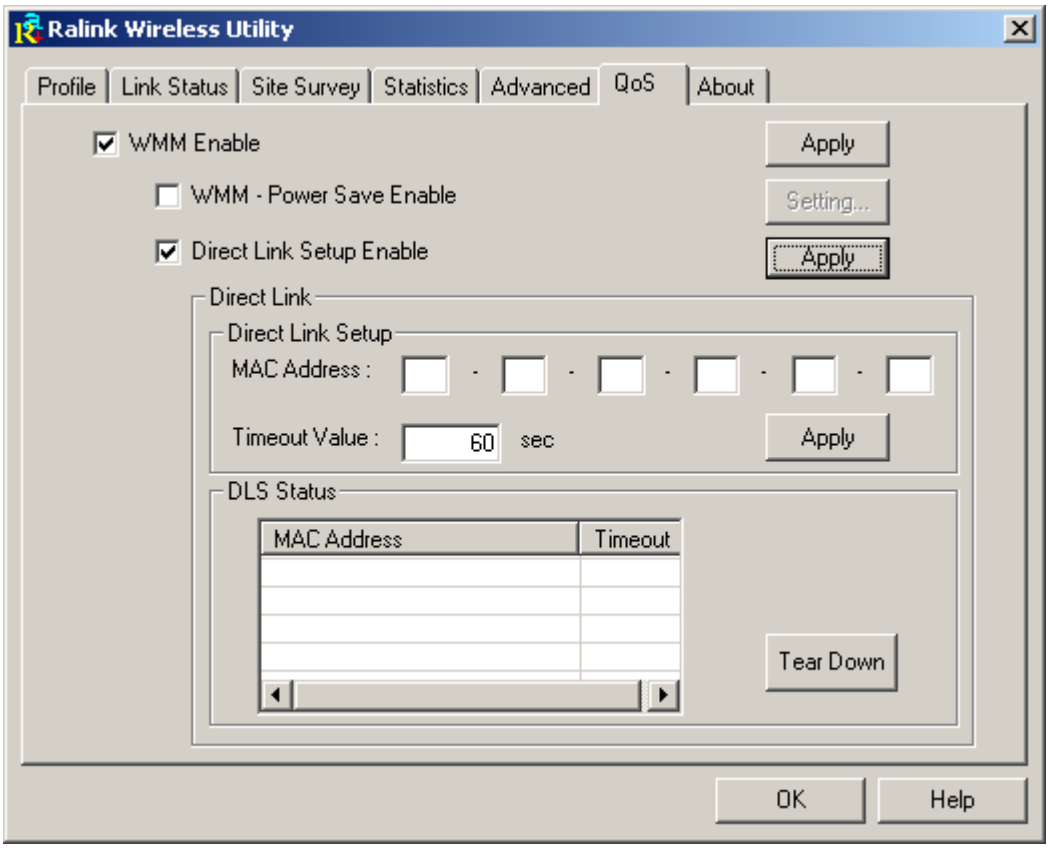
RaConfig Operation Manual

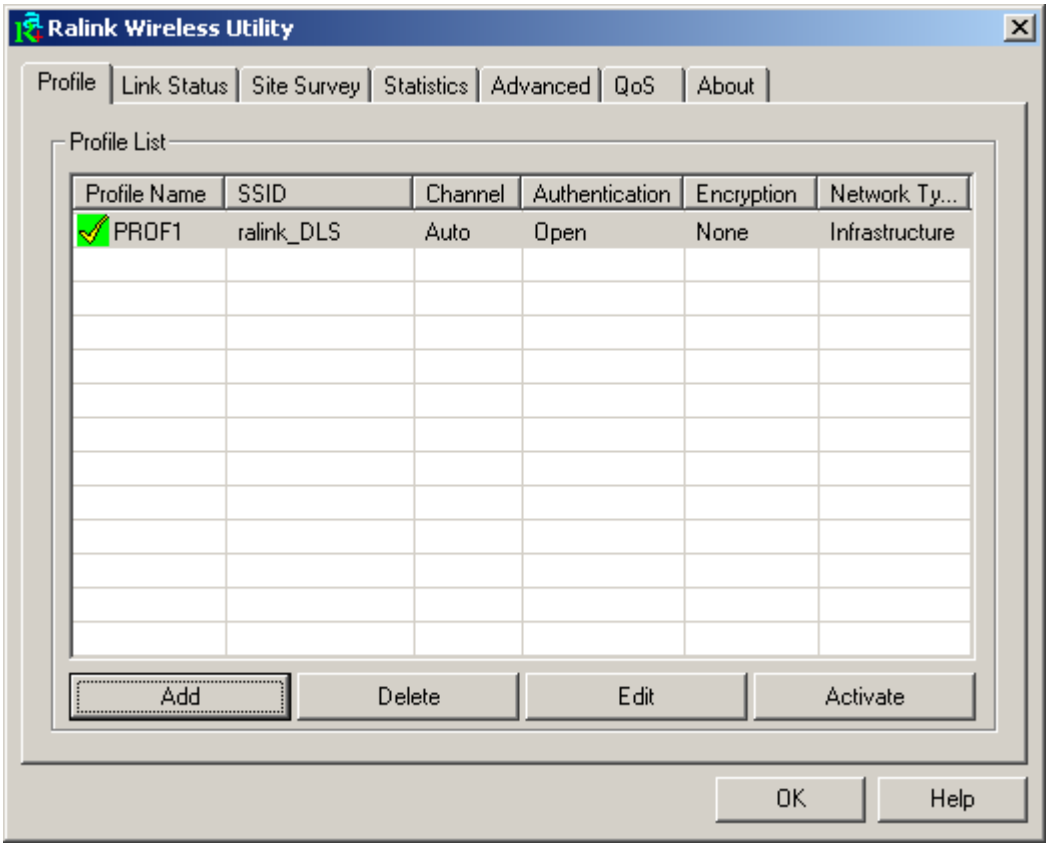
RaConfig or windows zero configuration
Start RaConfig Utility
Site Survey Page
Encryption Setting [WEP/TKIP/AES]
802.1X Authentication
CA Server Setting
Profile Page
Link Status Page
Statistic Page
Advance Page
Country Channel List
QoS Page
About Page
Example on adding profile in site survey page
Example 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.



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.

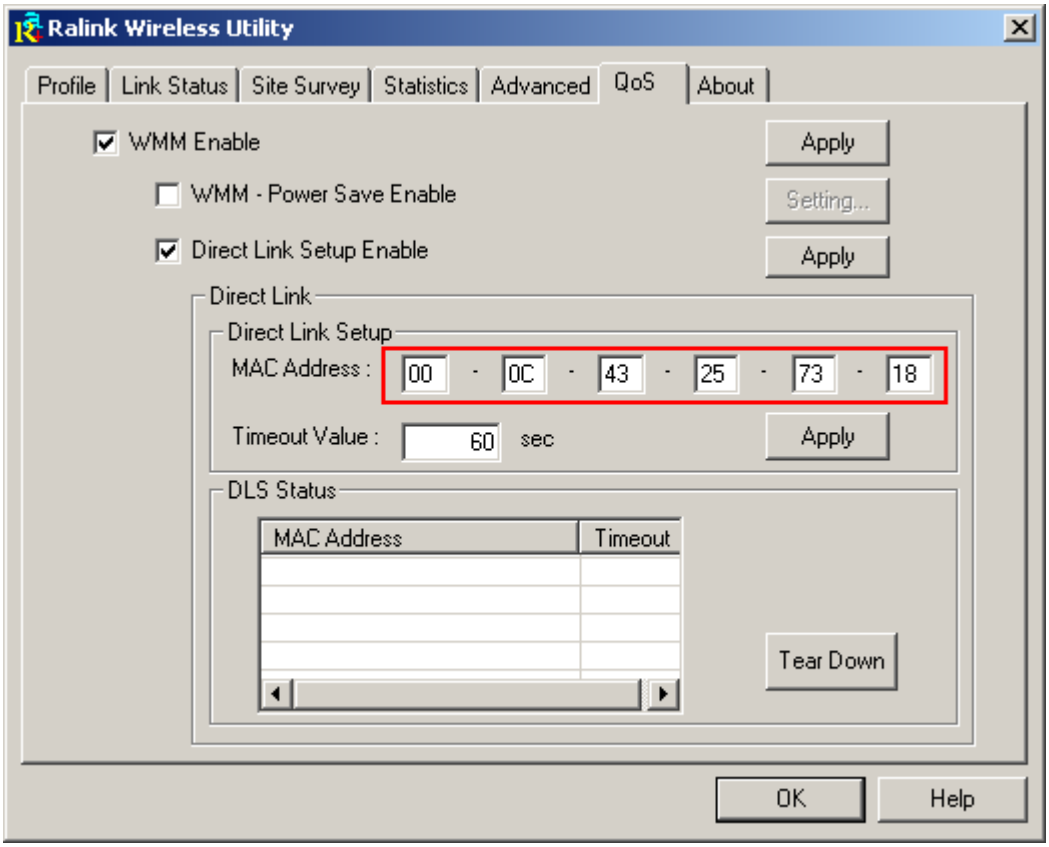


The setting of DLS indicates as follow:

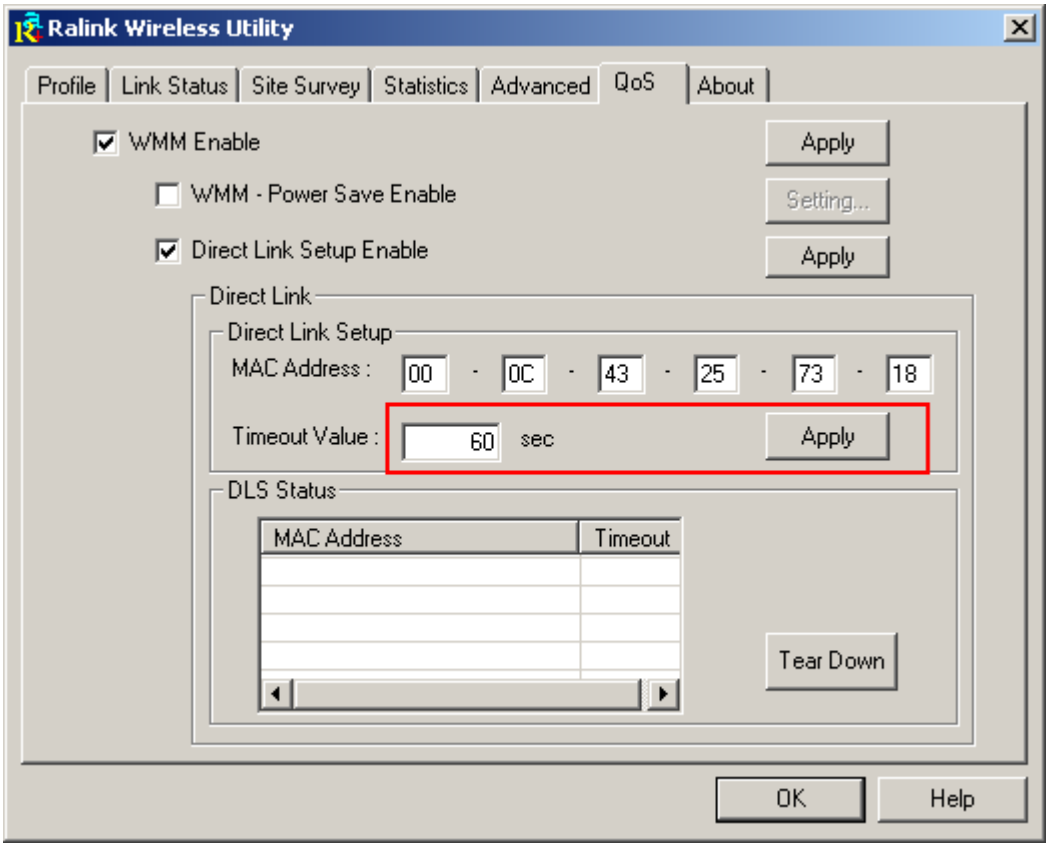
1. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to two conditions as follow:

   Connect with the same AP that support DLS features.

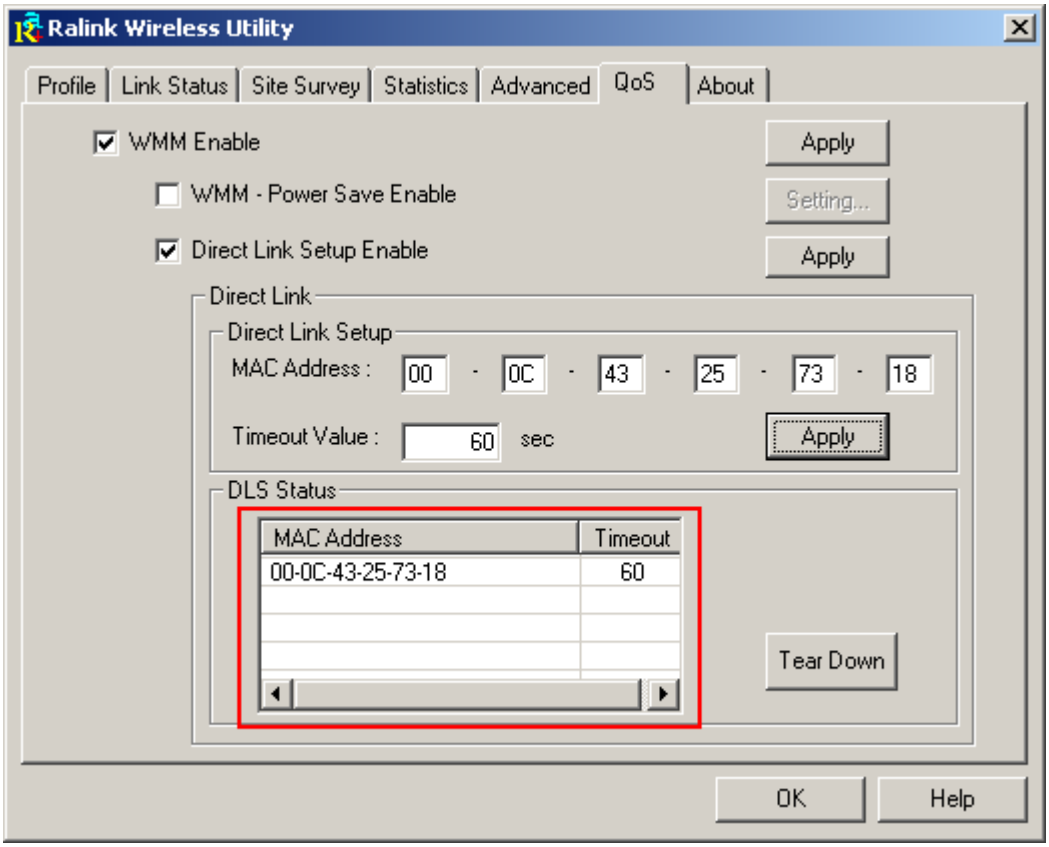
   Have to enable DLS.



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.



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

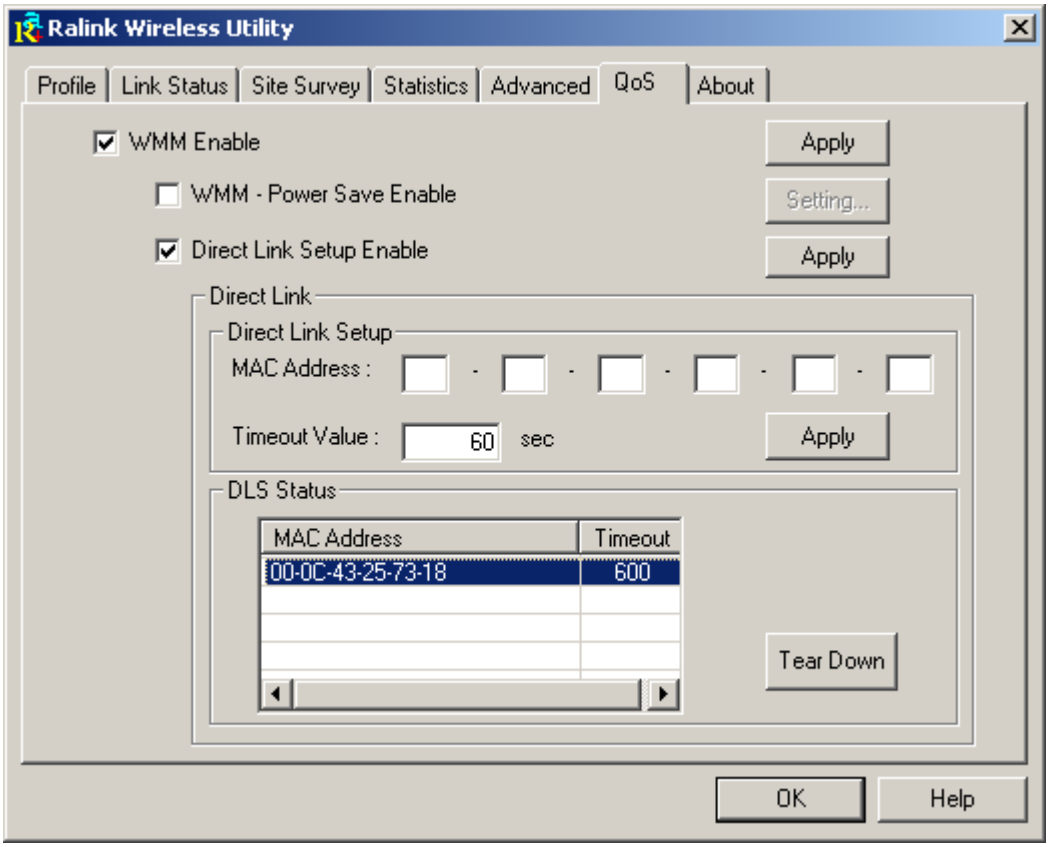


Describe “DLS Status” as follow:

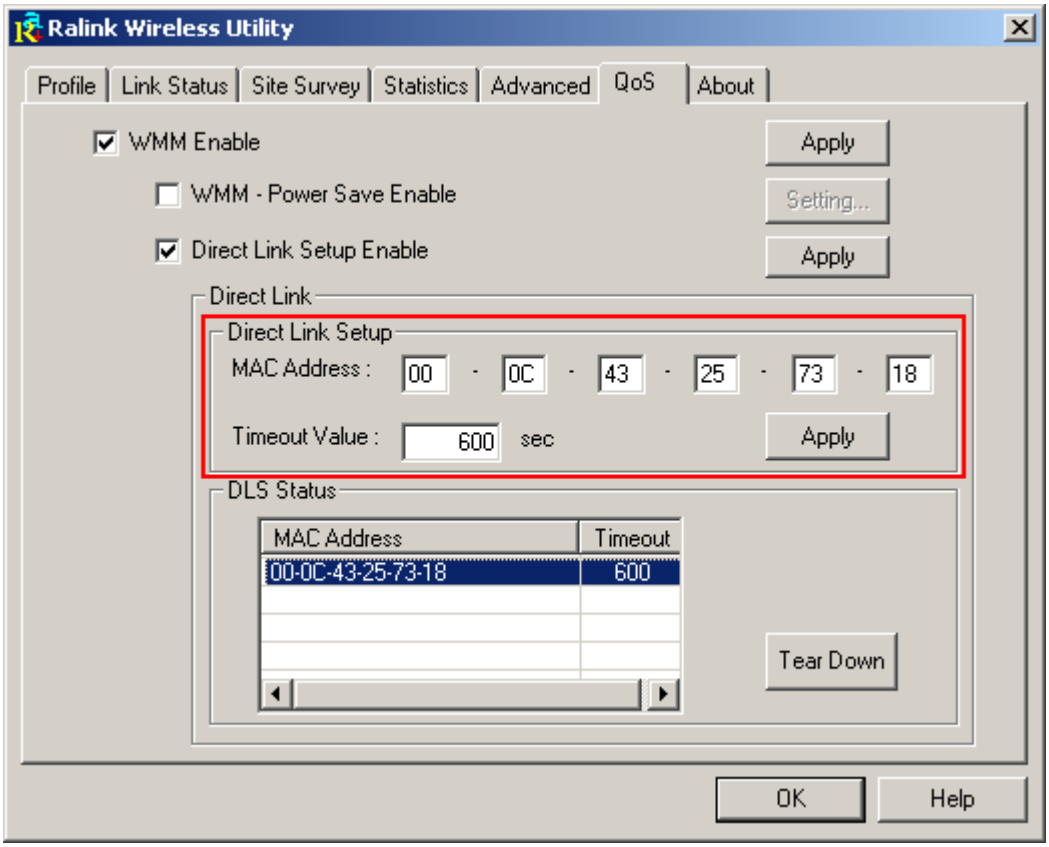
1. As the up figure, after configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in “DLS Status”. In “DLS Status” of the opposite side, it shows MAC address of myself and Timeout Value of setting.

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”.

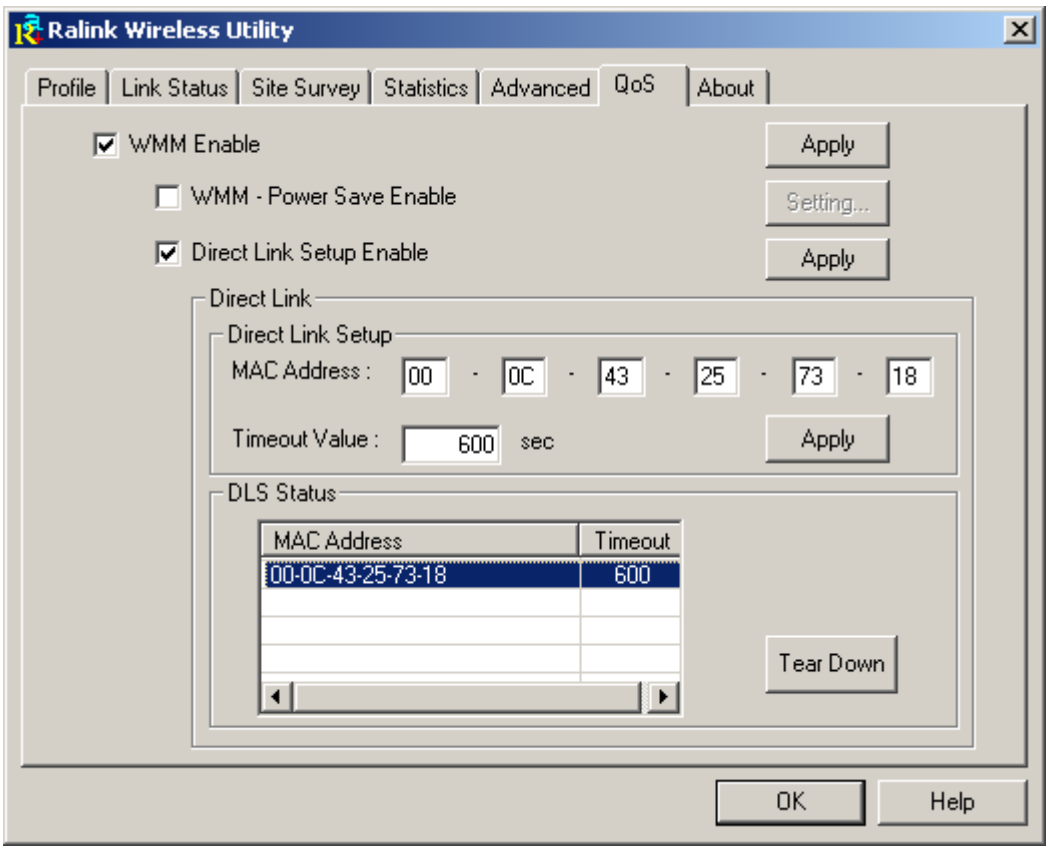


   2. Double click. And the result will look like the below figure.

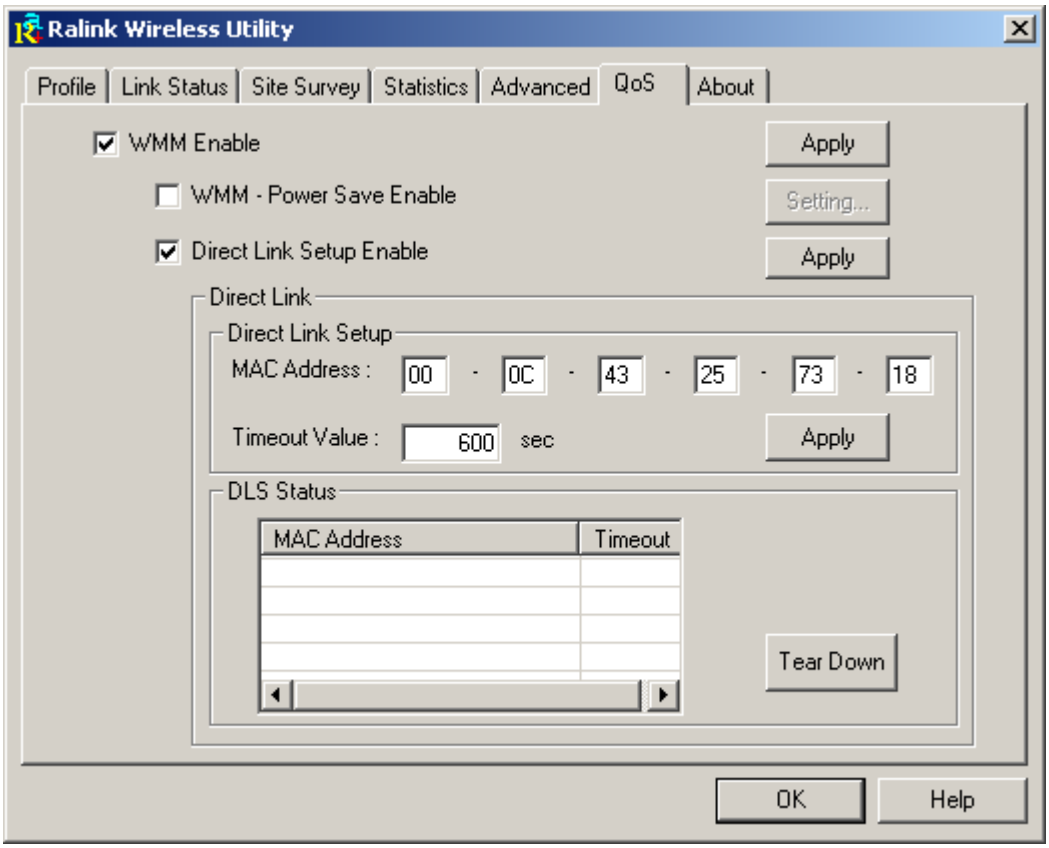


3. Disconnect Direct Link Setup as follow:

    1. Select a direct link STA.

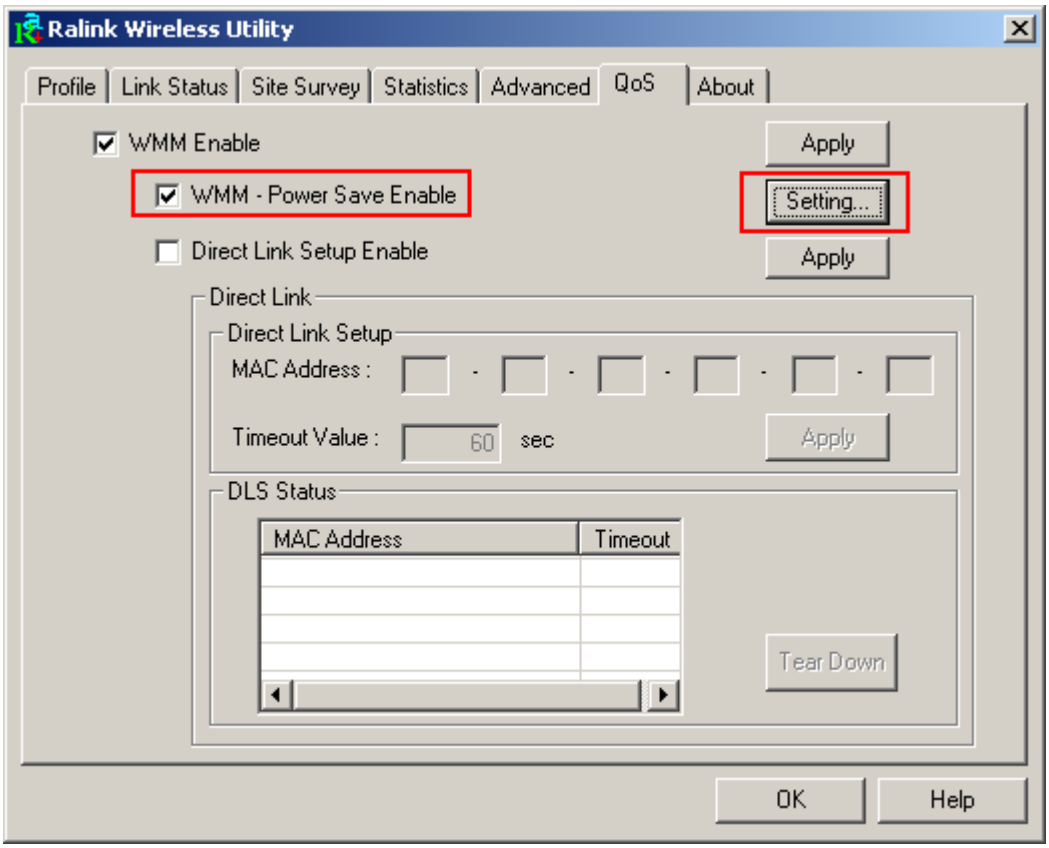


2. Click “Tear Down” button. The result will look like the below figure.

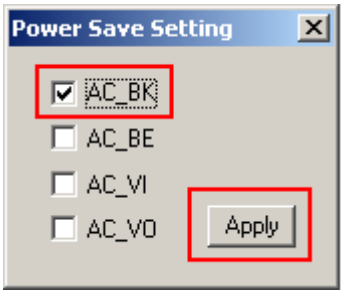


Example to configure to enable WMM – Power Save

1. Click “WMM – Power Save Enable”. And Click “Setting…” button.

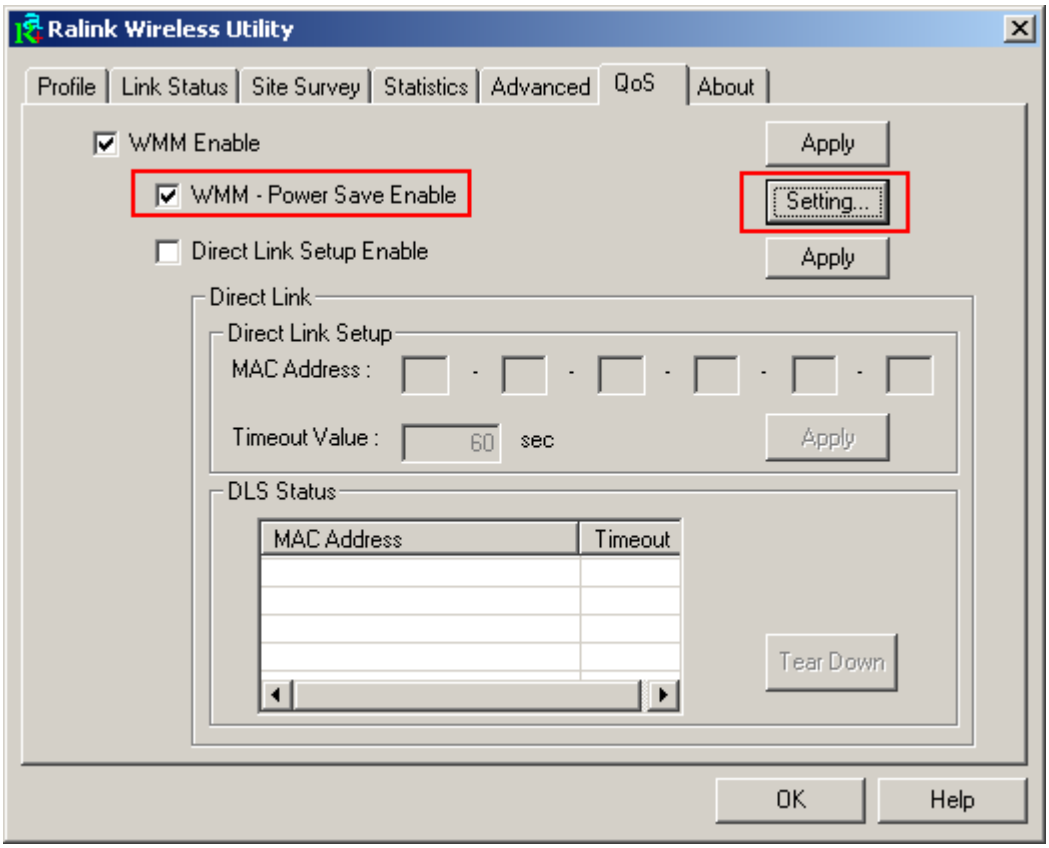


2. After clicking “Setting…” button, show “Power Save Setting” dialog. Please select which ACs you want to enable. Then click “Apply” button. The setting of enabling WMM – Power Save is successfully.

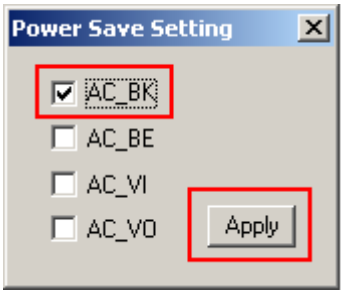


Example to configure to enable WMM – Power Save

1. Click “WMM – Power Save Enable”. And Click “Setting…” button.



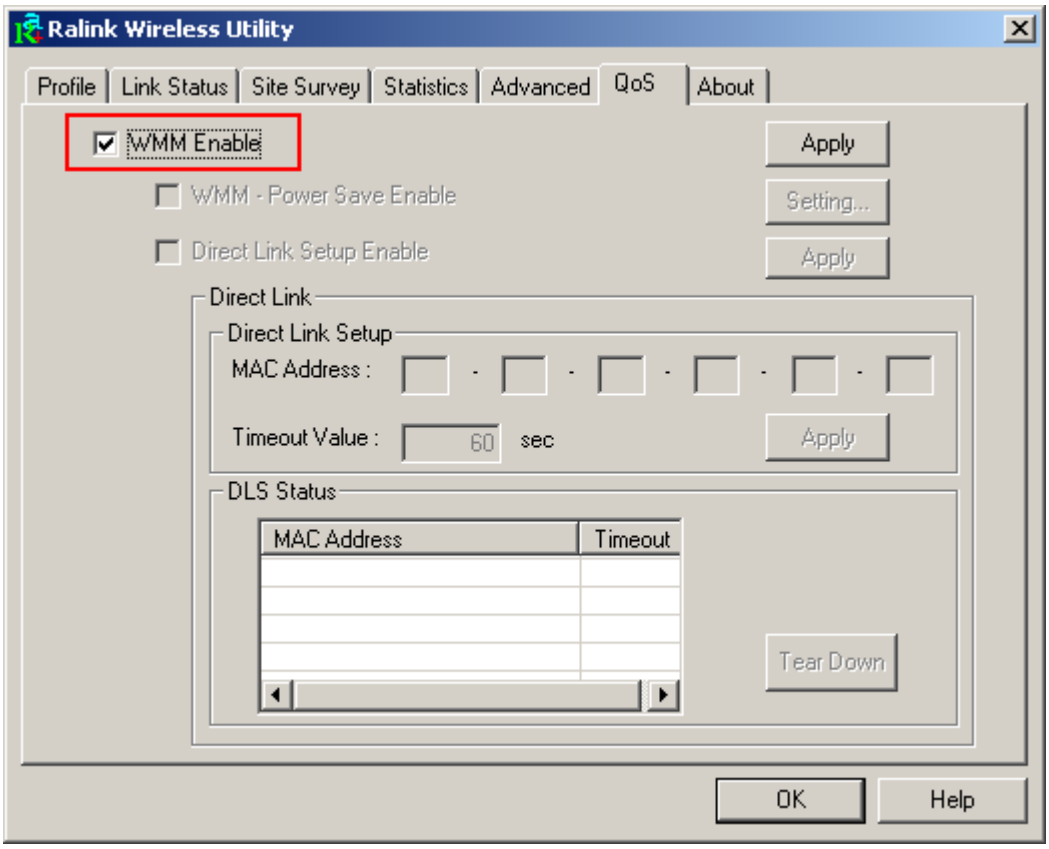
2. After clicking “Setting…” button, show “Power Save Setting” dialog. Please select which ACs you want to enable. Then click “Apply” button. The setting of enabling WMM – Power Save is successfully.



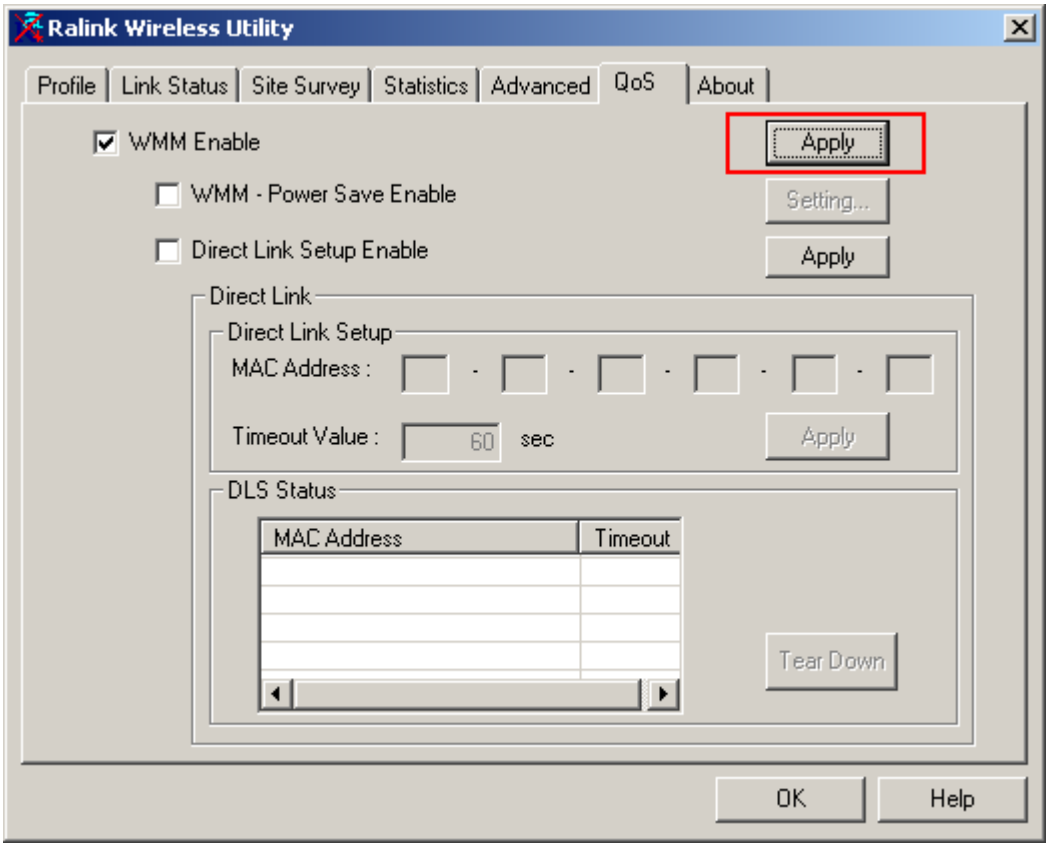
Example to configure to enable Wi-Fi Multi-Media

If you want to use “WMM – Power Save” or “Direct Link”, you must enable WMM. The setting method of enabling WMM indicates as follows:

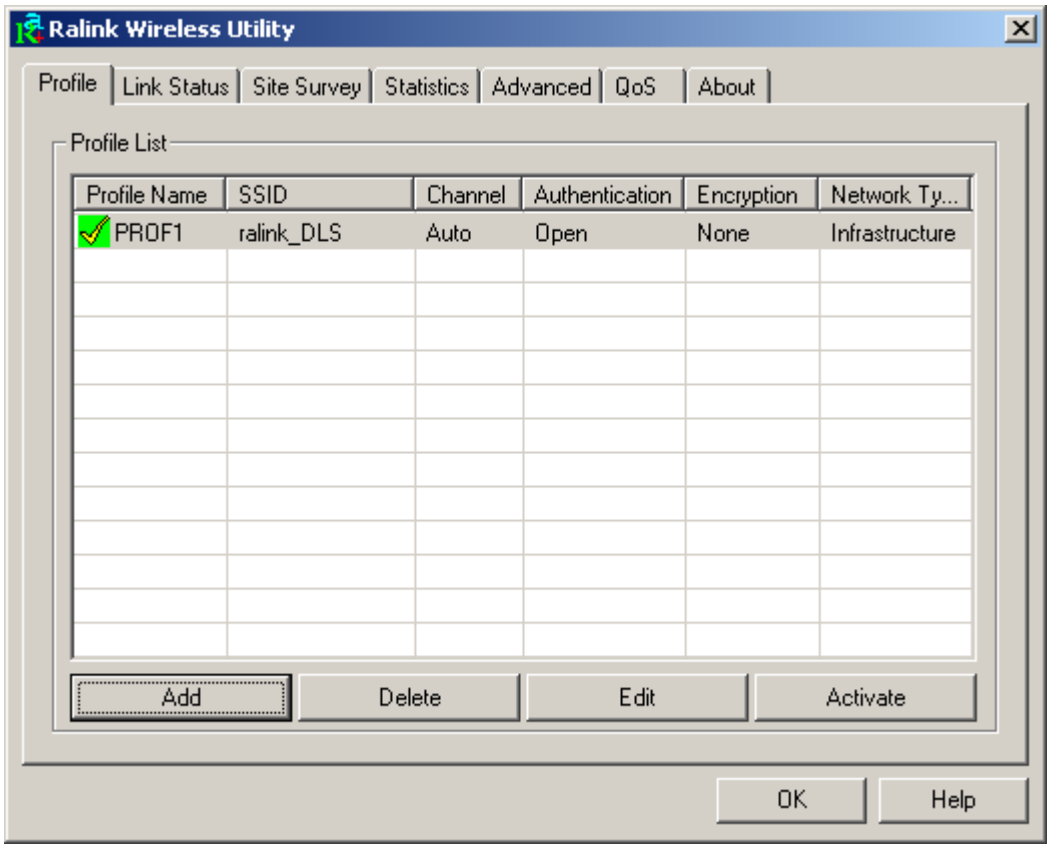
1. Click “WMM Enable”.



2. Click “Apply”.

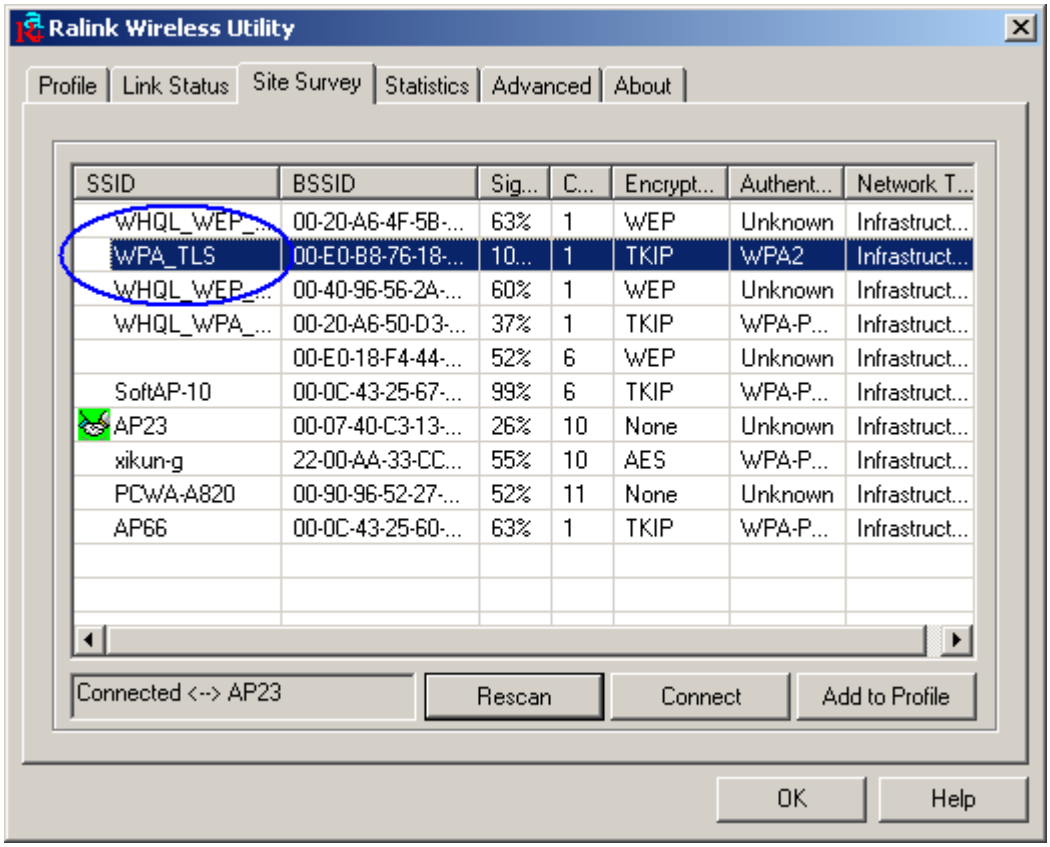


3. Change to “Site Survey Page”. And add a AP that supports WMM features to a Profile. The result will look like the below figure in Profile page.

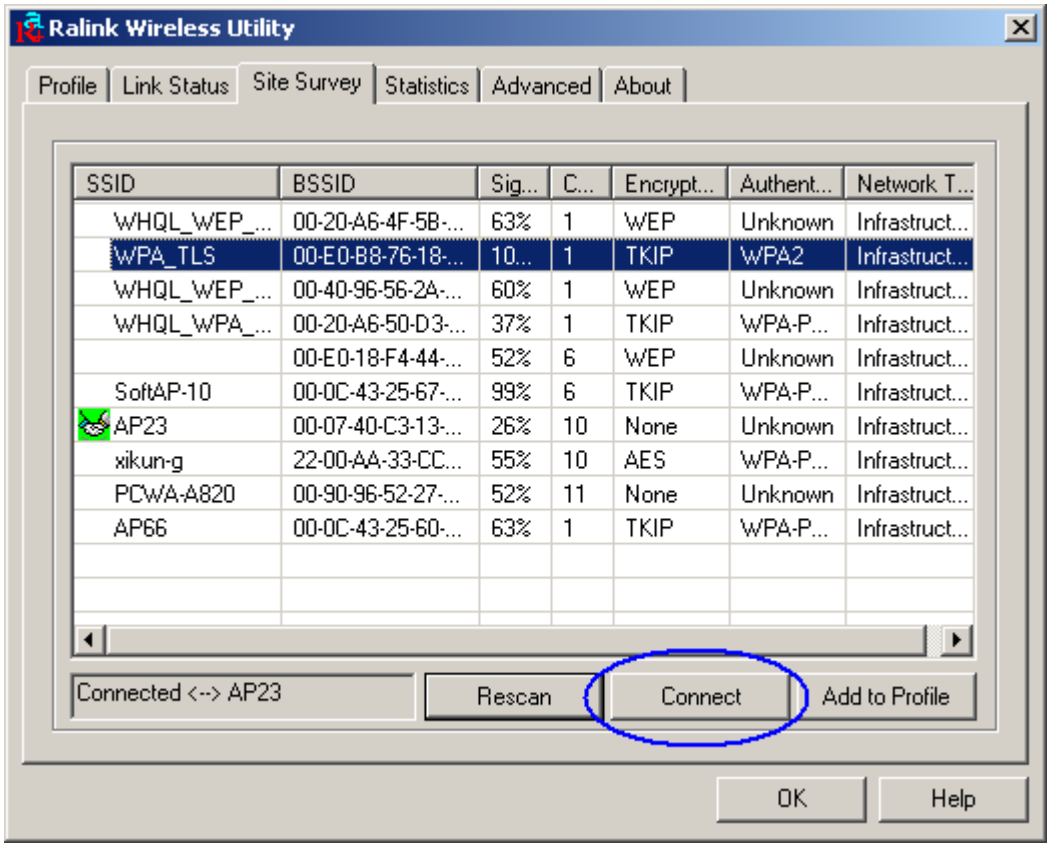


Configure connection with WPA2 by 802.1x setting

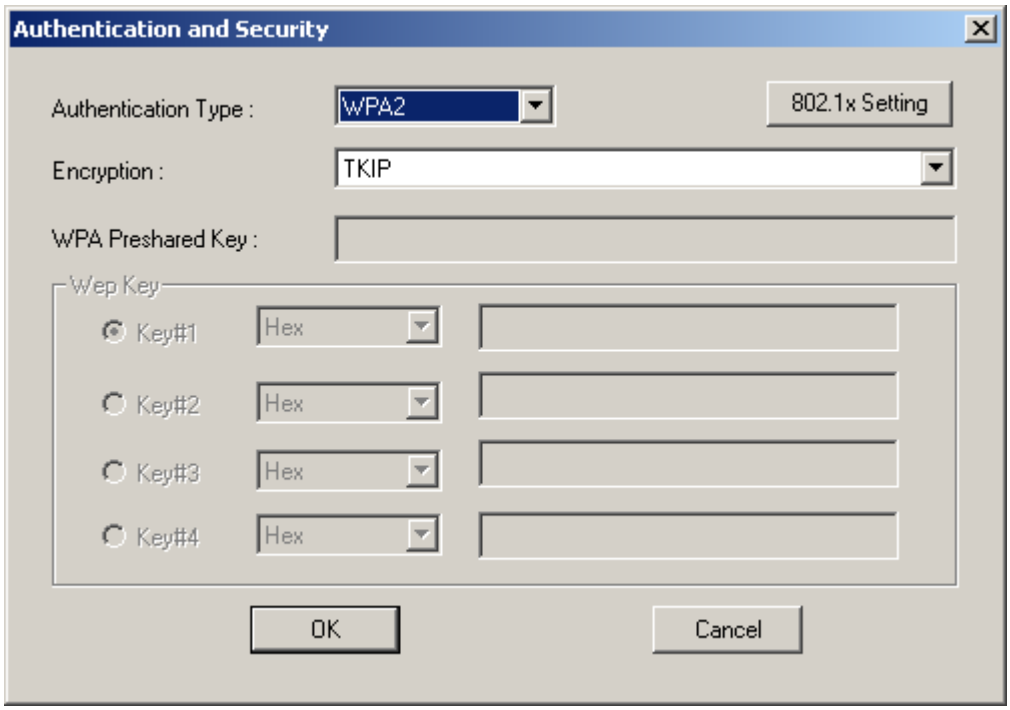
1. Select A.P with WPA2 authentication mode.



2. Click CONNECT or double click the intended network.

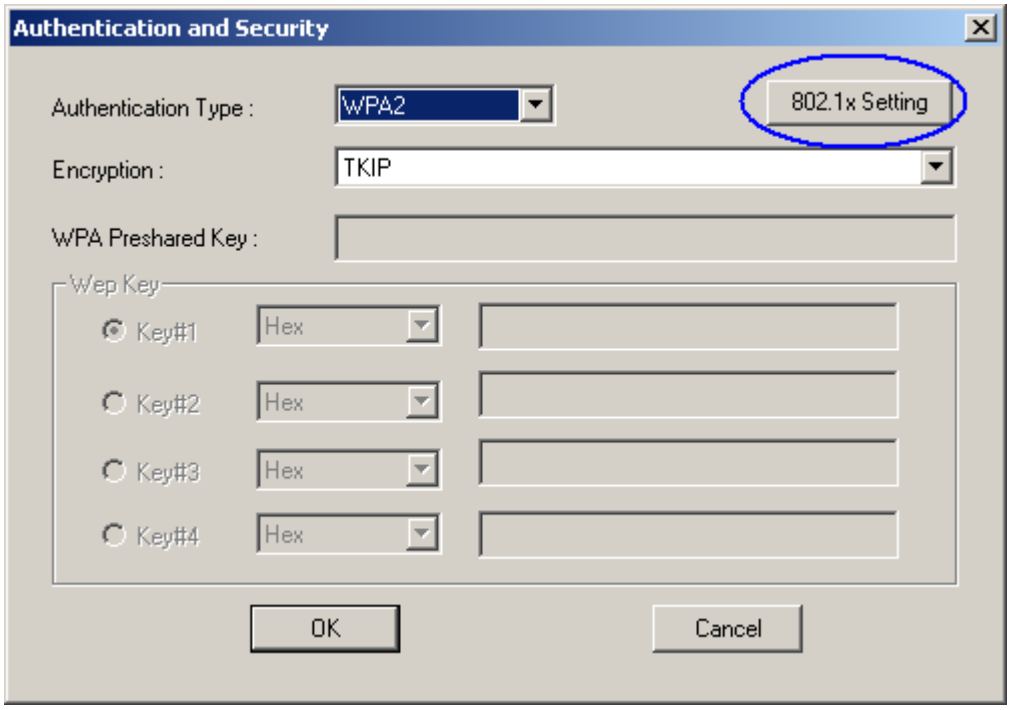


3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

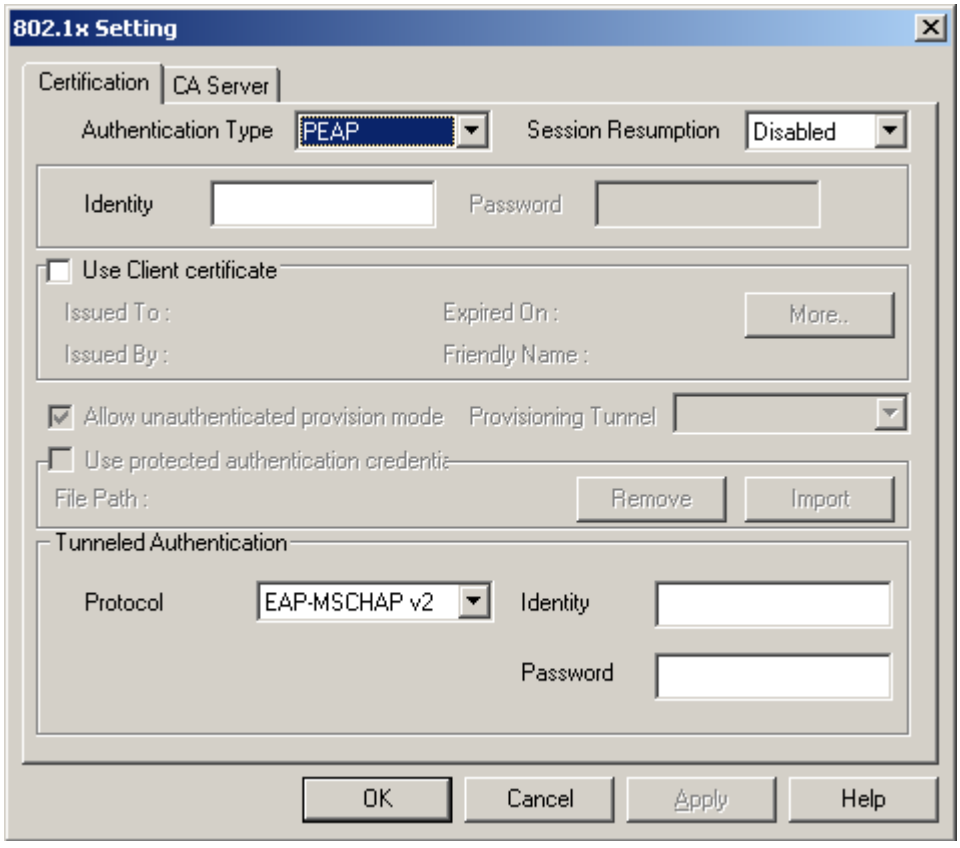


*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Click 802.1x setting.



5. 802.1x setting page will pop up.

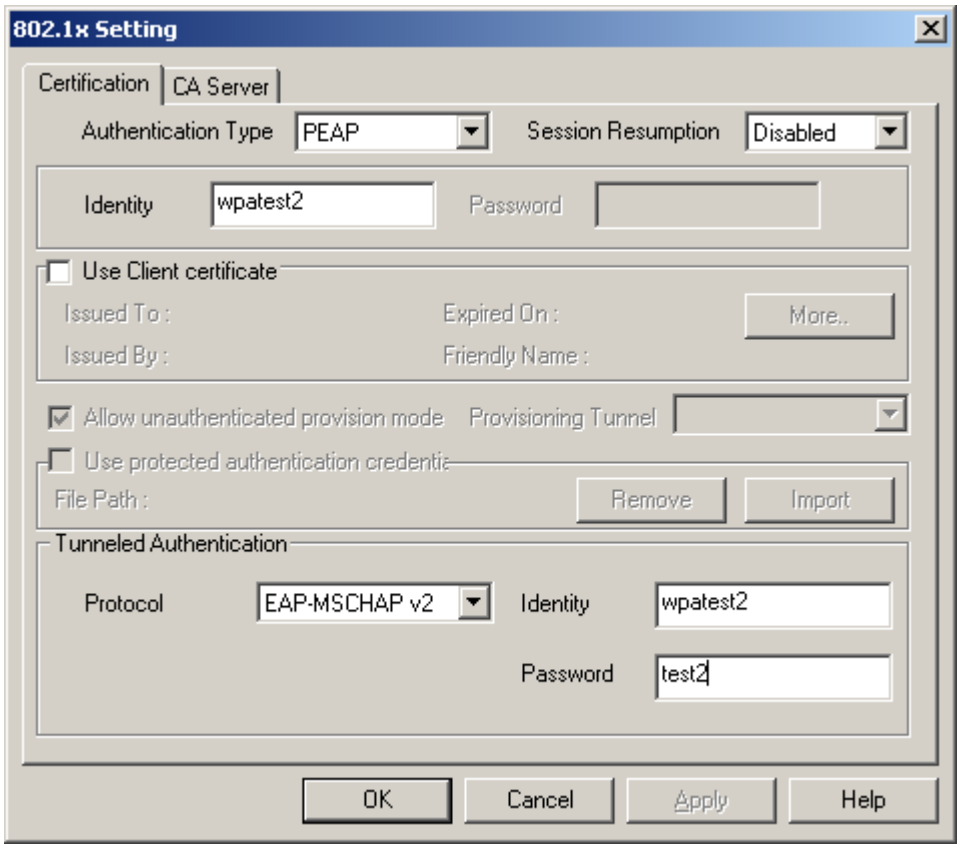


5. Authentication type and setting method:

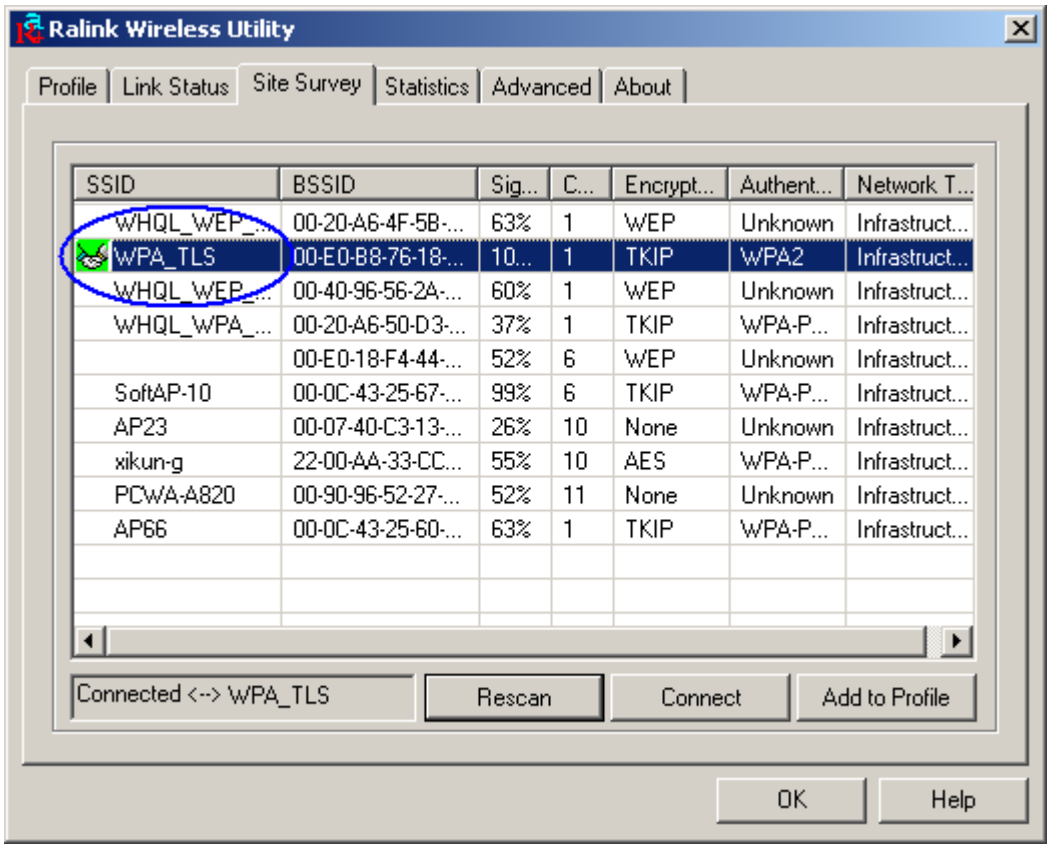
1 PEAP:

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.

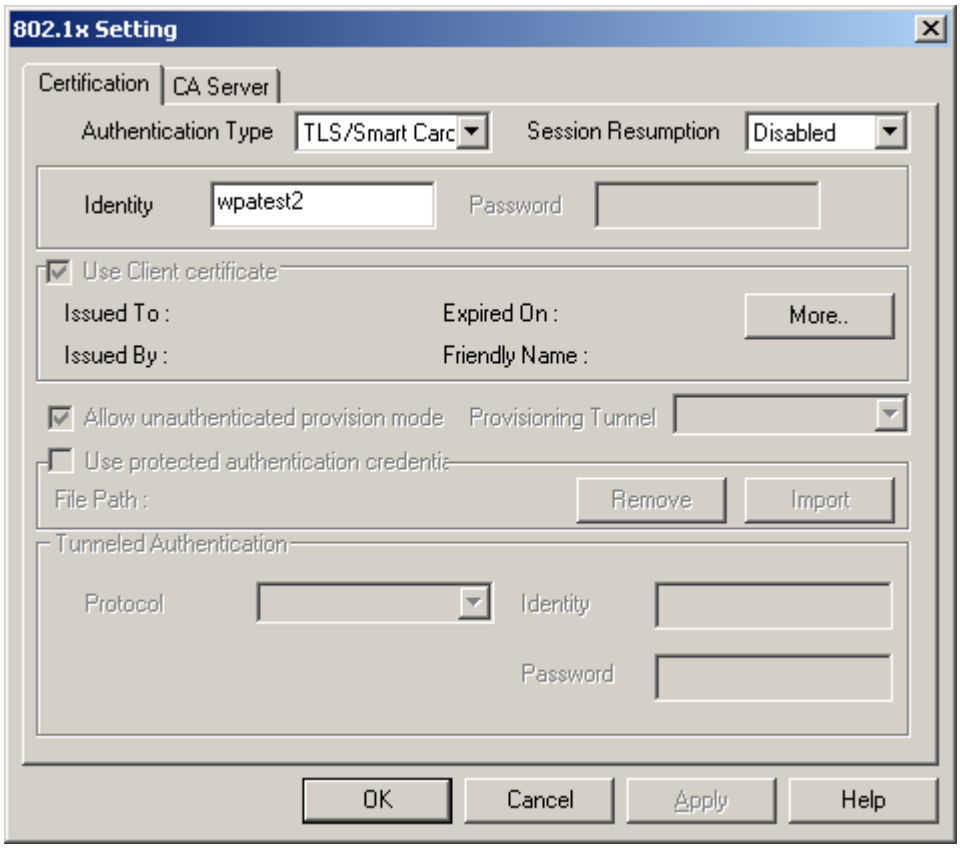


2. Click OK. The result will look like the below figure.

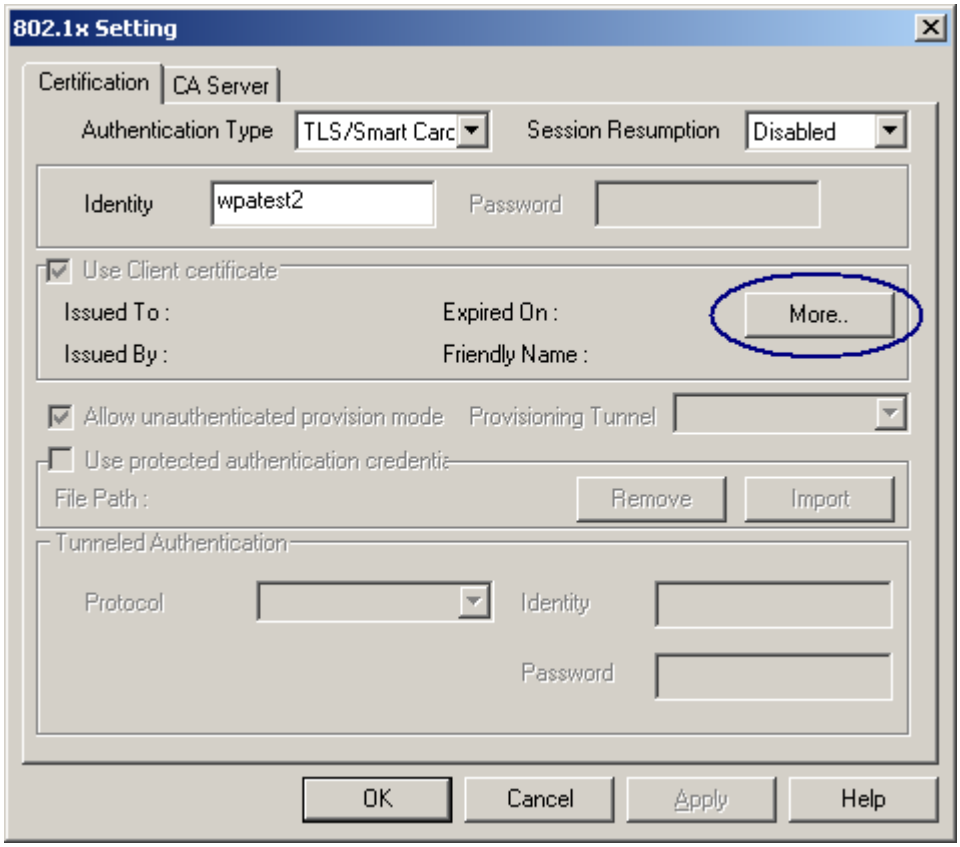


2 TLS / Smart Card:

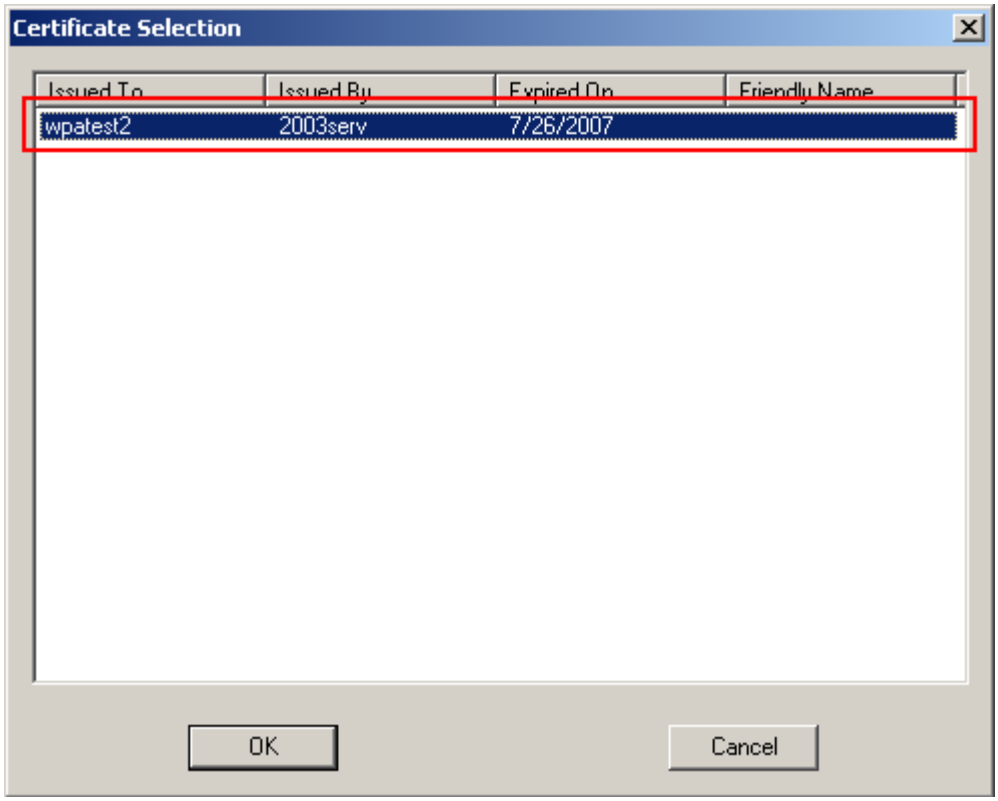
1. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.



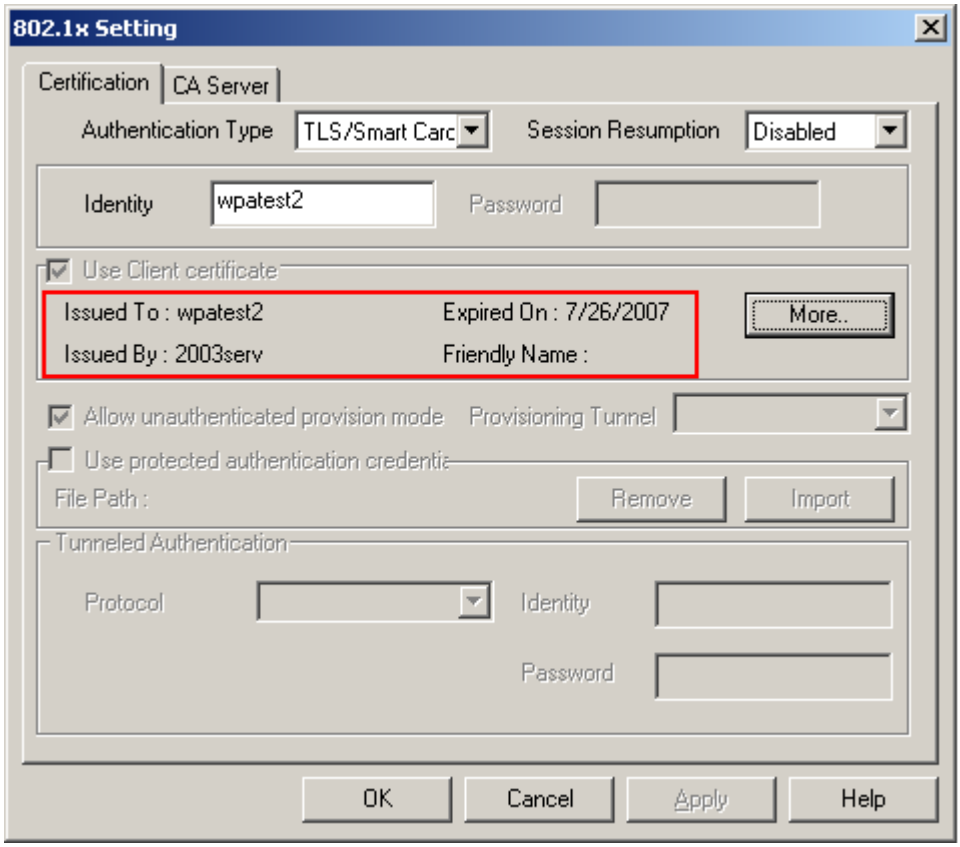
2. TLS must use client certicate. Click more to choose certicate.



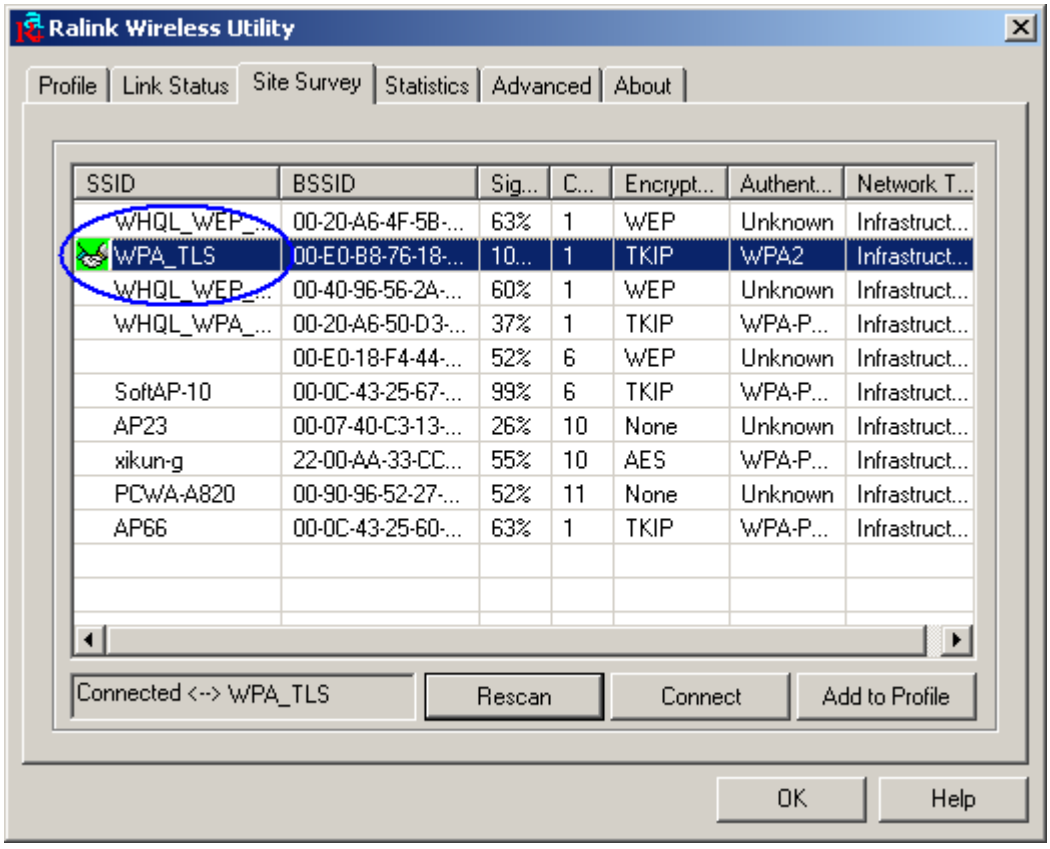
3. Certicate page will pop up; choose a certicate for server authentication.



3. Display certicate information in use client certicate page.

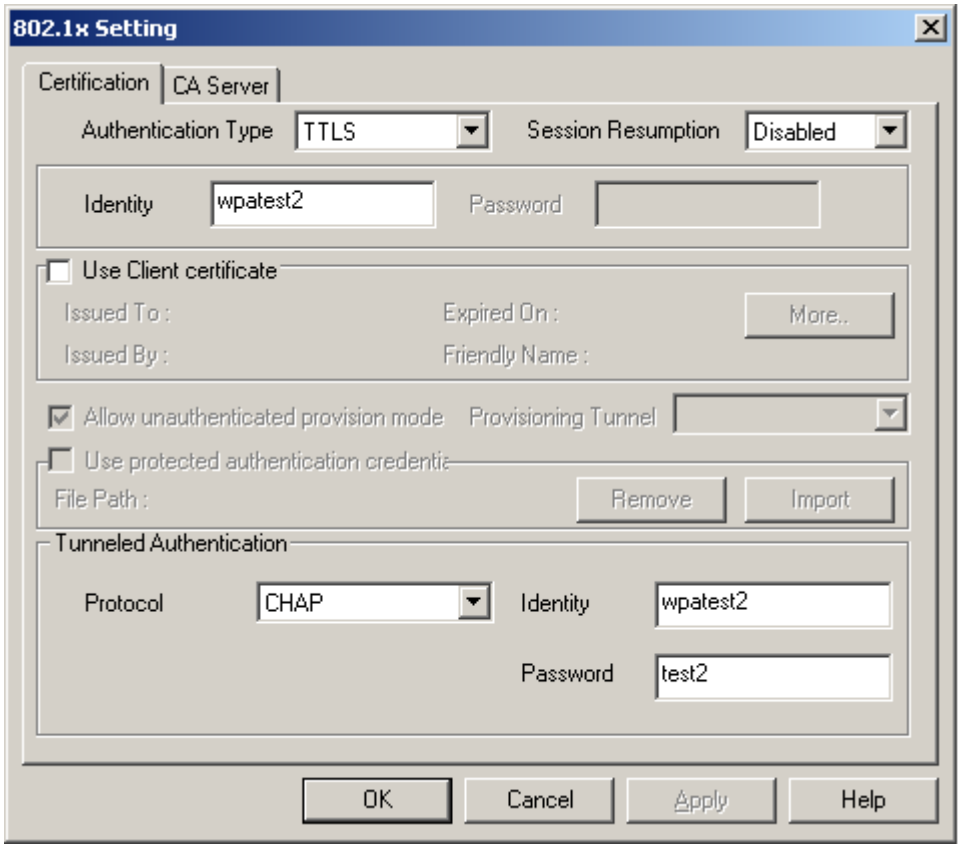


4. Click OK. The result will look like the below figure.

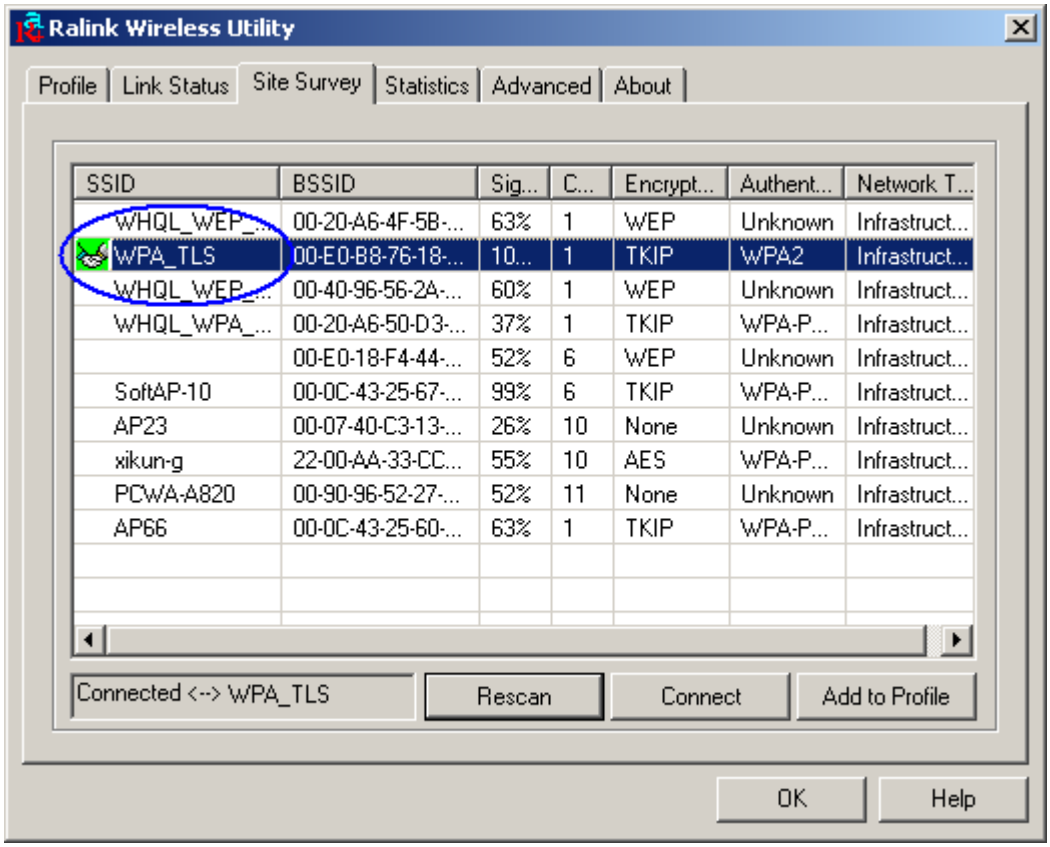


3 TTLS:

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.

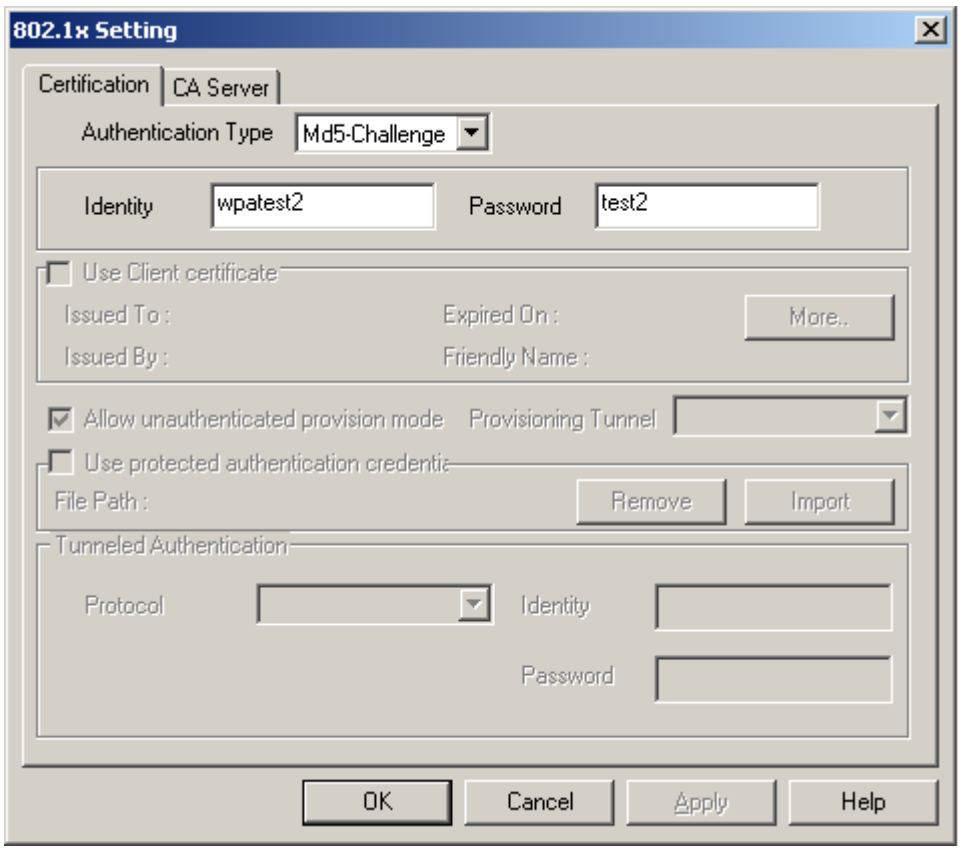


2. Click OK. The result will look like the below figure.

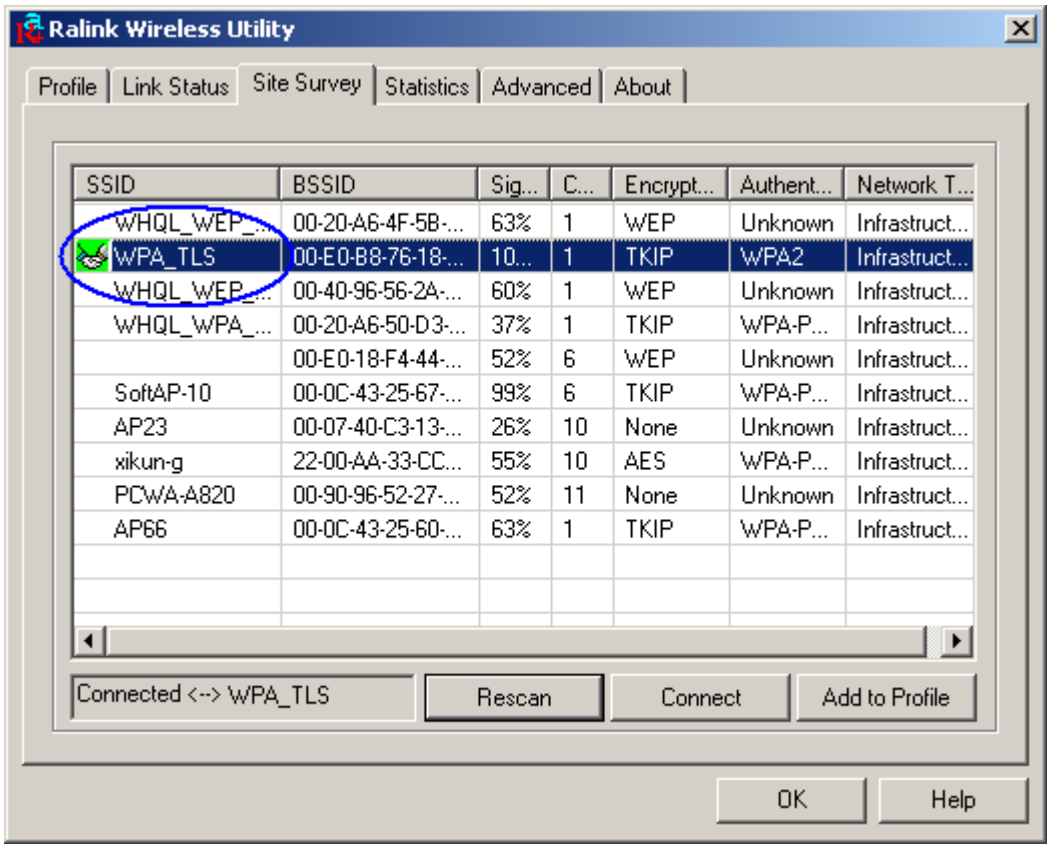


4 MD5:

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

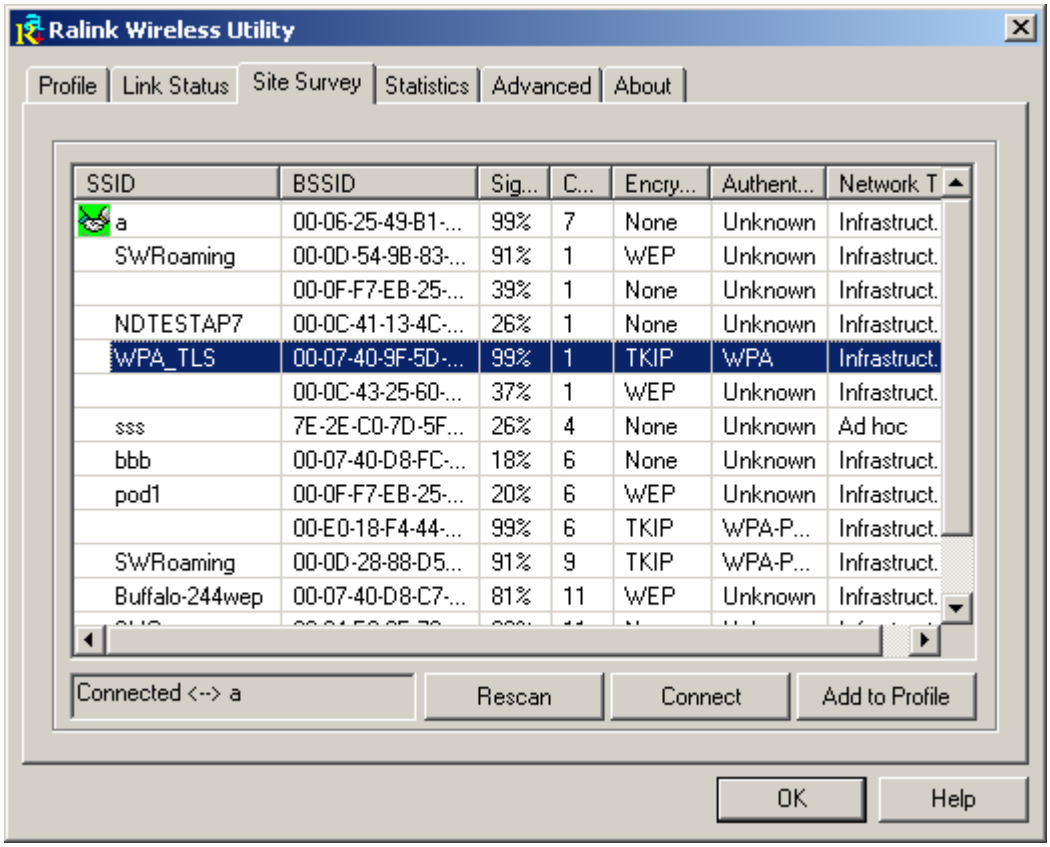


2. Click OK. The result will look like the below figure.

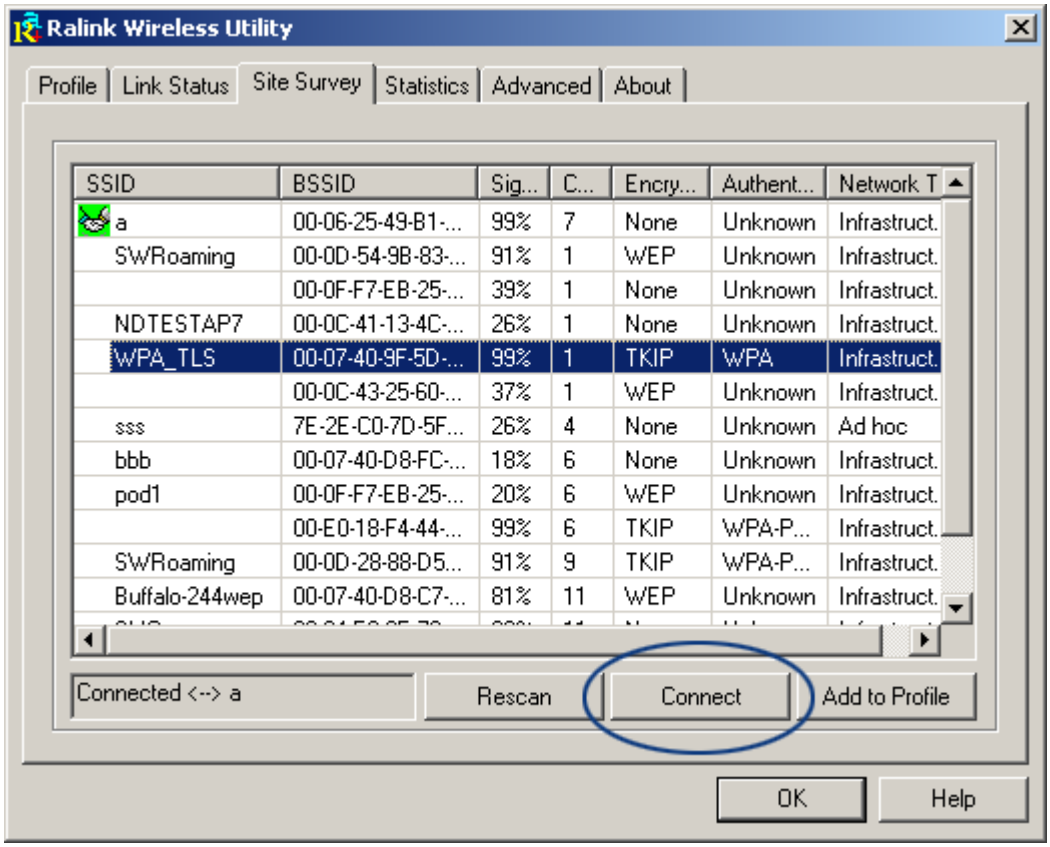


Configure connection with WPA by 802.1x setting

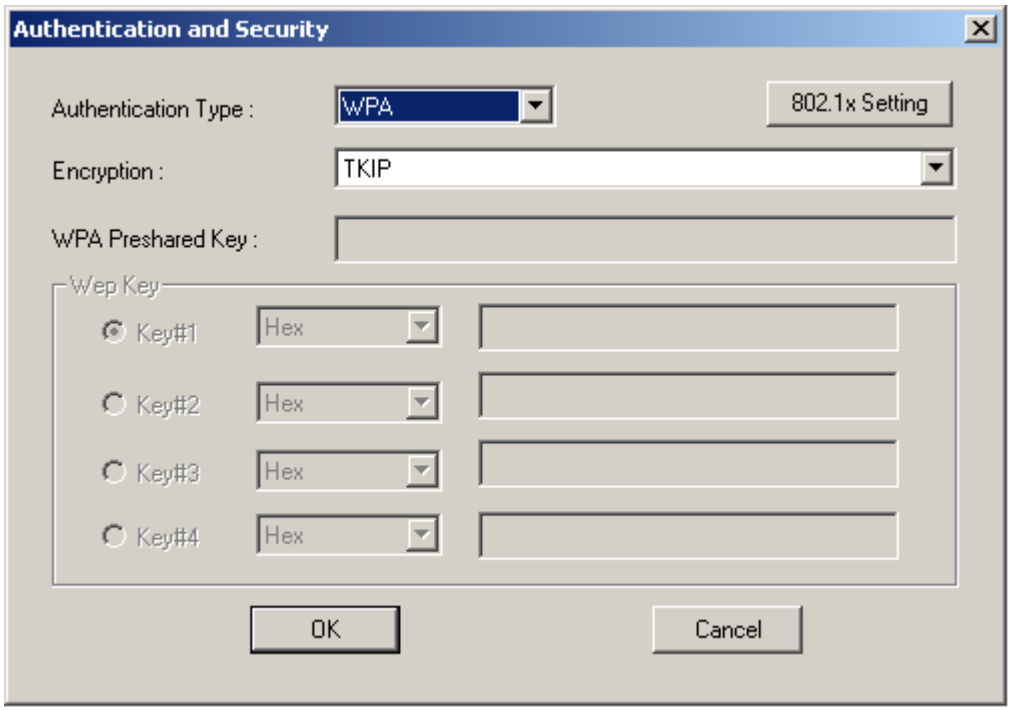
1. Select A.P with WPA authentication mode.



2. Click CONNECT or double click the intended network.

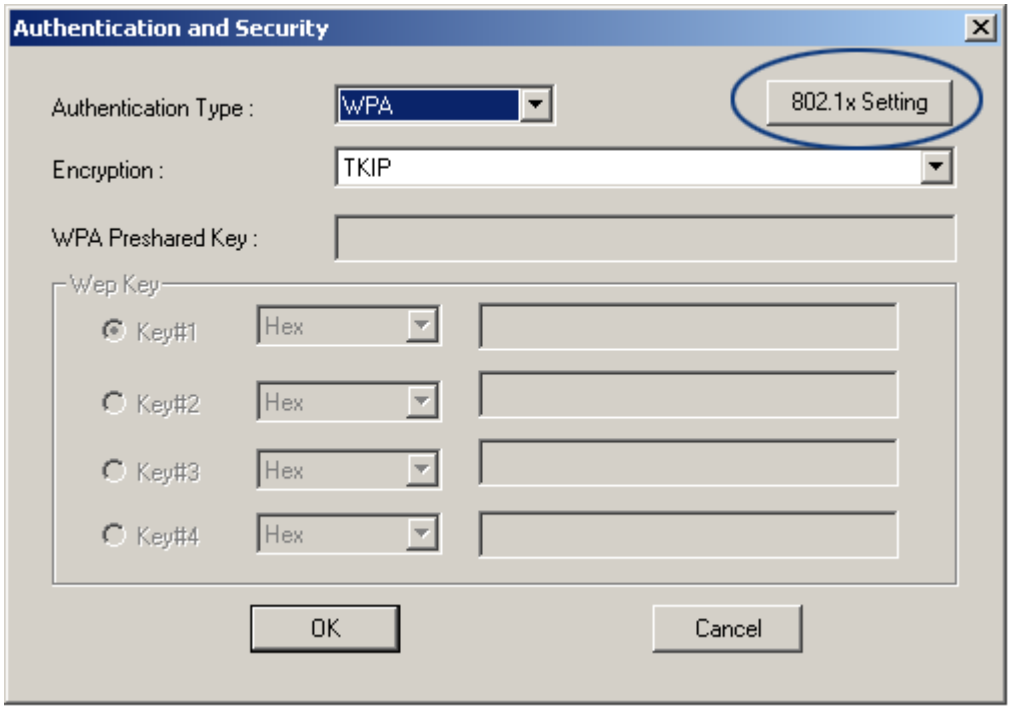


3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

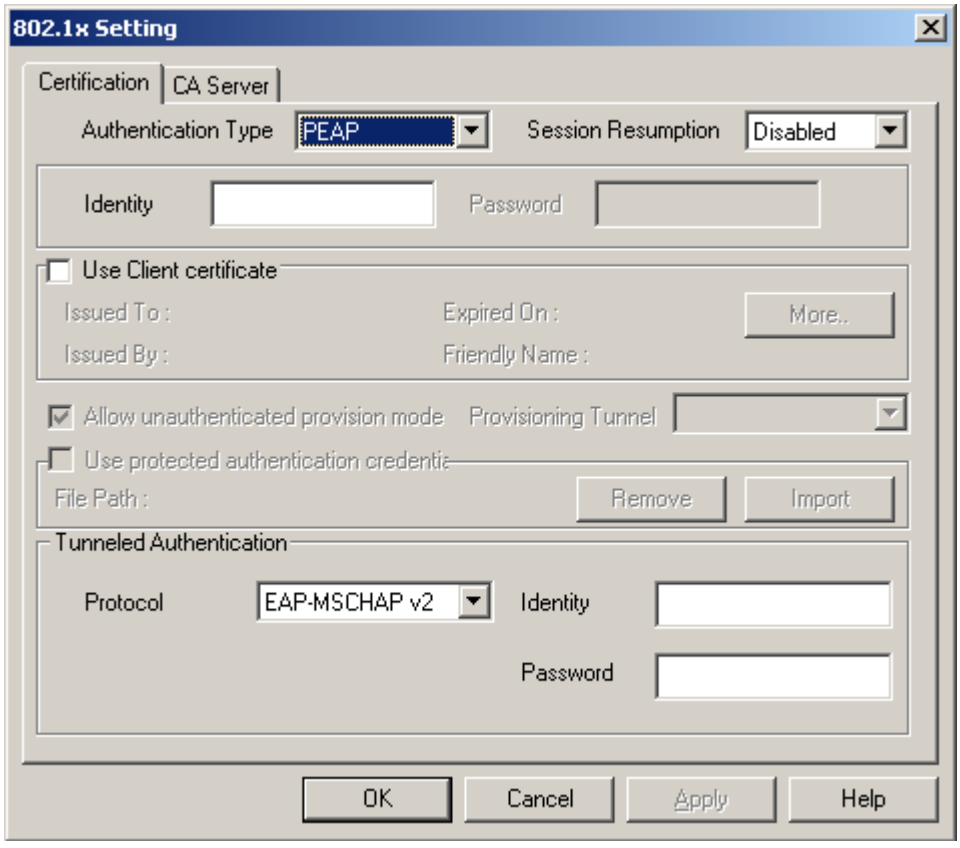


*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Click 802.1x setting.



5. 802.1x setting page will pop up.

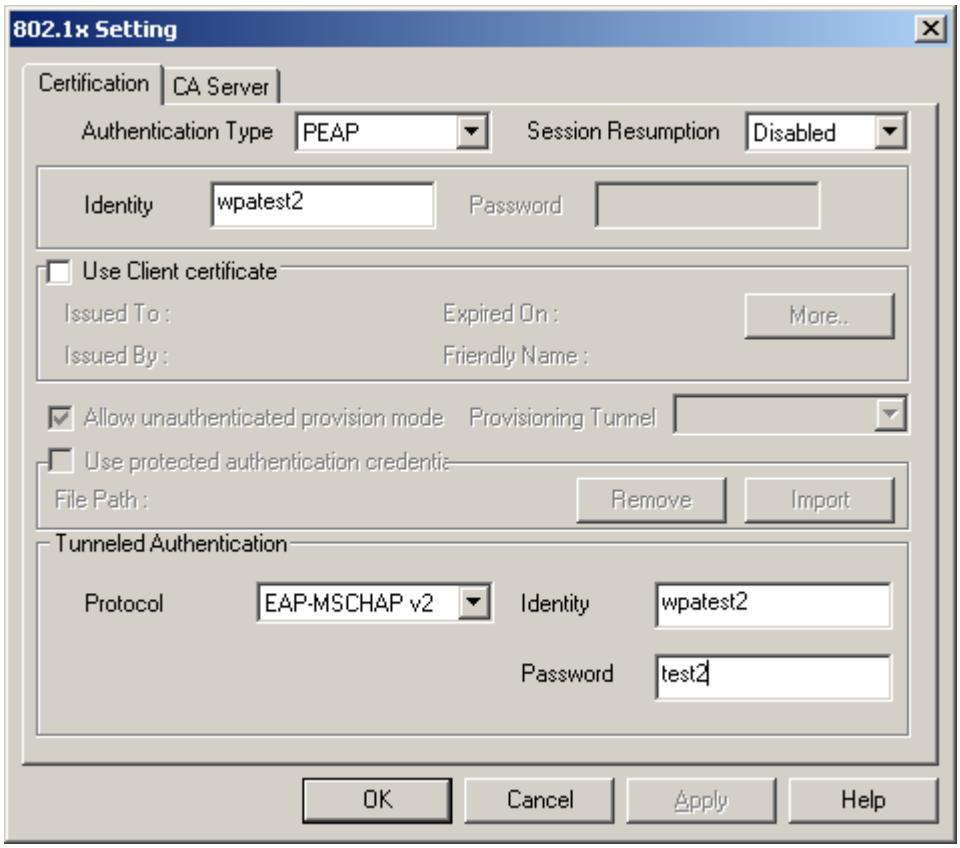


6. Authentication type and setting method:

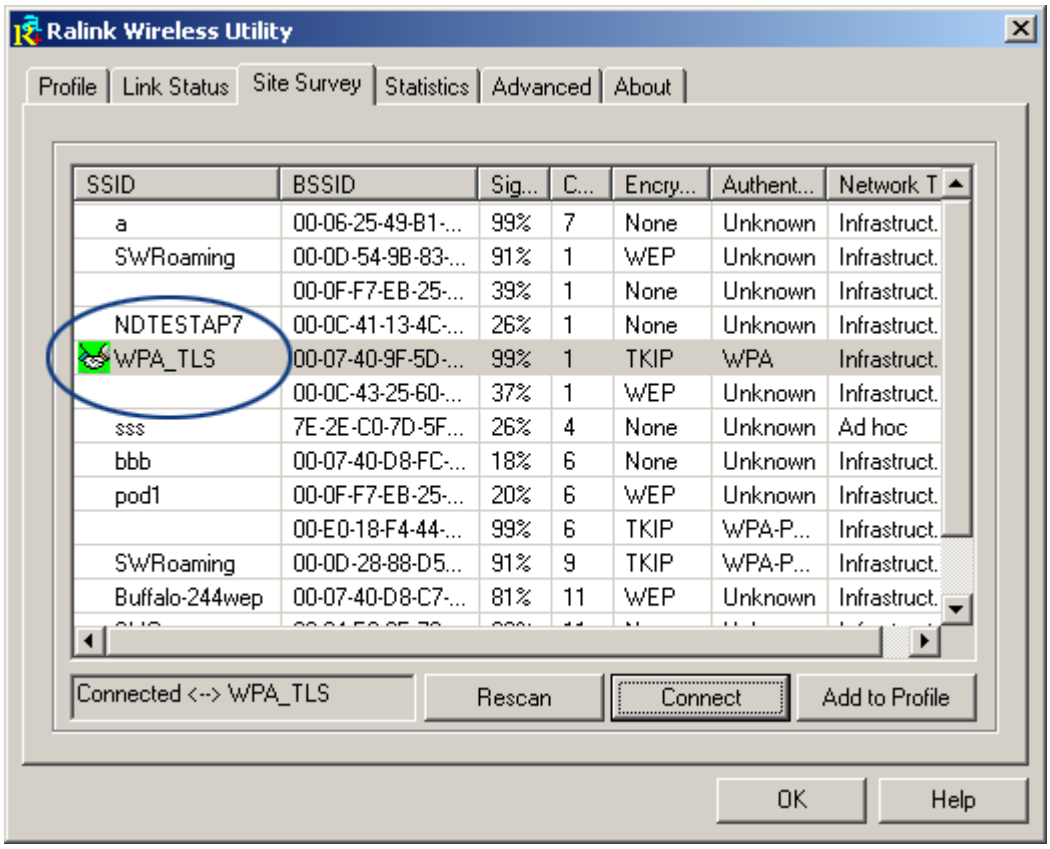
1 PEAP:

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.

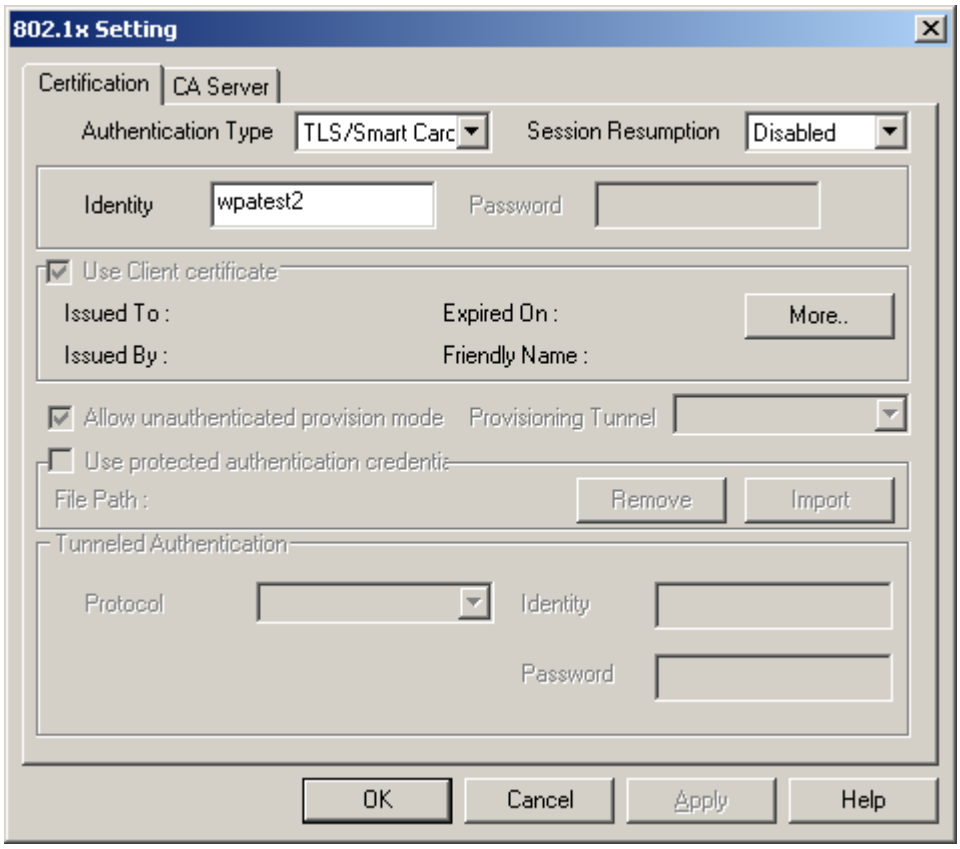


2. Click OK. The result will look like the below figure.

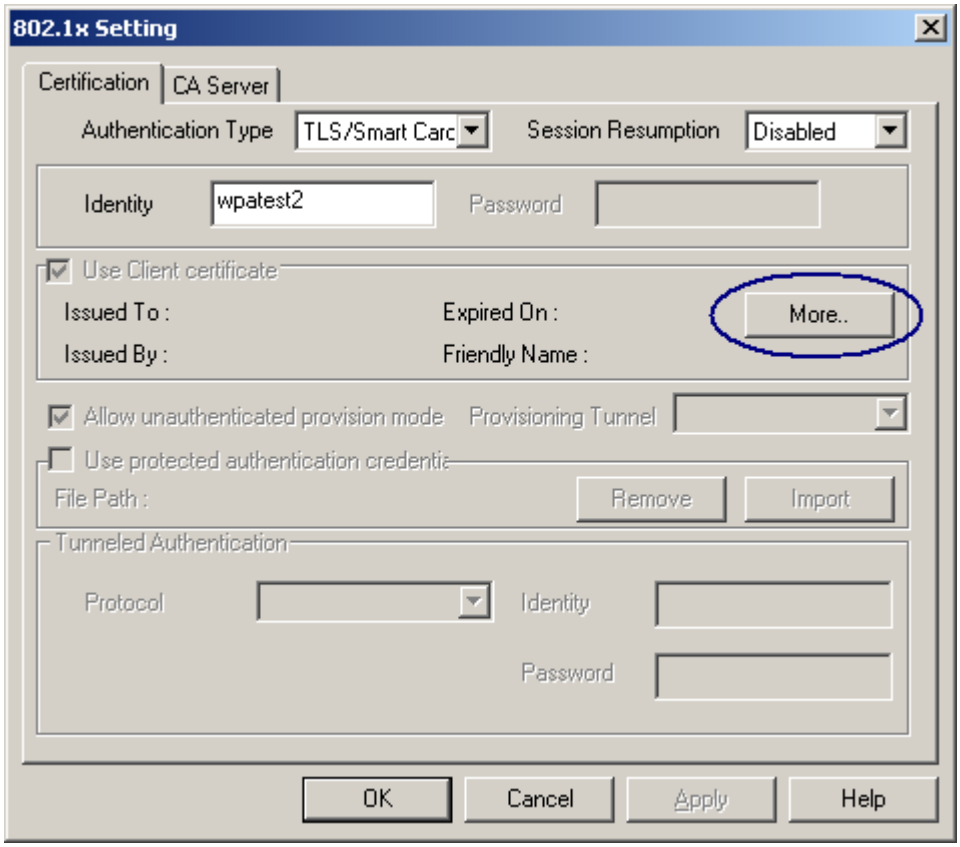


2 TLS / Smart Card:

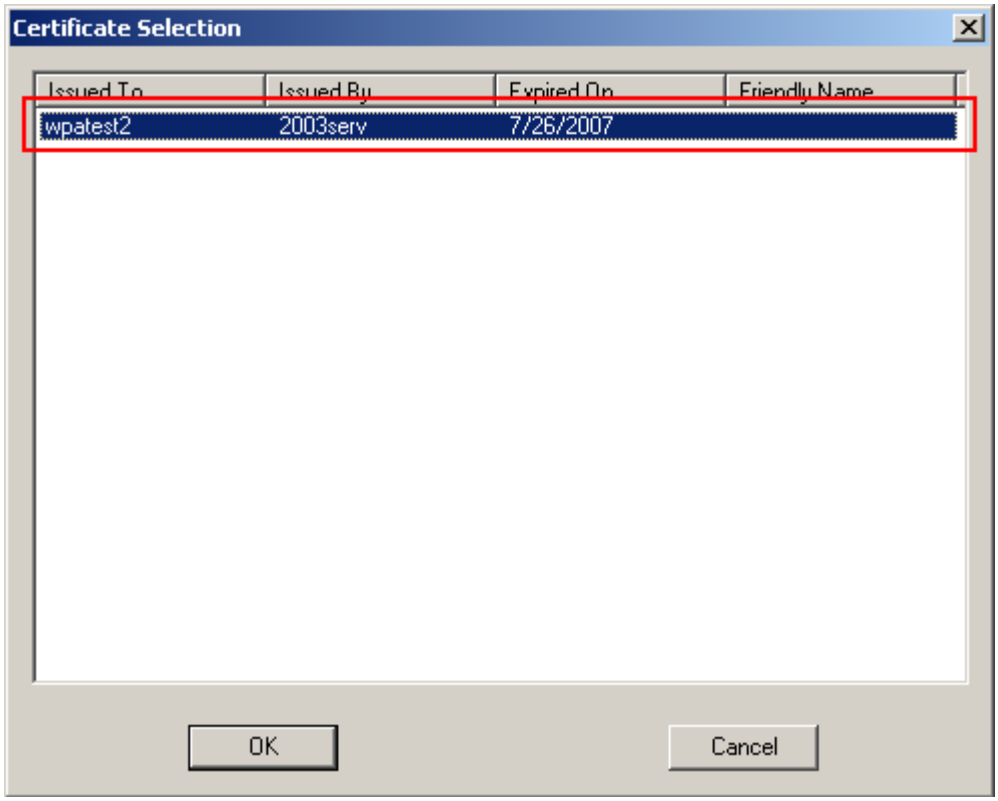
1. Authentication type chooses TLS / Smart Card, TLS only need identity that is wpatest2 for server authentication.



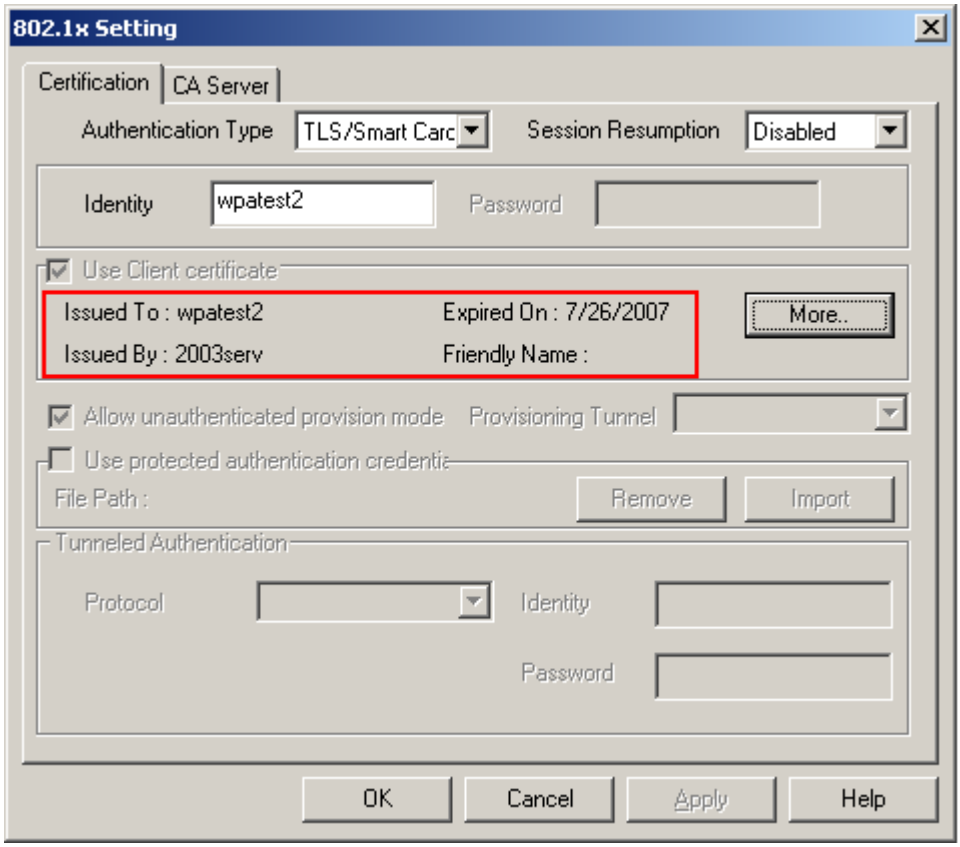
2. TLS must use client certicate. Click more to choose certicate.



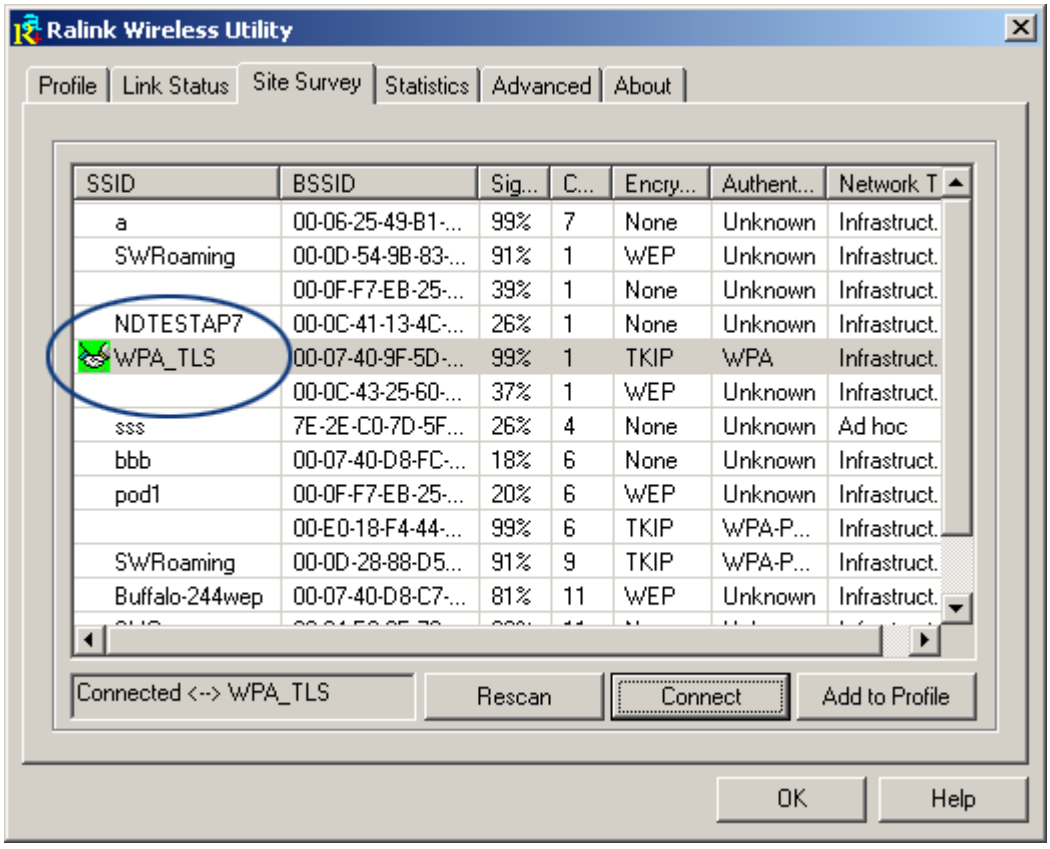
3. Certicate page will pop up; choose a certicate for server authentication.



4. Display certicate information in use client certicate page.

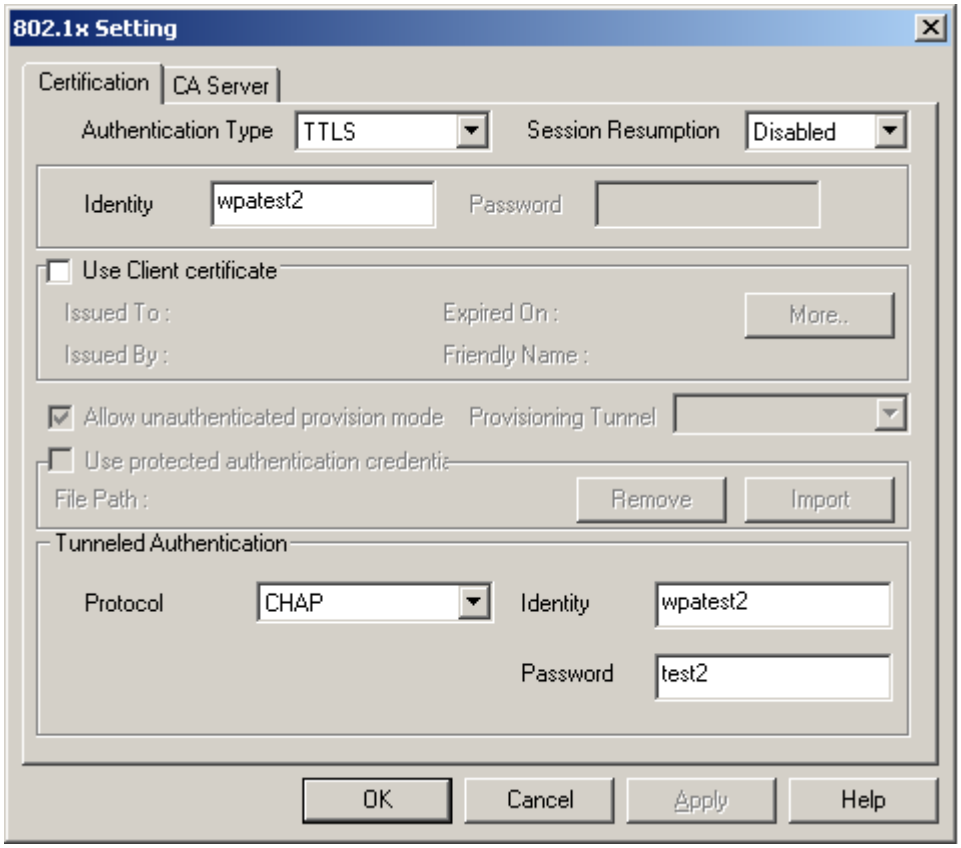


5. Click OK. The result will look like the below figure.

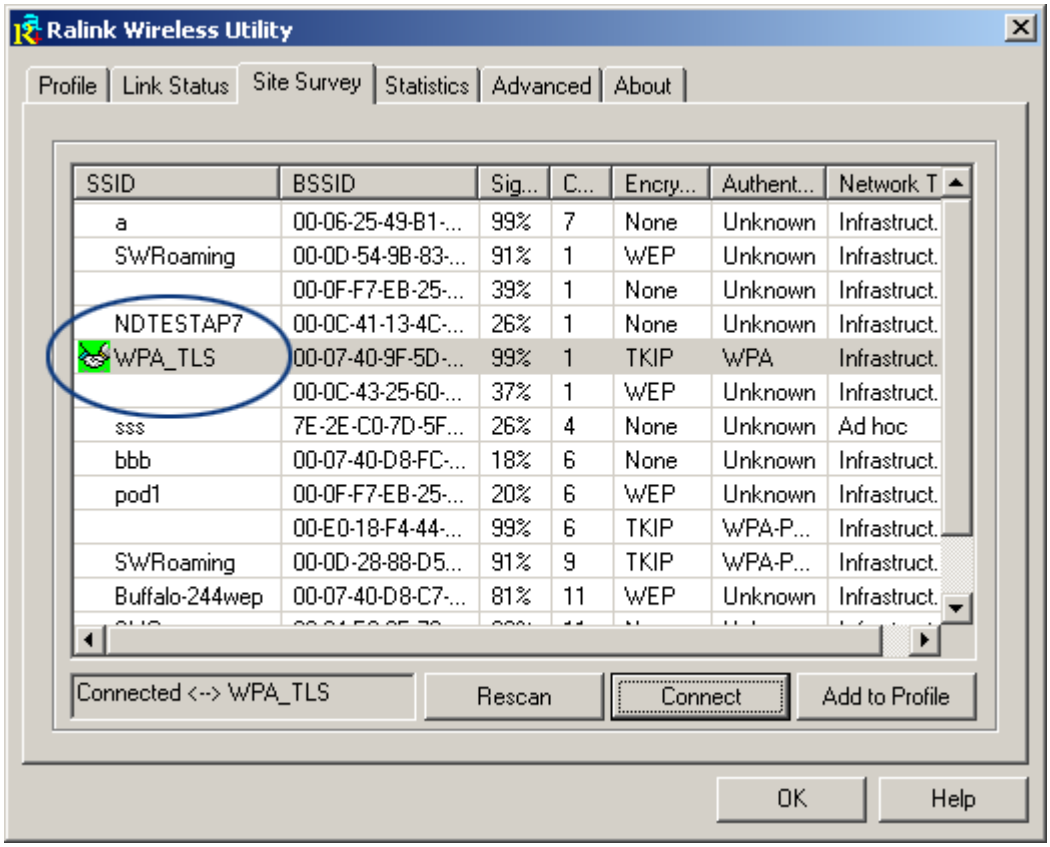


3 TTLS:

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.

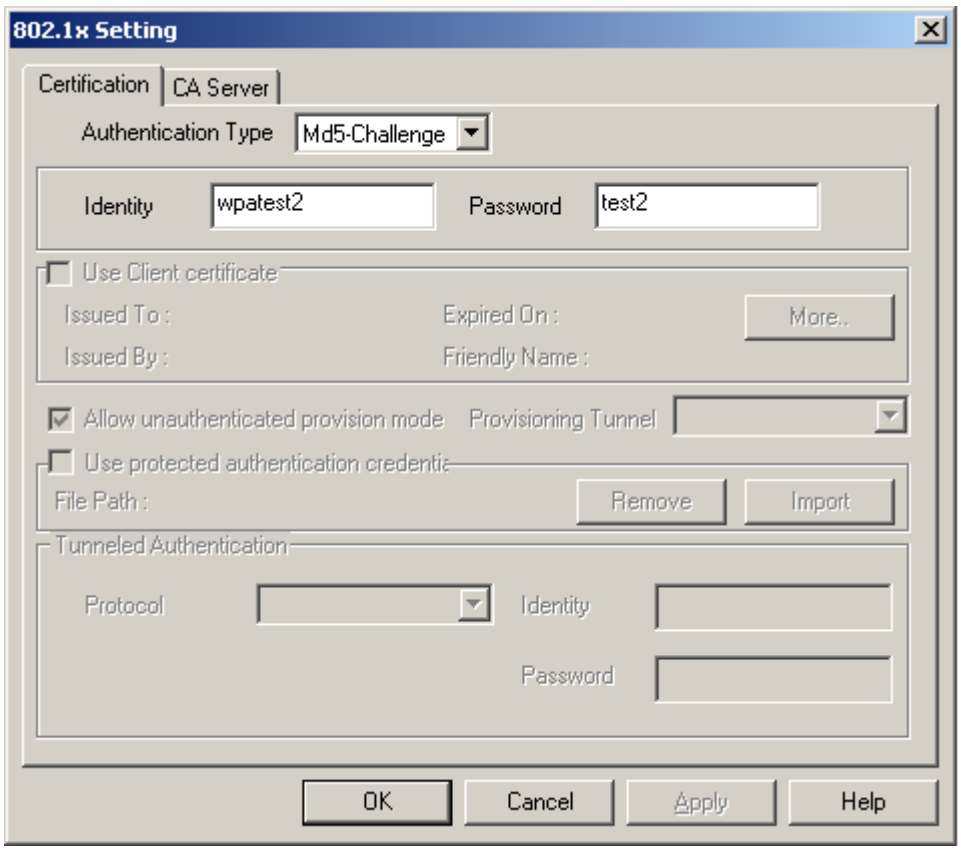


2. Click OK. The result will look like the below figure.

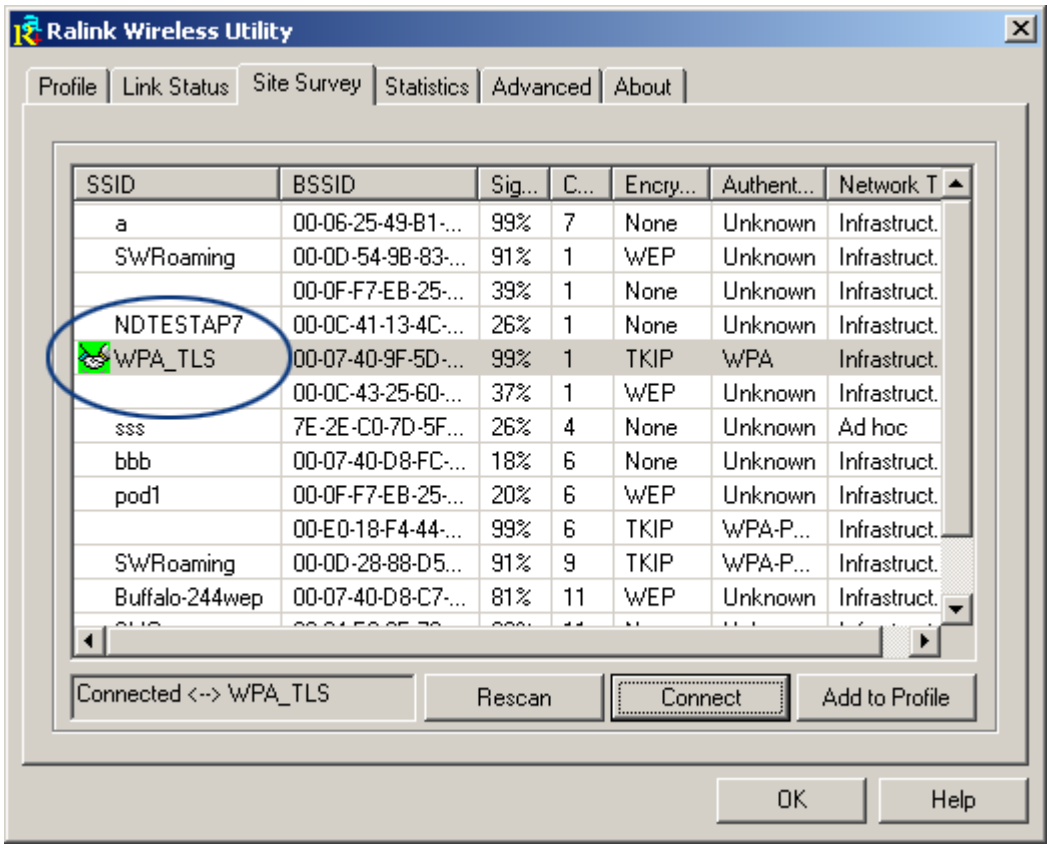


4 MD5:

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

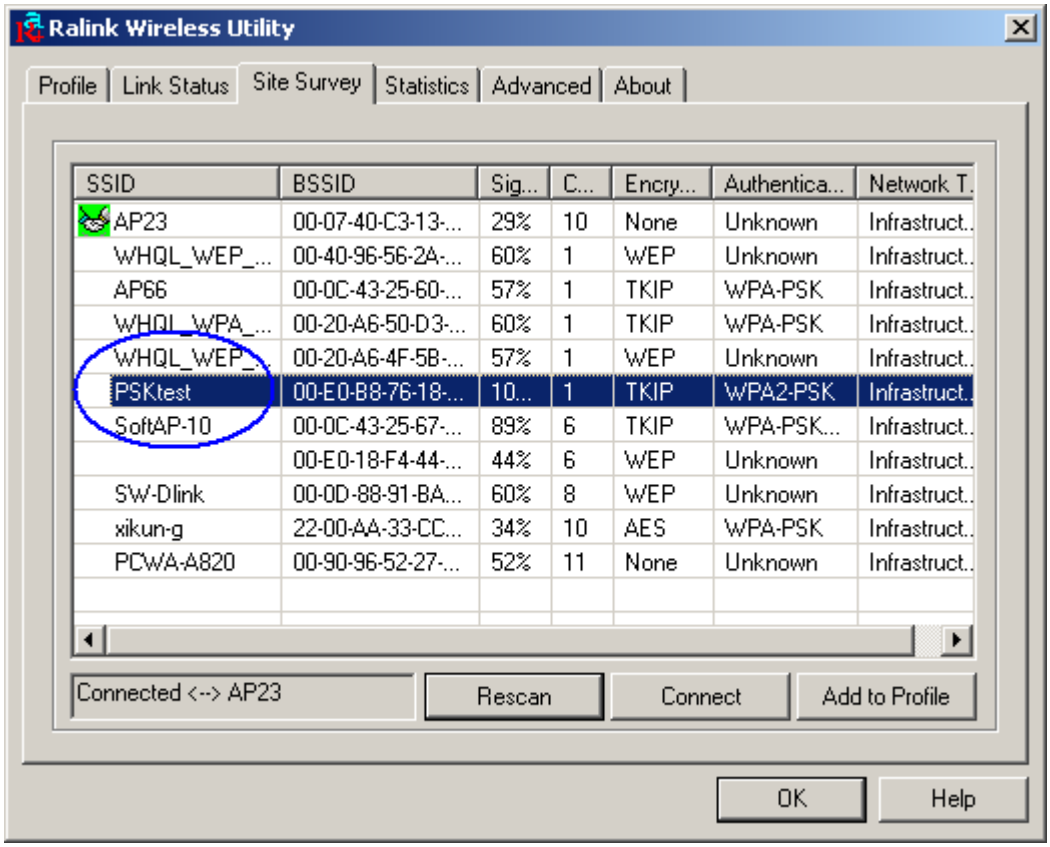


2. Click OK. The result will look like the below figure.

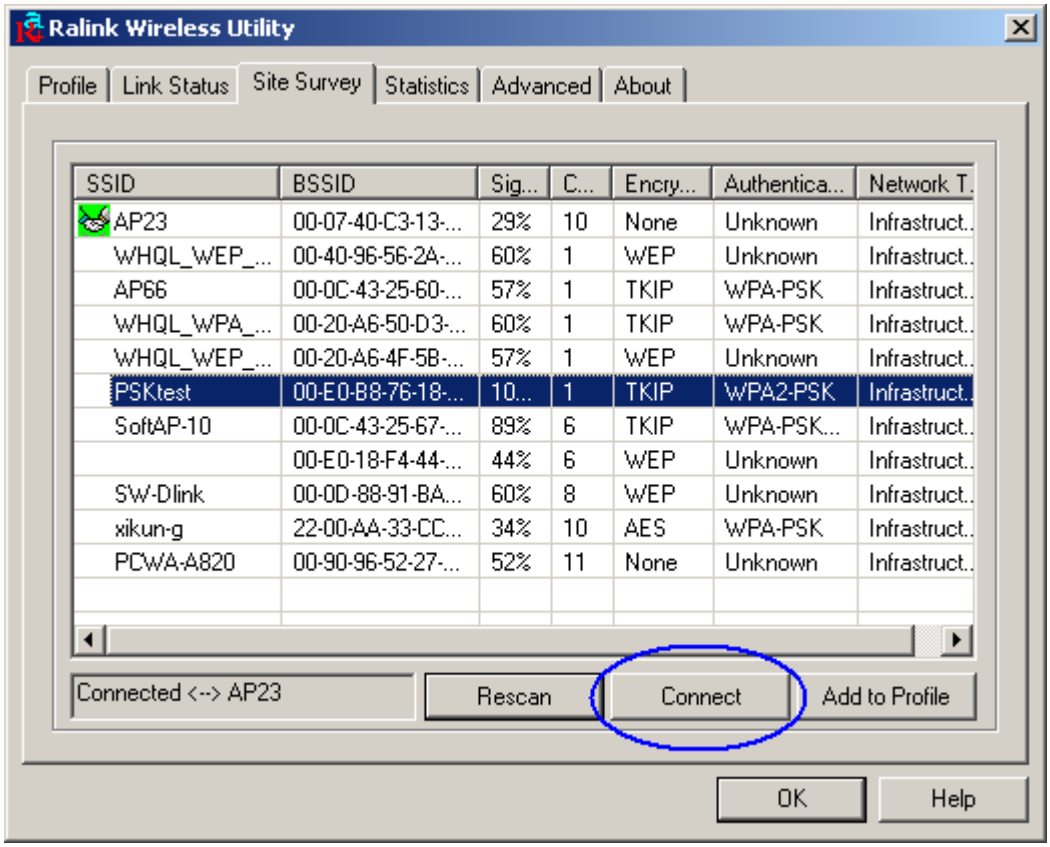


Configure connection with WPA2-PSK

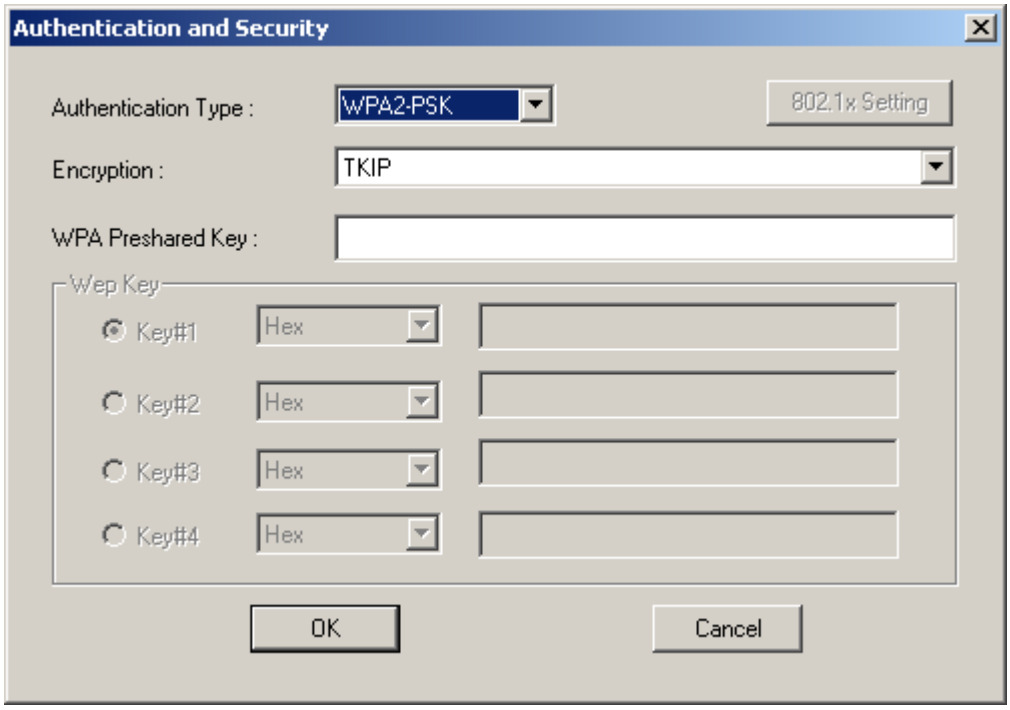
1. Select the AP with WPA2-PSK authentication mode.



2. Click CONNECT or double click the intended network.

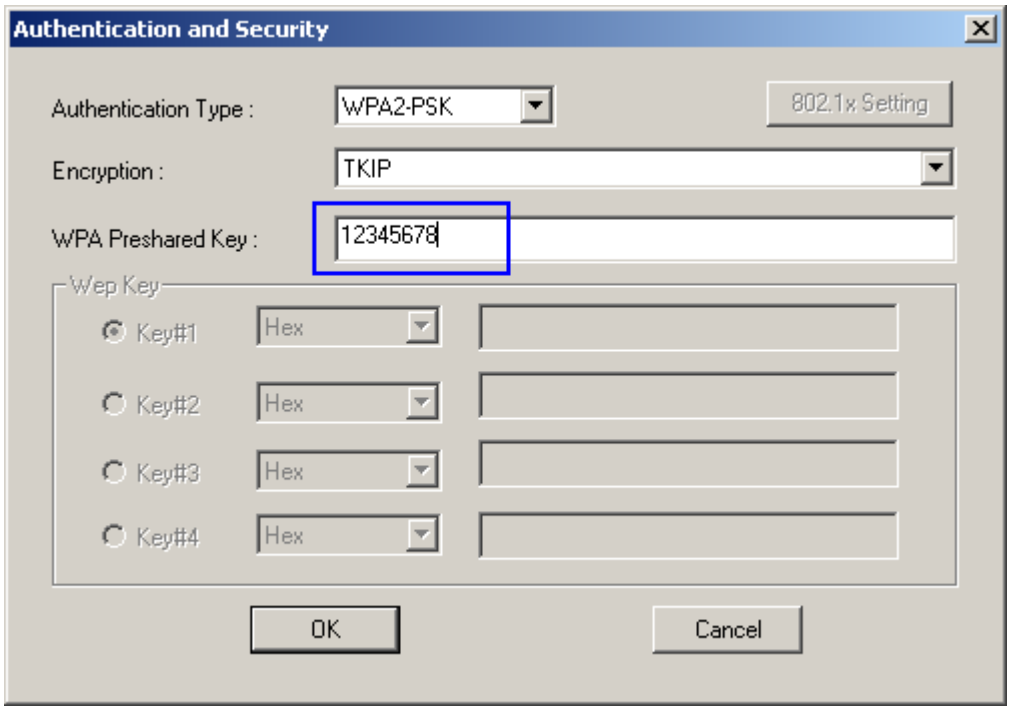


6. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

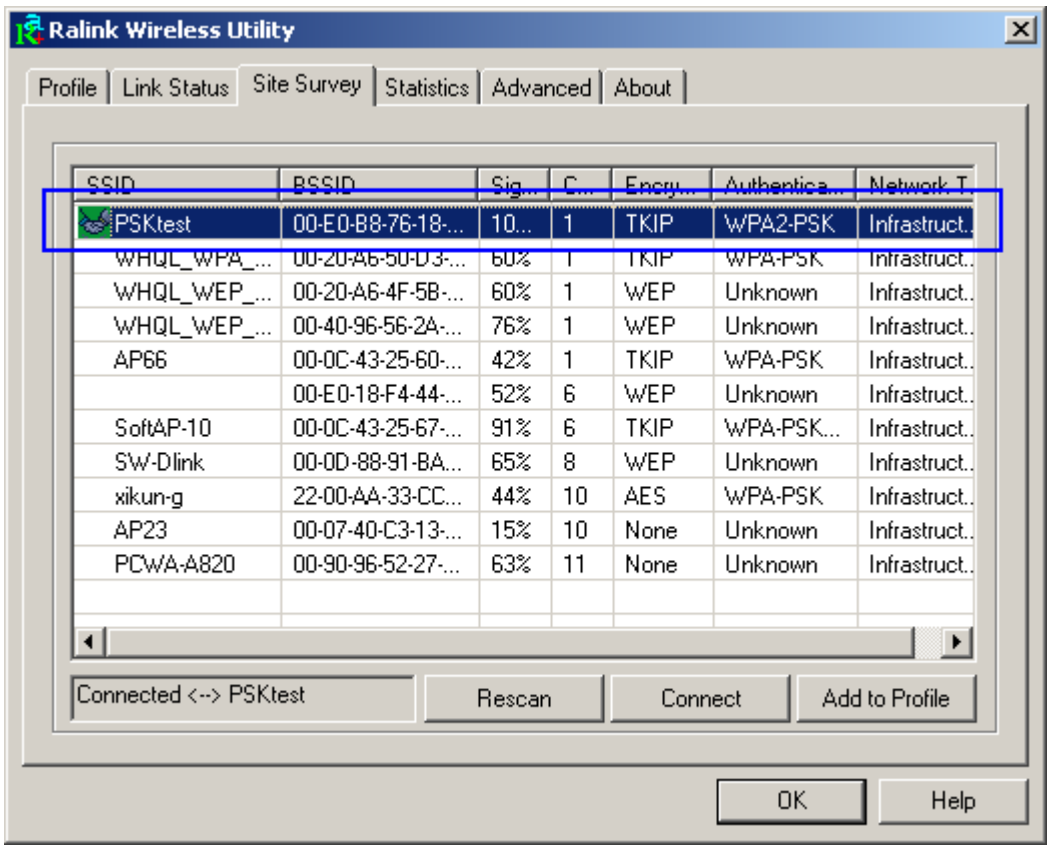


*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

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

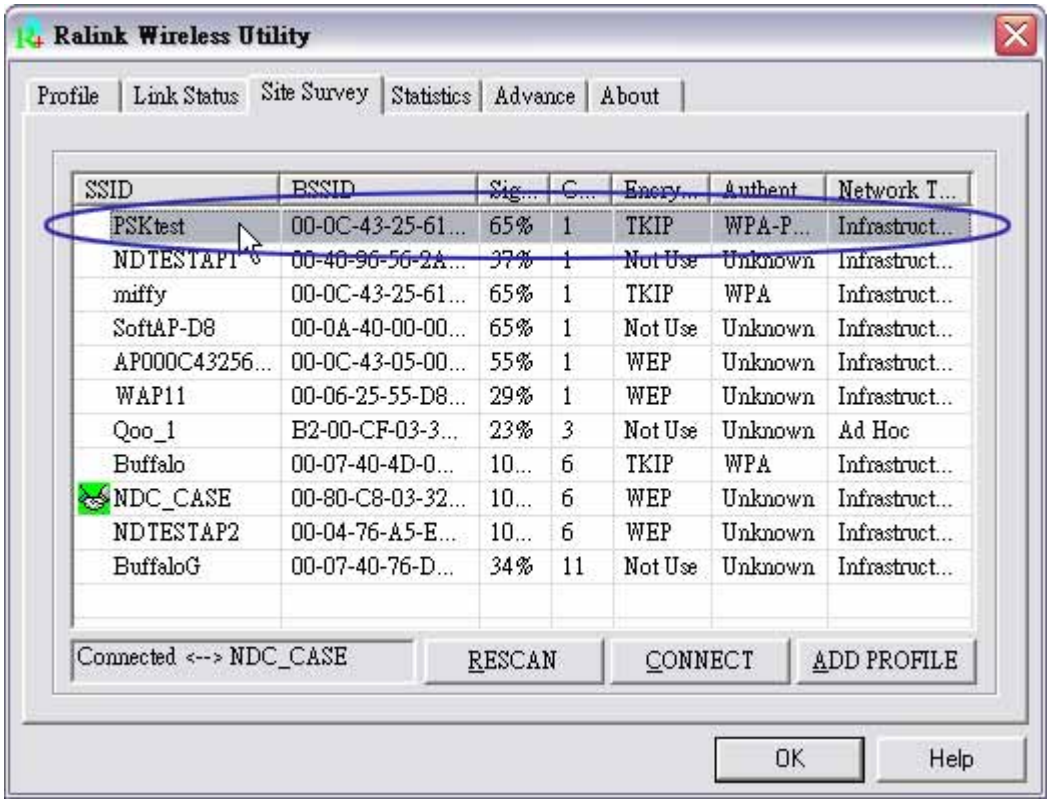


8. Click OK. Be careful, if the WPA Pre-Shared Key entered is not correct, even though the AP can be connected, but you won't be able to exchange any data frames.

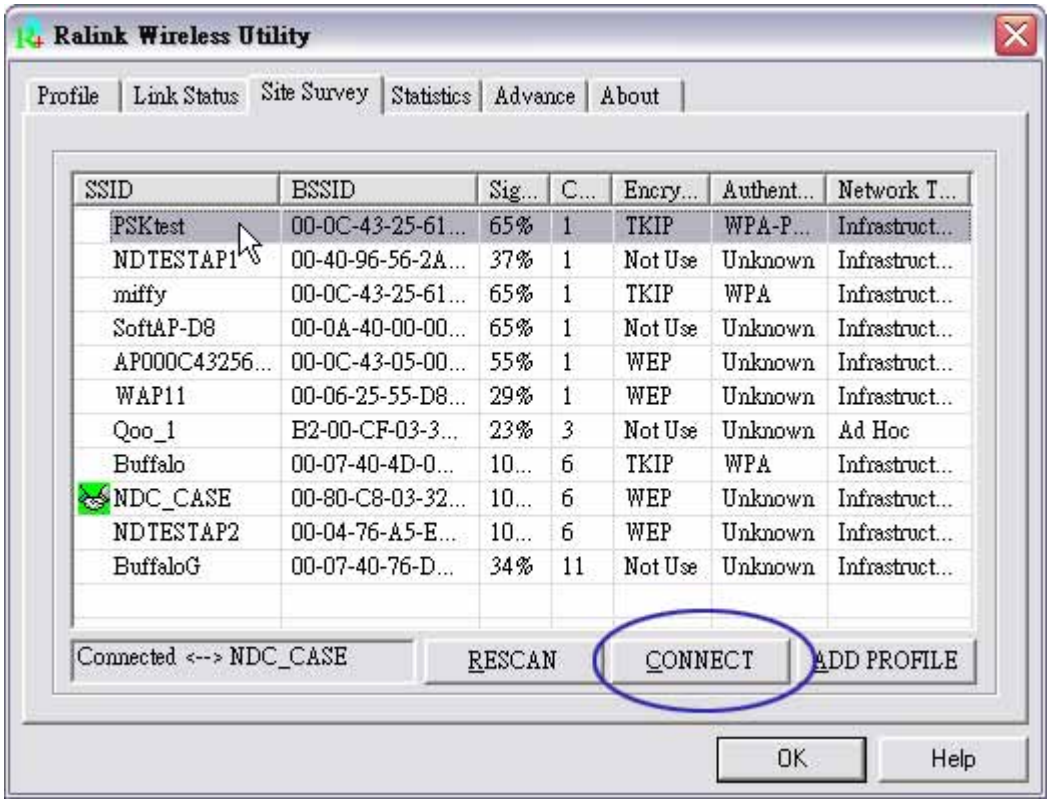


Configure connection with WPA-PSK

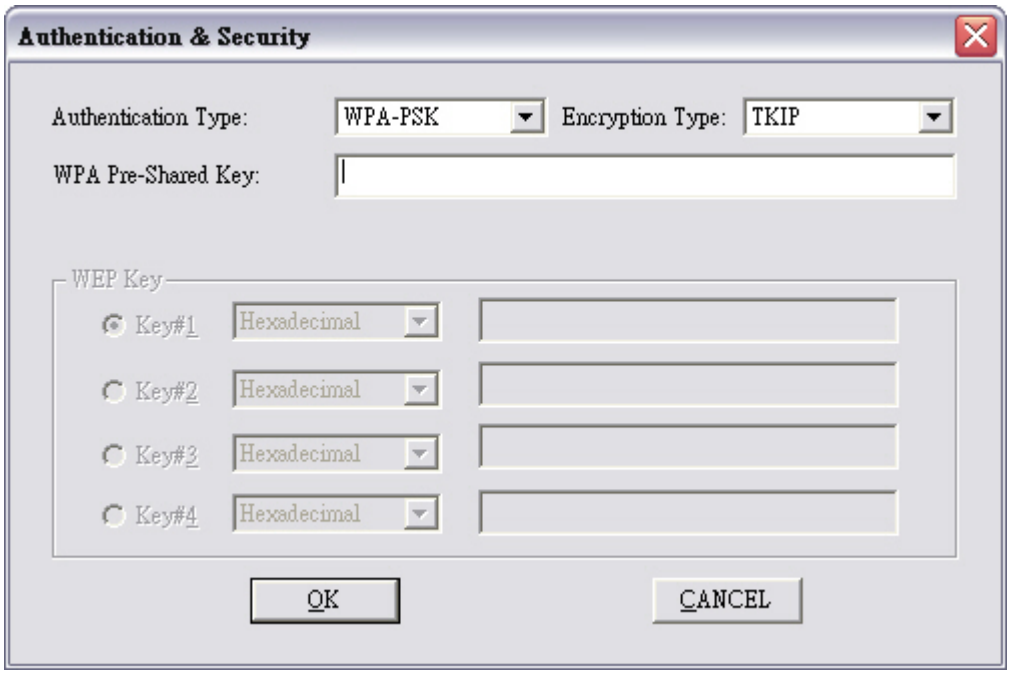
1. Select the AP with WPA-PSK authentication mode.



2. Click CONNECT or double click the intended network.

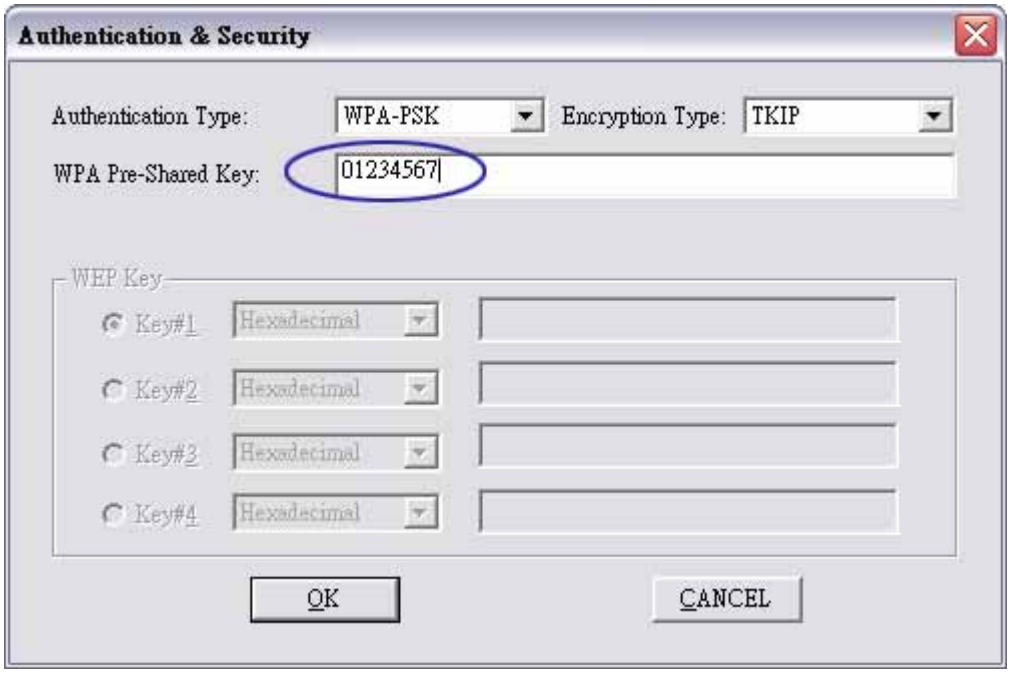


3. Authentication & Security page will pop up. TKIP, AES and Both (TKIP+AES) security are support.

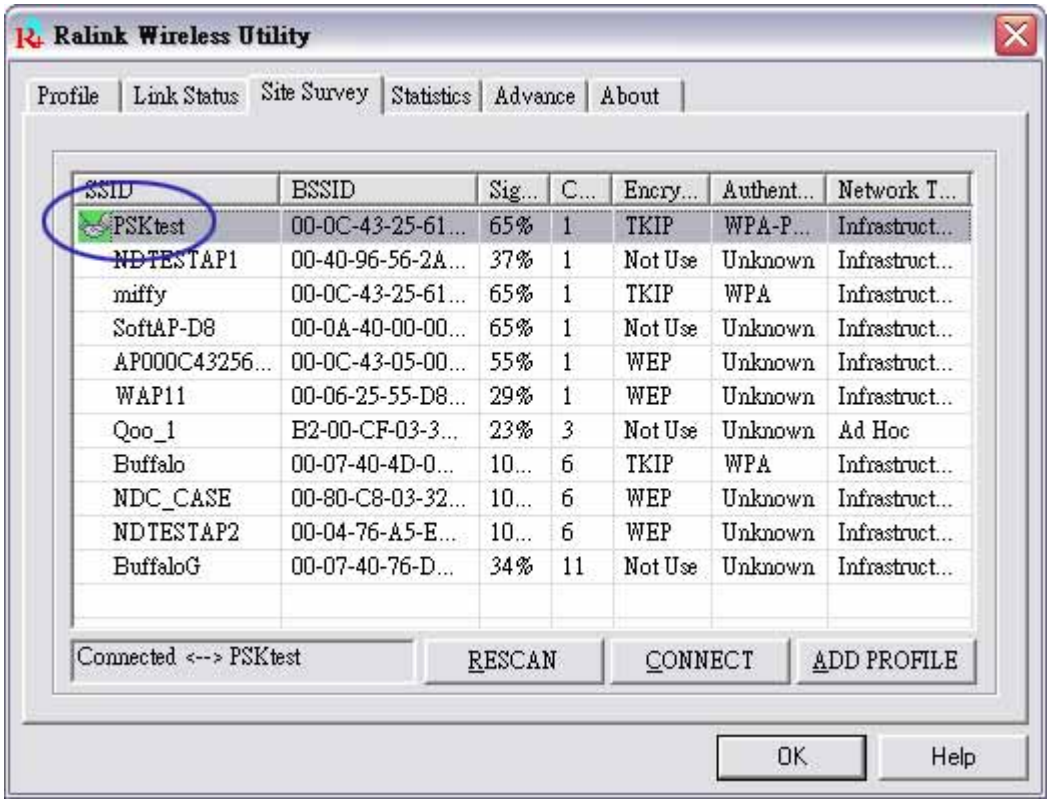


*If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.

4. Authentication Type is WPA-PSK. Select correct encryption (TKIP or AES). Enter WPA Pre-Shared Key secret as 01234567.

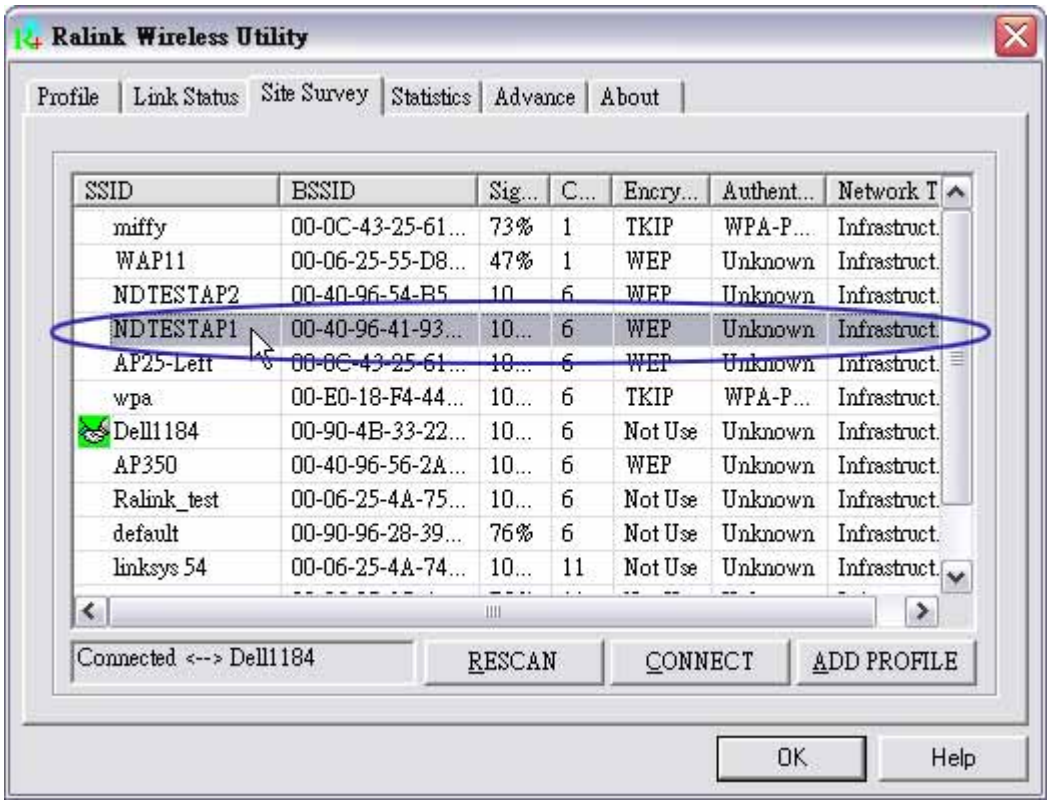


5. Click OK. Be careful, if the WPA Pre-Shared Key entered is not correct, even though the AP can be connected, but you won't be able to exchange any data frames.

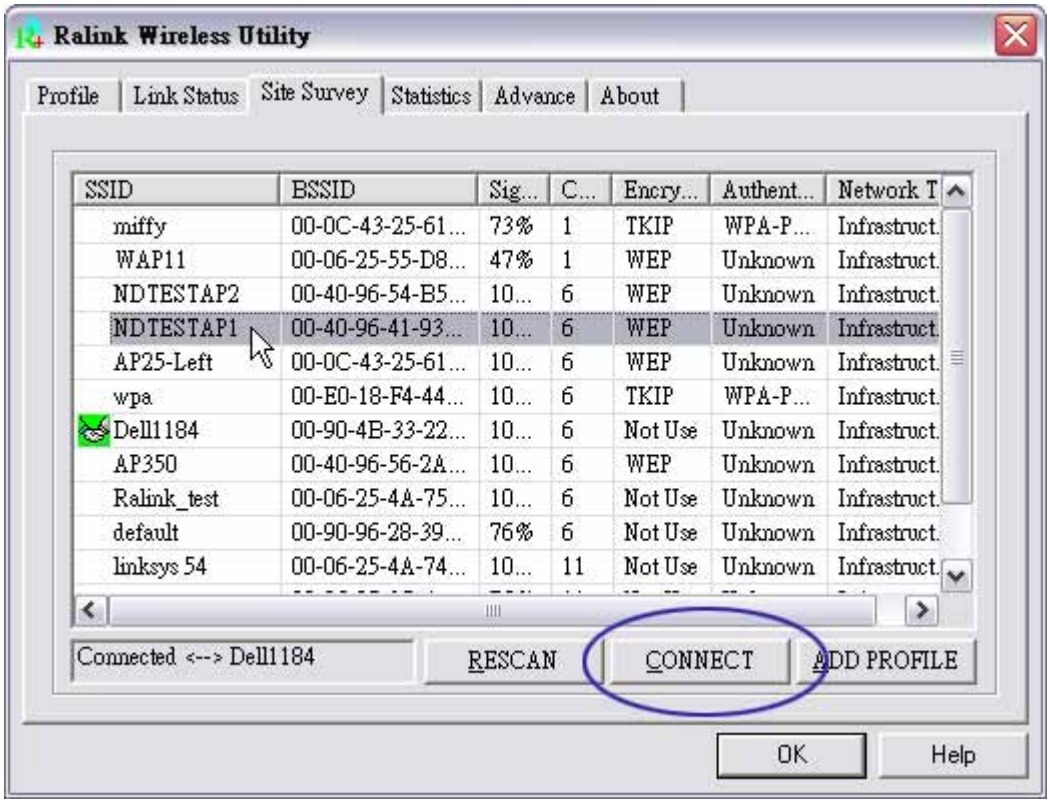


Configure connection with WEP on

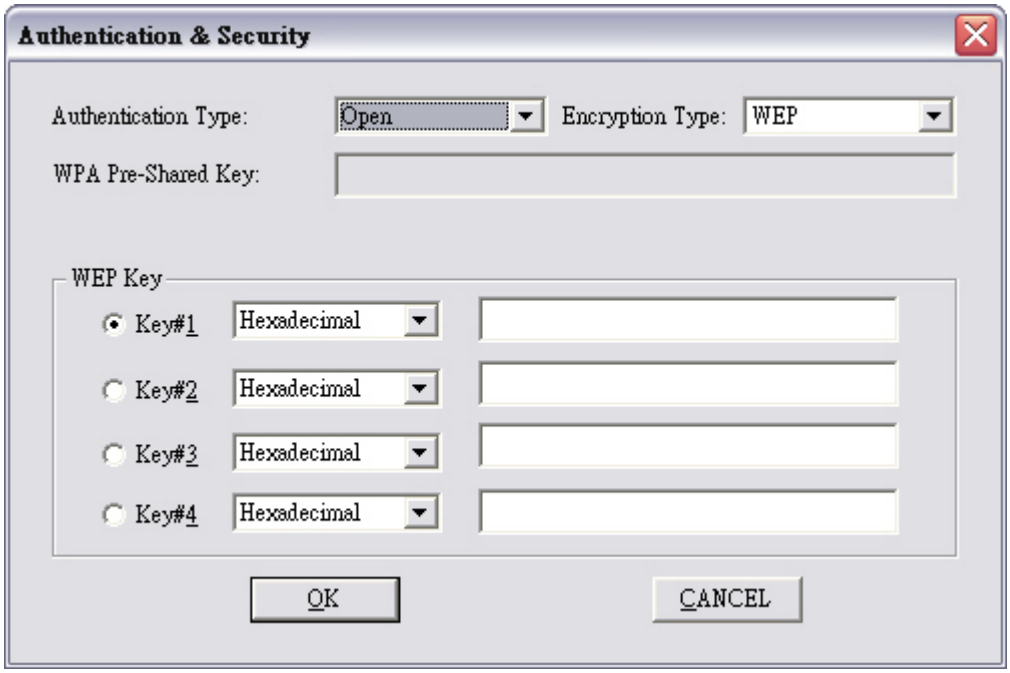
1. Select AP with WEP encryption.



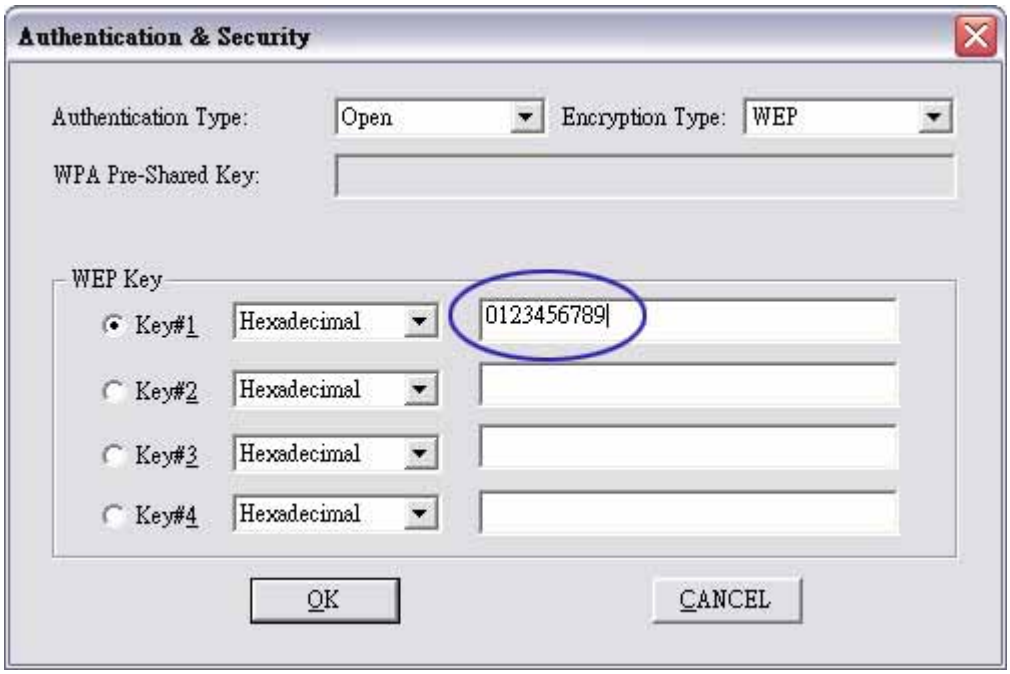
2. Click CONNECT or double click intended network.



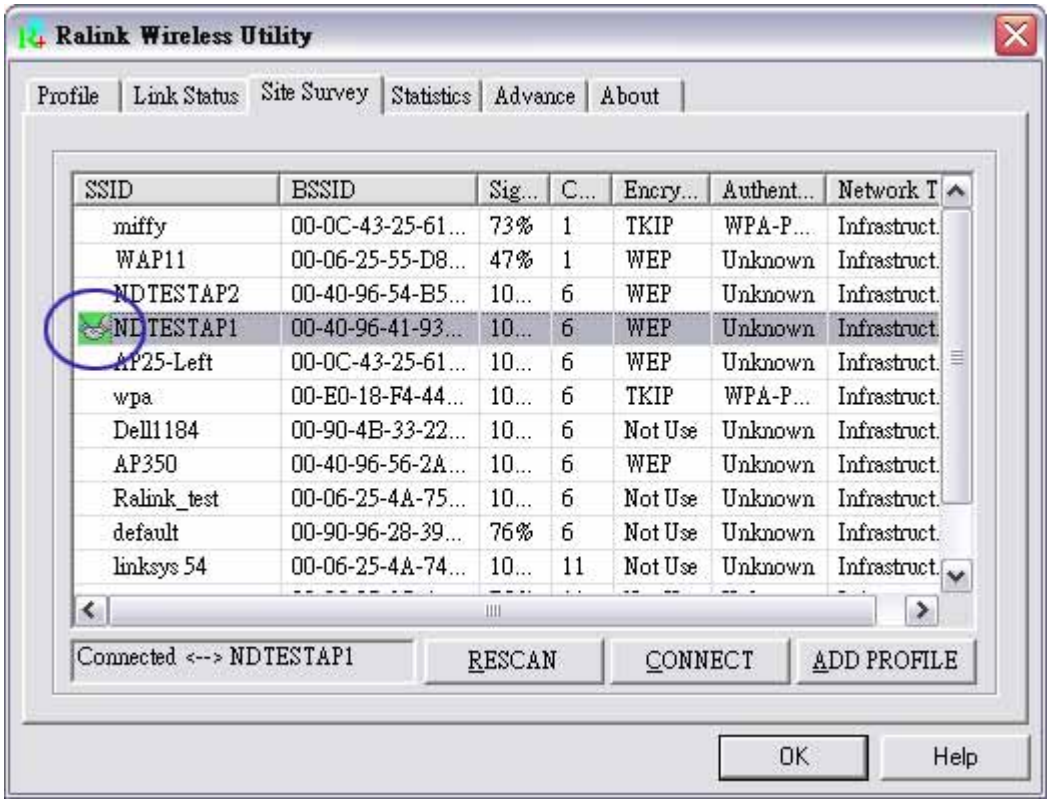
3. Authentication & Security page pop up.



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

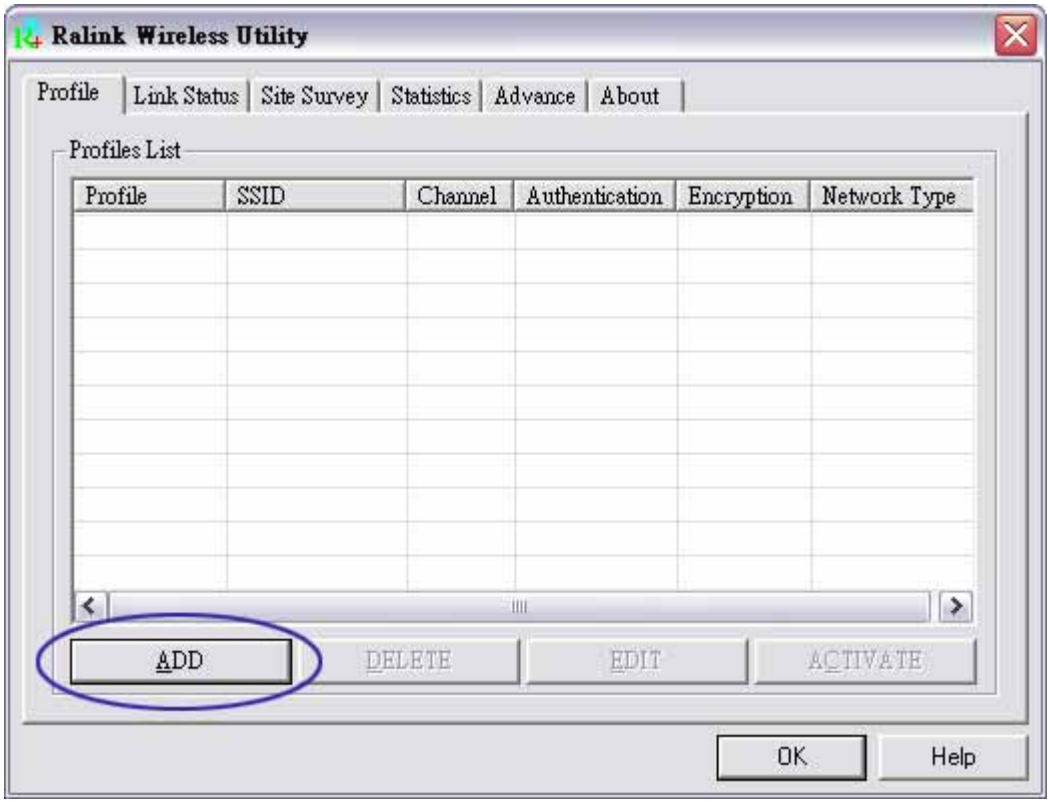


5. Click OK. The result will look like the below figure.

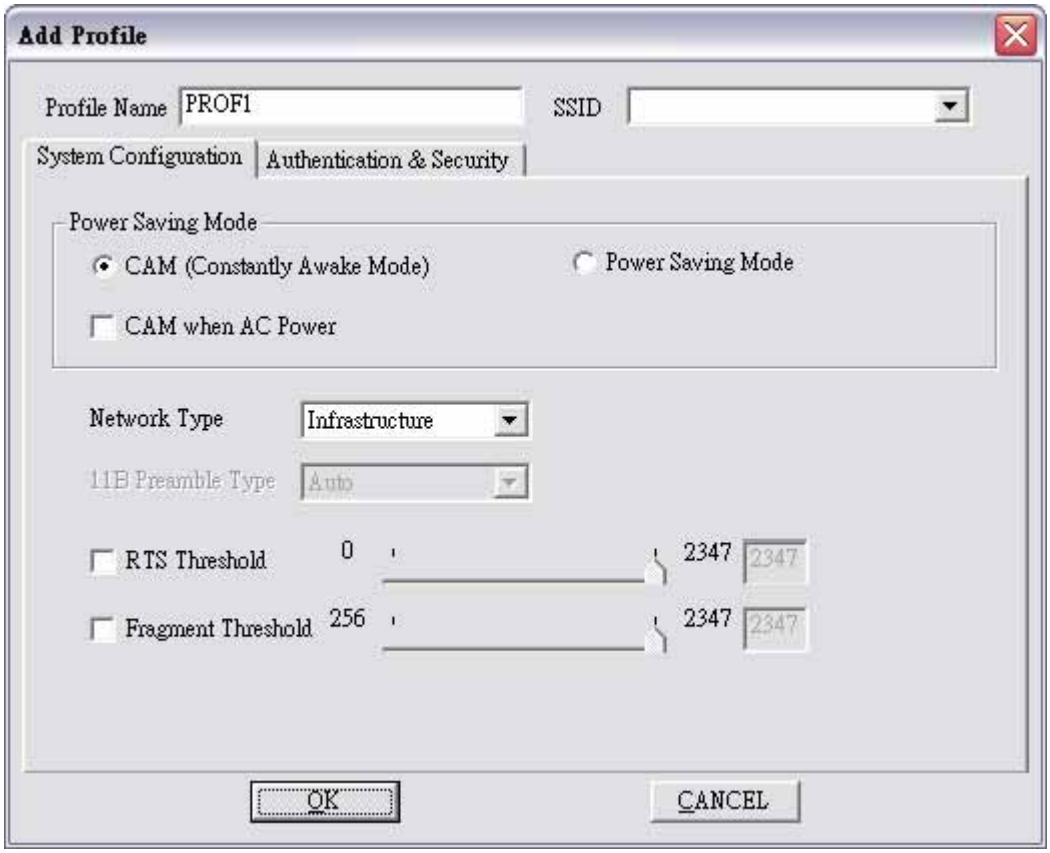

Ralink Wireless Utility
Profile
Link Status
Site Survey
Statistics
Advance
About
SSID
BSSID
Sig...
C...
Encry...
Authent...
Network T
miffy 00-0C-43-25-61... 73% 1 TKIP WPA-P... Infrastruct.
WAP11 00-06-25-55-D8... 47% 1 WEP Unknown Infrastruct.
NDTESTAP2 00-40-96-54-B5... 10... 6 WEP Unknown Infrastruct.
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.
Connected <--> NDTESTAP1
RESCAN
CONNECT
ADD PROFILE
OK
Help

Example to add profile in profile page

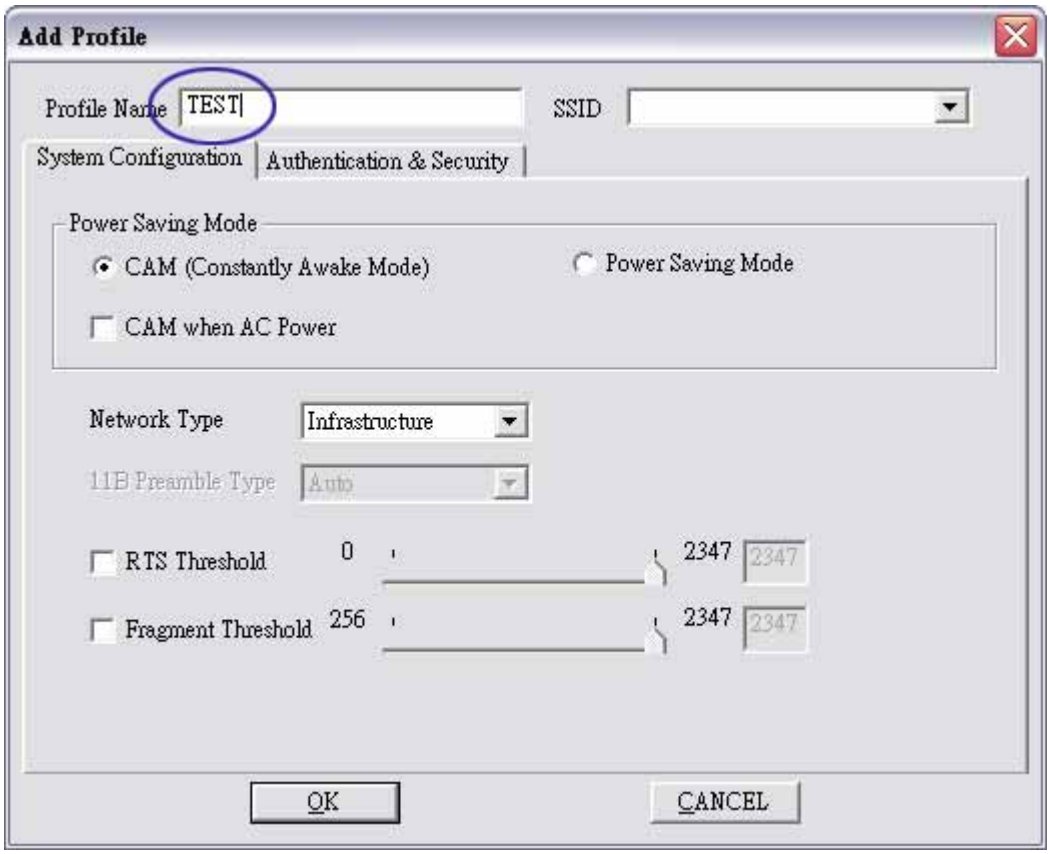
1. Click ADD in profile page



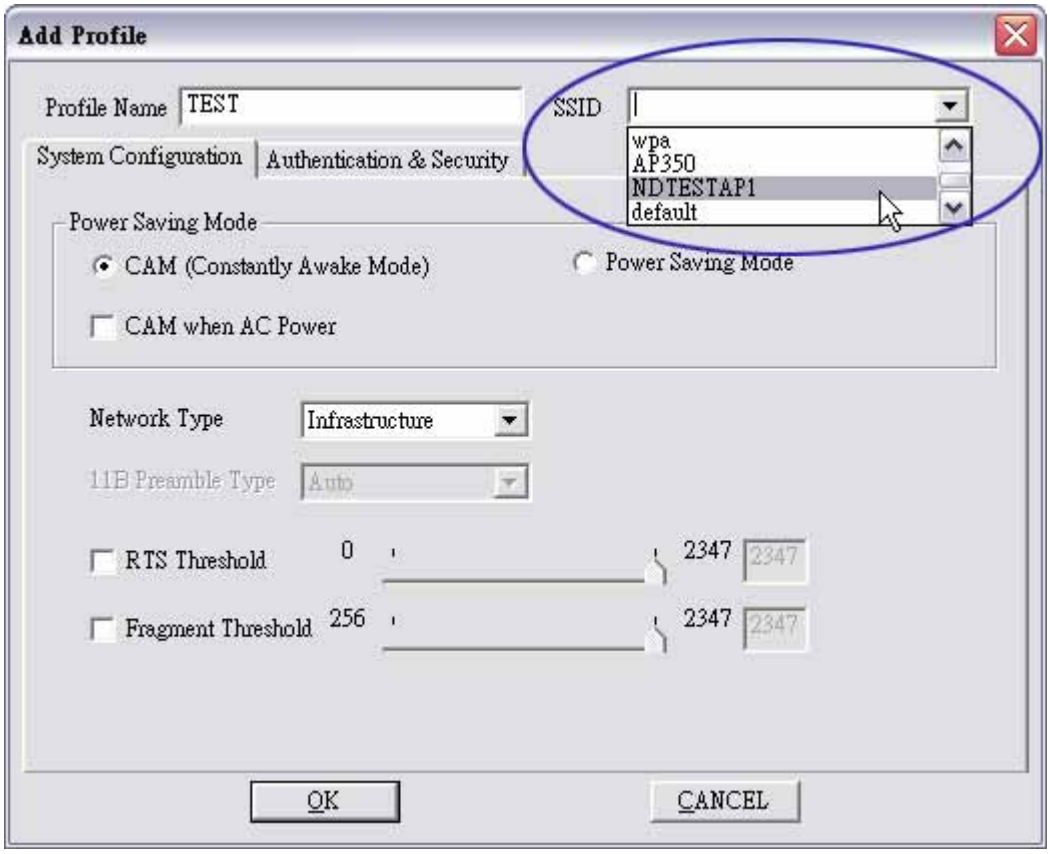
2. Add Profile page will pop up



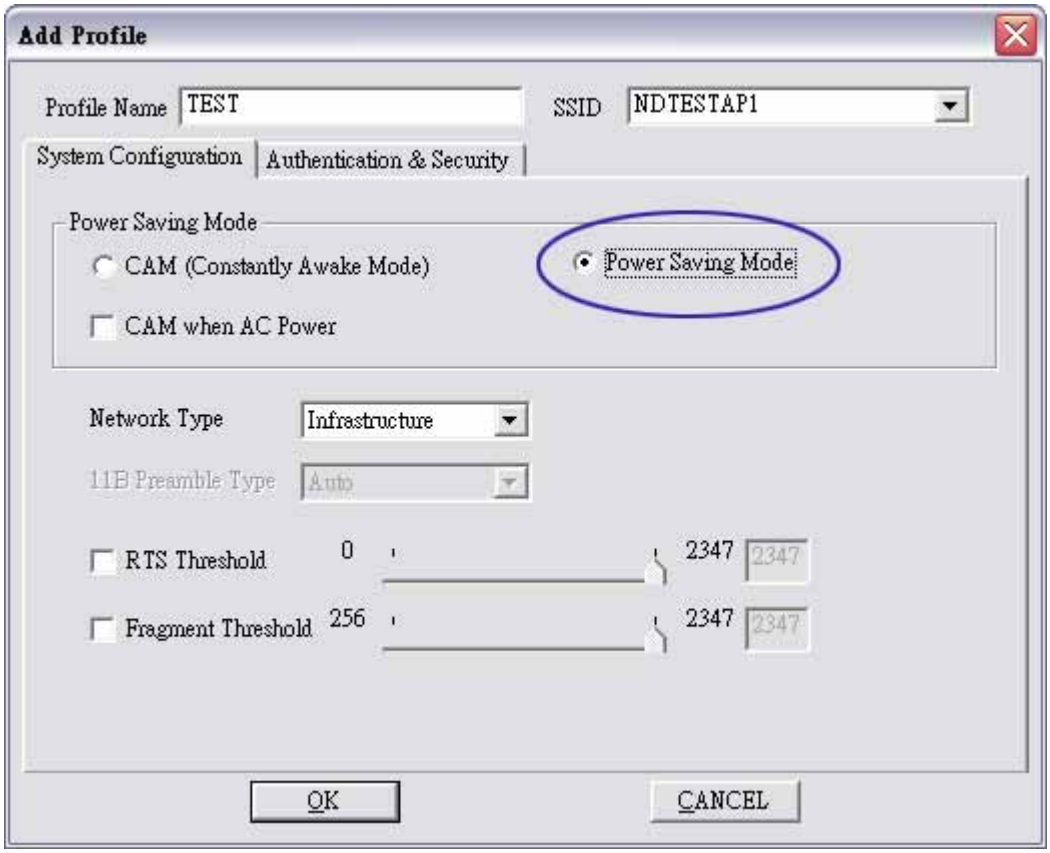
3. Change profile name to TEST.



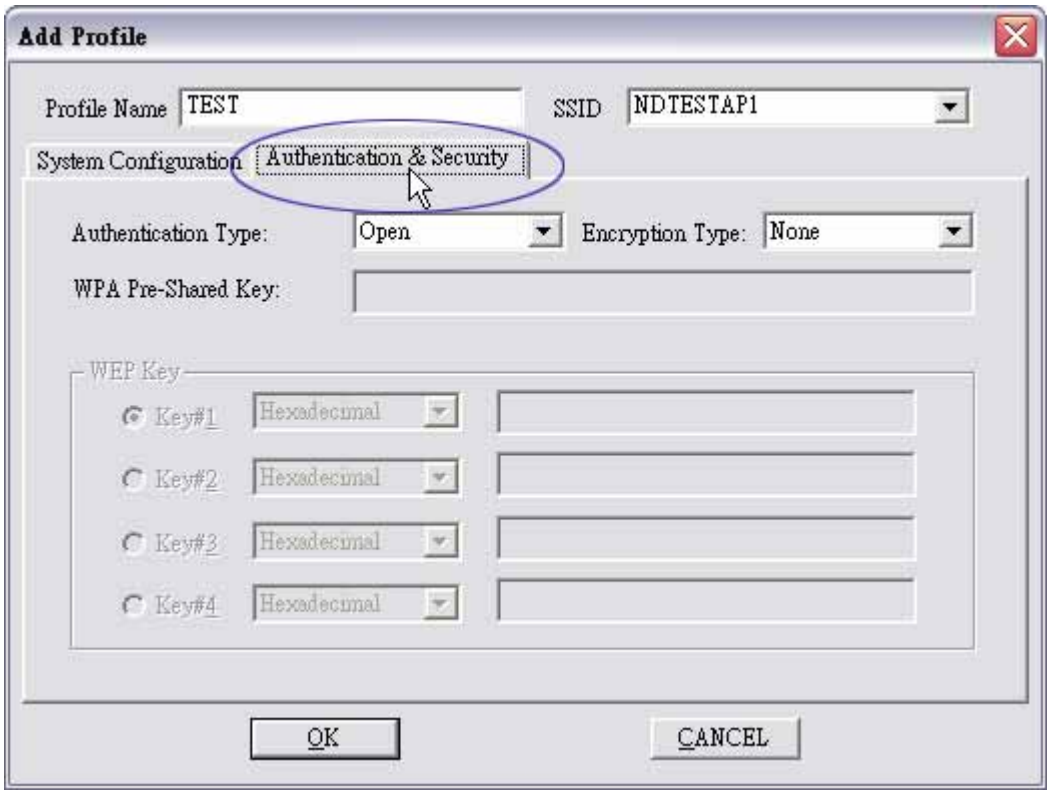
4. Pull down SSID and select one intended AP. The AP list is the result of last site survey.



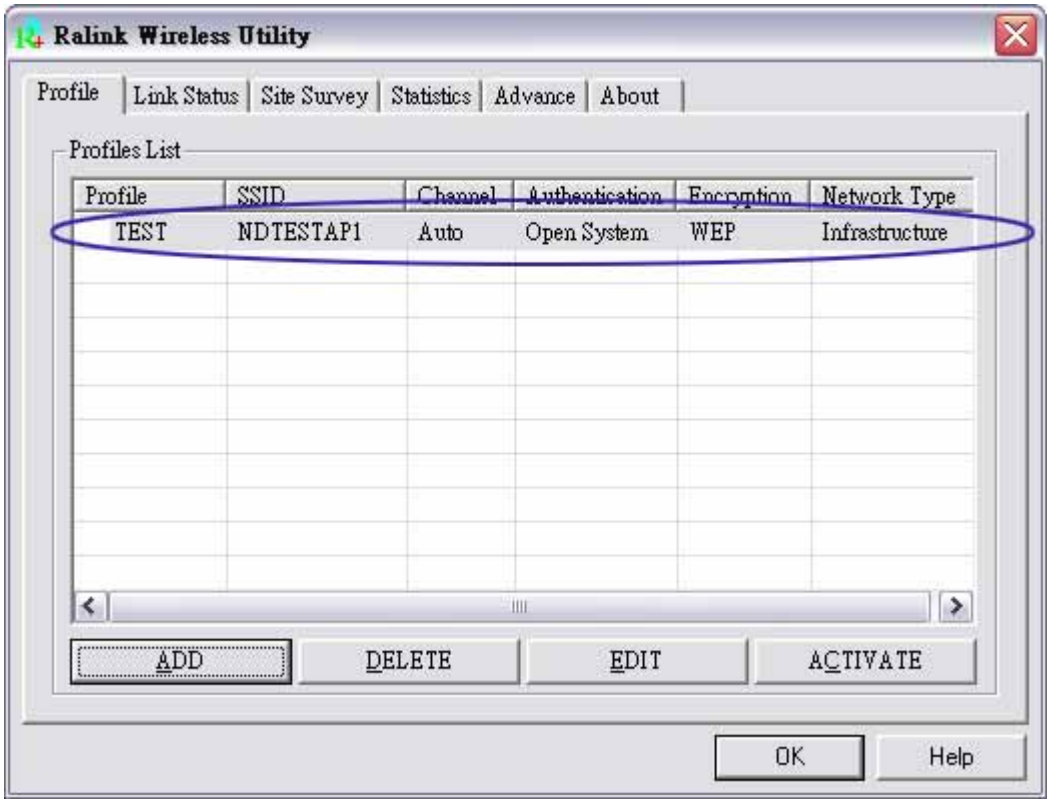
5. Set Power Saving Mode.



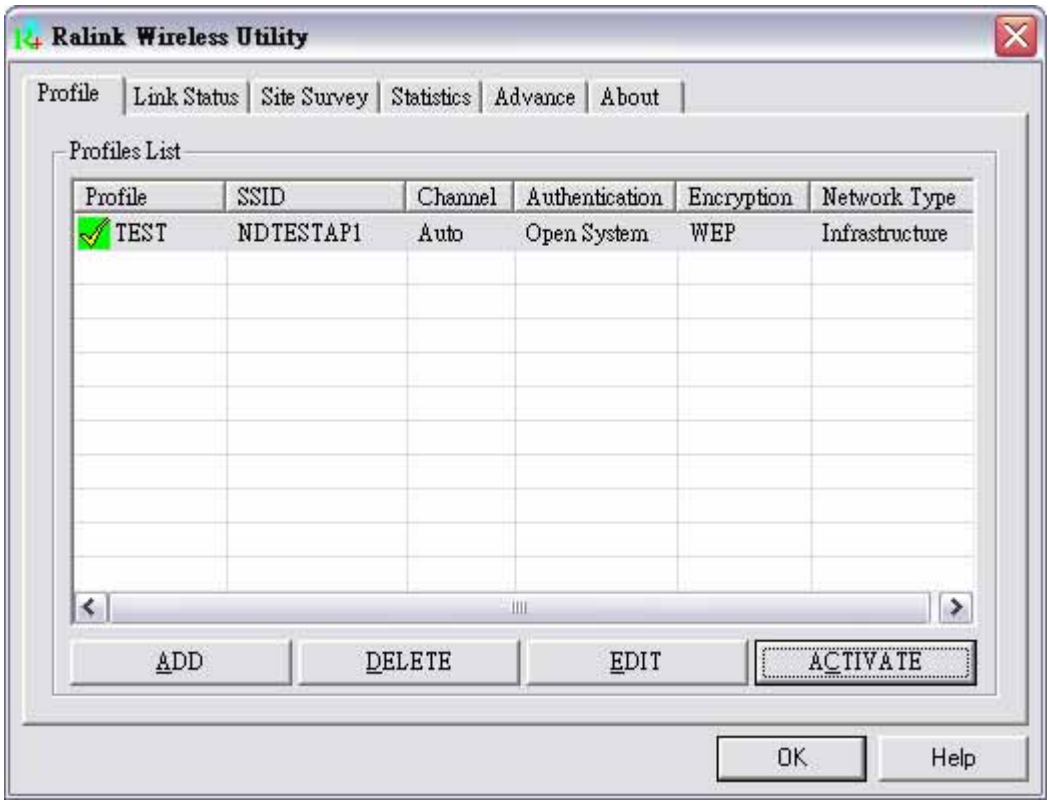
6. Click Authentication & Security page



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



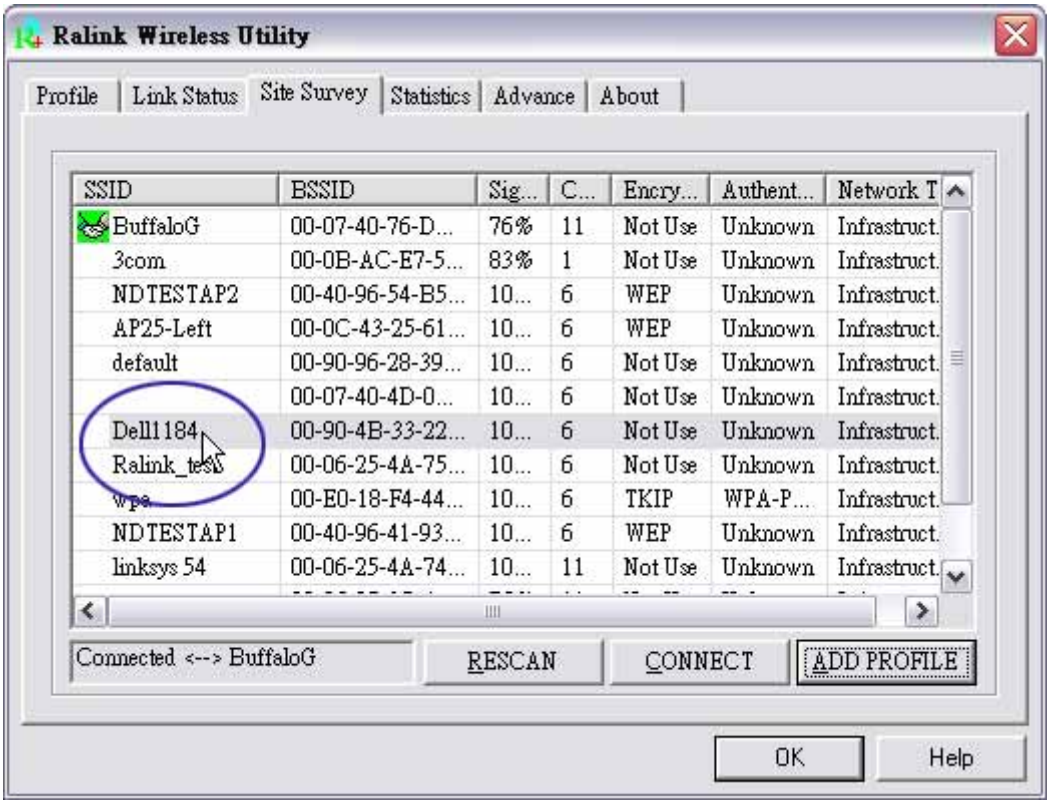
8. Click ACTIVATE. Activate the profile setting.



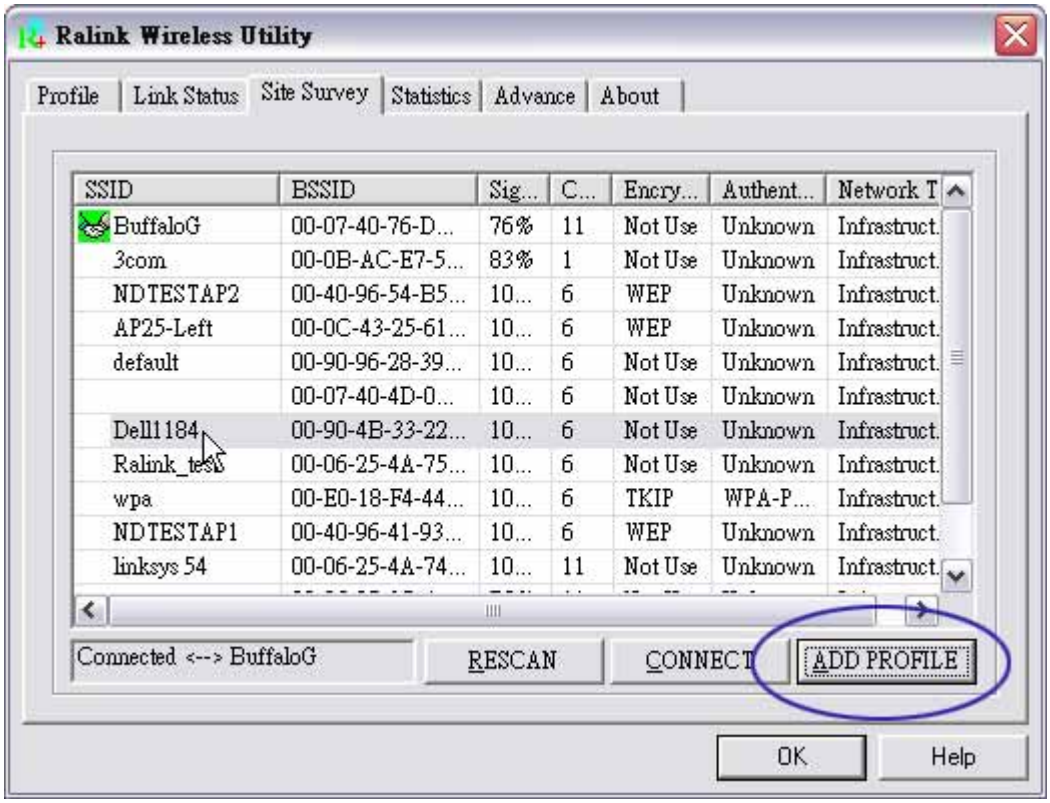
9. Follow section 12, section 13 and section 14 to set authentication and security page.

Example on adding profile in site survey page

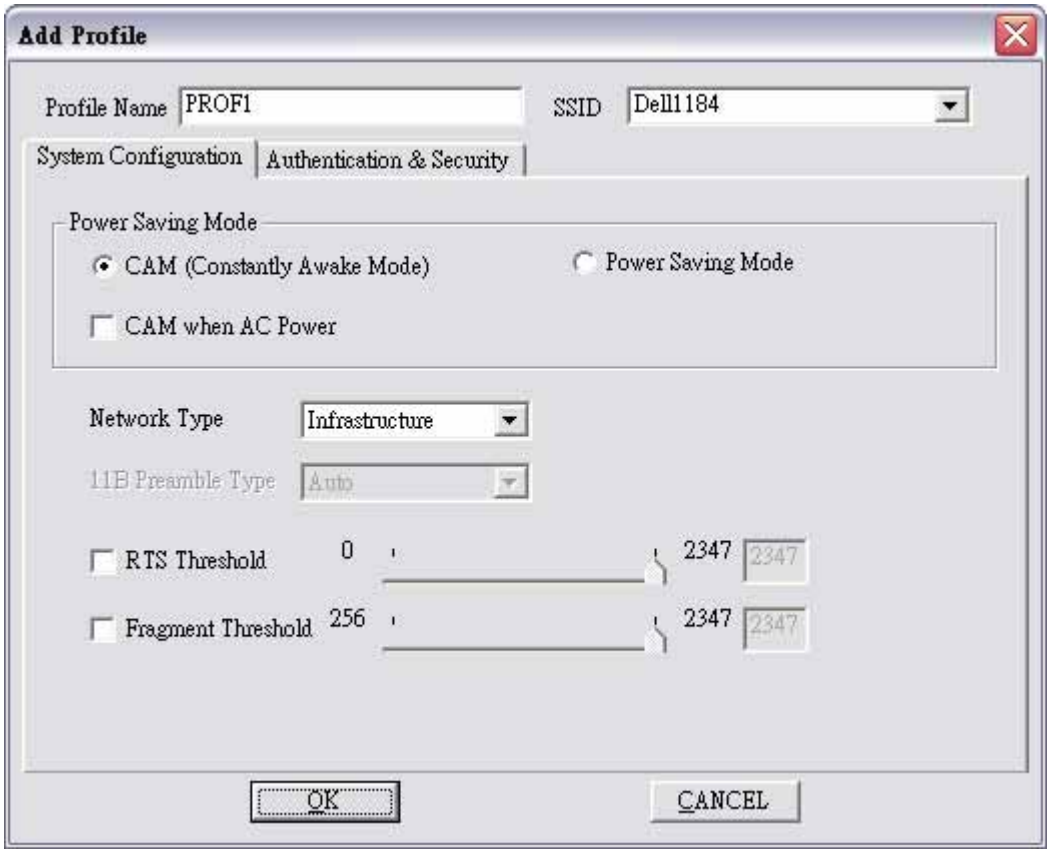
1. Select the indented network from site survey list.



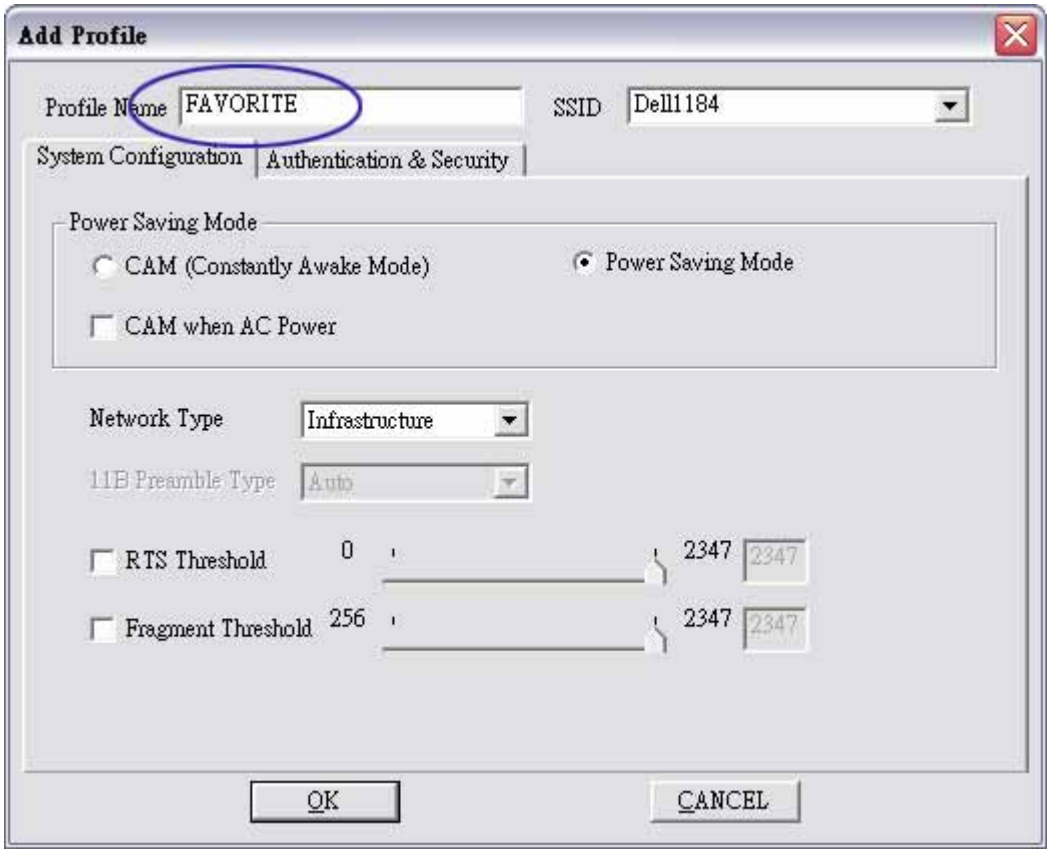
2. Click ADD PROFILE.



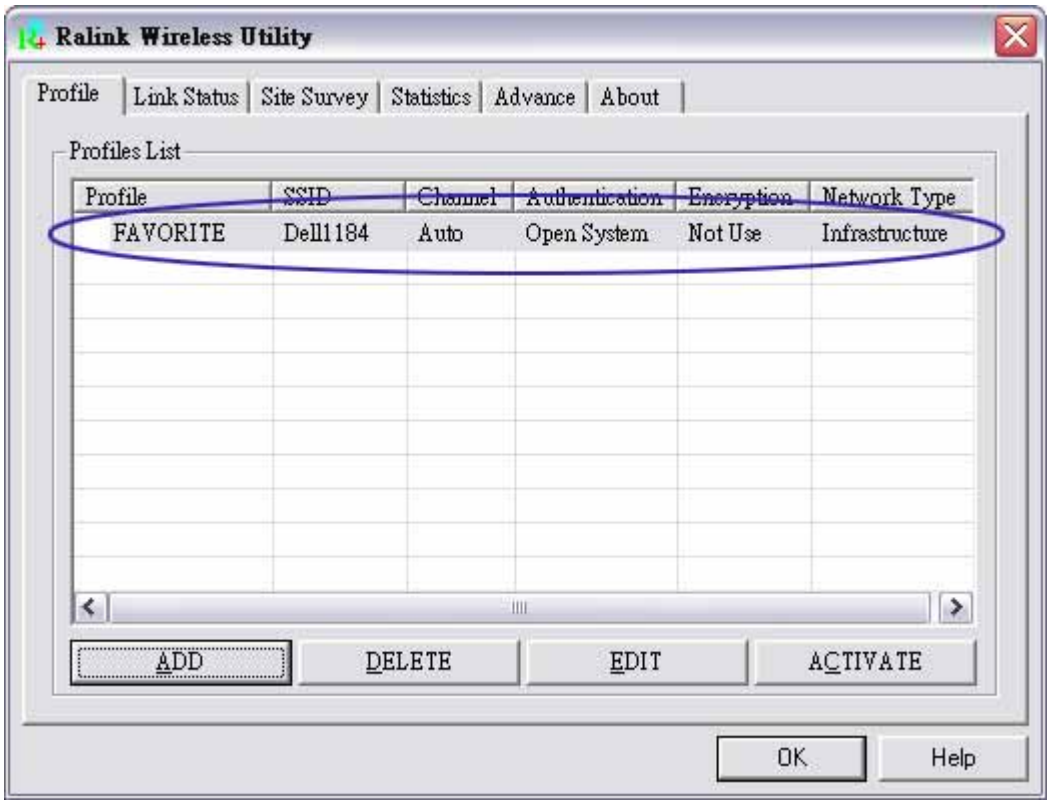
3. System will pop up Add Profile windows



4. Change profile Name from PROF1 to FAVORITE.



5. Click OK without changing other value.



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

About

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

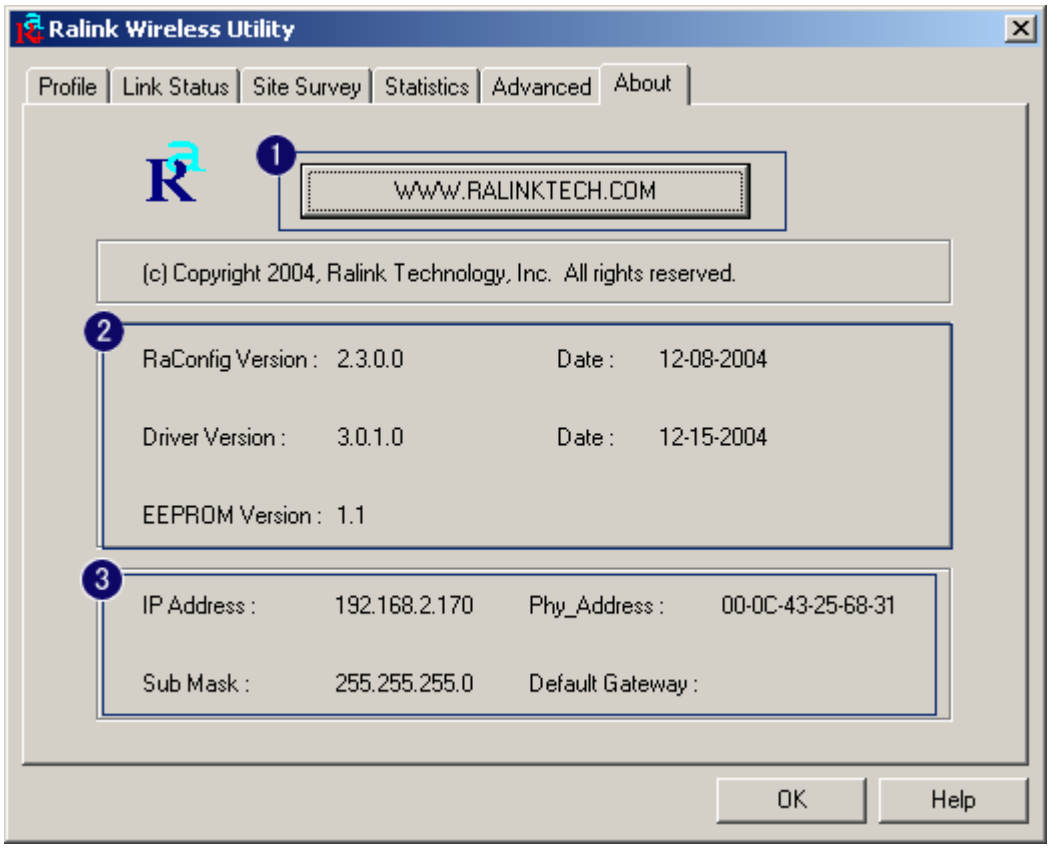


Figure 9-1 About Page

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

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

3 Display 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:

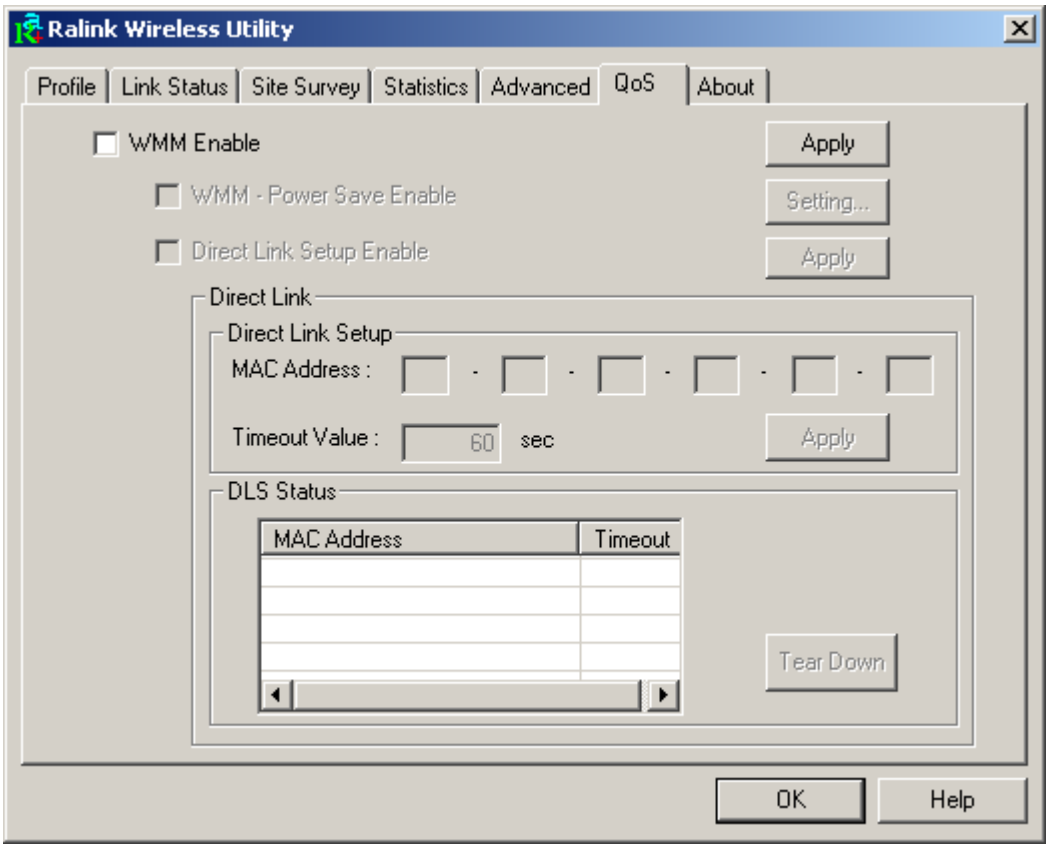


Figure 10-1 QoS Page

1. WMM Enable: Enable Wi-Fi Multi-Media. The setting method follows section 17.
2. WMM – Power Save Enable: Enable WMM Power Save. The setting method follows section 18.
3. Direct Link Setup Enable: Enable DLS (Direct Link Setup). The setting method follows section 19.

Country Channel List

Country channel list, channel classification and range.

According to your window, find out corresponding table.

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

Classification	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
Lebanon	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1~13
Luxembourg	1	CH1~13
Macedonia	1	CH1~13
Malaysia	1	CH1~13
Mexico	0	CH1~11
Morocco	1	CH1~13
Netherlands	1	CH1~13
New Zealand	1	CH1~13
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

Figure 8-1 shows advance setting page of RaConfig

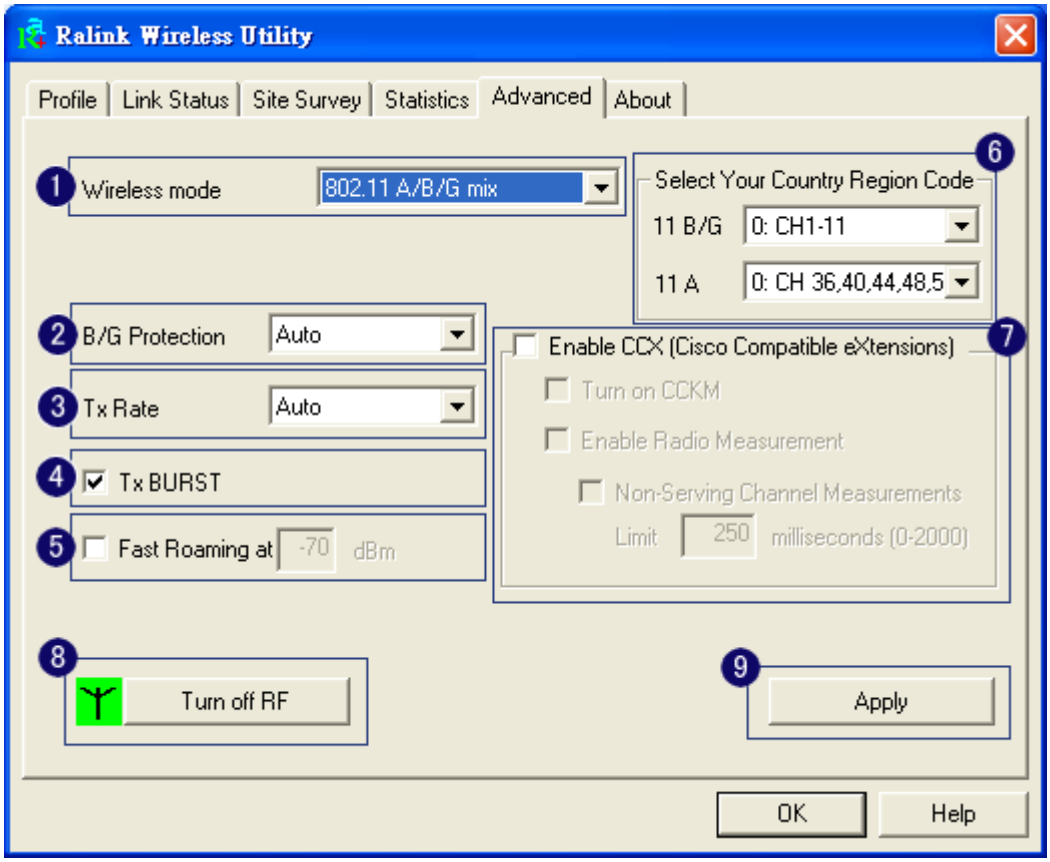


Figure 8-1 Advance setting

1 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.

2 11B/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.

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

4 TX Burst: Ralink's proprietary frame burst mode.

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

6 Select Your Country Region Code: eight countries to choose. Country channel list: Country channel list

7 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.

Radio On: Indicate to turn on radio.

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.

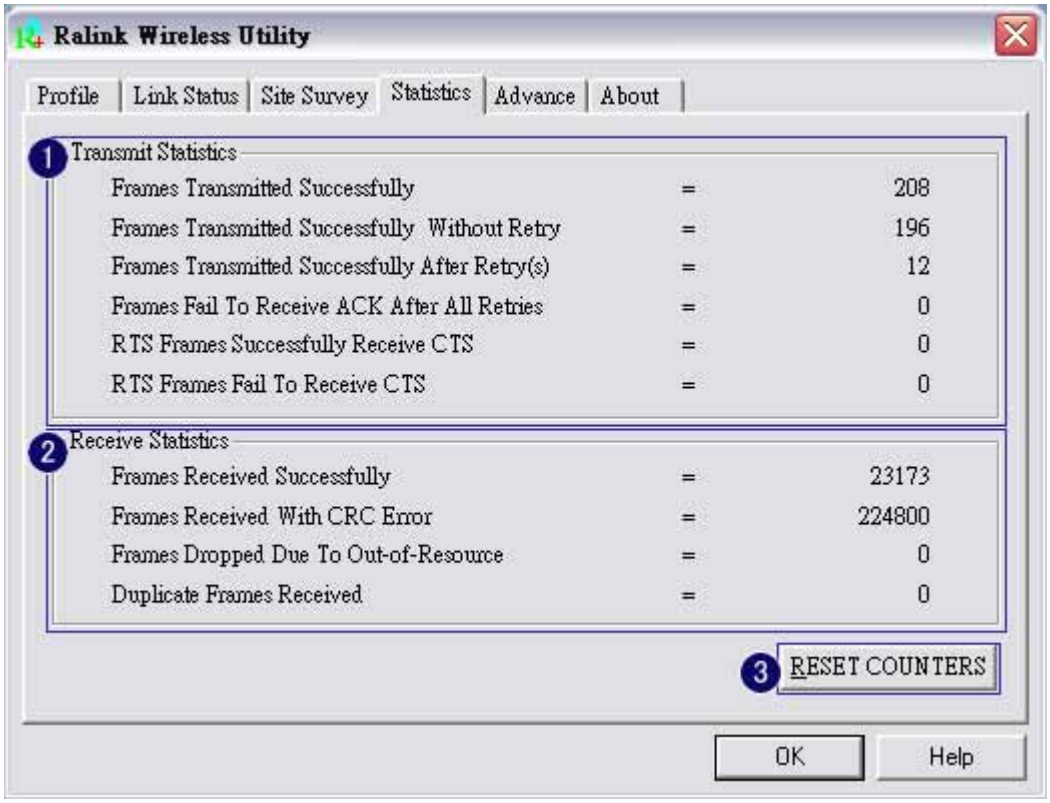


Figure 7-1 Transmit and Receive statistics

1 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.

2 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.

3 Reset counters to zero.

Link Status

Figure 6-1 is the link status page; it displays the detail information current connection.

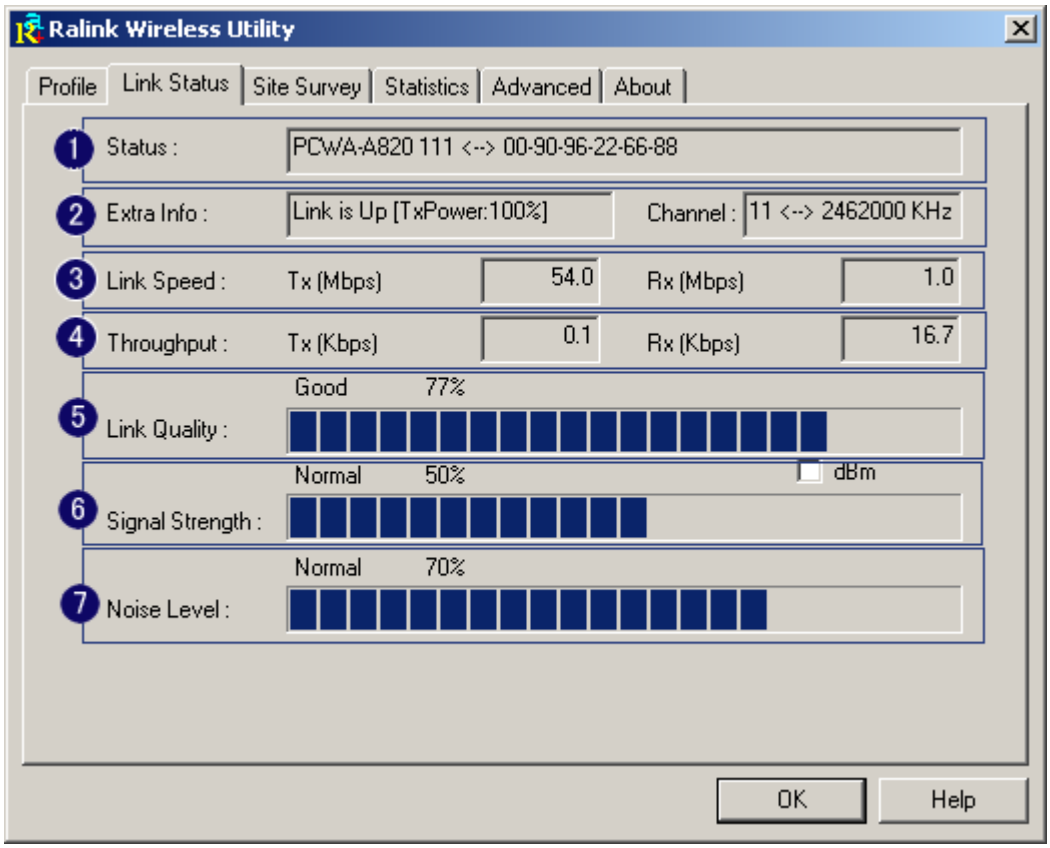


Figure 6-1 Link Status information

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

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

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

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

5 Link 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.

7 Noise Level: Display noise signal 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.

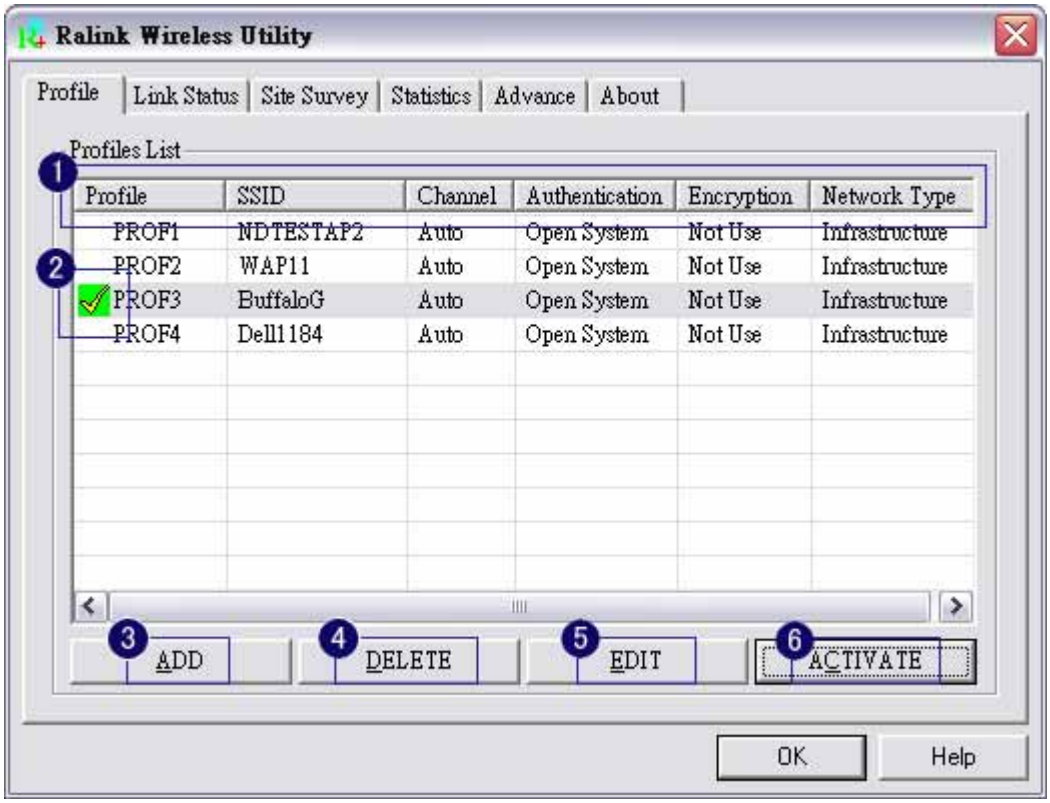


Figure 5-1 Profile page

❶Definition 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.

❷Connection 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.

❸Add a new profile.

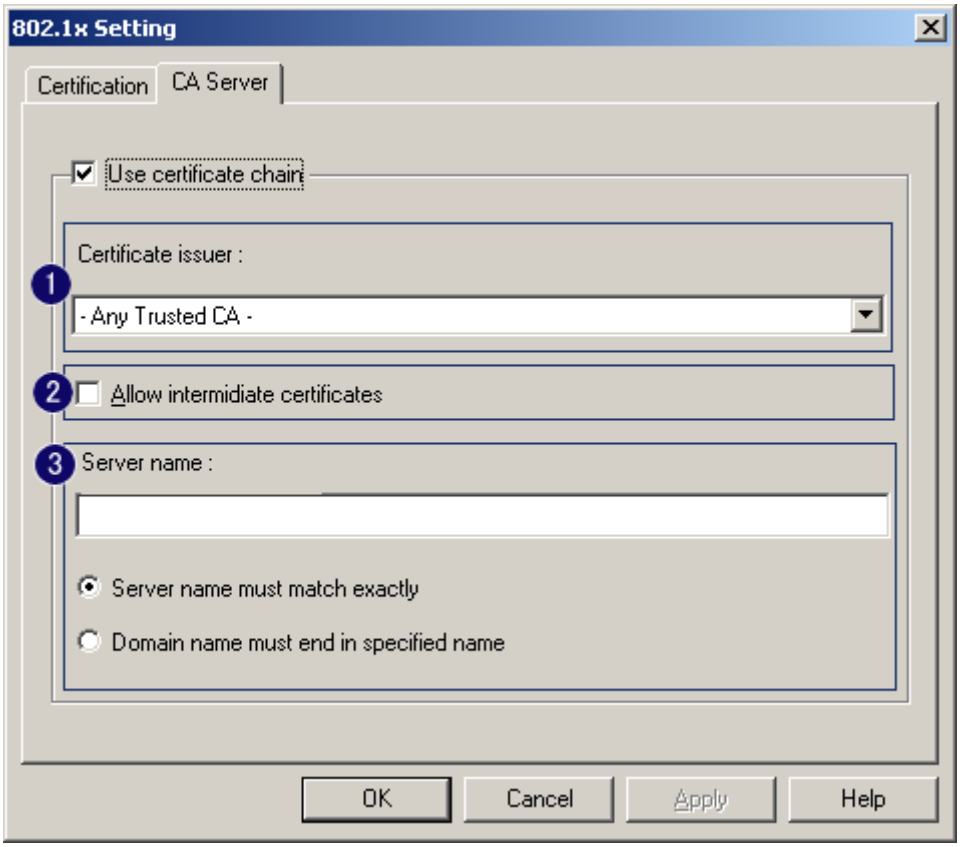
❹Delete an existing profile.

❺Edit Profile.

❻Activate 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.



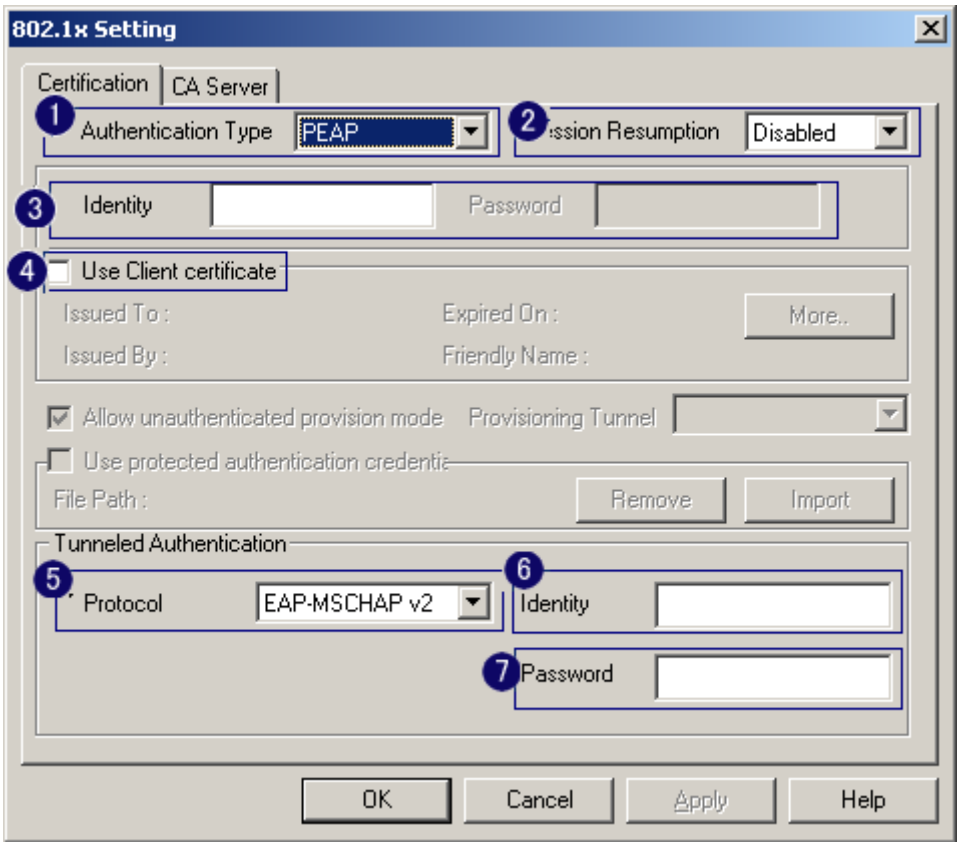
1 Certificate issuer: Choose use server that issuer of certificates.

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

3 Server name: Enter an authentication sever root.

802.1x Setting

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



1 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.

2 Session Resumption: user can choose “ Disable ” and “ Enable ”.

3 Identity and Password: Identity and password for server.

4 Use 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.

6 CA 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

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

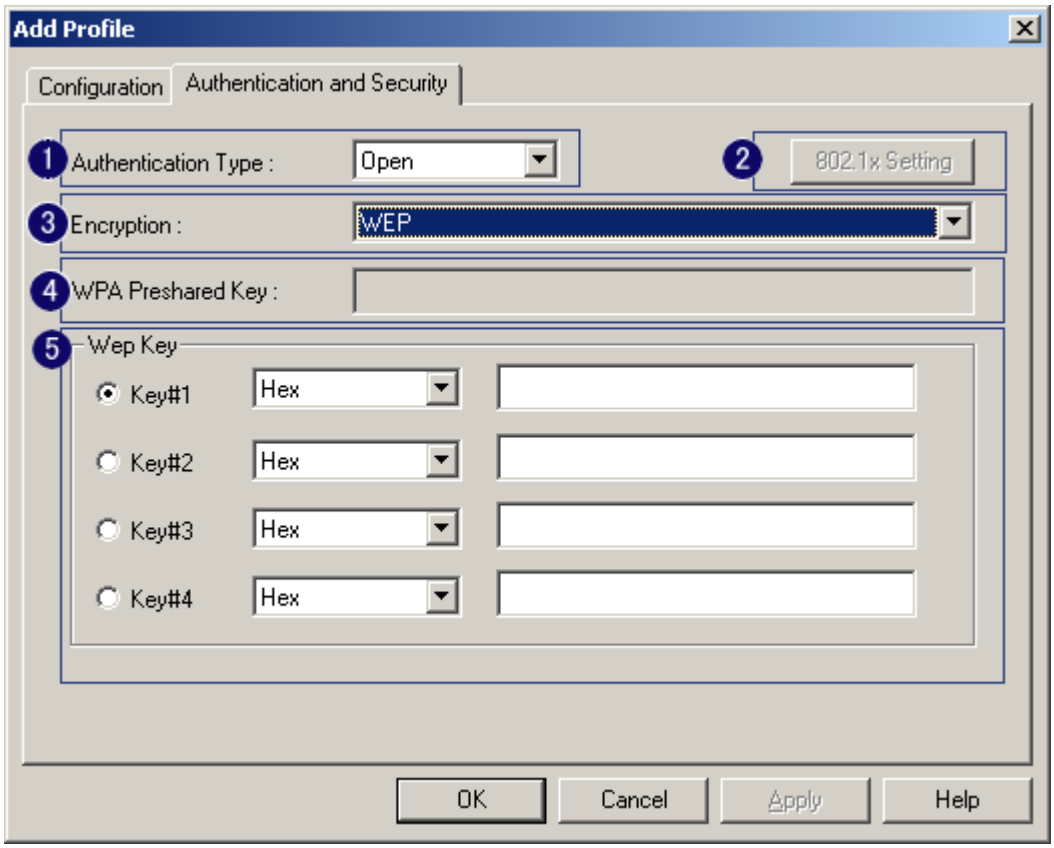


Figure 4-1 Authentication & Security setting

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

2 802.1x 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

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

4 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.

5 WEP 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 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.

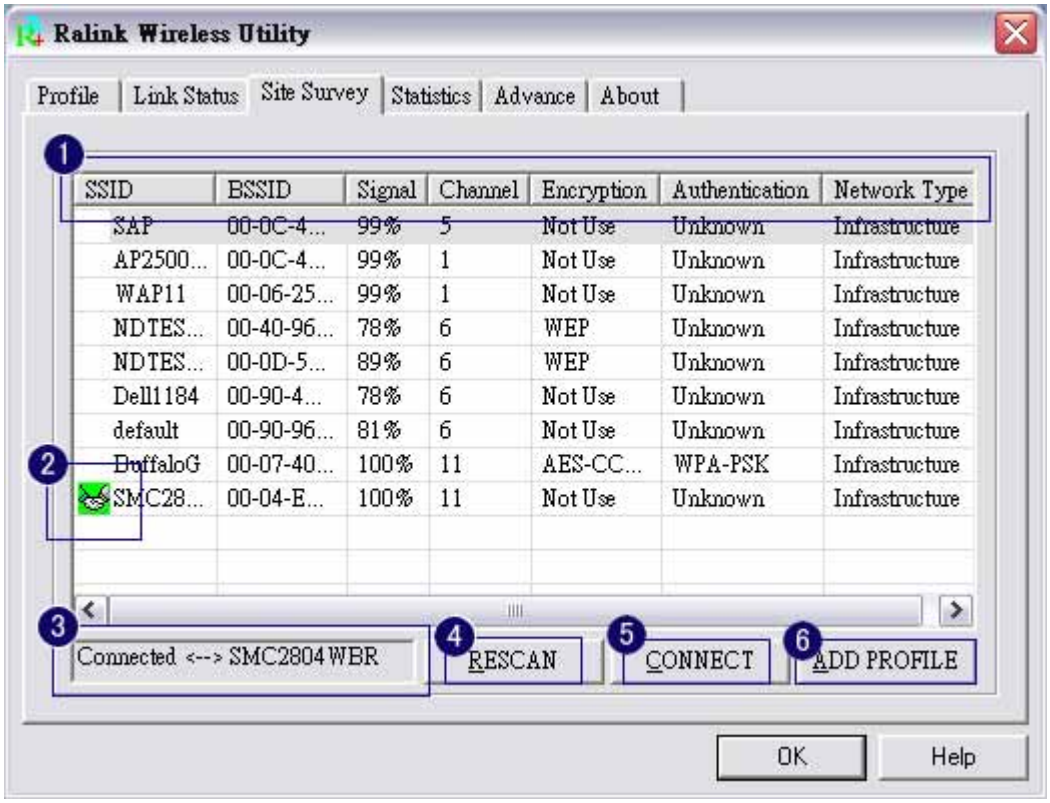


Figure 3-1 Detail information of site survey page

1 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.

2 Connected 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. Please refer to section 4 on how to fill the security

information.

This icon indicates the change is successful.

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

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

5 Command to connect to the selected network.

6 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.

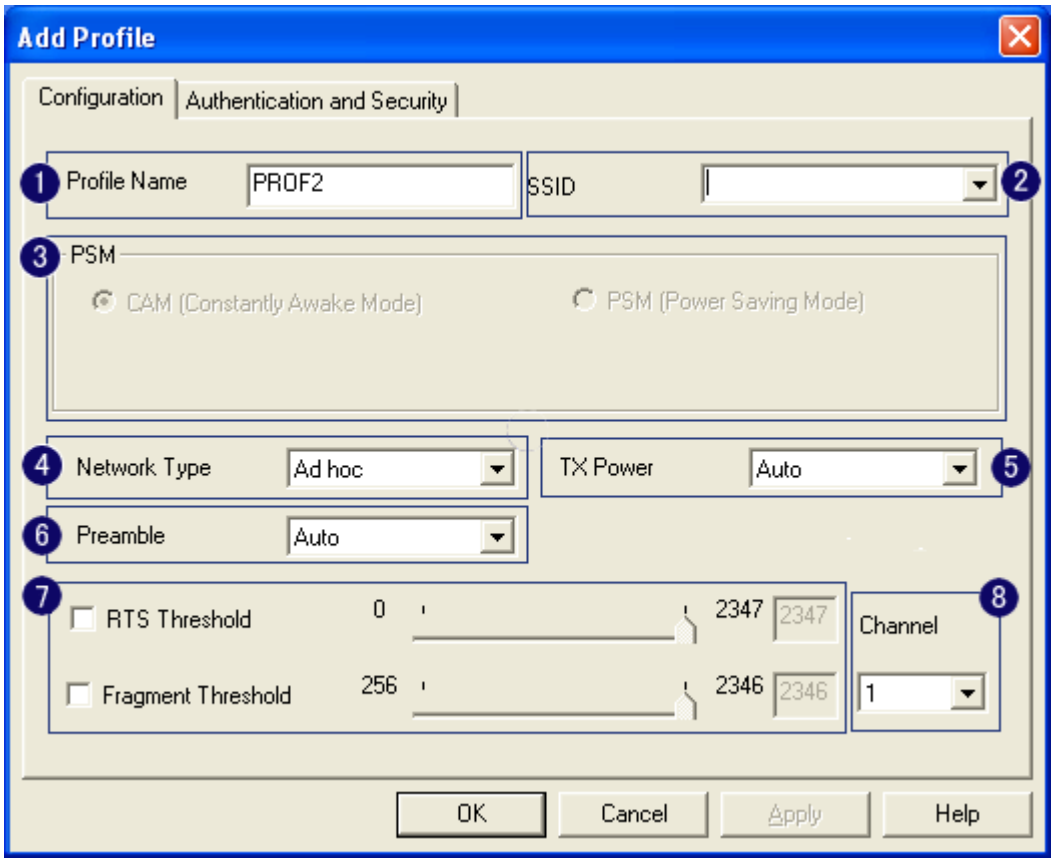


Figure 3-2 Profile system configuration

1 Profile Name: User chose name for this profile.

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

3 Power 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.

④Network 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.

⑦ 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.

⑧Channel: 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.

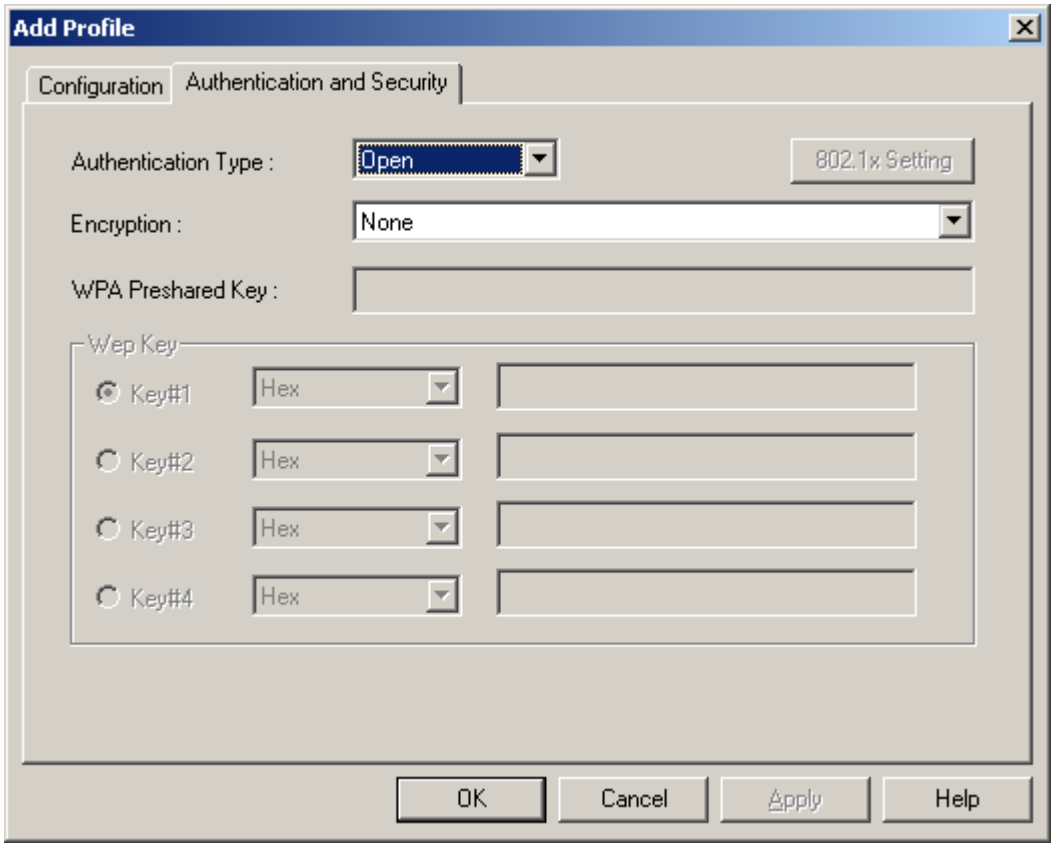


Figure 3-3 Profile Authentications and Security

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.

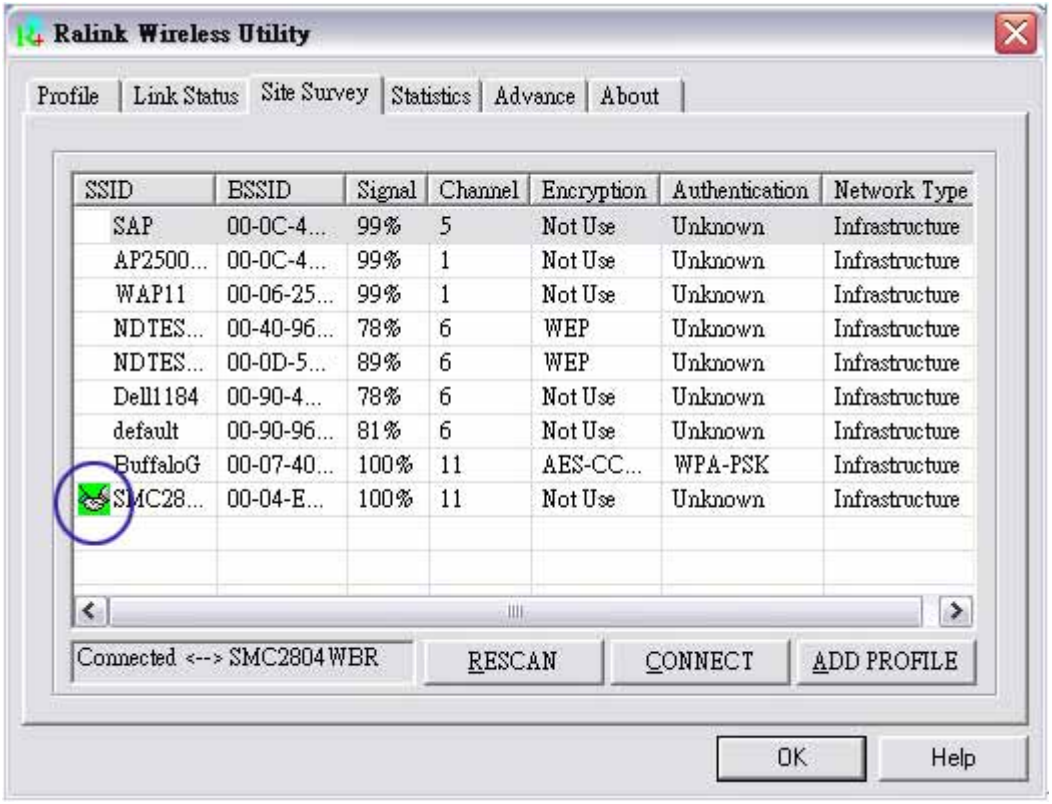


Figure 2-1 Fisrt page shown when starting RaConfig

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.

: 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.

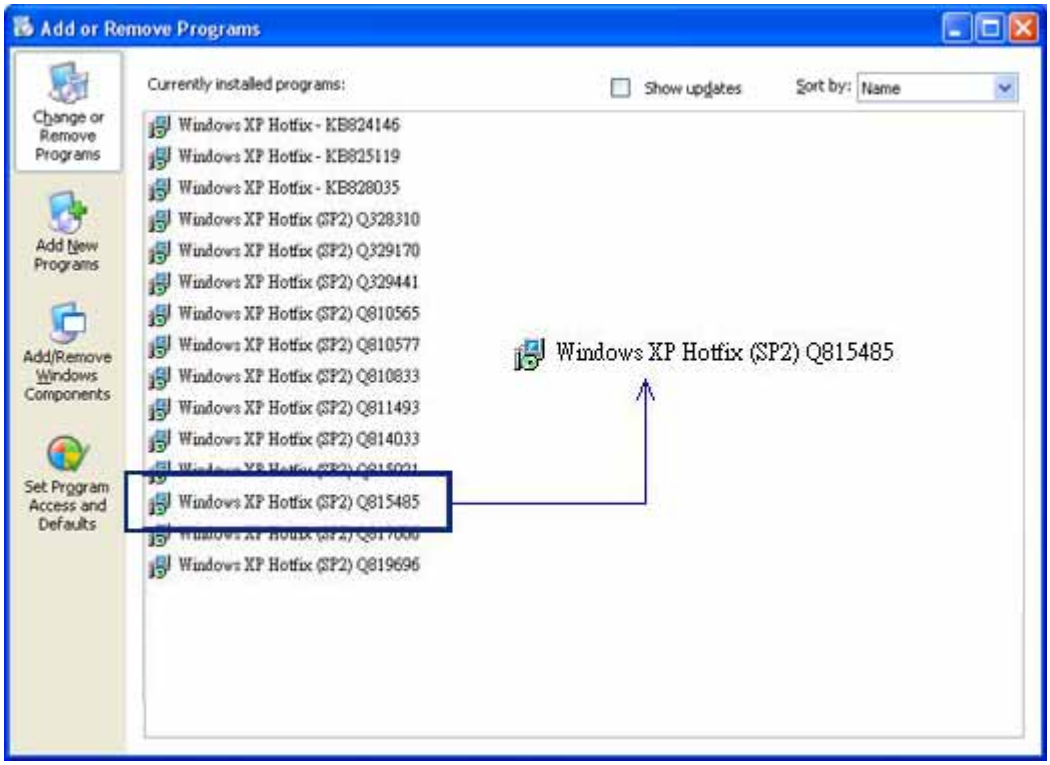


Figure 1-1 Windows XP Hotfix Q815485 installed

Currently, Ralink’s utility (RaConfig) provides WPA-PSK supplicant’s functionality. If user required WPA function. Please select WZC 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

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 WZC. When coexisting with WZC, 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.

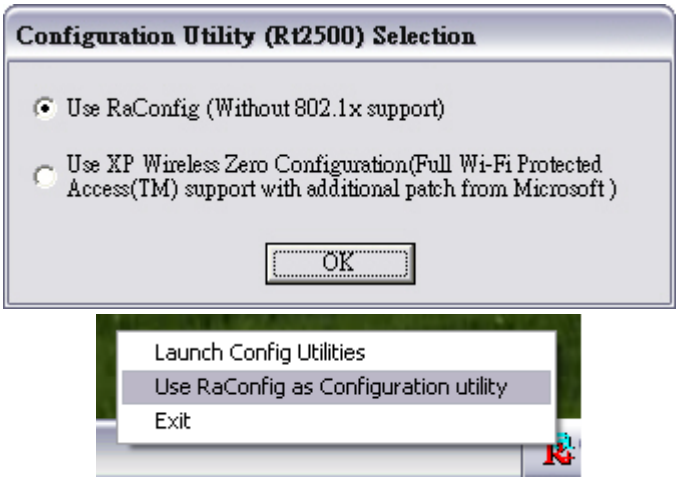


Figure 1-2 Select WZC or RaConfig

If " Use RaConfig (Without 802.1x support) " is selected, please jump to section 2-2 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 WZC. Figure 1-3 shows the RaConfig menu when WZC is active as main control utility.

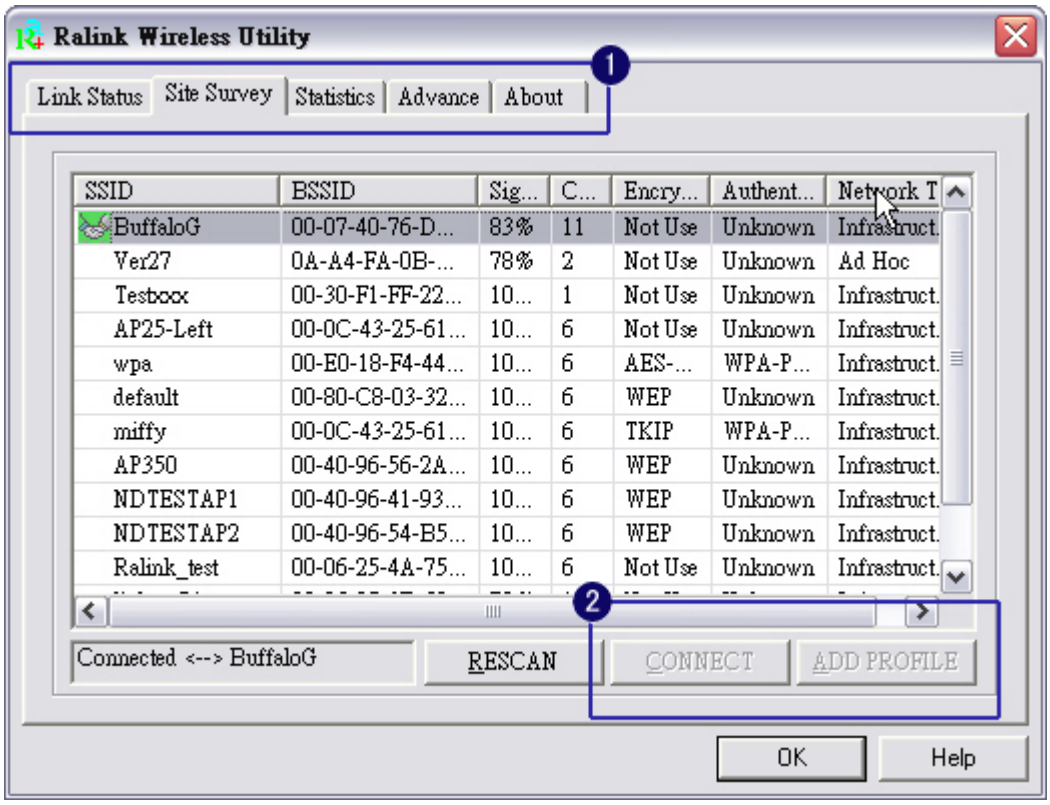


Figure 1-3 RaConfig menu with WZC active

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

❶Missing Profile page, profile function is removed since the NIC is controlled by WZC.

❷The connect and add profile function are removed from Site Survey Page. The reason is same as the first difference.

For all other functions provided by RaConfig, please read through this document for full detail.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The device is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

This device complies with Part15 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.

Excursus

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

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).