802.11n Wireless USB Adapter

WNL-U552

User's Manual

Version: 1.00

Date: August 2007

Copyright

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 USB Adapter

Model: WNL-U552

Rev: 1.0 (August 2007)

Part No. EM-WNLU552

CONTENTS

Chapter 1 Introduction

For higher wireless transfer performance, we are glad to introduce the PLANET 802.11n wireless USB adapter – WNL-U552. It is a USB 2.0 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-U552 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 the Network Card can send its data streams with greater distances and be more reliable. The WNL-U552 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-U552 supports two types of WPS, Push-Button Configuration (PBC) and PIN code (key Wireless adapter card pin number)

For WLAN security issues, the WNL-U552 supports both 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-U552 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

- 2.4GHz ISM band, unlicensed operation
- Supports Wi-Fi Protected Setup (WPS)
- Compliant with IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0)
- Compliant with USB 1.1/2.0 standard
- Support 64/128-bit WEP and WAP/WAP2 high-level security mechanisms
- Support Ad-Hoc / Infrastructure 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 and Vista

1.2 Specifications

Interface	USB 1.1 / 2.0, Type-A
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
RF Modulation	802.11b: DSSS, CCK, QPSK, BPSK 802.11g: OFDM 802.11n: 64QAM, 16QAM, QPSK, BPSK
Output Power	11b mode: 16~18dBm 11g mode: 14~16dBm 11n mode: 11~13dBm
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 / Vista
Environmental & Mechanical Characteristics	
Temperature	Operating: 0 °C ~ 55 °C Storage: -20 °C ~ 70 °C
Operating Humidity	Operating: 0 ~ 85% Storage: 0 ~ 95% Non-Condensing
Dimensions	83 x 27 x 10 mm (L x W x H)
Weight	14g
Certifications	FCC, CE

1.3 Package Contents

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

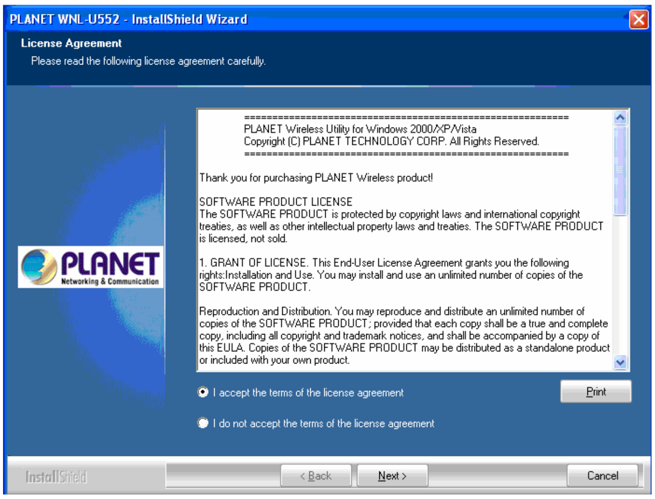
1 x WNL-U552
1 x Driver and User's manual CD
1 x Quick Installation Guide

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

Chapter 2 Installation Procedure

Utility Installation

1. Insert the bundled CD into the CD-ROM drive to launch the auto run program. Once completed, a menu screen will appear.
2. Click the “Configuration Utility” hyperlink in the WNL-U552 field to initiate the installation procedure. **Note**: If the menu screen does not appear, click “Start” at the taskbar. Then, select “Run” and type **“E:\Utility\WNL-U552\setup.exe”**, where the E is your CD-ROM drive.
3. Read the License Agreement carefully. Click “Yes” to accept it and continue.



PLANET WNL-U552 - InstallShield Wizard

License Agreement

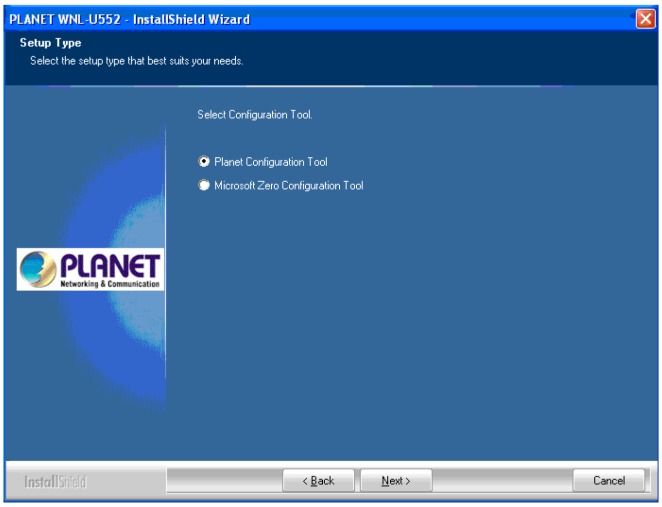
Please read the following license agreement carefully.

```
        =============================================================
        PLANET Wireless Utility for Windows 2000/XP/Vista
        Copyright (C) PLANET TECHNOLOGY CORP. All Rights Reserved.
        =============================================================

Thank you for purchasing PLANET Wireless product!

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright
treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT
is licensed, not sold.

1. GRANT OF LICENSE. This End-User License Agreement grants you the following
rights:Installation and Use. You may install and use an unlimited number of copies of the
SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of
copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete
copy, including all copyright and trademark notices, and shall be accompanied by a copy of
this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product
or included with your own product.
```

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

4. It is suggested to use “PLANET Configuration Tool” to manage the WNL-U552. Click “Next” to continue.



PLANET WNL-U552 - InstallShield Wizard

Setup Type

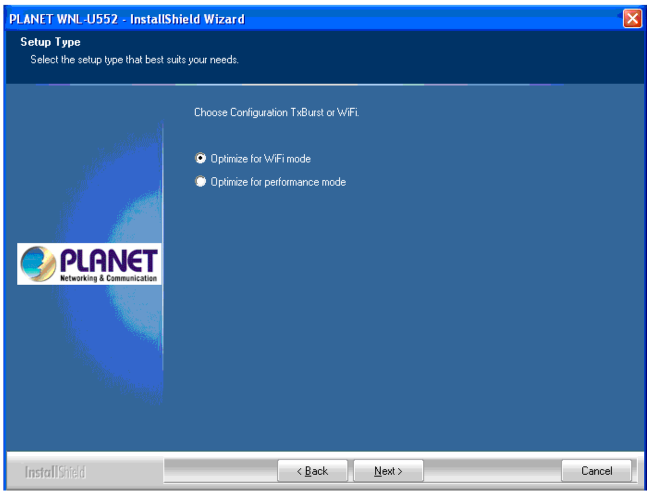
Select the setup type that best suits your needs.

Select Configuration Tool.

● Planet Configuration Tool

○ Microsoft Zero Configuration Tool

5. If “Optimize for performance mode” is selected, the “Tx BURST” option will be enabled to increase the transfer speed. However, the AP must support this feature as well. If the target AP is complying with 802.11b/g standard, please select “Optimize for WiFi mode”.


PLANET WNL-U552 - InstallShield Wizard

Setup Type

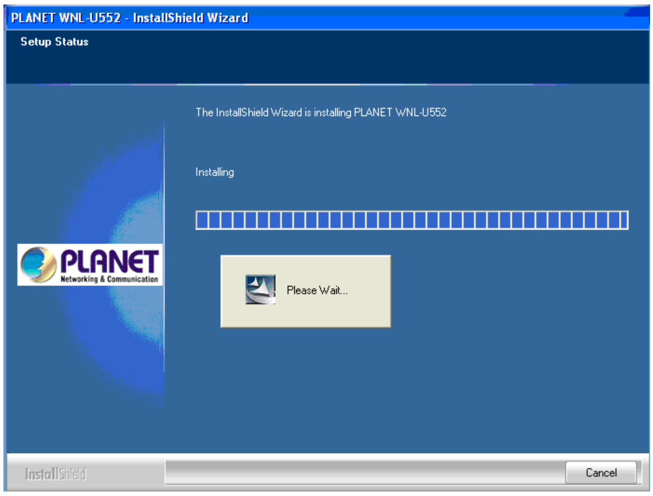
Select the setup type that best suits your needs.

Choose Configuration TxBurst or WiFi.

● Optimize for WiFi mode

○ Optimize for performance mode

6. You can see the installation progress in this screen.


PLANET WNL-U552 - InstallShield Wizard

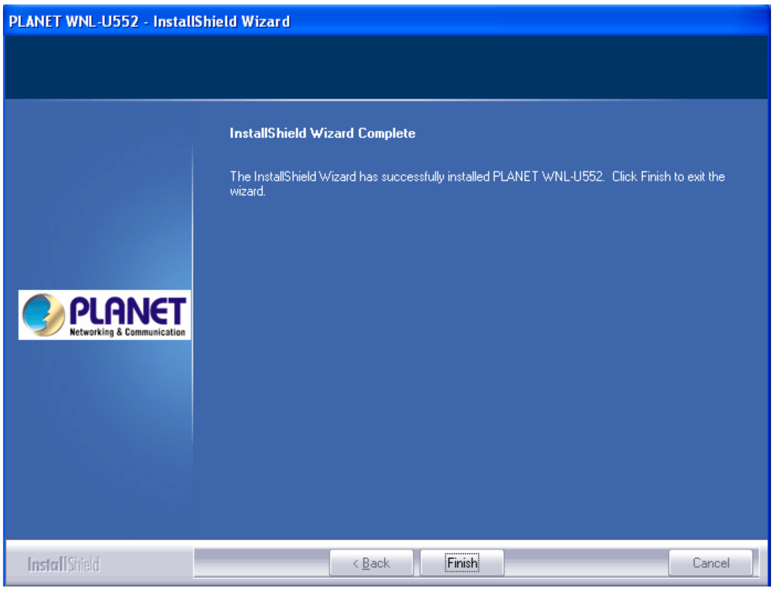
Setup Status

The InstallShield Wizard is installing PLANET WNL-U552

Installing

Please Wait...

7. Please click “Finish” to finish the installation.

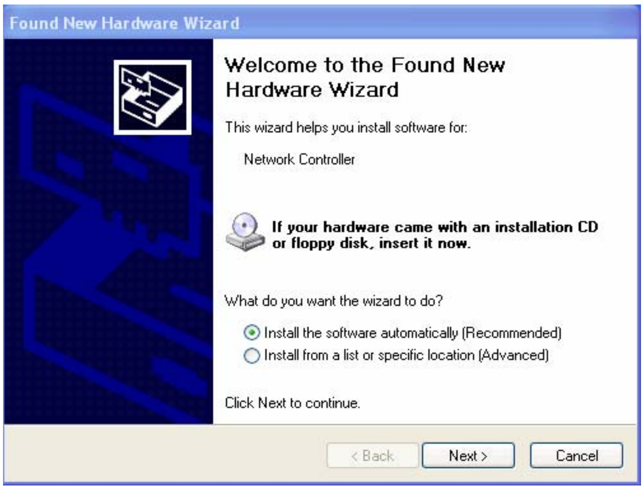

PLANET WNL-U552 - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed PLANET WNL-U552. Click Finish to exit the wizard.

Driver Installation

1. Please insert WNL-U552 into a vacant USB port of your PC.
2. Windows will detect this device automatically. When the “Found New Hardware Wizard” dialog box appears, please click “Cancel”.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

Network Controller

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

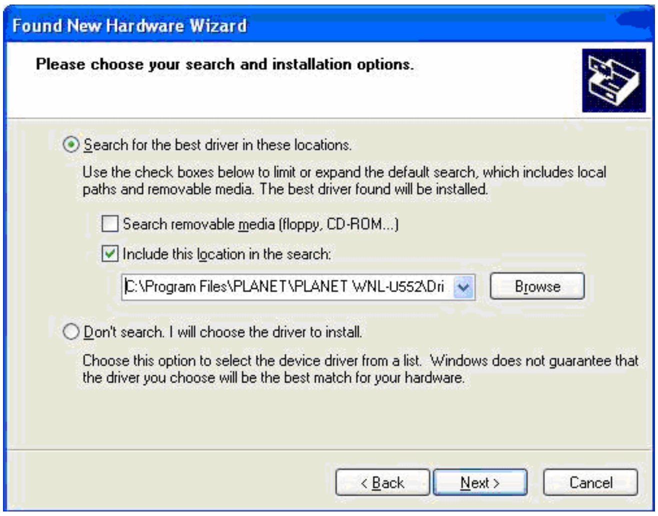
What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

3. Choose the first one “Search for the best driver in these locations” and tick the box of “include this location in the search:” and then to click “Browse” to direct the hardware driver where is in “**C:\Program Files\PLANET\ PLANET WNL-U552\Driver**” Then click “Next” to continue.



Found New Hardware Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

□ Search removable media (floppy, CD-ROM...)

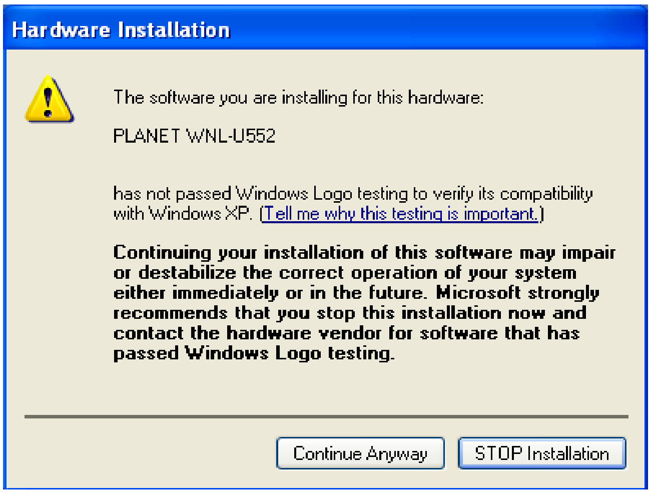
☑ Include this location in the search:

C:\Program Files\PLANET\PLANET WNL-U552\Dri

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

4. The screen will appear to inform that you are installing PLANET WNL-U552. Please click “Continue Anyway” to continue.



Hardware Installation

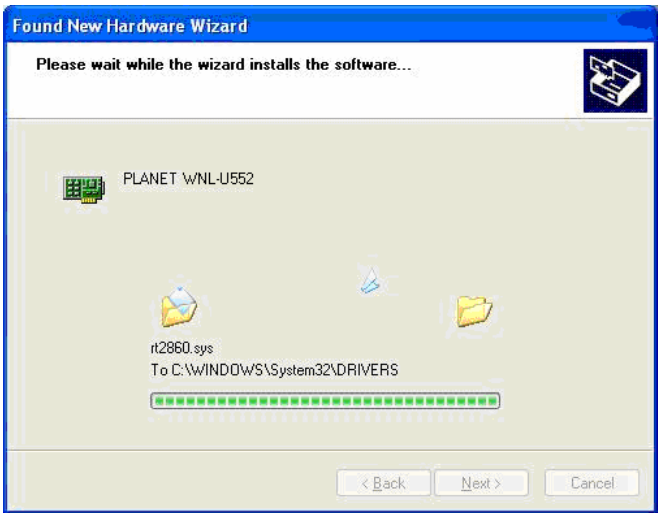
The software you are installing for this hardware:

PLANET WNL-U552

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

5. The screen will show the rate of progress for the installation of WNL-U552 as below.



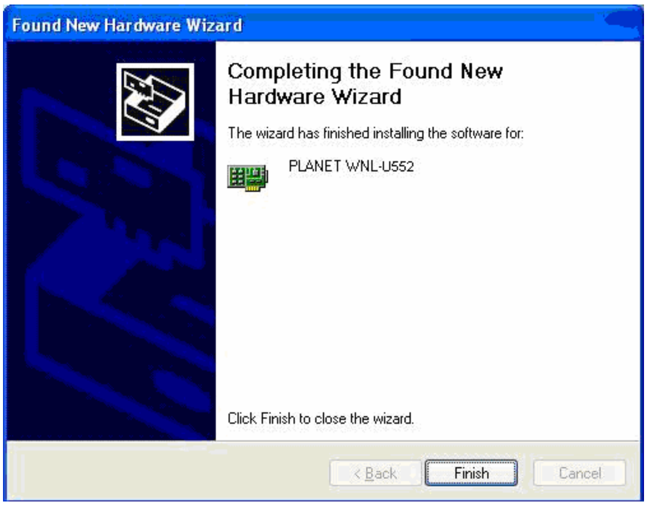
Found New Hardware Wizard

Please wait while the wizard installs the software...

PLANET WNL-U552

rt2860.sys
To C:\WINDOWS\System32\DRIVERS

6. Please click “Finish” to complete the driver installation



Found New Hardware Wizard

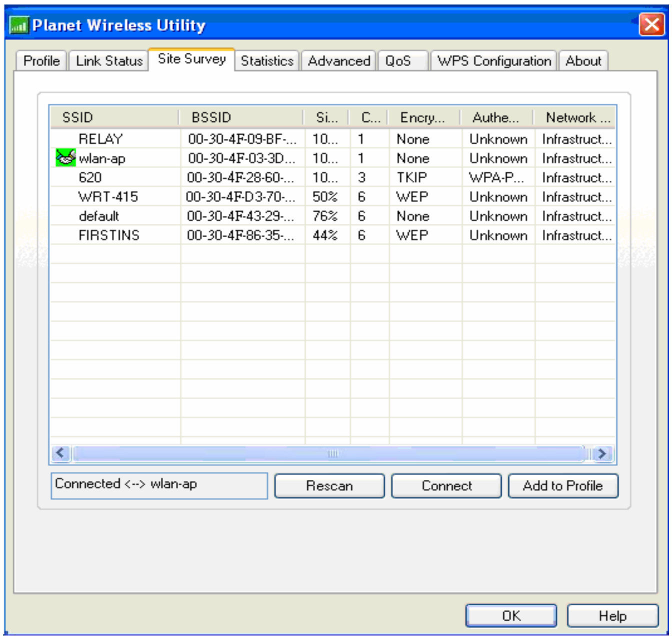
Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

PLANET WNL-U552

Click Finish to close the wizard.

7. The WNL-U552 utility will appear on the screen. Please select the AP you would like to connect and press “Connect” button to link it. Please click” OK” to continue.



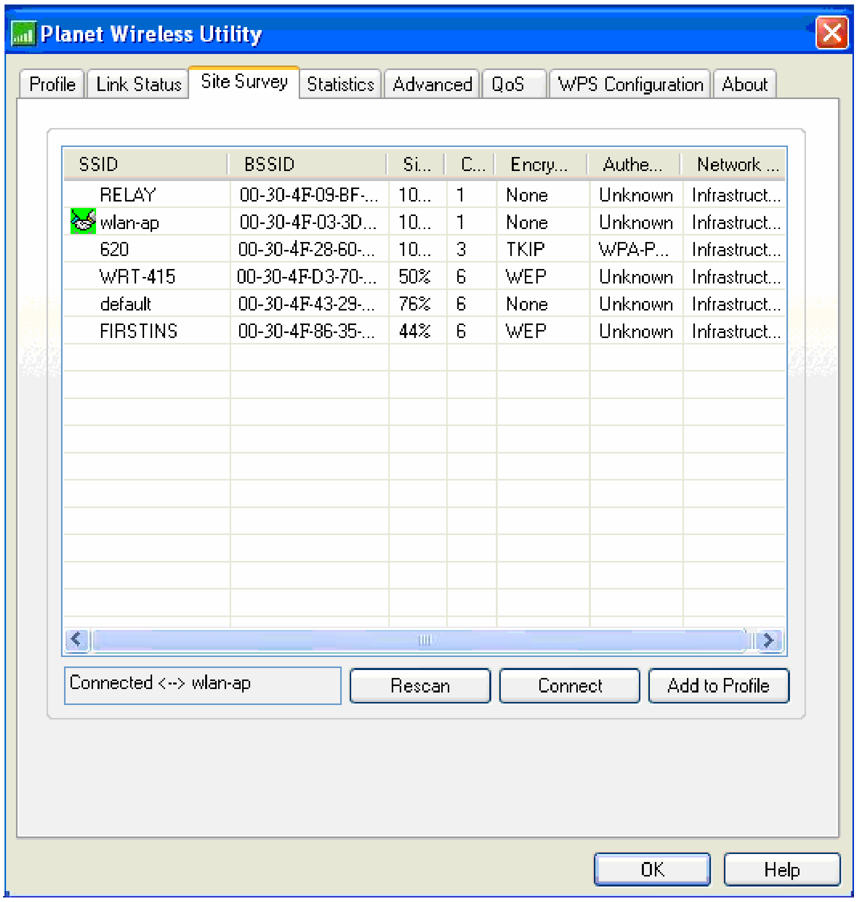
SSID	BSSID	Si...	C...	Encry...	Authe...	Network ...
RELAY	00-30-4F-09-BF-...	10...	1	None	Unknown	Infrastruct...
wlan-ap	00-30-4F-03-3D...	10...	1	None	Unknown	Infrastruct...
620	00-30-4F-28-60-...	10...	3	TKIP	WPA-P...	Infrastruct...
WRT-415	00-30-4F-D3-70-...	50%	6	WEP	Unknown	Infrastruct...
default	00-30-4F-43-29-...	76%	6	None	Unknown	Infrastruct...
FIRSTINS	00-30-4F-86-35-...	44%	6	WEP	Unknown	Infrastruct...

Connected <--> wlan-ap

Chapter 3 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the WNL-U552 and monitor the link status and the statistics during the communication process.

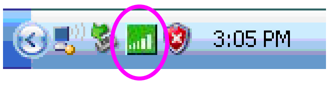
When the WNL-U552 is installed, the configuration utility will be displayed automatically. This card will auto connect to wireless device which has better signal strength and no wireless security setting.



SSID	BSSID	Si...	C...	Encry...	Authe...	Network ...
RELAY	00-30-4F-09-BF-...	10...	1	None	Unknown	Infrastruct...
wlan-ap	00-30-4F-03-3D...	10...	1	None	Unknown	Infrastruct...
620	00-30-4F-28-60-...	10...	3	TKIP	WPA-P...	Infrastruct...
WRT-415	00-30-4F-D3-70-...	50%	6	WEP	Unknown	Infrastruct...
default	00-30-4F-43-29-...	76%	6	None	Unknown	Infrastruct...
FIRSTINS	00-30-4F-86-35-...	44%	6	WEP	Unknown	Infrastruct...

Connected <--> wlan-ap

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 PLANET WNL-U552 Utilities**

  Select “Lauch PLANET WNL-U552 Utilities” to open the Configuration Utility tool.

- **Use Zero Configuration as Configuration Utility**

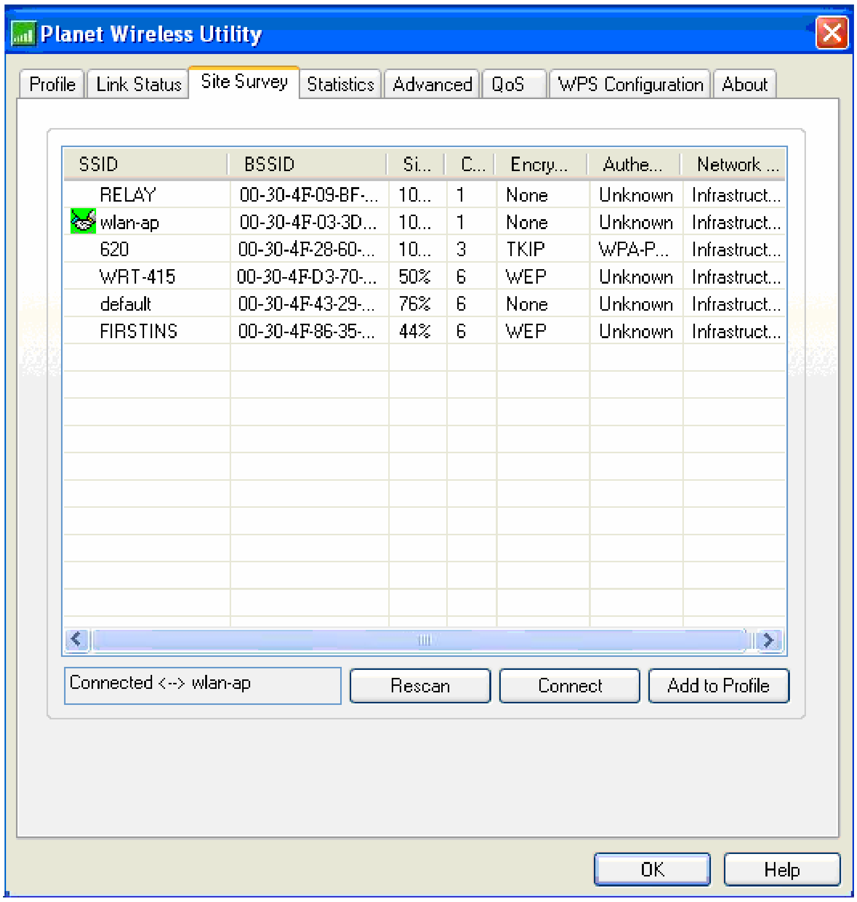
  Select “Use Zero Configuration as Configuration Utility” to use Windows XP built-in wireless configuration utility (Windows Zero Configuration) to configure the card.

- **Exit**

Select “Exit” to close the Configuration Utility tool.

3.1 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your card and automatically connect to the wireless device with the highest signal strength. From the “Site Survey”, 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.



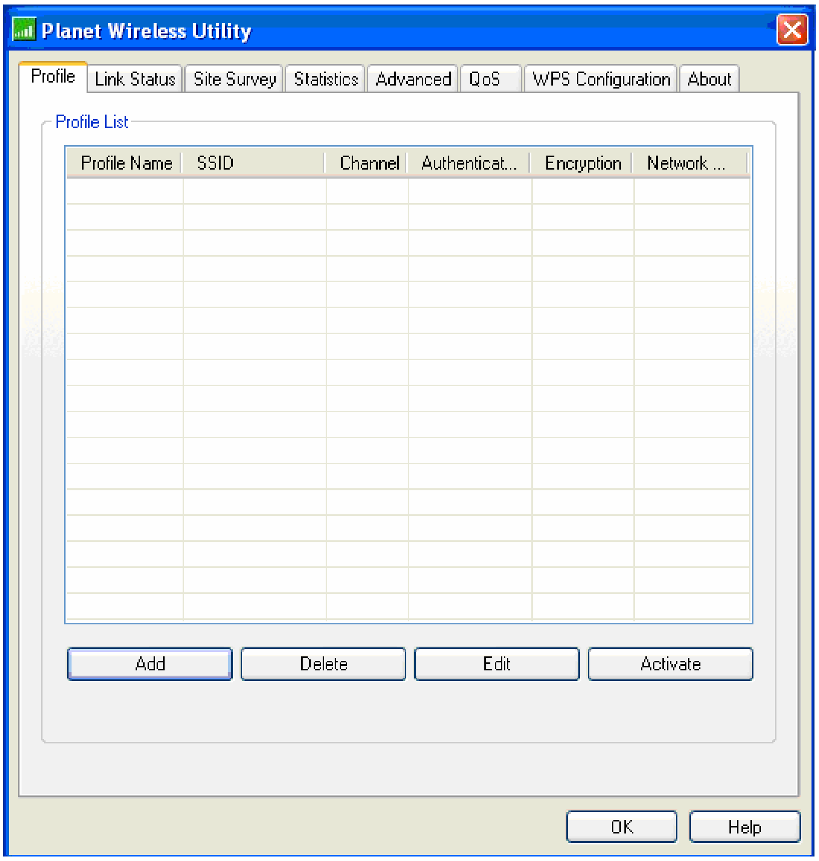
SSID	BSSID	Si...	C...	Encry...	Authe...	Network ...
RELAY	00-30-4F-09-BF-...	10...	1	None	Unknown	Infrastruct...
wlan-ap	00-30-4F-03-3D...	10...	1	None	Unknown	Infrastruct...
620	00-30-4F-28-60-...	10...	3	TKIP	WPA-P...	Infrastruct...
WRT-415	00-30-4F-D3-70-...	50%	6	WEP	Unknown	Infrastruct...
default	00-30-4F-43-29-...	76%	6	None	Unknown	Infrastruct...
FIRSTINS	00-30-4F-86-35-...	44%	6	WEP	Unknown	Infrastruct...

Connected <--> wlan-ap

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.

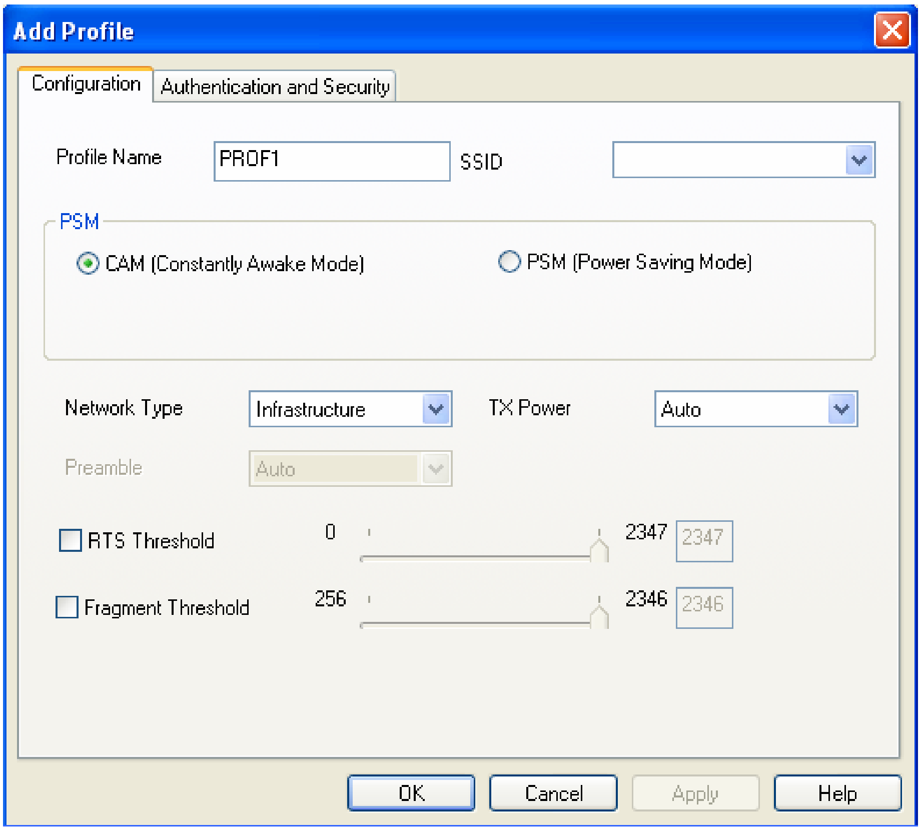
3.2 Profile

The “Profiles List” is for you to manage the networks you connect to frequently. You are able to Add/Delete/Edit/Activate a profile.



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.

3.2.1 Add Profile - Configuration



Profile Name PROF1

SSID

PSM

● CAM (Constantly Awake Mode) ○ PSM (Power Saving Mode)

Network Type Infrastructure

TX Power Auto

Preamble Auto

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346

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.

TX Power

If you want to lower the transmit power of the card for saving the power of the system, you can select the lower percentages from the list. The lower power will cause the lower signal strength and the coverage range.

Ad Hoc Wireless Mode

When the card is set in Ad Hoc (Peer to Peer Mode), you can designate the wireless connection mode for the Ad Hoc network.

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.

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. This mode is also the default setting.

802.11 G only – This card can be compatible with both 802.11g and 802.11b wireless stations. If there are only 802.11g wireless stations in the network, you can set the card to this mode.

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

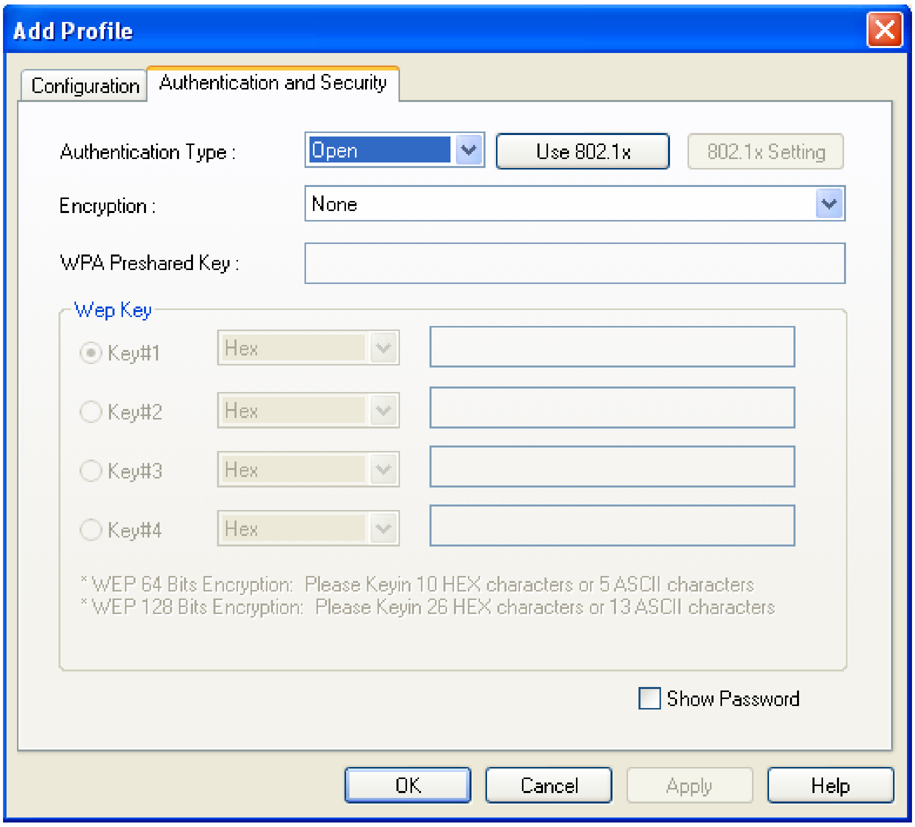
Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2347 bytes. Minor change is recommended.

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.

Channel	This setting is only available for Ad Hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same with the network you are connecting to.

3.2.2 Add Profile - Authentication and Security



Authentication Type : Open

Encryption : None

WPA Preshared Key :

○ Key#1 ○ Key#2 ○ Key#3 ○ Key#4

* 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

□ Show Password

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.
Authentication Type	**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. When you have set up LEAP authentication, you have to enter the user name and password of your computer.

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).

802.1x Setting

When you have set the Authentication Type to Open, Shared, WPA or WPA2, you can also enable IEEE 802.1x setting to use the authentication server or certification server to authenticate client users.

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”.

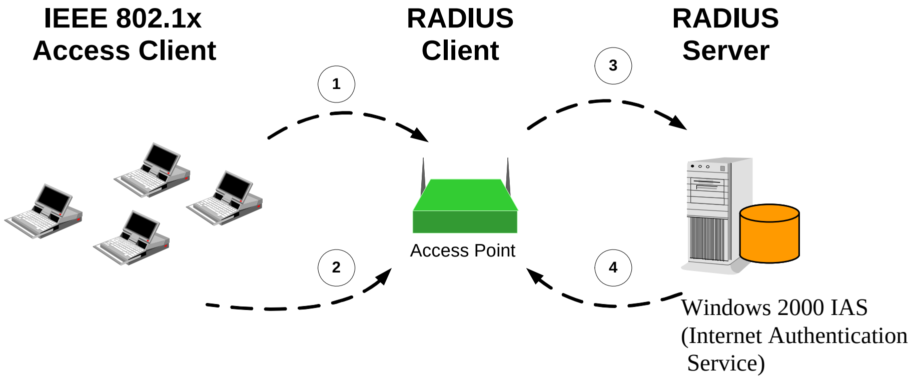
128-bit – Input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 13-digit ASCII characters (including “a-z” and “0-9”) as the encryption keys. For example: “01234567890123456789abcdef“ or “administrator”.

3.2.2.1 802.1x Setting - Certification

The IEEE 802.1X specification describes a protocol that can be used for authenticating both clients and servers on a network. The authentication algorithms and methods are those provided by the Extensible Authentication Protocol (EAP), a method of authentication that has been in use for a number of years on networks that provide Point-to-Point Protocol (PPP) support as many internet service providers and enterprises do.

When an AP acting as an authenticator detects a wireless station on the LAN, it sends an EAP-Request for the user's identity to the device. (EAP, or the Extensible Authentication Protocol, is an authentication protocol that runs before network layer protocols transmit data over the link.) In turn, the device responds with its identity, and the AP relays this identity to an authentication server, which is typically an external RADIUS server.

An example for MD5 Authentication

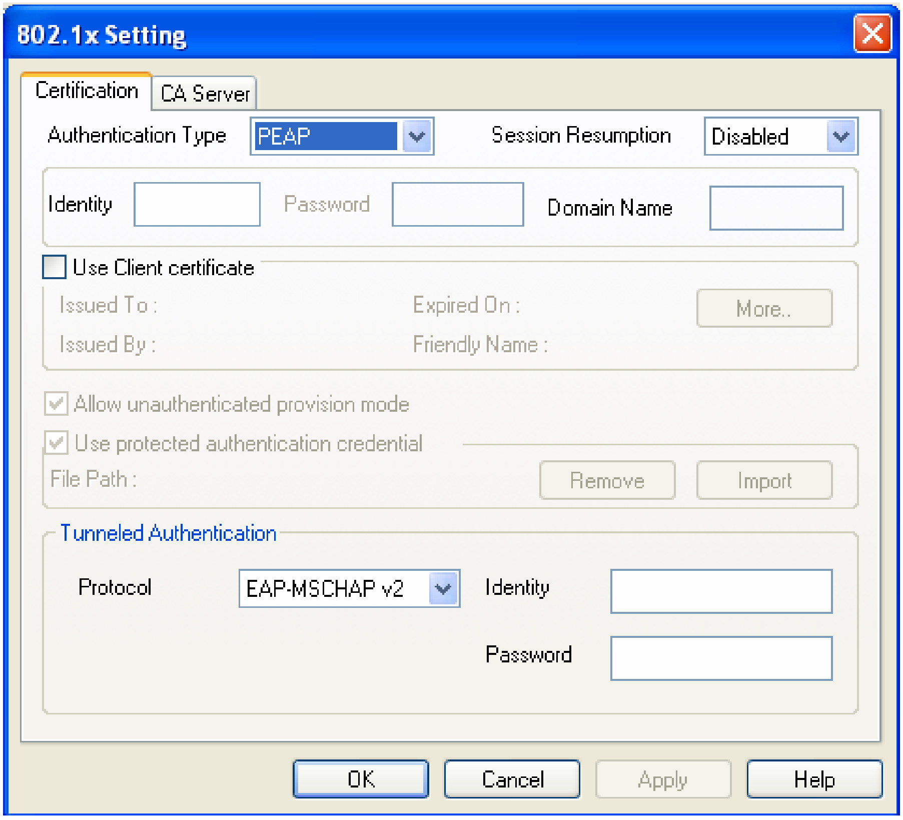


(1) Client requests to login the network.

(2) Login with username, password.

(3) Send username, password to RADIUS server.

(4) Approve or deny user login to the LAN.


802.1x Setting

Certification | CA Server

Authentication Type: PEAP

Session Resumption: Disabled

Identity:

Password:

Domain Name:

□ Use Client certificate

Issued To :

Expired On :

Issued By :

Friendly Name :

☑ Allow unauthenticated provision mode

☑ Use protected authentication credential

File Path :

Tunneled Authentication

Protocol: EAP-MSCHAP v2

Identity:

Password:

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.

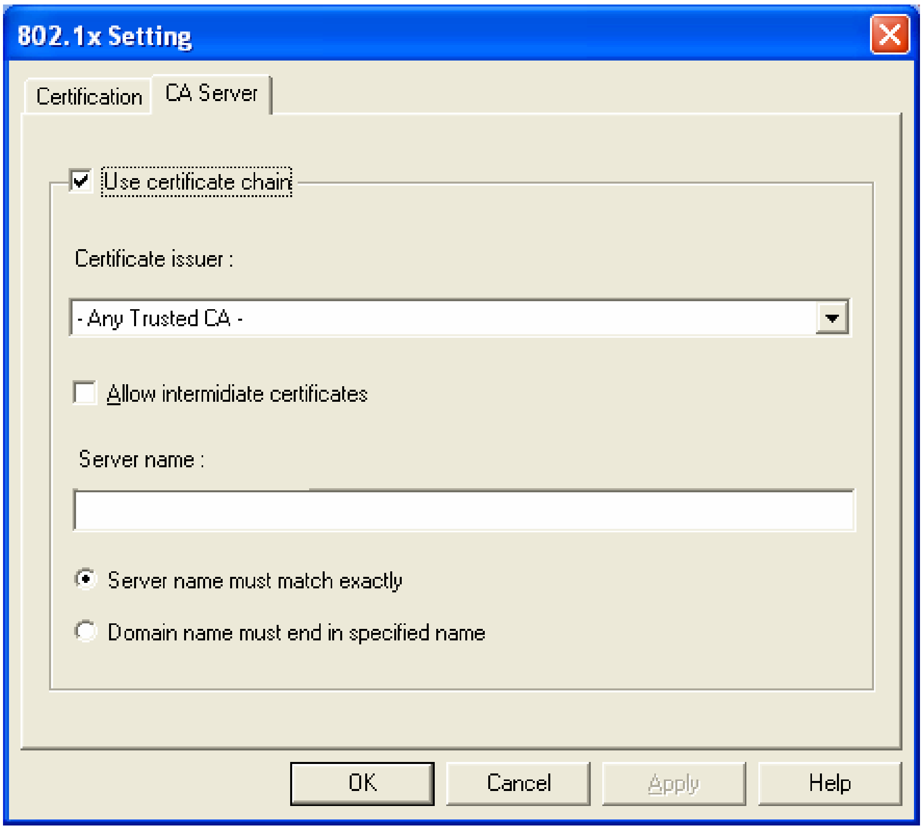
Identity

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.

3.2.2.2 802.1x Setting - CA Server



☑ Use certificate chain

Certificate issuer :

- Any Trusted CA -

□ Allow intermidiate certificates

Server name :

● Server name must match exactly

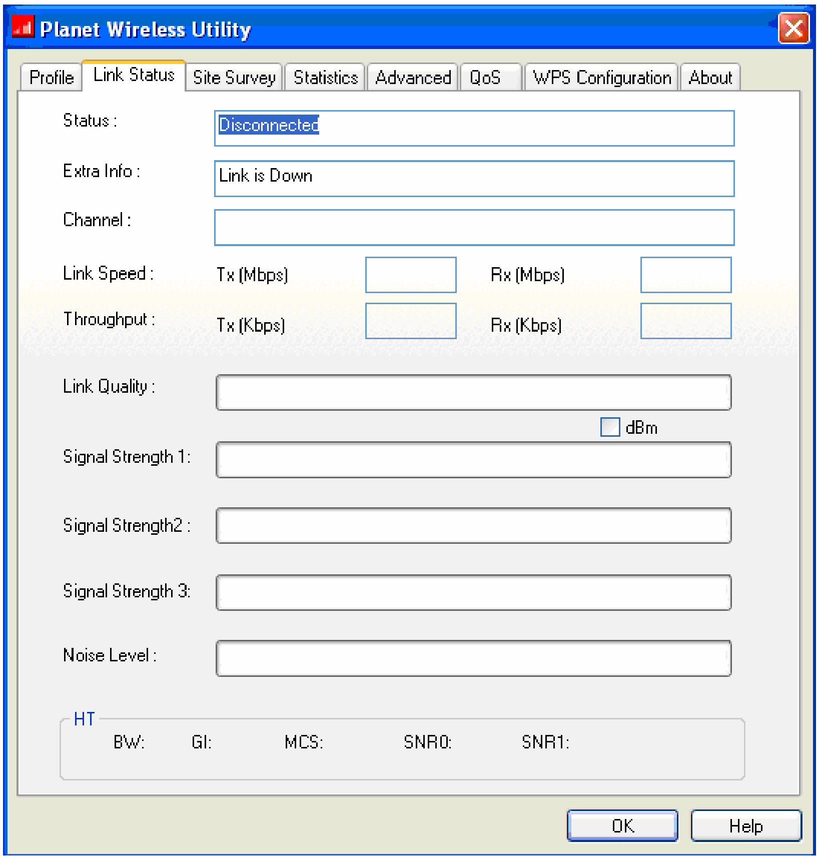
○ Domain name must end in specified name

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.

3.3 Link Status

From the “Link Status” option, you can view all the information of the network you are connecting to.



Status : Disconnected

Extra Info : Link is Down

Channel :

Link Speed : Tx (Mbps) Rx (Mbps)

Throughput : Tx (Kbps) Rx (Kbps)

Link Quality :

□ dBm

Signal Strength 1:

Signal Strength2 :

Signal Strength 3:

Noise Level :

HT

BW: GI: MCS: SNR0: SNR1:

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. The maximum transmission rate is 54Mbps.

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

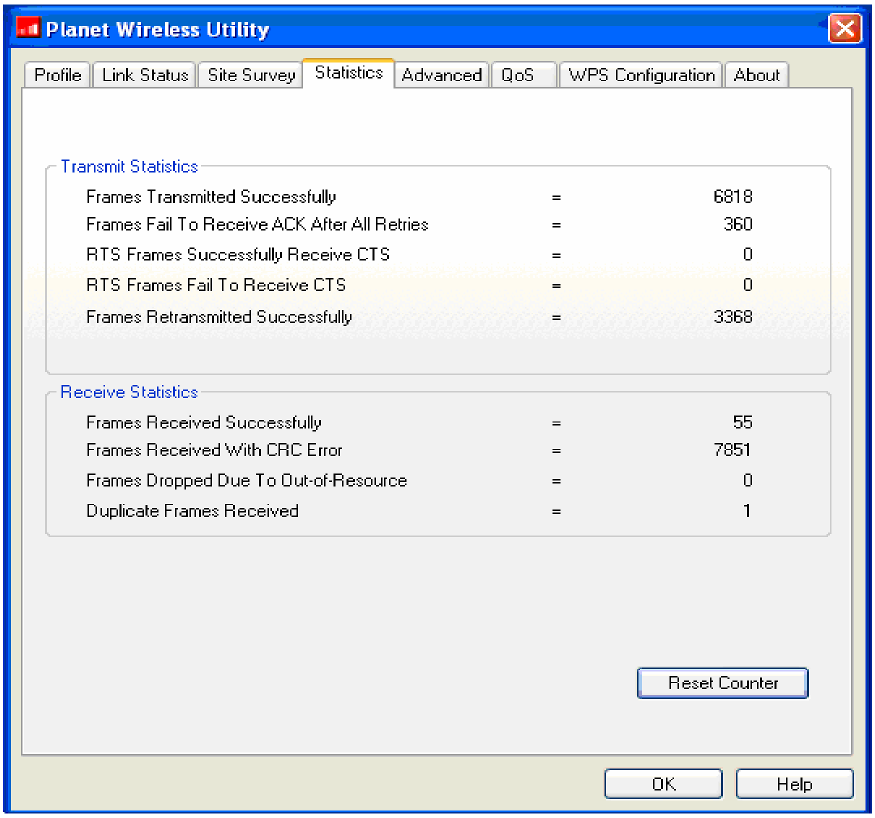
This bar shows the signal strength level. The higher percentage shown in the bar, the more radio signal been received by the card. This indicator helps to find the proper position of the wireless device for quality network operation.

Noise Level

Display the noise level in the wireless environment.

3.4 Statistics

This option enables you to view the statistic information of the connection including transmit statistics and receive statistics. You may reset the counters by clicking”Reset Counter”.



Transmit Statistics

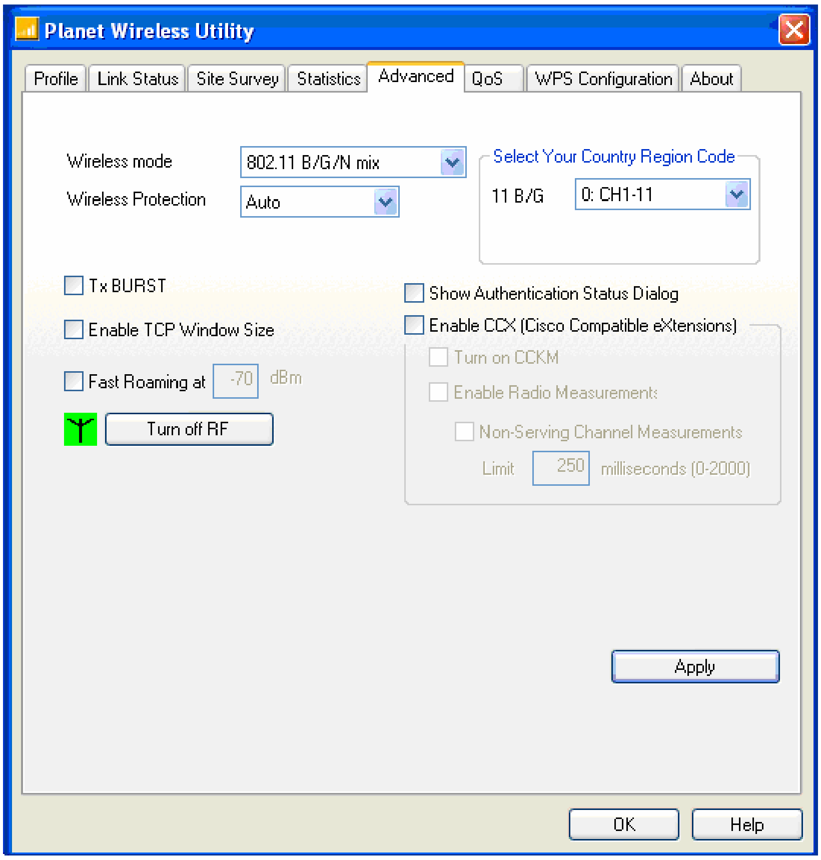
Frames Transmitted Successfully = 6818
Frames Fail To Receive ACK After All Retries = 360
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Frames Retransmitted Successfully = 3368

Receive Statistics

Frames Received Successfully = 55
Frames Received With CRC Error = 7851
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 1

3.5 Advance

This option enables you to configure more advanced settings, for example: wireless mode, protection mode and etc.



Planet Wireless Utility

Wireless mode: 802.11 B/G/N mix

Wireless Protection: Auto

Select Your Country Region Code

11 B/G: 0: CH1-11

□ Tx BURST

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements

Limit 250 milliseconds (0-2000)

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.
Select Your Country Region Code	The available channel differs from different countries. For example: USA (FCC) is channel 1-11, Europe (ETSI) is channel 1-13. The operating frequency channel will be restricted to the country user located before

importing. If you are in different country, you have to adjust the channel setting to comply the regulation of the country.

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.

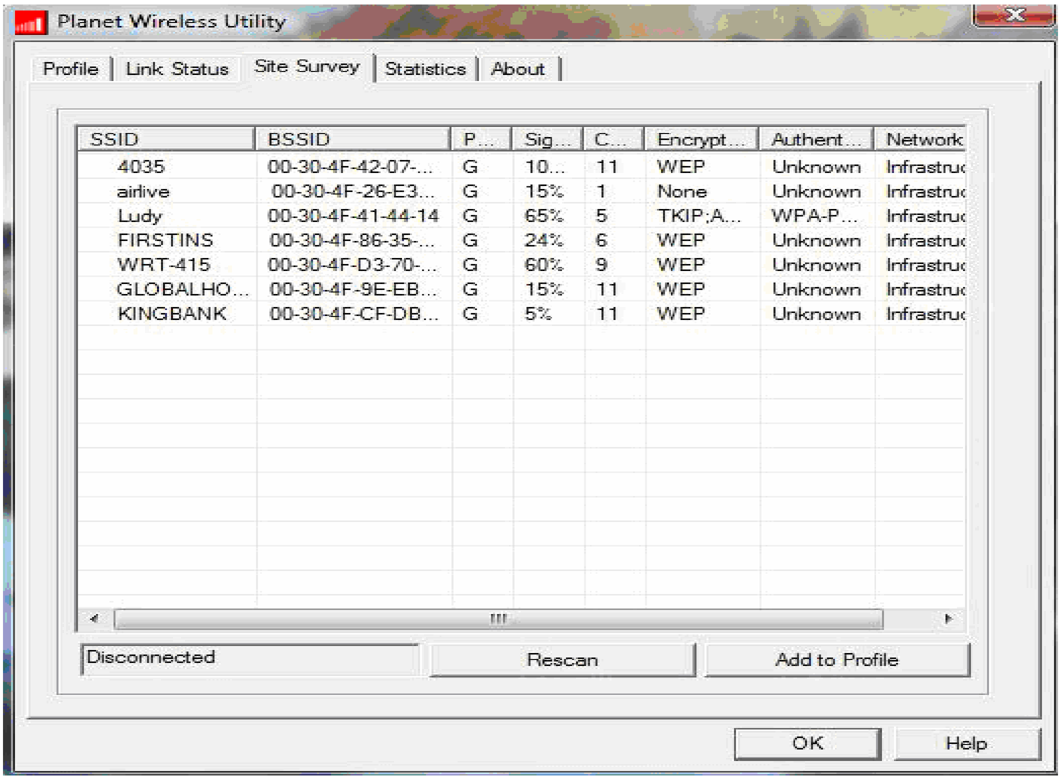
Non-Serving Channel Measurements

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.

Note: This function is not support in the OS of Windows VISTA.

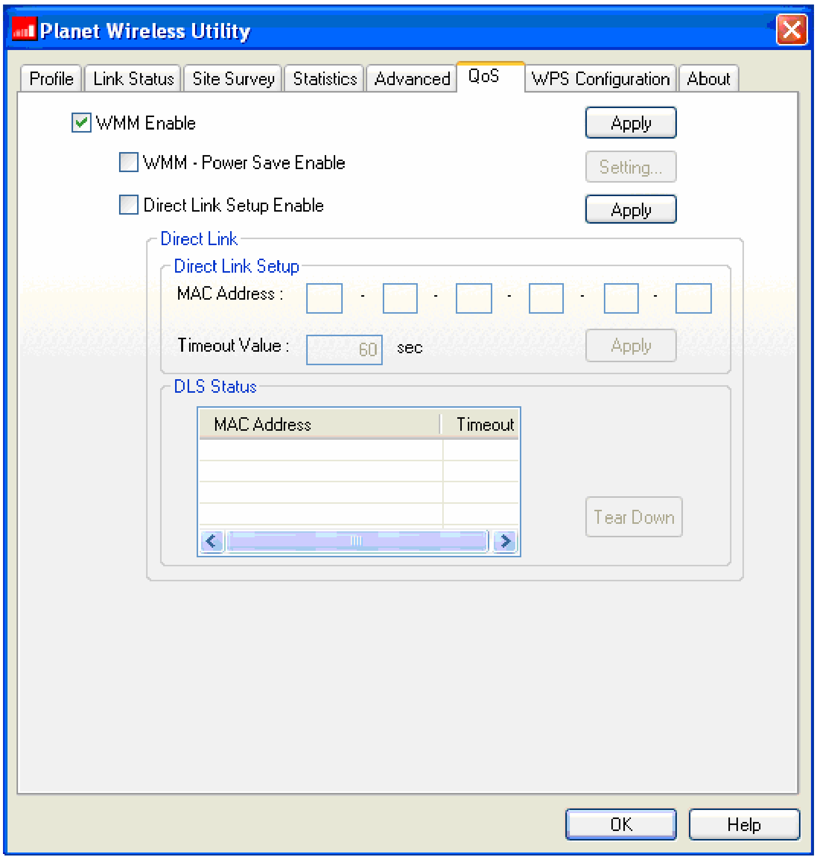


SSID	BSSID	P...	Sig...	C...	Encrypt...	Authent...	Network
4035	00-30-4F-42-07-...	G	10...	11	WEP	Unknown	Infrastruc
airlive	00-30-4F-26-E3...	G	15%	1	None	Unknown	Infrastruc
Ludy	00-30-4F-41-44-14	G	65%	5	TKIP;A...	WPA-P...	Infrastruc
FIRSTINS	00-30-4F-86-35-...	G	24%	6	WEP	Unknown	Infrastruc
WRT-415	00-30-4F-D3-70-...	G	60%	9	WEP	Unknown	Infrastruc
GLOBALHO...	00-30-4F-9E-EB...	G	15%	11	WEP	Unknown	Infrastruc
KINGBANK	00-30-4F-CF-DB...	G	5%	11	WEP	Unknown	Infrastruc

Disconnected

3.6 QoS

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.

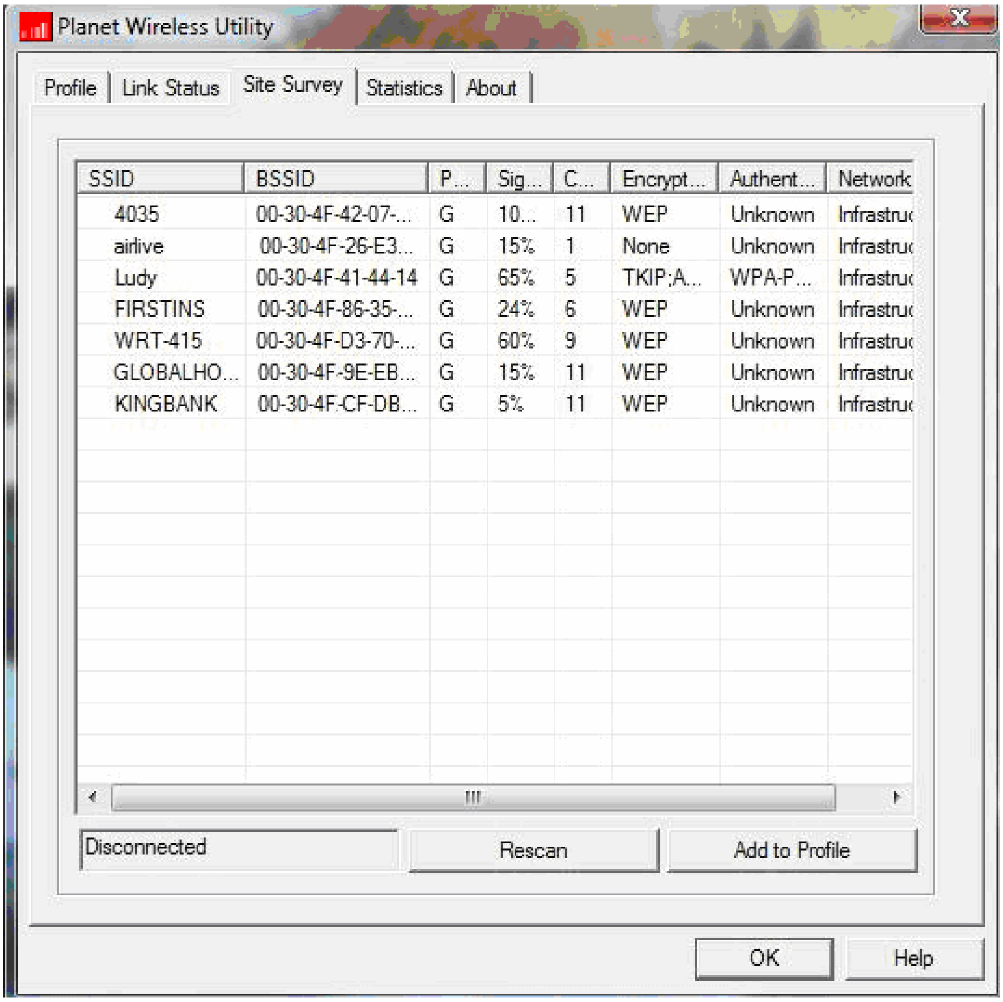
Timeout Value

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 is not support in the OS of Windows VISTA.



SSID	BSSID	P...	Sig...	C...	Encrypt...	Authent...	Network
4035	00-30-4F-42-07-...	G	10...	11	WEP	Unknown	Infrastruc
airlive	00-30-4F-26-E3...	G	15%	1	None	Unknown	Infrastruc
Ludy	00-30-4F-41-44-14	G	65%	5	TKIP;A...	WPA-P...	Infrastruc
FIRSTINS	00-30-4F-86-35-...	G	24%	6	WEP	Unknown	Infrastruc
WRT-415	00-30-4F-D3-70-...	G	60%	9	WEP	Unknown	Infrastruc
GLOBALHO...	00-30-4F-9E-EB...	G	15%	11	WEP	Unknown	Infrastruc
KINGBANK	00-30-4F-CF-DB...	G	5%	11	WEP	Unknown	Infrastruc

Disconnected

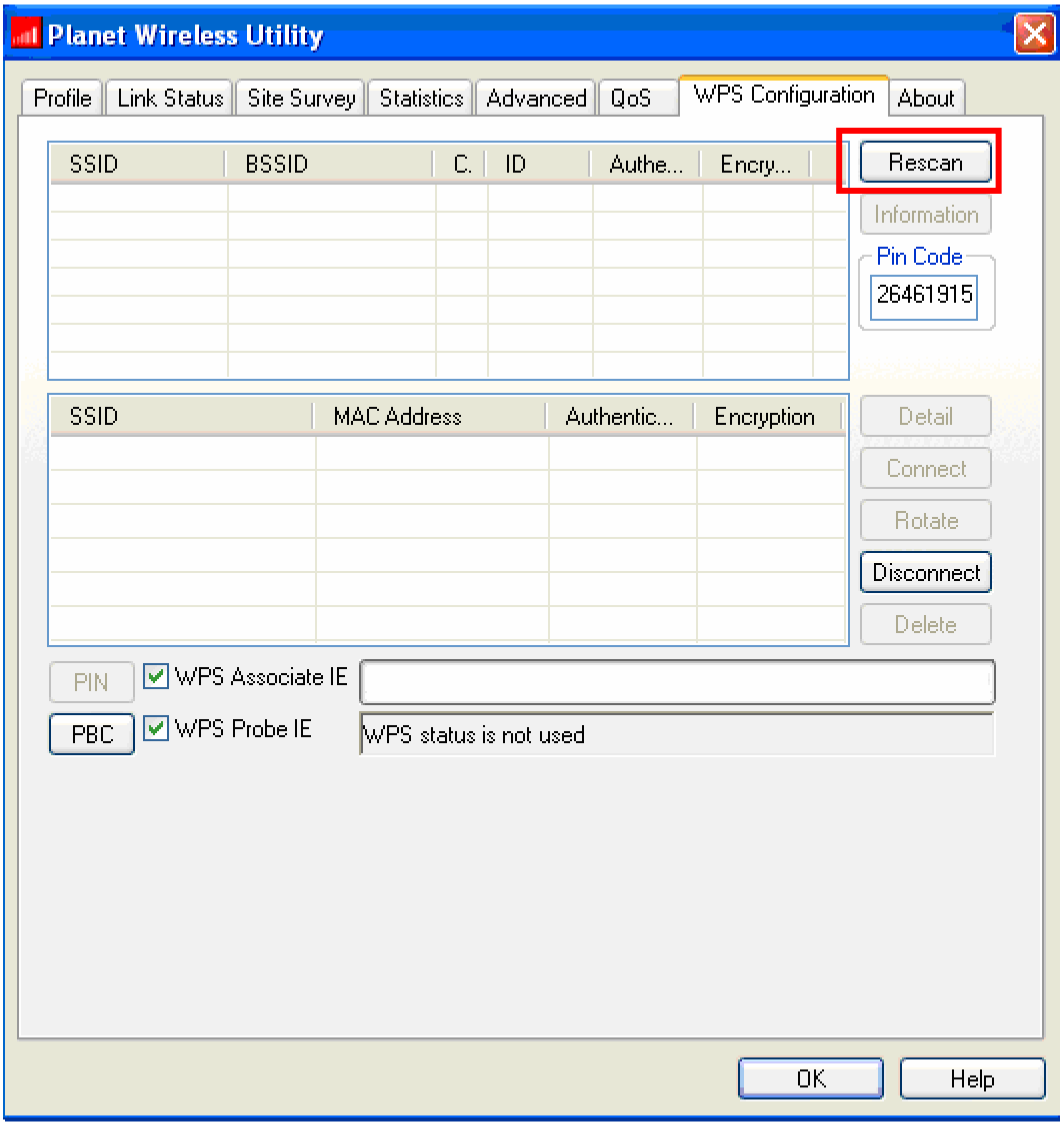
3.7 WPS Configuration

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!

For older wireless access points, it's possible to perform a firmware upgrade to become a WPS-enabled access point. Since they may not have a hardware button to press for WPS setup, you can use an alternative WPS setup method – input the pin code. Every WPS-compatible wireless network card comes with a unique WPS pin code; you can just input the code to wireless access point, and the wireless access point and wireless network card will do the rest for you.

This wireless network card 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:



Pin Code: 26461915

☑ WPS Associate IE

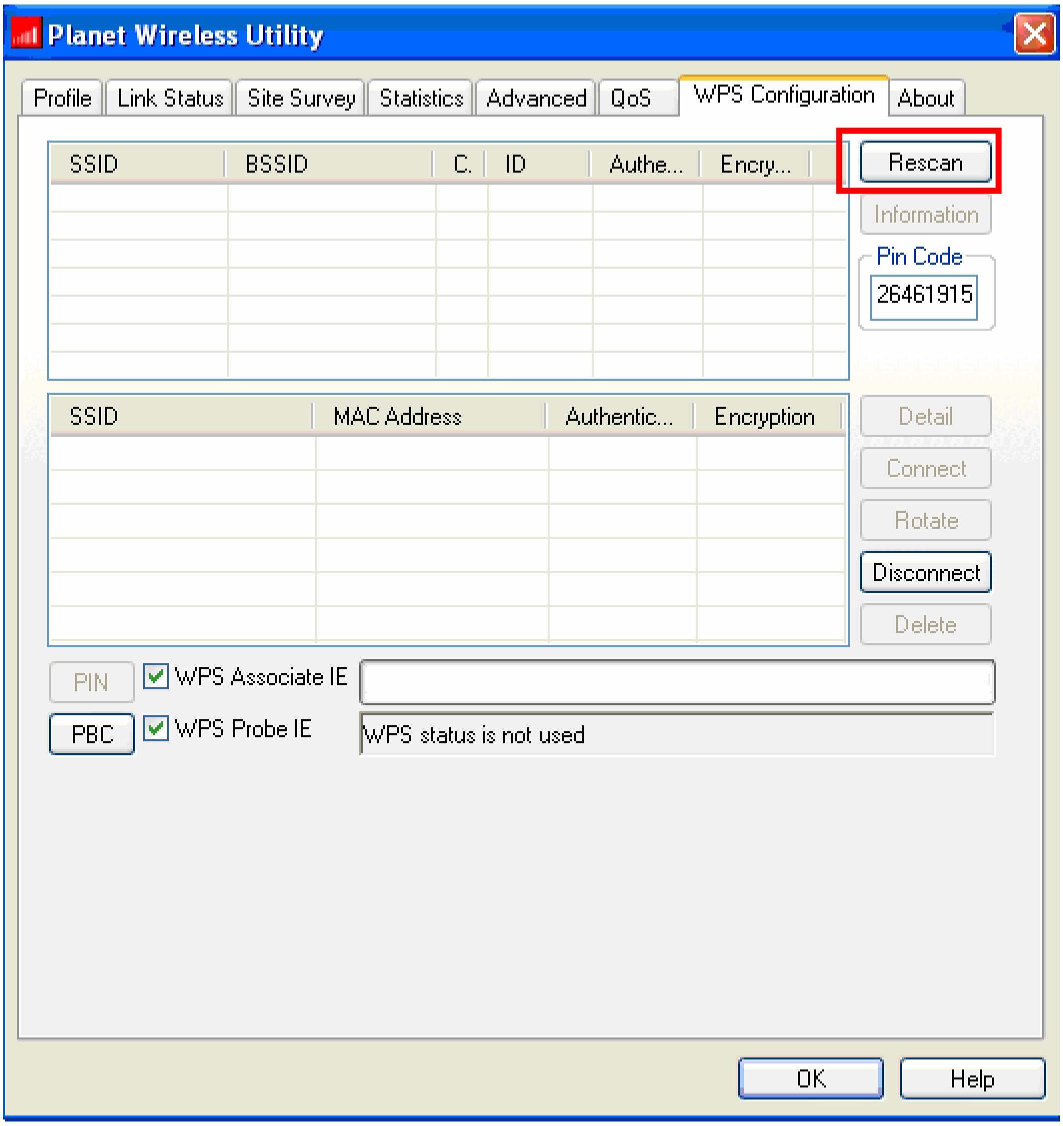
☑ WPS Probe IE

WPS status is not used

3.7.1 WPS Setup - PBC (Push-Button Configuration)

1. Push the ‘WPS’ button on your wireless access point (the button used to activate WPS standby mode), 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.



Pin Code: 26461915

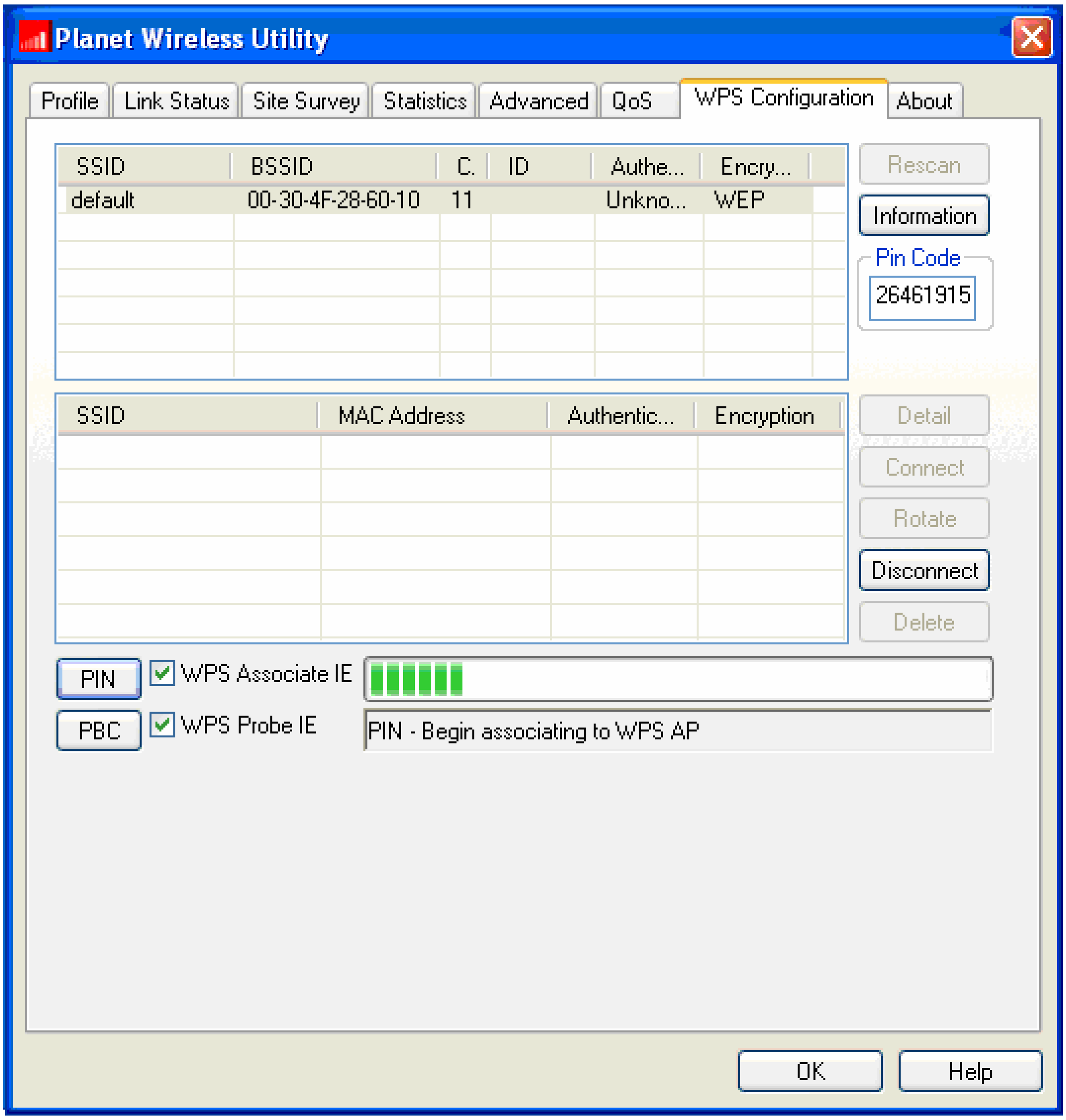
☑ WPS Associate IE

☑ WPS Probe IE

WPS status is not used

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.

5. 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, means the connection between your wireless network card and access point is successfully connected by WPS, and the information about access point you connected to will be displayed.



SSID	BSSID	C.	ID	Authe...	Encry...
default	00-30-4F-28-60-10	11		Unkno...	WEP

Pin Code: 26461915

SSID	MAC Address	Authentic...	Encryption

☑ WPS Associate IE

☑ WPS Probe IE

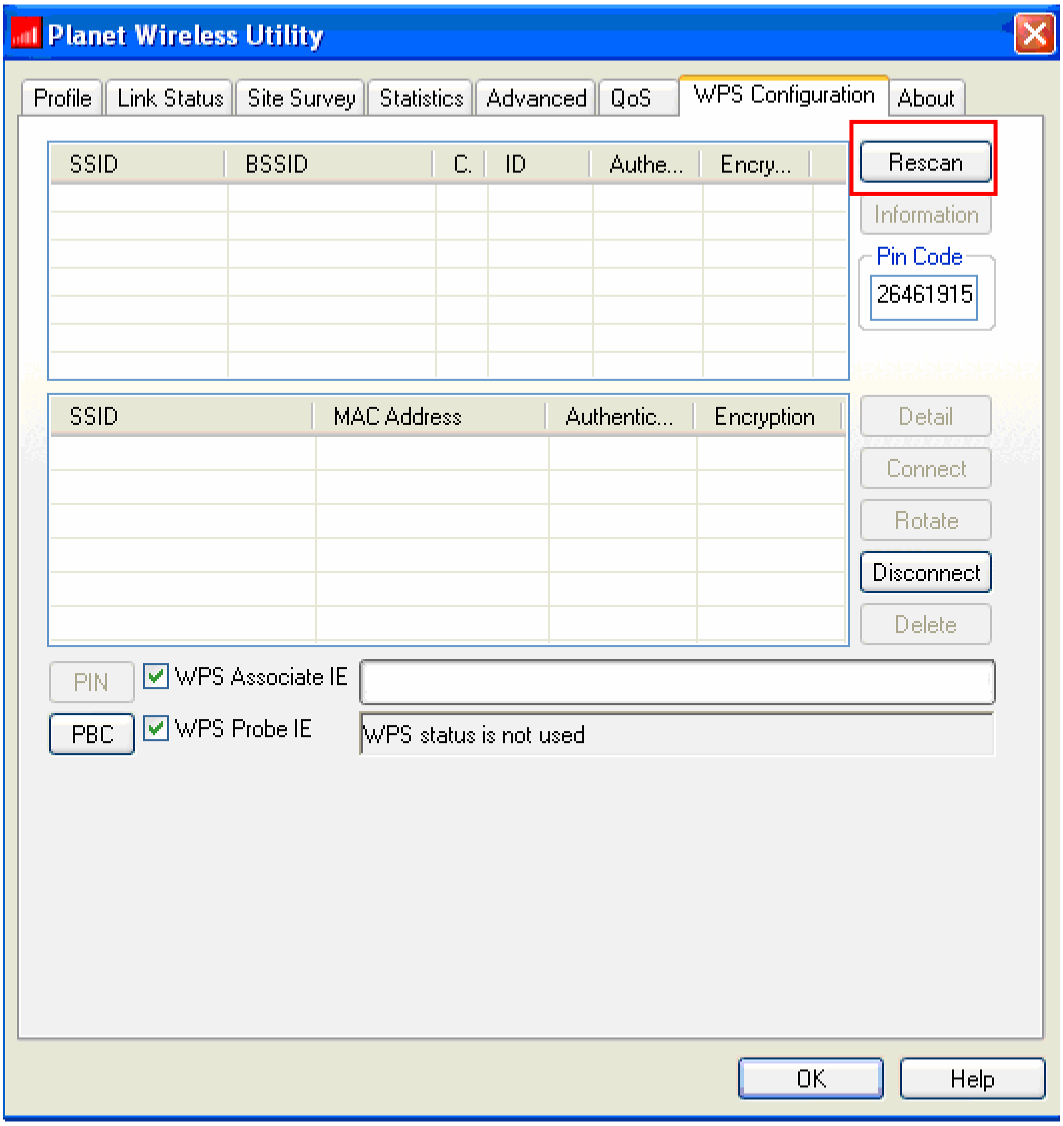
PIN - Begin associating to WPS AP

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.

3.7.2 WPS Setup - PIN

The PIN number of your wireless network card 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).



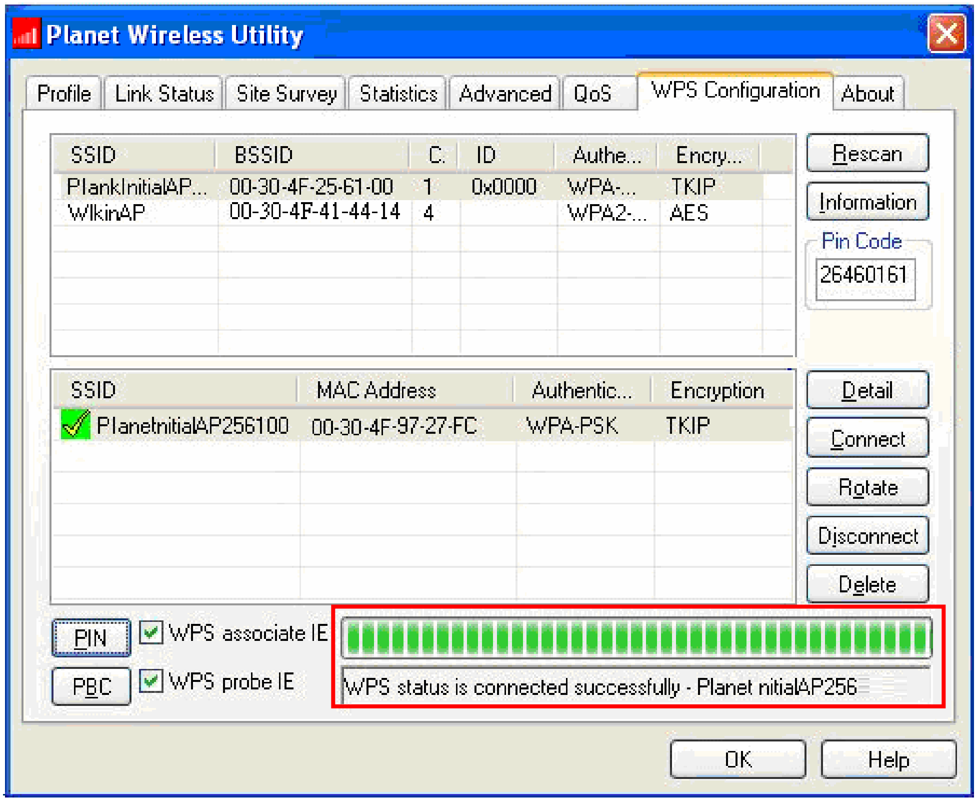
Pin Code: 26461915

☑ WPS Associate IE

☑ WPS Probe IE

WPS status is not used

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:



SSID	BSSID	C.	ID	Authe...	Encry...
PlankInitialAP...	00-30-4F-25-61-00	1	0x0000	WPA-...	TKIP
WlkinAP	00-30-4F-41-44-14	4		WPA2-...	AES

Pin Code: 26460161

SSID	MAC Address	Authentic...	Encryption
✓ PlanetnitialAP256100	00-30-4F-97-27-FC	WPA-PSK	TKIP

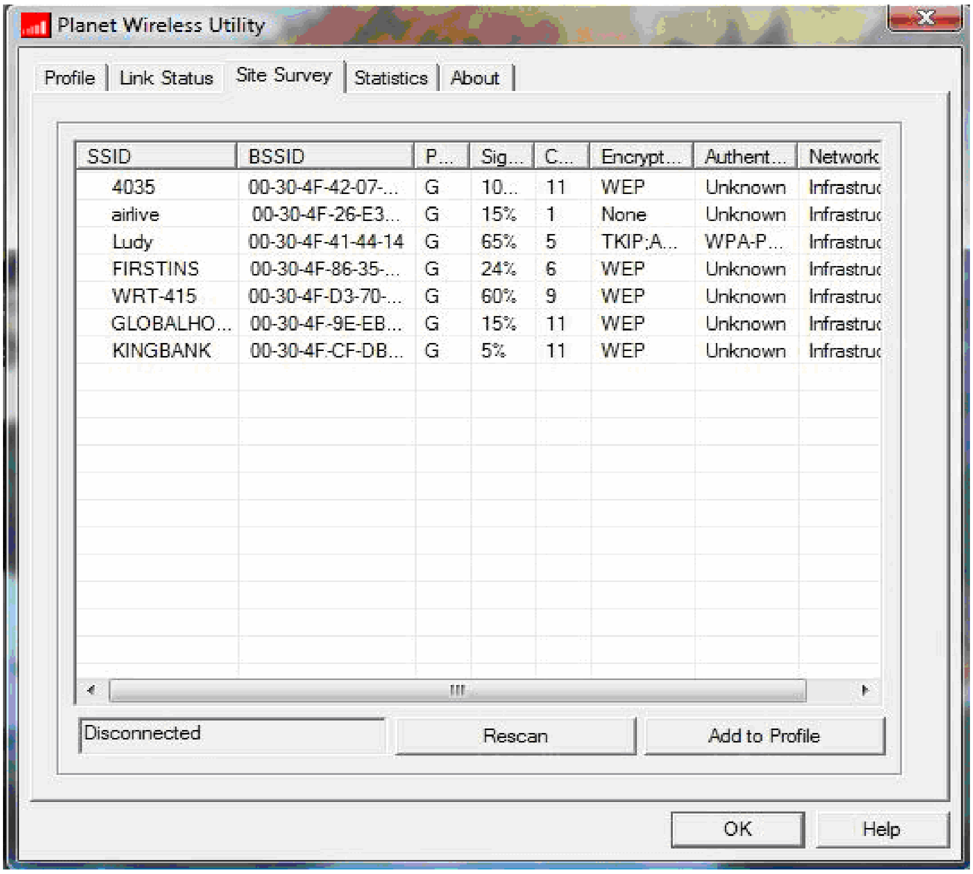
☑ WPS associate IE

☑ WPS probe IE

WPS status is connected successfully - Planet nitialAP256

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.

Note: This function is not support in the OS of Windows VISTA.

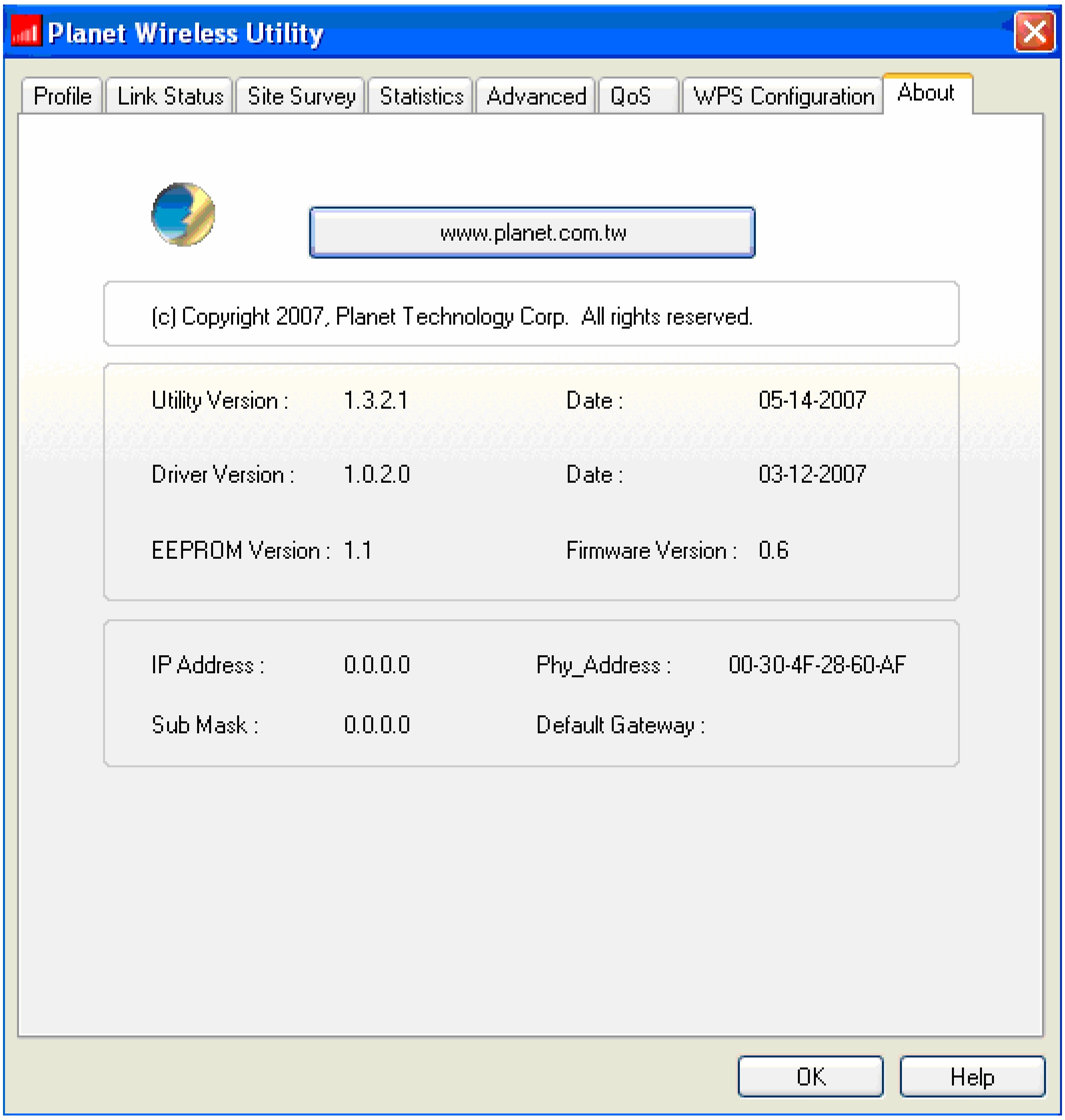


SSID	BSSID	P...	Sig...	C...	Encrypt...	Authent...	Network
4035	00-30-4F-42-07-...	G	10...	11	WEP	Unknown	Infrastruc
airlive	00-30-4F-26-E3...	G	15%	1	None	Unknown	Infrastruc
Ludy	00-30-4F-41-44-14	G	65%	5	TKIP;A...	WPA-P...	Infrastruc
FIRSTINS	00-30-4F-86-35-...	G	24%	6	WEP	Unknown	Infrastruc
WRT-415	00-30-4F-D3-70-...	G	60%	9	WEP	Unknown	Infrastruc
GLOBALHO...	00-30-4F-9E-EB...	G	15%	11	WEP	Unknown	Infrastruc
KINGBANK	00-30-4F-CF-DB...	G	5%	11	WEP	Unknown	Infrastruc

Disconnected

3.8 About

By choosing this option, you can click the hyperlink to connect the PLANET website. You can also obtain basic information about the WNL-U552 such as the Driver, Utility and EEPROM Version. The MAC Address of the card is displayed in the screen as well.



(c) Copyright 2007, Planet Technology Corp. All rights reserved.

Utility Version : 1.3.2.1 Date : 05-14-2007

Driver Version : 1.0.2.0 Date : 03-12-2007

EEPROM Version : 1.1 Firmware Version : 0.6

IP Address : 0.0.0.0 Phy_Address : 00-30-4F-28-60-AF

Sub Mask : 0.0.0.0 Default Gateway :

Chapter 4 Appendix

4.1 Troubleshooting

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

Q. The PLANET WNL-U552 does not work properly.

Ans.:

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.

Ans.:

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?

Ans.:

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 LED indicators on the wireless router are functioning properly. If not, check that the AC power and Ethernet cables are firmly connected.
3. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network.
4. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless clients and access points.
5. 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.

6. 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.

Ans.:

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'

Ans.:

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

Ans.:

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

Ans.:

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.

4.2 Glossary

1. **What is the IEEE 802.11g standard?**

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard？**

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support？**

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. **What is Ad-hoc？**

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. **What is Infrastructure？**

   An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. **What is BSS ID？**

   A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. **What is WEP？**

   WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. **What is TKIP?**

   TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. **What is AES?**

   AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. **Can Wireless products support printer sharing？**

    Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. **Would the information be intercepted while transmitting on air？**

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. **What is DSSS？What is FHSS？And what are their differences？**

    Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. 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.

15. 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.

16. 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.

17. 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.