ZyXEL AG-200

802.11a/b/g Wireless USB 2.0 Adapter

User's Guide

Version 1.0

October 2004

ZyXEL
Unleash Networking Power

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

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

Federal Communications Commission (FCC) Interference Statement[1]

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.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Caution

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

[1] Refer to the *Quick Start Guide* for model specific FCC statement.

Customer Support

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

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[2] FAX[2]	WEB SITE FTP SITE	REGULAR MAIL
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
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.

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

Table of Contents

Preface

Congratulations on the purchase of your new ZyXEL AG-200!

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 AG-200 802.11a/g Wireless USB 2.0 Adapter is referred to as the ZyXEL AG-200 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 AG-200 up and running right away. It contains a detailed easy-to-follow connection diagram and information on installing your ZyXEL AG-200.
- 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 Writing 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 AG-200 and prepares you to use the ZyXEL Utility.

1.1 About Your ZyXEL AG-200

The ZyXEL AG-200 is an IEEE 802.11a, 802.11b, and 802.11g compliant wireless LAN adapter. With the ZyXEL AG-200, you can enjoy wireless mobility within almost any wireless networking environment.

The following lists the main features of your ZyXEL AG-200.

- Your ZyXEL AG-200 can communicate with other IEEE 802.11a/b/g compliant wireless devices.
- Automatic rate selection.
- Standard data transmission rates up to 54 Mbps.
- Proprietary Atheros transmission rates of **108 Mbps**
- Offers 64-bit, 128-bit and 152-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- Low CPU utilization allowing more computer system resources for other programs.
- A built-in antenna.
- Driver support for Windows XP/2000

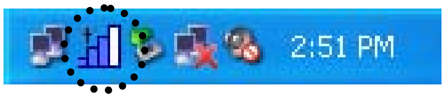
1.2 ZyXEL AG-200 Hardware and Utility Installation

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

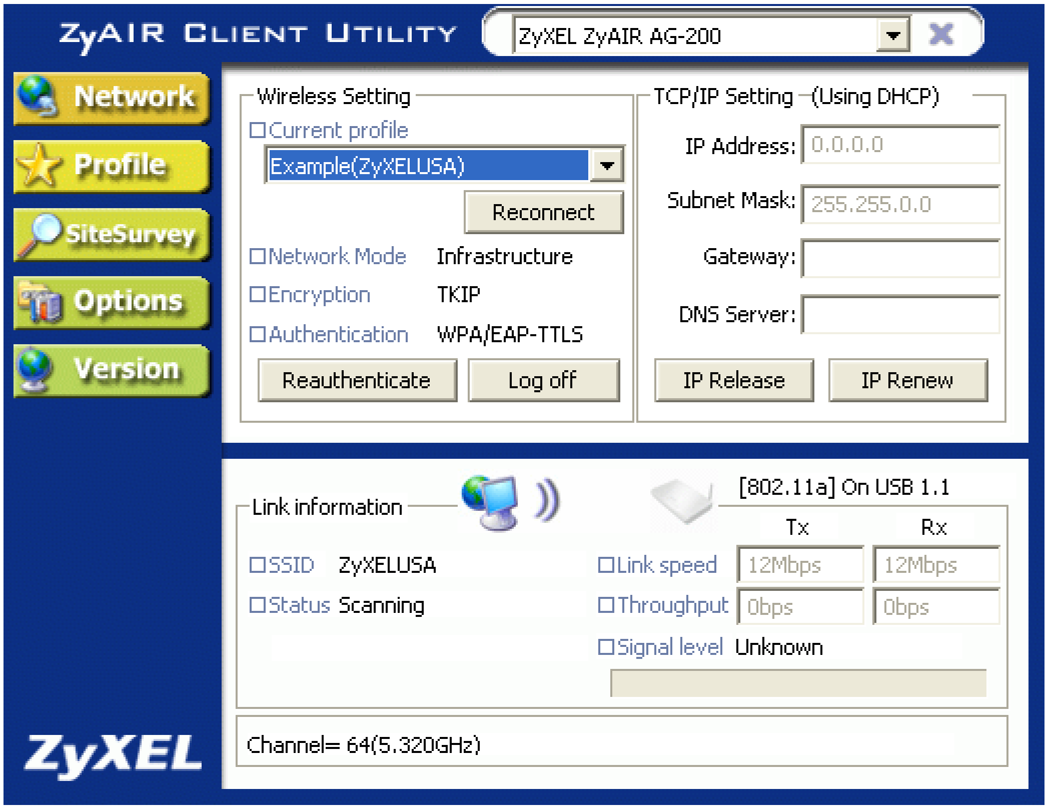
1.3 Using the ZyXEL Utility to Configure Your Network

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 new icon as shown below will automatically appear in the lower right tray bar.



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



ZyXEL ZyAIR AG-200

Wireless Setting

□Current profile Example(ZyXELUSA)

□Network Mode Infrastructure

□Encryption TKIP

□Authentication WPA/EAP-TTLS

TCP/IP Setting –(Using DHCP)

IP Address: 0.0.0.0

Subnet Mask: 255.255.0.0

Gateway:

DNS Server:

Link information

□SSID ZyXELUSA

□Status Scanning

[802.11a] On USB 1.1

	Tx	Rx
□Link speed	12Mbps	12Mbps
□Throughput	0bps	0bps

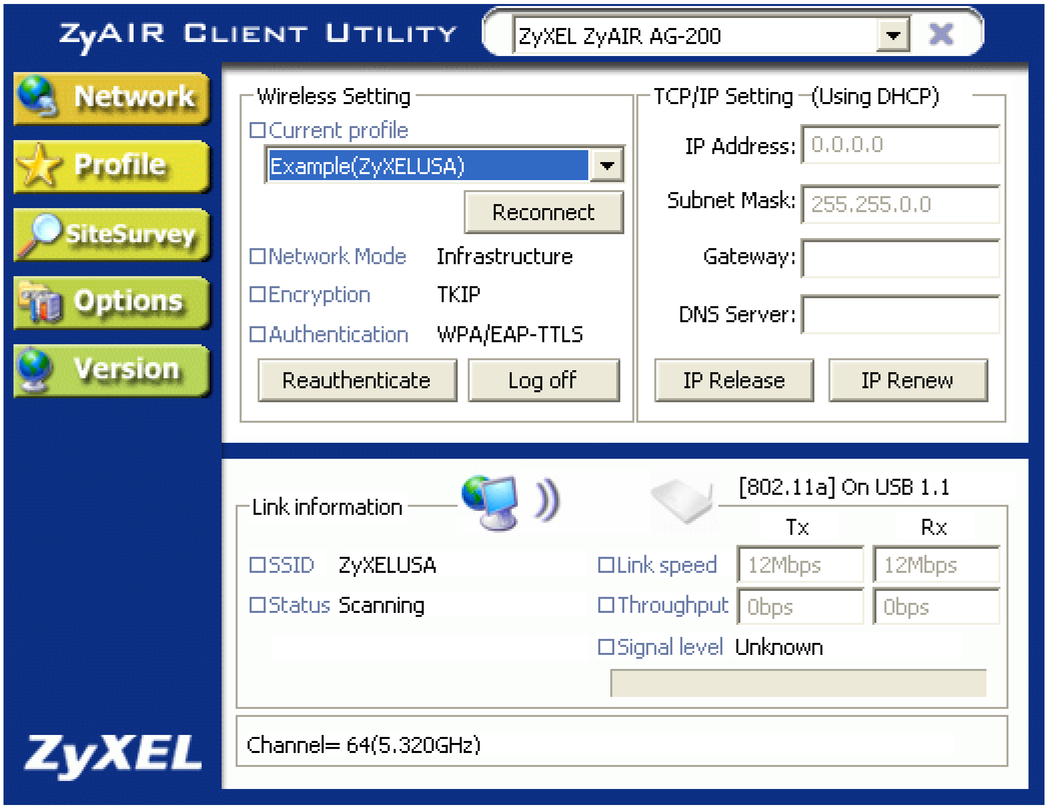
□Signal level Unknown

Channel= 64(5.320GHz)

Each of the pages (Network, Profile, Site Survey, Options, Version) presented in the ZyXEL Utility are explained in the following sections.

1.3.1 Network

This page shows how the network is presently configured: network mode, information on the connected AP, TCP/IP, etc. This information cannot be modified in the Network screen.



Wireless Setting

□Current profile Example(ZyXELUSA)

□Network Mode Infrastructure

□Encryption TKIP

□Authentication WPA/EAP-TTLS

TCP/IP Setting (Using DHCP)

IP Address: 0.0.0.0

Subnet Mask: 255.255.0.0

Gateway:

DNS Server:

Link information

[802.11a] On USB 1.1

	Tx	Rx
□Link speed	12Mbps	12Mbps
□Throughput	0bps	0bps

□SSID ZyXELUSA

□Status Scanning

□Signal level Unknown

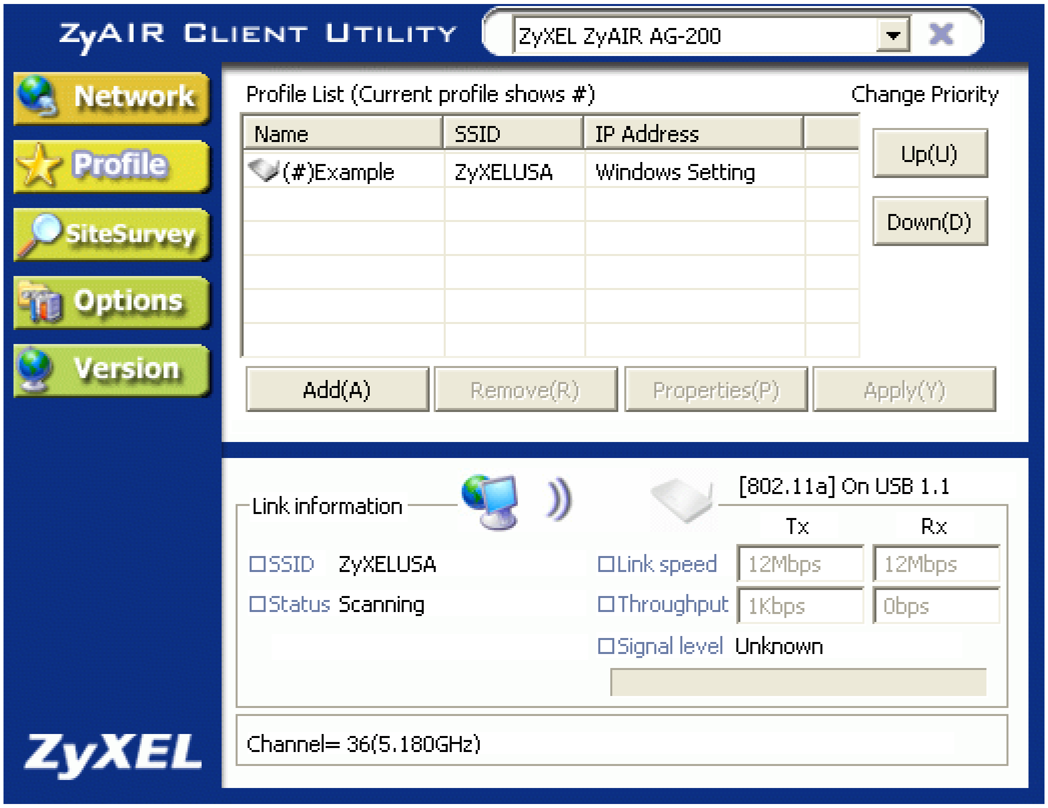
Channel= 64(5.320GHz)

The "Current Status" (lower) window shows the signal quality, signal strength, channel, etc. between the client and AP. It is always in view regardless of which page (Network, Profile, Search, Option, Version) is selected within the ZyXEL Utility.

1.3.2 Profile

This page is used to manage connections with Access Points. You can create different configuration profiles for connections with different APs and SSIDs.

The advantage of saving different profiles is the easiness of quickly changing connections without having to configure the PC with every single variable each time a connection change is made. Also, when configuring TCP/IP via the ZyXEL Utility you do not need to reboot the PC as when TCP/IP configuration is done via Windows' Control Panel.



Profile List (Current profile shows #)

Name	SSID	IP Address
(#)Example	ZyXELUSA	Windows Setting

Link information

[802.11a] On USB 1.1

			Tx	Rx
□SSID	ZyXELUSA	□Link speed	12Mbps	12Mbps
□Status	Scanning	□Throughput	1Kbps	0bps
		□Signal level	Unknown	

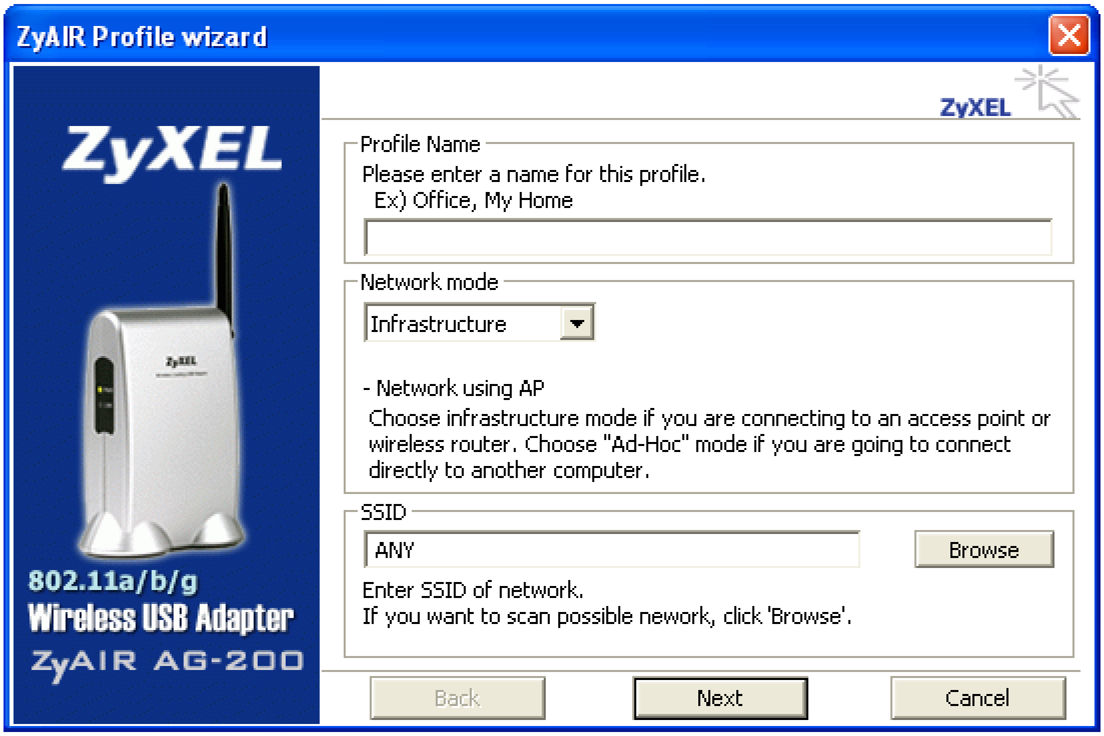
Channel= 36(5.180GHz)

Explanation of each button in this page is shown below.

Add

Clicking on this button enables you to create a new profile. The following steps show how this can be done.

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



Profile Name

Please enter a name for this profile.
Ex) Office, My Home

Network mode

Infrastructure

- Network using AP

Choose infrastructure mode if you are connecting to an access point or wireless router. Choose "Ad-Hoc" mode if you are going to connect directly to another computer.

SSID

ANY

Enter SSID of network.
If you want to scan possible nework, click 'Browse'.

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

   a. [Profile Name] Enter in a descriptive name for this profile.

   b. [Network Mode] If connecting to an access point or wireless router, choose "Infrastructure"[3]. If you are going to network one computer directly to another computer without an access point, then choose "Ad-Hoc"[4].

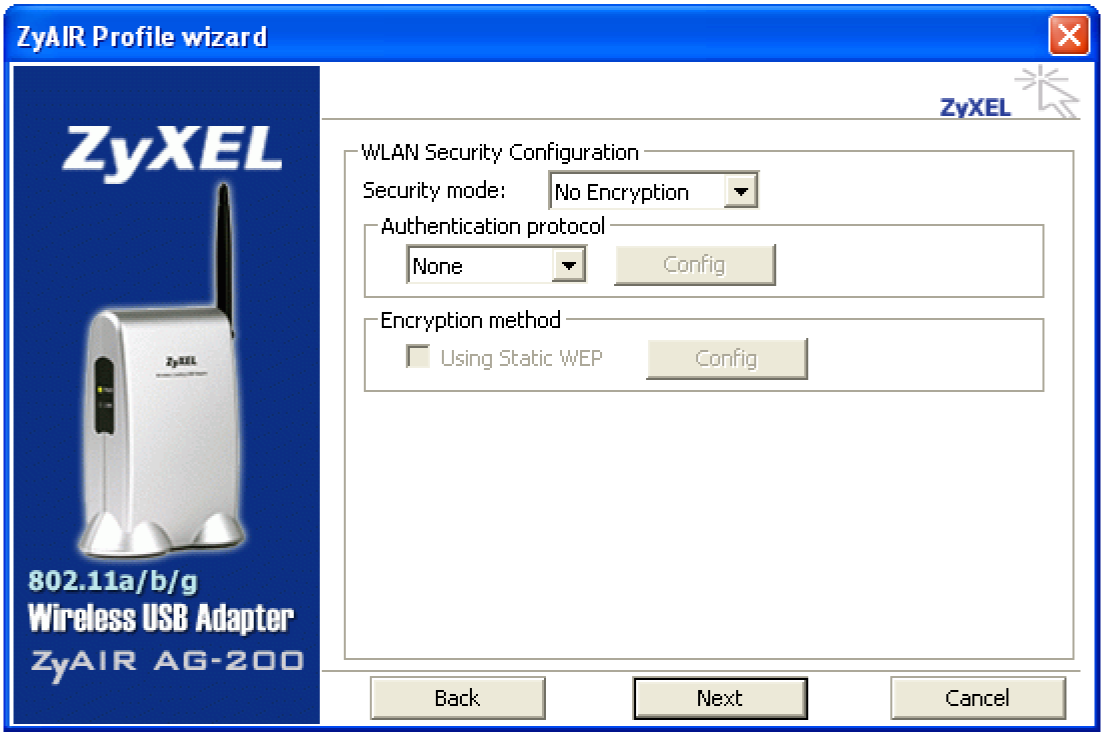
   c. [SSID] Select [Browse] The utility will perform a brief site survey and display the results to you. Click on the SSID[5] of the access point you would like to connect to and

[3] **Infrastructure:** You will need an access point to use the ZyXEL wireless adapter in Infrastructure mode. Because all communication will be done via the Access Point, the Access Point's SSID must be used.

[4] **Ad-Hoc:** In Ad-Hoc mode communication is made peer-to-peer between the client PCs and without the use of an Access Point. All PCs communicating in an Ad-Hoc should use the same SSID (whatever your choice is).

then click on [Add to Profile]. If the access point you choose has encryption enabled, a window will pop up reminding you to enter the encryption information on the next page. If your access point is not listed, close the [Site Survey] window, and type the name of the SSID into the [SSID] field.

d. Click [Next]. The following screen will appear.



ZyAIR Profile wizard

WLAN Security Configuration

Security mode: No Encryption

Authentication protocol: None

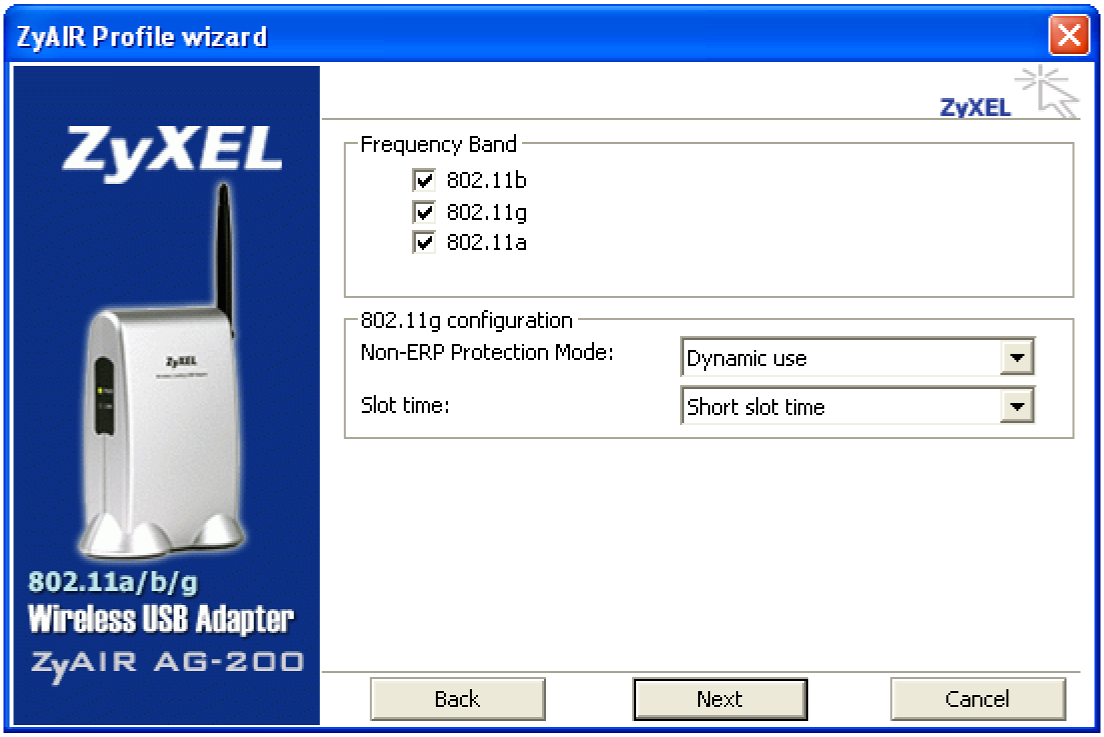
Encryption method: □ Using Static WEP

This screen will vary in appearance depending on whether any encryption was detected with your access point.

3) Enter in the appropriate security information.

[5] ***SSID:*** *The SSID is a group name used by users of a common wireless network. Only those devices using the same SSID are able to access each other. Also, you must use the same SSID as the Access Point you want to connect with. SSIDs are case sensitive so take care to make sure your capitalization matches.*

a. Click [Next]. The following screen will appear.



Frequency Band

☑ 802.11b
☑ 802.11g
☑ 802.11a

802.11g configuration

Non-ERP Protection Mode: Dynamic use

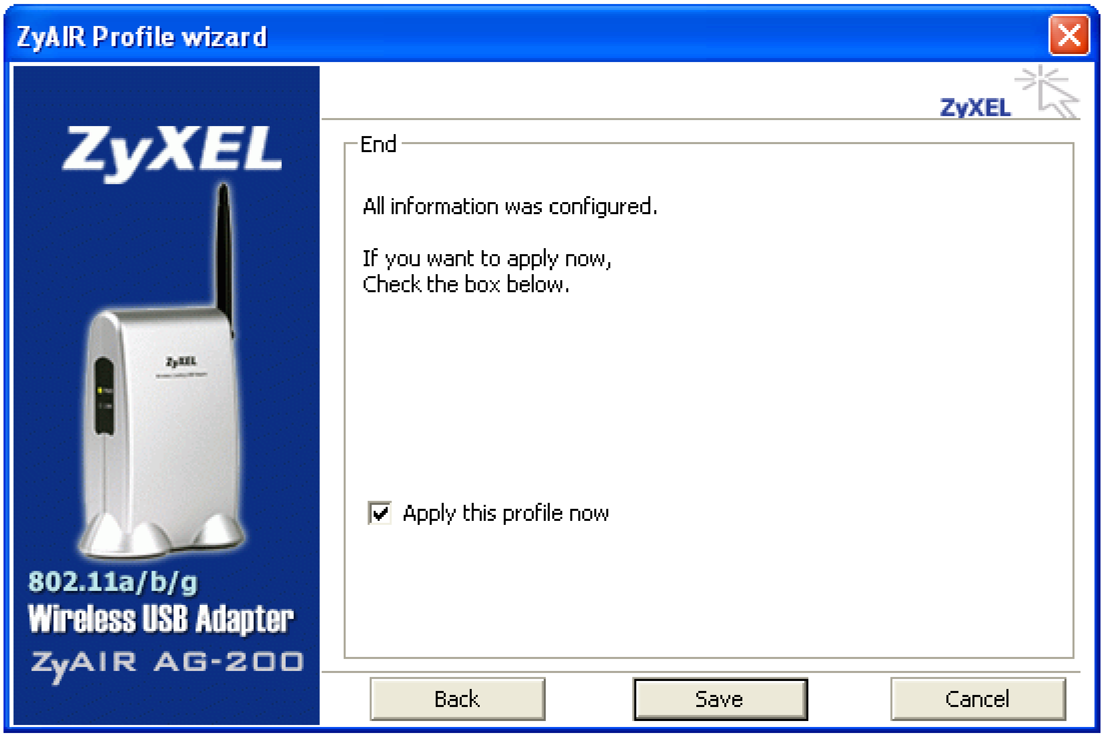
Slot time: Short slot time

4) On this screen you will configure the wireless modes supported by this profile.

a. Under [Frequency Band], put a check mark next to each wireless protocol you want this profile to support. If you are unsure of which protocol to choose, leave all checked.

b. For [802.11g Configuration] leave all settings at default unless instructed by your network administrator to change them.

c. Click [Next]. The following screen will appear.



End

All information was configured.

If you want to apply now,
Check the box below.

☑ Apply this profile now

5) Final Step

a. Uncheck the box [Apply this profile now] if you do not want to activate this profile at this time.

b. Click [Save] to complete the wizard and save the profile you have just created.

Remove

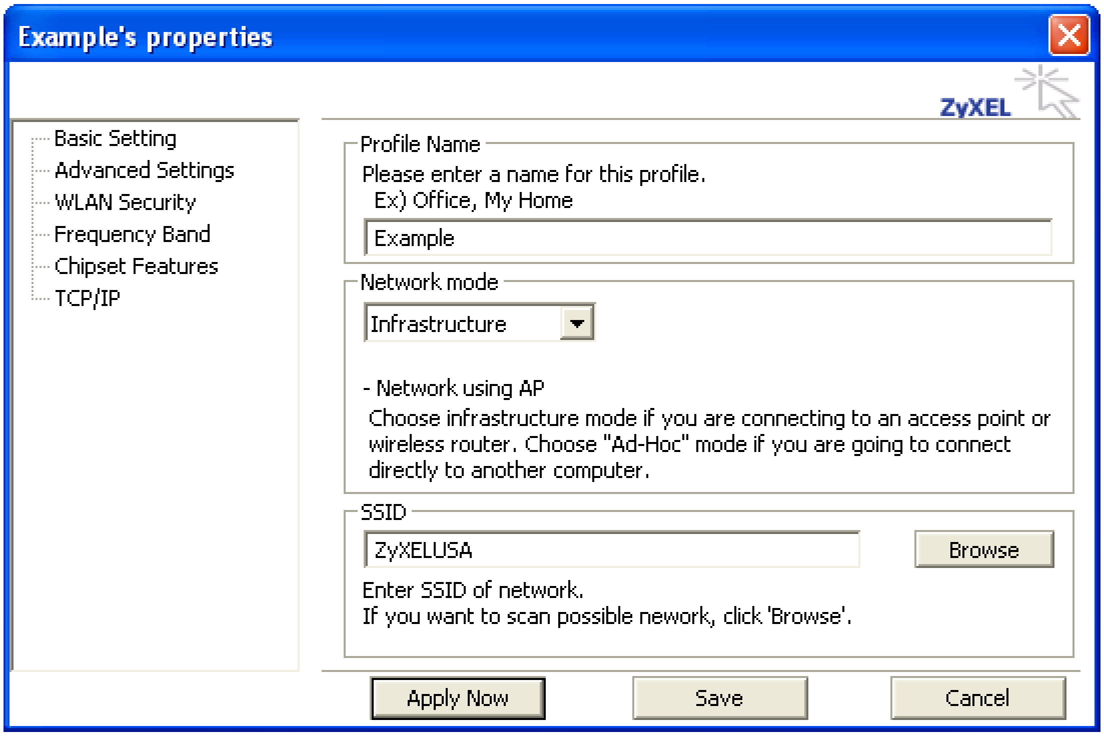
To remove a profile from the "Profile List" select it and then click on [Remove].

Apply

If you want to change the current profile with another profile from the "Profile List", select the desired profile and click on [Apply]. The new profile will immediately become the current profile and you will be connected with its SSID.

Properties

Selecting a profile from the "Profile List" and clicking on [Properties] will allow you to check and/or modify the properties of the selected profile. Clicking on [Properties] will take you to the following screen.



Profile Name

Please enter a name for this profile.
Ex) Office, My Home

Example

Network mode

Infrastructure

- Network using AP

Choose infrastructure mode if you are connecting to an access point or wireless router. Choose "Ad-Hoc" mode if you are going to connect directly to another computer.

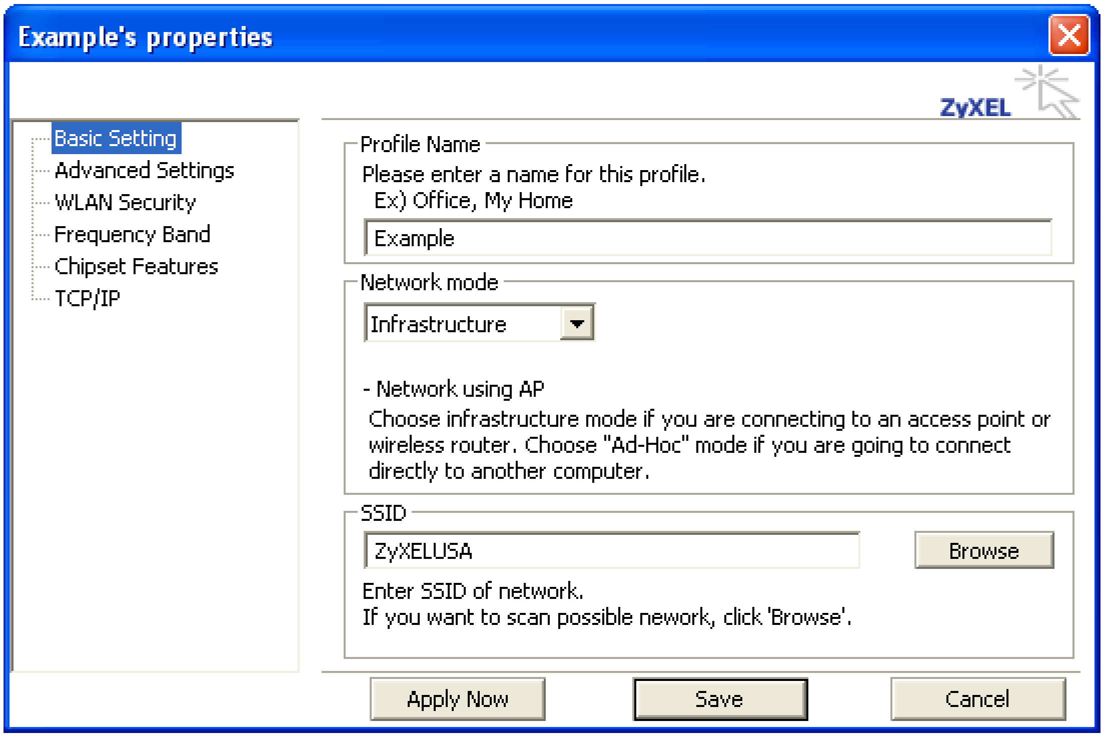
SSID

ZyXELUSA

Enter SSID of network.
If you want to scan possible nework, click 'Browse'.

Each page in [Properties] is explained below.

Basic Settings: In this page, you can verify the name of the current profile.



Profile Name

Please enter a name for this profile.
Ex) Office, My Home

Example

Network mode

Infrastructure

- Network using AP
Choose infrastructure mode if you are connecting to an access point or wireless router. Choose "Ad-Hoc" mode if you are going to connect directly to another computer.

SSID

ZyXELUSA

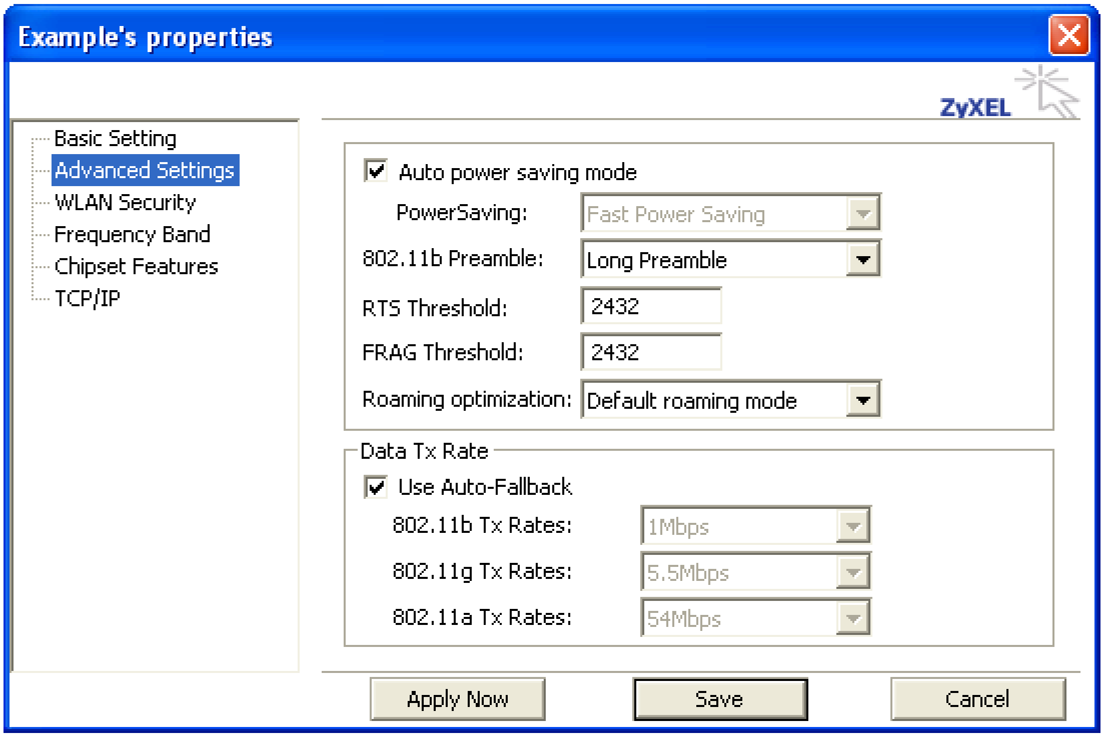
Enter SSID of network.
If you want to scan possible nework, click 'Browse'.

[Profile Name] Allows you to change the name of the current profile.

[Network Mode] Allows you to change between Infrastructure and Ad-Hoc networking modes.

[SSID] Allows you to change the SSID that this profile will associate with. Use the [Browse] button to perform a site survey and select the SSID from a list of available SSIDs. Keep in mind when manually entering an SSID that SSIDs are case sensitive.

Advanced Settings: This screen allows you to make changes to the default ways the adapter 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.



☑ Auto power saving mode

PowerSaving: Fast Power Saving

802.11b Preamble: Long Preamble

RTS Threshold: 2432

FRAG Threshold: 2432

Roaming optimization: Default roaming mode

Data Tx Rate

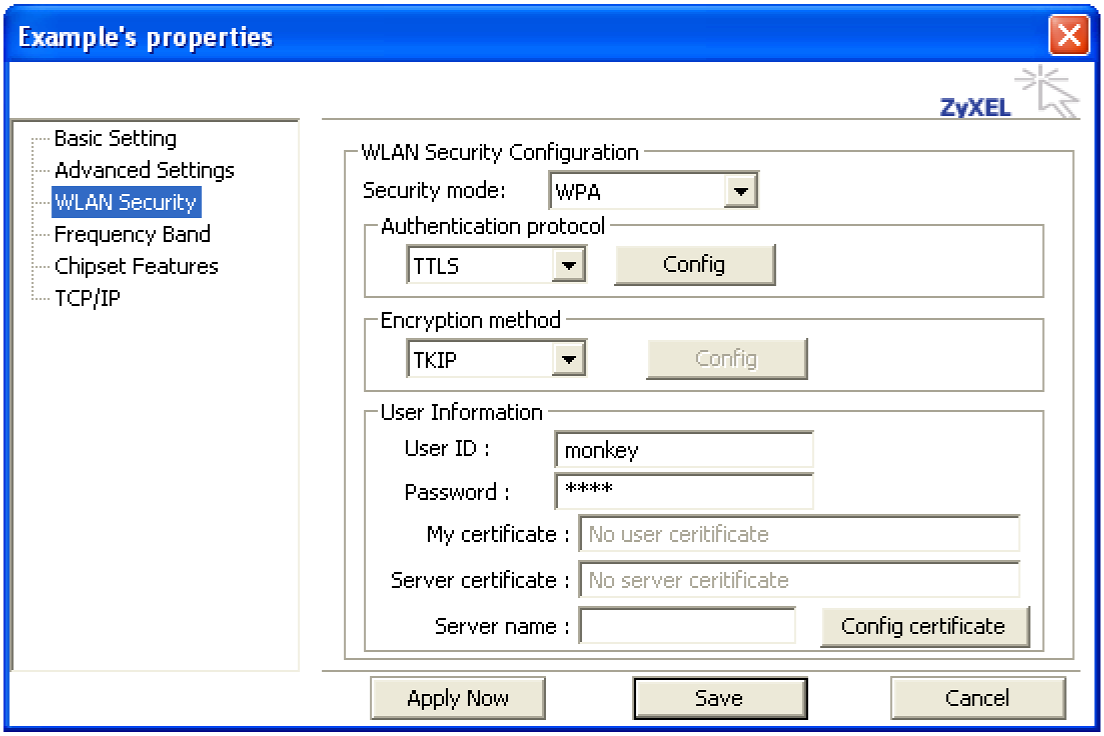
☑ Use Auto-Fallback

802.11b Tx Rates: 1Mbps

802.11g Tx Rates: 5.5Mbps

802.11a Tx Rates: 54Mbps

WLAN Security: This screen allows you to configure the security settings of your wireless LAN.



Security mode: WPA

TTLS

TKIP

User ID : monkey

Password : ****

My certificate : No user ceritificate

Server certificate : No server ceritificate

Server name :

Security Mode

1) No Encryption

   All data sent between the AP and the client is left unencrypted and may be viewed by other wireless devices.

2) 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 152-bit), only those APs and PCs using the same WEP Key are allowed to communicate with each other.

3) WPA

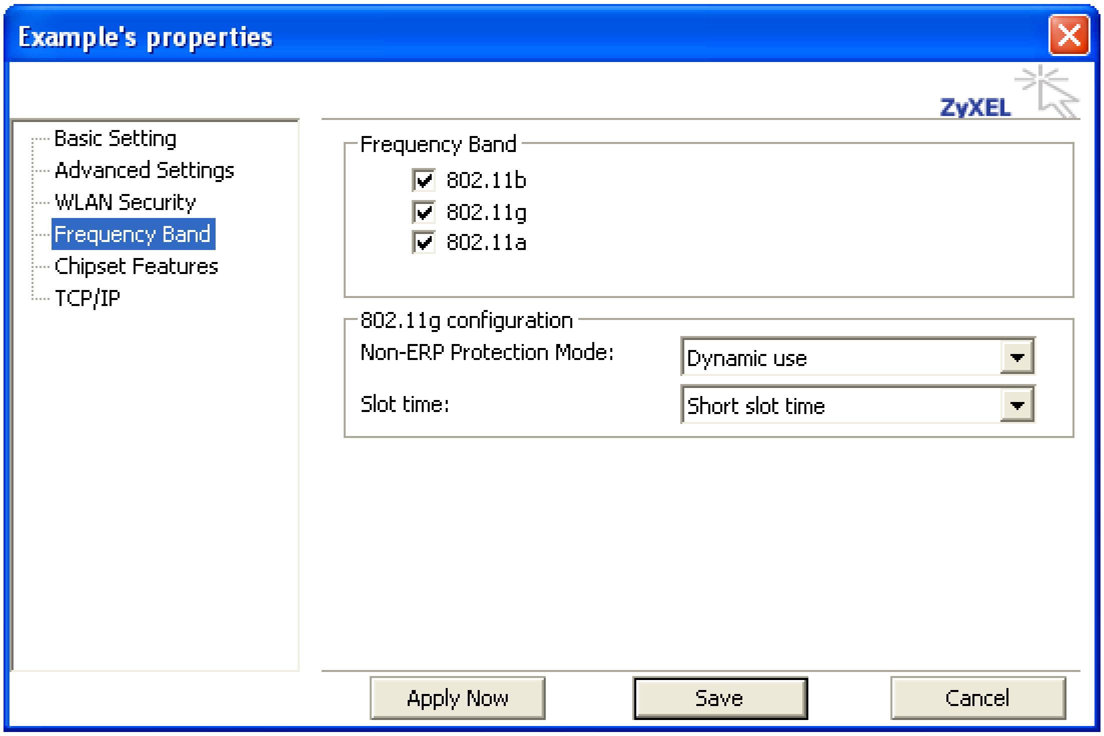
   Wi-Fi Protected Access – Encrypts all traffic between the access point and the client using either TKIP or AES encryption. Depending on the authentication protocol selected, each client must authenticate using their own unique username, password, and security certificate.

To learn more about WPA please see Chapter 2.

4) WPA-PSK

WPA-PSK is a compromise between WPA and WEP. 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 either TKIP or AES, which improve greatly over the encryption found in WEP. We recommend you use WPA or WPA-PSK whenever possible.

Frequency Band: This screen lets you define which 802.11 wireless standards to try to connect to. It also lets you change some 802.11g behaviors.



Frequency Band

☑ 802.11b

☑ 802.11g

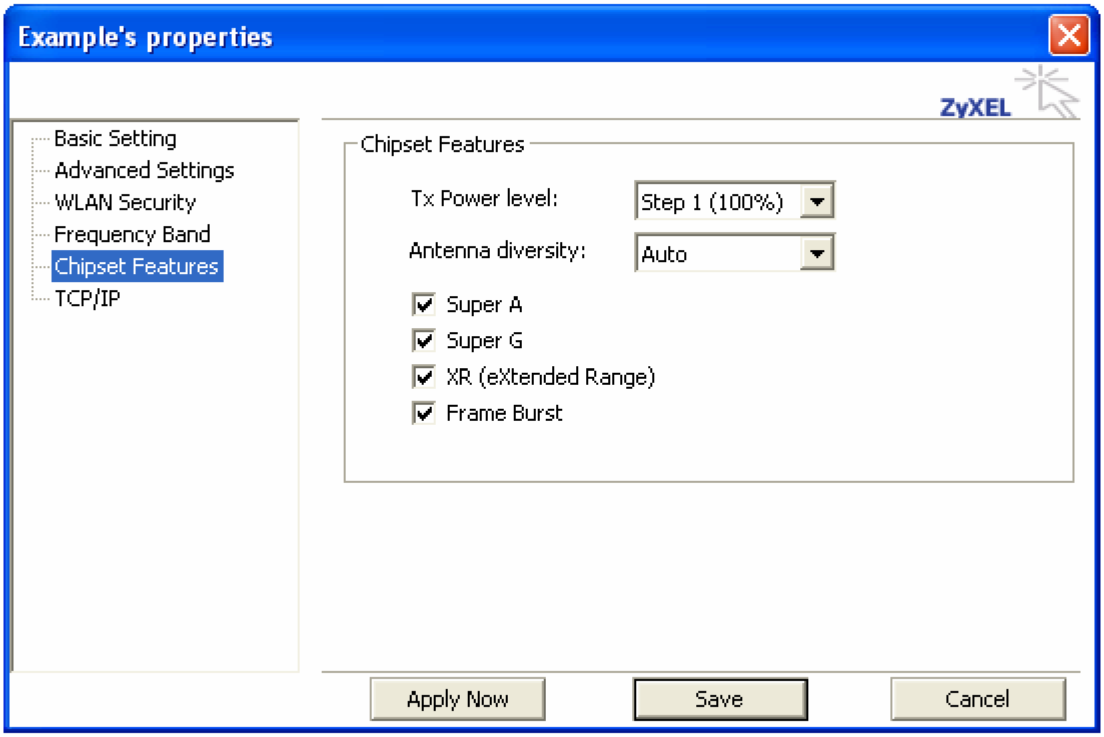
☑ 802.11a

802.11g configuration

Non-ERP Protection Mode: Dynamic use

Slot time: Short slot time

Chipset Features: This screen allows you to configure advanced features built into the wireless chipset.



Chipset Features

Tx Power level: Step 1 (100%)

Antenna diversity: Auto

☑ Super A

☑ Super G

☑ XR (eXtended Range)

☑ Frame Burst

[Tx Power Level] Allows you to adjust the output power of your radio. Reducing output power can reduce power usage of your laptop and will limit the distance that your wireless signal will reach.

[Antenna Diversity] Defines whether to use both internal antennas. Antenna Diversity usually provides a higher quality connection.

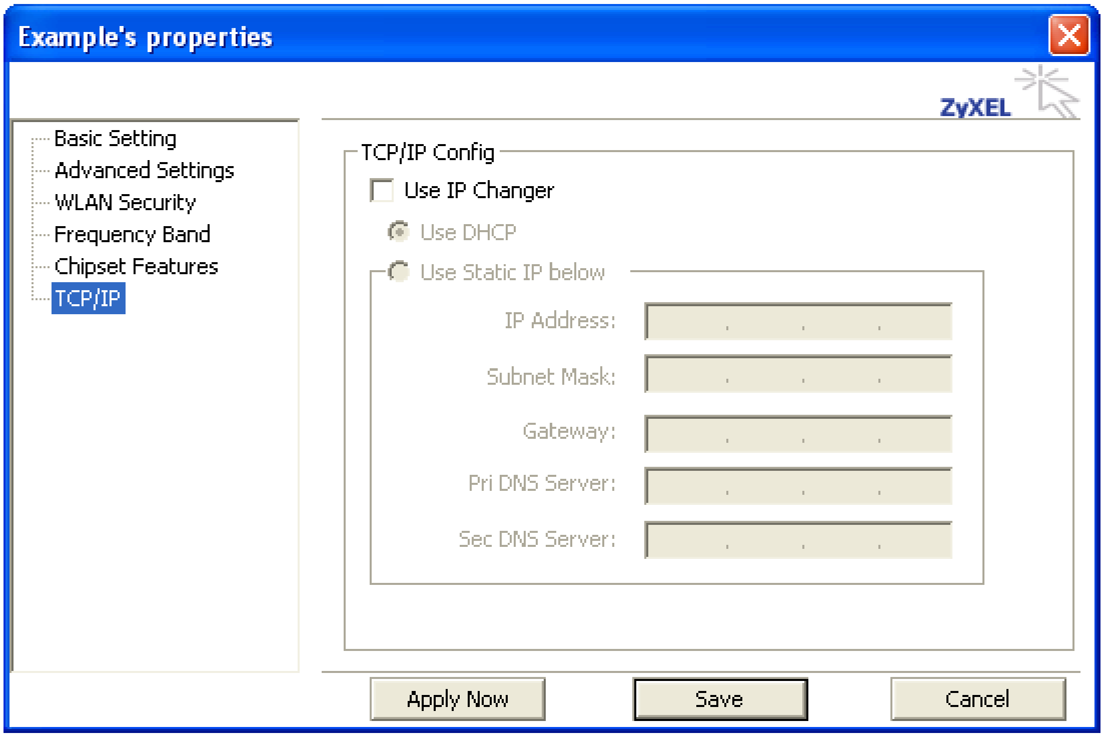
[Super A] Support for Atheros 108Mbps Super A mode.

[Super G] Support for Atheros 108Mbps Super G mode.

[XR] Support for Atheros Extended Range technology.

[Frame Burst] Allows for faster speeds while maintaining compatibility with other 802.11 devices which may be on your network.

TCP/IP: This allows you to change your TCP/IP settings.



Example's properties

□ Use IP Changer

● Use DHCP

○ Use Static IP below

IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

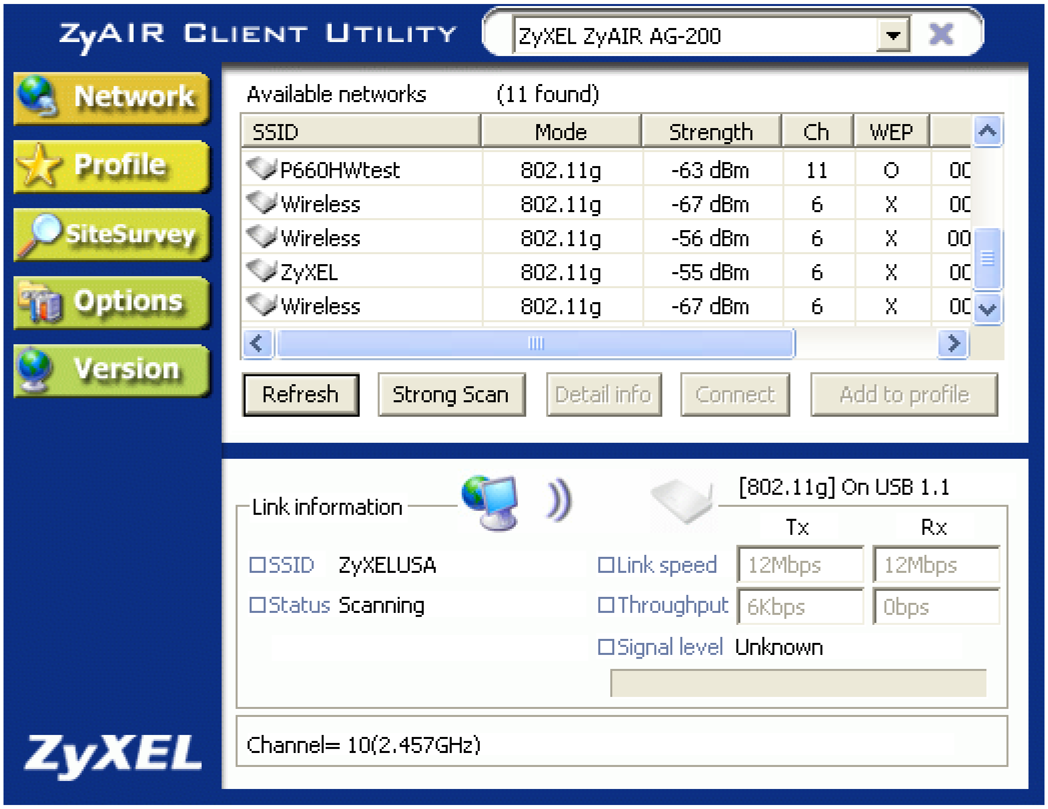
Pri DNS Server: . . .

Sec DNS Server: . . .

[Use IP Changer] By putting a checkmark in the box, you will overwrite your existing WLAN TCP/IP configuration and use the IP Changer software built-into the ZyXEL Utility. This allows you to configure TCP/IP settings for each profile.

1.3.3 Site Survey

This page shows a list of SSIDs in your vicinity. Information regarding each SSID is also shown: SSID, mode, signal strength, channel, BSSID (MAC address), data rate, and WEP/WPA status.



Available networks (11 found)

SSID	Mode	Strength	Ch	WEP	
P660HWtest	802.11g	-63 dBm	11	O	0C
Wireless	802.11g	-67 dBm	6	X	0C
Wireless	802.11g	-56 dBm	6	X	00
ZyXEL	802.11g	-55 dBm	6	X	0C
Wireless	802.11g	-67 dBm	6	X	0C

Link information

[802.11g] On USB 1.1

	Tx	Rx
□SSID ZyXELUSA		
□Status Scanning		
□Link speed	12Mbps	12Mbps
□Throughput	6Kbps	0bps
□Signal level Unknown		

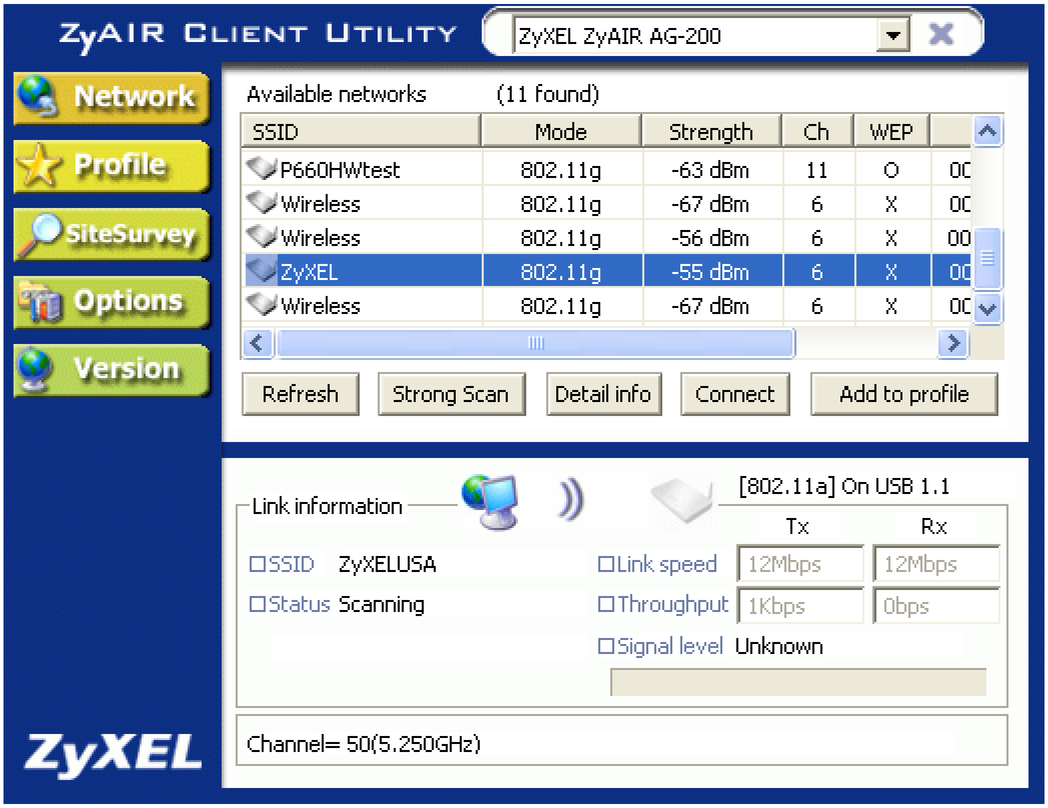
Channel= 10(2.457GHz)

Refresh

[Refresh] will scan the vicinity for a certain amount of time and display the scan results.

Strong Scan

[Strong Scan] will continuously scan the vicinity every 2.5 seconds until you click on [Stop], which appears in place of [Strong Scan] when scanning.



Available networks (11 found)

SSID	Mode	Strength	Ch	WEP	
P660HWtest	802.11g	-63 dBm	11	O	00
Wireless	802.11g	-67 dBm	6	X	00
Wireless	802.11g	-56 dBm	6	X	00
ZyXEL	802.11g	-55 dBm	6	X	00
Wireless	802.11g	-67 dBm	6	X	00

Link information

[802.11a] On USB 1.1

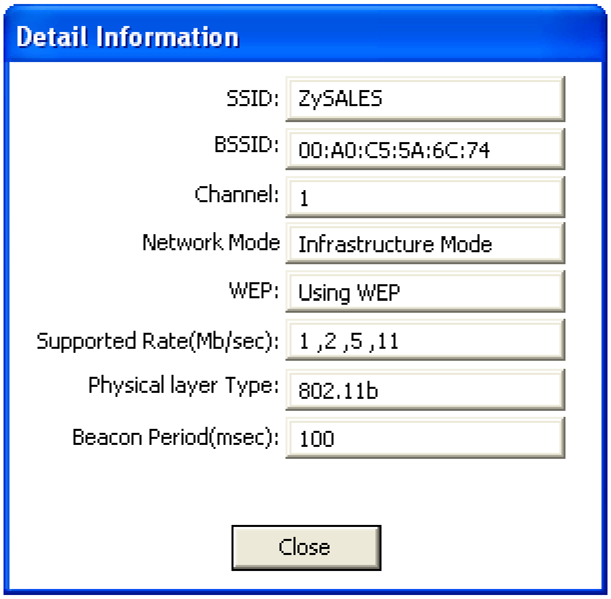
			Tx	Rx
□SSID ZyXELUSA		□Link speed	12Mbps	12Mbps
□Status Scanning		□Throughput	1Kbps	0bps
		□Signal level	Unknown	

Channel= 50(5.250GHz)

Selecting a network from the [Available Networks] list will enable the [Detail Info], [Connect] and [Add to profile] buttons.

Detail Info

[Detail info] will display the following screen showing the selected device's configuration information. An alternative to clicking on [Detail info] is double-clicking on the SSID of choice.



Detail Information

SSID:	ZySALES
BSSID:	00:A0:C5:5A:6C:74
Channel:	1
Network Mode	Infrastructure Mode
WEP:	Using WEP
Supported Rate(Mb/sec):	1 ,2 ,5 ,11
Physical layer Type:	802.11b
Beacon Period(msec):	100

Connect

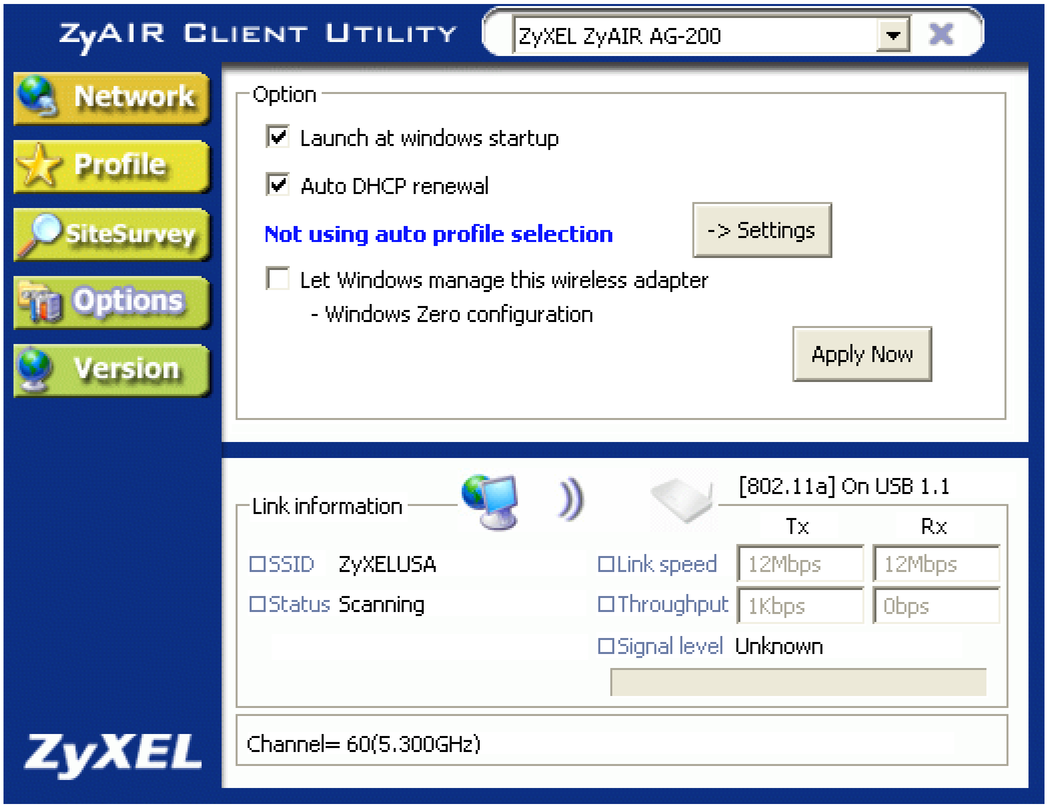
[Connect] will immediately connect you with the selected network.

Add to profile

[Add to profile] will have the same effect as clicking on [Add] in the [Profile] page

1.3.4 Options

In this page you can configure the behavior of the ZyXEL utility.



ZyXEL ZyAIR AG-200

Option

☑ Launch at windows startup

☑ Auto DHCP renewal

Not using auto profile selection

□ Let Windows manage this wireless adapter
- Windows Zero configuration

Link information

[802.11a] On USB 1.1

		Tx	Rx
□SSID ZyXELUSA	□Link speed	12Mbps	12Mbps
□Status Scanning	□Throughput	1Kbps	0bps
	□Signal level	Unknown	

Channel= 60(5.300GHz)

Launch at windows startup

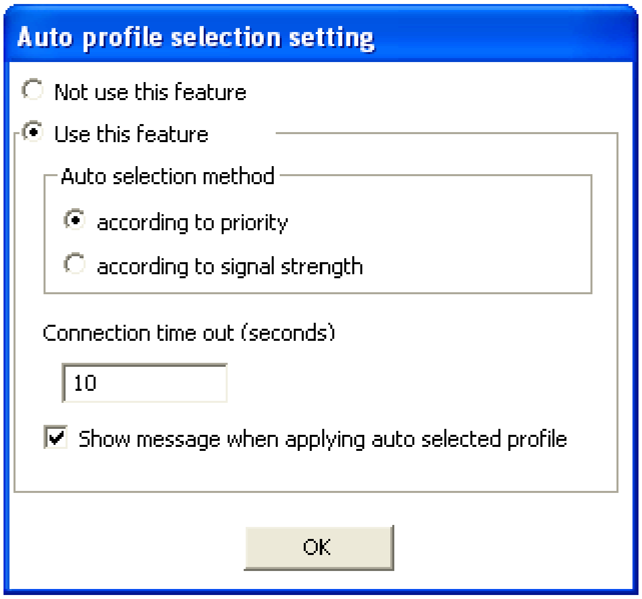
Selecting this option will automatically start the ZyXEL Utility program whenever you start Windows.

Auto DHCP renewal

Automatically renews the DHCP information after changing profiles.

Auto-Profile Selection

Allows you to define the behavior of the auto-profile selection algorithm. Click [Settings] to configure. See following screen shot for options.



Auto profile selection setting

○ Not use this feature

● Use this feature

Auto selection method

● according to priority

○ according to signal strength

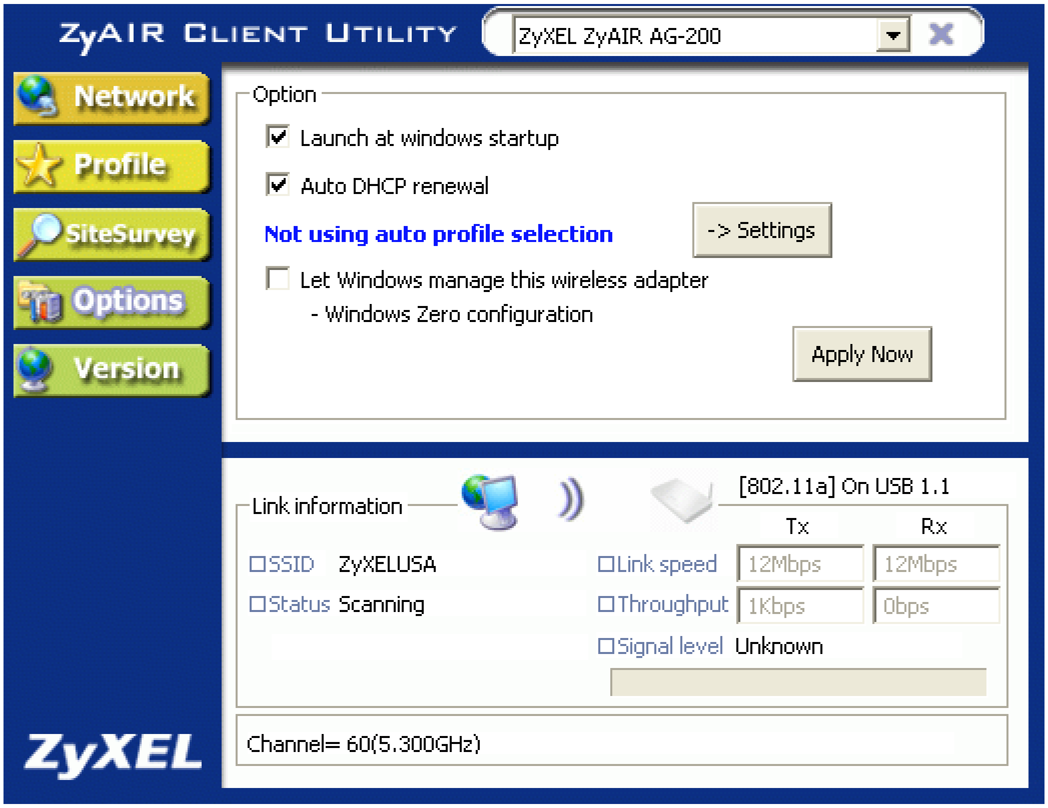
Connection time out (seconds)

10

☑ Show message when applying auto selected profile

1.3.5 Version

Software and Hardware information of the current client device.



ZyXEL ZyAIR AG-200

Option

☑ Launch at windows startup

☑ Auto DHCP renewal

Not using auto profile selection -> Settings

□ Let Windows manage this wireless adapter - Windows Zero configuration

Apply Now

			Tx	Rx
□SSID ZyXELUSA		□Link speed	12Mbps	12Mbps
□Status Scanning		□Throughput	1Kbps	0bps
		□Signal level	Unknown	

Channel= 60(5.300GHz)

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 AG-200 provides various transmission (data) rate options for you to select. Options include **Fully Auto**, **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **11 Mbps**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, **54 Mbps** and **108 Mbps**. In most networking scenarios, the factory default **Fully Auto** setting proves the most efficient. This setting allows your ZyXEL AG-200 to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the ZyXEL AG-200 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 AG-200 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 AG-200 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).

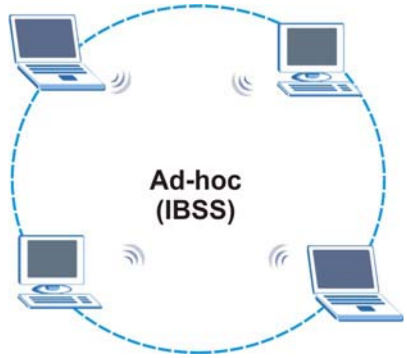


Figure 2-1 IBSS Example

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).

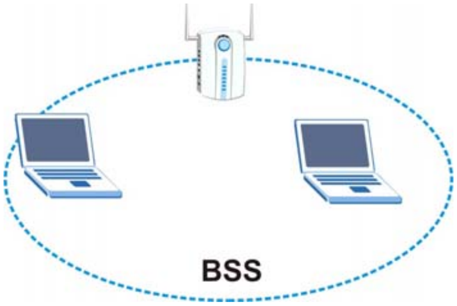


Figure 2-2 BSS Example

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.

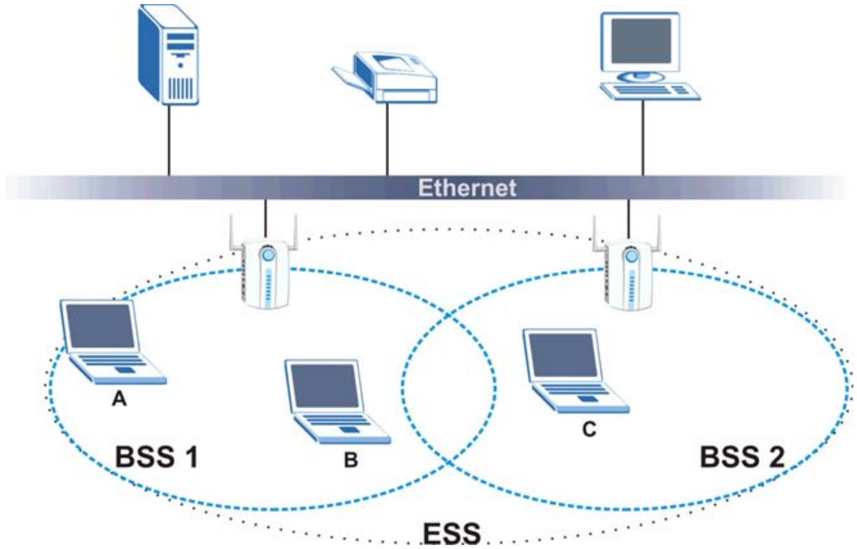


Figure 2-3 Infrastructure Network Example

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 AG-200 in wireless station **B** automatically switches the channel to the one used by access point **2** in order to stay connected to the network.

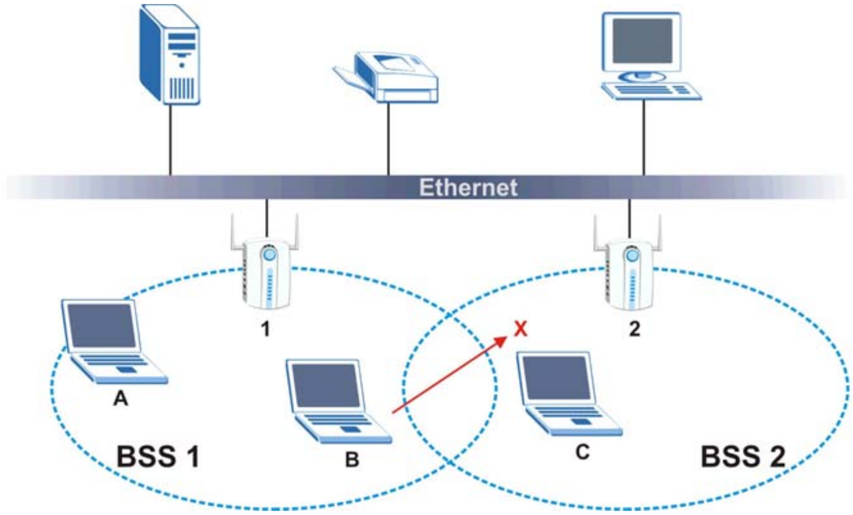


Figure 2-4 Roaming Example

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 AG-200. 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.

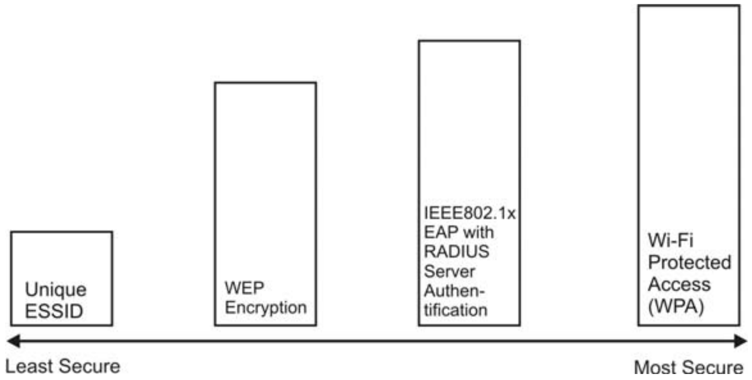

Unique ESSID
WEP Encryption
IEEE802.1x EAP with RADIUS Server Authen-tification
Wi-Fi Protected Access (WPA)
Least Secure
Most Secure

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 AG-200, the ZyXEL AG-200'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 AG-200 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 AG-200.

- 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 AG-200 allows you to configure up to four 64-bit, 128-bit or 152-bit WEP keys and only one key is used as the default key at any one time.

2.2.2 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 AG-200 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.

2.2.3 WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

Therefore, if you don't have an external RADIUS server, you should use WPA-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

Encryption

WPA improves data encryption by using either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. 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. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

2.2.4 WPA-PSK Application Example

A WPA-PSK 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.

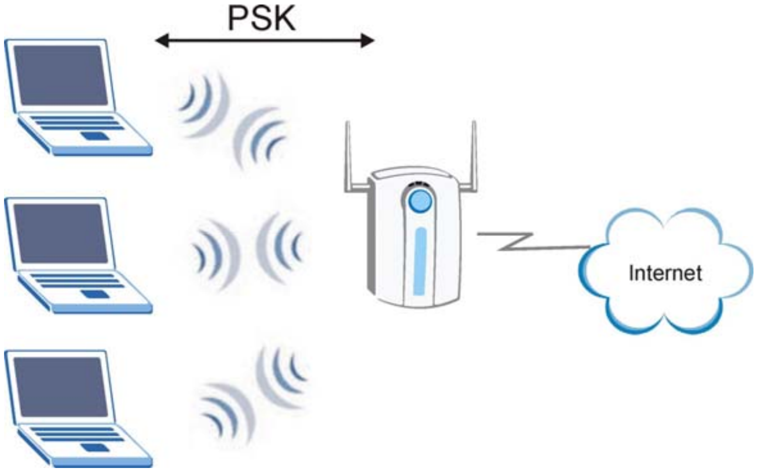


Figure 2-6 WPA-PSK Authentication

2.2.5 WPA 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 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.

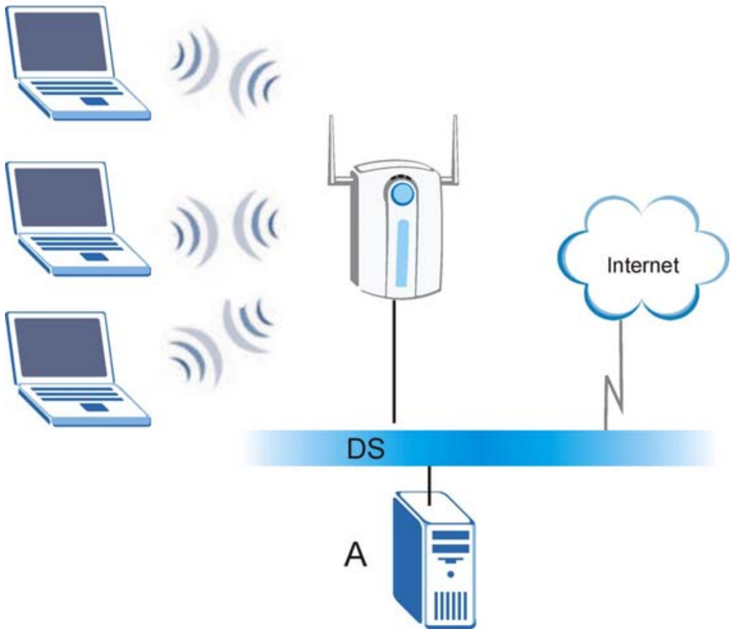


Figure 2-7 WPA with RADIUS Application Example

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 AG-200 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.

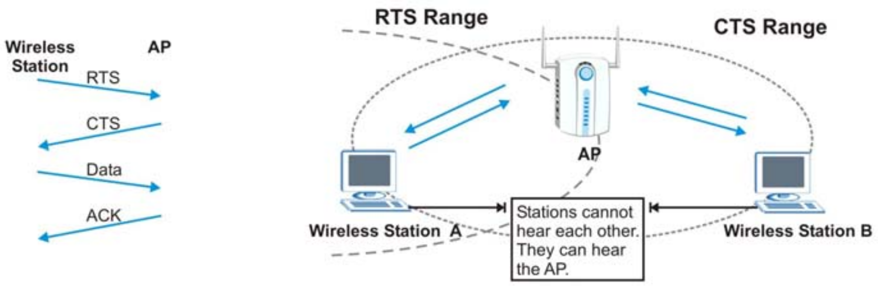


Figure 2-8 RTS Threshold

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 Authentication Type

The IEEE 802.11b standard describes a simple authentication method between the wireless stations and AP. Two authentication modes are defined: **Open** and **Share**.

Open authentication mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP do *not* share a secret key. Thus the wireless stations can associate with any AP and listen to any data transmitted plaintext.

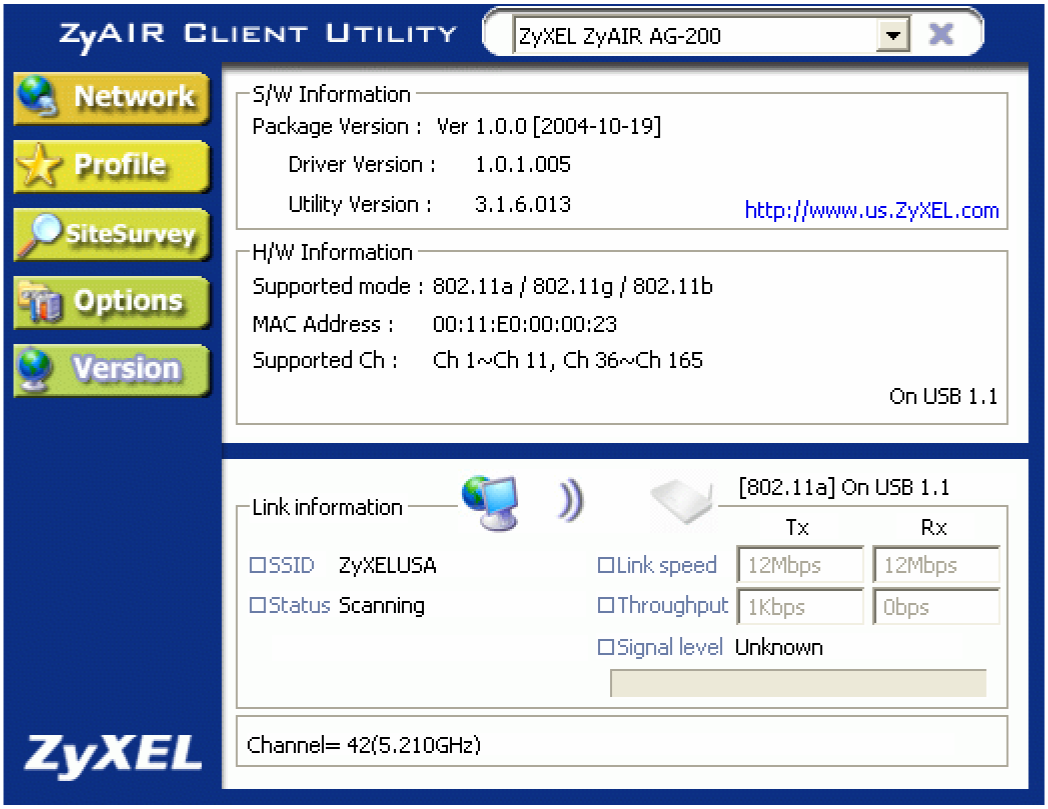
Shared authentication mode involves a shared secret key to authenticate the wireless station to the AP. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP.

Chapter 3 Maintenance

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

3.1 The Version Screen

The **Version** screen displays related version numbers of the ZyXEL AG-200.



S/W Information

Package Version : Ver 1.0.0 [2004-10-19]

Driver Version : 1.0.1.005

Utility Version : 3.1.6.013

http://www.us.ZyXEL.com

H/W Information

Supported mode : 802.11a / 802.11g / 802.11b

MAC Address : 00:11:E0:00:00:23

Supported Ch : Ch 1~Ch 11, Ch 36~Ch 165

On USB 1.1

Link information

[802.11a] On USB 1.1

				Tx	Rx
□SSID	ZyXELUSA		□Link speed	12Mbps	12Mbps
□Status	Scanning		□Throughput	1Kbps	0bps
			□Signal level	Unknown	

Channel= 42(5.210GHz)

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

About

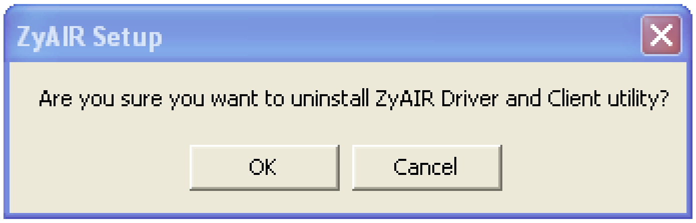
LABEL	DESCRIPTION
Package Version	This field displays the version number of the combination driver/utility package.
Driver Version	This field displays the version number of the ZyXEL driver.
Utility Version	This field displays the version number of the ZyXEL utility.

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 ZyAIR SW, Uninstall.**

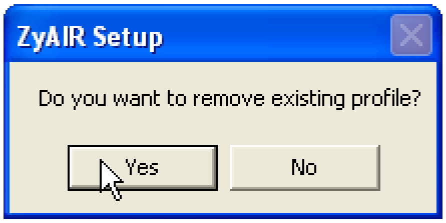
Step 2. When prompted, click [OK] to remove the driver and the utility software.



ZyAIR Setup

Are you sure you want to uninstall ZyAIR Driver and Client utility?

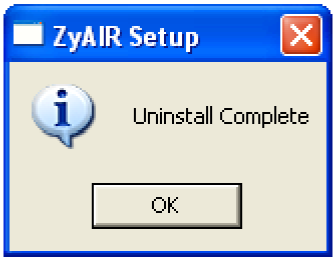
Step 3. When prompted select whether to remove or keep your existing profiles.



ZyAIR Setup

Do you want to remove existing profile?

Step 4. Click [Ok] to finish the uninstall process. Reboot your computer if prompted to do so.



ZyAIR Setup

Uninstall Complete

3.3 Upgrading the ZyXEL Utility

Before you uninstall the ZyXEL 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 **Version** screen to make sure the new utility is installed properly.

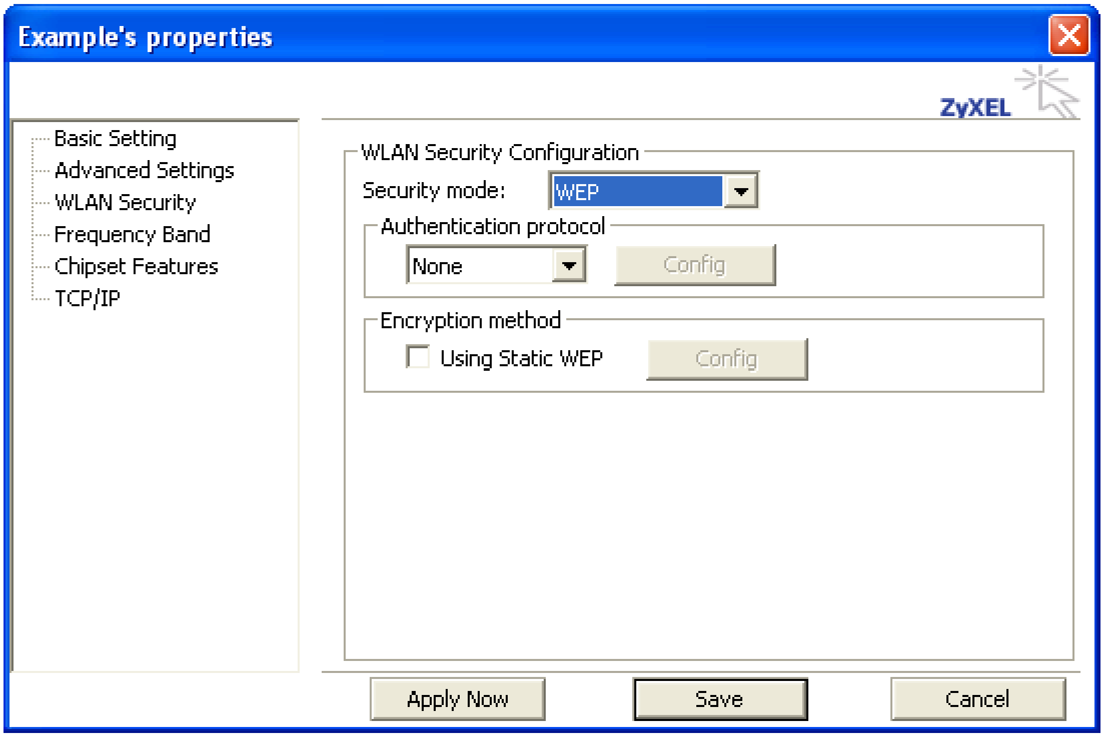
Chapter 4
Configuring Wireless Security

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 profile you wish to edit under the [Profile] tab, select [Properties] and then choose [WLAN Security]. You are also presented with the option to configure security during the profile creation process. Whether changing the security settings of an existing profile or creating a new profile, the steps to configure your security settings remain the same.

4.2 Configuring WEP



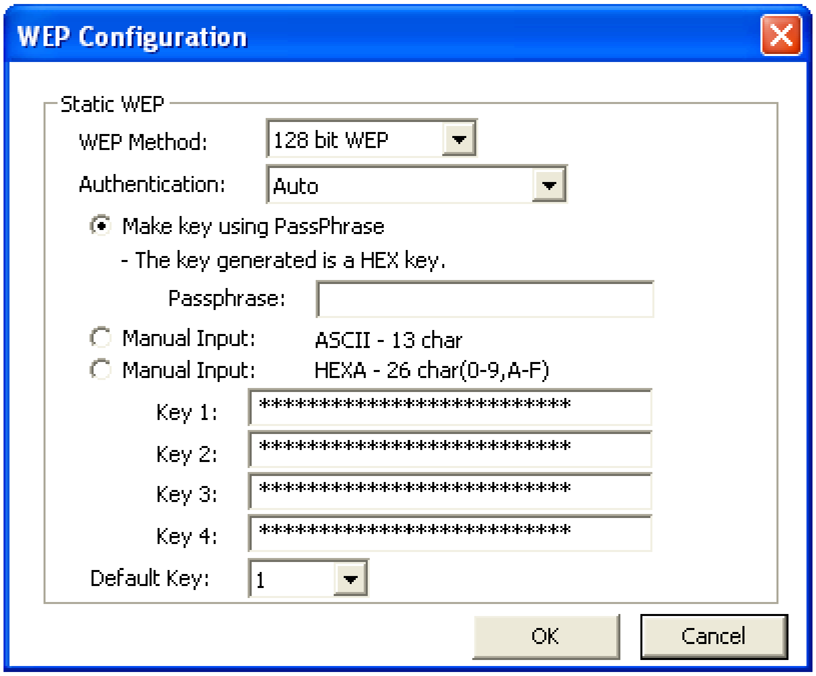
WLAN Security Configuration

Security mode: WEP

Authentication protocol: None

Encryption method: □ Using Static WEP

1. Select [WEP] under [Security Mode]
2. Put a check mark next to [Using Static WEP]
3. Click [Config]. You will then see the screen below.



WEP Configuration

Static WEP

WEP Method: 128 bit WEP

Authentication: Auto

● Make key using PassPhrase

- The key generated is a HEX key.

Passphrase:

○ Manual Input: ASCII - 13 char

○ Manual Input: HEXA - 26 char(0-9,A-F)

Key 1: **************************

Key 2: **************************

Key 3: **************************

Key 4: **************************

Default Key: 1

4. [WEP Method] Select the correct encryption level to match your access point. Either 64, 128, or 152-bit. The encryption level set her must match the encryption level used by your access point.

a. [Authentication] You can choose between Auto, Open System, and Shared. Please see section 2.5 for more information on the different types of authentication. For most installations choosing “Auto” is the best choice.

b. Enter the WEP key exactly as you did in your access point.

There are three ways of generating a WEP Key:

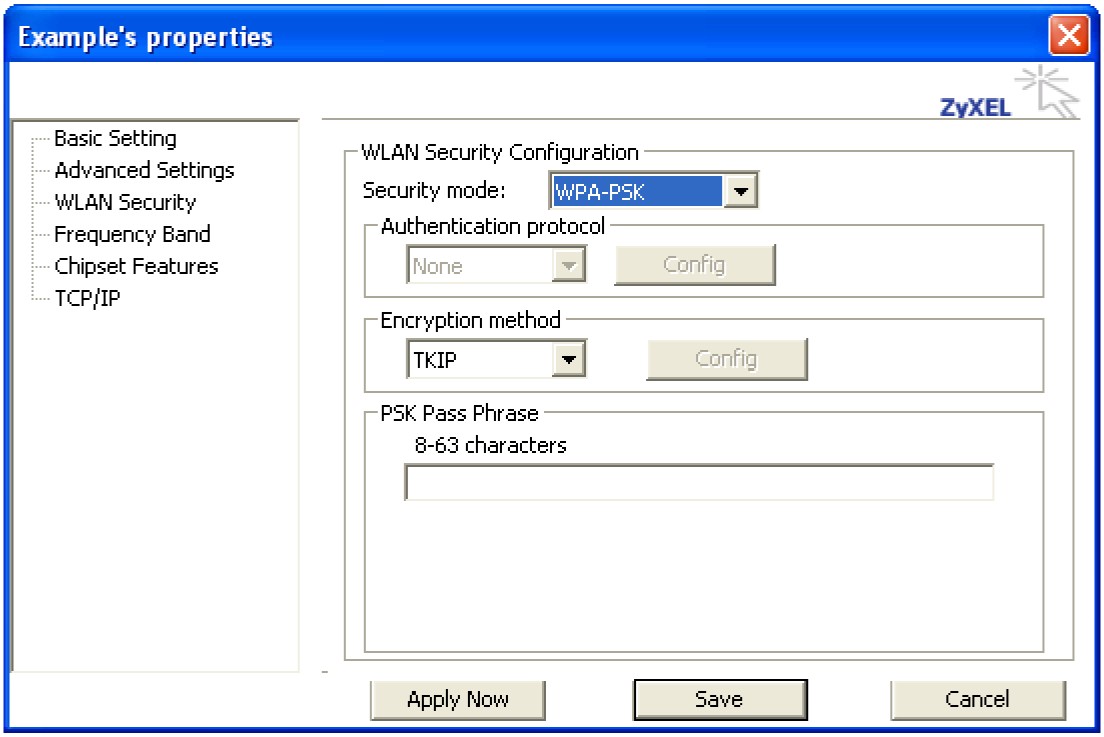
Make key using PassPhrase: a WEP Key is automatically generated as you type in any PassPhrase of your choice. Use this feature when you have used a PassPhrase to generate your WEP key on your access point.

Manual Input (ASCII): You generate your own WEP Key using ASCII characters (5 characters for 64-bit, 13 characters for 128-bit, 16 characters for 152-bit)

Manual Input (Hexadecimal): You generate your own WEP Key using hexadecimal characters (10 characters for 64-bit, 26 characters for 128-bit, 32 characters for 152-bit).

5. Click [OK] to save your settings and return to the previous screen.
6. If you want to use 802.1x authentication with WEP, you will need to configure your 802.1x settings. Please see section 4.5 for details on configuring 802.1x.

4.3 Configuring WPA-PSK



Example's properties

WLAN Security Configuration

Security mode: WPA-PSK

Authentication protocol: None

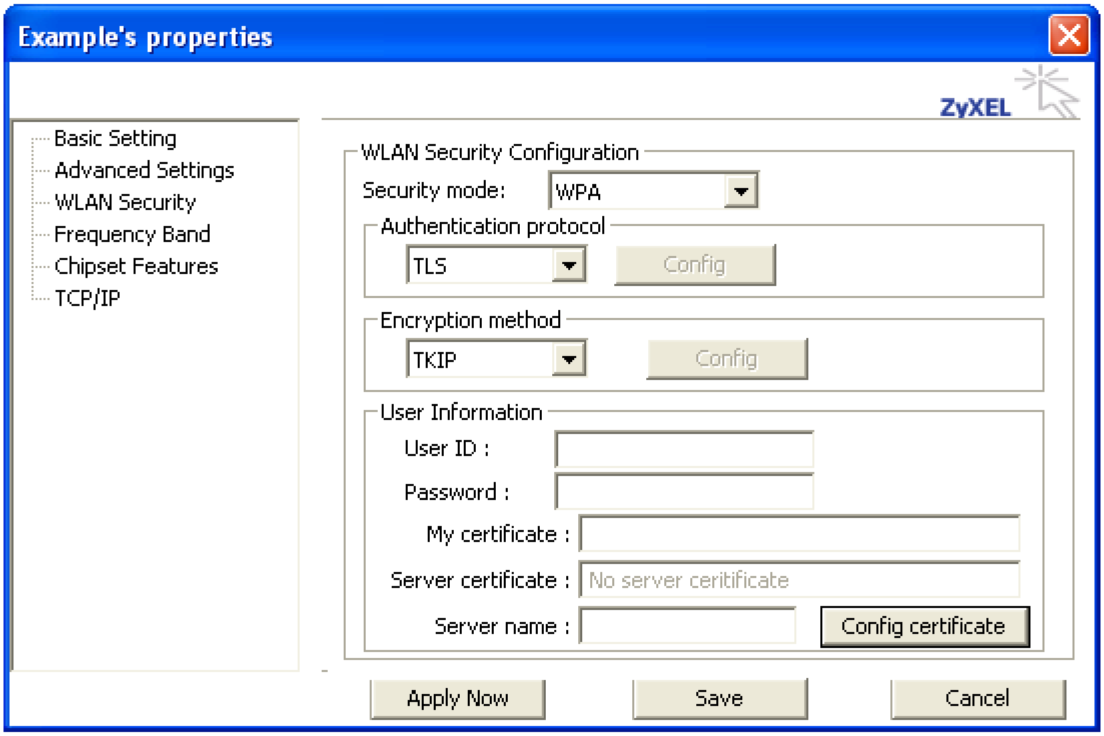
Encryption method: TKIP

PSK Pass Phrase

8-63 characters

1. Select [WPA-PSK] under [Security Mode].
2. Select [Encryption method]. You can choose between TKIP or AES. Most access points use TKIP for WPA-PSK.
3. Under [PSK Pass Phrase] enter the same pass phrase used to configure WPA-PSK on your access point.

4.4 Configuring WPA



Example's properties

WLAN Security Configuration

Security mode: WPA

Authentication protocol: TLS

Encryption method: TKIP

User Information

User ID :

Password :

My certificate :

Server certificate : No server ceritificate

Server name :

1. Select [WPA-PSK] under [Security Mode].
2. Select [Encryption method]. You can choose between TKIP or AES. Most access points use TKIP for WPA.
3. See section 4.5 for configuring 802.1x for WPA.

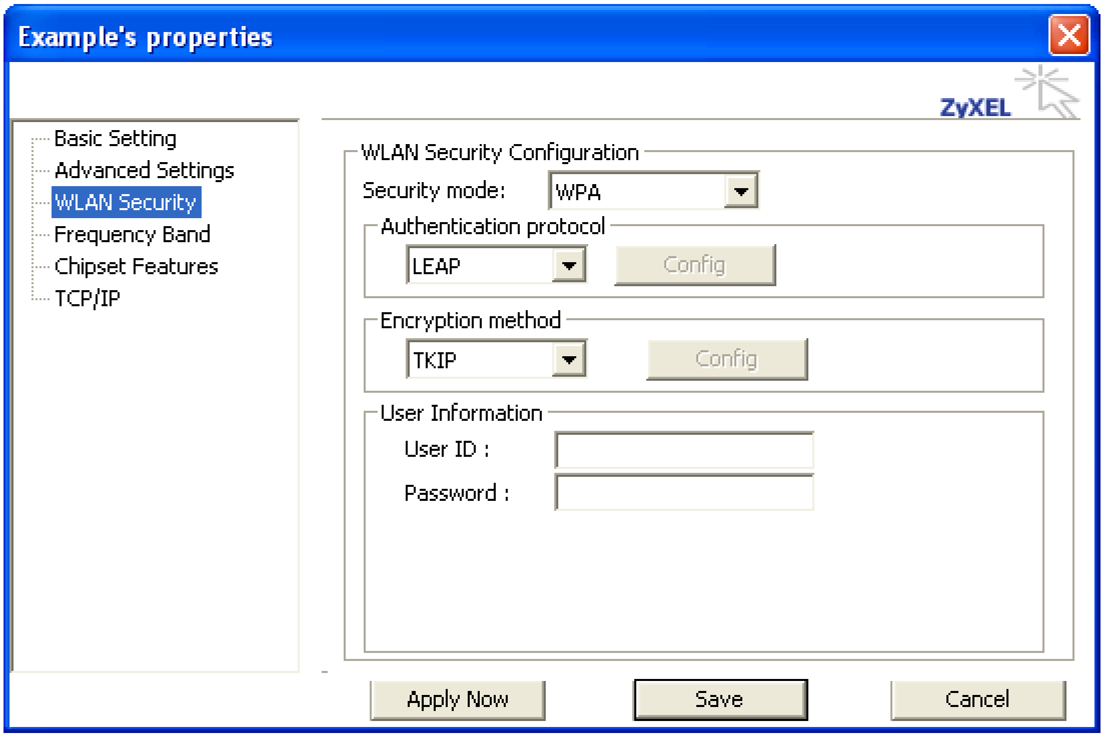
4.5 Configuring 802.1x

1. Choose the EAP method under [Authentication protocol].
2. Depending on the EAP method chosen the options under [User Information] will change.

4.5.1 Configuring 802.1x – EAP-MD5

1. EAP-MD5 is only a choice when use WEP. MD5 is not allowed for WPA.
2. Enter in unique User ID and Password under [User Information]

4.5.2 Configuring 802.1x – EAP-LEAP



WLAN Security Configuration

Security mode: WPA

Authentication protocol

LEAP

Encryption method

TKIP

User Information

User ID :

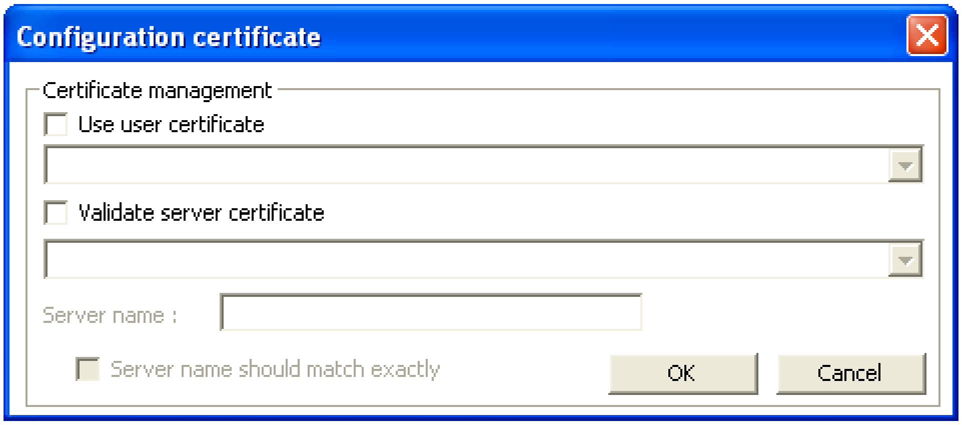
Password :

1. Enter in unique User ID and Password under [User Information]

4.5.3 Configuring 802.1x – EAP-PEAP

1. Click [Config] under [Authentication protocol]
2. Select inner PEAP protocol. You choices are [MS-CHAP v2] or [TLS].
3. Click [OK] to finish and return to the previous screen.
4. Enter in unique User ID and Password under [User Information].
5. If using a user[6] or server certificate click [Config certificate]. The following window appears:

[6] You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.


Configuration certificate
Certificate management
□ Use user certificate
□ Validate server certificate
Server name :
□ Server name should match exactly
OK
Cancel

[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.

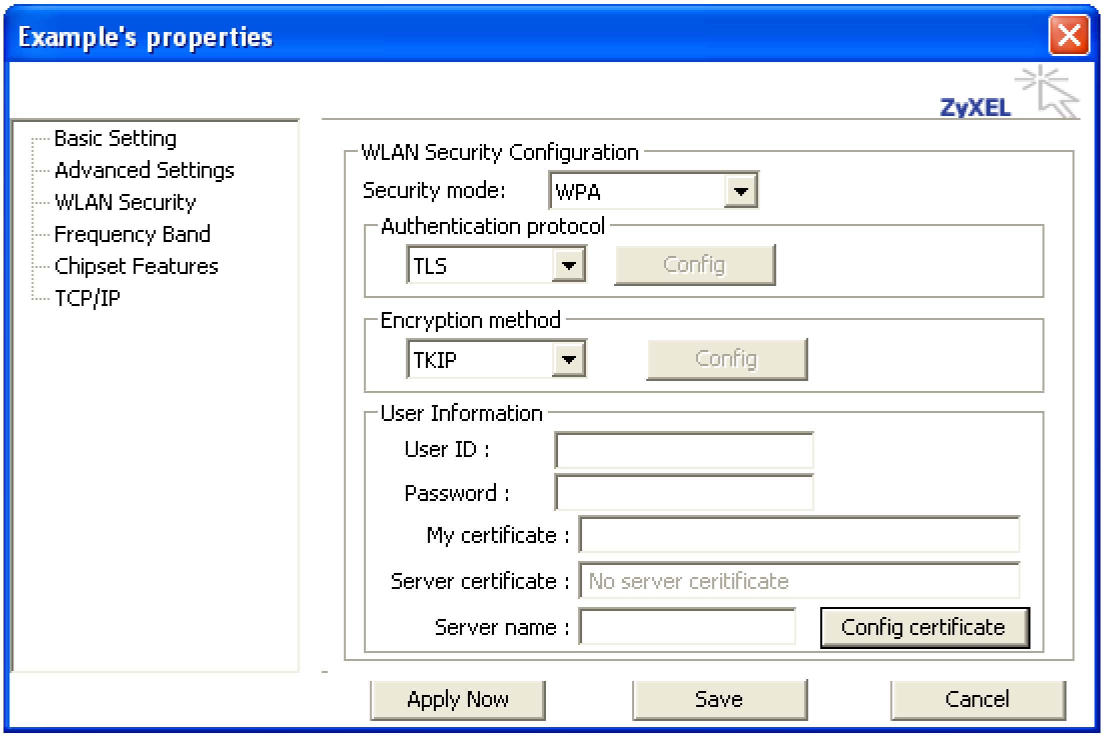
[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.

[Server name]: Name of server used for 802.1x authentication.

[Server name should match exactly]: Check this box to force server name to match exactly the name in the certificate.

6. Click [OK] to finish and return to the previous screen.

4.5.4 Configuring 802.1x – EAP-TLS



Example's properties

Security mode: WPA

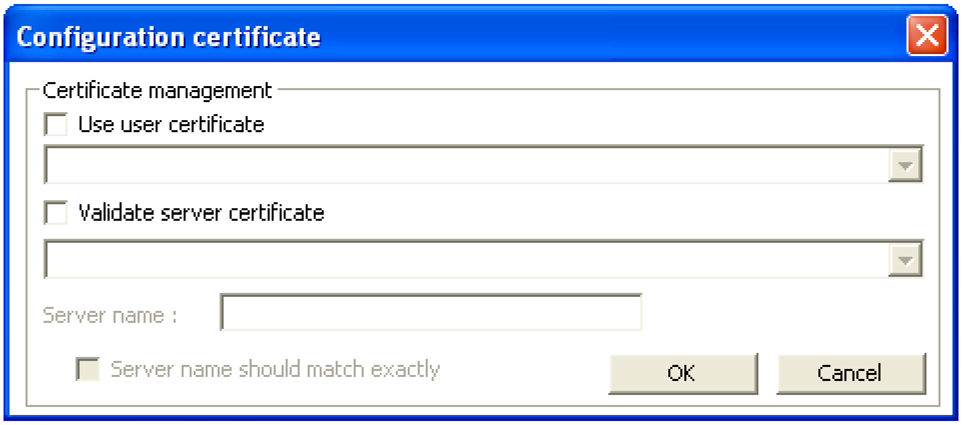
Authentication protocol: TLS

Encryption method: TKIP

Server certificate : No server ceritificate

1. Enter in unique User ID and Password under [User Information].
2. TLS requires you to configure both a server and user[7] certificate.
3. Click [Config certificate]. The following window appears:

[7] You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.


Configuration certificate
Certificate management
□ Use user certificate
□ Validate server certificate
Server name :
□ Server name should match exactly
OK
Cancel

[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.

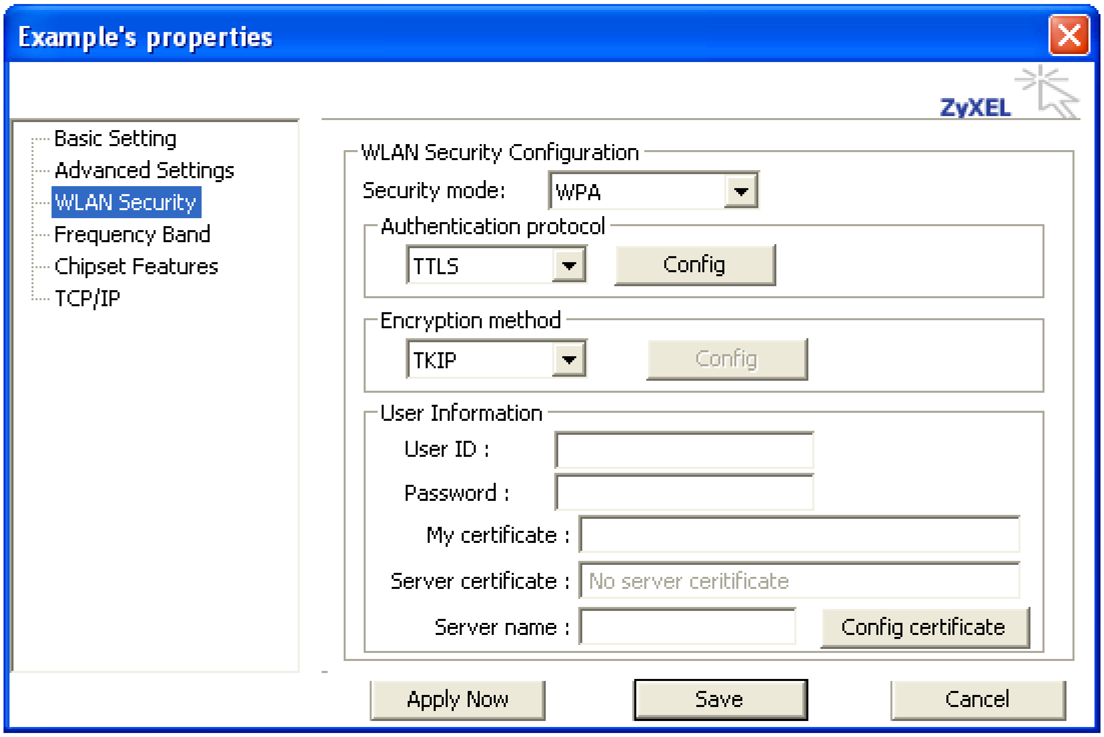
[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.

[Server name]: Name of server used for 802.1x authentication.

[Server name should match exactly]: Check this box to force server name to match exactly the name in the certificate.

4. Make selections and then click [OK] to finish and return to the previous screen.

4.5.5 Configuring 802.1x – EAP-TTLS



Example's properties

ZyXEL

- Basic Setting
- Advanced Settings
- WLAN Security
- Frequency Band
- Chipset Features
- TCP/IP

WLAN Security Configuration

Security mode: WPA

Authentication protocol: TTLS [Config]

Encryption method: TKIP [Config]

User Information

User ID :

Password :

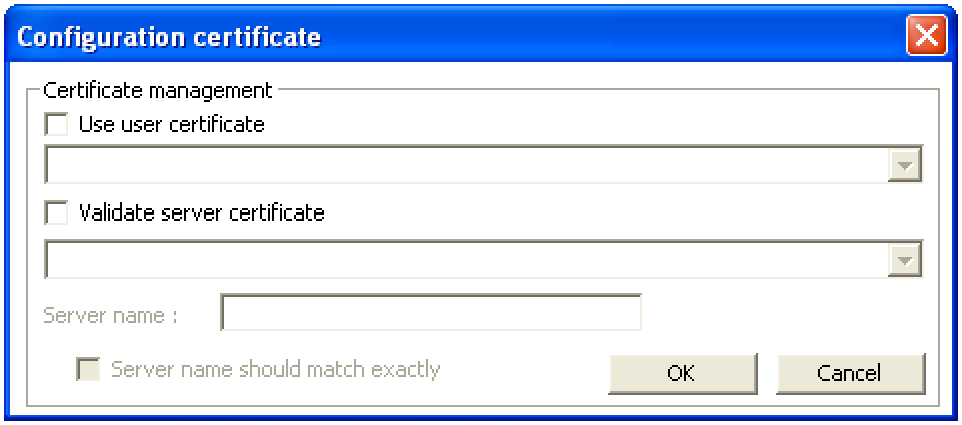
My certificate :

Server certificate : No server ceritificate

Server name : [Config certificate]

[Apply Now] [Save] [Cancel]

1. Enter in unique User ID and Password under [User Information].
2. Select inner TTLS protocol. You can choose between [PAP], [CHAP], [MS-CHAP], [MS-CHAP v2], or [MD5-Challenge].
3. Click [OK] to finish and return to the previous screen.
4. Click [Config certificate]. The following window appears:



□ Use user certificate

□ Validate server certificate

Server name :

□ Server name should match exactly

[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.

[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.

[Server name]: Name of server used for 802.1x authentication.

[Server name should match exactly]: Check this box to force server name to match exactly the name in the certificate.

5. Make selections and then click [OK] to finish and return to the previous screen. Server certificate must be configured for TTLS to work.

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
Cannot start the ZyXEL Wireless LAN Utility	Make sure the ZyXEL AG-200 is properly plugged in your USB port and the LED(s) is on. Refer to the *Quick Start Guide* for LED descriptions.
	Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the ZyXEL AG-200 under **Network Adapter**. (Steps may vary depending on the version of Windows).
	Install the ZyXEL AG-200 in another computer. If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.

5.2 Problem with the Link Status

Table 5-2 Troubleshooting Link Quality

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.

5.3 Problems Communicating With Other Computers

Table 5-3 Troubleshooting Communication Problems

PROBLEM	CORRECTIVE ACTION
The ZyXEL AG-200 computer cannot communicate with the other computer.	Make sure you 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 AG-200 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 AG-200 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.

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