ZyXEL G-162/G-360

(Hardware Revision v2)

802.11b/g Wireless LAN Adapter

User's Guide

Version 1.0
May 2005

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents' rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

NOTE

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization (RMA) number. Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Please click “Product Registration” in the installation program of your support CD for online registration.

Register online at http://us.zyxel.com/ for free future product updates and information.

Federal Communications Commission (FCC) Interference Statement

FCC Certification

The United States Federal Communication (FCC) and the Canadian Department of Communications have established certain rules governing the use of electronic equipment.

Part 15, Class B

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

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 commercial environment. 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.

If this equipment does cause harmful interference to radio/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 the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Caution

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Customer Support

When contacting your Customer Support Representative, please have the following information ready:

- Product model and serial number.
- Warranty Information.
- The Date you purchased your product.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
NORTH AMERICA	support@zyxel.com	800-255-4101 714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan

[1] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Preface

Congratulations on the purchase of your new ZyXEL G-162/G-360!

About This User's Guide

This manual provides information about the ZyXEL Wireless LAN Utility.

Syntax Conventions

- "Type" or "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- Window and command choices are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font.
- The ZyXEL G-162/G-360 802.11g Wireless LAN Adapters are referred to as the ZyXEL G-162/G-360 in this guide.
- The ZyXEL Wireless LAN Utility may be referred to as the ZyXEL WLAN Utility or, simply, as the ZyXEL Utility in this guide.

Related Documentation

- Support Disk

  Refer to the included CD for support documents and device drivers.

- Quick Start Guide

  Our Quick Start Guide is designed to help you get your ZyXEL G-162/G-360 up and running right away. It contains a detailed easy-to-follow connection diagram and information on installing your ZyXEL G-162/G-360.

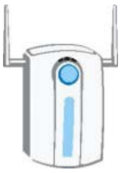
- ZyXEL Glossary and Web Site

  Please refer to www.us.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to sales@zyxel.com or send regular mail to The Technical Spport Team, ZyXEL Communications Inc., 1130 N Miller St, Anaheim, CA 92806, USA. Thank you.

Graphics Icons Key

 Wireless Access Point	 Computer	 Notebook computer
 Server	 Modem	 Wireless Signal
 Telephone	 Switch	 Router

Chapter 1 Getting Started

This chapter introduces the ZyXEL G-162/G-360 and prepares you to use the ZyXEL Utility.

1.1 About Your ZyXEL G-162/G-360

The ZyXEL G-162/G-360 is an IEEE 802.11b and 802.11g compliant wireless LAN adapters. With the ZyXEL G-162/G-360, you can enjoy wireless mobility within almost any wireless networking environment.

The following lists the main features of your ZyXEL G-162/G-360.

- Your ZyXEL G-162/G-360 can communicate with other IEEE 802.11b/g compliant wireless devices.
- Automatic rate selection.
- Standard data transmission rates up to 54Mbps.
- Proprietary transmission rates (Turbo Mode) of 22Mbps for 802.11b standard and up to 125Mbps for 802.11g standard when connected to the ZyXEL g+ access point or wireless router.
- Offers 64-bit, 128-bit and 256-bit [2]WEP (Wired Equivalent Privacy) data encryption for network security.
- Supports IEEE802.1x, WPA and WPA2 (Wi-Fi Protected Access).
- Low CPU utilization allowing more computer system resources for other programs.
- A built-in antenna for G-162 and a removable antenna with RP-SMA connector type for G-360.
- Driver support for Windows XP/2000/Me/98 SE.

1.2 ZyXEL G-162/G-360 Hardware and Utility Installation

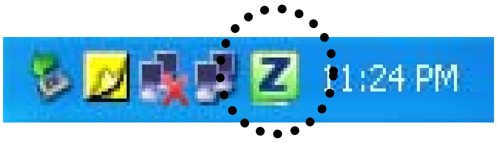
Follow the instructions in the *Quick Start Guide* to install the ZyXEL Utility and make hardware connections.

1.3 Using the ZyXEL Utility to Configure Your Network

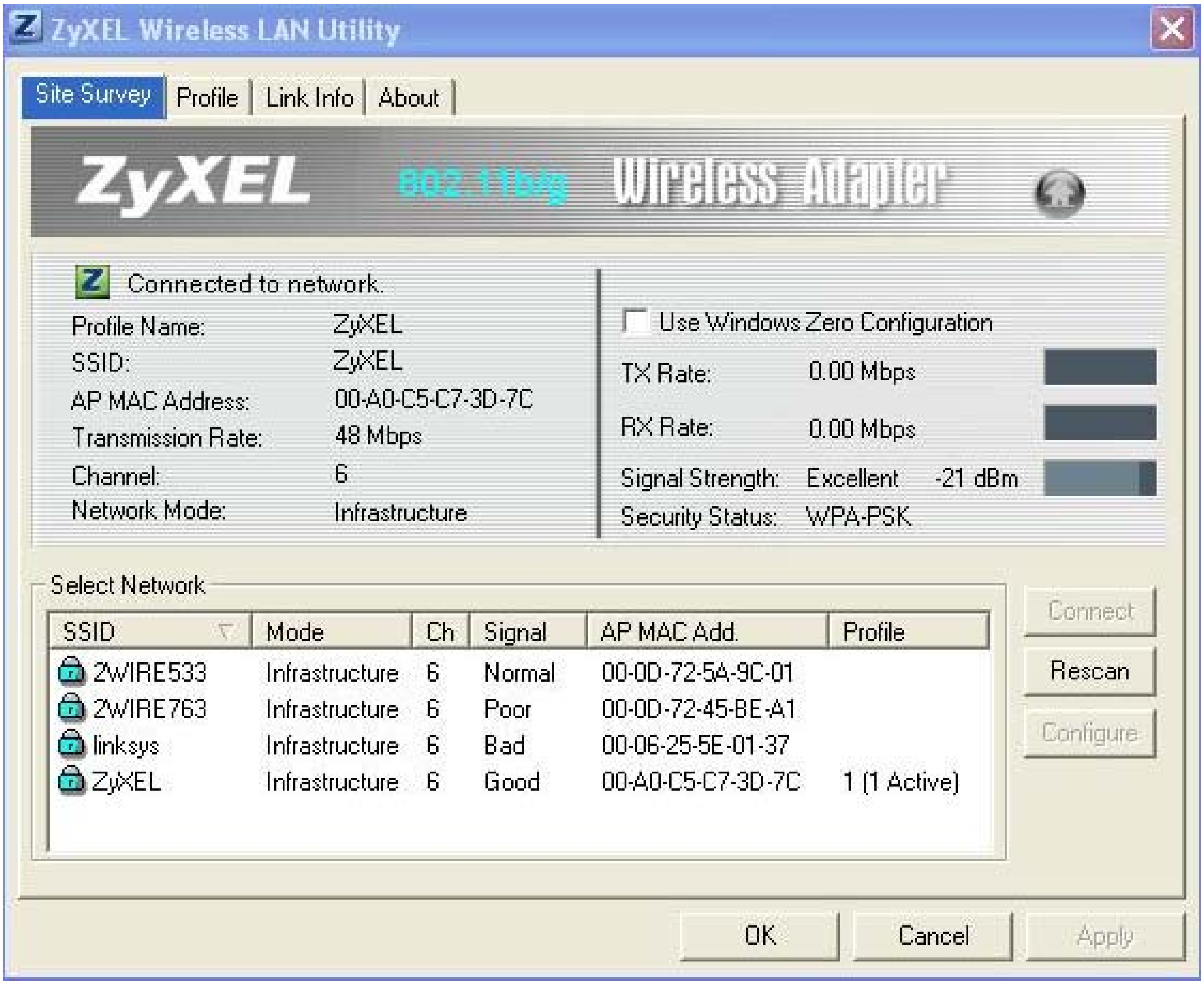
The following are explanations on how to configure and use the ZyXEL Utility program. For initial setup, please see the included Quick Start Guide.

After completing the installation procedure, a Z icon as shown below will automatically appear in the lower right tray bar.

[2] 256-bit WEP should be complied with your AP/Router's WEP setting



Double-clicking on the Z icon will display the following ZyXEL utility window.



Connected to network.

Profile Name:	ZyXEL
SSID:	ZyXEL
AP MAC Address:	00-A0-C5-C7-3D-7C
Transmission Rate:	48 Mbps
Channel:	6
Network Mode:	Infrastructure

☐ Use Windows Zero Configuration

TX Rate:	0.00 Mbps	
RX Rate:	0.00 Mbps	
Signal Strength:	Excellent	-21 dBm
Security Status:	WPA-PSK	

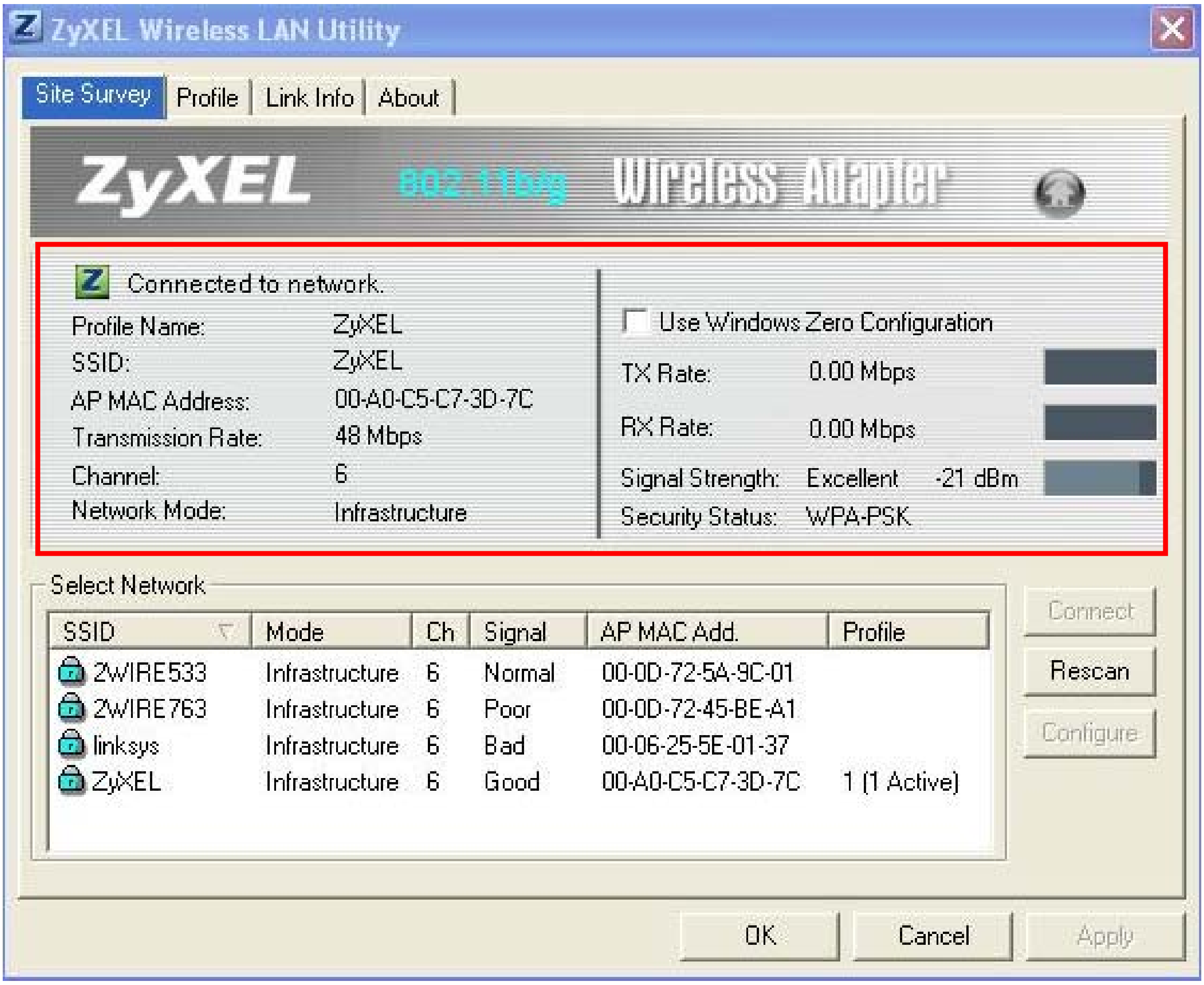
Select Network

SSID	Mode	Ch	Signal	AP MAC Add.	Profile
2WIRE533	Infrastructure	6	Normal	00-0D-72-5A-9C-01	
2WIRE763	Infrastructure	6	Poor	00-0D-72-45-BE-A1	
linksys	Infrastructure	6	Bad	00-06-25-5E-01-37	
ZyXEL	Infrastructure	6	Good	00-A0-C5-C7-3D-7C	1 (1 Active)

Each of the pages (Site Survey, Profile, Link Info, About) presented in the ZyXEL Utility are explained in the following sections.

1.3.1 Site Survey

Site Survey screen shows how the network is presently configured: network mode, information, channel, signal strength, etc. The Selected Network window shows you a list of SSIDs in your vicinity. Information regarding each SSID is also shown as Security Status, SSID, Mode, Ch, Signal, AP MAC Add and Profile.



Connected to network.

Profile Name: ZyXEL
SSID: ZyXEL
AP MAC Address: 00-A0-C5-C7-3D-7C
Transmission Rate: 48 Mbps
Channel: 6
Network Mode: Infrastructure

□ Use Windows Zero Configuration
TX Rate: 0.00 Mbps
RX Rate: 0.00 Mbps
Signal Strength: Excellent -21 dBm
Security Status: WPA-PSK

SSID	Mode	Ch	Signal	AP MAC Add.	Profile
2WIRE533	Infrastructure	6	Normal	00-0D-72-5A-9C-01	
2WIRE763	Infrastructure	6	Poor	00-0D-72-45-BE-A1	
linksys	Infrastructure	6	Bad	00-06-25-5E-01-37	
ZyXEL	Infrastructure	6	Good	00-A0-C5-C7-3D-7C	1 (1 Active)

The "Current Status" (Top Red Rectangle) windows shows the network status, Profile Name, SSID, AP MAC Address, Transmission Rate, Channel, Network Mode, TX Rate, RX Rate, Signal Strength and Security Status between the client and AP/Router.

Use Windows Zero Configuration

Checking this box will allow you to use Windows to configure your wireless network settings. When you check this box to configure, you will no longer use ZyXEL's utility.

Connect

Clicking on this bottom will guide you to the following Profile Configuration screen when you select an AP/Router to connect.

Rescan

Clicking on this bottom will scan the vicinity for a certain amount of time and display the scan results.

Configure

Clicking on this bottom will guide you to the following Profile Configuration screen when you select an AP/Router to connect.

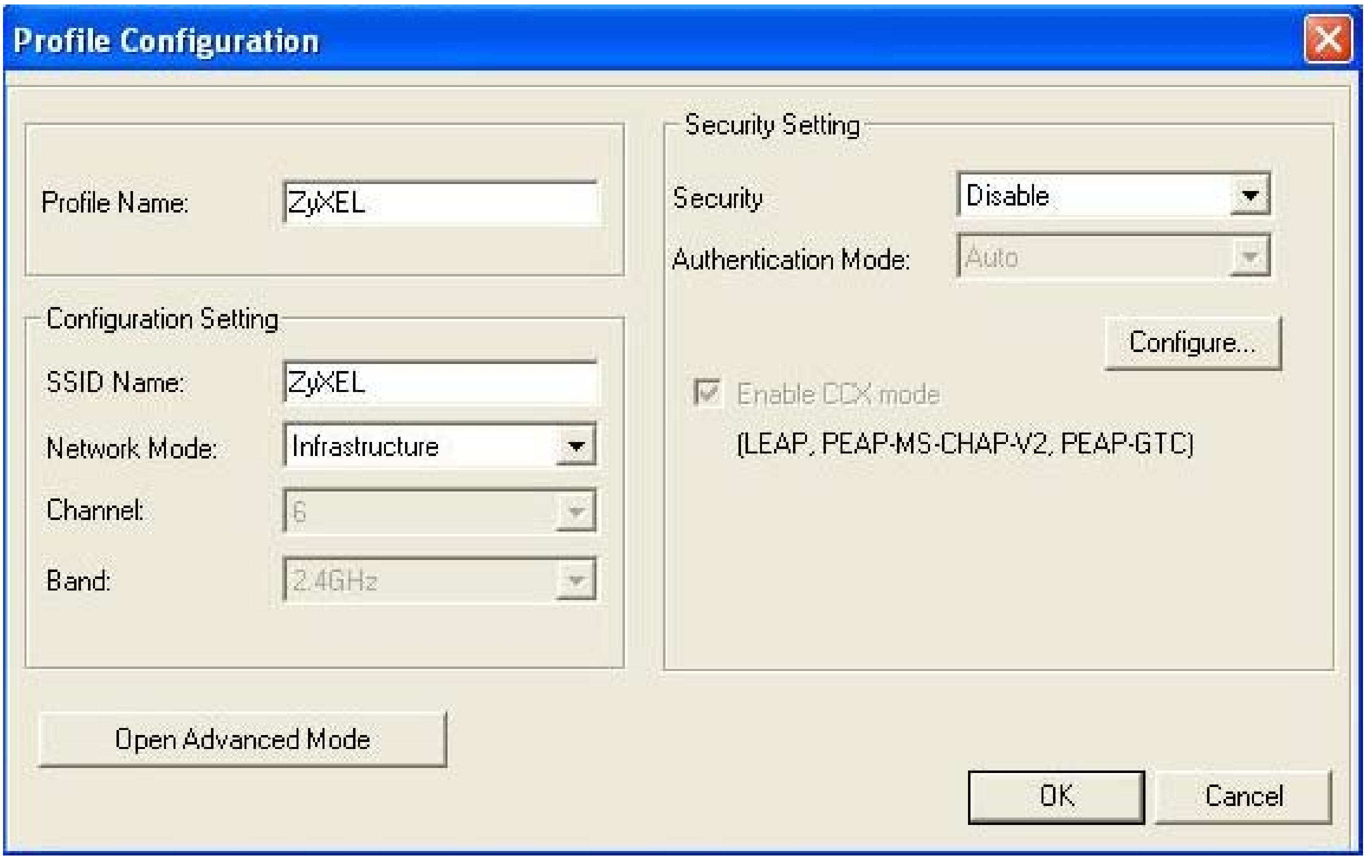
Table 1.1 Site Survey

LABEL	DESCRIPTION
Wireless Network Status	
Profile Name	This is the name of the profile you are currently using.
Network Name	The SSID identifies the Service Set to which a wireless station is associated. This
Security Logo	Unlock logo displays no security.
AP MAC Address	This field displays the MAC address of the wireless device to which the G-162/G-
Transmission Rate	This field displays the current data transmission rate in Megabit per seconds
Channel	This field displays the radio channel the G-162/G-360 is currently using.
Network Mode	This field displays the network type (Infrastructure (BSS) or Ad Hoc) of the

	should use the same SSID (whatever your choice is).
TX Rate	This field displays the current data transmission rate in Megabit per second (Mbps).
RX Rate	This field displays the current data receiving rate in Megabit per second (Mbps).
Signal Strength	This shows the strength of the signal (the range from Excellent, Good, Normal, Bad, Poor, No signal, which relate to the dBm)
Security Status	This field displays whether data encryption is activated (No Security, WEP, WEP+ 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK)

Profile Configuration allow you to insert some basic setting for your wireless mode

1) Click on [Configure] and the following screen will appear



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

Security: Disable

Authentication Mode: Auto

☑ Enable CCX mode

(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

2) On this screen you will insert some basic settings on your left for your wireless network.

a. [Profile] Default profile name is ZyXEL. You may also enter in a descriptive name for this profile.

b. [SSID Name] is depends on the AP/Router you connect to from Site Survey page.

c. [Network Mode] if connecting to an AP/Router, choose "Infrastructure". If you are going to network one computer directly to another computer without an AP/Router, then choose "Ad Hoc".

d. [Channel] is set default auto channel for the Infrastructure mode and default Ch6 for Ad-Hoc mode.

e. [Band] shows you 802.11b and 802.11g on the 2.4GHz.

f. [Security] will vary in appearance depending on whether any encryption was detected with your AP/Router. Select the appropriate security information.

g. Click [OK]. Your setting will be saved and apply.

2.1) Security Setting is on your right and the screen will vary in appearance depending on whether any encryption was detected with your AP/Router. Please enter in the appropriate security information.

[Security] shows you different types of security modes.

a. Disable

It represents no security. All data sent between the AP and the client is left unencrypted and may be viewed by other wireless devices.

b. WEP

Wired Equivalent Privacy – Encrypts all traffic sent between the AP and the client using a shared key. When using WEP encryption (available in 64, 128, or 256-bit[3]), only those APs and PCs using the same WEP Key are allowed to communicate with each other.

c. WPA-PSK

WPA-PSK is designed for home users. Like WEP, it uses a pre-shared key that every user of the network must have in order to be able to send and receive data. Like WPA, it uses TKIP, which improves greatly over the encryption found in WEP.

d. WPA2-PSK

WPA2-PSK is designed for home users. Like WEP, it uses a pre-shared key that every user of the network must have in order to be able to send and receive data. Like WPA, it uses AES, which improves greatly over the encryption found in WEP.

We recommend you use WPA-PSK/WPA2 or WPA-PSK/WPA2-PSK whenever possible.

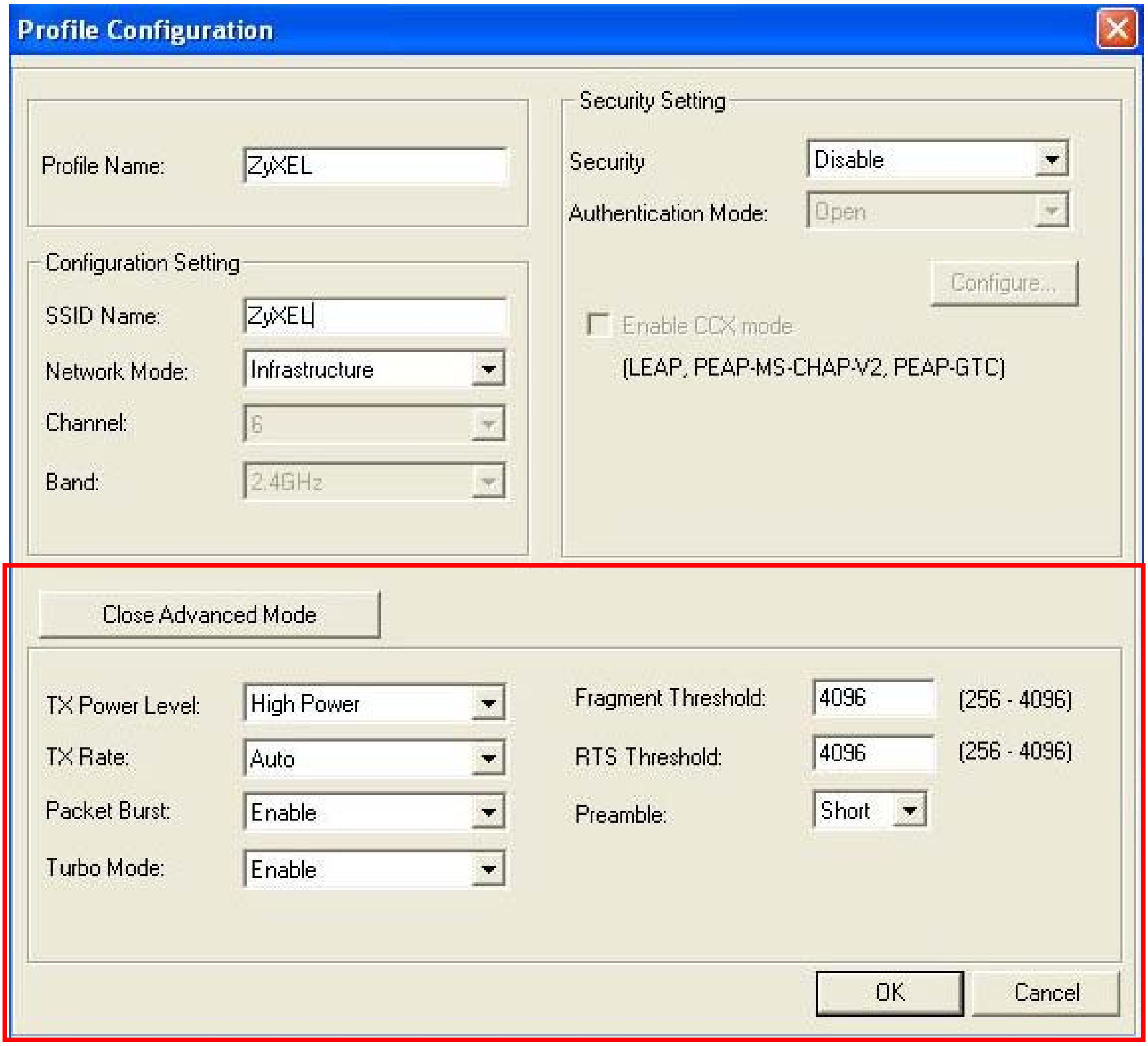
For the detail security setting, please refer to Chapter 4—Configuring Wireless Security.

[1] 256-bit WEP shall be complied with your AP/Router's WEP setting.

2.2) [Enable CCX Mode] refers the Cisco Compatible Extension, which is the certificate-based authentications (EAP-TLS, PEAP and LEAP) using dynamic keys for data encryption. Check this box will enable PEAP-MS-CHAP-V2, PEAP-GTC, TLS and LEAP. Please see your MIS administrator for these settings when you are about to enable one of these mode. Please refer to Ch4—Configuring Wireless Security for detail WEP-802.1x and WPA-802.1x authentication information. Also, please see the User Guide of Funk Odyssey software for more WPA-enterprise security settings.

2.3) [Authentication Mode] includes PEAP-MS-CHAP-V2, PEAP-GTC, TLS and LEAP. Please refer to Chapter 4—Configuring Wireless Security for the detail authentication information.

Advanced Mode: This screen (Bottom Red Rectangle) allows you to make changes to the default ways the card operates including advanced 802.11 settings. Unless you are an advanced user and have deep knowledge about each property on this page, it is recommended that you leave them at the default settings. For more information, please refer to section 2.3 and 2.4.



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

Security: Disable

Authentication Mode: Open

□ Enable CCX mode

(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

TX Power Level: High Power

TX Rate: Auto

Packet Burst: Enable

Turbo Mode: Enable

Fragment Threshold: 4096 (256 - 4096)

RTS Threshold: 4096 (256 - 4096)

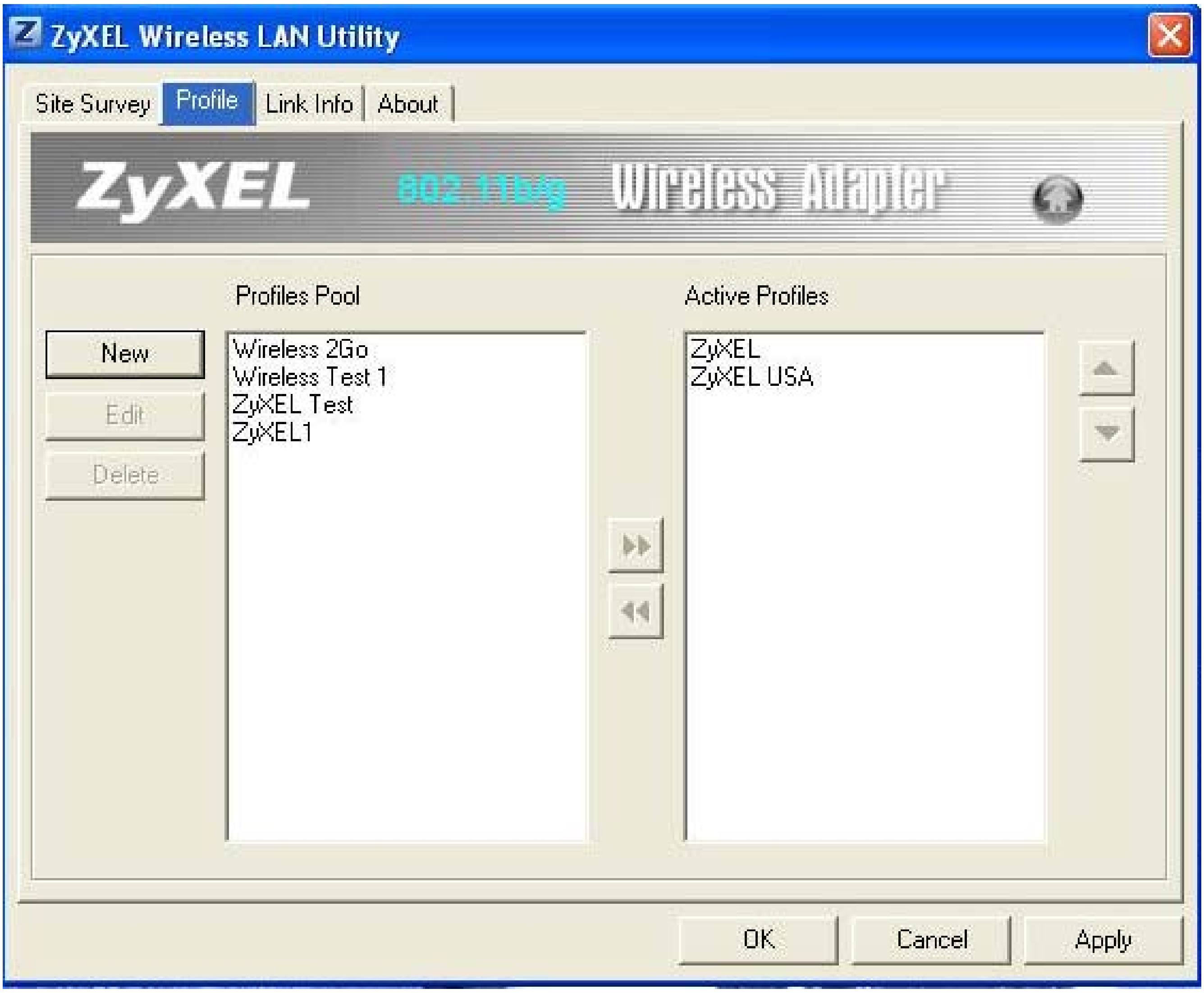
Preamble: Short

[Turbo Mode] allows you either "Active" or "Inactive" the 22Mbps and 125Mbps. The information will be also shown under Link Info screen. Please refer to 1.1.3 Link Info for the detail explanation.

[Packet Burst] allows you either "Active" or "Inactive" the packet burst. The information will be also shown under Link Info screen. Please refer to 1.1.3 Link Info for the detail explanation.

1.3.2 Profile

Profile screen enables you to create, edit and delete the profiles that the adapters used to connect AP/Router.



Profiles Pool

Wireless 2Go
Wireless Test 1
ZyXEL Test
ZyXEL1

Active Profiles

ZyXEL
ZyXEL USA

Explanation of each button in this page is shown below.

Profile Pool

A list of inactive profiles, which are not currently connected to AP/Router. Default profile name is set "ZyXEL". You can add new profile by clicking [New], modify profile by clicking [Edit] and delete it by clicking [Delete].

Active Profiles

1) A list of active profiles, which are currently connected to AP/Router. Each profile in the Active Profiles list has a priority based on its location on the list.

2) The higher in the list, the higher priority. When you connect the ZyXEL G-162/G-360 to AP/Router with a specific SSID, they will try to connect the AP/Router listed on the highest priority. If the connection is failed, it will connect to the second highest one. You can also select which AP/Router you want to connect to by clicking [up arrow] or [down arrow].

3) You may select AP/Router under the Profile Pool to the Active Profiles by clicking [right arrow]; likewise, clicking [left arrow] will move the AP/Router under the Active Profiles to the Profile Pool.

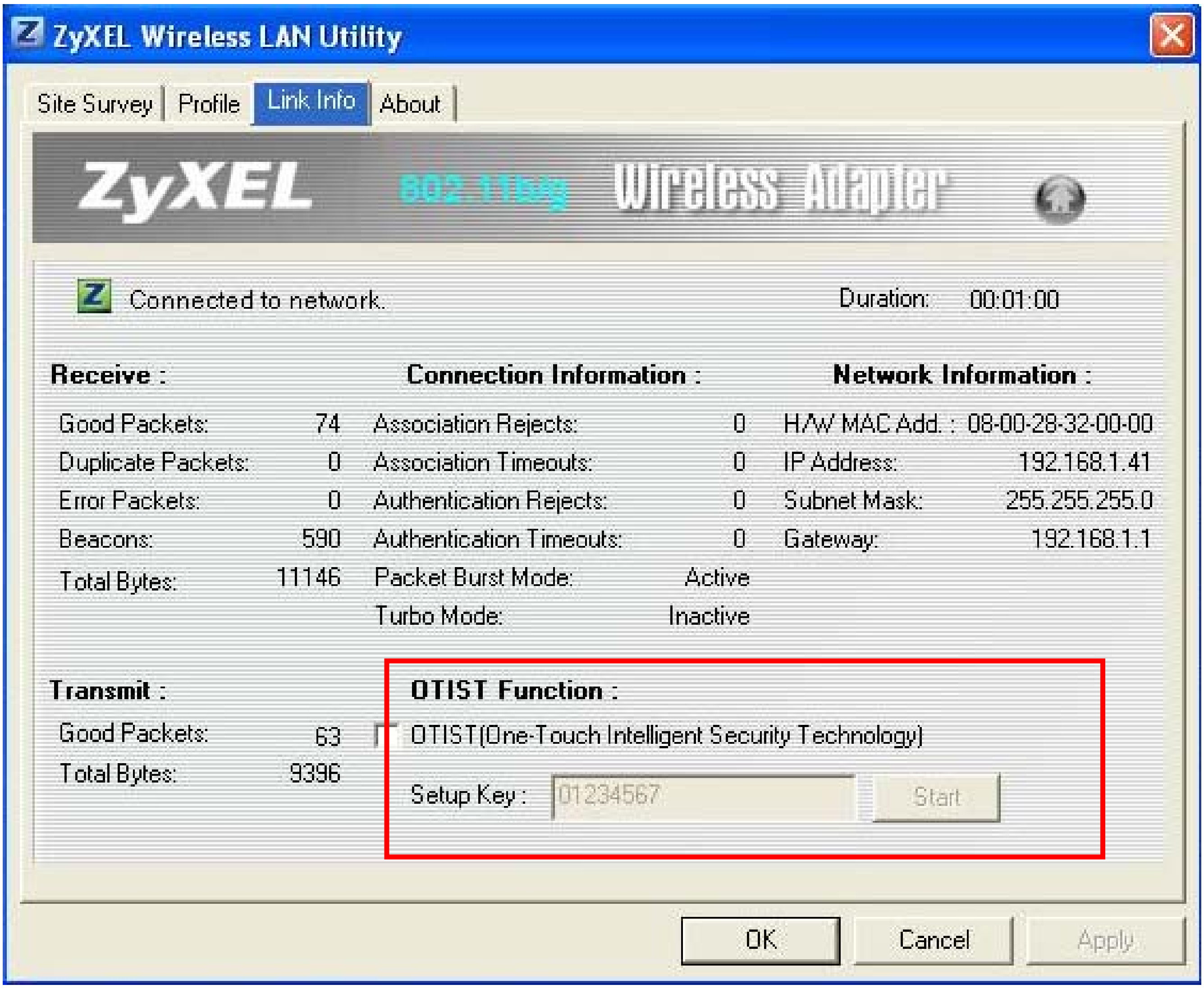
4) Click [Apply] will configure the profile you select.

Also, when you finish the settings under the *Profile Configuration*, please go back to **Profile** screen and select the AP/Router you will connect to and then click [Apply] to active the connection.

1.3.3 Link Info

Link Info screen shows the current configuration and connection status of your G-162/G-360.

The Link Info shows you the information including Receive, Transmit, Connection Information, Network information and OTIST.



Connected to network. Duration: 00:01:00

Receive :

Good Packets: 74
Duplicate Packets: 0
Error Packets: 0
Beacons: 590
Total Bytes: 11146

Connection Information :

Association Rejects: 0
Association Timeouts: 0
Authentication Rejects: 0
Authentication Timeouts: 0
Packet Burst Mode: Active
Turbo Mode: Inactive

Network Information :

H/W MAC Add. : 08-00-28-32-00-00
IP Address: 192.168.1.41
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

Transmit :

Good Packets: 63
Total Bytes: 9396

OTIST Function :

□ OTIST(One-Touch Intelligent Security Technology)

Setup Key : 01234567 Start

OTIST Function (Above Red Rectangle)

OTIST (One Touch Intelligent Security Technology) is the ZyXEL proprietary one bottom security technology. You must have the ZyXEL P-334WT router or other ZyXEL AP/Router supporting OTIST to set the wireless adapter to use the same wireless settings.

1. Check this box to enable OTIST
2. [Setup Key] Enter the same setup key (of exactly eight ASCII characters) as the ZyXEL P-334WT router or other ZyXEL AP/Router to which you want to associate. The default OTIST setup key is "01234567".

If you change the OTIST setup key on the ZyXEL P-334WT or other ZyXEL Routers supporting OTIST, you must also make the same change here.

3. Click [Start] to encrypt the wireless security data using the setup key and have the ZyXEL g+ AP or wireless router set your G-162/G-360 to use the same wireless settings as the ZyXEL g+ AP or wireless router at the same time. Please see the section for OTIST information.

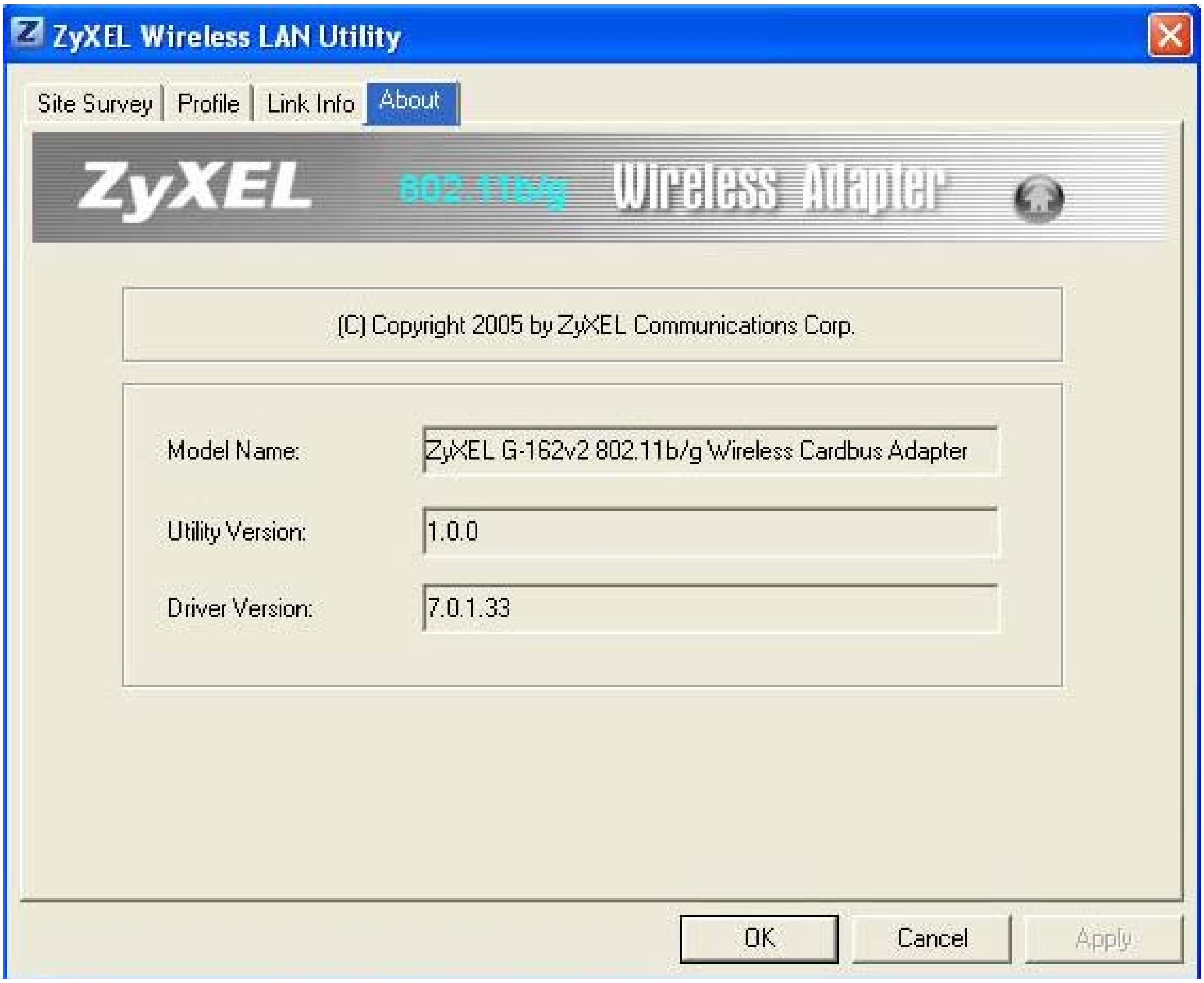
Table 1.2 Link Info

Link Status	Green Z icon displays "Connected to Network"
Duration	This field displays the period when users enable the connection.
Receive	
Good Packets	This field displays the total number of complete, uninterrupted, and
Duplicate Packets	This field displays the total number of duplicated data received.
Error Packets	This field displays the total number of incomplete, delayed or interrupted,
Beacons	This field displays a frame or message set by an adapter indicating a serious
Total Bytes	This field displays the total number of bytes received

Transmit	
Good Packets	This field displays the total number of good packets transmitted
Total Bytes	This field displays the total number of bytes transmitted
Connection Information	
Association Rejects	This field displays the total number of rejections when connecting between Access Point/Router and your adapter.
Association Timeouts	This field displays the total number of associations when connecting between AP/Router and your adapter failed after the certain period of time.
Authentication Rejects	This field displays the total number of rejections that occur during the authentication process
Authentication Timeouts	This field displays the total number of authentications when connecting between AP/Router and your adapter failed after certain period of time.
Packet Burst Mode	This is referring to an optional mode of transmitting data. Burst mode can significantly improve network performance because it allows more data to be sent without waiting for receiver acknowledgments. This field displays "Active" when enabling Packet Burst Mode. This field displays "Inactive" when disabling Packet Burst Mode.
Turbo Mode	This field displays "Active" when enabling either 22Mbps or 125Mbps. This field displays "Inactive" when disabling either 22Mbps or 125Mbps.
Network Information	
This section displays adapter's Hardware MAC Add, IP Address, Subnet Mask and Gateway information.	

1.3.4 About

About screen shows you the product name and software information of the current client device (G-162 or G-360) you are using.



(C) Copyright 2005 by ZyXEL Communications Corp.

Model Name: ZyXEL G-162v2 802.11b/g Wireless Cardbus Adapter

Utility Version: 1.0.0

Driver Version: 7.0.1.33

ZyXEL Website

Clicking 🏠, You can go to ZyXEL US website for upgrading driver, utility and updating user's guide as well as registering products.

Chapter 2
Wireless LAN Networking

This chapter provides background information on general wireless LAN networking technology and terminology.

2.1 Overview

This section describes the wireless LAN network terms and applications.

2.1.1 SSID

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

2.1.2 Channel

A radio frequency used by a wireless device is called a channel.

2.1.3 Transmission Rate (Transfer Rate)

The ZyXEL G-162/G-360 provides various transmission (data) rate options for you to select. Options include **Fully Auto**, **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **6 Mbps, 11 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps and 54 Mbps** and **125Mbps**. In most networking scenarios, the factory default **Fully Auto** setting proves the most efficient. This setting allows your ZyXEL G-162/G-360 to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the ZyXEL G-162/G-360 automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the ZyXEL G-162/G-360 gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

2.1.4 Wireless Network Application

Wireless LAN works in either of the two modes: ad-hoc and infrastructure.

To connect to a wired network within a coverage area using Access Points (APs), set the ZyXEL G-162/G-360 operation mode to **Infrastructure (BSS)**. An AP acts as a bridge between the wireless stations and the wired network. In case you do not wish to connect to a wired network, but prefer to set up a small independent wireless workgroup without an AP, use the **Ad-hoc (IBSS)** (Independent Basic Service Set) mode.

Ad-Hoc (IBSS)

Ad-hoc mode does not require an AP or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

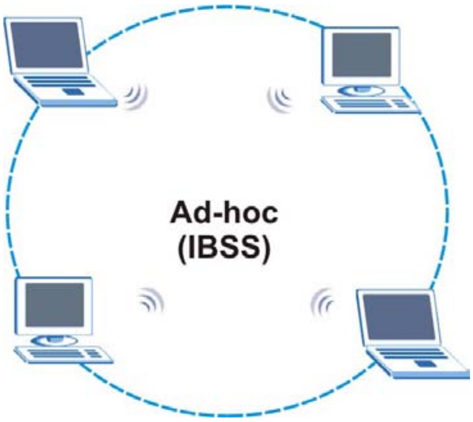


Figure 2-1 IBSS Example

To set up an ad-hoc network, configure all wireless stations in ad-hoc network type and use the same SSID and channel.

Infrastructure (BSS)

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

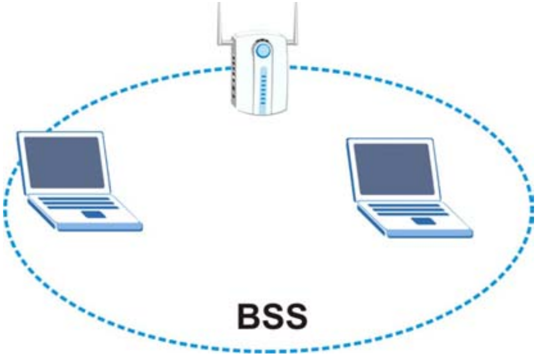


Figure 2-2 BSS Example

A series of overlapping BSS and a network medium, such as an Ethernet forms an Extended Service Set (ESS) or infrastructure network. All communication is done through the AP, which relays data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resource, such as the printer, on the wired network.

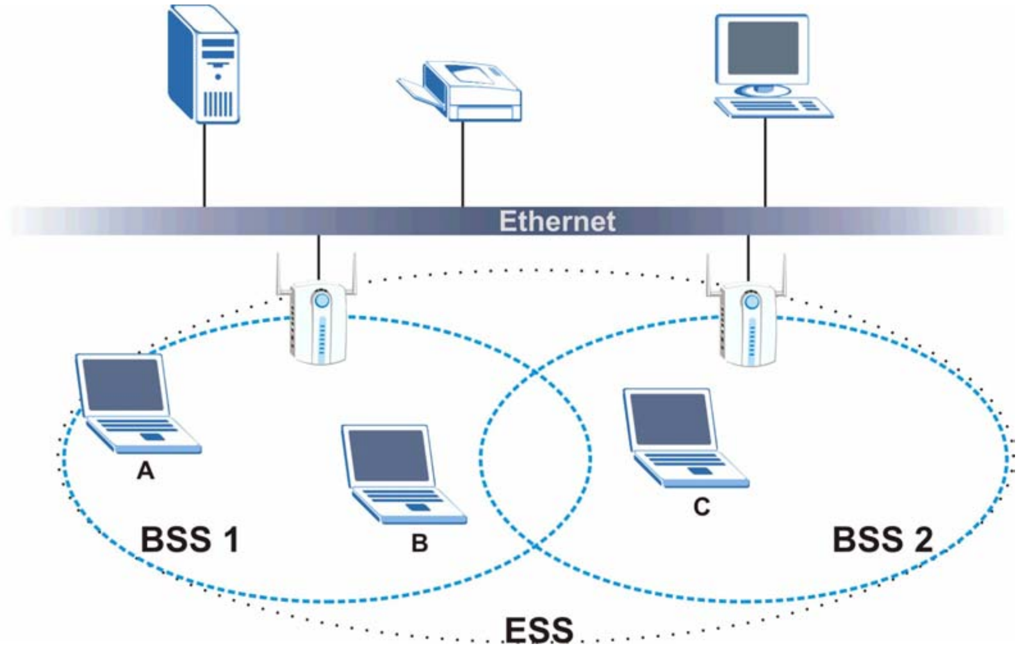


Figure 2-3 Infrastructure Network Example

2.1.5 Roaming

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization or other factors.

The following figure depicts a roaming example. When wireless station **B** moves to position **X**, the ZyXEL G-162/G-360 in wireless station **B** automatically switches the channel to the one used by access point **2** in order to stay connected to the network.

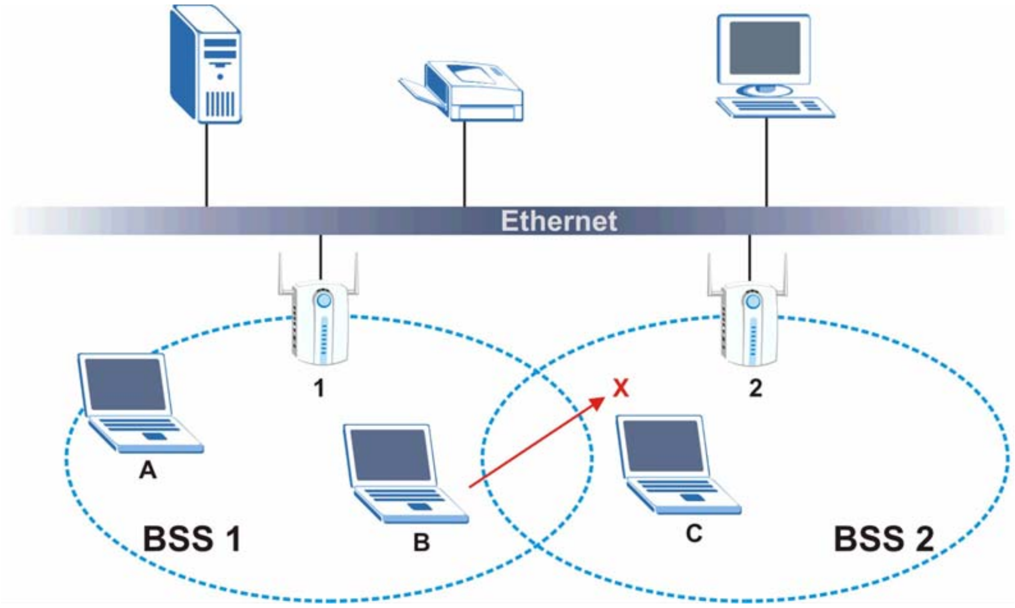


Figure 2-4 Roaming Example

2.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communication between wireless stations and the wired network.

The figure below shows the possible wireless security levels on your ZyXEL G-162/G-360. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

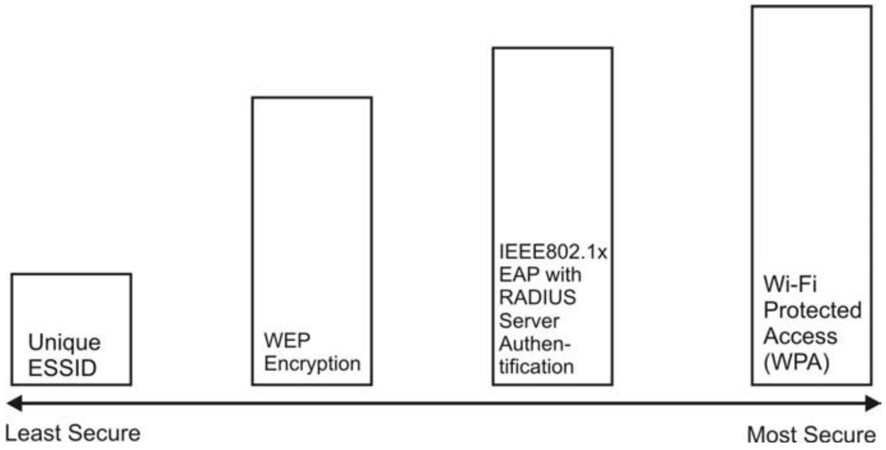

Unique ESSID
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authentication
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

Figure 2-5 Wireless LAN Security Levels

Configure the wireless LAN security using the **Profile Security Settings** screen. If you do not enable any wireless security on your ZyXEL G-162/G-360, the ZyXEL G-162/G-360’s wireless communications are accessible to any wireless networking device that is in the coverage area.

2.2.1 Data Encryption with WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the ZyXEL G-162/G-360 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your ZyXEL G-162/G-360.

- Automatic WEP key generation based on a “password phrase” called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
  For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the ZyXEL Utility and entering them manually as the WEP keys in the other WLAN adapter(s).
- Enter the WEP keys manually.

Your ZyXEL G-162/G-360 allows you to configure up to four 64-bit, 128-bit or 256-bit[4] WEP keys and only one key is used as the default key at any one time.

2.2.2 WPA-PSK and WPA2-PSK Application Example

A WPA-PSK/WPA-PSK2 application looks as follows.

Step 1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

Step 2. The AP checks each client’s password and (only) allows it to join the network if it matches its password.

Step 3. The AP derives and distributes keys to the wireless clients.

Step 4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

[4] 256-bit WEP shall be complied with your AP/Router’s WEP setting.

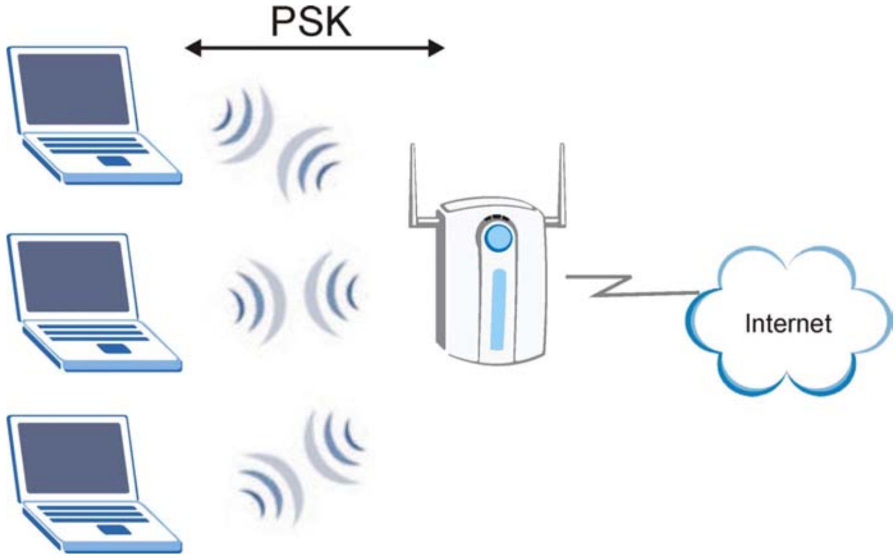


Figure 2-6 WPA-PSK/WPA2-PSK Authentication

2.2.3 WPA and WPA2 with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA/WPA2 application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

Step 1. The AP passes the wireless client's authentication request to the RADIUS server.

Step 2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

Step 3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

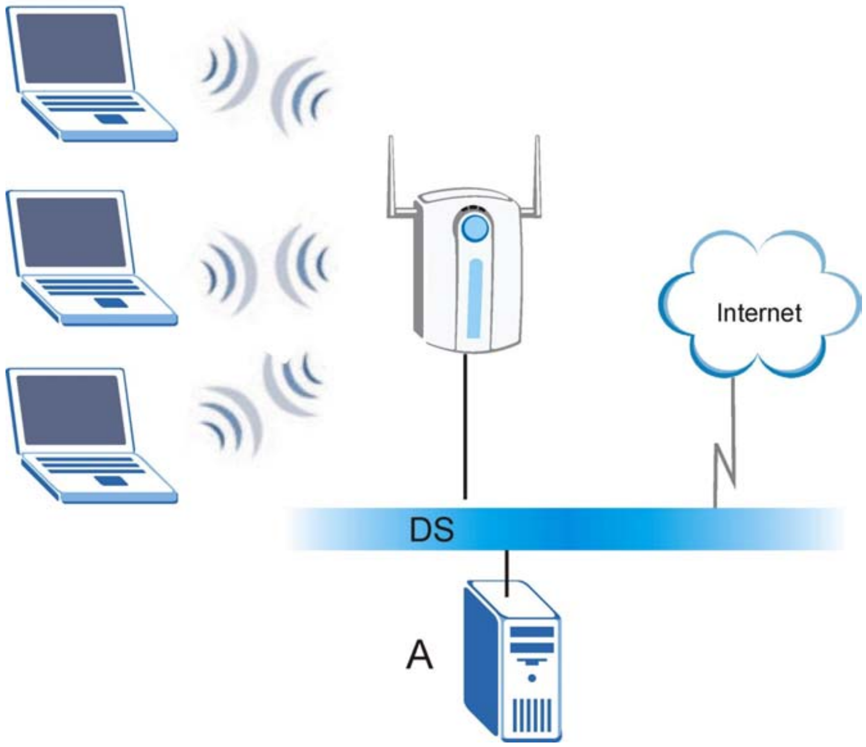


Figure 2-7 WPA/WPA2 with RADIUS Application Example

2.2.4 IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE802.1x. The ZyXEL G-162/G-360 supports EAP-TLS, EAP-TTLS and EAP-PEAP.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

2.3 Fragmentation Threshold

The **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyXEL G-162/G-360 will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS Threshold** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS Threshold** size.

2.4 RTS/CTS Threshold

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

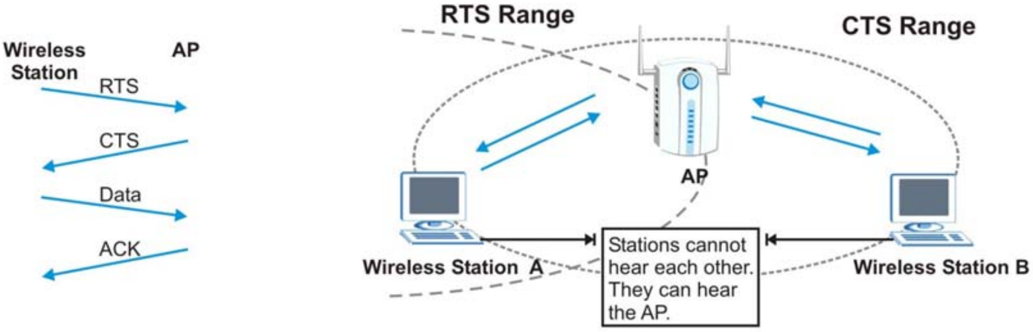


Figure 2-8 RTS Threshold

When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS Threshold is designed to prevent collisions due to hidden nodes. An **RTS/CTS Threshold** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS Threshold** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS Threshold** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS Threshold** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS Threshold** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS Threshold** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance.

2.5 OTIST (One Touch Intelligent Security Technology)

OTIST (One Touch Intelligent Security Technology) is the ZyXEL proprietary one bottom security technology. You must have the ZyXEL P-334WT router or other ZyXEL AP/Router supporting OTIST to set the wireless adapter to use the same wireless settings.

The wireless adapter must also support OTIST and have OTIST enabled.

The following are the wireless settings that the ZyXEL P-334WT or other ZyXEL AP/Router supporting OTIST assigns to the wireless adapter if OTIST is enabled on both devices and the OTIST setup keys are the same.

→SSID

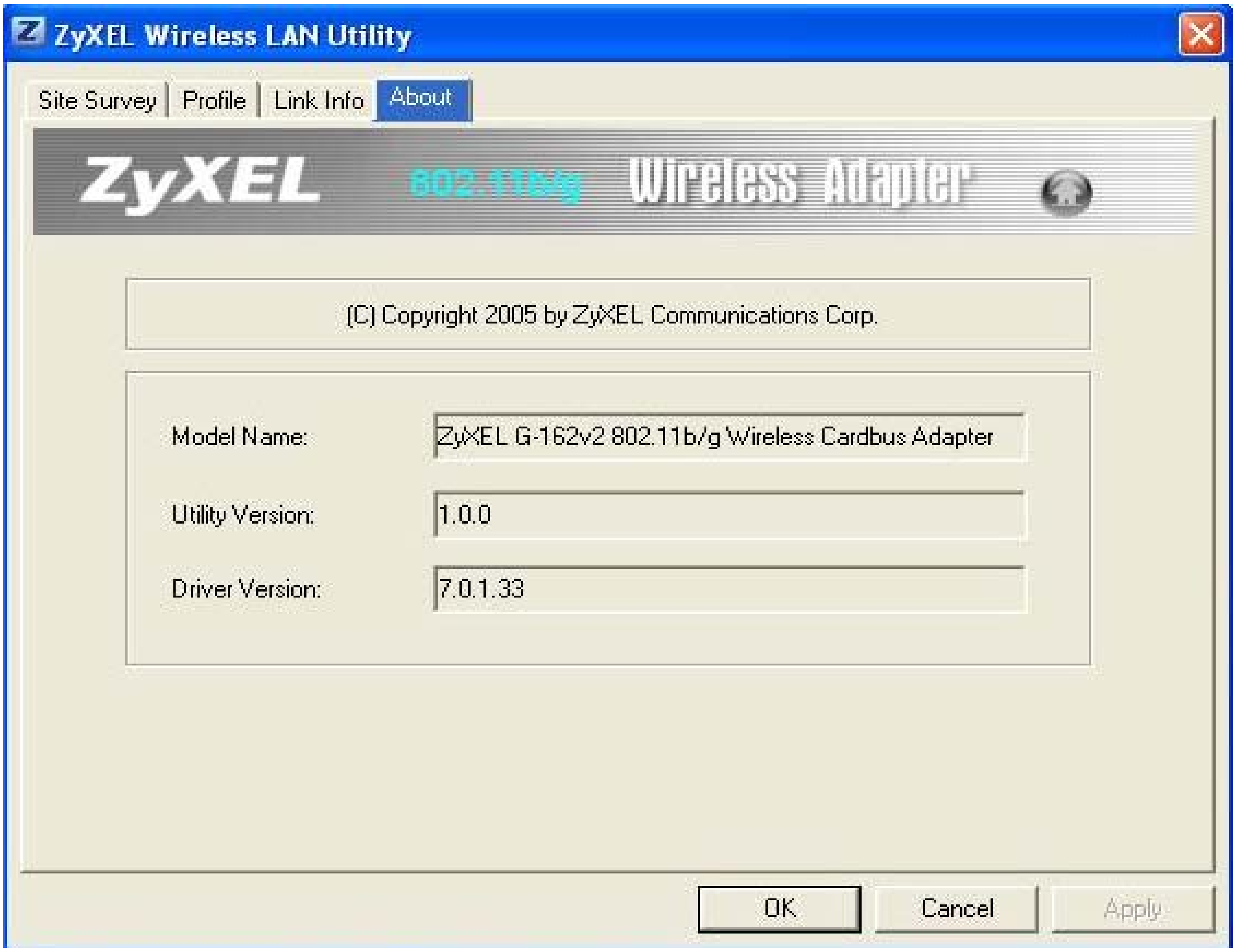
→Security (WEP or WPA-PSK)

Chapter 3 Maintenance

This chapter describes how to uninstall or upgrade the ZyXEL Utility and Driver.

3.1 The About Screen

About screen displays related version numbers of the ZyXEL Wireless LAN Adapter (G-162 or G-360). When you contact ZyXEL for the tech support, please tell us the utility and driver version as follows.



(C) Copyright 2005 by ZyXEL Communications Corp.

Model Name: ZyXEL G-162v2 802.11b/g Wireless Cardbus Adapter

Utility Version: 1.0.0

Driver Version: 7.0.1.33

The following table describes the read-only fields in this screen.

About

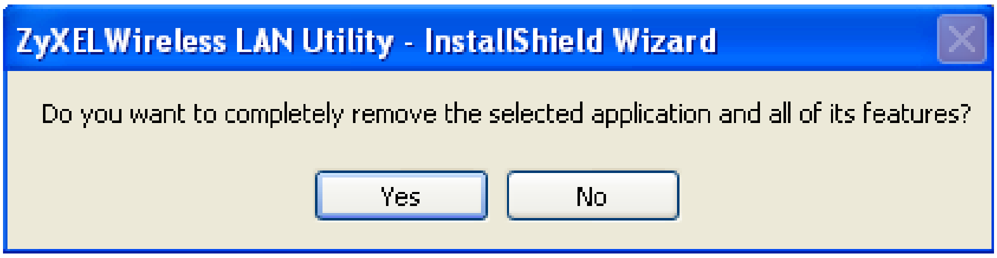
LABEL	DESCRIPTION
Model Name	This field displays the device's model name.
Driver Version	This field displays the version number of the ZyXEL driver.
Utility Version	This field displays the version number of the ZyXEL utility.

3.2 Uninstalling the ZyXEL Utility

Follow the steps below to remove (or uninstall) the ZyXEL Utility from your computer.

Step 1. Click **Start**, **Programs, ZyXEL G-162v2&G-360v2 Utility, Uninstall.**

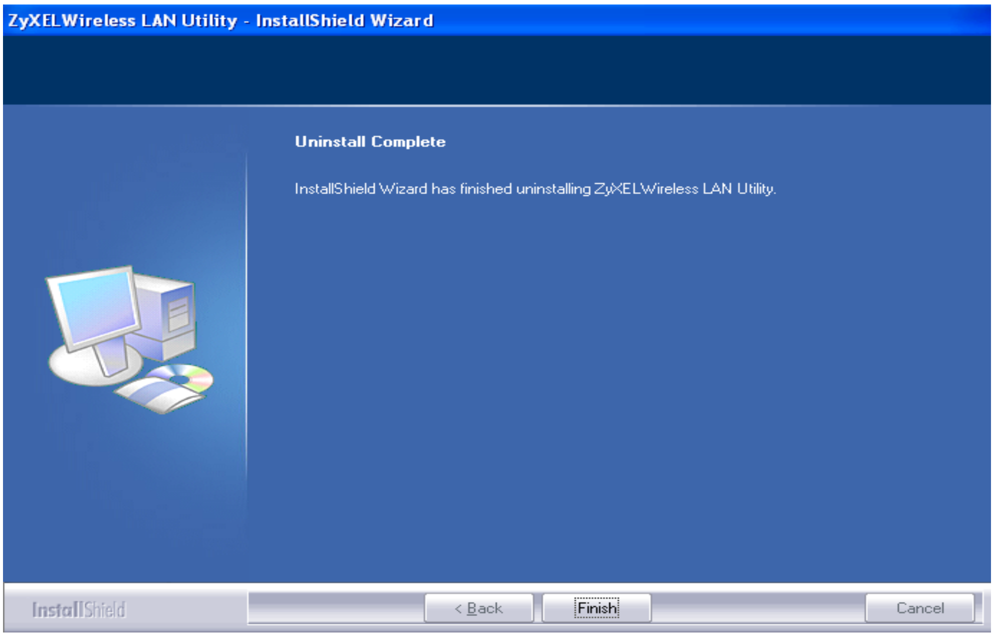
Step 2. When prompted, click [Yes] to remove the driver and the utility software.



ZyXELWireless LAN Utility - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

Step 3. Click [Finish] to finish the uninstall process. Reboot your computer if prompted to do so.



ZyXELWireless LAN Utility - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling ZyXELWireless LAN Utility.

3.3 Upgrading the ZyXEL Utility

Before you uninstall the ZyXEL G-162/G-360v2 Utility, take note of the current network configuration.

To perform the upgrade, follow the steps below.

Step 1. Download the latest version of the utility from the ZyXEL web site and save the file on your computer.

Step 2. Follow the steps in *Section 3.2* to remove the current ZyXEL Utility from your computer.

Step 3. Restart your computer if prompted.

Step 4. After restarting, refer to the procedure in the *Quick Start Guide* to install the new utility.

Step 5. Check the version numbers in the **About** screen to make sure the new utility is installed properly.

Chapter 4 Configuring Wireless Security

This chapter covers the configuration of security options in the ZyXEL Utility.

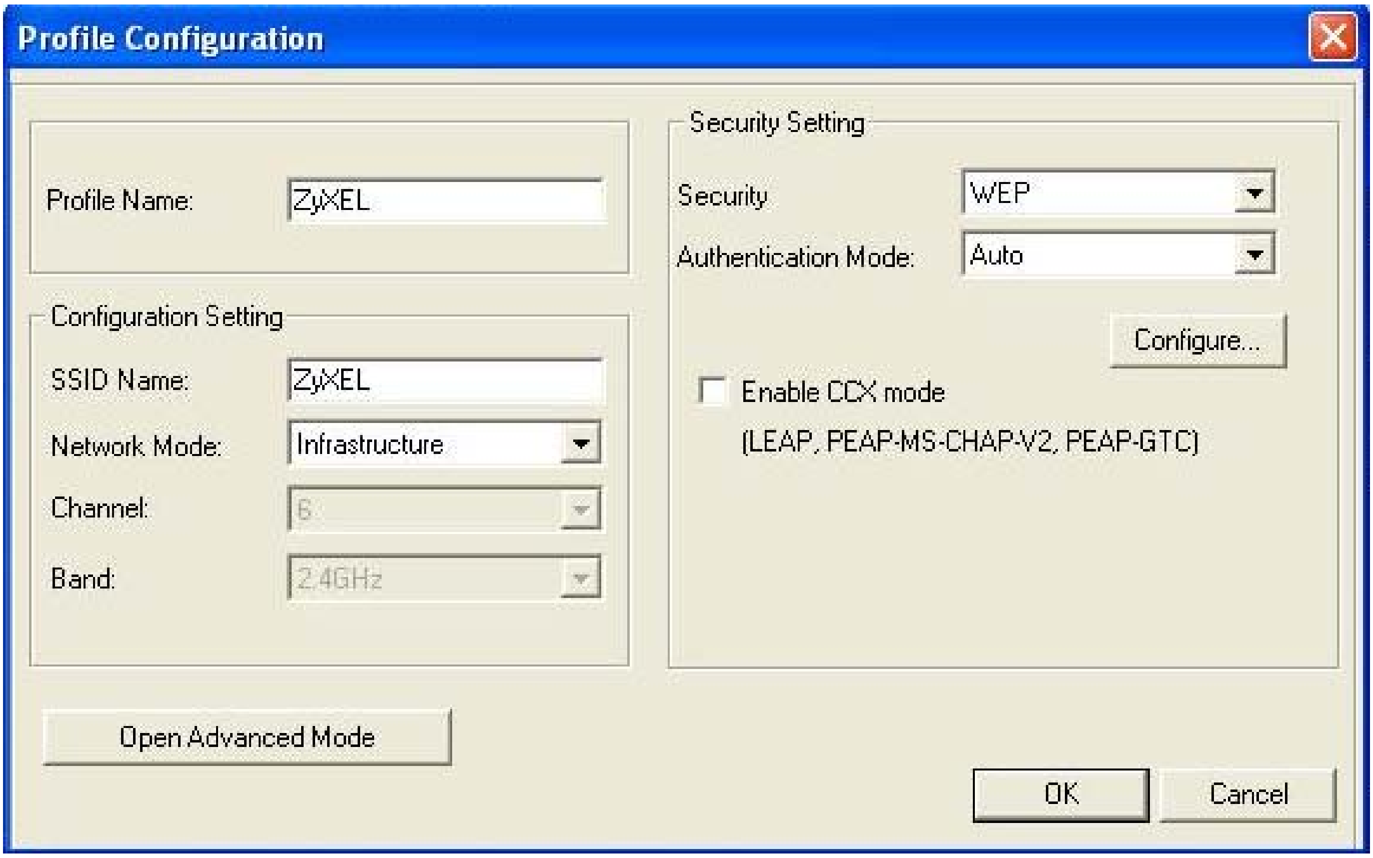
4.1 Configuring Security

You can configure your security settings at any time. Simply select the wireless AP/Router found under Site Survey, double click to land the *Profile Configuration* screen and then select [Security]. You are also presented with the option to configure security under the *Profile* creation process and double click the AP/Router you will connect to and then select [Security]. Whether changing the security settings of an existing profile or creating a new profile, the steps to configure your security settings remain the same. You also need to know the security settings of the AP/Router you will connect to and follow its setting.

When you configure the following security settings, you need to check and follow your AP/Router settings. If your adapter's setting is not complied with the AP/Router, it will fail to connect the network.

In addition, for users who need enhanced security settings for WPA, WPA-PSK and 802.1x as well as connecting from the wireless client to the corporate RADIUS server, you need to install Funk Odyssey Client software as well. Please see the User Guide of Funk Odyssey Client software.

4.2 Configuring WEP



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

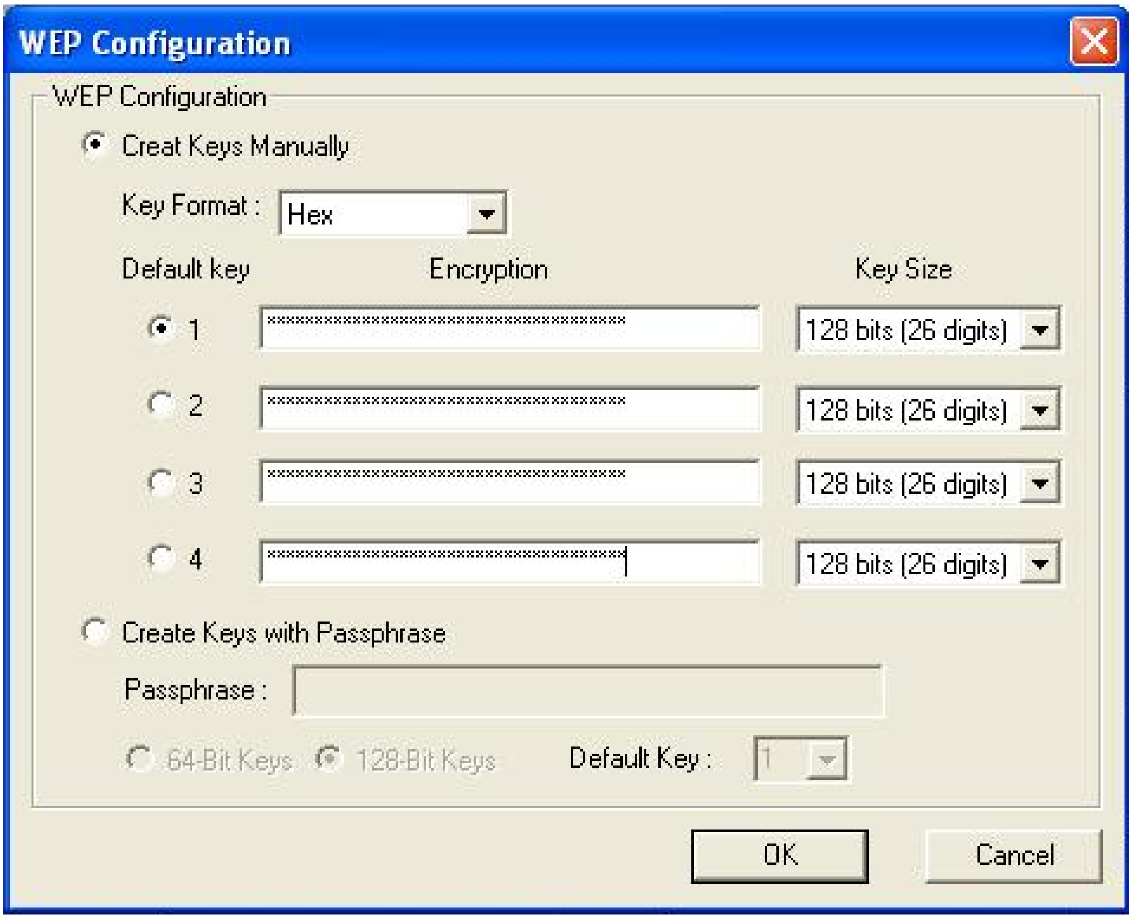
Band: 2.4GHz

Security Setting

Security: WEP

Authentication Mode: Auto

1. Select [WEP] under [Security]
2. Select [Auto] under [Authentication Mode]
3. Click [Configure]. You will then see the screen below.
4. Keep [Auto] in Authentication Mode, which depending on AP/Router's Authentication Mode.



WEP Configuration

WEP Configuration

● Creat Keys Manually

Key Format : Hex

Default key	Encryption	Key Size
● 1	**	128 bits (26 digits)
○ 2	**	128 bits (26 digits)
○ 3	**	128 bits (26 digits)
○ 4	**	128 bits (26 digits)

○ Create Keys with Passphrase

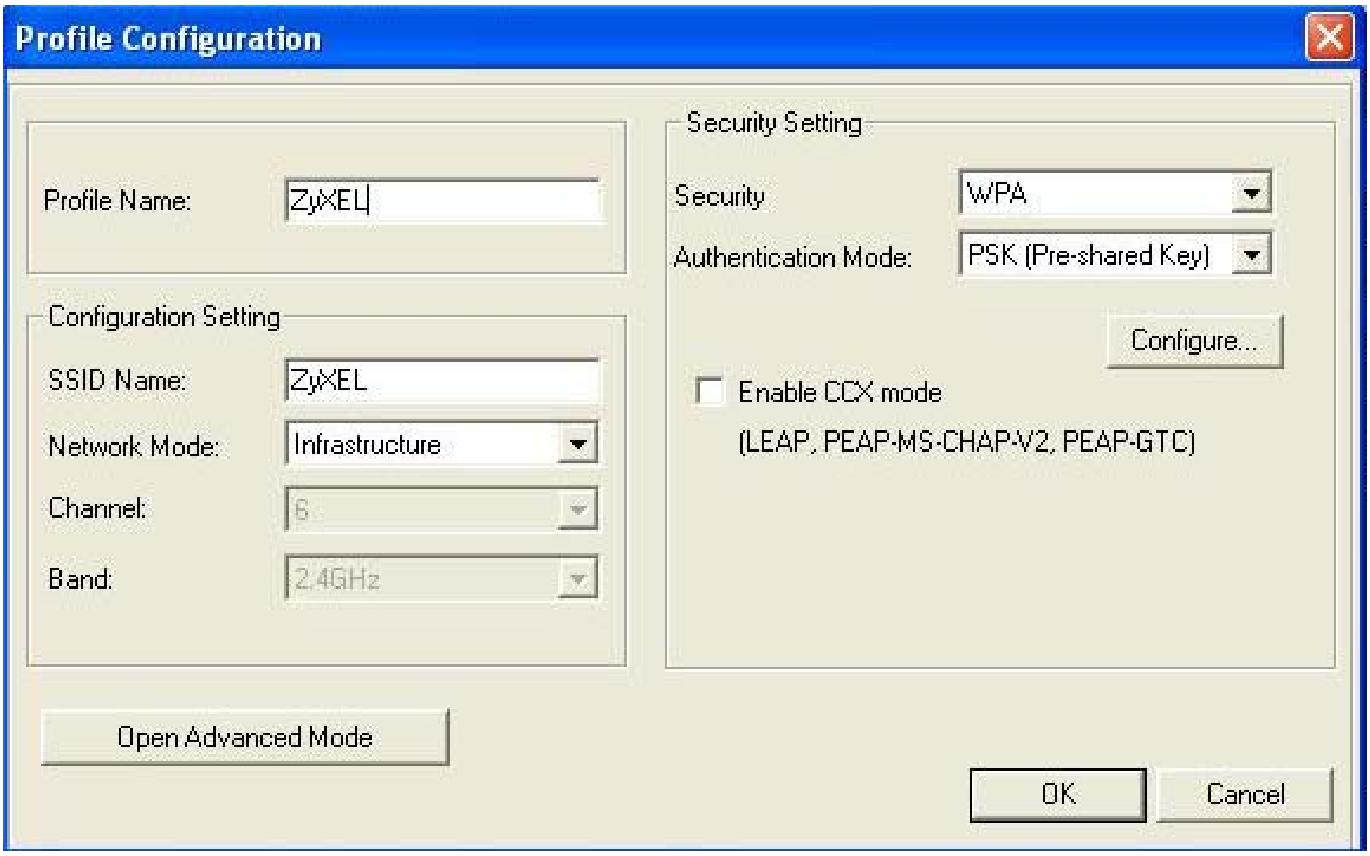
Passphrase :

○ 64-Bit Keys ● 128-Bit Keys Default Key : 1

5. [Create Keys Manually] Enter WEP key exactly as you did in your access point. Select the correct encryption level to match your access point. Either 64, 128, or 256-bit. The encryption level set her must match the encryption level used by your AP/Router.
6. [Key Format] Select either Hex or ASCII to enter the WEP key
   a. *Manual Input (Hexadecimal):* You generate your own WEP Key using hexadecimal characters (10 characters for 64-bit, 26 characters for 128-bit, 58 characters for 256-bit).
   b. *ManualIInput (ASCII):* You generate your own WEP Key (4 keys maximum) using ASCII characters (5 characters for 64-bit, 13 characters for 128-bit, 29 characters for 256-bit)
7. [Crete Keys with Passphrase] a WEP Key is automatically generated as you type in any PassPhrase of your choice. Use this feature when you have used a Pass Phrase to generate your WEP key on your access point.
8. [Default Key] the number of default key you select should match the key number you input.

9. Click [OK] to save your settings and return to the previous screen.
10. If you want to select 802.1 x authentications with WEP, you will need to configure your 802.1x settings by checking [enable CCX mode] to see advanced settings. To configure the 802.1x authentication, please refer to section 4.5. Also, you need to know if the AP/Router you will connect to supports the 802.1x or not and then follow your AP/Router setting.

4.3 Configuring WPA-PSK



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

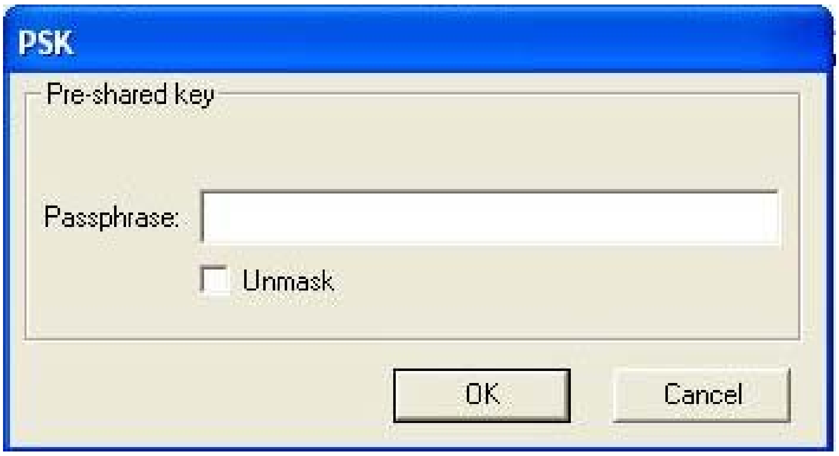
Security Setting

Security: WPA

Authentication Mode: PSK (Pre-shared Key)

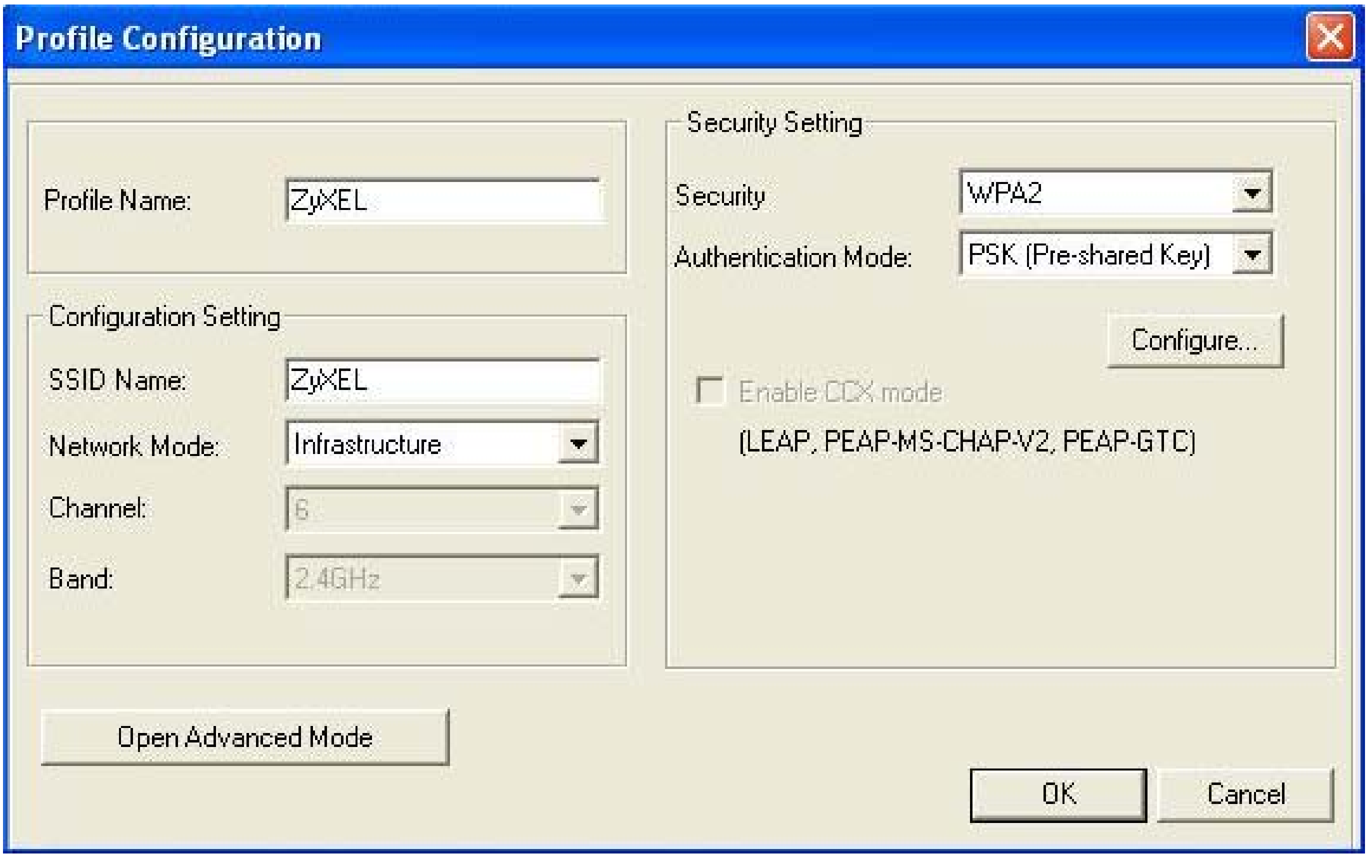
☐ Enable CCX mode (LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

1. Select [WPA] under [Security]
2. Select [PSK(Pre-Shared Key)] under [Authentication Mode]
3. Click [Configure] and then you will see the screen below.



4. Enter the same pass phrase used to configure WPA-PSK on your access point.
5. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].

4.4 Configuring WPA2-PSK



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

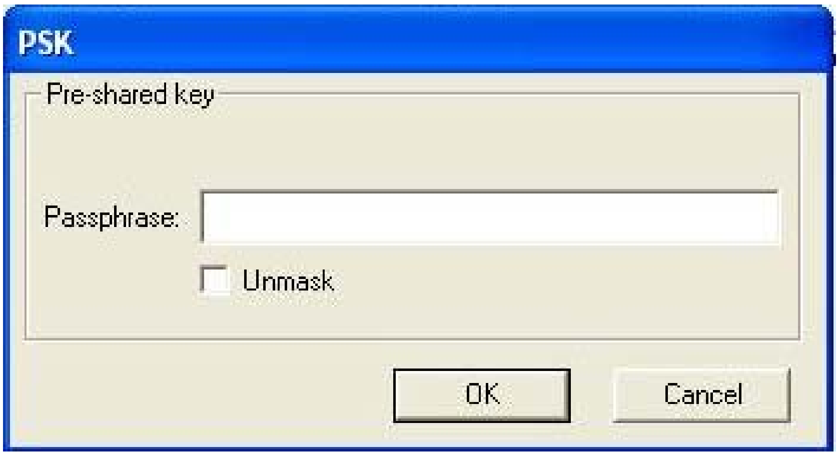
Security WPA2

Authentication Mode: PSK (Pre-shared Key)

□ Enable CCX mode

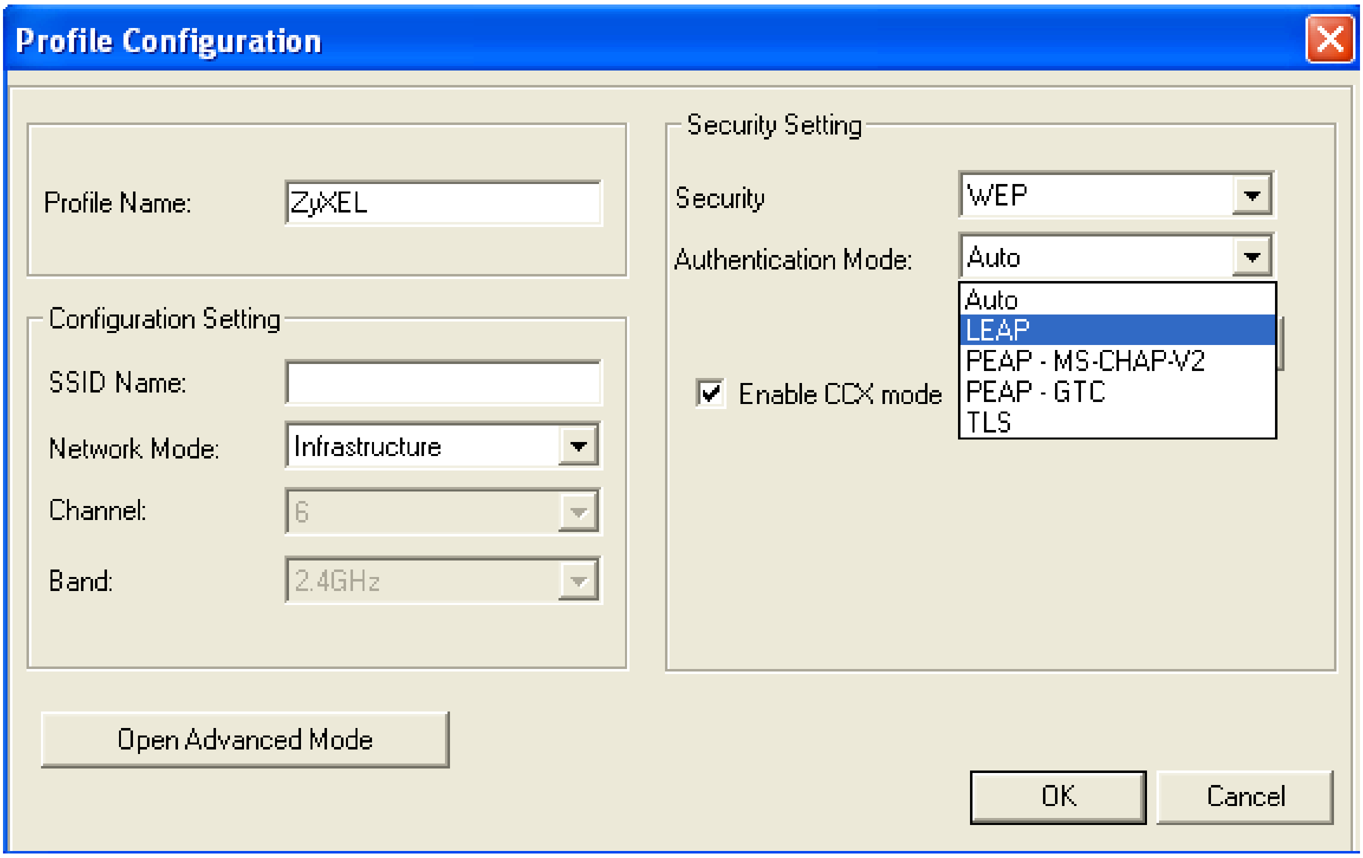
(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

1. Select [WPA2] under [Security Mode].
2. Select [PSK(Pre-Shared Key)] under [Authentication Mode].
3. Click [Configure] and then you will see the screen below.



4. Enter the same pass phrase used to configure WPA-PSK on your access point. The same pass phrase used to configure WPA-PSK/WPA2-PSK on your access point.
5. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].

4.5 Configuring WEP-802.1x



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name:

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

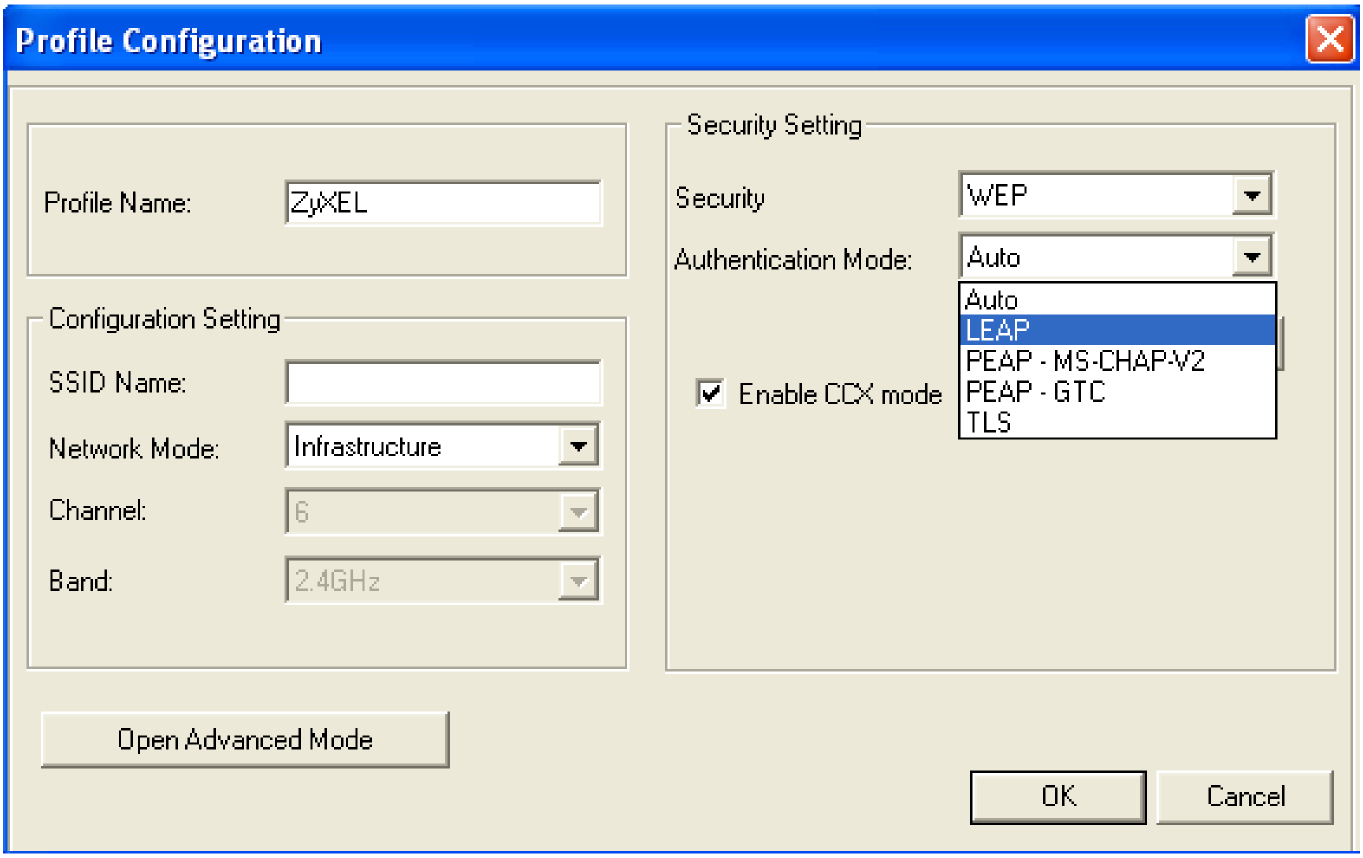
Security: WEP

Authentication Mode: Auto

☑ Enable CCX mode

1. You need to know if your AP/Router support 802.1x or not and then follow its configuration.
2. Check [Enable CCX mode] box when you need to enable the 802.1x setting. Then the EPA mode of LEAP, PEAP-MS-CHAP-V2, PEAP-GTC and TLS will be shown under [Authentication protocol]. For CCX mode information, please refer to Appendix A.

4.5.1 Configuring WEP-802.1x: EAP-LEAP



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name:

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

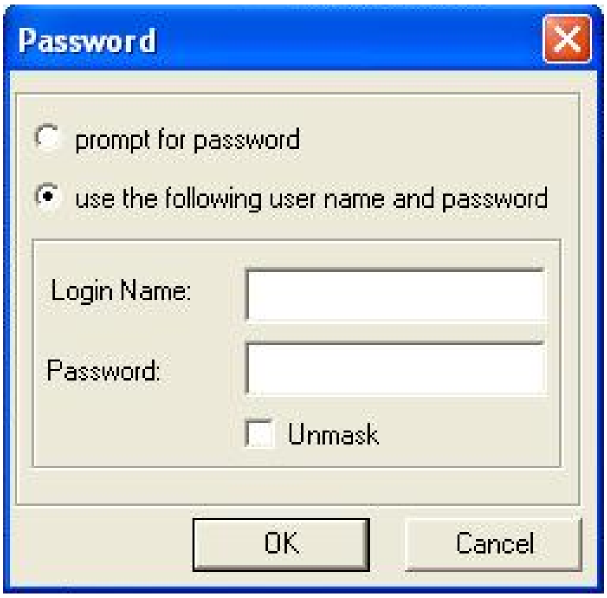
Security Setting

Security: WEP

Authentication Mode: Auto

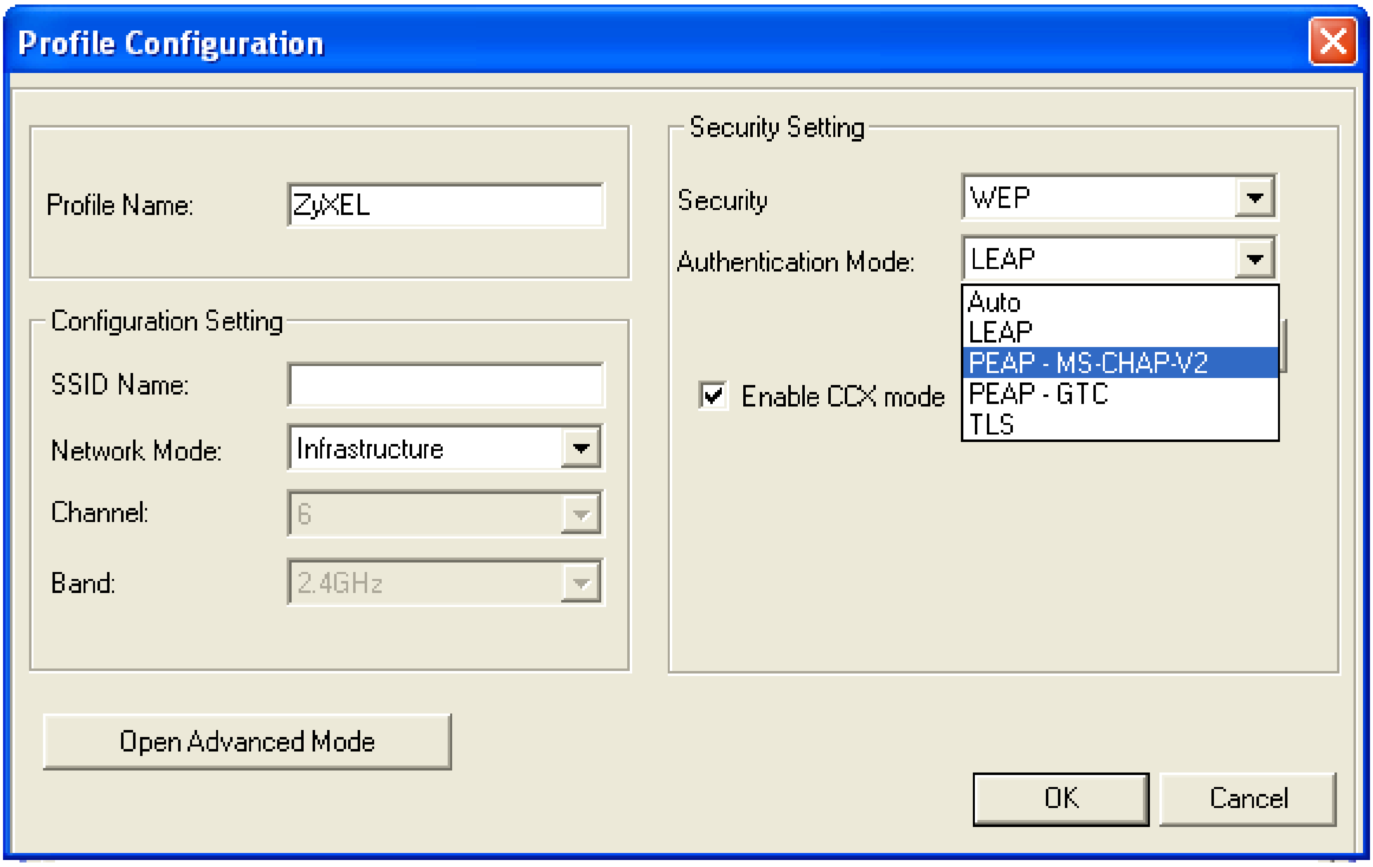
☑ Enable CCX mode

1. Select [WEP] under [Security].
2. Select [LEAP] under [Authentication Mode]
3. Click [Configure] and then you will see the screen below.



4. Select an appropriate AP/Router to indicate whether:
   a. The utility prompts you for them each time you try to connect to AP/Router
   b. Enter login name and password under the [Login Name] and [Password].
5. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].
6. Click [OK]

4.5.2 Configuring WEP-802.1x: EAP-PEAP-MS-CHAPv2



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name:

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

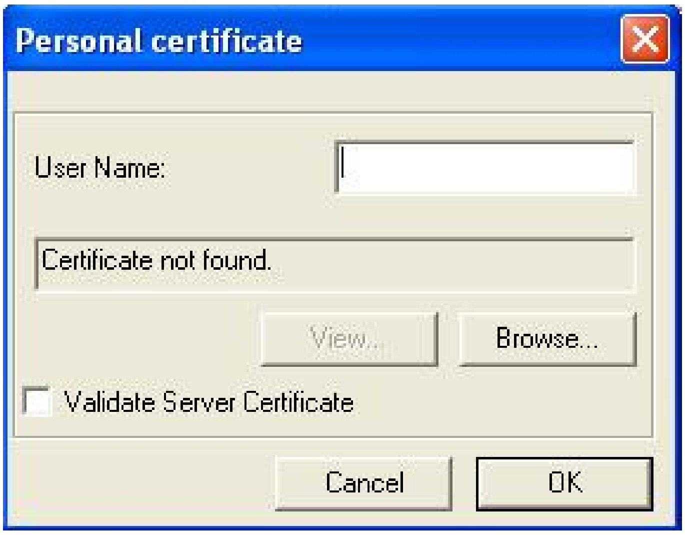
Security Setting

Security: WEP

Authentication Mode: LEAP

☑ Enable CCX mode

1. Select [WEP] under [Security].
2. Select [PEAP MS-CHAP-V2] under [Authentication protocol]
3. Click [Configure] and then you will see the screen below.

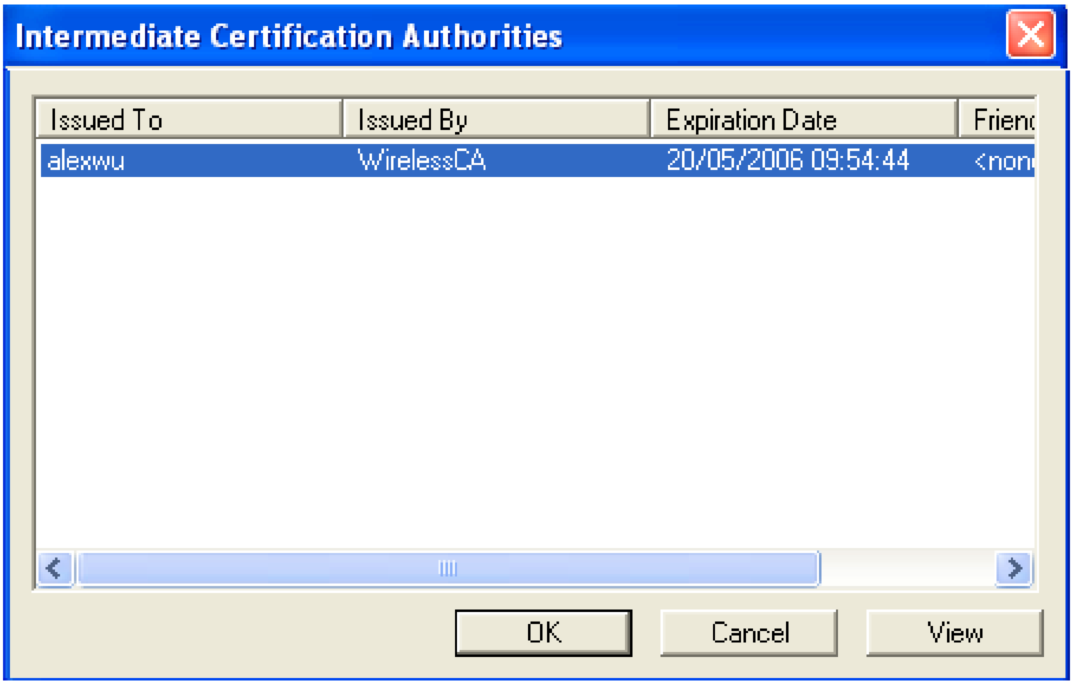


User Name:

Certificate not found.

□ Validate Server Certificate

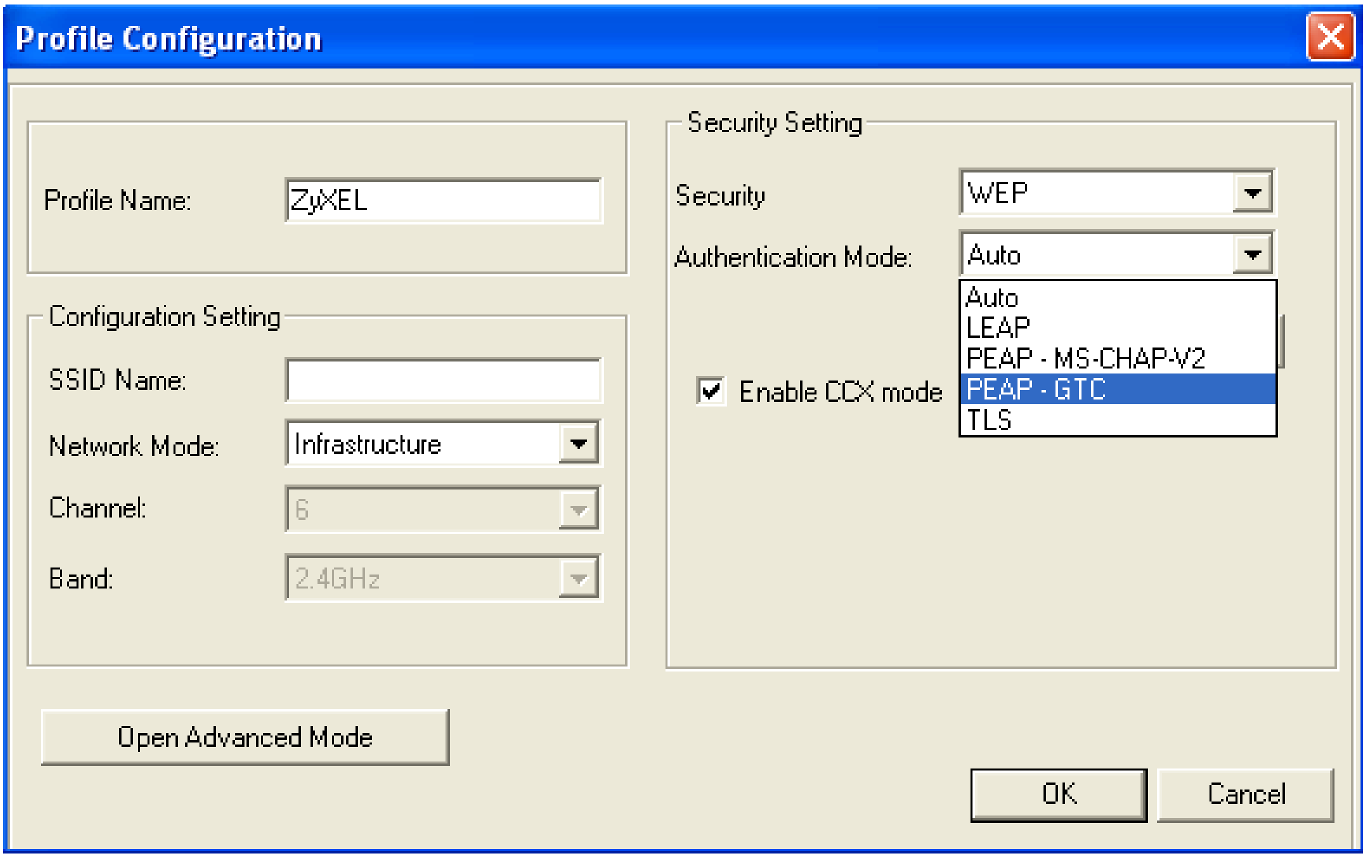
4. [Personal certificate] enables you to supply a personal certificate. This window is only applicable with Enterprise security. Please refer to your MIS administrator for this setting.
5. To supply a personal certificate, please enter the user name assigned to the certificate under [User Name]
6. Click [Browse] to see the [Intermediate Certification Authorities] screen below.
7. [Validate Server Certificate]: Put a check in the box to activate server certificate.



Issued To	Issued By	Expiration Date	Frienc
alexwu	WirelessCA	20/05/2006 09:54:44	<non

8. Select a certificate from the list, and click [OK] .

4.5.3 Configuring WEP-802.1x: PEAP-GTC



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name:

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

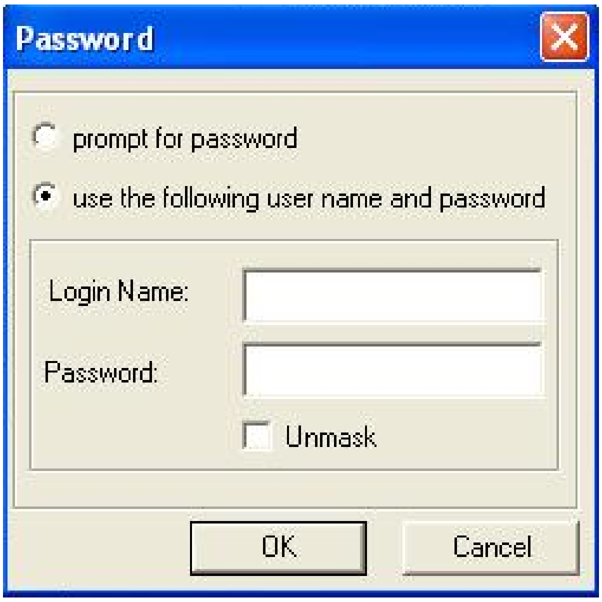
Security Setting

Security: WEP

Authentication Mode: Auto

☑ Enable CCX mode

1. Select [WEP] under [Security].
2. Select [PEAP-GTC] under [Authentication Mode].
3. Click [Configure] and then you will see the screen below.



Password

○ prompt for password

● use the following user name and password

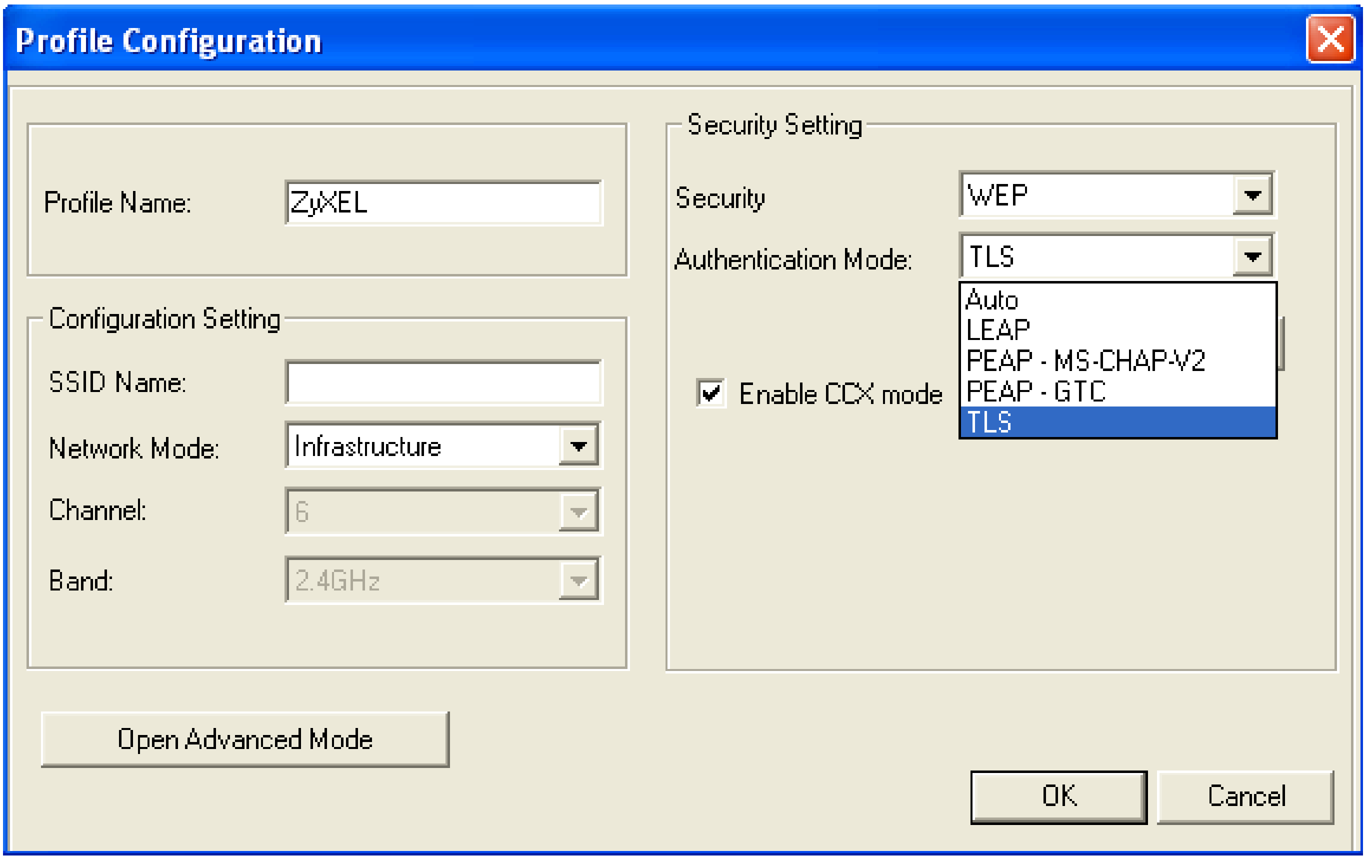
Login Name:

Password:

□ Unmask

4. Select an appropriate AP/Router to indicate whether:
   a. The utility prompts you for them each time you try to connect to AP/Router
   b. Enter login name and password under the [Login Name] and [Password].
5. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].
6. Click [OK]

4.5.4 Configuring WEP-802.1x: EAP-TLS



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name:

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

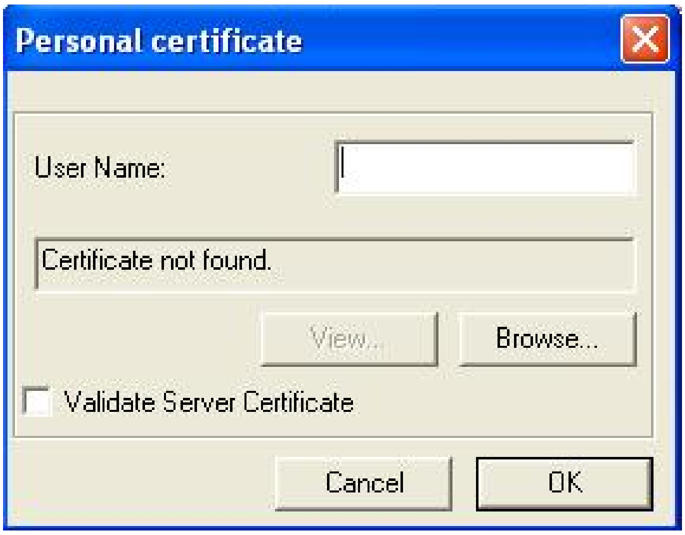
Security Setting

Security: WEP

Authentication Mode: TLS

☑ Enable CCX mode

1. Select [WEP] under [Security].
2. Select [TLS] under [Authentication protocol].
3. Click [Configure] and then you will see the screen below.

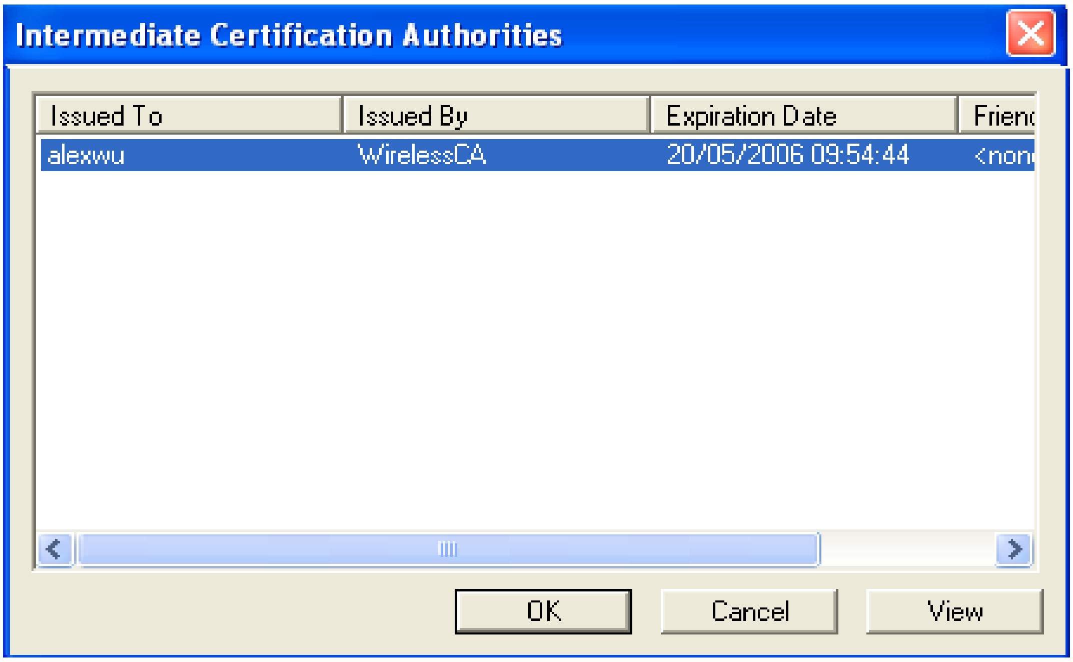


Personal certificate

User Name:

Certificate not found.

4. [Personal certificate] enables you to supply a personal certificate. This window is only applicable with Enterprise security. Please refer to your MIS administrator for this setting.
5. To supply a personal certificate, please enter the user name assigned to the certificate under [User Name]
6. Click [Browse] to see the [Intermediate Certification Authorities] below.
7. [Validate server certificate]: Put a check in the box to activate server certificate.



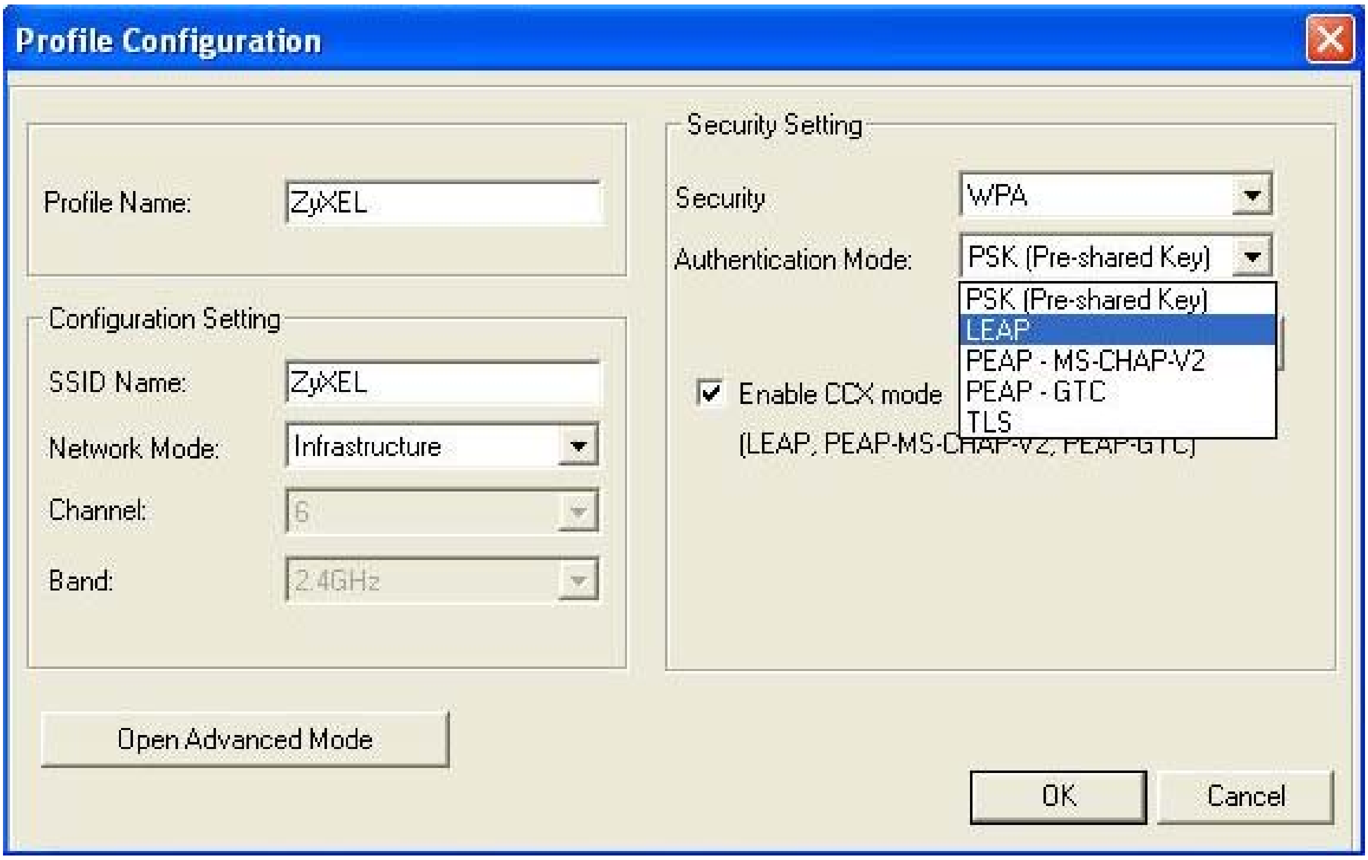
Intermediate Certification Authorities

Issued To	Issued By	Expiration Date	Frienc
alexwu	WirelessCA	20/05/2006 09:54:44	<non

.

8. Select a certificate from the list, and click [OK]

4.6 Configuring WPA-802.1x



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

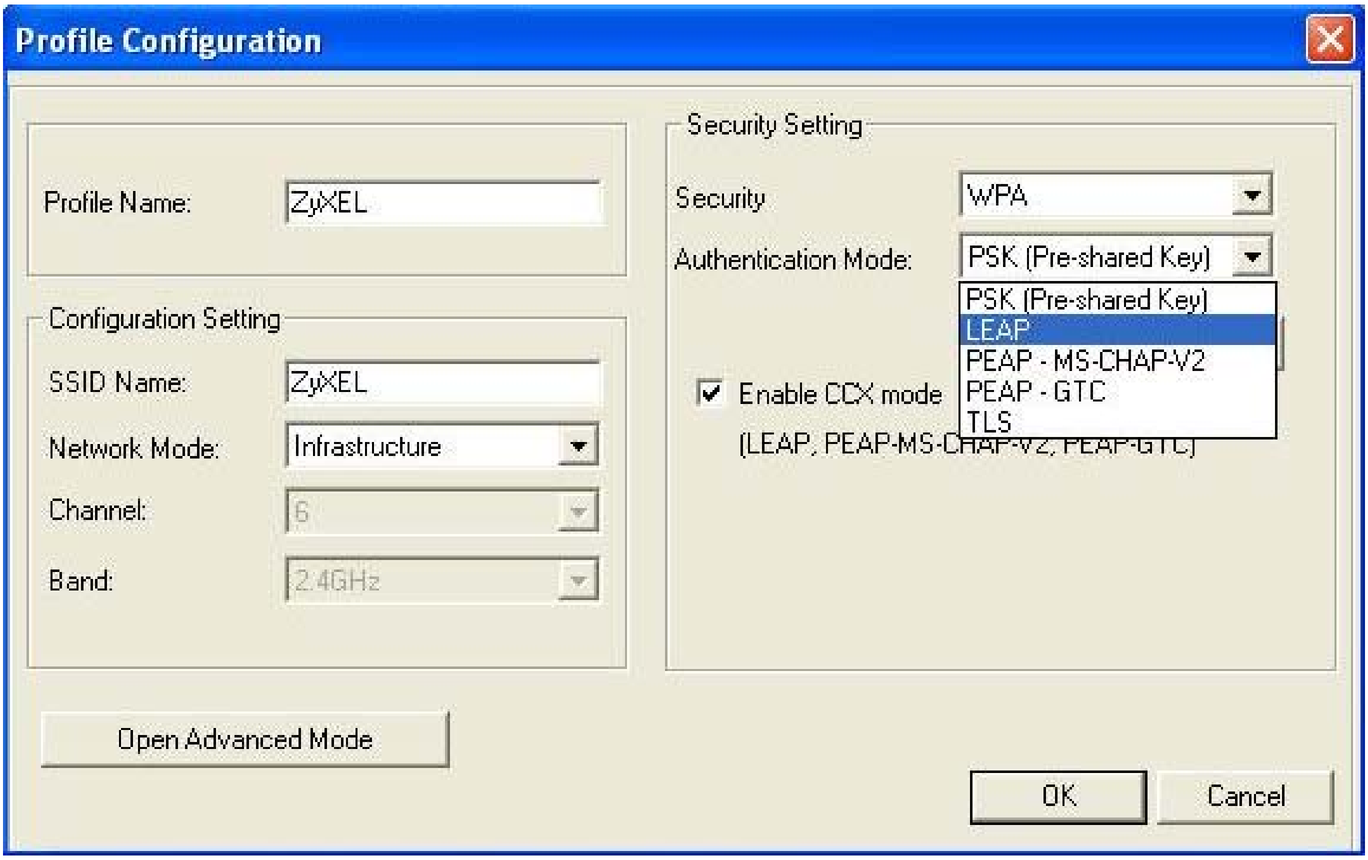
Security: WPA

Authentication Mode: PSK (Pre-shared Key)

☑ Enable CCX mode (LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

3. You need to know if your AP/Router support 802.1x or not and then follow up its configuration.
4. Check [Enable CCX mode] box when you need to enable the 802.1x setting. Then the EPA mode of LEAP, PEAP-MS-CHAP-V2, PEAP-GTC and TLS will be shown under [Authentication protocol]. For CCX mode information, please refer to Appendix A.
5. For more 802.1x and WPA-Enterprise security settings, please refer to the user's guide of Funk Odyssey client software.

4.6.1 Configuring WPA-802.1x: EAP-LEAP



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

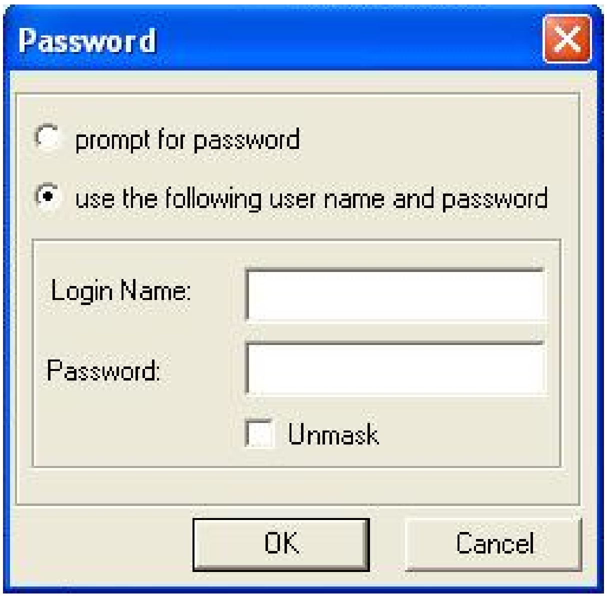
Security: WPA

Authentication Mode: PSK (Pre-shared Key)

☑ Enable CCX mode

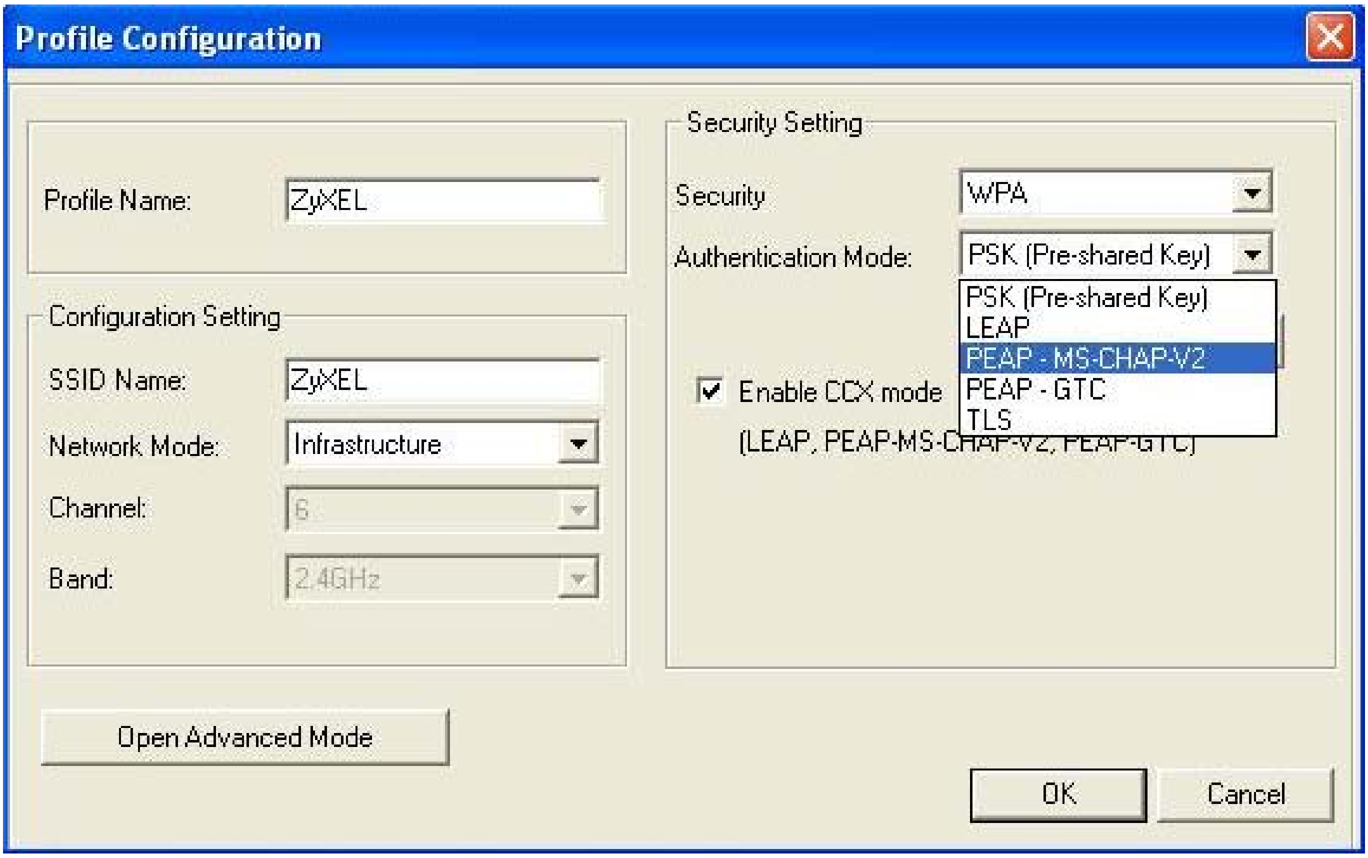
(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

7. Select [WPA] under [Security].
8. Select [LEAP] under [Authentication Mode]
9. Click [Configure] and then you will see the screen below.



10. Select an appropriate AP/Router to indicate whether:
    c. The utility prompts you for them each time you try to connect to AP/Router
    d. Enter login name and password under the [Login Name] and [Password].
11. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].
12. Click [OK]

4.6.2 Configuring WPA-802.1x: EAP-PEAP-MS-CHAPv2



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

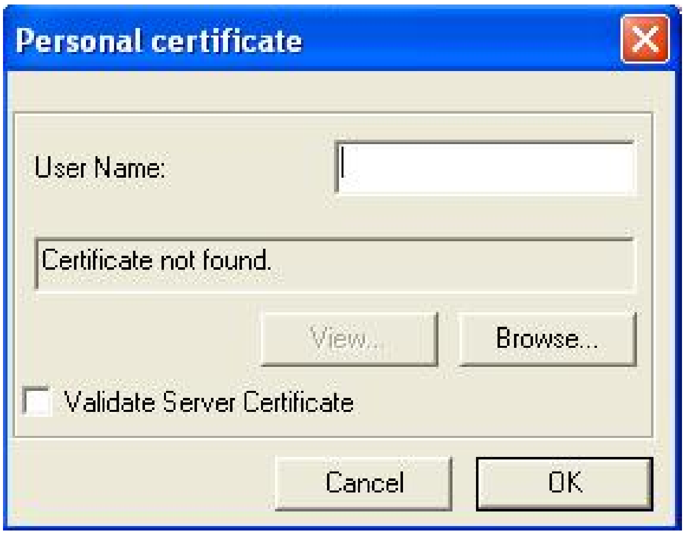
Security: WPA

Authentication Mode: PSK (Pre-shared Key)

☑ Enable CCX mode

(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

9. Select [WPA] under [Security].
10. Select [PEAP MS-CHAP-V2] under [Authentication protocol]
11. Click [Configure] and then you will see the screen below.

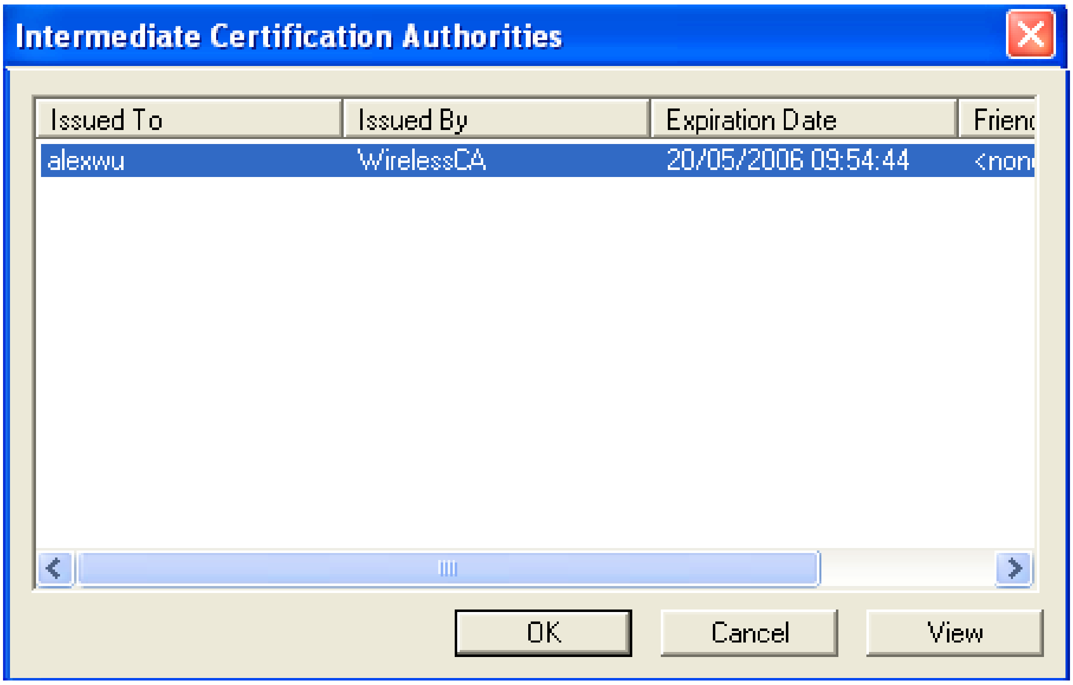


Personal certificate

User Name:

Certificate not found.

12. [Personal certificate] enables you to supply a personal certificate. This window is only applicable with Enterprise security. Please refer to your MIS administrator for this setting.
13. To supply a personal certificate, please enter the user name assigned to the certificate under [User Name]
14. Click [Browse] to see the [Intermediate Certification Authorities] screen below.
15. [Validate Server Certificate]: Put a check in the box to activate server certificate.

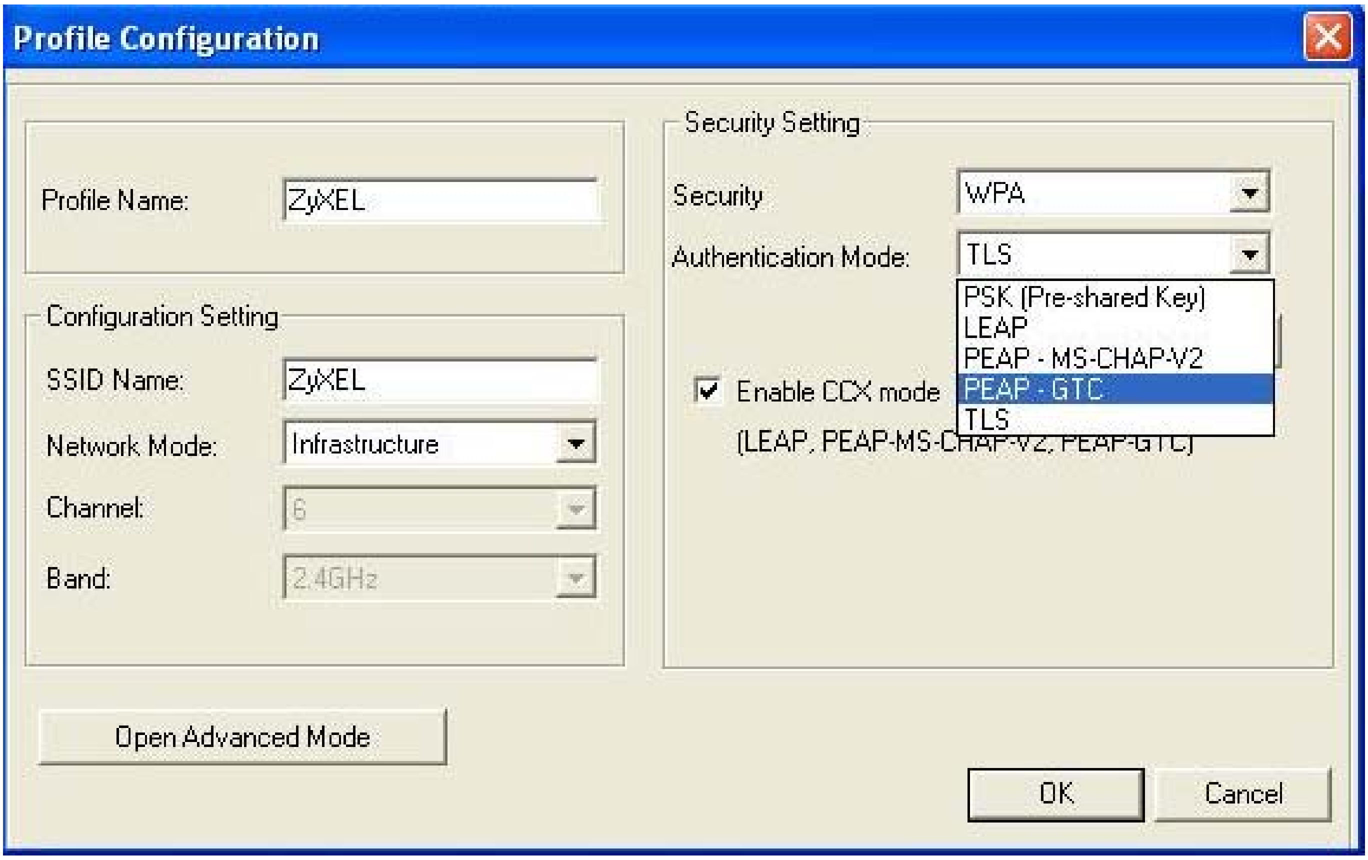


Intermediate Certification Authorities

Issued To	Issued By	Expiration Date	Frienc
alexwu	WirelessCA	20/05/2006 09:54:44	<non

16. Select a certificate from the list, and click [OK] .

4.6.3 Configuring WPA-802.1x: PEAP-GTC



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

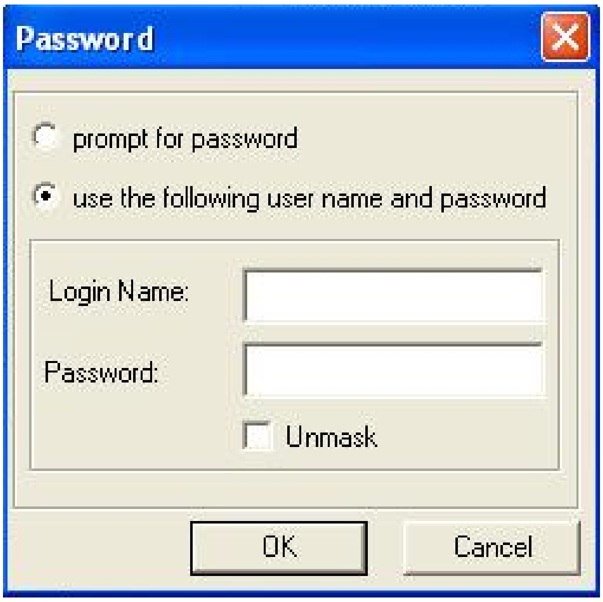
Security Setting

Security: WPA

Authentication Mode: TLS

☑ Enable CCX mode (LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

4. Select [WPA] under [Security].
5. Select [PEAP-GTC] under [Authentication Mode].
6. Click [Configure] and then you will see the screen below.



Password

○ prompt for password

● use the following user name and password

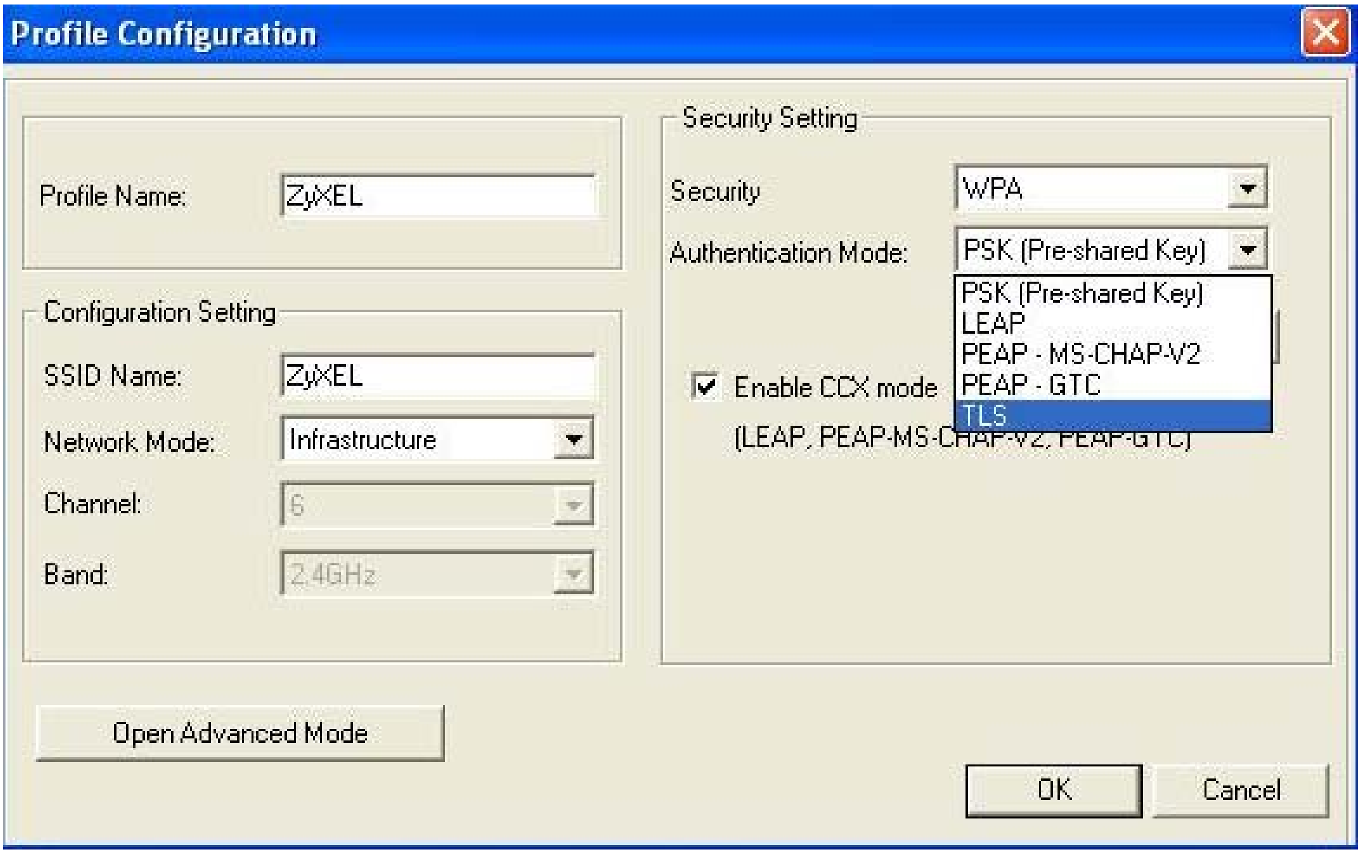
Login Name:

Password:

□ Unmask

4. Select an appropriate AP/Router to indicate whether:
    a. The utility prompts you for them each time you try to connect to AP/Router
    b. Enter login name and password under the [Login Name] and [Password].
5. The key you enter is masked by default with asterisks (*). To view the key that you entered, check [Unmask].
6. Click [OK]

4.6.4 Configuring WPA-802.1x: EAP-TLS



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

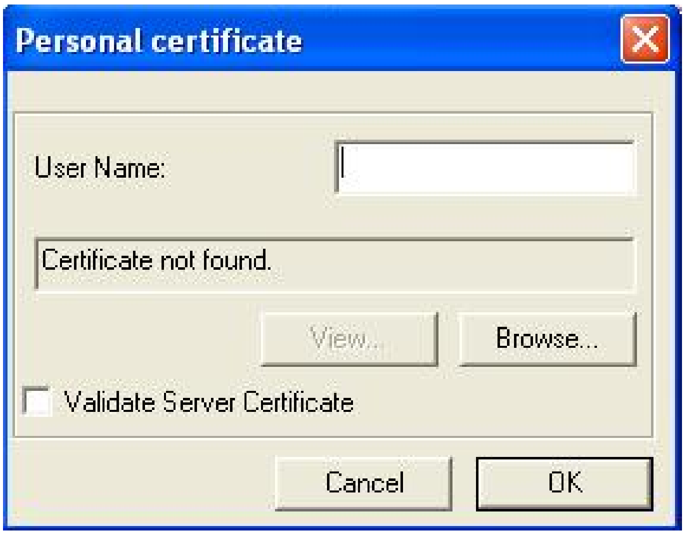
Security: WPA

Authentication Mode: PSK (Pre-shared Key)

☑ Enable CCX mode

(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

4. Select [WPA] under [Security].
5. Select [TLS] under [Authentication protocol].
6. Click [Configure] and then you will see the screen below.

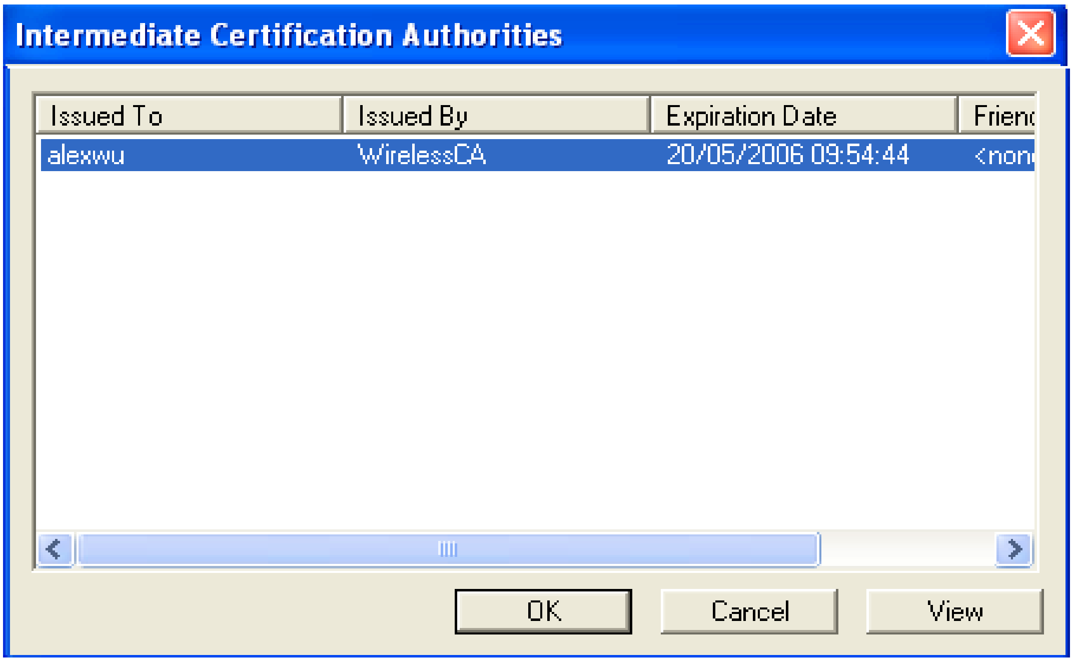


User Name:

Certificate not found.

□ Validate Server Certificate

4. [Personal certificate] enables you to supply a personal certificate. This window is only applicable with Enterprise security. Please refer to your MIS administrator for this setting.
5. To supply a personal certificate, please enter the user name assigned to the certificate under [User Name]
6. Click [Browse] to see the [Intermediate Certification Authorities] below.
7. [Validate server certificate]: Put a check in the box to activate server certificate.

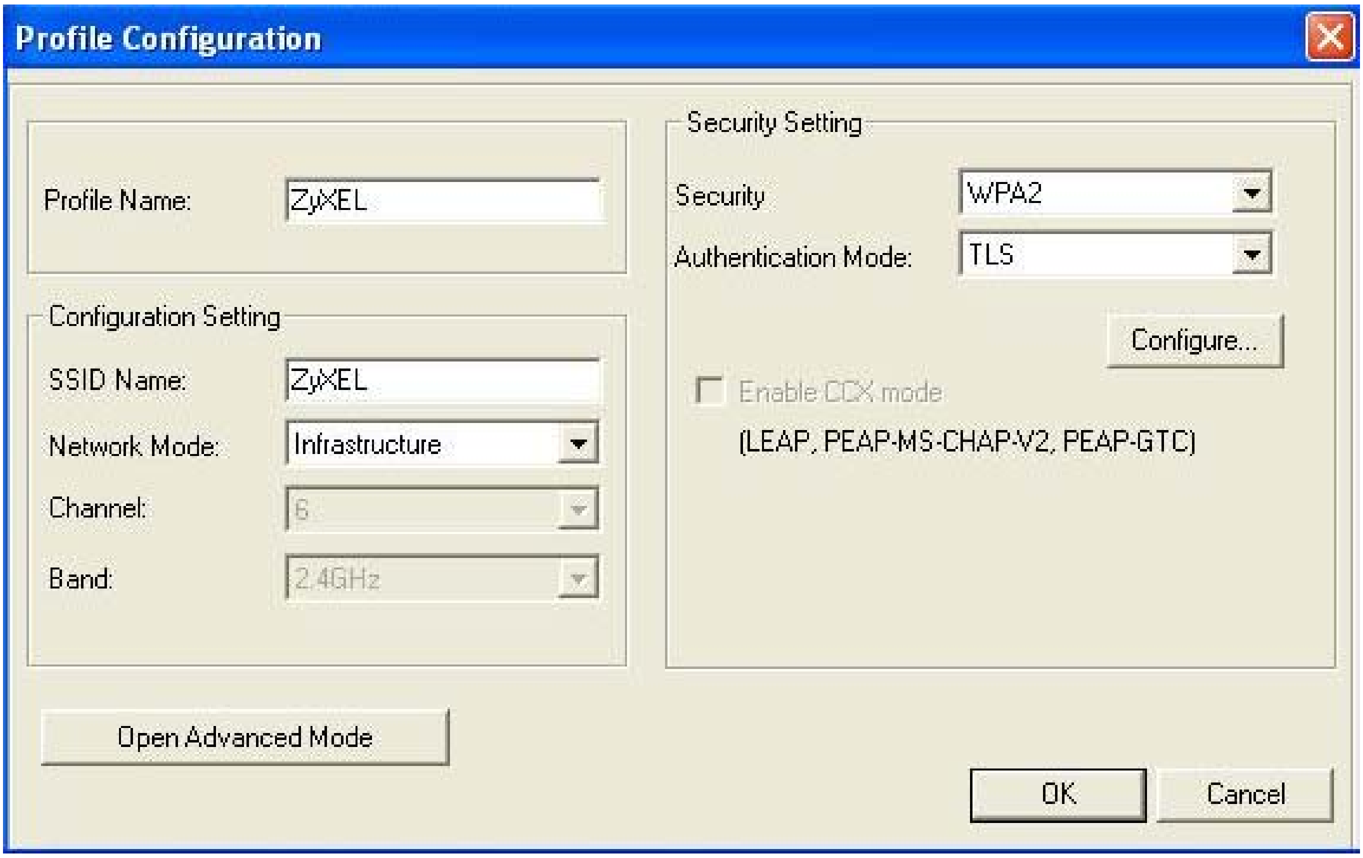


Issued To	Issued By	Expiration Date	Frienc
alexwu	WirelessCA	20/05/2006 09:54:44	<non

.

8. Select a certificate from the list, and click [OK]

4.6.5 Configuring WPA2-802.1x: EAP-TLS



Profile Configuration

Profile Name: ZyXEL

Configuration Setting

SSID Name: ZyXEL

Network Mode: Infrastructure

Channel: 6

Band: 2.4GHz

Security Setting

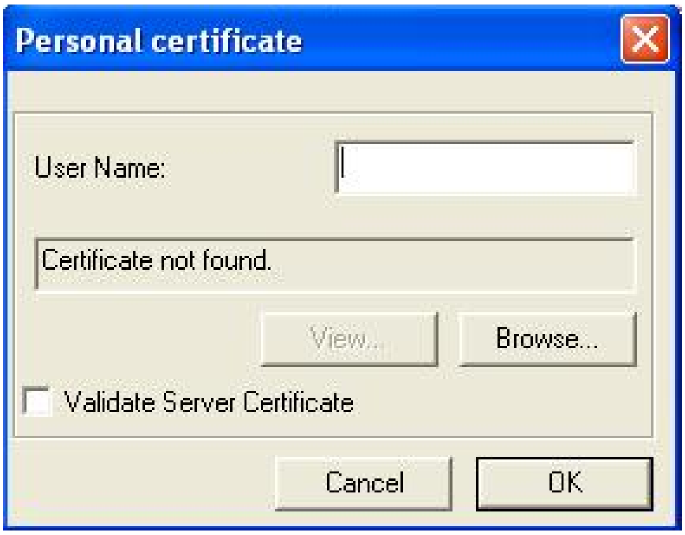
Security: WPA2

Authentication Mode: TLS

☐ Enable CCX mode

(LEAP, PEAP-MS-CHAP-V2, PEAP-GTC)

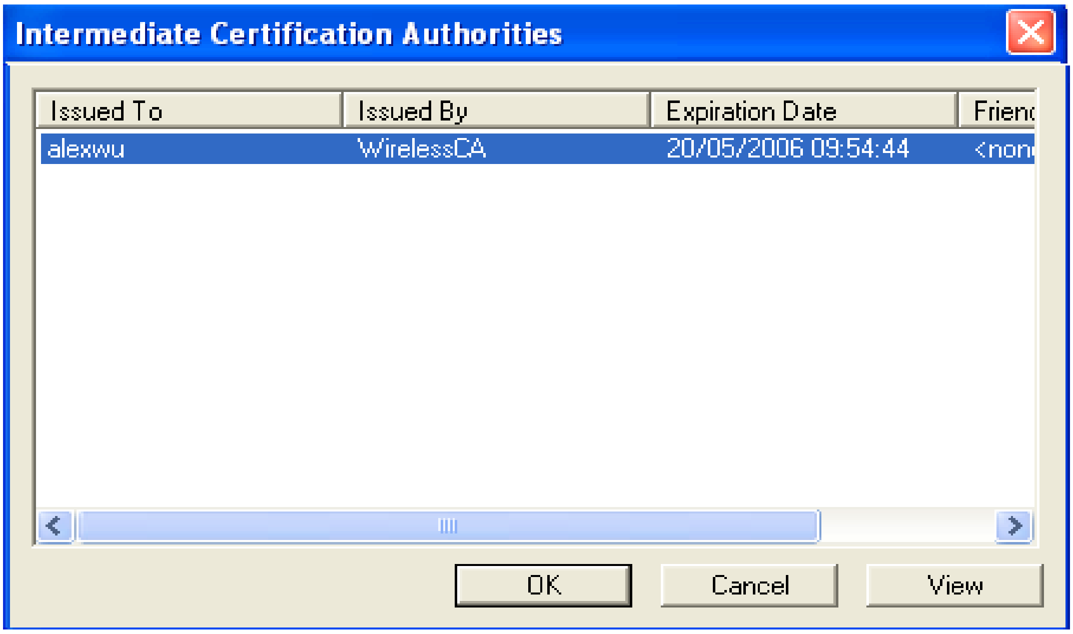
1. Select [WPA2] under Security.
2. Select [TLS] under [Authentication protocol]
3. Click [Configure] and then you will see the screen below.



Certificate not found.

□ Validate Server Certificate

4. [Personal certificate] enables you to supply a personal certificate. This window is only applicable with Enterprise security. Please refer to your MIS administrator for this setting.
5. To supply a personal certificate, please enter the user name assigned to the certificate under [User Name]
6. Click [Browse] to see the [Intermediate Certification Authorities] below.
7. [Validate server certificate]: Put a check in the box to activate server certification.



Issued To	Issued By	Expiration Date	Frienc
alexwu	WirelessCA	20/05/2006 09:54:44	<non

8. Select a certificate from the list, and click [OK]

Chapter 5 Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you diagnose and solve the problem.

5.1 Problems Starting the ZyXEL Utility Program

Table 5-1 Troubleshooting Starting ZyXEL Utility Program

PROBLEM	CORRECTIVE ACTION
Windows does not auto-detect the ZyXEL G-162/G-360.	Make sure the ZyXEL G-162 is properly inserted into the CardBus slot and then restart your computer. Once the computer has restarted, check the status of the LEDs on the ZyXEL G-162. Make sure the ZyXEL G-360 is properly inserted and the LED(s) is on. Check the status of the LEDs on the G-360. Refer to the *Quick Start Guide* for the LED descriptions.
	Perform a hardware scan by clicking **Start**, **Settings**, **Control Panel** and then double-click **Add/Remove Hardware**. (Steps may vary depending on Windows version). Follow the on-screen instructions to search for the ZyXEL G-162/G-360 and install the driver.
	Check for possible hardware conflicts. In Windows, click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and then click **Device Manager**. Verify the status of the ZyXEL G-162/G-360 under **Network Adapter**. (Steps may vary depending on the Windows version).
The ZyXEL Z icon does not display.	If you already installed the Funk Odyssey Client software on the computer, uninstall (remove) both the Funk Odyssey Client software and ZyXEL utility, and then install the ZyXEL utility again after restarting the computer.
	If you use the Windows Zero configuration tool and the ZyXEL Utility to configure the ZyXEL G-162/G-360 at the same time, the ZyXEL Z icon does not display. You need to disable the Windows Zero configuration tool. (Please refer to 1.3.1 Windows Zero Configuration for detail information.)
	Install the ZyXEL G-162/G-360 in another computer. If the error persists, there may be a hardware problem. In this case, please contact ZyXEL customer support at 800-978-7222 or on the web at http://www.us.zyxel.com.

5.2 Problems with LED Status

Table 5-2 Troubleshooting LED Status

LED PWR is not On	Make sure the ZyXEL G-162/G-360 is properly inserted.
LED LINK is not On or Blinking	Please check and make sure your AP/Router is up and running.

5.3 Problems with the Link Status

Table 5-3 Troubleshooting Link Status

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	Search and connect to another AP with a better link quality using the **Site Survey** screen. Change the channel used by your AP. Move your computer closer to the AP or the peer computer(s) within the transmission range. There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.
	When the ZyXEL G-360 happens into this problem, please also check the above corrective action. In addition, make sure your PC is not placed close to the wall or corner that the antenna cannot receive signal from the AP/Router. The antenna should be perpendicular to the ground but depending on your wireless environment, you may need to adjust the direction of antenna to get maximum signal.

5.4 Problems with Security Settings

Table 5-4 Troubleshooting Security Settings

Security Mode and Authentication Protocol cannot be configured	Make sure your AP/Router has the same setting as your client adapter and follow AP/Router's security settings.

5.5 Problems Communicating With Other Computers

Table 5-5 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The ZyXEL G-162/G-360 computer cannot communicate with the other computer.	Make sure your adapters are connected to the network.
A. **Infrastructure**	Make sure that the AP and the associated computers are turned on and working properly. Make sure the ZyXEL G-162/G-360 computer and the associated AP use the same SSID. Change the AP and the associated wireless clients to use another radio channel if interference is high. Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Settings** screen.
B. **Ad-Hoc (IBSS)**	Verify that the peer computer(s) is turned on. Make sure the ZyXEL G-162/G-360 computer and the peer computer(s) are using the same SS ID and channel. Make sure that the computer and the peer computer(s) share the same security option and key. Change the wireless clients to use another radio channel if interference is high.

Appendix A
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. Consult your network administrator for more information. For the EAP-MD5, please refer to the User’s Guide of Funk Odyssey software.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of five authentication types.

Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No