Enable Tx Burst: Ralink's proprietary frame burst mode.

Enable TCP Windows Size: Enhance throughout.

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

Select your Country Region Code: 8 countries to choose.

Show Authentication Status Dialog: When you connect AP with authentication, choose whether show "**Authentication Status Dialog**" or not. Authentication Status Dialog display the process about 802.11x Authentication.

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

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

Apply: Save the save changes

- ▼ → Show the information of Status Section
- Hide the information of Status Section

3.1.5 Statistics

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

[Transmit Statistics]

rames Transmitted Successfully	=	1432
rames Retransmitted Successfully	-	4
rames Fail To Receive ACK After All Retries	=	O
TS Frames Successfully Receive CTS	-	0
TS Frames Fail To Receive CTS	=	0

Frames Transmitted Successfully: Frames successfully sent.

Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit. **RTS Frames Successfully Receive CTS:** Successfully receive CTS after sending RTS frame.

RTS Frames Fail to Receive CTS: Fail to receive CTS after sending RTS frame.

Frames Retransmitted Successfully: Successfully retransmitted frames numbers

Reset Counter: Reset counters to zero

[Receive Statistics]

3153	=	uccessfully	Frames Received Su
201964	=	/ith CRC Error	Frames Received Wi
0	=	ue To Out-of-Resource	Frames Dropped Due
0	=	eceived	Duplicate Frames Re
	=	eceived)uplicate Frames Re

Reset Counter

Frames Received Successfully: Frames received successfully.

Frames Received With CRC Error: Frames receive with CRC error.

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

Duplicate Frames Received: Duplicate received frames.

Reset Counter: Reset counters to zero

▼ → Show the information of Status Section

▲ → Hide the information of Status Section

3.1.6 WMM

WMM function involves "WMM Enable", "WMM-Power Save Enable" and "DSL Setup".

WMM >> Enable	d Power	Save >> Disabled			Direct Link >> Disabled
WMM Enable					
WMM - Pow	ver Save Enable				
AC_B	вк 🔲 (AC_BE	AC_VI	AC_VO	
Direct Link	< Setup Enable				
MAC A	ddress >>		Timeout Value >>	60 sec	Apply
					Tear Down

WMM Enable: Enabe Wi-Fi Multi-Media.

WMM-Power Save Enable: Enable WMM Power Save.

Direct Link Setup Enable: Enable DLS (direct Link Setup).

[WMM Enable – Enable Wi-Fi Multi-Media]

If you want to use "WMM-Power Save" or "Direct Link Setup" you must enable WMM. The

setting methods of enabling WMM indicating as follow:

Step 1: Click "WMM Enable"

WMM >> Enabled	Power Save >> Disa	bled		Direct Link >> Disabled
WMM Enable				
WMM - Power Save	Enable			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup E	nable			
MAC Address >		Timeout Valu	e >> 60 sec	Apply

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

1 Ral	Л								×
(Profile	Lee Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	R	•
		Profile	e List						
PR	OF1	AP1		13		Profile Name	>> PROF1		
-				*		SSID	>> AP1		
						Network Type	>> Infrastructure		
						Authentication	i >> Open		
						Encryption	1 >> None		
						Use 802.1×	: >> NO		
						Channe	>> 1		
					Po	wer Save Mode	>> CAM		
						Ty Power	ss Auto		
						DTS Threshold	1 >> 2347		
					Fran	ment Threshold	122 2347		
-					Tidg	mone ninesnoie	177 2340		
-	Add	Edit	Delete	Activate	-				
	Status >	> AP1 <> 00-03-7F-	00-D7-A4			Lin	k Quality >> 100%		
	Extra Info >	> Link is Up [TxPowe	r:100%]						
	Channel >	> 6 <> 2437000 MH:	z			Signal	Strength 2 >> 100%		
AL	thentication >	> Open				Stignal	Strength 3 >> 100%		
	Encryption >	> NONE				Nois	e Strength >> 26%		
N	letwork Type >	> Infrastructure			Transmi	t	1144		4
	IP Address >	> 192.168.5.60			Link	< Speed >> 54.0) Mbps Max		
Def	suu mask >	> 192 168 5 254			Thro	ughput >> 0.00	0.002		
	ant datomay .	HT					Mbps		
			CNIDO se a la		Keceive	(Speed >> 54 (Max Max		
BV	l >> n/a	star ex 20M			Thro	ughput >> 0.00	33 Mbps		
9		1103 77 11/4	20121 22 1110				1.448 Mbps		
									1

[WMM-Power Save Enable – Enable WMM Power Save]

Step 1: Click "WMM-Power Save Enable"

	Fomer 24ve >> Disc			Direct Link >> Disabled
WMM Enable				
WMM - Power Save	Enable			
🔲 АС_ВК	AC_BE	AC_VI	AC_VO	
Direct Link Setup E	nable			
MAC Address >		Timeout Val	ue >> 60 sec	Apply
				Tear Down

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

WMM >> Enabled	Power Save >> Enab	led		Direct Link >> Disabled
WMM Enable				
WMM - Power Save E	nable			
С АС ВК	AC_BE	AC_VI	AC_VO	
Direct Link Setup Er	able			
MAC Address >>		Timeout Valu	ie >> 60 sec	Apply
				Tear Down

[Direct Link Setup Enable – Enable DLS (Direct Link Setup)]

Step 1: Click "Direct Link Setup Enable"

	Power Save >> Disable	ed		Direct Link >> Enabled
WMM Enable				
WMM - Power Save Enab	le			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Enable	9			
MAC Address >>		Timeout Value >>	60 sec	Apply
				Tear Down

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

Profil	e Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	R	0
	Profil	e List						
PROF1	AP1		5		Profile Name	>> PROF1		
					SSID)>> AP1		
					Network Type	>> Infrastructure		
					Authentication	n >> Open		
					Encryption	n >> None		
					Use 802.1x	< >> NO		
					Channel	>> 1		
				Po	wer Save Mode	9 >> CAM		
					Tx Power	<pre> / >> Auto </pre>		
					PTS Threshold	1 >> 2347		
					Kis micshold	177 2017		
				Erad	ment Threshold	1 23/6		
				Frag	ment Threshold	i >> 2346		
Add	Edit	Delete	Activate	Frag	ment Threshold	i >> 2346		
Add	Edit 15 >> AP1 <> 00-03-7F-	Delete 00-D7-A4	Activate	Frag	ment Threshold	1 >> 2346 k. Quality: >> 100%:		
Add Statu Extra Inf	Edit is >> AP1 <> 00-03-7F- o >> Link is Up (TxPowe	Delete 00-D7-A4 #1:100%]	Activate	Frag	ment Threshold Lin Signal	1 >> 2346 k Quality >> 100% I Strength 1 >> 100%		
Add Statu Extra Inf Chann	Edit is >> AP1 <> 00-03-7F- io >> Link is Up [T×Powe el >> 6 <> 2437000 MH	Delete 00-D7-A4 er: 100%] Iz	Activate	Frag	ment Threshold Lini Signal Signal	1 >> 2346 k Quality >> 100% Strength 1 >> 100% (Strength 2 >> 100%		
Add Statu Extra Inf Chann Authenticatio	Edit s>> AP1 <> 00-03-7F- o >> Link is Up [TxPowe al >> 6 <> 2437000 MH n >> Open	Delete 00-D7-A4 21:100% Iz	Activate	Frag	ment Threshold Lini Signai Signai Signai	 x> 2346 k: Quality: >> 100% Strength: 1 >> 100% Strength: 2 >> 100% Strength: 3 >> 100% 		
Add Statu Extra Ini Chann Authenticatio Encryptic	Edit s>> AP1 <> 00-03-7F- o >> Link is Up [TxPowe el >> 6 <> 2437000 MH n >> Open n >> NONE	Delete 00-D7-A4 er:100% Iz	Activate	Frag	ment Threshold Lini Signal Signal Nois	1 >> 2346 k Quality >> 100% Strength 1 >> 100% Strength 2 >> 100% Strength 3 >> 100% strength 3 >> 100%		
Add Statu Extra Inf Chann Authenticatio Encryptio Network Typ ID Addres	Edit s>> AP1 <> 00-03-7F- o >> Link is Up [TxPowe s) >> 6 <> 2437000 MH n >> Open n >> NONE e >> Infrastructure e >> 10frastructure	Delete 00-D7-A4 er:100%] Iz	Activate	Frag	ment Threshold Lim Signal Signal Signal Nois	<pre>1 >> 2346 k Quality >> 100% Strength 1 >> 100% Strength 2 >> 100% strength 3 >> 100% ise Strength >> 26%</pre>	× 1	
Add Statu Extra Inf Chann Authenticatio Encryptio Network Typ IP Addres Sub Mas	Edit is >> AP1 <> 00-03-7F- o >> Link is Up [TxPowe el >> 6 <> 2437000 MH n >> Open n >> NONE e >> Infrastructure is >> 192.168.5.60 k >> 255.255.255.0	Delete 00-D7-A4 rr:100%] Iz	Activate	Frag	Lin Signal Signal Nois t Speed >> 54.0	1 >> 2346 k Quality >> 100% Strength 1 >> 100% Strength 2 >> 100% Strength 3 >> 100% Strength 3 >> 100% Strength >> 26%		
Add Statu Extra Inf Chann Authenticatic Encryptic Network Typ IP Addres Sub Mas Default Gatewa	Edit s >> AP1 <> 00-03-7F- o >> Link is Up [TxPowe s >> 6 <> 2437000 MH n >> Open n >> NONE e >> Infrastructure s >> 192.168.5.60 k >> 255.255.0 y >> 192.168.5.254	Delete 00-D7-A4 rr:100%] Iz	Activate	Frag	Lini Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal Signal	5 >> 2346 k Quality >> 100% Strength 1 >> 100% Strength 2 >> 100% istrength 3 >> 100% istrength >> 26% 0 Mbps 0.00 0.00	× 12	
Add Statu Extra Inf Chann Authenticatio Encryptio Network Typ IP Addres Sub Mas Default Gatewa	Edit s >> AP1 <> 00-03-7F- o >> Link is Up [T×Powe s >> 6 <> 2437000 MH n >> Open n >> NONE e >> Infrastructure s >> 192.168.5.60 k >> 255.255.255.0 y >> 192.168.5.254 HT	Delete 00-07-A4 rr:100%] Iz	Activate	Frag Transmi Lini Thro	ment Threshold Lini Signal Signal Signal Nois t t Speed >> 54.0 ughput >> 0.00	f >> 2346 k Quality >> 100% (Strength 1 >> 100%) (Strength 2 >> 100%) (Strength 3 >> 100%) (Strength >> 26%) (Mbps	×)2 s	
Add Statu Extra Ini Chann Authenticatio Encryptio Network Typ IP Addres Sub Mas Default Gatewa	Edit s >> AP1 <> 00-03-7F- io >> Link is Up [TxPowe el >> 6 <> 2437000 MH n >> Open n >> NONE e >> Infrastructure ss >> 192.168.5.60 k >> 255.255.255.0 y >> 192.168.5.254 HT	Delete 00-D7-A4 07:100% 1z	Activate	Frag Transmi Lini Thro Receive Lini	Lini Signal Signal Signal Signal Nois t (Speed >> 54.0 (ughput >> 0.00) (Speed >> 54.5	1 >> 2346 k Quality >> 100% Strength 1 >> 100% Strength 2 >> 100% ist rength 3 >> 100% ist strength >> 26% D Mbps D Mbps D Mbps D Mbps Max D Mbps Max	× 12 12 14 14 14 14 14 14 14 14 14 14	

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 2

conditions as follow:

- → Connect with the same AP that support DLS features.
- → Have to enable DLS

WMM Enable WMM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WMM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM Enable				
AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM - Power Save Ena	ble			
MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	AC_BK	AC_BE	AC_VI	AC_VO	
MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	Direct Link Setup Enab	le			
	MAC Address >>	0 0c 43 28 60 00	Timeout Value >>	600 sec	Apply
Tear Down					Tear Down

(2) Timeout Value represent 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.

WMM Enable				
a contraction of the second				
WMM - Power Save	Enable			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup E	inable			
MAC Address >	> 00 0c 43 28 60 0	0 Timeout Value	>> 600 sec	Apply
				Tear Down

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

WMM Enable				
WMM - Power Save	Enable			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup E	nable			
MAC Address >	> 00 0c 43 28 60 0	0 Timeout Value >>	600 sec	Apply
	00-0C-43-28-60-00		600	Tear Down

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 itself and Timeout Value of setting.
- (2) Display the values of "DLS Status" to "Direct Link Setup" as follow:

Step 1: In "DLS Status", select a direct link STA what you want to show its values in "Direct Link Setup".

WMM >> Enabled	Power Save >> Disabled	1		Direct Link >> Enabled
WMM Enable				
WMM - Power Save	Enable			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup E	Enable			
MAC Address >	» [[[[[[[[[[[[[[[[[[[Timeout Value	>> 60 sec	Apply
	00-0C-43-28-60-00		600	Tear Down

Step 2: Double-Click and the result will look like the below figure.

WMM >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WMM Enable				
WMM - Power Save Ena	able			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Enab	ble		-	
MAC Address >>	00 0c 43 28 60 00	Timeout Value >>	600 sec	Apply
	00-0C-43-28-60-00		600	Tear Down

(3) Disconnect Direct Link Setup as follow:

Step 1: Select a direct link STA.

WMM Enable WMM - Power Save Enable AC_BK AC_BE AC_DIrect Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WMM - Power Save Enable AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM Enable				
AC_BK AC_BE AC_VI AC_VO Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	WMM - Power Save E	nable			
Direct Link Setup Enable MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	AC_BK	AC_BE	AC_VI	AC_VO	
MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply	Direct Link Setup En	able			
	MAC Address >>	00 Oc 43 28 60 00	Timeout Value >>	600 sec	Apply
UU-UU-43-28-60-00 000 Tear Down		00-0C-43-28-60-00		600	Tear Down

WMM >> Enabled	Power Save >> Disabled			Direct Link >> Enabled
WMM Enable				
WMM - Power Save E	nable			
AC_BK	AC_BE	AC_VI	AC_VO	
Direct Link Setup Er	able			
MAC Address >>	00 0c 43 28 60 00	Timeout Value >	> 600 sec	Apply
				Tear Down

3.1.7 WPS

1 Ral	JI								
4	Profile	Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	R About	
-	6			WPS AP	List				
							10.000	Rescan	
							Int	formation	
							6002	1670 Renew	
			10/P	S Profile List			Conf	ia Mode	
							Enro	llee 💌	
								Detail	
								Connect	
							-	Rotate	
							Di	sconnect	
	PIN	WPS Asso	ociate IE		Progress >>	0%	Exp	ort Profile	
	P <u>B</u> C	WPS Prot	be IE				in the	Delete	
	Status >> I	Default_11G <> 0	0-06-4F-44-CB-F0			Link	Quality >> 100%		
	Extra Info >>	Link is Up [TxPowe	r:100%]			Si <mark>gnal</mark>	Strength 1 >> 32%		
	Channel >> (6 <> 2437 MHz				Signal	Strength 2 <mark>>> 60%</mark>		
Au	thentication >> I	Unknown				Noise	Strength >> 26%		
0.00	Encryption >> I	None							
N	letwork Type >>	Infrastructure			Transmit	t			15
	IP Address >>	192.168.10.21			Link	Speed >> 48.0	Mbps Max		8
Defa	Sub Mask >> : ault Gateway >>	255.255.255.0 192.168.10.1			Throu	ughput >> 0.480) Kbps 1.472	2	
		нт					Kbps		
DW			CNIDO se a la		Receive Link	Speed >> 11.0	Max Max	dans 14	
G	>> n/a	MCS >> n/a	SNR1 >> n/a		Thro	ughput >> 6.788	3 Kbps 7.540 Kbps		

WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simply the security setup and management of Wi-Fi networks. Ralink STA as an Enrollee

41

or external Registrar supports the configuration setup using PIN configuration method or PBC configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS AP List: Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled. **Rescan:** Issue a rescan command to wireless NIC to update information on surrounding wireless network.

Information: Display the information about WPS IE on the selected network. List Information includes Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.

PIN Code: 8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each NIC Wireless has only one PIN Code of Enrollee.

Config Mode: Our station role-playing as an Enrollee or an external Registrar.

WPS Profile List: Display all of credentials got from the Registrar. List information includes SSID, MAC address, Authentication and Encryption Type. If STA Enrollee, credentials are created as soon as each WPS success. If STA Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.

Control items on WPS Profile List:

- → Detail: Information about Security and Key in the credential
- → Connect: Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
- → Rotate: Command to rotate to connect to the next inside credentials

→ Disconnect: Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.

→ Delete: Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.

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

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

★ When you click PIN or PBC, please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart PIN/PBC or press Disconnect to stop WPS connection.

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

WPS probe IE: Send the probe request with WPS IE during WPS setup. IT is optional for STA. **Progress Bar:** Display rate of progress from Start to Connected status.

Status Bar: Display currently WPS Status.

[WPS Information on AP]

WPS information contain authentication type, encryption type, config methods, device password ID, selected registrar, state, version, AP setup locked, UUID-E and RF bands.

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

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

Profile	Network	Advanced	Statistics	WAWA	WPS	Radio On/Off	R About	1
rted by >> 🧿	SSID	🥥 Channe	el 🥝) Signal t >>		Show dBm		
132		1 /2	B9	100%				
202		101	Ъg	70%				
213		11	Bg 🕈	29%				
215		106	Ъg	44%				
219		101	B9 7	81%				
243		1 /25	Bg e	100% 💼				
_Shiang_2860AP		11	B9n	91%				
AP		101	bg 9	50% 💼				
AP1		16	Bgn	100%				
APPA		1 /26	13 g 🖻	91%				
General	WPS	ridi to prome	cx	802.11n	_			
	thentication Typ	e >> Unknown			SI	tate >> Unknown		
Aut								
Aut	Encryption Type	e >> None			Ver	sion >> Unknown		
huA	Encryption Type	e >> None s >> Unknown			Ver AP Setup Loc	sion >> Unknown :ked >> Unknown		
Aut	Encryption Type Config Method	e >> None s >> Unknown			Ver AP Setup Loc	sion >> Unknown :ked >> Unknown		
Aut	Encryption Typ Config Method wice Password II	e >> None s >> Unknown) >>			Ver AP Setup Loc UU	sion >> Unknown :ked >> Unknown ID-E >> Unknown		
Aut De S	Encryption Typ Config Method avice Password II elected Registra	e >> None s >> Unknown) >> r >> Unknown			Ver AP Setup Loc UU RF Ba	sion >> Unknown Hed >> Unknown ID-E >> Unknown ands >> Unknown		
Aut De S	Encryption Typ Config Method avice Password II alected Registra	e >> None s >> Unknown) >> r >> Unknown			Ver AP Setup Loc UU RF Ba	sion >> Unknown :ked >> Unknown ID-E >> Unknown ands >> Unknown		

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

Value	Hardware Interface
0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label
0x0008	Display
0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	Push Button
0x0100	Keypad

Device Password ID: Indicate the method or identifies the specific password that the selected Registrar intends to use. AP 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

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

State: The current configuration state on AP. The value are "Unconfigured" and "Configured". **Version:** WPS specified version.

AP Setup Locked: Indicate if AP has entered a setup locked state.

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

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

3.1.8 About

About function display the wireless card and driver version information.

(c) Copyright 2007, Ralink Technology, Inc.	All rights reserved.
RaConfig Version >> 2.0.3.0	Date >> 08-02-2007
Driver Version >> 1.0.4.0	Date >> 07-28-2007
EEPROM Version >> 134.0	
Firmware Version >> 0.4	
Phy_Address >> 00-06-4F-55-88-77	
WWW.RAL	INKTECH.COM

- (1) Connect to Ralink's Website: WWW.RALINKTECH.COM
- (2) Display Configuration Utility, Driver, and EEPROM version information
- (3) Display Wireless NIC MAC Address.

3.1.9 Link Status

Link Status displays the detail information current connection

Status	>> Default_11G <> (00-06-4F-44-CB-F0	Link Quality >> 92%
Extra Info	Extra Info >> Link is Up [TxPower:100%]		Signal Strength 1 >> 41%
Channel	>> 6 <> 2437 MHz		Signal Strength 2 >> 50%
Authentication	>> Unknown		Noise Strength >> 26%
Encryption	>> None		
Network Type	>> Infrastructure		Transmit
IP Address	>> 192.168.10.21		Link Speed >> 48.0 Mbps
Sub Mask	>> 255.255.255.0		Throughput >> 2,320 Kbps
efault Gateway	>> 192.168.10.1		3.152 Khos
	HT		Receive
BW >> n/a		SNRO >> n/a	Link Speed >> 11.0 Mbps Max Max
Gl >> n/a	MCS >> n/a	SNR1 >> n/a	Throughput >> 7.420 Kbps 9.808 Khos

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

Extra Info: Display link status in use.

Channel: Display current channel in use.

Authentication: Authentication mode in use.

Encryption: Encryption type in use.

Network Type: Network type in use.

IP Address: IP address about current connection.

Sub Mask: Sub Mast about current connection.

Default Gateway: Default gateway about current connection.

Link Speed: Show current transmit rate and receive rate.

Throughout: Display transmits and receive throughput in unit of Mbps.

Link Quality: Display Connection quality based on signal strength and Tx/Rx packet error rate.

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

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

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

Noise Strength: Display noise signal strength.

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

3.1.10 Enable AP Mode Feature in Windows 2000 OS

In Windows 2000 Operation System, the local network won't be automatically established while using Wireless PCI adapter's AP mode. Please follow the below steps to enable Internet Connection Sharing feature first before you switch Wireless PCI adapter's AP mode.

Step 1: After the Wireless PCI Adapter is installed properly in Windows 2000 Operation System, go to **Start** \rightarrow **Settings** \rightarrow **Control Panel** \rightarrow **Choose** "Network and Dial-up **Connections**" option. Right-Click your local area connection (such as another LAN Card in the same computer), and choose "**Properties**".

🔁 Network and Dial-up Connection	15		٦×
File Edit View Favorites Tools	Advanced H	telp	
🖙 Back 🔹 🔿 👻 🔂 🥘 Search	🔁 Folders 🛛 🍏	📽 📽 🗙 🕥 🏢•	
Address 🔁 Network and Dial-up Conn	ections	. €	Go
	F Make New	Local Area	
Network and Dial-up Connections	Connection	Connection Connection 2 Disable Status	
Local Area Connection Type: LAN Connection		Create <u>S</u> hortcut Delete Rena <u>m</u> e	
SiS 900-Based PCI Fast Ethernet Adapter		P <u>r</u> operties)
Displays the properties of the selecte	ed connection.		

Step 2: In Sharing tab, enable Internet Connection Sharing for this connection and click "OK"

Local Area Connection Properties	? ×
General Sharing	
Lange Internet Connection Sharing allows other computers on local network to access external resources through this connection.	your
Internet Connection Sharing	
Local network operation may be momentarily disrupted.	
Enable Internet Connection Sharing for this connection	
Settings	-1
OK Car	

Step 3: Back to Network and Dial-up Connection screen, right-click "Local Area Connection2" (for 802.11n Wireless LAN card) and choose "Properties".

🔁 Network and Dial-up Connection	5			<u> </u>
File Edit View Favorites Tools	Advanced	Help		1
🔃 Back 🔹 🔿 👻 🔂 🎯 Search	🔁 Folders 🛛 🔮) 🕆 🕆 🗡	(M III+	
Address 📴 Network and Dial-up Conne	ections		•	∂Go
	æ	e	քե լ է դ	
Network and Dial-up	Make New Connection	Local Area Connection	Local Area Connection 2	
Connections	connoction	Connection	Disa <u>b</u> le	
			Stat <u>u</u> s	
Local Area Connection 2			Create <u>S</u> ho	rtcut
Type: LAN Connection			Delete	
Status: Enabled		-	Rena <u>m</u> e	
		(P <u>r</u> operties	
802.11n USB Wireless LAN Card				
Displays the properties of the selecte	d connection.			//.

Step 4: Select "**Internet Protocol (TCP/IP)**" and click "**Properties**". You will see 802.11n Wireless PCI adapter will be automatically assigned an IP address as Access Point.

Local Area Connection 2 Properties		
General Sharing	Internet Protocol (TCP/IP) Properties	? ×
Connect using:	General	
802.11n USB Wireless LAN Card	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	
Components checked are used by this connection:	O Obtain an IP address automatically	
Client for Microsoft Networks	Use the following IP address	
✓ ➡ File and Printer Sharing for Microsoft Networks ✓ ▲ EGIS Protocol (IEEE 802.1x) v3.5.3.0	IP address: 192.168.0.1	
Internet Protocol (TCP/IP)	Subnet mask: 255 . 255 . 255 . 0	
Install Uninstall	Default gateway:	
Description	C Obtain DNS server address automatically	2
Transmission Control Protocol/Internet Protocol. The default	Use the following DNS server addresses:	
across diverse interconnected networks.	Preferred DNS server	
Show icon in taskbar when connected	Alternate DNS server:	
OK Cancel	Advanced	
	OK Cance	el 🛛

Step 5: In the System tray, now you can switch 802.11n Wireless PCI Adapter to AP Mode.



Step 6: After switch to AP mode, Ralink Wireless Utility will automatically pup-up. The Wireless Default SSID is assigned as "**SoftAP-2C**".

🔏 Ralink Wireless Utility	×
Config Access Control Mac Table Event Lo	g Statistics About
SSID SoftAP-20	Channel 1
Wireless Mode 802.11 B/G/N mix 💌	<- Use Mac Address Security Setting
Country Region Code 11 B/G 0: CH1-11	No forwarding among wireless clients Hide SSID Allow BW 40 MHz
Beacon (ms) 100]
TX Power 100 %]
Idle time(60 - 3600)(s) 300	
	Default Apply
	Help

Step 7: To make sure your Soft AP is working properly, you need to use another computer which with Wireless LAN feature to access SoftAP-2C AP. In the below example, use another PC with Wireless feature in Vista Operation System. Go to Start \rightarrow Control Panel \rightarrow Choose "Network and Sharing Center" option \rightarrow Click "Connect to a network" to search the available networks.

Control Panel +	Network and Sharing Center - + Search	Q
Tasks View computers and devices	Network and Sharing Center	0
Connect to a network Manage wireless networks Set up a connection or network Manage network connections Diagnose and renair	WINNIE-PC (This computer)	View full map
See also Internet Options Windows Firewall	Wireless networks are available.	

Show All	•	4
WLAN_SW	Security-enabled network	llee
SoftAP-2C	Unsecured network	llee.
112233	Unsecured network	llee.
		-1

Step 8: Select the network "SoftAP-2C" and click "Connect" to establish the connection.

Step 9: After the computer is successful connected to SoftAP-2C, Network and Sharing Center screen will be shown as below. Click "**View Status**" to see the detail.

🔾 🗢 👯 🕨 Control Panel 🕨	Network and Sharing Center	✓ ⁴ y Search	
Tasks View computers and devices	Network and Sharing Co	enter	View full map
Connect to a network Manage wireless networks Set up a connection or network Manage network connections	WINNIE-PC (This computer	SoftAP-2C	Internet
Diagnose and repair	-		
	SoftAP-2C (Public networ	k)	Customiz
	Access	Local only	
	Connection	Wireless Network Connection (SoftAP-2C)	<u>View statu</u> Disconnec
	3 Sharing and Discovery		
111111	Network discovery	© Off	
1110 11	File sharing	● Off	
	Public folder sharing	● Off	
	Printer sharing	Off (no printers installed)	
	Password protected sharing	• On	
See also	Media sharing	© Off	
Internet Options	Show me all the files and folde	rs I am sharing	
	Show me all the chared networ	k folders on this computer	

Step 10: In General tab, click "**Detail...**", and then you can see the current Network connection details. If this computer is successful connect to SoftAP-2C Access Point, the DHCP server will be assigned to same IP address.



3.2 For Windows Vista

Ralink wireless utility is shown as below. There are 6 settings pages in Ralink wireless utility:

SSID	BSSID	Phy	Signal	🔺 C	Encryption	Authentic	Network Ty
Belkin_N1	00-17-3F-5A-8E-AD	N	76%	1	None	Unknown	Infrastructur
mony_test	00-06-4F-5B-13-2F	N	96%	3	None	Unknown	Infrastructur
Default_WL	00-06-4F-43-CF-8F	G	55%	6	None	Unknown	Infrastructur
Default_11N	00-06-4F-33-44-66	N	20%	6	None	Unknown	Infrastructur
WLAN_SW	00-07-40-F1-99-42	G	100%	9	TKIP	WPA-PSK	Infrastructur
MISO	00-06-4F-1F-34-A6	G	86%	10	None	Unknown	Infrastructur
mySSID	00-03-7F-FE-00-02	G	96%	11	None	Unknown	Infrastructur
•			111				

- Profile Page: Manage the profile.
- Link Status Page: Display current connection information.
- Site Survey Page: Display the available networks.
- Statistics Page: Display the packet counters
- **WPS Configuration** Page: Connect to WPS (Wi-Fi Protected Setup) capable APs.
- QoS Page: It involves "WMM Enable", "WMM Power Save Enable" and DLS setup
- About Page: Display Ralink driver and utility information.

3.2.1 Profile

In the "**Profile**", you can view and manage the current using Available Point(s). You can **Add**, **Delete**, **Edit**, or **Activate** the current Available Point(s). Also you can duplicate the AP or set current AP as Default.

Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure

Profiles Name: The Profiles List displays all the profiles and the relative settings of the profiles including Profile Name, SSID, and Channel...etc; preset to **PROF*** (* indicate 1,2,3,...) **SSID:** AP to Ad-hoc name.

Channel: Channel in use for Ad-Hoc mode.

Authentication: Authentication mode.

Encryption: Security algorithm in use.

Network Type: Network's type, including Infrastructure and Ad-hoc.

Indicate connection is successful on currently activated profile.

Indicate connection is failed on currently activate profile.

Add/Delete/Edit Button: Click these buttons to add/delete/edit the selected profiles.

Activate Button: Click "Activate" to connect the selected profile. When a profile is activated, the adapter will be initially connected to the profile.

n filo Lint					
Profile Name	SSID	Channel	Authentication	Encomtion	Network Type
Tonie Manie	1.0010	Channer	Admentication	Пакурион	Network Type
Add		Delete	E	dit	Activate

By either pushing the "Add" button on Profile Page or the "Add to Profile" button on Site Survey Page, it brings up the profile setting sheet which contains two setting pages --"Configuration" page and "Authentication and Security" page.

SSID	BSSID	Phy	Signal	▲ C	Encryption	Authentic	Network Ty
Belkin_N1	00-17-3F-5A-8E-AD	N	76%	1	None	Unknown	Infrastructur
morry_test	00-06-4F-5B-13-2F	N	96%	3	None	Unknown	Infrastructur
Default_WL	00-06-4F-43-CF-8F	G	55%	6	None	Unknown	Infrastructur
Default 11N	00-06-4E-33-44-66	N	20%	6	None	Unknown	Infrastructur
WLAN_SW	00-07-40-F1-99-42	G	100%	9	TKIP	WPA-PSK	Infrastructur
MISO	00-06-4F-1F-34-A6	G	86%	10	None	Unknown	Infrastructur
mySSID	00-03-7F-FE-00-02	G	96%	11	None	Unknown	Infrastructur
٠ [III.				+
P				Deserve	- (1	A-1 D6	

3.2.1.1 Add a profile

[Configuration page]

Add Profile				<u> </u>
Configuration Auth	entication and Security			
Profile Name	PROF1	SSID	WLAN_SW	-
Network Type	Infrastructure	TX Power	Auto	•
	ок	Cancel		Help

- Profile Name: Name of the profile
- SSID: Name of the desire network
- Network Type: Netowork of the desired network, either infrastructure or Ad-Hoc. Infrastructure – This operation mode requires the presence of a wireless Access Point. All communication is done via the Access Point or Router.

Ad-Hoc – Select this mode if you want to connect to another wireless station in the Wireless LAN network without through an Access Point or Router.

Tx-Power: The desired TX power level; the available options are 100%, 75%, 50% and Auto. If you want to lower the transmit power of the adapter for saving the power of the system, you can select the lower percentages from the list. The lower power will cause the lower signal strength and the coverage range.

onfiguration Authentication	and Security	
Authentication Type :	WPA-PSK	
Encryption :	ТКІР	
WPA Preshared Key :		
C Wep Key-		
€ Key#1 Hex	<u></u>	
C Key#2 Hex	<u> </u>	
C Key#3 Hex	<u></u>	
C Key#4 Hex	y	
* WEP 64 Bits Encryptic * WEP 128 Bits Encrypt	n: Please Keyin 10 HEX characters or 5 ion: Please Keyin 26 HEX characters or "	ASCII characters 13 ASCII characters
		Show Passward

[Authentication and Security page]

Authentication Type: The authentication of the desired network. For infrastructure network, the available modes are Open, Shared, WPA, WPA-PSK, WPA2, and WPA2-PSK.

Open: No authentication is needed among the wireless devices.

Shared: Only Wireless device using a shared key (WEP Key identified) is allowed to connecting each other. Setup the same key as the wireless device that the adapter intends to connect.

WPA: WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprise, small business and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

WPA-PSK – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

WPA2 – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The different between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

WPA2-PSK – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).

Encryption: The encryption of the desired network.

- -- For Open and Shared authentications, the available encryption modes are **None** and **WEP.**
- -- For WPA, WPA-PSK, WPA2 and WPA2-PSK authentications, the available modes are **TKIP** and **AES**.

None – Disable the Encryption mode.

WEP – Enabled the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Key Length & the key Index.

TKIP – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10000 packets (a packet is a kind of message transmitted over a network). This insures much greater security than the standard WEP security.

AES – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

Note: All devices in the network should use the same encryption method to ensure the communication.

- WPA Pre-Shared Key: The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
- WEP Key (Key1~Key4): The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit & 128-bit. Select the default encryption key form key1 to key4 by selected the radio button.

Fill the text box by following the rule below:

64-bit – Input 10-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 5-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**0123456aef**" or "**test1**"

128-bit – Input 26-digit Hex values (in the "**A-F**", "**a-f**, and "**0-9**" range) or 13-digit ASCII characters (including "**a-z**" and "**0-9**") as the encryption keys. For example: "**01234567890123456789abcdef**" or "**administrator**".

3.2.1.2 Edit a profile

Selecting an exiting profile then clicking the "**Edit**" button on Profile Page brings up the profile setting sheet filled with the profile information for user modification.

Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure

3.2.1.3 Delete a profile

Selecting an exiting profile then clicking the "Delete" button on Profile Page to deletes the profile.

Profile Link Statu	Utility s Site Survey Sta	tistics WPS (Configuration QoS	About		x
Profile List —						
Profile Name	e SSID	Channel	Authentication	Encryption	Network Type	
PROF1	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure	
A	dd 🗌	Delete	Б	dit	Activate	
					OK Help	

3.2.1.4 Active a profile

Selecting an exiting profile then clicking the "Active" button on Profile Page activates the profile.

Link Status Site Survey Statistics WPS Configuration QoS About Profile List					
Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN_SW	Auto	WPA-PSK	TKIP	Infrastructure
-					
4			<i></i>	~	
Add		Delete	E	dit	Activate
					or 1

3.2.2 Link Status

In this section, you can immediately monitor the current connected link status, such as Link Speed, Throughput, Link Quality, Signal Strength, Noise Level ...etc.

Ralink Wireless Utility						X
Profile Link Status Site Sur	vey Statistic	s WPS Config	uration	QoS About		
Status :	WLAN_SW	/ <> 00-07-40-F	1-99-42			-
Extra Info :	, Link is Up [TxPower:100%]				
Channel :	9 <> 2452	KHz				-
Link Speed :	Tx (Mbps)		54.0	Rx (Mbps)	54.0	
Throughput :	Tx (Kbps)		0.0	Rx (Kbps)	7.3	
Link Quality :	Good	100%				
	Good	100%			☐ dBm	
Signal Strength 1:						
Signal Strength 2	Good	100%				
	Low	26%				-
Noise Level :						
HT BW:n/a	Gl: n/a	MCS: n/a	E'	SNR0: n/a	SNR1:n/a	
					ОК	Help

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

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

Channel: Display the number of the radio channel and the frequency used for the networking. **Link Speed (Mbps):** Display the transmission and reception rate of the network. The maximum transmission rate is 54Mbps.

Throughput (Kbits/sec): Display transmits and receives throughout in unit of K bits/sec.

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

dBm: If you want to know the signal strength in the unit of dBm, select the check box.

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

Signal Strength2: Receive signal strength 2, user can choose to display as percentage or dBm format.

Noise Level: Display the noise signal strength.

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

3.2.3 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless device with the highest signal strength. From the **"Site Survey"**, all the network nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.

SSID	BSSID	Phy	Signal	🔺 C	Encryption	Authentic	Network Ty
morry_test	00-06-4F-5B-13-2F	N	91%	3	None	Unknown	Infrastructur
Default_11N	00-06-4F-33-44-66	N	15%	6	None	Unknown	Infrastructur
Default_WL	00-06-4F-49-C2-BB	G	55%	6	None	Unknown	Infrastructur
WLAN_SW	00-07-40-F1-99-42	G	100%	9	TKIP	WPA-PSK	Infrastructur
MISO	00-06-4F-1F-34-A6	G	91%	10	WEP	Unknown	Infrastructur
Belkin_N1	00-17-3F-5A-8E-AD	N	70%	11	None	Unknown	Infrastructur
3ComNokia	00-14-7C-BB-E0-1A	G	15%	11	None	Unknown	Infrastructur
myssid	00-03-7F-FE-00-02	G	34%	11	Ivone	Unknown	Infrastructur
			III.				

SSID: Name of BBS of IBSS network.

BSSID: MAC address of AP or randomly generated of IBSS.

Signal: Receive signal strength of specified network.

Channel: Channel in use.

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

Authentication: Authentication mode used within then network, including Unknown,

WPA-PSK, WPA2-PSK, WPA and WPA2.

Network Type: Network type in use, Infrastructure or Ad-Hoc.

Rescan: Issue an rescan command to wireless NIC to update information on surrounding wireless network.

Re-Scanning: Clicking the re-scan button to perform the re-scanning action.

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

[Connect A Network]

(1) When Raconfig first ran, it will select the best AP to connect automatically.

(2) 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.

This icon indicates the changes is successful.

⊙Example 1: Open and Non-Encrypted

Step 1 - Choose "Open" authentication type

Step 2 – Choose "None" encryption type

Authentication Type :	Open	✓ Use 802. ⁻	x	
Encryption :	None			•
WPA Preshared Key :				
- Wep Key				_
€ Key#1 Hex	<u></u>			
C Key#2 Hex	<u> </u>			
C Key#3 Hex	<u> </u>			
C Key#4 Hex	<u> </u>			
* WEP 64 Bits Encrypt * WEP 128 Bits Encryp	on: Please Keyin 10 H ition: Please Keyin 26	HEX characters or 5 HEX characters or 1	ASCII characters 3 ASCII characte	:rs

Step 3 – After the profile is saved, click "**Activate**" button on Profile Page to activate the profile.

Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	WLAN SW	Auto	WPA-PSK	TKIP	Infrastructure
PROF2	Default_11N	Auto	Open	None	Infrastructure
Add		Delete		Edit	Activate

• Example 2: WEP-Encrypted

Step 1 – Choose "Open" or "Shared" authentication type

Step 2 – Choose "WEP" encryption type

Step 3 –Enter the WEP KEY

uthentication Type :	Open 🗾 🗖 Use 802.1x
ncryption :	WEP
VPA Preshared Key :	
Wep Key	
	-
⊂ Key#2 Hex	_
⊂ Key#3 Hex	•
⊂ Key#4 Hex	•
* WEP 64 Bits Encrypt * WEP 128 Bits Encryp	on: Please Keyin 10 HEX characters or 5 ASCII characters tion: Please Keyin 26 HEX characters or 13 ASCII characters
	C Show Password