# ZyXEL G-210H

*802.11b/g Wireless USB Adapter*

# User's Guide

Version 1.0
Edition 1
1/2007

# 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 patent 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

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Certifications

## Federal Communications Commission (FCC) Interference Statement

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.

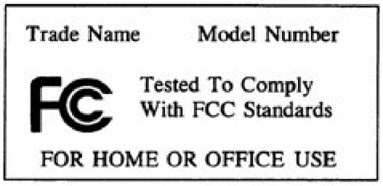
This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

## Caution

1. The 802.11g Wireless LAN Adapter has been tested to the FCC exposure requirements (Specific Absorption Rate).
2. The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
3. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.



注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用
者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現
有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍
受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

# 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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been 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 to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). 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 your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

# Customer Support

Please have the following information ready when you contact customer support.

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

| METHOD | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| LOCATION | SALES E-MAIL | FAX | FTP SITE | |
| CORPORATE HEADQUARTERS (WORLDWIDE) | support@zyxel.com.tw | +886-3-578-3942 | www.zyxel.com<br>www.europe.zyxel.com | ZyXEL Communications Corp.<br>6 Innovation Road II<br>Science Park<br>Hsinchu 300<br>Taiwan |
| | sales@zyxel.com.tw | +886-3-578-2439 | ftp.zyxel.com<br>ftp.europe.zyxel.com | |
| CZECH REPUBLIC | info@cz.zyxel.com | +420-241-091-350 | www.zyxel.cz | ZyXEL Communications<br>Czech s.r.o.<br>Modranská 621<br>143 01 Praha 4 - Modrany<br>Ceská Republika |
| | info@cz.zyxel.com | +420-241-091-359 | | |
| DENMARK | support@zyxel.dk | +45-39-55-07-00 | www.zyxel.dk | ZyXEL Communications A/S<br>Columbusvej<br>2860 Soeborg<br>Denmark |
| | sales@zyxel.dk | +45-39-55-07-07 | | |
| FINLAND | support@zyxel.fi | +358-9-4780-8411 | www.zyxel.fi | ZyXEL Communications Oy<br>Malminkaari 10<br>00700 Helsinki<br>Finland |
| | sales@zyxel.fi | +358-9-4780 8448 | | |
| FRANCE | info@zyxel.fr | +33-4-72-52-97-97 | www.zyxel.fr | ZyXEL France<br>1 rue des Vergers<br>Bat. 1 / C<br>69760 Limonest<br>France |
| | | +33-4-72-52-19-20 | | |
| GERMANY | support@zyxel.de | +49-2405-6909-0 | www.zyxel.de | ZyXEL Deutschland GmbH.<br>Adenauerstr. 20/A2 D-52146<br>Wuerselen<br>Germany |
| | sales@zyxel.de | +49-2405-6909-99 | | |
| HUNGARY | support@zyxel.hu | +36-1-3361649 | www.zyxel.hu | ZyXEL Hungary<br>48, Zoldlomb Str.<br>H-1025, Budapest<br>Hungary |
| | info@zyxel.hu | +36-1-3259100 | | |
| KAZAKHSTAN | http://zyxel.kz/support | +7-3272-590-698 | www.zyxel.kz | ZyXEL Kazakhstan<br>43, Dostyk ave.,Office 414<br>Dostyk Business Centre<br>050010, Almaty<br>Republic of Kazakhstan |
| | sales@zyxel.kz | +7-3272-590-689 | | |
| NORTH AMERICA | support@zyxel.com | 1-800-255-4101<br>+1-714-632-0882 | www.us.zyxel.com | ZyXEL Communications Inc.<br>1130 N. Miller St.<br>Anaheim<br>CA 92806-2001<br>U.S.A. |
| | sales@zyxel.com | +1-714-632-0858 | ftp.us.zyxel.com | |
| NORWAY | support@zyxel.no | +47-22-80-61-80 | www.zyxel.no | ZyXEL Communications A/S<br>Nils Hansens vei 13<br>0667 Oslo<br>Norway |
| | sales@zyxel.no | +47-22-80-61-81 | | |

| METHOD | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| LOCATION | SALES E-MAIL | FAX | FTP SITE | |
| **POLAND** | info@pl.zyxel.com | +48 (22) 333 8250 | www.pl.zyxel.com | ZyXEL Communications<br>ul. Okrzei 1A<br>03-715 Warszawa<br>Poland |
| | | +48 (22) 333 8251 | | |
| **RUSSIA** | http://zyxel.ru/support | +7-095-542-89-29 | www.zyxel.ru | ZyXEL Russia<br>Ostrovityanova 37a Str.<br>Moscow, 117279<br>Russia |
| | sales@zyxel.ru | +7-095-542-89-25 | | |
| **SPAIN** | support@zyxel.es | +34-902-195-420 | www.zyxel.es | ZyXEL Communications<br>Arte, 21 5ª planta<br>28033 Madrid<br>Spain |
| | sales@zyxel.es | +34-913-005-345 | | |
| **SWEDEN** | support@zyxel.se | +46-31-744-7700 | www.zyxel.se | ZyXEL Communications A/S<br>Sjöporten 4, 41764 Göteborg<br>Sweden |
| | sales@zyxel.se | +46-31-744-7701 | | |
| **UKRAINE** | support@ua.zyxel.com | +380-44-247-69-78 | www.ua.zyxel.com | ZyXEL Ukraine<br>13, Pimonenko Str.<br>Kiev, 04050<br>Ukraine |
| | sales@ua.zyxel.com | +380-44-494-49-32 | | |
| **UNITED KINGDOM** | support@zyxel.co.uk | +44-1344 303044<br>08707 555779 (UK only) | www.zyxel.co.uk | ZyXEL Communications UK<br>Ltd.,11 The Courtyard,<br>Eastern Road, Bracknell,<br>Berkshire, RG12 2XB,<br>United Kingdom (UK) |
| | sales@zyxel.co.uk | +44-1344 303034 | ftp.zyxel.co.uk | |

[a] “+” is the (prefix) number you enter to make an international telephone call.

# Table of Contents

# List of Figures

# List of Tables

# Preface

Congratulations on your purchase of the ZyXEL G-210H 802.11b/g Wireless USB Adapter Your G-210H allows you to connect and access wireless networks. Your G-210H also allows you to visually see the connection strength of the Access Point with its physical LED's.

Your G-210H is easy to install and configure.

## About This User's Guide

This manual is designed to guide you through the configuration of your G-210H for its various applications.

## Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.
- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains hardware installation/connection information.
- ZyXEL Glossary and Web Site

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

## User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

## Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choice.
- Mouse action sequences are denoted using a comma. For example, "In Windows, click **Start**, **Settings** and then **Control Panel**" means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".
- The ZyXEL G-210H 802.11b/g Wireless USB Adapter may be referred to as the G-210H  in this user's guide.

## Graphics Icons Key

| | | |
|---|---|---|
| Wireless Access Point<br> | Computer<br> | Notebook Computer<br> |
| Server<br> | Modem or Router<br> | Wireless Signal<br> |
| Internet Cloud<br> | | |

# CHAPTER 1
# Getting Started

This chapter introduces the G-210H and prepares you to use the ZyXEL utility.

## 1.1 About Your G-210H

The G-210H is an IEEE 802.11b/g compliant wireless LAN adapter that connects to the USB port on your computer and allows you to search for and connect to wireless networks. The ZyXEL utility is a tool that helps you configure your G-210H. When connectced to the USB port, you can search for the best direction to point the G-210H by simply looking at the number of LED's that illuminate.

For more information about using the G-210H when it is not connected to a computer, please see the Quick Start Guide.

## 1.2 Application Overview

This section describes some network applications for the G-210H.

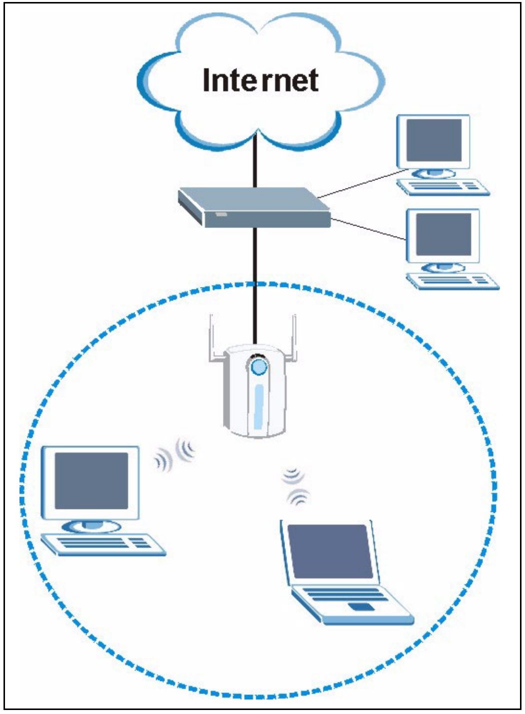
### 1.2.1 Station Mode

The G-210H is in wireless station mode by default. When the G-210H works as a wireless station (wireless client), you can either set the network type to **Infrastructure** and connect to an AP or use **Ad-Hoc** mode and connect to a peer computer (another wireless device in Ad-Hoc mode).

#### 1.2.1.1 Infrastructure

To connect to a network via an access point (AP), set the G-210H network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

**Figure 1** Application: Infrastructure

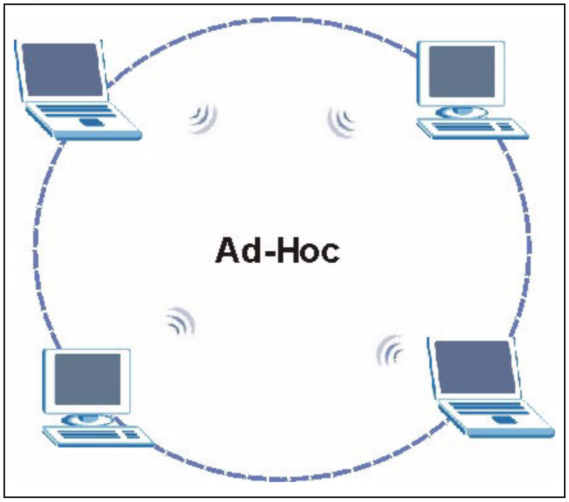


### 1.2.1.2 Ad-Hoc

To set up a small independent wireless workgroup without an AP, use **Ad-Hoc**.

**Ad-Hoc** does not require an AP or a wired network. Two or more wireless clients communicate directly with each other.

**Figure 2** Application: Ad-Hoc



# 1.3 G-210H Hardware and Utility Installation

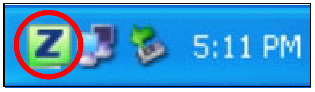
Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

## 1.3.1 ZyXEL Utility Icon

After you install and start the ZyXEL utility, an icon for the ZyXEL utility appears in the system tray.

**Note:** The ZyXEL utility system tray icon displays only when the G-210H is installed properly.

**Figure 3** ZyXEL Utility: System Tray Icon



The color of the ZyXEL utility system tray icon indicates the status of the G-210H. Refer to the following table for details.

**Table 1** ZyXEL Utility: System Tray Icon

| COLOR | DESCRIPTION |
|---|---|
| Red | The G-210H is operating in wireless station mode but is not connected to a wireless network. |
| Green | The G-210H is operating in wireless station mode and is connected to a wireless network. |
| Pale Blue | The G-210H is operating in access point mode. |

# 1.4 Configuration Methods

To configure your G-210H, use one of the following applications:

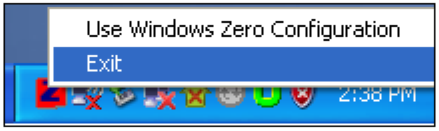
- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool)
- ZyXEL Utility (required when you want to use the G-210H as an access point)

## 1.4.1 Enabling WZC

**Note:** When you use the ZyXEL utility, it automatically disables WZC.

If you want to use WZC to configure the G-210H, you need to disable the ZyXEL utility by right-clicking the utility icon ( Z ) in the system tray and selecting **Exit**.

**Figure 4** Enable WZC



Refer to the appendices for information on how to use WZC to manage the G-210H.

To re-activate the ZyXEL utility, double-click the ( Z ) icon on your desktop or click **Start**, **(All) Programs**, **ZyXEL G-210H Wireless Adapter Utility**, **ZyXEL G-210H Wireless Adapter Software**.

## 1.4.2 Accessing the ZyXEL Utility

Double-click on the ZyXEL wireless LAN utility icon in the system tray to open the ZyXEL utility.

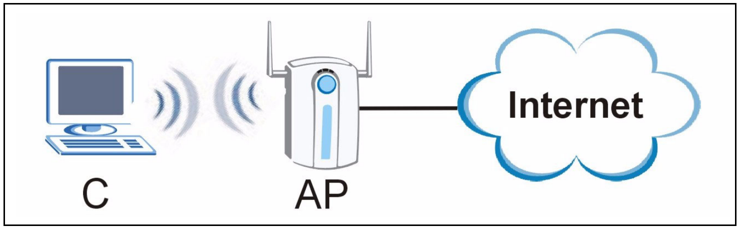
The ZyXEL utility screens are similar in all Microsoft Windows versions. Screens for Windows XP are shown in this User’s Guide.

**Note:** Click the ? icon (located in the top right corner) to display the online help window.

# CHAPTER 2
# Tutorial

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagrams. The wireless client is labeled **C** and the access point is labeled **AP**.

**Figure 5** Infrastructure Network



There are three ways to connect the wireless client (the G-210H in station mode) to a network.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network (see Section 2.1 on page 23).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see Section 2.2 on page 25).

This chapter also includes a simple example of how to configure the G-210H as an AP using the ZyXEL utility. See Section 2.3 on page 31 for more information.

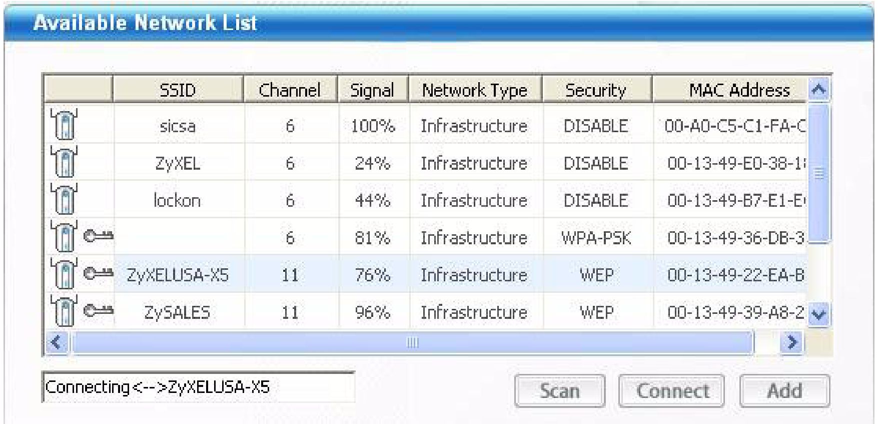
## 2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey".

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

**Figure 6** ZyXEL Utility: Site Survey



Available Network List

| SSID | Channel | Signal | Network Type | Security | MAC Address |
|---|---|---|---|---|---|
| sicsa | 6 | 100% | Infrastructure | DISABLE | 00-A0-C5-C1-FA-C |
| ZyXEL | 6 | 24% | Infrastructure | DISABLE | 00-13-49-E0-38-1 |
| lockon | 6 | 44% | Infrastructure | DISABLE | 00-13-49-B7-E1-E |
|  | 6 | 81% | Infrastructure | WPA-PSK | 00-13-49-36-DB-3 |
| ZyXELUSA-X5 | 11 | 76% | Infrastructure | WEP | 00-13-49-22-EA-B |
| ZySALES | 11 | 96% | Infrastructure | WEP | 00-13-49-39-A8-2 |

Connecting<-->ZyXELUSA-X5

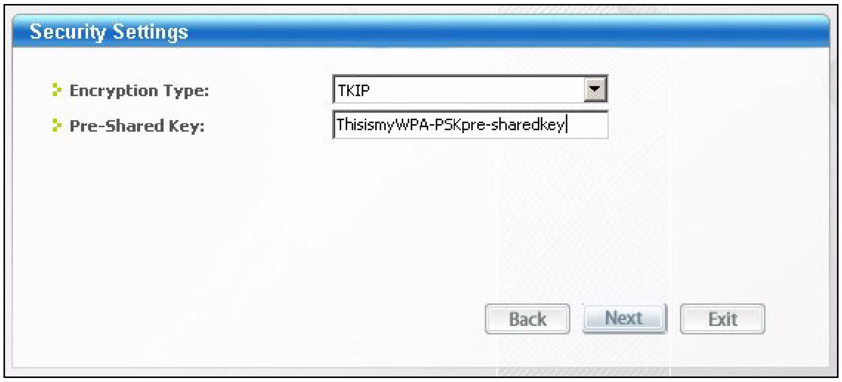
2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See Table 4 on page 35 for detailed field descriptions.

3 To connect to an AP or peer computer, either click an entry in the list and then click **Connect** or double-click an entry (**ZyXELUSA-X5** in this example).

4 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

**Figure 7** ZyXEL Utility: Security Settings



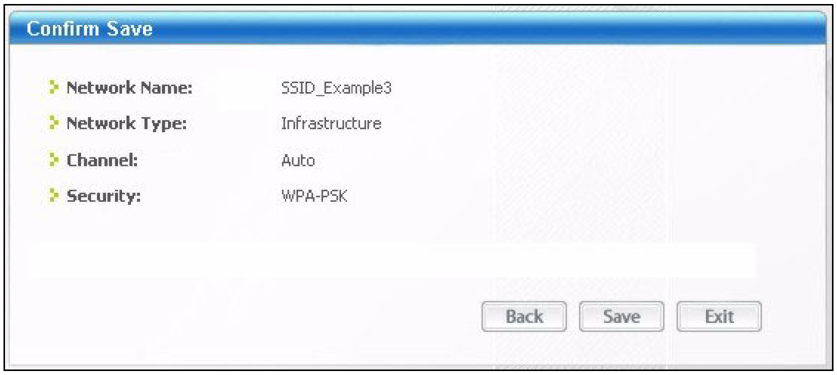
Security Settings

Encryption Type: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

5 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

**Figure 8** ZyXEL Utility: Confirm Save

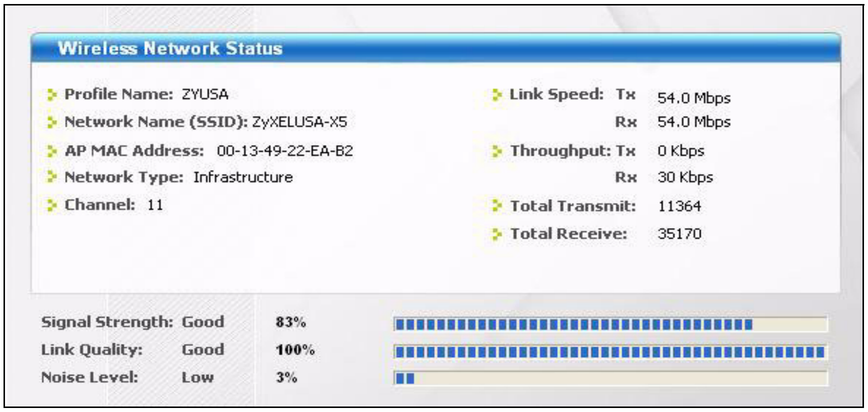


Confirm Save

- Network Name: SSID_Example3
- Network Type: Infrastructure
- Channel: Auto
- Security: WPA-PSK

6 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank. See Table 3 on page 34 for detailed field descriptions.

**Figure 9** ZyXEL Utility: Link Info



Wireless Network Status

- Profile Name: ZYUSA
- Network Name (SSID): ZyXELUSA-X5
- AP MAC Address: 00-13-49-22-EA-B2
- Network Type: Infrastructure
- Channel: 11
- Link Speed: Tx 54.0 Mbps
  Rx 54.0 Mbps
- Throughput: Tx 0 Kbps
  Rx 30 Kbps
- Total Transmit: 11364
- Total Receive: 35170

Signal Strength: Good 83%
Link Quality: Good 100%
Noise Level: Low 3%

7 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured. If you cannot access the web site, check the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

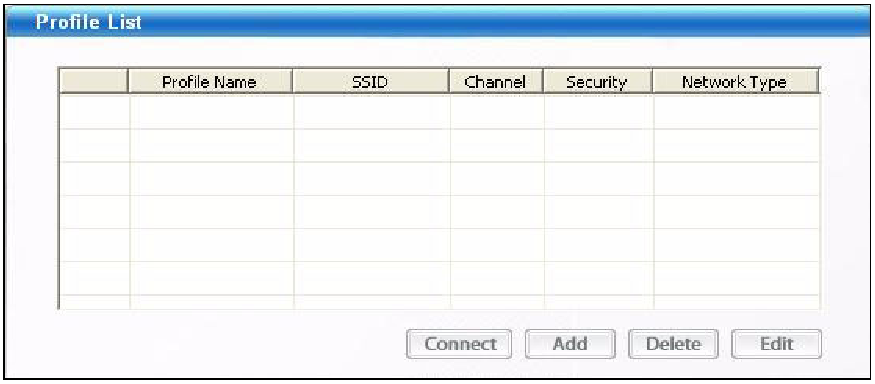
## 2.2 Creating and Using a Profile

A profile lets you automatically connect to the same wireless network every time you use the ZyXEL utility. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an access point configured for WPA-PSK security. In this example, the AP's SSID is "SSID_Example3" and its pre-shared key is "ThisismyWPA-PSKpre-sharedkey". You have chosen the profile name "PN_Example3".

**1** Open the ZyXEL utility and click the **Profile** tab to open the screen as shown. Click **Add** to configure a new profile.

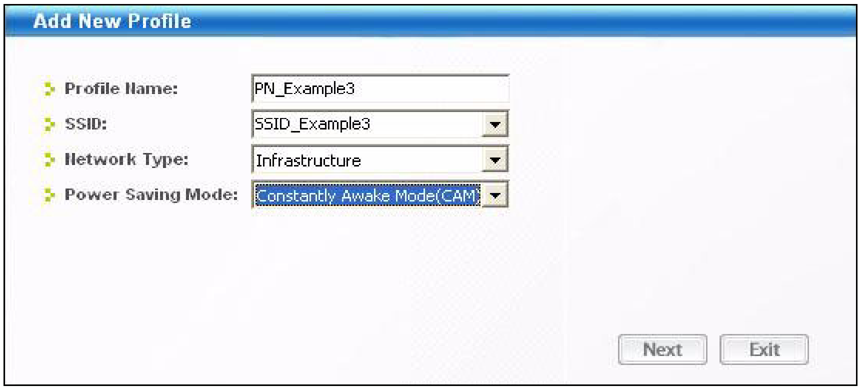
**Figure 10** ZyXEL Utility: Profile



|  | Profile Name | SSID | Channel | Security | Network Type |
|---|---|---|---|---|---|

**2** The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, which are displayed in the **Scan Info** box. You can also configure your profile for a wireless network that is not in the list.

**Figure 11** ZyXEL Utility: Add New Profile

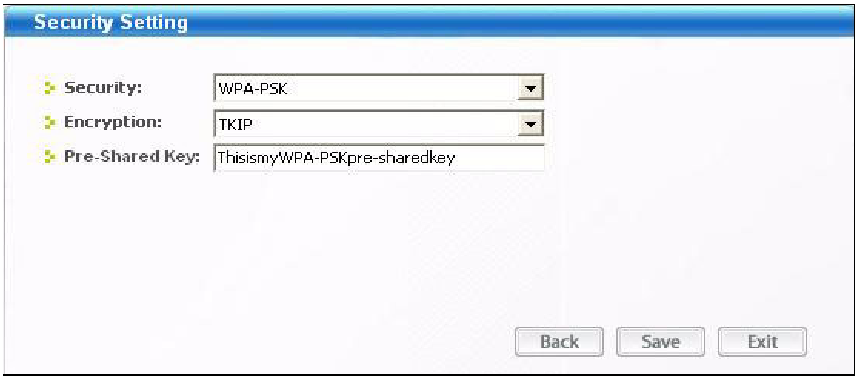


Profile Name: PN_Example3
SSID: SSID_Example3
Network Type: Infrastructure
Power Saving Mode: Constantly Awake Mode(CAM)

**3** Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **drop down menu**. Finally, choose whether or not you wish to have the G-210H be on the maximum power output level *default* or Power Save mode then click **Select**.

**4** Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK and TKIP). Then type in the appropriate Pre-Shared Key which in this case is ThisismyWPA-PSKpre-sharedkey.

**Figure 12** ZyXEL Utility: Profile Security



Security Setting

Security: WPA-PSK

Encryption: TKIP

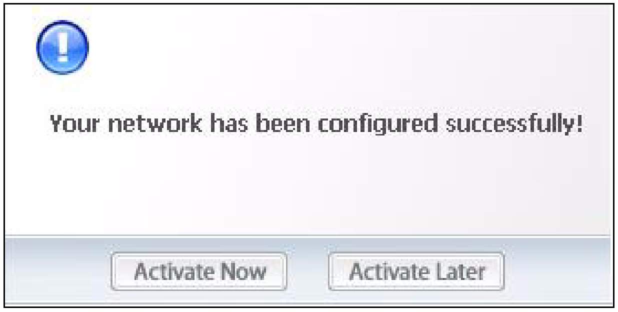
Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

5 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button to go back to the **Profile List** screen.

If you clicked **Activate Later** you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

**Note:** Only one profile can be activated and used at any given time.

**Figure 13** ZyXEL Utility: Profile Activate



Your network has been configured successfully!

6 When you activate the new profile, the ZyXEL utility goes to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

7 Make sure the selected AP in the active profile is on and connected to the Internet. Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

8 If you cannot access the Internet, go back to the **Profile** screen. Select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

# CHAPTER 3

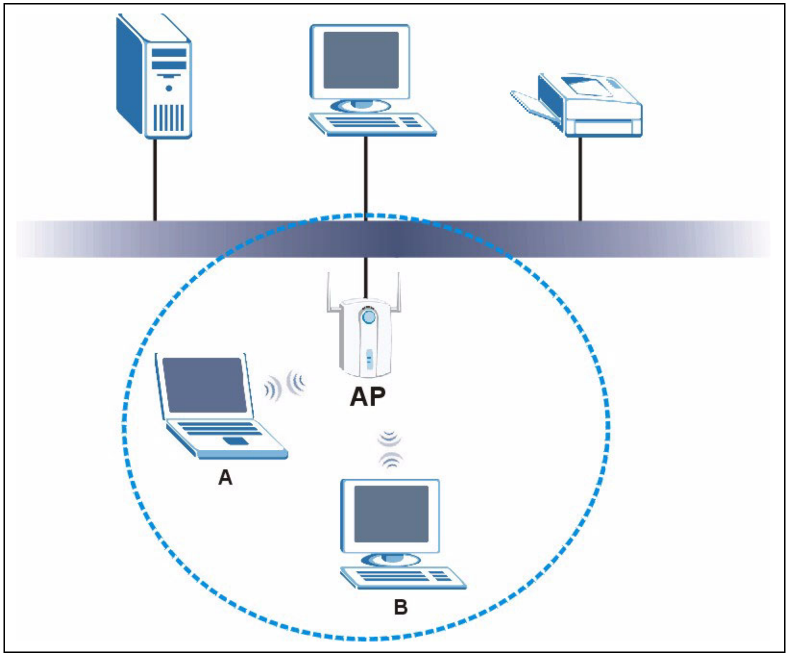
# Wireless LAN Network

This chapter provides background information on wireless LAN networks.

## 3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 2 on page 20 for an Ad Hoc network example.

**Figure 14** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use a different channel.

Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP or peer computer.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## 3.2 Wireless LAN Security

Wireless LAN security is vital to your network to protect wireless communications.

Configure the wireless LAN security using the **Configuration** or the **Profile Security Setting** screen. If you do not enable any wireless security on your G-210H, the G-210H's wireless communications are accessible to any wireless networking device that is in the coverage area.

**Note:** You can only use WEP encryption if you set the G-210H to Ad-hoc.

See the appendices for more detailed information about wireless security.

### 3.2.1 Hide SSID

This type of security is fairly weak, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 3.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to access the wireless network.

### 3.2.3 User Authentication and Encryption

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

### 3.2.3.1 WEP

#### 3.2.3.1.1 *Data Encryption*

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the G-210H 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 G-210H.

- 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 G-210H allows you to configure up to four 64-bit, 128-bit WEP keys and only one key is used as the default key at any one time.

#### *3.2.3.1.2 Authentication Type*

The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Two authentication types are defined: **Open** and **Shared**.

- Open mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.
- Shared mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

### 3.2.3.2 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.

#### 3.2.3.2.1 *EAP Authentication*

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x 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 IEEE 802.1x. The G-210H supports EAP-TLS, EAP-TTLS and EAP-PEAP. Refer to Appendix C on page 65 for descriptions.

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.

### 3.2.3.3 WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

# CHAPTER 4 Wireless Station Mode Configuration

This chapter shows you how to configure your G-210H in wireless station mode. See Chapter 5 on page 47 for how to configure the G-210H in access point mode.

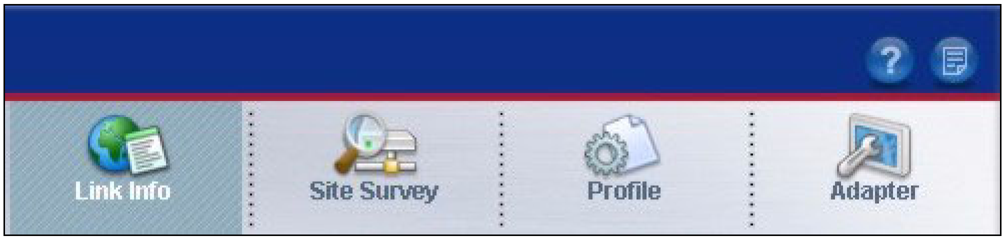
## 4.1 Wireless Station Mode Overview

The G-210H acts as a client bridge from the computer over to the Access Point in whats known as station mode.

### 4.1.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens when the G-210H is in station mode.

**Figure 15** ZyXEL Utility Menu Summary: Station Mode



The following table describes the menus.

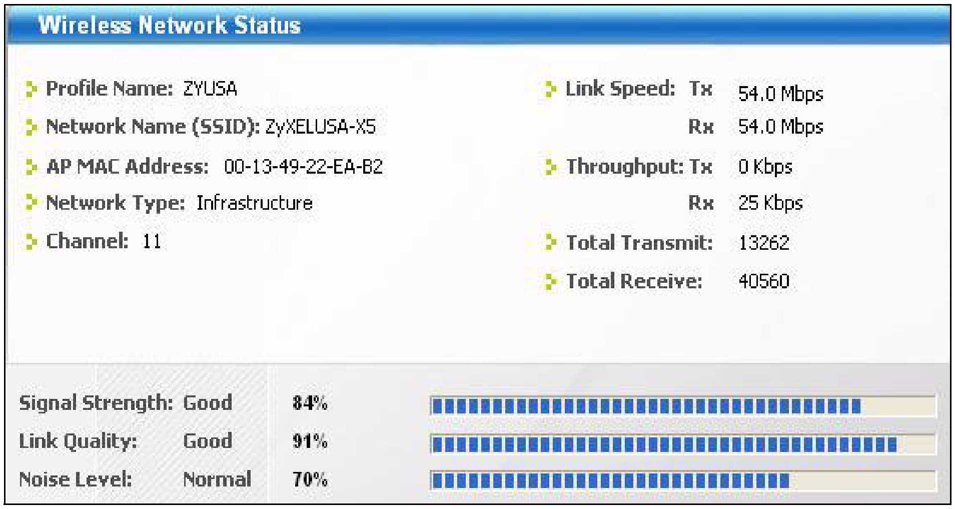
**Table 2** ZyXEL Utility Menu Summary: Station Mode

| TAB | DESCRIPTION |
|---|---|
| Station Mode | |
| Link Info | Use this screen to see your current connection status, configuration and data rate statistics. |
| Site Survey | Use this screen to<br>• scan for a wireless network<br>• configure wireless security (if activated on the selected network).<br>• connect to a wireless network. |
| Profile | Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings. |
| Adapter | Use this screen to configure a transfer rate and enable power saving. |

## 4.2 The Link Info Screen

When the ZyXEL utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your G-210H.

**Figure 16** Station Mode: Link Info



Wireless Network Status

Profile Name: ZYUSA

Network Name (SSID): ZyXELUSA-X5

AP MAC Address: 00-13-49-22-EA-B2

Network Type: Infrastructure

Channel: 11

Link Speed: Tx 54.0 Mbps

Rx 54.0 Mbps

Throughput: Tx 0 Kbps

Rx 25 Kbps

Total Transmit: 13262

Total Receive: 40560

Signal Strength: Good 84%

Link Quality: Good 91%

Noise Level: Normal 70%

The following table describes the labels in this screen.

**Table 3** Station Mode: Link Info

| LABEL | DESCRIPTION |
|---|---|
| Wireless Network Status | |
| Profile Name | This is the name of the profile you are currently using. |
| Network Name (SSID) | The SSID identifies the wireless network to which a wireless station is associated. This field displays the name of the wireless device to which the G-210H is associated. |
| AP MAC Address | This field displays the MAC address of the AP or peer computer to which the G-210H is associated. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad-Hoc**) of the wireless network. |
| Channel | This field displays the radio channel the G-210H is currently using. |
| Link Speed | This field displays the current maximum connection speed in Megabits per second (Mbps). |
| Throughput | This field displays the current data transmission rates in kilobits per second (Kbps). |
| Total Transmit | This field displays the total number of data frames transmitted. |
| Total Receive | This field displays the total number of data frames received. |
| Signal Strength | The status bar shows the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your G-210H and the AP or peer computer. |

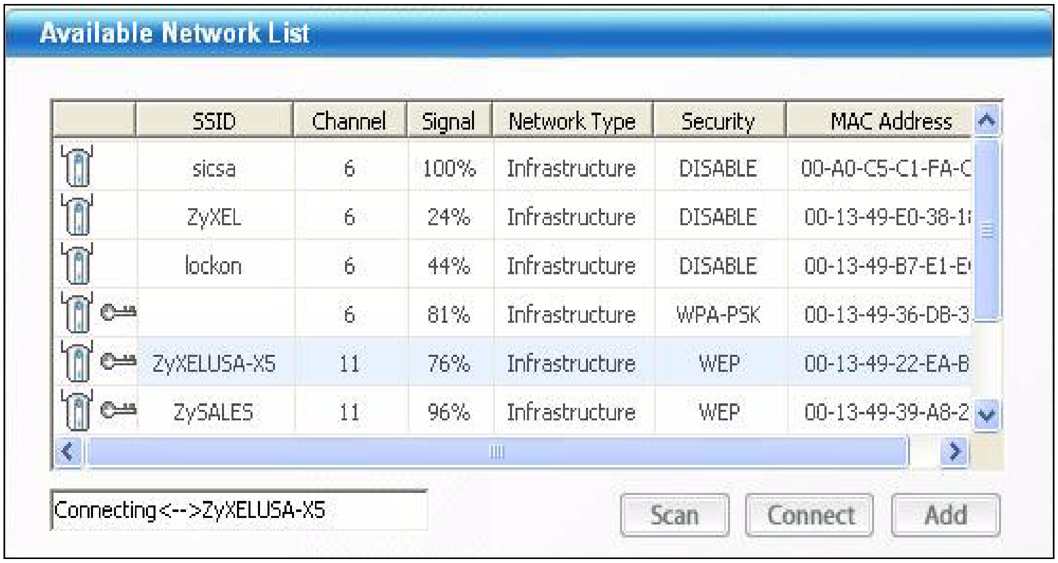
**Table 3** Station Mode: Link Info (continued)

| LABEL | DESCRIPTION |
|---|---|
| Link Quality | The status bar shows the quality of wireless connection. This refers to the percentage of packets transmitted successfully. If there are too many wireless stations in a wireless network, collisions may occur which could result in a loss of messages even though you have high signal strength. |
| Noise Level | This field displays the noise level that the G-210H is detecting while linked with the connected AP. |

## 4.3 The Site Survey Screen

Use the **Site Survey** screen to scan for and connect to a wireless network automatically.

**Figure 17** Station Mode: Site Survey



Available Network List

| | SSID | Channel | Signal | Network Type | Security | MAC Address |
|---|---|---|---|---|---|---|
| | sicsa | 6 | 100% | Infrastructure | DISABLE | 00-A0-C5-C1-FA-C |
| | ZyXEL | 6 | 24% | Infrastructure | DISABLE | 00-13-49-E0-38-1 |
| | lockon | 6 | 44% | Infrastructure | DISABLE | 00-13-49-B7-E1-E |
| 🔑 | | 6 | 81% | Infrastructure | WPA-PSK | 00-13-49-36-DB-3 |
| 🔑 | ZyXELUSA-X5 | 11 | 76% | Infrastructure | WEP | 00-13-49-22-EA-B |
| 🔑 | ZySALES | 11 | 96% | Infrastructure | WEP | 00-13-49-39-A8-2 |

Connecting<-->ZyXELUSA-X5

The following table describes the labels in this screen.

**Table 4** Station Mode: Site Survey

| LABEL | DESCRIPTION |
|---|---|
| Available Network List | Click a column heading to sort the entries. |
| 🔑 ,<br>,<br>🔑 or<br>. | 🔑 denotes that the wireless device is in infrastructure mode and the wireless security is activated. |
| | denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. |
| | 🔑 denotes that the wireless device is in Ad-Hoc mode and the wireless security is activated. |
| | denotes that the wireless device is in Ad-Hoc mode but the wireless security is deactivated. |
| SSID | This field displays the SSID (Service Set IDentifier) of each wireless device. |

**Table 4** Station Mode: Site Survey (continued)

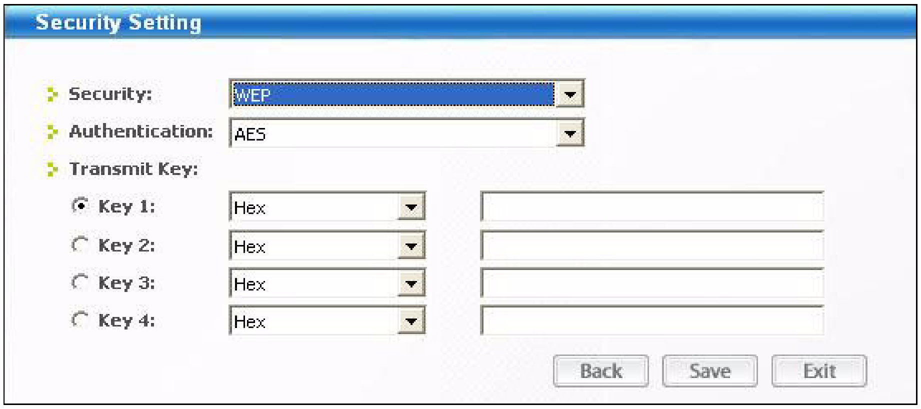
| LABEL | DESCRIPTION |
|---|---|
| Channel | This field displays the channel number used by each wireless device. |
| Signal | This field displays the signal strength of each wireless device. |
| Scan | Click **Scan** to search for available wireless devices within transmission range. |
| Connect | Click **Connect** to associate to the selected wireless device. |
| Add | Click **Add** to create a new profile. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless device. |
| Channel | This field displays the channel number used by each wireless device. |
| Security | This field shows whether data encryption is activated (**WEP** (WEP or 802.1x), **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**) or inactive (**DISABLE**). |
| MAC address | This field displays the MAC address of the wireless device. |

## 4.3.1 Security Settings

When you configure the G-210H to connect to a network with wireless security activated and the security settings are disabled on the G-210H, the screen varies according to the encryption method used by the selected network.

### 4.3.1.1 WEP Encryption

**Figure 18** Station Mode: Security Setting: WEP



Security Setting

Security: WEP

Authentication: AES

Transmit Key:

● Key 1: Hex

○ Key 2: Hex

○ Key 3: Hex

○ Key 4: Hex

The following table describes the labels in this screen.

**Table 5** Station Mode: Security Setting: WEP

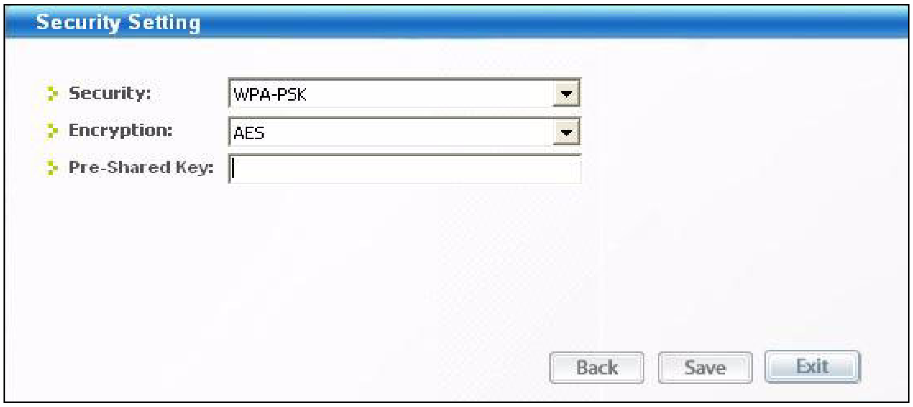
| LABEL | DESCRIPTION |
|---|---|
| Security Settings | |
| Authentication | Select an authentication method. Choices are **AES** or **TKIP**, please choose according to the type selected on the Access Point. |
| Transmit Key | Select a default WEP key to use for data encryption. The key displays in the field below. |

**Table 5** Station Mode: Security Setting: WEP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key x (where x is a number between 1 and 4) | Enter the WEP key in the field provided.<br>If you select **64 Bits** in the **WEP** field.<br>Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type.<br>or<br>Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type.<br>If you select **128 Bits** in the **WEP** field,<br>Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type<br>or<br>Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type.<br>**Note:** The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.<br>ASCII WEP keys are case sensitive. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Save | Click **Save** to confirm your selections and advance to the next screen. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

### 4.3.1.2 WPA-PSK/WPA2-PSK

**Figure 19** Station Mode: Security Setting: WPA-PSK/WPA2-PSK



Security Setting

Security: WPA-PSK

Encryption: AES

Pre-Shared Key:

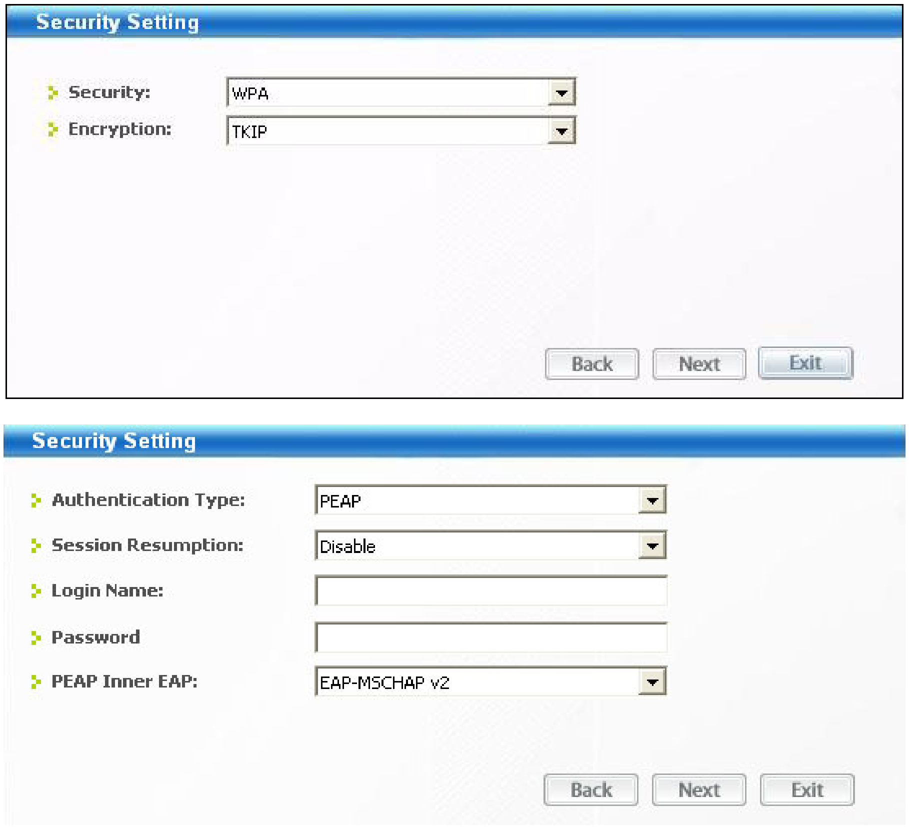
The following table describes the labels in this screen.

**Table 6** Station Mode: Security Setting: WPA-PSK/WPA2-PSK

| LABEL | DESCRIPTION |
|---|---|
| Encryption | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type (**TKIP** or **AES**) for data encryption.<br>Refer to Section 3.2.3 on page 30 for more information. |
| Pre-Shared Key | Type a pre-shared key (same as the AP or peer device) of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Save | Click **Next** to confirm your selections and advance to the next screen. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

### 4.3.1.3 WPA/WPA2

**Figure 20** Station Mode: Security Settings: WPA/WPA2



Security Setting

Security: WPA

Encryption: TKIP

Security Setting

Authentication Type: PEAP

Session Resumption: Disable

Login Name:

Password

PEAP Inner EAP: EAP-MSCHAP v2

The following table describes the labels in these screens.

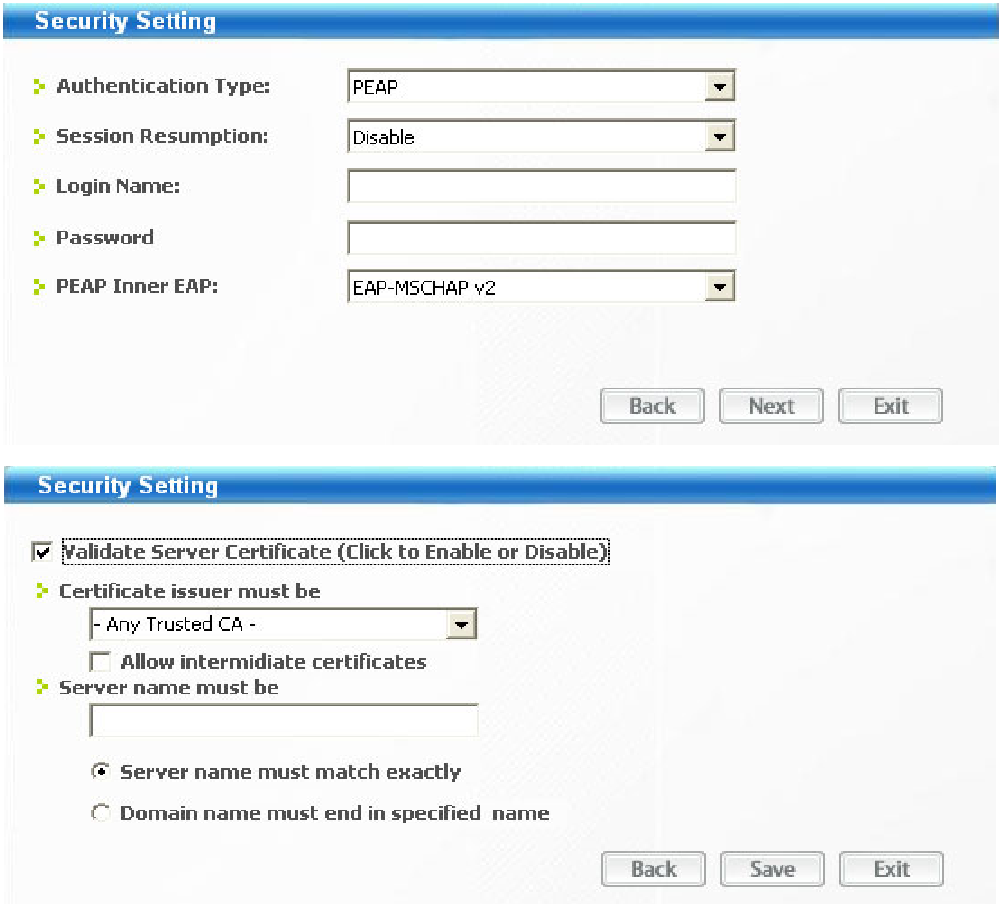
**Table 7** Station Mode: Security Setting: WPA/WPA2

| LABEL | DESCRIPTION |
|---|---|
| Encryption | The encryption mechanisms used for WPA/WPA2 and WPA-PSK/WPA2-PSK are the same. The only difference between the two is that WPA-PSK/WPA2-PSK uses a simple common password, instead of user-specific credentials.<br>Select the encryption type (**TKIP** or **AES**) for data encryption.<br>Refer to Section 3.2.3 on page 30 for more information. |
| Authentication Type | The type of authentication you use depends on the RADIUS server or AP.<br>Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**. |
| Session Resumption | Select either **Enable** or **Disable** depending on whether or not you wish for the utility to reconnect your session to the server when your session is over. |
| Login Name | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| Password | This field is not available when you select **TLS** in the **Authentication Type** field.<br>Enter the password associated with the user name above. |
| Certificate | This field is only available when you select **TLS** in the **Authentication Type** field.<br>Click **Browse** to select a certificate.<br>**Note:** 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. |
| Server CA | Select a certificate authority (CA) from the drop-down box to have the G-210H trust certificates from that CA only. Select **Trust Any** to accept certificates from any CA. |
| PEAP Inner EAP | This field is only available when you select **PEAP** in the **Authentication Type** field.<br>The PEAP method used by the RADIUS server or AP for client authentication are **EAP_TLS** and **EAP MS CHAP v2**. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Save | Click **Save** to confirm your selections and advance to the next screen. Refer to Section 4.3.2 on page 47. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

### 4.3.1.4 IEEE 802.1x

Configure IEEE 802.1x security with various authentication methods in this screen.

**Figure 21** Station Mode: Security Setting: 802.1x



Security Setting

Authentication Type: PEAP

Session Resumption: Disable

Login Name:

Password

PEAP Inner EAP: EAP-MSCHAP v2

Security Setting

☑ Validate Server Certificate (Click to Enable or Disable)

Certificate issuer must be

- Any Trusted CA -

□ Allow intermidiate certificates

Server name must be

● Server name must match exactly

○ Domain name must end in specified name

The following table describes the labels in these screens.

**Table 8** Station Mode: Security Settings: IEEE 802.1x

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | The type of authentication you use depends on the RADIUS server or AP.<br>Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**. |
| Session Resumption | Select either **Enable** or **Disable** depending on whether or not you wish for the utility to reconnect your session to the server when your session is over. |
| Login Name | Enter a user name.<br>This is the user name that you or an administrator set up on a RADIUS server. |
| Password | This field is not available when you select **TLS** in the **Authentication Type** field.<br>Enter the password associated with the user name above. |
| Certificate | This field is only available when you select **TLS** in the **Authentication Type** field.<br>Click **Browse** to select a certificate.<br>**Note:** 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. |
| Server CA | Select a certificate authority (CA) from the drop-down box to have the G-210H trust certificates from that CA only. Select **Trust Any** to accept certificates from any CA. |

**Table 8** Station Mode: Security Settings: IEEE 802.1x

| LABEL | DESCRIPTION |
|---|---|
| PEAP Inner EAP | This field is only available when you select **PEAP** in the **Authentication Type** field.<br>The PEAP method used by the RADIUS server or AP for client authentication is **MS CHAP v2**. |
| Validate Server Certificate | Check this box to open up the rest of the Certificate selection menu. |
| Certificate Issuer Must Be | From the drop down menu, please select the appropriate certificate issuer or if you are uncertain, then select **Any Trusted CA** |
| Server Name Must Be | You must specify the name of the server that the certificate is connecting to. Please type in the server name and then select the appropriate bullet below when finished typing the name in. |
| Back | Click **Back** to go to the **Site Survey** screen to select and connect to another network. |
| Save | Click **Save** to confirm your selections and advance to the next screen. Refer to Section 4.3.2 on page 47. |
| Exit | Click **Exit** to return to the **Site Survey** screen without saving. |

## 4.4 The Profile Screen

A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the G-210H, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the G-210H cannot connect to a network.

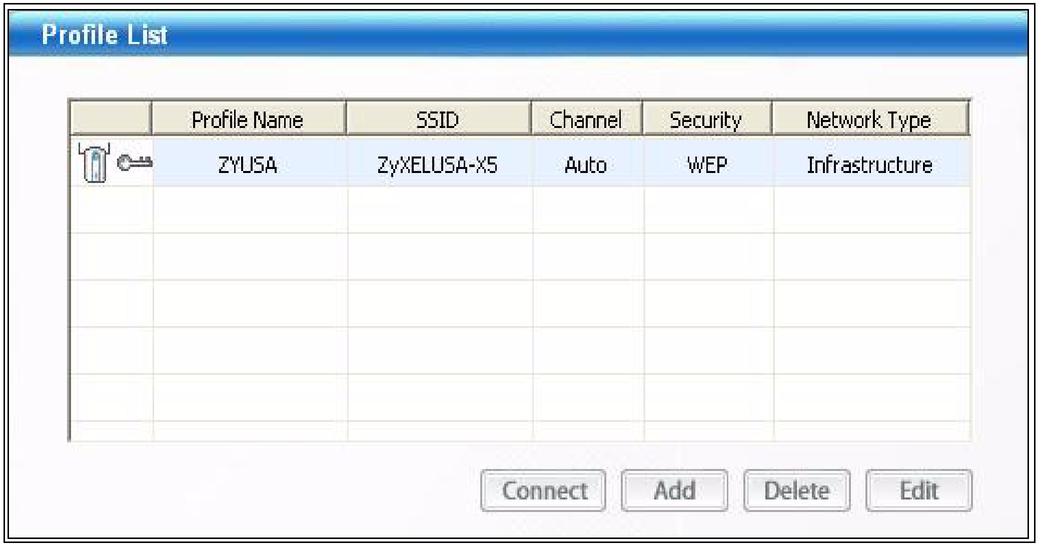
If you do not configure and activate a profile, each time you start the G-210H, the G-210H uses the default profile to connect to any available network that has no security enabled.

The default profile is a profile that allows you to connect to any SSID that has no security enabled.

Click the **Profile** tab in the ZyXEL utility program to display the **Profile** screen as shown next.

The profile function allows you to save the wireless network settings in this screen, or use one of the pre-configured network profiles.

**Figure 22** Station Mode: Profile



Profile List

| | Profile Name | SSID | Channel | Security | Network Type |
|---|---|---|---|---|---|
| 📶🔑 | ZYUSA | ZyXELUSA-X5 | Auto | WEP | Infrastructure |

The following table describes the labels in this screen.

**Table 9** Station Mode: Profile

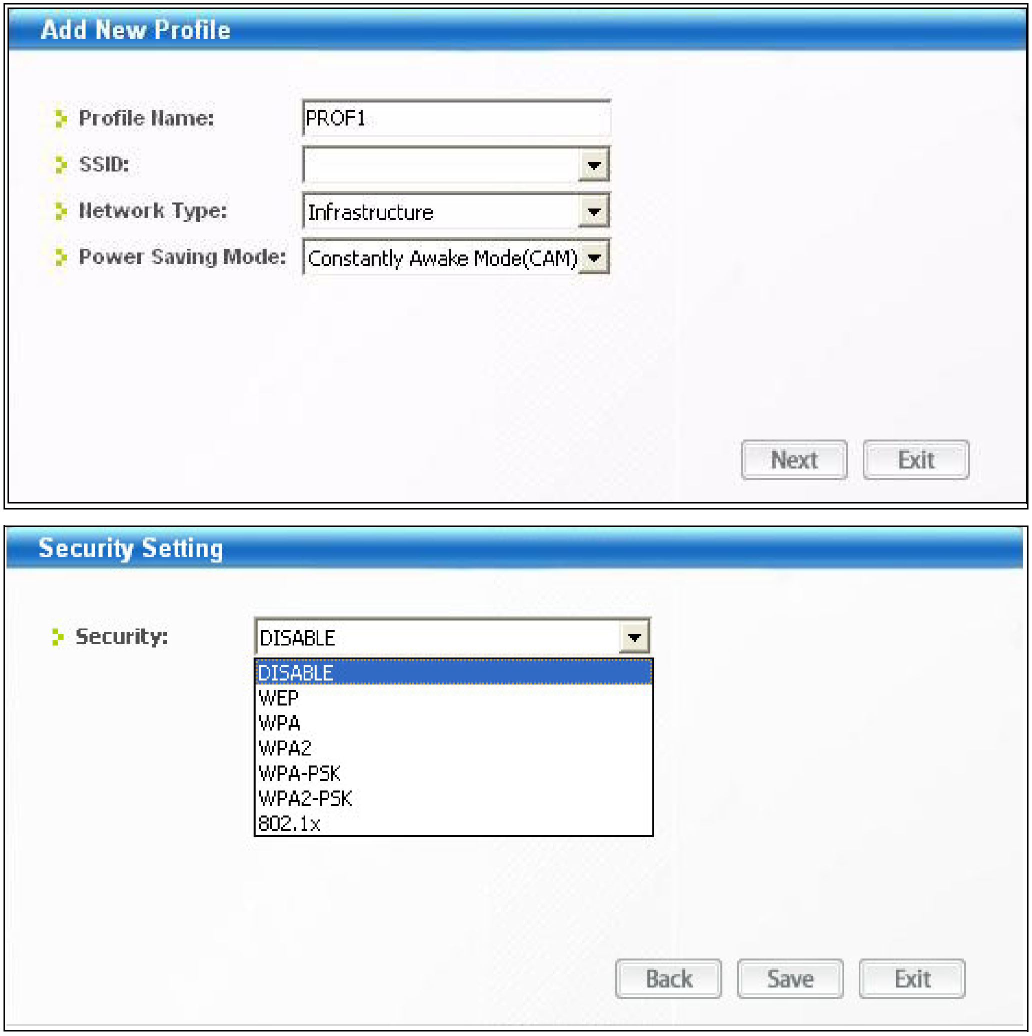
| LABEL | DESCRIPTION |
|---|---|
| Profile List | Click a column heading to sort the entries. |
| 📶🔑 ,<br>📶 ,<br>💻🔑 or<br>💻 . | 📶🔑 denotes that the wireless device is in infrastructure mode and the wireless security is activated. |
| | 📶 denotes that the wireless device is in infrastructure mode but the wireless security is deactivated. |
| | 💻🔑 denotes that the wireless device is in Ad-hoc mode and the wireless security is activated. |
| | 💻 denotes that the wireless device is in Ad-hoc mode but the wireless security is deactivated. |
| Profile Name | This is the name of the pre-configured profile. |
| SSID | This is the SSID of the wireless network to which the selected profile associate. |
| Connect | To use and activate a previously saved network profile, select a pre-configured profile name in the table and click **Connect**. |
| Add | To add a new profile into the table, click **Add**. |
| Delete | To delete an existing wireless network configuration, select a profile in the table and click **Delete**. |
| Edit | To edit an existing wireless network configuration, select a profile in the table and click **Edit**. |
| Network Type | This field displays the network type (**Infrastructure** or **Ad-hoc**) of the profile. |
| Channel | This field displays the channel number used by the profile. |
| Security | This field shows whether data encryption is activated (**WEP**, **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**, **802.1x**) or inactive (**DISABLE**). |

## 4.4.1 Adding a New Profile

Follow the steps below to add a new profile.

1 Click **Add** in the **Profile** screen. An **Add New Profile** screen displays as shown next. Click **Next** to continue.

**Figure 23** Station Mode: Profile: Add a New Profile



Add New Profile

Profile Name: PROF1

SSID:

Network Type: Infrastructure

Power Saving Mode: Constantly Awake Mode(CAM)

Security Setting

Security: DISABLE

The following table describes the labels in this screen.

**Table 10** Station Mode: Profile: Add a New Profile

| LABEL | DESCRIPTION |
|---|---|
| Add New Profile | |
| Profile Name | Enter a descriptive name in this field. |
| SSID | Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID of the wireless device to which you want to associate in this field manually. Otherwise, enter **Any** to have the G-210H associate to any AP or roam between any infrastructure wireless networks. |

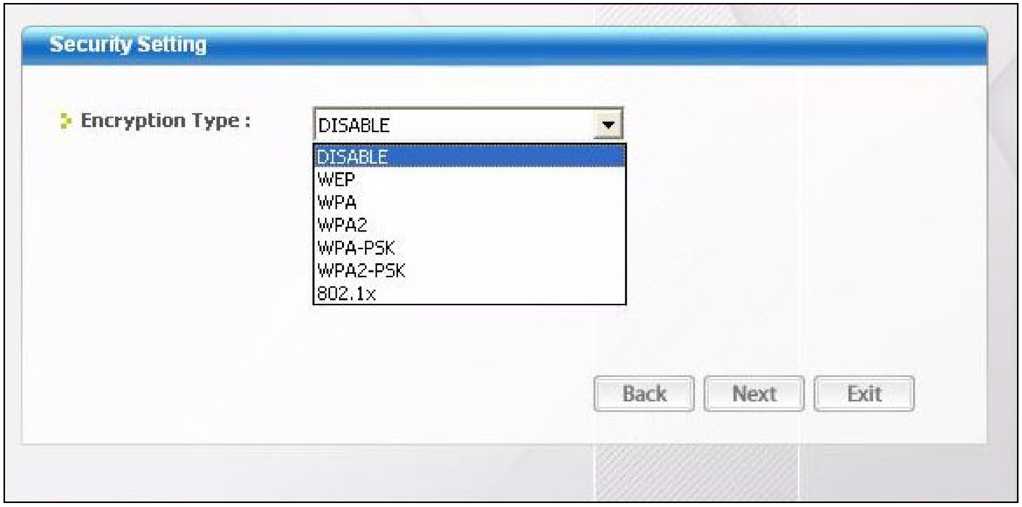
**Table 10** Station Mode: Profile: Add a New Profile (continued)

| LABEL | DESCRIPTION |
|---|---|
| Network Type | Select **Infrastructure** to associate to an AP. Select **Ad-hoc** to associate to a peer computer. |
| Power Saving Mode | Choose from **Constantly Awake Mode (CAM)** or **Power Saving Mode** depending on the type of usage you would like the computer to be in while connecting using this profile. |
| Security | Please choose from the appropriate security for the Access Point. Follow the subsequent screens accordingly. |
| Next | Click **Next** to go to the next screen. |
| Save | Click **Save** to confirm your selections and advance to the next screen. Refer to Section 4.3.2 on page 47. |
| Exit | Click **Exit** to go back to the previous screen without saving. |

**2** If you select the **Infrastructure** network type in the previous screen, skip to step 3. If you select the **Ad-Hoc** network type in the previous screen, a screen displays as follows. Select a wireless frequency and channel number and click **Next** to continue.

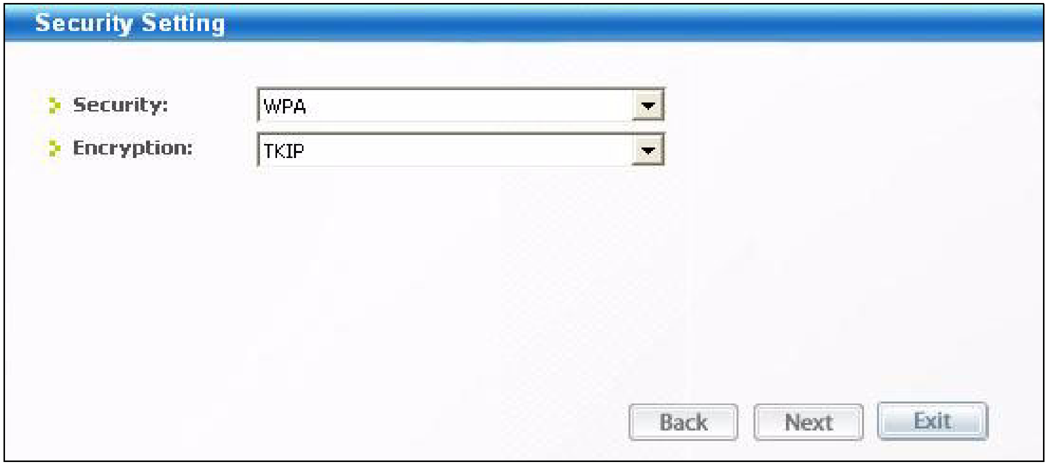
**Note:** To associate to an Ad-hoc network, you must use the same channel and wireless frequency as the peer computer.

**Figure 24** Station Mode: Profile: Wireless Settings



**3** The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless computers as they are on the G-210H. Refer to Section 4.3.1 on page 36 for detailed information on wireless security configuration.

**Figure 25** Station Mode: Profile: Security Settings



Security Setting

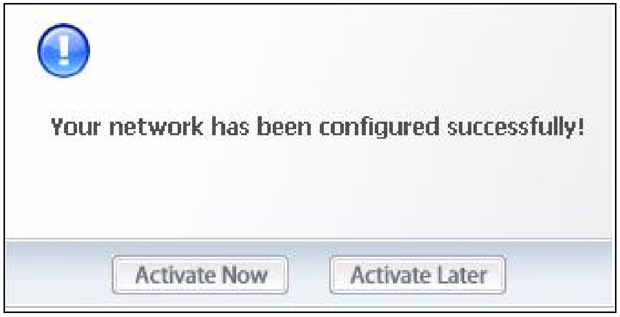
Security: WPA

Encryption: TKIP

4 To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button. You can activate only one profile at a time.

**Note:** Once you activate a profile, the ZyXEL utility will use that profile the next time it is started.

**Figure 26** Station Mode: Profile: Activate the Profile

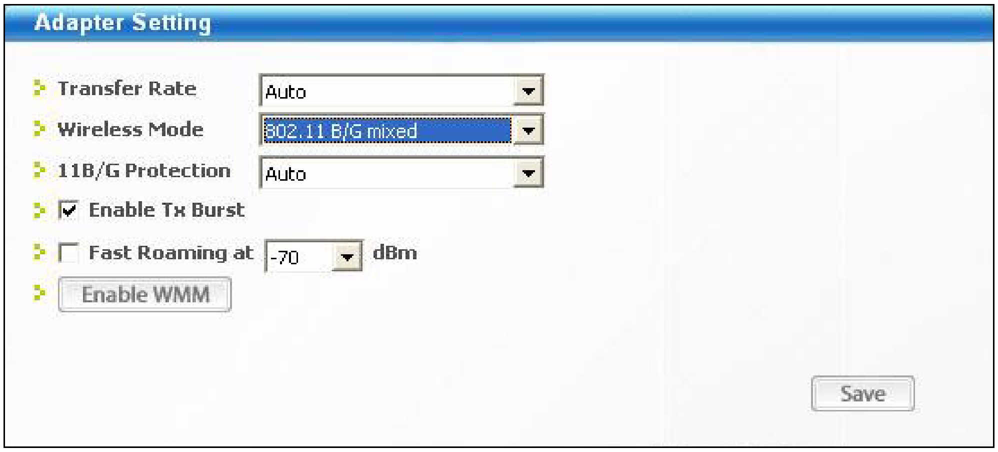


Your network has been configured successfully!

## 4.5 The Adapter Screen

To set the other advanced features on the G-210H, click the **Adapter** tab.

**Figure 27** Station Mode: Adapter



Adapter Setting

Transfer Rate: Auto

Wireless Mode: 802.11 B/G mixed

11B/G Protection: Auto

☑ Enable Tx Burst

□ Fast Roaming at -70 dBm

The following table describes the labels in this screen.

**Table 11** Station Mode: Adapter

| LABEL | DESCRIPTION |
|---|---|
| Adapter Setting | |
| Transfer Rate | In most networking scenarios, the factory default **Auto** setting is the most efficient and allows your G-210H to operate at the highest possible transmission (data) rate.<br>If you want to select a specific transmission rate, select one that the AP or peer wireless device supports.<br>**Note:** With USB1.0/1.1, the G-210H can only transmit at up to 11Mbps. |
| Wireless Mode | Select the wireless mode you wish to have the G-210H transmit in. Available options are to be transmitting in **802.11B/G Mixed** mode which will alternate between 802.11B and 802.11G depending on the network environment, or **802.11B Only** which will force the G-210H to broadcast in 802.11B network only. |
| 11B/G Protection | The factory default setting is on **Auto** which is the most efficient and will allow your G-210H to automatically configure the network settings to best navigate through interfering networks. |
| Enable Tx Burst | Transmission bursting is a method that can boost performance by pushing high number of frames of data per transmission packet. Check this box to enable this feature. |
| Fast Roaming at | Fast Roaming is a feature that allows your G-210H to search for Access Points while you're moving at a faster rate. Select at which dBm you wish for this feature to activate with the drop down menu |
| Enable WMM | WMM is the WiFi standard for wireless Quality of Service. Click on this button and then select from the two available check boxes **Direct Link** and **WMM-Power Save Enable**. |
| Save | Click **Save** to save the changes to the G-210H. |

# CHAPTER 5

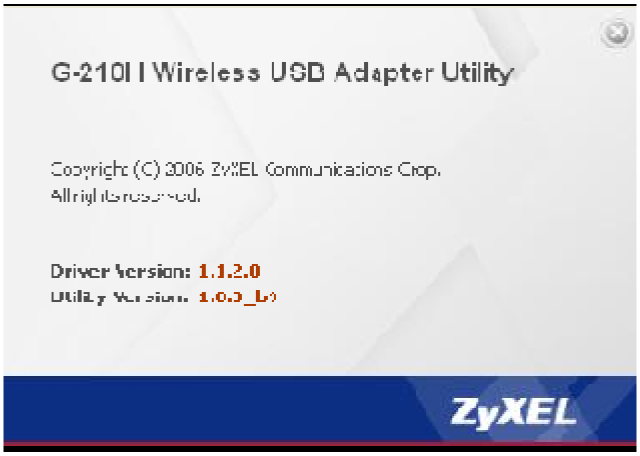
# Maintenance

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

## 5.1 The About Screen

The **About** screen displays driver and utility version numbers of the G-210H. To display the screen shown below, click the about (▤) button.

**Figure 28** About



G-210H Wireless USB Adapter Utility

Copyright (C) 2006 ZyXEL Communications Crop.
All rights reserved.

Driver Version: 1.1.2.0
Utility Version: 1.0.3_b3

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

**Table 12** About

| LABEL | DESCRIPTION |
|---|---|
| Driver Version | This field displays the version number of the G-210H driver. |
| Utility Version | This field displays the version number of the ZyXEL utility. |

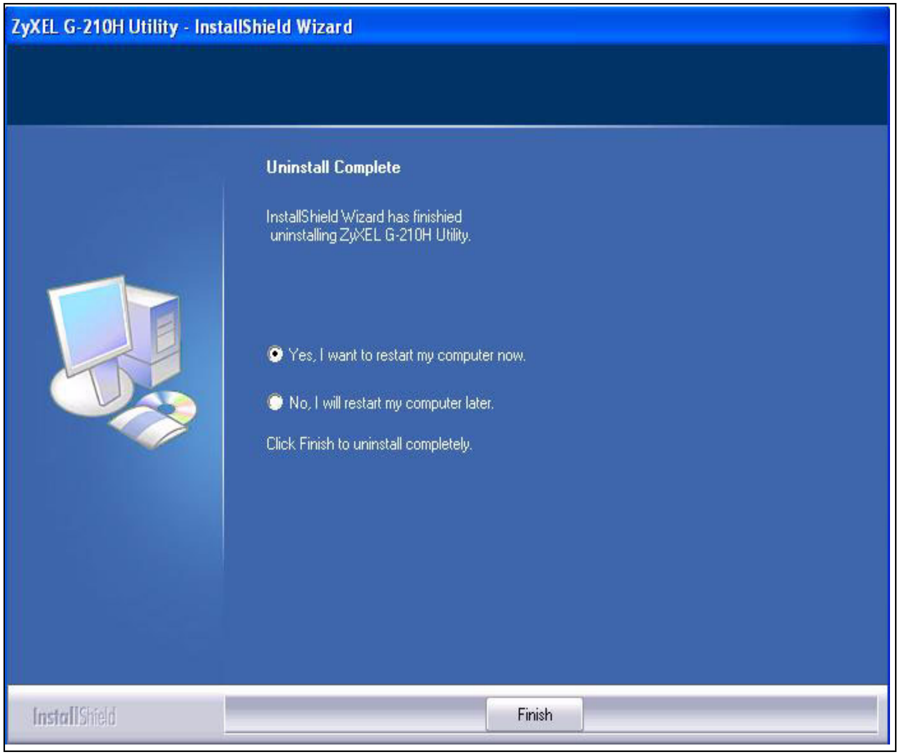
## 5.2 Uninstalling the ZyXEL Utility

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

1 Click **Start**, **(All) Programs**, **ZyXEL G-210H Wireless USB Adapter Utility**, **Uninstall ZyXEL G-210H Wireless USB Adapter Utility**.

2 Click **Finish** to complete uninstalling the software and restart the computer when prompted.

**Figure 29** Uninstall: Finish



Uninstall Complete

InstallShield Wizard has finishied uninstalling ZyXEL G-210H Utility.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Click Finish to uninstall completely.

## 5.3 Upgrading the ZyXEL Utility

**Note:** Before you uninstall the ZyXEL utility, take note of your current wireless configurations.

To perform the upgrade, follow the steps below.

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

2 Follow the steps in Section 5.2 on page 47 to remove the current ZyXEL utility from your computer.

3 Restart your computer when prompted.

4 Disconnect the G-210H from your computer.

5 Double-click on the setup program for the new utility to start the ZyXEL utility installation.

6 Insert the G-210H and check the version numbers in the **About** screen to make sure the new utility is installed properly.

# CHAPTER 6 Troubleshooting

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

## 6.1 Problems Starting the ZyXEL Utility

**Table 13** Troubleshooting Starting ZyXEL Utility

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot start the ZyXEL Wireless LAN utility | Make sure the G-210H is properly inserted and the LED is on. Refer to the Quick Start Guide for the LED descriptions.<br>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 G-210H under **Network Adapter**. (Steps may vary depending on the version of Windows).<br>Install the G-210H in another computer.<br>If the error persists, you may have a hardware problem. In this case, you should contact your local vendor. |
| The ZyXEL utility icon does not display. | Uninstall the utility from the computer, and try reinstalling it from the accompanying CD once more. If the error persists, please contact our technical support staff. |

## 6.2 Problem with the Link Quality

**Table 14** 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.<br>Move your computer closer to the AP or the peer computer(s) within the transmission range.<br>There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Lower the output power of each AP.<br>Make sure there are not too many wireless stations connected to a wireless network. |

## 6.3 Problems Communicating With Other Computers

**Table 15** Troubleshooting Communication Problem

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| The G-210H installed cannot communicate with the other computer(s). | In Infrastructure Mode<br>• Make sure that the AP and the associated computers are turned on and working properly.<br>• Make sure the G-210H computer and the associated AP use the same SSID.<br>• Change the AP and the associated wireless clients to use another radio channel if interference is high.<br>• Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Setting** screen.<br>• If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.<br>In Ad-Hoc (IBSS) Mode<br>• Verify that the peer computer(s) is turned on.<br>• Make sure the G-210H computer and the peer computer(s) are using the same SSID and channel.<br>• Make sure that the computer and the peer computer(s) share the same security settings.<br>• Change the wireless clients to use another radio channel if interference is high. |

# APPENDIX A
# Product Specifications

**Table 16** Product Specifications

| PHYSICAL AND ENVIRONMENTAL | |
|---|---|
| Product Name | ZyXEL G-210H 802.11g High Power Wireless USB Adapter |
| Interface | USB 2.0 compatible |
| Standards | IEEE 802.11b<br>IEEE 802.11g |
| Antenna Configuration | 5dBi Directional Diversity Antenna |
| Network Architectures | Infrastructure<br>Ad-Hoc |
| Operating Frequencies | IEEE 802.11b/g: 2.4 - 2.4835GHz |
| Operating Channels | IEEE 802.11b: 11 channels (North America)<br>IEEE 802.11g: 11 channels (North America)<br>IEEE 802.11b: 13 channels (Europe)<br>IEEE 802.11g: 13 channels (Europe)<br>IEEE 802.11b: 13 channels (Japan)<br>IEEE 802.11g: 13 channels (Japan) |
| Data Rate | IEEE 802.11b: 11, 5.5, 2, 1Mbps<br>IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps |
| Modulation | IEEE 802311b: Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).<br>IEEE 802.11g: Orthogonal Frequency Division Multiplexing |
| Operating Temperature | 0 ~ 55 degrees Centigrade |
| Storage Temperature | -20 ~ 70 degrees Centigrade |
| Operating Humidity | 20 ~ 90% (non-condensing) |
| Storage Humidity | 20 ~ 90% (non-condensing) |
| Power | TX power consumption: < 290mA<br>RX power consumption: < 220mA |
| Voltage | 5V |
| Weight | 35g |
| Dimension | (L) 111 mm × (W) 35 mm × (H) 12 mm |
| **RADIO SPECIFICATIONS** | |
| Media Access Protocol | IEEE 802.11 |
| Frequency | Industrial Scientific Medical Band<br>2.4 ~ 2.484 GHz (IEEE 802.11b/g) |
| Channels | 1 ~ 11 channels (USA, Canada and Taiwan)<br>1 ~ 13 channels (Europe)<br>1 ~ 13 channels (Japan) |

**Table 16** Product Specifications (continued)

| | |
|---|---|
| Data Rate | 54 Mbps with automatic fallback to 48, 36, 24, 18, 12, 9 and 6 Mbps |
| Modulation | IEEE 802.11b: CCK, DQPSK, DBPSK<br>IEEE 802.11g: OFDM |
| Output Power | IEEE 802.11b:<br>11dBm (+/- 1.5dBm) at 11Mbps<br><br>IEEE 802.11g:<br>14dBm (+/- 1dBm) at 54Mbps |
| RX Sensitivity | IEEE 802.11b: 11 Mbps: -85 dBm<br>IEEE 802.11g: 54 Mbps: -69 dBm |
| **SOFTWARE SPECIFICATIONS** | |
| Device Drivers | Windows 2000, XP, Vista, Mac OS X 10.3 or Higher |
| Security | 64/128-bit WEP<br>WPA/WPA-PSK/WPA2/WPA2-PSK<br>IEEE 802.1x |
| Roaming | IEEE 802.11b/g compliant |

# APPENDIX B
# Management with Wireless Zero Configuration

This appendix shows you how to manage your G-210H using the Windows XP Wireless Zero Configuration tool.

Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

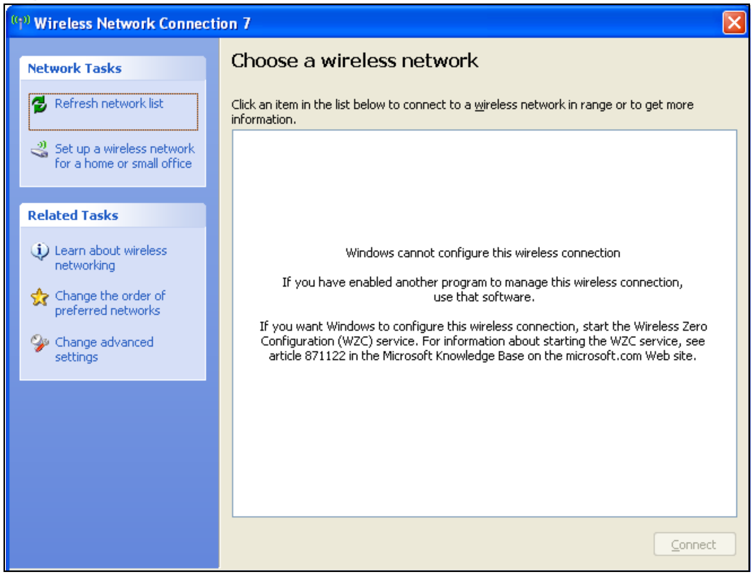
Windows XP SP2 screen shots are shown unless otherwise specified. Click the help icon ( ? ) in most screens, move the cursor to the item that you want the information about and click to view the help.

## Activating Windows Wireless Zero Configuration

Make sure the **Use Windows to configure my wireless network settings** check box is selected in the **Wireless Network Connection Properties** screen. Refer to Appendix A on page 45.

If you see the following screen, refer to article 871122 on the Microsoft web site for information on starting WZC.

**Figure 30** Windows XP SP2: WZC Not Available



Wireless Network Connection 7
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Windows cannot configure this wireless connection

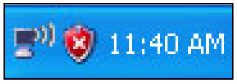
If you have enabled another program to manage this wireless connection, use that software.

If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.

# Connecting to a Wireless Network

**1** Double-click the network icon for wireless connections in the system tray to open the Wireless Network Connection Status screen.

**Figure 31** Windows XP SP2: System Tray Icon



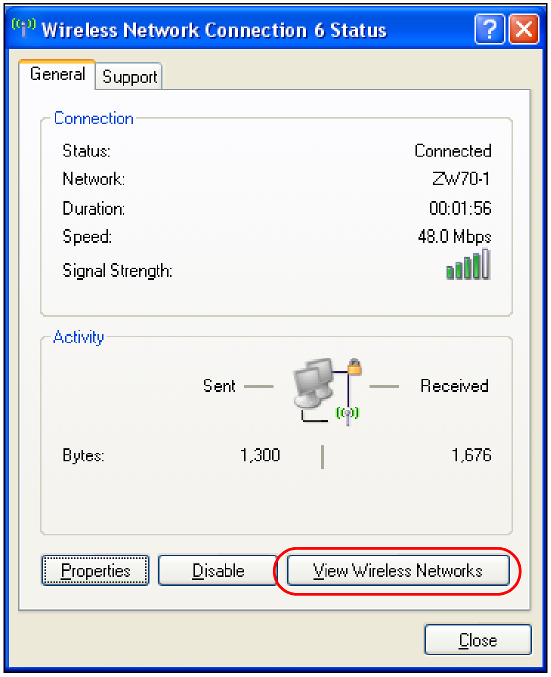
The type of the wireless network icon in Windows XP SP2 indicates the status of the G-210H. Refer to the following table for details.

**Table 17** Windows XP SP2: System Tray Icon

| ICON | DESCRIPTION |
|---|---|
| 📶 | The G-210H is connected to a wireless network. |
| 📶⏳ | The G-210H is in the process of connecting to a wireless network. |
| ⚠ | The connection to a wireless network is limited because the network did not assign a network address to the computer. |
| ✗ | The G-210H is not connected to a wireless network. |

**2** Windows XP SP2: In the **Wireless Network Connection Status** screen, click **View Wireless Networks** to open the **Wireless Network Connection** screen.

**Figure 32** Windows XP SP2: Wireless Network Connection Status



Wireless Network Connection 6 Status

General | Support

Connection

Status: Connected

Network: ZW70-1

Duration: 00:01:56

Speed: 48.0 Mbps

Signal Strength:

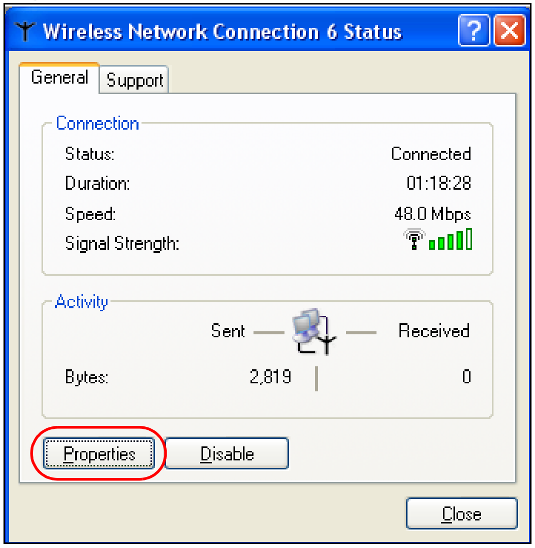
Activity

Sent — Received

Bytes: 1,300 | 1,676

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the **Wireless Network Connection Properties** screen.

**Figure 33** Windows XP SP1: Wireless Network Connection Status



Wireless Network Connection 6 Status

Connection

Status: Connected

Duration: 01:18:28

Speed: 48.0 Mbps

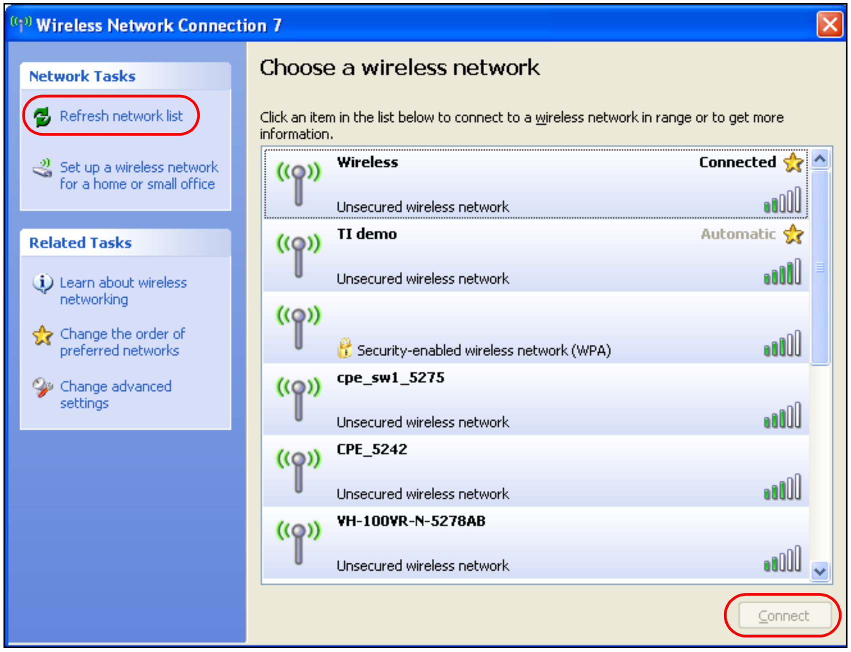
Signal Strength:

Activity

| | Sent | Received |
|---|---|---|
| Bytes: | 2,819 | 0 |

3 Windows XP SP2: Click **Refresh network list** to reload and search for available wireless devices within transmission range. Select a wireless network in the list and click **Connect** to join the selected wireless network.

**Figure 34** Windows XP SP2: Wireless Network Connection



Wireless Network Connection 7

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Wireless — Connected — Unsecured wireless network

TI demo — Automatic — Unsecured wireless network

Security-enabled wireless network (WPA)

cpe_sw1_5275 — Unsecured wireless network

CPE_5242 — Unsecured wireless network

VH-100VR-N-5278AB — Unsecured wireless network

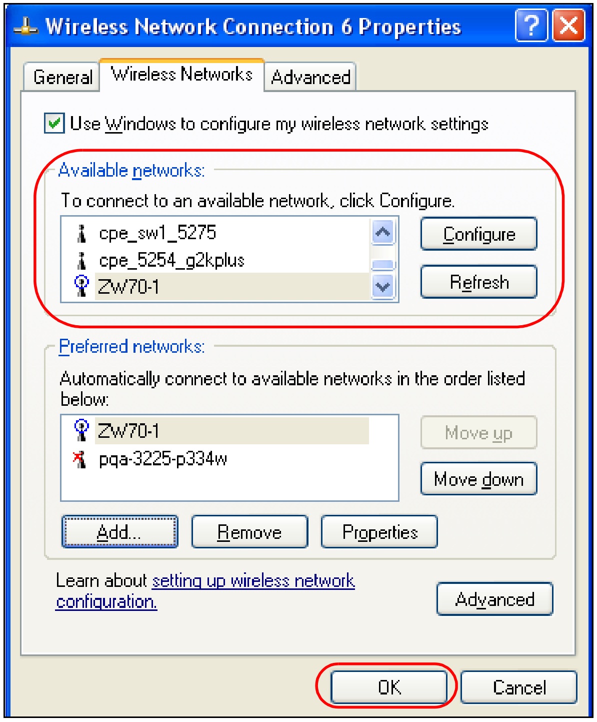
The following table describes the icons in the wireless network list.

**Table 18** Windows XP SP2: Wireless Network Connection

| ICON | DESCRIPTION |
|---|---|
| 🔒 | This denotes that wireless security is activated for the wireless network. |
| ⭐ | This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the G-210H tries to associate to the preferred network first in the order that you specify. Refer to the section on ordering the preferred networks for detailed information. |
| 📶 | This denotes the signal strength of the wireless network.<br>Move your cursor to the icon to see details on the signal strength. |

Windows XP SP1: Click **Refresh** to reload and search for available wireless devices within transmission range. Select a wireless network in the **Available networks** list, click **Configure** and set the related fields to the same security settings as the associated AP to add the selected network into the **Preferred** networks table. Click **OK** to join the selected wireless network. Refer to the section on security settings (discussed later) for more information.

**Figure 35** Windows XP SP1: Wireless Network Connection Properties



Wireless Network Connection 6 Properties

General | Wireless Networks | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

Preferred networks:

Automatically connect to available networks in the order listed below:

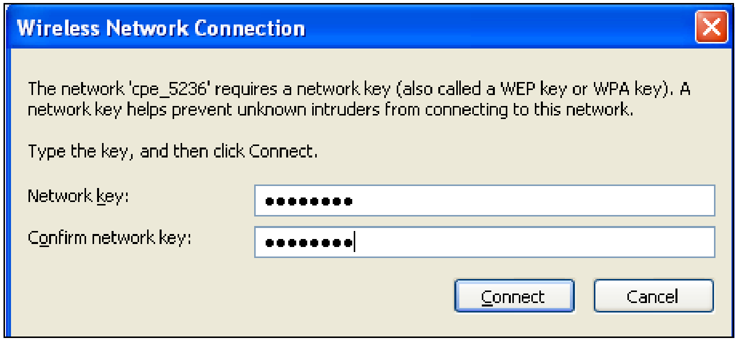
- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

**4** 4.Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about security settings for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption.

If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.

**Figure 36** Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK



Wireless Network Connection

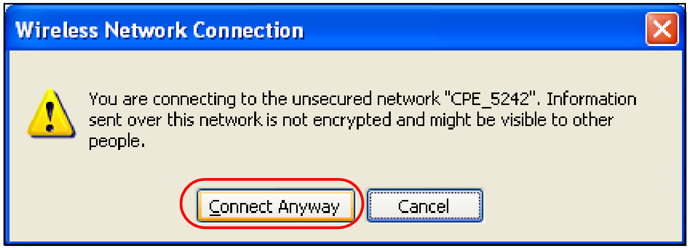
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ••••••••

Confirm network key: ••••••••

**Figure 37** Windows XP SP2: Wireless Network Connection: No Security



Wireless Network Connection

You are connecting to the unsecured network "CPE_5242". Information sent over this network is not encrypted and might be visible to other people.

**5** Verify that you have successfully connected to the selected network and check the connection status in the wireless network list or the connection icon in the **Preferred networks** or **Available networks** list.

The following table describes the connection icons.

**Table 19** Windows XP: Wireless Networks

| ICON | DESCRIPTION |
|---|---|
| 📡 | This denotes the wireless network is an available wireless network. |
| 📡 | This denotes the G-210H is associated to the wireless network. |
| ✗📡 | This denotes the wireless network is not available. |

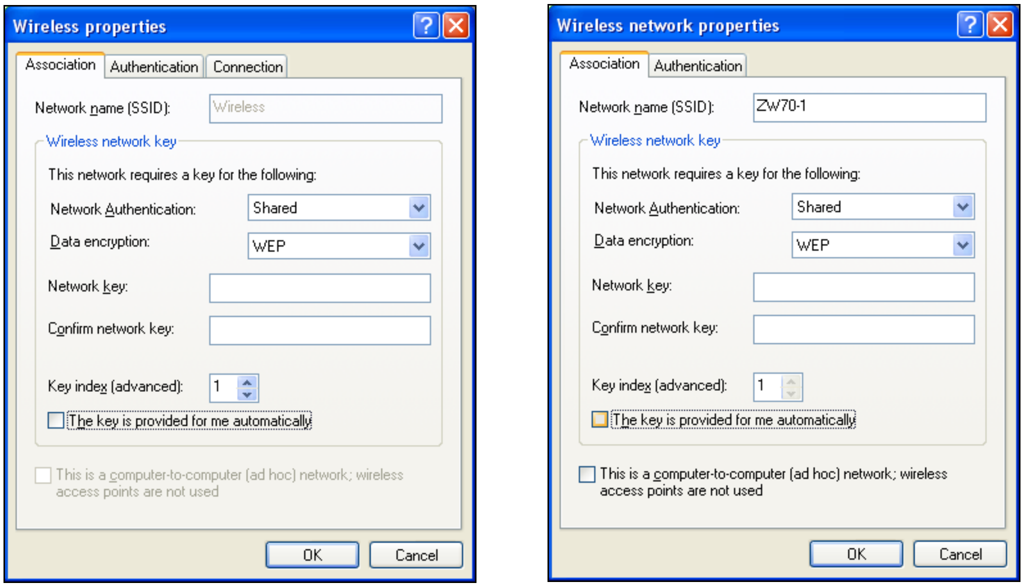
# Security Settings

When you configure the G-210H to connect to a secure network but the security settings are not yet enabled on the G-210H, you will see different screens according to the authentication and encryption methods used by the selected network.

## Association

Select a network in the Preferred networks list and click Properties to view or configure security.

**Figure 38** Windows XP: Wireless (network) properties: Association



Wireless properties

Network name (SSID): Wireless

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless network properties

Network name (SSID): ZW70-1

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

The following table describes the labels in this screen.

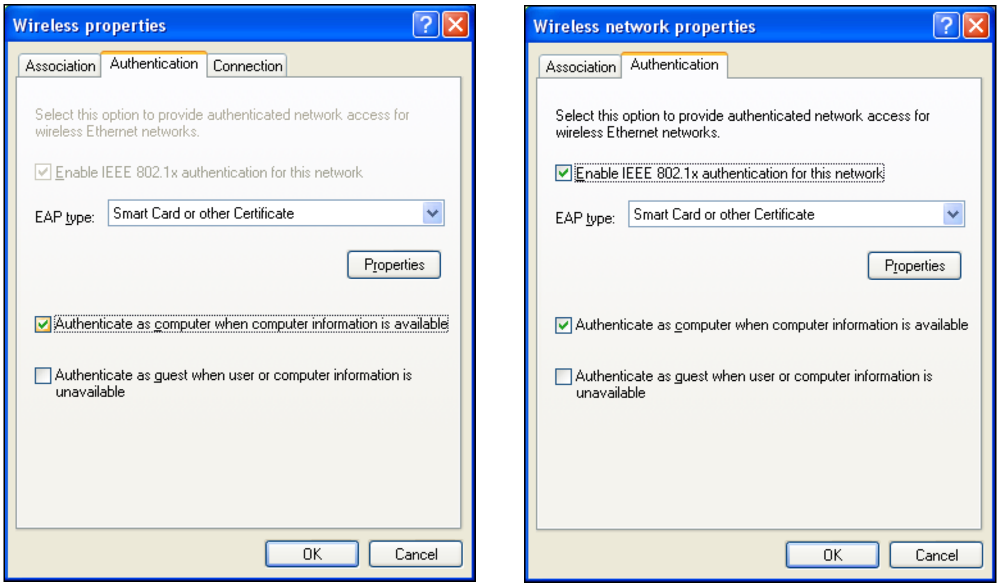
**Table 20** Windows XP: Wireless (network) properties: Association

| LABEL | DESCRIPTION |
|---|---|
| Network name (SSID) | This field displays the SSID (Service Set IDentifier) of each wireless network. |
| Network Authentication | This field automatically shows the authentication method (**Share**, **Open**, **WPA, WPA2** or **WPA-PSK, WPA2-PSK**) used by the selected network. |
| Data Encryption | This field automatically shows the encryption type (**AES**, **TKIP**, **WEP** or **Disable**) used by the selected network. |
| Network Key | Enter the pre-shared key or WEP key.<br>The values for the keys must be set up exactly the same on all wireless devices in the same wireless LAN. |
| Confirm network key | Enter the key again for confirmation. |
| Key index (advanced) | Select a default WEP key to use for data encryption.<br>This field is available only when the network use **WEP** encryption method and the **The key is provided for me automatically** check box is not selected. |
| The key is provided for me automatically | If this check box is selected, the wireless AP assigns the G-210H a key. |
| This is a computer-to-computer (ad hoc) network; wireless access points are not used | If this check box is selected, you are connecting to another computer directly. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

## Authentication

Click the **Authentication** tab in the **Wireless (network) properties** screen to display the screen shown next. The fields on this screen are grayed out when the network is in Ad-Hoc mode or data encryption is disabled.

**Figure 39** Windows XP: Wireless (network) properties: Authentication



Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

The following table describes the labels in this screen.

**Table 21** Windows XP: Wireless (network) properties: Authentication

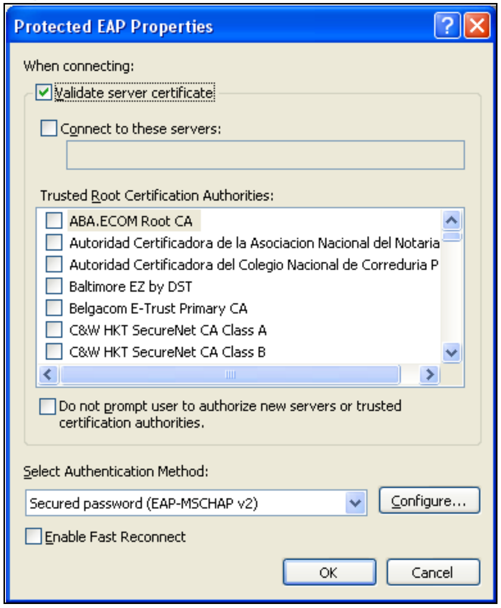
| LABEL | DESCRIPTION |
|---|---|
| Enable IEEE 802.1x authentication for this network | This field displays whether the IEEE 802.1x authentication is active.<br>If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature. |
| EAP Type | Select the type of EAP authentication. Options are **Protected EAP (PEAP)** and **Smart Card or other Certificate**. |
| Properties | Click this button to open the properties screen and configure certificates. The screen varies depending on what you select in the **EAP type** field. |
| Authenticate as computer when computer information is available | Select this check box to have the computer send its information to the network for authentication when a user is not logged on. |
| Authenticate as guest when user or computer information is unavailable | Select this check box to have the computer access to the network as a guest when a user is not logged on or computer information is not available. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

## Authentication Properties

Select an EAP authentication type in the **Wireless (network) properties: Authentication** screen and click the **Properties** button to display the following screen.

### *Protected EAP Properties*

**Figure 40** Windows XP: Protected EAP Properties



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria P
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method: Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

The following table describes the labels in this screen.

**Table 22** Windows XP: Protected EAP Properties

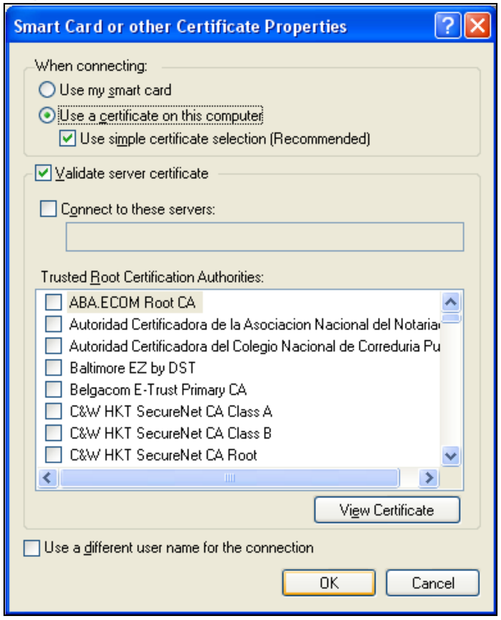
| LABEL | DESCRIPTION |
|---|---|
| Validate server certificate | Select the check box to verify the certificate of the authentication server. |
| Connect to these servers | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain. |
| Trusted Root Certification Authorities: | Select a trusted certification authority from the list below.<br>**Note:** 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. |
| Do not prompt user to authorize new server or trusted certification authorities. | Select this check box to verify a new authentication server or trusted CA without prompting.<br>This field is available only if you installed the Windows XP server pack 2. |
| Select Authentication Method: | Select an authentication method from the drop-down list box and click **Configure** to do settings. |

**Table 22** Windows XP: Protected EAP Properties

| LABEL | DESCRIPTION |
|---|---|
| Enable Fast Reconnect | Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

### *Smart Card or other Certificate Properties*

**Figure 41** Windows XP: Smart Card or other Certificate Properties



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B
□ C&W HKT SecureNet CA Root

□ Use a different user name for the connection

The following table describes the labels in this screen.

**Table 23** Windows XP: Smart Card or other Certificate Properties

| LABEL | DESCRIPTION |
|---|---|
| Use my smart card | Select this check box to use the smart card for authentication. |
| Use a certificate on this computer | Select this check box to use a certificate on your computer for authentication. |
| Validate server certificate | Select the check box to check the certificate of the authentication server. |
| Connect to these servers | Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain. |
| Trusted Root Certification Authorities: | Select a trusted certification authority from the list below.<br>**Note:** 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. |
| View Certificate | Click this button if you want to verify the selected certificate. |

**Table 23** Windows XP: Smart Card or other Certificate Properties

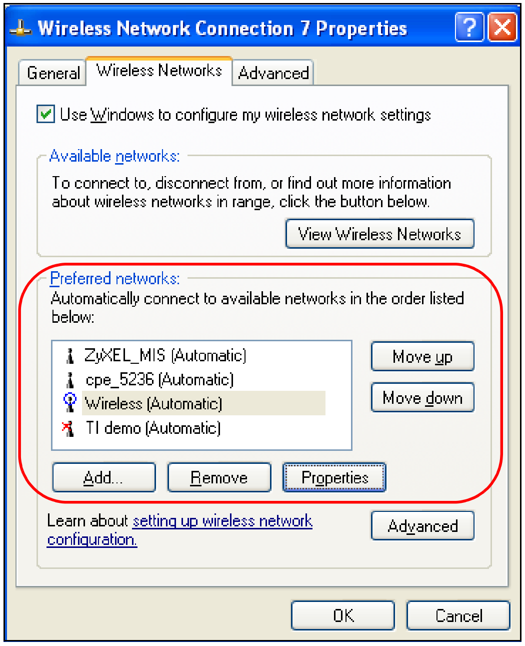
| LABEL | DESCRIPTION |
|---|---|
| Use a different user name for the connection: | Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to leave this screen without saving any changes you may have made. |

## Ordering the Preferred Networks

Follow the steps below to manage your preferred networks.

**1** Windows XP SP2: Click **Change the order of preferred networks** in the **Wireless Network Connection** screen (see Figure 34 on page 55). The screen displays as shown.

**Figure 42** Windows XP SP2: Wireless Networks: Preferred Networks



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

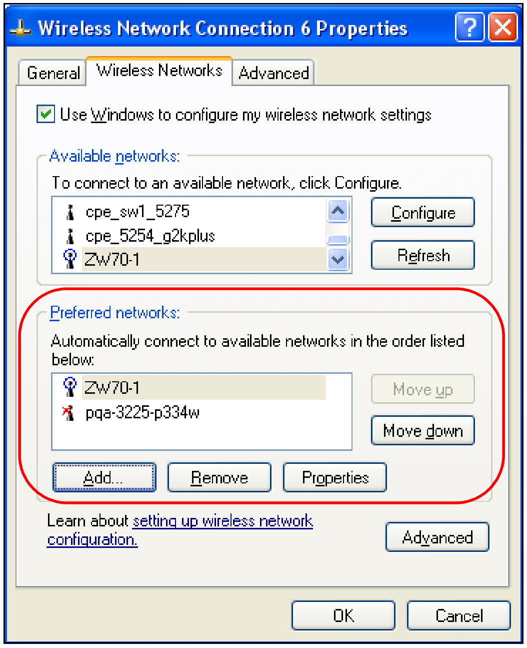
Automatically connect to available networks in the order listed below:

- ZyXEL_MIS (Automatic)
- cpe_5236 (Automatic)
- Wireless (Automatic)
- TI demo (Automatic)

Learn about setting up wireless network configuration.

Windows XP SP1: In the **Wireless Network Connection Status** screen, click **Properties** and the **Wireless Networks** tab to open the screen as shown.

**Figure 43** Windows XP SP1: Wireless Networks: Preferred Networks


Wireless Network Connection 6 Properties
General
Wireless Networks
Advanced
☑ Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
cpe_sw1_5275
cpe_5254_g2kplus
ZW70-1
Configure
Refresh
Preferred networks:
Automatically connect to available networks in the order listed below:
ZW70-1
pqa-3225-p334w
Move up
Move down
Add...
Remove
Properties
Learn about setting up wireless network configuration.
Advanced
OK
Cancel

2 Whenever the G-210H tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change it's order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

# APPENDIX C
# Wireless Security

## Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x 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 IEEE 802.1x.

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.

## 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 IEEE 802.1x.

# Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

**Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange

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 authentication types.

**Table 24** 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 |

# WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-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 wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include 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.

WPA and WPA2 regularly change and rotate 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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. 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), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

## User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## WPA(2)-PSK Application Example

A WPA(2)s-PSK application looks as follows.

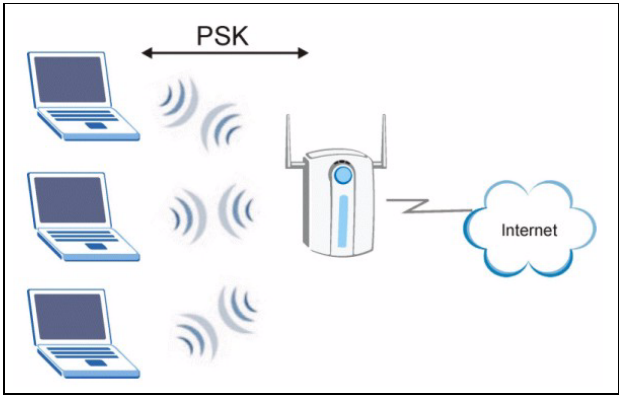
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

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

3 The AP and wireless clients use the pre-shared key to generate a common PMK.

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

**Figure 44** WPA-PSK Authentication



## WPA(2) with RADIUS Application Example

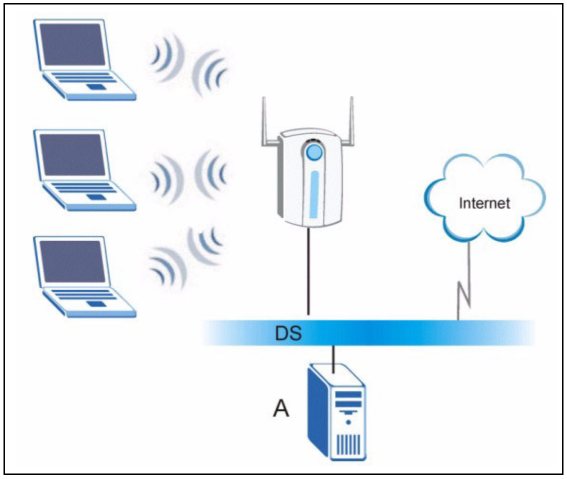
You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

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

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

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 45** WPA(2) with RADIUS Application Example



## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 25** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|---|---|---|---|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

# APPENDIX D
# Setting up Your Computer's IP Address

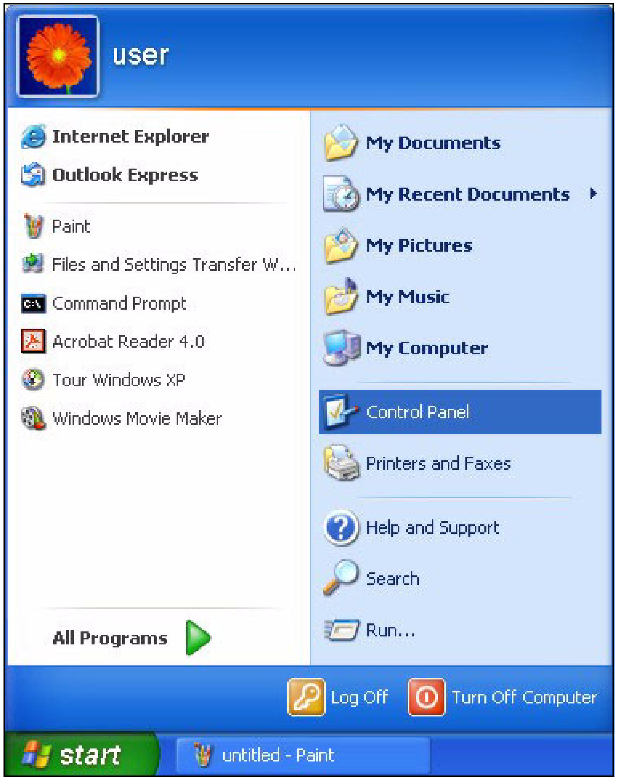
All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed. Windows 2000 and XP usually include TCP/IP.

Configure the TCP/IP settings in order to "communicate" with your network.

## Windows 2000/XP

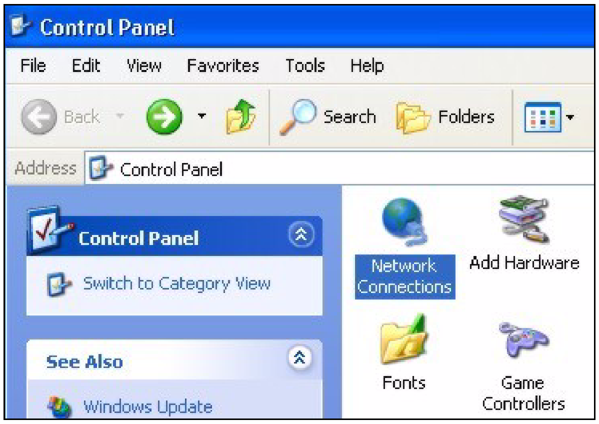
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

**Figure 46** Windows XP: Start Menu



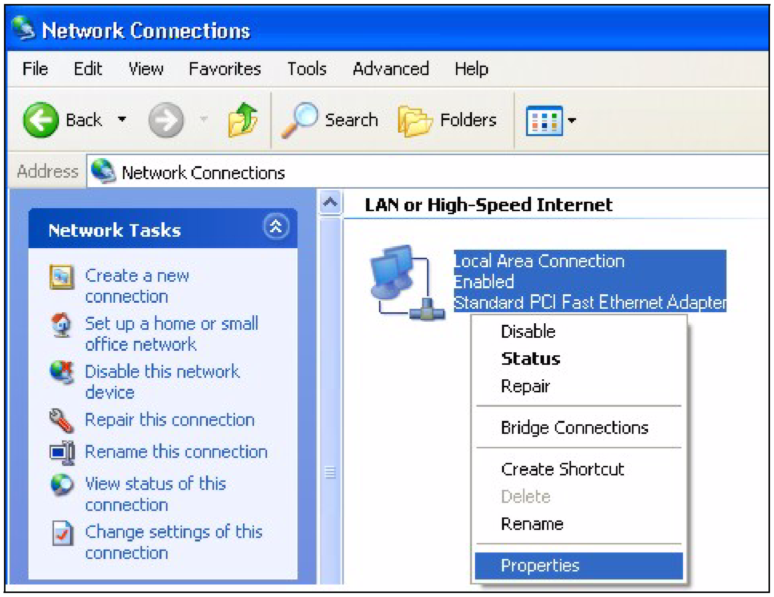
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 47** Windows XP: Control Panel



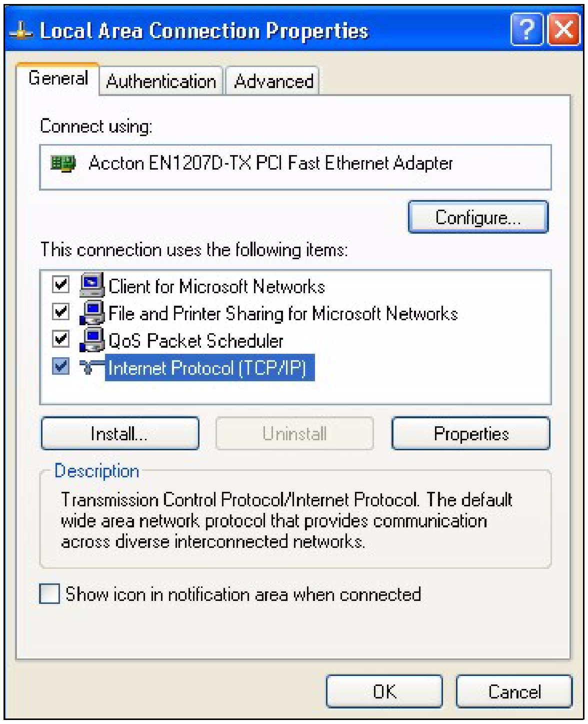
3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 48** Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

**Figure 49** Windows XP: Local Area Connection Properties



Local Area Connection Properties

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

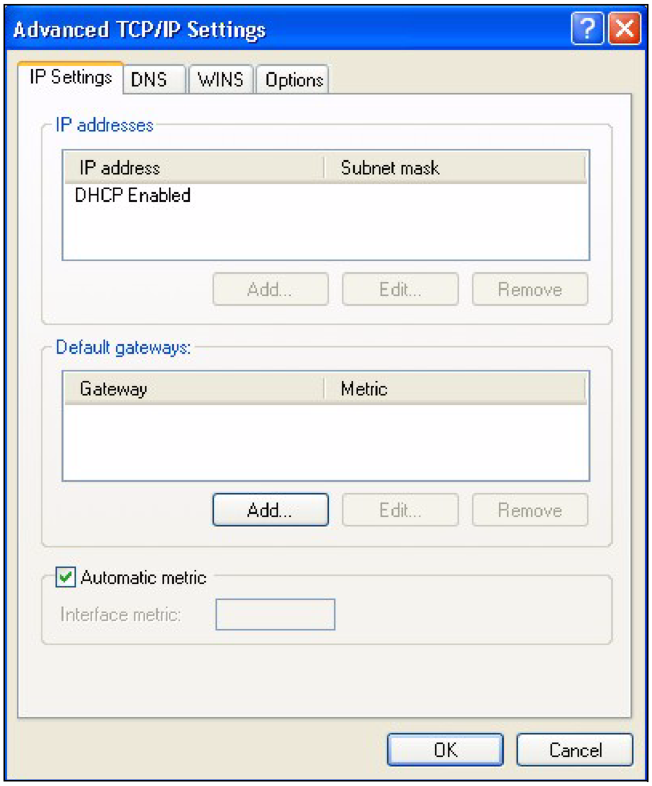
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

**5** The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

**Figure 50** Windows XP: Advanced TCP/IP Settings



| IP address | Subnet mask |
|---|---|
| DHCP Enabled | |

☑ Automatic metric

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

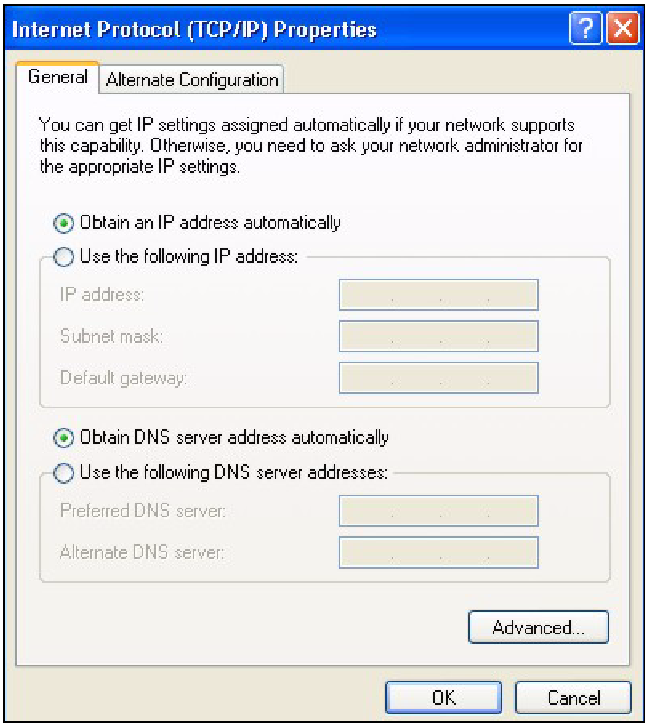
7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 51** Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

**8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

**9** Click **OK** to close the **Local Area Connection Properties** window.

**10**Restart your computer (if prompted).

## Verifying Settings

**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

**2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

# Index