國立交通大學

電機資訊學院 資訊學程

碩士論文

無線網路安全之研究

A Study on Wireless LAN Security

研 究 生：阮俊霖

指導教授：蔡文能 教授

中華民國九十三年七月

無線網路安全之研究
A Study on Wireless LAN Security

研 究 生：阮俊霖　　Student：Chun-Lin Juan
指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國 立 交 通 大 學
電機資訊學院 資訊學程
碩 士 論 文

A Thesis
Submitted to Degree Program of Electrical Engineering Computer Science
College of Electrical Engineering and Computer Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science
in
Computer Science
July 2004
Hsinchu, Taiwan, Republic of China

中華民國九十三年七月

授權書

(博碩士論文)

本授權書所授權之論文為本人在_____大學(學院)_____系所

_____組_____學年度第_____學期取得_____士學位之論文。

論文名稱：_____

1.□同意　　□不同意

本人具有著作財產權之論文全文資料，授予行政院國家科學委員會科學技術資料中心、國家圖書館及本人畢業學校圖書館，得不限地域、時間與次數以微縮、光碟或數位化等各種方式重製後散布發行或上載網路。

本論文為本人向經濟部智慧財產局申請專利的附件之一，請將全文資料延後兩年後再公開。(請註明文號:　　)

2.□同意　　□不同意

本人具有著作財產權之論文全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限地域與時間，惟每人以一份為限。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

指導教授姓名：

研究生簽名：　　學號：

（親筆正楷）　　（務必填寫）

日期：民國　　年　　月　　日

1. 本授權書請以黑筆撰寫並影印裝訂於書名頁之次頁。
2. 授權第一項者，所繳的論文本將由註冊組彙總寄交國科會科學技術資料中心。
3. 本授權書已於民國 85 年 4 月 10 日送請內政部著作權委員會（現為經濟部智慧財產局）修正定稿。
4. 本案依據教育部國家圖書館 85.4.19 台(85)圖編字第 712 號函辦理。

國 立 交 通 大 學

論 文 口 試 委 員 會 審 定 書

本校　電機資訊學院專班＿＿＿＿＿＿＿＿　組＿＿＿＿＿＿　君

所提論文

(中文)＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

(英文)＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

合於碩士資格水準、業經本委員會評審認可。

口試委員：＿＿＿＿＿＿＿＿＿＿　＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿　＿＿＿＿＿＿＿＿＿＿

指導教授：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

班主任：　＿＿＿＿＿＿＿＿＿＿＿＿＿＿

中 華 民 國　　年　　月　　日

無線網路安全之研究

學生：阮俊霖　　指導教授：蔡文能教授

國立交通大學電機資訊學院 資訊學程（研究所）碩士班

中文摘要

IEEE 組織在 1997 年公佈了 802.11 系列標準後，無線網路已經變成愈來愈流行。之後不少的學術或是商業研究指出，無線網路的安全性有許多漏洞陸陸續續被發掘出來。因此部分的無線網路廠商也都推出自己的標準冀能補強原本的安全問題。另外除了 IEEE 之外，非營利單位的 Wi-Fi 組織也積極地公佈其他標準，以加強無線網路安全性，成為新一代的無線網路安全標準。

本篇論文將針對目前所有的無線網路安全標準以及各家廠商的獨家規格做一綜合性的深入研究，並比較其優缺點，另外也針對目前現有的各種攻擊及防禦的方法做一個探討。另外本篇論文也提出了一個 Simple Proposal for Intrusion Defense in Enterprise wiReless LAN (SPIDER LAN) 方案，可以有效的防止非法 AP 及管理無線客戶端設備。冀本篇論文能對無線網路相關研究以及企業內部的無線網路建置提供貢獻。

關鍵字：無線網路，安全性。

A Study on Wireless LAN Security

Student：Chun-Lin Juan Advisor：Prof. Wen-Nung Tsai

Degree Program of Electrical Engineering Computer Science
National Chiao Tung University

英文摘要

WLAN is more and more popular since IEEE adopted 802.11 standards in 1997. More and More academic and commercial researches unveil the potential vulnerabilities of Wireless LAN. Therefore many vendors of wireless devices improved the wireless security by their proprietary solutions. Besides IEEE, non-commercial Wi-Fi organization also developd other standards to enhance the wireless security.

In this thesis, we will investigate all of the wireless security standards and many proprietary solutions. We will compare the advantages and disadvantages of each solution. We will also explore the mechanism of attack and defense in wireless network. This thesis also propose a Simple Proposal for Intrusion Defense in Enterprise wiReless LAN (SPIDER LAN). This proposal can prevent rogue AP and manage wireless users and devices in wireless network efficiently. We hope the thesis can provide some contributions in academic research, as well as in WLAN deployment for enterprise.

Keywords: Wireless，WLAN，Security。

誌謝

經過了在職班三年的努力，克服了種種困難，終於完成了我的碩士論文。這篇論文之所以能順利的完成，首先要感謝我的指導教授 — 蔡文能教授。由於他不辭辛勞地在我論文寫作及口試期間，給予給知識上的啟發以及學業上的指導，我才能夠順利的拿到碩士學位。還有學長、同學們熱心的討論與幫忙，這篇論文才能順利的完成。

目錄

表目錄

圖目錄

第一章　緒論(Introduction)

近幾年來，隨著電腦網路與無線區域網路的結合，帶給我們生活上許多便利與好處，人們可隨時隨地利用電腦上網、進行電子交易、下載電子地圖、電子信件、視訊會議、網路教學甚至進行線上遊戲等等。無線網路最大的好處即是帶給使用者機動性與便利性。目前所廣泛使用的無線網路技術幾乎都是遵循 IEEE 組織於 1999 年所定義的 802.11b 標準[1]，IEEE 802.11b 是運作於不需使用執照的 2.4GHz 頻率上，傳輸速率可達 11Mbps，距離大約可達 100 公尺遠。它只定義了 OSI 參考模型中的最底下兩層，即實體層及資料鏈結層，使用直接序列展頻(DSSS)的調變解調技術。同一時間，IEEE 也公佈了另一個運用於 5GHz 頻率上的 802.11a 標準[2]，以 54Mbps 速率來傳輸。最近 IEEE 甚至通過了 802.11g 標準，和 802.11b 一樣運用於 2.4GHz 的頻率上，但傳輸速率也可達 54Mbps。

由於無線上網時會有大量而重要的訊息在無線通道中傳遞，並且最近不論在學術領域或是商業研究上有許多的報告指出[3][4][5]，無線區域網路通信協定 IEEE 802.11 在身份認證與加密演算法全上有相當多的缺點存在，因此可能造成部分有心人士對這些資料進行擷取或偽造的動作，所以我們必須考量到重要訊息在無線通道中傳輸的安全問題。

對於任何網路通訊系統包括無線網路，為了保護無線網路的安全性就會提到下列幾個特性，包含「加密性」、「完整性」以及「存取控制」。加密性可以防止不法人士在網路上竊聽，並且確保只有接收端可以看得見傳輸內容。完整性可以防止攻擊者竄改資料內容，並且確保資料的確是由發送端所送出。存取控制分為兩個部分，一是認證

一是授權，認證可以防止非法使用者進入系統，授權可以確保只有合法使用者可以進入系統。為了達到上述這些目的，無線網路的安全機制使用了 SSID、對稱式加密演算法以及 checksum 等方法以確保其安全性[6]。

由於各種無線網路的問題不斷地被揭發出來，Wi-FI 組織在 2002 年 10 月時公佈了 WPA 安全機制[7]，冀能在不用汰換硬體的條件下，提升安全等級。各家廠商也積極的推出獨家解決方案來解決安全上的問題。目前 IEEE 正著手進行新一代 802.11i 安全標準的制訂，不過目前為止(93 年 7 月)還沒有正式通過，待通過後也必須等待各家產品上市後，才有辦法解決目前所面臨的大部分安全問題。

本篇論文將目前現有的安全標準、各家廠商的安全機制以及工具軟體做一綜合性分析比較，最後並提出一個 Simple Proposal for Intrusion Defense in Enterprise wiReless LAN (SPIDER LAN)解決方案，可以有效的防止非法企業內部私接非法 AP，並管理無線網路客戶端設備。

1.1. 802.3 V.S. 802.11

IEEE 802.3 最早於 1983 年正式通過，目前已經成為有線網路標準的最大宗。透過雙絞線或光纖線路可以構接 100 公尺甚至幾公里遠範圍內的電腦網路或其他設備。該標準定義了 OSI 模式中的最底下兩層，即實體層及資料鏈結層，底層使用曼徹斯特(Manchester)編碼及解碼方式，在資料鏈結層部分使用 48-bit 的 MAC 位址以區別不同的實體設備，並透過碰撞偵測的方式以達多重存取(CSMA/CD)[8]。

802.11 在制訂之初，考量與 802.3 的互通性，也使用 48-bit 的 MAC 位址。使得 802.11 設備可以直接與 802.3 設備溝通，才造就了

目前無線網路市場的蓬勃發展。表格 1 中列出了 802.3 與 802.11 的主要規格比較：

表格 1 802.3 V.S 802.11

	802.3	802.11
Media	Wired	Wireless
Transfer Rate	10/100/100 Mbps	1/2/5.5/11/54 Mbps
Security	None	WEP/WPA/802.11i
Adopted	Early in 1983	Early in 1997

1.2. 無線網路相關組織(WLAN Organizations)

對於任何的新興科技而言，我們有其必要了解目前在市場上、業界或學界的任何相關組織。因為這些組織可以推動技術的創新、加速商業的應用以及主導市場的走向。以下列出目前與無線網路相關的幾個組織。

1.2.1. 電子電機工程師協會 (IEEE)

IEEE 是大家耳熟能詳的組織，它成立於 1963 年，成立之初只有一個常設性的歷史委員會，負責於一些技術和專業活動的歷史資料推廣、撰寫或收集，這些資料不但包含 IEEE 所涉及的技術和專業的活動，同時也包含 IEEE 和它的前身的歷史資料。1980 年，IEEE 於紐約成立了一個電子工程師歷史中心，這個中心一開始只有主管、檔案管理員及一個兼職的研究員。不過他們卻為整個電子工程的歷史記錄奠定了一個良好的基礎。1990 年，整個中心搬到新澤西洲的 Rutgers 大學，由於有學校的贊助，中心才得以擴充至三個博士歷史研究員，四個 Rutgers 大學畢業的兼職研究員，以繼續他們的歷史資料收集與研究。

逐漸地 IEEE 已嚴然成為電子電機相關技術的重要推手，其中的 IEEE Standards Association(IEEE-SA)更是工業標準的領先發展者，包含的領域有電力與能源、生物與健康、資訊科技、電信工業、運輸工業、奈米科技、資訊保證等等議題。IEEE-SA 為這些標準建立了一個公平、公正、公開的發展程序。除了發展 802 相關的區域/都會型的有線/無線網路標準之外，IEEE-SA 也發展了下列相關標準：

- **智慧型高速公路系統及汽車科技**
- **分散式產生可更新能源**
- **投票設備電子數據交換**
- **個人電腦充電電池**
- **摩托車事件資料記錄器**
- **公開金鑰基礎建設憑證發送與管理元件**
- **加密分享媒體架構**

IEEE 區分成幾個不同的工作群組(Working Group)，分別針對不同的主題做研究，其中跟無線網路相關的是 802.11 這個工作群組。所有的工作群組都是透過投票的方式進行標準的訂定。[9]

1.2.2. Wi-Fi 聯盟

目前市場最活躍也是最熱門的無線網路組織即是Wi-Fi Alliance 組織[10]。它的前身是 Wireless Ethernet Compatibility Alliance(WECA)組織，成立於 1999 年，由 Intersil、Cisco、Agere Systems、3Com、Nokia 和 Symbol Technologies 幾家無線網路的領導廠商所共同組成。隨著 802.11b 的普及化，Wi-Fi 組織也愈來愈成功，從 1999 年至今，目前它已經有超過 200 個成員，並且測試超過 1000 項產品。因為每一家廠商都希望可以得到通過這項驗證以提供擁有互通性的無線網路設備給他們的客戶。眾所周知的微軟與 Intel 公司也分別於 2001

年七月及九月加入組織成員。

由於 802.11 系列標準在採用之初有許多的彈性，這樣的彈性造成各家設備會有不互通的情況發生，為了解決這個問題， Wi-Fi 組織成立的目的是希望透過驗證無線網路設備的互通性來推廣 802.11b 標準。

為了達成這個目的，Wi-Fi 組織於 2001 年四月開始驗證各家產品的互通性，只要是通過認證的產品即可獲得一個 Wi-Fi 的標誌。Wi-Fi 的全名是 Wireless Fidelity。這個 Wi-Fi 標誌代表著不同廠牌的 AP、無線網卡及其他的 802.11b 設備可以一起運作。在 2001 年 11 月，Wi-Fi 組織也開始驗證 802.11a 的產品，通過驗證的產品也可以得到 Wi-Fi5 的標誌。

這項測試的服務及驗證的程序是由 Agilent Technology 公司的互通認證實驗室(AICL)來操刀。AICL 成立於 1998 年，當時它叫做 Silicon Valley Network Lab(SVNL)。它最主要是提供各項的通訊產品的測試服務，包含乙太網路交換器、路由器、數位用戶迴路及 802.11b 等設備。Agilent Technology 公司於 1999 年時將這個實驗室買下，然後繼續提供 Wi-Fi 的測試程序。

1.2.3. 英國新漢普郡大學互通實驗室 (IOL)

另一個加入 802.11 互通性測試的組織是英國新漢普郡大學(New Hampshire University)的互通實驗室(InterOperability Lab，簡稱 IOL)。這個實驗室是由數個聯盟所組成，IOL 為了這個互通性的測試，發展了一套測試程序並且為這些測試提供一個論壇。這些聯盟是由各家通訊廠商所組成，其中當然也包含了 802.11 的廠商。這些廠商包括 Agere、Anixter、Atmel、Cisco、Conexant、Enterasys、InterMec、Intersil、Mobilan、netIQ、Network Associates、Sharewave、Wireless Solutions 以及 Zoom 等等。所有的成員都必須繳交年費並且提供設備

給實驗室做測試，如此一來就可以得知自己與其他廠牌設備的測試結果並且為自家產品增加了在學術研究上的曝光機會。

跟 ACIL 不一樣的是，IOL 並不是在認證設備，它只是在廠商的早期研發階段提供一個與他牌設備的測試環境[11]。

1.2.4. Wireless LAN Association (WLANA)

Wireless LAN Association 是歷史最悠久的 802.11 業界團體。它成立於 1996 年，由 IBM、Cisco、Agere System、3Com、Advanced Micro Devices、Compaq、Intersil、Intermec、Proxim、Symbol Technology、Raytheon Electronics 以及 Windata 等公司所共同組成。這十二家公司希望可以成立一個非營利性的教育團體來推廣 802.11 標準，並且透過它來交換一些無線網路標準的應用、問題、技術及趨勢等等議題，至今該組織已經擁有超過 30 個成員。WLANA 的前身稱為 Wireless LAN Alliance，它是在 2000 年五月更名為 Wireless LAN Association[12]。

1.2.5. OFDM 論壇

OFDM 論壇成立於 1999 年 12 月，至今已經擁有超過 50 個成員。論壇成立的目的即是在推廣 OFDM 技術應用於各種無線通訊系統之上。這個論壇的工作目前被區分為三大領域：WLAN、固定式無線網路(MMDS、LMDS、802.16 等等)以及機動寬頻(3G/4G)。OFDM 是在 802.11a 及 802.11g 標準中被定義於實體層中的一種傳輸機制，它也是 802.16 都會型網路中的主要技術[13]。

第二章　背景知識(Background)

自 1999 年 IEEE 組織通過了 802.11a/b 無線網路標準後，其中採行的是 WEP 的加密及認證方式，由於安全上的瑕疵，Wi-Fi 組織便推行 WPA 的安全機制，此一安全機制可以透過軟體或韌體的方式即可使用，而不用全面的更新舊有設備。目前，IEEE 組織更積極地在制訂新的 802.11i 標準，冀能全面改善舊有的無線網路安全問題。

2.1. WEP (Wired Equivalent Privacy)

在無線網路的傳輸過程中，存在一個非常明顯的問題就是竊聽者可以很容易地透過無線電波偷聽到傳輸的內容。無線網路的設計者知道這個問題，希望透過某一種安全標準可以解決這個問題，IEEE 802.11 無線網路中使用的安全標準就是 WEP (Wired Equivalent Privacy)。望文生義，WEP 的目的就是期望可以達到與有線網路相等的安全等級。它是 MAC 層的加密協定，使用 RC4 的加密演算法，其中所使用的秘密金鑰是由 AP 以及客戶端所共享。WEP 提供了資料的加密性、完整性以及使用者認證性等等功能[14] 。

WEP 標準同時包含資料加密性、完整性與認證性。目前 WEP 使用 2 種金鑰長度，分別是 64 與 128 位元，其中包含了 24 位元的初始向量(IV，Initialization Vector)與實際的秘密金鑰值(40 與 104 位元)。大家耳熟能詳的 40 位元編碼模式，其實相當於 64 位元編碼。該標準並沒有考慮到金鑰的管理問題，所有的設備必須以手動的方式管理金鑰；唯一的要求是，無線網卡與基地台必須使用同樣的加解密演算法。無線網路的每一個使用者會擁有同樣的加密金鑰，但是會使用不同的 IV，以避免封包總是使用同一把金鑰，而隨機產生的 RC4 亂數值。

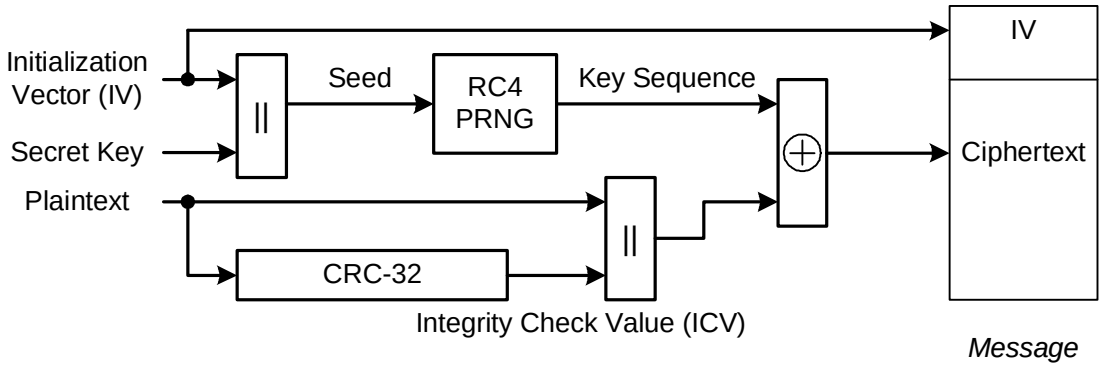


圖 1 WEP 加密流程

整個 WEP 的加密過程會把資料訊框透過 CRC-32 演算法產生一組 32-bit 的完整性檢查數值(Integrity Check Value，簡稱 ICV)，此 ICV 會串連在資料訊框的尾端，最後再使用 RC4 演算法所產生的亂數值與上述的資料訊框與 ICV 做 XOR 運算產生密文，請參考下圖 1。RC4 演算法則是透過發送端的 IV 值與金鑰做運算而產生一組亂算值。這個數值也會被 AP 端用來解密客戶端傳送過來的密文，因為 IV 是以明文的方式包含在密文前傳送過來的，所以接收端在收到 IV 之後再與自己的金鑰透過 RC4 演算法產生出同一組亂數值，再與密文做 XOR 的運算，可得原始的資料訊框與 ICV，接收端再將資料訊框做一次 CRC-32 的運算，與 ICV 比較後假使相同，即可確定該資料訊框是正確的，並沒有遭到竄改，請參考下圖 2。資料內容最後就可以交由上層的通訊協定處理。

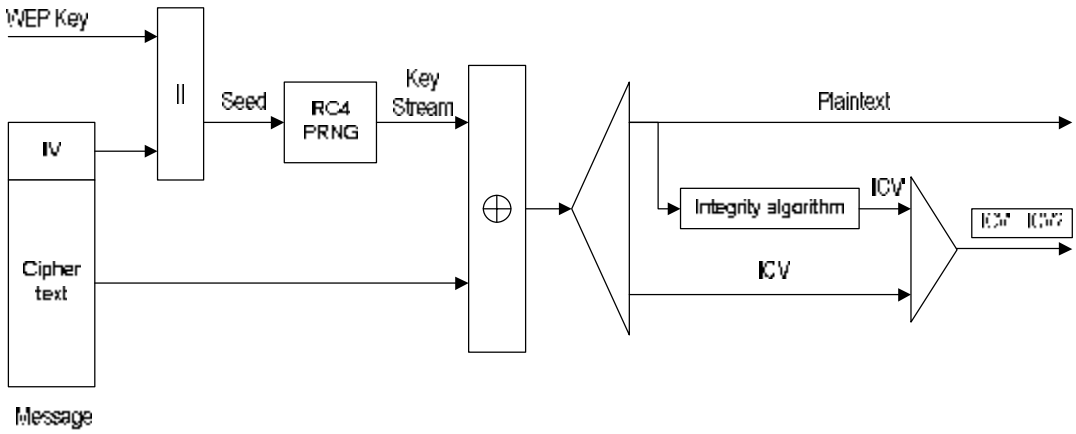


圖 2 WEP 解密流程

在認證性的部分，802.11 定義了兩種存取控制的認證模式：公開系統認證 (Open System Authentication) 以及分享金鑰認證 (Shared-key Authentication)兩種模式。公開系統認證模式是一個簡單的雙向式流程，使用者只需要提出正確的 SSID 值(SSID 是同一個無線網路區段中，使用者及 AP 所使用的網路識別名稱)，無需使用 WEP 的加密方式，待 AP 回應成功訊息後即可進入網路；另外客戶端設備可以使用「ANY」這個 SSID，無論這個 AP 原本使用的 SSID 為何，就可以連上任何 AP。在分享金鑰認證模式下，是由 AP 先傳送一個 challenge 給客戶端，客戶端再使用自己的金鑰將 challenge 加密傳回 AP，AP 再使用自己的金鑰將 challenge 加密與客戶端傳回的密文做比較。如果兩者相同，表示客戶端的確知道真正的金鑰為何，AP 則授權該客戶端連上網路。大部分的無線網路設備都是使用公開認證的模式。

公開系統認證模式

如圖 3，在公開系統認證模式中無線設備認證的流程如下：

1. 客戶端發送一個認證要求給 AP。
2. AP 將認證客戶端為成功或失敗。

3. 若認證成功，客戶端則能無線上網。

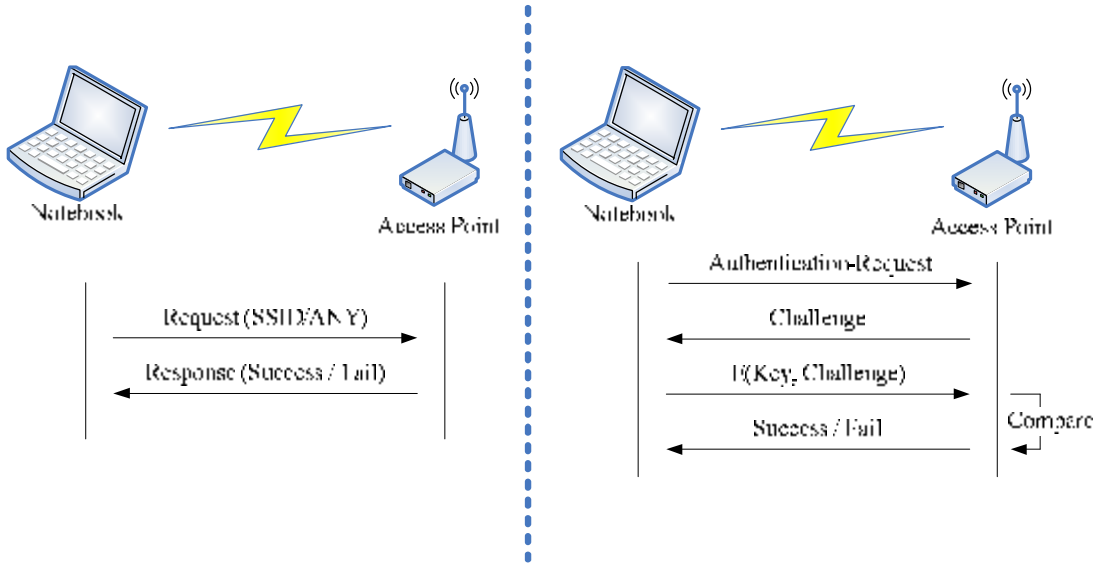


圖 3 公開認證 VS 分享金鑰認證

分享金鑰認證模式

分享金鑰認證模式的流程如下，如圖 3：

1. 客戶端發送一個認證要求給 AP。
2. AP 傳回一個挑戰訊息給客戶端。
3. 客戶端使用 64 或是 128-bit 的預設金鑰將挑戰訊息加密後，回傳至 AP 端。
4. AP 使用所設定的 WEP 金鑰對加密訊息解密。解密後與原本的挑戰訊息比較，如果相同表示 AP 與客戶端均擁有相同的加密金鑰，客戶端則認證成功。

如果解密後的訊息與原本的挑戰訊息不相同，表示 AP 與客戶端的加密金鑰不相同。AP 則會拒絕客戶端的認證，客戶端便無法連上無線網路。

2.1.1. WEP 的弱點

Borisov、Goldberg 以及 Wagner 的報告指出[15]，WEP 編碼的

弱點在於 IV 實作的基礎過於薄弱。例如說，如果駭客將兩個使用同樣 IV 的封包記錄起來，再施以互斥運算，就可以猜出訊息的明文。請參考下列公式。換句話說，也就是將兩個加密密文做互斥或的運算後，加密金鑰值就被消掉了，結果就和兩個明文做互斥或的運算相同。

If $C_1 = P_1 \oplus RC4(v,k)$

And $C_2 = P_2 \oplus RC4(v,k)$

Then $C_1 \oplus C_2 = (P_1 \oplus RC4(v,k)) \oplus (P_2 \oplus RC4(v,k))$
$= P_1 \oplus P_2$

如果我們使用的初始向量為 24 位元，那我們就可以在繁忙的網路點上（例如以 11Mbps 的頻寬，不斷傳送 1500 位元組的封包），以不到 5 小時的光景算出結果，請參考下列計算公式。以這樣的例子來說，總資料量為 24GB。因此，要在幾小時的時間內，記錄所有傳輸的封包，並以筆記型電腦算出其結果，是絕對可行的事情。

$$\frac{1500Bytes \times 2^{24}}{11Mbps} = \frac{1500 \times 8 \times 2^{24}}{11 \times 10^6} \approx 18302(\text{sec}) \approx 5.084(hr)$$

由於這標準並沒有規定 IV 所產生的相關事宜，所以並不是每家廠商都用到 IV 的 24 個位元，並在短時間內就重複用到相同的 IV，好讓整個程序快一點。所以駭客所要記錄的封包就更少了。以 Lucent（朗訊）的無線網卡來說，每次啟動時它就會將 IV 的初始值設為 0，然後再往上遞增。駭客只要記錄無線網路上幾個使用者的資料內容，馬上就可以找到使用同樣 IV 的封包。

Fluhrer、Martin 及 Shamir[16]三人也發現，設計不良的 IV 有可能會洩漏鍵值的內容（信心水準為 5%），所以說只要記錄 400～600 萬個封包（頂多 8.5 GB 的資料量），就有可能以 IV 來算出所有的 WEP 鍵值。更進一步探討，如果 WEP 鍵值的組合不是從 16 進位表，而是從 ASCII 表而來，那麼因為可用的字元數變少，組合也會變少。那麼

駭客猜中的機率就會大增，只要一兩百萬個封包，就可以決定 WEP 的值。

Arbaugh、Shankar 以及 Wan 的報告中也提到[17]，在分享金鑰模式認證模式下，由於挑戰訊息的明文與密文都是以未經加密的方式在空氣中傳輸，攻擊者可以用竊聽的方式取得明文、密文及 IV 值，所以攻擊者可以在不知道金鑰的狀況下，將明文與密文做互斥或的運算即可得到加密用的亂數值。接著自己要求一個分享金鑰認證的方式，從 AP 端得到另一組明文，再以剛剛計算出的亂數值計算，即可得到正確的挑戰訊息密文。

2.2. WPA (Wi-Fi Protected Access™)

WPA 的出現是為了加強 IEEE 在 1997 年所通過的 WEP 加密標準。在 2001 後 WEP 的加密弱點已經是眾所皆知，有一系列的學術研究或是商業組織指出，不法人士只要具備適當的工具及中等的技術能力即可輕易地進入 WEP 的網路中。

僅管 WEP 有其缺點所在，它確實提供了某種程度上的安全保護，至少比一點安全性都沒有來得好。在網路封包數量較少的家庭或是 SOHO 使用者而言，WEP 可能還有一點點用處。但是在大型企業而言，就必須透過其他的第三方的安全標準，諸如 VPN、802.1x 或是其他廠商自訂的協定，來加強原有的 WEP 加密方式。

Wi-Fi 聯盟與 IEEE 組織為了補足現有市場上無線網路產品安全性上的不足，合作訂定了 WPA 的安全標準，並於 2002 年 10 月 31 日公佈。它是為了可以立即取代現有市面上 802.11 標準中的 WEP 加密方式，直接透過軟體或韌體昇級即可達到較高的安全等級。使用者或企業主不需要全面更新所有的硬體設備，並且可運用於不同廠牌的無線

網路設備中。它不但提供了較為強化的資料加密功能，也新增了原本在 WEP 中沒有的使用者認證功能。WPA 的設計是為了加強所有 802.11 系列的產品，包括 802.11a/802.11b/802.11g 等。它不但可以向前和向後相容既有及未來的安全標準。

簡單地說，WPA 是 802.11i 的簡易版本，它包含了 TKIP (Temporal Key Integrity Protocol)和 802.1x 兩個機制。WPA 使用了一個加強型的加密機制，Temporal Key Integrity Protocol，TKIP 一樣也使用 RSA Security 公司的 RC4 串流加密演算法來加密每個傳輸的封包，並且在傳輸前加上了 CRC 檢查。結合 802.1x 與 EAP 的認證機制及訊息完整性檢查碼(Message Integrity Check，MIC)以防止封包被偽造。

另外，WPA 還有一個很大的好處，就是在設計之初考量到現有的無線網路設備的限制，因此一樣使用 RC4 的加密演算法，使得現有的設備只要透過軟體及韌體昇級的方式即可使用新的加密標準，而不用淘汰現有的無線網路設備。因此，如果您的設備不支援 WPA 功能的話，請至原廠網站查詢有無最新的韌體更新。如果您是最近才要購置無線網路設備，請記得認明有無圖 4 的標記。

圖 4 WPA 認證的標記

WPA 基本上仍然以 RADIUS(Remote Authentication Dial-In User Service)為基礎，透過 EAP(Extended Authentication Protocol)來進行使用者的驗證，主要包含了下列機制：

TKIP(Temporal Key Integrity Protocol)：定義了加密金鑰的交換方式，並利用雜湊函數(Hashing)以擾亂金鑰的組成，提供 Per-packet Keying。

Pre-shared Key：在沒有 RADIUS 的情況下，使用者與 AP 間可透過一組預先指定的金鑰先行溝通驗證，並在之後以這組主要金鑰再行產生各使用者自己的加密金鑰，並利用 TKIP 進行更換。

Re-keying：AP 會透過公告(Advertise)的方式將 Global Key 通知使用者，利用 TKIP 來交換唯一的金鑰(Unicast Key)。

Message Integration Check：對於資料完整性的檢查，除了原本 WEP 所使用的 CRC-32 演算法，另外利用 Michael 演算法產生 8bytes 的 MIC(Message Integrity Code)，以進行更周延的檢查，一方面避免無線傳輸過程中所產生的封包錯誤，另一方面也藉此避免有心人士透過竊取他人封包以 replay 的方式入侵。

同時支援 WPA 及 WEP 的使用者：WPA 的 AP 藉由固定 Global Key 的方式，達成與現有僅支援 WEP 的使用者相容，但也因此減低了 WPA 使用者一部分的安全性。

2.2.1. WPA 的特性

由於 WPA 應用了許多新的標準與協定，達到以下幾個特點：

加密性

TKIP 將金鑰長度由 40-bit 增加至 128-bit，以取代原本 WEP 的單

一固定金鑰機制，另外 TKIP 的金鑰也會自動地動態產生並且發佈至客戶端。另外 WPA 也結合了 802.1x 與 EAP 協定，透過認證伺服器針對每一個使用者的工作階段產生一個主鑰，認證伺服器之後會驗證使用者所提出的證明。

TKIP 會發佈這個主金鑰給 AP 及客戶端，並且建立一組金鑰階層管理系統，透過這個主鑰為每個使用者的工作階段動態地產生階段金鑰，來加密無線網路中傳輸的封包。

完整性

資料完整性的功能即是透過 TKIP 的訊息完整性檢查碼功能來達到。MIC 是設計用來防範攻擊者在收集封包後，而後偽造封包最後再重新發送出去。它提供了一個加強的機制可以讓接收端在收到封包後比較 MIC 值。如果數值不相符，就表示封包內容遭到竄收，這個封包就會被丟棄。

認證性

原本的 WEP 只使用了簡單的使用者認證功能。為了加強認證性的功能，WPA 結合了 802.1x 及支援多重的 EAP 協定來達到認證性的功能。多重的 EAP 協定可以處理使用者所提出的證明，包含單一的使用者名稱/密碼、智慧卡或是企業內已經配置的各種數位認證。它可彈性的應用任何一種 EAP 型態，包含 EAP-TLS、EAP-TTLS 及 PEAP 等等。

透過 EAP，802.1x 也可以達到使用者與認證伺服器間的雙向認證功能，這樣可以防止使用者被任何一台的非法或非授權的認證伺服器綁架，也確保只有合法的使用者才能連上網路。

2.2.2. WPA 的應用

WPA 提供以下兩種模式，企業模式(Enterprise Mode)及分享金鑰模式(Pre-shared Key Mode，簡稱 PSK 模式)，可以針對不同的無線網路環境調整不同的模式應用之：

企業模式

在企業模式中，需要存在一台集中式認證伺服器(例如 RADIUS 認證伺服器)，在客戶端上網後會與 AP 建立關聯，AP 會禁止這些人往外進行連線，除非這些客戶端已經通過認證。客戶端會出示自己的證明給認證伺服器，如果沒有通過認證客戶端的連線就會被擋下來，如果通過認證才會繼續進行下一步。接著認證伺服器會自動地將加密金鑰傳送到 AP 及客戶端，如此一來客戶端則可順利加入這個網路，所傳送的資料便會使用剛剛得到的加密金鑰來加密資料以確保資料安全。企業模式的流程與示意圖請參考下圖 5。

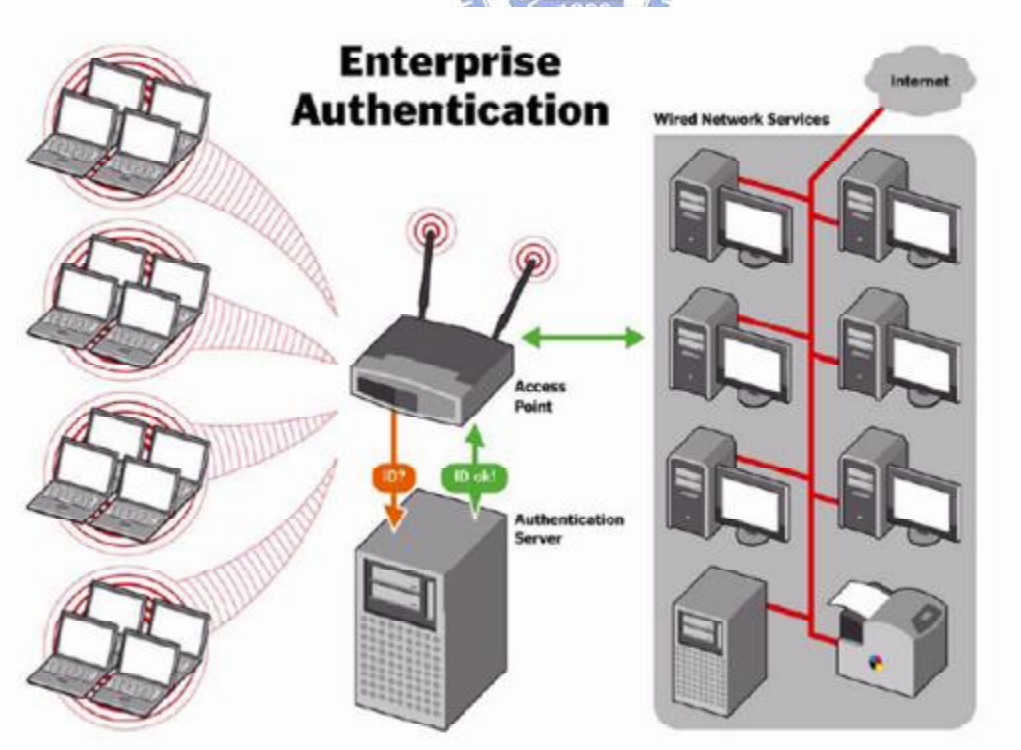


圖 5 WPA 企業模式示意圖

分享金鑰模式

由於一般的小型或是家庭辦公室(Small Office/Home Office，又稱為 SOHO)中，考量時間與人力成本的因素，不會建置認證伺服器。在 PSK 模式中，

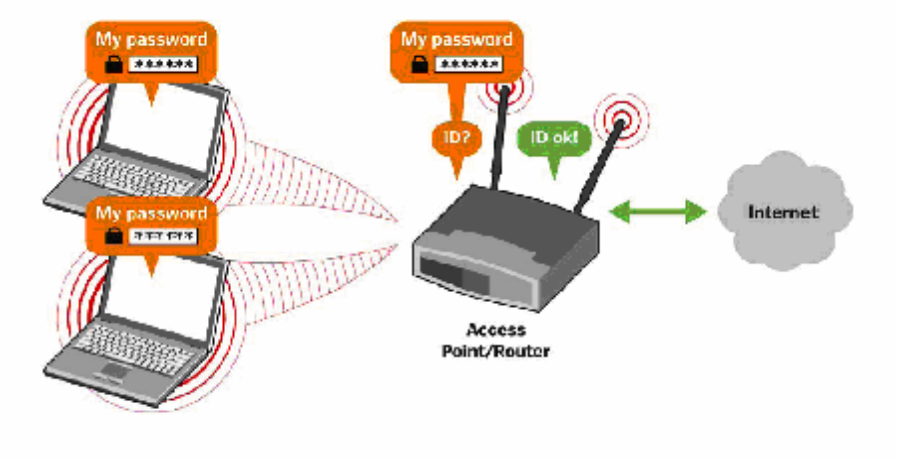


圖 6 WPA 的 PSK 模式示意圖

TKIP 提供下列幾項做法，以補 WEP 之不足：

- **48-bit 的初始向量值(IV)**

48-bit 的初始向量值相較於之前的 24-bit 值，可以提供多達 2^{24} 的數值，可以提供更多的變化以防止攻擊者計算出金鑰。

- **每一封包(Per-packet)均有不同加密金鑰**

TKIP 會對每個傳送的封包產生不同的加密金鑰，以確保封包在傳輸過程中不會被攻擊者所偷聽。

- **訊息完整性檢查碼(Message integrity code)**

TKIP 會為每個傳送的封包產生一組訊息完整性檢查碼，以確保封的完整性，不會被攻擊者所偽造。

2.3. 802.11i

IEEE 802.11i 是安全加密標準，不同於之前通過的 802.11a/b/g 屬於傳輸速度的標準，因此 802.11i 能與 802.11a/b/g 並存。802.11

工作群組最新 2004 年七月份的報告指出 802.11i 標準已經被 IEEE 標準委員會所認可，但尚未公佈。

IEEE 802.11i 定義兩種等級的安全性演算法：Robust Security Network Association(簡稱 RSNA 演算法)以及 pre-RSNA 兩種[18]。文件中並沒有禁止客戶同時使用這兩種演算法，但是也沒有定義如何同時使用。

RSNA 透過 TKIP 或是 CCMP 來提供資料的加密性，其中 CCMP 是必須的，而 TKIP 協定則是選擇性的。綜整如下，RSNA 是由下列元件所組成：

- **TKIP**
- **CCMP**
- **RSNA 建立及終止程序，包含 IEEE 802.1x 認證方式。**
- **金鑰管理程序**

而為提供舊有設備相容性，Pre-RSNA 是由下列元件所組成：

- **WEP**
- **IEEE 802.11 使用者認證**

2.4. 標準比較

下表為上述各種標準的比較表：

表格 2 WEP、WPA 及 802.11i 比較表

	WEP	WPA	802.11i
Cipher	RC4	RC4	AES
Key size	40-bit	128-bit encryption 64-bit authentication	128-bit
Key life	24-bit IV	48-bit IV	48-bit IV
Packet key	Concatenated	Mixing function	Not Needed
Data Integrity	CRC-32	MIC	CCM

Header Integrity	None	MIC	CCM
Key Management	None	EAP-based	EAP-based

第三章　相關技術(Related Technology)

3.1. XOR

XOR 又稱為 Exclusive OR，是一種非常簡易的對稱式加密法，運用於每一位元的數學運算。兩個位元交互運算後，只有一個「1」值時則得到「1」，兩個位元皆為「1」或皆為「0」時則得到「0」。運算表請參考表格 3。

表格 3 XOR 運算表

第一個位元	第二個位元	結果
0	0	0
0	1	1
1	0	1
1	1	0

XOR 運算非常適合用於將明碼的每一位元運算後成為密文。如果我們欲將「ABC」這組明文加密，預設一個金鍵值為「K」，所以每個英文字母都必須跟 K 做 XOR 運算。以 A 為例，A 的二進位表示法為「0110 0101」，K 的二進位表示法為「0110 1111」，兩者運算後即得密文「0000 1010」如下表。以此類推 B 的密文即為「0000 1001」，C 的密文即為「0000 1000」。

表格 4 明文 A 的加密結果

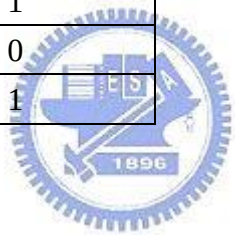
明文 A	金鑰 K	運算式	密文
0	0	0 xor 0	0
1	1	1 xor 1	0
1	1	1 xor 1	0
0	0	0 xor 0	0
0	1	0 xor 1	1
1	1	1 xor 1	0

0	1	0 xor 1	1
1	1	1 xor 1	0

相對的，接受端在收到密文後，以同樣的金鑰「K」分別對密文的每一個位元組解密，以 A 的密文為例可由下表得到明文 A 為「0110 0101」。

表格 5 明文 A 的解密結果

密文	金鑰 K	運算式	明文 A
0	0	0 xor 0	0
0	1	0 xor 1	1
0	1	0 xor 1	1
0	0	0 xor 0	0
1	1	1 xor 1	0
0	1	0 xor 1	1
1	1	1 xor 1	0
0	1	0 xor 1	1



3.2. RC4

RC4 全名是 Ron's Code #4，是由 RSA Security 公司的 Ron Rivest 在 1987 年所發明。Ron Rivest 同時也是 RSA 演算法的發明人之一。RC4 是一種對稱式的串流密碼(Stream Cipher)演算法，目前被廣泛應用於各式應用程式中，諸如 Microsoft Windows、Oracle SQL、Lotus Notes 以及 SSL[19]等等。

RC4 使用了從 1 到 256 Bytes 的可變動長度金鑰。由於美國出口限制的關係，RC4 通常使用 40-bit 當做金鑰長度，但是有時候也會使用 128-bit 長度當做金鑰。

RC4 演算法分為兩個階段，包含金鑰建立及加密兩個階段。金鑰建立是一個步驟也是最複雜的步驟，在建立一個 N 位元組的金鑰的過

程中，會經由 state array 及 key array 透過 N 次的交換、餘數及其他公式的運算產生一個加密變數。

當加密變數產生之後，緊接著就進入第二階段的加密運算。加密運算是透過與明文做 XOR 之後即產生密文。當接收端收到密文之後，再用加密變數與密文做 XOR 運算，即可得到原始的明文。

以下我們使用一個簡單地 4-byte 金鑰長度來示範 RC4 的演算法：

首先我們先建立一個 4-byte 的 state array 叫做 Si，包含由 0 到 3 的四個數字。

Si	=	0	1	2	3
		S0	S1	S2	S3

接著我們再建立一個 4-byte 的 key array 叫做 Ki，然後把我們所選擇的金鑰依序填滿整個 key array，假設我們選擇 17 當做金鑰。

Ki	=	1	7	1	7
		K0	K1	K2	K3

在運算的過程中，我們使用了 i 和 f 變數來控制 Si 及 Ki。開始時，i 和 f 變數皆為 0。這個運算的過程即是重複(f + Si + Ki)除以 4 的餘數，再交換 Si 及 Sf 的值，每次運算過後 i 值則累加 1。

第一次：

For i = 0, f = (0 + 0 + 1) mod 4 = 1

f S0 K0

於是交換 S0 與 S1

Si	=	1	0	2	3
		S0	S1	S2	S3

第二次：

For i = 1, f = (1 + 0 + 7) mod 4 = 0

f S1 K1

於是交換 S1 與 S0

Si	=	0	1	2	3
		S0	S1	S2	S3

第三次：

For i = 2, f = (0 + 2 + 1) mod 4 = 3

f S2 K2

於是交換 S2 與 S3

Si	=	0	1	3	2
		S0	S1	S2	S3

第四次：

For i = 3, f = (3 + 2 + 7) mod 4 = 0

f S3 K3

於是交換 S3 與 S0，最後得到

Si	=	2	1	3	0
		S0	S1	S2	S3

最後還必須產生一個 random byte 來做加密運算。再把 i 以及 f 重設為 0，設 i = (i + 1) mod 4，f = (f + Si) mod 4，交換 Si 與 Sf。再設一個 t 變數，使得 t = (Si + Sf) mod 4，即得 St 為 random byte。

i = (0 + 1) mod 4 = 1

f = (0 + S1) mod 4 = 1

交換 S1 與 S1，即代表 S1 數值不變

Si	=	0	1	2	3
		S0	S1	S2	S3

t = (1 + 1) mod 4 = 2

即得 random byte 為 S2 = 2

2 的二進位表示法為「0000 0010」假設我們有一組明文為「ABC」，每一個 byte 皆與上述 random byte 做 XOR 運算，可得

	A	B	C
	0110 0101	0110 0110	0110 0111
XOR	0000 0010	0000 0010	0000 0010
	0110 0111	0110 0100	0110 0101 **à** 密文

接收端在得到密文後，可再與 random byte 做一次 XOR 運算，即可得知明文為「ABC」。

3.3. EAP

EAP 的全名是 PPP Extensible Authentication Protocol，它提供了多種的認證型態以達認證的功能[20]。在 PPP 的協定之中，定義了如何透過兩個點對點之間的連線來傳輸資料，其中也包含了認證的功能。由於原本 PPP 協定中的認證只支援了簡單的認證功能[21]。而 EAP 便是針對 PPP 的認證功能所做的延伸，它可以支援多種認證方式。EAP 並不在 PPP 的 Link Control Phase 中指明使用何種認證方式，而是把認證的過程延後，如此一來可以於後端新增一個認證伺服器來支援多重認證方式的使用。於是 IETF 便公佈這個延伸的協定，透過了新增 PPP 協定中的 Authentication-Protocol 值為 C227，則表示可使用 EAP 用來認證。

整個 EAP 的過程是由認證者(Authenticator，通常指 AP 或後端伺服器)，對客戶端提出認證的請求，這個請求之中的一個欄位會包含所用的 EAP 型態，諸如 MD5、One-Time Password、Token Card 等等，之後客戶端送出回應給認證者，回應的封包會有兩種情形，第一種是回應封包中包含了認證者所提供的 EAP 型態及認證資訊，則認證者可以驗證資料正確與否；第二種情形是客戶端不支援認證者所要求的認

證型態，則客戶端回應封包中的 EAP 型態欄位中則會填入「NaK」，認證者收到 NaK 的封包後則會再次發起另一個 EAP 型態的要求封包，客戶端則再次回應另一個回應封包。最後認證者則回應成功或失敗的訊息給客戶端，而結束整個認證的過程。

整個 EAP 認證流程請參考下圖 7。

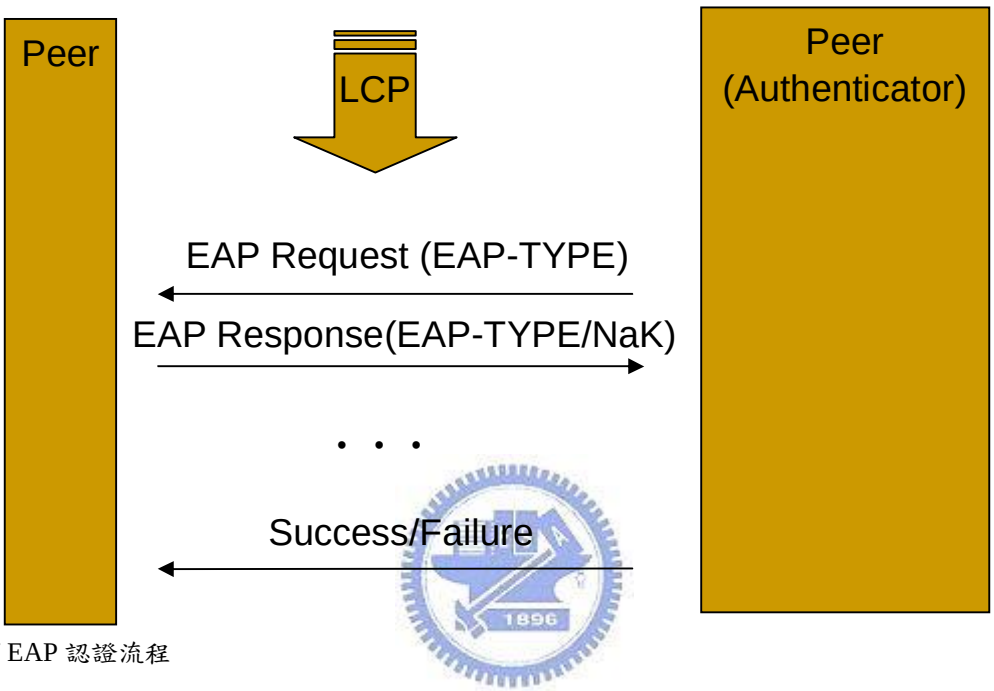


圖 7 EAP 認證流程

EAP 的優點

EAP 的好處在於可以支援多種 EAP 型態的認證，另外證明者也無需瞭解各種 EAP 型態如何認證，它可以當做一個代理者的角色把各種 EAP 型態的封包往後端的認證伺服器傳送。最後只要認得認證伺服器傳回的成功或失敗封包即可。

EAP 的缺點

現有的 PPP 協定必須修正為支援 EAP 功能。表示舊有的 PPP 設備必須透過昇級才能使用 EAP 認證。

3.4. 802.1x

802.1x 是由 IEEE 組織在 2001 年八月時所公佈[22]。目前許多新的無線網路設備加入了 802.1x 的標準以加強無線網路的安全性。儘管如此，如果可以適當的使用 802.1x 標準，的確可以提昇安全性的需求。

由於下列幾項新興的趨勢促進了 802.1x 的發展：

網路使用率在公眾與半公眾區域中的提昇

當網路從內部區域延伸到公眾區域後，管理者需要控制這些使用者的網路存取權力。在 802.1x 以前，使用者只要網路插上網路連接埠，就可以任意地使用網路資源，在無線網路的環境中使用者甚至只要接上無線網路卡，無需任何實體線路就可以無線上網。

控制每一個連接埠的需求提昇

網路連接埠是使用者連上網路的第一道關卡，在這道關卡上進行封包或是協定的過濾，就可以針對各別使用者來控制他們的存取權限。

認證、授權、紀錄(Authentication Authorization Accounting，簡稱 AAA)的需求提昇

傳統的做法可以透過遠端撥號服務或是經由防火牆來達到 AAA 的需求，目前許多地方都在投資 AAA 的基礎建設以達到對使用者上網的存取控制。802.1x 標準可以讓目前 802.1x 的設備結合 AAA 伺服器達到上述的功能。

傳遞動態加密金鑰的需求提昇

無線網路中的 WEP 做法是為了達到跟有線環境上相當的加密等級，它透過對稱式加密方式讓兩端使用者建立一個加密的通道來傳輸資料。如何安全地傳遞及管理這些加密金鑰是一項極大的挑戰。802.1x

提供了一個方法可以傳遞 WEP 金鑰給 AP 及用戶端。

3.4.1. 802.1x 概述

IEEE 802.1x，也稱為 Port Based Network Access Control，定義了一個以網路連接埠為基礎的存取控制認證方式。

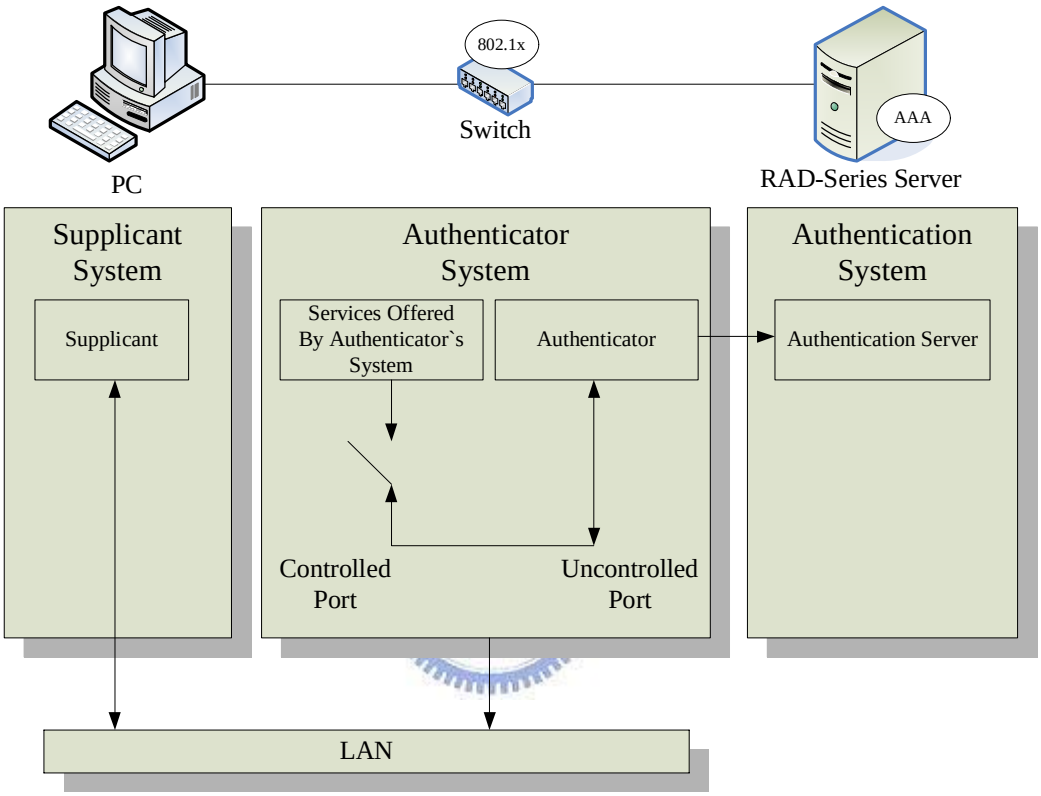


圖 8 Supplicant, Authenticator 與 Authentication Server 關係圖。在 802.1x 中每一個連接埠即需要一個 Authenticator。上圖表示連接埠未經授權，所以不允許網路封包通過。

3.4.2. 802.1x 用於無線網路

在無線網路中應用 802.1x 標準時，客戶端必須先與連線的 AP 建立關聯(association)，建立完成後才能與認證伺服器交換 EAP 訊息來認證邏輯連接埠。當邏輯連接埠被授權之前，AP 只能用來交換 EAP 訊息。建立關聯及 EAP 認證的流程如圖 9：

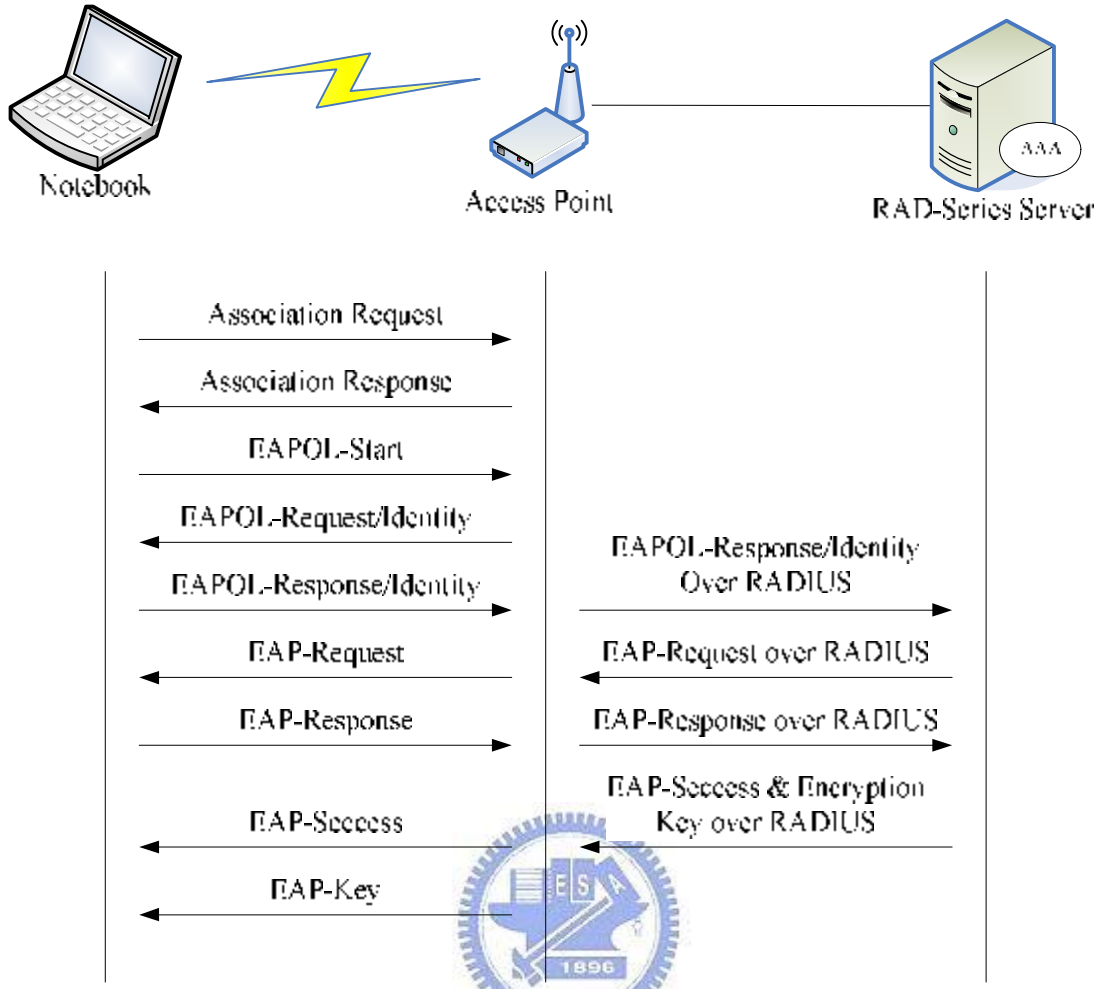


圖 9 無線網路中 Association, Authentication 及 Key Distribution 的過程

802.1x 標準利用下列兩個特點來達到每一個連接埠的存取控制：

- **建立邏輯連接埠**

在 EAPOL 協定的交換過程中使用了客戶端及 AP 的 MAC Address 以達到對邏輯層位址的控制。

- **金鑰管理**

客戶端在認證完成後，AP 才會送出或收到包含金鑰資訊的 EAPOL-Key 訊息。

建立邏輯連接埠

但在無線網路的環境中，每一個客戶端並不是透過實體的連接線

連上網路，甚至許多台電腦會經由一個 AP 來上網，因此 802.11 的環境中，客戶端必須透過一個建立關聯的過程才能上網。透過關聯的過程，AP 才能得到電腦的 MAC Address，客戶端即可以建立一個「邏輯連接埠」，之後才能與 AP 通訊。AP 必須使用 Open Authentication，才能讓客戶端在取得 WEP 金鑰前建立關聯。當關聯建立完成後，所連接的電腦即可使用 EAP 協定做認證的動作。

金鑰管理

802.1x 是一個認證協定，其中不包含 WEP 或其他的加密演算法，它透過 EAPOL-Key 訊息即可讓 AP 發佈加密金鑰的資訊到客戶端。這個訊息是每個 session 使用一次，如果有心人士想要擷取 WEP 金鑰，下個 session 後這個金鑰就沒有用了。

3.5. TKIP

TKIP 全名是 Temporal Key Integrity Protocol，是由 IEEE 802.11 TGi 所公佈的一個安全性的整合方案，為了加強舊有 802.11 設備的安全性。在 2003 年之後的無線設備上應該都已經支援 TKIP 的標準。

TKIP 相較於原本的 WEP 加密機制，多了以下的能力

- **48-bits 的 IV 值**
- **TKIP Per-Packet Key 加密機制 è 每個 Packet 都產生不同加密的 Key**
- **MIC(Message Integrity Code)<Michael> è 訊息完整性編碼機制**

在 TKIP 加密的機制下，會經過兩個階段產生之後要透過 RC4 加

密的 Key，也就是說基本上 TKIP 的加密機制與 128-bits WEP Key 是一樣的，只是在於產生 Key 的方式不同，主要的差別就是 WEP Key 是把使用者輸入的 WEP Key 與 IV 值直接作為加密的 RC4 Key 值，可是對於 TKIP 而言使用者所輸入的 TKIP Key 與封包的 IV 值都只是產生最後加密所用 128 bits 的參數，而不是直接把輸入或是夾帶的 IV 值拿來加密，相對的也就提高他的安全性。更可為每一個封包不同加密的 128 bits Key 值，提供最完整的安全性。而原本用來加密的 48 bits IV 值，被分為兩個部分(32 bits 與 16 bits)，分別在 Phase 1 與 Phase 2 的程序中參與加密 Key 的產生。

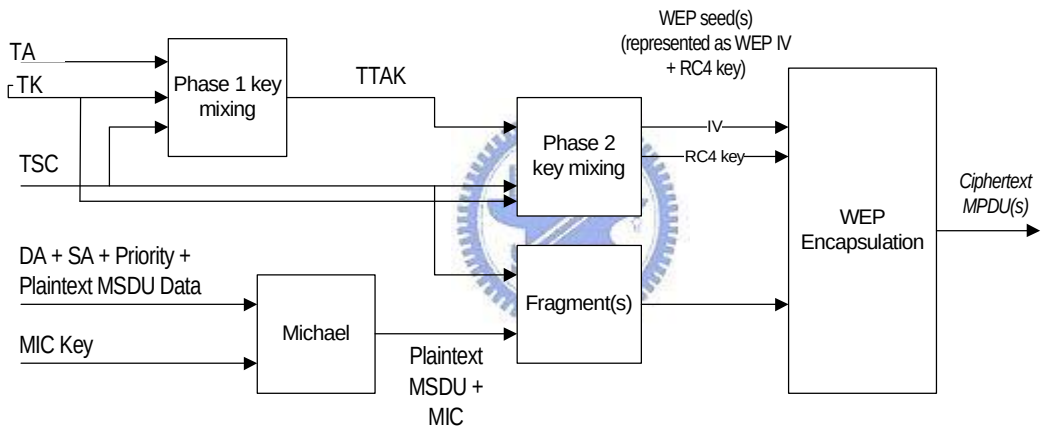


圖 10 TKIP 加密流程

在第一階段的 mixing function 中輸入 128-bit 的 TK、48-bit 的 TA 以及前 32-bit 的 TSC 值，經由 S-BOX 的轉換最後得到一個 80-bit 長度的 TTAK。在第二階段中則輸入了第一階段產生出來的 80-bit TTAK、128-bit 的 TK 及後 16-bit 的 TSC 值，經由互斥或、加、減、AND、OR 以及向右位移等運算元，產生 WEP 中所需要的 IV 及 seed 數值，整個 TKIP 的加密流程請參考圖 10。解密的過程則是加密過程的反向運算，請參考圖 11。

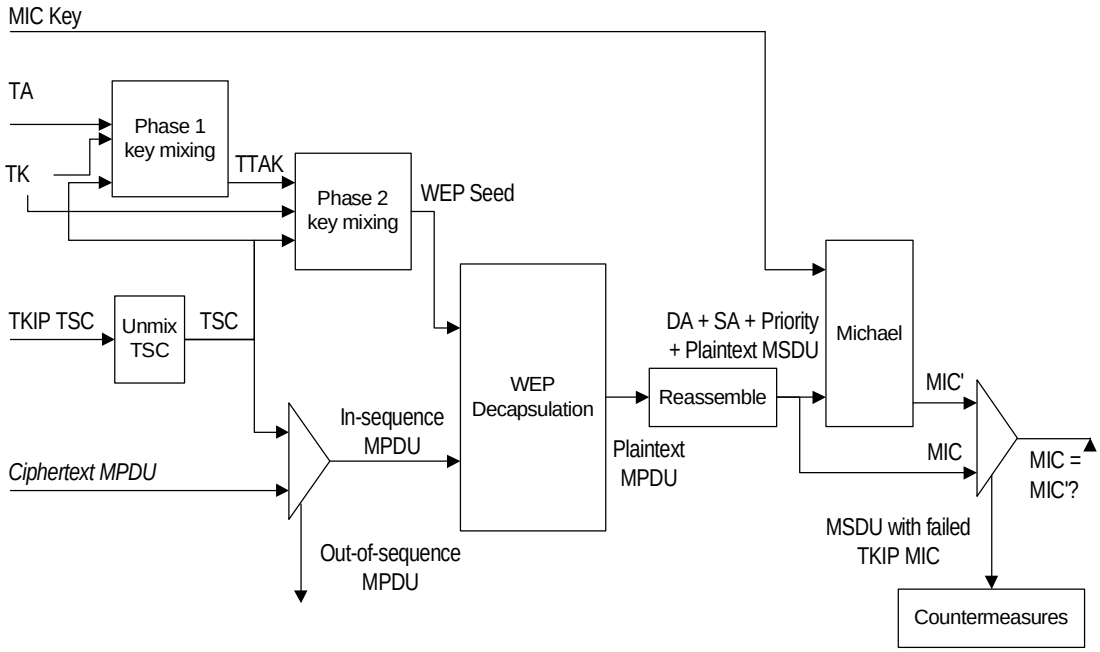


圖 11 TKIP 解密流程

除了產生 Key 的方式更為安全以外，TKIP 還多了對於傳送封包完整性的確認，如下圖 12 所示，在目前的 WPA 中還加入了 MIC(Message Integrity Code) 用來確認訊息完整性的編碼機制，透過在每一個封包的後面加入一個 MIC 值，來確認彼此封包的完整性，比起過去只單純的透過 CRC 值來確認封包的正確性，又提高了可靠度。

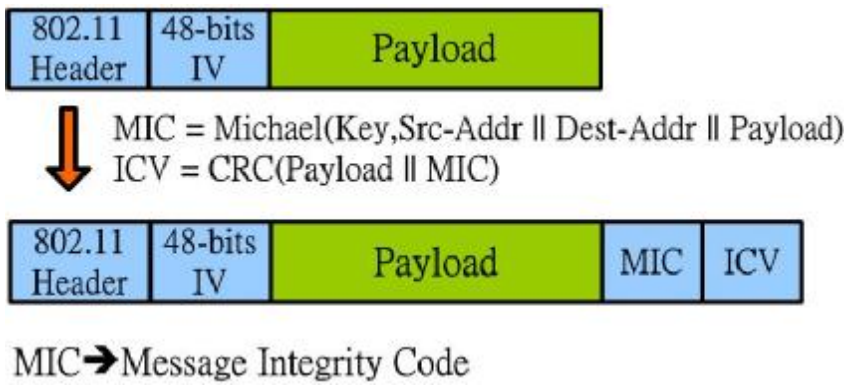


圖 12 在 802.11 WPA 下的封包格式

3.6. AES

由於 802.11 的認證問題與 WEP 的加密問題是眾所周知的，IEEE 組織於是使用 TKIP 及 802.1x 來補強這些問題。同時，IEEE 也在尋求一個更強而有力的加密機制。於是在 802.11i 的標準，IEEE 採用了 Advanced Encryption Standard (AES)來當做資料加密的標準。

AES 是由美國 National Institute of Standards and Technology(NIST)組織所認可的新一代資料加密的標準[23]。它也是目前美國政府單位所用來保護機敏資料的加密標準(FIPS-197)。當初是由 NIST 向各密碼學團體尋求一個新的加密演算法，這個演算法必須是完全公開而且無須負擔專利權版稅的。在 NIST 的規範中，AES 密碼系統最低需求必須符合下列幾點：

- **必須是區塊密碼系統**
- **區塊長度最低為 128-bit**
- **加密金鑰長度最低為 128-bit**
- **安全強度必須大於或至少等於 3DES，但效率必須大幅提高。**

在 NIST 公告徵求下一代的區塊密碼系統 AES 之後，共有 MARS 等 15 個 AES 候選者演算法；1998 年 8 月開始 15 個 AES 候選者演算法的第一回合技術分析；1999 年 3 月舉辦 AES 第二次會議，討論第一回合中提出的技術分析；同年 4 月結束第一回合的技術分析，選出 5 個 AES 候選者，分別是 MARS、RC6、Rijndael、Serpent、Twofish；2000 年 4 月舉辦 AES 第三次會議；NIST 並針對這 5 個 AES 候選者進行更深入的分析，2000 年 5 月發對這 5 個 AES 候選者的公開評論和分析；最後由 Rijndael 演算法脫穎而出，NIST 在 2000 年 10 月公開選定 Rijndael 的區塊密碼(Block Cepher)系統成為 AES 標準中的加密演算法。Rijndael 是由 Joan Daemen 和 Vincent Rijmen 所設計，它

是一個利用固定大小的區塊(state)及不同長度的 key，反覆運算的區塊加密器。區塊長度為 128-bit，加密金鑰的長度可為 128、192、256-bit，重複運算的次數分別為 10、12、14。AES 是以速度、安全及簡易度優勝，能在絕大部份的處理器及硬體上應用。

關於 Rijndael 演算法的細節，可參考 Rijndael 演算法的網站[24]，或是 NIST 組織中有關 AES 標準的網頁[25]。其讀法可讀為”rhine-doll"。

AES 是一個對稱式金鑰區塊加密法，這把對稱式的金鑰可以同時用來加密及解密。AES 支援了 128、192 及 256-bit 三種金鑰長度，愈長的金鑰代表其擁有愈強的安全性。區塊加密法是運作於固定長度的位元組，不像串流加密法(例如 WEP 中所使用的 RC4 演算法)，是一次轉換一個位元組。這個區塊的大小即稱為 block size，AES 使用了 128-bits 的 block size，如果欲加密的資料長度不是 block size 的倍數，使必需要有一個塞充的機制將資料長度擴充成 block size 的倍數。區塊加密法可以有許多的操作模式，例如 Electronic Codebook(ECB)模式、Counter(CTR)模式以及 Cipher-Block Chaining(CBC)模式等等。

ECB 模式

ECB 模式是最區塊加密法最簡單的方式，它先將加密訊息 M 切割成 $M_1,M_2...M_n$ 等等區塊，然後再將每個區塊單獨加密之，可用下列公式表示之：

For i=1 to n do C_i ß $E_k(M_i)$

E_k 表示使用 K 金鑰的加密函式，最後每個區塊會加密成 $C_1,C_2...C_n$ 等等的加密訊息。解密的話則反向操作之，如下列表示式：

For i=1 to n do M_i ß $D_k(C_i)$

D_k則表示使用 K 金鑰的解密函式。

ECB 是最不安全的加密模式，因為相同的兩個明文區塊會產生兩個相同的加密區塊，這些資訊對攻擊者會非常有用。ECB 的加解密流程可參考下圖。

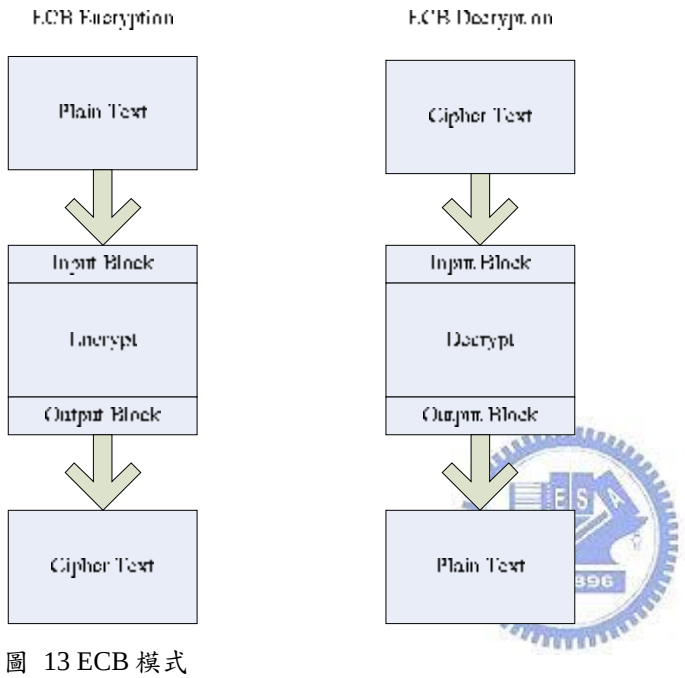


圖 13 ECB 模式

Counter 模式

Counter 模式則是透過計數器遞增的方式來輔助加密。我們一樣的把訊息 M 切割成 $M_1,M_2…M_n$ 等等區塊，可用下列公式表示之：

Counter ß 0

For each message M = $M_1,M_2…M_n$

Initial-counter ß counter

For i=1 to n do C_i ß $M_i \oplus E_k$(counter), counter ß counter+1

Encrypted-message = initial-counter $C_1,C_2…C_n$

由上述公式可知，CTR 模式是將 counter 加密再與明文做 XOR 運算來產生密文，之後再將 counter 遞增以運算後續的區塊。最後再將

initial-counter 包在加密區域之前傳送給對方，以告知 initial-counter 為何。解密端則依反向操作取得明文：

For an encrypted message C = initial-counter $C_1,C_2…C_n$

Counter ß initial-counter

For i=1 to n do M_i ß $C_i \oplus Ek(counter)$, counter ß counter+1

$M = M_1,M_2…M_n$

CBC 模式

CBC 模式是區塊加密法中最常被使用的方法，一開始先選定一個 initialization vector(簡稱 IV)，加密過後的區塊再當做下次的 IV 與下一個區塊一起加密。跟 CTR 模式一樣，CBC 模式也可以防止同樣的明文區塊產生一模一樣的密文區塊，以防有心人士攻擊。CBC 模式可用下列公式表示之：

For each message $M = M_1,M_2…M_n$

IV ß randomly selected value

For i=1 to n do C_i ß $E_k(M_i \oplus IV)$, IV ß C_i

Encrypted-message = initial-IV $C_1,C_2…C_n$

解密端則依反向操作取得明文：

For an encrypted message C = initial-IV $C_1,C_2…C_n$

IV ß initial-IV

For i=1 to n do M_i ß $C_i \oplus Dk(IV)$, IV ß C_i

$M = M_1,M_2…M_n$

CBC 模式的加密流程可參考圖 14。解密流程請參考圖 15。

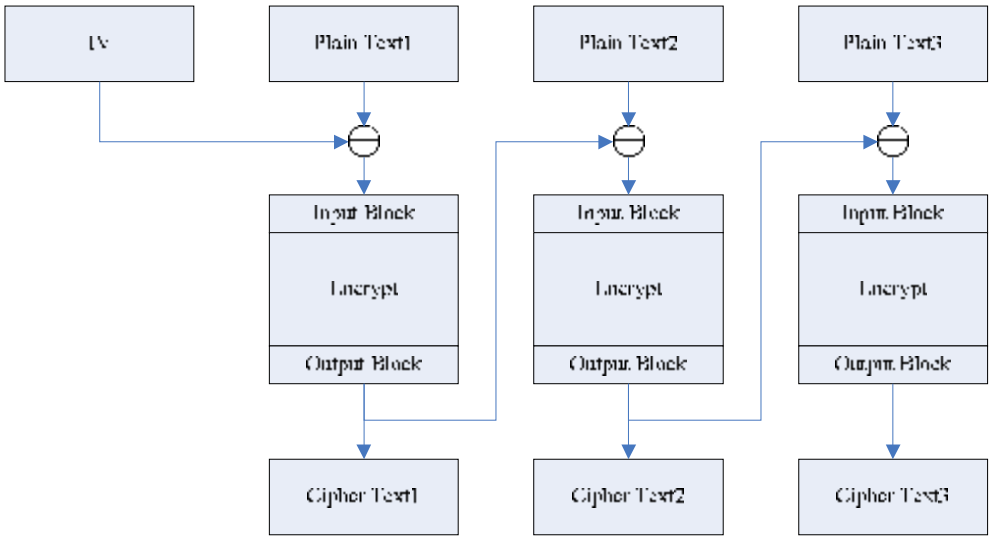


圖 14 CBC 模式的加密流程

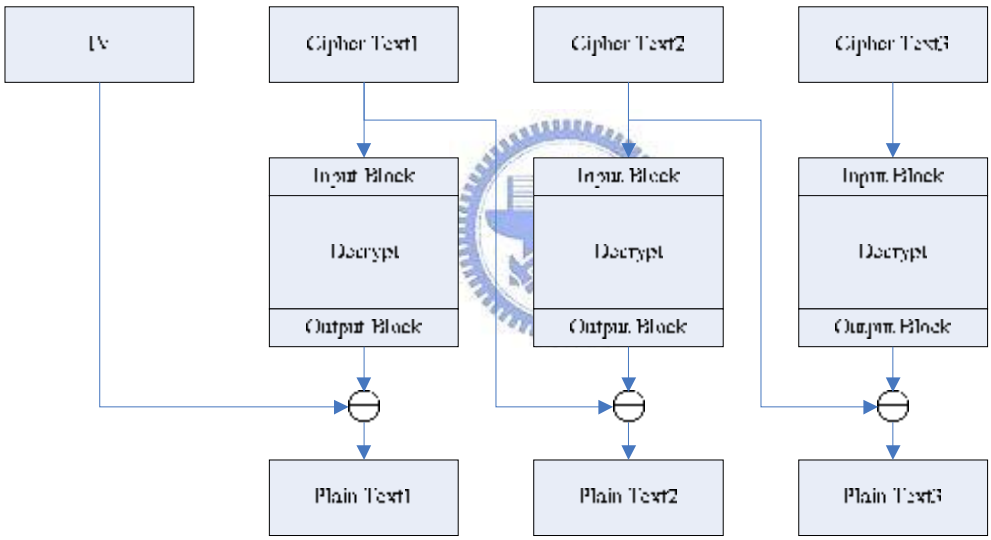


圖 15 CBC 模式的解密流程

3.6.1. AES 用於 802.11i

目前 IEEE 802.11 TGi(Task Group i)所定義的 802.11i 標準中是使用 CCMP (Counter-Mode/CBC-MAC Protocol)的加密協定來提供加密性、認證性以及完整性等功能。

CCMP 加密協定使用 AES 演算法中的 CCM 模式。CCM 結合了 Counter Mode 的方式提供資料加密性，另外以 CBC-MAC 方式來提供資料的完整性。CCM 是使用 128-bit 的金鑰長度來做資料加密。這樣

的方式不但擁有良好的加密特性，而且不管在軟體或硬體上皆可提供足夠的安全性及效能。

第四章　廠商獨家規格(Proprietary Solutions)

4.1. Cisco LEAP

Cisco LEAP(Lightweight Extensible Authentication Protocol)協定提供了以每個使用者為基礎的雙向認證功能,也提供了動態 WEP 金鑰的產生給每一個不同的工作階段，以加密每個在無線網路中傳輸的封包。通常用於認證 Cisco 的無線基地台 Aironet 系統與 Cisco 自己的無線客戶端網卡。

LEAP 需要三個元件才能提供認證功能：客戶端設備、支援 EAP 協定的無線設備以及後端的認證伺服器，由於 LEAP 是使用了 MSCHAP 加密通訊協定來加密使用者所提出的證明，所以後端伺服器可以使用 Cisco 自己的 Access Control Server 認證伺服器也可以使用微軟的 Windows 2000 AD 伺服器。以整合企業現有的系統帳號，這也是 LEAP 所提供的好處。

不過目前 Cisco LEAP 已經沒有繼續維護，也由於 LEAP 中存在字典攻擊的弱點,所以 Cisco 現在正積極的改推 PEAP 以及 EAP-FAST 兩個標準。

4.2. PEAP (Protected EAP)

PEAP，即 Protected EAP。是一個認證的協定，用來結合 802.1x/EAP 的機制以提供更安全的無線網路環境[26]。由於原本的 802.1x/EAP 安全機制由於只提供 MD5、TLS 等等的認證方式，它有以下幾項缺點：

- **安全性問題**

使用者的證明或 EAP 型態的資料並沒有被保護，這會造成有心人士可能在封包中塞入一個比較不安全的 EAP 型態，另外使用者的身份證明也是以明文的方式在 EAP 的協定中交換。

- **認證延遲的問題**

當使用者從某個無線網路設備漫遊至另一個無線網路設備時，原有的 EAP 型態需要執行整個認證的程序，這會造成應用程式的延遲還有連線失敗的問題。

Wi-Fi 組織建議使用 PEAP 以提供下列幾項功能：

- **使用者認證**
- **AP 與客戶端的雙向認證**
- **為 WEP 或 TKIP 產生動態金鑰**

PEAP 需要三個元件組成：第一是 TLS 的 Radius 認證伺服器(例如 Windows 2000 伺服器版本或是其他第三方的認證伺服器)；第二是 802.1x 相容的 AP；第三是 PEAP 的客戶端軟體。

4.2.1. PEAP 架構

PEAP 是由 Microsoft、RSA Security 與 Cisco 公司所支援的一項 IETF 草案，它跟 Funk Software 公司所推出的 EAP-TTLS 大同小異。PEAP 使用 TLS 加上一層保密層於 EAP 型態之上，這個 TLS 層是用來保護 EAP 認證訊息的完整性。

無線網路中的 PEAP 需要三個軟體和硬體的元件來實作之，請參考下圖 16。首先客戶端必須安裝 PEAP 的客戶端軟體，透過這個軟體連上證明者，這個證明者就是 PEAP-enable AP 或是無線網路交換器，在整個認證的過程中，證明者只是一個客戶端與認證伺服器間的中間

人，直接客戶端認證成功後，才能經由證明者上網。另外認證伺服器也必須支援 RADIUS、EAP 以及 TLS 的服務以驗證經由證明者轉送過來的使用者身份證明。

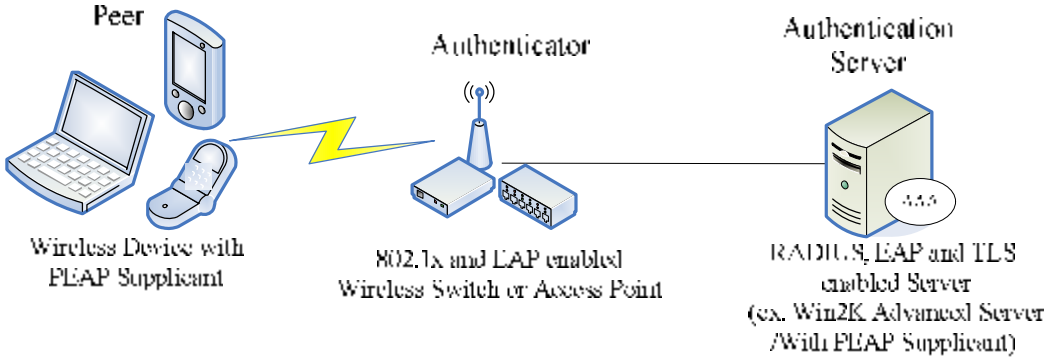


圖 16 PEAP 架構與組成元件

4.2.2. PEAP 運作方式

PEAP 安全機制分成兩個階段來完成認證的程序以傳送加密的網路資料。其流程請參考圖 17。

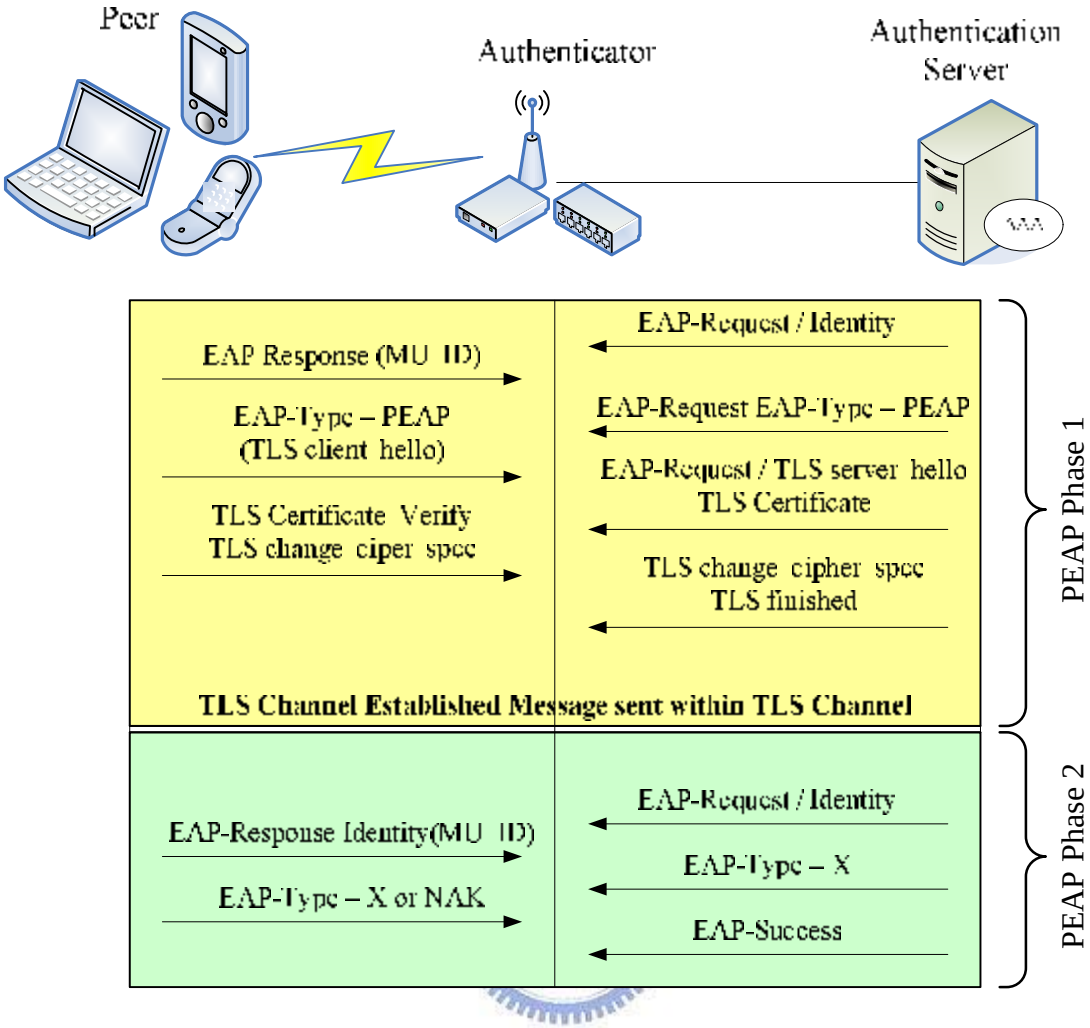


圖 17 PEAP 運作流程

第一階段

在第一階段中，證明者會使用 TLS 交握協定與客戶端建一個加密通道，底下是這個階段的流程：

客戶端先傳送一個訊息給後端的 EAP 伺服器，告知客戶端欲連接無線 AP。這個訊息告知伺服器一個新的連線應該要被初始化。此外客戶端也要告知自己所支援的加密演算法，如此一來在伺服器與客戶端兩邊才能瞭解所傳送的加密訊息。

伺服器在接收到初始訊息後，傳送一個回應給客戶端，其中包含一個新的工作階段 ID、所支援的演算法列表以及一個伺服器的公開金

鑰憑證。客戶端透過這個憑證才能得知自己的所連線的 AP 是網路上合法的無線設備。伺服器選擇一個由客戶端提出的加密演算法。PEAP 不需要實作 TLS(RFC 2246)中所列出的加密演算法，但是為了相容性的問題，PEAP 客戶端與證明都必須支援下列兩種加密演算法：

- **TLS_RSA_WITH_RC4_128_MD5**
- **TLS_RSA_WITH_RC4_128_SHA**

客戶端會使用事先預存的根憑認來驗證伺服器所提出的憑證，驗證後可得伺服器的公開金鑰，利用這組金鑰來加密一組秘密金鑰，最後把這個加密的訊息回應該給伺服器端。

如果伺服器可以解開這個回應訊息，表示客戶端被合法地授權。因為只有伺服器的秘密金鑰可以解開由公開金鑰所加密的訊息。

在這最後的交換訊息之後，AP 的認證算是完成，一個加密的 TLS 通道也會被建立起來以保護使用者的認證證明，這個認證證明會被傳送到第二階段。

另外 PEAP 跟 EAP 最大的不同之處在於，最後成功與失敗的封包是被封裝於 TLS 通道之中的，這樣一來可以防止有心人士將其偽造。因為一個偽造的失敗封包會讓客戶端連線失敗。一個偽造的成功封包會讓客戶端連線到一個非法的 AP。

第二階段

如果在第一階段中已經成功地建立了一個 TLS 通道，第二階段就是另一個完整的 EAP 流程，這個流程會在第一階段的 TLS 加密通道中來進行。這樣的方式可以確保第二階段的 EAP 訊息都在通道中被加密來傳輸，加密後的訊息使得使用者的 EAP 認證訊息被安全地傳送，這些訊息包括密碼、智慧卡或是數位憑證等等。以下即是第二階段中的

EAP 流程：

1. AP 與客戶端之間會交換受到 TLS 所保護的挑戰與回應訊息。這可以防止封包被偷聽以及修改。
2. 認證伺服器選擇一個 EAP 認證的型態，這個型態可以是 EAP-MD5 或是 EAP-TLS 等等。客戶端可以回應 NAK 訊息給伺服器，告知伺服器選擇另一個 EAP 型態來做認證。這個 NAK 訊息也會在 TLS 的加密通道中被加密然後傳送出去，以防封包被偷聽或修改。這使得攻擊者無法得知客戶端與伺服器之間是使用何者 EAP 型態進行認證。
3. 整個 EAP 流程繼續進行，直到客戶端收到成功或失敗的封包。
4. 當客戶端收到成功或失敗的封包後，TLS 的加密通道即被客戶端及伺服器所中止。

另外 TLS 也提供了一個連線重建的機制，可以讓使用者在漫遊到另一個新的 AP 時快速地重新認證。只要 session ID 仍然合法，客戶端及伺服器就可以使用舊的密鑰來進行交握(handshake)，確保整個連線持續及安全。

下表為各種 EAP 認證型態的比較：

表格 6 各種 EAP 型態的認證方式比較

EAP 認證型態	802.1x/EAP 應用	雙向認證	資料加密
EAP-MD5	Yes	No	No
EAP-TLS	Yes	Yes	Yes
LEAP	Yes	Yes	Yes
EAP-TTLS	Yes	Yes	Yes
PEAP	Yes	Yes	Yes

4.3. SonicalWALL WiFiSec

遠在西班牙的瓦倫西瓦科技大學使用了 Wireless 加上 VPN 的方

安來解決無線網路認證與加密的問題[27]。國內的中正大學電算中心[28]也使用了一樣的方案。淡江大學研究生也提出了 Linux 整合 IPSec 當做 AP 的做法[29]。不過 SonicWALL 公司把 VPN 整合到 AP 上，提出了 WiFiSec 的解決方案。

WiFiSec 是由 SonicWALL 公司所提出的無線網路保全方案[30]。它是透過 Access Point 內建 VPN 及防火牆來達成安全性的需求。SonicWall SOHO TZW 解決方案圖 18 中的 Access Point 即為 SonicWall 的 SOHO TZW 產品。

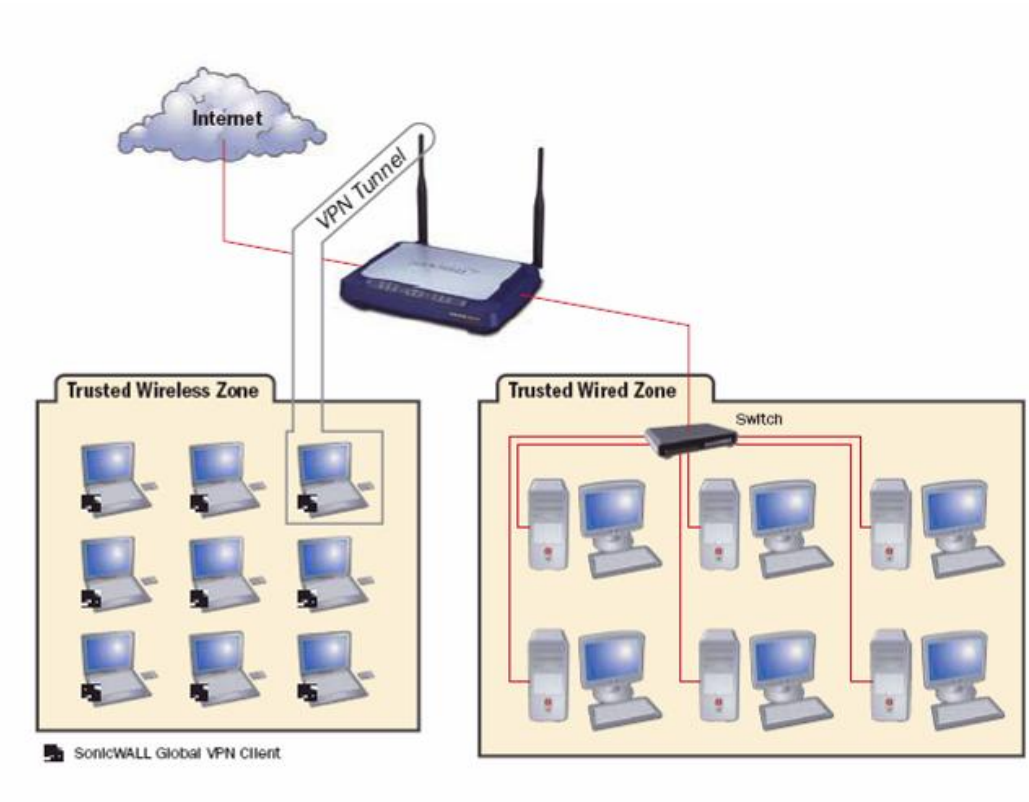


圖 18 SonicWall SOHO TZW 解決方案

SOHO TZW 提供了下列幾項特點：

整合三大元件

SOHO TZW 整合了 Access Point、VPN 及防火牆於一台設備之中。SonicWALL 是第一家將這些安全性功能整合於同一設備的公司。

SOHO TZW 使用了 802.11b 的標準，可與市面上其他的無線產品相容。

提供有線及無線網路完整的安全性

SOHO TZW 整合了防火牆功能於設備中，以保護有線及無線網路的安全性。SOHO TZW 可以同時容納 25 個使用者，或透過升級的方式提昇至 50 人或無限制人數。如此一來可以讓網管人員有彈性地配置於各種有/無線環境之中。

緊密地結合 SonicWALL Global VPN Client

SOHO TZW 整合了 SonicWALL Global VPN Client 產品。它使用了業界標準 3DES 加密演算法以保護資料的安全性；同時也提供了簡易的安裝精靈，來設備 VPN 的連線；另外也提供一個方便的使用者界面易於操作；另外它也會自動偵測 VPN 的設定，從 VPN gateway 下載後自動地連上線。

強制使用 VPN 技術

SOHO TZW 可以讓管理人員強制對所有無線環境使用 VPN 技術，以建立一個安全的無線網路環境。

無線訪客服務(Wireless Guest Services，簡稱 WGS)

SOHO TZW 可以為訪客使用者建立一個無線網路環境，並限制使用者無線網路的存取區域。管理人員可以為這些顧問、廠商、訪客等等使用者建立一組暫時的使用者名稱及密碼，這些人就可以連上網際網路，但連不進公司的內部網路，而且這些使用者也無法與對方建立連線。WGS 是一個理想的解決方案，可以提供一個暫時的網路服務給訪客、工讀生或是書店/咖啡店的顧客。

各式裝備皆適用

SOHO TZW 可以運作於桌上型電腦、筆記型電腦、個人數位助理

等等設備，也可以整合其他廠商的 802.11b 無線網卡。

完整地安全防護

SOHO TZW 提供了一整套的安全功能。之前曾經提到，它使用了 3DES 加密演算法，也包含了 VPN 通道的技術可以為上層的應用程式提供更完整的安全性。也可以整合於已經建置 802.11b 的企業。其他資訊可參考其網站。

4.4. 其他功能(Other Features)

上述的 40/64-bit WEP 以及 128-bit 的 WEP 加密方式已經屢見不鮮，部分廠商為了加強無線網路的安全性議題，無不攪盡腦汁開發出無線網路安全中所沒有定義到的功能，以下針對幾個常見的安全特性提出來討論：

4.4.1. 停止 SSID 廣播功能

大部分的無線網路設備會廣播自己的 SSID。這個功能可以很方便的讓訪客使用者得到 SSID 然後連線無線網路，不過也會讓駭客輕易的得知 SSID 的內容。所以記得要停止廣播 SSID。

4.4.2. 拒絕 ANY 的 SSID

在 802.11 的標準中定義中，公開認證模式可以允許使用 ANY 當做 SSID 的設備進入網路，部分的無線網路設備可以拒絕以 ANY 當做 SSID 的設備。

4.4.3. MAC 位址過濾器

部分的無線網路設備擁有 MAC 位址過濾的功能。開啟 MAC 位址

過濾功能，可以只讓記錄於 AP 內合法的網卡位址上網，其他的網卡一律無法連線。這樣駭客就無法使用亂數的網卡位址來連接無線網路，並且隱藏自己的位址了。

4.4.4. 防火牆

部分的無線網路設備擁有 IP 層以上的防火牆功能，可以讓使用者自行定義哪些封包可以通過，哪些封包不能通過防火牆。

4.4.5. 網址阻擋/家長控制服務

Linksys 的最新無線網路 AP 中擁有家長控制服務的功能，透過帳號密碼的管制，家長可以限制家中每一個成員可以上網的網址。AP 中擁有關於暴力、色情等等的存取範本，這些範本中記錄著全世界有哪些網站屬於這個範本，如果家中成員欲存取這個網站，AP 就會將這個連線擋下並且拒絕連線。所定義的範本可透過付費的方式來更新。其他廠牌的無線網路 AP 也有相同的功能，例如 Microsoft MN-700、D-Link DI-514、3COM OfficeConnect 系列以及 ASUS WL-500g 中都有相同的功能，不過它們僅能透過手動的方式來更新網址名單。

4.4.6. 無線網路閘道器

無線網路閘道器是透過後端集中式的帳號管理，讓使用者無論身在何處，都可以透過閘道器將認證服務重導至後端認證伺服器做認證，可以達到同一個帳號在多處都可以無線上網，也可以管制沒有帳號的使用者無法存取網路。

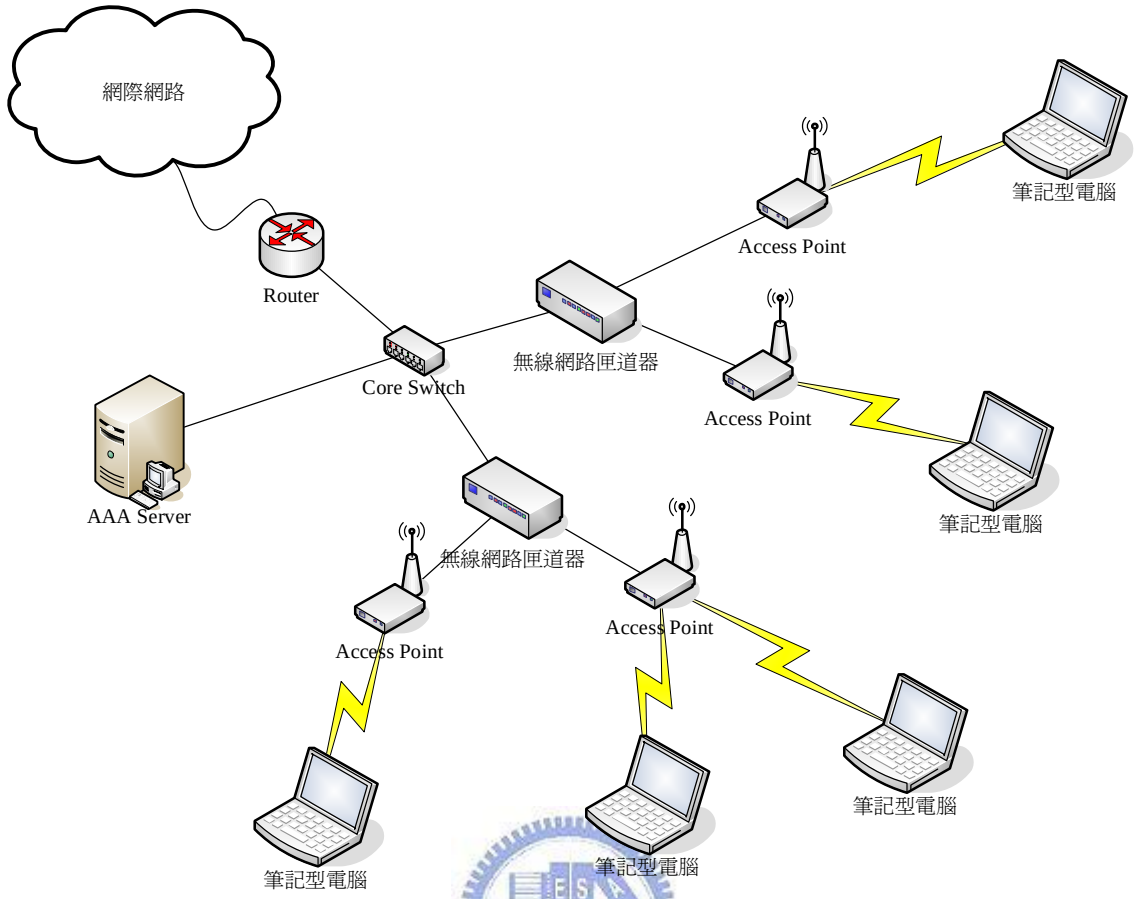


圖 19 無線網路閘道器示意圖

整個無線網路認證閘道器示意圖如圖 19，客戶端設備與 AP 產生關聯之後，無線網路認證閘道器會限制該客戶端電腦所有對外的連線，閘道器會攔截第一個 HTTP 的連線要求，將這個連線要求重導至閘道器或認證伺服器所提供的認證網頁，要求使用者輸入帳號及密碼，完成身份認證之後，閘道器才會開放所有的對外連線。

目前市面上流行的「熱點」(Hot Spot)服務，或是旅館、機場所提供的無線網路，有許多都是使用無線網路認證閘道器達到認證與管制使用者的功能。

4.4.7. 安全功能比較

我們將目前市面上各家廠商的最新產品安全功能綜整，表格 7 列出這些安全功能的比較。

表格 7 各家產品安全功能比較表

	40 and 104-bit WEP	WPA (包含 802.1x)	AES	Router/NAT	VPN	Stop SSID broadcasting	MAC Filter	Firewall	URL Blocking
3COM OfficeConnect	ü	ü		ü		ü	ü	ü	ü
ASUS WL-500g	ü	ü	ü	ü	○	ü	ü	ü	ü
Buffalo WHR3-G54	ü	ü	ü	ü		ü	ü	ü	
Cisco Aironet 1400	ü	ü	ü	ü		ü	ü	ü	
D-Link DI-624	ü	ü		ü	○		ü	ü	ü
IOGEAR GWA502	ü	ü		ü	○	ü	ü	ü	
Linksys WRT54GS	ü	ü	ü	ü	○	ü	ü	ü	ü
Microsoft MN-700	ü	ü		ü		ü	ü	ü	ü
Netgear WGT624	ü	ü		ü	○	ü	ü	ü	ü
SonicWALL SOHOTZW	ü			ü	ü	ü	ü	ü	ü
Zyxel ZyAIR-G2000	ü	ü		ü	○		ü	ü	ü

備註：○表僅能透過 PPTP Client 連接 ISP

第五章　相關研究(Related Researches)

5.1. Secure Wireless Access to a Campus Network

西班牙的瓦倫西瓦科技大學(Polytechnic University of Valencia)使用了 Wireless 加上 VPN 的方案來解決無線網路認證與加密的問題[27]。由於整個校園網路約有 34500 名學生、2030 位教職員及 1000 位的員工，如何保護校園內的無線網路安全便是一個很大的議題。該大學提出的網路架構如圖 20，使用無需透過複雜的程序即可上網，並且可以確保資料在無線網路上安全地傳遞。

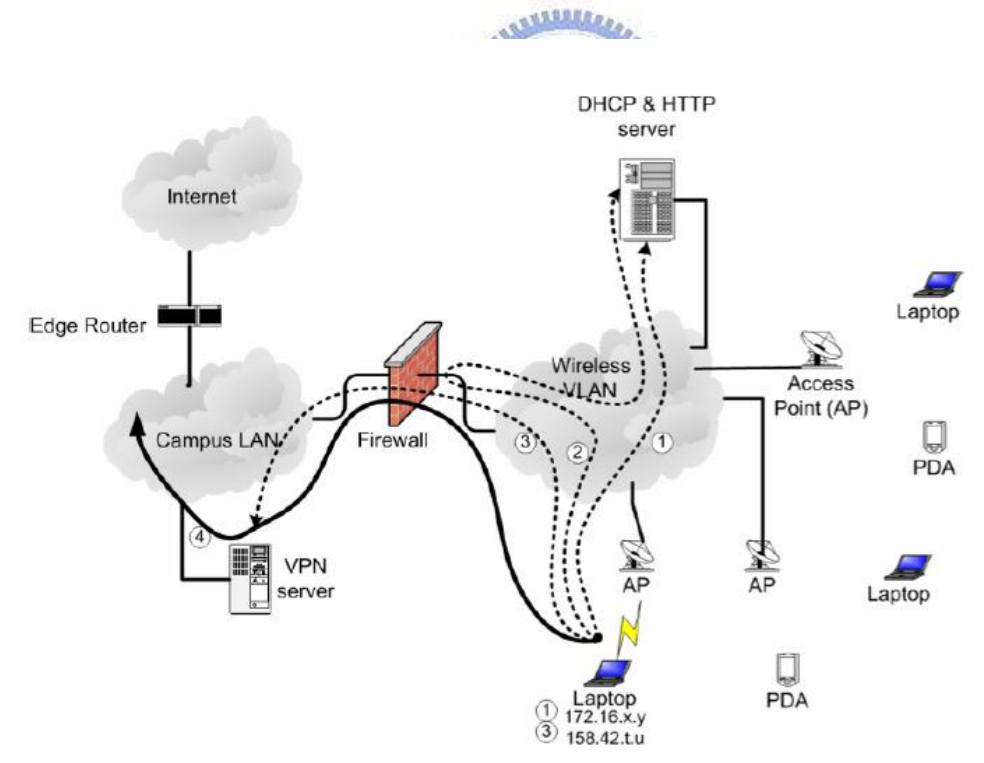


圖 20 瓦倫西瓦科技大學所使用無線網路安全方案

在上圖中，使用者首先透過內部的虛擬網路連上 DHCP 伺服器取得 IP 相關資訊。首次上網的 HTTP 連線要求會被重導到 HTTP 伺服

器，讓使用者下載 VPN 客戶端的軟體。第三步驟與 VPN 伺服器建立一個安全的通道，之後所有對外的連線與由 VPN 伺服器往外傳送，如此就可以確保資料是在加密過後的 VPN 通道中傳輸。

5.2. Wireless Security Threat Taxonomy

本文是由美國陸軍學院的 Welch 及 Lathrop 所提出的一個無線網路上的威脅分類法[32]。在這篇報告中描述了七種在無線網路上可見的攻擊手法，分別描述如下：

流量分析(Traffice analysis)

流量分析的攻擊通常都是透過一個接收端來偷聽無線網路上的封包資料，而後為了特定的資訊分析這些封包，這些資訊包含封包的數量、大小、來源地以及目的地等等。即使資料的內容經過加密，封包標頭的資料還是以明文的方式在網路上傳輸。

被動偷聽(Passive eavesdropping)

如果網路上所使用的加密方法是非常容易地就可以被破解(例如 WEP 以及其他的串流式加密方式等等)，那麼攻擊者就可以使用偷聽的方式來取得封包的來源、目的地、大小、次數等等資訊。不過在實際運用面上，這種攻擊只會用來對付很簡單的加密方式或是根本沒有任何加密方式的網路。

主動偷聽(Active eavesdropping)

主動偷聽是被動偷聽的一種延伸方式，它還額外地加入攻擊者的資料於封包中。要做到主動偷聽，攻擊者必須能夠接觸的使用者在傳輸過程中的資料(目的地機器就可以做到這一點)。IP 假造攻擊就是主動偷聽的其中一種方法，攻擊者可以將已經受控制的機器假造一個目的

地 IP，無線 AP 在傳送資料到目的地之前會先將資料解密，然後毫無警覺地傳送到這台假造的機器上，真實的機器由於沒有收到這些封包，所以只會簡單地要求使用者重送封包，而不會發生任何警訊。因為這種情形就像封包遺失一樣，在網路的傳輸過程中是很常發生的。

另一種主動偷聽的變形，即是加入資料到網路封包之中，如果資料可以很容易地被解密的話，攻擊就可以將自己的資料加入至原本的資料當中。

非授權存取(Unauthorized access)

非授權存取是針對網路上的一種攻擊方式，而不是針對資料本身，它的最終目的就是要進入你的網路內。這種方式的攻擊已經變成了網路上的一個主要的問題。對於無線網路而言，如果被入侵的話，攻擊者更可以在任何地方無限的存取無線網路。

中間人攻擊(Man-in-the-middle)

中間人攻擊是一種即時的攻擊方式，它是在傳輸的過程中將使用者原本的傳輸資料導向攻擊者所控制的機器上，將這些資料修改一下或著原封不動的傳輸到真正的目的地。

階段搶劫(Session hijacking)

階段搶劫是針對工作階段完整性的一種攻擊方式，攻擊者截取原本的使用者中授權及認證工作階段。使用者會以為是網路的問題而造成工作階段結束，但是卻不知道工作階段已經被別人取走。這樣攻擊方式發生在即時，並且可以延續使用下去。

重播攻擊(Replay)

重播攻擊通常是用來通過對方的授權，並且獲得網路存取權用的，一般來說使用者原本的工作階段並不會被修改或干擾。這種攻擊

方式並不會發生在即時，而是發生原本的工作階段之後。攻擊者會將使用者的認證封包截取下來，之後再重新傳送這個認證封包，或是另外發起另一個工作階段，如果這個認證訊息被認可了之後，攻擊者就可以在管理者不知情的狀況下成功地入侵網路。

5.3. Autonomic 802.11 Wireless LAN Security Auditing

本文是由 Rensselaer 理工學院的 Joel W.Branch、馬里蘭大學的 Nick L.Petroni Jr.以及 IBM 華盛頓研究中心的 Leendert Van Doorn 和 David Safford 所共同提出了一個分散式無線安全稽核(Distributed Wireless Security Auditor，簡稱 DWSA)架構[33]。透過 DWSA 可以發現大型企業內部的未經授權 AP，以提供一個自治及自律的網路保護。

防護 802.11b 的無線網路是一個重大且艱鉅的工作，在無線網路中有一個重大的問題即是非經授權的 AP、設定有誤的 AP 或者對等式(ad hoc)網路進入企業內部的無線網路，如此一來有可能造成有心人士從任何區域就可以進入企業內部的網路。DWSA 透過 Linux 及 Windows 系統當做感測器，可以不間斷地持續偵測網路狀況而後定時地回報到後端伺服器，以偵測非法或設定有誤的 AP，並將這些 AP 透過 3D 定位(例如 GPS)的演算法找出他們的位置。如此一來可以提供一個自律且即時的系統以保護整個無線網路的安全。

5.3.1. 運作原理

DWSA 的功能與其他的 802.11 偵測器相同，這篇研究報告提出了一個創新的概念是將這些大量且繁瑣的偵測工作運用於現有的無線網

路客戶端設備上，諸如桌上型、筆記型、Tablet PC 以及 PDA 等等裝備，透過這些設備來觀察 AP 的安全狀態。客戶端設備只做偵測與收集資料，而後經由安全通道輸送至後端伺服器，資料彙整則由後端伺服器完成。DWSA 架構圖請參考圖 21。

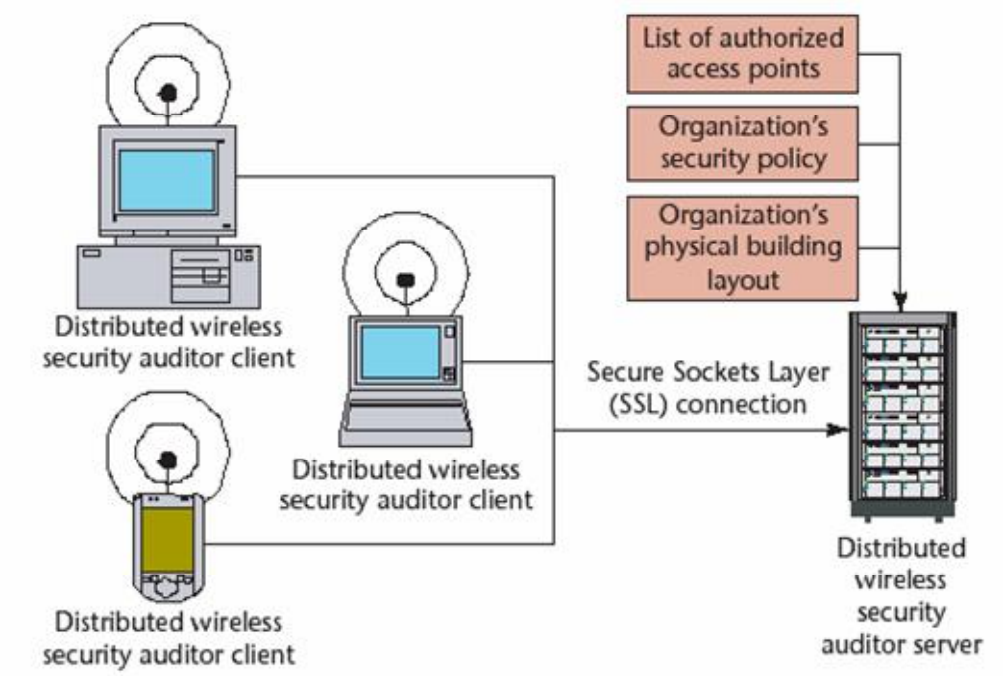


圖 21 DWSA 架構圖

5.3.2. DWSA 架構

由上述得知，DWSA 的基本策略是透過客戶端收集資料，而後傳送至伺服器端資料彙整，因此在本節會描述系統中的主要元件，另外 DWSA 也必須達到以下的幾個需求：

- **輕量化客戶端**

因為 DWSA 代理程式是運作在公司員工的電腦之上，為了不影響電腦的操作效率，代理程式必須運用少量且剩餘的系統資源來完成工作。此外，代理程式也應該要能在低電源的手持式裝備上運行。

- **移動性**

代理程式應能執行於所有的無線網路客戶端設備之上，包含筆記

型電腦及手持式設備。

- **安全傳輸**

在傳送資料到後端伺服器時，應能保證資料的正確性與完整性。

- **簡單使用且功能強大的政策訂定**

DWSA 的決策邏輯必須能簡單地的設定，並且能夠提供詳細的描述供管理者參考運用。

- **定位**

DWSA 應能透過所偵測的資訊得知其 3D 地理空間位置。即使客戶端設備是移動式的，也必須能夠計算出相關位置。

客戶端設備

DWSA 運用客戶端設備多餘的系統資源，透過一個在背景執行的代理程式，可以定時收集並回報無線網路的相關資料，由於計算工作是伺服器端負責，所以客戶端設備不須儲存資料。除此之外，代理程式也會傳送無線網路的電波強度供伺服器計算位置資訊。

DWSA 伺服器

伺服器具備足夠的系統資源以供進行大量資料運算，目前伺服器提供了三個主要的功能：互相相關、策略分析與回報以及互動式的 3D 顯示。互相相關是將客戶端所回報的資料綜整成一份有用的網路資料表，這份表格會隨著回報的資訊而變動，並且將舊有的記錄保存成歷史資訊。畫面結果請參考圖 22。策略分析則使用了跟防火牆類似的規則語言，如果與規則不符則會在畫面上以閃爍的方式警示管理者，並且將這些資料記錄下來。最後一個最有用的功能則是 3D 顯示的功能，它可以將客戶端設備、AP 或非法的 AP 以 3D 顯示的方式呈現出來圖

23。非法 AP 的位置是經過球面方程式所得，90%以上時間都可以算出非法 AP 的 6 呎的範圍內，並且可以經過多次的運算以得更正確的結果。

圖 22 回報資料畫面

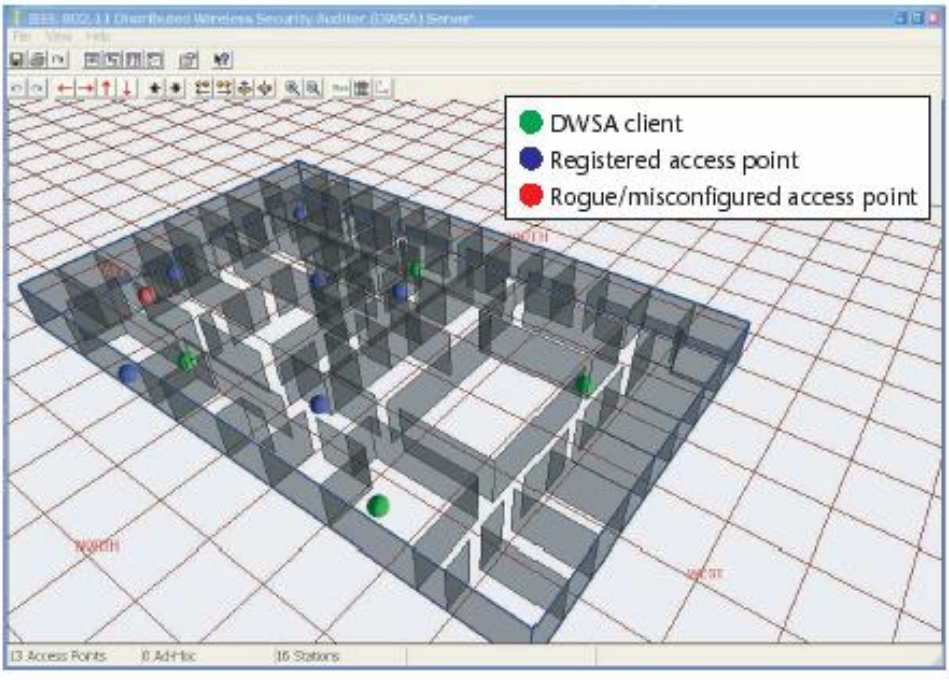


圖 23 3D 顯示效果

5.4. Linux 平台存取點與 IPSec 橋接器之研究

本篇論文是由淡江大學電機工程學系統 92 年畢業研究生曾左旭[29]所提出，主要在提出一種利用上層通訊協定的架構來解決目前無線網路通訊安全方面的問題。在 IEEE 802.11 的標準規範中，定義了 WEP (Wired Equivalent Privacy) 協定，用來保護目前的無線網路通訊環境。但是 WEP 協定卻有嚴重的安全漏洞問題，所以我們提出一個以 IPSec 為基本架構的 Linux 平台存取點（Access Point），使無線網路環境能夠有足夠的安全保障和較佳的管理系統，以符合我們的需求。IPSec 橋接器不但可以保障無線網路連線的安全，並且擁有較佳的系統效能，管理上面也比其它系統容易，而且以 Linux 為 OS 的關係，不但成本便宜，而且穩定性高，所以 IPSec 橋接器可以說是在無線網路安全系統中最好的選擇

第六章　攻擊與防禦(Attack and Defense)

由於無線網路的傳輸媒介是透過空氣來傳遞電波，所有的資訊可能會被躲在暗處的駭客所擷取，在網路上甚至有人利用脾酒罐或是洋芋片的包裝桶就可以做出翹鬍子天線[34]，這更是告訴我們在使用無線網路時的不安全程度。在 2.1.1 節中提到的 WEP 弱點，現在網路上也可以四處可見這些免費的入侵工具程式，所有程式支援的幾乎清一色是 Prism-2 晶片。使用這晶片的包括了 Compaq（康柏）WL100、友訊（D-Link）DWL-650、Linksys WPC11、以及 SMC 2632W 等，都是市面上常見的產品。會選用這晶片的原因是因為其 Linux 驅動程式（WLAN-NG）不需要登入網路，即可監聽封包。這程式會先搜尋設計不良、有漏洞的 IV，然後記錄 500～1,000 萬不等的封包，最後在剎那間將 WEP 金鑰算出來。以下將介紹一些在無線網路上的攻擊手段、駭客程式以及防禦的工具。

6.1.　一般常見攻擊手法(General Attack Methods)

攻擊的方法可以歸納為許多類型。有些攻擊方法通常是非常明顯的並且在許多案例中是廣為流傳的，例如病毒攻擊或是針對新硬體或軟體的漏洞進行攻擊。所幸大部分的問題事件都會在各大主流的媒體中所披露，這告訴我們需要常常去注意自己是不是可能陷入這些攻擊事件中，以下我們針對幾種常見的無線網路攻擊手法進行說明。

6.1.1.　偷聽(Eavesdropping)

偷聽是在網路上被動的擷取他人的資訊，就像在日常生活中有人在人群中偷聽別人的對話一樣。有許多程式即是透過這種手法方便地

在網路中擷取別人的資訊，例如 Airopeek、Airsnort、Net-Stumbler 以及 WEPCrack 等等。這些程式可以讓你得到 AP 的 SSID 及 MAC 位址等等資訊，甚至也可以知道 WEP 協定有無開啟。另外，透過他們也可以偷聽到一些諸如帳號、密碼等等的敏感資訊。

6.1.2. 插入攻擊(Insertion Attacks)

讓一台非法的設備獲得網路存取權稱為插入攻擊。只要在電腦上安裝無線網卡，並且進入無線網路的區域，這台電腦就有可能獲得無線上網的權限。或者是一台非法的 AP 安裝在網路上就有可能讓使用者誤認它是合法的 AP 而與之連線，造成資訊被非法 AP 所獲得。這些都稱為插入攻擊。

6.1.3. 中間人攻擊(Man-in-the-Middle Attacks)

傳統的中間人攻擊方式即是攻擊者從網路上將發送端的封包攔截下來，然後修改這些封包，再將這些封包重送回網路中。

6.1.4. 欺騙(Spoofing)

欺騙攻擊是指攻擊者假裝成別人取得上網權限或進行非法的動作，例如使用他人的帳號及密碼進入系統。著名的 IP 位址欺騙即是將自己的來源端 IP 位址改變，讓路由器不知該封包是由何著所發送。

6.1.5. 暴力攻擊(Brute-Force Password Attacks)

暴力攻擊法通常是用來破解密碼的，由於密碼可能是由各種數字、英文字母或符號的交叉組合，暴力攻擊法即是去試驗密碼的每一種可能，由第一種試驗到最後一種，直到試出密碼為止。

6.1.6. 阻絕服務攻擊(Denial of Service Attacks)

由於無法取得網路服務的關係，因此攻擊者會發動拒絕服務攻擊，使得其他使用者也無法取得網路服務。這樣的作法通常是針對某種服務，讓它負載過重然後造成服務失敗。這樣的攻擊可以針對很多種不同型態的資源著手，例如磁碟空間、頻寬、記憶體或暫存器等等。

6.2. AirSnort

AirSnort 是一個解開無線網路加密金鑰的工具。它採取被動的監聽方式，當擷取到足夠的封包時就可以計算出加密的金鑰值。由於 802.11b 中的 WEP 加密方式，已被 Scott Fluhrer、Itsik Mantin 及 Adi Shamir[4]證實了在 RC4 的 Key Scheduling Algorithm 中有嚴重的瑕疵，Adam Stubblefield[5]是第一個實現這個攻擊方式的人，但是他並沒有將程式公開，AirSnort 則是公開實現這個攻擊方式的程式，同一時間 WEPCrack 這支程式也同時發表出來。

AirSnort 需要收集大概五百萬至一千萬個加密封包，只要收集到足夠的封包數量，AirSnort 就可以在一秒鐘之內解開 WEP 的加密金鑰，相關的資訊可以參考其網站[35]。

6.3. WEPCrack

WEPCrack 跟 AirSnort 一樣是針對 Scott Fluhrer、Itsik Mantin 及 Adi Shamir 所提的 RC4 缺點所做的攻擊程式，另外它也是一個公開原始碼的程式。相關的資訊可以參考其網站[36]。

6.4. Kismet

Kismet 是一個 802.11 第二層的網路偵測器以及入侵偵測系統。它

可以在各種支援 rfmon 模式的無線網卡上運作，可以偵測 802.11 a/b/g 三種網路封包。Kismet 確認網路的方式也是採用被動收集網路封包來偵測沒有發出 beacon 訊號的隱藏網路。相關資訊可參考其網站。[37]

6.5. AirDefense

AirDefense 是一個商業性以及完整的安全性解決方案，它是由數個無線網路的智慧型偵測器及一個中央伺服器所組成的解決方案。這個智慧型的偵測器可以收集一般的辦公室環境內四萬到六萬平方尺範圍的網路封包。

AirDefense 包含下列幾點特性：

管理無線網路的資產：AirDefense 可透過偵測器偵測所有的無線網路設備、繪製出網路中各設備的關聯圖、並且針對沒有動作的 AP 發出系統警訊。另外，AirDefense 也會針對無線網路中的流量進行監視，發覺網路中的非法使用者以及 AP 的使用率。

偵測與分析無線網路的安全性：非法的無線網路設備是企業的最大威脅，因為一個非法 AP 的存在等於是替駭客在內部網路中開了一個大門。AirDefense 可以偵測出非法 AP、無線使用者、軟體 AP 以及無線讀條碼機等等設備。另外，AirDefense 透過流量的分析，可以偵測出 MAC Spoofing、Man-in-the-Middle、DoS、Dictionary 等等攻擊方式或其他的可疑活動。

訂定無線網路的安全策略：AirDefense 可以針對企業內部訂定不同的無線網路策略，並且隨時監控有無任何與現行策略不同的行為發生。這些策略包含 Configuration Policies、WLAN Device & Roaming Policies、Performance Policies、Channel Policies、Vendor Policies 等等。

提供無線網路在運作上的支援與協助。AirDefense 也可以隨時監控無線網路的健康狀態，並且隨時給予運作上的支援，以達無線網路的最大效能。AirDefense 會提供一份完整的評估報告，以協助管理者解決問題以及建議後續如何昇級等等。有關 AirDenfense，可參考其網站[38]。

6.6. Netstumbler

Netstumber 為一在 Windows 平台上的 Freeware，可用做 Site Survey 的工具。透過 Netstumbler，可以顯示在偵測範圍內無線 AP 的 SSID、頻道、訊號強度等等，也可以藉由 Netstumbler 在做 War-Driving 時，來掃描非法 AP 的存在。

6.7. 工具比較

表格 8 綜整了目前所廣泛使用的無線網路工具。

表格 8 各種無線網路工具比較表

	Crack WEP Key	Detect SSID	Detect Rogue AP	Location	Logging	Real-time Detecing	Asset Management	License	Platform
AirSnort	ü							O	U
WEPCrack	ü							O	U
Kismet	ü	ü	ü	ü	ü			O	U
AirDefense		ü	ü	ü	ü	ü	ü	C	H
Netstumbler	ü	ü		ü	ü			F	W

License: O:Open Source C:Commercial F:Freeware

Platform: U:UNIX/Linux H:Hardware W:Windows

第七章　SPIDER LAN 安全架構

本章將整理一般企業在建置無線網路時，各家廠商及研究所建議的安全做為。另外本篇論文也會提出一個較安全的無線網路建置方案，全名是 Simple Proposal for Intrusion Defense in Enterprise wiReless LAN(以下簡稱 SPIDER LAN)，透過此一方案以有效地防止不合法的 AP 及非授權的使用者進入該企業的網路。

7.1. 針對企業的一般性建議書

由於無線網路的便利性與機動性，使得許多企業主也趕著搭上這班列車。但也由於無線網路仍然存在許多安全性的問題，許多的學術研究以及商業報告會建議企業在建議無線網路時必須採取某些手段，以維持基本的安全性。一般性的無線網路建議方案如下：

7.1.1. 在 AP 的設定方面

通常網路管理者需要針對企業內部的安全政策與安全需求來設定並管理 AP，適當地設定管理密碼、加密設定、重置功能、自動網路連線、網卡位置存取控制清單、WEP 金鑰以及 SNMP 功能等等都可以避免許多的駭客攻擊事件。

變更預設的密碼

無線網路設備在出廠時就會預設一組管理密碼在設備中，部分的設備甚至根本沒有密碼。而且通常相同廠牌的設備會使用相同的密碼，使用這樣的密碼會帶來許多安全性的問題。如果沒有密碼，有心人士便可以輕易進入無線網路設備中更改網路的設備；如果有密碼的話，有心人士也可以用幾組廠商預設的密碼來試驗是否可以進入設

備。管理者應該要立即變更空白或是預設的密碼，最好依據上面的建議選擇一個複雜的密碼。

選用適當的加密設定

建議使用產品中提供的最高等級加密方式。WEP 具備 40-bit 及 104-bit 兩種金鑰長度，較長的金鑰長度也就代表著較強壯的保護。由於 WEP 只使用簡單的串流加密方式及互斥或演算法(XOR)，即使是 WPA，就現今的電腦系統而言，並不會浪費太多的電腦資源及運算時間。要注意的是，某些設備會提供 128-bit 長度的金鑰加密方式，使用這種加密方式時，會造成與其他設備的不相容。

控制重置功能

重置功能會造成一個嚴重的問題，它可以將管理者所做的任何安全設定全部取消，也就是回復到出廠時的原廠設定。如果回復到出廠的設定，AP 通常就沒有具備任何密碼(或使用該廠商的預設密碼)，或是具備任何的保密措施。有心人士通常只要用一根針或一支筆就可以按下設備背面的重置按鈕，就可以取消設備原本的 IP 設定，金鑰等等。因此最好具備 AP 的實體保護，將它束之高閣或是將重置按鈕封死等等，以減少威脅性。

使用 MAC 位址存取控制清單(ACL)功能

在網路上，每一張網路卡上具備唯一的 MAC 位址，管理者可以透過 MAC 位址來確認不同的電腦設備。有許多的無線網路設備都具備 MAC 位址存取控制清單的功能，透過一個 MAC 位址表格來允許或拒絕某一個 MAC 位址通過該設備。不過這樣的做法並不十分安全，由於 MAC 位址在無線網路傳輸的時候是以明碼的方式在空氣中傳遞，駭客可以輕易地擷取合法電腦的 MAC 位址，並且假造該位址。另外某些設備只能記錄固定數量的位址，這樣的設備就無法適用於中大型企業中。

改變預設的 SSID 值

無線網路設備的 SSID 值在出廠時通常是使用某個預設值或是該廠牌的名稱，這會使得有心人士輕易地就猜出 SSID 值。因此，改變預設的 SSID 值是必要的。雖然級數較高的駭客還是有可能從無線網路封包得知 SSID 的值，但是至少可以防止一般的駭客輕易的進入您的網路。

關閉 SSID 廣播功能

SSID 是無線網路中的一個識別名稱，大部分都會把它命名為網路名稱或是給一個簡單的代號。想要加入無線網路客戶端，只要提供正確的 SSID 名稱便可加入網路。SSID 是一個 0-32 位元組的值，0 則是代表廣播的意思，如果客戶端發出一個 0 位元組 SSID 值的偵測要求(probe request)封包，收到封包的 AP 則會回應自己的資訊包含 SSID 值。在某些廠牌的無線網路設備上具備關閉 SSID 廣播功能，開啟之後 AP 則會忽略該要求封包，這樣可以避免洩露自己的 SSID 值。

改變預設的加密金鑰值

某些無線網路設備在出廠時會使用預設的加密金鑰值，如果啟動了 WEP 或 WPA 的加密方式，或是卻沒有變更加密金鑰，有心人士一樣可以進入加密的網路中。所以無論您使用哪一種加密方式，記得改變預設的加密金鑰值。

使用 SNMP

部分的無線網路設備內建 SNMP Agent 的功能，可以讓網管軟體得知設備的狀態。前兩個版本的 SNMPv1 及 SNMPv2 只提供簡單的認證功能，而且是明碼的方式，這樣是不夠安全的。SNMPv3 則提供了一個較強化的認證方式。建議使用 v3 來代表 v1 及 v2，如果 SNMP

不是必要的，則建議關閉 SNMP 功能。另外，SNMP 的預設名稱通常是 public，有些設備甚至同時具備 read 和 write 的權限，記得變更預設名稱的值以及適當的設定讀和寫的權限。

改變預設的無線電波頻道

建議不要使用無線網路設備所提供的預設電波頻道。如果兩台無線設備在同一個電波範圍之內，使用同一個頻道，則會造成阻絕服務的攻擊。管理者必須事先做好現地勘查，確認無線網路設備的位置、電波含蓋範圍，以避免兩台設備使用同一個頻道。

關閉 DHCP 功能

DHCP 可以讓客戶端設備在上線時自動取得一個動態地網路 IP 位址。如果可行的話，將所有的設備設成固定 IP 位址，如此一來有心在上線後也無法自動的加入網路。

7.1.2. 在密碼方面

如何選用一個合適的密碼以及在選用密碼後如何保持與運用它都是很重的課題，以下針對如何選用以及維護密碼做些建議：

使用複雜的密碼

即使使用最安全的硬體或軟體系統，如果沒有一個複雜的密碼來保護資料，或是因為使用者的偷懶採用了預設的密碼，那麼再安全的密碼系統都是沒有用的。

讓密碼變得複雜

以下的方法可讓密碼變得複雜：

- **密碼愈長愈好。最好使用 7-8 個字元以上長度的密碼，因為長的密碼絕對比短的密碼更加地難以猜測。**
- **不要使用字典內找得到的字。這樣可以防止有心人士使用字典內的每一個字去嘗試密碼。**
- **使用大小寫組合而成的密碼。這樣可以避免密碼被輕易地猜測到。**
- **最少使用一個數字及一個字元當成密碼的一部分。例如不要全部使用數字來當成密碼，都是數字的組合要比文字數字的組合好猜。**
- **不要使用容易被猜到密碼，例如使用自己的相關資訊當成密碼的一部分。舉例來說，「john1966」這種名字加上生日年份就是一個不好的密碼。**

選用一個記得住的密碼

一個很複雜的密碼雖然很難破解，但是卻也增加了記憶的難度。切記千萬不能妥協！有一個小技巧，可以使用一個片語中每一個字的第一個字元來當成密碼，如此一來就比較容易記憶密碼，同時也可以是一個難以破解的複雜密碼。例如「My name is Andy, I am 20 years old.」就可以把「MniAIa20yo」當成一個很好的密碼。如果再將大小寫轉換，也是另一個很好的密碼。

好好地保護您的密碼

當您選用了一個良好的密碼後，切記要好好地保護它，底下是一些保護密碼的常識：

- 只有自己能知道，千萬不要告訴他人。
- 不要寫在任何地方。如果真的怕忘記而必須寫下來時，千萬不要把密碼寫在任何顯而易見的地方，諸如螢幕上、黑板上等等。
- 不要跟他人共享同一組密碼。如果因為工作或其他需要而必須共享同一組密碼，請記得之後一定要馬上變更密碼。
- 每幾個月便改變一次密碼。
- 為每一個敏感性的資料建立一組密碼。例如不要把所有的銀行帳號或所有的電子郵件信箱設成同一組密碼。

7.1.3. 其他的安全性建議

使用 WEP 功能

若無線 AP 設備中不使用任何的安全設定，表示所有的網路封包均是以明文的方式在空氣中傳輸，建議使用 WEP 加密方式，可提供固定等級的安全性。

使用 WPA 功能

WPA 加強了 WEP 的加密方式，若是設備具備 WPA 功能，則建議開啟 WPA 功能。

無線入侵偵測系統套件

定時使用入侵偵測系統套件，以偵測網路中是否存在非法 AP。

虛擬私人網路(Virtual Private Network，簡稱 VPN)

運用 VPN 技術可以在無線網路中建立一個安全且保密的傳輸通道。

7.2. SPIDER LAN 建議方案

由於無網線路的便利性與機動性，在各型企業中已經顯得愈形重要。基於安全的問題，企業內部的網路會管制所有的設備，許多企業在有線網路上會使用 MAC 過濾器的功能，以防止未經管制的電腦設備可以存取網路。本篇論文將這樣的概念套用在企業內部的無線網路上，透過上層的路由器或是交換器設備來管制非法 AP(Rogue AP)。

7.2.1. 已知問題

對於建置無線網路的企業而言，只會將 AP 配佈在合理的範圍，並且希望可以管制這些 AP，只能讓合法的使用者上線。由於無線網路設備的價格已經愈來愈便宜，部分使用者可以很容易地購買 AP 自行接上企業內部的網路，這些 AP 就會將企業內部的網路含蓋範圍延伸到管理人員管轄範圍以外的區域，使得有心人士可能在餐廳甚至停車場就可以直接使用無線網路，這是一個很嚴重的問題。為了防止這樣的情形發生，目前市面上已經有許多的無線網路的偵測設備，管理者可以透過這些設備定時地在企業內部偵測是否有員工私接非法 AP；另外，市面上也有昂貴的偵測套件，可以配佈偵測器於適當的位置，只要發現非法 AP 即回報管理者。不過第一種方式需要管理者定時用走路的方式來管理，無法做到即時的偵測，對於大型企業而言，也顯得費日曠時；而第二種方式則是需要花費大筆的建置費用於軟、硬體設備上。

在無線客戶端設備的管理上，許多管理者會開啟 AP 上的 MAC 過濾器功能，藉以管制公司的合法無線客戶端設備，如果 AP 的數量龐大，則必須為每台 AP 加入同一個客戶端設備的網卡位址，再假設面臨公司設備的定時汰換，管理者更是捉襟見肘、疲於奔命。因此管理者可能會將 MAC 過濾器的功能提昇至上層主要交換器來做，這麼一來有

可能會降低交換器的速度。

7.2.2. 解決方案

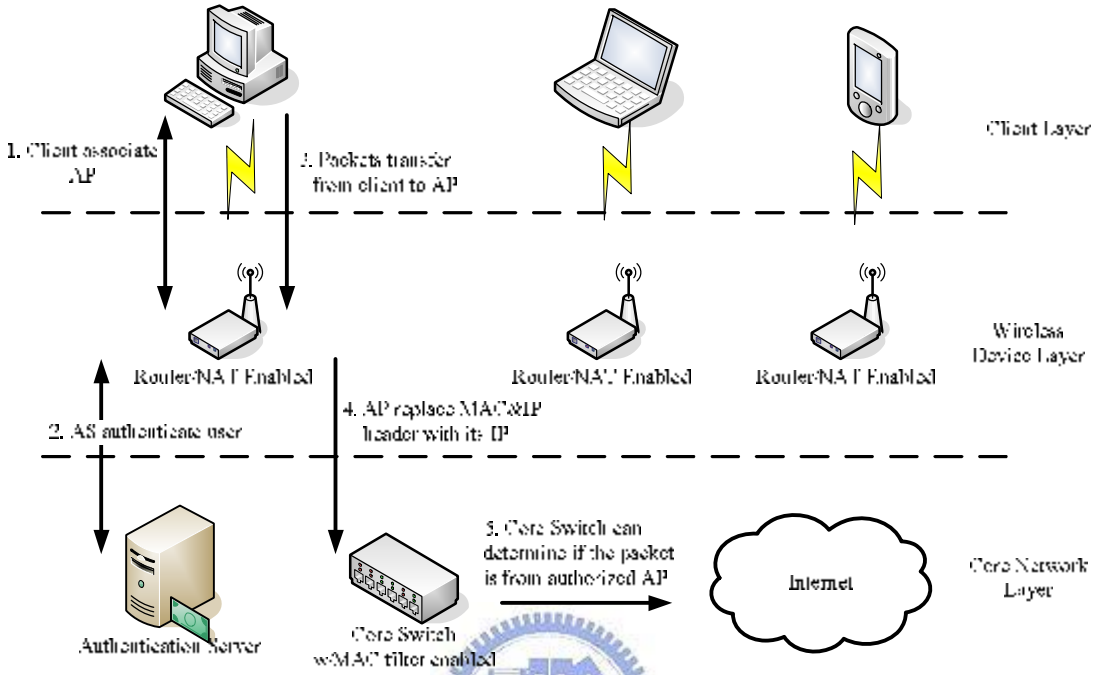


圖 24 SPIDER LAN 架構圖

在本篇論文中則提出了一個可以平衡上述兩大問題的建議方案，SPIDER LAN。我們將企業內部的網路環境區分為三大部分，在客戶端層的部分必須夠做到使用者管理的功能；在無線網路設備層必須能夠防止非法 AP 私接上線；而主網路層則代表企業內部的主要網路部分。企業內部網路必須具備下列三個條件：

- **必須開啟 AP 的路由路模式。**
- **必須開啟上層主要交換器的 MAC 過濾器功能。**
- **必須建置認證伺服器。**

目前市面上的 AP 均具備路由器模式或 NAT(Network Address Translation)功能。但是某些廠牌的 AP 只支援 NAT 模式，甚至無法變更其私有網路的設定。SPIDER LAN 的方式是將 AP 開啟路由器模式或 NAT 模式，則所有的網路封包通過 AP 後，會轉換成 AP 對外連線。另外我們將 MAC 過濾器的功能移至上層主要交換器中開啟，但是為避

免主要的交換器的效率降低，所以交換器中只允許 AP 的 MAC 位址通過。但是如果不管制客戶端設備的 MAC 或 IP 位址，可能會造成駭客經由合法 AP 進入網路，因此我們必須在網路中增加一台認證伺服器，再將 AP 的 802.1x 認證功能開啟，要求所有客戶端設備必須經過認證後始能上網。整個 SPIDER LAN 的架構圖與流程如圖 24，說明如下:

1. 客戶端與 AP 建立關聯，並由 AP 端發起 802.1x 認證要求。
2. 後端伺服器認證是否為合法使用者，若不是，則使用者無法上線；若是，則繼續進行第三步驟。
3. 客戶端設備送出封包到 AP，AP 將封包的 MAC Header 及 IP Header 改為 AP 的位址。再傳送至上層的主要交換器。
4. 主要交換器即可透過 MAC Address 驗證該封包是否來自合法 AP。
5. 來自合法 AP 的封包經由主要交換器向外連接網際網路。

另外管理者也可以額外增加憑證伺服器來加強使用者的認證方式，或是使用主要交換器中的 VLAN 功能來區隔有線網路與無線網路，也可以選擇使用 DHCP 來簡化 IP 管理的複雜度。因此下列三點做法是 SPIDER LAN 的選擇性方案：

- **新增認證伺服器。**
- **使用上層主要交換器的 VLAN 功能。**
- **開啟 DHCP 功能。**

上述各點做法分別說明如下：

開啟 AP 的路由器模式(NAT 模式)

在路由器模式下，客戶端設備必須設定 AP 為其閘道器，所有對外的封包會先傳送至路由器後再轉發出去，因此轉發出去的封包其 MAC

標頭則會是路由器自己的 MAC 位址，我們可以透過 MAC 位址來驗證封包是否由合法 AP 傳送出來；而 NAT 也是一種路由器模式最主要的目的是用來節省 IP 位址，透過 NAT 閘道器可以分配許多的私有的 IP 位址給內部使用者，讓內部使用者在對外連線時經過 NAT 閘道器把內部的私有 IP 位址取代成 NAT 對外的合法位址。透過 NAT 功能，傳送出去的封包其 MAC 標頭也會是 NAT 閘道器自己的 MAC 位址。使用 NAT 轉址功能也可以提供另一個層面的保護，以防止駭客直接從網際網路連線到企業內網路的電腦。NAT 把所有電腦的 IP 位址都隱藏起來，網際網路的使用者只能看到閘道器的外部 IP 位址，而無法得知內部電腦的 IP 位址或電腦數量。

開啟上層主要交換器的 MAC 過濾器功能

在本建議方案中，所有的 AP 均需開啟 NAT 功能，並在上層的主要交換器中開啟 MAC 過濾器的功能，設定成只能讓這些合法 AP 的 MAC 位址通過。

對於私接的非法 AP 而言，分成以下兩點來探討：

l 橋接器模式：

無論合法或是非法的無線客戶端設備，在上層交要交換器中均無記錄客戶端的 MAC 位址，所以使用者即使連上 AP 也無法對外連線。

l 路由器模式

即使非法 AP 擁有合法的 IP 位址，由於上層交換器中並沒有記錄該非法 AP 的 MAC 位址，所有經由非法 AP 的合法及非法客戶端均無法上線。

如果選擇了 IP 過濾器而非 MAC 過濾器的話，有心人士只要得知企業內部的合法 IP 位址並且開啟 AP 的 NAT 模式，則無法有效防止非

法私接企業網路。因此，綜合以上各點，開啟上層主要交換器的 MAC 過濾器功能，可以讓非法 AP 私接網路時造成無法連線的狀況，就可以防止駭客藉由無線網路入侵企業內部的網路，如圖 25。

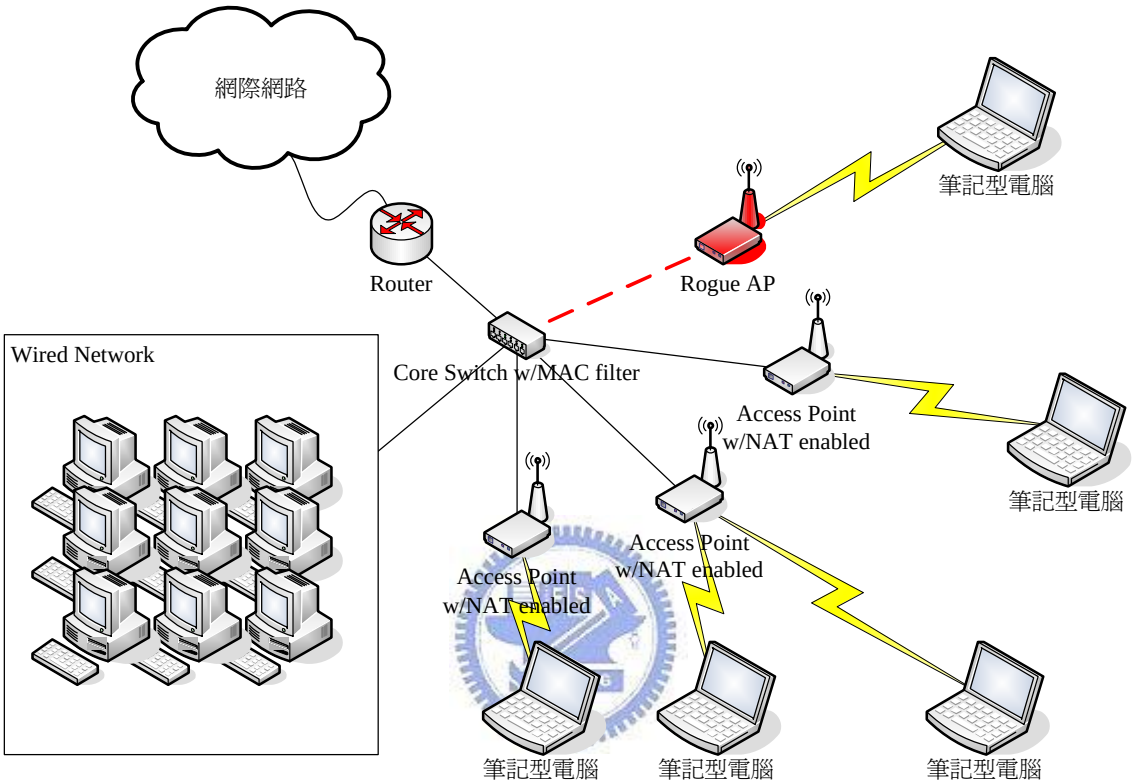


圖 25 開啟上層主交換器 MAC 過濾器，並開啟 AP 的 NAT 模式

建置認證伺服器

在本節一開始曾經提到，本建議方案必須防止沒有授權的無線網路客戶端進入企業內部的網路。如果只將 AP 開啟路由器或 NAT 模式，並且在上層主要交換器中加入 MAC 過濾器功能後，並無法防止駭客進入無線網路。因此駭客只要在無線網路的含蓋範圍之內，就可以連上網路。因此，我們建議企業內部也必須建置一認證伺服器，另外 AP 也必須具備 802.1x 的認證功能。所有欲上線的使用者都必須提供合法的使用者名稱及密碼甚至憑證，才能進入無線網路。架構圖如圖 26。

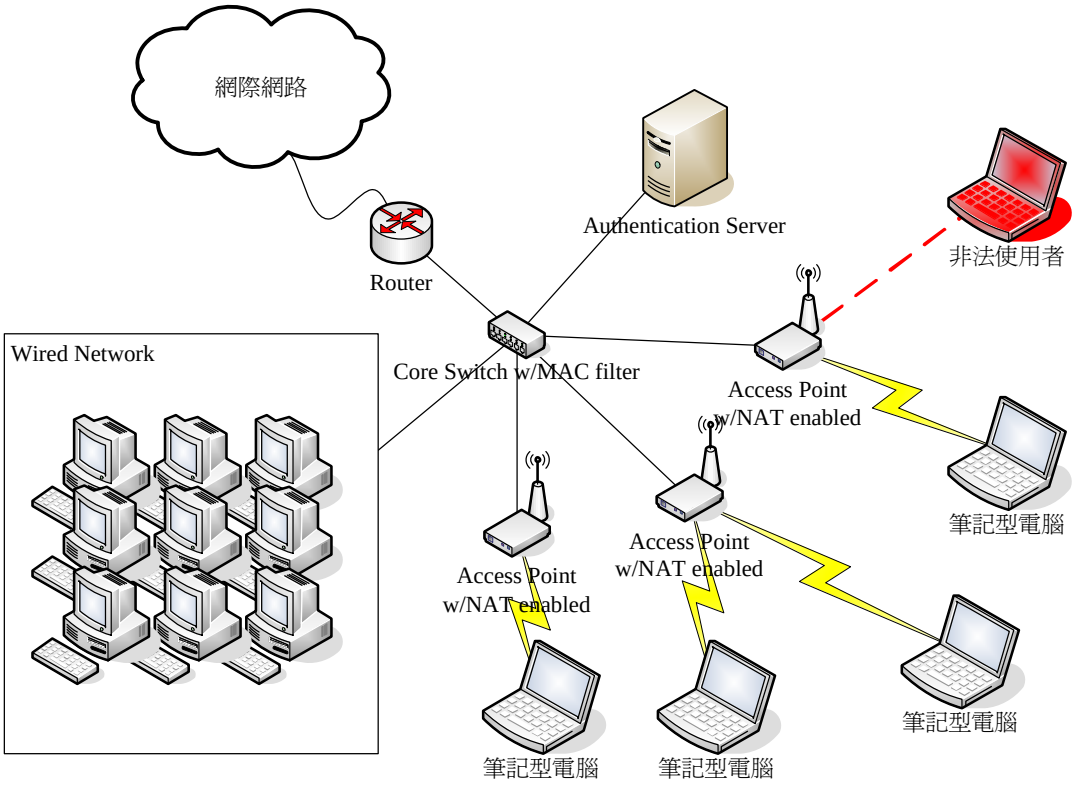


圖 26 非法無線網路使用者無法認證通過

上述三項功能是本建議方案中所必須具備的，管理者可以選擇建立其他的基礎建設以提供更安全的防護。分別介紹如下：

建置憑證伺服器

使用憑證伺服器結合 802.1x 之 EAP-TLS 或 PEAP 的認證協定，透過憑證伺服器簽發企業內部的憑證給使用者，可以強化原本的名稱/密碼認證功能。

使用 VLAN

主要交換器幾乎都會內建 VLAN 功能，VLAN 的作用是將同一台交換器中的不同連接埠或設備切割成各別的廣播區域(Broadcasting Domain)，可以有效地區隔不同 VLAN 的廣播封包。現在的有線網路環境中，一個連接埠都連接一台電腦設備，對於廣播封包的攻擊，只要找出交換器中的最大流量連接埠將之關閉，可以暫時解決威脅。由

於駭客可能在無線網路上發起廣播封包攻擊，如果將最大流量的 AP 斷線，恐會影響其他使用者的正常使用，所以短時間內較難找出攻擊者所在。如果企業內部的所有網路皆在同一個廣播區域內，無線網路的廣播攻擊則會影響到有線網路的使用，所以管理者可以將無線網路所銜接之有線網路區段使用 VLAN 將之隔離，可以區隔有線網路與無線網路使用者的網路封包。

使用 DHCP 功能

如 7.1.1 中提到的，DHCP 有可能會造成駭客輕易得知企業內部的 IP 配置情形。由於我們已經在內部建置了認證伺服器，除非駭客得知密碼或憑證，才有可能進入網路。因此我們可以選擇使用 DHCP 功能來減少 IP 管理的複雜度。

7.3. SPIDER LAN 總結

由於無線網路設備在價格上的普及化，使得人人都可以買到一台便宜的無線設備。在企業內部對於非法 AP 的管理，是管理者一個很頭痛的問題。另外，管理者也希望可以管制合法的使用者才能上線，以往的做法可能會在 AP 上開啟 MAC 過濾器的功能來管制設備，對於數量龐大的 AP 而言，在管理上增加了許多複雜度。本建議方案透過一個簡單又有效的方式來解決上述的問題。首先使用上層交換器的 MAC 過濾器來管制非法 AP，並且利用認證伺服器來加強人員及設備的管理。

由於企業內部網路環境通常會具備主要交換器，現今的主要交換器也幾乎都內建 MAC 過濾器的功能，因此透過 SPIDER LAN 的方式，企業無需再建置其他的軟硬體設備，即可提供更安全的網路環境。

第八章　結論與未來展望(Conclusion and Future Work)

8.1. 結論

自 IEEE 於 1999 年公佈 802.11a/b 無線網路以來，無線網路建置已經愈來愈普及，硬體的價格也愈來愈便宜，不管是企業甚至是家庭使用者幾乎都可以使用到無線網路的好處。雖然無線網路有其便利性，但是其中的安全問題也不容乎視。本篇論文針對所有無線網路的安全議題做一深入性的研究與探討，並比較現行市場上各家廠商的獨家規格與做法，冀能對無線網路有興趣的研究者做一些貢獻。

另外，在本篇論文中，我們也提出了一個 Simple Proposal for Intrusion Defense in Enterprises wiReless LAN (SPIDER LAN)建議書，對於各型企業在無線網路時，可以有效的管制非法 AP 及合理的管制企業內部的無線客戶端設備。

8.2. 未來展望

本篇論文所提的 SPIDER LAN 建議方案中，雖然可以有效地防止非法 AP 及管理合法的使用者，但是假設非法 AP 假造了合法的 MAC 位址，會造成合法 AP 的 DoS(Denial-of-Service)攻擊，也就會使得無線網路客戶端無法對外連線。這值得我們後續研究以解決 MAC 假造的問題。

參考文獻(References)

[1] *IEEE Std 802.11b-1999: Part11:* Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Authentication and privacy.

[2] *IEEE Std 802.11a-1999: Part11:* Wireless LAN medium access control (MAC) and physical layer (PHY) specifications..

[3] N. Borison, I.Godberg and D.Wangner, “Intercepting mobile communications: The insecurity of 802.11”. http://www.isaac.cs.berkeley.edu/Isaac/wep-draft.pdf.

[4] S.Fluhrer, I.Mantin and A.Shamir “Weaknesses in the key scheduling algorithm of RC4”. Eighth AnnualWorkshop on Selected Areas in Cryptography (August 2001).

[5] Adam Stubblefield, John Ioannidis, Aviel D. Rubin. “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, AT&T Labs Technical Report *TD-4ZCPZZ, 2001*.

[6] Matthew Gast. 802.11 Wireless Networks: The Definitive Guide. *O'Reilly & Associates, Inc.*, Sebastopol, CA, 2002

[7] Wi-Fi Alliance, "http://www.wi-fi.org/OpenSection/protected_access.asp".

[8] *IEEE Std 802.3-2002: Part3:* Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

[9] Institute of Electrical and Electronics Engineers, "http://www.ieee.org".

[10] Wi-Fi Alliance, "http://www.wi-fi.org".

[11] InterOperability of University of New Hampshire, "http://www.iol.unh.edu/".

[12] Wireless LAN Association, "http://www.wlana.org".

[13] OFDM Forum, "http://www.ofdm-forum.com".

[14] *IEEE Std 802.11-1999: Part11:* Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.

[15] Nikita Borisov, Ian Goldberg, David Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”, California at Berkeley, September 2001.

[16] Scott Fluhrer, Itsik Mantin, and Adi Shamir, “Weakness in the Key Scheduling Algorithm of RC4”.

[17] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", March 2001.

[18] *IEEE Std 802.11i-2004:* Wireless LAN medium access control (MAC) and physical layer (PHY) specifications.

[19] Alan O. Freier, Philip Karlton, Paul C. Kocher, “The SSL Protocol Version 3.0”, Internet Engineering Task Force, Internet-Draft, 1996.

[20] L.Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocl(EAP)." *IETF RFC2284, RFC3748*, March 1998.

[21] W. Simpson, Ed., "The Point-to-Point Protocol", *IETF RFC1661*, July 1994.

[22] *IEEE Std 802.1x-2001:* Port-Based Network Access Control.

[23] FIPS Publication 197, Advanced Encryption Standard (AES)” U.S. DoC/NIST, November 26, 2001.

[24] Rijndael web site, “http://www.esat.kuleuven.ac.be/~rijmen/rijndael/”.

[25] National Instidute of Standards and Technology AES Standard web page, "http://csrc.nist.gov/CryptoToolkit/aes/”.

[26] Ashwin Palekar, Dan Simon, Joe Salowey, Hao Zhou Glen Zorn, S. Josefsson, “Protected EAP Protocol (PEAP) Version 2”, Internet-Draft, Internet Engineering Task Force EAP Working Group, July 2004.

[27] Manuel Perez, Miguel Sanchez and Roman Garcia, "Secure Wireless Access to a Campus Network", Polytechnical Universary.

[28] 國立中正大學電算中心, “http://wireless.ccu.edu.tw/structure.html”.

[29] 曾左旭, Linux 平台存取點與 IPSec 橋接器之研究, 淡江大學電機工程學系 91 學年度碩士論文。.

[30] SonicWALL, Inc. “WiFiSec vs. WPA”, http://www.sonicwall.com/services/pdfs/WiFiSec_vs_WPA.pdf, Nov 15, 2003

[31] SonicWALL Inc., "http://www.sonicwall.com".

[32] Welch, D.; Lathrop, S., "Wireless Security Threat Taxonomy"; Information Assurance Workshop, 2003. *IEEE Systems, Man and Cybernetics Society , 18-20* June 2003, Pages:76 - 83 .

[33] Branch, J.W.; Petroni, N.L.; Van Doorn, L.; Safford, D., "Automonic 802.11 Wireless LAN Security Auditing”; *Security & Privacy Magazine, IEEE , Volume: 02 , Issue: 3* , May 2004, Pages:56 - 65.

[34] Gregory Rehm, “802.11b Homebrew WiFi Antenna Shootout”, http://www.turnpoint.net/wireless/has.html, February 2002.

[35] The Shmoo Group Airsnort web page, "http://airsnort.shmoo.com".

[36] SourceForge WEBCrack Project, "http://sourceforge.net/projects/wepcrack/".

[37] Kismet web site, "http://www.kismetwireless.net".

[38] AirDefense Inc., "http://www.airdefense.net".