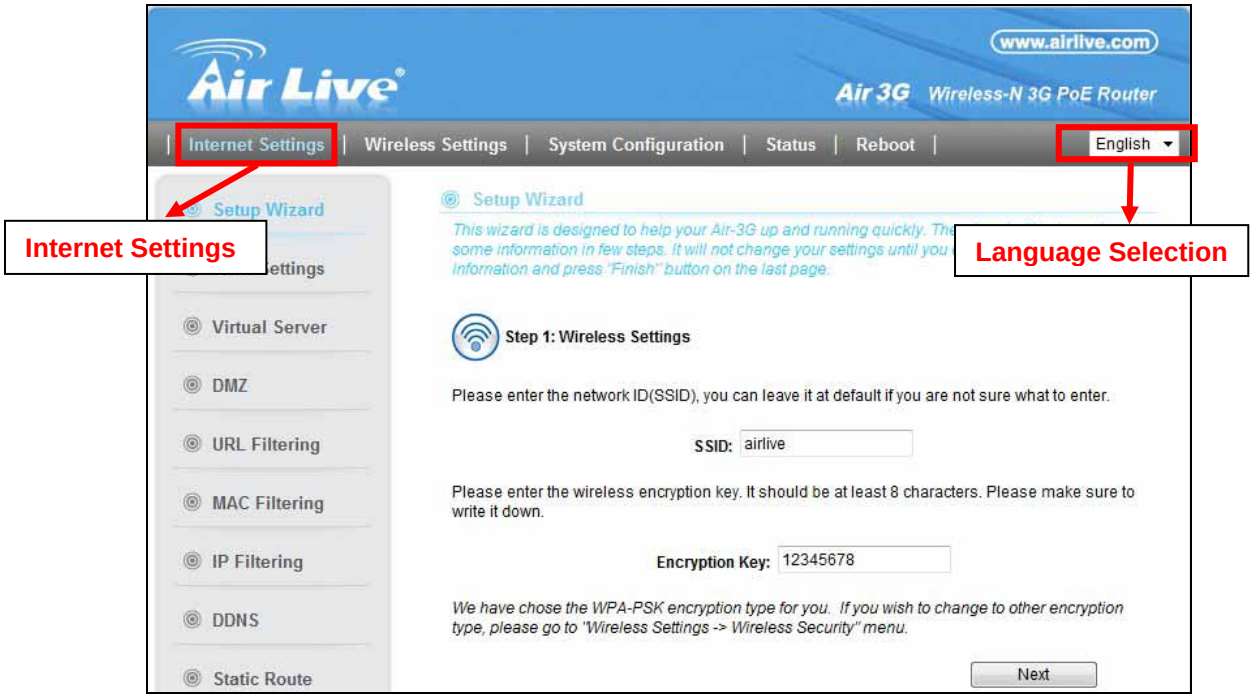
3.3.1 Getting into Web Management

To get into the Normal Web Management, simply type in the Air3G's IP address (default IP is 192.168.1.254) into the web browser's address field.

3.3.2 Web Menu Structure

We recommend users to browse through Air3G's web management interface to get an overall picture of the functions and interface.

After you enter the Web configuration, the following screen will appear:



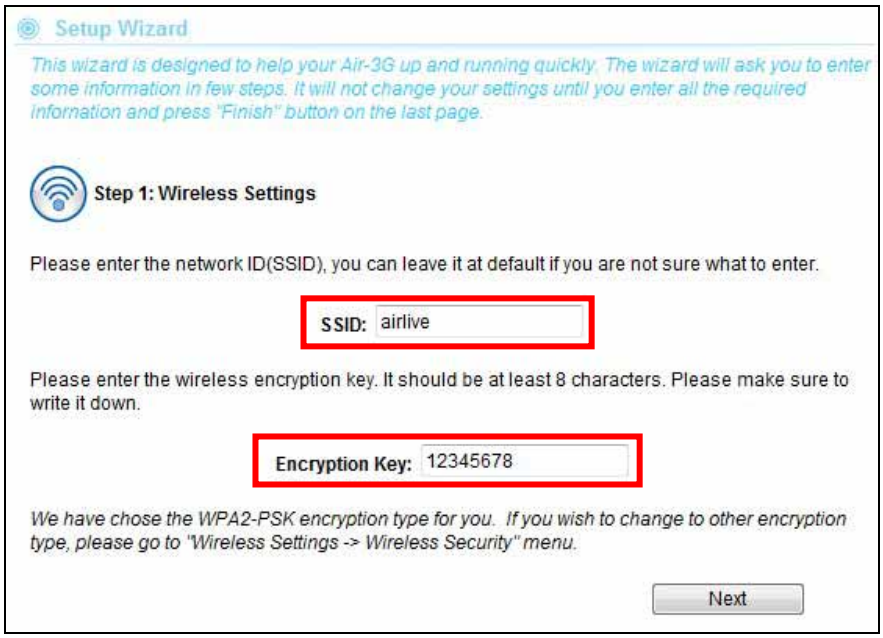
- **Internet Settings:** When you choose 3G Router mode, the "Internet Settings" bottom will be shown and you will be able to configure internet related functions here. This menu will disappear when you switch to other wireless mode.
- **Wireless Settings**: The Air3G's wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. You can also change the operation mode from this menu. For explanation of different wireless modes, please refer to Chapter 1.
- **System Configuration:** All non-wireless and router mode settings are in this category. The system configurations including changing password, upload firmware, backup configuration..
- **Status**: This section for monitoring the status of Air3G. It provides information on Device Information, Statistic, Client table, and Log.
- **Reboot:** Most of settings will require to click the "Reboot" bottom to take effect the settings you applied.

- **Language Selection:** You can change the language for the Web interface from here.

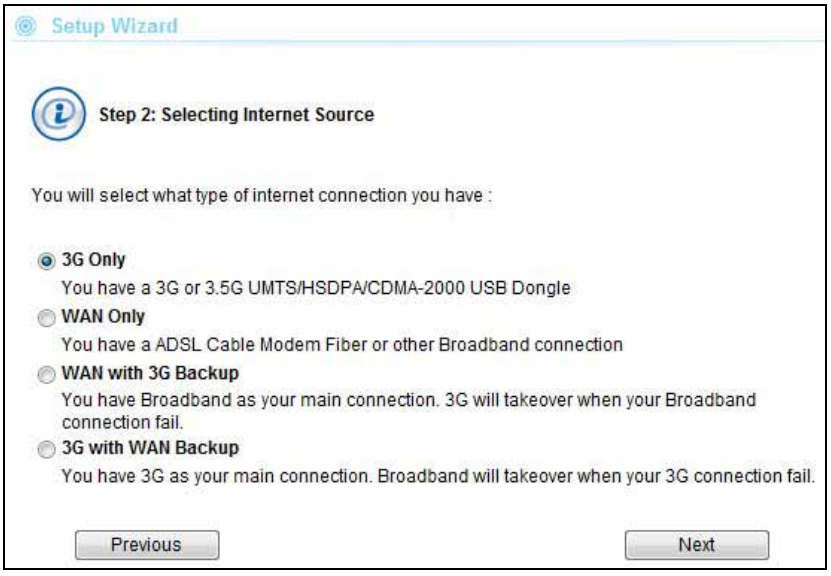
3.4 Configuration Wizard

The configuration Wizard is the first screen you will see after you login. It will ask you a few questions to setup your wireless and 3G broadband connection quickly.

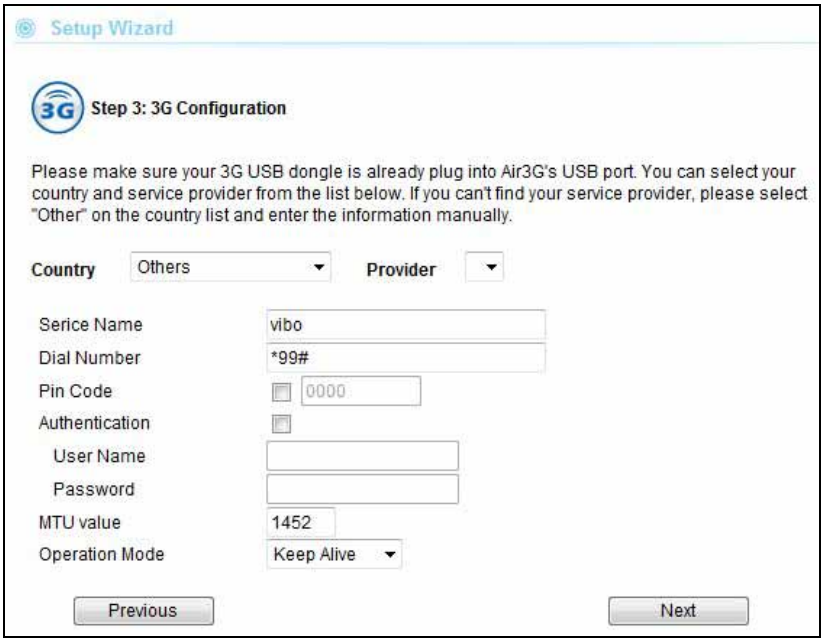
Step 1: Please enter your own SSID and Encryption Key. The default encryption type is WPA2-PSK(AES). The encryption key should be at least 8 alphanumeric characters.



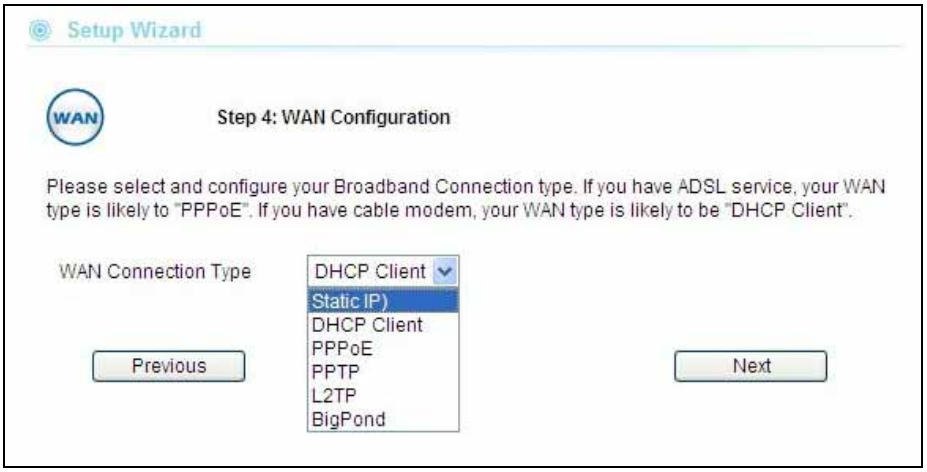
Step 2: Choose an internet connection type you need.



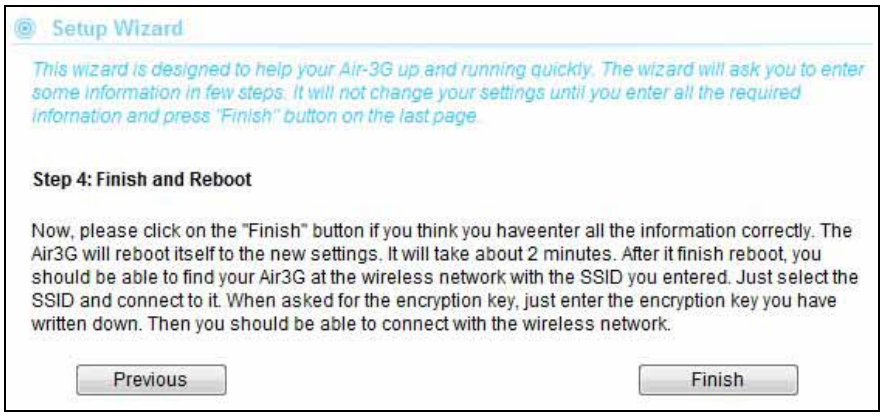
Step 3: Configure the 3G function if you have select 3G related connection types. Please make sure you have already plugin the 3G USB dongle. Now, select your country and 3G operator. If it is not on the list, please choose “others” and enter the information manually.



Step 4: If you have chosen WAN related connection type, the setup wizard will ask you to enter the WAN information. If you are not sure about setup information, please ask your ISP for parameters.



Step 5 : Please click “Finish” to reboot the system if you are sure about all settings.



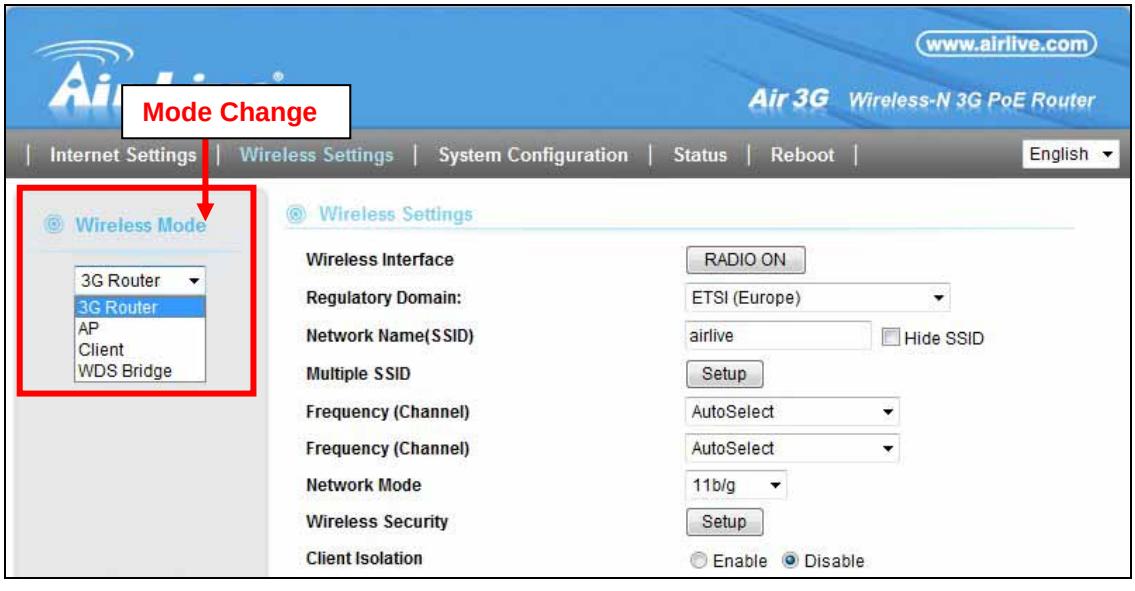
3.5 Change Operation Mode

The wireless settings of Air3G are dependant on the wireless operation mode you choose. For explanation on when to use what operation mode, please refer to Chapter 1

Changing Mode Procedure:

1. Select “Wireless Setting”
2. Choose your required wireless mode.
3. The AP might ask you to confirm the mode change. Once confirm, the AP will reboot to its new mode.

***Note**: When you change from 3G Router mode to other modes, the DHCP server will be turned off. In this case, **you must manually configure your PC’s IP address to the same subnet as the Air3G**. Likewise, when you change from other modes to 3G Router mode, the DHCP server will be turned on.*



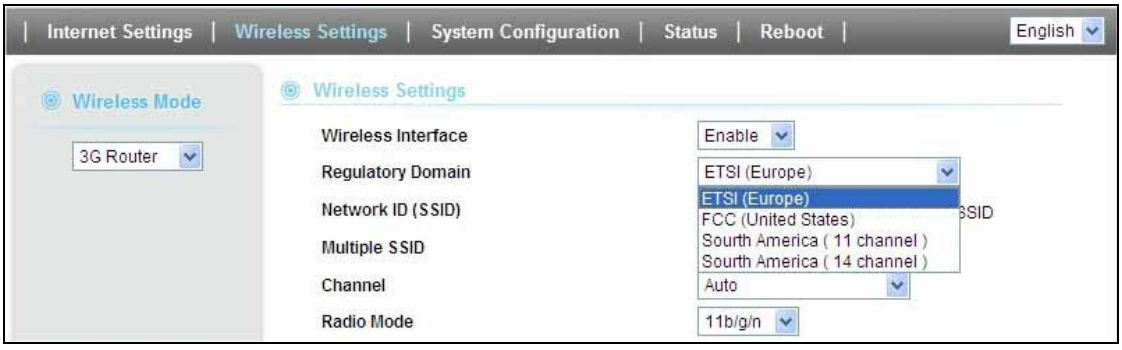
3.6 Change Regulatory Domain

The Regulatory Domain settings will decide what channels and output power are available for your Air3G. You must choose the correct Regulatory Domain for your country. Using the incorrect Regulatory Domain might be illegal. Please check the summary table below.

If you are unsure about what Regulatory Domain to use, please use "ETSI(Europe)" and restrict yourself to use only Channel 1 to 11.

Regulatory Domain Table			
Domain	**Channels**	**Maximum Tx Output Power**	**Countries**
ETSI (Europe)	1~13	20dBm	EU countries
FCC(United States)	1~11	23dBm	The United States and other countries that use U.S.A regulation for WiFi
South America (11ch)	1~11	30dBm	South American countries that follow channels of FCC domain.
South America (14ch)	1~14	30dBm	South American countries that allow use of all channels in 2.4GHz.

The default Regulatory domain is ETSI(Europe). If you need to change the Regulatory Domain, please go to "Wireless Settings"->"Regulatory Domain" menu. After changing the Regulatory Domain, the device will reboot to the new settings.



3.7 WPS (WiFi Protected Setup)

WPS is a system that simplifies the process to established wireless security. There are two ways to configure WPS connection:

1. **PBC** (Push Button Communication) using hardware or software:
   Push WPS buttons on both AP and Client site, the WPS connection will connect automatically. You can find Air3G's WPS Push button on the back of the router.

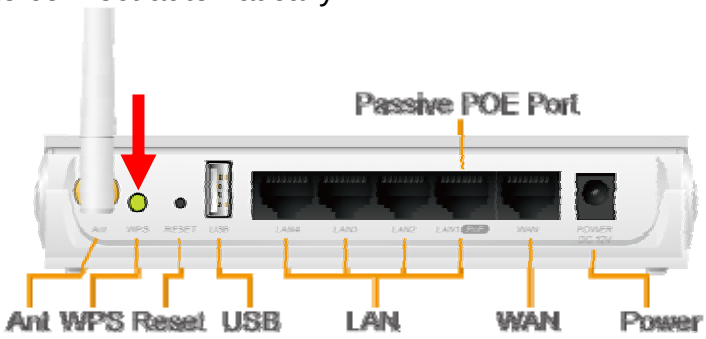
2. **PIN** (Personal Information Number) Enrollee and Registrar:
   WPS Registrar site should be entered the PIN Code from Enrollee site, the WPS connection will connect automatically.

It is recommended to use the first option as it is much simpler to configure.

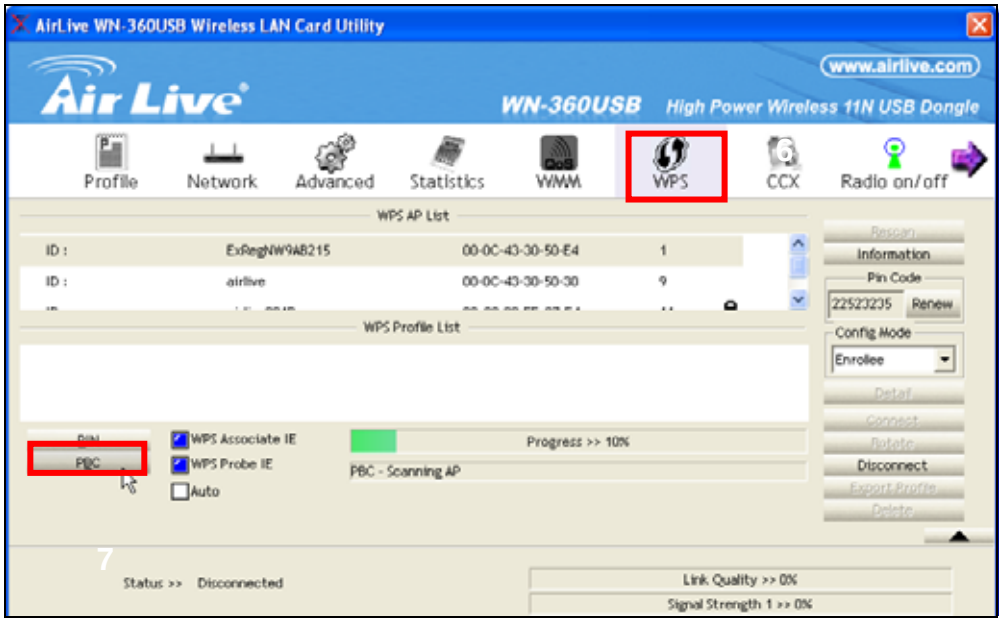
3.7.1 AP and 3G Router Modes

Example1: Using Hardware Push button

Please push WPS button directly on the back of the Air3G. The "WPS" LED flash will light and the Air3G will start to survey the client's WPS signal in the current environment. Please be noticed that, within **two minutes**, you have to turn on the utility of your wireless network card and click PBC to connect automatically.

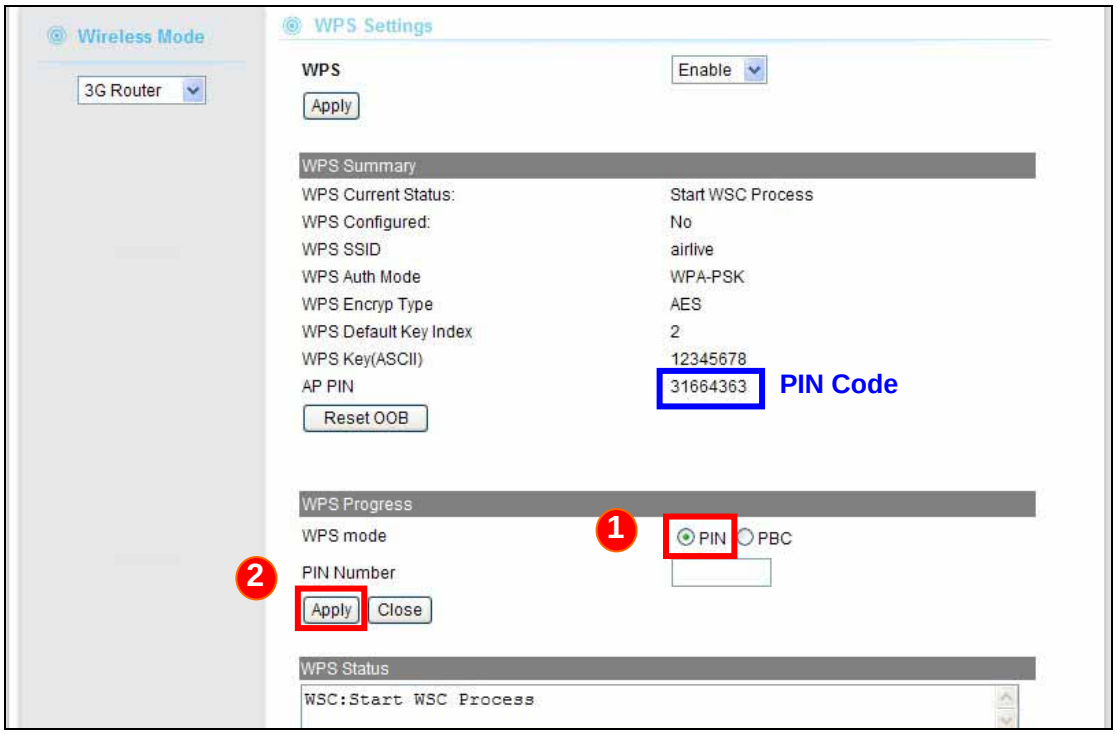


If you also have a hardware WPS button on your wireless card, you can push the button immediately now. If not, you can usually find the WPS PBC function in the wireless utility. Below is an example using AirLive WN-360USB wireless network card to connect with Air3G.

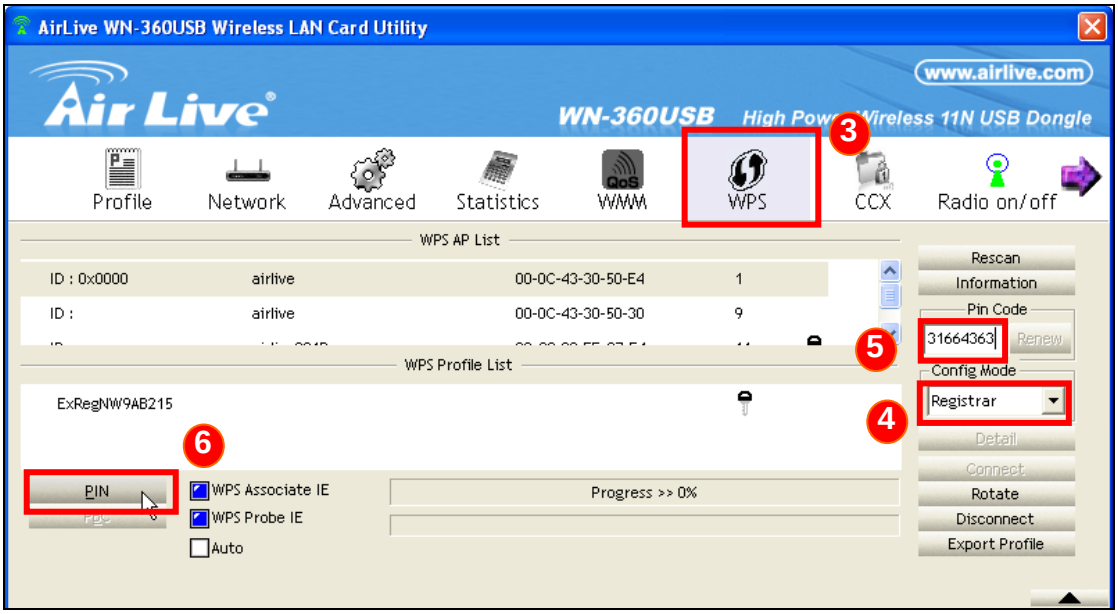


Example 2: WPS Using PIN

Please login Air3G's Web UI. Select Wireless Setting → WPS Setting. In the WPS Progress, select "PIN" then "Apply." You will get a PIN Code.



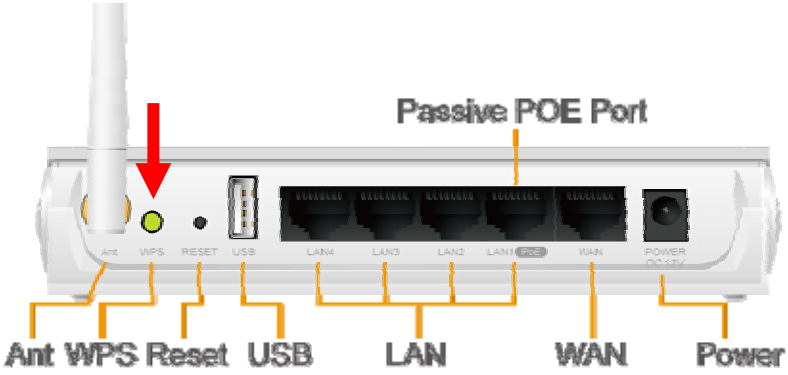
Then, please turn on the utility of your wireless network card. Choose WPS mode to "Registrar" and enter the PIN Code. Press "PIN" and the connection will automatically configure.



3.7.2 Client Mode

Example 1: Using WPS hardware button

Please push WPS button directly on the back of the device. The “WPS” LED flash will light and the Air3G will start to survey the AP’s WPS signal in the current environment.

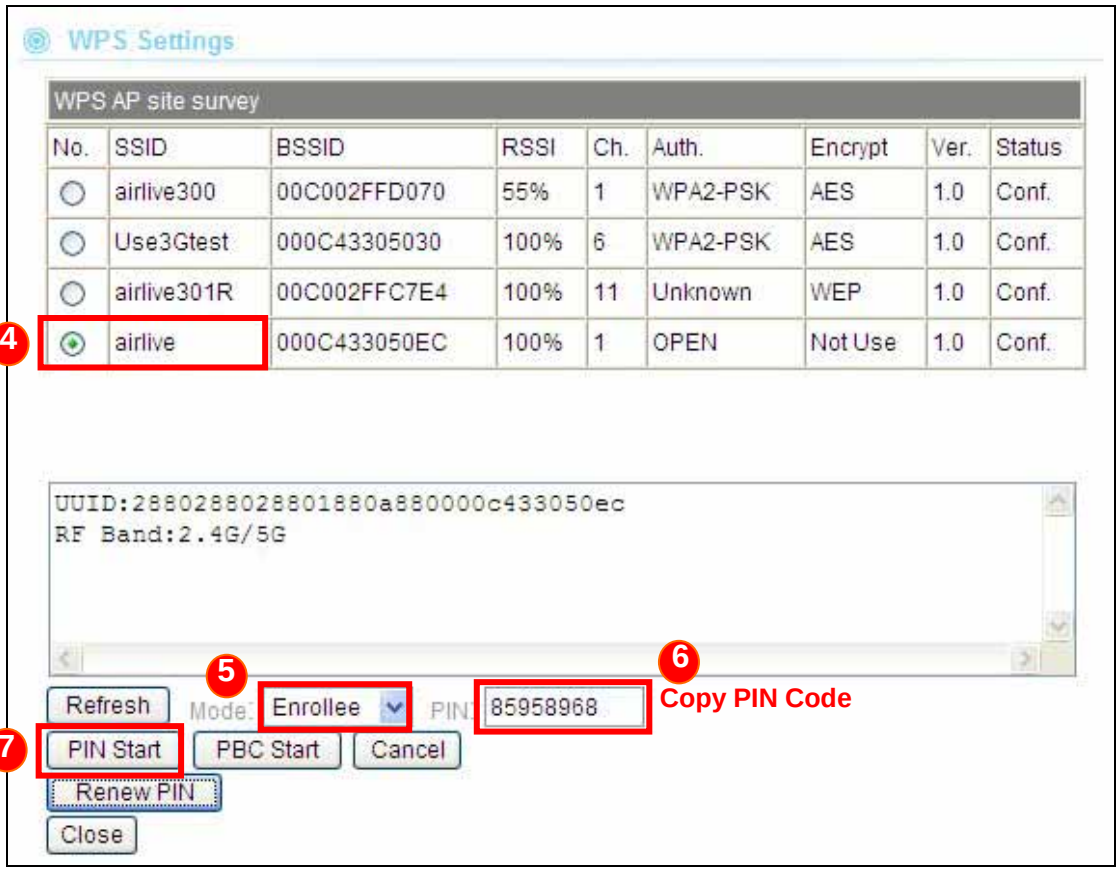


Within two minutes, please push WPS button on your AP device, the connection will automatic successfully.

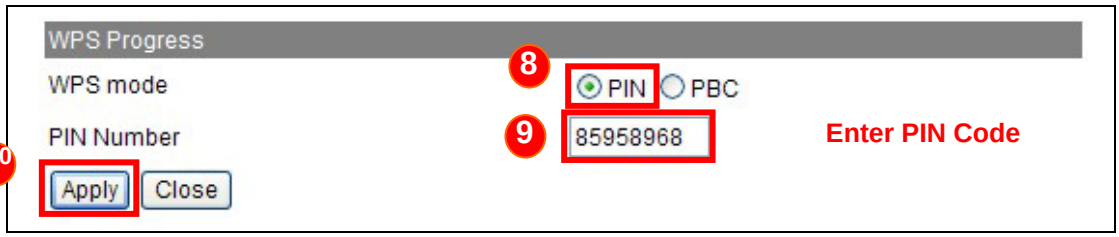
Example 2: WPS using PIN

Please login Air3G’s Web UI. Select Wireless Setting → change to Client mode → Client WPS Setting.

Select the SSID that you want to connect. Choose WPS mode to “Enrollee” and get a PIN Code in the field. Then press “PIN Start” and the “WPS” LED flash will light two minutes on the device’s housing.



Under AP site, Select Wireless Setting → WPS Setting. Choose WPS mode to "PIN" then enter the PIN Code → click "Apply" and the connection will automatically configure.



4 Configuration: 3G Router Mode

In this chapter, we will explain about the wireless settings for 3G Router Mode. Please be sure to read through Chapter 1.5 and Chapter 3's "*Introduction to Web Management*".

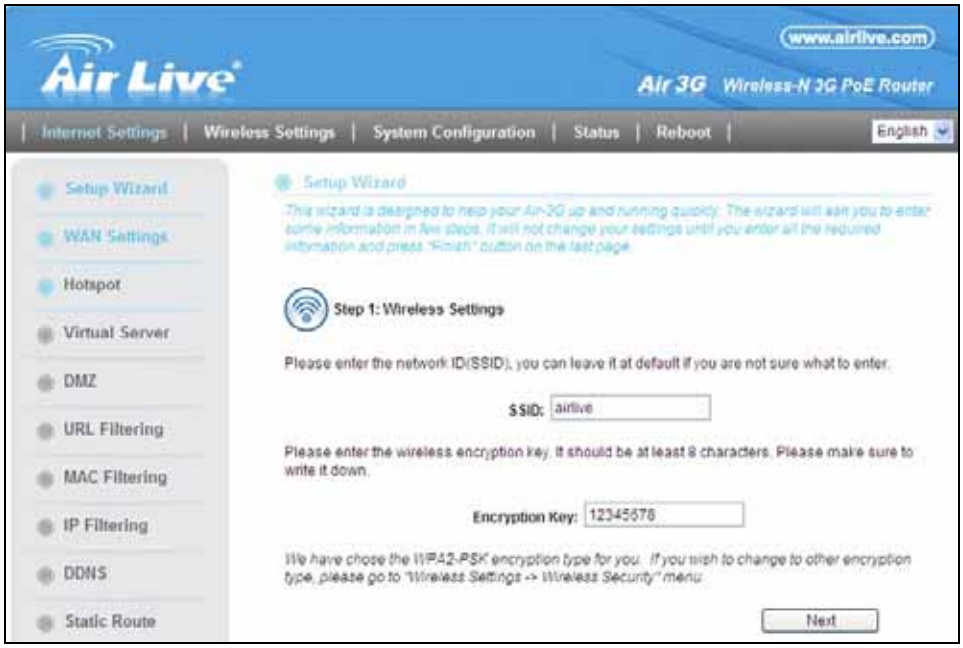
4.1 Application for 3G Router Mode

The 3G router mode is the main operation mode of the Air3G. This mode is more than just sharing 3G Internet connection. If you do not have a 3G USB dongle, you can still share your ADSL modem, xDSL modem, or Cable Modem connections. If you have both 3G and Broadband, you can use both for connection backup.

Due to Air3G's wider coverage and Hotspot Authentication function, it is also suitable to resell the Internet bandwidth. In addition, with the optional CAR-100DC car adapter, the Air3G can be used to provide Internet access on public transportations.

4.2 Internet Setting Menu

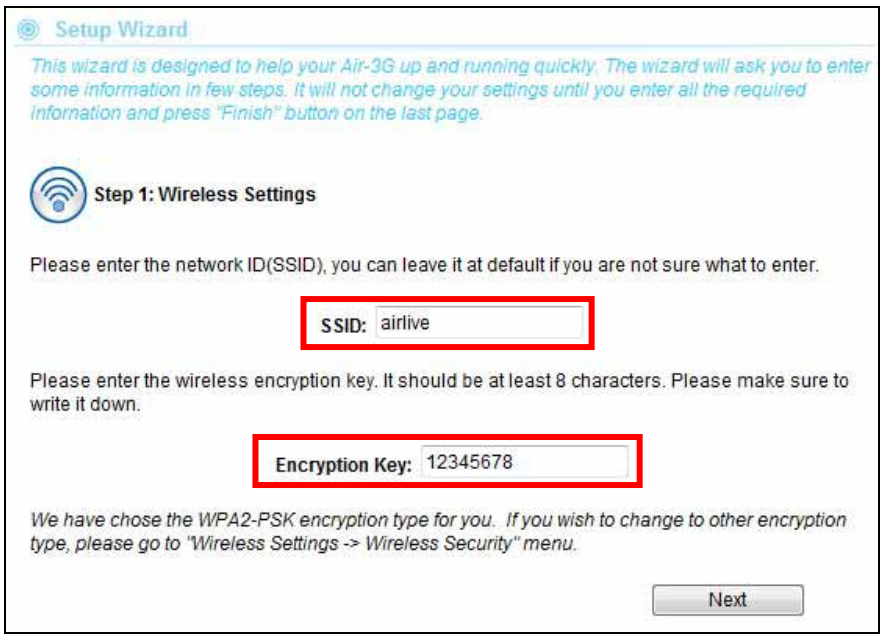
The Internet Setting Menu is the first menu you will see after login to Air3G. All WAN related configurations can be found here. This menu will not appear in any other modes.



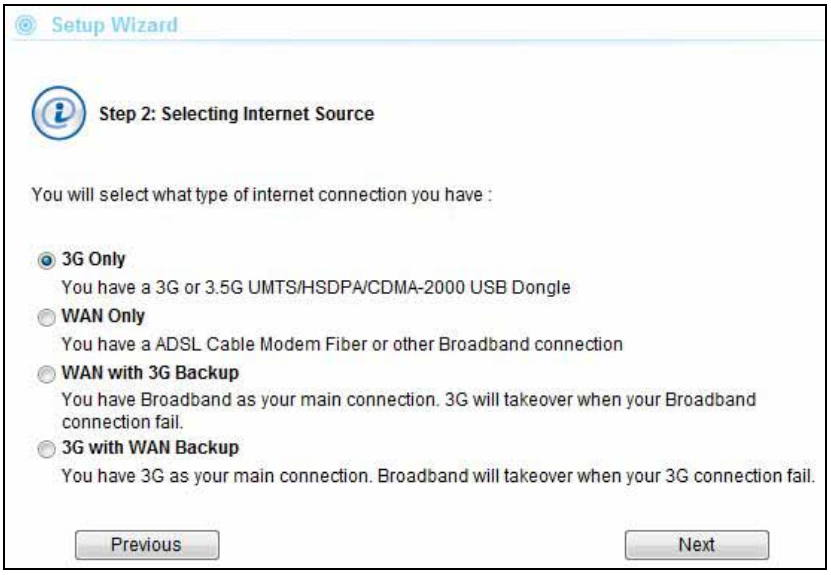
4.2.1 Setup Wizard

The configuration Wizard is the first screen you will see after you login. It will ask you a few questions to setup your wireless and 3G broadband connection quickly.

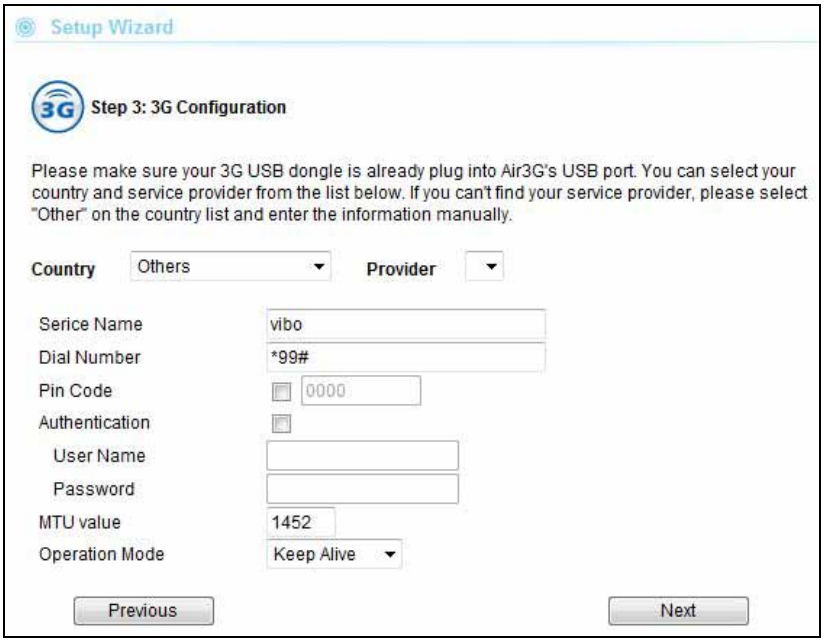
Step 1: Please enter your own SSID and Encryption Key. The default encryption type is WPA2-PSK(AES). The encryption key should be at least 8 alphanumeric characters.



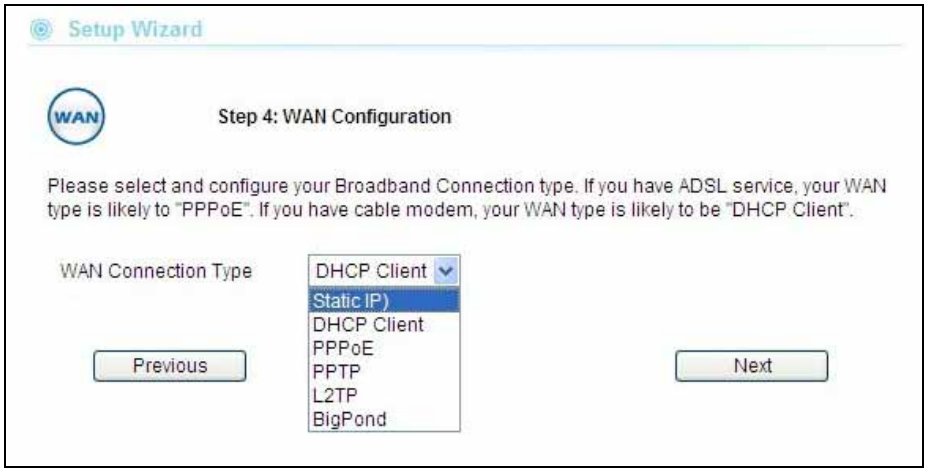
Step 2: Choose an internet connection type you need.



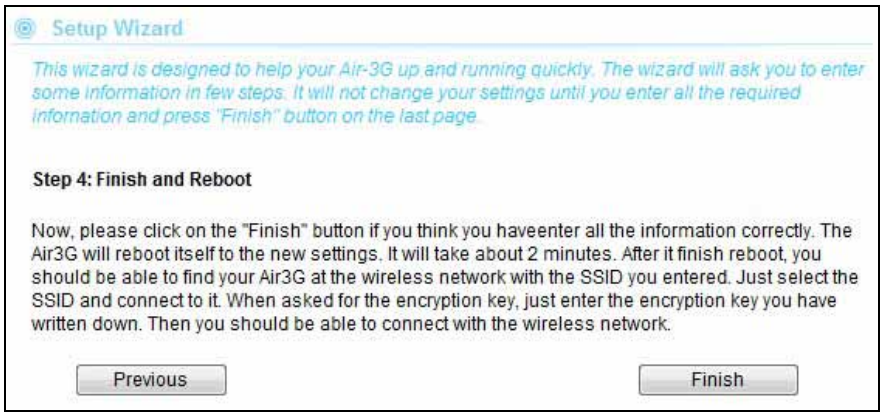
Step 3: Configure the 3G function if you have select 3G related connection types. Please make sure you have already plugin the 3G USB dongle. Now, select your country and 3G operator. If it is not on the list, please choose “others” and enter the information manually.



Step 4: If you have chosen WAN related connection type, the setup wizard will ask you to enter the WAN information. If you are not sure about setup information, please ask your ISP for parameters.



Step 5: Please click “Finish” to reboot the system if you are sure about all settings.

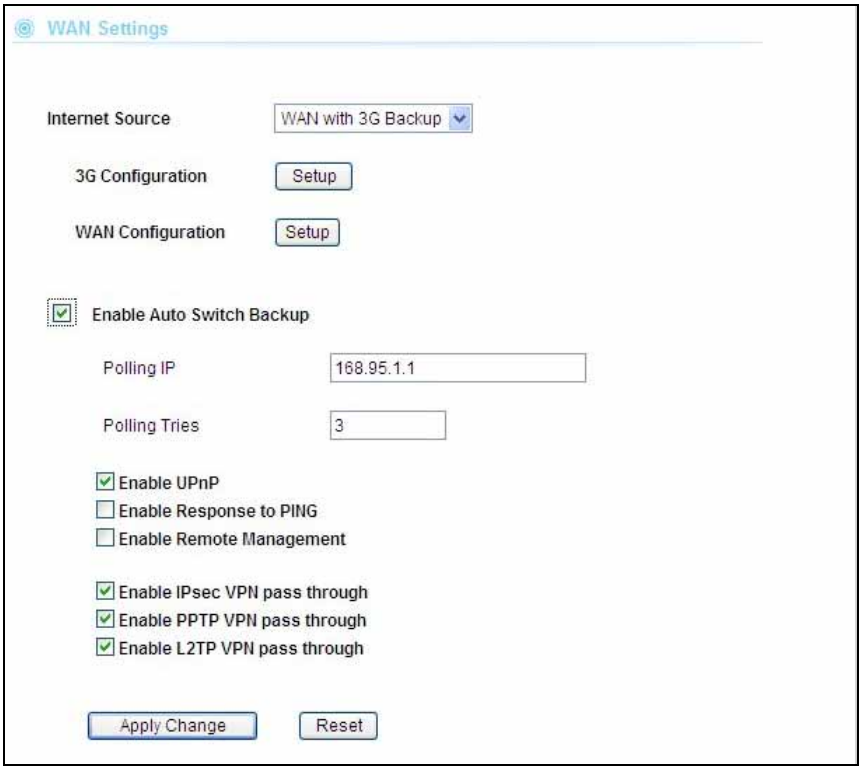


4.2.2 WAN Setting

Internet Settings -> WAN Settings

The Air3G provides four types of WAN connections, 3G Only, WAN Only, WAN with 3G Back up and 3G with WAN Back up. Please see the table below for details:

Internet Source table	
Internet Source	**Application**
3G only	Sharing 3G Internet Connection from the USB
WAN only	xDSL/Cable Broadband Sharing from WAN port
3G with WAN backup	3G as primary connection, Broadband as backup connection
WAN with 3G backup	Broadband as primary connection, 3G as backup connection.

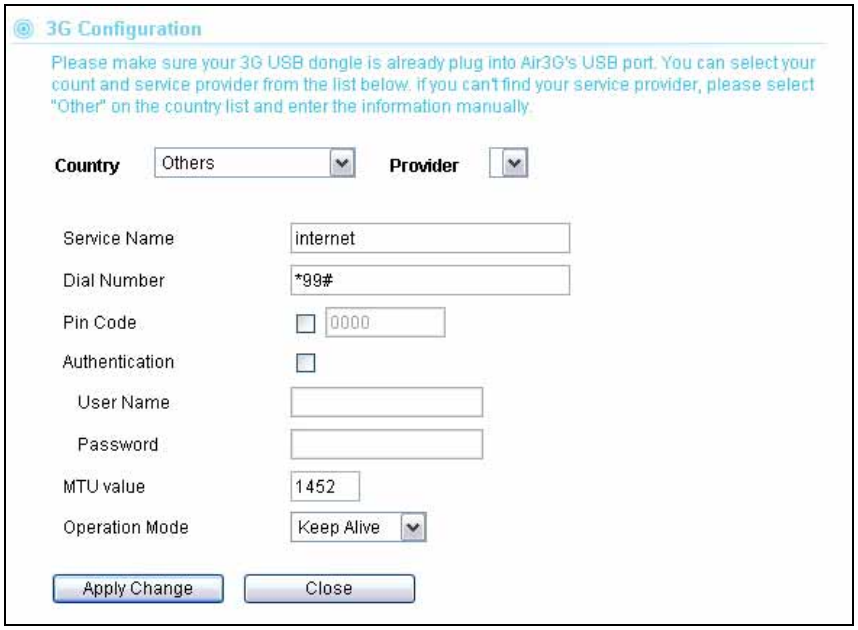


- **3G Configuration:** Click here to configure the 3G function
- **WAN Configuration:** Click here to Configure WAN port related function
- **Enable Auto Switch Backup:** Check this box to enable the Air3G to switch from secondary connection back to primary connection if the primary connection is back online. For example, if you choose "WAN with 3G Backup" as Internet Source. When this option is enabled, in the event of WAN failure and switched to 3G connection, the Air3G will monitor whether WAN is back online. If yes, then it will switch back to the WAN connection. ***Please note that during the connection switch, the Air3G will reboot. It might cause temporarily service disruption.*** For more information about this subject. Please read section 4.4 in this chapter.
- **Enable UPnP:** Enable universal plug and play
- **Enable Response to PING:** Please enable this if you want Air3G to response to remote PING command
- **Enable Remote Management:** Enable this option for remote access of the web management interface.
- **Enable VPN Pass Through:** If you have VPN servers in your local area network, you need to turn on the VPN pass through to allow remote access to the VPN networks.

3G Configurations

The 3G configuration features a setup wizard that allows you to select your country and service provider. If your country is not on the list or if the setup wizard information is

outdated; please select “others” as country and enter the information manually. Please ask your service provider for the setup parameters if you are not sure what to enter.



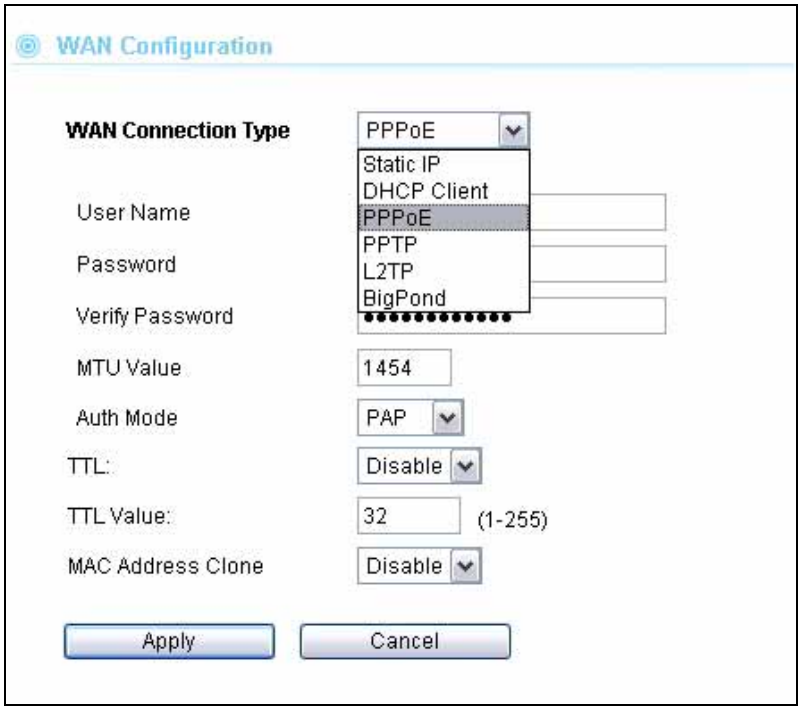
- **Service Name**: The service name of service provider
- **Dial Number**: The AT dial command to connect with your 3G service
- **PIN Code**: The identification code required to access your 3G USB dongle
- **Authentication**: Check this box if your service provider require username and password
- **MTU Value**: Maximum transmission unit. Please use default value unless your ISP has special setting.
- **Operation Mode**
  - **Keep Alive:** The 3G connection will auto reconnect if disconnection detect.
  - **On demand:** The 3G connection will reconnect only if there is a request from PC.

WAN Configurations

If you have xDSL or Cable Modem service, you can attach the internet connection to the WAN port. Then configure the settings accordingly.

The Air3G supports different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE, PPTP, L2TP, and Big Pond protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.

- **Clone MAC Address**: In this place, you can assign a MAC address for the WAN port. In case of WISP mode, it is Radio1's MAC address. For Gatway mode, it is the WAN/LAN1 MAC address.



4.2.3 Hotspot

Internet Settings -> Hotspot

Please go to section 4.3 for details on Hotspot Authentication function.

4.2.4 Virtual Server

Internet Settings -> Virtual Server

Virtual server 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.

If you want to allow your web server, ftp server, or email server to be accessible from Internet, you would need to open specific port on the virtual server to your local IP address.

The Air3G feature "Copy PC" and "Pre-defined" services to simply the process of creating virtual server.

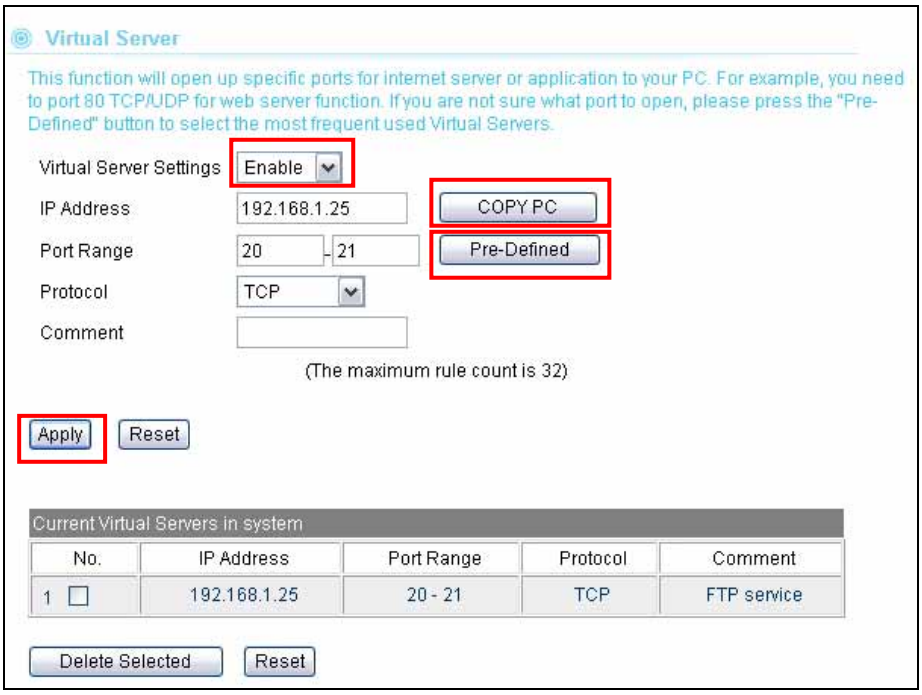
Example1: Open FTP service to your PC

Step 1: Enable the Virtual Server function

Step 2: Click on “Copy PC” icon to copy the IP address of your PC.

Step 3: Click on “Pre-Define” for a list of popular service and select “FTP”.

Step 4: Click on “Apply” and the new virtual server should appear on table list.

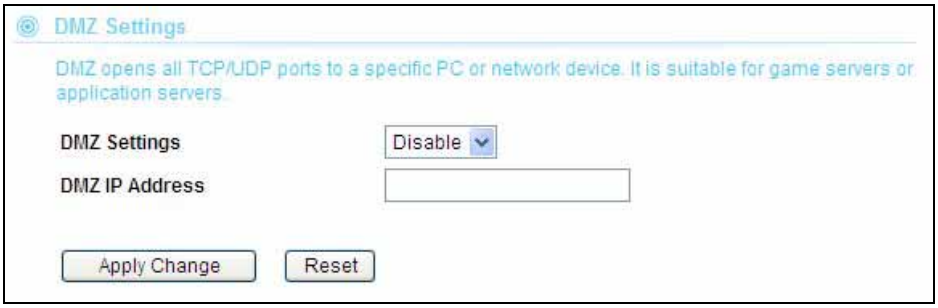


For a list of most frequent used TCP and UDP ports. Please visit
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

4.2.5 DMZ

Internet Settings -> DMZ

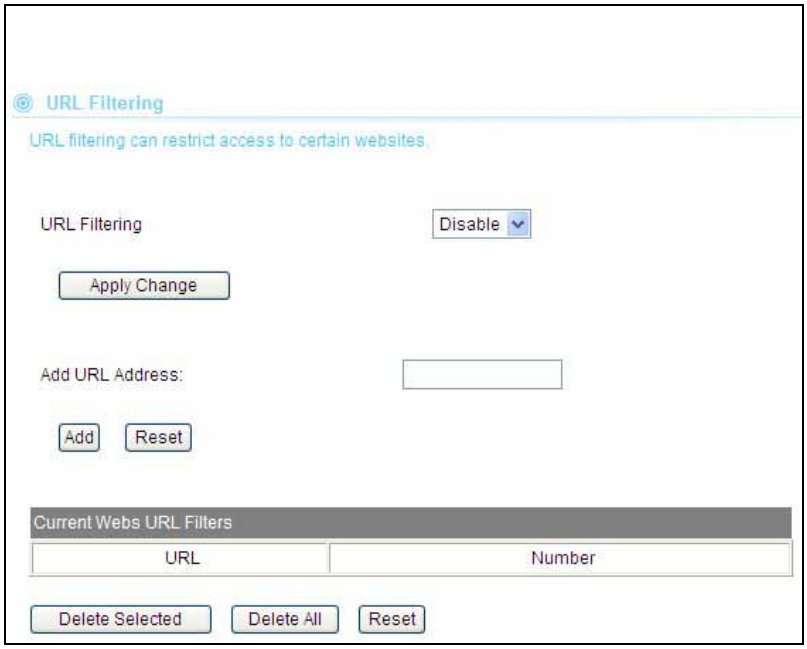
DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It is used mostly for setting gaming servers behind the Air3G.



4.2.6 URL Filtering

Internet Settings -> URL Filtering

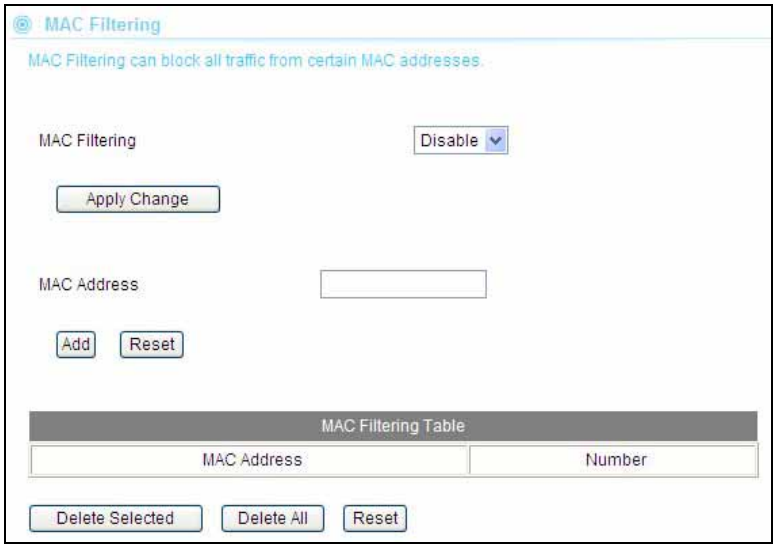
The Air3G provide URL filter function to stop access to certain website. It is useful for parents to stop children from accessing some websites.



4.2.7 MAC Filtering

Internet Settings -> MAC Filtering

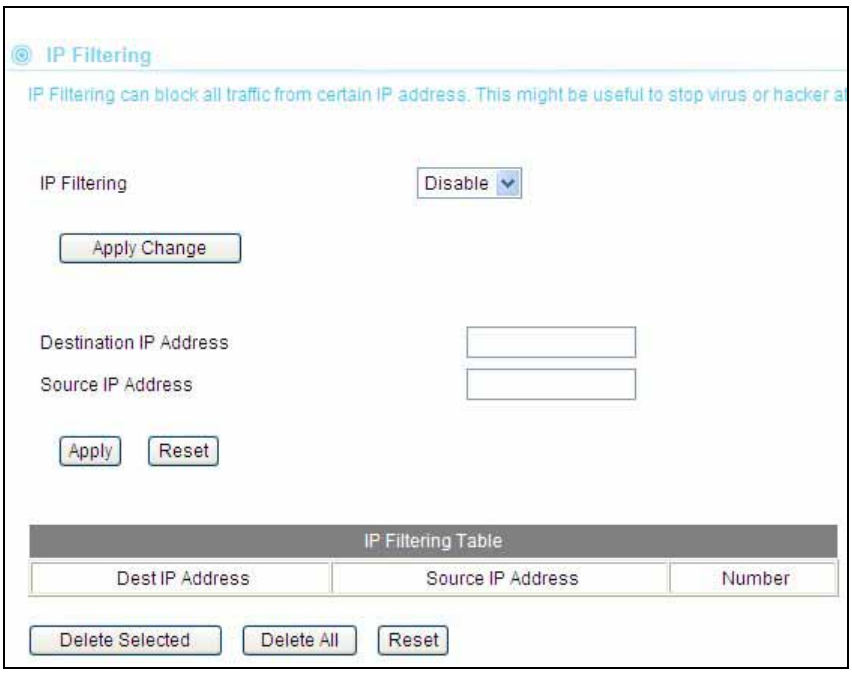
MAC filter can filter out traffic from certain MAC addresses. It can prevent access to internet from certain stations in the local LAN. Please enter the MAC address in XX-XX-XX-XX-XX format. For example: 00-4F-66-11-22-33



4.2.8 IP Filtering

Internet Settings -> IP Filtering

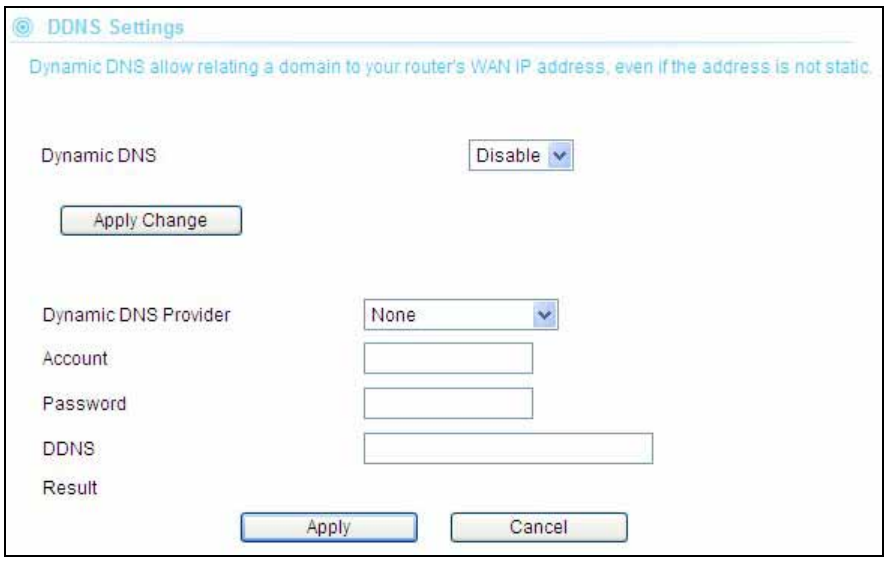
IP filtering allows you to block certain IP addresses from accessing the network.



4.2.9 DDNS

Internet Settings -> DDNS

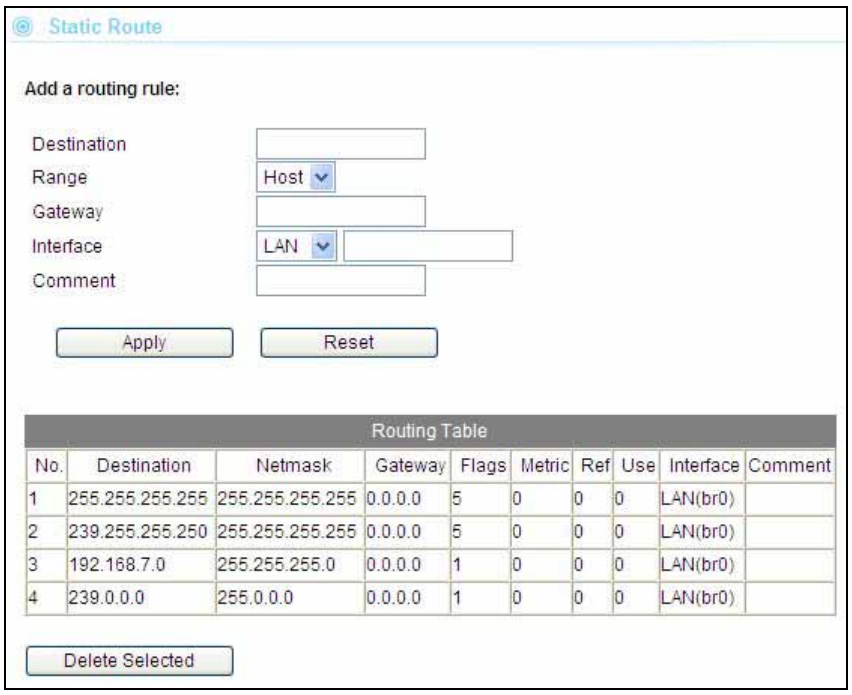
Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. The AIR3G support “Dyndns.org”, “zoneedit.com” and “no-ip.com” service.



4.2.10 Static Route

Internet Settings -> Static Route

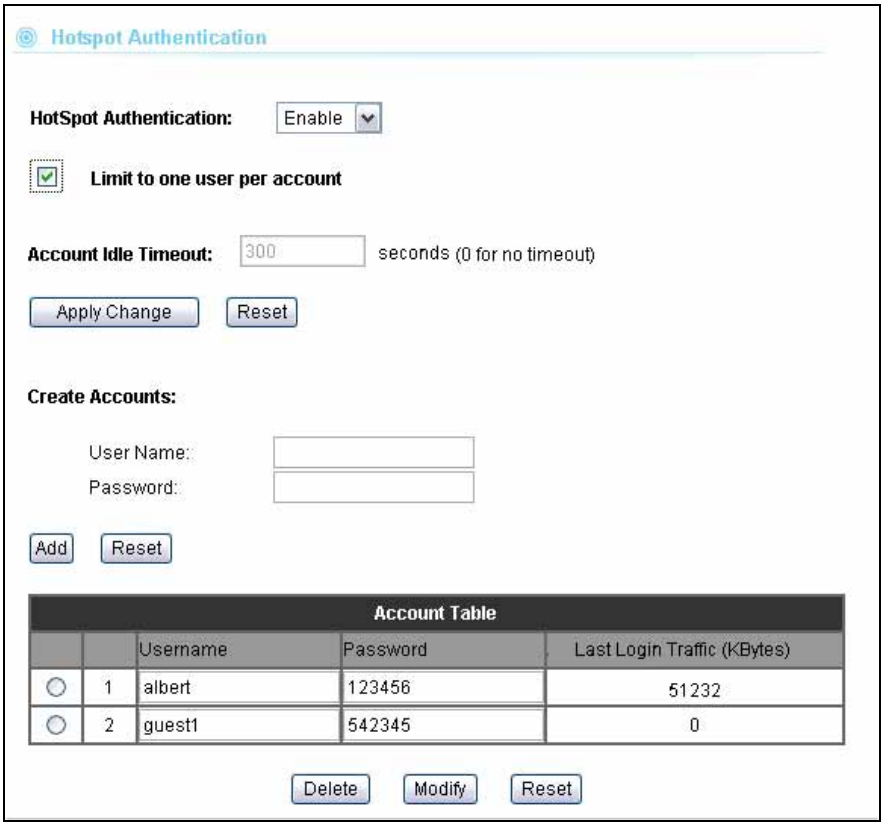
Static Route allows you to setup the routing table manually.



4.3 Hotspot Authentication

Hotspot authentication enables the administrator to manage Internet Access by username and password. When hotspot authentication is enabled, PCs that are connected to G.DUO will get a Pop-Up window when they try to access the Internet. They must enter correct username and password to access Internet. Please see diagram below.

To configure Hotspot Authentication function, please go to ***Internet Settings-> Hotspot*** menu. The following screen will appear:



- **Hotspot Authentication:** Enable your hotspot Authentication here. You must click on "Apply Change" to take effect.

- **Limit to one user per account:** If you want to each user must have its own account. Please check this box. You must click on "Apply Change" to take effect.

- **Account Idle Timeout:** After the period of inactivity, the Air3G will log out the user. Please enter zero if you don't want the account every expired. You must click on "Apply Change" to take effect.

- **Create Accounts:** Please enter the "Username" and "Password", then click on "Add" to create an account.

- **Account Table:** This field will display the information about accounts. You can modify the username/password directly on the table cell then click on the "*Modify*" button. The "*Last Login Traffic*" shows the data transmitted during the last login session.

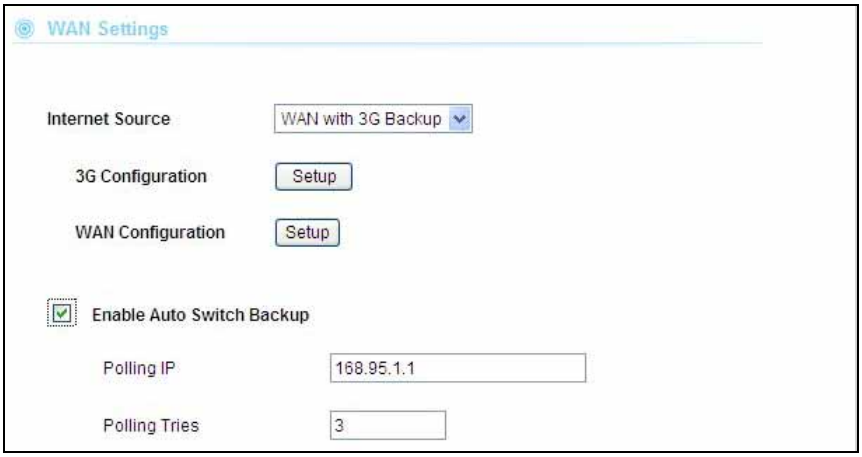
4.4 Connection Auto Backup Function

Internet Settings -> WAN Settings

When you select “WAN with 3G backup” or “3G with WAN Backup” as your Internet source, you will enable Air3G’s connection backup function. It means the Air3G will do fail over between your 2 Internet source. In the example of “WAN with 3G backup”; the WAN is the “Primary Connection” and the “3G” is the “Secondary Connection”. When the primary connection failed, the Air3G will switch to secondary connection.

Internet Source table	
Internet Source	**Application**
3G with WAN backup	3G as primary connection, Broadband as backup connection
WAN with 3G backup	Broadband as primary connection, 3G as backup connection.

When you select either of the 2 settings, the following screen will appear:



Enable Auto Switch Backup

Check this box to enable the Air3G to switch from secondary connection back to primary connection if the primary connection is back online.

For example, if you choose “WAN with 3G Backup” as Internet Source. When this option is enabled, in the event of WAN failure and switched to 3G connection, the Air3G will monitor whether WAN is back online. If yes, then it will switch back to the WAN connection. ***Please note that during the connection switch, the Air3G will reboot. It might cause temporarily service disruption.***

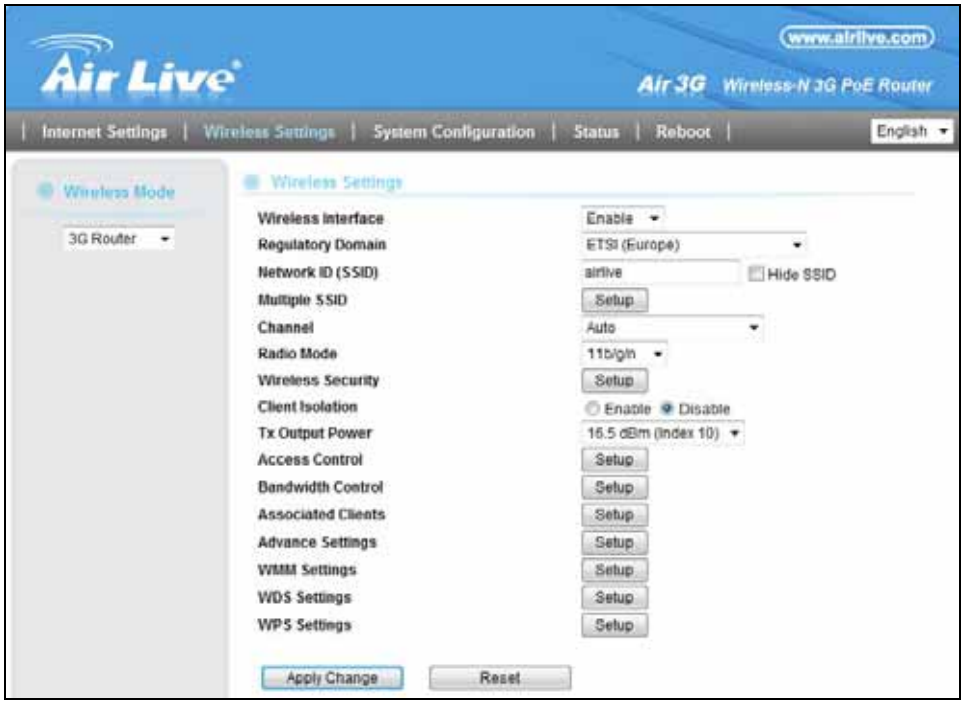
- **Polling IP**: This is the IP address for which the function will ping to monitor whether the primary connection is back online. The Air3G will ping this IP about once per minute.

- **Polling Tries**: How many successful PINGs to the Polling IP are needed before Air3G decides the primary connection is back online.

Once the primary connection is back on line, the Air3G will reboot back to the primary connection after about 5 minutes.

4.5 Wireless Settings Menu

When you select “*Wireless Settings*” on the top menu; the following screen will appear:



4.5.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

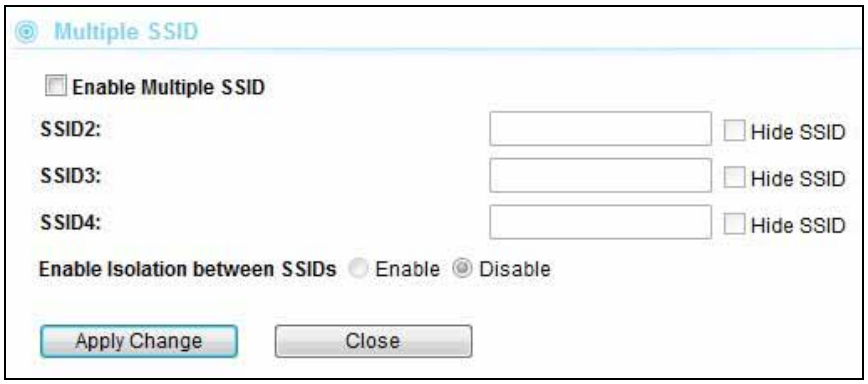
The Air3G is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	30dBm
South America(14 CH)	1~14	30dBm

4.5.2 Multiple SSID

Wireless Settings -> Multiple SSID

Multiple SSID allows Air3G to create up to **4** different wireless networks (SSID). It is also known as “Virtual AP” function. Each SSID can have its Encryption policy. The SSID1 is the main SSID under Wireless Setting page.



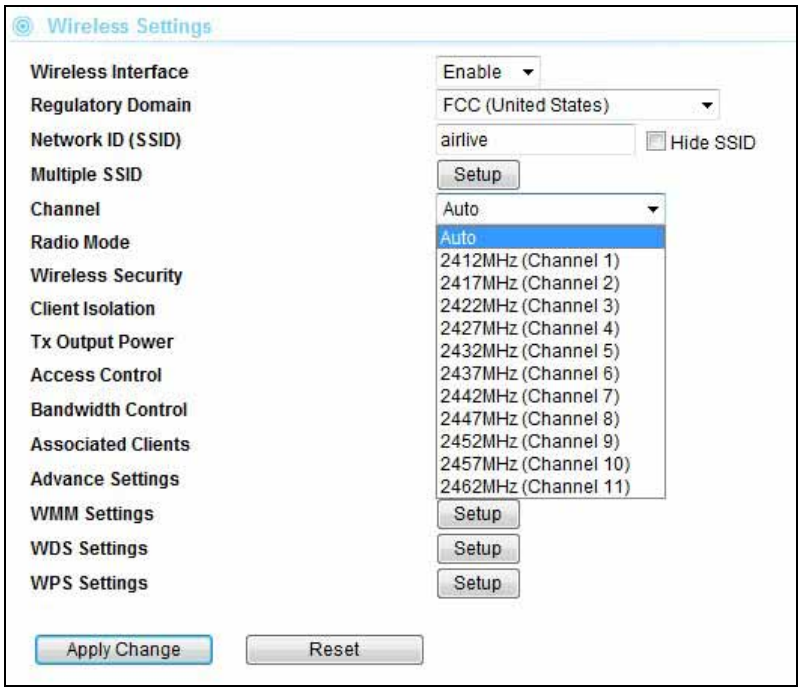
- **Hide SSID**: The wireless network will become invisible, only accessible to people who knows the SSID name.
- **Enable Isolation between SSIDs**: Enable this option will disable traffic between different SSIDs.

4.5.3 Channel

Wireless Settings -> Channel

The channel is the frequency range used by radio. In 802.11g/b standard, there are maximum of 14 Channels. However, the available channels in each country are dependant on the local regulation. If you are living in Europe, you can use channel 1 to 13. If you are living in the United States, you can use channel 1 to 11.

Each wireless channel takes between 22 to 25MHz of frequency width. But the channels are only 5MHz apart. Therefore, only every 5 channels can be free of interference with each other. It is recommended that you can do a site survey to find about what channels are used by surrounding AP and choose a channel that is not used by other APs.

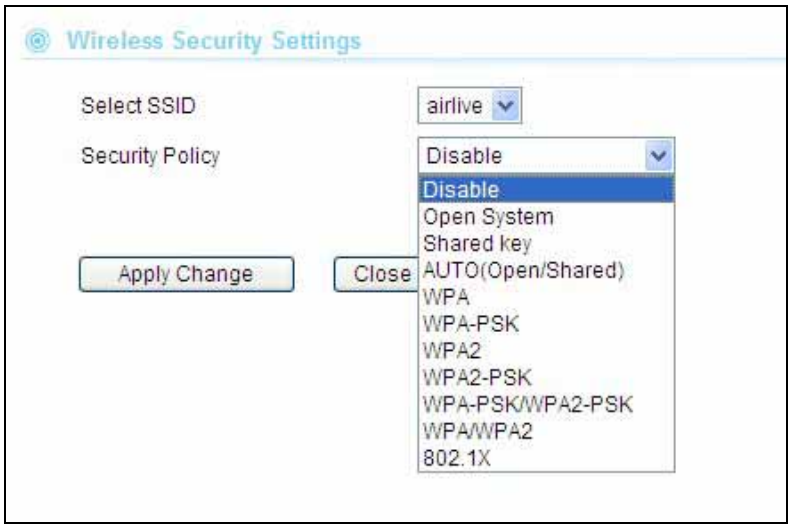


4.5.4 Wireless Security

Wireless Settings -> Wireless Security

You should set up the wireless security immediately to ensure the security of your data transmission and to prevent the unauthorized access. ***The easiest way to setup encryption is to use the "Setup Wizard". It automatically chooses the most secured and easiest scheme for your wireless security settings.*** However, if you wish to choose your own encryption scheme, the Air3G offers various type of encryption including WEP, WPA-PSK, WPA, WPA2, WPA2-PSK encryptions method. In general, the WPA-PSK and WPA2-PSK are the most popular and secured encryption scheme.

Procedure to make encryption

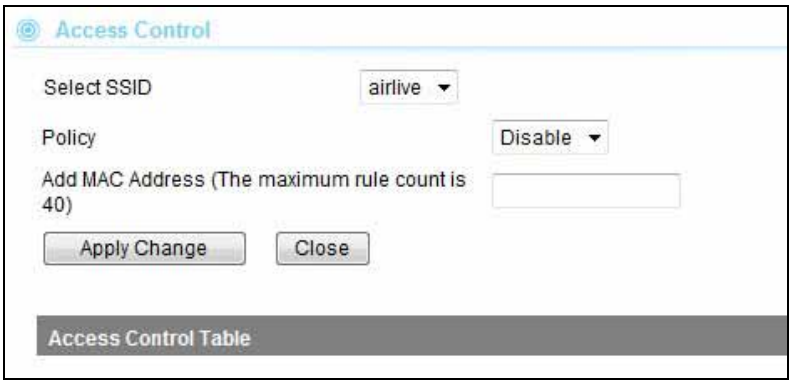


- **Step1**: **Select your SSID:** If you have enabled the "Multiple SSID" function, there will be more than one SSID to choose from. Each SSID(Virtual AP) can have its own security policy.
- **Step2**: **Select Security Policy**: Air3G offers a full suite of security policy including WEP(Pre-Shared Key), WPA(certificate), WPA-PSK(AES), WPA2-PSK(AES), and 802.1x Radius Authentication. Recently WiFi regulation prevent the use of TKIP encryption in 11n mode. Therefore, the TKIP is only available in 11b/g mode. ***We highly recommend using WPA2-PSK AES Encryption as the easiest and very secured scheme for encryption.***

4.5.5 Access Control

Wireless Settings -> Access Control

The Air3G allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and AP Router modes. This function is available only for Access Point and Gateway modes.



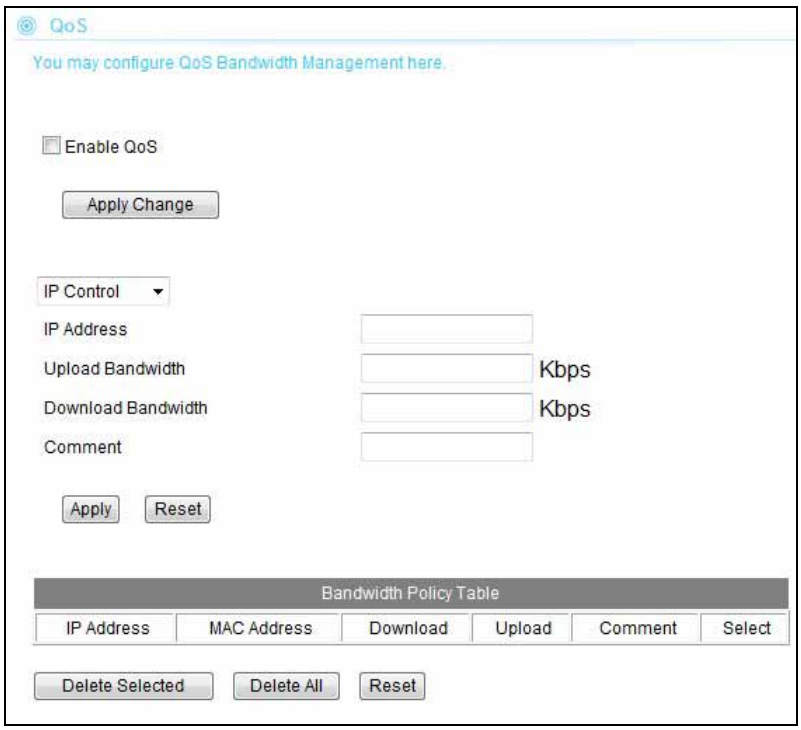
- **Disable:** When selected, no MAC address filtering will be performed.
- **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
- **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

4.5.6 Bandwidth Control

Wireless Settings -> Bandwidth Control

The Air3G can limit the bandwidth by IP address or MAC address. Please first enable the Bandwidth Control, then select IP Control or MAC Control.

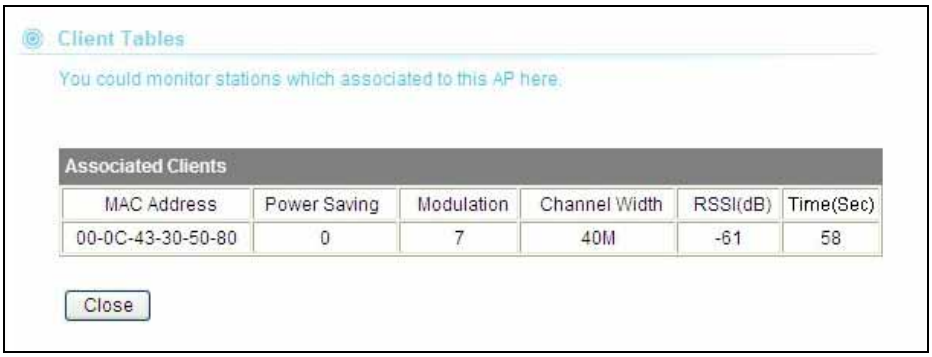
- **Enable Bandwidth Control:** Check this box and press "Apply Change" to enable bandwidth control
  - **IP Control:** To limit the bandwidth of one single IP address.
  - **MAC Control:** To limit the bandwidth of one single MAC address.
  - **Upload Bandwidth:** please input upstream bandwidth limit in Kbps
  - **Download Bandwidth:** please input downstream bandwidth limit in Kbps
  - **Comment:** note for the bandwidth policy



4.5.7 Associated Client

Wireless Settings -> Associated Client

You can check the wireless clients' status on this table



- **MAC Address**: MAC address of the wireless clients. If you need to find the IP address, please go to ***Status->Client Table*** menu.
- **Power Saving**: **0**: The power saving mode is off. **1**: The power saving mode is on.
- **Modulation**: Show the which MCS level is used in 11n mode
- **Channel Width**: This indicates whether client is using 20MHz or 40MHz channel wdith.
- **RSSI(dBm)**: The signal strength of the client device.
- **Time(Sec)**: The connected time of the wireless client.

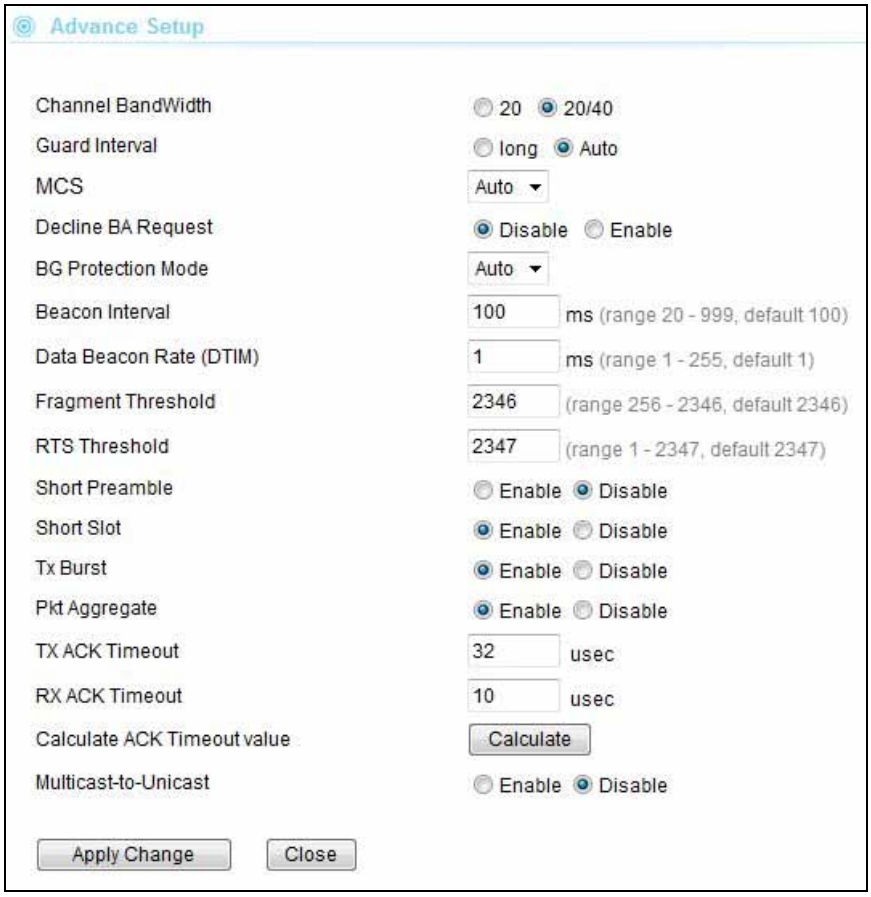
4.5.8 Advanced Settings

Wireless Settings -> Advance Settings

- **Channel Width:** You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

- **Guard Interval**: Guard interval is placed at the beginning of each transmission. It is used to reduce the interference effect of multi-path transmissions. The use of long Guard Interval may perform better in interference or multipath environment. However, it can reduce the performance.

- **MCS (Modulation and Code Scheme):** MCS level for the 11n mode. It is recommended to leave it at Auto.



- **Decline BA Request:** Enable this option to decline the Block ACK requests by other devices.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance..

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

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

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold

must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Short Preamble**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **Tx Burst and Packet Aggregate:** These are the scheme used for improving the performance of the data transmission in 11n and Turbo modes. It is recommended to keep the settings on.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. ***In most conditions, please do not change the Tx and Rx Acktimeout value. The Air3G's default value is correct in most case.s.***

4.5.9 WMM Settings

Wireless Settings -> WMM Settings

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM Settings is to specify parameters on multiple data queue for better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AP.

Configure the WMM QoS Parameters

- **AC Type**

  The queue and associated priorities and parameters for transmission are as follows:

  - **Data 0 (Best Effort, BE):** Medium priority queue, medium throughput anddel ay. Most traditional IP data is sent to this queue.
  - **Data 1 (Background, BK):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example):
  - **Data 2 (Video, VI):** High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
  - **Data 3 (Voice, VO):** Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.

  Packets in a higher priority queue will be transmitted before packets in a lower priority queue.

- **ECWmin and ECWmax**

  If an access point detects that the medium is in use, it uses the DCF random backoff timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum*

Contention Window increases exponentially up to a specified limit *Maximum Contention Window.*

The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.

The random backoff used by the access point is a configurable parameter. To describe the random delay, a "*Minimum Contention Window" (ECWMin*) and a "*Maximum Contention Window" (ECWMax)* is defined.

- **ECWmin**: The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- **ECWmax**: If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

- **AIFS**

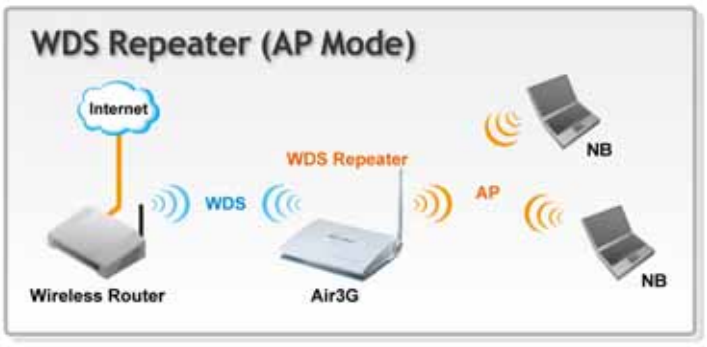
The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for data frames. 802.11e uses interframe spaces to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data. The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free. Valid values for AIFs are 1 through 255.

- **Transmission Opportunity**

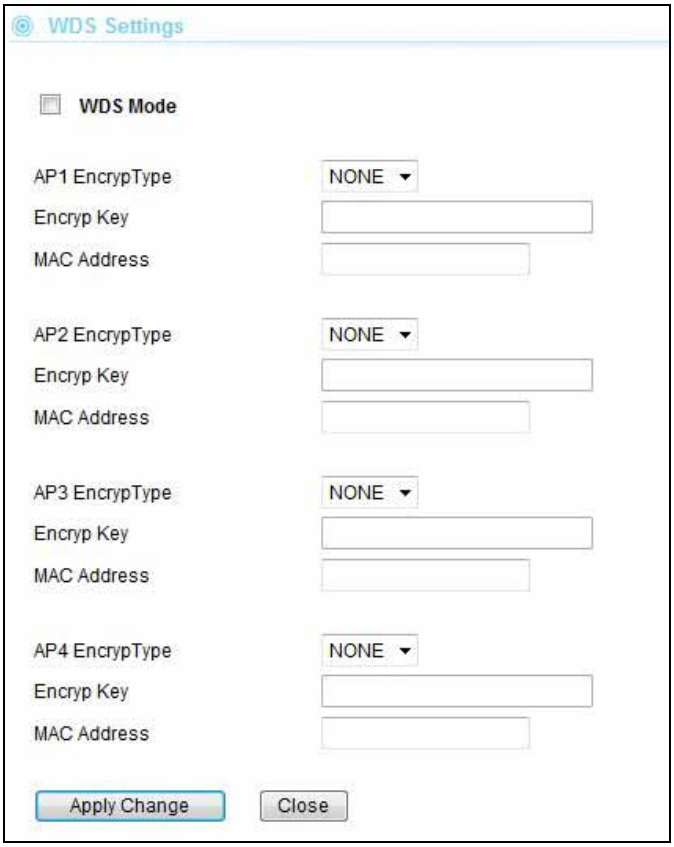
The Transmission Opportunity (TXOP) is an interval of time when a WMM client station has the right to initiate transmissions onto the wireless medium. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

We recommend that you use the default settings on the WMM QoS page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

4.5.10 WDS Settings (Repeater)



This is known as WDS Repeater function. Enable this setting to allow remote WDS equipped AP to extend the wireless signal of Air3G. Up to 4 WDS repeaters can be connect with Air3G. WDS works by entering the wireless MAC addresses (also known as BSSID) of remote Access Points.



- **EncrypType:** You can use one of the following 4 encryption type.
  - **None:** no encryption is made. This is not recommended as it posts serious security issue.
  - **WEP:** This is the most compatible type. However, it is also easier for hackers to break. Use this only if AES or TKIP doesn't work.
  - **TKIP:** Temporal Key Integrity Protocol, TKIP is more secured than WEP but less secure than AES.

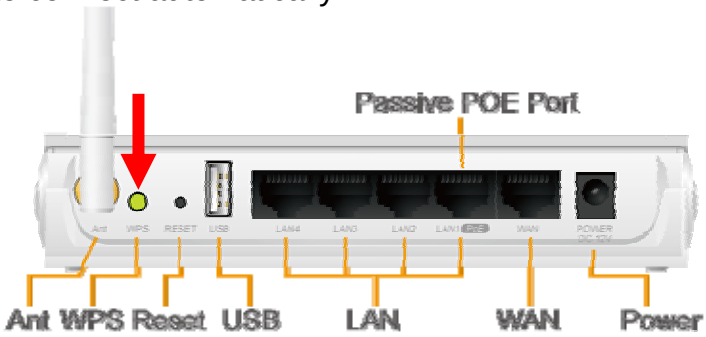
- **AES:** The most secured encryption method. It is highly recommended to use this method unless for compatibility issue.

- **Encryp Key:** Please enter your encryption key here.
- **MAC Address:** Please enter the Wireless MAC address or BSSID of the remote Bridge. You can usually find it at remote Bridge's device label.

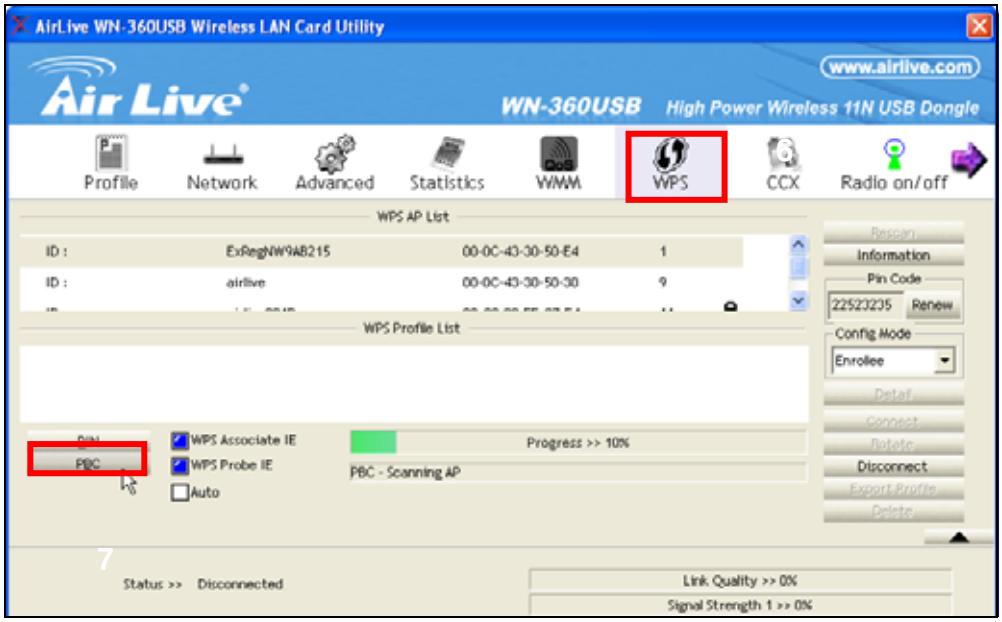
4.5.11 WPS Settings

Example1: Using Hardware Push button

Please push WPS button directly on the back of the Air3G. The "WPS" LED flash will light and the Air3G will start to survey the client's WPS signal in the current environment. Please be noticed that, within **two minutes**, you have to turn on the utility of your wireless network card and click PBC to connect automatically.

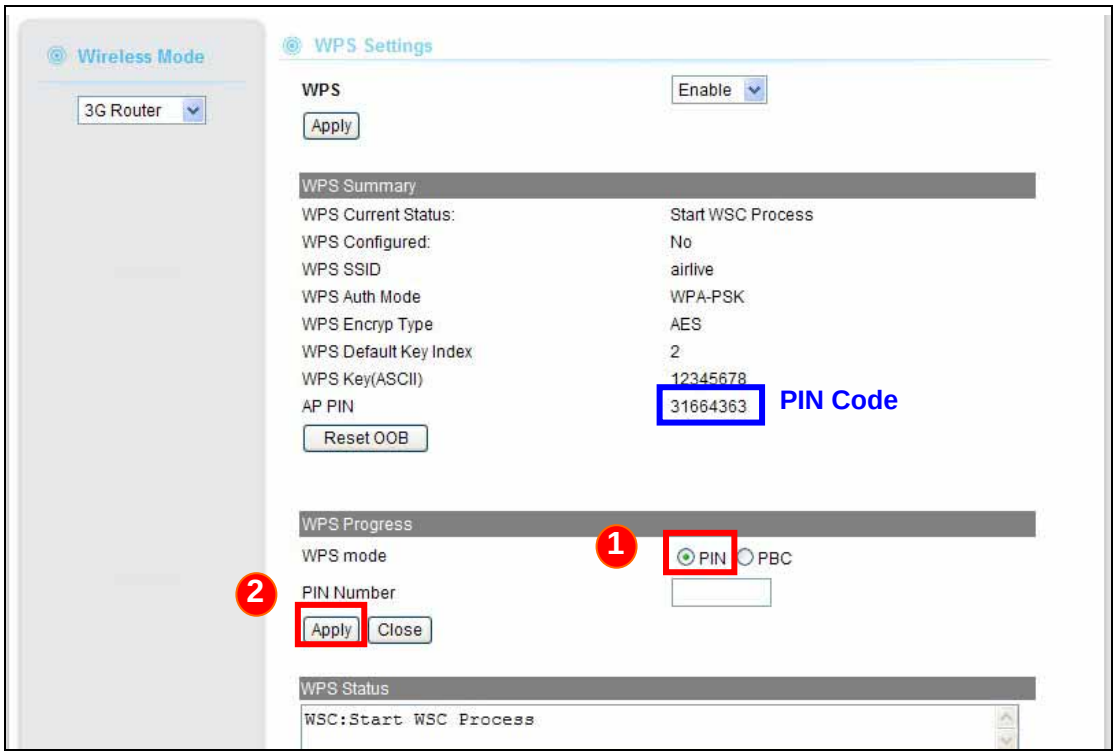


If you also have a hardware WPS button on your wireless card, you can push the button immediately now. If not, you can usually find the WPS PBC function in the wireless utility. Below is an example using AirLive WN-360USB wireless network card to connect with Air3G.

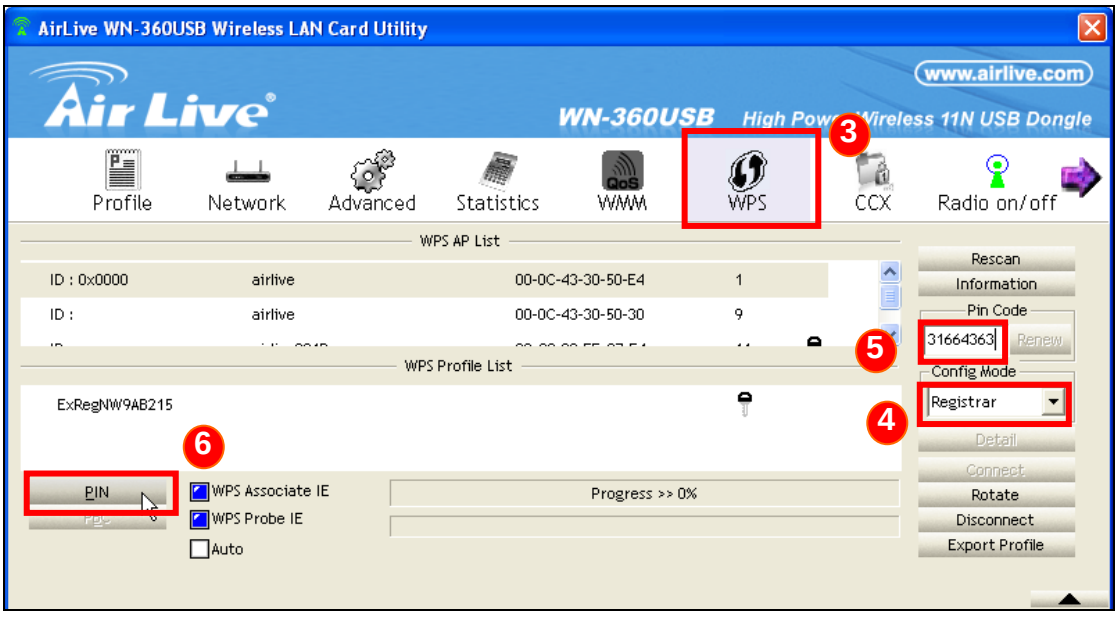


Example 2: WPS Using PIN

Please login Air3G's Web UI. Select Wireless Setting → WPS Setting. In the WPS Progress, select "PIN" then "Apply." You will get a PIN Code.



Then, please turn on the utility of your wireless network card. Choose WPS mode to "Registrar" and enter the PIN Code. Press "PIN" and the connection will automatically configure.

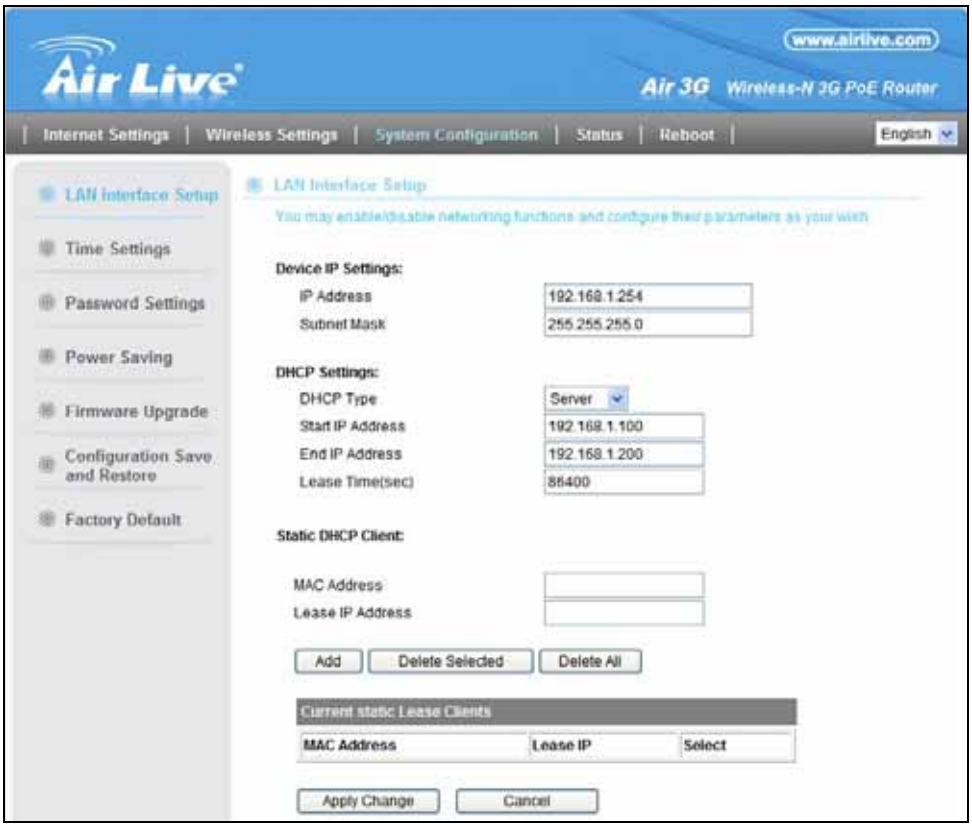


5 System Configuration and Status Menu

In this chapter, we will explain about *System Configurations* Menu and the Status Menu of the web management interface. Please be sure to read through Chapter 3's "*Introduction to Web Management"* first.

5.1 Menu Structure

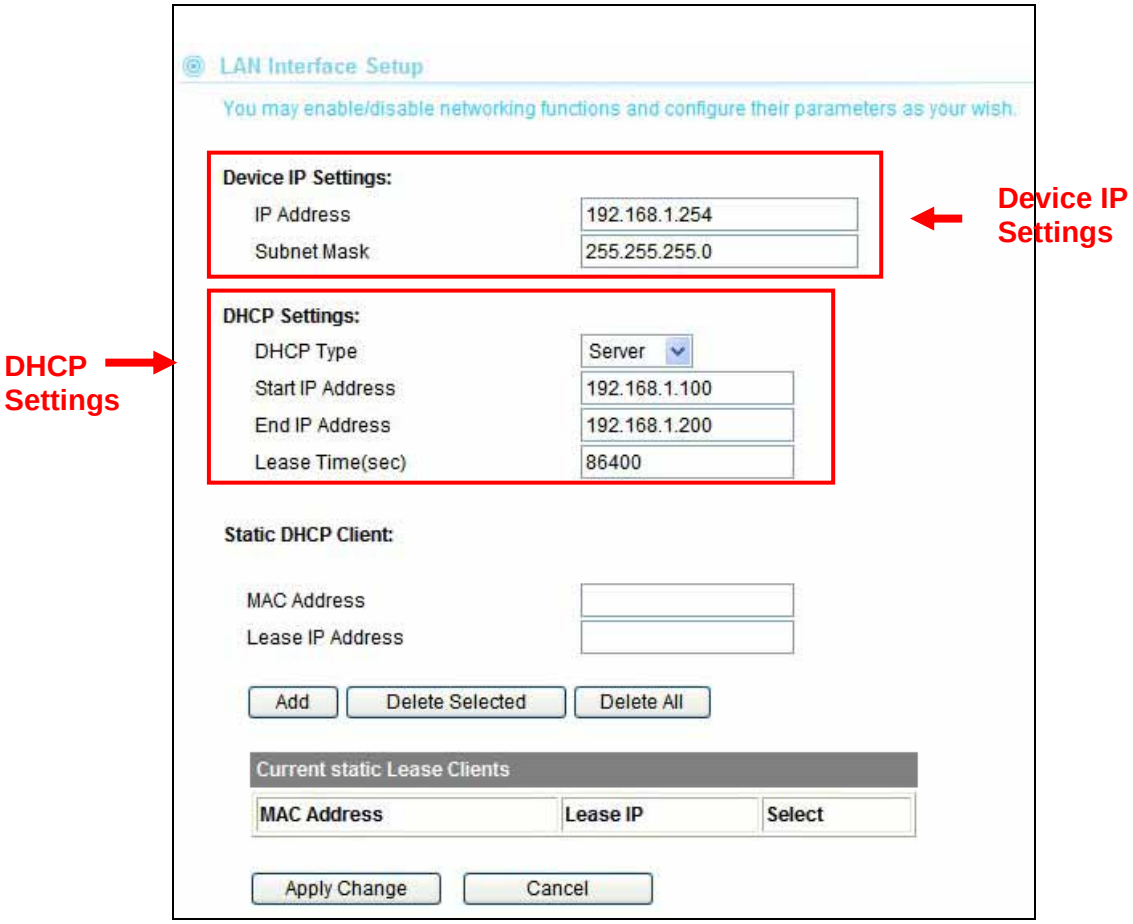
When you click on the "System Configuration" menu on the top menu bar, the following screen will appear. The system configuration includes all non-wireless settings. We will explain their functions here.



5.2 LAN Interface Setup

System Configuration>> LAN Interface Setup

This menu is where you can configure all the aspect about LAN interface including IP address, DHCP server settings..etc.



5.2.1 DHCP Settings

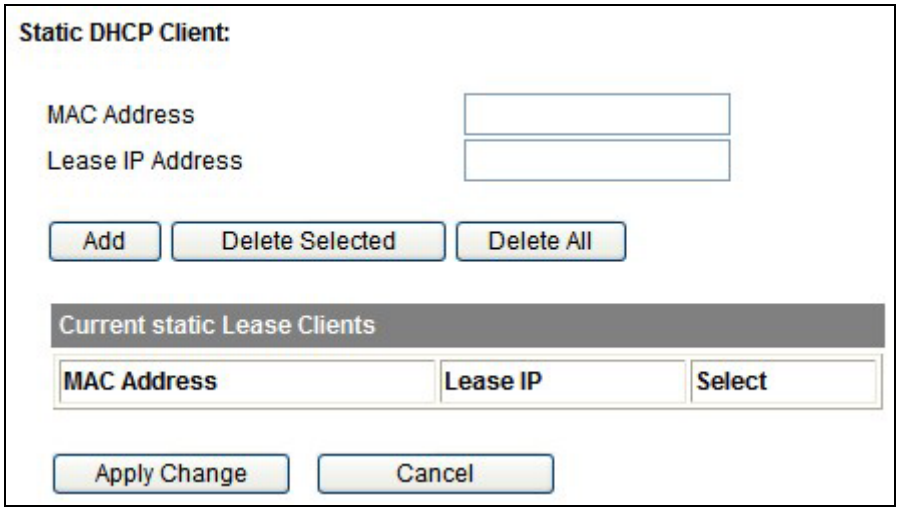
- **DHCP Service:** You can enable or disable DHCP server here.
  - **Disable**: Disable DHCP server. By default, the DHCP server is OFF in AP, Client, and WDS Bridge mode.
  - **Server**: The Air3G will act as DHCP server to provide IP addresses to the clients on the LAN/Wireless interface. By default, the DHCP server is on in 3G router mode.
- **DHCP Client Range**: You can define the IP pool from which the DHCP clients can get IP address.. Click on “Show Clients” to see the current DHCP client table.
- **Lease Time:** You can define how long the Air3G will reserve IP address for a

particular PC or Devices here.

5.2.2 Add DHCP Static Lease Client

If you want to lock IP address to a MAC address, you should add DHCP clients to the "Static DHCP Client". Up to 40 entries can be entered. Below is the procedure for adding an entry:

1. Enter the MAC address of the device
2. Enter the IP address of the device
3. Click on the "Add" button



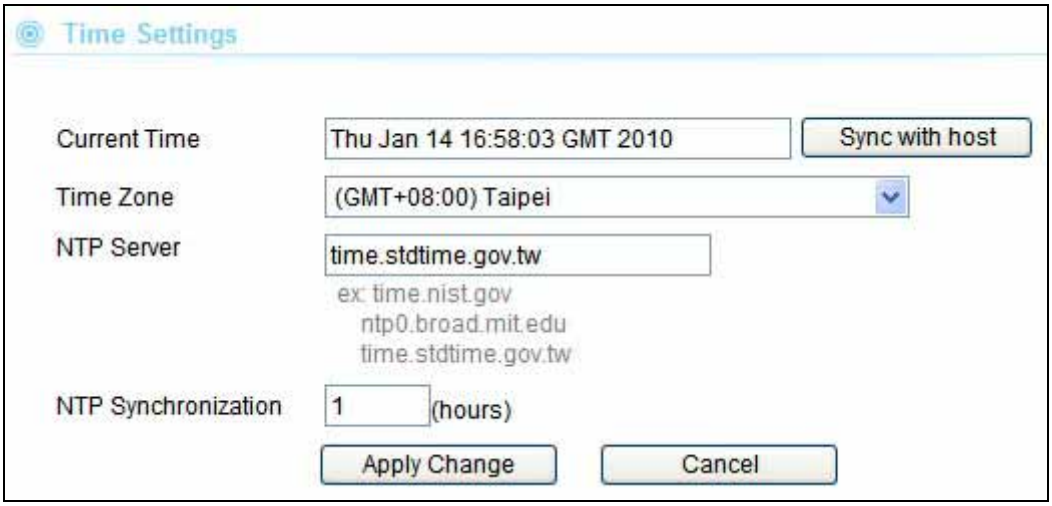
5.3 Time Settings

System Configuration ->Time Settings

You can set the Air3G's internal system clock by 2 methods. First is to enter the time manually. Second is to set the time by NTP server. We strongly recommend setting the time by NTP server because it will sync the time with remote server even after power recycling. In another word, you will not lose time settings after power off.

- **Sync with Host**: Push this button to copy the time from your PC
- **Time Zone**: Select your nearby city here
- **NTP Server**: This is the time server where your Air3G will sync the time with.
- **NTP Synchronization**: How often your Air3G will sync the time with remote NTP server.

Please remember to apply change after completing all settings.



5.4 Password Settings

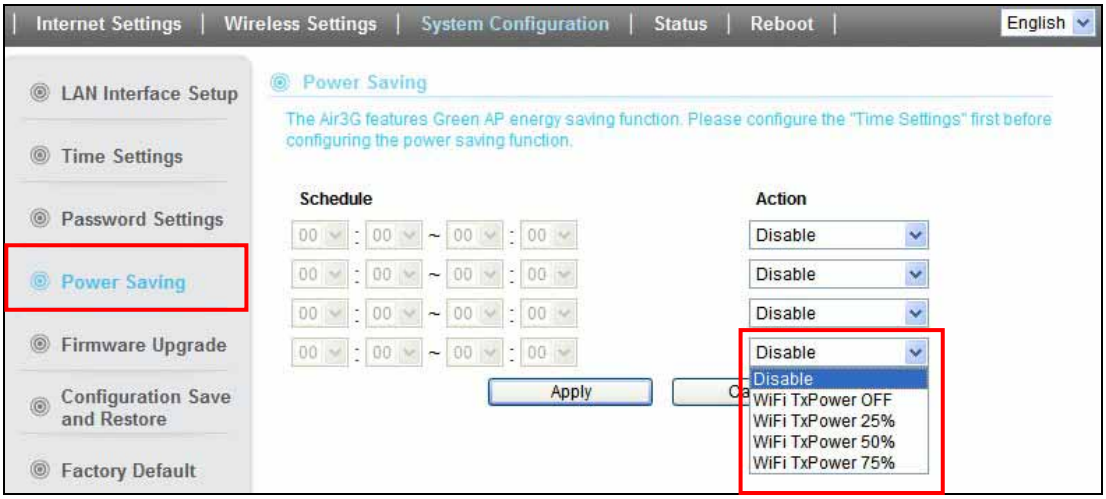
System Configuration -> Password Settings

You can change your username and password from the image below:

5.5 Power Saving (Green AP)

System Configuration -> Power Saving

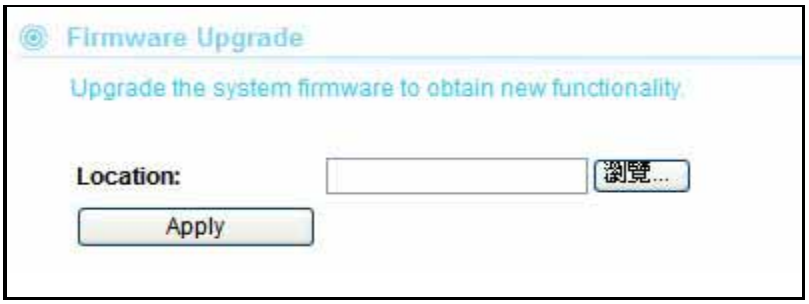
The power saving scheduling function allows user to define the wireless service time and output power level. It can be used to conserve the energy of your AP. Please remember to set the time first



5.6 Firmware Upgrade

System Configuration -> Firmware Upgrade

You can upgrade the firmware of your Air3G (the software that controls your Air3G's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version.



- **Upgrade Firmware:**

  To update the Air3G firmware, first download the firmware from AirLive web site to your local disk. Then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Apply** button to start.

The new firmware will be loaded to your Air3G. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

> ⚠ Do not power off the device while upgrading the firmware.
> It is recommended that you do not upgrade your Air3G unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

5.7 Configuration Save and Restore

System Configuration -> Configuration Save and Restore

The Air3G can save and restore the settings to a file.

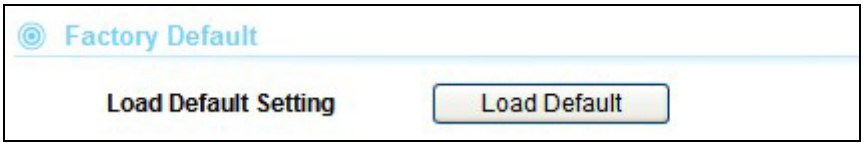
You can save system configuration settings to a file, and later download it back to the Air3G

- **Export Settings:** Export the configuration file to your PC so you can restore the settings later.
- **Import Settings file location:** Please browse for the configuration file location for restoration of settings

5.8 Factory Default

System Configuration -> Factory Default

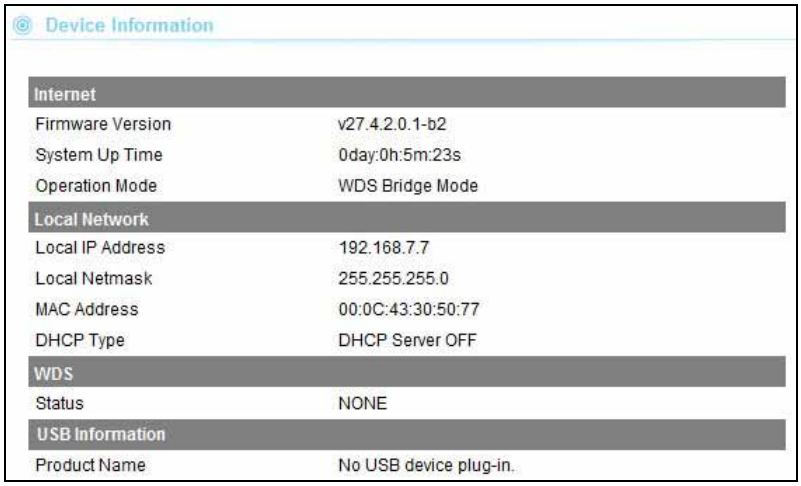
You can reset the configuration of your Air3G to the factory default settings.



5.9 Status Menu

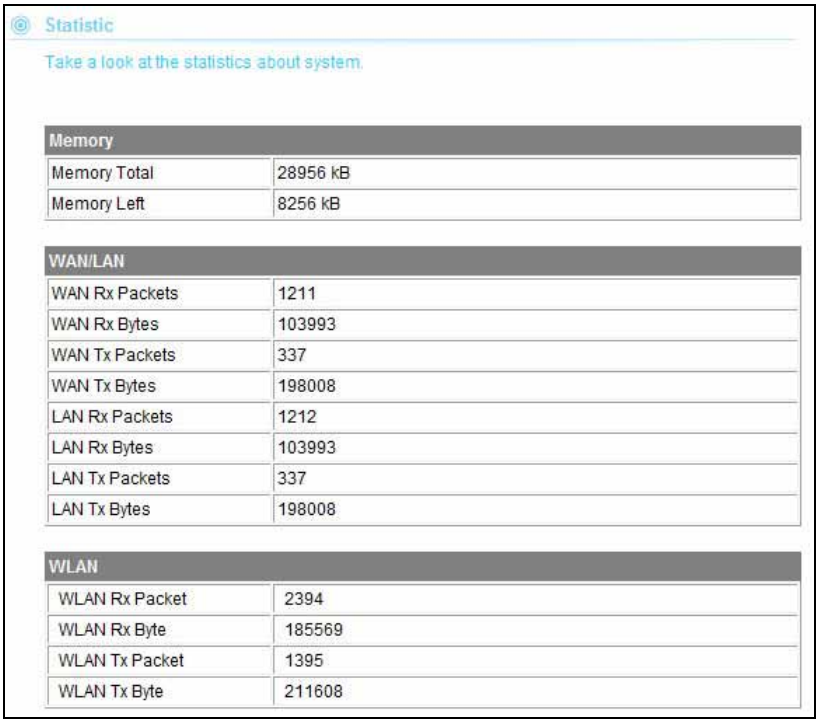
5.9.1 Device Information

From this menu, you can know the Firmware version, System Up time, IP and MAC addresses, and check whether the USB dongle is connected.



5.9.2 Statistic

The Statistic menu displays the memory status, WAN traffic, LAN traffic, and WLAN traffic conditions.

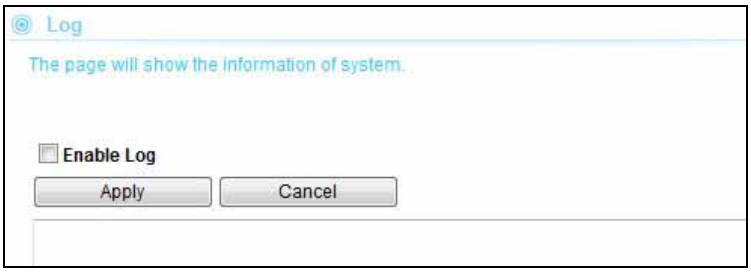


5.9.3 Client Table

The Client Table is also known as ARP table. It will show all the IP and MAC addresses of the devices that pass Air3G.

5.9.4 LOG

When you enable the log function, system will keep records of events and errors detected.



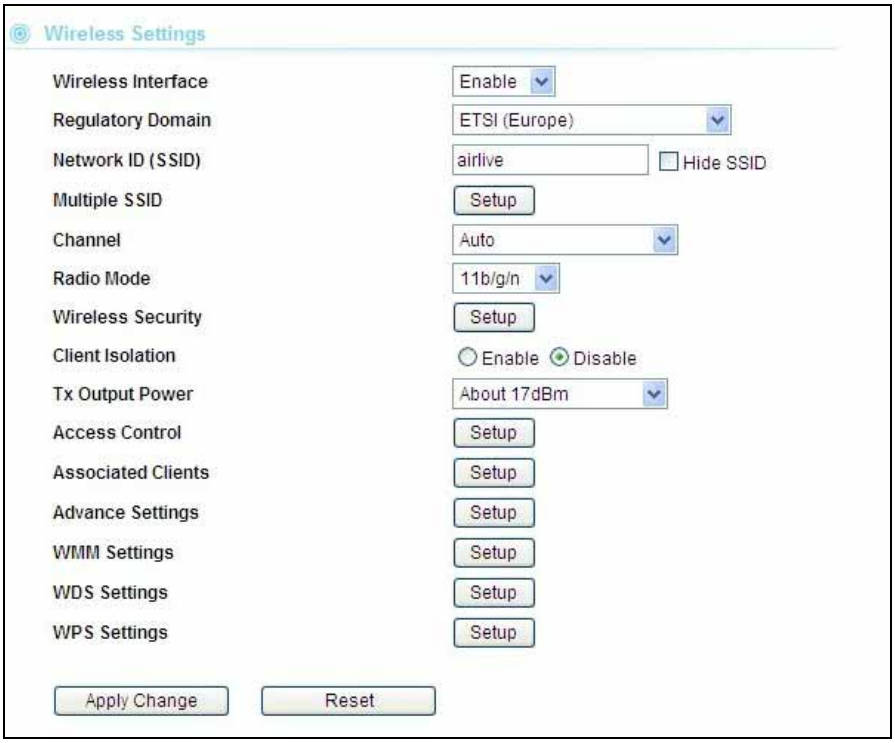
6 AP Mode

In this chapter, we will explain about the wireless settings for AP Mode. Please be sure to read through Chapter 1.4 and Chapter 3's *"Wireless Operation Mode"* first.

6.1 Application for AP Mode

When operating in the Access Point mode, the Air3G becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through Air3G. This type of network is known as "Infrastructure network". Other Air3G or 802.11 b/g/n devices can connect to AP mode through "Client Mode.

6.2 Wireless Settings



6.2.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

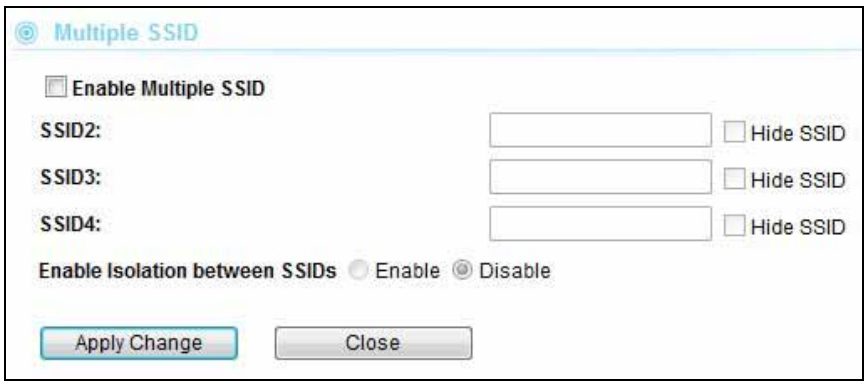
The Air3G is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	30dBm
South America(14 CH)	1~14	30dBm

6.2.2 Multiple SSID

Wireless Settings -> Multiple SSID

Multiple SSID allows Air3G to create up to **4** different wireless networks (SSID). It is also known as “Virtual AP” function. Each SSID can have its Encryption policy. The SSID1 is the main SSID under Wireless Setting page.



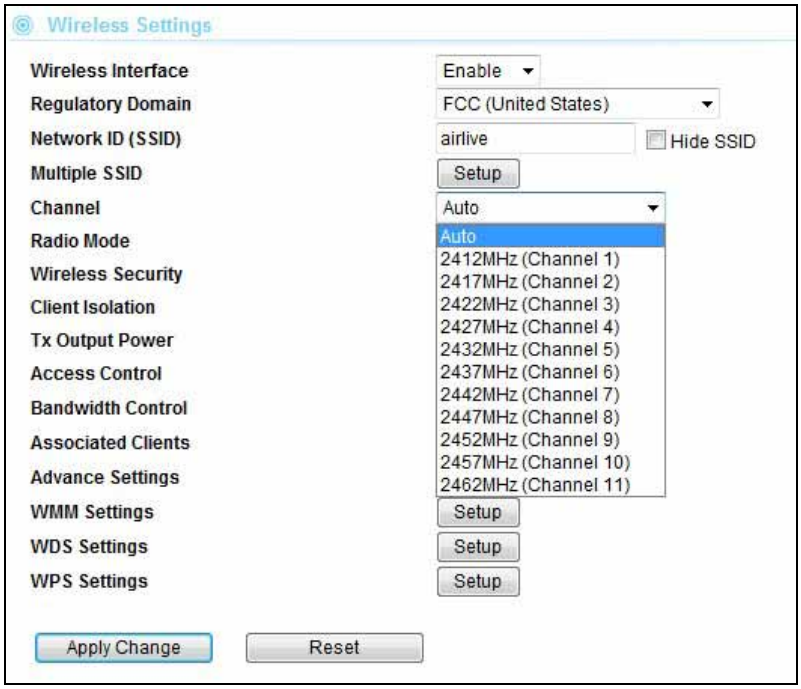
- **Hide SSID**: The wireless network will become invisible, only accessible to people who knows the SSID name.
- **Enable Isolation between SSIDs**: Enable this option will disable traffic between different SSIDs.

6.2.3 Channel

Wireless Settings -> Channel

The channel is the frequency range used by radio. In 802.11g/b standard, there are maximum of 14 Channels. However, the available channels in each country are dependant on the local regulation. If you are living in Europe, you can use channel 1 to 13. If you are living in the United States, you can use channel 1 to 11.

Each wireless channel takes between 22 to 25MHz of frequency width. But the channels are only 5MHz apart. Therefore, only every 5 channels can be free of interference with each other. It is recommended that you can do a site survey to find about what channels are used by surrounding AP and choose a channel that is not used by other APs.

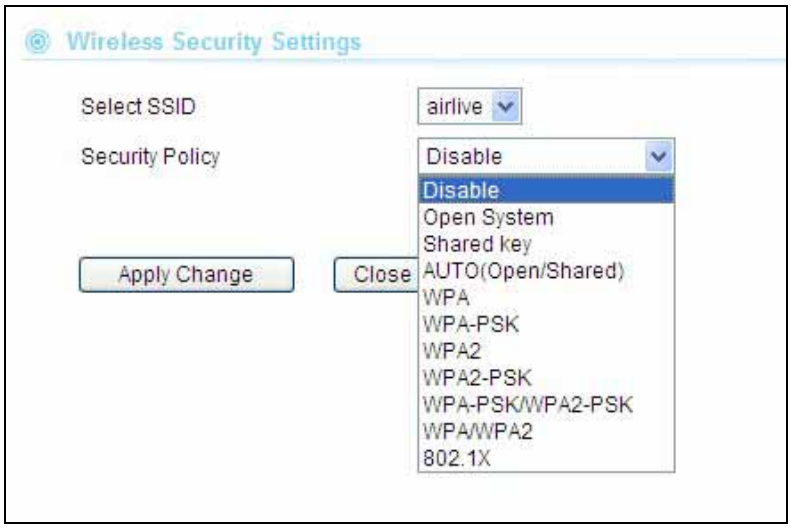


6.2.4 Wireless Security

Wireless Settings -> Wireless Security

You should set up the wireless security immediately to ensure the security of your data transmission and to prevent the unauthorized access. ***The easiest way to setup encryption is to use the "Setup Wizard". It automatically chooses the most secured and easiest scheme for your wireless security settings.*** However, if you wish to choose your own encryption scheme, the Air3G offers various type of encryption including WEP, WPA-PSK, WPA, WPA2, WPA2-PSK encryptions method. In general, the WPA-PSK and WPA2-PSK are the most popular and secured encryption scheme.

Procedure to make encryption

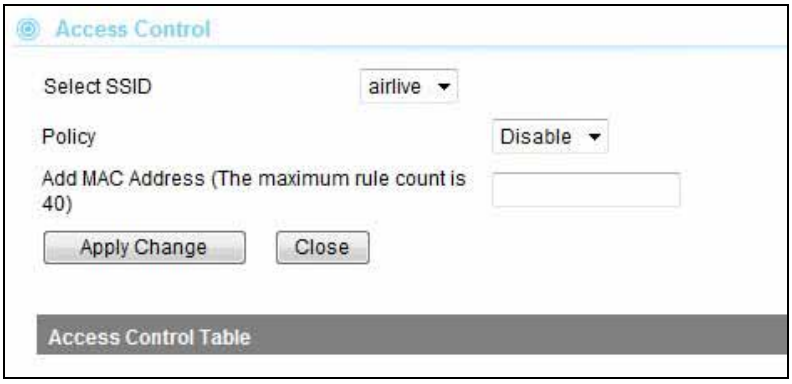


- **Step1**: **Select your SSID:** If you have enabled the "Multiple SSID" function, there will be more than one SSID to choose from. Each SSID(Virtual AP) can have its own security policy.
- **Step2**: **Select Security Policy**: Air3G offers a full suite of security policy including WEP(Pre-Shared Key), WPA(certificate), WPA-PSK(AES), WPA2-PSK(AES), and 802.1x Radius Authentication. Recently WiFi regulation prevent the use of TKIP encryption in 11n mode. Therefore, the TKIP is only available in 11b/g mode. ***We highly recommend using WPA2-PSK AES Encryption as the easiest and very secured scheme for encryption.***

6.2.5 Access Control

Wireless Settings -> Access Control

The Air3G allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and AP Router modes. This function is available only for Access Point and Gateway modes.



- **Disable:** When selected, no MAC address filtering will be performed.
- **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
- **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

6.2.6 Associated Client

Wireless Settings -> Associated Client

You can check the wireless clients' status on this table

- **MAC Address**: MAC address of the wireless clients. If you need to find the IP address, please go to ***Status->Client Table*** menu.
- **Power Saving**: **0**: The power saving mode is off. **1**: The power saving mode is on.
- **Modulation**: Show the which MCS level is used in 11n mode
- **Channel Width**: This indicates whether client is using 20MHz or 40MHz channel wdith.
- **RSSI(dBm)**: The signal strength of the client device.
- **Time(Sec)**: The connected time of the wireless client.

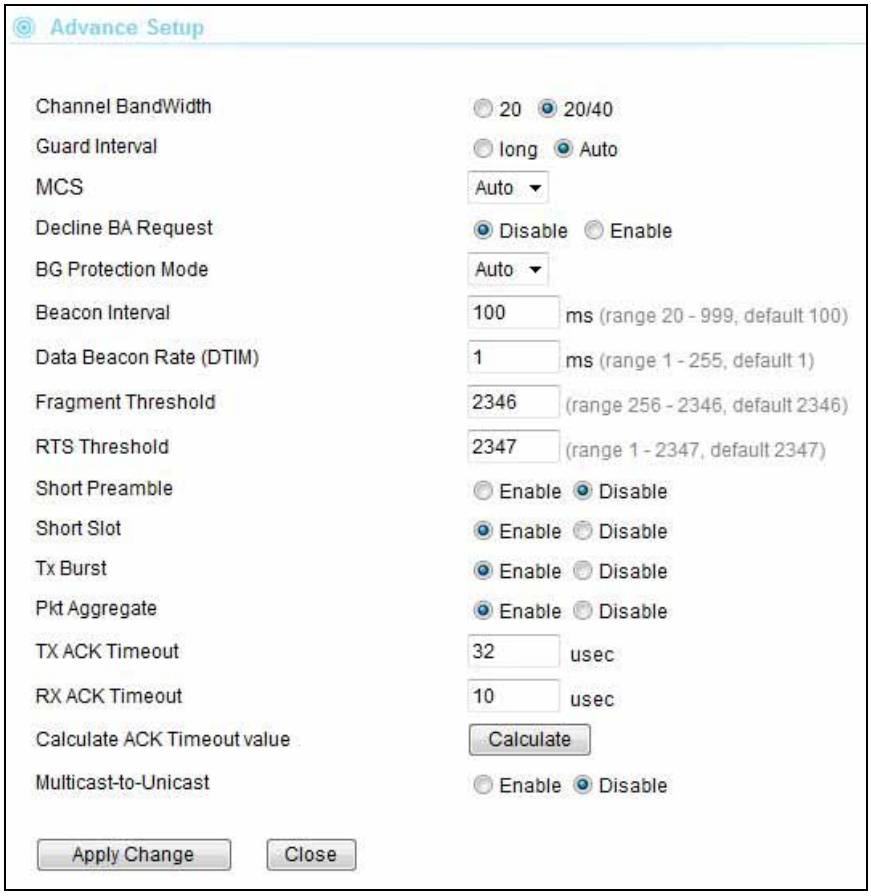
6.2.7 Advanced Settings

Wireless Settings -> Advance Settings

- **Channel Width:** You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

- **Guard Interval**: Guard interval is placed at the beginning of each transmission. It is used to reduce the interference effect of multi-path transmissions. The use of long Guard Interval may perform better in interference or multipath environment. However, it can reduce the performance.

- **MCS (Modulation and Code Scheme):** MCS level for the 11n mode. It is recommended to leave it at Auto.



- **Decline BA Request:** Enable this option to decline the Block ACK requests by other devices.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance..

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between

1 and 65,535.

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

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Short Preamble**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

- **Tx Burst and Packet Aggregate:** These are the scheme used for improving the performance of the data transmission in 11n and Turbo modes. It is recommended to keep the settings on.

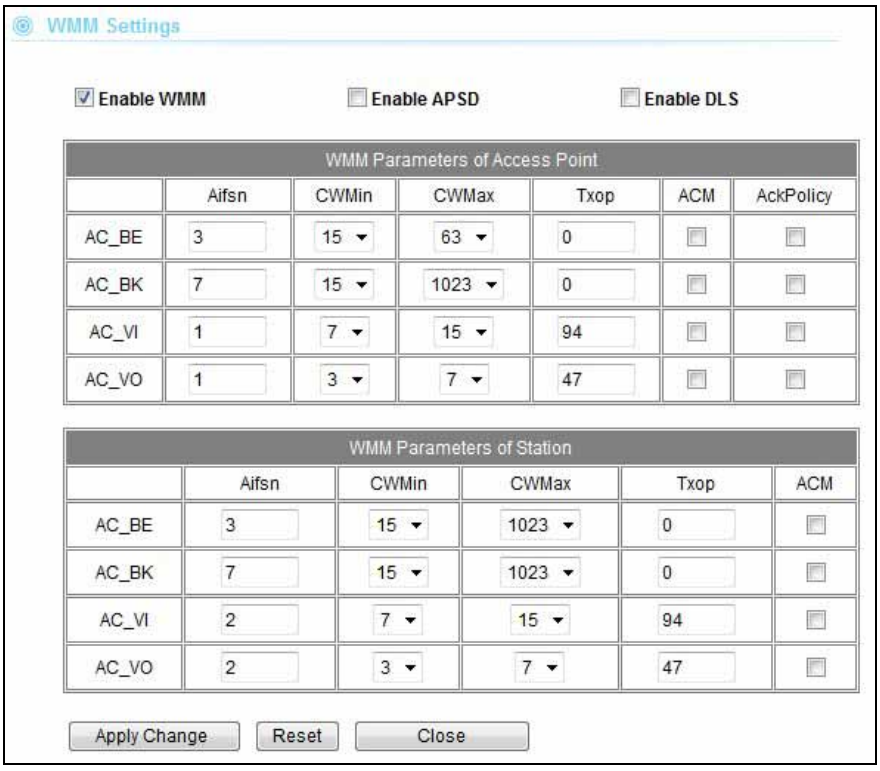
- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. ***In most conditions, please do not change the Tx and Rx Acktimeout value. The Air3G's default value is correct in most cases.***

6.2.8 WMM Settings

Wireless Settings -> WMM Settings

Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM Settings is to specify parameters on multiple data queue for better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AP.

Configure the WMM QoS Parameters



- **AC Type**

  The queue and associated priorities and parameters for transmission are as follows:

  - **Data 0 (Best Effort, BE):** Medium priority queue, medium throughput anddel ay. Most traditional IP data is sent to this queue.
  - **Data 1 (Background, BK):** Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example):
  - **Data 2 (Video, VI):** High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.
  - **Data 3 (Voice, VO):** Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.

  Packets in a higher priority queue will be transmitted before packets in a lower priority queue.

- **ECWmin and ECWmax**

  If an access point detects that the medium is in use, it uses the DCF random backoff timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum*

Contention Window increases exponentially up to a specified limit *Maximum Contention Window.*

The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.

The random backoff used by the access point is a configurable parameter. To describe the random delay, a "*Minimum Contention Window" (ECWMin*) and a "*Maximum Contention Window" (ECWMax)* is defined.

- **ECWmin**: The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- **ECWmax**: If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

- **AIFS**

The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for data frames. 802.11e uses interframe spaces to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data. The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free. Valid values for AIFs are 1 through 255.

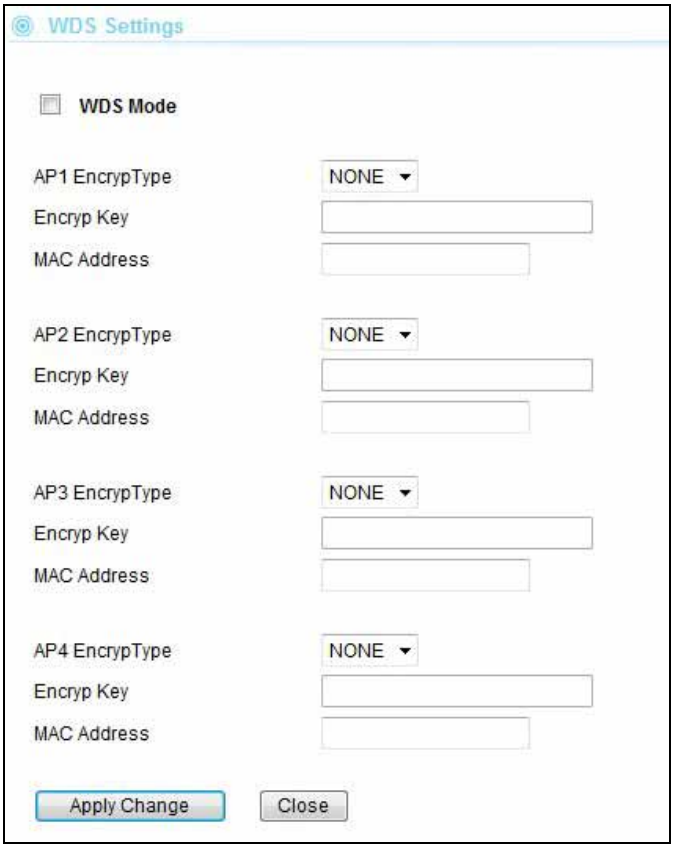
- **Transmission Opportunity**

The Transmission Opportunity (TXOP) is an interval of time when a WMM client station has the right to initiate transmissions onto the wireless medium. This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

We recommend that you use the default settings on the WMM QoS page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

6.2.9 WDS Settings (Repeater)

This is known as WDS Repeater function. In AP mode, the Air3G will repeat the wireless signal of remote AP/Router. Up to 4 WDS repeaters can be connect with Air3G. WDS works by entering the wireless MAC addresses (also known as BSSID) of remote Access Points.



- **EncrypType:** You can use one of the following 4 encryption type.
  - **None:** no encryption is made. This is not recommended as it posts serious security issue.
  - **WEP:** This is the most compatible type. However, it is also easier for hackers to break. Use this only if AES or TKIP doesn't work.
  - **TKIP:** Temporal Key Integrity Protocol, TKIP is more secured than WEP but

less secure than AES.

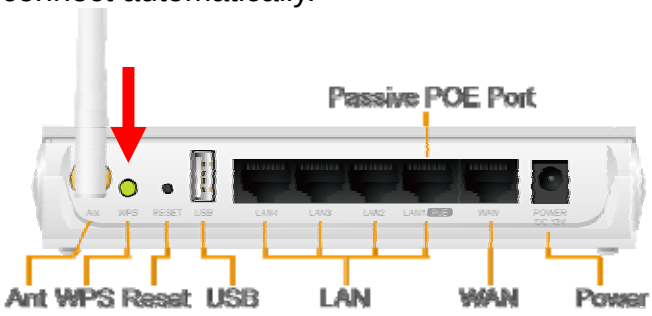
- **AES:** The most secured encryption method. It is highly recommended to use this method unless for compatibility issue.

- **Encryp Key:** Please enter your encryption key here.
- **MAC Address:** Please enter the Wireless MAC address or BSSID of the remote Bridge. You can usually find it at remote Bridge's device label.

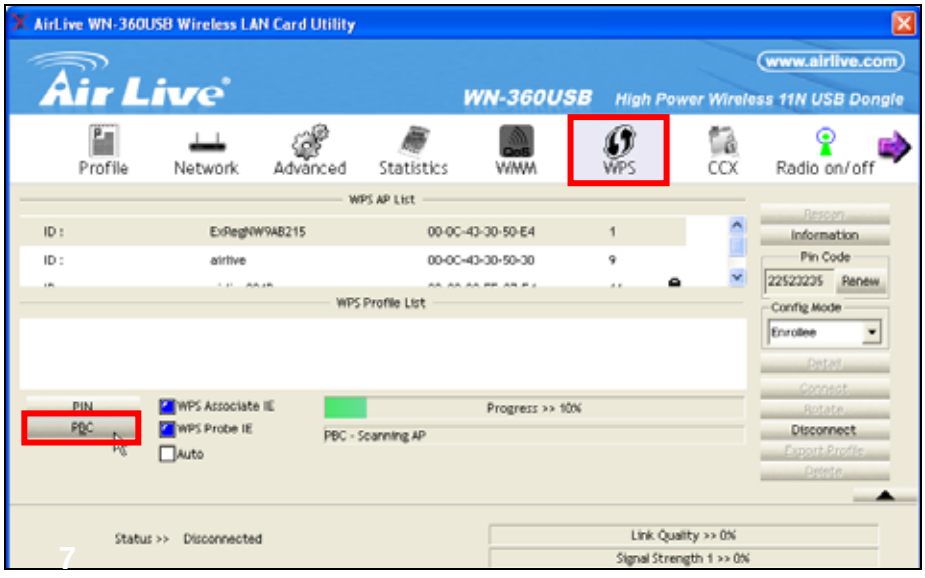
6.2.10 WPS Settings

Example1: Using Hardware Push button

Please push WPS button directly on the back of the Air3G. The "WPS" LED flash will light and the Air3G will start to survey the client's WPS signal in the current environment. Please be noticed that, within **two minutes**, you have to turn on the utility of your wireless network card and click PBC to connect automatically.

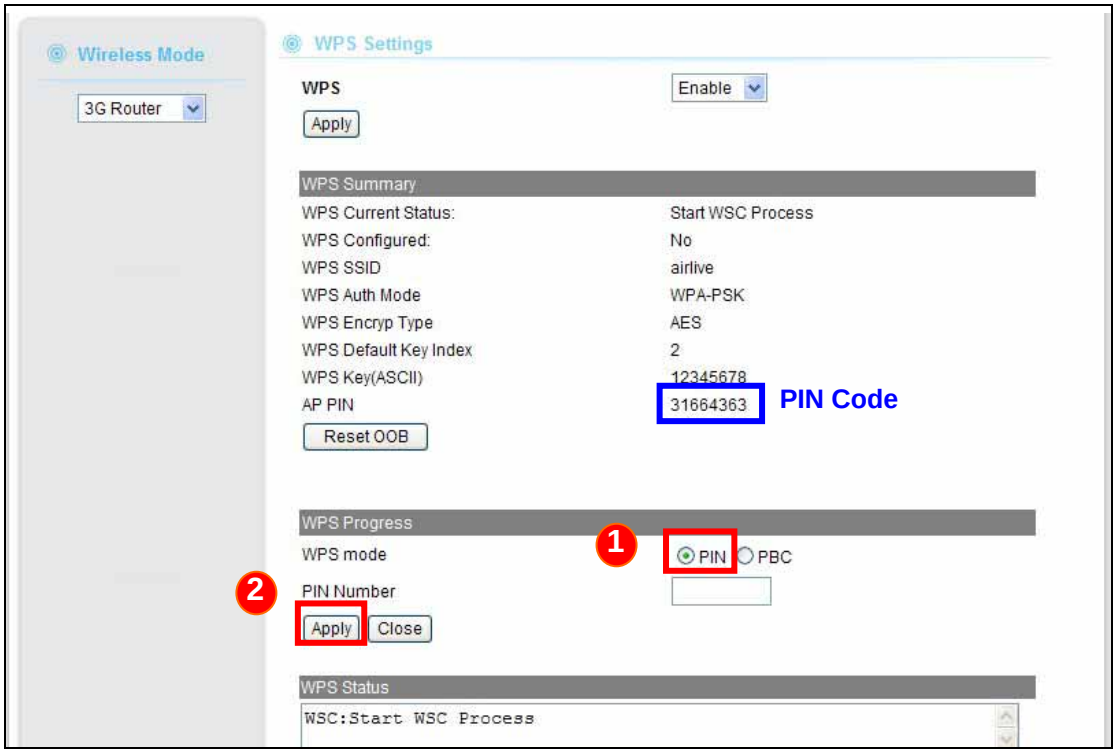


If you also have a hardware WPS button on your wireless card, you can push the button immediately now. If not, you can usually find the WPS PBC function in the wireless utility. Below is an example using AirLive WN-360USB wireless network card to connect with Air3G.

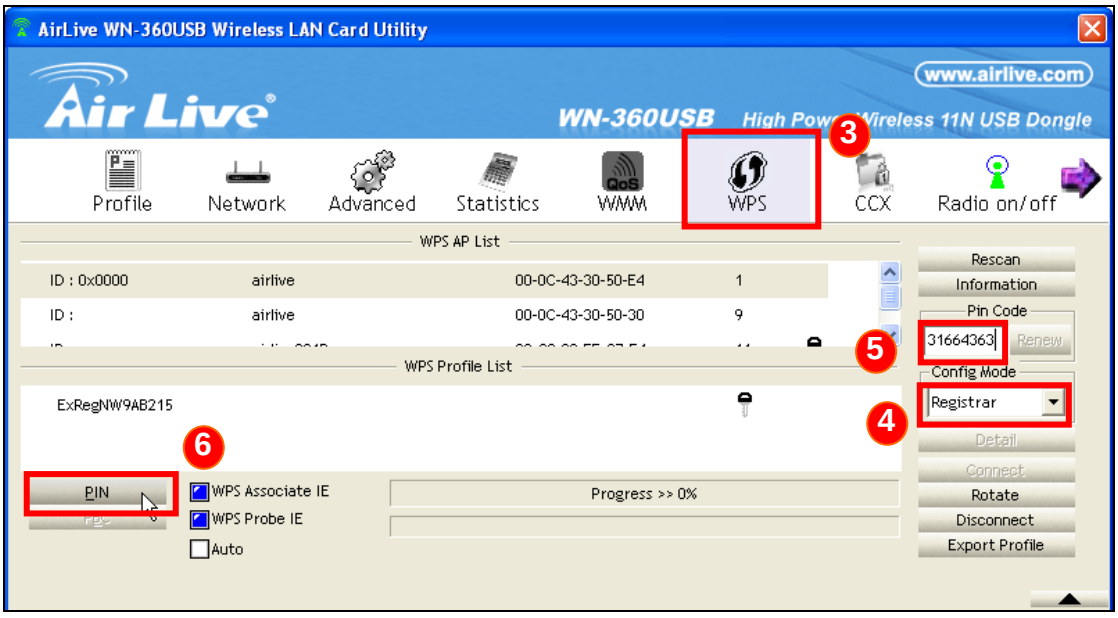


Example 2: WPS Using PIN

Please login Air3G's Web UI. Select Wireless Setting → WPS Setting. In the WPS Progress, select "PIN" then "Apply." You will get a PIN Code.



Then, please turn on the utility of your wireless network card. Choose WPS mode to "Registrar" and enter the PIN Code. Press "PIN" and the connection will automatically configure.



7 Client Mode

In this chapter, we will explain about the wireless settings for Client Mode. Please be sure to read through Chapter 1.4 and Chapter 3's *"Wireless Operation Mode"* first.

7.1 Application for Client Mode

This mode is also known as "Client" mode. The Air3G acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of Air3G to get network access.

7.2 Wireless Settings

7.2.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

The Air3G is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	30dBm
South America(14 CH)	1~14	30dBm

7.2.2 Profile Setting

Wireless Settings -> Profile Setting

A profile contains information about a remote AP's network. In Client mode, you can choose to connect with the remote AP using 2 methods.

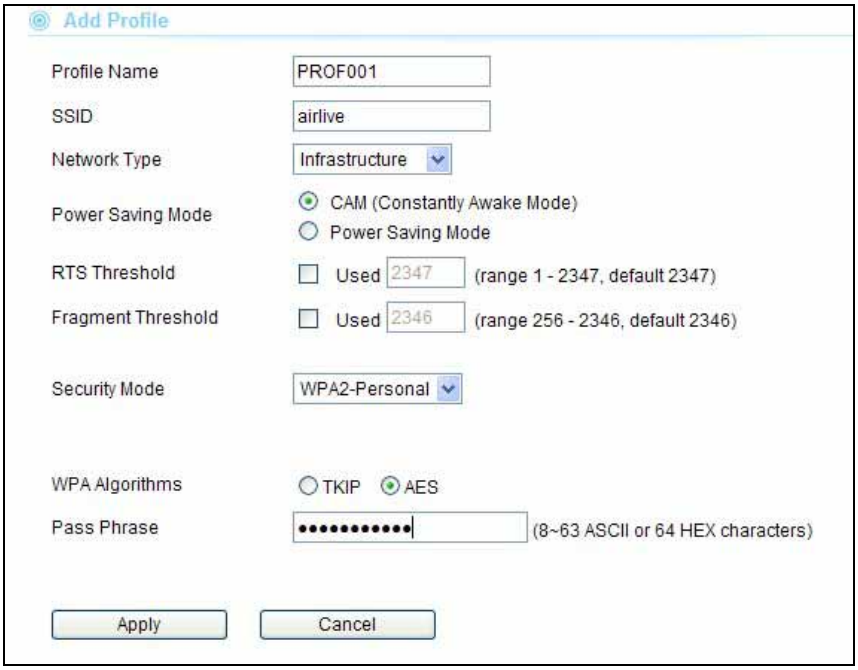
1. Using Site Survey to find the AP you want to connect with, then select the SSID to connect. This is the easiest way.

2. Create a profile about the remote AP you want to connect with. We will talk about Profile in this section.

Procedure to Add a Profile

1. Click on Profile Settings on the Wireless Settings Menu. Then click on "Add" to add a new profile

2. On the Add profile page, please enter the information about the remote AP network such as SSID, encryption. Click on “Apply” once finished



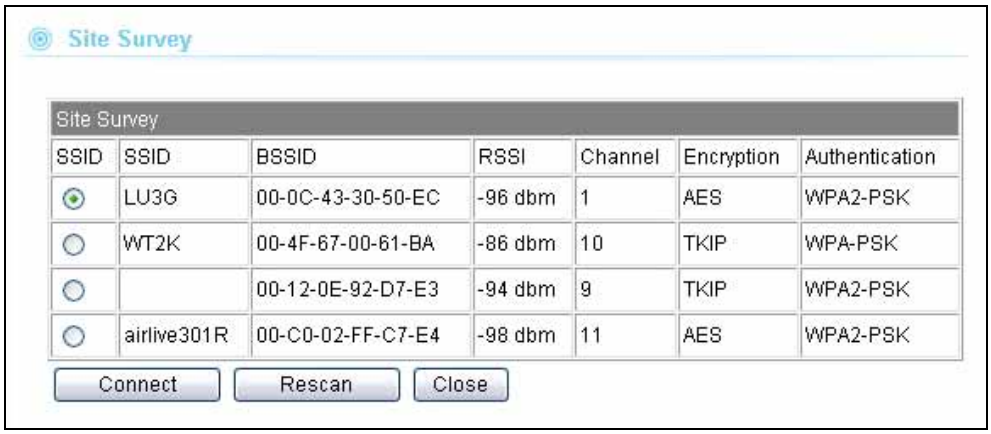
3. Once apply the new profile should appear on the list. Select the profile and click on “Activate” button to take effect Only one profile can be activated at a time.

7.2.3 Site Survey

Wireless Settings -> Site Survey

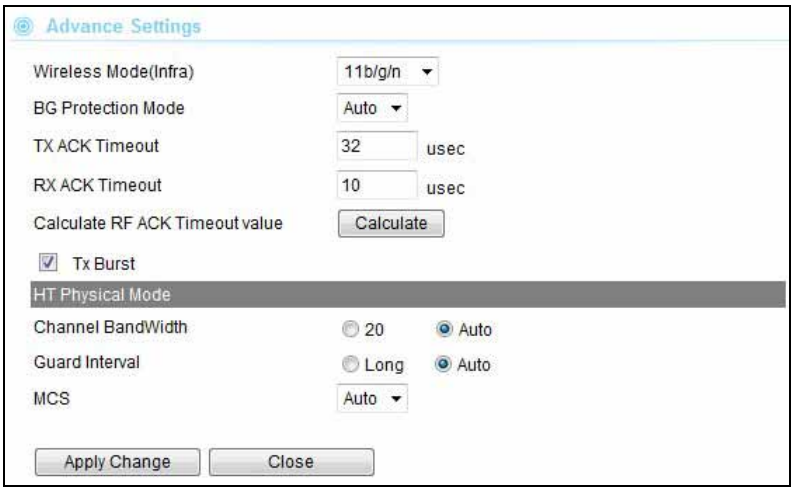
You can scan for wireless networks around your location using the Site Survey function. From the site survey function, you can also perform antenna alignment and establish wireless connection

When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area



You can now select the SSID you want to connect with, then press the “Connect” button. If encryption key is required, the AP will prompt you to enter the encryption information.

7.2.4 Advance Settings



- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network’s performance..

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. ***In most conditions, please do not change the Tx and Rx Acktimeout value. The Air3G’s default value is correct in most cases.***

- **Tx Burst:** These are the scheme used for improving the performance of the data transmission in 11n and Turbo modes. It is recommended to keep the settings on.

- **Channel Width:** You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

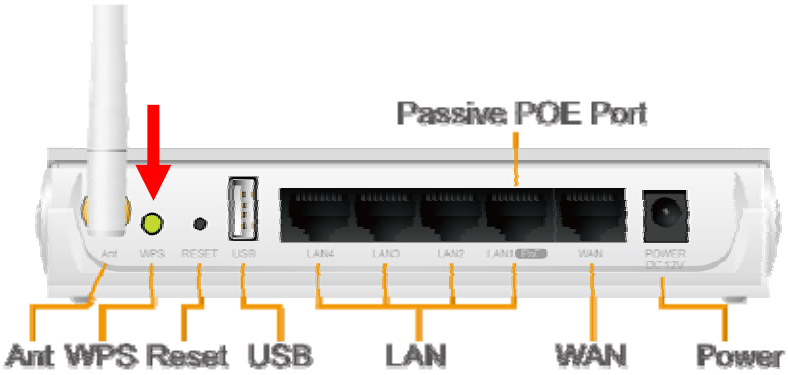
- **Guard Interval**: Guard interval is placed at the beginning of each transmission. It is used to reduce the interference effect of multi-path transmissions. The use of long Guard Interval may perform better in interference or multipath environment. However, it can reduce the performance.

- **MCS (Modulation and Code Scheme):** MCS level for the 11n mode. It is recommended to leave it at Auto.

7.2.5 WPS Settings

Example 1: Using WPS hardware button

Please push WPS button directly on the back of the device. The "WPS" LED flash will light and the Air3G will start to survey the AP's WPS signal in the current environment.

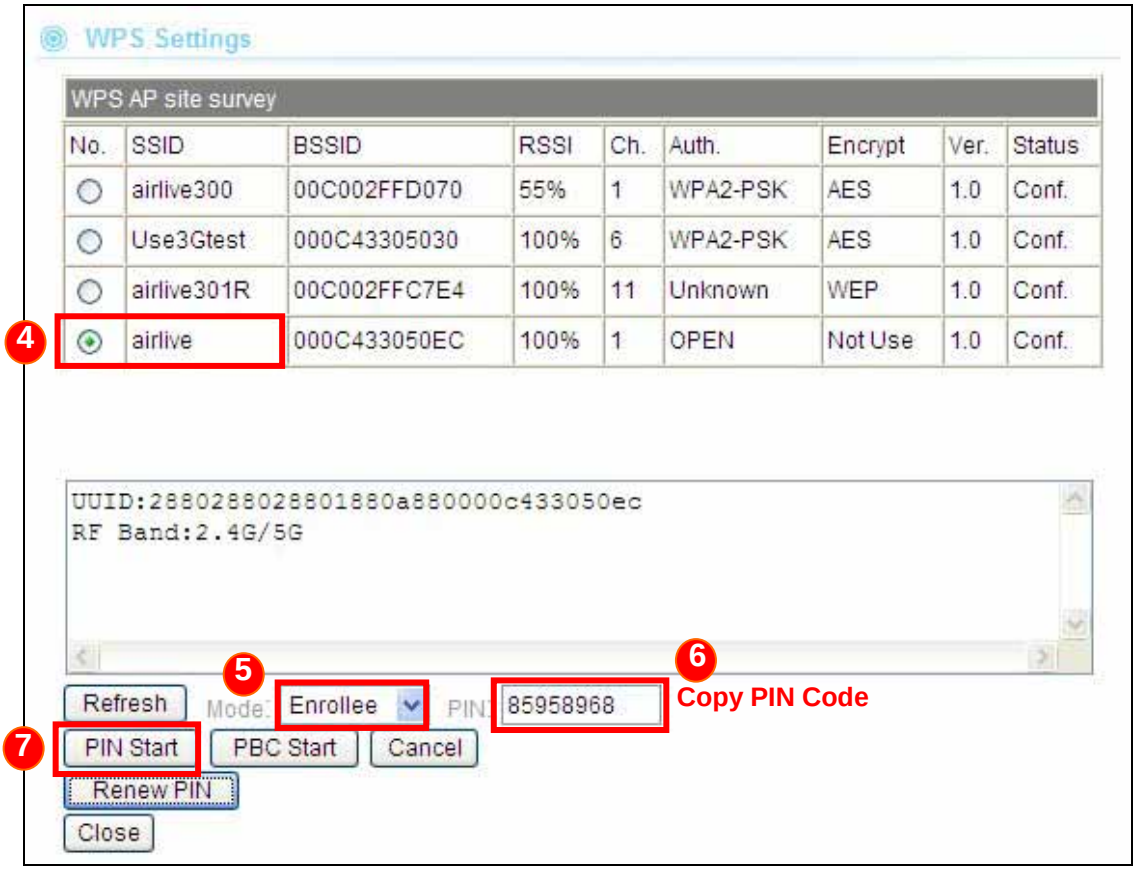


Within two minutes, please push WPS button on your AP device, the connection will automatic successfully.

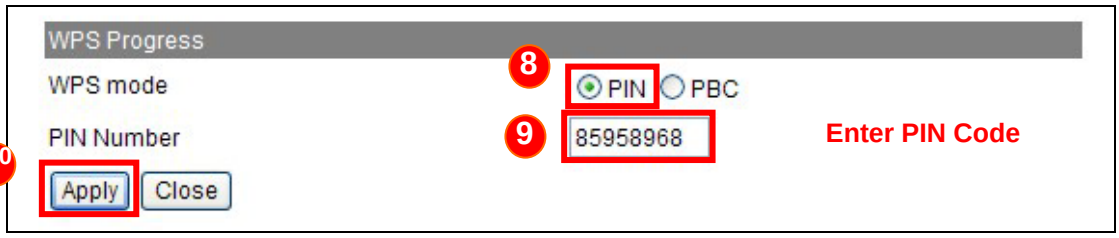
Example 2: WPS using PIN

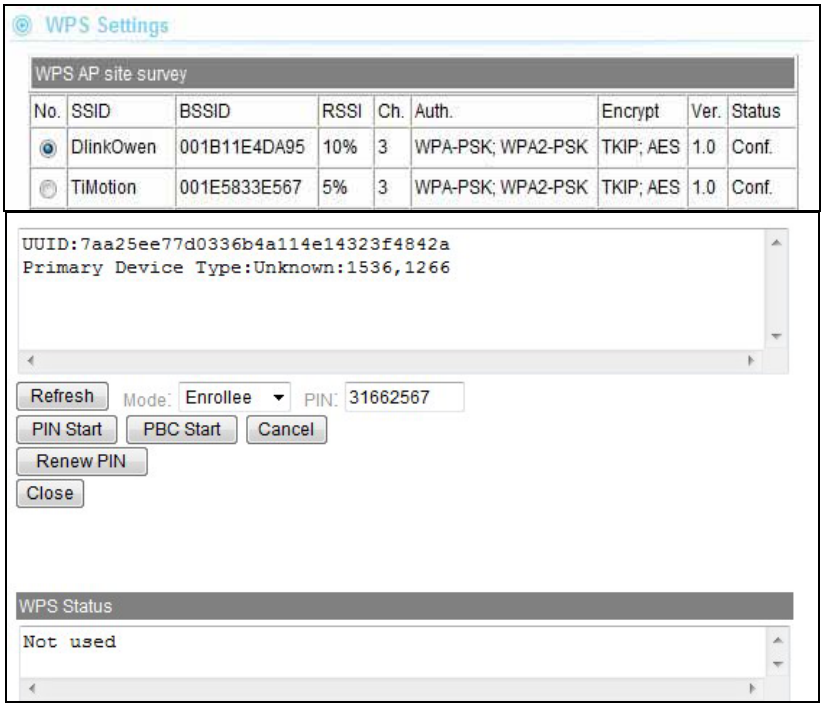
Please login Air3G's Web UI. Select Wireless Setting → change to Client mode → Client WPS Setting.

Select the SSID that you want to connect. Choose WPS mode to “Enrollee” and get a PIN Code in the field. Then press “PIN Start” and the “WPS” LED flash will light two minutes on the device’s housing.



Under AP site, Select Wireless Setting → WPS Setting. Choose WPS mode to “PIN” then enter the PIN Code → click “Apply” and the connection will automatically configure.


WPS Progress
WPS mode
8
PIN
PBC
PIN Number
9
85958968
Enter PIN Code
10
Apply
Close

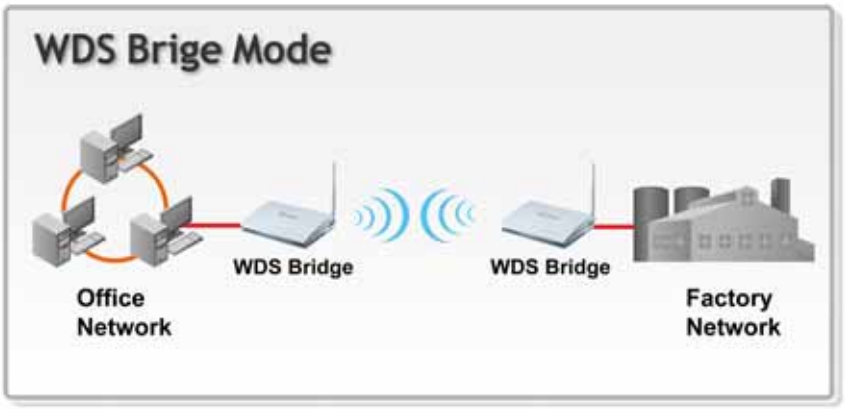

WPS Settings
WPS AP site survey
No. SSID BSSID RSSI Ch. Auth. Encrypt Ver. Status
DlinkOwen 001B11E4DA95 10% 3 WPA-PSK; WPA2-PSK TKIP; AES 1.0 Conf.
TiMotion 001E5833E567 5% 3 WPA-PSK; WPA2-PSK TKIP; AES 1.0 Conf.
UUID:7aa25ee77d0336b4a114e14323f4842a
Primary Device Type:Unknown:1536,1266
Refresh
Mode: Enrollee
PIN: 31662567
PIN Start
PBC Start
Cancel
Renew PIN
Close
WPS Status
Not used

8 WDS Bridge Mode

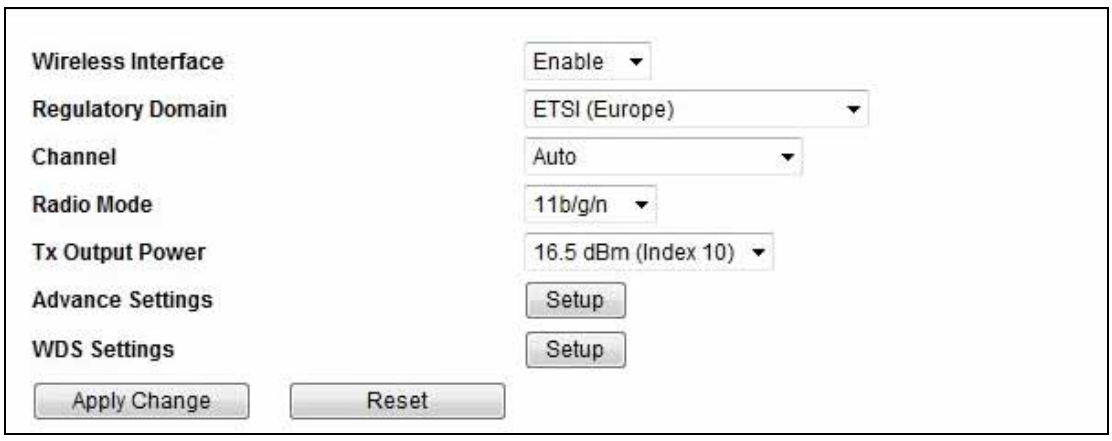
In this chapter, we will explain about the wireless settings for WDS Bridge Mode. Please be sure to read through Chapter 1.4 and Chapter 3's *"Wireless Operation Mode"* first.

8.1 Application for WDS Bridge Mode

This mode is also known as "WDS Pure MAC Bridge mode". Each bridge can associate with maximum of 4 other bridges in the WDS configuration. This mode is best used when you want to connect LAN networks together wirelessly (for example, between office and warehouse). This mode usually delivers faster performance than infrastructure mode.



8.2 Wireless Settings



8.2.1 Regulatory Domain

Wireless Settings -> Regulatory Domain

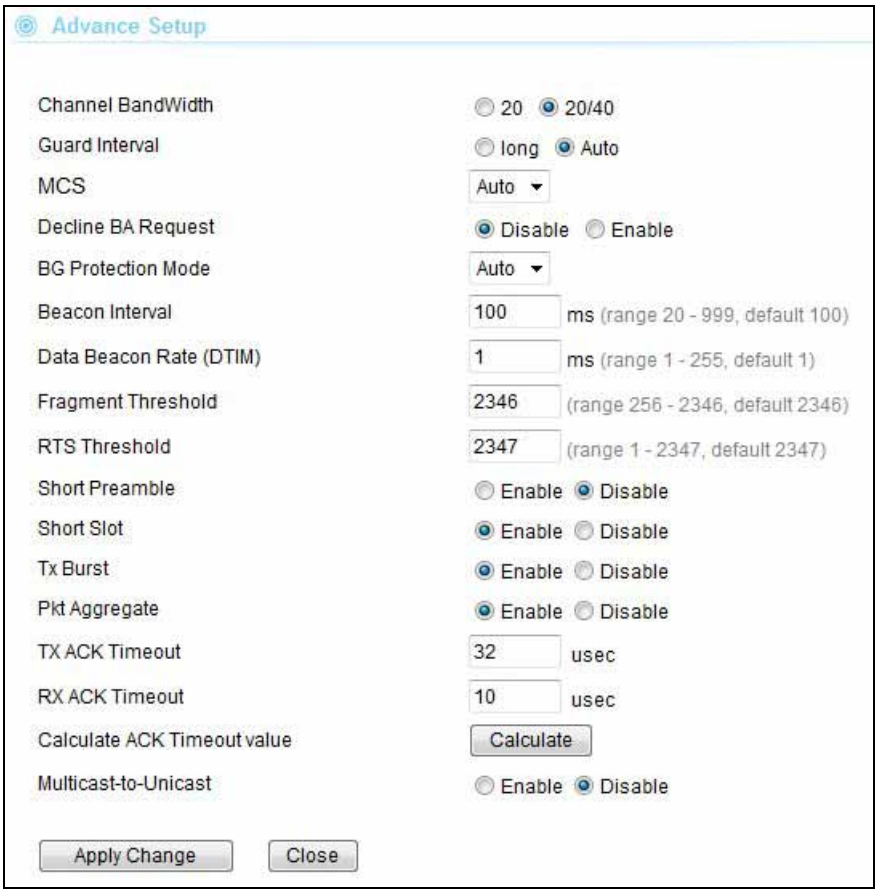
The Regulatory Domain decides what channels and Tx output power levels are available for your country. In most cases, the Regulatory Domain is already selected correctly for your country. Please note that using the wrong Regulatory Domain is strictly prohibited. If you live inside EU, you must use the ETSI Regulatory Domain. If you live in United States, you must use FCC domain.

The Air3G is available with the following Regulatory Domain:

Regulatory Domain	Available Channels	Maximum Tx Output Power
ETSI (Europe)	1 ~13	20dBm
FCC (United States)	1~11	23dBm
South America(11 CH)	1~11	30dBm
South America(14 CH)	1~14	30dBm

8.2.2 Advance Setup

Wireless Settings -> Advance Setup



- **Channel Width:** You can choose 20MHz or 20/40MHz channel width. Choose 20MHz for compliance with laws in some countries. 40MHz offers faster performance than 20MHz

- **Guard Interval**: Guard interval is placed at the beginning of each transmission. It is used to reduce the interference effect of multi-path transmissions. The use of long Guard Interval may perform better in interference or multipath environment. However, it can reduce the performance.

- **MCS (Modulation and Code Scheme):** MCS level for the 11n mode. It is recommended to leave it at Auto.

- **Decline BA Request:** Enable this option to decline the Block ACK requests by other devices.

- **BG Protection:** The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance..

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

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

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Short Preamble**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.

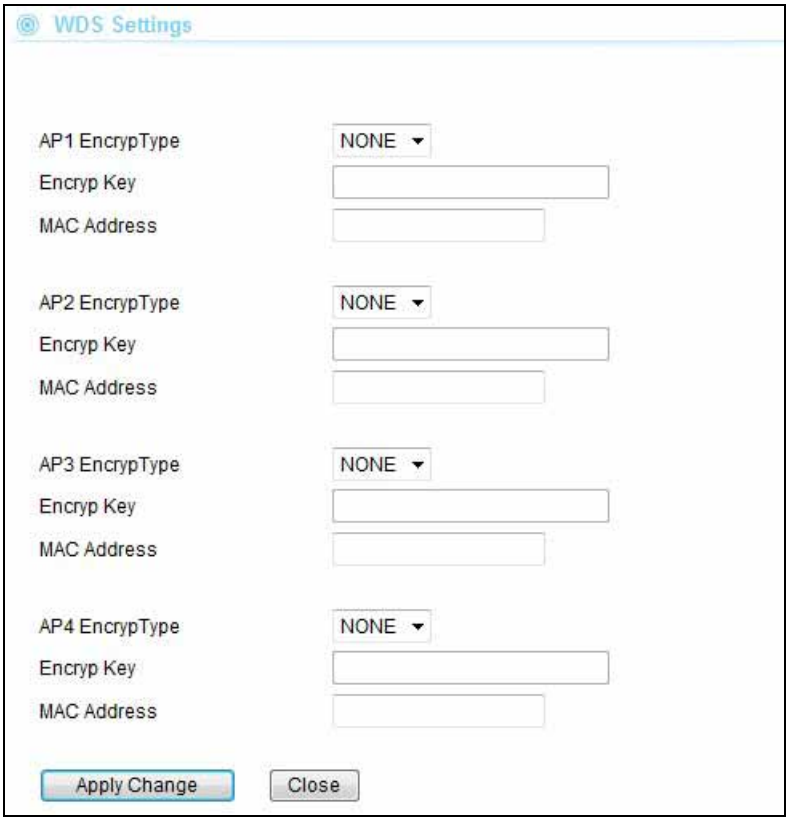
- **Tx Burst and Packet Aggregate:** These are the scheme used for improving the

performance of the data transmission in 11n and Turbo modes. It is recommended to keep the settings on.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. ***In most conditions, please do not change the Tx and Rx Acktimeout value. The Air3G's default value is correct in most case.s.***

8.2.3 WDS Settings

For Bridge network, it is required to enter the Wireless MAC address of all remote bridges that is connected directly to your Air3G. The wireless MAC address is also known as BSSID.



- **Encryp Type:** You can use one of the following 4 encryption type.
  - **None:** no encryption is made. This is not recommended as it posts serious security issue.
  - **WEP:** This is the most compatible type. However, it is also easier for hackers to break. Use this only if AES or TKIP doesn't work.

- **TKIP:** Temporal Key Integrity Protocol, TKIP is more secured than WEP but less secure than AES.
- **AES:** The most secured encryption method. It is highly recommended to use this method unless for compatibility issue.

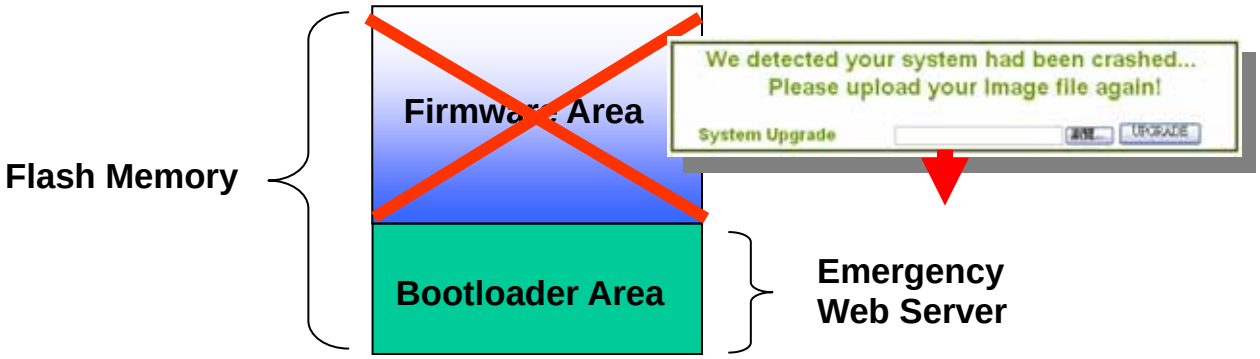
- **Encryp Key:** Please enter your encryption key here.
- **MAC Address:** Please enter the Wireless MAC address or BSSID of the remote Bridge. You can usually find it at remote Bridge's device label.

9 Emergency Firmware Recovery

The Air3G features emergency firmware upgrade function that can restore your AP from a firmware crashed. If you can't access your AP anymore, please first try to restore the setting to default by holding the RESET button (in the back) for more than 10 seconds. You should be able to find the AP at 192.168.1.254. If you can't find it, then please perform the emergency upgrade. Please visit www.airlive.com->support->download and type "Air3G" to the download page.

How Emergency Upgrade Works?

Air3G's flash memory is divided into "firmware" and "bootloader" area. The bootloader area is protected from writing and has a built-in emergency web server. Therefore, the AP can be recovered from emergency web server after a firmware crash. The emergency web server is enabled when AP is forced into emergency upgrade mode, it's IP will be changed to ***192.168.1.254***.



Procedure to Restore the AP using Emergency Upgrade

1. Please connect one of your LAN Ports (LAN1~LAN4) to your PC directly.
2. Set your PC's IP address to 192.168.1.50
3. Before connecting the power, please press and holding the "Reset" button (in the back of the AP). Then plug in the power. Keep press and hold the Reset button until the LED of the selected port goes on(about 3 seconds)

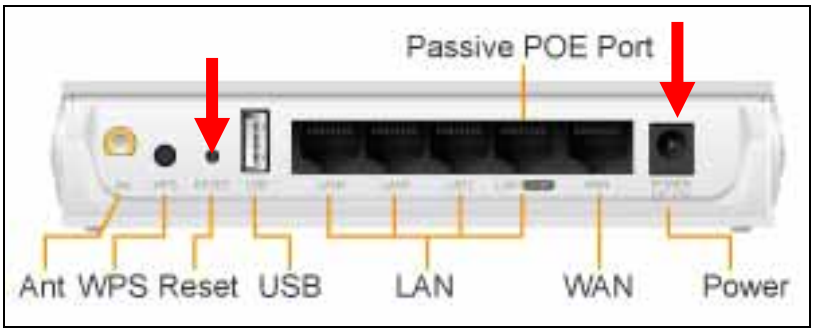
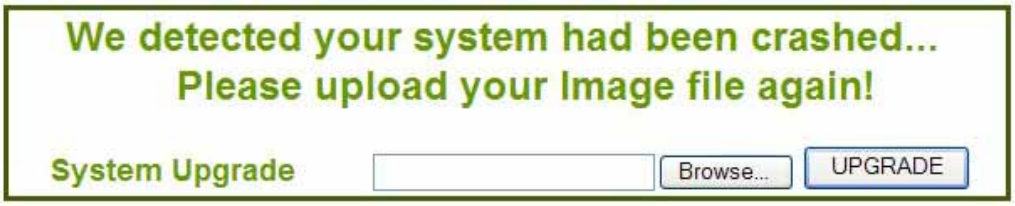


Fig 1-2 : Press and hold the reset button while plugging in the power.

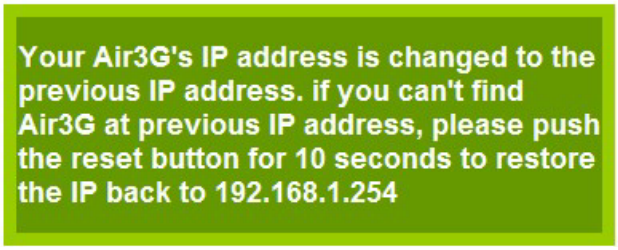
6. Open a browser; type “192.168.1.254” for the website address. The following screen should show up



7. Click the “Browse” button, select and open the correct firmware file.

8. Click on “UPGRADE” button. Do not touch the AP or PC until the upgrade is completed.

9. After upgrading, the configuration will recover from the previous settings. Please access your device at ***previous IP address***. If you forget what the previous IP address is or if you can’t access the device, please push the reset button for 10 seconds to restore your AP to factory default settings. The system will reboot. Then, you should be able to login into the normal Web UI at the default IP: 192.168.1.254.



10 Frequent Asked Questions

In this chapter, we will address some frequent asked questions about Air3G

Question: I plug my 3G USB dongle into Air3G, but it can not be recognized

Answer: Please go to Air3G webpage at www.airlive.com and check the USB compatibility list. If your USB is on the compatibility list, please make sure you plug in the USB dongle while the Air3G is powered off.

==========

Question: After Emergency Upgrade, I can't find my Air3G at 192.168.1.254

Answer: The Air3G will restore to the previous settings after successful Emergency upgrade. Therefore, the IP address will change to the previous IP address. If you still can't find Air3G in previous address, please do a restore to default and the Air3G should appear at 192.168.1.254

==========

Question: When I wan to use "Site Survey" tool to connect with a AP that has no encryption, why does the Air3G report "encryption type mismatch!" and ask me to configure the wireless security settings?

Answer: When you press "Connect" from site survey, the Air3G will first check if the current wireless encryption setting is correct. If not, it will ask you to modify the setting. Therefore, if your current wireless settings has encryption and the new AP you want to associate does not use encryption, then the Air3G will report the mismatch. In this case, simple select "Disable" in the encryption field and press "Apply Change".

==========

Question: When I change my wireless operation mode, why can't I find my AP anymore?

Answer: By Default, the DHCP server is turned on in 3G Router mode. In other modes, the DHCP server is turned off. If you get your IP address automatically, then when you change from 3G Router to AP/Client/WDS Bridge mode. Your PC will not be able to get IP address from DHCP server anymore; therefore, you should set the IP address manually.

==========

Question: Where is the POE port for Air3G?

Answer: The PoE system used for Air3G is 12V Passive PoE. LAN1 is also used as the passive PoE port.

==========

Question: When I use PoE power with 3G USB dongle, why do I get unstable performance sometimes?

Answer: Please use a 12VDC power adapter that supply more than 1.25A of current.

==========

Question: When I connect my PoE switch with Air3G, why doesn't it work?

Answer: The Air3G use a 12V Passive PoE system, it is not the same as the 48V system used by PoE switch. As matter of fact, connect the 48V system to the Air3G might damage the device!

==========

Question: I thought the Air3G has 30dBm output power, why do I only see 20dBm on the Tx Output Power option?

Answer: The maximum output power for Air3G is about 1watt(30dBm). However, it is limited to 20dBm in EU and 23dBm in the U.S. for compliance with regulations. Nevertheless, unlike normal 11n routers that typically provide less than 15dBm output power in 11n mode, the Air3G can provides up to 19dBm(EU) and 22dBm(FCC) in 11n mode. It means greater coverage in 11n mode.

If you are living in countries that allow use of 30dBm output power, you can change the Regulatory Domain to South America. Please be sure it is legal in your country, do not use the wrong regulatory domain.

11 Specifications

The specification of Air3G is subject to change without notice. Please use the information with caution.

11.1 Hardware Features

11.1.1 General Hardware Feature

- Long Range Wireless-N 3G Router
- Up to 30dBm Output Power (20dBm in EU, 23dBm in U.S.)
- Up to 9 times more wireless coverage than normal powered AP/Routers
- Work with 3G/3.5G/UMTS/EVDO/HSDPA USB Dongle
- 1 x USB 2.0 Port
- Green AP power saving function
- 150Mbps 1T1R Wireless-b/g/n standard
- 12V Passive POE Port
- WAN port for ADSL/Cable Modem support
- WAN/3G Connection Auto-Backup
- 3G Router, AP, Client, Bridge, Repeater modes
- Multiple SSID and Bandwidth Control
- 8MB Flash, 32MB SDRAM

11.1.2 Power Supply

- Power Adapter Voltage : input 100~240Vac/50~60Hz , output 12V/1A
- Passive PoE Port(Accept 12Vdc). Passive PoE DC Injector not included

11.1.3 Dimension and Weight

- Dimension: 154 x 130 x 316 mm
- AP Unit Weight(Approximate): 280g
- Package Weight(Approximate): 686g

11.2 Radio Specifications

11.2.1 Frequency Band

- USA (FCC) 11 Channels: 2.412GHz~2.462GHz
- Europe (ETSI) 13 Channels : 2.412GHz~2.472GHz
- South America: 11 Channels: 2.412GHz~2.462GHz
- South America: 14 Channels: 2.412GHz~2.477GHz

11.2.2 Rate and Modulation

- Data Rate:
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps
- Modulation
  - 802.11n
    - 20 MHz BW(LGI): 65, 58.5, 52, 39, 26, 19.5, 13, 6.5
    - 40 MHz BW(LGI): 135, 121.5, 108, 81, 54, 40.5, 27, 13.5
    - 20 MHz BW(SGI): 72.2, 65, 57.8, 43.3, 28.9, 21.7, 14.4, 7.2
    - 40 MHz BW(SGI): 150, 135, 120, 90, 60, 45, 30, 15
  - 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
  - 802.11b: 11, 5.5, 2 and 1 Mbps

11.2.3 TX Output Power

ETSI(Europe)

- 802.11b : About 20dBm max
- 802.11g : About 20dBm max
- 802.11n : About 19dBm max

FCC(The United States)

- 802.11b : About 23dBm max
- 802.11g : About 23dBm max
- 802.11n : About 22dBm max

South America

- 802.11b : About 30dBm max
- 802.11g : About 29dBm max
- 802.11n : About 27dBm max

11.2.4 Receiver Sensitivity

- 802.11b 11Mbps ≦ -90dBm
- 802.11g 54Mbps ≦ -73dBm
- 802.11n HT20 MCS7 ≦ -70dBm
- 802.11n HT40 MCS7 ≦ -67dBm

11.2.5 Supported WLAN Mode

- 3G Router Mode
- AP Mode
- Client Mode
- WDS Bridge Mode
- WDS Repeater Mode

11.3 Software Features

Management Interface

- Web HTTP

Advance Functions

- Setup Wizard
- Site Survey
- 3G service provider list
- Hotspot Authentication
- WAN/3G Connection Backup
- Bandwidth Control / Traffic Shaping
- Associated Client Table
- Wi-Fi, WPA compatible interoperability
- WPA with PSK/TKIP/AES support ,WPA2 support
- Virtual Server Function

- Privacy Separator support
- Hide SSID Support
- Support adjustable output power
- ACK Timeout Adjustment
- Bootloader Protection and Emergency Firmware Upload Code
- Radius Supported
- Up to 40 Static DHCP entries
- Firmware upgrade and configuration backup via Web

12 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.3ad
802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af
This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b
International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP
Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.11d
Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e
The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g
A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11i
The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1x
802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc
A Peer-to-Peer wireless network. An Adhoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)
The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout
Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost

due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value need to consider 3 factors: distance, AP response time, and interference. The Air3G provide ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the Air3G will automatically calculate the correct ACK timeout value.

Bandwidth Management (Traffic Control)

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader

Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge

A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client

Client means a network device or utility that receives service from host or server. A client

device means end user device such as wireless cards or wireless CPE.

CPE Devices
CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receive wireless broadband access from the WISP. The opposite of CPE is CO.

CTS
Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS
Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP
Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ
Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS
A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name
The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack
Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption
Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)
The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall
A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware
The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP
File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold
Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Gateway
In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot
A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping
Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode
A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address
IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a

server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC

Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH

Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO

Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to

increase the receiver sensitivity and to focus available power at intended Rx.

NAT

Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node

A network connection end point, typically a computer.

Packet

A unit of data sent over a network.

Passphrase

Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE

Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power ource. A POE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.

- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS

Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the

slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router

An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

SIGNAL STRENGTH

Receiver Sensitivity Index. SIGNAL STRENGTH is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher SIGNAL STRENGTH values. For SIGNAL STRENGTH value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold

RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's

firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

TCP

A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

TX Output Power
Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end..

UDP
User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade
To replace existing software or firmware with a newer version.

Upload
To send a file to the Internet or network device.

URL
Uniform Resource Locator. The address of a file located on the Internet.

VPN
Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

WAN
Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP
Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi
Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX
Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS
Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN
Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM
Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS
Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA

Wi-Fi Protected Access. It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2

Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.