Air Live®
Powered by OvisLink Corp.

WN-250USB

Wireless 11b/g/n 150Mbps
Mini USB Dongle

User's Manual

www.airlive.com

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.

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

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

FCC Caution

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

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.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

The specification is subject to change without notice.

Table of Contents

1 Introduction

Thank you for purchasing the AirLive WN-250USB Wireless 11b/g/n 150Mbps Mini USB Dongle. This ultra-compact high-speed adapter lets you connect your desktop computer or notebook computer to a wireless network with the link speed of up to 150Mbps. This handy and mini adapter supports the latest Wireless-N technology for greater wireless reception and enhanced the network link speed. You will soon be able to enjoy these additional features by following the instruction in this manual.

- Extremely compact design Wireless-N USB Adapter
- Advanced Wireless-N technology for greater wireless reception
- Hi-speed data transfer rate, up to 150Mbps network link speed
- Backward compatible with IEEE 802.11b/g standards
- Wi-Fi Protected Setup (WPS) simplifies the security settings
- Software AP function – turns wireless client into a wireless access point

1.1. System Requirements

- USB 2.0 port & CD-ROM drive
- Windows XP, Vista or Windowns 7 operating system
- At least 100MB of available disk space

Note: this device may not be able to work with USB 1.1 port

1.2. Package Contents

Before installing the adapter, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- WN-250USB
- Quick Setup Guide
- Software CD

1.3. Hardware Installation

- USB Connector
- Connector Cap (To protect the USB connector when not installed)
- Link/Activity LED (Green)

LED	Mode	Status
Link/ Activity	Flash	Linked to a wireless AP / transferring data
	Off	No link to any wireless AP / non active

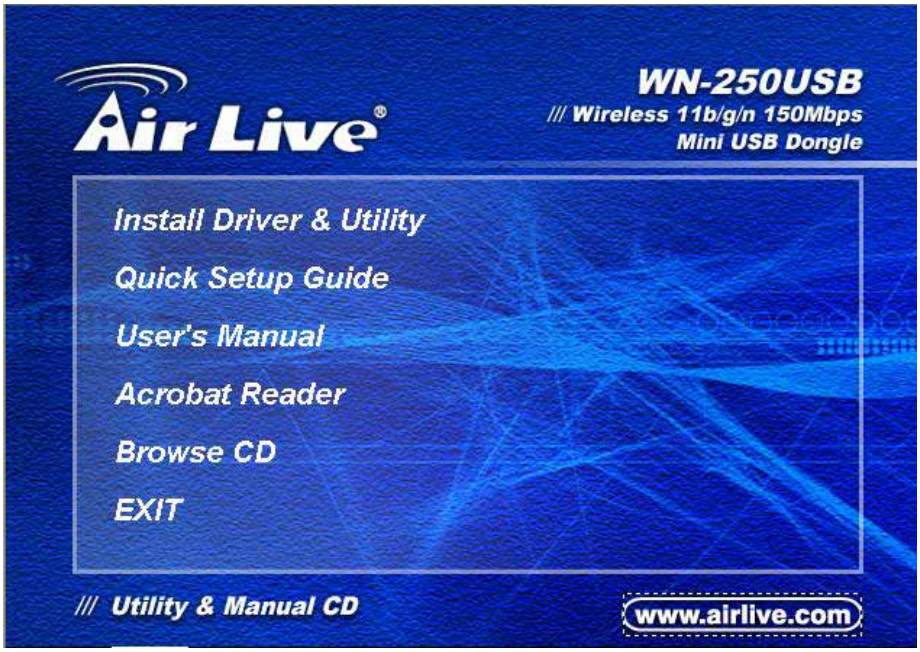
With the computer switched on, insert the WN-250USB adapter into an empty USB 2.0 port.

Caution: Never use force to insert the adapter.

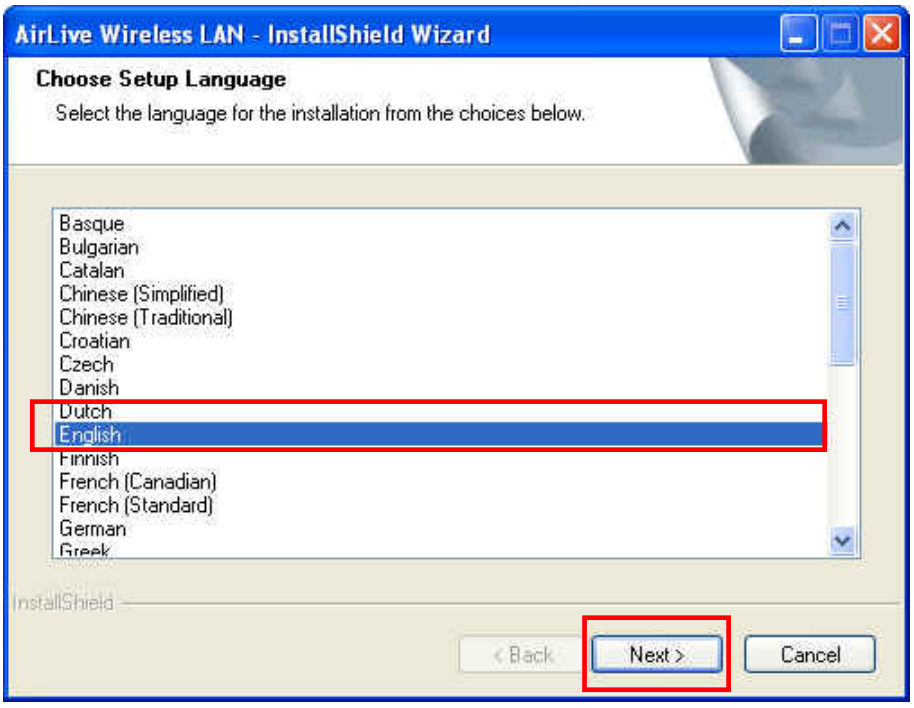
2 Software Installation

1. With the WN-250USB adapter inserted and computer is powered on, the Found New Hardware Wizard displays a screen, click "***Cancel***" to proceed the driver installation.

2. Insert the enclosed software CD in the CDROM drive and click "**Install Driver & Utility**" from the autorun screen. If the autorun screen did not appear, run the "**Setup.exe**" program in the "**Driver**" folder.

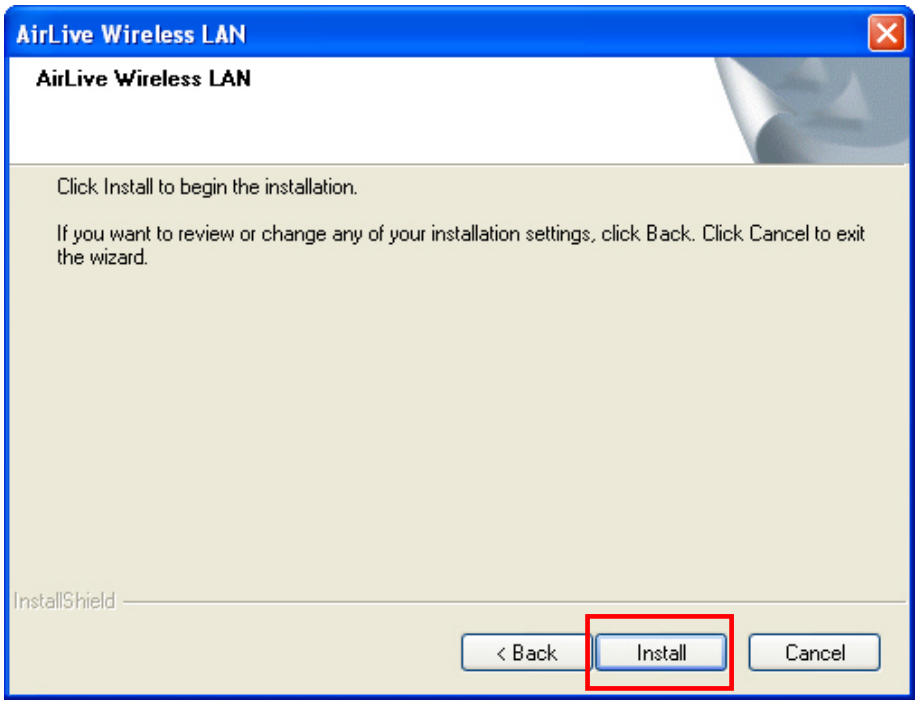


3. When the Choose Setup Language screen displays, highlight your preference and click “Next” to proceed.

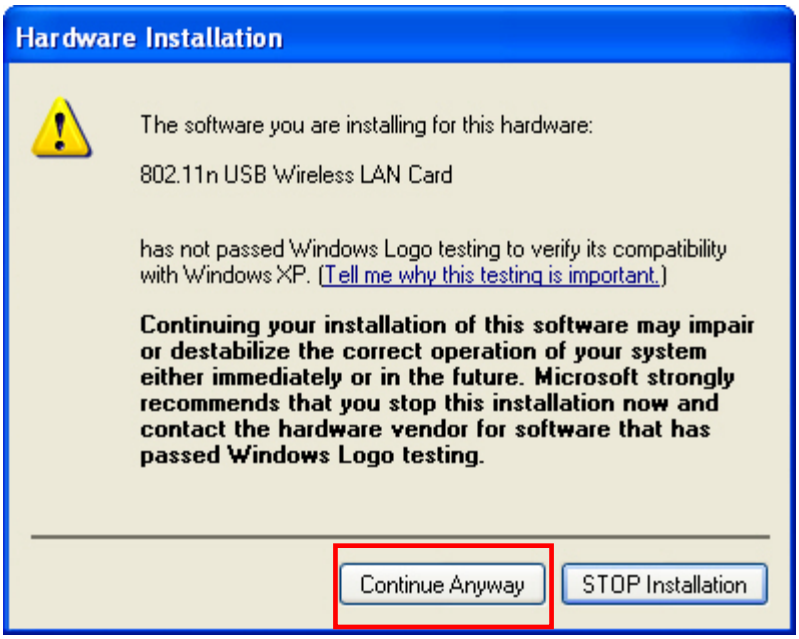


4. When the first of the AirLive Wireless LAN screen displays, click “Next.”

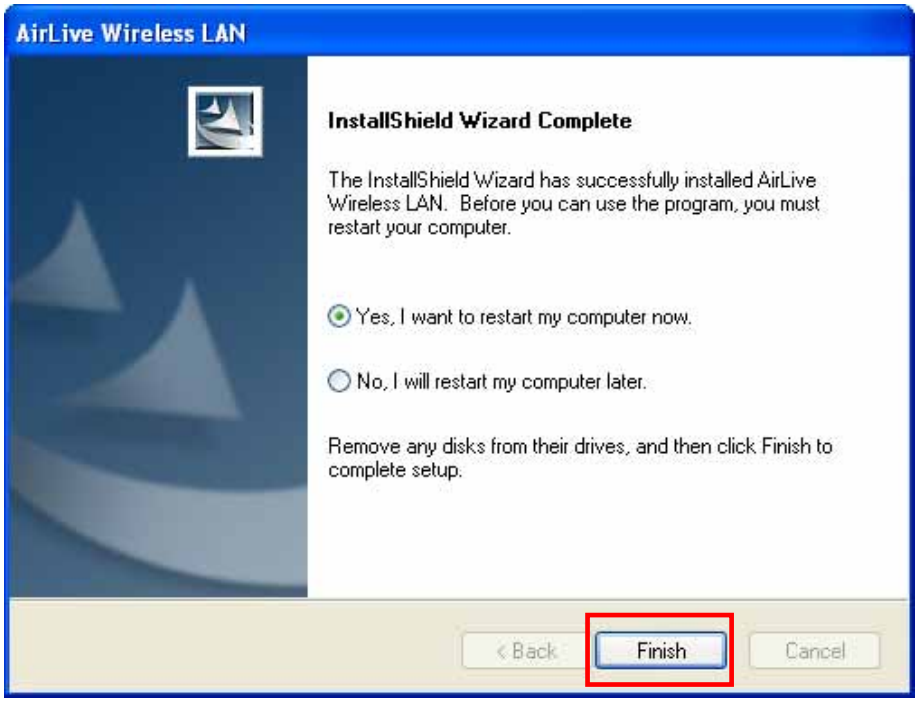
5. When the next screen displays, click “Install” to begin the installation. On any of the screens where they appear, click “Back” to return to a previous screen; click “Cancel” to exit the wizard.



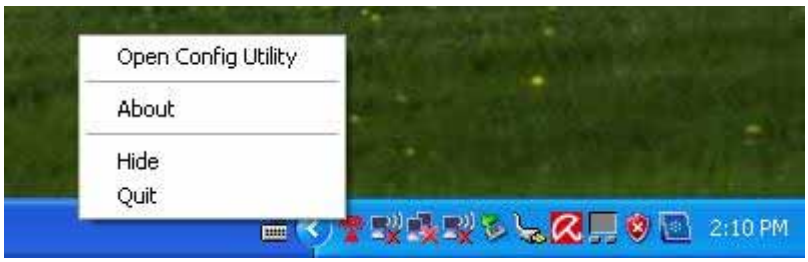
6. Click "**Continue Anyway**" if the below warning screen appears



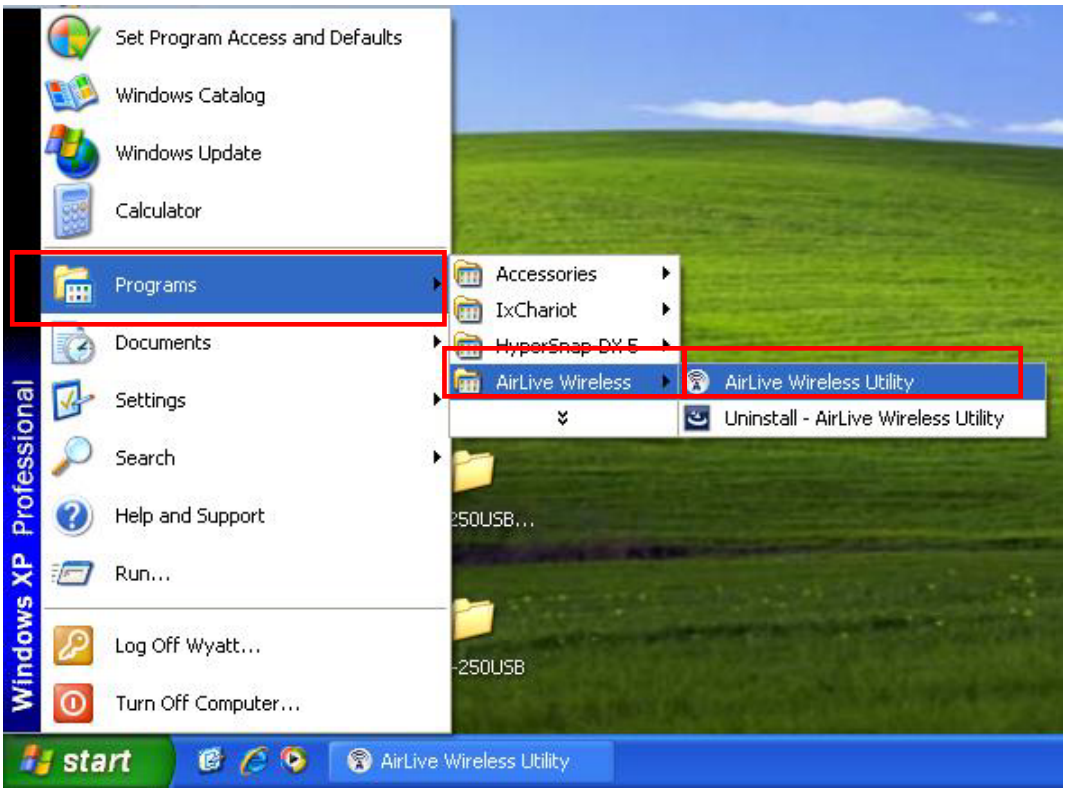
7. Please wait while the install procedure is running. When you see this message, please click "**Finish**" to complete the driver installation process. It is recommended to restart your computer once the driver/utility installation is complete.



8. After the system reboot, a new AirLive icon appears in the desktop menu, presenting the status of the USB adapter. To begin configuring the wireless connection, right-click on the icon and select "**Open Config Utility**" from the pop-up menu or simply double click the icon. To close the configuration utility, right-click on the icon and click "**Quit**"

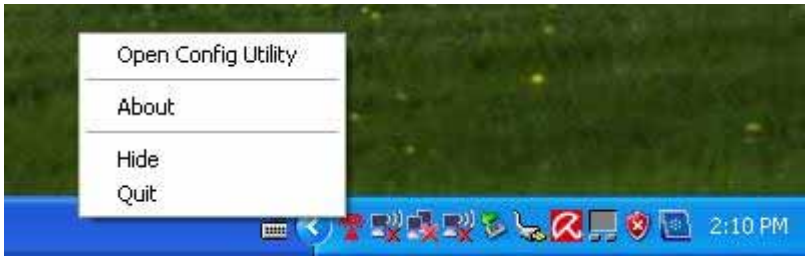


9. Clicking "**Exit**" to stop the configuration utility prevents you from maintaining the wireless link to the access point you wish to use. In this case, you can re-start the configuration utility by clicking Wireless utility icon as shown. (Start -> Programs -> AirLive Wireless -> AirLive Wireless Utility)



2.1. Configuration Utility

The configuration utility is a powerful application that helps you configure you USB adapter and monitor the link status and statistics during the transmission process. The utility appears as an icon in the system tray and on the desktop of Windows. You can open it by double-clicking the desktop icon. Right-click the icon in the system tray and an options menu displays.



Open Config Utility: Select to open the configuration utility.

About: Select to display utility information.

Hide: Select to hide the utility in the system tray.

Quit: Select to quit the utility in the system tray.

The Configuration Utility opens to the General screen, with another five tabs near the top of the screen you can select for specific configuration options. Whichever of the tabs you select, several additional options are always displayed at the top, left and bottom of the screen, as shown on the General screen in the first of the detailed sections that follow.

Refresh: This updates the adapter list in the left-side window

Mode: This allows you to select one of two modes: Station or Access Point.

• With Station, the adapter works as a wireless adapter

• With Access Point, the adapter works as a wireless AP (Chapter 2.8, SoftAP)

About: This lets you check the version of the utility.

Show Tray Icon: Select to show the utility icon in the system tray

Radio Off: Select to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work.

Disable Adapter: This allows you to disable or enable the adapter

Windows Zero Config: Select to configure the adapter using Windows XP Zero Configuration.

The status of wireless connection will be displayed by AirLive configuration utility icon as indicated below.

 Wireless connection is established, excellent signal reception.

 Wireless connection is established, normal signal reception.

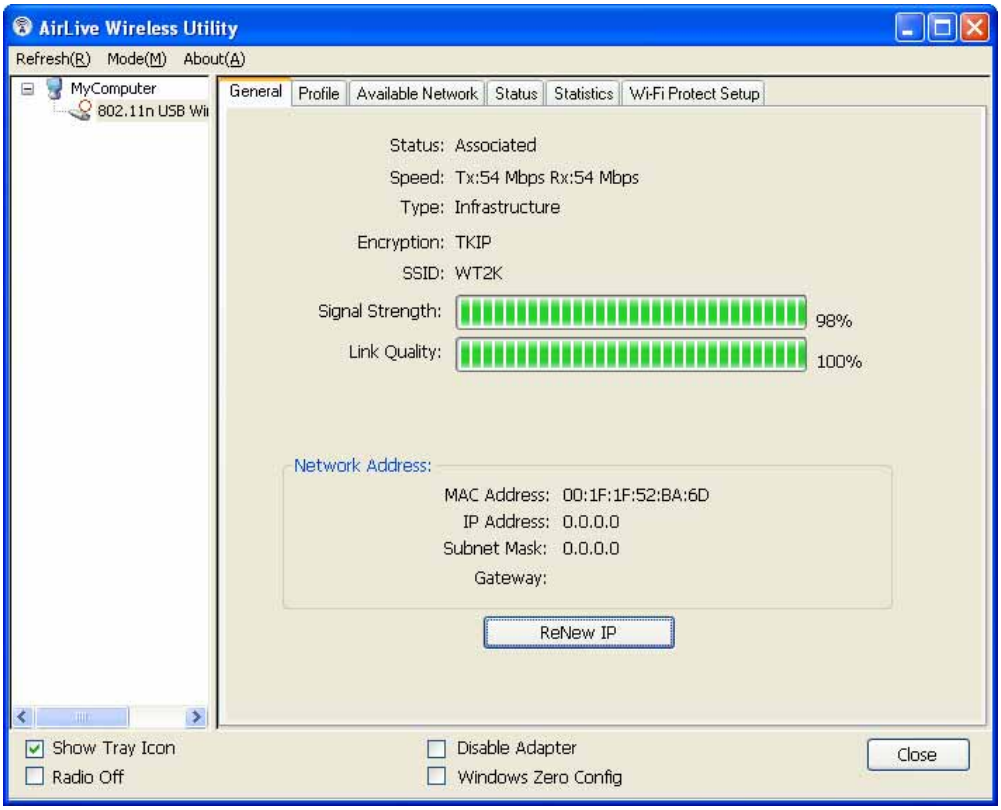
 Wireless connection is established, weak signal reception.

 Connection is not established yet.

 Wireless network card is not detected.

2.2. Utility/General

This screen is primarily for checking connection related items and information about the selected adapter: Status, Speed, Type, Encryption, SSID, Signal Strength, Link Quality and Network Address. The other references on this screen reflect the settings configured on the Profile screen.



Type: This displays either “Infrastructure” or “Ad Hoc” based on the selection made on the Profile screen.

Encryption: This displays the encryption setting of the current connection “None,” “WEP,” “TKIP” or “AES” based on the selection .made on the Profile screen.

SSID: The Service Set ID (up to 32 printable ASCII characters) is the unique name identified in a WLAN that prevents the unintentional merging of two co-located wireless networks. This can be entered on the Profile screen.

Signal Strength: Indicates the wireless signal strength

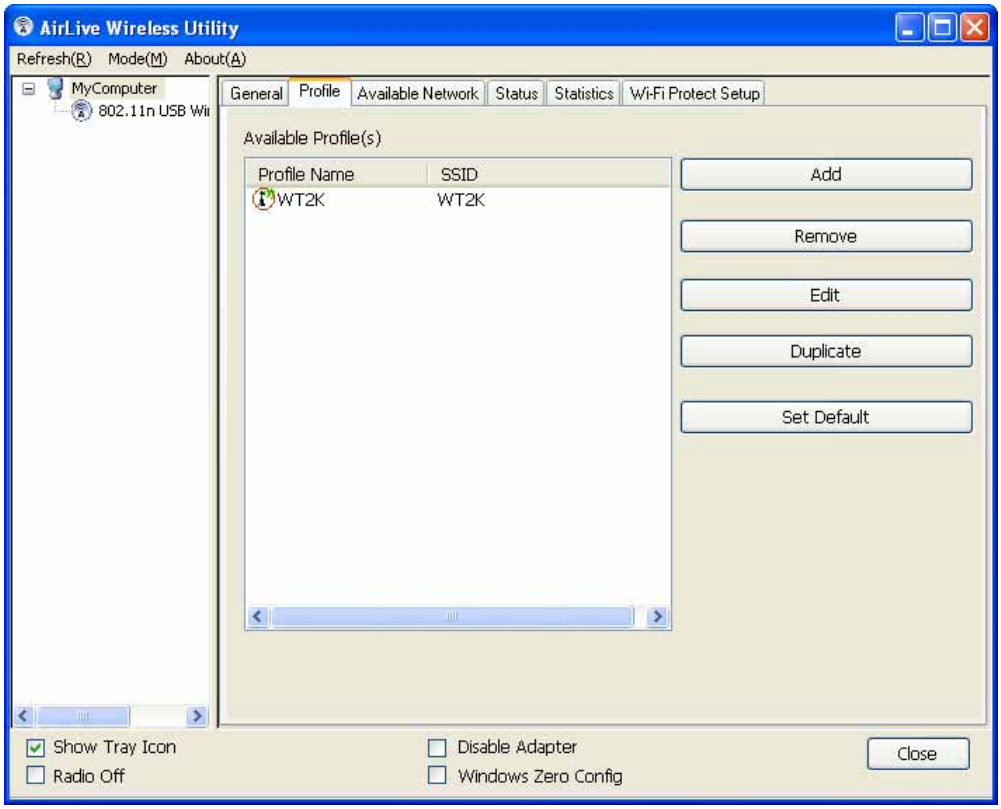
Link Quality: Indicates the wireless link quality

Network Address: Shows the MAC/IP address and Subnet Mask, Gateway information

Renew IP: Click to renew the IP address of the adapter

2.3. Utility/Profile

The Profile screen is for managing networks you connect to frequently. You can add, delete, edit and activate a profile on this screen.



Available Profile(s): This list shows the preferred networks for the wireless connection. You can add, remove, edit and duplicate the preferred networks, and you can also set one of the networks as the default connection.

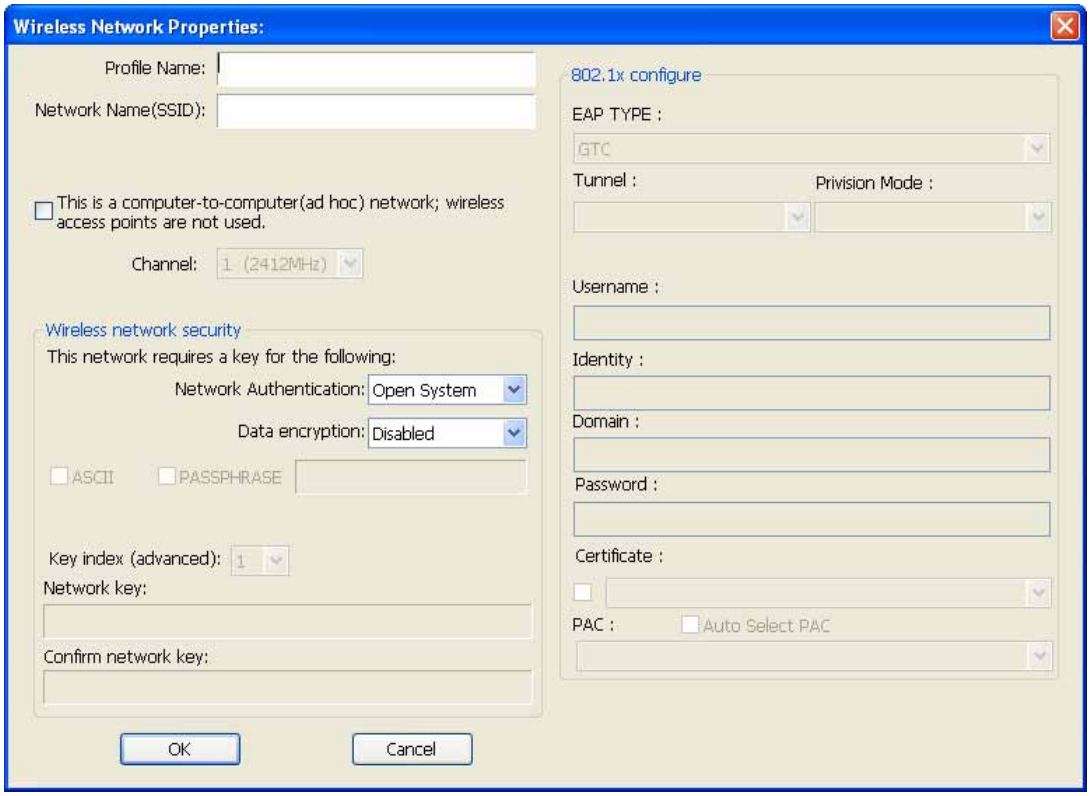
Add/Remove/Edit: Click with a profile selected to make desired changes.

Duplicate: Click to create a new profile with the same settings as the current one.

Set Default: Click to designate a selected profile on the Available Profile(s) list as the default network.

2.3.1 Configuring a Profile

Clicking “Add” or “Edit” on the Profile screen will display a Wireless Network Properties screen that allows you to set various parameters required with the devices you connect to wirelessly.



Profile Name: Enter an easily recognizable name to quickly differentiate among multiple networks.

Network Name (SSID): The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. If you specify an SSID for the adapter, then only the device with the same SSID can connect to the adapter.

This is a computer-to-computer (ad hoc) network; wireless access points are not used: When this option is selected, the adapter will operate in Ad Hoc mode (connecting to another wireless adapter in the WLAN without an access point or router)

Channel: This setting is only available for Ad Hoc mode. Select the radio channel used for the network you're connecting to.

Network Authentication: This setting needs to be consistent with the wireless networks the adapter is intended to be connected to. There are seven options:

• Open System means that no authentication is needed within the wireless network.

• Shared Key means that only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other.

• WPA-PSK is a special mode designed for home and small business users who don't have access to network authentication servers. In this mode, also known as Pre-Shared Key, the user manually enters the password in their access point or router, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users who don't have the matching password from joining the network while encrypting the data traveling between authorized devices.

• WPA2-PSK is also for homes and small businesses. It differs from WPA-PSK in that it provides data encryption via the Advanced Encryption Standard (AES). In contrast, WPA-PSK uses the Temporal Key Integrity Protocol (TKIP).

• WPA 802.1X (or just WPA) provides a scheme of mutual authentication using either IEEE 802.1x / Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

• WPA2 802.1X, like WPA, supports IEEE 802.1x / EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required for corporate and government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES, whereas WPA uses the Temporal Key Integrity Protocol (TKIP).

• WEP 802.1X is a special mode for using IEEE 802.1x / EAP technology for authentication and WEP keys for data encryption.

Data Encryption: All devices in the network should use the same encryption method. The drop-down menu offers four options.

• Disabled disables the WEP data encryption.

• WEP enables the WEP data encryption. When this is selected, you need to continue with the setting of the WEP encryption keys.

• TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets. (A packet is a kind of message transmitted over a network.) This ensures much greater security than standard WEP security.

• AES has been developed to ensure the highest degree of security and authenticity for digital information. It's the most advanced solution defined by IEEE802.11i for security in the wireless network.

EAP Type:

• GTC is an authentication protocol that allows the exchange of clear text authentication credentials across the network.

• TLS is the most secure of the EAP protocols, but isn't easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client and, after validating the server's certificate, the client presents a client certificate to the server for validation.

• LEAP is a pre-EAP, Cisco-proprietary protocol with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited brand choice for client, access-point and server products is not a concern. Once you've set up LEAP authentication, you need to enter the username and password of your computer.

• PEAP & TTLS are similar to, yet easier than, TLS in that they specify a stand- alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adapter supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. That a client certificate be required for authentication is optional.

Tunnel: Options are MD5, GTC, TLS and MSCHAP-v2.

Username: This is the certificate username on the RADIUS server.

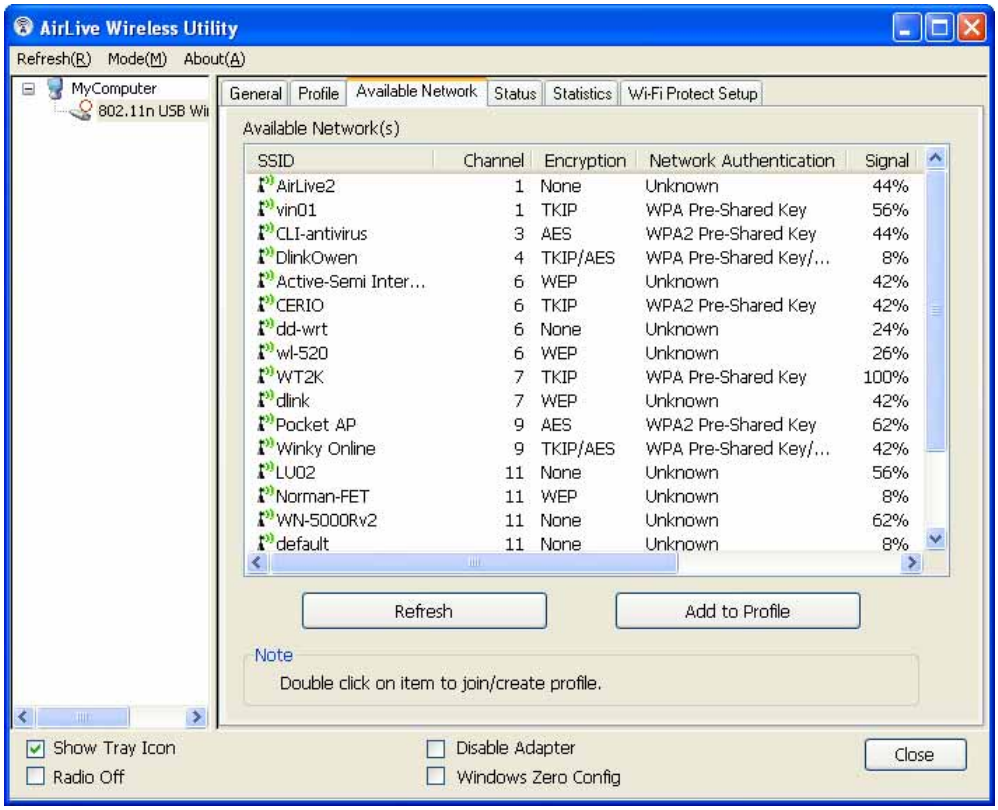
Identity: This is the user's identity on the RADIUS server.

Password: This is the user's password on the RADIUS server.

Certificate: Select the certificate for RADIUS server authentication.

2.4. Utility/Available Network

When you open the configuration utility and select "Available Network" menu tab, the system scans all the channels to find access points/stations within the accessible range. On the Available Network screen, all the networks nearby are listed. You can change the connection to another network or add one of the networks to your own profile list.



Available Network: This list shows all available wireless networks within the range of the adapter. It also displays network information: SSID, BSSID, Signal Strength, Channel, Encryption, Authentication and Network Type. To connect to a network on the list, double-click the item and the adapter will connect automatically to it.

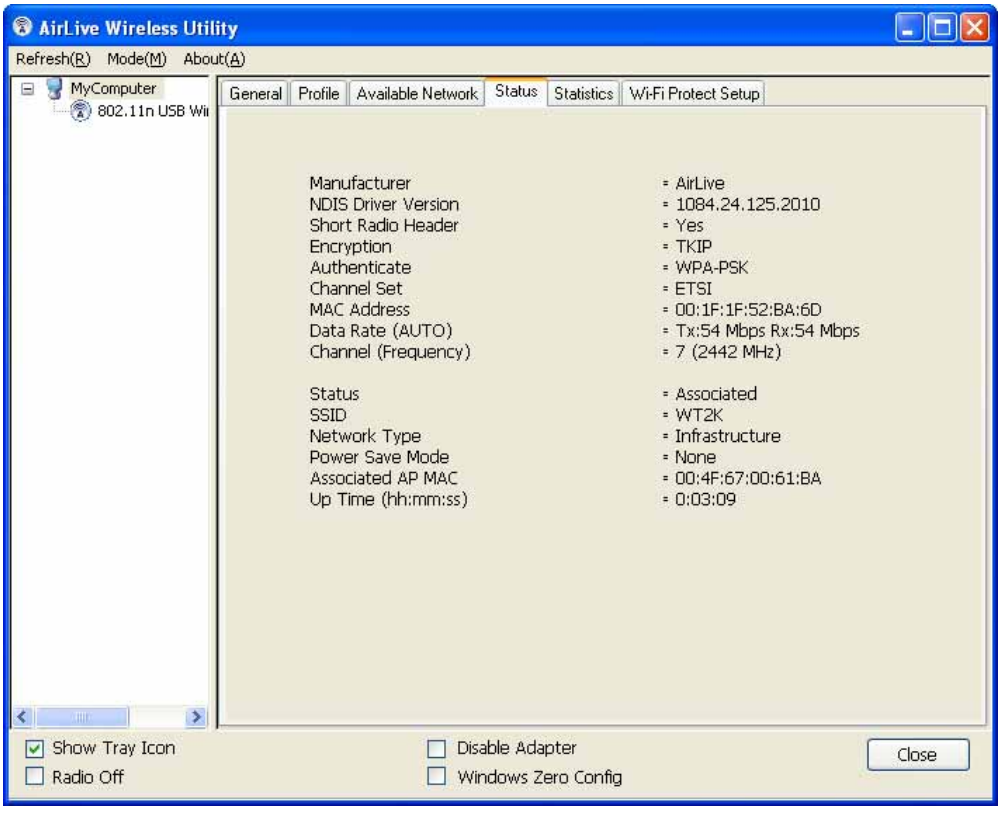
Refresh: Click “Refresh” to collect the new information of all the wireless networks nearby.

Connect: Double click the selected network

Add to Profile: Click to add the selected network to the Profile list.

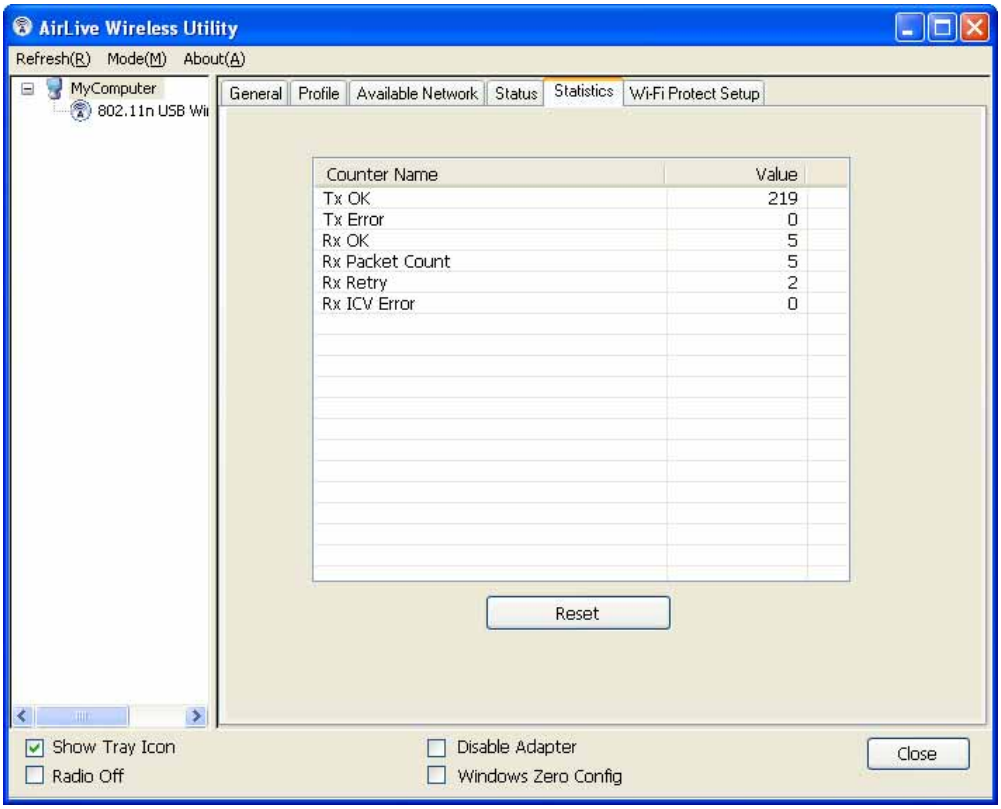
2.5. Utility/Status

This screen shows the information of manufacturer, driver version and settings of the wireless network the adapter is connecting to. It also shows the current connection time.



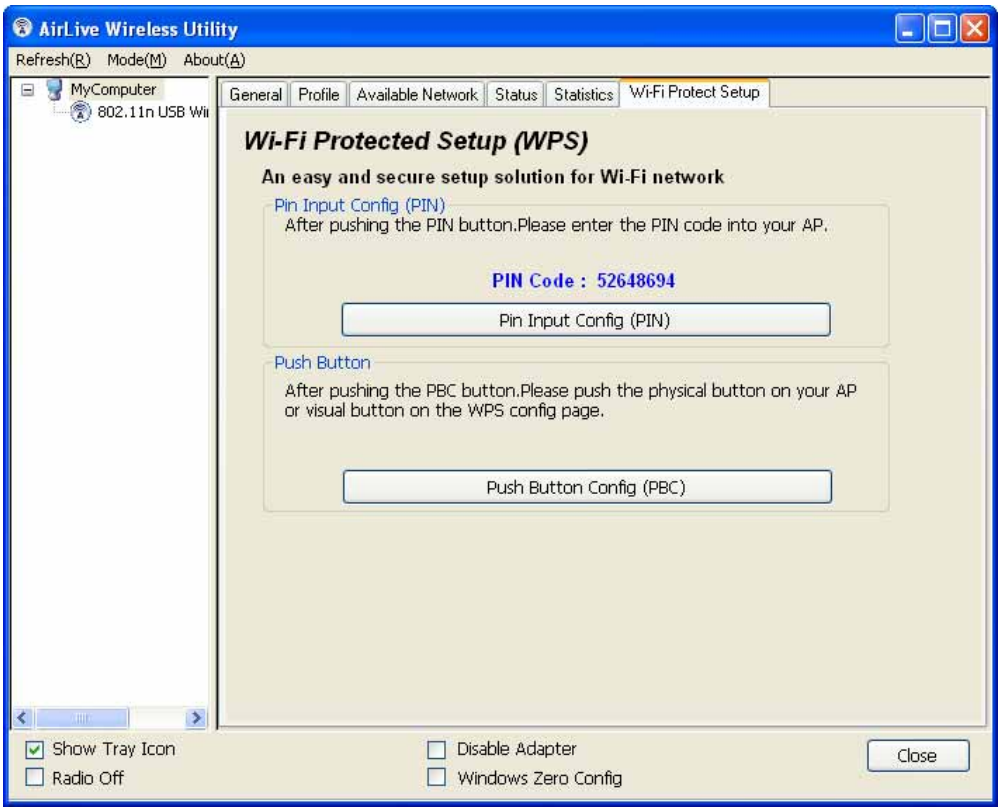
2.6. Utility/Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click “Reset“.



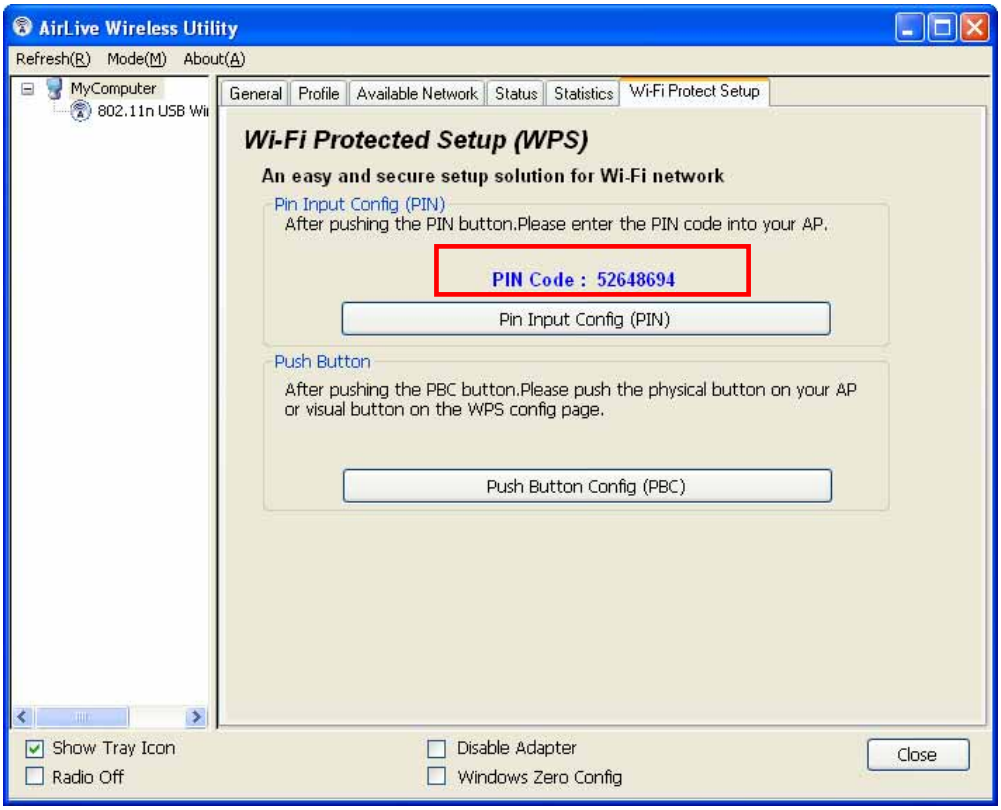
2.7. Utility/Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the latest wireless network technology and makes wireless network setup very simple. If you have a WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption all by yourself. All you need to do is go to the this setup page and click either "PBC" or "PIN" and then press a WPS button or enter a set of 8-digit code on the wireless access point you wish to establish a secure connection.



2.7.1 PIN Input Config (PIN)

1. Enter the PIN code of your wireless adapter (displayed right above the “PIN” button — see image below) on the wireless access point you want to connect to. If necessary, refer to the user manual of the wireless AP for instructions.



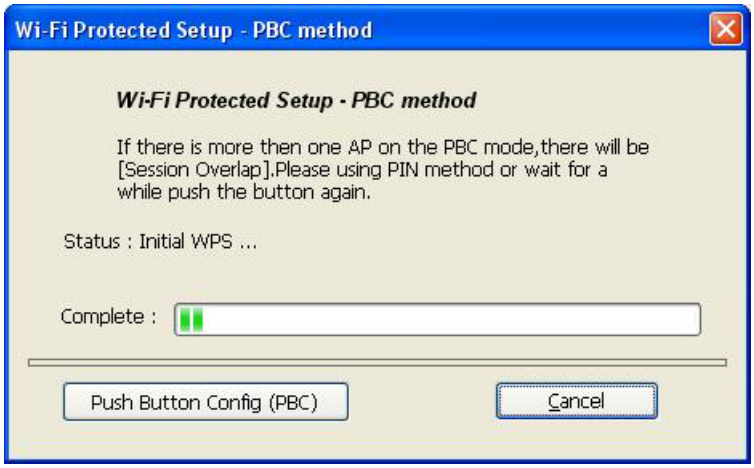
2. Click “Pin Input Config (PIN)” button now, and the following message will appear on your computer, click “Yes” to select a specific wireless access point or click “No” to start PIN method of WPS .

3. If you click “Yes” and the following message will appear on your computer, please select the SSID of wireless access point that you wish to connect and click “Select”.

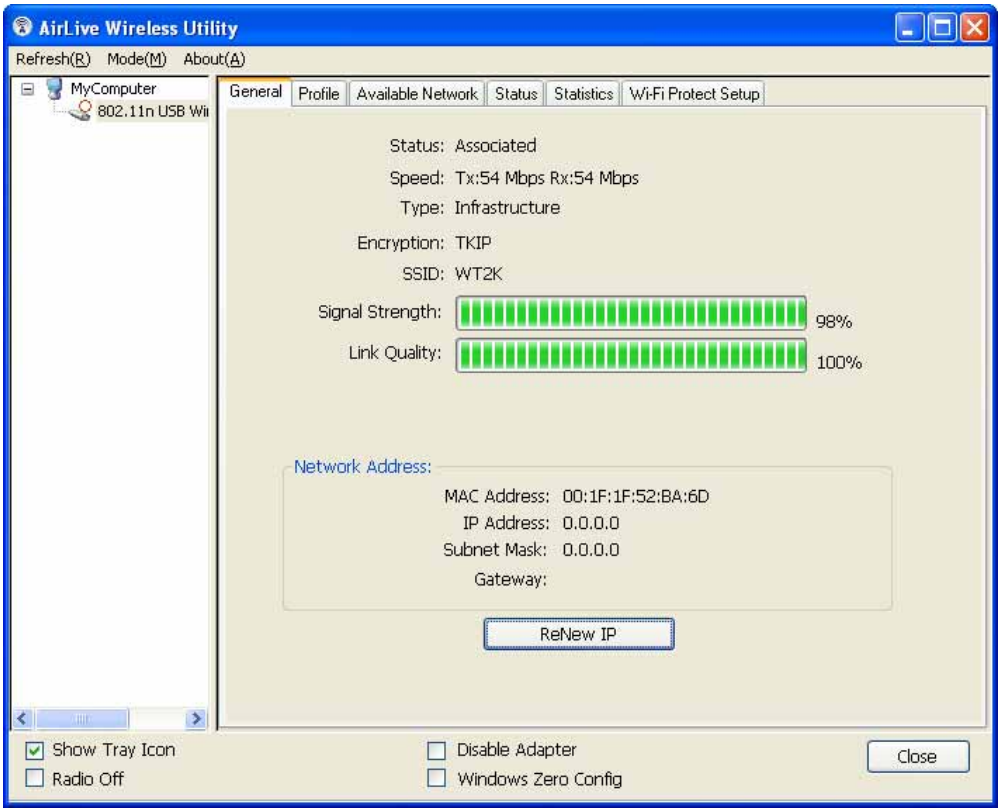
A Status screen will display to indicate the progress of the procedure, which can take up to two minutes or so. If a wireless access point with the correct PIN code found, you’ll be connected to it.

2.7.2 Push Button Config (PBC)

1. Begin the PBC pairing procedure by setting up the access point. Refer to the user manual of the wireless AP for instructions. Click “Push Button Config (PBC)” on the Wi-Fi Protected Setup screen to begin the wireless connection using WPS. This procedure can take up to a minute to complete.

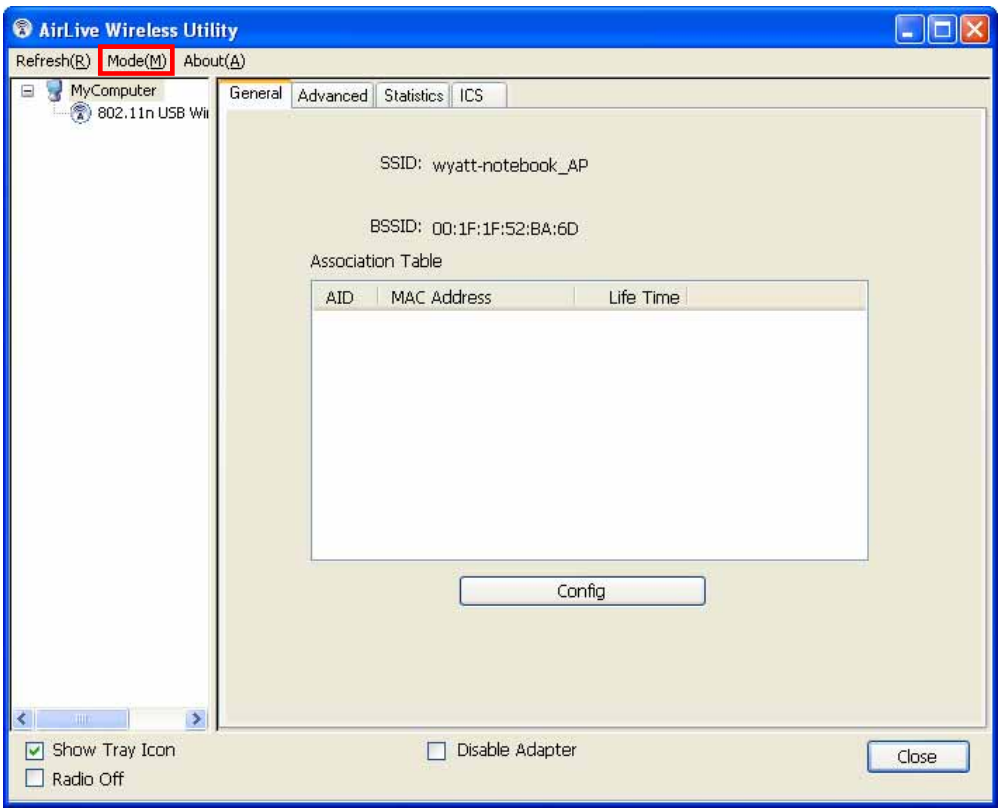


2. Once a successful WPS connection has been made between the wireless adapter and the access point, details about the connected access point will be displayed (as shown below).


AirLive Wireless Utility
Refresh(R) Mode(M) About(A)
MyComputer
802.11n USB Wi
General
Profile
Available Network
Status
Statistics
Wi-Fi Protect Setup
Status: Associated
Speed: Tx:54 Mbps Rx:54 Mbps
Type: Infrastructure
Encryption: TKIP
SSID: WT2K
Signal Strength:
98%
Link Quality:
100%
Network Address:
MAC Address: 00:1F:1F:52:BA:6D
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway:
ReNew IP
Show Tray Icon
Radio Off
Disable Adapter
Windows Zero Config
Close

2.8 Software AP

This wireless adapter can also be used as a wireless access point. On any of the menu screens, go to Mode(M) and select “Access Point.”



2.8.1 General

SSID: The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN that prevents unintentional merging of two co-located WLANs. The default SSID of the AP is <Full Computer Name> + "_AP." Wireless adapters connected to the AP should set up the same SSID as the AP.

BSSID: This is the MAC address of the adapter.

Association Table: All wireless adapters connected to the software AP will be listed in the window.

Config: Click to access configuration options for the AP (shown at below). Refer to 2.3 Utility/Profile for details, and note that Ad Hoc mode is not enabled for the AP.

2.8.2 AP Advanced

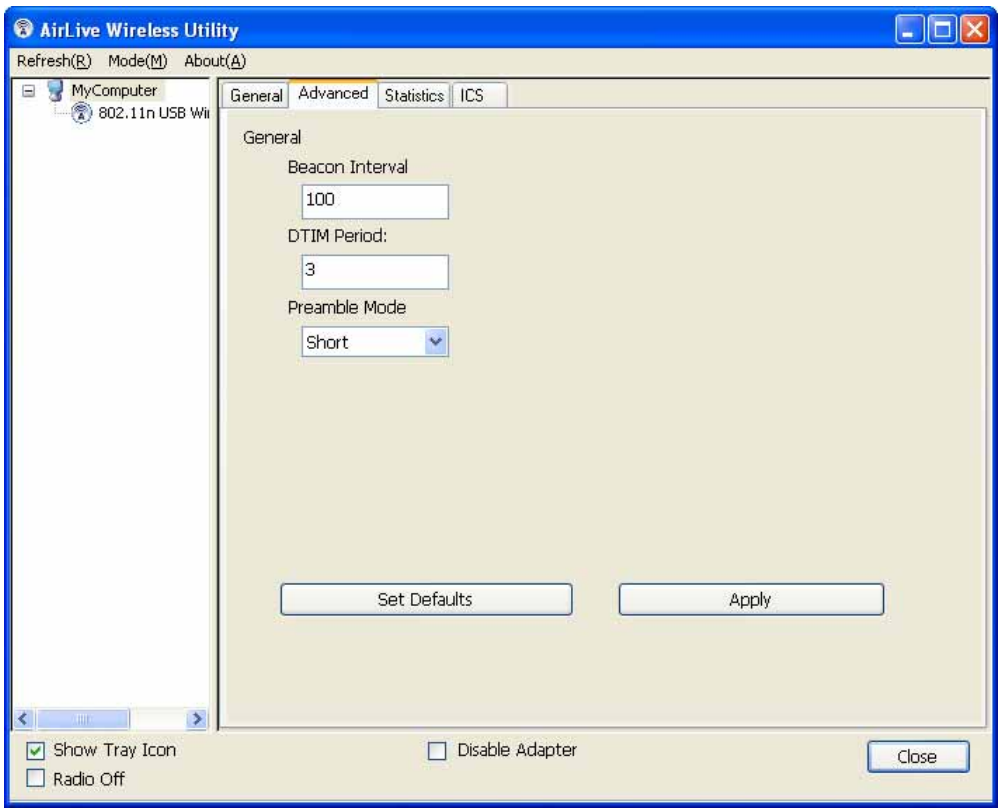
Beacon Interval: Specify the duration between beacon packets (milliseconds). The range for the beacon period is 20-1000 milliseconds, with a typical value of 100.

DTIM Period: This is the sending interval of the AP's traffic broadcast. The default value is 3 beacons.

Preamble: This is the length ("Short" or "Long") of the CRC block for communication among wireless stations. High network traffic areas should use "Short."

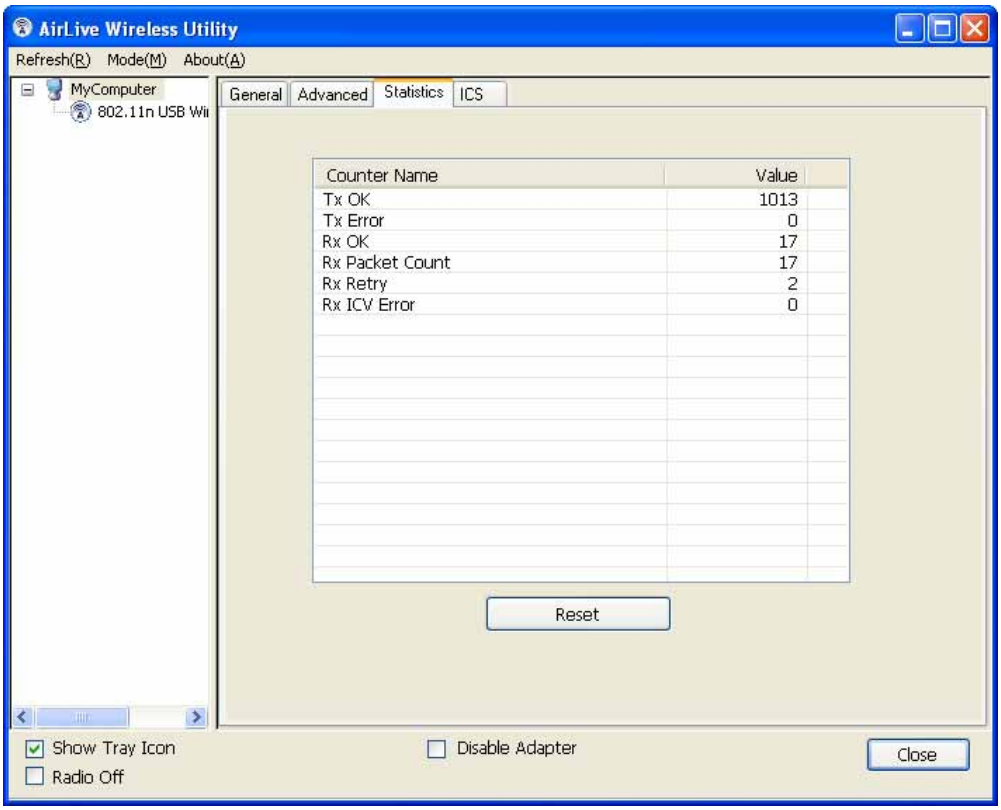
Set Defaults: Click to return to default settings.

Apply: Click to confirm the settings.



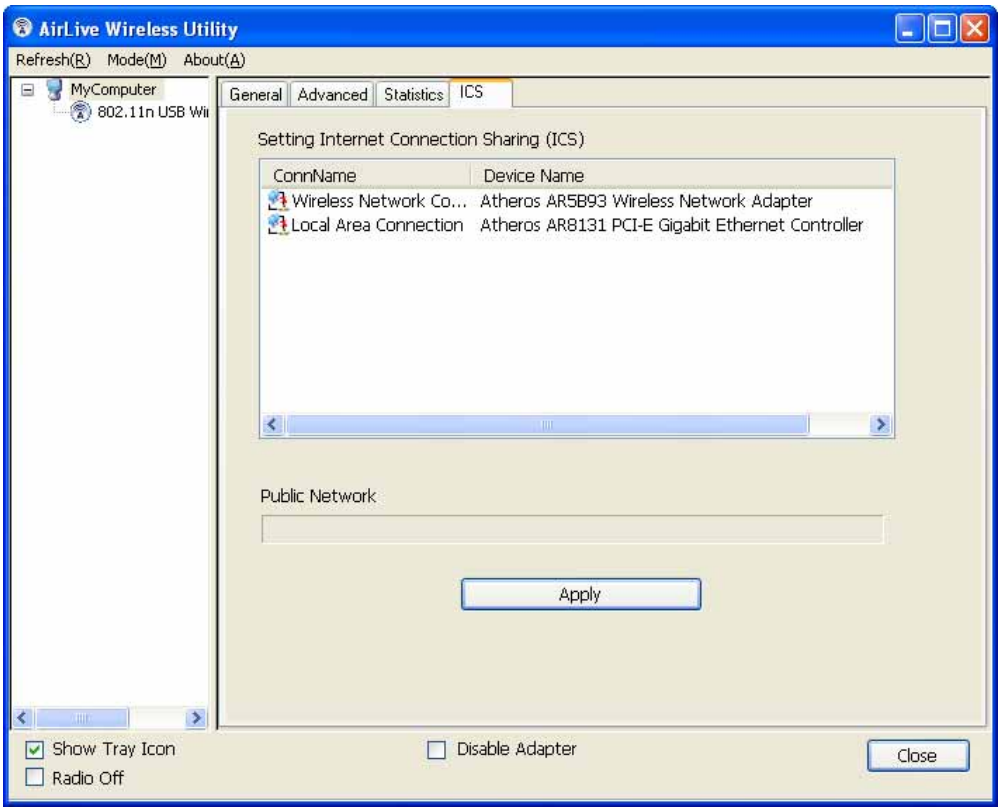
2.8.3 AP Statistics

You can get the real-time information about packet transmissions and the receiving status during wireless communications from this screen. To update the statistics values, click “Reset.”



2.8.4 ICS

To connect to the Internet through this adapter using SoftAP, you need to make abridge between SoftAP and the Internet connection. Select the Internet connectionand click “Apply.”



3 Specifications

Standards

• IEEE 802.11b (1/2/5.5/11Mbps Wireless LAN)
• IEEE 802.11g (6/9/12/24/36/48/54Mbps Wireless LAN)
• IEEE 802.11n (20MHz up to 72Mbps Wireless LAN)
11n (40MHz up to 150Mbps Wireless LAN)

General

• Interface: Hi-Speed USB 2.0
• Chipset: Realtek
• Frequency band: 2.4000 – 2.4835 GHz (Industrial Scientific Medical Band)
• Modulation technologies:
- 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
- 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM

• Security:
- 64/128-bit WEP data encryption
- WPA and WPA2
- 802.1x
• Transmit power:
- 11n: 14 dBm +/- 1.5 dBm
- 11g: 14 dBm +/- 1.5 dBm
- 11b: 17 dBm +/- 1.5 dBm
• Certification: FCC Class B, CE

LEDs

• Link/Activity

Environmental

• Dimensions: 7 (H) x 15 (W) x 27 (L) mm
• Weight: 0.14 kg
• Operating temperature: 0 ~ 40°C (32 ~ 104°F)
• Operating humidity: 10 ~ 90% RH, non-condensing
• Storage temperature: -20 ~ 60°C (-4 ~ 14°F)

4 Frequent Asked Questions

If you encounter any problem when you're using this wireless USB dongle, please check this FAQ table for possible solution.

Question:
I can't find any wireless access point / wireless device in "Site Survey" function.

Answer:
1. Click "Rescan" and see if you can find any wireless access point or wireless device.
2. Try to move closer to any known wireless access point.

Please adjust the position of network card (you may have to move your computer if you're using a notebook computer) and click "Rescan" button for few more times. If you can find the wireless access point or wireless device you want to connect by doing this, try to move closer to the place where the wireless access point or wireless device is located.

Question:
Nothing happens when I click "Open Config Utility"

Answer:
1. Please make sure the wireless USB dongle is inserted into your computer's USB port. If the AirLive configuration utility's icon is not activated, the dongle is not detected by your computer.
2. Reboot the computer and try again.
3. Remove the dongle and insert it into another USB port.
4. Remove the driver/utility and then re-install it.

Question:

I can not establish connection with a certain wireless access point

Answer:

1. Click “Connect” for few more times.
2. If the SSID of access point you wish to connect is hidden (nothing displayed in **SSID** field in **Site Survey** function), you have to input the correct SSID of the access point you wish to connect. Please contact the administrator of the access point for SSID.
3. You have to input the correct security key to connect an access point with encryption.
   Please contact the administrator of the access point for security password.
4. The access point you wish to connect only allows network cards with specific MAC address to establish connection.

5 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.

802.11a
An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.850 GHz) with a maximum of 54Mbps data transfer rate. The 5GHz frequency band is not as crowded as the 2.4GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

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

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 2.4GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11h

This IEEE standard define the TPC (transmission power control) and DFS (dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

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.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment and it was published in October 2009. Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal. 802.11n provides a throughput up to 300Mbps using OFDM technology.

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.

802.1d 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.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID (called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

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.

Ad-hoc

A Peer-to-Peer wireless network. An Ad-hoc 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 needs to consider 3 factors: distance, AP response time, and interference.

Bandwidth Management

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 receives 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.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

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 Ad-hoc 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-Input-Multi-Output)
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.

RSSI

Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI 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.

Super A

Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose “Super-A without Turbo) if you need more speed than 11a mode

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.

Turbo A

Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used of channel binding might be prohibited in EU countries.

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 which 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.

Walled Garden
On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

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.

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.

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.