802.11n Wireless PCI Adapter



USER MANUAL 1.0.0



Table of Contents

Chapter I	Introduction	4
1. Welcome.		
2 Product F	eature	4
2. 1 1000001 1		
3. Contents of	от Раскаде	4
4. Before yo	u begin	4
Chapter II	Designing Your PCI Adapter	5
Chapter III	Installation	5
1. Install You	Ir PCI Adapter	
2 Install Driv	ver and Utility	6
2. mstan Driv		
Chapter IV	Utility Config	11
- 1 WZC		11
1 1 Polink Wi	roloco (Itility (Polli) or Windows Zoro Configuration (W/ZC)	11
1.1 Kallink Wi 1.2 Use WZC	to configure wireless NIC	
2. RaUI		
2 1 Start		18
2.1. Start Ra	UI	
2.2 Profile	-	24
2.2. Profile		24
2.2. Add/Edi	tProfile	26
2.2. Example	e to Add Profile in Profile	27
2.3 Network		
2.3. Network	(31
2.3. Example	e on Adding Profile in Network	
2.4 Advanced		
2.4. Advanc	ed	
2.5 Statistics		
2.5. Statistic	S	
	a ta Canfigura ta Enabla DI S (Direct Link Satur)	
	e to Configure to Enable DES (Direct Link Setup)	
2.6 Example	e to Configure to Enable WMM - Power Save	
2.0. Example		53
2.7. WPS		53
2.7. WPS Inf	ormation on AP	
2.7. Example	e to Add to Registrar Using PIN Method	
2.7. Example	e to Add to Registrar Using PBC Method	63
2.7. Example	e to Configure a Network/AP Using PIN or PBC Method	
2.8 About		70
2.8. About		70
2.9 Link Statu	IS	71

Chapter	V Trouble Shooting 10)3
	3.6 Example to Configure Connection with WPA	.87
	3.5 Example to Configure Connection with WPA-PSK	.83
	3.4 Example to Configure Connection with WEP on	.80
	3.3 Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is	Failed in Profile
	3.2 802.1x Setting	.73
	3.1 Auth. \ Encry. Setting - WEP/TKIP/AES	.73
3	B. Security	73
	2.9. Link Status	71

1 Introduction

1.1 Welcome

PCI Adapter connects you with IEEE802.11n(Draft 2.0) networks at receiving rate up to an incredible 150Mbps! By using the reflection signal, 802.11n technology increases the range and reduces "dead spots" in the wireless coverage area. Unlike ordinary

wireless networking of 802.11b/g standards that are confused by wireless reflections, 802.11n can actually use these reflections to increase four times transmission range of 802.11g products. Besides, when both ends of the wireless link are 802.11n products, The PCI can utilize twice radio band to increase three times transmission speed of ordinary 802.11g standard products, and can comply with backwards 802.11b/802.11g standards.

Soft AP supported by PCI Adapter can help you establish wireless LAN networking with lowest cost. Besides, WPS (PBC and PIN) encryption method can free you from remembering the long passwords. Complete WMM function makes your voice and video more smooth.

1.2 Product Feature

- Complies with IEEE 802.11n (Draft 2.0), IEEE 802.11g, IEEE 802.11b standards
- Provides 32-bit PCI interface
- Provides 150Mbps receiving rate and 150Mbps sending rate
- Supports 20MHz/40MHz frequency width
- Auto-detects and changes the network transmission rate
- Provides two work modes: Infrastructure and Ad-Hoc
- Supports Soft AP to establish your wireless LAN networking with lowest cost
- Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standard
- Supports WPS (PBC and PIN) encryption method to free you from remembering long passwords
- Supports WMM to make your voice and video more smooth
- Supports Windows® 2000, XP 32/64, Vista 32/64, Win 7 32/64

1.3 Contents of Package

- One PCI Adapter
- One Installation CD w/User Manual
- One dipole antennas

Contact your local authorized reseller or the store purchased from for any items damaged and/or missing.

1.4 Before you begin

- You must have the following:
- A desktop PC with an available 32-bit PCI slot
- Minimum 300MHz processor and 32MB memory
- Windows 2000, XP, 2003, Vista, Win7
- A CD-ROM Drive
- PCI controller properly installed and working in the desktop PC
- 802.11n or 802.11b/g Access Point (for infrastructure Mode) or another 802.11n or 802.11b/g wireless adapter (for Ad-Hoc; Peer-to-Peer networking mode.)

2 Designing Your PCI Adapter

PCI Adapter supports up to 150Mbps connections. It is fully compliant with the specifications defined in 802.11n (Draft 2.0) standard.



The status LED indicators of PCI Card are described in the following.

- Lnk/Act ON (Green): Indicates a valid connection.
- Lnk/Act Flashing: Indicates the Adapter is transmitting or receiving data.

3 Installation

3.1 Install Your PCI Adapter

- Open your PC case and locate an available PCI on the motherboard.
- Slide PCI Adapter into the PCI slot. Make sure that all of its pins are touching the slot's contacts. You may have to apply a bit of pressure to slide PCI Adapter all the way in. after it is firmly in place, secure its fastening tab to your PC's chassis with a mounting screw. Then close your PC.
- Attach the external antennas to PCI Adapter's antenna port.
- Power on the PC.

Note:Select Cancel when "Found New Hardware" window appears.



3.2 Install Driver and Utility

NOTE: Snap-shot screens of the following installation procedure are based on Windows XP. Installation procedures will be similar for other windows operating systems.

- 1. Insert Installation CD to your CD-ROM drive. And click **Driver Installation**. The wizard will run and install all necessary files to your computer automatically.
- 2. Click Next to accept the Agreement. Or click Cancel to cancel the installation.



3. Click Next.



- 4. Select Ralink Configuration Tool or Microsoft Zero Configuration Tool then click Next.
- a. It's recommended to select **Ralink Configuration Tool**, which provides fully access to all function of PCI Adapter.
- b. If you prefer to use the wireless configuration tool provided by Windows XP or Vista, please select **Microsoft Zero Configuration Tool**.

alink Wireless LAN - Instal	IShield Wizard	X
Setup Type Select the setup type that best	suits your needs.	
	Select Configuration Tool	
	Raink Contiguation Tool	
	Microsoft Zero Configuration Tool	
Zora		
- Halink		
Installigid	<back next=""> Ca</back>	nosi



5. Click **Finish** to complete the software installation.

Ralink Wireless LAN - Instal	IShield Wizard
	InstallShield Wizard Complete
Ralink	The InstalSheld Wized has successfully installed Rialink Wireless LAN. Click Firsth to exit the elizard
InstallSidd	c gack Finally Canool

4 Utility Config

4.1 WZC

4.1.1 Ralink Wireless Utility (RaUI) or Windows Zero Configuration (WZC)

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to the Ralink Wireless NIC. Ralink's utility (RaUI) additionally provides WPA functionality. To make it easier for the user to select the correct utility. RaUI will let users make a selection when it first runs after windows XP boots.

Double-clicking the icon will bring up the selection window and allow the user make a selection.



RaUI can co-exist with WZC. When coexisting with WZC, RaUI only provides monitoring functions, such as surveying the link status, network status, statistic counters, advanced feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-2.



Figure 1-2 Select WZC or RaUI

If "Use RaConfig as Configuration utility" is selected, please jump to Section 2 on running RaUI.

If "Use Zero Configuration as Configuration utility" is selected, please continue.

We will explain the difference between RaUI and WZC. Figure 1-3 shows the RaUI status when WZC is activated as the main control utility.

R Rell		90						8
Profile	Network	Advanced	Statistics		Ø WPS	Radio On/Off	About	1
Sorted by ++	🔘 SSID	 Channe 		Signal		Show dBn		
Shiang 2860 M	p	11	800	81%				
331		#3	89 9	55%				
AlbertY-200		26	89 9	768				
AP		61	89 9	553				
AP1		26	89	100%				. 11
APPA		106	090	703		_		
asus		1011	89	81%			-	
Broadcom		611	89	81%				
Buffalo 54		1011	89	768				
Cobra		100	89 9	340				
Rescan	Add to Portfor	Constant						
Status	>> AP1 <> 00-03-7F-	00-07-44	1		Line Q	uality ++ 100%	-	
Extra Info	** Link is Up (D:Powe	H110019			Signal 11	ningth 1 ++ 100N		
Channel	>> 6 e> 2437000 AP	ta:			Signal Sh	rengto 2 so 1005		_
Encryption	>> Orectowes				Mone C	handle to Stat		-
Network Type	** Infractructure			a anomali	Page 2	creation of some		
IP Address	>> 192.168.5.4D			Live Speed >>	54.0 Mbps	Maxe		
Sub Heck	>> 255.255.255.0			Throughput >>	0.000 Mbps	0.104		
Default Gateway	** 192.168.5.254					Hops		
	HT		5	lecelve			1.1.1	
E₩ >> n/a		SNRD >> n/a		Link Speed >>	54.0 Mbps			
GI >> n/a	WCS >> n/a	SNR1 >> n/a		initiaghput >>	D TOAR MODE	05.746 Alber		

Figure 1-3 RaUI status with WZC active

When activating WZC, there are several difference with the RaUI status, compared to the RaUI status without WZC running.

• The profile button will be gray. Profile functionality is removed since the NIC is controlled by WZC.

² The connect and add profile function will be gray. Profile functionality is removed since the NIC is controlled by WZC.

Please read through this document for full details on the other functions provided by RaUI.

4.1.2 Use WZC to configure wireless NIC

• If there is no connection or it is lost, the status prompt will pop up, as shown in Figure 1-4.



Figure 1-4 status prompt for no connection

2 Right-click the network connection icon in taskbar.

Change Windows Firewall settings	
Open Network Connections	
Repair	23
View Available Wireless Networks	11 12
	X

Figure 1-5 Select WZC main status

3 Select "View Available Wireless Networks" and the "Wireless Network Connection" dialog box will pop up, as shown in Figure 1-6.



Figure 1-6 Wireless Network Connection

• Select the intended access point and click "Connect". Then click "Connect Anyway" as shown as Figure 1-7.



Figure 1-7 Select intended AP : AP1, then click "Connect"



Figure 1-8 Connect AP : AP1 successfully

⁶ If you want to modify information about the AP, click "Change advanced settings" as shown in Figure 1-9. Then select the "Wireless Networks" tab shown as Figure 1-10.



Figure 1-9 Click "Change advanced settings"

🕹 Wireless Network Connection Properties 🛛 🔹 🔀
General Wireless Networks Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
View Wireless Networks
Preferred networks: Automatically connect to available networks in the order listed below:
P AP1 (Automatic) Move up
Move <u>d</u> own
Add <u>R</u> emove <u>Properties</u>
Learn about <u>setting up wireless network</u> Ad <u>v</u> anced
OK Cancel

Figure 1-10 Choose the "Wireless Networks" tab

6 Click "Properties" as shown in Figure 1-11. Then click "OK" button.

AP1 properties		?×
Association Authentication Cor	nnection	
Network <u>n</u> ame (SSID): AP1	1	
Wireless network key		
This network requires a key for	the following:	
Network <u>A</u> uthentication:	Open	~
Data encryption:	Disabled	~
Network <u>k</u> ey:		
Confirm network key:		
Key inde <u>x</u> (advanced): 1 ✓ T <u>h</u> e key is provided for me a	automatically	
This is a <u>c</u> omputer-to-computer access points are not used	er (ad hoc) network; wireles	:S
	ОК	Cancel

Figure 1-11 AP's properties

? After filling in the appropriate value, click "OK." The pop-up will indicate the status. as shown in Figure 1-12.

👘 Wireless Network Connection is now connected 🗵
Connected to: AP1 Signal Strength: Excellent
47 👻 🖉 💊
Figure 1 12 Notwork connection status

Figure 1-12 Network connection status

[®] Clicking the Ralink icon will bring up the RaUI main window. Users can find the surrounding APs in the list. The currently connected AP will be shown with a blue icon beside it, as shown in Figure 1-13. Users may use the advanced tab to configure more advanced features provided by Ralink's wireless NIC. For details on configuring the advanced features, please check the Advance setting section.

Rell		90						
Profile	Network	Advanced	Statistics		() WPS	Radio On/Off	About	
iorted by >>	🔘 SSID	 Channe 	4214	Signal		Show dBn		
Shiang 28604	ø	10	890	81%				-
331		43	89 9	55%		_		
AlbertY-200		36	Bg e	768				
AP		61	89 9	55%		-		
AP1		100	Bg	100%				
APPA		66	000	703				
8545		1011	Bg	81%				
Broadcom		611	Bg	81%				
Buffalo 54		1011	Bg	768				
Cobra		36	89 9	34%				
Rescan	Add to Portion	Gameriat						
Stabus	>> AP1 <> 00-03-7F-	00-07-44			Line C	uality ++ 100%		
Extra Info	++ Link to Up (FxPowe	H110010			Lignal 11	wight 1 ++ 100N		
Channel	>> 6 +> 2437000 AP	ta .			Signal Sh	engto 2 in 1005		
Encountion	>> Unknown				Hers Pr	engeni) in 1004		
Network Type	>= Infractructure			a second	PROTEIN 2	crenges >> acce		
IP Address	>> 192.168.5.40			LKR. Speed >>	54.0 Mbps	Max		
Sub Hark	>> 255.255.255.0			Throughput >>	0.000 Mbps	0.004		
Default Gateway	>> 192.168.5.254					HEIPS		
	нт		6	lecelve			1.1	
ttw >> n/a		SNRD >> n/a		Link Speed >>	54.0 Mbps	Max		
GI >> n/a	WCS >> n/a	SNR1 >> n/a		Throughput >>	0.098 Wbps	35.746 Hbox		

Figure 1-13 Show connection status by using WZC to initiate the connection

4.2 RaUI

4.2.1 Start

4.2.1.1 Start RaUI

When starting RaUI, the system will connect to the AP with best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 2-1.

Utility Config

RAUL									E
Profile	i.	Network	Advanced) Statistics	VIII	M WPS	Radio On/Off	About	
Sorted by >>	0	SSID	 Channel 	(2)	Signal		Show dBn		
_Shiang_2860	10		611	890	81%	-			6
333			13	69	P 55%	-			
AlbertY-200			26	Ba ·	• 76%	-			
AP			101	Ba ·	· 55%	_			
b AP1			130	R.a	100%	_			- 11
APPA			100	nan.	718	_			- 1
acca.			101		818	_		-	
Reading			10		0.4%			-	
Buffele Ed			10		3.0	_			
Cobra			100	Ba	9 343				
Reican		Add to Profil	Connec	t					
Statu	>> AP	1	00-07-#4			10	Quality ++ 1015	_	1
Extra info	>> Lit	k II Up (TxPowe	r: 100N]			2404	Alter at 1 +> 60%		
Channe	100 6 4	-> 2407000 WH	व			Signal	Shrength 2 in KEM	-	
Authentication	i an Un	known				200	gth 3 >> 50%		
Encryption	1 >> NO	ne				Note	e Strength >> 26%		
IP Address	535 IM	2 149 5 113				Tranumit.	Alace		
Sub Mark	10 25	5,255,255.0				Link Speed ++ 54.0	Mbps		
Default Gateway	19 19	2.168.5.254				throughout >> 0.00	PICLE IDAN OF		
		нт				Bacelue	MODS		
DW >> m/a			240 >> n/a			Link Speed >> 54.0	Max Max		
GI⇒≻n/ð	,	₩CS >> n/e	SVR1 >> n/a			Throughput >> 0.01	14 Mbps 0.090		

Figure 2-1-1 RaUI section introduction

There are three sections to the RaUI dialog box. These sections are briefly described as follow.

1 Button Section: Include buttons for selecting the Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, the About button, Radio On/Off button and Help.



2 Function Section: Appears to present information and options related to the button.

Profile List		
	Profile Name >>	
	SSID >>	
	Network Type >>	
	Authentication >>	
	Encryption >>	
	Use 802.1x >>	
	Channel >>	
	Power Save Mode >>	
	Tx Power >>	
	RTS Threshold >>	
	Fragment Threshold >>	
Add Date Delete Arthure		
Maa Don Donote Wolffeld		



Sorted by >>	SSID	Channel	AP List	Signal	Show d8m
_Shiang_2860AP aaa AlbertY-200		1011 1月3 106	890 897 89 7	81% 55% 76%	
AP AP1 APPA		101 106 106	89 † 89 890	55% 100% 70%	
asus Broadcom Buffalo 54 Cobra		日 11 日 11 日 11	59 69 69	81% 81% 76% 34%	
Rescan	Add to Profile	Connect	-		_

Figure 2-1-6 Network page

Wireless mode >>	2.4+5G	Enable CCX (Cisco Compatible eXtensions)
		Turm on CCXW
		Enable Radio Measurements
Enable TX Burst		Non-Serving Channel Aeasurements limit 250 ns (0-2000)
Enable TCP Wind	ow Stze	
Fast Roaming at	-70 dBm	
Show Authentice	tion Status Dialog	
Select Yo	ur Country Region Code	
11 B/G >>	: CH1-11 •	
11 A >> 7	?: CH 36,40,44,48,52,56,60,64,100 ▼	
Apply		

Figure 2-1-7 Advance page

rames Transmitted Successfully		1432
rames Retransmitted Successfully		4
rames Fail To Receive ACK After All Retries		٥
ITS Frames Successfully Receive CTS		0
US Frames Fall To Receive CTS	•	0



WWW Setup Status WWWW >> Enabled	Power Save >> Disabled			Direct Link >> Disabled
WHM Enable				
WWW - Power Save Enab	e			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Enable	L. C.			
HAC Address >>		Timeout Value >>	60 580	Apply
				Tear Room

Figure 2-1-9 WMM page

hsinchu1	00-11-26-71-27-68	6	ę	Rescan Informatio Pin Code 64093345 A	алем
	WPS Profile List			Config Node	
				Enrolee	*
				Corriso	
				Rotate	
				Dtsoonner	rt.
EIN WPS Associate IE	Progress >> 0%			Esport Pro	(iis
POC WPS Probe IE				Delete	-
Automatically select the M	2				

Figure 2-1-10 WPS page

(c) Copyright 2007, Ralink Technology, Inc.	All rights reserved.	
ReConfig Version >> 2.0.0.3	Date >> 04-06-2007	
Driver Version >> 1.0.2.0	Date >> 03-12-2007	
EEPROW Version >> 1.1		
Firmware Version >> 0.6		
Phy_Address >> 00-0C-43-29-60-04		
WWW.BAL	INKTECH.COM	

Figure 2-1-11 About page

3 Status Section: This section includes information about the link status, authentication status, AP's information and configuration, and retrying the connection when authentication is failed.



Figure 2-1-12 Link Status

	Authentication Sta	itus
Card Name >> Rahnk. 802. 11n Wireless LAN Card		Connected by manual
16:37:25.062 16:37:25.171 16:37:25.201 16:37:28.375	Starting network connection Network is connecting PEAP Authenticating Wireless client is authenticated.	
	Cancel	

Figure 2-1-13 Authentication Status

General	WPS	CCX	
	SSID >> AP1		
MAC A	ddress >> 00-03-7F-00-1	07-44	Signal Strength ++ 102%
Authenticatio	n Type >> Uhknown		Supported Rates (Mbps)
Encryptio	n Type 😣 None		1, 2, 5, 5, 11, 6, 12, 24, 36, 9, 18, 48, 54
¢	hannel >> 6> 240700	0.1042	
Network	. Type Infrastructur		
Beacon In	/terval >> 100		
			~

Figure 2-1-14 AP's Information

identity >>	
Password ++	
Cancel	
1.1.1	
	identity >> Password >> Cancel

Figure 2-1-15 Retry the connection

Authentication	NPA T	Encryption >> TKIP V	
an Keu			
ieb weż			
@ ney#1	recidection 💌	1	
@ terri	Perinterral 🖛		
0.100	noutcone		
@ 10041	(Receiption) (W		Show Password

Figure 2-1-16 Configuration

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close RaUI utility.



Figure 2-1-17 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:



R+ : Indicates the connected and signal strength is good.

 \mathbb{K}_{+} : Indicates the connected and signal strength is normal.

: Indicates that it is not yet connected.

: Indicates that a wireless NIC can not be detected.

 $\mathbf{R}_{\mathbf{F}}$: Indicates that the connection and signal strength is weak.

4.2.2 **Profile**

4.2.2.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 shows the basic profile section.

Profile List	
	Profile Name >>
	SSID >>
	Network Type >>
	Authentication >>
	Encryption >>
	Une 802.1x >>
	Channel >>
	Power Save Mode >>
	Tx Power >>
	RTS Threshold >>
	Fragment Threshold >>
Add Edit Deinte Activate	

Figure 2-2-1 Profile function

Definition of each field:

Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).

2 SSID: The access point or Ad-hoc name.

3 Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.

Authentication: Indicates the authentication mode used.

5 Encryption: Indicates the encryption Type used.

Use 802.1x: Shows if the 802.1x feature is used or not.

Cannel: Channel in use for Ad-Hoc mode.

⁸ Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.

9 Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.

(O RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.

• Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

Icons and buttons:

• ^a: Indicates if a connection made from the currently activated profile.

2 **b**: Indicates if the connection has failed on a currently activated profile.

3 9: Indicates the network type is infrastructure mode.

Indicates the network type is in Ad-hoc mode.

6	Sorted by >>	SSID	🖉 Channel	Ø Signa	Indicates if
the	e network is sec	urity-enabled.			
6	Rescan	: Click to add a	new profile.		
0	Connect	: Click to edit ar	n existing profile.		
8	Add to Profile	: Deletes an exi	sting profile.		
9	Activate	: Activates the s	elected profile.		
10	: Shows inf	ormation of the r	related status section		
0	🔺 : Hides info	ormation of the re	elated status section.		

There are three methods to open the Profile Editor dialog box.

You can open it by clicking the "Add to Profile" button in the Site Survey tab.

2 You can open it by clicking the "Add" button in the Profile tab.

³You can open it by clicking the "Edit" button on the Profile tab.

Profile N	ame >> PROF1				Network Type >>	Infrastructure	
	SSID >> AP1			-	To Power >>	Auto	•
Power Save A	ode >> 🥥 CAN	PSM			Prestary	2649	Ψ.
RTS Threshold		6			1 297	2543*	
Fragment Threat	old	256			-) 226	2346	
ystem Config Authentication =	Auth, \ Encry,	187	CK Encryption >>	Cancel		802.1X	
ystern Config Authentication + WPA Preshared	Auth, \ Encry,	187	OK Encryption >>	Cancel None 🔻		802.1X	
ystern Config Authentication = WPA Preshared up Key	Auth, \ Encry, Cpen 👻	197	CK Encryption >>	Cancel None 🔻		802.1X	
Authentication = WPA Preshared To Key Key#1	Auth, \ Encry, Cpen 👻 Key >> Hecadecinal	•	OK Encryption >>	Cancel		802.1X	
vstern Config Authentication = WPA Preshared op Key Key#1 Key#2	Auth, \ Encry, • Open • Key >> Hecadectrial Hecadecimal	•	OK Encryption >>	Cancel		802.1X	
Authentication = WPA Preshared op Key Key#1 Key#2 Key#3	Auth, \ Encry, Open • Key 35 Hecadectrial Hecadectrial Hecadectrial	•	CK Encryption >>	Cancel		802.1X	

Figure 2-2-2 Configuration

• Profile Name: The user can chose any name for this profile, or use the default name defined by system.

2 SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.

Ower Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.

• Network Type: There are two types, infrastructure and 802.11 Ad-hoc mode. Under Ad-hoc mode, user can also choose the preamble type. The available preamble type includes auto and long. In addition, the channel field will be available for setup in Ad-hoc mode. **9** RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or key in the value directly. The default value is 2347.

6 Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-hoc network.

⁽⁸⁾ Authentication Type: There are 7 type of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

⁹ Encryption Type: For open and shared authentication mode, the selection of available encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.

0 802.1x Setting: This is introduced in the topic of "Section 3-2 : 802.1x Setting".

WPA Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys.

- 1. Hexadecimal 40bits : 10 Hex characters.
- 2. Hexadecimal 128bits : 26Hex characters.
- 3. ASCII 40bits : 5 ASCII characters.
- 4. ASCII 128bits : 13 ASCII characters.

4.2.2.3 Example to Add Profile in Profile

Olick "Add" below the Profile List.



2 The "Add Profile" will appear.

Utility Config

Profile List Profile Name >> SSD >> Network Type >> Network Ty
Profile Name >> SSID >> Network Type >> Authentication >> Encryption >> Use 802.1x >> Channel >> Tic Power >> RTS Threshold >> Fragment Threshold >> Fragment Threshold >>
Add Edit Tetter Articles
Add Tetra Authors Authors Authors Authors Authors Authors Authors Add Authors
Autheritication >> Encryption >> Use 802.1x >> Channel >> Tx Power >> Tx Power >> RFS Threshold >> Fragment Threshold >> Fragment Threshold >>
Add Entryption ** Ute 802.1x ** Power Save Hode ** Tic Power ** R75 Threshold ** Fragment Threshold ** Fragment Threshold **
Add Edit Tettra Article
Power Save Hode >> Tic Power >> R75 Threshold >> Pragment Threshold >> Fragment Threshold >> Fragment Threshold >>
Add Edit Teltra Article
Add Ent Dente Activity
Add Edit Defite Activate
Ass For Performance
stem Config Auth. \ Encry.
stem Config Auth. \ Epcry.
Profile Name >> PROF1 Network Type >> Infrastructure 👻
TX Power >> Auto
Parment and
Power Seve Hode >> @ CAN @ PSM
Ars Inventoo

3 Specify a Profile Name. Select an AP from the SSID drop-down list. The AP list from the last Network.



Onw the profile which the user set appears in the profile list. Click "Activate".

Utility Config



4.2.3 Network

4.2.3.1 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as shown in Figure 2-3-1-1.

Sorted by >>	🙆 SSID	Channel	AP List	Signal	Show dBm	
_Shiang_2860AP		1 /11	890	81%		<u>^</u>
333		3	69 7	55%		
AlbertY-200		106 101	59 T	76%		
AP1		6	69	100%		- 1
APPA		106	690	70%		
asus		11	69	81%		-
Broadcom Brefelo 54		10 ¹¹	69	81%		
Cobra		6	89 9	34%		~
Rescan	Add to Profi	e Connec	1			

Figure 2-3-1-1 Network function

Definition of each field :

SSID: Name of BSS or IBSS network.

Overwork Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.

³ Channel: Channel in use.

O Wireless Mode: AP support wireless mode. It may support 802.11b, 802.11g or 802.11n wireless mode.

5 Security-Enable: Indicates if the AP provides a security-enabled wireless network.

6 Signal: Receive signal strength of the specified network.

Icons and buttons :

• a : Indicates that the connection is successful.

2 9: Indicates the network type is in infrastructure mode.

Indicates the network type is in Ad-hoc mode.

3 Sorted by >> O SSID O Channel Signal : Indicates

that the wireless network is security-enabled.

● ⓑ: Indicates 802.11b wireless mode.

🥑 🖳 : Indicates 802.11g wireless mode.

🕴 🗓 : Indicates 802.11n wireless mode.

 Sorted by >>
 SSID
 Channel
 Signal
 Indicates

 that the AP list is sorted by SSID, Channel or Signal.

Connect : Button to connect to the selected network.

Rescan : Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

^{Add to Profile}: Adds the selected AP to the Profile setting. It will bring up a profile page and save the user's setting to a new profile.

📵 💌 : Shows the Status Section.

🕑 本 : Hides the Status Section.

Connected network:

• When RaUI firstruns, it will select the best AP to connect to automatically.

2 If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.

³ If the intended network uses encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to the example on how to fill in the security information.

When you double click an AP, you can see detailed information about that AP.

The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode.) The introduction is as follows:

• General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.

First Pro	ofile	Network	Advanced	M		1000	69		\sim	1.0	
Sorted by >>	٥			Statistic	5	WWW	WPS	Radio On/Off	About	-	
132		5510	Channel	1		Signal		Show dBm			
202			102	89	1001	100%					
4114			101	Bg		703.					
213			1011	Bg	-	29%					
215			36	Bg		443		-			
219			101	69	•	81%				. 1	
243			\$5	69	•	100%					
_SNang_2	8604P		811	890	1	911			-		
AP			101	Bg	•	50%		_			
AP1			80	890	0	100%					
APPA			106	690		918					
Restar		Add to Profile	Connec	1							
General WPS CCX					802.11n						
		5510 >> AP1									
	HAC -	Address >> 00-0	0-7F-00-07-44				Ngnai Strengtr	11.102%			
*	uthenticatk	an Type >> Unkin	own		Su	ported Rates	(adM)				
	Increate	an Type None			1, 2, 5, 5, 11, 6, 12, 24, 36, 9, 18, 48, 54						
	1000	unanna >> o s	> 2437000 MH2								
	Netwo	rk. Type >> Infra	structure								
	Seacon	nterval >> 100									

Figure 2-3-1-2 General information about the Access Point

2 WPS information contains the authentication type, encryption type, config. methods, device password ID, selected registrar, state, version, AP setup lock status, UUID-E and RF bands, as shown in Figure 2-3-1-3. The information is further explained as follows :

• Authentication Type: There are three types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

² Encryption Type: For open and shared authentication mode, the choices of the encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

³ Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars, (a bitwise OR of values.)

Value	
0x0001	
0x0002	
0x0004	
8000x0	

Hardware Interface USBA (Flash Drive) Ethernet Label Display

0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	Push Button
0x0100	Keypad

• Device Password ID: Indicates the method or identifies the specific password that the selected Registrar intends to use. The AP in PBC mode must indicate 0x0004 within the two-minute Walk Time.

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	PushButton (PBC)
0x0005	Registrar-specified
0x0006-0x000F	Reserved

⁶ Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

State: The current configuration state of the AP. The values are "Unconfigured" and "Configured".

Version: The specified WPS version.

⁶ AP Setup Locked: Indicates if the AP has entered a locked setup state.

9 UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. The value is 16 bytes.

(O RF Bands: Indicates all of the RF bands available to the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

Ε,	Profile		Network.	Advan	¢ ced) Statistic	s		Ø WPS	Radio On/Off	About	
iorted by	-93-	0	SSID		Channe	13 A		Signal		Show dBm		
132					102	89	0.00	100%				
202					31	Bg		70%		_		
213					1011	Bġ	-	29%				
215					36	69		443		-		
219					61	69	•	81%				
243					\$5	69	9	100%				
_SNianj	g_28604P				111	891	n	91%				
AP					61	69	1	50%		_		
AP1					36	69	0	100%				
APPA					106	69	0	91%				
Ren	ican		Add to Profile	line ne	Carner	t						
General			WPS		C	x		802.11n				
		Aut	hentication Typ	e >> Unkry	win					tate >> Unknown		
			Forevotion Tun	e st None					144	rtion >> Uningen		
Encryption Type >> None Config Methods >> Unknown Device Password ID >> Selected Registrar >> Unknown												
						AP Setup Locked ++ Unknown						
							UUID-E >> Unknown					
						Rf Bands >> Unknown						

Figure 2-3-1-3 WPS Detailed information about the AP

3 CCX information contains the CCKM, Cmic and Ckip information. It is shown in Figure 2-3-1-4.
Utility Config

Profile		Network	Advanced) Statistics	e.		Ø WPS	Radio On/Off	About	5
orted by >>	0	SSID	Channel	1	0	Signal		Show dBm		
132			1 /2	89	cut	100%				
202			101	Bġ		70%				1
213			1311	Bġ	•	29%				
215			36	Bg		448		-		
219			101	Bg	•	81%				
243			\$5	Bg	9	100%				
_Shlang_286044	i.		1011	890		91%			-	
AP			61	69	•	50%		-		
AP1			86	690	0	100%				
АРРА			10 to	690		918 💼				
Pescan		Add to Profi	e Connec	-						
General		WPS	00	x		802.11n				
0 0	KM >> TiC >> KID >>	PALSE FALSE FALSE								

Figure 2-3-1-4 CCX information about AP's detail information

• 802.11n information contains some related 802.11n information. It is shown in Figure 2-3-1-5.

E-												_
Profile	1	letwork	Advan	₿ ced) Statistic	s			() WPS	Radio On/Off	About	-
orted by >>	0 5	SID		Channe	-		Signal			Show dBm		
132				102	89	0.001	100%					
202				b1	80		70%					-
212				1511			728		_			
245				sh.		. 1				_		
213				4			448				_	
219				01	D 9	I	81%					
243				105	Бg	Ť	100%					
_SNiang_28604P				611	69(9	91%				-	
AP				61	69	9	50%					
AP1				36	690	3	100%					
АРРА				10	890	0	918				-	
Restan	-	Add to Profile	State State	Connec	1							
General		WPS		cc	x		802.11n					
Secondary Ch Secondary Char	innet (inei Off	Miset eleme set					0	33			1	
HT Information	Exchan	ge Support	etenent				FALSE					
Alobiity Domain	ert elen	bent					FALSE					
High Throughpu	t						FALSE					
HT Capabilities	elene	Int					19400					
HT Capability	nahiti-						FALSE					
Supported Char	nel Wid	th Set.					0					
Serie - P							×.				1	ŧ.

Figure 2-3-1-5 802.11n information

4.2.3.2 Example on Adding Profile in Network

• Select the AP from the list on the Network tab

Utility Config

Profile	8	Network.	Advanc) :ed !) Statistics		Vitte			Radio	n/Off	About	
orted by >>	0	SSID		Channel			Signal				Show dBm		
AlbertY-200				ibi	89		603	_			-		
AP				10	Bg	•	70%	_			-		
AP1				66	89		100%	-					
Broadcam	_			юп	<u>C</u> g	_	70%	-					-
BroadcomWPS				101	89	٩	100%						11
DennisAP				10	890		76%	-					
Fiona-Ap				1011	890		441	-		-			
159-3F-asus11b				10		•	20%	_					
knilar				10B	(Ba	•	603	_					
NB27-PC_Netw	ork			106	890	19	81%	_					
Rescan	-	Add to Profil	an in	Connect									
Status	11 JO	t +-+ 00-03-7F-	00-07-44							s. Quetty /	1 1005		
Extra Info	>> Lm	k to Up (ToPowe	r:1001g						ing to	(It)mugh	1 1+ 100%		
Channel	** 6 *	> 2437000 MH	z								2		
Authentication	++ Uni	known							Tarr	the set	2++ IDIN		
Encryption	>> No	ne-							Not	se Strengt	n >> 26N		
IP Address	sp. 192	2, 168, 5, 60					31	irensmit -		n lilbert	Max		
Sub Hask	>> 25	5.255.255.0						Througho	eg >> 94, ut >> 0.0	0 Mops 00 Whee			
Default Gateway	** 192	2.168.5.254						in order to			7,498		
		нт					R	ROSTINE				12.41	
B₩ >> n/a			SNED =	⊳n/a				Line Spe	ed >> 48.	D Mbps	Max		
$\mathbf{G} \mapsto \mathbf{n}/\mathbf{a}$	3	ACS → n/a	SNR1 ×	n/a				Throughp	ut >> 0.1	D4 Hbpc	89.620		

Olick "Add to Profile"

Rall1				_										
	Profile		Network	Advan	₿ ced	Statistics	6	Ville		O WPS	Radio	On/Off	About	
eted t	py sə	0	SSID		Channel		•	Signal				Show dBm		
Albert	416,700				iki:		0	20						
AD	11-200				131			2018				_		
API					ib.	00	1	100%				_		
Bros	deam				1011	R9		70%						-
Broan	dcom/WPS				101	C q	•	100%	_					
Denn	is AP				10	Ban		76%	_					
Fiena	Ap				1011	Bad		441	-					
1551-3	F-asus11b				100		•	20%	_					
knilar					BB	Bq.	•	60%	_					
NB27	-PC_Netwo	wk_		_	106	890	19	81%	-			-		
R	sican		Add to Profil	-	Connec	tt								
	Status -	. 10	t «→ 00-03-7F-	00-07-44				1		1.0	E. Quelty 1	100%		1
3	Extra Info >	+ 111	k to Up (ТиРоне	Hr:1001g						101	Through 1	1+ 100%	-	
	Channel >	* 6 *	> 2437000 MH	tz i								100%		
Auth	entication >	+ Uni	chowin							ligna	Channel and Chan	ee IDIN		
Nets	work Type >	+ Inf	astructure							MQR	e strength	>> 25%		
	P Address >	n 192	168.5.60						Link Sor	ert as \$4.	0 Mhot	Hax		1
	Sub Hask >	» 25	5.255.255.0						Through	out >> 0.0	00 Hibps			
befault	t Gateway >	+ 192	2.168.5.254									7,496 Albps		
			HT						Receive			18	10.08	
BW >:	> n/a			SNED >	⊳n/a				Link Spe	red >> 48.	D. Molpii	Max		
	n min		Con mia	Outra .	h 19.5 m				Throughe	1.0 ec tue	04 Wbpc			

3 The System section will appear at the bottom of the Add Profile window. You can specify your own profile name.

Utility Config

Profile		Network.	Advanced) Statistics	8		Ø	Radio	0n/Off	About	-
orted by >>	0	SSID	Channel	1 40	•	Signal			Show dBm		
AlbertY-200			6	89	•	60%					
AP			101	69	٠	70%			-		
AP1			86	00		100%					
Broadcom			611	69		70%					
BroadcomWP:	5		61	69	٩	100%					• 1
DennisAP			66	890	1	76%					
Fiona-Ap			611	690	1	442					
159-3F-asust1	b		63	B	9	20%					
knilar			60	69	٩	60%					
NB27-PC_Netv	vork		16	690	19	81%					
Rescan		Add to Profi	le Connec	t							
System Co	nfig	Auth. \ E	nory.	15							
	Profile	Name >> PROF	1			-	Network Ty	pe io ii	nfrastructure	-	
		551D >> AP1	0		•		Tx Pow	er əə	Auto	-	
Pow	r Seve	Hade 12 Q	CAN @ PSM		7		Primer		TANK	Ψ.	
1.57	1223										
RTS Three	shold		11				1 234	E	547.	_	
Fragmen	t Threa	hold	254				- 254	1	54(
E Fragmen	t Three	hold					_1	1	241		

• Next, you will see the new profile in the profile list. Click "Activate"



4.2.4 Advanced

4.2.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

Wireless mode >>	2.4+5G •	Enable CCX (Cisco Compatible eXtensions)
		Turm on COW
		Enable Radio Measurements
Enable TX Burst		Non-Serving Channel Weasurements (Imit 250 ns. (0-2000)
Enable TCP Winds	ow Size	
Fast Roaming at	-70 dBm	
Show Authentical	tion Status Dialog.	
Select You	ur Country Region Code	
11 B/G >> 0	: CH1-11	
11A>> 7	CH 36,40,44,48,52,56,60,64,100 💌	
Apply		

Figure 2-4 Advance function

Uireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported.

Wireless Protection: Users can choose from Auto, On, and Off. (This is not supported by 802.11n adapters.)

• Auto: STA will dynamically change as AP announcement.

2 On: The frames are always sent with protection.

Off: The frames are always sent without protection.

3 TX Rate: Manually select the transfer rate. The default setting is auto. (802.11n wireless cards do not allow the user to select the TX Rate.)

G Enable TX Burst: Ralink's proprietary frame burst mode.

Inable TCP Window Size: Optimise the TCP window size to allow for greater throughput.

6 Fast Roaming at-: enables fast roaming, which is set by the transmit power.

Select Your Country Region Code: There are eight countries to choose from in the country channel list.

8 Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.

Inable CCX (Cisco Compatible Extensions): Choose whether Cisco Compatible Extensions are supported or not.

1 LEAP turn on CCKM.

2 Enable Radio Measurement: can measure the channel every 0~2000 milliseconds.

Apply the above changes.

Icons and buttons:

● ▼ : Show the Status Section information.

I Hide the Status Section information.

4.2.5 Statistics

4.2.5.1 Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to

understand. Figure 2-5-1 shows the detailed page layout.

anes Transmitted Successfully		1432
anes Retransmitted Successfully		4
ames Fail To Receive ACK After Al Retries	-	0
IS Frames Successfully Receive CTS	•	0
IS Frames Fail To Receive CTS	•	0

Figure 2-5-1 Statistics function

Transmit Statistics:

rames Transmitted Succ	cessfully	-	1432
ranes Retransmitted Su	uccessfully		4
rames Fail To Receive A	CK After Al Retries		٥
TS Frames Successfully I	Receive CTS	-	0
15 Frames Fall To Recei	ve CTS	•	0

• Frames Transmitted Successfully: Frames successfully sent.

Prames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.

³ RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.

GRTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.

⁶ Frames Retransmitted Successfully: Successfully retransmitted frames numbers.

⁶ Reset counters to zero.

Receive Statistics:

Corner Benetium Concernfully		2453
Terres received successing		5155
rames Received With CRC Error	*	201964
ranes Dropped Due To Out-of-Resource		0
Suplicate Francis Received		0

• Frames Received Successfully: The number of frames successfully received.

2 Frames Received With CRC Error: The number of frames received with a CRC error.

³ Frames Dropped Due To Out-of-Resource: The number of frames dropped due to a resource issue.

Ouplicate Frames Received: The number of duplicate frames received.

Reset all the counters to zero.

Icons and buttons:

- ▼ : Show the Status Section information.
- In the status Section information.

4.2.6 WMM

4.2.6.1 WMM

Figure 2-6-1 shows WMM function of RaUI. It involves "WMM Enable", "WMM - Power Save Enable" and DLS setup. The introduction indicates as follow :

Setup Status WWW H	> Enabled	Power Save >> Disabled			Direct Link >> Disabled
WWW En	abie				
w	MM - Power Save Enable				
0	AC_BK	AC_BE	AC_VI	AC_VO	
D Di	rect Link Setup Enable				
	HAC Address >>		Timeout Value >>	60 580	Apply
					Tear Down

Figure 2-6-1 WMM function

WMM Enable : Enable Wi-Fi Multi-Media. The setting method follows Section 2-6-2.

2 WMM - Power Save Enable : Enable WMM Power Save. The setting method follows Section 2-6-3.

³ Direct Link Setup Enable : Enable DLS (Direct Link Setup). The setting method follows Section 2-6-4.

Icons and buttons:



Show the information of Status Section.

2 📥

Hide the information of Status Section.

4.2.6.2 Example to Configure to Enable DLS (Direct Link Setup)

Click the "Direct Link Setup Enable" checkbox

WWW Setup Status WWW >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WWW Enable				
WHW - Power Save Enable				
□ AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Enable				
NAC Address >>		Timeout Value >>	60 sec	Apply
				Tear Down

2 Change to "Network" function. Add an AP that supports DLS features to the Profile. The result will look like the Profile Page in the figure below.

16. R e	010								×
+	Profile	Network	Advanced) Statistics		() WPS	Radio On/Off	About	->
		Profil	e List						
) 29	ÚF1	AP1		B		Profile Name	>> PROF1		
						220	>> AP1		
						Network Type	>>> Infrastructure		
					3	Authentication	a sa Open		
						Encryption	>> None		
						Use 802.15	c⇒> NO		
						Channel	iss t		
					Po	mer Seve Hode	>> CNH		
						Tx Power	r ** Auto		
						RTS Threshold	1>> 2347		
					Fran	ment Threatest	1++ 2345		
	188		4000						
-	400	EDK	Delete	Activate	-			-	
	Status ++	AP1 00-03-7F-	00-07-44			Ler	Country ++ 100%	-	
	Extra Info ++	Link to Up (ToPowe	r:100%			- Dgra	Strength 1 ++ 100%		
	Channel >>	6 «~> 2437000 MH	12			Syna	Strength 2 ++ 100%		
**	uthentication ++	Open				Serve	Strength 2 ++ 100%		
1.1	Encryption >>	NONE				Note	re Strength >> 26%		
	etwork Type ++	Inniastructure			Trarond	t.		_	÷0
	Didt Mark as	144-100-1-00 185 385 385 0			Lts	Speed >> \$4.1	0 Mbps	22	
Det	auft Gateway ++	192.168.5.254			Thro	ughput >> 0.0	0.002		
		HT			Receive		1000	- Land	3
-	K>> n/a		SNR0 >> n/a		Lini	Speed >> 54.0	0 Mbps Max		0.0
0	ii >> n/a	WCS \mapsto n/a	SHR1 >> n/a		Thro	aghput >> 0.03	33 Hbps 1.448		

The DLS settings are explained as follows:

• Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform

to these two conditions:

- 1. Connect with an AP that support DLS features.
- 2. Ensure that DLS is enabled.

WWW >> Enabled	Power Save >> Dtsabled	đ		Direct Link >> Enabled
WMM Enable				
WIKM - Power Save Er	able			
AC_BX	AC_BE	AC_VI	□ AC_V0	
Direct Link Setup Ene	£80	_		
MAC Address >>	00 0c 43 28 60 00	Timeout Value >	> 600 sec	Apply
				Tear Down

² The Timeout Value indicates the time in seconds before it disconnects automatically. The value is an integer. The integer must be between 0~65535. A zero value specifies that it stays connected. The default Timeout Value is 60 seconds.

		Power Save >> Dtsabled			Direct Link >> Enabled
— ••	WMM Enable				
[WIKM - Power Save Enable				
	AC_BK	□ AC_BE	AC_VI	□ AC_V0	
I	Direct Link Setup Enable		_		
	MAC Address >> 00	0c 43 28 60 00	Timeout Value >>	600 sec	Apply
					Tear Down

3 Click "Apply"

A Setup Sta WW	tus H >> Enabled	Po	wer Sa	sve >	> Dt	sabled	1					Dire	ot Link >> Ene	bied
· · · · ·	Enable													
	WIMM - Power Save En	able												
	□ AC_BK		J AC,	36				AC_V						
	Direct Link Setup Ena	ible												
	MAC Address >>	00 00	43	28	60	00		Time	out Value >>	600	sec		Apply	
		00-0	C-43-0	28-60	-00					600		-	Tear Down	

Describe "DLS Status" as follow :

• After configuring the DLS successfully, the MAC address and Timeout Value are displayed in the "DLS Status". In "DLS Status" on the opposite side, the users local MAC address and Timeout Value are displayed.

Oisplay the values of "DLS Status" to "Direct Link Setup" as follow :

1. In "DLS Status" select a direct link STA what you want to show it's values in "Direct Link Setup".

WWW Enable WWW - Power Save Enable AC_BR AC_BE AC_BR AC_SE Direct Link Setup Enable MAC Address >> Timeout Value >> 60 sec Apply 00-00-40-20-60-00 600 Tear Down	WMM >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WMM - Power Save Enable AC_BR AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> Timeout Value >> 60 sec Apply 00-00-40-20-60-00 600 Tear Down	WAIM Enable				
AC_BK AC_BE AC_W AC_W AC_W Direct Link Setup Enable AAC Address >> Timeout Value >> 60 sec Apply 00-00-40-20-40-00 600 Tear Down	WMM - Power Save En	able			
Direct Link Setup Enable MAC Address >> Direct Link Setup Enable MAC Address >> Direct Link Setup Enable Orectored Content Value >> 60 sec Apply Tear Down	AC_BK	AC_BE	□ AC_91	AC_VO	
MAC Address >> Timeout Value >> 60 sec Apply 00-00-43-28-60-00 600 Tear Down	Direct Link Setup End	ble			
00-00-40-20-60-00 600 Tear Down	MAC Address >>		Timeout Value >	> 60 sec	Apply
		00-00-40-28-60-00		600	Tear Down

2. Double click. And the result will look like the below figure.

WWW >> Enabled	Power Save >> Dtsabled			Direct Link >> Enabled
WWW Enable				
WIMM - Power Save Ena	ble			
L AC_BK	□ 40_8€	AC_VI	AC_VO	
Direct Link Setup Enab	le			
MAC Address >> 0	0 00 43 28 60 00	Timeout Value >>	600 sec	Apply
	00-00-43-28-60-00		600	Tear Down

3 Disconnect Direct Link Setup as follow :

1. Select a direct link STA.

WWW Enable WWW Enable WWW Power Save Enable 40_BK A0_BE A0_BK A0_BE A0_BK A0_BE MAC Address >> 00 00-00-43-28-60-00 600 Tear Down	WWW >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WHM - Power Save Enable AC_PK AC_PE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 00 43 28 600 Timeout Value >> 600 sec Apply 00-00:-43-28-60-00 600 Tear Down	WWW Enable				
AC_BK AC_BE AC_VI AC_VO Divect Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply 00-0C+43-28-60-00 600 Tear Down	WINM - Power Save E	inable			
Direct Link Setup Enable MAC Address >> 00 00 43 28 60 00 Timeout Value >> 600 sec Apply 00-00-43-28-60-00 600 Tear Down	AC_BK	AC_BE	AC_VI	AC_V0	
MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply 00-00-43-28-60-00 600 Tear Down	Direct Link Setup En	able			
00-0C-43-28-60-00 600 Tear Down	MAC Address >>	00 00 43 28 60 00	Timeout Value	>> 600 sec	Apply
		00-00-43-28-60-00		600	Tear Down

2. Click "Tear Down" button. The result will look like the below figure.

W Setup Status WWW >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WWW Enable				
W1664 - Power Save D	nable			
□ AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup En	sble			
MAC Address >>	00 00 43 28 60 00	Timeout Value	600 sec	Apply
				Tear Down

4.2.6.3 Example to Configure to Enable Wi-Fi Multi-Media

If you want to use "WMM-Power Save" or "Direct Link" you must enable WMM. The setting method of enabling WMM indicates as follows:

Click "WMM Enable".

WWW Setu	p Sta WW	tus i >> Enabled	Power Save >> Dtsabled	Direct Link >> Disabled		
	www	Enable				
		WHM - Power Save Enable				
		AC_BK	AC_BE	AC_VI	AC_VO	
		Direct Link Setup Enable				
		HAC Address >>		Timeout Value >>	60 sec	Apply:
						Teor Down

2 Change to "Network" function. And add a AP that supports WMM features to a Profile. The result will look like the below figure in Profile page.



4.2.6.4 Example to Configure to Enable WMM - Power Save

Olick "WMM-Power Save Enable".

WAM Setup Status WAM >> Enabled	Power Save >> Disabled			Direct Link >> Disabled
WMM Enable				
- 4C_BK	AC_BE	□ AC_VI	AC_VO	
Direct Link Setup Enable		Timeout Value >>	60 sec	
				Tever, Down,
				_

2 Please select which ACs you want to enable. The setting of enabling WMM-Power Save is successfully.

WIWM Setup Status WIWM >> Enabled	Power Save >> Enabled			Direct Link >> Dirabled
WWW Enable				
WAMA - Power Save Enable				
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Enable				
WAG Address >>		Timeout Value >>	60 sec	Apply:
				Ten: Down

4.2.7 WPS

4.2.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.

	Profile	Network	Advanced) Statistics		() WPS	Radio On	/Off Abo	ar 🛯	
				WPS A	List					
î	ID : Unknown	تذ تذ	e-wes		00-10-15-90-25-27	1	-	Resoan		
11	ID : Unknown	ut	vicom_Sample		00-00-40-29-60-20	1		Information		
	ID : Unknown	ar	vint-2860AP		00-00-40-25-60-60	3	•	Pin Code		
	ID : Unknown	de	rlault		00-18-02-44-04-68	6	•	64993945 Ren	ion :	
				WPS Pro	file List		-	Config Hode		
								Enrolee	4	
								Sociect.		
								.Forfaite		
	PIN	WPS Asso	ciate IE		Progress so ON			Disconnect		
10	- HT.	THE LASS David						ter-thun	in the second	
1.0	har.	Mes Prot	# E	rs status is disco	nnected			Dertra		
		Automati	celly select the AP							
	Status >> AF	P1 ↔+> 00+03-7F+	00-D7-A4			119	Quality >> W	The second s		
	Extra Info +> Li	nk ti Up (TcPowe	r:100%					63%		
	Channel >> 6	<> 2407000 APt	2			Ng H	Chimpti 2 48	60%		
Aut	hentication ++ W	PA				Lignel 1	strength 3 ++	74.5		
	Encryption so Th	(IP+AES				Notre	Strength >> 2	R.W.		
	PAddress ++ 15	2.168.2.8			Traront			Ker I		
	Sub Wesk >= 25	5.255.255.0			Through	aut >> 54.07	Wapii Wanz			
Defa	It Gateway >> 19	2.168.2.254				nes 500000	rago.	5.112		
		HT			Receive				-	
333	>> n/a		thR0 >> n/a		Line. Spe	red >> 49.0.1	Https	Max 1		
TH:			Contraction of the local sectors of the		Throughout as 145,052 Kbox					

Figure 2-7-1 WPS function

• WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.

2 WPS AP List: Displays the information of the surrounding APs with WPS IE from the last scan result. The detailed information includes the SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.

³ Rescan: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

Information: Displays the information about WPS IE on the selected network. The detailed list includes the Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. Further details are available here: WPS Information on AP.

⁵ PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to re-generate a new PIN Code.

⁶ Config Mode: The station serving as an Enrollee or an external Registrar.

Table of Credentials: Displays all credentials obtained by the Registrar. The detailed list includes information about the SSID, MAC Address, Authentication and Encryption Type. If STA is the Enrollee, the credentials are created immediately with each WPS success. If STA is the Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change this until switching to STA Registrar.

8 Control items for credentials.

1. Detail: Command to obtain Information about Security and the Key in the credential.

2. Connect: Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.

3. Rotate: Command to rotate to connect to the next network inside credentials.

4. Disconnect: Stops the WPS action and disconnects the active link. It then selects the most recent profile on the Profile Page of RaUI. If there are no profiles, the driver will select any non-security AP.

5. Export Profile: Exports all credentials to a Profile.

6. Delete: Deletes an existing credential. And then selects the next credential. If there is not another credential, the driver will select any non-security AP.

9 PIN: Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.

PBC: Start to add to AP using PBC configuration method.

After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

UWPS associate IE: Sends the association request with WPS IE during the WPS setup. It is optional for STA.

WPS probe IE: Sends the probe request with WPS IE during WPS setup. It is optional for STA.

¹⁰ Progress Bar: Displays the rate of progress from Start to Connected.

Output: Content of the status of the stat

(b Automatically select the AP: Starts to add to AP by using to select the AP automatically in PIN method.

There are examples in section 2-7-3(PIN Enrollee Setup), section 2-7-4(PBC Enrollee Setup) and section 2-7-5(Registrar Configures and AP)

Icons and buttons:

- I Show the information of Status Section.
- 2 🛋 : Hide the information of Status Section.

4.2.7.2 WPS Information on AP

The WPS information (shown below) includes the authentication type, encryption type, config methods, device password ID, selected registrar, state, version, AP setup locked, UUID-E and RF bands.

Profile		Network	Advanc	ed.) Statistics	5		Ø VÆS	Radio On/Off	About	=
Sorted by >>	•	SSID		Channel	-		Signal		Show d8n		
132 202 213 215 219 243 				82 85 85 85 85 85 85 85 85 85 85 85 85 85			100% 70% 29% 44% 81% 100% 91% 50% 100% 91%		-		
General	Aut De	WPS hentication Typ Encryption Typ Config Method vice Pacaword I elected Registra	e >> Unknox e >> None E >> Unknox D >= r >> Unknox		×		902.11n	Ve "AP Setup Lo UL RF 8	itate >> Unknown rsion >> Unknown cked >> Unknown IID-E >> Unknown ands >> Unknown		•

• Authentication Type: There are three authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

2 Encryption Type: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK

authentication mode, the encryption type supports both TKIP and AES.

³ Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (a bitwise OR of values)

Value	
0x0001	
0x0002	
0x0004	
8000x0	
0x0010	
0x0020	
0x0040	
0x0080	
0x0100	

Hardware Interface USBA (Flash Drive) Ethernet Label Display External NFC Token Integrated NFC Token NFC Interface Push Button Keypad

Oevice Password ID: Indicates the method or identifies the specific password that the selected Registrar intends to use. APs in PBC mode must indicate 0x0004 within two-minute Walk Time.

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	PushButton (PBC)
0x0005	Registrar-specified
0x0006-0x000F	Reserved

⁵ Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

⁶ State: The current configuration state on AP. The values are "Unconfigured" and "Configured".

Version: WPS specified version.

⁶ AP Setup Locked: Indicates if the AP has entered a setup locked state.

9 UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. This is a 16 byte value.

(! RF Bands: Indicates all the RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

4.2.7.3 Example to Add to Registrar Using PIN Method

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The following image outlines the process.



• Select "Enrollee" from the Config Mode drop-down list.

		WPS AP List			
ID : Unknown	Ubicom_Sample	00-00-43-28-60-20	1	^	Rescan
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	P	Information
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	з	- P.	Pin Code
ID : Unknown	default	00-18-02-44-04-68	6	P 🖂	64893945 Ramew
		WPS Profile List			Config Mode
					Enrollee
					Detail
					Connect
					Rotate:
					Disconnect
gin 🛛	WPS Associate IE	Progress >> 0%			Export Profile
FBC 🛛	WPS Probe IE	WPS status is disconnected			Delete
	1	40			

Click "Rescan" to update available WPS APs.

Utility Config

ID : Unknown	Ubicom_Sample	00-00-43-28-60-20	1	^	Respan
ID : Unknown	AP 1-WPS	00-10-18-90-2E-27	1	P	Information
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	з	- -	Pin Code
ID : Unknown	default	00-18-02-4A-0A-68	6	9 💌	64893945 Renev
		WPS Profile List			Config Mode
					Enrollee 👻
					Detail
					Connect
					Rotate
					Disconnect
RIN 🛛	WPS Associate IE	Progress >> 0%			Export Profile
		Land to the second seco			

³ Select an AP (SSID/BSSID) that STA will join to.

		WPS AP List			
ID : Unknown	AP 1-WPS	00-10-18-90-25-27	1	7^	Rescan
ID : Unknown ID : Unknown ID : Unknown	Ubicom_Sample arvint-2860AP default	00-0C-43-28-60-20 00-0C-43-28-60-60 00-18-02-44-0A-68 WPS Profile List	1	•	Information Pin Code 64893945 Renew Config Mode Enrolee V Octof Connect Rotate
EIN	WPS Associate IE	Progress >> 0%			Export Profile
PBC	WPS Probe IE Automatically select the	WPS status is disconnected			DADLO

Click "PIN" to enter the PIN

6 Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	9 1	Rescan
ID : Unknown	Ubicon_Sample	00-0C-43-28-60-20	1		Information
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	з	•	Pin Code
ID : Unknown	default	00-18-02-44-04-6B	6	9 💌	64093945 Rene
		WPS Profile Ltst			Config Mode
					Enrolee
					Detel
					Connect.
					Rotate
					Disconnect
EIN 🗹	WPS Associate IE	Progress >> 5%			Export Profile
PEC 2	WPS Probe IE Start PI	N connection - AP1-WPS			Delate

Allow of an exchange between Step 4 and Step 5.

If you use <u>Microsoft Window Connection Now</u> as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

6 The result should appear as the image below.

		WPS AP List			
ID : Unknown	AP 1-WPS	00-10-18-90-25-27	1	9 ^	Research
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1		Information
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	з	•	Pin Code
ID : Unknown	default	00-19-02-4A-0A-68	6	7 💌	64893945 Renew
		WPS Profile List			Config Mode
					Enrollee 🗸
					Detail
					Connect
					Rotate
					Disconnect
PIN	WPS Associate IE	Progress >> 60 <mark>%</mark>			Export Profile
PBC 🖉	WPS Probe IE	PIN - Sending K3			Delete
	Automatically select the	AP			

Oconfigure one or more credentials

Utility Config

ID : Unknown	Ubicon_Sample	00-0C-43-28-60-20	1	<u>^</u>	Rescan	-	
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3	9	Informatio	n	
ID : Unknown	WinceWps	00-14-85-E3-D7-88	7	•	Pin Code		
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	9 💌	64893945 R	enew	
		WPS Profile List			Config Hode		
AP1-WPS		•			Enrollee	~	
		-			Detail		
					Connect		
					Rotate		
					Disconnec	, t	
EIN E	WPS Associate IE	Programs >> 100N			Export Pro	194	
PBC E	WPS Probe IE	PIN - Get WPS profile successfully.		_	Delete	-	

⁸ Then connect successfully. The result appear as the following image.

ID : Unknown	Ubicon_Sample	00-00-43-28-60-20	1	^	Rescan
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	3		Information
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7	• • •	Pin Code
ID : Unknown	AP1-WP5	00-10-18-90-25-27	1	7 🖂	64893945 Renew
		WPS Profile List			Config Node
AP1-WPS		٩			Enrolee Y
					Detail
					Connect.
					Rotate
					Disconnect
ein 🔛	WPS Associate IE	Progress >> %	10N		Export Profile
PBC	WPS Probe IE	PIN - Get WPS profile successfully.			Delete
	buttom a bis a bis colorade the				

Olick "Detail"

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1	^	Rescan
ID : Unknown	arvint-2860AP	00-0C-40-28-60-60	з	•	Information
ID : Unknown	WinceWps	00-14-85-E3-D7-88	7	•	Pin Code
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	9 🗸	64893945 Renew
		WPS Profile List			Config Mode
AP1-WP5		٥			Enrollee 👻
					Detail
					Connect
					Rotate
					Disconnect
EIN Z	WPS Associate IE	Progress >> 100%			Export Profile
29C	WPSProbe IE	PIN - Get WPS profile successfully.			Delete

U You will look like the below figure.

SSID IN	AP1-WPS			
Authentication Type >>	WPAPSK		Encryption Type ++ TKIP	
Key Length >> Key Aaterial >>	64		Key Index >> Key#1	
	9 Show Password			
		CK	Cancel	

If Credential#1 is reliable and present, the system will connect with Credential#1. If not, the system will automatically rotate to the next existing credential.

The user can also click "Rotate" to rotate to the next credential usable credential.

Describe "WPS Status Bar" - "PIN - xxx" as follow:

Acceptable PIN Configurations:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Req (Start) ~> Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

2 WPS configuration doesn't complete after a two-minute connection:

WPS EAP process failed.

³ When errors occur within two minutes of connecting, the WPS status bar might report "WPS Eap process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. Error PIN Code.
- 4. An inappropriate EAP-FAIL received.

4.2.7.4 Example to Add to Registrar Using PBC Method

The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately begin running the Registration Protocol.

If the Enrollee discovers more than one Registrar in PBC mode, it MUST abort its connection attempt at this scan and continue searching until the two-minute timeout.

*Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC mode or APs using PBC mode have left their Walk Time.

Push PBC button on both Registrar and Enrollee



• Select "Enrollee" from the Config Mode drop-down list.

ID : Unknown	Libicom_Sample	00-00-43-28-60-20	1	^	Rescan
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	•	Information
ID : Unknown	arvint-2860AP	00-00-43-29-60-60	э	•	Pin Code
ID : Unknown	default	00-18-02-44-04-68	6	÷ 🗸	64893945 Raney
		WPS Profile List			Config Mode
					Enrollee
					Detail
					Connect
					Astete
					Disconnect
EIN 🖬	WPS Associate IE	Progress >> 0%			Export Profile
P0/2	WPS Probe IE	WPS status is disconnected		_	Delete

2 Click PBC to start the PBC connection.

3 Push the PBC on AP.

		WPS AP List			
ID : Unknown	Ubicon_Sample	00-00-43-28-60-20	1	^	Respan
ID: 0x0004	AP 1-WPS	00-10-18-90-2E-27	1	9 -	Information
ID : Unknown	default	00-18-02-4A-0A-6B	6	9	Pin Code
ID : Unknown	WinceWps	00-14-05-E3-D7-08	7	7 🖂	64090945 Ranaw
		WPS Profile List			Config Wode
					Enrolee 👻
					Detwi
					Connest.
					Rotate
					Disconnect
ein 🛛	WPS Associate IE	Progress >> 0%			Export Profile
PBC	WPS Probe IE	Start PBC connection			Delete
	Automatically select the	AP			

*Allow time for an exchange between Step 2 and Step 3.

• The progress bar as shown in the figure below indicates that scanning progress.

Utility Config

ID : Unknown	Ubicon_Sample	00-00-43-28-60-20	1	^	Rescen
ID : Unknown	arvint-2860AP	00-00-43-28-60-60	э	7 -	Information
ID : Unknown	default	00-18-02-44-04-68	6	9	Pin Code
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7	9 💌	64893945 Renev
		WPS Profile List			Config Hode
					Enrolee 💙
					Detail
					Connect
					Rotate
					Disconnect
PIN I	WPS Associate IE	Progress >> 10%			Export Profile
-					Delete
PEC	WPS Probe IE PBC - Sc	anning AP			

⁽⁶⁾ When one AP is found, join it.

1	٩.	Respen
з	P	Information
10		Pin Code
		64893945 Renew
		Config Mode
		Enrolee 🛩
		Ostal
		Connect
		Rotate
		Disconnect
		Export Profile
		Delete
		-

Charles and Complex and
prace >> computed
Version >> 1.0
AP Setup Locked >> Unknown
UUID-E >> Unknown
RP Bands >> Unknown

6 Check WPS Information on the available WPS APs

Configure and receive one or more credential(s).

ID:0x0004	AP 1-WPS	00-10-18-90-2E-27	1	9 1	Rescan
ID : Unknown	Ubicom_Sample	00-00-43-28-60-20	1		Information
ID : Unknown	default	default 00-18-02-44-04-68 6 🕈			Pin Code
ID : Unknown	WinceWps	00-14-05-03-07-08	7	9 🖬	64093945 Renew
		WPS Profile List			Config Mode
AP1-WP5		9			Enrollee 💌
					Detail
					Connect
					Rotete
					Disconnect
EIN [WPS Associate IE	Progress >> 100%			Export Profile
	WPS Probe IE	t WPS nonfile successfully.			Delete

⁶ Then connect successfully. The result will be displayed as it is in the figure below.

		WPS AP List			
ID: 0x0004	AP1-WP5	00-10-10-90-25-27	1	9 ^	Rescan
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1		Information
ID : Unknown	default	00-18-02-4A-0A-6B	6	-	Pin Code
ID : Unknown	WinceWps	00-14-85-E3-D7-88	7	9 🗸	64093945 Renew
		WPS Profile List			Config Mode
AP1-WPS		ę			Enrolee 👻
,					Detail
					Connect
					Rotate
					Disconnect
EIN	WPS Associate IE	Progress >> 100N			Export Profile
PBC	WPS Probe IE PBC	- Get WPS profile successfully.			Delete
	Automatically select the AP				

Describe "WPS Status Bar" - "PBC - xxx" as follow :

A successful PBC Configuration :

Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Rsp (Start) ~> Sending M1 ~> Received M2 ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp (Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

ONO PBC AP available :

Scanning AP ~> No PBC AP available ~> Scanning AP ~> No PBC AP available

~>...

3 Too Many PBC AP available :

Scanning AP ~> Too Many PBC AP available ~> Scanning AP ~> Too Many PBC AP available ~>...

WPS configuration doesn't complete after **two-minute connection**:

WPS Eap process failed.

⁶ When Errors occur within **two-minutes of establishing a connection**, the WPS status bar might report "WPS Eap process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. An inappropriate EAP-FAIL received.

Describe "Multiple PBC session overlaps" as follow :

Dual bands:

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a A-Band AP using PBC mode. (ID = 0x0004)

They have the same UUID-E.

STA would regard these two APs as a dual-radio AP and select one band to connect.

2 Different UUID-E :

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a G-Band AP using PBC mode. (ID = 0x0004)

They have the different UUID-E.

STA would regard these two APs as two different APs and wait until only one PBC AP is available.

4.2.7.5 Example to Configure a Network/AP Using PIN or PBC Method



Select Registrar from the Config Mode drop-down list.

ID :	Claude WpsAP	00-14-05-ED-D7-08	1	•	Rescan
ID : Unknown	AP 1-WPS	00-10-16-90-2E-27	1	٩	Information Plin Code 64893945 Receiv
		MPS Profile List			Config Hode
E=RegNW286004		٩			Registrar 🗸
					Detail
					Connect
					Rotate
					Disconnect
EIN 🔚 1	WPS Associate IE	Progress >> 0%			Export Profile
PBC 🚺	WPS Probe IE	WPS status is disconnected			
	internationally calact the	aD.			

² Enter the details of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if needed.

1010	E30450104				
BSSID >>	00-00-00-00-00				
Authentication Type >>	WPA2-PSK	•	Encryption Type >>	AES	•
Key Length >>	5	-	Key Index >>	1	
Key Material >>	******		*****		
	Show Passee	brd			

³ If the PIN configuration is setup, enter the PIN sent from the Enrollee.

		WPS WP Ltst			
ID :	Claude/WpsAP	00-14-85-E3-D7-88	1	٩	Rescan
ID : Unknown	AP 1-WPS	00-10-18-90-25-27	1	٩	Information Pin Code 64890945 Sense
		WPS Profile List			- Config Mode
ExRegNW286004		۲			Registrar V Detail Connect Rotate
					Lisconnect
EIN	WPS Associate IE	Progress >> 0%			Export Profile
PBC	WPS Probe IE Automatically select the	WPS status is disconnected			j

• Start PIN or PBC. The following procedures are as similar as section 2-7-3 (PIN Enrollee Setup) or section 2-7-4 (PBC Enrollee Setup),

⁵ If your AP Enrollee has been configured before the WPS process, the credential you set in advance will be updated to the AP itself. Otherwise, after a successful registration, the AP Enrollee will be re-configured with the new parameters, and the STA Registrar will connect to the AP Enrollee with these new parameters.

ID :	ClaudeWpsAP		00-14-85-E3-D7-88	1	- 1	Rescan	
ID :	arvint-2860-WP	SAP	00-00-40-28-60-60	6	•	Informatio	on
					-	Pin Code	
						64893945	enew.
		WPS Profile List				- Config Mode	
ExRegNW286004			0			Registrar	~
						Detail	
						Connect	
						Rotate	-
						Disconnec	it.
EIN 🔚	WPS Associate IE		Progress >> 100%			Export Pro	file
PDC 🖬	WPS Probe IE	PIN - Get WPS profi	le successfully.				

Describe "WPS Status Bar" - "PIN - xxx" as follow :

A successful PIN Configuration :

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

Describe "WPS Status Bar" - "PBC - xxx" as follow :

A successful PBC Configuration :

Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

4.2.8 About

4.2.8.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-8.

(c) Copyinght 2007, Hamil Technology, Inc.	All rights reserved.
ReConfig Version >> 2.0.0.3	Date >> 04-06-2007
Driver Version >> 1.0.2.0	Date >> 03-12-2007
EEPROM Version >> 1.1	
Firmware Version >> 0.6	
Phy_Address >> 00-0C-43-28-60-04	
WWW.RA	LINKTECH, COM

Figure 2-8 About function

Connect to Ralink's website : Ralink Technology, Corp.

2 Display Configuration Utility, Driver, and EEPROM version information.

3 Display Wireless NIC MAC address.

Icons and buttons:

Image: Show the information of Status Section.

I Hide the information of Status Section.

4.2.9 Link Status

4.2.9.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-9.

Status Extra Info Channel Authentication Encryption	>> AP1 <-> 00-03-7F- >> Link is Up [TxPowe >> 6 <-> 2437000 AH >> Unknown >> None	00-07-44 rr: 10094 2	Link Quality +> 100% Signal Strength 1 >> 100% Signal Strength 2 >> 100% Signal Strength 3 >> 100% Notes Strength >> 20%		
Network Type IP Address Sub Hask Default Gateway	>> Infrastructure >> 192.168.5.40 >> 255.255.255.0 >> 192.168.5.254 HT		Transmit Link Speed >> 54.0 Mbps Throughput >> 0.000 Mbps	Max 0.004 Mbps	
51¥i≫ n/a Gi≫ n/a	₩CS >> n/a	94RD≫ n/a 94R1 ≫ n/a	Receive Link Speed >> 54.0 Mbps Throughput >> 0.111 Mbps	Max 0.245 yr dinte diastantau Mbps	

Figure 2-9 Link Status function

• Status : Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.

- 2 Extra Info : Display link status in use.
- ³ Channel : Display current channel in use.
- Authentication : Authentication mode in use.
- ⁶ Encryption : Encryption type in use.
- ⁶ Network Type : Network type in use.
- IP Address : IP address about current connection.
- ⁶ Sub Mask : Sub mask about current connection.
- 9 Default Gateway : Default gateway about current connection.
- Ulink Speed : Show current transmit rate and receive rate.
- Throughout : Display transmits and receive throughput in unit of Mbps.

¹² Link Quality : Display connection quality based on signal strength and TX/RX packet error rate.

⁽⁸⁾ Signal Strength 1 : Receive signal strength 1, user can choose to display as percentage or dBm format.

Gignal Strength 2 : Receive signal strength 2, user can choose to display as percentage or dBm format.

I Signal Strength 3 : Receive signal strength 3, user can choose to display as percentage or dBm format.

¹⁰ Noise Strength : Display noise signal strength.

U HT : Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value. (Show the information only for 802.11n wireless card.)
4.3 Security

4.3.1 Auth. \ Encry. Setting - WEP/TKIP/AES

A	uthentication >>	WPA-PSK	63) 	Encryption	>> AES 🔻	
	WPA Preshared K	iey >>				
Vep Ke	a.					
0	KestP1	HEXEDECTION	* [-
0	h41#2	Newsdoctrol	* [-
0	10:575	Hereiterteit	+ [-
0	Note:	(Hesashirmi)	· • [Show Password

Figure 3-1 Auth.\Encry. Settings

• Authentication Type: There are 7 authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

Encryption Type: For open and shared authentication mode, the available encryption types are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

3 8021X: This is introduced in the topic of Section 3-2.

• WPA Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

⁵ WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.

• Hexadecimal - 40bits: 10 Hex characters.

Period - 128bits: 32Hex characters.

③ASCII - 40bits: 5ASCII characters.

• ASCII - 128bits: 13 ASCII characters.

**Powered by Meetinghouse.

4.3.2 802.1x Setting

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.

	TCH -				LAP HOUSE 12		
ID \ PASSWO	ORD	Client C	ertification	Server	Certification		
Authentication ID / P	assword						
Identity	22	_	Persistent ++		Dorre	n Harts	
	1						
funnel ID / Password	· · · · · · · · · · · · · · · · · · ·	1.1	12 1 1				
Identify	2.5		Pacsword >>				

Authentication type:

• PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

2 TLS/Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

3 TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

• EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.

6 LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.

⁶ MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

Session Resumption: The user can choose "Disable" and "Enable".

Tunnel Authentication:

• Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".

² Tunnel Identity: Identity for tunnel.

³ Tunnel Password: Password fortunnel.

ID \ PASSWORD

• Authentication ID/Password: The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.

² Tunnel ID/Password: Identity and Password for the server.

Client Certification

EAP Method >>	PEAP	👻 Turne	Authentication >>	EAP-MSCHAP v2	•	Session Resumption
ID \ PASSWO	ORD	Client Certifica	ition Serv	er Certification		
Use Client cert	ricate	wpatest2 2003serv 4/9/2008				
		inst	ed To >> wpatest2			
		Iso	ed By >> 2003serv			
		Expir	ed On >> 4/9/2008			
		Friendly	Name >>			

Use Client certificate: Client certificate for server authentication.

EAP Fast

EAP Method >>	EAP-FAST		ication >> Generic Teleniderd (Session Resumption
ID \ PASS	WORD	EAP Fast		
	provident subject p	ryvinten mode.		
🚺 Use p	votected authentik	cation credential	Remove Import	
🖬 Use (File Path >>	cation credential	Remove Import	

• Allow unauthenticated provision mode: During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.

2 Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method.

Server Certification

ID \ PASSW	DRD	Tunnel Authentice Client Certification	Server Certification	Session Resumption
Use certificate	chain	Anno enterendiste or Server care or Denner care nuet au	erntentes fait exactly	ڭ

• Certificate issuer: Select the server that issues the certificate.

Output: Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.

³ Server name: Enter an authentication sever root.

4.3.3 Example to Reconnect 802.1x Authenticated Connection after 802.1x Authenticated connection Is Failed in Profile

There are two situations where a user is able to reconnect an 802.1x authenticated connection and authenticate successfully after an 802.1x authenticated connection has failed on the profile page. They are as follows:

When keying in an identity, password or domain name error:

• Authentication type chooses "PEAP", key identity into test. Tunnel Protocol is "EAP-MSCHAP-v2, the tunnel identity and tunnel password are tested. Those settings are the same as our intended AP's setting.

ID \ PASSWORD	Client Certification	Server Certification	
Authentication ID / Password			
Identity >> test	(Palasson) ee	Dec	and farmers
funnel ID / Password			
identity >> test	Password >>	test	

2 Because of keying identity and password errors, the result will appear as in the image below.

Card Name >> Ralink.002.11n Wireless LAN Card	Identity >>
Profile Name >> PROF1	Password >>
Wessage >> Invalid identity or password	
OK	Cancel
	CONCO

If you want to disconnect, click "Cancel" on the Authentication Failure dialog box. If you want to reconnect, key the identity into wpatest2. The tunnel identity is wpatest2 and the tunnel password is test2. Those setting are the same as our intended AP's setting.

Card Name >> Ralink 802.11n Wireless	LAN Card	Identity >>	wpatest2
Profile Name >> PROF1		Password >>	test2
Message >> Inwalid identity or pass	eord		
	OK	Cancel	

Click "OK". If it has connected successfully. The result will appear as the image below.



When a "Timeout" occurs;

• Choose "PEAP" as the Authentication type and key-in "wpatest2" as the identity . Tunnel Protocol is "EAP-MSCHAP-v2, and the tunnel identity is "wpatest2". The tunnel password is "test2". These settings are the same as our intended AP's setting.

ID \ PASSWORD	Client Ce	rtification	Server Ce	rtification	• •	Session Resumption	
Authentication ID / Password							
Identity >> wpatest2	6 <u>1</u>	Fatament ++		Ormity	Gate II		
Tunnel ID / Password							
identity >> wpatest2	S.	Password >>	test2				

When a "Timeout" occurs, The following dialog box will be displayed;



3 If it has connected successfully, the dialog box will appear as follows;

Rel	1								
4	Profile	LLL Network	Advanced) Statistics		Ø WPS	Radio On/Off	About	->
		Profil	e List						
FRO	et 🛛	AP1		- P Ø		Profile Name	>>> PROF1		
				10.0		390)⇒⇒ AP1		
						Network Type	>> Infrastructure		
						Authentication	n>+ WPA		
						Encryption	134 AES		
						Use 802.1x	(23 YES		
						Channe	1++ 6		
					R	wer Seve Hode	>> CAH		
						T:: Power	r >> Auto		
						RTS Threshold	1 >> 2347		
					Fran	ment Threshold	1 >> 2346		
	Add	Edit	Delete	Activate					
	Data and	NO	00.07.14		-				*
	Fetra Info as	ink tiln Frena	e:10050-				A QUARTY IN KORK		
	Channel +>	6 2437000 MH	2			Contra Contra	This contraction		
Rist	tentication >>	WPA				2014	Thready St. + 100%		
	Encryption >>	AES				Not	te Strength >> 26%		
14	rtwork. Type >>	Infrastructure			Transmi	t.			
	IP Address >>	192.168.5.91			Lini	Speed >> 54.1	0 Mbps		
	Sub Wask ++	255.255.255.0			Thro	ughput >> 0.0	00 Mbps	č i	
Defa	ult Gateway >>	192.168.5.254					Kbps		10
					Receive	Station and			
BW	>> n/a		SNED >> n/a		Les	L Speed >> \$4.1	0 Mbps		
G	»> h/a	MCS >> n/a	SNR1 >> n/a		Thro	ughput >> 90.1	26.916 Mbps	1	

4.3.4 Example to Configure Connection with WEP on

Relli														1
	Profile		Network.	Advanced	5	atistic:				() WPS	Radio	P On/Off	About	
Sorted t	by >>	0	SSID	 Char 	unal.			Signal				Show dBm		
202				ih.			188	22	_			_		
202								DUIA						
219				the state			-	018						
230				62		D S	T	50%						
243				05		69	Τ.	81%						
99				60		69t	9	81%	_					
AP1				126		U.d.	T	100%						
arsca	dre			61		69(100%						
Broa	doom			BI		69		60%				-		
Bros	dcomWPS			61		69		603						
BUFF	ALO_A			64	- 1	a (29%						8
A	escan	-	Add to Pyofie	Con	nect	-								
	Status -	+ ars	cadre> 00-0	C-40-28-70-11						U	e Quetty I	+ 100%		
1	Extra Info >	+ LIN	k is Up (TxPowe	e:10039					-	Sign	al Strength	1 ++ 17%		
	Channel :	+ 1+	> 2412000 MH	2; central channe	112					lign	e Litrength	2 ++ 100N		
Authe	entication :	in Uni	ODDARD.					1	_	Sig	al Strengt	n 3 >+ 0%		
	noryption >	+ Mor	ie 							Not	se Strengt	h HH 26N		
THEFT	P addance o	. 145	2 764 73 484					Te	ansnit -	10 22	2.52	1.00		
	Sub Wask a	255	1255.0.0						Link Spe	ed >> 270	0.0 Mbps			
Default	t Gateway :		100000000000000000000000000000000000000						inconflut	ALC PP GUD	on Mage	0.006		
			— нт —					24	cetue			Webs		
BW -	- 40			9460 >> n/a					Link Spe	ed >> 1.0	Mbps	Hax		
GI >	> long		VCS >> 15	SNR1 >> n/a					Through	ut >> 0,0	Q6 Hibps	0.000		

• Select an AP with WEP encryption and click "Connect".

Interaction will appear as below;

Profile Network Advanced Statistics WWWA WPS Radio Dn/Off About Statistics WWWA WPS Radio Dn/Off About Statistics WWWA WPS Radio Dn/Off About Statistics WWWA WPS Radio Dn/Off About Statistics WWWA WPS Radio Dn/Off About Statistics WWA WPS Radio Dn/Off About Statistics WPA Radio Dn/Off About Statistics WPA Radio Dn/Off About Statistics WPA Radio Dn/Off About Statistics WPA Radio Dn/Off About Dn/Off											(Relli
Sorted by >> So	r 🔳	About	Radio On/Off	() WPS		5) Statistic	anced .	Network Adv		Profile	(
202 01 0 60x 219 01 0 63x 231 02 0 90x 243 05 0 91x 99 05 0 91x AP1 06 0 90x wscadre 01 00x Broadcon 011 0 00x Broadcon 011 0 00x Broadcon 011 0 00x ButFALO_A 044 0 29x Auth- \ Encry Connect 000x Wep Key 0 000x 000x			Show dBn		mai		È.	Channel	SSID	0	by ++	Sorted
202 0/1 0 00x 219 0/1 0 0 65x 230 0/2 0 9 50x 240 0/5 0 9 91x 99 0/6 0 91x AP1 0/6 0 91x 4P1 0/6 0 91x arcadre 0/1 0 90x Broadcon 0/11 0 60x Broadcon 0/11 0 60x BuffALO_A 0/44 0 29x Authentication >> Open Encryption >> wtp Wep Key 000000000000000000000000000000000000						Pliet :		12				
219 230 243 99 4P1 0 6 8 99 4P1 0 6 8 9 4P1 0 6 8 9 8 8 8 8 8 8 8 8 8 8 8 8 8					20%		69	61				202
230 230 230 9 50x 243 253 9 5 9 9 81x 99 266 9 9 81x AP1 256 9 9 100x excadre 211 9 9 100x Broadcon 211 9 9 60x Broadcon 211 9 9 60x Broadcon 211 9 9 60x BuffFALO_A 29 44 29 x Authr. \ Encry. 44d to Profile Connect Authr. \ Encry. 60x 60x Wep Rey Wep Rey Modectmal 60x					18	٩	69	61				219
243 Ø5 Ø Ø B1% 99 Ø6 Ø Ø B1% AP1 Ø6 Ø Ø B1% erscadre Ø 1 Ø 100% Broadcon Ø 1 Ø 0 Broadcon Ø 1 Ø 60% BufFALO_A Ø Ø 29% Auth, \ Encry, Auth, \ Encry Box, 1% WEP Aresthared Key >> Wep Key Box, 1%					50% -	٩	69	62				230
99 \$6 \$1 \$100x AP1 \$6 \$100x erscadre \$1 \$9 100x Broadcon \$11 \$9 60x BuffALO_A \$44 \$0 29x Auth. \ Encry. Auth. \ Encry. Wep Key Wep Key Wep Key Hexadecinal					118	7	69	68				243
AP1 000 1000 erceadre 01 000 Broadcom 01 000 Broadcom WPS 01 000 BuffALO_A 01 00 Reman Add to Profile Connect Auth. \ Encry. Authentication >> Open • Encryption >> wgp • 0 800.1% WPA Preshared Key >> Wep Key @ Key#1 Hexadecinal •					81%		69(\$6				99
encedre Broadcon BuffALO_A Auth. V Encry.					00%	-	69	66				AP1
Broadcom WPS BLEFFALO_A Authon V Encryption >> wep					00%		69(61			dre	• artc
BrowdcomWPS bit bit of a grant of			_		20% 🗾		69	611			doom	Вгра
BUFFALO_A Add to Profile Connect Auth. \ Encryption >> Copen Encryption >> wep Connect Wep Key Key#1 Hexadecimal Hexadecimal			_		20% mm		69	61			dcomWPS	Bros
Remain Add to Profile Connect Auth. \ Encryption >> Authentication >> Open Authentication >> Open Encryption >> WPA Preshared Key >> Image: Connect in the second in the secon					29%		a	B44			ALO_A	BUFF
Auth. \ Encry.	-						1	Connec	Add to Profile	-	accan	
Authentication >> Open										y.	th. \ Encr	Aut
WPA Preshared Key >> Wep Key Wep Key Wep Key			002.1X		WEP -	tan 22	Encrypt		• Open 🐨	tion 7	Authentica	
Wep Rey Wep Rey Key#1 Hexadecinal					167 18		2002/228		(Key 22	hared	WPA Pres	
Key#1 Hexadecinal ▼											Key	Wep
			-					•	Hexadecinisi		Key#1	0
Key#2 Hexadecinal ▼								-	Hexadecimal		Key#2	
🙆 Key#3 Hexadecinal 👻								-	Hexadeclinal		Key#3	0
	barre	the Parriet							Manu and Annu and		Kerth	-
	-Sid	1 0.0.001						· .	Parcaulte, d'hill			

3 Enter 1234567890 in the Key#1 Hexadecimal field. This value is same as our intended AP's setting.

R401			-	-			
Profile	Network	Advanced	Statistics	WANA	O WPS	Radio On/Off	About
rted by >> 🔘	SSID	Channe	d 🥥	Signal		Show dBm	
		14	AP List	22			
202		61	89	60%		-	
219		61	69 9	61%			
230		62	69 7	50% 💼			
243		68	69 9	81%			-
99		60	690	81%			
AP1		66	09 *	100%			
erscadre		61	690	100%			
Broadcom		611	69	60%		_	
BroadconWPS		101	69	603.		_	
BUFFALO_A		B44	a 🛈	29%			
Rescan	Add to Pyofile	Conne	rt.				-
Auth. \ Encry.	190711						
Authenitication	175 Open	•	Encryption >:	wep 🔻	ŝ.	002.1X	
WPA Preshan	ed Key >>	199972	NO DA COLONIA.			Contraction Street	
Wep Key	- 1						
Key#1	Hexadect	nsi 👻 [1234	567890				
G Key#2	Hexadect	nsi 🐨					
A Key#3	Hesadecil	nai 🕶 🗌					
Q 1000	1 August 1	-					Down Darrented
and the state of t	racables						a sole raccelory

Click "OK". The dialog box will appear as below;

R.UI	•													
	Profile		Network	Advance	đ) Statisti	cs			() WPS	Radio	n/Off	About	
orted	by >>	0	SSID		hannel		9	Signal				Show dBn		
				12		1	AP LIS	t 22						
219				ь	1	69	1	76%						
223				ь	1	69	9	50%	-		_			
243				6	-5	Bġ	-	948	-					
99				в	6	Bġ	1	61%	-			_		
Shi	ang_2860.40			8	11	Bg	ň٩	60%	-					
AP1				B	6	Bġ	•	100%	-					
8710	adre			B		a.		89%	_				-	1
Broa	deamWPS			B	-1	na.	•	702				-		
RUE	FALO A			N.				402	_		_			
Clau	de AP			10	1	"na	٠.	60%	-		_			
	Rescen		Add to Profit		Connec	e 🌔			_					
	Status -	· AP	I «> 00-03-7¥-	00-D7-#4							e Quetto	++ VOX		
	Extra Info >	+ Lm	k is Up (TxPowe	P(10039								1 >> 55%		3
	Channel :	* 6 *	> 2407000 MH	2						Tiere	distances in the	2 =+ 100N		
Auth	entication :	o UN	(nown)								Strength	J >> J9%		
	Encryption	+> WE	P							Not	te Strength	>>> 26N		
Net	MORE Type	in litt	natructure						Transnit			-	-	
	P Address >	191	2.160.5.113						Link Spr	eed >> 54.	0 Mblps	Max		
Defeat	H Gatessey 1	4 100	168 8,254						Through	put >> 0.0	DQ Mbpc	0.021		
Cores	. uncomedy -		HT									Mbps		
2	1.11		04490	-	10			8	Link Con		n Mhron	Have	1	
GI :	io nia io nia	-	Ci ya n/a	SNRD >> n	da.				Through	put >> 0.0	22 Hbps	100000		

4.3.5 Example to Configure Connection with WPA-PSK

• Select the AP with a WPA-PSK authentication mode and click "Connect".

RAUI	i .											
	Profile		Network	Advanced) Statistic	5	Ville	O VIPS	Radio	n/Off	About	1
orted	by >>	0	SSID	Change	vel		Signal			Show dBm		
0148	ii.			ம்ல	a	r. 1.01	20%	-				
tin				121	80		50%	_	_			
132				132	80	•	60%	_	_	-		
202				sh.	30		409					
246				14.			7.7	_		-		
219				the second			768	_		_		
20				0,	Dy	T.	918	_				
99				0.	59		811					
Shi	ang_2860.65	-		611	69	17	61%	-		_		
APT	S.,			(An an	69	1	100%					
arso	adre			61	69	0	99%					
	Rescan		Add to Profi	le Com	ect							
	Status	+ ar	cadre +> DO-	0C-40-28-70-11			4		Les Quality y	1005		Î
	Extra Info	o Lin	k tr.Up (TxPove	er:1001g				54	gnal Strength	1 >> 18%		
	Channel	. 1.	> 2412000 HP	Hz; central channel :	3			1	and Strength.	2++995		Į.
Auth	entication -	in Op	en					\$	ignal Strength	3 >> 0%		
1	Encryption	IN NO	NE .						kokse Strength	×> 26%		
net	B boltone	- 01	istructure				T	enanik			_	
	Oth Mark 1	. 0.1	10.0					Link Speed >> 2	270-0 Hbps	1420		
Defau	It Gateway							inroughput >> (1/000 MDps	0.115		
			HT					in the last		Alopis	15.1	
Ref -	o an			SNED 33 22				Link Speed >> 5	4.0 Mbps	Max		
GI .	·· ing		ACS >> 15	SNR1 >> n/a				Throughput >> 0	1.012 Hbpc	0.204		

2 Auth.\Encry. function appears.

Profile	Network	Advanced) Statistics		Ø WPS	Radio On/Off	About
arted by >> 🔘	SSID	Channel	AP List	Signal		Show d8n	
0148-1		60	a	20%			
11n		101	8901	50%		_	
132		102	69	60%		_	
202		131	69	60%		_	
219		61	89 9	76%			1000
243		\$5	69 9	91%			
99		66	890	atx 💼			
_Shiang_2860AP		1011	8901	65%			
AP1		66	09 9	100%			
arscadre		101	690	99%			
Rescan	Add to Profile	Connec	t				
Auth. \ Encry.	TOP IN						
Authentication	++ WPA-PSK	•	Encryption +	AEL 🔻	6		
WPA Preshare	d Key >>						
Wep Key	20						
O NAVIT	Automatica P						
O Reat	Familiers						
@ Heart	PRIAMOR						
@ 1044	Heikter					2	noe Password

³ Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption. Enter the WPA Pre-Shared Key as "12345678".

P		11	A.	M		Ø	P	2
Profil	e	Network	Advanced	Statistics	WWW	WPS	Radio On/Off	About
orted by >>	0	SSID	Chan	nel 🥥	Signal		Show dBm	
0148-1			\$ 60	a	20%			
11n			101	8909	50%		_	
132			102	Bg	60%		_	
202			101	Bg	603		_	
219			61	69 9	76%			
243			105	69 1	913			
99			66	890	atx 💼			
_Shiang_2860	AP.		1011	6901	65%		_	
AP1			66	09 9	100%			
arscadre			1¢1	890	998			
Resoan	-	Add to Profile	e Con	nect.				
Auth, 3 Er	cry.							
Authent	ication	·· WPA-PSK	•	Encryption	· AES -	e i i		
WPA P	reshare	d Key >> 12345	678					
West Kest								
@ holar								
O Keyat		Paradan	THE T					
@ http:		Ppil.kom	TT: T					
@ 1044		Anna Actor	TE T				S 2	hoe Password

Olick "OK". Be careful, if the WPA Pre-Shared Key entered is not correct, you won't be able to exchange any data frames, even though the AP can be connected.

(Fill)	1.3	- AB	æ			
Profile	Network	Advanced	Statistics	WANA	WPS Radio	On/Off About
orted by >>	SSID	Channel		Signal		Show dBm
0148-1		P ₆₀	a	202		
tin		101	Bane	50%		
132		132		603		
202		101	30	60%		
219		10		2.5		
242		25		918		_
00		5				_
57 (h) 29/04		200	8889	100		_
Strang_2000k	F.	- the		61.6		_
artadre		100	000	998		
Recan	Add to Profile	Corre				
		an an an		_		
10 A A A A A A A A A A A A A A A A A A A	++ APT +-+ 00-00-7F4	00-07-44			Lin Quilly 2	
Status Evites Inte		1.1000			Eq.	1.1.2 4995
Status Extre Info Channel	22 6 6-2 2437000 MH	2				A STRING
Status Extra Info Channel Authentication	>> 6> 2437000 AH ++ WPA-PSK	2			Signa Sciengella Signal Strength	A + 101N
Status Extra Info Channel Authantication Encryption	>> 6 <> 2437000 HH >> WPA-PSK >> TRIP+AES	z			Signal Strength Note Strength	3 >> 0% >> 26N
Status Extre Info Channel Authentication Encryption Network Type	++ 6 +-+ 2437000 HH ++ WPW/PSK ++ Infrastructure ++ Infrastructure	z		Traromi	Signal Strength Signal Strength Noise Strength	2 + 1005 3 +> 0% >> 26%
Status Extre Info Channel Authentication Encryption Network Type IP Address	 >> 6 <-> 2437000 HH >> WPA-PSK >> TRIP+AES >> Infrastructure >> 192.168.5.113 	2		Transmi	Signal Strength Notre Strength t t Speed >> \$4.0 Mbps	2 + 26% >> 26%
Status Extra Info Channel Authantication Encryption Network Type IP Address Sub Wask	 >> 6 <-> 2437000 HH >> WP4-P3K >> TNIP+4ES >> Infrastructure >> 192.168.5.113 >> 255.255.255.0 	z		Tranumi Lisa Thro	Signal Strength Signal Strength Notre Strength t Speed >> 54.0 Mbps Ngtput >> 0.001 Hbps	44 1005 3 ×> 055 >> 265 Hax 0.115
Status Extre Info Channel Authentication Encryption Network Type IP Address Sub Hask Default Gateway	 +> 6 <-> 2437000 HH +> WP4.P3K >> TRIP+AES +> Infrastructure >> 192.168.5.113 >> 255.255.255.0 >> 192.168.5.254 	2		Traromi Lini Thro	Signal Strength Signal Strength Note Strength t t t Speed >> 54.0 Mbps Naghput >> 0.001 Mbps	2 × 1015 3 × 105 >> 26% Hax 0.115 Aloga
Status Extre Info Channel Authentication Encryption Network Type IP Address Sub Hask Default Gateway	 +> 6 <-> 2437000 HH +> WPA-PSK >> TRIP+AES >> Infrastructure >> 192.168.5.113 >> 255.255.255.0 >> 192.168.5.254 HT 	2		Trancent Les Thro Receive	Signal Strength Signal Strength Noise Strength t Speed >> 54.0 Mbps rughput >> 0.001 Mbps	A TOUS 3 >> 25% >> 26% Hax 0.115 Abps Wat
Status Extra Info Channel Authantication Encryption Network Type IP Address Sub Wesk Default Gateway IBW >> n/a	 >> 6 <-> 2437000 HH >> WP4-P3K >> TNIP+4ES >> Infrastructure >> 192.168.5.113 >> 255.255.255.0 >> 192.168.5.254 HT 	2 SNR0 >> n/a		Traromi Les Thro Receive Lins	Signal Strength Signal Strength Notre Strength t Speed >> 54.0 Mbps Ngtput >> 0.001 Hbps	64 1005 3 ×> 075 >> 26% Hax 0.115 Alapa Wes

4.3.6 Example to Configure Connection with WPA

• Select an AP with WPA authentication mode and click "Connect".

		20						
8	Network	Advanced	a Statistics		Ø WPS	Radio On/Off	About	
0	SSID	Channel		Signal		Show dBn		
		10.00	AP LET					
		the state		018			_	
		011	090	91%				
		64	69	29%				
		60	590	91%			1	
P		611	6907	91%				
		611	69 9	70%				
		10 m	@g =	100%				
		61	89 9	29%				
		101	8989	100%				
		67	8901	863				
	Add to Profile	e Conner	at					
>> Dis	connected			1	11	nk Quality >> 0%		
**					Signa	al Strength 1 >> 0%		
32					Signe	sl Strength 2 >> 0%		
28					Signa	siStrength 3 → 0%		
34-5					Not	te Strength >> 0%		
**				Transmit	NOTE:			1
29				Link	Speed **	Wat		
				Throu	aghput >>	0.000		
22.2	нт					Wops		
	1996	100212-010		Receive	and and	15ar		
		SNRD >>		LINA	speed >>			
				78.000	and south the second			
	P 22 De 23 De 24 25 25 25 25 25 25 25 25	Add to Profile	Advanced Network Advanced SSID Channel U11 U11 U11 U11 U11 U11 U11 U1	Network Advanced Statistics SSID Channel APLier Advanced Statistics SSID Channel APLier APLier Advanced Statistics APLier APLier P P P P P P P P P P P P P	Image: Network Advanced Statistics WWWW SSID Channel Signal Signal SSID Channel Signal Signal SSID Channel Signal Signal SSID Channel Signal Signal SSID SSID Signal Signal SSID SSID Signal Signal SSID SSID SSID Signal SSID SSID SSID SSID Add to Profile Connect SSID SSID SSID SSID SSID	Network Advanced Statistics WWW WPS SSID Channel Signal AP List >> AP List >> District District Signal AP List >> AP List >> District District Signal AP List >> District AP List >> District District District AP List >> District District District District District AP List >> District District District District District AP List >> District District District District District District District District AP List >> District District District District District District District District AP List >> District District AP List >> District District District District District AP List >> District District	Network Advanced Statistics WWW WPS Radio On/Off SSID Channel Signal Image: Signal statistics Signal statistics	Matwork Advanced Statistics WWW WPS Radio On/Off About © SSD Channel Signal StowedBin #P List >* P11 9 65% P11 9 65% P11 9 P11 9 91% P11 P11 P11 9 91% P11 P11 P11 P11 9 91% P11 P11 P11 P11 9 91% P11 P11 P11 P11 9 P11 P11 P11 P11 P11 9 P10 P11 P11 P11 P11 9 P100% P11 P11 P11 P11 9 P11 P11<

The Auth.\Encry. function pop up. (If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)

Profile	Network	Advanced) Statistics		Ø VÆS	Radio On/Off	About
iorted by >> 🛛 🥥	SSID	Channel	ł 🥥	Signal		Show dilm	
240		611	890	91%			
243		104	Bg	15%			
99		66	690	91%			
_Shiang_2860AP		11	8907	968 💻			-
Ap-03		611	89 9	70%		_	
AP1		106	69 *	100%	-		
AP47-g		61	89 9	24%			
arscadre		61	6907	91%			
arvint-2860AP		67	6907	91%			
Broadcom		611	69	768 💻			
Rescan	Add to Profile	Corne	ct				-
Auth, \ Encry.	8021X	2					
Authentication	++ WPA	*	Encryption >>	AES	•		
WPA Presbar	ed Key >>						
Wep Key							
@ news	The second						
 Neyd2 	(Version 1	NF T					
(here)	hearter	19 W					
O - Projekt	Hespera	ns w				9	how Password
			14421				

3 Click "8021X" and the setting page will appear.

(m.	Profile		Network	Advanced) Statistics		O WPS	Radio On/Off	About	
orted t	by >>	0	SSID	Channel	al Q	Signal		Show dBn		
202				yh.	80	0.48			_	
202				ibu	80 9	6/1%				
219				10		768		_		
223				1011	80	4/8		_		
240				1011	Ban	863		_	-	
00				eb.	Ban	999			_	
Shie	ing 28684P			1011	8009	813				
Ap-03	3			1011	89 9	618				
APT				26	80 9	100%				
arsoa	adre			101	2909	100%				
	kescan		Add to Profile	Cane	ect					
Aut	th. \ Encn	y.	8021X						_	
	EAP Method	77	PEAP		Turnel Authentica	etton >> E	SAP-IKSCHAP v2	· Section	Repurption	
	ID VP	400	WORD	Client Cor	tification	Server	Cartification			
	unt antipatio		(Barner)	Administration of the second						
1	-unencean.	in its	+ rassword		- anterior (6	-	a there are t	_	
		- Centra								
	funnel ID / Po	955000	bu			51			_	
		Identi	ty »»		Patheord +>					
					OK	Cancel				

• Authentication type and setting method :

PEAP :

1. Select "PEAP" as the Authentication type from the drop-down list. Key-in "wpatest2" for the identity. "Select "EAP-MSCHAP v2" from the drop-down list for tunnel authentication and key-in the tunnel identity as "wpatest2" and the tunnel password as "test2". These settings are the same as our intended AP's setting.

Profile	Network	Advanced) Statistics		Ø	Radio On/Off	About	
iorted by >> 🕻	ssid	Channel		Signal		Show dBn		
240		b 11	10 0 0	91%				
243		134	89	15%				
99		36	890	91%				
_Shiang_2860AP		11	8901	968 💼				
Ap-03		611	89 9	70%		_		
AP1		106	89 *	100%				
AP47-g		61	89 1	24%				
arscadre		61	6907	91%				
arvint-2860AP		\$7	8907	91%				
Broadcom		1011	89	768				×
Rescen	Add to Profile	Connec	t					
Auth. \ Encry.	80210	6						
EAP Method >>	PEAP	• 1	unnel Authenticat	tion >> EAP	HISCHAP V2	▼ 🔲 Session i	esumption	
ID \ PAS	SWORD	Client Cert	fication	Server Ce	rtification	1000		
Authentication	D / Pessword	1						
ide	ntity >> wpatert	2	Passent		- inna	to Annual Area		
Turnel (D. / Barr	and					and the second s		
Line Line	atity as anotest	2	Reconstruction It	esta				
	and the second		Water second					
			1000					

2. Click OK. The dialog box should appear as below.

RaUI	2			æ	M		Ø	Ŷ	Z	
-	Profile	18 - I	Network.	Advanced	Statistics	WWW	WPS	Radio On/Off	About	
orted	by >>	0	SSID	Channel	0	Signal		Show dBm		
-				ak a	AP Let	33				
223				2		BU R			_	
290				011	090	80%				
3344				411		50%				
99				00		99%				•
_SNI	ang_28604	₽		011	DODT	86%				
Ap-0	0			611	69 T	65%				
AP1				66	69 1	100%				
Bek	in_N1_Wir	eless_	FAFB15	66	690	50%				
Broa	adcom			611	69	86%				
Bros	adcom/WPS			61	69	91%				
- 1	Rescan	and a	Add to Prof	le Connec	t					
					Authenticat	ion Status				
		ardN	ame >> Ralink 8	32. 11n Wireless LAN C	and		Connected	by manual		
	1	20:30	26.765	Starting note	ors. connection.					
		20:30:	26.890	Network is co	nnecting					
		20:30:	27.000	PEAP Withents	ceting					
					ок	Cancel				
				-						

*If you want to disconnect, please click cancel button in Authentication Status function.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

3. If the connection is successful, the dialog will appear as below.

RAUL											
(m.	Profile		Network.	Advanced) Statistics	8		Ø WPS	Radio On/Off	About	
Sorted I	by ++	0	SSID	Channe	t.		Signal		Show dBn		
					4P	Est	22				
202				61	69		81%				
213				11	69	9	60%		_		
219				61	69	•	76%				
223				611	69		44%		-		
240				811	690		863				
99				106	890		99%				
Shie	ing_2860AF	2		11	Bad	•	81%				
Ap-00	3			1011	Ba	•	65%		_		
AP1				26	89		100%				1
arso	adre			61	890	9	100%				
	heican		Add to Profil	e Conne	et						
	Status	· AP	I ↔ 00-03-7¥-	00-D7-M				10	a Quilty ++ DPS		1
1	Extra Info >	i Lin	k is Up (TxPowe	wi10099				្រព្វផ	Strength 1 als 1000	1.1	L
	Channel :	+ 6 +	> 2407000 MH	2				Sana	Drength 2 ++ 100%		
Auth	entication :	is WP	W					Signal	Strength 3 -+ 100K		
-	Incryption	++ THI	P+AES					Nots	e Strength >> 26%		
Net	могії. Туря	·· Inf	natructure				Transm	it		_	
33	Cub Harks	191	C-160.5.79				Lin	sk Speed >> 54.0) Mbps		
Defeat	t Gatesay :	1. 190	168.8.254				The	oughput >> 0.00	0 Kbps 30,248	Ę.	
			HT				1422.40		Apps		
Den							Receive	a Grand as Add	1 Mbrut Higgs	1	
GI >	> n/a	-	NCS >> n/a	SNR1 >> n/a			The	oughput >> 57.1	148 Kbps 1.919		

TLS / Smart Card :

1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server authentication.

Profile		Network	Advanced	Statistics		()	Radio On/Off	R	1
eted by >>	0	SSID	Channel	4	Signal		Show dilm		
				AP Lt	t >>				
			60	69 9	508		_		
			11	Бg	50%				
132			62	69	81%				
185			00	5 1	60%				
202			61	59	76%				
219			61	B9 T	768				
240			011	090	86%		_		
Ap-03			0 II	59 1	61%				
AP1			00	89 1	100%				
Broadcom		1100101004	011	88	16.8				
Rescan	100	Add to Profil	e Connec	1					
Auth \ End	n.	9021	X.						
EID Walk	aye.				and the second				
EAP WITH	201.99	TLS/Smartc	and v I	unnel Authentric	atson >>		Session 1	Resumption	
ID 1	PASS	WORD	Client Certi	fication	Server	Certification	-		
Authentica	tion ID	/ Pespword			2	25		_	
	lden	ity >> wpater	12	Parameter ++		- Appen	en heren en E		
Tunnel ID /	Раззы	ord							
		tty w	1						

2. TLS must use client certification. Click "Client Certification" and select a certification for server authentication.

RaLI		i i	A	ja ja		a	۲	X
Profile		Network.	Advanced	Statistics	VAMAA	VIPS	Radio On/Off	About
iorted by >>	•	SSID	Channel		Signal		Show dBm	
			6	B9 9	50%			
			1011	Bg	50%			
132			62	Bg	81%			
185			\$6	8 9	60%		_	
202			101	89	76%			() ()
219			101	89 9	768			1.1
240			611	890	863			
Ap-03			1011	89 9	618		_	
AP1			100	89 9	100%			
Broadcom			611	89	768			
Rescan	1	Add to Profile	Connec	t.				
Auth. \ Encry	y.	8021X						
EAP Wethod	in .	TLS/SmartCar	d 🕶 1	unelAuthentica	rtion >>	141	Session i	esumption
ID \ P	ASS	WORD	Client Certi	fication	Server	Certification		
Use Che	nt o	ertificate	wpatest2	2003	erv.	4/9/200)	
				Issued To >> N	petert2			
				Issued By >> 21	000serv			
			- 24	Entret On your	19.0008			
			Frie	indly Name >>				
					Carried			
			-	-m	19.08			

3. Click "OK". The dialog box should appear as the image below.

(m.)	Profile	8	Network.	Advanc	ed !) Statistics	\$			() WPS	Radio On/Off	About	
iorted (by +>	0	SSID		Channel	i.		Signal			Show dBn		
					di.		Plet	25	_				
202					2			STR	_				1
213					011	6g	Ţ	60%					
219					61	6g	٣	76%				•	
223					011	69		44%			-		
240					611	69(1	863					
99					66	690	n	99%					
Shie	ing_2860/	P			1011	690	19	813					
Ap-03	3				611	69	•	65%			_		
APT					26	80		100%	-				1
arso	adre				10	890	19	100%	-		_		
	Rescan	-	Add to Profi		Connect								
						Authen	ticati	on Status					_
		ardNa	me >> Ratink 80	2.11n Winds	HIS LAN CO	rd			0	annected	by manual		
		20:54-0	2.234	Nets	ork Link i	NOT care	arted						
	1	20:51:0	12.343	Start	ing netwo	R. connect	tan						
	1	20:51:0	12.453	Netw	ork is can	necting							
		20:51:0	5.484	TLS#	whentica	ting							
						~			_				

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. If it connected successfully, the result will appear as in the image below.

RAUL											E
	Profile		Network.	Advanced) Statistics	8		Ø WPS	Radio On/Off	About	
iorted t	y >>	0	SSID	@ Channe	ıt		Signal		Show dBn		
				12	4P	Est	22				
202				61	69		81%				-
213				11	69	9	60%		_		
219				61	69	•	768			i	
223				611	69		44%		-		
240				811	690	1	863 💼				
99				106	890		99%				1
Shie	ng_2860AF	2		611	890	•	813.				
Ap-03	3			611	Bg	•	612		_		
AP1				26	80		100%			-	
arsca	dre			61	090	19	100%				
	escan	-	Add to Profil	e Conne	et						
	Status	· AP	I ←→ 00-03-7¥-	00-07-44				Lin	N Quality of Des		-
1	Extra Info >	+ Lin	k is Up (TxPowe	Pr:10099				Ugui	Strength 1 ab 100%	2.5	
	Channel		> 2407000 MH	12				Signal	Dirength 2 ++ 100%		
Authe	entication :	> WF	¥					Signal	Strength 3 ++ 100%		
E	noryption	+> THI	PHAES					Nois	e Strength >> 26N		
THEFT	P addant :	. 12	1401 E 79				Transm	it			
10	Sub Hask	+ 25	5.255.255.0				10	supped >> 54.0	n Molpis	6	
Default	t Gaternay		2.168.5.254					orighter as more	30.248		
			HT				Recete		1005		
BW >	> n/a			9160 >> n/a			Ltr	sk Speed >> \$4.0	Mbps Hax		
GI >	> n/a	4	ACS >> n/a	SNR1 => n/a			The	oughput >> 57.1	48 Kbps 1.919		

TTLS:

1. Select TTLS from the Authentication type drop-down list. Key-in the identity as "wpatest2". Select CHAP for tunnel authentication, and key-in the identity as "wpatest2" and tunnel password as "test2". These settings are the same as our intended AP's setting.

Profile		Network.	Advanced	Statistics	Varm.	() WPS	Radio On/Off	About	
arted by >>	0	SSID	Channel		Signal		🔲 Show dilm		
			ih.		53				
			10	80	578				
177			10	80	818		_	-	
185			106		603		_		
202			101	Bg.	768				
219			101	89 9	768		_	-	
240			611	890	86%				
Ap-03			1011	89 9	618		_		
AP1			100	89 9	100%				
Broadcom			11	89	768				
Rescan		Add to Profile	Connec	+					
Auth. \ End	ry.	8021X	6						
EAP Weth	+(.bs	TTLS	¥ 1	unei Authentica	tion >>	OHAP	▼ 🖸 Session i	Resumption	
ID 1	PASS	WORD	Client Certi	fication	Server Ce	rtification			
Authenitica	tion ID	/ Pespword							
	iden	ity >> wpatert	2	Parameter		-Inn	an taxas or		
Turnel ID /	Patta	ord							
	Iden	ity >> wpatest	2	Password >> [test2	6			
		and the second		un service of a					

2. Click "OK". The dialog box should appear as the image below.

	Preside President President
Network Link is NOT connected.	
Network is connecting	
Network is connecting	
TTLS Authenticating	
	Network Link is NOT connected. Network is connecting Network is connecting TTLS Authenticating

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

RAUL														1
(m	rofile		Network.	Advan) ced) Statistic:	3	Villa	1	() WPS	Radio	n/off	About	
Sorted by a	•	0	SSID		Channel			Signal				Show dBm		
					12	10	Ebt	22						
202					61	69		81%						1
213					611	69	٩	60%				-		
219					61	69	٩	761					1	
223					611	69		44%	-		_			
240					811	690		86%	-					
99					16	690		99%	-					12
_Shieng	,2860AP				1011	890	9	813	-					
Ap-03					1011	69	-	653	-			-		
> AP1					26	69		100%	-					1
arscadre					101	690	19	100%	-					
Reit	an		Add to Profile	-	Connec	1								
	Status >	> API	I ↔ 00-03-7¥-	00-D7-A4						LI.	in Quilty	+ DPS -		
Ext	ra Info »	+ Lm	к is Up (ТхРоме	Pr110039						Ugu	Strength	1 ++ 100%	2.5	
c	hannet +	× 6 +	> 2407000 MH	2						Den	e Dreiningste	2 -+ 100%		
Authenti	ication »	> WP	¥							Sign	(Strength)	3++-100%		
Encr	yption >	+ THI	PHAES							Not	se Strengt	0 >> 26N		
PA	defenses a	. 193	140.5.79					1	ransmit	10 23		1614		
54	b Hask >	× 255	5.255.255.0						Link spe	ed >> 54.	0 MDps			
Default Ge	terney >	+ 193	2.168.5.254						mosert	an ee av	and Palgers	30.248		
			HT						ecetar			wops		
BWARD	la.			960 -	* n/a				Link Spe	red >> \$4.	0 Mbpt	Hax		6
GI >> h	/a	W	VCS >> n/a	SNR1 +	⊳n/a				Through	out >> 57.	143 Kbps	1.919 Mbps		

3. If the connection is successful, the dialog box will appear as the image below.

EAP-FAST :

1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. Tunnel Protocol only supports "Generic Token Card" now. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's setting.

E		11	R	18		a	۲	Ø	
Profile		Network	Advanced	Statistics	Vitter	WPS	Radio On/Off	About	1
arted by >>	0	SSID	Channel		Signal		🔲 Show dBm		
			aka:	AP Lt	233				
			5.	89	509				
477			5	80	318		_	_	
185			b.		60%		_		
202			10	80	748		_		
219			b1	80 9	768		_		
240			1011	Ban	863				
Ap-03			1011	Rg P	658				
AP1			100	89 9	100%				
Broadcom			1011	69	768		_		
Rescan		Add to Profile	Connec	at					
Auth. \ En	cry.	8021X	6						
EAP Wett	ee ba	EAP-FAST	• 1	unnel Authentica	tion >> - Germa	in Toten Cela	- Session	Resumption	
ID 1	PASS	WORD	EAP F	ast			1070		
Authentic	tion ID	/ Pessword	n						
	iden	tity >> wpatest	2	Parameter		Dom	an Name +>		
Turnel ID	Patria	and							
	Iden	tity ** wpatest	2	Password ++	test2				
	- 523			1019192925013	and an				
Pass	WORD M	odé 👀 🎯 Sef	t Token 🥥 Sta	rtic Password					

2. Click "OK". The dialog box should appear as the image below.

Profi	le	Network.	Advanced) Statistics	8		Ø WPS	Radio (Dn/Off	About	=
iorted by >>	0	SSID	Channel		•	Signal			how dBm		
Ap-03			b 11	89	-	558	-				
AP1			86	69		100%					
arvint-2860A	р		67	690	19	86%					
Broadcom			1011	69		86%					
BroadcomW	PS		61	69		948				-	
Cobra			\$6	69	•	34%					
dlink			611	690		86%					
, tan			\$6	690		100%					•
SeftAP-03			61	690		55%					
SoftAP-koe			B1	69		70%			-		
Rescan	-	Add to Profil	e Connec	ł							
				Authent	ticati	on Status					
	Card N	ame >> Ralink 80	2.11n Wireless LAN Co	and			Connecte	d by manual			
	20:31: 20:31: 20:31: 20:31:	19,062 19,905 42,904	Starting notwo Network is con EAP-PAST Auth	enticeting	kan						

3. If the connection is successful, the dialog box will appear as the image below.

Profil	e	Network	Advanced) Statistics	1		Ø WPS	Radio On/Ot	r About	
orted by ++	0	SSID	Channel	1	0 9	ignal		Show d	Bm	
202			44.1		C.R.C. 3-5	9.19			_	
213			1011		•	108				
219			No.			748		_		
202			×		1	100		_		
223			5			948		_		
240			ch.			80.8				
99			06			992				1
_Shieng_2860	NP		011	090	T	815.				
Ap-03			611	<u>B</u> a	T	613				
AP1			66	69	7	100%				
arscadre			B1	680	1	100%				- 3
Rescan	-	Add to Profi	e Correc	t						
Statu	e >> AF	1 ↔ 00-03-7¥	-00-D7-A4					Quilty + DES		
Extra Inf	0 »+ L1	nik is Up (TxPowe	er:10099				Signal	Strength 1 av 1003		
Chann	# ++ 6	+> 2407000 MP	12				Signal	Etrength 2 -+ 1001		
Authenticatio	n av W	PA					Signal	Strength 3 ++ 100		
Matwork Two		(PFRE)					Nots	e Strength >> 26%		
IP Addres	5 30 19	2.168.5.79				Transmi	E Creative Ett	lilbor III	a.c	
Sub Has	k >> 25	5.255.255.0				Thre	National >> 0.00	0 Kbcs	9.00 B	
Default Gabeza	y >= 15	2.168.5.254						20	.248	
		HT				Receive	4			
BW >> n/a			SNRD >> n/a			Lin	. Speed >> \$4.0	Mbps	iax.	2
		CONTRACTOR OF STREET, S				Three	interit as \$7.1	49 Khor		

*If you want to disconnect, please click "Cancel" on the Authentication Status function page. *In Profile function, show "Profile Name" option only in adding AP to Profile function.

5 Trouble Shooting

This chapter provides solutions to problems that may occur during the installation and operation of PCI Adapter. Read the descriptions below to solve your problems.

1. The PCI Adapter does not work properly.

Reinsert PCI Adapter into your PC's PCI slot. Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find PCI Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of PCI Adapter. If there is a yellow question mark, please check the following: Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.) Make sure that you have inserted the right adapter and installed the proper driver. If PCI Adapter does not function after attempting the above steps, remove it and do the following: Uninstall the driver software from your PC. Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2.I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.

Make sure that the PC to which PCI Adapter is associated is powered on. Make sure that PCI Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

3.What should I do when the computer with PCI Adapter installed is unable to connect to the wireless network and/or the Internet?

Check that the LED indicators for the broadband modem are indicating normal activity. If not, there may be a problem with the broadband connection. Check that the LED indicators on the wireless router are functioning properly. If not, check that the AC power and Ethernet cables are firmly connected. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points. In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it might be necessary to set up one client to establish a BSS (Basic Service Set) and wait briefly before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it. Check that the Network Connection for the wireless client is configured properly. If Security is enabled, make sure that the correct encryption keys are entered on both PCI Adapter and the access point.

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user' s authority to operate the equipment

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. No change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The 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 instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose 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 or more 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.

The user should not modify or change this equipment without written approval Form Loopcomm Technology Inc. .Modification could void authority to use this equipment.