

Wireless Adapter RNX-N2X User Manual

1.	INTRODUCTION	4
	 1.1 FEATURES & BENEFITS	4 5 5 5
2.	USB ADAPTER FOR WINDOWS VISTA	5
	 2.1 BEFORE YOU BEGIN	5 5 8 9 10 10 11 12 13 .14 .15 .16 .17
3.	USB ADAPTER FOR WINDOWS 2000/XP	. 21
	 3.1 BEFORE YOU BEGIN 3.1 INSTALLING THE DRIVERS. 3.3 PROFILES. 3.3 PROFILES. 3.3.1 Infrastructure Mode. 3.3.2 Ad-hoc Mode. 3.4 AUTHENTICATION AND SECURITY. 3.4.1 WEP Encryption. 3.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption. 3.4.3 WPA-PSK Authentication & TKIP, AES Encryption	21 24 24 26 26 27 28 29 30 31 32 33 35 37 38 40 40 42 43
4.	USB ADAPTER FOR MAC OS 10.3/10.4/10.5	. 44
	4.1 INSTALLING THE DRIVERS	44 47

	4.2.1 Infrastructure Mode	47
	4.2.2 Ad-hoc Mode	48
	4.3 AUTHENTICATION AND SECURITY	49
	4.3.1 WEP Encryption	50
	4.3.2 WPA-PSK Authentication & TKIP, AES Encryption	50
	4.4 LINK STATUS	51
	4.5 SITE SURVEY	52
	4.6 Statistics	53
	4.7 Advanced Configuration	54
	4.8 About	56
5.	HARDWARE INSTALLATION	57
	5.1 LAPTOP CLIP HARDWARE INSTALLATION/ UNINSTALLATION	57
	5.2 RNX-N2X Application Direction.	57
6.	APPENDIX A – GLOSSARY	59
-		70
1.	APPENDIX B - SPECIFICATIONS	10
8.	APPENDIX C – FCC INTERFERENCE STATEMENT	71

1. INTRODUCTION

The high-speed wireless USB 2.0 client adapter is the most convenient way to let you put a desktop/notebook computer almost anywhere without the hassle of running network cables. Now you don't need to suffer from drilling holes and exposed cables. Once you are connected, you can do anything, just like the wired network. This USB client adapter operates seamlessly in 2.4GHz frequency spectrum supporting the 802.11b, 802.11g, and 802.11nwireless standards. It's the best way to add wireless capability to your existing wired network or simply surf the web.

To protect your wireless connectivity, the high-speed wireless USB 2.0 client adapter can encrypt all wireless transmissions through 64/128-bit WEP, WPA, WPA-PSK and WPA-AES encryption and authentication allowing you to experience the most secure wireless connectivity available.

The Rosewill 802.11n USB Adapter (RNX-N2X) implements the latest 11n 2.0 technology which extremely improves wireless signal for your computer than existing wireless 802.11g technology. It supports the 2T2R MIMO architecture with fully forward compatibility with IEEE802.11n. The incredible speed of RNX-N2X USB adapter makes heavy traffic networking activities more flexible and takes the wireless into practical road. You could enjoy the racing speed of wireless connection, surfing on Internet without string wires.

Adding Rosewill RNX-N2X to your Notebook or Computer, it provides an excellent performance and cost-effective solution for doing media-centric activities such as streaming video, gaming, and enhances the QoS (WMM) without any reduction of performance. It extends 3 times network coverage and boosts 6 times transmission throughput than existing 11g product. Advanced power management and low power consumption among 11n products.

For more security-sensitive application, RNX-N2X supports Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES. Also, it supports Wi-Fi alliance WPA and WPA2 encryption and is Cisco CCX V1.0, V2.0 and V3.0 compliant.

Features	Benefits
Racing Speed up to 300Mbps data rate (2.4GHz 11N technology)	Enjoy the Internet connection in crazy-fast speed, without the bottleneck of stringing
	wires.
Advanced power management	Low power consumption
WPA/WPA2 (IEEE 802.11i), WEP 64/128	Powerful data security.
Support	
Support 2Tx * 2Rx Radios	With Intelligent Antenna enables
WMM (IEEE 802.11e) standard support	Wireless Multimedia Enhancements Quality of Service support (QoS) / enhanced power saving for Dynamic Networking
USB 2.0/1.1	USB 2.0 interface and compatible with USB 1.1

1.1 FEATURES & BENEFITS

1.2 PACKAGE CONTENTS

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless LAN USB Adapter-RNX-N2X
- One Laptop clip
- One USB Cable (15cm)
- One CD-ROM with Drivers and User's Manual Included
- One Flexible Stainless Steel USB 2.0 Extended Connector

1.3 USB ADAPTER DESCRIPTION

The USB adapter is a standard USB adapter that fits into any USB interface. The USB adapter has two LED indicators and a built-in antenna.



1.4 SYSTEM REQUIREMENTS

The following are the minimum system requirements in order to use the USB adapter.

- PC/AT compatible computer with a USB interface.
- Windows 2000/XP/Vista or MAC OS 10.3, 10.4 and 10.5 operating system.
- 30 MB of free disk space for installing the USB adapter driver and utility program.

2. USB ADAPTER FOR WINDOWS VISTA

2.1 BEFORE YOU BEGIN

During the installation, Vista may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers.

2.2 INSTALLING THE DRIVERS

Follow the steps below in order to install the USB adapter drivers:

• Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.



• Once the setup begins you will see the **InstallShield Wizard**. Select **Rosewill Configuration Tool** and then click on the **Next>** button.

Rosewill Wireless Network 11N U	JSB adapter RNX-N2X - InstallShield Wizard	53
Setup Status		
	The InstallShield Wizard is installing Rosewill Wireless Network 11N USB adapter RNX-N2X Installing Please Wait	
InstallShield	Cance	el

• Click on the **Install** button to begin the installation.

Rosewill Wireless Network 11N USB adapter RNX-N2X - InstallShield Wizard							
Ready to Install the Program The wizard is ready to begin installa	tion.						
	Click Install to begin the installation.						
InstallShield	< Back	Cancel					

• The installation is complete. Click on the **Finish** button.

tosewill Wireless Network 11N	USB adapter RNX-N2X - InstallShield Wizard InstallShield Wizard Complete The InstallShield Wizard has successfully installed Rosewill Wireless Network 11N USB adapter RNX-N2X. Click Finish to exit the wizard.
InstallSitield	K <u>B</u> ack

• Carefully insert the USB adapter into the USB port. Windows will then detect and install the new hardware.



• An **R** icon will then appear in the system tray. Right click on the **R** icon and then click on Launch Config Utilities.



Note: Click on Use **Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.

2.3 PROFILES

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and

encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.

(000000)	released anty		_	~		_		
P			Gos	Ø	8	R		
Profile	Network	Statistics	WMM	WPS	Radio On/Off	About		
		– Profile List –			-)			
					Profile Nam	e >>		
					SSI	D >>		
					Network Typ	e >>		
					Authenticatio	n >>		
					Use 802.1	x >>		
					Tx Powe	er >>		
Add	Edit	De	lete	Activate				
Add	Edit	De	lete	Activate				
Add	Edit	De	ete	Activate				
Add System (Edit	De	lete 8021X	Activate				
Add System (Edit	De	ete 8021X	Activate	rk Tune SS - Infra	tructure		
Add System (Pro	Edit Config Auth ofile Name >> PRO	De . \ Encry. F1	8021X	Activate Netwo	rk Type >> Infra	structure	•	
Add System (Pro	Edit Config Auth ofile Name >> PRO SSID >>	De . \ Encry. F1	8021X	Activate Networ	rk Type >> Infra Power >>	structure	• •	
Add System (Pro	Config Auth Stile Name >> PRO SSID >>	De . \ Encry. F1	8021X	Activate Netwo Tx	rk Type >> Infra Power >>	structure Auto	•	
Add System (Pro	Config Auth ofile Name >> PRO SSID >>	De . \ Encry. F1	8021X	Activate Netwo Tx	rk Type >> Infra Power >>	structure Auto	•	
Add System (Edit Config Auth ofile Name >> PRO SSID >>	De . \ Encry. F1	8021X	Activate Netwo Tx	rk Type >> Infra Power >>	structure Auto	•	
Add System (Pro	Edit Config Auth ofile Name >> PRO SSID >>	De . \ Encry. F1	8021X	Activate Netwo Tx	rk Type >> Infra Power >>	structure Auto	•	
Add System (Config Auth	De . \ Encry. F1	8021X	Activate Netwo Tx	rk Type >> Infra Power >>	structure Auto	•	
Add System (Pro	Edit	De . \ Encry. F1	8021X	Activate Networ Tx	rk Type >> Infra Power >>	structure	•	
Add System (Edit	. \ Encry.	8021X	Activate Networ	rk Type >> Infra Power >>	structure	•	

2.3.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.

ofile	Network	Statistics	GoS	WPS	Radio On/Off	About		
		— Profile List —						
					Profile Na	me >>		
					5	5ID >>		
					Network T	pe >>		
					Authenticat	ion >>		
					Encrypt	ion >>		
					Use 802	.1x >>		
					TX PO			
Add	Edil	De	lete Act	tivate				
Add	Edit	De	lete Act	tivate				
Add	Edit) Encov	Act	tivate				
Add ystem (Edit	De	lete Act 8021X	tivate				
Add ystem (Edit	De . \ Encry.	lete Act 8021X	tivate Networ	k Type >>	astructure	•	
Add ystem (Pro	Edit	De . \ Encry.	lete Act 8021X	tivate Networ	k Type >> Infr	astructure d hoc	•	
Add ystem (Pro	Edit Config Auth offile Name >> PRC SSID >>	De . \ Encry.	ete Act 8021X	tivate Networ Tx	k Type >> Infr Power >> A	astructure d hoc frastructure	-	
Add ystem (Pro	Edit Config Auth offle Name >> PRC SSID >>	De . \ Encry.	lete Act 8021X	tivate Networ Tx	k Type >> Infi Power >> A I Ir	astructure d hoc frastructure	•	
Add ystem (Pro	Edit Config Auth ofile Name >> PRC SSID >>	De . \ Encry.	lete Act 8021X	tivate Networ Tx	k Type >> Infr Power >> A Ir	astructure d hoc frastructure	·	_
Add ystem (Pro	Edit Config Auth offle Name >> PRC SSID >>	De . \ Encry.	lete Act 8021X	tivate Networ Tx	k Type >> Infr Power >> A I I I	astructure d hoc frastructure	•	_
Add ystem (Pro	Edit Config Auth offle Name >> PRC SSID >>	De . \ Encry.	lete Act 8021X	Networ Tx	k Type >> Infi Power >> A • Ir	astructure d hoc frastructure	Ĭ	_
Add ystem (Pro	Edit Config Auth offle Name >> PRC SSID >>	De . \ Encry.	lete Act 8021X	Networ Tx	k Type >> Infi Power >> A Infi	astructure d hoc frastructure	·	_

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- Network Type: Select Infrastructure from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

2.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In adhoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.

Rosewill Wireless Utility			X
Profile Network Statistics WMM	WPS Radio	On/Off About	
Profile List Add Edit Delete System Config Auth. \ Encry.	Activate	Profile Name >> SSID >> etwork Type >> thentication >> Encryption >> Use 802.1x >> Tx Power >>	
Profile Name >> PROF1 SSID >>	Network Type >> Tx Power >>	Ad hoc Infrastructure Infrastructure	

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- Network Type: Select Ad-hoc from the drop-down list.
- **TX Power**: Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

2.4 AUTHENTICATION AND SECURITY

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK. Each security option is described in detail below.

2.4.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.

🖪 Rosewill Wi	reless Utility						X
Profile	لیے Network	Statistics	QOS WMM	Ø WPS	Radio On/Off	R About	
7a		- Profile List					
					Profile Name	e >>	
					SSII	D >>	
					Authenticatio	e * * n >>	
					Encryptio	n >>	
					Use 802.1	(>> (>>	
Add	Edit	Dele	te	Activate			
System (Config Auth.	\ Encry.	8021X				
	Authentication >>	• Open	•	Encryption >	WEP 🖣	,	802.1X
v	VPA Preshared Key >>						
	Wep Key	1					
	🕜 Key#1	Hexadecimal	▼ 111				Show Password
	Keu#7	Linux da simul					
	U noyez	nexaueumai					
	🖉 Key#3	Hexadecimal	*				
	🖉 Key#4	Hexadecimal					
			OK		Cancel		

- Authentication Type: Select Open or Shared from the drop-down list.
- Encryption: Select WEP from the drop-down list.
- WEP Key: Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **Apply** button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

2.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't

been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

			Gos	0	8	R
rofile	Network	Statistics	WMM	WPS	Radio On/Off	About
		— Pro <mark>file List</mark> ——				
					Profile Nam	e >>
					SSI Network Typ	D >>
					Authenticatio	n >>
					Encryptic	>> n
					Use 802.1	X >>
					TX POW	ci //
444	540	Dela	to	Activita		
Add	Edit	Dele	te	Activate		
Add	Edit	Dele	ţe.	Activate		
Add System (Edit.	Dele	8021X	Activate		
Add System (Edit	Dele . \ Encry. >> WPA	8021X	Activate Encryption >>	TKIP	-
Add System (Edit	. \ Encry.	8021X	Activate Encryption >>	TKIP None	-
Add System (W	Edit	Dele . \ Encry. >> WPA >>	8021X	Activate Encryption >>	TKIP None WEP	-
Add System (Edit Config Auth. Authentication = /PA Preshared Key = Wep Key —	. \ Encry. >> WPA >>	8021X	Activate Encryption >>	TKIP None WEP TKIP	-
Add System (w	Edit Config Auth. Authentication > /PA Preshared Key : Wep Key @ Key#1	. \ Encry. >> WPA >> Hexadecimal	8021X *	Activate Encryption >>	TKIP None WEP TKIP AES	Show Password
Add System (w	Edit Config Auth. Authentication > /PA Preshared Key = Wep Key Key#1 Key#2	. \ Encry. >> WPA >> Hexadecimal Hexadecimal	8021X	Activate Encryption >>	TKIP None WEP TKIP AES	Show Password
Add System (Edit Config Auth. Authentication = /PA Preshared Key = Wep Key & Key#1 & Key#2 & Key#3	Pele Pele WPA WPA Hexadecimal Hexadecimal Hexadecimal	8021X	Activate Encryption >>	TKIP None WEP TKIP AES	Show Password
Add System (Edit Config Auth. Authentication = /PA Preshared Key = Wep Key & Key#1 & Key#2 & Key#3	Pele Venery. WPA WPA Hexadecimal Hexadecimal	8021X	Activate Encryption >>	TKIP None WEP TKIP AES	Show Password

- Authentication Type: Select WPA or WPA2 from the drop-down list.
- Encryption: Select TKIP or AES from the drop-down list.
- Click on the Apply button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

2.4.3 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

Rosewill Wir	eless Utility							X
Profile	LLL Network	Statistics	WMM	() WPS	Radio On/Off	B		
		Profile List			Profile Name SSIE	9 >>) >>		
					Network Type Authentication Encryption	9>> 1>> 1>>		
					Use 802.17 Tx Powe	(>> r >>		
Add	Edit	Dele	ie in and	Activate				
System C	onfig Auth.		8021X	Encryption	AFC	,		_
w	PA Preshared Key >>		•••••					
	Wep Key	Hexadecimal	•	28			Show Password	
	🙆 Key#2	Hexadecimal	-					
	⊘ Key#3	Hexadecimal	•					
	Key#4	Hexadecimal	- CH		ancel			
			UN	and a start				

- Authentication Type: Select WPA or WPA2 from the drop-down list.
- Encryption: Select TKIP or AES from the drop-down list.
- WPA Preshared key: Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

2.5 NETWORK

The **Network** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.

Wireless Adapter RNX-N2X



Status >>	caviumg <> 0	0-03-7F-0C-E0-73	Link Q	uality >> 69%	
Extra Info >>	Link is Up [TxPower:100%]		Signal St	rength 1 >> 18%	
Channel >>	6 <> 2437 MHz; central channel : 4		Signal Strength 2 >> 24%		
Authentication >>	Open		Noise Strength >> 26%		
Encryption >>	NONE				
Network Type >>	Infrastructure		Transmit		
IP Address >>	192.168.1.121		Link Speed >> 216.0 Mbps	Max	
Sub Mask >>	255.255.255.0		Throughput >> 18,576 Kbps	25 524	
Default Gateway >>	192.168.1.1			25.530 Kbps	
	нт	y	Receive	May	
BW >>40		SNR0 >> 10	Link Speed >> 40.5 Mbps	70 774	
GI >> long	MC5 >> 13	SNR1 >> n/a	inrougnput >> /0.//6 Kbps	/0.776	

- Status: This indicates the state of the client. There are three options:
 - 1. **Associated**: Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
 - 2. Scanning: Indicates that the wireless client is searching for an AP in the area.
 - 3. Disconnected: Indicates that there are no APs or clients in the area.
- Extra Info: Displayed here are information about the link stats and the percent of output power.
- **Current Channe**: The operating frequency channel that the client is using (infrastructure mode).
- Link Speed: The current rate at which the client is transmitting and receiving.
- Throughput (bytes/sec): Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- Link Quality: In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- Signal Strength: This bar displays the strength of the signal received from an AP or client.
- Noise Level: Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.
- **dBm Check Box.** When you click on the check box as the drawing below. The signal strength and noise level will be shown as the dBm measurements.

2.6 SITE SURVEY

The Network tab also displays a list of Access Points and Stations in the area, and allows you to

connect to a specific one. The following information is included in this tab, as the image depicts below.

Rosewill Wire	eless Utility						.
Profile	LLL Network	Statistics	Qos WMM	W PS	Radio On/Off	B About	
Sorted by >>	. 0	SID	Channel	Signal		Show dBm	
AMX caviumg		ע ע ע	211 D 26 D 26 D	AF LIST >> − 1 65% 5% 1 20%	-		
Rescan	Add	to Profile					÷

- **SSID**: Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **BSSID**: Displays the MAC address of the Access Point.
- Signal: Displays the receiving signal strength from the Access Point.
- Channel: Displays the channel number of the Access Point.
- Encryption: Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- Authentication: displays the authentication on the Access Point, this includes WPA, WPA-PSK, WPA2, or Unknown.
- **Network Type**: Indicates whether the SSID is a Station (Ad-hoc) or Access Point (Infrastructure).
- **Rescan**: Click on this button to view a list of Access Points in the area.
- **Connect**: to connect with a specific Access Point, select the SSID from the list, and then click on the Connect button.
- Add to Profile: Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

2.7 STATISTICS

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.

Rosewill Wi	reless Utility	Statistics	Gos WMM	Ø WPS	Radio On/Off	B	E
Transn	nit Re	ceive					
	Frames Transmitte	d Successfully		-		1879	
1	Frames Retransmit	ted Successfully		=		1871	
	Frames Fail To Rece	eive ACK After Al Re	etries	=		0	
	RTS Frames Succes	sfully Receive CTS		-		0	
	RTS Frames Fail To	Receive CTS		-		0	
Reset Cou	unter						
							_

2.8 WPS

Click on the **WPS Configuration** tab. WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.

🖥 Rosewill Wi	ireless Utility						
Profile	Network Statisti	cs WMM	Ø WPS	Radio On/Off	Abo	ut	
ID :	RD6_ADSL	WPS AP List -	00-02-	6F-4C-64-AA	13	•	Rescan Information Pin Code
•		III WPS Profile List	·			•	01281415 Renew Config Mode
<		m	-			•	Detail Connect
P <u>B</u> C	WPS Probe IE		Pro	ogress >> 0%			Rotate Disconnect Export Profile Delete

- **Rescan**: Click on this button to view a list of Access Points in the area.
- Click on the **OK** button if you have made any changes.

2.9 ABOUT

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.

🖪 Rosewill Wi	reless Utility						
Profile	LL Network	Statistics		Ø WPS	Radio On/Off	B	
Tronke		Statistics			nualo oni oni	About	
		(c) Copyright 200)7, Rosewill Inc. /	All rights rese	rved.		
		Utility Version >>	2.0.8.0		Date >>	12-27-2007	
		Driver Version >>	2.1.3.0		Date >>	11-21-2007	
		EEPROM Version >>	1.1				
		Phy_Address >>	00-02-6F-4	A-52-85			

2.10 UNINSTALL THE DRIVERS & CLIENT UTILITY

If the USB client adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

• Click on Start > Rosewill Wireless > Uninstall Rosewill RNX-N2X

Ro	sewill Wireless
R	Rosewill Wireless Utility
27	Uninstall - Rosewill RNX-N2X

• The un-installation process will then begin.

2	Rosewill Wireless Network 11N USB adapter RNX-N2X Setup is preparing the InstallShield Wizard, which will guide you through
	the rest of the setup process. Please wait.

• Select the **Remove all** button and then click on the **Next** button.

Rosewill Wireless Network 11N	USB adapter RNX-	-N2X - InstallShield Wizard	
Please select one way to cor	tinue install.		
	There have exist	ed an older version. Which way do you like to do? Remove all. Overwrite the older version install without remove.	
InstallShield		< <u>B</u> ack. <u>N</u> ext >	Cancel

• Click on the Yes button to confirm the un-installation process.

Rosewill Wireless Network 11N USB adapt	pter RNX-N2X - InstallSh	ield Wizard 🛛 🔀
Do you want to completely remove the features?	selected application and	d all of its
	im	(N)

• The un-installation process is complete. Select **Yes, I want to restart my computer now** radio button and then click on the **Finish** button. Then remove the USB adapter.

Rosewill Wireless Network 11	N USB adapter RNX-N2X - InstallShield Wizard
	Uninstall Complete InstallShield Wizard has finished uninstalling Rosewill Wireless Network 11N USB adapter RNX-N2X.
	Yes, I want to restart my computer now. No, I will restart my computer later. Remove any disks from their drives, and then click Finish to complete setup.
InstallShield	K Back Finish Cancel

3. USB ADAPTER FOR WINDOWS 2000/XP

3.1 BEFORE YOU BEGIN

During the installation, 2000/XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS \OPTIONS\CABS directory.

3.1 INSTALLING THE DRIVERS

Follow the steps below in order to install the USB adapter drivers:

• Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.



• Once the setup begins you will see the InstallShield Wizard. Select Rosewill Configuration Tool and then click on the Next> button.

InstallShield Wizard						
2	Rosewill Wireless Network 11N USB adapter RNX-N2X Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.					
	Cancel					

• Click on the **Install** button to begin the installation.

Rosewill Wireless Network 11 Ready to Install the Progra The wizard is ready to begin in	N USB adapter RNX-N2X - InstallShield Wizard 🔀 n stallation.
la de la comunicación Comunicación de la comunicación de	Click Install to begin the installation.
InstallShield	< Back Install Cancel

• Wait for a few seconds until the driver and client utility is installed.

Rosewill Wireless Network 11	N USB adapter RNX-N2X - InstallShield Wizard	×
Setup Status		
	The InstallShield Wizard is installing Rosewill Wireless Network 11N USB adapter RNX-N2X $$	
	Installing	
	Please Wait	
Install Shield	Cancel	

• The installation is complete. Click on the **Finish** button.

Rosewill Wireless Network 1	IN USB adapter RNX-N2X - InstallShield Wizard
	InstallShield Wizard Complete
	The InstallShield Wizard has successfully installed Rosewill Wireless Network 11N USB adapter RNX-N2X. Click Finish to exit the wizard.
InstallShield	< <u>B</u> ack Finish Cancel

- Carefully insert the USB adapter into the USB port. Windows will then detect and install the new hardware.
- An R icon will then appear in the system tray. Right click on the R icon and
 Image: Imag
- then click on Launch Config Utilities.



Note: Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.

3.3 PROFILES

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and

encryption/authentication settings. A profile can be configured as Infrastructure or Ad-hoc mode. The configuration settings for each mode are described below.

🖪 Rosewill Wi	reless Utility							×
Profile	Land Network	ل Advanced	Statistics	www.	Ø WPS	Radio On/Off	B About	
		— Profile List —						
Add	default Edit	D	elete	k Activate	Profile Netword Authenti Encr Use 6 Tx C Power Save RTS Thr Fragment Thr	Name >> SSID >> k Type >> cation >> yption >> 302.1x >> Power >> hannel >> eshold >> eshold >>		•
				Network	Tupe ss	ofestructure	-	
Pro				TX P	ower>>	Auto	▼	
Po	wer Save Mode >>	O CAM (_ 2 РЅМ	Prea	mble >>	Auto	~	
	RTS Threshold		0	د <u> </u>	2347	2347		
	Fragment Thres	hold 2	256	د	2346	2346		
			ОК	Ca	ancel			

3.3.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.

🖪 Rosewill Wi	reless Utility							X
Profile	Land Hetwork	ر Advanced	Statistics	Gos WWW	Ø WPS	Radio On/Off	B About	
		— Profile List —						
					Prof	ile Name >>		
						SSID >>		
					Netwo	ork Type >>		
					Auther	itication >>		
					EDi	cryption >> e 802.1x >>		
					1	x Power >>		
						Channel >>		
					Power Sa RTS T	ve Mode >> breshold >>		
Add	Edit	D	elete	Activate	Fragment T	hreshold >>		
			and a second second					
System C	onfig Auth	. \ Encry.	8021X					
Prot	file Name >> PRO	F1		Network 1	(ype >>	Infrastructure 🔻	•	
				Tx Po	wer>>	Ad hoc		
	22ID >>			1		Infrastructure		
Der	uar Caus Hada as	О сан (a ncu	Prear	nole >> L	Mara	,	
FOU	1001 3000 MIDDE 22		- Family					
	RTS Threshold		0) :	2347	2347		
	Fragment Thre	shold 2	.56	<u>)</u> 2	2346	2346		
			OF	Car	ocel			
			UIC	Ca	1001			

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **PSM**: Select a power saving mode (PSM) option.
 - 1. **CAM** (Continuously Awake Mode): Select this option if your notebook is always connected to the power supply.
 - 2. **PSM** (Power Saving Mode): Select this option if your notebook uses its battery power. This option minimizes the battery usage while the network is idle.
- Network Type: Select Infrastructure from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- **RTS Threshold**: Place a check in this box if you would like to enable RTS Threshold. Any packet in the RTS/CTS handshake larger than the specified value (bytes) will be discarded.
- **Fragment Threshold**: Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be discarded.
- Click on the **OK** button to save the changes.

3.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In adhoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.

Rosewill Wireless Utility	
Profile Network Advanced Statistics	WWW WPS Radio On/Off About
Profile List	
	Profile Name >>
	SSID >>
	Network Type >>
	Authentication >>
	Encryption >>
	Tx Power >>
	Channel >>
	Power Save Mode >>
idd Edit Delete id	RTS Threshold >>
	ragment inresnoid >>
System Config Auth. \ Encry. 8021X	
Profile Name >> PROF1	Network Type >> Infrastructure 💌
, 	Tx Power >> 💽 Ad hoc
221D >>	Infrastructure
Power Save Mode >> 🥥 CAM 🛛 🥥 PSM	Preamole >>
RTS Threshold	
Fragment Threshold 256	
ок	Cancel

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- Network Type: Select Ad-hoc from the drop-down list.
- **TX Power**: Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- Click on the **OK** button to save the changes.

3.4 AUTHENTICATION AND SECURITY

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK, WPA2, and 802.1x. Each security option is described in detail below.

B Rosewill Wireless Utility				X
Profile Network A	dvanced Statistics	www.	WPS Radio On	/Off About
	Profile List			
Add Edit	Delete	Pr Activate Frag	Profile Name >> SSID >> Network Type >> Authentication >> Encryption >> Use 802.1x >> Tx Power >> Channel >> ower Save Mode >> RTS Threshold >> gment Threshold >>	
Authentication >>	Open 👻	Encryption >>	None 🔻	802.1X
WPA Preshared Key >>	• Open			
Wep Key	 Shared Leap WPA WPA-PSK WPA2-PSK WPA2-PSK WPA-None 			Show Password
	0	(Cancel		

3.4.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.

_								_
Rosewill Wireless	Utility							X
Profile Ne	LLL etwork	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	B About	
		Drofile List						
		- Profile List -			Dusfile	blama		
					Profile	selb >>		
					Network	ssilu >>		
					Authenti	cation >>		
					Encr	yption >>		
					Use 8	302.1x >>		
					Tx	Power >>		
					C Bower Sour	hannel >>		
					POwer save RTS Thr	eshold >>		
Add	Edit	[Delete	Activate	Fragment Thr	eshold >>		
System Config	g Auth.	\Encry.	8021X					
Auth	entication >>	> Open	•	Encryption >>	WEP	▼ [802.1X	
WPA Pres	shared Key >>	>						
Wer	n Kev	,						
	•••••			****			Chau Dagaward	
C	🕑 Key#1	Hexadecir	nal 🔻				211000 Pa2200010	
6	🕘 Key#2	 Hexade 	cimal 🖵 🗌					
	7 Kou#2	• ASCII	- L					
	er ney#3	Hexadecin						
6	🥘 Key#4	Hexadecin	nal 🔻					

- Authentication Type: Select Open or Shared from the drop-down list.
- Encryption: Select WEP from the drop-down list.
- WEP Key: Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the Apply button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

3.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

KOSEWIII WILEIESS OIIIIIY						X
Profile Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About
	Profile List					
				Profile	Name >>	
					SSID >>	
				Network	<type>></type>	
				Authenti	cation >>	
				Enor: Lise 8	yption >> 802 1y >>	
				Tx	Power >>	
				с	hannel >>	
				Power Save	: Mode >>	
Add	Edit De	lete	Activate	Fragment Thr	eshold >>	
Internet internet	increasing transmission	interest in the second				
System Config Au	uth. \ Encry.	8021X				
System Config Au	uth.\Encry.	8021X	Encryption >>	ТКІР	•	
System Config Au Authenticat WPA Preshared H	uth. \ Encry. ion >> WPA	8021X	Encryption >>	TKIP None	•	
System Config Au Authenticat WPA Preshared H	ion >> WPA	8021X	Encryption >>	TKIP None WEP	•	
System Config Au Authenticat WPA Preshared H Wep Key —	uth. \ Encry. ion >> WPA Key >>	8021X	Encryption >>	TKIP None WEP	▼	
System Config Au Authenticat WPA Preshared H Wep Key — @ KeyA	uth. \ Encry. ion >> WPA (ey >>	8021X -	Encryption >>	TKIP None WEP TKIP AES	▼ 	In the second se
System Config Au Authenticat WPA Preshared H Wep Key — @ Key# @ Key#	uth. \ Encry. ion >> WPA Key >> #1 Hexadecima #2 Hexadecima	8021X 	Encryption >>	TKIP None WEP TKIP AES	▼ St	Iow Password
System Config Au Authenticat WPA Preshared H Wep Key - @ KeyA @ KeyA @ KeyA	th. \ Encry. ion >> WPA key >> f1 Hexadecima f2 Hexadecima f3 Hexadecima	8021X	Encryption >>	TKIP None WEP TKIP AES	▼ Sr	now Password
System Config Au Authenticat WPA Preshared H Wep Key @ Key @ Key @ Key @ Key @ Key	uth. \ Encry. ion >> WPA Key >>	8021X	Encryption >>	TKIP None WEP TKIP AES	► S+	iow Password

- Authentication Type: Select WPA or WPA2 from the drop-down list.
- Encryption: Select TKIP or AES from the drop-down list.
- Click on the **Apply** button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

3.4.3 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

Rosewill W	ireless Utility						
Profile	↓ Network	کی Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About
		Drofile List					
		Profile List			Profile	Name >>	
						SSID >>	
					Networl	k Type >>	
					Authenti	cation >>	
					Encr	yption >>	
					Use 8	302.1x >> Power >>	
					í.	hannel >>	
					Power Save	e Mode >>	
Add	Edit	Del	oto	Activate	RTS Thr	eshold >>	
AUU	Eult	Dei	ete	Activate	Fragment Ihr	eshold >>	
							100000
System	Config Auth.	\Encry.	8021X				
	Authentication >>	WPA-PSK	•	Encryption >>	ткір	•	
					None		
v	what he shared key >				WEP		
	Wep Key ———				 TKIP 		
	🖉 Key#1	Hexadecimal		******	• AES	🗖 si	now Password
	A Key#2	Hexadecimal					
	Key#3	Hexadecimal					
	🖉 Key#4	Hexadecimal	-				
			,				
			OK		naal		

- Authentication Type: Select WPA or WPA2 from the drop-down list.
- Encryption: Select TKIP or AES from the drop-down list.
- WPA Preshared key: Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

3.4.4 LEAP Authentication

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN. **EAP** (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client

R	Rosewill Wi	ireless Utility							×
	Profile	Land Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About	
_			— Profile List —						
						Profile I	Name >>		
							SSID >>		
						Network	Type >>		
						Authentic	ation >>		
						Encry	ption >>		
						Use 80	02.1× >>		
						Tx F	ower >>		
						Power Save	Mode >>		
						RTS Thre	shold >>		
1	Add	Edit	D	elete	Activate	Fragment Thre	eshold >>		
									.
	System C	Config Auth	. \ Encry.	8021X					
		Authentication	>> IFAP	-					
		Hadnendoacion		·					
				Identity >>	admin				
			P	assword >>	*****			now Password	
			_						
			Doma	in Name >>	domain.com				
				O WEP	WPA-TK	IP 🥥	WPA2-AES		
				ОК	Ca	ncel			

- Authentication Type: Select LEAP from the drop-down list.
- Identity: Enter the user name.
- **Password:** Enter the password.
- **Domain**: Enter a domain name.
- Encryption: Select WEP, WPA-TKIP or WPA2-AES encryption.
- Click on the OK button to save the changes.

3.4.5 802.1x with PEAP

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. **EAP** (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

3.4.5.1 PEAP AUTHENTICATION WITH EAP/TLS SMARTCARD

EAP/TLS Smartcard 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.

	Client Certification	Server Certification	Session Resumption
uthentication ID (Recoverd	cache cortification	Server certifieddon	
Identity >>	Password >>	Domai	n Name >>
unnel ID / Password			
Identity >>	Password >>		
		Show Password	

- Authentication Type: Select PEAP from the drop-down list.
- **Protocol:** If your network uses TLS or Smart Card to authenticate its users, select TLS/Smartcard from the drop down list. **TLS** (Transport Layer Security) is an IETF standardized authentication protocol that uses **PKI** (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.
- Identity: Enter the user name.
- Click on the **OK** button to save the changes.

3.4.6 802.1x with TTLS with EAP-MD5, MS-CHAP, MS-CHAPv2

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. **EAP** (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client. **TLS** (Transport Layer Security) is an IETF standardized authentication protocol that uses **PKI** (Public Key Infrastructure) certificate based authentication of both the client and authentication server.

B Rosewill Wireless Utility			×
Profile	d Statistics WWW	₩PS Radio On/Off	B About
Profile List	:	_	
		Profile Name >>	
		SSID >>	
		Authentication >>	
		Encryption >>	
		Use 802.1x >>	
		Tx Power >>	
		Power Save Mode >>	
		RTS Threshold >>	
Add Edit	Delete Activate	Fragment Threshold >>	
System Config Auth. \ Encry.	8021X		
EAP Method >> PEAP 🔻	Tunnel Authentication >>	EAP-MSCHAP v2 🔻 🚺 Sessi	on Resumption
ID \ PASSWORD Client	Certification Server Cer	tification	
Authentication ID / Password			
Identity >>	Password >>	Domain Name >>	
Tunnel ID / Password			
Identity >>	Password >>	Show Password	
	ОК	Cancel	

- Authentication Type: Select TTLS from the drop-down list.
- Protocol: Select EAP-MSCHAP v2, MS-CHAP, or CHAP from the drop-down list.
- **Identity**: Enter the user name.
- **Password**: Enter the password.
- Click on the **OK** button to save the changes.

3.4.7 802.1x CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial Certificate Authority.

Wireless Adapter RNX-N2X

🖥 Rosewill	Wireless Utility							X			
Profile	Lage Network	ر Advanced	Statistics	Gos WMM	Ø WPS	Radio On/Off	B About				
		— Profile List —									
					Profile	Name >>					
						SSID >>					
Network Type >>											
Authentication >>											
Encryption >>											
					Use t	BUZ.1X >>					
					c	hannel >>					
					Power Save	Mode >>					
				1-12-1-1-	RTS Thr	eshold >>					
Add	Edit	Di	elete	Activate	Fragment Thr	eshold >>					
											
Syster	n Config Auth.	. \ Encry.	8021X								
EAP	Method >> PE4	γP ▼	Tunnel Authentica	tion >> EAP	-MSCHAP v2	👻 🔽 Sessio	n Resumption				
				0.110							
	ID / PASSWORD	Client Ce	rtification 5	erver Certific	cation						
	🔼 Use Client	certificate				•					
	—										
		Issued To	>>								
		Issued By	>>								
		Expired On	>>								
		Friendly Name	>>								
			ОК	Ca	ncel						

🖪 Rosewill	Wireless Utility							X			
Profile	La Network	ر Advanced	Statistics	Gos WAWA	Ø WPS	Radio On/Off	B About				
		— Profile List —									
					Profile	Name >>					
						SSID >>					
Network Type >>											
Authentication >>											
					Enor: Lise 8	yption >> 302 1x >>					
					Tx	Power >>					
					с	hannel >>					
					Power Save	Mode >>					
Add	Edit	D	elete A	Activate	Fragment Thr	eshold >>					
			and the second second		0						
System	I Config Auth	. \ Encry.	8021X								
EAP /	/lethod >> PE	AP 🔻	Tunnel Authenticat	tion >> EAP	-MSCHAP v2	▼ Session	n Resumption				
1000		Client Ce	rtification Se	nver Certific	ation						
	E (TASSNOLE	client co		Aver cereire	acion						
	🔼 Use certii	ficate chain	- Any Trus	ted CA -			•				
			Allow i	intermidiate cer	tificates						
	Server name >>										
	Server name must end in specified name										
			ОК	Ca	ncel						

- Use certificate chain: Place a check in this to enable the certificate use.
- Certificate issuer: Select the Certification Authority from the drop-down list.
- Allow intermediate certificates: During tunnel creation the client must verify the server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the client will also accept a signature from a trusted intermediate certificate authority, otherwise it will not.
- Server name: Enter the server name if not selected from the existing drop-down list above.
- Click on the **OK** button to save the changes.

3.5 NETWORK

The **Network** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.

Profile Network Advanced Statistics WMM WPS Radio	On/Off About
Status >> Disconnected Link Q	uality >> 0%
Extra Info >> Signal Str	rength 1 >> 0%
Channel >> Signal Str	rength 2 >> 0%
Authentication >> Noise St	rength >> 0%
Encryption >>	
Network Type >> Transmit	
IP Address >> Link Speed >>	Max
Sub Mask >> Throughout >>	0.000
Default Gateway >>	Kbps
Receive	
HT Link Speed >>	Max
BW >>n/a SNRO >> n/a Throughput >> Gl >> n/a MCS >> n/a SNR1 >> n/a	0.000

- Status: This indicates the state of the client. There are three options:
 - 1. **Associated**: Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
 - 2. Scanning: Indicates that the wireless client is searching for an AP in the area.
 - 3. Disconnected: Indicates that there are no APs or clients in the area.
- Extra Info: Displayed here are information about the link stats and the percent of output power.
- Channel: The operating frequency channel that the client is using (infrastructure mode).
- Authentication: Displays the authentication type.
- Encryption: Displays the encryption type.
- **Network Type**: Displays the network type; infrastructure or ad-hoc.
- IP Address: Displays the IP address.
- Sub Mask: Displays the subnet mask IP address.
- Default Gateway: Displays the IP address of the default gateway.
- Link Speed: The current rate at which the client is transmitting and receiving.
- **Transmit/ReceiveThroughput**: Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- Link Quality: In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- Signal Strength: This bar displays the strength of the signal received from an AP or client.
- **Noise Level**: Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.

3.5.1 Site Survey

The **Network** tab also displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.

B	Rosewill Wi	reless Utility									
	Profile	Land Hetwork	Advanced	Stati	istics	ļ	QoS VMM	Ø WPS	Radio On/Off	B About	
	Sorted by >	> 🧿	SSID (🖉 Chan	nel	e ap i) Signal ist >>		Show	dBm	
				b 11	Ь	9	10%	-			^
	PM_demo			1 0	₿ <mark>g</mark>	-	10%	-			
	RD6_ADSL			1 0	B <mark>g</mark>	Ø	44%				E
	RD6_Greg3			b 7	<mark>b</mark>	1	34%				
	RD6_Greg3			6 2	<mark>b</mark>	1	34%				
	RD8_3054			1 1	<mark>6</mark> 9	1	29%		•		
				b 11	<mark>b</mark> g	Ŧ	29%		•		~
	Rescan	Add	to Profile	Conn	lect						-

- **SSID**: Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Channel**: Displays the channel number of the Access Point.
- Encryption: Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- Signal: Displays the receiving signal strength from the Access Point.
- Rescan: Click on this button to view a list of Access Points in the area.
- **Connect**: to connect with a specific Access Point, select the SSID from the list, and then click on the Connect button.
- Add to Profile: Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

3.6 ADVANCED CONFIGURATION

The **Advanced** tab is used to configure the wireless mode (802.11g, 802.11b/g-mixed, or 802.11b/g/n-mixed), Tx burst, and CCX.

Rosewill Wireless Utility												
Profile Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About						
Wireless mode >> 802.11 B c 802.11 B c 802.1	nly a mix nly a/N mix dBm us Dialog		Enab	le CCX (Cisco (Turn on CCKM Enable Radio <i>M</i> Non-Servinş 250 ms	Compatible eXtensions easurements 3 Channel Measuremen (0-2000)) its limit						
Authentication >	> WPA	▼	Encryption >>	TKIP	•							
WPA Preshared Key >	»											
Wep Кеу ———												
Key#1	Hexadecimal	-			st	how Password						
Key#2	Hexadecimal	-										
🙆 Key#3	Hexadecimal	-										
Key#4	Hexadecimal	-										
		ок	Car	ncel								

- Wireless mode: Select 802.11 b/g/n mix if the wireless network uses both 11b, 11g, and 11n stations and APs. B/G Protection: This is the ERP protection mode of 802.11g. Selecting auto will dynamically send frames with and without protection. Select **On** to send a frame without protection, and Off to send it with protection.
- Enable Tx BURST: Click the check box will enhance the throughput
- Enable TCP Window Size: Enhance the throughput if enable this function.
- CCX: Enable this option if the network supports Cisco Compatible Extensions.
- Click on the Apply button to close this window.

3.7 STATISTICS

The **Statistics t**ab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.

B Rosewill W	ireless Utility	~		-	~			X
Profile	Network	Advanced	Statistics	Cos WAWA	O WPS	Radio On/Off	R About	
Transr	nit Re	ceive						
	Frames Transmitte	d Successfully		-		1934		
	Frames Retransmit	ted Successfully		=		0		
	Frames Fail To Rece	eive ACK After All R	etries	=		0		
	RTS Frames Succes	sfully Receive CTS		=		0		
	RTS Frames Fail To	Receive CTS		-		0		
Reset Col	unter							Ŧ
B Rosewill Wi	reless Utility							×

Profile	LLL Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About
Transr	nit Re	eceive					
F	rames Received Su	ccessfully		-		24	
F	rames Received Wi	ith CRC Error		-		59767	
F	rames Dropped Due	e To Out-of-Resour	се	=		97349	
C	uplicate Frames Re	eceived		=		0	
Reset Co	unter						

3.8 WMM (WIRELESS MULTIMEDIA)

Click on the **WMM** tab. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

B Rosewill Wireless	Utility					×					
Profile Ne	LL 🧔 twork Advan	ced Statistics	www.	Ø WPS	Radio On/Off	R About					
WMM Setup Status											
WMM >> Enabled Power Save >> Enabled:AC_BE:AC_BK:AC_VI:AC_VO Direct Link >> Enabled											
2 w# 2	M Enable WMM - Power Save Er C AC_BK Direct Link Setup Ena MAC Address >>	able	AC_VI	AC_VO	sec						
			1	1		Apply Tear Down					

- WMM Enable: Choose to enable or disable WMM.
- WMM Power Save Enable: Choose to enable or disable power save mode on WMM.
- Direct Link Setup Enable: Specify a MAC address and timeout value.
- Click on the **Apply** button to close this window.

3.9 WPS

WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.

🖪 Rosewill W	Rosewill Wireless Utility											
Profile	Left Network	Advance	ed Stat	istics	Cos WAMA	Ø WPS	Radio On/Off	About				
			WP	S AP List —								
	WPS Profile List											
PBC WPS Associate IE Progress >> 0% PBC WPS Probe IE D Auto Ex												
System Config Auth. \ Encry. 8021X												
	indenoire oddeloir	- 0	H2 T									
۷	VPA Preshared Key >:	> • •	pen ward									
	Wep Key ———		an an									
	Key#1	W	PA	/			Shou	w Password				
	() Key#2	• W	PA-PSK PA2									
	🖉 Key#3	• W	PA2-PSK	/								
	Key#4	• W	PA-None									
	OK Cancel											

- Rescan: Click on this button to view a list of Access Points in the area.
- WPS Information: Display the information about WPS on the selected network. List information include 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** using PIN method. When RNX-N2X is **Enrollee**, you can use "Renew" button to re-generate new PIN Code.
- Config Mode: The RNX-N2X role-playing as an Enrollee or an external Registrar
- Detail: Information about Security and Key in the credential.
- **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 of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.
- Export Profile: Export all credentials to Profile.
- **PBC:** Start to add to AP using PBC configuration method.
- WPS Associate IE: Send the association request with WPS IE during WPS setup. It is optional for RNX-2X
- WPS Probe IE: Send the probe request with WPS IE during WPS setup. It is optional for RNX-2X
- Click on the **OK** button if you have made any changes.

3.10 ABOUT

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.

📕 Rosewill Wi	ireless Utility							×
Profile	LLL Network	Advanced	Statistics	oos WMM	Ø WPS	Radio On/Off	B About	
		(c) Copyright 20	107, Rosewill Inc.	All rights reserve	ed.			
		Utility Version >>	2.0.8.0		Date >>	12-27-2007		
		Driver Version >>	1.0.5.0		Date >>	11-16-2007		
		EEPROM Version >>	1.1	Firmwa	are Version >>	0.5		
		Phy_Address >>	00-02-6F-4	IA-52-B3				
								T

3.11 RADIO

The **Radio** tab allows you to enable or disable the radio.

🖪 Rosewill W	ireless Utility							
Profile	Land Hetwork	Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About	
							-	
		(c) Copyright 20	007, Rosewill Inc.	All rights reserve	ed.			
		Utility Version >>	> 2.0.8.0		Date >>	12-27-2007		
		Driver Version >>	> 1.0.5.0		Date >>	11-16-2007		
		EEPROM Version >>	• 1.1	Firmw	are Version >>	0.5		
		Phy_Address >>	• 00-02-6F-4	4A-52-B3				

3.12 UNINSTALL THE DRIVERS & CLIENT UTILITY

If the USB client adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

• Click on Start > Rosewill Wireless > Uninstall Rosewill Wireless USB Adapter

🖪 Rosewill Wireless Utility 🛛

🛃 Uninstall - Rosewill RNX-N2X 🚽

• The un-installation process will then begin.



• Select the **Remove all** button and then click on the **Next** button.

• Click on the Yes button to confirm the un-installation process.

Rosewill Wireless Network 11N USB adapter RNX-N2X - InstallShield Wizard	\ge
Do you want to completely remove the selected application and all of its features?	

• The un-installation process is complete. Select **Yes, I want to restart my computer now** radio button and then click on the **Finish** button. Then remove the USB adapter.

Rosewill Wireless Network 11N	I USB adapter RNX-N2X - InstallShield Wizard
	Uninstall Complete
	InstallShield Wizard has finished uninstalling Rosewill Wireless Network 11N USB adapter RNX-NZX.
	 Yes, I want to restart my computer now. No, I will restart my computer later.
	Remove any disks from their drives, and then click Finish to complete setup.
InstallShield	< Back Finish Cancel

4. USB ADAPTER FOR MAC OS 10.3/10.4/10.5

4.1 INSTALLING THE DRIVERS

Follow the steps below in order to install the USB adapter drivers:

• Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the

setup file from the CD-ROM drive.



• Click on the **Continue** button to configure the next step.

000	🤿 Install USB Wireless Utility – Leopard
Introduction Destination Se Installation Ty Installation Summary	Standard Install on "Macintosh HD" This will take 3.2 MB of space on your computer. Click Install to perform a standard installation of this software for all users of this computer.
Ver	Go Back Install

• Select the Macintosh HD and then click on the Continue button.



• Click on the **Continue** button to configure the next step.



• The installation is complete. Click on the **Restart** button.



- Carefully insert the USB adapter into the USB port. MAC OS X will then detect and install the new hardware.
- The Client Utility is installed in the Applications folder.

4.2 PROFILES

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.

4.2.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.

Profile Name	PROF2	SSID	-
<u> </u>			
S	ystem Configuration	Authentication & Se	curity
Power Saving Mod	e		
CAM (Co	nstantly Awake Mode)	O Power Saving M	lode
Network Type	Infrastructure	▼ Tx Power Channel	100 •
RTS Threshol	d 0		02347
E Fragment Thr	reshold 256		O ²³⁴⁶ 2346

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **PSM**: Select a power saving mode (PSM) option.
- 1. **CAM (Continuously Awake Mode)**: Select this option if your notebook is always connected to the power supply.
- 2. **PSM (Power Saving Mode)**: Select this option if your notebook uses its battery power. This option minimizes the battery usage while the network is idle.
- Network Type: Select Infrastructure from the drop-down list.
- TX Power: Select a transmit power from the drop-down list. If your notebook is connected to external power then select 100% or auto, if not, select one of the lower values for power saving.
- **RTS Threshold**: Place a check in this box if you would like to enable RTS Threshold. Any packet in the RTS/CTS handshake larger than the specified value (bytes) will be discarded.
- **Fragment Threshold**: Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be discarded.
- Click on the **Apply** button to save the changes.

4.2.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In adhoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive

Profile Name		/ireless Utility	
rionic manie	PROF2	SSID	•
	System Configuration	Authentication & Se	curity
Power Saving Mod	le		
• CAM (Co	nstantly Awake Mode)	O Power Saving M	ode
Network Type	802.11 Ad Hoc	Tx Power Channel	100 •
RTS Threshol	id 0		
Eragment Th	reshold 256		2346

way for the SOHO to set up a wireless network.

- **Profile**: Enter a name for the profile; this does not need to be the same as the SSID.
- SSID: Enter the SSID of the network or select one from the drop-down list. The SSID is
 a unique name shared among all points in your wireless network. The SSID must be
 identical for all points in the network, and is case-sensitive.
- Network Type: Select Ad-hoc from the drop-down list.
- **TX Power**: Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- **Preamble**: Select Auto from the drop-down list, unless you are aware of the preamble type (long or short) used in each station.
- Ad-hoc wireless mode: Select a wireless mode from the drop-down list depending on the type of stations used in the ad-hoc network. Select B/G Mix if the network consists of 11b and 11g stations. Select B-only or G-only if the network consists of only one type of wireless mode.
- **RTS Threshold**: Place a check in this box if you would like to enable RTS Threshold. Any packet in the RTS/CTS handshake larger than the specified value (bytes) will be discarded.
- **Fragment Threshold**: Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be discarded.
- Click on the Apply button to save the changes.

4.3 AUTHENTICATION AND SECURITY

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK, WPA2, and 802.1x. Each security option is described in detail below.

4.3.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.

_	bysten. c		atron	7 101 1.1.1		in a seco	<u> </u>	
Authentication Type Encryption Type		WPA-	PSK					•
		TKIP	TKIP					•
WPA Pre-Sha	red Key							
Box								
⊙ Key#1	Hexade	cimal	•					
◯ Key#2	Hexade	cimal	•					
⊖ Key#3	Hexade	cimal	•					
○ Key#4	Hexade	cimal	•					

- Authentication Type: Select Open or Shared from the drop-down list.
- Encryption: Select WEP from the drop-down list.
- WEP Key: Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the Apply button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

4.3.2 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services

is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

	System C	onfigur	ation	Auth	enticatio	on & Se	curity	
Authentication Type Encryption Type		WPA-	WPA-PSK					
		TKIP						•
WPA Pre-Sha	red Key							
Box								
• Key#1	Hexade	cimal	•					
◯ Key#2	Hexade	cimal	-					
⊖ Key#3	Hexade	cimal	•					
○ Kev#4	Hexade	cimal	•					

- Authentication Type: Select WPA or WPA2 from the drop-down list.
- Encryption: Select TKIP or AES from the drop-down list.
- WPA Preshared key: Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- Show Password check box. If you want to make sure the accuracy of password you type, click the Show Password box to check it.

4.4 LINK STATUS

The **Link Status** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.

Profile	Link Status	Site Surv	te Survey Statistics Advanced			About	
► Statu	15	cav	iumg <	<> 00-0	3-7F-	0C-E0-7	3
▶ Curr	ent Channel	6 <	> 2	437 MHz (C	Centra	l Channe	l:4)
► Link	Speed (Mbps)	Тх	81.0		Rx	27.0	
► Thro	ughput (Kbps)	Тх	0.0		Rx	31.0	
► Link	Quality	Good	1 85%		d	Bm format	
▶ Sign	al Strength 1	Weal	12%				
▶ Sign	Weal	Weak 18%					
► Nois	e Level	Low	36%				
HT Int	fo						

- Status: This indicates the state of the client. There are three options:
 - 1. **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
 - 2. Scanning: Indicates that the wireless client is searching for an AP in the area.
 - 3. Disconnected: Indicates that there are no APs or clients in the area.
- Extra Info: Displayed here are information about the link stats and the percent of output power.
- **Current Channel**: The operating frequency channel that the client is using (infrastructure mode).
- Link Speed: The current rate at which the client is transmitting and receiving.
- Throughput (bytes/sec): Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- Link Quality: In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- Signal Strength: This bar displays the strength of the signal received from an AP or client.
- Noise Level: Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.
- **dBm Check Box**. When you click on the check box as the drawing below. The signal strength and noise level will be shown as the **dBm** measurements.

4.5 SITE SURVEY

The Site Survey tab displays a list of Access Points and Stations in the area, and allows you to

connect to a specific one. The following information is included in this tab, as the image depicts below.

				- AP Li	st			
	SSID	BSSIC)	Signal	Channel	Authen	Encryp	NetworkTyp
1	caviumg	00-03-7	7F-0C	15	6	Unknov	Not Us	Infrastruct
		00-02-6	5F-48	55	1	Unknov	WEP	Infrastruct
		00-02-6	5F-48	29	1	Unknow	WEP	Infrastruct
	SQA_3220B	00-02-6	5F-49	20	3	Unknov	WEP	Infrastruct
	RD8-dlink-d	00-1B-1	1-5E	55	6	WPA-PS	TKIP	Infrastruct
	1	00-E0-4	C-81	60	7	Unknov	Not Us	Infrastruct
	RD2_roaming	00-1A-7	70-EC	29	9	Unknov	WEP	Infrastruct
	RD8_3054	00-02-6	5F-37	60	11	WPA-PS	TKIP	Infrastruct
	RD6_ADSL	00-02-6	5F-4C	81	9	WPA2-I	AES-CO	Infrastruct
		00-02-6	5F-36	55	10	Unknov	WEP	Infrastruct
		00-02-6	5F-48	70	11	Unknov	WEP	Infrastruct
_					-)) + >

- **SSID**: Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- BSSID: Displays the MAC address of the Access Point.
- **Signal**: Displays the receiving signal strength from the Access Point.
- Channel: Displays the channel number of the Access Point.
- Encryption: Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- Authentication: displays the authentication on the Access Point, this includes WPA, WPA-PSK, WPA2, or Unknown.
- **Network Type**: Indicates whether the SSID is a Station (Ad-hoc) or Access Point (Infrastructure).
- Rescan: Click on this button to view a list of Access Points in the area.
- **Connect**: to connect with a specific Access Point, select the SSID from the list, and then click on the Connect button.
- Add Profile: Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

4.6 STATISTICS

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after

retry, received with CRC error, duplicate frames received, etc.

C Kosewill Wire			ess Utility		
Profile	Link Status	Site Survey	Statistics	Advanced	About
- Transmit	t Statistics				
Frames Tran	smitted Successfu	lly	3	=	267
Frames Tran	smitted Successfu	lly Without Retry	3	-	0
Frames Tran	smitted Successfu	lly After Retry(s)		=	267
Frames Fail	To Receive ACK Af	ter All Retries	1	=	0
RTS Frames	Successfully Recei	ve CTS		=	0
RTS Frames	Fail To Receive CT	S	=		0
- Receive S	Statistics				
Frames Rece	ived Successfully			=	135
Frames Rece	ived With CRC Err	or		=	237589
Frames Drop	ped Due To Out-	of-Resource	3	=	0
Duplicate Fra	ames Received			-	0
				RESET CO	UNTERS

4.7 ADVANCED CONFIGURATION

The **Advanced** tab is used to configure the wireless mode (802.11b-only, 802.11g-only, or 802.11b/g-mixed), B/G protection and country/channel setting.

Wireless Adapter RNX-N2X

Profile	Link Status	Site Survey	Statistics	Advanced	About
	Wireless Mode	2.4G		\$	
	TX Rate	Auto	\$		
	🗹 Enable TX Bu	ırst			
¥					
dio Off					APPL

- Wireless mode: Select 802.11 B/G/N mixed if the wireless network uses both 11b, 11g and 11n stations and APs.
- **Tx Rate**: The transmit rate should be set to auto, however you may manually select a transmit rate from the drop-down list.
- **Tx BURST**: Click the check box will enhance the throughput
- Click on the **Apply** button to save the changes.

4.8 ABOUT

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.

	Site Survey S	tatistics	Advanced	About
(D		•	
<u> </u>	lose	wi	<u>u</u>	
Wireless Utility			3 0.000 	
Version: 1.4.9.0	Date	: 2008-	01-25	
NIC Driver				
Version: 1.0.4.0	Date	: 2007-	12-24	
Version: 1.0.4.0	Date	: 2007-	12-24	

5. HARDWARE INSTALLATION

5.1 LAPTOP CLIP HARDWARE INSTALLATION/ UNINSTALLATION



3. **Uninstallation:** Take off the laptop clip from RNX-N2X as picture.



5.2 RNX-N2X APPLICATION DIRECTION

A type (For Laptop)





B type (For Laptop)



C type (For Desktop)





6. APPENDIX A – GLOSSARY

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Α

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

В

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

С

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the sane time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to

obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

Ε

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet **Full-duplex**

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

н

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

L

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

Κ

Kbps

Kilobits per second

Kbyte

Kilobyte

L

L2TP

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

Μ

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packetbased network like the Internet

Multicast

Sending data from one device to many devices on a network

Ν

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

0

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

Ρ

Password

A sequence of characters that is used to authenticate requests to resources on a network **Personal Area Network**

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

ΡοΕ

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

Stateful Packet Inspection

SPI

SSH

ээп

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

Т

ТСР

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VolP

Voice over IP

W

Wake on LAN

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

Х

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Υ

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

7. APPENDIX B – SPECIFICATIONS

Data Rates

1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, 72, 84, 150 and 300Mbps (300 Rx PHY rate; 150Mbps Tx PHY support) Standards / Compliance IEEE802.3, IEEE802.3u, IEEE802.11b, IEEE802.11g, 802.11n (2.0) **Regulation Certifications** FCC Part 15, ETSI 300/328/CE **Operating Voltage** 5 V ± 0.25V Status LEDs POWER / LINK **Drivers** Windows 2000/XP/Vista MAC OS 10.3/10.4/10.5 **RF** Information **Frequency Band** U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations Media Access Protocol Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Modulation Technology 802.11g: OFDM (64-QAM, 16-QAM, QPSK. BPSK) 802.11b: DSSS (DBPSK, DQPSK, CCK) **Operating Channels** 11 for North America, 14 for Japan, 13 for Europe **Receive Sensitivity (Typical)** 2.412~2.472G(IEEE802.11b) (1Rx) -91dBm @ 1Mbps -87dBm @ 11Mbps 2.412~2.472G(IEEE802.11g) (2Rx) -90dBm @ 6Mbps -75dBm @ 54Mbps

 2.412~2.472G(IEEE802.11N) (2Rx) -88 dBm MCS 8 -65 dBm MCS 15

Available transmit power

- 2.412~2.472G(IEEE802.11b) 18dBm @1~11Mbps
- 2.412~2.472G(IEEE802.11g) 15 dBm @6Mbps 14 dBm @54Mbps
- 2.412~2.472G(IEEE802.11N) 15dBm

Antenna Configuration 2T2R Mode

Networking

Topology

Ad-Hoc, Infrastructure

Security

WPA/WPA2 (AES, 64,128-WEP with shared-key authentication) Cisco CCS V1.0, V2.0 and V3.0

compliant Physical

Form Factor

Dimensions (HxWxD) 77(L) mm x 23.5(W) mm x 11(H) mm Weight

USB 2.0/1.1

40 g/ 1.5oz

Environmental

Temperature Range

Operating: 0°C to 50°C Storage: -10°Cto 75°C

Humidity (non-condensing) 5%~95% Typical

Package Contents

- One Wireless-N USB Dongle-RNX-N2X
- One CD-ROM with User's Manual and Drivers
- One FLEX USB cable (15cm) One
- One Flexible Stainless Steel USB 2.0 Extended Connector

8. APPENDIX C – FCC INTERFERENCE STATEMENT

Federal Communication Commission Interference Statement

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

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

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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

Thank you for purchasing a quality Rosewill Product.

Please register your product at : www.rosewill.com for complete warranty information and future support for your product.