**WLAN是什麼？**

　「無線」有很多種，如藍芽(Bluetooth)、GSM/GPRS、3G或對講機使用的無線技術，都可算是廣義無線技術，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，大部分時候談到「無線網路」，都是指WLAN(Wireless Local Area Network)，也就是「無線區域網路」。嚴謹的講，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**

WLAN無線區域網路就只是指透過無線化的區域網路，可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。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；如果真的想要隨時隨時無線上網，那麼或許選擇手機就可以上網的GPRS較符合需求。

**串連WLAN：熱點**

雖然上面講到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。

**WLAN基礎規格**

**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5GHz，因此802.11b/g是可相容的，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，不過實際也僅一半而已。

**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。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。

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的安全性**

**WEP**: WEP全名為(Wired Equivalent Privacy)，它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(64bit或128bit)，但數年前，靜態金鑰式的技術便已經被證明容易被破解。

**WPA**: WPA(Wi-Fi protected access)是WEP的加強版，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。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(例如不斷使用駭客程式嘗試各種密碼)。

**802.11i**

802.11i是IEEE通過的802.11系列無線網路安全機制標準。802.11i涵蓋了之前加密技術的原理，在802.11i通過後，Wi-Fi聯盟也開始展開WPA2的認證，WPA2的規格包含在802.11i規定之內。802.11i和之前WPA最大的不同是增加「先進加密標準」(Advanced Encryption Standard)安全機制，可支援128、192及256位元金鑰的編碼。

**無線基地台(無線AP)**

　　無線基地台通常被稱為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。

**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。它提供四個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，因此即便使用虛擬IP，內部網路的使用者也可架設一台伺服器。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。

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**網路上常用的加密有兩種**：

* WEP加密，將密碼編成 64 bit 或 128 bit 密碼，由於演算法的漏洞，所以有被竄改資料和密碼的可能。
* WPA加密，又分為兩種不同加密機制，透過802.1X認證伺服器(密碼儲存於RADIUS伺服器上)以及PSK (Pre-shared key預設公鑰，此方法又被稱為WPA person version)。後者較不安全但設定簡單。由於WPA用的RC4加密法仍有弱點，較安全的作法是使用WPA2(使用AES加密)。

設定加密機制，除了用戶端需要支援WPA2加密外，AP的韌體也須支援WPA2加密。有些AP僅支援TKIP演算法而不支援AES演算法。因為AES會自動偵測加密機制，用戶端完全不需要任何設定即可使用，使用TKIP則需要事先建立加密設定檔，並儲存SSID（AP 編號）與加密設定檔的關聯。如前所述認證是用來管制無線網路的使用權限，常見的方式有兩種：

* 鎖定網卡Mac位址。
* 使用Captive Portal機制，當用戶上網時將網頁重導向到認證網頁上進行認證。

802.1x協議起源於802.11協議，後者是標準的無線局域網協議，802.1x協議的主要目的是為了解決無線局域網用戶的接入認證問題。802.1x是IEEE為解決基於端口的接入控制(Port-Based Access Control)而定義的一個標準。  
1、802.1X是一個認證協議，是一種對用戶進行認證的方法和策略。  
2、802.1X是基於端口的認證策略(端口可以是實在的物理端口或像VLAN的邏輯端口，無線局域網的“端口”即一條信道)。  
3、802.1X的認證的最終目的是確定端口是否可用。一個端口如果認證成功就“打開”端口，允許所有的報[文通](http://corp.it168.com/corp/1772_index.shtml)過；如果認證失敗就使端口保持“關閉”，只允許802.1X的認證報文EAPOL(Extensible Authentication Protocol over LAN)通過。

802.1X的認證體系分為三部分結構：(1) [Supp](http://corp.it168.com/corp/3055_index.shtml)licant System，客戶端(PC/網絡設備)。(2) Authenticator System，認證系統。(3) Authentication Server System，認證[服務器](http://product.it168.com/files/0402search.shtml" \t "_blank)。

**認證過程**:

1、認證通過前，通道的狀態為unauthorized，只能通過EAPOL的802.1X認證報文；

2、認證通過時，通道的狀態切換為authorized，從遠端認證[服務器](http://server.it168.com/)可傳遞來用戶的信息，如VLAN、CAR參數、優先級、用戶的訪問控制列表等等；用戶的流量就將接受上述參數的監管，此時該通道可通過任何報文，只有認證過後才有DHCP等過程。

3、Supplicant System-Client(客戶端)是—需要接入LAN，及享受switch提供服務的設備(如PC機)，客戶端需要支持EAPOL協議，客戶端必須運行802.1X客戶端[軟件](http://software.it168.com/" \t "_blank)，如：802.1 X-complain、Windows XP等

# Wi-Fi Protected Access

**Wi-Fi Protected Access** (**WPA**) and **Wi-Fi Protected Access II** (**WPA2**) are two security protocols and security certification programs developed by the [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, [WEP (Wired Equivalent Privacy)](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy).

## WPA

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the [Temporal Key Integrity Protocol](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol) (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the [cyclic redundancy check](http://en.wikipedia.org/wiki/Cyclic_redundancy_check) (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled.

## WPA2

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces [CCMP](http://en.wikipedia.org/wiki/CCMP), a new [AES](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)-based encryption mode with strong security.

## Hardware support

WPA was specifically designed to work with wireless hardware that was produced prior to the introduction of the WPA protocol which had only supported inadequate security through [WEP](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy). Some of these devices support the security protocol only after a [firmware](http://en.wikipedia.org/wiki/Firmware) upgrade. Firmware upgrades are not available for some legacy devices.

Wi-Fi devices certified since 2006 support both the WPA and WPA2 security protocols. WPA2 may not work with some older network cards.

## Security

[Pre-shared key](http://en.wikipedia.org/wiki/Pre-shared_key) mode (PSK, also known as *Personal* mode) is designed for home and small office networks that don't require the complexity of an [802.1X](http://en.wikipedia.org/wiki/802.1X) authentication server. Each wireless network device encrypts the network traffic using a 256 bit [key](http://en.wikipedia.org/wiki/Key_(cryptography)). This key may be entered either as a string of 64 [hexadecimal](http://en.wikipedia.org/wiki/Hexadecimal) digits, or as a [passphrase](http://en.wikipedia.org/wiki/Passphrase) of 8 to 63 [printable ASCII characters](http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters). If ASCII characters are used, the 256 bit key is calculated by applying the [PBKDF2](http://en.wikipedia.org/wiki/PBKDF2) [key derivation function](http://en.wikipedia.org/wiki/Key_derivation_function) to the passphrase, using the [SSID](http://en.wikipedia.org/wiki/SSID#Service_set_identification_.28SSID.29) as the [salt](http://en.wikipedia.org/wiki/Salt_(cryptography)) and 4096 iterations of [HMAC](http://en.wikipedia.org/wiki/HMAC)-[SHA1](http://en.wikipedia.org/wiki/SHA1).

## WPA terminology

Different WPA versions and protection mechanisms can be distinguished based on the version of WPA, the target end-user (according to the method of authentication key distribution), and the encryption protocol used.

### Version

**WPA:** Initial WPA version, to supply enhanced security over the older WEP protocol. Typically uses the TKIP encryption protocol.

**WPA2:** Also known as *IEEE 802.11i-2004*, is the successor of WPA, adds support for CCMP which is intended to replace TKIP encryption protocol.

### Target users (authentication key distribution)

**WPA-Personal:** Also referred to as *WPA-PSK* (Pre-shared key) mode, it is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase.

**WPA-Enterprise:** Also referred to as *WPA-802.1X mode*, and sometimes just *WPA* (as opposed to WPA-PSK). It is designed for enterprise networks and requires a [RADIUS](http://en.wikipedia.org/wiki/RADIUS) authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). An Extensible Authentication Protocol (EAP) is used for authentication, which comes in different flavors.

Note that the WPA-Personal and WPA-Enterprise modes are available with both WPA and WPA2.

[**Wi-Fi Protected Setup**](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)

An alternative authentication key distribution method intended to simplify and strengthen the process, but which, as widely implemented, creates a major security hole (see above).

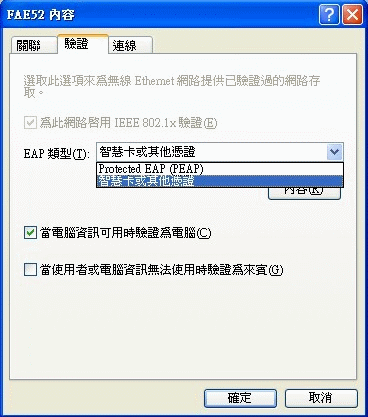
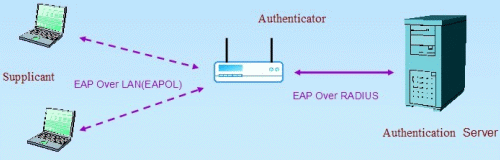
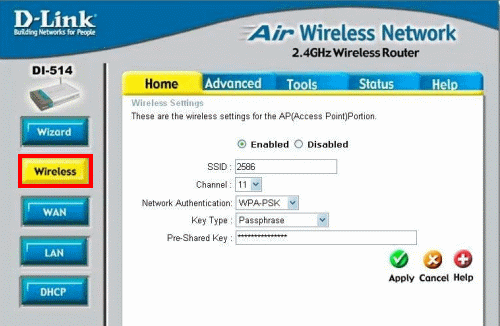
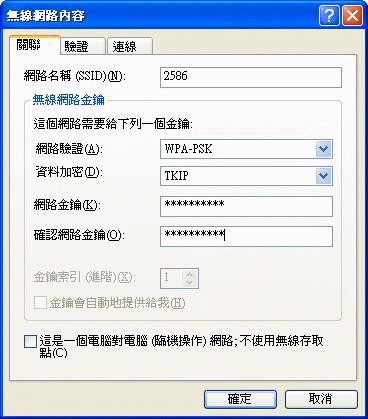
### Encryption protocol

[**TKIP**](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)**(Temporal Key Integrity Protocol):** The [RC4](http://en.wikipedia.org/wiki/RC4) stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. Used by WPA.

[**CCMP**](http://en.wikipedia.org/wiki/CCMP)**:**An AES-based encryption mechanism that is stronger than TKIP. Used by WPA2. Among informal names are "AES" and "AES-CCMP". According to the 802.11n specification, this encryption protocol must be used to achieve the fast [802.11n high bitrate schemes](http://en.wikipedia.org/wiki/IEEE_802.11n-2009#Data_rates), though not all implementations enforce this. Otherwise, the data rate will not exceed 54 MBit/s.

## EAP extensions under WPA and WPA2 Enterprise

In April 2010, the Wi-Fi alliance announced the inclusion of additional [Extensible Authentication Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. This was to ensure that WPA-Enterprise certified products can interoperate with one another.

**一、前言**  
WPA 無線安全是為針對802.11安全漏洞所提出的一種無線安全過渡解決方案，這些安全漏洞包括缺乏認證機制與 WEP(Wired Equivalency Privacy)加密的缺點。以網路驗證機制而言802.11有「開放系統」與「共用金鑰」這兩種方式，但「開放系統」沒有安全性，而「共用金鑰」也因以明碼方式傳送挑戰本文(Challenge Text)，反而因WEP密鑰的暴露而更不安全，至於WEP的加密問題，姑且不談其加密方式已被破解的問題，單單就金鑰的管理，金鑰設定的一致性就可以發現有相當的不方便，若要用於企業環境著實令人擔心。  
**二、WPA安全特性**  
要說明WPA最簡潔的方式就是以WPA = 802.1x + EAP + TKIP + MIC來表示。802.1x與EAP(Extensible Authentication Protocol，延伸驗證協定)是WPA身分驗證的基礎，EAP是實際用來作為802.1x驗證的方法。因為是延伸驗證所以可以作到使用者層級，至於驗證的類型有很多種，就Windows無線網路支援而言，包括支援憑證與智慧卡驗證的 EAP-TLS (EAP -Transport Layer Security)，與支援密碼驗證作業的Protected-EAP-Microsoft Challenge Handshake Authentication Protocol (PEAP-MS-CHAP v2)。  
  
TKIP(Temporal Key Integrity Protocol，暫時密鑰完整性協定)是WPA取代WEP的資料加密方法，以動態方式產生及交換金鑰取代了WEP的單一靜態金鑰，每個封包的金鑰都不一樣，因此安全性大幅改善；至於8位元組的MIC(Message Integrity Protocol，訊息完整性編碼)則取代802.11中的ICV(Integrity Check Value，完整性檢查值)以防止攻擊者攔截、更改甚至重送資料封包，確保資料的完整性。當接收端與傳送端算出來的MIC值不符時，表示資料遭竄改，該封包即被丟棄。  
**三、支援 WPA所需的條件**  
由於WPA必須使用到IEEE802.1x，因此必須架設作為帳號認證的認證伺服器(Authentication Server)，例如微軟的ISA (Internet Authentication Service)伺服器用來管理用戶認證與授權，實際應用上通常會另外架設AD伺服器作為帳號認證的資料庫，AD伺服器可以與IAS伺服器裝在同一台機器上，也可以分開架設。  
  
支援WPA的無線基地台，角色其實只是很單純地轉送無線用戶端與認證伺服器之間的封包傳遞，一般而言無線基地台可以透過韌體升級來支援WPA。關於無線用戶端，必須具有處理WPA資訊能力的無線網路卡與驅動程式，驅動程式可以透過更新來達成。至於無線用戶端所使用的作業系統，如果使用的作業系統是Windows XP SP2或Windows Server 2003，那只需啟用Windows內建的Wireless Zero Configuration service，即可支援WPA；如果作業系統是Windows 2000或是 Windows XP/Windows Server 2003但不打算使用Windows內建的Wireless Zero Configuration service，那您就必須安裝符合 WPA 的無線網路卡設定公用程式。  
**四、WPA的SOHO解決方案**  
對於企業體而言WPA的無線安全方案，是必然的解決方案之一，但對於一般家庭顯得不切實際，因為架設AD或IAS伺服器都不是小工程，況且家庭數位資料並無企業相對的重要性，因而WPA的需要另一套替代方案。WPA-PSK (Pre-Shared Key)不需要驗證伺服器，使用單一字母數字型式的密碼，不像WEP有四組的密鑰選項，設定比WEP簡單安全且具有一致性，比較適合SOHO用戶環境使用。然而在共享密鑰的設定上仍需考慮應有的長度與複雜性，以避免密鑰被破解的危險。  
**五、WPA-PSK 實例應用**  
**《步驟1》** WPA-PSK的設定很容易，以D-Link DI-514無線路由器作為範例。首先進入DI-514設定畫面，選擇 Wireless 選單，選填SSID (Service Set Identification)與Channel之後，最主要在Network Authentication 項目選擇「WPA-PSK」，並且在Pre-Shared Key欄位輸入一組金鑰並且把它記下來。  
  
**《步驟2》**接著在無線用戶端，請開啟無線網路內容再新增一組設定，同樣地在網路驗證選項選擇 WPA-PSK，並且把先前 AP Router 設定紀錄下來的密鑰，在網路金鑰欄位照樣輸入。以上設定必須與AP Router設定相符合，關於網路金鑰設定必需 8~63 個ASCII字元或64個16進位字元，應有一定的複雜性以避免被暴力破解法突破。  
  
**《步驟3》**確定設定無誤之後，我們檢視連線後的畫面(Windows XP SP2)，右上角顯示「已連線」，表示已經正常連線。  
