**WLAN是什麼？**

　　其實所謂的「無線」有很多種，例如藍芽（Bluetooth）、GSM/GPRS、3G或對講機使用的無線技術，都可以算是廣義無線技術的一種，因此如果廣泛的講「無線產品」或「無線網路產品」事實上不是很精確，我們大部分時候談到「無線網路」，其實都是指WLAN（Wireless Local Area Network），也就是「無線區域網路」。更用嚴謹的方式來講，WLAN指基於IEEE訂製的802.11系列的無線傳輸標準，最常見的便是傳輸頻寬包括802.11a、802.11b、802.11g，或安全標準802.11i等。

**只是無線的「區域」網路**

其實WLAN無線區域網路顧名思意就只是指透過無線化的區域網路，可視為取代或延伸傳統乙太網路的一種方式。簡單而言，它所能發揮的功能就是把家中原本用來連結ADSL Modem和電腦的那條網路線換成無線而已，也就是說，除非廠商在希臘該景點或玉山頂拉一條ADSL或T1網路，然後架起WLAN，不然廣告中的美好情景基本上是不太可能發生在現實生活。

　　在前幾年網路興起時，「最後一哩」（Last mile）這個名詞相當流行，最後一哩泛指從ISP業者連接到用戶端（家庭或企業）的線路，從這個角度來看，WLAN只是最後一哩的最後幾公尺而已；如果你真的想要隨時隨時無線上網，那麼或許選則手機會通就可以上網的GPRS會比較符合你的需求。

**串連WLAN：熱點**

雖然我們在上面講到WLAN只是區域的無線技術，傳輸距離可能只有幾十公尺，但實際上還是讓在外奔波的我們有一個上網的好管道。所謂「hot spot」是指可提供消費者透過WLAN無線上網的地點，消費者只需自備裝WLAN筆記型電腦，或掌上型電腦即可接收到「熱點」所發出的高速無線訊號。

　　無線上網的熱點已經相當普遍，例如全台麥當勞都已經建制WLAN，台北市政府也正在推動一個網路新都計畫，目前已在多個捷運站建制hot spot，未來計畫逐漸覆蓋台北市90%以上的區域；其他縣市也有類似的hot spot建制，在「無線網路示範計畫」下，淡水八里一帶也已經有帶狀的熱點區域，各縣市都有類似這種示範區域。雖然仍然不太可能出現上述廣告中那種連玉山也可上網的情形，但確定的是，只要帶台WLAN NB/PDA出門，可以上網的地點越來越多。

**Wi-Fi CERTIFIED** Wi-Fi認證標誌

WLAN還有另一種Wi-Fi的說法。IEEE制訂802.11系列標準時，仍然有些模糊地帶，為了確保WLAN產品的互通性，便有些廠商成立Wi-Fi聯盟進行認證的工作，只要認證過的WLAN產品，Wi-Fi聯盟都會給予一個Wi-Fi認證標誌(Wi-Fi CERTIFIED)；當然大部分的802.11產品可以互相連結，但為防萬一，在選購時最好找到有Wi-Fi聯盟認證的產品。

**WLAN基礎規格**

　　現在我們對WLAN常見名詞及使用方式已經有一些概念，我們在這裡進一步討論基礎WLAN規格。

**802.11a/b/g**

　　802.11a/b/g是WLAN的頻寬規格，基本上802.11b/g採用同樣的2.4GHz頻段，802.11a則使用5.XGHz，因此802.11b/g是可以相容的，但802.11a只能和802.11a的產品相互連結。頻寬部分，802.11a/g都號稱理論值達54Mbps(每秒約6.75MB)，不過實際上都只有一半22Mbps約每秒2.75MB；802.11b理論值達11Mbps，不過實際使用也僅一半。

**802.11a/b/g比較表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 標準名稱 | 傳輸頻寬（理論/實際） | 傳輸距離 | 使用頻段 | 普及度 |
| 802.11a | 約54Mbps（22Mbps） | 約30公尺 | 5GHz | 少 |
| 802.11b | 11Mbps（5Mbps） | 40-50公尺 | 2.4GHz | 最多 |
| 802.11g | 約54Mbps（22Mbps） | 40-50公尺 | 2.4GHz | 多 |

　　不管802.11a/b/g，其實傳輸距離主要都在幾十公尺之間，差異不大，我們在上表列出是一般廠商會宣稱的距離，不過有些產品會特別加強這部分，例如裝上更好的接收天線或加強訊號功率等，有些產品更可以達1公里以上，如果對距離有特定需求，例如想透過WLAN無線分享兩棟大樓的網路，可能就得選購高階一點的產品，或購買指向性天線強化雙方訊號。

　　那麼我們要怎麼選擇802.11a/b/g呢？很簡單，首先是802.11a，如果你的電腦或企業網路並沒有802.11a的需求，那麼建議就直接排除這種規格，由於802.11a在台灣的普及度最低，導致產品價格較高，雖然拿到歐洲還是日本某些地方或許802.11a反而比較普及，但在台灣還是其他兩種規格的天下。

　　802.11b/g都是使用2.4GHz頻段，兩者也相容，前年Intel推動Centrino時，主要搭配的就是802.11b的無線網卡，雖然有逐漸轉換到802.11b/g雙模的趨勢，但目前的確還是802.11b最為普及，大部分的熱點也都是用802.11b規格。

　　建議802.11b/g的選擇還是得由價格與需求為考量，如果你挑到的AP或無線網卡802.11g價格與802.11b差不多，那麼直接選購802.11g，反之就選擇802.11b。因為只要802.11g WLAN環境中有個802.11b裝置，那麼整體傳輸速率就會受到影響，除非全部都是採用802.11g的裝置；另外一個原因是除非你有透過WLAN區域網路檔案對傳的需求，因為g的傳輸速度為每秒2.75MB左右，b的速度為大約每秒600k，如果真的對區域網路速度很敏感，那麼就選購還是比較快的g。

　　至於連外上網，因為目前大部分的ADSL下傳速度為2M(每秒250K)，802.11b已經比較快了，因此單傳的連外上網是不會因為b或g而改變，因此b和g並沒有差別。

**WEP/WPA/802.11i**

簡單介紹這三種WLAN安全規格。

　　WEP全名為(Wired Equivalent Privacy)，是最早也是最基礎的一種WLAN加密技術，運作原理是透過靜態、非交換式的金鑰加密，金鑰有一定長度(可能為64bit或128bit)，靜態金鑰式的技術便已被證明容易被破解，設定方式也相當簡單，只要在無線橋接器(Access Point)及電腦端設定一樣的密碼(金鑰)即可。

　　WPA(Wi-Fi protected access)則是WEP的加強版，也是我們下面要提到的802.11i標準的一部份；WPA在2003年時獲得Wi-Fi聯盟支持。簡單來說，WPA的加入是讓WLAN在WEP之外多了一層保護。之前已經談到WEP的金鑰是靜態的，但WPA在連線過程中，會有動態不同加密金鑰產生，在傳輸過程中會不斷改變，比較不容易被暴力破解(如不斷使用駭客程式嘗試各種密碼)。由於很多WLAN可以透過韌體升級支援WPA，如果購買到僅具有WEP的WLAN產品，最好上廠商網站看看是否有升級程式，幫脆弱的WEP加密增加一些安全性。

**無線基地台(無線AP)**

　　無線基地台(無線AP)無線基地台通常也會被稱為AP(Access Point)。無線AP可以視為WLAN中的hub，就像過去使用區域網路連線一樣，兩台電腦想要互連，除了用跳線之外，就必須使用hub，此外兩台電腦想要同時連上網路(Cable、ADSL)，如果Cable Modem或ADSL modem沒有多個RJ-45接孔，那也必須透過hub來連接上Internet。

　　 如果你已經有了一個可提供IP分享功能的ADSL Modem或是IP分享器，那麼想要建構無線網路環境最便宜的方案就是直接加一個無線基地台在網路中，僅需用一條網路線連接IP分享器和無線AP，做好設定即可。

　　這種最基本的無線AP只具備溝通Internet來源(Cable、ADSL等等)和用戶端無線網路的功能，當然應該也會有一點基本的加密保護，如WEP，不過這種純粹當作無線AP的產品越來越少了，主要原因在於現在已經可以用軟體將無線網卡模擬成AP，雖然在安全性和部分功能依然比不上硬體AP，但是因為便宜，對於一般使用者也是不錯的方法。

　　單純僅AP功能的裝置還有另外一個優勢，就是因為僅需提供一個RJ-45接孔，所以可以做的很小，如先前提到的華碩WL-330g和蘋果的AirPort Express，提供攜帶方便的選擇。

**無線路由器(無線寬頻分享器)**

無線路由器是目前市面上最常見的提供無線連接的裝置，有些廠商則會命名為無線寬頻分享器。和無線AP相比，無線路由器很像IP分享器+無線AP，也就是它可以提供四個RJ-45接孔(較常見的數量)的乙太網路連線，還可以提供無線網路連接的功能。大部分的無線路由器都具備DHCP伺服器的功能，也就是可以自動分配每一個客戶端一個虛擬IP，所以即便你只有一個真實IP，也可以讓全家人一起同時上網。目前大部分的無線路由器功能差異性不大，通常都會具有DHCP、NAT、DMZ等功能，少數為了強調差異性則會再加入如FTP Server、Print Server等功能。

NAT和DMZ的目的為了讓外面的使用者能夠連上內部的虛擬IP，也就是說即便是使用虛擬IP，內部網路的使用者也可以架設一台伺服器。

　　NAT是network address translation，使用者可以自行指定某一個連接埠要對應到某一個內部網路的虛擬IP中，如果是192.168.1.2這台PC架了一個Web Server，那麼NAT就要設定成將80 port(http協定的預設連接埠)連接到192.168.1.2。

　　DMZ是 DeMilitarized Zone，和NAT不同的是，NAT是將某一個或多個連接埠對應到某一個IP上，而DMZ則是直接將內部某一個IP對應到外部真實IP上。

　　其他的功能則要看使用者的需求而定，一般來說，越多的功能、越高的安全性，代表著越高的價格，這是必然的事情。