# 無線乙太網路通訊協定安全弱點研究
# Study on Wireless LAN Security

中山科學研究院資訊通訊研究所指管通情組
國立交通大學資訊工程學系
NSC91-2623-7-009-012

期末報告

執 行 時 間　：91年01月01日 至 91年12月31日
計畫執行單位　：國立交通大學　資訊工程學系
計畫主持人　　：林一平　教授
計畫共同主持人：蔡文能副教授
日　　期　：中華民國九十一年十二月三十一日

# 目錄

目錄 III

圖目錄 IV

1. 計畫概述 1

2. 無線網路簡介 2

3. 無線網路相關技術 4

3.1. 無線區域網路傳輸技術 4

3.2. 無線區域網路標準 6

3.2.1. IEEE 802 7

3.2.2. IEEE802.11 無線網路標準 8

3.3. CSMA/CA存取控制 11

4. 無線網路通訊協的安全探討 14

4.1. WEP安全協定 14

4.2. WEP安全的弱點 16

4.3. WEP破解 19

4.4. WEP補強 – 802.11i 20

5. 結論 22

參考文獻 24

附錄. 無線網路802.11弱點研究 28

# 圖目錄

Figure 1. 跳頻展頻（Frequency Hopping Spread Spectrum；FHSS）..... 5
Figure 2. 直接序列展頻（Direct Sequence Spread Spectrum）. 6
Figure 3. 直接序列展頻架構的無線設備範例 ..... 10
Figure 4. 隱形端末(Hidden terminal)範例 ..... 12
Figure 5. CSMA/CA 運作機制 ..... 13
Figure 6. WEP key 設定範例 ..... 14
Figure 7. WEP 使用RC4演算法加密解密 ..... 15
Figure 8. 破解WEP所需時間與空間 ..... 18

# 計畫概述

本計畫的主要目的是要研究無線乙太網路通訊協定安全弱點。網際網路(Internet)的蓬勃發展給企業帶來許多商機，給個人帶來了許多便利，因此網路已經成為日常生活不可或缺的一項工具，但它也引來許多新問題、新風險，如非法入侵(Intrusion)、網路攻擊(Attack)、電腦病毒(Computer virus)等等。近年來無線網路價格普及化後發展得特別快，因為透過無線網路可以達到任何時候任何地方(any time, any where)都可以使用網路資源的好處。

在802.11b標準推出後，因為頻寬有11Mbit/sec，無線區域網路產品的市場開始升溫，價格也逐步普及化。國內最大的網路服務業者Hinet 已開始與無線網路業者合作準備提供全省無線網路接取服務。然而無線網路的安全是一個大問題，可能被監聽，也可能被攻擊。在此，我們把意圖癱瘓系統或網路的行為歸類為攻擊，把意圖進入系統竊取資料或進入系統做一些事的歸類為入侵。

無線網路除了也是有有線網路的缺點，而且它是通過公用波段來進行傳輸資訊的，和電視信號、廣播和手機使用的媒介相同，在空中就會被截聽。無線網路中有一個內建的安全功能對傳輸的資料進行加密，就是有線等效保密標準（Wired Equivalent Privacy, WEP），也稱為802.11b網路安全標準。

本計畫的研究重點是無線乙太網路的通訊協定(802.11b)究竟有哪些弱點可能導致安全上的問題。我們已經研究了IEEE802.11相關的文件，並且將在本期末報告中詳細敘述研究成果。

# 無線網路簡介

傳統的乙太網路（Ethernet）使用者的電腦必須有一條網路線連上資訊插座與區域網路相連，而無線網路（Wireless Network）則透過無線電技術取代網路線。無線區域網路（Wireless LAN; WLAN）的發展超已經過十年，但始終未能真正普及，原因不外於成本與效能因素，但隨著技術逐漸成熟，產品價格也日漸下滑，使得無線區域網路開始被用戶接受，市場也開始起飛。

在1971年時，夏威夷大學在無線電上面採用『封包式』技術，在不需要電話公司的電纜線之情形下，將四個夏威夷島嶼連接起來。此一無線電網路被命名為ALOHNET，採用雙向的星狀網路拓樸，整個網路上面共有七台電腦連接。但是隨著網際網路的發展，無線網路的並沒有太大的進展。1991年，為了要振興無線區域網路市場，各個製造商聯合起來決定建立一個標準，一直到1997年，標準組織IEEE發表了802.11，各家廠商才有了一個主要的依循標準，終止了長久以來的紛爭。無線網路只是一個通稱，事實上，在無線領域裡有許多無線網路的工業標準存在，其中最重要的兩個應該屬HomeRF和IEEE 802.11（又稱Wi-Fi）這兩大派系。其中，802.11獲得比較多的廠商支援。事實上，IEEE 802.11b之所以迅速席捲全球無線區域網路市場主要是廠商促進產品相容性與成立推動組織推廣所致。在1999年8月，3Com、Aironet、Intersil、Lucent、Nokia與Symbol共同發起成立WECA( Wireless Ethernet Compability Alliance），致力於教育與推廣IEEE 802.11b無線區域網路應用、協助解決產品相容問題，並且研擬WiFi（Wireless Fidelity）互通標準。

無線區域網路依其連接運作方式可分為兩種：Ad-Hoc LAN(隨意連)和Infrastructured WLAN (有基礎架構的無線網路)，分述如下。

- Ad-Hoc WLAN：

  數個可攜帶式節點（例如：筆記型電腦），同處於一個小區域，彼此以點對點（peer-to-peer）方式通訊，而不必透過有線或無線主幹的輔助。

- Infrastructured WLAN：

  包含有線或無線主幹（backbone），網路交通可分為兩種： uplink（station 到 backbone）及 downlink（backbone 到 station），通往 backbone 的接點稱之為存取點(Access Point)，Access Point 可以是有線主幹或無線橋接的基地台(base station)。

簡單說來，無線區域網路是由兩個基本元件構成：存取點(access point)和用戶端介面卡。存取點有多樣式的產品設計，其角色是當成一個無線網路中心點，或是有線和無線網路之間的一個連接點，多重存取點可以部署在大樓或重要網路存取地點，讓配備WLAN介面卡的使用者能自由地在區域內移動並保持與網路之間的持續連接性。透過WLAN，任何建築物中一組與無線存取接點串連的配線裝置，皆可為配備有WLAN 介面卡的PC提供網路存取點服務，這種配置模式能突破佈線架構的位置限制，將PC資源的運用效率發揮到極致，例如筆記型電腦在此環境中，可移至任何地點使用。

# 無線網路相關技術

## 1.1. 無線區域網路傳輸技術

無線區域網路（Wireless LAN; WLAN）傳輸技術大約可分為三種：

- **微波（Microwave）**：主要用於大樓間LAN網路 連接，這須要使用到碟形天線，且天線必需位於 視線範圍(Line-of-sight)。

- **紅外線（Infrared ray）**：使用紅外線傳送資料，又可分為兩種：a.散射式（Difused）紅外線，一種非直線式傳輸方式，只要在一定區域內，可介藉由物體表面反射方式，達到傳送資料目的。b.直射式（Directed）紅外線，以直線型態傳輸資料，若途中遇到任何障礙，接收端將無法收到資料，因此網路環境必須在視線範圍（Line-of-sight）。

- **展頻（Spread Spectrum）**：為目前無線區域網路使用最廣的傳輸技術，1940年代二次世界大戰時期，美軍將無線電加上編碼技術加密後使用在軍事通訊上面，用以避免信號的擁擠與被監聽，此即所謂展頻技術(Spread Spectrum)。

1997年，標準組織IEEE發表了802.11，規定以跳頻展頻（Frequency Hopping Spread Spectrum；FHSS）、直接序列展頻（Direct Sequence Spread Spectrum；DSSS）或紅外線傳輸等技術來實作 2.4

GHz 頻帶中 1 至 2Mbps 之數據傳輸。

展頻技術又可分為兩種：(1) 跳頻展頻(Frequency Hopping Spread Spectrum；FHSS)。就是把信號透過切割成許多頻道的一系列頻率範圍廣播出去，傳送裝置會先去傾聽（listens）頻道（channel），當此頻道處於閒置狀態，信號會利用此頻道傳送出去，若此頻道已經在使用，傳送端便會跳躍（hops）到另一個頻道，因此接收端必須知道傳送端的跳躍程序，且傳送端與接收端必須同步切換頻道才可正常收送資料。(2) 直接序列展頻(Direct Sequence Spread Spectrum；DSSS)，簡稱直序展頻。所謂「直序展頻」是將原來1個位元(bit)的訊號，加入多餘資料位元，這些資料稱為"chips"，每一位元必須加入至少10個chips，使得原來高功率、窄頻率的訊號，變成低功率、寬頻率。

跳頻展頻和直接序列展頻兩種技術分別如以下二圖所示：

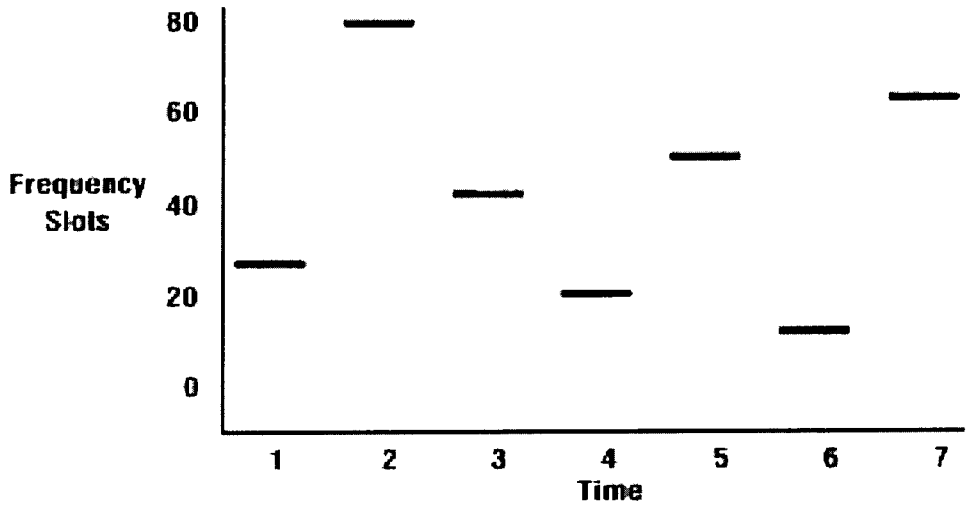
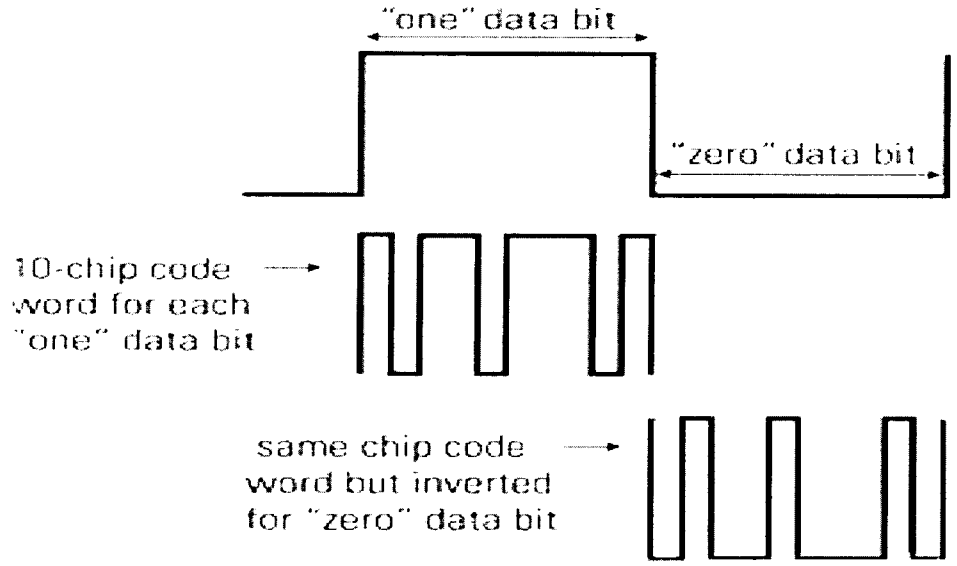



Figure 1.　跳頻展頻（Frequency Hopping Spread Spectrum；FHSS）

Figure 2.　直接序列展頻（Direct Sequence Spread Spectrum）




但是1997年IEEE802.11這個標準還是很慢（每秒2 Mbits），此時大部份的業者對WLAN仍興趣缺缺，主因是IC零組件成本太高，普及化不易；再者2Mbps的速度，和當時有線區域網路主流邁入100Mbps的Fast Ethernet，相差太大，更使企業界深覺此昂貴的投資沒有太大的價值。直到1999年9月IEEE 802.11 Task Group b確定了IEEE 802.11b標準，以直序展頻(又稱DSSS；Direct Sequence Spread Spectrum)做為調變技術，傳送速率可達每秒11Mega bits的實用範圍，無線區域網路又開始廣被重視。

## 1.2. 無線區域網路標準

## 1.2.1. IEEE 802

IEEE 802為「電機電子工程師協會(Institute of Electrical and Electronic Engineers，IEEE)」所推動的標準，此標準是定義區域網路中的第一層實體層(physical layer) 及第二層資料連結層(data-link layer) 在網路上的存取控制。簡單的說，IEEE802所定義的標準，就是網路上資料存取的方法(Access Method)，在網路上，所謂的存取方法是指如何將資料放在纜線上傳輸、如何從纜線上取得資料的規定。

常見的 IEEE 802 規範有下列各種：

802.1 → 高層介面、網路互連
802.2 → 邏輯鏈結控制 (LLC)
802.3 → CSMA/CD 乙太網路(Carrier-Sense Multiple Access with Collision Detection)網路
802.4 → 權杖匯流排 (Token bus) 網路，也有人稱記號匯流排網路
802.5 → 權杖環 (Token ring) 網路，也有人稱記號環網路
802.6 → 都會網路 (MAN，Metropolitan Area Network)
802.7 → 寬頻區域網路 (Broadband LAN)
802.8 → 光纖區域網路 (Fiber Optic LAN)
802.9 → 多媒體傳輸 (Multimedia traffic)，整合聲音與網路資料
802.10→ 網路保全 (Security)
**802.11→ 無線網路 (Wireless Network)**
802.12→ 需求優先存取區域網路 (100BaseVG-AnyLAN)

其中802.3就是我們熟悉的有線乙太網路(Ethernet)，802.11則規範了與有線乙太網路相容的無線網路(Wireless Network)。

## 1.2.2. IEEE802.11 無線網路標準

自從 1997 年無線區域網路 IEEE 802.11 確立之後，原本各自為政的無線區域網路產品，才有了藉以連通的標準，因此自 1997 年後無線區域網路的發展才逐漸看到產值及產量。曾經熱門的藍芽（bluetooth），HomeRF 等等，都是在 IEEE 802.11 的標準下衍生出來的。IEEE 在 1997 年公布了相關的標準----輸出功率為 1W，天線增益至少 6db。並以跳頻展頻（Frequency Hopping Spread Spectrum；FHSS）、直接序列展頻（Direct Sequence Spread Spectrum；DSSS）或紅外線傳輸等技術來從事 2.4 GHz 頻帶中 1 至 2Mbps 之數據傳輸，該標準並可支援同步及非同步之語音、數據傳輸。1999 年 9 月 IEEE802.11 的 Task group b 完成制定源自 IEEE 802.11 直接序列展頻技術且別名 IEEE 802.11 HR（High Rate）的 IEEE 802.11b 標準，每秒傳輸速率可達 11Mbits。隨後，Task group a 也完成了奠基於跳頻展頻(FHSS)技術的 IEEE 802.11a 的標準，傳輸速率可達每秒 54Mbits。在 2001 年 11 月 IEEE 通過了 IEEE 802.11g 暫定標準，傳輸速率也可達每秒 54Mbits，且使用與 802.11b 相同的頻段。預計會在 2002 年底或是 2003 年初正式通過 802.11g 標準。

在標準規範方面，802.11b 標準和 802.11g 的頻率是 2.4GHz，但實際上是在 2412～2484MHz 的 14 個頻道，每個頻道間隔 5MHz，但每個頻道使用 22MHz。美國用前 11 個，歐洲用前 13 個，最後一個

頻道只有日本使用。而 5GHz 的 802.11a 在 5.15～5.35MHz 間有 8 個頻道，5.725～5.825 有 4 個頻道。

在頻道選擇方面，802.11b有3個non-overlapping，北美(唯一選擇是頻道1, 6, 11)與歐洲略有不同；802.11a的頻道間距為20MHz，值得注意的是5.15～5.35GHz一開始的頻道間距為30MHz，與5.725～5.825GHz保持20MHz有所不同。

IEEE802.11b的傳輸速度依調變方式分為1Mbps（BPSK）、2Mbps（QPSK）、5.5Mbps與11Mbps（CCK）四種。802.11a的調變方式是採用OFDM，而802.11g的調變方式，可以有OFDM或PBCC的方式。兩者都是採用資料傳送高速化的調變技術－OFDM。雖然是相同的調變技術，然而802.11 a/g的頻帶也有所差異，因此兩者之間是不可以相互連接的。

OFDM-Orthogonal Frequency Division Multiplexing，有人譯為「正交頻率分割多重」。這種調變技術的最大特徵，是使用了多數個副載波(Sub-Carrier)的方法。以下是依然使用2.4Ghz頻帶之802.11g所使用的調變方式。

- BPSK - 1Mbps, 6Mbps, 9Mbps
- QPSK - 2Mbps, 12Mbps, 18 Mbps
- CCK - 5.5 Mbps, 11Mbps
- PBCC - 22 Mbps, 33 Mbps
- 16-QAM - 24 Mbps, 36 Mbps
- 64-QAM - 48 Mbps, 54 Mbps

802.11g 中有幾個選項(Option)，第一個選項PBCC-Packet Binary Convolutional Coding是德州儀器所提案的調變技術。而更令人眼花撩亂的是，802.11g中所使用的OFDM調變技術，有一些是必須，有一些

卻是選項。主要是以Intersil的提案為基礎，兩者的分隔點就是24Mbps的傳送速率。低於這個速率的部分是隸屬於「必須規格」，高於此則是「選項規格」。

以下將802.11g規格，細分成底下4個項目：

a. 802.11b的必備規格：CCK、QPSK、BPSK/DSSS、FHSS調變技術的通信傳送速度為11Mbps、5.5Mbps、2Mbps、1Mbps。

b. 802.11g的必備規格(即802.11b的高速化)：OFDM調變技術的通信傳送速度為24Mbps、12Mbps、6Mbps。

c. 802.11g的選項規格一(即802.11b的高速化延伸)：PBCC調變技術的通信傳送速度為33Mbps、22Mbps。

d. 802.11g的選項規格二(即是維持802.11a的相同速度)：OFDM調變技術的通信傳送速度為54Mbps、48Mbps、36Mbps、18Mbps、9Mbps。

以下是一個直接序列展頻架構的無線設備範例。

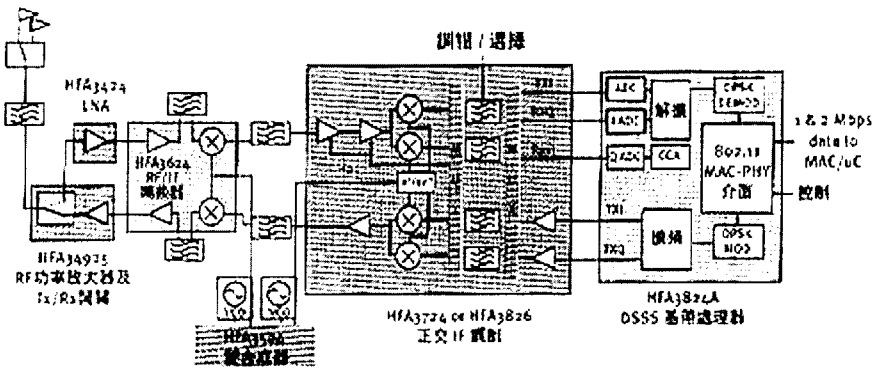



Figure 3.　直接序列展頻架構的無線設備範例

# 1.3. CSMA/CA存取控制

CSMA/CA是802.11無線網路的媒體存取控制(Media Access Control)方式。什麼是Media Access Control？Media就是傳送媒體transmission media，就是看你用什麼來傳東西，如果用Ethernet的話，那條cable就是media，如果用無線電，就是無線電的media。那什麼叫Access Control？就是共用存取控制，比如說無線電，每一個人都發信號出來，訊號撞在一起就變成亂碼，所以同一時間只能一個人用，這種情況下就需要Media Access Control，就是決定誰可以用，誰可以傳資料。Ethernet是怎樣的控制呢？原則上只要沒人講話，我就去抓或去傳，這是多方存取CSMA(Carrier Sense Multiple Access)。那這衍生一個問題，兩個人同時去傳，就是collision，所以CSMA，carrier sense就是去看有沒有人在講話，collision detection等於說去抓的時候，有人同時抓，你可能會相撞。撞到的時候你怎麼辦？在802.3乙太網路的存取控制方式是CSMA/CD - Carrier Sense Multiple Access with Collision Detection。乙太網路的collision是什麼？就是說兩個電腦，同時把資料送出去，那所有的人都可以聽得到，所以兩個電腦，送個信號到同一個電腦去，這個電腦同時接到兩個信號，這叫collision。因為802.3有線網路環境上有許多資料封包 (packet)在線上傳遞，同一條傳輸線路上不可能同時存在兩個封包一起傳送，這個協定定義了碰撞偵測的法則，以定義兩封包碰撞時的解決方式：通常工作站在使用網路之前，會先偵測網路上是否已經有資料傳輸。在802.3乙太網路可以偵測到是否發生collision，但是在無線電，你怎麼樣知道有沒有collision？無線網路對於衝突的檢測(Collision Detection)，有其困難度所在，因此要改用別的方法。

802.11所規定的存取方式，稱做多重存取與碰撞避免(CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance)。利用成功無誤地接收資料後，送一個接收通知資料框(ACK)到傳送端作為確認之用。如果，傳送端送出資料之後，在一定時間之內並未收到確認的信號，就認定資料傳送失敗，稍後再重新再送。這樣子的迴避衝突的機制，以一句話帶過就是「CSMA/CA +ACK」。

此外，還有無線網路還有hidden terminal的問題。在有線網路上如果A看得到B，B看得到C，則A一定看得到C，可是在無線網路則不一定這樣。舉一個在無線網路很有可能發生的案例，假設存在有端末機器甲與端末機器乙，以及一個存取點(Access Point；就是無線基地台)，端末機器甲與存取點可以通信，端末機器乙與存取點也可以通信，偏偏端末機器甲與端末機器乙，兩者之間可能因為電波範圍不足而不能互通，這種狀況往往被稱做「隱形端末」(hidden terminal)的情況。

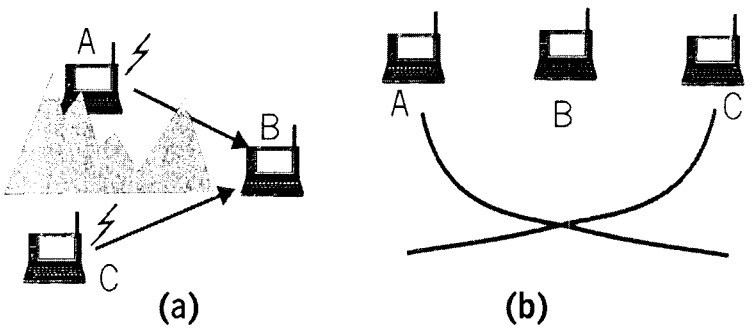



Figure 4.　隱形端末(Hidden terminal)範例

為了要迴避這種問題的發生，遂導入了傳送端與接收端在傳送區域內先行通知以避免collision的手段。方法是端末設備開始通信的時

候，送出一個RTS-Request To Send 資料框給基地台，目的是在等待CTS-Clear To Send的回應，一旦CTS送出，所有其他收到CTS訊號的任何設備就不可以送資料，剛才送出RTS的端末設備必須趕緊在時限內完成資料傳送動作。然而，RTS-CTS的協定目前是選項，目的就是要去感測載波，是否可以探查到。

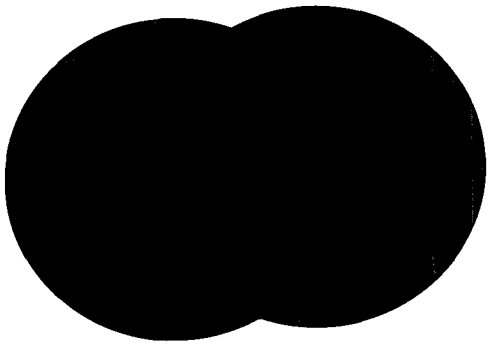


Figure 5. CSMA/CA 運作機制

無線網路帶給人們最大的便利在於增加使用者的移動性(Mobility)。然而，由於無線區域網路無須依靠實體線路而是藉由電磁波在空氣中傳輸資料，因此資料傳輸範圍不若有線網路來的容易掌控。有心者可以在有效傳輸距離內設立監聽設備以竊取任何有用的資料。目前常見的無線區域網路保護措施是 WEP (Wired Equivalent Privacy)。

## 1.4. WEP安全協定

無線網路為了防止竊聽，802.11b標準中規定可以使用WEP(Wired Equivalent Protection)將資料加密(Encryption)處理，必須無線基地台與無線端末設備都啟動WEP機制才有用，例如在使用無線網路卡的電腦上我們必須做與基地台對應的設定：

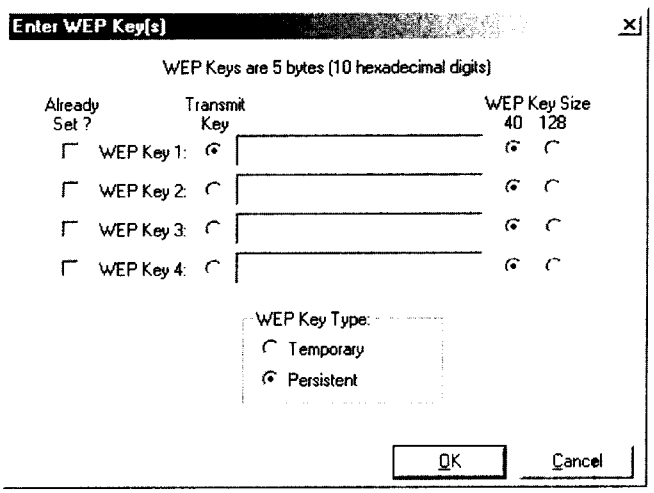



Figure 6. WEP key 設定範例

一般廠商會提供WEP 64bits與WEP 128bits讓使用者選擇，也有廠商甚至提供更多bits的選擇。WEP 64bits 的 Encryption 乃是 IEEE 802.11 的標準規範，事實上是用40bit的key加上24bit的Initial Vector(IV)，合起來成為64bits的亂數種子(seed)，使用RSA公司的RC4演算法，產生一連串的亂數以便與資料做Xor運算後再送出去。

必須注意的是24-bit的IV是沒有加密的，WEP加密解密如下圖：

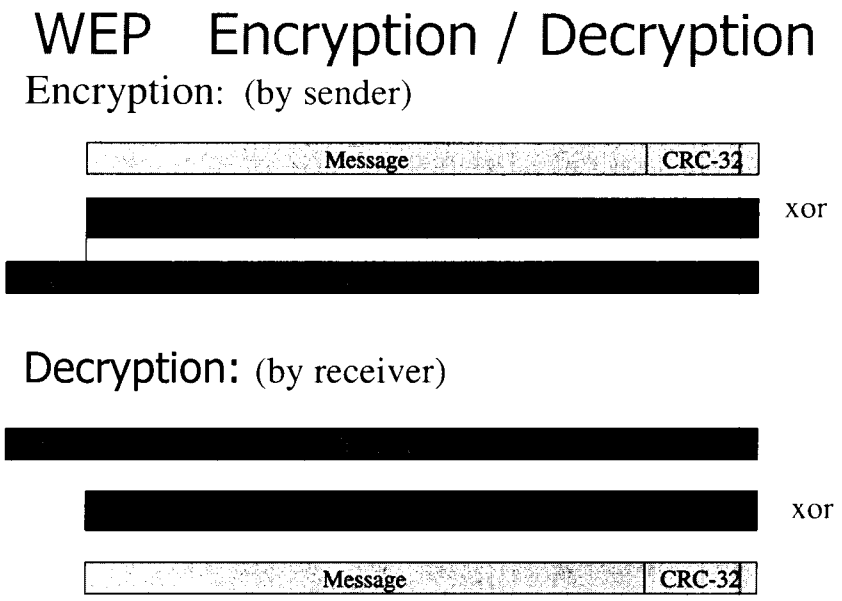



Figure 7. WEP 使用RC4演算法加密解密

WEP 要求傳送端和接收端要選一個共同的秘密金鑰(secret key)做加解密運算。每次當有一個封包(packet)要傳送時，先對明文訊息封包算出 32-bit 的 CRC 檢查和以確保訊息的完整性。並取一個 24-bit

的值作為 IV(Initial Vector;初始向量)，串上 40-bit 成為 64 bits 的 key(或是串上 104-bit 的秘密金鑰成為 128-bit 的 Key)當作亂數的種子，利用 RSA 公司的 RC4 演算法產生一連串的亂數，直到與明文訊息加上明文訊息之 CRC 檢查碼(32 bits)長度為止。然後把這一個亂數串流(stream)與明文串接 CRC 檢查值做 xor(互斥或)運算，所得結果稱之為密文(cipher text)；最後把沒有加密的 IV (24-bit)串接上這個密文串後就傳送出去。

訊息接收端收到封包後，先取下起始的 24-bit 初始向量(IV)，拿來串接上與傳送端約定好的秘密金鑰(Secret key)當作亂數的種子，利用 RSA 公司的 RC4 演算法產生一連串的亂數，把這一個亂數串流與去掉 IV 後的密文做 xor(互斥或)運算，所得結果就是原來的明文和明文的 CRC 檢查碼(32 bits)，此時也可以重新計算 CRC 檢查碼比對。

## 1.5. WEP安全的弱點

目前市售的無線區域網路產品在安全性上均強調利用：一、SSID(Service Set Identifier)，二、WEP(Wired Equivalent Privacy)這兩項功能達到前述企業用戶對無線網路使用者身分認證及資料傳輸之安全性的需求。但事實上是，SSID充其量僅可視為一組密碼，而且其

必須事先設定於所有使用者的無線網卡及AP(Access Point；類似行動電話基地台的無線區域網路設備)中，所有人共用這組密碼，因此較易使密碼洩漏出去，而失去資料存取之認證安全性，系統管理者也無法利用不同的密碼作不同網路存取政策之控管；至於WEP部分，其主要的功能是針對在無線區域網路上傳輸之資料作加密，資料即使被攔截也因加密的關係沒有被破解之虞，但事實上是，資料加密或解密的運算通常需要一組金鑰做為加解密演算之參考值，WEP也不例外，但現今在802.11b標準中，WEP的金鑰與SSID類似，是靜態地存放在所有使用者之無線網卡及AP基地台中，所有人共用這組金鑰，因此同樣地較易使金鑰洩漏出去，而失去資料傳輸之保密性。

在 2001 年 1 月的 Mac-Crypto 研討會上，美國加州大學柏克萊分校的 Nikita Borisov, Ian Goldberg, 和 David Wagner 特別針對無線區域網路通訊協定標準上實作的 WEP 安全機制提出質疑，而發表了一篇文章揭露其中安全之漏洞，包括初始向量(IV)的不當使用。(參看 http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf)

該文作者們認為像 RC4 這種串流密碼(Stream cipher)做法就有弱點。例如，假設 EA 和 EB 都是用同一組 Key (IV 串上秘密金鑰)做 xor 得到的密文，則若我們把 EA 和 EB 這兩個密文做 xor，則 Key 本身就抵銷掉了(因為等於對同一個 key 做兩次 xor)，此時的值就等於原先的明文互相 xor 在一起，只要我們知道其中的一個明文，與之 xor 後就可以得出另一個明文。由於 IV 本身是沒有加密的，因此這意謂著駭客並不需要有 WEP 的 key 也照樣能夠破解密碼。

WEP 標準建議每個封包都更換初始向量 IV，但是事實上像朗訊公司(Lucent)的 Orinoco 無線網路卡其實在每次重新插入電腦時都把初始向量值歸零，此後則每送出一個封包就把該 IV 值加一，這使得大部分是在使用較小值的初始向量，更使得被破解的機會大增。

由以上討論可知問題出在金鑰串流(keystream)的重複使用，由於

keystream是由IV串上所有此時與該基地台溝通者都知道的秘密金鑰當亂數種子用RC4演算法產生的，所以只要我們把所有可能的IV值被用來傳送已知明文的對應密文都存起來，之後當我們截到一個加密訊息時只要把與該訊息相同IV的密文串拿出與之xor再與已知明文串做xor就可得出訊息的內容。因為IV是用24 bits，每個封包以1500位元組計算，所需的空間約24GBytes，以現在硬碟容量根本不是問題。802.11b理論上是每秒可達11Mbits，事實上平均大約每秒5Mbits，：

$$\frac{1500Bytes}{packet}\times\frac{8bits}{1byte}\times\frac{1\sec}{11Mbits}\times\frac{1Mbits}{10^6bits}\times 2^{24}\,packets\approx 18300\sec\approx 5hrs$$

$$2^{24}\times 1500\ bytes\ \approx\ 24\ GB$$

Figure 8.　破解WEP所需時間與空間

如上圖所顯示的，以此估算，有心者大約在五個小時左右就可以把所有可能的IV值都試驗過並且把用它對一個已知明文加密後的所有資料串都存到硬碟上備用。注意這個方法是不管使用的秘密金鑰，所以不論你的key是48bits或是104bits(連IV共64 bits與128bits)都是一樣。也就是問題出在IV，不是秘密金鑰。為此，有人建議把24-bit的IV改用更長的IV，以便使得需要記下的資料大到變成這個破解方法不可行。

## 1.6. WEP破解

在美國加州大學柏克萊分校的Nikita Borisov, Ian Goldberg, 和David Wagner於Mac-Crypto研討會上發表過對WEP安全機制提出質疑的文章之後，第一個被公開的破解工具是WEPCrack，它是在2001/08/12公佈到bugtraq上，使用Perl語言寫的。可以從這個網址抓到：http://sourceforge.net/projects/wepcrack/

大約一個禮拜之後，另一個叫做Airsnort 的工具也被公佈出來，也是用Perl語言寫的，包括了收集封包以及破解WEP的程式。

依據AirSnort網站所發表的訊息顯示，AirSnort在接收了100MB到1GB的網路流量後，可以在幾秒鐘之內就找出WEP用來加密的金鑰。由於目前無線網路設備廠商在使用WEP的方式上都還是使用靜態的加密金鑰（也就是說不會自動更換金鑰），因此，要累積到這樣多的網路流量是一件很簡單的事。AirSnort程式設計師認為，大多數無線網路使用者對現有所謂纜線等效加密（WEP）的無線加密技術不是不了解，就是漠不關心。AirSnort設計師表示，他們要表達的訴求是，當企業透過無線網路傳輸重要資料時須格外小心，安全上勢必得有所提昇，因為錯誤的安全認知，比毫無安全概念還糟糕。AirSnort的程式以及相關訊息可以參看http://airsnort.shmoo.com/網站。

另一個跟無線網路安全測試有關的程式是NetStumbler ，可以參看http://www.netstumbler.com，不過目前的NetStumbler只適用在朗訊公司(Lucent) Orinoco晶片組的無線網路卡上（目前NetStumbler沒有支援Cisco、Intel、3Com等晶片組）。NetStumbler不但可以偵測802.11b

的無線電訊號，並且可以找出Access Point的MAC位址、無線網路的名稱、SSID、製造廠商、目前所使用的頻道、有沒有使用WEP加密技術、信號強度、乃至噪訊比，以及其他一些參數等等。此外，如果使用者有接上可以輸出標準NMEA（National Marine Electronics Association）訊號的GPS設備時，NetSumbler也會同時將所在地的經緯度一併記錄下來。

第一篇發表宣稱實作WEP破解的文章是Rice University的學生與兩名AT&T實驗室的員工(Adam Stubblefield與John Joannidis、Aviel D. Rubin）在2001年8月底發表的。令人驚訝的是，其中完全沒有牽扯到任何特殊裝置，你只要有一台可以連上無線網路的個人電腦，從網路上下載更新過的驅動程式，接下來就可以開始記錄網路上來往的所有封包，再加以解碼即可。

## 1.7. WEP補強 – 802.11i

有些無線產品的廠商如思科(Cisco)系統公司，賣給企業的802.11 系統在 WEP 以外又配備了其他自行增加的安全措施。

針對現行的無線加密容易被破解的WEP安全協議，IEEE 802.11i工作小組正忙於製訂被稱為802.11i的新安全標準，Wi-Fi聯盟主席Dennis Eaton說，該聯盟計劃在明年2月把該規範作為一項可選擇的機制推出，大約6個月後就須按新的Wi-Fi規範執行了。因預計該標準在

2003年9月才能得到批准，因此Wi-Fi聯盟只是讓大家對802.11i有所了解。Eaton又說：“他們的工作正在進行中，但對於Wi-Fi設備來說，安全是個大問題，而且今天的市場的確需要一個安全解決方案。”

被稱為無線保護存取(WPA)的 Wi-Fi 聯盟的規範包括為資料加密以及網路存取控制而新製訂的 802.11i 標準。WPA 使用臨時密鑰集成協議(TKIP)進行加密，其運演算法則與 WEP 一樣，但創建密鑰的方法有所不同。

WPA 也將使用 IEEE 802.1x 協議進行存取控制，這是最近才完成的網路使用認證標準。是一個既可控制登錄有線也可控制登錄無線區域網的標準，所以說 802.1x 不是無線標準而是網路標準。

運用 WPA 技術，每一個用戶都有自己的加密密鑰，並且可以定期更改密鑰。在企業裏，用戶身份認證將透過認證伺服器進行，與 WEP 相比，它能擴展更多的用戶。家庭網路用戶透過“預置共用密鑰”模式就能使用，不需要身份認證伺服器。

據 Eaton 透露，預計 WPA 的合格試驗將於明年(2003 年)2 月 3 日進行。Wi-Fi 聯盟計劃採用 802.11i 標準作為 WPA 的第二個版本，並於 2004 年初開始實行。

# 結論

無線網路的安全性確實有問題，只要有了Airsnort這種免費軟體程式，攻擊者完全有可能破解WEP密碼(即使使用128位元加密也是如此)。有一種新型攻擊手段稱作"戰爭駕駛（war driving）"，就是拿著無線網路WLAN終端設備(例如筆記型電腦或是帶有無線網路卡的PDA)，一邊開著汽車，一邊尋找可以捕捉到的無線電波，這樣就可以準確地確定所在地區內所有802.11網路的位置及它們是否使用WEP。

在2002年初美國報導這種概念之後，四月初的一天下午，日本《日經網路》編輯部在東京街頭嘗試了用什麼頻率可以接收到無線LAN電波。他們乘坐公交車從澀穀車站出發，經過六本木和神穀町，最後到達新橋車站。他們提著執行Windows XP且配備WLAN卡的筆記本電腦，並隨時顯示可使用的無線網路。由於Windows XP具備在接收到接入點的電波之後，就會在"可以使用的網路"視窗畫面上顯示無線LAN網路名稱（ESS-ID：extended service set ID）的功能，他們在試驗中就使用了這一功能。雖然乘車時間只有30分鐘，行駛距離大約也就是4km左右，但是Windows XP竟然收集到了35個ESS-ID。其中，有的ESS-ID上還直接顯示著企業的名字和產品供貨時的內定(Default)名稱。事實上如果同樣的實驗在新竹科學園區裡面各廠商附近做一遍，相信也會有類似的結果。

有許多的實驗顯示大約百分之七十以上的無線網路並沒有啟動WEP加解密機制，在倫敦一項長達7個月的調查顯示，甚至有94%的

無線區網都沒有設定正確，無法遏止駭客入侵。不過誠如以上我們討論的，就算啟動了WEP機制也仍有可能被破解。WEP的理論出發點是防止不經意的偶然竊聽而不是刻意的攻擊，IEEE正努力在標準中增強內在安全性。其中包括WEP密鑰的動態分配以及IEEE 802.1x的認證機制。

在本計畫執行的過程中，我們對無線網路的通訊協定以及其安全的相關課題作深入的探討。很顯然，WEP最大的弱點是所有使用者都使用相同的 key，這使得key很難保密也很難隨時更換。然因為WEP已被證明經過數小時就會被破解，所以最好經常換加密解密的key。雖然目前無線網路通訊協定的標準802.11i已經開始在安全性方面補強，並且有802.1x網路認證協定配合，但是因為大部份的無線網路產品尚未實作出該新的安全協定，所以使用無線網路仍是很不安全的。

# 參考文獻


[1] C. Gao, "Security Issues in Wired and Wireless Networks," CprE537X Project Report, Iowa State University, Ames, Iowa, 2000.

[2] Nikita Borisov , Ian Goldberg , David Wagner, "Intercepting mobile communications: the insecurity of 802.11," The seventh annual international conference on Mobile computing and networking, 2001 July 2001 http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[3] N. Golmie, R. E. Van Dyck, and A. Soltanian, "Interference of bluetooth and IEEE 802.11: simulation modeling and performance evaluation," Proceedings of the 4th ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems, 2001, Rome, Italy

[4] Adam Stubblefield, John Ioannidis, and Aviel D. Rubin , "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001 (http://www.cs.rice.edu/~astubble/wep/ )

[5] N. Leavitt, "Malicious Code Moves to Mobile Devices", Computer, pp 16-19, December 2000

[6] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the sixth annual International conference on Mobile computing and Networking (MobiCom 2000), Boston, Aug 2000

[7] LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifica-tions. IEEE Standard 802.11, 1999 Edition, 1999.

[8] E. Dawson and L. Nielsen. Automated cryptanaly-sis of XOR plaintext strings. *Cryptologia*, (2):165–181, April 1996

[9] Stephen Kent and Randall Atkinson. Security ar-chitecture for the Internet Protocol. Internet Re-quest for Comment RFC 2401, Internet Engineer-ing Task Force, November 1998.

[10] T. Mallory and A. Kullberg. Incremental updat-ing of the Internet checksum. Internet Request for Comments RFC 1141, Internet Engineering Task Force, January 1990.

[11] B. Braden, D. Borman, and C. Partridge. Com-putting the Internet checksum. Internet Request for Comments RFC 1071, Internet Engineering Task Force, September 1988.

[12] R.L. Rivest, "The RC4 Encryption Algorithm," RSA Data Security, Inc., Mar 1992.

[13] R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apr 1992.

[14] R.L. Rivest, "The MD4 Message Digest Algorithm," *Advances in Cryptology - CRYPTO '90: Proceedings*, Springer-Verlag, 1991, pp. 303-311.

[15] Bruce Schneier and Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). *5th ACM Conference on Computer and Communications Security*, pages 132–140, San Francisco, California, November 1998. ACM Press.

[16] S. Kent and R. Atkinson, "Security Architecture for the Internet

Protocol," RFC 2401, Nov. 1998

[17] "Extranet Security and Management: The Difference Between Extranets and VPN's", Aventail Technical Paper, MAR 1999

[18] R.S Sandhu, P. Samarati, "Access control: principle and practice",IEEE Communication, vol.32, Sept. 1994

[19] ISI for DARPA, RFC 793: Transport Control Protocol, September 1981.

[20] W. Richard Stevens, "TCP/IP Illustrated, Volume1", Addison Wesley,1999

[21] CCITT Recommendation X.509 - The Directory: Authentication Framework, 1993

[22] A. Shamir, "How to share a secret," *Communications of the ACM*, v. 22, n. 11, 1979

[23] J. Schiller, Mobile Communications, Addison-Wesley, New York, 2000.

[24] Nicholad J. Puketza, Kui Zhang, Mandy Chung, "A Methodology for Testing Intrusion Detection Systems," ***IEEE Trans. on Software Engineering***, Vol. 22, No.10.October, 1996.

[25] 3COM, "IEEE 802.11b Wireless LANs," 3COM Corp. website, Santa Clara, CA, 2000

[26] Charlie Kaufman, etc., "Network Security: Private Communication in a PUBLIC World," **PTR Prentice Hall**, New Jersey, 1995.

[27] Shih-Kun Huang and Shiao-Rong Tyan, "Intrusion Detection and Vulnerability Analysis for GCA Service, " 1999 Project for Institute of Telecommunication.

[28] Michael Sobirey, "Currently 83 Intrusion detection Systems," http://www-mks.informatik.ut-cottbus.de/~sobirey/ids.html,

[29] 999Elliott, J. IT Professional, "Distributed denial of service attacks and the zombie ant effect" Volume: 2 Issue: 2 , March-April 2000

[30] Airsnort : http://airsnort.sourceforge.net/

[31] Wepcrack: http://sourceforge.net/projects/wepcrack

[32] IEEE802.g homepage: http://standards.ieee.org/getieee802/

# 附錄. 無線網路802.11弱點研究投影片

* Introduction
* IEEE 802.11 Standard
* WLAN architecture
* WLAN Security and WEP
* WEP problems & solutions

# Wireless LAN & IEEE 802.11

## 無線乙太網路弱點研究

林一平 liny@csie.nctu.edu.tw
蔡文能 tsaiwn@csie.nctu.edu.tw
交通大學資訊工程學系



# OUTLINE

- Introduction
- IEEE 802.11 Standard
- WLAN architecture
- WLAN Security and WEP
- WEP problems & solutions

# Wi-Fi Introduction

- **Wi-Fi 是 Ethernet (802.3)相容的無線通信協定**
  - **802.3 通訊協定: CSMA/CD**
  - **802.11 (Wi-Fi) 通訊協定: CSMA/CA**
- Wi-Fi技術代號是**IEEE 802.11**，也叫做Wireless LAN
- 適用範圍在 50 到 150 公尺之間，Transmission rate 可到 11Mbps (802.11b), 甚至 54 Mbps (802.11a 和 802.11g)

3

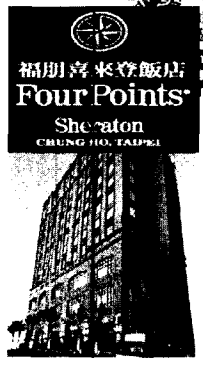
# Intended Use

Any Time Any Where

**隨時隨地都可上網遨遊**

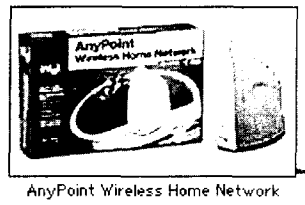
- Wireless Internet access inside hotel lobbies, conference rooms, etc.

← Wireless at the Airport




- Wireless with your Latte?

- Wireless home networking →




AnyPoint Wireless Home Network

4

## Wireless Growth


**"By 2003, 20% of B2B traffic and 25% of B2C traffic will be wireless."**

**"By 2004 nearly 50% of business applications will be wireless."**

Meta Group Research

5

## Wi-Fi Standard (802.11)


- Mission: promote 802.11 interoperability as the global wireless LAN standard
- Wi-Fi Board members include AMD, Apple, Cisco, Compaq, Dell, Epson, Ericsson, Fujistu, Gateway, HP, IBM, Intel, Microsoft, NEC, Nokia, Nortel, Philips, Samsung, Sharp, Sony, TDK, Toshiba, . . .

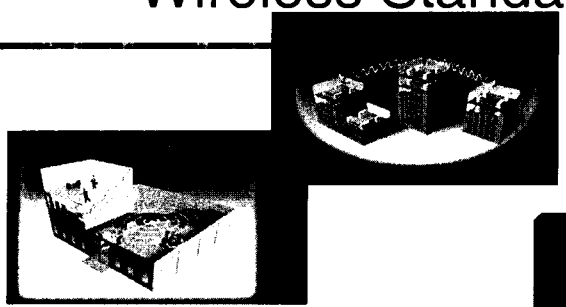
6

# Wireless Ethernet Compatibility Alliance (WECA)

- Mission statement—WECA's mission is to certify interoperability of Wi-Fi™ (IEEE 802.11b) products and to promote Wi-Fi as the global wireless LAN standard across all market segments
- Goal—Provide users with a comfort level for interoperability
- Presently over 150 different product certified and growing

7

# Wireless Standard



Network
Radio
Speed

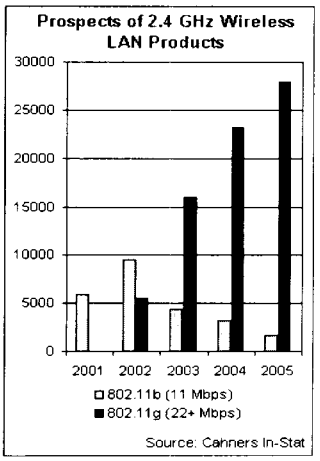
▼ IEEE 802.11a/b
Ratified

1999 2000 2001 2002 2003

8

# Flavors of 802.11x

- 802.11 (2 Mbps)
  - Older standard
- 802.11b (11 Mbps)
  - Current technology
- 802.11a (54 Mbps)
  - 5 GHz (not 2.4 GHz)
- 802.11g (22~54 Mbps)
  - 2001/11 draft standard
- HiperLAN/2 (European standard, 54 Mbps in 5 GHz band)




9

# Status of IEEE 802.11g

- 2000/3 - Interoperable w/IEEE 802.11b-1999 and lead to 20+Mbps.
- 2000/9/21 - TGg first meeting. Function Requirement and Comparison Criteria were adopted.
- 2001/11 – First Draft issued. Data Rates up to 54Mbps in 2.4GHz band.
- 2001/12/21 – Draft 1.1.
- 2002/1 – Enable balloting on the 802.11g standard.
- 2003/6 – Estimated Final Approval of IEEE 802.11g.

http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm

10

# Status of IEEE 802.11i


- 2002/2 – preparing TGi draft
- WEP2 – Increases IV spaces to 128Bits.
- Kerberos
- 802.1X
- The purpose of Task Group I is to:

  Enhance the current 802.11 MAC to provide improvements in security.

http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm 11

# IEEE 802 family


- 802.1 → 高層介面、網路互連
- 802.2 → 邏輯鏈結控制 (LLC = ***Logical Link Control*** )
- 802.3 → CSMA/CD 乙太網路(Carner-Sense Multiple Access with Collision Detection)
- 802.4 → 權杖匯流排 (Token bus) 網路，或稱記號匯流排網路
- 802.5 → 權杖環 (Token ring) 網路，也有人稱記號環網路
- 802.6 → 都會網路 (MAN，Metropolitan Area Network)
- 802.7 → 寬頻區域網路 (Broadband LAN)
- 802.8 → 光纖區域網路 (Fiber Optic LAN)
- 802.9 → 多媒體傳輸 (Multimedia traffic)，整合聲音與網路資料
- 802.10→ 網路保全 (Security)
- **802.11→ 無線網路 (Wireless Network)**
- 802.12→ 需求優先存取***Demand Priority***區域網路 (100BaseVG-AnyLAN)
- 802.14→ 有線電視通訊網
- 802.1x→ **Port Based Network Access Control** (Authentication)

12

# IEEE 802.11 Work Groups

http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

| Group | Label | Description | Status |
|---|---|---|---|
| **IEEE 802.11 Working Group** | WG | The Working Group is comprised of all of the Task Groups together | |
| **Task Group** | TG | The committee(s) that are tasked by the WG as the author(s) of the Standard or subsequent Amendments | |
| **MAC Task Group** | MAC | develop one common MAC for Wireless Local Area Networks | IEEE Std. 802.11-1997 |
| **PHY Task Group** | PHY | three PHY's for Wireless Local Area Networks (WLANs) applications, using Infrared (IR), 2.4 GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4 GHz Direct Sequence Spread Spectrum (DSSS) | IEEE Std. 802.11-1997 |
| **Task Group a** | TGa | develop a PHY to operate in the newly allocated UNII band | IEEE Std. 802.11a-1999 |

13

# IEEE 802.11 Work Group(Cor

| Group | Label | Description | Status |
|---|---|---|---|
| **Task Group b** | TGb | develop a standard for a higher rate PHY in the 2.4GHz band | IEEE Std. 802.11b-1999 |
| **Task Group b-cor1** | TGb-Cor1 | correct deficiencies in the MIB definition of 802.11b | Ongoing |
| **Task Group c** | TGc | add a subclause under 2.5 Support of the Internal Sub-Layer Service by specific MAC Procedures to cover bridge operation with IEEE 802.11 MACs | Part of IEEE 802.1D |
| **Task Group d** | TGd | define the physical layer requirements | Ongoing |
| **Task Group e** | TGe | Enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms | Ongoing |

14

# IEEE 802.11 Work Group(Cont'd)

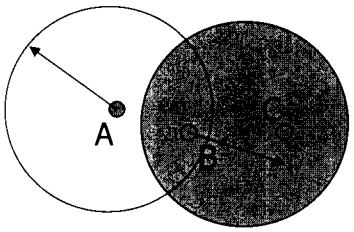
| Group | Label | Description | Status |
|---|---|---|---|
| **Task Group f** | TGf | develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor Access Point interoperability | Ongoing |
| **Task Group g** | **TGg** | develop a higher speed(s) PHY extension to the 802.11b standard | Ongoing |
| **Task Group h** | TGh | Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz Band | Ongoing |
| **Task Group i** | **TGi** | Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms | Ongoing |
| **Study Group** | SG | Investigates the interest of placing something in the Standard | |

15

# IEEE 802.11 (Wireless Ethernet)

- Why can't we use regular Ethernet for wireless?
  - Ethernet: A sees B, B sees C, → A sees C
  - Wireless: Hidden node problem

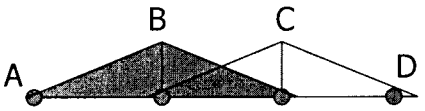
    A sees B, B sees C, yet A does not see C




16

# IEEE 802.11 (Wireless Ethernet) vs. Ethernet

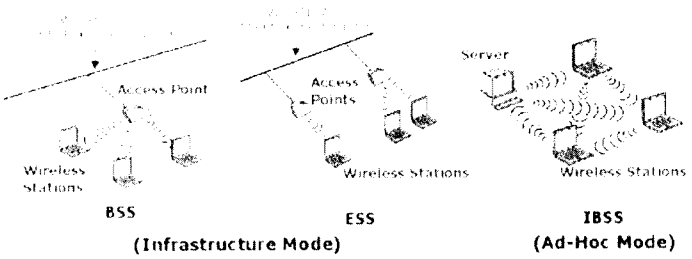
- Why can't we use regular Ethernet for wireless?
  - Ethernet: B sees C, C sees D → B & C can't send together
  - Wireless: B can send to A while C sends to D




17

# WLAN architecture

- Infrastructured wireless LAN

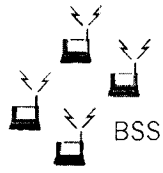



- Ad-Hoc LAN
  Independent Basic Service Set Network

18

# Ad Hoc Wireless Networks

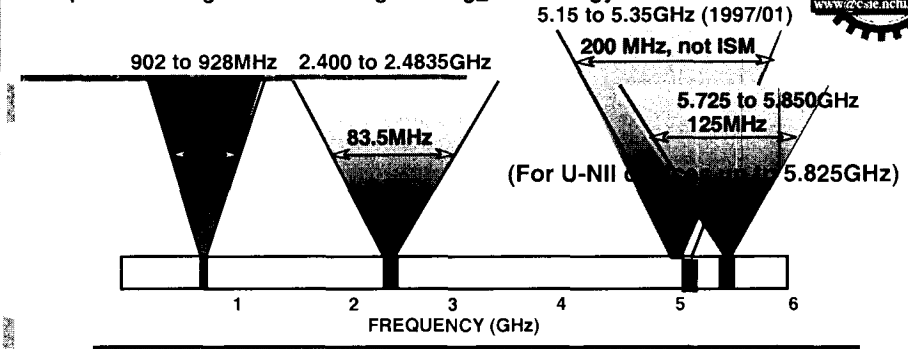
- IEEE 802.11 stations can dynamically form a group without AP(Access Point; 無線基地台)
- Ad Hoc Network: no pre-existing infrastructure
- Applications: "laptop" meeting in conference room, car, airport; interconnection of "personal" devices (see bluetooth.com); battelfield; pervasive computing (smart spaces)
- IETF MANET
  (Mobile Ad hoc NETworks) working group




19

## Industrial, Scientific and Medical (ISM) Bands

http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1997/fcc97005.pdf




UNII: Unlicensed National Information Infrastructure

AP96358 3-4

20

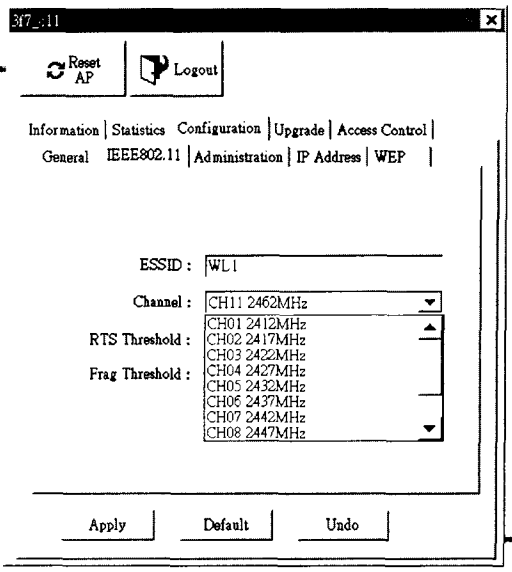
# Channel allocation for 802.11b

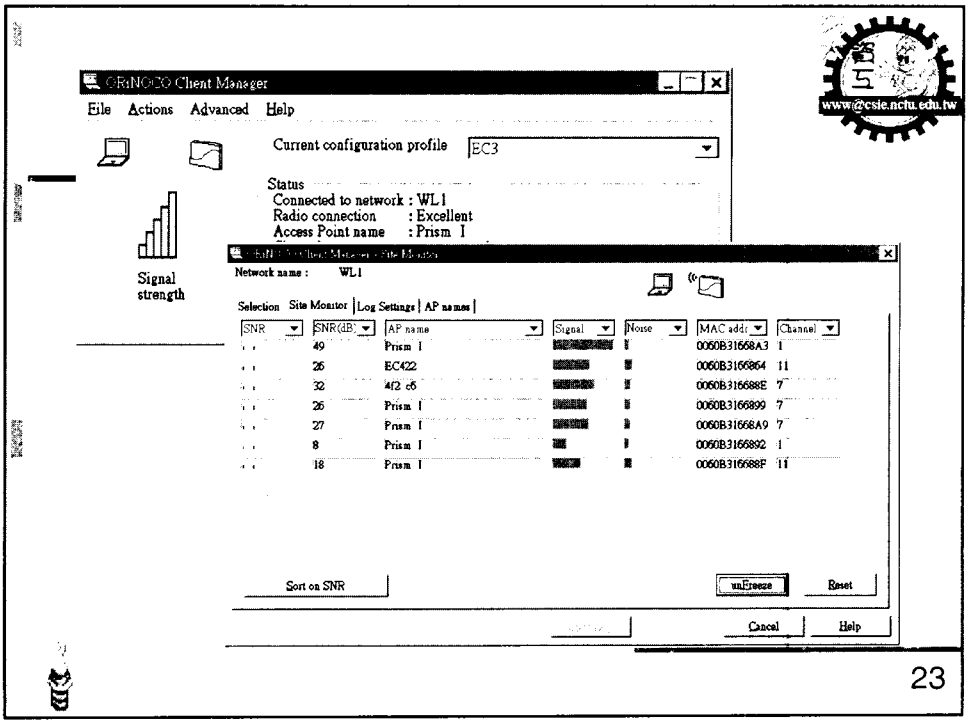
- Ch1: 2.412GHz (2.401GHz ~ 2.423GHz)
- Ch2: 2.406GHz ~ 2.428GHz
- Ch3: 2.411GHz ~ 2.433GHz
  2.416GHz，2.438GHz
- Ch6: 2.426GHz ~ 2.448GHz
  2.442，2.447，2.452，2.457，
- Ch11: 2.462GHz (2.451GHz ~ 2.473GHz)

歐洲 ~ ch 13, 日本 ~ ch14



# Channel Assignment






23

# Channel assignment (cont.)

三樓 Ch11 Ch 1 Ch6

二樓 Ch6 Ch11 Ch 1

一樓 Ch 1 Ch6 Ch11

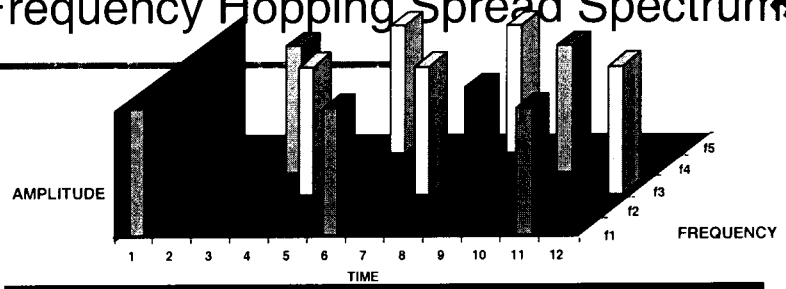
24

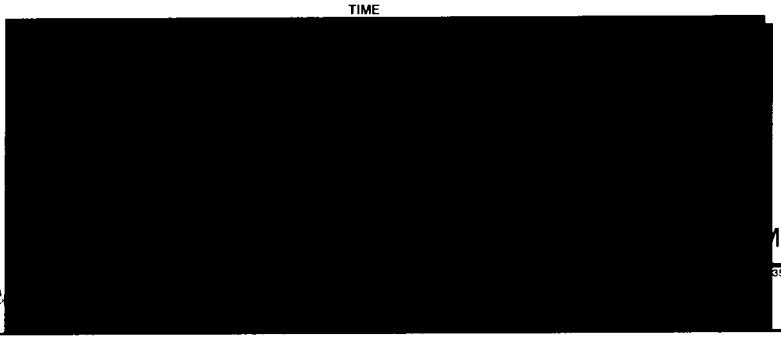
# IEEE 802.11 Physical Layer: Spread Spectrum


- Frequency Hopping Spread Spectrum (FHSS)
  - **The FHSS physical layer has 22 hop patterns to choose from. The frequency hop physical layer is required to hop across the 2.4GHz ISM band covering 79 channels. Each channel occupies 1Mhz of bandwidth and must hop at the minimum rate specified by the regulatory bodies of the intended country. A minimum hop rate of 2.5 hops per second is specified for the United States.**
- Direct Sequence Spread Spectrum (DSSS)
  - **The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. Each bit transmitted is modulated by the 11-bit sequence. This process spreads the RF energy across a wider bandwidth than would be required to transmit the raw data. The processing gain of the system is defined as 10x the log of the ratio of spreading rate (also know as the chip rate) to the data. The receiver despreads the RF input to recover the original data.**

25

# Frequency Hopping Spread Spectrum

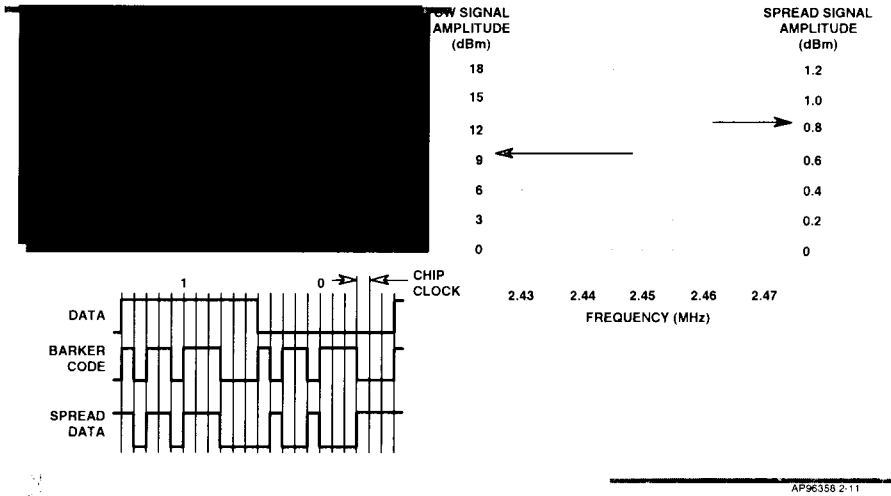



ME

358 2-13

26

# Direct Sequence Spread Spectrum (DSSS)



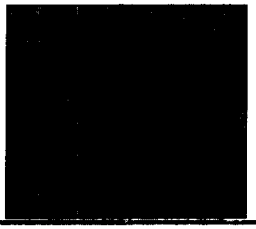

AP96358 2-11

27

# DSSS in 802.11b

- 雖然在802.11定義了跳頻展頻(FHSS)、直序展頻(DSSS)窄頻微波、紅外線等傳輸方式，但是在802.11b中僅僅定義了直序展頻(DSSS)，也因此直序展頻成了目前所有廠商的標準。同時最高傳輸速率由802.11的2Mbps提高到11Mbps，使用的頻道在2.4~2.4835GHz
- 同時爲了向下相容早期802.11所定義的1~2Mbps的傳輸速率，因此802.11b實際上可以4種不同的傳輸速率。

| 傳輸速率(Mbps) | 調變方式 |
|---|---|
| 1 | BPSK |
| 2 | QPSK |
| 5.5 | CCK |
| 11 | Complementary Code Keying (CCK) |



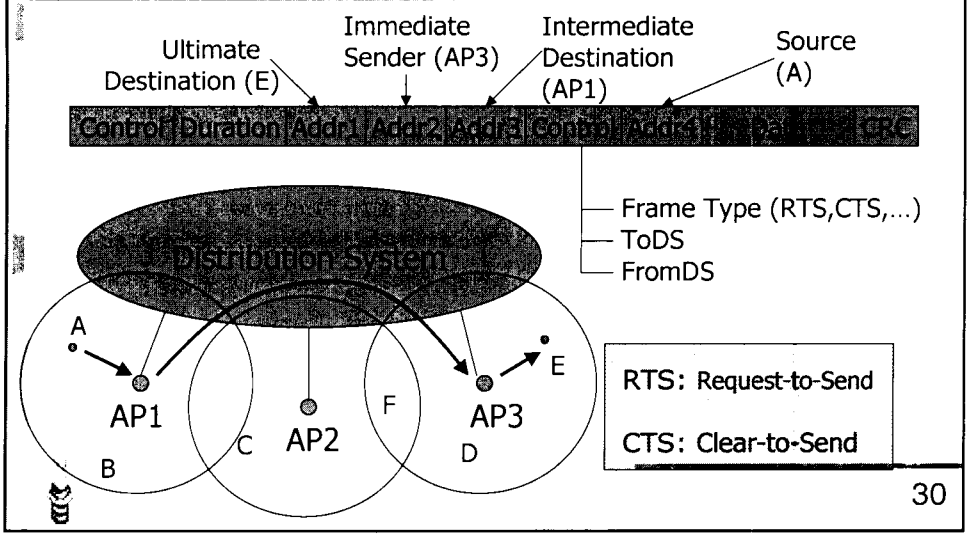
資料來源：IEEE 28

# DSSS in 802.11b

- 無線電通訊系統是利用正弦波的三個特性：振幅(amplitude)、頻率(frequency)和相位(phase)。這三個特性代表的意義分別是：訊號有多大(聲)、訊號移動的有多快、它位於正弦波上哪一個位置。
- 相位調變被廣泛地應用在數位通訊系統上，例如：802.11標準相位鍵控移位(PSK)的「鍵控」通訊協定所產生的序列(sequence)，就是用來決定調變訊號的相位變化，以傳輸數據我們常看到BPSK(Binary PSK)、QPSK(Quadrature PSK)、和M-PSK或M-ary PSK(M是符號狀態數目。若符號數目是n，則M=2n。
- BPSK是二進位制相位鍵控移位，具有兩個符號狀態(symbol states)；QPSK是象限相位鍵控移位，具有四個符號狀態；M-PSK是多階(multilevel)相位鍵控移位，符號狀態數由M值決定，M值越大通訊效果越佳。

29

# IEEE 802.11 Physical Layer : Frame format




30

# IEEE 802.11 Physical Layer : Frame format (con't)

| Frame control | Duration /ID | Addressing 1 | Addressing 2 | Addressing 3 | Sequence control | Addressing 4 | Frame body | CRC |
|---|---|---|---|---|---|---|---|---|

Header : 30Bytes including control information、addressing、sequence number、duration

Data : 0~2312Bytes,changing with frame type

Error control : 4Bytes,with CRC32

31

# 802.11 Collision Resolution

- Two senders might send RTS at the same time
- Collision will occur corrupting the data
- No CTS will follow
- Senders will time-out waiting for CTS and retry with exponential backoff

RTS: Request-to-Send

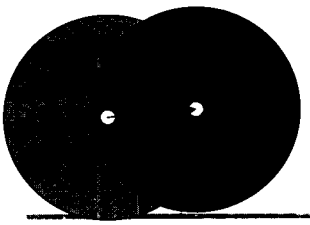
CTS: Clear-to-Send

CSMA/CA:
Carrier Sense Multiple Access/Collision Avoidance

32

# 802.11 transmission Protocol

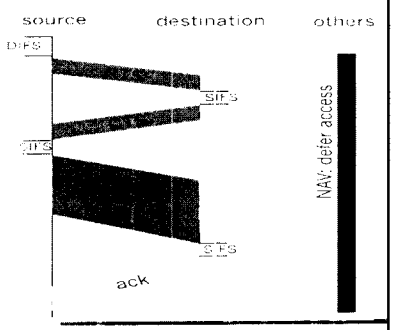
- Sender A sends Request-to-Send (RTS)
- Receiver B sends Clear-to-Send (CTS)
  - Nodes who hear CTS cannot transmit concurrently with A (red region)
  - Nodes who hear RTS but not CTS can transmit (**green region**)
- Sender A sends data frame
- Receiver B sends ACK
- Nodes who hear the ACK can now transmit



33

# CSMA/CA (Collision Avoidance)

- **sense channel idle for DISF sec (Distributed Inter Frame Space), send RTS**
- **receiver returns CTS after SIFS (Short Inter Frame Space)**
- **CTS "freezes" stations within range of receiver (but possibly hidden from transmitter); this prevents collisions by hidden station during data**
- **transmit data frame (no Collision Detection)**
- **receiver returns ACK after SIFS (Short Inter Frame Space)**
- **- if channel sensed busy then binary backoff**
- **NAV: Network Allocation Vector (min time of deferral) (= min packet size in 802.3)**
- **RTS and CTS are very short: collisions during data phase are thus very unlikely (the end result is similar to Collision Detection)**




34

# 802.11b security features


- ESSID
  - Network name, not encrypted
  - Rudimentary because the ESS ID is broadcast in beacon frames
- Association
  - Capability to register a station with a WLAN
- WEP (Wired Equivalent Privacy)
  - encrypts data using RC4 with 40 to 128-bit shared keys
  - Some vendors do in software, others in hardware
  - Symmetric Scheme – Same Key For Encrypt/Decrypt
  - Intended For:
    - Access Control (no WEP key, no access)
    - Privacy (encrypt data stream)



# Wired Equivalent Privacy


- Why Wired Equivalence Privacy?
  - Wireless medium has no packet boundaries
    - WEP control access to LAN via authentication
  - Wireless is an open medium
    - Provides link-level security equivalent to a closed medium (note: no end-to-end privacy)
- Two Types of Authentication
  - Set on Client/Access Points (Same)
  - Open (Default): Clear-Text Authentication
    - No WEP key required for access
  - Shared-Key: Clear-Text Challenge (by AP)
    - Must respond with the correct WEP key, or no access
- Broken due to bad use of the cipher [Walker, Berkeley Team, Arbaugh, Fluhrer]

# WEP (cont.)


- RSA "Fast-Packet Keying"
  - Fix Approved By IEEE Committee (2001)
  - Generates Unique Encryption Keys For Data Packets
  - Reduces Similarities Between Successive Packets
- Temporal Key Integrity Protocol (TKIP)
  - Approved 2002/01/25, Optional 802.11 Standard
  - Helps Defeat Passive Packet Snooping
  - Dynamic Keys Defeat Capture of Passive Keys (WEP Hole)
  - Some Vendors Starting to Incorporate



# Auth: Captive portal

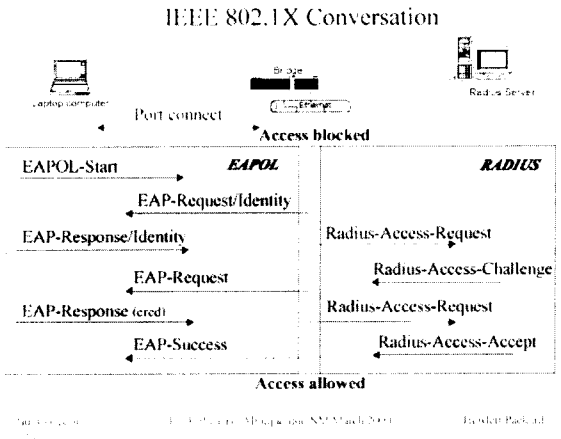

- Synopsis:
  - Intercepts first HTTP connection
  - Redirect to authentication page using SSL
  - Does access control based on login / password
- Products
  - NoCatAuth (freeware)
  - Vernier Networks (commercial)
  - E-Passport, EZone
- Costs:
  - Not intrusive nor expensive

# Auth: 802.1X

- Synopsis:
  - authentication before giving access to the network
  - Requires a PKI certificate on each client
  - Requires a central RADIUS server with EAP
- Products:
  - CISCO *Aironet 350 Series*
  - Microsoft Windows XP
- Costs:
  - Deployment is intrusive
  - Maintenance is expensive
  - Can be a corporate wide solution

39

# Extensible Authentication Protocol (EAP [RFC 2284])

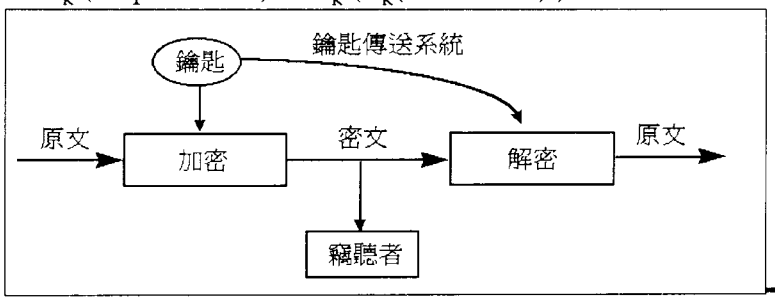



- **A port begins in an unauthorized state, which allows EAP traffic only.**
- **Once the Authenticator has received a Supplicant's request to connect (an *EAPOL-Start*), the Authenticator replies with an *EAP Request Identity* message.**
- **The returning *Response Identity* message is delivered to the Authentication Server.**

40

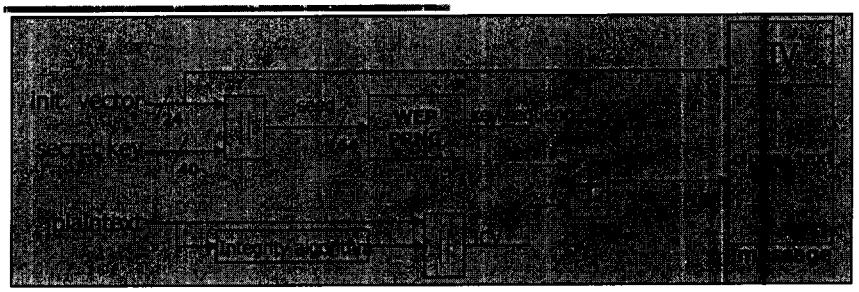
# WEP Wired Equivalent Privacy

- ~~k is the shared key~~
- Message + checksum(message) = plaintext
  - $E_k$(PlainText) = CipherText
  - $D_k$ ( CipherText) = $D_k$ ($E_k$(PlainText) ) = PlainText




41

# WEP crypto function

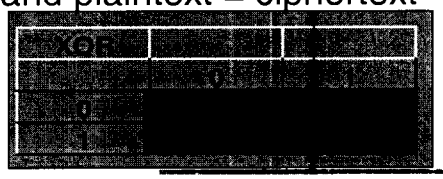



- WEP uses RC4 PRNG (Pseudo Random Number Generator) from RSA (stream cipher)
- CRC-32 for Integrity algorithm
- IV is renewed for each packet (usually iv++)
- **key size = (vendor advertised size – 24) bits**

42

# WEP Process

- Integrity Check (IC): checksum of message
  - Message + checksum(message) = plaintext
- Encryption
  - Using RC4 and Initialization Vector (IV)
  - RC4 generates keystream (PseudoRandom string of bytes as a function of the IV and the key)
- XOR (⊕) keystream and plaintext = ciphertext
- Send ciphertext and IV over network

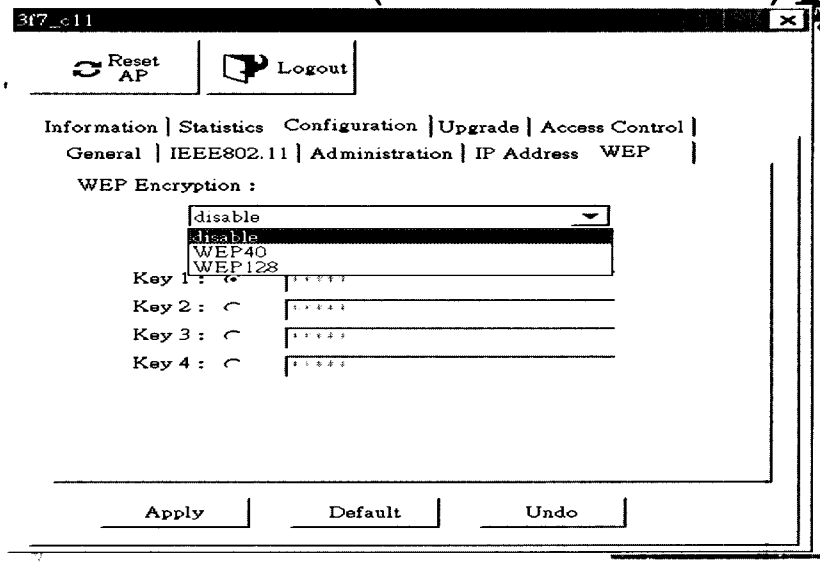





# Integrity Check (IC): CRC-32 checksum

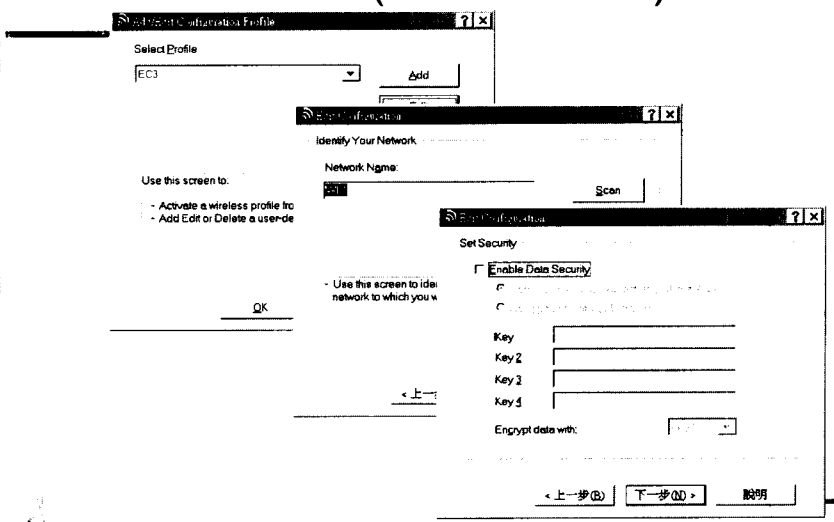
- Message Authentication using linear checksum : CRC-32
- WEP protocol uses *integrity checksum field* to ensure packets are not modified in transit.
- Implemented as a CRC-32 checksum, and is a part of the encrypted payload of the packet.
  - Very good for detecting random bit errors, but is it as good for malicious bit errors ?
- Can the WEP checksum protect data integrity – one of the main goals of the WEP protocol. Lets see ...

# WEP enable (on Access Point)



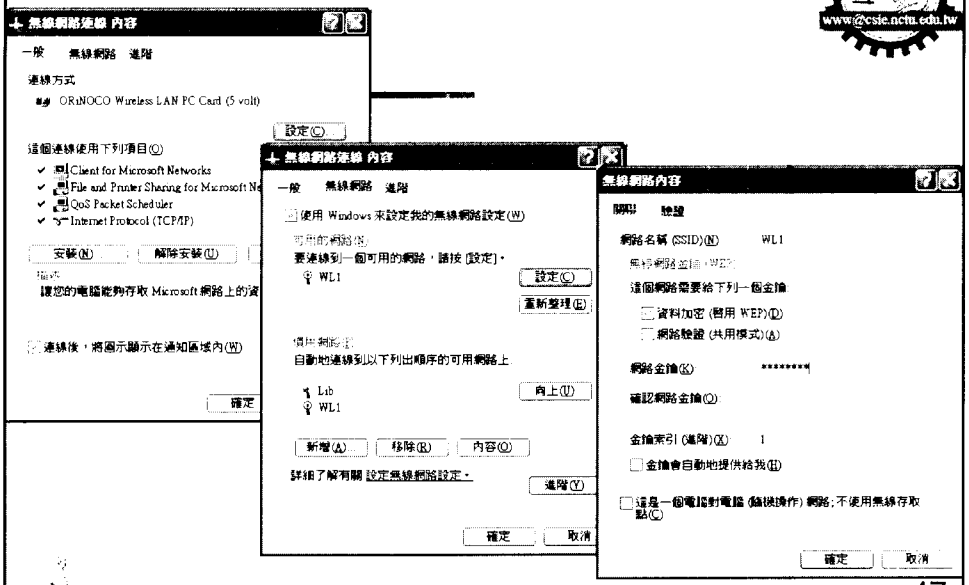

45

# WEP enable (on PC card)




46

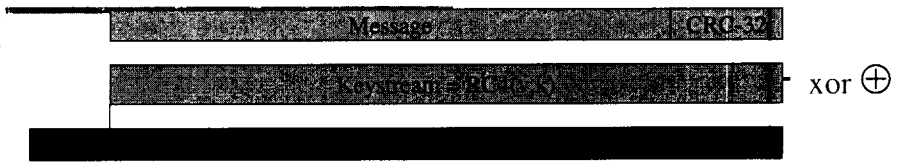
# Lucent OriNOCO Wireless NIC



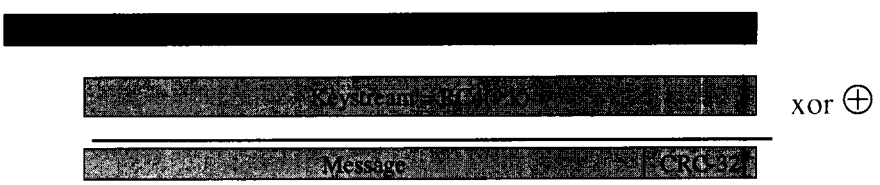



# WEP Encryption / Decryption

Encryption: (by sender)




Decryption: (by receiver)



# Problems with WEP


- IC is a 32 bit checksum and is part of the encrypted payload
  - It is possible to compute the bit differences between the 2 ICs based on the bit differences of the messages
  - An attacker can then flip bits in both to make a message appear to be valid

IC: Integrity Check

49

# Problems with WEP (2)


- IV is a 24 bit field sent in the clear text portion of the message
  - 24 bits guarantees eventual reuse of keys
  - $2^{24}$ possibilities (16,777,216)
  - Max data
  - A busy access point will reuse keys after a couple of days

IV: Initialization Vector

50

# Problems with WEP (3)


- WEP is a per packet encryption method
  - This allows data streams to be reconstructed from a response to a known data packet
  - For ex. DHCP, ICMP, RTS/CTS
  - In addition to decrypting the streams, this allows for the attack known as packet spoofing.
- Serious problem becoz same shared key is used by all the mobile users.



# Problem with RC4


- If 2 ciphertexts are known, it is possible to obtain the XOR of the plaintexts
- Knowledge of the XOR can enable statistical attacks to recover plaintext
- Once one of the two plaintexts is known, it is simple to recover others

$RC4(X) \oplus X \oplus Y = RC4(Y)$

Plaintext: X, Y
Ciphertext: RC4(X), RC4(Y)

## Attacks against WEP

- **Table-based Attack**

$2^{24} \times 1500 bytes \approx 24GB$



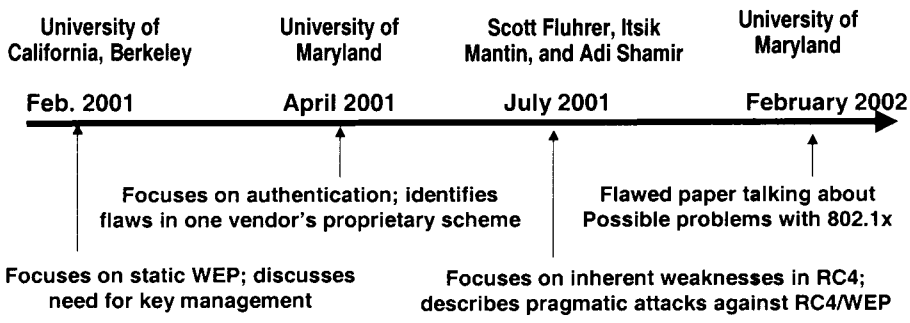
## How to Read WEP Encrypted Traffic

Ways to accelerate the process:

- Send spam into the network: no pattern recognition required!
  - **Get the victim to send e-mail to you**
  - **The AP creates the plaintext for you!**
- Decrypt packets from one Station to another via an Access Point
- If you know the plaintext on one leg of the journey, you can recover the key stream immediately on the other
- –Etc., etc., etc.

http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm

# Papers on WLAN Security


*** "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe..."**

– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

55

# 'Off-the-shelf' hack breaks wireless encryption


http://www.cnn.com/2001/TECH/ptech/08/10/wireless.hack/index.html

(CNN) -- A group of researchers from Rice University and AT&T Labs have used off-the-shelf methods to carry out an attack on a known wireless encryption flaw -- to prove that it "could work in the real world."

The researchers from Rice University in Houston, Texas, and AT&T performed their recent attack after reading a detailed and highly scientific description of the vulnerability written several weeks ago by Scott Fluhrer from Cisco Systems, and Itsik Mantin and Adi Shamir from The Weizmann Institute of Science in Israel.

56

# Hackers poised to land at wireless AirPort

http://zdnet.com.com/2102-11-527906.html

By Jared Sandberg, The Wall Street Journal Online

http://airsnort.shmoo.com/

AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

http://sourceforge.net/projects/wepcrack

WEPCrack is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.

http://www.netstumbler.com/ NETSTUMBLER.COM

57

# AirSnort "Weak IV" Attack

- Initialization vector (IV) is 24-bit field that changes with each packet
- RC4 Key Scheduling Algorithm creates IV from base key
- Flaw in WEP implementation of RC4 allows creation of "weak" IVs that give insight into base key
- More packets = more weak IVs = better chance to determine base key
- To break key, hacker needs 100,000-1,000,000 packets


*WEP frame*

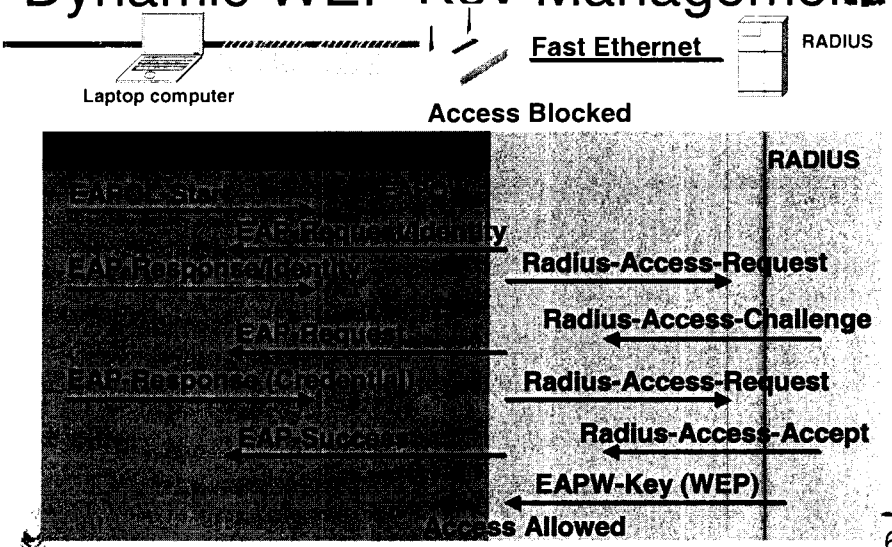
58

# Security improvements (2nd Gen)

- WEP2
  - Increases size of IV to 128 bits
  - Use of Kerberos for authentication within IEEE 802.1X
- Be device independent => be tied to the user
- Have changing WEP keys
  - WEP keys could be generated dynamically upon user authentication



# Dynamic WEP Key Management



# References


- http://www.personaltelco.net/index.cgi/WepCrack
- http://sourceforge.net/projects/wepcrack
- **http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf**
- Airsnort : http://airsnort.sourceforge.net/
- http://airsnort.shmoo.com/
- http://www.wlana.org/learn/80211.htm
- http://www.cs.rice.edu/~astubble/wep/
- http://www.isp-planet.com/technology/2001/wep.html
- http://www.isp-planet.com/fixed_wireless/technology/2001/better_wep.html
- http://www.isp-planet.com/fixed_wireless/technology/2001/wlan_primer_part2.html
- http://rr.sans.org/wireless/equiv.php
- http://rr.sans.org/wireless/wireless_sec.php


61

# References (2)


- http://www.cs.tamu.edu/course-info/cpsc463/PPT/
- http://www.newwaveinstrums.com/resources/
- http://vip.poly.edu/seminar/
- **http://www.ietf.org/rfc/rfc2284.txt**
- Nikita Borisov , Ian Goldberg , David Wagner, **"Intercepting mobile communications," The seventh annual international conference on Mobile computing and networking, 2001** July 2001
- **N. Golmie, R. E. Van Dyck, and A. Soltanian, "Interference of bluetooth and IEEE 802.11: simulation modeling and performance evaluation," Proceedings of the 4th ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems, 2001, Rome, Italy**


62

# References (3)


- http://www.ieee802.org/11/
- http://standards.ieee.org/getieee802/
- http://www.wi-fi.org
- http://www.homerf.org
- http://www.hiperlan2.com
- http://www.commsdesign.com
- http://www.80211-planet.com
- http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm
- http://www.dgt.gov.tw
- http://www.wirelesscorp.net/802.11_HACK.htm




# Wireless LAN & IEEE 802.11

## 謝謝捧場


林一平 *liny@csie.nctu.edu.tw*

蔡文能 *tsaiwn@csie.nctu.edu.tw*

交通大學資訊工程學系