考試目錄

1. 介紹

- Why wireless

- types of wireless

- types of transmission Mediums

- types of transmission Signal

- Broadband Wireless Technology

- Limitations and Difficulties of Wireless Technologies

1. MAC層

- Why MAC

- Sollution Desigin Choices

- Constraint

- Performance Metrics

- Base Technologies (FDMA,TDMA,CDMA) (接入技術)

- FDD and TDD (雙工技術)

-Classification of Multiple-Access Schemes

- Classification of MAS

- CSMA

- CSMA/CD

- CSMA/CA

- Hidden Terminal and Exposed Terminal Problems

- RTS/CTS

1. Wireless LAN

- Different Wired & Wireless

- Mobile vs Wireless

- IEEE 802 （無綫標準）

- Spread Spectrum Modulation ()

- 解決信號在頻率傳輸過程中的各種問題

- Wireless NICs

-AP

- Basic Service Set (BSS)

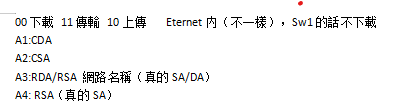
- IBSS,ESS,SSID

-DS

- Probing Phase

- Association & Reassociation

- 802.11 Authentication Methods

- WEP Encapsulation & Decapsulation

- WPA & WPA2

- 802.1X

- 802.11 Key Management

考試要點

**Chap 1**

- Cellular Network蜂巢網路，它是一種無綫通信網路架構，通過將覆蓋區域劃分成多個小區cells來實現可以覆蓋更大範圍的無綫通信。每一個cell都有一個基站base station提供無綫信號的覆蓋，然後這些base station也通過分佈式連接用戶，最後形成網路。

**Types of Wireless Systems**

1. Wireless PANs (WPANs) 無綫個人網路

例如：bluetooth

1. Wireless Lans (WLANs) 無綫區域網路

覆蓋範圍取決於Access Point的數量和信號强度

例如：居家，辦公室，或學校有區域網名的無綫網路

通常都是路由器通過AP點連接到有綫網路，然後把有綫網路轉換為無綫網路，再透過路由器發送出去

1. Wireless Wans (WWANs) 無綫廣域網路

通過Cellular Network分佈的無綫訊號，允許設備在大範圍移動中，都能保持連接

比如data(4G/5G)

1. Un-infrastructure Wireless Network 無基礎設施無綫網路

應用場景：災難救援，軍事通信，車載網路等

- WLAN 可以訪問 WWAN 上的數據：當您連接到 Wi-Fi 時，您可以訪問互聯網上的資源，這些資源可能位於 WWAN 或更廣泛的網絡範圍內。

- WWAN 無法直接訪問 WLAN 的數據：WWAN（如手機數據）無法直接訪問局域網中的設備或數據，除非設置了專門的遠程訪問服務。

**Types of Transmission Mediums**

- Radio (無線電廣播)

- Narrowband Microwave（窄頻微波）

- WLAN（無綫區域網路）

- Bluetooth（藍牙）

- GSM（Global System for Mobile Communications）

- Optical（光學通信）

- Infrared（紅外綫）

- Laser（鐳射）

不同的無綫通信技術都有各自不同的應用場景，並根據傳輸範圍，性能要求，傳輸速度，成本及環境來使用不用的使用。

**Types of Transmission Signal**

**Analog modulation**

AM：適用於大範圍傳播，需要頻寬較小，有連續變化的特性

FM：更寬的頻寬，在信號質量和抗干擾能力更强，用於高品質音頻傳輸。

共同特性：具有連續變化的特性，比Digital Modulation更少的頻寬，需要接收端來負責對接並對信號進行調整重構恢復原始訊號。

**Digital modulation**

特性：使用1和0來表示信號，對於重構還原信號上更簡單，但數位傳輸所需要的電路更複雜。

**Broadband wireless technology**

獲得更高的數據速率，廣汎用於圖形，視訊及音訊等 （高帶寬，高速，大範圍，低延遲）

- share some advantages of all wireless services:方便及低成本，無線基站的建設更快，因爲是無綫的所以無需cable plant的成本，然後服務是可移動性的，可以在任何地方部署

**Wireless technologies的優勢和限制**

- wireless is convenient and less expensive（優）

- Limitaions of political and technical difficulities（限）

- Lack of an industry-wide standard（限）缺乏統一標準

- Device limitations（限）

比如：在手機上無法像電腦上顯示大篇文章内容·，因此在手機上常常使用的是輕量化的WML語言，而不是HTML。

**Chap2 MAC（Media Access Control）**

因爲早期的設備都是共享無綫頻譜的，然後一個頻譜同時只有一個設備能夠使用。因此帶來了一個問題:當多設備同時發送數據時候，會出現干擾和信息碰撞，導致失敗。因此MAC因而產生。MAC層主要是減少或避免這些衝突，保證個設備閒可以有效穩定地傳輸。

**Goal:**

- maximize message throughput 最大化吞吐量

-minimize mean waiting time最小化等待時間

**Solution：**

- 在time domain/frequency domain , to 隔離isolate traffic from different stations

- 選擇如何allocate a limited number of transmission resources 給更多的競爭用戶

**Distributed design:**

- Centralized vs Distributed

Centralized:會有一個master station，其他都是slaves station

Distributed:所有station都是對等的peers

**- Circuit Mode vs Packet Mode**

Circuit Mode: 用於連續，穩定的數據流傳輸(steady streams) ：音頻，視頻等，因此不需要為每個封包競爭資源，因爲如果每次都爭取傳輸資源，反而會造成延遲浪費，降低連續傳輸效率。

Packet Mode: 將數據拆分成一個個封包，每個封包可以獨立送到des，然後再組合(bursts of packet)：網頁游覽，電子郵件。由於是拆成一個個packet去發送，所以可以在傳輸前，要被使用到前才爭取頻寬，這樣就能最大化地使用到頻寬，並動態分配傳輸資源。

**Constraint: Spectrum Scarcity頻譜稀缺性**

1. 有限的無綫頻譜資源

因為無綫頻譜是有限的資源，，然後可以供通信的頻率範圍是有限的，不同的通信技術都需要不同的頻段來避免互相干擾。因此解決頻譜稀缺性是無綫通信系統中的根本問題。

1. 長距離通信頻率有限

尤其是在長距離通信中，一般需要更低的頻率範圍來保持信號强度。可是這些頻段經常被其他通信技術占用，也因此剩餘的可使用頻譜更有限。

1. 更高效的多重接入技術

因此需要不同的接入技術來保證各個設備能夠在不被干擾的情況下，共享有限的頻譜資源。

不僅要解決分配有限的頻譜，還要減少碰撞，干擾，及最大化每一單位的頻寬使用效率。這樣就可以滿足更多用戶使用。

**Constraint: Radio Link Properties無綫鏈路特性限制**

在傳輸過程中，因無綫傳輸媒介的特殊，而受到的多種限制。會影響穩定，準確及效率。

1. Error-Prone Links 錯誤率高

在無綫傳輸中更容易收到外界因素的干擾，導致信號衰弱。影響可靠性

1. Fading 衰弱

隨距離，時間，環境導致信號減弱現象。導致信號强度不足，影響傳輸質量和穩定性

1. Multipath 多重干擾

由不同路徑（反射，折射）到底接收端時，會導致信號重叠或干擾。多路徑干擾可能會造成信號失真。使得數據解讀變得苦難，降低通信系統的準確性。

1. Interference 干擾

在傳輸時，也會受到其他信號（非通信：微波爐 /通信）的干擾。

1. Hidden Terminal Problem 隱藏節點問題

當兩個無法彼此偵測到，互相聽見的發送端，同時向同一接收端發送數據。由於無法感知彼此的存在，因此信號會在接受端發生碰撞。

1. Capture Effect 捕捉效應

當上面的情況發生時候，接收端往往只會抓取功率高的信號，而忽略功率低的信號。因此功率低的設備可能會一直無法成功傳輸數據。

**Parameter ‘a’**

描述了一個source傳輸數據包時，從最遠端的station接收到該數據的第一位之前，source所發送的數據包數量。

a值越大，網路延遲越高,數據傳輸速率越低 ;

a值越小，網路延遲越低，數據傳輸速率越快

a = d / T

d：網路延遲（propagation delay） T：傳輸時間（one packet）

**Performance Metric: Normalized Throughput （效能指標）**

衡量網路效能的指標，用於評估實際有效的數據傳輸率(Goodput)。也可以理解為傳輸不需要重傳的有效數據比例。

Normalized Throughput = Goodput/Link Capacity

Goodput：有效數據傳輸速率 ； Link Capacity：鏈路理論的最高容量/最大速率。

**Performance Metric: Stability 穩定性**

當網路負載很重時，網路的許多時間都會用來解決競爭問題。

競爭問題：當多設備試圖使用共享的通信媒介，會導致數據碰撞，進而需要進行重傳。

如果競爭解決方法不夠高效，網路會變得不穩定。

穩定的算法可以在負載大時，仍能保持穩定的吞吐量，而吞吐量不會隨著負載增加而顯著下降。

因此要在重負載的情況下保持網路穩定，source需要在檢測到過載時，減少負載。這樣就可以保持穩定性。

**Performance Metrics: Mean Delay & Fairness 平均延遲 & 公平性**

評估網路在不同負載和使用情況下的表現。

Mean Delay

- 一個設備成功發送一個數據包之前，必須等待的時間 waiting time，反映了設備等待傳輸的長短。 負載越高，站點直接的競爭越激烈，waiting time就越長。

- 傳輸媒介的特性（有較多干擾/較低帶頻率）會影響數據的傳輸速度，和等待時間。

Fairness

- 衡量網路多個station是否能均等獲得資源，確保沒有station因爲過度競爭，資源不均而長時間無法傳輸數據。

No Starvation ：指即使網路繁忙，每個source都有一樣的機會發送數據

No single definiton：不同場景和需求會有不同的公平性定義。每個應用注重的功能不同。

**Base Technologies**

Isolates data from diferent sources，解決多用戶在同一通信媒體上共享資源的問題

**FDMA（Frequency division multiple access）頻分多址**

將可用的頻譜分成多個頻率通道，再分配給用戶，用戶在特定的比率上傳資料，互不干擾

1. 每個station分配有一個獨立的頻率帶寬

每個用戶會被分配一個特定的頻率範圍來傳輸數據，頻段之間會有保護帶(guard band)，用來防止相鄰頻段之間的干擾。

1. 接收器調整至正確頻率

每個接受器根據分配給它的頻段進行調配，來接受正確的信號。

1. 頻率資源有限
2. 降低發射功率

爲了避免過度干擾和提高效率，會降低發射頻率，以減少信號的範圍

1. 頻率重用

爲了最大化頻率資源的利用，相鄰小區中的用戶不能使用相同的頻率，以避免干擾。但是可以在非相鄰的小區中重用。

-（優）都有自己的頻率，互不干擾，實現方式簡單

-（缺）利用效率低，會出現空閑的頻道無人使用

**TDMA（Time division multiple access）時分多址**

將時間劃分多個時隙,在同一個時間上只有一個用戶在傳輸數據,因此不同的用戶就可以在相同的頻率上傳輸數據。

1. 時間分割

所以station共用一個頻率，但在不同時間段傳輸數據。雖然傳輸時間是間隔的，但是可以共享同個頻率

1. 時間同步

需要對所有station進行時間同步，確保每個station在正確的時間段内傳輸數據。意味著每個station都必須知道何時開始和結束傳輸。

-（優）提高頻譜利用率，多個用戶可以共享同一頻率，數字通信實現更會容易，尤其適合同步數據通信。

-（缺）需要嚴格的時間同步，否則會導致用戶閒數據重叠。當用戶增加時，時延會增加。同部開銷

**CDMA（Code division multiple access）**

使用擴頻技術，允許多個用戶在同時同一頻率上進行通信。每個用戶的數據都通過一個唯一的擴頻碼進行編碼，接收端通過這個碼來區分不同用戶的信號。

-（優）頻譜利用率高，所有用戶都可以同時使用全部頻譜。用戶的增加不會導致明顯的干擾增加，系統容量可以更靈活擴展。抗干擾能力強，能有效抵抗多徑衰落和其他信號干擾。

-（缺）編碼解碼過程複雜，實現難度較大。隨著用戶增加，系統性能會下降。

**FDD vs TDD**

- 在共享的無線頻譜上實現雙向通信，用於解決雙向通信中（上行鏈路）上傳和（下行鏈路）下載直接的數據傳輸問題。它們決定了如何分配頻譜資源給上行和下行傳輸。可以與FDMA/TDMA做結合。

**FDD (Frequency Division Duplex) - 頻分雙工**

- 使用兩個不同的頻率通道來同時進行上行和下行傳輸，可以同一時間使用，因此可以在同一時間進行雙向通信

-（優）同時雙向通信，低延遲

-（缺）頻譜利用不靈活，需要更寬的頻譜，因爲FDD需要兩個獨立的頻率範圍，這對頻譜資源要求較高。

**TDD (Time Division Duplex) - 時分雙工**

- 使用同個頻率通道，但將時間劃分多個時隙再分配給上行下行傳輸。在不同時間點，上行下行之間交替使用頻率。

-（優）頻譜利用靈活，頻譜效率高

-（缺）延遲稍高，會出現一定的延遲，時間同步要求高。

**Classification of Multiple-Access Schemes**



**Centralized Access Schemes 集中式存取方案**

會有一個主站(master)負責管理所有從站(slave)通信，從站(slave)只有在主站允許的情況下才能進行傳輸。

1. 主站是所有設備的控制中心，從站只能在主站的指導下進行通信。使得通信管理變得更加有序。
2. 主站能夠發佈指令，決定何時允許從站進行傳輸，可以有效避免設備閒的碰撞。
3. 適合一個權威或集中管理的環境，尤其在無綫通信中，主站的範圍通常涵蓋了所有從站。

wireless LAN：where base station is the only station that can see everyone

cellular telephony：where base station is the only one capable of high transmit power

-（優）管理簡單，避免碰撞，高效能（master擁有較高的傳輸功率，能夠覆蓋大範圍）

-（缺）單點故障（master出現問題，整個系統都會受影響），依賴主站能力

**Centralized Circuit-Mode Access Schemes 集中式電路模式存取方案**

通常用於需要確保穩定，持續傳輸的情況，且是主從系統。

當slave傳輸數據時，會發送請求信息給master。master收到親求后，分配適當的資源給slave。并且在數據傳輸過程中，slave能夠使用這些resources,直到數據傳輸完成。避免了數據傳輸過程中的競爭。提供穩定的通信質量

- 無競爭的數據傳輸

- 適用與穩定，持續數據流的應用

- 資源分配（在slave發數據前，master要分配一定的傳輸resources給slave使用）

**Centralized Packet-Mode Access Scheme: Polling輪詢**

master會按照順序詢問每個slave是否有數據傳送。

1. 輪詢機制：master會逐一詢問slave，檢查它們是否有數據要發送，slave會在輪到自己時向master回報，如果有數據要發送，就開始傳送，如果沒有，就等待下一輪。
2. 無競爭：由於是master控制各個slave的傳輸時機，slave就不需要競爭資源，可以避免碰撞和資源爭用，減少重傳的需求，提高數據的傳輸效率。
3. 簡單易實現：這種存取方式的控制邏輯相對簡單，適合部署在需要中央控制的系統

-（缺）效率低下（系統中只有少數站點活躍的時候，大部分slave長時間都不發送數據，但是master還是會繼續polling，因此會帶來很大的開銷，另外每一輪Polling后都要等待下一輪才輪到自己，會造成延遲

**Centralized Packet-Mode Access Scheme: Probing探測**

master通過對slave進行探測來檢查哪些slave需要發送數據，

1. 站點編號：所有station都會被allocate一個連續的logical addresses。這些addr可以幫助系統在探測時能夠更有效地辨識並選擇活躍站點。
2. 多播地址：every station都能接受到自己地址的信息，并且接收到的是一組多播地址信息。意味著station能夠同時監聽多個地址，而不僅僅是自己專屬的地址
3. 二分查找：master通過使用binary search來定位下一個活躍station。加快搜尋速度。

**Centralized Packet-mode Access:Reservation-Based Schemes基於預約的方案**

Master負責協調鏈接上所有的訪問，使用預約機制來分配傳輸時段：

1. 預約時段：一部分時間槽專門用於預約消息（而不是數據傳輸），這些時段被稱爲預約槽(reservation slots)，再根據需求分配給slave。
2. 迷你槽(minislots)：預約槽比實際的數據槽小，稱爲迷你槽。slave可以在minislots内競爭，或是master直接分配給slave.
3. 競爭機制：slave在minislot競爭，並向master請求預約。master會在所有response中選擇(贏家)並授權其進行數據傳輸。這樣，在數據傳輸時段就不會出現競爭，減少collide。
4. 降低開銷：只在minislots中競爭，所以即使出現數據碰撞，影響的也只是minislots而已，降低了因爭奪數據槽導致的開銷。

**Distributed Schemes分佈式方案**

1. 可靠性更高：沒有單一的中央控制節點，故障風險降低。
2. 消息延遲較低：節點之間可以直接通信，不需要等待master來下指令
3. 允許更高的網路利用率：分佈式方案下的節點能更靈活地根據當前需求進行數據傳輸，無需依賴master，提高頻譜資源利用率，和整體吞吐量
4. 更爲複雜：由於缺乏master管理，節點閒需要協調訪問頻道的方式更爲複雜。需要更高要求以及更複雜的算法設計。

Almost all distributed schemes are packet mode (why?)

- 幾乎所有分佈式方案都采用packet-mode，因爲packet-mode適合在頻繁競爭和傳輸不穩定的環境下使用。

- 在packet-mode下發生的碰撞開銷較低，發生碰撞后，只需要重新發送衝突的分組，而不是全部重發。

- 適合處理不連續的數據傳輸請求，使得分佈式方案更爲靈活。

**Decentralized Polling去中心化輪詢**

與集中式輪詢類似，只有（系統沒有master）不同。

1. 無master協調管理：系統中的每個節點都分配到自己的時隙，當輪到該時隙時，節點就可以進行傳輸。
2. 資源浪費：當一個節點在它的時隙中沒有數據要發送。則該時隙會被浪費掉，在負載較低時，導致頻譜資源利用率下降。
3. 時間同步要求：去中心化輪詢要求所有節點具有共同的時間基準。即每個節點必須精確地知道時隙的開始與結束，以便避免干擾，確保數據傳輸的有序性。

**Decentralized Probing去中心化探測**

也稱爲樹形多重接入，不依賴master進行協調。該方法base on binary tree structure進行節點探測和數據傳輸管理。

1. 樹形結構：每個節點分配一個樹形邏輯地址。網路按照這個邏輯對binary tree進行探測。通過binary search來尋找活躍節點，逐步縮小範圍來定位需要傳輸的節點。
2. 無主節點：每個節點都可根據探測結果來自行決定是否發送數據
3. 活躍節點負載問題：當活躍節點數量增多或所有活躍節點集中在一個subtree時，系統性能會顯著地下降。因爲探測過程會在同一範圍内多次執行，導致探測延遲增加。

先把所有地址0\*\*開頭的節點都進行傳輸，如果發生碰撞，代表裏面有超過1個活躍節點，然後數根據階段往下走，對00\*内的節點重複動作，然後逐步將地址細分直到找到具體節點。

**Carrier Sense Multiple Access(CSMA)**

是一種通訊協議，用於讓多個節點共用一條傳輸介質，避免傳輸時的碰撞問題。它核心概念是[載波感測]（Carrier Sensing）。在傳輸數據前，節點會先檢查該介質是否正被使用。如果檢測到是空閑的，則該節點進行傳輸。

1. 載波感測(Carrier Sensing)
2. 無需等待輪詢或排隊：不像polling 和probing需要等待master允許，或在時間表輪到自己時才動作，CSMA的節點只需要在介質空閑時就能立即傳輸
3. 碰撞檢測與解決：如果傳輸期間發生collide,系統會檢測並執行解決機制。例如隨機等待一段時間再重新嘗試傳送。從而減少重複碰撞的可能。
4. 使用與parameter ’a’較小的情況：如果延遲較小，CSMA的性能會更好，因爲節點能迅速地檢測到是否有其他節點正在使用該介質，從而避免頻率的碰撞。

**Simplest CSMA Scheme**

目標是盡量減少碰撞並提高傳輸效率。

操作流程：

1. 立即傳送：當檢測到傳輸介質空閑時，理解傳送一個packet
2. 等待空間后傳輸：當檢測到傳輸介質busy時，會有兩種等待策略：
   1. Persistent持續等待：節點會被持續檢查傳輸介質，並檢測到idle時立即傳送。但有一個問題
   2. Non-persistent非持續等待：節點不會一直等待，而是設計一個計時器。隨機等待一個時間再回來檢測狀態。雖然會導致一些等待延遲，但可以減少同時發送而引起碰撞。
3. Persistent的缺點：如果有兩個節點都在等待idle，則會在idle瞬間，兩者同時發送，產生碰撞。

**Reducing Collision Probability: P-Persistent CSMA**

減少CSMA碰撞機率，通過在idle時以一定的概率發送packet，避免傳輸過程的碰撞。

在傳統的CSMA中，一旦idle出現，等待的節點就會立即發送packet，因此容易出現多個節點同時發送，導致碰撞。而P-persistent讓等待的節點在介質idle時，不是立即發送，而是根據概率p來決定是否發送packet。

p是發送packet的幾率：當medium idle時，每個節點都有p的幾率發送packet，剩餘的1-p機率則讓它等待下次嘗試。

如何選擇p:

p小：那麽節點發送packet的機會就少，可以降低碰撞機率，但是會浪費很多idle的時間。

p大：更多機會在medium idle時發送packet，減少idle時間的浪費，但是增加碰撞機率。

**Handling the Collision Problem: Exponential Backoff**

指數退避(Exponential Backoff) 是CSMA/CD中解決碰撞問題的一個重要機制。

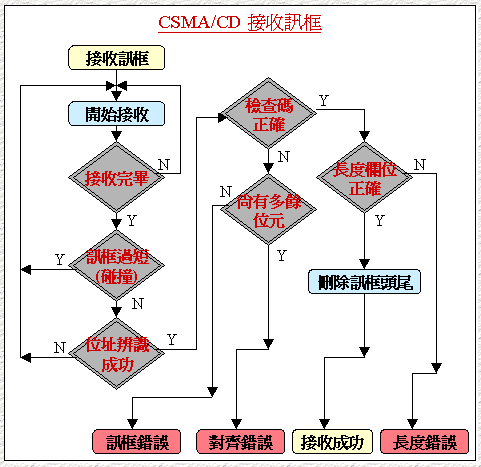
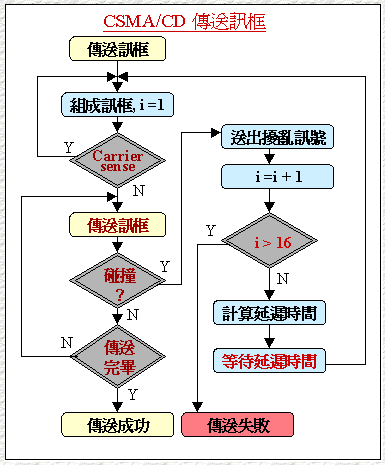
1. 傳輸與碰撞偵測：在CSMA的運作方式下，station同時監聽是否會發生碰撞，監聽其他station有沒有同時發送1資料，如果有，參與碰撞的station則會停止傳輸
2. 指數退避機制：當發生碰撞時，參與碰撞的station不會立即嘗試傳送資料，而是使用Backoff Algorithm.s隨機選擇一個時間等待再傳送，然後Backoff的時間範圍會在每次碰撞后加倍。EXP：（第一次碰撞：0-1個時間槽；第二次碰撞：0-3個時間槽；第三次碰撞：0-8個時間槽）
3. 適應競爭站點數量：隨著競爭的station越來越多，Backoff的範圍會根據競爭情況自動調整
4. 無需選擇概率p：與p-persistent CSMA不同，不用station選擇傳輸的概率p。Backoff time是根據碰撞自動決定的。
5. 碰撞偵測電路：CSMA/CD需要在傳輸的station中配置碰撞偵測電路，以便在發生碰撞時，station會自動停止並進入backoff。

**CSMA/CD Transmit Algorithm in Ethernet 载波监听多路访问碰撞检测**

是Ethernet中用於處理數據傳輸和衝突的一種算法。通過監聽信道來避免衝突，在發生衝突時，通過Backoff來減少網絡擁堵，提高數據傳輸效率和穩定性。

1. 如果綫路空閑時：
   1. 設備會立即發送數據包
   2. Ethernet的消息大小有上限，通常為1500字節
   3. 在連續發送多個幀時，需要等待9.6微秒(us)最小時間間隔。以避免幀之間衝突。
2. 如果綫路忙碌時：
   1. 設備會監聽綫路，直到綫路空閑
   2. 一旦綫路空閑，就是立即發送數據(Persistent Sending持續發送)
3. 如果發生衝突(Collision時)：
   1. 一旦檢測到衝突，設備會立即停止發送數據
   2. 發送一個32bit的jam sequence信號（信號擾亂傳輸過程，通知其他設備發生了衝突）
   3. 然後設備停止當前數據傳輸，開始執行Backoff Algortihm。

**-** 冲突检测 是通过监听线路是否有其他设备同时发送数据来实现的。



**注意：**

1. Frame cannot be too short

- 因爲CSMA/CD依賴于發送設備在傳輸數據的同時，也能檢測是否發生衝突。如果幀太過短，發送數據在設備檢測衝突之前已經發送完畢，設備就會無法及時察覺衝突，從而無法采取行動。

- 因此Ethernet規定了幀的最小字節為64bit.

- 避免短幀的碰撞盲點：如果帧太短，发生碰撞时，接收方和发送方可能都没有意识到有冲突发生，因为在发送方完成发送之前，碰撞信号可能尚未返回

**CSMA/CA (Collision Avoidance)碰撞避免的载波监听多路访问**

是一種用於無綫局域網(WLAN)的協議。用於控制多個設備共享一個通信信道。主要用於無綫網路，因爲無綫網路無法進行碰撞檢測，因此無法使用CSMA/CD

1. 發射器信號强於接收器：由於發送方無法聽到自己發送的數據（信號强過接收端），因此無法檢測碰撞。
2. 隱藏終端問題：當兩個設備距離較遠或有障礙物時，他們可能無法聽到彼此的信號，從而導致它們在同一時間發送數據，產生未檢測的碰撞。

**CSMA/CA Algorithm**

1. 檢查信道是否繁忙：發送數據前，檢查信道是否空閑，如被占用,則等待medium至空閑。
2. 等待信道變空閑：設備會監聽信道，等到信道變idle
3. 等待幀間隔Interframe Spacing：一旦medium idle后，再等待一個interframe spacing，有助於避免medium 忙碌后，立即發送數據的衝突。
4. 設置爭用計時器(Contential Timer)：當interframe spacing結束后，設備會隨機選擇一個時間間隔設置Contential Timer.它決定了等待的最大時間。初始時，CW（Contention Window競爭窗口）是一個固定的值，之後再發生衝突后，CW會增加。 range[1,CW]
5. 發送數據並等待確認(ACK)：當Timer到期後，設備才會開始發送數據，發送方會等待receiver的ACK，確認數據包已經成功傳輸。如果在規定時間内未收到，則sender會認爲數據丟失，並準備重新發送。
6. 處理碰撞：重試和Backoff：在發送數據時發送碰撞，執行Backoff（sender會根據碰撞次數，成倍地增加CW）。
7. 信道busy時，凍結和解凍競爭窗口CW：如果設備在還在等待Timer的時候，其他設備同時發送數據，那麽設備就會暫停Timer，並凍結CW。直到其他設備完成傳輸才開始繼續計時。

**Hidden terminal Problems**

- some stations in an area cannot hear transmissions from others, though base can hear both

例：站A和站B無法檢測到彼此的信號，但是都能監測站C的信號。當他們同時向站C發送信號時就會發生碰撞。

**Exposed terminal problems**

- some (but not all) stations can hear transmissions from stations not in the local area

例：站A與站B通信，站B也聽到站A的信號，但是站B錯誤認爲它不能向站C發送數據，因此它會等待，導致效率降低。

**Solution (Hidden Terminal Problem)**

Hidden terminal問題只會出現在無綫環境中，在有綫中不存在這個問題，因爲有綫信號可以直接在所有設備之間傳輸。

Virtual Carrier Sensing：sender會在發送數據前，先發送一個RTS/CTS，詢問receiver是否還有接收到其他設備的信號。如果有，那麽它會回傳一個’busy’的信號，通知sender。

EXP:

A and C want to send to B

A send RTS to B

B send CTS to A

C “overhears” CTS from B

C wats for duration of A’s transmission

**RTS（Request To Send）**

**-** sender發送給receiver詢問

**CTS（Clear To Send）**

- Receiver接收到sender的RTS后，可以發送CTS給sender告知，sender才可以傳送。

**BTMA（Busy Tone Multiple Access）:**

用於管理多個用戶在通道上傳輸的技術，當通道繁忙時，系統發送忙音信號。

**MACA（Multiple Access with Collision Avoidance）:**

一種避免碰撞的多路訪問技術，通常用於無線網絡中。

**ALOHA:**

一種簡單的接入協議，用於隨機訪問通道。用戶隨時可以發送數據，但如果發生碰撞，則需要重發。

**Chap3 Wireless Lan**

**Difference Between Wired and Wireless LANs**

- The medium impacts the design

- Stations are mobile

- Different MAC

**Medium Impacts**

- Shared medium

- Unprotected from outside signals

- Significantly less reliable than wired PHYs

- Dynamic topologies

**Mobile Vs. Wireless**

Mobile: Moved from location to location, but is only used while at a fixed location

Wireless: Access the LAN while in motion

**802.11 Specifications**

- MAC specifications

-CSMA/CA

- Three Physical specifications

1.Radio無綫電波：使用無綫電波進行資料傳輸，最常見的WIFI傳輸方式

2.頻率跳躍擴頻 (Frequency Hopping Spread Spectrum, FHSS)：透過頻率的快速切換來增強訊號的抗干擾性，每次數據傳輸使用不同頻率，使訊號更難被干擾或攔截。

3.直接序列擴頻 (Direct Sequence Spread Spectrum, DSSS)：將數據訊號分散在更寬的頻帶中，從而提高抗干擾能力。DSSS 更適合對抗干擾和訊號衰減，通常用於較高資料傳輸需求的情境。

4.紅外線 (Infrared)：利用紅外線進行短距離資料傳輸，但因訊號容易被阻隔，目前已較少使用。

**Spread Spectrum modulation schemes 擴頻調變方案**

爲了解決無綫通訊中的干擾，訊號衰弱和多路徑干擾等問題。

DSSS：將訊號能量分散到一個較寬的頻帶中，以抵抗干擾。它將數據訊號和一組偽隨機碼相乘，使得每個數據位元展開成多個較短的「碼片」（chip）。具有良好的抗干擾能力。

OFDM：將傳輸位元轉換成多條平行的子信號載波，每個載波都負責傳輸一小部分的資料，這樣能有效減少多路徑效應帶來的干擾。

**Wireless NICs**

**Access Point(AP) 無綫存取點**

通常用來連接無綫網路與有綫網路，讓無綫設別，可以通過AP存取有綫網路的資源。

-有綫網路和無綫網路的橋梁

-可以轉換wifi的無綫訊號 to 有綫訊號

-不同價位支持的能量不同。

- AP可以支援的無綫設備數量取決於其性能和設備規格，設備增加會導致網路速度和穩定性可能會下降。

**Basic Service Set(BSS)**

BSS是無綫網路的最小單位，由一個AP和其覆蓋範圍内的無綫設備組成。

BSSID : 每個BSS都有一個唯一的識別碼，通常是AP的MAC位址，用於區分不同的BSS。

**Independent Basic Service Set(IBSS)**

IBSS是不需要AP的網路配置，通常用於[對等網路模式]的WIFI連接，也稱爲Ad-Hoc模式。

在IBSS中，設備之間直接通訊，不經過任何中央管理的存取點。所有設別相互連接形成臨時網路。

**Extended Service Set(ESS)**

由多個BSS所組成的擴展網路，允許用戶在多個AP之間無縫漫游。

這些BSS透過一個DS相互鏈接（Ethernet）

**Distributed System(DS)**

是無線網路中重要的架構層，負責協調和管理多個無線存取點 (AP) 之間的數據流量和連接。

在大型無線網路（如擴展服務組 ESS）中，DS 起著「橋接」的作用，使得無線設備可以在不同 AP 覆蓋的區域間無縫漫遊，並維持穩定的網路連接。

DS的功能與角色：

1. 輕薄層（Thin Layer）：DS是AP内的一個輕量層，它不需要複雜的處理，但卻負責將每個AP整合在一起。
2. 數據幀傳送(Delivers frames between APs)：DS 負責將數據幀（Frame）從一個AP傳送到另一個 AP，使設備無論在哪個 AP 覆蓋範圍內，都可以互相通信。
3. AP-MN associations：DS會追踪每個AP與移動設備之間的關聯，當移動設備在不同 AP 之間漫遊時，DS會更新設備所屬的AP資訊。

Three types:

1. 整合型Integrated：單一AP在獨立網路中運行，無需額外的DS。
2. 有綫分配系統Wired：使用cable來互聯多個AP
3. 無綫分配系統Wireless DS：使用無綫連接來互聯多個AP

Service Set Identifier(SSID)

在BSS,ESS,IBSS中，用來識別不同無線網路的名稱。

· 在 **ESS** 中，SSID 用來識別一組 AP 和其覆蓋範圍內的無線設備組成的網路。

· 在 **IBSS** 中，SSID 是用來識別設備間的對等網路，這些設備並未通過 AP 連接。

· 在 **IBSS** 中，無需 AP，所有設備直接連接。此時，如果沒有 AP，網路中的設備使用 **BSSID**來進行識別。BBSID是一個48bit標識碼，通常是設備的MAC地址

· 在有 AP 的 **ESS** 中，使用 ESSID來識別整個網路。ESSID是一個可設定的名稱，通常是用戶為無線網路設定的名稱（例如 "Home\_Network" 或 "Office\_WiFi"）。

**Probing Phase探測階段**

是無線客戶端設備在嘗試連接無線網路時的第一步，主要目的是尋找並識別可用的無線存取點 (AP).涉及設備如何掃描不同的頻道以發現 AP，並在特定時間內保持掃描，直到找到合適的 AP 或達到預設的時間限制。

1. 尋找available AP
2. APs 可以運作在不同的頻道上，最多有11個頻道可用。
3. **掃描時間**：
   1. 在每個頻道上，設備需要保持掃描一定時間，這段時間被稱為 **MinChannelTime**（最小頻道掃描時間）。
   2. **MinChannelTime** 是設備在一個頻道上進行掃描的最短時間，這樣可以確保設備能夠接收到該頻道上廣播的 AP 信息。
   3. 如果設備在掃描一個頻道時發現了可用的 AP，掃描應該持續 **MaxChannelTime**（最大頻道掃描時間），這樣設備可以有足夠的時間來處理來自不同 AP 的回應。如果設備在 **MaxChannelTime** 內沒有發現任何 AP，它會切換到下一個頻道進行掃描。

**WEP key Management**

What is “KeyID”?

Each entity in the wireless LAN (AP, clients) is configured with four static WEP keys

KeyIDs 0,1,2,3

The keys are shared by an AP and all the wireless stations accessing it

The ID of the key used for encryption/decryption appears in the packet WEP header

**Details - Checksum**

CRC-32 - detecting single random bit errors

If CRC is correct, WEP assumes

Packet has not been modified

Packet is from authorized user

Linear Property:

CRC (XOR(A,B)) = XOR(CRC (A), CRC(B))

**RC4**

Developed by Rivest in 1987

Kept as a trade secret (but leaked in 1994)

Key can be between 1 and 256 bytes

Used as a simple and fast generator of pseudo-random sequences of bytes (to be used as “one-time-pad”)

Should discard first 256 bytes of generated pad

Passes all usual randomness tests

**802.11 Vulnerabilities**

RC 4 stream cipher not suited for data with lots of packet loss

Loss of data requires re-synch, new key every time

Poor key management

WEP uses same key for authentication/encryption

Provides no mechanism for session key refreshing

one-way authentication:

has no provision for MNs to authenticate/verify the integrality of AP

**802.1X**

based on EAP (extensible authentication protocol, RFC 2284)

both supplicant and authenticator have a port access entity (PAE)

PAE controls the authorized/unauthorized state of its controlled port

EAP messages between the supplicant and authenticator

EAP messages from the supplicant are relayed to the authentication server by the authenticator PAE

Once the supplicant is authenticated successfully, the controlled port in the authenticator is authorized

Supplicant will go through the controlled port to acquire the necessary services

**Three Main Components**

supplicant: usually the client software

authenticator: usually the access point

authentication server: usually a Remote Authentication Dial-In User Service (RADIUS) server

**802.1X – How it works**

1. 未授權狀態：設備（MN）初始處於未授權狀態，只有 802.1X 流量會被轉發，其他流量（如 DHCP、HTTP 等）會被阻止。
2. 身份驗證過程：

客戶端發送 EAP-start 消息。

AP 回應 EAP-request identity 消息，要求客戶端提供身份。

客戶端將身份信息發送給 認證伺服器。

1. 認證伺服器驗證：

認證伺服器根據特定算法驗證設備身份，並返回 接受 或 拒絕 消息。

1. 授權連接：

如果認證通過，AP 將客戶端端口轉換為授權狀態，開始轉發所有流量。

1. 登出過程：客戶端發送 EAP-logoff 消息，將端口轉為未授權狀態。

**802.11 Key Management**

Key Management:

BKR (broadcast key rotation)

AP periodically broadcasts WEP shared key

The initial WEP key only used for registration at the first time.

So the WEP key is used less frequently.

TKIP (temporal key integrity protocol)

hashing the key before using it for encrypting a packet

**Inter-Frame Space訊框間隔**

1.短訊框間隔(Short IFS):最短的IFS，用於發送要求傳送RTS，允許傳送CTS，回覆ACK等訊息。

2.中樞協調功能訊框間隔(PCF IFS):次短的IFS，在免競爭時期，有資料待傳的工作站需等待PIFS期間過後再進行傳送。

3.分散式協調功能訊框間隔(DCF IFS):第三短的IFS，競爭時期需傳資料的工作站需等待medium閒置再等待至少DIFS時間，才可進行傳送。

4.延長訊框間隔(Extended IFS):最長之IFS，針對需要重送的Frame需等待至少EIFS才可以進行傳送。

**Short Interframe Space (SIFS)**

是無線網路中設備處理接收到的資料幀並回應的時間間隔。它指的是回應幀的第一個符號開始傳送與接收到的幀最後一個符號結束之間的時間差。

SIFS 包括接收無線信號的延遲、物理層協定的延遲（PLCP），以及 MAC 層處理的延遲。這段時間通常用於以下情況：

* 傳送確認訊息 (ACK)。
* 傳送 **Clear To Send (CTS)** 幀、塊確認幀或資料片段的第二個或後續幀。
* 在 **Point Coordination Function (PCF)** 中的競爭自由期或設備回應輪詢時。

簡單來說，SIFS 是一個用於快速回應的短時間間隔，確保網路中的即時回應與順序傳輸。

**PCF IFS (PIFS)：**

- 由啟用 **Point Coordination Function (PCF)** 的 AP 使用，這段時間比 **DIFS** 短，但比 **SIFS** 長 (DIFS > PIFS > SIFS)。

- AP 擁有較高的優先權，可以在 PIFS 時間內佔用媒介。

**DCF IFS (DIFS)：**

- 用於控制 **Distributed Coordination Function (DCF)**，這是標準的無線媒介訪問機制。

- 設備在傳輸前必須檢查媒介是否空閒。如果發現媒介空閒，則可以傳輸；如果媒介忙碌，則需要等待。

- 計算公式：**DIFS = SIFS + (2 \* Slot time)**

**Extended Interframe space (EIFS)**

當接收到的幀包含錯誤時，設備需要等待 EIFS 時間再發送幀，而不是等待 DIFS。這樣做的原因是，雖然設備未能解碼幀，但可能接收方已經能解碼並能回傳確認幀 (Ack)。EIFS 確保接收方可以無干擾地發送確認回應。

EIFS 計算方法：EIFS = 確認幀的傳輸時間（最低物理層速率）+ SIFS + DIFS

**「輪詢」(polling)**

通常用於 免競爭週期 (Contention-Free Period, CFP)。在這段時間內，協調者負責輪詢工作站，確保順序和無衝突的資料傳輸。

在輪詢過程中，根據工作站的角色，訊框回應方式分為三種：

1. 協調者接收訊框：

協調者可在發送下一筆訊框或輪詢其他工作站時，同時回覆訊框：Data+CF-Poll+CF-ACK 或 CF-Poll+CF-ACK。

1. 被輪詢的工作站接收訊框：

如果有資料要傳送，則回覆：Data+CF-ACK。

如果沒有資料要傳送，則專程回覆：CF-ACK。

1. 非被輪詢的工作站接收訊框：

這些工作站應使用 DCF ACK 的方式回應，等待一個 SIFS 間隔後傳送回應訊框。

**MAC Management Layer**

1. 同步 (Synchronization)：

時間同步功能 (TSF) 用於確保網路中所有設備的時間一致，幫助協調傳輸。

1. 電源管理 (Power Management)：

使設備可以在不錯過訊息的情況下進行休眠。

功能包括定期休眠、幀緩存和流量指示圖，這些都幫助設備在低功耗模式下運行。

1. 關聯與重新關聯 (Association & Reassociation)：

關聯 (Association) 是設備加入網路的過程。

重新關聯 (Reassociation) 是設備在移動過程中從一個 AP 切換到另一個 AP 時，保持網路連接。

**Synchronization in 802.11**

在 802.11 中的 同步 (Synchronization)，所有工作站維持本地計時器。時間同步功能 (TSF) 用來保持網路中所有設備的時鐘同步。具體方法是通過定期發送 Beacon 訊框，其中包含整個 BSS 的 時間戳 (Timestamp)，設備利用這些時間戳來校準自己的本地時鐘。這樣可以確保網路中的所有設備時間一致，便於協調傳輸與接收。

**802.11 Time Synchronization Function (TSF)**

時間同步功能 (TSF) 透過 Beacon 訊框 來保持網路設備時間一致。以下是一些關鍵概念：

1. Beacon Period：是 Beacon 訊框的發送週期。
2. Target Beacon Transmission Times (TBTTs)：是預定發送 Beacon 訊框的時間點，每個 TBTT 相隔一個 Beacon Period。
3. CSMA 延遲：Beacon 訊框的發送可能會受到 CSMA 的延遲影響。
4. 時間戳 (Timestamp)：Beacon 訊框中包含的時間戳，記錄了傳送時的計時器值，幫助設備同步時鐘。

**Power Management**

電源管理 對於電池供電的移動設備非常重要。現有的 LAN 協定假設工作站隨時準備接收數據，但在空閒接收狀態下，網路適配器的電力消耗會較高。

802.11 電源管理協定 允許無線收發器在不需要接收數據時盡量處於關閉狀態，從而節省電力。這種管理方式對現有協定透明，不會干擾正常的資料傳輸。

**Power Management in Infrastructure Mode**

允許閒置的工作站進入休眠模式:

1. 工作站的省電模式會存儲在 AP 中。
2. AP 會為進入休眠模式的工作站緩存數據包。
3. AP 會公告哪些工作站有緩存的數據包。
4. 每個 Beacon 訊框 都會帶有 流量指示圖 (TIM)，告訴工作站是否有待接收的數據包。

省電模式工作站 會定期醒來，並檢查 Beacon 訊框。具體流程如下：

1. 當工作站醒來時，會聆聽 Beacon。
2. 如果 AP 有為該工作站緩存的數據包，工作站會發送 省電輪詢請求 (power-save poll request) 訊框給 AP。
3. AP 會將緩存的數據發送給工作站。
4. 數據傳送完畢後，工作站可以再次進入休眠狀態。

**Power Management in Ad Hoc Mode**

在 Ad Hoc 模式 中的 電源管理 類似於 基礎設施模式，但沒有 AP，數據緩存由發送工作站處理。具體流程如下：

1. 休眠工作站定期醒來，聆聽 Beacon 和 ATIM。
2. 如果有緩存的數據，工作站會發送 Ack 並保持喚醒。
3. 發送工作站將數據發送給喚醒的工作站。