

802.11n Wireless Mini-PCI Adapter

Manual

FCC Information

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 Communications Commission (FCC) Statement.

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

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

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Introduction

The 802.11n wireless mini-PCI adapter allows you to connect to your wireless networking. It provides more throughput rate on data communication than traditional 802.11g wireless adapters. With the built advanced wireless configuration utility, it let it more easily for you to surf your wireless LAN.

Features and Benefits

System

- Standard: IEEE 802.11b/g/n.
- Host Interface: mini-PCI.
- Data rate: 1, 2, 5.5, 11Mbps for 802.11b;
6, 9, 12, 18, 24, 36, 48, 54Mbps for 802.11g;
6, 6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 104, 117, 130Mbps for 802.11n.
- Operating range: Indoor, 30-100m; outdoor, 100-400m (depends on surrounding environment).

RF

- Frequency band: 2.400 ~ 2.4835 GHz (subject to local regulation).
- Modulation: OFDM(Orthogonal Frequency Division Multiplexing) for 802.11g/n; DSSS(Direct Sequence Spread Spectrum) for 802.11b.
- RF radiated output power: 16dBm for 802.11g/n; 18dBm for 802.11b. (± 1 dBm).

Software

- Driver: Microsoft Windows 2000, XP, XP64, and Vista.
- Operation mode: Infrastructure mode (Seamless roaming supported), Ad-Hoc mode (peer to peer connection).
- Security: 64/128 bit WEP encryption, WPA, WPA-PSK, WPA2, WPA2-PSK, and 802.1x.

LEDs and Physical connections

- Link: external.
- Activity: external.
- Antenna: external.

Package Contents

- Wireless adapter.
- Manual
- Quick installation guide
- CD: includes adapter drivers, manual, and quick installation guide.

**** If any of the above items are missing, please contact your reseller.**

System Requirements

Before installing the adapter and related software, make sure your system meets the minimum requirements described below.

IBM compatible desktop or notebook PC with available mini-PCI container.

- CPU level: no restricted.
- Memory size: no restricted.
- CDROM drive: no restricted.
- Operation system: Microsoft Windows 2000, XP, XP64, or Vista.


Installation


- Insert the Product CD into the CD-ROM drive.
- Execute “Setup.exe” in the root directory of the CD, it will guide you to install the Driver and Utility.
- Insert the wireless adapter into the mini-PCI container.

Management

Load up utility

After the installation, one utility will be run and minimized on Windows system tray bar.

 : Indicate wireless adapter detected, and connected to one site.

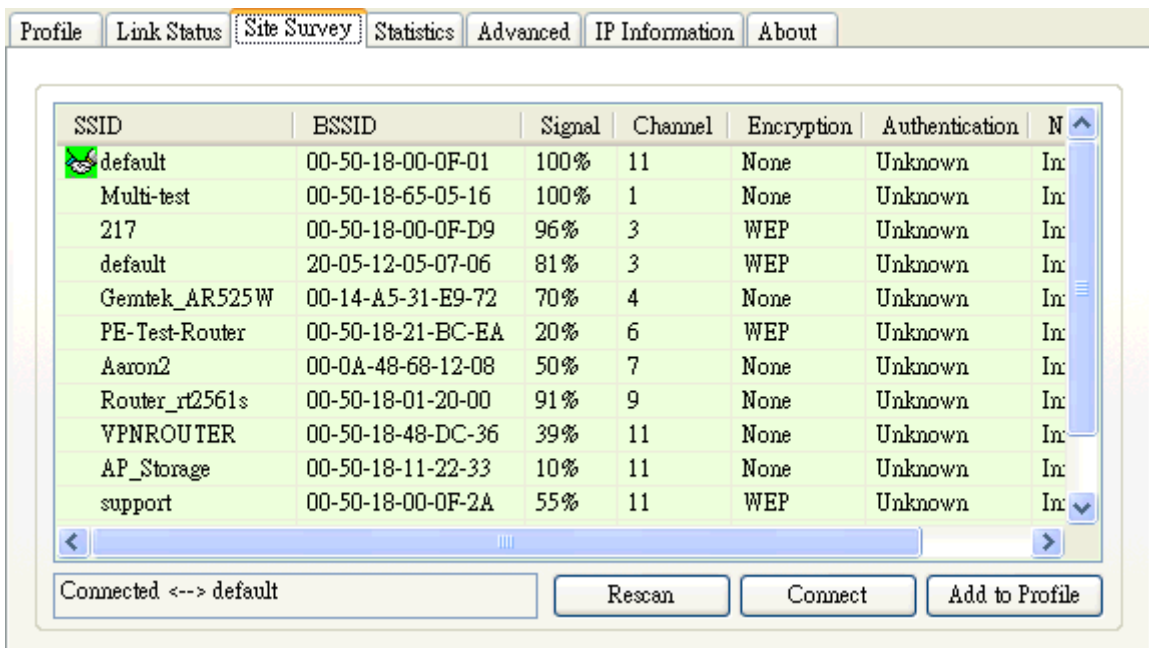
 : Indicated wireless adapter not detected, or not connected to one site.


You may double click it to bring up the main menu. You may also use mouse right button to launch or to close it. For Windows XP, the utility provides one option to manage the wireless adapter with Windows Zero Configuration.

Launch Utility
Use Windows Zero Configuration
Exit

Site Survey Page

Under the site survey page, system will display the information of surrounding APs from last scan result. List information include SSID, BSSID, Signal, Channel, Encryption algorithm, and Network type.



| SSID | BSSID | Signal | Channel | Encryption | Authentication | N |
|---|-------------------|--------|---------|------------|----------------|----|
|  default | 00-50-18-00-0F-01 | 100% | 11 | None | Unknown | In |
| Multi-test | 00-50-18-65-05-16 | 100% | 1 | None | Unknown | In |
| 217 | 00-50-18-00-0F-D9 | 96% | 3 | WEP | Unknown | In |
| default | 20-05-12-05-07-06 | 81% | 3 | WEP | Unknown | In |
| Gemtek_AR525W | 00-14-A5-31-E9-72 | 70% | 4 | None | Unknown | In |
| PE-Test-Router | 00-50-18-21-BC-EA | 20% | 6 | WEP | Unknown | In |
| Aaron2 | 00-0A-48-68-12-08 | 50% | 7 | None | Unknown | In |
| Router_rt2561s | 00-50-18-01-20-00 | 91% | 9 | None | Unknown | In |
| VPNROUTER | 00-50-18-48-DC-36 | 39% | 11 | None | Unknown | In |
| AP_Storage | 00-50-18-11-22-33 | 10% | 11 | None | Unknown | In |
| support | 00-50-18-00-0F-2A | 55% | 11 | WEP | Unknown | In |

Connected <--> default Rescan Connect Add to Profile

Definition of each field

- SSID: Name of BSS or IBSS network.
- BSSID: MAC address of AP or randomly generated of IBSS.
- Signal: Receive signal strength of specified network.
- Channel: Channel in use.
- Encryption: Encryption algorithm used within than BSS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.
- Authentication: Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.
- Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.

Connected network

When utility first ran, it will select the best AP to connect automatically. It is available to connect to other site by double click the intended item. If the intended network has encryption other than " Not Use " or "Unknown", the security page will pop up for you to setup the appropriate information to make the connection.

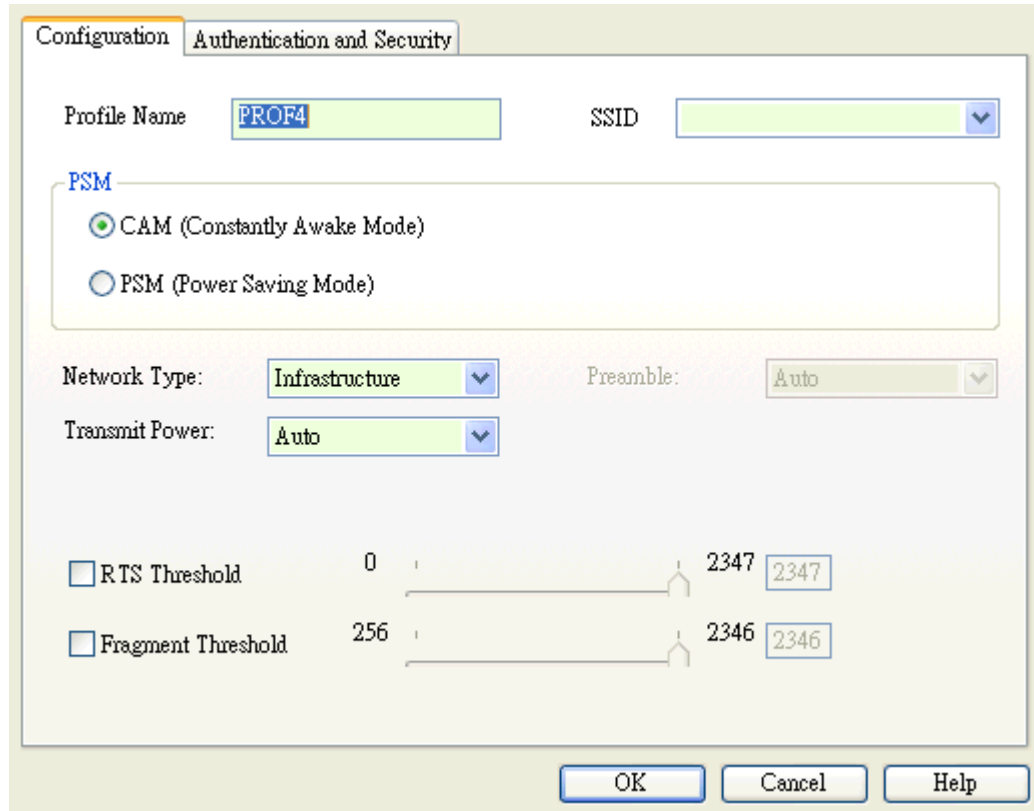


This icon indicates the change is successful.

- Connection box: Indicate connection status, the connected network SSID will show up here.
- Rescan: Issue an rescan command to wireless NIC to update information on surrounding wireless network.
- Connect: Command to connect to the selected network.
- Add to Profile: Add the selected AP to profile setting. It will bring up profile page and save the setting to a new profile.

Add/Edit Profile

System Configuration



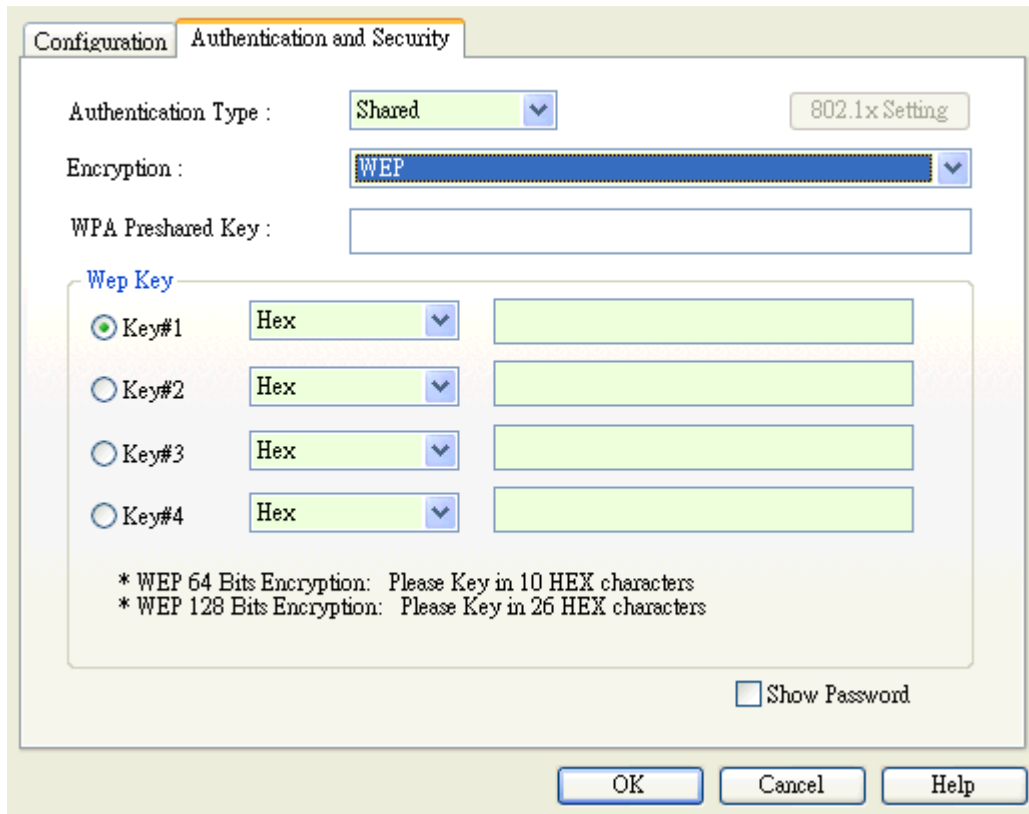
- Profile Name: User chose name for this profile.
- SSID: User can key in the intended SSID name or use pull down menu to select from available APs.
- Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode. There is a check box for CAM when AC power. When this is checked, the wireless NIC will stay full power when AC power cord is plug into power outlet.
- Network Type: There are two types, infrastructure and 802.11 ad-hoc modes. Under ad-hoc mode, user can also choose the preamble type; the available preamble type includes short and long. In addition to that, the channel and Ad hoc wireless mode field will be available for setup in ad-hoc mode.
- TX Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. User can choose power value by sliding the bar.
- Preamble: There are three types, Auto, Long and Short are supported.
- Ad hoc wireless mode: 802.11b only, 802.11b/g mixed and 802.11g only modes are supported.
- RTS Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
- Fragment Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2346.
- Channel: Only available for setting under ad-hoc mode. User can choose the channel frequency to start their ad-hoc network.

Profile function is based on the needs to set up the most linkable AP in order to record the system configuration and to

set up the authentication security. The function of each session is shown below

Authentication & Security

When the Encryption feature is enabled, the other setups are same as the WEP setting.



- Authentication Type: There are three type of authentication modes supported. They are open, Shared, WPA-PSK and WPA system.
- 802.1x Setting: It will display to set when user use radius server to authenticate client certificate for WPA authentication mode.
- Encryption Type: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
- WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.
- WEP Key: Only valid when using WEP encryption algorithm. The key must matched AP key. There are several formats to enter the keys.
 - Hexadecimal, 40bits : 10 Hex characters.
 - Hexadecimal, 128bits : 32Hex characters.
 - ASCII, 40bits : 5 ASCII characters.
 - ASCII, 128bits : 13 ASCII characters.

802.1x Setting

The screenshot shows the 'CA Server' configuration window. It has two tabs: 'Certification' and 'CA Server'. The 'CA Server' tab is active. The window contains the following fields and options:

- Authentication Type:** A dropdown menu set to 'PEAP'.
- Session Resumption:** A dropdown menu set to 'Disabled'.
- Identity:** A text input field.
- Password:** A text input field.
- Use Client certificate**
- Issued To:** A text input field.
- Issued By:** A text input field.
- Expired On:** A text input field.
- Friendly Name:** A text input field.
- More...** A button.
- Tunneled Authentication** (Section Header)
- Protocol:** A dropdown menu set to 'EAP-MSCHAP v2'.
- Identity:** A text input field.
- Password:** A text input field.

802.1x is a authentication for 『WPA』 and 『WPA2』 certificate to server.

- Authentication type:

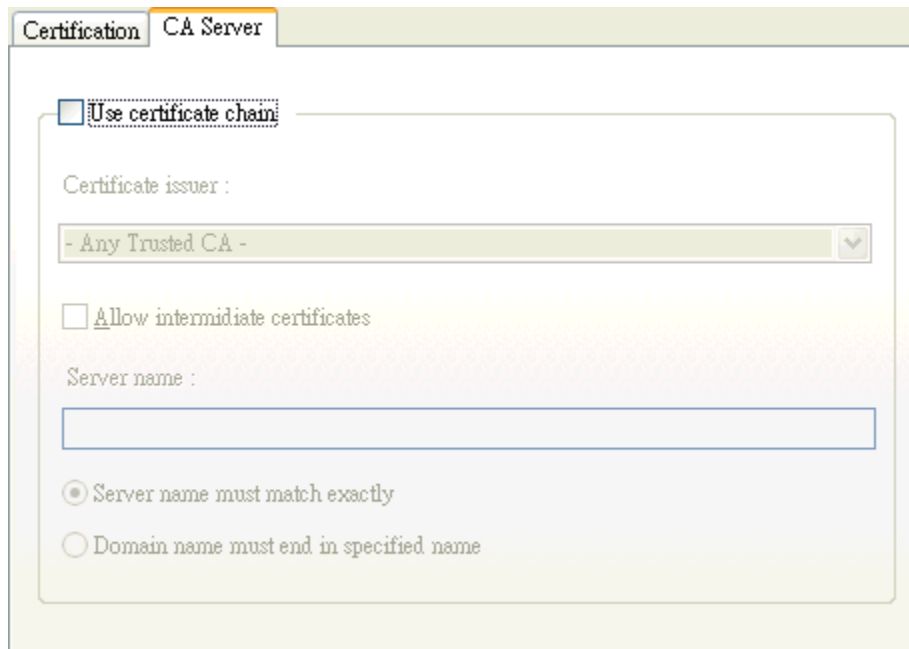
- i. PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- ii. TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
- iii. TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- iv. LEAP: Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
- v. MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

- Session Resumption: user can choose “ Disable ”, “ Reauthentication ”, “ Roaming ”, “ SameSsid ” and “ Always ”.
- Identity and Password: Identity and password for server.
- Use Client Certificate: Client Certificate for server authentication.
- Tunnel Authentication
 - Protocol: Tunnel protocol, List information include “ EAP-MSCHAP ”, “ EAP-MSCHAP v2 ”, “ CAHAP ” and “ MD5 ”
 - Tunnel Identity: Identity for tunnel.
 - Tunnel Password: Password for tunnel.
- CA Server: Certificate Authority Server. Each certificate is signed or issued by it.

CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial CA. Show as the figure.

1. Certificate issuer: Choose use server that issuer of certificates.
2. Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.
3. Server name: Enter an authentication sever root.

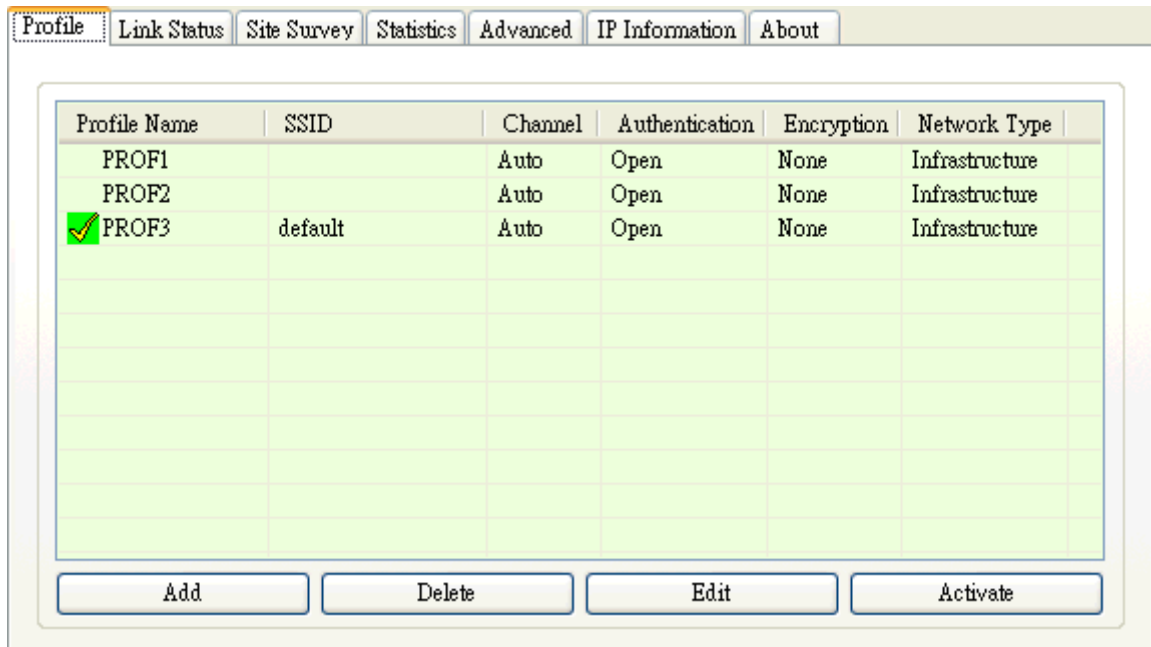


The screenshot shows a configuration window titled "CA Server" with the following elements:


- Use certificate chain
- Certificate issuer :
- Any Trusted CA -
- Allow intermediate certificates
- Server name :
[Empty text box]
- Server name must match exactly
- Domain name must end in specified name

Profile Page

Profile can book keeping your favorite wireless setting among your home, office, and other public hot spot. You may save multiple profiles, and activate the correct one at your preference.



The screenshot shows a web interface with a tabbed menu at the top: Profile (selected), Link Status, Site Survey, Statistics, Advanced, IP Information, and About. Below the menu is a table with the following columns: Profile Name, SSID, Channel, Authentication, Encryption, and Network Type. The table contains three rows of data. The third row, labeled PROF3, has a green checkmark icon in the first column. Below the table are four buttons: Add, Delete, Edit, and Activate.

| Profile Name | SSID | Channel | Authentication | Encryption | Network Type |
|---|---------|---------|----------------|------------|----------------|
| PROF1 | | Auto | Open | None | Infrastructure |
| PROF2 | | Auto | Open | None | Infrastructure |
|  PROF3 | default | Auto | Open | None | Infrastructure |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Buttons: Add, Delete, Edit, Activate

Definition of each field

- Profile: Name of profile, preset to PROF* (* indicate 1, 2, 3,).
- SSID: AP or Ad-hoc name.
- Channel: Channel in use for Ad-Hoc mode.
- Authentication: Authentication mode.
- Encryption: Security algorithm in use.
- Network Type: including infrastructure and Ad-Hoc.

Connection status



Indicate connection is successful on currently activated profile.



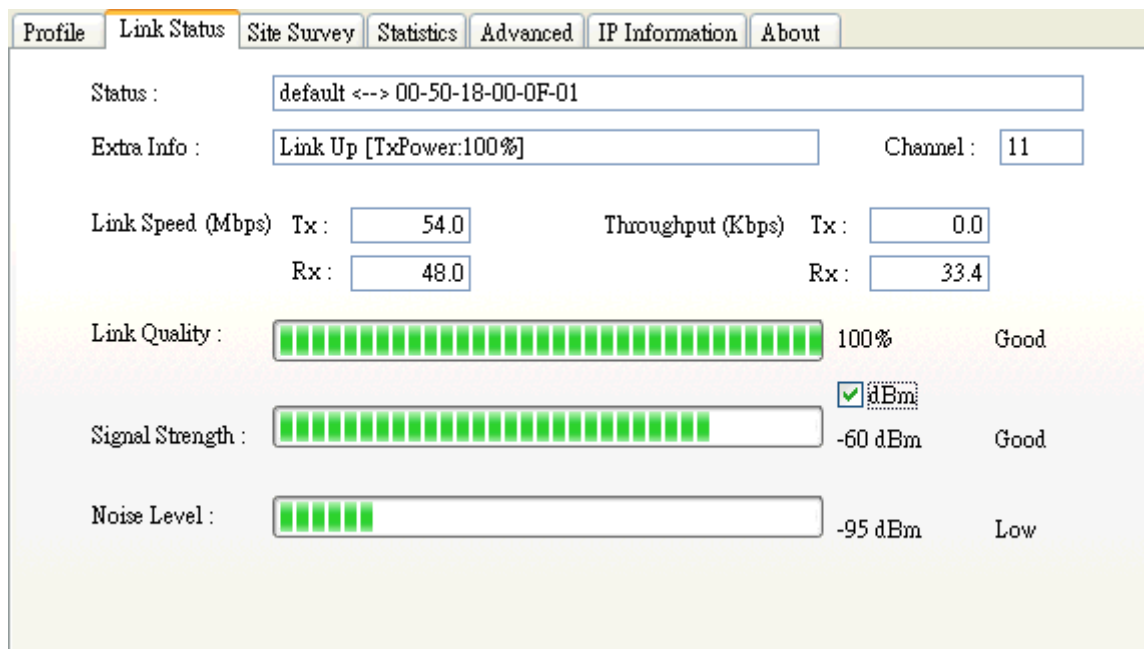
Indicate connection is failed on currently activated profile.

Note: When use site survey to make the connection. None of the profile will have the connection status icon.

- Add: Add a new profile.
- Delete: Delete an existing profile.
- Edit: Edit profile content.
- Activate: Activate selected profile.

Link Status Page

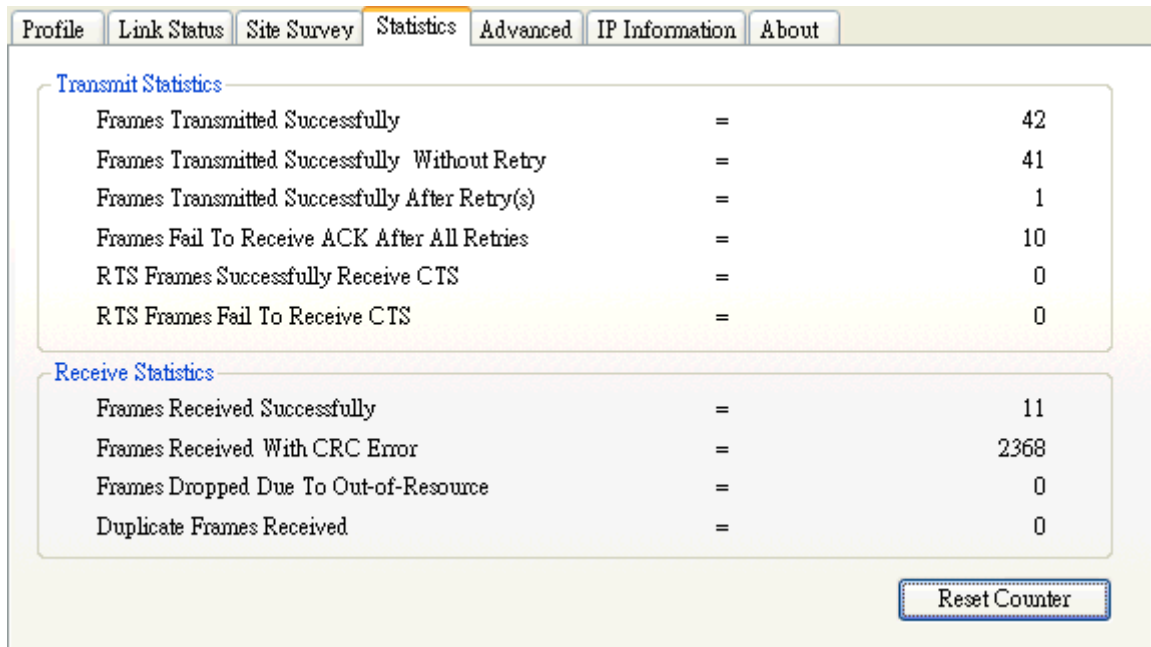
The page displays the detailed information of the current connection.



- Status: Current connection status. If no connection, it will show Disconnected. Otherwise, the SSID and BSSID will show here.
- Extra Info: Display link status and current channel in use.
- Link Speed: Show current transmit rate and receive rate.
- Throughput: Display transmits and receive throughput in unit of K bits/sec.
- Link Quality: Display connection quality based on signal strength and Tx/Rx packet error rate.
- Signal Strength: Receive signal strength, user can choose to display as percentage or dBm format.
- Noise Level: Display noise signal strength.

Statistics Page

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



The screenshot shows a web interface with a navigation bar containing tabs: Profile, Link Status, Site Survey, Statistics (selected), Advanced, IP Information, and About. Below the navigation bar, there are two sections: 'Transmit Statistics' and 'Receive Statistics'. Each section contains a table of statistics. At the bottom right of the interface is a 'Reset Counter' button.

| Transmit Statistics | | |
|--|---|----|
| Frames Transmitted Successfully | = | 42 |
| Frames Transmitted Successfully Without Retry | = | 41 |
| Frames Transmitted Successfully After Retry(s) | = | 1 |
| Frames Fail To Receive ACK After All Retries | = | 10 |
| RTS Frames Successfully Receive CTS | = | 0 |
| RTS Frames Fail To Receive CTS | = | 0 |

| Receive Statistics | | |
|---------------------------------------|---|------|
| Frames Received Successfully | = | 11 |
| Frames Received With CRC Error | = | 2368 |
| Frames Dropped Due To Out-of-Resource | = | 0 |
| Duplicate Frames Received | = | 0 |

Reset Counter

Transmit Statistics

- Frames Transmitted Successfully: Frames successfully sent.
- Frames Transmitted Successfully Without Retry: Frames successfully sent without any retry.
- Frames Transmitted Successfully After Retry: Frames successfully sent with one or more retries.
- Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
- RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
- RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.

Receive Statistics

- Frames Received Successfully: Frames received successfully.
 - Frames Received With CRC Error: Frames received with CRC error.
 - Frames Dropped Due To Out-of-Resource: Frames dropped due to resource issue.
 - Duplicate Frames Received: Duplicate received frames.
- Reset Counter: Reset all counters to zero.

Advance Page

1. - Wireless mode: Select wireless mode. 802.11b only, 802.11 b/g mixed and 802.11b/g/n mixed modes are supported.
- 11b/g Protection: ERP protection mode of 802.11g definition.
 - Auto: STA will dynamically change as AP announcement.
 - On: Always send frame with protection.
 - Off: Always send frame without protection.
- Tx Rate: Manually force the Transmit using selected rate. Default is auto.
- Tx Burst: Proprietary frame burst mode of this utility.
- Enable TCP Window Size:.
- Fast Roaming at: fast to roaming, setup by transmit power.
- 11b/g/n Country Region Code: country to choose. Country channel list: Country channel list

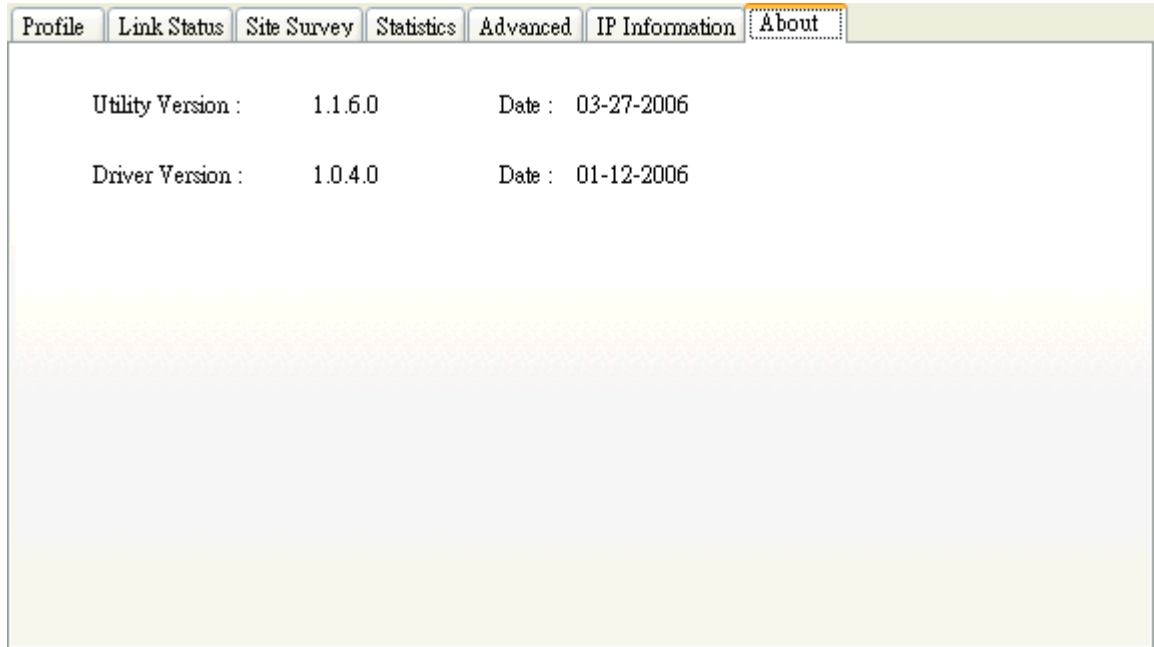
- CCX2.0: support Cisco Compatible Extensions function:
 - LEAP turn on CCKM
 - Enable Radio Measurement: can channel measurement every 0~2000 milliseconds.

- Radio On: To turn on radio.
- Radio Off: To turn off radio.

- Apply: Apply the above changes.

About Page

About page display the utility and driver version information of the wireless adapter.



FCC Statements:

1. 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.
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
4. This device is for OEM installation only, the End User manual shall not contain information about how to install the module.
5. This compliance to FCC radiation exposure limits for an uncontrolled environment, and minimum of 20 cm separation between antenna and body.
6. Only the type of antenna tested may be used.
7. The end product must carry a label stating "Contains TX FCC ID:PBLWL581MAM".

Information for OEM integrator:

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the users manual of the end product which integrate this module.

The users manual for OEM integrators end users must include the following information in a prominent location

IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.