

Chung Nam Electronics(CNE)
IEEE 802.11b/g USB WLAN Module
(Model#:WLC300GA)

OEM Manual

Rev: 1.0

Oct 2008

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.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Information to User

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

FCC Guidelines for Human Exposure

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or Transmitter.

Contents

Chapter 1 Introduction.....	3
1.1 Features.....	3
1.2 LED Status.....	3
1.3 System Requirements.....	3
1.4 Network Configuration.....	4
Chapter 2 Installation Guide.....	4
Chapter 3 Uninstall Guide.....	7
Chapter 4 Software Configuration.....	8
4.1 Station Mode Configuration.....	8
4.1.1 More Setting.....	9
4.1.1.1 General Connection Setting.....	9
4.1.1.2 WEP Encryption.....	11
4.1.1.3 WPA/WPA2 Authentication with TKIP/AES Encryption.....	12
4.1.1.4 WPA-PSK Authentication.....	14
4.1.1.5 Profiles.....	14
4.2 Wireless network mode configuration.....	16
Chapter 5 OEM installation guide.....	17
Appendix A: Glossary.....	17
Appendix B: Specifications.....	19

Chapter1 Introduction

The WLC300GA 54M wireless USB adapter is a USB 2.0 interface wireless adapter supporting IEEE 802.11b/g 2.4GHz radio operation. It provides high-speed wireless connection with data rate up to 54Mbps.

1.1 Features

- Compatibility: compatible with IEEE 802.11b and IEEE 802.11g high data rate standard to provide wireless speed up to 54Mbps data rate.
- Compliance with FCC/CE standards
- Dynamic data rate: auto fallback switching with 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and 1Mbps
- Wireless data encryption with 64, 128 encryption for security
- Drivers supports Windows 98, ME, 2000 , XP and Linux
- User-friendly tool for wireless configuration
- Supports infrastructure and Ad-hoc modes
- RoHS compliant
- Provides USB2.0 interface
- On board antenna or extended antenna (factory option)

1.2 LED Status

The WLC300GA 54M wireless USB adapter has a LED indicator for wireless connectivity.

LED Indicator:

When not connected, the LED is off for 1 second and on for 2 seconds repeatedly. When connected, the LED will always ON. When send data, the LED is blinking.

1.3 System Requirements

The following are the minimum system requirements in order to use the **The WLC300GA 54M wireless USB adapter**

Compatible computer with a USB interface.

Windows 98/ME/2000/XP/2003 operating system.

Requires minimum Pentium 166MHz with MMX technology.

1.4 Network Configuration

Ad-hoc (peer-to-peer) Mode

In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.

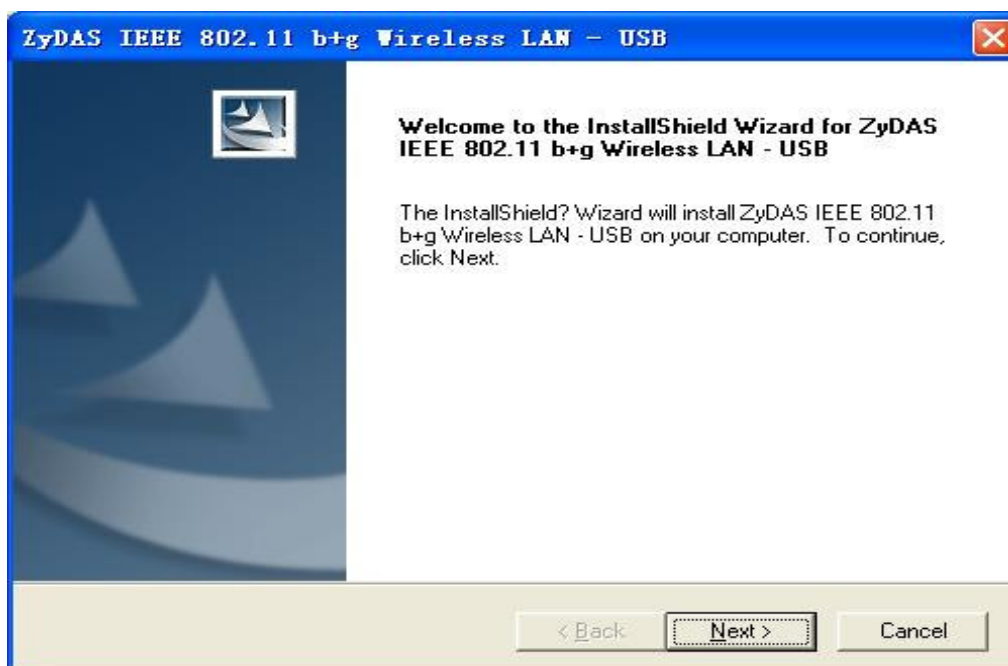
Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computer has to be via the AP.

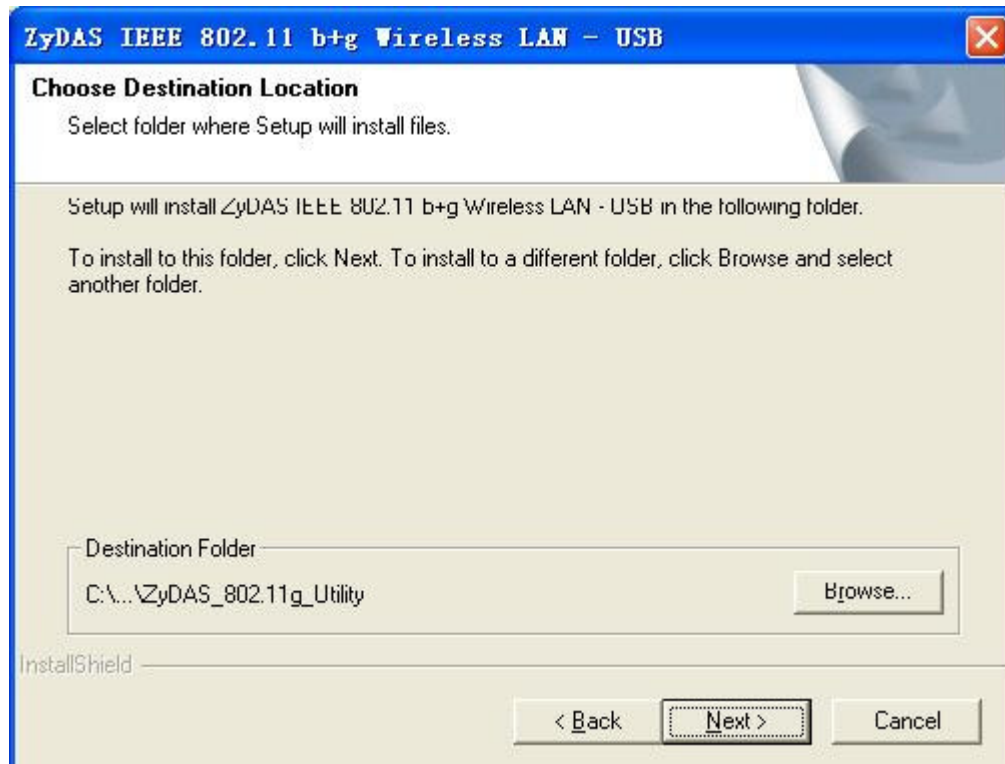
Chapter 2 Installation Guide

Follow the steps below in order to install the WLANTUBG 54M Wireless USB Adapter drivers:

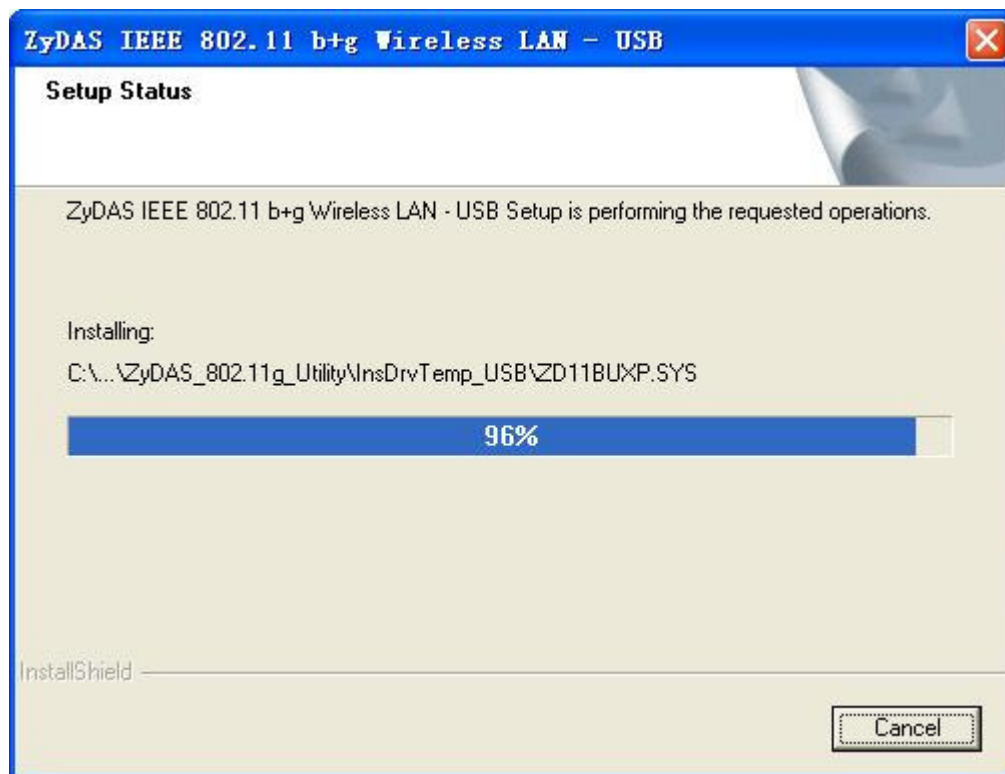
- ◆ Find and come into the driver subdirectory, run the **setup.exe**.
- ◆ Once the setup begins you will see the **Install Shield Wizard**, as the image depicts below.



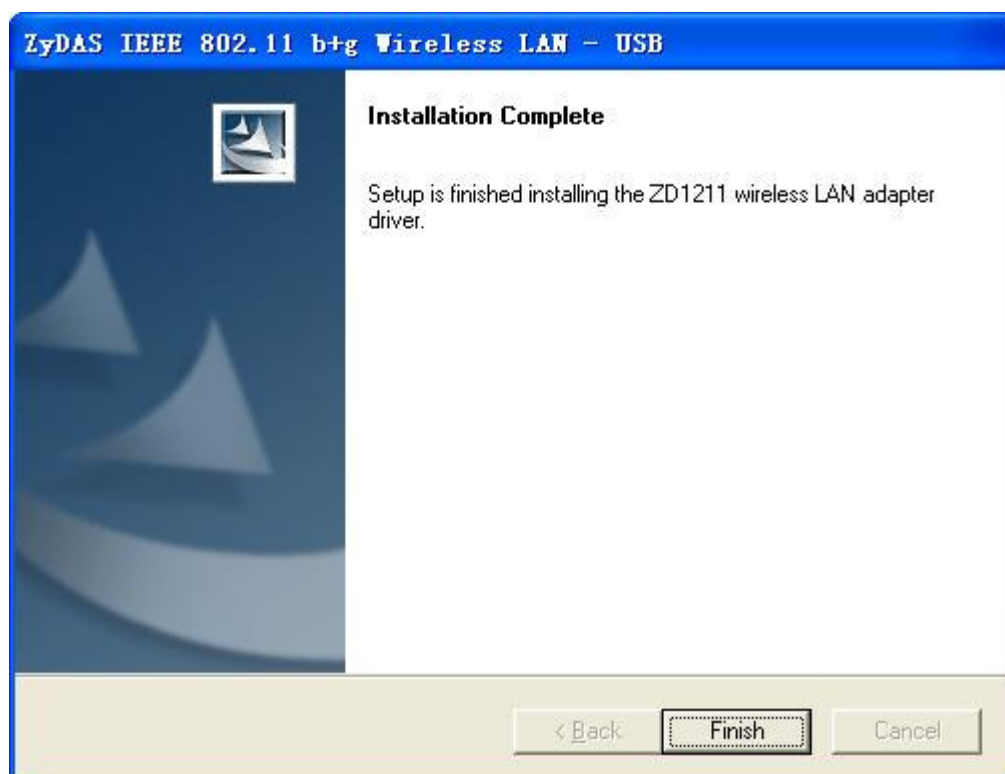
- ◆ Click on the **Next** button to continue.
- ◆ Select the location where you would like the driver installed. Click on the **Browse** button to change the directory, or click on the **Next** button to continue using the default directory.



- ◆ Wait a few moments until the files are copied to the computer.



- ◆ The first part of the installation is complete. Click on the **Finish** button.



- ◆ At this point, carefully insert the device into the USB port of your computer.

Windows will automatically detect the device and display the icon  and below in the taskbar.

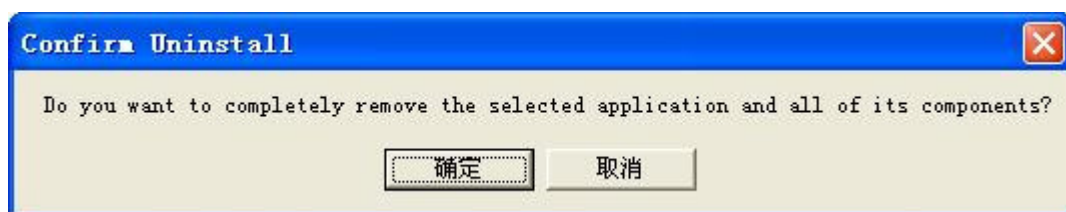
Chapter 3 Uninstall Guide

If the device installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the device and its utility and repeat the installation procedure again.

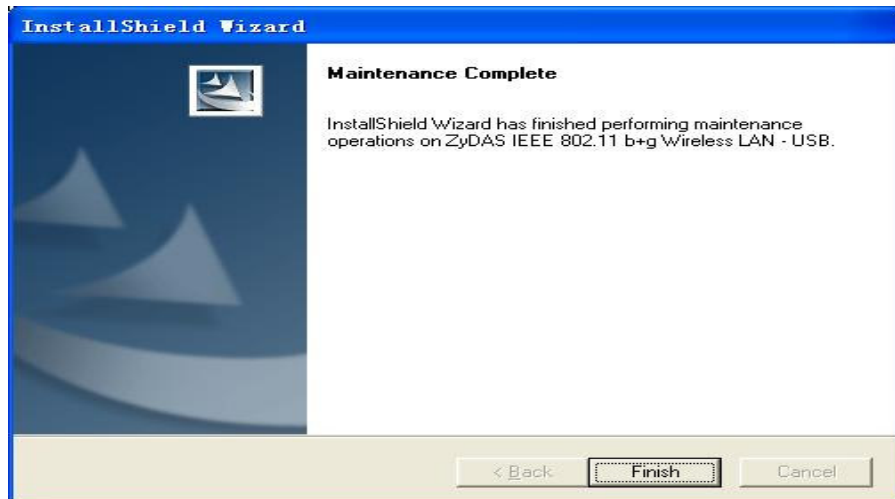
- ◆ Click on **Start > Settings > Control Panel > Add or Remove Programs**,

Select the **ZyDAS IEEE 802.11 b+ g Wireless LAN – USB** and then click on **Remove**; or click on **Start > programs > ZyDAS IEEE 802.11 b+ g wireless LAN – USB > Uninstall ZD1211 Application**.

- ◆ Click on the **OK(确定)** button to confirm the Uninstalling process.



- ◆ The process will then remove ZyDAS Wireless Utility and the drivers from your computer. Click on the **Finish** button and then remove the WLANTUBG 54M Wireless USB adapter.

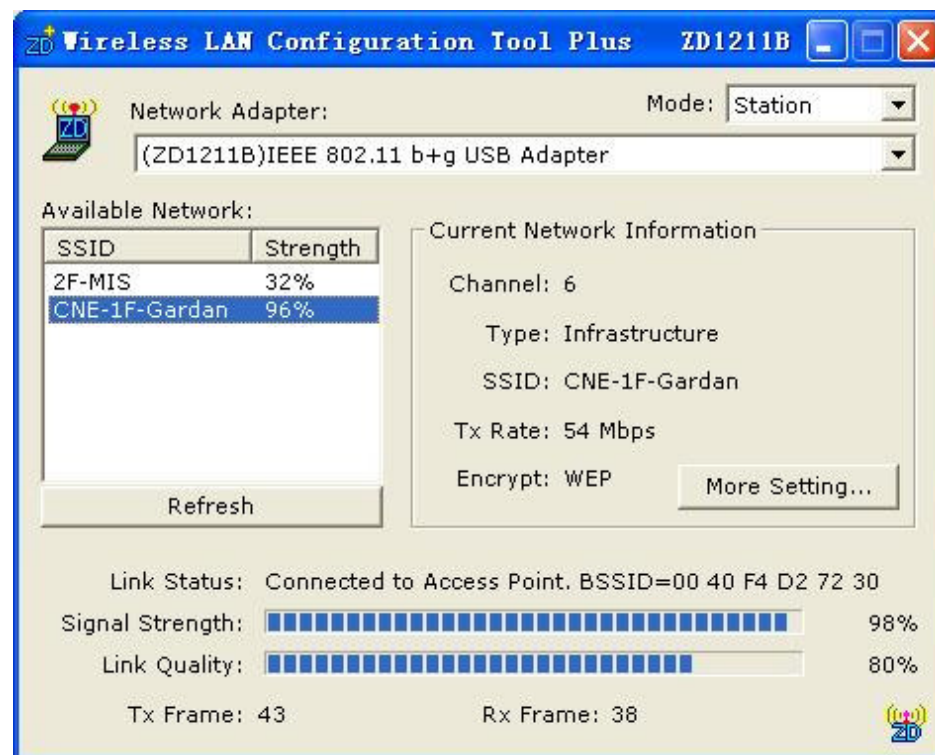


Chapter 4 Software Configuration

4.1 Station Mode Configuration

This chapter focuses on how to configure the device in Station mode (wireless LAN client).

The figure as below displays the current status of the wireless radio as a station.



4.1.1 More Setting

4.1.1.1 General Connection Setting

The **General Connection Setting** allows you to configure the SSID, network type, authentication, and encryption type.



The screenshot shows a Windows-style dialog box titled "More Setting...". It contains four main sections:

- General Connection Setting:** This section includes several dropdown menus: "WirelessMode" set to "2.4GHz(802.11b+g)", "Channel" set to "6", "Tx Rate" set to "Auto", "SSID" set to "CNE-1F-Gardan" with an "any" checkbox, "Network Type" set to "Infrastructure", "Authentication" set to "Auto", and "Encryption" set to "WEP". A "Change" button is located next to the Encryption dropdown.
- Encryption Setting:** This section contains two buttons: "WEP Encryption Key Setting" and "WPA Encryption Setting".
- Profile:** This section has a "Profile Name" dropdown menu and three buttons: "Load", "Save Current", and "Delete".
- Other:** This section contains the text "For more advanced setting, information..." and two buttons: "Advanced Setting..." and "Information".

You can click “**Change**” button to change general connection settings.



The screenshot shows a window titled "More Setting..." with a close button in the top right corner. The window contains several sections for configuring wireless settings:

- General Connection Setting:** This section includes dropdown menus for "WirelessMode" (set to "2.4GHz(802.11b+g)"), "Channel" (set to "6"), and "Tx Rate" (set to "Auto"). It also has a text field for "SSID" (set to "CNE-1F-Gardan") with an "any" checkbox to its right. Below these are dropdowns for "Network Type" (set to "Infrastructure") and "Authentication" (set to "Auto"). At the bottom of this section is an "Encryption" dropdown (set to "WEP") and an "Apply" button.
- Encryption Setting:** This section contains two buttons: "WEP Encryption Key Setting" and "WPA Encryption Setting".
- Profile:** This section has a "Profile Name" dropdown, followed by "Load", "Save Current", and "Delete" buttons.
- Other:** This section contains the text "For more advanced setting, information..." and two buttons: "Advanced Setting..." and "Information".

SSID: Enter the SSID of the network. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive. Place a check in the **any** box if you would like the device to connect to the first available Access Point with the strongest signal.

Network Type: Select a network type from the drop-down list.

Infrastructure or **Ad-hoc:** If you select infrastructure, the device must be connected to an Access Point. If you select ad-hoc, you may connect the device to another WLAN client adapter.

Authentication: Select an authentication type from the drop down list. Options available are: **Auto, Open System, Shared Key, WPA, WPA-PSK, WPA2, WPA2-PSK.**

Encryption: Select an encryption type from the drop-down list. Options available are: **Disable, WEP, TKIP, AES.**

Note: Refer to the **WEP encryption** and **WPA encryption** sections in this chapter to configure the security settings.

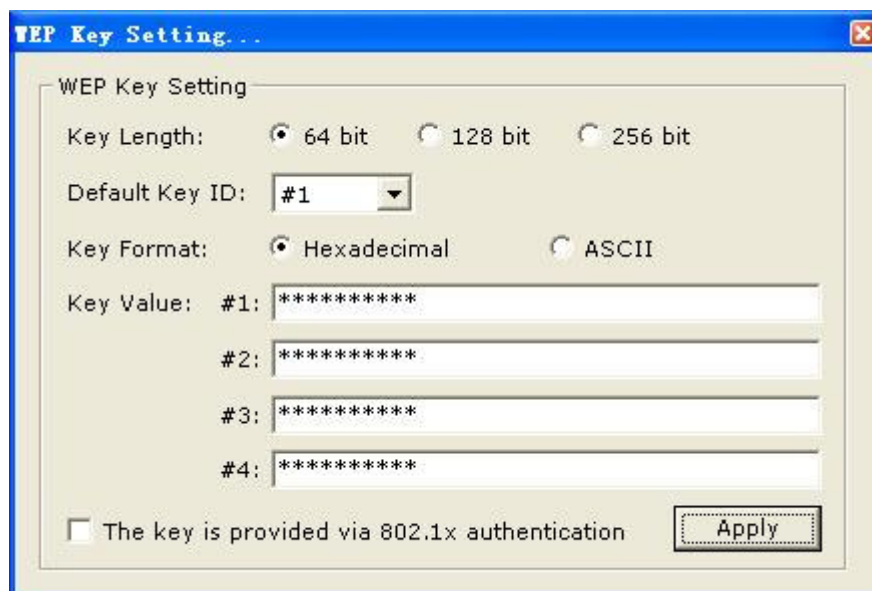
4.1.1.2 WEP Encryption

You may select 64, 128 or 256 bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase.

Authentication: Select **Open System** or **Shared Key** from the drop-down list. If you are not sure what to choose, please select **auto**.

Encryption: Select WEP from the drop-down list.

Click on the **WEP Encryption Key Setting** button. You will see the figure below.



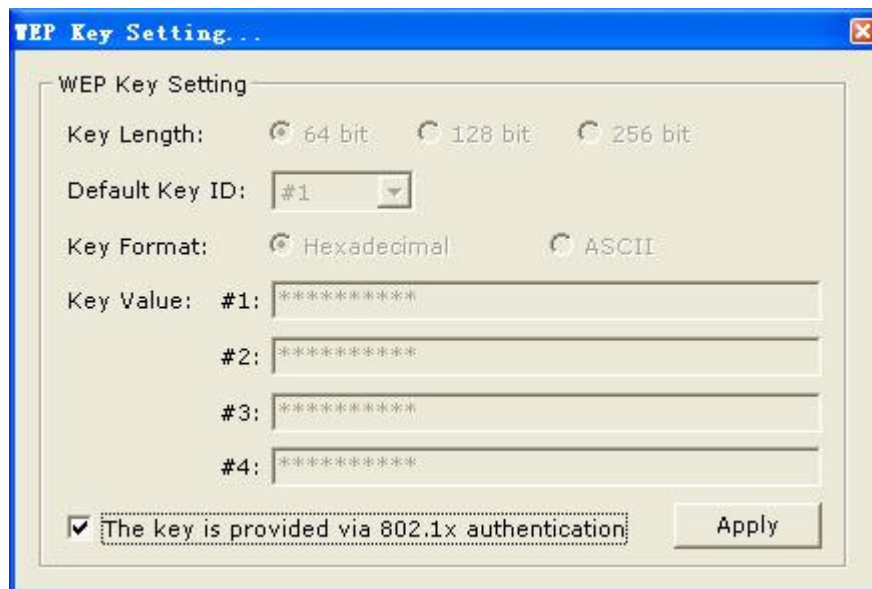
Key Length: Select an encryption key length: **64**, **128** or **256 bit**. The setting must be the same as the Access Point.

Default Key ID: Since you can specify up to 4 different WEP keys, select the WEP

key value that will be used for this network.

Key Format: Select Hexadecimal or ASCII.

Key Value #1 – #4: You may enter up to 4 different WEP keys. However, only that WEP key will be used that is defined by the **Default Key ID**.



The key is provided via IEEE 802.1X authentication: Place a check in this box is IEEE 802.1X authentication is used. By selecting this option, the WEP key settings will be disabled.

Click on the **Apply** button, and then you can use the IEEE 802.1X authentication.

4.1.1.3 WPA/WPA2 Authentication with TKIP/AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal key Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which

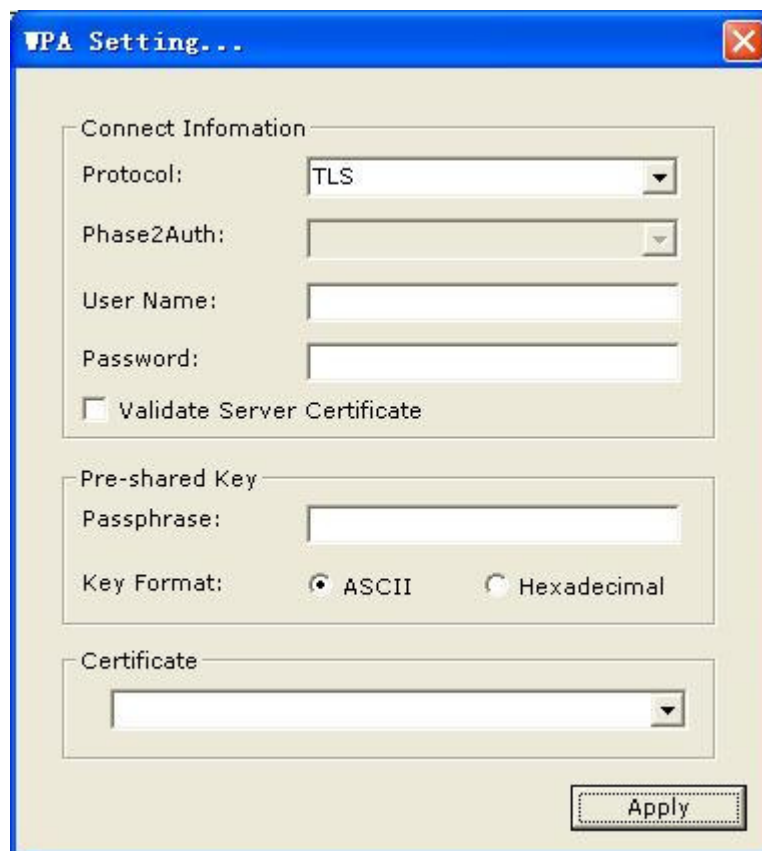
makes sure that keys haven't been tampered with.

Authentication: Select **WPA** from the drop-down list.

Encryption: Select **TKIP** or **AES** from the drop-down list.

Click on the **WPA Encryption Setting** button.

In this section you can configure the settings for TLS or PEAP. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

The image shows a Windows-style dialog box titled "WPA Setting...". It contains three main sections: "Connect Information", "Pre-shared Key", and "Certificate". The "Connect Information" section has a "Protocol:" dropdown menu set to "TLS", a "Phase2Auth:" dropdown menu, a "User Name:" text box, a "Password:" text box, and a checkbox labeled "Validate Server Certificate" which is currently unchecked. The "Pre-shared Key" section has a "Passphrase:" text box and a "Key Format:" section with two radio buttons: "ASCII" (which is selected) and "Hexadecimal". The "Certificate" section has a dropdown menu. An "Apply" button is located at the bottom right of the dialog box.

Protocol: Select **TLS** from the drop-down list.

User Name: Enter the user name that is used for authentication purposes.

Passphrase: Enter a WPA passphrase. For ASCII text, enter 8-63 characters, for hexadecimal enter 64 characters).

Certificate: Make sure that you have downloaded and installed the certificate on the computer. Then select the appropriate certificate from the drop-down list.

Click on the **Apply** button to save the changes.

The PEAP authentication type is based on EAP TLS authentication, but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key, which is derived from the device and RADIUS server, to encrypt data.

4.1.1.4 WPA-PSK Authentication

Authentication: Select **WPA-PSK** from the drop-down list.

Encryption: Select an encryption type from the drop-down list.

Click on the **Apply** button to save the changes.

4.1.1.5 Profiles

Multiple profiles can be created for different Network Names (SSIDs) and security settings. This allows a user to quickly associate with another network, instead of entering the credentials each time.



Profile Name: Displays the name of current profile. One device can have many profiles, but only one profile can be loaded at a time.

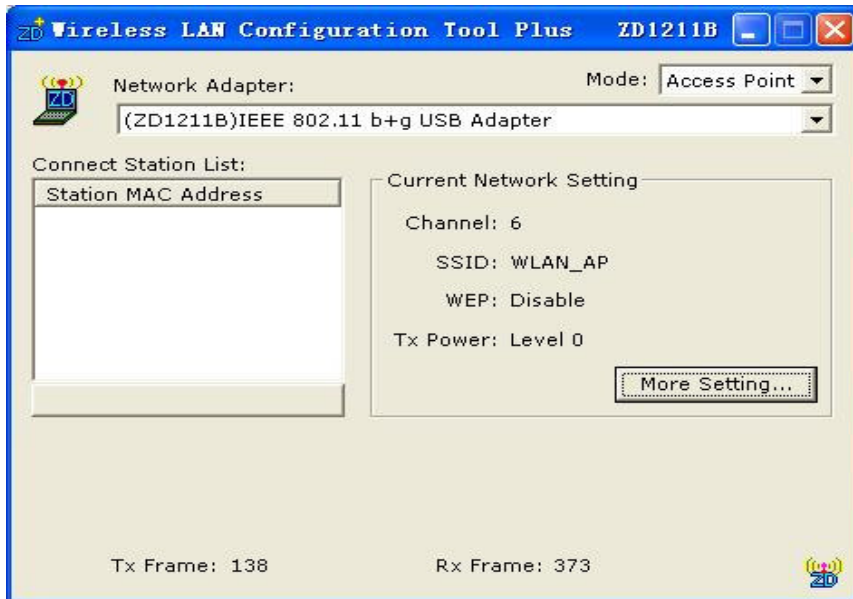
Load: Select a profile from the drop-down list and then click on the **Load** button.

Save Current: Enter a new profile name and then click on the **Save Current** button to save the profile.

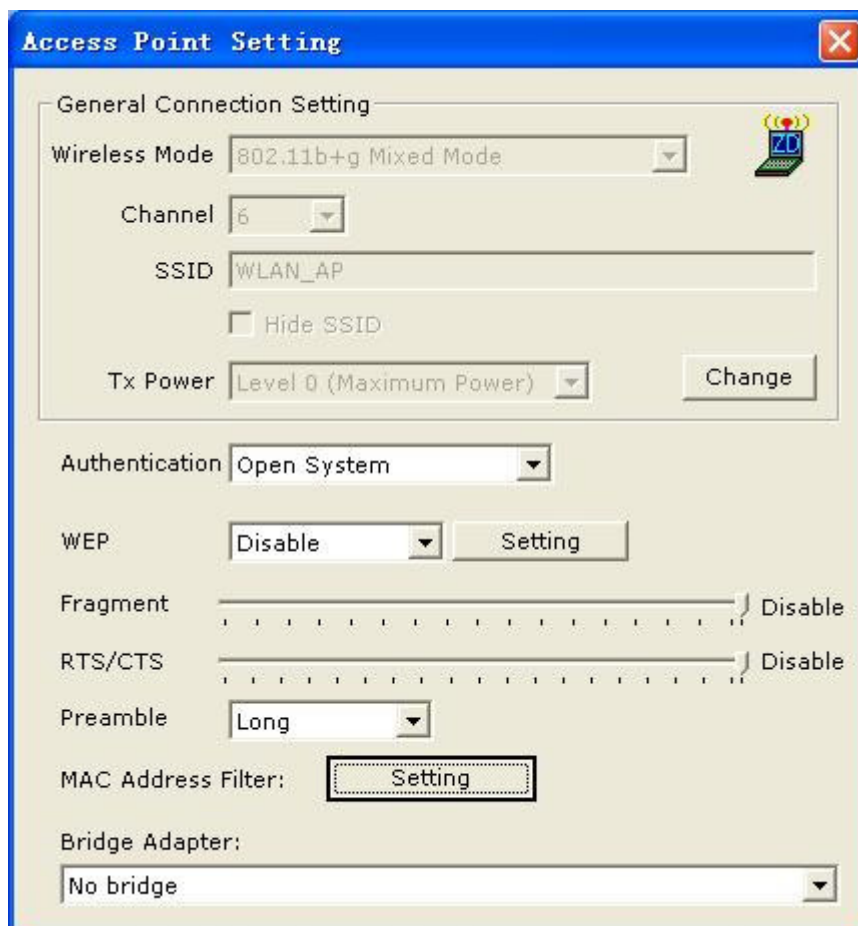
Delete: To delete an existing profile, select it from the drop-down list and then click on the **Delete** button.

4.2 Wireless network mode configuration

The screen of wireless network mode displays as below :



The more setting screen :



Chapter 5 OEM Installation Guide

If you would like to put this device as an embedded module into your end product and if the original FCC ID label is covered up, please display a label in visible area on the end product with the following:

Contains Transmitter Module FCC ID: Q72WLC300GA
--

Guide to OEM integrators

This device is intended only for OEM integrators under the following conditions:

- (1) The antenna must be installed such that 20 cm is maintained between the antenna and users;
- (2) The transmitter module may not be co-located with any other transmitter or antenna;
- (3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change. As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product (host of this device) for any additional compliance requirements required.

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the integrated antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: “Contains FCC ID: Q72WLC300GA”.

Manual Information To the End User

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 user’s manual of the end product which integrates this module. The end user manual shall include all required regulatory information/warning as show in this manual.

Appendix A: Glossary

IEEE 802.11b – The IEEE 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. IEEE 802.11b networks are also referred to as Wi-Fi networks.

IEEE 802.11g – Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

Ad-hoc Network – An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent IEEE 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

Infrastructure Network – An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an IEEE 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

SSID – A **S**ervice **S**et **I**dentification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (Wired Equivalent Privacy) – A data privacy mechanism based on a 64 bit or 128 bit or 256 bit shared key algorithm, as described in the IEEE 802.11g standard.

Wi-Fi – A trade name for the IEEE 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among IEEE 802.11b devices.

WLAN (Wireless Local Area Network) – A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

WPA (Wi-Fi Protected Access) – A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

AP– Access Point

PSK– Pre-Shared Key

TKIP– Temporal Key Integrity Protocol

AES– Advanced Encryption Standard

TLS– Transport Layer Security

TTLS– Tunnel Transport Layer Security

PEAP– Protected Extended Authentication Protocol

RADIUS– Remote Authentication Dial In User Service

Appendix B: Specifications

Radio Emission Type	Comply with IEEE 802.11b and 802.11g physical layer.
Operating Frequency	2.4 GHz ~ 2.4835 GHz ISM band

Data Modulation types	OFDM (Orthogonal Frequency Division Multiplexing) CCK (Complementary Code Keying) DQPSK (Differential Quadrature Phase Shift Keying), DBPSK (Differential Binary Phase Shift Keying)
Data Rate (Physical Layer)	54Mbps with fall back rates of 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps
Security	64/128bits WEP Encryption, 802.1x Authentication, WPA
Operating Voltage	5 VDC $\pm$ 5%
Bus Interface	A-type USB 2.0 Connector