淺談無線區域網路

引用自：**Matt Foster**，Tom's Hardware Guide 消費性及週邊指南

無線網路歷史概觀

說到無線網路的歷史起源，可能比各位想像的還要古早。無線網路的初步應用，可以追朔到五十年前的第二次世界大戰期間，當時美國陸軍採用無線電信號做資料的傳輸。他們研發出了一套無線電傳輸科技，並且採用相當重度的編碼技術。當初美軍和盟軍都廣泛使用這項科技。這項科技讓許多學者得到了一些靈感，在 1971 年時，夏威夷大學（University of Hawaii） 的研究員創造了頭一個採用封包式技術的無線電通訊網路。這被稱作 ALOHNET 的網路架構，可以算是相當早期的無線區域網路（wireless local area network，WLAN）。這最早的 WLAN 包括了 7 台電腦，它們採用雙向星狀架構（bi-directional star topology，請參考 http://www.its.bldrdoc.gov/fs-1037/ 以及 http://www.webopedia.com/－這兩個網站都是不錯的電腦、通訊用語的資訊來源）橫跨四座夏威夷的島嶼，主電腦則為在主導歐胡島（Oahu Island）上。從這時開始，無線網路可說是正式誕生了。

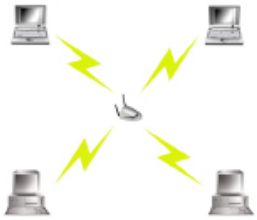
雖然目前幾乎所有的區域網路（LAN）都仍舊是有線的架構，不過近年來無線網路的應用卻日漸增加。主要應用範圍在學術界（像是大學校園）、醫療界、製造業和倉儲業等。而且相關的技術也一直在進步，對企業而言要轉換到無線網路也更加容易、更加便宜了。

無線網路架構

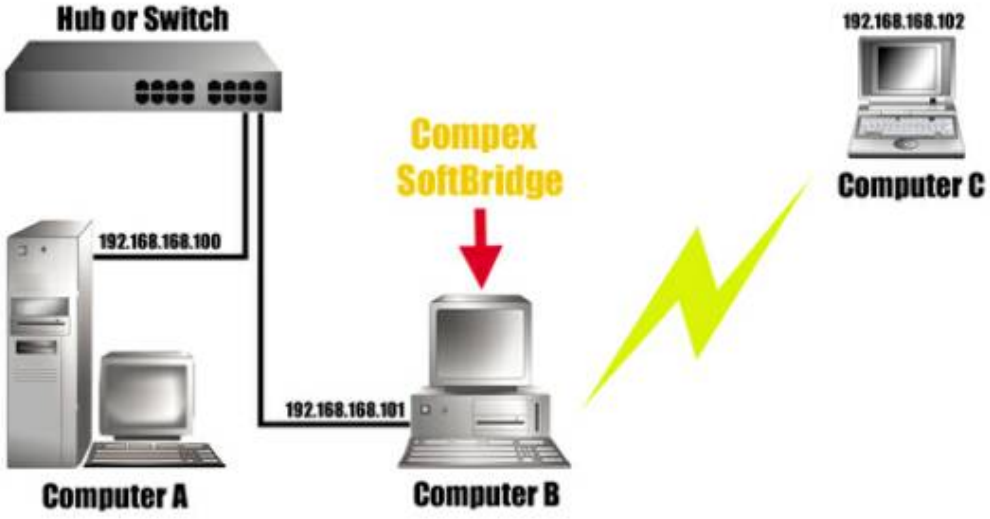
拓樸（Topology）：許多元件的實體（真實）或邏輯（虛擬）群集。

根據以上的定義，我們可以將拓樸看成是「許多節點（是電腦、網路印表機、伺服器等等）在互通網路上的群集」。目前有線網路有五大網路拓樸，分別是匯流排（Bus），環狀（Ring），星型（Star），樹狀（Tree）以及網狀（Mesh）拓樸，不過在無線網路中，只有星狀和網狀兩種派的上用場。

星型拓樸（star topology）是目前最常見的一種，這種架構包含一個通訊用的中央電腦或是存取點（Access Point，AP）。資料封包由來源節點發出後，由中央電腦接收，並且轉送到正確的無線網路目標節點。



這台中央電腦，可以用來當作與有線 LAN 的通訊橋樑，並且用來存取其他有線客戶端、網際網路或是其他網路設備等等。在我們稍後介紹的產品中，Compex SoftBridge 程式就扮演著「軟體橋接器（Bridge）」的角色，讓您不需要使用特殊的硬體或 AP 就可以和有線客戶端與服務做溝通。藉著這套軟體，任何有接上有線網路，並且還配備一塊無線網路卡（Network Interface Card，NIC）的電腦都可以擔任橋接器的任務。



網狀拓樸（mesh topology）和星型拓樸有些不一樣，主要是網狀拓樸並沒有中央電腦。每個節點都散佈在其他電腦可以自由溝通的位置上。

IEEE 802.11，802.11a 和 802.11b 規格標準

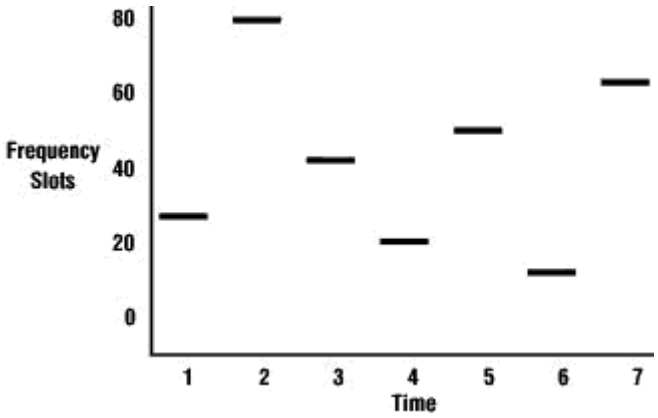
為了讓 WLAN 技術能夠被廣為使用，這些技術必須要建立一種業界標準，以確保各廠商生產的設備都能具有相容性與穩定性。這些標準是由 IEEE（電機電子工程師協會，The Institute of Electrical and Electronics Engineers）所制定的，最早的規格 IEEE 802.11 是在 1997 年提出，接著在 1999 年 9 月又提出了 IEEE 802.11a 和 IEEE 802.11b。

初期的規格制定了在 RF 射頻頻段 2.4GHz 上的運用，並且提供了 1Mbps、2Mbps 和許多基礎訊號傳輸方式與服務的傳輸速率規格。IEEE 802.11a 和 IEEE 802.11b 標準則分別為 5.8GHz 和 2.4GHz 頻段做定義。這兩組新的標準也定義了 IEEE 802.11a 中 5Mbps，11Mbps 到 54Mbps 速率的新實體層。這些標準可以在 ISM（Industrial，Scientific and Medical－工業、科學與醫療應用）頻段上使用，這些頻道包括 902-928MHz（可利用頻寬 26MHz），2.4-2.4835 GHz（可利用頻寬 83.5 MHz），以及 5.725-5.850 GHz（可利用頻寬 125MHz），最後一項也符合 IEEE 802.11a 標準的最高資料速率應用。

這些業界標準定義了無線通訊的實體層（physical/PHY layer）以及媒體存取控制層（Media Access Control/MAC layer）。在這裡所謂的「層（layer）」簡單來說就是一些相關功能的集合，這些功能與其他各自相關的功能有所區別。而在無線網路中層代表的意義，我們用個比喻來說明好了：假設您現在要把一本書（代表資料封包）從房間一角的書架上，拿到另一角的書桌上，那麼 MAC 層就可以當成是一個人把書給拿起來的動作，而 PHY 層則代表了人在房間中走動的動作。

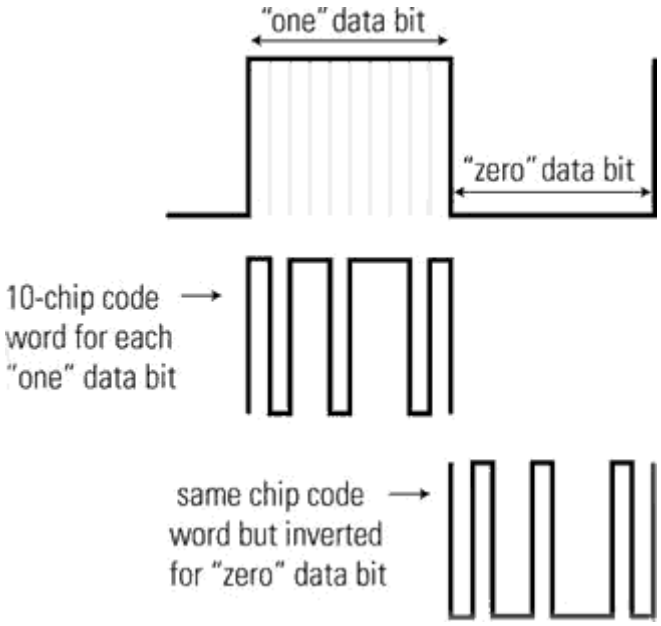
標準中定義的 PHY 層還包括兩種不同的射頻通訊調變方法：分別為直接序列展頻技術（Direct Sequence Spread Spectrum，DSSS）以及跳頻展頻技術（Frequency Hopping Spread Spectrum，FHSS）。兩種方式都是由軍方所研發，並且針對高信賴性、正確性和安全性而設計，它們各有一套獨特的方法來傳送資料。

FHSS 技術是將可用的頻寬帶區域分割成好幾個頻道，它使用的窄頻載波藉著 2 到 4 階的高斯頻移鍵控（Gaussian Frequency Shift Keying，GFSK）不斷的改變。換句話說，傳送時的頻率會在收發雙方節點都知道的範圍間，利用虛擬亂碼（pseudorandom）做任意變動。這對 PHY 層加入了一些安全性。有心的駭客基本上沒有辦法知道接下來要切換到哪一組頻率來接收整個訊號。另外 FHSS 也有一項優點，就是可以讓許多網路共存在一個實體區域中。



DSSS 採用的方法則不太一樣。DSSS 將資料流與一組較高頻率的數位碼結合。每一個資料位元都被對映成一組只有收發兩方才知道的位元樣式。這個位元樣式稱作碎碼（chipping code），它是一串有高有低的訊號，並且各代表原本的位元。接著將碎碼反轉，以代表資料流中相對的位元。如果傳輸同步正確，那麼這種方式可以提供

獨自的錯誤校正功能，並且對干擾的容錯率也比較高。



MAC 層定義的是存取 PHY 層的方法，機動性管理與無線電資源控制等。在資料傳輸上，這和有線乙太網路的定義差不多，不同的地方是在資料碰撞（data collision）的處理方式。在有線網路標準中，資料封包可以被任意的送到網路上，只有在兩個封包於某些情況下互相碰撞（collide）時，才會有其他方式來確保資料封包被正確送到目的地。在 802.11 標準中有定義到避免碰撞（collision avoidance）的動作。在這些標準中，無線網路中的接收端在成功收到資料封包後，會回覆確認（ACK）封包給發送端。如果發送端沒有收到 ACK 封包，那麼它會等待一段時間後，再嘗試重送封包。

但不幸的是，802.11 標準中仍然有一些必須要解決的問題存在。制定標準的目的，無非是要達到標準化（Standardization）以及相容結合性（interoperability）的目標。不過在標準中仍舊有一些與廠商間相容結合性有關的課題。這些包括 AP 點漫遊協定，在標準規格中沒有明確制定出由某個 AP 範圍移動到另外一個 AP 範圍時的處理機制。另外無論設備是否符合標準，到目前為止還沒有一套完整的測試方法來測試無線網路。

網路安全與私密性

無線網路比起有線網路來說，本來就比較不安全。因為無線網路卡使用空氣作為資料傳輸介質，對越權存取和竊聽的行為也比較不容易防備。對一個網路竊聽專家而言，他們在面對有線網路時，通常得要有高度的警覺性與相當程度的知識。不過由於無線網路不需要用到實體連接，要滲透進去其實很容易。他們只需要一片無線網路卡，和一些無線網路的漏洞與弱點知識就夠了。

為了防堵這些自稱駭客的攻擊，標準規格中也制定了稱為有線安全等級協定（wired equivalency protocol，WEP）的事項。理論上，這個構想可以保護網路的私密性，另外 WEP 協定也可以防止未經授權就存取無線網路。不過根據許多研究人員的分析，這項協定實際上還無法達到上述的兩項目標。目前為止已知可行的攻擊手法有下列幾項：

- 根據統計分析結果，對流通的資料展開被動式解碼攻擊
- 根據已知明文內容，可以由未經授權的通訊站發出新資料流以作主動攻擊
- 藉著對 AP 動手腳，可以對流通的資料展開主動式解碼攻擊
- 當每天的資料流動遭到監控與分析時，有可能藉著字典建立式（Dictionary-building）攻擊，對所有流通資料做即時的解碼

WEP 協定使用共享於一個基本服務組合（basic service set，BSS）的祕密鍵值做傳輸。BSS 指的是一個無線 AP 與一組相關節點的組合，這個鍵值用來在資料封包傳輸前作加密的動作，封包也必須經過整合性的檢查，以確保在傳輸中沒有被竄改。而在 802.11 標準中的小漏洞，是裡頭沒有定義共享鍵值要如何建立。在大部分無線網路中，是使用單一鍵值在區域內共享，並且必須要手動設定。

這種加密方法的問題是出在加密的演算法。WEP 使用的是 RC4 演算法，這是一種串流加密器（stream cipher），它將短的鍵值展開成為無限制的虛擬亂數鍵值串。發送者使用這個鍵值串與明文資訊做 XOR 運算處理並產生密文。XOR「exclusive or」（互斥或）邏輯運算指的是是一種二進位系統的邏輯運算子，若兩個運算元不同，則結果為１，當兩個運算元相同時，其結果為０。依照這項原則，接收者則使用鍵值產生適當的鍵值串。並且對密文做 XOR 及鍵值串演運之後，就可以得到原始的明文了。

這種串流加密器也製造了幾種遭攻擊的機會。其中一種攻擊方式，是攻擊者篡改攔截到封包中的位元，這麼一來原本可以解密的封包就解不開了。另外一種攻擊可能導致所有寄送的明文曝光，竊聽者只要攔截到兩組使用同一組鍵值串加密的密文就可以了。用這兩組密文可以算出原本明文的 XOR 表，而這個 XOR 資料可以用展開統計式攻擊以解開所有明文。只要掌握越多同一鍵值串加密的密文，這種攻擊就越有效。一旦其中一道明文被解開，那要解開其他明文自然不是難事。

不過 WEP 對這兩種攻擊倒也不是束手無策。它使用完整性的檢查（Integrity Check，IC）檔來確保傳輸中資料不會被篡改，另外它也使用初始向量（Initialization Vector，IV）來產生共享的鍵值，以防使用相同鍵值串來加密兩份明文。研究則指出這兩項方法運作的都不太正確，導致在安全性上效果不彰。

IC 值採用相當常見的錯誤偵測方式－CRC-32 檢查碼。但這種方法也有問題存在，就是它是線性的值。由於可以根據資料封包的位元差異，來算出兩個 CRC 碼的位元差異，攻擊者也可以在更改實際位元的同時，算出應該要修改 CRC32 碼中的哪一個位

元，好讓封包看起來是正確的。

WEP 演算法的另一項弱點，是它使用 24-bit 的初始向量。這導致 IV 可能組合的範圍很小，也就是說在很短的時間內就可能重複用到同一組鍵值串。在一個資料流量普通的忙碌 AP 上，大約只要 5 小時就可能會出現重複的鍵值串。如果封包大小縮小，那時間還會更短。這讓攻擊者有機會在很短的時間內收集到兩個採相同鍵值串加密的密文，並開始做統計分析以找出明文。更糟的是由於所有節點都用相同的鍵值，IV 重複的可能大大的增加。而且在 802.11 標準中，變動 IV 還不是預設使用的功能。

這時使用更先進的鍵值管理方法，可以用來防止上述的攻擊。這些攻擊並非一般人所想的那麼容易，當然啦，市面上的各種 802.11 規格產品讓許多自稱駭客的人在解碼 2.4GHz 信號時不再那麼困難，不過最大的難點還是在硬體本身。許多 802.11 設備都設計成要是沒有持有相對應的鍵值，那麼就會無視於加密的內容。如果對驅動程式動手腳，並且讓硬體搞混，那麼還是可以把無法辨識的密文給抓回來研究。需要資料傳輸動作的主動式攻擊雖然難得多，不過卻也不是不可能。

目前無線網路科技受到蠻嚴重的挫折，因為無線規格中的加密基礎本身就有誤解與濫用的問題。除非日後又制定了能夠修正 802.11 標準安全性的規格，不然想達到 100%私密與安全的無線網路架構實在是不可能。

網路效能：個案研究 (略)

測試內容 (略)

結論

對 SOHO 族來說，這項產品蠻吸引人的。有了它，您就不必在地毯或牆壁上費心牽線了。SOHO 使用者也不再需要找船塢點（docking station）來接筆記型電腦，或是和一堆雜亂的網路線惡戰苦鬥。無線網路提供了連線能力，卻省了一堆接線和昂貴的船塢點。而且隨著公司的擴展或縮減，您也不需要再牽線給新電腦用。如果公司搬了家，只要電腦搬過去網路也可以照用。對像倉儲業等無法牽線的地方來說，無線網路的確是唯一的替代品，隨著無線網路速度的提升，使用者的日子相信會更好過了。

我們所測得的資料也顯示對需要高頻寬的家庭使用者來說，這其實不算是個實用的產品。那些想要在室內網路放 DVD 電影，或是玩非常吃頻寬的網路遊戲的重度使用者，可能會發現這玩意實在不能滿足他們。

我也要建議那些需要傳送高機密與私人資訊的使用者，最好別用 802.11 的產品。這些安全標準如果用在監理所、有線電視、電信局或是紐約證券交易所上基本上都是不合格的。

這些結論代表什麼？這代表著當無線網路更成熟，安全性與私密性也都經過修正時，它的確有機會一舉搶下有線網路佔領多年的網路市場。隨著掌上型裝置，行動式電腦和其他設備的大量普及，無線網路也漸漸具有實用價值。因為 IEEE 802.11a 的頻寬可以上到 5Ghz 頻段，而且相關的頻道也越來越廣，每秒 54Mb 的速度也不是夢想。如果在市面上普及，對家用及 SOHO 使用者來說是相當具吸引力的產品。

我們會繼續注意無線網路產品，並且將我們測試與研究的範圍更加擴大。就像我們一開始提到的，這並不是完整的一項測試，不過這也算是我們頭一次嘗試，能將這類有用的數據呈現給各位表現應該還不錯吧？相信各位看過本篇評析後，應該可以自己思考無線網路真正的價值了。