G-210H

802.11b/g Wireless USB Adapter

User’s Guide

Version 1.00
3/2007
Edition 1

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the G-210H using the ZyXEL utility in Windows. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The G-210H may be referred to as the "device" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** submenu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons.

AP 	Computer 	Notebook computer
Server 	Wireless Signal 	Modem or Router
Internet Cloud 		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Antenna Warning! This device meets FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

This product is recyclable. Dispose of it properly.

Contents Overview

Table of Contents

List of Figures

List of Tables

1

Getting Started

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

1.1 About Your G-210H

The G-210H is an IEEE 802.11b/g compliant wireless LAN adapter. The ZyXEL utility is a tool that helps you configure your G-210H. See the appendix for detailed product specifications.

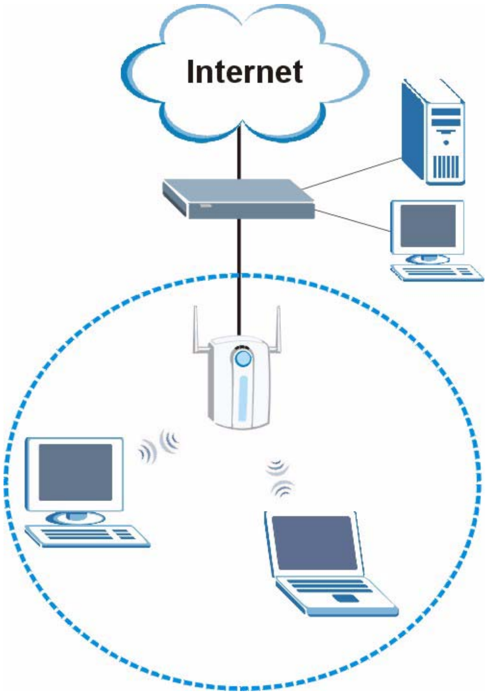
1.2 Application Overview

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

1.2.1 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

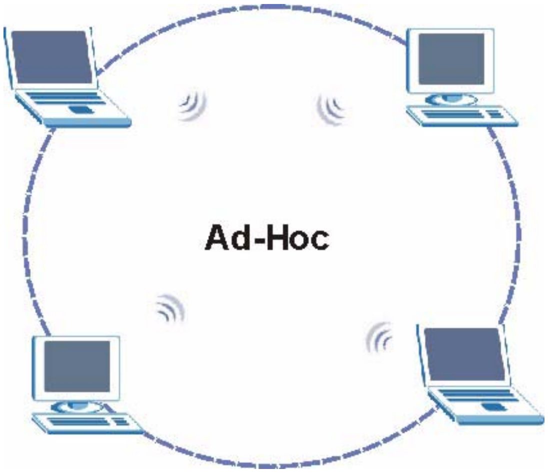


1.2.2 Ad-Hoc

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 (wireless stations) in Ad-Hoc mode communicate directly to each other.

Figure 2 Application: Ad-Hoc



1.3 G-210H Hardware and Utility Installation

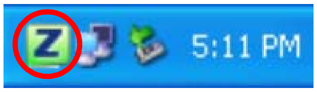
Follow the instructions in the Quick Start Guide to install the ZyXEL utility and make hardware connections.

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.

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

Figure 3 ZyXEL Utility: System Tray Icon in Windows



In Windows, 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 in Windows

COLOR	DESCRIPTION
Red	The G-210H is not connected to a wireless network or is searching for an available wireless network.
Green	The G-210H is connected to a wireless network.

1.4 Configuration Methods

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

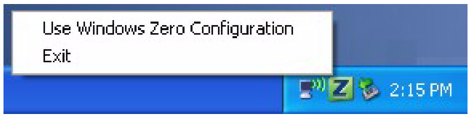
- ZyXEL Utility
- Wireless Zero Configuration (WZC) (the Windows XP wireless configuration tool) or WLAN AutoConfig (the Windows Vista wireless configuration tool)

1.4.1 Enabling WZC

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 **Windows Zero Configuration**.

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 Utility**, **ZyXEL G-210H Utility**.

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 2000 are shown in this User's Guide.

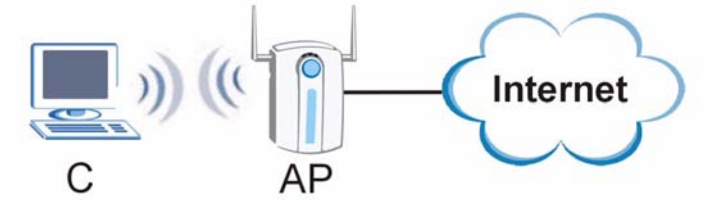
✍ Click the ? icon (located in the top right corner) to display the online help window.

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) 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 19).
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer (see Section 2.2 on page 21).

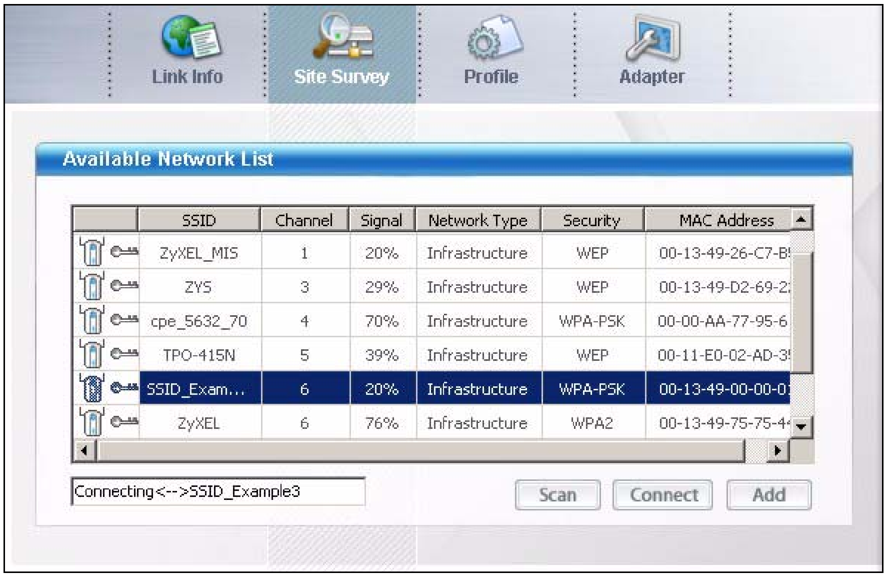
2.1 Connecting to a Wireless LAN

This example illustrates how to manually connect your wireless client to an access point (AP) which is 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 SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey” in the AP.

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 as shown next.

Figure 6 ZyXEL Utility: Site Survey



	SSID	Channel	Signal	Network Type	Security	MAC Address
	ZyXEL_MIS	1	20%	Infrastructure	WEP	00-13-49-26-C7-B
	ZYS	3	29%	Infrastructure	WEP	00-13-49-D2-69-2
	cpe_5632_70	4	70%	Infrastructure	WPA-PSK	00-00-AA-77-95-6
	TPO-415N	5	39%	Infrastructure	WEP	00-11-E0-02-AD-3
	SSID_Exam...	6	20%	Infrastructure	WPA-PSK	00-13-49-00-00-0
	ZyXEL	6	76%	Infrastructure	WPA2	00-13-49-75-75-4

Connecting<-->SSID_Example3

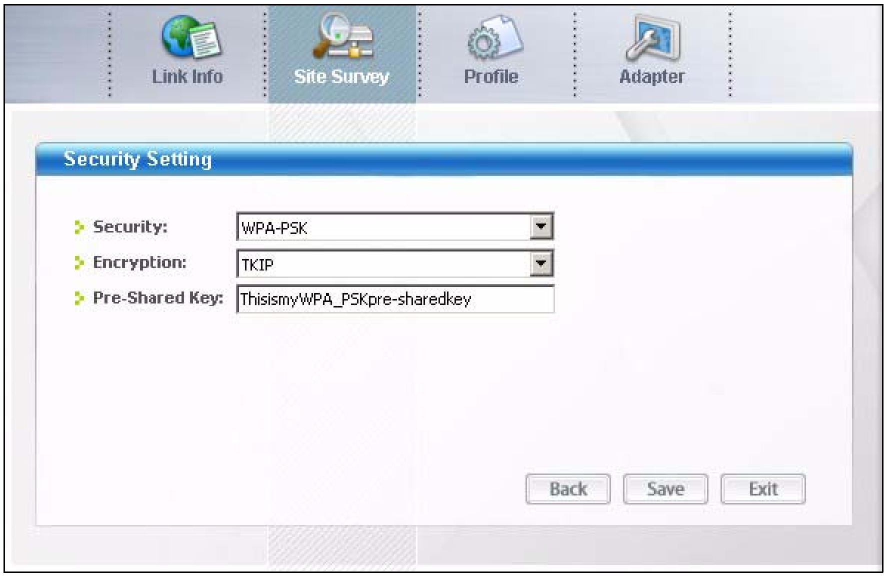
2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on, or move the wireless client closer to the AP or peer computer. See Table 4 on page 32 for detailed field descriptions.

3 To connect to an AP or peer computer, click an entry (with a SSID of **SSID_Example3** in this example) in the list and then click **Connect**.

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 or click **Save** to save your settings and go 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 Setting



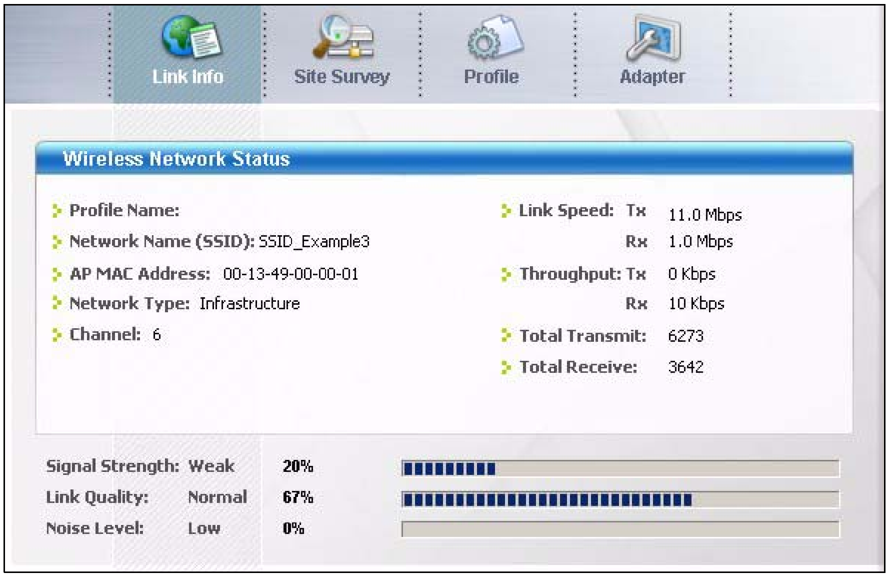
Security: WPA-PSK

Encryption: TKIP

Pre-Shared Key: ThisismyWPA_PSKpre-sharedkey

5 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 30 for detailed field descriptions.

Figure 8 ZyXEL Utility: Link Info



Profile Name:
Network Name (SSID): SSID_Example3
AP MAC Address: 00-13-49-00-00-01
Network Type: Infrastructure
Channel: 6

Link Speed: Tx 11.0 Mbps
Rx 1.0 Mbps
Throughput: Tx 0 Kbps
Rx 10 Kbps
Total Transmit: 6273
Total Receive: 3642

Signal Strength: Weak 20%
Link Quality: Normal 67%
Noise Level: Low 0%

6 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.

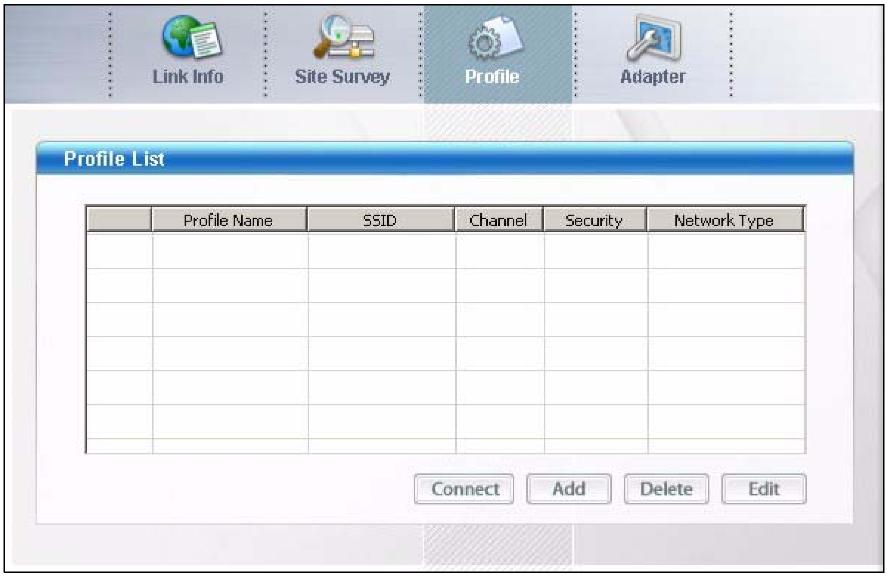
2.2 Creating and Using a Profile

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 SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey” in the AP. 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 9 ZyXEL Utility: Profile

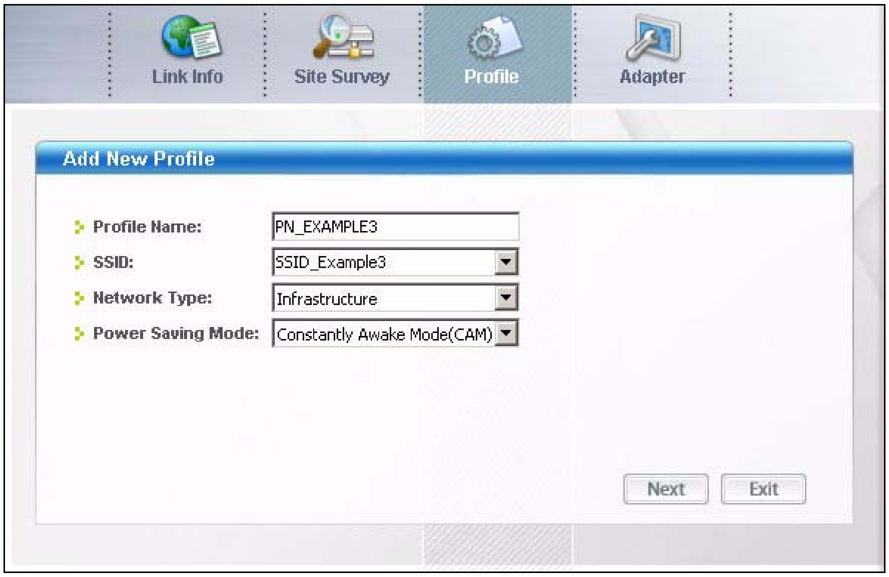


Profile List

	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 **SSID** drop-down list box. You can also configure your profile for a wireless network that is not in the list.

Figure 10 ZyXEL Utility: Add New Profile



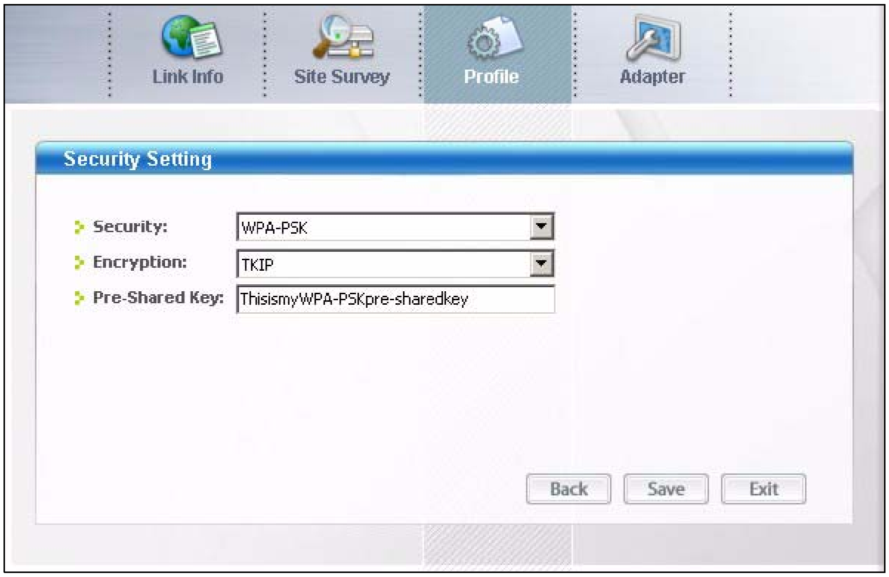
Add New Profile

Profile Name:	PN_EXAMPLE3
SSID:	SSID_Example3
Network Type:	Infrastructure
Power Saving Mode:	Constantly Awake Mode(CAM)

3 Give the profile a descriptive name. Select **Infrastructure** and either manually enter or select the AP's SSID in the **SSID** drop-down list box.

4 Choose the same security mode as the AP to which you want to connect (In this example, WPA-PSK).

Figure 11 ZyXEL Utility: Profile Security



Security: WPA-PSK

Encryption: TKIP

Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey

5 This screen varies depending on the security mode you selected. In this example, enter the pre-shared key and leave the encryption type at the default setting.

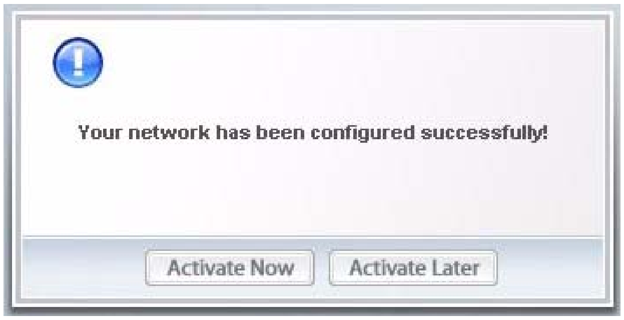
6 Click **Save** to save and go to the next screen.

7 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.

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

Figure 12 ZyXEL Utility: Profile Activate



Your network has been configured successfully!

8 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.

9 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.

10 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.

3

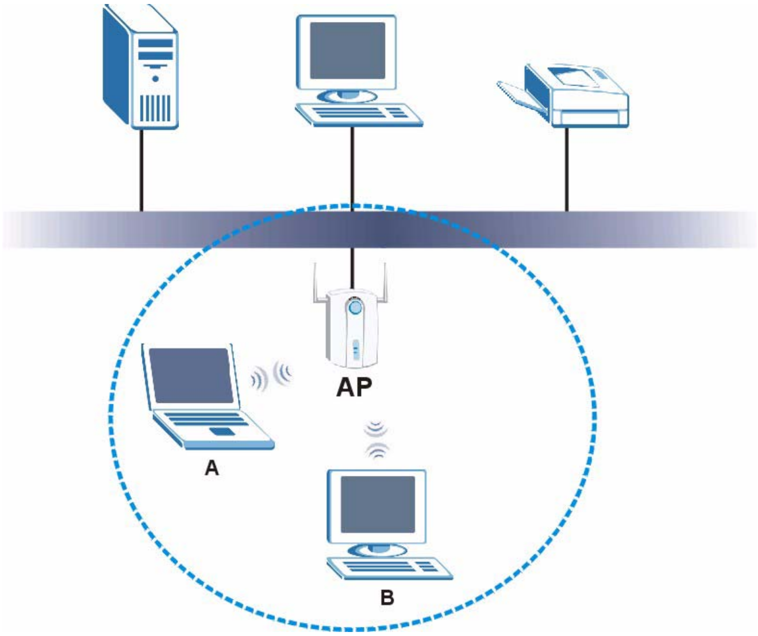
Wireless LAN Network

This chapter provides background information on wireless LAN network.

3.1 Wireless LAN Overview

The following figure provides an example of a wireless network with an AP. See Figure 2 on page 16 for an Ad Hoc network example.

Figure 13 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 **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.

You can only use WEP or WPA-NONE if you set the G-210H to Ad-hoc mode.

See the appendices for more detailed information about wireless security.

3.2.1 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.

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.

3.2.1.1 WEP

3.2.1.1.1 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.

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

3.2.1.1.2 Authentication Method

The IEEE 802.11 b/g standard describes a simple authentication method between the wireless stations and AP or peer computer. The authentication types are defined: Open system and Shared key.

- Open system 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 key 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.

3.2.1.2 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.

3.2.1.2.1 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 TLS, TTLS and PEAP. Refer to Appendix C on page 71 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.

3.2.1.3 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.

3.2.1.4 WPA-None

Similar to static WEP encryption, WPA-None uses a static pre-shared key to encrypt data transmitted between the wireless devices (in Ad-hoc mode), and there is no authentication involved (unlike WPA-PSK). But WPA-None provides stronger encryption than static WEP by using either TKIP or AES.

4

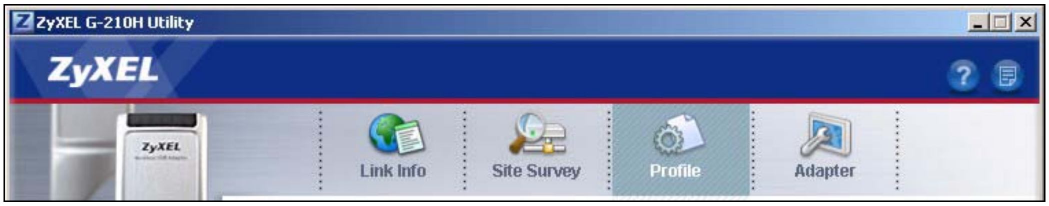
ZyXEL Utility Configuration

This chapter shows you how to use the ZyXEL utility to configure your G-210H.

4.1 ZyXEL Utility Screen Summary

This section describes the ZyXEL utility screens.

Figure 14 ZyXEL Utility Menu Summary



The following table describes the menus.

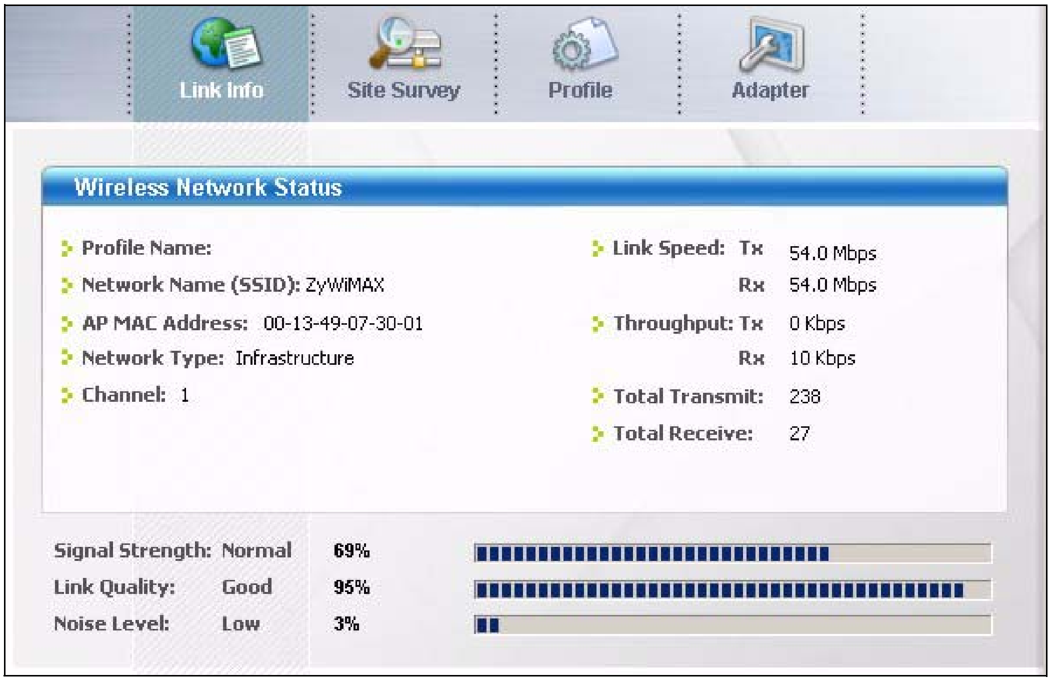
Table 2 ZyXEL Utility Menu Summary

TAB	DESCRIPTION
Link Info	Use this screen to see your current connection status, configuration and data rate statistics.
Site Survey	Use this screen to • scan for a wireless network • configure wireless security (if activated on the selected network). • 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 • select a transfer rate, • configure wireless mode, • enable fast roaming and Tx burst, • configure WMM settings.

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 15 Link Info



Wireless Network Status

- Profile Name:
- Network Name (SSID): ZyWiMAX
- AP MAC Address: 00-13-49-07-30-01
- Network Type: Infrastructure
- Channel: 1
- Link Speed: Tx 54.0 Mbps
  Rx 54.0 Mbps
- Throughput: Tx 0 Kbps
  Rx 10 Kbps
- Total Transmit: 238
- Total Receive: 27

Signal Strength:	Normal	69%
Link Quality:	Good	95%
Noise Level:	Low	3%

The following table describes the labels in this screen.

Table 3 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 number of the channel used by the AP or peer computer.
Link Speed	
Tx	This field displays the current data transmission rate in megabits per second (Mbps).
Rx	This field displays the current data receiving rate in megabits per second (Mbps).
Throughput	
Tx	This field displays the current transmission throughput in kilobits per second (Kbps).
Rx	This field displays the current receiving throughput 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.

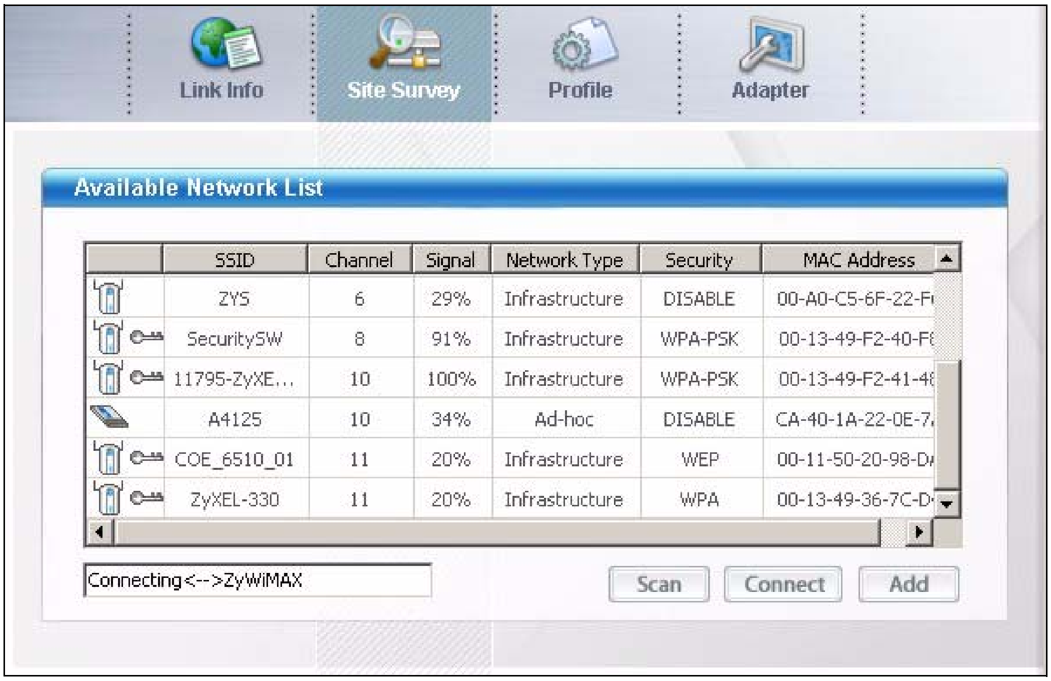
Table 3 Link Info (continued)

LABEL	DESCRIPTION
Signal Strength	This field displays whether the signal strength is **Weak**, **Normal** or **Good**, and the percentage of the G-210H's 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.
Link Quality	This field displays whether the link quality is **Weak**, **Normal** or **Good**, and the percentage of packets transmitted successfully. The status bar shows the quality of wireless connection. 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 whether the noise level is **Low** or **High**, and the percentage of noise in wireless transmissions. The status bar shows the level of noise.

4.3 The Site Survey Screen

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

Figure 16 Site Survey



	SSID	Channel	Signal	Network Type	Security	MAC Address
	ZYS	6	29%	Infrastructure	DISABLE	00-A0-C5-6F-22-F
	SecuritySW	8	91%	Infrastructure	WPA-PSK	00-13-49-F2-40-F
	11795-ZyXE...	10	100%	Infrastructure	WPA-PSK	00-13-49-F2-41-4
	A4125	10	34%	Ad-hoc	DISABLE	CA-40-1A-22-0E-7
	COE_6510_01	11	20%	Infrastructure	WEP	00-11-50-20-98-D
	ZyXEL-330	11	20%	Infrastructure	WPA	00-13-49-36-7C-D

Connecting<-->ZyWiMAX

The following table describes the labels in this screen.

Table 4 Site Survey

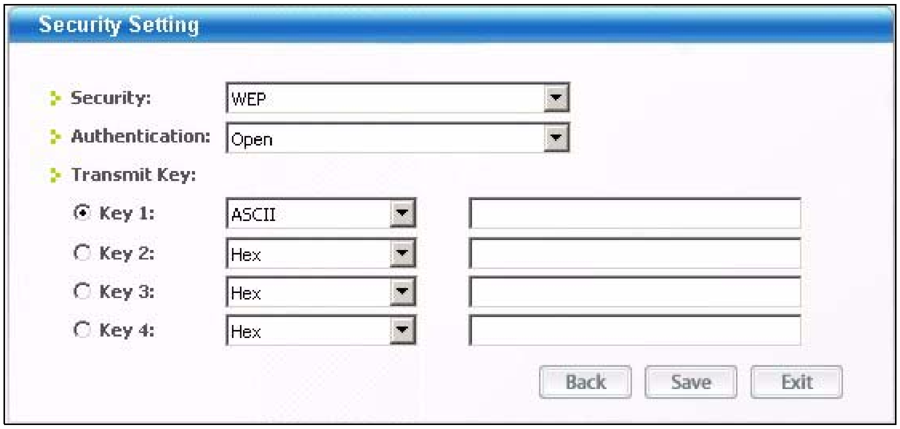
LABEL	DESCRIPTION
Available Network List	Click a column heading to sort the entries. Click an entry in the **Available Network List** table to display the information of the selected wireless device.
📡🔑 , 📡 , 💻🔑 or 💻	📡🔑 denotes that the wireless device is in infrastructure mode and the wireless security 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.
Channel	This field displays the channel number used by each wireless device.
Signal	This field displays the signal strength of each wireless device.
Network Type	This field displays the network type (**Infrastructure** or **Ad-hoc**) of the wireless device.
Security	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA**, **OPEN - Use 802.1X**, **WPA2**, **WPA2-PSK**) or inactive (**DISABLE**).
MAC Address	This field displays the MAC address of the wireless device.
	The text box under the available network table shows whether the G-210H is connected to a wireless network and to which network the G-210H is connected.
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. See Section 4.4 on page 40 for more information.

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 different on the G-210H, the screen varies according to the security mode used by the selected network.

4.3.1.1 WEP Encryption

Figure 17 Security Setting: WEP



Security Setting

Security: WEP

Authentication: Open

Transmit Key:

● Key 1: ASCII

○ Key 2: Hex

○ Key 3: Hex

○ Key 4: Hex

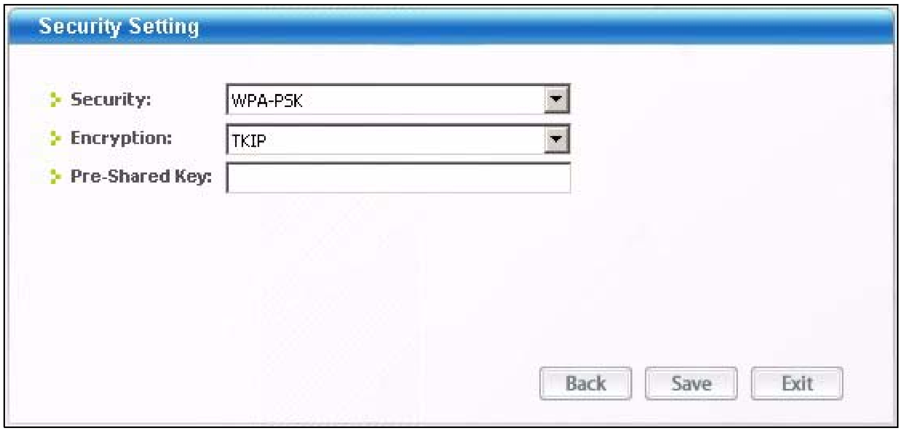
The following table describes the labels in this screen.

Table 5 Security Setting: WEP

LABEL	DESCRIPTION
Security Setting	
Security	Select **WEP** from the drop-down list.
Authentication	Select an authentication method. Choices are **Open** and **Shared**. Refer to Section 3.2.1.1.2 on page 26 for more information.
Transmit Key	Select a default WEP key to use for data encryption.
Key 1 ~ Key 4	The WEP keys are used to encrypt data. Both the G-210H and the AP or peer device must use the same WEP key for data transmission. Enter the WEP key in the field provided. If you select **Hex**, enter 10 or 26 hexadecimal characters in the range of “A-F”, “a-f” and “0-9” (for example, 11AA22BB33) for a 64-bit or 128-bit WEP key respectively. If you select **ASCII**, enter any 5 or 13 ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey) for a 64-bit or 128-bit WEP key respectively. Note: The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.
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 **Link Info** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.2 WPA-PSK/WPA2-PSK

Figure 18 Security Setting: WPA-PSK/WPA2-PSK



Security: WPA-PSK

Encryption: TKIP

Pre-Shared Key:

The following table describes the labels in this screen.

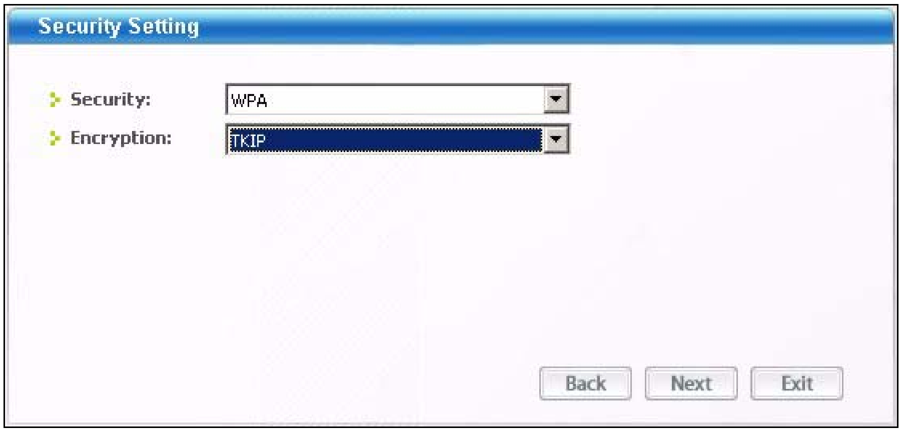
Table 6 Security Setting: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list.
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. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.1.3 on page 27 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 **Save** to confirm your selections and advance to the **Link Info** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.3 WPA/WPA2

4.3.1.3.1 Encryption

Figure 19 Security Setting: WPA/WPA2: Encryption



Security: WPA

Encryption: TKIP

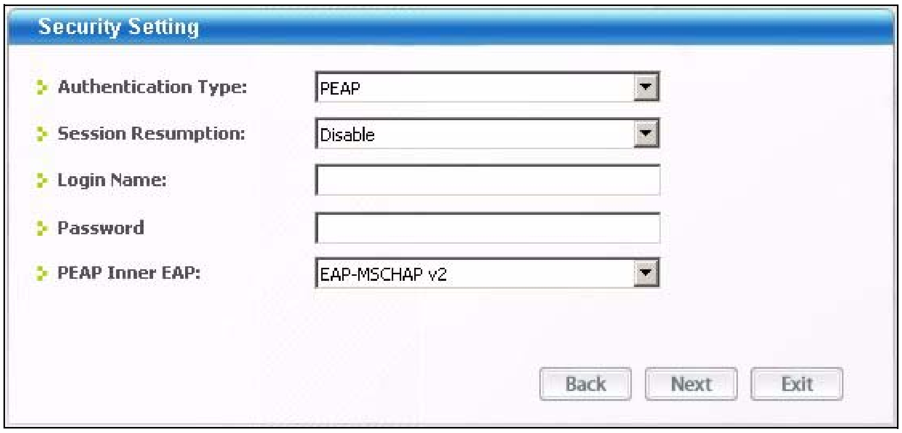
The following table describes the labels in this screen.

Table 7 Security Setting: WPA/WPA2: Encryption

LABEL	DESCRIPTION
Security	Select **WPA** or **WPA2** from the drop-down list.
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. Select the encryption type (**TKIP** or **AES**) for data encryption. Refer to Section 3.2.1.3 on page 27 for more information.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the next screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.3.2 Authentication

Figure 20 Security Setting: WPA/WPA2: Authentication



Authentication Type: PEAP

Session Resumption: Disable

Login Name:

Password

PEAP Inner EAP: EAP-MSCHAP v2

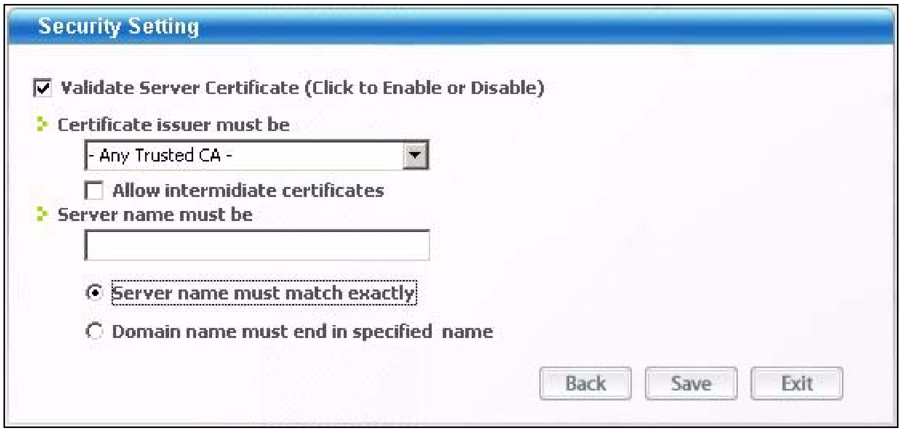
The following table describes the labels in this screen.

Table 8 Security Setting: WPA/WPA2: Authentication

LABEL	DESCRIPTION
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**.
Session Resumption	Select **Enable** to turn on session resumption (EAP fast re-authentication). This allows a client to attempt a fast reconnect to a server if the server and client have already established an identifier in a previous connection. The key was stored and full handshakes are not required. Otherwise, select **Disable** to turn off session resumption.
Login Name	Enter a user name. 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. Enter the password associated with the user name above.
Certification	This field is only available when you select **TLS** in the **Authentication Type** field. Specify the location and name of a certificate used by the authentication server to authenticate the G-210H. Otherwise, click **Change** to locate it. Note: You must first obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Change	This field is only available when you select **TLS** in the **Authentication Type** field. Click this button to display a screen where you can select a certificate and click **Apply**. If you didn't get the certificate first, no certificate displays in the screen.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. Select the PEAP method used by the RADIUS server or AP for client authentication. Options are **EAP-MS CHAP v2** or **EAP-TLS**.
TTLS Inner authentication	This field is only available when you select **TTLS** in the **Authentication Type** field. Select a TTLS protocol that the RADIUS server uses. Options are **CHAP**, **MS-CHAP**, **MS-CHAP-V2**, **PAP** and **EAP-MD5**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the next screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.3.3 Certificate

Figure 21 Security Setting: WPA/WPA2: Certificate



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 this screen.

Table 9 Security Setting: WPA/WPA2: Certificate

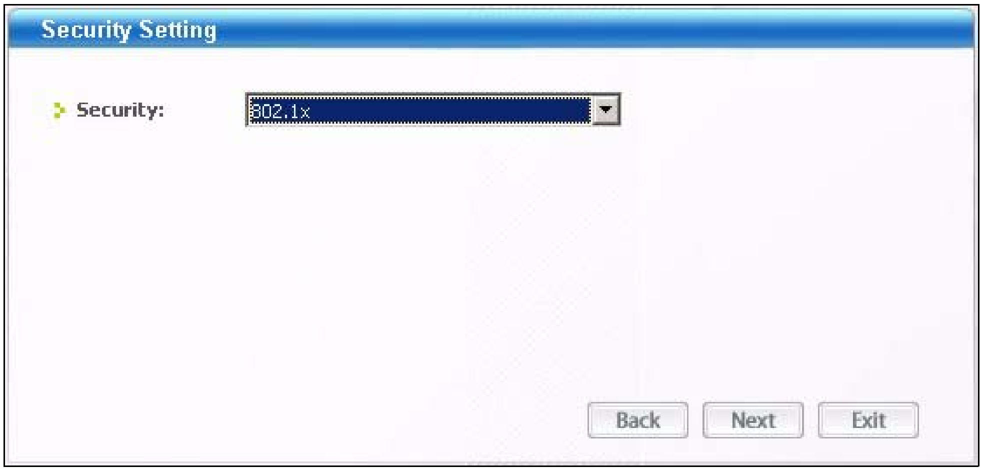
LABEL	DESCRIPTION
Validate Server Certificate	Select the check box to check the certificate of the authentication server. The fields below display only when the **Validate Server Certificate** check box is selected.
Certificate issuer must be	Select a trusted CA (certification authority) to accept only certificates signed by the selected CA or select **Any Trusted CA** to accept certificates signed by any CAs.
Allow intermediate certificates	Select the check box to accept an intermediate certificate which is issued by the Trusted Root CA.
Server name must be	Enter the name of the authentication server. You can use up to 19 English keyboard characters. Spaces are allowed.
Server name must match exactly	Select this option to allow only the authentication server whose server name is exactly the same as what you configured above.
Domain name must end in specified name	Select this option to allow only the authentication server whose domain name ends with what you configured above. For example, if you entered “org.com” in the **Server name must be** field, a server with the domain name of either abc.org.com or 123.org.com is allowed.
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 **Link Info** screen.
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.

4.3.1.4.1 Encryption

Figure 22 Security Setting: IEEE 802.1x: Encryption



Security Setting

Security: 802.1x

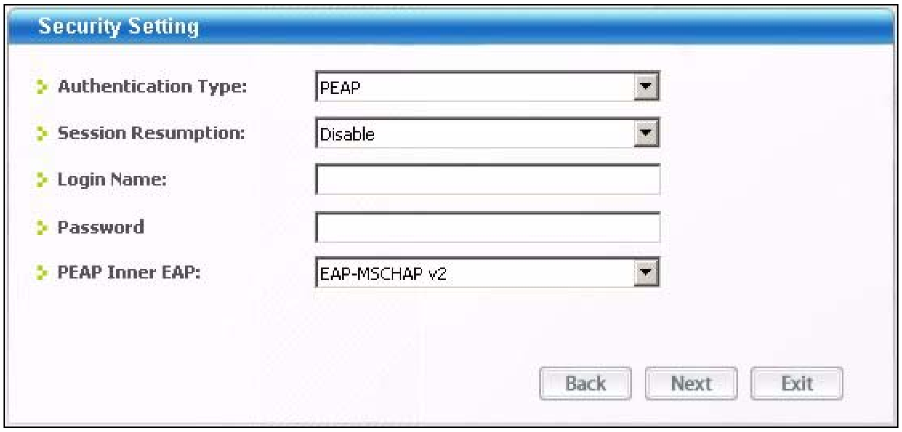
The following table describes the labels in this screen.

Table 10 Security Setting: IEEE 802.1x: Encryption

LABEL	DESCRIPTION
Security	Select **802.1x** from the drop-down list.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the next screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.4.2 Authentication

Figure 23 Security Setting: IEEE 802.1x: Authentication



Security Setting

Authentication Type: PEAP

Session Resumption: Disable

Login Name:

Password

PEAP Inner EAP: EAP-MSCHAP v2

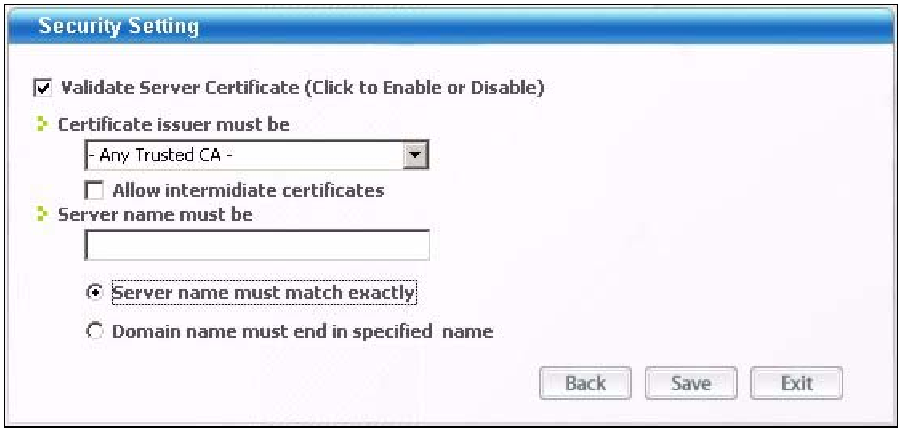
The following table describes the labels in this screen.

Table 11 Security Setting: IEEE 802.1x: Authentication

LABEL	DESCRIPTION
Authentication Type	The type of authentication you use depends on the RADIUS server or AP. Select an authentication method from the drop down list. Options are **TLS**, **TTLS** and **PEAP**.
Session Resumption	Select **Enable** to turn on session resumption (EAP fast re-authentication). This allows a client to attempt a fast reconnect to a server if the server and client have already established an identifier in a previous connection. The key was stored and full handshakes are not required. Otherwise, select **Disable** to turn off session resumption.
Login Name	Enter a user name. 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. Enter the password associated with the user name above.
Certification	This field is only available when you select **TLS** in the **Authentication Type** field. Specify the location and name of a certificate used by the authentication server to authenticate the G-210H. Otherwise, click **Change** to locate it. Note: You must first have and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Change	This field is only available when you select **TLS** in the **Authentication Type** field. Click this button to display a screen where you can select a certificate and click **Apply**. If you didn't get the certificate first, no certificate displays in the screen.
PEAP Inner EAP	This field is only available when you select **PEAP** in the **Authentication Type** field. Select the PEAP method used by the RADIUS server or AP for client authentication. Options are **EAP-MS CHAP v2** or **EAP-TLS**.
TTLS Inner authentication	This field is only available when you select **TTLS** in the **Authentication Type** field. Select a TTLS protocol that the RADIUS server uses. Options are **CHAP**, **MS-CHAP**, **MS-CHAP-V2**, **PAP** and **EAP-MD5**.
Back	Click **Back** to go to the **Site Survey** screen to select and connect to another network.
Next	Click **Next** to confirm your selections and advance to the next screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.3.1.4.3 Certificate

Figure 24 Security Setting: IEEE 802.1x: Certificate



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 this screen.

Table 12 Security Setting: IEEE 802.1x: Certificate

LABEL	DESCRIPTION
Validate Server Certificate	Select the check box to check the certificate of the authentication server. The fields below display only when the **Validate Server Certificate** check box is selected.
Certificate issuer must be	Select a trusted CA (certification authority) to accept only certificates signed by the selected CA or select **Any Trusted CA** to accept certificates signed by any CAs.
Allow intermediate certificates	Select the check box to accept an intermediate certificate which is issued by the Trusted Root CA.
Server name must be	Enter the name of the authentication server. You can use up to 19 English keyboard characters. Spaces are allowed.
Server name must match exactly	Select this option to allow only the authentication server whose server name is exactly the same as what you configured above.
Domain name must end in specified name	Select this option to allow only the authentication server whose domain name ends with what you configured above. For example, if you entered “org.com” in the **Server name must be** field, a server with the domain name of either abc.org.com or 123.org.com is allowed.
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 **Link Info** screen.
Exit	Click **Exit** to return to the **Site Survey** screen without saving.

4.4 The Profile Screen

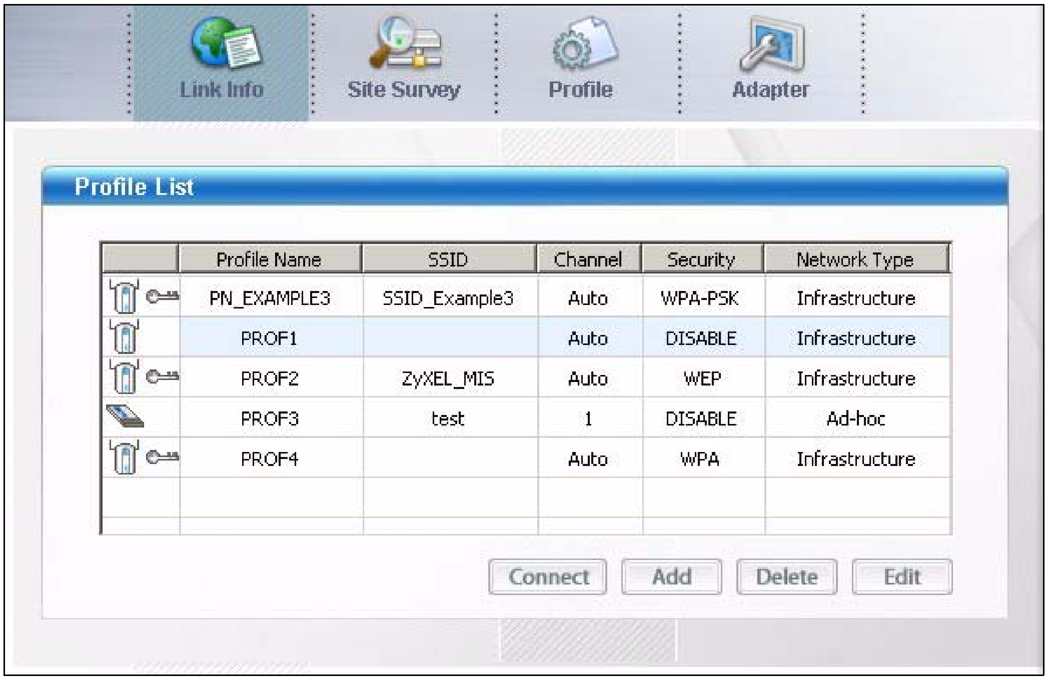
A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the G-210H, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available,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

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 25 Profile



	Profile Name	SSID	Channel	Security	Network Type
	PN_EXAMPLE3	SSID_Example3	Auto	WPA-PSK	Infrastructure
	PROF1		Auto	DISABLE	Infrastructure
	PROF2	ZyXEL_MIS	Auto	WEP	Infrastructure
	PROF3	test	1	DISABLE	Ad-hoc
	PROF4		Auto	WPA	Infrastructure

The following table describes the labels in this screen.

Table 13 Profile

LABEL	DESCRIPTION
Profile List	Click a column heading to sort the entries.
, , or	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 associates.
Channel	This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA**, **OPEN - Use 802.1X**, **WPA2**, **WPA2-PSK**) or inactive (**DISABLE**).
Network Type	This field displays the network type (**Infrastructure** or **Ad-hoc**) of the profile.
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**.

Table 13 Profile (continued)

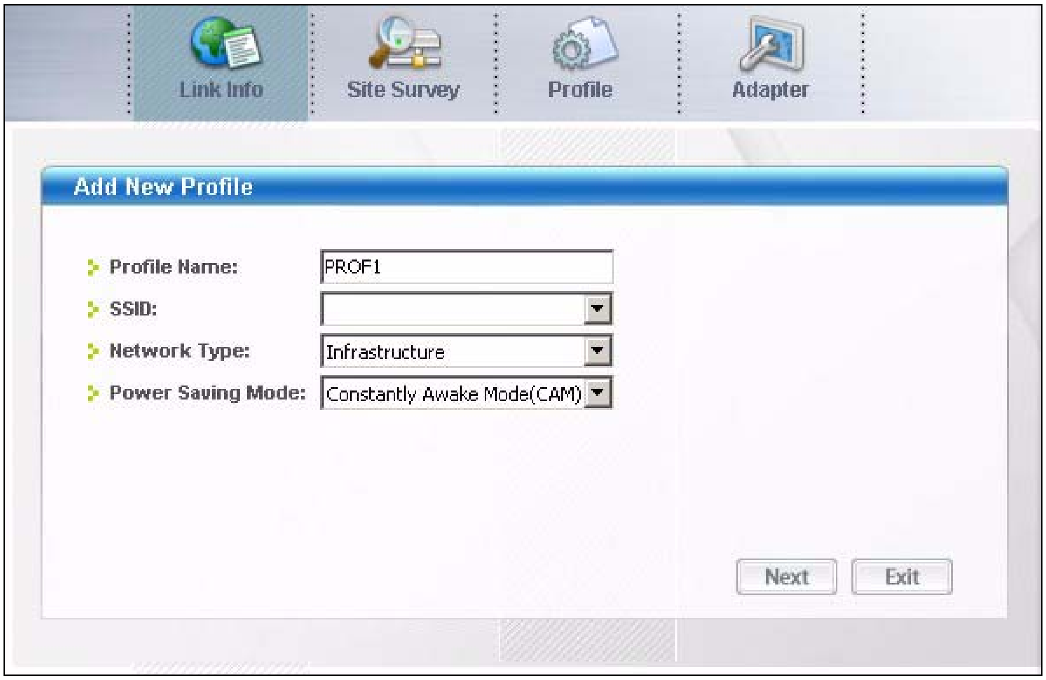
LABEL	DESCRIPTION
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.

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. The screen varies slightly depending on the network type you selected.

Figure 26 Profile: Add a New Profile



Profile Name: PROF1
SSID:
Network Type: Infrastructure
Power Saving Mode: Constantly Awake Mode(CAM)

The following table describes the labels in this screen.

Table 14 Profile: Add a New Profile

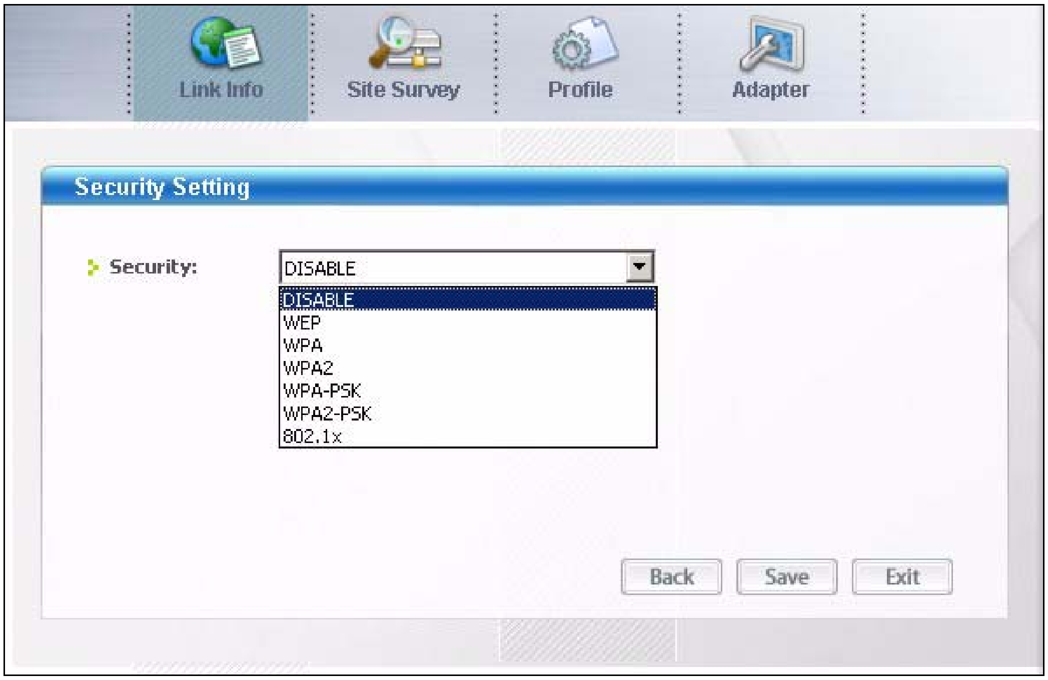
LABEL	DESCRIPTION
Add New Profile	
Profile Name	Enter a descriptive name in this field.
SSID	Select an available wireless device from the drop-down list box, or enter the SSID of the wireless device to which you want to associate in this field manually.
Network Type	Select **Infrastructure** to associate to an AP. Select **Ad-Hoc** to associate to a peer computer.

Table 14 Profile: Add a New Profile (continued)

LABEL	DESCRIPTION
Power Saving Mode	This field is available only when you select **Infrastructure** in the **Network Type** field. Select **Constantly Awake Mode (CAM)** to disable power saving and the G-210H will never go to sleep mode. Select **Power Saving Mode** to save power (especially for notebook computers). This forces the G-210H to go to sleep mode when it is not transmitting data.
Preamble	This field is available only when you select **Ad-hoc** in the **Network Type** field. Preamble is used to signal that data is coming to the receiver. Select the preamble type that the peer device uses. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support **Long Preamble**, but not all support short preamble. Select **Auto** to have the G-210H automatically use short preamble when all wireless stations support it; otherwise the G-210H uses long preamble. Note: The G-210H and the peer device MUST use the same preamble mode in order to communicate.
Channel	This field is available only when you select **Ad-hoc** in the **Network Type** field. Select a channel number. Note: To associate to an ad-hoc network, you must use the same channel as the peer device.
Next	Click **Next** to go to the next screen.
Exit	Click **Exit** to go back to the previous screen without saving.

2 If you select **Infrastructure** network type in the first screen, select **WEP**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2** or **802.1x** from the drop-down list box to enable data encryption. If you select **Ad-hoc** network type in the first screen, you can only use **WPA-NONE** or **WEP** encryption method. Otherwise, select **DISABLE** to allow the G-210H to communicate with the access points or other peer wireless computers without any data encryption and skip to step 4.

Figure 27 Profile: Security Settings



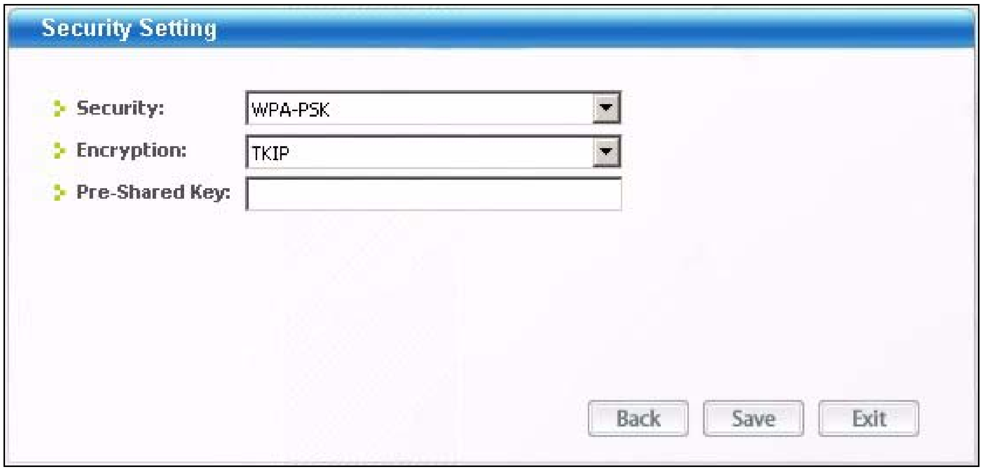
Security Setting

Security: DISABLE

DISABLE
WEP
WPA
WPA2
WPA-PSK
WPA2-PSK
802.1x

3 The screen varies depending on the encryption method you selected 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 32 for detailed information on wireless security configuration.

Figure 28 Profile: Security Settings



Security Setting

Security: WPA-PSK

Encryption: TKIP

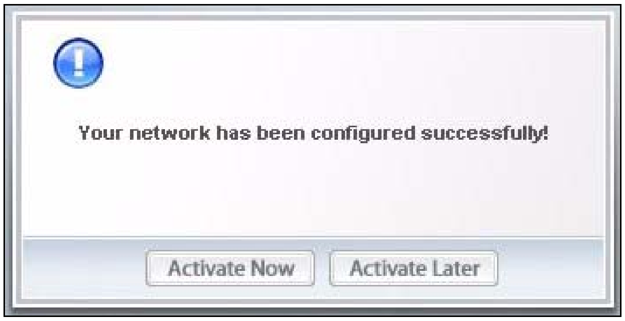
Pre-Shared Key:

4 Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen. Otherwise, click **Exit** to go back to the **Profile** screen without saving.

5 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.

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

Figure 29 Profile: Activate the Profile

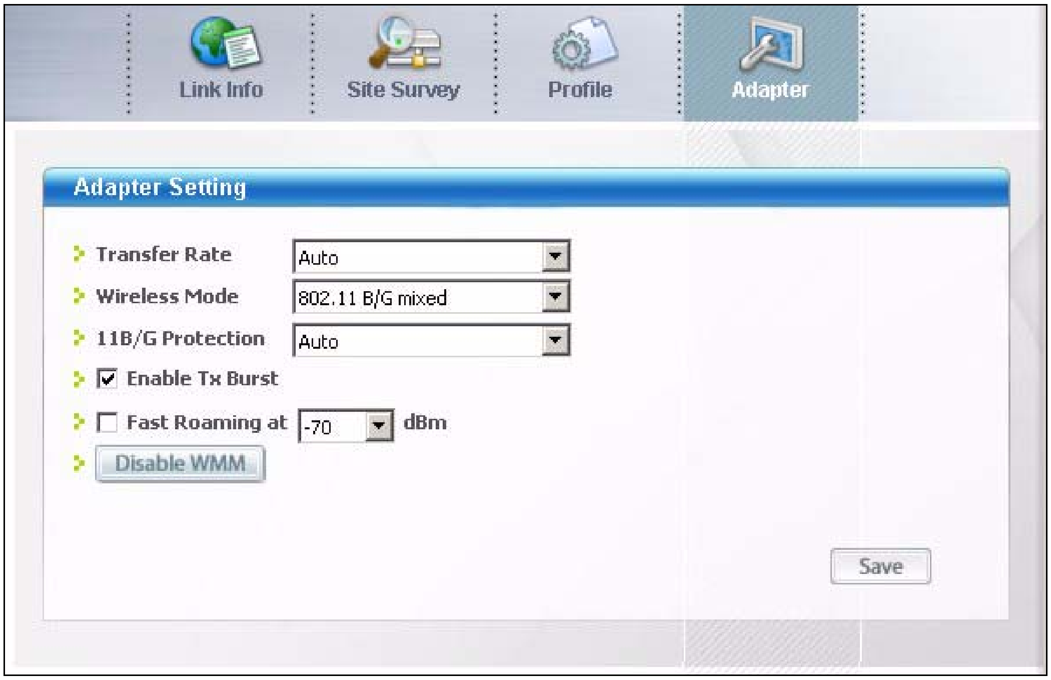


Your network has been configured successfully!

4.5 The Adapter Screen

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

Figure 30 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.

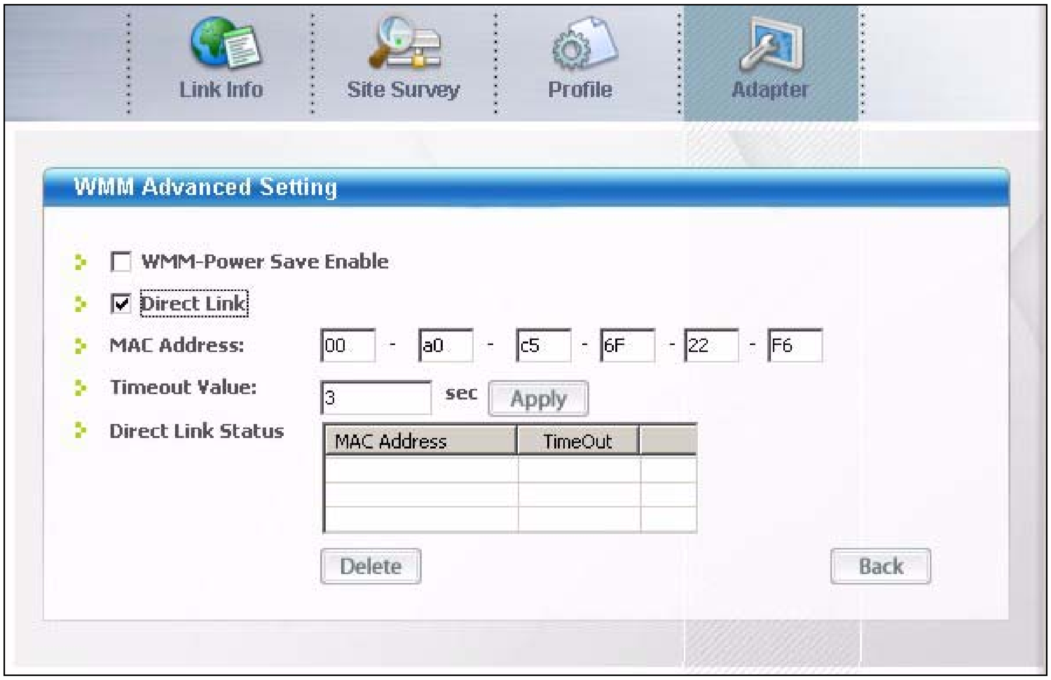
Table 15 Adapter

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. If you want to select a specific transmission rate, select one that the AP or peer wireless device supports.
Wireless Mode	Select **802.11 B/G mixed** to have the G-210H connect to either an IEEE 802.11g or IEEE 802.11b wireless device. Select **802.11 B only** to have the G-210H connect to an IEEE 802.11b wireless device only.
11B/G Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the G-210H send an RTS (Request to Send) message to the AP and wait for AP's CTS (Clear to Send) response before transmitting data when the G-210H is connecting to an AP with this feature enabled. Select **On** to have the G-210H always transmit data after a RTS/CTS handshake even when the G-210H is connecting to an AP with this feature disabled. Select **Off** to disable 11B/G protection.
Enable Tx Burst	Select the check box to increase the throughput and improve transmission speed. This only works when an AP or peer device supports this function.
Fast Roaming at	When the signal strength is too low, you may want to connect to a closer AP. Fast roaming allows you to connect to the closer AP without interrupting the wireless connection. Select the check box to enable fast roaming at the specified transmitting power. The G-210H will enter roaming mode when dBm reaches a certain level.
Disable WMM/ Enable WMM	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services. To do this, you must enable WMM QoS on all wireless devices in your network. Click **Disable WMM** to deactivate WMM QoS on the G-210H. Click **Enable WMM** to activate WMM QoS on the G-210H and display the **WMM Advanced Setting** screen.
Save	Click **Save** to save the changes to the G-210H.

4.5.1 WMM Advanced Setting

Click **Enable WMM** in the **Adapter** screen to configure advanced WMM settings.

Figure 31 Adapter: WMM Advanced Setting



WMM Advanced Setting

□ WMM-Power Save Enable

☑ Direct Link

MAC Address: 00 - a0 - c5 - 6F - 22 - F6

Timeout Value: 3 sec

Direct Link Status

MAC Address	TimeOut

The following table describes the labels in this screen.

Table 16 Adapter: WMM Advanced Setting

LABEL	DESCRIPTION
WMM-Power Save Enable	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The G-210H goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the G-210H till the G-210H "wakes up". The G-210H wakes up periodically to check for incoming data. Note: This works only if the wireless device to which the G-210H is connected also supports this feature.
Direct Link	Select this option to enable DLS (Direct Link Setup) on the G-210H. If there are two DLS-enabled devices in the same wireless network, this allows the two devices to communicate with each other directly. The packets will not go through the AP and can increase throughput. You need to enter the peer device's MAC address in this screen. The G-210H can associate with up to four DLS clients at a time, but you can only enter one device's MAC address in the G-210H's utility. To have the G-210H set up a second DLS connection, enter the G-210H's MAC address in another peer device. Note: This feature is applicable only when the G-210H is in Infrastructure mode and the connected AP or wireless router is also DLS-enabled.
MAC Address	Enter the MAC address of the peer device that supports DLS.
Timeout Value	Enter the time in seconds (from 1 to 65535) for the G-210H to wait before it automatically disconnects from the peer device when there is no traffic between them.
Apply	Click **Apply** to save your changes in this section.
Direct Link Status	

Table 16 Adapter: WMM Advanced Setting (continued)

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the DLS-enabled device to which the G-210H is connecting directly.
TimeOut	This field displays the timeout value.
Delete	Select an entry and click **Delete** to remove it from the table.
Back	Click **Back** to return to the **Adapter** screen.

5

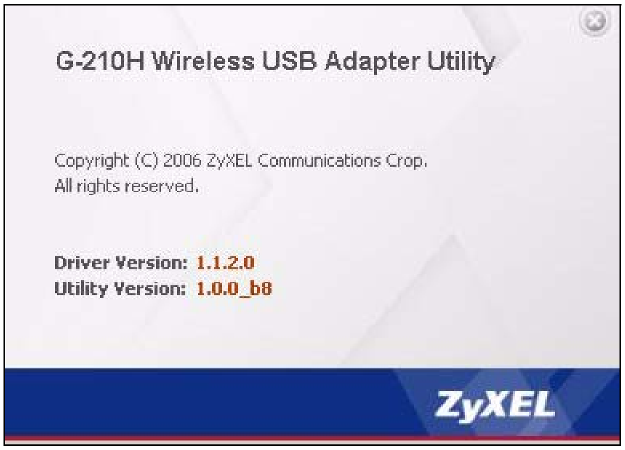
Maintenance

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 as shown below, click the about (▤) button.

Figure 32 About



G-210H Wireless USB Adapter Utility

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

Driver Version: 1.1.2.0
Utility Version: 1.0.0_b8

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

Table 17 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

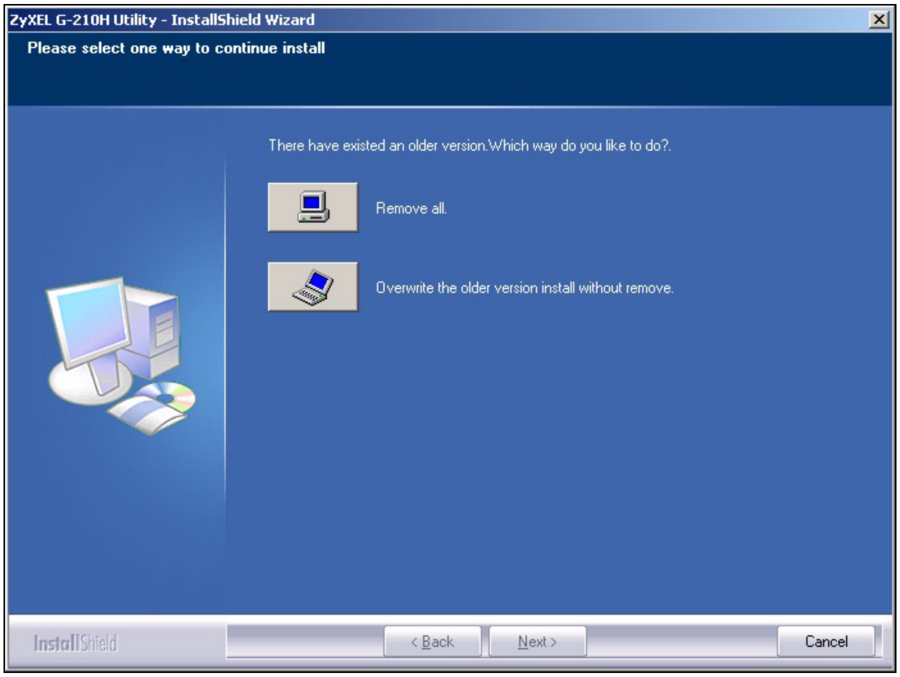
Follow the steps below to remove (or uninstall) the ZyXEL utility from your computer.

5.2.1 Windows

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

2 When prompted, click **Remove all** to remove the driver and the utility software.

Figure 33 Windows: Uninstall: Confirm



ZyXEL G-210H Utility - InstallShield Wizard

Please select one way to continue install

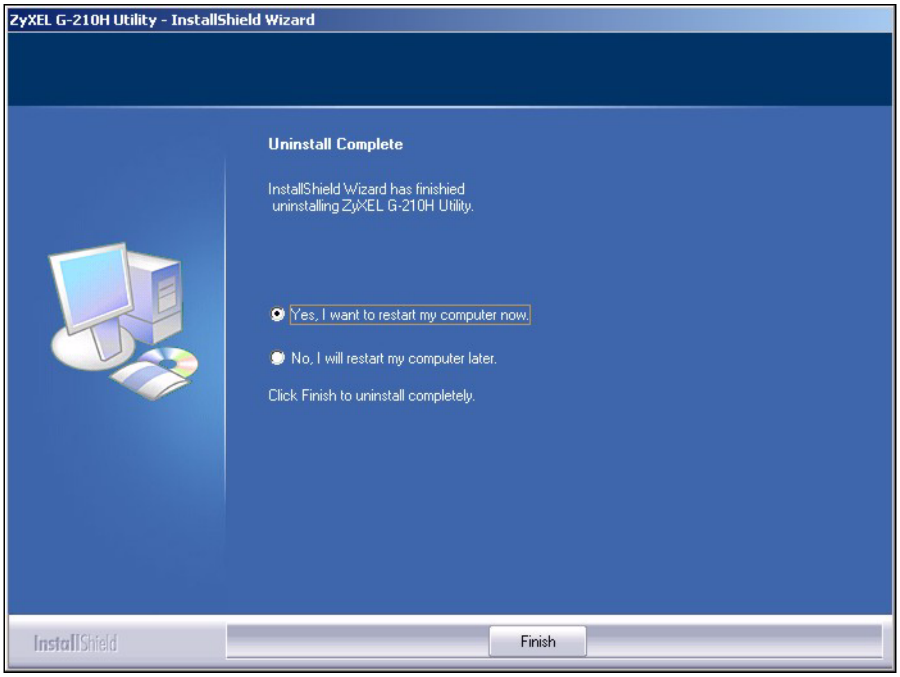
There have existed an older version.Which way do you like to do?.

Remove all.

Overwrite the older version install without remove.

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

Figure 34 Windows: Uninstall: Finish



ZyXEL G-210H Utility - InstallShield Wizard

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.

5.2.2 Macintosh

1 Insert the included CD into the CD-ROM drive. An icon for the CD appears.

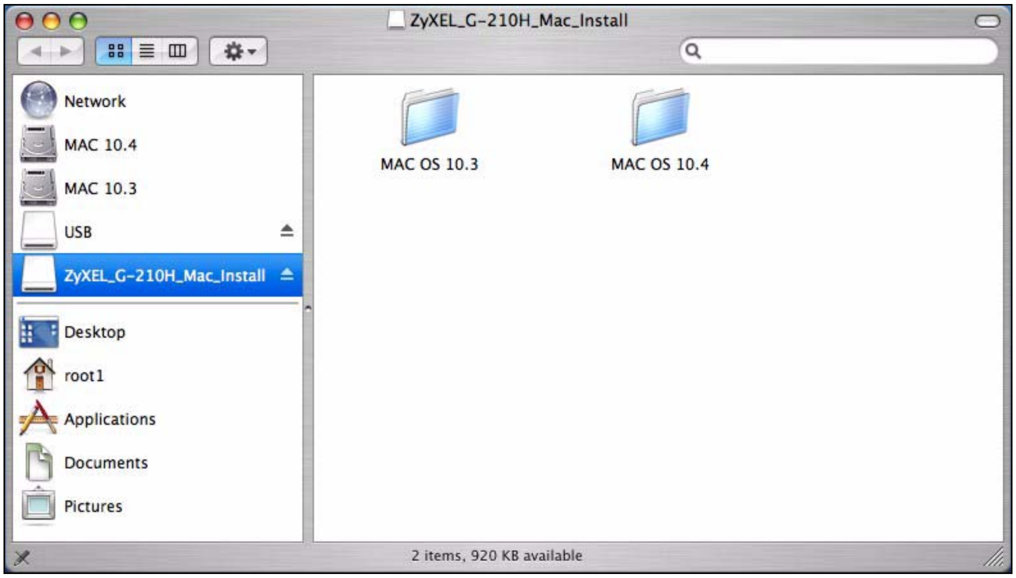
2 Double-click the CD's icon.

3 Double-click the **Mac Driver** folder.

4 Double-click the .dmg file.

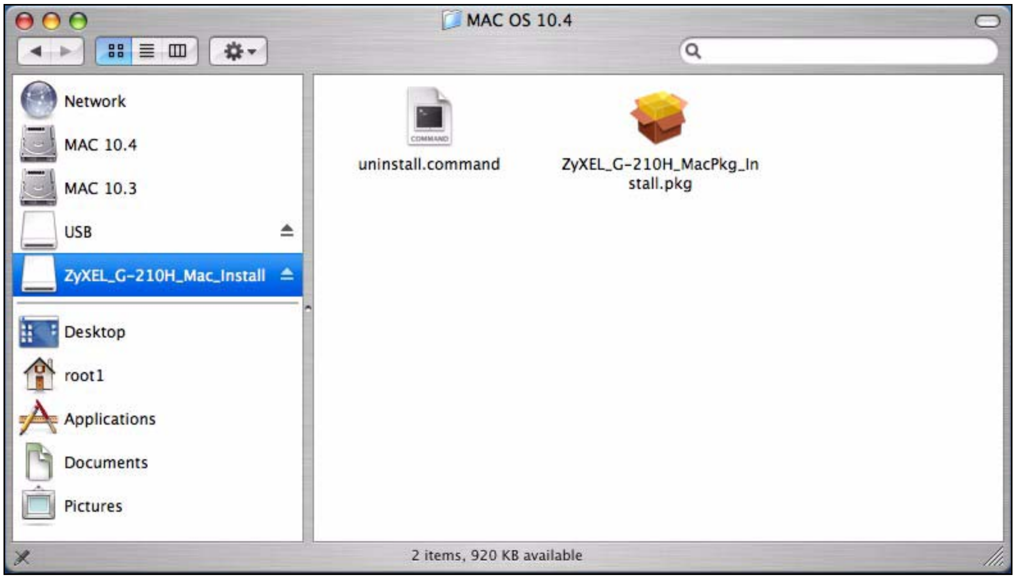
5 Double-click your Macintosh OS's driver folder. The .command and .pkg files will be created.

Figure 35 Mac OS 10.4: Driver folder



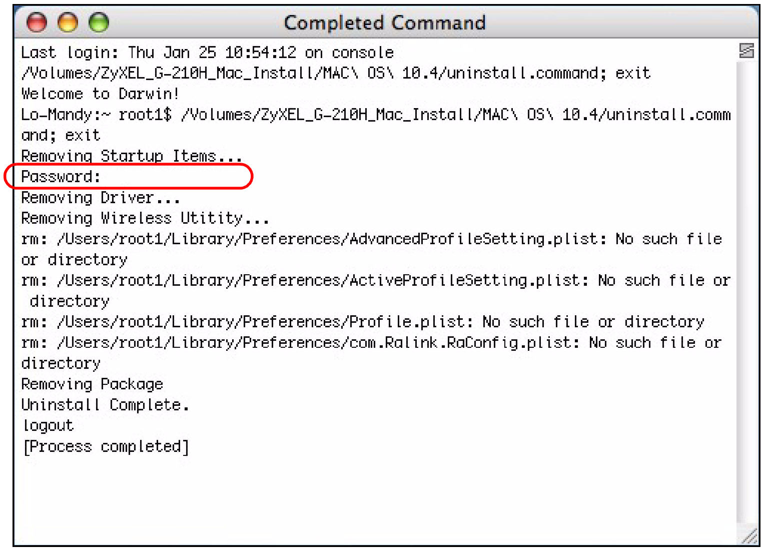
6 Double-click the file **uninstall.command**.

Figure 36 MAC OS 10.4: Uninstall command



7 The command screen displays. Enter the administrative password you use to log in to the Mac computer and press [ENTER].

Figure 37 Mac OS 10.4: Uninstall command completed



```
Last login: Thu Jan 25 10:54:12 on console
/Volumes/ZyXEL_G-210H_Mac_Install/MAC\ OS\ 10.4/uninstall.command; exit
Welcome to Darwin!
Lo-Mandy:~ root1$ /Volumes/ZyXEL_G-210H_Mac_Install/MAC\ OS\ 10.4/uninstall.comm
and; exit
Removing Startup Items...
Password:
Removing Driver...
Removing Wireless Utitity...
rm: /Users/root1/Library/Preferences/AdvancedProfileSetting.plist: No such file
or directory
rm: /Users/root1/Library/Preferences/ActiveProfileSetting.plist: No such file or
 directory
rm: /Users/root1/Library/Preferences/Profile.plist: No such file or directory
rm: /Users/root1/Library/Preferences/com.Ralink.RaConfig.plist: No such file or
directory
Removing Package
Uninstall Complete.
logout
[Process completed]
```

5.3 Upgrading the ZyXEL Utility

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 49 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.

6

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

? The ZyXEL utility icon does not display.

1 If you install the Funk Odyssey Client software on the computer, uninstall (remove) both the Funk Odyssey Client software and ZyXEL utility, and then install the ZyXEL utility again after restarting the computer.

? I Cannot start the ZyXEL utility.

1 Make sure the G-210H is properly inserted and the LEDs (lights) are on.

2 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)

3 Install the G-210H in another computer.

4 If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.

? The link quality and/or signal strength is poor all the time.

1 Search and connect to another AP with a better link quality using the **Site Survey** screen.

2 Move your computer closer to the AP or the peer computer(s) within the transmission range.

3 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.

4 Make sure there are not too many wireless stations connected to a wireless network.

The computer with the G-210H installed cannot communicate with the other computer(s).

In Infrastructure Mode

1 Make sure that the AP and the associated computers are turned on and working properly.

2 Make sure the G-210H computer and the associated AP use the same SSID.

3 Change the AP and the associated wireless clients to use another radio channel if interference is high.

4 Make sure that the computer and the AP share the same security option and key. Verify the settings in the **Profile Security Setting** screen.

5 If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.

In Ad-Hoc (IBSS) Mode

1 Verify that the peer computer(s) is turned on.

2 Make sure the G-210H computer and the peer computer(s) are using the same SSID and channel.

3 Make sure that the computer and the peer computer(s) share the same security settings.

4 Change the wireless clients to use another radio channel if interference is high.

A

Product Specifications

Table 18 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	ZyXEL G-210H 802.11b/g Wireless USB Adapter
Interface	USB 2.0 compatible
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Temperature	0 ~ 45 degrees Centigrade
Storage Temperature	-30 ~ 70 degrees Centigrade
Operating Humidity	90% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Voltage	5 V
Weight	34.5 g
Dimension	(W) 35 mm × (L) 111 mm × (H) 12 mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.11
Operating Frequencies	IEEE 802.11b: 2.412~2.462GHz IEEE 802.11g: 2.412~2.462GHz
Operating Channels	IEEE 802.11b: 11 Channels (North America and Taiwan) IEEE 802.11g: 11 Channels (North America and Taiwan) IEEE 802.11b: 13 Channels (Europe) IEEE 802.11g: 13 Channels (Europe)
Data Rate	IEEE 802.11b: 11, 5.5, 2, 1Mbps IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802311b: PBCC, Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK). IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK)
Output Power (Average)	IEEE 802.11b: 18 dBm at 11 Mbps CCK, QPSK, BPSK IEEE 802.11g: 15 dBm at 54 Mbps OFDM
RX Sensitivity	54 Mbps (OFDM): < -85 dBm 11 Mbps (CCK): < -69 dBm
SOFTWARE SPECIFICATIONS	
Device Drivers	Windows 2000, Windows XP, Windows Vista, Mac OS 10.3 or later

Table 18 Product Specifications (continued)

ZyXEL Utility	ZyXEL Wireless Configuration Tool
Security	64/128-bit WEP WPA/WPA-PSK/WPA2/WPA2-PSK WPA-None (Ad-Hoc mode) IEEE 802.1x

B

Management with Wireless Zero Configuration

This appendix shows you how to manage your G-210H using the Windows XP wireless zero configuration tool.

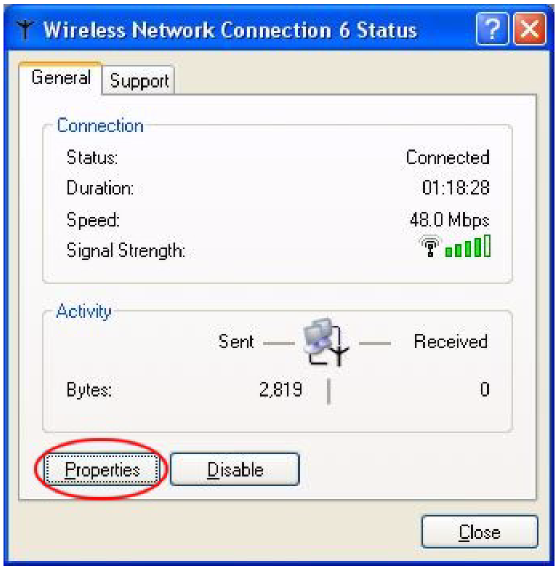
Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

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 Wireless Zero Configuration

1. Click **Start**, **Control Panel** and double-click **Network Connections**.
2. Double-click on the icon for wireless network connection.
3. The status window displays as shown below. Click **Properties**.

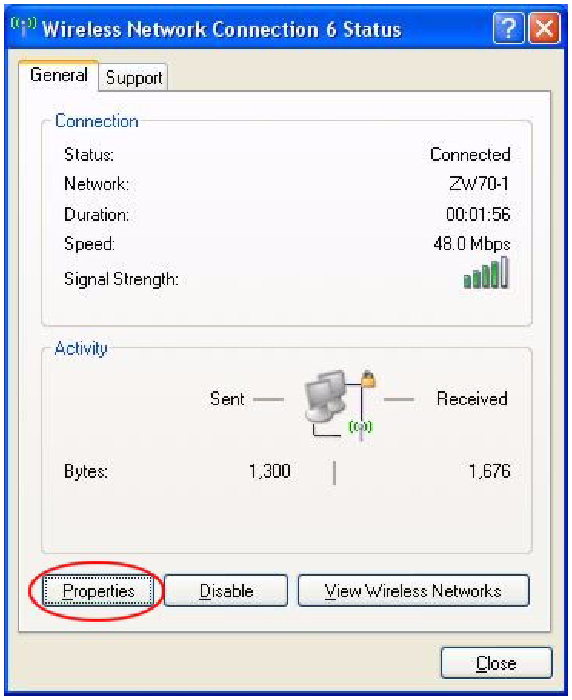
Figure 38 Windows XP SP1: Wireless Network Connection Status



Status: Connected
Duration: 01:18:28
Speed: 48.0 Mbps
Signal Strength:

Bytes: 2,819 | 0

Figure 39 Windows XP SP2: Wireless Network Connection Status



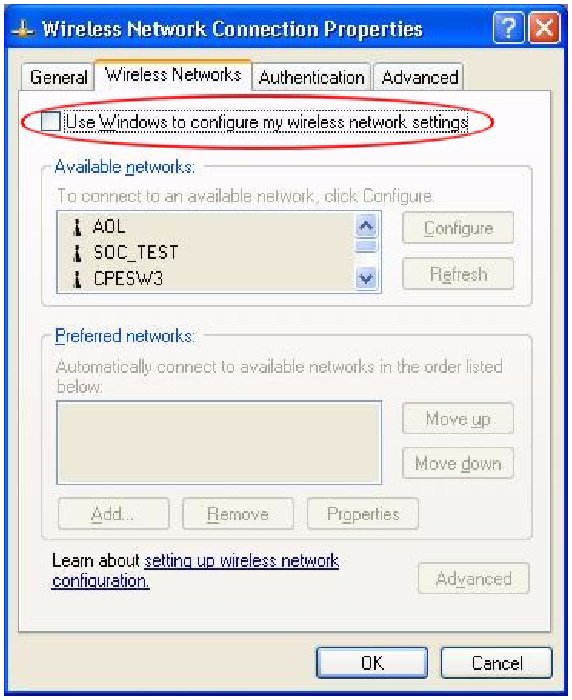
Status: Connected
Network: ZW70-1
Duration: 00:01:56
Speed: 48.0 Mbps
Signal Strength:

Bytes: 1,300 | 1,676

4 The **Wireless Network Connection Properties** screen displays. Click the **Wireless Networks** tab.

Make sure the **Use Windows to configure my wireless network settings** check box is selected.

Figure 40 Windows XP SP1: Wireless Network Connection Properties



□ Use Windows to configure my wireless network settings

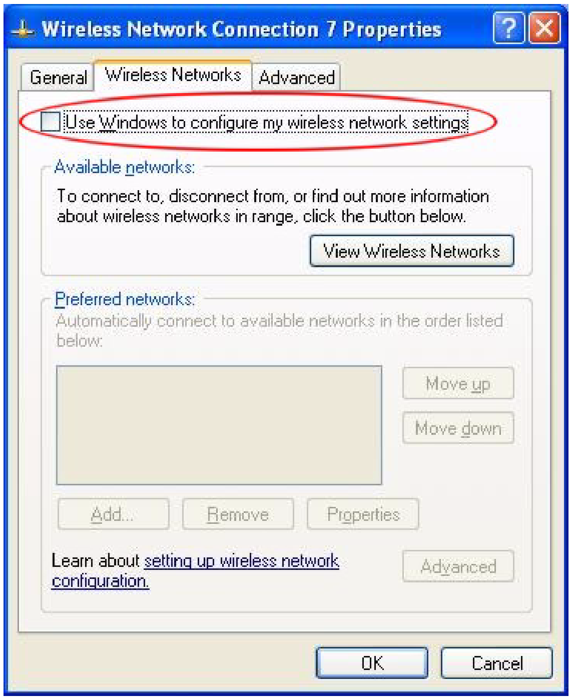
To connect to an available network, click Configure.

AOL
SOC_TEST
CPESW3

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

Figure 41 Windows XP SP2: Wireless Network Connection Properties



Wireless Network Connection 7 Properties

☐ 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.

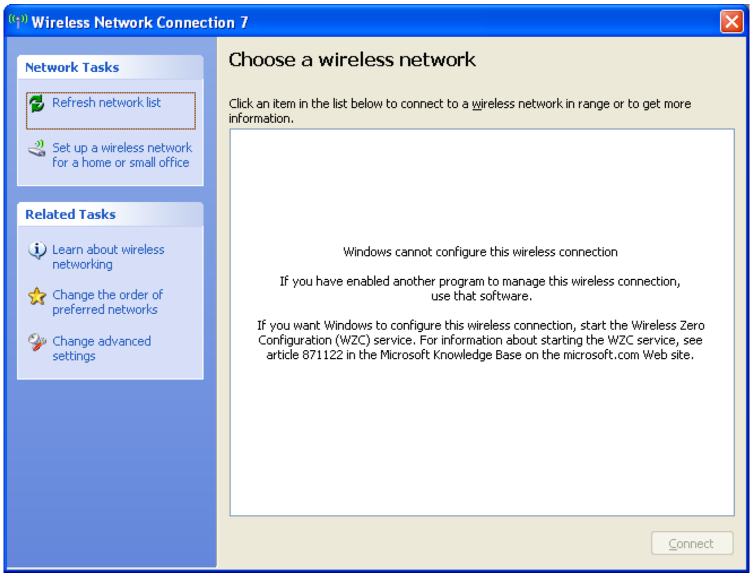
Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

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

Figure 42 Windows XP SP2: WZC Not Available



Wireless Network Connection 7

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.

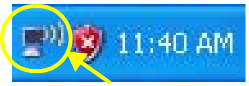
If you want Windows to configure this wireless connection, start the Wireless Zero Configuration (WZC) service. For information about starting the WZC service, see article 871122 in the Microsoft Knowledge Base on the microsoft.com Web site.

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

Connecting to a Wireless Network

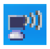
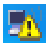
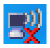
1 Double-click the network icon for wireless connections in the system tray to open the **Wireless Network Connection Status** screen.

Figure 43 Windows XP SP2: System Tray Icon



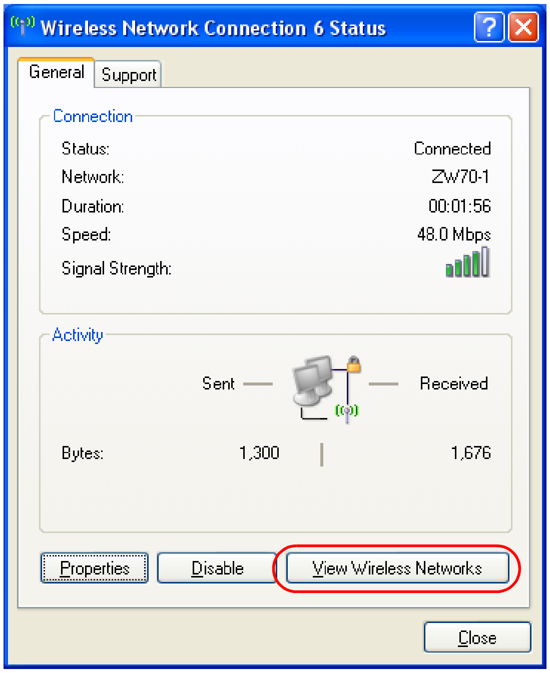
The type of the wireless network icon in Windows XP SP2 indicates the status of the G-210H. Refer to the following table for details.

Table 19 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 44 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:

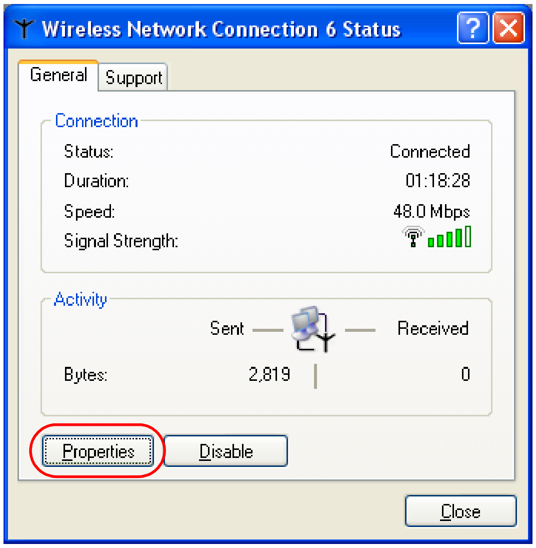
Activity

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 45 Windows XP SP1: Wireless Network Connection Status



Wireless Network Connection 6 Status

General | Support

Connection

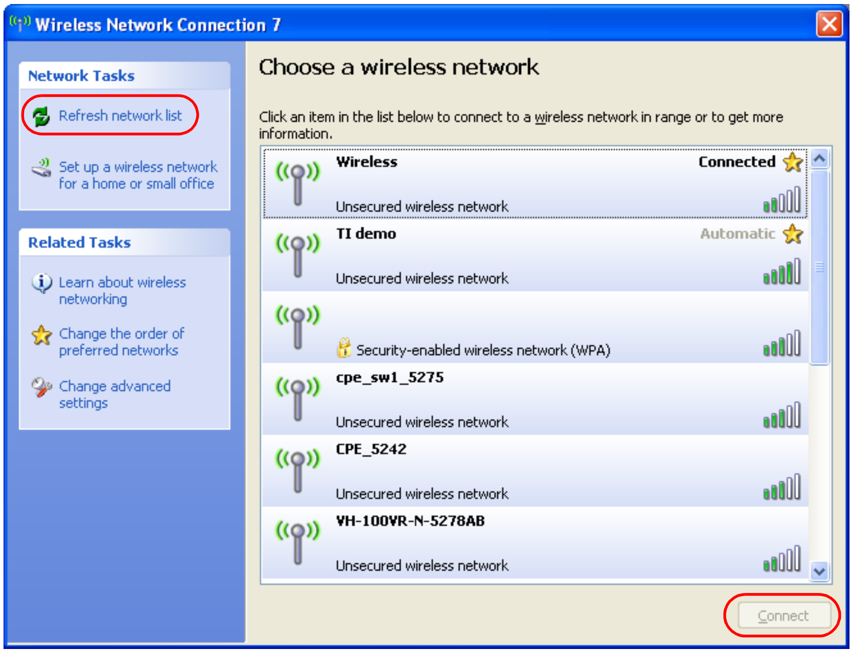
Status:	Connected
Duration:	01:18:28
Speed:	48.0 Mbps
Signal Strength:	

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 46 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	Unsecured wireless network	Connected ☆
TI demo	Unsecured wireless network	Automatic ☆
	Security-enabled wireless network (WPA)	
cpe_sw1_5275	Unsecured wireless network	
CPE_5242	Unsecured wireless network	
VH-100VR-N-5278AB	Unsecured wireless network	

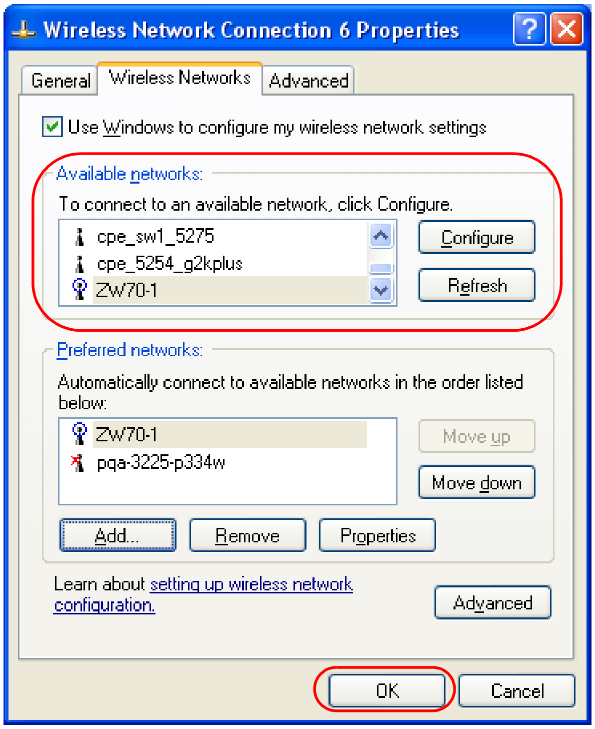
The following table describes the icons in the wireless network list.

Table 20 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. 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 47 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

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

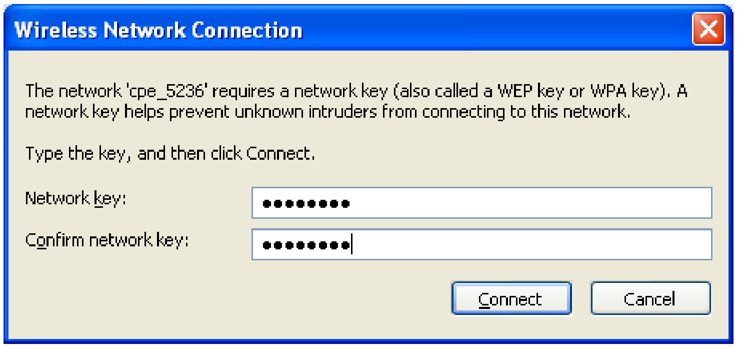
Learn about setting up wireless network configuration.

Advanced

OK | Cancel

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 48 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK



Wireless Network Connection

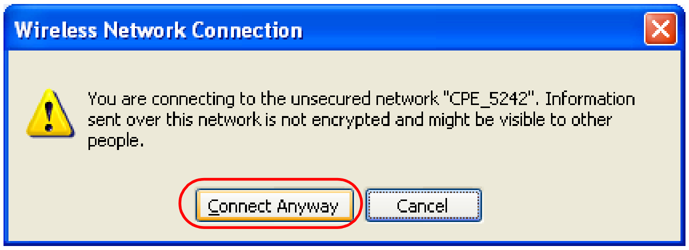
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Figure 49 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 21 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.

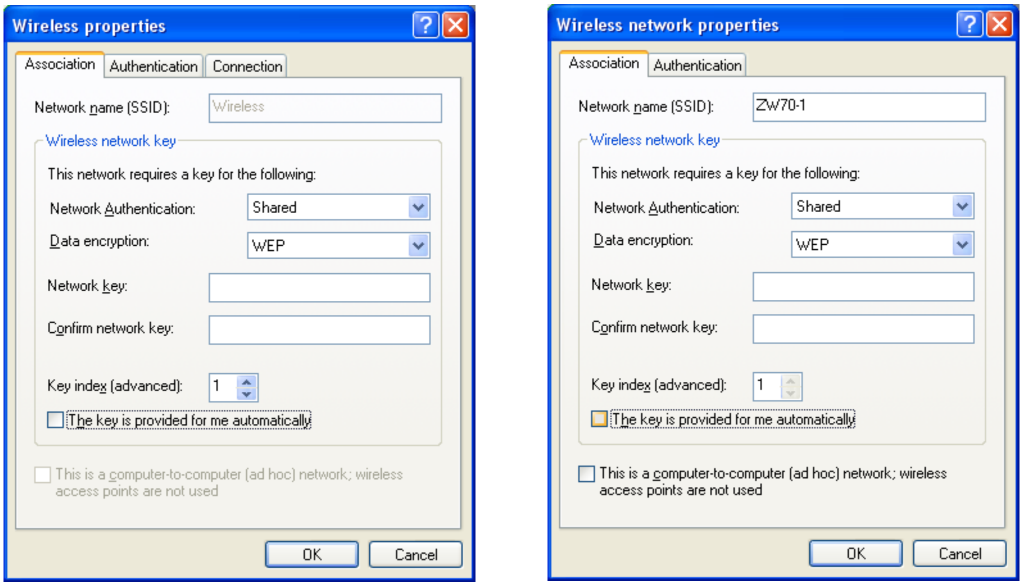
Security Settings

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 50 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.

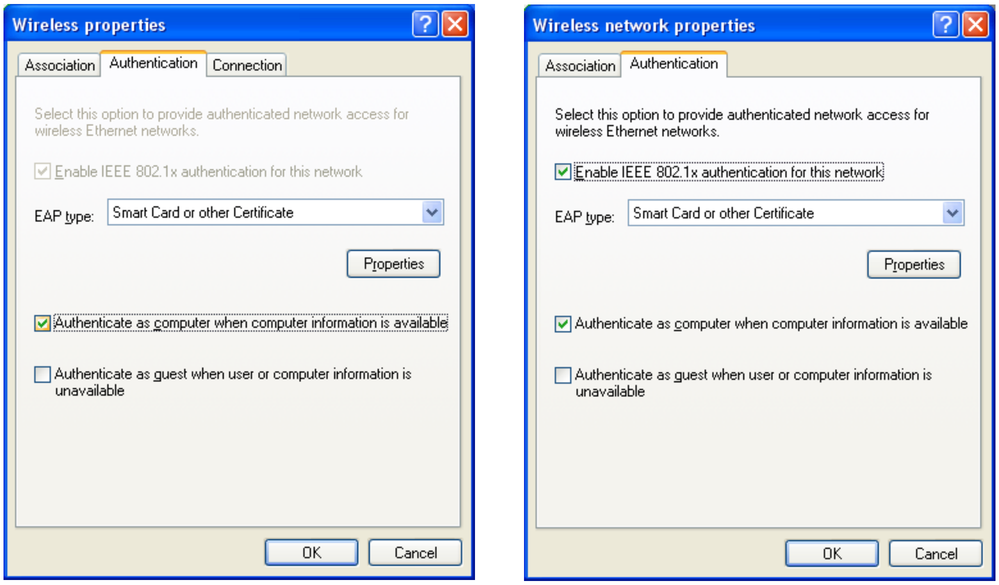
Table 22 Windows XP: Wireless (network) properties: Association

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** or **WPA-PSK**) used by the selected network.
Data Encryption	This field automatically shows the encryption type (**TKIP**, **WEP** or **Disable**) used by the selected network.
Network Key	Enter the pre-shared key or WEP key. 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. 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 51 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 23 Windows XP: Wireless (network) properties: Authentication

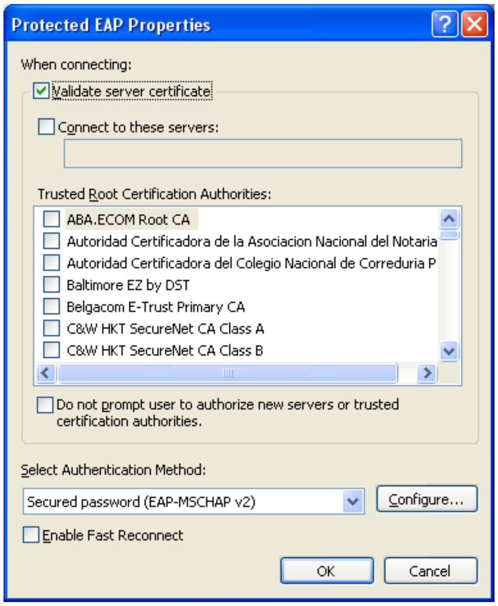
LABEL	DESCRIPTION
Enable IEEE 802.1x authentication for this network	This field displays whether the IEEE 802.1x authentication is active. If the network authentication is set to **Open** in the previous screen, you can choose to disable or enable this feature.
EAP Type	Select the type of EAP authentication. 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 52 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 24 Windows XP: Protected EAP Properties

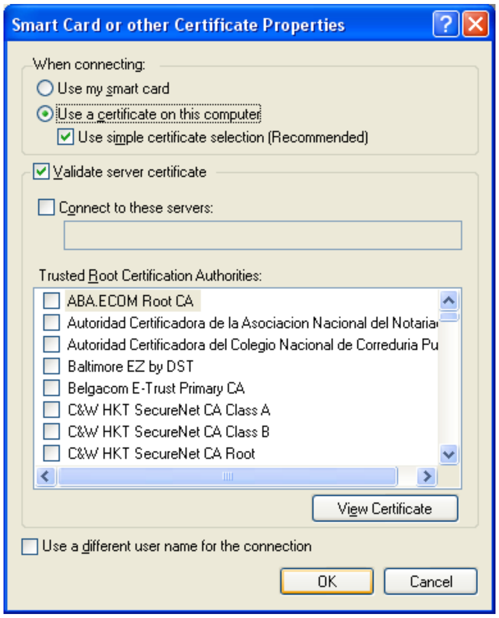
LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. 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. 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.
Enable Fast Reconnect	Select the check box to automatically reconnect to the network (without re-authentication) if the wireless connection goes down.

Table 24 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
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 53 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

View Certificate

□ Use a different user name for the connection

OK Cancel

The following table describes the labels in this screen.

Table 25 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. 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.
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.

Table 25 Windows XP: Smart Card or other Certificate Properties

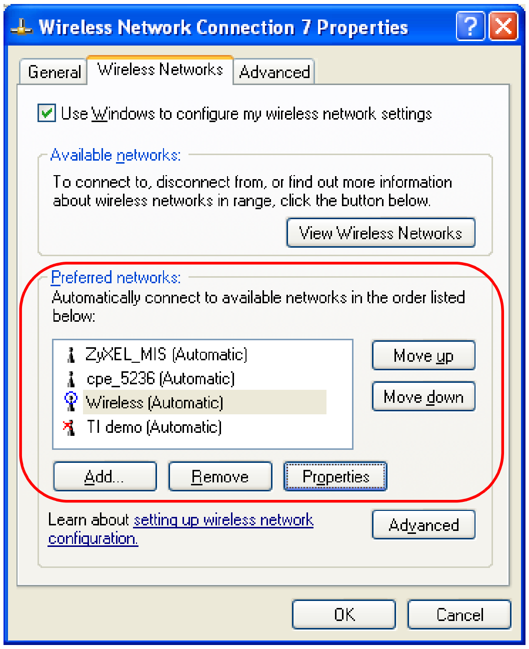
LABEL	DESCRIPTION
OK	Click **OK** to save your changes.
Cancel	Click **Cancel** to leave this screen without saving any changes you may have made.

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 46 on page 61). The screen displays as shown.

Figure 54 Windows XP SP2: Wireless Networks: Preferred Networks



☑ Use Windows to configure my wireless network settings

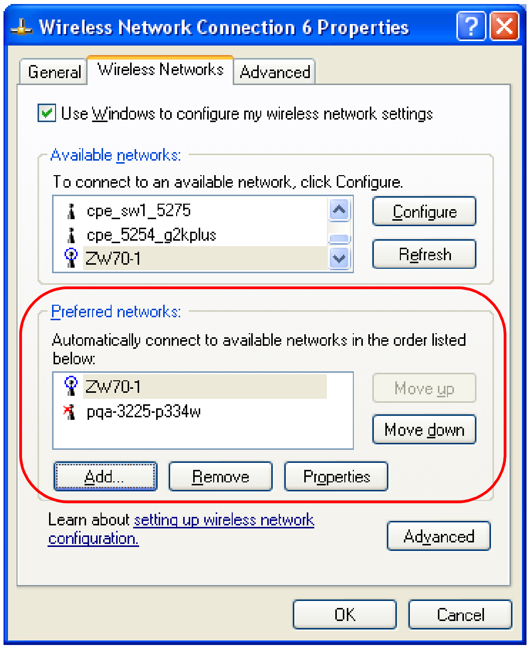
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Automatically connect to available networks in the order listed below:

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 55 Windows XP SP1: Wireless Networks: Preferred Networks



☑ Use Windows to configure my wireless network settings

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

Automatically connect to available networks in the order listed below:

- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

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.

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 security configuration screen. You may still configure and store keys, but they will not be used while Dynamic WEP is enabled.

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 26 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

Table 26 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
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 sucessful 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.

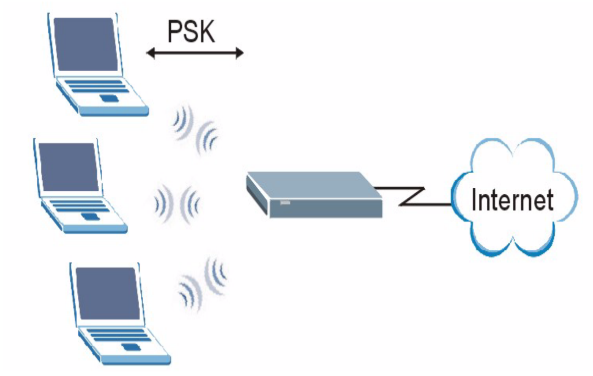
Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

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 wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.
4. The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 56 WPA-PSK Authentication

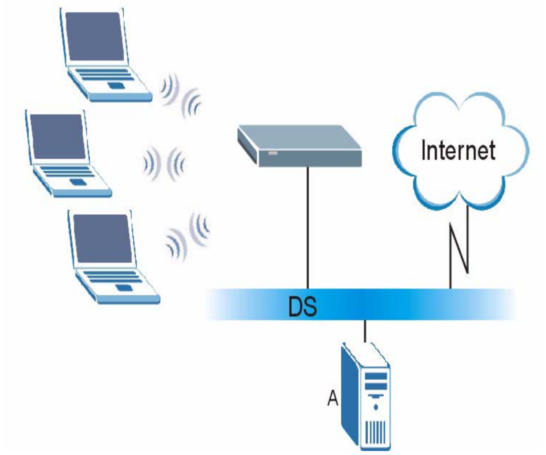


WPA(2) with RADIUS Application Example

To set up WPA(2), 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 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 57 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 or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 27 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

D

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

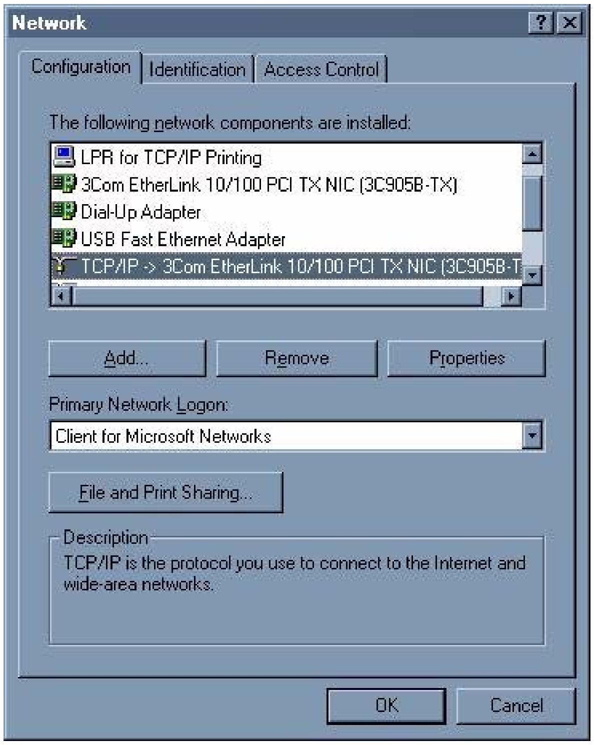
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 58 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.
2 Select **Adapter** and then click **Add**.
3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.
2 Select **Protocol** and then click **Add**.
3 Select **Microsoft** from the list of **manufacturers**.
4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.
2 Select **Client** and then click **Add**.
3 Select **Microsoft** from the list of manufacturers.
4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5 Restart your computer so the changes you made take effect.

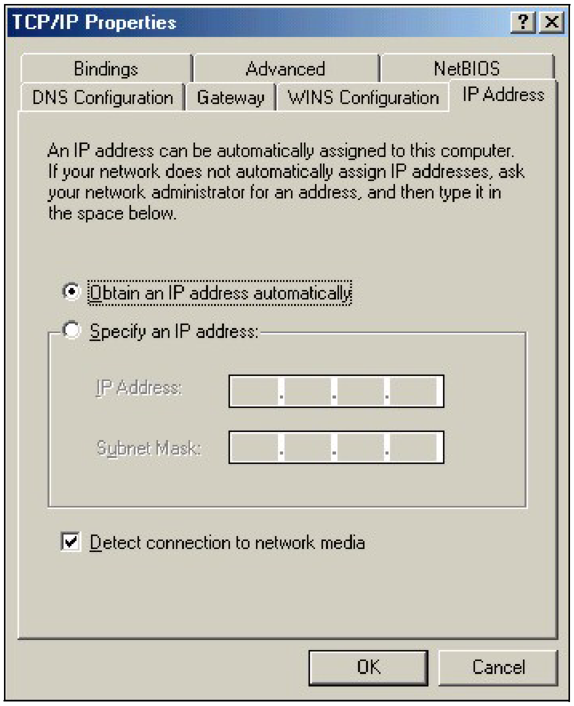
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 59 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

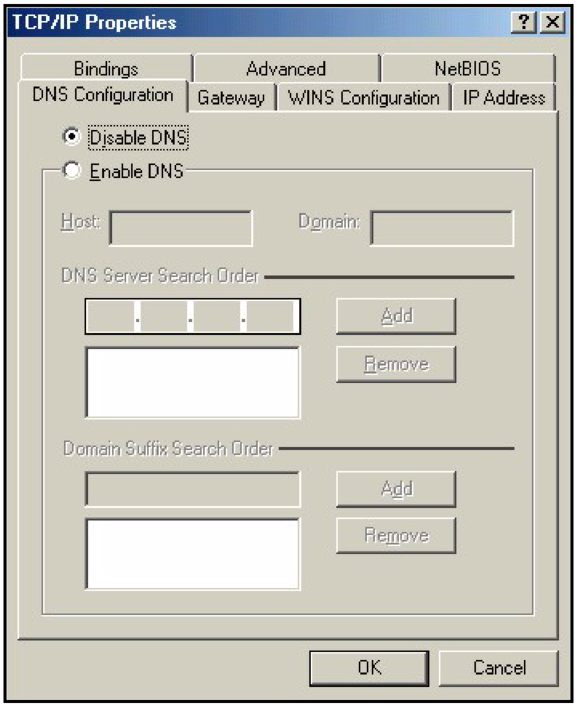
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 60 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

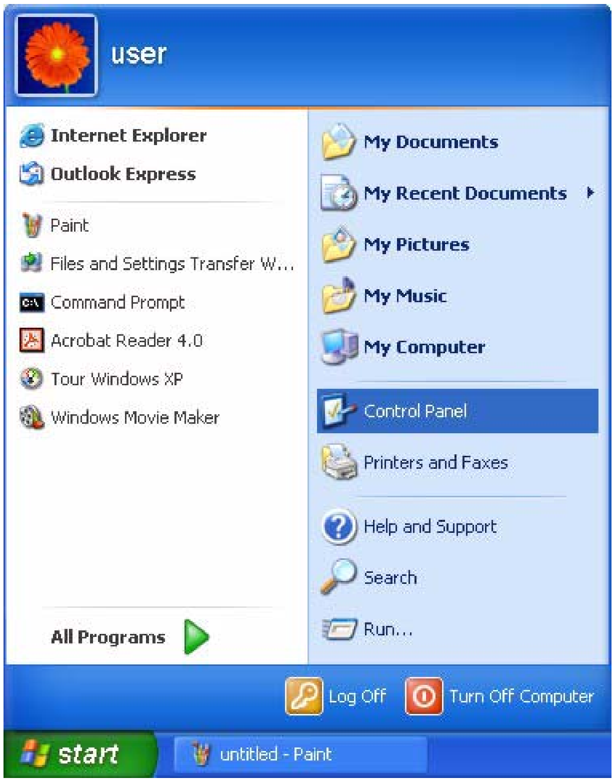
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

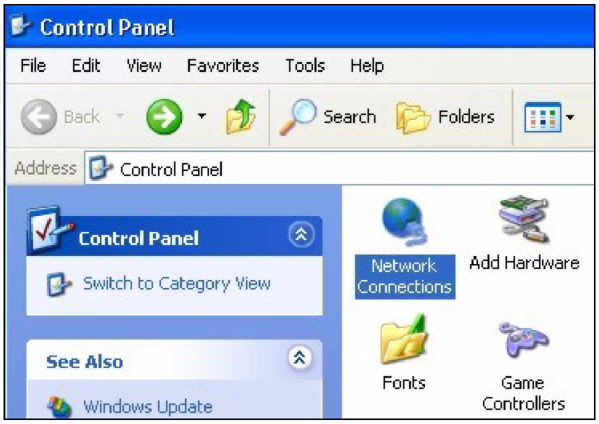
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 61 Windows XP: Start Menu



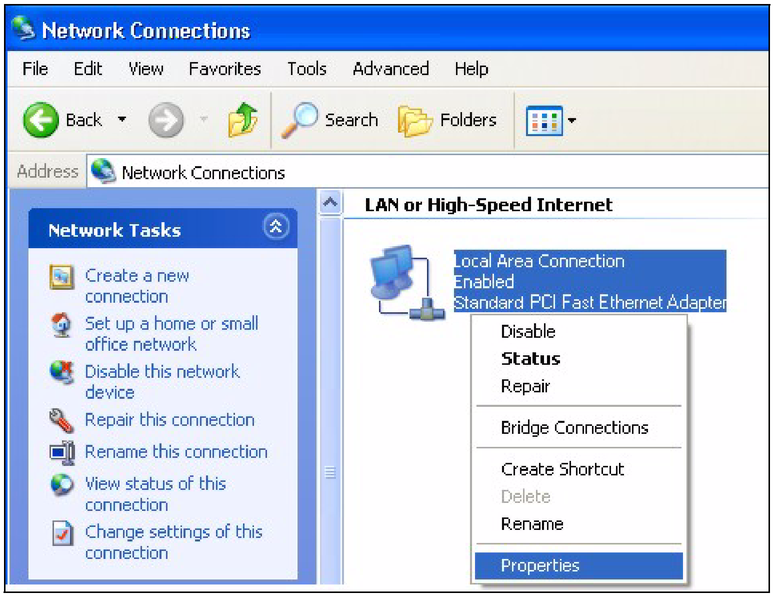
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 62 Windows XP: Control Panel



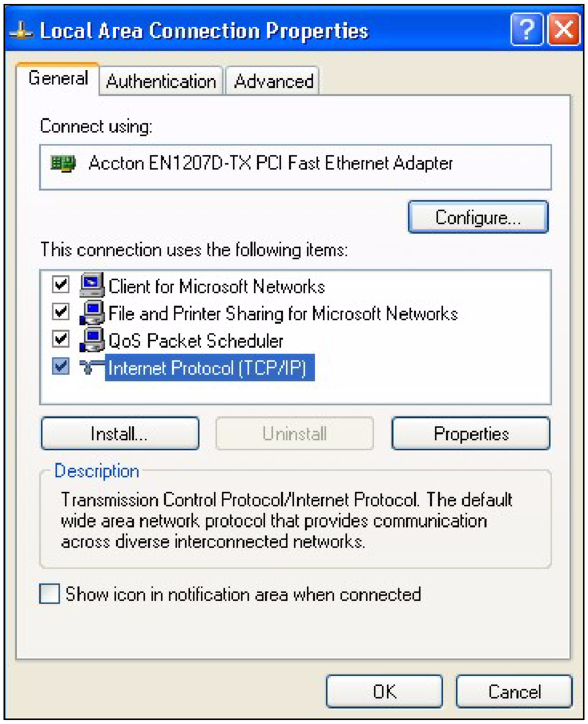
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 63 Windows XP: Control Panel: Network Connections: Properties



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

Figure 64 Windows XP: 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

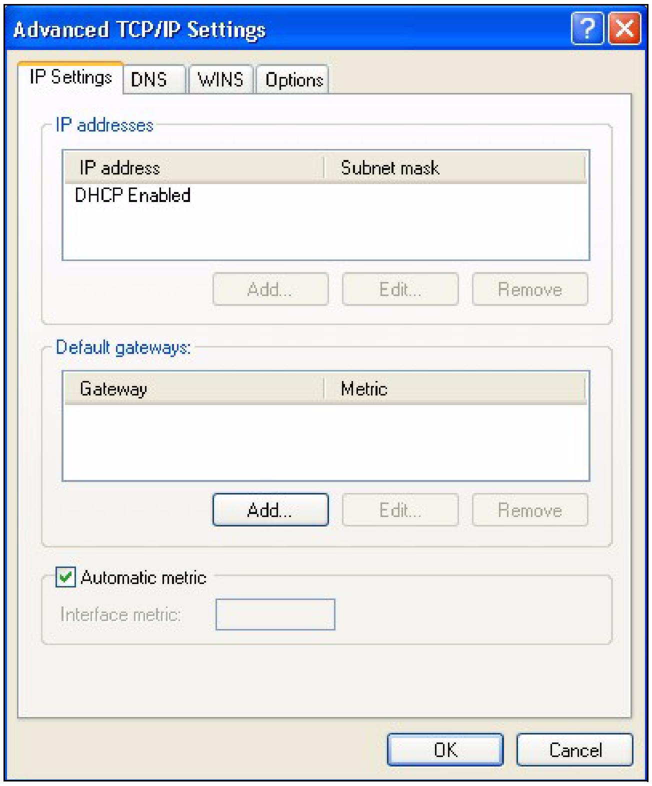
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ 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 65 Windows XP: Advanced TCP/IP Settings



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

☑ Automatic metric

Interface 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:

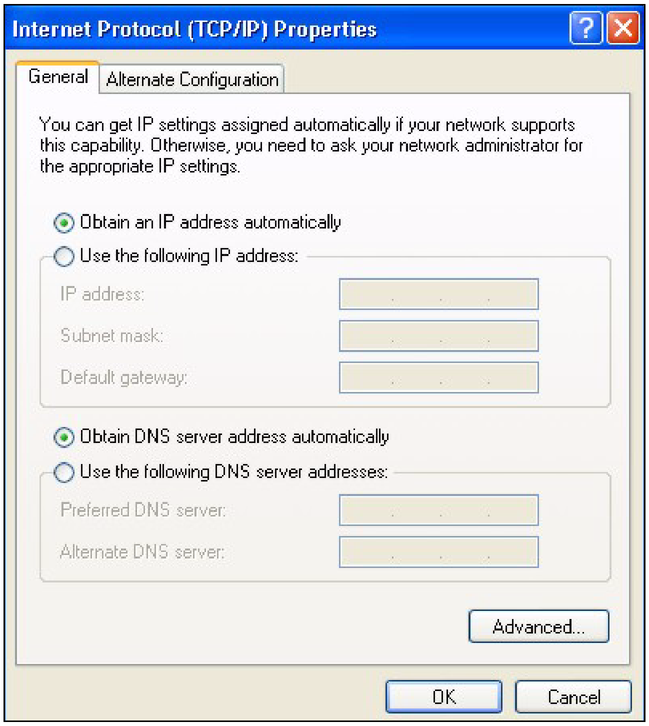
- In the **IP Settings** tab, in **IP addresses**, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **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 66 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

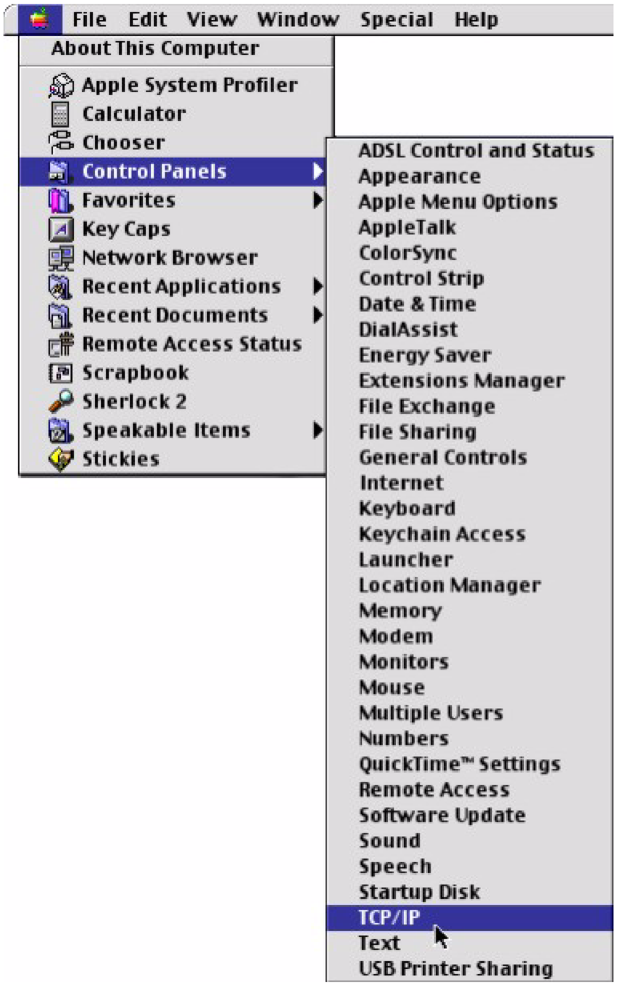
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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.

Macintosh OS 8/9

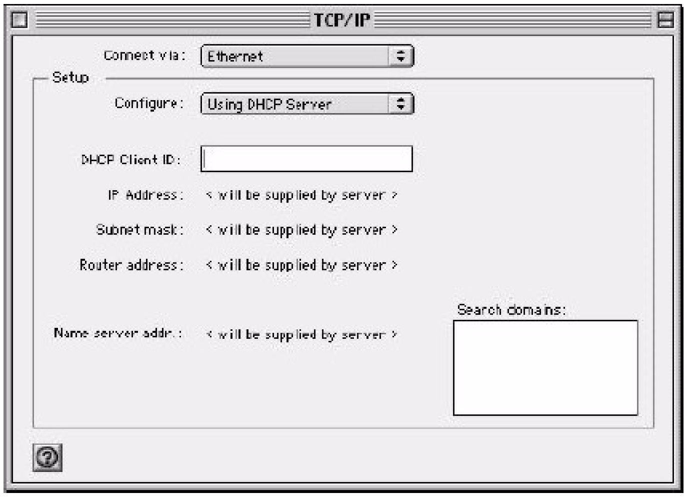
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 67 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 68 Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box if you have one.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Restart your computer (if prompted).

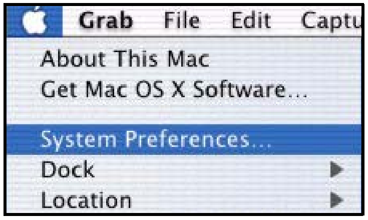
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 69 Macintosh OS X: Apple Menu

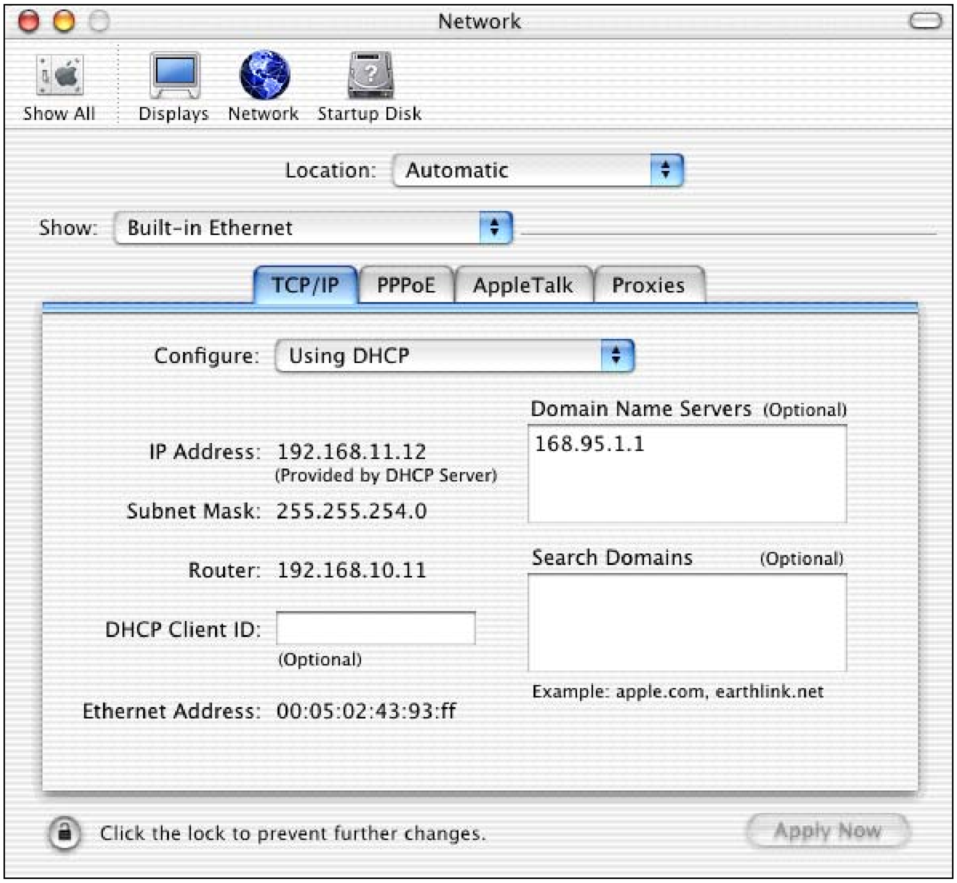


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 70 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

4 For statically assigned settings, do the following:
- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your gateway in the **Router address** box if you have one.

5 Click **Apply Now** and close the window.

6 Restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Legal Information

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 device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device 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.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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。

Notices

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

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

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

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

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 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

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

Required Information

- 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.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-0
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: ftp.us.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

“+” is the (prefix) number you dial to make an international telephone call.

Index