



**ALL0233**  
**Wireless-N USB Dongle**

---

---

**User Guide**

---

---

# Table of Contents

---

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
Package Contents .....	1
Features .....	1
LEDs .....	1
Operation .....	2
<b>CHAPTER 2 INITIAL INSTALLATION .....</b>	<b>3</b>
Requirements .....	3
Procedure .....	3
<b>CHAPTER 3 USING THE WINDOWS UTILITY .....</b>	<b>7</b>
Overview .....	7
System Tray Icon .....	7
Network Screen .....	8
Link Status Screen .....	11
Profile Screen .....	12
Advanced Screen .....	17
Statistics Screen .....	19
WMM Screen .....	21
WPS Screen .....	23
Radio on/off Screen .....	25
About Screen .....	26
<b>APPENDIX A SPECIFICATIONS .....</b>	<b>27</b>
Wireless-N USB Dongle .....	27
<b>APPENDIX B ABOUT WIRELESS LANS .....</b>	<b>28</b>
Modes .....	28
BSS/ESS .....	28
Channels .....	29
WEP & WPA-PSK .....	29
WPA2-PSK .....	29
Wireless LAN Configuration .....	30

P/N: 956YMJ0030

Copyright © 2008. All Rights Reserved.

Document Version: 1.0 (2008)

All trademarks and trade names are the properties of their respective owners.

# Chapter 1

## Introduction



*This Chapter provides an overview of the Wireless-N USB Dongle's features and capabilities.*

Congratulations on the purchase of your new Wireless-N USB Dongle. The Wireless-N USB Dongle provides a wireless network interface for your Notebook or PC.

### Package Contents

The following items should be included:

- The Wireless-N USB Dongle Unit
- Quick Start Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

### Features

- Compatible with Draft IEEE 802.11n, 802.11b and 802.11g 2.4GHz
- Data transmission rate is up to 300Mbps
- Supports Turbo Mode which can enhance the data transmission rate within the specific wireless network
- Supports WMM (Wi-Fi Multimedia) function (IEEE 802.11e QoS standard) and can meet the requirement of the multi-media data bandwidth
- Supports 64/128-bit WEP, WPA (TKIP with IEEE802.1x) and WPA2 (AES with IEEE 802.1x) functions for high level security
- Supports CCS (Cisco Compatible Extensions) for the radio monitoring and fast roaming
- Automatic fallback which increases the data security and reliability
- Supports USB 2.0 interface

### LED

#### Wireless-N USB Dongle

The Wireless-N USB Dongle has a single Link/Activity LED.

<b>Link/Act LED (Blue)</b>	<ul style="list-style-type: none"><li>• On - Associated with the network.</li><li>• Off - Not associated with the network.</li><li>• Blinking - Data being transferred.</li></ul>
--------------------------------	---

## Operation

**You should install the supplied software on the CD-ROM before inserting the Wireless-N USB Dongle.**

**If you have any form of the wireless utility beforehand, please uninstall it.**

## Chapter 2

# 2

# Initial Installation

*This Chapter covers the software installation of the Wireless-N USB Dongle.*

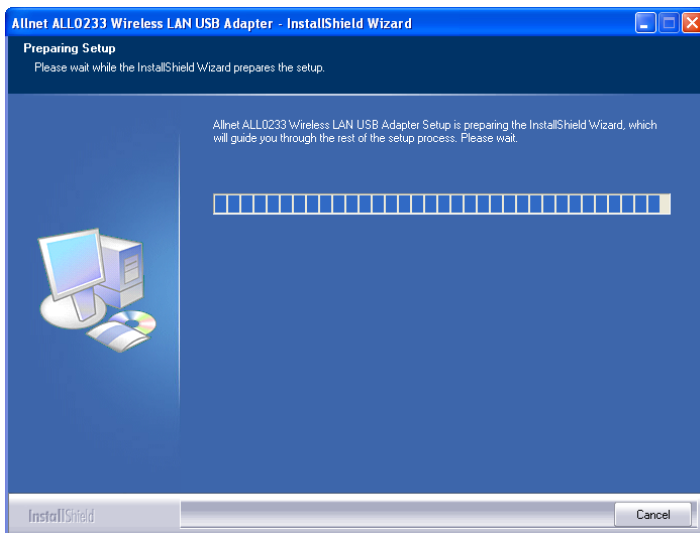
## Requirements

- Windows 2000/XP/Vista.
- Available USB port.
- CD-ROM drive.
- IEEE802.11b, IEEE802.11g or IEEE802.11n wireless LAN.

## Procedure

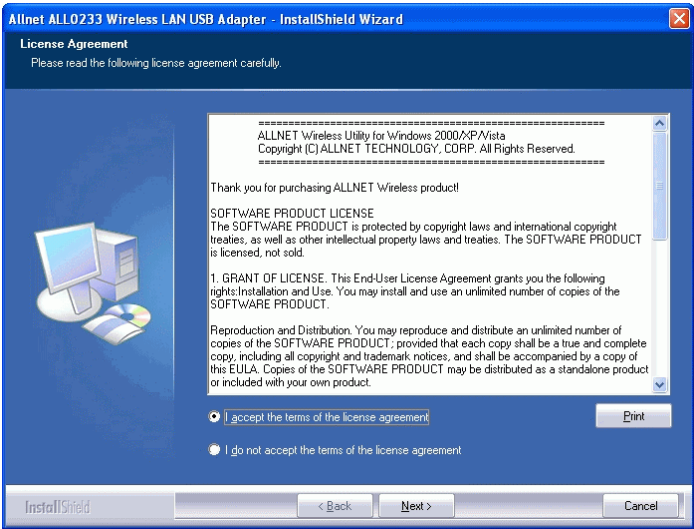
**You should install the supplied software BEFORE inserting the Wireless-N USB Dongle.**

1. Insert the CD-ROM into the drive on your PC.
2. The installation program should start automatically. If it does not, run the Setup.exe program.



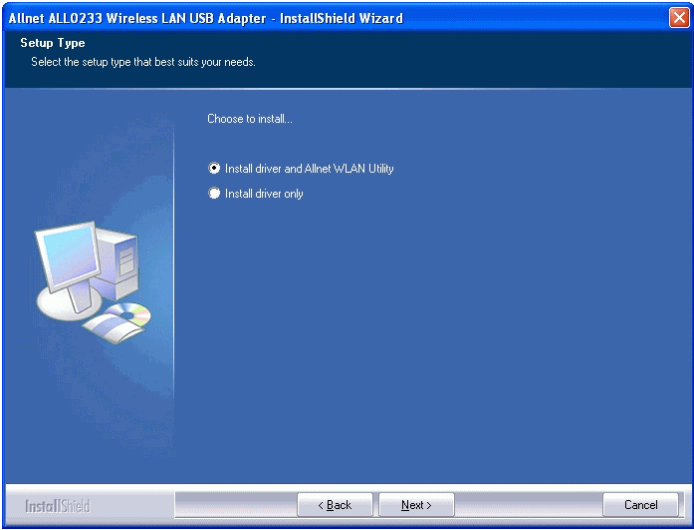
**Figure 1: Start Installation**

3. On the License Agreement screen, select *I accept the terms of the license agreement*. Click *Next*.



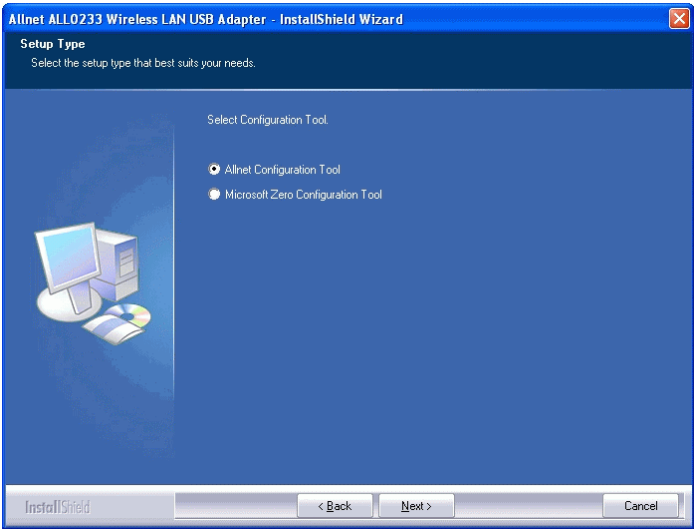
**Figure 2: License Agreement Screen**

4. Choose *Install driver and Allnet WLAN Utility* to install both the driver and Allnet utility software, or *Install driver only*.



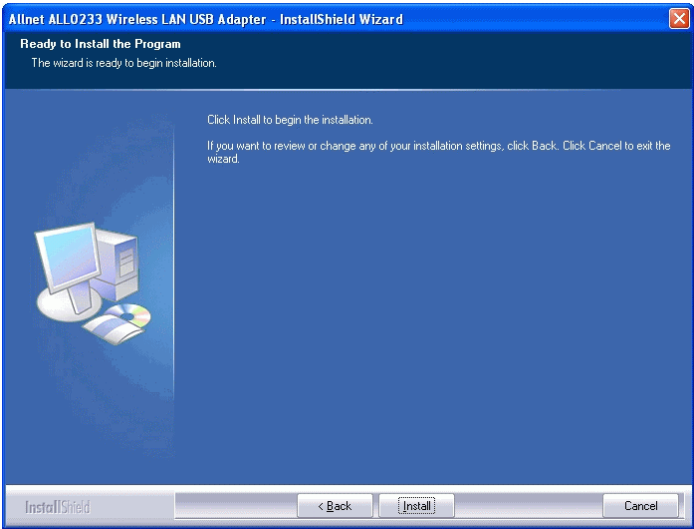
**Figure 3: Setup Type Screen**

5. Select either *Allnet Configuration Tool* or *Microsoft Zero configuration Tool* on the following screen.



**Figure 4: Windows New Hardware Screen**

6. On the following screen, click *Install*.






7. Click *Finish* to exit the Wizard.
8. Insert the Wireless-N USB Dongle firmly into USB port of the PC.
9. If the Wireless-N USB Dongle was installed properly, you will now have a new icon in your system tray, as shown below.



**Figure 5: System Tray Icon**

**Wireless-N USB Dongle Icon Table**

	Connection to the Wireless-N USB Dongle is established. The length of green color indicates the signal strength.
	No connection to the Wireless-N USB Dongle.
	The Wireless-N USB Dongle is unplugged.

10. You can double- click this icon to configure the Wireless interface. See the following chapter for details.



## Chapter 3

# Using the Windows Utility



*This Chapter provides Setup details for the AP mode of the Wireless-N USB Dongle.*

### Overview

If using Windows, you can use the supplied utility to configure the Wireless interface.

#### To Use the supplied Windows utility for Configuration

- Double-click the *Wireless Utility* icon in the desktop.
- Click *Start - Programs - Allnet-All0233 - Wireless Utility*.

This Chapter assumes you are using the supplied Wireless utility.

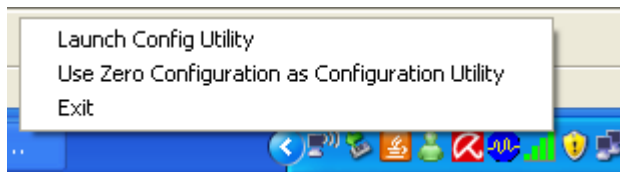
### System Tray Icon

If the Wireless Utility program is running, you can double-click the icon in the System Tray or right-click the icon and select "Launch Config Utility" to open the application.

### Status Information

The menu options available from the System Tray icon are:

- **Launch Config Utility** - This will display the main screen of the Utility.
- **Use Zero Configuration as configuration Utility** - Wireless Zero Configuration (WZC), is a service of Microsoft Windows which dynamically selects a wireless network to connect.
- **Exit** - Terminate the connection to the Wireless-N USB Dongle.



**Figure 6: Wireless-N USB Dongle menu**

## Connecting to a Wireless Network

Double-click the Icon to open the Network screen, where you can select the Wireless network you wish to join.

## Network Screen

This screen is displayed when you double-click the system tray icon. You can also click the Network tab in the screen.

When you open the utility program, it will scan all the channels to find all the access points/stations within the accessible range and automatically connect to one of the wireless devices which have the highest signal strength.

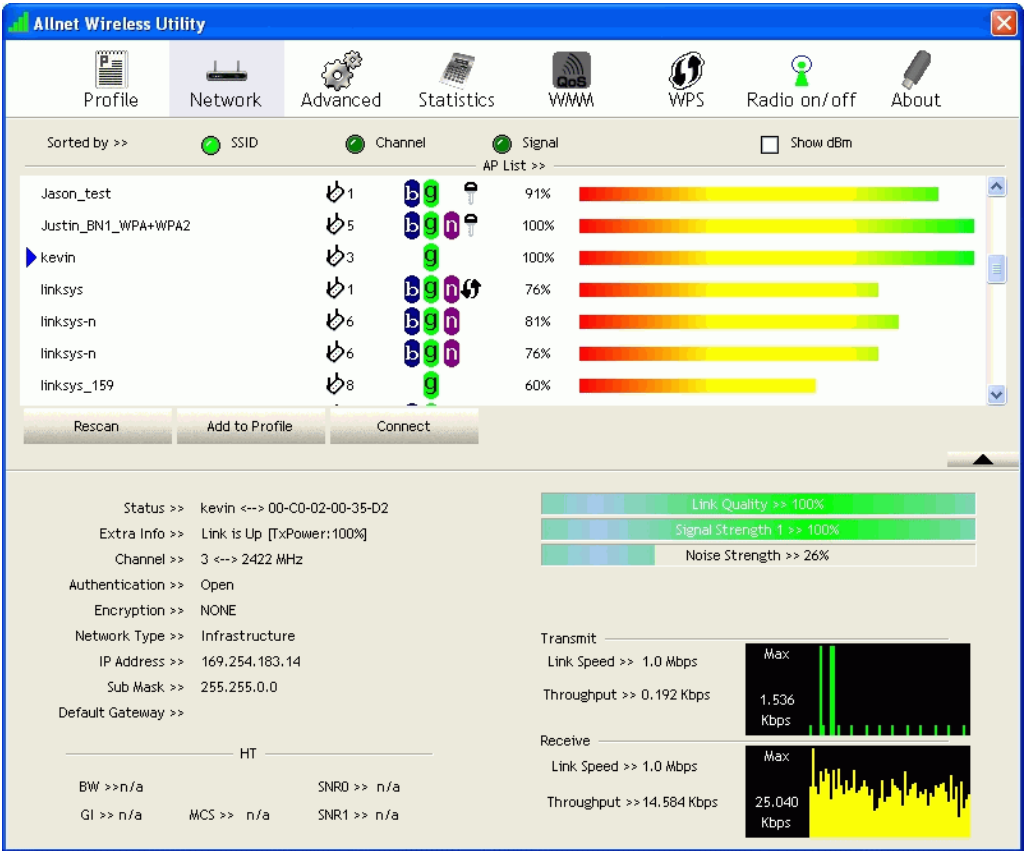


Figure 7: Network Screen

## Data - Network Screen

SSID	The SSID (up to 32 printable ASCII characters) is a unique name identified in a WLAN.
Network Type	It displays the Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
Channel	The channel used by the Wireless network.
Wireless Mode	AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode

<b>Security-Enable</b>	Whether AP provides security-enabled wireless network.
<b>Signal</b>	This is displayed as percentage (0 ~ 100%) of specified network.
<b>Rescan</b>	Click this button to rescan for all Wireless networks.
<b>Add to File</b>	Click this button to add the selected AP to Profile setting. It will bring up profile page and save user's setting to a new profile.
<b>Connect</b>	Click this button to connect the Wireless network.

### Wireless Network Sequence (order)

You can click the radio buttons in the **Sort by >>** section (ex. SSID, Channel or Signal) to arrange the Wireless network in the desired order.

### To Connect to a Wireless Network

- Click the name of the wireless network to which you want to connect, and then click **Connect**.

Note that once you are connected to a Wireless network, the **Network** screen will identify the current wireless network with a blue arrow icon, as shown below.

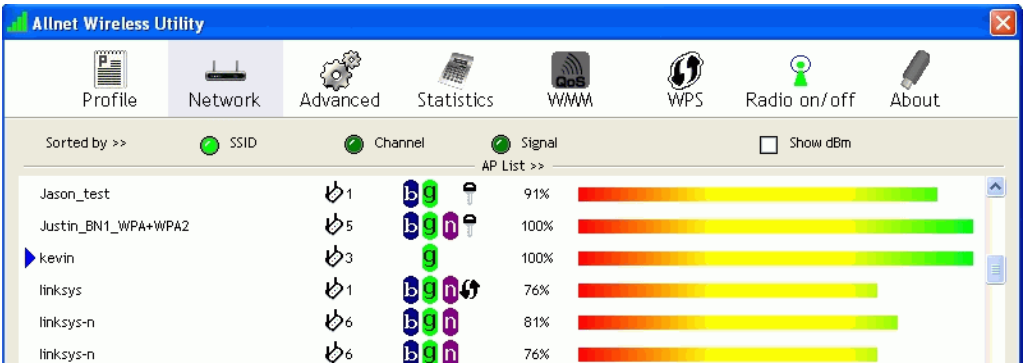


Figure 8: Network Screen – Connected

## Icons



It indicates network type is infrastructure mode.



It indicates network type is Ad-hoc mode.



802.11b wireless mode



802.11g wireless mode



802.11n wireless mode



It indicates security-enabled wireless network.




It shows the information of Link Status Section.



It hides the information of Link Status Section.

## Link Status Screen

The Link Status section displays the detailed information of the current connection. Click  button to show the status screen.

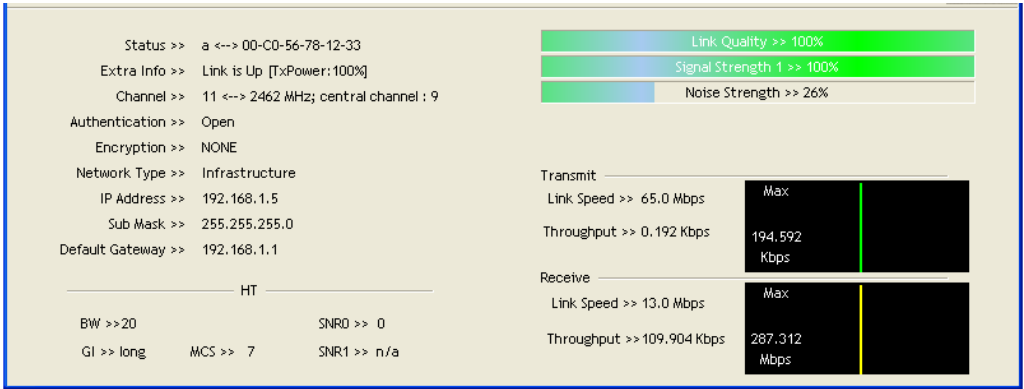


Figure 10: Link Status

### Data - Link Status

Link Information	
Status	It will indicate the current link status.
Extra Info	It shows the link status.
Channel	It displays the current channel in use.
Authentication	It will indicate the current authentication mode in use.
Encryption	It shows the wireless security that the wireless network is using.
Network Type	This will indicate "Infrastructure" or "Ad-hoc".
IP Address	It shows the current IP address on the wireless interface.
Subnet Mask	Subnet mask for the current IP address.
Default Gateway	Gateway IP address associated with the current IP address.
HT	It displays current HT status in use (802.11n wireless card only).
Link Quality	It displays connection quality based on signal strength and TX/RX packet error rate.
Signal Strength (1~3)	It receives signal strength (1~3), user can choose to display as percentage or dBm format.
Noise Strength	It displays noise signal strength.
Link Speed	It will show current transmit rate and receive rate.
Throughout	It displays transmits and receive throughput in unit of Mbps.

## Profile Screen

Click *Add to Profile* button on the Network tab, or you can choose *Profile* tab of the utility, then click *Add*, the Add Profile window will pop up. Users can setup the general settings, encryption and authentication settings and so on. If you want to do the general settings, please follow the instructions below.

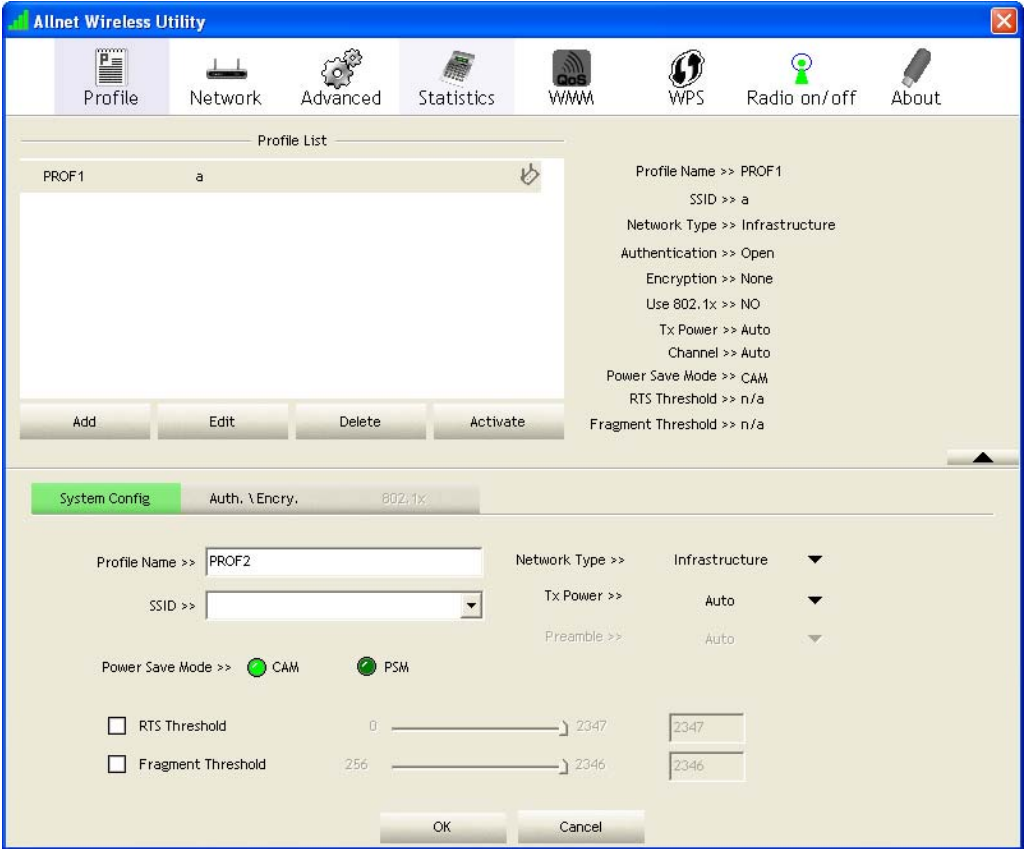


Figure 10: Profile Screen

### Data - Profile Screen

System Config	
Profile Name	Enter or select a suitable name for this profile. Each profile must have a unique name.
SSID	If the desired wireless network is currently available, you can select its SSID. Otherwise, type in the SSID of the desired wireless network.
Power Save Mode	Select either CAM (Constantly Awake Mode) or PSM (Power Saving Mode).
RTS Threshold	Select a value within the range of 0 to 2347 bytes
Fragment Threshold	Select the value from 256 to 2346 bytes. The default value is 2346.

<b>Network Type</b>	<p>Select the desired option:</p> <ul style="list-style-type: none"> <li>• <b>Infrastructure</b> - Select this to connect to an Access point.</li> <li>• <b>Ad-Hoc</b> - Select this if you are connecting directly to another computer.</li> </ul>
<b>Tx Power</b>	Select the Tx (transmission) power according to the real environment.
<b>Preamble</b>	The preamble defines the length of the CRC (cyclic redundancy check). Select either <i>Auto</i> or <i>Long Preamble</i> .
<b>OK button</b>	Click this button to save the settings and close the page.
<b>Cancel button</b>	The "Cancel" button will discard any data you have entered and exit the page.
<b>Auth./Encyp.</b>	
<b>Authentication</b>	<p>You MUST select the option to match the Wireless LAN you wish to join. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Open</b> - Broadcast signals are not encrypted. This method can be used only with no encryption or with WEP.</li> <li>• <b>Shared</b> - Broadcast signals are encrypted using WEP. This method can only be used with WEP.</li> <li>• <b>LEAP</b> - Light Extensible Authentication Protocol is a pre-EAP, Cisco-proprietary protocol. If selected, you have to enter the identity, password and domain name of your computer.</li> <li>• <b>WPA</b> - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.</li> <li>• <b>WPA-PSK</b> - PSK means "Pre-shared Key". You must enter this Passphrase value; it is used for both authentication and encryption.</li> <li>• <b>WPA2</b> - This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.</li> <li>• <b>WPA2-PSK</b> - This is a further development of WPA-PSK, and offers even greater security. You must enter this Passphrase value; it is used for both authentication and encryption.</li> <li>• <b>WPA None</b> - If selected, you can only set encryption and WPA-Preshared Key settings.</li> </ul>

<b>Encryption</b>	<p>The available options depend on the Authentication method selected above. The possible options are:</p> <ul style="list-style-type: none"> <li>• <b>None</b> - No data encryption is used.</li> <li>• <b>WEP</b> - If selected, you must enter the WEP data shown below. This WEP data must match the Access Point or other Wireless stations.</li> <li>• <b>AES, TKIP</b> - These options are available with WPA-PSK, WPA2-PSK, WPA and WPA2. Select the correct option.</li> </ul>
<b>Use 802.1x</b>	<p>This setting only takes effect when using Open, Shared, WPA or WPA2 mode. If enabled, click the <i>802.1x</i> tab to configure the related settings.</p>
<b>WPA Preshared Key</b>	<p>For WPA-PSK and WPA2-PSK modes, you need to enter the desired value (8~63 characters). Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.</p>
<b>WEP Key (1~4)</b>	<p>This setting is only available for Open or Shared mode. There are 2 modes:</p> <ul style="list-style-type: none"> <li>• <b>Hex</b> - Only "A~F", "a~f", and "0~9" are allowed to be entered.</li> <li>• <b>ASCII</b> - Numerical values, characters or signs are all allowed to be entered.</li> </ul>



<b>802.1x</b>	
<b>EAP Method</b>	<p>There are 5 methods in the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>PEAP</b> - Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.</li> <li>• <b>TLS-Smart Card</b> - Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.</li> <li>• <b>TTLS</b> - Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.</li> <li>• <b>EAP-FAST</b> - Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution.</li> <li>• <b>MD5-Challenge</b> - Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.</li> </ul>
<b>Tunnel Authentication</b>	Select the desired option from the drop-down list.
<b>Session Resumption</b>	After reconnecting the signal which broke up, you can enable the session resumption to reduce the transferring packet to accelerate the speed.
<b>Authentication ID / Password</b>	Enter the required data into the fields.
<b>Tunnel ID / Password</b>	Enter the ID and Password for the tunnel.
<b>Use Client certificate</b>	Click the checkbox to enable certificate authority server function.
<b>Use certificate chain</b>	When the EAP authentication type such as TLS, TTLS or PEAP is selected and required a certification to tell the client what server credentials to accept from the authentication server in order to verify the server, you have to enable this function and enter the required data in the related fields.

### **To add a profile**

1. On the Profile tab, click *Add* button.
2. Complete and verify the settings on this screen are correct.
3. Click *OK*.

### **To delete a profile**

1. On the Profile tab, select the profile that you want to delete.
2. Click *Delete*.

### **To edit a profile**

1. On the Profile tab, select the profile that you want to edit.
2. Click *Edit* button.
3. Change the profile settings as necessary.
4. Click *OK*.

### **To enable a profile**

1. In the list of available profiles, click the profile that you want to enable.
2. Click *Activate*.

# Advanced Screen

Click *Advanced* tab of the utility, you can configure the detailed settings in this page.

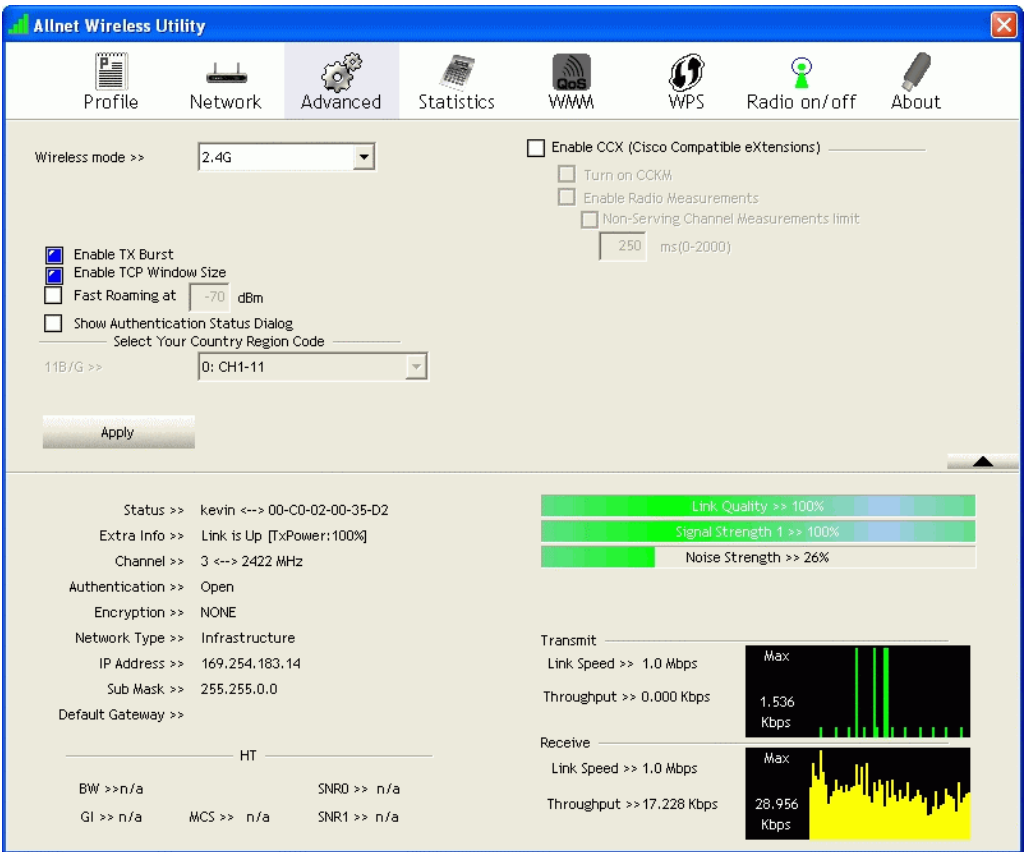


Figure 9: Advanced Screen

## Data - Advanced Screen

Advanced	
Wireless Mode	Select the desired wireless mode.
Enable Tx Burst	Tx Burst enables the adapter to deliver better throughput during a period of time but the function only takes effect when connecting with the AP which also supports Tx Burst.
Enable TCP Window Size	The TCP Window is the amount of data which a sender can send on a particular connection before it gets an acknowledgement back from the receiver that it has gotten some of it. When the router or AP which the adapter is connecting to has set up the TCP Window, you can enable the parameter to meet the data size for the router or AP connection. The larger TCP Window the better performance.
Fast Roaming at..	When you want fast roaming to the network nearby without intercepting the wireless connection especially the adapter is applied to the multimedia application or a voice call, you can enable this function.

<b>Show Authentication Status Dialog</b>	When connecting to an AP with authentication, if enabling this function, it will display dialogs about 802.1x authentication during the process.
<b>Select Your Country Region Code</b>	There are 8 kinds of Country Region Codes to choose from.
<b>Enable CCX (Cisco Compatible eXtensions)</b>	<p>CCX (Cisco Compatible Extensions) is developed by Cisco for the radio monitoring and fast roaming.</p> <ul style="list-style-type: none"> <li>• <b>Turn on CCKM:</b> During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server. When you configure your wireless LAN for fast re-association, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications.</li> <li>• <b>Enable Radio Measurement:</b> When this parameter is enabled, the Cisco AP can run the radio monitoring through the associated CCX-compliant clients to continuously monitor the WLAN radio environment and discover any new Aps that are transmitting beacons.</li> </ul>
<b>Apply</b>	Click this button to save the changes you made.

Statistics Screen

Click *Statistics* tab of the utility, the page will display the transmitted and received results.

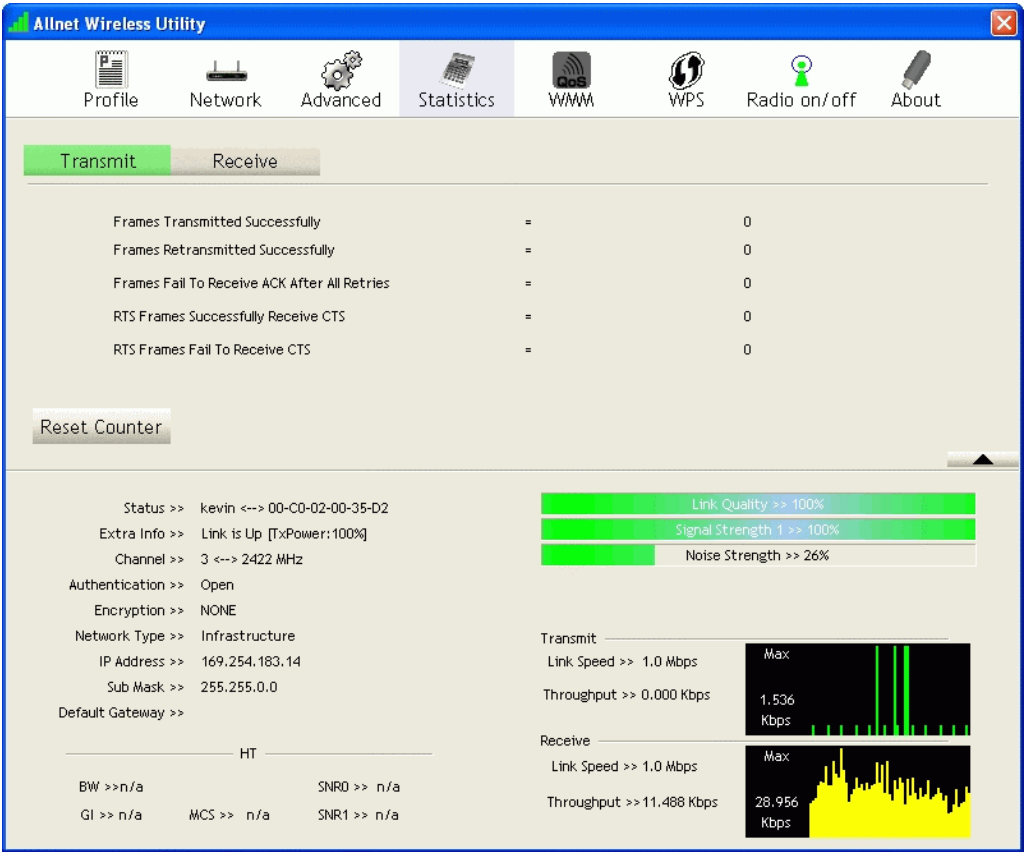


Figure 10: Statistics Screen

Data - Statistics Screen

Transmit	
Frames Transmitted Successfully	Frames successfully sent.
Frames Retransmitted successfully	Frames successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Frames failed to transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Successfully receive CTS (Clear To Send) after sending RTS (Request To Send) frame.
RTS Frames Fail To Receive CTS	Failed to receive CTS (Request To Send) after sending RTS (Clear To Send).

Receive	
<b>Frames Receive Successfully</b>	Frames received successfully.
<b>Frames Receive With CRC Error</b>	Frames received with CRC error.
<b>Frames Dropped Due To Out-of-Resource</b>	Frames dropped due to resource problem.
<b>Duplicate Frames Received</b>	Frames received more than twice.
<b>Reset Counter</b>	Click the button to reset counters to zero.

WMM Screen

Click *WMM* tab of the utility, and you will see the following screen:

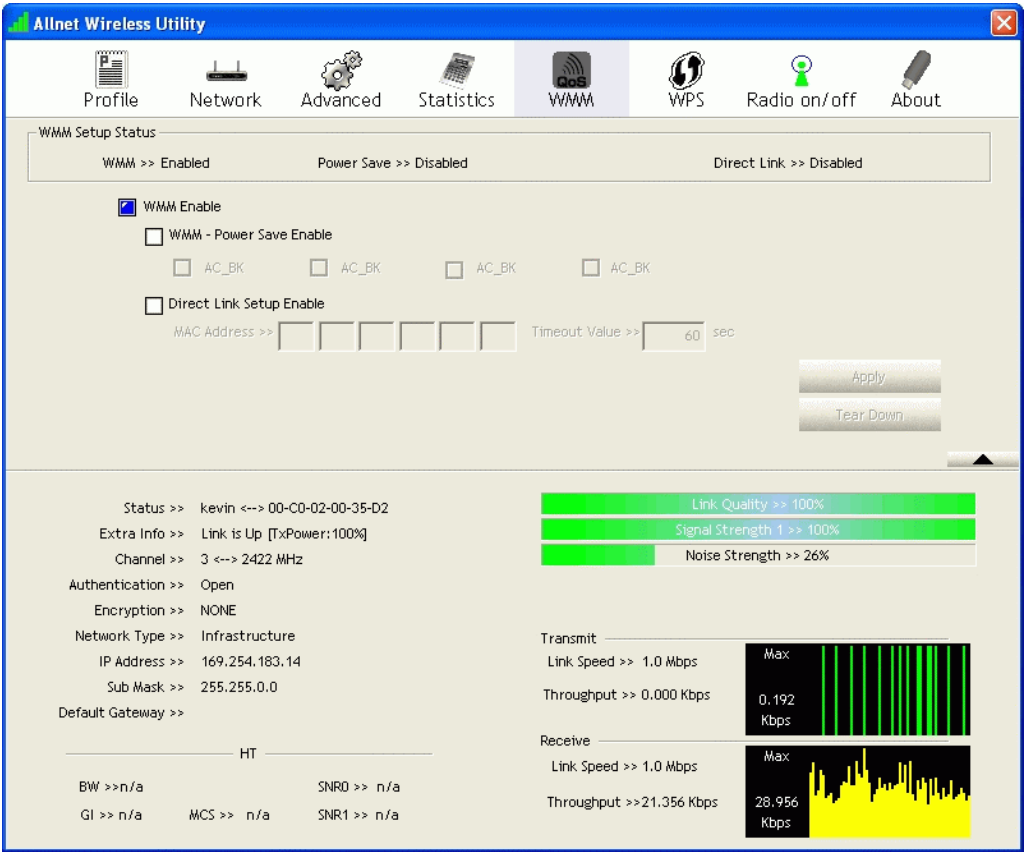


Figure 11: WMM Screen

Data - WMM Screen

WMM Enable	WMM is short for Wi-Fi Multimedia. It is a standard created to define quality of service (QoS) in Wi-Fi networks. It is a precursor to the upcoming IEEE802.11e WLAN QoS draft standard, which is meant to improve audio, video and voice applications transmitted over Wi-Fi. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. Click the check box and then click "Apply" button to apply this function to the system.
WMM - Power Save Enable	Click the check box, and select the desired type of power saving mode.
Direct Link Setup Enable	Enable the check box and you may start to set MAC Address, Timeout Value and check the DLS Status. Click "Apply" and this setting will be applied to the system.

<b>MAC Address</b>	Enter the remote system which you want to connect with. When you want to enable this function, you have to make sure that your wireless network supports WMM function and then enter the MAC address of the adapter which wants to connect with the remote system.
<b>Timeout Value</b>	The utility performs time-outs so that the program does not sit idle waiting for input that may never come. Set a value to apply to the system with WMM.
<b>Apply</b>	Click this button to save the changes you made.
<b>Tear Down</b>	Click this button will disconnect the selected Direct Link Setup.



# WPS Screen

WPS (Wi-Fi Protected Setup) can simplify the process of connecting any device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering a PIN code.

You will use the WPS screen when you try to connect the wireless network with the WPS function.

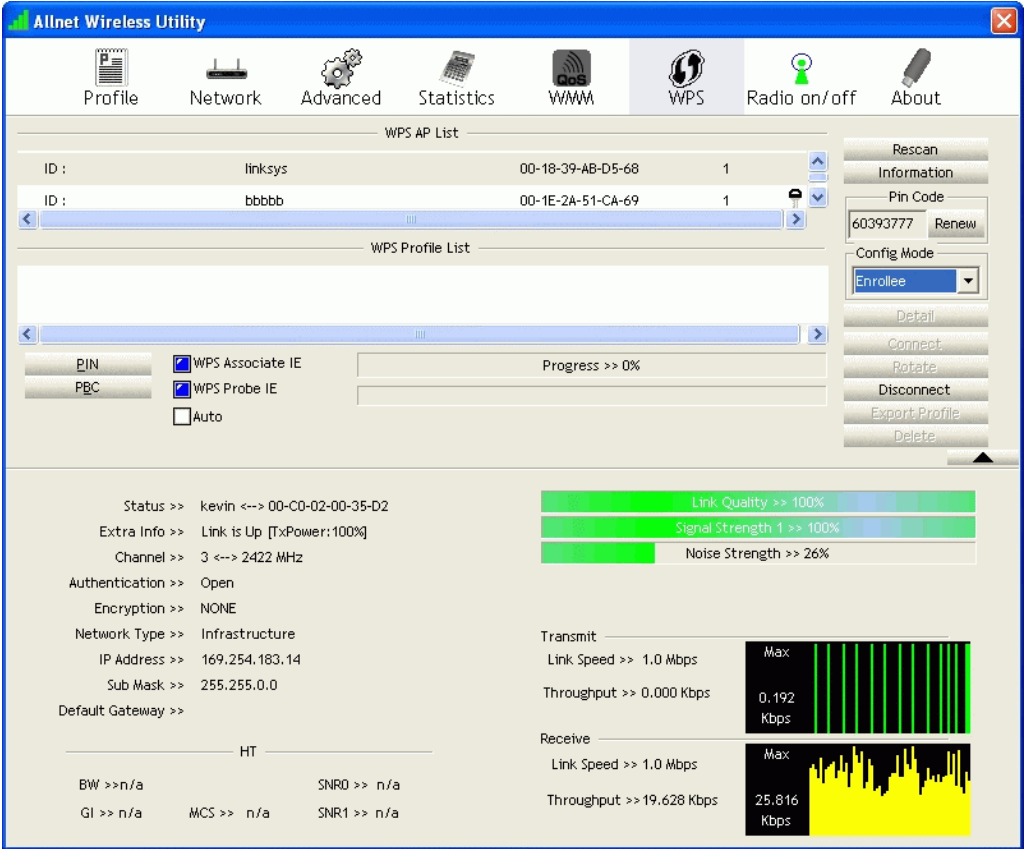


Figure 12: WPS Screen

## Data - WPS Screen

WPS	
WPS AP List	It displays the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, Channel, ID (Device Password ID) and Security-Enabled.
Rescan	Click this button to update information on surrounding wireless network.
Information	Display the information about WPS on the selected network. List information includes Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.

<b>PIN Code</b>	Enter the PIN code displayed in the following field to the WPS screen of the access point. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.
<b>Config Mode</b>	Our station role-playing as an <i>Enrollee</i> or an external <i>Registrar</i> .
<b>Detail</b>	Information about Security and Key in the credential.
<b>Connect</b>	Click this button to connect to the selected network inside credentials.
<b>Rotate</b>	Click this button to rotate to connect to the next network inside credentials.
<b>Disconnect</b>	Click this to stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of utility if exist. If there is an empty profile page, the driver will select any non-security AP.
<b>Export Profile</b>	Export all credentials to Profile.
<b>Delete</b>	Click to Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
<b>PIN</b>	Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
<b>PBC</b>	Start to add to AP using PBC configuration method.
<b>WPS associate IE</b>	Send the association request with WPS IE during WPS setup. It is optional for STA.
<b>WPS Probe IE</b>	Send the probe request with WPS IE during WPS setup. It is optional for STA.
<b>Progress Bar</b>	Display rate of progress from Start to Connected status.
<b>Status Bar</b>	Display currently WPS Status.

Radio on/off Screen

Yu can turn the radio signal on/off by clicking this button.

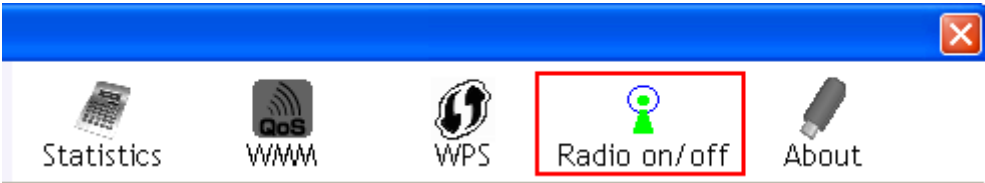




Figure 13: Radio on/off

 Radio on/off	The radio signal is on.
 Radio on/off	The radio signal is off.

# About Screen

This screen displays details of the traffic sent or received on the current Wireless network.



Figure 14: About Screen

This tab shows the following information:

- RaConfig Version
- Driver Version
- EEPROM Version
- Phy\_ Address
- Date
- Firmware Version

# Appendix A

## Specifications



### Wireless-N USB Dongle

<b>Model:</b>	ALL0233
<b>Standards:</b>	IEEE 802.11b, IEEE 802.11g, Draft 802.11n compliant
<b>Computer Slot Type:</b>	USB
<b>Chipset:</b>	Ralink RT3070(MAC/BB/RF)
<b>Tx:</b>	1
<b>Rx:</b>	1
<b>Date Rates:</b>	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 (802.11n)
	54, 48, 36, 24, 18, 12, 9, and 6 Mbps (802.11g)
	11, 5.5, 2, 1 Mbps (802.11b)
<b>Operating Channels:</b>	11 for North America, 13 for Europe and Japan
<b>Operating Frequency:</b>	2.4 ~ 2.4835 GHz
<b>Modulation Technique:</b>	
Draft 802.11n:	BPSK, QPSK, 16-QAM, 64-QAM
802.11g:	OFDM
802.11b:	CCK,QPSK,BPSK
<b>Media Access Protocol:</b>	CSMA/CA
<b>Operating Voltage:</b>	5V +/- 5%
<b>Transmit Power:</b>	802.11n: 13.5 +/- 1 dBm 802.11g: 13.5 +/- 1 dBm 802.11b: 17 +/- 1 dBm
<b>Security:</b>	WPA/WPA2; 128-bit TKIP/AES encryption, 40/64-, 128-bit WEP shared-key encryption  802.1x, and EAP-TLS, and PEAP authentication
<b>OS Requirements:</b>	Windows Vista/XP/2000

## Appendix B



# About Wireless LANs

*This Appendix provides some background information about using Wireless LANs (WLANs).*

## Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

### Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

### Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.



**Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.**

## BSS/ESS

### BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

**Using the same SSID is essential.** Devices with different SSIDs are unable to communicate with each other.

### ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points **SHOULD** use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

## Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

## WEP & WPA-PSK

Both WEP and WPA-PSK are standards for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

WPA-PSK is a later standard than WEP, and is more secure.

## WPA2-PSK

This is a later version of WPA (WPA-PSK). The major change is the use of AES (Advanced Encryption System) for protecting data. AES is very secure, considered to be unbreakable. The PSK (Pre-shared Key) must be entered on each Wireless station.

**If WPA2-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:**

<b>WPA2 PSK (Pre-shared Key)</b>	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
<b>Encryption</b>	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

## Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

<b>Mode</b>	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
<b>SSID (ESSID)</b>	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
<b>Security</b>	<p>The Wireless Stations and the Access Point must use the same settings for Wireless security (Disabled, WEP, WPA-PSK, WPA2-PSK, WPA, WPA2)</p> <ul style="list-style-type: none"><li>• If Wireless security remains disabled on the Access Point, all stations must have wireless security disabled.</li><li>• If Wireless security is enabled on the Access Point, each station must use the same settings.</li></ul>





Germering, October 2008

## **EC – Declaration of conformity**

for

### **ALL0233 Wireless-N USB Dongle**



This equipment conforms with the requirements of the Council Directive

**Applicable to R&TTE Directive 1999/5/EC (The Radio and Telecommunications Terminal Equipment Directive)**

and the mutual recognition of their conformity.

The safety advice in the documentation accompanying the products shall be obeyed.  
The conformity to the above directive is indicated by the CE sign on the device.

The ALLNET ALL0233 Wireless-N USB Dongle conform to the European Directives R&TTE 1999/5/EC, and EC Low Voltage Directive, 2006/95/EC.

This equipment meets the following conformance standards:

**EN 301 489-1 V1.6.1 : (2005-09)**

**EN 301 489-17 V1.2.1 : (2002-08)**

**EN 300 328 V1.6.1 (2004-11)**

**AS/NZS CISPR 22 Class B and AS/NZS 4268 :2003**

**EN 300 328 V1.7.1 : (2006-10)**

**IEC 60950-1: 2001**

**EN 60950-1: 2001+A11 :2004**

This equipment is intended to be operated in all countries.

This declaration is made by

ALLNET Computersysteme GmbH

Maistr. 2

82110 Germering

and can be downloaded from <http://www.allnet.de/ce-certificates/> .