#### Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

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

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

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

#### **User Authentication**

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

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

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

#### **Wireless Client WPA Supplicants**

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

#### WPA(2) with RADIUS Application Example

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

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- **2** The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- **3** A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- **4** The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

#### Figure 89 WPA(2) with RADIUS Application Example



#### 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 or 64 hexadecimal characters (including spaces and symbols).
- **2** The AP checks each wireless client's password and allows it to join the network only if the password matches.

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



#### Figure 90 WPA(2)-PSK Authentication

# **Security Parameters Summary**

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

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

**Table 25** Wireless Security Relational Matrix

# Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

# **Antenna Characteristics**

#### Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

#### **Radiation Pattern**

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

#### Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

# **Types of Antennas for WLAN**

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

# **Positioning Antennas**

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to-point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

C

# **Windows Wireless Management**

This appendix shows you how to manage your NWD210N using the Windows Vista and Windows XP wireless configuration tools.

# Windows Vista

Take the following steps to connect to a wireless network using the Windows Vista wireless configuration tool (WLAN AutoConfig).

#### **Connecting to a Wireless Network**

1 In the Windows Vista taskbar, click Start ( 🚱 ) > Connect To.





The Connect To window displays, showing all available networks.

Select a	network to cor	nnect to	
Sho	w	•	
Dial-up	and VPN		· ·
2	ADSL	PPPoE Connection	-
Wireless	Network Connectio	n	· ·
4	Ad-Hoc	Security-enabled network	Utre-
<u>.</u>	ZyXEL_WLAN	Security-enabled network	- 1111-
Set up a c	onnection or netwo	<u>rk</u>	

#### Figure 92 Vista: The Connect To Window

The security status of each wireless network displays, as well as an indication of its signal strength. If you use the mouse pointer to hover over a network's entry, additional information about the network displays.

#### Figure 93 Vista: Additional Information



2 Double-click the network's name to join the network, or select a network and click **Connect**.



If the network to which you want to connect does not display, see the section on setting up a connection manually on page 120.

**3** If security is enabled, you may be prompted to enter your security key.

Genect to a network	
Type the network security key or passphrase for ZyXEL_WLAN	
The person who setup the network can give you the key or passphrase.	
Security key or passphrase:	
Display characters	
If you have a USB flash drive with network settings for ZyXEL_WLAN, insert it now	ι.
Connect	Cancel

Figure 94 Vista: Enter Security Key

Your computer tries to connect to the wireless network.

#### Figure 95 Vista: Connecting

Connect to a network	
Connecting to ZyXEL_WLAN	
i 🔍 💐	
	Cancel

If your computer has connected to the wireless network successfully, the following screen displays.



Figure 96 Vista: Successful Connection

- **4** If you will use this network again, ensure that **Save this network** is selected. If you save the network, you do not have to configure its settings again.
- 5 Select Start this connection automatically if you want Windows to always try to use this network when you start up your computer. If you do not select this (but select Save this network) you can connect manually each time by clicking Start > Connect to and selecting the network's name from the list.

#### **Connecting to a Network Manually**

If the wireless network to which you want to connect does not appear in the **Connect to** window (if your network's SSID is hidden, for example), take the following steps to configure your network connection manually

1 Click Set up a connection or network at the bottom of the Connect to screen. The following screen displays.

Internet			
ss, broadband, or dial-u	) connection to the In	ternet.	
ss router or access point			
rireless network for your	home or small busine	\$5.	
			=
ect to a wireless networ	2		
connect to a nidden ne	work of create a new t	wireless prome-	
ss ad hoc (computer-to-	computer) network		
orary network for sharing	files or an Internet co	nnection.	
p connection			
	e Internet iss, broadband, or dial-up iss router or access point vireless network for your nect to a wireless networf connect to a hidden net iss ad hoc (computer-to- orary network for sharing	e Internet iss, broadband, or dial-up connection to the Int iss router or access point vireless network for your home or small busine nect to a wireless network o connect to a hidden network or create a new v iss ad hoc (computer-to-computer) network orary network for sharing files or an Internet co	e Internet iss, broadband, or dial-up connection to the Internet. iss router or access point. vireless network for your home or small business. nect to a wireless network o connect to a hidden network or create a new wireless profile. iss ad hoc (computer-to-computer) network orary network for sharing files or an Internet connection.

Figure 97 Vista: Choose a Connection Option

2 Click Manually connect to a wireless network. The following screen displays.

Figure 98 Vista: Connect Manually

🚱 🔨 Manually connect to a v	vireless network
Enter information for th	e wireless network you want to add
N <u>e</u> twork name:	
Security type:	[Choose an option]
Encryption type:	Ţ
Se <u>c</u> urity Key/Passphrase:	Display characters
Start this connection au	tomatically
Connect even if the net Warning: If you select t	work is not broadcasting his option, your computer's privacy might be at risk.
	Next Cancel

The following table describes the labels in this screen.

#### Table 26 Vista: Connect Manually

LABEL	DESCRIPTION
Network name	Enter your network's SSID (Service Set IDentifier).
Security type	Select the type of security used by the network to which you want to connect. The types of available security shown depend on your computer's wireless client. In this field, <b>WPA(2)-Personal</b> is the same as <b>WPA(2)-PSK</b> , and <b>WPA(2)-Enterprise</b> is the same as <b>WPA(2)</b>

LABEL	DESCRIPTION
Encryption type	Select the type of encryption used by the network. When you use <b>WEP</b> or <b>802.1x</b> , <b>WEP</b> displays. When you use a <b>WPA</b> mode ( <b>WPA(2)-Personal</b> or <b>WPA(2)-Enterprise</b> ) you can choose <b>AES</b> or <b>TKIP</b> (if supported by your computer's wireless client).
Security Key / Passphrase	If your network uses <b>WEP</b> or <b>WPA(2)-Personal</b> security, enter the key here.
Display Characters	Select this if you do not want the security key characters to be hidden.
Start this connection automatically	Select this box if you always want to try to connect to this network at startup. If you leave this box unchecked, you will need to connect manually each time.
Connect even if the network is not broadcasting	Select this box if you always want to try to connect to this network at startup, even if the network is not broadcasting its SSID. The warning in this field refers to the fact that if you do this, your computer sends out probe request packets, which contain the network's SSID and could be used by an attacker to access the network.
Next	Click this to save your settings and move on to the next page.
Cancel	Click this to stop setting up your network.

 Table 26
 Vista: Connect Manually

**3** When you have finished filling in the fields, click **Next**. the following screen displays.

Figure 99 Vista: Successfully Added Network



**4** If you want to make any changes to the settings you just configured, click **Change connection settings**. Otherwise, click **Connect to...**. In the window that displays, double-click the new network's name to connect to the network.

### Setting Up An Ad-Hoc Network

Take the following steps to set up a wireless connection between two computers in Windows Vista.

Click Start ( )> Connect To. In the Connect to screen, click Set up a connection or network. The following screen displays.

Figure 100 Vista: Set Up An Ad-hoc Network

Choos	e a connection option	
0	Connected to Detuning	
1	Set up a wireless, broadband, or dial-up connection to the Internet.	
- K		
11	Set up a wireless router or access point Set up a new wireless network for your home or small business.	
0		=
	Manually connect to a wireless network	
-	Choose this to connect to a hidden network or create a new wireless profile.	
N	Set up a wireless ad hoc (computer-to-computer) network	
-	Set up a temporary network for sharing files or an Internet connection.	
an	Set up a dial-up connection	
4	Connect through a dial-up connection to the Internet.	

2 Select Set up a wireless ad hoc (computer-to-computer) network and click Next. The following screen displays.

Figure 101 Vista: Ad-hoc Options

$\bigcirc$	🔮 Set up a wireless ad ho	oc (computer-to-computer) networ	k
	Give your network a r	name and choose security o	ptions
	Ne <u>t</u> work name:	Test2	
	Security type:	WPA2-Personal 🔻	Help me choose
	S <u>e</u> curity key/Passphrase:	•••••	Display characters
	Sa <u>v</u> e this network		
			Next Cancel

**3** Enter the **Network name** (SSID) you want to use for your network. Select a **Security type**. If you are not sure what kind of security you want to use, click the **Help me choose** link.



Make sure all the wireless clients on your ad-hoc network can support the type of security you select.

- 4 Enter the Security key/Passphrase. Everybody on the network must enter this key in their computer's wireless client in order to access the network. If you want to see the characters you entered, select the Display characters box. Otherwise, leave it empty (dots display instead of the characters).
- 5 If you will use this ad-hoc network again, select the Save this network box. If you do this, the next time you click Start > Connect to, you can select the network from the list.
- 6 Click Next. The following screen displays.

Figure 102 Vista: Ad-hoc Network Ready

To share files, open Network and Sharing Center in Control Panel and turn on file sharing.	The 1	Test2 network is ready to use	
Wireless network name: Test2 Network security key: •••••• To share files, open <u>Network and Sharing Cented</u> in Control Panel and turn on file sharing.	this n discon to con	etwork will appear in the list of wireless networks and will stay active until everyone inects from it. Give the network name and security key (if any) to people you want nect to this network.	
To share files, open Network and Sharing Cented in Control Panel and turn on file sharing.		Wireless network name: Test2 Network security key: ••••••	
	To sha	re files, open <u>Network and Sharing Centes</u> in Control Panel and turn on file sharing.	

7 If you want to share files with other computers on the ad-hoc network, or let other computers use your Internet connection, click the Network and Sharing Center link. Otherwise, click Close.

# Windows XP

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

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

#### **Activating Wireless Zero Configuration**

1 Click Start, Control Panel and double-click Network Connections.

- **2** Double-click on the icon for wireless network connection.
- **3** The status window displays as shown below. Click **Properties**.

Figure 103 Windows XP SP1: Wireless Network Connection Status

eneral Support	
Connection	
Status:	Connected
Duration:	01:18:28
Speed:	48.0 Mbps
Signal Strength:	T •••••
Activity	ent — 🕺 — Received
Bytes:	2,819   0
Properties Dis	able

Figure 104 Windows XP SP2: Wireless Network Connection Status

eneral Support		
Connection		
Status:		Connected
Network:		ZW70-1
Duration:		00:01:56
Speed:		48.0 Mbps
Signal Strengt	h:	UBBae
Activity	-	A
	Sent — 🕎	P) Received
Bytes:	1,300	1,676
Properties	<u>D</u> isable <u>V</u> iew	v Wireless Networks

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

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

Use	Windows to configure	e my wireless n	etwork settings
Avail	able <u>n</u> etworks:		
lo c	onnect to an available	network, click	Configure.
i	AOL		
i	SOC_TEST		Refresh
Auto	rred networks: matically connect to av	vailable networl	ks in the order listed
Auto	rred networks: matically connect to av	vailable networl	ks in the order listed
Auto Delov	rred networks: matically connect to av w	vailable networl	Ks in the order listed           Move up           Move down
Auto belov	rred networks: matically connect to av w: Add	vailable networf	ks in the order listed Move <u>up</u> Move <u>down</u> erties

Figure 105 Windows XP SP1: Wireless Network Connection Properties

Figure 106 Windows XP SP2: Wireless Network Connection Properties

Use	Windows to configu	re my wirel	ess network	settings
Availa	able <u>n</u> etworks:			
To co abou	onnect to, disconnect t wireless networks in	t from, or fi range, cli	nd out more ck the butto	e information on below
		ſ	View Wirel	ess Networks
belov	e.			Move <u>up</u> Move <u>d</u> own
_	<u>A</u> dd <u>B</u> emo	ove ] [	Properties	
	1 1 11	lecc hetw	DIK	Advanced

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



Figure 107 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.

#### Figure 108 Windows XP SP2: System Tray Icon



The type of the wireless network icon in Windows XP SP2 indicates the status of the NWD210N. Refer to the following table for details.

Table 27	Windows XP	SP2: System	Tray Icon
----------	------------	-------------	-----------

ICON	DESCRIPTION
	The NWD210N is connected to a wireless network.
	The NWD210N is in the process of connecting to a wireless network.
4	The connection to a wireless network is limited because the network did not assign a network address to the computer.
2	The NWD210N 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.

<sup>((†))</sup> Wireless Netwo	rk Connection 6 Status	
General Support		
Connection		
Status:	Connected	
Network:	ZW70-1	
Duration:	00:01:56	
Speed:	48.0 Mbps	
Signal Strength:	Ulian	
Activity	Sent — 🐨 — Received	
Bytes:	کر (م) 1,300   1,676	
Properties	Disable	
	<u>C</u> lose	

Figure 109 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.

Figure 110 Windows XP SP1: Wireless Network Connection Status

★ Wireless Netwo	rk Connection 6 Status	<u> </u>
General Support		
Connection		
Status:	Connected	
Duration:	01:18:28	
Speed:	48.0 Mbps	
Signal Strength:	?	
Activity	Sent — 褽 — Received	
Bytes:	2,819 0	
Properties	<u>D</u> isable	-

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



Figure 111 Windows XP SP2: Wireless Network Connection

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

 Table 28
 Windows XP SP2: Wireless Network Connection

ICON	DESCRIPTION
8	This denotes that wireless security is activated for the wireless network.
\$	This denotes that this wireless network is your preferred network. Ordering your preferred networks is important because the NWD210N 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.
1000	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 <u>W</u> indows to configure my wireless network settings					
Available networks:					
t ope sw1 5275					
cpe_5254_g2kplus					
♀ ZW70-1					
Automatically connect to available networks in the order listed below:					
P Zw70-1 Move up					
A pqa-3225-p334w Move down					
Add <u>R</u> emove Properties					
Learn about <u>setting up wireless network</u> <u>configuration.</u> Ad <u>v</u> anced					
OK Cancel					

Figure 112 Windows XP SP1: Wireless Network Connection Properties

**4** 4.Windows XP SP2: If the wireless security is activated for the selected wireless network, the **Wireless Network Connection** screen displays. You must set the related fields in the **Wireless Network Connection** screen to the same security settings as the associated AP and click **Connect**. Refer to the section about security settings for more information. Otherwise click **Cancel** and connect to another wireless network without data encryption. If there is no security activated for the selected wireless network, a warning screen appears. Click **Connect Anyway** if wireless security is not your concern.

Figure 113 Windows XP SP2: Wireless Network Connection: WEP or WPA-PSK

Wireless Network Conne	ction	×			
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.					
rype the key, and then thick (					
Network <u>k</u> ey:	•••••				
C <u>o</u> nfirm network key:	••••••				
	<u>C</u> onnect Cancel				

Figure 114 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.

 Table 29
 Windows XP: Wireless Networks

ICON	DESCRIPTION
ž	This denotes the wireless network is an available wireless network.
-0	This denotes the NWD210N is associated to the wireless network.
×	This denotes the wireless network is not available.

#### **Security Settings**

When you configure the NWD210N to connect to a secure network but the security settings are not yet enabled on the NWD210N, 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		? 🗙	1	Wireless ne	twork proper	ties
Association Authentication C	onnection			Association	Authentication	
Network name (SSID):	/ireless			Network <u>n</u> a	ame (SSID):	ZW70-1
Wireless network key				-Wireless I	network key —	
This network requires a key I	or the following:			This netw	vork requires a ke	y for the following:
Network Authentication:	Shared	~		Network	Authentication:	Shared
Data encryption:	WEP	~		<u>D</u> ata end	cryption:	WEP
Network <u>k</u> ey:				Network	<u>k</u> ey:	
Confirm network key:				C <u>o</u> nfirm n	network key:	
Key inde <u>x</u> (advanced): 1	•			Key inde <u>x</u>	<u>x</u> (advanced):	1
The key is provided for m	e automatically			The k	ey is provided for	me automatically
This is a <u>c</u> omputer-to-compu access points are not used	uter (ad hoc) network; wireless			This is a access	a <u>c</u> omputer-to-con points are not use	nputer (ad hoc) network; wireles: ed
	OK Ca	incel	'			ок с

Figure 115 Windows XP: Wireless (network) properties: Association

? 🗙

Y

Cancel

The following table describes the labels in this screen.

Table 30	Windows XP <sup>.</sup> Wireless	(network) n	ronerties: A	Association
		(HELWORK) P	$r_{0}$	133001411011

LABEL	DESCRIPTION
Network name (SSID)	This field displays the SSID (Service Set IDentifier) of each wireless network.
Network Authentication	This field automatically shows the authentication method ( <b>Share</b> , <b>Open</b> , <b>WPA</b> or <b>WPA-PSK</b> ) used by the selected network.
Data Encryption	This field automatically shows the encryption type ( <b>TKIP</b> , <b>WEP</b> or <b>Disable</b> ) 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 <b>WEP</b> encryption method and the <b>The key is provided for me automatically</b> check box is not selected.
The key is provided for me automatically	If this check box is selected, the wireless AP assigns the NWD210N 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.
ОК	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to leave this screen without saving any changes you may have made.

#### Authentication

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



Figure 116 Windows XP: Wireless (network) properties: Authentication

The following table describes the labels in this screen.

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

Table 31	Windows	XP:	Wireless	(network)	pro	perties:	Authent	ication
	*******	/ · · ·	11101000	(1101110111)	, p. o	poi 100.	/ (01110111	oution

#### **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:
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

Figure 117 Windows XP: Protected EAP Properties

The following table describes the labels in this screen.

 Table 32
 Windows XP: Protected EAP Properties

LABEL	DESCRIPTION
Validate server certificate	Select the check box to verify the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
Do not prompt user to authorize new server or trusted certification authorities.	Select this check box to verify a new authentication server or trusted CA without prompting. This field is available only if you installed the Windows XP server pack 2.
Select Authentication Method:	Select an authentication method from the drop-down list box and click <b>Configure</b> 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.
ОК	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> 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 smat card ● Use a certificate on this computer ✓ Use simple certificate selection (Recommended)
✓ Validate server certificate □ Connect to these servers:
Trusted Boot Certification Authorities: ABA.ECOM Root CA Autoridad Certificadora de la Asociacion Nacional del Notaria Autoridad Certificadora del Colegio Nacional de Correduria Pu Baltimore EZ by DST Belgacom E-Trust Primary CA C&W HKT SecureNet CA Class A C&W HKT SecureNet CA Class B C&W HKT SecureNet CA Root
View Certificate           Use a different user name for the connection           OK         Cancel

Figure 118 Windows XP: Smart Card or other Certificate Properties

The following table describes the labels in this screen.

Table 33         Windows XP: Smart Card or other Certificate Property
---

LABEL	DESCRIPTION
Use my smart card	Select this check box to use the smart card for authentication.
Use a certificate on this computer	Select this check box to use a certificate on your computer for authentication.
Validate server certificate	Select the check box to check the certificate of the authentication server.
Connect to these servers	Select the check box and specify a domain in the field below to have your computer connect to a server which resides only within this domain.
Trusted Root Certification Authorities:	Select a trusted certification authority from the list below. Note: You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.
View Certificate	Click this button if you want to verify the selected certificate.
Use a different user name for the connection:	Select the check box to use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain that you are logged on to.
ОК	Click <b>OK</b> to save your changes.
Cancel	Click <b>Cancel</b> to leave this screen without saving any changes you may have made.

# **Ordering the Preferred Networks**

Follow the steps below to manage your preferred networks.

1 Windows XP SP2: Click Change the order of preferred networks in the Wireless Network Connection screen (see Figure 111 on page 129). The screen displays as shown.

Figure 119 Windows XP SP2: Wir	eless Networks: Preferred Networks
--------------------------------	------------------------------------

📥 Wireless Network Connection 7 Properties 👘 🥤	? 🗙
General Wireless Networks Advanced	
✓ Use <u>W</u> indows 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.	
View Wireless Networks	וו
Preferred networks:         Automatically connect to available networks in the order listed below:         I ZyXEL_MIS (Automatic)         Move up         I cpe_5236 (Automatic)         Wireless (Automatic)         Wireless (Automatic)         I I demo (Automatic)         Add         Remove       Properties         Learn about setting up wireless network         Adyanced	
OK Cano	cel

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

Figure 120 Windows XP SP1: Wireless Networks: Preferred Networks

🕹 Wireless Network Connection 6 Properties 🛛 🕐 🔀
General Wireless Networks Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
i cpe_sw1_5275
A cpe_5254_g2kplus     P ZW70-1     Refresh
Preferred networks: Automatically connect to available networks in the order listed below:
Y Zw70-1 Move up
A pqa-3225-p334w Move down
Add Bemove Properties
Learn about <u>setting up wireless network</u> <u>configuration</u> . Ad <u>v</u> anced
OK Cancel

**2** Whenever the NWD210N 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.

D

# **Legal Information**

# Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

#### Disclaimers

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

#### Trademarks

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

## Certifications

#### Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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



#### **FCC Radiation Exposure Statement**

- This device has been tested to the FCC exposure requirements (Specific Absorption Rate).
- This device complies with the requirements of Health Canada Safety Code 6 for Canada.
- Testing was performed on laptop computers with antennas at 0mm spacing. The maximum SAR value is: 0.680 W/kg. The device must not be collocated with any other antennas or transmitters.
- This equipment has been SAR-evaluated for use in laptops (notebooks) with side slot configuration.
- The device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2). End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.



依據 低功率電波輻射性電機管理辦法

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

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

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備,限於室內使用。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

#### Notices

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

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

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

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

#### **Viewing Certifications**

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

# **ZyXEL Limited Warranty**

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

#### Note

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

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

#### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

E

# **Customer Support**

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

#### **Required Information**

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

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

#### **Corporate Headquarters (Worldwide)**

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

#### **Costa Rica**

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

#### **Czech Republic**

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

 Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 -Modrany, Ceská Republika

#### Denmark

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

#### Finland

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

#### France

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

#### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

#### Hungary

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

#### India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

#### Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

#### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

#### Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

#### **North America**

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

• Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

#### Norway

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

#### Poland

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

#### Russia

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

#### Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

#### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

#### Sweden

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

#### Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

#### Ukraine

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

#### **United Kingdom**

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

# Index

## Α

About 67 about your ZyXEL Device 21 Access Point (AP) 37 Access point (AP) 37 Access Point. See also AP. ACT LED 22 activating a profile 61 adapter 61 Ad-Hoc 23, 59 Advanced Encryption Standard 39 See AES. advanced settings 61 AES 112 antenna directional 115 gain 115 omni-directional 115 AP 105 See also access point. AP MAC address 48 authentication 48 authentication type 39 auto 39 open system 39 shared key 39 auto authentication 39 automatic connection 49 automatic network scan 32, 56

## В

band 77 Basic Service Set, See BSS 103 BSS 103

## С

CA 39, 110 CCMP 39 Certificate Authority See CA. certifications 139 notices 141 viewing 141 channel 38, 48, 50, 59, 77, 105 interference 105 configuration method 24 important note 24 Wireless Zero Configuration (WZC) 24 ZyXEL utility 24 configuration status 47 connection status 47 contact information 143 continuous access mode 62 copyright 139 creating a new profile 58 credentials 65 CTS (Clear to Send) 106 current configuration 47 current connection status 47 customer support 143

## D

data encryption 50 data rate 77 digital ID 39 dimensions 77 disclaimer 139 download 69 driver version 67 dynamic WEP key exchange 111

## Ε

EAP (Extensible Authentication Protocol) **39** EAP Authentication **109** EAP authentication **39** EAP type **64** EAP-PEAP **39** EAP-TLS **39**  EAP-TTLS **39** encryption encryption type **39**, **51**, environmental specifications ESS **104** Extended Service Set, See ESS

# F

fast power save 62 FCC interference statement 139 fragmentation threshold 106 frequency 38, 77

# G

getting started 21

## Η

hardware connections 24 help 25 hidden node 105 humidity 77

# I

IBSS 103 IEEE 802.11g 107 IEEE 802.1x 39, 54, 64 Independent Basic Service Set See IBSS 103 Industrial Scientific Medical Band 77 infrastructure 22 Initialization Vector (IV) 112 installation 24 interface 77 Internet access 22

## L

LEDs 22 lights 22 link information 47 LINK LED 22 link quality 48, 49

## Μ

manual network connection **32** Message Integrity Check (MIC) **39**, **112** modulation **77** 

## Ν

network mode 48 network name 48 network overlap 37 network scan 56 network type 48, 50

## 0

online help 25 output power 77

### Ρ

packet collisions Pairwise Master Key (PMK) **112**, passphrase **38**, password **38** PEAP **64** peer computer **22**, physical specifications power consumption power saving power saving mode preamble **61** preamble **61** product registration product specifications 77 profile 48, 57 activation 61 add new 58 configure 32, 34 default 56 delete 57 edit 57 information 57 new 57, 58 PSK 112

# Q

Quick Start Guide 24, 74

# R

radio band 77 radio interference 74 radio specifications 77 RADIUS 39, 40, 108 message types 109 messages 109 shared secret key 109 real-time data traffic statistics 49 receive rate 48 registration product 141 related documentation 3 RTS (Request To Send) 106 threshold 105, 106

# S

safety warnings 6 save power 62 scan 49 scan info 59 search 49 security 38, 48, 78 data encryption 38 security settings and Vista 64 sensitivity 78 Service Set Identity (SSID) 32, 37 signal strength 49, 50 site information 50 site survey 49 scan 50 security settings 51 sleep mode 62 SSID 32, 37, 48, 50, 74 statistics 48 syntax conventions 4 system tray 24

# Т

temperature 77 Temporal Key Integrity Protocol (TKIP) **39**, The **64** TLS **64**, **65** total receive total transmit trademarks transmission rate **48**, transmit key transmit rate trend chart **48**, TTLS **64** 

## U

uninstalling the ZyXEL utility 68 upgrading the ZyXEL utility 68 important step 69 user authentication 38 utility installation 24 utility version 67

## V

Vista 64, 65 voltage 77

### W

warranty 141 note 141

weight 77 WEP 38, 51 automatic setup 38 manual setup 38, 51 passphrase 38, 51 WEP (Wired Equivalent Privacy) 38 WEP Encryption 51 WEP key generation 38 Wi-Fi Protected Access 39, 111 Wi-Fi Protected Setup 47 Windows 64 Windows XP 24, 25 wireless client 37 wireless client WPA supplicants 113 wireless LAN introduction 37 security 38 wireless LAN (WLAN) 37 wireless network 37 wireless security 107 wireless standard 48, 77 wireless station mode adapter 61 security settings 51 site survey 49 trend chart 49 wireless tutorial 27 WLAN interference 105 security parameters 114 WPA 39, 52, 64, 111 key caching 112 pre-authentication 112 user authentication 112 vs WPA-PSK 112 wireless client supplicant 113 with RADIUS application example 113 WPA2 39, 52, 64, 111 user authentication 112 vs WPA2-PSK 112 wireless client supplicant 113 with RADIUS application example 113 WPA2-Pre-Shared Key 40, 111 WPA2-PSK 40, 52, 111, 112 application example 113 WPA-PSK 40, 52, 111, 112 application example 113 WPS see also Wi-Fi Protected Setup 47 WZC activating 124 network connection 127 not available 126 preferred network 135

security setting 131 system tray icon 127 WZC (Wireless Zero Configuration) 24

## Ζ

ZyXEL Utility accessing 25 ZyXEL utility 24 accessing 25 driver version number 67 exiting 25 help 25 reactivating 25 status 24 system tray icon 24 upgrading 68 version number 67