第十五章 Wireless LAN 網路

首先介紹無線網路的展頻技術，再介紹 IEEE 802.11 系列的運作原理及通訊技術，也涵蓋了 HomeRF 與 HiperLAN 無線網路。

15-1 無線網路簡介

『無線網路』(Wireless Network) 係利用光或無線電波所構成的網路，不似有線網路利用實際傳導媒介（光纖纜線或對絞線）來連結；因此在傳輸媒介的存取技術方面比有線網路困難許多，這也是本章主要的探討重點。雖然無線網路的傳輸速度和傳輸品質很難達到有線網路的高穩定性，但它的方便性確是有線網路難以比擬的。尤其目前網路普及，無論筆記型電腦、掌上型電腦、甚至手機電話都必須連結上網，因此無線網路隱藏無限的發展空間。目前**『無線區域網路』(Wireless LAN, WLAN)** 大多以 IEEE 802.11 為主要標準規範，本章就某些觀點先來探討無線網路的特性，再詳述無線區域網路的運作原理。

15-1-1 無線網路的優點

我們將無線網路的優點歸類如下：

(1) 高移動性 (Mobility): 無線網路的工作站可隨時在網路涵蓋範圍內移動，甚至可經由漫遊功能，跨越多個網路之間的連接，而不受網路連『線』的影響。譬如，商場、機場或醫院，這些地區的工作人員都必須隨時移動工作位置，如採用無線網路較為方便。

(2) 節省建設費用 (Cost Saving): 只要電波可以傳送的地方，便可以連結網路，不必架設昂貴的網路連線。

(3) 縮短建構時間 (Saving Time): 架設有線網路必須經由挖掘管道再佈放纜線，比架設電波發射站更耗時且困難許多。因此針對臨時商場或需要快速完成的網路，還是使用無線網路來得方便。

(4) 克服環境困難 (Difficult-to-Wire): 許多環境佈放實體連線或許有所困難，採用無線網路便可迎刃而解。譬如網路若須經過交通要道、河流或山脈，則佈放無線網路較容易達成。

15-1-2 無線網路的缺點

雖然無線網路具有許多優點，但相對也存在許多缺點，從事無線網路工作者必須特別注意，在此就幾個常見的問題歸類如下：

(1) **電波干擾問題(Radio Interference Problem):** 電波干擾是無線網路應用上最大的障礙，目前大量的電氣用品都會產生電磁訊號，之間的干擾情形已非常的嚴重，電波干擾可能來自**『同頻干擾』(Co-Channel Interference)** 或**『鄰頻干擾』(Next-Channel Interference)**。

(2) **保密問題 (Security Problem):** 保密問題是發展無線網路的重大挑戰之一，無線電波在空中傳輸，任何人都可以由空中接收到該訊號，進而盜取傳輸資料或從事破壞的工作。因此一般無線網路都利用傳輸技巧 (如 DSSS 或 FHSS)、身分確認 (如 login)、以及資料加密 (如 WEP) 來提供網路的安全性。

(3) **連線問題(Connection Problem):** 無線網路裝置也許會經由漫遊而跨越不同的網路區域，這可必須經由基地台之間的換手 (Handoff) 來連接，才能保持網路的通暢，但所跨越不同運作型態的網路，可能會出現許多連線問題。

(4) **架設問題 (Installation Problem):** 無線網路大多必須架設發射站，然而發射站所選擇的位置是否容易發射訊號、不受其他訊號干擾、或不影響人體健康，這都是必須考量的問題。

(5) **標準問題 (Standard Problem):** 目前無線網路有許多不同的標準，又目前這些標準之間的互通性太少，這也是發展無線網路的一大隱憂。

(6) **電源管理問題 (Power Management Problem):** 絕大部份的無線網路裝置都是使用電池來供電，這些電池大多無法長期提供電力，因此在無線裝置上必須謀求許多節省電源的機制。譬如，無線裝置長時間不發射訊息但又必須保持連線的情況下，如何使電源消耗降到最低的問題。

15-1-3 無線網路的類別

隨著使用環境不同，無線網路可分成以下幾種型態：

(1) 無線區域網路（Wireless LAN, WLAN）：無線區域網路的通訊範圍侷限於某一較小的範圍內，在此範圍內無線裝置可自由移動，且仍能保持與基地台及其他無線裝置之間的連線通暢。WLAN 大多使用無授權的共享頻段來傳輸訊息，頻率之間的干擾較為嚴重，因此都會限定通訊範圍。較普遍的 WLAN 為 IEEE 802.11 系列、HomeRF、或 HiperLAN/2 網路。

(2) 無線寬頻網路（Wireless Broadband）：無線寬頻所訴求的重點是連結各地的 WLAN，構成一個較大型的無線網路。也就是說，無線寬頻網路為連結 WLAN 的傳輸骨幹，因此通訊範圍會較為廣闊一點，可使用共享頻段或專屬頻道來傳輸。常見的網路是 HiperLink 或 IEEE 802.11a 網路。

(3) 無線長程網路（Wireless Long-Hual）：無線網路的長距離傳輸大多必須使用經過授權合法的頻道來傳遞訊息，通常採用**『窄頻微波』（Narrowband Microwave）** 的傳輸技術，主要的用途是連結各地區的無線寬頻網路。常見的網路是 HiperAccess 網路。

(4) 無線區域通訊（Wireless Local Communication）：使用於近距離的通訊，傳輸速率比較低，主要的功能是取代有線連結，譬如 Bluetooth 網路。

15-2 無線網路之傳輸技術

依照各種無線網路的協定標準，大多使用 ISM（Industrial, Scientific, Medical Bands）頻段來傳輸訊息，這些頻段本來是開放給工業、科學和醫學界自由使用，使用者無須經由申請便可以自由使用，頻率為 902 ~ 928 MHz、2.4 G ~ 2.4835 GHz 和 5.725 ~ 5.850 GHz，如圖 15-1 所示。

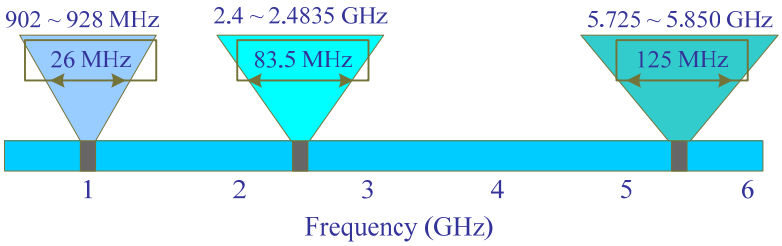

圖 15-1 ISM 頻段範圍

由圖 15-1 所示，任何無線通訊設備都可使用這三個頻段來傳遞訊息，由此可見這些頻段上訊號必然是非常擁擠的。如何克服這些頻段的共享問題？除了限制各個無線通訊設備的傳

送功率，以減少通訊設備之間的互相干擾外，並使用『展頻』(Spread Spectrum) 技術來解決頻段共用的問題。有關展頻技術可區分為『跳頻展頻』(Frequency Hopping Spread Spectrum, FHSS) 和『直接序列展頻』(Direct Sequence Spread Spectrum, DSSS) 兩種技術，本節將分別介紹。另一方面，許多無線網路也採用光的傳輸，這也是本節介紹的重點。

15-2-1 展頻通訊模型

『展頻』(Spread Spectrum) 技術原來是使用於軍事或情報單位的訊號傳輸，基本構想是將資訊的訊號延展成較寬的頻寬，以避免電波干擾或被攔截，目前大多將此技術應用在無線網路或無線電話上。我們就以下幾個步驟來介紹展頻技術的基本原理。

(A) 何謂展頻技術

與『展頻』技術相對應的是一般無線傳輸的『窄頻』(Narrow Spectrum) 技術。所謂『窄頻傳輸』，表示任何一個通訊發送器都必須藉由一個私有的頻道進行傳輸，當然同一地區發射電台的頻道都不可以相同，否則會發生『蓋台』的現象。任何一個國家為了重複使用這些頻道，都會對每一發射電台的區域與發射功率有所限制。也就是說，利用窄頻技術傳輸的頻道，都必須通過申請才可以使用，並且會限制發射功率，以免干擾到其他鄰近電台。

在無線網路（或行動電話）上，任何一部電腦（或通訊器）都可能會發送訊號，如要每一部電腦都享有一個獨立的頻道（窄頻技術），那幾乎是不可能的，此時便須利用展頻技術來解決多部發送器之間共享一個頻道的問題。基本上，展頻技術是利用共享頻道（如 ISM 頻道）來傳輸訊號，並且通訊雙方利用一個私有的頻道編碼表，來決定傳送與接收的順序，其他通訊器雖然也可接收訊號，但沒有此編碼表便無法知曉通訊內容。為了避免通訊器之間互相干擾，展頻傳輸都會限制每一發送器的功率大小。

展頻技術主要原理是為了對抗或抑制『同頻干擾』(其他系統在同一頻道上傳輸訊號)、或『多重路徑』(Multi-paths) 傳輸（容後介紹）所造成的不利影響，而將傳輸訊號以一種甚至低於背景雜訊的功率來做傳輸，以避免被他人的偵測，進一步達到通訊的私密化。譬如圖 15-2 為一般窄頻的傳輸技術，假設信號在傳輸過程中遭受到一個高功率的同頻干擾，如此接

收端所收到的是傳送信號和同頻干擾的合成訊號；由於同頻干擾的功率比信號強，而導致信號無法被有效的辨識出來。

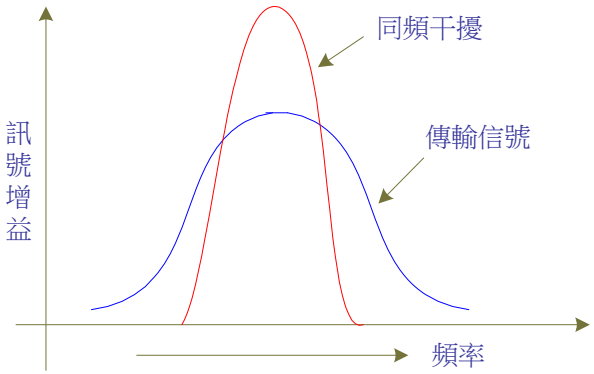

圖 15-2 窄頻傳輸的同頻干擾

如採用展頻技術，信號發射之前先將信號頻譜以某種方式展開後再傳送，傳輸中所受的同頻訊號干擾如圖 15-3 (a) 所示。而在接收端則以先前展頻的方式逆向操作，信號回復原來的頻寬範圍，而干擾訊號反而被展開成較低的增益，原訊號也因此較容易被辨識出來，解展頻後的訊號增益與頻譜關係如圖 15-3 (b) 所示。

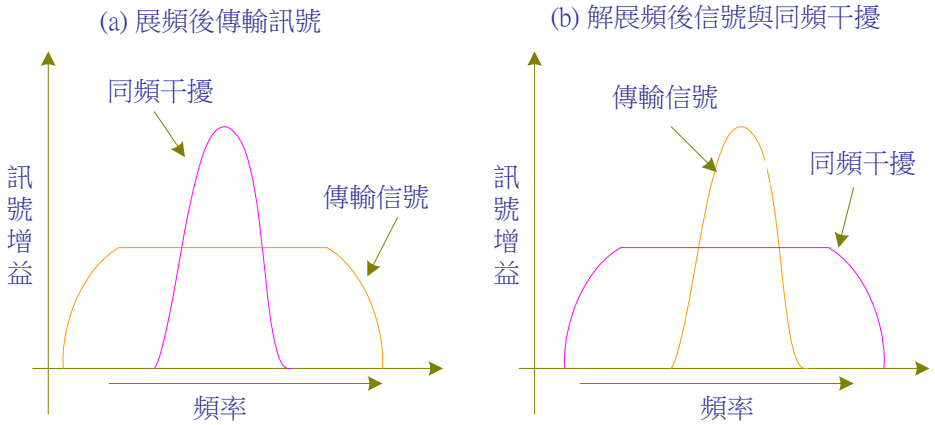

圖 15-3 以展頻技術抗同頻干擾的頻譜圖

(B) 展頻通訊模型

圖 15-4 為展頻通訊的基本模型，通訊中雙方為了達到保密目的，將各持有一個**『虛擬雜訊序列』(Pseudo-Noise Sequence, PNS)**。傳送端將資料(數位資料)送進**『編碼器』(Encoder)**編碼成一序列的數位訊號 (Non-Return Zero, NRZ 訊號)，此數位訊號再和虛擬雜訊序列器所產生的數字序列相混合，調變在一個頻寬較大的載波頻率上，達到**『展頻』**的功能。接收端收到訊號後，再利用相同的虛擬雜訊序列解碼，將展頻訊號解碼成原訊號。

其他接收器雖然可以接收到訊號，但它的虛擬雜訊序列與傳送端不相同，也無法解碼出原來訊號，如此便能讓同一頻道給多人共同使用。常用的展頻傳輸技術有 FHSS 和 DSSS 兩種，又任何一種展頻技術也都有其相對應的編碼技巧，以下分別介紹之。

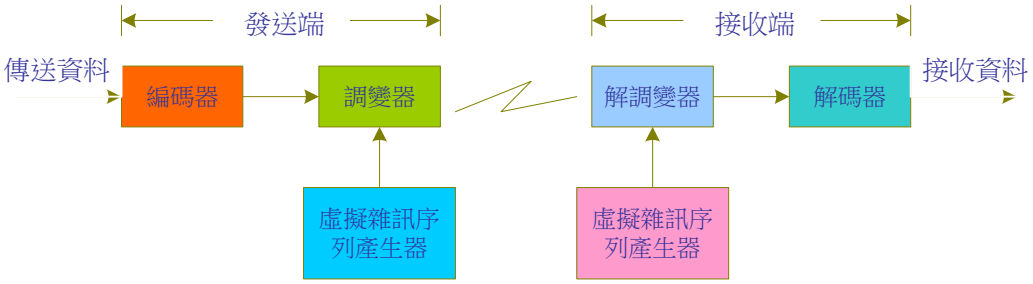

圖 15-4 展頻通訊模型

15-2-2 跳頻展頻技術

『跳頻展頻』(Frequency Hopping Spread Spectrum, FHSS) 技術是將可使用的頻段劃分為若干個小頻道，傳送端在這些小頻道之間變換 (跳越) 傳送，接收端也在相同跳越順序下接收訊號，如此便可達到雙方通訊的目的。如圖 15-5 所示，發送訊號將在 fx、fy、fz、fk、fm、… 頻道之間跳越傳送，接收端也在相同跳越順序下收取訊號。在一般規範下每秒至少跳越四個頻道，至於傳輸頻段中可區分為多少小頻道以供跳越，各個國家皆有不同規範，但至少需要 20 個頻道以上。以 IEEE 802.11 規範為例，它採用 2.4 ~ 2.4835 GHz 頻道 (ISM 頻道)，區分為 75 個跳越頻道，每一頻道頻寬為 1 MHz，規定每 250 ms 必須跳越一個頻道，也就是說每秒跳越 4 個頻道來傳輸信號。

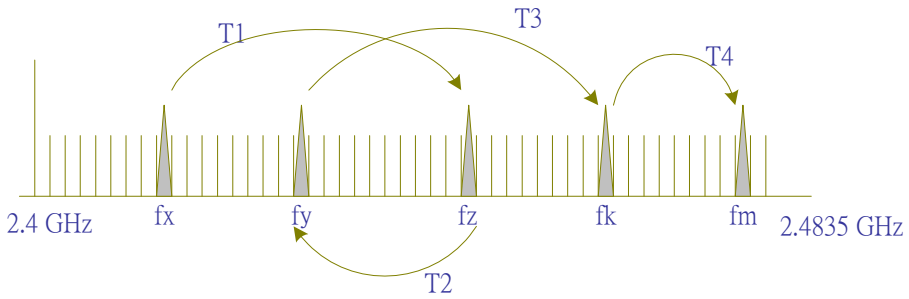

圖 15-5 FHSS 跳頻傳輸

如將圖 15-5 中的每一個頻道各給予一個順序編號，而發送端傳輸信號時所應填入的頻道號碼，就由圖 15-4 中的『虛擬雜訊序列』(PNS) 產生器來產生，譬如，0, 3, 6, 9, 12, 15, 18, …

的順序號碼。接收端以同樣的號碼順序由頻道上接收訊號，如果雙方的時序達到同步時，便能順利接收訊號而達到通訊的目的。

如圖 15-4，當傳送端將訊號發送到各頻道之前，也必須將訊號調變到該頻道上，一般在較低速率（2 Mbps 以下）的展頻傳輸（FHSS 或 DSSS）都採用 BPSK（Binary Phase-Shift Keying）或 QPSK(Quadrature Phase-Shift Keying)調變方式。如以 IEEE 802.11 規格(BPSK) 而言，每一訊號週期傳送兩個位元，頻寬為 1 MHz，則傳輸速率為 2 Mbps。(有關 BPSK 請參考第二章；QPSK 請參考第十四章介紹)

15-2-3 直接序列展頻

『直接序列展頻』(Direct Sequence Spread Spectrum, DSSS) 和跳頻展頻（FHSS）之間最大的不同點是，FHSS 的虛擬雜訊產生器是產生一序列的頻道編號，而傳輸訊號便在這些頻道之間跳越傳送；至於 DSSS 的**『虛擬雜訊序列』(PNS)** 產生器則是產生一週期性的雜訊序列，將欲傳送的訊號和此 PNS 相調變，如果 PNS 的頻譜遠高於信號頻率，則信號就被展開在這 PNS 的頻譜上，因此稱之為**『直接序列展頻』**。接收端收取訊號後，也利用同樣的 PNS 訊號來解碼，如果雙方時序同步，便能順利由頻譜上解調變出原來的訊號。其他接收器雖然可以收到此訊號，但沒有相對應的 PNS 序列，也無法解調變出原來的訊號。

DSSS 調變技術是利用**『互斥或閘』(Exclusive-OR, XOR)** 的基本原理，其運作方式如下：(類似加密/解密技術)

(a) 傳送訊號為： S(t)

(b) 虛擬雜訊序列（PNS）為：PN(t)

(c) 傳送訊號與 PNS 序列以 XOR 方式調變的結果為：PN(s) ⊕ S(t)

(d) 接收端以同樣的 PNS 序列解調變為：PN(t) ⊕ PN(s) ⊕ S(t) = S(t)

(f) 又 XOR 的真值表為：

0 ⊕ 0 = 0　　0 ⊕ 1 = 1　　1 ⊕ 0 = 1　　1 ⊕ 1 = 0

表示任何數 XOR 自己的結果是 0（PN(t) ⊕ PN(s) = 0），任何數和 0 執行 XOR 命令的結果不會改變原來的值（0 ⊕ S(t) = S(t)）。因此傳送端將傳送訊號和虛擬雜訊序列以 XOR

方式調變後發送出去，接收端受到訊號後也以同樣的虛擬雜訊序列執行 XOR 方式調變，便可得到原來的傳送訊號。

圖 15-6 為 DSSS 的編碼範例，假設傳輸資料 A（傳輸速率為 1/T）與 PNS 訊號 B（頻寬為 1/Tc）經過 XOR 調變後，成為傳輸訊號 C，此時便將傳輸訊號展開到 PNS 訊號上（T > Tc）（如圖 15-6 (a) 所示）。接收端將訊號再經過同樣的 PNS 序列調變，便會回復原來的輸入訊號，如圖 15-6 (b) 所示。在圖 15-6 中，展頻後頻寬是 PNS 頻寬的倍數，亦即 fc = T/Tc，此頻寬又稱為 Chip-Rate，如本範例之 fc = 4，一般稱為 4-chip 的展頻碼。

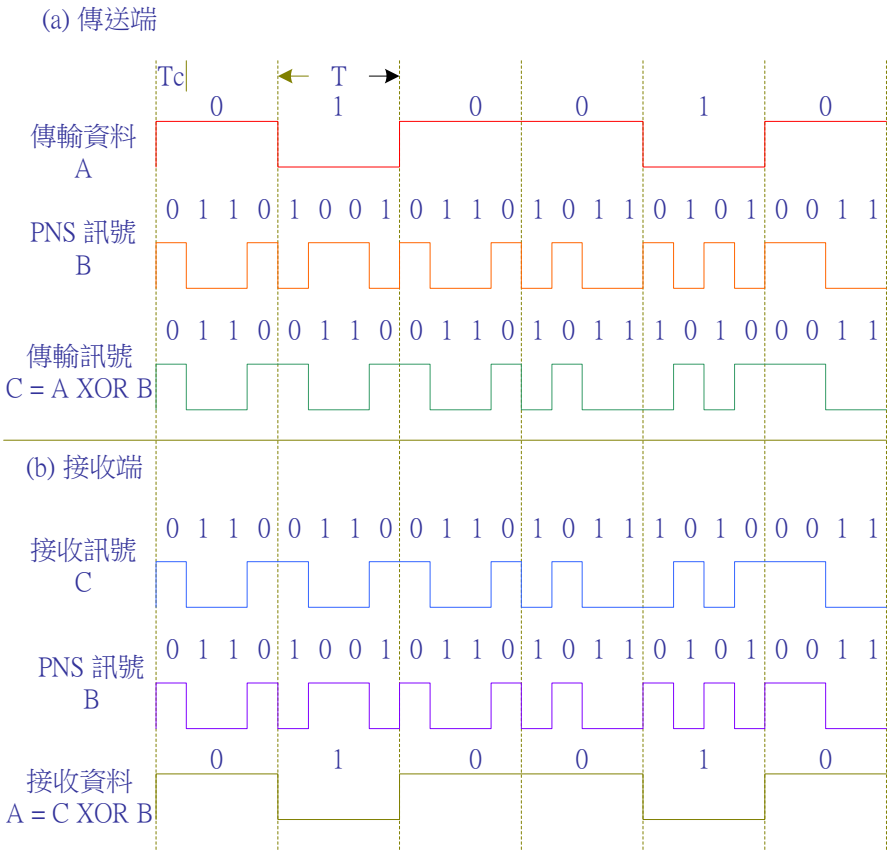

圖 15-6 DSSS 的編碼及解碼範例

圖 15-6 僅說明 DSSS 的基本原理，一般在無線傳輸方面，都必須將傳輸訊號（數位訊號）調變到某一個載波頻道上，而以類比傳輸技術來發送及接收訊號。比較完整的 DSSS 調變功能可如圖 15-7 所示，輸入數位資料經由 BPSK（Binary Phase-Shift Keying）調變後成一類比訊號，再和虛擬雜訊序列調變後，展開成較寬的頻譜（展頻功能）再發送出去。圖 15-8 為圖 15-7 中每個功能步驟的輸出波形。

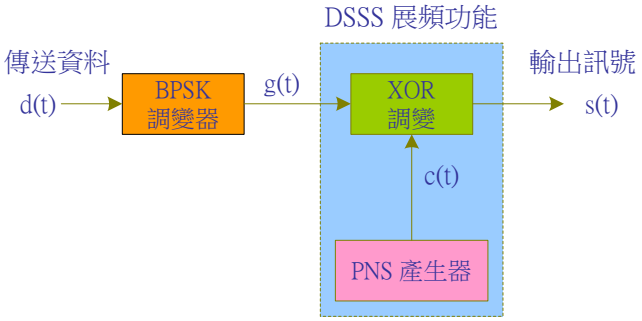

圖 15-7 BPSK 經由 DSSS 展頻的功能圖

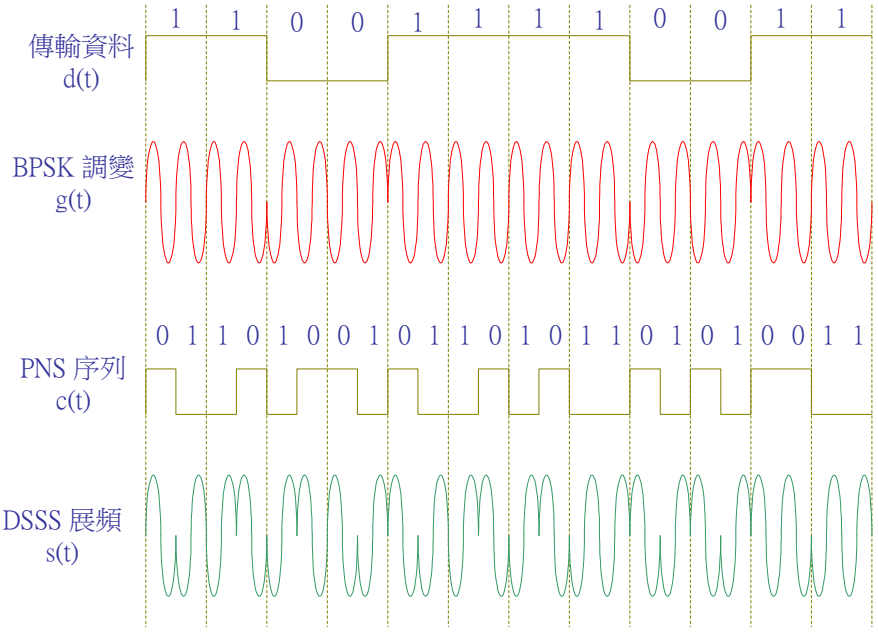

圖 15-8 BPSK 經由 DSSS 展頻之訊號變化圖

圖 15-8 為 BPSK 調變技巧，每一個訊號變化可承載一個位元，但 DSSS 展頻傳輸一般都使用在高傳輸速率上，而編碼技術大多採用 QAM (Quadrature Amplitude Modulation)，每個訊號變化可以承載 8 個位元 (256 QAM) 以上 (請參考第十四章 ADSL 部份)，傳輸速率可達 10 Mbps 以上。

以上介紹了 FHSS 和 DSSS 兩種展頻技術，接下來，我們來討論兩者的差異。如以單一頻寬來比較，由於 DSSS 每個頻道在傳輸訊號時，所使用的頻寬 (22 MHz) 遠大於 FHSS 的頻寬 (1 MHz)，一般而言，頻寬愈寬表示可承載的傳輸速率愈高，因此，DSSS 可獲得的資料傳輸速率大於 FHSS 展頻傳輸。

接下來比較兩者對於『**多重路徑訊號**』(**Multi-Path Fading**) 的解析能力。首先來介紹何謂『多重路徑訊號』？如圖 15-9 所示，當傳送端發送訊號之後，訊號在空中以發散方式傳

播出去，各個發散電波也許會經由折射、反射或延遲，以不同的路徑到達接收端。因此有可能接收端所收到多筆訊號都是同一筆訊號所產生的，這就是多重路徑訊號。接收端如何去分辨與過濾掉其他較弱的訊號，而只接收較強的一筆訊號即可，這就是多重路徑訊號需具解析能力的原因。在這方面，由於 DSSS 使用較寬的頻寬來傳遞訊號，當遇到多重路徑干擾時，由於干擾訊號大於展頻訊號頻寬的機率不大，因此訊號傳遞也不會被中斷。但在相同情況下，FHSS 則會因為多重路徑干擾的影響而造成部份訊號被中斷；當訊號無法傳遞時，系統會被要求重送；如果重傳的頻率很高時，整個系統運作的效能就會大大降低。

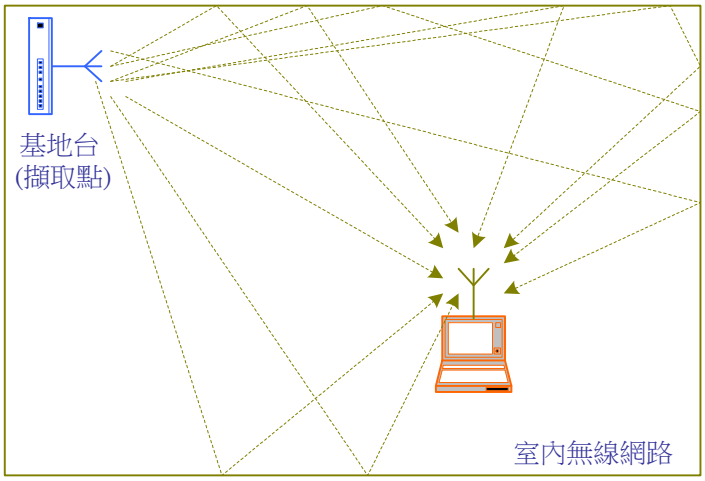

圖 15-9 多重路徑訊號

對於頻帶（如 2.4GHz 頻帶）使用率而言，FHSS 則充分運用了頻道的資源。由於 FHSS 是以跳越形式的相位差異來區分不同的通訊連線，因此可以充分運用 2.4 GHz 頻帶的所有頻寬。然而 DSSS 是以不同頻道來區別不一樣的無線連線，加上展頻後的訊號頻寬高達 22 MHz，在考慮同頻及鄰頻的干擾情況下，整個 2.4GHz 的頻帶只能劃分出三個完全不會互相干擾、且可同時使用的頻道（各個國家規範有所不同），這三個群組頻道之間，至少必須相隔 25 MHz 以上，無形中浪費許多可使用的頻道。

15-2-4 多重存取技術

無線電（Radio）傳輸的**『多重存取』（Multiple Access, MA）**技術有下列幾種類型：

(1) 『分頻多重存取』（Frequency Division Multiple Access, FDMA）：主要是將可用的頻

段劃分成若干個頻道，不同使用者同時使用各自的頻道來通訊，以達到多重存取的目的。

(2) 『分時多重存取』(Time Division Multiple Access, TDMA)：TDMA 是將時間分個為若干個時槽（Time Slot），使用者在不同時槽裡，使用所有的頻道來通訊，以達到多使用者通訊的目的。

(3) 『分碼多重存取』(Code Division Multiple Access, CDMA)：CDMA 是不分割頻道與時間，使用者之間以不同的通訊語法來通訊，就好像許多人在同一空間內，以不同語言方式來溝通一樣，雖然同一時間及頻道有許多人在發言，但可由不同語言來分辨交談的對象。

(4) 『分域多重存取』(Space Division Multiple Access, SDMA)：分域多重存取是利用天線及信號處理的技巧，來分辨空間上不同位置但可能同時使用相同頻率及編碼方式的使用者。

(5) 『混合式多重存取』(Hybrid Multiple Access, HMA)：混合式的多重存取有混合分頻及分碼的 FCDMA(Frequency –Code Division MA)，以及混合分時及分碼的 TCDMA（Time –Code Division MA）等。

有關 FDMA 與 TDMA 部分，本書第二章已詳細介紹過，這裡只針對無線區域網路較常用的 CDMA 加以介紹。

CDMA 是一種多工技術，主要應用於展頻傳輸上。我們可以回顧一下 FHSS 和 DSSS 兩種展頻技術，它們的展頻技巧都是利用**『虛擬雜訊序列』(PNS)**將傳輸信號展開到較寬的頻譜上，傳送端和接收端以相同的虛擬雜訊序列來互相辨識對方的通訊。如果欲達到多重存取的目的，便需要產生多個虛擬雜訊序列讓不同的使用者使用，通訊雙方皆用各自的虛擬雜訊序列來互相辨識。也就是說，對每一個通道都必須給予一個獨立的虛擬雜訊序列，而此虛擬

雜訊序列是一連串的 0 或 1 字碼所構成，也稱之為『**數碼**』(**Code**)；而不同通道皆只以各自的數碼（Code）來通訊，因此稱之為『**分碼多重存取**』(**Code Division MA, CDMA**)。

圖 15-10 為 CDMA 應用在 DSSS 展頻環境下的概略圖，假設網路中有 k 個工作站，每個工作站皆有一獨立的虛擬雜訊序列（cn(t), n = 1, 2, .., k），發送端和接收端以相同的 PNS 序列來辨識雙方的通訊訊息。譬如，接收端以 c1(t) 序列來解調變出 d1(t) 的訊號。

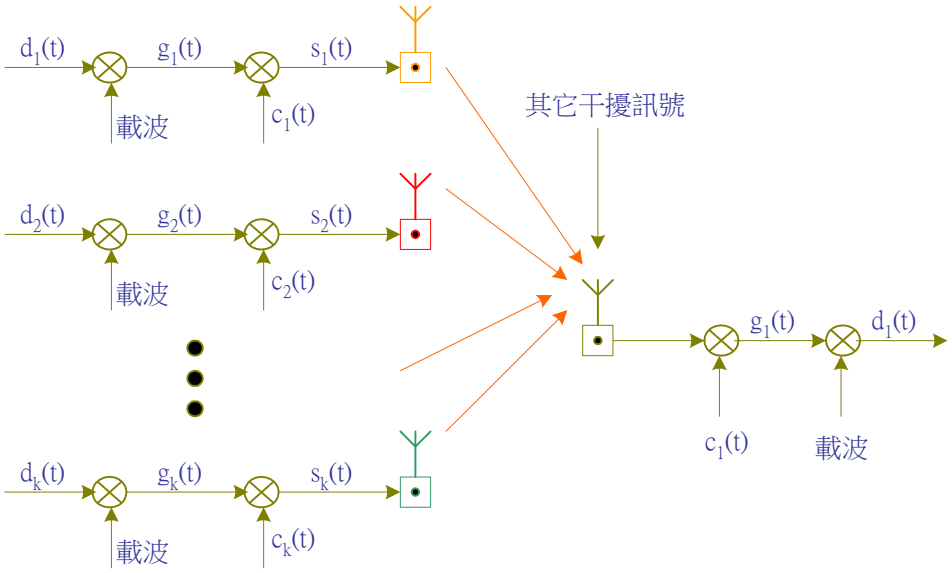

圖 15-10 CDMA 在 DSSS 上的應用環境

15-2-5 紅外線傳輸技術

『**紅外線**』(**Infrared, IR**)傳輸是以『**光**』(**Optical**)做為傳輸媒介，這與前面所述的無線電波（Radio）傳輸技術有很大的不同點。一般而言，可見光的波長大致上是介於 400（藍光）～700（紅光）nm 之間，只要光的波長大於 700 nm，就屬於紅外線的範圍了，因此，紅外線的頻譜相當的寬廣，要發展出高傳輸速率的無線網路環境也比較容易。一般紅外線網路所採用的波長都介於 850～900 nm 之間，如圖 15-11 所示。

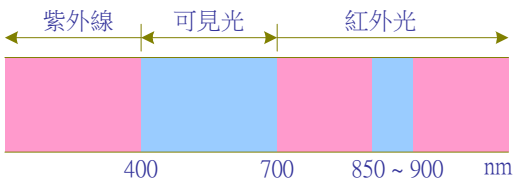

圖 15-11 紅外線傳輸的波長

另外，紅外線的頻譜完全不受管制，不像無線電波網路，除了特定的頻段(如 ISM 頻帶) 可以不受管制外，其餘頻帶在使用之前都必須經過申請核准後才可使用。由於光無法穿透障礙物，因此紅外線網路可以被限制在特定範圍之內，不必像無線電波必須防範不明人士的竊聽行為。再者，只要是在不同房間，也不用擔心不同的無線網路之間互相干擾。但是紅外線也有缺點，由於紅外線容易受到燈光及日光燈的干擾，因而易造成傳輸距離的縮短；一般的做法是將輸出功率加大，以克服其他光源的干擾。

一般將利用紅外線所構成的網路稱之為**『IR/DA』(Infrared Data Association)**，目前紅外線傳輸大致有下列三種模式：

(1) 『直接光束 IR』(Direct Beam IR, DB/IR) 模式：表示紅外線僅能夠做直線方向傳遞，其原因為光無法經過折射或反射來傳導，發送端和接收端之間必須完全對應在同一**『視線』(Line of Sight)** 上傳輸。另一方面，光若集中在某一方向傳遞，其能量較不容易發散掉，如此也能延伸傳遞的距離。因此，DB/IR 大多是應用於建築物之間的點對點 (Point-to-Point) 連線使用，之間的傳輸距離也可達數公里；但它並不適合室內無線網路或移動式 (Mobile) 接收器使用。

(2) **『全向性 IR』(Ominidirectional IR, Omini/IR) 模式**：在 Omini/IR 模式中，必須有一台全向性的基地台(Base Station)，而發射出方向性較為廣泛的紅外線。無線裝置(如移動式 Notebook 電腦) 只要對準該基地台，便可以透過基地台和無線網路通訊，如圖 15-12 所示。基地台和無線裝置之間也是以『視線』方向通訊，之間如有任何障礙也會阻擋紅外線通過，並將使通訊中斷。Omini/IR 模式在一般無線網路上應用也非常普遍，每一個基地台所負責傳遞的區域稱之為**『細胞區域』(Cell Zone)**，一個無線網路所涵蓋的地區可由多個全向性基地台來構成。

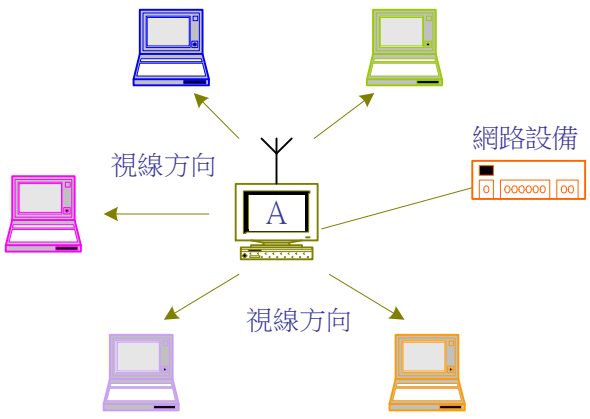

圖 15-12 Omini/IR 模式的傳遞方式

(3)『散射式 IR』(Diffused IR, DF/IR)模式：DF/IR 模式表示發射的紅外線經過折射後，仍然可以通訊，也就是說，發射與接收設備之間不需要是『視線』方向，兩者位置之間也不需要完全淨空才可通訊，這種特性非常接近無線電波的傳輸，但 DF/IR 只能侷限於同一房間內才可以通訊。

紅外線傳輸原理如同無線電波一樣，必須利用編碼技術將資料調變成訊號，再附加到載波頻率上，發送訊號時再將載波訊號轉換成紅外線發送出去，其調變技術一般都採用**『脈衝位置調變』(Pulse Position Modulation, PPM)**。以 IEEE 802.11 (1 Mbps DF/IR) 為範例，它是採用 16-PPM (PPM with 16 Positions) 的調變技術，這種調變技術是利用 4 bits 的資料位元分別表示 16 種調變記號 (Symbols)，表示方法如表 15-1 所示。每筆資料的符號變化： 1 表示較高的發射能量； 0 表示能量較低。圖 15-13 為每一調變符號的週期，分為 16 個間隔時間，每一間隔時間如表 10-4 中的調變記號，而間隔時間為 250 us，也就是說，每 16 個間隔時間 (16 × 250 ns) 傳遞 4 個位元，因此其傳送速率計算如下：

傳輸速率 = 4 / (16 × 250 × 10-9) = 1 × 106 = 1 Mbps

表 15-1 16-PPM 調變記號表

資料位元	16-PPM 調變記號
0000	0000000000000001
0001	0000000000000010
0011	0000000000000100
0010	0000000000001000
0110	0000000000010000
0111	0000000000100000
0101	0000000001000000
0100	0000000010000000
1100	0000000100000000
1101	0000001000000000
1111	0000010000000000
1110	0000100000000000
1010	0001000000000000

1011	0010000000000000
1001	0100000000000000
1000	1000000000000000

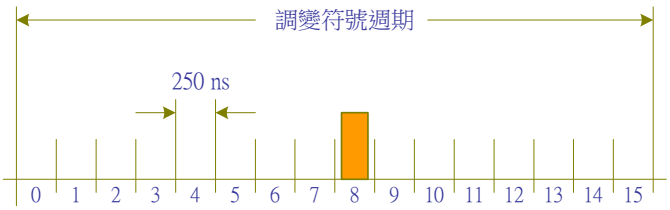

圖 15-13 16-PPM 的調變模式（傳送 0100 資料）

如以 IEEE 802.11 的 2 Mbps DF/IR 標準，係採用 4-PPM（PPM with 4 Positions）調變技術，利用 2 bits 的資料位元分別表示四種調變記號，如表 15-2 所示。如同圖 15-13 一樣，每個調變記號間隔時間為 250 ns，每 4 個間隔時間（4 × 250 ns）傳送兩個位元，則其傳輸速率計算如下：

傳輸速率 = 2 / (4 × 250 × 10-9) = 2 × 106 = 2 Mbps

表 15-2 4-PPM 調變記號表

資料位元	4-PPM 調變記號
00	0001
01	0010
11	0100
10	1000

15-3 IEEE 802.11 系列規範

1997 年『美國電機電子協會』（Institute of Electrical and Electronics Engineer, IEEE）公佈了 IEEE 802.11 『無線區域網路』（Wireless LAN, WLAN）標準；1999 年更進一步提出 IEEE 802.11 的延伸規格：IEEE 802.11a（5 GHz 頻帶，最高頻寬 54 Mbps）和 IEEE 802.11b（2.4 GHz 頻帶，11 Mbps），這兩個延伸規格讓無線網路的速度可以和有線網路相抗衡，更增加了無線網路的競爭力。也因為頻寬的增加，使得一些網路的應用可以推展到無線網路上，譬如視訊會議、網路電話等。到了 2001 年底，6 ~ 54 Mbps 的 IEEE 802.11g 草案被提出來，

這個草案規範中有一個很大的特性，就是可以和目前流行的 IEEE 802.11b 相容（這與 IEEE 802.11a 無法與 IEEE 802.11b 相容有很大的不同），同時又利用與 IEEE 802.11a 類似的技術達到更高的頻寬。表 15-3 是 IEEE 802.11 系列規範，先讓大家有一個概略印象，接下來再探討它們的網路技術。

表 15-3 各無線區域網路標準

標準	頻帶	傳輸速率	展頻技術	調變技術	傳輸距離
IEEE 802.11	2.4 GHz	2 Mbps	DSSS/FHSS	BPSK/QPSK	100 公尺
IEEE 802.11b	2.4 GHz	11 Mbps	DSSS	BPSK/QPSK	100 公尺
IEEE 802.11a	5 GHz	54 Mbps	OFDM	QPSK/QAM	50 公尺
IEEE 802.11g	2.4 GHz	54 Mbps	DSSS	CCK/OFDM	100 公尺

15-3-1 網路特性

IEEE 802.11 主要目的是在現有的區域網路之下，另外制定一套無線區域網路的規範，這方面相當於 IEEE Project（請參考第七章介紹）中的『媒介存取層』（Medium Access Control, MAC）部份。我們先來探討 IEEE 802.11 的標準規範後，再來介紹其延伸規格（802.11a 與 802.11b）所增加的功能。IEEE 802.11 家族的特性歸類如下：

(1) 傳輸速率：1 Mbps、2 Mbps、11 Mbps（IEEE 802.11b）、54 Mbps（IEEE 802.11a）。

(2) 訊框：IEEE 802.11 訊框。

(3) 傳輸媒介：無線電波（2.4 GHz 及 5 GHz 頻帶）或紅外線（850～900 nm）。

(4) 通訊協定：『載波感測多重存取附碰撞避免』（Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA）。它的工作模式非常類似 CSMA/CD，當有兩個或兩個以上的工作站同時傳送訊框而發生碰撞時，都會將已碰撞的訊框拋棄，雖然 CSMA/CA 採另一種工作模式來避免發生碰撞的機會，但仍無法保證不會發生碰撞。

(5) 傳輸模式：IEEE 802.11 採用**『分散式協調功能』（Distributed Coordination Function, DCF）**和**『集中協調功能』（Point Coordination Function, PCF）**等兩種傳輸模式。DCF 模式是由工作站之間利用 CSMA/CA 方式來取得傳輸媒介（頻帶）的使用權；而 PCF 是由網路上的集中控制器來分配各個工作站使用傳輸媒介的優先次序。

(6) 提供『認證』(Authentication) 及『資料隱密』(Privacy) 的功能：無線電波是一種開放性的傳輸媒介，任何人都可以容易的入侵或竊聽網路，認證是防止入侵並確認使用者身分；而資料隱密則是預防傳輸中資料被竊聽的加密措施 (Cipher)。

15-3-2 協定堆疊

如同其他區域網路的通訊協定(如 IEEE 802.3)一樣，IEEE 802.11 也是屬於 IEEE 802 系列協定標準中的 MAC (Medium Access Control) 層 (如第七章介紹)，同樣包含了傳輸媒介 (無線電波或紅外線) 的介面標準。圖 15-14 為 IEEE 802.11 的協定堆疊，上層的通訊協定也是連結**『邏輯鏈路控制層』(Logical Link Control, LLC)**，合乎 IEEE 802 系列的連結規範。在 IEEE 802.11 協定中包含了 MAC 層與 PHY (Physical Layer) 層兩大部份，MAC 層包含**『無競爭服務』(Contention-Free Service)** 和**『競爭服務』(Contention Service)** 兩種服務，前者是利用集中協調功能 (PCF) 的傳輸模式；而後者是利用分散式協調功能 (DCF)；另外，集中式協調功能也需透過分散式協調功能的介面服務來達成。另外，PHY 層制定了各種傳輸技巧。

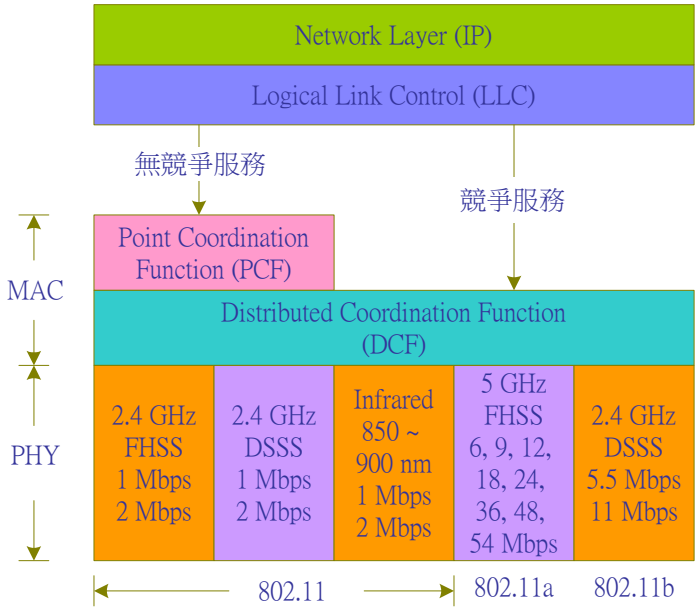

圖 15-14 IEEE 802.11 協定堆疊

如圖 15-14 所示，不同協定皆有各自的實體層規範，802.11 和 802.11b 都採用 ISM 2.4 GHz 頻帶，而 802.11a 是採用 5 GHz U-NII (Unlicensed National Information Infrastructure) 頻帶，在調變技術上也會有所不同。

5-3-3 網路實體架構

IEEE 802.11 基本上提供了『**對等架構**』(**Ad Hoc**)與『**基礎架構**』(**Infrastructure**)兩種網路連結型態。所謂『對等架構』表示網路之中並沒有一部主控制站，各個工作站之間都以『端對端』(Pear-to-Pear)模式互通。也就是說，在這個模式之下不需要『擷取點』(Access Point, AP)，各端點的地位是相等的，如圖 15-15 所示【備註：Access Point 有許多不同的譯詞，如：基地台、擷取點或無線橋接器】。

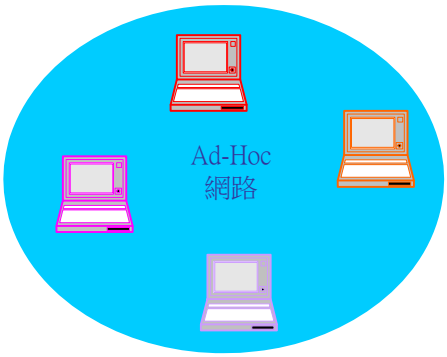

圖 15-15 Ad-Hoc 無線區域網路架構

圖 15-16 為『基礎架構』的 WLAN 網路，網路主要的特點是透過『擷取點』來和現有的有線網路(如 Ethernet 網路)相結合。擷取點可發射功率較強的電波，各個無線連結的電腦只要能接收到擷取點所發射的電波，便可連結上網路，此即表示網路的涵蓋範圍可較廣。

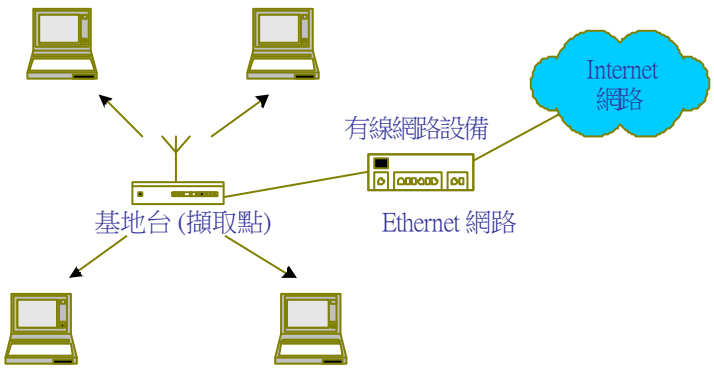

圖 15-16 有基礎架構的無線區域網路

一般而言，無線區域網路並不像圖 15-15 和 15-16 那麼單純，反之它會隨著不同的環境延伸出多種網路型態，為了使讀者能更瞭解網路實體架構，我們先針對下列相關元件做一簡單的說明：

(1) 工作站（Station, STA）：只要配備有符合 IEEE 802.11 實體層及媒介存取層的任何設備，均可稱為工作站。

(2) 擷取點（Access Point, AP）：提供無線網路連接至分散式系統（其他有線網路）的連結設備，並提供所有無線工作站的存取連結。

(3) 基本服務集（Basic Service Set, BSS）：在幾何空間上，一個基本建構區塊內所有工作站的集合，稱為一個基本服務集。一般都將一個擷取點（或稱基地台）所能涵蓋的範圍稱為一個基本服務集。

(4) 分散式系統（Distributed System, DS）：基本上都是由有線網路來構成，但該網路有提供無線網路連結的相關服務，並能將若干個基本服務集整合在一起。

(5) 擴充服務集（Extended Service Set, ESS）：由分散式系統連結若干個基本服務集所構成。

比較圖 15-15 與圖 15-16 兩種架構，雖然兩者的範圍都在一個基本服務集之內，但圖 15-15 是由多個工作站之間互相通訊而成，而圖 15-16 所呈現的則是連結到一個分散式系統環境的無線網路，此分散式系統是由一般有線網路（如 Ethernet 網路）所構成。通常一個無線區域網路並無法由一個基本服務集建構而成，因為一個基地台所能涵蓋的範圍大多僅在 100 公尺範圍內，因此，必須結合若干個基本服務集來擴充網路範圍。

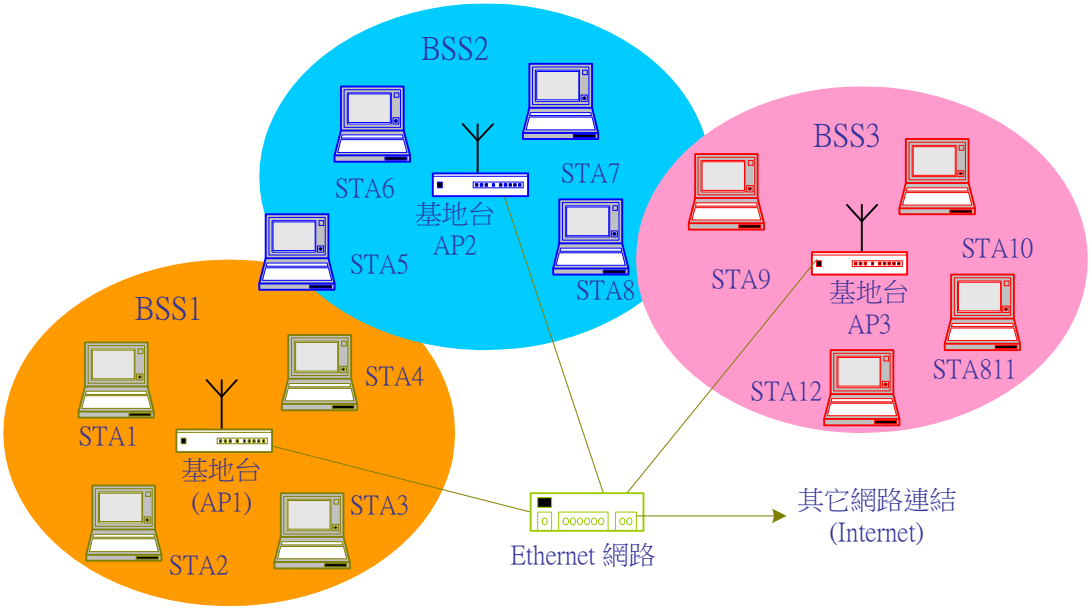

圖 15-17 無線區域網路架構

圖 15-17 是一般 WLAN 的架構圖，整個網路是由多個基本服務集所構成，每個服務集都有一個擷取點（AP）來負責無線電腦和有線網路之間的連結，每一基本服務集所能涵蓋的範圍大多在 100 公尺以內（視不同規範而定），服務集之間都必須互相重疊。網路內任何電腦都可在網路範圍內移動，譬如 STA5 工作站原來是連結到 BSS1 的擷取點，當它移動至超出 BSS1 的範圍邊緣時，便會發現所接收來自 AP2 的訊號漸漸比 AP1 強，因此，STA5 便轉向 AP2 要求連線；如經 AP2 同意連線後，STA5 便放棄 AP1 的連線，而轉由 AP2 服務。無線工作站在這擴充服務集內通訊，必須在多個基本服務集之間交換服務基地台，這個交換服務的行為稱之為『游牧』（Wandering）（逐水草而居的意思）。

圖 15-17 中各個擷取點之間的連線是透過一般有線網路（如 Ethernet 網路）來達成，許多地區為了克服環境因素，也會採用無線寬頻（如 HiperAccess）來連結，但無論如何，WLAN 還是會限制在某一範圍內通訊，並不像行動電話通訊那麼複雜。

15-3-4 網路服務架構

網路服務架構表示整個網路的運作系統，IEEE 802.11 將 WLAN 的運作模式區分為**『工作站服務』（Station Service, SS）**和**『分散式系統服務』（Distributed System Service, DSS）**兩大類，但規範中並沒有規定這兩大類的服務系統的實現標準，而僅描述其應具有的功能；不過也需要具備這些功能，才能建構一個完整的無線區域網路。兩大類的服務功能如下：

(1) 工作站服務（SS）：是由工作站所提供的服務。此類服務可使工作站具有正確傳送與接收訊框的能力，且為考慮傳輸資料的安全性，並包含有**『身分確認服務』（Authentication）**與**『隱密性服務』（Privacy）**等兩種服務。

(2) 分散式系統服務（DSS）：此類服務是由分散式系統所提供，主要功能是使 MAC 訊框能在不同 BSS 之間傳送。在無線網路上，無論工作站移動到任何位置，都要使工作站的資料傳送與接收能保持通暢；此項功能大多是由**『擷取點』（Access Point, AP）**來負責工作站之間的呼叫及轉送。擷取點同時也是無線工作站和有線網路之間的橋樑，因此，也將它稱為『橋接器』（Bridge）。分散式系統提供下列服務：

(a) 聯結服務（Association）
(b) 取消聯結服務（Disassociation）
(c) 分送服務（Distribution）

(d) 整合服務（Integration）

(e) 重聯結服務（Re-association）

圖 15-18 為無線區域網路服務的邏輯概念圖，是由一分散式系統結合 IEEE 802.x 的有線網路和 IEEE 802.11 無線區域網路，其中無線區域網路是由兩個 BSS 網路所結合而成的 ESS。工作站在無線網路上的任何移動，都可能需要不同的聯結服務，在未討論各種服務之前，先來探討『**移動性**』(**Mobility**) 的觀念，有下列三種情況：

(1) 無變動：表示工作站的移動還是停留在原基本服務區 (BSS) 內，譬如 STA1 保持在 ESS1 內移動。

(2) 基本服務區的變動：表示工作站由一個基本服務區移動到另一個基本服務區，但仍然在同一擴充服務區（ESS）內，譬如 STA1 移動到 BSS2 範圍內。

(3) 擴充服務區的變動：表示工作站由一個擴充服務區的基本服務區移動到另一個擴充服務區內，譬如 STA1 移動到 ESS1 的範圍之外，由其他的 ESS 管轄區來服務。

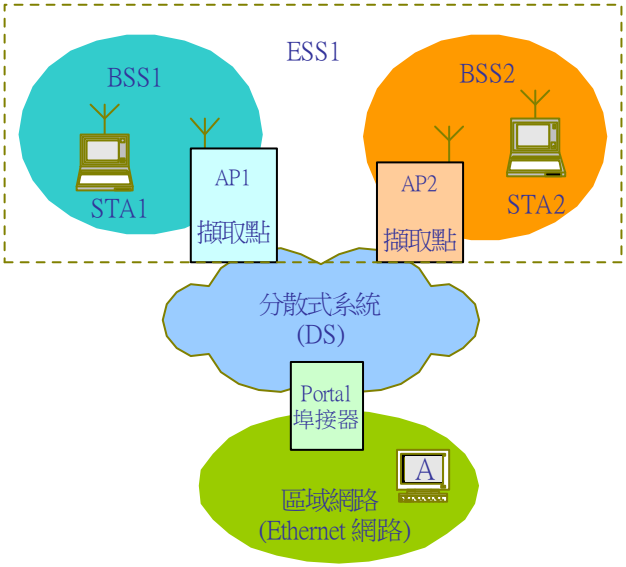

圖 15-18 無線區域網路的服務架構

有了上述的基本概念後，接下來，我們將分散式系統所提供七種服務的功能介紹如下：

(A) 分送服務（Distribution Service）

『**分送服務**』的主要工作是將分散式系統中所傳送的資料送到適當的地方。如圖 15-18 中，若 STA1 欲傳送資料到 STA2，首先得將該筆訊框發送給 AP1(稱為輸入擷取點)，再由 AP1 轉送給 AP2（稱之為輸出擷取點），AP2 才將訊框傳送給 STA2。在 IEEE 802.11 中並沒有

制定如何轉送的規範，但它制定有『聯結』、『取消聯結』和『重新聯結』等服務，來達成分送服務的功能。

(B) 整合服務（Integration Service）

『整合服務』的功能是要將 WLAN 和現存的有線網路(如 Ethernet 網路)整合在一起，也就是說，所傳送的訊框能在無線網路與有線網路之間流通。如圖 15-18，擷取點（AP）是連接無線網路和分散式系統的介面，而埠接器（Portal）是分散式系統和有線網路之間的連接器。當一筆訊框被發送出來時，分散式系統必須判斷應該將它轉送到擷取器或埠接器；另外，埠接器也須有能力進行 IEEE 802.11 和有線網路之間的位址格式轉換，這就是整合服務所須提供的功能。

(C) 聯結服務（Association Service）

『聯結服務』的功能是要在工作站和擷取點之間建立一條通訊連線。一般無線工作站啟動後，便會尋找最近的擷取點來要求連線，連線後擷取點上便會登錄該工作站的位址。唯有在工作站登錄位址之後，分散式系統在轉送訊框時，才知道該工作站是屬於哪一個擷取點所管轄。又如果有任何訊框傳送給該工作站時，分散式系統也才會將該訊框轉送到適當的擷取點上。一部無線工作站僅能夠和一個擷取點建立連線，亦即僅能向一部擷取器登錄。但一個擷取點上可能會登錄多部工作站位址，這些工作站也都屬於同一基本服務區（BSS），這也是擷取點發送或接收訊框時主要的依據。如果同一基本服務區的工作站之間要互相通訊，便不需要發送到分散式系統上；另外，不屬於本服務區的工作站位址，也不需要接收及轉送（類似橋接器的過濾功能）。

(D) 重新聯結服務（Reassociation Service）

『重新聯結服務』的主要功能是將移動中的工作站由一個擷取點轉移到另一個擷取點。當工作站由一個基本服務區移到另一個基本服務區，便會啟動重新聯結服務，此服務會在工作站和新區域的擷取點之間建立一個通訊連線，並將工作站資料登錄到新的擷取點上。此項工作大多由工作站來完成。

(E) 取消聯結服務（Disassociation Service）

當工作站傳送資料結束後，可以啟動『取消聯結服務』來中斷和擷取點之間的連線。另外，當一部工作站由一個基本服務區移動到另一個服務區時，也會向原服務區的擷取點要求『取消聯結服務』，並向新服務區的擷取點要求『重新聯結服務』。此項服務可以是由工作站或擷取點來啟動，但不論哪一方啟動，另一方都不能拒絕。取消聯結服務也可能發生在網路太過忙碌的情況，此時擷取點可要求工作站暫時取消連線服務。

(F) 認證服務（Authentication Service）

『認證服務』是用來確認每一工作站的身分。IEEE 802.11 支援兩種認證方法：『開放系統認證』（Open System）及『盤問/回應』（Challenge/Response）。認證服務通常是要求雙向式的身分認證，一個工作站可以同時和多個工作站（包含擷取點）之間作身分確認。

(G) 隱密性服務（Privacy Service）

『隱密性服務』是為了避免傳輸中的資料被竊聽，而實施的加密和解密服務。無線網路的訊號在空中傳播，任何工作站只要有 IEEE 802.11 的網路卡，都能輕易地由空中竊取到傳輸中的資料。IEEE 802.11 制定一個『有線等效保密演算法』來實現隱密性服務。

15-4 IEEE 802.11 MAC 協定

IEEE 802.11 又稱為『無線乙太網路』（Wireless Ethernet），這是因為 802.11 的存取技術與 Ethernet 網路非常相似。Ethernet 的 MAC 協定是 CSMA/CD（Carrier Sense Multiple Access with Collision Detection）；而 802.11 是『載波偵測多重存取附碰撞避免』（Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA），兩者之間的運作模式非常接近。它們的基本原理都是在一個多重存取的環境下，制定一個標準的競爭模式，而各個工作站就依照此競爭模式來取得傳輸媒介（有線媒介或無線電波）的使用權。CSMA/CD 的運作是在一個有線的傳輸媒介（同軸電纜）上，工作站比較容易偵測到所發送的訊號是否有和其他工作站碰撞；但在無線網路的環境裡，要偵測訊號是否有和其他工作站碰撞可就難了，因此，IEEE 802.11 採用另一種運作模式來避免工作站之間發生碰撞，這個模式就是 CSMA/CA 通訊協定。

15-4-1 CSMA/CA 協定

圖 15-19 為 CSMA/CA 的運作模式，首先發送端會去偵測網路（或環境），假如頻道中沒有其他訊號傳遞時，發送端會再等待一段隨機時間，在這段時間過後，如果還是沒有偵測到任何信號在傳遞，發送端就會將封包傳送出去。假如一開始就偵測到有訊號使用了這個頻道，發送端會等到頻道淨空之後、再等待一個隨機的後退（Backoff）時間，才重新進入頻道的競爭模式。由此可見 CSMA/CA 和 CSMA/CD 的運作有一個關鍵性的不同點：在 CSMA/CD 運作下的工作站，如偵測到網路是淨空時，立即將訊框發送到網路上，再來偵測是否有和其他工作站發生碰撞；而 CSMA/CA 則是先等待一段時間之後，再判斷網路是否真正淨空，最後才決定是否發送資料，如此來儘可能避免碰撞的發生。

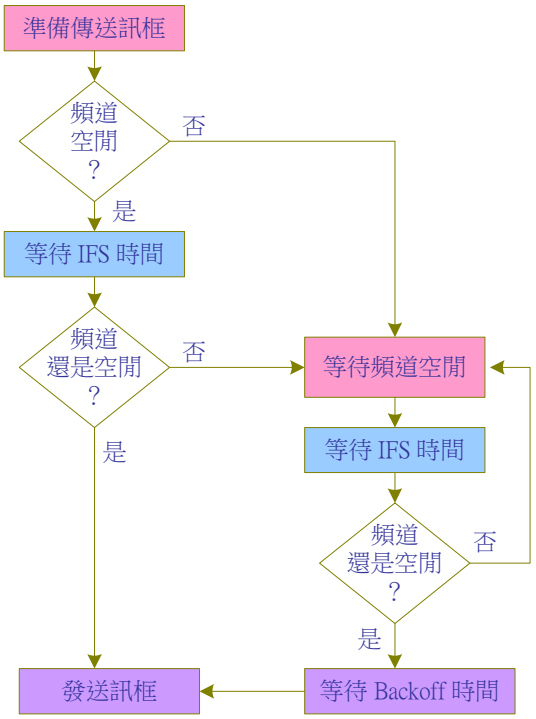

圖 15-19 CSMA/CA 運作模式

當發送端偵測出頻道空閒時，都會再等待一段時間之後，再來偵測頻道是否還是保持空閒，這段時間稱之為**『訊框間隔』（Interval Frame Space, IFS）**。IEEE 802.11 利用不同長度的 IFS 時間，來分辨它所提出兩種傳輸媒介的擷取方式：

(1) 分散式協調功能（Distributed Coordination Function, DCF）

(2) 集中式協調功能（Point Coordination Function, PCF）

所謂**『協調功能』（Coordination Function）**是指用什麼機制來決定工作站可以使用傳輸媒介的時機。**『分散式協調功能』（DCF）**是所有工作站利用 CSMA/CA 協定，由競爭模式取

得傳輸媒介的機制。而『**集中式協調功能**』(**PCF**)是表示網路上有一個『集中協調站』(Point Coordination)，由它來輪詢(Polling)所有工作站，看看是否有資料準備傳送；而被詢問到的工作站就可以取得傳輸媒介來傳輸資料。因此，IEEE 802.11 的 MAC 協定就有『無競爭式服務』(Contention-Free Server)和『競爭式服務』(Contention Service)兩種。圖 15-20 為 IEEE 802.11 的兩種服務模式，要特別注意的是 PCF 必須要透過 DCF 才能實現出來，也就是說，無競爭服務是經由集中協調站決定出哪一個工作站(屬於無競爭工作站群組)取得傳輸的優先權之後，再以競爭式服務取得傳輸媒介的使用權。這也表示在一個 WLAN 上允許無競爭式服務與競爭式服務同時存在，而各自有其工作站群組。

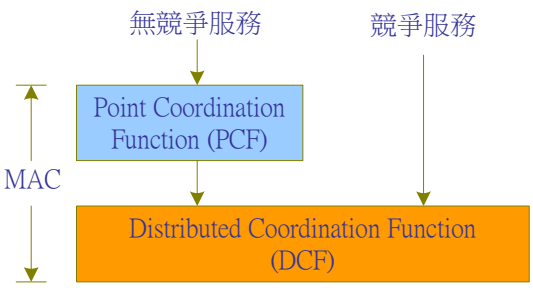

圖 15-20 分散式與集中式協調功能

15-4-2 基本存取機制

圖 15-21 為 MAC 的基本存取機制，其中包含 DCF 與 PCF 兩種傳輸模式。至於如何來區分 DCF 和 PCF 之間取得傳輸媒介的時機，乃依照『訊框間隔』(Interval Frame Space, IFS)的長短來辨識。 IEEE 802.11 利用 IFS 的長短將訊框區分為三種不同優先等級，每一種優先等級的訊框在傳送之前，都必須等待一段固定大小的 IFS 時間。在 IEEE 802.11 標準之下，有下列四種 IFS 格式(如圖 15-21)：

(1) 短訊框間隔(Short Interval Frame Space, SIFS)：此間隔時間是用來做立即回應的訊框使用，屬於 SIFS 等級的訊框有：**『允許傳送』(Clear to Send, CTS)**、**『確認回覆』(Acknowledge, ACK)** 或 **『輪詢回應』(Poll Response)** 等。

(2) PCF 訊框間隔(PCF IFS, PIFS)：此間隔時間是在無競爭式傳輸服務時，PCF 工作站傳送訊框前所必須等待的時間。

(3) DCF 訊框間隔(DCF IFS, DIFS)：此間隔時間是在競爭傳輸模式下，DCF 工作站傳送訊框前所必須等待的時間。

(4) 延長訊框間隔 (Extended IFS, EIFS): 此間隔時間是工作站進行重送訊框時，所必須等待的時間 (不在圖 15-21 中顯示，容後說明)。

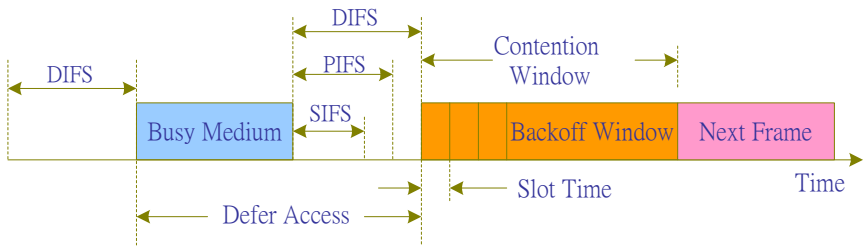

圖 15-21 基本存取機制

當任何一個工作站感測到頻道空閒後，必須等待一個不等的 IFS 間隔時間，隨著間隔時間的長短來區分各種訊框的優先等級，其中 SIFS < PIFS < DIFS < EIFS，這也表示各種訊框的優先權是 RTS/CTS/ACK > PCF > DCF > 重送訊框 (有關 RTS/CTS 容後介紹)。

15-4-3 分散式協調功能

『分散式協調功能』(DCF) 是 IEEE 802.11 最基本的媒介存取機制，在此模式下，所有工作站都以 CSMA/CA 協定來競爭取得媒介 (頻道) 使用權。它的運作方式如圖 15-21 所示，傳送端感測到頻道空閒時，必須再等候一段 DIFS 的間隔時間，如果頻道仍然是空閒著，便可以開始發送訊號。但在網路上可能有多個工作站等待準備傳送資料，它們也都等待了 DIFS 的間隔時間後再發送訊號，因此，雖然經過延遲發送訊號，但不同工作站之間發生碰撞的機率還是很大。解決此問題的方法是，工作站在等待訊框間隔 (DIFS) 後，再等待一段由亂數所產生的時間才將訊框發送出去，因為每個工作站所產生的後退 (Backoff) 時間大多不會相同，所以便可以降低訊框發生碰撞的機率。後退演算法也如同 CSMA/CD 的演算法一樣，都是以某一個**『時槽』(Time Slot)** (容後介紹) 時間為基準，而亂數所產生的數目為時槽時間的倍數，做為後退等待的時間。

至於後退時間的計算，並非每次感測到頻道空閒都必須重新計算，而且每部工作站的後退時間是可以保留使用的。其運作方式如圖 15-22 所示，假設一開始工作站 A 正在傳送資料，而同時工作站 B 和 C 也欲傳輸資料，於是都去感測網路是否空閒 (時段 1)。當工作站 A 傳送完畢後，經過 DIFS 間隔時間，工作站 A、B 和 C 都有資料準備傳送，也各自計算後退時間 (10, 8, 5)。因工作站 C 的後退時間較短 (5)，便優先發送資料 (時段 2)。工作站 C 傳送完後，網路上又出現三個工作站準備競爭取得傳輸媒介，此時工作站 B 所保

留的後退時間為 3（8-5 = 3），較工作站 A（10-5=5）和工作站 D 為短，因此工作站 B 先發送資料，而工作站 A 和 C 必須再等待（時段 3）。下一次換工作站 A 的保留後退時間最短，而先發送資料到頻道上（時段 4）。由上例可以發現，每一工作站所產生的後退等待時間幾乎不可能相同，因此，發生碰撞的機會也較少。採用保留後退等待時間的做法，是希望在這種不公平的競爭模式下，保證每一個工作站都能取得媒介使用權，而不論它隨機所產生的後退等候時間（容後介紹）有多長。

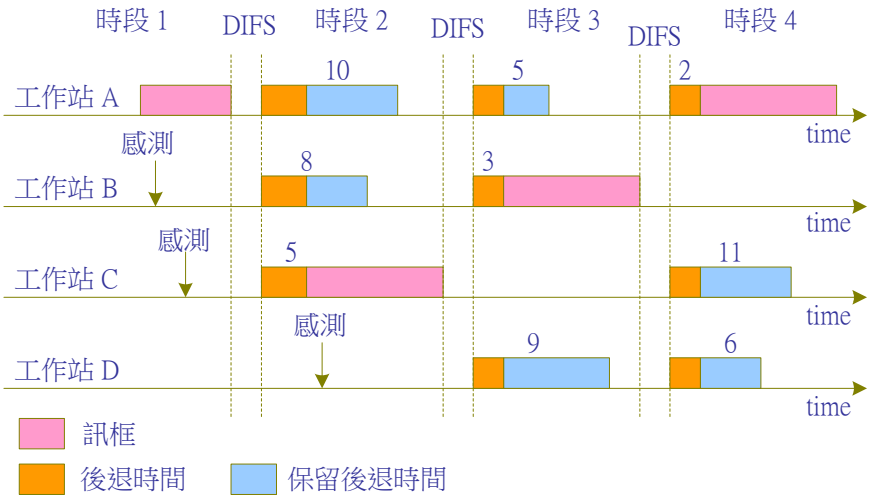

圖 15-22 分散式協調的運作

15-4-4 RTS/CTS 協調功能

在無線網路系統中，除了不容易偵測出碰撞現象外，在載波感測方面，要判斷網路是否真正空閒也同樣非常困難。無論在 DCF 或 PCF 的運作模式下，都不能確定訊框在傳送之中會不會和其他訊框發生碰撞。為了克服此困難，IEEE 802.11 採用「交談式」的傳輸方式，亦即傳送端欲發送訊框給接收端之前，必須尋求對方同意。另一方面，接收端收到訊框後，也必須即時回應確認訊號給傳送端，這就稱之為**『RTS/CTS 協調功能』（RTS/CTS coordination Function）**，包含有下列訊框訊號：

(1) 確認（Acknowledge, ACK）：當工作站收到一個位址指向自己的訊框（並非多重傳播或廣播），便會在 SIFS 時間間隔後（如圖 15-21 所示），立即回應一個確認訊框（ACK）給原發送端。

(2) 要求傳送（Request to Send, RTS）：工作站欲傳送資料之前，首先送出 RTS 訊框給接收端，得到接收端回應後，才將資料訊框發送到網路上。

(3) 允許傳送（Clear to Send, CTS）：當工作站收到 RTS 訊框，並確認有工作站欲傳送資料給自己時，便在 SIFS 時間間隔後（如圖 15-21 所示），立即回應一個允許傳送（CTS）給 RTS 訊框的發送端。

圖 15-23 為 RTS/CTS 傳送機制，傳送端與接收端利用 RTS 和 CTS 訊框來達到交談式的傳輸；而接收端在收到資料之後，也會回應一個 ACK 訊框給傳送端。

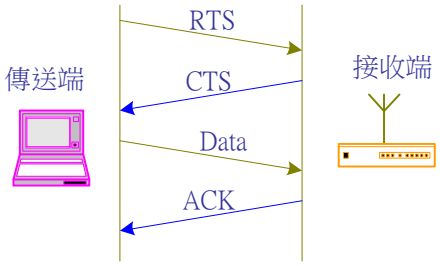

圖 15-23 RTS/CTS 傳送機制

RTS/CTS 協調機制的主要特性是，工作站首先利用較小的訊框（RTS 訊框）來測試網路是否空閒，如果可以收到對方的回應訊框（CTS 訊框），那表示網路是真正的空閒。並且 CTS 訊框是在 SIFS 間隔時間（較短間隔）後立即回應，這也有先下手為強的味道。另外，為了克服無線網路上偵測是否空閒的困難，我們希望每一工作站隨時都能隨時瞭解網路情況，依此來判斷它是否空閒，而不需完全依賴載波感測，這個方法稱之為**『虛擬載波偵測』（Virtual Carrier Sense）**。它的基本原理是工作站只要由網路上收到（或聽到）某個訊框（網路傳輸是用廣播的，所有工作站都能收到其他工作站的傳送訊號），便知道另一工作站正準備傳送訊號，如果能夠大略知曉所需傳送的時間，在這段時間內該工作站就不需要去做載波感測，等時間過後才去偵測。如此便能減少工作站載波感測的次數，也能減少因載波感測發生誤解（沒空閒卻以為空閒）。做一個簡單的結論，虛擬載波偵測的做法是每一工作站都備有一個**『網路配置向量』（Net Allocation Vector, NAV）**，此向量記載其他著其他工作站還需要多久的時間來傳送訊框，而這段時間內網路一定是忙碌的；所以要等到 NAV 紀錄內的時間過了之後，再去偵測網路是否真正空閒。

每一工作站上的 NAV 向量值是如何填入的？IEEE 802.11 的做法是利用 RTS 和 CTS 訊框來承載，亦即在 RTS 和 CTS 訊框裡都包含了一個**『持續時間』（Duration Time）**欄位，標示緊接其後的資料訊框會佔用多少時間。其他工作站收到（或聆聽到）RTS 或 CTS 訊框後，便將該訊框的『持續』欄位的內容登錄到工作站的 NAV 向量內。如果網路一直忙碌著，

則網路配置向量所記載的等待時間可能會一直累積，在未歸零之前，工作站都不能傳送資料。如此一來，網路配置向量（NAV）就好像具備載波偵測的功能，能告訴工作站目前傳輸媒介是否空閒，因此稱之為**『虛擬載波偵測』（Virtual Carrier Sense）**。

圖 15-24 為配置向量的運作模式，其中 RTS 訊框所攜帶的持續時間值（單位為微秒）是預估所要傳遞資料的長度，另外，CTS 也攜帶著預估收取資料的時間，其他工作站收到這些訊息後，便將它填入本身的 NAV 向量值內，並開始計時。在 NAV 值歸零之前，工作站是不會去感測網路是否空閒的。然而，當工作站收到其他工作站發送 ACK 訊框時，它便知道前面所傳送 RTS/CTS 的資料都已傳送完畢，因此將 NAV 歸零，並進入頻道競爭的階段。

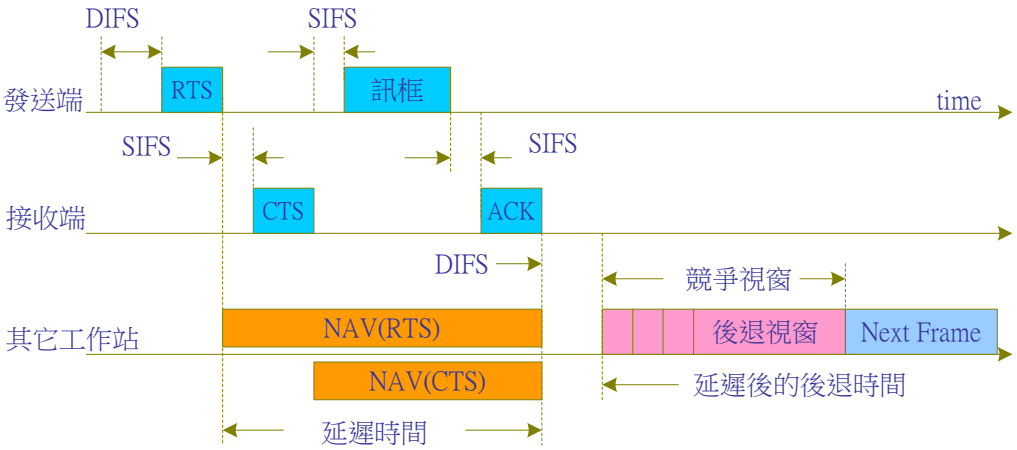

圖 15-24 網路配置向量的運作模式

RTS/CTS 的運作模式也可以解決**『隱藏工作站』（Hidden Terminals）**的問題。我們用圖 15-25 來說明何謂**『隱藏工作站』**問題，由於無線電波有一定的涵蓋範圍，假如有兩個工作站（STA1 與 STA2）同時有資料要傳送給基地台（AP1），而且這兩個工作站都不在彼此涵蓋範圍內，也就是說，STA1 和 STA2 彼此根本不知道對方的存在，這種情況下，當某一方與基地台（AP1）通訊時，另一方的工作站並不知道。譬如，當 STA1 發送訊號給基地台（AP1），而 STA2 收不到 STA1 所發送的訊號，就以為目前頻道是空閒的，而將訊號發到頻道上，如此便會發生碰撞的現象。

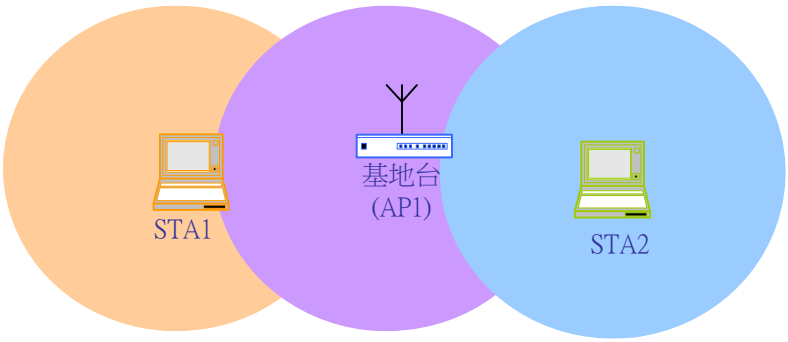

圖 15-25 隱藏工作站問題

我們用 STA1 欲傳送資料給 AP1 為範例，來說明 RTS/CTS 機制如何解決隱藏工作站的問題。當 STA1 向 AP1 要求傳送資料時，雖然 STA2 無法收到 STA1 發送出 RTS 訊框的訊號，但當 AP1 發送 CTS 訊號時，STA2 仍可以收到該訊號，並設定 NAV 向量值，保持一段時間不會去強用頻道，如此便能解決隱藏工作站問題。

另外值得特別注意的是，在 IEEE 802.11 標準中，傳遞訊息並非完全使用 RTS/CTS 機制。如果不是使用 RTS/CTS 機制，接收端收到資料之後，也都必須在 SIFS 間隔時間之後，立即回應一個 ACK 訊框給傳送端。當網路上其他工作站收到 ACK 訊框後，便知道通訊中的工作站已經結束工作了，網路又可以恢復競爭取得傳輸媒介的狀態，如圖 15-26 所示。

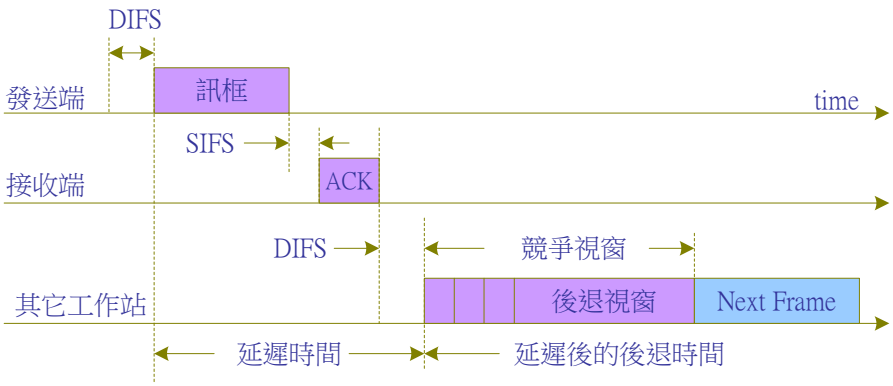

圖 15-26 直接傳送訊框模式

15-4-5 後退演算法與碰撞延遲

在分散式協調機制下，工作站偵測到頻道空閒之後，會再等待一段 DIFS 時間，才進入『競爭視窗』(Contention Window, CW，如圖 15-26 所示)。

工作站進入競爭視窗後，會依照後退演算法計算出一個隨機時間，再等待這段隨機時間之後，才將訊框發送到頻道上。另一種情況是，當傳送端在發送訊框後的預期時間內沒有收到接收端回應 ACK 訊框，便判斷所發送的訊框和其他工作站發生碰撞(也有可能訊號太弱，對方接收不到)，此時，傳送端也會經由後退演算法，來計算重送訊框所必須等待的時間。因此，後退演算法在無線區域網路是個重要的計算公式，其時間計算方式如下：

Backoff = INT(CW * Random()) * Time-Slot

其中：INT(x)為整數函數，表示小於 x 或等於 x 的最大整數；

CW 是介於 CWmin 與 CWmax 之間的某一個數值；

Random() 為介於 0 與 1 之間的隨機 (Random) 數值；

Time-Slot = 傳送端啟動延遲 + 媒介傳遞延遲 + 感測媒介反應延遲。

其中 CW 是一個競爭視窗參數，是由最小值 (CWmin) 到最大值 (CWmax) 的排列中，取得其中一個數值。在標準規範中，CW 數值的排列為(7, 15, 31, 63, 127, 255, 255, 255, …)。每一筆訊框在第一次傳送時，CW 值都會採用最小值 (CWmin = 7)，當該訊框第一次發生碰撞，重送時會採用第二個 CW 值 (CW=15)，如連續發生碰撞，則依此類推；到了第五次重送以後，CW 值會選擇最大值 (CWmax = 255)。但選擇出來的值還要乘以 Random() 的隨機值，因此連續發生碰撞的訊框，經過後退演算法所計算出較長時間的機率較大。工作站發生碰撞後，再經由後退演算法所計算出的必須等待時間，就會比一般後退時間為長，也稱之為『延長訊框間隔』(Extended IFS, EIFS)。

圖 15-27 為工作站後退演算法的運作程序，首先工作站 B、C 和 D 感測到工作站 A 傳送結束，經過 DIFS 間隔時間後，假設所有工作站都有資料要傳送，也經過各自的後退演算法 (CW=7) 計算出後退等待時間 (10、10、5 和 14); 又因工作站 C 的後退等待時間較短，而得以先發送資料到頻道上 (時段 1)。當工作站 C 結束傳送資料後 (如圖 15-27 的運作程序)，再進入競爭視窗，因為工作站 A 和 B 的遺留後退等候時間相同 (5)，於是同時將訊框發送到頻道上，而發生碰撞的情形 (時段 2)。工作站 A 和 B 發送訊後，沒有收到 ACK 回應訊框，因此都決定重送訊框，也分別以 CW =15 再計算出等候時間 (25 和 29)，同時也依此後退等待時間來競爭頻道的使用權 (時段 3)。

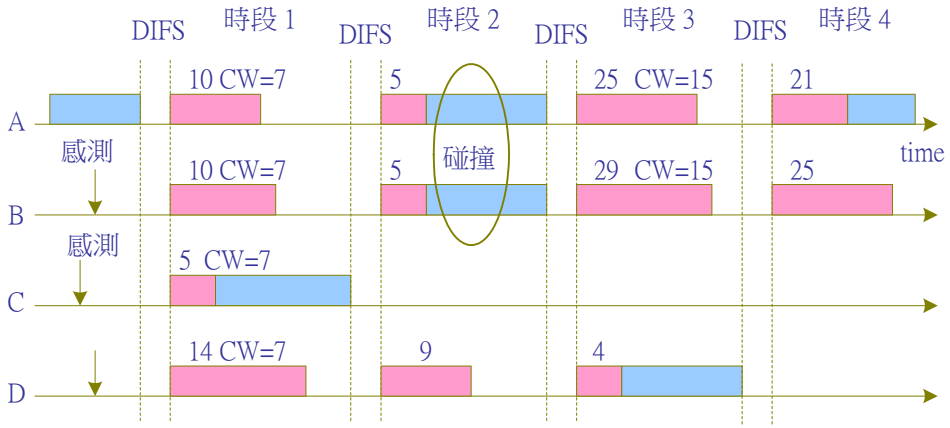

圖 15-27 後退演算法的運作程序

15-4-6 集中式協調功能

IEEE 802.11 除了提供分散式協調機制，讓工作站得以透過競爭方式取得傳輸媒介的使用權之外，也提供『無競爭』(Contention Free) 方式，使工作站以公平分配的方式，來取得傳輸媒介的使用權。它的無競爭模式稱之為『集中式協調功能』(Point Coordination Function, PCF)。顧名思義，集中式協調功能必須有一部『集中協調者』(Point Coordinator)，來負責整個網路的協調工作。通常在一個基本服務區域內的集中協調者，都是由該區域的『擷取點』(Access Point) 來負責。另外，在一個基本服務區內的工作站都可自行選擇是否願意加入被協調的行列，未加入者只能在競爭模式下取得傳輸媒介使用權。首先，我們來介紹一些有關集中式協調的元件及其特性：

(1) **可輪詢工作站 (CF_Pollable)**：參與被協調之列的工作站，或者具有被輪詢能力的工作站。

(2) **非輪詢工作站 (Non_CF_Pollable)**：未參與被輪詢的工作站。

(3) **無競爭輪詢 (Contention Free Poll, CF_Poll) 訊框**：即為集中協調者用以輪流詢問參與協調的工作站是否有資料要傳送。

(4) 當可輪詢工作站被協調者詢問到時，必須在一個 SIFS 時間間隔後，立即回應是否有資料要傳送。

(5) 可輪詢工作站在無競爭週期可以傳送訊框，傳送對象可以是協調者、可輪詢工作站或非輪詢工作站。

(6) 非輪詢工作站在無競爭週期內不可以傳送訊框，但可以接收訊框、或回應 ACK 確認訊框。

(7) 在無競爭週期內所傳遞的訊框可以攜帶一個回覆（ACK）訊息，用以回覆前一筆由協調者傳送而來的訊框。

(8) 當工作站傳送訊框後沒有收到回覆訊息時，此工作站不可以立即進行重送的程序，而必須等到下一次被詢問時，或等到進入競爭週期時，才能重送訊框。

(9) 如果可輪詢工作站傳送訊框的對象是非輪詢工作站，則該非輪詢工作站必須依照 DCF 的運作模式，在 SIFS 時間間隔後立即回應 ACK 訊息。

(10) 在 PCF 週期中，協調者和被詢問者在傳送訊框時，都不使用 RTS/CTS 控制訊框。

(11) 在無競爭週期中，傳送訊框發生碰撞而重新傳送時，都不採用 DCF 的後退(Backoff) 演算法，而是在下一次被詢問到時、或 DCF 週期時才重送訊框。

(A) 無競爭週期的時序

在一個基本服務區內傳輸媒介（頻道）的使用時序，是由無競爭週期和競爭週期輪流出現著，其中無競爭週期是由 PCF 機制所控制；而競爭週期是由 DCF 所控制，如圖 15-28 所示。另外，由一個無競爭和一個競爭週期所構成的週期，稱之為『超級訊框』(Superframe)，超級訊框的出現率是固定的，如果因為某種因素使上一個超級訊框延遲，則在下一個超級訊框內會減少無競爭週期的時間，以保持超級訊框固定的出現率。

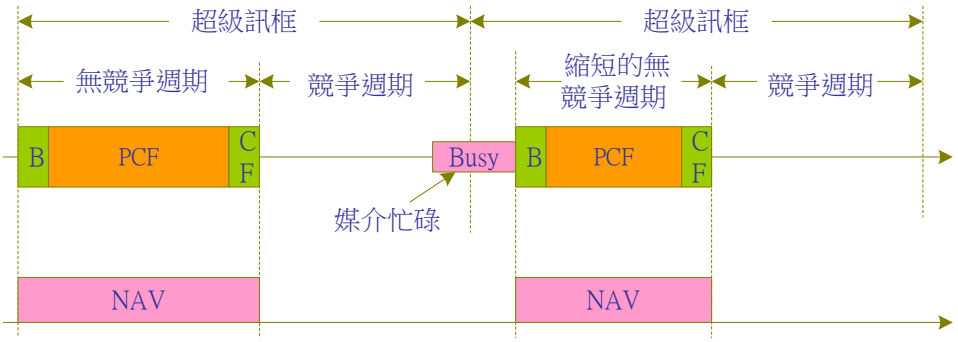

圖 15-28 超級訊框週期

無競爭週期是由協調者發送出一個 Beacon 訊框來開啟，而結束於協調者送出 CF_End 或 CF_End+ACK 訊框。當協調者送出 Beacon 訊框時，訊框內會包含著 PCF 持續的時間（CFPDurRemaining），其他工作站收到 Beacon 訊框後，便將該值填入『網路配置向量』（NAV），並保持在這段時間內不會強用傳輸媒介。又當協調者送出 CF_End 訊號來表示無競爭週期結束時，工作站再將 NAV 設定為零，並進入競爭週期。協調者會依照系統所設定的週期時間（CFPMaxDuration）發送 Beacon 訊框，表示無競爭週期的開始。但當協調者計時期滿而須發送 Beacon 訊框時，此時網路並非一定空閒，說不定還有工作站正在發送，或是競爭不到傳輸媒介使用權，而發生延後進入無競爭週期的現象。但為了保持超級訊框的固定週期，延後的時間必須由縮短無競爭週期來彌補，如圖 15-28 所示。

(B) PCF 基本運作程序

協調者是在傳輸媒介空閒後的 PIFS 時間間隔內將 Beacon 發送出去，因 PIFS 小於 DIFS 時間間隔，而使協調者比一般競爭者優先取得媒介使用權。在一個基本服務區（BSS）內的協調者大多是由擷取點的 PCF 程式來控制。所有位於 BSS 中的工作站在無競爭週期開始後，都將 NAV 設定為無競爭週期的最大值（CFPMaxDuration），也保證這段時間不會參與傳輸媒介的競爭，以避免發生碰撞的機會。

在未討論 PCF 運作程序之前，先來討論無競爭週期中訊框的回覆方式。依照訊框之目的位址，可歸類為下面三種：

(1) 接收該訊框的工作站是協調者：協調者收到訊框後，可在傳送下一筆資料及詢問給別的工作站時，順便攜帶回覆訊號，訊框為 Data + CF_Poll + CF_ACK 格式（一個訊框）。或在輪詢給別的工作站時，順便攜帶回覆訊框，訊框為 CF_Poll + CF_ACK（一個訊框，容後說明此訊框格式）。

(2) 接收該筆訊框的工作站剛好被輪詢到：該工作站收到訊框後，如有資料要傳送，則發送 Data + CF_ACK；否則直接回覆 CF_ACK。

(3) 接收該訊框的工作站不是剛好被輪詢到的工作站：訊框的目的工作站可能是可輪詢工作站或非輪詢工作站，此時該工作站必須於 SIFS 時間間隔內回應 ACK 訊號。

當進入無競爭週期後，協調者依照本身內部的輪詢名單，發送輪詢訊號（CF_Poll）給可輪詢工作站（CF_Pollable）。圖 15-29 為典型的無競爭週期運作程序，圖中由協調者發送的資料訊號稱之為『**下傳訊務』(Down Traffic)**；而由一般工作站發送的資料訊號稱之為『**上傳訊務』(Up Traffic)**，另外 Dx 表示下傳的第 x 筆資料；Ux 表示上傳的第 x 筆資料。在協調者發送 Beacon 訊框進入無競爭週期後，協調者會在經過 SIFS 時間間隔後送出輪詢的訊框（CF_Poll）；而被詢問到的工作站也會在下一個 SIFS 間隔後送出資料訊框，或表明無資料須傳送。

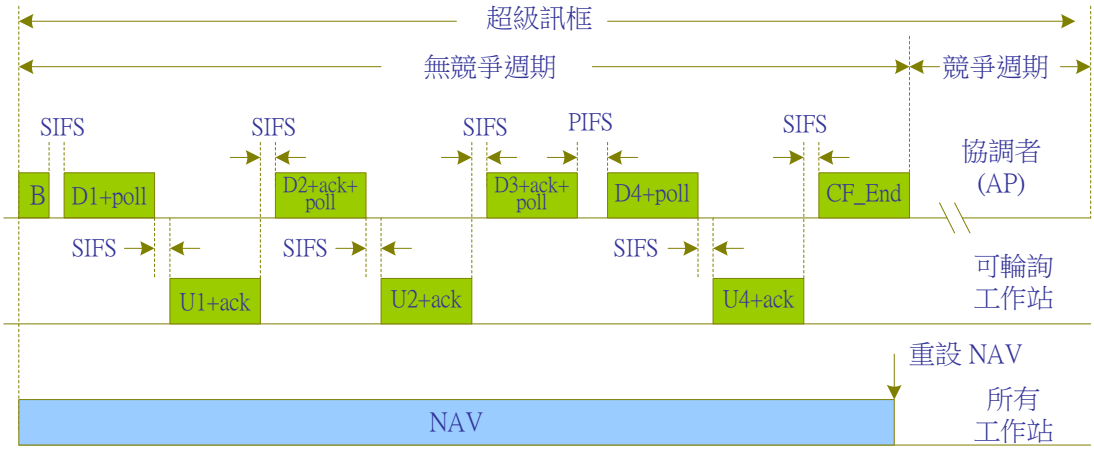

圖 15-29 典型無競爭週期的運作程序

當協調者送出詢問訊框時，也有可能會連續送出詢問訊框，或回應 ACK 訊框，然而，這些訊框的目的位址並不一定相同；但網路是屬於廣播型態，任何工作站都可以接收到這些訊框，因此，不會影響各自訊框的傳遞動作。同樣的，當工作站被詢問到時，在傳送資料當中，也可以攜帶確認（ACK）訊框。

一般無線網路都是透過擷取點和有線網路聯結，同時將協調程式安裝在擷取點上，因此，無線工作站大部份的通訊是透過擷取點來連接有線網路，也就是說，大部份的通訊是發生在工作站和協調者之間。因此可將 PCF 的運作模式以：(1) 當協調者是傳送工作站或接收站，與 (2) 當協調者不是傳送及接收工作站，兩種模式來探討，以下分別敘述其運作程序。

(C) 當協調者是傳送工作站或接收站的運作程序

圖 15-29 為協調者是傳送工作站或接收工作站的運作程序範例，在這種情況下，協調者傳送給輪詢工作站的訊框可能是下列七種訊框之一：

(1) Data 訊框：協調者傳送資料訊框給某一工作站，該工作站不是剛好被輪詢到的（或是非可輪詢工作站），而且協調者沒有未回覆訊息。

(2) Data+CF_ACK 訊框：協調者傳送資料訊框給某一工作站，該工作站不是剛好被輪詢到的，協調者並回覆一個確認訊框給另一工作站（或同一工作站）。

(3) Data+CF_Poll 訊框：協調者傳送資料給某一工作站，並且詢問它是否有資料要傳送。

(4) Data+CF_ACK+CF_Poll 訊框：協調者傳送資料給某一工作站，同時回覆一個確認訊息，並且詢問它是否有資料要傳送。

(5) CF_Poll 訊框：協調者僅依照輪詢名單，傳送詢問訊框給某一工作站，詢問該工作站是否有資料要傳送。

(6) CF_ACK+CF_Poll 訊框：協調者詢問工作站，並送出一個回覆訊框。

(7) CF_ACK：協調者僅送出回覆訊框。

當工作站收到協調者送來的 CF_Poll 訊框時，就可以在 SIFS 間隔後傳送一個 Data 訊框，如果沒有資料要傳送，必須回覆一個 Null 訊框給協調者。協調者在無競爭週期內，可直接傳送 Data 訊框或管理訊框給工作站（輪詢工作站或非輪詢工作站），這些工作站收到資料訊框後必須在 SIFS 間隔後回應一個 ACK 訊框。當協調者送出 CF_Poll 訊框時，可視需要攜帶 Data 或 CF_ACK 訊框，如圖 15-29 中的 D1 或 D2；工作站傳送 Data 訊框時，也可視需要攜帶 ACK 訊框，如 U1 或 U2 訊框。當協調者發送完訊框（資料或詢問訊框），若經過 SIFS 間隔後還未收到對方回應，此即表示對方工作站不存在或收不到訊號，這時協調者會等到 PIFS 間隔後再送出下一個訊框（詢問或資料）。如圖 15-29 中，協調者發送 D3 + ACK + Poll 後卻未收到回應訊號，於是直到 PIFS 間隔後再送出下一個訊框（D4 + Poll）。圖 15-29 同時可看出，協調者送出 Beacon 訊框後，所有工作站都將 NAV 設定成 PCF 的最大週期時間，一直到收到 CF_END 後，才將 NAV 清除為零。

(D) 當協調者不是傳送工作站或接收站的運作程序

第二種情況是當協調者非傳送或接收工作站時，其運作情況如圖 15-30 所示。此種情形是發生在工作站被輪詢到時，傳送資料訊框給同一 BSS 中另一個工作站（而不是協調者），

此時資料訊框的接收與回覆必須採用 DCF 規則，亦即接收訊框者（任何工作站）必須在一個 SIFS 間隔後回送一個 ACK 訊框。如圖 15-30 中，協調者詢問到某一工作站時（D1 + Poll），該工作站傳送訊框給另一工作站（S-To-S），收到訊框者必須在 SIFS 間隔後，發送 ACK 訊框來表示正常接收。此時，協調者必須等到一個 PIFS 間隔後，才可再發送詢問訊框（或資料訊框）給其他工作站。

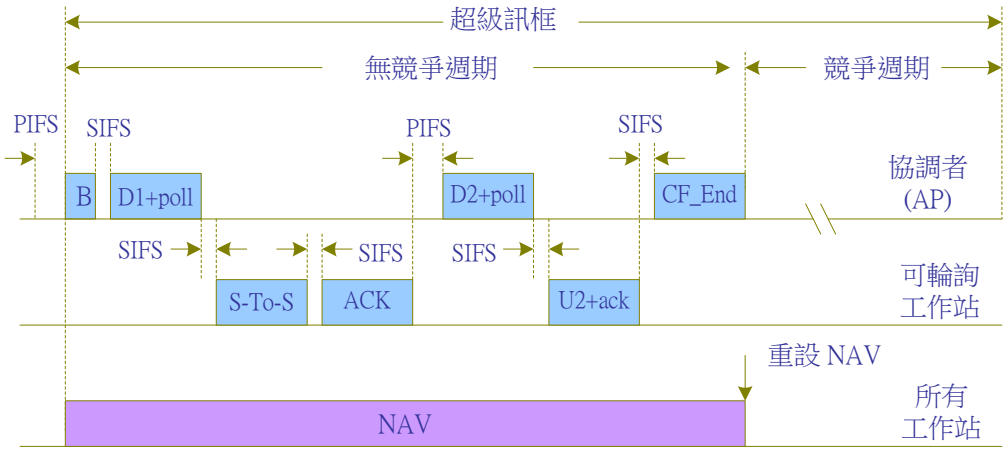

圖 15-30 協調者非傳送或接收工作站運作範例

另一種重要的情況，無線區域網路上所傳送的訊框都是屬於短訊框格式，然其所連接的其他網路大多是採用長訊框來傳遞訊息，因此，一筆傳送的資料大多由多個資料訊框所構成，亦是所謂的資料片段（Fragments）。在這種情況下，傳送端取得媒介使用權（經協調者授權）後，會連續傳送多個資料訊框，其間每當它收到接收端回應 ACK 訊框後，也需要在 SIFS 間隔後立即發送出下一個訊框。由此可見，雖然無競爭週期沒有使用 RTS/CTS 機制，仍可達到連續傳送訊框的功能。

(E) 輪詢名單的建立與維護

在無競爭週期中，協調者是利用輪詢名單來分配可輪詢工作站的媒介使用權，因此輪詢名單的建立與維護就顯得非常重要。輪詢名單的建立方法是，當工作站啟動時會向協調者（擷取點）要求連線，在建立通訊連線（Association）時，就必須表明是否願意加入被輪詢名單。工作站如欲退出輪詢名單，也需要重新連線（Reassociation）來表明欲退出。雖然加入輪詢名單的工作站較能保證取得媒介使用權，但也有缺點，譬如進入省電狀態的工作站，會在每次被詢問到時又被叫醒，來回答是否有資料要傳送。因此，對於時常處於省電狀態的工作站，最好不要加入輪詢名單；但未加入輪詢名單時，又僅能在競爭週期傳送資料。

協調者依據輪詢名單來詢問工作站，也有不同的做法，例如輪詢名單過長時，可能需要經過幾個無競爭週期才能輪詢一遍；但輪詢名單較少時，輪詢一遍可能還有剩餘時間。一般情況下，可依據訊務（Traffic）流量的分佈情形，或是不同服務品質的要求，來選擇輪詢工作站的優先次序，或是給予某些工作站較多的傳輸機會，如此便牽涉到協調者的排程演算法。然而在規範中並沒有制定標準演算法，都是由製造廠商各自制定。

15-5 認證與保密

『認證』（Authentication）是確定對方身份的真實性，以避免他人入侵或冒名進入系統，或與身分不明的對象溝通；**『保密』（Privacy）**是保護傳輸中的資料不被他人竊聽。一般在單一基本服務區（BSS）內，多半只會發生工作站向擷取點要求認證的程序，也就是說，擷取點負責整個 BSS 內工作站的登入工作站；但有時候也會發生在兩個工作站之間的身分認證。IEEE 802.11 提供兩種認證方式：**『開放式系統』（Open System）**與**『共享式密匙』（Shared Key）**，前者是內定的認證方式，不過工作站提出認證要求時，可以指定採用哪種方法來進行雙方認證。至於保密措施，IEEE 802.11 採用**『有線等效保密演算法』（Wired Equivalent Privacy Algorithm）**，以下針對這三個主要措施來加以介紹。

15-5-1 開放式系統認證

『開放式系統』（Open System）認證是最簡單的認證方式，欲登入網路的工作站只要依照本身的 MAC 位址，即可詢問系統是否同意。大部份的無線網路都採用**『MAC 位址控制』（MAC Address Control）**方式，它的做法是網路上有一控制中心（大多由擷取點負責），登錄可登入工作站的 MAC 位址，當任一工作站啟動而欲登入網路時，便由控制中心檢視 MAC 登錄表，決定是否同意該工作站登入網路。因此，工作站欲加入某一網路之前，必須向該控制中心登錄本身的 MAC 位址。

圖 15-31 為開放式系統的運作圖，工作站欲加入網路時，送出一個『要求』（Request）訊號給控制中心，其中包含工作站位址（SA）與認證模式（Open System），訊號格式（部份訊息）如圖 15-31 所示。控制中心收到要求認證訊息後，檢視其工作站位址是否合乎登入權限，而回應同意或不同意訊息，其中包含工作站位址（SA）、認證模式（Open System）與認證結果。工作站通過認證後，系統才會給予服務，否則無法進入。

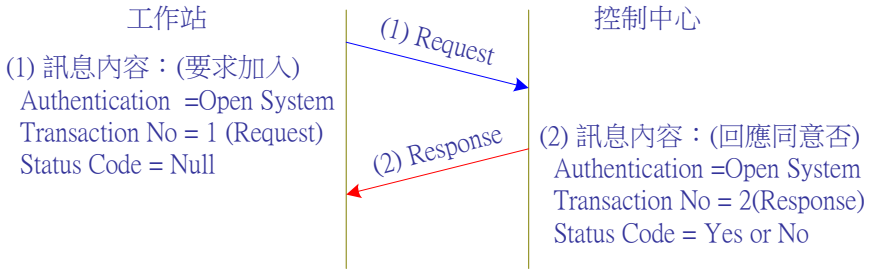

圖 15-31 開放系統式認證的運作程序

15-5-2 共享密匙式認證

『共享式密匙』(Shared Key) 認證表示求證雙方都共同擁有一隻秘密鑰匙，認證時便依照此秘密鑰匙來證實對方的身分。這隻秘密鑰匙也許是透過某一個認證系統所分配，或是透過人工的傳遞，這已不是 IEEE 802.11 所管轄的範圍，而需要另一個系統來製作(如 RADIUS 系統)。秘密鑰匙是屬於個人性的，這表示每一登入網路者都擁有一個獨立的秘密鑰匙；如果網路上有許多工作站的話，控制中心就必須管理許多秘密鑰匙，這也是非常困擾。在許多情況下，秘密鑰匙都屬群體性的，也就是說，同一群組 (或同一無線網路) 共同使用一個秘密鑰匙，這對於控制中心來講比較容易管理，但多人共用容易洩漏秘密鑰匙，造成網路安全問題。

共享式密鑰的運作方式是採用**『盤問與回應』(Challenge/Response)** 機制，簡單的原理是要測試對方所擁有的密匙是否和自己的相同。它的做法是先送一段資料給對方，對方用密匙加密後回應給測試端，測試端再用自己的密匙來解密。解密後的資料若和原來傳送的資料相同，便表示雙方的密鑰相同，可以認證對方的身分。

圖 15-32 為共享式密匙的運作程序，其中包含有四個步驟：

(1) 一開始工作站送出要求加入網路訊息(Request)(訊息 (1))，也指明認證方式(Shared Key)。

(2) 控制中心收到對方要求認證時，便隨機產生一串長度為 128 位元組的盤問全文 (Challenge Text)，附加在回應訊息傳送給對方 (訊息 (2))。

(3) 接下來，工作站收到對方的盤問命令 (Transaction No=2)，便將訊息內的盤問全文以共享密匙來加密，並回應給控制中心 (訊息 (3))。

(4) 控制中心收到對方再要求訊號（Transaction No=3），便知道是經由盤問回來的回應，於是將訊息內的盤問全文以自己的共享密匙來解密。如果經解密後的全文和原來傳送的盤問全文相同，即表示對方所擁有的秘密鑰匙和自己的相同，於是就能確認對方身分（和自己屬於同一群組的成員），而回應同意加入訊息（訊息 (4)）。

圖 15-32 共享式密匙認證的運作程序

15-5-3 有線等效保密法

『有線等效保密演算法』（Wired Equivalent Privacy Algorithm，簡稱 WEP 演算法）是希望建立一個類似有線網路保密功能的演算法。由於無線電波是廣播式傳遞，只要能接收到該廣播訊號，就能竊聽到網路上所傳輸的資料，這比有線網路還不安全。欲竊聽有線網路所傳輸的資料，至少還需要連接到有線網路上，對一般入侵者仍保有相當的防護功能。為了解決這個問題，IEEE 802.11 標準中制定了一個與有線網路具有同等功效的資料保密演算法，這就是 WEP 演算法。

簡單的說，WEP 演算法是屬於一般**『加密/解密』（Enciphering /Deciphering）**的機制，傳送者與接收者都擁有一支秘密鑰匙，資料傳輸之前利用鑰匙加密後再傳送給對方，對方收到資料後也利用解密鑰匙解密來得到原來的資料；加密與解密都用同樣一把秘密鑰匙，因此對於鑰匙的管理就顯得特別重要。另一方面，IEEE 802.11 所採用的共享密匙機制中，秘密鑰匙大多屬於群組共用，亦即同一群組的成員都擁有一隻相同的秘密鑰匙，這對安全防護上又是一個大漏洞。但如讓每個工作站都有一支獨立的秘密鑰匙，控制中心的管理負荷將相對繁

重，因為它可能必須隨時處理使用者變更或遺失鑰匙的問題。IEEE 802.11 為了彌補這個缺憾，便使用一個變動的向量值，來和共享密匙組合成一個新的秘密鑰匙，如果向量值隨使用者及時間改變，則此秘密鑰匙便可隨時處於改變中，如此便能提高保密措施的完整性，這就是 WEP 演算法的基本原理。

(A) WEP 演算法特色

IEEE 802.11 規範中提到 WEP 演算法有下列特色：

(1) 抗竊聽性強：一般入侵者欲盜取資料大多使用『暴力攻擊法』(Brute-force Attack)，也就是連續用不同的鑰匙來嘗試解密，如解密出有效資訊便表示密匙破解成功。WEP 為了防護暴力攻擊，於是利用共享密匙和一個『起始向量值』(Initialization Vector, IV) 來組合成它的密匙，並隨時藉由 IV 的改變來變動秘密鑰匙，讓暴力攻擊來不及破解密匙。

(2) 具有自我同步能力：WEP 針對每一筆資料都具有『自我同步』(Self-synchronization) 的能力。如使用於資料流失率低，並且能盡力傳送的環境下，它的效益已接近於資料鏈結層 (Data-Link Layer) 的加密演算法功能。

(3) 效率高：WEP 演算法的執行效率高，並可用硬體或軟體技術來製作。

(4) 出口爭議性：美國基於國防安全性的考量，對於安全性較高的加密演算法一般都有限制出口。WEP 所使用的加密演算法是否可以依照商業環境需求而順利出口，還是存在許多爭議性的問題。

(5) 選項功能：在 IEEE 802.11 的標準規範下，WEP 是一種選項設施，使用者可以決定是否採用 WEP 演算法。也有許多公司為了安全性考量，而採取不同的加密演算法，來提高系統的安全性。

(B) WEP 運作原理

所謂『加密』(Encryption) 就是用特殊方法將原始二進位資料處理成亂碼，以將資料隱藏起來。未經加密的資料稱之為**『原文』(Plaintext, P，或稱明文)**，而經過加密處理的資料，則稱之為**『密文』(Ciphertext, C)**。將密文還原成原文的過程稱之為**『解密』(Decryption)**。

密碼演算法（Cryptographic Algorithm, 簡稱 Cipher）就是用來對資料進行加密和解密的數學函數。近代密碼學都採用『**鑰匙』(Key, K，一般又稱 "金鑰")** 技術來進行加密或解密的工作，而 WEP 是採用共享密匙方式，也就是說，解密和加密是採用同樣一把秘密鑰匙。圖 15-33 為加密/解密的基本過程，其中『**加密函數』(Encryption Function, E)** 處理原文 P 後得到密文 C 的運算式如下：

$$EK(P) = C$$

欲還原時，經由『**解密函數』(Decryption Function, D)**，利用相同的鑰匙 K 處理密文 C，而得到原文 P 的運算式如下：

$$DK(C) = D_K(E_K(P)) = P$$

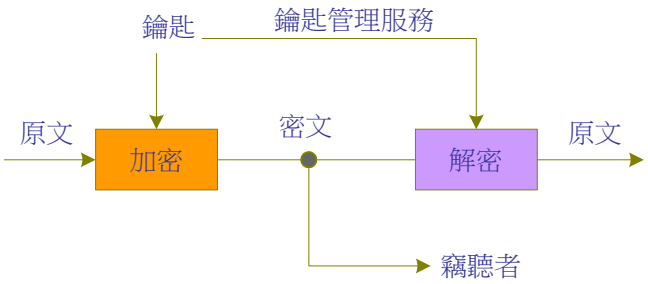

圖 15-33 加密/解密的基本過程

WEP 演算法是將一段原文區塊（Plaintext Block）與一個等長度的『**隨機鑰匙序列』(Random Key Sequence)** 做位元與位元之間的互斥運算（XOR Operation），此隨機鑰匙序列是由 WEP 所產生。另外，WEP 演算法是一種對稱性的演算法，加密和解密都是用同一串的隨機鑰匙序列來做 XOR 運算。

圖 15-34 為 WEP 加密演算法的處理過程，乃先藉由一個『**密匙』(Secret Key)** 和初始向量(IV)組合成一個『**種子』(Seed)**，並將此種子作為『**虛擬亂數產生器』(Pseudo Random Number Generator, PRNG)** 的輸入參數。隨後 PRNG 產生一個具有隨機性質的『**鑰匙序列』(Key Sequence)**，其長度也是隨機改變，但一定能符合 MPDU（MAC Protocol Data Unit）的最大長度限制。而原文不僅經過加密處理，為了檢驗出傳遞當中的訊息是否發生錯誤，原文必須先經過『**完整演算法』(Integrity Algorithm)**計算後，得到一個『**完整檢查碼』(Integrity Ckeck Value, ICV)**，再經過加密後，隨著密文（資料）傳送給對方。

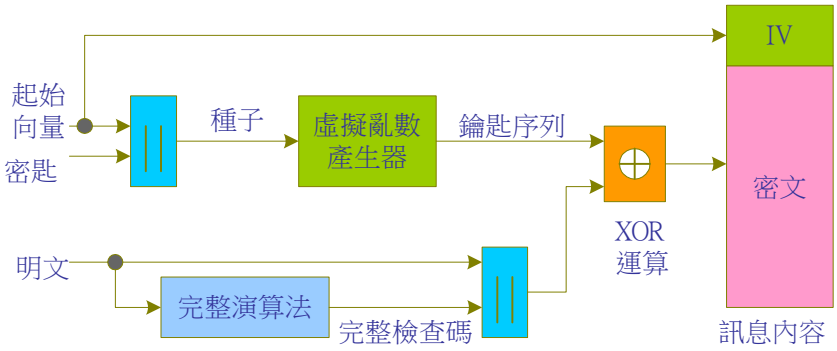

圖 15-34 WEP 演算法的加密過程

初始向量為 24 位元，可以週期性的變化，它與密匙（40 位元）結合而成為 64 位元的種子（Seed），種子的結構是最左邊 40 位元填放密匙（40 位元），而右邊 24 位元則放置初始向量。種子的結構如下所示：

圖 15-34-1

在加密過程中，虛擬隨機亂數產生器（PRNG）為最主要的關鍵組件，它負責將相對較短的密匙轉換成任意長度（與 MPDU 同樣長度）的鑰匙序列，如此可以簡化密匙的傳遞負荷。在通訊進行期間，由於起始向量（IV）可以週期性的變化，而密匙則可以保持不變，如此，雖然使用同樣的密匙來加密，但所產生的鑰匙序列也能週期性的變化。如果遭受暴力攻擊，竊聽者也很難有足夠的時間來破解，甚至可以每一個 MPDU 都使用不同的起始向量來增加安全性。另一方面，雖然初始向量是隨訊息傳送給對方（未經加密處理），但初始向量和密匙沒有任何關係，盜取者雖然取得初始向量，也無法計算出密匙及鑰匙序列。另有一重要的特性，就是 WEP 也利用初始向量的改變來達到自我同步的功能。

WEP 演算法是針對一個 MPDU（MAC Protocol Data Unit）為處理單位，輸出的訊息結構如圖 15-35 所示，其中起始向量（IV）欄位和完整檢查碼欄位（ICV）都是 4 個位元組。一般完整演算法都是利用 CRC-32 演算法，因此，完整檢查碼欄位的內容是 CRC 檢查碼經過加密後的結果。另外，初始向量雖然佔用了 4 個位元組空間，但事實上它本身的長度只有 3 個位元組，另外一個位元組則包含一個填塞（PAD, 6 位元）及鑰匙碼（Key ID, 2 位元），其中鑰匙碼是用來通知接收端在解密時應該使用四種個可能密匙中的哪一個。

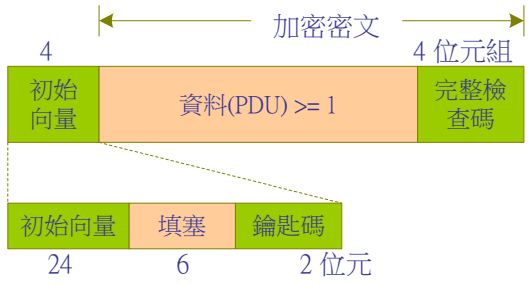

圖 15-35 經 WEP 處理後的訊息格式

圖 15-36 為 WEP 解密處理的運作程序，當工作站收到一筆 MPDU 訊框時，首先由訊框的前頭取出初始向量，並與事先協調的密匙組合成虛擬亂數產生器的種子；種子經由 PRNG 處理後可得到鑰匙序列，此序列會和傳送端的序列相同。鑰匙序列與密文進行 XOR 運算後便得到明文和完整向量檢查碼，明文再經過完整演算法（CRC 除法器）後，與解密所得的完整檢查碼相比較（ICV = ICV′ ?），如果兩者相同，表示傳輸資料正常；如不相同，表示資料可能被竄改過，此時除了不能將錯誤資料傳送給上層外，並應通知 MAC 管理軟體。

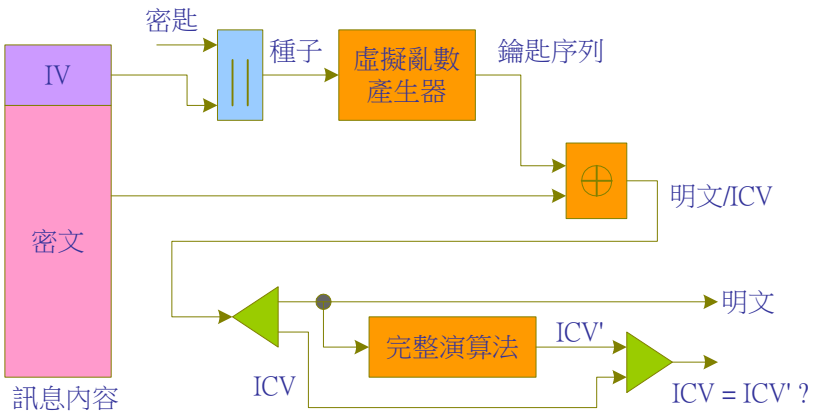

圖 15-36 WEP 演算法的解密過程

15-6 訊框格式

IEEE 802.11 協定如同一般區域網路（如 Ethernet）協定一樣，上層通訊軟體也是透過 IEEE 802.1 LLC（Logical Link Control）（請參考第七章說明）。LLC 提供多工傳輸模式，讓多個應用程式能透過 LLC 連接到 MAC 通訊軟體。但為了提高傳輸效率，LLC 點對點傳輸大多採用較長的訊框，稱之為『**MAC 服務資料單元**』（**MAC Service Data Unit, MSDU**）。但無線網路的電波傳遞容易受到其他訊號的干擾，並不適合傳遞長訊框，因此，MAC 傳訊框

前會將長訊框的 MSDU 切割（Fragment）為若干個『**MAC Protocol Data Unit, MPDU**』，接收端收到 MPDUs 後再將其組合回原來的 MSDU，分割方式如圖 15-37 所示。

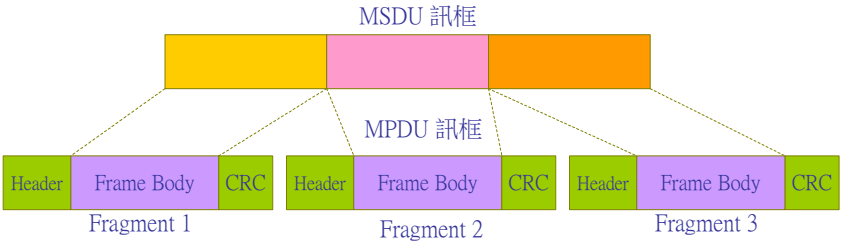

圖 15-37 MSDU 切割範例

在 IEEE 802.11 規範中，可設定一個最大訊框長度，稱之為『**切割臨界值**』**(Fragmentation Threshold)**。當一個 MSDU 訊框的長度大於切割臨界值時，就必須被切割，亦即每一個 MPDU 的資料長度都必須小於切割臨界值。在傳送時，每一個 MPDU 都代表一個獨立的訊框，也都必須分別收到對方的回覆訊息。不過屬於同一個 MSDU 的 MPDUs 在傳送時，是以密集方式一個接一個傳送，而每一個 MPDU 也都必須收到回覆訊息（Stop-and-Wait 流量控制法）。一個 MSDU 訊框只要呼叫一次 DCF 或 PCF，便可以連續傳送所屬的 MPDUs，不需要每個 MPDU 都呼叫一次。另外，不論欲傳送訊框的 MSDU 長度是否超過切割臨界值，只有指定單一目的地的訊框才能被切割，且廣播及群播的訊框也都不可以分割。另外值得注意的是，『切割臨界值』是依照系統內定的 aMPDUMaxLength 參數大小而定，一般在 FHSS/1Mbits 設定為 400 Bytes；而 FHSS/2Mbits 設定為 800 Bytes，由此可見，MPDU 是屬於短訊框傳輸方式。

15-6-1 MPDU 訊框格式

圖 15-38 為 IEEE 802.11 的 MPDU（MAC Protocol Data Unit）訊框格式，其中包含：

(1) **訊框標頭(Header):** 長度為 30 Bytes，包含訊框控制(Frame Control)、位址(Address 1 ~ 4)、順序控制（Sequence Control）與持續時間（Duration/ID）等欄位。

(2) 訊框實體（Frame Body）: 為 0 ~ 2312 Bytes 的不定長度，欄位中可能存放資料或其他控制訊息，依訊框型態（Frame Type）而有所不同。這裡必須強調的是，如果是廣播或多重傳播的訊框是不可以分割的，因此訊框實體內可能包裝著一個未經分割的 MSDU，而其長度可能會較長。

(3) 訊框檢查序列（Frame Check Sequence）：長度為 4 Bytes，採用 CRC-32 檢查碼。

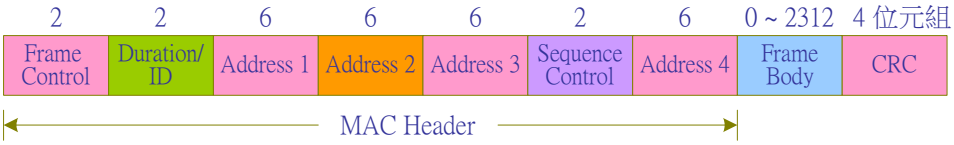

圖 15-38 MPDU 訊框格式

以下分別介紹各欄位的功能。

(A) 訊框控制欄位

『訊框控制』（Frame Control）欄位格式如圖 15-39 所示，其包含 11 個子欄位，功能如下：

圖 15-39 訊框控制欄位格式

(1) Protocol Version：802.11 協定版本。

(2) **Type and Subtype：**Type 欄位表示此訊框型態，目前定義有三種：Data、Control 與 Management 訊框，每一種型態都包含若干種子型態，由 Subtype 欄位指定，如表 15-4 所示。

(3) **To DS：**此旗號為 1 表示此 Data 訊框（包含廣播與群播訊框）是要傳遞給分散式系統（透過 AP 轉送）。若為其他種類訊框，則其值應該為 0。

(4) **From DS：**此旗號為 1 表示此 Data 訊框是由分散式系統傳送下來的（透過 AP 轉送）；若為其他種類訊框，則其值應該為 0。To DS 與 From DS 之間有四種組合，各表示不同的意義，如表 15-5 所示。

(5) **More Frag：**此旗號值若為 1，表示此訊框後面還有其他片段（Fragment）會繼續傳送過來。若後面已無其他片段訊框，則為 0。

(6) **Retry**：此旗號值為 1，表示此 Data 訊框（或管理訊框）為重送的訊框，接收端可依此判斷接收或拋棄。

(7) **Pwr Mgt**：此旗號用來顯示工作站是否處於電源管理模式（Power Management）。如其值為 1，表示此工作站正處於省電模式；其值為 0，表示此工作站處於正常工作狀態。

(8) **More Data**：AP 可用此旗號來通知處於省電模式的工作站，已有資料準備傳送給它；另一種用途是，如在 Data 訊框上此旗號為 1，表示至少還有一個 MPDU 準備傳送。若為其他種類的訊框，該值應為 0。

(9) **WEP**：此旗號值為 1 時，表示該訊框所攜帶的資料已經過 WEP 加密處理，否則該值為 0。

(10) **Order**：此旗號為 0 時，表示此 Data 訊框是經由**『嚴格依序服務等級』（Strictly Ordered Service Class）**所分類。若為其他訊框，則該值為 0。

表 15-4 有效訊框型態與次型態的組合

Type value b3 b2	Type Desciption	Subtype value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110~0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement Traffic Indication Message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101~1111	Reserved
01	Control	0000~1001	Reserved

01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-END
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF_Ack (no data)
10	Data	0110	CF_Poll (no data)
10	Data	0111	CF_Ack + CF_Poll (no data)
10	Data	1000~1111	Reserved
11	Reserved	0000~1111	Reserved

表 15-5 To DS 與 From DS 組合的意義

To DS 值	From DS 值	代表意義
0	0	Data 訊框由一個工作站直接傳送給同一分散式系統下的另一個工作站
1	0	Data 訊框傳送給分散式系統
0	1	Data 訊框由分散式系統傳下來
1	1	在無線分散式系統（Wireless Distribution System, WDS）下，由一個 AP 傳送給另一個 AP。

(B) 持續/識別欄位

持續/識別（Duration/ID）欄位共有 16 個位元，依照訊框格式可能存放**『持續時間』（Duration）**或**『聯結識別碼』（Association Identify, AID）**，其用法如表 15-6 所示，說明如下：

(1) 若訊框為『控制型態』(Control Type，如表 15-4 所示)，而且次型態為 PS_Poll (省電詢問)，則此欄位攜帶聯結識別碼 (AID)，其最左邊兩個位元都是 1，而剩下的 14 個位元表示傳送此訊框工作站的 AID；AID 值的範圍由 1 到 2007。

(2) 若為其他訊框，則此欄位代表一個『持續時間』(Duration)，其值依各訊框型態而定。但對於所有在無競爭週期所傳送的訊框來說，此欄位的值應該設為 3274。當 Duration/ID 欄位的內容小於 3278 時，表示其為一個 Duration 值，而且是用來修正 NAV 值的。

表 15-6 Duration/ID 欄位的意義

Bit 15	Bit 14	Bit 13~0	用途
0	0 ~ 32767		持續時間 (由此訊框結束後起算，單位為 us)
1	0	0	無競爭週期傳送固定值 (32768)
1	0	1 ~ 16383	保留
1	1	0	保留
1	1	1 ~ 2007	在 PS_Poll 訊框中指定的 AID
1	1	2008 ~ 16383	保留

(C) 位址欄位

在 IEEE 802.11 規範中，位址型態 (48 個位元) 可能是下列兩種型態之一：

(1) 個別位址 (Individual Address)：表示連結在網路上的某一獨立工作站位址，可做為目的或來源位址使用。

(2) 群組位址 (Group Address)：表示某一工作站群組位址，僅能做為目的位址使用，可分為下列兩種類型：

(a) 群播群組位址 (Multicast-Group Address)：某一位址代表一個工作站群組，此群組成員可接收該位址為目的地的訊框。

(b) 廣播位址(Broadcast Address)：廣播位址的格式是所有位元都是 1(48 個位元)，任何工作站都可接收該位址為目的地的訊框。

MAC 訊框格式共有四個位址欄位，這些欄位是用來記錄『**基本服務區 ID**』(**BSS Identifier, BSSID**)、起始位址 (Source Address, SA)、目的地位址 (Destination Address, DA)、傳送器位址 (Transmitter Address, TA)、以及接收器位址 (Receiver Address, RA)，至於哪一個欄位存放何種位址，隨不同訊框型態而異。其中目的位址 (DA) 可以是個別或群播位址，也可以是該訊框的最終目的；起始位址 (SA) 是產生此訊框的工作站位址；而傳送器位址 (TA) 是指無線媒介上傳送此訊框的位址；接收器位址 (RA) 則是指在無線媒介上接收此訊框的位址；然而 TA 與 RA 大多屬於擷取點 (AP) 位址。每一個位址都符合 IEEE 802 標準的 48 位元長度，但有些訊框型態不會使用到所有欄位。

有些位址欄位在使用時，與其在欄位的相對位址 (1 ~ 4) 有關，和位址型態無關。例如，當一個工作站接收到一筆訊框時，皆以 Address 1 來判斷是否傳送給自己，而 CTS 訊框 (ACK 訊框) 中的 RA，是等於 RTS 訊框 (需要被回覆的訊框) 中的 Address 2 位址。至於每一欄位存放何種位址，在介紹控制訊框與資料訊框時會提到。

(D) 順序控制欄位

『順序控制』(Sequence Control) 欄位是用來表示該訊框是屬於那一個 MSDU 號碼下的第幾個分段 (Segment) 號碼，包含兩個次欄位：順序號碼 (Sequence Number，12 個位元) 與片段號碼 (Segment Number, 4 個位元)，如圖 15-40 所示。其中順序號碼為該訊框的 MSDU 號碼，每一個 MSDU 都有一個順序號碼，其值由 0 到 4095，可以重複輪流使用。片段號碼是指由 MSDU 分割出來的片段順序號碼，其值由 0 到 15，可重複使用；如果片段號碼為 0，表示是第一個片段或沒有分段的訊框。

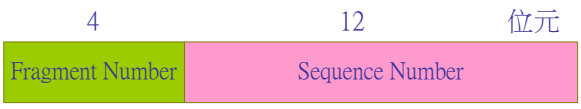

圖 15-40 順序控制欄位

15-6-2 控制訊框格式

如表 15-4 所列，訊框型態可區分為控制 (Control)、資料 (Data) 和管理 (Management) 等三大類，每一型態都有不同的訊框格式，首先我們來介紹控制訊框格式，接下來兩小節再介紹資料和管理訊框格式。

控制訊框可區分為 RTS、CTS、ACK、PS_Poll、CF_End 與 CF_End+CF_Ack 等訊框，由訊框欄位中的 Type 和 Subtype 次欄位來分別表示（如表 15-4）。而各種控制訊框的『訊框控制』（Frame Control）欄位都相同，如圖 15-41 所示。圖 15-42 為各控制訊框的格式，其『訊框控制』欄位如圖 15-41 所示。然而控制訊框並沒有包含『訊框實體』（Frame Body）欄位，四個位址欄位中也依各訊框使用不同的欄位，但並不一定每一欄位都使用到。各訊框的說明如下：

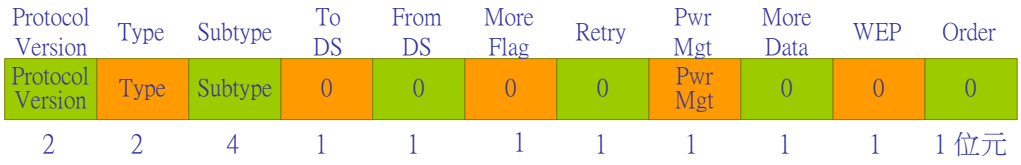

圖 15-41 控制訊框的控制欄位內容

圖 15-42 各控制訊框的格式

(D) RTS 訊框

『**RTS 訊框**』格式如圖 15-42 (a) 所示，其中 RA 為接收此訊框的位址；TA 為發送此訊框的位址，兩者位址皆是一個無線媒介的位址（如擷取點）。Duration 的值（單位為 μs）

為準備發送訊框的長度再加上一個 CTS 訊框、一個 ACK 訊框、以及三個 SIFS 間隔時間，而取整數計算。

(E) CTS 訊框

『**CTS 訊框**』格式如圖 15-42 (b) 所示，其中 TA 欄位內容應該等於上一個對應之 RTS 訊框的 TA 內容。Duration 值為前一個對應之 RTS 訊框中的 Duration 值，再減去傳送此 CTS 訊框及一個 SIFS 間隔時間，也採整數計算。

(F) ACK 訊框

『**ACK 訊框**』格式如圖 15-42 (c) 所示，其中 RA 的內容應該等於前一個對應訊框的 Address 2 欄位，前面訊框可能是 Data、Management 或 PS_Poll 等訊框。如果前一訊框的 More Fragment 欄位為 0 時，則本訊框的 Duration 的值應該設為 0；如果為 1 時，則本訊框的 Duration 的值為前一訊框的 Duration 值，再減掉傳送本訊框的時間和一個 SIFS 間隔時間，而採整數計算。

(G) PS_Poll 訊框

『**省電輪詢**』(**Power Save Poll, PS_Poll**) 訊框格式如圖 15-42 (d) 所示，其中 AID (Association ID) 是接收工作站和 AP 之間所建立的聯結號碼，而 AID 的最前面兩位元都應該為 1；BSSID 是接收工作站所屬的 AP 位址；TA 是傳送此訊框的 AP 位址。所有收到 PS_Poll 訊框者，都必須修正自己的 NAV 值，修正的值為傳送一個 ACK 訊框及一個 SIFS 間隔時間。

(H) CF_End 訊框

『**無競爭週期結束**』(**Contention-Free End, CF_End**) 訊框格式如圖 15-42 (e) 所示，其中 RA 為廣播位址；Duration 值為 0；BSSID 為隸屬於 AP 的工作站位址。

(I) CF_End + CF_Ack 訊框

『無競爭週期結束及回覆』(Contention-Free End and Acknowledge, CF_End+CF_Ack)

訊框格式如圖 15-42 (f) 所示，如同 CF_End 訊框一樣，其中 BSSID 為隸屬於 AP 中的工作站位址；RA 為廣播位址；Duration 的值為 0。

15-6-3 資料訊框格式

在表 15-4 中，雖然**『資料訊框』(Data Frame)**可依照 Type 和 Subtype 欄位，來區分各種資料訊框的使用時機，但訊框格式並沒有差異，訊框標頭也如同圖 15-38 一樣。但資料訊框會隨著傳輸時機，來改變位址欄位 (Address 1 ~ Address 4) 的表示方法。資料訊框傳送的時機如表 15-5 所示，其中以 To DS 和 From DS 欄位來區分，而位址表示方式如表 15-7 所示，其中 N/A 表示該欄位可以取消。

表 15-7 資料訊框的 Address 欄位內容

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

管理訊框是利用 Address 1 來存放目的位址(DA)、Address 2 存放來源工作站位址(SA)、Address 3 存放 BSSID 位址。其中 BSSID 為一個基本服務區 (BSS) 的識別碼，表示方式如同資料訊框的 BSSID 一樣。在所有無競爭週期 (CFP) 內傳送的管理訊框，Duration 欄位都設定為 32768；而在競爭週期 (DCF) 內，Duration 欄位會依照下列情況而異：

15-6-4 管理訊框格式

在 IEEE 802.11 規範下，管理訊框 (Management Frame) 可區分為 Beacon、Disassociation、Association Request、Association Response、Reassociation Request、Reassociation Response、Probe Request、Probe Response、Authentication、 Deauthentication 與 ATIM (Announcement Traffic Indication Message) 等 11 種訊框格式，訊框標頭如圖 15-43 所示 (減少 Address 4 欄位)。如同控制及資料訊框一樣，是由 Type 和 Subtype 欄位來區分各種訊框，如表 15-42 所示。

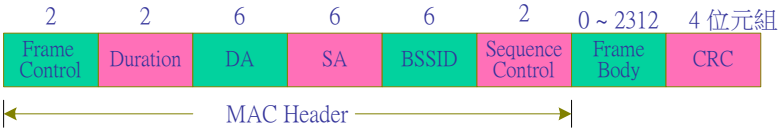

圖 15-43 管理訊框的格式

管理訊框是利用 Address 1 來存放目的位址(DA)、Address 2 存放來源工作站位址(SA)、Address 3 存放 BSSID 位址。其中 BSSID 為一個基本服務區（BSS）的識別碼，表示方式如同資料訊框的 BSSID 一樣。在所有無競爭週期（CFP）內傳送的管理訊框，Duration 欄位都設定為 32768；而在競爭週期（DCF）內，Duration 欄位會依照下列情況而異：

(1) 如果目的位址（DA）為一群體位址，則 Duration 的值為 0。

(2) 如果 More Fragment 欄位為 0，並且 DA 為一個別位址，則 Duration 的值（單位為 μs）為傳送一個 ACK 訊框所需時間，再加上一個 SIFS 間隔時間。

(3) 如果 More Fragment 欄位為 1，並且 DA 為一個別位址，則 Duration 的值為緊接著傳送下一個訊框的時間，再加上傳送兩個 ACK 訊框時間及三個 SIFS 間隔時間：

管理訊框是利用 Frame Body 來攜帶各種控制訊息，每一種管理訊框都有其各自的控制訊息，有關控制訊息部份請讀者參考 IEEE 802.11 規格書說明，本書侷限於篇幅不另介紹(太多了)。

15-7 IEEE 802.11 實體層

IEEE 802.11 在實體層方面，規範了三種傳輸方式：

(a) 跳頻展頻（Frequency Hopping Spread Spectrum, FHSS）

(b) 直接序列展頻（Direct Sequence Spread Spectrum, DSSS）

(c) 紅外線（Infrared, IR）

這裡值得注意的是，雖然展頻傳輸有如同軍方通訊的保密功能，然而在無線網路上最主要的功能是希望在共享頻段上提供一個傳輸通道；但在同一 BBS（Basic Service Set）內也只能供一部工作站使用該傳輸通道，超過兩部工作站使用該頻段則會發生碰撞的現象。亦即，

同一 BBS 內所使用的『虛擬隨機亂序列』(PNS) 都是相同，任何工作站都依此 PNS 來接收或傳遞訊號，因此，便有需要制定 CSMA/CA 協定來協調工作站之間的競爭行為。在 IEEE 802.11 規格中，FHSS 和 DSSS 都是使用 2.4 GHz 的 ISAM 頻道，以下針對各種傳輸規範加以介紹：(運作原理請參考 15-2 節說明)

15-7-1 跳頻展頻規範

『跳頻展頻』技術是在同步的情況下，通訊雙方利用相互協議的無線電波訊號來傳遞，而此訊號被載入在不同頻道之間跳越。在美國 FCC 的規定下，跳頻可使用的頻段為 2400 ~ 2483.5 MHz，必須使用 75 個以上的跳躍頻道 (Channel)，每一個頻道的頻寬為 1 MHz，發射功率不可大於 1 W，若加上天線不可超過 4 W；歐洲地區 ETS 規定，可使用頻段為 2400 ~ 2483.5 MHz，至少需有 20 個跳頻頻道，發射功率不可大於 100 mW；日本地區則使用 2471 ~ 2497 MHz 頻段，至少分為 10 個頻道。跳越相隔兩個頻道所需的『間隔時間』(Dwell Time) 最大值為 400 ms，而在 IEEE 802.11 中規定的間隔時間為 250 ms，亦即每秒至少跳越 4 次。

IEEE 802.11 FHSS 是使用 GFSK (Gaussian Frequency Shift Key) 的調變技術，基本頻寬為 1 Mbps (2 level GFSK)，同時 IEEE 802.11 也規範進階規格，採用 4 level GFSK，傳輸速率可達 2 Mbps。

『跳頻技術』是利用一個很寬的頻段來傳輸資料，雖然細分成許多小頻道，但傳輸訊號時在這些頻道之間跳躍的速度非常快，就好像使用了整個頻段，因此稱之為『展頻』。IEEE 802.11 同時也規範了全球『跳頻順序』(Hopping Sequence) 的形式，這主要目的是在建立一個 FHSS 無線網路時，溝通雙方必須使用相同的跳躍模式 (Pattern)，才能互相溝通，也同時降低無線電波之間的相互干擾 (Interference)，以下列出歐美和日本的跳躍模式：

(a) 北美與大部份歐洲地區：

Set1：0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 60, 63, 66, 69, 72, 75

Set2：1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 56, 58, 61, 64, 67, 70, 73, 76

Set3 : 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, 57, 59, 62, 65, 68, 71, 74, 77

(b) 日本：

Set1：6, 9, 12, 15

Set2：7, 10, 13, 16

Set3：8, 11, 14, 17

15-7-2 直接序列展頻規範

『直接序列展頻』(Direct Sequence Spread Spectrum, DSSS) 的基本原理，是將要傳送的基頻 (Base Band) 訊號轉換為能量較低、而頻寬更寬的展頻訊號傳送出去。IEEE 802.11 是利用 11-chips 的**『虛擬雜訊序列』(Pseudo Noise Sequence, PNS)** 將原始訊號展開，這種展頻碼有一個重要的特性，就是原始資料經過二次展頻處理後，會還原為原訊號。

11-chips 的數位結構為**『+1 –1 +1 +1 –1 +1 +1 +1 –1 –1 -1』**，原始訊號首先經由展頻碼將其展開為 11 倍的訊號 (如圖 15-6 所示)，這展頻後的訊號透過天線被發送出去，當接收端收到該訊號後，再利用相同的展頻碼將這訊號還原回原來訊號。在標準規範中，傳輸速率為 1 Mbps (BPSK 編碼) (可經由不同編碼技術來提高傳輸速率)，經過 11-chips 展頻後的頻寬為 22 MHz，亦即使用 DSSS 傳輸技術的頻寬需要 22 MHz；但又考慮同頻及鄰頻之間的干擾情形，還需要增加頻寬來間隔。因此，將 2.4 GHz 的頻帶以每頻道為 5 MHz 劃分為 14 個小頻道，而每一區域所使用 DSSS 傳輸頻段佔有 5 個小頻道，也就是傳輸頻寬與頻道間隔 (Channel Spacing，此處為 5 MHz) 共佔了 30 MHz 頻寬。這樣的結果減低了 DSSS 的使用率，也就是在同一個範圍內只能存在三個無線網路群組，當有更多群組欲加入時，便會產生互相干擾而減低傳輸效率。依照特地區環境不同，所採用的頻段也會有所不同，如下：

(a) 北美 (FCC/CA) :

1 (2.412 GHz) , 2 (2.417) , 3 (2.422) , 4 (2.427) , 5 (2.432) , 6 (2.437) , 7 (2.442) , 8 (2.447) , 9 (2.252) , 10 (2.457) , 11 (2.462)

(b) 歐洲 (ETSI) 與日本 (Telec) :

1（2.412 GHz）, 2（2.417）, 3（2.422）, 4（2.427）, 5（2.432）, 6（2.437）, 7（2.442）, 8（2.447）, 9（2.252）, 10（2.457）, 11（2.462）, 12（2.462）, 13（2.472）

15-7-3 紅外線規範

IEEE 802.11 規範中，**『紅外線』（Infrared, IR）**是採用**『散射式』（Defuse, DF）**的傳輸技術，這種傳輸模式並不要求發射端與接收端必須在同一線上（Line of Sight），但也侷限於某一區域，並沒有『游牧』 的功能。紅外線涵蓋的範圍很小，大約是 10 公尺左右，傳輸速率為 1～2 Mbps。IEEE 802.11 所規範的 IR 波長範圍是 850～950 nm，調變模式為 PPM（Pulse Position Modulation），最大輸出功率為 2 W。在 1 Mbps DF/IR 的標準中是採用 16-PPM（PPM with 16 Position）的調變技術；而在 2 Mbps DF/IR 的標準中是採用 4-PPM（PPM with 4 Positions）調變技術（編碼原理請參考 15-2-5 節介紹）。

15-8 IEEE 802.11 延伸規格

自從 1997 年 IEEE 802.11 規範被提出以後，隨著市場大量的推展，基本規範中的 2 Mbps 傳輸速率已不敷應用環境需求。緊接著 IEEE 802.11 工作小組於 1999 研訂出新的延伸規格：IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g。目前大部份的無線區域網路都採用 IEEE 802.11b，相信 IEEE 802.11a 與 IEEE 802.11g 的產品也將會很快問世。基本上，這些延伸規格的運作原理都和 IEEE 802.11 相同，只不過再提昇傳輸技術，來提高傳輸速率，使無線網路的傳輸速率能接近於有線網路，進而使無線網路的應用範圍更為廣闊。

15-8-1 IEEE 802.11b 規格

IEEE 802.11b 規範的實體層延伸自 802.11，為目前無線區域網路最普遍的規範，傳輸速率也接近**『有』**線的 Ethernet 網路，確實是**『無線 Ethernet』（Wireless Ethernet）**的代表作。802.11b 採用**『高速直接展頻』（High Rate DSSS, HR/DSSS）**技術，利用 2.4 GHz ISM 頻段，可提供的資料傳輸速率為 11 Mbps，使用的調變技術為 CCK（Complementary Code Keying）。為了相容於 IEEE 802.11 早期的 DSSS 規範，802.11b 規定其系統必須自動降低速率，使能與 2 Mbps 的 DSSS 相容。可見 IEEE 802.11b 中應提供兩種傳輸功能：其一為 HR/DSSS 模式，可提供 5.5 Mbps 與 11 Mbps 的傳輸速率；另一為 802.11 DSSS 模式，可提供 1 Mbps 和 2 Mbps 的速率，所以在 IEEE 802.11b 規範中有：1 Mbps、2 Mbps、5.5 Mbps、

以及 11 Mbps 等四種傳輸速率。其中 1 Mbps 採用 DBPSK（Differential Binary Phase Shift Keying）調變技術，2 Mbps 採用 DQPSK（Differential Quadrature Phase Shift Keying），這兩種都採用 11-chip 的展頻碼。

至於高速傳輸模組（HR/DSSS）（5.5 Mbps 與 11 Mbps）是採用 CCK 調變方式，展頻碼長度為 8，而且建構於互補碼（Complementary Code）的機制下，這種展頻碼隨時間展開而形成一種複數型態的 8-chip 記號。HR/DSSS 是利用每個符號週期（Symbol Period）傳送的資料，來區別 5.5 Mbps 或 11 Mbps，在 5.5 Mbps 的傳輸模式下，每個符號週期傳送 4 個位元；而在 11 Mbps 的模式下，每個符號週期是傳送 8 個位元。

15-8-2 IEEE 802.11a 規格

IEEE 802.11a 規範的實體層是採用 5 GHz 的 U-NII（Unlicensed Nation Information Infrastructure）頻段，使用 5.725 ~ 5.850 GHz 之間的頻段，因此有 125 MHz 的傳輸頻帶可以使用。另外，展頻傳輸系統是採用**『正交分頻多工』（Orthogonal Frequency Division Multiplexing, OFDM）**技術，OFDM 是利用多個頻道來同時傳送資料，以提高傳輸速率。而且 IEEE 802.11a 為了合乎各種情況使用，可採用不同的調變方式，提供多種傳輸速率，如表 15-8 所示。其中調變方式有 BPSK（Binary Phase-Shift Keying）、QPSK（Quadrature Phase-Shift Keying）以及 QAM（Quadrature Amplitude Modulation）。

表 15-8 IEEE 802.11a 的各種傳輸速率

傳輸速率	調變方式
6 Mbps	BPSK
9 Mbps	BPSK
12 Mbps	QPSK
18 Mbps	QPSK
24 Mbps	16 QAM
36 Mbps	16 QAM
48 Mbps	64 QAM
54 Mbps	64 QAM

OFDM 技術也如同傳統 FDM 技術一樣，都是將所使用的頻帶劃分為若干個小頻道，再分別將訊號載入每一頻道上，來提高傳輸速率。譬如，每一頻道可傳送 8 Kbits/s，則 100 個

頻道便可以傳送 800 Kbits/s；至於將傳輸資料載入頻道的調變技術有 BPSK、QPSK 與 QAM 等技術。但 OFDM 與 FDM 有很大的不同點，在 FDM 技術上為了避免頻道之間的訊號互相產生干擾，頻道之間都必須預留某些空閒頻寬，如此便會造成許多頻寬的浪費。OFDM 不但不必預留空閒頻寬，甚至允許頻道之間的頻率互相重疊，可節省許多頻寬，也就是說，同一個頻帶頻寬，OFDM 所能劃分的小頻道比 OFM 技術還要多，亦是，所能承載的傳輸速率也比較高，如圖 15-44 所示。

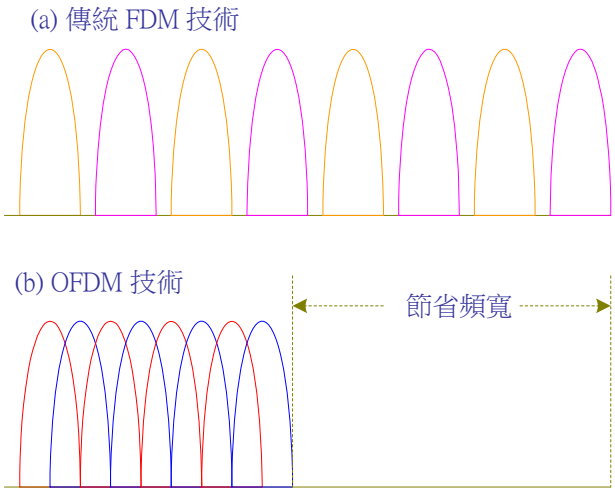

圖 15-44 OFDM 與傳統 FDM 之比較

從另一個觀點來看，OFDM 好像是一個多工技術，而非展頻技術。但由通訊連線的對象而言，它的確也可說是展頻技術的一種，這是因為雖然 OFDM 利用多個頻道來傳送資料（又稱為多重承載），但也可以依照通訊環境來更改每一頻道的傳輸速率，乃至停止某些頻道的傳送（此功能與 ADSL 連線相似）。此功能剛好可用來分辨多重路徑訊號的傳輸，在許多路徑到達的訊號之中，選擇功率較強的訊號，這也是 OFDM 應用於無線網路的主要原因。

在北美規格中，5 GHz NII 頻帶被切分為三個頻寬為 100 MHz 的頻段，較低頻帶（Lower Band）為 5.15 ~ 5.25 GHz、中頻帶（Middle Band）為 5.25 ~ 5.35 GHz、最高頻帶（Upper Band）為 5.725 ~ 5.825 GHz；並且規範各頻帶的輸出功率：Lower Band 為 40 mW、Middle Band 為 200 mW、Upper Band 為 800 mW，因此 Lower Band 和 Middle Band 比較適合於室內的無線網路使用，而 Upper Band 的輸出功率較強，可做為戶外網路聯結使用。

15-8-3 IEEE 802.11g 規範

IEEE 802.11g 目前還是一個草案（2003 年之前）。由於 802.11a 雖然可將傳輸速率提高到 55 Mbps，但它所用的傳輸頻道為 5 GHz U-NII，並不相容於 802.11b 所使用的 2.4 GHz ISM 頻段。因此，802.11g 希望在 2.4 GHz ISM 頻段中將傳輸速率提高到 54 Mbps，並且保證能和現有的 802.11b 相容，皆採用 DSSS 展頻技術。

在 802.11g 規範中，它必須支援 OFDM 和 CCK 兩種調變方式，其中 OFDM 調變模式可以獲得較高的傳輸速率（大於 20 Mbps，最高可達 54 Mbps），而 CCK 則是與現有的 802.11b 相容。同時在草案中也提出兩個選項的調變模式：一者是由 Intersil 提出的 CCK/OFDM；另一者是 TI 提出的 PBCC-22（Packet Binary Convolution Coding）。在 CCK/OFDM 模式下，封包標頭（Header）採用 CCK 調變，而承載（Payload）採用 OFDM 調變方式；然而在 PBCC 模式下，封包標頭以 CCK 調變，承載則以 PBCC 調變上。

CCK、OFDM 與 PBCC 等調變模式之間最大的不同在於訊號的承載方式，CCK 與 PBCC 都是屬於**『單一承載』(Single Carrier)**，而 OFDM 是屬於**『多重承載』(Multiple Carrier)**的調變模式。PBCC 與 CCK 的差異在於對訊號的處理，PBCC 使用 8-PSK 編碼，而 CCK 則採用 BPSK/QPSK 編碼方式。

15-8-4 安全性規範

在 IEEE 802.11 系列的標準裡，網路安全規範係採用 WEP（Wired Equivalent Privacy）協定，而通訊雙方是以**『秘密鑰匙』(Secret Key)** 做為雙方處理資料的依據。處理方法是資料傳輸之前，以 RC4 演算法先產生 24 Bits 的起始向量（IV），並且與密匙兩項參數彙整演算，再和明文資料封包進行 XOR 運算，來完成加密處理，最後附加起始向量發送出去。

WEP 的安全缺失是在網路上蒐集大量封包後，便有機會歸納出初始向量的編碼型態，依序找出密匙，進而解讀出原始資料。舉例來說，若每個封包長度為 1500 Bytes，所有初始向量在 5 個小時內將會被使用完，也就是會產生另一個相同的初始向量，如此便可輕易找出初始向量的順序。

至於密匙長度方面，儘管 128 bits 要比 40 bits 長，但由於真正的關鍵在於 RC4 編碼演算法機制本身，如採用 128 bits，最多也僅能延長被破解的時間效果而已。更何況目前無線

區域網路都只設定單一固定的密匙，也就是說，當網路封包被破解時，所有使用者的資料就完全曝露在駭客威脅之下，面臨資料遭到取、破壞或是成為免費的上網平台。

由上述可以瞭解，雖然無線區域網路提供了許多方便性，但它的安全性問題一直是最受詬病的。因此，提高無線網路安全的問題，也有許多方案被提出來，雖然這些方案還未成熟，仍值得我們來探討：

(1) 修正 WEP 機制：目前 IEEE 802.11e 工作小組正積極修正 WEP 機制，其中包含無線網路的 QoS、網路安全、以及用戶認證等功能。

(2) 採用 IPSec 技術：將 VPN(Virtual Private Network)的 IPSec 技術加入無線網路上，以提高網路安全。

15-9 其他無線網路

在無線區域網路領域裡，並不只有 IEEE 802.11 系列規範，其實還存在著許多網路型態，同時被廣泛應用中，其中較常見的有 HomeRF、HiperLAN 與 Bluetooth，以下分別介紹前兩個規範，至於 Bluetooth 技術將會在下一章介紹。

15-9-1 HomeRF 網路

HomeRF（Home Radio Frequency）是由 ITU（International Telecommunication Union）所制定，這個標準是為了提供一個便宜，同時可以支援語音及數據的家庭網路，而功率也不高，大約為 100 mW，涵蓋範圍約為 50 公尺。HomeRF 是以**『共享式無線存取協定』(Shared Wireless Access Protocol, SWAP)**為基礎，而採用跳頻展頻 (FHSS) 傳輸模式，也運用於 2.4 GHz ISM 頻段。

HomeRF 可說是簡化的 IEEE 802.11 FHSS，亦採用 CSMA/CA 的存取協定，但取消了 RTS/CTS 機制以及無競爭傳輸服務(PCF)。在傳輸模式方面，FHSS 的跳越頻率為每秒 50 次。在資料編碼方面，語音訊號以 DECT（Digital European Cordless Telephone）方式；資料編碼同時支援 2-Level FSK（1 Mbps 傳輸速率）及 4-Level FSK（2 Mbps 傳輸速率）。

為了可以在同一空間中同時存在多個無線網路，HomeRF 的位址採用了 48 位元格式，這個碼類似於 IEEE 802.11 的 ESS ID。在保密方面，使用 Blowfish 加密法來保護資料的傳輸。

在語音方面，除了採用 DECT 標準外，也使用分時多工（TDM）的多重存取技術，可支援 6 個全雙工的數位語音頻道，每個頻道的傳輸率為 32 Kbps。在資料框架中，可以包含 TCP/IP 的資料及語音訊號，一個網路可以提供 128 個節點。

15-9-2 HiperLAN/2 網路

HiperLAN（High Performance Radio LAN）是由**『歐洲電信標準協會』（Europen Telecommunication Standards Institute, ETSI）**所制定的眾多標準之一。ETSI 所發展一系列**『寬頻無線電存取網路』（Broadband Radio Access Network, BRAN）**的無線網路規範中，一共涵蓋了四個標準：HiperLAN/1、HiperLAN/2、HiperLink 與 HiperAccess。各種規範都有其應用範圍，其中 HiperLAN/1 與 HiperLAN/2 為無線區域網路（WLAN），而 HiperAccess 是作為長距離的無線網路連接，HiperLink 為無線寬頻聯結；由此可以觀察到，ETSI 在無線網路所製作的標準比 IEEE 802.11 完善。IEEE 802.11 的無線網路還是侷限於有線網路之間的聯結，亦即區域網路上雖可以使用 IEEE 802.11 系列的標準，但在傳輸骨幹方面還是要仰賴原有的有線網路。ETSI 的標準則不然，他們希望提出一個完整的無線網路環境，由區域網路到傳輸骨幹，甚至遠距離之間的傳輸標準，都能一併提出完整的解決方案。圖 15-45 為各種標準在無線網路上的應用。

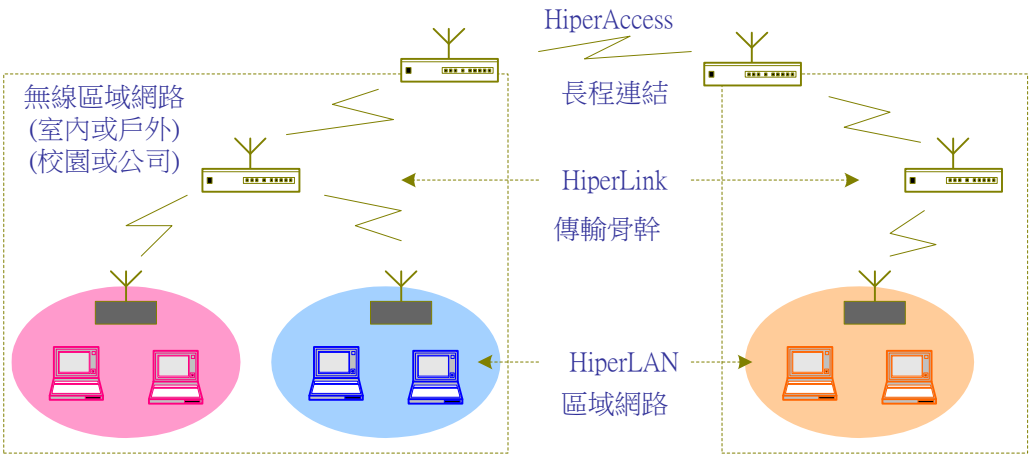

圖 15-45 ETSI BRAN 系列在無線網路的應用

表 15-9 為 ETSI BRAN 系列的規範，由表中可以發現，雖然 HiperLAN/1 的傳輸速度達到 23.5 Mbps（比 IEEE 802.11b 還要高），但還是侷限於一般無線區域網網路的規範；然而 HiperLAN/2 卻有很大的變革，它可選擇長訊框或短訊框傳送，短訊框的格式甚至符合 ATM 網路的 53 Bytes，因此也稱之為『**Wireless ATM**』。由此可見，用 HiperLAN/2 來連結一般網路的 ATM 傳輸骨幹會較為容易，而且它的傳輸速率也可達 54 Mbps。

總括來看，目前無線網路最具競爭力的規格就是 HiperLAN/2 和 IEEE 802.11a，而兩種規範之間又有許多相符的地方，因此，許多人相信它們最終很有可能會被整合在一起。以下我們就針對 HiperLAN/2 來詳加介紹，相信這對大家了解未來無線網路的發展將會非常有幫助。

表 15-9 ETSI BRAN 系列標準的規範

規範	HiperLAN/1	HiperLAN/2	HiperAccess	HiperLink
網路型態	Wireless LAN	ATM 短程連結	ATM 長程連結	無線寬頻連結
操作環境	室內/戶外	室內/戶外	戶外	室內/戶外
最大距離	50 公尺	50 公尺	5000 公尺	150 公尺
頻段	5 GHz	5 GHz	5 GHz	17 GHz
傳輸速率	23.5 Mbps	54 Mbps	25 Mbps	155 Mbps
最大功率	1 W	1 W	1 W	100 mW

HiperLAN/2 的特性

HiperLAN/2 最大的特色是高傳輸速率 – 54 Mbps，並且可以同時支援資料、影音、以及視訊資料的傳遞。如同 IEEE 802.11a 一樣，它也採用 5 GHz 頻段及 OFDM 傳輸技術。HiperLAN/2 的特性簡述如下：

(1) 高傳輸率：HiperLAN 利用 OFDM 的傳輸技術，在 5 GHz 頻段上傳輸，並可用不同的速率（最高 54 Mbps）來進行。OFDM 可對多重路徑（Multi-path）的現象做有

效的解析，因此非常適合於室內使用。室內的涵蓋範圍可達 50 公尺，戶外可達 150 公尺。

(2) 連結導向：針對媒介存取方面，HiperLAN/2 採用集中管理的連結導向。資料在傳遞之前必須先建立連線，連結技術是採用『**分時多工**』(**Time Division Multiplex**)系統，連結模式有點對點（Point-to-Point）與點對多點（Point-to -Multipoint）等兩種。

(3) QoS 功能：在連結導向模式中，可以針對連線品質來分配傳輸量，藉此達成 QoS 服務品質的要求。也因此，HiperLAN/2 適合語音、視訊的傳輸。

(4) 自動頻寬分配：HiperLAN 為集中控制，可依照不同連線之間的頻寬使用量，來選擇連線要求或分配其他連線服務，因此，可輕易達成自動頻寬分配。

(5) 安全系統：HiperLAN/2 採用 DES（Data Encryption Standard）及 3DES 加密標準，提高傳輸資料的隱密性。

HiperLAN/2 協定堆疊

圖 15-46 為 HiperLAN/2 的協定堆疊，包含了三個層次，簡述如下：

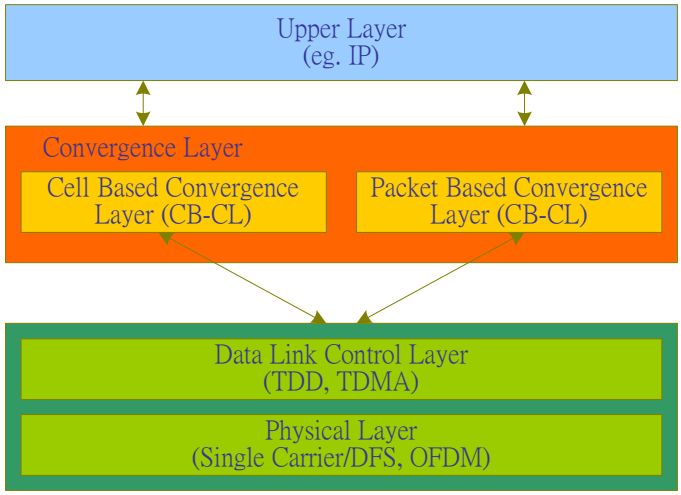

圖 15-46 HiperLAN/2 協定堆疊

(1) 收斂層（Convergence Layer）：收斂層是連接上層（網路層）通訊協定與資料連結，上層通訊協定可以是 IP 或 IPX 等等，主要的功能是轉換之間的資料格式。為了符合不同環境的應用，目前有 Packet-Based 與 Cell-Based 等兩種型態。如果 HiperLNA/2 是連結一般區域網路（如 Ethernet），則使用 Packet-Based 型態（長訊

框格式）；如果是連結 ATM 網路，則使用 Cell-Based 型態（符合 ATM Cell 的 53 Bytes）。

(2) 資料鏈路控制層（Data-Link Control Layer）: 這個層次是 HiperLAN/2 的主要核心，其功能就如同交換機一般。HiperLAN/2 是連接導向機制，它不同於 IEEE 802.11 系列的分散式控制，反之針對傳輸媒介的存取都是由此層次來集中分配。它採用**『分時雙工』（Time-Division Duplex, TDD）**和**『動態分時多工存取』（DynamicTime-Division Multiple Access, DTMA）**的多工存取技術，這種模式是利用時槽（Time Slot）的觀念，讓上傳（Up-Link）及下傳（Down-Link）可以在同一時槽之內進行傳遞。

(3) 實體層（Physical Layer）: HiperLAN/2 的實體層是採用 OFDM 傳輸方式，這種方式的基本概念就是將傳輸頻道分為若干個小頻道，而將傳輸資料分配到這些小頻道，同時平行發送出去。不過在實際應用時，它還會選擇那些傳輸不良的小頻道來調整傳輸速率，這對多重路徑的選擇非常有好處。例如某一些小頻道會因折射而傳輸不良，這時便可減低或停止這些頻道的傳輸，於是整個系統不僅不會因而中斷，反而能提昇整體的速率。HiperLAN/2 可提供多種傳輸速率，其調變方式如表 10-10 所示。

表 15-10 HiperLAN/2 的調變方式

模式	調變方式	傳輸速率
1	BPSK	6 Mbps
2	BPSK	9 Mbps
3	QPSK	12 Mbps
4	QPSK	18 Mbps
5	16 QAM	27 Mbps
6	16 QAM	36 Mbps
7	64 QAM	54 Mbps

HiperLAN/2 運作方式

在 HiperLAN/2 規範中，提到兩種運作方式：**『基礎架構網路』（Infrastructure Network）**與**『漫遊網路』（Roaming Network）**。圖 15-47 為基礎架構網路，在多個 HiperLAN/2 網路

之間透過固定網路的連結(如 Ethernet 或 ATM)，有線網路做為傳輸骨幹，在 HiperLAN/2 網路中，『**漫遊終端設備**』(**Mobile Terminal, MT**) 透過『**存取點**』(**Access Point, AP**) 連結到固定網路。

當 MT 啟動後，首先測量訊號強度來選擇適合的 AP 連線，並且向 AP 要求登錄並取得一個 MAC-ID，經認證程序或加密作業後，MT 和 IP 之間便可以通訊。當 MT 移動時，如果偵測到另一個 AP 訊號較強，AP 之間便會產生換手(Handover 或 Hand-off)，讓 MT 不會產生斷線的現象。

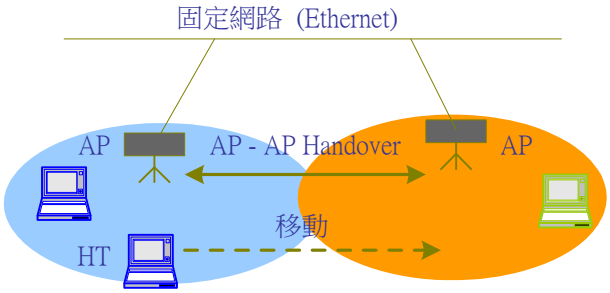

圖 15-47 HiperLAN/2 連結固定網路之範例

圖 15-48 為『漫遊網路』型態，漫遊終端設備 (MT) 在網路內移動，各個 AP 之間只要透過 HiperLAN/2 (H/2) Handover 交換即可，但 MT 必須做 MAC-ID 和 IEEE 位址格式轉換。如果漫遊到另一個網路，MT 必須做 IP 位址、IEEE 位址和 MAC-ID 之間的轉換 (類似 ARP 功能)。一般 MT 在不同網路之間移動，IP 網路位址會隨不同網路而更改；但使用者不可能每移動至另一個網路就需要重新設定網路位址，因此，這方面必須由 Mobile IP 協定來完成。比較簡單的做法是，MT 移動到任何一個網路，即由該網路的 DHCP 伺服器分配一個動態 IP 給 MT。

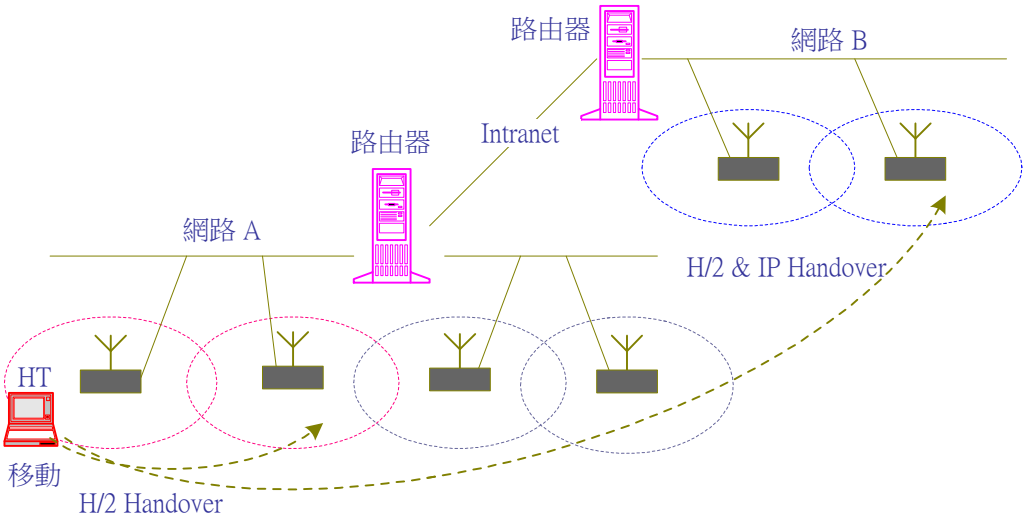

圖 15-48 HiperLAN/2 漫遊網路之範例

依目前無線網路的發展趨勢而言，ETSI/BRAN 系統 (歐洲規格) 和 IEEE 802.11 系列互為主要競爭對象，然而在無線寬頻方面，IEEE 802.11a 和 HiperLAN/2 又是兩大主流發展規格。兩個規範間的差異主要是在媒介存取技術方面，IEEE 802.11a 採用分散式的 CSMA/CA 協定，而 HiperLAN/2 使用集中控制式的 TDD 和 TDMA 機制；其次，雖然 IEEE 802.11a 的 PCF 服務也可以提供 QoS 的功能，但標準規範一直還未定案，也無法如 HiperLAN/2 的 QoS 那麼完善。另一方面，無線區域網路與行動電話之間的結合，也是最高的利益所在，雖然雙方在這方面都有很大的發展潛力，但以目前情況而言，HiperLAN/2 似乎略勝一籌，但未來的發展尚無法預料。表 15-11 為 802.11 系列與 HiperLAN/2 的規格比較，供讀者做個參考 (有關 TDD 與 DTMA 技術請參考下一章 Bluetooth 介紹)。

表 15-11 HiperLAN/2 與 IEEE 802.11 系列的比較

特性	802.11	802.11b	802.11a	HiperLAN/2
傳輸頻段	2.4 GHz	2.4 GHz	5 GHz	5 GHz
最高傳輸速率	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Layer 3 最高速率	1.2 Mbps	5 Mbps	32 Mbps	32 Mbps
媒介存取	CSMA/CA	CSMA/CA	CSMA/CA	TDD/TDMA
連接性	Conn.-less	Conn.-less	Conn.-less	Conn.-oriented

群播	Yes	Yes	Yes	Yes
QoS 功能	(PCF)	(PCF)	(PCF)	ATM/802.1p
展頻方式	DSSS/FHSS	DSSS/FHSS	OFDM	Single Carrier with Dynamic Frequency Selection
認證（資料加密）	RC4-40	RC4-40	RC4-40	DES, 3DES, X.509
固定網路連結	Ethernet	Ethernet	Ethernet	Ethernet, IP, ATM,
管理方式	802.11 MIB	802.11 MIB	802.11 MIB	HiperLAN/2 MIB
無線電波鏈路品質控制	No	No	No	Link Adaption

習題

1. 請簡述無線網路有哪些優點？
2. 請簡述架設無線網路應注意哪些事項？
3. 何謂『展頻』（Spread Spectrum）技術？
4. 何謂『虛擬雜訊序列』（Pseudo-Noise Sequence）？功能為何？
5. 請簡略說明『跳頻展頻』（Frequency Hopping Spread Spectrum）傳輸技術的運作原理。
6. 請簡略說明『直接序列展頻』（Direct Sequence Spread Spectrum）傳輸技術的運作原理。
7. 何謂『多重路徑訊號』（Multi-Path Fading）？為何直接序列展頻傳輸系統對於多重路徑有較高的分析能力？
8. 何謂『分頻多重存取技術』（FDMA）？
9. 何謂『分時多重存取技術』（TDMA）？
10. 何謂『分碼多重存取技術』（CDMA）？
11. 何謂『分域多重存取技術』（SDMA）？
12. 紅外線（IR）傳輸技術有哪三種模式？請分別敘述其特性。
13. 請說明紅外線傳輸技術所採用『相位位置調變』（Pulse Position Modulation）的運作原理（以 16-PPM 為範例）。
14. 請說明無線網路中的兩個基本架構:『對等架構』(AD Hoc)與『基礎架構』(Infrastructure)的特性。
15. 請繪圖說明『無線區域網路』（Wireless LAN, WLAN）的架構。
16. 在 IEEE 802.11 規範中有『工作站服務』（SS）與『分散式系統服務』（DSS），請簡略說明這兩個服務架構所提供的功能。
17. 請說明 CSMA/CA 協定的運作原理？並比較它與 CSMA/CD 協定有何差異？
18. 何謂『分散式協調功能』（DCF）？

19. 何謂『集中式協調功能』（PCF）？

20. 請簡略說明 IEEE 802.11 媒介存取的基本存取機制，並說明如何來分辨不同的存取功能？

21. 何謂『RTS/CTS』協調功能？

22. 請說明如何達成『虛擬載波偵測』（Virtual Carreir Sense）的功能？

23. 請說明 RTS/CTS 機制如何解決『隱藏工作站』（Hidden Terminals）的問題？

24. 請說明 CSMA/CA 協定的後退演算法。

25. 何謂 IEEE 802.11 的『超級訊框』（Superframe）？並說明如何保持固定的出現率？

26. 請說明『集中式協調功能』（PCF）的基本運作程序。

27. 在 IEEE 802.11 規範中，提出哪兩種認證方式？

28. 何謂『開放系統式』（Open System）認證方式？並請說明其運作程序。

29. 何謂『共享密匙式』（Shared Key）認證方式，並請說明其運作程序。

30. 請說明 IEEE 802.11『有線等效保密』（WEP）演算法的運作程序？

31. 請說明 WEP 演算法中『初始向量』（IV）所扮演的角色為何？

32. 請說明 IEEE 802.11a 延伸規格中『正交分頻多工』（OFDM）傳輸技術的基本原理？

33. 何謂『Wireless LAN』？