第二章　文獻探討

802.11 無線網路適合建構中小型的區域網路，例如家中、辦公室、圖書館等，跟傳統的有線網路比起來節省了佈線的成本，而且能更快速的架構起網路環境，對於使用者而言，方便的是不再需要侷限於網路插座所在的位置，可以隨意將支援無線網路的設備帶到任何可以存取無線網路的位置，就可以使用網路。

第一節　無線網路 802.11

IEEE 802.11 與 IEEE 802.3 所規範的均為區域網路，後者是我們熟悉的有線 Ethernet 網路，前者即為本研究要探討的無線網路。此兩者均規範媒介存取控制子層(medium access control sublayer, MAC Sublayer)及實體層(physical layer)但內容大不相同。

802.11 是以服務群(service set)來描述整個運作的範圍及方式，它制定了兩種服務群，第一種是基本服務群(basic service set, BSS)，所代表的是一群無線客戶端所成的集合，又稱為基礎網路架構(infrastructure network)。如圖 2-1

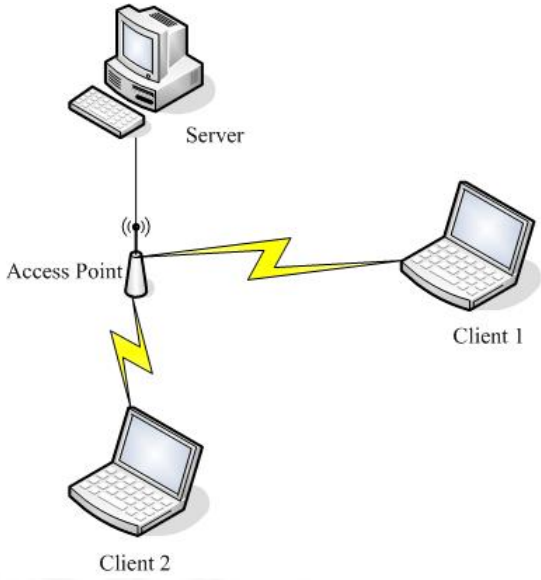

圖 2-1 BSS

Gast (2006)提到，一個 BSS 只能涵蓋一個辦公室或是家庭的範圍，如果想要擴大其服務範圍，我們可以使用 ESS (extended service set)，它是使用數個存取點串連起來，延伸無線網路的範圍，所有存取點都會使用同一個 SSID (service set identifier)，也就是該網路的名稱。如圖 2-2

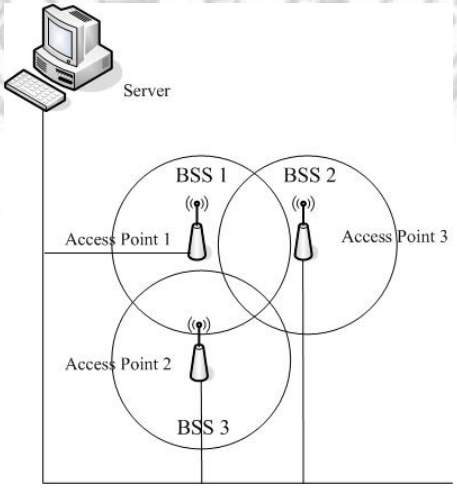

圖 2-2 ESS

第二種是獨立服務群(independent service set)又稱為 Ad-hoc 也是一群無線客戶端的集合，Ad-hoc 是指客戶端彼此能直接通

訊，而兩者間的距離必須在可以直接通訊的範圍內，有點對點(peer-to-peer)的特性，常見於會議中，會議一開始時，參與會議人員就可以彼此傳輸資料，形成一個小型的網路。如圖 2-3 所示。

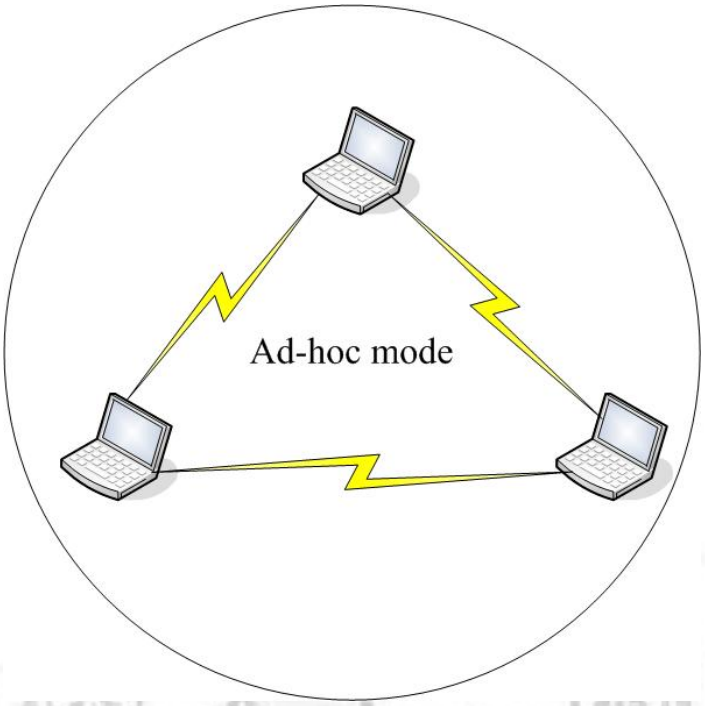

圖 2-3　Ad-hoc

IEEE 802.11 是由 IEEE 的 802 專案中 第 11 個工作小組(IEEE working group)所制定的標準，因此稱做 802.11，而每個工作小組又會分成許多任務小組，如 802.11b，就是任務小組 b 所制定。以下為 802.11 各版本的簡介：

802.11　1997 年首次制定的標準。

802.11a　1999 年制定的標準。其載波的頻率為 5GHz，原始傳送速率為 54Mbps。

802.11b　1999 年制定的標準。其載波的頻率為 2.4GHz，傳送速率為 11Mbps。

802.11g　2003 年所發表。其載波的頻率為 2.4GHz(跟 802.11b 相同)，原始傳送速度為 54Mbps，能與 802.11b 相容。

802.11i 2004 年改善資料鏈結層的安全性。

802.11n 在 2007 年一月推出 Draft 1.1 年，速率最快可到 540Mbps，實際速度為 200Mbps。

第二節 實體層

IEEE 802.11 工作小組重新制定了 OSI 實體層與資料連結層的子層 MAC 層在 802.11 的規範，如下圖 2-4 所示

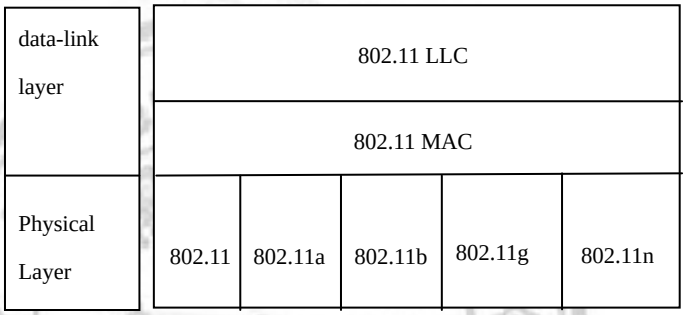

圖 2-4 802.11 之 MAC 與 Physical Layer

資料來源：M. S. Gast (2006)，802.11 無線網路技術通論(黃裕彰譯)，台北：歐萊禮出版。

802.11a 使用 5GHz 的 OFDM (orthogonal frequency division multiplexing)，可提供 八種不同資料傳輸率，其範圍 6Mbps 到 54Mbps，OFDM 裝置會將一個較寬的頻道切割成幾個子頻道，每個子頻道均用來傳輸資料，所有這些較慢的子頻道最後會被多工的方式組合成較快的頻道。

802.11b 使用 2.4GHz 的 DSSS (direct sequence spread spectrum)。在 802.11b 的傳輸模式中，包含了四種資料傳輸率：1Mbps、 2Mbps、 5.5Mbps、 11Mbps。

802.11g 使用 2.4GHz 的 OFDM，且可與 802.11b 相容，包含

了 6Mbps、9Mbps、12Mbps、4Mbps、18Mbps、36Mbps、48Mbps 和 54Mbps 等傳輸速率。

表 2-1　802.11 a/b/g 的比較

	頻段	調變技術	最高傳輸速度 (Mbps)
802.11a	5 GHz	OFDM	54 Mbps
802.11b	2.4 GHz	DSSS	11 Mbps
802.11g	2.4 GHz	OFDM	54 Mbps

資料來源：M. S. Gast (2006)，802.11 無線網路技術通論(黃裕彰譯)，台北：歐萊禮出版。

第三節　MAC 層

802.11 使用了一種基礎的存取模式，DCF (distributed coordination function)，以讓所有設備互相競爭以取得存取權，DCF 在傳送資料前會先檢查無線網路是否為淨空狀態(idle)，以避免遽爾傳送造成碰撞(collision)使得資料損失，詳細步驟請參考圖 2.5，DCF 又稱為 CSMA/CA。此外，DCF 可利用 RTS/CTS 選項，進一步減少碰撞發生的可能性，發送端在送出資料前會先廣播送出 RTS 的控制訊框，接收端收到之後便送出 CTS 控制訊框。當鄰近客戶端聽到這兩種訊框的任何一種，便需再等待一段時間，不得傳送任何資料，如此一來碰撞頂多發生在 RTS/CTS 的控制訊號上，碰撞機率自然降低很多，但相對的可能會使傳送效能降低。

如果需要用到免競爭服務，有另一種存取模式，稱之為 PCF (point coordination function)。PCF 優先權比 DCF 高，能提供免競爭服務，使用 PCF 服務需要有一個特別的工作站擔任網路協調者(point coordinator)，以掌控無線媒介的存取使用權力，通常此

PCF 的功能是由基礎網路架構下的存取點負責，因此 PCF 只能在基礎網路架構下運作。

若與 802.3 使用的 CSMA/CD (carrier sense multiple access/collision detection)相比較，則因 802.3 使用有線網路，故 CSMA/CD 可偵測封包碰撞，802.11 使用的 CSMA/CA (carrier sense multiple access with collision avoidance)，因使用無線的媒介故無法偵測碰撞，如下圖 2-5 所示。

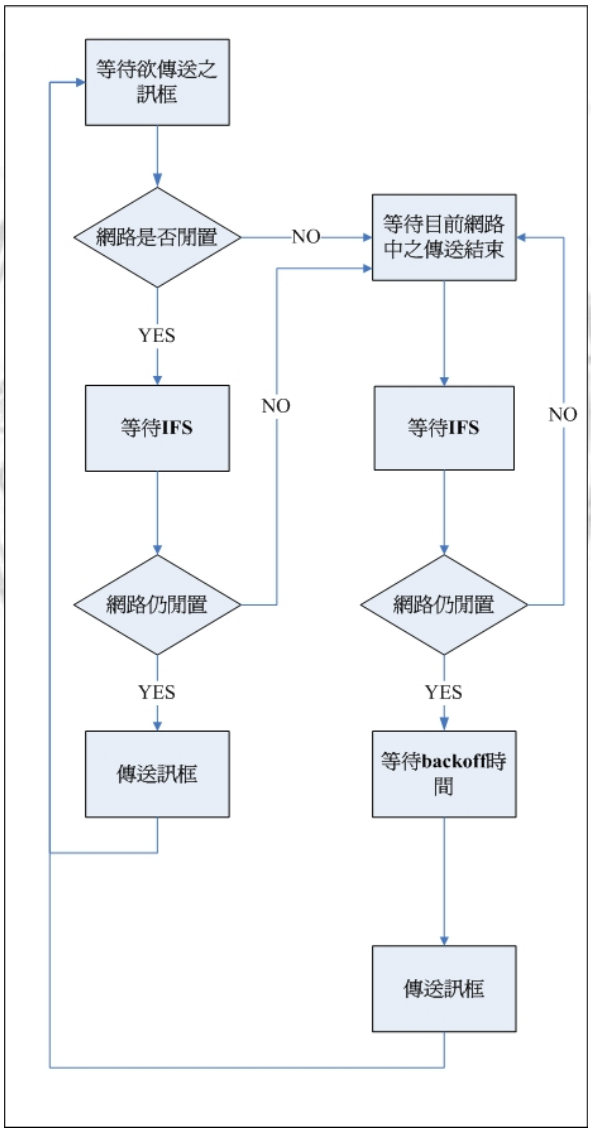

圖 2-5　CSMA/CA 之流程圖

一開始要準備發送訊框時，客戶端會先偵測網路媒介是否為空閒的狀態，而如果有封包在媒介上，便等待一段時間，接著再等待 IFS (interframe spacing，在 CSMA/CA 中為 DIFS)，確認沒有其它人在使用後，便等待一個時間為隨機的 backoff time，避免同時太多競爭者同時發聲要求傳送。

IFS (interframe spacing)在協調存取扮演重要的角色，從上文可知，電腦送資料時為了避免碰撞會等待一段時間，之後會有個 IFS 等待時間，這時優先度高的 IFS 便會勝出。

下圖 2-6 為各種訊框間隔的關係

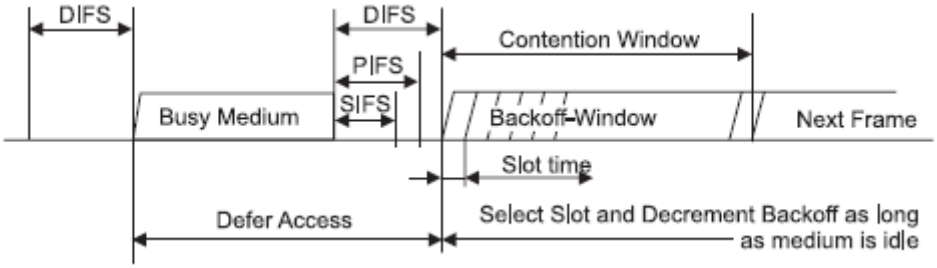

圖 2-6　各 IFS 的關係圖

資料來源：IEEE Computer Society (2003). *LAN MAN Standards Committee of the IEEE Computer Society ,Part11: Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specification*[Online]. Available: http://standards.ieee.org/getieee802/ [2007, June 12].

IFS 有分為四種：

一、SIFS (short interframe space)

SIFS 屬於優先性高也是最短的 IFS，它通常用於 RTS/CTS 或是 ACK 之前。

二、PIFS (point coordination function interframe space)

PIFS 為免競爭的 IFS，有資料待傳的客戶端可以等待 PIFS 期間過後加以傳送，因其長度較 DIFS 短，在與其競爭時，PIFS 絕對會獲得優先權。AP 只有在 PCF 時才會使用 PIFS，且 PCF 是在 DCF 時才能使用，一旦 AP 結束 polling，PCF 便結束，DCF 才能開始運作。

三、DIFS (distributed coordination function interframe space)

DIFS 為 802.11 DCF 模式啟動中 CSMA/CA 所採用的時間間隔，任何客戶端必須等待媒介是處於空閒狀態後，再等待 DIFS 的時間才能開始競爭發言權。

四、EIFS (extended interframe space)

EIFS 沒有固定的時間間隔，只有在訊框發生錯誤時才會用到 EIFS。

其中 slot time 為統一的時間間隔標準，就好比時鐘的秒針一樣，但根據 WLAN 不同的技術，slot time 也會不同，如 FHSS 的 slot time 就比 DSSS 還長。

第四節　802.11 之安全機制

雖然無線網路十分方便，但是架構在 802.11 最早期的安全機制 WEP 卻有嚴重的漏洞存在，因而有心人士能非法存取無線網路，使得在無線網路上傳輸的資料無法受到保障，更甚者有心人士也可能使用無線網路來進行一些攻擊行為。

802.11b 制定的標準要求無線網路提供三種網路安全機制：

一、使用者認證(authentication)

認證的主要目的在於確認對方身份的合法性，如同查看

身份證一樣，無線網路是利用廣播的方式來傳送，因此只需要一張網路卡就可能與這些 AP 連線，在這樣的形態下，認證機制就當然非常重要，802.11b 無線網路驗查身份的方法有三種：

(一)開放系統認證(open system authentication)

用 SSID 來判定，任何人都能與存取點連線，存取點並不會認證使用者的身份，可以說完全沒有任何保護。

(二)封閉系統認證(close system authentication)

用 SSID 來判定但對 NULL SSID 不回應，使用者必須輸入正確的 SSID 才能與存取點連線，就像輸入密碼一般，比開放系統認證提高了一點安全性。但由於無線網路的特性，是以廣播方式傳送資料，因此只要以擷取封包的方法，取得 SSID，便得以進入網路。

(三)分享密鑰認證(shared-key authentication)

這也叫作「挑戰與回應」(challenge/response)。當使用者對 AP 發出一個認證的請求，AP 會隨機產生一個 128 位元長度的挑戰字串給使用者，使用者將這字串使用密鑰進行 RC4 的加密演算並傳回給 AP，AP 使用 WEP 及 RC4 演算法進行解密，將其與原傳送明文進行比對，然後對使用者發出確認身份成功的封包。如圖 2-7：

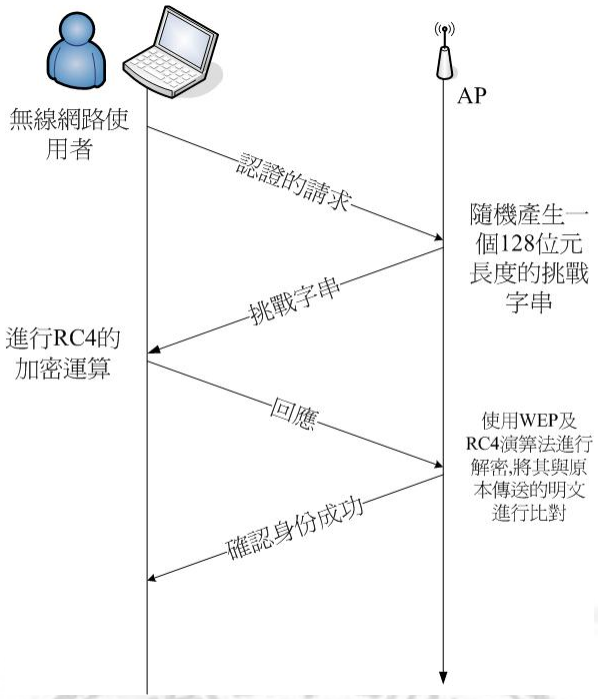

圖 2-7　Challenge-Response 使用者認證模式

二、加密(encryption)

WEP 是屬於對稱式加解密系統，原始密鑰長度是 40 位元及 104 位元。透過 WEP 加密後，整個封包只有 MAC Address 與 IV (initial vector)欄位是明碼，其餘的部分會經過 RC4 編碼，而 RC4 為串流加密(stream cipher)，WEP 利用有限長度的 KEY 再加上 PRNG (pseudorandom number generator)產生不限長度的虛擬隨機數位串流，KEY 與 PRNG 產生的串流作 RC4 運算後型成密鑰，再與整個明文作 XOR 運算得到密文。因為 WEP 是用對稱式加密，所以兩端必須要有相同的密鑰，但是根據 802.11b 的標準，這個密鑰的長度必須是 40 位元或是 104 位元。為避免靜態密鑰被破解，因此在密鑰產生時，加入一個長度 24 位元的初始向量 IV (initial vector)；利用動態的 IV 再加上靜態密鑰的方式，藉此打亂整個密鑰的組合。

三、資料完整性(integrity)

Peikari (2003)提到 IEEE 802 系列的網路通訊協定,絕大部份都採用 CRC (cyclic redundancy check)的方法,來做為資料完整性的檢查及確認的動作;這種方法能夠有效的檢查資料在傳輸的過程中，因電氣因素或外來不明因素的干擾(像天候或線材・・・等)產生的錯誤。此法是透過單向雜湊函數 (one-way hash function)來進行完整性的確認。接收的一方可以將收到的資料,經過同樣雜湊函數來進行運算,將得到的數值和封包內存放的 CRC 的值來進行比對。如果值相同則表示資料是完整,如果不相同則是封包在傳輸的過程發生錯誤。

在 802.11 的加密選項中，WEP 是最容易見到的，也提供了一定程度的保護，而 WEP 的資料格式由三個部份構成：

一、初始向量(iv)

由 24 個位元的初始向量與 8 個位元鑰匙選擇位元組合而成。

二、訊息

長度在 1 到 2312 Bytes 之間。

三、檢查碼(icv)

32 個位元組合而成的。

初始向量的產生方式由設計者自行定義，依標準 WEP Key 最多可定義四組，因此在傳送時，可藉由鑰匙選擇位元，來指定使用第幾組 key，負責加密或解密的工作。WEP 是採 Share-key 的方式，所有的端點都採用同一組 key 來完成加解密；而如前面提到的，key 的長度分別是 40 位元與 104 位元這兩種，因此，WEP 40 位元的格式中共享鑰匙的長度是 40 位元加上 IV 的 24

位元，這樣就變成了有一個總長度為 64 位元的 key。

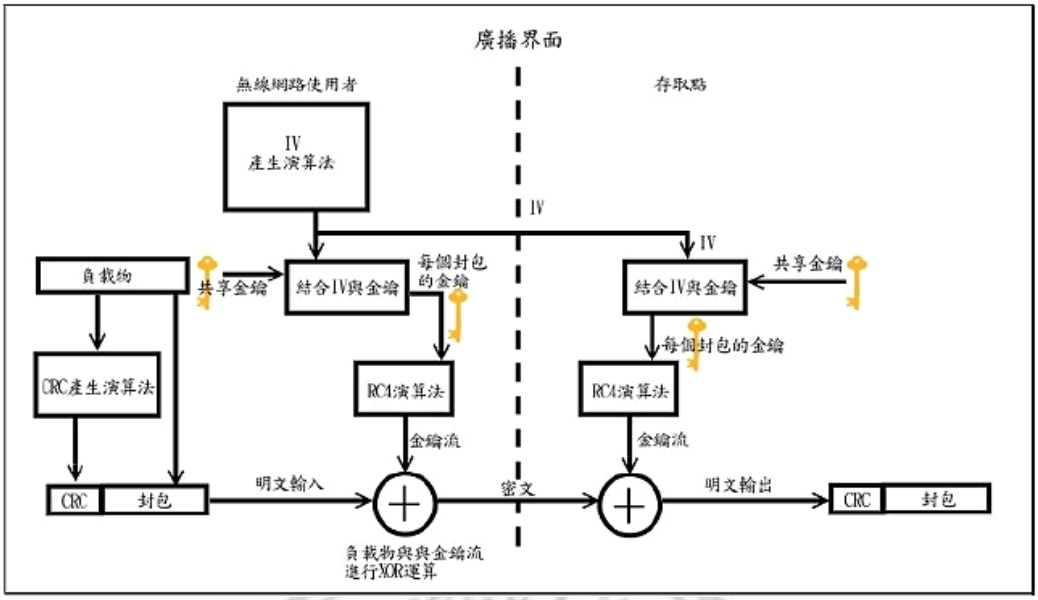

圖 2-8　WEP 運作流程圖

資料來源：台灣電腦網路危機處理暨協調中心(2003)，802.11無線網路安全白皮書[線上資料]，來源：http ://www.cert.org.tw/document/docfile/Wireless_Security.pdf [2007, June 5]。

而 WEP 的加密的過程一開始

(一)發送端會將封包中的內容進行 CRC 運算，然後利用這個值產生一個完整性檢查碼，並將此檢查碼附在封包中。

(二)接下來，由發送端利用產生 IV 值的演算法來產生一個 IV，再將 IV 及共享鑰匙進行 RC4 PRNG 函數運算，來獲得一個加密金鑰。最後再利用這個加密金鑰，將原先的明文封包進行 XOR 運算來加密，如此密文資料就產生了。

(三)最後再將 24 位元的 IV 附在密文封包中傳送。

當接收端收到封包後，便開始整個解密的過程，首先將附在封包的 IV 取下，接著將取得的 IV 再和密鑰進行 RC4 PRNG 的運算，這樣便得知該封包的加密金鑰；再利用這個加密金鑰對密文進行 XOR 運算還原密文，然後再進行 CRC 完整性確認。如圖 2-8。

Gast (2006)提到 WEP 有以下弱點：

(一)IV 重複率過高，在 WEP 的設計中避免密碼被猜出，因此加入了 24 位元的 IV，但經過 2^24 的封包傳送後，這組動態 IV 可能再度重複，這樣的方式可能在數天後就可以收集到同樣的 IV 資料進而破解 WEP 的密鑰。

(二)利用 CRC 是線性演算法的缺點把原文篡改卻不知道。

(三)單向認證的缺失，由於 WEP 的認證方式是採用單向認證，因此很難避免連線截取及假冒撷取點等像 Man-In-The-Middle 方式的攻擊行為，雙向認證方式可互相確認使用者以及無線區網的身分。

(四)密鑰產生的問題，WEP 密鑰的組成是動態 IV+40 位元的分享密鑰組成，而通常管理者會將分享密鑰設成易記的密碼，因此可用字典攻擊法猜測密鑰。

第五節 802.11 安全機制的問題及解決方案

一、802.11 安全的問題大致可分為三大類：

(一)無線通訊的特性

由於無線網路設計是以無線技術為基礎，使得攻擊得以無線電波涵蓋的範圍內進行通訊內容的監聽。如果用者未將傳送的資訊適當的進行加密，則入侵者很容易

的可以竊取所有的通訊內容。另外由於無線通訊只要電波收訊範圍內即可使用，也造成了管控上的大麻煩， 管理者無法完全的進行存取控制。

(二)WEP 設計的不當

在 802.11 的標準中訂定 WEP 的標準，希望透過這種加密技術能讓使用獲得更好的資料安全性，但是由於某些設計及實作上的不當使得 WEP 所獲得的效果無法百分之百保證資料內容的機密性。此外由於設計協定時沒有考慮金鑰管理的問題， 因此如果你有一個很大的無線區域網路的話，金鑰的修改及配送會是一個很大的管理問題。

(三)設備安全管理措施不當

所有的網路設備出廠時都有一些預設的設定值， 許多的管理者與使用者將網路設備當成家電般的隨插即用(plug and play)，沒有更改系統內定的相關管理資訊；這些缺失可能造成攻擊者反客為主，獲得設備的管理權限，「幫助」管理者進行網路的管理。

二、解決方案

(一) 802.1X Port-Based Network Access Control

IEEE 802.1X 於 2001 年七月由 IEEE 核可，是個認證的技術能將無法通過認證的使用者隔絕於網路之外，使 其無法利用任何網路資源。802.1X 是用連結埠控制連線的安全架構， 在 802.1X 架構下有幾個主要的角色：

1. Authenticator：要求並且接受未受信任端網路節點的認證請求的實體，通常是 Access Point。

2. Supplicant：請求網路存取權，並且需接受

Authenticator 的認證稽核，通常是客戶端。

3. Authentication Server：對 Authenticator 提供身分認證服務的實體，可能與 Authenticator 存在同一主機內，但大多數的狀況下是一台獨立的伺服器。如圖 2-9

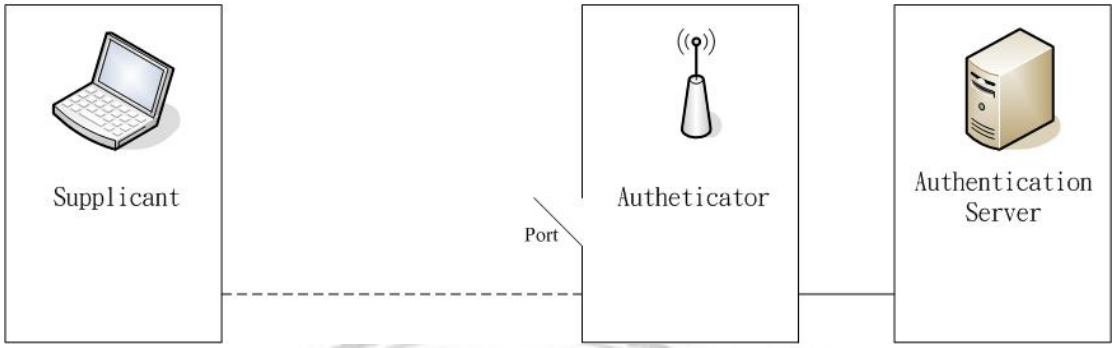

圖 2-9　802.1x 架構

Authenticator 跟 Radius server (authentication server) 會做協議，假如 Authenticator 收到來自 Authentication Server 的 Access-Reject 訊息，代表使用者認證遭 Radius Server 否決，不能連線；反之收到 Access-Accept 時，便獲准進入網域。

802.1X 也提供動態 WEP 加密的服務，每過一段時間認證伺服器會產生一組新的 session key，這樣可以增加有心者想搜集一定封包並加以破解的難度。

(二)WPA (Wi-Fi protected access)

由於 WEP 在加密和資料整合上的缺點，在 2003 年時誕生了 WPA，它包含了新的驗證、加密、完整性確認的加強內容。

1. 驗證：在 WPA 未出現前的安全機制中，802.1X 驗證屬於選項設定，但是 WPA 機制中，802.1X 是強制的，WPA 驗證是 open system 與 802.1X 驗證的結合，第一

階段使用 open system 驗證，以告知無線用戶可以傳送訊框到無線 AP，第二階段使用 802.1X 執行使用者層級的驗證。

2. 加密： Davies (2004)提到 TKIP (temporal key integrity protocol)用來變更每一個訊框的單一播送(unicast)加密鑰匙，每次的改變都是在無線用戶和無線 AP 同步進行。在 802.1X 的運作裡，更新單一播送加密鑰匙是選擇性的，同時，802.11 和 802.1X 沒有提供機制來更新 global 加密鑰匙(作為多重播送和廣播播送傳輸用)，透過 WPA 來運作，更新單一播送和 global 加密鑰匙是必要的。對 802.11 而言，WEP 屬於選項設定，但對 WPA 而言，TKIP 是必須的，TKIP 以新的加密演算方法取代 WEP，不過也可以使用無線硬體提供的演算方法來執行。

3. 完整性確認：802.11 WEP 的資料完整性是由 32 位元 ICV (integrity check vector)提供，以確保訊框在傳送過程中不會被竄改，ICV 是在加密之前，透過 CRC 計算而產生。32-位元 ICV 附加在 802.11 payload 和 IV 之後，雖然 ICV 有加密，但駭客可透過密碼破解方法，來變更其加密承載的位元。

在 WPA 中，為增加完整性，使用 Michael 演算法，它是以目前無線硬體現有的計算工具，來計算 8 位元訊息整合程式碼(MIC)，MIC 放置在 802.11 訊框的資料部分和 4 位元的 ICV 之間。MIC 區域和訊框資料及 ICV 一起加密。如圖 2-10 所示

WPA 的加密及完整性確認過程如下面敘述：

(1)IV、DA (destination address)、資料加密金鑰三者會混合，並計算出每個封包的加密金鑰。

(2)DA、SA (source address)、優先等級、資料與資料加密金鑰會以 Michael 演算法運算出 MIC。

(3)IV 及每個封包的的加密金鑰會使用 PRNG 產生與[資料+MIC+ICV]一樣大小的金鑰資料流，並與它做 XOR 運算，產生 802.11 的加密部分。

(4)把 IV 加到 802.11 裝載框架中的 IV 及延伸的 IV 欄位，加入標頭與結尾進行封裝。

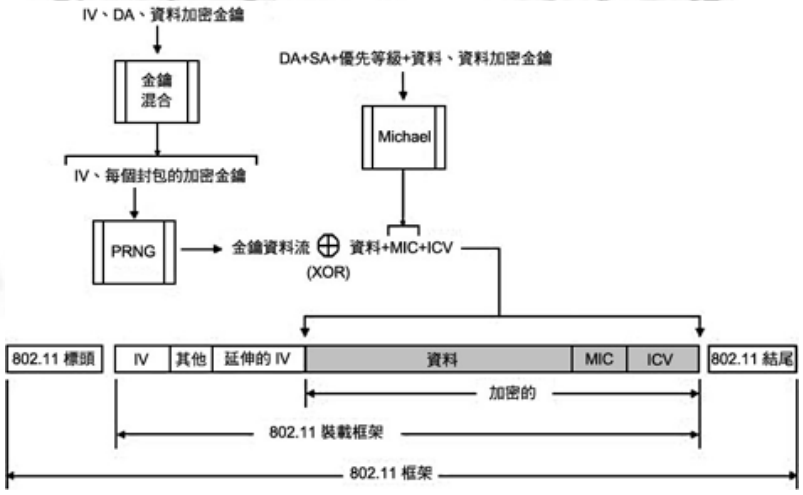

圖 2-10　WPA 加密程序

資料來源：Microsoft (2004). *Wi-Fi Protected Access Data Encryption and Integrity*[Online]. Available: http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx [2007, July 13].

解密的過程為下圖

(1)IV 值由 802.11 裝載框架中的 IV 和延伸的 IV 欄位抽出，並與 DA 和資料加密金鑰輸入到金鑰混合函式，進而產生每個封包的加密金鑰。

(2)IV 和每個封包的加密金鑰都輸入到 RC4 PRNG 函式以產生和加密資料、MIC 及 ICV 大小相同的金鑰資料流。

(3)金鑰資料流透過和加密資料、MIC 及 ICV 的 XOR 運算，產生出未加密的資料、MIC 及 ICV。

(4)由計算獲得 ICV，並與未加密的 ICV 值比較。如果 ICV 值不符合，就會將資料捨棄。

(5)DA、SA、資料及資料完整性金鑰都會輸入到 Michael 完整性演算法以產生 MIC。

(6)MIC 的計算值會與未加密 MIC 的值做比較。如果 MIC 值不符合，就會將資料捨棄。如果 MIC 值符合，資料就會傳遞到較高網路層級以進行處理。如圖 2-11

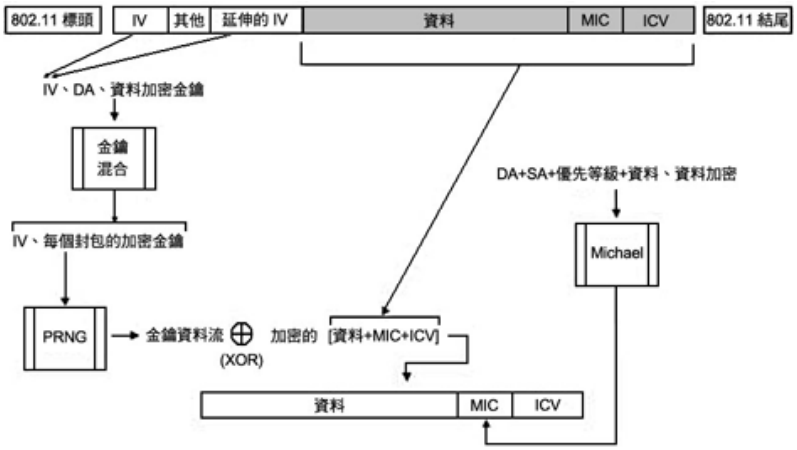

圖 2-11 WPA 解密程序

資料來源：Microsoft (2004). *Wi-Fi Protected Access Data Encryption and Integrit*[Online]. Available http://www.microsoft.com/technet/community/columns/cableguy/cg1104.mspx [2007, July 13].

(三)EAP-TLS

EAP (extension authentication protocol)是 802.1X 的驗證方法，它提供了許多不同的方案(如 EAP-MD5、EAP-TLS、EAP-LEAP 等)，因為相對於其它 EAP 方法，EAP-TLS 提供了強效的驗證方法，所以本實驗中使用的是 EAP-TLS。EAP-TLS 是一個使用憑證的安全架構，可以使用 smart card 或是使用認證伺服器所發佈的安全憑證，使用者才能進去網域內。圖 2-12 是 EAP-TLS 與 Radius server 及使用者的認證過程。

(1)客戶端對存取點發出 EAPOL start 的訊框，接著存取點對客戶端發出請求 id 的訊框。

(2)客戶端對存取點發出回應並附上使用者名稱的訊框，存取點接著將訊框以 RADIUS Access-Request 的格式

傳送到認證伺服器。

(3) 認證伺服器對存取點發出一個格式為 RADIUS Access-Challenge(含有一個 EAP TYPE 為 TLS 的訊息)EAP-TLS start 的訊框,存取點接著將訊框傳送到認證伺服器。

(4)客戶端發出回應一個格式 EAP TYPE 為 TLS 及一個 TLS 客戶端為"hello"的訊框，存取點將訊框以 RADIUS Access-Request 的格式傳送至認證伺服器。

(5) 認證伺服器對客戶端發出一個格式為 RADIUS Access-Challenge 訊框並附上認證伺服器憑證的訊框。

(6)客戶端回應訊框並附上客戶端憑證，存取點將訊框以 RADIUS Access-Request 的格式傳送至認證伺服器。

(7) 認證伺服器對客戶端發出一個格式為 RADIUS Access-Challenge 訊框，並附上密碼組和 TLS 驗證交換已完成的資料。

(8)客戶端發出一個 EAP-RESPONSE，EAP TYPE 為 TLS 的訊息，存取點傳送一個 RADIUS Access-Request 的格式傳送至認證伺服器。

(9)認證伺服器傳給存取點 EAP-TLS success 的訊框,並附上 TLS session key 。

(10)存取點傳送 EAP-TLS success 的訊框給客戶端。

(11)存取點開始產生動態 WEP key。

(12)存取點將 Multicast/global KEY(用每個用戶獨有 session key 加密)給客戶端。

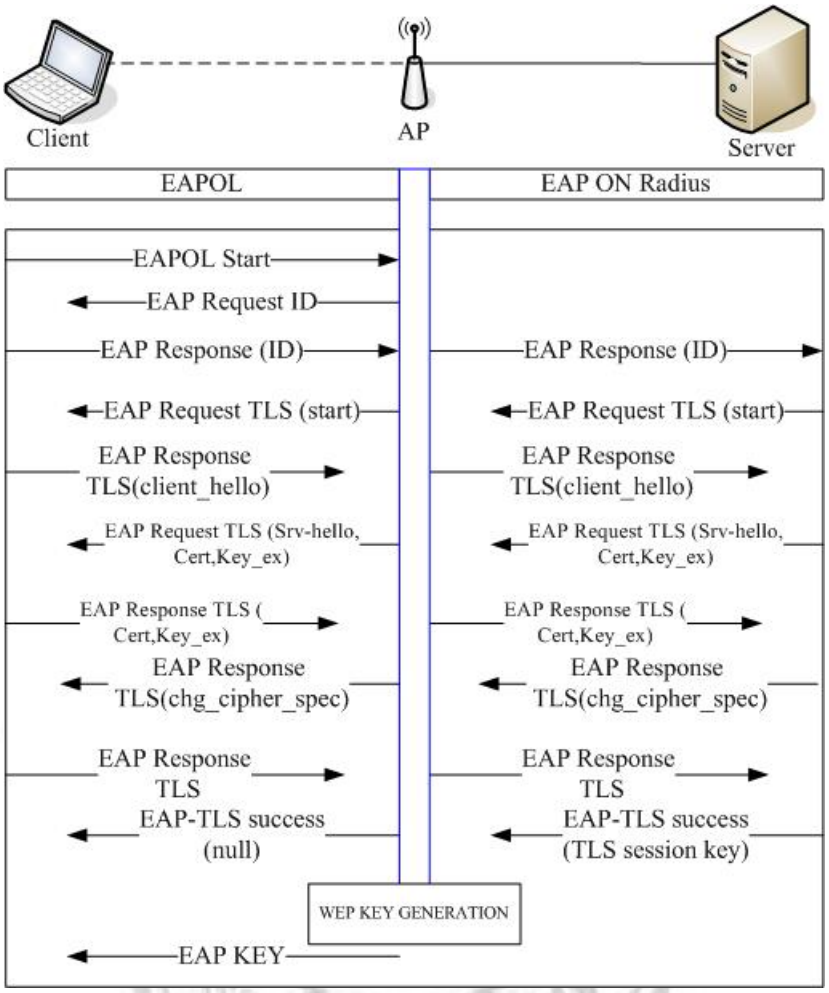

圖 2-12 EAP-TLS 流程

資料來源：張得榮(2004)，Windows Server 2003 伺服器安全解決方案，台北：博碩文化出版。