



第十三章

IEEE 802.11 Wireless LAN 網路

13.1 網路架構及特性簡介

由於可攜式電腦（包含筆記型電腦 (**notebook**) 和掌上型電腦 (**laptop**)）普及率的快速成長，無線區域網路對今日的電腦及通訊工業來講，將成爲一項重要的觀念及技術。在無線區域網路的架構中，電腦主機不需要像在傳統的有線網路裡，必需保持固定在網路架構中的某個節點上，而是可以在任意的時間作任何的移動，也能對網路上的資料作任意的擷取。大體說來，無線網路有四項特性與傳統的有線網路不同：

一、無線網路的目的位址(**Destination Address**)通常不等於目的位置(**Destination Location**)：

在有線網路裡，一個位址通常就代表一個固定的位置，然而在無線網路裡，這件事不一定成立，因爲在無線網路中，事先被給定位址的一部電腦，隨時都有可能移動到不同的地方。

二、無線網路的傳輸媒介會影響整體網路的設計：

無線網路的實體層和有線網路的實體層基本上有很大的不同，無線網路的實體層有下列特性：

點和點之間的連結範圍是有限的，因爲這牽涉到訊號強弱的關係。

使用了一個需要共享的傳輸媒介。

傳送的訊號未被保護，易受外來雜訊干擾。

在資料傳送的可靠性來講，較有線網路來的差。

具有動態的網路拓模結構。

因爲上述的原因，使得設計整個網路的軟硬體架構，就會和傳統的有線網路不同。舉例而言，由於訊號傳送範圍的受限，使得無線區域網路硬體架構的設計，就必需考慮到只能在一個有著合理幾何距離的區域內。

三、無線網路要有能力處理會移動的工作站：

對無線網路來講，一個重要的要求就是，不但能處理可攜式的工作站 (**portable station**)，更要能處理移動式的工作站 (**mobile station**)，可攜式的工作站也會從某一個位置移動到另一個位置，但長時間來看，它通常還是會固定在某一個位置上。而移動式的工作站就有可能在短時間內不斷的移動，且會在移動中仍對網路上的資料作擷取。

四、無線網路和其它 **IEEE 802** 網路層間的關係不同：

爲了達到網路的透明化，無線區域網路希望做到在邏輯鏈結層就能和別的網路相通，這使得無線區域網路必需將處理移動性工作站及保持資料傳送可靠性的能力全做在網路媒介擷取層 (**MAC Layer**) 中，這和傳統有線網路在媒介擷取層所需具有的功能是不同的。

無線區域網路正逐漸受到重視，爲了使各種競爭產品之間能相容互通，標準的製定就成了重要的工作，而 **IEEE 802.11** 無線區域網路 (**wireless LAN**) 的標準就在這樣的情況下誕生。

IEEE 802.11 主要目的是要製定一套適合在無線區域網路環境下作業的通訊協定，最重要的工作，就是要製定出 **MAC** 層和實體層。因此 **IEEE 802.11** 的參考模式主要分成兩部份，第一部份是製定出適用於所有無線網路系統的 **MAC** 規格，設計出和實體層無關的 **MAC** 協定。第二部份則是製定出和傳輸媒介相關的 **PHY** 規格。**IEEE 802.11** 所支援的每一種傳輸訊號頻寬，都有不同的 **PHY** 規格。例如，**915MHz** 頻寬、**2.4GHz** 和 **5.2GHz** 頻寬以及紅外線頻寬等，都有不同的 **PHY** 規格。此外功率的管理和時限性的服務等也包括在 **IEEE 802.11** 的定義範圍內。本章討論的重點將著重在 **IEEE 802.11** 所製訂出的 **MAC** 通訊協定上。**IEEE 802.11** 無線區域網路的主要特性如下：

多重傳輸速率。**IEEE 802.11**可以讓工作站使用不同的傳輸速率（單位爲**100kbps**）在網路上通訊。例如 **0.5 Mbps**, **1 Mbps** 或 **2 Mbps**。

訊框爲 **IEEE 802.11** 訊框。

傳輸媒介爲無線電。

基本通訊協定爲 **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**。如果同時有二個或二個以上的工作站傳送訊框將造成衝撞，發生衝撞的訊框視爲無效並丟棄。**IEEE 802.11**所採用的 **CSMA/CA**通訊協定雖可避免大部分不必要的衝撞，但仍無法完全排除衝撞的現象。因此只適合用來傳送非即時性的資料。

提供兩種傳送服務。分散式協調功能 (**Distributed Coordination Function, DCF**) 使用 **CSMA/CA**，適合傳輸非即時資訊。集中式協調功能 (**Point Coordination Function, PCF**) 由網路協調者 (**Point Coordinator**) 掌控並且以輪詢 (**polling**) 的方式安排工作站傳送訊框的時機及順序。由於工作站傳送的時間可事先安排，因此可提供保證傳送延遲的服務。

非即時傳輸使用之頻寬不保證公平分配。在 **DCF** 部份由於工作站利用 **CSMA/CA** 通訊協定來互相競爭傳送訊框的機會，並沒有輪流傳送的特性，因此每個工作站實際使用的頻寬量可能不同。

提供認證 (**Authentication**) 及資料保密 (**Privacy**) 功能。無線電是一種開放性的介質，任何人都可以很容易的干擾或竊聽。任證是確任對方的身分，免得在不知情的狀況下因爲與陌生人通訊而洩漏重要的資訊。保密是利用加密 (**Encryption**) 及解密 (**Decryption**) 的技術來保護傳送的資料，使得竊聽者即使竊聽到資料也無法得知其內容。

較不適合多媒體資訊傳輸。雖然網路提供保證的傳送延遲服務，但目前最高的傳送速率只有 **2 Mbps**。此頻寬尚不足以應付具有即時要求的多媒體資訊。如果無線網路上同時存在許多工作站，則每一部工作站平均分配到的頻寬將更少。

13.2 無線區域網路硬體架構

要了解無線區域網路硬體架構之前，要先了解無線區域網路協定的功能需求，因為 **IEEE 802.11** 就是根据這些需求，擬訂了一套無線區域網路系統的基本架構。**IEEE 802.11**將最低的功能頻寬訂為 **1Mbps**，這對於一般性的操作，像檔案傳輸、程式載入、交易處理等，是絕對必要的。對於需要傳輸即時資料的應用軟體，像數位式聲音、影像等，**IEEE 802.11**也提供了時限性 (**time bounded**)的服務。另外，**IEEE 802.11**也定義了包括財務、辦公室、學校以及工業大樓等各種環境中的可靠操作需求。此外，還定義了行動式的電腦系統至少必須支援每小時幾哩的行人速度。而爲了整合這些需求，**IEEE 802.11**就製訂出兩種不同類型的無線區域網路基本架構：

- 有基礎架構的無線區域網路 (**Infrastructure Wireless LAN**)
- 無基礎架構的無線區域網路 (**Ad Hoc Wireless LAN**)

所謂的基礎架構通常指的就是一個現存的有線網路分散式系統 (**wired distribution system**)，在這種網路架構中，會存在一種特別的節點，稱作擷取點 (**access points**)，這個擷取點的功能就是要將一個或多個的無線區域網路和現存的有線網路分散系統相連結，以提供某個無線區域網路中的工作站，能和較遠距離的另一個無線區域網路的工作站通訊，另一方面也促使無線區域網路中的工作站，能擷取有線分散式系統中的網路資源。這一類型的無線網路通訊範圍，通常是以同一棟建築物出現，例如，商店、醫院、或是同一棟樓層。

無基礎架構的無線區域網路主要是要提供不限量的用戶，能即時架設起無線通信網路，在這種架構中，通常任二個用戶間都可直接通訊，這一類的無線網路架構在會議室裡經常用得上。**IEEE 802.11**所製訂的架構允許「無基礎架構的無線區域網路」和「有基礎架構的無線區域網路」同時使用同一套基本擷取協定。然而，一般討論 **IEEE 802.11** 無線區域網路硬体架構，還是偏重在「有基礎架構的無線網路上」。**IEEE 802.11** 所定義的無線網路硬体架構，主要由下列元件所組成（參考圖13-1）：

- Wireless Medium (WM)**：無線傳輸媒介，無線區域網路實體層所使用到的傳輸媒介。
- Station (STA)**：工作站，任何設備只要擁有 **IEEE 802.11** 的 **MAC** 層和 **PHY** 層的介面，就可稱爲一個工作站。
- Station Services (SS)**：工作站服務，提供工作站送收資料的服務。
- Basic Service Area (BSA)**：在「有基礎架構的無線區域網路」中，每一個幾何上的建構區塊 (**building block**) 就稱爲一個基本服務區域 (**Basic Service Area**, 簡稱 **BSA**)，每一建構區塊的大小依該無線工作站的環境和功率而定。
- Basic Service Set (BSS)**：基本服務區中所有工作站的集合。
- Distribute System (DS)**：分散式系統，通常是由有線網路所構成，可將數個 **BSAs** 連結起來。
- Access Point (AP)**：擷取點，連結 **BSS** 和 **DS** 的設備，不但具有工作站的功能，還提供工作站具有擷取分散式系統的能力，通常在一個 **BSA** 內會有一個擷取點。
- Extended Service Area (ESA)**：數個 **BSAs** 經由 **DS** 連結在一起，所形成的區域，就叫作一個擴充服務區。
- Extended Service Set (ESS)**：數個經由分散式系統所連接的 **BSS** 中的每一基本工作站集，形成一個擴充服務集。
- Distribution System Services (DSS)**：分散式系統所提供的服務，使得資料能在不同的 **BSSs** 間傳送。

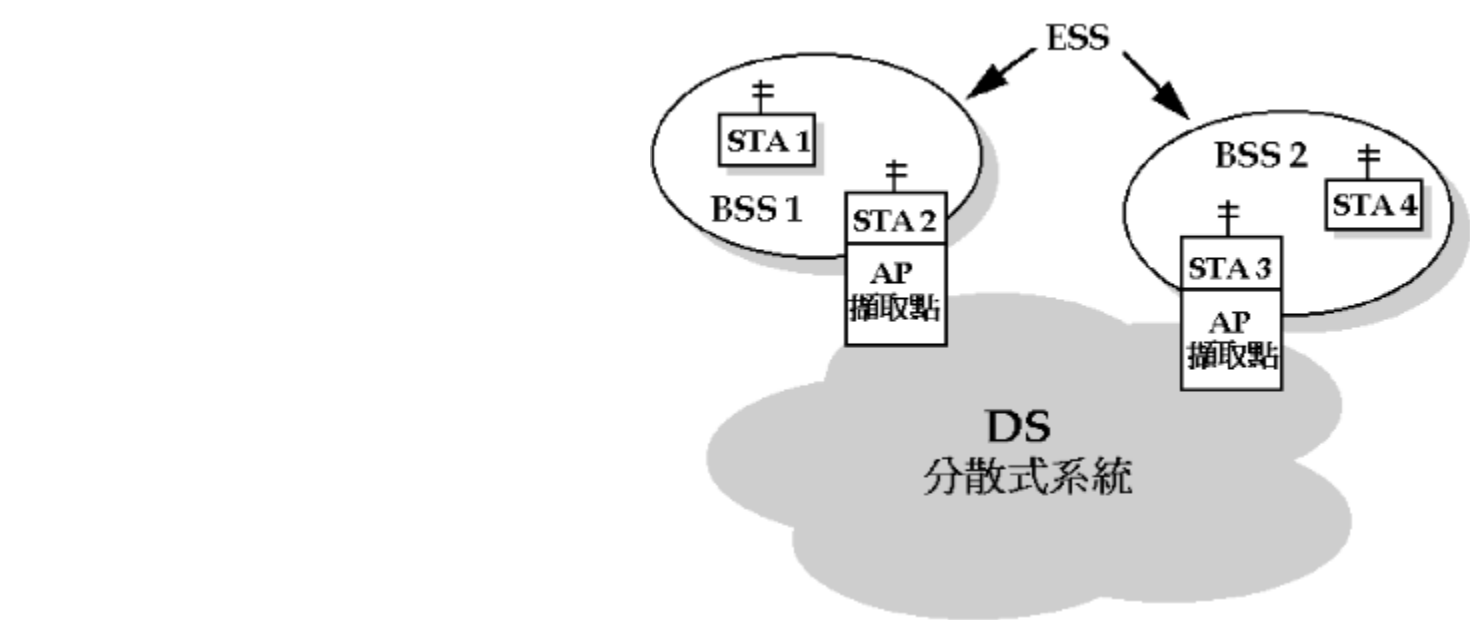


圖13-1 無線網路硬体架構組成元件

IEEE 802.11 無線網路系統與傳統的有線區域網路相連結是經由一個稱爲「埠接器」(**Portal**)的連結設備，如圖13-2 所示。埠接器的主要功能是將資料從有線區域網路送入無線網路系統，或將來自無線區域網路的資料送入有線區域網路中。這之間除了必須考慮通訊協定的不同外也要考慮到傳輸媒介的差異。

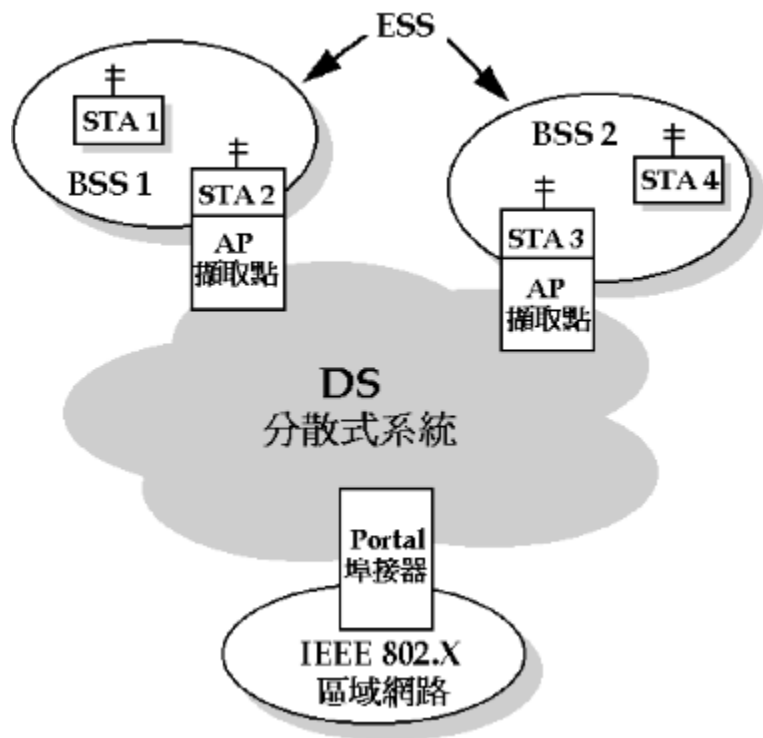


圖13-2 無線區域網路與有線區域網路之相連結

13.3 無線區域網路軟體架構

IEEE 802.11的軟體架構主要可分為工作站軟體和分散式系統軟體二部份。標準中並無規定應如何實作此分散式系統軟體，取而代之的是，它描述了這個分散式系統應提供那些服務才能滿足整個系統所需。因此，無線網路的軟體架構可看成是由下列二大類的服務所組成（參考圖13-3）：

工作站服務 (Station Services, 簡稱 SS), 由工作站所提供。此類服務提供工作站具有正確送收資料的能力，另外也考慮傳送資料的安全性。包含下列兩種服務：

身份確認服務(Authentication)

隱密性服務(Privacy)

分散式系統服務(Distribution System Services, 簡稱 DSS), 由分散式系統所提供。此類服務使 MAC 訊框能在同一個 ESS 中的不同 BSS 間傳送。無論工作站移動到那裡，也都要能收到它該收到的資料，這類服務大部份是由一個特別的工作站呼叫使用，此工作站本身也同時提供這些服務，因此也稱為擷取點(Access Point, 簡稱AP)。擷取點是唯一同時提供 SS 和 DSS的無線網路元件，它也是工作站與分散式系統間的橋樑。分散系統提供下列五種服務：

聯結服務(Association)

取消聯結服務(Disassociation)

分送服務(Distribution)

整合服務(Integration)

重聯結服務(Reassociation)

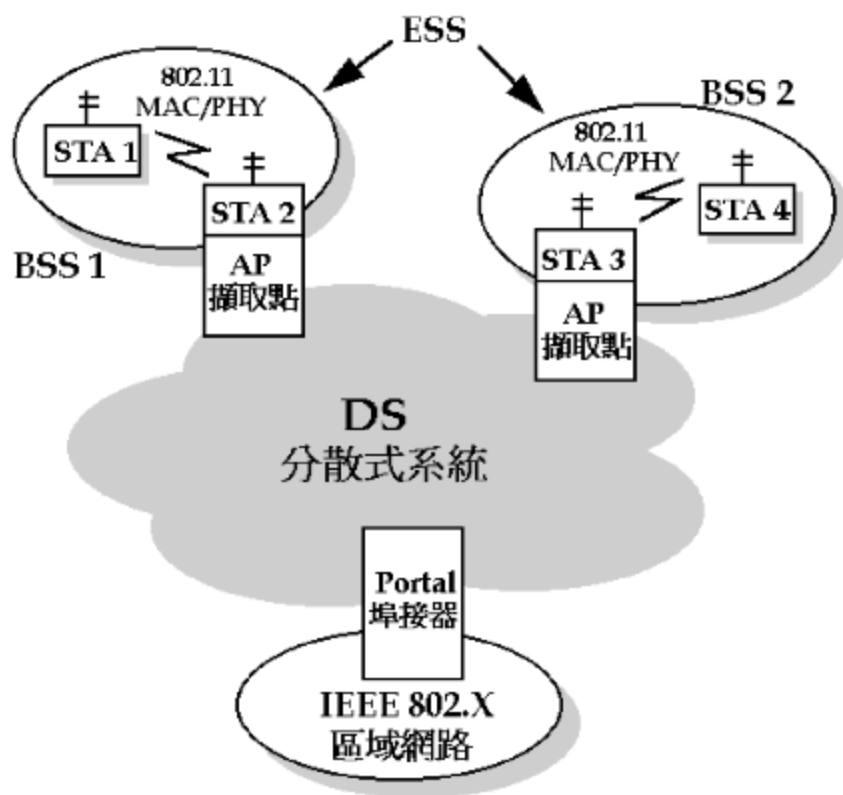


圖13-3 無線網路軟體服務架構

IEEE 802.11 所指定的七種服務中有五種是用來支援使「媒介擷取服務資料單元」(MAC service data unit,簡稱 MSDU) 能在不同的 BSS 間傳送。另外二種則是用來控制工作站對 IEEE 802.11區域網路的擷取，及資料的隱私性。其功能分述如下：

分送服務(Distribution)：此服務的主要工作就是將分散式系統中的資料送到該送到的地方。以圖13-3 為例，假設有一筆訊框要從 工作站 1 送到 工作站 4，一開始這筆訊框會先被送到工作站 2 (輸入擷取點)，接著工作站 2 會透過

「分送服務」將這筆訊框送到工作站 **3** (輸出擷取點)，而工作站 **3** 再透過無線媒介將訊框送達工作站 **4**。**IEEE 802.11** 並沒有規定分散系統要如何將訊框正確的送達目的位置，但它說明了在「聯結」(**Association**)、「取消聯結」(**Disassociation**)及「重聯結」(**Reassociation**)等服務中該提供那些資訊，使得分散系統可以決定該筆訊框該送往那個輸出擷取點，而將訊框送達正確的目的地位置。

整合服務(Integration)：此服務的主要目的是要使訊框能在分散系統和現存的傳統區域網路間傳送。如果分送服務知道該筆訊框的目的地位置是一個現存的 **IEEE 802.x** 有線區域網路，則該筆訊框在分散系統中的輸出點將是埠接器而不是擷取點。分送服務若發現該訊框是要被送到埠接器將會使得分散系統在訊框送達埠接器後接著驅動「整合服務」，而整合服務的任務就是將該筆訊框從分散系統轉送到相連的區域網路媒介。其中整合服務要做的主要工作就是將不同的位址空間做一個轉換。爲了要了解以下所將要介紹的「聯結」(**Association**)、「取消聯結」(**Disassociation**)及「重聯結」(**Reassociation**)等服務的意義，我們先介紹一個叫做「移動性」(**mobility**)的觀念，**IEEE 802.11**對工作站，定義了三種程度的「移動性」，分別描述如下：

無變動：此程度的移動性又可分爲以下兩種型式：靜止（工作站根本就沒動）及區域性的移動（工作站只在一個基本服務區內移動）。

基本服務區的變動：工作站會從一個基本服務區移動到另一個基本服務區，但仍保持在同一個擴充服務區內。

擴充服務區的變動：工作站會從某一個擴充服務區內的基本服務區移動到另一個擴充服務區內的基本服務區。

聯結服務(Association)：此服務的主要目的是要在工作站和擷取點之間建立一個通訊連線。當分散式系統要將資料送給工作站時，它必需事先知道這個工作站目前是透過那個擷取點來擷取分散式系統，這些資訊就是由聯結服務來提供。一個工作站在被允許藉由某個擷取點送資料給分散系統之前，它必須先和此擷取點作聯結，通常在一個基本服務區內有一個擷取點，因此任何在這個基本服務區內的工作站想和外界作通訊，就必須先向此擷取點相聯結。此動作類似註冊，因爲當工作站作完聯結的動作後，擷取點就會記住此工作站目前在它的管轄範圍之內。請注意在任一瞬間，任一個工作站只會和一個擷取點作聯結，這樣才能使得分散系統能在任一時候知道哪一個工作站是由哪一個擷取點所管轄。然而，一個擷取點卻可同時和多個工作站作聯結。聯結服務都是由工作站所啓動的，通常工作站會藉由啓動聯結服務來要求和擷取點作一個聯結。

重聯結服務(Reassociation)：此服務的主要目的是要將一個移動中工作站的聯結，從一個擷取點轉移到另一個擷取點。當工作站從一個基本服務區移動到另一個基本服務區時，它就會啓動一個「重聯結的服務」，此服務會將工作站和它所移入的基本服務區內的擷取點作一個聯結，使得分散系統將來能知道此工作站目前已由另一個擷取點所管轄了。重聯結的服務也都是由工作站所啓動的。

取消聯結服務(Disassociation)：此服務的主要目的是取消一個聯結。當一個工作站傳送資料結束時，可以啓動「取消聯結服務」。另外，當一個工作站從一個基本服務區移動到另一個基本服務區時，它除了會對新的擷取點啓動「重聯結服務」外，也會對舊的擷取點啓動「取消聯結服務」。此服務可由工作站或擷取點來啓動。不論是哪一方啓動，另一方都不能拒絕。擷取點可能因爲網路負荷的原因，而啓動此服務對工作站取消聯結。

身份確認服務(Authentication)：此服務的主要目的是用來確認每一個工作站的身份。**IEEE 802.11** 支援一種叫做「盤問/回應」(**Challenge/Response**，簡稱 **C/R**)的身份確認方法。一般 **C/R** 身份確認的方法主要有下列三個步驟：

聲明身份 (**Assertion of Identity**)

盤問聲明 (**Challenge of Assertion**)

回應盤問 (**Response to Challenge**)

以下爲 **C/R** 身份確認方法的實例

聲明 (**Assertion**)：我是工作站 **4**

盤問 (**Challenge**)：証明你的身份

回應 (**Response**)：這是我的密碼

結果 (**Result**)：如果密碼 **OK**，工作站就完成身份確認

IEEE 802.11 通常要求雙向式的身份確認。在任一瞬間，一個工作站能同時和多個工作站（包含擷取點）作身份確認的動作。身份確認的服務是屬於工作站服務。

隱密性服務 (Privacy)：此服務的主要目的是避免傳送資料的內容被竊聽。無線網路和有線網路不太相同的地方，其中一點就在於無線網路的資料是在空氣這開放的介質中傳播，因此任何只要裝有 **IEEE 802.11** 介面卡的工作站都能接收到別人的資料，所以資料的保密性若做的不好，資料就很容易被別人所竊聽。「隱密性服務」的主要功能就是提供一套「隱密性服務」的演算法 (**privacy algorithm**) 將資料做加密與解密。「隱密性服務」也是屬於工作站服務。

13.4 訊框格式

IEEE 802.11 的 **MAC** 訊框格式如圖**13-4** 所示，其中包含

訊框標頭 (**Header**)：30位元組，此部份主要包括了控制資訊 (**control information**)，位址 (**addressing**)，順序號碼 (**sequencing number**)，持續時間 (**duration**) 等欄位。

資料：長度不一（**0 - 2312** 位元組），此部份依訊框型態 (**frame type**) 有所不同。

錯誤檢查碼：4 位元組，記錄訊框的檢查碼，採用 **CRC-32** 技術。

2 2 6 6 6 2 6 0-2312 4 位元組

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC
---------------	-------------	-----------	-----------	-----------	------------------	-----------	------------	-----

÷ 7 ----- MAC Header -----® ÷

圖13-4 MAC 訊框格式

13.4.1 訊框控制欄位

訊框控制欄位之格式如圖13-5 所示。其中

2 2 4 1 1 1 1 1 1 1 1 位元

Protocol	Type	Subtype	To	From DS	More	Retry	Pwr	More	WEP	Order
Version			DS		Flag		Mgt	Data		

圖13-5 訊框控制欄位格式

Protocol Version : 802.11 標準版本，目前值為 00。

Type and Subtype：訊框型態，目前定義的有三種：Data 訊框, Control 訊框, Management 訊框。每一種型態有可分為若干次型態，如表13-1 所示。

To DS：此旗標值為 1 表示此 Data 訊框（包括廣播或群播訊框）要傳送給分散式系統。若為其他種類的訊框，則其值應為 0。

From DS：此旗標值為 1 表示此 Data 訊框（包括廣播或群播訊框）是由分散式系統傳送下來。若為其他種類的訊框，則其值應為 0。To DS 與 From DS之組合有四種，期代表意義如表13-2 所示。

More Fragments：此旗標值為 1 表示工作站尚有其他片段(Fragments) 待傳送。若為其他種類的訊框，則其值應為 0。

Retry：此旗標值為 1 表示此 Data 訊框（或Management訊框）為重送之訊框。接收端可依此訊息來丟棄重複之訊框。

Power Management：此旗標用來顯示工作站之電源管理模式。其值為 1 表示此工作站處於省電模式，其值為 0 表示此工作站處於正常模式。所有由 AP 傳送的訊框上此值都必須為 0。

More Data：此旗標由 AP 用來通知處於省電模式之工作站說 AP 目前仍有MSDUs 欲傳送給該工作站。在 Data 訊框上其值為 1 表示至少還有一個 MSDU 待轉送。若為其他種類的訊框，則其值應為 0。

WEP：此旗標值為 1 表示此 Data 訊框（或Management訊框）中所攜帶的資料已經過 WEP 演算法處理過。若為其他的訊框，則其值應為 0。

Order：此旗標值為 1 表示此 Data 訊框經由嚴格依序服務等級 (Strictly-Ordered service class) 來傳送。若為其他的訊框，則其值應為 0。

表13-1 各式訊框型態及次型態

Type value b ₃ b ₂	Type Description	Subtype Value b ₇ b ₆ b ₅ b ₄	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	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	PS-Poll
01	Control	1011	RTS
01	Control	1100	CLS
01	Control	1101	ACK
01	Control	1110	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13-2 To DS 與 From DS組合與意義

To DS From DS值	代表意義
To DS = 0 From DS = 0	Data訊框由一個工作站直接傳送給另外一個在相同BSS中的工作站
To DS = 1 From DS = 0	Data訊框傳送給分散式系統
To DS = 0 From DS = 1	Data訊框由分散式系統傳下來
To DS = 1 From DS = 1	由一個AP 傳給另外一個AP 的WDS訊框

13.4.2 Duration/ID 欄位

Duration /ID 欄位長度為16位元，其用法如下（請參考表13-3）：

若訊框為控制型態(Control Type)，且次型態為PS-Poll, 則此欄位代表一個SID, 其最左邊兩個位元都是1, 而剩下的 14 位元則是傳送此訊框之工作站之SID。SID 值的範圍為 1 到 2007。

若為其他訊框，則此欄位代表一個duration, 其值依各訊框型態而定。不過對於所有在免競爭期間所傳送的訊框來說，此欄位之值應設為32768。當Duration/ID 欄位的內容小於 32768 時，表示其為一個duration 值，應該被拿來修正NAV。

表13-3 Duration /ID 欄位意義

Bit 15	Bit 14	Bits 13-0	用途
0	0-32767		Duration (由此訊框結束後起 算，單位為us)

1	0	0	在免競爭期間所傳送之訊框使用之固定值(32768)
1	0	1-16383	保留
1	1	0	保留
1	1	1-2007	在PS-Poll訊框中指定之工作站 ID
1	1	20013-16383	保留

13.4.3 位址欄位

MAC訊框格式中共有四個位址欄位。這些欄位用來記錄BSSID (BSS Identifier), 起始工作站位址 (Source Address, SA)，目地的工作站位址(Destination Address, DA)，傳送工作站位址(Transmitter Address, TA)，及接收工作站位址(Receiver Address, RA)。其中目地的工作站位址(DA) 可以是各別或群播位址。是該訊框的最終目的地。起始工作站位址 (SA) 是產生此訊框的工作站位址。傳送工作站位址(TA) 是指在無線媒介上傳送此訊框的工作站位址。接收工作站位址(RA) 則是指在無線媒介上接收此訊框的工作站位址。每一個位址長度都是符合 IEEE 802 標準之 48 位元。有些訊框並不需要用到所有的位址欄位。有些位址欄位在使用時和其在位址欄位的相對位址(1-4)有關而與位址型態無關。例如當一個工作站接收到一筆訊框時，都是用 Address 1 的內容來判斷該訊框是否傳送給自己。而 CTS 訊框 (ACK訊框) 中的 RA 則等於 RTS 訊框 (需要被回覆之訊框) 中的 Address 2 的內容。

每個 BSS 都有一個具唯一性的辨識碼 (BSSID, 長度為 48 位元), 對於有基礎架構的BSS, 此辨識碼為擷取點 (AP) 中的工作站的位址。對於無基礎架構的BSS (IBSS), 此辨識碼最左邊兩個位元為 01, 而剩下的 46 位元則以亂數產生。廣播性BSSID (48 位元都為 1) 只能用在管理訊框且次型態為Probe (Type = 00, Subtype = 0100 或 0101)。

13.4.4 順序控制欄位 (Sequence Control)

順序控制欄位包含兩個次欄位：順序號碼 (Sequence Number, 12 位元) 及片段號碼 (Segment Number, 4 位元), 如圖13-6 所示。其中順序號碼為該訊框攜帶之 MSDU 的順序號碼。每一個 MSDU 都有一個順序號碼, 其值由 0 開始, 到4095, 然後重複輪流使用。由同一個 MSDU 切割出來的片段都應該使用相同的順序號碼。片段號碼則是指該片段在原來MSDU所切割出來的片段順序。第一個片段（或沒有切割的MSDU）其值為0。以後則依序加一，到 15 為止，然後重複輪流使用。



圖13-6 順序控制欄位

🌟 13.5 各式訊框型態之格式

13.5.1控制訊框

控制訊框之控制欄位內容如圖13-7所示。

Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order
Protocol Version	Control	Subtype	0	0	0	0	Pwr Mgt	0	0	0

2 2 4 1 1 1 1 1 1 1 1 位元

圖13-7 控制訊框之控制欄位內容

RTS 訊框格式如圖13-8(a) 所示，其中 RA 應該是無線媒介上的一個位址，也就是待送Data 訊框或 Management 訊框的立即目的地位址。TA 則是傳送此訊框之工作站之位址。Duration 的值（單位是us） 應該等於傳送該待送 Data 訊框或 Management 訊框，加上一個 CTS 訊框，加上一個 ACK 訊框及加上三個 SIFS 訊框間隔的時間。如果Duration 計算的結果不是整數，則進位為整數。如 250.1 us 及 2413.7 us可分別進位為 251 us 及 248 us。

CTS 訊框格式如圖13-8(b) 所示，其中 CTS 訊框中的 RA 內容應該等於前一個對應之 RTS 訊框中之 TA 內容。Duration 的值（單位是us） 應該等於前一個對應之 RTS 訊框中之 Duration 值減掉傳送此 CTS 訊框及一個 SIFS 訊框間隔的時間。如果 Duration 計算的結果不是整數，則進位為整數。

ACK 控制訊框格式如圖13-8(c) 所示，其中 ACK 訊框中的 RA 內容應該等於前一個對應之 Data 訊框, Management 訊框, 或 PS-Poll 控制訊框中之 Address 2 欄位內容。如果前一個對應之 Data 訊框或 Management 訊框中之訊框控制欄位中之More Fragment旗標為0，則 Duration 的值應設為零。如果More Fragment旗標為1，則Duration 的值（單位是us） 應該等於前一個對應之Data 訊框或 Management 訊框中之 Duration 值減掉傳送此 ACK 訊框及一個 SIFS 訊框間隔的時間。如果 Duration 計算的結果不是整數，則進位為整數。

省電輪詢 (Power Save Poll, PS-Poll) 訊框之格式如圖13-8(d) 所示。其中BSSID是隸屬於AP中之工作站之位址，TA是傳送此訊框之工作站之位址，而SID則是傳送訊框之工作站之 SID 值，此值是 AP 先前經由Association Response分配給該工作站的。SID值的最左邊兩個位元都是1。所有收到PS-Poll 輪詢訊框的工作站都應該修正其 NAV 值。修正時所使用的duration 值為傳送一個 ACK 訊框所需要的時間加上一個 SIFS 訊框間隔。

免競爭週期結束 (**Contention-Free End, CF-End**) 訊框之格式如圖**13-8(e)**所示。其中**BSSID** 是隸屬於 **AP** 中之工作站之位址，而 **RA** 則是廣播位址。**Duration** 值應設為 **0**。

免競爭週期結束回覆 (**Contention-Free End Acknowledge, CF-End+CF-Ack**) 訊框之格式如圖**13-8(f)** 所示。其中**BSSID** 是隸屬於 **AP** 中之工作站之位址，而 **RA** 則是廣播位址。**Duration** 值亦應設為 **0**。

2 2 6 6 4 位元組

Frame Control	Duration	RA	TA	CRC
------------------	----------	----	----	-----

(a) RTS 訊框格式

2 2 6 4 位元組

Frame Control	Duration	RA	CRC
------------------	----------	----	-----

(b) CTS 訊框格式

2 2 6 4 位元組

Frame Control	Duration	RA	CRC
------------------	----------	----	-----

(c) ACK 訊框格式

2 2 6 6 4 位元組

Frame Control	SID	BSSID	TA	CRC
------------------	-----	-------	----	-----

(d) PS-Poll 訊框格式

2 2 6 6 4 位元組

Frame Control	Duration	RA	BSSID	CRC
------------------	----------	----	-------	-----

(e) CF-END 訊框格式

2 2 6 6 4 位元組

Frame Control	Duration	RA	BSSID	CRC
------------------	----------	----	-------	-----

CF-End + CF-Ack 訊框格式

圖13-8 MAC 控制訊框格式

13.5.2 數據訊框

數據訊框的格式與次型態無關，如圖**13-9**所示。數據訊框的四個位址的內容與**To DS** 及 **From DS** 位元有關，其用法如表**13-4**所示。其中**N/A**代表該欄位可取消。

2 2 6 6 6 2 6 0-2312 4 位元組

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC
------------------	-------------	-----------	-----------	-----------	---------------------	-----------	------------	-----

圖13-9 數據訊框格式

表13-4 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

工作站在決定要不要收一個數據訊框時是依據**Address 1**的內容來判斷的。如果**Address 1**的內容與自己的位址相同則可接收。如果**Address 1**的內容是一個群體位址，則**BSSID**也要一併檢查，以確定該廣播或群播訊框是來自相同的**BSS**。如果接收訊框的工作站需要傳送回覆訊息時，則以**Address 2** 欄位的內容為回覆位址。**DA** 代表此訊框的最終目的地位址，而 **SA** 則代表產生此訊框的工作站位址。在**DS** 是無線分散式系統下，**RA**代表接受此訊框的下一個工作站位址，此工作站應屬於某一個連結在無線分散式系統上的擷取點 (**Access Point**)。 **TA** 則代表在無線分散式系統上傳送此訊框的工作站位址，此工作站也應屬於某一個連結在無線分散式系統上的擷取點。**BSSID**的值則依據傳送此訊框之工作站之性質來決定。如果該工作站是一個擷取點或已經與某一個擷取點建立連結關係，則此**BSSID**的值為隸屬於該擷取點的工作站的位址。如果該工作站為一個獨立**BSS (IBSS)** 的成員，則此**BSSID**的值為該 **IBSS** 的**BSSID** 值。

13.5.3 管理訊框

管理訊框之通用格式如圖**13-10**所示。各式管理訊框之格式則如下所述。

2 2 6 6 6 2 0-23 12 4 位元組

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	CRC
---------------	----------	----	----	-------	------------------	------------	-----

圖**13-10** 管理訊框格式

13.5.3.1 各式管理訊框之格式

圖 **13-11** 所示為各式管理訊框之訊框主體。

順序	資訊	註解
1	Timestamp	
2	Beacon Interval	
3	Capability Information	
4	SSID	
5	Supported Rates	
6	FH Parameter Set	註1
7	DS Paramter Set	註2
8	CF Parameter Set	註3
9	IBSS Parameter Set	註4
10	TIM	註5

Beacon 訊框主體

順序	資訊	註解
1	Reason Code	

Disassociation 訊框主體

順序	資訊	註解
1	Capability Information	
2	Listen Interval	

3	SSID	
4	Supported Rates	

(c) Association Request 訊框主體

順序	資訊	註解
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

Association Response 訊框主體

順序	資訊	註解
1	Capability Information	
2	Listen Interval	
3	Current AP Address	
4	SSID	
5	Supported Rates	

Reassociation Request 訊框主體

順序	資訊	註解
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

Reassociation Response 訊框主體

順序	資訊	註解
1	Capability Information	
2	SSID	
3	Supported Rates	

(g) Probe Request 訊框主體

順序	資訊	註解
1	Timestamp	
2	Beacon Interval	
3	Capability Information	
4	SSID	
5	Supported Rates	
6	FH Parameter Set	註1
7	DS Parameter Set	註2

8	CF Parameter Set	註3
9	IBSS Parameter Set	註4

(h) Probe Response 訊框主體

順序	資訊	註解
1	Authentication Algorithm Number	
2	Authentication Transaction Sequence Number	
3	Status Code	註6
4	Challenge Text	註7

(i) Authentication 訊框主體

Authentication Algorithm Number	Authentication Transaction Sequence Number	Status Code	Challenge Text
Open System	1	保留	不包含
Open System	2	Status	不包含
Shared Key	1	保留	不包含
Shared Key	2	Status	包含
Shared Key	3	保留	包含
Shared Key	4	Status	不包含

(j) Challenge Text 資訊呈現時機

順序	資訊	註解
1	Reason Code	

Deauthentication 訊框主體

圖13-11 管理訊框之各類主體格式

註1：FH Parameter Set 只能出現在實體層採用跳頻技術 (Frequency Hopping) 之工作站所傳送之Beacon 訊框中。

註2：DS Parameter Set 只能出現在實體層採用直接順序技術 (Direct Sequence) 之工作站所傳送之Beacon 訊框中。

註3：CF Parameter Set 只能出現在具有 PCF 功能之 AP 所傳送之Beacon 訊框中。

註4：IBSS Parameter Set 只能出現在隸屬於一個獨立BSS (IBSS) 之工作站所傳送之Beacon 訊框中。

註5：TIM (Traffic Information Map) 只能出現在AP 所傳送之Beacon 訊框中。

註6：在某些Authentication訊框中，Status code應該被保留並且設為零，如表中所定義。

註7：Challenge Text 只能出現在某些Authentication訊框中，如表中所定義。

13.5.3.2 管理訊框主體元件

爲了方便起見，管理訊框中必要且固定長度的欄位稱為固定欄位 (Fixed Fields)，必要但不固定長度或屬於選項的欄位稱為訊息元件 (Information elements)。以下分別說明這兩部份。

固定欄位

管理訊框可能包含的固定欄位有 10 種，如下所述：

Authentication Algorithm Number (2 位元組)：記錄工作站採用之認證演算方法（0: Open System, 1: Shared Key）。

Authentication Transaction Sequence Number (2 位元組)：記錄認證過程中的訊框交換順序。

Beacon Interval (2 位元組)：記錄 **Beacon** 訊框預計傳送時間 (**Target Beacon Transmission Time, TBTT**) 的間隔，單位為**Kus**。

Capability Information (2 位元組)：記錄所要求或回應之功能。此欄位又分爲 5 個次欄位：

ESS (Bit 0)

Independent BSS (Bit 1)

CF-Pollable (Bit 2)

CF Polling Request (Bit 3)

Reserved (Bits 4-15)

協調者所傳送的 **Beacon** 訊框及 **Probe Response** 訊框中，**ESS = 1, IBSS = 0**。屬於 **IBSS** 的工作站所傳送的 **Beacon** 訊框及**Probe Response** 訊框中，**ESS = 0, IBSS = 1**。工作站爲了偵測 **ESSs** 而傳送的 **Probe** 訊框中，**ESS =1**。工作站爲了偵測 **IBSSs** 而傳送的 **Probe** 訊框中，**IBSS =1**。工作站如果想同時偵測所有存在的**ESSs**及**IBSSs**, 則可同時設定 **ESS =1, IBSS=1**。

可輪詢工作站在傳送 **Association** 及 **Reassociation** 訊框時，應設定 **CF-Pollable = 1**。協調者所傳送的 **Beacon** 訊框，**Association Response** 訊框, **Reassociation Response** 訊框, 及**Probe Response** 訊框時，應設定 **CF-Pollable = 1**。

可輪詢工作站如果欲加入被輪詢名單中，則在傳送 **Association** 及 **Reassociation** 訊框時，應設定 **CF-Polling Request = 1**。協調者在傳送回應這些要求的 **Association Response** 及 **Reassociation Response** 訊框時，也應設定 **CF-Polling Request = 1**，表示已經將提出要求的工作站加入輪詢名單中。

Current AP Address (6 位元組)：記錄工作站目前連結的擷取點的 **MAC** 位址。

Listen Interval (2 位元組)：處於省電模式之工作站應該醒來接收**Beacon** 訊框的時間間隔（單位爲**Beacon Interval**）。協調者可依據此參數了解工作站的行爲並且決定屬於該工作站之訊框之儲存時間。

Reason Code (2 位元組)：記錄產生非邀請性管理訊框（**Disassoication** 或**Deauthentication**）的理由。

Station ID (SID) (2 位元組)：記錄在連結期間協調者所分配的工作站識別碼 **SID_i**（**14** 位元，其值介於**1 ~ 2007**）。此欄位之最左邊兩個位元都應設爲 **1**。在 **TIM** 訊息元件中，協調者利用 **SID₀**（不代表工作站）來顯示其是否儲存廣播或群播訊框。

Status Code (2 位元組)：記錄要求訊框的處理結果。**Status Code = 0** 表示成功，其餘代表失敗的原因。

Timestamp (8 位元組)：記錄傳送此訊框之工作站之 **TSFTIMER**值 (**Timing Synchronization Function Timer**)。此值爲網路上工作站間達成同步運作的參考時間值。

訊息元件

所有訊框中所攜帶的訊息元件 (**Information Elements**) 都使用相同的格式來表達（如圖**13-12(a)** 所示）：一個位元組的元件識別碼 (**Element ID**) 欄位，一個位元組的訊息長度 (**Length**) 欄位，以及不固定長度的訊息 (**Information**) 欄位。目前已經定義的元件種類則如表**13-5** 所示。

表**13-5** 訊息元件種類及代碼

訊息元件	元件識別碼
SSID	0
Supported Rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Reserved	7-15
Challenge Text	16
Reserved for Challenge Text extention	17-31
Reserved	32-255

SSID (Service Set Identity) 元件的格式如圖**13-12(b)** 所示。其中 **SSID** 是一個**ESS (Extended Service Set)** 或**IBSS (Independent BSS)** 的識別碼。長度欄

位值若等於零表示所攜帶的是廣播 SSID (broadcast SSID)。

Supported Rates 元件的格式如圖13-12(c) 所示。此元件主要是讓工作站來聲明其所能接收的有哪些傳輸速率。訊息欄位中的每一個位元組攜帶一種可接收的傳輸速率（單位是**100 kbps**）。速率的表示式依管理訊框的種類而有所不同，在**Beacon, Probe Response, Association Response, 及 Reassociation Response**等四種管理訊框中之速率表示法如下：如果該速率屬於 **aBSSBasicrateSet** 所定義的速率，則最左邊的位元（第七位元）應設為**1**。否則最左邊的位元應設為 **0**。例如假設 **1Mbps (=10x100 kbps)** 於 **aBSSBasicrateSet** 中有定義，則其代碼為**10001010 (0x8A)**。又假設 **2Mbps (=20x100 kbps)** 於 **aBSSBasicrateSet** 中無定義，其代碼為**00010100 (0x14)**。在其他種類的管理訊框中之速率表示法則忽略最左邊位元的值。例如 **10010100 (0x94)** 及 **00010100 (0x14)** 都代表**2Mbps**。

FH Parameter Set 元件的格式如圖13-12(d) 所示。以跳頻技術 (**Frequence Hopping, FH**) 為實體層傳輸技術之工作站間必須達到彼此同步的狀態才能正確的通訊。此元件主要攜帶完成此任務所需要的參數。訊息欄位內容包含 **Dwell time**（單位為**kus**），**Hop Set, Hop Pattern, 及 Hop Index**; 其中**Hop Set** 表示所使用的頻率跳躍順序組 (**Hopping Sequence Set**)，例如北美地區目前已制定三組頻率跳躍順序組。

CF Parameter Set 元件的格式如圖13-12(e) 所示。此元件攜帶支援**PCF**功能所需要的參數。訊息欄位內容包含**CFP Count, CFP Period, CFPMaDuration, 及CFPDurRemaining**; 其中 **CFP Count** 記錄在下次免競爭週期開始前應該出現幾次**DTIM** (包含目前這次), **CFP Period** 記錄免競爭週期間應該有幾個**DTIM**間隔, **CFPMaDuration** 記錄此免競爭週期的最長時間（單位為**kus**, 工作站可依此設定其NAV值）, **CFPDurRemaining** 則記錄此免競爭週期尚餘多少時間（單位為**kus**, 工作站可依此修正其 NAV 值）。在競爭週期內所傳送之 **Beacon** 訊框之**CFPDurRemaining** 值應設為**0**。

DS Parameter Set 元件的格式如圖13-12(e) 所示。此元件主要讓使用直接順序技術 (**Direct Sequence, DS**) 為實體層擷取技術之工作站能辨識出目前所使用之通道編號。

TIM 元件的格式如圖13-12(g) 所示。協調者利用此元件通知所有工作站其儲存訊框的最新狀況。訊息欄位內容包含**DTIM Count, DTIM Period, Bitmap Control, 及Partial Virtual Bitmap**; 其中**DTIM Count** 記錄在下次**DTIM**出現前應該出現幾次**Beacon** 訊框 (包含目前這個)。 **DTIM = 0** 表示目前這個**TIM** 元件就是一個 **DTIM**。 **DTIM Period** 記錄**DTIM** 間應該有幾個 **Beacon** 間隔。如果所有的 **TIM** 元件都是 **DTIM**元件，則 **DTIM Period**之值應為**1**。 **Bitmap Control** 欄位（**1** 位元組）分為兩個次欄位：**Bitmap Offset** 次欄位（**7** 位元）及 **Traffic Indicator** 次欄位（**1** 位元），其中**Traffic Indicator** 位元記錄協調者是否儲存有廣播或群播訊框。如果有則在傳送 **DTIM** 時此位元應設為**1**，其他情形此位元應設為 **0**。 **Bitmap Offset** 次欄位之值介於 **0** 到 **250** 之間，如下所述：虛擬位元對照表 (**virtual bitmap**) 應包含 **2008** 位元，每一個位元對照一部工作站（無線網路上最多可同時存在 **2007** 部工作站）。此 **2008** 位元應以**251** 個位元組 (**2008/8 = 251**) 來表示，使得第 **k** 個位元, **0 £ k £ 2007**, 被安置於第 $\lceil k/8 \rceil$ 個位元組中的第 **(k mod 8)** 位元。這裡假設最左邊的位元組編號為第 **0** 個位元組，而一個位元組中，最右邊位元為第 **0** 個位元，最左邊位元為第 **7** 個位元。例如 **k = 200**, 則其代表位元為第 **25** 個位元組中的第 **0** 個位元。 **k = 209**, 則其代表位元為第 **26** 個位元組 ($\lceil 209/8 \rceil = 26$) 中的第 **1** 個位元 (**209 mod 8 = 1**)。協調者如果有儲存 **SIDk** 的訊框，則第 **k** 個位元應設為 **1**。由於網路上同時存在的工作站數量通常不會太多而且協調者也可能只儲存少量的訊框（此時絕大部份的位元值為**0**），如果每次都固定傳送 **251** 位元組的對照表似乎顯得過於浪費頻寬。因此這裡只傳送部份的對照表（只傳送最左邊的 **1** 到最右邊的 **1** 之間的部份），方法如下：**Partial Virtual Bitmap** 只包含第 **N1** 個位元組到第**N2** 個位元組，其中**N1** 是滿足對照表中位元 **1** 至位元 **(N1x8)-1** 都為 **0** 的最大偶數，**N2** 是滿足對照表中位元 **(N2+1)x8** 至位元 **2007** 都為 **0** 的最大偶數。例如假設協調者只儲存工作站 **195, 200** 及 **209** 的訊框，則其部份對照表內容為：**00...000,00001000,00000001,00000010,000...00**。其中最左邊第一個**1** (第**24** 個位元組的第 **3** 個位元, **bitmap**中的第 **196** 位元) 代表 **SID195**, 第二個**1** (第 **25** 個位元組的第 **0** 個位元) 代表**SID200**, 最右邊的 **1** (第 **26** 個位元組的第 **1** 個位元, **bitmap**中的第 **214** 位元) 代表**SID209**。此時**N1 = 24**（**(N1x8)-1 = 191**, 此例中，位元 **0-191** 都為**0**）, **N2 = 26**（**(N1+1)x8 = 216**, 此例中，位元**216-2007** 都為 **0**）。再舉一例說明，假設協調者只儲存工作站 **191** 及 **216** 的訊框，則其部份對照表內容為：**00...000,10000000,00000000,00000000,00000000,00000001,000...00**。其中最左邊第一個**1** (第**23** 個位元組的第 **7** 個位元, **bitmap**中的第 **176** 位元) 代表 **SID191**, 最右邊的 **1** (第 **27** 個位元組的第 **0** 個位元, **bitmap**中的第 **215** 位元) 代表**SID216**。此時**N1 = 22**（**(N1x8)-1 = 175**, 此例中，位元 **0-175** 都為**0**）, **N2 = 26**（**(N1+1)x8 = 216**, 此例中，位元 **216-2007** 都為 **0**）。

在**TIM**元件格式中，**Bitmap Offset** 記錄 **N1** 的值，而 **N2** 的值則隱藏於**Length** 中。方法是設定**Length = N2-N1+4**。在前面兩個例子中，其**Length** 欄位分別等於 **6 (26-24+4=6)** 及 **8 (26-22+4=8)**。工作站收到此 **TIM**元件後可分別解出**N2 = Length+N1-4 = 6+24-4 = 26** 及 **N2 = Length+N1-4 = 8+22-4 = 26**。 **Partial Virtual Bitmap** 的長度則分別為 **3** 個位元組 (**00001000,00000001,00000010**) 及 **5** 個位元組 (**10000000,00000000,00000000,00000000,00000001**)。

如果**virtual bitmap**中除了第 **0** 個位元 (**SID0**代表廣播或群播，不代表某一工作站) 之外的所有位元都是 **0** (協調者無儲存訊框)，則**Partial Virtual Bitmap** 欄位的長度為 **1** 位元組，內容則為**00000000**。而且**Bitmap Offset = 0, Length = 4**。也就是說，**N1 = 0, N2 = Length+N1-4 = 0**。

IBSS Parameter Set 元件的格式如圖13-12(h) 所示。此元件包含支援**IBSS**所需要的參數，訊息欄位為**ATIM Window**的長度（單位為**kus**）。

Challenge Text 元件的格式如圖13-12(i) 所示。此元件包含認證過程所需之盤問全文，其長度與所採用的認證演算法以及認證過程之交換順序有關。

1 1 Length 位元組

Element ID	Length	Information
------------	--------	-------------

訊息元件格式

1 1 0-32 位元組

Element ID	Length	SSID
(=0)		

(b) SSID 訊息元件格式

1 1 1-8 位元組

Element ID	Length	Supported Rates
(=1)		

(c) Supported Rates 訊息元件格式

1 1 2 1 1 1 位元組

--	--	--	--	--	--

Element ID (=2)	Length	Dwell Time (Kus)	Hop Set	Hop Pattern	Hop Index
--------------------	--------	------------------	---------	----------------	--------------

(d) FH Parameter Set 訊息元件格式

1 1 1 位元組

Element ID (=3)	Length	Current Channel
--------------------	--------	--------------------

(e) DS Parameter Set 訊息元件格式

1 1 1 1 2 2 位元組

Element ID (=4)	Length	CFP Count	CFP Period	CFP Max Duration (Kus)	CFP Duration Remaining (Kus)
--------------------	--------	--------------	---------------	---------------------------	---------------------------------

(f) CF Parameter Set 訊息元件格式

1 1 1 1 1 1-251 位元組

Element ID (=5)	Length	DTIM Count	DTIM Period	Bitmap Control	Partial Virtual Bitmap
--------------------	--------	---------------	----------------	-------------------	---------------------------

(g) TIM 訊息元件格式

1 1 2 位元組

Element ID (=6)	Length	ATIM Window
-----------------	--------	-------------

(h) IBSS Parameter Set 訊息元件格式

1 1 1-253 位元組

Element ID (=16)	Length	Challenge text
---------------------	--------	----------------

Challenge Text 訊息元件格式

圖13-12 訊息元件格式

13.6 認證與保密

認證 (**Authentication**) 的目的是確認對方身分的合法性，以免與身分不明的對象溝通，洩漏了重要的機密。也就是雙方進行通訊之前，必須先經過認證的程序。**IEEE 802.11** 提供兩種認證的服務：開放系統式 (**Open System**) 及共享密匙式 (**Shared Key**)。前者是**IEEE 802.11** 內定的認證方法，不過工作站提出認證要求時可指定要採用哪種方式進行雙向認證。

13.6.1 開放系統式認證 (Open System)

開放系統式認證可以說是所有認證方法中最簡單的一種。事實上就是一種不須認證演算法的認證方法。任何提出以此方式進行認證的工作站都可通過認證，只要對方支援並允許開放系統式認證。這種方式主要是讓工作站簡單表明身分，以便雙方可儘速進行通訊。就好像如果有一天突然有人打電話給我們時說“我是某某，我是你的小學同學 ”（表明身分）。如果我們並不在意對方是否真的就是某某，當然接下來就可以開始進行溝通。如果對方有特殊要求，我們可能就會想進一步確認對方就是某某（假設多年不見，聲音已經認不出），我們於是可提出一些諸如“班上最高的同學是誰？”，“坐在你旁邊的女生是誰？”，“和我最要好的同學是誰？”，或“當時你家養的小狗叫什麼名字？”等等的問題。可依確認的重要性提出不同難度的問題。當然有個條件是我們必須先知道這些問題的答案。共享密匙式認證就是用來支援這種需要進一步確認身分的方法。

開放系統式認證包含兩個認證步驟。第一個步驟是要求認證者聲明自己的身份 (**Identity assertion**) 並且送出認證訊框 (**Authentication frame**) 要求認證，如圖**13-13(a)** 所示。這裡所謂的身分聲明就是利用訊框標頭中的 **SA** 欄位內容 (**Station ID**)。第二個步驟是被要求認證者回送一個認證訊框其中記錄認證結果，如圖**13-13(b)** 所示。如果被要求認證者同意採用開放系統式認證，則表示認證成功，否則就是失敗。這兩個認證訊框在傳送時都不經過加密處理 (**WEP = OFF**)。否則對方將無法解讀認證內容。

Authentication Algorithm Number = 0 (開放系統式)
Authentication Transaction Sequence Number = 1 (要求)

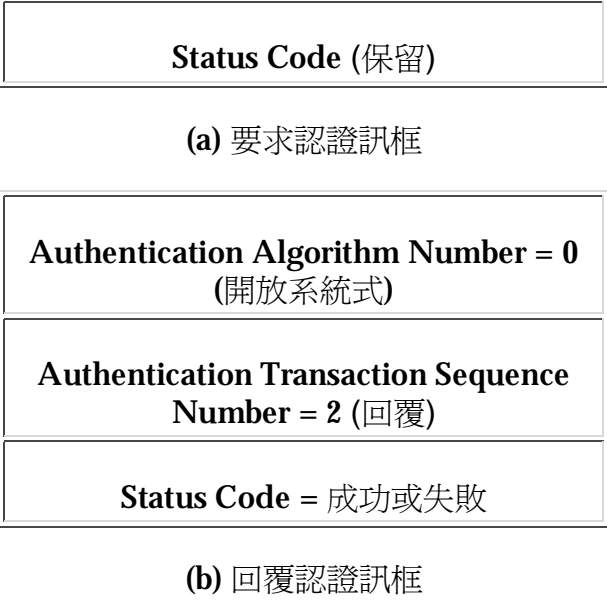
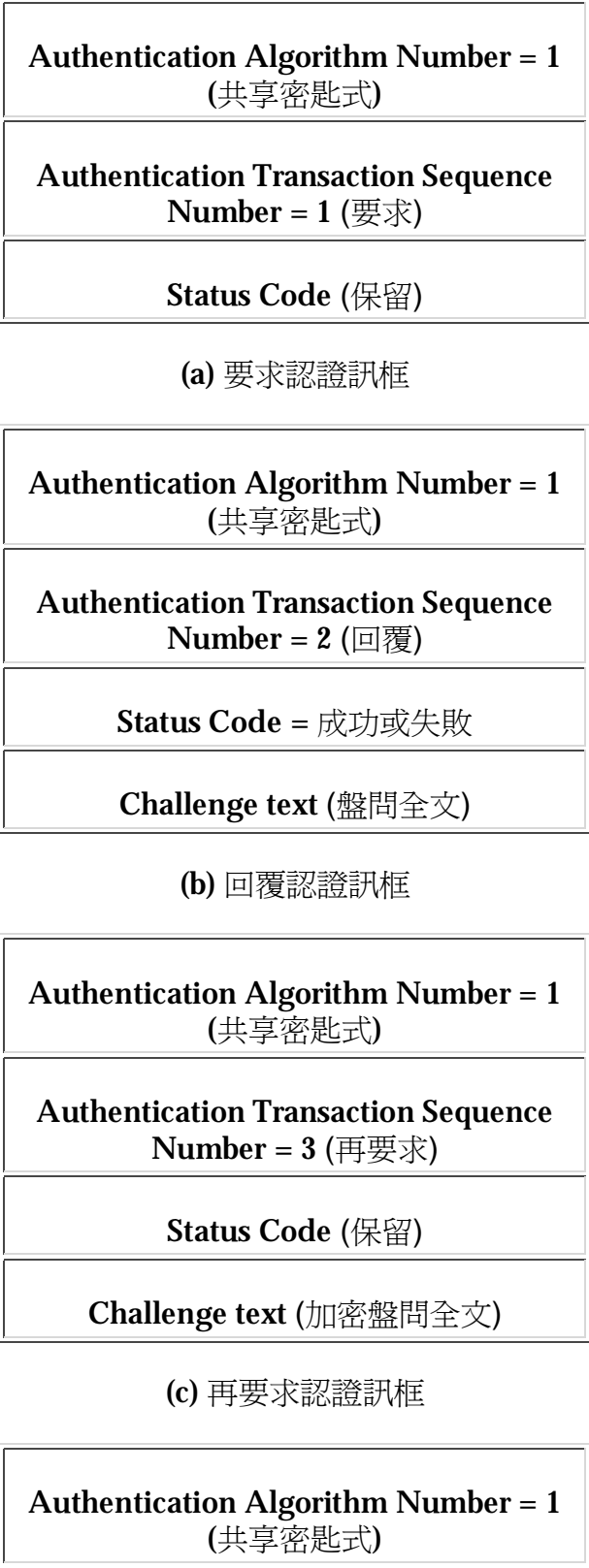


圖13-13 開放系統式認證訊框主體內容

13.6.2 共享密匙式認證 (Shared Key)

共享密匙式認證是假設有一群工作站擁有共同的密匙 (**Shared Key**)。然後當有工作站聲明它屬於這個群體時，我們要有能力判斷對方是否真的屬於此群體（例如查詢對方密匙為何？）。至於一群工作站如何能擁有共同的密匙則不是**IEEE 802.11**的任務範圍。通常群體的發起人應該透過特殊的管道將密匙安全的送給每一個會員。在查詢時，如果對方不屬於此群體，當然就交不出密匙。如果對方的確是會員，則會送回正確的密匙。此時如果恰巧有人竊聽，則將造成密匙曝光。爲了避免密匙曝光，我們需要利用**WEP** 加密演算法。

共享密匙式認證包含四個認證步驟。第一個步驟是要求認證者送出認證訊框 (**Authentication frame**) 要求對方認證，如圖**13-14(a)** 所示。此訊框任務是聲明身份 (**Identity assertion**)，這是利用訊框標頭中的 **SA** 欄位內容 (**Station ID**) 來聲明。第二個步驟是被要求認證者先檢查雙方認證方法是否相同。如果被要求認證者沒有支援共享密匙式認證法，則認證結果 (**result**) 失敗。此時認證程序結束，不再傳送認證訊框。如果成功（被要求認證者支援共享密匙式認證法）則被要求認證者利用 **WEP** 演算法產生一個長度爲**128**位元組之盤問全文 (**Challenge text**)。並將此盤問全文送給要求認證者，如圖**13-14(b)** 所示。此全文的目的是要檢驗對方的密匙，因此其內容並不重要。此兩個訊框在傳送時都不可以經過加密處理 (**WEP = OFF**)。否則對方將無法解讀認證內容。第三個步驟是要求認證者將此盤問全文由前一個認證訊框中拷貝至第三個認證訊框，並且再送給對方，如圖**13-14(c)** 所示。不過此認證訊框必須經過加密的處理 (**WEP = ON**)。第四個步驟是被要求認證者將收到的密文用手上的共享密匙解密。如果發現所解出來的盤問全文與當初送出去的相同，則表示要求認證者也有相同的密匙，此時認證成功。否則表示雙方之密匙不同，認證失敗。被要求認證者於是將認證結果用第四個認證訊框通知要求認證者，如圖**13-14(d)** 所示。此認證訊框亦不經過加密處理 (**WEP = OFF**)。



Authentication Transaction Sequence Number = 4 (回覆)
Status Code = 成功或失敗

(d) 再回覆認證訊框

圖13-14 共享密匙式認證訊框主體內容

13.6.3 有線等效保密演算法 (Wired Equivalent Privacy Algorithm, WEP)

在無線通訊中，傳輸資料被竊聽是常見的現象。由於無線電波的廣播特性，任何欲竊聽者只要將其竊聽器的接收頻率調至傳送頻率即可順利進行竊聽的工作。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同等功效的資料保密演算法。也就是要保護無線網路之授權使用者使之免於被竊聽的煩惱。有線網路上要進行竊聽的工作至少要連接到線上，這種不方便性在某種程度上也可說是一種安全屬性。無線網路雖然不具備這種特有的安全屬性，802.11卻希望能提供與此功能相當的安全性。

802.11採用了將傳送資料加密 (enciphering) 的方法。這種方式通常也必須將資料解密 (deciphering) 所需的鑰匙 (key) 透過某種管道傳給接收端。這就需要一種有效的鑰匙管理服務。

WEP 演算法特色

抗竊聽性強：此演算法所提供的安全性程度有賴於利用各種暴力方式 (brute-force) 去發現鑰匙的困難度。如果困難度夠高，則竊聽者就必須花很長的時間來猜鑰匙，等到猜到時，資料內容可能已經過時，不具竊取價值。而這又與鑰匙的長度與更換鑰匙的頻率有關。**WEP**演算法允許變更鑰匙及頻繁變更加密時的初始向量 (Initialization Vector, IV)。

具自我同步功能：針對每一筆資料，**WEP**都能做到自我同步 (self-synchronization) 的功能。在資料流失率較高且採用儘力式傳送的環境下，此特性對於一個位於鏈結層 (data-link level) 的加密演算法來說，是相當具關鍵性的。

效率佳：**WEP** 演算法的執行效率佳，並且可以用硬體或軟體的技術來製作。

出口爭議性：**WEP** 系統在設計時就考慮到要盡量提高此產品自美國出口的可行性。但由於密碼技術的爭議性較高（雖然可反竊聽，也是犯罪時保密通訊的利器），到目前為止並無法保證使用 **WEP** 技術的 **802.11** 產品能自美國出口。

選項功能：**WEP** 是一種選項配備，**802.11** 產品可包含 **WEP** 演算法（可能有出口問題），也可不包含**WEP** 演算法。

WEP 運作原理

所謂加密 (encryption) 就是將原始二進位資料經過處理後，將其資訊內容隱藏起來。沒有經過加密處理的資料稱為原文 (plaintext, 簡稱 P)，而經過加密處理的資料則稱為密文 (ciphertext, 簡稱 C)。將密文還原成原文的過程稱為解密 (decryption)。密碼演算法 (cryptographic algorithm, 或稱為 cipher) 就是一種用來對資料進行加密及解密的數學函式。近代密碼演算法大都採用鑰匙 (key, 簡稱 k) 技術來進行加密及解密的工作。加密函式 (Encryption function, 簡稱 E) 處理原文 P 後得到密文 C：

$$E_k(P) = C$$

欲還原時，解密函式 (Decryption function, 簡稱 D) 利用相同的鑰匙處理密文 C 後得到原文 P：

$$D_k (C) = D_k (E_k(P)) = P$$

圖13-15 所示為原文經過加密及解密的過程。

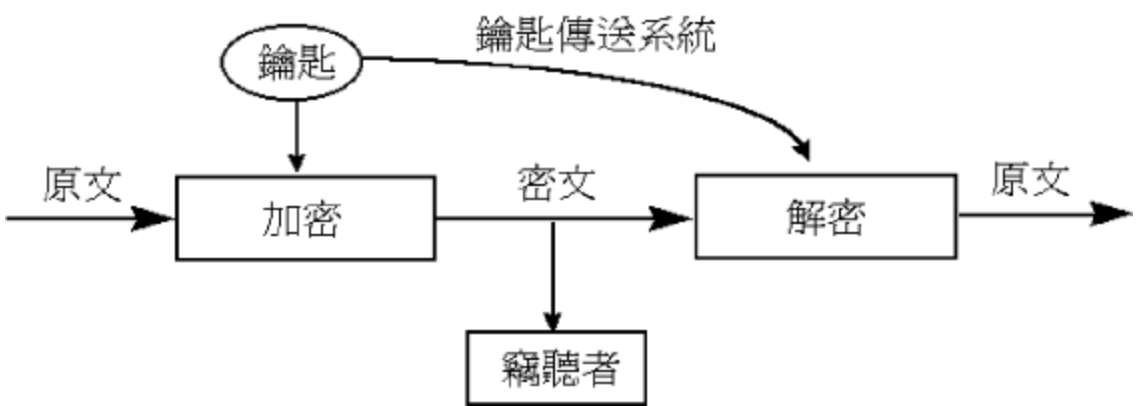


圖13-15 原文加密及解密基本過程

WEP 演算法的主要技術在於將一段原文區塊 (plaintext block) 與一個等長的隨機鑰匙 (random key sequence) 做位元與位元間的互斥運算 (XOR operation)。而此隨機鑰匙則是由 **WEP** 演算法所產生。**WEP** 演算法是一種對稱性的演算法，也就是加密與解密都用相同的鑰匙。在此我們假設鑰匙可經由另外的鑰匙管理服務將之傳給其他有關的工作站。如圖13-16 所示，加密的過程由一個重要的密匙 (secret key) 開始。此密匙後面串接一個初始向量 (Initialization Vector, IV) 後成為一個種子 (seed)，此種子則是亂數產生器 (pseudo random number generator, PRNG) 的一個輸入參數。亂數產生器則輸出一個具隨機性質的鑰匙順序 (key sequence, k), 其長度等於 (MAC Service Data Unit) 的可能最大長度。原文則必須經過兩種處理程序。第一個是為了解保護原文未經授權被修改，原文先經過一個完整演算法 (Integrity algorithm) 的處理得到一個完整檢查碼 (Integrity Check Value, ICV)。另一方面，原文則和鑰匙順序進行互斥的運算得到密文。結果所輸出的訊息 (message) 則包含三部分：密文，初始向量 (IV)，及完整檢查碼 (ICV)。

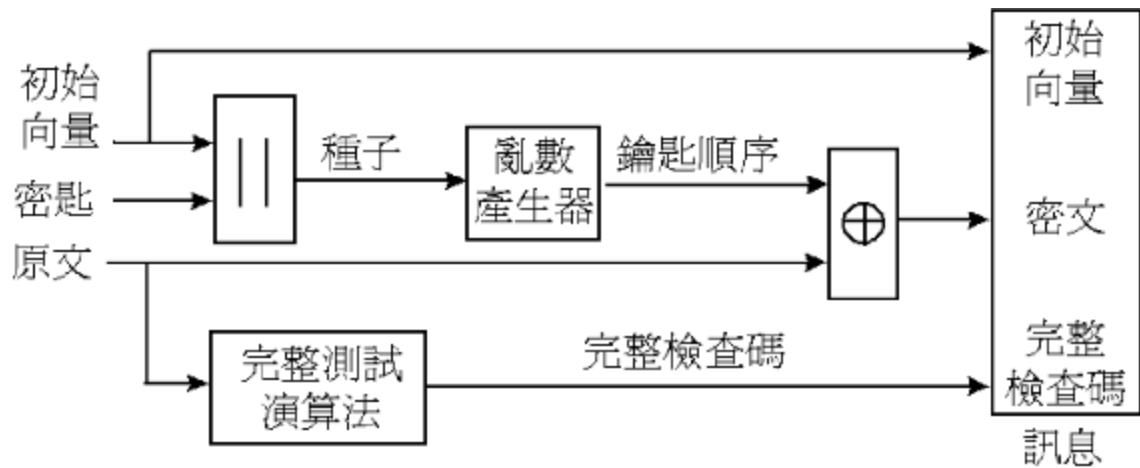


圖13-16 WEP 演算法加密過程

在整個過程中，**WEP** 亂數產生器可說是最關鍵的零組件。它負責將相對較短的密匙轉換成任意長的鑰匙順序。這樣做可以簡化鑰匙傳遞的負擔因為欲進行通訊之工作站間只要傳遞密匙即可。在通訊進行期間，由於初始向量 (**IV**) 可以週期性的變換而密匙則可保持不變，因此初始向量具有延長密匙有效期的功用並且提供此演算法自我同步的重要特性。每一個新的初始向量都可以得到一個新的種子及鑰匙順序，因此初始向量 (**IV**) 與鑰匙順序 (**k**) 間具有一對一的關係。為了避免竊聽者有足夠的時間或資訊破解密文，初始向量可以經常變換，甚至每一個**MPDU**都使用不同的初始向量。由於初始向量和訊息是一起傳送的，接收端工作站可以很容易的用來解密。並不會因為初始向量經常變換而造成困擾。另外由於初始向量並無提供任何與密匙有關的資訊，因此在傳送上不必加密。竊聽者可以清楚看到初始向量，但是無法用它來猜出密匙。

WEP演算法處理的資料單位是一個**MPDU (MAC Protocol Data Unit)**，輸出則依序是 {**IV**, **MPDU**, **ICV**}。其中 **IV** 與 **ICV** 的長度都是 4 個位元組。值得注意的是，輸入亂數產生器的種子長度為 64 位元，其組成方式是將密匙當成是最左邊的 40 位元，而將初始向量當成是最右邊的 24 位元。如圖13-17所示，初始欄位雖然佔 4 個位元組，初始向量事實上只有 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個可能的密匙中的哪一個。至於 **WEP** 所採用的完整檢查演算法事實上就是最常用的 **CRC-32** 演算法。

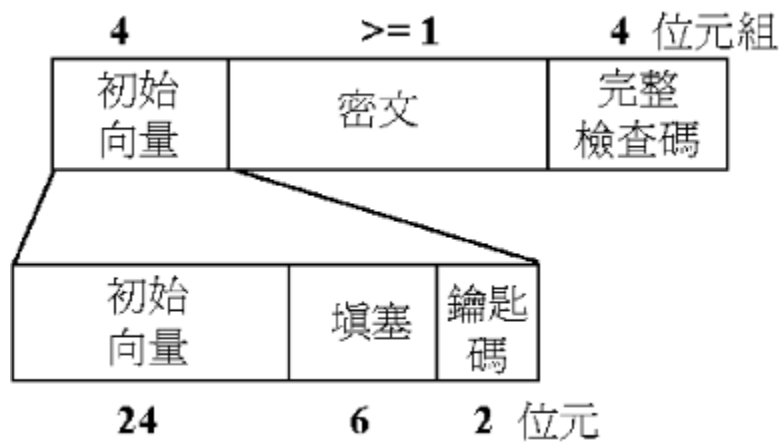


圖13-17 經 WEP 處理過的 MPDU 架構

WEP 演算法解密的過程和加密的過程相反。如圖13-18所示，當工作站收到一筆訊框時，其上的初始向量先與事先取得的密匙合併成為亂數產生器的種子，經由亂數產生器的處理後得到鑰匙順序。此順序與密文進行**XOR**的運算後便得到原文。為了進一步檢查資料在傳送的過程中是否被修改過，此原文還必須經過完整檢查演算法的處理，所得到的完整檢查碼則與訊框上的完整檢查碼比較。如果不同則表示資料被竄改過。此時除了通知**MAC** 管理軟體外，並不將錯誤的訊框傳給上層軟體。

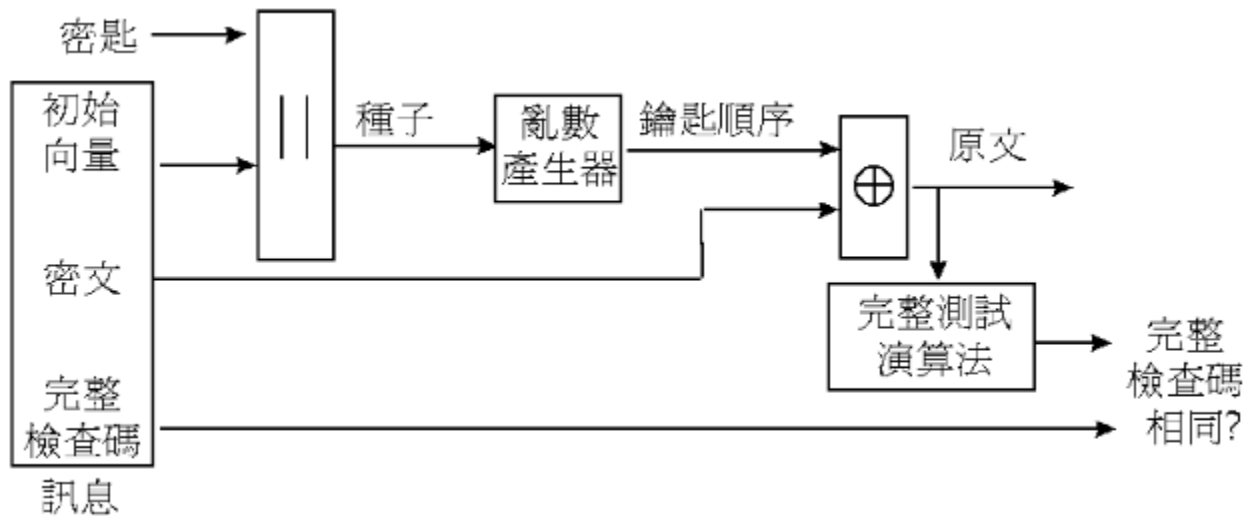


圖13-18 WEP 演算法解密過程

13.7 MAC 通訊協定

IEEE 802.11 MAC 主要提供了二種不同功能的擷取方法：

分散協調式功能 (**Distributed Coordination Function**, 簡稱 **DCF**)

集中協調式功能 (**Point Coordination Function**, 簡稱 **PCF**)

所謂的「協調式功能」(**Coordination Function**) 是指一個用來決定什麼時候那個工作站能開始送收資料的機制。**DCF** 是 **IEEE 802.11 MAC** 的基本擷取方法，它主要是利用一種叫做載波感測多重擷取及衝撞避免(**carrier-sense multiple access/collision avoidance**, 簡稱 **CSMA/CA**)的技術，來提供工作站送收非同步資料，這種方法可用在 **Ad Hoc** 和 **Infrastructure** 的無線區域網路架構中。**PCF** 提供工作站送收具有時限性 (**time bounded**) 的資料，在使用上屬於免競爭(**contention free**)方法，因此也不會發生訊框衝撞的情形，但只能用在某種基礎架構的無線區域網路中。圖13-19描述了**IEEE 802.11 MAC** 通訊協定的架構，其中 **PCF** 是透過 **DCF** 來完成的。在一個**BSS**運作範圍內，這兩種功能是可以共存並容的。一個**BSS**中，如果有一個「協調站」(**Point coordinator**)，則由其來負責督導這兩種服務的交替進行。也就是先進行一段時間的免競爭式傳輸，再跟著進行一段時間的競爭式傳輸。如此一個週期稱為一個超級訊框 (**Superframe**)。超級訊框的長短不

固定，而每一個超級訊框中免競爭式傳輸的時間及競爭式傳輸的時間也可以不固定長短。以下介紹此二種方法的運作原理。

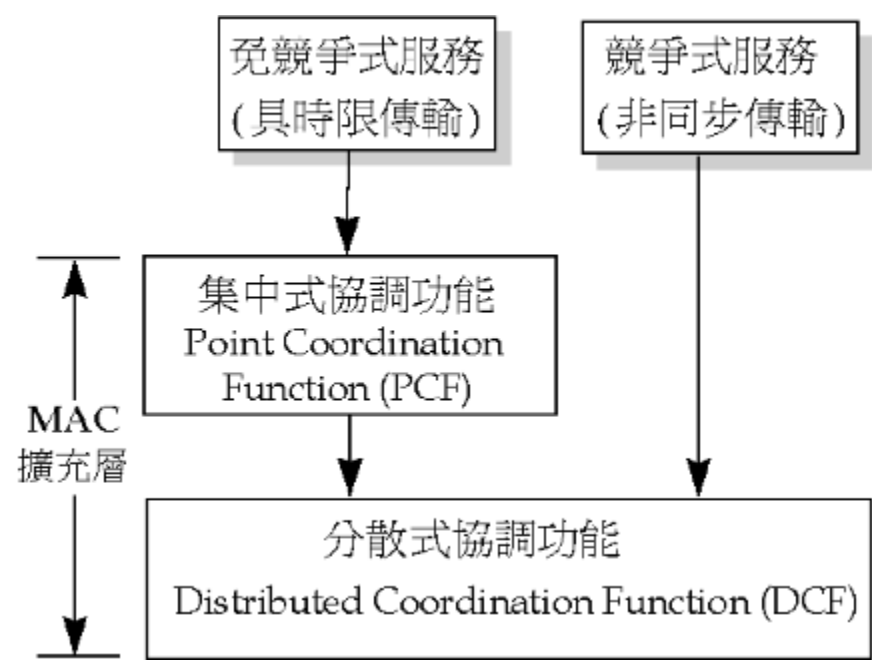


圖13-19 MAC 架構的另一種表示方式

訊框之切割與組合

所謂訊框之切割(**fragmentation**) 是指將一個**MSDU** 訊框切割成許多較小的**MPDU** 訊框。切割的目的是提升訊框傳送的可靠度，因為無線電波的易受干擾性並不適合傳送過長的訊框。切割的工作由傳送器負責。將許多收到的 **MPDU**s 組合成原來的 **MSDU** 則稱為訊框組合 (**Reassembly**)。接收器必須負責將屬於同一個 **MSDU** 的**MPDU**s 收齊後立刻進行組合的工作，不可以將各別的 **MPDU** 轉送出去。只有指定單一目的地的訊框才能被切割，廣播及群播的訊框即使其長度大於切割臨界值 (**aFragmentation Threshold**) 也不能進行切割。

圖13-20 所示為訊框切割的範例。當一個**MSDU**訊框的長度大於切割臨界值就必須被切割。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，都必須分別收到對方的回覆訊息。不過屬於同一個 **MSDU** 的 **MPDU**s 在傳送時是以密集式的方式一個接著一個傳送，當然每一個**MPDU** 都必須收到回覆訊息。一個 **MSDU** 訊框只要呼叫一次**DCF**或**PCF** 的傳送服務就可以傳送其所屬的**MPDU**s, 不必每一個 **MPDU** 都呼叫一次。

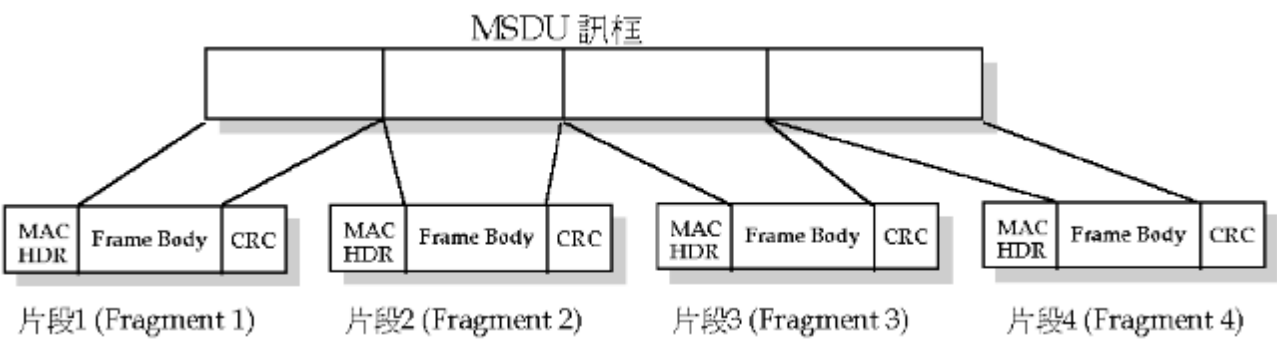


圖13-20 訊框切割範例

13.7.1 分散式協調功能 (DCF)

分散式協調功能是 **IEEE 802.11** 最基本的擷取方法。無論是無基礎架構網路 (**Ad hoc**) 或有基礎架構網路 (**infrastructure**), 所有工作站都應該具有分散式協調功能。如圖13-21 所示，利用 **CSMA/CA** 的技術，不同工作站間能共享同一傳輸媒介，並且解決不同工作站間可能發生的擷取衝突。**CSMA/CA** 是利用所謂的載波感測技術，來判斷某一頻寬中的信號能量是否達到一個基準點，如果信號的強度在這基準點之下，就表示該頻寬未被佔用，因此工作站就可使用該頻寬來送收資料。反之，若信號強度在基準點之上，則表示傳輸媒介目前是忙碌的，在這種情況之下，工作站必需延緩 (**defer**) 訊框傳送時間，直到發現傳輸媒介是空閒的，才能傳送訊框。實際上， **IEEE 802.11** 又將訊框分為三種不同的優先權等級，每種優先權等級的訊框在傳送之前都必需等待一段固定大小的時間，稱為「訊框間隔」(**Inter-Frame Space, IFS**)：

- SIFS (Short IFS)**；短訊框間隔，用來做立即的回應動作。下列訊框送出的等候時間都是 **SIFS**等級：要求傳送訊框 (**RTS**)、允許傳送訊框 (**CTS**)、回覆訊框 (**ACK**) 等等。
- PIFS(PCF IFS)**；**PCF** 訊框間隔。在進行 **PCF** 免競爭式傳輸功能時，工作站傳送訊框前所必須等待的時間。
- DIFS(DCF IFS)**； **DCF** 訊框間隔。在進行 **DCF** 競爭式傳輸功能時，工作站傳送訊框前所必須等待的時間。
- EIFS (Extended IFS)**：延長訊框間隔。工作站在進行重送訊框時所必須等待的時間。

其中 **SIFS < PIFS < DIFS < EIFS**。優先權等級越高的訊框其訊框間隔越短，因此其使用傳輸媒介的機會就越大。這也就是說，工作站發現媒介由忙碌變成空閒時，還不能馬上送出訊框，要依訊框的優先權等級等待一段適當的訊框間隔時間，且在這段時間內媒介仍保持是空閒的才能將訊框送出去。在這種方式之下，同一種優先權等級的訊框發生衝撞的機會仍很高，因為同一種權限的訊框在等候了相同的訊框間隔之後，若發現這段時間內媒介為空閒，就會同時將訊框傳送出去造成衝撞情形。解決此問題的方法是，工作站在等候了訊框間隔的時間後，再等待一段由亂數決定的時間才將訊框傳送出去。因為每個工作站產生的後退時間極可能不同，所以訊框發生衝撞的機會就會降低。這就是後退 (**backoff**) 演算法的精神，與 **IEEE 802.3 CSMA/CD** 的後退演算法相似。

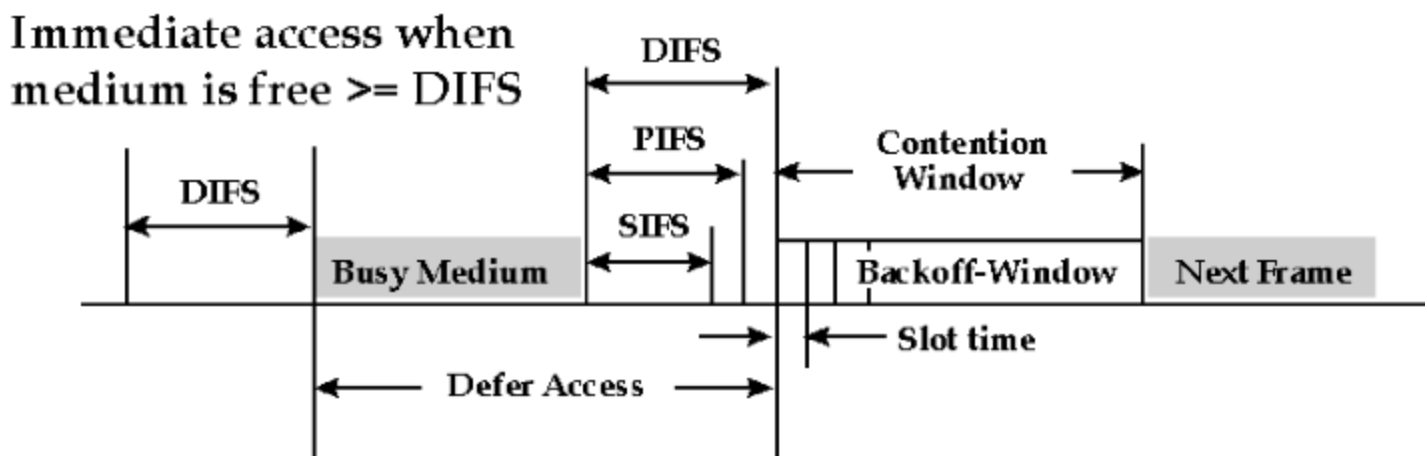


圖13-21 基本擷取方式

雖然 **CSMA/CA** 和 **CSMA/CD** 都是採用載波感測的原理來判斷是否有其它工作站正在使用傳輸媒介，二者之間還是有些不同。其主要差別在於當工作站發現傳輸媒介由忙碌變成空閒時，**CSMA/CD** 會將訊框立刻傳送出去，然後監聽是否發生衝撞，若發生衝撞，則立刻停止傳送訊框並且等待一段隨機延遲時間後再從載波感測開始。**CSMA/CA** 的做法則是在發現傳輸媒介由忙碌變成空閒時，先產生一段隨機延遲時間 (為了說明**CSMA/CA**和**CSMA/CD**的差異，在此暫不考慮訊框間隔)，然後才傳送訊框。其傳送訊框和產生隨機延遲時間的順序正好和 **CSMA/CD**的做法相反。先產生隨機延遲時間的目的是想預先避免發生衝撞，所以此方法叫「衝撞避免」(**collision avoidance**)。這樣做主要是因為在無線網路的系統中衝撞偵測的任務較不容易順利完成，無法做的如有線網路中那樣好。因為在無線網路系統中，不同工作站在傳輸媒介上所使用的信號強度範圍是不定的，因此實體層很難在每次衝撞發生時，都能偵測出發生衝撞。避免發生衝撞並不表示衝撞就不會發生。由 **CSMA/CA** 的特性可以知道，訊框傳送前雖然延遲亂數時間但還是可能發生衝撞，而當衝撞發生時又偵測不出來，此時傳送的訊框就會漏失掉。為了提供可靠的通訊環境，**IEEE 802.11**在衝撞避免的功能中加入了訊框傳送の確認動作，以確保每一筆訊框完整無損。

在無線網路系統中，除了衝撞不易偵測出來外，實體層在使用載波偵測技術時也容易誤判傳送媒介是否忙碌。**IEEE 802.11** 解決前者的方法如下：在傳送端要傳送訊框前，先送出一個「要求傳送」控制訊框 (**Request to Send, RTS**)，而接收端在收到這個控制訊框時則在經過一個 **SIFS** 訊框間隔後立刻回送另一種「允許傳送」控制訊框 (**Clear to Send, CTS**)。只有當傳送端正確的收到接收端所回覆的 **CTS** 時 (表示傳送端所傳送的 **RTS** 沒有發生衝撞)，傳送端才能送出訊框。同時其他工作站看到此送給傳送端的**CTS** 時，也會暫時停止嘗試傳送訊框，因此傳送端傳送的訊框與其他工作站訊框發生衝撞的可能性就會大大的降低。**IEEE 802.11** 解決後者的方法是利用所謂的「虛擬載波偵測」(**Virtual Carrier Sense**)，說明如下：虛擬載波偵測利用一個「網路配置向量」(**Net Allocation Vector, 簡稱 NAV**)，此向量記載其他工作站還需要多久的時間來傳送訊框，而使工作站根据這些資訊能知道傳輸媒介現在是否忙碌。

前面曾說過，在用**RTS/CTS** 的技術送收訊框時，當其他工作站看到接收端送回的 **CTS** 時，也會暫時停止傳送訊框。事實上，正確的說法應是，在 **RTS** 訊框和 **CTS** 訊框裡都包含了一記載著傳送端將來要傳送訊框的持續時間(**duration**)的欄位，而當別的工作站在看到傳送端送出的 **RTS** 訊框，或接收端送出的 **CTS** 訊框時，就會將裡面記載的持續時間登錄到自己的網路配置向量裡。網路配置向量所記載的等待時間可能一直累積，如此一來，時間未歸零前，就表示這個工作站現在不能傳送訊框，因為網路現在是忙碌的（其他工作站傳送訊框的時間還沒結束）。此網路配置向量就好像具備了載波偵測功能，能告訴工作站傳輸媒介現在是否忙碌，因此也就稱為虛擬載波偵測法。

RTS 訊框及 **CTS**訊框必須成對使用，但是傳送訊框之前卻不一定要使用**RTC/CTS**，如圖13-22 所示。使用與否決定在於訊框的長度。系統會定義一個參數稱為**RTSThreshold**, 訊框長度必須大於或等於 **RTSThreshold** 的值才使用**RTS/CTS**。主要的觀念是傳送端在傳送訊框後應該收到回覆訊息才能確認正確傳送。而重要的是訊框在傳送的同時萬一發生衝撞，傳送端由於無法立刻發現，而必須繼續傳送完畢。傳送端必須等不到對方的回覆後才能認定發生衝撞。由於較長的訊框在傳送時被干擾或衝撞的機會也較大，而且長訊框在傳送時也會花較長的時間。在網路狀況未清楚之前直接將長訊框送上網路是非常冒險的，尤其是網路負載較重時，更會嚴重影響網路頻寬使用效率。因此長訊框先用短小的 **RTS** 訊框打頭陣是較聰明的作法。如果 **RTS** 訊框與其他訊框發生衝撞，也可以早點發現。**RTS** 訊框上中的 持續時間值則帶有預約的性質。如果 **RTS** 訊框沒發生衝撞，則接下來的長訊框應該可以成功的傳送出去（還是可能受到干擾，但至少不會衝撞）。

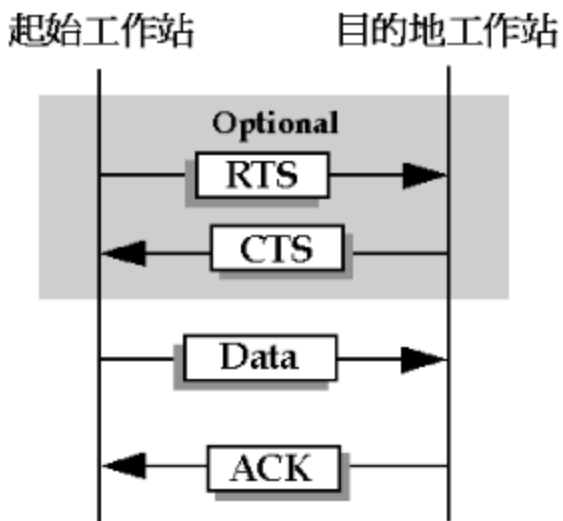


圖13-22 RTS/ CTS 屬於選項使用

圖13-23 所示為傳送端不使用 **RTS/CTS** 而直接傳送訊框之範例。傳送端於等待媒介空閒期達 **DIFS** 時開始傳送訊框。如果沒有發生衝撞，則經過一個 **SIFS** 時間間隔後可收到回覆訊框。此表示訊框傳送成功。其他工作站如果於其間想傳送訊框都必須等到回覆訊框傳送結束後，依照**DCF**的規則爭取傳送權。

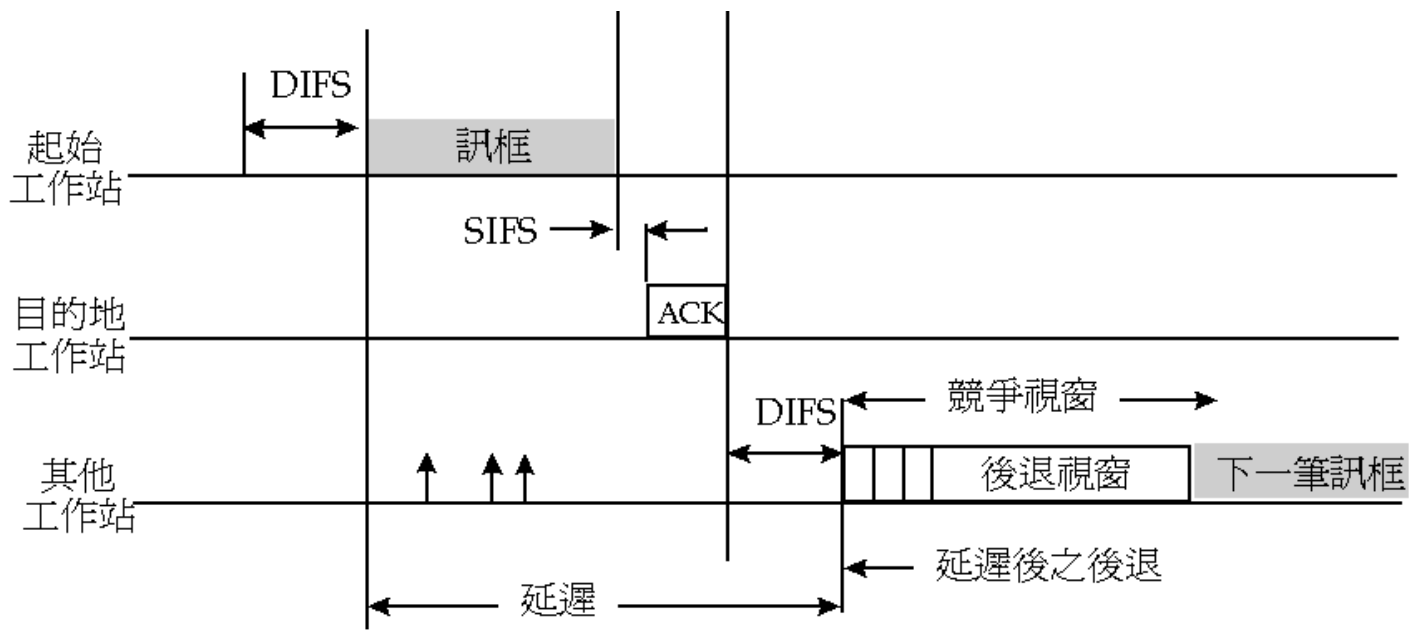


圖13-23 直接傳送訊框範例（不使用RTS/CTS）

圖13-24 所示為使用 **RTS/CTS** 訊框時工作站網路配置向量的設定範例。其中**RTS** 訊框所攜帶的持續時間值（單位為us）為預估其本身傳送完畢至下一筆傳送訊框收到回覆訊框為止。由圖中可發現，所有聽到此 **RTS** 訊框的工作站都將其**NAV**設為此值。相同的，接收端（通常是擷取點）回送的 **CTS** 訊框中也攜帶一持續時間值，其內容也是等於等於其本身 (**CTS** 訊框)傳送完畢至下一筆傳送訊框收到回覆訊框為止之預估時間。其他工作站在其 **NAV** 值不等於零之前不可以傳送訊框。在 **NAV** 值為零後則以 **DCF** 的方式進行訊框的傳送。

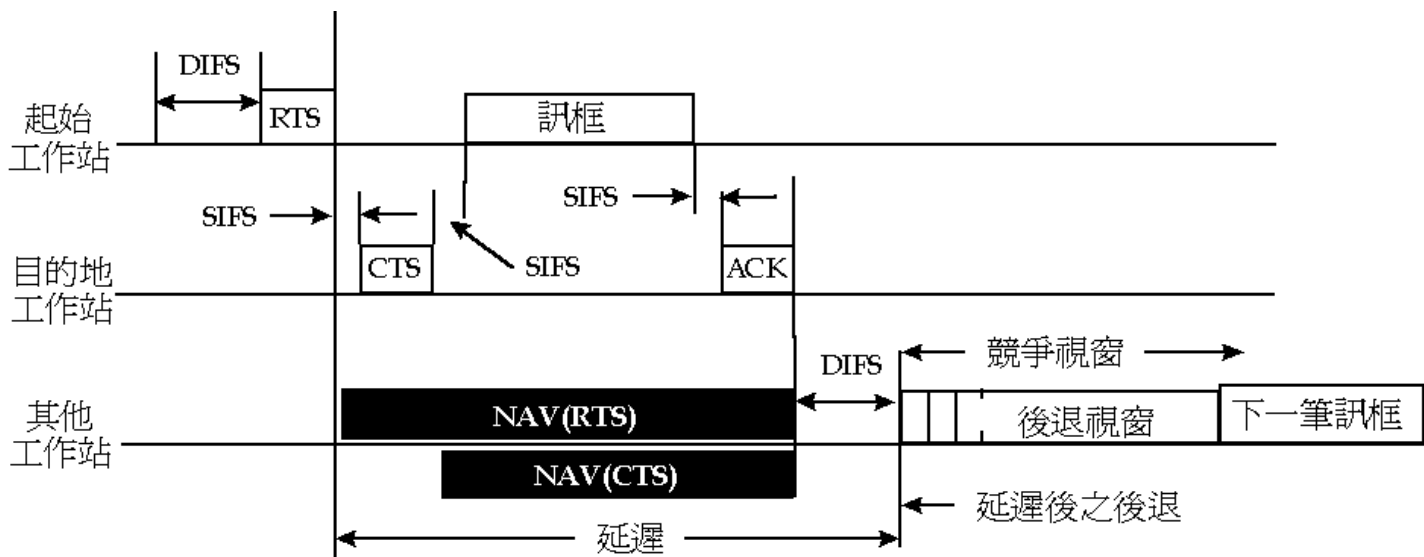


圖13-24 網路配置向量使用範例

RTS 訊框與 **CTS** 訊框都需要攜帶持續時間值的目的是要解決可能存在的隱藏工作站 (**hidden terminals**) 問題。如圖 13-25 所示，工作站 **x** 及工作站 **y** 分別位於擷取點的左邊及右邊。他們都可以和擷取點通訊但彼此之間因功率較小無法直接通訊。當工作站 **x** 傳送 **RTS** 訊框時，擷取點收到此訊框，但是工作站 **y** 沒有收到此訊框，如果 **CTS** 訊框不攜帶持續時間值，則可能發生工作站 **x** 在傳送長訊框時工作站 **y** 也傳送訊框給擷取點。結果兩筆訊框到達擷取點時將造成衝撞，擷取點無法同時接收兩筆在同一頻道傳送的訊框。如果 **CTS** 訊框也攜帶持續時間 值，則工作站 **y** 將聽到此訊框並且設定其 **NAV** 值。結果就不會在工作站 **x** 傳送訊框時又傳送訊框給擷取點。如此便能解決隱藏工作站可能造成的衝撞的問題。

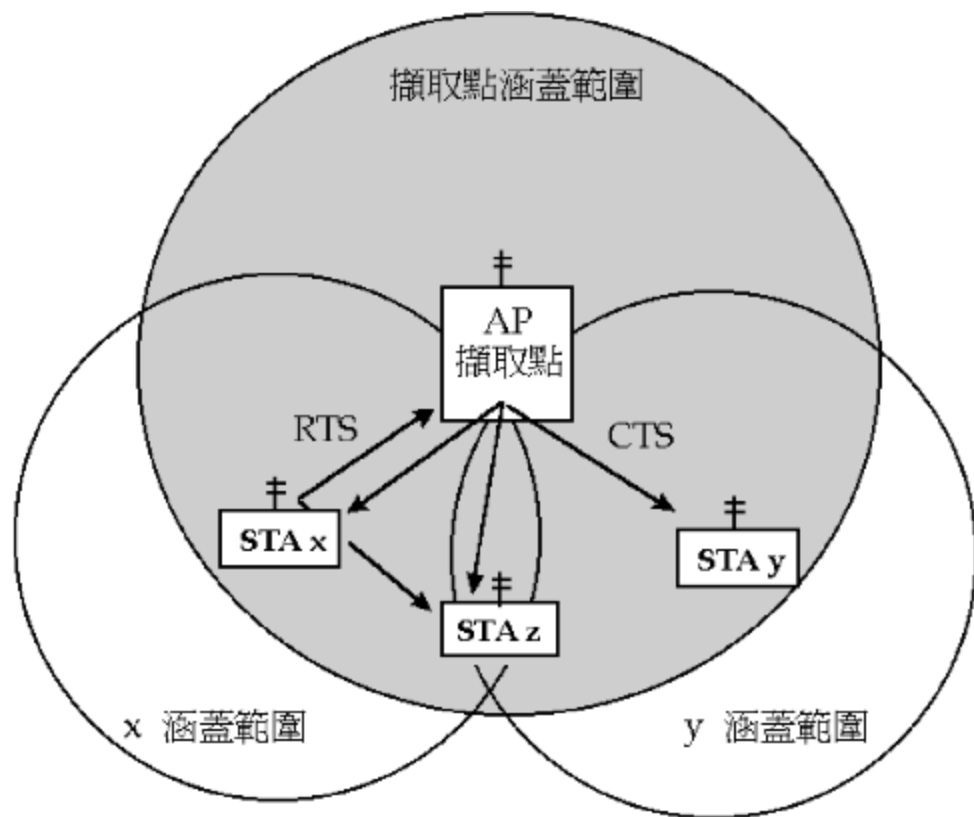


圖13-25 避免隱藏工作站干擾傳送範例

圖13-26所示為傳送端不藉助 **RTS/CTS** 訊框而直接傳送片段 (**fragments**) 的情形。欲傳送的訊框如果過長，傳送端可以事先切割成若干較小的片段，並且在取得傳送權時將這些片段連續的傳送出去，不必為每一個片段爭取傳送權。由於片段比較小，因此可以不需藉助 **RTS/CTS** 訊框來減少衝撞的影響。其方法是利用較短的 **SIFS** 間隔。傳送第一個片段時當然還是可能發生衝撞，如果沒有衝撞並且收到回覆訊框，則此工作站便在 **SIFS** 間隔後就送出下一個片段。當然每一個片段都必須收到一個回覆訊框，而且之間的時間都等於 **SIFS**。其他工作站如果要依照 **DCF** 的原則來爭取傳送權必須至少等待媒介空檔 **DIFS** 間隔，由於 **SIFS** < **DIFS**，其他工作站將沒有機會在片段傳送的過程中奪取傳送權。

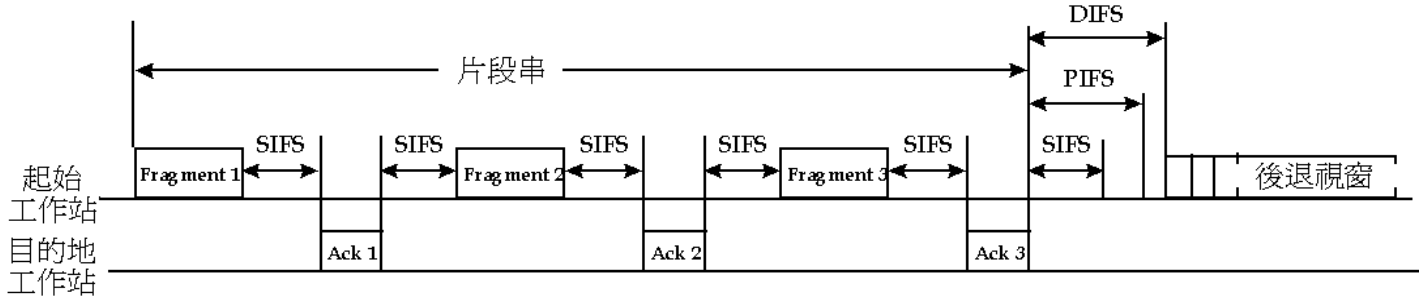


圖13-26 不藉助 **RTS/CTS** 時之多片段傳送範例（利用 **SIFS**）

工作站欲連續傳送一般長度的片段當然也可以藉助 **RTS/CTS** 訊框來預約頻道。其方法如圖13-27 所示。假設

- a** = 傳送**CTS** 所需的時間,
- b** = 傳送**Fragment1** 所需的時間,
- c** = 傳送**ACK1** 所需的時間,
- d** = 傳送**Fragment2** 所需的時間,
- e** = 傳送**ACK2** 所需的時間。

傳送端首先傳送一個 **RTS** 訊框，其所攜帶的持續時間值為預估其本身傳送完畢至下一個片段收到回覆訊框為止（= **3SIFS+a+b+c**）。所有聽到此 **RTS** 訊框的工作站都在**RTS**結束時將其**NAV** 設為此值。相同的，接收端回送的 **CTS** 訊框中也攜帶一持續時間值，其內容也是等於其本身 (**CTS** 訊框) 傳送完畢至下一個片段收到回覆訊框為止之預估時間（= **2SIFS+b+c**）。不同於前的是，片段本身及回覆訊框也都攜帶有持續時間值（與 **RTS/CTS** 訊框之預約功能相同）。此值為對應之回覆訊框傳送完畢至下一個片段收到回覆訊框為止的預估時間(= **2SIFS+d+e**)。也就是說，此值為 **NAV** 延長量。其他工作站在片段傳送結束時則將當時之 **NAV** 值加上此延長值。以圖13-26為例，在 **RTS/CTS** 訊框傳送完畢後，其他工作站之**NAV** 值應剩下 **NAV(CTS)** = **2SIFS+b+c**。工作站待第一個片段傳送完時，將其當時之**NAV**值（**NAV** = **SIFS+c**）加上延長值。也就是說，**NAV**的值修正為等於 (**3SIFS+c+d+e**)。圖中就是等於 **ACK2** 傳送結束的時間。回覆訊框所攜帶的持續時間值則等於本身傳送完畢至下一個片段收到回覆訊框為止的預估時間(= **2SIFS+d+e**)。最後一個片段及所對應之回覆訊框所攜帶的持續時間值則等於 **0**。其他工作站收到此訊框時就知道其為最後一個片段。此時 **NAV** 不做延長的修正，待 **NAV** 減為 **0** 時則以 **DCF** 的方式進行訊框之傳送。

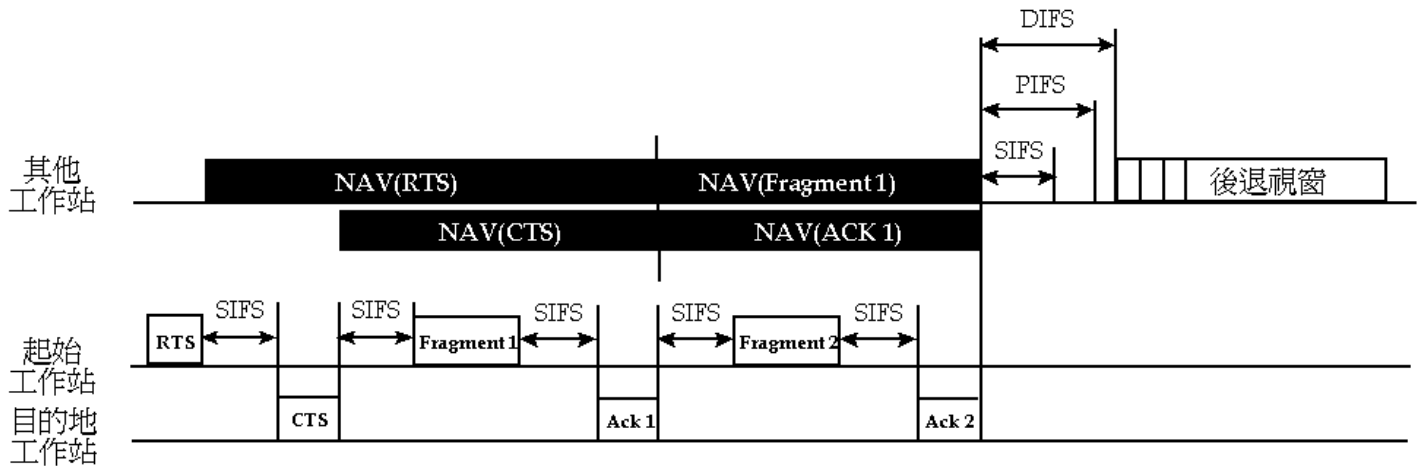


圖13-27 使用**RTS/CTS** 傳送連續片段範例

圖13-28 說明使用 **RTS/CTS** 傳送連續片段但發生回覆訊框流失時的處置範例。如圖所示，其他工作站在第一個片段傳送結束時之 **NAV** = **3SIFS+c+d+e**。如果 **ACK1** 流失，則其他工作站不會延長其 **NAV** 值，而打算於 **NAV=0** 時依照 **DCF** 規則競爭傳送機會。值得注意的是，傳送端如果沒收到 **ACK1**，則認定 **Fragment1** 傳送失敗，必須重送一次。不過此時傳送端不能立刻進行重送的工作，因為其已失去傳送權的絕對優勢，而必須於預計 **ACK1** 傳送結束時間後也依照 **DCF** 規則競爭傳送機會。

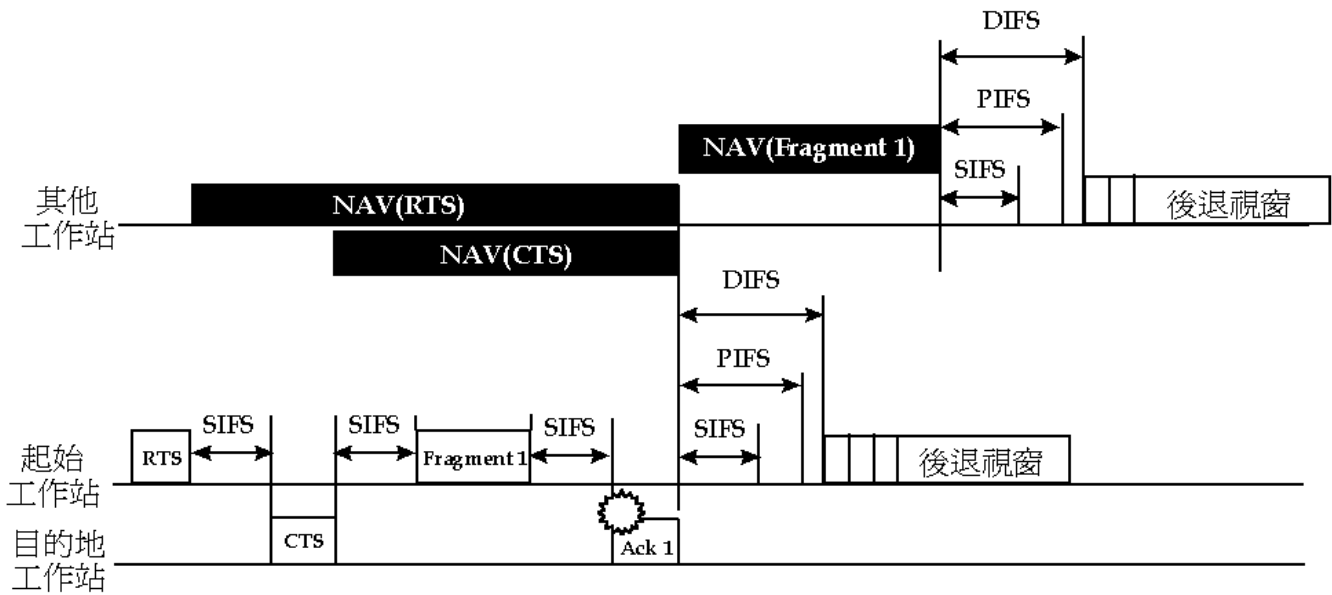


圖13-28 使用**RTS/CTS**傳送訊框範例(**ACK** 流失)

前面曾提過，在 **DCF** 的方法中，當工作站想傳送訊框時，必須先檢測是否有其他工作站正在傳送訊框。即使此時媒介呈現空間的狀態也不能立刻傳送訊框，必須開始等待一段訊框間隔時間(**DIFS**)。在這段時間中，如果仍然沒有其他工作站傳送訊框，則在時間到時可立即傳送訊框。如果開始時媒介就忙碌或在 **DIFS** 時間到之前有其他工作站率先傳送訊框，則必須繼續監聽此訊框之傳送，待訊框傳送結束後再繼續等待一段訊框間隔時間(**DIFS**)。在這段時間中，如果仍然沒有其他工作站傳送訊框，則接著進入所謂的競爭視窗 (**Contention Window, CW**)。此時工作站會產生一隨機時段（稱為後退時間, **backoff time**）。此後退時間隨時間遞減，工作站必須等到其後退時間減為零時才能傳送訊框。值得注意的是，此後退時間不一定能順利的持續遞減。如果只有一部工作站進入競爭視窗，則其後退時間可以持續遞減到零。如果有許多工作站同時進入競爭視窗，則在遞減的過程中，只要有其他工作

站傳送訊框就表示此輪之競爭視窗結束，此時就必須暫停遞減的工作，待下次再進入競爭視窗時才繼續遞減。舉例來說，如果有n部工作站 **S1, S2, ..., Sn** 在前一筆訊框傳送期間陸續想要傳送訊框，則這些工作站都會在該筆訊框傳送結束並且等待一個 **DIFS** 時段後同時進入競爭視窗。假設這些工作站分別產生**b1,b2,...,bn**的後退時間，其中 **b1 < b2 < ... < bn**。則工作站 **S1** 的後退時間可以持續遞減到零並且在此輪的競爭中率先傳送出去因為其後退時間（**b1**）最短。其他工作站 **Si** 則會在其後退時間遞減到等於 **bi - b1** 時偵測到此傳送行為。此表示其在此競爭視窗中沒有成功，於是暫時將其後退時間凍結起來，待下次再進入競爭視窗時則以此值為其退後時間起始值。依此方式，如果中間沒有其他新的工作站加入競爭的行列，則這些工作站傳送訊框的順序將是 **S1, S2, ..., Sn**。換句話說，工作站必須等到其後退時間減到零時才能將訊框傳送出去。如果所有工作站的後退時間都不相同，則訊框在傳送時就不會發生衝撞的情形。如果有兩個或兩個以上的工作站剛好產生相同的後退時間，則這些工作站將同時傳送訊框並且發生衝撞的現象。前面曾說過，每一筆訊框的傳送都必須收到對方的回覆訊息才能算傳送成功。如果發生衝撞的情形（或訊框傳送時發生錯誤）則參與的工作站都不會收到任何回覆訊息。此時該工作站將進行重送階段 (**Retransmission**)。進行重送階段的工作站在進入競爭視窗前所等待的時間將是延長訊框間隔時間(**EIFS**), 而不是訊框間隔時間(**DIFS**)。在進入競爭視窗時其後退時間的計算也將不同。以下說明工作站如何產生後退時間的初始值。後退時間計算方式如下：

Backoff = INT(CW x Random()) x 時槽時間

其中**INT(x)** 整數函示，表示小於或等於 **x** 的最大整數,

CW 是一個介於 **CW_{min}** 和 **CW_{max}** 間的整數,

Random() 為介於 **0** 與 **1** 間的實數，

時槽時間= 傳送器開啓延遲 + 媒介傳遞延遲 + 媒介忙碌偵測反應時間。

CW是一個競爭視窗參數，每一筆訊框第一次傳送時採用的值為**Cw_{min}**。每當因為工作站傳送的訊框發生衝撞或錯誤現象而必須進行重送的程序時，**CW** 值就會依序增加，直到其值達到**Cw_{max}** 為止。在標準中，此值之順序依序為 **(7,15,31,63,127,255,255,255,...)**, 如圖**13-29** 所示。也就是說，當一筆訊框第一次進入競爭視窗時其**CW = Cw_{min} = 7**，並且依此產生後退時間。如果此筆訊框第一次傳送時（後退時間遞減為零，其間可能經過許多競爭視窗）沒有成功，則下一次再進入競爭視窗時其**CW=15**，並且依此產生第二個後退時間。依此類推，第五次重送時其值將為**CW = Cw_{max} = 255**。第六次以上的重送則仍然採用 **Cw_{max} = 255**。

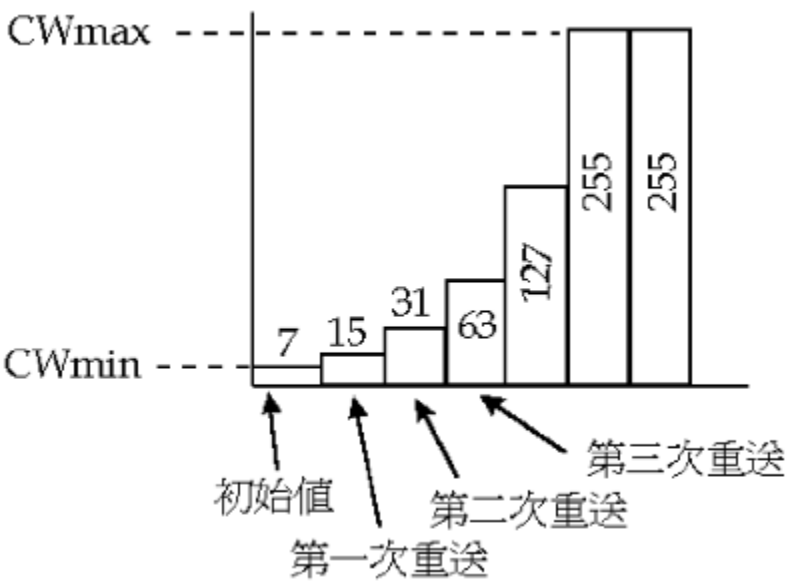
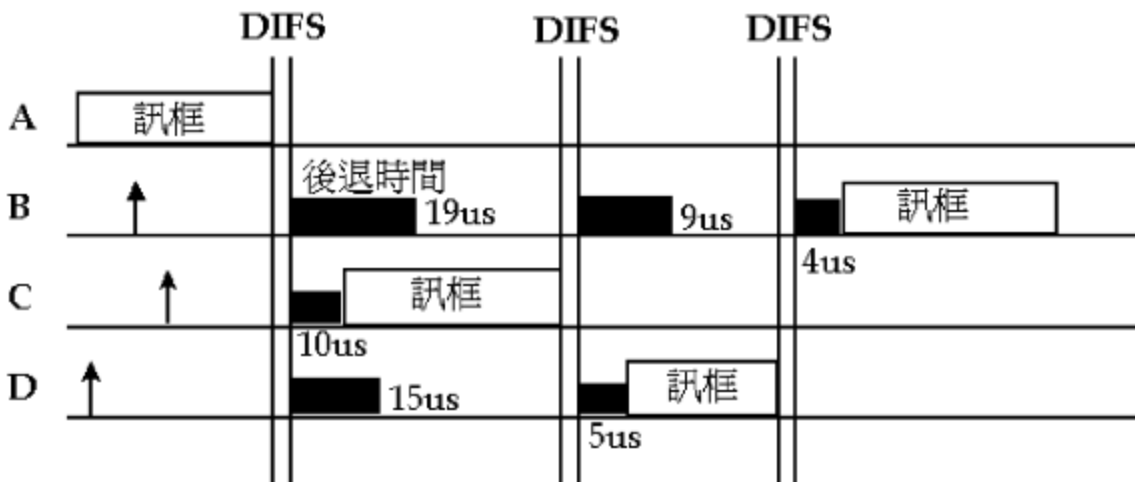


圖13-29 CW 值增加方式

圖**13-30(a)** 所示為一個工作站傳送訊框時後退程序的例子。此例中，一開始工作站 **B、C、D** 想傳送訊框，而傳輸媒介為工作站 **A** 所使用。當工作站 **A** 送完訊框時，工作站 **B、C、D** 在等待了一個 **DIFS** 時間後，就分別利用 **CW = Cw_{min} = 7** 產生一個隨機後退時間（假設分別為 **19us, 10us, 及 15us**），然後開始進行遞減的工作。在這個例子中，由於工作站 **C** 產生的後退時間最小(**10 us**)，於是率先遞減為零並且在這次的競爭視窗中取得了傳輸媒介的使用權並且傳送出訊框。此時工作站 **B、D** 的後退時間分別剩下 **9us** 及 **5us**。工作站 **C** 傳送訊框的過程中，此兩個後退時間被暫時凍結。在進入第二個競爭視窗時則分別以此值為其後退時間繼續遞減。結果在 **5us** 後工作站**D** 開始傳送其訊框，而工作站 **B** 必須等到進入第三個競爭視窗 **4us**後才會開始傳送其訊框。

圖**13-30(b)** 所示為另一個工作站傳送訊框時後退程序的例子。開始時一樣假設工作站 **A**正在傳送訊框而工作站 **B、C、D** 陸續想傳送訊框。當工作站 **A** 送完訊框時，工作站 **B、C、D** 在等待了一個 **DIFS** 時間後，就分別產生一個隨機後退時間（假設分別為 **19us, 10us, 及 15 us**），然後開始進行遞減的工作。由於工作站 **C** 產生的後退時間最小，於是在這次的競爭視窗中取得了傳輸媒介的使用權並且傳送出訊框。當工作站 **C** 傳送訊框時，假設工作站 **E** 也想傳送訊框，於是變成工作站 **B、D、E** 共同競爭媒介使用權。在進入下一個競爭視窗時，工作站 **B、D** 的後退時間分別為 **9us** 及 **5us**。而工作站 **E** 則利用 **CW = Cw_{min} = 7** 產生一個隨機後退時間（假設為 **7us**）。結果在 **5us** 後工作站 **D** 開始傳送其訊框，而工作站 **B、E** 的後退時間則分別剩下 **4us** 及 **2us**。結果在下一個競爭視窗中工作站 **E** 將可較早傳送訊框，而工作站 **B** 則必須等到進入第四個競爭視窗 **2us** 後才會開始傳送其訊框。

圖**13-30(c)** 所示為工作站傳送及重送訊框時後退程序的例子。開始時一樣假設工作站**A** 正在傳送訊框而工作站 **B、C、D、E** 陸續想傳送訊框。當工作站 **A** 送完訊框時，工作站 **B、C、D、E** 在等待了一個 **DIFS** 時間後，就分別利用 **CW = Cw_{min} = 7** 產生一個隨機後退時間（假設分別為**15us, 10us, 15 us** 及**18 us**），然後開始進行遞減的工作。由於工作站 **C** 產生的後退時間最小，於是在這次的競爭視窗中取得了傳輸媒介的使用權並且傳送出訊框。此時工作站 **B、D、E** 的後退時間分別剩下 **5us, 5us, 及 8us**。工作站 **C** 傳送訊框的過程中，此三個後退時間被暫時凍結。在進入第二個競爭視窗時則分別以此值為其後退時間繼續遞減。結果在 **5us** 後工作站**B** 及 **D** 同時開始傳送其訊框，結果造成衝撞的現象。由於沒有收到回覆訊息，工作站 **B** 及 **D** 分別進入重送階段，並且在下一個競爭視窗中(工作站 **B** 及 **D** 此時必須等待 **EIFS** 時段才能進入競爭視窗) 分別利用 **CW = 15** 產生一個隨機後退時間（假設分別為 **20 us** 及 **25 us**）。而工作站 **E** 則在第三個競爭視窗中(工作站**E** 只需等待 **DIFS** 時段即可進入競爭視窗) 等待 **3us** 後開始傳送訊框。此時工作站 **B、D** 的後退時間分別剩下 **17us** 及**22us**。結果工作站**B** 必須等到進入第四個競爭視窗 **17us** 後才會開始傳送其訊框，而工作站 **D** 則必須等到進入第五個競爭視窗 **5us** 後才能開始傳送其訊框。



The diagram illustrates the CSMA/CD protocol with five stations (A, B, C, D, E) and four DIFS (Distributed Inter Frame Space) intervals. Station A transmits a frame. Stations B, C, and D attempt to transmit but detect a collision and abort. Station E attempts to transmit but also detects a collision and aborts. The diagram shows the backoff times for each station after each collision.

Station	Initial Attempt	Collision Detected	Backoff Time	Final Action
A	Transmits frame	Collision at 10us	19us	Retransmits frame
B	Attempts to transmit	Collision at 10us	9us	Aborts
C	Attempts to transmit	Collision at 10us	4us	Aborts
D	Attempts to transmit	Collision at 10us	2us	Aborts
E	Attempts to transmit	Collision at 10us	10us	Aborts

	DIFS	DIFS	DIFS	DIFS
A	訊框			
B	↑ 後退時間 15us	5us 訊框	CW = 15 20us	訊框
C	↑ 10us 訊框	5us 5us 訊框		17us
D	↑ 15us	5us 5us 訊框	CW = 15 25us	22us
E	↑ 18us	5us 8us	3us 訊框	

圖13-30 工作站傳送訊框時後退程序範例

IEEE 802.11 除了提供上節所描述 **DCF** 方法來傳送非同步訊框外，也提供了另一個方法來支援「免競爭」的服務，以傳送具時限性的訊框。此方法稱為「集中協調式功能」(**Point Coordination Function**, 簡稱 **PCF**)。**PCF** 運作的特色是在一個具有協調者 (**Point Coordinator**) 的 **BSS** 中，所有工作站都能接收在 **PCF** 控制下所傳送的所有訊框。至於工作站有無能力回覆由協調者所傳送的免競爭輪詢 (**Contention Free Poll**, **CF-Poll**) 則屬於一種選項。有能力回覆免競爭輪詢的工作站稱為可輪詢 (**CF-Pollable**) 工作站。無能力回覆免競爭輪詢的工作站稱為非輪詢 (**Non CF-Pollable**) 工作站。可輪詢工作站可以要求加入協調者的輪詢名單中。每次被輪詢到時可以傳送一筆訊框。非輪詢工作站則在免競爭週期中不能傳送訊框，只能在收到訊框時回送一個回覆訊框。可輪詢工作站所傳送的訊框的目的地工作站可以是任何工作站 (協調者，可輪詢工作站，或非輪詢工作站)。此訊框也可順便攜帶一回覆 (**ACK**) 訊息，用以回覆前一筆由協調者傳送來的訊框。如果此訊框本身沒有收到回覆訊息，則此工作站不可以立刻進行重送的程序，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此訊框。如果可輪詢工作站所傳送的訊框的目的地工作站是一個非輪詢工作站，則此非輪詢工作站必須依照 **DCF** 的方式在一個 **SIFS** 間隔時回送一個回覆訊框。在 **PCF** 週期中，協調者與被輪詢者在傳送訊框時都不使用 **RTS/CTS** 控制訊框。協調者在免競爭週期內重送訊框時並不像 **DCF** 所採用的後退方法 (**backoff**)。它等到該目的地工作站再次成為輪詢名單中的首位時才重送此訊框。也可以在免競爭週期內等到一個 **PIFS** 的空檔時重送此訊框。

在免競爭週期 (**Contention Free Period, CFP**) 內，訊框的傳送由 **PCF** 控制，而在競爭週期(**Contention Period, CP**) 內，訊框的傳送則由**DCF** 所控制。免競爭週期與競爭週期應該輪流出現，如圖**13-31** 所示。免競爭週期起始於一個由協調者所傳送而攜帶 **DTIM** 元件的 **Beacon** 訊框，終止於由協調者所傳送的 **CF-End** 訊框或 **CF-End+ACK** 訊框。

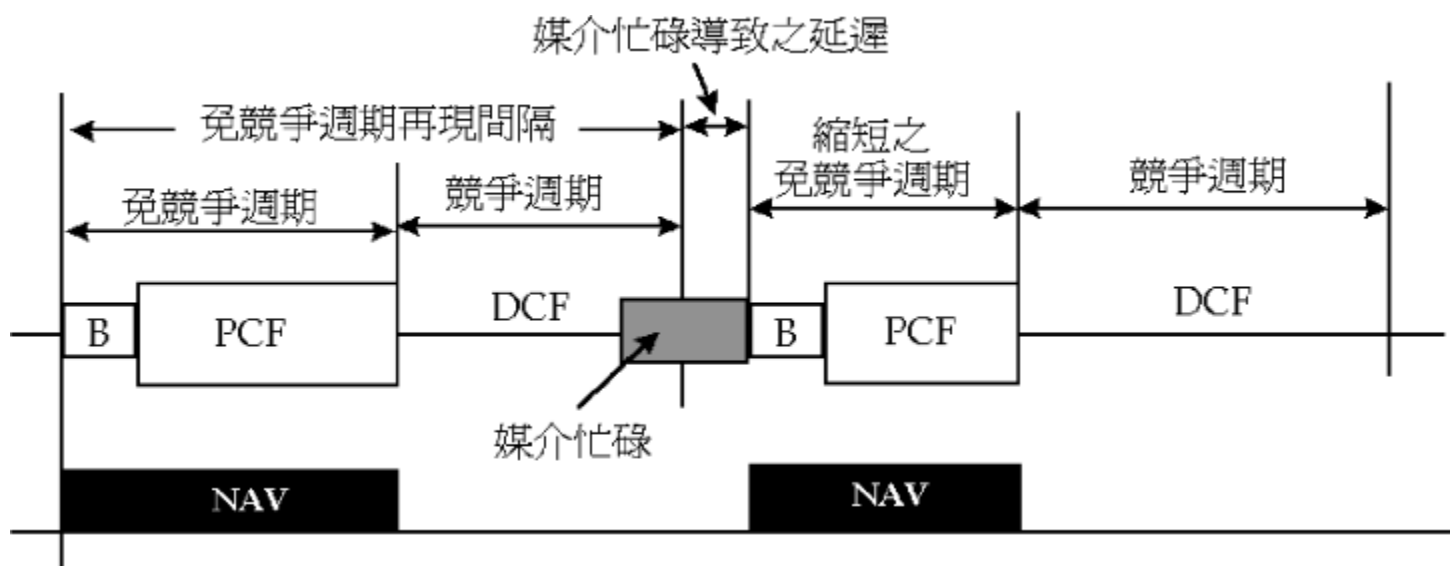


圖13-31 免競爭週期/競爭週期 交替出現

協調者依照系統之免競爭再現率 (**Contention-Free Repetition Rate, CFPRate**) 產生免競爭週期。免競爭出現率是以包含幾個**DTIM** 間隔來定義。協調者必須利用**Beacon** 訊框中的 **CF Parameter Set** 元件中的 **CFPPeriod** 欄位將此值傳送給所有屬於同一個 **BSS** 的工作站知道。免競爭週期的長度由協調者決定，其最大值由**MAC MIB**中的**aCFPMaxDuration** 物件所定義。免競爭週期的最大長度或實際長度不一定要是 **Beacon** 間隔的整數倍。如果免競爭週期的長度大於 **Beacon** 間隔，則協調者在免競爭週期間會於適當的時機送出 **Beacon**訊框。這些**Beacon** 訊框 （包括第一個**Beacon** 訊框 ）所攜帶的 **CF Parameter Set** 元件中的 **CFPDurRemaining** 欄位值 （記錄此免競爭週期之最大剩餘時間，單位為毫秒 **ms**）都不等於零。在競爭週期間所傳送的 **Beacon** 訊框的 **CFPDurRemaining** 欄位值則都應該等於零。圖**13-32** 所示為這些參數間的關係範例。圖中 **CFPRate** 等於兩個 **DTIM** 期間，也就每經過兩個 **DTIM** 期間，就必須開始啟動一個免競爭週期。圖中一個 **DTIM** 期間等於三個 **Beacon** 期間。也就是一個超級訊框的長度等於六個 **Beacon** 期間。協調者在此期間將傳送六個 **Beacon** 訊框，其中第一個 **Beacon**及第四個 **Beacon** 訊框將攜帶 **DTIM** 元件。圖中免競爭週期大約是**2.5** 個 **Beacon** 期間。

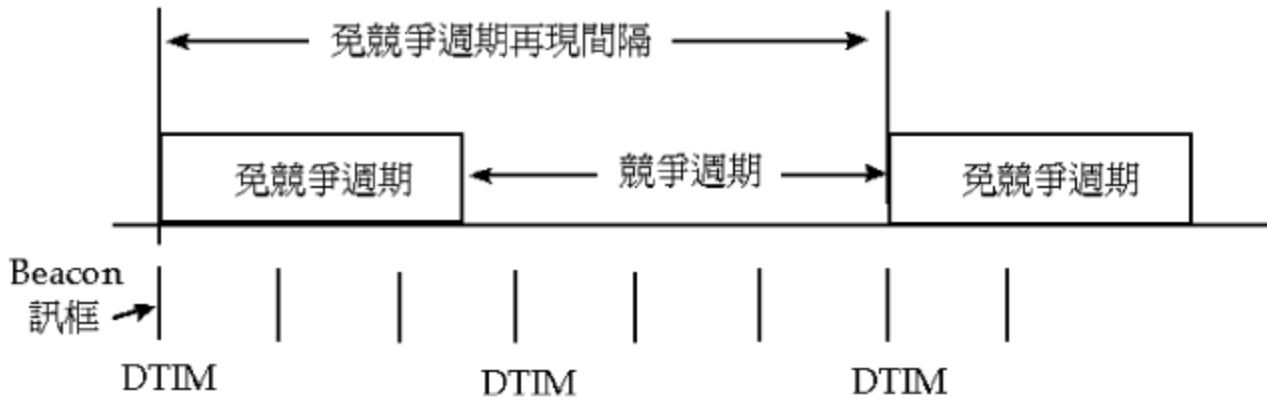


圖13-32 Beacon 間隔與免競爭週期範例

協調者可以根據其必須處理的交通量及輪詢工作站數量而提早或及時終止免競爭週期。由於原定傳送 **Beacon** 訊框的時間 (**Target Beacon Transmission Time, 簡稱 TBTT**) 可能恰巧有其他訊框正在傳送（媒介忙碌中），因此傳送 **Beacon** 訊框的時間可能會被延後（必須等該訊框傳送結束且完成回覆工作後）。這使得此免競爭週期必須被迫縮短，縮短的時間就是 **Beacon** 訊框被延後傳送的時間，如圖**13-33** 所示。此最大的延遲時間發生在該訊框是一筆 **MSDU**訊框且其長度大於**aRTSThreshold** 臨界值及 **aFragmentationThreshold** 臨界值。此時最多會包含一個 **RTS** 訊框，一個 **CTS** 訊框，若干 **Fragment** 訊框，而且每一個 **Fragment** 訊框後面都跟著一個 **ACK** 訊框。連續兩個訊框間則有一個**SIFS** 時間間隔。如果 **Beacon** 訊框真的發生被延後傳送的情形，則在免競爭週期開始的第一個**Beacon** 訊框上之**CFPDurRemaining** 應該要仔細計算，以保證此免競爭週期可以在 **TBTT + aCFPMaxDuration** 之前結束。

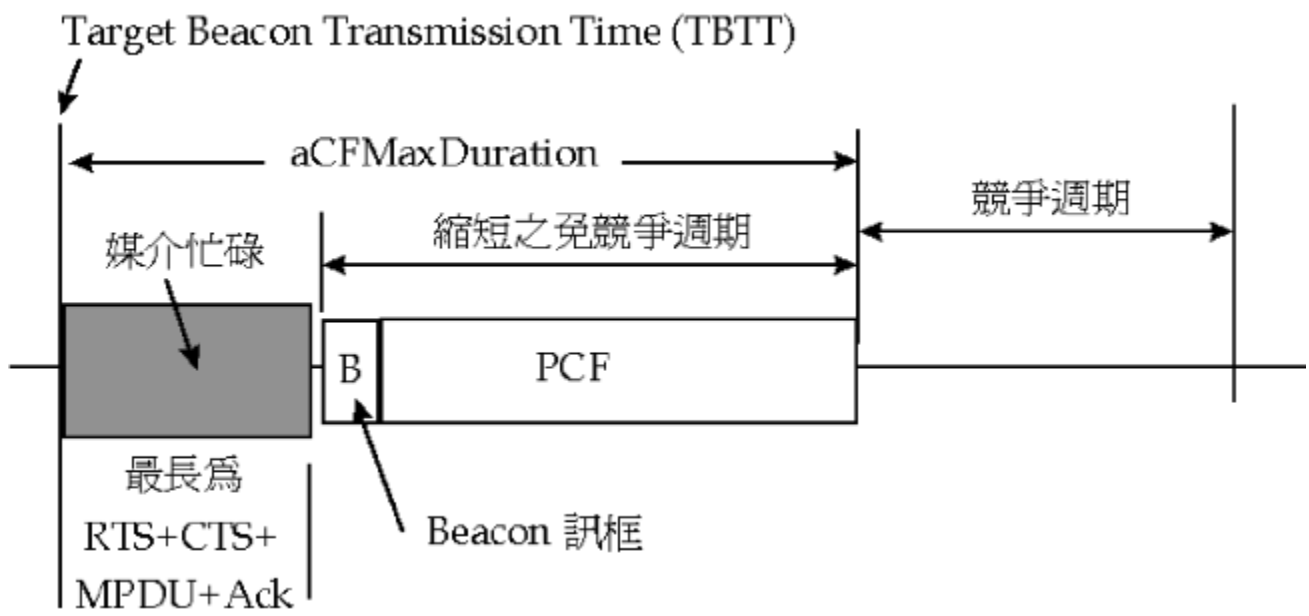


圖13-33 延遲傳送之 Beacon 訊框與縮短之免競爭週期範例

PCF 運作程序

在免競爭週期中工作站傳送訊框的方式是依照一種稱為「輪詢」(**polling**)的方法上，並且由 **BSS** 中擷取點內部的協調者來控制。協調者在免競爭週期的開始就取得傳輸媒介的使用控制權，並且在免競爭週期中以等待較短的訊框間隔 (**PIFS < DIFS**) 方式來維持傳輸媒介的控制權。所有在 **BSS**中的工作站 (協調者除外) 於免競爭週期開始時都將其 **NAV** 值設為免競爭最大週期 (**CFPMaxDuration**)。這樣可以避免因工作站未被輪詢到卻傳送訊框所造成的問題。

在免競爭週期中訊框的回覆方式依該筆訊框的目的地工作站性質分為三種：(1) 接收該筆訊框的工作站是協調者。此時協調者可在傳送下一筆訊框及輪詢給別的工作站時順帶回覆此訊框：**Data+CF-Poll+CF-ACK**, 或在傳送輪詢給別的工作站時順帶回覆此訊框：**CF-Poll+CF-ACK**。(2) 接收該筆訊框的工作站剛好也是被協調者輪詢的工作站。該工作站若有訊框要傳送則可在傳送訊框時順帶回覆此訊框：**Data+CF-ACK**。若無訊框要傳送則專程回覆此訊框：**CF-ACK**。(3) 接收該筆訊框的工作站不是剛好被輪詢的工作站（包括未輪詢工作站及非輪詢工作站）。此時該工作站應該以 **DCF ACK** 的方式回覆此訊框：等待一個 **SIFS** 間隔候傳送一個回覆訊框。

在免競爭週期開始前，協調者應該先偵測傳輸媒介，並且在媒介空檔時間達一個 **PIFS** 時傳送一個**Beacon** 訊框啟動此免競爭週期。此 **Beacon** 訊框中帶有**CF Parameter Set** 元件及 **DTIM** 元件。之後協調者必須等待至少一個**SIFS**間隔後傳送下列四種訊框的一種：**Data** 訊框，**CF-Poll** 訊框, **Data+CF-Poll** 訊框, 或 **CF-End** 訊框。如果免競爭週期是空的（協調者沒有資料要送給工作站，也沒有輪詢名單），則 **Beacon** 訊框後應立即跟上一個 **CF-End** 訊框。

在免競爭週期中處理**NAV**的方法主要是考慮到網路上可能存在重疊但彼此協調的**BSS**。前面已說過，所有在 **BSS**中的工作站 (協調者除外) 於免競爭週期開始時都將其 **NAV** 值設為免競爭最大週期 (**CFPMaxDuration**)。之後每次收到一個 **Beacon** 訊框，就根據其上的**CFPDurRemaining** 值來修正 **NAV** 值。這包括由其它重疊**BSS** 的協調者所送來的 **Beacon** 訊框。在 **NAV** 值不等於零之前工作站是不會主動傳送訊框的，這樣可以避免工作站在免競爭週期間取得媒介的控制權。尤其是當免競爭週期橫跨許多個媒介佔用週期（**medium-occupancy intervals**,如採用跳頻實體層之 **dwell** 週期）時，這個方法更是重要。此方法同時也有降低隱藏工作站 (**hidden stations**) 在免競爭週期中因偵測媒介空檔達**DIFS** 時間而傳送訊框的可能性。這種傳輸可能破壞一筆正在傳送中的訊框。協調者在免競爭週期終止時會傳送一個**CF-End** 訊框或 **CF-End+ACK** 訊框。工作站如果收到此類訊框，無論是由哪一個 **BSS** 收到，都應該將其 **NAV** 值設為零，並且開始進入競爭週期。

當工作站加入一個含有協調者且正運作中的**BSS**時，必須先設定其**NAV**值，不能立刻傳送訊框。方法是利用接收到的任何 **Beacon** 訊框或 **Probe**

Response 訊框中的 CFDurRemaining 值。

PCF傳輸程序

PCF傳送訊框的次序通常是先由協調者送給工作站，然後由工作站送給協調者，如此重複交替進行。至於工作站傳送訊框的先後順序則由協調者來控制。圖13-34 為免競爭週期中訊框傳送的典型範例。

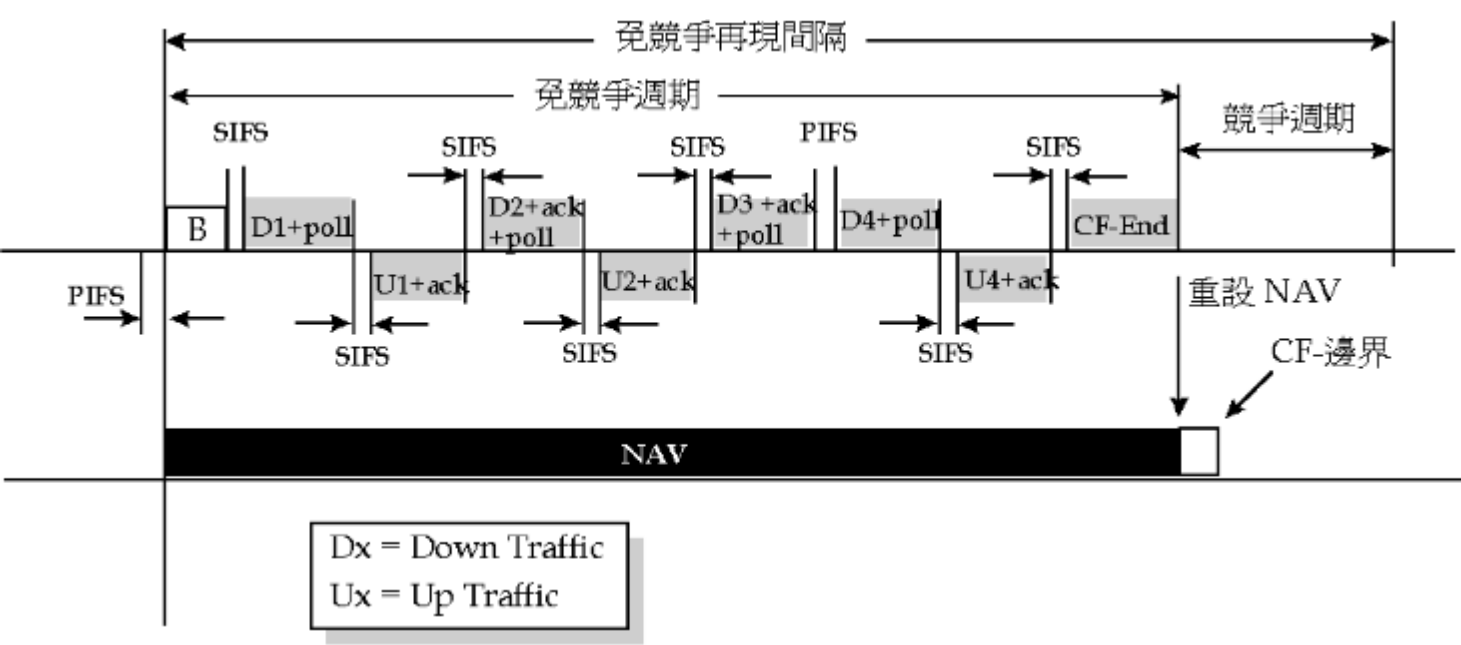


圖13-34 免競爭週期中訊框傳送範例

工作站如果配置跳頻式實體層 (FH PHY), 則每次取得頻道使用權時，有效期只有一個dwell time boundary。因此工作站如果要傳送訊框，則必須在dwell time boundary之前傳送完成，並且收到對應之回覆訊框。被輪詢的工作站如果預期不能在dwell time boundary之前完成此事，則應該延遲傳送至下一次機會，並且傳送一個 ACK 訊框或 CF-ACK 訊框。如果dwell time boundary已經非常逼近，使得工作站連傳送一個 ACK 訊框或 CF-ACK 訊框都無法及時完成時，則協調者就不應該輪詢該工作站。也就是說，協調者輪詢某工作站時，一定保證該工作站至少有足夠的時間傳送一個 ACK 訊框或 CF-ACK 訊框。

PCF 傳送訊框的運作模式可以分為兩種：(1) 當協調者是傳送工作站或接收工作站時，(2) 當協調者不是傳送工作站也不是接收工作站時。以下說明此兩種模式的運作情形。

首先是當協調者是傳送工作站或接收工作站時。協調者傳送給可輪詢工作站的訊框可以是下列七種的任何一種：

Data 訊框: 使用時機是當協調者欲傳送 Data 訊框給某一工作站，而該接收工作站不是被輪詢的工作站，而且協調者手上無尚未回覆的訊框。

Data+CF-ACK 訊框：使用時機是當協調者欲傳送 Data 訊框給某一工作站，而該接收工作站不是被輪詢的工作站，而且協調者手上有一筆 SIFS 時間以前從可輪詢工作站收到但尚未回覆的訊框。

Data+CF-Poll 訊框：使用時機是當協調者欲傳送 Data 訊框給某一工作站，而該接收工作站正好是下一個被輪詢的工作站，而且協調者手上無尚未回覆的訊框。

Data+CF-ACK+CF-Poll 訊框：使用時機是當協調者欲傳送 Data 訊框給某一工作站，而該接收工作站正好是下一個被輪詢的工作站，而且協調者手上有一筆 SIFS 時間以前從可輪詢工作站收到但尚未回覆的訊框。

CF-Poll 訊框：使用時機是當協調者並無 Data 訊框給某一工作站，但該工作站正好是下一個被輪詢的工作站，而且協調者手上無尚未回覆的訊框。

CF-ACK+CF-Poll 訊框：使用時機是當協調者並無 Data 訊框給某一工作站，但該工作站正好是下一個被輪詢的工作站，而且協調者手上有一筆 SIFS 時間以前從可輪詢工作站收到但尚未回覆的訊框。

CF-ACK 訊框：使用時機是當協調者並無 Data 訊框給某一工作站，也不輪詢工作站。不過協調者手上有一筆 SIFS 時間以前從可輪詢工作站收到但尚未回覆的訊框。（例如協調者下一個欲傳送的訊框是屬於管理類的訊框，如Beacon訊框，則是使用此CF-ACK 訊框的適當時機）。

協調者也可以在免競爭週期內傳送Data 訊框或管理訊框給非輪詢工作站 (non-CF-Pollable) 及非省電工作站 (non-Power Save)。這些工作站則應該在一個 SIFS 間隔後回送一個 ACK 訊框。協調者當然也可以在免競爭週期內傳送廣播訊框或群播訊框。因為啟動免競爭週期的Beacon 訊框帶有DTIM元件，如果某些已連結的工作站處於省電模式，則這些欲廣播或群撥給省電模式工作站的訊框應該在此Beacon 訊框後立刻傳送。

可輪詢工作站只要收到任何由協調者送來而且設定 CF-Poll 的訊框，就可以在一個 SIFS 間隔後傳送一個 Data 訊框。如果工作站剛好沒有訊框要送，則傳送一個Null 訊框。如果攜帶 CF-Poll 的訊框需要回覆，則可傳送一個 Data+CF-ACK 訊框（或 Null+CF-ACK 訊框）。如圖13-35 所示，U1 訊框同時也攜帶前一個 D1 訊框的回覆訊息，而 D2 訊框則攜帶 U1 訊框的回覆訊息。

在免競爭週期中，協調者傳送訊框的時間間隔是 SIFS, 除非原定 SIFS 間隔後應該出現的訊框沒有出現。此時協調者在繼續等待至一個 PIFS 間隔後，立刻送出下一個訊框。這樣協調者就不會因為某些回覆或回應訊框的流失而喪失主控權。如果協調者等待時間過久（大於 DIFS），則某些剛加入的非輪詢工作站可能在偵測媒介空檔期達 DIFS 時開始傳送訊框，造成混亂。如圖13-35 所示，D3 訊框除了攜帶前一個U2 訊框的回覆訊息外，也攜帶CF-Poll 輪詢某工作站，但該工作站沒有任何反應（也許已當機）。協調者在繼續等待至一個 PIFS 間隔後，立刻送出下一個 D4 訊框。

當協調者無訊框可傳送且輪詢名單空白時，或 CFPDurRemaining 時間等於零時，可以送出一個 CF-End 訊框終止此免競爭週期。如果之前尚有訊框須回覆，則可傳送 CF-End+ACK 訊框。所有收到 CF-End 訊框或 CF-End+ACK 訊框的工作站都應該將其 NAV 值設為零，並且開始進入競爭週期。如圖13-35 所示，協調者送出一個 CF-End 訊框後（如果U4訊框須回覆，則應該是 CF-End+ACK 訊框），所有工作站將其 NAV 值設為零。由於此時 CFPDurRemaining 時間尚不等於零 (CFP < CF-Max-Duration),此免競爭週期的終止應該是屬於協調者無訊框可傳送且輪詢名單為空白的情況。

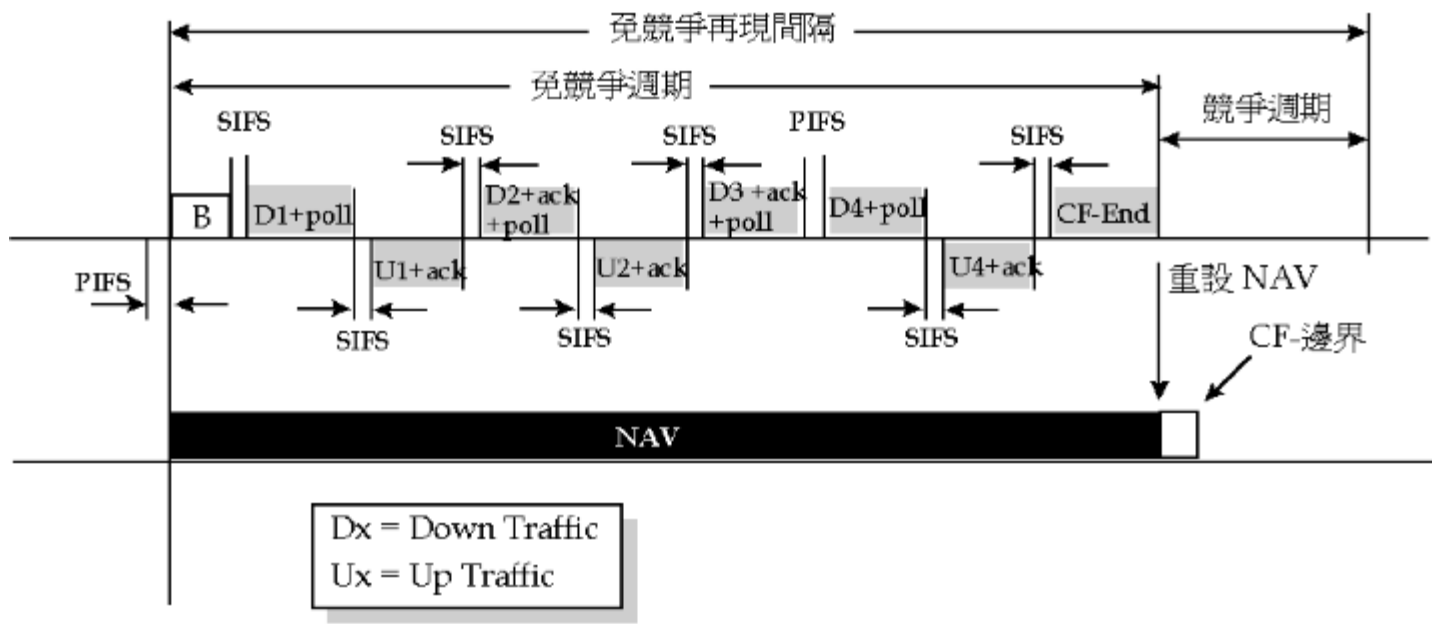


圖13-35 免競爭週期訊框傳送範例（協調者是傳送工作站或接收工作站）

協調者不是傳送工作站也不是接收工作站的情形發生在可輪詢工作站被輪詢時可傳送一個 **Data** 訊框或**Management** 訊框給同一個 **BSS** 中的任何一個工作站。此時 **Data** 訊框的接收與回覆方式必須採用**DCF**的規則，即目的地工作站必須在收到訊框後一個 **SIFS** 間隔回送一個**ACK**訊框。如圖13-36 所示，由於 **D1** 訊框攜帶輪詢訊息，因此 **D1** 訊框的接收工作站可以傳送一個 **Data** 訊框。圖中此工作站將 **Data** 訊框傳送給其他的工作站而不是傳給協調者。因此該目的地工作在收到訊框後一個 **SIFS** 間隔回送一個**ACK**訊框。值得注意的是，此 **Data** 訊框可以包含若干個片段 (**Fragments**)，此時每一個片段都必須有一個 **ACK** 訊框。協調者取回控制權的時機是在 **ACK** 訊框後的一個 **PIFS** 間隔。由於片段與 **ACK** 訊框間間隔等於一個 **SIFS**，因此協調者會在最後一個 **ACK** 訊框後的一個 **PIFS** 間隔取回控制權。另外即使此 **Data** 訊框的長度大於**aRTSThreshold**,在傳送前也不須使用**RTS/CTS** 控制訊框。這是因為在免競爭週期中所有工作站之**NAV**已事先設定，因此不須擔心訊框衝撞的問題。

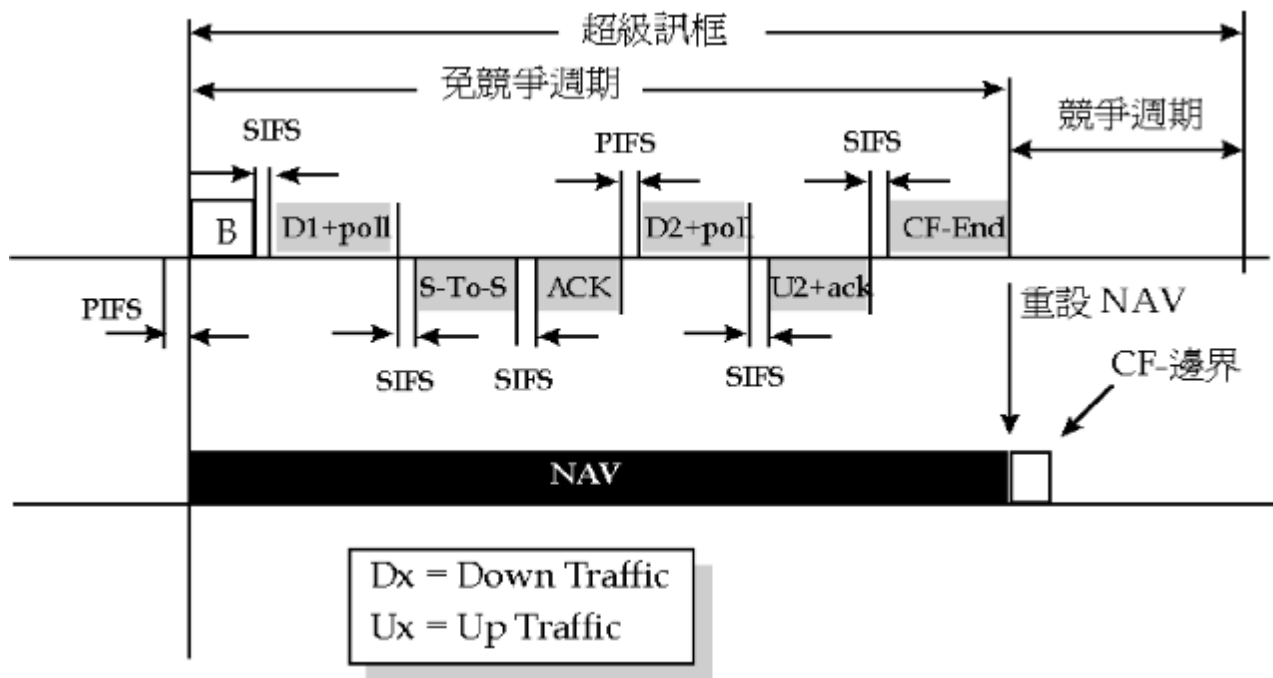


圖13-36 免競爭週期訊框傳送範例（協調者非傳送工作站或接收工作站）

輪詢名單之建立與維護

在免競爭週期中協調者是依靠輪詢名單來進行輪詢的任務。因此輪詢名單的建立與維護是相當重要的。前面已介紹過，工作站在開始通訊之前，必須先利用**Association** 控制訊框與協調者建立連結關係。在此訊框中工作站就可以表明是否加入輪詢名單中。加入輪詢名單當然可以有被輪詢傳送訊框的機會，但是不加入輪詢名單也有好處。例如有些較常處於省電模式的工作站在沒有訊框要傳送的時候不希望常常被輪詢而受到干擾。因為每次被輪詢到就必須由省電狀態被叫起來回答。而協調者如果有訊框要轉送給省電模式工作站，則只要在免競爭週期的開始階段將之叫起即可（這些省電模式工作站必須接收第一個 **Beacon** 訊框中的 **DTIM** 訊息）。給省電模式工作站的訊框通常在免競爭週期的前段先傳送。工作站加入輪詢名單後則可以利用**Reassociation** 控制訊框要求退出輪詢名單。不在輪詢名單內的工作站只能在競爭週期中以**DCF**的規則傳送訊框。

協調者根據輪詢名單輪詢時也有不同的做法。例如輪詢名單較長時可能必須經過幾個免競爭週期才能輪詢一遍。在一個免競爭週期中如果已完成輪詢一遍而尚有剩餘時間，則可以根據交通量分布情形或不同的服務品質要求挑幾個比較重要的工作站給於較多的傳送機會。當然協調者也可以提早結束免競爭週期。此部份相當於有一個排程演算法，至於協調者要採用哪一種排程演算法就不是標準的規範範圍了。

13.7.3 多重傳輸速率

有些實體層的技術具有支援多重傳輸速率 (**multiple rates**) 的功能。因此爲了能提高系統的效率，工作站有時也希望能以不同的速率來傳送訊框。例如傳送聲音時可能只需要 **64 kbps**，而傳送壓縮影像時可能就需要**1.5 Mbps**。如果一律使用 **2Mbps** 的頻道則在效率上反而不是最好。多重速率的好處就是工作站可以依情況隨時切換傳送速率。但是爲了讓具有多重傳輸速率能力的實體層間能共存及互通，**IEEE 802.11**標準於是制定了一些多重速率的設計及使用規範。首先 **aBSSBasicRateSet** 定義了基本傳輸速率的集合。而爲了讓所有的工作站都能順利接收控制訊框，所有的控制訊框 (**Control frames**) 都應該只用基本傳輸速率集合中的某一個速率來傳送。所有的廣播 (**Broadcast**) 或群播 (**Multicast**) 訊框也只能用基本傳輸速率集合中的某一個速率來傳送。各別訊框 (**Unicast**) 或管理訊框 (**Management**) 則可以使用速率切換法所選擇的速率來傳送。工作站傳送訊框給目的地工作站時，不能以該目的地工作站沒有支援的速率來傳送。而這些資訊可以在管理訊框中的速率支援元件 (**Supported Rates Elements**) 中取得。我們知道工作站在傳送 **RTS** 訊框或 **Data** 訊框時會帶有持續時間值，其值是預估工作站傳送一筆訊框及收到回覆訊框所需要的時間。而此時間的計算就和工作站所採用的傳輸速率有關。爲了避免實際所花的時間比原預估值還長（會影響其他工作站 **NAV** 值的正確性），目的地工作站回送 **CTS** 訊框 (**ACK** 訊框) 所採用的傳輸速率也應該和 **RTS** 訊框 (**Data** 訊框) 所採用的傳輸速率相同。

13.8 同步

爲了讓網路能正確運作，一個BSS中的所有工作站都應該同步 (**synchronized**)。所謂同步就是有一個相同的時序 (**clock**)。事實上，每一部工作站都有自己的時序，不過彼此間可能不完全相同，這會造成時間計算的誤差。例如當協調者傳送 **Beacon** 訊框時，工作站應該要在正確的時間接收，時序如果太慢就會來不及接收而發生錯誤。

IEEE 802.11 的做法是讓所有的工作站都配置一個「時序同步功能」計時器 (**Timing Synchronization Function Timer, TSF Timer**)。希望每部工作站內的 **TSF Timer** 值都能相同。在有基礎架構的網路環境下，擷取點爲時序的主控者，應該負責執行時序同步的功能。由於 **BSSs** 所涵蓋的範圍可以部份或全部重疊，因此各個BSS 的擷取點彼此之間應該不要同步，否則有可能在同一時間都送出**Beacon** 訊框，使得其所管轄的工作站在接收**Beacon** 訊框時造成衝撞的現象。擷取點爲了完成將其所管轄的工作站同步的任務，必須週期性的傳送攜帶其 **TSF Timer** 值的 **Beacon** 訊框。工作站本身的 **TSF Timer** 值如果與 **Beacon** 訊框上的不同，就應該修正爲相同。工作站 **TSF Timer** 的大小爲 **64** 位元，計數範圍最大爲 **2⁶⁴**（單位爲微秒）。

13.9 電源管理

工作站可以依其所需決定其電源管理模式是處於啓動模式 (**Active Mode**) 或省電模式 (**Power Save Mode, PS Mode**)。工作站更改模式時必須利用所傳送訊框中的訊框控制欄位 (**Frame Control Field**) 內的電源管理位元 (**Power Management bit**) 來通知協調者。協調者有訊框要送給省電模式工作站時，不可以隨時傳送，必須先將這些訊框儲存起來而在特定的時間傳送。至於有哪些工作站有訊框儲存在協調者中待送則是記錄在訊務指示對照表 (**Traffic Indication Map, TIM**) 中。協調者每次傳送 **Beacon** 訊框時都會將此對照表放入其中。處於省電模式的工作站應該定時的起來接收 **Beacon** 訊框（時間間隔由工作站內部之 **aListenInterval** 參數定義）。工作站取得 **TIM** 後可自行研判其是否有訊框儲存在協調者中。每一個與協調者建立連結關係的工作站都被分配一個工作站辨識碼 (**Station ID, SID**)。TIM 則是以虛擬位元對照表 (**Virtual Bitmap**) 的方式記錄工作站是否有訊框儲存在協調者中。例如第 **i** 個位元等於 **1** 表示 **SID_i** 有訊框儲存在協調者中。**SID₀** 則保留給廣播或群播訊框，第 **0** 個位元等於 **1** 表示有廣播或群播訊框儲存在協調者中。

處於省電模式的工作站可以是非輪詢工作站或可輪詢工作站。在 **PCF** 運作環境的競爭週期 (**Contention period**) 或 **DCF** 運作環境之下，處於省電模式的工作站（非輪詢或可輪詢）如果發現其有訊框儲存在協調者處，就會傳送一個短的 **PS-Poll** 訊框給協調者，協調者則會儘早將此訊框（一個**PS-Poll** 針對一筆訊框）傳送給工作站。此訊框中的**More data** 欄位會記錄是否還有訊框儲存於協調者處。如果有則工作站再次以 **PS-Poll** 訊框要回第二筆訊框，如此重複進行，直到協調者清光屬於該工作站的訊框爲止。這裡必須特別注意的是，工作站如果在 **TIM** 中發現還有其他工作站的訊框也同時儲存在協調者處時，則不能立刻傳送 **PS-Poll** 訊框。否則其他工作站也會做相同的動作，結果將造成 **PS-Poll** 訊框的衝撞。正確的做法是工作站隨機延後一段時間再傳送**PS-Poll** 訊框，以降低衝撞機率。此隨機延遲則平均分布於 **[0, aCWmin]**之間。送出 **PS-Poll** 訊框的工作站必須維持其啓動的狀態直到收到對應的訊框爲止，或收到另外的 **Beacon** 訊框而其中顯示其訊框已不在協調者處（可能已於免競爭週期中送出）。

協調者對於廣播或群播訊框的處理方式又有所不同。**BSS** 中只要有任何工作站處於省電模式，協調者就必須先將欲傳送之廣播或群播訊框儲存起來，直到在帶有 **DTIM** (**Delivery TIM**) 元件的 **Beacon** 訊框後面才傳送（一個免競爭週期中協調者可以傳送多個帶有 **DTIM** 元件的 **Beacon** 訊框）。這是因爲處於省電模式的工作站只會在特定適當的時間起來接收 **Beacon** 訊框，在 **Beacon** 訊框後傳送可以讓處於省電模式之工作站比較準確的規劃其接收廣播或群播訊框的時間。避免爲了接收不定時傳送之廣播或群播訊框而造成電源管理模式切換過於頻繁。

訊務指示對照表 (**TIM**) 又可分爲兩類：**TIM** 及 **DTIM**。協調者每次傳送 **Beacon** 訊框時都會放入訊務指示對照表。平常放的是**TIM**，不過每隔一個 **aDTIMPeriod**時間，就放入**DTIM**。協調者在 **DTIM** 後必須先傳送廣播或群播訊框才能傳送各別訊框。圖**13-37** 所示爲在**DCF**運作環境下，**TIM** 及 **DTIM** 的傳送範例。圖中假設每送兩次 **TIM** 後傳送一次 **DTIM**。也就是一個 **DTIM** 間隔等於三個 **Beacon** 訊框間隔。其中第一行代表時間軸，第二行是協調者的動作，第三及第四行分別代表處於省電模式工作站（假設分別爲**SID₁** 及 **SID₂**）之行爲。而 **SID₂** 又被設定爲超低功率狀態，以致於不醒來接收所有的 **DTIM** 元件。首先先說明協調者的動作。原先協調者會安排每隔一段 **Beacon** 訊框間隔 (**TBTT**) 就送一個 **Beacon** 訊框。但該時間可能有訊框尚在傳送，因此 **Beacon** 訊框可能會被延遲。假設第一個 **TIM** 沒有延遲，而且其中記錄協調者儲存有 **SID₁** 及 **SID₂** 的訊框。此時 **SID₁** 已醒來接收此 **TIM**，但 **SID₂** 尚未醒來。**SID₁** 於是傳送一個**PS-Poll**訊框給協調者，協調者於是將該筆訊框傳給 **SID₁**。**SID₂**的訊框則繼續儲存在協調者處。接下來的一個 **TIM**及**DTIM** 都受到一點延遲，不過其中只記錄協調者有儲存 **SID₂** 的訊框（尚未轉送）。但是**DTIM** 後則有傳送廣播或群播訊框。**SID₁** 收到了這些廣播訊框，但 **SID₂** 則因爲沒有醒來而沒有收到這些廣播訊框。**SID₂** 一直到第五個**Beacon** 訊框之前才醒來接收該 **TIM**，其中仍然記錄協調者儲存有**SID₂** 的訊框。**SID₂** 於是傳送一個**PS-Poll**訊框給協調者，協調者於是將該筆訊框傳給 **SID₂**。最後一個 **DTIM** 後面仍然有傳送廣播或群播訊框，不過由於只有 **SID₁** 醒來接收此 **DTIM**，因此只有 **SID₁** 收到了這些廣播訊框。由此例可知，處於省電模式的工作站要不要醒來，或在何時醒來接收**TIM** (**DTIM**) 是其本身的問題。如果每次都定期醒來接收**Beacon** 訊框，則不會漏掉任何其他工作站所傳來的訊框（包括廣播或群播訊框），不過模式切換頻率較高（較費電）。如果以省電爲優先考量，則可間隔較長的時間後才醒來接收**Beacon** 訊框。不過其他工作站所傳來的訊框可能會較晚收到（儲存在協調者處），而且可能會漏掉一些廣播或群播訊框。

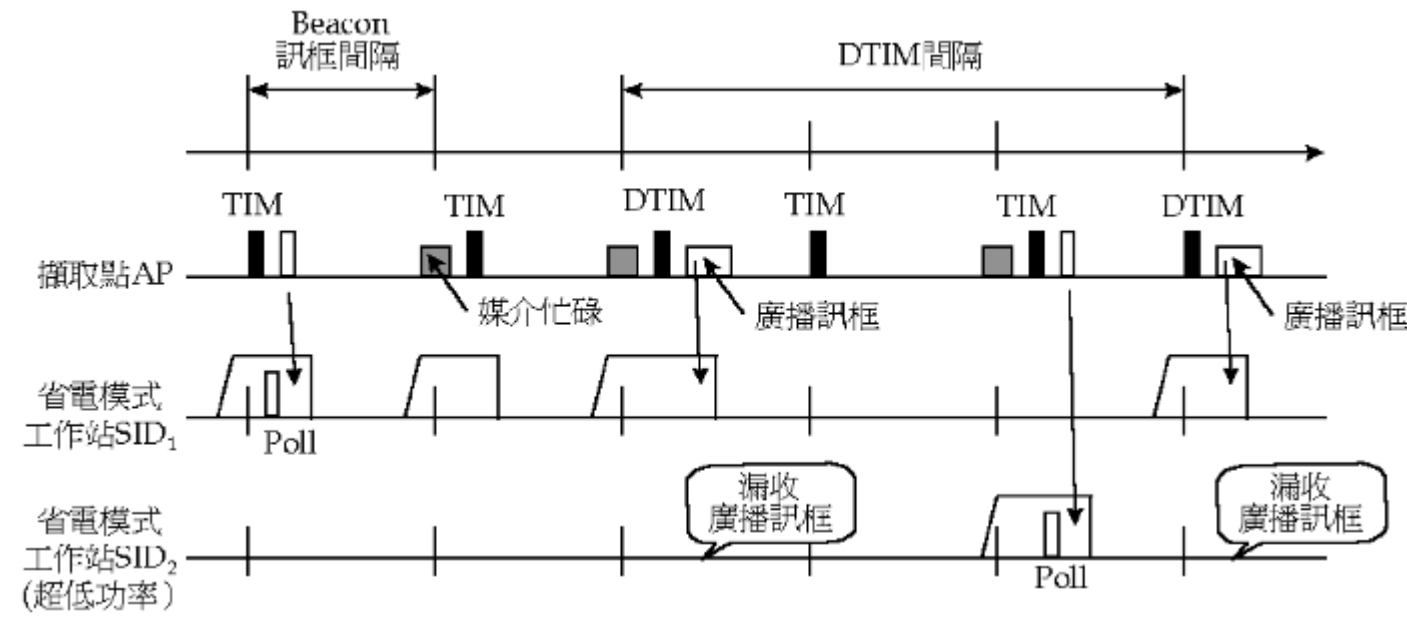


圖13-37 TIM 及 DTIM 的傳送範例（在DCF運作環境下）

習題

13.1 請說明無線網路與傳統的有線網路在特性上有何不同。

- 13.2 請說明 IEEE 802.11 無線網路的主要特性。
- 13.3 請說明有基礎架構 (Infrastructure) 的無線區域網路與無基礎架構 (Ad Hoc)的無線區域網路的差異性。
- 13.4 請說明下列服務的任務：

(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(Reassociation)
- 13.5 IEEE 802.11 訊框中包含 duration/ID 欄位，請說明此欄位在何種狀況下應當成持續時間(duration)，在何種狀況下應當成ID。其用法又如何？
- 13.6 請說明 IEEE 802.11 訊框中下列位址所代表的意義：

SA (Source Address)

DA (Destination Address)

RA (Receiver Address)

TA (Transmitter Address)
- 13.7 IEEE 802.11 訊框中最多可包含四個位址 (Address1-Address4)。請參考表13-4 說明這些位址的適用狀況。
- 13.8 Beacon 訊框攜帶許多網路運作的重要資訊。請說明下列資訊的意義為何：

Timestamp

Beacon Interval

Capability Information

SSID

Supported Rates

FH Parameter Set

DS Parameter Set

CF Parameter Set

IBSS Parameter Set

TIM (Traffic Indication Map)
- 13.9 協調者(Point Coordinator) 利用 TIM 元件來通知所有工作站其儲存訊框的情形。

請說明 TIM 的格式及各欄位的使用方法。

假設協調者只儲存工作站 196, 202 及210 的訊框, 則其Partial Virtual Bitmap 內容為何？N1 及 N2 值又各為何？

假設協調者儲存工作站 198, 203, 210, 及216 的訊框, 則其Partial Virtual Bitmap 內容為何？N1 及 N2 值又各為何？
- 13.10 請說明以下IEEE 802.11 所採用的認證方法及認證過程：

開放系統式認證 (Open System)

共享密匙式認證 (Shared Key)
- 13.11 請說明 IEEE 802.11 採用之有線等效保密演算法 (Wired Equivalent Privacy, WEP) 的加密過程。其中使用初始向量 (Initialization Vector, IV) 及完整檢查碼 (Integrity Check Value, ICV) 的目的為何？
- 13.12 請說明 IEEE 802.11 採用之有線等效保密演算法 (WEP) 的解密過程。接收端如何判斷資料有無被竊聽者竄改？

13.13 分散式協調功能 (Distributed Coordination Function, DCF) 是IEEE 802.11 MAC 最基本的擷取方法。請參考圖13-21 說明其運作方式。

13.14 請說明 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 通訊協定的運作原理。其與 CSMA/CD 有何異同？

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) 通訊協定號稱可避免訊框傳送衝撞，但是仍然會造成衝撞。為什麼？

何謂「訊框間隔」(Inter-Frame Space, IFS)？請說明下列訊框間隔的意義及使用時機。

(a) SIFS (Short IFS)

(b) PIFS (PCF IFS)

DIFS (DCF IFS)

EIFS (Extended IFS)

13.17 請說明 **IEEE 802.11 CSMA/CA** 通訊協定中何時需使用到「要求傳送」控制訊框 (**Request to Send, RTS**) 及「允許傳送」控制訊框 (**Clear to Send, CTS**)。為什麼？

13.18 何謂「虛擬載波偵測」法？為什麼 **IEEE 802.11** 通訊協定需使用虛擬載波偵測法？

13.19 何謂「網路配置向量」(**Net Allocation Vector, NAV**)？使用網路配置向量的目的為何？工作站如何設定及維護其網路配置向量值？

13.20 在 **CSMA/CA** 通訊協定中為了減少衝撞的機率，工作站必須產生後退時間 (**backoff time**)。請說明工作站如何產生後退時間的初始值。其中競爭視窗 (**Contention Window, CW**) 的值又如何選擇？

13.21 以圖**13-30(a)** 為例。假設工作站 **B**、**C**、**D** 在等待了一個 **DIFS** 時間後，產生的隨機後退時間分別為 **8us**, **10us**, 及**16us**。請依照圖**13-30(a)** 畫出工作站傳送訊框的順序。

13.22 以圖**13-30(b)** 為例。假設工作站 **B**、**C**、**D**、**E** 在等待了一個 **DIFS** 時間後，產生的隨機後退時間分別為 **8us**, **15us**, **20us** 及 **7us**。請依照圖**13-30(b)** 畫出工作站傳送訊框的可能順序。

13.23 以圖**13-30(c)** 為例。假設工作站 **B**、**C**、**D**、**E** 在等待了一個 **DIFS** 時間後，產生的隨機後退時間分別為 **8us**, **15us**, **8us** 及 **20us**。又假設工作站 **B**、**D** 在衝撞後產生的隨機後退時間分別為 **12us** 及 **15us**。請依照圖**13-30(c)** 畫出工作站傳送訊框的可能順序。

13.24 何謂「超級訊框」(**Superframe**)？其架構為何？

13.25 請說明免競爭週期 (**Contention Free Period, CFP**) 的結構。協調者如何開啓一個免競爭週期？又如何結束免競爭週期？

13.26 請說明協調者如何將其所儲存的訊框傳送給工作站？又如何傳送廣播及群播訊框給工作站？

13.27 PCF 傳送訊框的運作模式可以分為兩種：**(1)** 當協調者是傳送工作站或接收工作站時，**(2)** 當協調者不是傳送工作站也不是接收工作站時。請說明此兩種模式的運作情形。

13.28 請說明協調者如何建立及維護輪詢名單 (**Polling list**)？工作站可分為可輪詢工作站 (**CF-Pollable**) 及非輪詢工作站 (**Non-CF-Pollable**)。後者永遠不會出現在輪詢名單中。請說明協調者如何將訊框傳送給非輪詢工作站？

13.29 請說明 **IEEE 802.11** 如何支援多重傳輸速率 (**Multiple Rates**)？為了達到多重傳輸速率環境，工作在實體層（收發器）的要求為何？

13.30 工作站可以處於啟動模式 (**Active Mode**) 或省電模式 (**Power Save Mode**)。請說明處於省電模式的工作站如何接收訊框？

13.31 請說明 **PCF** 如何提供具時限性 (**Time-bounded**) 的傳送服務。工作站應如何要求此類服務？協調者又如何能給於服務品質 (**Quality of Service, QoS**) 的保證呢？