ZyXEL G-162

802.11g Wireless CardBus Card

User's Guide

Version 3.0
8/2005

Copyright

Copyright ©2005 by ZyXEL Communications Corporation

Disclaimer

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

Trademarks

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

ZyXEL Limited Warranty

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

NOTE

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

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

Online Registration

Register online at www.zyxel.com for free future product updates and information.

Federal Communications Commission (FCC) Interference Statement

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

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

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.

Caution

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

Certifications

Refer to the product page at www.zyxel.com.

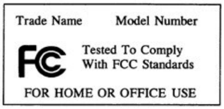


Table of Contents

List of Figures

List of Tables

Chapter 1
Getting Started

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

1.1 About Your G-162

The G-162 is an IEEE 802.11g compliant wireless LAN adapter.

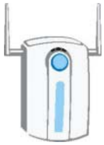
The following lists the main features of your G-162. See the product specifications in the appendix for detailed features.

- Automatic rate adjustment to that of the associated wireless network
- Security: WEP (Wired Equivalent Privacy), IEEE 802.1x, WPA-PSK, WPA (Wi-Fi Protected Access), WPA2-PSK and WPA2
- A built-in antenna
- Driver support for Windows 98 Second Edition, Windows Me, Windows 2000 and Windows XP

1.2 Syntax Conventions

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

1.3 Graphics Icons Key

 Wireless Access Point	 Computer	 Notebook computer
 Server	 Modem or Router	 Wireless Signal

1.4 Application Overview

1.4.1 Infrastructure

To connect to a network via an Access Point (AP), set the G-162 network type to **Infrastructure**. Through the AP, you can access the Internet or the wired network behind the AP.

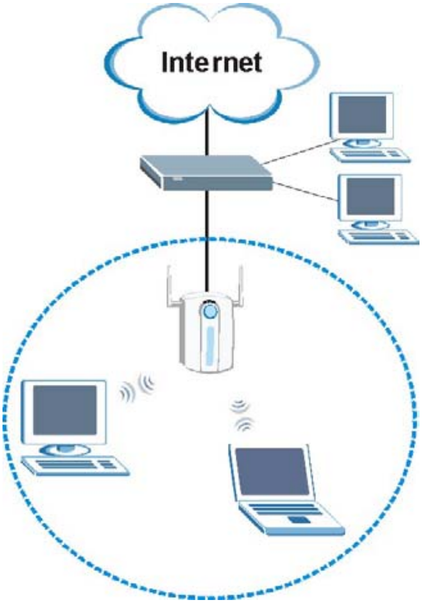


Figure 1-1 Infrastructure Example

1.4.2 Ad-Hoc

In case you prefer to set up a small independent wireless workgroup without an AP, use the **Ad-Hoc** mode.

Ad-hoc mode does not require an AP or a wired network. Two or more wireless clients communicate directly to each other.

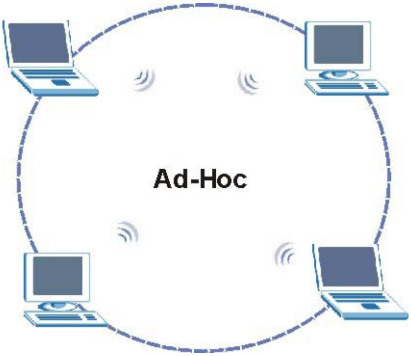


Figure 1-2 Ad-Hoc Example

To set up an Ad-Hoc network, configure all wireless clients in Ad-Hoc network type and use the same SSID, channel and security.

1.5 G-162 Hardware and Utility Installation

Follow the instructions in the Quick Start Guide to install the ZyXEL Utility and make hardware connections. The ZyXEL Utility is a program that lets you configure wireless parameters in the G-162. These parameters must be the same as the access point (AP) or peer WLAN device that you are connecting with.

1.6 Configuration Methods

To configure your G-162, use one of the following applications:

- ZyXEL Utility (This guide shows you how to configure the G-162 using the ZyXEL Utility)
- Wireless Zero Configuration (WZC) (recommended for Windows XP)

In Windows XP, you must disable WZC if you want to use the ZyXEL Utility. Refer to the appendices on how to deactivate WZC or how to use WZC to manage the G-162.

- Odyssey Client Manager (not supplied)

  Refer to the Odyssey Client documentation for more information.

DO NOT use WZC or the Odyssey Client Manager and the ZyXEL Utility at the same time.

1.7 Accessing the ZyXEL Utility

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

When the ZyXEL Utility system tray icon displays, the G-162 is installed properly.

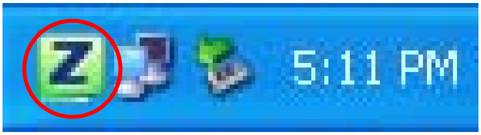


Figure 1-3 ZyXEL Utility: System Tray Icon

The color of the ZyXEL Utility system tray icon indicates the status of the G-162. Refer to the following table for details.

Table 1-1ZyXEL Utility: System Tray Icon

COLOR	DESCRIPTION
Red	The G-162 is not connected to a wireless network or is searching for an available wireless network.
Green	The G-162 is connected to a wireless network.

Double click on the ZyXEL Utility icon in the system tray to open the ZyXEL Utility. The ZyXEL Utility screens are similar in all supported Microsoft Windows operating systems. Screens for Windows XP are shown in this guide.

Click the ? icon (located in the top right corner) to display the on-line help window.

1.7.1 ZyXEL Utility Screen Summary

This summarizes the ZyXEL Utility screens.

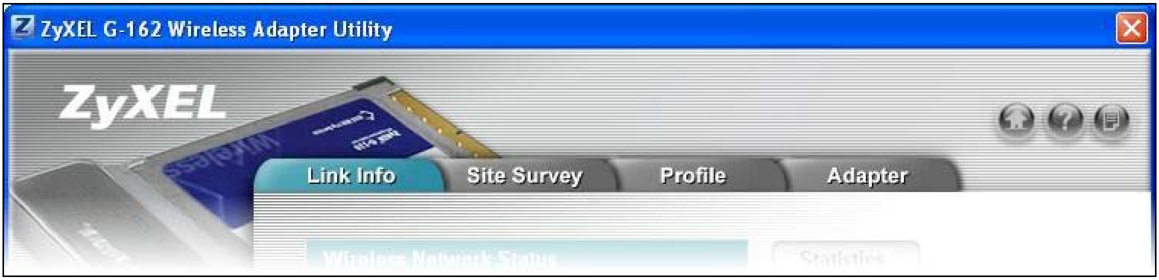


Figure 1-4 Screen Overview

The following table describes the labels in this screen.

Table 1-2 Screen Summary

SCREEN	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 configure a transfer rate, enable power saving and use OTIST (One-Touch Intelligent Security Technology).
About (▤)	Use this screen to view the ZyXEL Utility and driver versions.

1.8 Network Connection Methods

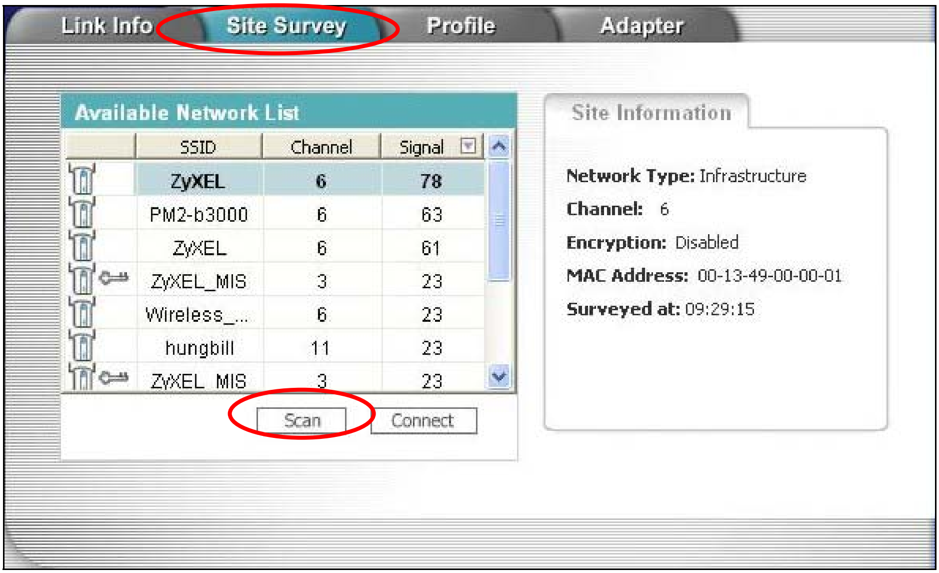
The following sections show you how to associate with a network using the ZyXEL Utility. You can either manually connect to a network or configure a profile to have the G-162 automatically connect to a specific network. Otherwise, configure nothing and leave the G-162 to automatically scan for and connect to any other available network without security.

See the next chapters for detailed field descriptions.

1.8.1 Site Survey

After you install the ZyXEL Utility and then insert the G-162, follow the steps below to connect to a network using the **Site Survey** screen.

1. Make sure a wireless network is available and within range.
2. Open the ZyXEL Utility and click the **Site Survey** tab to open the screen as shown next.
3. Click **Scan** to search for available wireless networks.



Available Network List

	SSID	Channel	Signal
	ZyXEL	6	78
	PM2-b3000	6	63
	ZyXEL	6	61
🔑	ZyXEL_MIS	3	23
	Wireless_...	6	23
	hungbill	11	23
🔑	ZyXEL_MIS	3	23

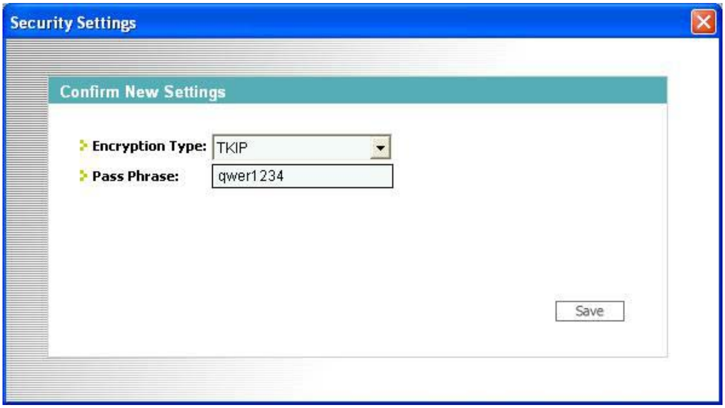
Site Information

Network Type: Infrastructure
Channel: 6
Encryption: Disabled
MAC Address: 00-13-49-00-00-01
Surveyed at: 09:29:15

Figure 1-5 Site Survey

4. To join a network, either click an SSID in the table and then click **Connect** or double-click an SSID.
5. If the wireless security is activated for the selected wireless network, the **Security Settings** screen displays. This screen varies according to the network’s encryption method. Configure the same security settings as the associated network.

If the selected network is unavailable or security settings are not correct, the G-162 will be disconnected.



Security Settings

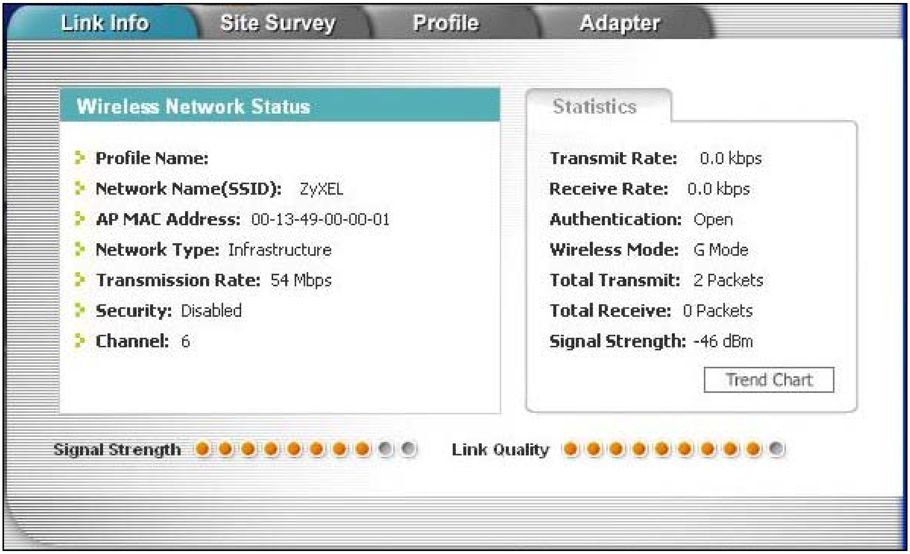
Confirm New Settings

Encryption Type: TKIP

Pass Phrase: qwer1234

Figure 1-6 Site Survey: Security Settings

6. Verify that you have successfully connected to the selected network and check the network information in the **Link Info** screen. If the G-162 is not connected to a network, the fields in this screen are blank.



Wireless Network Status

- Profile Name:
- Network Name(SSID): ZyXEL
- AP MAC Address: 00-13-49-00-00-01
- Network Type: Infrastructure
- Transmission Rate: 54 Mbps
- Security: Disabled
- Channel: 6

Statistics

Transmit Rate: 0.0 kbps

Receive Rate: 0.0 kbps

Authentication: Open

Wireless Mode: G Mode

Total Transmit: 2 Packets

Total Receive: 0 Packets

Signal Strength: -46 dBm

Figure 1-7 Link Info

1.8.2 Profiles

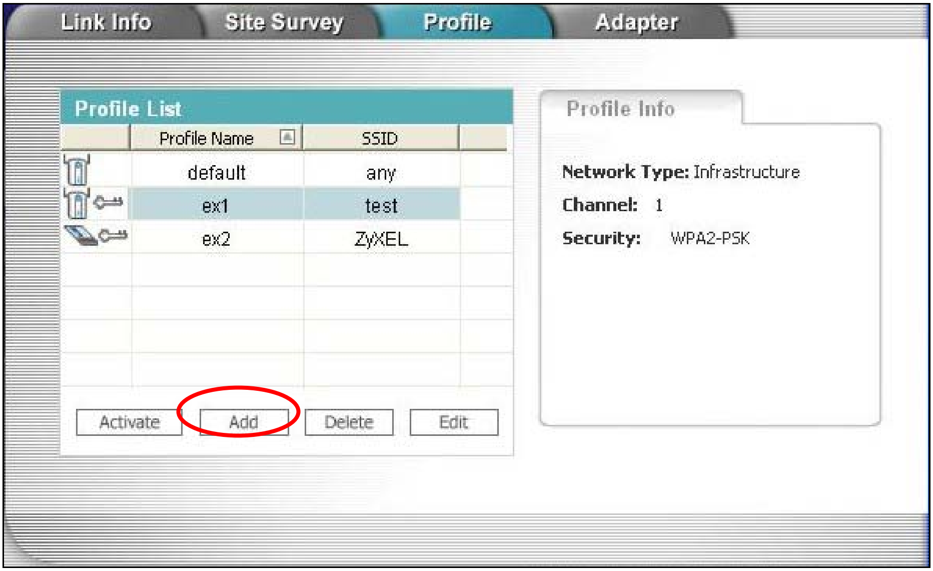
A profile is a set of wireless parameters that you need to connect to a wireless network. With a profile activated, each time you start the G-162, it automatically scans for the specific SSID and joins that network with the pre-defined wireless security settings. If the specified network is not available, the G-162 will be disconnected.

If you do not configure and activate a profile, each time you start the G-162, the G-162 uses the default profile to connect to any available network with security disabled.

The default profile is a profile that allows you to connect to any SSID without security.

Creating a Profile

1. Make sure a wireless network is available.
2. Open the ZyXEL Utility and click the **Profile** tab to open the screen as shown.
3. Click **Add** to configure a new profile.



	Profile Name	SSID
	default	any
	ex1	test
	ex2	ZyXEL

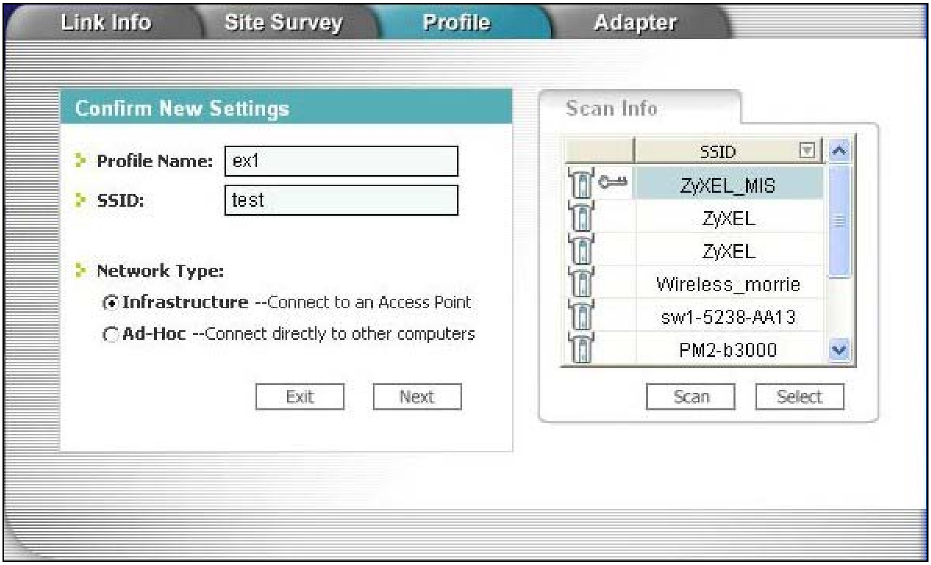
Network Type: Infrastructure

Channel: 1

Security: WPA2-PSK

Figure 1-8 Profile

4. Give the profile a descriptive name (of up to 32 printable ASCII characters). If you want to connect to an AP, select **Infrastructure** and enter the AP’s SSID. If you want to connect to another peer wireless device directly (without an AP), select **Ad-Hoc** and enter the same SSID as that device.



Confirm New Settings

Profile Name: ex1

SSID: test

Network Type:

● Infrastructure --Connect to an Access Point

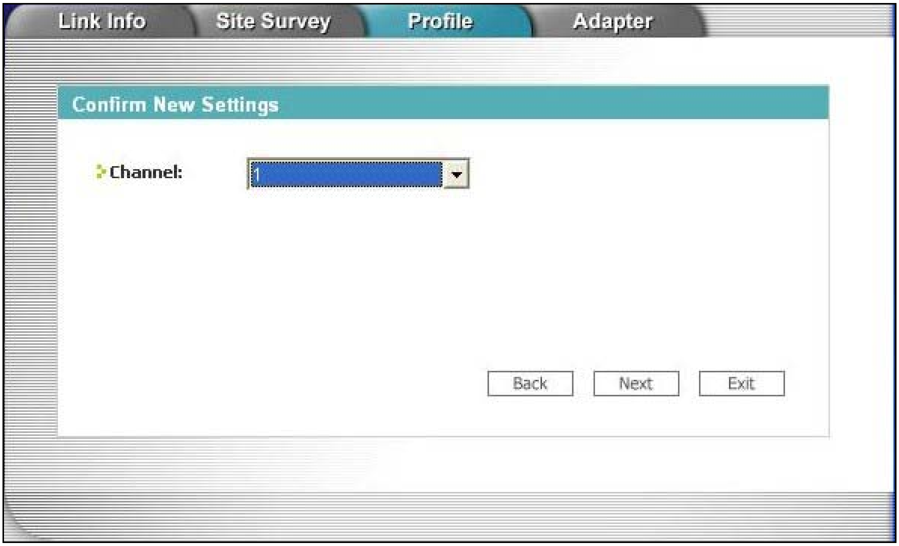
○ Ad-Hoc --Connect directly to other computers

Scan Info

SSID
ZyXEL_MIS
ZyXEL
ZyXEL
Wireless_morrie
sw1-5238-AA13
PM2-b3000

Figure 1-9 Profile: Add

5. If you selected **Infrastructure**, skip to the next step. If you selected **Ad-Hoc**, use the same channel as the peer wireless device.

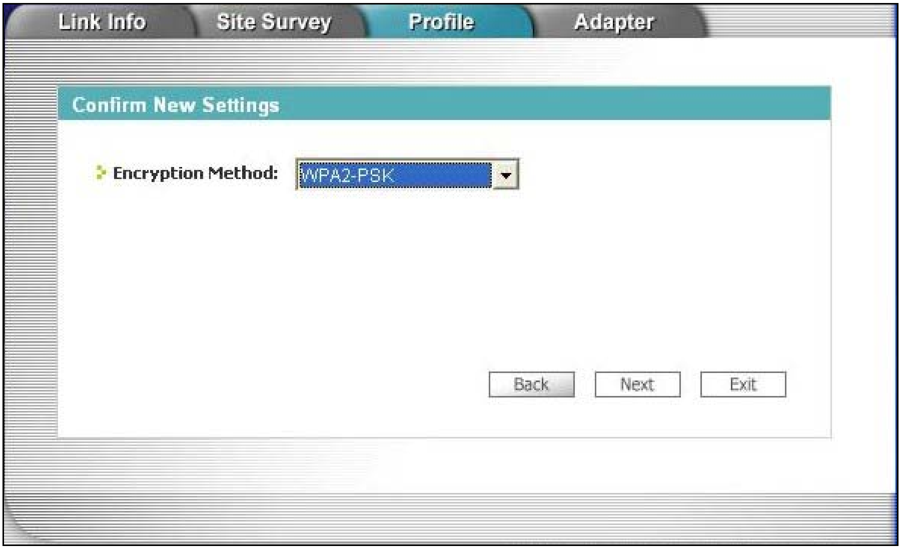


Confirm New Settings

Channel: 1

Figure 1-10 Profile: Channel

6. If you selected **Infrastructure**, choose the same encryption method (**Disable**, **WEP**, **WPA**, **WPA2**, **WPA-PSK**, **WPA2-PSK** or **802.1x**) as the AP to which you want to connect. If you selected **Ad-Hoc**, you can only use **WEP**.

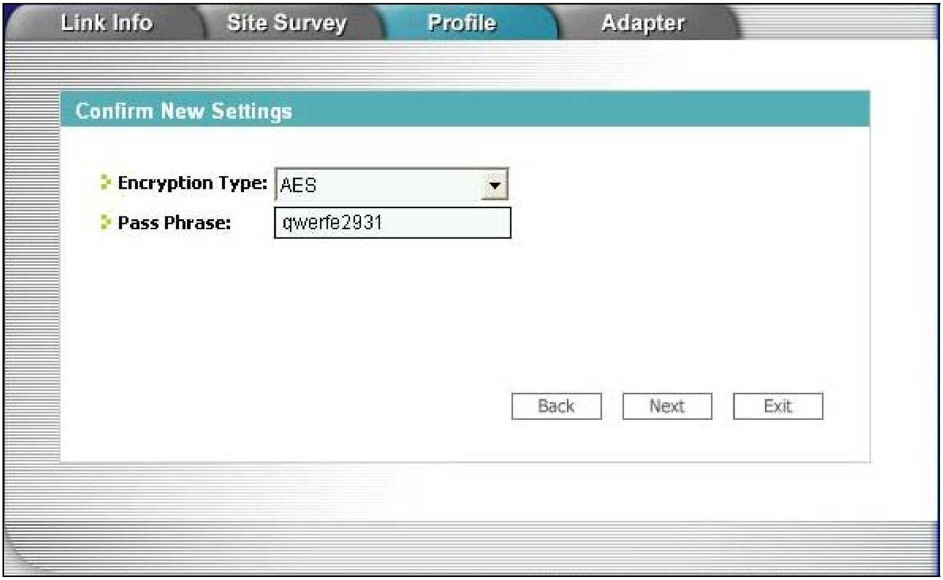


Confirm New Settings

Encryption Method: WPA2-PSK

Figure 1-11 Profile: Encryption

7. This screen varies depending on the encryption method you selected in the previous screen. Enter the same settings as the associated network.



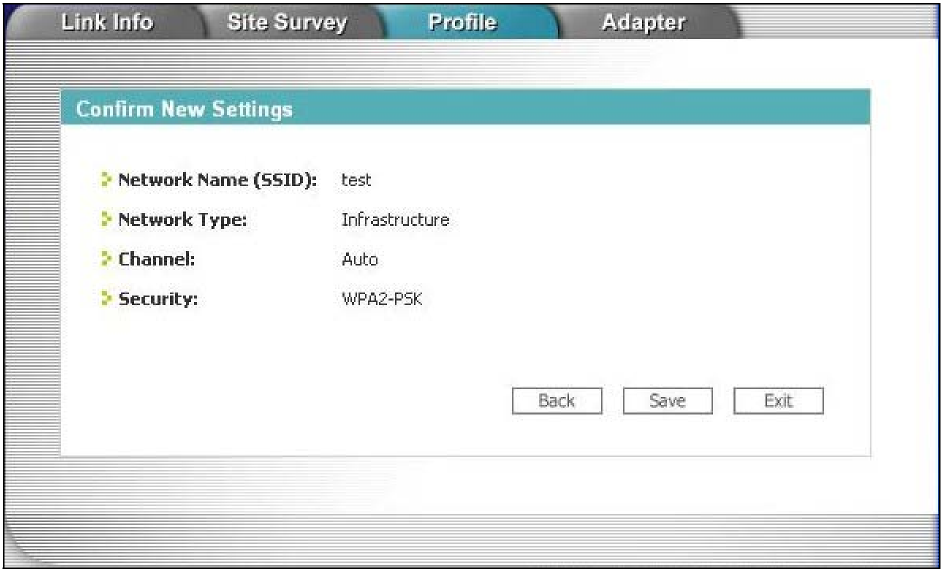
Confirm New Settings

Encryption Type: AES

Pass Phrase: qwerfe2931

Figure 1-12 Profile: Security

8. Verify the profile settings in the ready-only screen. Click **Save** to save and go to the next screen. Click **Back** to return to the previous screen.



Confirm New Settings

Network Name (SSID):	test
Network Type:	Infrastructure
Channel:	Auto
Security:	WPA2-PSK

Figure 1-13 Profile: Confirm

9. Click **Activate Now** to use the new profile immediately. Otherwise, click **Activate Later** and go back to the Profile screen. You can follow the previous steps to create another profile.

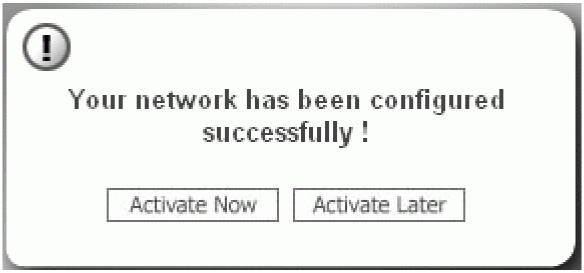

Your network has been configured successfully !

Figure 1-14 Profile: Activate

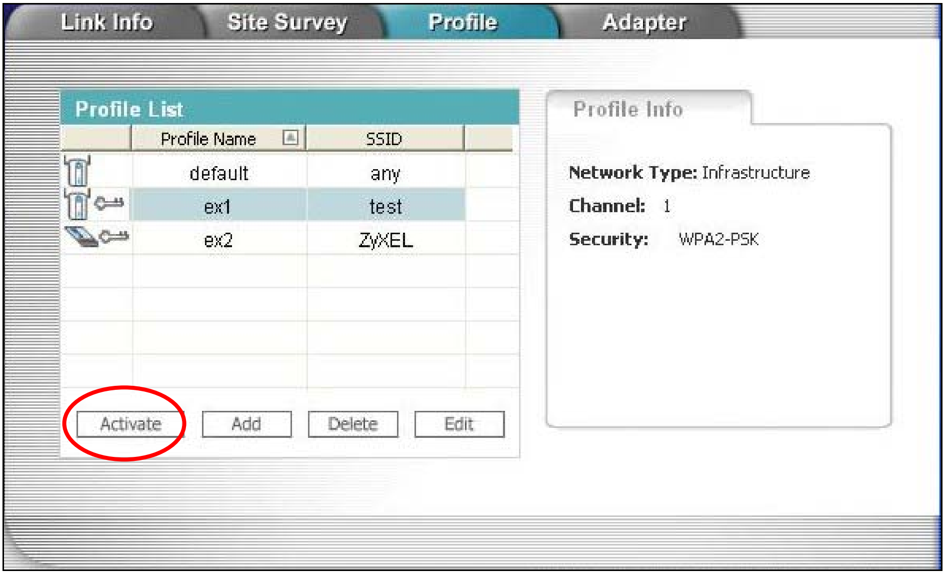
10. If you clicked **Activate Now**, check the network information in the **Link Info** screen to see if you have successfully connected to the specified network. If the G-162 is not connected to a network, the fields in this screen are blank.

Activating a Profile

If you have more than one profile, you can use one of the pre-configured profiles to connect to a wireless network by activating it. Follow the steps below to activate a profile.

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

1. In the ZyXEL Utility, click the **Profile** tab to open the screen as shown next.
2. Select a profile and click **Activate** to use the selected profile.



Profile List

	Profile Name	SSID
	default	any
	ex1	test
	ex2	ZyXEL

Profile Info

Network Type: Infrastructure

Channel: 1

Security: WPA2-PSK

Figure 1-15 Profile

Chapter 2
Link Info

*This chapter shows you detailed information about the **Link Info** screen.*

2.1 Transmission Rate (Transfer Rate)

The G-162 provides various transmission (data) rate options for you to select. Options include **Fully Auto**, **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **11 Mbps**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, **54 Mbps** and **125 Mbps**.

In most networking scenarios, the factory default **Fully Auto** setting is the most efficient. This setting allows your G-162 to operate at the highest possible transmission (data) rate. When the communication quality drops below a certain level, the G-162 automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the G-162 gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

If you want to select a specific transmission rate, select one that the AP or peer wireless device supports. **1 Mbps** or **2 Mbps** are often used in networking environments where the range of the wireless connection is more important than speed.

Your G-162 can transmit at 22Mbps or up to 125 Mbps when connected to a ZyXEL g+ AP or wireless router.

Actual speeds attained also depend on the distance from the AP, noise, etc.

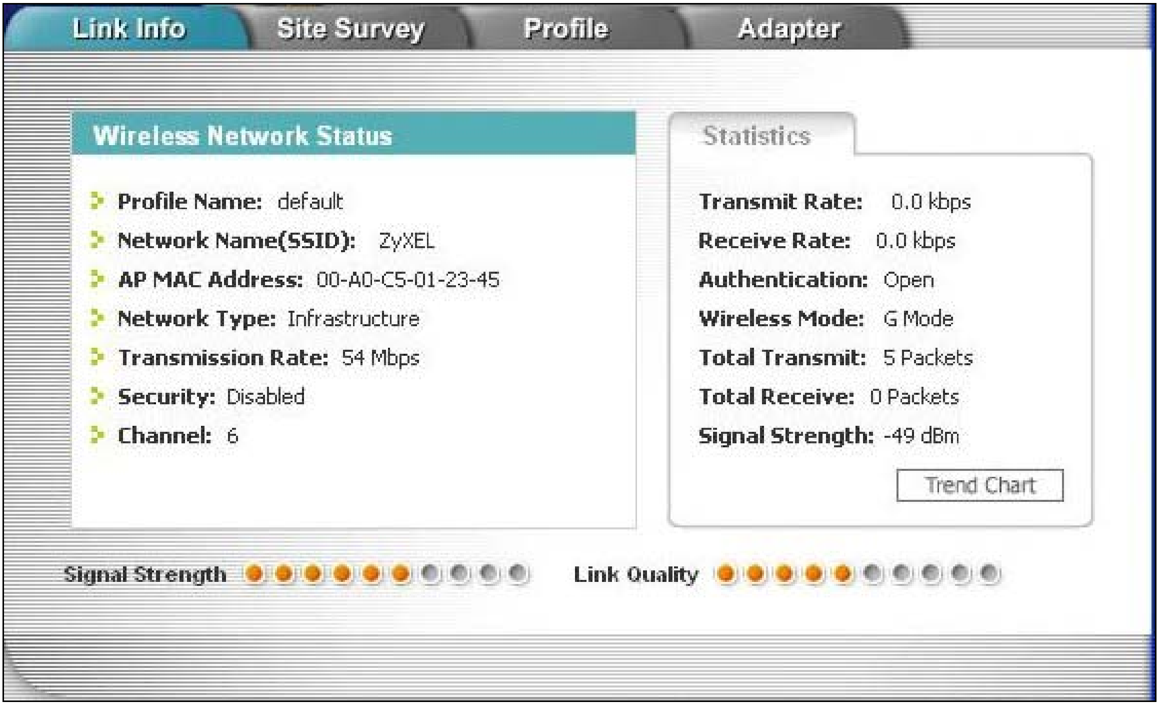
2.1.1 G-plus

G-plus is an enhancement to the IEEE 802.11g wireless standard. G-plus combines multiple frames into a larger frame size. This increases wireless transmission speeds by allowing larger frames (up to 4 KB) to be sent.

G-plus speed applies only to unicast traffic (not broadcast or multicast). G-plus is automatically disabled if wireless transmission speeds fall below 11 Mbps.

2.2 Configuring the Link Info screen

When the ZyXEL Utility starts, the **Link Info** screen displays, showing the current configuration and connection status of your G-162. You can also click the **Link Info** tab to display the screen as shown next.



Profile Name: default
Network Name(SSID): ZyXEL
AP MAC Address: 00-A0-C5-01-23-45
Network Type: Infrastructure
Transmission Rate: 54 Mbps
Security: Disabled
Channel: 6

Transmit Rate: 0.0 kbps
Receive Rate: 0.0 kbps
Authentication: Open
Wireless Mode: G Mode
Total Transmit: 5 Packets
Total Receive: 0 Packets
Signal Strength: -49 dBm

Figure 2-1 Link Info

The following table describes the labels in this screen.

Table 2-1 Link Info

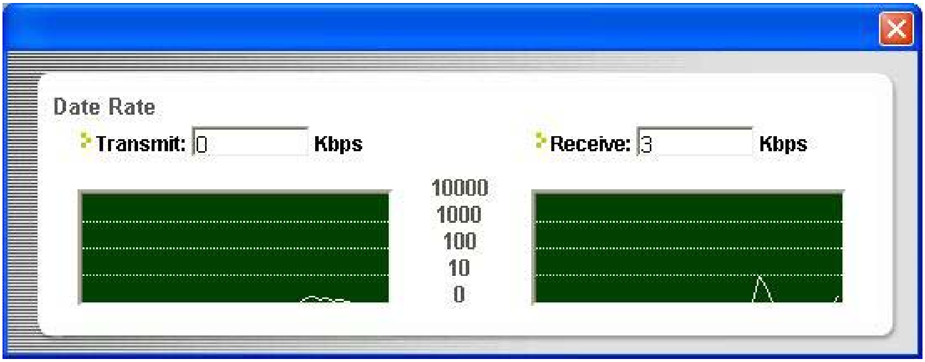
LABEL	DESCRIPTION
Wireless Network Status The following fields show the information of the network to which the G-162 is connected. If there is no associated wireless network, they are blank.	
Profile Name	This is the name of the profile you are currently using. A profile is a set of wireless parameters that you need to connect to a wireless network. If you do not configure and activate a new profile, each time you start the G-162, the G-162 uses the default profile to associate with an available network.
Network Name (SSID)	This field displays the name (SSID) of the wireless network to which the G-162 belongs. The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

Table 2-1 Link Info

LABEL	DESCRIPTION
AP MAC Address	This field displays the MAC address of the wireless device to which the G-162 is associated. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless network.
Transmission Rate	This field displays the current transmission rate of the G-162 in megabits per second (Mbps).
Security	This field displays whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-RADIUS**, **WPA2-RADIUS** or **RADIUS**) or not (**Disabled**).
Channel	This field displays the radio channel the G-162 is currently using. A radio frequency used by a wireless device is called a channel.
Statistics The following fields show the connection status with the associated network. If there is no associated wireless network, they are blank.	
Transmit Rate	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive Rate	This field displays the current data receiving rate in kilobits per second (Kbps).
Authentication	This field displays the authentication method of the G-162.
Wireless Mode	This field indicates the wireless standard (802.11b or 802.11g) of the wireless device. This field displays **G Mode**, **B Mode** or **Mixed Mode**.
Total Transmit	This field displays the total number of data frames transmitted since the G-162 was associated with the wireless network.
Total Receive	This field displays the total number of data frames received since the G-162 was associated with the wireless network.
Signal Strength	This field displays the signal strength of the G-162.
Trend Chart	Click this button to display the real-time statistics of the data rate in kilobits per second (Kbps).
Signal Strength	The status bar shows the strength of the signal.
Link Quality	The status bar shows the quality of the signal.

2.2.1 Trend Chart

Click **Trend Chart** in the **Link Info** screen to open the read-only screen as shown next.



Date Rate

Transmit: 0 Kbps

Receive: 3 Kbps

Figure 2-2 Link Info: Trend Chart

The following table describes the labels in this screen.

Table 2-2 Link Info: Trend Chart

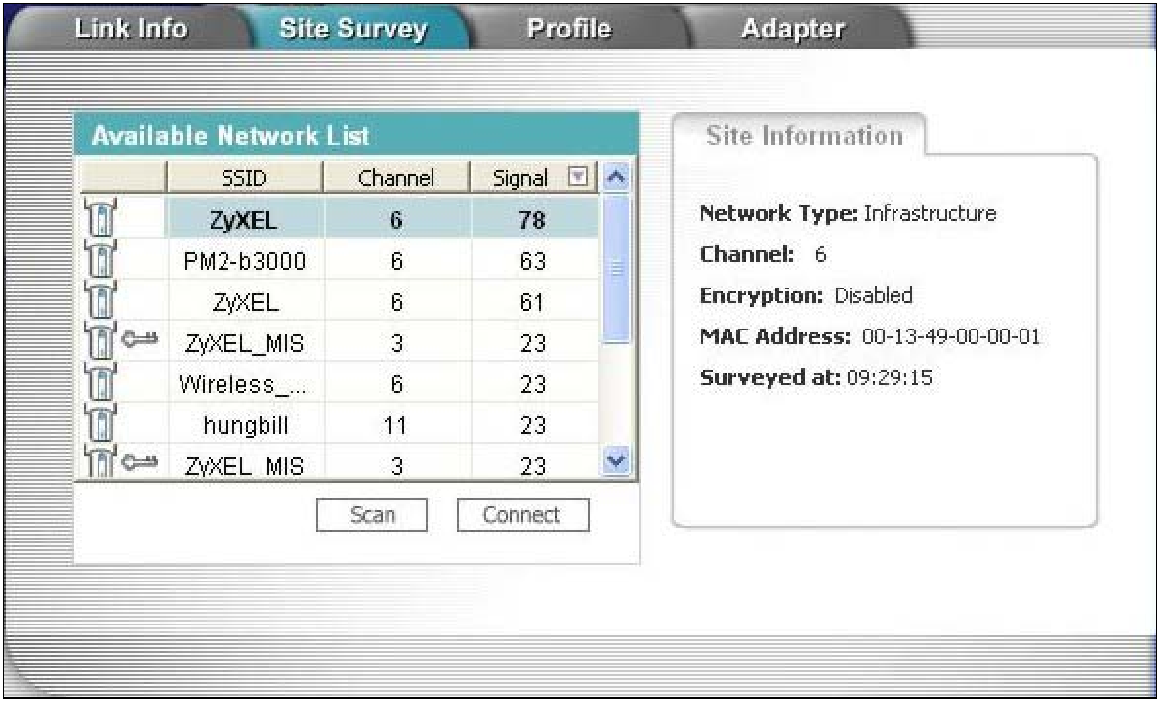
LABEL	DESCRIPTION
Transmit	This field displays the current data transmission rate in kilobits per second (Kbps).
Receive	This field displays the current data receiving rate in kilobits per second (Kbps).

Chapter 3
Site Survey

This chapter provides a detailed description about the ***Site Survey*** *screen. See the* ***Getting Stated*** *chapter for how to connect to a network using the* ***Site Survey*** *screen.*

3.1 Configuring the Site Survey screen

Click the **Site Survey** tab and use this screen to scan for a wireless network and connect to it.



	SSID	Channel	Signal
	ZyXEL	6	78
	PM2-b3000	6	63
	ZyXEL	6	61
🔑	ZyXEL_MIS	3	23
	Wireless_...	6	23
	hungbill	11	23
🔑	ZyXEL_MIS	3	23

Network Type: Infrastructure

Channel: 6

Encryption: Disabled

MAC Address: 00-13-49-00-00-01

Surveyed at: 09:29:15

Figure 3-1 Site Survey

The following table describes the labels in this screen.

Table 3-1 Site Survey

LABEL	DESCRIPTION
Available Network List The wireless network to which the G-162 is associated is bolded. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.	
📡, 💳 or 🔑	📡 denotes that the wireless device is in infrastructure mode. 💳 denotes that the wireless device is in Ad-Hoc mode. 🔑 displays with the previous two icons if the wireless devices are using security.
SSID	This field displays the SSID (Service Set IDentifier) of each wireless network. The SSID is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.
Channel	This field displays the channel number used by each wireless network. A radio frequency used by a wireless device is called a channel.
Signal	This field displays the signal strength of each wireless network.
Scan	Click **Scan** to search for available wireless networks within transmission range.
Connect	Click **Connect** to associate with the selected wireless network.
Site Info Click an entry in the **Available Network List** table to display the information of the selected wireless network.	
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the wireless network.
Channel	This field displays the channel number used by each wireless network.
Encryption	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-RADIUS**, **WPA2-RADIUS** or **RADIUS**) or inactive (**Disabled**).
MAC address	This field displays the MAC address of the AP or peer wireless device.
Surveyed at	This field displays the time when the G-162 scanned the wireless network.

Chapter 4
Security Settings

This chapter discusses how to configure wireless security on the G-162.

4.1 Wireless LAN Security

Wireless LAN security is vital to protect wireless communications.

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

Table 4-1 Wireless LAN Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with SSID Hidden
	MAC Address Filtering
↕	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2 (IEEE 802.11i)

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

4.1.1 Data Encryption with WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the G-162 and the AP or other peer wireless device to keep them private. Both the wireless clients and the access points must use the same WEP key for data encryption and decryption.

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

- Automatic WEP key generation based on a “password phrase” called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.

For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the **Security Settings** screen of the ZyXEL Utility and entering them manually as the WEP keys in the other WLAN adapter(s).

- Enter the WEP keys manually.

Your G-162 allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys. Only one key is used as the default key at any one time.

See the wireless LANs appendix for more information about WPA, WPA2 and IEEE 802.1x.

4.2 Authentication Type

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

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

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

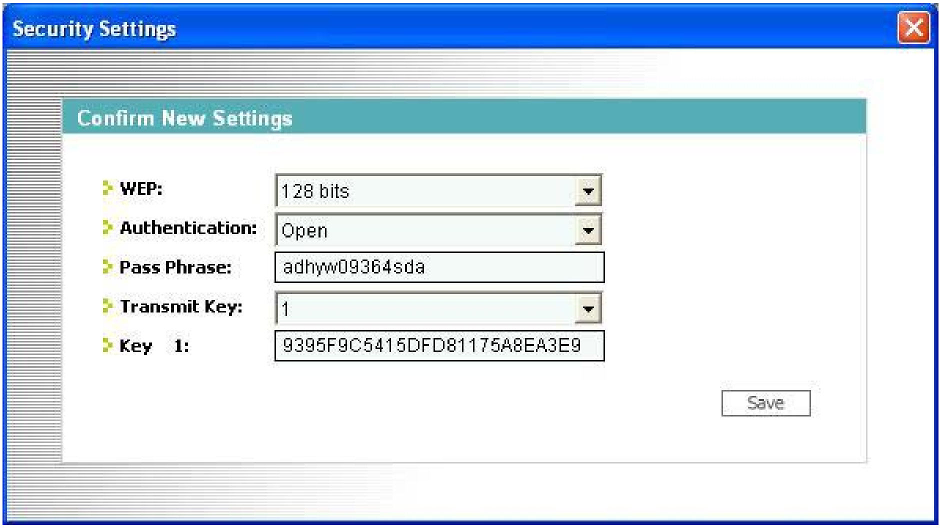
4.3 Configuring Security Settings

The **Security Settings** screen displays when you configure the G-162 to connect to a network with wireless security activated. This screen also displays when you add a new profile or edit an existing profile.

The screen varies according to the selected encryption method.

Enter the exact same settings (for example the encryption type, key or certificate) as the wireless network you want to join.

4.3.1 WEP Encryption



WEP: 128 bits

Authentication: Open

Pass Phrase: adhyw09364sda

Transmit Key: 1

Key 1: 9395F9C5415DFD81175A8EA3E9

Figure 4-1 Security Settings: WEP

The following table describes the labels in this screen.

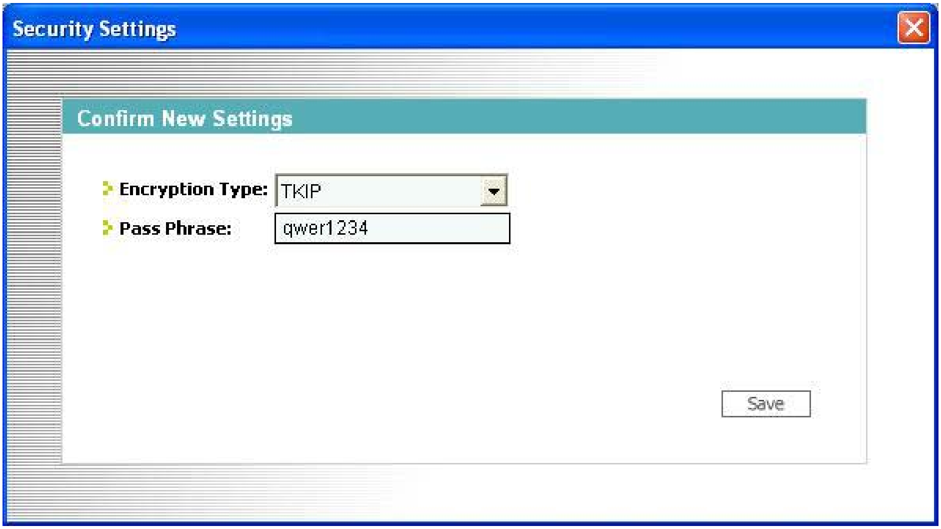
Table 4-2 Security Settings: WEP

LABEL	DESCRIPTION
WEP	Select **64 Bits**, **128 Bits** or **256 Bits** to activate WEP encryption and then fill in the related fields.
Authentication	Select **Share** to authenticate the G-162 to an AP or peer WLAN device using the key(s) configured below. Otherwise, select **Open** if you want to connect to any AP or peer device without sharing a key. Refer to *Section 4.2* for more information.
Pass Phrase	As you enter the passphrase, the G-162 automatically generates four different WEP keys and displays one in the key field below. Refer to *Section 4.1.1* for more information.
Transmit Key	Select a default WEP key to use for data encryption. The key displays in the field below.

Table 4-2 Security Settings: WEP

LABEL	DESCRIPTION
Key x (where x is a number between 1 and 4)	If you want to manually set the WEP keys, enter the WEP key (same as the AP or peer device) in the field provided. If you select **64 Bits** in the **WEP** field. ◆ Enter either 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 11AA22BB33) for HEX key type or ◆ Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for ASCII key type. If you select **128 Bits** in the **WEP** field, ◆ Enter either 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 00112233445566778899AABBCC) for HEX key type or ◆ Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for ASCII key type. If you select **256 Bits** in the **WEP** field, ◆ Enter either 58 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0000111122223333444455556666777788889999AAAABBBBCCCC000011) for HEX key type or ◆ Enter 29 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey111122223333444455556678) for ASCII key type. **The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN.** **ASCII WEP keys are case sensitive.**
Save	Click **Save** to save the changes and display the **Link Info** screen. Otherwise, click the close (☒) button to discard changes and go back to the previous screen.

4.3.2 WPA-PSK/WPA2-PSK



Encryption Type: TKIP

Pass Phrase: qwer1234

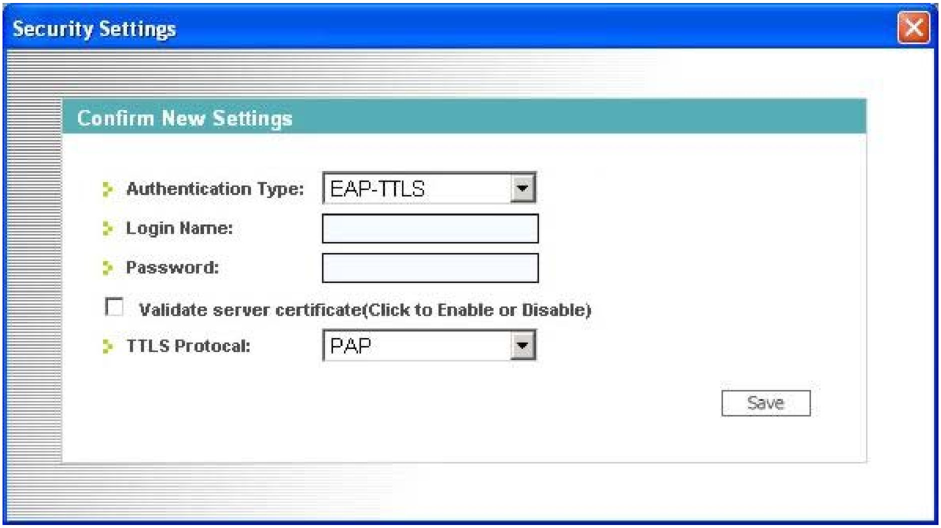
Figure 4-2 Security Settings: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 4-3 Security Settings: WPA-PSK/WPA2-PSK

FIELD	DESCRIPTION
Encryption Type	WPA uses **TKIP** and WPA2 uses **AES** to improve data encryption.
Pass Phrase	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. Type the passphrase (same as the AP or peer device) from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Save	Click **Save** to save the changes and display the **Link Info** screen. Otherwise, click the close (☒) button to discard changes and go back to the previous screen.

4.3.3 WPA/WPA2 or 802.1x



Authentication Type: EAP-TTLS

Login Name:

Password:

□ Validate server certificate(Click to Enable or Disable)

TTLS Protocal: PAP

Figure 4-3 Security Settings: WPA/WPA2 or 802.1x

The following table describes the labels in this screen.

Table 4-4 Security Settings: WPA/WPA2 or 802.1x

FIELD	DESCRIPTION
Authentication Type	Select the authentication method that the RADIUS server uses from the drop down list. Options are **EAP-TLS**, **EAP-TTLS** and **EAP-PEAP**.
Login Name	Enter a user name. This is the user name that is set up on a RADIUS server.
Password	This field is not available when you select **EAP-TLS** in the **Authentication Type** field. Enter the password associated with the login name above.

Table 4-4 Security Settings: WPA/WPA2 or 802.1x

FIELD	DESCRIPTION
Certificate	This field is only available when you select **EAP-TLS** in the **Authentication Type** field. Specify the location and name of a certificate in the **Certificate** field or click **Browse** to locate it. **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.**
Browse	This field is only available when you select **EAP-TLS** in the **Authentication Type** field. Click this button to display the **Select Certificate** screen, select a certificate and click **OK**. If you didn’t get the certificate first via a wired connection, no certificate displays in the **Select Certificate** screen.
Validate Server Certificate	Select the check box to check the certificate of the authentication server.
TTLS Protocol	This field is only available when you select **EAP-TTLS** in the **Authentication Type** field. Use the drop-down list box to select a TTLS protocol that the RADIUS server uses. Options are **PAP**, **CHAP**, **MS CHAP**, **MS CHAP v2** and **EAP**.
PEAP Inner EAP	This field is only available when you select **EAP-PEAP** in the **Authentication Type** field. Use the drop-down list box to select a PEAP protocol that the RADIUS server uses. Options are **EAP-GTC** and **MS CHAP v2**.
Save	Click **Save** to save the changes and display the **Link Info** screen. Otherwise, click the close (☒) button to discard changes and go back to the previous screen.

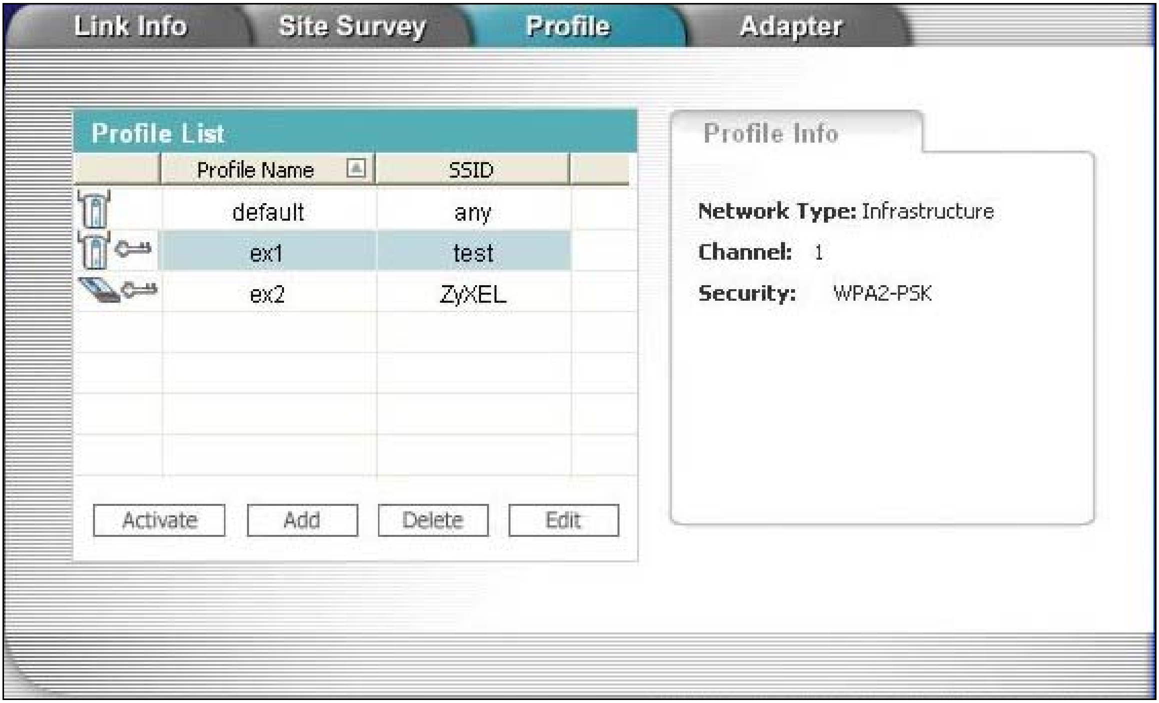
Chapter 5
Profile

This chapter describes how to configure and use a profile.

5.1 Configuring the Profile Screen

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

The profile function allows you to save a wireless network's settings, so you can use them again later.



	Profile Name	SSID
	default	any
	ex1	test
	ex2	ZyXEL

Network Type: Infrastructure

Channel: 1

Security: WPA2-PSK

Figure 5-1 Profile

The following table describes the labels in this screen.

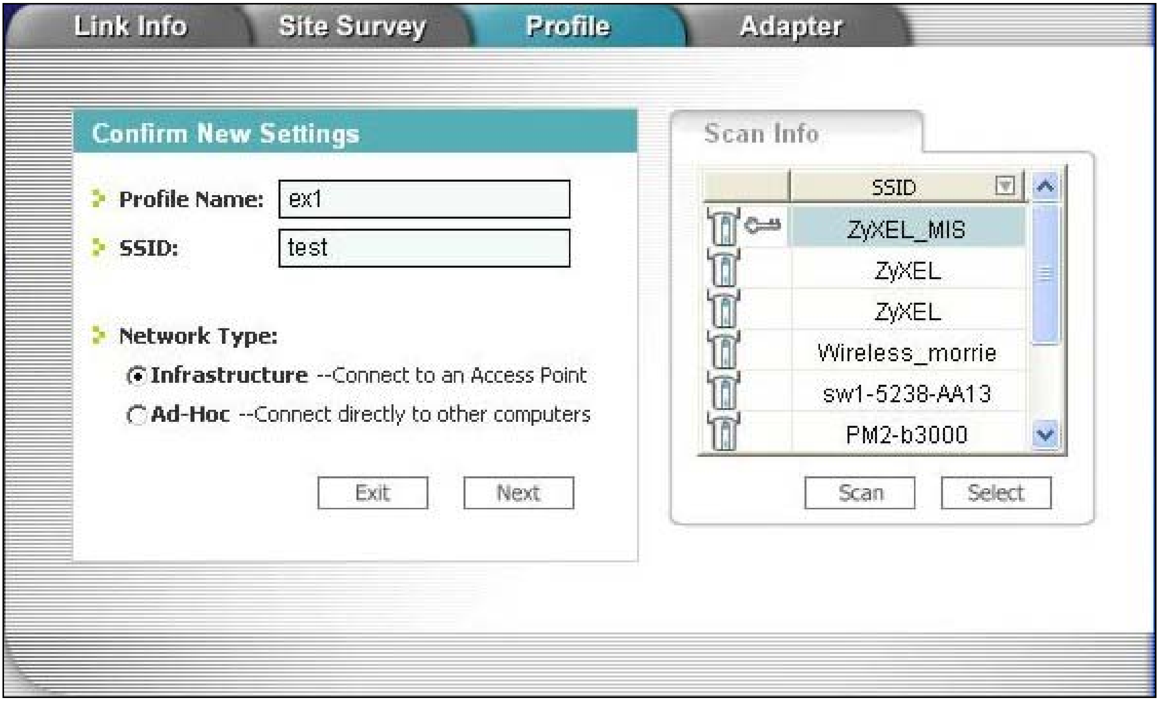
Table 5-1 Profile

LABEL	DESCRIPTION
Profile List Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.	
📡, 💳 or 🔑	📡 denotes that the wireless device is in infrastructure mode. 💳 denotes that the wireless device is in Ad-Hoc mode. 🔑 displays with the previous two icons if the wireless devices are using security.
Profile Name	This is the name of the profile.
SSID	This is the SSID of the wireless network to which the G-162 connects using this profile.
Connect	To use a previously saved network profile, select a profile name in the table and click **Connect**.
Add	To add a new profile into the table, click **Add**.
Delete	To delete an existing wireless network configuration, select a profile in the table and click **Delete**.
Edit	To edit an existing wireless network configuration, select a profile in the table and click **Edit**.
Profile Info The following fields display detailed information about the selected profile in the **Profile List** table.	
Network Type	This field displays the network type (**Infrastructure** or **Ad Hoc**) of the profile.
Channel	A radio frequency used by a wireless device is called a channel. This field displays the channel number used by the profile.
Security	This field shows whether data encryption is activated (**WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-RADIUS**, **WPA2-RADIUS** or **RADIUS**) or inactive (**Disabled**).

5.1.1 Adding a New Profile

Follow the steps below to add a new profile.

Step 1. Click **Add** in the **Profile** screen to display the screen as shown next. Click **Next** to continue.



Confirm New Settings

Profile Name: ex1

SSID: test

Network Type:

● Infrastructure --Connect to an Access Point

○ Ad-Hoc --Connect directly to other computers

Scan Info

SSID
ZyXEL_MIS
ZyXEL
ZyXEL
Wireless_morrie
sw1-5238-AA13
PM2-b3000

Figure 5-2 Profile: Add New Profile

The following table describes the labels in this screen.

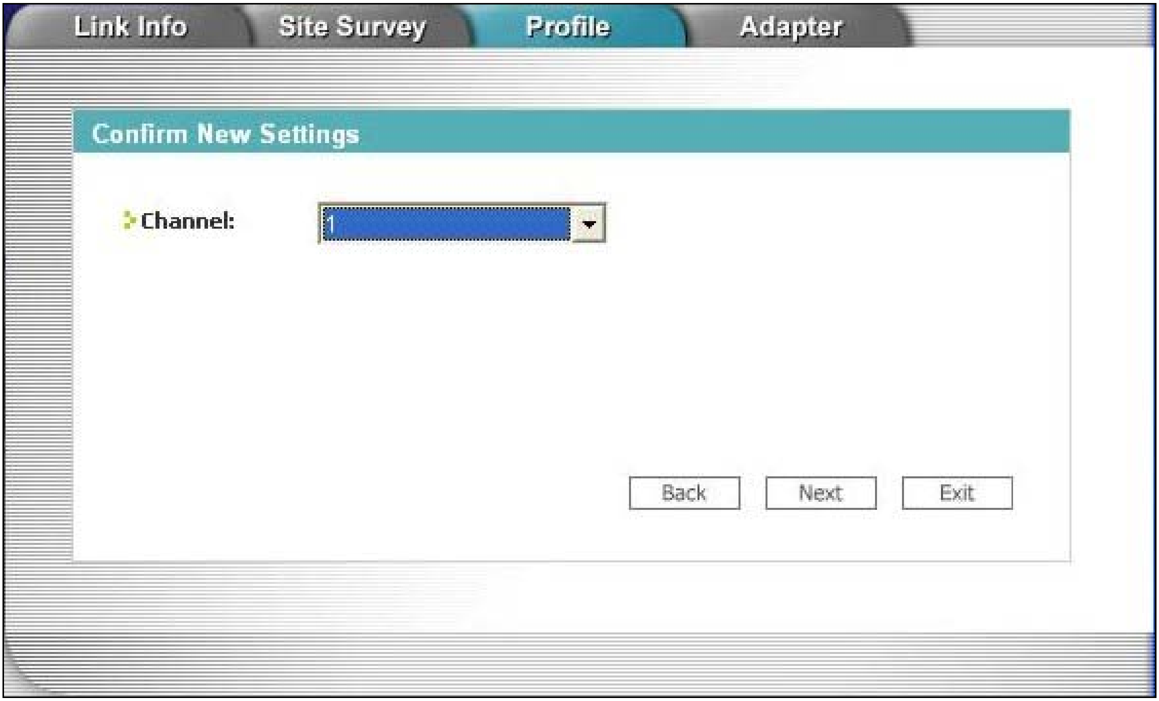
Table 5-2 Profile: Add New Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name (of up to 32 printable ASCII characters) in this field.
SSID	Select an available wireless device in the **Scan Info** table and click **Select**, or enter the SSID (Service Set IDentifier) of the AP or the peer ad-hoc device to which you want to associate in this field. To associate with an ad-hoc network, you must enter the same SSID as the peer ad-hoc device. Otherwise, leave this field blank or enter **any** to have the G-162 associate with or roam between any infrastructure wireless networks.
Network Type	Select the **Infrastructure** radio button to associate with an AP. Select the **Ad-Hoc** radio button to associate with a peer device.
Next	Click **Next** to go to the next screen.

Table 5-2 Profile: Add New Profile

LABEL	DESCRIPTION
Exit	Click **Exit** to go back to the previous screen without saving.
Scan Info This table displays the information of the available wireless networks within the transmission range.	
📡, 💳 or 🔑	📡 denotes that the wireless device is in infrastructure mode. 💳 denotes that the wireless device is in Ad-Hoc mode. 🔑 displays with the previous two icons if the wireless devices are using security.
SSID	This field displays the SSID (Service Set IDentifier) of each wireless device.
Scan	Click **Scan** to search for available wireless devices within transmission range.
Select	Select an available wireless device in the table and click **Select** to add it to this profile. Whenever you activate this profile, the G-162 associates with the selected wireless network only.

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

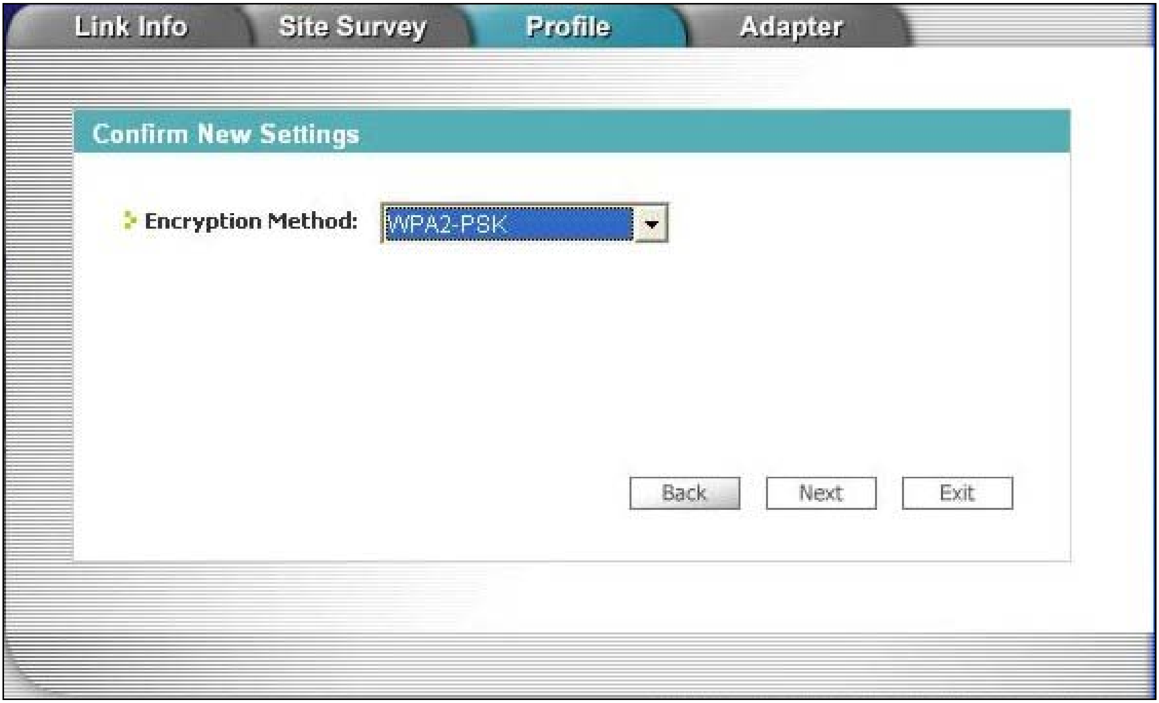


Confirm New Settings

Channel: 1

Figure 5-3 Profile: Select a Channel

Step 3. If you select **Infrastructure** network type in the first screen, select the same encryption method as the AP (**WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA**, **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 **WEP** encryption method. Otherwise, select **Disabled** to allow the G-162 to communicate with the access points or other peer wireless devices without any data encryption and skip to *Step 5*.

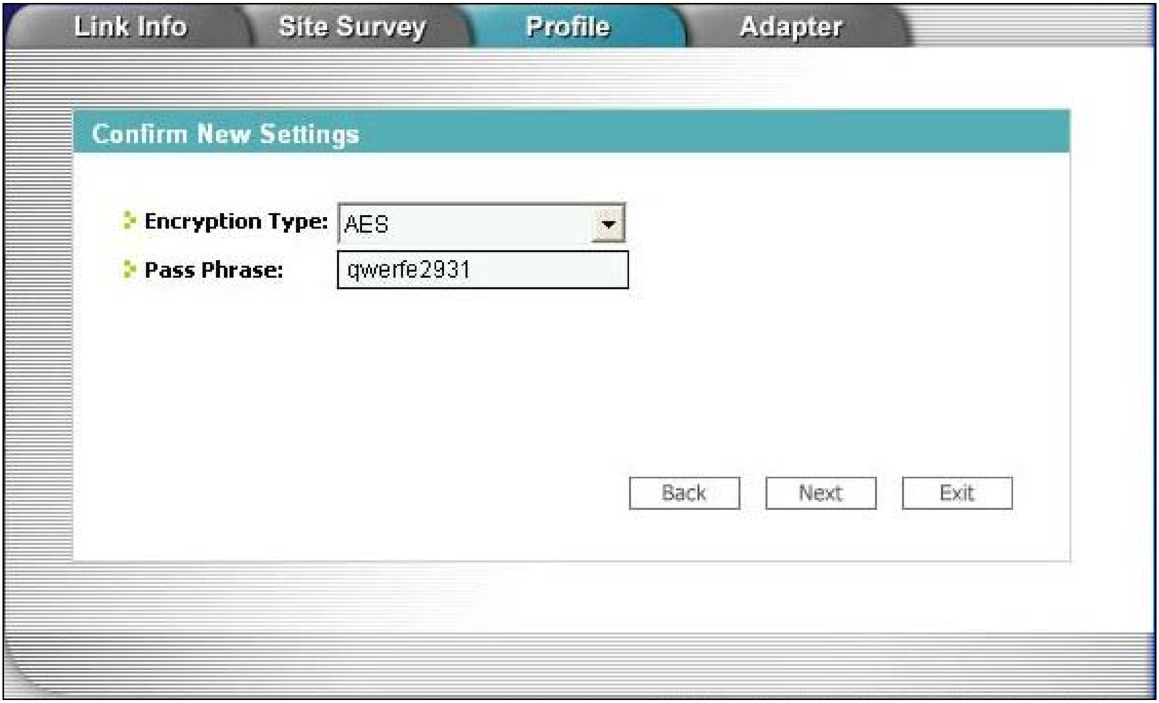


Confirm New Settings

Encryption Method: WPA2-PSK

Figure 5-4 Profile: Wireless Settings

Step 4. The screen varies depending on the encryption method you select in the previous screen. The settings must be exactly the same on the APs or other peer wireless devices as they are on the G-162. Refer to *Section 1.1* for detailed information on wireless security configuration.

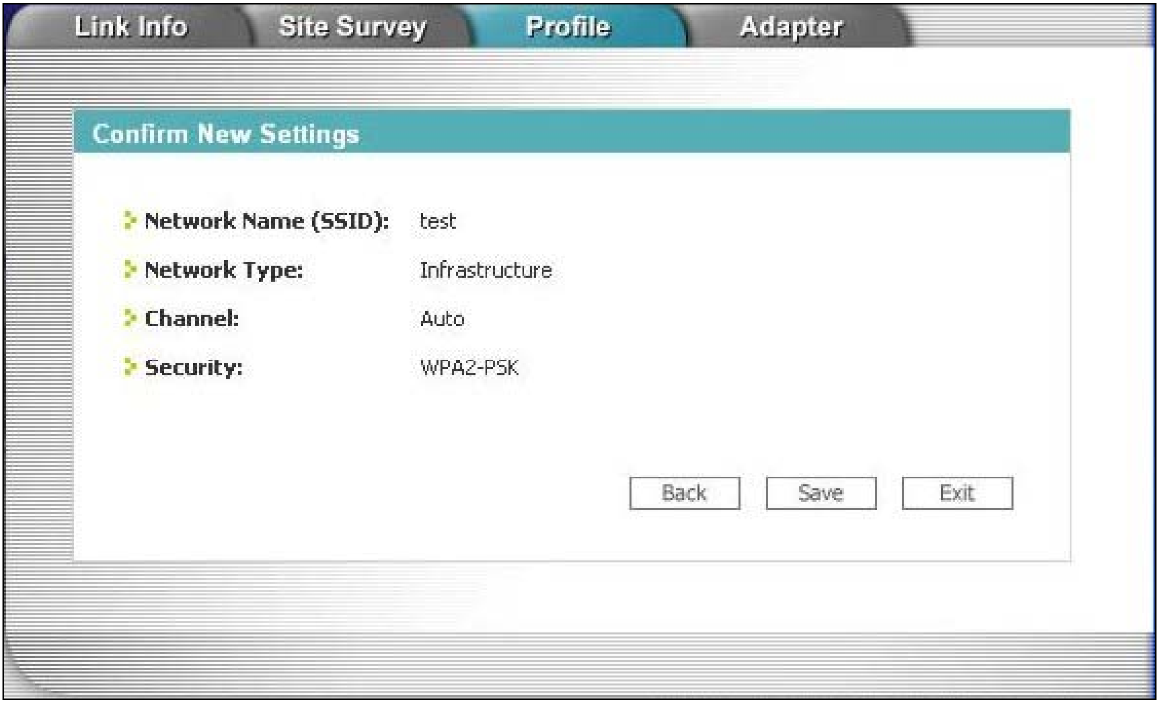


Encryption Type: AES

Pass Phrase: qwerfe2931

Figure 5-5 Profile: Security Settings

Step 5. This read-only screen shows a summary of the new profile settings. Verify that the settings are correct. 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.



Confirm New Settings

Network Name (SSID): test

Network Type: Infrastructure

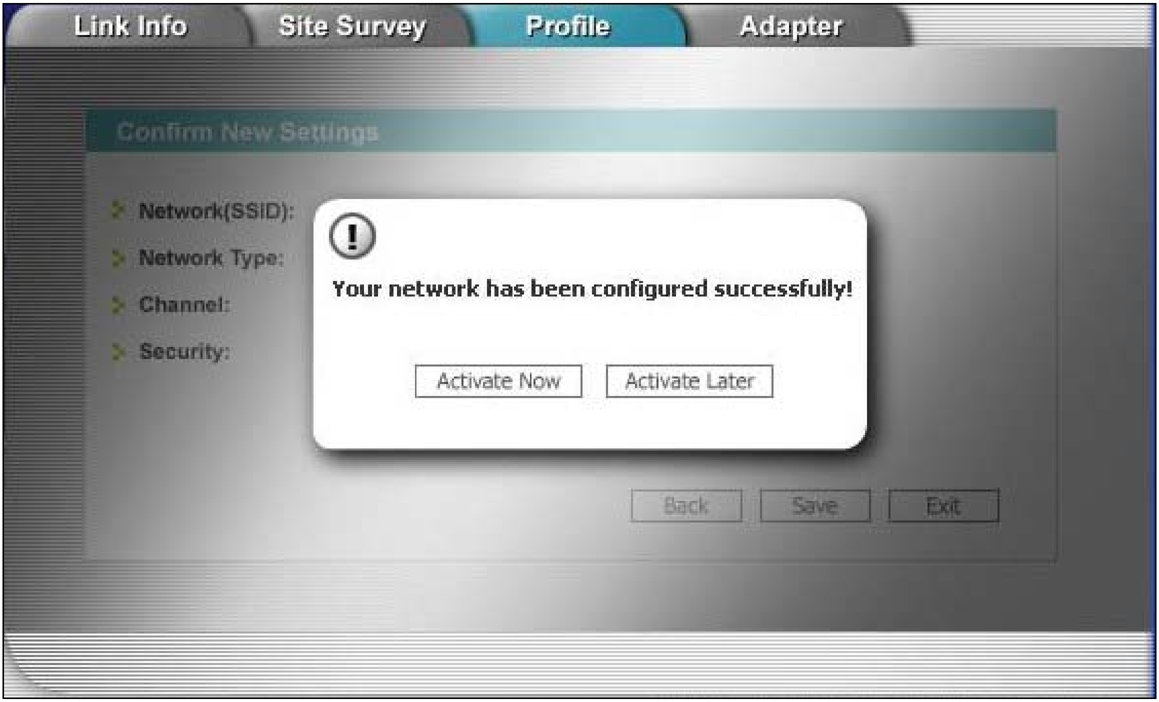
Channel: Auto

Security: WPA2-PSK

Figure 5-6 Profile: Confirm New Settings

Step 6. To use this network profile, click the **Activate Now** button. Otherwise, click the **Activate Later** button.

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



Your network has been configured successfully!

Figure 5-7 Profile: Activate the Profile

Chapter 6
Adapter

This chapter discusses OTIST and how to configure the ***Adapter*** *screen.*

6.1 Introduction to OTIST

In a wireless network, the wireless clients must have the same SSID and security settings as the access point (AP) or wireless router (we will refer to both as "AP" here) in order to associate with it. Traditionally this meant that you have to configure the settings on the AP and then manually configure the exact same settings on each wireless client.

OTIST (One-Touch Intelligent Security Technology) allows you to transfer your AP's SSID and WEP or WPA(2)-PSK security settings to wireless clients that support OTIST and are within transmission range. You can also choose to have OTIST generate a WPA(2)-PSK key for you if you didn't configure one manually.

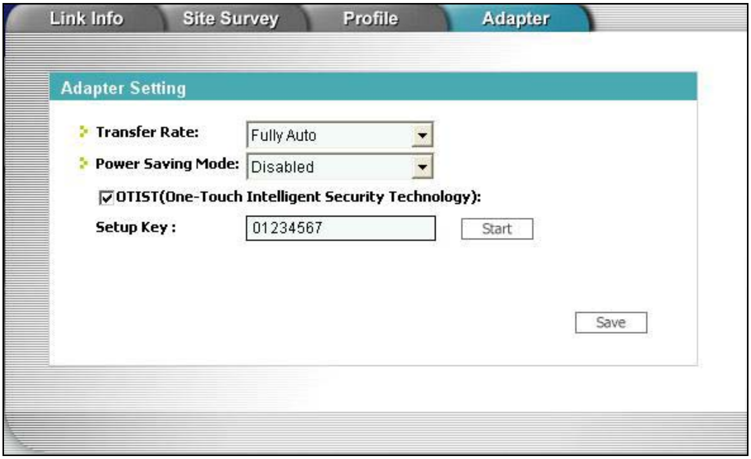
6.1.1 Enabling OTIST

You must enable OTIST on both the AP and wireless client before you start transferring settings.

The AP and wireless client(s) MUST use the same Setup Key**.**

Wireless Client

Start the ZyXEL Utility and click the **Adapter** tab. Select the **OTIST** check box, enter the same **Setup Key** as your AP's and click **Save**.



Transfer Rate: Fully Auto

Power Saving Mode: Disabled

☑ OTIST(One-Touch Intelligent Security Technology):

Setup Key : 01234567

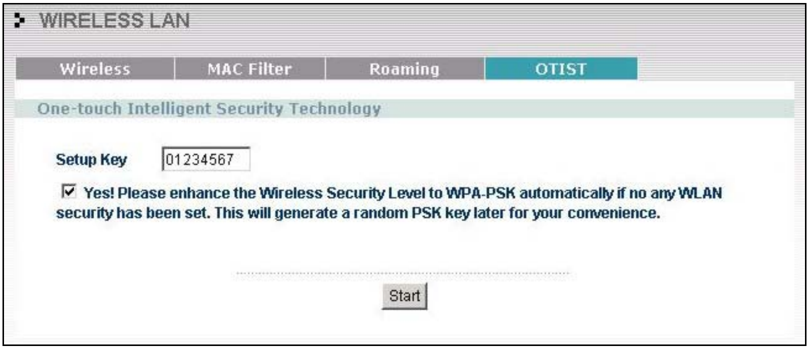
AP

You can enable OTIST using the reset button or the web configurator. If you use the reset button, the default (01234567) or previous saved (through the web configurator) **Setup Key** is used to encrypt the settings that you want to transfer.

Hold in the **Reset** button for one or two seconds.

If you hold in the Reset **button too long, the device will reset to the factory defaults!**

In the web configurator, go to the **Wireless LAN** main screen and then select **OTIST**. To change the **Setup Key**, enter up to eight printable characters. To have OTIST automatically generate a WPA(2)-PSK key, select the **Yes** check box. If you manually configured a WEP key or a WPA(2)-PSK key and you also selected this check box, then the key you manually configured is used.



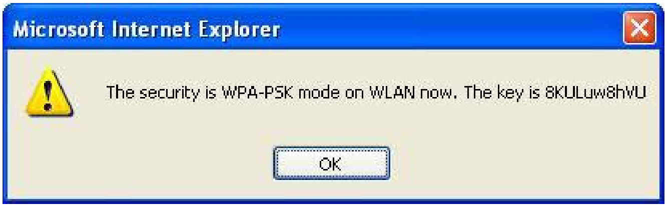
Setup Key 01234567

☑ Yes! Please enhance the Wireless Security Level to WPA-PSK automatically if no any WLAN security has been set. This will generate a random PSK key later for your convenience.

6.1.2 Starting OTIST

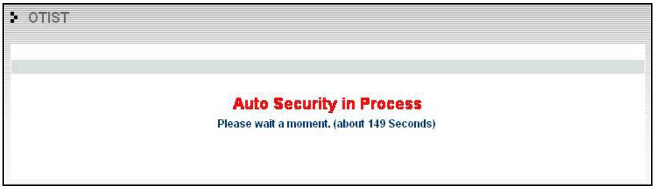
You must click **Start** in the AP **OTIST** web configurator screen and in the wireless client(s) **Adapter** screen all within three minutes (at the time of writing). You can start OTIST in the wireless clients and AP in any order but they must all be within range and have OTIST enabled.

1. In the AP, a web configurator screen pops up showing you the security settings to transfer. After reviewing the settings, click **OK**.



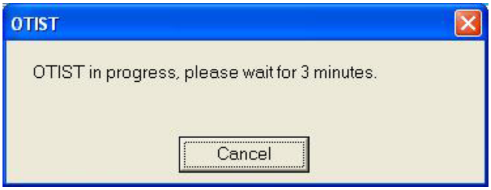
The security is WPA-PSK mode on WLAN now. The key is 8KULuw8hVU

2. This screen appears while OTIST settings are being transferred. It closes when the transfer is complete.



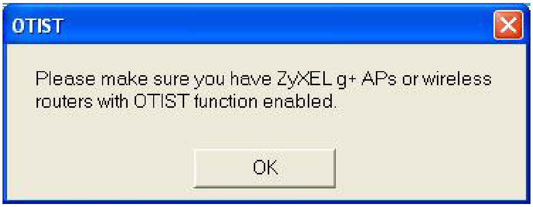
Auto Security in Process

Please wait a moment. (about 149 Seconds)



OTIST in progress, please wait for 3 minutes.

- In the wireless client, you see this screen if it can't find an OTIST-enabled AP (with the same **Setup Key**). Click **OK** to go back to the ZyXEL Utility main screen.

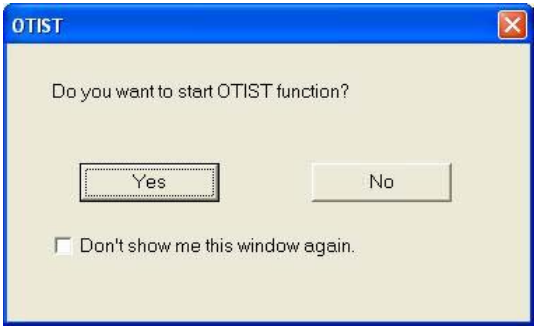


Please make sure you have ZyXEL g+ APs or wireless routers with OTIST function enabled.

- If there is more than one OTIST-enabled AP within range, you see a screen asking you to select one AP to get settings from.

6.1.3 Notes on OTIST

1. If you enabled OTIST in the wireless client, you see this screen each time you start the ZyXEL Utility. Click **Yes** for it to search for an OTIST-enabled AP.



Do you want to start OTIST function?

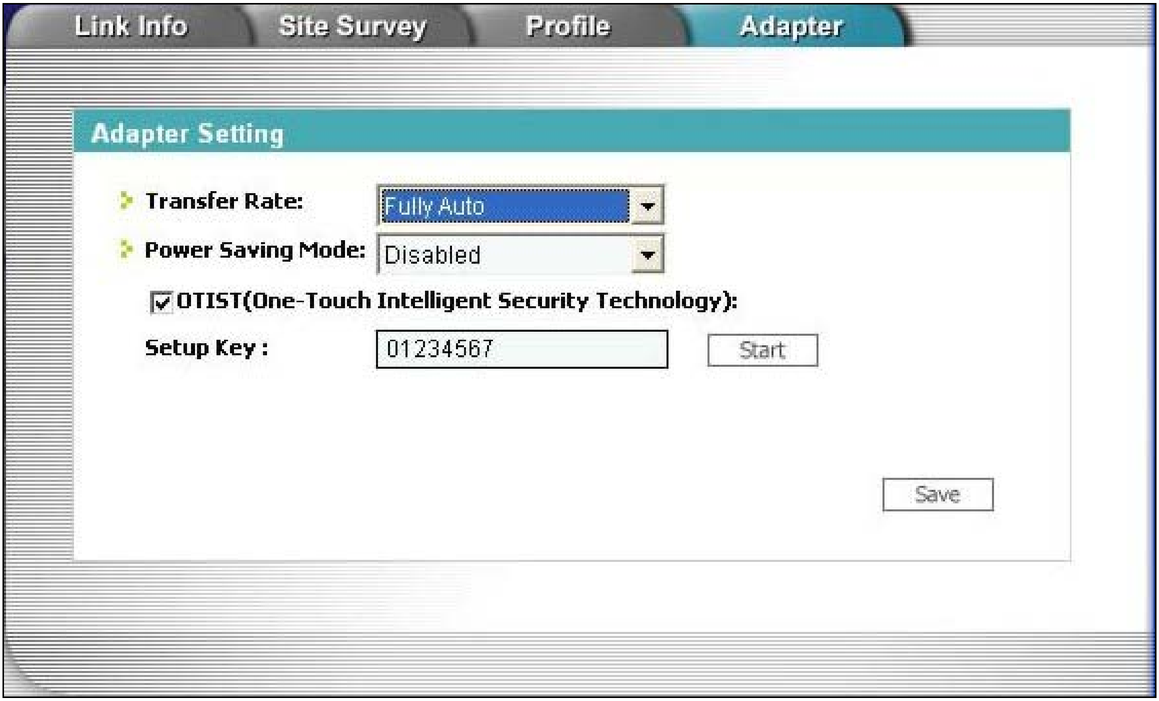
□ Don't show me this window again.

2. If an OTIST-enabled wireless client loses its wireless connection for more than ten seconds, it will search for an OTIST-enabled AP for up to one minute. (If you manually have the wireless client search for an OTIST-enabled AP, there is no timeout; click **Cancel** in the OTIST progress screen to stop the search.)
3. When the wireless client finds an OTIST-enabled AP, you must still click **Start** in the AP OTIST web configurator screen or hold in the **Reset** button (for one or two seconds) for the AP to transfer settings.

4. If you change the SSID or the keys on the AP after using OTIST, you need to run OTIST again or enter them manually in the wireless client(s).
5. If you configure OTIST to generate a WPA(2)-PSK key, this key changes each time you run OTIST. Therefore, if a new wireless client joins your wireless network, you need to run OTIST on the AP and ALL the wireless clients again.

6.2 Configuring the Adapter Screen

Use the **Adapter** screen to set a transfer rate, enable power saving and activate OTIST.



Transfer Rate: Fully Auto

Power Saving Mode: Disabled

☑ OTIST(One-Touch Intelligent Security Technology):

Setup Key : 01234567

Figure 6-1 Adapter

The following table describes the labels in this screen.

Table 6-1 Adapter

LABEL	DESCRIPTION
Adapter Setting	

Table 6-1 Adapter

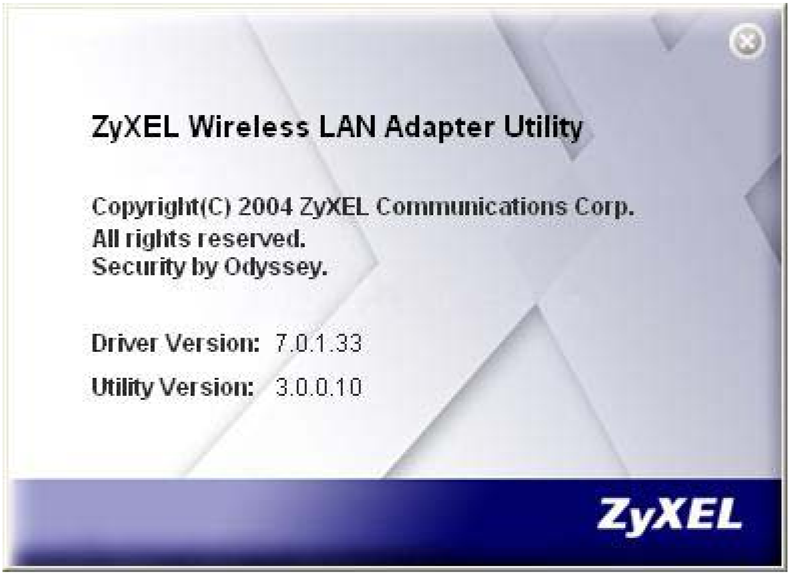
LABEL	DESCRIPTION
Transfer Rate	Select a transmission speed from the drop-down list box. Options are **Fully Auto** (default), **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **11 Mbps**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **22 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, **54 Mbps** and **125 Mbps**. Select **Fully Auto** to allow your G-162 to operate at the maximum available transmission rate. Otherwise, select a number based on your network environment.
Power Saving Mode	Power consumption is reduced (especially good for notebooks that use batteries) in power saving mode. Select **Enabled** and then click **Save** to immediately cut wireless transmission to/from the G-162. If the G-162 resides in a Windows 98 computer, it may also reboot. The G-162 remains in power saving mode until there is traffic to transmit or receive. Otherwise, select **Disabled**.
OTIST (One-Touch Intelligent Security Technology)	Select this check box to enable OTIST.
Setup Key	Enter the same setup key (of exactly eight ASCII characters) as the OTIST-enabled AP or wireless router to which you want to associate. The default OTIST setup key is "01234567". **If you change the OTIST setup key on the OTIST-enabled AP, you must also make the same change here.**
Start	Click **Start** to encrypt the wireless security data using the setup key and have the OTIST-enabled AP set your G-162 to use the same wireless settings as the OTIST-enabled AP or wireless router. You must also activate and start OTIST on the OTIST-enabled AP at the same time. The process takes about three minutes to complete.
Save	Click **Save** to save the changes.

Chapter 7
Maintenance

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

7.1 The About Screen

The **About** screen displays related version numbers of the G-162. To display the screen as shown next, click the about (📄) button.



ZyXEL Wireless LAN Adapter Utility

Copyright(C) 2004 ZyXEL Communications Corp.
All rights reserved.
Security by Odyssey.

Driver Version: 7.0.1.33

Utility Version: 3.0.0.10

Figure 7-1 About

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

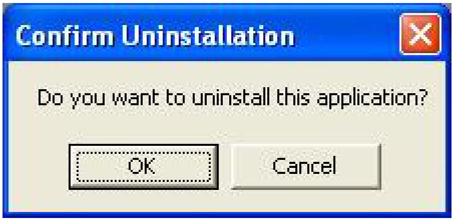
Table 7-1 About

LABEL	DESCRIPTION
Driver Version	This field displays the version number of the ZyXEL driver.
Utility Version	This field displays the version number of the ZyXEL Utility.

7.2 Uninstalling the ZyXEL Utility

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

1. Click **Start**, **Programs**, **ZyXEL G-162 802.11g Wireless CardBus Card**, **Uninstall**.
2. When prompted, click **OK** to remove the driver and the utility software.



Confirm Uninstallation

Do you want to uninstall this application?

Figure 7-2 Confirm Uninstall

3. Restart your computer if prompted.

7.3 Upgrading the ZyXEL Utility

Before you install the new ZyXEL Utility, take note of the current network configuration and uninstall the existing utility on your computer.

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 7.2* to remove the current ZyXEL Utility from your computer.
3. Restart your computer if prompted.
4. After restarting, refer to the procedure in the Quick Start Guide to install the new utility.
5. Check the version numbers in the **About** screen to make sure the new utility is installed properly.

Chapter 8
Troubleshooting

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

8.1 Problems Starting the ZyXEL Utility Program

Table 8-1 Troubleshooting Starting ZyXEL Utility Program

PROBLEM	CORRECTIVE ACTION
Cannot start the ZyXEL Utility	Make sure the G-162 is properly inserted and the LED(s) is on. Refer to the *Quick Start Guide* for the LED descriptions.
	Use the **Device Manager** to check for possible hardware conflicts. Click **Start**, **Settings**, **Control Panel**, **System**, **Hardware** and **Device Manager**. Verify the status of the G-162 under **Network Adapter**. (Steps may vary depending on the version of Windows).
	Install the G-162 in another computer. If the error persists, you may have a hardware problem. In this case, you should contact your local vendor.
The ZyXEL Utility icon does not display.	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. If you use the Windows XP configuration tool and the ZyXEL Utility to configure the G-162 at the same time, the ZyXEL Utility icon does not display. You need to disable the Windows XP configuration tool (refer to *Appendix B* for more information).

8.2 Problem with the Link Status

Table 8-2 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
The link quality and/or signal strength is poor all the time.	Search and connect to another AP with a better link quality using the **Site Survey** screen. Move your computer closer to the AP or the peer computer(s) within the transmission range. There may be too much radio interference (for example microwave or another AP using the same channel) around your wireless network. Relocate or reduce the radio interference.

8.3 Problems Communicating With Other Computers

Table 8-3 Troubleshooting Communication Problems

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

8.4 Related Documentation

- Support Disk

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

- Quick Start Guide

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

- ZyXEL Glossary and Web Site

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

8.5 User Guide Feedback

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

8.6 Customer Support

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

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

METHOD / LOCATION	SUPPORT E-MAIL	TELEPHONE[1]	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 – Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		

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

METHOD	SUPPORT E-MAIL	TELEPHONE[1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11, The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

Appendix A
Product Specifications

Product Name	ZyXEL G-162 802.11g Wireless CardBus Card
Type	3.3V 32-bit CardBus card
Standards	IEEE 802.11b IEEE 802.11g
Network Architectures	Infrastructure Ad-Hoc
Operating Frequencies	2.412-2.483GHz (Industrial Scientific Medical Band)
Operating Channels	IEEE 802.11b: 11 Channels (North America) IEEE 802.11g: 11 Channels (North America) IEEE 802.11b: 13 Channels (Europe) IEEE 802.11g: 13 Channels (Europe)
Data Rate	IEEE 802.11b: 22, 11, 5.5, 2, 1Mbps IEEE 802.11g: 125, 54, 48, 36, 24, 18, 12, 9, 6 Mbps
Modulation	IEEE 802.11g: Orthogonal Frequency Division Multiplexing (64QAM, 16QAM, QPSK and BPSK) IEEE 802.11b: PBCC, Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).
Security	64/128/256-bit WEP, 802.1x, WPA-PSK, WPA, WPA2-PSK, WPA2
Operating Temperature	0 ~ 50 degrees Centigrade
Storage Temperature	-30 ~ 60 degrees Centigrade
Operating Humidity	20 ~ 95% (non-condensing)
Storage Humidity	20 ~ 95% (non-condensing)
Power Consumption	IEEE 802.11g: TX: 600mA RX: 450mA (max.) IEEE 802.11b: TX: 600mA RX: 450mA (max.)
Voltage	3.3V±5%
Weight	< 50g
Dimension	(W) 115 mm × (D) 54.5 mm × (H) 9.3 mm

Output Power	17 dBm (typical) at 11Mbps DBPSK, DQPSK, CCK 14 dBm (typical) at 54Mbps OFDM
RX Sensitivity	802.11g (OFDM): 54 Mbps: < -68 dBm (typ.) < -69 dBM (max.) 802.11b (PBCC): 22 Mbps: < -83 dBm (typ.) < -88 dBM (max.)
Temperature	Operating: 0° ~ 50° C Storage: -30° ~ 60° C
Relative Humidity	20% to 95% (non-condensing)

Appendix B Disable Windows XP Wireless LAN Configuration Tool

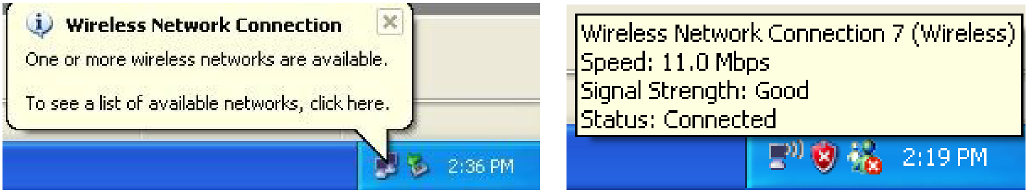
Windows XP includes a configuration tool (also known as Wireless Zero Configuration (WZC)) for wireless devices.

Follow the steps below to disable the configuration tool in Windows XP after you install the ZyXEL Utility. The screen varies depending on the version of Windows XP service pack.

Via the Wireless Network System Tray Icon

If the network icon for wireless connections is not present in the system tray, see the next section.

1. Double-click the network icon for wireless connections in the system tray.



Wireless Network Connection

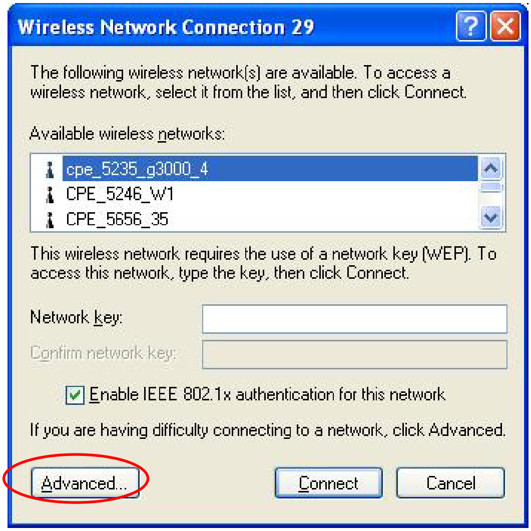
One or more wireless networks are available.

To see a list of available networks, click here.

Wireless Network Connection 7 (Wireless)
Speed: 11.0 Mbps
Signal Strength: Good
Status: Connected

Diagram 1 Windows XP: System Tray Icon

2. Windows XP SP1: When a **Wireless Network Connection** window displays, click **Advanced…**.



Wireless Network Connection 29

The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.

Available wireless networks:

- cpe_5235_g3000_4
- CPE_5246_W1
- CPE_5656_35

This wireless network requires the use of a network key (WEP). To access this network, type the key, then click Connect.

Network key:

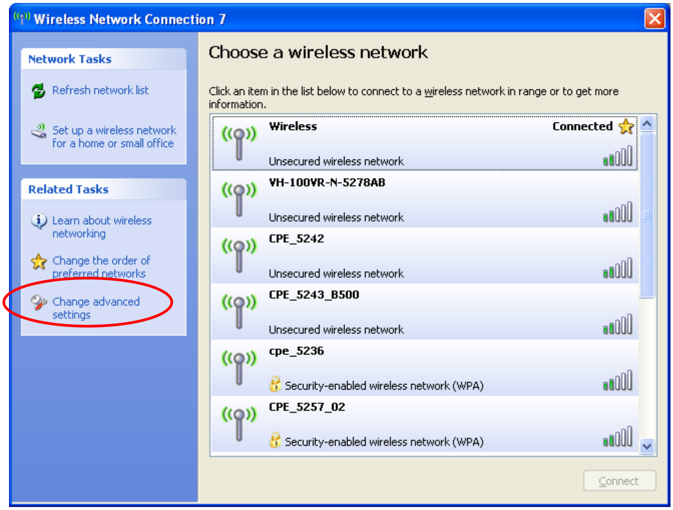
Confirm network key:

☑ Enable IEEE 802.1x authentication for this network

If you are having difficulty connecting to a network, click Advanced.

Diagram 2 Windows XP SP1: Wireless Network Connection

Windows XP SP2: When a **Wireless Network Connection** window displays, click **Change advanced settings** under **Related Tasks** and then the **Wireless Networks** tab.



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

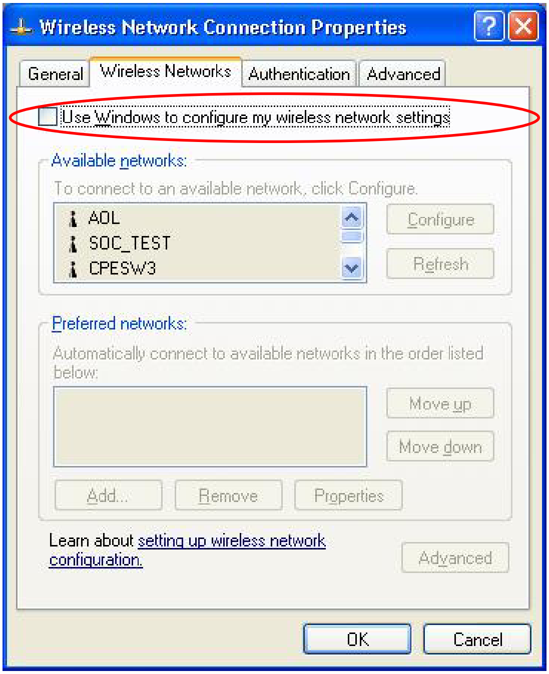
Choose a wireless network

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
VH-100VR-N-5278AB	Unsecured wireless network	
CPE_5242	Unsecured wireless network	
CPE_5243_B500	Unsecured wireless network	
cpe_5236	Security-enabled wireless network (WPA)	
CPE_5257_02	Security-enabled wireless network (WPA)	

Diagram 3 Windows XP SP2: Wireless Network Connection

3. In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is *not* selected. Click **OK**.



Wireless Network Connection Properties

General | Wireless Networks | Authentication | Advanced

□ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

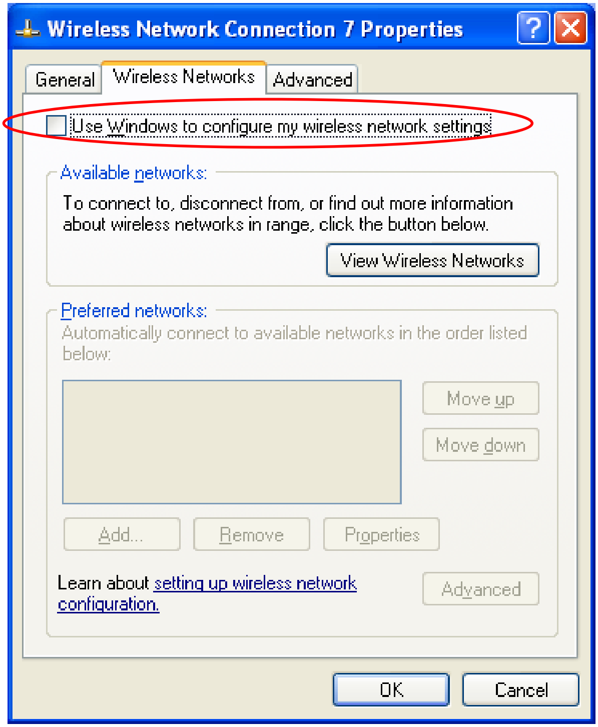
- AOL
- SOC_TEST
- CPESW3

Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

Diagram 4 Windows XP SP1: 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:

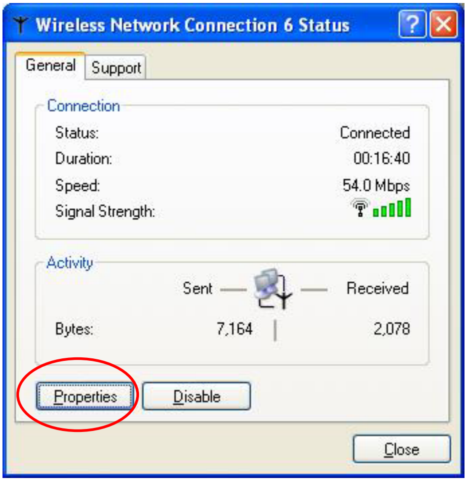
Learn about setting up wireless network configuration.

Diagram 5 Windows XP SP2: Wireless Network Connection Properties

Via the Control Panel

1. If the icon for the wireless network connection is not in the system tray, click **Start**, **Control Panel** and double-click **Network Connections**.

2. Double-click on the icon for wireless network connection to display a status window as shown below.



Wireless Network Connection 6 Status

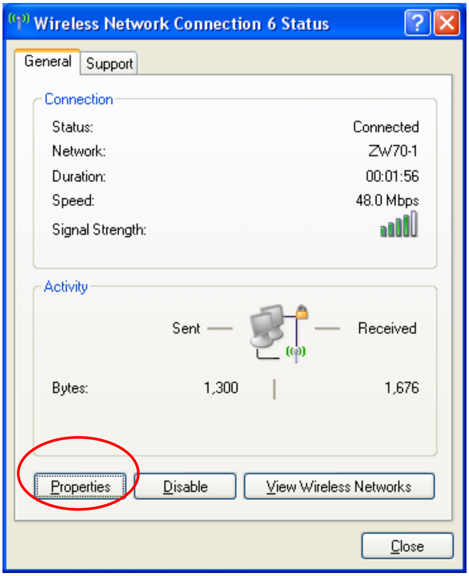
Connection

Status: Connected
Duration: 00:16:40
Speed: 54.0 Mbps
Signal Strength:

Activity

Bytes: Sent 7,164 Received 2,078

Diagram 6 Windows XP SP1: Wireless Network Connection Status



Wireless Network Connection 6 Status

Connection

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

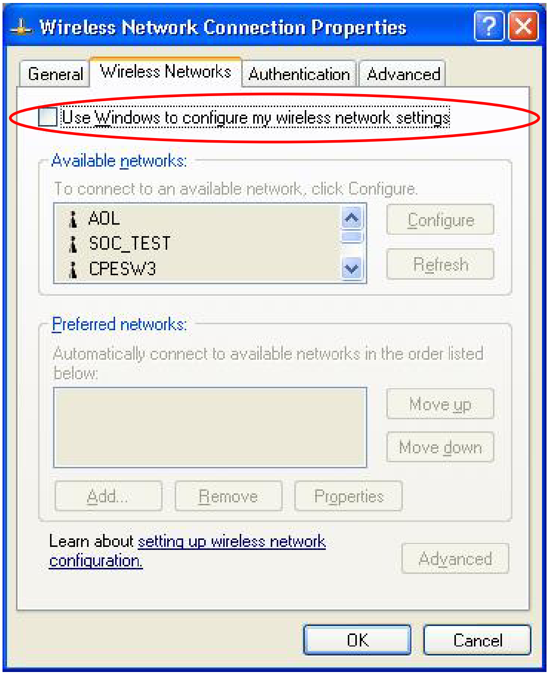
Activity

Bytes: Sent 1,300 Received 1,676

Diagram 7 Windows XP SP2: Wireless Network Connection Status

3. Click **Properties** and click the **Wireless Networks** tab.

4. In the **Wireless Network Connection Properties** window, make sure the **Use Windows to configure my wireless network settings** check box is *not* selected. Click **OK**.



Wireless Network Connection Properties

□ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

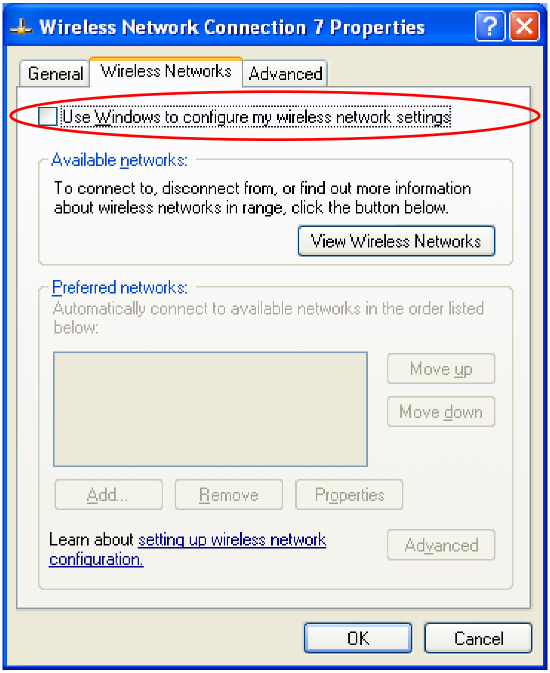
AOL
SOC_TEST
CPESW3

Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

Diagram 8 Windows XP SP1: 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.

Diagram 9 Windows XP SP2: Wireless Network Connection Properties

Appendix C Management with Wireless Zero Configuration

This appendix shows you how to manage your G-162 using the Windows XP wireless zero configuration tool.

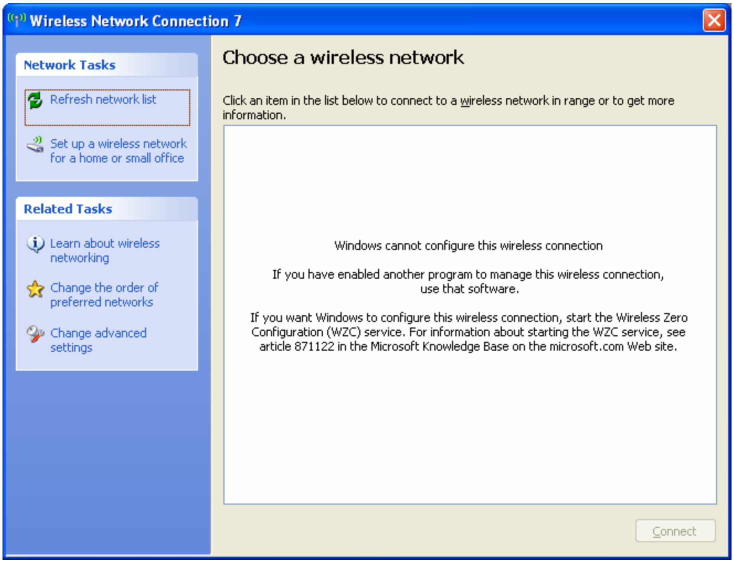
Be sure you have the Windows XP service pack 2 installed on your computer. Otherwise, you should at least have the Windows XP service pack 1 already on your computer and download the support patch for WPA from the Microsoft web site.

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

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

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



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

Choose a wireless network

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

Windows cannot configure this wireless connection

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

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

Diagram 10 Windows XP SP2: WZC Not Available

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.

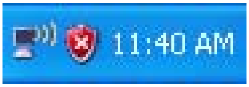
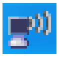
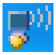
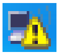
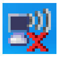


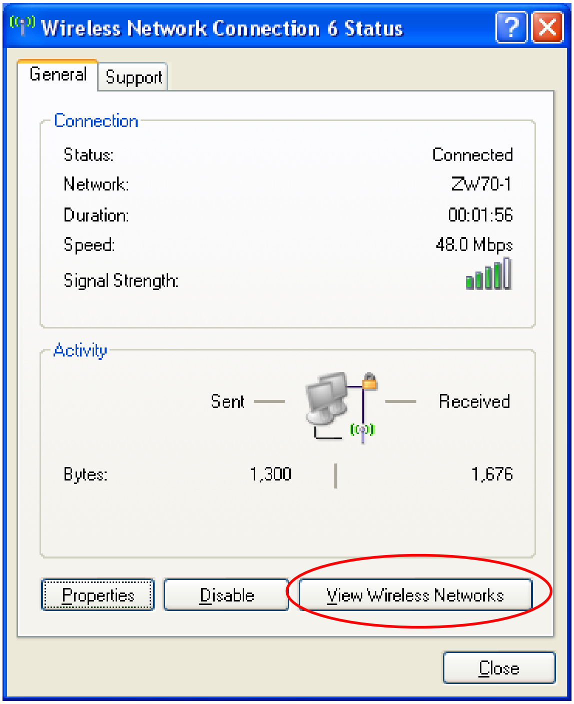
Diagram 11 Windows XP SP2: System Tray Icon

The type of the wireless network icon in Windows XP SP2 indicates the status of the G-162. Refer to the following table for details.

Chart 1 Windows XP SP2: System Tray Icon

ICON	DESCRIPTION
	The G-162 is connected to a wireless network.
	The G-162 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-162 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.



Wireless Network Connection 6 Status

Connection

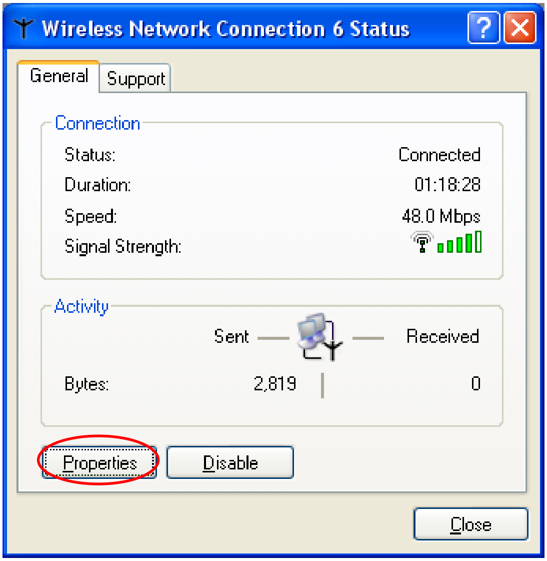
Status: Connected
Network: Zw70-1
Duration: 00:01:56
Speed: 48.0 Mbps
Signal Strength:

Activity

Bytes: Sent 1,300 Received 1,676

Diagram 12 Windows XP SP2: Wireless Network Connection Status

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.



Connection

Status: Connected

Duration: 01:18:28

Speed: 48.0 Mbps

Signal Strength:

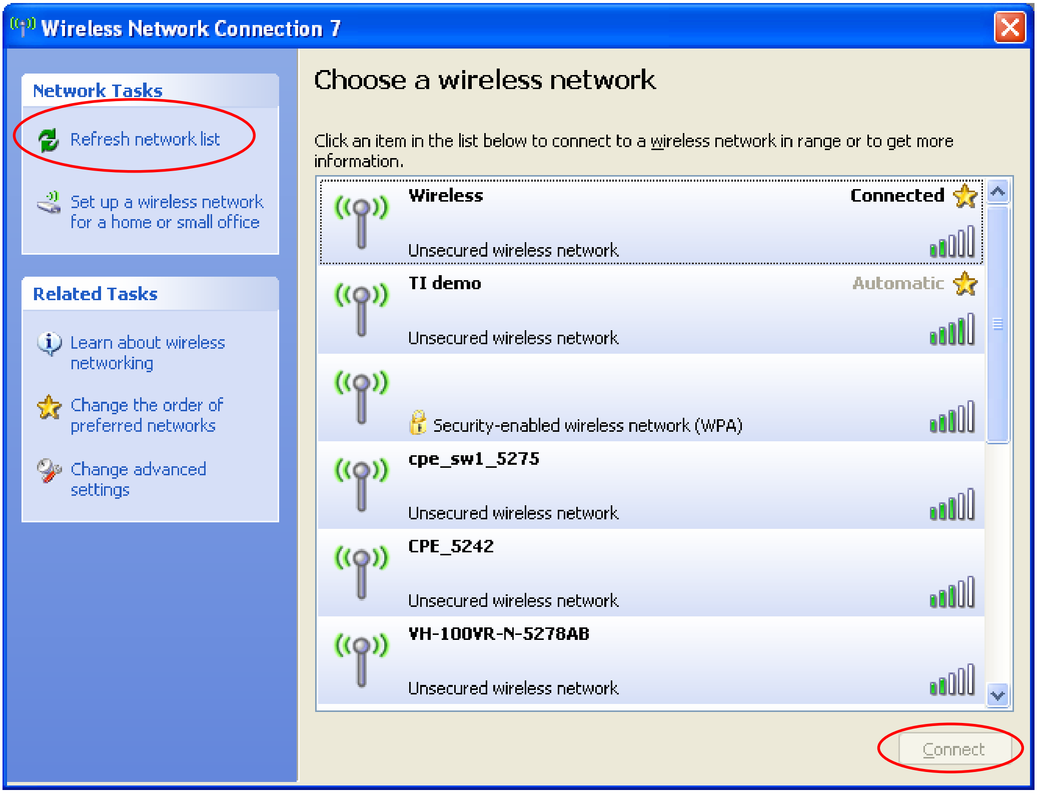
Activity

Sent — Received

Bytes: 2,819 | 0

Diagram 13 Windows XP SP1: Wireless Network Connection Status

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.


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
Connect

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

Wireless — Connected — Unsecured wireless network

TI demo — Automatic — Unsecured wireless network

Security-enabled wireless network (WPA)

cpe_sw1_5275 — Unsecured wireless network

CPE_5242 — Unsecured wireless network

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

Diagram 14 Windows XP SP2: Wireless Network Connection

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

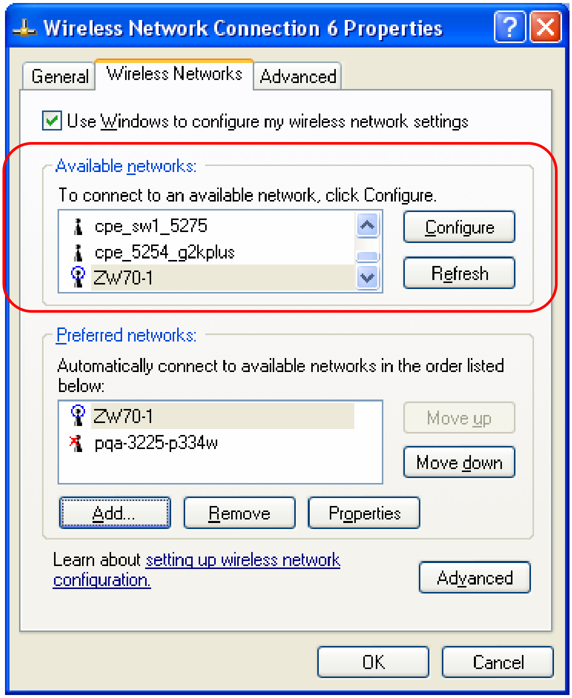
Chart 2 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
🔒	This denotes that wireless security is activated for the wireless network.

Chart 2 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
★	This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the G-162 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.



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

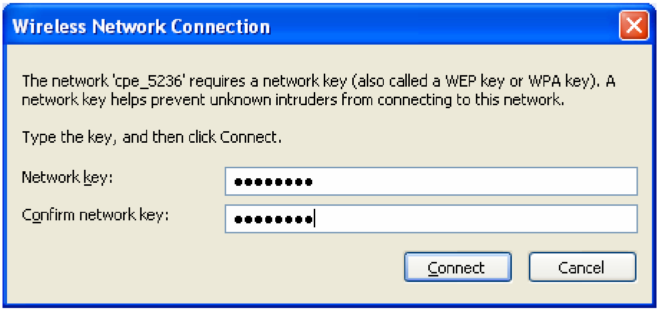
Learn about setting up wireless network configuration.

Advanced

OK | Cancel

Diagram 15 Windows XP SP1: Wireless Network Connection Properties

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. Refer to *Section 0* 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.



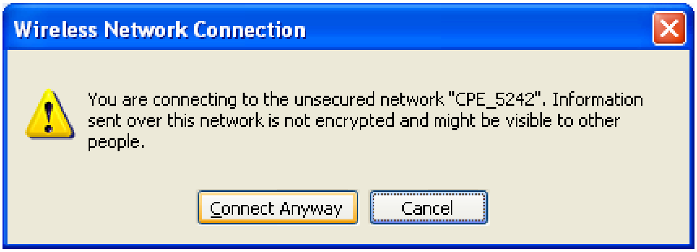
The network 'cpe_5236' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Diagram 16 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK



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

Diagram 17 Windows XP SP2: Wireless Network Connection: No Security

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.

Chart 3 Windows XP: Wireless Networks

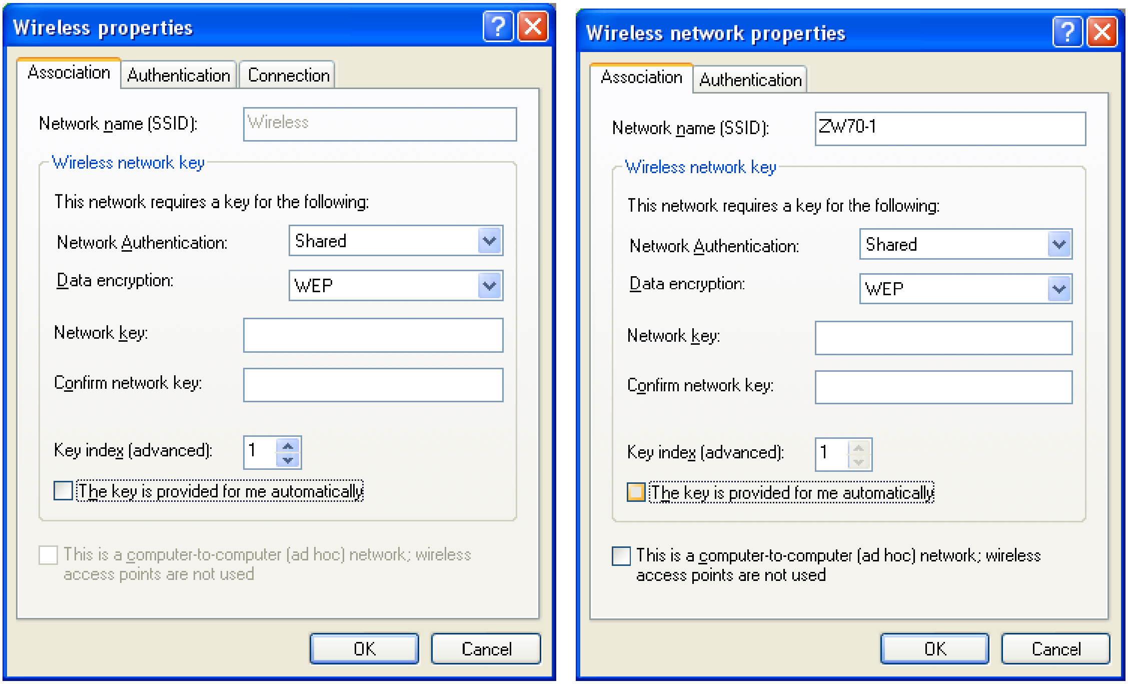
ICON	DESCRIPTION
📶	This denotes the wireless network is an available wireless network.
◎	This denotes the G-162 is associated to the wireless network.
✗	This denotes the wireless network is not available.

Security Settings

When you configure the G-162 to connect to a secure network but the security settings are not yet enabled on the G-162, 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.



Wireless properties

Network name (SSID): Wireless

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

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

Diagram 18 Windows XP: Wireless (network) properties: Association

The following table describes the labels in this screen.

Chart 4 Windows XP: Wireless (network) properties: Association

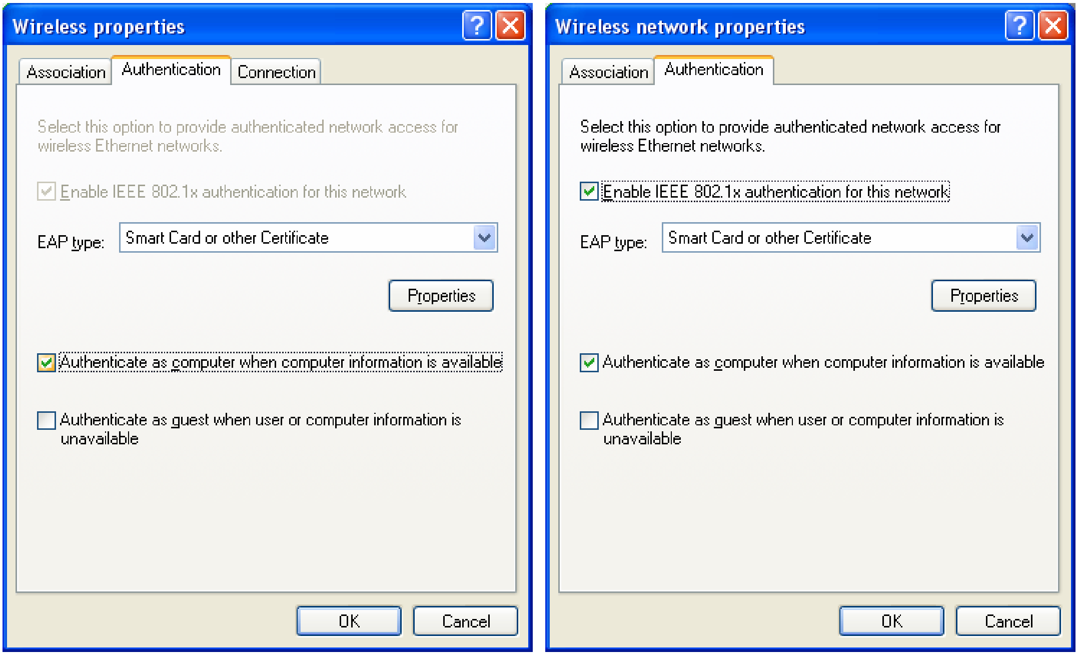
LABEL	DESCRIPTION
Network name (SSID)	This field displays the SSID (Service Set IDentifier) of each wireless network.

Chart 4 Windows XP: Wireless (network) properties: Association

LABEL	DESCRIPTION
Network Authentication	This field automatically shows the authentication method (**Share**, **Open**, **WPA** or **WPA-PSK**) used by the selected network. Refer to *Section 4.2* for more information.
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-162 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.



Wireless properties

Association | Authentication | Connection

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

Properties

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

OK | Cancel

Wireless network properties

Association | 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

Properties

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

OK | Cancel

Diagram 19 Windows XP: Wireless (network) properties: Authentication

The following table describes the labels in this screen.

Chart 5 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.

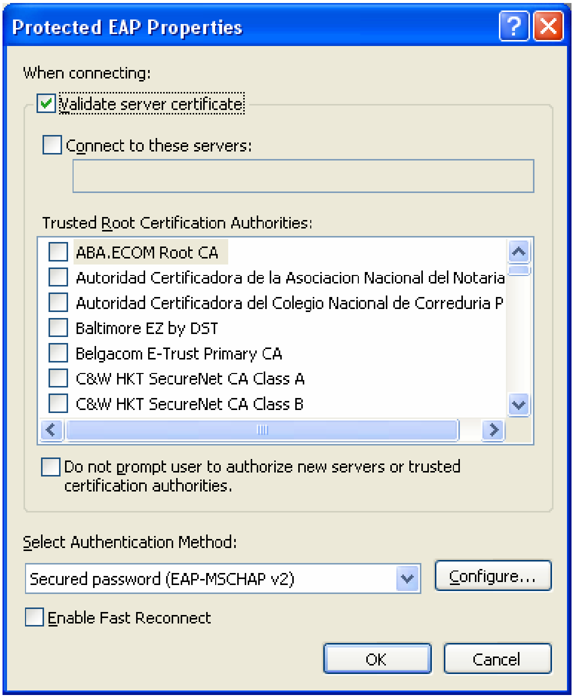
Chart 5 Windows XP: Wireless (network) properties: Authentication

LABEL	DESCRIPTION
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 close 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



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

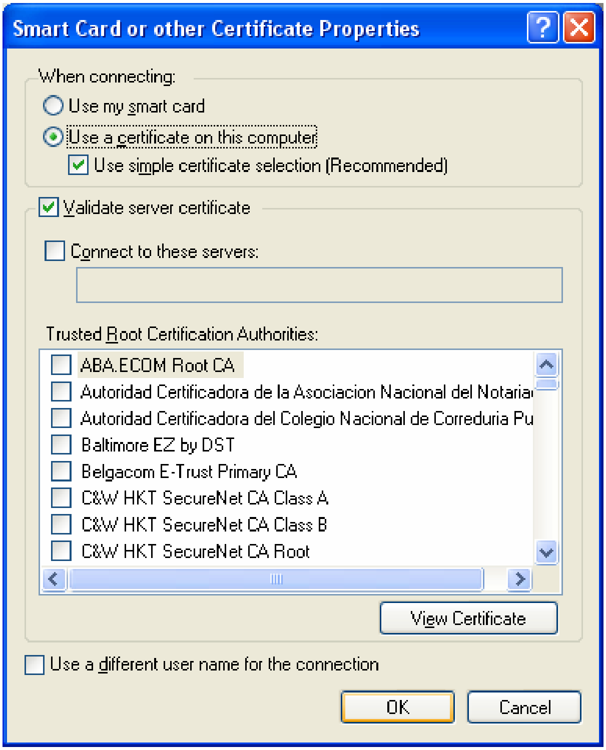
Diagram 20 Windows XP: Protected EAP Properties

The following table describes the labels in this screen.

Chart 6 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. **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.
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



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

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

□ Use a different user name for the connection

Diagram 21 Windows XP: Smart Card or other Certificate Properties

The following table describes the labels in this screen.

Chart 7 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.

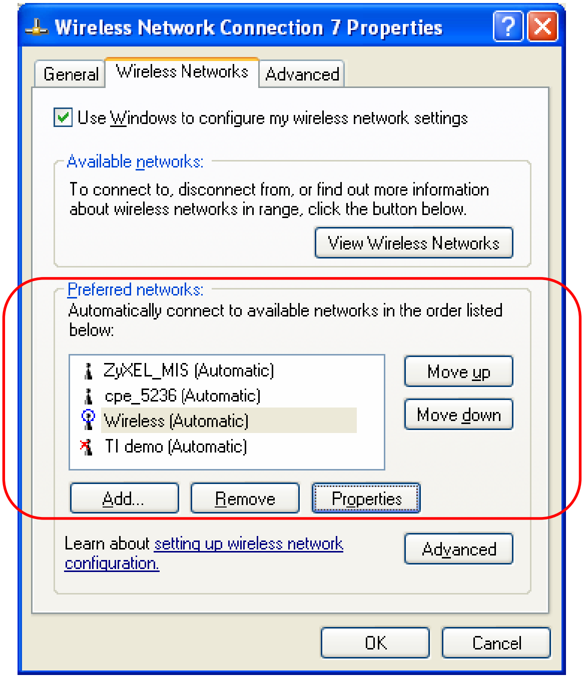
Chart 7 Windows XP: Smart Card or other Certificate Properties

LABEL	DESCRIPTION
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. **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.
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 *Diagram 14*). The screen displays as shown.



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:

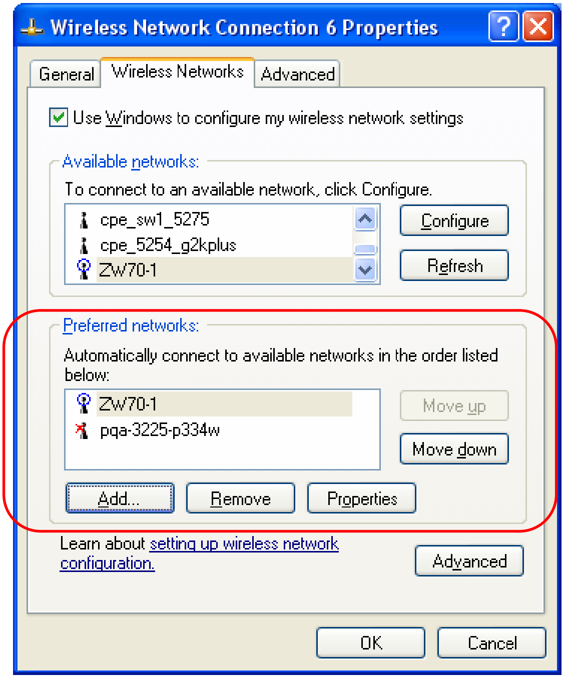
Automatically connect to available networks in the order listed below:

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

Learn about setting up wireless network configuration.

Diagram 22 Windows XP SP2: Wireless Networks: Preferred Networks

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



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- cpe_sw1_5275
- cpe_5254_g2kplus
- ZW70-1

Preferred networks:

Automatically connect to available networks in the order listed below:

- ZW70-1
- pqa-3225-p334w

Learn about setting up wireless network configuration.

Diagram 23 Windows XP SP1: Wireless Networks: Preferred Networks

2. Whenever the G-162 tries to connect to a new network, the new network is added in the **Preferred networks** table automatically. Select a network and click **Move up** or **Move down** to change it's order, click **Remove** to delete it or click **Properties** to view the security, authentication or connection information of the selected network. Click **Add** to add a preferred network into the list manually.

Appendix D
Wireless LANs

Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-Hoc (IBSS)

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless clients. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN. Ad-hoc mode does not require an AP or a wired network.

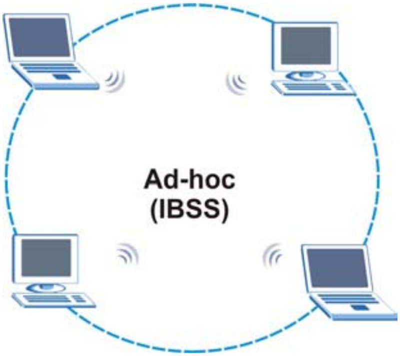


Diagram 24 IBSS Example

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

Infrastructure (BSS)

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

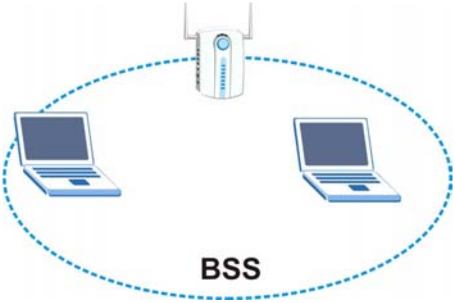


Diagram 25 BSS Example

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

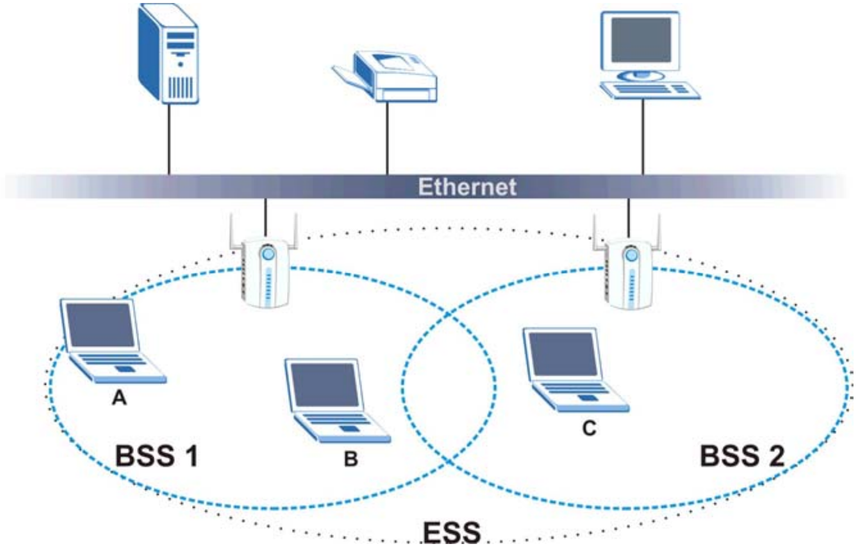


Diagram 26 Infrastructure Network Example

IEEE 802.1x

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

EAP Authentication

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

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

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA 2 (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.

Encryption

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

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

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

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

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

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

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

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.

WPA(2)-PSK Application Example

A WPA(2)-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 (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

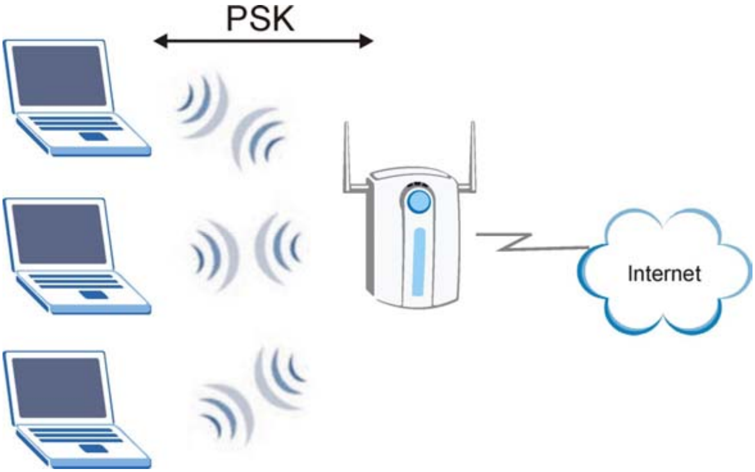


Diagram 27 WPA(2)-PSK Authentication

WPA(2) with RADIUS Application Example

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

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

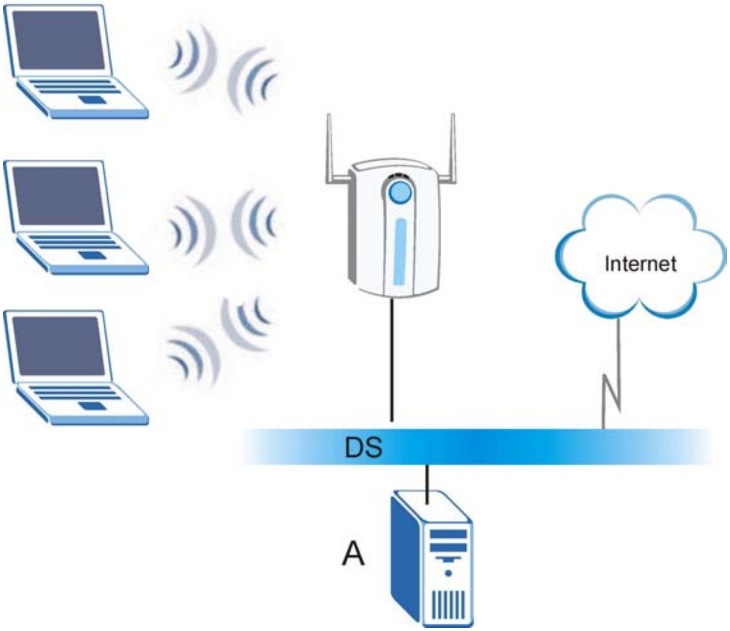


Diagram 28 WPA(2) with RADIUS Application Example

Appendix E Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client '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 clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

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

PEAP (Protected EAP)

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

LEAP

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

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

Comparison of EAP Authentication Types

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

Appendix F Index