PLANET
Networking & Communication

802.11n Wireless PCI Express Adapter

WNL-9500

User's Manual

Version: 1.00

Date: November 2007

Copyright

Copyright © 2007 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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 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 or more of the following measures:

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

FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the

equipment.

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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, and France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted

municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 802.11n Wireless PCI Express Adapter

Model: WNL-9500

Rev: 1.0 (November 2007)

Part No. EM-WNL9500

C A T A L O G

Chapter 1: Introduction

For higher wireless transfer performance, we are glad to introduce the PLANET 802.11n wireless PCI Express adapter – WNL-9500. It is a PCI Express wireless adapter that can operate in either Ad-Hoc mode (Point to Point/Point to Multipoint without an Access Point) or Infrastructure mode (Point to Point/Point to Multipoint with an Access Point) 2.4GHz frequency band; it's backward compatible with 802.11b and 802.11g for users to create a new wireless environment based on the existing wireless network. With integrating the latest innovative 802.11n technology, the maximum data rate of WNL-9500 is up to 300Mbps which is almost six times of standard G.

Featuring smart antenna technology, the 802.11n design helps combat distortion and interference, so this Network Card can send its data streams with greater distances and be more reliable. The WNL-9500 supports the most convenient security, " Wi-Fi Protected Setup (WPS) "which is the way to build connection between wireless network clients and this wireless router. This WNL-9500 supports two types of WPS, Push-Button Configuration (PBC) and PIN code (key Wireless adapter card pin number).

For WLAN security issues, the WNL-9500 supports 64/128-bit WEP (Wired Equivalent Privacy) and WPA/WPA2 (Wi-Fi Protected Access) for securing wireless network connections. The driver and utility support most popular operating systems, Windows 2000 / XP and Vista. With advanced features and high performance capability, the WNL-9500 is an excellent choice for constructing a wide range of wireless solutions.

The power consumption of the card is also very low. This card provides several levels of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices.
.

1-1 Features

- Compliant with PCI Express 1.0a - x1 PCI Express standard
- 2.4GHz ISM band, unlicensed operation
- Supports Wi-Fi Protected Setup (WPS) utility and hardware button
- Compliant with IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0)
- 802.11n provides up to 300Mbps data rate
- Support 64/128-bit WEP , WAP/WAP2 , and WPA/WPA2-PSK high-level security mechanisms
- Support Ad-Hoc (support 802.11b and 802.11b/g mode) / Infrastructure mode (support 802.11b , 802.11b/g and 802.11b/g/n mix mode)
- Support WMM (WiFi Multi-Media) function to meet the multi-media data bandwidth requirement. (the connected AP and the application must support WMM as well)
- Support of Power Save mode
- High-efficiency antenna expands the scope of your wireless network

- QoS function: Control the bandwidth required for different applications
- Support of most popular operating systems including Windows 2000 / XP / 2003 server and Vista
- Smart Antenna Technology with 2 transmit and 3 receive antennas

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the safety instructions:

1. This wireless network card is designed for indoor use only. DO NOT expose this network card to direct sun light, rain, or snow.

2. DO NOT put this network card at or near hot or humid places, like kitchen or bathroom. Also, do not left this wireless network card in the car in summer.

3. This network card is small enough to put in a child's mouth, and it could cause serious injury or could be fatal. If they throw the network card, the card will be damaged. PLEASE KEEP THIS NETWORK CARD OUT THE REACH OF CHILDREN!

4. This network card will become hot when being used for long time (This is normal and is not a malfunction). DO NOT put the network card on a paper, cloth, or other flammable objects after the network card has been used for a long time.

5. There's no user-serviceable part inside the network card. If you found that the network card is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the network card by your self, warranty will be void.

6. If the network card falls into water, DO NOT USE IT AGAIN BEFORE YOU SEND THE CARD TO THE DEALER OF PURCHASE FOR INSPECTION.

7. If you smell something strange or even see some smoke coming out from the network card, switch the computer off immediately, and call dealer of purchase for help.

1-3 Specification

|	
Interface	PCI Express 1.0a – x1 PCI Express
Standards Conformance	Compliant with 802.11b / 802.11g / 802.11n (draft 2.0)
Data Transfer Rate	IEEE 802.11b: 11/5.5/2/1M IEEE 802.11g: 54/48/36/24/18/12/9/6 IEEE 802.11n: 300/270/243/240/216/180/162/120/108Mbps in 40Mhz mode 145/130/117/104/ 78Mbps in 20Mhz mode
Operating Mode	Infrastructure Mode, Ad-Hoc Mode
Security	WEP 64/128bit, WPA, WPA2,WPA-PSK,WPA2-PSK
RF Modulation	802.11b: DSSS, CCK, QPSK, BPSK 802.11g: OFDM 802.11n: 64QAM, 16QAM, QPSK, BPSK
Media Access Protocol	CSMA / CA
Output Power	11b mode: 14-16dBm 11g mode: 14-16dBm 11n mode: 12-14dBm
LED Indicators	Tx/Rx, Link
Channels	2.412~2.462GHz(FCC, Canada)/11 Channels 2.412~2.4835GHz(Japan, TELEC)/14 Channels 2.412~2.472GHz(Euro ETSI)/13 Channels
Management	Built-in utility or Windows XP Zero Configuration utility
Operating systems	Windows 2000 / XP / 2003 server / Vista
Environmental & Mechanical Characteristics	
Temperature	Operating: 0 - 55 degree C Storage: -20 - 70 degree C
Operating Humidity	Operating: 0 ~ 85% Storage: 0 ~ 95% Non-Condensing
Dimensions	120×45 mm (Non-Bracket)
Weight	60g
Certifications	FCC, CE

1-4 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

1 x WNL-9500
3 x External Antenna
1 x Driver and User's manual CD
1 x Quick Installation Guide

If any of the above items is missing, contact your supplier as soon as possible.

1-5 Hardware Intro
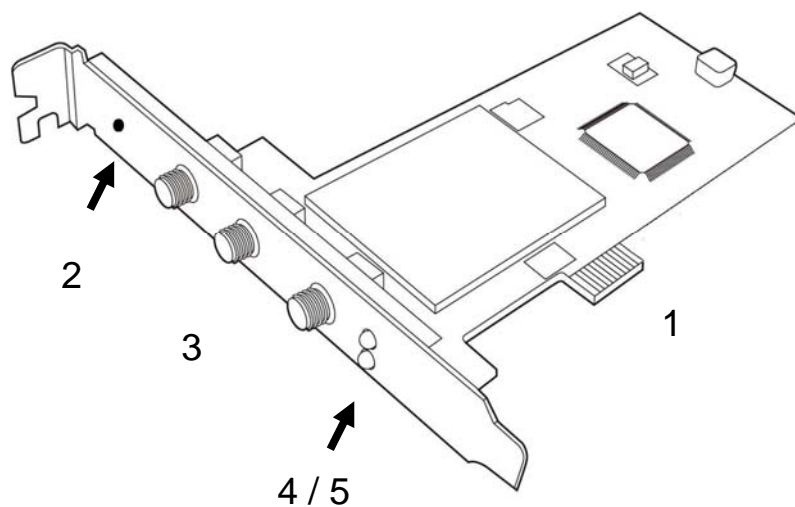
1. PCI Express Interface
2. WPS Button
3. Antenna Connectors (3x)
4. 'Link' LED
5. 'Tx/Rx' LED

| LED Name	Light Status	Description
Link	On	Linked to a wireless access point
	Off	Not linked to any wireless access point
Tx/Rx	Blinking	Transferring / receiving data
	Off	No wireless activity

Chapter 2: Installation

2-1 Hardware Installation

1. SWITCH THE COMPUTER OFF, remove the cover and insert the wireless network card into an empty PCIe slot of your computer.
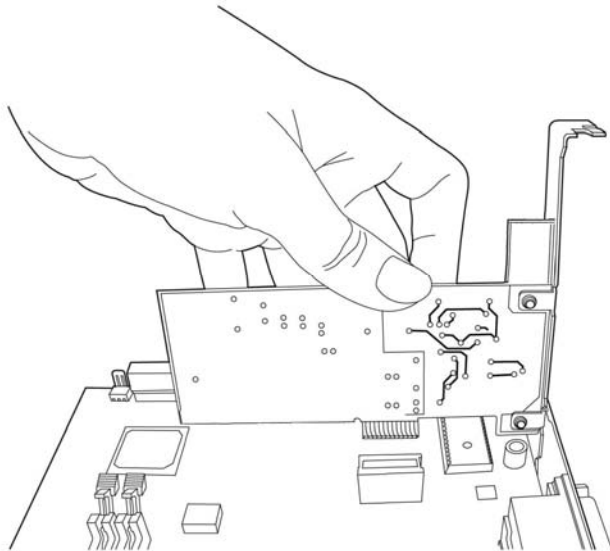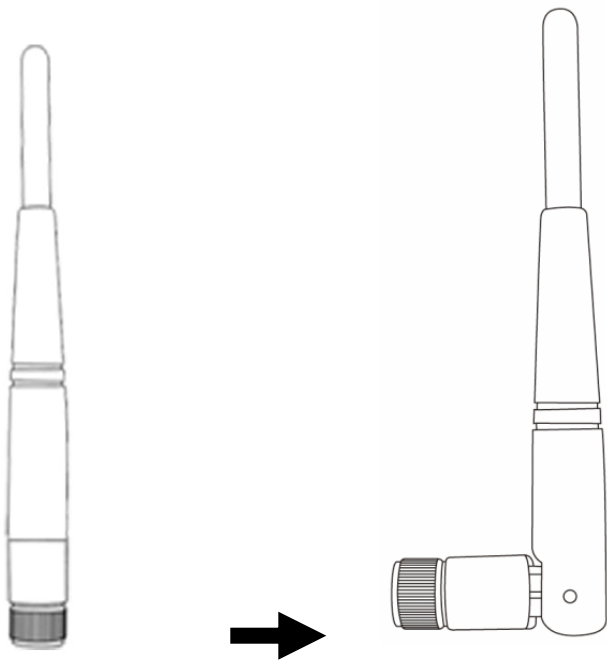

> *Tip: It's recommended to touch some metal material before installing the network card, or the static on your body may damage the components on network card and computer.*

2. Fasten the antennas to the antenna connectors on the network card by clockwise direction.
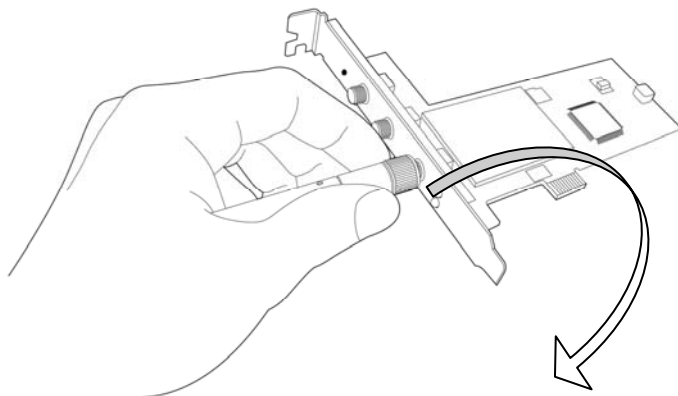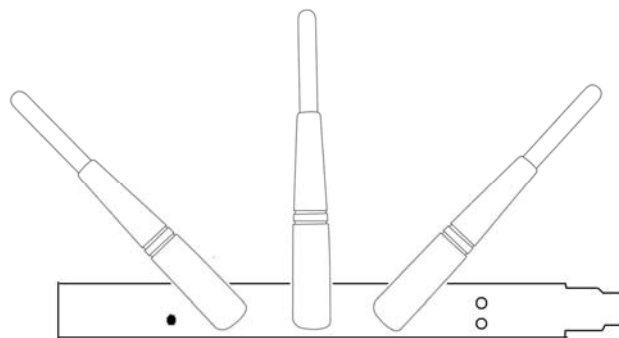

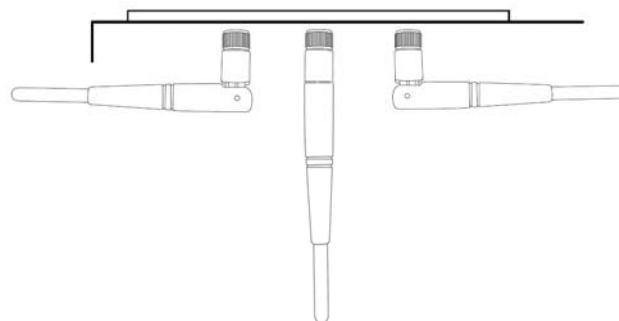3. You can bend the antenna to fit actual needs:

4.   To improve radio reception, please adjust antennas to the position shown in the picture.
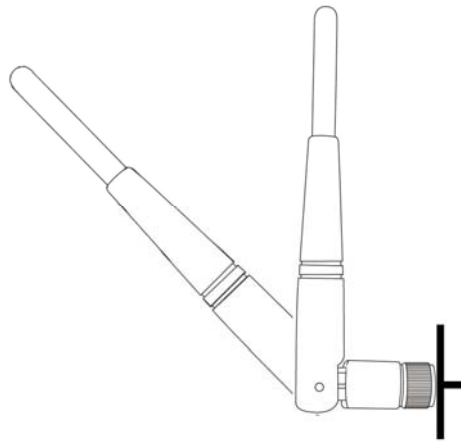
Rear view

Top view

Side view

2-2 Utility Installation

Note 1: If you had ever installed the other Wireless Cards before, please uninstall the existed drivers and utilities first.

Note 2: The installation below is performed in Windows XP system. The installations in Windows 2000 and Vista are silimar.

1. Power on the computer. The system will find the new hardware and display the below message. Click "Cancel" to skip.


2. Insert the bundled CD into the CD-ROM drive to launch the auto run program. Once completed, a menu screen will appear.

3. Click the "2000/XP Utility" hyperlink to initiate the install wizard.

4. Read the License Agreement carefully. Click "Yes" to accept it and continue.
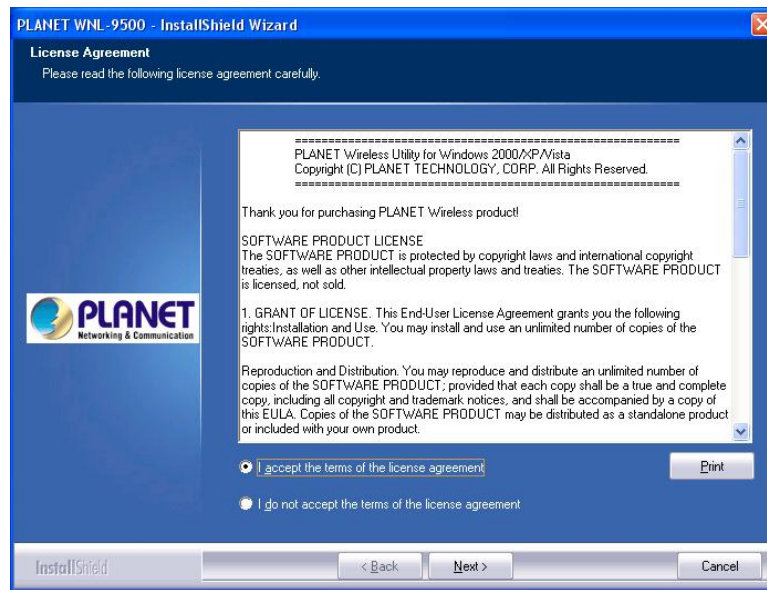
5. It is suggested to use "PLANET Configuration Tool", which provides fully access to all functions, to manage the WNL-9500. Click "Next" to continue.
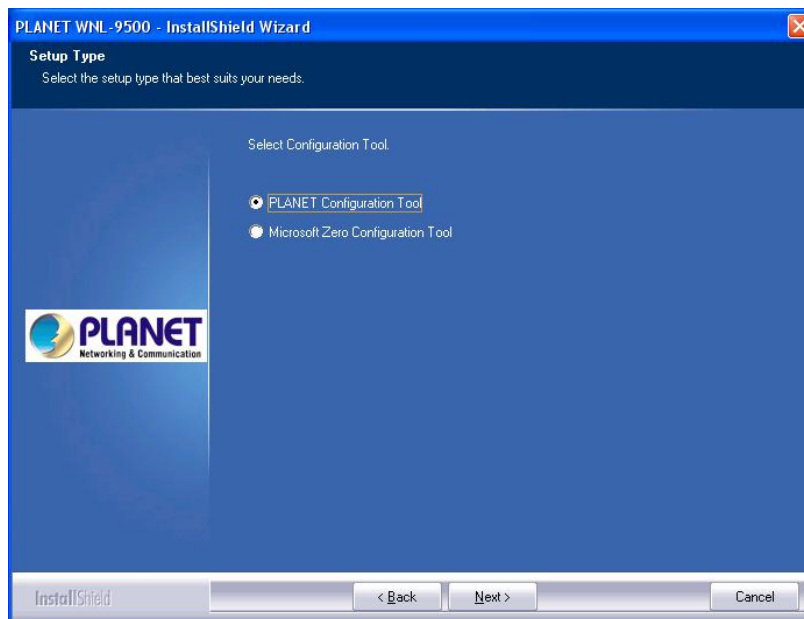
6. There are two wireless performance mode you can select here:

   Optimize for WiFi mode   or

   Optimize for performance mode

   If you want to enhance wireless performance, please select 'Optimize for performance mode'. However, wireless compatibility is not guaranteed in this mode. If you want to use this mode, you may not be able to communicate with older wireless devices and wireless access point, such as 802.11b devices, but the data transfer rate will be enhanced in this mode. You can select this mode when you only plan to communicate with 802.11 Draft-N

devices.

If you want to keep compatibility and communicate with older wireless devices, please select 'Optimize for WiFi Mode'.

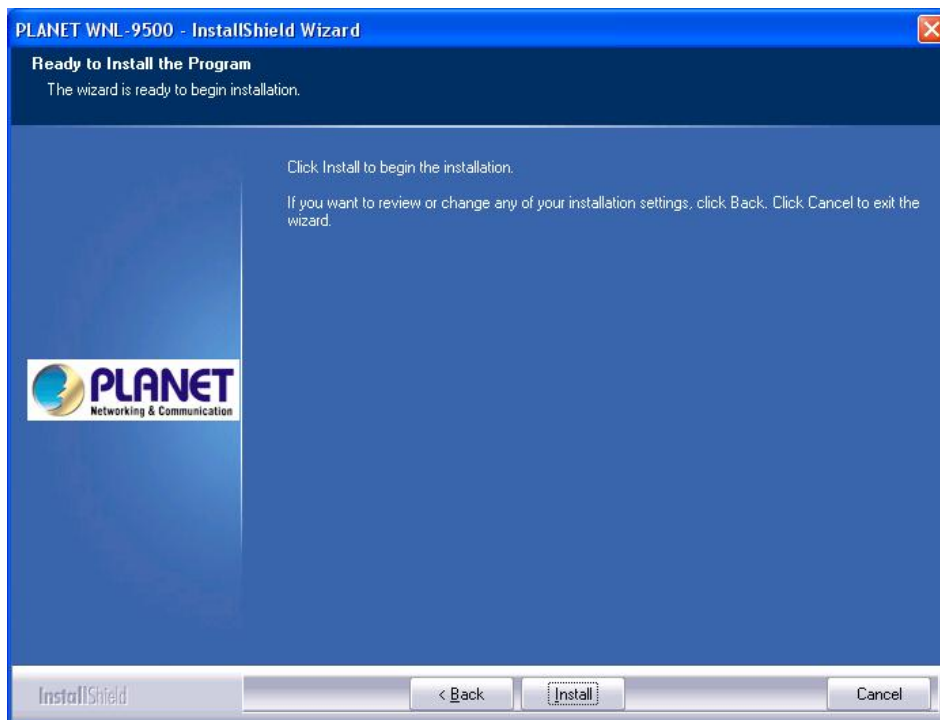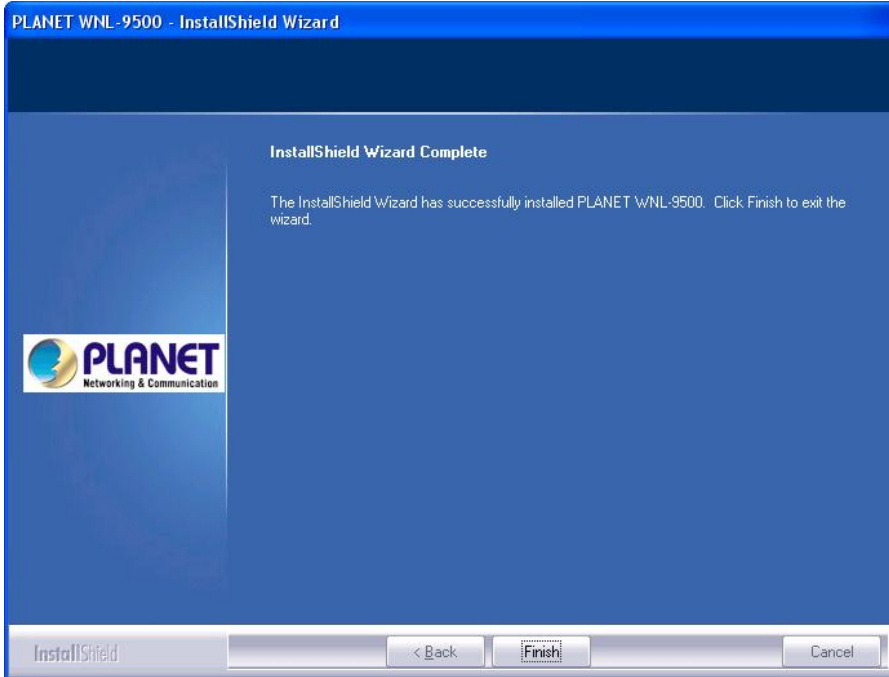After you finish the selection, please click 'Next' to continue. **If you see 'Found New Hardware' message again, please ignore it and wait.**
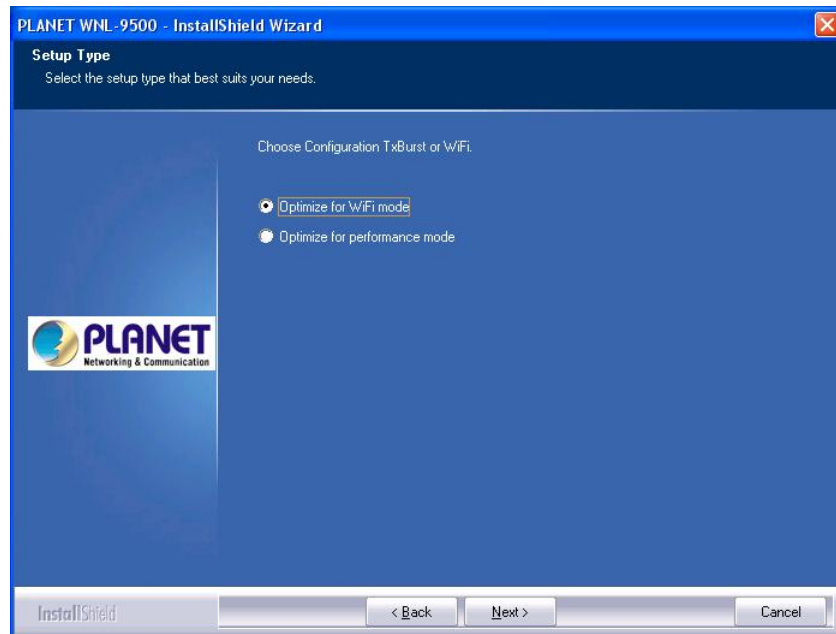
7. Click "Install" to begin the installation.

8. Please click "Finish" to finish the installation.

Chapter 3: General Configuration

The Configuration Utility appears as an icon on the system tray of Windows while the card is running. You can open the utility by double-click on the icon.

Right click the icon; there are some items for you to operate the configuration utility.

Lauch Config Utilities: open the Configuration Utility tool.

Use Zero Configuration as Configuration Utility: use Windows XP built-in wireless configuration utility (Windows Zero Configuration) to configure the card.

Switch to AP Mode: the WNL-9500 can act as an AP. Please refer to next chapter for details.

Exit: close the Configuration Utility tool.
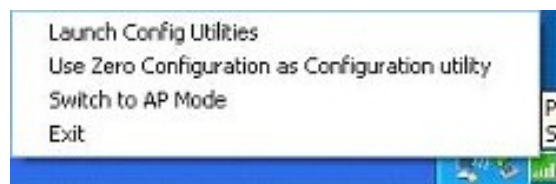
3-1 Connection Profile Management

If you need to connect to different wireless access points at different time, like to access point of your home, office, cybercafe, or public wireless service, you can store the connection parameters (encryption, passphrase, security etc, etc.) as a profile for every access point, so you don't have to input these parameters every time you want to connect to a specific wireless access point.

3-1-1 Make a profile for an access point or wireless device

There are two ways to add a new connection profile:

Create a new profile,

Add a profile from an existing wireless access point or wireless device

If you want to click new profile, click 'Profile' tab, then click 'Add' button:

Parameter	Description
Profiles List	The profiles list display all the profiles and the relative settings of the profiles including Profile Name, SSID, Channel, etc. ✅ This sign indicates the activated profile is been connecting. ✅ This sign indicates the activated profile is not been connecting.
Add/Delete/Edit Button	Click these buttons to add/delete/edit the selected profiles.
Activate Button	Click "Activate" to connect to the selected profile. When a profile is activated, the card will be initially connected to the profile.

Or, you can add a connected wireless access point or wireless device to a profile by clicking 'Site Survey' tab, then click 'Add to Profile' button:
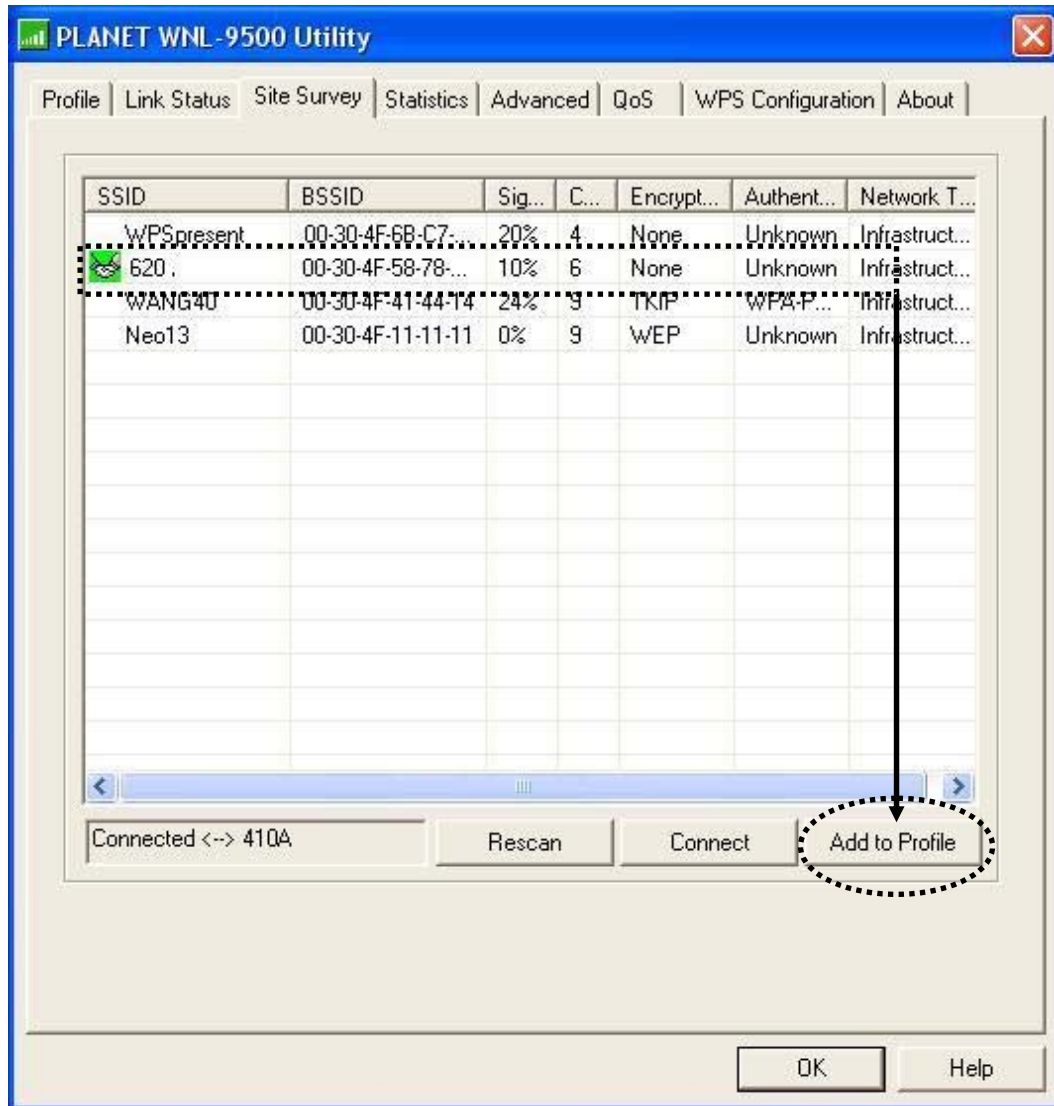
And you can set the parameter for this profile here:

Parameter	Description
Profile Name	Define a recognizable profile name for you to identify the different networks.
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the card and then only the device with the same SSID can interconnect to the card. If you want to add the network nearby to the profile list, pull down the menu, all the networks will be listed for you to add one of them to the profile list.
PSM (Power Saving Mode)	The power saving function is only available when the network type is in Infrastructure. **CAM (Constantly Awake Mode)** – The card will always set in active mode. **PSM (Power Saving Mode)** – Enable the card in the power saving mode when it is idle.
Network Type	**Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad-Hoc** – Select this mode if you want to connect to another wireless

station in the Wireless LAN network without through an Access Point or Router.

Preamble	The preamble defines the length of the CRC block for communication among wireless devices. This option is only active in the Ad Hoc network. There are two modes including Auto and Long Preamble. If "Auto"mode is selected, the card will auto switch the preamble mode depending on the wireless devices the card is connecting to.
RTS Threshold	Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2347 bytes. Minor change is recommended.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2346 bytes. Minor change is recommended.
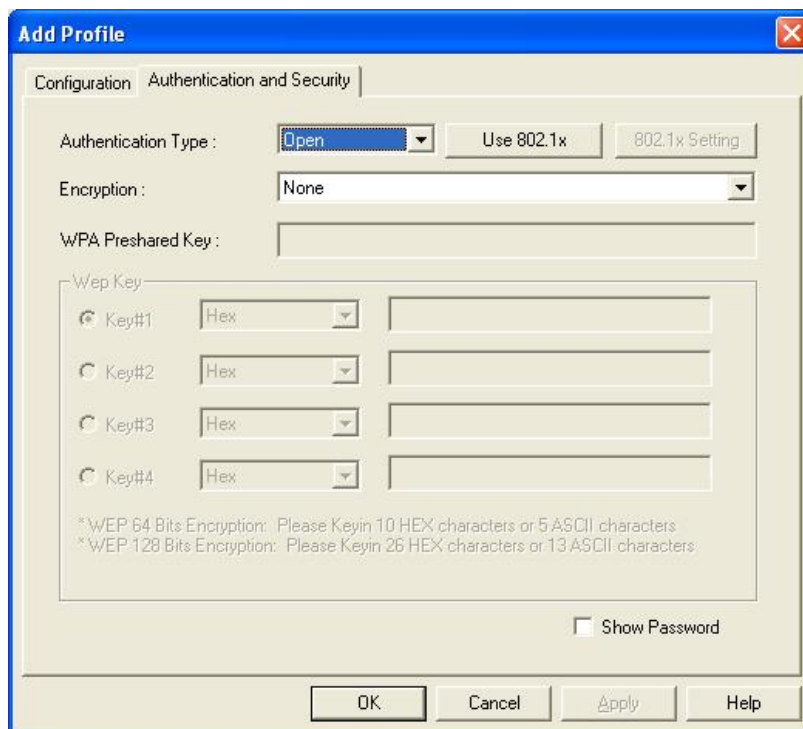
Parameter	Description

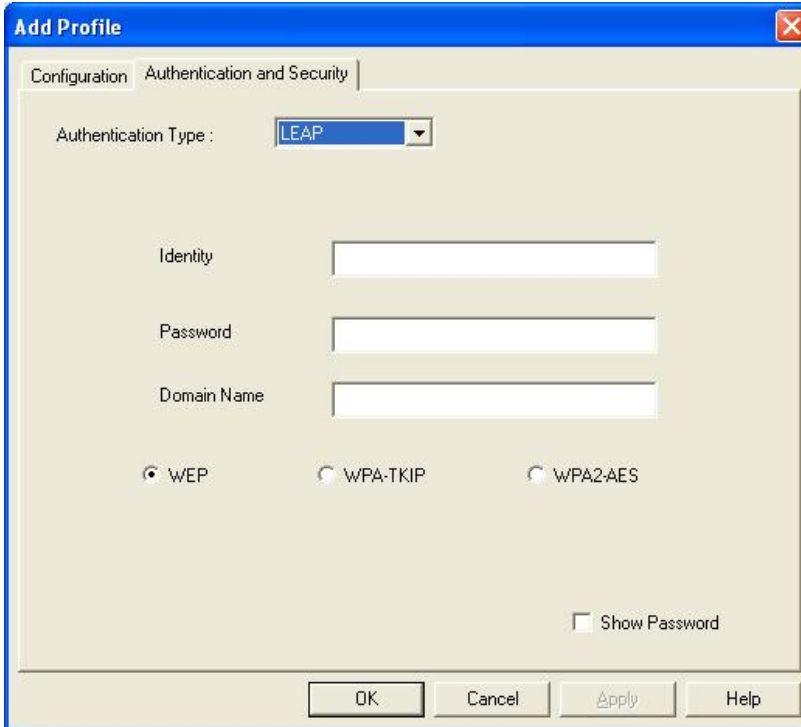|	
Authentication Type	This setting has to be consistent with the wireless networks that the card intends to connect. **Open** – No authentication is needed among the wireless network. **Shared** – Only wireless devices using a shared key (WEP Key identified) are allowed to connecting each other. **LEAP** – LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern. If you select 'LEAP', the following message will be displayed. Please input LEAP identity, password, domain name, and select encryption type. You can check 'Show Password' box so the password you inputted will be displayed as you type, but not replace by asterisk.

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

WPA-PSK – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in

their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

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

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

Use 802.1x	Enable 802.1x wireless authentication. Please click '802.1x Setting' button to set 802.1x parameters. (See next section).
Encryption Mode	**None** – Disable the encryption mode. **WEP** – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys. **TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. Note: All devices in the network should use the same encryption method to ensure the communication.
WPA Pre-Shared Key	The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.
WEP Key (Key1 ~ Key4)	The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit and 128-bit. Select the default encryption key from Key 1 to Key 4 by selected the radio button.

Fill the text box by following the rules below.

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

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

After you finish all settings, click 'OK' to save settings and exit. The profile you just created will be displayed:
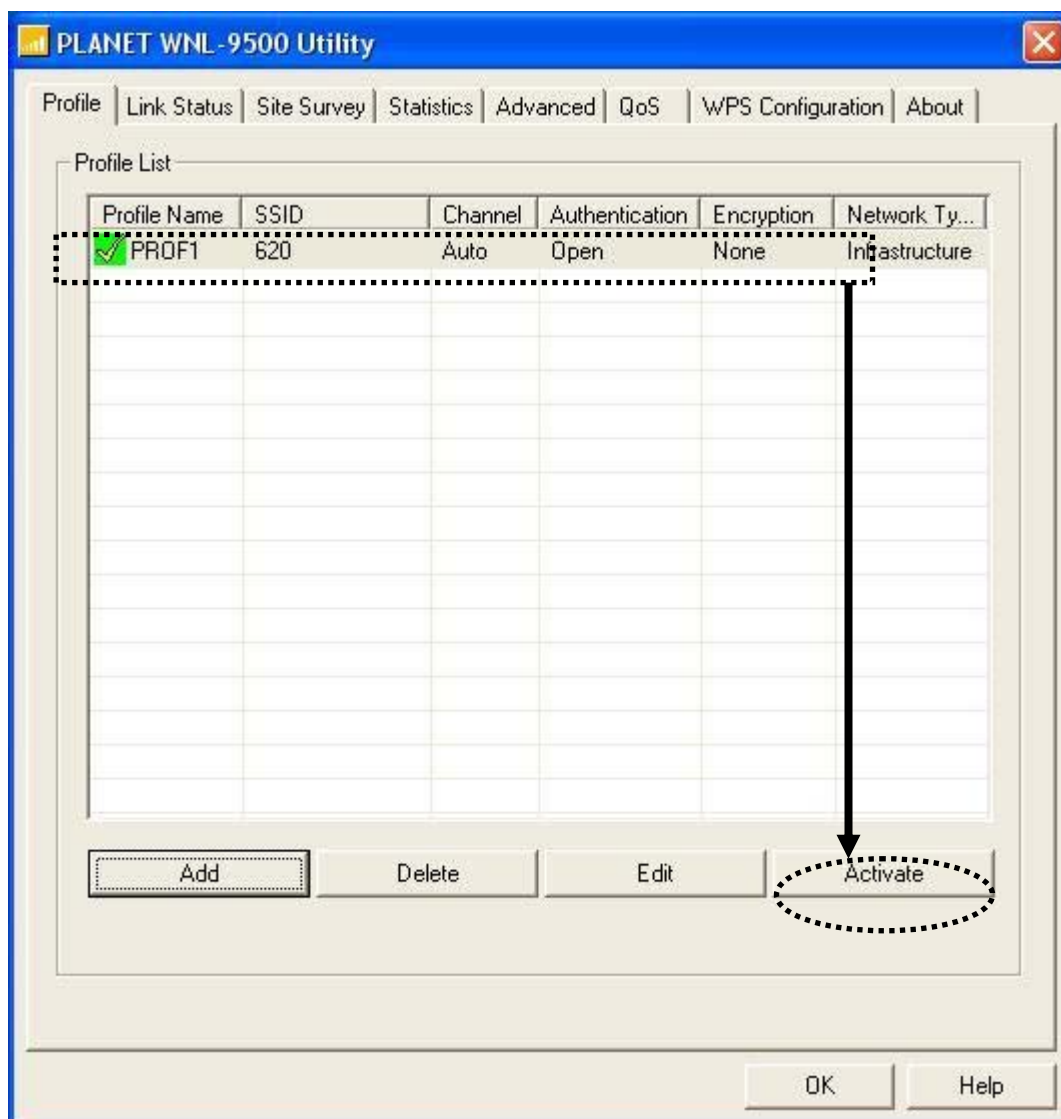
Select the profile you wish to use, and click 'Activate' to use the profile you selected. You can only activate a profile a time, and the profile which is activated currently will have a green

check () before its name. If the wireless access point is not reachable, a red check () will be displayed before its name.
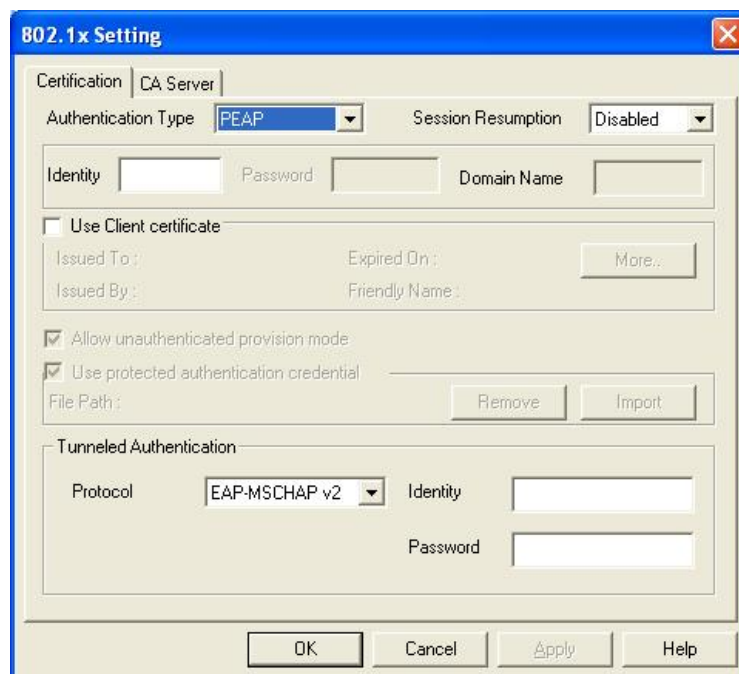
If you want to change the connection parameters of a specific profile, just select it and click 'Edit' button, you'll be prompted to input the connection parameters, just like you're creating a new profile.

If you no longer need a profile, select the profile then click 'Delete'.

3-1-2 Using 802.1x – Certification

After you click '802.1x Setting', a new window will appear:

Parameter	Description
Authentication Type	The EAP authentication protocols this card has supported are included as follows. This setting has to be consistent with the wireless APs or Routers that the card intends to connect.
	PEAP &TTLS – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MS-CHAP, MS-CHAPv2, PAP and EAP-MD5. PEAP specifies that an EAP-compliant authentication protocol must be used; this card supports EAP-MSCHAP v2, EAP-TLS/Smart card and Generic Token Card. The client certificate is optional required for the authentication.

TLS/Smart Card –TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client. After validating the server's certificate, the client presents a client certificate to the server for validation.

MD5-Challenge – MD5-Challenge is the easiest EAP Type. It requires the wireless station to enter a set of user name and password as the identity to RADIUS Server.

Session Resumption	There are "Disabled", "Reauthentication", "Roaming", "SameSsid" and "Always" selections for you to choose whether to recovery the session in different status.
Identity	Enter the name as the identity for the server.
Password	Enter the password as the identity for the server.
Use Client Certificate	A client certificate is required for TLS, and is optional for TTLS and PEAP. This forces a client certificate to be selected from the appropriate Windows Certificate Store and made available to the RADIUS server for certification.
Tunneled Authentication	
Protocol	When the authentication type is PEAP or TTLS, select a protocol to be used to build the encrypted tunnel.
Identity	This is the protected user EAP Identity used for authentication. The identity specified may contain up to 63 ASCII characters, is case sensitive and takes the form of a Network Access Identifier, consisting of <name of the user>@<user's home realm>. The user's home realm is optional and indicates the routing domain.
Password	The password used for authentication. It may contain up to 63 ASCII characters and is case sensitive.

3-1-3 Using 802.1x - CA Server

If you want to use CA server, please click 'CA Server' tab. And the following message will be displayed:

Parameter	Description
Use Certificate Chain	When the EAP authentication type such as TLS, TTLS or PEAP is selected and required a certification to tell the client what server credentials to accept from the authentication server in order to verify the server, you have to enable this function.
Certificate Issuer	Choose the server from the list to issue the certificate. If "Any Trusted CA" is selected, any CA included in the list (provided by the Microsoft Certificate Store) is permitted.
Allow Intermediate Certificates	A server designates an issuer as a trusted root authority by placing the issuer's self-signed certificate, which contains the issuer's public key, into the trusted root certification authority certificate store of the host computer. Intermediate or subordinate certification authorities are trusted only if they have a valid certification path from a trusted root certification authority.
Server Name	Enter the authentication server name.

Server name must match exactly	When selected, the server name must match exactly the server name found on the certificate.
Domain name must end in specified name	When selected, the server name field identifies a domain. The certificate must use a server name belonging to this domain or to one of its sub-domains (e.g. zeelans.com, where the server is blueberry.zeelans.com) but it may be any name used in the certificate name field.

3-2 Site Syrvey

From the "Site Survey" screen, all the networks nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.
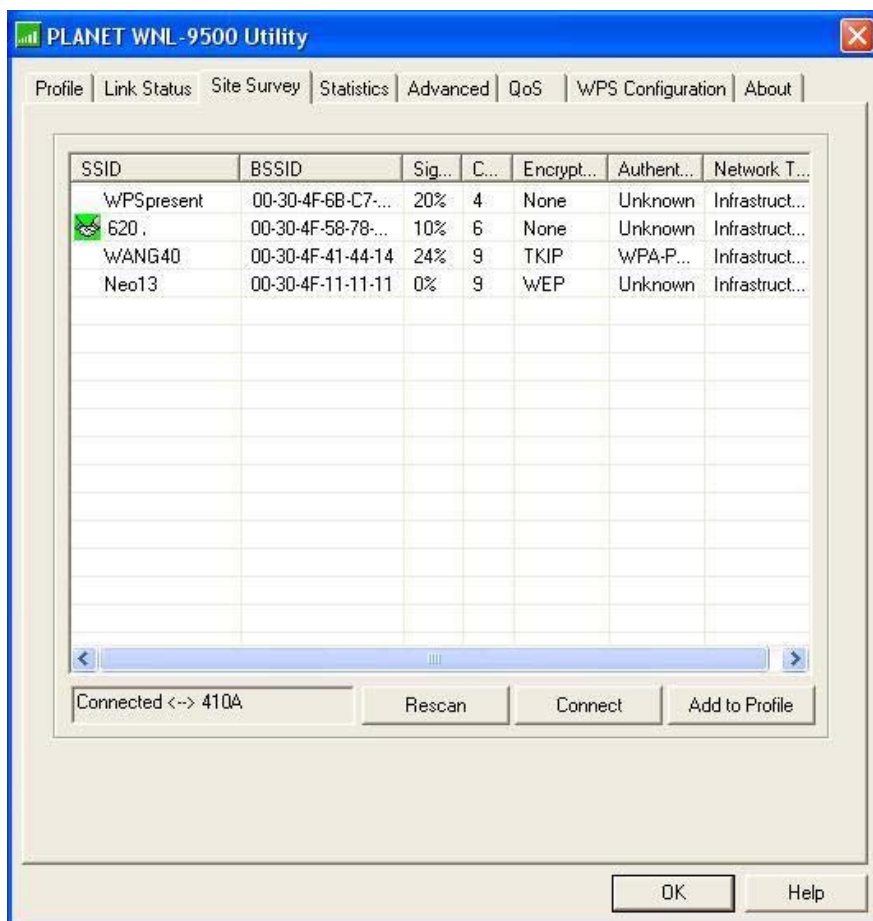
Parameter	Description
Available Networks	This list shows all available wireless networks within range of your card. It also displays the information of the networks including the SSID, BSSID, Signal Strength, Channel, Encryption,

Authentication and Network Type. If you want to connect to any networks on the list, double-click the item on the list, and the card will automatically connect to the selected network.

Rescan Button   Click "Rescan" button to collect the new information of all the wireless networks nearby.

Connect Button   Click "Connect" to connect to the selected network.

Add to Profile Button   Add the selected network to Profiles list.

1. If the access point you selected does not enable encryption (The content of 'Encryption' field of the access point you selected is 'None', you'll be connected to this wireless access point within one minute.

2. If the access point you selected enables encryption, please proceed to next step.

3. If the wireless access point does not have SSID, you'll be prompted to input it here. Please ask the administrator of this AP and input the exact SSID here, then click 'OK' when ready. If the SSID you provided here is wrong, you'll not be able to connect to this access point.
If the wireless access point you selected have SSID, please skip this step.
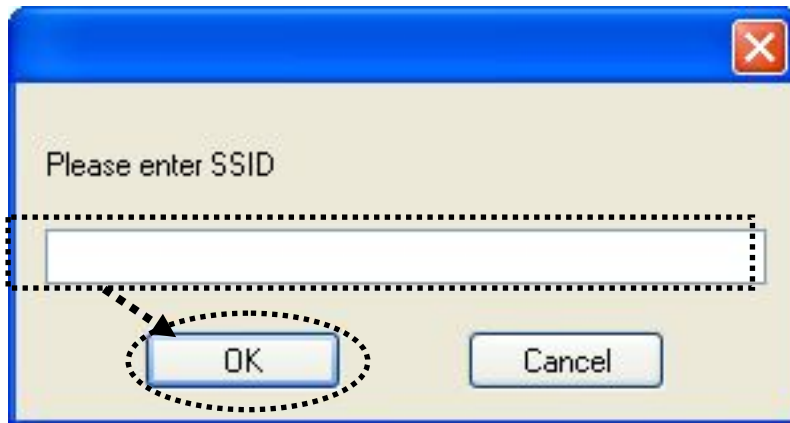
4. If the AP uses encryption, you have to input WEP passphrase or WPA preshared key. Please ask the administrator, and input the correct passphrase / preshared key here, then click 'OK'. If the value you inputted here is wrong, you will not be able to connect to this wireless access point.

Authentication type is selected automatically, please don't change it.

If the access point you selected does not enable encryption and does not require authentication, please skip this step.

5. You'll see 'Connected <-> SSID' ('SSID' is the SSID of the AP you connected to) message displayed at lower-left corner of configuration utility. Now, you're successfully connected to the access point or wireless device you selected!
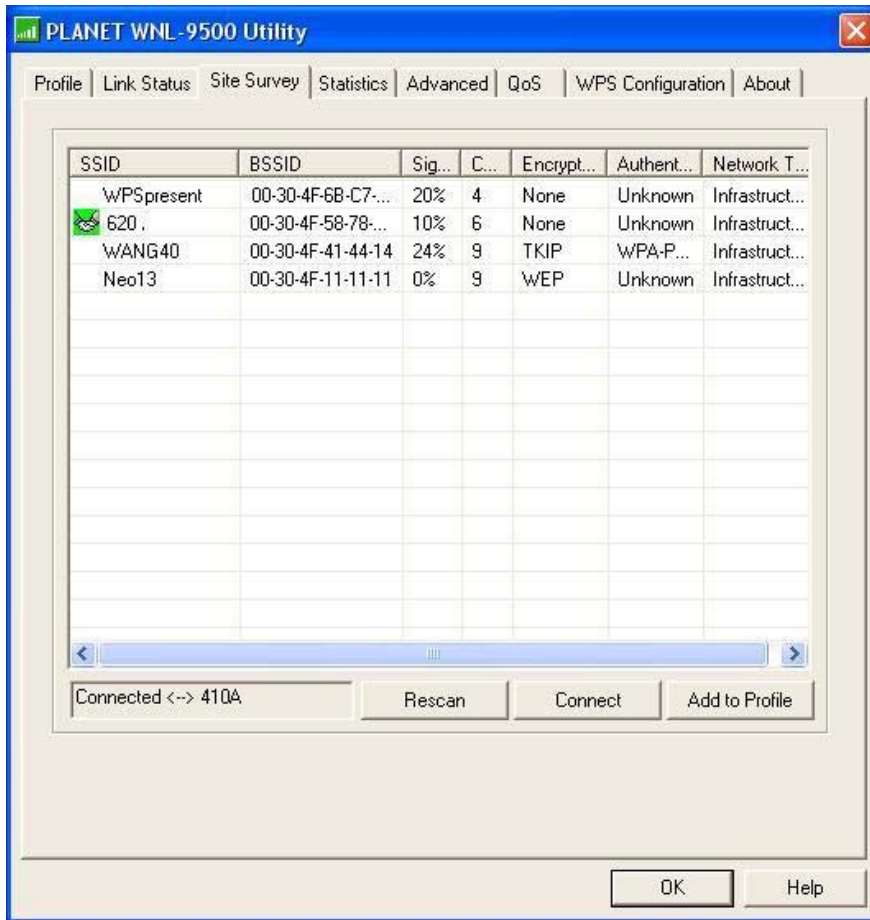
3-3 View Network Link Status and Statistics

The configuration utility provides information about network statistics and link status.

3-3-1 Link Status
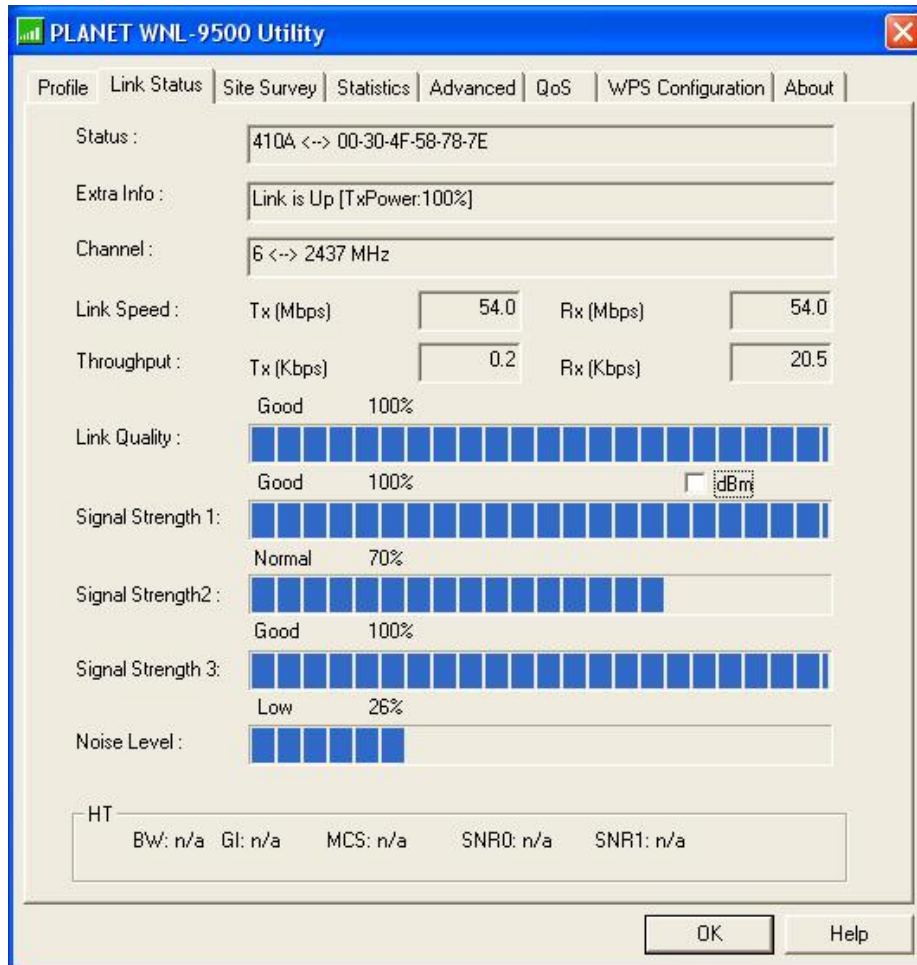
Parameter	Description
Status	Display the SSID and MAC ID of the network the card is connecting to.
Extra Info	Display the link status.
Channel	Display the number of the radio channel and the frequency used for the networking.
Link Speed (Mbps)	Display the transmission and reception rate of the network.
Throughput (Kbits/sec)	Display the speed of data transmitted and received.
Link Quality	This bar indicates the quality of the link. The higher the percentage, the better the quality.
dBm	If you want to know the signal strength in the unit of dBm, select this check box.

Signal Strength	This bar shows the signal strength level. The higher percentage shown in the bar, the more radio signal been received by the card. This indicator helps to find the proper position of the wireless device for quality network operation.
Noise Level	Display the noise level in the wireless environment.

3-3-2 Statistics
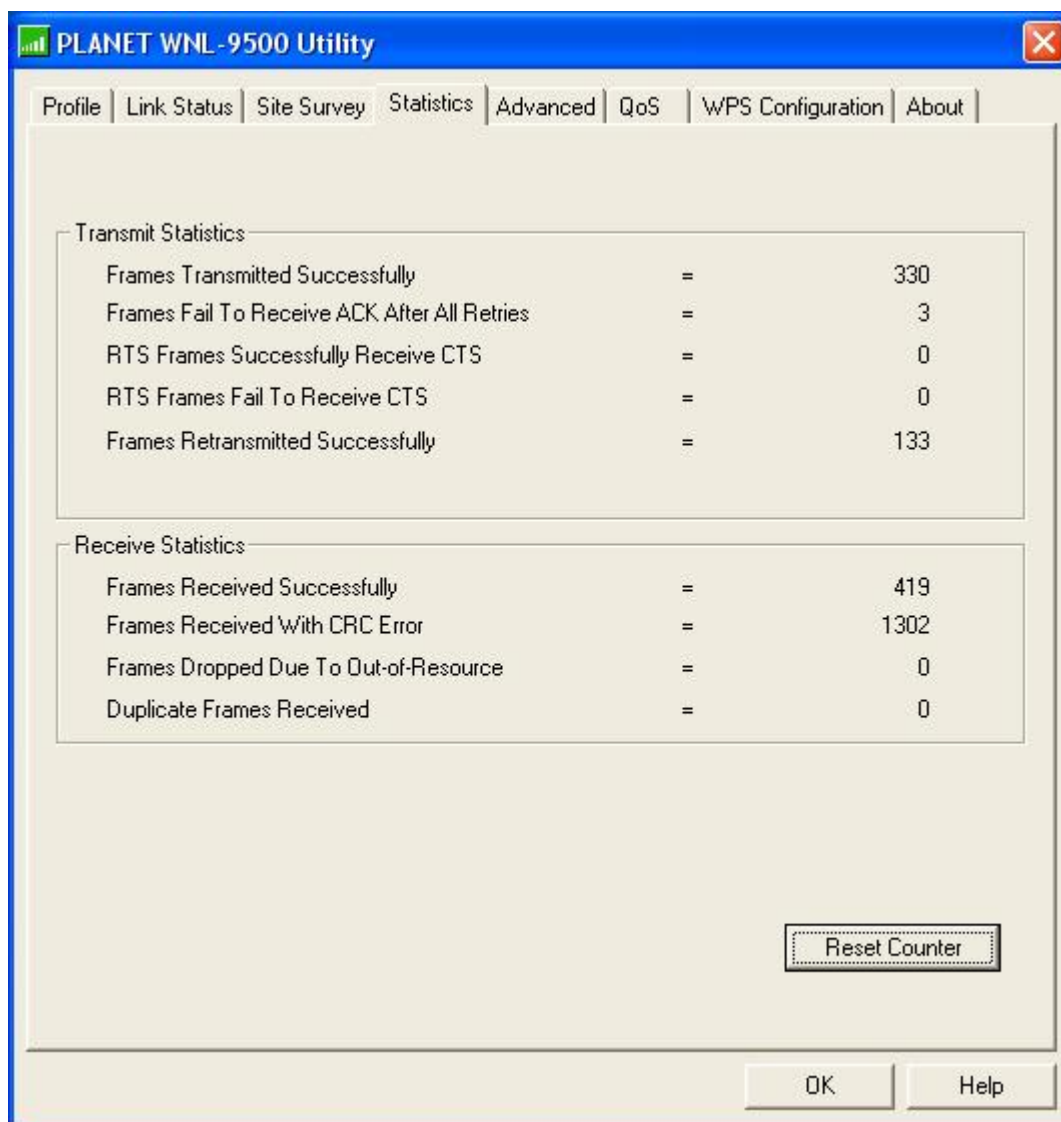
All connection-related statistics is displayed here. You can click 'Reset Counter' to reset the statistics of all items back to 0.

3-4 Advanced Settings

Parameter	Description
Wireless Mode	**802.11 B/G/N mix** – If you have a mix of 802.11b, 802.11g, and 802.11n wireless stations in your network, It is to maximize wireless compatibility with wireless access points and other wireless devices. it is recommended to setting the card to this mode. This mode is also the default setting. **802.11 B/G mix** – If you have a mix of 802.11b and 802.11g wireless stations in your network, it is recommended to setting the card to this mode. **802.11 B only** – This card can be compatible with both 802.11g and 802.11b wireless stations. If there are only 802.11b wireless stations in the network, you can set the card to this mode.

Wireless Protection	If you have a mix of 802.11b and 802.11g wireless stations in the network, it is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the card will be a little lower due to many of frame traffic should be transmitted. **Auto** – Based on the status of the network and automatically disable/enable protection mode. **On** – Always enable the protection mode. **Off** – Always disable the protection mode.
Tx BURST	Tx Burst enables the card to deliver the better throughput in the same period and environment. This feature only takes effect when the connected AP also supports Tx Burst.
Enable TCP Window Size	The TCP Window is the amount of data a sender can send on a particular connection before it gets an acknowledgment back from the receiver that it has gotten some of it. This feature only takes effect when the connected AP also supports TCP Window Size. The larger TCP Window the better performance.
Fast Roaming at -70dBm	When you want to fast roaming to the network nearby without intercepting the wireless connection especially the card is applied to the multimedia application or a voice call, you can enable the parameter. The card will fast roaming to the near network when the receive sensitivity (signal strength) is lower to the value you have set up.
Turn Off RF Button	If you want to turn off the radio of the card temporarily, click this button. To turn on the radio, click this button again.
Show Authentication Status Dialog	When your computer is being authenticated by wireless authentication server, a dialog window with the process of authentication will appear. This function is helpful to find out the problem when you can not be authenticated, and you can provide this information to authentication server's administrator for debugging purpose.
Enable CCX	Enable Cisco Compatible eXtensions. CCX is a wireless feature developed by Cisco used to improve the wireless performance with CCX compatible wireless devices. Check this box if you need to connect to CCX-compatible wireless devices.

|	
Turn on CCKM	During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server. When you configure your wireless LAN for fast re-association, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications.
Enable Radio Measurement	When this parameter is enabled, the Cisco AP can run the radio monitoring through the associated CCX-compliant clients to continuously monitor the WLAN radio environment and discover any new APs that are transmitting beacons.
Non-Serving Channel Measurements	The Cisco AP can perform monitoring measurements through the CCX-compliant clients on the non-serving channels when this parameter is enabled.
Limit xxx milliseconds (0-2000)	It limits the channel measurement time. The default value is 250 milliseconds.

After you finish the settings, click 'Apply' to apply new settings, and click 'OK' to close configuration utility.

Note: This function does not support in Windows VISTA.

3-5 QoS Setting

This wireless network card provides QoS (Quality of Service) function, which can improve the performance of certain network applications, like audio / video streaming, network telephony (VoIP), and others. When you enable WMM (Wi-Fi MultiMedia) function of this network card, you can define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
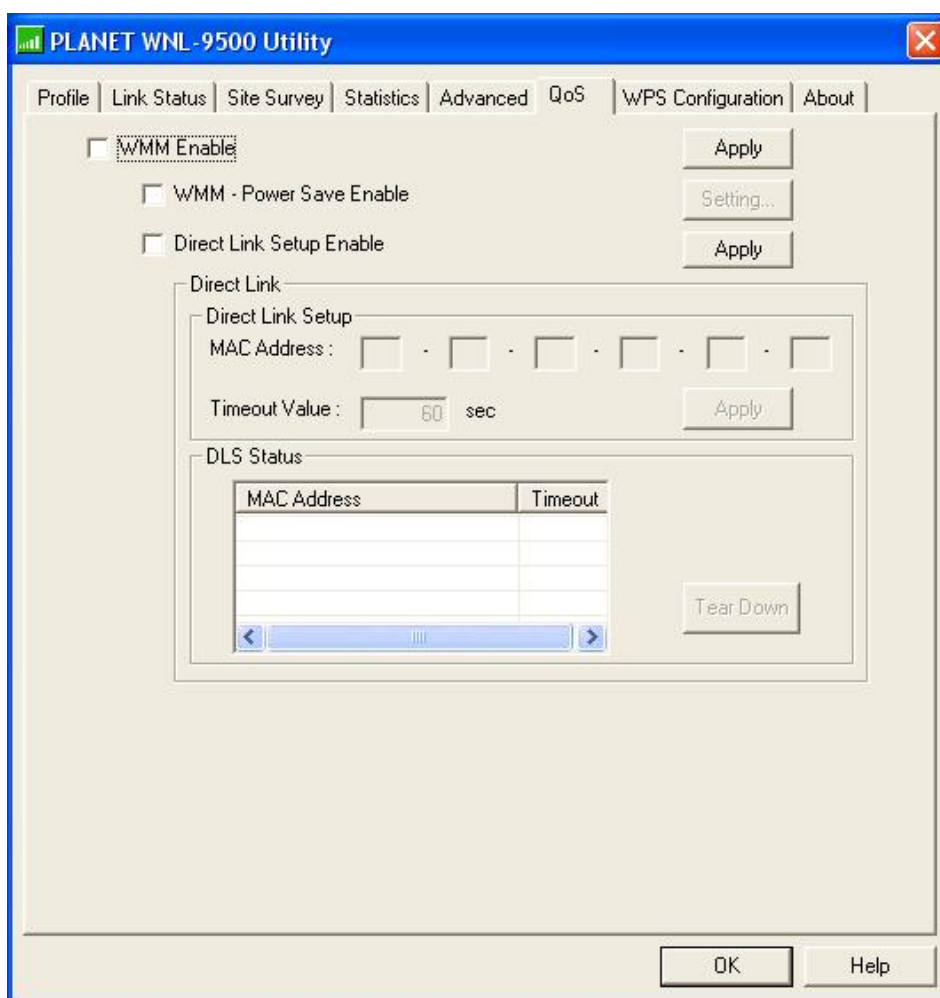
Parameter	Description
WMM Enable	Check this box to enable WMM function. Please click 'Apply' button on the right of this check box after you check or uncheck this box, so corresponding settings in this window will be activated or deactivated respectively.
WMM - Power Save Enable	Enable WMM power saving mode to save energy and lets your battery live longer.

|	
Setting...	Click this button to select the WMM data type which will suppress the function of power saving. When this kind of data is transferring, power saving function will be disabled. Available data types are AC_BK (Background / Low Priority), AC_BE (Best Effort), AC_VI (Video First), and AC_VO (Voice First).
Direct Link Setup Enable	Enable or disable direct link setup (DLS) function. This function will greatly improve the data transfer rate between WMM-enabled wireless devices. Please click 'Apply' button on the right of this check box after you check or uncheck this box, so corresponding settings in this window will be activated or deactivated respectively.
MAC Address	Input the MAC address of another WMM-enabled wireless device you wish to establish a direct link here, then click 'Apply' to add this MAC address to DLS address table.
Timeout Value	Input the timeout value of this WMM-enabled direct link wireless device. If the wireless device is not responding after this time, it will be removed from DLS table.
Tear Down	If you want to remove a specific wireless device from DLS table, select the device and click this button to remove it.

Note: This function does not support in Windows VISTA.

3-6 WPS Configuration

Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption. All you have to do is go to the WPS setup page of this wireless card, click a button, and then press a specific button on the wireless access point you wish to establish a secure connection - just three simple steps!

The WNL-9500 is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the following instructions to establish secure connection between WPS-enabled wireless access point and your wireless network card:

Click 'WPS Configuration' tab, and the following settings will appear:
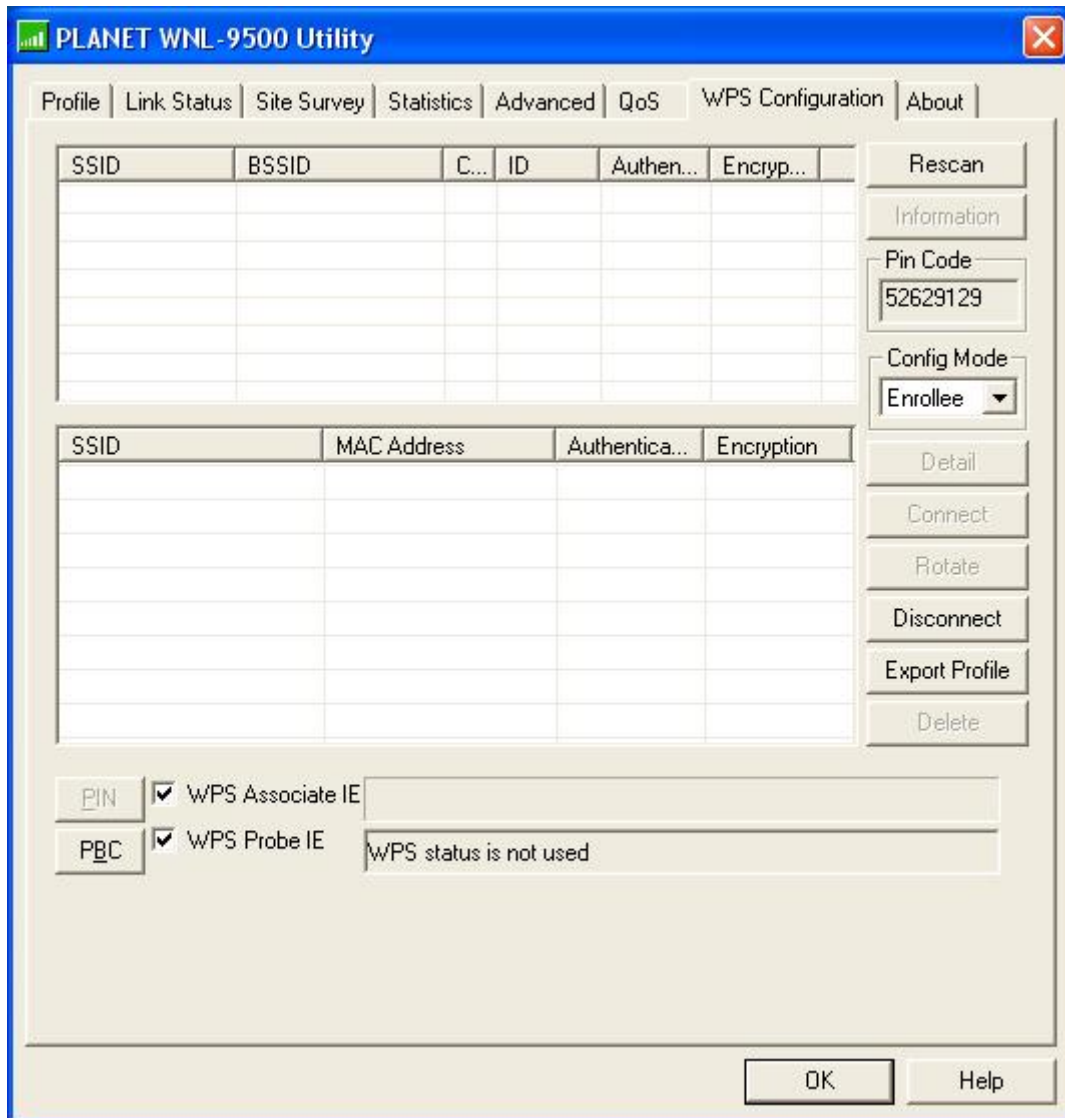
3-6-1 WPS Setup - PBC (Push-Button Configuration)

1.Set 'Config Mode' to 'Enrollee', and then push the 'WPS' button on your wireless access point (the button used to activate WPS standby mode may have another name), or use other way to start WPS standby mode as the instruction given by your wireless access point's user manual.
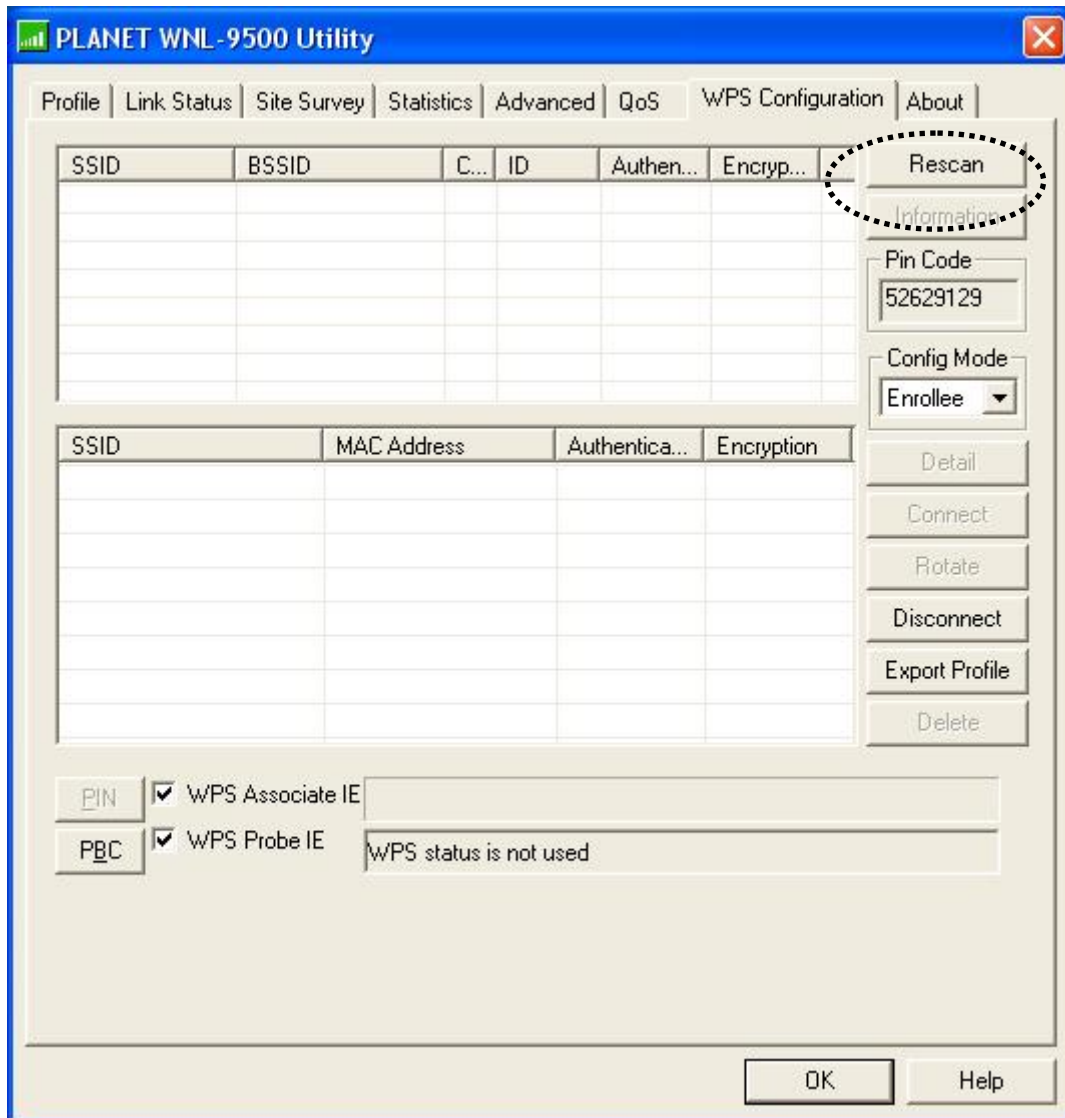
2. Before you start to establish the wireless connection by using WPS, you can click 'Rescan' button to search for WPS-enabled access points near you, to make sure the WPS function of your access point is activated.
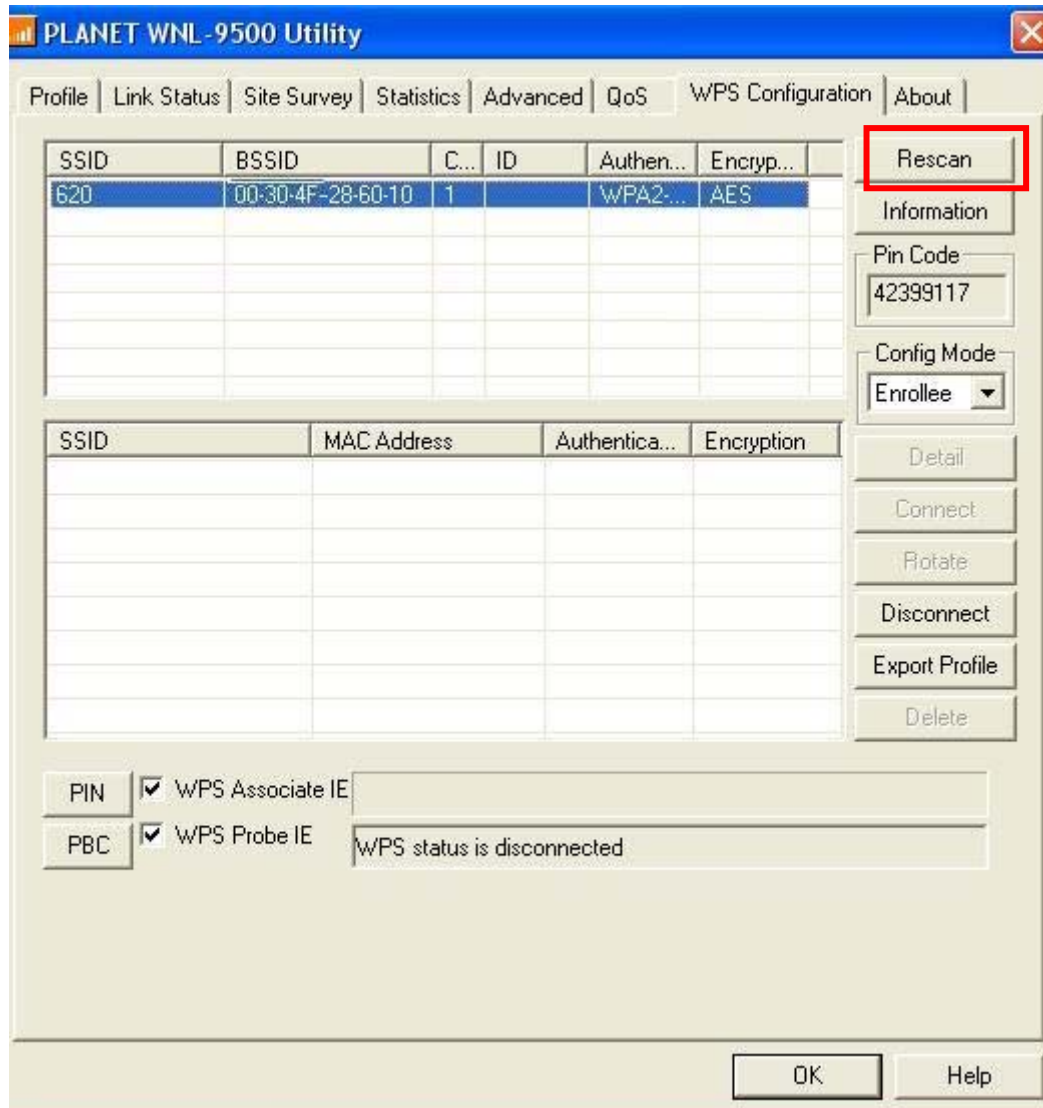
3.All access points found will be displayed. Please make sure the access point you wish to connect is displayed. If not, please click 'Rescan' few more times. You can also click 'Information' button to see the detailed information about selected access point.

4.Click 'PBC' button now to start to establish wireless connection by WPS, and please be patient (This may require several seconds to one minute to complete). When you see 'WPS status is connected successfully' message, it means the connection between your WNL-9500 and access point is successfully connected by WPS, and the information about access point you connected to will be displayed.
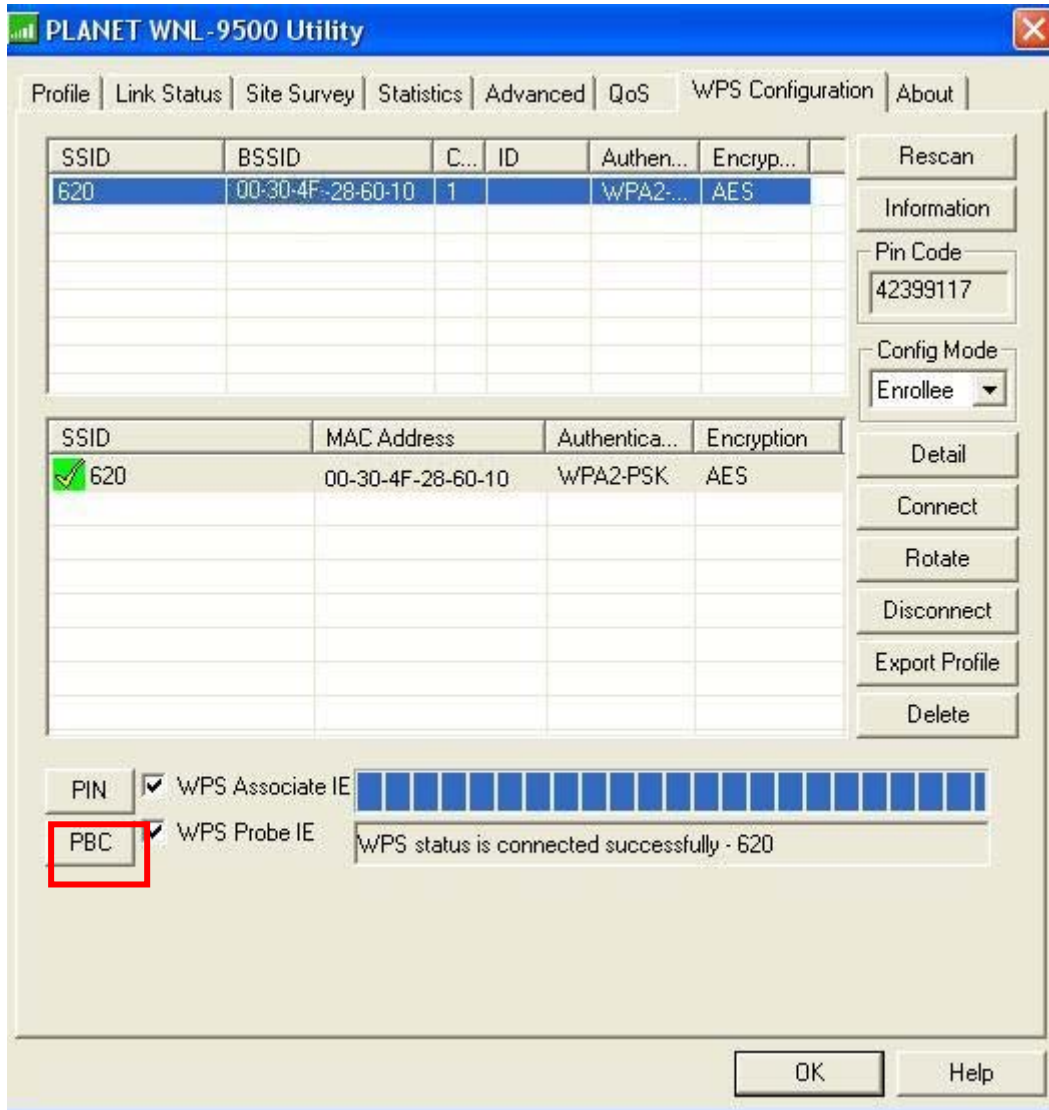
Sometime WPS may fail, and you can click 'PBC' button few more times to try again. When an access point is connected, you can click 'Disconnect' to disconnect your wireless network card from a connected access point, or select another WPS-enabled wireless access point, then click 'Connect' to establish connection to selected access point, if there are more than one WPS-enabled access point found. You can also click 'Rotate' button, and next access point on the list will be selected to establish connection.
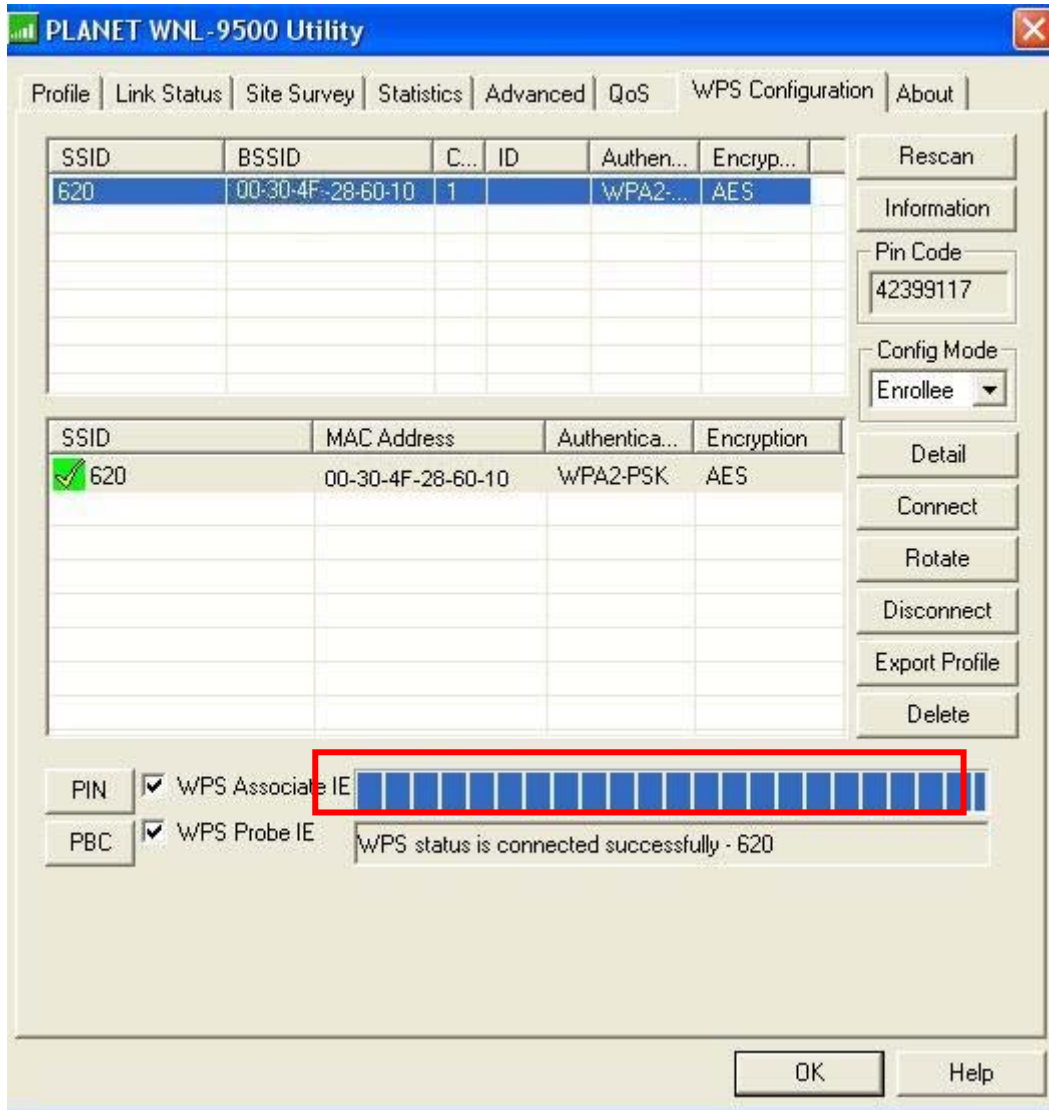
If you want to delete a found access point from the list, select it and click 'Delete' button.

3-6-2 WPS Setup - PIN

The PIN number of your WNL-9500 is an eight-digit number located at the upper-right position of configuration utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this).
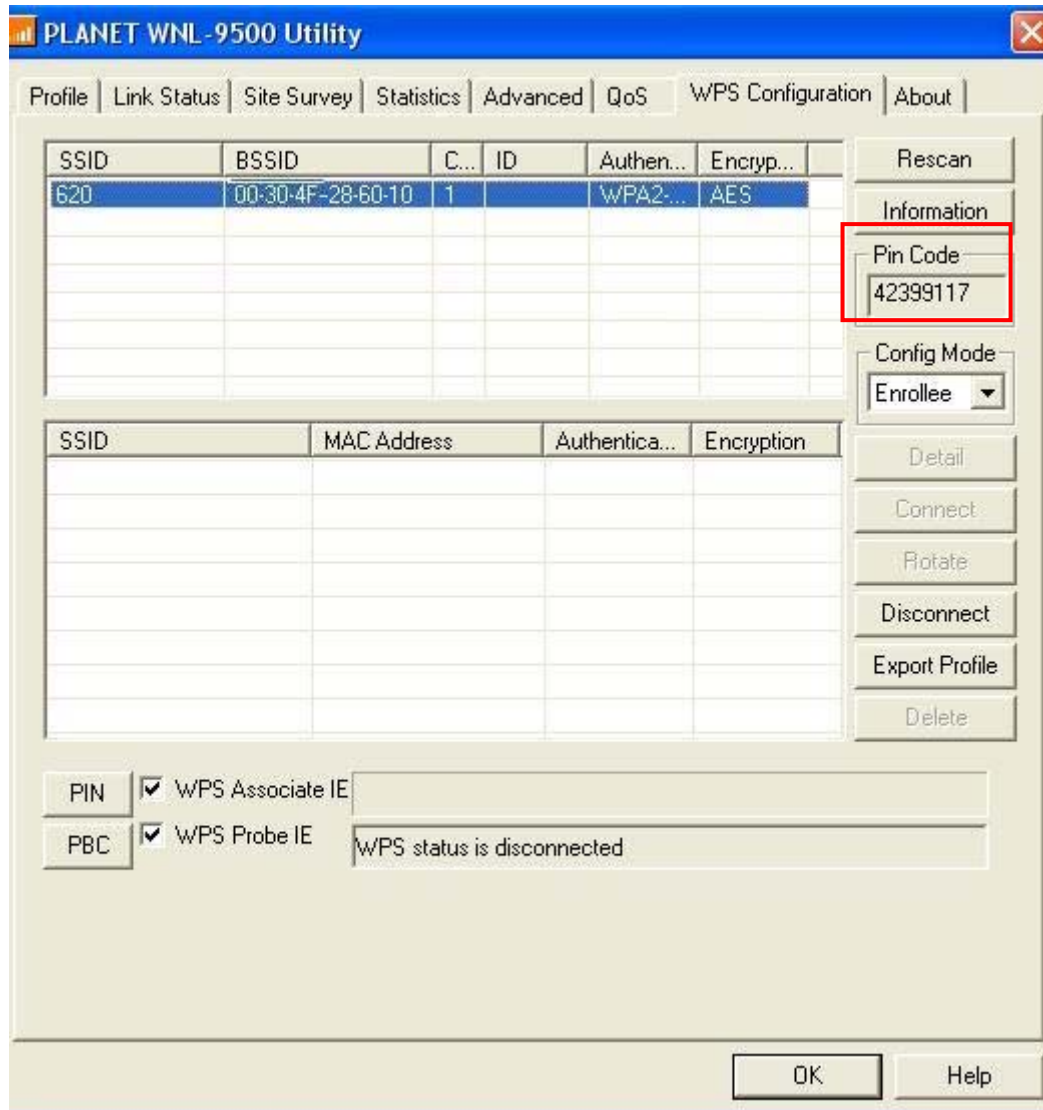
Click 'PIN' button now, and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, you'll be connected to that access point:
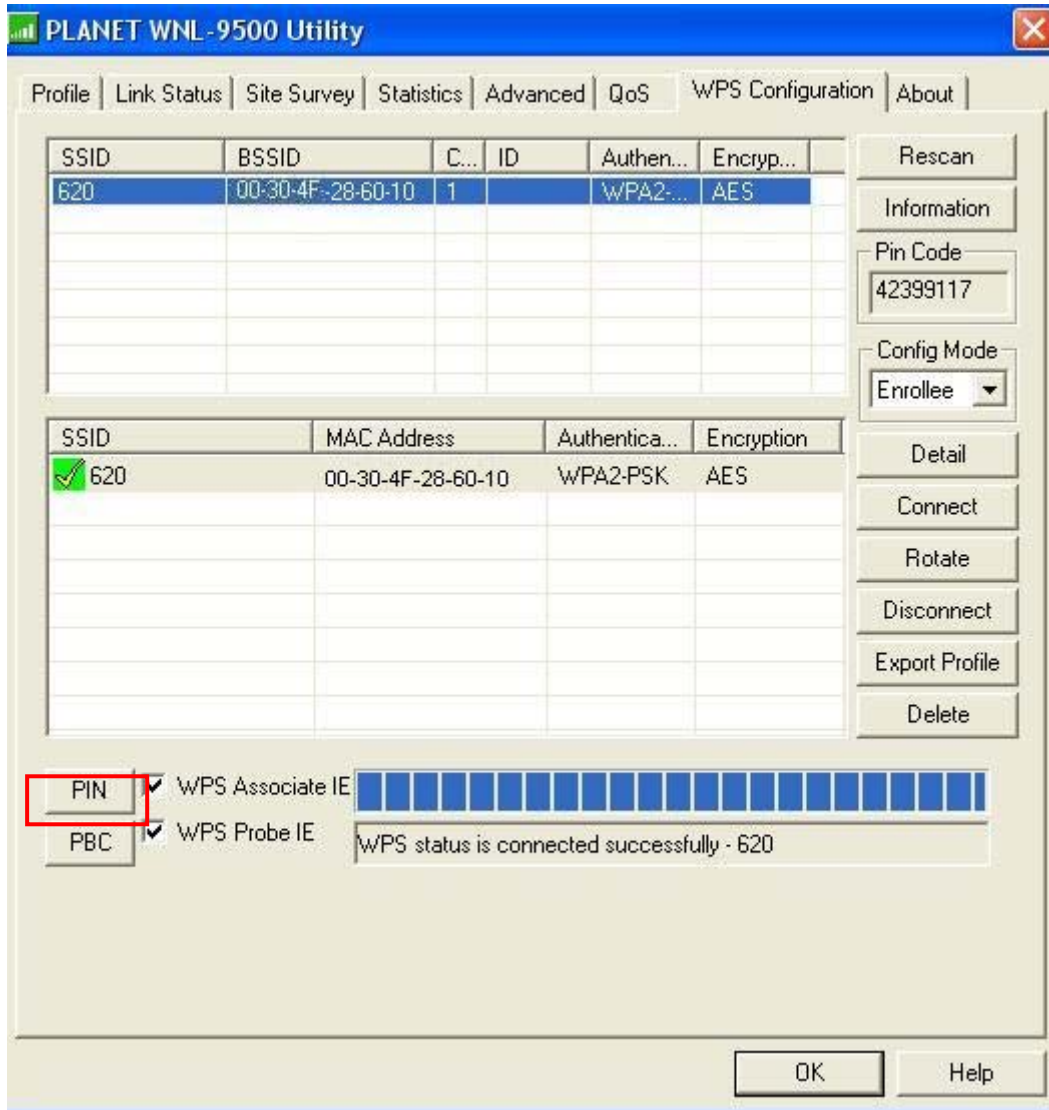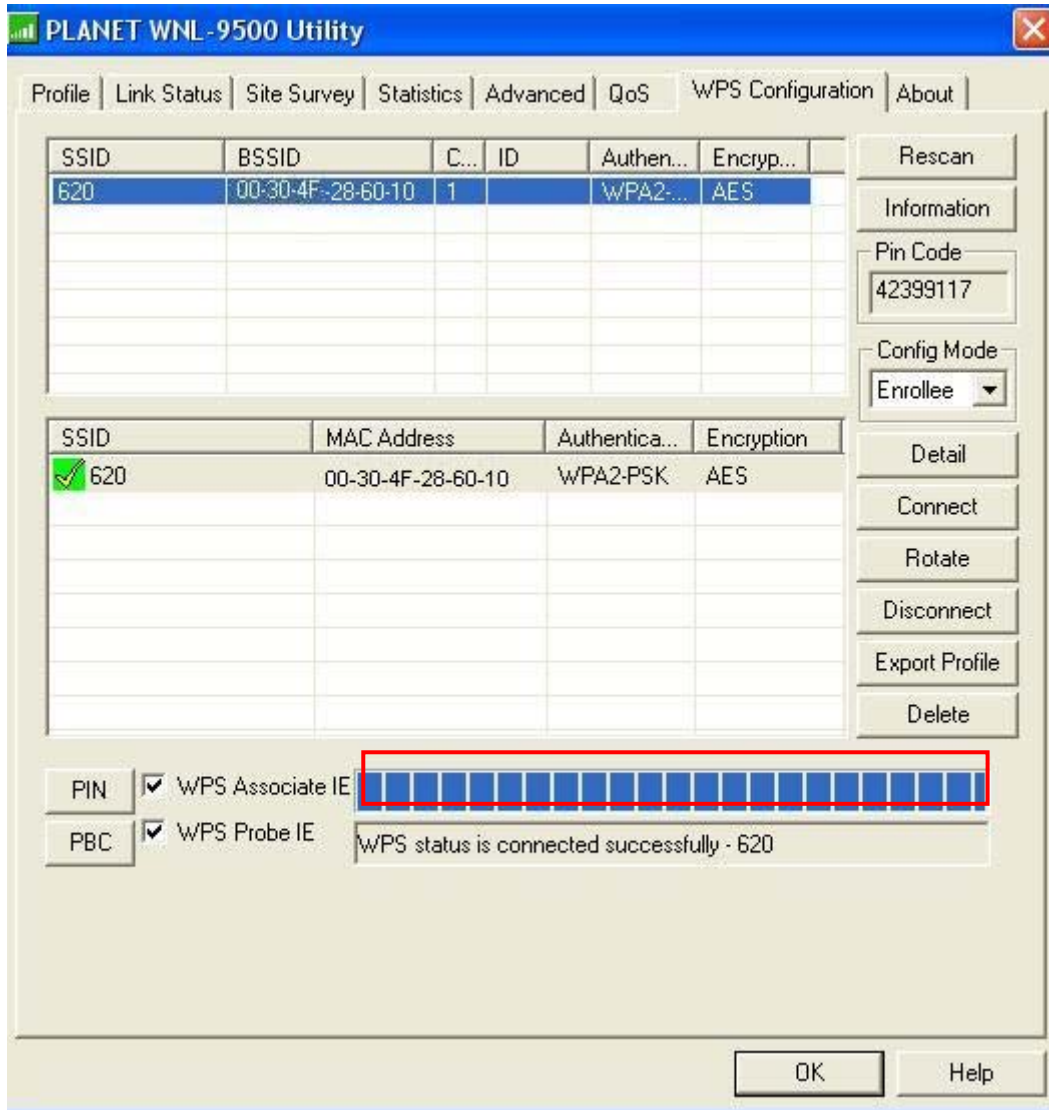
You may have to click 'PIN' for few more times to try again. If you still can not connect to access point by this way, please make sure the PIN code you provided to access point is correct.

3-7 About

By choosing this option, you can click the hyperlink to connect the PLANET website. You can also obtain basic information about the WNL-9500 such as the Driver, Utility and EEPROM Version. The MAC Address of the card is displayed in the screen as well.
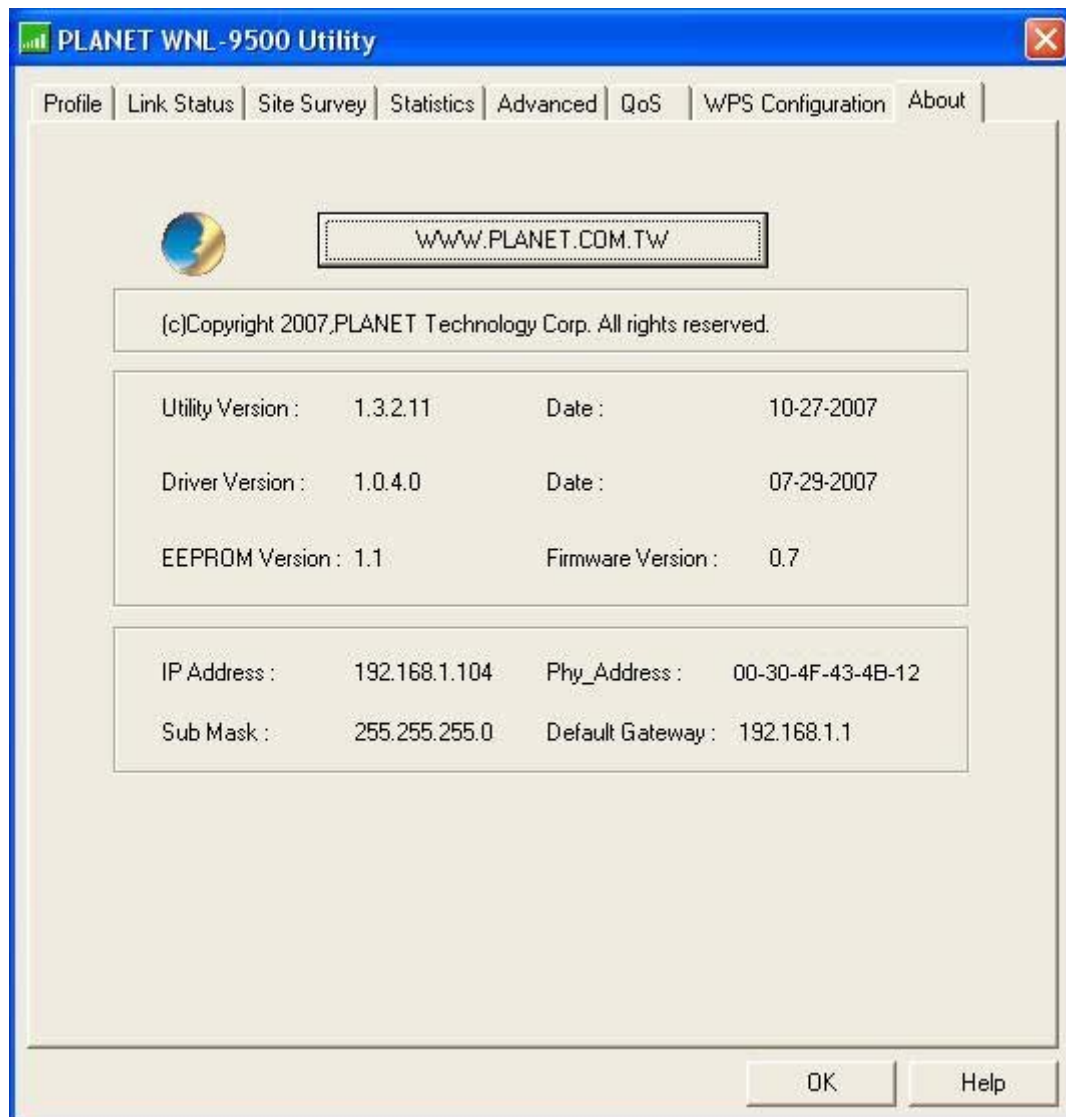
Please click 'OK' to close configuration utility.

Chapter 4: Soft-AP Function

Except becoming a wireless client of other wireless access points, the WNL-9500 can act as a wireless service provider also! You can switch the WNL-9500's operating mode to 'AP' mode to simulate the function of a real wireless access point by software, and all other computers and wireless devices can connect to your computer wirelessly, even share the internet connection you have!

4-1 Switch to AP Mode and Basic Configuration

The operating mode of the wireless card is 'Station Mode' (becoming a client of other wireless access points) by default. If you want to switch to AP mode, please right-click WNL-9500 utility icon, and select 'Switch to AP Mode'.
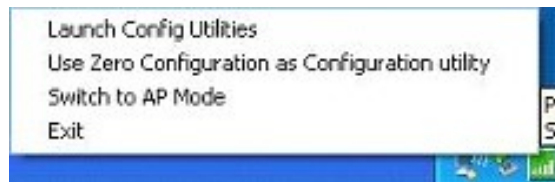
After you select 'Switch to AP Mode', the WNL-9500 available options will change.

If you want to switch the wireless card back to station mode (become a client of other wireless access points), click 'Switch to Station Mode'.
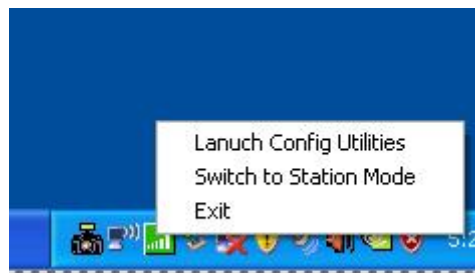
A configuration window will appear after you switch the operation mode to 'AP' or click 'Launch Config Utilities' after you right-click the WNL-9500 configuration utility, which asks you to assign an existing network card with internet connection:
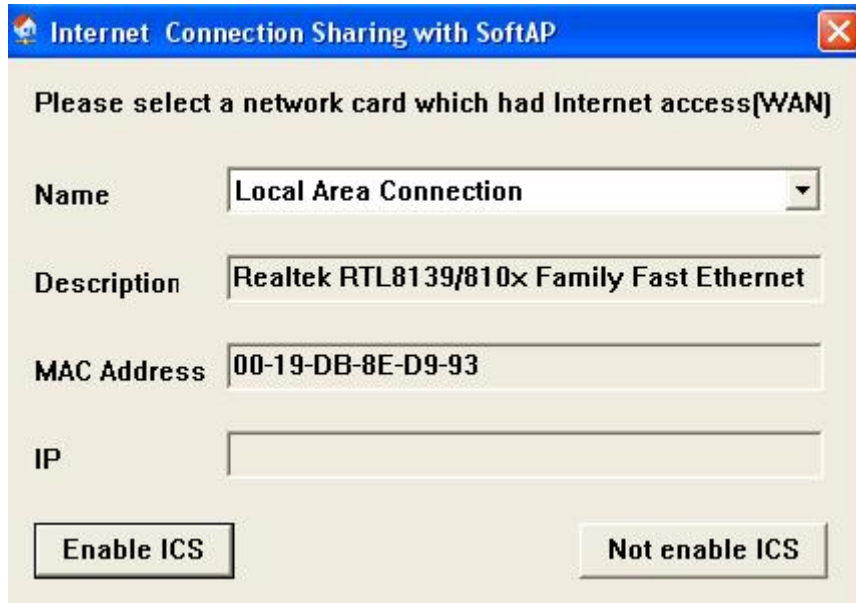
If your computer has another network card which is connected to Internet, please select it from 'Name' dropdown menu, and click 'Enable ICS'; if your computer does not have another network card with Internet connection, please click 'Not enable ICS'.

After you click 'Enable ICS' or 'Not enable ICS', you'll see the basic configuration menu of the AP function:

Parameter	Description
SSID	Please input the SSID (the name used to identify this wireless access point) here. Up to 32 numerical characters can be accepted here, excepting space.
Channel	Please select the wireless channel you wish to use. The number of channels available here will vary depends on the setting of 'Country Region Code'.
Wireless Mode	Please select the wireless operating mode. You can limit the type of wireless client to 802.11b or 802.11g only, or allow 802.11b/g, and 802.11b/g/n clients. It's safe to select '802.11 B/G/N mix' to allow all kinds of wireless client to connect to your computer, unless you want to limit the type of wireless client allowed to connect to your computer.

Use MAC Address	Click this button to use the MAC address of the wireless card as SSID. A prefix of 'AP' will be added.
Security Setting	Set the security options (wireless data encryption).
Country Region Code	Available options are 0-7, which will affect the available wireless channels you can use: 0: FCC (US, Canada, and other countries uses FCC radio communication standards) 1: ETSI (Europe) 2: SPAIN 3: FRANCE 4: MKK 5: MKKI (TELEC) 6: ISERAL (Channel 3 to 9) 7: ISERAL (Channel 5 to 13) The operating frequency channel will be restricted to the country / region user located before importing
Beacon (ms)	You can define the time interval that a beacon signal should be send. Default value is 100. Do not modify this value unless you know what will be affected
Idle Time	Select the idle time of your wireless network card. Default value is 300. Do not modify this value unless you know what will be affected
No forwarding among wireless clients	Check this box and wireless clients will not be able to share data with each other.
Hide SSID	Check this box and the SSID will not be broadcasted to the public. Your wireless clients must know the exact SSID to be able to connect to your computer. This option is useful to enhance security level.
Allow BW 40MHz	Check this box to allow BW 40MHz capability.

Default	Click this button to restore all settings in this page back to default value.
Apply	Click this button to activate current settings.

To exit, click 'X' button at the upper-right corner of configuration window.

4-2 Security Settings

This wireless card supports wireless encryption in AP mode, which will encrypt the data being transferred over the air to enhance data security level. It's recommended to enable data encryption unless you wish to open your computer (and its internet connection) to the public.

When you click 'Security Setting' in WNL-9500 configuration utility, the following window will appear:

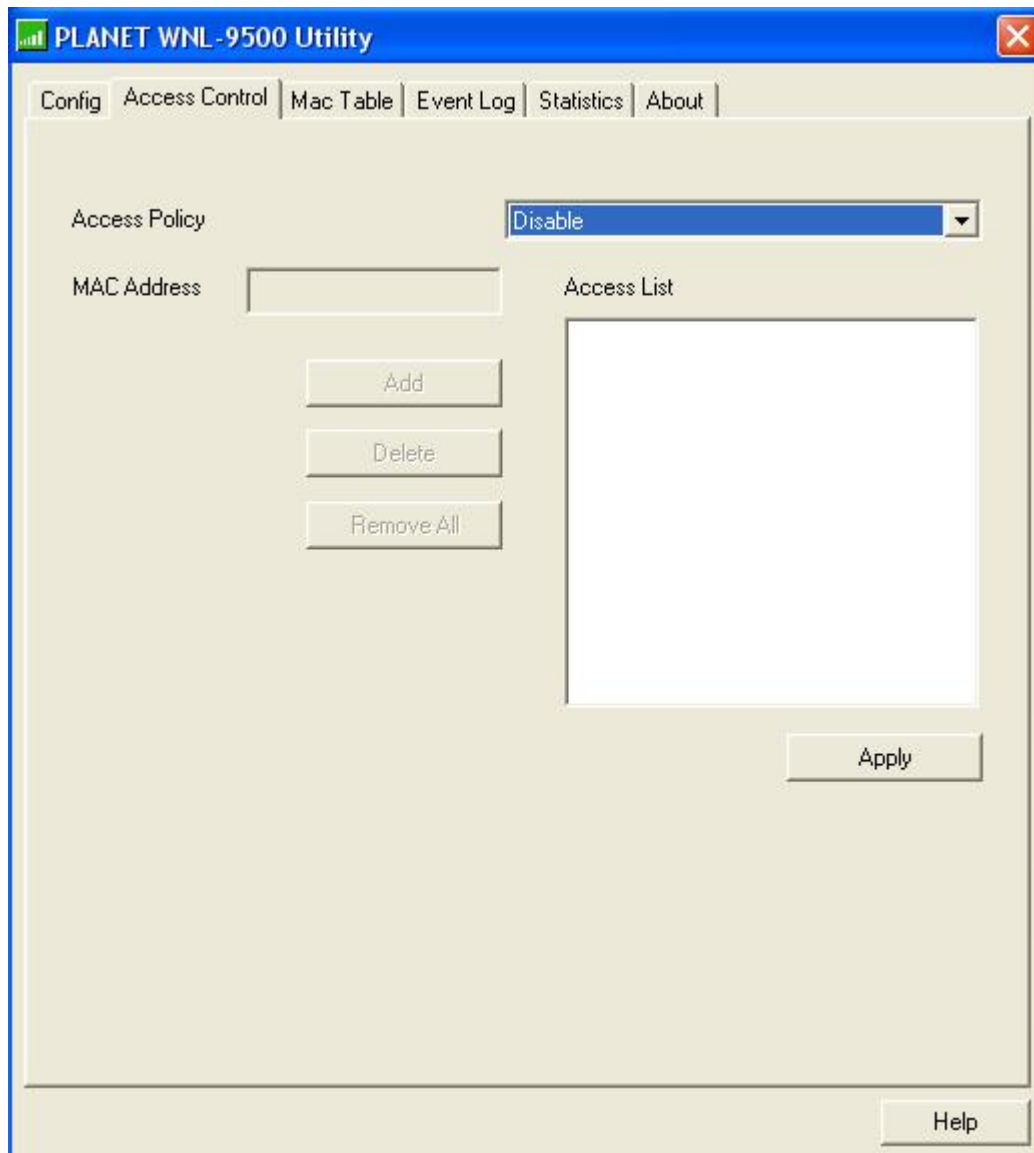| Parameter	Description
Authentication Type	Please select a wireless authentication type you wish to use. Available options are 'Open', 'Shared', 'WPA-PSK', 'WPA2-PSK', and 'WPA-PSK / WPA2-PSK'. If you want to disable wireless data encryption, you must select 'Open' or 'Shared'.

Encryption Type	Please select an encryption mode. The available options in this setting item will vary depending on the authentication type you select. If you select 'Not Use', data will not be encrypted and people with some networking knowledge will be able to read the data you transfer with proper tool.

NOTE: WPA encryption is safer than WEP, however, some older wireless clients don't support WPA encryption. |
| WPA Pre-shared-key | Please input the WPA pre-shared key here. Only clients with the same pre-shared key you inputted here will be able to connect to your computer. This setting is only available when you select one of WPA encryptions. |
| Group Rekey Interval | You can specify the time interval to re-issue the key to your wireless clients here. You can click the button '10 seconds' or 'Kpackets' to change the unit of time interval. (every 10 seconds or a thousand data packets times the value you specified in 'Group Rekey Interval' field) |
| WEP Key #1-4 | Please input the WEP encryption key here when you select 'WEP'

If you want to use WEP 64 bits encryption, please input 10 characters if you select HEX, or input 5 characters if you select ASCII; If you want to use WEP 128bits encryption, please input 26 characters if you select HEX, or input 13 characters if you select ASCII. 128 bits encryption is safer then 64 bits, but the data transfer speed will be slightly reduced. |
Show Password	Check this box and the WPA pre-shared key or WEP key you inputted will be shown, but not replaced by asterisk (*).
OK	Click this button to save changes you made in this page.
Cancel	Click this button to discard all changes you made in this window.

4-3 Access Control

If you're not going to open your computer and wireless resources to the public, you can use MAC address filtering function to enforce your access control policy, so only wireless clients with MAC address you defined by this function can be connected to your software access point.

Click 'Access Control' tab, and the following messages will appear:

Parameter	Description
Access Policy	Select the policy type of your access rule: Disable: Allow any wireless client with proper authentication settings to connect to this access point. Allow All: Only allow wireless clients with MAC address listed here to connect to this access point. Reject All: Reject wireless clients with MAC address listed here to be connected to this access point.
MAC Address	Input the MAC address of the wireless client you wish to allow or reject here. No colon (:) or hyphen (-) required.

Add	Add the MAC address you inputted in 'MAC address' field to the list.
Delete	Please select a MAC address from the list, then click 'Delete' button to remove it.
Remove all	Delete all MAC addresses in the list.
Apply	Save and apply changes you made.

4-4 Connection table

If you want to see the list of all wireless clients connected to this access point, please follow the following instructions:

Click 'Mac Table' tab, and a list containing all connected wireless clients will appear:
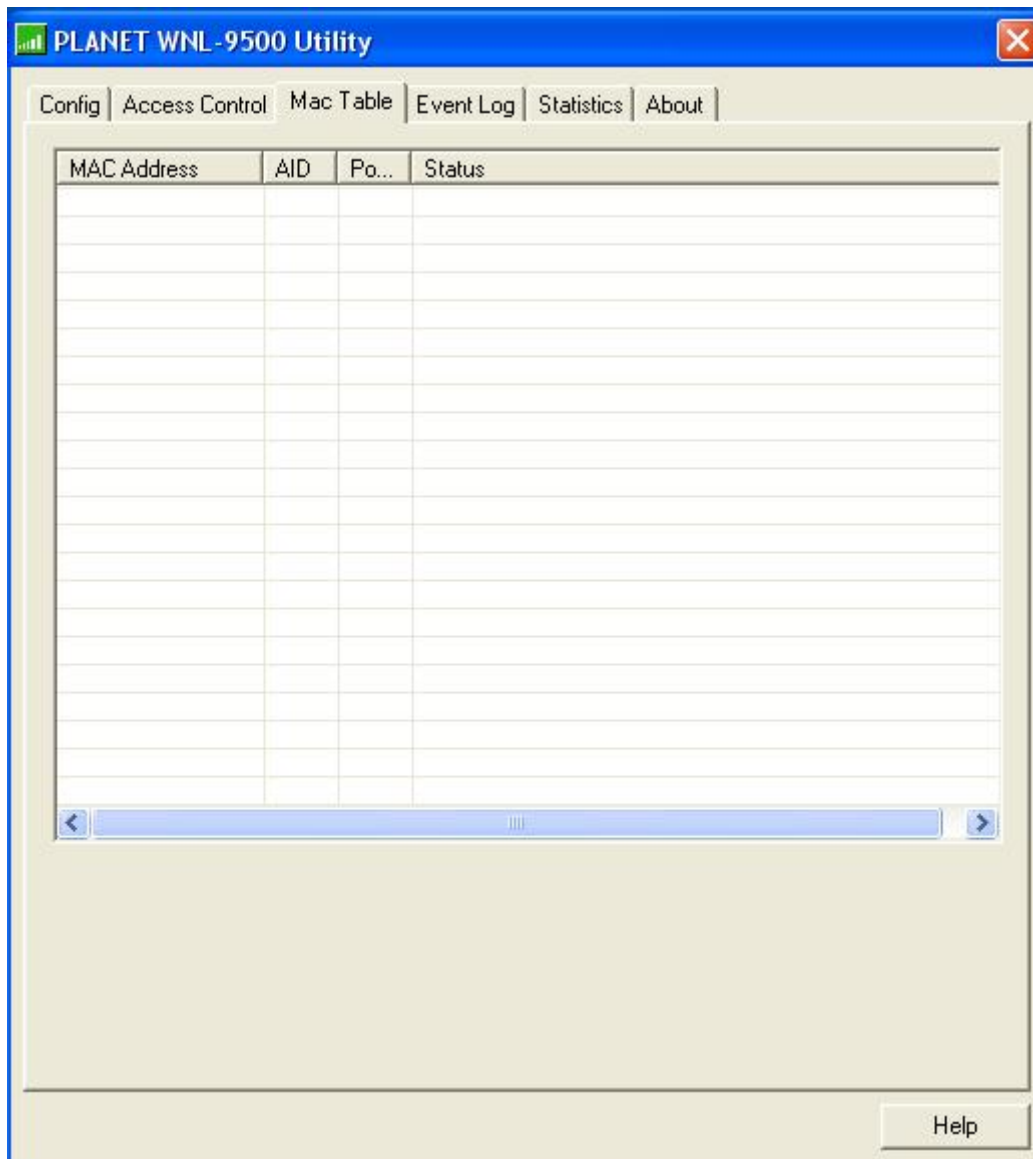
Parameter	Description
MAC address	Displays the MAC address of this wireless client
AID	The serial number of this wireless connection.
Power Saving Mode	Displays the capability of power-saving function of this wireless client.
Status	Displays additional information of this wireless Connection, like current wireless operating mode and data transfer rate.

4-5 Event Log

This software access point will log all wireless-related activities as a log. You can follow the following instructions to view the content of the event log:

Click 'Event Log' tab, and the event log will be displayed:

You can click 'Clear' to remove all entries in the log.

4-6 Statistics

If you want to know detailed information about how your software access point works, you can follow the following instructions to view the statistics of the access point:

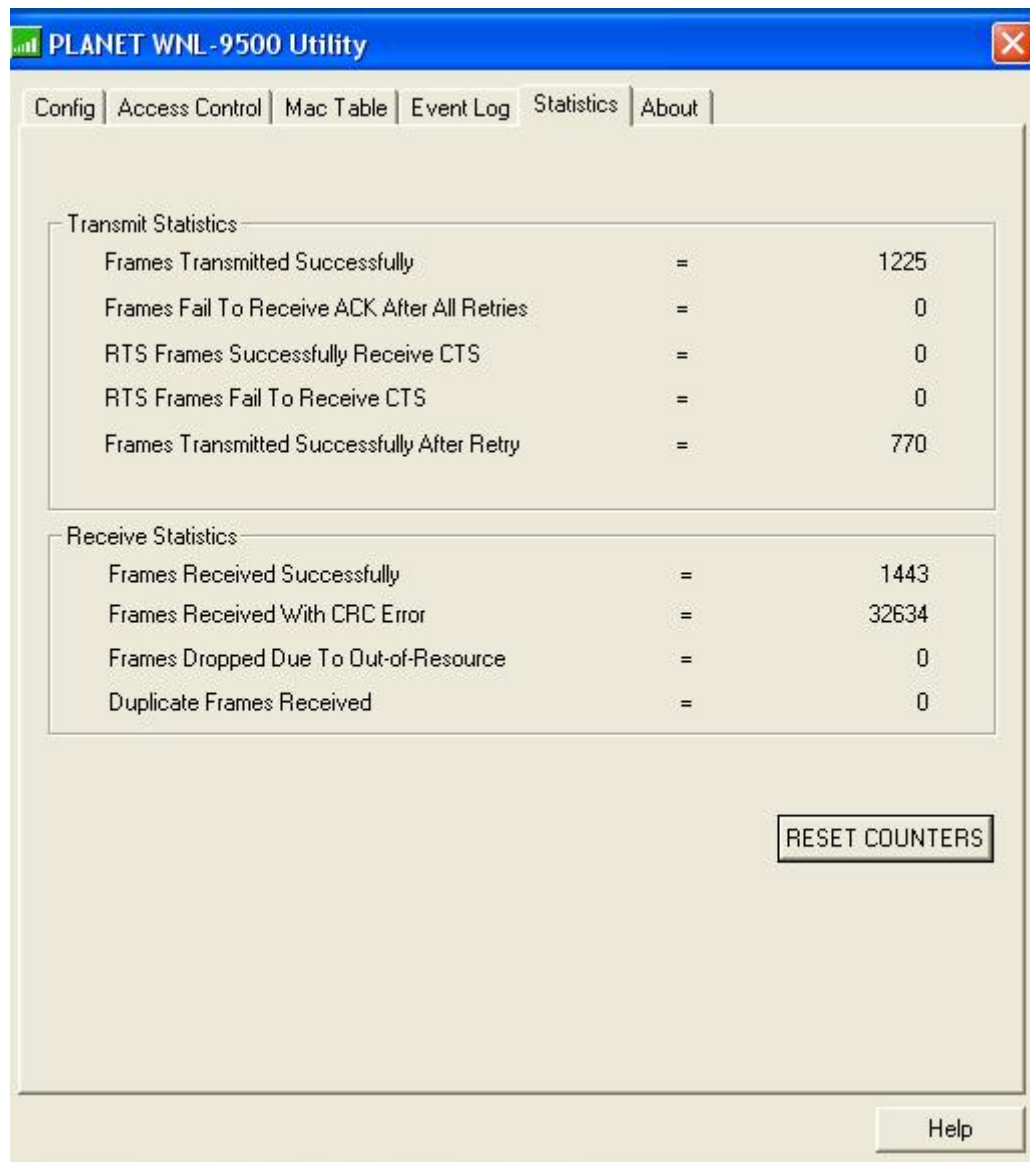Click 'Statistics' tab, and the event log will be displayed:

You can click 'RESET COUNTERS' button to reset all counters to zero.

CHAPTER 5:   APPENDIX

5-1 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

Q. The PLANET WNL-9500 does not work properly.

A.

1. Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find the Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of the Adapter. If there is a yellow question mark, please check the following:

2. Make sure that your PC has a free IRQ (Interrupt Request, a hardware interrupt on a PC.)

3. Make sure that you have inserted the right adapter and installed the proper driver. If the Adapter does not function after attempting the above steps, remove the adapter and do the following:

4. Uninstall the driver software from your PC.

5. Restart your PC and repeat the hardware and software installation as specified in this User Guide.

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

A.

1. Make sure that the PC to which the Adapter is associated is powered on.

2. Make sure that your Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

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

A.

1. Check that the LED indicators for the broadband modem are indicating normal activity. If not, there may be a problem with the broadband connection.

2. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network.

3. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points.

4. In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it

might be necessary to set up one client to establish a BSS (Basic Service Set) and wait briefly before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it.

5. Check that the Network Connection for the wireless client is configured properly.
   If Security is enabled, make sure that the correct encryption keys are entered on both the Adapter and the access point.

Q. I can't find any wireless access point / wireless device in 'Site Survey' function.
A.
1. Click 'Rescan' for few more times and see if you can find any wireless access point or wireless device.

2. Please move closer to any known wireless access point.

3. 'Ad hoc' function must be enabled for the wireless device you wish to establish a direct wireless link.

4. Please adjust the position of network card (you may have to move your computer if you're using a notebook computer) and click 'Rescan' button for few more times. If you can find the wireless access point or wireless device you want to connect by doing this, try to move closer to the place where the wireless access point or wireless device is located.

Q. Nothing happens when I click 'Launch config utilities'
A.
1. Please make sure the wireless network card is firmly inserted into your computer's PCI slot. If the Planet configuration utility's icon is black, the network card is not detected by your computer. Switch the computer off and insert the card again. If this doesn't work, contact the dealer of purchase for help.

2. Reboot the computer and try again.

3. Remove the driver and re-install.

4. Contact the dealer of purchase for help.

Q. I can not establish connection with a certain wireless access point
A.
1. Click 'Connect' for few more times.
2. If the SSID of access point you wish to connect is hidden (nothing displayed in 'SSID' field in 'Site Survey' function), you have to input correct SSID of the access point you wish to connect. Please contact the owner of access point to ask for correct SSID.
3. You have to input correct passphrase / security key to connect an access point with encryption. Please contact the owner of access point to ask for correct passphrase / security key.
4. The access point you wish to connect only allows network cards with specific MAC address to establish connection. Please go to 'About' tab and write the value of 'Phy_Addess' down,

then present this value to the owner of access point so he / she can add the MAC address of your network card to his / her access point's list.

Q. The network is slow / having problem when transferring large files

A.

1. Move closer to the place where access point is located.
2. Enable 'Wireless Protection' in 'Advanced' tab.
3. Try a lower TX Rate in 'Advanced' tab.
4. Disable 'Tx Burst' in 'Advanced' tab.
5. Enable 'WMM' in 'QoS' tab if you need to use multimedia / telephony related applications.
6. Disable 'WMM – Power Save Enable' in 'QoS' tab.
7. There could be too much people using the same radio channel. Ask the owner of the access point to change the channel number.

5-2 Glossary

1.   What is WMM?

Wi-Fi Multimedia (WMM), a group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

2.   What is WMM Power Save?

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio, or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power saves. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power "dozing" state.

3.   What is GI?

GI stands for Guard Interval. It's a measure to protect wireless devices from cross-interference. If there are two wireless devices using the same or near channel, and they are close enough, radio interference will occur and reduce the radio resource usability.

4.   What is STBC?

STBC stands for Space-Time Block Coding, which is a technique used to transfer multiple

copies of data by multiple antenna, to improve data transfer performance. By using multiple antennas, not only data transfer rate is improved, but also the wireless stability.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com