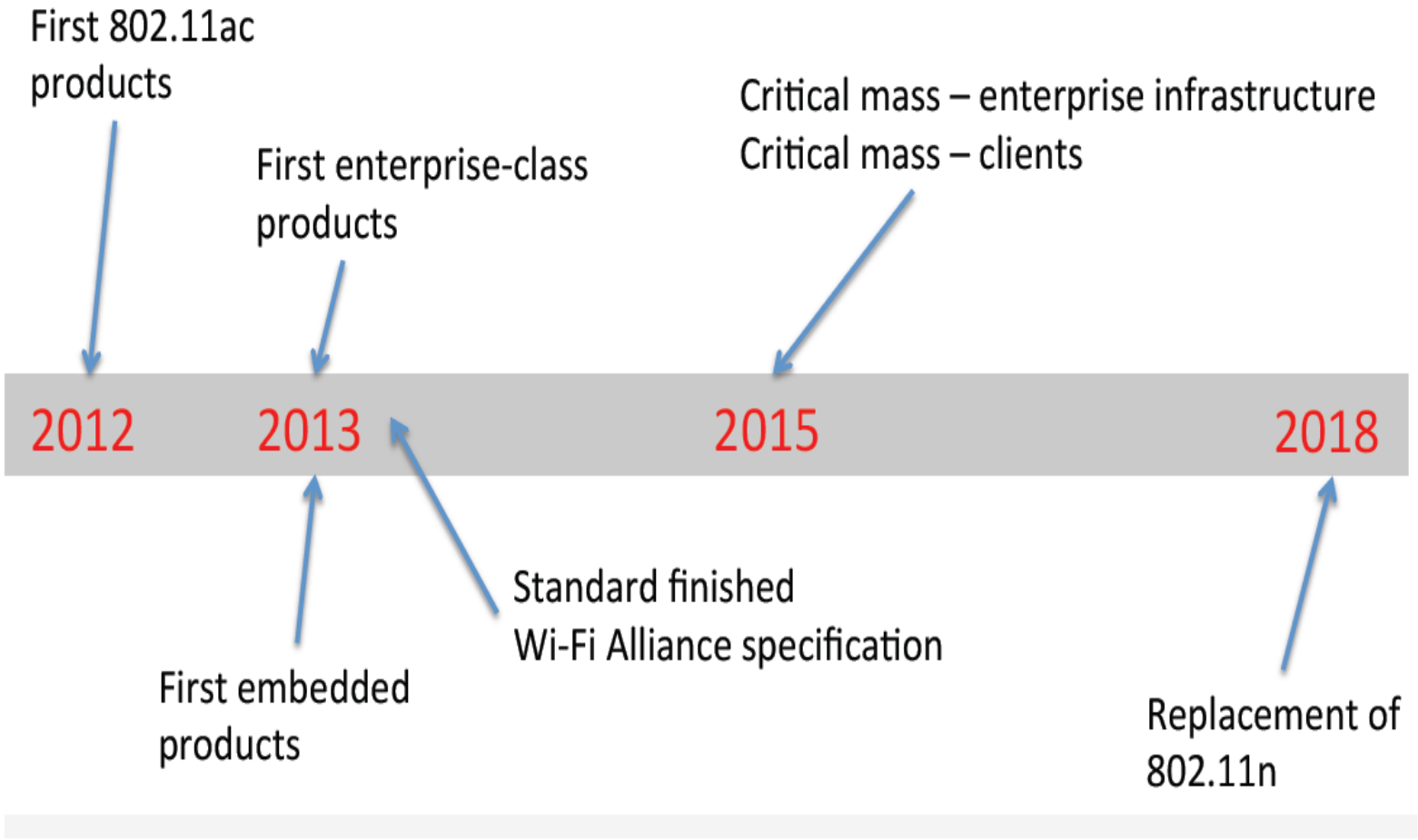
無線網路安全與管理

台大計資中心
曾保彰
E-mail : bjtseng@ntu.edu.tw

802.11ac簡介

- 802.11a 使用5GHz, 會演進為802.11ac, 目前最高速度是1300Mbps(俗稱5G WIFI)
- 802.11n 使用2.4GHz及5GHz, 目前最高速度是450Mbps
- 使用DUAL BAND可達1750Mbps
- 現802.11ac已是IEEE standard, 預計2015年會普遍

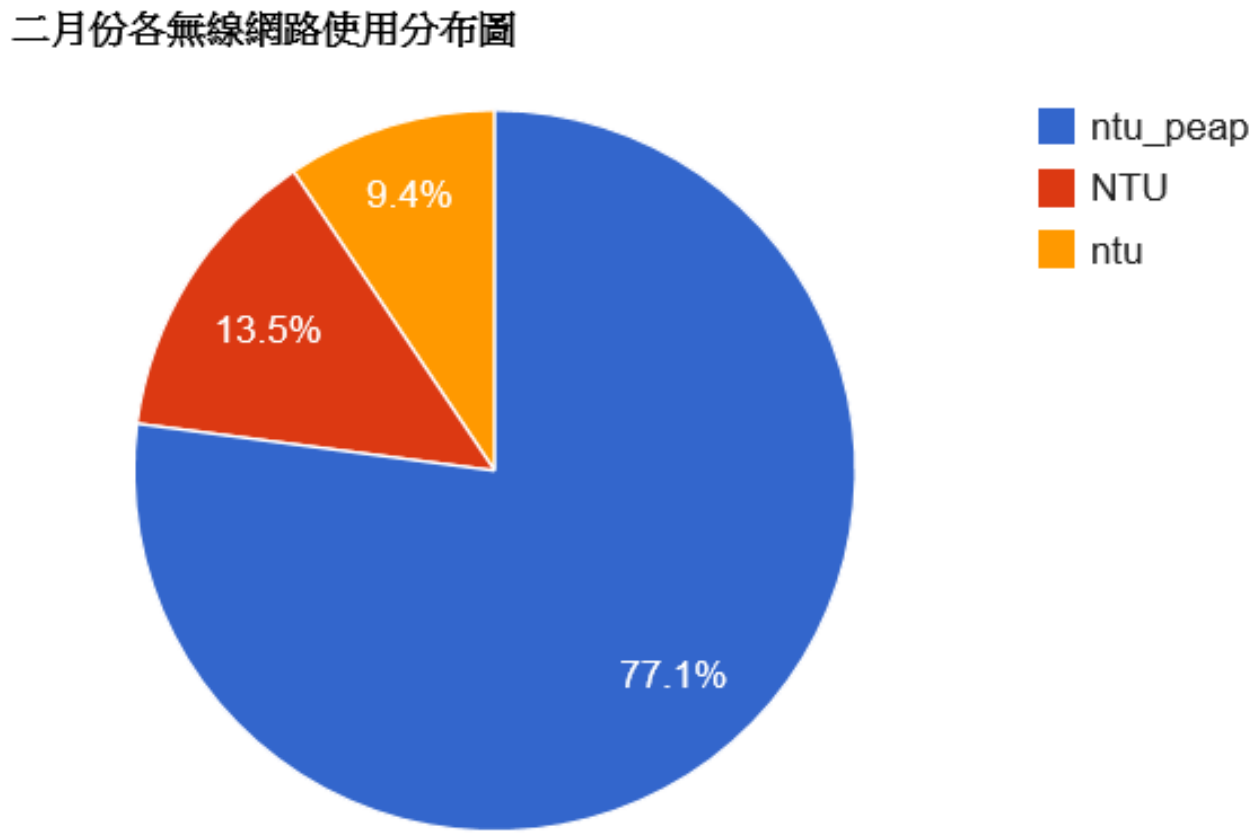
The 802.11ac Action Plan



本校無線網路同時上次人數

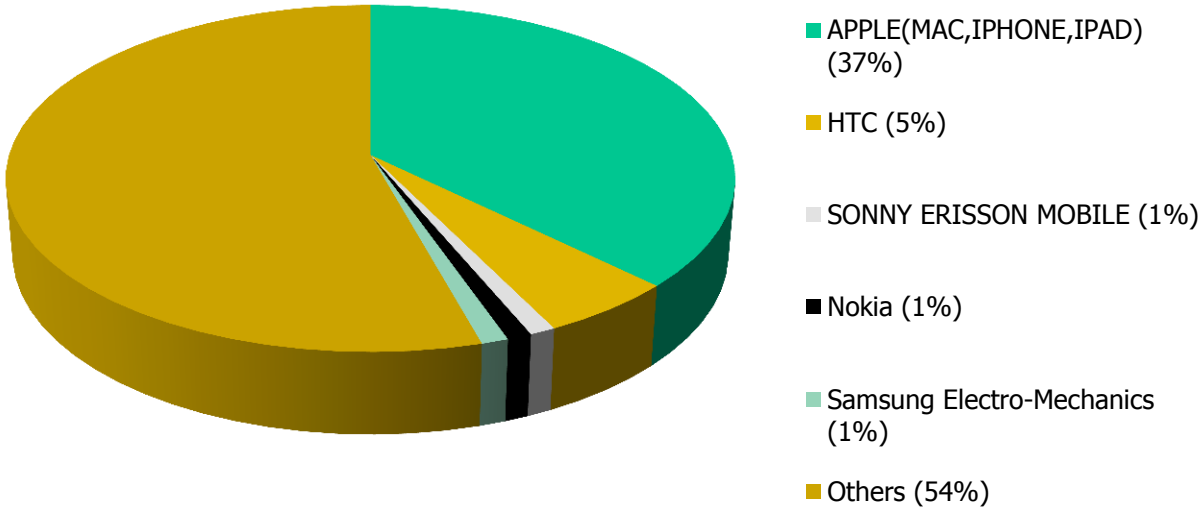
- 2012-01-01至2012-12-31止,有14,255,816人次。
- 2013-01-01至2013-12-31止,有29,287,934人次。(是去年2倍)
- 這學期同時上線人數,上課每天最高都接近二萬人。

2014 年二月份各SSID人數比例



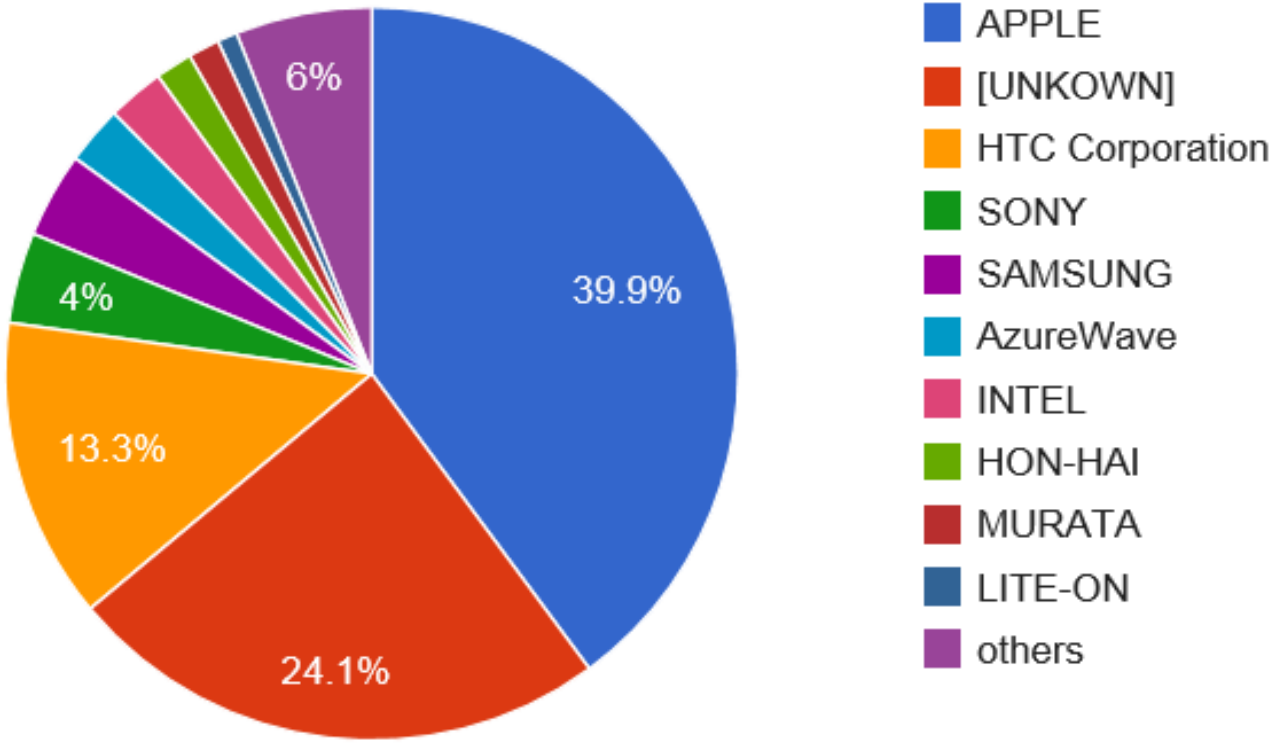
NTU wireless devices

- 2010-11-16至2011-7-12共4,222,853筆



2014 年二月份各上網裝置比例

二月份各廠牌設備使用分布圖



iNTU

- 已完成IPHONE版本及ANDROID版本
- 直接到APP STORE及GOOGLE MARKET免費下載


臺灣大學
單位查詢
通訊錄
行事曆
地圖
電子報
圖書館
部落格
研討會
演講
活動
緊急
近期
NTUbe
網路測速
關於

台大測速(speed.ntu.edu.tw)

台大測速手機版（增加動畫）

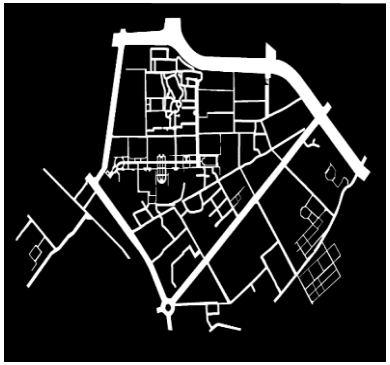
- L 1　　L 2　　L 3　　L 4

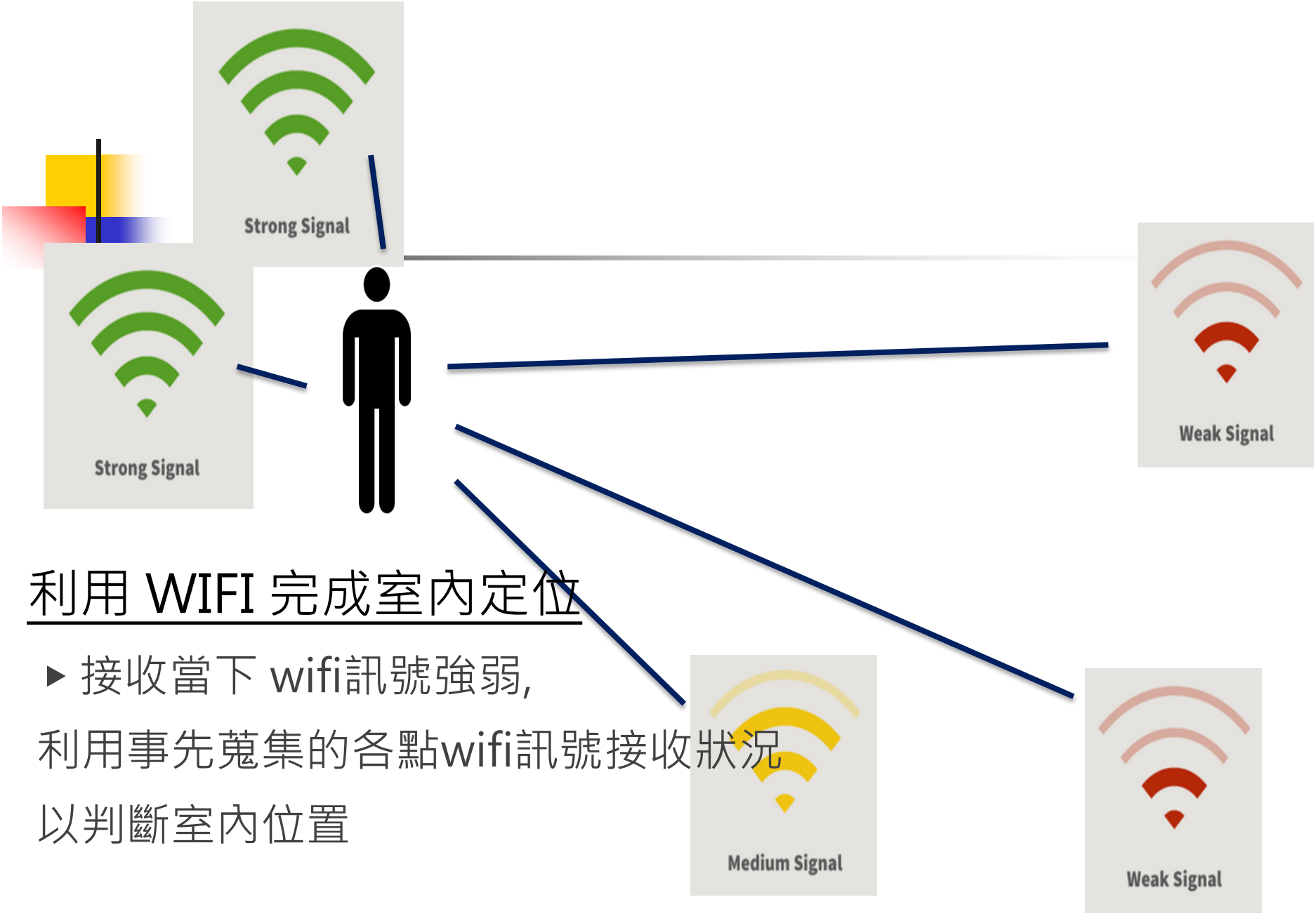
HAMI-台大室內室外導覽

- 台大校園導覽, 包含室內室外
- 定位
- 路徑規劃
- 景點導覽

Innovation

- 利用 WIFI 完成**室內定位**
- 利用 2張地圖 完成**路徑規劃**





利用 WIFI 完成室內定位

- 接收當下 wifi訊號強弱,

利用事先蒐集的各點wifi訊號接收狀況

以判斷室內位置

無線區域網路介紹

- 透過無線電波或光傳導等無線傳輸媒介進行資訊存取之網路架構.
- Wireless Local Area Network:利用射頻(radio frequency)技術取代傳統佈線之lan
- WLAN 機動性高,擴充性大.但網路安全問題,干擾問題,耗電問題(行動設備).=>locale (GOOGLE APP)

常見無線區域網路標準

- 802.11
- Bluetooth
  - 手機與電腦共同制定的一種技術, low power, short distance.
- 行動通訊網路技術
  - 2G GSM
  - 3G CDMA
  - 4G LTE
- 802.16(WiMAX)

Bluetooth

- Bluetooth 1994年由Ericsson 發展
- Bluetooth提供短距離、無線、低價、高度整合、群體溝通及語音數據之資訊傳輸環境.一個設備最多可與七個設備連結傳輸.
- 使用ISM的2.4G頻段
- APPLE -- iBeacon

Wireless Network

- 3G,4G …
  - Mobility&Range High
  - Data rate low(<100Mb/s)
  - High cost
- Wireless Lan 802.11a/b/g/n/ac….
  - Mobility&Range low
  - Data rate High(>11Mb/s)
  - Low cost
  - 802.11ac max rate 1300Mb/s

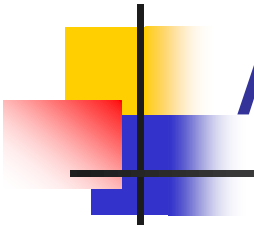
Wireless AP 電波問題

- 2007年元月18日yahoo首頁 “電磁波超量千倍 環團籲校園無線上網喊停”
- 台大圖書館量到的無線基地台功率約
  -40dbm(0.0001mw)(天線旁邊)至
  -70dbm(0.0000001mw)(約10公尺遠)

  手機功率國家規定不得超過1mw/cm^2
- 量測儀器最好用頻譜分析儀,針對2.4GHz(802.11bg)及5GHz(802.11a)量測

IEEE 802.11 History

- 1990,IEEE 802.11 committee
- 1997,IEEE 802.11 standard=>1,2M
- 1999,WECA(Wireless Ethernet Compatibility Alliance)=>802.11a,b
  - Intel、Intersil、IBM、Nokia、Lucent、Compaq、Toshiba…
- Wi Fi (wireless fidelity)
- 2003, 802.11g
- 2009,802.11n
- 2014,802.11ac



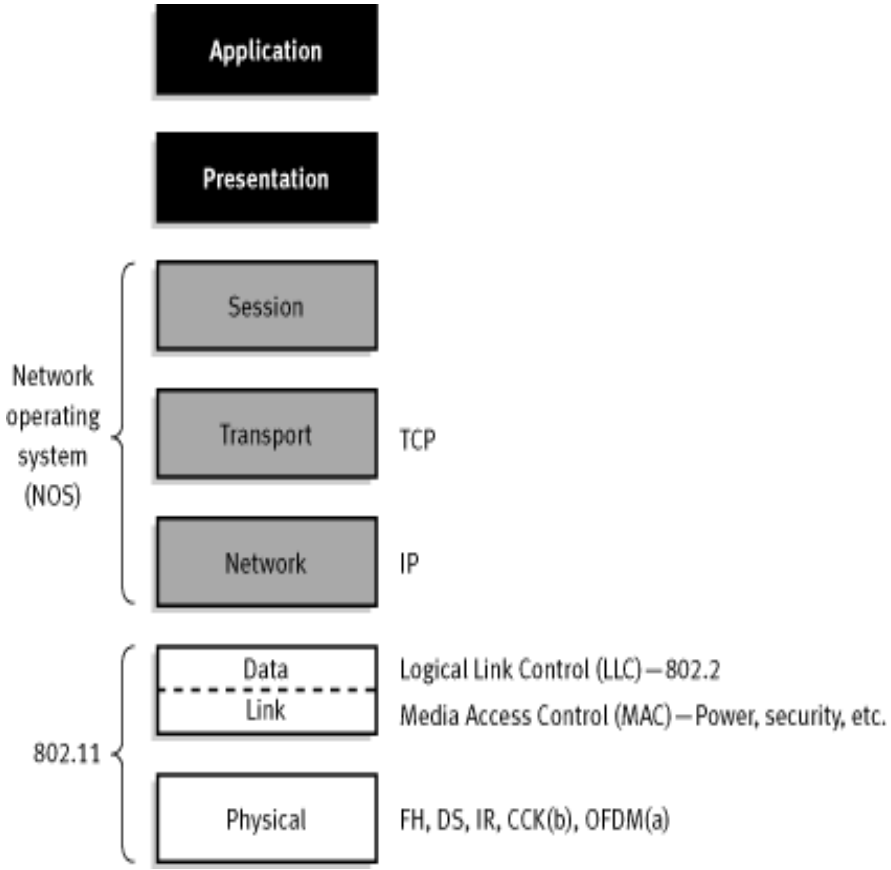
ANSI/IEEE 802.11

Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications

802.11 Design issue

- The media impact the design
  - Neither absolute nor readily observable boundaries
  - Unprotected from outside signals
  - Less reliable than wired PHYs
  - Dynamic topologies
  - Lack full connectivity
  - Time-varing and asymmetric propagation properties

802.11 ISO Model



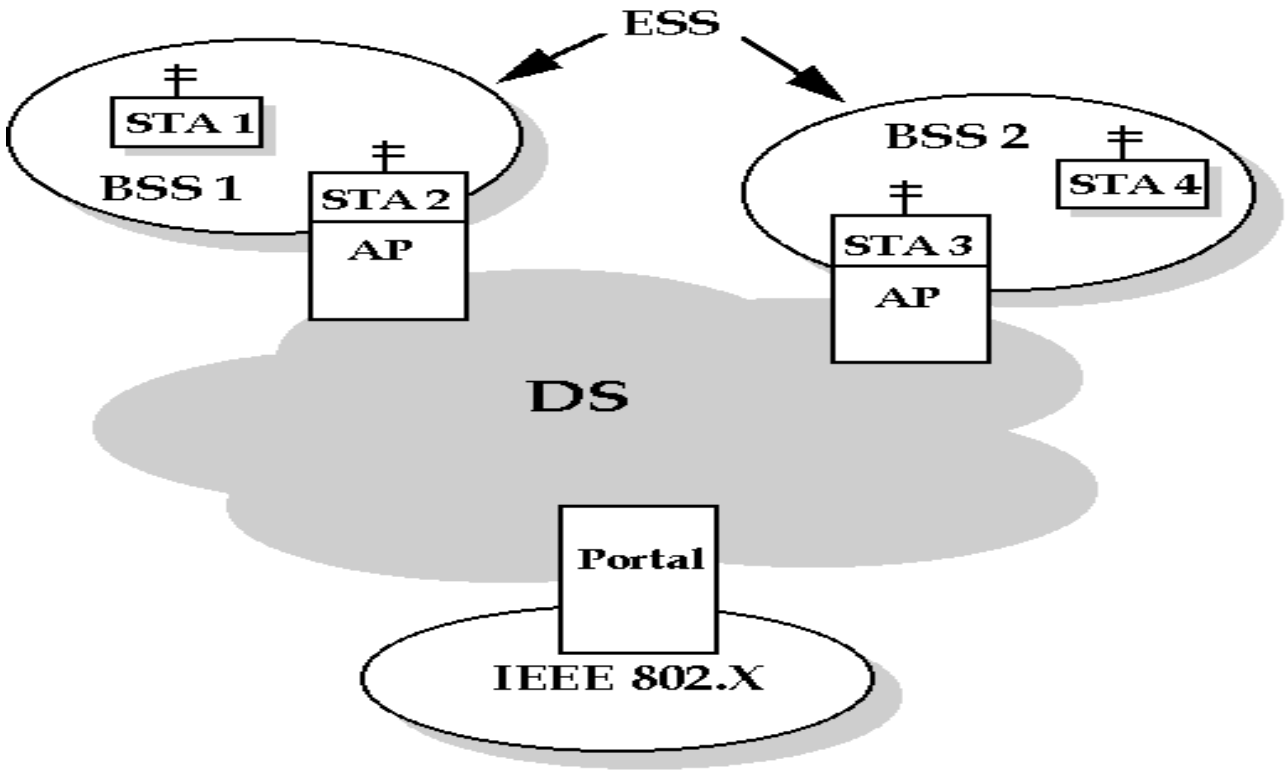
802.11 Componets(1)

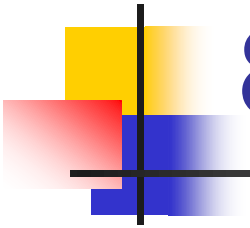
- Wireless Medium(WM)
  - The medium used to implement a wireless LAN
- Station(STA)
  - Any device that contains an 802.11 conformant MAC and PHY interface to the wireless medium
- Station Service
  - The set of services that support transport of MSDU(Mac Service Data Units) between Stations within a BSS
- Basic Service Set(BSS)
  - The BSS is the basic building block of an 802.11 LAN
- Distribution system(DS)
  - A system used to interconnect a set of BSSs to create an ESS

802.11 Componets(2)

- **Distribution System Services(DSS)**
  - The set of services provided by the DS which enable the MAC to transport MSDUs between BSSs within an ESS
- **Access Point(AP):**
  - Any entity that has STA functionality and provides access to the DS
  - An AP is a STA which provides access to the DS by providing DS services in addition to Station Services.

802.11 Network Infrastructure

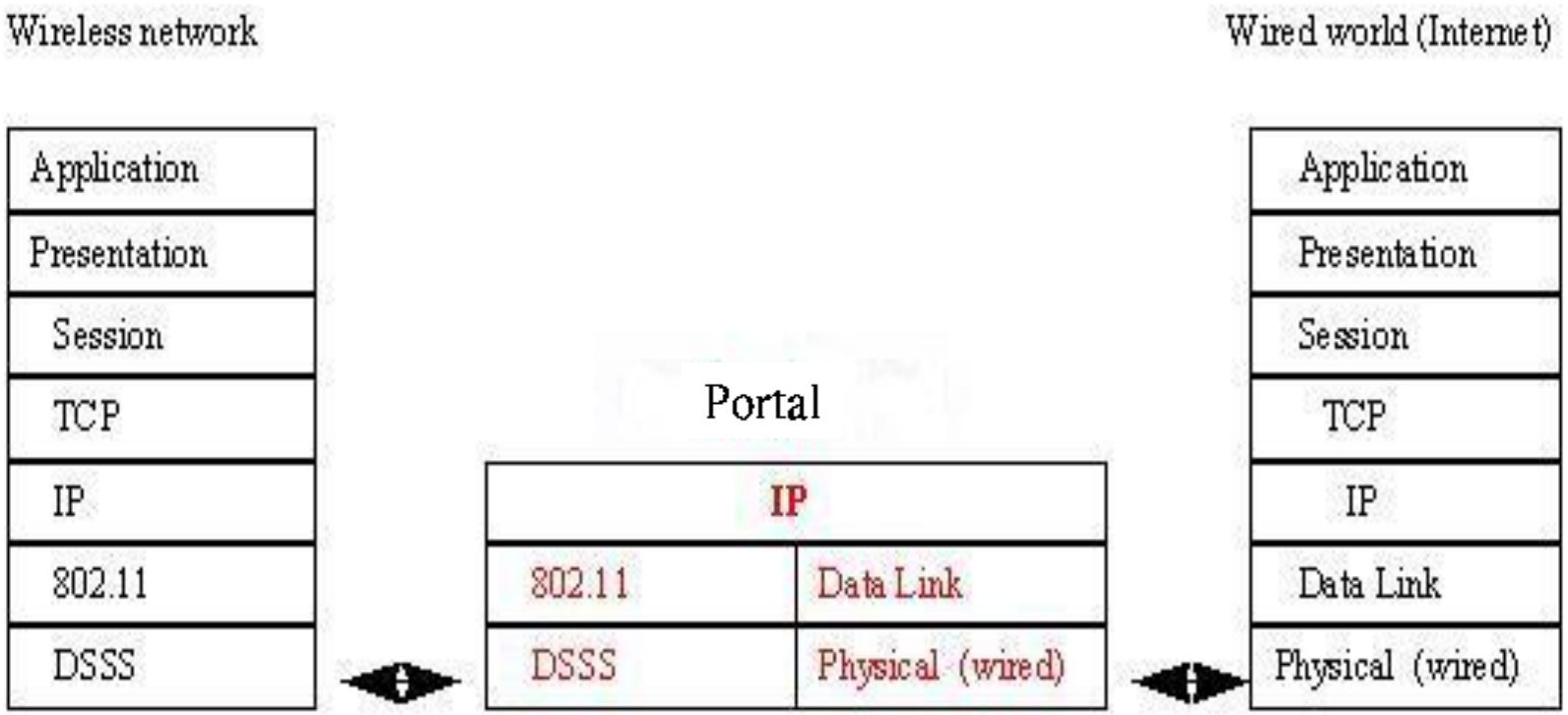




802.11 Services

- Station Services
  - Authentication, Deauthentication
  - Privacy
  - MSDU delivery
- Distribution System Services
  - Association, Disassociation
  - Distribution(route to 802.11)
  - Integration(route to 802.x)
  - Reassociation(hand-off, roaming)

802.11 Portal



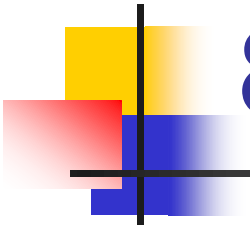
802.11 Phy(1)

- Operate within the 2.4 GHz
  - 802.11-base products do not require user licensing (2.4GHz and 5G are ISM band)or special training
  - FHSS(frequency hopping spread spectrum)
  - DSSS(direct sequence spread spectrum)

- Operate within the 2.4GHz and 5GHz(54Mbps)
  - OFDM(orthogonal frequency division multiplexing)

802.11 Phy(2)

- FHSS and DSSS are fundamentally different signaling mechanisms and will not interoperate with one another
- Spread-spectrum increase reliability, boost throughput, and allow many unrelated products to share the spectrum without explicit cooperation and with minimal interference



802.11 FHSS

- More security and without interfere
  - 2nd War
  - 1600 hops/sec
  - Limited speeds no higher than 2Mbps(hopping overhead)

802.11 DSSS

- Divides the 2.4 GHz band into 14 twenty-two MHz channels
- Adjacent channels overlap on another partially, only 3 of 14 being completely nonoverlapping
- No hopping
- 11-bit chipping-Barker sequence

802.11

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11(Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11(Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8(CCK)	QPSK	1.375 MSps	4
11 Mbps	8(CCK)	QPSK	1.375 MSps	8

- BPSK-Binary Phase Shift Keying
- QPSK-Quadrature Phase Shift Keying
- Complementary Code Keying

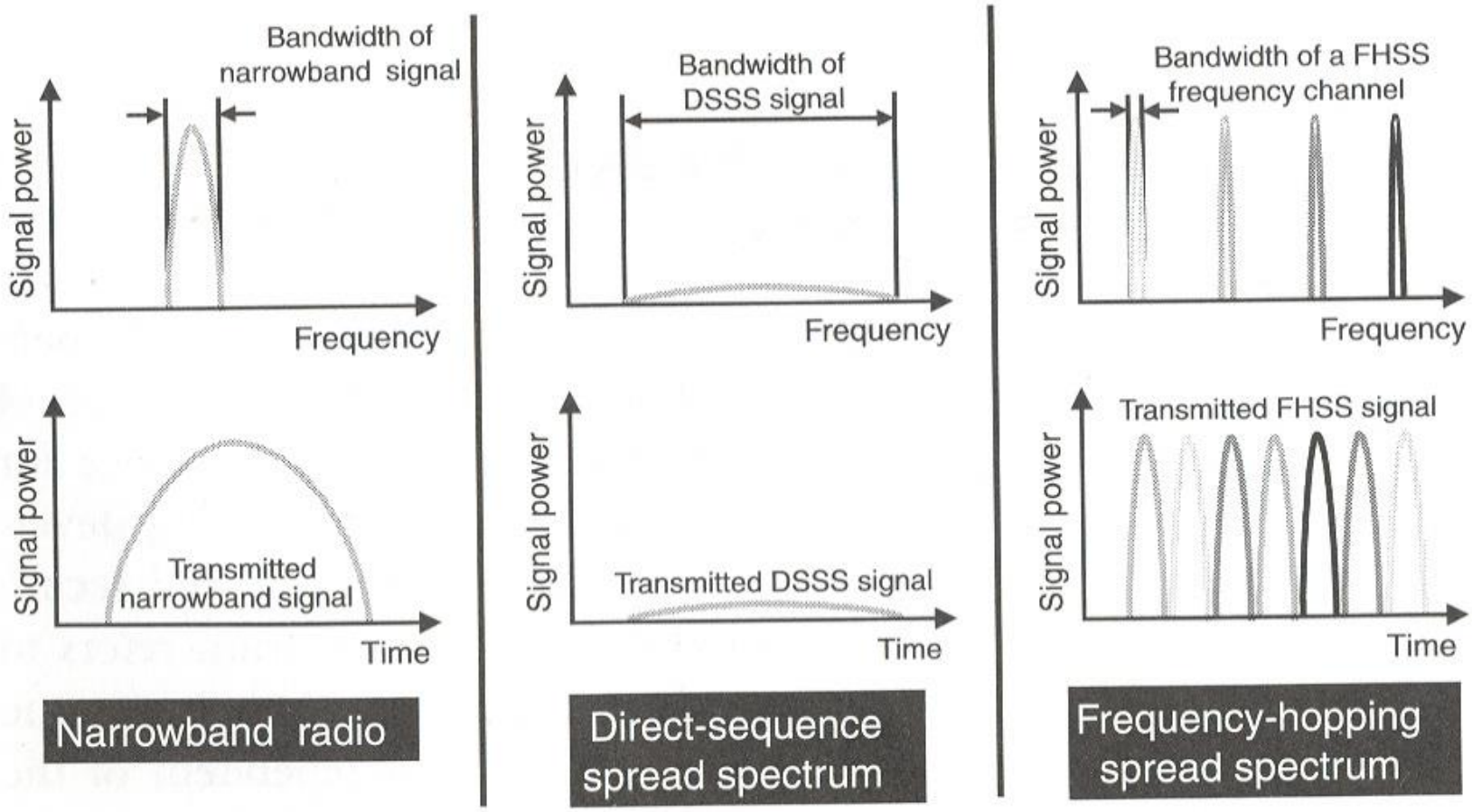


Figure 2.1 Narrowband radio, DSSS, and FHSS.

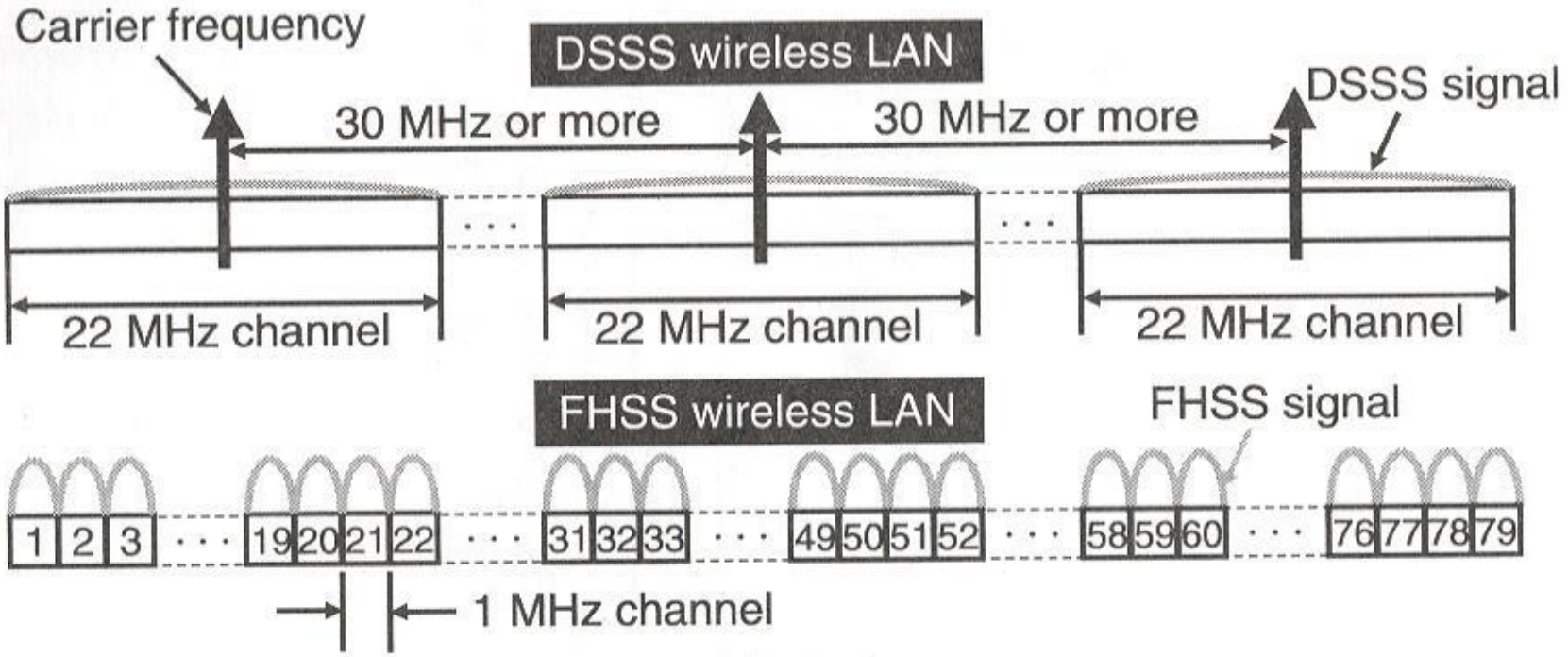


Figure 2.10 Frequency channels for 2.4 GHz DSSS and FHSS

802.11 DSSS Frequency

Channel ID	Frequency (GHz)	地區					
		美國	加拿大	歐洲	西班牙	法國	日本
1	2.412	O	O	O			
2	2.417	O	O	O			
3	2.422	O	O	O			
4	2.427	O	O	O			
5	2.432	O	O	O			
6	2.437	O	O	O			
7	2.442	O	O	O			
8	2.447	O	O	O			
9	2.452	O	O	O			
10	2.457	O	O	O	O	O	
11	2.462	O	O	O	O	O	
12	2.467			O		O	
13	2.472			O		O	
14	2.484						O

ODFM spectrum

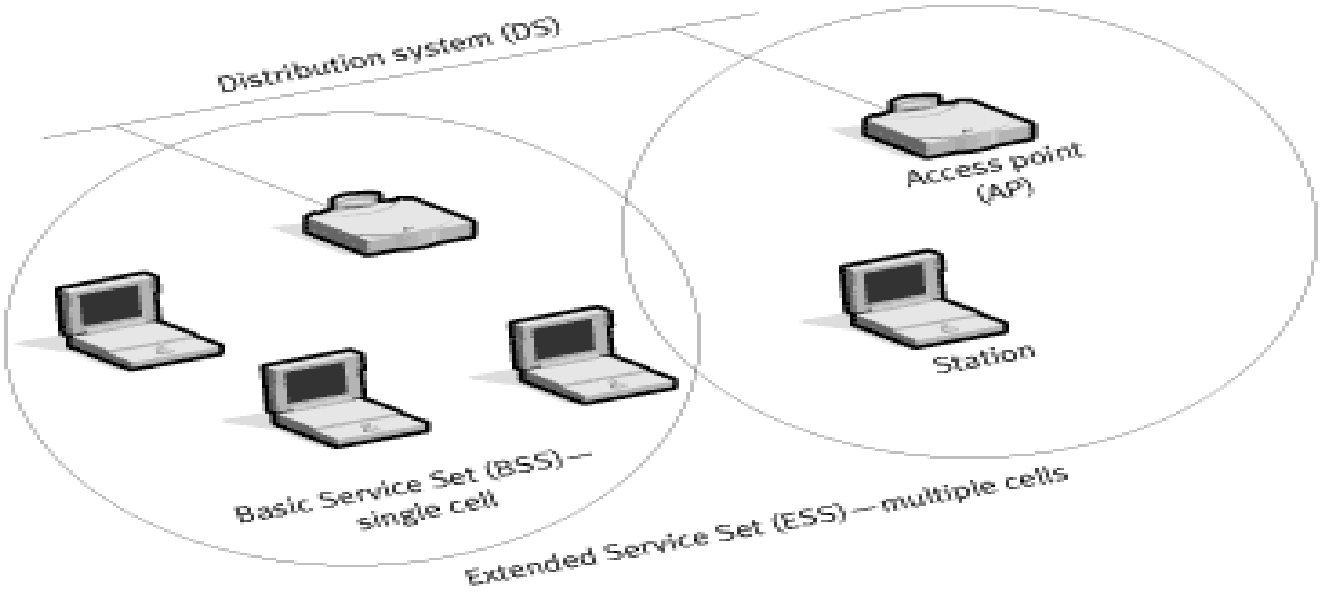
- 802.11b=802.11g:2.4-2.4835GHz (total:83.5MHz)(3 non-Overlapping CH)
- 802.11a:5.15-5.25GHz,5.25-5.35GHz,5.725-5.825GHz,(total 300MHz) (12 non-Overlapping CH)
- Center frequency: 5.18,5.20,5.22,5.24,5.26,5.28,5.30,5.32, 5.745,5.765,5.785,5.805
- Ch.36..Ch.161

Data Rate	6,9,12,18,24,36,48,54 Mbps
Modulation	BPSK, QPSK, 16-QAM, 64 QAM
Coding Rate	1/2, 2/3,3/4
# of Sub-Carriers	52
# of pilots	4
OFDM Symbol Duration	4 us
Guard Interval	800 ns
Sub-Carrier Spacing	312.5 kHz
3 dB bandwidth	16.56 MHz
Channel Spacing	20 MHz

802.11

Infrastructure_mode

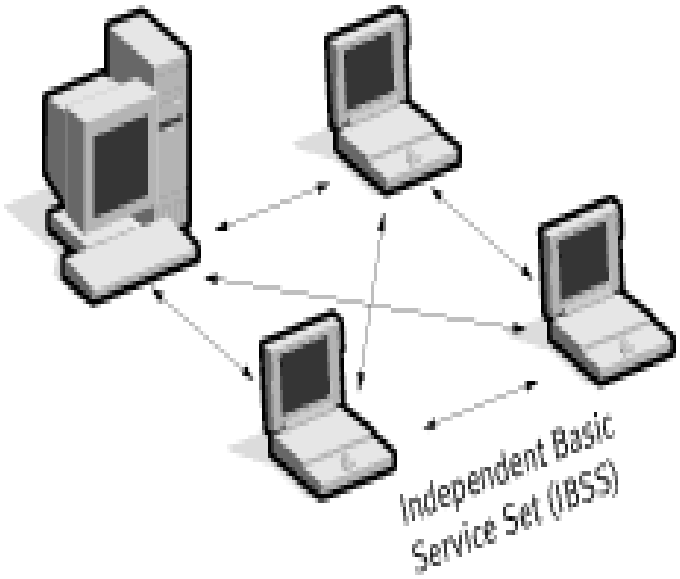
- The wireless network consists of at least one access point connected to the wired network infrastructure



802.11

Ad hoc mode

- It's a simply set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network

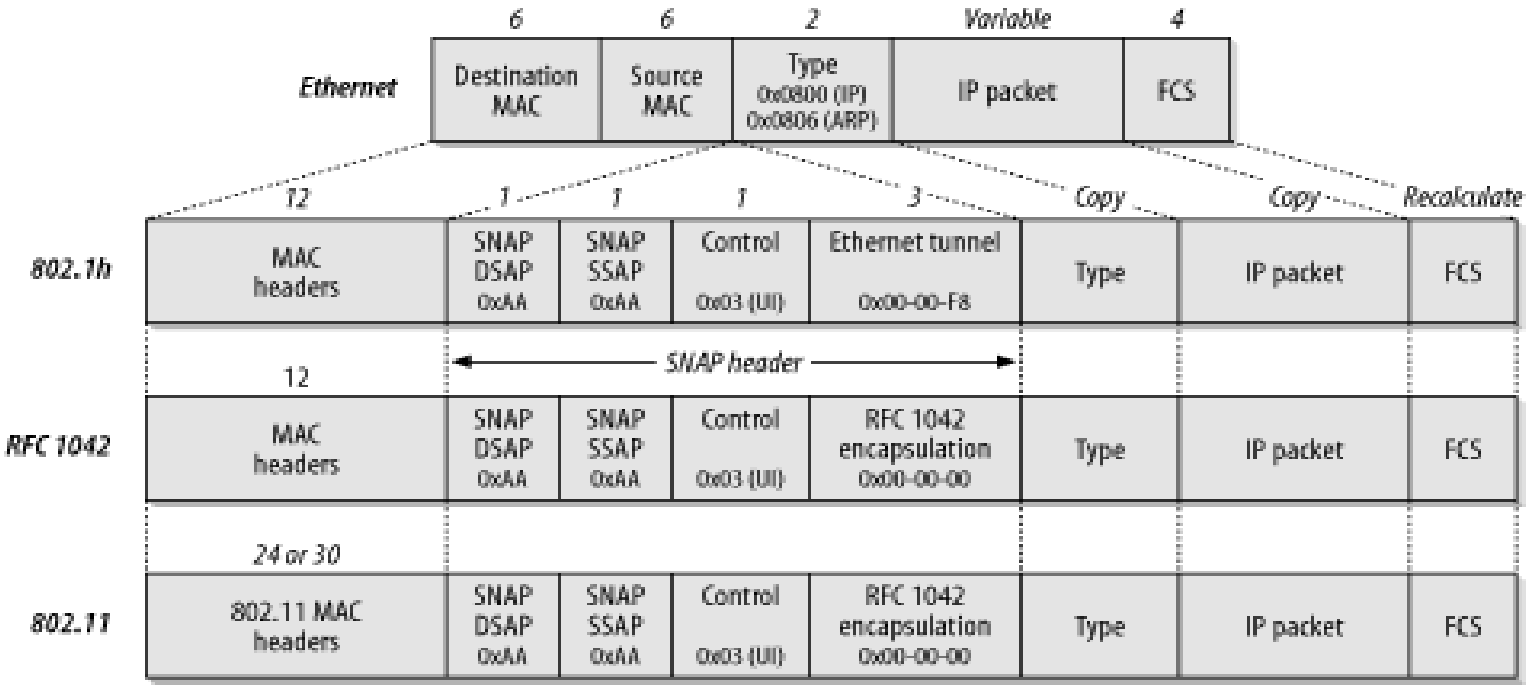


802.11 LLC & MAC

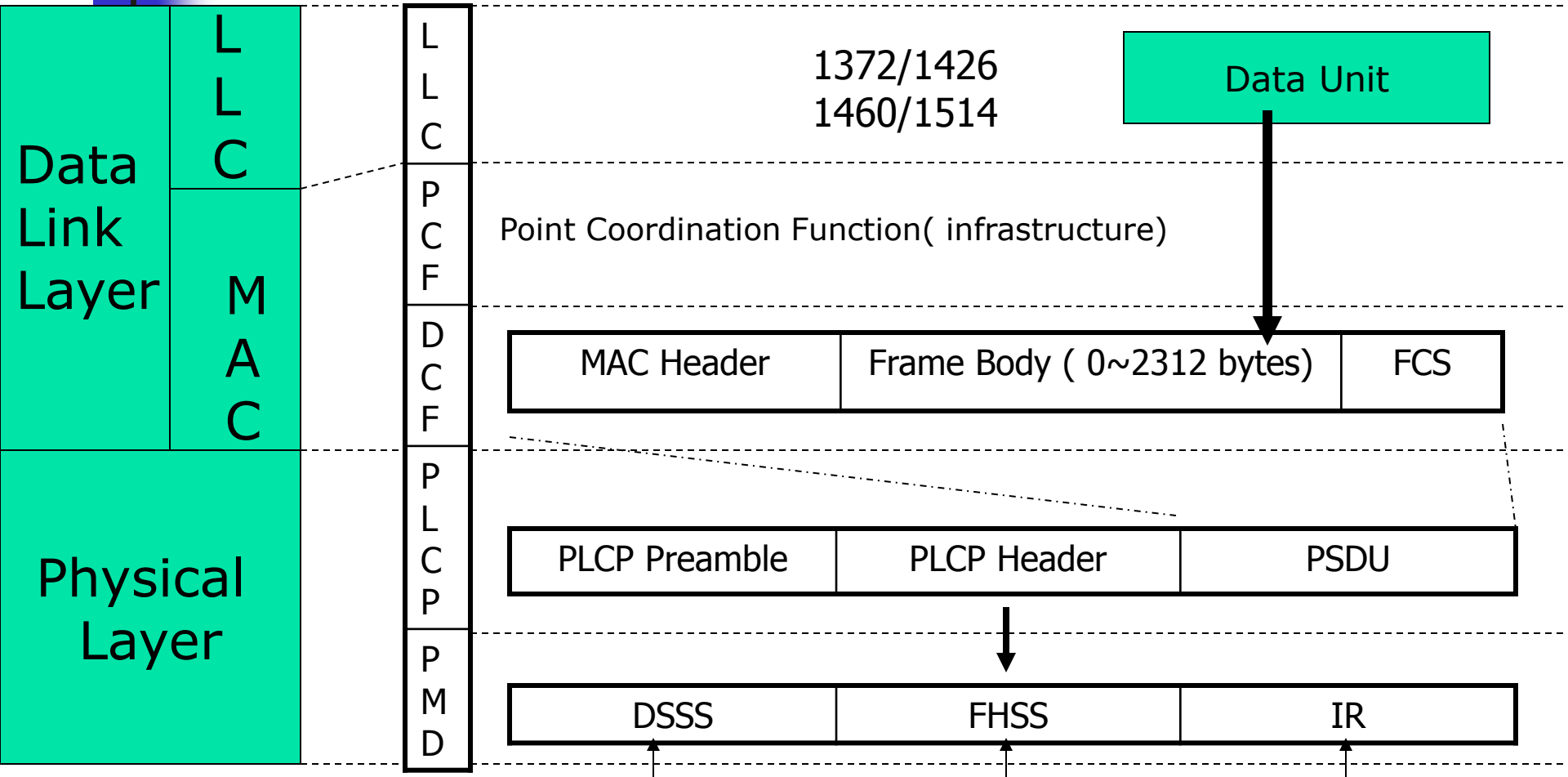
- LLC-Logical Link Control
  - The same 802.2 and 48 bits addressing
  - MAC is different
- CSMA/CA(Carrier sense multiple access/collision avoidance)
  - By using explicit packet ACK, which means an ACK is sent by receiving station to confirm that the data packet arrived intact.

Carry Existing Traffic

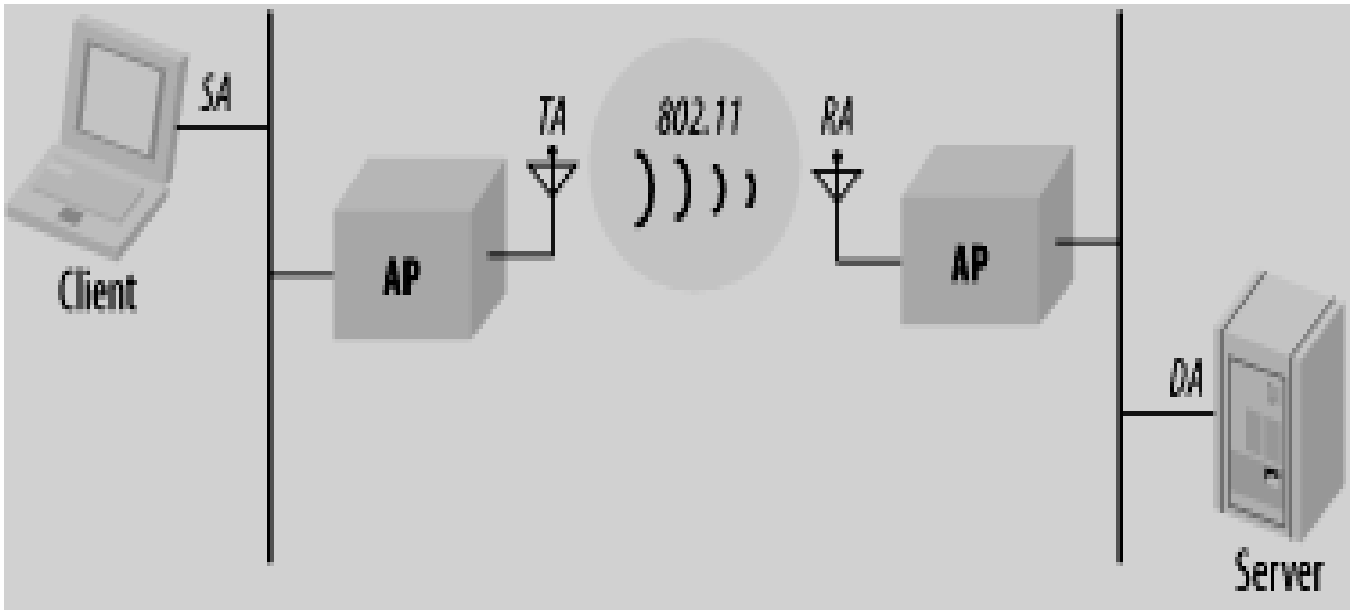
- Ethernet frames are encapsulated within 802.11



802.11 Protocol Stack



Four Addresses of the Protocol

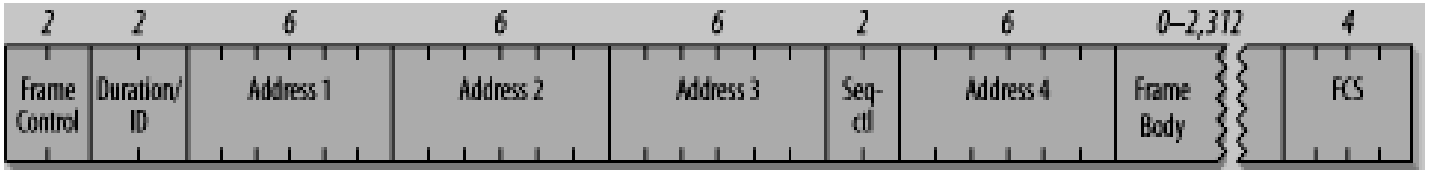


802.11 used as

Distribution System (DS)

Four Addresses of the Protocol

- *Wireless Transmissions are fundamentally* ***point-to-point.***



- Four address fields to support distinction between
  - Transmitter
  - Receiver
  - Sender
  - Destination

802.11 DCF &PCF

- DCF(distributed coordination function):
  - A class of coordination function where the same coordination function logic is active in ***every station*** in the BSS
  - Both Ad Hoc and Infrastructure mode
- PCF(point coordination function)
  - A class of possible coordination functions in which the coordination function logic is active in ***only one station*** in a BSS
  - Only Infrastructure mode

802.11 CSMA/CA

- SIFS(Short interframe space)
  - Used for an ACK ,CTS, the second or subsequent MPDU of a fragment burst, and by a STA responding to any polling by the PCF.
- PIFS(PCF interframe space)
  - STAs operating under the PCF to gain priority access the medium
- DIFS(DCF interframe space)
  - STAs operating under the DCF to transmit data frames and management frames

802.11 Access Priority

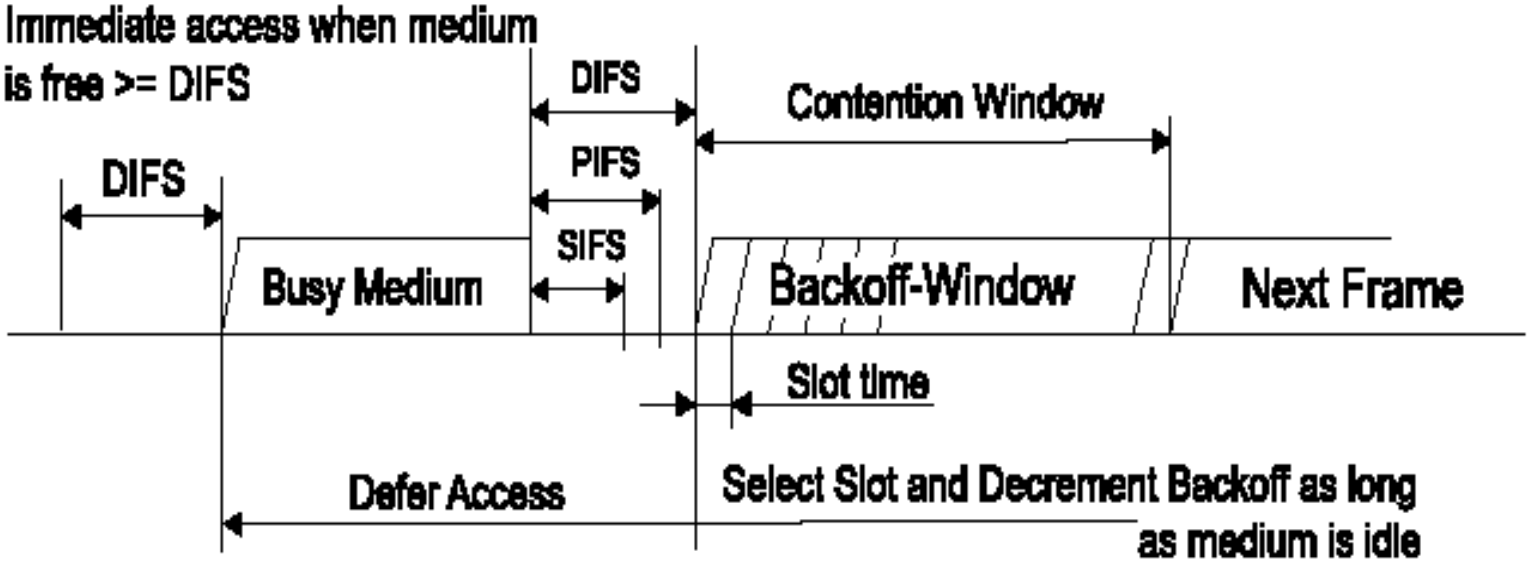
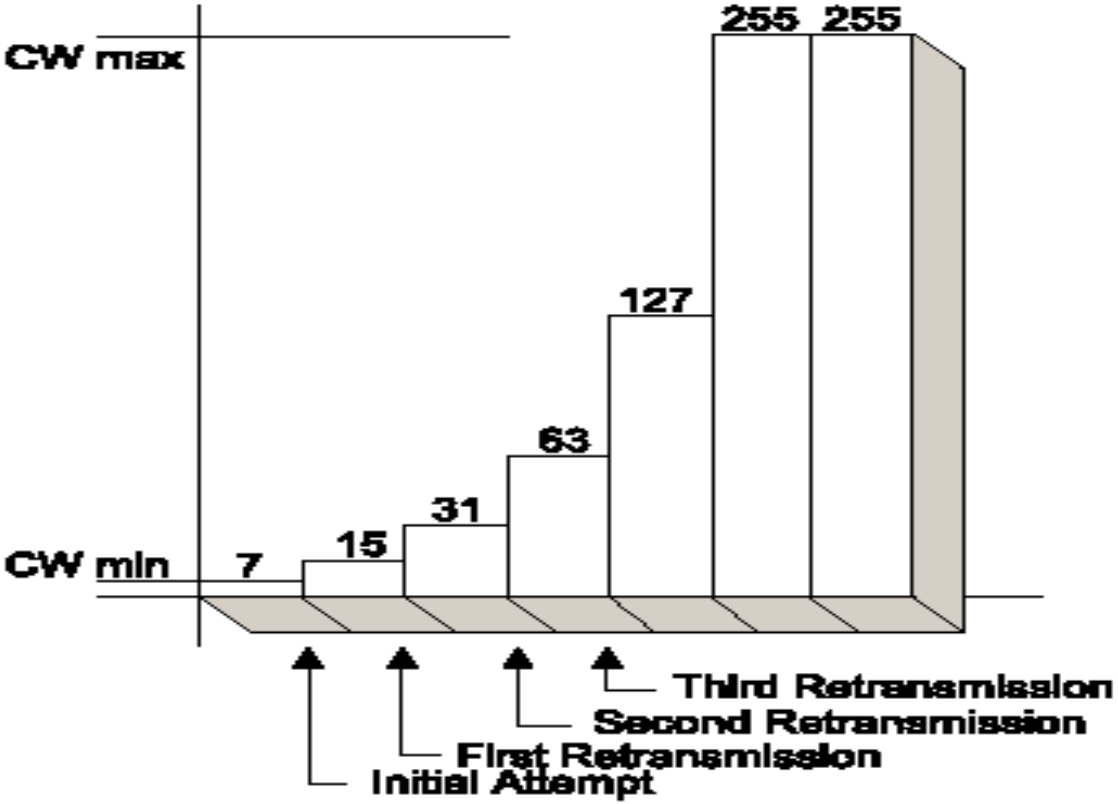


Figure 51—Basic access method

802.11 Contention Window

- Backoff Time = Random * a SlotTime



802.11 Backoff procedure

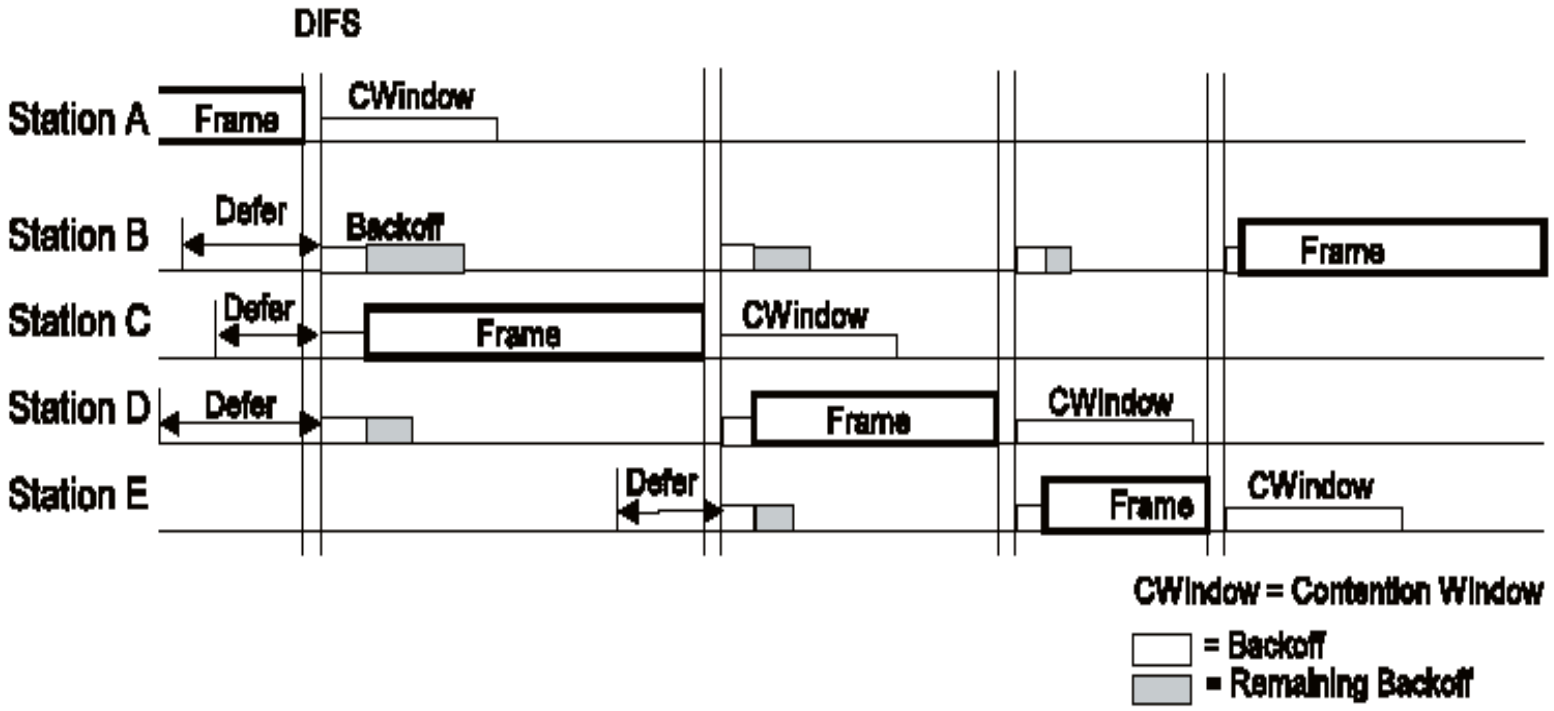


Figure 52—Backoff procedure

802.11 RTS/CTS(Optional)

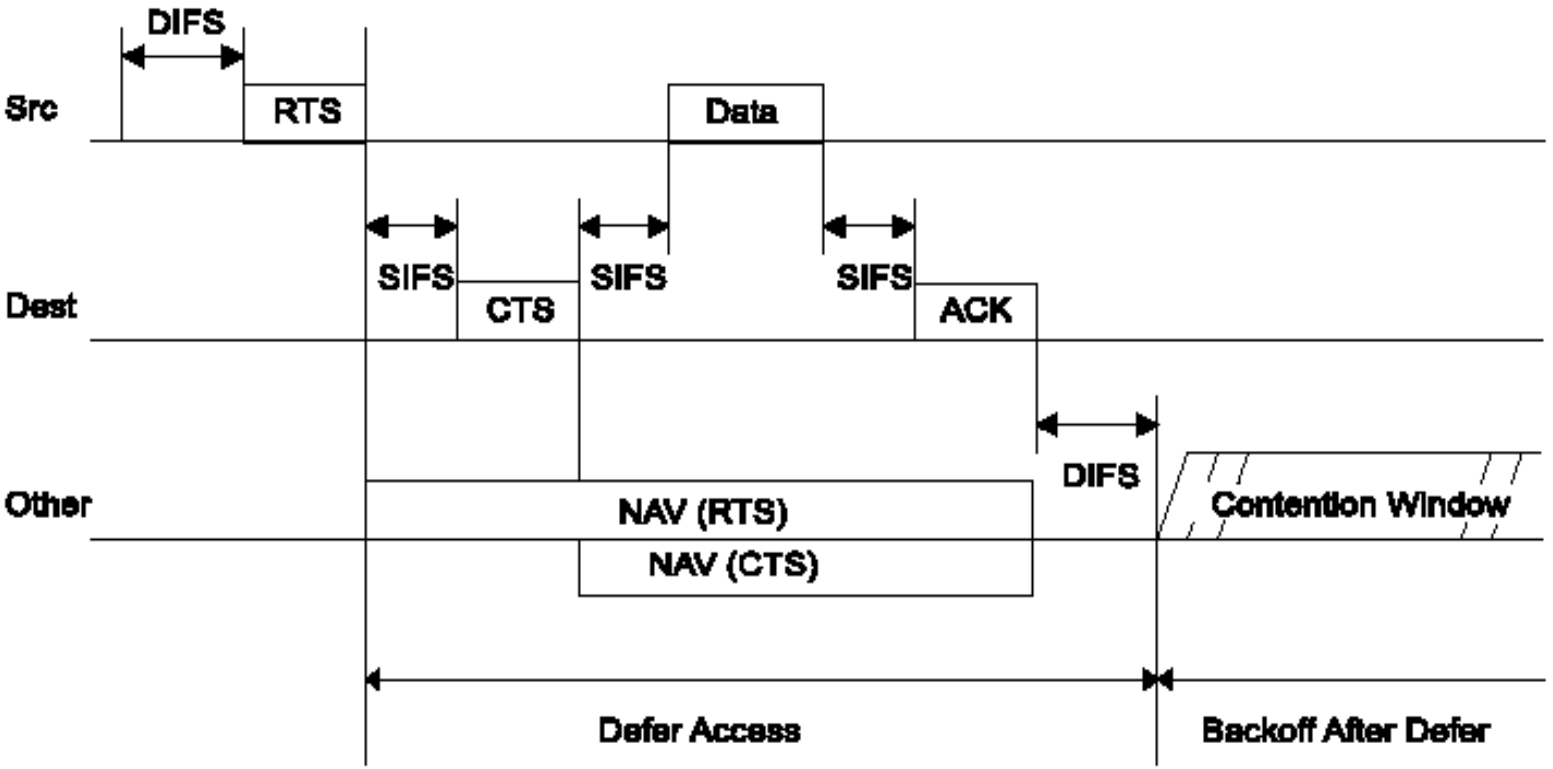
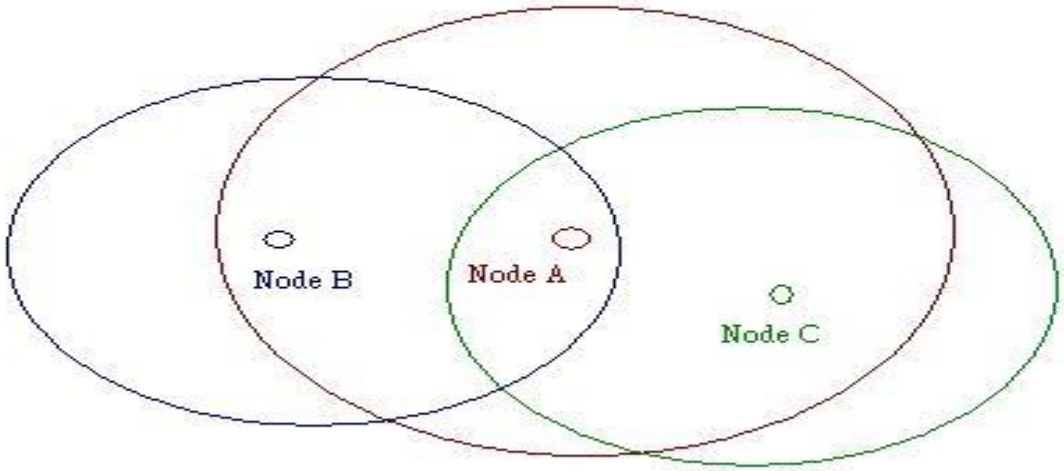


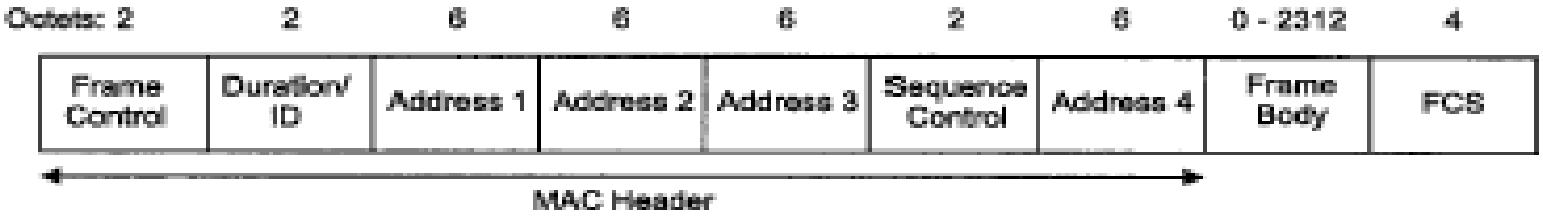
Figure 53—RTS/CTS/data/ACK and NAV setting

Hidden sender problem

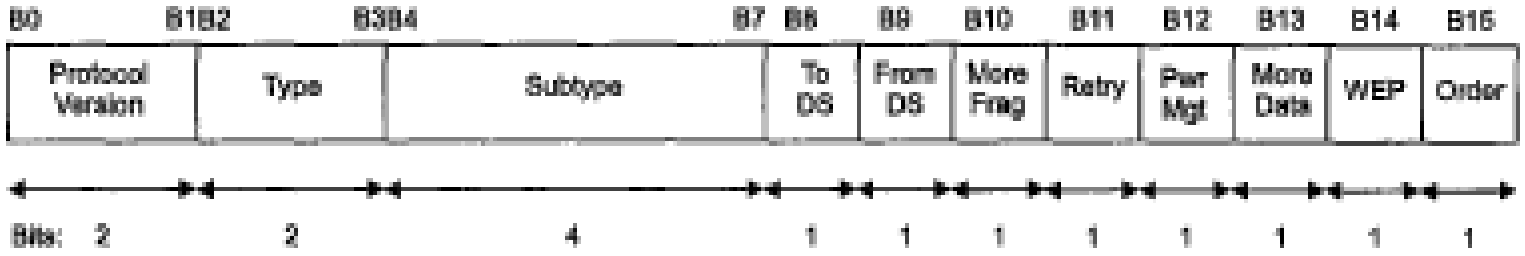


802.11 Mac Frame Format

- Mac frame format



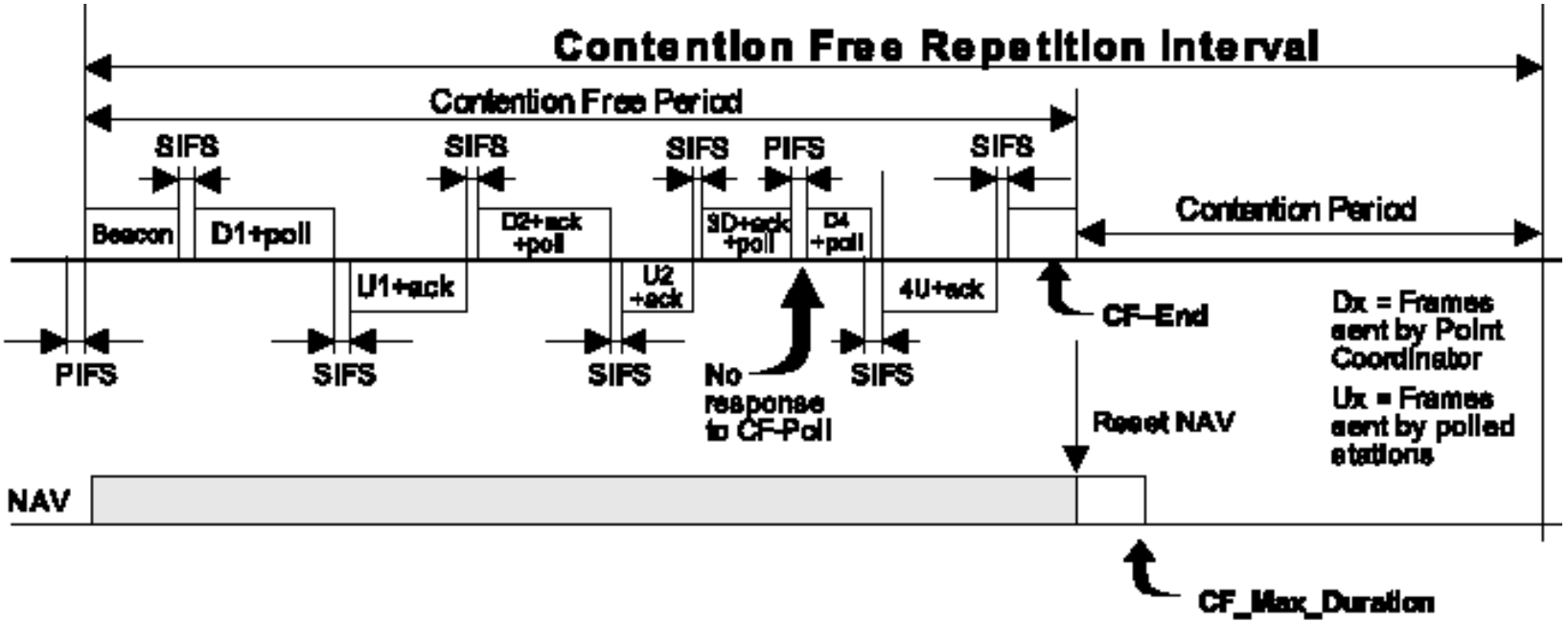
- Frame Control field



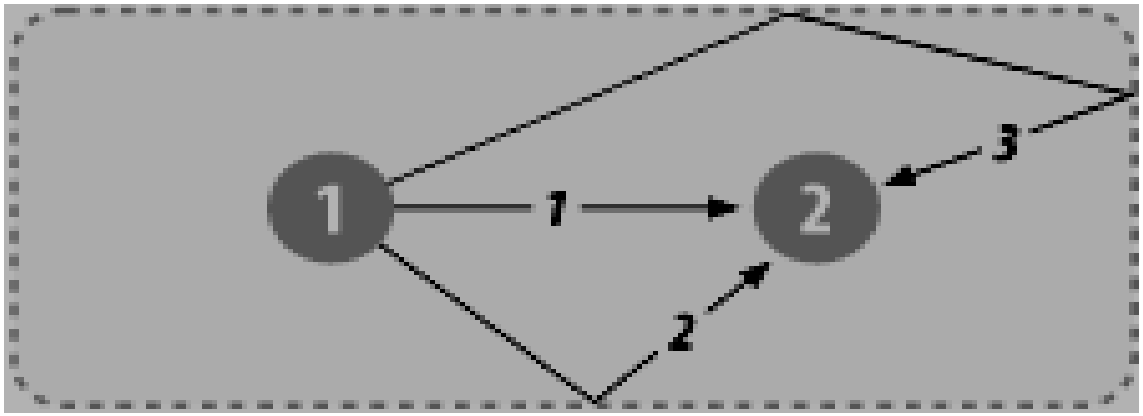
802.11 Mac Frame Type

- Data
  - Handled via the MAC data service path
- Management
  - Handled via the MAC Management Service data path
  - Association request, Authentication…
  - De-association, De-authentication..
- Control
  - RTS, CTS, ACK, Power Save-Poll…

802.11 PCF Transfer Procedure



802.11 Multipath Problem(1)



2.4GHz ≈7.4cm wavelength

5GHz ≈3.8cm wavelength

***Inter-Symbol Interference**

****Out-of-phase impulses garble signal***

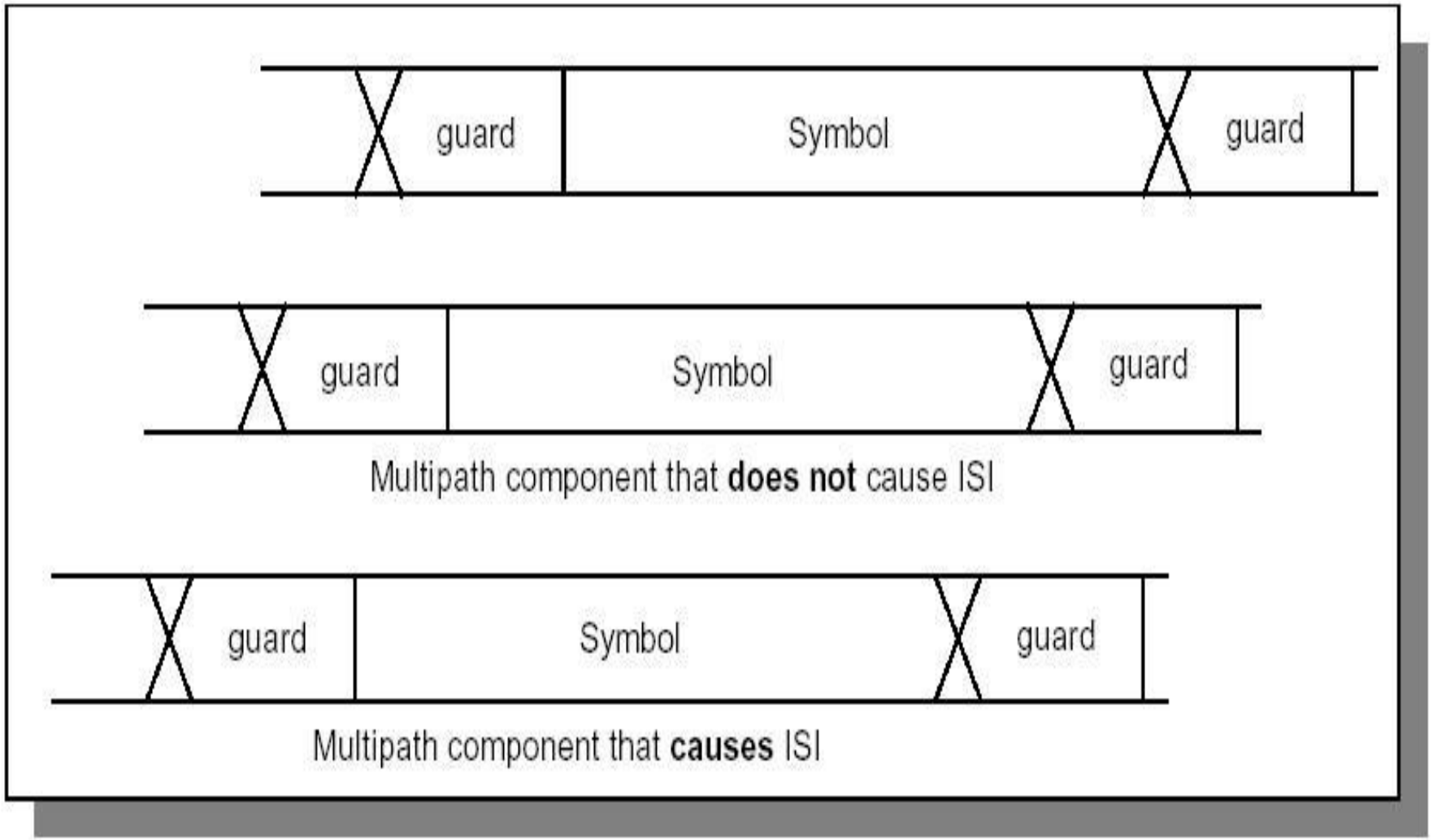
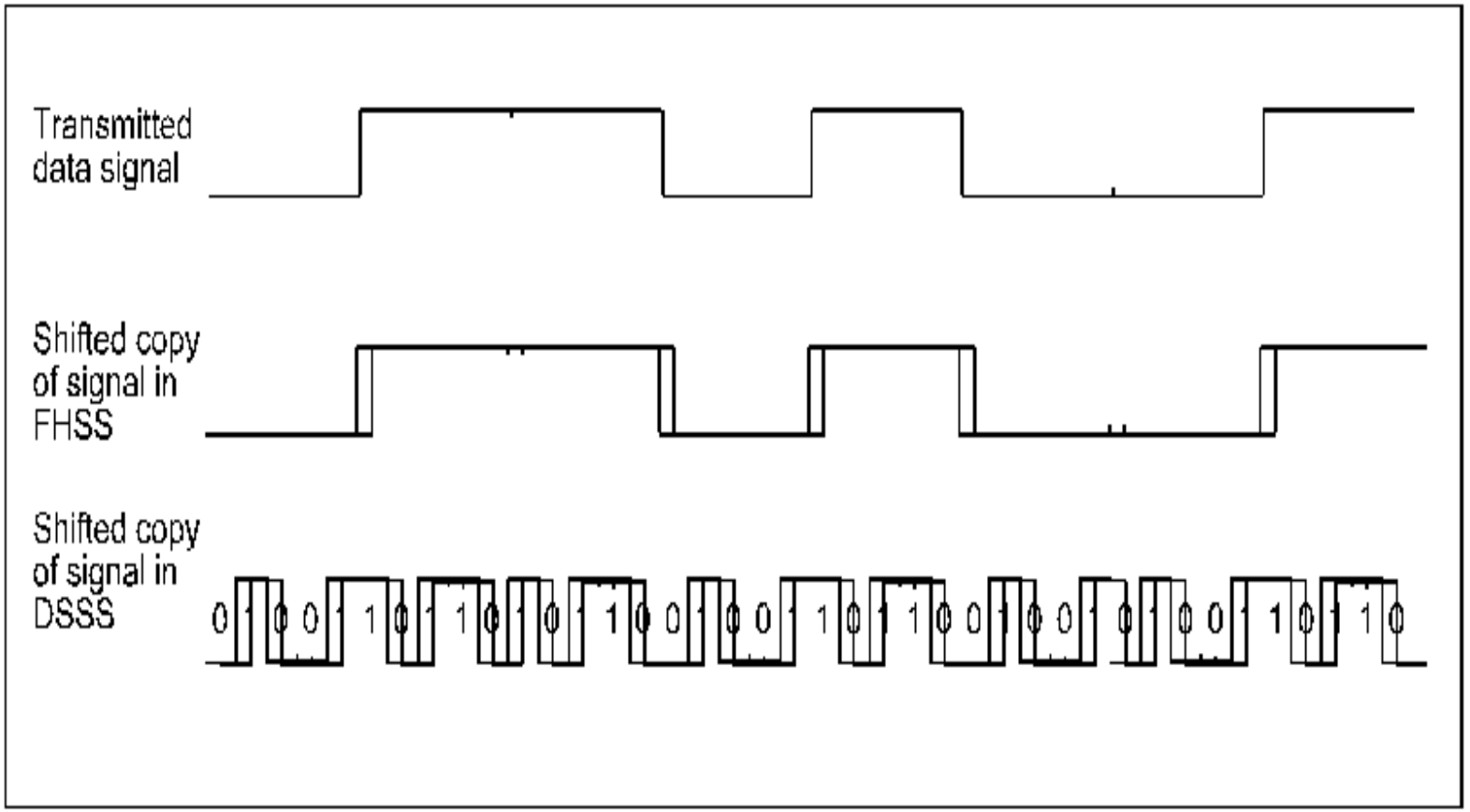


Figure 4 : Guard Time and Cyclic Extension - Effect of Multipath

802.11 Multipath Problem(2)

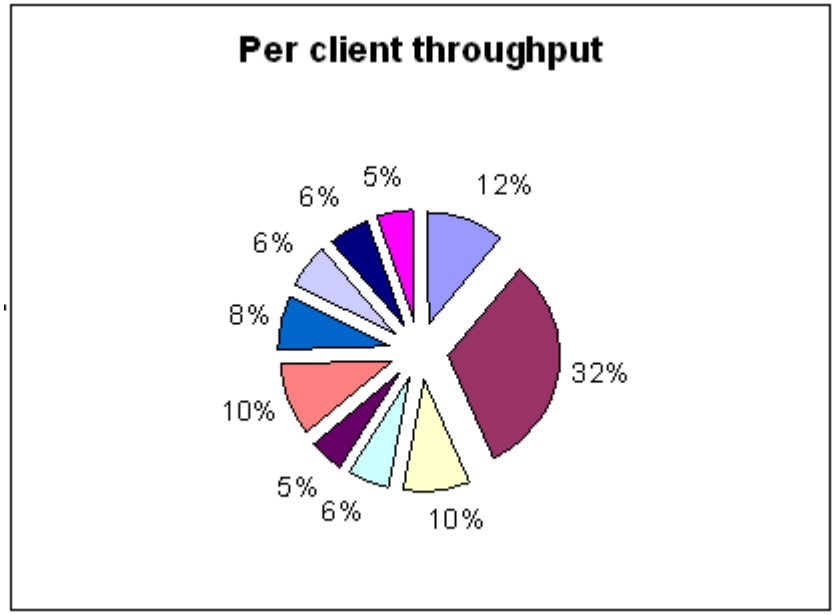


Hot spot problem?

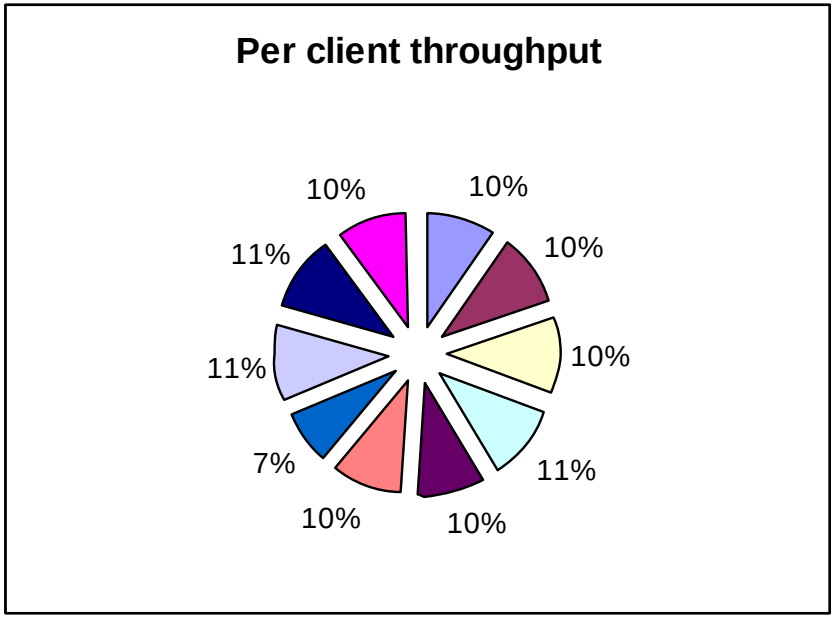
- 一間教室同時有60個人上網,三台ap是否可解決問題?
- Solution 1: maximum users =20/ap ?
- Solution 2: access management system is controlled by switch =>load balance , =>deassociation, deauthentication
- traffic balance or user balance?
- 畢業典禮有沒有解?

Load balance

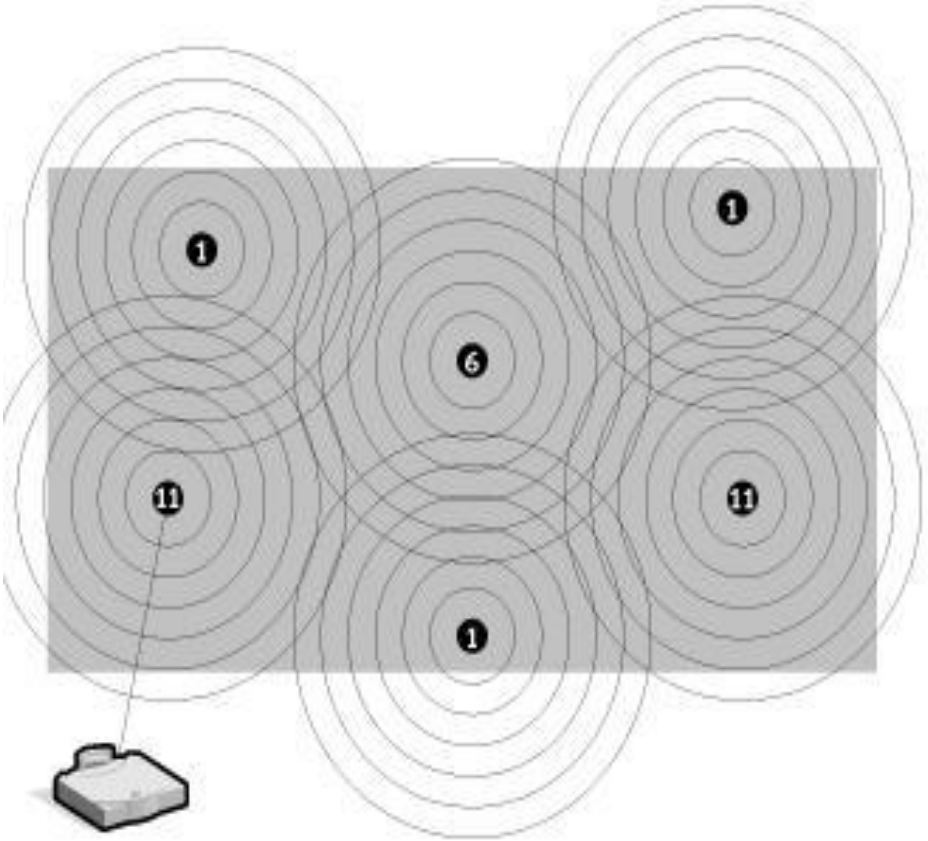
before



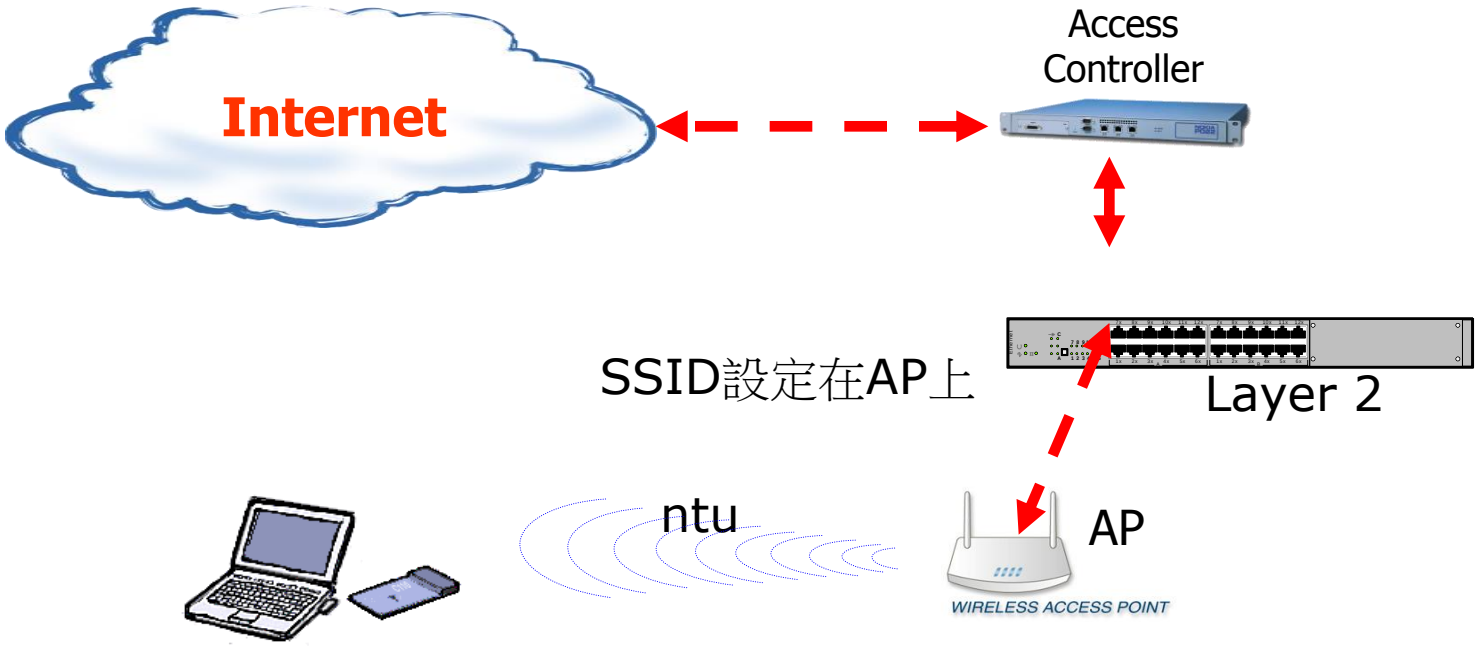
after



802.11 DSSS (Frequency usage example)

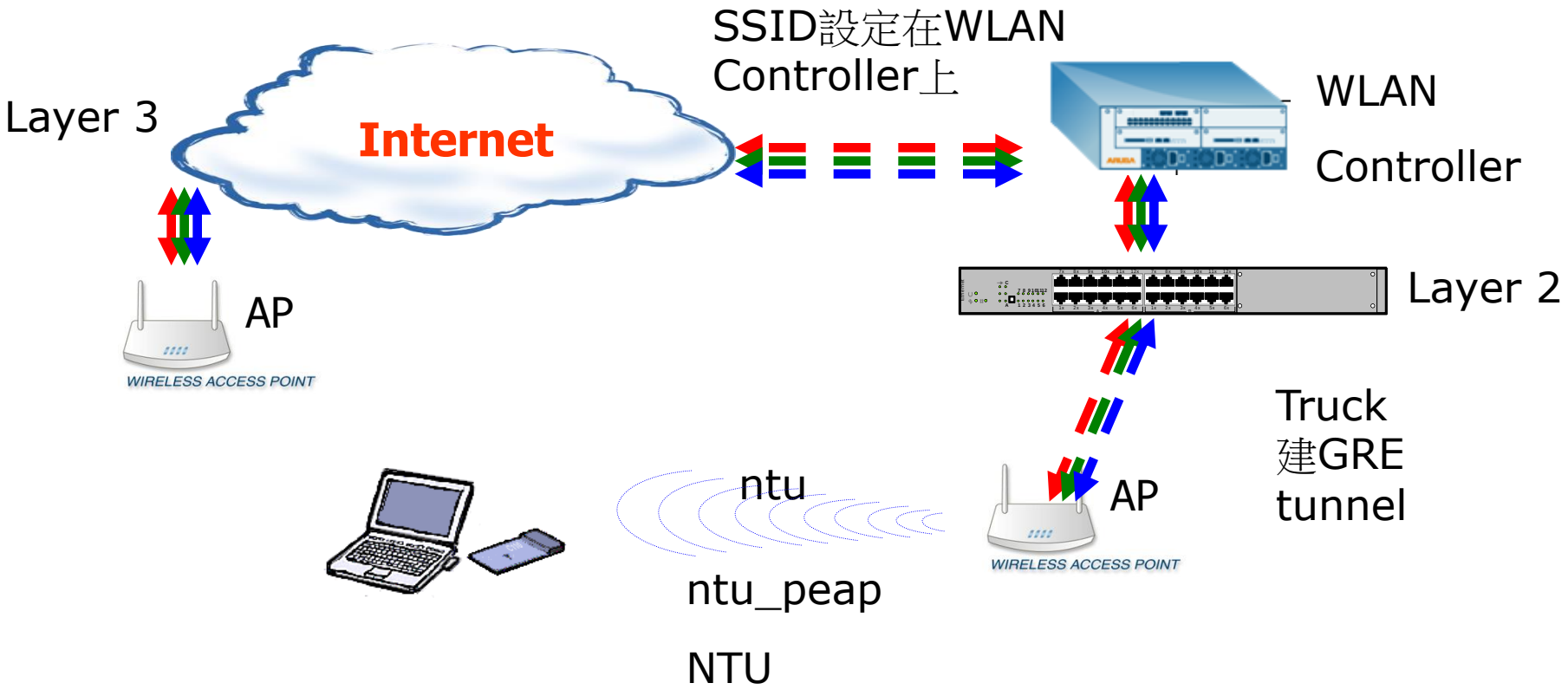


早期無線網路技術(91&93)



95年新購系統為thin AP系統

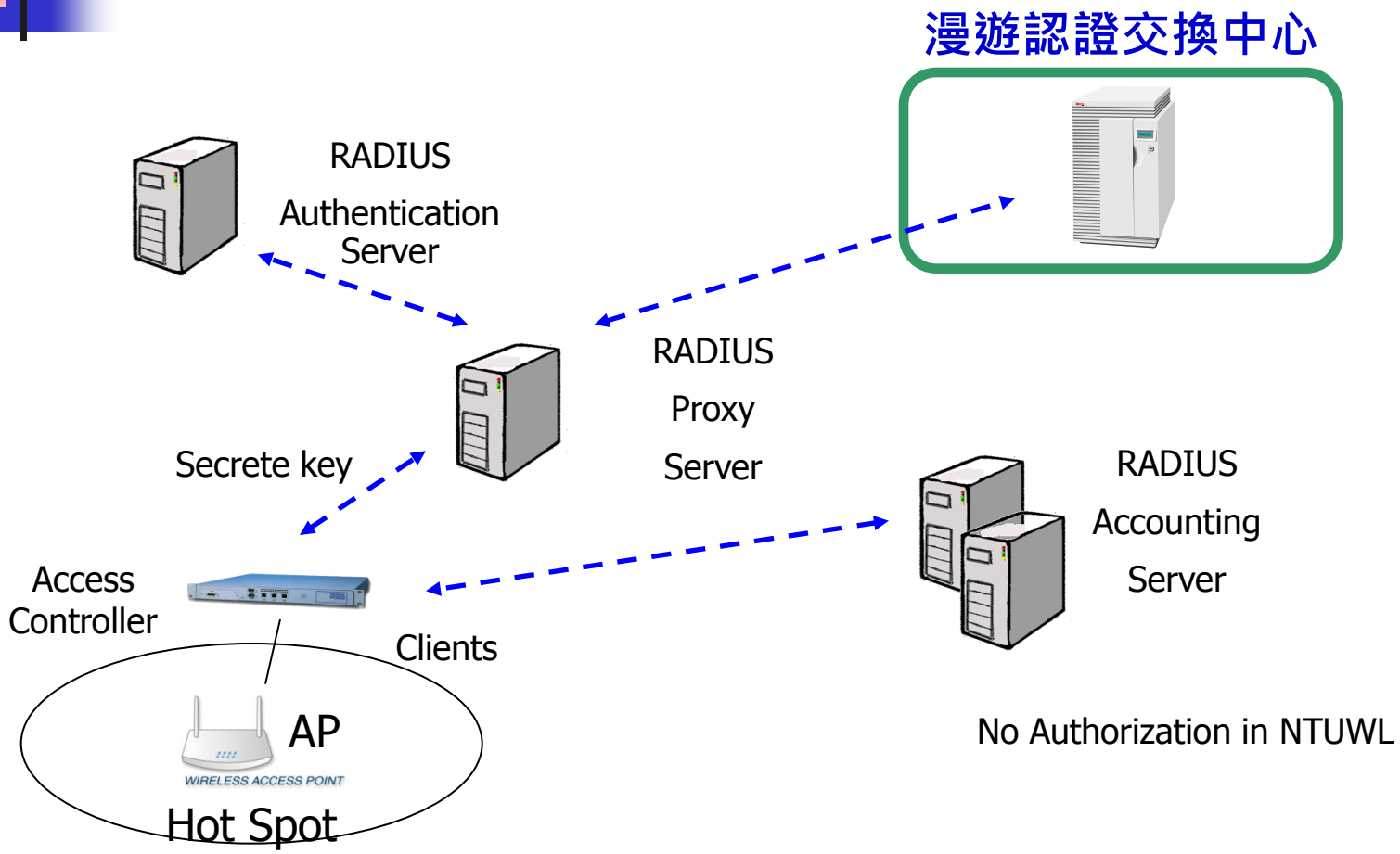
- Nortel,Aruba,CISCO,motorola,D-Link

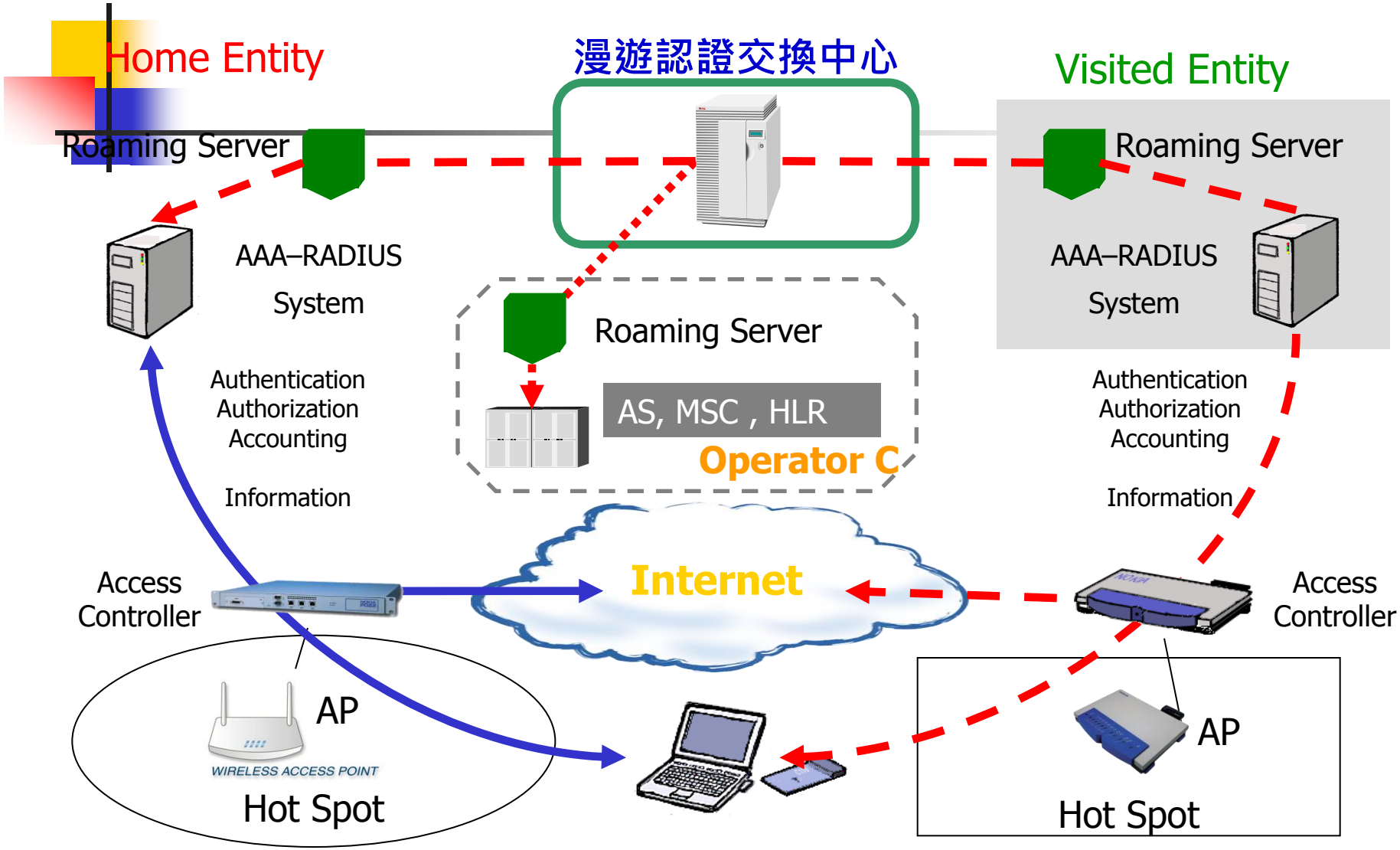


Free Radius

- http://freeradius.org/
- The world's most popular RADIUS Server
- Version 1.1.3才支援vista peap,Version 2.x.x支援wimax
- 主要設定檔有radiusd.conf clients.conf proxy.conf sql.conf(mysql) eap.conf
- DB: mssql.conf postgresql.conf

實際案例


漫遊認證交換中心
RADIUS
Authentication
Server
RADIUS
Proxy
Server
Secrete key
RADIUS
Accounting
Server
Access
Controller
Clients
AP
WIRELESS ACCESS POINT
Hot Spot
No Authorization in NTUWL


Home Entity
漫遊認證交換中心
Visited Entity
Roaming Server
Roaming Server
AAA–RADIUS
System
AAA–RADIUS
System
Roaming Server
AS, MSC , HLR
Operator C
Authentication
Authorization
Accounting
Information
Authentication
Authorization
Accounting
Information
Internet
Access
Controller
Access
Controller
AP
WIRELESS ACCESS POINT
Hot Spot
AP
Hot Spot

802.11n簡介

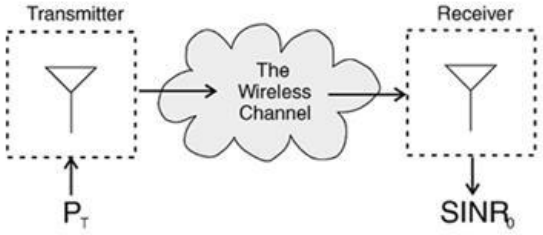
- 四大特色
  - 多輸入多輸出(Multiple-input multiple-output, MIMO)
  - 支援40MHz的頻寬
  - 管理用(overhead)網路封包縮減
  - 802.11n向下相容

多輸入多輸出(Multiple-input multiple-output, MIMO)

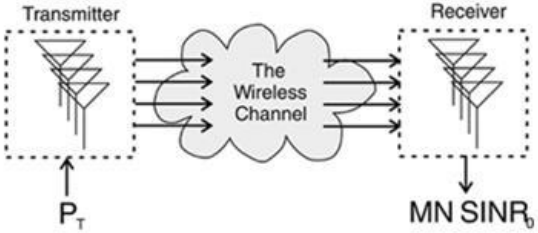
- 多輸入多輸出(Multiple-input multiple-output, MIMO)，多輸入多輸出系統採用天線陣列，利用空間多工技術來提高所使用頻寬的效率。這系統從多個天線發送或在多個天線處接收，採用空間多工，系統能在一個頻率上同時傳輸一個以上的空間數據串流。所以從外表來看，802.11n無線網路基地台的天線數比以前的802.11abg天線多，考慮價格性能比，最佳是3x3的天線陣列，而3x3的天線陣列支援2個空間的串流，傳輸效率直接升成2倍

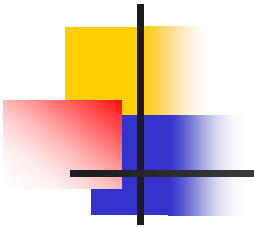
多輸入多輸出(Multiple-input multiple-output, MIMO)

Single In Single out



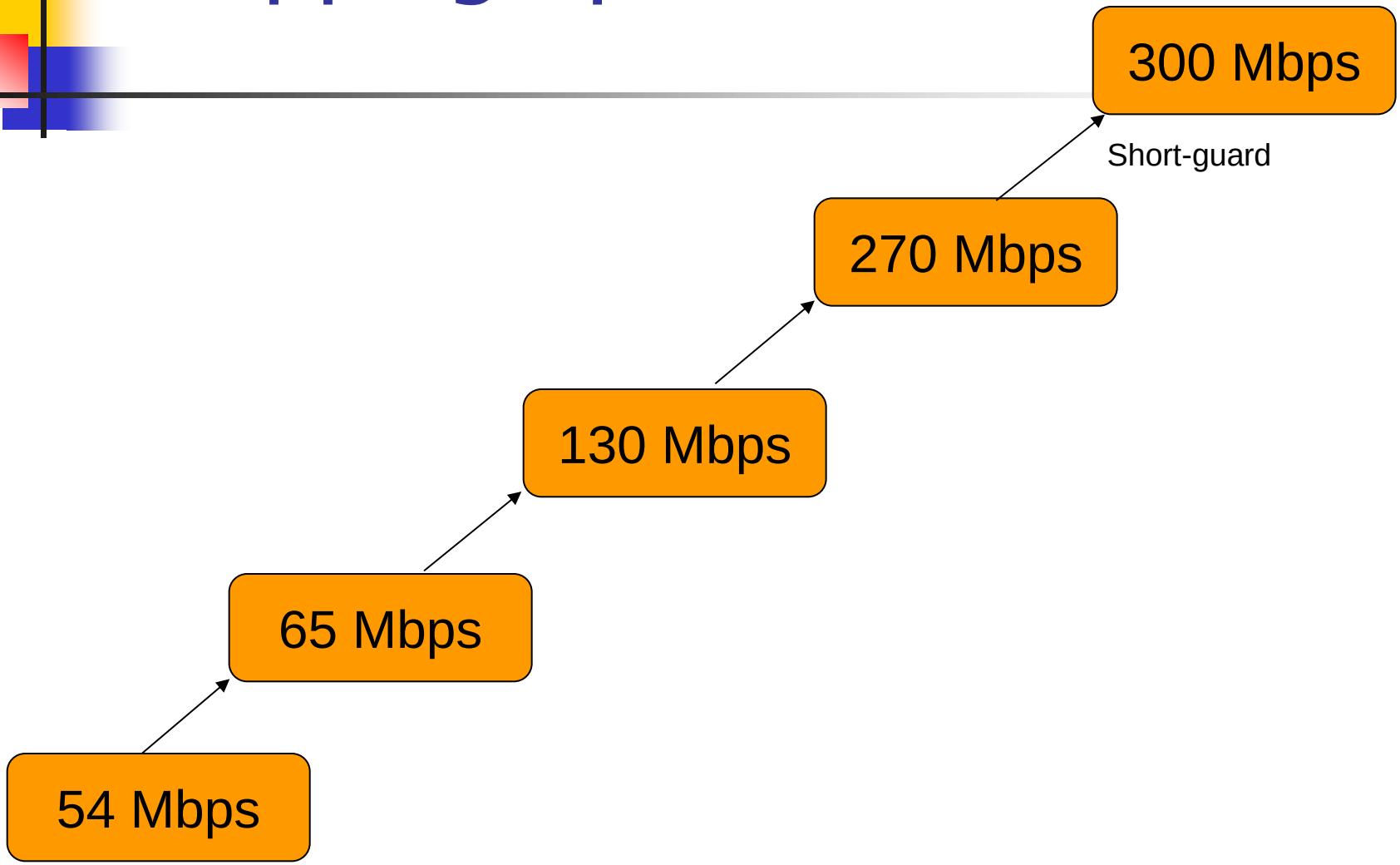
Multiple In Multiple Out





- 支援40MHz的頻寬，原本802.11abg只使用20MHz的頻寬，到了802.11n可使用40MHz的頻寬，傳輸效率直接升成2倍以上。
- 管理用(overhead)網路封包縮減，以及縮短保護間隔(Short Guard Interval)或中框空間的縮減(Reduced Interframe Space)，如此大概可以提升傳輸效率百分之十。

Stepping up to 802.11n - PHY



MCS Index	Number of spatial streams	Modulation	Coding rate	N_{SD}		N_{CBPS}		GI = 800ns		GI = 400ns	
				20	40	20MHz	40MHz	Rate in 20MHz	Rate in 40MHz	Rate in 20MHz	Rate in 40MHz
0	1	BPSK	½	52	108	52	108	6.5	13.5	7 2/9	15
1	1	QPSK	½	52	108	104	216	13	27	14 4/9	30
2	1	QPSK	¾	52	108	104	216	19.5	40.5	21 2/3	45
3	1	16-QAM	½	52	108	208	432	26	54	28 8/9	60
4	1	16-QAM	¾	52	108	208	432	39	81	43 1/3	90
5	1	64-QAM	2/3	52	108	312	648	52	108	57 7/9	120
6	1	64-QAM	¾	52	108	312	648	58.5	121.5	65	135
7	1	64-QAM	5/6	52	108	312	648	65	135	72 2/9	157.5
8	2	BPSK	½	52	108	104	216	13	27	14 4/9	30
9	2	QPSK	½	52	108	208	432	26	54	28 8/9	60
10	2	QPSK	¾	52	108	208	432	39	81	43 1/3	90
11	2	16-QAM	½	52	108	416	864	52	108	57 7/9	120
12	2	16-QAM	¾	52	108	416	864	78	162	86 2/3	180
13	2	64-QAM	2/3	52	108	624	1296	104	216	115 5/9	240
14	2	64-QAM	¾	52	108	624	1296	117	243	130	270
15	2	64-QAM	5/6	52	108	624	1296	130	270	144 4/9	300

802.11n是否在公眾網路佈置

- 802.11bg only 3 of 12 being completely nonoverlapping. 不建議啟用40MHz的頻寬,所以最高速只有144Mbps
- 802.11a has 12 completely nonoverlapping,啟用40MHz的頻寬,所以最高速有450Mbps

802.11b/g exp

APg:ON, APb:OFF(or ON), USERg:ON, USERb:ON→OFF(no download)

7Mbps up to 17Mbps.

台大無線網路 SSID 現況

- NTU(no WEP Key)支援802.11n
- ntu_peap(WPA2 key)支援802.11n
- ntu(WEP Key)不支援802.11n
  - 預計於2014年9月1日停用ntu

Ref. from Intel

intel

商用 | 家用 | 產品 | 技術支援 | 關於Intel

下載 | 工具與資源 | 保固 | 社群 | 說明

機器翻譯免責聲明

查看此頁面的英語原版。

選擇不同的產品

請引導我完成
識別您的產品
搜尋驅動程序
搜尋文件
搜尋產品規格

您是否認為這個資訊對您有幫助嗎？

是 否

如果您有其他意見，敬請告訴我們。

剩餘字符： 300

提交

我們非常感謝您所有的意見，但無法提供客服或技術支援。請不要輸入聯繫資訊。如果您需要我們的回應，與我們聯繫。

無線網路連線

英特爾無線產品

當 WEP 或 TKIP 加密配置資料速率將不會超過 54 Mbps

症狀：

用戶端設備 Wi-fi 的資料率不會超過 54 Mbps 當有線等位私密 (WEP)，或配置時間性金鑰完整性協定 (TKIP) 加密。

原因：

IEEE * 802.11 n 草案禁止作為單播加密 WEP 或 TKIP 使用較高的輸送量。如果您使用這些加密方法（例如，WEP、 WPA TKIP），您的資料率將下降到 54 Mbps。最新的英特爾® 無線配接器用戶端驅動程式連接使用舊式的 IEEE 802.11 g 連接，而不是不能連接，共有符合 IEEE 802.11 n 草案。

http://www.intel.com/support/tw/wireless/wlan/4965agn/sb/cs-025643.htm

Ref. from Apple

http://support.apple.com/kb/TS3361?viewlocale=zh_TW&locale=zh_TW

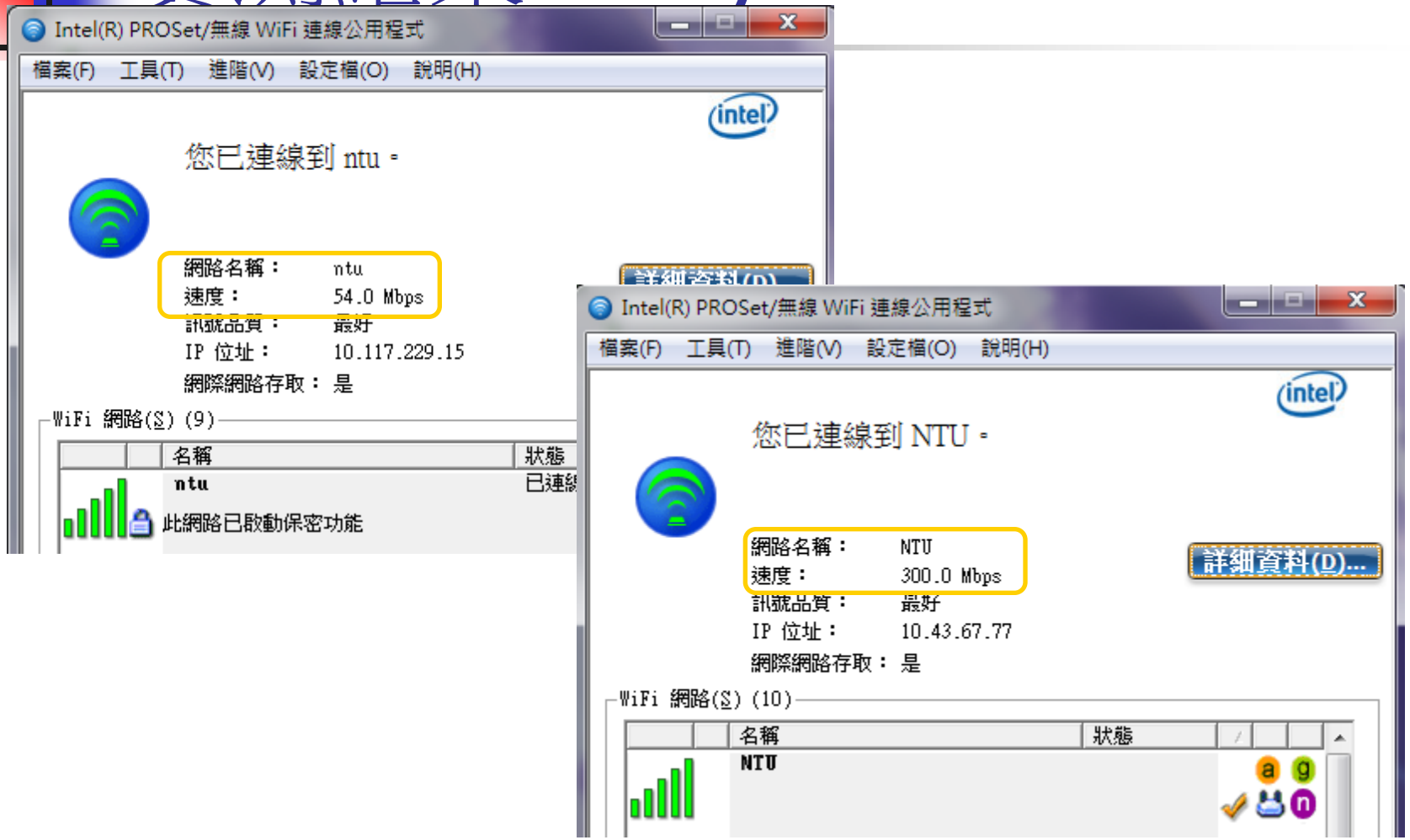
Ref. from 2009, Wi-Fi Alliance

Wi-Fi CERTIFIED n devices must also pass the following Wi-Fi CERTIFIED programs:

- Wi-Fi CERTIFIED 802.11a, Wi-Fi CERTIFIED 802.11b/g (depending on frequency bands supported) to verify legacy modes of operation,
- Wi-Fi Multimedia (WMM) to verify the device implements essential QoS mechanisms, and
- WPA2 security including EAP types (extensible authentication protocol) for the latest generation of security protections.

© 2009, Wi-Fi Alliance

實測結果 Sony NB


Intel(R) PROSet/無線 WiFi 連線公用程式
檔案(F) 工具(T) 進階(V) 設定檔(O) 說明(H)
intel
您已連線到 ntu。
網路名稱： ntu
速度： 54.0 Mbps
訊號品質： 最好
IP 位址： 10.117.229.15
網際網路存取： 是
WiFi 網路(S) (9)
名稱
狀態
ntu
已連線
此網路已啟動保密功能
Intel(R) PROSet/無線 WiFi 連線公用程式
檔案(F) 工具(T) 進階(V) 設定檔(O) 說明(H)
intel
您已連線到 NTU。
網路名稱： NTU
速度： 300.0 Mbps
訊號品質： 最好
IP 位址： 10.43.67.77
網際網路存取： 是
詳細資料(D)...
WiFi 網路(S) (10)
名稱
狀態
NTU

新聞案例

- 受害人:電信總局副局長
- 時間:93年7月16日自由時報第11頁

- 發生在93年7月16日，受害人多達30幾位，其中有一位是熟稔電信網路業務的電信總局副局長，事件大致是兩位嫌犯利用30幾位被害人家中的無線網路溢波，利用偽卡盜刷購買線上遊戲及色情光碟……等，並轉售牟利，藉以躲避警方查緝。

卡皇熱賣

- 在98年10月14日，內容是有關最近相當流行的產品——卡皇，此一產品的功能，竟是盜用私人的家中無線路網路金鑰（WEP key）的工具，使用者安裝後能自動搜索周遭無線網路，然後破解其網路金鑰上網，引起網友爭相搶購！
- 後來警察取締
- 20100628, 盜用無線上網 最重罰150萬!

無線網路安全嗎?

- 家裏無線網路會被盜用嗎?**傳輸內容**會外漏嗎?
- 在學校用無線網路**帳號密碼**會外漏嗎?
- 在學校用無線網路**傳輸內容**會外漏嗎?
- 無線網路電波對人有無傷害嗎?

既有AP Encryption

- 40bit/64bit/128bit/152bit WEP
- TKIP (Temporal Key Integrity Protocol)
- AES (Advanced Encryption Standard)
- WPA　(802.11i draft) ,2004
- WPA2 (802.11i) ,2006

https簡介

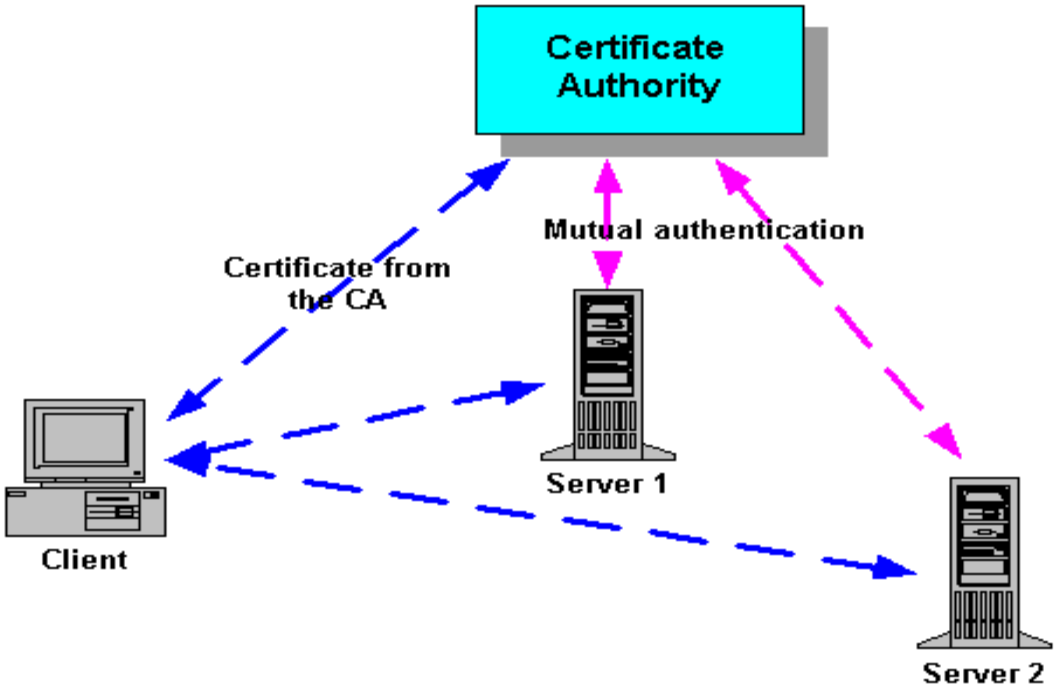
- 約2012年前,商用憑證採用1024bits(309 decimal digits)公論,二年換一次
- 美國政府規定,2012以後,商用憑證採用2048bits公論,可三年換一次
- 看NTU PORTAL教學

公開鑰匙加密法破解時間

Number of Decimal Digits	Approximate Number of Bits	Data Achieved	MIPS-years	Algorithm
100	332	April 1991	7	quadratic sieve
110	365	April 1992	75	quadratic sieve
120	398	June 1993	830	quadratic sieve
129	428	April 1994	5000	quadratic sieve
130	431	April 1996	500	generalized number field sieve

- 140 465 Feb 1999 2000
- 155 512 Aug 1999 8000

憑證中心


Certificate Authority
Mutual authentication
Certificate from the CA
Server 1
Client
Server 2

校園常見的無線網路安全(一)違法使用無線網路

- 校園無線網路比較常發生的是寄廣告信，侵犯智慧財產權；而駭客最喜歡用的無線網路是不需經過認證的無線網路，例如學校師生常自行架設無線網路，並使用完全沒有更改出廠設定之無線網路存取點，就很容易被駭客利用作違法的事，而最後背黑鍋的是架設無線網路存取點的師生。

校園常見的無線網路安全(二)竊聽(Eavesdropping)

- 竊聽是指入侵者針對無線網路通訊內容進行監控，利用竊聽內容來獲取被害人的個人資料如帳號／密碼等；最常見的例子是於無線網路登入時竊取被害人的登入帳號密碼。
- telnet PTT

校園常見的無線網路安全(三)通訊分析(Traffic Analysis)

- 流量分析是針對無線網路通訊的流量、內容、以及行為等等進行分析，透過通訊內容或者流量的分析可以獲得目標網路可觀的資料， 如：伺服器位址、通訊模式等等。

校園常見的無線網路安全(四)偽裝(Masquerade)

- 偽裝是指攻擊者架設欺騙使用者的非法偽裝無線網路系統。 例如：攻擊者可任意設需要認證之無線網路識別碼(SSID, Service Set Identifier)，如偽裝台大校園無線網路ntu系統，騙取被害人的計中帳號密碼後，登入學校使用計中帳號密碼認證的任何系統。

校園常見的無線網路安全(五)
服務阻斷攻擊(Denial of Service)

- 服務阻斷攻擊大概是大家最耳熟能詳的攻擊方式，攻擊者透過各種可能的方法 (ICMP flooding、UDP flooding等等方式)使得使用者與管理者無法取得系統資源及服務。不過受限於無線網路使用者的頻寬遠低於後端的有線設備的網路頻寬，所以遇到服務阻斷攻擊時，無線網路正在使用的其他使用者不會輕易發覺。不過有另外一種服務阻斷攻擊是利用IP協定的漏洞，如攻擊者自己當DHCP server，讓使用者要IP時得到不正確的IP；又如攻擊者透過ARP(Address Resolution Protocol)告訴使用者攻擊者電腦是預設閘道(Default Gateway) ，這時使用者的流量皆到攻擊者電腦，被害人就無法使用無線網路。

家用AP設定注意事項

- 無線網路預設出廠名稱(SSID)一定要改
- SSID 廣播(Broadcast)一定要關掉(Disable)
- 安全模式(Security Mode)請設定為WPA2+AES
- 金鑰更新時間(key renewal)愈短愈好
- 限定特定網卡才能使用這個AP