

ZG-760E User Manual

Wireless Local Area Network Dual-band USB Card

(For 802.11b/g Wireless Networks)

1 Overview

1.1 Product Introduction

Thank you for purchasing the ZG-760E.

The adapter is designed to provide a high-speed and unrivaled wireless performance for your PC. With a faster wireless connection, you can get a better Internet service, such as downloading, gaming, video streaming and so on. The ZG-760E supports IEEE 802.11b/g 2.4GHz radio operation. With auto-sensing capability, the adapter packet transfer rate is up to 54 Mbps. Additionally, the ZG-760E has good capability on anti-jamming and supports WEP, TKIP, AES, WPA, and WPA2 encryption, which prevents outside intrusion and protect your personal information from being exposed. Featuring high-performance transmission rate, simple installation and adaptability, as well as strong security, the ZG-760E is the perfect solution for small office and home needs.

1.2 System Requirements

Recommended system requirements are as follows:

- = Windows XP, Windows 2000 or Windows Vista
- = Standard USB 2.0 port
- = 32MB system memory or larger
- = 300MHz processor or higher

1.3 Packing List

The packing list of the ZG-760E contains the following items:

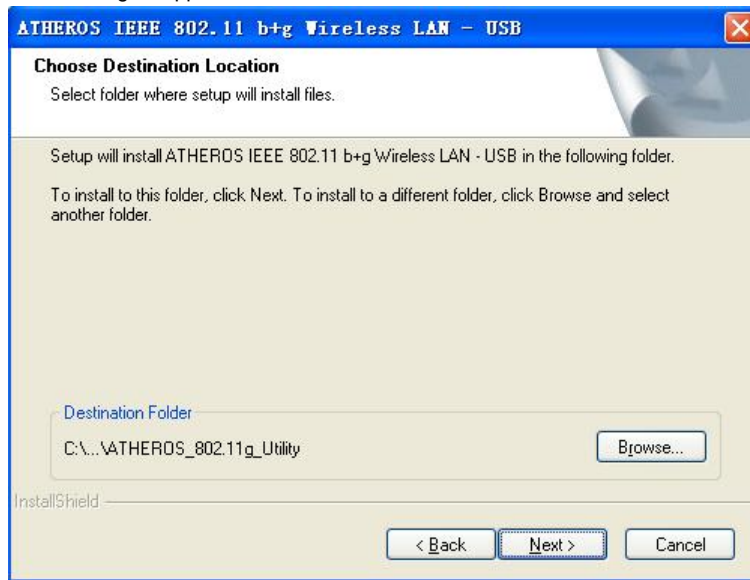
- = 1x ZG-760E
- = 1 x quick installation guide
- = 1 x user manual

2 Installation

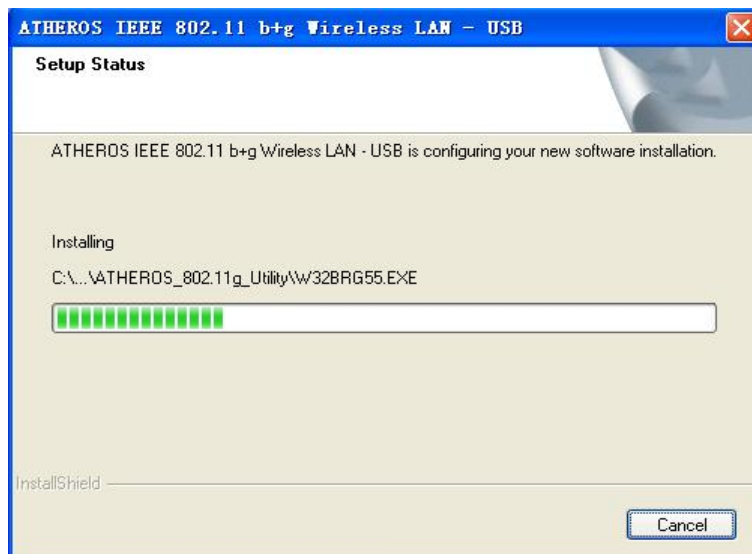
This chapter describes how to install driver and utility of the ZG-760E. The following procedure is illustrated in Windows XP.

2.1 Installation Guide

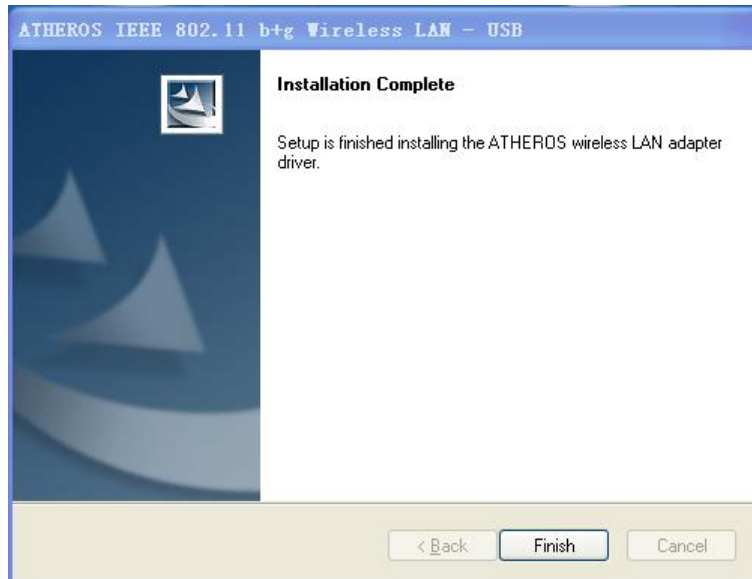
- Step 1** Find the setup file named **ZG-760E .exe**, and then double-click ZG-760E.exe to start the installation. The page shown in the following figure appears.



- Step 2** Select the destination folder where setup will install files. The page shown in the following figure appears within seconds.



Step 3 After the installation has been completed, click **Finish** to finish the wizard.



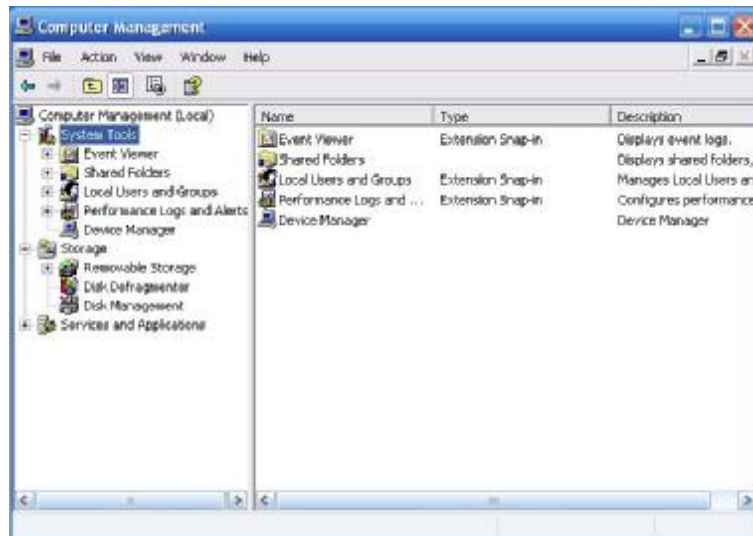
2.2 Uninstall the Software

2.2.1 Uninstall the driver software from your PC

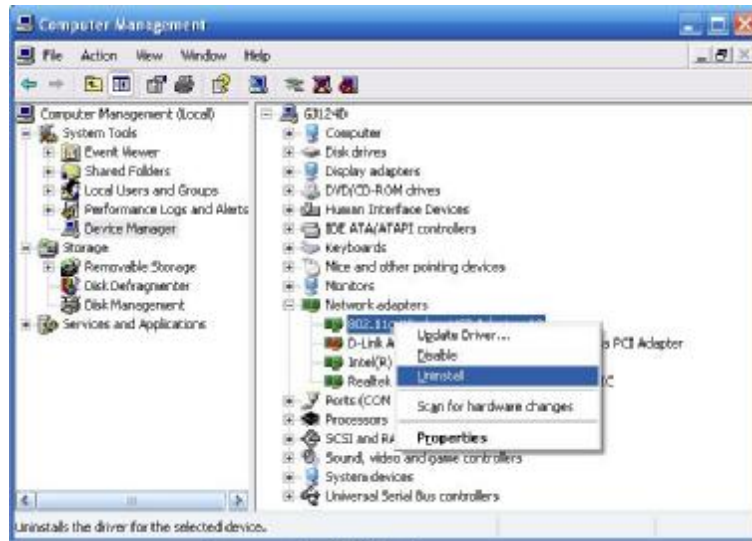
- Step 1** Right-click **My Computer** and choose **Manage** from the shortcut menu.
The page shown in the following figure appears.



Step 2 The page shown in the following figure appears.



Double-click **Device Manager** and the page shown in the following page appears. Double-click **Network adapters**, and then right-click **802.11 USB Wireless LAN Card USB Adapter**.



Step 3 Choose **Uninstall** from the shortcut menu. Then the system uninstalls the driver software of the ZG-760E from your PC.

2.2.2 Uninstall the utility software from your PC

Step 1 Choose **Start > All Programs > Atheros_technology_corporation**, and the page shown in the following figure appears. Then choose **Uninstall atheros Application** from the menu.



Step 2 Follow the **Install Shield Wizard** to uninstall the utility software from your PC.


3 Configuration


The ZG-760E can be configured by its utility in Windows 2000, Windows XP or Windows Vista. This chapter describes how to configure in the Windows XP, which guides you to configure your wireless adapter for wireless connectivity with trustable data security encryption features. The configuration procedures in Windows 2000, Windows Vista and Windows XP are similar. For the configuration in Windows 2000 and Windows Vista, refer to the instructions in Windows XP.

**Note:**

If your operation system (OS) is Windows XP, you can use Windows XP to configure the wireless network settings. (To use this function, you must upgrade the OS with SP2).

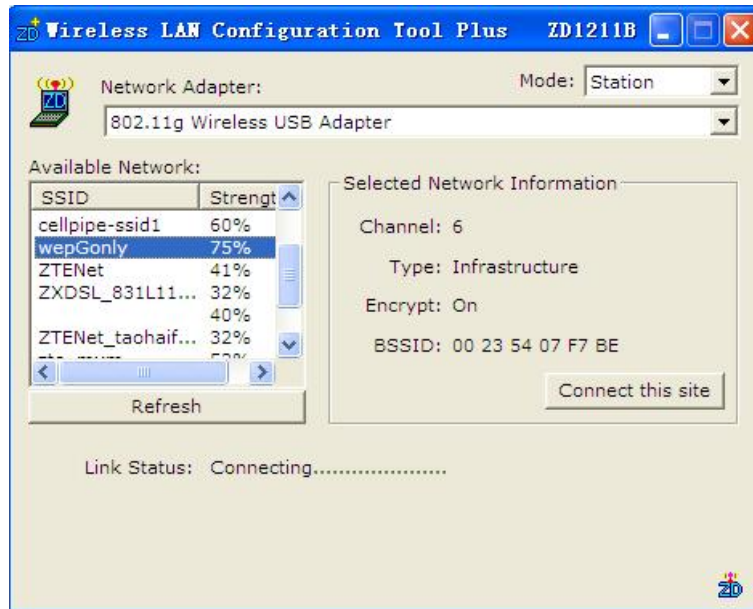
Checking the Utility

After completing the adapter's driver, choose **Start > All Programs > Atheros_technology_corporation > ZDWlan.exe** to run the utility. Then the adapter's icon  will appear in the system tray.

If you want to configure wireless network settings in Windows XP, right-click the icon  in the system tray. Then choose **Use Zero Configuration as Configuration utility** to switch the utility.

3.1 Station Mode

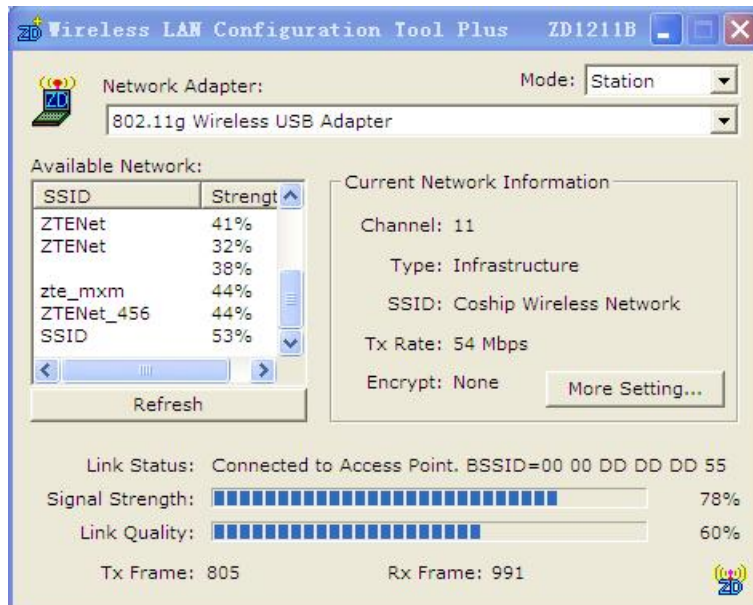
In the **Wireless LAN Configuration Tool Plus** page, there are two modes: **Station** and **Access Mode**. If you choose **Station** mode, the icon  will appear in the system tray.



Network Connection

The AP that is connected with the adapter is not set to security mechanism network

Choose the corresponding AP from the **Available Network** drop-down list and click **Connect this site**. If it connects the site successfully, the page shown in the following figure appears.



The following table describes the parameters of this page.

Field	Description
Channel	The network channel.
Type	The network connection type.
SSID	The name of the IEEE 802.11 wireless network. It has a maximum limit of 32 characters.
Tx Rate	The transmission rate.
Encrypt	It displays whether the AP is encrypted or not.
Signal Strength	It displays the signal strength of the AP that the adapter is connected to.
Link Quality	It displays the signal quality.
Tx Frame	The transmitted frames.
Rx Frame	The received frames.

The AP that is connected with the adapter is set to security mechanism network

Choose the corresponding AP from the **Available Network** drop-down list and click **Connect this site**. If it connects the site successfully, the page shown in the above figure appears. If it is failed to connect the site, click **More Settings**. Click **Change** in the **More Setting...** page, and the following page appears.

The screenshot shows a 'More Setting...' dialog box with a blue title bar and a close button. It contains several sections for configuring a wireless connection:

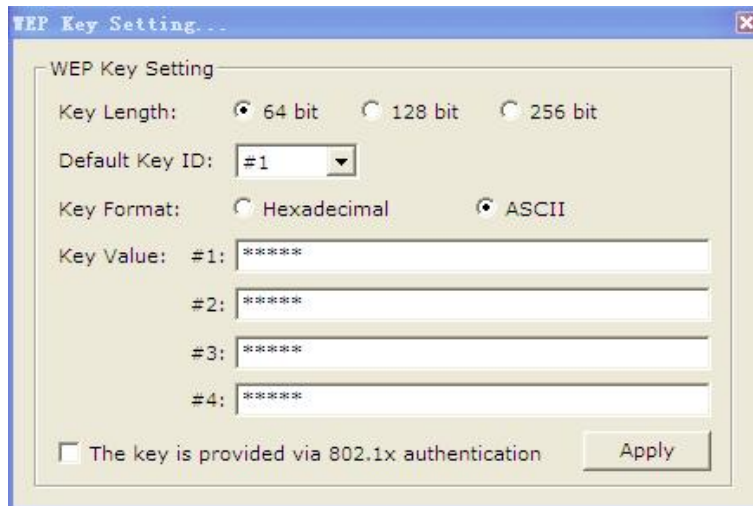
- General Connection Setting:** Includes dropdowns for WirelessMode (2.4GHz(802.11b+g)), Channel (11), Tx Rate (Auto), SSID (Coship Wireless Network), Network Type (Infrastructure), Authentication (WPA PSK), and Encryption (TKIP). There is an 'Apply' button and a small wireless adapter icon.
- Encryption Setting:** Contains two buttons: 'WEP Encryption Key Setting' and 'WPA Encryption Setting'.
- Profile:** Includes a 'Profile Name' dropdown, and 'Load', 'Save Current', and 'Delete' buttons.
- Other:** Includes the text 'For more advanced setting, information...' and two buttons: 'Advanced Setting...' and 'Information'.

The following table describes the parameters of this page.

Field	Description
General Connection Setting	
WirelessMode	It contains the wireless mode of the adapter. It is chosen by the adapter automatically.
Channel	The network channel. It is chosen by the adapter automatically.
Tx Rate	You can choose the transmission rate from the drop-down list.
SSID	You can enter the SSID of the connected AP. Normally, it is chosen by the adapter automatically.
Network Type	You can choose Infrastructure or Ad-Hoc . = If the wireless adapter connects to the AP, choose Infrastructure . = If several wireless adapters are interconnected, choose Ad-Hoc .
Authentication	Choose the authentication of the AP that is connected to the adapter. Auto indicates that the AP does not set the security mechanism.
Encryption	It displays the encryption type that the driver is using. = If you choose Open System or Shared-Key System as authentication, there are two types of encryption: WEP and None . = If you choose WPA , WPA-PSK , WPA2 , or WPA2-PSK as authentication, there are two types of encryption: TKIP and AES .

Encryption Setting

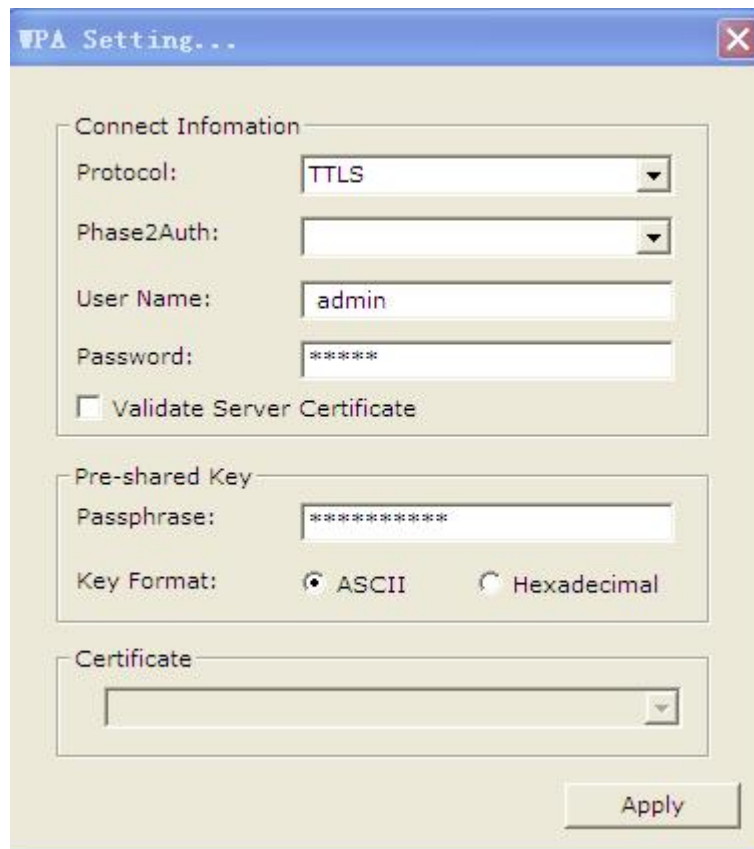
Set the AP encryption to **WEP**, and then click **WEP Encryption Key** in the **Encryption Setting** field. The page shown in the following figure appears.



The image shows a 'WEP Key Setting' dialog box. It has a title bar with 'WEP Key Setting...' and a close button. Inside, there's a section titled 'WEP Key Setting'. Under 'Key Length', there are three radio buttons: '64 bit' (selected), '128 bit', and '256 bit'. Below that is 'Default Key ID' with a dropdown menu showing '#1'. Then 'Key Format' has two radio buttons: 'Hexadecimal' and 'ASCII' (selected). The 'Key Value' section has four input fields labeled '#1:', '#2:', '#3:', and '#4:'. Each field has a small icon indicating the expected input format (hexadecimal or ASCII). At the bottom, there's a checkbox labeled 'The key is provided via 802.1x authentication' which is unchecked, and an 'Apply' button.

Key Value: #1, #2, #3, #4. For these key groups, you can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F) or 5 ASCII characters for 64-bit (also called 40 bits) encryption. You can also enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F) or 13 ASCII characters for 128-bit (also called 104 bits) encryption.

Set the AP authentication to **WPA**, **WPA-PSK**, **WPA2**, or **WPA2-PSK**, and then click **WPA Encryption Setting** in the **Encryption Setting** field. The page shown in the following figure appears.



The image shows a Windows-style dialog box titled "WPA Setting...". It contains three main sections: "Connect Information", "Pre-shared Key", and "Certificate". In the "Connect Information" section, "Protocol" is set to "TTLS", "Phase2Auth" is empty, "User Name" is "admin", and "Password" is masked with asterisks. There is an unchecked checkbox for "Validate Server Certificate". The "Pre-shared Key" section has a "Passphrase" field masked with asterisks and "Key Format" set to "ASCII" with a selected radio button. The "Certificate" section has an empty dropdown menu. An "Apply" button is at the bottom right.

Connect Information	
Protocol:	TTLS
Phase2Auth:	
User Name:	admin
Password:	*****
<input type="checkbox"/> Validate Server Certificate	

Pre-shared Key	
Passphrase:	*****
Key Format:	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal

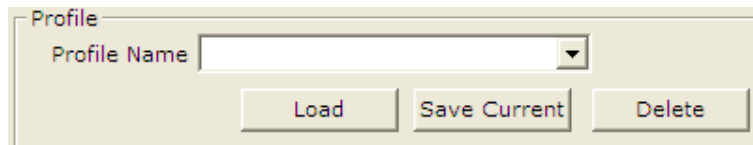
Certificate	

Apply

Enter the encryption key of the connected AP in the **Passphrase** field. Enter **User Name**, **Password**, or other information of the AP in the corresponding fields according to the authentication type.

Profile

The page shown in the following figure displays profile settings.



Profile

Profile Name

Load Save Current Delete

The following table describes the buttons of this page.

Field	Description
Save Current	After entering the profile name, click it to save the current settings.
Load	Click it and choose the profile name from the drop-down list, and then import the configuration.
Delete	Choose the profile name, and then click it to delete it.

Advanced Setting

Click **Advanced Settings** in the **Other** field and the page shown in the following figure appears.

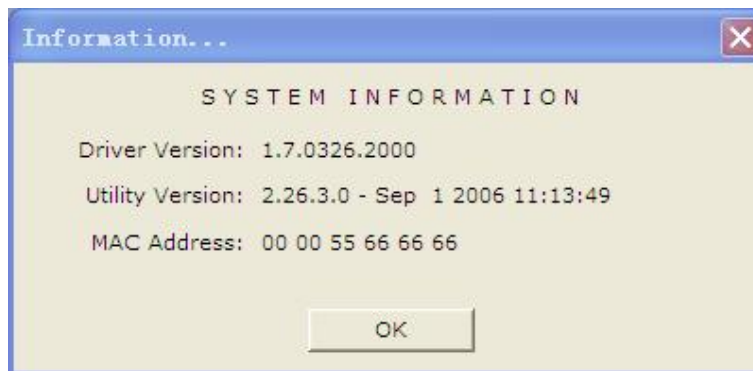
The following table describes the parameters of this page.

Field	Description
User Interface	Choose the user interface language.
Power Consumption Setting	<p>You can select the power consumption.</p> <ul style="list-style-type: none"> = Continuous Access Mode (CAM): Continuous power supply with the maximum power and transmitted power. = Maximum Power-Saving Mode: The maximum power saving with the minimum power consumption and transmitted power. = Fast Power-Saving Mode: Fast power saving with the average power consumption and transmitted power.
Country Roaming	You can select World Mode or User Selected . If you select User Selected , you can choose your country from the drop-down list.


Field	Description
PSP XLink Mode	PSP accesses the Internet through XLink.
WMM QoS Mode	It allows the wireless communication defines a priority level according to the data type.
Fragmentation Threshold	This value is the maximum size determining whether packets will be fragmented. Setting the fragmentation threshold too low may result in poor network performance since excessive packages. The default value is 2346 and it is recommended.
RTS/CTS Threshold	You can specify the request to send (RTS) threshold. The default value is 2347.

Information

Click **Information** in the **Other** field and the page shown in the following figure appears. This page displays the information of driver version, utility version, and MAC address.



3.2 Access Point Mode

Choose **Access Point** mode, the icon  will appear in the system tray. The page shown in the following figure appears.



Connect Station List: It displays the wireless adapter that is connected to the adapter.

Click **More Setting** and the **Access Point Setting** page appears.

Access Point Setting

General Connection Setting

Wireless Mode: 802.11b+g Mixed Mode

Channel: 6

SSID: WLAN_AP

☐ Hide SSID

Tx Power: Level 0 (Maximum Power)

Apply

Authentication: Open System

WEP: Disable Setting

Fragment: Disable

RTS/CTS: Disable

Preamble: Long

MAC Address Filter: Setting

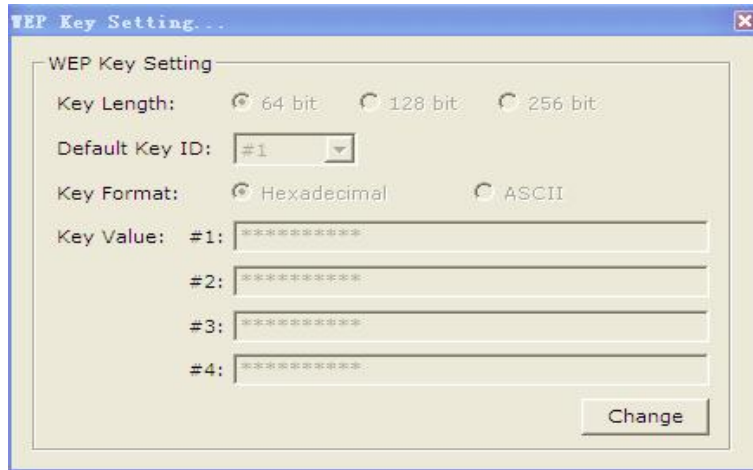
Bridge Adapter: No bridge

The following table describes the parameters of this page.

Field	Description
Wireless Mode	Choose the wireless mode.
Channel	Choose the channel.
SSID	Enter the SSID of the adapter.
Tx Power	Choose transmission power.
Authentication	Choose the authentication.
WEP	Enable or disable WEP encryption.

Field	Description
Preamble	Choose the length of message header.

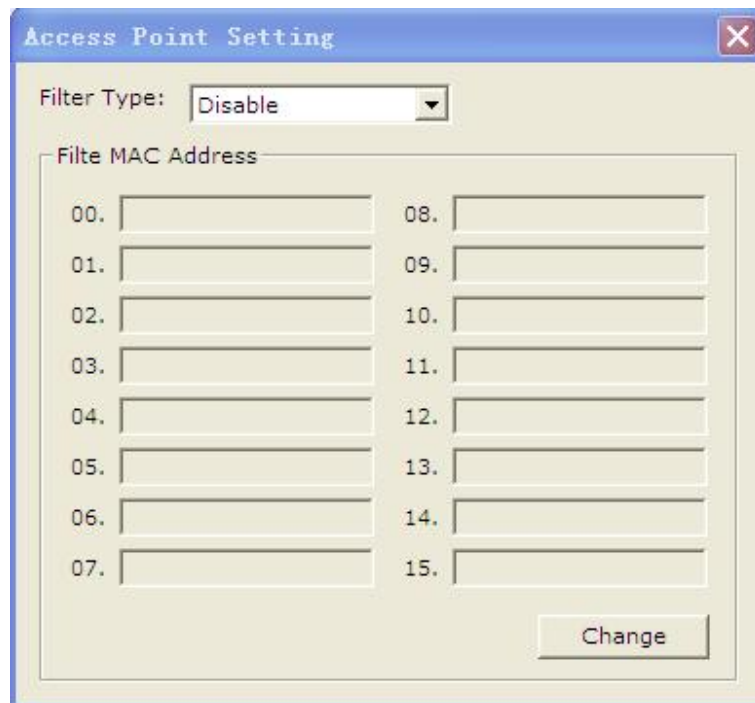
Click **Setting** in the WEP field and the **WEP Key Setting** page appears.

The image shows a 'WEP Key Setting' dialog box. It has a title bar with 'WEP Key Setting...' and a close button. Inside, there's a section titled 'WEP Key Setting'. Under 'Key Length', there are three radio buttons: '64 bit' (selected), '128 bit', and '256 bit'. Below that is a 'Default Key ID' dropdown menu showing '#1'. Under 'Key Format', there are two radio buttons: 'Hexadecimal' (selected) and 'ASCII'. Below these are four 'Key Value' input fields labeled '#1:', '#2:', '#3:', and '#4:'. Each field contains a series of asterisks. At the bottom right is a 'Change' button.

Key Value: #1, #2, #3, #4. For these key groups, you can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F) or 5 ASCII characters for 64-bit (also called 40 bits) encryption. You can also enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F) or 13 ASCII characters for 128-bit (also called 104 bits) encryption.

MAC Address Filter

Click **Setting** in the **MAC Address Filter** field and the page shown in the following figure appears. In this page, you can set the MAC address filter.



The image shows a software window titled "Access Point Setting". At the top, there is a "Filter Type:" label followed by a dropdown menu currently set to "Disable". Below this is a section titled "Filter MAC Address" which contains a grid of 16 input fields, numbered 00 through 15. The fields are arranged in two columns: the first column contains fields 00 to 07, and the second column contains fields 08 to 15. Each field is a small rectangular box. At the bottom right of the dialog, there is a "Change" button.

Filter Type:
Disable

Filter MAC Address	
00.	
01.	
02.	
03.	
04.	
05.	
06.	
07.	
08.	
09.	
10.	
11.	
12.	
13.	
14.	
15.	

Change

There are three filter types: **Disable**, **Accept**, and **Reject**.

- = If you choose **Accept**, the adapter accepts the configured MAC address.
- = If you choose **Reject**, the adapter denies the configured MAC address.

Appendix A Glossary

802.11n - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.

802.11b - The 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. 802.11b networks are also referred to as Wi-Fi networks.

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 PCs, each with a wireless adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless PCs 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.

DSSS (Direct-Sequence Spread Spectrum) - DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver 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. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).

FHSS (Frequency Hopping Spread Spectrum) - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according

to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.

Infrastructure Network - An infrastructure network is a group of PCs or other devices, each with a wireless adapter, connected as an 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.

Spread Spectrum - Spread Spectrum technology is a wideband radio frequency technique.

Appendix B Country Channel List

The following table displays the country channel list, channel classification, and range.

Country	Classification	Range
Argentina	0	CH1~11
Australia	1	CH1~13
Austria	1	CH1~13
Bahrain	1	CH1~13
Belarus	1	CH1~13
Belgium	1	CH1~13
Bolivia	1	CH1~13
Brazil	0	CH1~11
Bulgaria	1	CH1~13
Canada	0	CH1~11
Chile	1	CH1~13
China	1	CH1~13
Colombia	0	CH1~11
Costa Rica	1	CH1~13
Croatia	1	CH1~13
Cyprus	1	CH1~13
Czech Republic	1	CH1~13
Denmark	1	CH1~13
Ecuador	1	CH1~13
Egypt	1	CH1~13
Estonia	1	CH1~13
Finland	1	CH1~13
France	3	CH10~13
France2	1	CH1~13
Germany	1	CH1~13
Greece	1	CH1~13
Hong Kong	1	CH1~13
Hungary	1	CH1~13
Iceland	1	CH1~13

Country	Classification	Range
India	1	CH1~13
Indonesia	1	CH1~13
Ireland	1	CH1~13
Israel	6	CH3~9
Italy	1	CH1~13
Japan	5	CH1~14
Japan2	4	CH14~14
Japan3	1	CH1~13
Jordan	3	CH10~13
Kuwait	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1~13
Luxembourg	1	CH1~13
Macedonia	1	CH1~13
Malaysia	1	CH1~13
Mexico	0	CH1~11
Morocco	1	CH1~13
Netherlands	1	CH1~13
New Zealand	1	CH1~13
Nigeria	1	CH1~13
Norway	1	CH1~13
Panama	1	CH1~13
Paraguay	1	CH1~13
Peru	1	CH1~13
Philippines	1	CH1~13
Poland	1	CH1~13
Portugal	1	CH1~13
Puerto Rico	1	CH1~13
Romania	1	CH1~13

Country	Classification	Range
Russia	1	CH1~13
Saudi Arabia	1	CH1~13
Singapore	1	CH1~13
Slovakia	1	CH1~13
Slovenia	1	CH1~13
South Africa	1	CH1~13
South Korea	1	CH1~13
Spain	2	CH10~11
Sweden	1	CH1~13
Switzerland	1	CH1~13
Taiwan	0	CH1~11
Thailand	1	CH1~13
Turkey	1	CH1~13
United Arab Emirates	1	CH1~13
United Kingdom	1	CH1~13
United States of America	0	CH1~11
Uruguay	1	CH1~13
Venezuela	1	CH1~13
Yugoslavia	0	CH1~11

FCC Information

FCC Information

This equipment complies with CFR 47, Part 15.19 of the FCC rules. Operation of the equipment is subject to

the following 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.

This device must not be co-located or operating in conjunction with any other antenna or transmitter

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

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.

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included

in the user documentation provided with the product. Any changes or modifications (including the antennas)

made to this device that are not expressly approved by the manufacturer may void the user's authority to

operate the equipment. The manufacturer is not responsible for any radio or television interference caused by

unauthorized modification of this device, or the substitution of the connecting cables and equipment other

than manufacturer specified. It is the responsibility of the user to correct any interference caused by such

unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or

distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated

with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna,

modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF)

signal.

Safety Information

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed

and operated with minimum distance 20cm between the radiator and your body. Use only with supplied

antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate

FCC regulations.

Nanjing Z-Com Wireless Co.,Ltd.
Z-Com Building, NO. 30 Jiangsu Software Park, NO. 699-22
Xuanwu Avenue, Nanjing, China
Telephone / Fax: 025-83652821/83652899

