# 802.11n/b/g WLAN Module WM5208

User's Manual

## FCC Certification

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.

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



#### CAUTION

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 with any other transmitters except in accordance with FCC multi-transmitter product procedures.

Refering to the multi-transmitter policy, multiple-transmitter(s) and module(s) can be operated simultaneously without C2P.

#### **IMPORTANT NOTE:**

This module is intended for OEM integrator. The OEM integrator is responsible for the compliance to all the rules that apply to the product into which this certified RF module is integrated. Additional testing and certification may be necessary when multiple modules are used.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

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

#### USERS MANUAL OF THE END PRODUCT:

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users manual: This device complies with Part 15 of 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.

#### LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX FCC ID: MQ4WM5208 ". If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of 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.

#### **IC** Certification

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and its antenna(s) must not be co-located with any other transmitters except in accordance with IC multi-transmitter product procedures.

Refering to the multi-transmitter policy, multiple-transmitter(s) and module(s) can be operated simultaneously without reassessment permissive change.

Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

#### **IMPORTANT NOTE:**

#### IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This module is intended for OEM integrator. The OEM integrator is still responsible for the IC compliance requirement of the end product, which integrates this module.

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

#### USERS MANUAL OF THE END PRODUCT:

In the users manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the IC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. 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.

#### LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX IC : 2826B-WM5208 ".

#### Antenna list:

Ant.	Brand	Model Name	Antenna Type	Connector	Gain (dBi)	Remark
1	Abocom	M30-05+++-000	PIFA Antenna	N/A	2.92	TX/RX
2	Abocom	M30-05+++-000	PIFA Antenna	N/A	3.14	RX

Note: The EUT has two antennas (1TX, 1RX).

# Table of Contents

CHAPTER 1: INTRODUCTION	1
Features	
Physical Details	1
CHAPTER 2: INSTALLATION	2
For Windows 2000/XP	2
Install Software	2
Install Hardware	4
Verification	4
For Windows Vista	5
Install Software	5
Install Hardware	7
Verification	7
For Windows 7	8
Install Software	8
Install Hardware	
Verification	
CHAPTER 3: NETWORK CONNECTION	11
How to Make a Connection	11
How to Add a Profile	
CHAPTER 4: UTILITY CONFIGURATION	14
For Windows 2000/XP	14
Station Mode	
Switch to AP Mode	23
Soft AP mode	
For Windows Vista	
Station Mode	
Switch to AP Mode	
Soft AP mode	
For Windows 7	
Station Mode	44
Switch to AP Mode	53
Soft AP mode	54

СНАРТЕ	ER 5: UNINSTALL	59
For	R WINDOWS 2000/XP	59
For	r Windows Vista	51
For	r Windows 7	33

# Chapter 1: Introduction

WM5208 measures just around 15 mm long and 15mm wide that make it hold the distinction of being the smallest USB dongle in the world at present. WM5208 give mobile workers the freedom of staying connected to the network while roaming around a building or multiple buildings maintaining access to the Internet, e-mail, networked applications with the best convenience in narrow or crowded space for it's ultra micro size.WM5208 is expected to be able to reach 150Mbps, which is relatively lower than normal, but still far more than sufficient to receive media streaming to the from access point.

# **Features**

- □ 1T1R Mode with 150Mbps PHY Rate
- Complies with IEEE 802.11n and IEEE 802.11 b/g standards
- □ Supports WEP 64/128, WPA, WPA2
- □ Supports USB 2.0 interface

# **Chapter 2: Installation**

# For Windows 2000/XP

## **Install Software**

#### Note:

# Do not insert the Wireless USB Adapter into the computer until the InstallShield Wizard finished installing.

1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click **Install** to begin the installation.



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



## Install Hardware

#### Note:

#### Insert the Wireless USB Adapter when finished software installation.

Insert the Wireless USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.

## Verification

To verify the device is active in the computer. Go to **Start > Control Panel > System > Hardware> Device Manager**. Expand the **Network adapters** category. If the **802.11n/b/g 2cm Wireless LAN USB2.0 Adapter** is listed here, it means that the device is properly installed and enabled.



# For Windows Vista

## Install Software

#### Note:

# Do not insert the Wireless USB Adapter into the computer until the InstallShield Wizard finished installing.

1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click **Install** to begin the installation.



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



## Install Hardware

#### Note:

#### Insert the Wireless USB Adapter when finished software installation.

Insert the Wireless USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.

## Verification

To verify the device is active in the computer. Go to **Start >Control Panel > Hardware and Sound > Device Manager**. Expand the **Network adapters** category. If the **802.11n/b/g 2cm Wireless LAN USB2.0 Adapter** is listed here, it means that the device is properly installed and enabled.



# For Windows 7

## Install Software

#### Note:

# Do not insert the Wireless USB Adapter into the computer until the InstallShield Wizard finished installing.

1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically. Please click **Next** to process the installation.



2. When prompt to the following message, please click Install to begin the installation



3. When the following screen appears, click **Finish** to restart the computer to complete the software installation.



## Install Hardware

#### Note:

#### Insert the Wireless USB Adapter when finished software installation.

Insert the Wireless USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.

## Verification

To verify the device is active in the computer. Go to **Start > Control Panel > Device Manager**.

Expand the Network adapters category. If the 802.11n/b/g 2cm Wireless LAN USB2.0 Adapter is

listed here, it means that the device is properly installed and enabled.



# Chapter 3: Network Connection

# How to Make a Connection

To make a connection with an access point, please follow below steps. Here takes Windows XP OS for example.

**Step 1**: After set up the Wireless USB Adapter successfully, please launch the Configuration Utility. There are two ways to launch the utility by:

(1) Double clicking the Intelligent Wireless LAN Utility icon on the desktop.



(2) Or go to Start →All Programs →Intelligent Wireless Utility → Intelligent Wireless LAN



**Step 2:** Please go to the **Available Network** tab, the system will automatically scan access points nearby, or click **Refresh** button to site survey again.

MyComputer	General Profile Available Ne	etwork clatu	s Statistics V	√i-Fi Protect Setup	
	Available Network(s)				
	SSID	Channel	Encryption	Network Authentication	Signal 📥
	649 3Q3Q	1	WEP	Unknown	42%
	(m) WR254E	1	None	Unknown	42%
	4/12 ZyXEL	1	None	Unknown	62%
	102 ZyXEL-1	1	None	Unknown	46%
	<sup>(1)</sup> planexuser	1	None	Unknown	42%
	Mairlive 2 None Unknown	Unknown	42%		
	""ZyXEL_3090_AP	3	AES	WPA2 Pre-Shared Key	56%
Implication         4         TKIP         WPA Presentation           Implication         5         None         Unknown	4	TKIP	WPA Pre-Shared Key	8%	
	Unknown	70%			
	( <sup>40)</sup> 412	6	TKIP/AES	WPA Pre-Shared Key/	88%
	Maintenance And Annual Annu	6	None	Unknown	60%
	MP ArthurAP	6	WEP	Unknown	62%
	40 ZyXEL_3090	8	AES	WPA2 Pre-Shared Key	74%
	(mina	9	TKIP	WPA Pre-Shared Key	72%
	M/DA Dro Charod Vov	70%			
	Refre	sh		Add to Profile	
	Note Double click on item	to join/creat	te profile.		
-		co jon yeree	to promo.		

**Step 3**: Then, double click preferred access point or click **Add to Profile** button to make a connection (if the access point has been set up security, please enter passwords and then click **OK**.)

MyComputer	General Profile Available Netwo	rk Statu	s Statistics V	Vi-Fi Protect Setup	
302.11n/b/g 2cn	Available Network(s)				
	SSID	Channel	Encryption	Network Authentication	Signal 🛆
	1490 3Q3Q	1	WEP	Unknown	42%
	499 WR254E	1	None	Unknown	42%
	(in) ZyXEL	1	None	Unknown	62%
	10 <sup>40</sup> ZyXEL-1	1	None	Unknown	46%
	<sup>(M)</sup> planexuser	1	None	Unknown	42%
	((m) airlive	2	None	Unknown	42%
	6/12 ZyXEL_3090_AP	З	AES	WPA2 Pre-Shared Key	56%
	<sup>11</sup> ZyXEL-giga	4	TKIP	WPA Pre-Shared Key	8% -
	10815SID.00c473db	5	None	Unknown	70%
	494 Cherry	6	TKIP/AES	WPA Pre-Shared Key/	88%
	ADOCOM-Wireless	0	None	Unknown	5U%
	M <sup>10</sup> ArthurAP	6	WEP	Unknown	62%
	"( <sup>1)</sup> ZyXEL_3090	8	AES	WPA2 Pre-Shared Key	74%
	(mina	9	TKIP	WPA Pre-Shared Key	72%
		10	TVID	M/DA Dro Charod Kov	700/.
	Refresh			Add to Profile	
	Note				
	Der ble eliel, en itere te	inter from al	ka uwa Ala		
	Double click on item to	ioin/crea	te pronie.		

# How to Add a Profile

After launched Wireless LAN Utility and selected preferred access point, please click **Add to Profile** button to enter **Wireless Network Properties** windows. If the access point has been set up security, please enter passwords, and then click **OK** to save profile settings.

state namenti rap	51 (105).			_
Profile Name:	Cherry	802.1x configure		
Network Name(SSID):	Cherry	EAP TYPE :		
		GTC		
		Tunnel :	Privision Mode :	
access points are no	o-computer(ad hoc) hetwork; wreless t used.		*	
Channel:	11 (2462MHz)			
Cridini Ion	The solution ray	Username :		
Wireless network secu	arity			
This network requires	a key for the following:	Identity :		
Netw	vork Authentication: WPA2-PSK			
	Data encryption: AES	Domain :		
CHACH COPAG	PHRAL	Password :		
Key index (advanced)		Certificate :		
Network key:				10
1		PAC : Auto	Select RAC	
Confirm network key:				15

After finished above settings, please go to **Profile** tab to check the profile list (Available Profile(s)).

Refresh(R) Mode(M) About	:(A)		
MyComputer     S02,11n/b/g 2cn	General Profile Availa	able Network Status Statistics W	'i-Fi Protect Setup
	Available Profile(s)		
	Profile Name Cherry	SSID Cherry	Add
	a i		Remove
			Edit
			Duplicate
			Set Default
	<		×
Show Tray Icon	_	Disable Adapter	

# Chapter 4: Utility Configuration



- Show Tray Icon: Check to show the wireless adapter icon at the tray.
- Disable Adapter: Check this to disable the wireless adapter.
- Radio off: Check this to turn OFF radio function.
- Close: Click to leave the Intelligent 11n USB Wireless LAN Utility.

#### <u>General</u>

The General page displays the detail information of current connection.

Refresh(R) Mode(M) Abo	ut(A)	
MyComputer	General Profile Available Network Status Statistics Wi-Fi Protect Setup	
	Status: Associated	
	Speed: Tx:150 Mbps Rx:150 Mbps	
	Type: Infrastructure	
	Encryption: AES	
	SSID: Cherry	
	Signal Strength: 100%	
	Link Quality:	
	Notwerk Advacci	
	MAC Address: 00:E0:4C:71:00:01	
	IP Address: 192.168.1.102	
	Subnet Mask: 255,255,255,0	
	Gateway; 192,168,1,123	
	ReNew IP	
< >		
Show Tray Icon	🗌 Disable Adapter	Close

#### **General Tab**

Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Туре	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the Wireless USB Adapter.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.
Renew IP	Click the <b>Renew IP</b> button to obtain IP address form the connected gateway.

#### **Profile**

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.

😰 Intelligent 11n USB W	/ireless LAN Utility		
Refresh(R) Mode(M) About	(A)		
MyComputer	General Profile Avail Available Profile(s)	able Network    Status    Statistics    Wi-	Fi Protect Setup
	Profile Name	SSID	Add
	Cherry	Cherry	
			Remove
			Edit
			Duplicate
			Set Default
	¢		
Show Tray Icon		🔲 Disable Adapter	Close

Profile Tab		
Profile Name	Here shows a distinctive name of profile in this column.	
SSID	The <b>SSID</b> is the unique name shared among all wireless access points in the wireless network.	
Add	Click <b>Add</b> button to add a profile from the drop-down screen.	

Profile Name:	802.1x configure
Network Name(SSID):	EAP TYPE :
	GTC
	Tunnel : Privision Mode :
This is a computer-to-computer(ad hoc) network; wireless access points are not used.	-
Channel: (1 (2412/442)	Username :
Wireless network security	
This network requires a key for the following:	Identity :
Network Authentication: Open System 😽	
Data encryption: Disabled	Domain :
	Password :
Key index (advanced):	Certificate :
Network key:	
	PAC : Auto Select PA/S
Confirm network key:	

Profile Name: Users can enter profile name at will.

**Network Name (SSID)**: The SSID is the unique network name (case-sensitive) shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network.

This is a computer-to-computer (ad hoc) network; wireless access points are not used: This function is selected to enable the ad hoc network type that computers should be setup at the same channel to communicate to each other directly without access point, users can share files and printers between each PC and laptop. User can select channels form the pull-down menu.

#### Wireless network security

**Network Authentication:** There are several types of authentication modes including Open System, Shared Key, WPA-PSK, WPA2-PSK, WPA 802.1X, WPA2 802.1X and WEP 802.1X.

**Data encryption:** For Open System, Shared Key and WEP 802.1X authentication mode, the selection of encryption type is WEP. For WPA-PSK, WPA2-PSK, WPA 802.1X and WPA2 802.1X authentication mode, the encryption type supports both TKIP and AES.

#### When encryption is set to WEP...

**ASCII:** Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).

**PASS PHRASE:** Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).

**Key index (advanced):** Select 1~4 key index form the pull-down menu, must match with the connected AP's key index.

When encryption is set to WPA-PSK/ WPA2-PSK...

Network key: Enter network key at least 8 to 64 characters.

Confirm network key: Enter network key again to confirm.

	When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X
	When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge).
	EAP TYPE:
	• <b>TLS</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.
	• <b>LEAP:</b> Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
	• <b>TTLS</b> : Tunnelled 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.
	• <b>PEAP</b> : Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling 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.
	<ul> <li>MD5: 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:</b> This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2.
	Username: Enter the username for server.
	Identity: Enter the identity for server.
	<b>Domain:</b> Enter the domain of the network.
	<b>Certificate:</b> Choose server that issuer of certificates
Remove	Click <b>Remove</b> button to delete selected profile.
Edit	Click <b>Edit</b> button to edit selected profile.
Duplicate	Click <b>Duplicate</b> button to copy selected profile.
Set Default	Click <b>Set Default</b> button to set selected profile to be connected first.

#### **Available Network**

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate (s), and Mode.

😪 802,11n/b/g 2cn	and the second sec		2 STAURUCE A	VI-FI Protect Setup					
	Available Network(s)								
	SSID Ch	annel	Encryption	Network Authentication	Signal 🖄				
	1490 3Q3Q	1	WEP	Unknown	42%				
	(49) WR254E	1	None	Unknown	42%				
	teril ZyXEL	1	None	Unknown	62%				
	Ma ZyXEL-1	1	None	Unknown	46%				
	<sup>(ky)</sup> planexuser	1	None	Unknown	42%				
	<sup>((p)</sup> airlive	2	None	Unknown	42%				
	<sup>@</sup> <sup>®</sup> ZyXEL_3090_AP	З	AES	WPA2 Pre-Shared Key	56%				
	M <sup>31</sup> ZyXEL-giga	4	TKIP	WPA Pre-Shared Key	8% -				
	MPISSID-00c473db	5	None	Unknown	70%				
	47 <sup>44</sup> Cherry	6	TKIP/AES	WPA Pre-Shared Key/	88%				
	(*P) Abocom-Wireless	6	None	Unknown	60%				
	M <sup>1</sup> ArthurAP	6	WEP	Unknown	62%				
	<sup>((4)</sup> ZyXEL_3090	8	AES	WPA2 Pre-Shared Key	74%				
	(ip) mina	9	TKIP	WPA Pre-Shared Key	72%				
		10	חזעד	MOA Dro Charod Koy	700%				
	Refresh			Add to Profile	1				
	Note Double click on item to joir	n/creat	te profile.						
		_							

Network Tab	
SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Туре	Network type in use, Infrastructure or Ad-Hoc mode.
BSSID	Shows Wireless MAC address.
Supported Rate(s)	Shows the transmitting data rate.

Mode	<b>le</b> Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.		
Refresh	Click Refresh button to search and rescan the available network.		
Add to Profile	Select an available network (SSID) on the list and then click Add to Profile button to add it into the profile list.		
Note	Double click on item to join/create profile.		

#### <u>Status</u>

This tab listed the information about the wireless USB adapter and connected access point.

Intelligent 11n USB 1	Vireless	LAN U	tility				
Refresh(R) Mode(M) Abou	it(A)				-		
☑ ♥ MyComputer ♀ 802,11n/b/g 2cn	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup	
		Manu NDIS Shorn Auth Chan MAC Data Chan Statu SSID Netv Powe Asso Up T	afacturer Driver Version t Radio Header yption ienticate inel Set Address Rate (AUTO) inel (Frequency) us vork Type er Save Mode ciated AP MAC Time (hh:mm:ss)			<ul> <li>Intelligent</li> <li>1084.19.1113.</li> <li>No</li> <li>AES</li> <li>WPA2-PSK</li> <li>FCC</li> <li>00:E0:4C:71:00</li> <li>Tx:150 Mbps R</li> <li>11 (2462 MHz)</li> <li>Associated</li> <li>Cherry</li> <li>Infrastructure</li> <li>None</li> <li>00:E0:4C:33:11</li> <li>0:39:10</li> </ul>	2009 D:01 x:150 Mbps
Show Tray Icon			Disa	ible Ada	pter		Close

## **Statistics**

The Statistics screen displays the statistics on the current network settings.

fresh(R) Mode(M) Abou	t(A)							
MyComputer	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup		
002,111/b/g 201								
		Co	unter Name				Value	
		Тх	ОК				2969	
		TX	Error				0	
		Rx	Packet Count				964	
		Rx	Retry				93	
		Rx	ICV Error				0	
		-						
- 11								
				<u> </u>	4	_		
					Reset			
>								
1 Chow Tray Icon			Dis:	hla Ada	ntor		-	

Statistics			
Тх ОК	Shows information of packets successfully sent.		
Tx Error	Shows information of packets failed transmit after hitting retry limit.		
Rx OK	Shows information of packets received successfully.		
Rx Packet Count	Shows information of packets received successfully.		
Rx Retry	Shows information of packets failed transmit after hitting retry limit.		
Rx ICV Error	Shows information of packets received with ICV error.		
Reset	Click to reset counters to zero.		

#### <u>WPS</u>

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.

1 Intelligent 11n USB	Wireless LAN Utility	
Refresh(R) Mode(M) Abou	ut(A)	
MyComputer	General       Profile       Available Network       Status       Statistics       Wi-Fi Protect Setup         Wi-Fi Protected Setup (WPS)         An easy and secure setup solution for Wi-Fi network         Pin Input Config (PIN)         After pushing the PIN button.Please enter the PIN code into your AP.         PIN Code :       63912111         Pin Input Config (PIN)         Push Button         After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.         Push Button         Push Button Config (PBC)	
Show Tray Icon	Disable Adapter	Close

WPS Tab				
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use " <b>Renew</b> " button to re-generate new PIN Code.			
Pin Input Config (PIN)	Click the <b>Pin Input Config (PIN)</b> button to select specific AP to process PIN Config.			
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.			

#### <u>About</u>

This page displays the information of the Wireless USB Adapter Version.



## Switch to AP Mode

To access the soft AP mode, please select the Mode on the function list of the Utility to make the

Wireless USB Adapter act as a wireless AP.

👔 Intelligent 11- USB W	ireless LAN Utility	
Refresh(P) Mode(M) About(		
Construction Access Point	Veral       Profile       Available Network       Status       Statistics       Wi-Fi Protect Setup         Wi-Fi Protected Setup (WPS)         An easy and secure setup solution for Wi-Fi network         Pin Input Config (PIN)         After pushing the PIN button.Please enter the PIN code into your AP.         PIN Code :       63912111         Pin Input Config (PIN)         After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.	
	Push Button Config (PBC)	
Show Tray Icon	Disable Adapter	Close

# Soft AP mode

### <u>General</u>

8 Intelligent 11n USB Wir	eless LAN Utility 📃 🗖 🔀
Refresh(R) Mode(M) About(A)	
MyComputer Gi	eneral Advanced Statistics ICS
	SSID: softAP
	BSSID: 00:E0:4C:71:00:01 Association Table
	AID MAC Address Life Time
Show Tray Icon	Config Disable Adapter Close
General	
SSID	Shows the network name of the AP.
BSSID	Shows the MAC address of the AP.
Association Table	This table shows the connected client here.
Config	Click the Config button to set up the Wireless Network Properties.

Wireless Network Properties:
Profile Name: Aucuess Form Module
Network Name(SSID): SOTTAP
This is a computer-to-computer (ad hec) nerwork: wreless
Wireless network security
This network requires a key for the following:
Network Authentication: Open System
Data encryption: Disabled
AGCII PASSPHRÄSE
Key index (advanced):
Network key:
Casifien instrume lange
Continu reework key.
OK Cancel
<b>Network Name (SSID):</b> User can change the network name of this access
point.
<b>Channel:</b> User can select the channel form the pull-down list.
Wireless network security
<b>Network Authentication:</b> There are several types of authentication
modes including Open System Shared Key WPA-PSK and WPA2-PSK
<b>Data encryption:</b> For Open System and Shared Key authentication mode
the selection of encryption type is WEP For WDA DSK WDA2 DSK
authentiation mode the energy tion type is while from with A-1 SK, with A2-1 SK,
authentication mode, the encryption type supports both TKIP and AES.
When encountion is got to WED
when encryption is set to wEr
<b>ASCII:</b> Only valid when using WEP encryption algorithm. When key
length is set to 64 bits user can enter 5 ASCII characters (case sensitive),
and 128 bits for 13 ASCII characters (case sensitive).
PASS PHRASE: Only valid when using WEP encryption algorithm.
When key length is set to 64 bits user can enter 10 Hexadecimal characters
(0~9, a~f) and 128 bits for 26 Hexadecimal characters $(0~9, a~f)$ .
· · · · · · · · · · · · · · · · · · ·
<b>Key index (advanced):</b> Select 1~4 key index form the pull-down menu.
must match with the connected AP's key index
mast match whit the connected in 5 key index.
When encryption is set to WPA-PSK/ WPA2-PSK
The out proved by the test of the test
Network key: Enter network key at least 8 to 64 characters
THE WOLK REY. LINCE HELWOLK REY at least 0 to 04 characters.
Confirm network key: Enter network key again to confirm.

#### **Advanced**

👔 Intelligent 11n USB \	Wireless LAN Utility	
Refresh(R) Mode(M) Abou	ut(A)	
B MyComputer	General Advanced Statistics ICS	
002,111(b)g 201	General Beacon Interval	
	100	
	DTIM Period:	
	3	
	Preamble Mode	
	Long	
	Set Defaults Apply	
<u>&lt; &gt;</u>		
Show Tray Icon	Disable Adapter	Close

Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into <b>Short</b> or <b>Long</b> .
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

#### **Statistics**

👔 Intelligent 11n USB 1	/ireless LAN Utility			
MyComputer	(A) General Advanced Statis	stics ICS		
	Counter Nar Tx OK Tx Error Rx OK Rx Packet Co Rx Retry Rx ICV Error	Dunt	Value 15930 0 658 658 576 0	
Show Tray Icon	-	Disable Adapter		Close

Statistics	
Тх ОК	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

### <u>ICS</u>

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.

Intelligent 11n USB V	Vireless LAN Utility	
Refresh(R) Mode(M) About	t(A)	
MyComputer 802.11n/b/g 2cm	General Advanced Statistics ICS Setting Internet Connection Sharing (ICS)	
	Local Area Connection Realtek RTL8139 Family PCI Fast Etherr	net NIC
	Public Network	*
	Apply	
Show Tray Icon	Disable Adapter	Close

# For Windows Vista

## **Station Mode**

B Synthesis Boost Strain	General	Profile	Available N	letwork	Status	Statistics	Wi-Fi Protect Setup	
			Status:	Associa	ted			
			Speed:	Tx:150	Mbps R	x:150		
			Type:	Infrastr	ucture			
		E	ncryption:	AES				
			SSID:	Cherry				
		Signal :	Strength:					100%
		Lin	k Quality:					100%
	Netwo	ork Addı	ess: MAC Add IP Add Subnet N Gate	dress: ( lress: 1 Mask: 2 way: 1	00:E0:40 92.168. 55.255. 92.168.	::71:00:01 1.100 255.0 1.123		
					ReNev	v IP	)	

- Show Tray Icon: Check to show the wireless adapter icon at the tray.
- **Disable Adapter:** Check this to disable the wireless adapter.
- **Radio off:** Check this to turn OFF radio function.
- Close: Click to leave the Intelligent 11n USB Wireless LAN Utility.

#### **General**

The General page displays the detail information of current connection.



General Tab	
Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Туре	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the Wireless USB Adapter.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.
Renew IP	Click the <b>Renew IP</b> button to obtain IP address form the connected

gateway.

#### **Profile**

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.

MyComputer	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup			
	Available Profile(s)								
	Profil	e Name	SSID		Add				
	()) Cl	herry	Cherr		Remove				
						[	Edit		
						[	Duplicate		
							Set Default		
111 F									

Profile Tab	
Profile Name	Here shows a distinctive name of profile in this column.
SSID	The <b>SSID</b> is the unique name shared among all wireless access points in the wireless network.
Add	Click <b>Add</b> button to add a profile from the drop-down screen.

Wireless Network Properties:	
This is a computer-to-computer(ad hoc) net access points are not used.	work; wireless
Profile Name:	
Network Name(SSID):	
Channel: 1 (2412MHz) *	
Wireless network security	
This network requires a key for the following:	en Sustem
Data encryption: Dia	abled -
Data end yptorn. Dis	abled
ASCII PASSPERASE	
Kay index (advanced):	
Network key:	
Confirm network key:	
ОК	ancel
This is a computer to commute	ton (od hoo) notworks
nins is a computer-to-comput points are not used. This funct	tion is selected to enable the ad hoc
network type that computers sh	ould be setup at the same channel to
communicate to each other dire	ectly without access point, users can share
files and printers between each	PC and laptop.
Profile Name: Users can anter	profile name at will
	prome name at will.
Network Name (SSID): The S	SID is the unique network name
(case-sensitive) shared among a	all wireless access points in the wireless
network. The name must be ide	entical for all devices and wireless access
points attempting to connect to	the same network.
Channel: If set to ad hoc netwo	ork type, user can select channels form the
pull-down menu.	
Wireless network securit	tv
The second second second second	-J
Network Authentication: The	re are several types of authentication
modes including Open System,	Shared Key, WPA-PSK, WPA2-PSK,
WPA 802.1X, WPA2 802.1X a	and WEP 802.1X.
Data encryption: For Open Sys	stem, Shared Key and WEP 802.1X
authentication mode, the selecti	on of encryption type is WEP. For
WPA-PSK, WPA2-PSK, WPA	802.1X and WPA2 802.1X authentication
mode, the encryption type supp	orts dotn 1 KIP and AES.
When encryption is set to WE	ZP
ASCII: Only valid when using	
length is set to 64 bits user can	WEP encryption algorithm. When key
lengur is set to or blus user cuir t	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive),
and 128 bits for 13 ASCII chara	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive), acters (case sensitive).
and 128 bits for 13 ASCII chara PASS PHRASE: Only valid wi	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive), acters (case sensitive). hen using WEP encryption algorithm.
and 128 bits for 13 ASCII chara PASS PHRASE: Only valid wi When key length is set to 64 bit	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive), acters (case sensitive). hen using WEP encryption algorithm. as user can enter 10 Hexadecimal characters
and 128 bits for 13 ASCII chara <b>PASS PHRASE:</b> Only valid wi When key length is set to 64 bit (0~9, a~f) and 128 bits for 26 H	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive), acters (case sensitive). hen using WEP encryption algorithm. ts user can enter 10 Hexadecimal characters lexadecimal characters (0~9, a~f).
ASS PHRASE: Only valid will Vhen key length is set to 64 bit 0~9, a~f) and 128 bits for 26 H Key index (advanced): Select	WEP encryption algorithm. When key enter 5 ASCII characters (case sensitive), acters (case sensitive). hen using WEP encryption algorithm. as user can enter 10 Hexadecimal characters lexadecimal characters (0~9, a~f). 1~4 key index form the pull-down menu,

	When encryption is set to WPA-PSK/ WPA2-PSK
	Network key: Enter network key at least 8 to 64 characters.
	Confirm network key: Enter network key again to confirm.
	When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X
	When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge).
	EAP TYPE:
	• <b>TLS</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.
	• <b>LEAP:</b> Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
	• <b>TTLS</b> : Tunnelled 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.
	• <b>PEAP</b> : Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling 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.
	<ul> <li>MD5: 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:</b> This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2.
	Username: Enter the username for server.
	Identity: Enter the identity for server.
	<b>Domain:</b> Enter the domain of the network.
	<b>Password:</b> Enter the password for server.
	Ceruncate: Choose server that issuer of certificates.
Remove	Click <b>Remove</b> button to delete selected profile.
Edit	Click <b>Edit</b> button to edit selected profile.
Duplicate	Click <b>Duplicate</b> button to copy selected profile.
Set Default	Click <b>Set Default</b> button to set selected profile to be connected first.

#### **Available Network**

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate(s), and Mode.

Computer	General Profile Available Net	work Statu	s Statistics	Wi-Fi Protect Setup					
)2.11n/b/g 2c	Available Network(s)								
	SSID	Channel	Encryption	Network Authentication	Signa 🔺				
	((a) ZyXEL	1	None	Unknown	70%				
	(m) ZyXEL-1	1	None	Unknown	60%				
	(10) ZyXEL_3090_AP	3	AES	WPA2 Pre-Shared Key	44%				
	((q)) airlive	4	None	Unknown	26%				
	(69) 412	6	TKIP/AES	WPA Pre-Shared Key/	72%				
	((%)) Abocom-Wireless	6	None	Unknown	44%				
	((a)) Abocom-Wireless	6	None	Unknown	42%				
	((a) ArthurAP	6	WEP	Unknown	72% ≡				
	(@) ZyXEL_3090_62	8	AES	WPA2 Pre-Shared Key	56%				
	((p)) mina	9 TKIP	TKIP	WPA Pre-Shared Key	76%				
	(m) 3GSHARE	10	TKIP	WPA Pre-Shared Key	62%				
	GT2000Adhoc	10	None	Unknown	72%				
	((9) Untitled	10	None	Unknown	88%				
	(m) ZyXEL	10	None	Unknown	56%				
	((a)) ZyXEL	10	None	Unknown	42%				
	(tol) Abocom-Wireless	11	None	Unknown	96%				
	(M) Cherry	11	AES	WPA Pre-Shared Key/	100%				
	((p)) airlive	11	None	Unknown	48% -				
	*				+				
	Defead			Add to Profile	1				

#### Network Tab

SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Туре	Network type in use, Infrastructure or Ad-Hoc mode.

BSSID	Shows Wireless MAC address.
Supported Rate(s)	Shows the transmitting data rate.
Mode	Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.
Refresh	Click Refresh button to search and rescan the available network.
Add to Profile	Select an available network (SSID) on the list and then click Add to Profile button to add it into the profile list.
Note	Double click on item to join/create profile.

#### <u>Status</u>

This tab listed the information about the wireless USB adapter and connected access point.

MyComputer	General Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup	
₩~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~						
	М	anufacturer			Intelligent	
	N	DIS Driver Version		1084.19.1028.2009		
	SI	ort Radio Header			No	
	Er	theopticate		AES		
	A			WPA2-PSK		
	M	AC Address			00·E0·4C·71·0	0.01
	Di	ata Rate (AUTO)			Tx:150 Mbns	Rx:150 Mbns
	Ch	nannel (Frequency)			11 (2462 MHz	:)
	St	atus			Associated	
	S	SID			Cherry	
	N	etwork Type			Infrastructure	
	P	ower Save Mode			None	212
	A	sociated AP MAC			00:E0:4C:33:1	12:01
	U	o Time (hh:mm:ss)			0:16:34	
Show Tray Icon		Disal	ble Adap	ter		Close

### **Statistics**

The Statistics screen displays the statistics on the current network settings.

stresh(K) Mode(M) A	bout( <u>A</u> )				_		
O 802 11 p/b/g 2c	General Pr	ofile	Available Network	Status	Statistics	Wi-Fi Protect Setup	
002.111/0/92C							
	Counter Name Val						e
	Tx OK						7
		Tx Error 0					
		Rx C	Ж			9	9
		Rx P	acket Count			9	9
		RX R	etry V Error				/ n
		100 10	ev Ellor				<u> </u>
	-						
			ſ	_	P		
			l		Reset		
HI F							
and the second se							

Statistics			
Тх ОК	Shows information of packets successfully sent.		
Tx Error	Shows information of packets failed transmit after hitting retry limit.		
Rx OK	Shows information of packets received successfully.		
Rx Packet Count	Shows information of packets received successfully.		
Rx Retry	Shows information of packets failed transmit after hitting retry limit.		
Rx ICV Error	Shows information of packets received with ICV error.		
Reset	Click to reset counters to zero.		

#### <u>WPS</u>

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.

	Wi-Fi Protect Setup	Status Statistics	Available Network	I Profile	Gener	⊡
		p (WPS)	otected Setu	-Fi Pro	N	
	<b>Wi-Fi network</b> the PIN code into your AP	<b>IP solution for</b> on.Please enter t	and secure set t Config (PIN) shing the PIN but	An easy Pin Inpu After pu		
	620	I Code : 54285	PI			
	PIN)	Pin Input Config (				
			tton	Push Bu		
IF.	ne pnysical button on you ).	con.Please push t WPS config page	sning the PBC but sual button on the	After pu AP or vis		
	(PBC)	sh Button Config	P			
						m F
0		le Adapter	📄 Disa			<ul> <li>III →</li> <li>Show Tray Icon</li> <li>Radio Off</li> </ul>

WPS Tab				
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use " <b>Renew</b> " button to re-generate new PIN Code.			
Pin Input Config (PIN)	Click the <b>Pin Input Config</b> ( <b>PIN</b> ) button to select specific AP to process PIN Config.			
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.			

#### <u>About</u>

This page displays the information of the Wireless USB Adapter Version.



## Switch to AP Mode

To access the soft AP mode, please select the **Mode** on the function list of the Utility to make the Wireless USB Adapter act as a wireless AP.

Intelligent 11n USB Wirele	ess LAN Utility
Refresh(R) Mode(M) Ab	out(A)
Access Po	Status Status Status Status VII-H Protect Setup Status: Associated Speed: Tx:150 Mbps Rx:150 Type: Infrastructure Encryption: AES SSID: Cherry Signal Strength: 100%
	Link Quality: 100% Network Address: MAC Address: 00:E0:4C:71:00:01 IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Gateway: 192.168.1.123
✓ TTT → ↓ ✓ Show Tray Icon ■ Radio Off	ReNew IP

## Soft AP mode

#### <u>General</u>

Intelligent 11n USB Wirele	ess LAN Utility				
MyComputer	General Advanced Statistics ICS				
	BSSID: 00:E0:4C:71:00:01 Association Table				
	AID MAC Address Life Time				
	Config				
<ul> <li>III → </li> <li>Show Tray Icon</li> <li>Radio Off</li> </ul>	Disable Adapter	Close			
General					
SSID	Shows the network name of the AP.				
BSSID	Shows the MAC address of the AP.				
Association Table	This table shows the connected client here.				
Config	Click the Config button to set up the Wireless Network Pr	operties.			

Wireless Network Prop	erties:		
This is a computer-t	o-computer(ad hoc) network; i	Wireless	
Profile Name:	Access Point Mode		
Network Name(SSID):	Cherry-PC_AP	_	
Channel:	1 (2412MHz) 🔻		
Wireless network sec	urity		
This network requires	ork Authentication: Open Sys	tem 💌	
	Data encryption: Disabled	-	
ASCII PAS	SPHRASE		
Key index (advanced) Network key: Confirm network key:	)r 1		
Channel: User c Wireless netv Network Authe	an select the chann work security ntication: There ar	el form the pull	-down list.
Data encryption he selection of e	For Open System, Sna r: For Open System encryption type is W ode, the encryption	and Shared Ke /EP. For WPA- type supports b	y authentication mode, PSK, WPA2-PSK, poth TKIP and AES.
When encryptic	on is set to WEP		
ASCII: Only val ength is set to 64 and 128 bits for	lid when using WE 4 bits user can enter 13 ASCII character	P encryption alg 5 ASCII chara s (case sensitive	gorithm. When key cters (case sensitive), e).
PASS PHRASE When key length 0~9, a~f) and 12	• Only valid when to a is set to 64 bits use 28 bits for 26 Hexae	using WEP encr er can enter 10 l decimal characte	yption algorithm. Hexadecimal characters ers (0~9, a~f).
Key index (adva nust match with	anced): Select 1~4 the connected AP'	key index form s key index.	the pull-down menu,
When encryptio	on is set to WPA-P	SK/ WPA2-PS	К
		1 . 0	
Network key: E	inter network key at	t least 8 to 64 cl	naracters.
onfirm netwoi	rk key: Enter netwo	ork key again to	confirm.

#### **Advanced**

Refresh( <u>R</u> ) Mode( <u>M</u> ) A	pout( <u>A</u> )	
MyComputer	General Advanced Statistics ICS General Beacon Interval DTIM Period: 3 Preamble Mode Short  Stort Set Defaults	Арріу
III     F     Show Tray Icon     Radia Off	Disable Adapter	Close

Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into <b>Short</b> or <b>Long</b> .
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

#### **Statistics**

Refresh( <u>R</u> ) Mode( <u>M</u> ) About(	<u>A</u> )	
Brite Strain Str	eral Advanced Statistics ICS	
	Counter Name	Value
	Tx OK	3436
	Tx Error	0
	Rx OK	218
	Rx Packet Count	218
	Ry ICV Error	208
	Reset	
Show Tray Icon Radio Off	Disable Adapter	Close

#### **Statistics**

Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

### <u>ICS</u>

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.

ce (Personal Area Network) #2 PCI Fast Ethernet Adapter
ce (Personal Area Network) #2 PCI Fast Ethernet Adapter
ce (Personal Area Network) #2 PCI Fast Ethernet Adapter
ast Ethernet Adapter
ast Ethernet Adapter
ast Ethernet Adapter

# For Windows 7

## **Station Mode**

efresh( <u>R</u> ) Mode( <u>M</u> ) A	bout( <u>A</u> )					_		
MyComputer	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup	_	
802.11n/b/g 2c								
			Speed: Tx:150	Mbps R	x:150			
			Type: Infrastr	ucture				
		E	ncryption: AES					
			SSID: Cherry					
		Signal	Strength:				92%	
		Lin	k Quality:				99%	
			. Constr.					
	Nation							
	Netwo	ork Add	MAC Address: r	0:E0:40	.71:00:01			
	IP Address: 192.168.1.102							
	Subnet Mask: 255.255.255.0							
			Gateway: 1	32.168.	1.123			
			[	ReNev	w IP	1		
111 1								

- Show Tray Icon: Check to show the wireless adapter icon at the tray.
- **Disable Adapter:** Check this to disable the wireless adapter.
- **Radio off:** Check this to turn OFF radio function.
- Close: Click to leave the Intelligent 11n USB Wireless LAN Utility.

#### **General**

- - × Intelligent 11n USB Wireless LAN Utility Refresh(R) Mode(M) About(A) General Profile Available Network Status Statistics Wi-Fi Protect Setup 802.11n/b/g 2c Status: Associated Speed: Tx:150 Mbps Rx:150 Type: Infrastructure Encryption: AES SSID: Cherry Signal Strength: 92% Link Quality: 99% Network Address: MAC Address: 00:E0:4C:71:00:01 IP Address: 192.168.1.102 Subnet Mask: 255.255.255.0 Gateway: 192.168.1.123 ReNew IP \* III ÷ Show Tray Icon Disable Adapter Close Radio Off

The General page displays the detail information of current connection.

Conorol Toh	
General Tab	
Status	Shows the current connected status. If there is no connection, it will show Not Associated. If been connected, the system will show Associated. When connecting, the system will show checking Status.
Speed	Shows the current transmitting rate and receiving rate.
Туре	Network type in use, Infrastructure or Ad-Hoc.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
SSID	Shows the connected access point network name.
Signal Strength	Shows the receiving signal strength.
Link Quality	Shows the connection quality based on signal strength.
MAC Address	The physical address of the Wireless USB Adapter.
IP Address	Shows the IP address information.
Subnet Mask	Shows the Subnet Mask information.
Gateway	Shows the default gateway IP address.

Renew IP	Click the	Renew	IP	button	to	obtain	IP	address	form	the	connected
	gateway.										

#### **Profile**

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, Remove, Edit, Duplicate** and **Set Default** profiles.

fresh( <u>R</u> ) Mode( <u>M</u> ) Al	out( <u>A</u> )	-								
MyComputer	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup				
	Available Profile(s)									
	Profil	e Name	SSID		Add					
	(m) cl	nerry	Cherr	Remove						
							Edit			
							Duplicate			
							Set Default			
			ìn		ŀ					
III +				ble Ada	oter					

Profile Tab	
Profile Name	Here shows a distinctive name of profile in this column.
SSID	The <b>SSID</b> is the unique name shared among all wireless access points in the wireless network.
Add	Click <b>Add</b> button to add a profile from the drop-down screen.

Wireless Network Properties:
This is a computer-to-computer (ad hoc) network; wireless access points are not used.
Profile Name:
Network Name(SSID):
Channel: 1 (2412MHz) +
Wireless network security This network requires a key for the following:
Network Authentication: Open System 🔻
Data encryption: Disabled 👻
Key index (advanced):
Confirm network key:
This is a computer-to-computer (ad hoc) network: wireless access
<b>points are not used:</b> This function is selected to enable the ad hoc
network type that computers should be setup at the same channel to
communicate to each other directly without access point, users can share files and printers between each PC and lapton
Thes and printers between each r C and raptop.
Profile Name: Users can enter profile name at will.
Network Name (SSID): The SSID is the unique network name
(case-sensitive) shared among all wireless access points in the wireless
network. The name must be identical for all devices and wireless access
points attempting to connect to the same network.
<b>Channel:</b> If set to ad hoc network type, user can select channels form the
pull-down menu.
Wireless network security
<b>Network Authentication:</b> There are several types of authentication
modes including Open System, Shared Key, WPA-PSK, WPA2-PSK,
WPA 802.1X, WPA2 802.1X and WEP 802.1X.
Data encryption: For Open System, Shared Key and WEP 802.1X
authentication mode, the selection of encryption type is WEP. For
WPA-PSK, WPA2-PSK, WPA 802.1X and WPA2 802.1X authentication mode, the encryption type supports both TKIP and AES
mode, the encryption type supports obtain <b>TKIF</b> and <b>AES</b> .
When encryption is set to WEP
<b>ASCII:</b> Only valid when using WEP encryption algorithm. When key
<b>ASCII:</b> Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive),
<b>ASCII:</b> Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).
<ul><li>ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).</li><li>PASS PHRASE: Only valid when using WEP encryption algorithm.</li></ul>
<ul> <li>ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).</li> <li>PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0.0, a. 6) and 128 bits for 26 Unreds along the user (0.0, a. 6).</li> </ul>
<ul> <li>ASCII: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 5 ASCII characters (case sensitive), and 128 bits for 13 ASCII characters (case sensitive).</li> <li>PASS PHRASE: Only valid when using WEP encryption algorithm. When key length is set to 64 bits user can enter 10 Hexadecimal characters (0~9, a~f) and 128 bits for 26 Hexadecimal characters (0~9, a~f).</li> </ul>

	When encryption is set to WPA-PSK/ WPA2-PSK
	Network key: Enter network key at least 8 to 64 characters.
	Confirm network key: Enter network key again to confirm.
	When encryption is set to WPA 802.1X/ WPA2 802.1X/ WEP 802.1X
	When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge).
	EAP TYPE:
	• <b>TLS</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.
	• <b>LEAP:</b> Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
	• <b>TTLS</b> : Tunnelled 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.
	• <b>PEAP</b> : Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling 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.
	<ul> <li>MD5: 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:</b> This is enabled under TTLS and PEAP type. For TTLS, the selections of tunnel are CHAP, MSCHAP, MSCHAP-V2, PAP. For PEAP, the selections of tunnel are MD5, GTC, TLS and MSCHAP-V2.
	Username: Enter the username for server.
	Identity: Enter the identity for server.
	<b>Domain:</b> Enter the domain of the network.
	<b>Password:</b> Enter the password for server.
	Ceruncate: Choose server that issuer of certificates.
Remove	Click <b>Remove</b> button to delete selected profile.
Edit	Click <b>Edit</b> button to edit selected profile.
Duplicate	Click <b>Duplicate</b> button to copy selected profile.
Set Default	Click <b>Set Default</b> button to set selected profile to be connected first.

#### **Available Network**

This page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Channel, Encryption, Network Authentication, Signal, Type, BSSID, Supported Rate(s), and Mode.

esh( <u>R</u> ) Mode( <u>M</u> ) A	bout( <u>A</u> )									
MyComputer	General Profile Available Netwo	ork Statu	s Statistics	Wi-Fi Protect Setup						
802.11n/b/g 2c	Available Network(s)									
	SSID	Channel	Encryption	Network Authentication	Signa 🔺					
	[[m]] ZyXEL	1	None	Unknown	58%					
	(19) ZyXEL_3090_AP	3	AES	WPA2 Pre-Shared Key	60%					
	(🗐 SSID-00c473db	5	None	Unknown	92%					
	((a)) 412	6	TKIP/AES	WPA Pre-Shared Key/	60%					
	((m) AIR3G_DEMO	6	None	Unknown	76%					
	((a)) Abocom-Wireless	6	None	Unknown	48%					
	((9)] ArthurAP	6	WEP	Unknown	56% _					
	(19) 3GDEMO_WR5204U	7	AES	WPA Pre-Shared Key	58%					
	[[9] ZyXEL_3090	8	AES	WPA2 Pre-Shared Key	58%					
	((q)) mina	9	TKIP	WPA Pre-Shared Key	100%					
	((9) 3GSHARE	10	TKIP	WPA Pre-Shared Key	62%					
	((a)) Untitled	10	None	Unknown	92%					
	((9) Abocom-Wireless	11	None	Unknown	92%					
	(P) Cherry	11	AES	WPA Pre-Shared Key/	62%					
	((a) ZyXEL	11	None	Unknown	74%					
	((q)) airlive	11	None	Unknown	76%					
	[(9)] x1	11	None	Unknown	26%					
	((a)) x2	11	None	Unknown	42% =					
	·				*					
	Refresh			Add to Profile						
	Note Double click on item to	join/crea	ite profile.							
111. F			_							

#### Network Tab

SSID	Shows the network name of the access points.
Channel	Shows the currently channel in use.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, None and TKIP/AES.
Network Authentication	Show the device network authentication.
Signal	Shows transmit power, the amount of power used by a radio transceiver to send the signal out.
Туре	Network type in use, Infrastructure or Ad-Hoc mode.

BSSID	Shows Wireless MAC address.		
Supported Rate(s)	Shows the transmitting data rate.		
Mode	Supported wireless mode. It may support 802.11b, 802.11g and 802.11n wireless mode.		
Refresh	Click Refresh button to search and rescan the available network.		
Add to Profile	Select an available network (SSID) on the list and then click Add to Profile button to add it into the profile list.		
Note	Double click on item to join/create profile.		

#### <u>Status</u>

This tab listed the information about the wireless USB adapter and connected access point.

Refresh(R) Mode(M) Al	bout( <u>A</u> )					
By MyComputer Building 2c Building 2c	General	Profile	Available Network	Status	Statistics	Wi-Fi Protect Setup
		Ma NE Sh En Au Ch Da Ch St SS Ne Po As Up	Inufacturer DIS Driver Version ort Radio Header cryption Ithenticate annel Set AC Address ta Rate (AUTO) annel (Frequency atus ID stwork Type wer Save Mode sociated AP MAC o Time (hh:mm:ss)	)		Intelligent 1086.5.1111.2009 No AES WPA2-PSK FCC 00:E0:4C:71:00:01 Tx:120 Mbps Rx:120 Mbps 11 (2462 MHz) Associated Cherry Infrastructure None 00:E0:4C:33:12:01 0:22:28
<ul> <li>III →</li> <li>Show Tray Icon</li> </ul>			Disa	ble Ada	pter	Close

### **Statistics**

The Statistics screen displays the statistics on the current network settings.

fresh( <u>R</u> ) Mode( <u>M</u> ) A	bout( <u>A</u> )				
MyComputer	General Profil	e Available Network Status	Statistics Wi-Fi Protect Setup		
002.11h/b/g.2c					
	C	ounter Name	v	alue	
	T	( OK		250	
	T	Error		0	
	R	Rx OK			
	R	Packet Count		52	
	R	ICV Error		0	
		LICY END			
		-			
			Reset		
Chow Troy Icon		Dirable Ada	ator		
ALCON VELLAV ICOL		USdue Aud			

Statistics			
Тх ОК	Shows information of packets successfully sent.		
Tx Error	Shows information of packets failed transmit after hitting retry limit.		
Rx OK	Shows information of packets received successfully.		
Rx Packet Count	Shows information of packets received successfully.		
Rx Retry	Shows information of packets failed transmit after hitting retry limit.		
Rx ICV Error	Shows information of packets received with ICV error.		
Reset	Click to reset counters to zero.		

#### <u>WPS</u>

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.

fresh( <u>R</u> ) Mode( <u>M</u> )	About( <u>A</u> )				
MyComputer	General Profile Available Network Status Statistics Wi-Fi Protect Setup				
	Wi-Fi Protected Setup (WPS)				
	An easy and secure setup solution for Wi-Fi network				
	Pin Input Config (PIN) After puebing the DIN button Please enter the DIN code into your AP				
	PIN Code: 43022793				
	Pin Input Config (PIN)				
	Push Button				
	After pushing the PBC button.Please push the physical button on your				
	AP or visual button on the WPS config page.				
	Push Button Config (PBC)				
111 1					
Show Tray Icon	Disable Adapter				
Padia Off					

WPS Tab			
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use " <b>Renew</b> " button to re-generate new PIN Code.		
Pin Input Config (PIN)	Click the <b>Pin Input Config</b> ( <b>PIN</b> ) button to select specific AP to process PIN Config.		
Push Button Config (PBC)	Click this button to connect with AP that supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.		

#### <u>About</u>

This page displays the information of the Wireless USB Adapter Version.



## Switch to AP Mode

To access the soft AP mode, please select the **Mode** on the function list of the Utility to make the Wireless USB Adapter act as a wireless AP.



## Soft AP mode

#### <u>General</u>

Intelligent 11n USB Win	eless LAN Utility	
Refresh( <u>R</u> ) Mode( <u>M</u> ) A	bout( <u>A</u> )	
MyComputer 802.11n/b/g 2c	General Advanced Statistics ICS SSID: Abocom-PC_AP BSSID: 00:E0:4C:71:00:01 Association Table	
	AID MAC Address Life Time	
	Config	
<ul> <li>Show Tray Icon</li> <li>Radio Off</li> </ul>	Disable Adapter Close	
General		
SSID	Shows the network name of the AP.	
BSSID	Shows the MAC address of the AP.	
Association Table	This table shows the connected client here.	
Config Click the Config button to set up the Wireless Network Properties		

- This is a computer-to-computer(ad boc) potworks a	
access points are not used	ireless
Profile Name: Access Point Mode	
Network Name(SSID): Abocom-PC_AP	
Channel: 1 (2412MHz) V	
Wireless network security	
This network requires a key for the following:	
Network Authentication: Open Syst	em 🔻
Data encryption: Disabled	•
ASCII	
Key index (advanced):	
Network key:	
Confirm network key:	
construction Rey :	
	-
OK <u>C</u> ancel	
Network Authentication: There are nodes including Open System, Share Data encryption: For Open System a ne selection of encryption type is Wi uthentication mode, the encryption t	several types of authentication ed Key, WPA-PSK and WPA2-PSK. and Shared Key authentication mode, EP. For WPA-PSK, WPA2-PSK, ype supports both TKIP and AFS
unentreation mode, the eneryption (	spe supports cour rith and riths.
hen encryption is set to WEP	
When encryption is set to WEP SCII: Only valid when using WEP ength is set to 64 bits user can enter nd 128 bits for 13 ASCII characters	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive).
Vhen encryption is set to WEP SCII: Only valid when using WEP ength is set to 64 bits user can enter nd 128 bits for 13 ASCII characters PASS PHRASE: Only valid when us Vhen key length is set to 64 bits user 0~9, a~f) and 128 bits for 26 Hexado	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive). sing WEP encryption algorithm. can enter 10 Hexadecimal characters ecimal characters (0~9, a~f).
Vhen encryption is set to WEP SCII: Only valid when using WEP ength is set to 64 bits user can enter nd 128 bits for 13 ASCII characters CASS PHRASE: Only valid when us When key length is set to 64 bits user D~9, a~f) and 128 bits for 26 Hexade Key index (advanced): Select 1~4 k nust match with the connected AP's	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive). sing WEP encryption algorithm. can enter 10 Hexadecimal characters ecimal characters (0~9, a~f). ey index form the pull-down menu, key index.
Vhen encryption is set to WEP SCII: Only valid when using WEP ength is set to 64 bits user can enter nd 128 bits for 13 ASCII characters PASS PHRASE: Only valid when us Vhen key length is set to 64 bits user D~9, a~f) and 128 bits for 26 Hexade Cey index (advanced): Select 1~4 k nust match with the connected AP's Vhen encryption is set to WPA-PS	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive). sing WEP encryption algorithm. can enter 10 Hexadecimal characters ecimal characters (0~9, a~f). ey index form the pull-down menu, key index. <b>K/ WPA2-PSK</b>
hen encryption is set to WEP SCII: Only valid when using WEP agth is set to 64 bits user can enter d 128 bits for 13 ASCII characters ASS PHRASE: Only valid when us hen key length is set to 64 bits user -9, a~f) and 128 bits for 26 Hexado ey index (advanced): Select 1~4 k ist match with the connected AP's hen encryption is set to WPA-PS	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive). sing WEP encryption algorithm. can enter 10 Hexadecimal characters ecimal characters (0~9, a~f). ey index form the pull-down menu, key index. <b>K/ WPA2-PSK</b> least 8 to 64 characters.
<b>cII:</b> Only valid when using WEP gth is set to 64 bits user can enter 128 bits for 13 ASCII characters <b>SS PHRASE:</b> Only valid when using ten key length is set to 64 bits user 9, a~f) and 128 bits for 26 Hexado <b>y index (advanced):</b> Select 1~4 k st match with the connected AP's <b>ten encryption is set to WPA-PS</b> <b>twork key:</b> Enter network key at	encryption algorithm. When key 5 ASCII characters (case sensitive), (case sensitive). sing WEP encryption algorithm. can enter 10 Hexadecimal characters ecimal characters (0~9, a~f). ey index form the pull-down menu, key index. <b>K/WPA2-PSK</b> least 8 to 64 characters.

#### **Advanced**

efresh( <u>R</u> ) Mode( <u>M</u> ) A	out( <u>A</u> )
	General Advanced Statistics ICS General Beacon Interval 100
	DTIM Period:
	3 Preamble Mode
	Long
	Set Defaults Apply
111 +	

Advanced	
Beacon Interval	The time between two beacons. (The system default is 100 ms.)
DTIM Period	The delivery traffic indication message (DTIM) is an element included in some beacon frames. User can specify a value from 1 to 255 beacons.
Preamble	Select from the pull-down menu to change the Preamble type into <b>Short</b> or <b>Long</b> .
Set Defaults	Click to use the system default value.
Apply	Click to apply the above settings.

#### **Statistics**

include into a company	bout( <u>A</u> )	
By Computer By Bog 2c By Bog 2c	General Advanced Statistics ICS	
	Counter Name	Value
	Tx OK	785
	Tx Error	0
	Rx OK	136
	Rx Packet Count	136
	Rx Retry	123
	Reset	

#### **Statistics**

Tx OK	Shows information of packets successfully sent.
Tx Error	Shows information of packets failed transmit after hitting retry limit.
Rx OK	Shows information of packets received successfully.
Rx Packet Count	Shows information of packets received successfully.
Rx Retry	Shows information of packets failed transmit after hitting retry limit.
Rx ICV Error	Shows information of packets received with ICV error.
Reset	Click to reset counters to zero.

### <u>ICS</u>

This page displays setting Internet connection sharing (ICS). Select a sharing public network and click Apply button to make a connection.

erresn(K) Wode(M) A	bout( <u>A</u> )
ByComputer Boot State Boot St	General Advanced Statistics ICS
	Setting Internet Connection Sharing (ICS)
	ConnName Device Name
	Elecal Area Connection Atheros L1 Gigabit Ethernet 10/100/1000Base-T Con
	4 ¥
	Public Network
	Apply

# **Chapter 5: Uninstall**

# For Windows 2000/XP

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

1. Go to Start →All Programs →Intelligent Wireless Utility→ Uninstall –Intelligent.



2. Click **Yes** to completely remove the selected application and all of its features.



3. Then click **Finish** to complete uninstall.



# For Windows Vista

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

1. Go to Start → Programs →Intelligent Wireless LAN Utility→ Uninstall –Intelligent.



2. Click **Yes** to complete remove the selected application and all of its features.

![](_page_66_Picture_5.jpeg)

3. Finally, click **Finish** to complete uninstall.

![](_page_67_Picture_1.jpeg)

# For Windows 7

To remove the utility and driver, please refer to below steps. (When removing the utility, the driver will be removed as well.)

1. Go to Start → Programs →Intelligent Wireless Utility→ Uninstall –Intelligent.

![](_page_68_Picture_3.jpeg)

2. Click **Yes** to complete remove the selected application and all of its features.

![](_page_69_Picture_1.jpeg)

3. Finally, click **Finish** to complete uninstall.

![](_page_69_Picture_3.jpeg)