IEEE 802.11n Wireless Series

Wireless USB Adapter

User Manual

Version: 2.0

Date: January 13, 2009

FCC Certifications

Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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.

IEEE 802.11b/g or 802.11n operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

CE Mark Warning

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022
Class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademars:

All trade names and trademarks are the properties of their respective

TABLE OF CONTENTS

Overview

Thank you for purchasing this product. Read this chapter to know about your IEEE 802.11n Wireless USB Adapter.

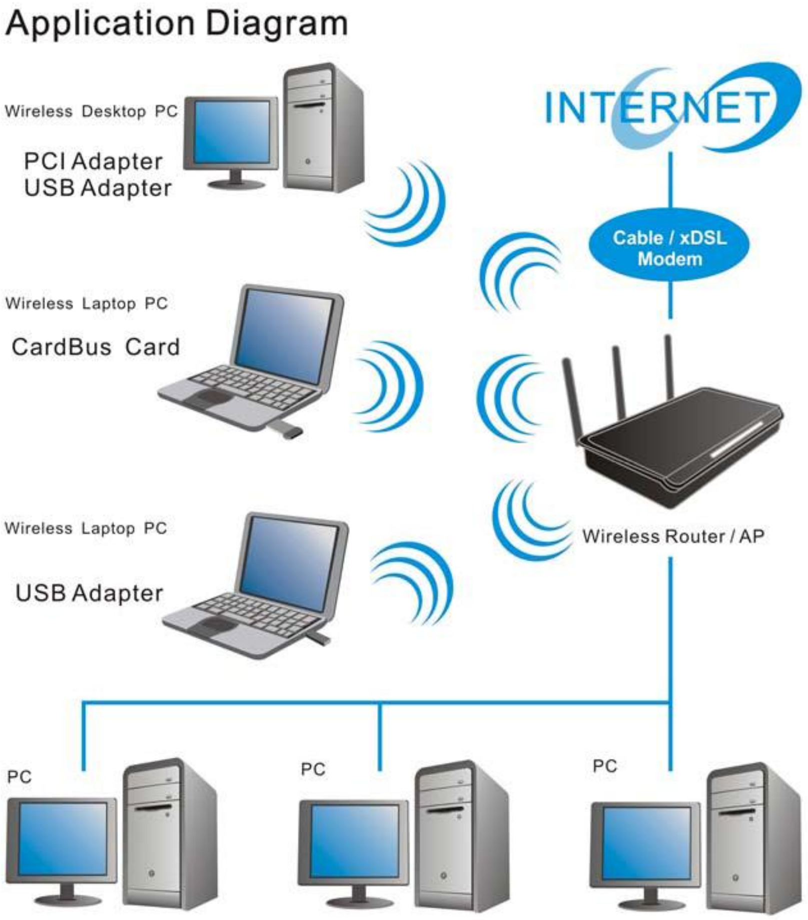
Unpacking Information

Before getting started, please verify that your package includes the following items:

1. IEEE 802.11n Wireless USB Adapter.
2. One Utility/ Manual CD.

Introduction to the IEEE 802.11n Wireless USB Adapter

The IEEE 802.11n Wireless USB adapter provides users to launch IEEE 802.11n wireless network at 150 Mbps in the 2.4GHz band, which is also compatible with IEEE 802.11b/g wireless devices at 11/54 Mbps. You can configure this adapter with ad-hoc mode to connect to other 2.4GHz wireless computers, or with Infrastructure mode to connect to a wireless AP or router for accessing to Internet. This adapter includes a convenient Utility for scanning available networks and saving preferred networks that users usually connected with. Security encryption can also be configured by this utility.

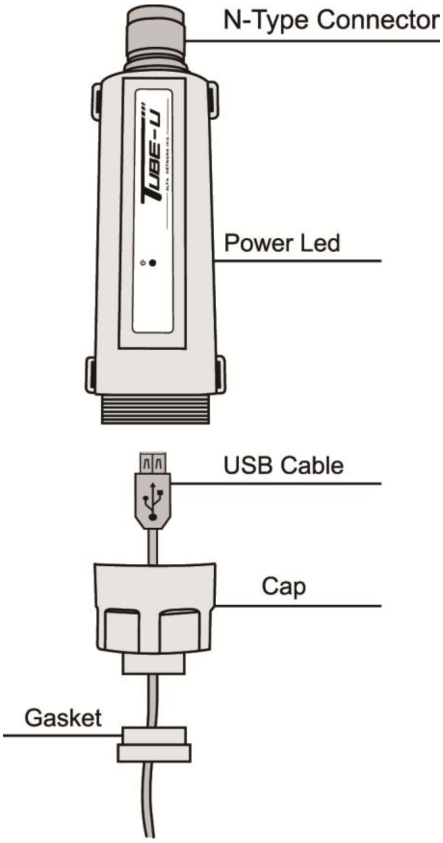


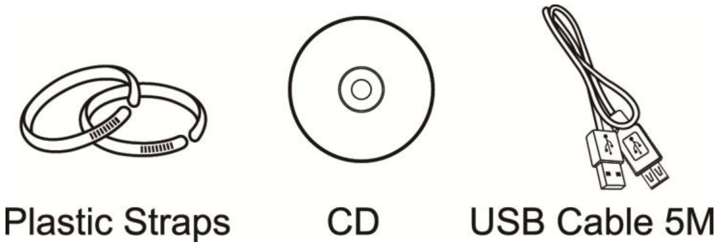
Key Features

- Complies with IEEE 802.11n/b/g wireless standards
- 2.4GHz frequency band, MIMO 1T1R
- Complies with USB 2.0
- High speed transfer data rate up to 150 Mbps
- Supports auto-installation
- Supports wireless data encryption with 64/128-bit WEP, WPA, WPA2, TKIP, AES
- Supports QoS: WMM, WMM-PS
- Supports multiple BSSID
- Supports driver for Windows 2000, XP 32/64, Vista 32/64, Linux (2.4.x/2.6.x), and Mac (10.4.x/10.5.x) Power PC & PC

Installation Guide

Hardware Installation





Use the plastic strap to secure your unit with a cylinder.
Connect your 5M USB cable to the button of the unit.

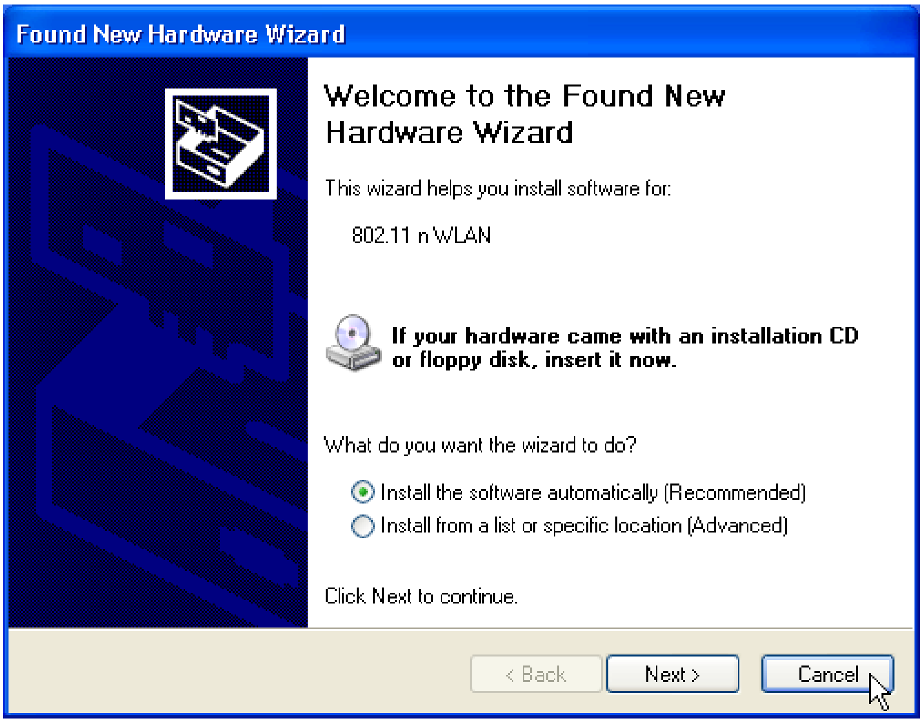
Software Installation

Note:

y For Linux or Mac driver installation guide, please refer to the instruction in **/Driver/Linux/README** or **/Driver/Mac/README** in the CD-Rom.

y The following driver installation guide uses Windows XP as the presumed operation system. The procedures and screens in Windows 2000 and Vista are familiar with Windows XP.

1. The system finds the newly installed device automatically. Click **Cancel** to close this window.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

802.11 n WLAN

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)

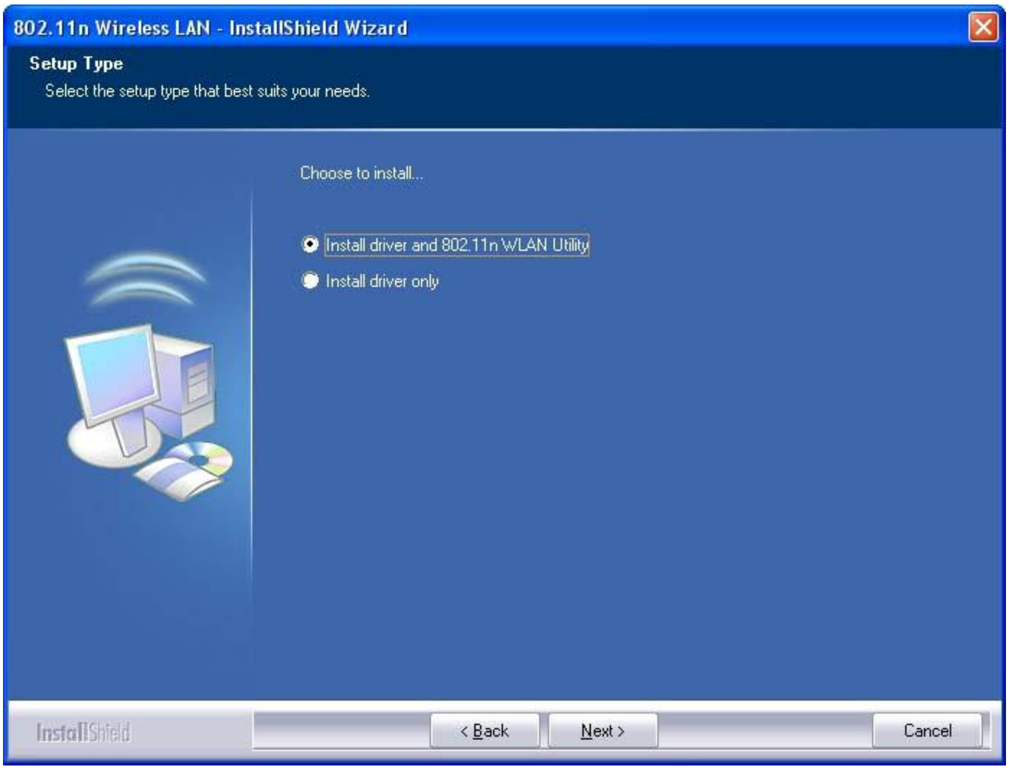
○ Install from a list or specific location (Advanced)

Click Next to continue.

2. Insert the CD-Rom that came with this product to your CD-Rom drive. The menu window pops up automatically. Please click the **Driver** button of this product.

   Note: If the CD-Rom fails to auto-run, please click on **My Computer** > **your CD-Rom drive > (folder of this product) > Driver** then double-click the **Setup** icon to start this menu.

3. Select if you are going to install the driver and wireless utility; or install the driver only.



802.11n Wireless LAN - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

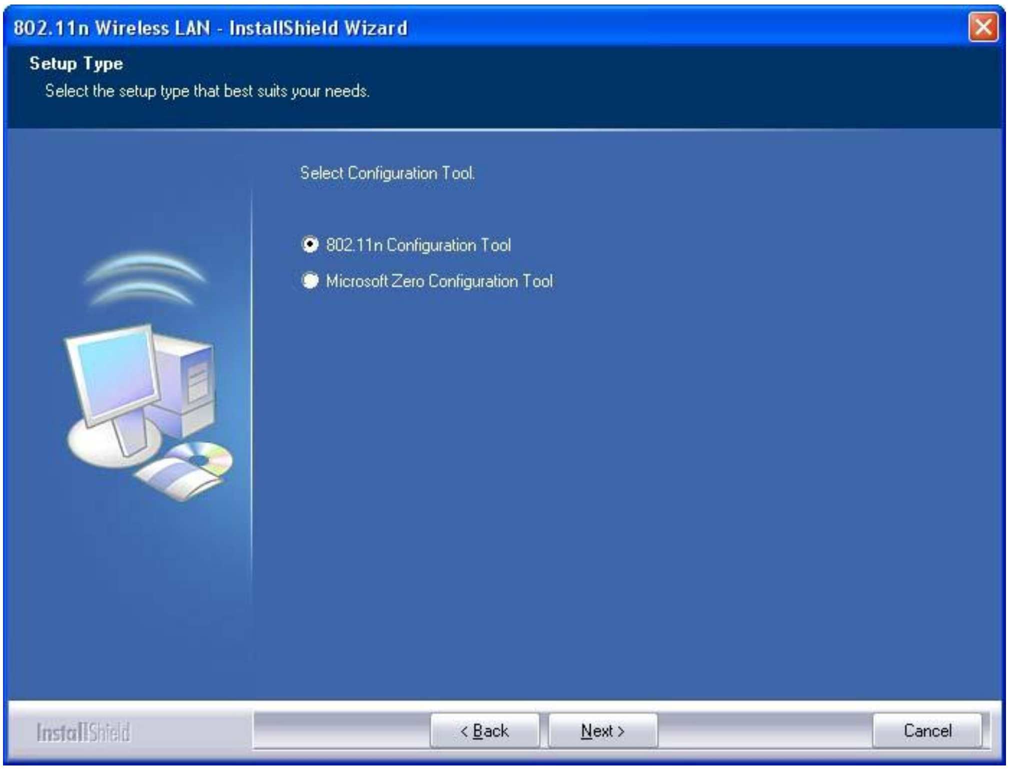
Choose to install...

● Install driver and 802.11n WLAN Utility

○ Install driver only

4. Select if you are going to configure your wireless network with this device or with Microsoft Zero Configuration tool.

Note: This can be changed after installing this software.



802.11n Wireless LAN - InstallShield Wizard

Setup Type

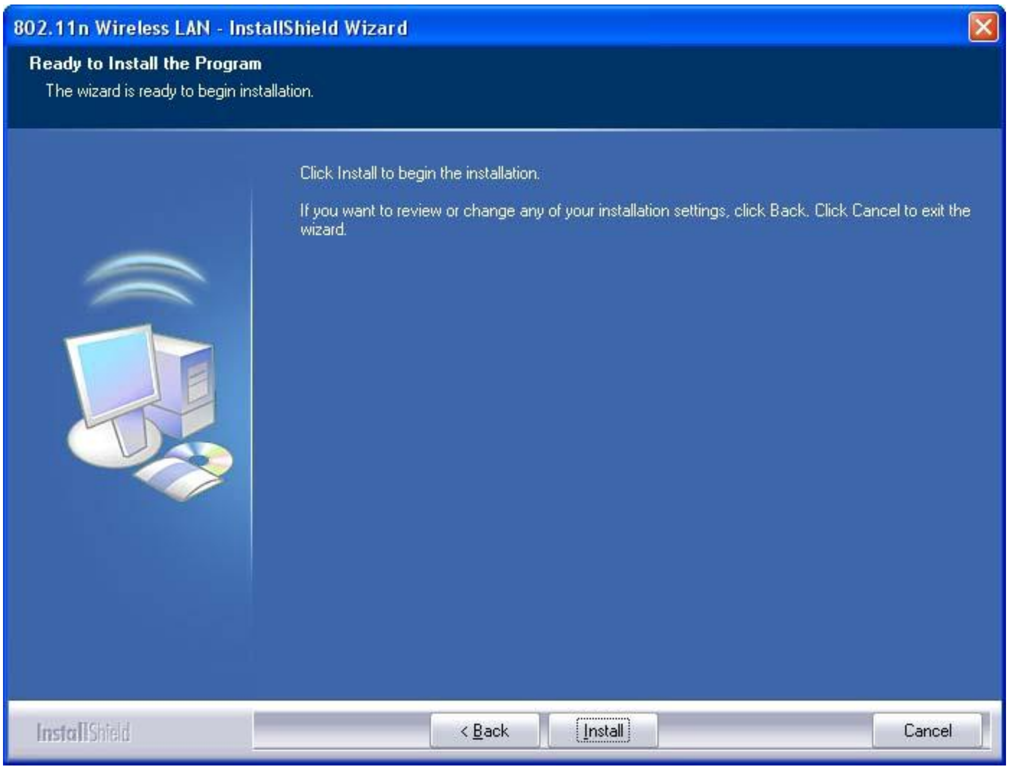
Select the setup type that best suits your needs.

Select Configuration Tool.

● 802.11n Configuration Tool

○ Microsoft Zero Configuration Tool

5. Click the **Install** button to start installing.



802.11n Wireless LAN - InstallShield Wizard

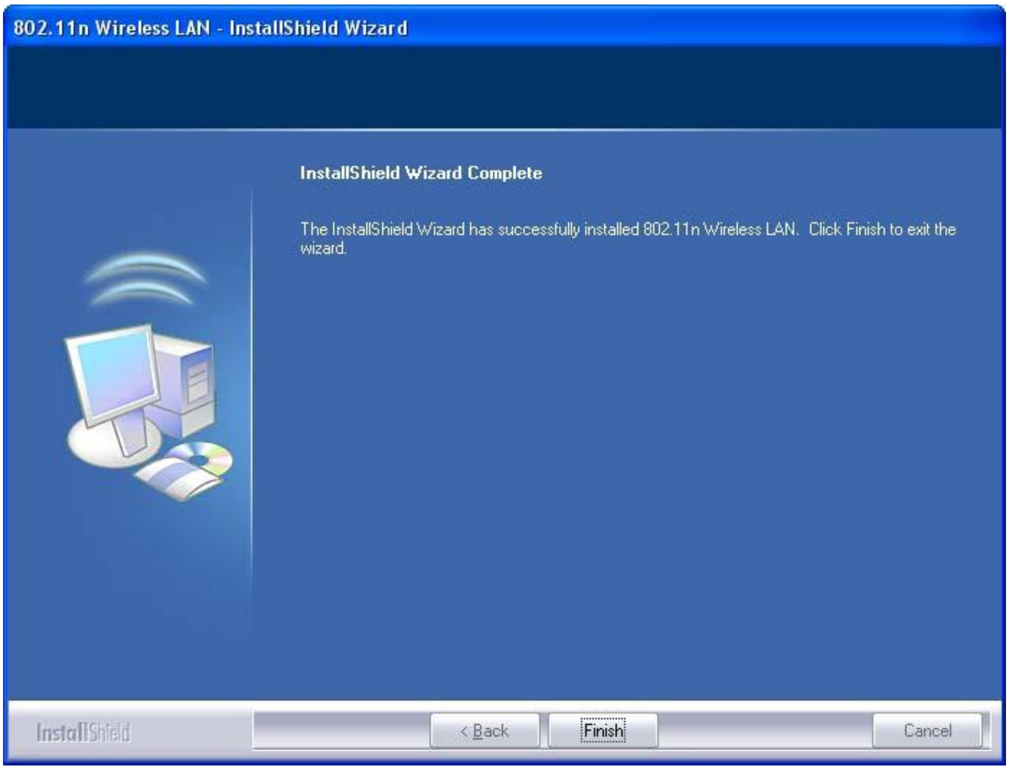
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

6. Click the **Finish** button to complete installation.



802.11n Wireless LAN - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed 802.11n Wireless LAN. Click Finish to exit the wizard.

Management Guide

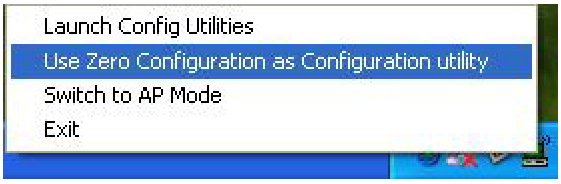
Read this chapter to understand the management interface of the device and how to manage the device.

Making a Basic Network Connection

Select a configuration tool

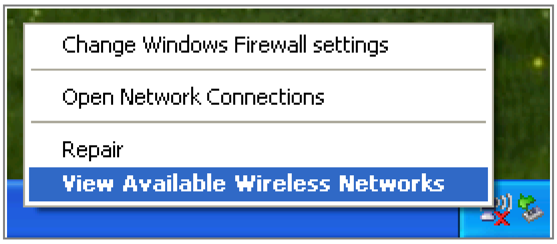
In the following instruction for making a network connection, we use the Utility we provide to configure your wireless network settings.

Note: You could use either the software we provide or Microsoft Zero Configuration tool to configure this adapter. To switch between the two configuration tools, please right click on the.. icon on system tray to select.

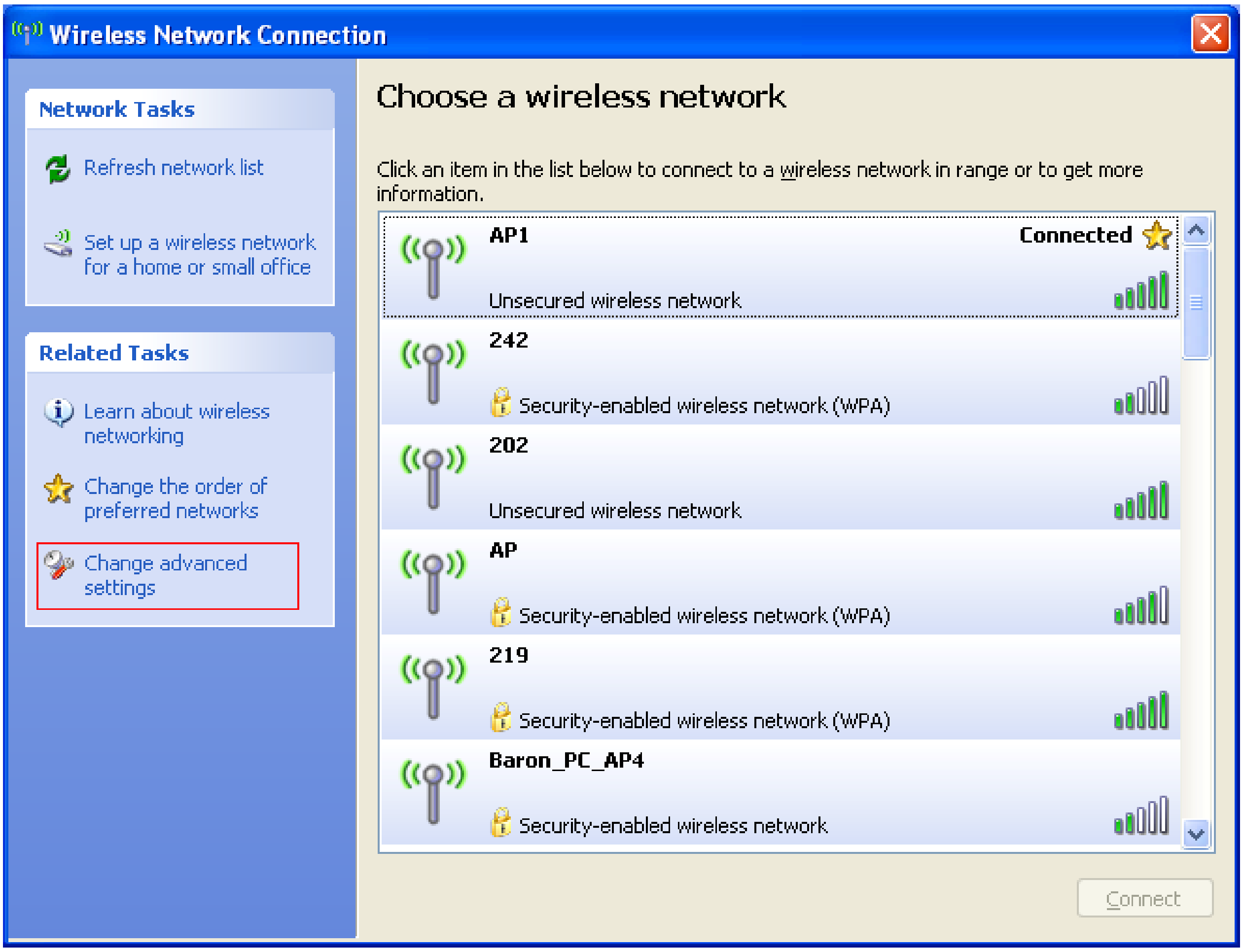


To connect with Microsoft Zero Configuration tool

After specifying the Microsoft Zero Configuration tool to configure your wireless network, right click on the icon on system tray. Select **View Available Wireless Networks** to specify your wireless network.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

The tool shows the available wireless networks. Select your demanding network to connect with. To connect to a wireless network with more security settings, please click **Change advanced settings** to be compatible with your wireless network security settings.



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

AP1 — Connected — Unsecured wireless network

242 — Security-enabled wireless network (WPA)

202 — Unsecured wireless network

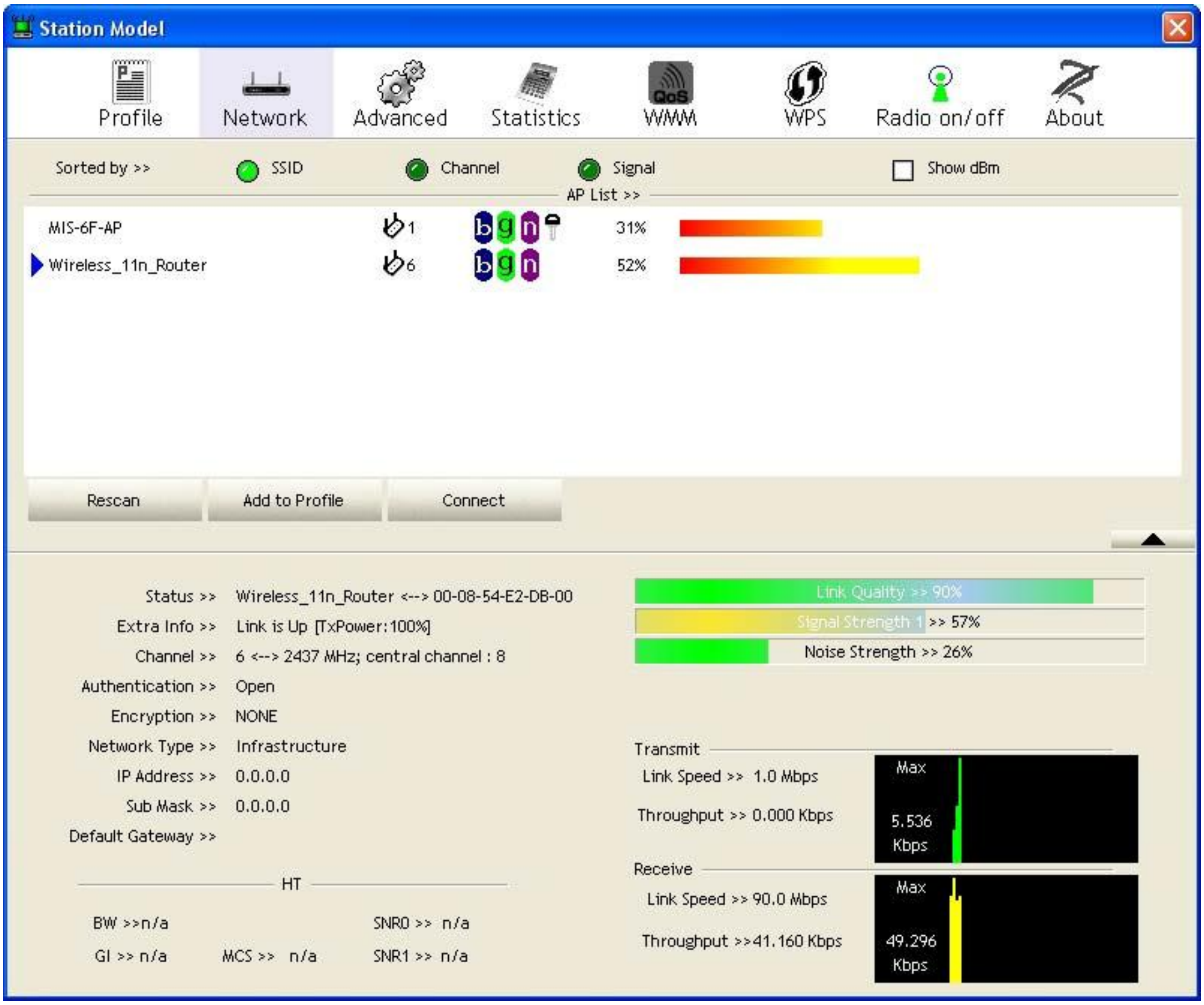
AP — Security-enabled wireless network (WPA)

219 — Security-enabled wireless network (WPA)

Baron_PC_AP4 — Security-enabled wireless network

To connect with 802.11n Wireless LAN Utility

We provide this Utility for users to connect to a wireless network easily. It provides more information and configuration for this adapter. As default, the Utility is started automatically upon starting your computer and connects to a connectable wireless network with best signal strength and with no security setting. Right click on the icon in the system ray and select **Launch Config utilities** if the Utility does not start. Please refer to the following chapters to get information regarding to the functions of this Utility.



SSID	Channel		Signal
MIS-6F-AP	1	b g n	31%
Wireless_11n_Router	6	b g n	52%

Status >> Wireless_11n_Router <--> 00-08-54-E2-DB-00

Extra Info >> Link is Up [TxPower:100%]

Channel >> 6 <--> 2437 MHz; central channel : 8

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 0.0.0.0

Sub Mask >> 0.0.0.0

Default Gateway >>

BW >>n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 90%

Signal Strength 1 >> 57%

Noise Strength >> 26%

Transmit

Link Speed >> 1.0 Mbps

Throughput >> 0.000 Kbps

5.536 Kbps

Receive

Link Speed >> 90.0 Mbps

Throughput >>41.160 Kbps

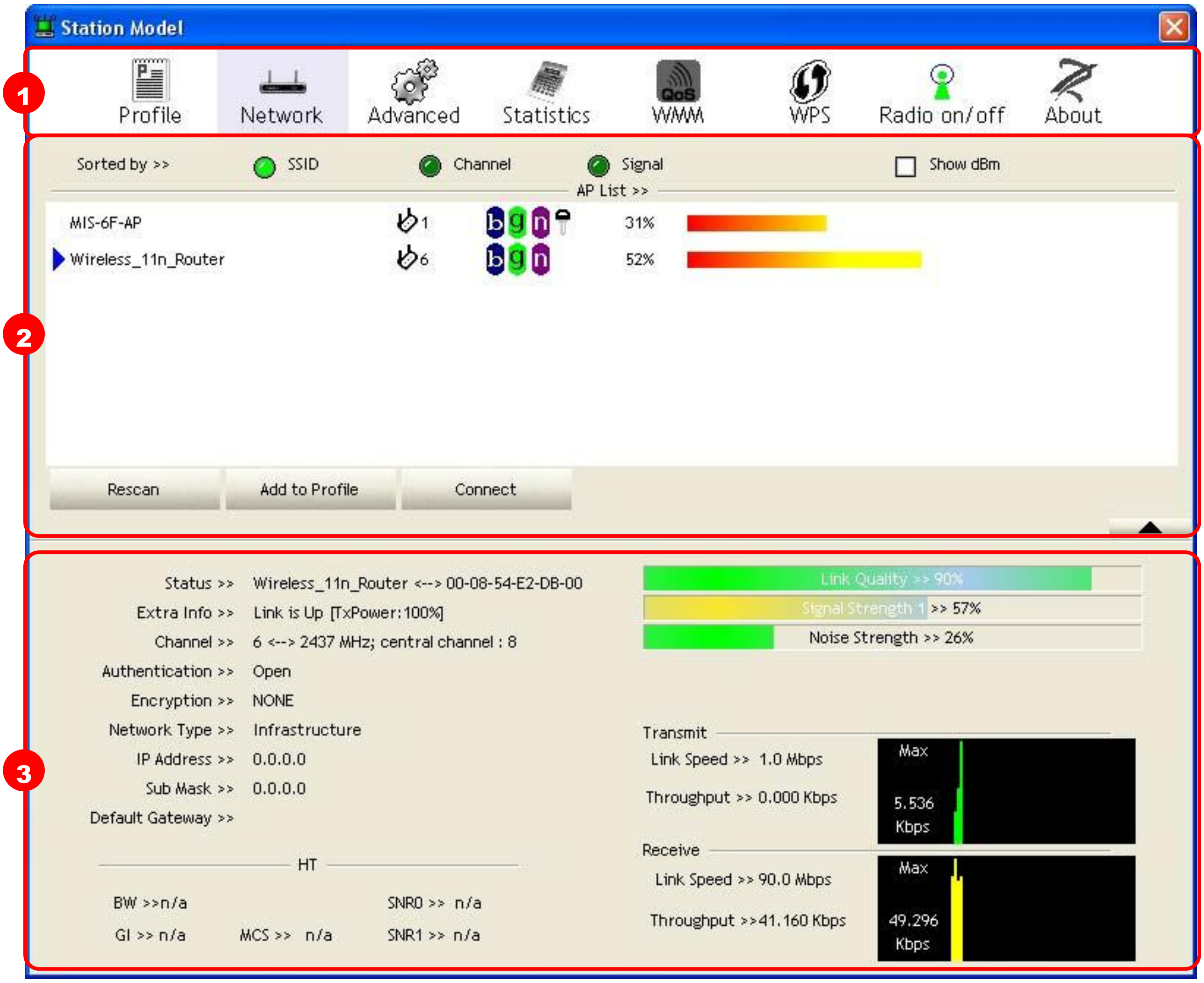
49.296 Kbps

Introduction to the 802.11n Wireless LAN Utility

Note: The Utility in Linux and Mac are different from the following.

Interfaces

This Utility is basically consisted of three parts:



SSID	Channel		Signal
MIS-6F-AP	1	bgn	31%
Wireless_11n_Router	6	bgn	52%

Status >> Wireless_11n_Router <--> 00-08-54-E2-DB-00
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437 MHz; central channel : 8
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 0.0.0.0
Sub Mask >> 0.0.0.0
Default Gateway >>

BW >>n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 90%
Signal Strength 1 >> 57%
Noise Strength >> 26%

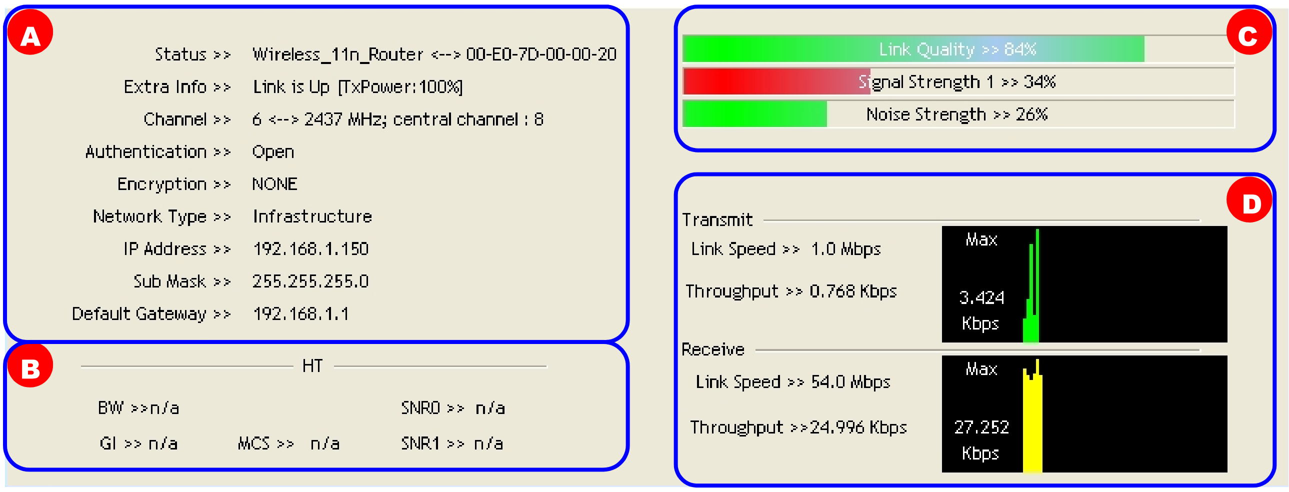
Transmit
Link Speed >> 1.0 Mbps
Throughput >> 0.000 Kbps
5.536 Kbps

Receive
Link Speed >> 90.0 Mbps
Throughput >>41.160 Kbps
49.296 Kbps

1. **Functional Buttons:** on top of the window. You can click each button to access each configuration window.

   Note: Click 📡 to enable/disable wireless connection status.
2. **Configuration Column:** Center of the Utility window. Make your changes for each function in this part.
3. **Link Status Information:** bottom of the utility window. Shows the connection status and system information.

Link Status Information



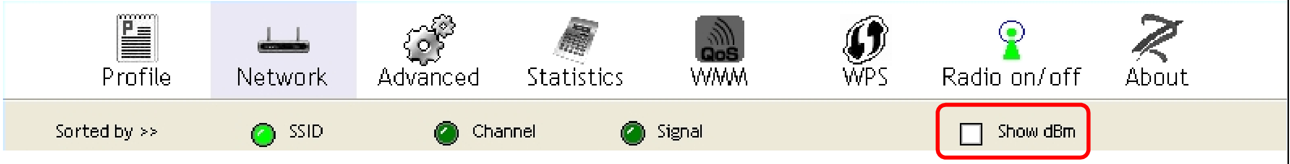
```
Status >>  Wireless_11n_Router <--> 00-E0-7D-00-00-20
Extra Info >>  Link is Up [TxPower:100%]
Channel >>  6 <--> 2437 MHz; central channel : 8
Authentication >>  Open
Encryption >>  NONE
Network Type >>  Infrastructure
IP Address >>  192.168.1.150
Sub Mask >>  255.255.255.0
Default Gateway >>  192.168.1.1

HT
BW >>n/a                     SNR0 >> n/a
GI >> n/a    MCS >>  n/a     SNR1 >> n/a

Link Quality >> 84%
Signal Strength 1 >> 34%
Noise Strength >> 26%

Transmit
Link Speed >> 1.0 Mbps             Max
Throughput >> 0.768 Kbps           3.424 Kbps
Receive
Link Speed >> 54.0 Mbps            Max
Throughput >>24.996 Kbps           27.252 Kbps
```

A. Network Information:

Items	Information
Status	Show the connecting status. Also shows the SSID while connecting to a valid network.
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 of current connection.
Sub Mask	Subnet mask of current connection.
Default Gateway	Default gateway of current connection.
Link Speed	Show current transmit rate and receive rate.
Throughput	Display transmit and receive throughput in Mbps.

B. HT: Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value.

C. Link Quality and Strength Bar:

Items	Information
Link Quality	Display connection quality based on signal strength and TX/RX packet error rate.
Signal Strength 1	Receive signal strength 1.
Noise Strength	Display noise signal strength.
User can choose to display Signal and Noise Strength as percentage or dBm format by mark the dBm checkbox. 	

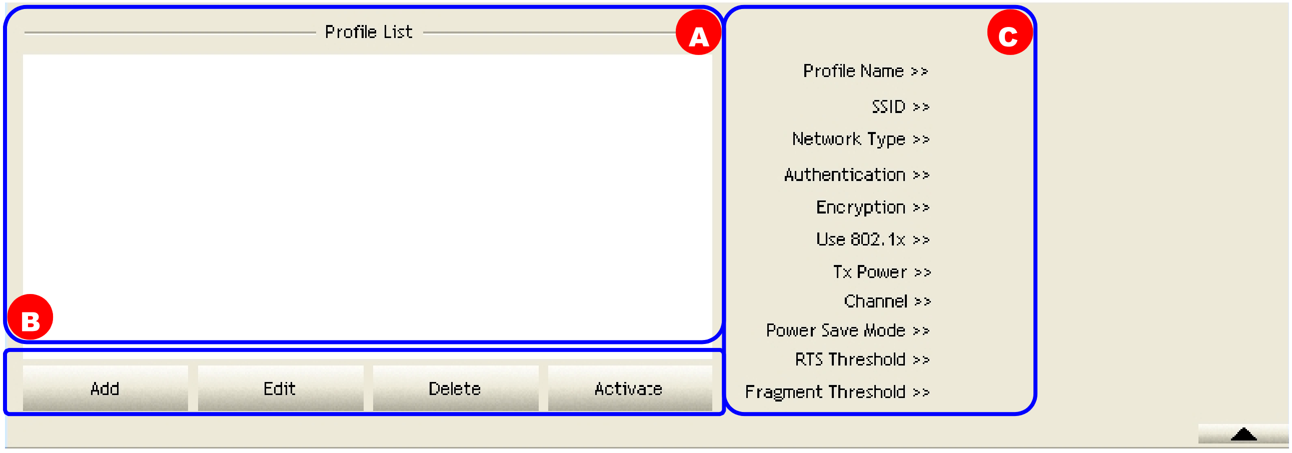
Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

D. Statistics:

Items	Information
Link Speed	Show current transmit rate and receive rate.
Throughput	Display transmit and receive throughput in Mbps.

Profile

This profile page allows users to save different wireless settings, which helps users to get access to wireless networks at home, office or other wireless network environments quickly.



A. Profile List: The list shows all the profiles you have added before.

B. Buttons: You can click on these buttons to add a new profile, edit, delete or activate an old profile.

Note: For Vista user, there are extra Import and Export buttons in this feature. Click on these buttons to import or export the selected profile.

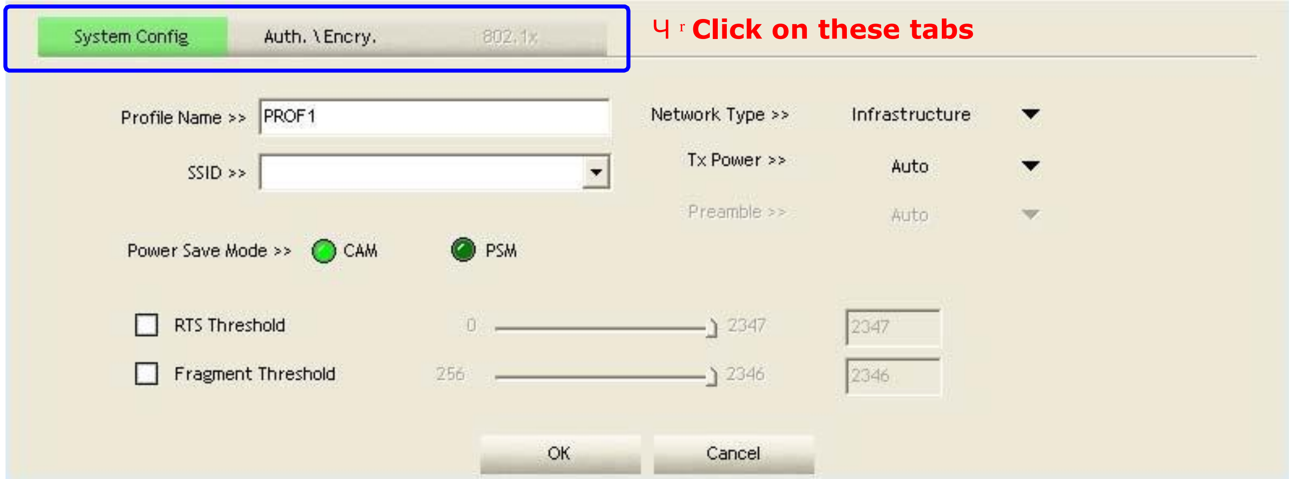
C. Profile Information: While you select a profile in the profile list, you can see the profile information shows on here.

Items	Information
Profile Name	The name of the selected profile.
SSID	The SSID of the wireless system.
Network Type	Shows Infrastructure / Ad-hoc to indicate the network type of the selected profile.
Authentication	Shows the authentication mode in use. There are total 8 modes: Open, Shared, LEAP, WPA, WPA-PSK, WPA2, WPA2-PSK and WPA-NONE.
Encryption	Shows the encryption mode in use. There are total 4 modes: None, WEP, TKIP and AES.
Use 802.1x	Shows Yes/No to indicate whether the selected profile use the 802.1x feature or not.
Tx Power	Shows the transmit power in use. There are total 7 types: Auto, 100%, 75%, 50%, 25%, 10% and Low.
Channel	Shows the channel in use (1~11) for Ad-Hoc mode.
Power Save Mode	Shows the power save mode in use. Two selections: CAM (Constantly Awake Mode) and PSM (Power Saving Mode).
RTS Threshold	Shows the RTS threshold value in use.
Fragment Threshold	Shows the fragment threshold in use.

To add a new profile:

1. Click the **Add** button. The add profile window pops up.

   Note: you could also add a new profile quickly by selecting an available network in the **Network** function then click the **Add to Profile** button.



Profile Name >> PROF1

SSID >>

Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

Power Save Mode >> ● CAM ● PSM

☐ RTS Threshold 0 2347 2347

☐ Fragment Threshold 256 2346 2346

2. There are three tabs on the window:

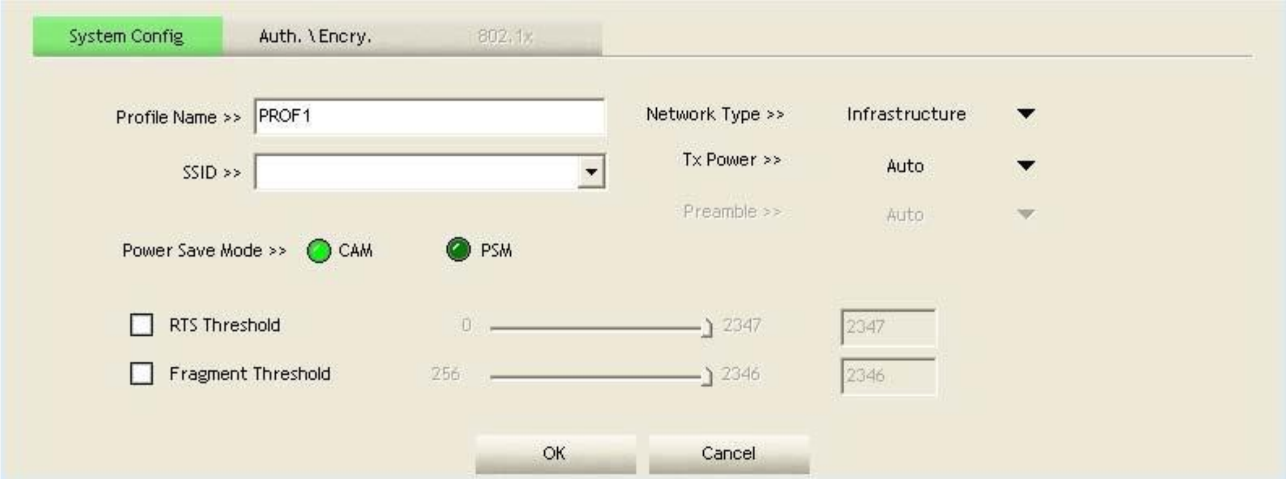
   System Config — Settings for: Profile Name, SSID, Network Type, Tx Power, Preamble, Power Save Mode, RTS Threshold, and Fragment Threshold.

   Auth. \ Encry. — Settings for: Authentication, Encryption, Preshared Key, and WEP Key.

   802.1x — Settings for: EAP Method, Tunnel Authentication, and Session Resumption. For different EAP Method, you also have to configure different require of ID/Password, Client Certificate, or Server Certificate.

   Please follow the steps below to fill in the information gradually.

3. In System Config section, fill in information for this profile:



Profile Name >> PROF1

SSID >>

Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

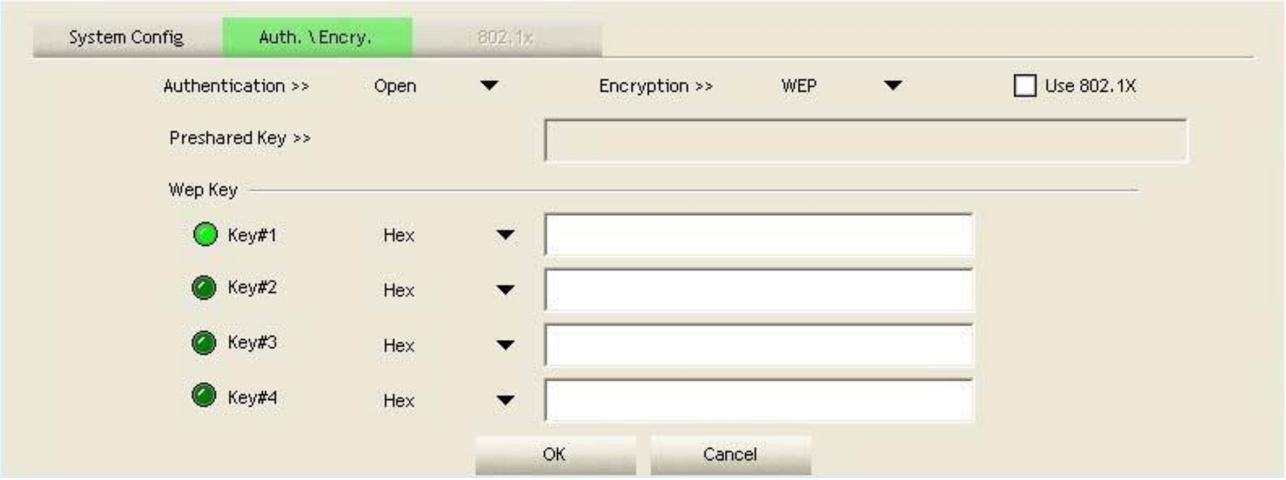
Power Save Mode >> ● CAM ● PSM

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

Items	Information
Profile Name	Choose a name for this profile, or use default name defined by system.
SSID	Fill in the intended SSID name or use the drop list to select from available APs.
Network Type	There are two types, infrastructure and 802.11 Ad-hoc modes. Under Ad-hoc mode, you could also choose the preamble type; the available preamble type includes auto and long. In addition to that, the channel field will be available for setup in Ad-hoc mode.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Preamble	Two selections: Auto, and Long Preamble. This can only be set up in Ad –hoc mode.
Channel	Channel in use for Ad-Hoc mode.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode).
RTS Threshold	For adjusting the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
Fragment Threshold	Adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

4. In Auth. \Encry. section, select an encryption type and fill in the corresponding wireless network information:



Authentication >> Open

Encryption >> WEP

□ Use 802.1X

Preshared Key >>

Wep Key

Key#1 Hex

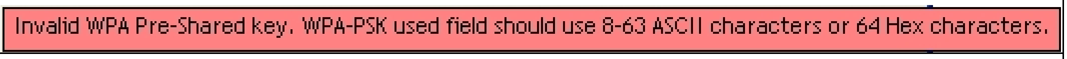
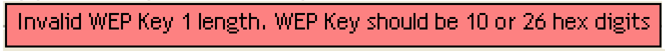
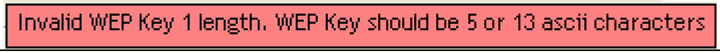
Key#2 Hex

Key#3 Hex

Key#4 Hex

<table>
<tr><th>Items</th><th>Information</th></tr>
<tr><td><b>Authentication Type</b></td><td><b>For Windows 2000 User</b>
There are 7 types supported: Open, Shared, LEAP, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-NONE[1]. Please select a type from the drop down list.
<b>For Vista User</b>
There are 7 types supported: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, and CCKM. Please select a type from the drop down list.</td></tr>
<tr><td><b>Encryption Type</b></td><td><b>For Windows 2000 User</b>
There are 4 types supported: None, WEP, TKIP and AES.
The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open</td><td>NONE, WEP</td></tr>
<tr><td>Shared</td><td>WEP</td></tr>
<tr><td>LEAP</td><td>(no selection)</td></tr>
<tr><td>WPA/WPA2/WPA-PSK
WPA2-PSK/WPA-NONE</td><td>TKIP, AES</td></tr>
</table>
<b>For Vista User</b>
There are 6 types supported: None, WEP, TKIP, AES, TKIP (MFP) and AES (MFP).
The available encryption selection will differ from the authentication type you have chosen, the result is shown below:
<table>
<tr><th>Authentication</th><th>Available Encryption Selection</th></tr>
<tr><td>Open</td><td>NONE, WEP</td></tr>
<tr><td>Shared</td><td>WEP</td></tr>
<tr><td>WPA/ WPA-PSK/ WPA2-PSK</td><td>TKIP, AES</td></tr>
<tr><td>WPA2</td><td>TKIP, AES, TKIP(MFP), AES(MFP)</td></tr>
<tr><td>CCKM</td><td>WEP, TKIP, AES</td></tr>
</table></td></tr>
</table>

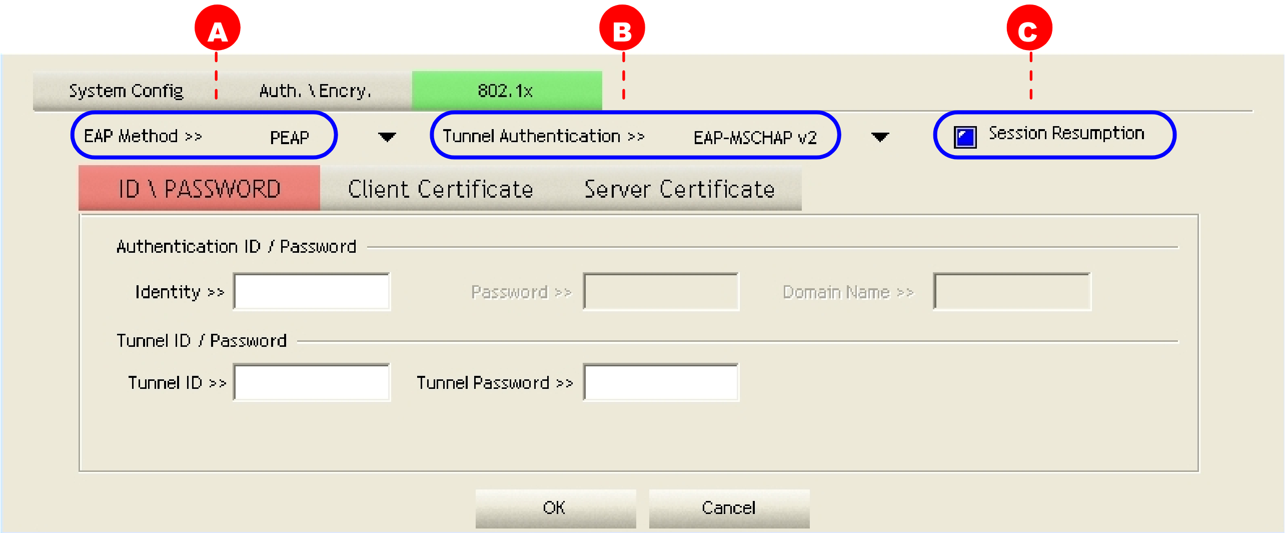
[1] WPA-NONE is only available in Ad-hoc mode.

Use 802.1x	This checkbox appears while the environment is set to an Open authentication with WEP encryption. Mark the checkbox to make the 802.1x section available. The 802.1x section is also available in WPA and WPA2 authentication types.
Preshared Key	This is the shared secret between AP and STA. For WPA-PSK, WPA2-PSK and WPA-NONE authentication mode, this field must be filled with characters longer than 8 and less than 32 lengths. The following dialog appears if you have input invalid values.  Invalid WPA Pre-Shared key. WPA-PSK used field should use 8-63 ASCII characters or 64 Hex characters.
WEP Key	Only available when using WEP encryption algorithm. The key must match AP's key. Select Hex[1] or ASCII[2] to setup the key value. The following dialog appears if you have input invalid values.  Invalid WEP Key 1 length. WEP Key should be 10 or 26 hex digits  Invalid WEP Key 1 length. WEP Key should be 5 or 13 ascii characters

[1] Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

[2] ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127.

5. Specify the 802.1x information if you are using the 802.1X certification method. Users that do not use this function or connecting to an open-wireless network please skip this part.



A. EAP Method:

For Windows 2000 User: There are total 5 modes: PEAP, TLS/Smart Card, TTLS, EAP-FAST, and MD5-Challenge.

For Vista User: There are total 4 modes: PEAP, TLS/Smart Card, EAP-FAST, and LEAP.

Please select an EAP method from the drop down list.

Items	Information
PEAP	Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
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.
TTLS	Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
EAP-FAST	Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.
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.
LEAP	Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.

B. Tunnel Authentication: The tunnel authentication will differ from the EAP method you have chosen, the result is shown below:

For Windows 2000 User:

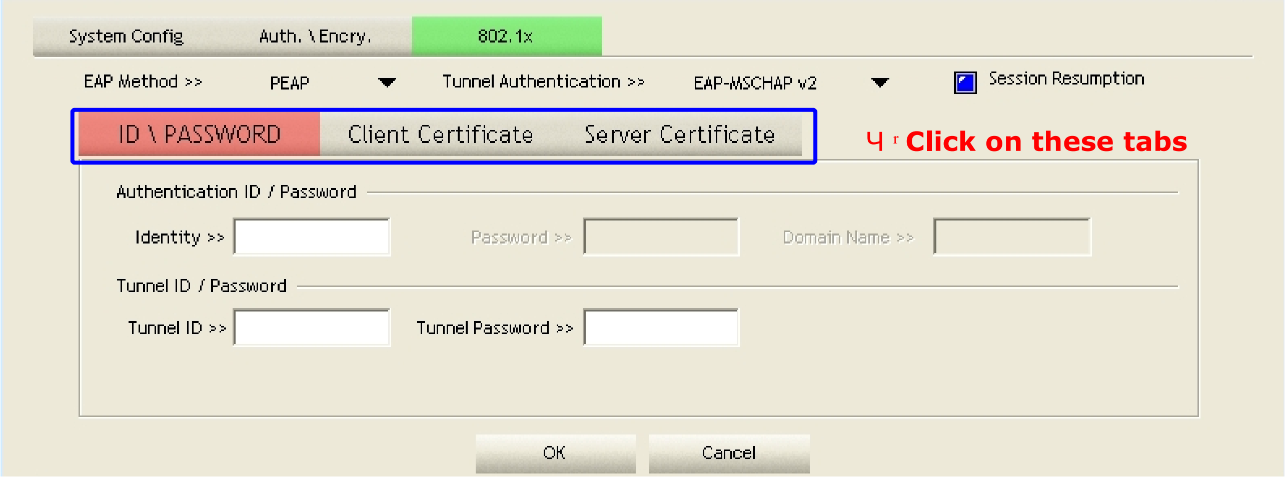
EAP Method	Tunnel Authentication
PEAP	EAP-MSCHAP v2 , EAP-TLS/Smart Card, Generic Token Card
TLS/Smart Card	(no selection)
TTLS	CHP, MS-CHAP, MS-CHAP-V2, PAP, EAP-MD5
EAP-FAST	Generic Token Card
MD5-Challenge	(no selection)

For Vista User:

EAP Method	Tunnel Authentication
PEAP	EAP-MSCHAP v2 , EAP-TLS/Smart Card, Generic Token Card
TLS/Smart Card	(no selection)
EAP-FAST	(no selection)
LEAP	(no selection)

C. Session Resumption: Mark to enable this function or unmark it to disable.

After doing the above settings, please click on the tabs below. There are several tabs on the window, please fill in the information gradually.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

ID \ PASSWORD — Settings for: Authentication ID/Password, Tunnel ID/Password and Password Mode[1].

Client Certificate — Settings for using the Client Certificate function or not.

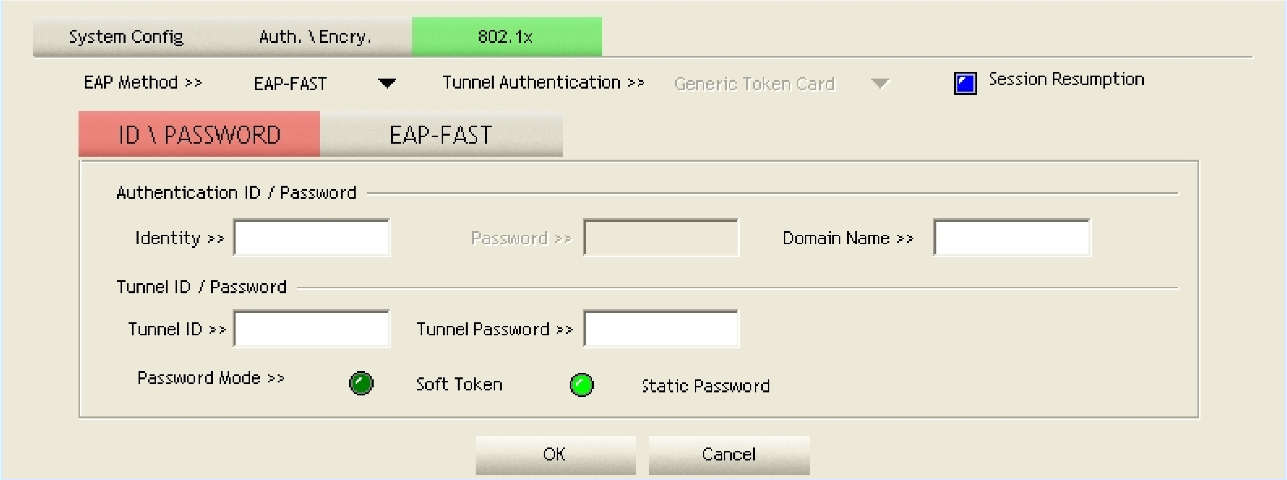
Server Certificate — Settings for using the Server Certificate function or not.

EAP-FAST — Setting for EAP-FAST method.

SSO — Settings for Single Sign On. **Note:** This tab only appears in Vista system.

[1] Password mode is only available in EAP-FAST method.

ID \ PASSWORD



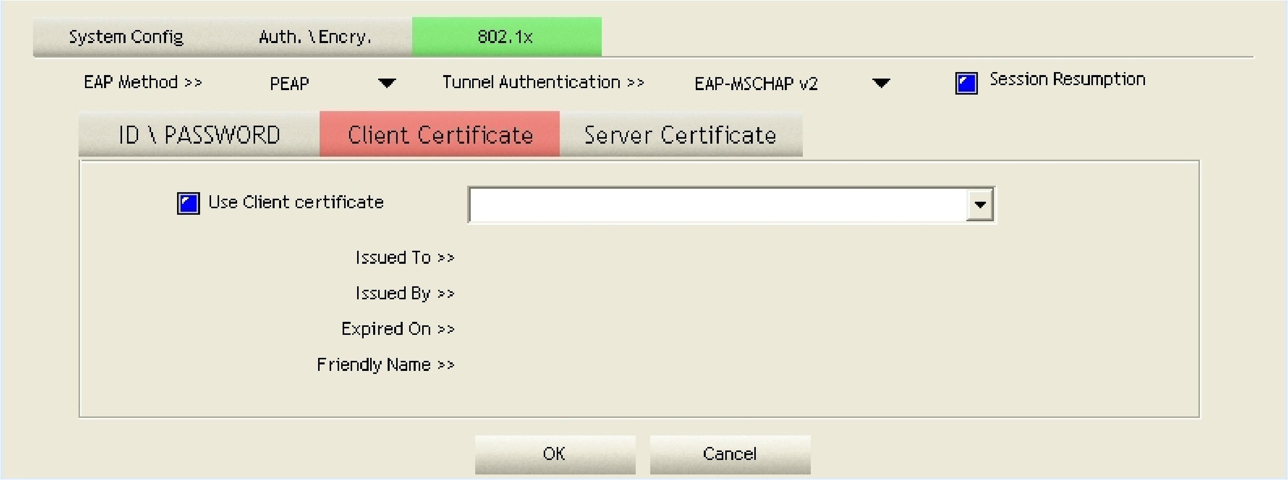
EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card

☑ Session Resumption

Items	Information
Authentication ID / Password	The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can be keyed in domain name. Blank space can be keyed in domain name.
Tunnel ID / Password	Identity and Password for server.
Password Mode	Select the power save mode. **For Windows 2000 User** There are two selections: Soft Token and Static Password. **For Vista User** There are four selections: Soft Token, Static Password, Windows Logon and Prompt User.

Client Certificate



EAP Method >> PEAP

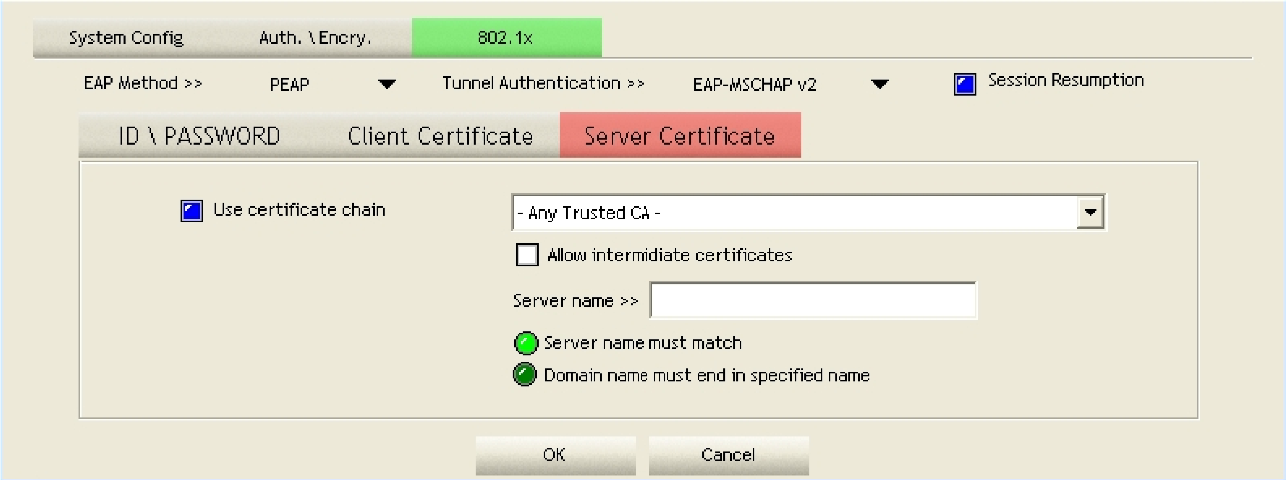
Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

☑ Use Client certificate

Items	Information
Use Client certificate	Client certificate for server authentication.
Use my smart card	Client certificate for server authentication.

Server Certificate



System Config | Auth. \ Encry. | 802.1x

EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

ID \ PASSWORD | Client Certificate | Server Certificate

☑ Use certificate chain

- Any Trusted CA -

□ Allow intermidiate certificates

Server name >>

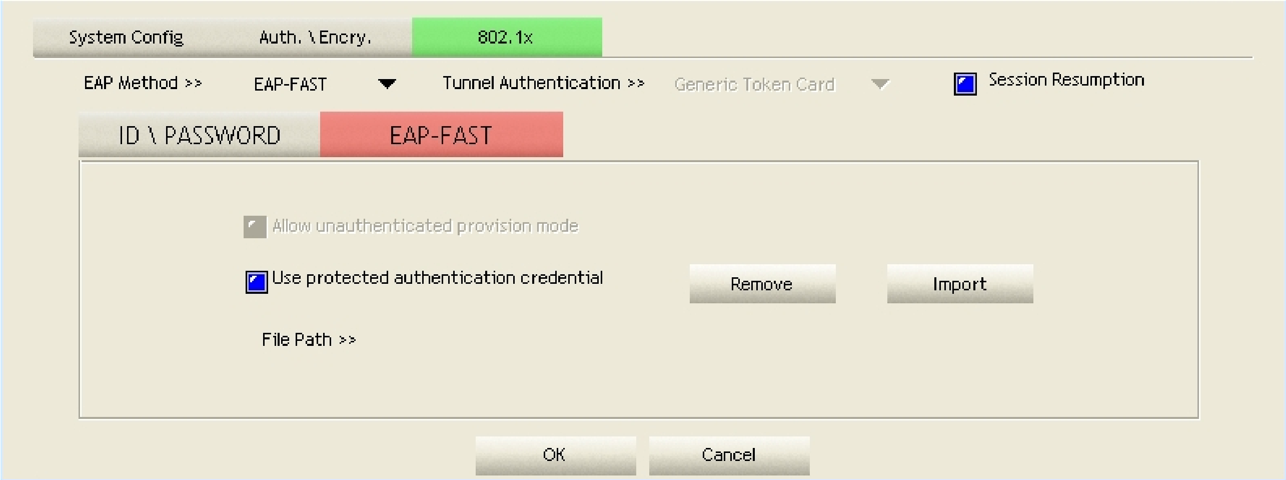
● Server name must match

● Domain name must end in specified name

OK | Cancel

Items	Information
Use Certificate chain	Mark the checkbox to enable using certification chain.
Allow intimidate certificates	Mark to allow intimidates certification.
Server name	Enter an authentication sever root.

EAP Fast



System Config | Auth. \ Encry. | 802.1x

EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card

☑ Session Resumption

ID \ PASSWORD | EAP-FAST

☑ Allow unauthenticated provision mode

☑ Use protected authentication credential

Remove | Import

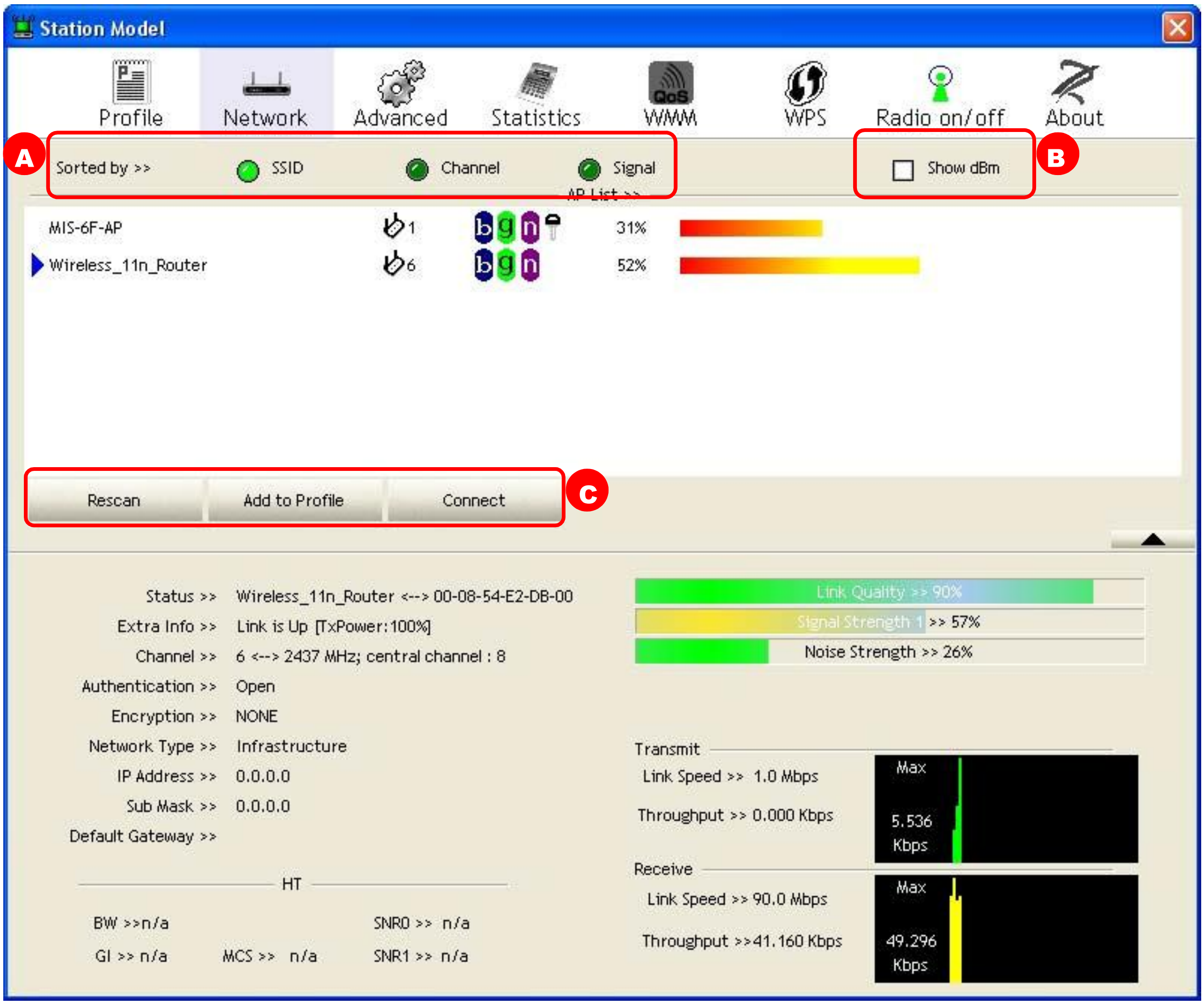
File Path >>

OK | Cancel

Items	Information
Allow unauthenticated provision mode	During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server. Mark to enable unauthenticated provision mode.
Use protected authentication credential	Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method. Mark to use protected authentication credential.

Network

This network lists the available wireless networks. The Utility connects to a wireless network with best signal strength automatically. You can change the connecting network by clicking on the network name and click the **Connect** button. To see detail information of each network, please double click on each item to pop up the information window.



MIS-6F-AP 1 b g n 31%
Wireless_11n_Router 6 b g n 52%

Status >> Wireless_11n_Router <--> 00-08-54-E2-DB-00
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437 MHz; central channel : 8
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 0.0.0.0
Sub Mask >> 0.0.0.0
Default Gateway >>

BW >>n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

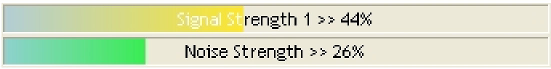
Link Quality >> 90%
Signal Strength 1 >> 57%
Noise Strength >> 26%

Transmit
Link Speed >> 1.0 Mbps
Throughput >> 0.000 Kbps
5.536 Kbps

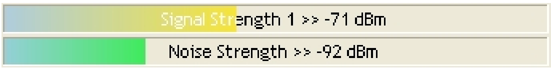
Receive
Link Speed >> 90.0 Mbps
Throughput >>41.160 Kbps
49.296 Kbps

A. Sorted by: Click each button to sort the listing networks by SSID, channel and Signal strength.

B. Show dBm: Mark the checkbox to show the signal and noise strength in dBm, unmark to show in percentage.



Signal Strength 1 >> 44%
Noise Strength >> 26%



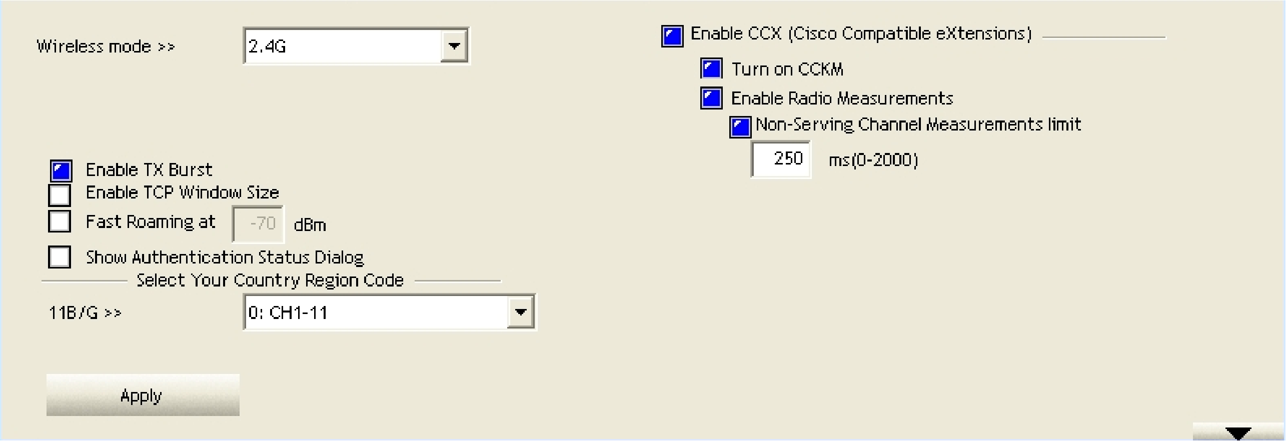
Signal Strength 1 >> -71 dBm
Noise Strength >> -92 dBm

C. Buttons: You can click on these buttons to add a new profile, edit, delete or activate an old profile.

Items	Information
Rescan	To rescan available wireless networks.
Connect	To connect to a designated network.
Add to Profile	To add a network to profile after selecting a network.

Advanced

This page provides advanced configurations to this adapter. Please refer to the following chart for definitions of each item.



Wireless mode >> 2.4G

☑ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

Select Your Country Region Code

11B/G >> 0: CH1-11

Apply

☑ Enable CCX (Cisco Compatible eXtensions)

☑ Turn on CCKM

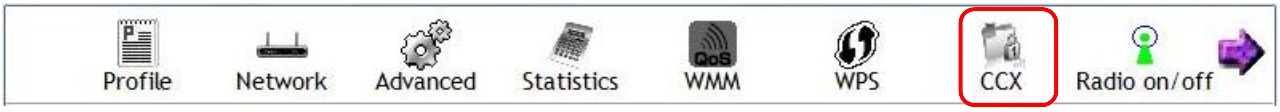
☑ Enable Radio Measurements

☑ Non-Serving Channel Measurements limit

250 ms(0-2000)

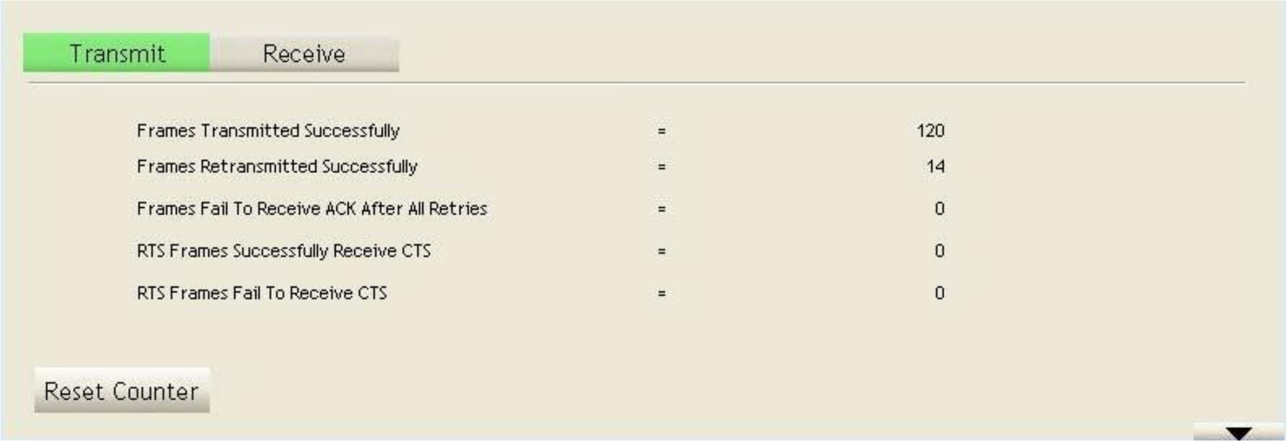
Items	Information
Wireless mode	Select wireless mode. Only 2.4G is supported.
Enable TX Burst	Select to enable connecting to a TX Burst supported device.
Enable TCP Window Size	Mark the checkbox to enable TCP window size, which help enhance throughput.
Fast Roaming at ___dBm	Mark the checkbox to enable fast roaming. Specify the transmit power for fast roaming.
Show Authentication Status Dialog	Mark the checkbox to show "Authentication Status Dialog" while connecting to an AP with authentication. Authentication Status Dialog displays the process about 802.1 x authentications.
Enable CCX (Cisco Compatible extensions)	Select to enable CCX. This function can only be applied when connecting to a Cisco compatible device.
Turn on CCKM	Mark to enable CCKM.
Enable Radio Measurements	Mark to enable channel measurement every 0~2000 milliseconds.
Non-Serving Channel Measurements limit	Mark to revise the channel measurement.

Note: For Vista user, click on the CCX button to do more configuration. Please refer to CCX for more information.



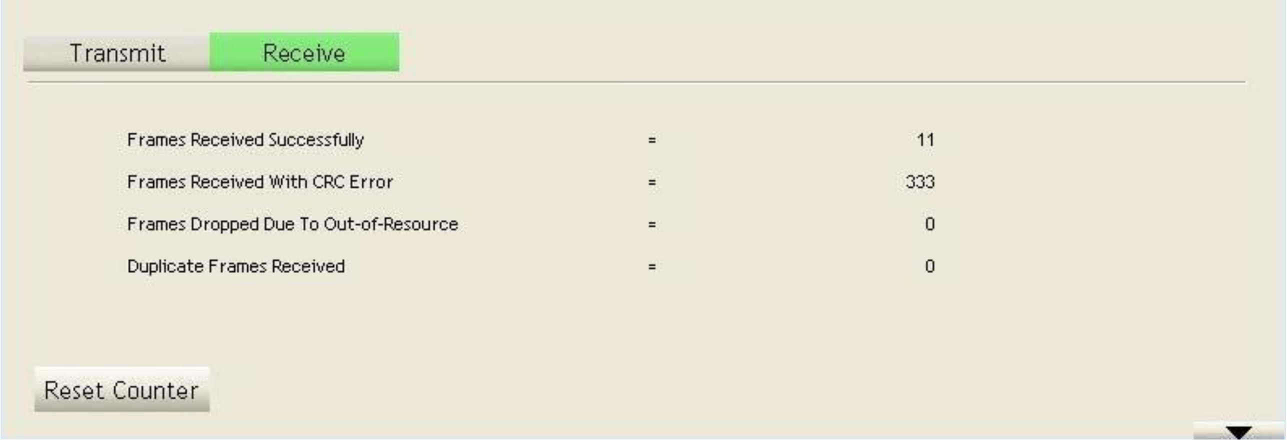
Statistics

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.



Frames Transmitted Successfully	=	120
Frames Retransmitted Successfully	=	14
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0

Items	Information
Frames Transmitted Successfully	Frames successfully sent.
Frames Retransmitted Successfully	Successfully retransmitted frames numbers.
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	Failed to receive CTS after sending RTS.
Reset Counter	Reset counters to zero.

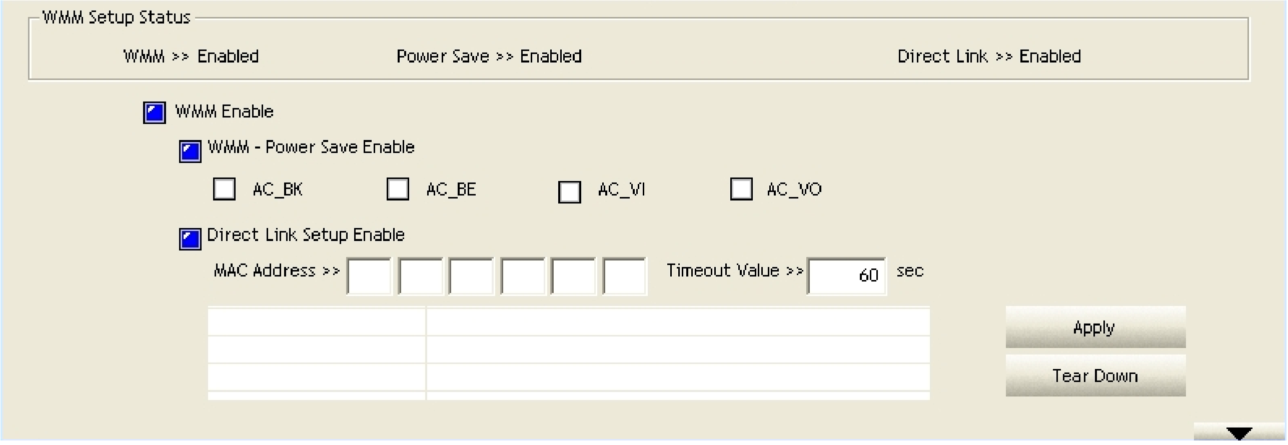


Frames Received Successfully	=	11
Frames Received With CRC Error	=	333
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

Items	Information
Frames Received Successfully	Frames received successfully.
Frames Received With CRC Error	Frames received 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.

WMM

This page allows users to activate the WMM function for this device. Please note that this function only works while connecting to a WMM compatible device.



WMM Setup Status

WMM >> Enabled Power Save >> Enabled Direct Link >> Enabled

☑ WMM Enable

☑ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

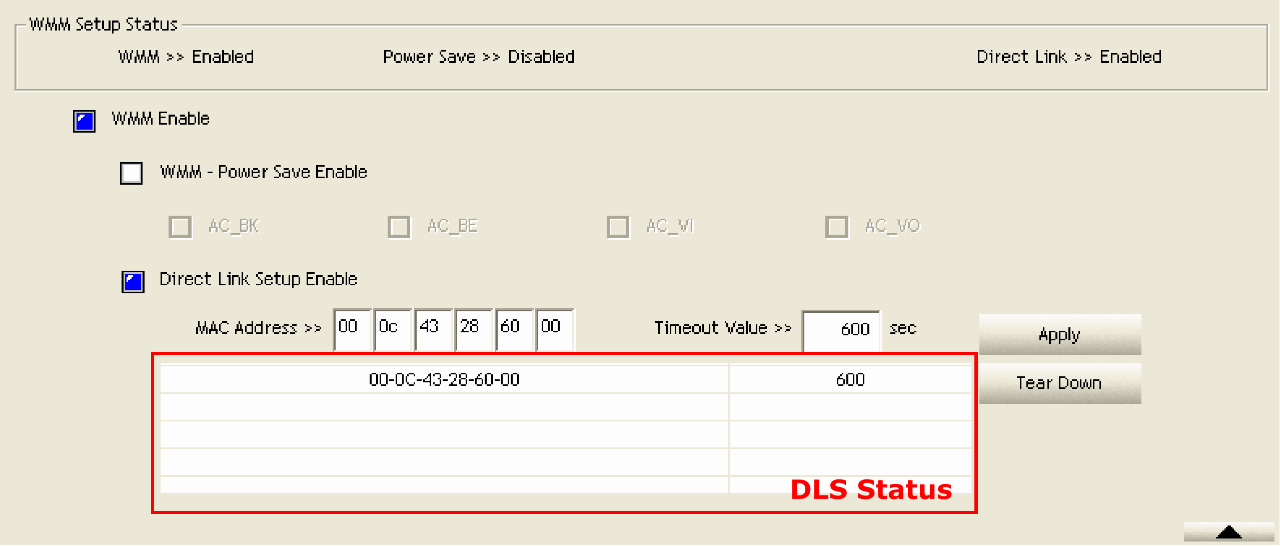
☑ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

Items	Information
WMM Enable	Enable Wi-Fi Multi-Media.
WMM - Power Save Enable	Enable WMM Power Save. Please enable WMM before configuring this function.
Direct Link Setup Enable	Enable DLS (Direct Link Setup). Please enable WMM before configuring this function.
MAC Address	Fill in the blanks of Direct Link with MAC Address of STA.
Timeout Value	Time of automatically disconnect 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.
Apply / Tear Down	After fill in the "MAC Address" and "Timeout Value", click "Apply" button to save your configuration. The result will appear in the following "DLS Status" blanks. To remove the configuration, please select the configuration in the blanks and then click "Tear Down" button.

Steps to enable Direct Link Setup function:

1. Click the "Direct Link Setup Enable" checkbox.
2. Change to "Network" function. Add an AP that supports DLS features to the Profile.
3. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to these two conditions:
   y Connect with an AP that supports DLS features.
   y Ensure that DLS is enabled
4. Fill in the Timeout Value and then click Apply.
5. After configuring the DLS successfully, the MAC address and Timeout Value are displayed in the "DLS Status".



WMM Setup Status

WMM >> Enabled   Power Save >> Disabled   Direct Link >> Enabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

☑ Direct Link Setup Enable

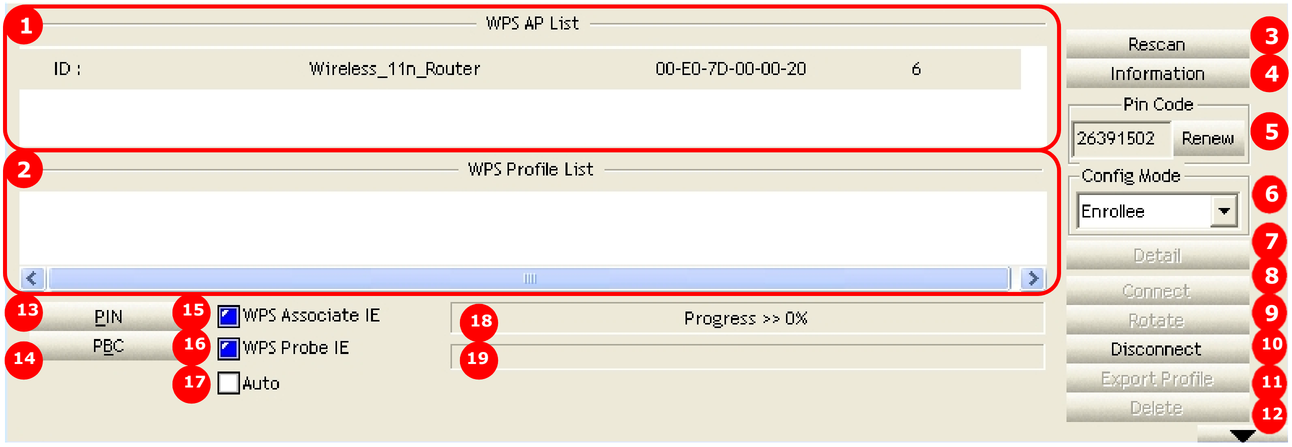
MAC Address >> 00 0c 43 28 60 00   Timeout Value >> 600 sec

00-0C-43-28-60-00	600

6. If you want to disconnect Direct Link Setup, select the list in "DLS Status" and then click on the Tear Down button.

WPS

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



ID : Wireless_11n_Router 00-E0-7D-00-00-20 6

Pin Code: 26391502

Config Mode: Enrollee

☑ WPS Associate IE
☑ WPS Probe IE
□ Auto

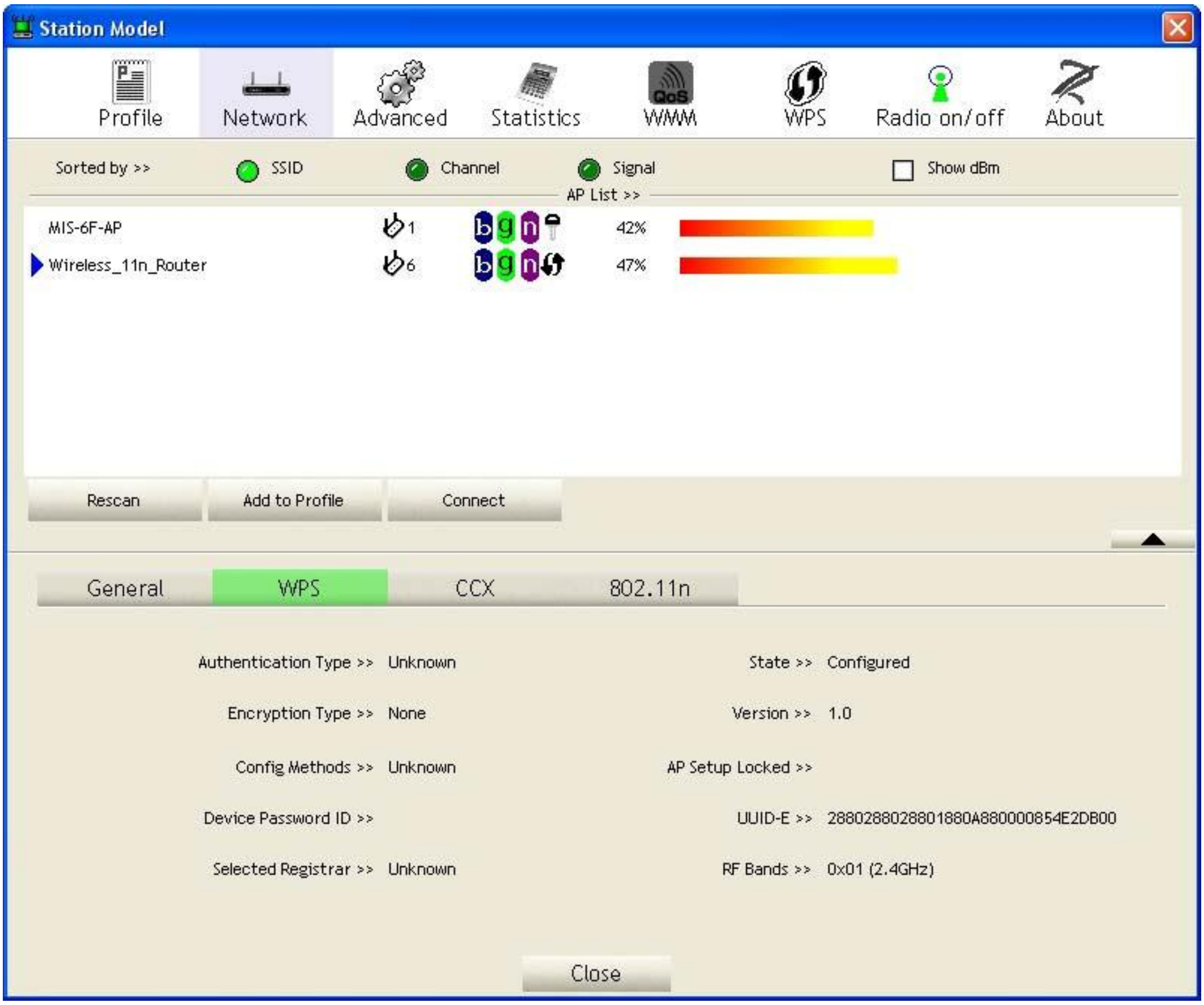
Progress >> 0%

Items	Information
1. 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), and Security-Enabled.
2. 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, Utility creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.
3. Rescan	Click to rescan the wireless networks.
4. 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.
5. Pin Code	8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each Network card has only one PIN Code of Enrollee. Click on the Renew button to renew the PIN code.
6. Config Mode	Enrollee or an external Registrar.
7. Detail	Information about Security and Key in the credential.
8. Connect	Command to connect to the selected network inside credentials.
9. Rotate	Command to connect to the next network inside credentials.
10. Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of Utility if exists. If there is an empty profile page, the driver will select any non-security AP.
11. Export Profile	Click the "Export Profile" button will export the WPS profile.
12. 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.
13. PIN	Start to add to Registrar using PIN configuration method.
14. PBC	Start to add to AP using PBC configuration method.
15. WPS associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
16. WPS probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
17. Auto	Select the AP automatically.
18. Progress Bar	Display rate of progress from Start to Connected status.
19. Status Bar	Display currently WPS Status.

The following description divides into four parts:

A. **WPS Information on AP**
B. **Example of Adding to Registrar Using PIN Method**
C. **Example of Adding to Registrar Using PIN Method**
D. **Example of Configuring a Network/AP Using PIN or PBC Method**

A. WPS Information on AP: On Network AP list, double click on the AP then you can see the information appears below.



MIS-6F-AP	1	b g n	42%
Wireless_11n_Router	6	b g n	47%

Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Configured

Version >> 1.0

AP Setup Locked >>

UUID-E >> 2880288028801880A880000854E2DB00

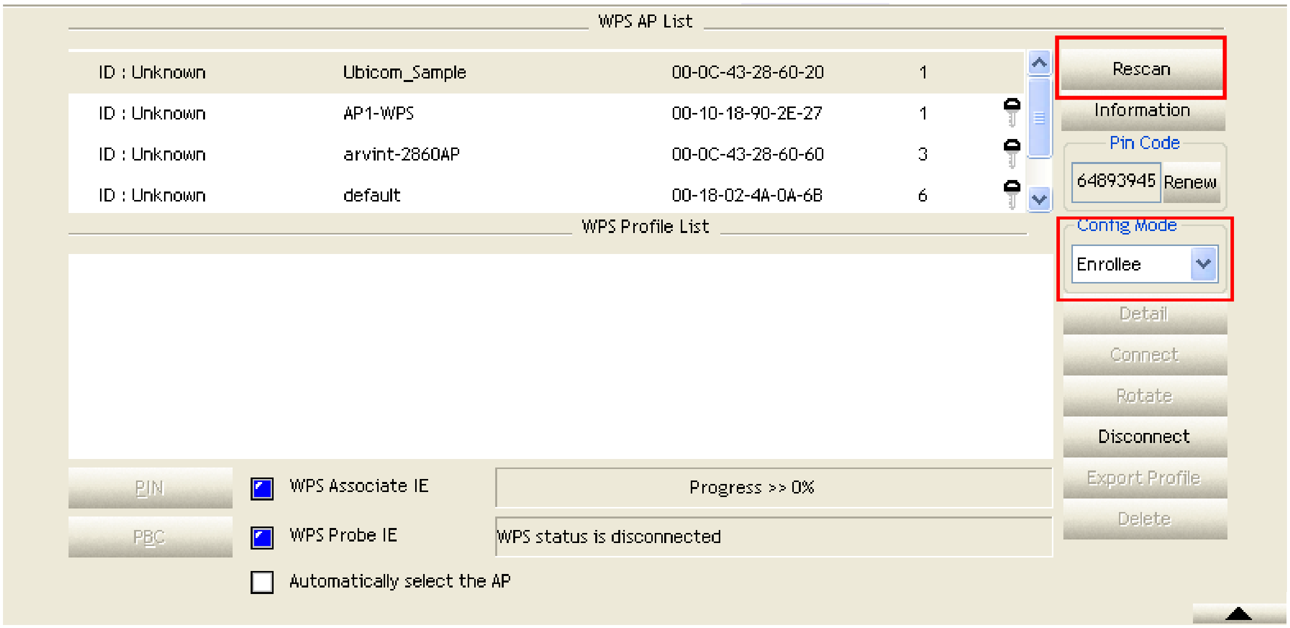
RF Bands >> 0x01 (2.4GHz)

Items	**Information**
Authentication Type	There are three authentication modes supported by this utility. They are open, Shared, WPA-PSK and WPA system.
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.
Config Methods	Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (a bitwise OR of values)
Device Password ID	Indicates the method or identifies the specific password that the selected Registrar intends to use. APs in PBC mode must indicate 0x0004 within two-minute Walk Time.
Selected Registrar	Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
State	The current configuration state on AP. The values are "Unconfigured" and "Configured".
Version	WPS specified version.
AP Setup Locked	Indicates if the AP has entered a setup locked state.
UUID-E	The universally unique identifier (UUID) element generated by the Enrollee. This is a 16 byte value.
RF Bands	Indicates all the RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

B. Example of Adding to Registrar Using PIN Method

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. Please follow the step below.

1. Select "Enrollee" from the Config Mode drop-down list.
2. Click "Rescan" to update available WPS APs.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

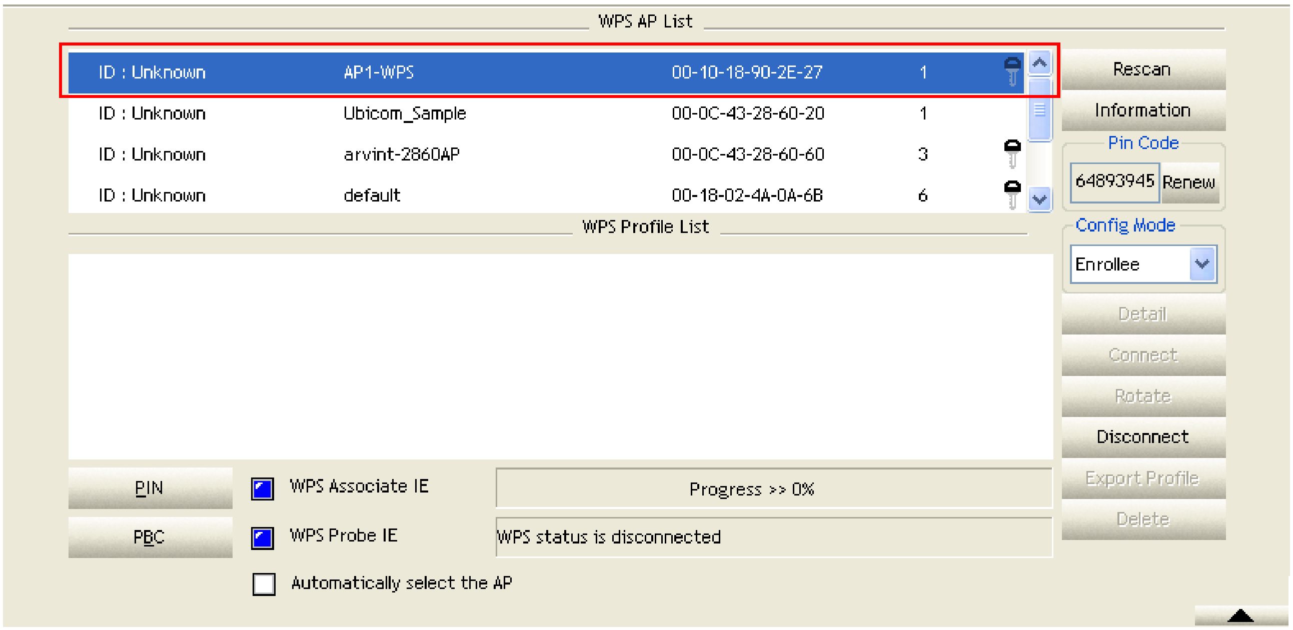
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

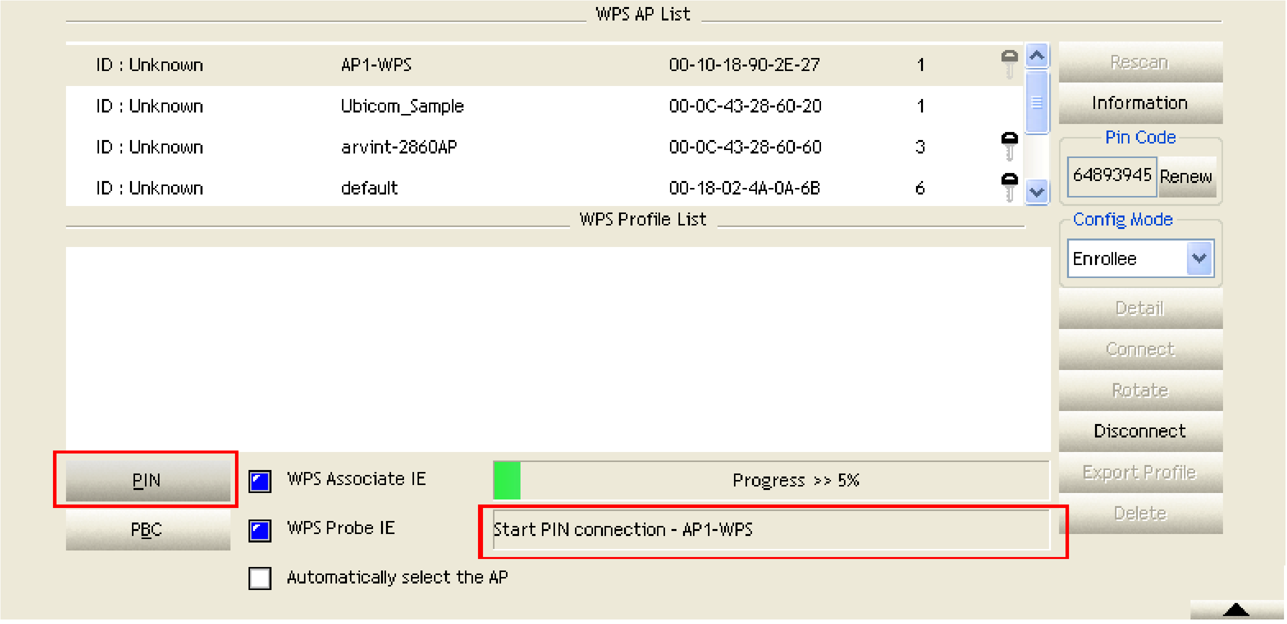
□ Automatically select the AP

Progress >> 0%

WPS status is disconnected

4. Click "PIN" to enter the PIN.

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



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 5%

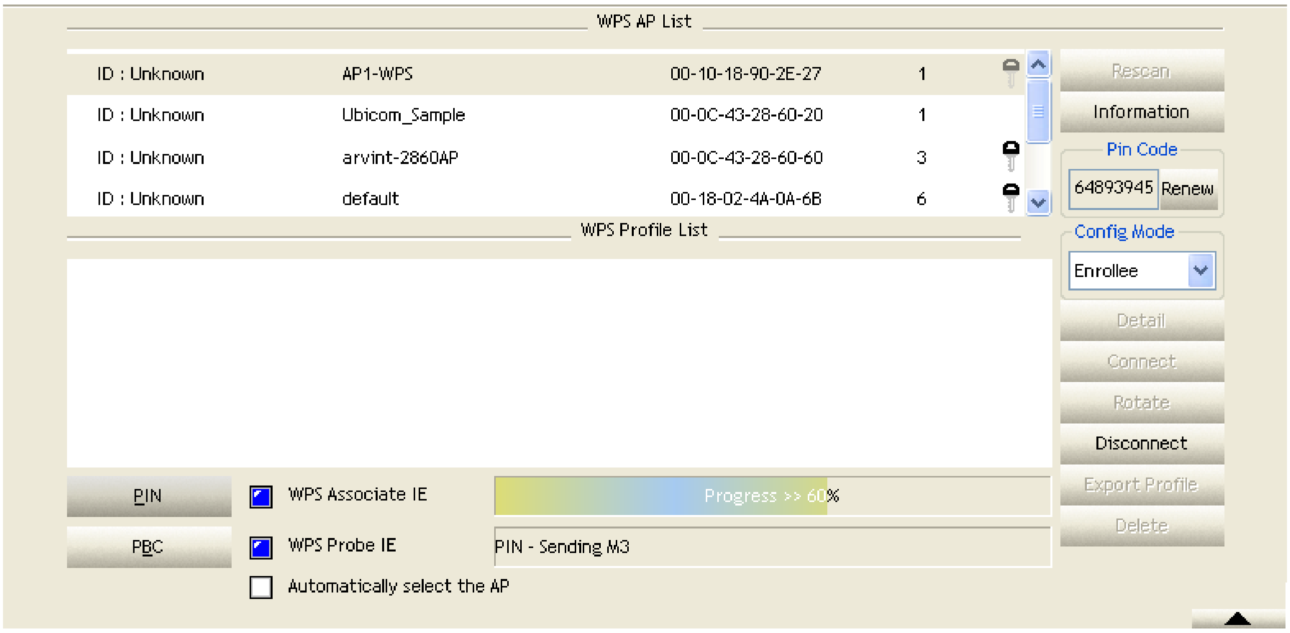
Start PIN connection - AP1-WPS

Note:

y Allow of an exchange between Step 4 and Step 5.

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

6. The result should appear as the image below.



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

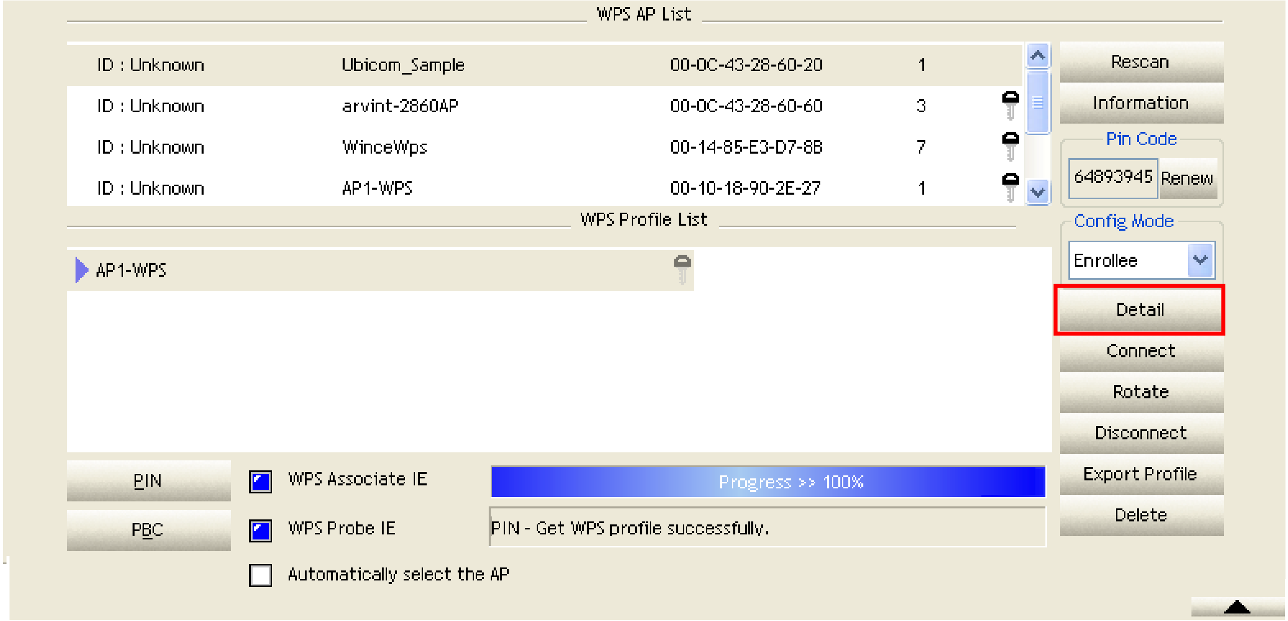
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 60%

PIN - Sending M3

7. Configure one or more credentials. Then connect successfully.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

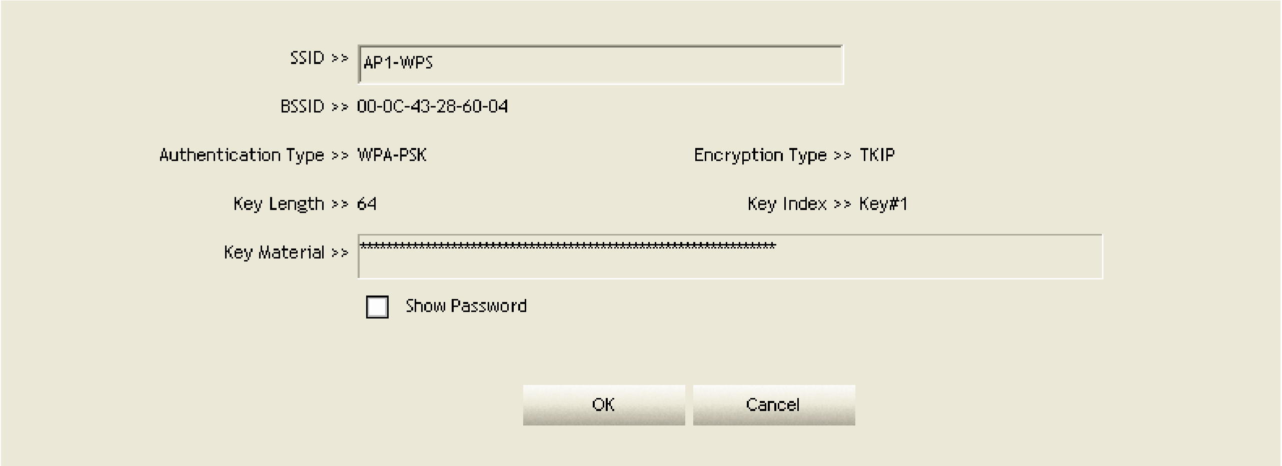
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

8. Click "Detail." You can see the figure below.



SSID >> AP1-WPS

BSSID >> 00-0C-43-28-60-04

Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Key Length >> 64

Key Index >> Key#1

Key Material >> **

□ Show Password

C. Example of Adding to the Registrar Using the PBC Method

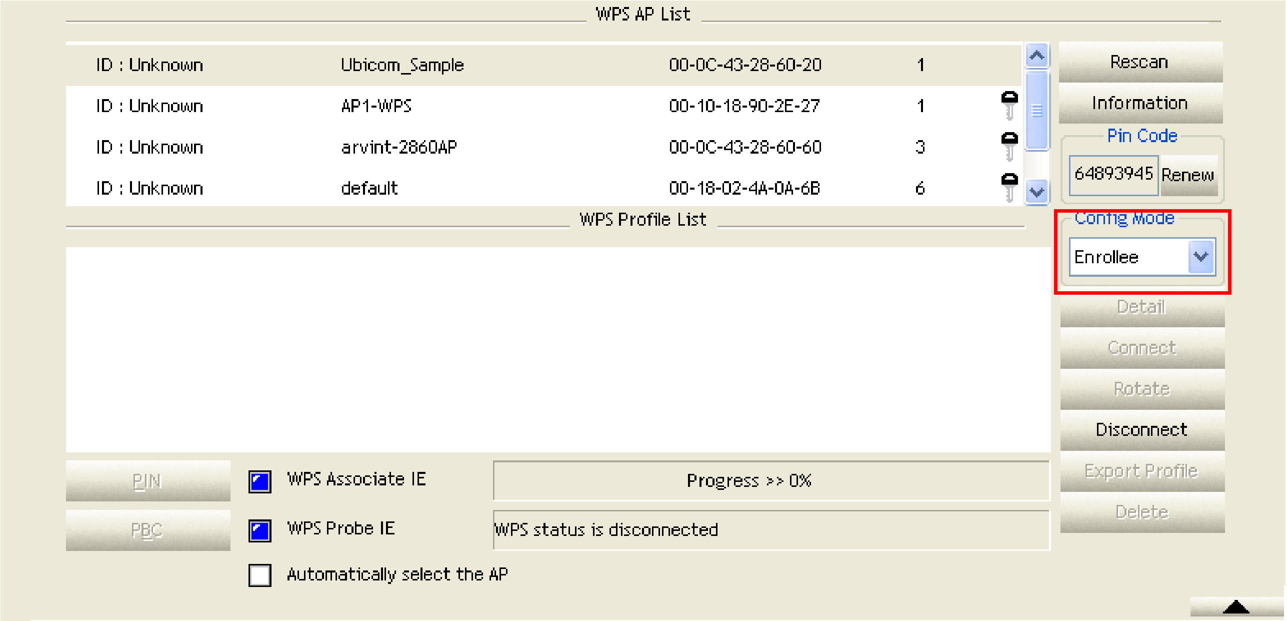
The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately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

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

Note: Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC mode or APs using PBC mode have left their Walk Time. The user can configure WPS profiles with either PIN method or PBC method.

Please follow the steps below.

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



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

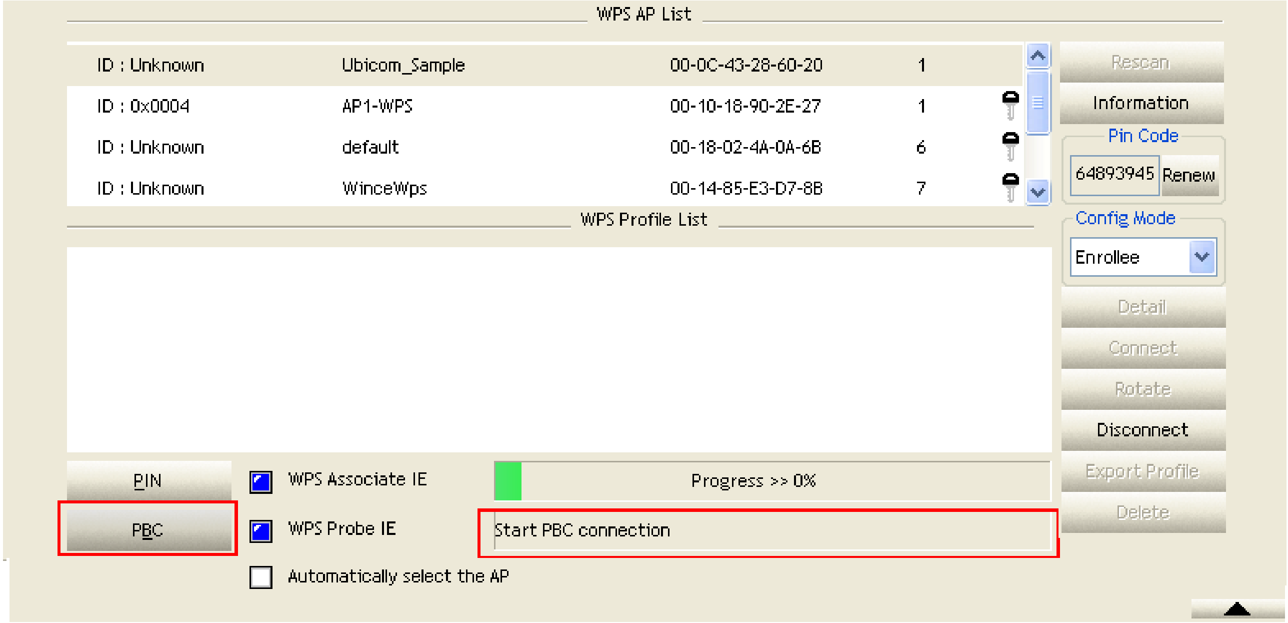
Progress >> 0%

WPS status is disconnected

2. Click PBC to start the PBC connection.

3. Push the PBC on AP.

Note: Allow time for an exchange between Step 2 and Step 3.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

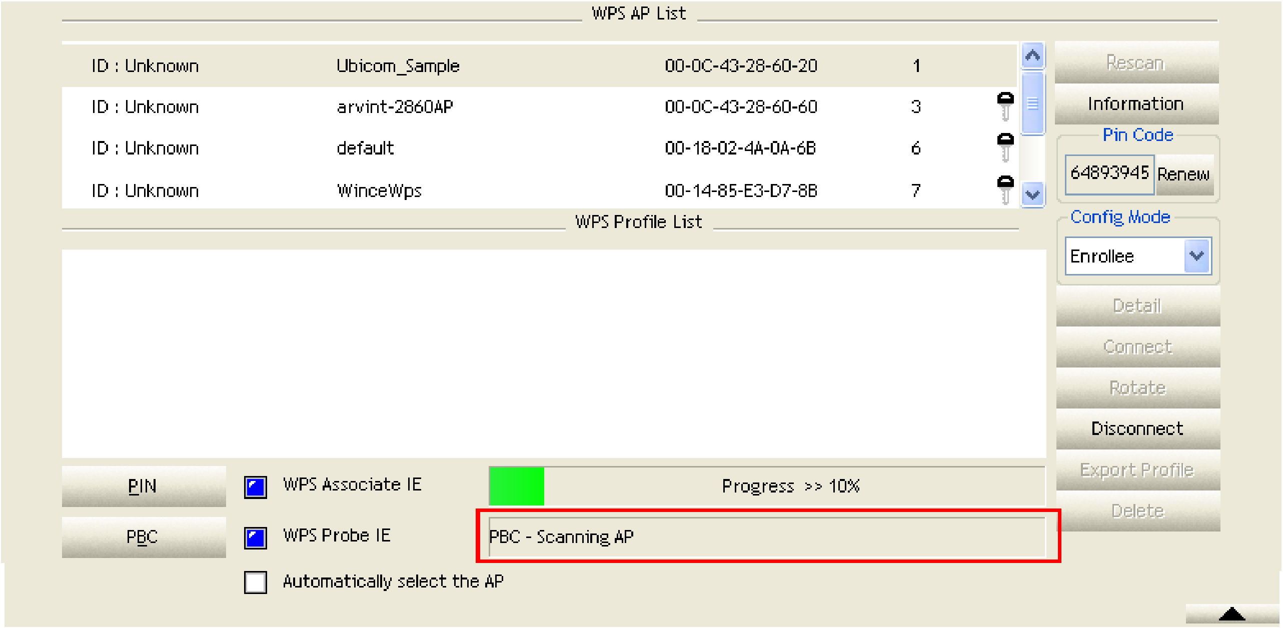
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

Start PBC connection

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



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1	
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3	🔑
ID : Unknown	default	00-18-02-4A-0A-6B	6	🔑
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7	🔑

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

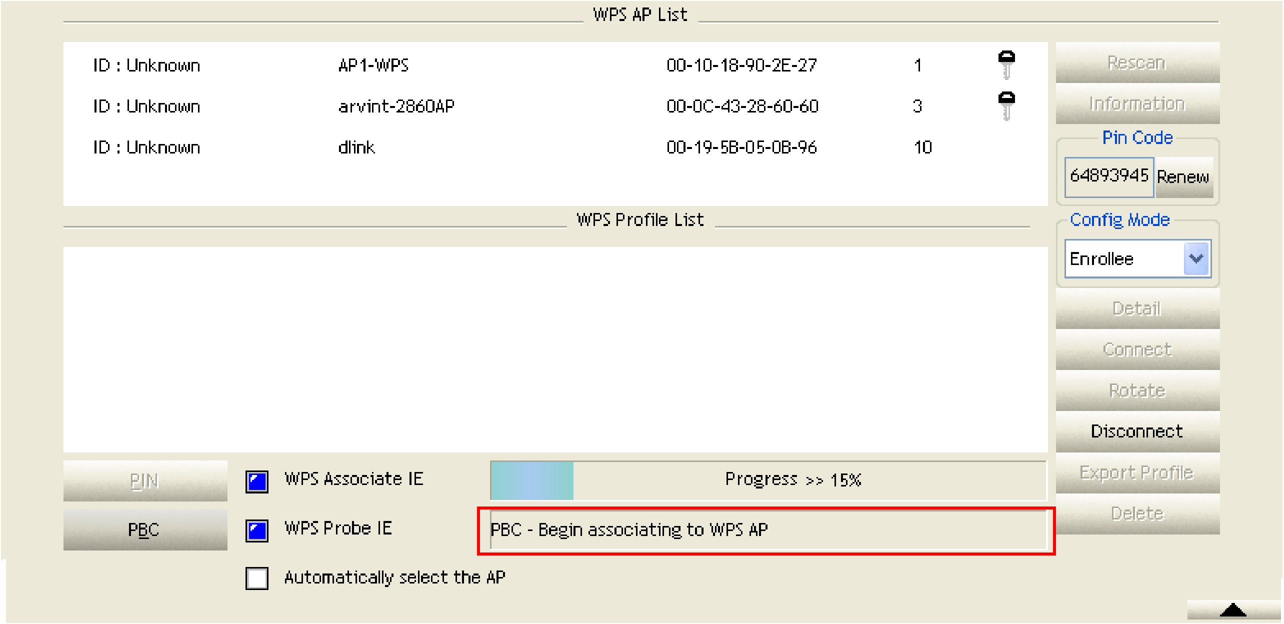
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 10%

PBC - Scanning AP

5. When one AP is found, join it.



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1	🔑
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3	🔑
ID : Unknown	dlink	00-19-5B-05-0B-96	10	

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

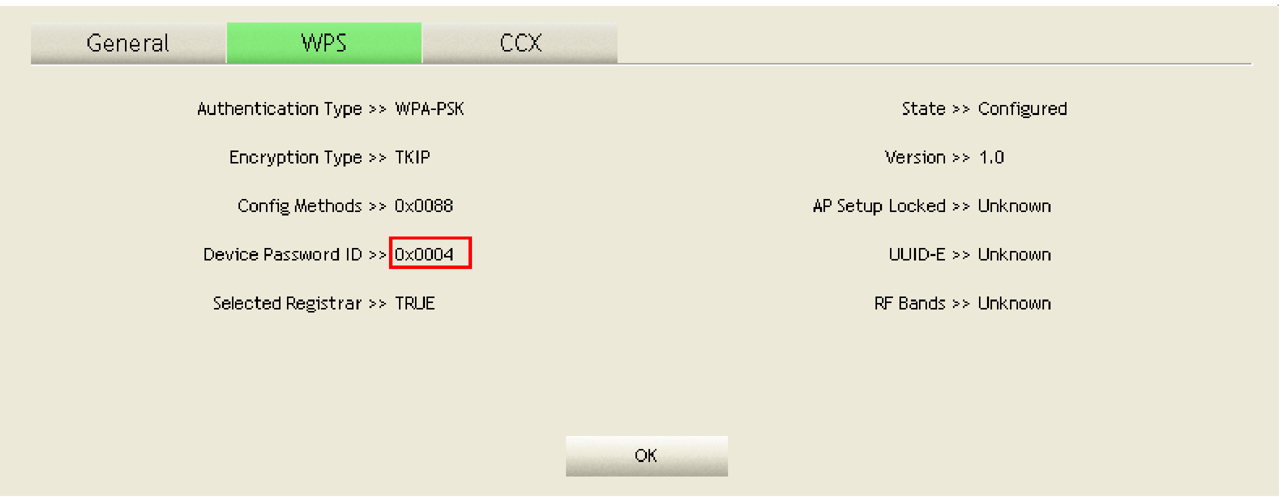
☑ WPS Probe IE

□ Automatically select the AP

Progress >> 15%

PBC - Begin associating to WPS AP

6. Check WPS Information on the available WPS APs.



Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Config Methods >> 0x0088

Device Password ID >> 0x0004

Selected Registrar >> TRUE

State >> Configured

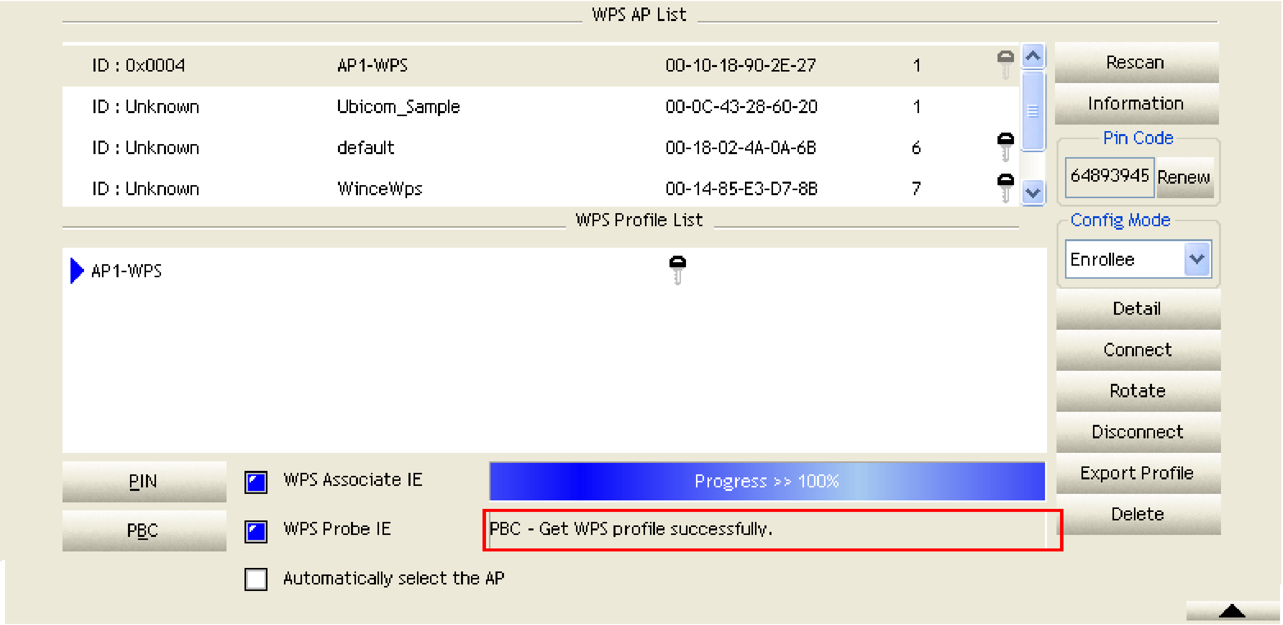
Version >> 1.0

AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

7. Configure and receive one or more credential(s).Then connect successfully. The result will be displayed as it is in the figure below.



ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

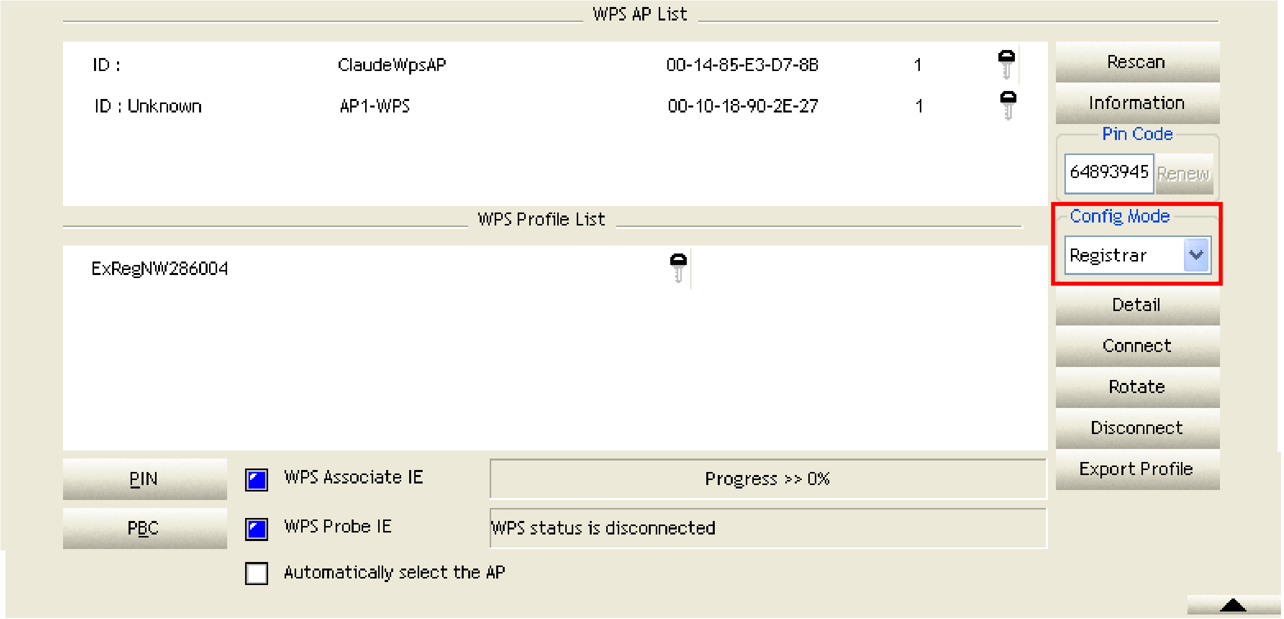
□ Automatically select the AP

Progress >> 100%

PBC - Get WPS profile successfully.

D. Example of Configuring a Network/AP Using PIN or PBC Method

1. Select "Registrar" from the Config Mode drop-down list.



WPS AP List

ID :	ClaudeWpsAP	00-14-85-E3-D7-8B	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

WPS Profile List

ExRegNW286004

Pin Code: 64893945

Config Mode: Registrar

☑ WPS Associate IE

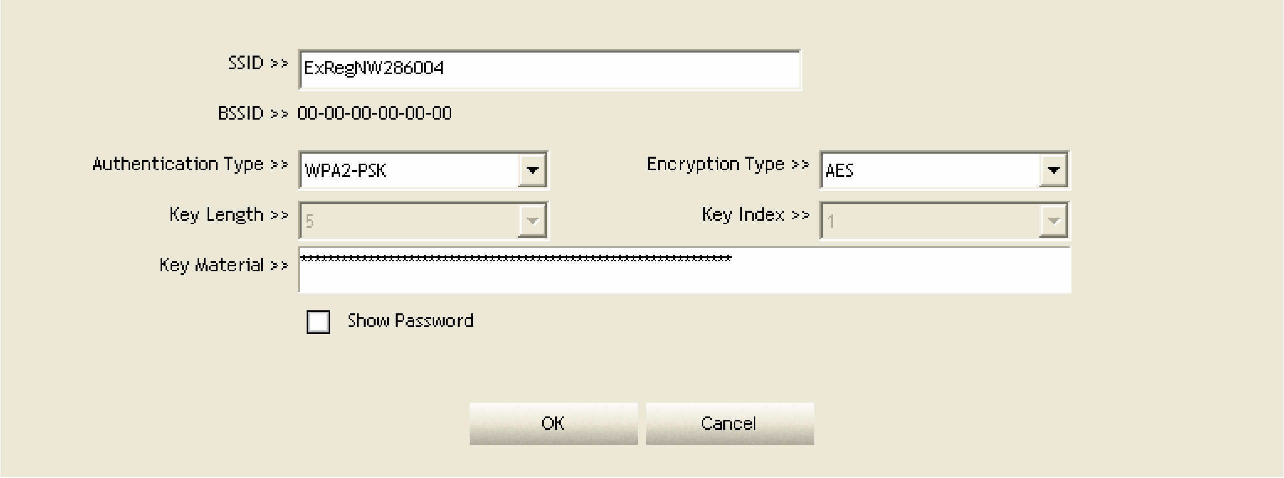
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



SSID >> ExRegNW286004

BSSID >> 00-00-00-00-00-00

Authentication Type >> WPA2-PSK

Encryption Type >> AES

Key Length >> 5

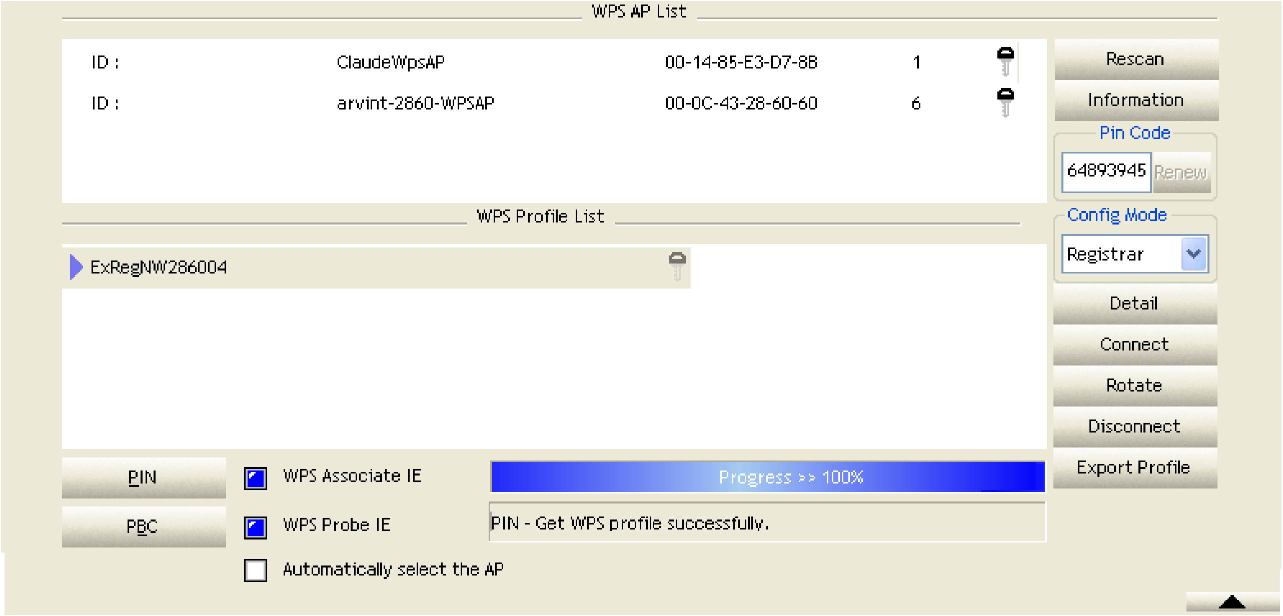
Key Index >> 1

Key Material >> **

☐ Show Password

3. If the PIN configuration is setup, enter the PIN sent from the Enrollee.
4. Start PIN or PBC. The following procedures are as similar as section PIN Enrollee Setup or PBC Enrollee Setup.

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



WPS AP List

ID :	ClaudeWpsAP	00-14-85-E3-D7-8B	1
ID :	arvint-2860-WPSAP	00-0C-43-28-60-60	6

Pin Code: 64893945

Config Mode: Registrar

WPS Profile List

ExRegNW286004

☑ WPS Associate IE

☑ WPS Probe IE

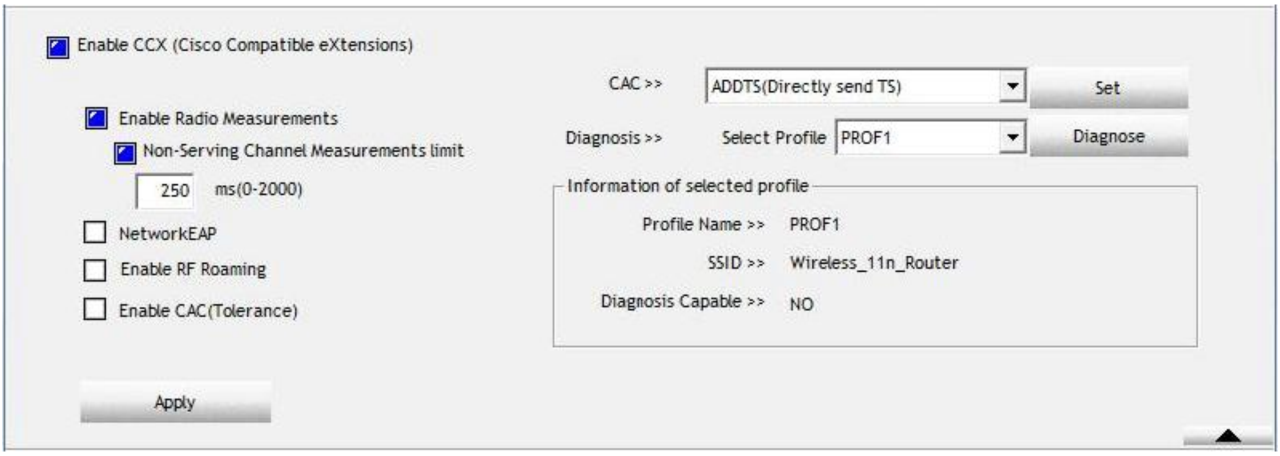
□ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

CCX

This page is available for ***Vista user only***. It provides CCX configurations to this adapter. Please refer to the following chart for definitions of each item.



☑ Enable CCX (Cisco Compatible eXtensions)

☑ Enable Radio Measurements

☑ Non-Serving Channel Measurements limit

250 ms(0-2000)

☐ NetworkEAP

☐ Enable RF Roaming

☐ Enable CAC(Tolerance)

Apply

CAC >> ADDTS(Directly send TS) Set

Diagnosis >> Select Profile PROF1 Diagnose

Information of selected profile

Profile Name >> PROF1

SSID >> Wireless_11n_Router

Diagnosis Capable >> NO

Items	Information
Enable CCX (Cisco Compatible extensions)	Select to enable CCX. This function can only be applied when connecting to a Cisco compatible device.
Turn on CCKM	Mark to enable CCKM.
Enable Radio Measurements	Mark to enable channel measurement every 0~2000 milliseconds.
Non-Serving Channel Measurements limit	Mark to revise the channel measurement.
Network EAP	Enable the NetwrokEAP authentication algorithm.
Enable RF Roaming	Enable RF roaming function
Enable CAC (Tolerance)	Enable the call admission control
CAC	There are four selections: ADDTS (Directly send TS), DELTS, and RESET. Select an item from the drop down list and then click on the Set button.
Diagnosis	Select a profile which the user wants to diagnose, and then click on the Diagnose button to perform the Diagnose test.

Radio On/Off

Click on the button to enable/disable wireless connection status.

Connected: Radio On/Off

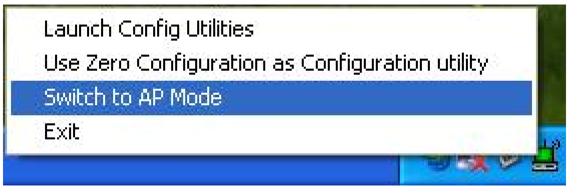
Disconnected: Radio On/Off

AP mode management guide for Windows 2000/XP/Vista

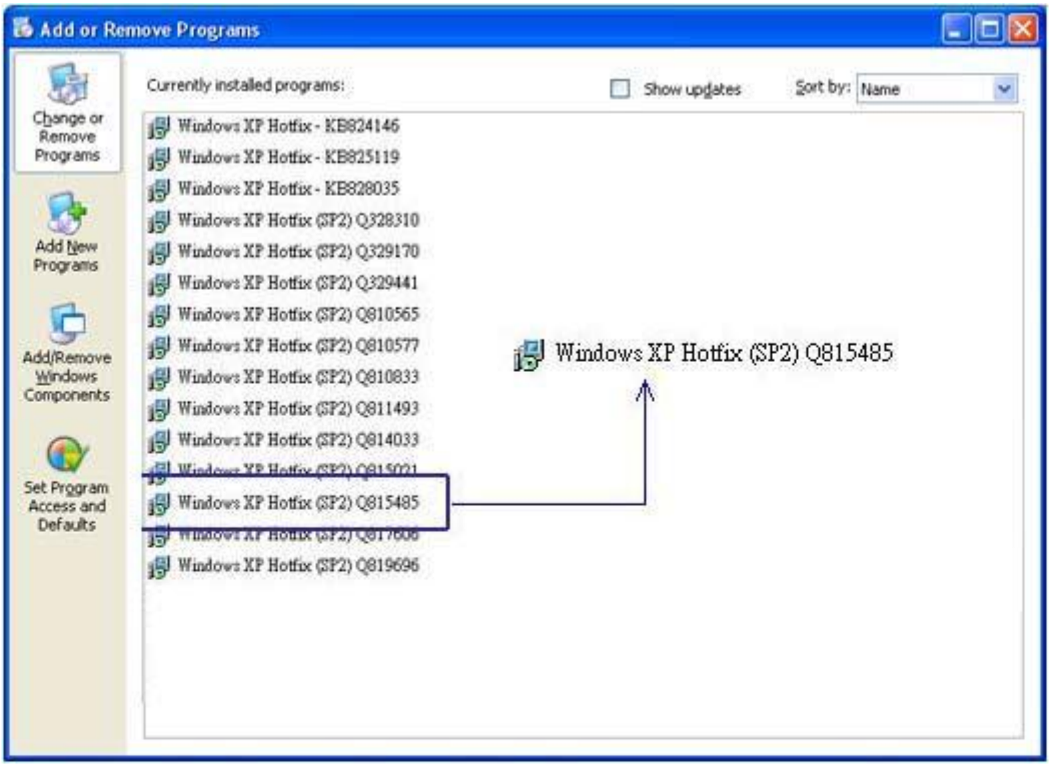
If you wish to share the Internet access with the wireless stations in your environment, you can configure this wireless adapter as a software access point (Soft AP). In this mode, this wireless adapter becomes the wireless access point that provides local area network and Internet access for your wireless stations.

To use this adapter as an access point, please right click the icon on system tray and

select **Switch to AP mode**. Please refer to the following introduction and information about this AP-mode utility.



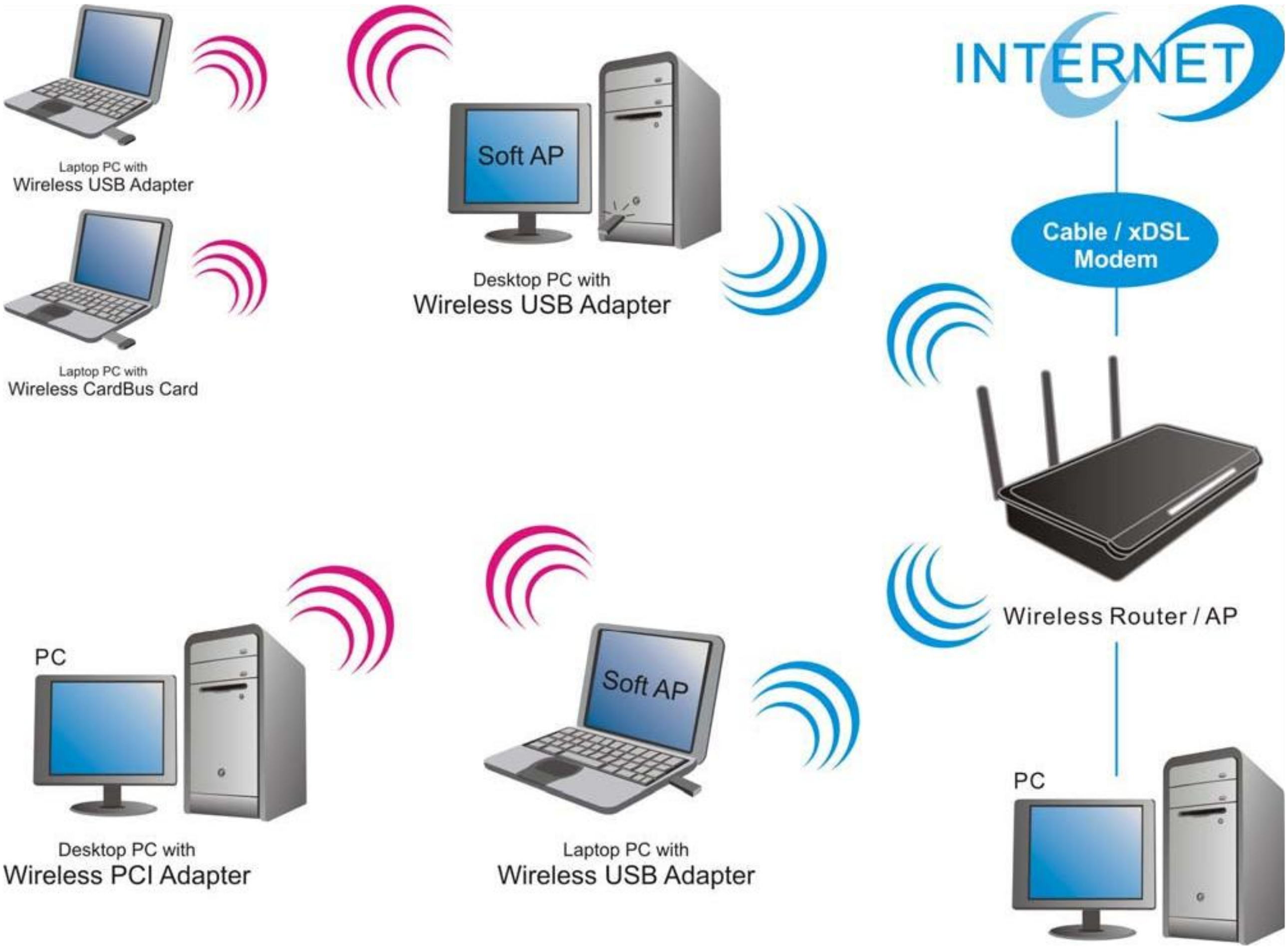
Note: In windows XP, it provides WPA support at hotfix Q815485. However; you have to make sure that hotfix Q815485 (require XP SP1 installed) has been installed in your system before you can start using WPA features. You can check the installation of hotfix in add/remove software page under control panel.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Show updates
Sort by:
Name
Windows XP Hotfix (SP2) Q815485

Currently installed programs:

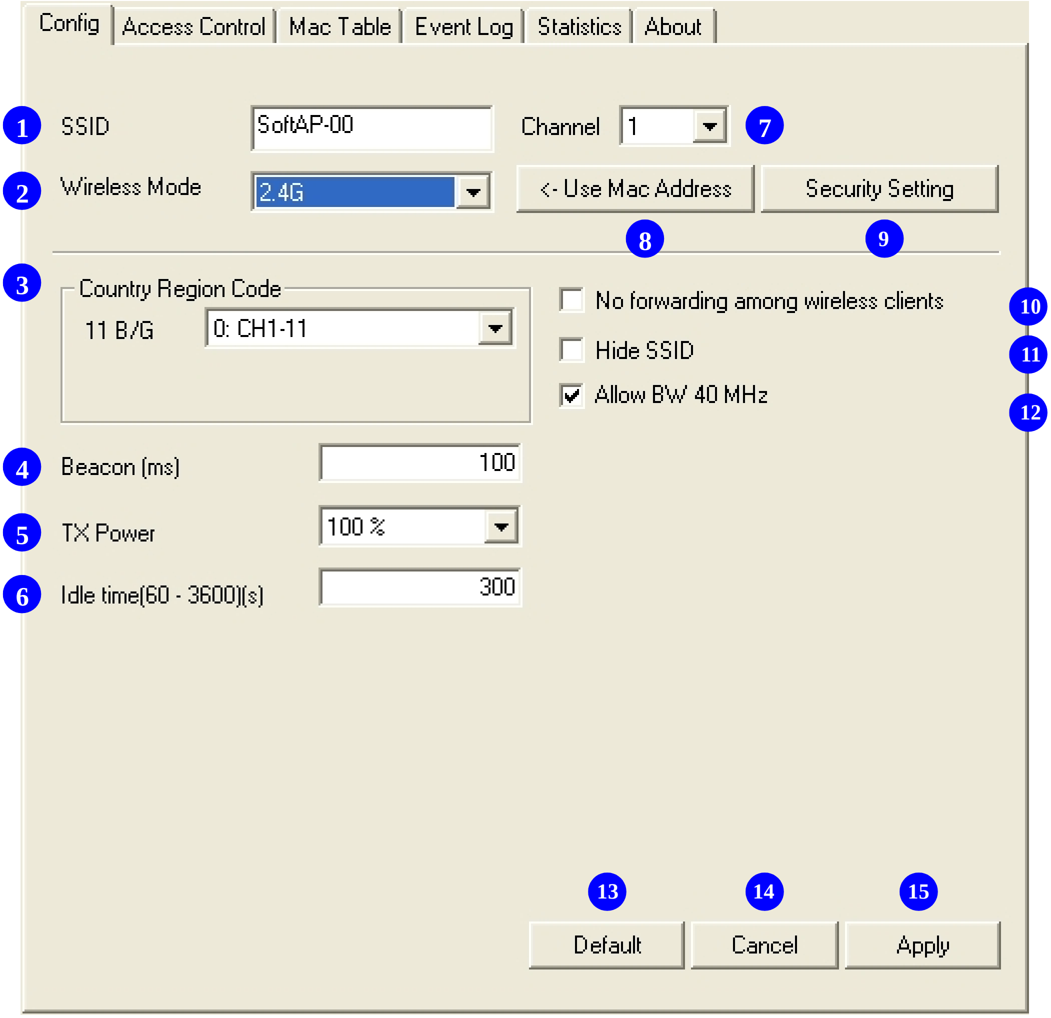
- Windows XP Hotfix - KB824146
- Windows XP Hotfix - KB825119
- Windows XP Hotfix - KB828035
- Windows XP Hotfix (SP2) Q328310
- Windows XP Hotfix (SP2) Q329170
- Windows XP Hotfix (SP2) Q329441
- Windows XP Hotfix (SP2) Q810565
- Windows XP Hotfix (SP2) Q810577
- Windows XP Hotfix (SP2) Q810833
- Windows XP Hotfix (SP2) Q811493
- Windows XP Hotfix (SP2) Q814033
- Windows XP Hotfix (SP2) Q815021
- Windows XP Hotfix (SP2) Q815485
- Windows XP Hotfix (SP2) Q817606
- Windows XP Hotfix (SP2) Q819696

Software Access Point (Soft AP) Application



Config

This page provides overall configuration to this adapter. Please find the following items for identification to each field.



SSID: SoftAP-00

Channel: 1

Wireless Mode: 2.4G

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

1. **SSID:** AP name of user type. User also can select [Use Mac Address] to display it.
2. **Wireless Mode:** Select wireless mode. Only 2.4G is supported.

3. **Beacon (ms):** The time between two beacons. System default is 100

   ms.

4. **TX Power:** Manually force the AP transmits power. System default is 100%.

5. **Idle Time:** Manually force the Idle Time using selected value. Default is 300.

6. **Channel:** Manually force the AP using the channel. System default is channel 1.

7. **Use Mac Address:** Use MAC address of used wireless card to be AP name. System default is APX (X is last number of Mac Address).

8. **Security Setting:** Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.

9. **No forwarding among wireless clients:** If there is no beacon among the wireless clients, they can't share information with each other.

10. **Hide SSID:** Prevent this AP from recognized in wireless network. This is disabled as default.

11. **Allow BW40 MHz:** Allow BW40 MHz capability.

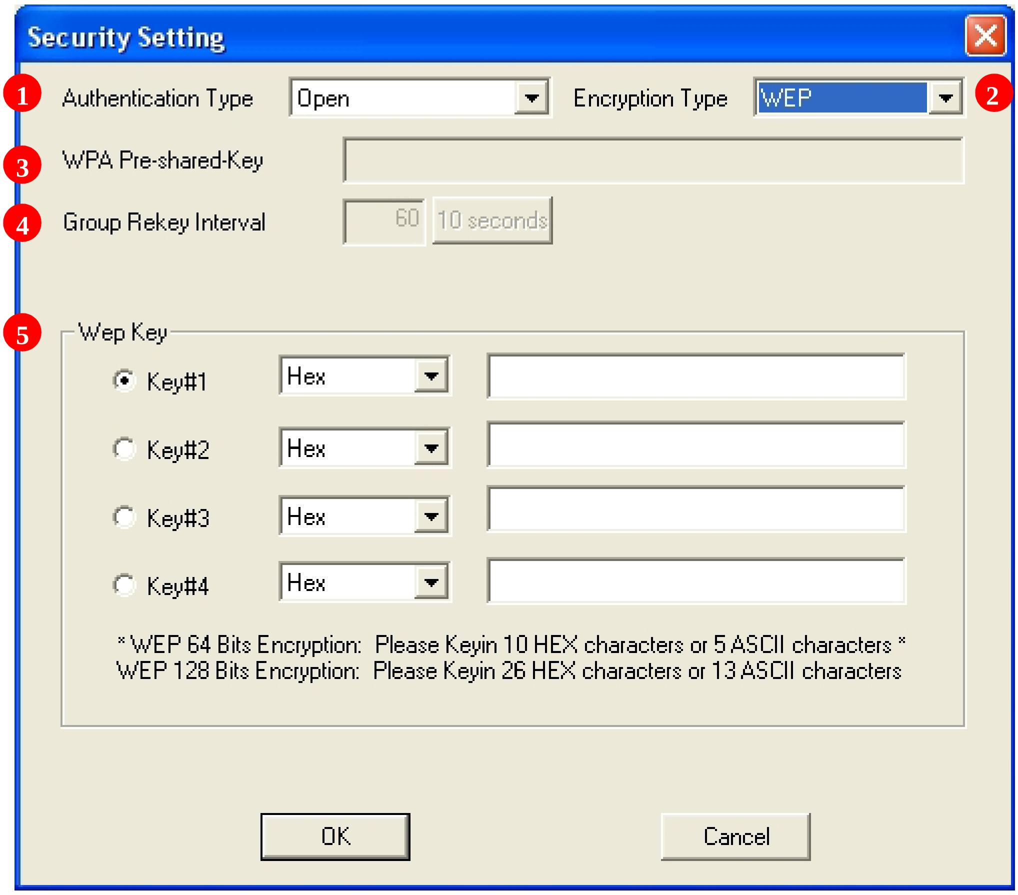
12. **Default:** Use system default value.

13. **Cancel:** Cancel the above changes.

14. **Apply**: Apply the above changes.

Security Setting

This page pops up after clicking the **Security Setting** button. Please follow the instructions below:



* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters *
WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

1. **Authentication Type:** Select to be open, shared, WPA-PSK, WPA2-PSK, or WPA PSK/WPA2-PSK system.
2. **Encryption Type:** Select an encryption type from the drop list.
3. **WPA Pre-shared Key:** A shared string between AP and STA. For WPA-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 lengths.
4. **Group Rekey Interval:** Only valid when using WPA-PSK encryption algorithm. The key will change compliance with seconds or beacon that user set.
5. **WEP Key:** Only valid when using WEP encryption algorithm. The key must match the key on AP. There are several formats to enter the keys.

   a. Hexadecimal (40bits): 10 Hex characters.

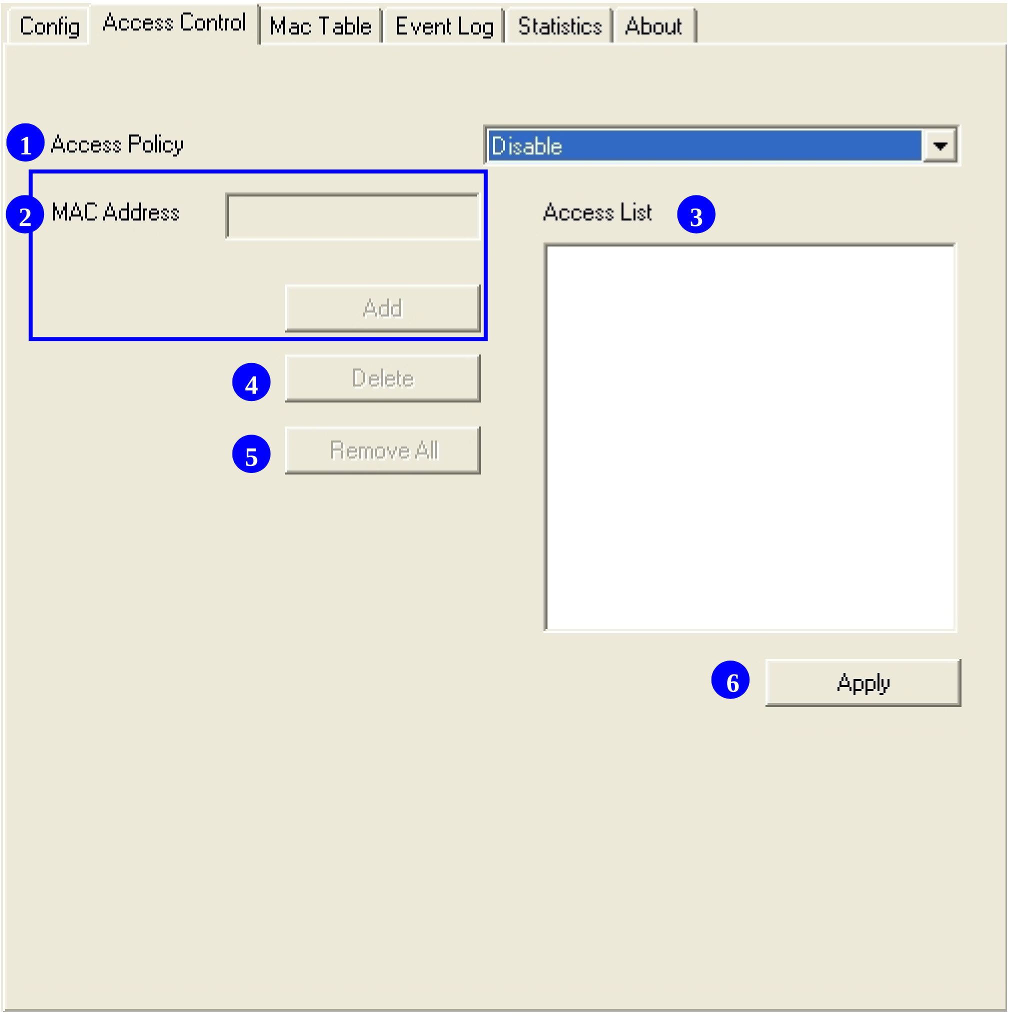
   b. Hexadecimal (128bits): 32Hex characters.

   c. ASCII (40bits): 5 ASCII characters.

   d. ASCII (128bits): 13 ASCII characters.

Access Control

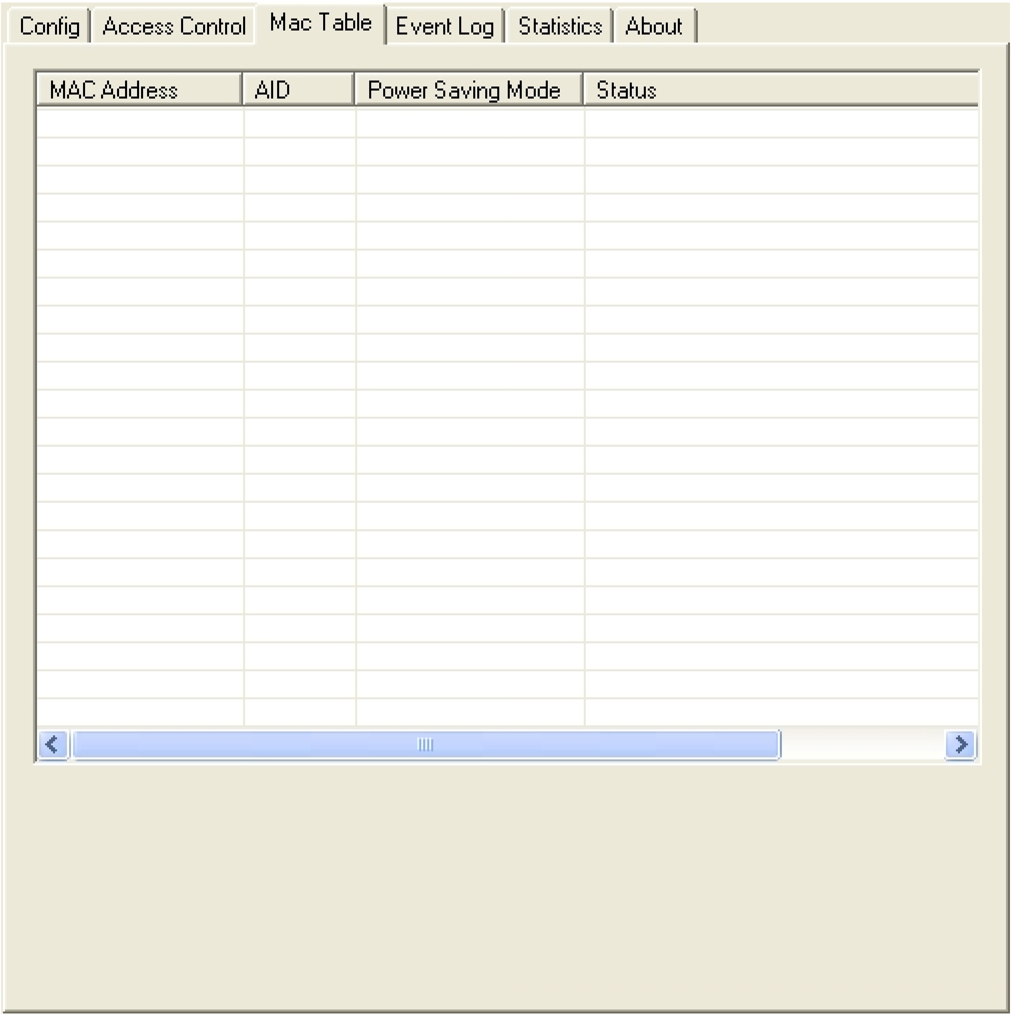
This function filters users to use this device by designating MAC address. Please refer to the following chart for introduction.



1. **Access Policy:** Choose a method to process access control from the drop list to determine the MAC addresses that you designated are allowed to access the AP or not.
2. **MAC Address:** Add allowed (or denied) MAC addresses to the MAC address list.
3. **Access List:** Display all Mac Addresses that you designated.
4. **Delete:** Delete Mac addresses that you selected.
5. **Remove All:** Remove all Mac address in [Access List].
6. **Apply:** Apply changes.

MAC Table

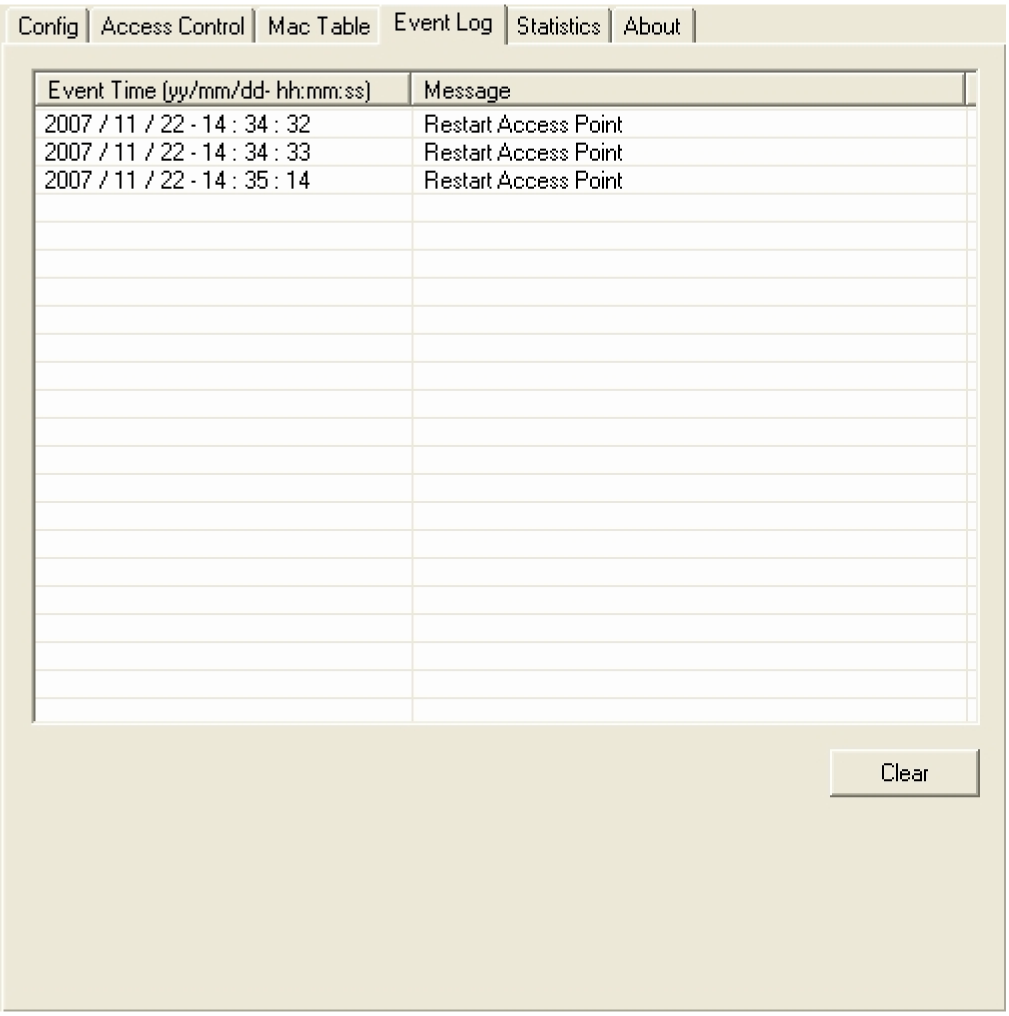
This page displays the station detail information of current connection.



Items	Information
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	Check if the connected station supports power saving.
Status	The connection status.

Event Log

Record Soft AP all event time and message.

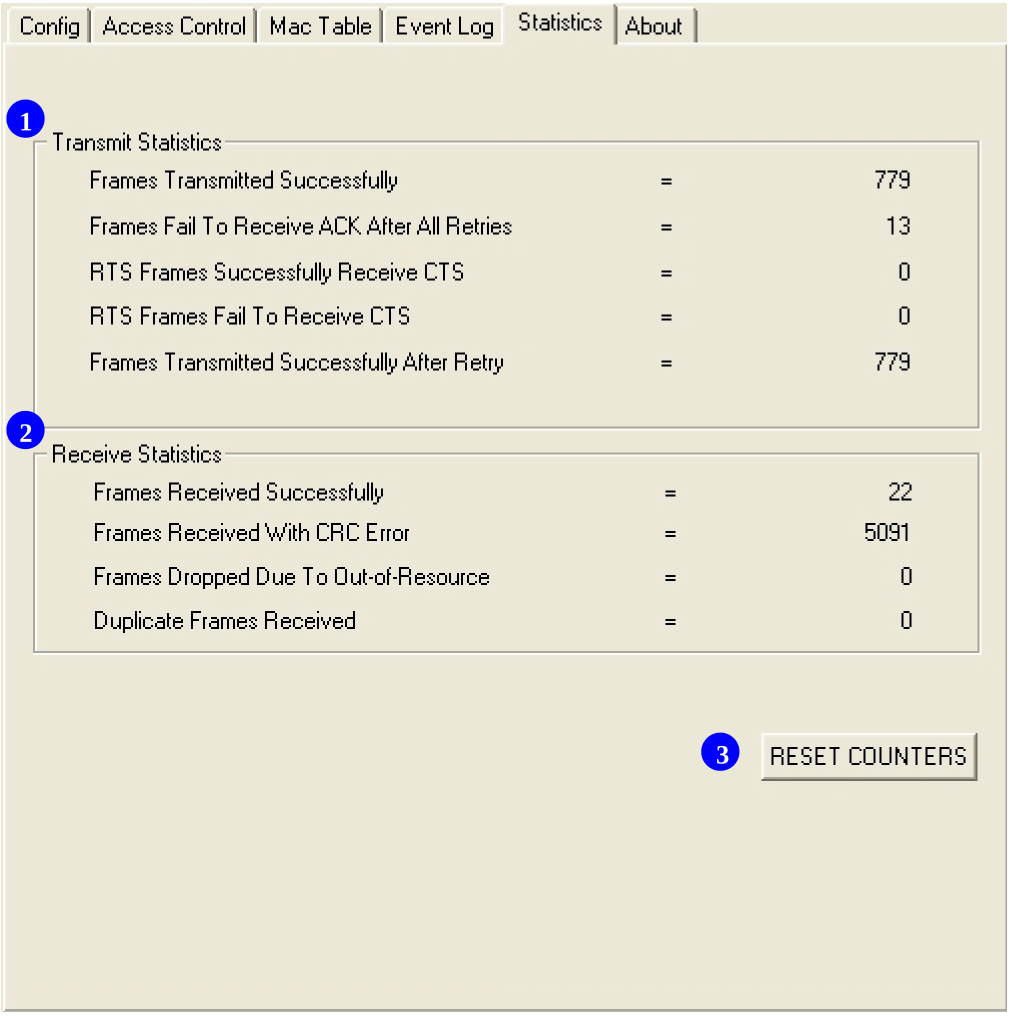


Event Time (yy/mm/dd- hh:mm:ss)	Message
2007 / 11 / 22 - 14 : 34 : 32	Restart Access Point
2007 / 11 / 22 - 14 : 34 : 33	Restart Access Point
2007 / 11 / 22 - 14 : 35 : 14	Restart Access Point

Items	**Information**
Event Time (yy/mm/dd-hh:mm:ss)	Record event time.
Message	All event messages.

Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters.



Transmit Statistics

```
Frames Transmitted Successfully                =      779
Frames Fail To Receive ACK After All Retries   =       13
RTS Frames Successfully Receive CTS            =        0
RTS Frames Fail To Receive CTS                 =        0
Frames Transmitted Successfully After Retry    =      779
```

Receive Statistics

```
Frames Received Successfully                   =       22
Frames Received With CRC Error                 =     5091
Frames Dropped Due To Out-of-Resource          =        0
Duplicate Frames Received                      =        0
```

1. Transmit Statistics

Items	Information
Frames Transmitted Successfully	Frames that successfully sent.
Frames Fail To Receive ACK After All Retries	Frames that failed to transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Counts of CTS that successfully received after sending RTS frame.
RTS Frames Fail To Receive CTS	Counts of CTS that fail to be received after sending RTS frame.
Frames Retransmitted Successfully	Successfully retransmitted frames numbers.

2. Receive Statistics

Items	Information
Frames Received Successfully	Frames received successfully.
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue.
Duplicate Frames Received	Duplicate received frames.

3. Reset Counters: Reset counters to zero.