802.11 b/g/n

Micro Mini Wireless LAN

USB2.0 Adapter

User's Manual

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

Country Code Statement

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

To maintain compliance with FCC RF exposure requirements, use only belt-clips, holsters or similar accessories that do not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

CAUTION:

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

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. This equipment should be installed and operated with minimum distance 2.5cm between the radiator & your body.

CE Statement:

Hereby, AboCom, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Driective 1999/5/EC.

1	Model Name: WU5205
1	Trade Name: AboCom
5	FC CE ①
1	FCC ID : MQ4WU520
1	Made in TA/WAN





Trade Mark: AboCom

Table of Contents

INTRODUCTION1
Features1
Windows 2000/XP Installation2
INSTALL THE SOFTWARE
INSTALL THE HARDWARE
Windows Vista Installation
INSTALL THE SOFTWARE
INSTALL THE HARDWARE
VERIFICATION
NETWORK CONNECTION9
IP Address9
IP Address
UTILITY CONFIGURATION FOR WINDOWS 2000/XP10
UTILITY CONFIGURATION FOR WINDOWS 2000/XP10 STATION MODE
UTILITY CONFIGURATION FOR WINDOWS 2000/XP
UTILITY CONFIGURATION FOR WINDOWS 2000/XP
UTILITY CONFIGURATION FOR WINDOWS 2000/XP

WPS
Radio On/Off
About
UTILITY MENU LIST
SOFT AP MODE
Config
Access Control
MAC Table40
Event Log41
Statistics
About
UTILITY CONFIGURATION FOR WINDOWS VISTA
STATION MODE
STATION MODE

Soft A	AP MODE	68
	Config	68
	Access Control	71
	MAC Table	72
	Event Log	73
	Statistics	74
	About	75
UNINST	ALLATION FOR WINDOWS 2000/XP	76
UNINST	ALLATION FOR WINDOWS VISTA	78

INTRODUCTION

The **WU5205** is an IEEE802.11b/g/n USB adapter that connects your notebook to a wireless local area. The **WU5205** fully complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance.

The **WU5205** is a very small adapter that can connects notebook, handheld or desktop computer equipped with USB interface for wireless network applications. It allows you to take full advantage of your notebook's mobility with access to real-time information and online services anytime and anywhere.

Features

- > 1T1R Mode with 150Mbps PHY Rate for both.
- > Complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards.
- > Supports WEP 64/128, WPA, WPA2.
- > Supports WMM and WMM-PS.
- > Supports WPS configuration.
- > Supports USB 2.0/1.1 interface.
- > Portable and mini-size design.
- > Compatible with Microsoft Windows Vista, XP, 2000.

- 1 -

Windows 2000/XP Installation

Install the Software

Caution:

Do not insert the wireless card into your computer until the InstallShield Wizard finish installing.

- 1. Exit all Windows programs. Insert the included CD-ROM into your computer. The CD-ROM will run automatically.
- 2. When the License Agreement screen appears, please read the contents and select "I accept the terms of the license agreement " then click Next to continue.

License Agreement Please read the following lice	ise agreement carefully.
	SOFTWARE PRODUCT LICENSE The SOFTWARE PRODUCT increases The SOFTWARE PRODUCT increases The SOFTWARE PRODUCT increases and international copyright teating, as well as other intellectual property laws and treates. The SOFTWARE PRODUCT is increased, not soid. Software PRODUCT. Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT. provided that each copy shall be a true and complete tor included with your own product. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on Reverse Engineering. Decompilation, and Distributed as a standalone product or included with your own product. Methods of the SOFTWARE PRODUCT is a standalone product or included with your own product. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on Reverse Engineering. Decompilation, and Distributed as a not reverse Compared and the terms of the locense agreement I do not accept the terms of the locense agreement
InstallShield	< Back Next > Cancel

- 2 -

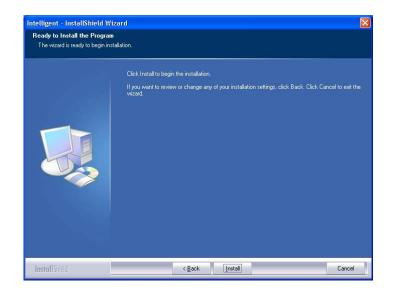
- 3. Select the check box to choose a **Configuration Tool** from the listed two choices.
 - **Configuration Tool**: Choose to use our configuration utility.
 - Microsoft Zero Configuration Tool: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU).

Click Next to continue.

Intelligent - InstallShield W	izard	×
Setup Type Select the setup type that best	suits your needs.	
	Select Configuration Tool	
	 Configuration Tool 	
	Microsoft Zero Configuration Tool	
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel	

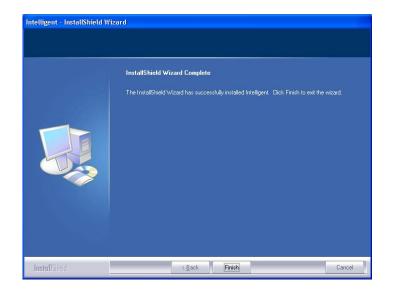
5. When you are prompted the following message, please click **Install** to begin the installation.

- 3 -



6. When the following screen appears, click **Finish** to complete the software installation.

- 4 -



Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

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

- 5 -

Windows Vista Installation

Install the Software

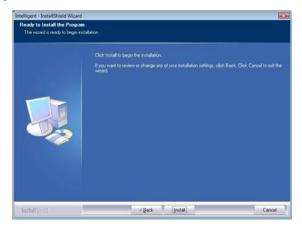
Do not insert the wireless LAN adapter into your computer until the procedures in "Driver& Utility Installation" have been performed.

- 1. Insert the included CD-ROM into the CD-ROM drive of your computer.
- 2. When the Main Menu screen appears, click "Driver & Utility Installation" to start the software installation.
- 3. When the License Agreement screen appears, please read the contents and select "I accept the terms of the license agreement " then click Next to continue.

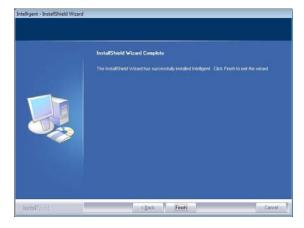


- 6 -

4. When you are prompted the following message, please click **Install** to begin the installation.



5. When the following screen appears, click **Finish** to complete the software installation.



- 7 -

Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

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

Verification

To verify if the device exists in your computer and is enabled, go to **Start** > **Control Panel** > **System** > **Hardware** > **Device Manager**. Expand the **Network Adapters** category. If the **802.11 USB Wireless LAN Card** is listed here, it means that your device is properly installed and enabled.

🖴 Device Manager	
File Action View Help	
Batteries Computer	^
B ← Disk drives Display adapters B ← Dis ATA/ATAPI controllers Di ← ↓ EEE 1394 Bus host controllers	
 Infrared devices Intel ALM 3.0 Codec Keyboards ™ Mice and other pointing devices 	
Mondems Monitors Metwork adapters Monitors	
B 802.11 USB Wireless LAN Card Wireless LAN Card Wireless LAN Card Wireless Ca	
Cher devices Cher devices PCMCIA adapters Cher devices Cher devices Cher devices Cher devices Cher devices Cher devices C	~

- 8 -

NETWORK CONNECTION

IP Address

Note: When assigning IP Addresses to the computers on the network, remember to have the IP address for each computer set on the same subnet mask. If your Broadband Router use DHCP technology, however, it won't be necessary for you to assign Static IP Address for your computer.

- 1. To configure a dynamic IP address (i.e. if your broadband Router has the DHCP technology), check the **Obtain an IP Address Automatically** option.
- To configure a fixed IP address (if you broadband Router is not DHCP supported, or when you need to assign a static IP address), check the Use the following IP address option. Then, enter an IP address into the empty field; for example, enter *192.168.1.1* in the IP address field, and *255.255.255.0* for the Subnet Mask.

Internet Protocol (TCP/IP) Properties	Internet Protocol (TCP/IP) Properties
General Alternate Configuration	General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
O Dbtain an IP address automatically	Obtain an P address automatically
Use the following IF address:	Use the following IP address:
IP address:	IP address: 192 . 168 . 1 . 1
Subnet mask:	Subnet mask: 255 . 255 . 0
Default gateway:	Default gave more .
 Obtain DNS server address automatically 	Obtain DNS server address automatically
O Use the following DNS server addresses:	O Use the following DNS server addresses:
Preferred DNS server:	Preferred DNS server:
Alternate DNS server:	Alternate DNS server:
Advanced	Advanced
OK Cancel	DK Cancel

- 9 -

UTILITY CONFIGURATION FOR WINDOWS 2000/XP

After the Wireless adapter has been successfully installed, users can use the included Configuration Utility to set their preference.

Go to Start→ (All) Program→ Intelligent Wireless→ Intelligent Wireless Utility.



You can also open the Configuration Utility by double clicking the icon or right clicking to select **Launch Config Utility**.

Launch Config Utility
Use Zero Configuration as Configuration Utility
Switch to AP Mode
Exit

- 10 -



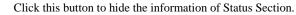
Notice: Under screen resolution 800 x 600 pixels, click the triangle button at the right down corner of the utility to expand the information of the station, the information will not be displayed completely.

Profile

Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. The Profile manager enables you to **Add**, **Edit**, **Delete** and **Activate** profiles.



Click this button to show the information of Status Section.



í In	elligent Wirele	ess Utiltiy							
	Profile	Network	Advanced	Statistics	Gos WMM	Ø WPS	Radio On/Off	About	
		Pro	file List						
P	ROF1	Cherry_test_	11n_Router		5	Profile Name >	> PROF1		
						SSID >	> Cherry_test_11n_Ro	uter	
						Network Type >	> Infrastructure		
						Authentication >	> Open		
						Encryption >	> None		
						Use 802.1x >	> NO		
						Tx Power >	>> Auto		
						Channel >	> Auto		
					P	ower Save Mode >			
						RTS Threshold >	> 2347		-
	Add	Edit	Delete	Activat	e Frag	gment Threshold >	> 2346	(

Profile Tab	
Profile Name	You can see a distinctive name of profile in this column. The default is PROF# (# 1, #2, #3)
SSID	The SSID is the unique name shared among all points in your wireless network.

- 11 -

Network Type	Shows the network type of the device, including					
	Infrastructure and Ad-Hoc.					
Authentication	Shows the authentication mode.					
Encryption	Shows the encryption type.					
Use 802.1x	Whether or not use 802.1x feature.					
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.					
Channel	Shows the selected channel that is currently in use.					
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)					
RTS Threshold	Shows the RTS Threshold of the device.					
Fragment Threshold	Shows the Fragment Threshold of the device.					
Add	Shows the Fragment Threshold of the device. Click to add a profile from the drop-down screen. System Configuration tab:					

- 12 -

SSID : The SSID is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network. User can use pull-down menu to select from available APs.
 Power Save Mode: CAM (Constantly Awake Mode): When this mode is selected, the power supply will be normally provided even when there is no throughput. PSM (Power Saving Mode): When this mode is selected, this device will stay in power saving mode even when there is high volume of throughput.
Network Type : There are two types, Infrastructure and Ad-hoc modes. Under Ad-hoc mode user can also choose the preamble type, the available preamble type includes Auto and Long . In addition to that, the channel field will be available for setup in Ad-hoc mode.
• The Infrastructure is intended for the connection between wireless network cards and an Access Point. With the wireless adapter, you can connect wireless LAN to a wired global network via an Access Point.
• The Ad-hoc lets you set a small wireless workgroup easily and quickly. Equipped with the wireless adapter, you can share files and printers between each PC and laptop.
Tx Power : Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including Auto , 100%, 75%, 50%, 25%, 10% and Lowest.
Preamble : This function will show up when Ad-hoc network type be selected. A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. Select from the pull-down menu to change the

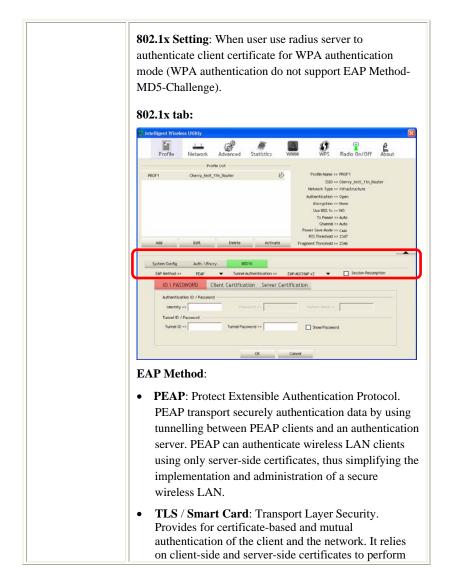
- 13 -

Preamble type into Auto or Long.
RTS Threshold : User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347. RTS/CTS Threshold is a mechanism implemented to prevent the " Hidden Node " problem. If the "Hidden Node" problem is an issue, users have to specify the packet size. <u>The RTS/CTS mechanism will be</u> activated if the data size exceeds the value you set.
This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Fragment Threshold : User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346. The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If your Wireless LAN Adapter often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.
Authentication and Security tab:
System Config Authoritocution >> Copen Encryption >> None ID02: 1X WTRA Produced Key >>
Kinifi Heradooled



need to be set to the same authentication type.
• Shared : Shared key is when both the sender and the recipient share a secret key.
• LEAP: 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 (only with CCX mode enabled.)
• WPA/ WPA-PSK/ WPA2/ WPA2-PSK: WPA or WPA-PSK authentications offer two encryption methods, TKIP and AES. For WPA-PSK, select the type of algorithm TKIP or AES and then enter a WPA Shared Key of 8-64 characters in the WPA Pre-shared Key field.
Encryption Type: For Open and Shared authentication mode, the selection of encryption type are None and WEP . For WPA , WPA2 , WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES .
WPA Pre-shared Key : This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.
WEP Key : Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.
 Hexadecimal (128bits): 26 Hex characters (0~9, a~f). ASCII (128bits): 13 ASCII characters.
Show Password : Check this box to show the password you en02tered.

- 15 -





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.	
• TTLS : 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.	l
• EAP-FAST : Flexible Authentication via Secure Tunnelling. 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. For tunnel authentication, only support "Generic Token Card" authentication now.	
• MD5-Challenge : Message Digest Challenge Challenge is an EAP authentication type that provide base-level EAP support. It provides for only one-wa authentication - there is no mutual authentication of wireless client and the network. (Only Open an Shared authentication mode can use this function.)	es y of
 Tunnel Authentication: Protocol: Tunnel protocol, List information including EAP-MSCHAP v2, EAP-TLS/ Smart Card, and Generic Token Card. 	r
• Tunnel Identity : Identity for tunnel.	

- 17 -

• Tunnel Password: Password for tunnel.
Session Resumption : Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. User can click the box to enable or disable this function.
ID\PASSWORD tab:
<form></form>
Friendy name
Use Client certificate: Choose to enable server

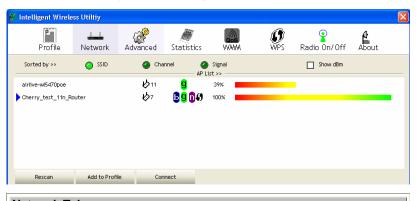
- 18 -

	authentication.				
	OK : Click to save settings and exit this page. Cancel: Click to call off the settings and exit.				
	Server Certification tab:				
	System Config Auth. LEncry, 802194				
	EVP Methods >> PDVP				
	Use certificate chain				
	OK Canon				
	certificates.				
	certificates. Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.				
	Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the				
	Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.				
	 Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. Server name: Enter an authentication sever root. Server name must match: Click to enable or disable this 				
	 Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. Server name: Enter an authentication sever root. Server name must match: Click to enable or disable this function. Domain name must end in specified name: Click to 				
	 Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. Server name: Enter an authentication sever root. Server name must match: Click to enable or disable this function. Domain name must end in specified name: Click to enable or disable this function. 				
Delete	 Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. Server name: Enter an authentication sever root. Server name must match: Click to enable or disable this function. Domain name must end in specified name: Click to enable or disable this function. OK: Click to save settings and exit this page. 				
Delete Edit	 Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field. Server name: Enter an authentication sever root. Server name must match: Click to enable or disable this function. Domain name must end in specified name: Click to enable or disable this function. OK: Click to save settings and exit this page. Cancel: Click call off the settings and exit. 				

- 19 -

Network

The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.



Network Tab			
Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.		
Show dBm	Check the box to show the dBm of the AP list.		
SSID	Shows the name of BSS network.		
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.		
Channel	Shows the currently used channel.		
Wireless mode	AP support wireless mode. It may support 802.11b, 802.11g or 802.11n wireless mode.		
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, Not Use and WPS.		
Signal	Shows the receiving signal strength of specified network.		
Rescan	Click to refresh the AP list.		
Add to Profile	Select an item on the list and then click to add it into the profile list.		

- 20 -

Connect	Select an item on the list and then click to make a
	connection.

AP Information

When you double click on the intended AP, you can see AP's detail information that divides into four parts. They are General, WPS, CCX and 802.11n information. The introduction is as following:

General	General V#PS CCX 802,11n				
	SSD >> Oterry_start_11n_Bouter MAC Address >> 00 DP-40-56-51-01 Segred (Seegen) == K00.5 Authenticution Type >> UBROWN Segred (Seegen) == K00.5 Doughtion Type >> Name Segred (Seegen) == K00.5 Outhernicution Type >> Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Outhernicution Type >> Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Outhernicution Type >> Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Notation Type >> Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5 Segred (Seegen) == K00.5				
	General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates. Close : Click this button to exit the information screen.				
WPS	General WPS CCX 802,11n				
	Authentication /pge => Ukinown State >> Configured Encryption /pge => Now Version >> 1.0 Config Method; >> Ukinown AP Setup Looked >> Device Rasserd ID >> Ukinown AP Setup Looked >> Device Rasserd ID >> Ukinown AP Band; >> Ukinown				
	Close				
	WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.				

- 21 -

Authentication Type: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK and WPA system.
Encryption Type : For Open and Shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
Config Methods : Correspond to the methods the AP supports as an Enrollee for adding external Registrars.
Device Password ID : Indicate the method or identifies the specific password that the selected Registrar intends to use. Selected Registrar : Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
State : The current configuration state on AP. The values are "Unconfigured" and "Configured". Version : WPS specified version.
AP Setup Locked: Indicate if AP has entered a setup locked state. UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.
RF Bands : Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz".
Close : Click this button to exit the information screen.
General WPS CCX 802.11n COM >> FALSE COM >> FALSE COM >> FALSE COM >> FALSE
Clore

- 22 -

	information Close: Clic		itton to	exit the informa	tion screen.
802.11n	General	WPS	CCX	802.11n	
	Secondary Channel Secondary Channel C			0	1
	Extended Capability HT Information Exch	ies information eleme anna Support	hin	FALSE	
	Neighbor Report el	lement			
	Mobility Domain High Throughput			FALSE	
	HT Capabilities elec	nent		PALSE	
	HT Capability			TRUE	
	LDPC Coding Capabil			FALSE	
	Supported Channel W	ingth Set		1	
				Close	
			100		
	This tab wi	11 shows		w calact the AD	hat anna art 11
	This tab wi	II SHOW	ир п ус	ou select the AP t	nat support 11
	mode Here	showe	the con	nected AP 802.1	1n related

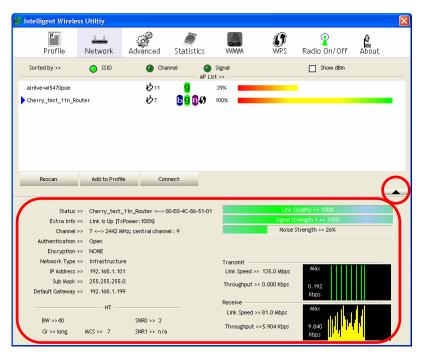
Link Status

Click the triangle button at the right down corner of the windows to expand the link status. The link status page displays the detail information of current connection.



Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.



Link Status Tab		
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.	
Extra Info	Shows the link status and Tx power percentage.	
Channel	Shows the current channel in use.	
Authentication	Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.	
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.	

- 24 -

Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
IP Address	Shows the IP address information.
Sub Mask	Shows the Subnet Mask information.
Default Gateway	Shows the default gateway information.
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.
Signal Strength 1	Shows the Receiving signal strength, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.
Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for your wireless network.

- 25 -

Profile	Lee Network	ر Advanced	Statistics	WMM	Ø WPS	Radio On/Off	About
Wireless mode >>	2.4G	•		Turn o	n CCKM Radio Measure	ble eXtensions) nents el Measurements limit	
Enable TX Bu	/indow Size g at -70 dBm			2	50 ms (0-200		
	tication Status Dialo t Your Country Regi 0: CH1-11						
Apply							

Advanced Tab	
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the adapter to deliver better throughput during a period of time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at dBm	Check to set the roaming interval, fast to roaming, setup by transmits power. Default setting is -70dBm.
Show Authentication Status Dialog	When you connect AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.
Enable CCX (Cisco Compatible extensions)	 Check to enable the CCX function. Turn on CCKM. Enable Radio Measurements: Check to enable the Radio measurement function. Non-Serving Measurements limit: User can set channel measurement every 0~2000 milliseconds. Default is set to 250 milliseconds.

- 26 -

Apply	Click to apply above settings.
-------	--------------------------------

Statistics

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

Y Intelligent Wireless Utiltiy				
Profile Network Advanced Statis	tics WWW	WPS Radio O	~	
Transmit Receive				
Frames Transmitted Successfully Frames Retransmitted Successfully	:	30836 30836		
Frames Fail To Receive ACK After All Retries RTS Frames Successfully Receive CTS	-	174		
RTS Frames Fail To Receive CTS	-	0		
Transmit Frames Transmitted Successfully Shows information of frames successful sent.				
Frames Retransmitted Successfully		mation of fram le or more retie	es successfully s.	
Frames Fail To Receive ACK After All Retries		mation of fram er hitting retry l		
RTS Frames Successfully Receive CTS	Shows information of successfully receive CTS after sending RTS frame			
RTS Frames Fail To Receive CTS	Shows infor after sending		d to receive CTS	
Reset Counter	Click this b	utton to reset co	ounters to zero.	

- 27 -

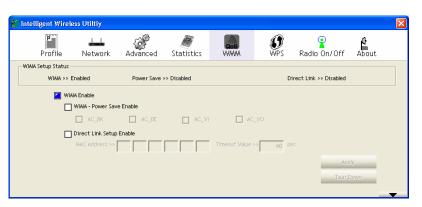
Intelligent Wirel	ess Utiltiy	Advanced	Statistics	Cos WAMA	Ø WPS	Radio On/Off	About	
Transmit	Receive							
Frames Received Successfully					1541			
Frames F	eceived With CRC	Error		= 627				
Frames Dropped Due To Out-of-Resource				- 0		0		
Duplicate Frames Received				-		0		
Reset Counter								•

Receive Statistics	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of frames received more than twice.
Reset Counter	Click this button to reset counters to zero.

WMM / QoS

The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup that ensure your wireless network quality.

- 28 -



WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	 The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: Connecting with the same AP that supports DLS feature. DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.

- 29 -

Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA, then click "Tear Down"
Tear Down	button to disconnect the STA.

WPS

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.

P		6		<u></u>	G	Q	A	
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
		W	PS AP List					
							Rescan	-
						100	Information	-
							Pin Code	
						1	6912113 Ren	ew
		WPS	Profile List			<u>_</u>	Config Mode	
Cherry_test_11n	_Router					F	Enrollee	•
							Detail	
						>	Connect	
EIN	WPS Associate I	-		Progress >> 100)%		Rotate	
PBC	WPS Probe IE	PPO C	Get WPS profile suc				Disconnect	

WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information	Display the information about WPS IE on the selected

- 30 -

	network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.		
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.		
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.		
Detail	Click the Detail button to show the information about Security and Key in the credential. Image: Click the Detail button to show the information about Security and Key in the credential. Image: Click the Detail button to show the information about Security and Key in the credential. Image: Click the Detail button to show the information about Security and Key in the credential. Image: Click the Detail button to see more AP information. SSID: Shows the connected AP network name.		



	BSSID : The MAC address of the connected AP. Fixed and cannot be changed.
	Authentication Type : The authentication type support Open, WPA-PSK and WPA2-PSK.
	Encryption Type: For Open authentication mode, the selection of encryption type are NONE and WEP . For WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES .
	Key Length: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.
	Key Index: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index. Key Material: The key material can be used to ensure the security of your wireless network. Fill in the appropriate value or phrase in Key Material field.
	Show Password : Check this box to show the passwords that have been entered.
	OK : Click to save and apply the new settings.
	Cancel : Click to leave and discard the settings.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.
Export Profile	Export all credentials to Profile.

- 32 -

Delete	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.	
PIN	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.	
РВС	Start to add to AP using PBC (Push Button Configuration) method.	
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.	
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.	
Auto	Check this box the device will connect the AP automatically.	
Progress Bar	Display rate of progress from Start to Connected status.	
Status Bar	Display currently WPS Status.	

Radio On/Off

Click this Radio On/Off button to turn ON or OFF radio function.





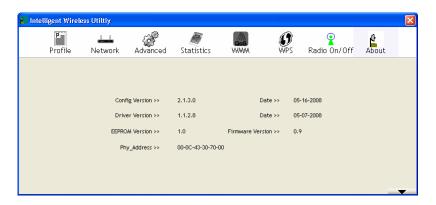
This icon shows radio on, click to turn it off.

This icon shows radio off, click to turn it on.

- 33 -

About

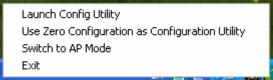
This page displays the information of the wireless card including, Config Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.



- 34 -

Utility Menu List

To access the utility menu list, please right click the utility icon on the task bar.



- Launch Config Utility: Select to open the utility screen.
- Use Zero Configuration as Configuration Utility: Select to use the Window XP built-in utility (Zero configuration utility).
- Switch to AP Mode: Select to make your wireless USB adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

- 35 -

Soft AP mode

Config

nt	Hide SSID	Security Setting
100	Hide SSID	-
	IX BURST	
100 % 🗸 🗸	[
300		
	Default	Apply
	300	300 Defauit

Config	
SSID	AP name of user type. User also can click Use Mac Address button to display it.
Channel	Manually force the AP using the channel. The system default is CH 1.
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. The system default is no authentication and encryption.

- 36 -

	- Wep Key	Encryption Type Not Use	•
	С Кеу#2 Нех С Кеу#3 Нех С Кеу#4 Нех		
		☐ Show Password	
	ОК	Cancel	
] a t	authentication mode, type are Not Use and WPA2-PSK , and W I	or Open and Shared the selections of encryptio WEP . For WPA-PSK , PA-PSK/ WPA2-PSK the encryption type suppor	
			115
be W aı	etween AP and STA /PA2-PSK and WP. athentication mode,	ey: This is the shared secre A. For WPA-PSK and A-PSK/ WPA2-PSK this field must be filled wi 8 and less than 64 lengths.	et ith

- 37 -

	 WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are two formats to enter the keys. Hexadecimal (128bits): 26 Hex characters. ASCII (128bits): 13 ASCII characters. Show Password: Check this box to show the password you entered.
Beacon (ms)	The time between two beacons. The system default is 100 ms.
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and lowest. The system default is 100%.
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. Default value of idle time is 300 seconds.
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. The system default is no forwarding.
Hide SSID	Do not display AP name. System default no hide.
Allow BW 40MHz	Click to disable this function. Default is enabled.
Tx BURST	Check to enable this function.
Default	Use the system default value.
Apply	Click to apply the above settings.

- 38 -

Access Control

Access Policy		Disable	•
MAC Address		Access List	
		1	
	Delete		
	Remove All		
	Hemove All		
			Apply

Access Contro	Access Control		
Access Policy	User chooses whether AP start the function or not. System default is Disable.		
	 Disable: Do not use this access control function. Allow All: Only the MAC address listed in the Access List can connect with this soft AP. Reject All: Only the MAC address listed in the Access List can NOT connect with this soft AP. 		
Mac Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.		
Access List	Display all Mac Address that you have set.		

- 39 -

Add	Add the MAC address that you would like to set.	
Delete	Delete the Mac address that you have set.	
Remove All	Remove all Mac address in the Access List.	
Apply	Apply the above changes.	

MAC Table

onfig Access Control Mac Table	Event Log	Statistics /	About	
MAC Address	AID	Power S	Status	
<				>

MAC Table		
MAC Address	The station MAC address of current connection.	
AID	Raise value by current connection.	
Power Saving Mode	The station of current connect whether it have to support.	
Status	The status of current connection.	

- 40 -

Event Log

Event Time (yy/mm/dd-hh:mm:ss)	Message	
2008 / 06 / 03 - 14 : 19 : 44	Restart Access Point	
		Clear

Event Log	
Event Time (yy/mm/dd-hh:mm:ss)	Records the event time.
Message	Records all the event messages.

- 41 -

Statistics

🖌 Intelligent Wireless Utility		
Config Access Control Mac Table Event Log	Statistics About	
Transmit Statistics		
Frames Transmitted Successfully	=	185
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	-	0
Frames Transmitted Successfully After Retry	-	0
Receive Statistics		
Frames Received Successfully	=	0
Frames Received With CRC Error	=	718
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0
		RESET COUNTERS
		i

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

- 42 -

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About

This page displays the wireless card and driver version information.

🖌 Inte	elligent Wireless U	tility			X
Config	g Access Control Ma	c Table Event Lo	g Statistics About		
	Utility Version :	2.0.2.1	Date :	05-16-2008	
	Driver Version :	1.1.2.8	Date :	05-07-2008	
	EEPROM Version :	1.0 F	Firmware Version :	0.9	
	IP Address :	192.168.123.1	Phy_Address :	00-0C-43-30-70-00	
	Sub Mask :	255.255.255.0	Default Gateway :		

- 43 -

UTILITY CONFIGURATION FOR WINDOWS VISTA

After the Wireless adapter has been successfully installed, users can use the included Configuration Utility to set their preference.

Go to Start→ (All) Program→ Intelligent Wireless→ Intelligent Wireless Utility.



You can also open the Configuration Utility by double clicking the icon or right clicking to select **Launch Config Utility**.



- 44 -

Station Mode

Profile

Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. The Profile manager enables you to **Add, Edit, Delete** and **Activate** profiles.



Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.

Profile	Legendre Network	Î	Statistics	Qos WMM	() WPS	Radio On/Off	About
Profile	Network	Advanced	Statistics	AA WOM	WPS	Radio On/On	ADOUL
	Pro Pro	file List					
PROF1	Cherry_test_	11n_Router		5	Profile Name	>> PROF1	
					SSID	>> Cherry_test_11n_Rd	outer
					Network Type	>> Infrastructure	
					Authentication	>> Open	
					Encryption	>> None	
					Use 802.1x	>> NO	
					Tx Power	>> Auto	
					Channel	>> Auto	
				1	Power Save Mode	>> CAM	
					RTS Threshold	>> 2347	
Add	Edit	Delete	Activate	e Fra	agment Threshold	>> 2346	_

Profile Tab	
Profile Name	You may enter a distinctive name of profile in this column. The default is PROF# (# 1, #2, #3)
SSID	The SSID is the unique name shared among all points in your wireless network.
Network Type	Shows the network type of the device, including Infrastructure and Ad-Hoc.

- 45 -

Authentication	Shows the authentication mode.
Encryption	Shows the encryption type.
Use 802.1x	Whether use 802.1x feature or not.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Channel	Shows the selected channel that is currently in use.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	Click to add a profile from the drop-down screen.
	System Configuration tab:

- 46 -

Intelligent Wireless	s Utility						1
		(P)	M		Ø	Radio On/Off	£
Profile	Network	Advanced	Statistics	WMM	wps	Radio On/Off	About
PROFI	Cherry_best_		Activ	e e e e e e e e e e e e e e e e e e e		Cherry_test_tin, Infrastructure Inf	lauter
System Config	Auth. \ Enci	ry. :					_
Profile Na	ame >> PROF1			Network Typ	r⇒> infrast	ructure 👻	
2	SID >> Cherry_tes	st_11n_Router		Tx Power			
Power Sa	we Mode >> 🙆 C	AM 🙆 PSM	0	Prearbh	10	to 👻	
C 873	5 Threshold			j 238	2347		
D Pa	agment Threshold	298		j (D)	2346		
			OK	Carce	and a		
ooints in dentical o the sau select fro	for all me netvor	vireless device work. U ilable A	s netw s and Jser ca APs.	ork. T points an use	The names attemne pull-d	red amor ne must pting to lown me	be connec nu to
Networl Ad hoc r		: There	e are tv	vo typ	bes, Inf	rastructu	ire and
betwe	en wire					e connec n Access	
						nnect wi Access	

- 47 -

Tx Power : Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including Auto , 100% , 75% , 50% , 25% , 10% and Lowest .
Preamble : This function will show up when Ad-hoc network type be selected. A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. Select from the pull-down menu to change the Preamble type into Auto or Long .
RTS Threshold : User can adjust the RTS threshold
number by sliding the bar or key in the value directly. The default value is 2347. RTS/CTS Threshold is a mechanism
implemented to prevent the " Hidden Node " problem. If
the "Hidden Node" problem is an issue, users have to
specify the packet size. The RTS/CTS mechanism will be
activated if the data size exceeds the value you set. This
value should remain at its default setting of 2347. Should
you encounter inconsistent data flow, only minor
modifications of this value are recommended.
Fragment Threshold: User can adjust the Fragment
threshold number by sliding the bar or key in the value
directly. The default value is 2346. The mechanism of
Fragmentation Threshold is used to improve the efficiency
when high traffic flows along in the wireless network. If
your Wireless LAN Adapter often transmits large files in
wireless network, you can enter new Fragment Threshold
value to split the packet. The value can be set from 256 to
2346.
Authentication and Encryption tab:

- 48 -

	ss Utiltiy				
Profile	Network	Advanced St	atistics W	WI WPS	Radio On/Off Abou
PROFI	Profile Cherry_test_Th	List	U	Network Type Authentication Encryption Use 802.1x Tx Power Channel Power Save Mode	PROP1 Cherry_testtin_Bouter Infrastructure Open None None Auto Auto Auto Auto Cher
Add	tat	Celete	Activate	RTS Threshold Fragment Threshold	
System Config					
	reshared Key >>	Open 🔻	Encryption >>	None 💌	802.1X
W	lep Key		2		
	÷	outerinal 👻	2		Show Password
		enterrent 👻			
	KeyAl Ha	adernal V			
	•	Souther -			
modes n	iciuaing	Upen. S			
and WP.	A2-PSK.	· ·	nared,	WPA, W	PA-PSK, W
• Open "Ope	: If your	access j nticatio	point/ w n, then t	ireless ro he wirel	outer is using ess adapter v
Open "Ope need Share	: If your n" authe to be set	access j intication to the sa	point/ w n, then t ame aut	ireless ro he wirel henticati	outer is using ess adapter on type.
 Open "Open need Shard recipition WPA WPA 	 If your n" authe to be set ed: Share ient share / WPA-I s two encorpe of alg 	access j ntication to the sa ed key is e a secre PSK/ W cryption corithm, Key of 8	point/ w n, then t ame aut when t t key. PA2/ V method TKIP o	ireless ro he wirel henticati both the s VPA2-P S s, TKIP r AES an	outer is using ess adapter v

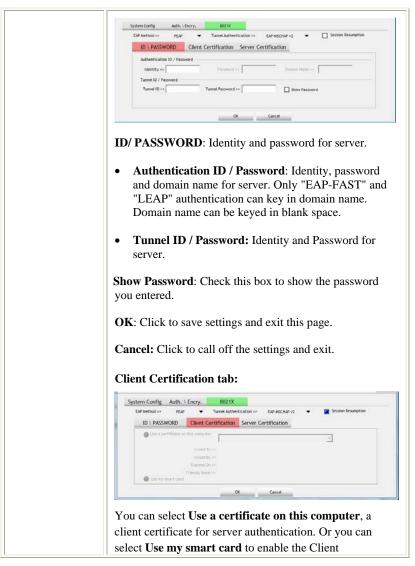
- 49 -

WPA Pre-shared Key : This blank is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.
 WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys. Hexadecimal (128bits): 26 Hex characters (0~9, a~f). ASCII (128bits): 13 ASCII characters.
Show Password: Check this box to show the password you entered.
802.1x Setting : When user use radius server to authenticate client certificate for WPA authentication mode.
802.1x tab:
Profile Network Advanced Statistics WMMM WPS Radio On/Off About
Profile List Profile Name >> PROFI S00 >> Cherry_tell_tin_Nouter S00 >> Cherry_tell_tin_Nouter Network Type >> Unit Solutions Authentications >> Open Excryptions >> Nene Use 80:List >> None Use 80:List >> N
Poet Size Note >> C.M. RTS Threads >> 2247 Add Eath Delete Activate Prognet Threads >> 2346
System Config Auto. \ Encry. BR210: SAP Nethod >> PLAP
Adhetication (0) Prepared identity vs pression (0) Prepared Turnel (0) Prepared Turnel (0) Prepared
Turnel ID >> Turnel Password >> D Show Password
OK Carcel
EAP Method:

- 50 -

• PEAP : 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.
• TLS / Smart Card : 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.
Tunnel Authentication:
• Protocol : Tunnel protocol, List information including EAP-MSCHAP v2 and EAP-TLS/ Smart Card .
• Tunnel Identity : Identity for tunnel.
• Tunnel Password: Password for tunnel.
Session Resumption : Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. User can click the box to enable or disable this function.
ID\PASSWORD tab:

- 51 -





	Certification function.
	OK : Click to save settings and exit this page.
	Cancel: Click to call off the settings and exit.
	Server Certification tab:
	System Config Auth. \ Encry. 8021X
	EAP Nethod >> PEUP Tunnis Authentication >> EAP Section Peup Peup Peup Peup Peup Peup Peup Peup
	Use certificate chain
	Server taste ==
	OK Cancel
	Use certificate chain: Choose use server that issuer of
	certificates.
	Server name: Enter an authentication sever name.
	OK : Click to save settings and exit this page.
	Cancel: Click call off the settings and exit.
Delete	Click to delete an existing profile.
Edit	Click to edit a profile.
Activate	Click to make a connection between devices.

Network

The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

- 53 -

Profile Network Advanced Statistics WMM WPS Radio On/Off Ab Sorted by >> Image: SSID Image: Channel Image: Signal Image: Signal Image: Show dBm > Cherry_test_11n_Router Image: V7 Image: Signal Image: Show dBm Image: Show dBm Abcom-Wireless Image: V11 Image: Show dBm Image: Show dBm Image: Show dBm airdive-wIS470poe Image: Show dBm Image: Show dBm Image: Show dBm Image: Show dBm	out
AP List >> AP List >> Cherry_test_11n_Router 107 10 100% Abocon-Wireless 10 10 100%	
ک Cherry_test_11n_Router 67 کو 10 کو 100% Abocom-Wireless 66%	
Abocom-Wireless 🔌 11 😼 9 86%	
airtive-wt5470poe 💋 11 🧧 50%	
ski 🥠 10 🧕 44% 💶	
Abocom-Wireless 🤣 6 📴 🧕 29% 📩	
PINGOO 💋 11 📴 24%	
802.11g-AP 💋 15%	

Network Tab	
Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b or 802.11g or 802.11n wireless mode.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Signal	Shows the receiving signal strength of specified network.
Rescan	Click to refresh the AP list.
Add to Profile	Select an item on the list and then click to add it into the profile list.

AP information

When you double click on the intended AP, you can see AP's detail information that divides into three parts. They are General, WPS, CCX information. The introduction is as following:

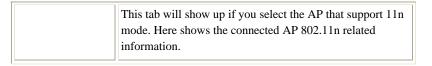
- 54 -

1	
General	General WPS CCX 802.11n
	SSID >> Cherry_lest_itin_Bouter
	MAC Address >> . 00-E0-4C-86-51-01. Signal Strength >> 1000 Authentication Type >> . Unknown
	Encryption Type >> None 1, 2, 5,5, 11, 6, 9, 12, 18, 24, 36, 48, 54
	Enamelicy 7 < < >> 242 MHz 1 / 24 / 2019 1 / 10 / 10 / 24 / 100 / 10 / 2019 100 / 2019 Hetwork Type >> Infrastructure
	Beacon Interval >> 100
	Close
	General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates.
	Close : Click this button to exit the information screen.
WPS	General WPS CCX 802.11n
	Authentication Type >> Unknown State >> Configured
	Encryption Type >> None Version >> 1.0
	Config Methods Sh0086 AP Setup Locked
	Device Passward ID >> UUID-E >> 6304125310142006122800E04C805101 Selected Registrar >> Unknown 8F Bands >> Unknown
	And and the Annual of Annual and A
	Close
	WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.
	Authentication Type : There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK and WPA system.
	Encryption Type: For open and shared authentication
	mode, the selection of encryption type are None and WEP.
	For WPA, WPA2, WPA-PSK and WPA2-PSK
	authentication mode, the encryption type supports both
	TKIP and AES.
	Config Methods: Correspond to the methods the AP
	supports as an Enrollee for adding external Registrars.

- 55 -

	Device Password ID : Indicate the method or identifies	s the
	specific password that the selected Registrar intends to	use.
	Selected Registrar: Indicate if the user has recently	
	activated a Registrar to add an Enrollee. The values are	e
	"TRUE" and "FALSE".	
	State: The current configuration state on AP. The valu	es
	are "Unconfigured" and "Configured".	
	Version: WPS specified version.	
	AP Setup Locked: Indicate if AP has entered a setup	
	locked state.	
	UUID-E : The universally unique identifier (UUID) ele	emen
	generated by the Enrollee. There is a value. It is 16 byt	tes.
	RF Bands : Indicate all RF bands available on the AP.	
	dual-band AP must provide it. The values are "2.4GHz	z".
	Close: Click this button to exit the information screen.	
CXX		-
	General WPS CCX 802,11n	
	COMING FU OF	
	CIPIC FALSE	
	CHID >> FALSE	
	Close	
	Cove	
	CCX information contains CCKM, Cmic and Ckip	
	CCX information contains CCKM, Cmic and Ckip information.	
	CCX information contains CCKM, Cmic and Ckip	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.	

- 56 -

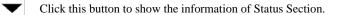


Link Status

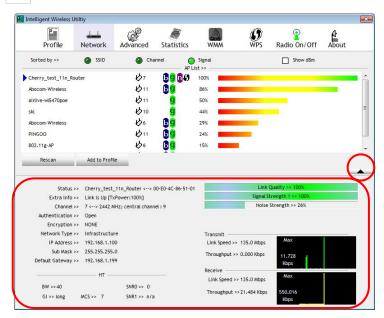
Click the triangle button at the right down corner of the windows to expand the

link status. The link status page displays the detail information of current

connection.



Click this button to hide the information of Status Section.



- 57 -

Link Status Tab				
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.			
Extra Info	Shows the link status and Tx power percentage.			
Channel	Shows the current channel in use.			
Authentication	Authentication mode used within the network, including Unknown, Open, WPA-PSK, WPA2-PSK, WPA and WPA2.			
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.			
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.			
IP Address	Shows the IP address information.			
Sub Mask	Shows the Subnet Mask information.			
Default Gateway	Shows the default gateway information.			
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.			
Signal Strength 1	Shows the Receiving signal strength, you can choose to display as percentage or dBm format.			
Noise Strength	Shows the noise signal strength in the wireless environment.			

- 58 -

Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for your wireless network.

Contraction Contraction Contraction	Utiltiy						
		()		QoS WMM	() WPS	Partia Or (Off	4
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About
Wireless mode >>	2.4G	•					
Enable TX Bur Enable TCP W							
Fast Roaming							
Select	Your Country Regi	on Code					
11 B/G >>	0: CH1-11		-				
			_				
Apply							

Advanced Tab	
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the adapter to deliver better throughput during a period of

- 59 -

	time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at	Check to set the roaming interval, fast to roaming, setup by transmits power.
Apply	Click to apply above settings.

Statistics

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

ofile Network Advanced Statistics WMM		WPS	Radio On/Off	About		
Receive						
ransmitted Succe	ssfully				1294	
Frames Retransmitted Successfully				1294		
Frames Fail To Receive ACK After All Retries		-		15		
RTS Frames Successfully Receive CTS			=		0	
RTS Frames Fail To Receive CTS			-		0	
	Prenerive Transmitted Succe tetransmitted Succe fail To Receive ACI tes Successfully Re	Receive ransmitted Successfully letransmitted Successfully Fall To Receive ACK After All Retries les Successfully Receive CTS	Receive ransmitted Successfully letransmitted Successfully rail To Receive ACK After All Retries les Successfully Receive CTS	Receive ransmitted Successfully etransmitted Successfully all To Receive ACK After All Retries ese Successfully Receive CTS	Receive ransmitted Successfully letransmitted Successfully rail To Receive ACK After All Retries ese Successfully Receive CTS	Receive ransmitted Successfully = 1294 letransmitted Successfully = 1294 ail To Receive ACK After All Retries = 15 ses Successfully Receive CTS = 0

Transmit Statistics Tab	
Frames Transmitted Successfully	Shows information of frames successfully sent.
Frames Retransmitted Successfully	Shows information of frames successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Shows information of frames failed

- 60 -

	transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Shows information of failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.

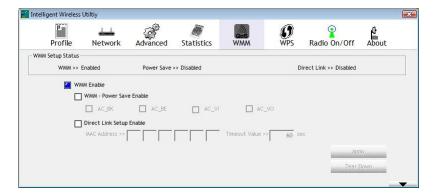
Profile Network Advanced		Statistics	WMM	WPS	Radio On/Off	About	
ansmit	Receive						
Frames R	eceived Successfu	lly				452	
Frames Received With CRC Error				731			
Frames Dropped Due To Out-of-Resource						0	
Duplicate	Frames Received					0	

Receive Statistics Tab	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of frames received more than twice.
Reset Counter	Click this button to reset counters to zero.

- 61 -

WMM / QoS

The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup that ensure your wireless network quality.



WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	 The setting of DLS(Direct Link Setup) indicates as follow: Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: Connecting with the same AP that supports DLS feature.

- 62 -

	• DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA, then click "Tear Down" button to disconnect the STA.

WPS

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.

Profile	Network	Advanced	Statistics	WMM	Ø WPS	Radio On/	Off About
		WP	S AP List				
ID :	Cherry	_test_11n_Router		00-E0-4C-86-51-01	7		Rescan Information
							Pin Code 57055251 Renew
		WPS	Profile List				Config Mode
Cherry_test_11r	_Router						Enrollee 👻
							Detail
			m			•	Connect
<u>P</u> IN	WPS Associate	IE		Progress >> 100%			Rotate
PBC	WPS Probe IE	PBC - G	et WPS profile si	uccessfully.			Disconnect
							Export Profile
							Delete

Display the information of surrounding APs with WPS IE from last scan result. List information included SSID,

- 63 -

	BSSID, Channel, ID (Device Password ID), Security-Enabled.			
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.			
Information	Display the information about WPS IE on the selected network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.			
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.			
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.			
Detail	Click the Detail button to show the information about security and Key in the credential.			

- 64 -

	If you select the AP that listed in the WPS Profile List field, you can click the Detail button to see more AP information.
	 SSID: Shows the connected AP network name. BSSID: The MAC address of the connected AP. Fixed and cannot be changed. Authentication Type: The authentication type support Open, WPA-PSK and WPA2-PSK.
	Encryption Type: For Open authentication mode, the selection of encryption type are NONE and WEP . For WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES .
	Key Length: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.
	Key Index: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.
	Key Material: The key material can be used to ensure the security of your wireless network. Fill in the appropriate value or phrase in Key Material field.
	Show Password : Check this box to show the passwords that have been entered.
	OK : Click to save and apply the new settings.
	Cancel: Click to leave and discard the settings.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And

- 65 -

	then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.
Export Profile	Export all credentials to Profile.
Delete	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.
PIN	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
РВС	Start to add to AP using PBC (Push Button Configuration) method.
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

Click this button to turn on or off radio function.





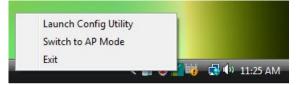
About

This page displays the information of the wireless card including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version and Phy_Address.

Markelli Intelli	igent Wireless L	Itiltiy							X
			(S)		GoS	0	8	4	
	Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
		Conf	ig Version >>	2.1.3.0	D	ate >> 05	5-16-2008		
			-						
		Drive	er Version >>	2.1.6.7	Da	ate >> 05	5-02-2008		
		EEPRO	M Version >>	1.0	Firmware Vers	ion >> 0.	9		
		Ph	y_Address >>	00-0C-43-30-70-00	D				
			-						
								-	•

Utility Menu List

To access Windows Vista utility menu list, please right click the utility icon on the task bar.



- Launch Config Utility: Select to open the utility screen.
- Switch to AP Mode: Select to make your wireless USB adapter act as a wireless AP.
- **Exit**: Select to close the utility program.



Soft AP mode

Config

1	telligent	Channel 1 - Use Mac Address Security Setting
- Country Region Codi 11 B/G 0: CH1		No forwarding among wireless clients Hide SSID Allow BW 40 MHz
Beacon (ms)	100 %	-
TX Power Idle time(60 - 3600)(s)	30	-
		Default Apply

Config	
SSID	AP name of user type. User also can click Use Mac Address button to display it.
Channel	Manually force the AP using the channel. The system default is CH 1.
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. The system default is no authentication and encryption.

- 68 -

					X
Authentication Ty	ype Open	•	Encryption Type	Not Use	•
WPA Pre-shared	J-Key				
Group Rekey Inte	terval 60	0 10 seconds			
	1				
-Wep Key					
€ Key#1	Hex	-			
C Kev#2	Hex	-			-
C Kev#3	Hex	- , 			-
	,				_
C Key#4		<u> </u>			
* WEP 64 8 WEP 128 8	Bits Encryption: Pleas Bits Encryption: Pleas	se Keyin 10 HE se Keyin 26 HE	X characters or 5 X characters or 13	ASCII character 3 ASCII characte	s ^a Ifs
				Show Passv	vord
	ОК		Ca	ncel	
VPA-PSK	K, WPA2-P K/WPA2-PS	SK, and SK.	1	, Shared	,
PA-PSK ncryption thenticat pe are No PA2-PS thenticat	K, WPA2-P	SK, and SK. or Oper the sele WEP . PA-PSI the enc	and Sha ections of For WPA	ared f encrypt A-PSK, 2-PSK	tion
PA-PSK cryption henticat he are No PA2-PS henticat h TKIP PA Pre- ween A PA2-PSI henticat	K, WPA2-P K/WPA2-PS In Type : Fo tion mode, ot Use and K , and WI tion mode,	SK, and SK. or Oper the sele WEP . PA-PSH the enc ey: This A. For W A-PSK/ this fie	and Sha ections of For WPA (WPA2 ryption ty is the sh /PA-PSK WPA2-I ld must b	ared f encrypt A-PSK, 2-PSK ype supp ared sec and PSK be filled	tion ports cret with

- 69 -

	WEP Key : Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.
	 Hexadecimal (64bits): 10 Hex characters. Hexadecimal (128bits): 26 Hex characters. ASCII (64bits): 5 ASCII characters. ASCII (128bits): 13 ASCII characters.
	Show Password : Check this box to show the password you entered.
Beacon (ms)	The time between two beacons. The system default is 100 ms.
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. The system default is 100%.
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. Default value of idle time is 300 seconds.
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. The system default is no forwarding.
Hide SSID	Do not display AP name. System default no hide.
Allow BW 40MHz	Click to disable this function. Default is enabling.
Default	Use the system default value.
Apply	Click to apply the above settings.

- 70 -

Access Control

Access Policy		Disable	-
MAC Address		Access List	
	Add	1	
	Delete		
	Remove All		
		3	
			Apply

Access Control	
Access Policy	 User chooses whether AP start the function or not. System default is Disable. Disable: Do not use this access control function. Allow All: Only the MAC address listed in the Access List can connect with this soft AP. Reject All: Only the MAC address listed in the Access List can NOT connect with this soft AP.
MAC Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that you have set.

- 71 -

Add	Add the MAC address that you would like to set.
Delete	Delete the MAC address that you have set.
Remove All	Remove all MAC address in the Access List.
Apply	Apply the above changes.

MAC Table

			410		
	 Status	Power S	AID		MAC Address
•					< [
				m	

MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

- 72 -

Event Log

Event Time (yy/mm/dd-hh:mm:ss)	Message	
008 / 06 / 06 - 11 : 26 : 49	Restart Access Point	
008 / 06 / 06 - 11 : 26 : 50	Restart Access Point	
008 / 06 / 06 - 11 : 26 : 50	Restart Access Point	
		Clear

Event Log	
Event Time (yy/mm/dd-hh:mm:ss)	Records the event time.
Message	Records all the event messages.

- 73 -

Statistics

nfig Access Control Mac Table Event Log Stati	in the second se	
Transmit Statistics		
Frames Transmitted Successfully	=	331
Frames Fail To Receive ACK After All Retries	= 1	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
Frames Transmitted Successfully After Retry		0
Receive Statistics		
Frames Received Successfully	=	206
Frames Received With CRC Error	=	123
Frames Dropped Due To Out-of-Resource	-	0
Duplicate Frames Received	-	0
	1	RESET COUNTERS
	<u>I</u>	ILSET COONTEND

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

- 74 -

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About This page displays the wireless card and driver version information.

Utility Version :	2.0.2.1	Date :	05-16-2008
Driver Version :	2.1.6.7	Date :	05-02-2008
EEPROM Version :	1.0	Firmware Version :	0.9
IP Address :	192.168.123.1	Phy_Address :	00-0C-43-30-70-00
Sub Mask :	255.255.255.0	Default Gateway :	0.0.0.0

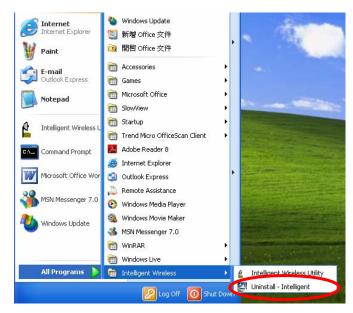
- 75 -

UNINSTALLATION FOR WINDOWS

2000/XP

In case you need to uninstall the Utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

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

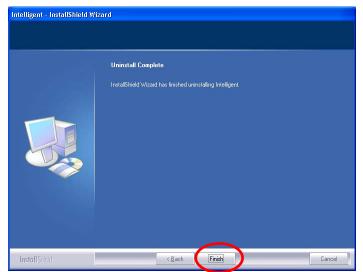


- 76 -

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



3. Then click **Finish** to complete the uninstallation.



- 77 -

UNINSTALLATION FOR WINDOWS

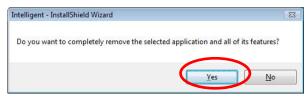
VISTA

In case you need to uninstall the utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

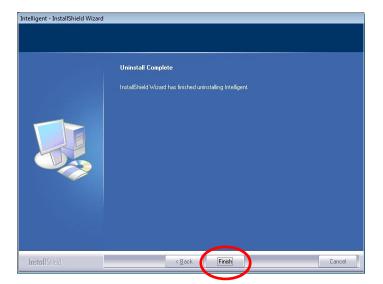
- ⑦ Default Programs
 ⑧ Internet Explorer
 ⑧ Windows Calendar Windows Contacts
 Windows Defender Cherry iiii Windows Fax and Scan a Windows Live Messenger Download Documents 🚮 Windows Mail Windows Media Player 😰 Windows Meeting Space Music Windows Movie Maker 🛅 Windows Photo Gallery Recent Items Windows Update
 Accessories Computer Extras and Upgrades Network Games Intelligent Wireless 🛃 Uninstall - Intelligent Control Panel Maintenance 📕 Startup Default Programs Help and Support Back **(**) Start Sear 2
- 1. Go to Start → Programs →Intelligent Wireless → Uninstall –Intelligent.



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



3. Then click **Finish** to complete the uninstallation.



- 79 -