RaConfig Operation Manual

RaConfig or windows zero configuration Start RaConfig Utility Site Survey Page Encryption Setting [WEP/TKIP/AES] 802.1X Authentication CA Server Setting Profile Page Link Status Page Statistic Page Advance Page Country Channel List QoS Page About Page Example on adding profile in site survey page Example to add profile in profile page Example to configure connection with WEP on Example to configure connection with WPA-PSK Example to configure connection with WPA2-PSK Example to configure connection with WPA Example to configure connection with WPA2 Example to configure to enable Wi-Fi Multi-Media Example to configure to enable WMM – Power Save Example to configure to enable DLS (Direct Link Setup) EXCURSUS

Example to configure to enable DLS (Direct Link Setup)

1. Click "Direct Link Setup Enable". And Click "Apply" button.

🥀 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable	
Direct Link Direct Link Setup MAC Address :	
Tear Down OK Help	

2. Change to "Site Survey Page". And add a AP that supports DLS features to a Profile. The result will look like the below figure in Profile page.

ı 🔁 Ralin	k Wireless	Utility					x
Profile	Link Status	Site Survey Sta	atistics Ad	vanced QoS	About		
⊢ ^{Prol}	file List						
Pr	rofile Name	SSID	Channel	Authentication	Encryption	Network Ty	
-	PROF1	ralink_DLS	Auto	Open	None	Infrastructure	
			. 1	= 0	1		
	Add	Del	ete	Edit		Activate	
					OK	Help	

The setting of DLS indicates as follow:

1. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to two conditions as follow:

Connect with the same AP that support DLS features.



Have to enable DLS.

🥀 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
✓ Direct Link Setup Enable	
Direct Link	
MAC Address : 00 · 0C · 43 · 25 · 73 · 18	
Timeout Value : 60 sec Apply	
DLS Status	
MAC Address Timeout	
Tear Down	
OK Help	

2. Timeout Value represents that it disconnect automatically after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.

Ralink Wireless Utility
Profile Link Status Site Survey Statistics Advanced QoS About
VMM Enable Apply
WMM - Power Save Enable Setting
Direct Link Setup Enable
Direct Link Direct Link Setup MAC Address : 00 · 0C · 43 · 25 · 73 · 18
Timeout Value : 60 sec Apply DLS Status
Tear Down
OK Help

3. Click "Apply" button. The result will look like the below figure.

Ralink Wireless Utility
Profile Link Status Site Survey Statistics Advanced QoS About
VMM Enable Apply
WMM - Power Save Enable Setting
Direct Link Setup Enable
Direct Link Direct Link Setup MAC Address: 00 · 0C · 43 · 25 · 73 · 18 Timeout Value: 60 sec Apply DLS Status MAC Address Timeout 00-0C-43-25-73-18 60 Tear Down
OK Help

Describe "DLS Status" as follow:

- 1. As the up figure, after configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in "DLS Status". In "DLS Status" of the opposite side, it shows MAC address of myself and Timeout Value of setting.
- 2. Display 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".

📌 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Direct Link Setup MAC Address:	
Tear Down	
OK Help	

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

🥂 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Setup MAC Address : 00 · 0C · 43 · 25 · 73 · 18 Timeout Value : 600 sec Apply DLS Status MAC Address Timeout 00-0C-43-25-73-18 600	
Tear Down	
OK Help	

- 3. Disconnect Direct Link Setup as follow:
 - 1. Select a direct link STA.

📌 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Setup MAC Address: 00 · 0C · 43 · 25 · 73 · 18 Timeout Value : 600 sec Apply DLS Status MAC Address Timeout 100-0C-43-25-73-18 600 Tear Down	
ОК Нер	

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

🥂 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Setup MAC Address : 00 · 0C · 43 · 25 · 73 · 18 Timeout Value : 600 sec Apply DLS Status MAC Address Timeout	
Tear Down	
OK Help	

Example to configure to enable WMM – Power Save

1. Click "WMM – Power Save Enable". And Click "Setting..." button.

Profile Link Status Site Survey Statistics Advanced QoS About Image: WMM Enable Apply Image: WMM - Power Save Enable Image: Setting] Image: Direct Link Setup Image: Setting] Image: Direct Link Setup Image: Direct Link	😤 Ralink Wireless Utility	×
WMM Enable Apply WMM - Power Save Enable Setting Direct Link Setup Apply Direct Link Setup MAC Address : MAC Address : • Timeout Value : 60 sec Apply DLS Status MAC Address Timeout Tear Down	Profile Link Status Site Survey Statistics Advanced QoS About	
WMM - Power Save Enable Direct Link Setup Enable Direct Link Setup MAC Address : • </td <td>VMM Enable Apply</td> <td></td>	VMM Enable Apply	
Direct Link Setup Enable	WMM - Power Save Enable	
Direct Link Direct Link Setup MAC Address:	Direct Link Setup Enable Apply	
Tear Down	Direct Link Direct Link Direct Link Setup MAC Address:	
OK Help	Tear Down	

2. After clicking "Setting..." button, show "Power Save Setting" dialog. Please select which ACs you want to enable. Then click "Apply" button. The setting of enabling WMM – Power Save is successfully.



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:

1. Click "WMM Enable".

18 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
VMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Setup MAC Address:	
Tear Down	
OK Help	

2. Click "Apply".

🕂 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
WMM Enable	
WMM - Power Save Enable Setting	
Direct Link Setup Enable	
Direct Link Direct Link Direct Link Setup MAC Address:	
Tear Down	
OK Help	

3. Change to "Site Survey Page". And add a AP that supports WMM features to a Profile. The result will look like the below figure in Profile page.

🤹 Ralinl	(Wireless	Utilit y					x
Profile	Link Status	Site Survey Sta	itistics Ad	vanced QoS	About		
Prof	ile List						
Pr	ofile Name	SSID	Channel	Authentication	Encryption	Network Ty	
	PROF1	ralink_DLS	Auto	Open	None	Infrastructure	
[Add	Del	ete	Edit		Activate	
					OK	Help	

Configure connection with WPA2 by 802.1x setting

1. Select A.P with WPA2 authentication mode.

暮 Ralink Wireless Utilit	Ralink Wireless Utility					×	
Profile Link Status Sit	e Survey Statistics	Advar	nced	About]			
							1
Sein	PSSID	Sig	C	Enorupt	Authorit	Notwork T	
WHOL WEP	00-20-46-4E-5B-	63%	1	WEP	Hinknown		
WPA_TLS	00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct	
WHQL_WEP	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct	
WHQL_WPA	00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct	
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct	
SoftAP-10	00-0C-43-25-67	99%	6	TKIP	WPA-P	Infrastruct	
AP23	00-07-40-C3-13	26%	10	None	Unknown	Infrastruct	
xikun-g	22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct	
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct	
AP66	00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct	
•	1			1	1		
Connected 4 > AP22	, [_	~			
Connected K-> AF23	Connected <> AP23 Rescan Connect Add to Profile						
					пк	Heb	
				_	- OK		

2. Click CONNECT or double click the intended network.

t y						×
e Survey Statistics	Advar	nced	About			
						,
BSSID	Sig	C	Encrypt	Authent	Network T	
00-20-A6-4F-5B	63%	1	WEP	Unknown	Infrastruct	
00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct	
00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct	
00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct	
00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct	
00-00-43-25-67	99%	6	TKIP	WPA-P	Infrastruct	
00-07-40-C3-13	26%	10	None	Unknown	Infrastruct	
22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct	
00-90-96-52-27	52%	11	None	Unknown	Infrastruct	
00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct	
					•	
Connected <> AP23 Rescan Connect Add to Profile						
				OK	Help	
	Ly te Survey Statistics BSSID 00-20-A6-4F-5B 00-E0-B8-76-18 00-40-96-56-2A 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-A6-50-D3 00-20-43-25-67 00-00-43-25-60 00-90-96-52-27 00-00-43-25-60 00-90-96-52-27	Ly te Survey Statistics Advar BSSID Sig 00-20-A6-4F-5B 63% 00-E0-88-76-18 10 00-40-96-56-2A 60% 00-20-A6-50-D3 37% 00-E0-18-F4-44 52% 00-00-C43-25-67 99% 00-00-740-C3-13 26% 22-00-AA-33-CC 55% 00-90-96-52-27 52% 00-0C-43-25-60 63%	ty te Survey Statistics Advanced BSSID Sig C 00-20-A6-4F-5B 63% 1 00-E0-88-76-18 10 1 00-20-A6-50-13 37% 1 00-20-A6-50-D3 37% 1 00-20-A6-50-D3 37% 1 00-20-A6-50-D3 37% 1 00-0-20-A6-50-D3 37% 1 00-0-20-A6-50-D3 37% 1 00-0-20-A6-50-D3 37% 1 00-0-20-A6-50-D3 52% 6 00-0-C43-25-67 99% 6 00-00-43-25-67 55% 10 00-90-96-52-27 52% 11 00-0C-43-25-60 63% 1 00-0C-43-25-60 63% 1 00-0C-43-25-60 63% 1	ty te Survey Statistics Advanced About BSSID Sig C Encrypt 00-20-A6-4F-5B 63% 1 WEP 00-20-A6-4F-5B 63% 1 WEP 00-20-A6-4F-5B 63% 1 WEP 00-20-A6-4F-5B 60% 1 WEP 00-20-A6-50-03 37% 1 TKIP 00-20-A6-50-D3 37% 1 TKIP 00-20-A6-50-D3 37% 1 TKIP 00-20-A6-50-D3 52% 6 WEP 00-20-A6-50-03 98% 6 TKIP 00-00-43-25-67 99% 6 TKIP 00-00-43-25-60 55% 10 AES 00-00-43-25-60 63% 1 TKIP 00-00-43-25-60 63% 1 TKIP 00-00-43-25-60 63% 1 TKIP 00-00-43-25-60 63% 1 TKIP 00-00-43-25-60 63% 1 TKIP	ty te Survey Statistics Advanced About BSSID Sig C Encrypt Authent 00-20-A6-4F-5B 63% 1 WEP Unknown 00-20-A6-4F-5B 63% 1 WEP Unknown 00-20-A6-4F-5B 60% 1 WEP Unknown 00-20-A6-50-13 60% 1 WEP Unknown 00-20-A6-50-D3 37% 1 TKIP WPA-P 00-00-C43-25-67 99% 6 TKIP WPA-P 00-90-96-52-27 52% 10 Aes WPA-P 00-90-96-52-27 52% 1 None Unknown 00-0C-43-25-60 63% 1 TKIP WPA-P 00-90-9	Ly te Survey Statistics Advanced About BSSID Sig C Encrypt Authent Network T 00-20-A6-4F-5B 63% 1 WEP Unknown Infrastruct 00-20-A6-4F-5B 63% 1 WEP Unknown Infrastruct 00-40-96-56-2A 60% 1 WEP Unknown Infrastruct 00-20-A6-50-D3 37% 1 TKIP WPA-P Infrastruct 00-20-A6-50-D3 37% 1 TKIP WPA-P Infrastruct 00-20-A6-50-D3 37% 1 TKIP WPA-P Infrastruct 00-02-43-25-67 99% 6 TKIP WPA-P Infrastruct 00-07-40-C3-13 26% 10 None Unknown Infrastruct 22-00-AA-33-CC 55% 10 AES WPA-P Infrastruct 00-0C-43-25-60 63% 1 TKIP WPA-P

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

Authentication and	Security			×
Authentication Type	e: WPA2	V	802	1x Setting
Encryption :	TKIP			•
WPA Preshared Ke	y:			
r Wep Key				
€ Key#1	Hex			
C Key#2	Hex			
C Key#3	Hex			
C Key#4	Hex			
	ОК	[Cancel	

*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Click 802.1x setting.

Authentication and	Security		×
Authentication Typ	e: WPA2	802.1x Sett	ing
Encryption :	TKIP		•
WPA Preshared Ke	ey:		
– Wep Key			
💿 Key#1	Hex		
C Key#2	Hex		
C Key#3	Hex		
C Key#4	Hex 💌		
	ОК	Cancel	

5. 802.1x setting page will pop up.

802.1x Setting			×
Certification CA	Server		
Authentication	n Type PEAP	Session Resumption	Disabled 💌
Identity	Pa	ssword	
🔲 Use Client ce	rtificate		
Issued To :	Expire	ed On :	More
Issued By :	Friend	lly Name :	
Allow unauth	enticated provision mode Pro d authentication credentia	visioning Tunnel	•
File Path :		Remove	Import
Tunneled Auther	ntication		
Protocol	EAP-MSCHAP v2	Identity	
		Password	
	ОК	Cancel Apply	Help

5. Authentication type and setting method:

OPEAP:

1. Authentication type chooses PEAP, key identity into wpatest2. Protocol chooses EAP-MSCHAP v2 for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our

intended AP's setting.

02.1× Setting		×
Certification C4	A Server	
Authenticati	ion Type PEAP 💌 Session Resumption Disabled	•
Identity	wpatest2 Password	
Use Client o	certificate	
Issued To :	Expired On : More	
Issued By :	Friendly Name :	
Allow unaut	thenticated provision mode Provisioning Tunnel	7
File Path :	ted authentication credentia Remove Import	
- Tunneled Auth	nentication	
Protocol	EAP-MSCHAP v2 💌 Identity wpatest2	
	Password test2	
	OK Cancel Apply He	elp

2. Click OK. The result will look like the below figure.

Ralink Wireless Utilit	У						
Profile Link Status Site	e Survey Statistics	Advar	nced	About			
SSID	BSSID	Sig	C	Encrypt	Authent	Network T	
WHQL_WEP	00-20-A6-4F-5B	63%	1	WEP	Unknown	Infrastruct	l
<mark>{</mark> ₩PA_TLS	00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct	l
WHQL_WEP	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct	l
WHQL_WPA	00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct	l
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct	l
SoftAP-10	00-00-43-25-67	99%	6	TKIP	WPA-P	Infrastruct	l
AP23	00-07-40-C3-13	26%	10	None	Unknown	Infrastruct	l
xikun-g	22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct	l
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct	l
AP66	00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct	
•						Þ	
Connected <> WPA_TLS Rescan Connect Add to Profile							
					OK	Help	

2TLS / Smart Card:

1. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.

302.1x Setting		×
Certification	A Server	
Authenticat	tion Type TLS/Smart Carc Session Resumption Disabled	-
Identity	wpatest2 Password	
Use Client (certificate	5
Issued To :	Expired On : More	
Issued By :	Friendly Name :	-
Allow unau Use protec File Path :	thenticated provision mode Provisioning Tunnel	
Protocol	Identity Password	
	OK Cancel Apply Help	,

2. TLS must use client certicate. Click more to choose certicate.

802.1x Setting	×
Certification CA Server	
Authentication Type TLS/Smart Car	c▼ Session Resumption Disabled ▼
Identity wpatest2	Password
Use Client certificate	
Issued To :	Expired On : (More)
Issued By :	Friendly Name :
Allow unauthenticated provision mode	Provisioning Tunnel
FIL Use protected authentication credenti File Path :	Remove Import
Tunneled Authentication	
Protocol	Identity
	Password
ОК	Cancel Apply Help

3. Certicate page will pop up; choose a certicate for server authentication.

Certifica	te Selection				×
Issued	tΤo.	Issued By	Expired On	Friendly Name	T,
wpate	st2	2003serv	7/26/2007		Ĭ
1					
		к		Cancel	

3. Display certicate information in use client certicate page.

802.1x Setting
Certification CA Server
Authentication Type TLS/Smart Carc 💌 Session Resumption Disabled 💌
Identity wpatest2 Password
Use Client certificate
Issued To: wpatest2 Expired On: 7/26/2007 Issued By: 2003serv Friendly Name :
Allow unauthenticated provision mode Provisioning Tunnel
File Path : Remove Import
Tunneled Authentication
Protocol Identity
Password
OK Cancel Apply Help

4. Click OK. The result will look like the below figure.

					A all and	Network T
5510	BSSID	5ig	U	Encrypt	Authent	INEtWORK I
WHUL_WEP	UU-2U-A6-4F-5B	63%	1	WEP	Unknown	Infrastruct
WPA_TLS	00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct
WHQL_WEP	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct
WHQL_WPA	00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct
SoftAP-10	00-00-43-25-67	99%	6	TKIP	WPA-P	Infrastruct
AP23	00-07-40-C3-13	26%	10	None	Unknown	Infrastruct
xikun-g	22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct
AP66	00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct
Connected <> WPA	_TLS	Rescan	,	Connec	ct Ac	d to Profile

3TTLS:

1. Authentication type chooses TTLS, identity is wpatest2. Protocol chooses CHAP for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

802.1× Setting	×
Certification CA Server	
Authentication Type TTLS Session Resumpti	on Disabled 💌
Identity wpatest2 Password	
Use Client certificate	
Issued To : Expired On :	More
Issued By : Friendly Name :	
Allow unauthenticated provision mode Provisioning Tunnel Use protected authentication credentia File Path :	Import
Tunneled Authentication	
Protocol CHAP Identity wpa	atest2
Password test	2
OK Cancel Ar	pply Help

2. Click OK. The result will look like the below figure.

SSID	BSSID	Sig	C	Encrypt	Authent	Network T.
WPA TLS	00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct
WHQL_WEP_	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct
WHQL_WPA	00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct
SoftAP-10	00-0C-43-25-67	99%	6	TKIP	WPA-P	Infrastruct
AP23	00-07-40-C3-13	26%	10	None	Unknown	Infrastruct
xikun-g	22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct
AP66	00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct
 ✓ Connected <> WPA 	_TLS	Rescar	1	Conne	ct Ac	dd to Profile

3MD5:

1. Authentication type chooses MD5, MD5 only need identity and password that are wpatest2 and test2 for server authentication.

802.1x Setting		×
Certification C4	A Server	
Authenticati	ion Type Md5-Challenge 💌	
Identity	wpatest2 Password test2	
Use Client o	pertificate	
Issued To :	Expired On : More	
Issued By :	Friendly Name :	
✓ Allow unau ✓ Allow unau ✓ Use protect File Path :		
	OK Cancel Apply Help	

2. Click OK. The result will look like the below figure.

Ralink Wireless Utilit	У						>
Profile Link Status Site	e Survey Statistics	Advar	nced	About			
							,
SSID	BSSID	Sig	C	Encrypt	Authent	Network T	
WHQL_WEP	00-20-A6-4F-5B	63%	1	WEP	Unknown	Infrastruct	
<mark>{</mark> ₩PA_TLS	00-E0-B8-76-18	10	1	TKIP	WPA2	Infrastruct	
WHQL_WEP_	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct	
WHQL_WPA	00-20-A6-50-D3	37%	1	TKIP	WPA-P	Infrastruct	
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruct	
SoftAP-10	00-00-43-25-67	99%	6	TKIP	WPA-P	Infrastruct	
AP23	00-07-40-C3-13	26%	10	None	Unknown	Infrastruct	
xikun-g	22-00-AA-33-CC	55%	10	AES	WPA-P	Infrastruct	
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct	
AP66	00-0C-43-25-60	63%	1	TKIP	WPA-P	Infrastruct	
Connected <> WPA	TLS	Bescan		Conner		d to Profile	
1		nescan		Connec	<u> </u>		
					ОК	Help	

Configure connection with WPA by 802.1x setting

1. Select A.P with WPA authentication mode.

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
🔊 a	00-06-25-49-B1	99%	7	None	Unknown	Infrastruct.
SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.
	00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.
NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.
WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.
	00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.
SSS	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc
ьрр	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.
pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.
	00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.
SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.
Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 🖕
d ⁰¹¹⁰	00.04.50.05.70	0001				i i i
·				_		
			••			

2. Click CONNECT or double click the intended network.

SSID	BSSID	Sig	C	Encry	Authent	Network T
😸 a	00-06-25-49-B1	99%	7	None	Unknown	Infrastruct.
SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.
	00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.
NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.
WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.
	00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.
SSS	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc
ьрр	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.
pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.
	00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.
SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.
Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 🖕
▲ ⁽¹⁾	00.04.50.05.70	0001				
Connected <> a		Bescan	. (Conr		Add to Profile

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

Authentication and !	5ecurit y					×
Authentication Type	: 🔽	PA	•		802.1x Setting	
Encryption :	ТК	JP			•]
WPA Preshared Kej	y: [1
r Wep Key						
€ Key#1	Hex	~				
C Key#2	Hex	~				
C Key#3	Hex	~				
C Key#4	Hex	7				
	OK			Cancel		

*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Click 802.1x setting.

Authentication and	Security		×
Authentication Type	e: WPA	802.1x Sett	ing
Encryption :	TKIP		
WPA Preshared Ke	y:		
– Wep Key			
🖲 Key#1	Hex		
C Key#2	Hex		
C Key#3	Hex		
C Key#4	Hex 💌		
	ОК	Cancel	

5. 802.1x setting page will pop up.

02.1x Setting				×
Certification CA 9	erver			
Authentication	Type PEAP Sess	sion Resumption	Disabled 💌]
Identity	Password			
Use Client cer	tificate			1
Issued To :	Expired On :		More	
Issued By :	Friendly Nam	e:		
Use protected File Path :	nucated provision mode ===rovisionin authentication credentic	Remove	Import]
Tunneled Auther	tication			1
Protocol	EAP-MSCHAP v2 🔽 Ident	ity		
	Pass	word		
	OK Cance	l <u>A</u> pply	Help	

6. Authentication type and setting method:

OPEAP:

1. Authentication type chooses PEAP, key identity into wpatest2. Protocol chooses EAP-MSCHAP v2 for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our

intended AP's setting.

2.1x Setting		
Certification	Server	
Authenticatio	on Type PEAP	Session Resumption Disabled
Identity	wpatest2	Password
🔲 Use Client c	ertificate	
Issued To :	E	Expired On : More
Issued By :	F	Friendly Name :
Use protecte File Path :	ed authentication credentia	Remove Import
- Tunneled Authe	entication	
	EAP-MSCHAP v2	▼ Identitu wpatest2
Protocol	1	
Protocol	,	Password test2
Protocol		Password test2

2. Click OK. The result will look like the below figure.

ofile Link Status Site	e Survey Statistics	Advar	iced	About		
SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
а	00-06-25-49-B1	99%	7	None	Unknown	Infrastruct.
SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.
	00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.
NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.
🥁 WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.
	00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.
SSS	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc
bbb	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.
pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.
	00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.
SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.
Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 🖵
A 100	00.04.50.05.30					
Connected <> WPA	TLS	Rescan		Conn	iect /	Add to Profile

2TLS / Smart Card:

1. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.

802.1× Setting		×
Certification	A Server	
Authenticati	ion Type TLS/Smart Carc Session Resumption Disabled	1
Identity	wpatest2 Password	
🔽 Use Client d	certificate	
Issued To :	Expired On : More	
Issued By :	Friendly Name :	
Allow unaut Use protect File Path :	thenticated provision mode Provisioning Tunnel ted authentication credentia Remove Import nentication	
Protocol	Identity	
	Password	
	OK Cancel Apply Help	

2. TLS must use client certicate. Click more to choose certicate.

802.1x Setting	×
Certification CA Server	
Authentication Type TLS/Smart Card	Session Resumption Disabled 💌
Identity wpatest2	Password
Use Client certificate	
Issued To : E	xpired On : More
Issued By : F	iriendly Name :
Allow unauthenticated provision mode Use protected authentication credentiation File Path : Tunneled Authentication Protocol	Provisioning Tunnel
OK	Cancel Apply Help

3. Certicate page will pop up; choose a certicate for server authentication.

Certificate Selection				×
Issued To	Issued By	Expired On	Friendly Name	I,
wpatest2	2003serv	7/26/2007		ii i
1				
0	к		Cancel	

4. Display certicate information in use client certicate page.

802.1x Setting
Certification CA Server
Authentication Type TLS/Smart Carc 💌 Session Resumption Disabled 💌
Identity wpatest2 Password
Use Client certificate
Issued To: wpatest2 Expired On: 7/26/2007 Issued By: 2003serv Friendly Name :
Allow unauthenticated provision mode Provisioning Tunnel
File Path : Remove Import
Tunneled Authentication
Protocol Identity
Password
OK Cancel Apply Help

5. Click OK. The result will look like the below figure.

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
a	00-06-25-49-B1	99%	7	None	Unknown	Infrastruct.
SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.
	00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.
NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.
😸 WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.
	00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.
SSS	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc
ьрр	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.
pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.
	00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.
SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.
Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 🖕
1 0000	00.04.50.05.70	0001				

3TTLS:

1. Authentication type chooses TTLS, identity is wpatest2. Protocol chooses CHAP for tunnel authentication, tunnel identity is wpatest2 and tunnel password is test2. Those setting are same as our intended AP's setting.

802.1x Setting	-	×
Certification CA	A Server	
Authenticati	on Type TTLS Session Resumption Disabled	
Identity	wpatest2 Password	
🔲 Use Client c	ertificate	
Issued To :	Expired On : More	
Issued By :	Friendly Name :	
Allow unaut	henticated provision mode Provisioning Tunnel ed authentication credentic Remove Import	
Tunneled Auth	entication	
Protocol	CHAP Identity wpatest2	
	Password test2	
	OK Cancel Apply Help	

2. Click OK. The result will look like the below figure.

SSID	BSSID	Sia	C	Eneru	Authent	Network T 🔺
3	00-06-25-49-81-	99%	7	None	Unknown	Infrastruct
SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.
	00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.
NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.
WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.
	00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.
\$\$\$	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc
ЬЬЬ	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.
pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.
	00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.
SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.
Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 🖵
▲	00.04.50.05.70					
Connected <> WPA_TLS Rescan Connect Add to Profile						

MD5:

1. Authentication type chooses MD5, MD5 only need identity and password that are wpatest2 and test2 for server authentication.

802.1x Setting		x
Certification C4	4 Server	
Authenticati	ion Type Md5-Challenge 💌	
Identity	wpatest2 Password test2	
Use Client o	ertificate	
Issued To :	Expired On : More	
Issued By :	Friendly Name :	
Allow unaut Use protect File Path : Tunneled Auth Protocol	thenticated provision mode Provisioning Tunnel ied authentication credentia rentication Identity Password	
	OK Cancel Apply Help	

2. Click OK. The result will look like the below figure.

🧟 Ra	alink Wireless Utilit	У						x
Pro	ofile Link Status Site	e Survey Statistics	Advar	nced	About			
	SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺	
	а	00-06-25-49-B1	99%	7	None	Unknown	Infrastruct.	
	SWRoaming	00-0D-54-9B-83	91%	1	WEP	Unknown	Infrastruct.	
		00-0F-F7-EB-25	39%	1	None	Unknown	Infrastruct.	
	NDTESTAP7	00-0C-41-13-4C	26%	1	None	Unknown	Infrastruct.	
(🥁 WPA_TLS	00-07-40-9F-5D	99%	1	TKIP	WPA	Infrastruct.	
		00-0C-43-25-60	37%	1	WEP	Unknown	Infrastruct.	
	SSS	7E-2E-C0-7D-5F	26%	4	None	Unknown	Ad hoc	
	ьрр	00-07-40-D8-FC	18%	6	None	Unknown	Infrastruct.	
	pod1	00-0F-F7-EB-25	20%	6	WEP	Unknown	Infrastruct.	
		00-E0-18-F4-44	99%	6	TKIP	WPA-P	Infrastruct.	
	SWRoaming	00-0D-28-88-D5	91%	9	TKIP	WPA-P	Infrastruct.	
	Buffalo-244wep	00-07-40-D8-C7	81%	11	WEP	Unknown	Infrastruct. 😈	
	▲ 1000	00.04.50.05.70	0001					
					[
	Connected <> WPA	_TLS	Rescar	·	Conr	iect /	Add to Profile	
	, 							-
_							1	_
						OK	Help	

Configure connection with WPA2-PSK

1. Select the AP with WPA2-PSK authentication mode.

SSID	BSSID	Sig	C	Encry	Authentica	Network T
😸 AP23	00-07-40-C3-13	29%	10	None	Unknown	Infrastruct.
WHQL_WEP	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct.
AP66	00-0C-43-25-60	57%	1	TKIP	WPA-PSK	Infrastruct.
WHOL_WPA	00-20-A6-50-D3	60%	1	TKIP	WPA-PSK	Infrastruct.
WHQL_WEP_	00-20-A6-4F-5B	57%	1	WEP	Unknown	Infrastruct.
PSKtest	00-E0-B8-76-18	10	1	TKIP	WPA2-PSK	Infrastruct.
SoftAP-10	00-00-43-25-67	89%	6	TKIP	WPA-PSK	Infrastruct.
	00-E0-18-F4-44	44%	6	WEP	Unknown	Infrastruct.
SW-Dlink	00-0D-88-91-BA	60%	8	WEP	Unknown	Infrastruct.
xikun-g	22-00-AA-33-CC	34%	10	AES	WPA-PSK	Infrastruct.
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct.
•						
xikun-g PCWA-A820	22-00-AA-33-UU 00-90-96-52-27	34% 52%	10	AES None	WPA-PSK Unknown	Infrastr

2. Click CONNECT or double click the intended network.

SSID	BSSID	Sig	C	Encry	Authentica	Network T.
😸 AP23	00-07-40-C3-13	29%	10	None	Unknown	Infrastruct
WHQL_WEP	00-40-96-56-2A	60%	1	WEP	Unknown	Infrastruct
AP66	00-0C-43-25-60	57%	1	TKIP	WPA-PSK	Infrastruct
WHQL_WPA	00-20-A6-50-D3	60%	1	TKIP	WPA-PSK	Infrastruct.
WHQL_WEP	00-20-A6-4F-5B	57%	1	WEP	Unknown	Infrastruct.
PSKtest	00-E0-B8-76-18	10	1	TKIP	WPA2-PSK	Infrastruct.
SoftAP-10	00-0C-43-25-67	89%	6	TKIP	WPA-PSK	Infrastruct.
	00-E0-18-F4-44	44%	6	WEP	Unknown	Infrastruct.
SW-Dlink	00-0D-88-91-BA	60%	8	WEP	Unknown	Infrastruct.
xikun-g	22-00-AA-33-CC	34%	10	AES	WPA-PSK	Infrastruct.
PCWA-A820	00-90-96-52-27	52%	11	None	Unknown	Infrastruct
•						
Connected <> AP23 Rescan Connect Add to Profile						

6. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

Authentication and Se	curity		×
Authentication Type :	WPA2-PSK	•	802.1x Setting
Encryption :	TKIP		•
WPA Preshared Key :			
€ Key#1	Hex 🔽		
C Key#2	Hex 🔽		
C Key#3	Hex		
C Key#4	Hex		
[ОК	Canc	el

*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

7. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Key secret as 12345678.

Authentication and Securi	y 2	×
Authentication Type :	WPA2-PSK	
Encryption :	TKIP	
WPA Preshared Key :	12345678	
€ Key#1 Hex		
C Key#2 Hex		
C Key#3 Hex	V	
C Key#4 Hex		
	OK Cancel	

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

SID	BSSID	Sig	<u> </u>	Encry	Authentica	Network.
PSKtest	00-E0-B8-76-18	10	1	TKIP	WPA2-PSK	Infrastruc
WHQL_WPA	00-20-A6-50-D3	60%	1	TKIP	WPA-PSK	Infrastruc
WHQL_WEP	00-20-A6-4F-5B	60%	1	WEP	Unknown	Infrastruc
WHQL_WEP	00-40-96-56-2A	76%	1	WEP	Unknown	Infrastruc
AP66	00-0C-43-25-60	42%	1	TKIP	WPA-PSK	Infrastruc
	00-E0-18-F4-44	52%	6	WEP	Unknown	Infrastruc
SoftAP-10	00-00-43-25-67	91%	6	TKIP	WPA-PSK	Infrastruc
SW-Dlink	00-0D-88-91-BA	65%	8	WEP	Unknown	Infrastruc
xikun-g	22-00-AA-33-CC	44%	10	AES	WPA-PSK	Infrastruc
AP23	00-07-40-C3-13	15%	10	None	Unknown	Infrastruc
PCWA-A820	00-90-96-52-27	63%	11	None	Unknown	Infrastruc

Configure connection with WPA-PSK

1. Select the AP with WPA-PSK authentication mode.

SSID	BSSID	Sig	-C	Enery	Authent	Network T
PSKtest N	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
NDTESTAPI S	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
MDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct
Connected <> NDC	_CASE]	RESCAI	N	CONN	ect A	DD PROFILE

2. Click CONNECT or double click the intended network.

SSID	BSSID	Sig	C	Encry	Authent	Network T
PSKtest N	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
NDTESTAP1	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
SNDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct
	CASE				TOT D	

3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

uthentication &	Security						2
Authentication Ty	pe:	WPA-PSI	<u>·</u>	 Encrypt 	tion Type:	TKIP	 •
WPA Pre-Shared	Кеу:						
- MEP Ver							
€ Key# <u>1</u>	Hexadec	imal 🔽] [
€ Key# <u>2</u>	Hexadec	imal 🔽] [
C Key# <u>3</u>	Hexadec	imal 📃]				
С Кеу# <u>4</u>	Hexadec	imal 🗾] [
		K			CANC	EL	

*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Key secret as 01234567.
| Authentication Typ
WPA Pre-Shared K | e: WP.
ey: 012 | A-PSK
34567 | Encryp | tion Type: Tk | ΊΡ | • |
|--|-------------------|----------------|--------|---------------|----|---|
| - WEP Key | | | | | | |
| € Key#1 | Hexadecimal | <u>*</u> | | | | |
| € Key# <u>2</u> | Hexadecimal | ×. | | | | |
| € Key# <u>3</u> | Hexadecimal | Ŧ | | | ļ | |
| C Key#4 | Hexadecimal | Ŧ | | | | |

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

SID	BSSID	Sig	C	Encry	Authent	Network T
PSK test	00-0C-43-25-61	65%	1	TKIP	WPA-P	Infrastruct
NDTESTAP1	00-40-96-56-2A	37%	1	Not Use	Unknown	Infrastruct
miffy	00-0C-43-25-61	65%	1	TKIP	WPA	Infrastruct
SoftAP-D8	00-0A-40-00-00	65%	1	Not Use	Unknown	Infrastruct
AP000C43256	00-0C-43-05-00	55%	1	WEP	Unknown	Infrastruct
WAP11	00-06-25-55-D8	29%	1	WEP	Unknown	Infrastruct
Qoo_1	B2-00-CF-03-3	23%	3	Not Use	Unknown	Ad Hoc
Buffalo	00-07-40-4D-0	10	6	TKIP	WPA	Infrastruct
NDC_CASE	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct
NDTESTAP2	00-04-76-A5-E	10	6	WEP	Unknown	Infrastruct
BuffaloG	00-07-40-76-D	34%	11	Not Use	Unknown	Infrastruct
onnected <> PSKt	est J	RESCAI	v	CONN	ECT A	DD PROFILE

Configure connection with WEP on

1. Select AP with WEP encryption.

SSID	BSSID	Sig	C	Encry	Authent	Network T	~
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.	
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.	
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.	
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.	
AP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct.	=
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.	
😸 Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.	
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.	
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.	
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.	
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct.	-
<				1,22, 22.97		· >	
Connected <> Dell1	184	REGULAN	J	CONN	ECT A	UD PROFIL	F

2. Click CONNECT or double click intended network.

SSID	BSSID	Sig	C	Encry	Authent	Network T 🔺
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	б	WEP	Unknown	Infrastruct.
AP25-Left は	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct. 🗏
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.
🥳 Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct.
4				1.44 (44)		

3. Authentication & Security page pop up.

Authentication & Security
Authentication Type: Open Encryption Type: WEP WPA Pre-Shared Key:
WEP Key • Key#1 Hexadecimal • Key#2 Hexadecimal • Key#3 Hexadecimal • Key#4 Hexadecimal
<u>O</u> K <u>C</u> ANCEL

4. Enter 1234567890 at Key#1 which is same as our intended AP's setting.

Authentication Type: WPA Pre-Shared Key:	Open	💌 Encryp	otion Type: WEP	•
WEP Key Key# <u>1</u> Hex Key# <u>2</u> Hex	adecimal 💌 adecimal 💌	0123456789)	
⊂ Key# <u>3</u> Hexa	decimal 💌			
⊂ Key# <u>4</u> Hexa	adecimal 💌			

5. Click OK. The result will look like the below figure.

SSID	BSSID	Sig	C	Encry	Authent	Network T	~
miffy	00-0C-43-25-61	73%	1	TKIP	WPA-P	Infrastruct.	1
WAP11	00-06-25-55-D8	47%	1	WEP	Unknown	Infrastruct.	
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.	
MITESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.	
hP25-Left	00-0C-43-25-61	10	6	WEP	Unknown	Infrastruct.	=
wpa	00-E0-18-F4-44	10	6	TKIP	WPA-P	Infrastruct.	
Dell1184	00-90-4B-33-22	10	6	Not Use	Unknown	Infrastruct.	
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.	
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct.	
default	00-90-96-28-39	76%	6	Not Use	Unknown	Infrastruct.	
linksys 54	00-06-25-4A-74	10	11	Not Use	Unknown	Infrastruct.	~
<			1.69				
Connected <> ND	TESTAP1	RESCA	N I	CONN	ECT A	DD PROFIL	E

Example to add profile in profile page

1. Click ADD in profile page

Profile	SSID	Channel	Authentication	Encryption	Network Type

2. Add Profile page will pop up

Add Profile	
Profile Name PROF1	SSID
System Configuration Authentication & Security	y
Power Saving Mode	
CAM (Constantly Awake Mode)	C Power Saving Mode
CAM when AC Power	
Natural Trees	
Infrastructure	
11B Preamble Type Auto	*
┌─ RTS Threshold 0 '	2347 2347
Fragment Threshold 256	2347 2347
OK	CANCEL

3. Change profile name to TEST.

dd Profile			D
Profile Name TEST		SSID	•
System Configuration A	uthentication & Security	1	
Power Saving Mode —			
CAM (Constantly	y Awake Mode)	🔘 Power Saving Mode	
CAM when AC I	'ower		
Network Type	Infrastructure 💌]	
11B Preamble Type	Auto]	
🖵 R TS Threshold	0 .	2347 2347	
Fragment Thresh	old 256 ,	2347 2347	
MERCE RECEIPTION OF CASE	-	1 /	
[OK	CANCEL	

4. Pull down SSID and select one intended AP. The AP list is the result of last site survey.

dd Profile			
Profile Name TEST	/	SSID I	J
System Configuration Aut)	nentication & Security	wpa AP350 NDTESTAP1	
Power Saving Mode		default b	Ť
CAM when AC Pow	ver		
11B Freamble Type	Auto 🗾		
🖵 RTS Threshold	0 .	2347 2347	
Fragment Threshold	1 256 .	2347 2347	
	Ōĸ	CANCEL	

5. Set Power Saving Mode.

ldd Profile			
Profile Name TEST		SSID NDTESTAP1	-
System Configuration A1	uthentication & Securit	ע	
Power Saving Mode CAM (Constantly CAM when AC P	v Awake Mode) ower	Power Saving Mode	
Network Type	Infrastructure	• •	
🕅 RTS Threshold	0 ,	<u>}</u> 2347 2347	
🦵 Fragment Thresh	old 256 ,	Y 2347 2347	
	OK	CANCEL	

6. Click Authentication & Security page

rstem Configuratio	n Authentic	ation & Secu	nty			
Authentication T	ype:	Open	Enc	ryption Type: 🛛	one	•
WPA Pre-Shared	Кеу:					
- WEP Key						
€ Key#1	Hexadecu	nal 💌			ļ,	
C Key#2	Hexadecii	nal 💌			Ĩ.	
€ Key# <u>3</u>	Hexadecu	nal 💌				
C Key# <u>4</u>	Hexadecu	nal 💌				

7. Click OK. Then we can find the profile name appears in the grid.

Profile	SSID	Channel	Authentication	Encryption	Network Type
TEST	NDTESTAP1	Auto	Open System	WEP	Infrastructure
					1.000 C
				1	
¢]	<u>31</u>	- Li	IIII		>

8. Click ACTIVATE. Activate the profile setting.

le LinkS	tatus Site Survey	Statistics A	dvance About	1	
rofiles List - Profile	SSID	Channel	Authentication	Encryption	Network Type
🖌 TEST	NDTESTAP1	Auto	Open System	WEP	Infrastructure
(
<u>A</u> DI	o	DELETE	EDIT		A <u>c</u> tivate

9. Follow section 12, section 13 and section 14 to set authentication and security page.

Example on adding profile in site survey page

11 1 6	Not Use Not Use	Unknown	Infrastruct.
1 6	Not Use	TT 1	The second s
6		Unknown	Infrastruct.
	WEP	Unknown	Infrastruct.
6	WEP	Unknown	Infrastruct.
6	Not Use	Unknown	Infrastruct.
6	Not Use	Unknown	Infrastruct.
6	Not Use	Unknown	Infrastruct.
6	Not Use	Unknown	Infrastruct.
6	TKIP	WPA-P	Infrastruct.
6	WEP	Unknown	Infrastruct.
11	Not Use	Unknown	Infrastruct.
	1,441,94497		- >
	6 6 6 6 6 6 11	6 Not Use 6 WEP 11 Not Use	6 Not Use Unknown 6 Not Use Unknown 6 Not Use Unknown 6 Not Use Unknown 6 TKIP WPA-P 6 WEP Unknown 11 Not Use Unknown

1. Select the indented network from site survey list.

2. Click ADD PROFILE.

GGID	DeetD	0.0		Error	A seal and	Not the T	
SOLD MILCI	BSSID	51g	1.1	Encry	Aument	Network I	^
BullaloG	00-07-40-76-D	10%	11	NotUse	Unknown	Infrastruct.	
3com	00-0B-AC-E7-5.	83%	1	NotUse	Unknown	Infrastruct.	
NDTESTAP2	UU-4U-96-54-B5.	10	6	WEP	Unknown	Infrastruct.	
AP25-Left	00-0C-43-25-61.	10	6	WEP	Unknown	Infrastruct.	
default	00-90-96-28-39.	10	6	Not Use	Unknown	Infrastruct.	=
	00-07-40-4D-0	10	6	Not Use	Unknown	Infrastruct.	
Dell1184	00-90-4B-33-22.	10	6	Not Use	Unknown	Infrastruct.	
Ralink_tess	00-06-25-4A-75.	10	6	Not Use	Unknown	Infrastruct.	
wpa	00-E0-18-F4-44.	10	6	TKIP	WPA-P	Infrastruct.	
NDTESTAP1	00-40-96-41-93.	10	6	WEP	Unknown	Infrastruct.	
linksys 54	00-06-25-4A-74.	10	11	Not Use	Unknown	Infrastruct.	~
<			- K.		· · · ·		-
Connected <> Bu	ffaloG	RESCA	N I	CONN	ECT I	DD PROFIL	E

3. System will pop up Add Profile windows

dd Profile	
Profile Name PROF1	SSID Dell1184
System Configuration Authentication & Securit	v
Power Saving Mode	
💿 CAM (Constantly Awake Mode)	🔿 Power Saving Mode
CAM when AC Power	
·	
Network Type Infrastructure	-
11B Preamble Type Auto	Y
□ RTS Threshold 0 '	2347 2347
256	. 2247
Fragment Threshold	
<u>OK</u>	CANCEL

4. Change profile Name from PROF1 to FAVORITE.

Add Profile			×
Profile Name FAVORITE		SSID Dell1184	-
System Configuration Aut	rentication & Security		
Power Saving Mode —			
C CAM (Constantly I	Awake Mode)	Power Saving Mode	
CAM when AC Po	wer		
Network Type	Infrastructure 💌		
11B Preamble Type	Auto		
🔽 RTS Threshold	0 ,	\$ 2347 2347	
Ersonant Threshol	, 256 ,	2347 2347	
1 Hagment Hieston		J [2300]	
	OK I	CANCEL	
		CANCED	

5. Click OK without changing other value.

System Not Us	e Infrastructure

6. Follow <u>section 12</u>, <u>section 13</u>, <u>section 14</u>, <u>section 15</u> and <u>section 16</u> to set authentication and security page.

About

About page display the wireless card and driver version information as figure 9-1 shown.

🛱 Ralink Wireless Utility	X
Profile Link Status Site Survey Statistics Advanced About	
(c) Copyright 2004, Ralink Technology, Inc. All rights reserved.	
2 RaConfig Version : 2.3.0.0 Date : 12-08-2004	
Driver Version : 3.0.1.0 Date : 12-15-2004	
EEPROM Version : 1.1	
3 IP Address : 192.168.2.170 Phy_Address : 00-0C-43-25-68-31	
Sub Mask : 255.255.255.0 Default Gateway :	

Figure 9-1 About Page

Oconnect to Ralink's website: <u>Ralink Technology, Corp.</u>

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

3Display Wireless NIC MAC address.

QoS

Figure 10-1 shows QoS Page of RaConfig. It involves "WMM Enable", "WMM – Power Save Enable" and DLS setup. The introduction indicates as follow:

1🚭 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics Advanced QoS About	
WMM Enable Apply	
WMM - Power Save Enable Setting	
Direct Link Setup Enable Apply	
Direct Link Direct Link Setup MAC Address:	
Tear Down OK	

Figure 10-1 QoS Page

WMM Enable: Enable Wi-Fi Multi-Media. The setting method follows <u>section 17</u>.
WMM – Power Save Enable: Enable WMM Power Save. The setting method follows <u>section 18</u>.

Oirect Link Setup Enable: Enable DLS (Direct Link Setup). The setting method follows <u>section 19</u>.

Country Channel List

Country channel list, channel classification and range.

According to your window, find out corresponding table.

Classification	Rang	ge
0:	CH1 ~	CH11
1:	CH1 ~	CH13
2:	CH10 ~	CH11
3:	CH10 ~	CH13
4:	CH14 ~	CH14
5:	CH1 ~	CH14
6:	CH3 ~	CH9
7:	CH5 ~	CH13

\sim			
112	CCITI	rati	nn
	22111	Lau	OIL

Range

		-
0: FCC	CH1 ~	CH11
1: IC (Canada)	CH1 ~	CH11
2: ETSI	CH1 ~	CH13
3: SPAIN	CH10 ~	CH11
4: FRANCE	CH10 ~	CH13
5: MKK	CH14 ~	CH14
6: MKKI (TELEC)	CH1 ~	CH14
7: ISRAEL	CH3 ~	CH9

Country Name	Classification	Range
Argentina	0	CH1~11
Australia	1	CH1~13
Austria	1	CH1~13
Bahrain	1	CH1~13
Belarus	1	CH1~13
Belgium	1	CH1~13
Bolivia	1	CH1~13
Brazil	0	CH1~11
Bulgaria	1	CH1~13
Canada	0	CH1~11
Chile	1	CH1~13
China	1	CH1~13
Colombia	0	CH1~11
Costa Rica	1	CH1~13
Croatia	1	CH1~13
Cyprus	1	CH1~13
Czech Republic	1	CH1~13
Denmark	1	CH1~13
Ecuador	1	CH1~13
Egypt	1	CH1~13
Estonia	1	CH1~13
Finland	1	CH1~13
France	3	CH10~13
France2	1	CH1~13
Germany	1	CH1~13

Greece	1	CH1~13
Hong Kong	1	CH1~13
Hungary	1	CH1~13
Iceland	1	CH1~13
India	1	CH1~13
Indonesia	1	CH1~13
Ireland	1	CH1~13
Israel	6	CH3~9
Italy	1	CH1~13
Japan	5	CH1~14
Japan2	4	CH14~14
Japan3	1	CH1~13
Jordan	3	CH10~13
Kuwait	1	CH1~13
Latvia	1	CH1~13
Lehanon	1	CH1~13
Latvia	1	CH1~13
Lehanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1.13
Luxombourg	1	CH1.13
Macadopia	1	
Malaysia	1	
Maxiaa		
Managan	1	
	1	CH1~13
Netherlands	1	CHI~13
New Zealand	1	CHI~13
Nigeria	1	CH1~13
Norway	1	CH1~13
Panama	1	CH1~13
Paraguay	1	CH1~13
Peru	1	CH1~13
Philippines	1	CH1~13
Poland	1	CH1~13
Portugal	1	CH1~13
Puerto Rico	1	CH1~13
Romania	1	CH1~13
Russia	1	CH1~13
Saudi Arabia	1	CH1~13
Singapore	1	CH1~13
Slovakia	1	CH1~13
Slovenia	1	CH1~13
South Africa	1	CH1~13
South Korea	1	CH1~13
Spain	2	CH10~11
Sweden	1	CH1~13
Switzerland	1	CH1~13
Taiwan	0	CH1~11
Thailand	1	CH1~13
Turkey	1	CH1~13
United Arab Emirates	1	CH1~13
United Kingdom	1	CH1~13
United States of America	0	CH1~11
Uruguay	1	CH1~13
Venezuela	1	CH1~13
Yugoslavia	0	CH1~11
-		

Advance

🛱 Ralink Wireless Utility	×
Profile Link Status Site Survey Statistics	Advanced About
_	6
Wireless mode 802.11 A/B/G mi	Select Your Country Region Code
	11 A 0: CH 36,40,44,48,5 -
2 B/G Protection Auto	Enable CCX (Cisco Compatible eXtensions)
3 Tx Rate Auto 💌	Tum on CCKM
	Enable Radio Measurement
TXBURST	Non-Serving Channel Measurements
5 🗖 Fast Roaming at -70 dBm	Limit 250 milliseconds (0-2000)
3	9
Turn off RF	Apply
	OK Help

Figure 8-1 shows advance setting page of RaConfig

Figure 8-1 Advance setting

Wireless mode: Select wireless mode. 802.11B only, 802.11 B/G mixed 802.11A only, 802.11 A/B/G mixed and 802.11G only modes are supported.

211B/G Protection: ERP protection mode of 802.11G definition. User can choose from Auto, On, and Off.

- 1. Auto: STA will dynamically change as AP announcement.
- 2. On: Always send frame with protection.
- 3. Off: Always send frame without protection.

3TX Rate: Manually force the Transmit using selected rate. Default is auto.

GTX Burst: Ralink's proprietary frame burst mode.

⁶Fast Roaming at: fast to roaming, setup by transmit power.

⁶Select Your Country Region Code: eight countries to choose. Country channel list: <u>Country channel list</u>

Enable CCX (Cisco Compatible eXtensions): support Cisco Compatible Extensions function:

- 1. LEAP turn on CCKM
- 2. Enable Radio Measurement: can channel measurement every 0~2000 milliseconds.

8 Turn radio ON/OFF for FAA requirement.

EADIO ON Radio On: Indicate to turn on radio.

T Radio Off: Indicate to turn off radio.

9 Apply the above changes.

Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for user to understand. Figure 7-1 shows the detail page layout.

ofile Link Status Site Survey Statistics Advance Al	out	
Transmit Statistics		
Frames Transmitted Successfully	=	208
Frames Transmitted Successfully Without Retry	=	196
Frames Transmitted Successfully After Retry(s)	=	12
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
Receive Statistics		
Frames Received Successfully	=	23173
Frames Received With CRC Error	=	224800
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0
	3	RESET COUNTER:

Figure 7-1 Transmit and Receive statistics

Transmit Statistics:

1. Frames Transmitted Successfully: Frames successfully sent.

2. Frames Transmitted Successfully Without Retry: Frames successfully sent without any retry.

3. Frames Transmitted Successfully After Retry: Frames successfully sent with one or more reties.

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

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

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

Receive Statistics:

- 1. Frames Received Successfully: Frames received successfully.
- 2. Frames Received With CRC Error: Frames received with CRC error.

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

4. Duplicate Frames Received: Duplicate received frames.

③Reset counters to zero.

Link Status

connection.	
Ralink Wireless Utility	×

Figure 6-1 is the link status page: it displays the detail information current

	T (041)	54.0	D. (Mar)	10
Link Speed :		J 34.0	HX (MDps)	1.0
Throughput :	Tx (Kbps)	0.1	Rx (Kbps)	16.7
	Good 77%			
🖓 Link Quality :				
	Normal 50%			dBm
Signal Strength :				
	Normal 70%			
Noise Level :				

Figure 6-1 Link Status information

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

2Extra Info: Display link status and current channel in use.

3Link Speed: Show current transmit rate and receive rate.

GThroughout: Display transmits and receive throughput in unit of K bits/sec.

⁶Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.

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

One of the second strength of the second strength.

Profile

Profile can book keeping your favorite wireless setting among your home, office, and other public hotspot. You may save multiple profiles, and activate the correct one at your preference. Figure 5-1 shows the profile page setting.

Profile	SSID	Channel	Authentication	Encryption	Network Type
PROF1	NDTESTAP2	Auto	Open System	Not Use	Infrastructure
PROF2	WAP11	Auto	Open System	Not Use	Infrastructure
/PROF3	BuffaloG	Auto	Open System	Not Use	Infrastructure
	Dell1184	Auto	Open System	NotUse	Infrastructure
1			101		16

Figure 5-1 Profile page

• Definition of each field:

- 1. Profile: Name of profile, preset to PROF* (* indicate 1, 2, 3,).
- 2. SSID: AP or Ad-hoc name.
- 3. Cannel: Channel in use for Ad-Hoc mode.
- 4. Authentication: Authentication mode.
- 5. Encryption: Security algorithm in use.
- 6. Network Type: Network's type, including infrastructure and Ad-Hoc.

Onnection status

Indicate connection is successful on currently activated profile.

Indicate connection is failed on currently activated profile.

Note: When use site survey to make the connection. None of the profile will have the connection status icon.

3Add a new profile.

Oelete an existing profile.

6 Edit Profile.

6 Activate selected profile.

CA Server

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

802.1x Setting
Certification CA Server
Use certificate chain
Any Trusted CA -
2 Allow intermidiate certificates
3 Server name :
 Server name must match exactly Domain name must end in specified name
OK Cancel Apply Help

Certificate issuer: Choose use server that issuer of certificates.

2Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.

³Server name: Enter an authentication sever root.

802.1x Setting

 $802.1x\ is\ a\ authentication\ for\ [WPA]\ and\ [WPA2]\ certificate\ to\ server.$ Show as figure

Authentication 1	Type PEAP	Disabled 💌
Identity	Password	
Use Client certif	icate	
Issued To :	Expired On :	More
Issued By :	Friendly Name :	
Allow unauthen Use protected a File Path :	ticated provision mode Provisioning Tunnel	Import
	cation	
Tunneled Authenti		
Tunneled Authenti Protocol	EAP-MSCHAP v2	

Authentication type:

- 1. PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication 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.
- 4. LEAP: Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.

5. 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: user can choose " Disable " and " Enable ".

3 Identity and Password: Identity and password for server.

GUse Client Certicate: Client Certicate for server authentication.

5 Tunnel Authentication

- 1. Protocol: Tunnel protocol, List information include "EAP-MSCHAP", "EAP-MSCHAP v2", "CAHAP" and "MD5".
- 2. Tunnel Identity: Identity for tunnel.
- 3. Tunnel Password: Password for tunnel.

⁶CA Server: Certificate Authority Server. Each certificate is signed or issued by it. The detail operation will explain in section 6.

Encryption Setting - WEP/TKIP/AES

Add Profile	×
Configuration Authentication and Security	
Authentication Type : Open 2 802.1x Setting	
Cencryption :	
WPA Preshared Key :	
6 Wep Key	
© Key#1 Hex ▼	
C Key#2 Hex	
C Key#3 Hex	
C Key#4 Hex	
OK Cancel Apply Help	

Authentication & Security setting, shown as figure 4-1.

Figure 4-1 Authentication & Security setting

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

802.1x Setting: It will display to set when user use radius server to authenticate client certificate for WPA authentication mode. The detail operation will explain in section 5

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

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.

⁶WEP Key: Only valid when using WEP encryption algorithm. The key must matched AP's key. There are several formats to enter the keys.

- 1. Hexadecimal (40bits): 10 Hex characters.
- 2. Hexadecimal (128bits): 32Hex characters.
- 3. ASCII (40bits): 5 ASCII characters.
- 4. ASCII (128bits): 13 ASCII characters.

There are examples in section 12, section 13 and section 14 section 15, section $\underline{16}^{}$

**Powered by Meetinghouse.

Site Survey

Under the site survey page, system will display the information of surrounding APs from last scan result. List information's include SSID, BSSID, Signal, Channel, Encryption algorithm, and Network type as Figure 3-1 shown.

SSID	BSSID	Signal	Channel	Encryption	Authentication	Network Type
SAP	00-0C-4	99%	5	NotUse	Unknown	Infrastructure
AP2500	00-0C-4	99%	1	Not Use	Unknown	Infrastructure
WAP11	00-06-25	99%	1	Not Use	Unknown	Infrastructure
NDTES	00-40-96	78%	6	WEP	Unknown	Infrastructure
NDTES	00-0D-5	89%	6	WEP	Unknown	Infrastructure
Dell1184	00-90-4	78%	6	Not Use	Unknown	Infrastructure
default	00-90-96	81%	6	Not Use	Unknown	Infrastructure
- DuffaloG	00-07-40	100%	11	AES-CC	WPA-PSK	Infrastructure
SMC28	00-04-E	100%	11	Not Use	Unknown	Infrastructure
<	- SMC 2004 IV		4	.N 0	ONNECT 6	

Figure 3-1 Detail information of site survey page

Definition of each field

- 1. SSID: Name of BSS of IBSS network.
- 2. BSSID: MAC address of AP or randomly generated of IBSS.
- 3. Signal: Receive signal strength of specified network.
- 4. Channel: Channel in use.

5. Encryption: Encryption algorithm used within than BSS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.

6. Authentication: Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.

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

Connected network:

 When RaConfig first ran, it will select the best AP to connect automatically.
 If user wants to connect to other AP. He can double click mouse on the intended AP to make connection.

3. If the intended network has encryption other than " Not Use ", RaConfig will bring up the security page and let use input the appropriate information to make the connection. Please refer to section 4 on how to fill the security

information.

Whis icon indicates the change is successful.

3Indicate connection status, the connected network's SSID will show up here.

Susce an rescan command to wireless NIC to update information on surrounding wireless network.

Openation of the selected network.

1 Add the selected AP to Profile settin. It will bring up profile page and save user's setting to a new profile.

ADD/EDIT Profile

1. System Configuration: as figure 3-2 shown.

Configuration Authentication and Security Profile Name PRDF2 SSID 2 PSM © CAM (Constantly Awake Mode) © PSM (Power Saving Mode)
Profile Name PROF2 SSID 2 3 PSM © CAM (Constantly Awake Mode) © PSM (Power Saving Mode)
Profile Name PROF2 SSID SSID SSID C PSM (Constantly Awake Mode) PSM (Power Saving Mode)
3 PSM © CAM (Constantly Awake Mode) © PSM (Power Saving Mode)
CAM (Constantly Awake Mode) C PSM (Power Saving Mode)
4 Network Type Ad hoc 🔽 TX Power Auto 💽 5
6 Preamble Auto
Channel
Fragment Threshold 256 2346 2346 1
OK Cancel Apply Help

Figure 3-2 Profile system configuration

Profile Name: User chose name for this profile.

2SSID: User can key in the intended SSID name or use pull down menu to select from available APs.

Orever Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode. There is a check box for "CAM when AC power". When this is checked, the wireless NIC will stay full power when AC power cord is plug into power outlet. Network Type: There are two types, infrastructure and 802.11 ad-hoc modes. Under ad-hoc mode, user can also choose the preamble type; the available preamble type includes short and long. In addition to that, the channel and Ad hoc wireless mod field will be available for setup in ad-hoc mode.

⁵TX Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. User can choose power value by sliding the bar.

⁶Preamble: There are three types, Auto, Long and Short are supported.

RTS Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.

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

⁽³⁾Channel: Only available for setting under ad-hoc mode. User can choose the channel frequency to start their ad-hoc network.

2. Authentication & Security setting shown in figure 3-3. The detail operation will explain in section 4 for more through detail.

Add Profile		×
Configuration Authentication ar	nd Security	
Authentication Type :	Open 802.1x Setting	
Encryption :	None	
WPA Preshared Key :		
г Wep Кеу		
€ Key#1 Hex		
C Key#2 Hex		
C Key#3 Hex		
C Key#4 Hex		
	OK Cancel Apply Help	

Figure 3-3 Profile Authentications and Security

Start RaConfig

When starting RaConfig and selecting "Use RaConfig (Without 802.1x support)" for the first time, system will connect to the AP with best signal strength and matching security setting. When starting RaConfig, it will issue a scan command to wireless NIC. After two seconds, the list will updated with the result of BSS list scan. The list include most used fields, such as SSID, signal percentage, channel used, encryption status, authentication mode, and network type. The green handshake icon indicates the connected BSS or IBSS network. The page is shown as figure 2-1.

				and Lincon	. 1	
SSID	BSSID	Signal	Channel	Encryption	Authentication	Network Type
SAP	00-0C-4	99%	5	Not Use	Unknown	Infrastructure
AP2500	00-0C-4	99%	1	Not Use	Unknown	Infrastructure
WAP11	00-06-25	99%	1	Not Use	Unknown	Infrastructure
NDTES	00-40-96	78%	6	WEP	VEP Unknown	
NDTES	00-0D-5	89%	6	WEP	Unknown	Infrastructure
Dell1184	00-90-4	78%	6	Not Use	Unknown	Infrastructure
default	00-90-96	81%	6	Not Use	Unknown	Infrastructure
BuffaloG	00-07-40	100%	11	AES-CC	WPA-PSK	Infrastructure
S 1/C28	00-04-E	100%	11	Not Use	Unknown	Infrastructure
<			im			
Connected <	> SMC2804 W	BR	<u>R</u> ESC.	AN C	ONNECT	ADD PROFILE

Figure 2-1 Fisrt page shown when starting RaConfig

At the mean time of starting RaConfig, there is also a small ralink icon appears within windows taskbar as figure 2-2. You may double click it to bring up the main menu if you selected to close RaConfig menu eariler. You may also use mouse's right button to close RaConfig utility. When RaConfig exits from the system, it will restore WZC to its initial state before starting RaConfig. For example, if WZC is stopped before RaConfig started. WZC will stay stopped after RaConfig terminated. If WZC is running before RaConfig started, it will be re-enabled after RaConfig exited.



Figure 2-2 Ralink icon

Besides, the small icon will change color to reflect current wireless network connection status. The status indicates as follow:

🙀: Indicate Connected and Signal Strength is Good.

🔥: Indicate Connected and Signal Strength is Normal.

- : Indicate Connected and Signal Strength is Weak.
- K: Indicated not connected yet.
- : Indicated wireless NIC not detected.

RaConfig or windows zero configuration

In windows XP, it provides wireless configuration utility named "windows zero configuration" which provides basic configuration function for RaLink wireless NIC. It also provides WPA support at hotfix Q815485 However; you have to make sure that hotfix Q815485 (require XP SP1 installed) has been installed in your system before you can start using WPA features. You can check the installation of hotfix in add/remove software page under control panel. The page is shown as Figure 1-1.

. Ba	Currently installed programs:	Show upgates	Sort by: Name	~
Change or Remove Programs	III Windows XP Hottix - KB824146 III Windows XP Hottix - KB825119			
Add New Programs	 Windows XP Hottix - KB828035 Windows XP Hottix (SP2) Q328310 Windows XP Hottix (SP2) Q329170 Windows XP Hottix (SP2) Q329441 			
Add/Remove Windows Components	Windows XP Hotfix (SP2) Q810565 Windows XP Hotfix (SP2) Q810577 Windows XP Hotfix (SP2) Q810833 Windows XP Hotfix (SP2) Q811493	👸 Windows XP Hotfix (S	P2) Q815485	
Set Program Access and	Windows XP Hotfix (SP2) Q814033 Windows XP Hotfix (SP2) Q815031 Windows XP Hotfix (SP2) Q815485			
Derauts	15) Windows XP Hottix (SP2) Q819696			

Figure 1-1 Windows XP Hotfix Q815485 installed

Currently, Ralink's utility (RaConfig) provides WPA-PSK supplicant's functionality. If user required WPA function. Please select <u>WZC</u> as main utility. To make it easier for user to select the correct utility. RaConfig will let user make the selection when it first ran after XP boot. Click



RaConfig.exe

the icon of will bring up the selection window and let user make the selection. It is shown as Figure 1-2.

RaConfig can co-exist with <u>WZC</u>. When coexisting with <u>WZC</u>, RaConfig only provides monitoring function, such as link status, site surveying, statistic counters and advance feature status. It won't interfere with WZC's configure or profile functions.



Figure 1-2 Select WZC or RaConfig

If "Use RaConfig (Without 802.1x support) " is selected, please jump to <u>section 2-2</u> on Running RaConfig.

If "Use XP Wireless Zero Configuration (Wi-Fi Protected Access(TM) support with additional patch from Microsoft)" is selected, please continue on the section. We will explain the difference between RaConfig and <u>WZC</u>. Figure 1-3 shows the RaConfig menu when WZC is active as main control utility.

SSID	BSSID	Sig	С	Enery	Authent	Network T
BuffaloG	00-07-40-76-D	83%	11	Not Use	Unknown	Infrashruct.
Ver27	0A-A4-FA-0B	78%	2	Not Use	Unknown	Ad Hoc
Testoox	00-30-F1-FF-22	10	1	Not Use	Unknown	Infrastruct.
AP25-Left	00-0C-43-25-61	10	6	Not Use	Unknown	Infrastruct.
wpa	00-E0-18-F4-44	10	6	AES	WPA-P	Infrastruct.
default	00-80-C8-03-32	10	6	WEP	Unknown	Infrastruct.
miffy	00-0C-43-25-61	10	6	TKIP	WPA-P	Infrastruct.
AP350	00-40-96-56-2A	10	6	WEP	Unknown	Infrastruct.
NDTESTAP1	00-40-96-41-93	10	6	WEP	Unknown	Infrastruct.
NDTESTAP2	00-40-96-54-B5	10	6	WEP	Unknown	Infrastruct.
Ralink_test	00-06-25-4A-75	10	6	Not Use	Unknown	Infrastruct. 🗸
<			- 2			
Connected kine's Bu	ffeloG		π []	CONN	ROT 1	DD BROELE

Figure 1-3 RaConfig menu with WZC active

When activates \underline{WZC} , there are couple difference on RaConfig menu compared to that without \underline{WZC} running.

• Missing Profile page, profile function is removed since the NIC is controlled by <u>WZC</u>.
2The connect and add profile function are removed from Site Survey Page. The reason is same as the first difference

A WLAN device operating according to Section 15.247 on Channels 1-11 between 2400-2483.5 MHz must not have any user controls or software to allow the device to operate on channels 12 and 13 which are outside of the allowed USA band. Therefore, the function of country code selection already be disable on the device.

The transmitter shall not be collocated with other transmitters or antennas.

This device is intended only for OEM integrators under the following conditions: 1)The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2)The transmitter module may not be co-located with any other transmitter or antenna. As long as the 2 conditioons above are met, further transmitter testing will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.)

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

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ASDL modems, and similar equipment). The final end product must be labeled in a visible area with the following: "Contains TX FCC ID:RC6AWI-922T".

The users manual for end users must include the following information in a prominent location "IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna 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."

The end user should NOT be provided any instructions on how to remove or install the device.

Excursus

The above setting is test platform by RaLink technology corp. User can set the function in accordance with A.P.

This device complies with Part 15 of the Fcc Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including. Interference that may cause undesired operation.

Acknowledgements:

"This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)". This product includes cryptographic software written by Eric Young (eay@cryptsoft .com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).