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.

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.

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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

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

SAR compliance has been established in typical laptop computer(s) with USB slot, and product could be used in typical laptop computer with USB slot. Other application like handheld PC or similar device has not been verified and may not compliance with related RF exposure rule and such use shall be prohibited.

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.

Table of Contents

INTRODUCTION	1
Features	1
Windows 2000/XP Installation	2
INSTALL THE SOFTWARE	2
INSTALL THE HARDWARE	4
Windows Vista Installation	5
INSTALL THE SOFTWARE	5
INSTALL THE HARDWARE	7
VERIFICATION	7
NETWORK CONNECTION	8
IP Address	8
UTILITY CONFIGURATION FOR WINDOWS 2000/XP	9
STATION MODE	
Profile	
Network	16
Link Status	
Advanced	20
Statistics	21
WMM / QoS	22
WPS	23
Radio On/Off	25
About	25
UTILITY MENU LIST	26
Soft AP mode	26
Config	
Access Control	
MAC Table	
Event Log	
Statistics	
About	
UTILITY CONFIGURATION FOR WINDOWS VISTA	
STATION MODE	34

UNINSTALLATION FOR WINDOWS VISTA	
UNINSTALLATION FOR WINDOWS 2000/XP	55
About	54
Statistics	53
Event Log	
MAC Table	51
Access Control	50
Config	
Soft AP mode	48
UTILITY MENU LIST	48
About	47
Radio On/Off	47
WPS	45
WMM / QoS	44
Statistics	43
Advanced	42
Link Status	41
Network	
Profile	

Chapter 1: Introduction:

The **802.11 b/g/n Micro Mini Wireless LAN USB2.0 Adapter** is an IEEE802.11b/g/n USB adapter that connects your notebook to a wireless local area. The **802.11 b/g/n Micro Mini Wireless LAN USB2.0 Adapter** fully complies with IEEE 802.11n and IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance. The **802.11 b/g/n Micro Mini Wireless LAN USB2.0 Adapter** 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 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.

Chapter 2:

Installation

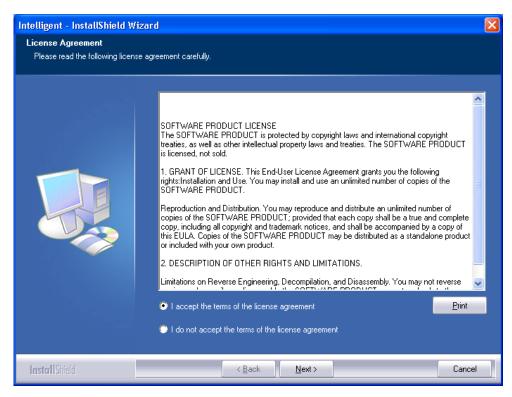
Windows 2000/XP Installation

Install the Software

Caution!

Do not insert the wireless card into your computer until the Install Shield 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.



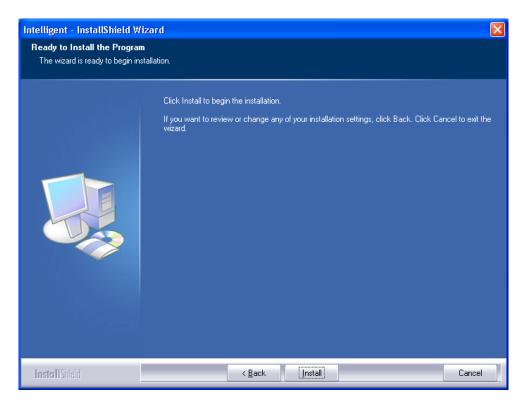
- 3. Select the check box to choose a **Configuration Tool** from the listed two choices.
 - **Configuration Tool**: Choose to use our configuration utility.

• Microsoft Zero Configuration Tool: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU).

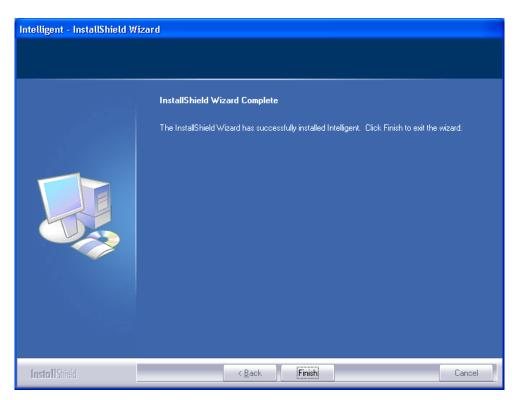
Click Next to continue.

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	< Back Next >	Cancel

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



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



Install the Hardware

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

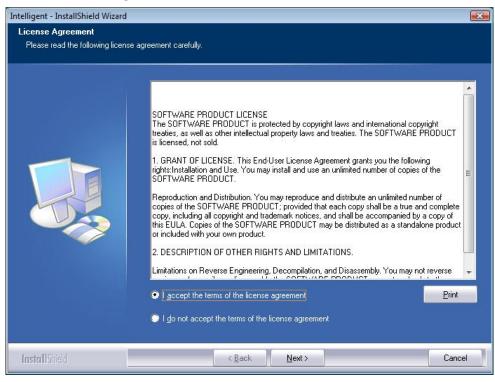
Insert the USB Adapter into the USB Port of your computer. The system will automatically detect the new hardware.

Windows Vista Installation

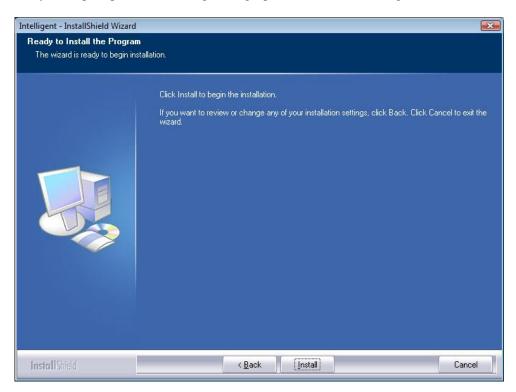
Install the Software

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

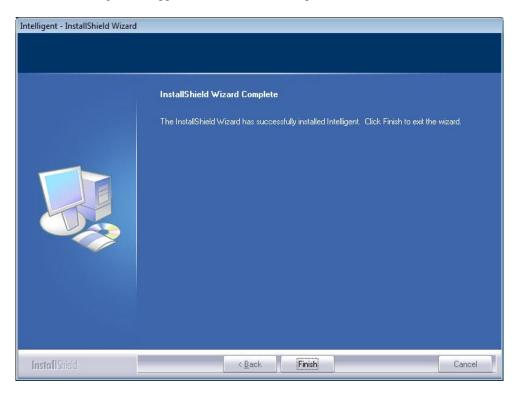
- 1. Insert the included CD-ROM into the CD-ROM drive of your computer.
- 2. When the Main Menu screen appears, click "**Driver & Utility Installation**" to start the software installation.
- 3. When the License Agreement screen appears, please read the contents and select "I accept the terms of the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



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.



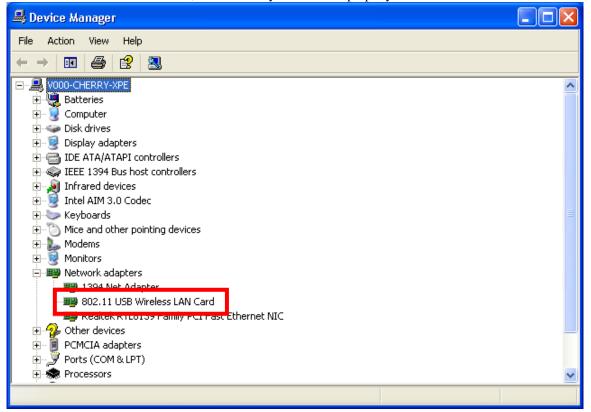
Install the Hardware

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.



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.
- 2. 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 *255.255.25.0* for the Subnet Mask.

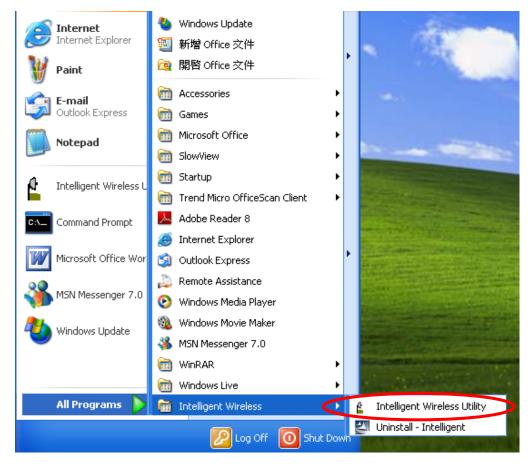
Internet Protocol (TCP/IP) Properties	Internet Protocol (TCP/IP) Properties
General Alternate Configuration	General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically	Obtain an IP address automatically
O Use the following IP address:	Use the following IP address:
IP address:	IP address: 192.168.1.1
Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Default gateway:	Refault gateway:
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	OK Cancel

Chapter 3: Utility Configuration

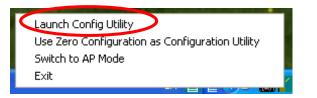
Utility Configuration for Windows 2000/XP

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.



Station Mode

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.

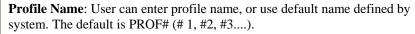


Click this button to hide the information of Status Section.

🖌 Int	telligent Wire	less Utiltiy							
	Profile	Lage Network	کی Advanced	Statistics	oos WMM	Ø WPS	Radio On/Off	About	
		Pro-	file List						
P	ROF1	Cherry_test_	11n_Router		\$	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		
					F	ower Save Mode :			
						RTS Threshold >	»> 2347		
10000	Add	Edit	Delete	Activat	e Fra	gment Threshold :	>> 2346	(
	Add	Edit	Delete	Activat	e Fra			(

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.
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.
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:

Profile	La Network	ر Advanced	Statistics		Ø WPS	Radio On/C)ff Abo
	Prot	file List					
PROF1	Cherry_test_	11n_Router		¢	Network Type Authentication Encryption	>> Cherry_test_1 >> Infrastructure >> Open	1n_Router
Add System Config	Edit	Delete ry. 80	Activ 21X		Use 802.1x Tx Power Channel ower Save Mode RTS Threshold gment Threshold	>> Auto >> Auto >> CAM >> 2347	
System Config					Tx Power Channel ower Save Mode RTS Threshold gment Threshold	>> Auto >> Auto >> CAM >> 2347 >> 2346	
System Config Profile Na	Auth. \Enci	ry. 80		ate Frag	Tx Power Channel ower Save Mode RTS Threshold gment Threshold >> Infrast	>> Auto >> Auto >> CAM >> 2347 >> 2346 ructure ▼	
System Config Profile Na Si	Auth. \Enci	ry. 80 t_11n_Router	21X	ate Frag Network Type >	T× Power Channel ower Save Mode RTS Threshold gment Threshold > Infrast > Au	>> Auto >> Auto >> CAM >> 2347 >> 2346 ructure ▼	
System Config Profile Na S Power Sa	Auth. \Enci me >> PROF1 SID >> Cherry_tes	t_11n_Router	21X	Ate Frag Network Type > Tx Power > Preamble >	T× Power Channel ower Save Mode RTS Threshold gment Threshold > Infrast > Au	>> Auto >> Auto >> CAM >> 2346 ructure to	



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 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</u> <u>RTS/CTS mechanism will be activated if the data size exceeds the value you set.</u>

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:

Authentication >>	Open	•	Encryption >>	None	▼ 802.1X
WPA Preshared Key >>					
Wep Кеу					
Key#1	Hexadecimal	-			Show Passwori
🙆 Key#2	Hexadecimal	-			
🙆 Key#3	Hexadecimal	[
Key#4	Hexadecimal	- T			

Authentication Type: There are several types of authentication modes including Open, Shared, Leap, WPA, WPA-PSK, WPA2 and WPA2-PSK.

- **Open**: If your access point/wireless router is using "**Open**" authentication, then the wireless adapter will 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.

802.1x Setting: When user use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method-MD5-Challenge).

P	ess Utiltiy					
Profile	Network A	dvanced Statistic	s WMM	Ø WPS R	adio On/Off	About
PROF1	Profile Li		Ni Au Powe	etwork Type >> Ini thentication >> Op Encryption >> No Use 802.1x >> No Tx Power >> Au Channel >> Au rr Save Mode >> CA	erry_test_11n_Rout irastructure en ne) to to M	er
Add	Edit	Delete Ac		TS Threshold >> 23 nt Threshold >> 23		
System Config EAP Method >:	Auth. \Encry.	8021X Tunnel Authenticatio	n >> EAP-MSCHAP	12 🔻	Session Resumpt	ion
ID \ PAS	SWORD Client	t Certification Ser	ver Certification			
Authentic	ation ID / Password			_		
Identity	/ Password	Password >>	Do	main Name >>		
Tunnel ID Tunnel II		Tunnel Password >>		Show Password		
		ОК	Cancel			
authenti authenti	cation data cation server ver-side centration of a	ensible Authe by using tun er. PEAP car rtificates, thu secure wirel : Transport I	nelling bet n authentica is simplifyin ess LAN.	ween PE. tte wirele ng the im	AP clients ess LAN c plementa	s and an lients u tion an
adminis TLS / S and mut client-si used to secure s access p	tual authent de and serv dynamically ubsequent opoint.	ication of the er-side certify generate us communicati	e client and ficates to pe ser-based ar ons betwee	the netwerform au ad session n the WI	rork. It rel athenticati n-based W AN clien	on and /EP ke t and t
adminis TLS / S and mut client-si used to secure s access p TTLS: for certi through	ual authent de and serv dynamically ubsequent ooint. Tunnelled 7 ficate-based	ication of the er-side certify generate us communicati Fransport La d, mutual aut ed channel. U	e client and ficates to pe ser-based ar ons betwee yer Security thentication	the netw erform au ad session n the WI y. This se of the cl	ork. It rel athenticati n-based W AN clien ecurity me ient and n	on and /EP ke t and th ethod protections

- 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 provides base-level EAP support. It provides for only one-way authentication there is no mutual authentication of wireless client and the network. (Only Open and Shared authentication mode can use this function.)

Tunnel Authentication:

- **Protocol**: Tunnel protocol, List information including **EAP-MSCHAP v2**, **EAP-TLS**/ **Smart Card**, and **Generic Token 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:

AP Method >>	PEAP	 Tunnel Authentica 	tion >> EAP-MSCHAI	°v2 ▼	Session Resumption
ID \ PASSWO	ORD	Client Certification S	erver Certification		
Authentication	ID / Passwo	rd			
Identity >>		Password >>		Domain Name >>	
Tunnel ID / Pas:	word				
Tunnel ID >>		Tunnel Password >>		Show Password	

- ID/ PASSWORD: Identity and password for server.
- Authentication ID / Password: Identity, password and domain name for server. Only "EAP-FAST" EAP method and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
- Tunnel ID / Password: Identity and Password for server.

Show Password: Check this box to show the password you entered. OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:

AP Method >> PEAP	 Tunnel Auther 	ntication >> EAP-MSCHAP v2	 Session Resumption
ID \ PASSWORD	Client Certification	Server Certification	
🔲 Use Client cer	tificate		T
	issued To >>		
	issued By >>		
	Expired On >>		
F	Friendly Name >>		

Use Client certificate: Choose to enable server authentication.

OK: Click to save settings and exit this page. **Cancel:** Click to call off the settings and exit.

Server Certification tab:

ID \ PASSWORD Client C	Certification Server Certification
Use certificate chain	
	Allow intermidiate certificates
	Server name >>
	Server name must match
	Obmain name must end in specified name
	OK. Cancel

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.			
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.

🖌 Intelligent Wirele	ss Utiltiy							×
Profile	Lee Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
Sorted by >>	🙆 SSID	🥥 Cha) Signal ist >>		Show dBm		
airiive-wl5470poe Cherry_test_11n_R Rescan	outer Add to Profi	じ11 じ7	g g g s s s s s s s s s s s s s s s s s	39%				•

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.			
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	file Select an item on the list and then click to add it into the profile list.			
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 WPS CCX 802.11n SSID >> Cherry_test_11n_Router MAC Address >> 00-E0-4C-86-51-01 Authentication Type >> Unknown Supported Rates (Mbps) Encryption Type >> None 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Channel >> 7 <--> 2442 MHz Network 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 >> Unknown AP Setup Locked >> Device Password ID >> UUID-E >> Unknown Selected Registrar >> Unknown RF Bands >> Unknown 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. 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.

СХХ	General WPS CCX 802.11n
	CCKM >> FALSE
	Cmic >> FALSE
	Ckip >> FALSE
	Close
802.11n	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.
	General WPS CCX 802.11n
	Secondary Channel Offset element
	Secondary Channel Offset 0
	Extended Capabilities information element
	HT Information Exchange Support FALSE Neighbor Report element
	Adobity Domain FALSE
	High Throughput FALSE
	HT Capabilities element
	HT Capability TRUE LDPC Coding Capability FALSE
	LDPC Coding Capability FALSE Supported Channel Width Set 1
	Clase
	This tab will show up if you select the AP that support 11n mode. Here shows t connected AP 802.11n related information.

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.

	La transiti	<u>s</u>		Qos	Ø		
Profile	Network	Advanced	Statistics	WWW	WPS	Radio On/Off	About
Sorted by >>	🙆 SSID	🥥 Cha	annel 🖉 🎱	Signal		Show dBm	
airlive-wl5470poe		11	g		_		
Cherry_test_11n_Ro	uter	1 /27	B <mark>9</mark> 🖬 🕄	100%			
Rescan	Add to Profil	e Cor	nnect				<i>C</i>
Rescan			nnect 00-E0-4C-86-51-01		Link (Quality >> 100%	
	> Cherry_test_	_11n_Router <> (Signal St	rength 1 >> 100%	_
Status Extra Info Channel	 > Cherry_test_ >> Link is Up [Tx >> 7 <> 2442 M 	_11n_Router <> (00-E0-4C-86-51-01		Signal St		-6
Status Extra Info Channel Authentication	 >> Cherry_test_ >> Link is Up [Tx >> 7 <> 2442 M >> Open 	_11n_Router <> (Power:100%]	00-E0-4C-86-51-01		Signal St	rength 1 >> 100%	-6
Status Extra Info Channel Authentication Encryption	 > Cherry_test_ > Link is Up [Tx > 7 <> 2442 M >> Open >> NONE 	_11n_Router <> (Power: 100%) Hz; central chann	00-E0-4C-86-51-01		Signal St	rength 1 >> 100%	-6
Status Extra Info Channel Authentication Encryption Network Type	 > Cherry_test_ > Link is Up [Tx > 7 <> 2442 M >> Open >> NONE >> Infrastructur 	_11n_Router <> (Power: 100%) Hz; central chann re	00-E0-4C-86-51-01	Transmit —	Signal St	rrength 1 >> 100% Strength >> 26%	
Status Extra Info Channel Authentication Encryption Network Type IP Address	 > Cherry_test_ >> Link is Up [Tx >> 7 <> 2442 M >> Open >> NONE >> Infrastructur >> 192.168.1.10 	_11n_Router <> (Power:100%) Hz; central chann re 1	00-E0-4C-86-51-01	Link Speed >>	Signal St Noise : 135.0 Mbps	rength 1 >> 100%	
Status Extra Info Channel Authentication Encryption Network Type IP Address	 > Cherry_test_ >> Link is Up [Tx >> 7 <> 2442 M >> Open >> NONE >> Infrastructur >> 192.168.1.10 >> 255.255.255. 	_11n_Router <> (Power:100%) Hz; central chann re 1 0	00-E0-4C-86-51-01	Link Speed >> Throughput >>	Signal St Noise : 135.0 Mbps	rrength 1 >> 100% Strength >> 26%	
Status Extra Info Channel Authentication Encryption Network Type IP Address Sub Mask	 > Cherry_test_ >> Link is Up [Tx >> 7 <> 2442 M >> Open >> NONE >> Infrastructur >> 192.168.1.10 >> 255.255.255. 	_11n_Router <> (Power:100%) Hz; central chann re 1 0	00-E0-4C-86-51-01	Link Speed >> Throughput >> Receive	Signal St Noise : 135.0 Mbps • 0.000 Kbps	Max 0.192 Kbps	
Status Extra Info Channel Authentication Encryption Network Type IP Address Sub Mask	 Cherry_test_ Link is Up [Tx 7 <> 2442 M Open NONE Infrastructur 192.168.1.10 255.255.255. 192.168.1.19 	_11n_Router <> (Power:100%) Hz; central chann re 1 0	00-E0-4C-86-51-01	Link Speed >> Throughput >>	Signal St Noise : 135.0 Mbps • 0.000 Kbps	strength 1 >> 100% Strength >> 26% Max 0.192	

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.
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.
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.

🖌 Inte	lligent Wireless	Utiltiy							
	Profile	Land Hetwork	کی Advanced	Statistics	N	Ø WPS	Radio On/Off	About	
Wire	eless mode >>	2.4G	•		Turn on	CCK₩ ladio Measureπ	ne eXtensions) nents el Measurements limit		
	Enable TX Burst Enable TCP Windo Fast Roaming at Show Authenticat Select You 18/G	-70 dBm	-		25	0 ms (0-2000	1)		
	Apply								•

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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.
Apply	Click to apply above settings.

Statistics

Profile 1	Vetwork	Advanced	Statistics	oos WMM	Ø WPS	Radio On/Off	About
ansmit	Receive						
Frames Tran	smitted Succe	essfully		-	30	0836	
Frames Retra	ansmitted Suc	cessfully		=	30	0836	
Frames Fail T	o Receive ACI	K After All Retries		-		174	
RTS Frames S	iuccessfully Re	eceive CTS		=		0	
RTS Frames F	ail To Receive	• CTS		=		0	
t Counter							

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

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 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.

崔 Intelligent Wireles						×		
Profile	Land Hetwork	کی Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
Transmit 🕻	Receive	>						
Frames Rec	ceived Successful	ly		-	15	41		
Frames Rec	ceived With CRC I	Error		=	6	27		
Frames Dro	opped Due To Out	-of-Resource		=		0		
Duplicate F	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.

🖌 Intelligent Wireless Utiltiy						
Profile Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About
WMM Setup Status						
WMM >> Enabled	Power Save >	>> Disabled		Di	irect Link >> Disabled	
📶 WMM Enable						
WMM - Power Sav						
AC_BK	AC_BE	AC_VI	AC	_YO		
Direct Link Setup	Enable		The second Markers			
MAC Address >>			Timeout Value :	>> 60 se		
					App	ly.
					Tear D	lown
WMM Enable					function that is	
			•	•	transmitted over	
WMM- Power Save Enable			want to ena gory Backgr		wer saving mod	le.
LIADIC			gory Best Ef			
		ccess Categ		1011)		
	AC_VO (A	Access Cate	gory Voice)			
Direct Link Setup Enable	Check the	box to enab	le Direct Lii	nk Setup.		
MAC Address	The setting	g of DLS(D	irect Link S	etup) indi	cates as follow	:
				ith MAC	Address of STA	A, and the STA
		orm to two c		.1 .		
		cting with ti nabled.	ne same AP	that suppo	orts DLS feature	Э.
Timeout Value			ents that it d	isconnect	automatically a	fter few
Thirebut Value		-			etween 0~65535	
			0		Default value of	-
	Value is 60) seconds.				
Apply	Click this b	outton to ap	ply the setting	ngs.		
Tear Down	Select a din STA.	rect link ST.	A, then clicl	k "Tear Do	own" button to o	disconnect the

<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.

e h	ntelligent Wire	less Utiltiy						×
	Profile	LLL Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About
			WF	PS AP List				
			WPS	Profile List			L	Rescan Information Pin Code 912113 Renew onfig Mode
•	Cherry_test_11n	_Router					Er	rollee
<								Detail Connect
	PIN	🖉 WPS Associate I	E		Progress >> 10)0%		Rotate
1000	PBC	WPS Probe IE	PBC - G	iet WPS profile suc	cessfully.			Disconnect
		Auto	,					Export Profile
								Delete

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 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.

	T				
	Intelligent Wireless Utility				
	Profile Network Advanced Statistics WWW WPS Radio On/Off About				
	WPS AP List Rescan				
	rescan				
	16912113 Renew				
	WPS Prome List Cherry_test_11n_Router Enrollee				
	Connect				
	PIN WPS Associate IE Progress >> 100% Rotate PBC WPS Probe IE PBC - Get WPS profile successfully. Disconnect				
	Auto Export Profile Delete				
	SSID >> Cherry_test_11n_Router				
	BSSID >> 00-0C-43-30-70-00				
	Authentication Type >> OPEN Encryption Type >> NONE				
	Key Length >> Key Index >>				
	Key Material >>				
	Show Password				
	OK Cancel				
	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 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.		
PBC	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.



<u>About</u>

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

Ņ	Intelligent Wireles	s Utiltiy							×
	Profile	Land Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
		Conf	ig Version >>	2.1.3.0		Date >> 05	5-16-2008		
		Drive	er Version >>	1.1.2.8		Date >> 05	5-07-2008		
		EEPRO	M Version >>	1.0	Firmware Ve	ersion >> 0.	9		
		Phy	/_Address >>	00-0C-43-30-70-00					
									-

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.

Soft AP mode

Config

Config Access Control Mac Table Event Log Statistics About SSID Intelligent Channel Image:	🖌 Intelligent Wireless Utility	
Wireless Mode 2.4G <use address<="" mac="" th=""> Security Setting Country Region Code In B/G No forwarding among wireless clients Hide SSID 11 B/G 0: CH1-11 In Hide SSID Hide SSID Beacon (ms) 100 Tx BURST Idle time(60 - 3600)(s) 300</use>	Config Access Control Mac Table Event Log	Statistics About
11 B/G 0: CH1-11 Image: High state stat		· - · · · · · · · · · · · · · · · · · ·
TX Power 100 % 💽 Idle time(60 - 3600)(\$) 300	11 B/G 0: CH1-11	☐ Hide SSID ✓ Allow BW 40 MHz
Default	TX Power 100 %	
		Default Apply

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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.					
	Security Setting					
	Authentication Type Open 💌 Encryption Type Not Use					
	WPA Pre-shared-Key					
	Group Rekey Interval 60 10 seconds					
	Wep Key					
	© Key#1 Hex ▼ C Key#2 Hex ▼					
	C Key#3 Hex V					
	C Key#4 Hex 💌					
	* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters * WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters					
	Show Password					
	OK Cancel					
	Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK.					
	 Encryption Type: For Open and Shared authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK, and WPA-PSK/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 and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths. 					
	Group Re-key Interval : Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. User can set to change by seconds or packets. Default is 600 seconds.					
	 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.			

Access Control

Config Access Co		Log Statistics About	
Cornig Theodore Co.	Inter Liniac Laple Lin Activ		
Access Policy		Disable	•
MAC Address		Access List	
	Add		
	Delete		
	Remove All		
		1	And
			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.		

AddAdd 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

MAC Address	AID	Power S	Status
<			2

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.	

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.

Statistics

Intelligent Wireless Utility		٥
Config Access Control Mac Table Event Log St	atistics 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
	R	SET COUNTERS

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.	

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.	

<u>About</u>

This page displays the wireless card and driver version information.

<mark>/</mark> Intel	lligent Wireless Ut	ility		Σ
Config	Access Control Mad	c Table Event Log	Generatistics 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	irmware Version :	0.9
Γ	IP Address :	192.168.123.1	Phy_Address :	00-0C-43-30-70-00
	Sub Mask :	255.255.255.0	Default Gateway :	
L				

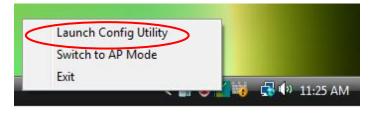
Utility Configuration for Windows Vista

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.



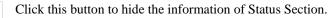
Station Mode

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.



MI Inte	ligent Wireless l	Jtiltiy							X
	P	Network	کی Advanced	Statistics	WMM	() WPS	Radio On/Off	About	
ie		Prot	file Lis <mark>t</mark>		- 4011				
PR	DF1	Cherry_test_	11n_Router		6	Profile Name >	> PROF1		
						SSID	observe to the st th	outer	
						Network Type :	Infrastructure		
						Authentication	>> Open		
						Encryption	> None		
						Use 802.1x :	> NO		
						Tx Power	>> Auto		
						Channel	>> Auto		
						Power Save Mode :	>> CAM		
						RTS Threshold :	»> 2347		
Contraction of	Add	Edit	Delete	Activate	Fr Fr	agment Threshold >	»> 2346		
1								6	-

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.
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.
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:

Profile	Network	Advanced	Statistics	Gos WMM	() WPS	Radio On/Off	A
	Profile	e List					
PROF1	Cherry_test_11	1n_Router		\$	Profile Name >		
						> Cherry_test_11n_R	louter
					Network Type > Authentication >	> Infrastructure	
					Encryption >		
					Use 802.1x >		
					Tx Power :		
				Re	Channel : wer Save Mode >		
				10			
Add	Edit	Delete	Activa	te Frag	RTS Threshold > ment Threshold >		
System Config			021X	te Frag	nent Threshold >	> 2346	
System Config Profile N	Auth. \ Encry	. 80	021X		nent Threshold >	> 2346	
System Config Profile N	Auth. \ Encry	. 80	J21X	Network Type >>	ment Threshold > Infrastr Aut	> 2346 ucture	
System Config Profile N	Auth. \ Encry	. ac	J21X	Network Type >> Tx Power >>	nent Threshold > Infrastr Aut	> 2346 ucture	
System Config Profile N Power S	Auth. \ Encry Iame >> PROF1 SSID >> Cherry_test_	. 80 .11n_Router M @ PSN	J21X	Network Type >> Tx Power >>	nent Threshold > Infrastr Aut	> 2346 ucture	
System Config Profile N Power S	Auth. \ Encry lame >> PROF1 SSID >> Cherry_test_ Save Mode >> CA	. 80 .11n_Router M @ PSN	721X	Network Type >> Tx Power >> Preamble >>	ment Threshold > Infrastr Aut	> 2346 ucture	

Profile Name: User can enter profile name, or use default name defined by system. The default is PROF# (# 1, #2, #3....).

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.

Network Type: There are two types, Infrastructure and Ad hoc modes.

- 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 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 activated if the data size exceeds the value you set</u>. 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:

Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About
	P	rofile List					
PROF1 Add	Cherry_te: Edit	t_11n_Router Delete	Activate	Pov		 Cherry_test_11n_Rc Infrastructure Open None NO Auto Auto CAM 2347 	uter
WPA	ig Auth. \ E Authentication >> Preshared Key >> Wep Key	ncry. 8 Open v	021X Encryp	tion >> N	one 🔻	802.1×	
	 Key#1 Key#2 Key#3 	Hexadecimal Hexadecimal Hexadecimal	* 1			Show Pass	word

Authentication Type: There are six type of authentication modes including Open, Shared, WPA, WPA-PSK, WPA2 and WPA2-PSK.

- **Open**: If your access point/ wireless router is using "**Open**" authentication, then the wireless adapter will need to be set to the same authentication type.
- **Shared**: Shared key is when both the sender and the recipient share a secret key.
- WPA/WPA-PSK/WPA2/WPA2-PSK: WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8-63 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 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:

Intelligent Wireless Utility
Profile Network Advanced Statistics WMM WPS Radio On/Off About
Profile List
PROF1 Cherry_test_11n_Router Profile Name >> PROF1 SSID >> Cherry_test_11n_Router SSID >> Cherry_test_11n_Router Mathematical Construction SSID >> Cherry_test_11n_Router Add Edit Delete Activate Profile Name >> PROF1 SSID >> Cherry_test_11n_Router Network Type >> Infrastructure Authematication >> Open Encryption >> None Use 802.1x>> NO Tx Power >> Auto Channel >> Auto Power Save Mode >> CAM RTS Threshold >> 2347 Fragment Threshold >> 2346
Sustem Config Auth \ Encry 8021Y EAP Method >> PEAP Tunnel Authentication >> FAP-MSCHAP v2 Session Resumption
EAP Method >> PEAP ▼ Tunnel Authentication >> EAP-MSCHAP v2 ▼ Session Resumption
Authentication ID / Password
Identity >> Password >> Domain Name >>
Tunnel ID / Password
Tunnel ID >> Tunnel Password >> Show Password
OK Cancel
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.
Protocol : Tunnel protocol, List information including EAP-MSCHAP v2 and EAP-TLS / Smart Card .
Tunnel Identity: Identity for tunnel.
Tunnel Password: Password for tunnel.
ession Resumption: Reconnect the signal while broken up, to reduce the tacket and improve the transmitting speed. User can click the box to enable disable this function.
PASSWORD tab:

	System Config Auth. \ Encry. 8021X
	EAP Method >> PEAP Tunnel Authentication >> EAP-MSCHAP v2 Session Resumption
	ID \ PASSWORD Client Certification Server Certification
	Authentication ID / Password
	Identity >> Password >> Domain Name >>
	Tunnel ID / Password
	Tunnel ID >> Tunnel Password >> Show Password
	OK Cancel
]	ID/ PASSWORD: Identity and password for server.
	• Authentication ID / Password: Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
	• Tunnel ID / Password: Identity and Password for server.
	Show Password: Check this box to show the password you entered.
L L	non a assivera. Check and box to show the password you childred.
	OK : Click to save settings and exit this page.
	Cancel: Click to call off the settings and exit.
	Client Certification tab:
	System Config Auth. \ Encry. 8021X
	EAP Method >> PEAP Tunnel Authentication >> EAP-MSCHAP v2 EAP Session Resumption
	ID \ PASSWORD Client Certification Server Certification
	Ouse a certificate on this computer
	Issued To >>
	Issued By >> Expired On >>
	Friendly Name >>
	Use my smart card
	OK Cancel
	You can select Use a certificate on this computer , a client certificate for server authentication. Or you can select Use my smart card to enable the Client 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 Method >> PEAP Tunnel Authentication >> EAP-MSCHAP v2 Session Resumption
	ID \ PASSWORD Client Certification Server Certification
	Use certificate chain
	,
	Server name >>
	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. 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.

Profile	Network	Advanced	Statistics	Qos WMM	() WPS	Radio On/Off	About
Sorted by >>	SSID	Chan	inel 🥝			Show dBm	
Cherry_test_11n_R	louter	67	B910	100%			
Abocom-Wireless		11	bg	86%			
airlive-wl5470poe		11	g	50%			
skl		10	g	44%			
Abocom-Wireless		6	bg	29%			
PINGOO		11	bg	24%			
802.11g-AP		6	B9	15%	1		
Rescan	Add to Profile						

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.			
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:

SSID >>	Cherry_test_11n_Router	
MAC Address >>	00-E0-4C-86-51-01	Signal Strength >> 100%
Authentication Type >>	Unknown	
Encryption Type >>	None	Supported Rates (Mbps)
Channel >>	7 <> 2442 MHz	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
Network Type >>	Infrastructure	
Beacon Interval >>	100	
	100	Close

	Supported Rates.								
WPS	Close: Click this button to exit the information screen.								
	General WPS CCX 802.11n								
	Authentication Type >> Unknown State >> Configured								
	Encryption Type >> None Version >> 1.0								
	Config Methods >> 0x0086 AP Setup Locked >>								
	Device Password ID >> UUID-E >> 6304125310192006122800E04C865101								
	Selected Registrar >> Unknown RF Bands >> Unknown								
	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 fo 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 encoified version								
	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.								
CXX	General WPS CCX 802.11n								
	CCKM >> FALSE Cmic >> FALSE								
	Ckip>> FALSE								
	Close								
	CCX information contains CCKM, Cmic and Ckip information.								

Secondary Channel Offset element		
Secondary Channel Offset	0	E
Extended Capabilities information element		
HT Information Exchange Support	FALSE	
Neighbor Report element		
Mobility Domain	FALSE	
High Throughput	FALSE	
HT Capabilities element		
HT Capability	TRUE	
LDPC Coding Capability	FALSE	
Supported Channel Width Set	1	-
511 D 5	2	127 T
	Close	
This tab will show up if you select		

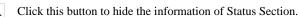
Link Status

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.





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.
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.

	Utiltiy							
Profile	Network	Advanced	Statistics	Gos WMM	() WPS	Radio On/Off	About	
Vireless mode >>	2.4G	•						
Easter TV Pure								
Enable TX Burs Enable TCP Wi Fast Roaming	indow Size							
Enable TCP Wi	indow Size	on Code	-					

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.



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	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.

📔 Intelligent Wireless U	Jtiltiy							X
P		<u> </u>		Gos	0	8	e	
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
Transmit	Receive							
Transmit	Receive							
Frames T	ransmitted Succe	ssfully		=		1294		
Frames R	etransmitted Suc	cessfully		=		1294		
Frames F	ail To Receive ACI	(After All Retries		-		15		
RTS Fram	es Successfully Re	eceive CTS		-		0		
RTS Fram	es Fail To Receive	CTS		-		0		
Reset Counter								
								-

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 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	leceived Successfu	lly	:			452	
Frames R	Received With CRC	Error	=		731		
Frames D	Propped Due To Ou	t-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.					

WMM / QoS

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

	-63-					
Network	Advanced	Statistics	WMM	W PS	Radio On/Off	About
nabled	Power Save >	> Disabled		Di	irect Link >> Disabled	
M Enable WMM - Power Save	Enable					
AC_BK	AC_BE	AC_VI	AC_VO			
Direct Link Setup E	inable		Timeout Value >>	60 se	c	
					Apr	ky
					Tear	Down
	M Enable WMM - Power Save AC_BK Direct Link Setup E	M Enable WMM - Power Save Enable AC_BK AC_BE Direct Link Setup Enable	M Enable WMM - Power Save Enable AC_BK AC_BE AC_VI Direct Link Setup Enable	M Enable WMM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable	M Enable WMM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable	A Enable WAM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable

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. 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.

Intelligent Wireles	s Utiltiy							(
P	Network	Advanced	Statistics	WMM	Ø WPS	Radio On/C	Off Abo	ut
		W	PS AP List				Reso	
ID:	Cherry	_test_11n_Route	r	00-E0-4C-86-51-01	7	,	Inform	16,290
							Pin C	ode
							57055251	Renew
•		WPS	Profile List —				Config Mo	de
Cherry_test_11	n_Router						Enrollee	•
							Det	ail
	10		m			•	Conn	ect
PIN	WPS Associate	IE		Progress >> 100%			Rota	ite
PBC	WPS Probe IE	PBC - C	Get WPS profile s	uccessfully.			Discon	
							Export	
							Dele	te

WPS Tab	
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 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.
	Intelligent Wireless Utility
	Profile Network Advanced Statistics WMM WPS Radio On/Off About
	ID: Cherry_test_11n_Router 00-E0-4C-86-51-01 7 Information Pin Code
	WPS Profile List Config Mode
	Cherry_test_11n_Router
	PIN WPS Associate IE Progress >> 100% Connect PBC @ WPS Probe IE PBC - Get WPS profile successfully. Disconnect
	Export Profile Delete
	SSID >> Cherry_test_11n_Router
	BSSID >> 00-E0-4C-86-51-01
	Authentication Type >> OPEN Encryption Type >> NONE Key Length >> Key Le
	Key Length >> Key Index >> Key Material >>
	Show Password
	OK Cancel
	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 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.

MI Intell	igent		-						x
	Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
?	This ico	n shows radi	o on, click t	o turn it off.					
1	This ico	n shows radi	o off, click t	o turn it on.					

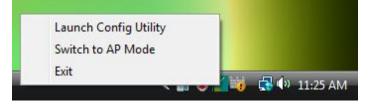
About

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

Markellig	gent Wireless l	Jtiltiy							X
			Ĩ		QoS	0	?	A	
	Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
		Drive	ig Version >> er Version >> M Version >> y_Address >>	2.1.3.0 2.1.6.7 1.0 00-0C-43-30-70-00	Date Date Firmware Version	>> 05	-16-2008 -02-2008		•

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

SSID Inte Wireless Mode 2.4	elligent G		unnel 1 _	Security Setting
Country Region Code 11 B/G 0: CH1-		<u> </u>	 □ No forwarding amo □ Hide SSID □ Allow BW 40 MHz 	ong wireless clients
Beacon (ms)		100		
TX Power	100 %	•		
Idle time(60 - 3600)(s)		300		
			Default	Apply

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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.
	Security Setting
	Authentication Type Open Encryption Type Not Use
	WPA Pre-shared-Key
	Group Rekey Interval 60 10 seconds
	Kep Key
	С Кеу#2 Нех т
	* WEP 64 Bits Encryption. Please Keyin 10 HEX characters or 5 ASCII characters *
	WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters
	C Show Password
	OK Cancel
	 Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. Encryption Type: For Open and Shared authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections of encryption type are Not Use and WEP. For WPA-PSK, WPA2-PSK authentication mode, the selections approximately approximate
	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 and WPA2-PSK (WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.
	Group Re-key Interval : Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK authentication mode to renew key. User can set to change by seconds or packets. Default is 600 seconds.
	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.

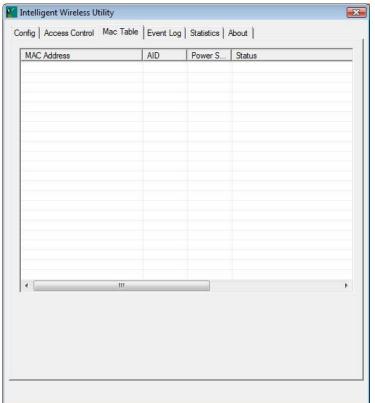
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. The system default is no forwarding.
Hide SSID	Do not display AP name. System default no hide.
Allow BW 40MHz	Click to disable this function. Default is enabling.
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control

Access Policy		Disable	
MAC Address		Access List	
	Add		
	Delete		
	Remove All		
			Apply

Access Contro	l
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.
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



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.

Event Log

Event Time (yy/mm/dd-hh:mm:ss)	Message	
2008 / 06 / 06 - 11 : 26 : 49	Restart Access Point	
2008 / 06 / 06 - 11 : 26 : 50	Restart Access Point	
2008 / 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.			

Statistics

Transmit Statistics		
Frames Transmitted Successfully	= 331	
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	= 206	
Frames Received With CRC Error	= 123	
Frames Dropped Due To Out-of-Resource	= 0	
Duplicate Frames Received	= 0	
	RESET COUNT	ERS
Frames Received With CRC Error Frames Dropped Due To Out-of-Resource	= 123 = 0 = 0	

T				
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.			
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.

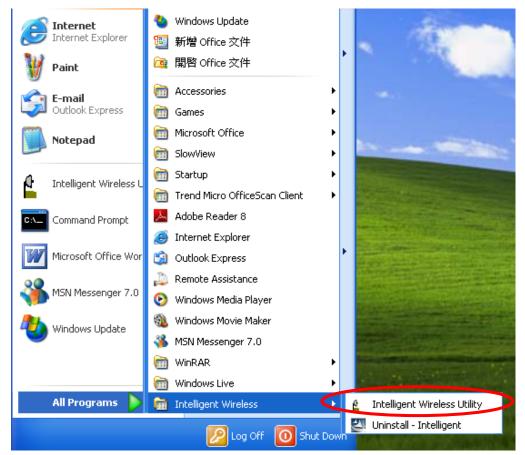
ſ	Utility Version :	2.0.2.1	Date :	05-16-2008
	Driver Version :	2.1.6.7	Date :	05-02-2008
	EEPROM Version :	1.0	Firmware Version :	0.9
Ī	IP Address :	192.168.123.1	Phy_Address :	00-0C-43-30-70-00
	Sub Mask :	255.255.255.0	Default Gateway :	0.0.0.0

Chapter 4: Uninstallation

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.)

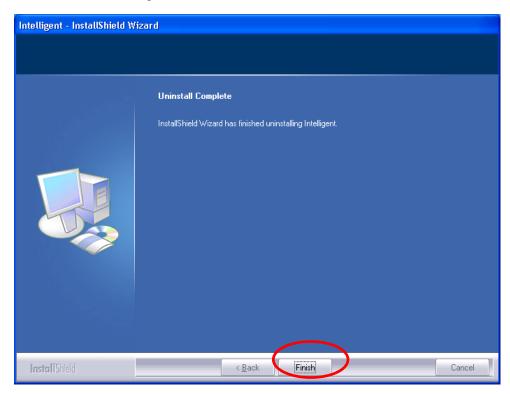
1. Go to Start →All Programs →Intelligent Wireless → Uninstall –Intelligent.



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

Intelligent - InstallShield Wizard	\times
Do you want to completely remove the selected application and all of its feature Yes No	es?

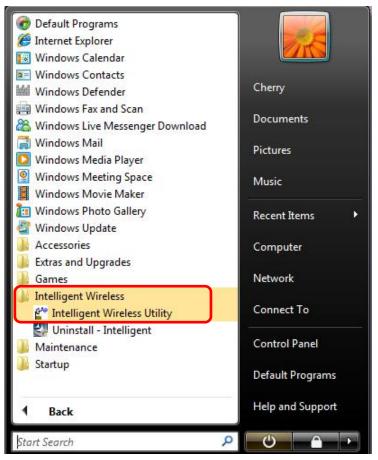
3. Then click **Finish** to complete the uninstallation.



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.)

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



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

Intelligent - InstallShield Wizard	23
Do you want to completely remove the selected application and all of its features?	
<u>Y</u> es <u>N</u> o	

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

