

WM5204Z

Wireless LAN USB 2.0 Adapter

User's Manual

Release 2.0

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 to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

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

channels 1 through 11.



This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna,

3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ASDL modems, and similar equipment). The final end product must be labeled in a visible area with the following: "Contains TX FCC ID: **I88WM5204Z**

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how

to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

注意!

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機,非經許可,公司、商號或使用 者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現 有干擾現象時,應立即停用,並改善至無干擾時方得繼續使用。 前項合法通信,指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信 或工業、科學及醫療用電波輻射性電機設備之干擾。

<u>本模組於取得認證後將依規定於模組本體標示審合格籤,並要求平台上標示「本</u>產品內含射頻模組:ID編號」

About this manual

This User's Manual describes how to install and operate your 802.11b/g Wireless LAN Module. Please read this manual before you install the product. This manual includes the following topics:

- I Product description and features.
- I Software installation procedure for certification use

Table of Contents

CHAPTER 1: INTRODUCTION	1
Features	1
CHAPTER 2: INSTALLATION	2
For Windows 2000/XP	2
Install the Software	2
Install the Hardware	4
Verification	
For Windows Vista	
Install the Software	
Install the Hardware	
Verification	
Network Connection	9
IP Address	9
For Linux Kernel 2.4/2.6 Installation	
Install the Hardware	
Install the Software	
For Mac OS 10.5 Installation	
Install the Software	
Install the Hardware	
CHAPTER 3: UTILITY CONFIGURATION	14
For Windows 2000/XP	14
Station Mode	
Utility Menu List	
Soft AP mode	
For Windows Vista	
Station Mode	
Utility Menu List	
Soft AP mode	
CHAPTER 4: UNINSTALLATION	
For Windows 2000/XP	6E
FOR WINDOWS 2000/AP FOR WINDOWS VISTA	
For Mac OS 10.5	
For Linux Kernel 2.4/2.6	

Chapter 1: Introduction

The Wireless LAN Module is an IEEE802.11b/g Module that connects your notebook to a wireless local area network. The Wireless LAN Module fully complies with IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance. 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

- \emptyset 1T1R Mode with 54Mbps PHY Rate for both.
- Ø Complies with IEEE 802.11 b/g standards.
- Ø Supports WEP 64/128 bits, WPA, WPA2.
- Ø Supports WMM and WMM-PS.
- Ø Supports WPS configuration.
- Ø Portable and mini-size design.
- Ø Compatible with Microsoft Windows 2000/XP/Vista, Mac OS 10.3/10.4/10.5, and Linux Kernel 2.4/2.6 operating systems.

Chapter 2: Installation

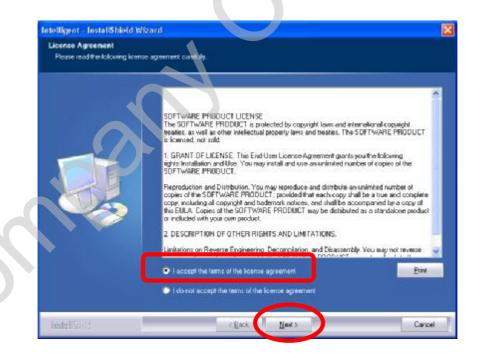
For Windows 2000/XP

Install the Software

Note:

Do not insert the Wireless LAN Module into the computer until the Install Shield Wizard has finished installing.

- 1. Exit all Windows programs. Insert the included Installation CD into the 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.



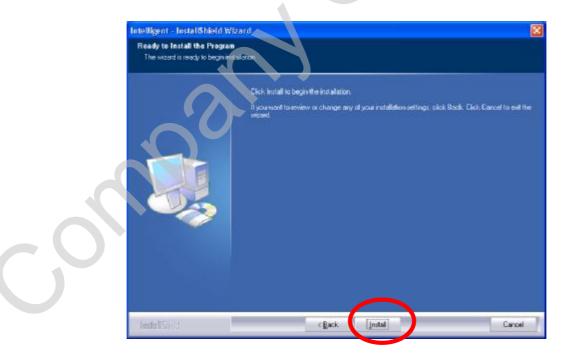
- 3. Select the check box to choose a **Configuration Tool** from the listed two choices.
 - **I** Configuration Tool: Choose to use the configuration utility.

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

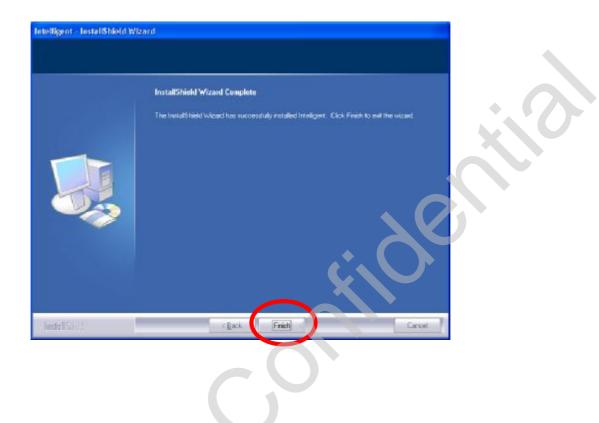
Click Next to continue.

Intelligent - InstallShield & Setup Type Select the setup type that bes		
	Select Configuration Tool Configuration Tool Microsoft Zero Configuration Tool	
InstallSind	CEACH. List 2	Carcel

5. When prompt to 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 LAN Module after software installation.

Insert the Wireless LAN Module into the computer. The system will automatically detect the new hardware.

Verification

To verify if the device is active in the computer. Go to **Start > Setting > Control Panel > System**

> Hardware > Device Manager. Expand the Network Adapters category. If the 802.11b/g

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

🚇 Device Manager	
File Action View Help	<u>.</u> (
W000-CHERRY-XPE Batteries Computer Source Disk drives Disk drives Display adapters Modems Display adapters Display adapters	
■ ■ Realtek RTL8139 Family PCI Fast Ethernet NIC	
PCMCIA adapters Ports (COM & LPT)	
Processors	

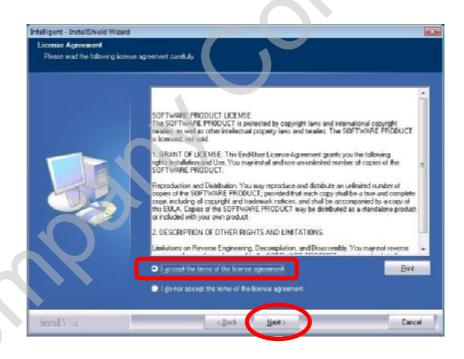
For Windows Vista

Install the Software

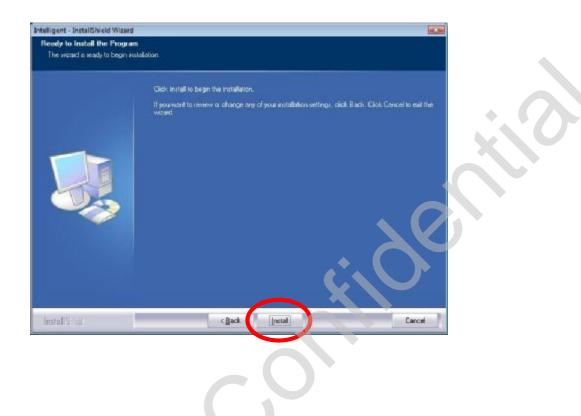
Note:

Do not insert the Wireless LAN Module into the computer until the Install Shield Wizard has finished installing.

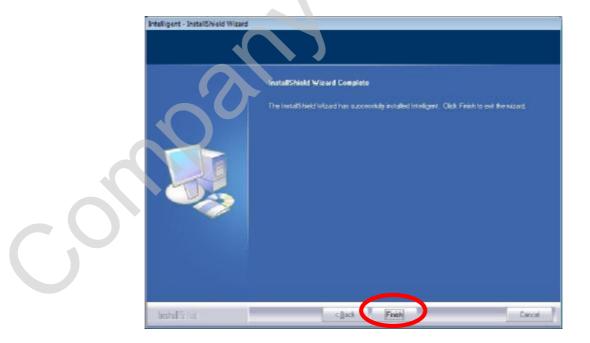
- 1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically.
- 2. When the License Agreement screen appears, please read the contents and select "I accept the terms of the license agreement " then click Next to continue.



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



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



Install the Hardware

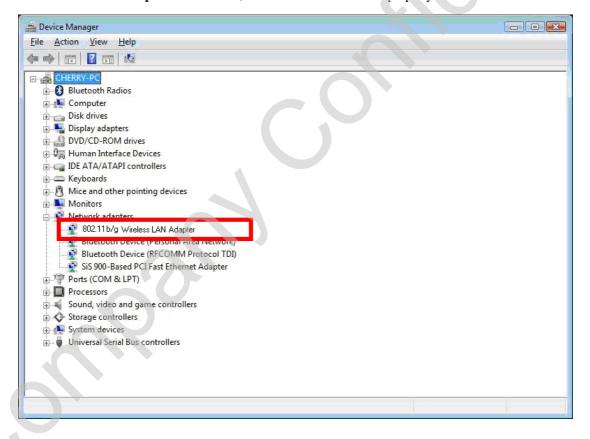
Note:

Insert the Wireless LAN Module when finished software installation.

Insert the Wireless LAN Module into the computer. The system will automatically detect the new hardware.

Verification

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



Network Connection

IP Address

Note:

When assigning IP address(es) to computers on the network, remember to have IP address for each computer set on the same subnet mask. If the Broadband Router has enabled its DHCP server function, it won't be necessary to assign static IP address for PC.

- 1. To configure a dynamic IP address (i.e. if the broadband Router has enabled the DHCP server funciton), check the **Obtain an IP address automatically** option.
- To configure a fixed IP address (if DHCP server function is not enabled in Broadband Router, or when PC needs to be assigned 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, 255.255.255.0 for the Subnet Mask, and 192.168.1.254 for the default gateway.

eneral Alternate Configuration	General	
You can get IP settings assigned automatically if your network supports his capability. Otherwise, you need to ask your network administrator for he appropriate IP settings.		d automatically if your network supports eed to ask your network administrator fo
Obtain an Fraduress automatically	Obtain an IP address autor	matically
O Use the following IP address:	Use the following IP addres	ec.
IP address:	IP address:	192.168.1.1
Subnet mask:	Subnet mask:	255 . 255 . 255 . 0
Default gateway:	Default gateway:	192 . 168 . 1 . 254
Obtain DNS server address automatically	O Obtain DNS server address	s automatically
O Use the following DNS server addresses:	 Use the following DNS service 	ver addresses:
Preferred DNS server.	Preferred DNS server:	
Alternate DNG server	Alternate DNS server:	· · ·
Advanced		Advanced.
	L	OK Can

For Linux Kernel 2.4/2.6 Installation

Install the Hardware

Note:

Please insert the Wireless LAN Module into the PC USB port BEFORE the driver installation.

Install the Software

Please execute the Terminal program and follow the steps below to install the driver of Wireless LAN Module.

		root@localhost:-	_ 0
	liew Ierminal	Tabs Help	
[root@loca]	lhost ~]# 📕		
	0		

cd DRIVER

cp xxx_RT3070_Linux_STA_x.x.x.tar.bz2 /home/DRIVER

2. # tar -jxvf xxx_RT3070_Linux_STA_x.x.x.tar.bz2

go to "./xxx_RT3070_Linux_STA_x.x.x.x" directory.

3. # make clean

4. # make

PS: If there is ERROR Message after compile, then user may need to recheck the Makefile or .c and .h

5. # cd /etc/Wireless/

6. # mkdir RT2870STA

7. go to "./home/DRIVER/xxx_RT3070_Linux_STA_x.x.x." directory

8. # cp RT2870STA.dat /etc/Wireless/RT2870STA/RT2870STA.dat

9. go to "./home/DRIVER/xxx_RT3070_Linux_STA_x.x.x/os/linux/" directory.

Load driver

[kernel 2.4]

#/sbin/insmod rt3070sta.o

#/sbin/ifconfig ra0 inet YOUR_IP up

[kernel 2.6]

#/sbin/insmod rt3070sta.ko

#/sbin/ifconfig ra0 inet YOUR_IP up

Unload driver

#/sbin/ifconfig ra0 down

#/sbin/rmmod rt3070sta

10. Scan AP

iwlist ra0 scanning

11. Connect to AP

iwpriv ra0 set SSID="AP's SSID'

12. Check status

iwconfig ra0 or # ifconfig ra0

Note:

- Supporting Kernel: Linux kernel 2.4 and 2.6 series. Tested in Redhat
 7.3 or later.
- 2. Clear DHCP on ra0
 - # killall dhclient
- 3. Get DHCP from AP # dhclient ra0

For Mac OS 10.5 Installation

Install the Software

Note:

Do not insert the Wireless LAN Module into the computer until the installation finished.

- 1. Insert the included CD-ROM into the CD-ROM drive of your computer. Please find and execute the xxx.dmg file, then select the install Mac version of your PC, and click the USBWireless-Leopard.pkg file to install.
- 2. When the Welcome screen appears, click **Continue** to start.



3. Please click Install to process the installation.



	Go Back	Install
--	---------	---------

4. The computer restart message will show up, please click Continue Installation to install.



5. After finished the installation, please click **Restart** to complete the installation.



Note: Mac OS support version 10.3, 10.4, 10.5.

Install the Hardware

Note:

Insert the Wireless LAN Module when finished software installation.

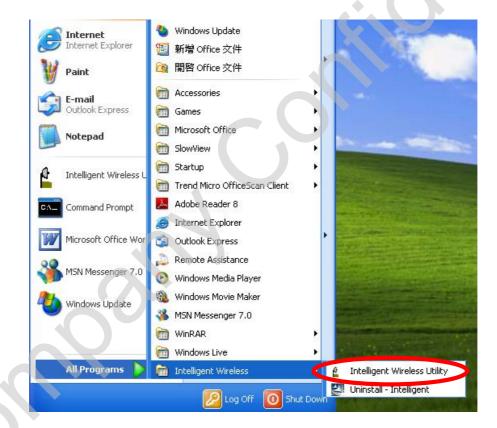
Insert the Wireless LAN Module into the USB Port of the computer. The system will automatically detect the new hardware.

Chapter 3: Utility Configuration

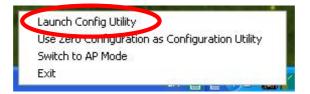
For Windows 2000/XP

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

Go to Startg (All) Programg Intelligent Wirelessg Intelligent Wireless Utility.



Users can also open the Configuration Utility by double clicking or right clicking the icon in the task tray to select **Launch Config Utility**.



Station Mode

IMPORTANT NOTICE:

Under screen resolution 800 x 600 pixels, if users click the triangle button, at the lower right corner of the utility window, to expand the station linking information, it will NOT be displayed completely.

Profile

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add, 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	elligent Wirele	ess Utiltiy							
	Profile	Jetwork	ر Advanced	Statistics	WWW	Ø WPS	Radio On/Off	About	
		Pro	file List ———						
PF	ROF1	Cherry_test_	Router		8	Profile Name :	>> PROF1		
							>> Cherry_test_Router		
						Network Type	>> Infrastructure		
					1	Authentication	>> Open		
						Encryption	>> None		
						Use 802.1x	>> NO		
						Tx Power	>> Auto		
						Channel	>> Auto		
					Pot	wer Save Mode	>> CAM		
<u> </u>						RTS Threshold	>> 2347		
-	Add	Edit	Delete	Activate	Fragn	nent Threshold	>> 2346		
								1	

Profile Tab	
Profile Name	Here shows 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 wireless access points in the wireless network.
Network Type	Shows the network type of the device, including Infrastructure.
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	Click to add a profile from the drop-down screen.

System Configuration tab:

2.1	colligent Wirek	or Office							
	- 101 Pc	LLL Notwerk	💣 Adžai ted	ale is in		🖉 De	in chroi	je 2011.	
_		P a	14 ··· t						
	PSOF1	George Maria	plater -		¢ :	of 6 (100 × 200)			
						CODE - Char Indi Tense - Indi A	rj_Jack_Route din od je		
						here the state			
						Frankrich (* 4455) 1946 - 1957 (* 4455)			
						ан нь нь 1997 година - Кал			
/					٣	7 Throate dive 2047			
	ut	11	:-inho		Гқти	k Threetic 3 - + 50%.			
1	Alternative state	a state and	v <u>v 1999</u>						1
L	Profile Har	ar (19594)			Hohamik Type ik	I-1 s - n	-		
L	~	ow Gary_M	-Jane	-	The Design of the	ALC:	•		
L					President 1		-		
	Participation -	***** 🔅 '	u						
	□ R ⁻¹	h-put	т. –		<u>1 viz</u>	100			
	🗆 tis	an Chicker	¥15 -			2046			
1				*	Carson			/	

Profile Name: Users 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 wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network. Users can use pull-down menu to select from available access points.

Network Type:

The **Infrastructure** is intended for the connection between wireless network cards and an access point. With the Wireless LAN Module, users can connect wireless LAN to a wired global network via an access point.

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.

	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. (Default power save mode is CAM.)	
	• 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.	
	RTS Threshold : Users 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 values that have been set.</u>	0
	This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.	
	Fragment Threshold : Users 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 the Wireless LAN Module often transmits large files in wireless network, users 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 Auft-100mm, end Auft-100mm, open Cocryption to None More Document WRAFECUINSUBSY * Present Present of T Present Present Present of T Present Present Pres	
	Authentication Type: There are several types of authentication modes including Open, Shared, Leap, WPA, WPA-PSK, WPA2 and WPA2-PSK.	
	• Open : If the access point or wireless router is using " Open " authentication, then the Wireless LAN Module 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.	
G	• 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 key 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 four formats to enter the keys. • ASCII (64 bits): 5 ASCII characters (case sensitivity). • ASCII (128 bits): 13 ASCII characters (case sensitivity). • Hexadecimal (64 bits): 10 Hex characters (0~9, a~f). • Hexadecimal (128 bits): 26 Hex characters (0~9, a~f). Show Password: Check this box to show the passwords that have been entered. 802.1x Setting: When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method- MD5-Challenge). 802.1x tab: desi (URB) Intelligent Wi N. NU IS ात्र स्टार्थ्य स्टार्थ M Ŷ Tadu Chrof ê. Alu Network stelling in Plotte int 104 × 20014 わ 15.051 الديكي بياريز Gau CODE - Chain, Jack 4 n. Rocker root Track Infactor a Henrice Color Den verste sie den Potentische Noter in 1999 MR Threche dies 2045 ---ent Threats 31 - 504 -----11.2.3 Pursel (Altheory packed as Principal and 🔲 Seen Warrich 19-1 In 1953-4680 Gint Car first in Some Car first in Automostics II - Formers Densh Skile () G. 6.0 Assound in The Line section Turne Faceto di -Costorado ж Cance EAP Method: • PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless

• **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

LAN clients using only server-side certificates, thus simplifying the

implementation and administration of a secure wireless LAN.

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.
- **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 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. Users can click the box to enable or disable this function.

ID\PASSWORD tab:

Weithod >> PEAP	👻 🗧 Tuneel Authentication 🖂	BAN NGCHALING 🗢	🗋 Section Recuription
IE V PASSWORD	Client Certification Server	Certification	
Autombication ID 7 Pag	need		
OW/CV/v >>	entines en	LONGERVICE	F
TurnellD / Perswere			
Turnel D ++	Turnol Porswerd ++	Stor Passes	6

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 passwords that have been entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

	Client Certification tab:
	System Gening Auth Ubrans, 800.00 - Guil Mattud -> Fguin - Turawa Authentitudian -> Buin McCraming - Distains Becamption IE \ PASSWORD Client Centification Service Centification
	Use discus infacts
	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:
	System Garding Auth 10morts, 80000 600 Method >> Figur Runae Authentitudion >> EMP Moderning Considering the option IE \ PASSWORD Client Certification Una wertificate abula
	Manayi Harri waka kari 14 mila. Manayi Harri waka kari 14 mila. Manayi Harri waka kari 14 mila. Manayi Manay
	Use certificate chain: Choose use server that issuer of 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.
	Server name: Enter an authentication sever.
	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.

<u>Network</u>

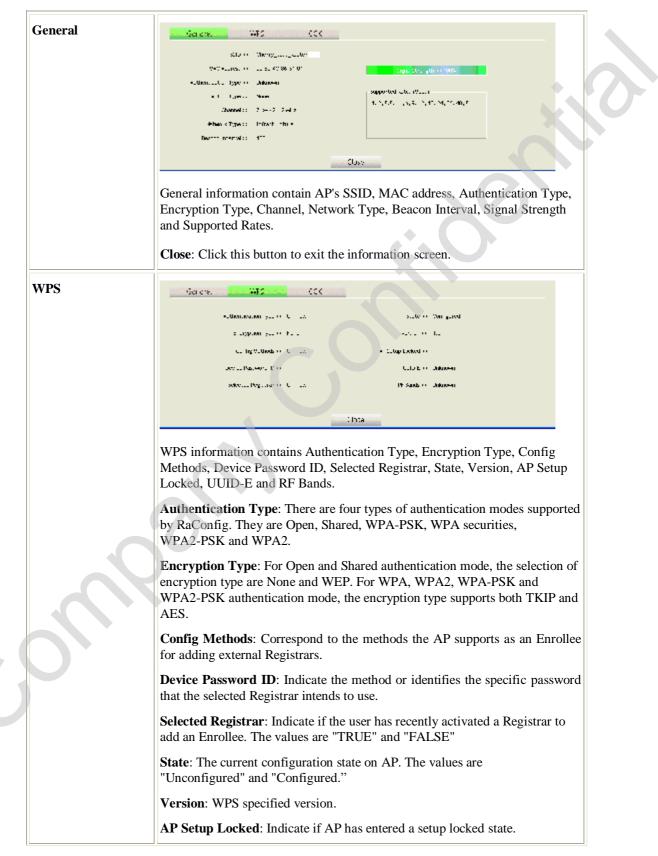
The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

🕻 Intelligent Wireles	s Utiltiy						
Profile	Left Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About
Sorted by >>	🙆 SSID	Char	-) Signal ist >>		Show dBm	
airlive-wl5470poe		11	g	39%			
Cherry_test_Router		6 7	6 <mark>9</mark> 4)	100%		. 0	
Rescan	Add to Profile	e Conr	nect				

Network Tab	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.					
Channel	Shows the currently used channel.					
Wireless mode	AP support wireless mode. It may support 802.11b, 802.11g 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 search and refresh the access point list.					
Add to Profile	Select an item (SSID) on the list and then click to add it into the profile list.					
Connect	Select an item (SSID) on the list and then click to make a connection.					

Access Point (AP) Information

Double click on the intended AP to see AP's detail information that divides into four parts. They are General, WPS, CCX information. The introduction is as following:



	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.	
CCX	000 cm. WES CCC 0.490 mile 01.00 mile grow 1417	3
	Clasy	
	CCX information contains CCKM, Cmic and Ckip information.	
	Close : Click this button to exit the information screen.	

Link Status

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

- Click this button to show the information.
- Click this button to hide the information.

telligent Wireless	sumy.							
Profile	Lee Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
Sorted by >>	SSID	🖉 Cha	-) Signal .ist >>		Show dBm		
irlive-wl5470poe		11	9	39%				
herry_test_Router		1 /27	6 <mark>9</mark> 6	100%				
								•
Rescan	Add to Profile	e Con	nnect				C	
Rescan	Add to Profile	e Con	nnect					
Rescan Status >>		e Con Router <> 00-E0		_		Quality >> 100%		
	Cherry_test_f	Router <> 00-E0			Signal St	rength 1 >> 100%		
Status >> Extra Info >>	Cherry_test_F Link is Up [T×F	Router <> 00-E0	-4C-86-51-01	-	Signal St			2
Status >> Extra Info >> Channel >> Authentication >>	Cherry_test_ Link is Up [TxF 7 <> 2442 MH Open	Router <> 00-E0 Power:100%]	-4C-86-51-01		Signal St	rength 1 >> 100%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE	Router <> 00-E0 Power:100%]	-4C-86-51-01		Signal St	rength 1 >> 100%		
Status >> Extra Info >> Channel >> Authentication >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE	Router <> 00-E0 Power:100%] Hz; central chann	-4C-86-51-01	Transmit —	Signal St	rength 1 ->> 100% Strength >> 26%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE	Router <> 00-E0 Power:100%) Hz; central chann e	-4C-86-51-01	Transmit — Link Speed >>	Signal St Noise :	rength 1 >> 100%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >> IP Address >>	Cherry_test_F Link is Up (TxF 7 <> 2442 MH Open NONE Infrastructure	Router <> 00-E0 Power:100%) Hz; central chann e	-4C-86-51-01	Link Speed >>	Signal St Noise : > 135.0 Mbps	rength 1 >> 100% Strength >> 26%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >> IP Address >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE Infrastructur 192.168.1.101 255.255.255.0	Router <> 00-E0 Power:100%) Hz; central chann e 1)	-4C-86-51-01		Signal St Noise : > 135.0 Mbps	rength 1 ->> 100% Strength >> 26%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >> IP Address >> Sub Mask >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE Infrastructure 192.168.1.101 255.255.255.2	Router <> 00-E0 Power:100%) Hz; central chann e 1)	-4C-86-51-01	Link Speed >>	Signal St Noise : > 135.0 Mbps	rength 1 >> 100% Strength >> 26% Max 0.192 Kbps		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >> IP Address >> Sub Mask >> Default Gateway >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE Infrastructur 192.168.1.101 255.255.255.0	Router <> 00-E0 Power:100%) Hz; central chann e 1)	-4C-86-51-01	Link Speed >> Throughput >	Stenal St Noise : > 135.0 Mbps > 0.000 Kbps	rength 1 >> 100% Strength >> 26%		
Status >> Extra Info >> Channel >> Authentication >> Encryption >> Network Type >> IP Address >> Sub Mask >>	Cherry_test_F Link is Up [TxF 7 <> 2442 MH Open NONE Infrastructure 192.168.1.101 255.255.255.2	Router <> 00-E0 Power:100%) Hz; central chann e 1)	-4C-86-51-01	Link Speed >> Throughput > Receive	Stenal St Notse 3 > 135.0 Mbps > 0.000 Kbps > 81.0 Mbps	rength 1 >> 100% Strength >> 26% Max 0.192 Kbps		

Link Status Ta	b					
Status	Shows the current connected AP SSID and MAC address. If there is a 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, Shared, Leap, 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.					
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, users 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.

<u>Advanced</u>

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

					•			
🔒 Intelligent Wire	less Utiltiy							
Profile	↓ ⊥ Network	Advanced	Statistics	WMM	W RS	Radio On/Off	About	
	indow Size			Turn or Enable	CCKM Radio Measure	nel Measurements limit		

Advanced Tab					
Wireless mode	Here supports 2.4G (included 802.11b/g) wireless mode.				
Enable TX Burst	Check to enable this function. This function enables the Wireless LAN Module 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 connected AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.				

Enable CCX	Check to enable the CCX function.					
(Cisco Compatible extensions)	• Turn on CCKM.					
(Attristons)	• Enable Radio Measurements: Check to enable the Radio measurement function.					
	• Non-Serving Measurements limit: Users can set channel measurement every 0~2000 milliseconds. (Default is set to 250 milliseconds.)					
Apply	Click to apply above settings.					

Statistics

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

🐔 Intelligent Wire	less Utiltiy						X	
Profile	لمعلم Network	Advanced	Statistics	waxa.	WPS Radio On/	Off About		
Transmit	Receive				\mathbf{O}		;	
Frame:	s Transmitted Succe	essfully		-	30836			
Frame:	s Retransmitted Suc	cessfully		= 30836				
Frame:	s Fail To Receive AC	K After All Retries		-	174			
RTS Fr	ames Successfully Re	eceive CTS		± 1	0			
RTS Fr	ames Fail To Receive	e CTS		=	0			
Reset Counte	r							

Transmit					
Frames Transmitted Successfully	Shows information of packets successfully sent.				
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more reties.				
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.				
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.				
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.				
Reset Counter	Click this button to reset counters to zero.				

Profile Network Advanced Statistics WWW WPS Radio On ransmit Receive	/Off About
ransmit Receive	
ansmit Receive	
Frames Received Successfully = 1541	
Frames Received With CRC Error = 627	
Frames Dropped Due To Out-of-Resource = 0	
Duplicate Frames Received = 0	

Receive Statistics				
Frames Received Successfully	Shows information of packets received successfully.			
Frames Received With CRC Error	Shows information of packets received with CRC error.			
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.			
Duplicate Frames Received	Shows information of packets 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 (DLS) that ensure the wireless network linking quality.

Profile Network	ن Advanced	Statistics	www.	Ø WPS	Radio On/Off	Abou
WMM Setup Status	A description in the			10.000		(0)/00/0
WMM >> Enabled	Power Save >	>> Disabled		Di	rect Link >> Disabled	
WMM Enable						
WMM - Power Sa	ive Enable					
AC_BK	AC_BE	AC_VI	AC_VO			
🔲 Direct Link Setu	ip Enable					
MAC Address >:			Timeout Value >>	60 se		
					App	
						Down

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 a power save mode that preferred. 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 (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
MAC Address	 The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions: I Connecting with the same AP that supports DLS feature. I 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 setting of Timeout Value is 60 seconds.)
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA MAC address, then click "Tear Down" button to disconnect the STA.

<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.

Intelligent Wi	reless Utiltiy						
P		- 			A	Q	A
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Of	f About
		W	PS AP List				
						1	Rescan Information
							Pin Code
							16912113 Renew
		WPS	Profile List				Config Mode
Cherry_test_F	Router						Enrollee
							Detail
						<u>></u>	Connect
PIN	WPS Associate	e IE		Progress >> 100			Rotate
PBC	WPS Probe IE	PBC - 0	Get WPS profile suc	cessfully.			Disconnect
	Auto	,					Export Profile
							Delete

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, users 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.					

	A Intelligent Mitches Unity 201 Profile Network Adverced Statistics WWW WFS Redio Cn/Off About
	WPL&File*-
	PPI Dole WES Profile List Config Mode Config Mode
	C Crany, Inc., 11 (Neuror Data
	PEC MATSTruke IS PEC - Get WPC profile outpactsdy: WIGO PEC Recomment Coart Firstle Coart F
	8500 ··· 00001-45-0070-80 Automitation Type ··· C4Eti Encryption Type ··· NOME
	Kay Langton xx Kag Index xx Kag Index xx Kag Index xx
	These Percented
	Cand
	If selected the AP that listed in the WPS Profile List field, users 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 the 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	Registrar : Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.					
	Enrollee : Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.					
PBC	Start to add to AP using PBC (Push Button Configuration) method. Click					
N - 4 -	this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.					
connection. If user	minutes. Meanwhile, the AP should also click the PBC button					
After the users clic connection. If user	minutes. Meanwhile, the AP should also click the PBC button simultaneously. k PIN or PBC, please do not rescan within two minutes of the s want to stop this setup within the interval, restart PIN/PBC or					
After the users clic connection. If user click "Disconnect"	 minutes. Meanwhile, the AP should also click the PBC button simultaneously. k PIN or PBC, please do not rescan within two minutes of the swant to stop this setup within the interval, restart PIN/PBC or to stop WPS action. Send the association request with WPS IE during WPS setup. It is optional 					
After the users clic connection. If user click "Disconnect" WPS Associate IE	minutes. Meanwhile, the AP should also click the PBC button simultaneously. k PIN or PBC, please do not rescan within two minutes of the swant to stop this setup within the interval, restart PIN/PBC or to stop WPS action. Send the association request with WPS IE during WPS setup. It is optional for STA. Send the probe request with WPS IE during WPS setup. It is optional for					
After the users clic connection. If user click "Disconnect" WPS Associate IE WPS Probe IE	minutes. Meanwhile, the AP should also click the PBC button simultaneously. k PIN or PBC, please do not rescan within two minutes of the swant to stop this setup within the interval, restart PIN/PBC or to stop WPS action. Send the association request with WPS IE during WPS setup. It is optional for STA. Send the probe request with WPS IE during WPS setup. It is optional for STA.					

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 LAN Module including, Config Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.

Intelligent Wirel	less Utiltiy							×
Profile	Lee Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
								5
	Config Ve	ersion >> 2.1.5	.0		Date >>	06-23-2008		
	Driver Ve	ersion >> 1.2.1	.0		Date >>	07-30-2008		
	EEPROM Ve	ersion >> 1.0		Firmware	Version >>	0.12		
	Phy_Ad	ldress >> 00-1:	2-0E-6B-58-3B					
								•

Utility Menu List

To access the utility menu list, please right click the utility icon in the task tray.



I Launch Config Utility: Select to open the utility screen.

Use Zero Configuration as Configuration Utility: Select to use the Windows XP built-in utility (Zero configuration utility).

Switch to AP Mode: Select to make the Wireless LAN Module act as a wireless AP.

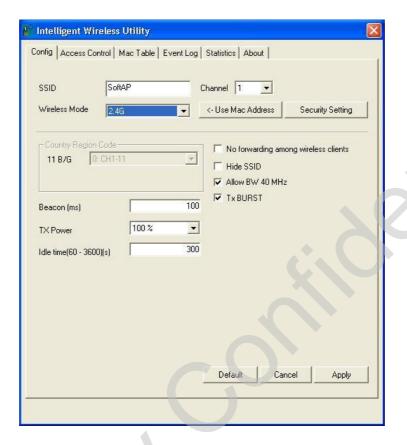
Exit: Select to close the utility program.

I.

L

Soft AP mode

<u>Config</u>



Config	
SSID	AP name of user type. Users 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) wireless mode. (The system default is 2.4G.)
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
	Wep Key
	☞ Key#1 Hex 💌
	© Key#2 Hex ✓
	C Key#3 Hex
	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. (System authentication type default is Open.)
	Encryption Type: For Open and Shared authentication mode, the selections of anorymtion type are Not Use and WEP. For WPA, PSK
	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. (System authentication
	type default is Not Use.)
	WPA Pre-shared Key: This is the shared secret between AP and STA.
	For WPA-PSK and WPA2-PSK and WPA-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. Users
	can set to change by seconds or packets. (Default is 600 seconds.)
	WED Kow Only valid when using WED encryption algorithm. The law
	WEP Key : Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.
	• ASCII (64 bits): 5 ASCII characters (case sensitivity).
	• ASCII (128 bits): 13 ASCII characters (case sensitivity).
	• <u>Hexadecimal (64 bits): 10 Hex characters</u> (0~9, a~f).
	• <u>Hexadecimal (128 bits): 26 Hex characters</u> (0~9, a~f).
	Show Password: Check this box to show the passwords that have been
	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%)
	1570, 5070, 2570 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.)
	between our source seconds. (Detault value of fulle time is 500 seconds.)

No forwarding among wireless	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
clients Hide SSID	Do not display AP name. (System default is disabled.)
Tx BURST	This function enables the adapter to deliver better throughput during a period, it only takes effect when connecting with the AP that supports this function. (Default setting is enabled.)
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control

Config Access Control	Mac Table Event Log] Statistics About	
Access Policy		Disable	
MAC Address		Access List	
	Add		
	Delete		
	Remove All		
			Apply

Access Policy User chooses whether AP start the function or not. (System default is Disable.)	Access Co	ontrol
	Access Policy	
		Allow All: Only the MAC address listed in the Access List can connect with this soft AP.

	I 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. Enter the MAC address in the column and click Add button, then the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that have been set.
Add	Add the MAC address that users would like to set.
Delete	Delete the Mac address that has been set.
Remove All	Remove all Mac address in the Access List.
Apply	Apply the above changes.

MAC Table

10.		Statistics A		
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.			

Event Log

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

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

Statistics

onfig Access Control Mac Table Event Log Statist		
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

Transmit Statistics	
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Shows information of packets successfully sent with one or more reties.
Receive Statistics	
Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	The number of duplicate packets received.

Reset Counter

<u>About</u>

This page displays the Wireless LAN Module and driver version information.

Utility Version :	2.0.5.0	Date :	06-23-2008
Driver Version :	1.2.1.0	Date :	07-30-2008
EEPROM Version :	1.0	Firmware Version :	0.12
IP Address :	192.168.123.1	Phy_Address :	00-12-0E-6B-58-3B
Sub Mask :	255.255.255.0	Default Gateway :	

For Windows Vista

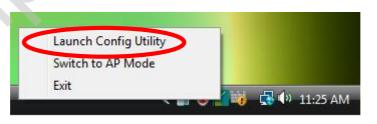
After the Wireless LAN Module has been successfully installed, users can use the included

Configuration Utility to set the preference.

Go to Startg (All) Programg Intelligent Wirelessg Intelligent Wireless Utility.



Open the Configuration Utility by double clicking or right clicking the icon in the tray to select Launch Config Utility.



Station Mode

Profile

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

- Click this button to show the information.
- Click this button to hide the information.



Profile Tab	
Profile Name	Users 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 wireless access points in the wireless network.
Network Type	Shows the network type of the device, including Infrastructure.
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: Notice the second statistic with the second	0
	Add the line of the second second	
R	 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 LAN Module, users can connect wireless LAN to a wired global network via an access point. The Ad hoc lets users set a small wireless workgroup easily and quickly. Equipped with the Wireless LAN Module, users 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 .	
	 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. (Default power save mode is CAM.) 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.

RTS Threshold: Users 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 that have been set</u>. This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: Users 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 the Wireless LAN Module often transmits large files in wireless network, users can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.

Authentication and Encryption tab:

Frotile	1 I Network	Atranced	Statistics	WAA	2	Radio Ch/Off	About
PON	Charry_her	Roster		25			
						- LINERY TEST MOLTER	
					internation	- Integratione	
					Correction .		
					Do DEZ To		
					it have	en 44.11	
					Ching		
					er Sove Wook 205 Threehold		
A11	7/8	Telefo			ent Tonechold		
No. In case	nite the			in Suga			
No. In contraction of the		A		in Suga	ent Tarecooli	: 2346	
Notesciada A Note	india tea uthertication hosticare Rights	A		in Suga	ent Tarecooli	: 2346	
Notesciada A Note	in alter (a utsettentor () histore (ki) (a Mei (a)	Open -		in Suga	ent Tarecooli	: 2346	<u></u>
Notesciada A Note	adds too ubsettorior (hostore k y to Masilay @ 10541	000	- Daris	in Suga	ent Tarecooli	±+ 2246 ☐ 803./3	<u></u>
Notesciada A Note	ndfalte utbestkatter + - Niskare k (; in Mentey © siget Wert	Open -	- Darry	in Suga	ent Tarecooli	±+ 2246 ☐ 803./3	<u></u>
Notesciada A Note	adds too ubsettorior (hostore k y to Masilay @ 10541	000	- Daris	in Suga	ent Tarecooli	±+ 2246 ☐ 803./3	<u></u>
Notesciada A Note	ndfalte utbestkatter + - Niskare k (; in Mentey © siget Wert	Open -	- 2arg	in Suga	ent Tarecooli	±+ 2246 ☐ 803./3	<u></u>

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

- **Open**: If the access point or wireless router is using "**Open**" authentication, then the Wireless LAN Module 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 key 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 four formats to enter the keys.	
	 <u>ASCII (64 bits): 5 ASCII characters</u> (case sensitivity). <u>ASCII (128 bits): 13 ASCII characters</u> (case sensitivity). <u>Hexadecimal (64 bits): 10 Hex characters</u> (0~9, a~f). <u>Hexadecimal (128 bits): 26 Hex characters</u> (0~9, a~f). 	2
	Show Password: Check this box to show the passwords that have been entered.	
	802.1x Setting : When users use radius server to authenticate client certificate for WPA authentication mode.	
	802.1x tab:	
	Honthe Network Advanced Statistics WAN WPS Radio Ch/OH About	
	#001 Cherry_Leve_Souther Future access 4 point 1 #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Second Spect - Second #001 Second Spect - Second Spect - Second Scond Spect - Second Scond Spect - Second Scond	
	W services v.2 Transf interesting to a service (service v.) ✓ Section Securities RS (198550000) Cleant Contributions Section Securities Section Securities Section of the Contributions Section of the Contributions Section Securities Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Section of the Contributions Sec	
	06	
	EAP Method:	
- 6	• 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. Users can click the box to enable or disable this function.
	ID\PASSWORD tab:
	lysteen frantig with LFForry MU12 Sef Restant >> y_jer → Tarmel Auftertication >> _jer-spj_ker/rg → □ Secon Resumption
	ID PASSWORD Client. Certification Advertisation ID / Password Advertisation Demark larger on Identity on Particular of the Demark larger on Demark larger on Turnel ID /> Turnel ID to Turnel Password to Communication Demark larger on Demark larger on
	Dis Cascel
	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 passwords that have been entered.
	OK : Click to save settings and exit this page.
	Cancel: Click to call off the settings and exit.
	Client Certification tab:
2	System Config Auth. \ Encry, 80212 GP wethod >> PC,P Tennel Authentication >> gp=r00craf rg Genetar becauge to a ID + PASSWORD Client Certification Server Certification Constitution the computer formal factor formal factor
\mathbf{O}^{*}	Users can select Use a certificate on this computer , a client certificate for server authentication. Or users 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 Auto. \ Socry. BXXXXX EAP Acthod >> PEAP
	UT PASSWORD Client Certification Server Certification
	Use cent fixate chain
	Sarras marks o
	DK Canal
	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.

Profile	L Network	Advanced	Statistics	WMM	() WPS	Radio On/Off	About
Sorted by >>	SSID	🖉 Cha		Signal List >>		Show dBm	
Cherry_test_Router		67	B9 Ø	100%			
Abocom-Wireless		11	Ьg	86%			
airlive-wl5470poe		11	g	50%			
skl		10	g	44%			
Abocom-Wireless		6	Bg	29%			
PINGOO		11	Bg	24%			
802.11g-AP		6	bg	15%			
Rescan	Add to Prof						
orted by	Inc	licate that A	P list are so	orted by SSII	D, Channe	el or Signal.	
	Ch	eck the box	to show the	e dBm of the	AP list.		
ow dBm							

Network Type	Network type in use, Infrastructure for BSS.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b or 802.11g 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.

Access Point (AP) Information

Double click on the intended AP to see AP's detail information that divides into four parts. They are General, WPS, CCX information. The introduction is as following:

	10	SSID xx Charry fect Poster CAUFess ++ UD ED 4C 86 s1 01	12 Section	u w tan
	Entry Not	diar type (* 2 minow) star type (* 19mi) Sharret (* * * 2422,0%) was type (* 11 fustoatury) minowing (* 100	5 Sapter ford Police (Maper 1, 2, 5,5, 11, 6, 9, 12, 1	C. COMP. CONTR.
			Close	
	Supported	Rates.		ess, Authentication Type Interval, Signal Strength
WPS	Supported Close: Clic	Rates.		Interval, Signal Strength
WPS	Supported	Rates. Ck this button to exit the	information scre	Interval, Signal Strength
WPS	Supported Close: Clic	Rates. Ck this button to exit the wire exit wire exit wire exit wire exit	information scre	Interval, Signal Strength een.
WPS	Supported Close: Clic	Rates. Ck this button to exit the	information scre	Interval, Signal Strength een.
WPS	Supported Close: Clic	Rates. ek this button to exit the wirk to exit the wirk to exit the wirk to exit the biological of the exit the biological of the biological of the exit the biolo	State 35 Wrate 44 Wrate 44	Interval, Signal Strength een.
WPS	Supported Close: Clic	Rates. Ek this button to exit the WBS CCX Authoritection Type + Unknown Encryption Type + Unknown Encryption Type + Unknown	State 35 Wrate 44 Wrate 44	Interval, Signal Strength een. Configured 1.0

	Locked, UUID-E and RF Bands.
	Authentication Type: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK, WPA securities, WPA2-PSK and WPA2.
	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.
CCX	General WES CCX Chanse re-or- Context re-or- Contex
	CCX information contains CCKM, Cmic and Ckip information.
	Close : Click this button to exit the information screen.
	close. Click this button to exit the information screen.

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.
- Click this button to hide the information.

Natherlay Sz Nall Otherny Lest No Otherny Lest No Abcom-Wineless No Ablog No </th <th>Profile</th> <th>Network</th> <th>Advanced</th> <th>Statistics</th> <th>WIM</th> <th>WPS</th> <th>Radio On/Off</th> <th>About</th> <th></th> <th></th>	Profile	Network	Advanced	Statistics	WIM	WPS	Radio On/Off	About		
Cherry_test_Router Ø/ Ø/ 000 Abcoom-Whreess Ø/11 0.03 alrthve-WC470poe Ø/11 0.03 sid Ø/10 448 Abcoom/Wireless Ø/6 0.03 sid Ø/6 0.04 Abcoom/Wireless Ø/6 0.04 Abcoom/Wireless Ø/6 0.04 M000 Ø/11 0.04 Abcoom/Wireless Ø/6 0.04 Motor Ø/6 0.04 Statusse Cherry Lest Backers + 00 F0/4C 86 \$1.01 Mag at Nice (pf0 1/20005C) Our adve 7 < 2 / 248 M4/2 (cold statusse) f0	ed by se	🌢 witi	🏩 the				N OS dBo			
Inthre-wid-5470poe 011 000 445 a 010 445 booom Wireless 066 01 295 intro 0 011 01 245 intro 0 011 01 245 intro 0 011 01 245 intro 0 010 011 01 245 intro 0 010 011 01 245 intro 0 010 010 Nestar Ald to Profile Statistics - Cherry Inst. Foods ris = 00 F0 4C 8A 51 01 Foldschafter - Link bills (Tabler s = 00 F0 4C 8A 51 01 Foldschafter - Link bills (Tabler s = 00 F0 4C 8A 51 01 Foldschafter - Link bills (Tabler s = 00 F0 4C 8A 51 01 Foldschafter - Link bills (Tabler s = 00 F0 4C 8A 51 01 Mis 42 (4019 28 1005 Mis 40 (4019 28 1005 Mis	y_test_Router		61	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				1000	 • 	
sel 010 44% Aboosm Wholces 066 00 20% Mix200 011 00 24% about 2	m-Wareless		811	E 9	36.5					
Aboom Wholess 06 0 298 MHOOO 011 248 AD2.11g An 04 A 2015 Restar: Add to Profile Stating 24 A 2015 Restar: Add to Profile Stating 24 A 2015 Stating 24 A 2015	e-w10470ppe		10	0	20%					
Nixtoo 0 0 1 0 248 802.11g AD 0 1 1 1 Neture Add to Profile 1 1 1 Statissor Cherry, Isst. Boaler, s. + 00 E0 40 56 51 01 1 1 1 Pathetins are to be to be to be to be to be stated? 1 1 1 1 Owned be are to be to be to be to be to be to be stated? 1 1 1 1 Add to Profile 1 1 1 1 1 1 Owned be are to be tob be to				Ū.	44%				Ŧ	
MidDoo MidDoo MidDoo MidDoo 8072.11g Ah All to Profile Restar: All to Profile Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Restar: All to Profile Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Restar: All to Profile Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Restar: All to Profile Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Stadius.2* Cherry, Inst. Booker x + 00 Fb 4C 8A 51 01 Middenth at indice: This State 100 Mig 42 Mid yor 100% Statilizenth: at indice: Theorem x 10001 Middenth: at indice: Theorem X Middenth: at indice: Theorem X <t< td=""><td>m Wireless</td><td></td><td>106</td><td>80</td><td>29%</td><td></td><td></td><td></td><td></td><td></td></t<>	m Wireless		106	80	29%					
A02.11g A ² A 4 15k Restar: A.D. to Profile Statissure: Cherry: Inst. Boald: r. s. + 07 F0 40 56 51 01 R 630 660 yrs. 1006 Faits: Intervention: Nag 40 for g16 12 57 660 x Outmark: Table intervention: Nag 40 for g16 12 57 660 x Autor Provide: Dome 400001 Nag 40 for g16 12 57 660 x Autor Provide: Transmit Non-Miter g16 12 57 660 x Poddress: 10 yrd 10 x 10 yrd 10 x IP Address: 10 yrd 10 x Unit Speed 12 10 yrd Maps	00		1011		248					
Hestar: ALI to Provide Statissor: Cherry, Inst. Boaler, s. + 00 E0 4C 56 51 01 Fatra Infraze: Fatra Infrazer, Fatk is Traffore val0001 O'smaller: Fatra Infrazer, Fatk is Traffore, Val0001 Fatra Infrazer, Fatk Fatra Infrazer, Fatk Provider: Fatra Infrazer, Fatk Provide: Transmit IP Address: 192,402,1100	IF AD		- D -		158					
Falls: Infaste Falls: Infastructure O summitive 7 < x 2442 MHz; stantist channel: 9 Mathematication: 2* Typen Emorphies: 2* NORE Metwork Type 2: Infrastructure TP Address 2: 192,163,1100										
Oranicity 7 C > 2442 M4/2 (control channel: 9 Auttentication 2: Tipen Encryption 2: NORE Metwork Type 1: Infrastructure Trensmit Trensmit IP Address 1: 192/162/1100				40.85.51.01				- 20.		
Authentik ali kut 22 - Egen Encryptikus 22 - KCMP Network Eges : Entrastructure Trensmit EP Address : E192,162,1100 Eink Speed : > 135,0 Mops				n						
Network Type : Infrastructure Trensmit IP Address : 192,162,1700 Enk Speed : - 135,0 Mops			, and a later	83					4	
IP Address = 192.163-1.100 Link Speed = 135.0 Maps										
The Address - Task use hard Entry Speed - Task unops	Network Type :									
					Link Speed :	 135.0 Mops 				
500 Mask 2 2.5/25/2050-0 Default Sateway 5- 192,165,1,199					Throughpull a	- 0.000 Kites	11.725			
Brooke					Repeive		Maps	1		
HT Link Spacel at 135.0 Maps		HT			Link Spaced +	v 135.0 Mars	Mix			
0w/v.40 SHR0 v 0 Throughput v 1 484 Kbox 550 0 5	207 I.S. 20		2.02010.000		Throughput	1 . 484 Kbos	550.016			

	\mathbf{C}
Link Status	
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, Shared, 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.
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, users 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.

<u>Advanced</u>

Apply

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

Y Intelligent Wireless Utiltiy						×
Profile Netw	vork Advanced	Statistics	WMM	WPS Radio On/Off	About	
Wireless mode >> 2.4G	Ţ					
Select Your Count	dBm ry Region Code 11-13					•
Advanced Ta	b					
Wireless mode	Here supports	2.4G (includ	led 802.11b	/g) wireless mode.		
Enable TX Burst	Module to dela	iver better th	roughput du	nction enables the Wirele aring a period of time, it at supports this function	only take	es
Enable TCP Window Size	Check to increase better perform		smission qu	ality. The large TCP w	indow siz	the the
Fast Roaming at	Check to set th	ne roaming in	nterval, fast	to roaming, setup by tra	nsmits po	ower.

Click to apply above settings.

Statistics

Col

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

Profile Network Advanced	Statistics WM	M WPS Radio On/Of	f About
Transmit Receive			•
Frames Transmitted Successfully	=	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	~
set Counter			

Transmit Statistics	Tab
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS frame.
RTS Frames Fail To Receive CTS	Shows information of packets 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
ransmit	Receive						
Frames R	eceived Successfu	lly		=		452	
Frames R	eceived With CRC	Error		=	1	731	
Frames D	ropped Due To Ou	t-of-Resource		=		0	
Duplicate	Frames Received			-		0	

Receive Statistics T	ab
Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	Shows information of packets 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 the wireless network linking quality.

Profile Network	ि Advanced	Statistics	wmm	() WPS	Radio On/Off About
WMM Setup Status WMM >> Enabled	Power Save	>> Disabled		Di	rect Link >> Disabled
WMM Enable	ve Enable				
AC_BK	AC_BE	AC_VI	AC_VO		
Direct Link Setu	and the second second		2011 (1111)		
MAC Address >>			Timeout Value >>	60 Sec	5
					Apply Tear Down

WMM/QoS Ta	b
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	Select a power save mode that preferred.
Enable	AC_BK (Access Category Background)
	AC_BE (Access Category Best Effort)
	AC_VI (Access Category Video)
	I AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
MAC Address	The setting of DLS(Direct Link Setup) indicates as follow :
	 Fill in the blanks of Direct Link with MAC Address of target 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.

<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.

Profile	Network	Advanced	Statistics	WMM	() WPS	Radio On/	Off About
		w	PS AP List				
ID :	Cherr	y_test_ Router		00-0C-43-28-60-E0		6	Rescan Information
							Pin Code
							30650121 Renew
		WPS	Profile List				Config Mode
Cherry_test_ Route	er				0		Enrollee
							Detail
•	- 52		· III				Connect
<u>P</u> IN	WPS Associate	e IE		Progress >> 100%			Rotate
PBC	WPS Probe IE	PBC - 0	Get WPS profile s	uccessfully.			Disconnect
		1.7.7					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 surrounding wireless network.	ss NIC to update information on	
Information	Display the information about WP information included Authentication Methods, Device Password ID, Se Locked, UUID-E and RF Bands.		
	General WPS CCX	N N	
	Authentikation Type ++ Unknown	State >> Configured	
	Encryption type or Hone	Version (*** 1.0	
	Carly McCrab. ++ debide	APSchip usdeed ()	
	Device Resovered (D. ++	ULID 5 *** 6504125510192008122800604(2865101	
	Scouled logistration Chlorien	19 Sanda () Unintern	
		Clove	
PIN Code		nter PIN Code into Registrar when using ee, users can use " Renew " button to	
Config Mode	Select from the pull-down menu to Enrollee or an external Registrar.	b decide the station role-playing as an	
Detail	Click the Detail button to show the the credential.	e information about Security and Key in	

	Contract Westwart N By
	Frottle Network Advanced Statistics WAN WPS Radio Gn/Off About
	12. Dens fed Baler (DED-DAVIS) / Handlan Particular
	STORES Baller
	The second
	25 participation (no. 1) participation acceleration by Disconnect Control to Control Tradition To Control Tradition
	with Uning to Classica
	BALLET IN DE 20 ST UT Antendez d'un lagre si 1991 Al la sergener (gen si balan
	For instance For Keynakova
	La Sacra de Caracteria de C
	16 (1999)
	If selected the AP that listed in the WPS Profile List field, 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 the 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	Registrar : Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.			
	Enrollee : Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.			
РВС	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.			
Noto	Meanwhile, the AP should also click the PBC button simultaneously.			
connection. If use	Meanwhile, the AP should also click the PBC button simultaneously. ick PIN or PBC, please do not rescan within two minutes of the ers want to stop this setup within the interval, restart PIN/PBC or " to stop WPS action.			
After the users cli connection. If use	ick PIN or PBC, please do not rescan within two minutes of the ers want to stop this setup within the interval, restart PIN/PBC or			
After the users cli connection. If use click "Disconnect	ick PIN or PBC, please do not rescan within two minutes of the ers want to stop this setup within the interval, restart PIN/PBC or " to stop WPS action. Send the association request with WPS IE during WPS setup. It is optional			
After the users cli connection. If use click "Disconnect WPS Associate IE	 ick PIN or PBC, please do not rescan within two minutes of the ers want to stop this setup within the interval, restart PIN/PBC or " to stop WPS action. Send the association request with WPS IE during WPS setup. It is optional for STA. Send the probe request with WPS IE during WPS setup. It is optional for 			

Radio On/Off

Click this button to turn on or off radio function.



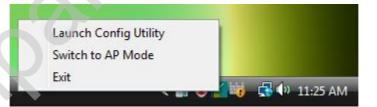
<u>About</u>

This page displays the information of the Wireless LAN Module including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version and Phy_Address.

	4	<u></u>		QoS	() WPS	2	About	
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
	Config Ve	ersion >> 2.1.	5. <mark>0</mark>		Date >>	06-23-2008		
	Driver Ve	ersion >> 2.2.	1.0		Date >>	07-31-2008		
	EEPROM Ve	ersion >> 1.0		Firmwar	e Version >>	0.12		
	Phy_Ad	dress >> 00-	1 <mark>2-0E-6</mark> B-58-3B					
							_	

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 the Wireless LAN Module act as a wireless AP.

Exit: Select to close the utility program.

I

Soft AP mode

<u>Config</u>

Intelligent Wireless Util	ity			
onfig Access Control 1	Mac Table Ev	ent Log	Statistics About	
SSID Soft Wireless Mode 2.40			Channel 1	Security Setting
Country Region Code- 11 B/G 0: CH1-1	1	<u></u>	 No forwarding am Hide SSID ✓ Allow BW 40 MH 	
Beacon (ms)		100		
TX Power	100 %	•		
Idle time(60 - 3600)(s)	[300		
			Default Ca	ncel Apply
	_			

Config		
SSID	AP name of user type. Users 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) 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 Image: Key#1 Image: Key#2 Image: Key#2 Image: Key#3 Image: Key#3 Image: Key#4 Image: Key#4 Image: WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters * WEP 128 Bits Encryption: Please Keyin 10 HEX characters or 13 ASCII characters
	Cancel
	 Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. (System authentication type default is Open.) 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. (System authentication type default is Not Use.)
	 WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-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. Users can set to change by seconds or packets. (Default is 600 seconds.)
2	 WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys. ASCII (64 bits): 5 ASCII characters (case sensitivity). ASCII (128 bits): 13 ASCII characters (case sensitivity). Hexadecimal (64 bits): 10 Hex characters (0~9, a~f). Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).
0.	Show Password: Check this box to show the passwords that have been 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 beacon among wireless client, clients can share information each other. (The system default is no forwarding.)	
Do not display AP name. (System default no hide.)	
Use the system default value.	
Click to apply the above settings.	
	other. (The system default is no forwarding.) Do not display AP name. (System default no hide.) Use the system default value.

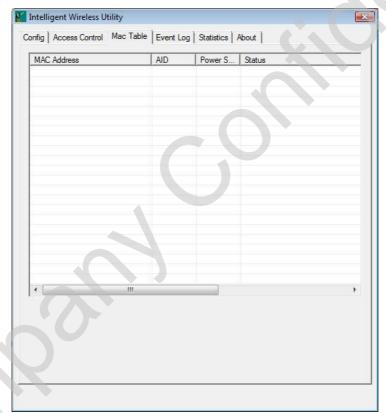
Access Control

📔 Intelligent Wireless U	Itility		
Config Access Control	Mac Table Event L	.og Statistics About	
Access Policy		Disable	
MAC Address		Access List	
	Add		
	Delete		
	Remove All		
			Apply

Access Control		
Access Policy	User chooses whether AP start the function or not. (System default is Disable.)	
	I Disable: Do not use this access control function.	
	I Allow All: Only the MAC address listed in the Access List can connect with this soft AP.	
	I 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. Enter the MAC address in the column and click Add button, then the MAC address will be listed in the Access List pool.	
Access List	Display all MAC Address that users have set.	
Add	Add the MAC address that users would like to set.	
Delete	Delete the MAC address that users 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 2008 / 06 / 06 - 11 : 26 : 50	Restart Access Point Restart Access Point		
		Clear	
	C A		

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

Statistics

onfig Access Control Mac Table Event Log Statis	tics About	
<u> </u>	1 1	
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
	Γ	RESET COUNTERS

Transmit Statistics			
Frames Transmitted Successfully	Shows information of packets successfully sent.		
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.		
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.		
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.		
Frames Transmitted Successfully After Retry	sfully Shows information of packets successfully sent with one o more reties.		
Receive Statistics			
Frames Received Successfully	Shows information of packets received successfully.		
Frames Received With CRC Error	Shows information of packets received with CRC error.		
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.		
Duplicate Frames Received	The number of duplicate packets received.		

Reset Counter

<u>About</u>

This page displays the Wireless LAN Module and driver version information.

1	Utility Version :	2.0.5.0	Date :	06-23-2008
(Driver Version :	2.2.1.0	Date :	07-31-2008
1	EEPROM Version :	1.0	Firmware Version :	0.12
	IP Address :	192.168.123.1	Phy_Address :	00-12-0E-6B-58-3B
	Sub <mark>Mask</mark> :	255.255.255.0	Default Gateway :	0.0.0

Chapter 4: Uninstallation

For Windows 2000/XP

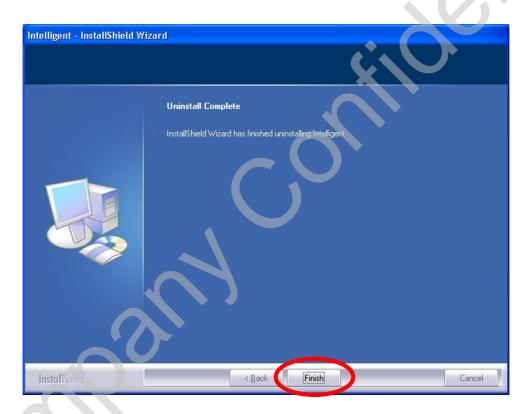
To uninstall the utility and driver, please refer to below steps. (When uninstalling the utility, the driver will be uninstalled as well.)

- Windows Update Internet Internet Explorer 新增 Office 文件 開啓 Office 文件 Ces Paint Accessories E-mail Outlook Express m Games Microsoft Office Notepad SlowView 111 m Startup Intelligent Wireless Trend Micro OfficeScan Client m Adobe Reader 8 ٨., Command Prompt C:\ Internet Explorer Microsoft Office Wor 6 Outlook Express **Remote Assistance** MSN Messenger 7.0 Windows Media Player \mathbf{e} Windows Movie Maker Windows Update MSN Messenger 7.0 WinRAR Windows Live All Programs 📷 Intelligent Wireless Intelligent Wireless Utility Þ ê 🛃 Uninstall - Intelligent 🔎 Log Off n
- 1. Go to Start à All Programs à Intelligent Wireless à Uninstall –Intelligent.

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



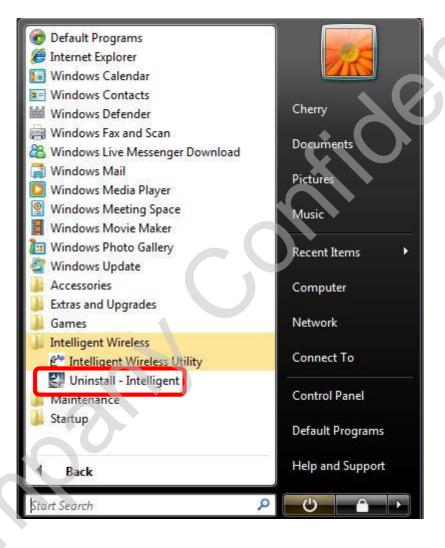
3. Then click **Finish** to complete the uninstallation.



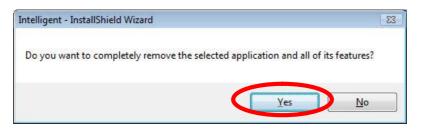
For Windows Vista

To uninstall the utility and driver, please refer to below steps. (When uninstalling the utility, the driver will be uninstalled as well.)

1. Go to Start à Programs à Intelligent Wireless à Uninstall -Intelligent.



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



Caution:

Under Vista 64-bit operation system, when process uninstallation the following screen will show up and request to insert Wireless LAN Module to complete the uninstallation.



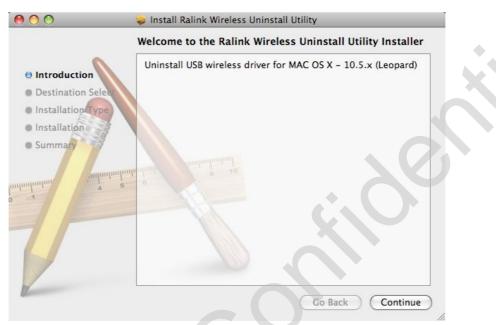
3. Finally, click **Finish** to complete the uninstallation.

	Intelligent - InstallShield Wizard	
C		Uninstall Complete InstallShield Wizard has finished uninstalling Intelligent.
	InstallShield	< Back Finish Cancel

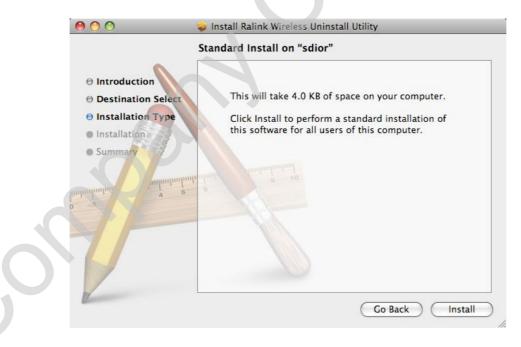
For Mac OS 10.5

To remove the Mac driver, please go to execute the Wireless- Leopard-Uninstall.pkg file to start.

1. When this Welcome screen shows, please click **Continue** to go on.



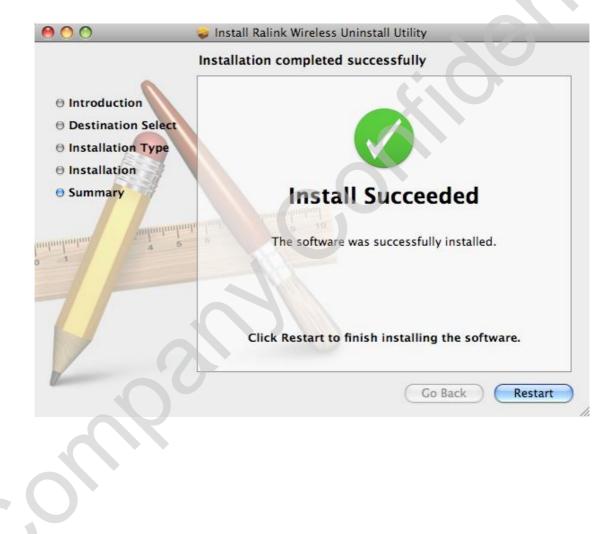
2. Click **Install** to perform the uninstallation.



3. The computer restart message will show up, please click **Continue Installation** to install.



4. Click **Restart** to finish installing the software.



For Linux Kernel 2.4/2.6

To remove the Linux kernel driver, please enter the commands as following in the Terminal program.

	root@localho	ist:~	
Eile Edit View Terr			
[root@localhost ~]			
L			
1. unload driv	r		
\$/sbin/ifconfig	ra0 down		
\$/sbin/rmmod 1	t3070sta		