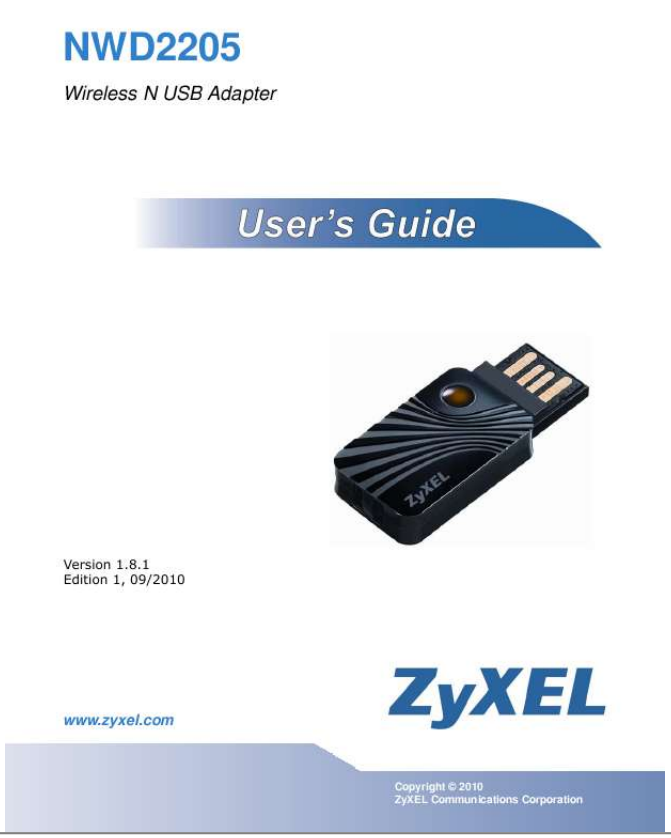

Manual abstract:

This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader. · To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen. · Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF. Related Documentation · Quick Start Guide The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access. · Online Help Embedded web help for descriptions of individual screens and supplementary information. · Support Disc Refer to the included CD for support documents.

Documentation Feedback Send your comments, questions or suggestions to: techwriters@zyxel.com.tw NWD2205 User's Guide 3 About This User's Guide Thank you! The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan. Need More Help? More help is available at www.

zyxel.com. · Download Library Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product. · Knowledge Base If you have a specific question about your product, the answer may be here.

This is a collection of answers to previously asked questions about ZyXEL products. · Forum This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well. Customer Support Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

· 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. 4 NWD2205 User's Guide Document Conventions Document Conventions Warnings and Notes These are how warnings and notes are shown in this User's Guide. Warnings tell you about things that could harm you or your NWD2205. Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations. Syntax Conventions · The NWD2205 may be referred to as the "NWD2205", the "device", the "system" or the "product" in this User's Guide. · Product labels, screen names, field labels and field choices are all in bold font. · A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.

· "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices. · A right angle bracket (>) within a screen name denotes a mouse click. For example, Maintenance > Log > Log Setting means you first click Maintenance in the navigation panel, then the Log sub menu and finally the Log Setting tab to get to that screen. · Units of measurement may denote the "metric" value or the "scientific" value.

For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on. · "e.g.," is a shorthand for "for instance", and "i.e.

," means "that is" or "in other words". NWD2205 User's Guide 5 Document Conventions Icons Used in Figures Figures in this User's Guide may use the following generic icons. Wireless Access Point Computer Notebook computer Server Modem Telephone Internet Wireless Signal 6 NWD2205 User's Guide Safety Warnings Safety Warnings · Do NOT use this product near water, for example, in a wet basement or near a swimming pool. · Do NOT expose your device to dampness, dust or corrosive liquids. · Do NOT store things on the device. · Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning. · Connect ONLY suitable accessories to the device. · Ground yourself (by properly using an anti-static wrist strap, for example) whenever working with the device's hardware or connections. · ONLY qualified service personnel should service or disassemble this device.

· Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s). Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately. NWD2205 User's Guide 7 Safety Warnings 8 NWD2205 User's Guide Contents Overview Contents Overview Introduction and Configuration ....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 17 Getting Started ..
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.. 15 1.3.2 Installing the ZyXEL Utility .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

... 15 1.3.3 Uninstalling the ZyXEL Utility .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

19 1.4 Hardware Installation .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
... 21 1.5 Device Applications .
.....

.....
.....
.....
.....

.....
.....

.
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.... 38 3.
3 The Link Status Screen .....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
..... 39 3.4 The Profile Screen .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
40 3.4.1 The Profile Properties Screen .....

.....
.....
.....
.....the operation of the NWD2205's LEDs. Table 2 NWD2205 LEDs LED COLOR Amber STATUS Slow Blinking Rapid Blinking DESCRIPTION The NWD2205 is turned on, connected to an AP, and is not transmitting or receiving data. The NWD2205 is turned on, connected to an AP, and is transmitting or receiving data. It also blinks when the WPS feature is being used or a WPS connection is being initiated. The NWD2205 is either not connected or the device to which it is connected is turned off.

Off 14 NWD2205 User's Guide Chapter 1 Getting Started 1.3 Software Installation This section shows you how to install the Mac OS X version of the ZyXEL Utility. For detailed information on using it, see Chapter 3 on page 37. 1.3.1 Minimum System Requirements In order to install the ZyXEL Utility for Mac OS X, your computer must meet the following minimum system requirements: · 20 MB of free hard drive space · 128 MB RAM · Mac OS X 10.4 and higher 1.3.2 Installing the ZyXEL Utility Screen shots for Macintosh 10.4 are shown in the following procedure unless otherwise specified.
The screens on your computer may differ slightly from the screens shown here depending on the version of your operating system. To install the ZyXEL utility:

1 Make sure the NWD2205 is disconnected from your computer before you begin the installation process. Close all programs and applications. Insert the included CD into the CD-ROM drive. 2 3 NWD2205 User's Guide 15 Chapter 1 Getting Started Open the folder for your version of Mac OS X on the included disc.

For example, if you are using 10.4 then open the MacOS10.4 Driver folder. Double-click the Installer.mpkg to run the installation program.

4 5 A welcome screen appears. Follow the on-screen instructions. 16 NWD2205 User's Guide Chapter 1 Getting Started When you see the Select a Destination screen, select a destination (this must be on an actual physical hard drive on the Macintosh, not a virtual drive) and click Continue. 6 7 When you see the Authenticate screen, enter the administrative password you use to log in to the Mac computer and click OK. NWD2205 User's Guide 17 Chapter 1 Getting Started You then see a screen telling you that you must restart the computer after the installation completes. Click Continue Installation. The driver will automatically install. 8 9 After installing the ZyXEL utility and device driver, you must restart your computer. Click Restart to reboot your computer and complete the driver installation. 18 NWD2205 User's Guide Chapter 1 Getting Started 10 Once your computer restarts, you can find the ZyXEL utility in your Applications folder.

11 The ZyXEL utility starts automatically after you connect the NWD2205 to the computer. 1.3.3 Uninstalling the ZyXEL Utility You need to remove the ZyXEL utility from your computer only when you want to upgrade the ZyXEL utility or the ZyXEL utility cannot work properly. Note: Disconnect the NWD2205 if you are going to uninstall or upgrade the ZyXEL utility. While you can drag the ZyXEL Utility from your Applications folder directly to the Trash and remove it that way, the best and safest course of action is to run the uninstallation program bundled on the included disc. This ensures that all components of the application are properly removed, especially the device driver. To uninstall the ZyXEL Utility: 1 Insert the included CD into the CD-ROM drive. NWD2205 User's Guide 19 Chapter 1 Getting Started Double-click your Macintosh OS's driver folder on the included disc. Double-click the file Uninstall.

command. 2 3 The command screen displays. Enter the administrative password you use to log in to the Mac computer and press [ENTER]. 20 NWD2205 User's Guide Chapter 1 Getting Started 1.4 Hardware Installation This sections shows you how to install your NWD2205.

1 2 Locate an available USB port on the computer. Insert the NWD2205 into an available USB port on the computer. The NWD2205's LED (light) turns on if it is properly inserted. Note: Never bend, twist or force the NWD2205 into the port. If there is not enough space to attach the NWD2205, use the included USB cable.

NWD2205 User's Guide 21 Chapter 1 Getting Started 1.5 Device Applications This section describes some network applications for the NWD2205. You can either set the network type to Infrastructure and connect to an AP or use Ad-Hoc mode and connect to a peer computer (another wireless device in Ad-Hoc mode). Infrastructure To connect to a network via an access point (AP), set the NWD2205 network type to Infrastructure. Through the AP, you can access the Internet or the wired network behind it. Figure 2 Application: Infrastructure 22 NWD2205 User's Guide Chapter 1 Getting Started Ad-Hoc To set up a small independent wireless workgroup without an AP, use Ad-Hoc. Ad-Hoc does not require an AP or a wired network. Two or more wireless clients communicate directly with each other. Note: Wi-Fi Protected Setup (WPS) is not available in ad-hoc mode. Figure 3 Application: Ad-Hoc NWD2205 User's Guide 23 Chapter 1 Getting Started 24 NWD2205 User's Guide CHAPTER 2.

1 Overview 2 Wireless LANs This section provides background information on wireless Local Area Networks. 2.1.1 What You Can Do in This Section · Connect securely to an AP using many of the strongest and most common encryption protocols. See Section 2.3 on page 27 for details. · Connect securely either to an AP or computer-to-computer using WPS. See Section 2.4 on page 29 for details. 2.

1.2 What You Need to Know The following terms and concepts may help as you read through this section. Server When two or more devices are connected digitally to form a network, the one that distributes data to the other devices is known as the "server". A RADIUS (Remote Authentication Dial-In User Service) is a kind of server that manages logins and logout, among other things, for the network to which it is connected. Client When two or more devices are connected digitally to form a network, the one that contacts and obtains data from a server is known as the "client".

Each client is designed to work with one or more specific kinds of servers, and each server requires a specific kind of client. Wireless adapters are clients that connect to a network server through an AP. Authentication Authentication is the process of confirming a client's or user's digital identity when they connect to a network. Turning off authentication means disabling all security protocols and opening your network to anyone with the means to connect to it. NWD2205 User's Guide 25 Chapter 2 Wireless LANs Encryption The process of taking data and encoding it, usually using a mathematical formula, so that it becomes unreadable unless decrypted with the proper code or pass phrase.

2.1.3 Before You Begin · You should have valid login information for an existing network Access Point, otherwise you may not be able to make a network connection right away. 2.2 Wireless LAN Overview The following figure provides an example of a wireless network with an AP. See Figure 3 on page 23 for an Ad Hoc network example. Figure 4 Example of a Wireless Network The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet Every wireless network must follow these basic guidelines. · Every device in the same wireless network must use the same SSID.

The SSID is the name of the wireless network. It stands for Service Set IDentity. 26 NWD2205 User's Guide Chapter 2 Wireless LANs · If two wireless networks overlap, they should use a different channel. Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information. · Every device in the same wireless network must use security compatible with the AP or peer computer. Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network. 2.3 Wireless LAN Security Wireless LAN security is vital to your network to protect wireless communications. If you do not enable any wireless security on your NWD2205, the NWD2205's wireless communications are accessible to any wireless networking device that is in the coverage area.
Note: You can use only WEP encryption if you set the NWD2205 to Ad-hoc mode. See the appendices for more detailed information about wireless security. 2.3.1 User Authentication and Encryption You can make every user log in to the wireless network before they can use it.
This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this. Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code.
If you do not know the secret code, you cannot understand the message. 2.3.1.1 WEP 2.3.1.1.1 Data Encryption WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the NWD2205 and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

There are two ways to create WEP keys in your NWD2205. NWD2205 User's Guide 27 Chapter 2 Wireless LANs · 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 NWD2205 allows you to configure up to four 64-bit or 128-bit WEP keys. Only one key is used as the default key at any one time. 2.3.
1.1.2 Authentication Type The IEEE 802.11b/g standard describes a simple authentication method between the wireless stations and AP. Three authentication types are defined: Auto, Open and Shared.
· Open mode is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted. · Shared mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.
· Auto authentication mode allows the NWD2205 to switch between the open system and shared key modes automatically. Use the auto mode if you do not know the authentication mode of the other wireless stations. 2.3.1.2 IEEE 802.1x The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server. 2.

3.1.2.1 EAP Authentication EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication. The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. The NWD2205 supports EAP-TLS, EAP-TTLS (at the time of writing, TTLS is not available in Windows Vista) and EAPPEAP. Refer to Appendix A on page 57 for descriptions.
28 NWD2205 User's Guide Chapter 2 Wireless LANs 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). Certificates (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner. 2.3.1.
3 WPA and WPA2 Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.
Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP. If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN. If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not. Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2. 2.

4 WiFi Protected Setup Your NWD2205 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure). NWD2205 User's Guide 29 Chapter 2 Wireless LANs Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves. 2.4.

1 Push Button Configuration WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information. Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button. Take the following steps to set up WPS using the button.

1 Ensure that the two devices you want to set up are within wireless range of one another. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button. Press the button on one of the devices (it doesn't matter which). Within two minutes, press the button on the other device.

The registrar sends the network name (SSID) and security key through an secure connection to the enrollee. If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful. 2 3 4 2.4.2 PIN Configuration Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface). Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method. 30 NWD2205 User's Guide Chapter 2 Wireless LANs When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router).

Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network. Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method. 1 2 Ensure WPS is enabled on both devices. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface. Enter the client's PIN in the AP's configuration interface. 3 4 Note: If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which. 5 Start WPS on both devices within two minutes.

Note: Use the configuration utility to activate WPS, not the push-button on the device itself. 6 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful. If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

NWD2205 User's Guide 31 Chapter 2 Wireless LANs The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method. Figure 5 Example WPS Process: PIN Method ENROLLEE WPS This device's WPS PIN: 123456 REGISTRAR WPS Enter WPS PIN from other device: WPS WPS START START WITHIN 2 MINUTES SECURE EAP TUNNEL SSID WPA(2)-PSK COMMUNICATION 2.4.3 How WPS Works When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the Registrar (the device that supplies network and security settings) and the other device acts as the Enrollee (the device that receives network and security settings.

The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPAPSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is 32 NWD2205 User's Guide Chapter 2 Wireless LANs already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly. The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point. Figure 6 How WPS works ACTIVATE WPS WITHIN 2 MINUTES ACTIVATE WPS WPS HANDSHAKE ENROLLEE SECURE TUNNEL REGISTRAR SECURITY INFO COMMUNICATION The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary. The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device. Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee.

All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients. By default, a WPS devices is "unconfigured". This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes "configured". A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all NWD2205 User's Guide 33 Chapter 2 Wireless LANs subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults. 2.4.

3.1 Example WPS Network Setup This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step 1, both AP1 and Client 1 are unconfigured. When WPS is activated on both, they perform the handshake.

In this example, AP1 is the registrar, and Client 1 is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information. Figure 7 WPS: Example Network Step 1 ENROLLEE REGISTRAR SECURITY INFO CLIENT 1 AP1 In step 2, you add another wireless client to the network. You know that Client 1 supports registrar mode, but it is better to use AP1 for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, AP1 must be the registrar, since it is configured (it already has security information for the network).

AP1 supplies the existing security information to Client 2. Figure 8 WPS: Example Network Step 2 REGISTRAR EXISTING CONNECTION CLIENT 1 AP1 ENROLLEE ITY UR EC S O INF CLIENT 2 34 NWD2205 User's Guide Chapter 2 Wireless LANs In step 3, you add another access point (AP2) to your network. AP2 is out of range of AP1, so you cannot use AP1 for the WPS handshake with the new access point. However, you know that Client 2 supports the registrar function, so you use it to perform the WPS handshake instead. Figure 9 WPS: Example Network Step 3 EXISTING CONNECTION CLIENT 1 E ION CT NE N CO ING T XIS AP1 REGISTRAR CLIENT 2 SE CU RIT Y INF O ENROLLEE AP1 2.4.4 Limitations of WPS WPS has some limitations of which you should be aware. · WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP). · When you use WPS, it works between two devices only.

You cannot enroll multiple devices simultaneously, you must enroll one after the other. For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way. NWD2205 User's Guide 35 Chapter 2 Wireless LANs · WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS. WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK). · When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device.

This is a possible way for a hacker to gain access to a network. You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP. 36 NWD2205 User's Guide CHAPTER 3.1 Overview 3 ZyXEL Utility - Mac OS X This chapter shows you how to use the ZyXEL utility to configure your NWD2205 using the Macintosh operating system, Mac OS X. 3.

1.1 What You Can Do in This Chapter · The Link Status screen (Section 3.3 on page 39) lets you see your current connection details, monitor signal strength and quality, and more. · The Profiles screen (Section 3.4 on page 40) lets you create, delete and manage your wireless network profiles. · The Available Network screen (Section 3.5 on page 44) lets you connect to any available unsecured wireless network in range of the NWD2205, or open the security settings screen for any secured wireless network in range. · The Advanced Setting screen (Section 3.6 on page 45) lets you configure your NWD2205 with advanced settings. · The WPS screen (Section 3.

7 on page 46) lets you configure your NWD2205's Wi-Fi Protected Setup (WPS) options as well as establish and manage WPS connections. · The Information screen (Section 3.8 on page 48) lets you view the information about which version of the driver and utility you are currently using. 3.1.2 What You Need to Know The following terms and concepts may help as you read through this chapter. Wired Equivalent Privacy (WEP) Although one of the original wireless encryption protocols, WEP is also the weakest. Many people use it strictly to deter unintentional usage of their wireless network by outsiders. NWD2205 User's Guide 37 Chapter 3 ZyXEL Utility - Mac OS X Wi-Fi Protected Access (WPA) The WPA protocol affords users with vastly stronger security than WEP. It comes in two different varieties: WPA and WPA2.

Always try to use WPA2 as it implements the full version of the security standard and WPA does not. Pre-Shared Key (PSK) A pre-shared key is a password shared between the server and the client that unlocks the algorithm used to encrypt the data traffic between them. Without the proper password, the client and the server cannot communicate. Extensible Authentication Protocol (EAP) An enhanced security framework designed to improve an existing security protocol, such as WPA-PSK or WPA2-PSK. 3.

1.3 Before You Begin · Make sure the Mac OS X version of the ZyXEL utility is already installed on your computer. See Section 1.3 on page 15 for more information. · After installation, make sure you repair permissions on your installation drive.

Click Applications > Utilities > Disk Utility or do a Spotlight search for the key words "Disk Utility" and select it from the search results list. When the Disk Utility application opens, select your installation drive and then click the Repair Disk Permissions button. 3.2 ZyXEL Utility Screen Summary This section describes the ZyXEL utility screens in Mac OS X. Figure 10 ZyXEL Utility: ZyXEL Utility Menu Summary The following table describes the menus.

Table 3 ZyXEL Utility: Menu Summary TAB Link Status Profiles DESCRIPTION Use this screen to see your current connection status, configuration and data rate statistics. Use this screen to add, delete, edit or activate a profile with a set of wireless and security settings. 38 NWD2205 User's Guide Chapter 3 ZyXEL Utility - Mac OS X Table 3 ZyXEL Utility: Menu Summary (continued) TAB Available Network DESCRIPTION Use this screen to: · · · scan for a wireless network configure wireless security (if activated on the selected network) connect to a wireless network Advanced Setting WPS Information Use this screen to configure advanced settings on your NWD2205. Use this screen to configure the WPS (Wi-Fi Protected Security) settings on your NWD2205. Use this screen to find the utility and driver version.

3.3 The Link Status Screen This screen allows you to view the status of the NWD2205's wireless connection with an AP or peer computer. Figure 11 ZyXEL Utility: Link Status NWD2205 User's Guide 39 Chapter 3 ZyXEL Utility - Mac OS X The following table describes the labels in this screen. Table 4 ZyXEL Utility: Link Status LABEL MAC Address SSID DESCRIPTION This field displays the MAC address of the NWD2205. The SSID (Service Set IDentifier) identifies the wireless network to which a wireless station is associated. @@@@@@@@@@This displays the channel number of the current wireless connection. @@@@@This shows the strength of the antenna's signal. @@@@@@This is the name of the pre-configured profile. @@@@Click this to create a new profile. Click this to alter the settings of a selected profile.
Click this to delete a selected profile from the list. @@@@Channel DESCRIPTION Enter a descriptive name in this field. Enter the SSID of the wireless device to which you want to associate. @@@@@@@@@@@@@@SHARED_KEY mode security is used with WEP (Wired Equivalent Privacy). WPA_PSK security uses a pre-shared key.
All the wireless devices on the network use the same key to access the network. This option is not available in ad-hoc mode. WPA2_PSK is an improved version of WPA-PSK security. This option is not available in ad-hoc mode. WPA-None is available only when you select to connect to another wireless-enabled computer.
When you select OPEN_SYSTEM in the Network Authentication field, either select No Encryption to use no security (Open), or select WEP to use Wired Equivalent Privacy security (Shared) for data encryption. When you select SHARED_KEY in the Network Authentication field, this displays WEP and the NWD2205 uses Wired Equivalent Privacy security for data encryption. When you select WPA-None, WPA_PSK or WPA2_PSK in the Network Authentication field, select TKIP to use the Temporal Key Integrity Protocol. Alternatively, select AES to use the Advanced Encryption Standard. Data Encryption · · · ASCII This field is configurable when you select to use WEP for data encryption. Select this option to enter ACII keys that use numerals and all letters. Otherwise, you need to enter Hexadecimal keys that use numerals and the letters a~f only. Network Key Enter the network's pre-shared key (8~64 uppercase or lowercase letters and numbers) or WEP key. Check with your network's administrator for the correct settings. Enter the network key again for confirmation.

This field is configurable when you select to use WEP for data encryption. Select the key number (1~4) and enter the WEP key in the network key fields. Confirm network key. Key index (advanced) Cancel OK Click this to return to the previous screen without saving your settings. Click this to save your settings and return to the previous screen. NWD2205 User's Guide 43 Chapter 3 ZyXEL Utility - Mac OS X 3.5 The Available Network Screen This screen allows you to view available networks and connect to a network. Figure 14 ZyXEL Utility: Available Network The following table describes the labels in this screen. Table 7 ZyXEL Utility: Available Network LABEL Associated SSID Channel Network Type Encryption DESCRIPTION An "" (asterisk) indicates a connection to the associated wireless device. This displays the network's Service Set IDentifier.*
The SSID is the name of the network. This displays the wireless channel on which the network is operating. This field displays the network type (Infrastructure or Ad Hoc) of the wireless device. This displays whether WEP, WPA, WPA2, WPA-PSK TKIP or WPA2PSK AES, WPA(2)-PSK AES/TKIP is used on the network. If the network uses no security, No Encryption displays.
This displays the Basic Service Set IDentifier. The BSSID is the MAC (Media Access Control) address of the access point or peer wireless device. Every networking device has a unique MAC address, which identifies it on the network. Click this to update the list. Click this to connect to the highlighted wireless network.
Click this to go to the Profile Properties screen to add the selected wireless device in a profile. BSSID Refresh Connect Add to Profile 44 NWD2205 User's Guide Chapter 3 ZyXEL Utility - Mac OS X 3.6 The Advanced Setting Screen This screen allows you to configure advanced network settings on your NWD2205. Figure 15 ZyXEL Utility: Advanced Setting The following table describes the labels in this screen. Table 8 ZyXEL Utility: Advanced Setting LABEL 802.11b Preamble Mode DESCRIPTION Preamble is used to signal that data is coming to the receiver. Select the preamble type that the AP uses. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support Long preamble, but not all support short preamble.

Select Auto to have the NWD2205 automatically use short preamble when all access point or wireless stations support it; otherwise the NWD2205 uses long preamble. Note: The NWD2205 and the access point or wireless stations MUST use the same preamble mode in order to communicate. QOS Mode PSP XLink Mode Select Enable to enable Wi-fi MultiMedia Quality of Service on the NWD2205. Select Enable to allow ad-hoc network building with the PSP KAI game server. Otherwise, select Disable. NWD2205 User's Guide 45 Chapter 3 ZyXEL Utility - Mac OS X Table 8 ZyXEL Utility: Advanced Setting (continued) LABEL Fragment Threshold RTS Threshold Refresh Apply Set Default DESCRIPTION Select the packet size above which the NWD2205 fragments (breaks up) the packet into smaller pieces. Select the packet size above which the NWD2205 transmits an RTS (Request To Send) message. Click this to update this screen. Click this to save your settings. Click this to set every field in this screen to its default value.
3.7 The WPS Screen This screen allows you to configure the NWD2205's Wi-Fi Protected Security (WPS). Figure 16 ZyXEL Utility: WPS The following table describes the labels in this screen.

Table 9 ZyXEL Utility: WPS LABEL SSID Channel DESCRIPTION This field indicates the WPS-compatible AP's Service Set Identification (SSID), which is within range of the NWD2205. This field indicates the channel on which the AP is broadcasting.

46 NWD2205 User's Guide Chapter 3 ZyXEL Utility - Mac OS X Table 9 ZyXEL Utility: WPS (continued) LABEL Security BSSID SCAN PIN PIN DESCRIPTION This field indicates the type of authentication and encryption required by the AP. This field indicates the AP's MAC address. Click this button to rescan the local area for WPS-compatible devices. This field displays a randomly generated 8-digit personal identification code for your NWD2205. Click this button to make a PIN-based WPS connection.

For details, see Section 2.4.2 on page 30. Note: For most WPS connections, this button or the PBC button are all you need. PBC Click this button to make a PBC-based WPS connection. For details, see Section 2.4.1 on page 30. Note: For most WPS connections, this button or the PIN button are all you need. Cancel Click this button to stop scanning and/or making a WPS connection.

NWD2205 User's Guide 47 Chapter 3 ZyXEL Utility - Mac OS X 3.8 The Information Screen This screen shows you the driver, utility version of your NWD2205. Figure 17 ZyXEL Utility: About The following table describes the labels in this screen. Table 10 ZyXEL Utility: About LABEL Version DESCRIPTION This section displays the version number and release date of the NWD2205's wireless utility application. 48 NWD2205 User's Guide CHAPTER 4.1 Overview 4 Troubleshooting This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories. · Power, Hardware Connections, and LEDs · Accessing the ZyXEL Utility · Link Quality · Problems Communicating with Other Computers 4.2 Power, Hardware Connections, and LEDs The NWD2205 does not turn on. None of the LEDs turn on.

1 2 3 Make sure the NWD2205 is correctly installed. Restart the computer to which the NWD2205 is attached. If the problem continues, contact the vendor. One of the LEDs does not behave as expected. 1 Make sure you understand the normal behavior of the LED.

See Section 1.2 on page 14. Check the hardware connection. Restart the computer to which the NWD2205 is attached. 2 3 NWD2205 User's Guide 49 Chapter 4 Troubleshooting If the problem continues, contact the vendor.

4 4.3 Accessing the ZyXEL Utility I cannot access the ZyXEL Utility 1 2 3 Make sure the NWD2205 is properly inserted and the LEDs are on. Install the NWD2205 on another computer. If the error persists, you may have a hardware problem. In this case, you should contact your vendor. 4.4 Link Quality The link quality and/or signal strength is poor. 1 Scan for and connect to another AP with a better link quality using the Available Network 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 from a microwave oven, or another AP using the same channel) around your wireless network.

Lower the output power of each AP. Make sure there are not too many wireless stations connected to a wireless network. 2 3 4 50 NWD2205 User's Guide Chapter 4 Troubleshooting 4.5 Problems Communicating with Other Computers The computer with the NWD2205 installed cannot communicate with the other computer(s). In Infrastructure Mode · Make sure that the AP and the associated computers are turned on and working properly. · Make sure the NWD2205 computer and the associated AP use the same SSID. · Change the AP and the associated wireless clients to use another radio channel if interference is high. · Make sure that the computer and the AP share the same security option and key. Verify the settings in the Profile Properties screen. · If you are using WPA(2) or WPA(2)-PSK security, try changing your encryption type from TKIP to AES or vice versa.

In Ad-Hoc Mode · Verify that the peer computer(s) is turned on. · Make sure the NWD2205 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 settings. · Change the wireless clients to use another radio channel if interference is high. NWD2205 User's Guide 51 Chapter 4 Troubleshooting 52 NWD2205 User's Guide CHAPTER Table 11 Product Specifications PHYSICAL AND ENVIRONMENTAL Product Name Interface Standards NWD2205 Wireless N USB Adapter USB 2.

0 IEEE 802.11b IEEE 802.11g IEEE 802.11n Operating Frequency Antenna Type Antenna Peak Gain 2.4GHZ PIFA (Planar Inverted F Antenna) Left: 2.8 dBi Right: 2.9 dBi Operating Temperature 0 - 50 degrees Celsius 5 Product Specifications Storage Temperature Operating Humidity Storage Humidity Voltage -30 - 70 degrees Celsius 20 - 90% (non-condensing) 10 - 90% (non-condensing) 5V Power Saving Mode Current Consumption Yes Transmit: <315 mA Receive: <250 mA Device Weight Device Dimensions 3g 18 mm (L) x 6 mm (W) x 36 mm (H) RADIO SPECIFICATIONS Transmit Power (+/- 1.5 dB) 802.11b: 18.5 dBm 802.11g: 16.5 dBm 802.11n: @ HT20: 16.5 dBm @ HT40: 16.5 dBm NWD2205 User's Guide 53 Chapter 5 Product Specifications Table 11 Product Specifications (continued) FCC and NCC RF Output Power 802.

11b: 18.1 dBm 802.11g: 24.5 dBm 802.11n: @ HT20: 28.3 dBm @ HT40: 27.7 dBm Receiver Sensitivity 802.11b: 11Mbps at -88 dBm 802.11g: 54Mbps at -74 dBm 802.11n: HT20 at -65 dBm HT40 at -63 dBm WIRELESS STANDARDS IEEE 802.

11b Operation Frequency Operation Channels Dynamically shifts between 11, 5.5, 2, and 1 Mbps network speed. 2.412GHz~2.472GHz N. America & Taiwan 2.412GHz~ 2.462GHz 1-11 Euro ETSI 2.412GHz~ 2.472GHz 1-13 IEEE 802.

11g Operation Frequency Operation Channels Dynamically shifts between 54, 48, 36, 24, 18, 12, 9 and 6 Mbps network speed. 2.412GHz~2.472GHz N. America & Taiwan 2.412GHz~ 2.462GHz 1-11 Euro ETSI 2.412GHz~ 2.472GHz 1-13 IEEE 802.11n Downstream data rate Upstream data rate Operation Frequency Operation Channels 300 Mbps 300 Mbps 2.

412GHz~ 2.472GHz 1-13 N. America & Taiwan HT20 2.412GHz~ 2.462GHz 1-11 N. America & Taiwan HT40 2.422GHz~ 2.452GHz 3-9 Euro ETSI HT20 2.412GHz~ 2.472GHz 1-13 Euro ETSI HT40 2.

422GHz~ 2.462GHz 3-11 Networking Mode Infrastructure, Ad-Hoc, SoftAP Support 54 NWD2205 User's Guide Chapter 5 Product Specifications Table 11 Product Specifications (continued) Approvals Safety European Union: EN60950 (CE-LVD) EMI United States: FCC Part 15B Class B Canada: ICES-003 European Union: CE EN 55022 Class B, CE EN 301489-1 Australia: C-Tick EMS European Union: CE EN55024, CE EN 301489-17 RF United States: FCC Part 15C, FCC SAR Canada: RSS-210 European Union: CE EN 300 328 Taiwan: NCC LP0002 Wi-Fi Certification 11 b/g/n WPA/WPA2/WPS Microsoft Certification WHQL: Windows 7 (32- and 64-bit), Windows Vista (32and 64-bit), Windows XP (32- and 64-bit) SOFTWARE SPECIFICATIONS Device Drivers Windows 7 (32- and 64-bit) Windows Vista (32- and 64-bit) Windows XP (32- and 64-bit) Mac OS X (10.

4/10.5/10.6) WIRELESS FEATURES Wireless Security WEP 64bit, 128bit, WPA, WPA-PSK, WPA2, WPA2-PSK 802. 1x (EAP-TLS, EAP-TTLS, EAP-PEAP), WPS. Note: EAP-TTLS is not supported in Windows Vista and Windows 7. Wireless QoS Wi-Fi Protected Setup (WPS) Other Wi-Fi Multi Media (WMM) Push button configuration Use device's PIN WMM power-saving support Compatible with Windows Zero Configuration NWD2205 User's Guide 55 Chapter 5 Product Specifications 56 NWD2205 User's Guide APPENDIX Ad-hoc Wireless LAN Configuration A Wireless LANs This appendix discusses ad-hoc and infrastructure wireless LAN topologies. The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). 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. Figure 18 Peer-to-Peer Communication in an Ad-hoc Network NWD2205 User's Guide 57 Appendix A Wireless LANs 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). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client A and B can still access the wired network but cannot communicate with each other. Figure 19 Basic Service Set 58 NWD2205 User's Guide Appendix A Wireless LANs ESS An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS). This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. An ESSID (ESS IDentification) uniquely identifies each ESS.

All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate. Figure 20 Infrastructure WLAN Channel A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance. Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an NWD2205 User's Guide 59 Appendix A Wireless LANs adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11. RTS/CTS A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node.

Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other. Figure 21 RTS/CTS When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations. RTS/CTS is designed to prevent collisions due to hidden nodes. An RTS/CTS defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked. When a data frame exceeds the RTS/CTS value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission. Stations can send frames smaller than the specified RTS/CTS directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure RTS/CTS if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake. 60 NWD2205 User's Guide Appendix A Wireless LANs If the RTS/CTS value is greater than the Fragmentation Threshold value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. Fragmentation Threshold A Fragmentation Threshold is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames. A large Fragmentation Threshold is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference. If the Fragmentation Threshold value is smaller than the RTS/CTS value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach RTS/CTS size. Preamble Type Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.

11 compliant wireless adapters support long preamble, but not all support short preamble. Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks. Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications. Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NWD2205 uses long preamble. Note: The wireless devices MUST use the same preamble mode in order to communicate.

NWD2205 User's Guide 61 Appendix A Wireless LANs IEEE 802.11g Wireless LAN IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.

11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.

11g data rate and modulation are as follows: Table 12 IEEE 802.11g DATA RATE (MBPS) 1 2 5.5 / 11 6/9/12/18/24/36/ 48/54 MODULATION DBPSK (Differential Binary Phase Shift Keyed) DQPSK (Differential Quadrature Phase Shift Keying) CCK (Complementary Code Keying) OFDM (Orthogonal Frequency Division Multiplexing) Wireless Security Overview Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network. Wireless security methods available on the NWD2205 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NWD2205 identity. The following figure shows the relative effectiveness of these wireless security methods available on your NWD2205.

Table 13 Wireless Security Levels SECURITY LEVEL Least Secure SECURITY TYPE Unique SSID (Default) Unique SSID with Hide SSID Enabled MAC Address Filtering WEP Encryption IEEE802.1x EAP with RADIUS Server Authentication Wi-Fi Protected Access (WPA) WPA2 Most Secure 62 NWD2205 User's Guide Appendix A Wireless LANs Note: You must enable the same wireless security settings on the NWD2205 and on all wireless clients that you want to associate with it. IEEE 802.1x In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are: · User based identification that allows for roaming. · Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.

· Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients. RADIUS RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks: · Authentication Determines the identity of the users. · Authorization Determines the network services available to authenticated users once they are connected to the network. · Accounting Keeps track of the client's network activity. RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server. Types of RADIUS Messages The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication: · Access-Request Sent by an access point requesting authentication. NWD2205 User's Guide 63 Appendix A Wireless LANs · Access-Reject Sent by a RADIUS server rejecting access. · Access-Accept Sent by a RADIUS server allowing access.

· Access-Challenge Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message. The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting: · Accounting-Request Sent by the access point requesting accounting. · Accounting-Response Sent by the RADIUS server to indicate that it has started or stopped accounting. In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know.

The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access. Types of EAP Authentication This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types. EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.

1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication. The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. . For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner. 64 NWD2205 User's Guide Appendix A Wireless LANs 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.