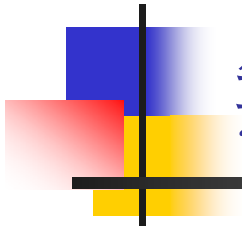
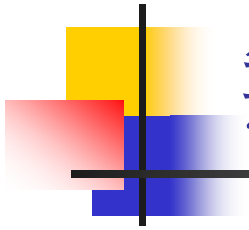


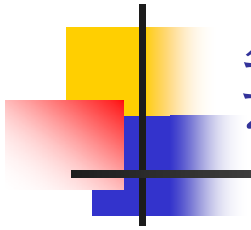
無線網路管理與RADIUS協定簡介

台大計資中心
曾保彰
E-mail：bjtseng@ntu.edu.tw



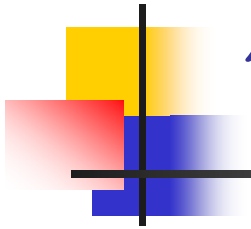
無線區域網路介紹

- 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 省下約20%之網路架設費用,機動性高,擴充性大.but網卡價錢較高,速度問題,相容性問題,資通安全問題,干擾問題.



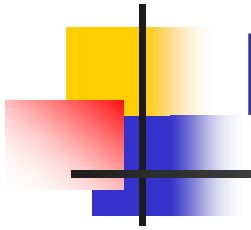
無線網路存取技術

- 窄頻微波技術(Narrowband Microwave)
  - 需付費使用,如GSM(Global System for Mobile Communications), 3G
- 展頻技術(Spread Spectrum)
  - ISM:2.4-2.4835GHz, 5.25-5.35GHz,5.725-5.825GHz
- 紅外線技術(Infrared,IR)
  - 700-1500nm



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
  - 2.5G GPRS
  - 3G WAP
- 802.16(WiMAX)



Bluetooth

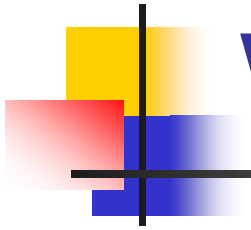
- Bluetooth 1994年由Ericsson 發展
- Bluetooth提供短距離、無線、低價、高度整合、群體溝通及語音數據之資訊傳輸環境.一個設備最多可與七個設備連結傳輸.
- 使用ISM的2.4G頻段

新興行動通訊科技(一)

- GSM泛歐式數位行動電話系統
  - GSM900MHz,GSM1800MHz,GSM1900MHz
- GSM最高9.6kbps,壓縮後13.4kpbs, HSCSD(High Speed Circuit Switched Data)修改軟體進行時槽整合可達38.4kps.
- GPRS(General Packet Radio Service)可達115kbps.

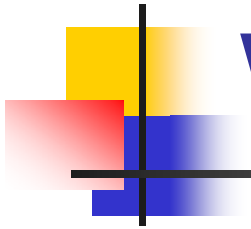
新興行動通訊科技(二)

- 3G, 2Mbps
- WCDMA(wideband code division multiple access)是3G的一種協定,可達2Mbps, (歐州)
- CDMA 2000 (美國)
- PHS(personal handphone system), NTT輕型手提無線電話,64k-128k
- TD-SCDMA (大陸)



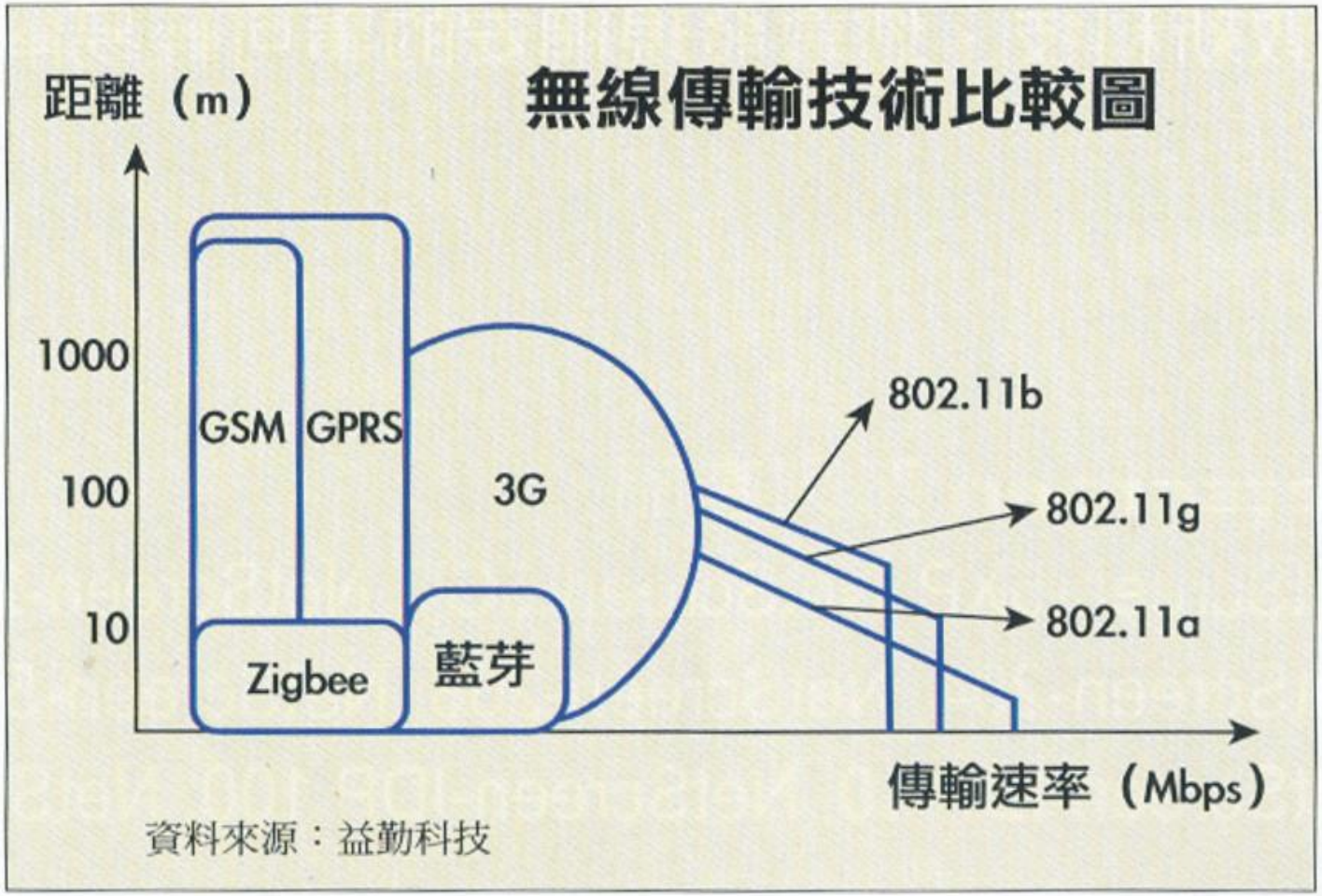
WiMAX

- **W**orldwide **I**nteroperability for **M**icrowave **Acc**ess
- IEEE 802.16e
- 70Mb/s
- OFDM
- Replace ADSL
- 50km
- But GSM業者卻看好Long Term Evolution (LTE)



Wireless Network

- GSM,PHS,3G …
  - Mobility&Range High
  - Data rate low(<2Mb/s)
  - High cost
- Wireless Lan 802.11a/b/g….
  - Mobility&Range low
  - Data rate High(>11Mb/s)
  - Low cost


無線傳輸技術比較圖
距離（m）
1000
100
10
GSM
GPRS
3G
Zigbee
藍芽
802.11b
802.11g
802.11a
傳輸速率（Mbps）
資料來源：益勤科技

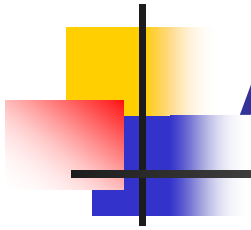
Wireless AP 電波問題

- 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)



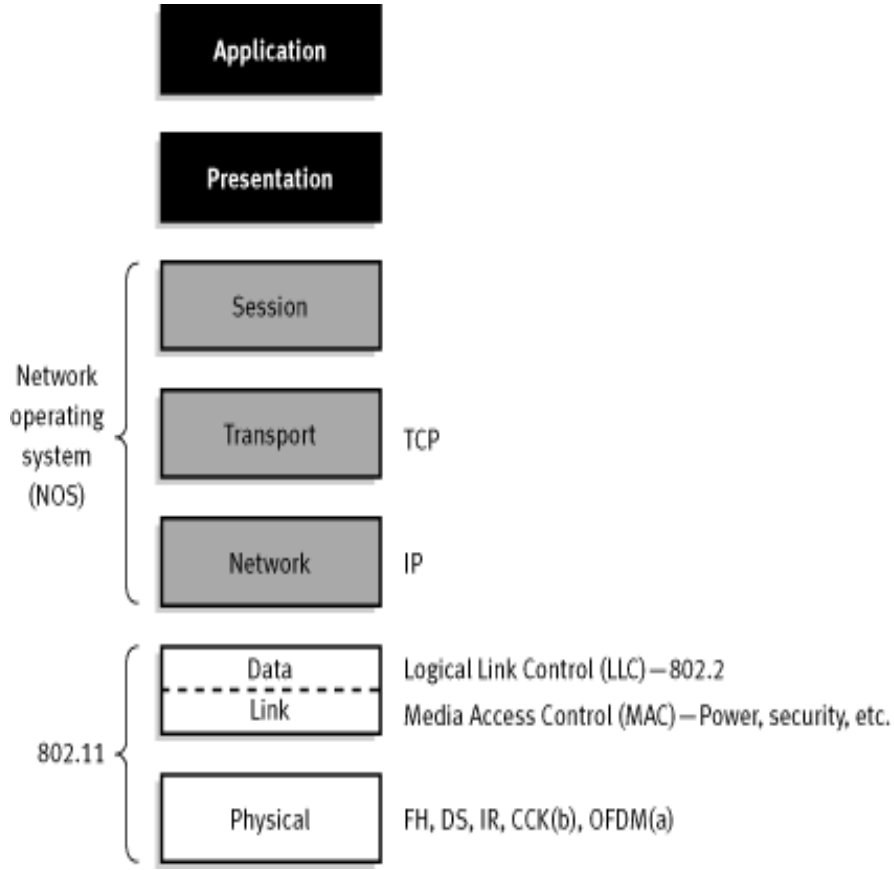
ANSI/IEEE 802.11

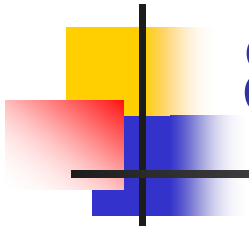
Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications

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

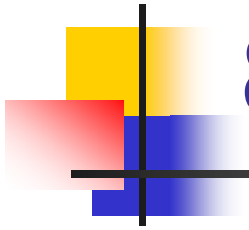
802.11 ISO Model





802.11 Componets(1)

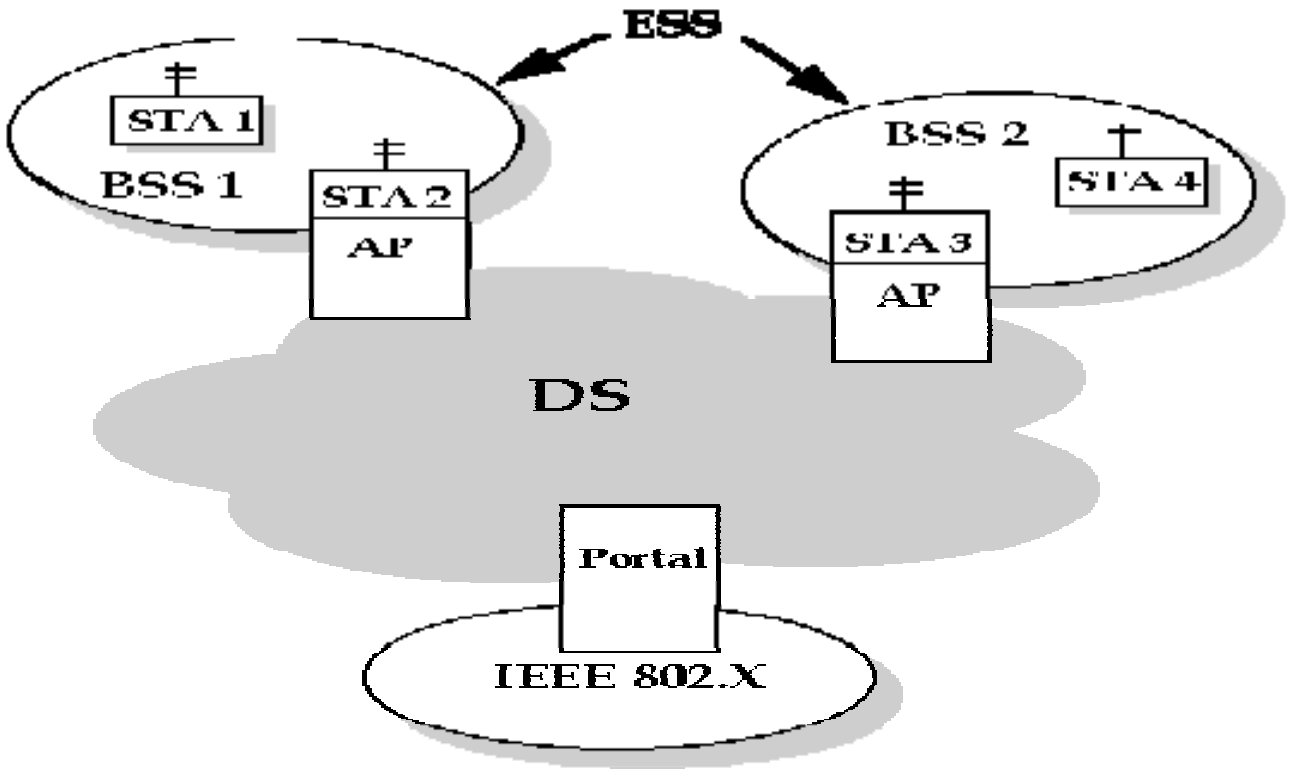
- Wireless Medium(WM)
  - The medium used to implement a wireless LAN
- Station(STA)
  - Any device that contains an 802.11 conformant MAC and PHY interface to the wireless medium
- Station Service
  - The set of services that support transport of MSDU(Mac Service Data Units) between Stations within 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

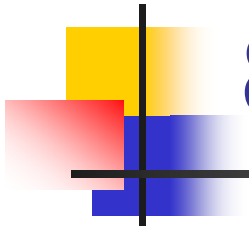


802.11 Componets(2)

- **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

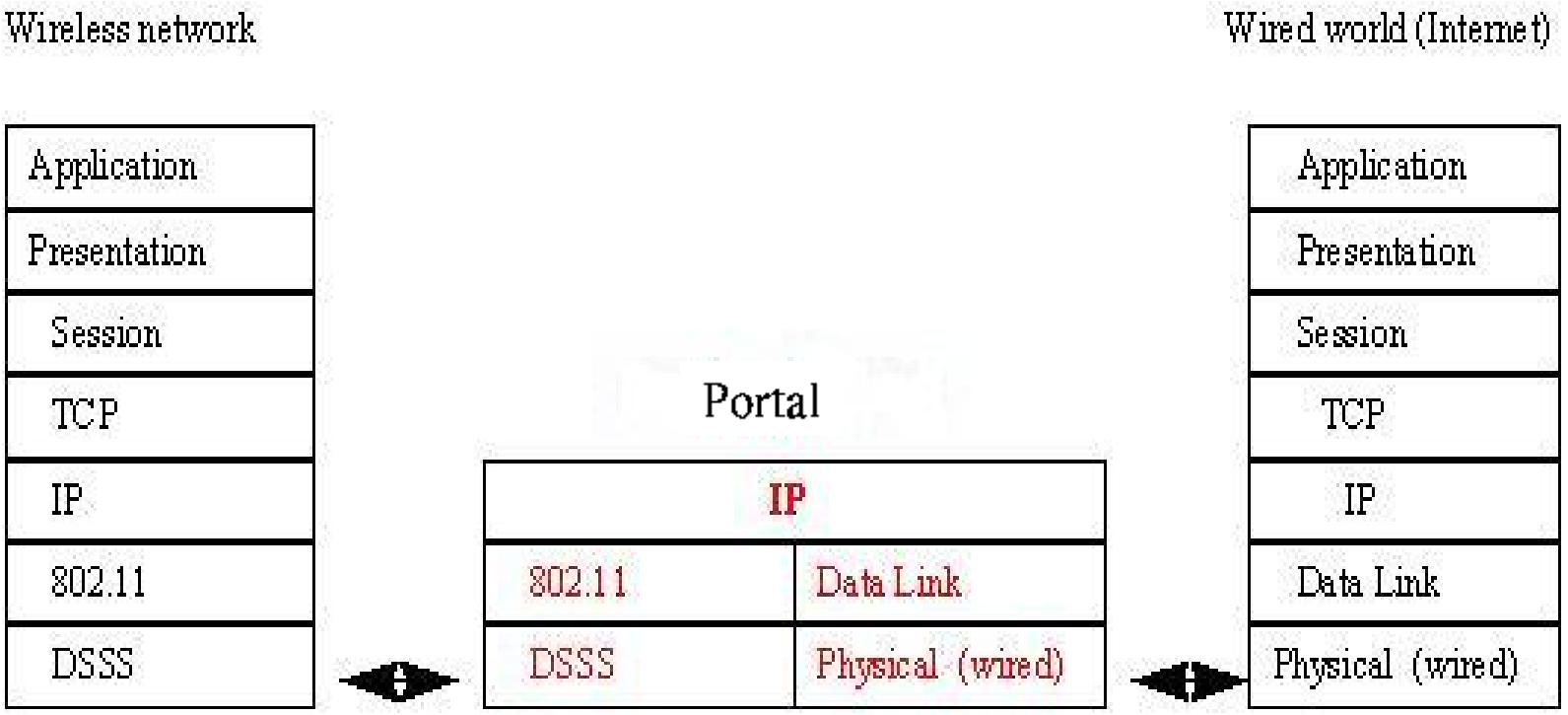




802.11 Services

- 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

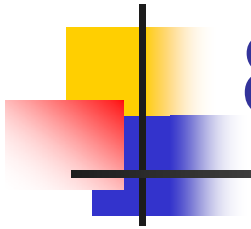


802.11 Phy(1)

- 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

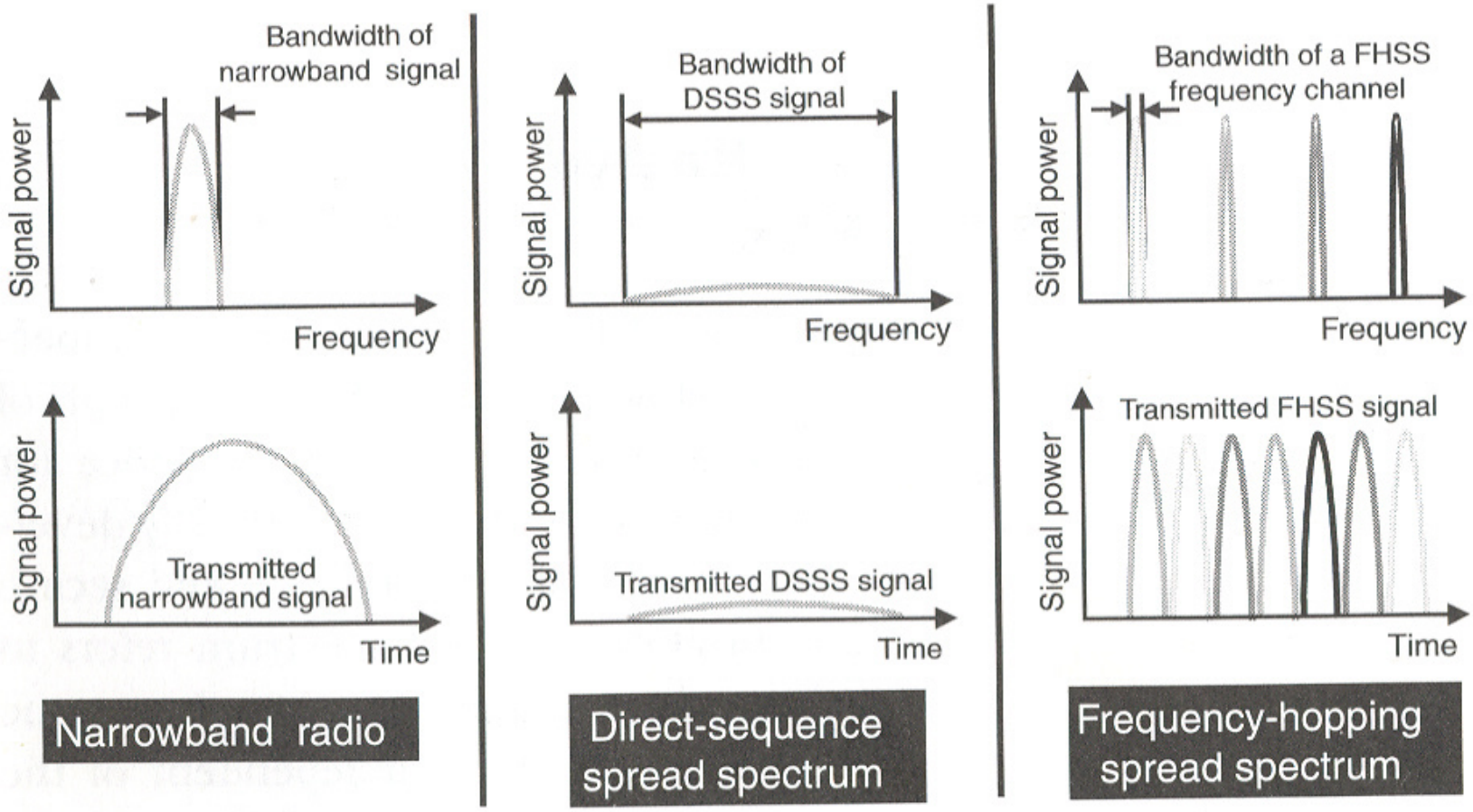


Figure 2.1 Narrowband radio, DSSS, and FHSS.

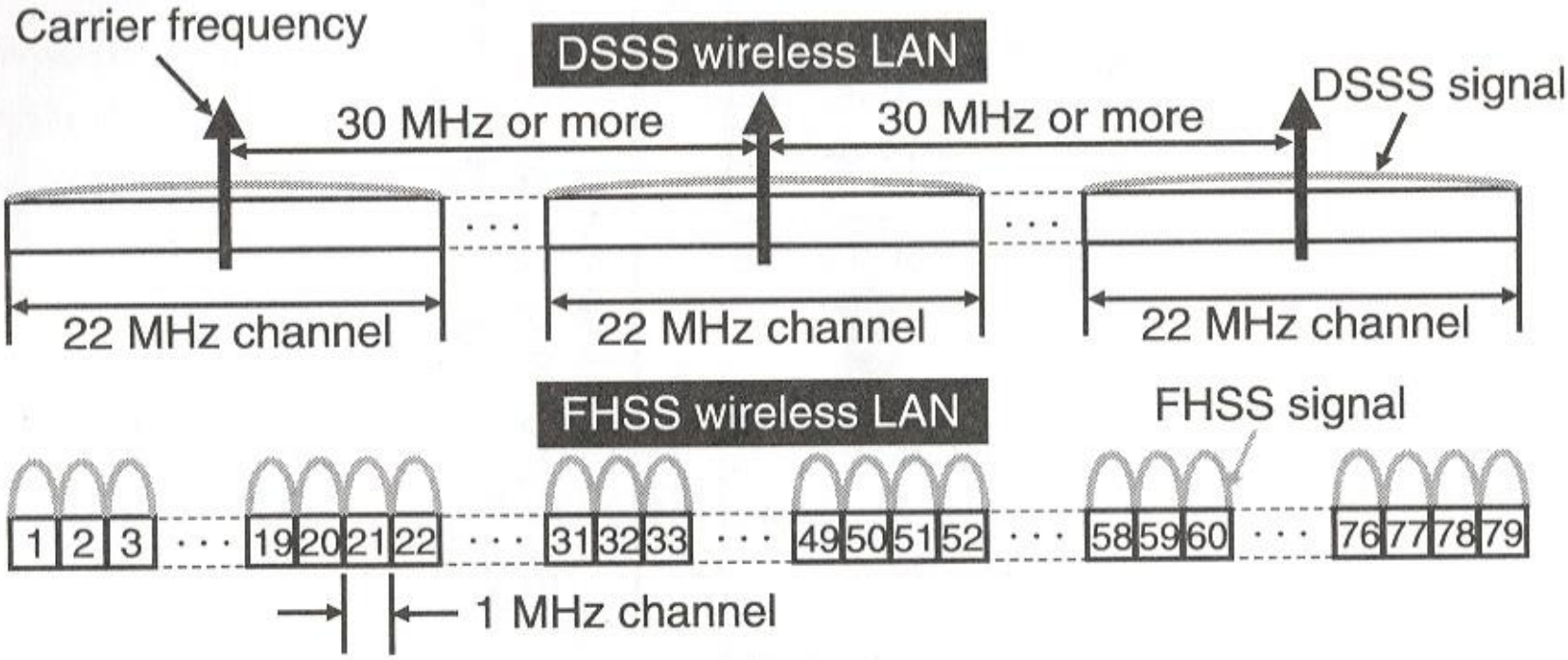


Figure 2.10 Frequency channels for 2.4 GHz DSSS and FHSS

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

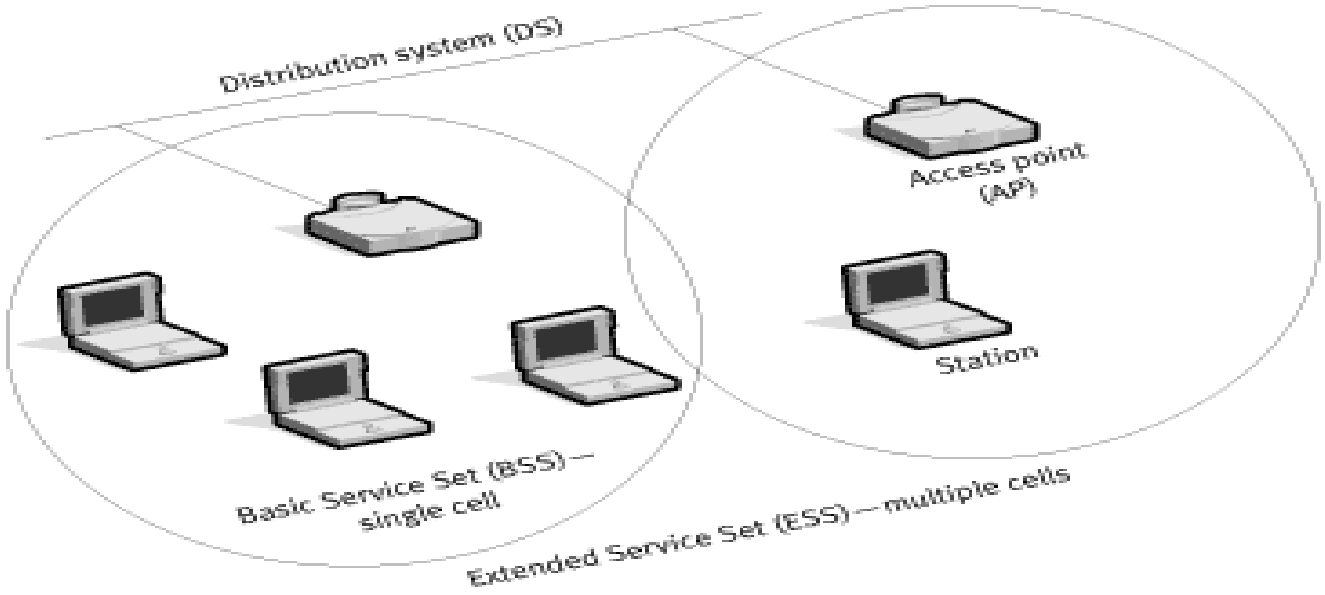
- 802.11b=802.11g:2.4-2.4835GHz (total:83.5MHz)(3 non-Overlapping CH)
- 802.11a:5.15-5.25GHz,5.25-5.35GHz,5.725-5.825GHz,(total 300MHz) (12 non-Overlapping CH)
- Center frequency: 5.18,5.20,5.22,5.24,5.26,5.28,5.30,5.32, 5.745,5.765,5.785,5.805
- Ch.36..Ch.161

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

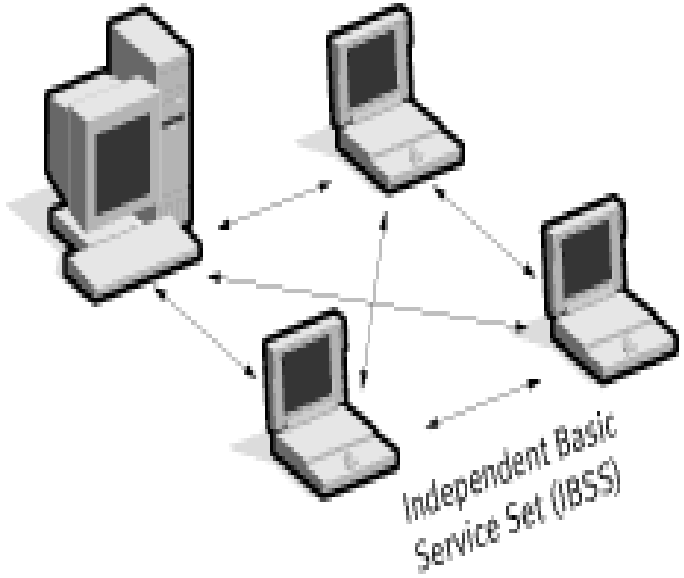
- The wireless network consists of at least one access point connected to the wired network infrastructure



802.11

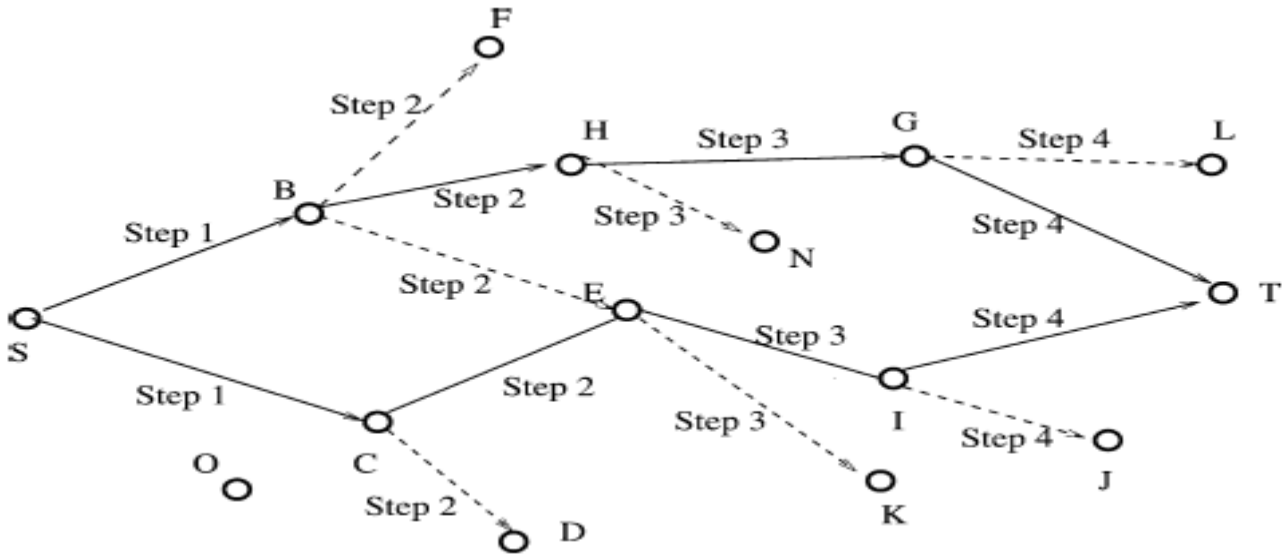
Ad hoc mode

- 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



Wireless Mesh Network

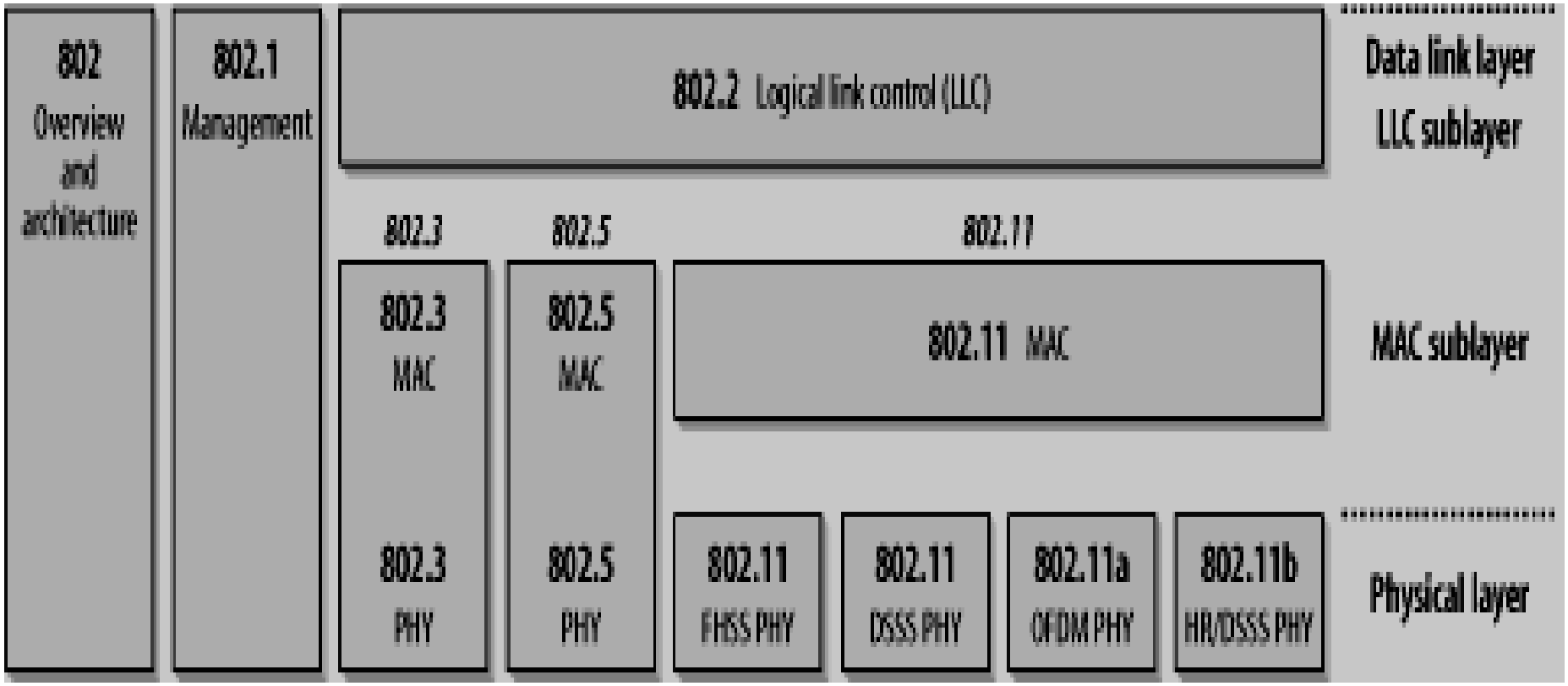
- A hot research subject from 2001
- Using Ad hoc Network mode
- Routing protocol : OSPF



802.11 LLC & MAC

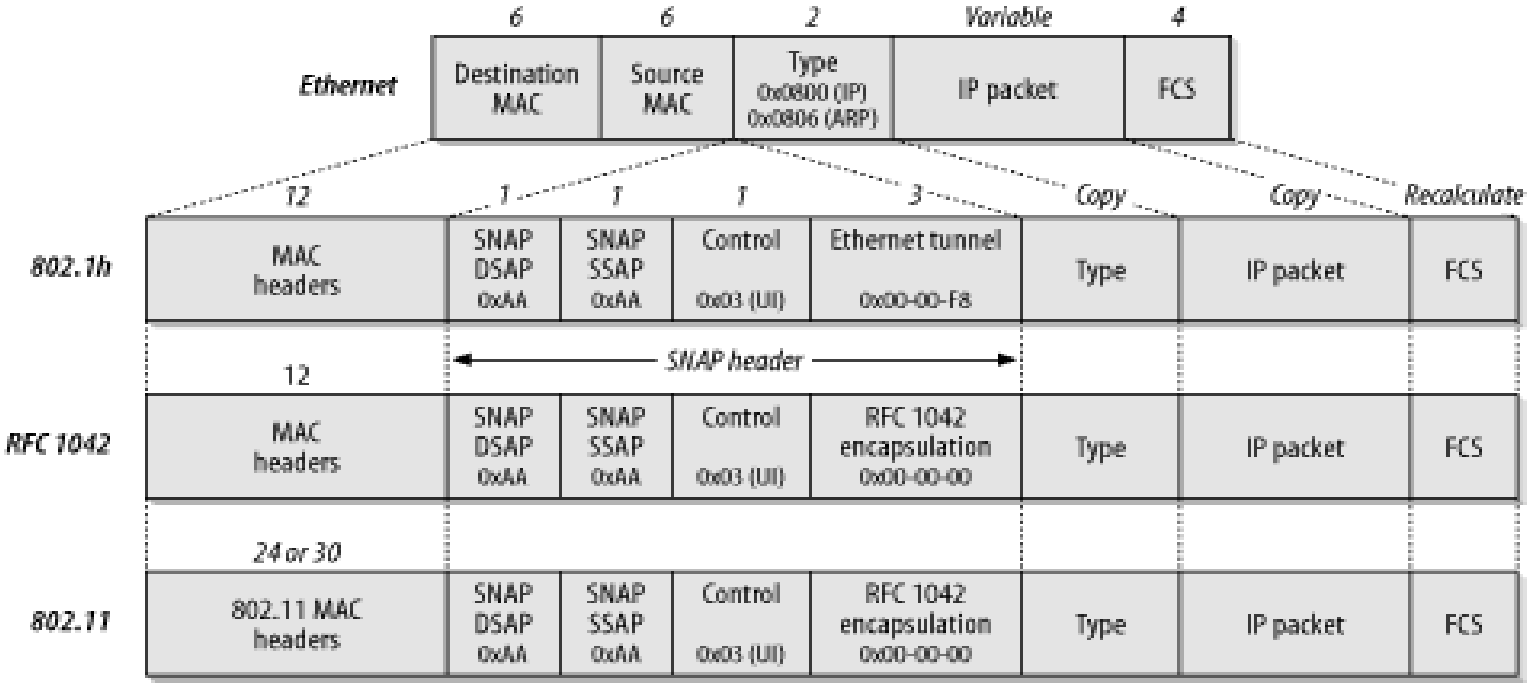
- LLC-Logical Link Control
  - The same 802.2 and 48 bits addressing
  - MAC is different
- CSMA/CA(Carrier sense multiple access/collision avoidance)
  - By using explicit packet ACK, which means an ACK is sent by receiving station to confirm that the data packet arrived intact.

IEEE Group 802

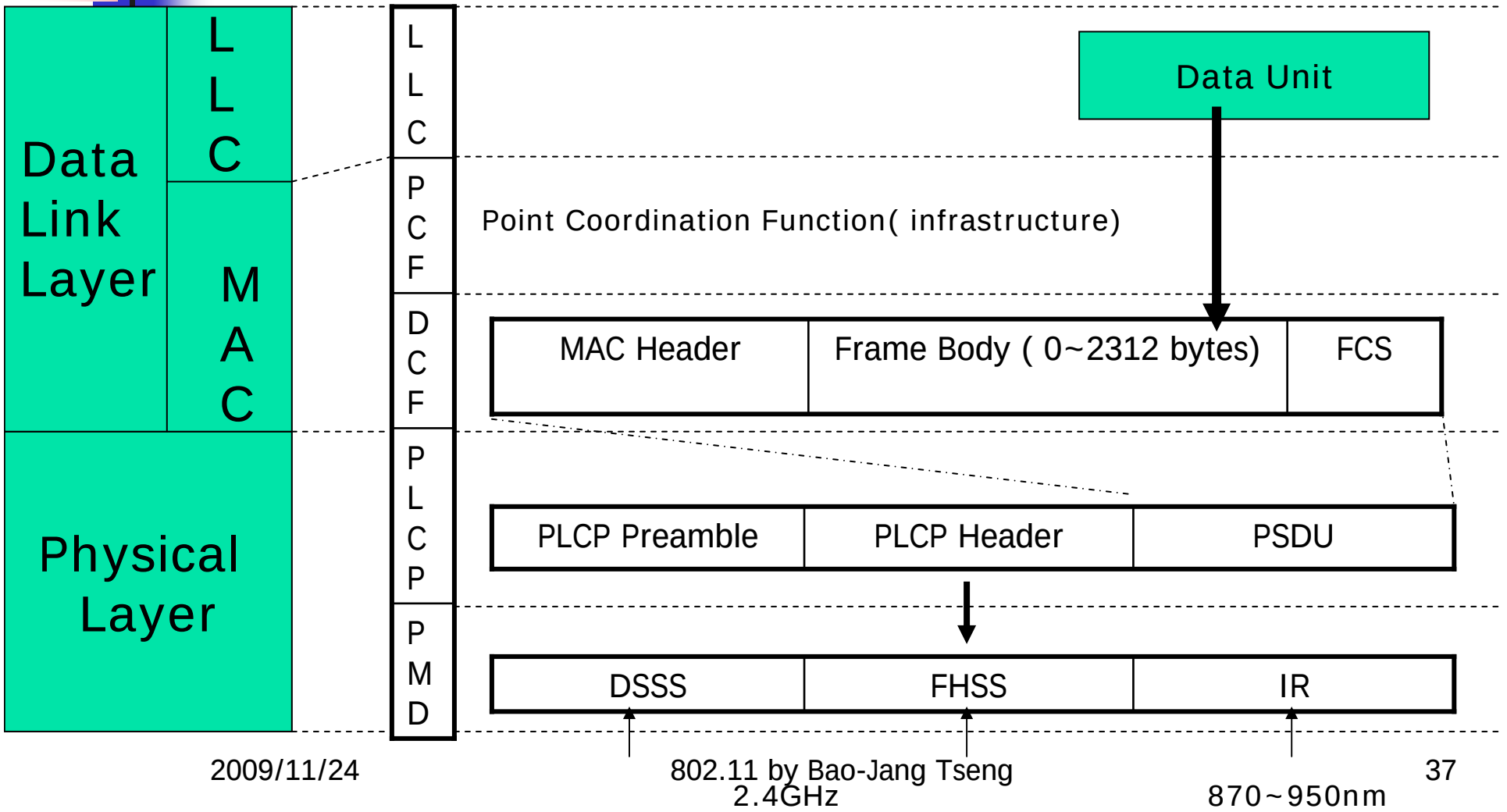


Carry Existing Traffic

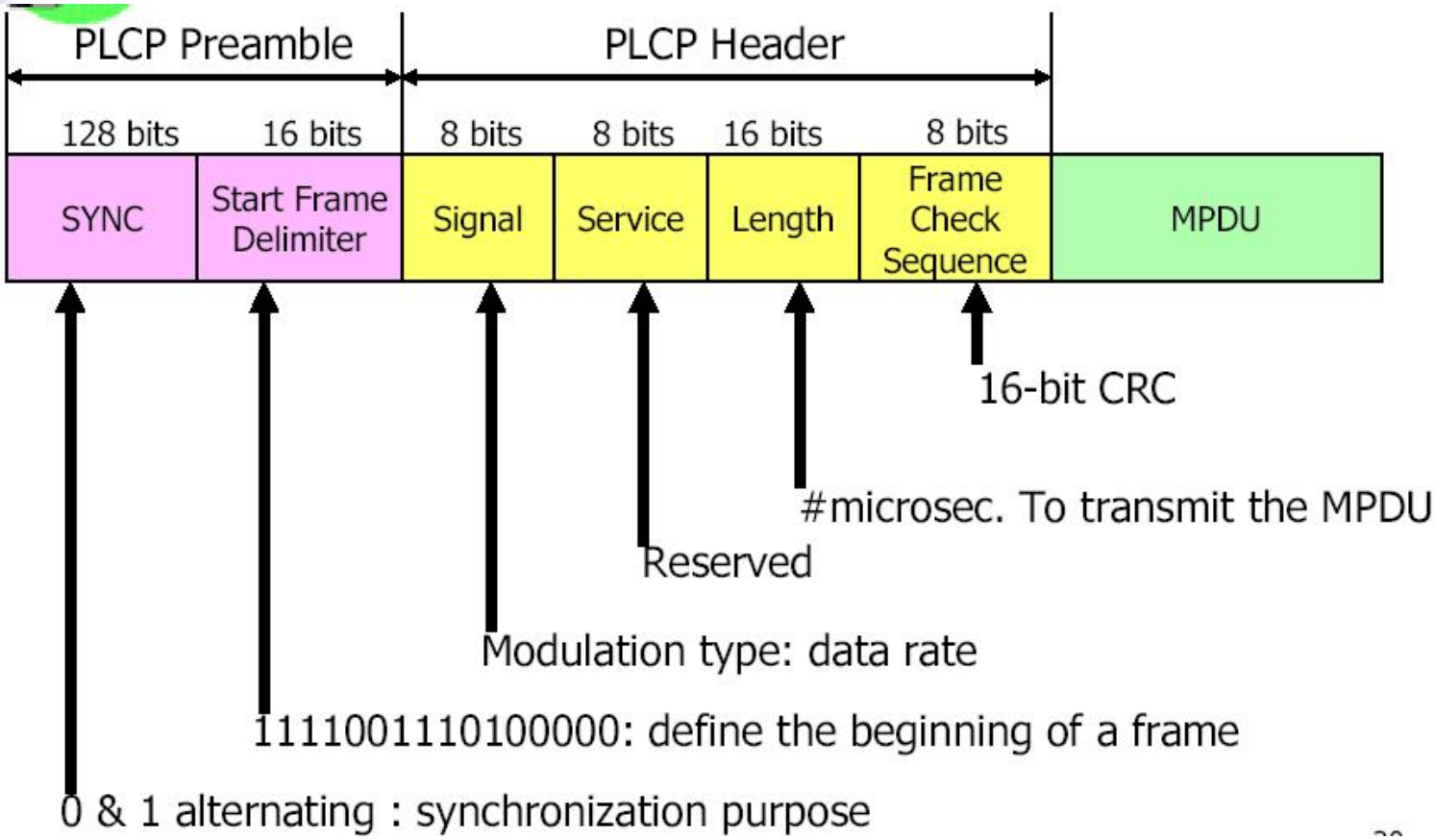
- Ethernet frames are encapsulated within 802.11



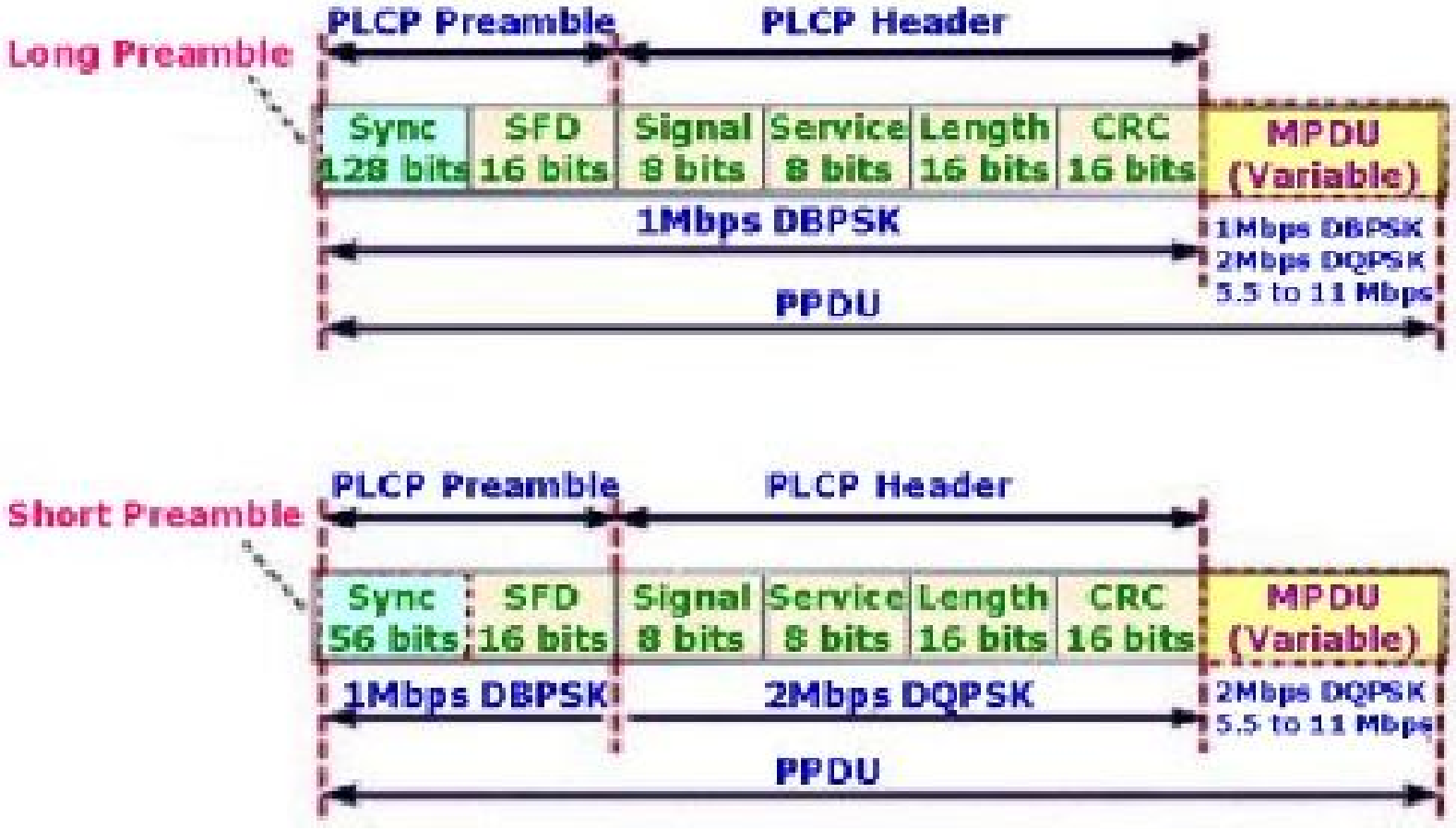
802.11 Protocol Stack



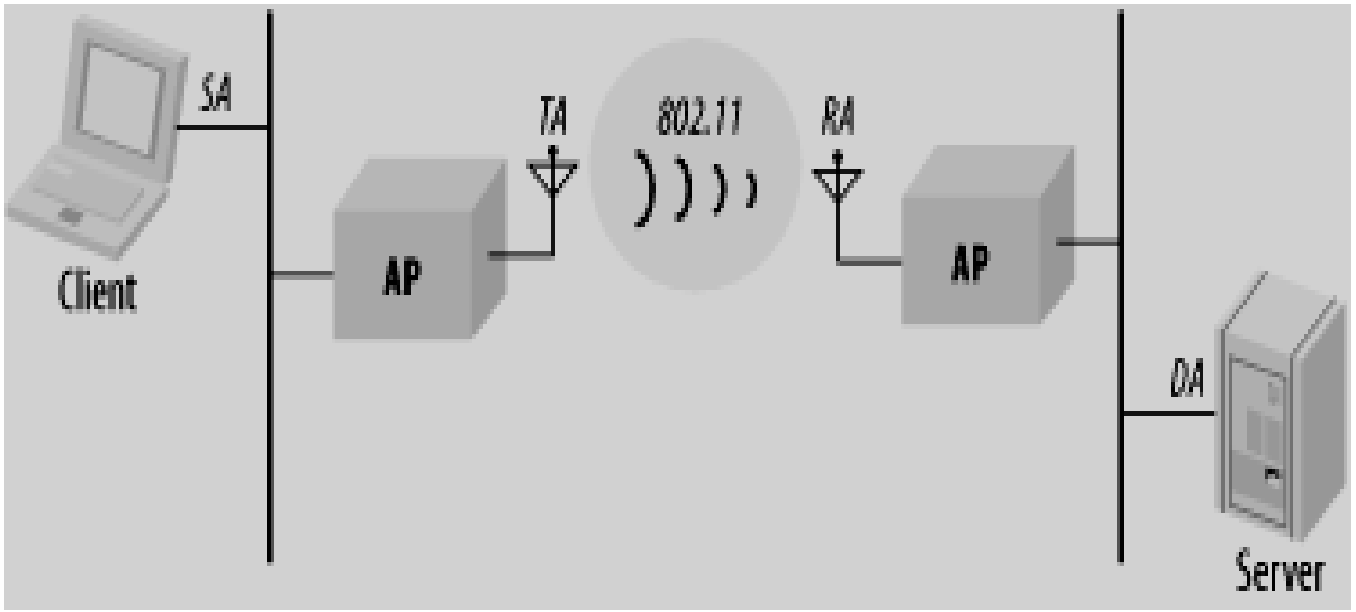
DSSS PLCP(physical layer convolution protocol)



DSSS PLCP(2)


Long Preamble
PLCP Preamble
PLCP Header
Sync
128 bits
SFD
16 bits
Signal
8 bits
Service
8 bits
Length
16 bits
CRC
16 bits
MPDU
(Variable)
1Mbps DBPSK
1Mbps DBPSK
2Mbps DQPSK
5.5 to 11 Mbps
PPDU
Short Preamble
PLCP Preamble
PLCP Header
Sync
56 bits
SFD
16 bits
Signal
8 bits
Service
8 bits
Length
16 bits
CRC
16 bits
MPDU
(Variable)
1Mbps DBPSK
2Mbps DQPSK
2Mbps DQPSK
5.5 to 11 Mbps
PPDU

Four Addresses of the Protocol

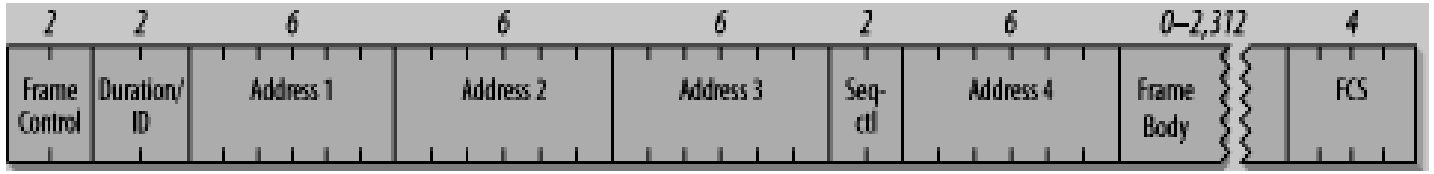


802.11 used as

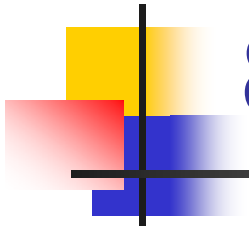
Distribution System (DS)

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

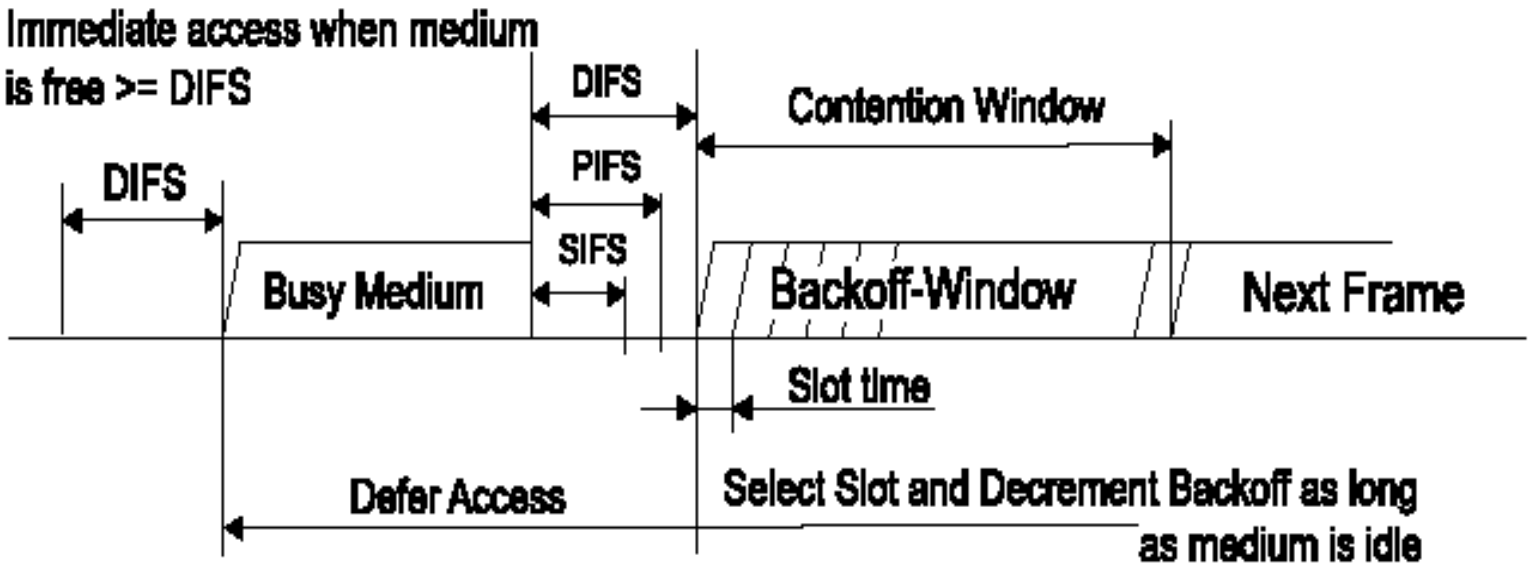
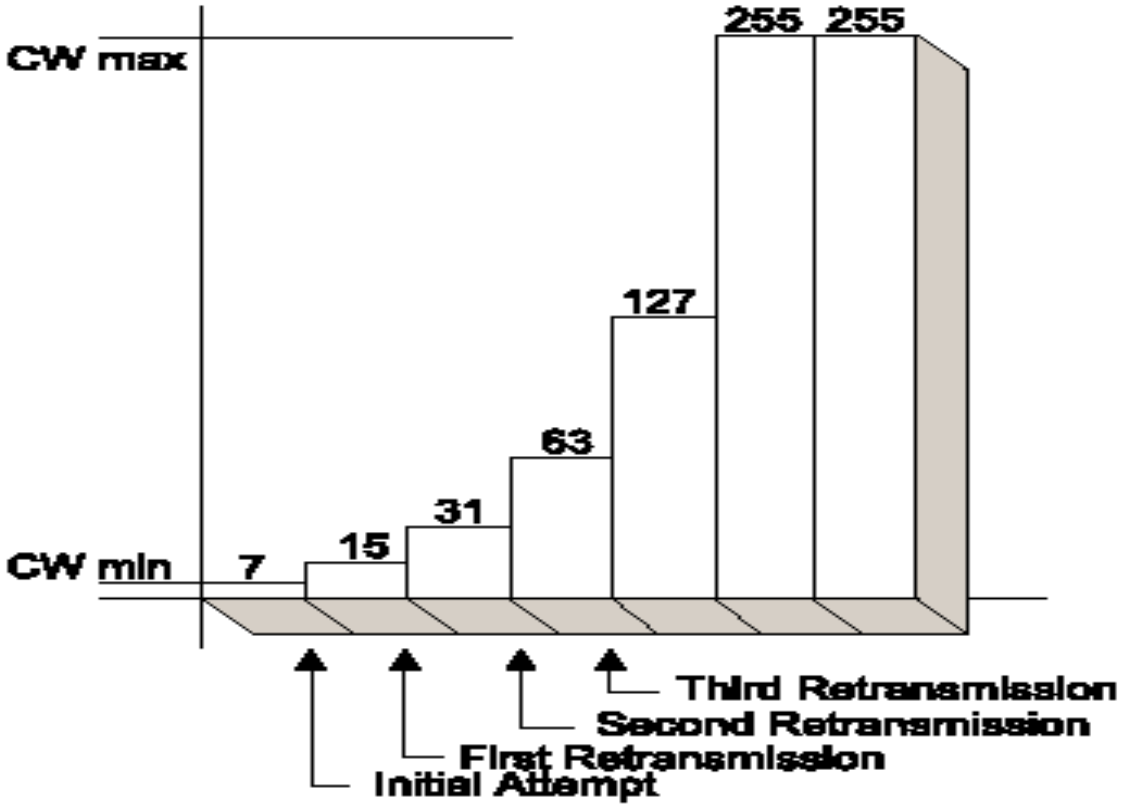


Figure 51—Basic access method

802.11 Contention Window

- Backoff Time = Random * a SlotTime



802.11 Backoff procedure

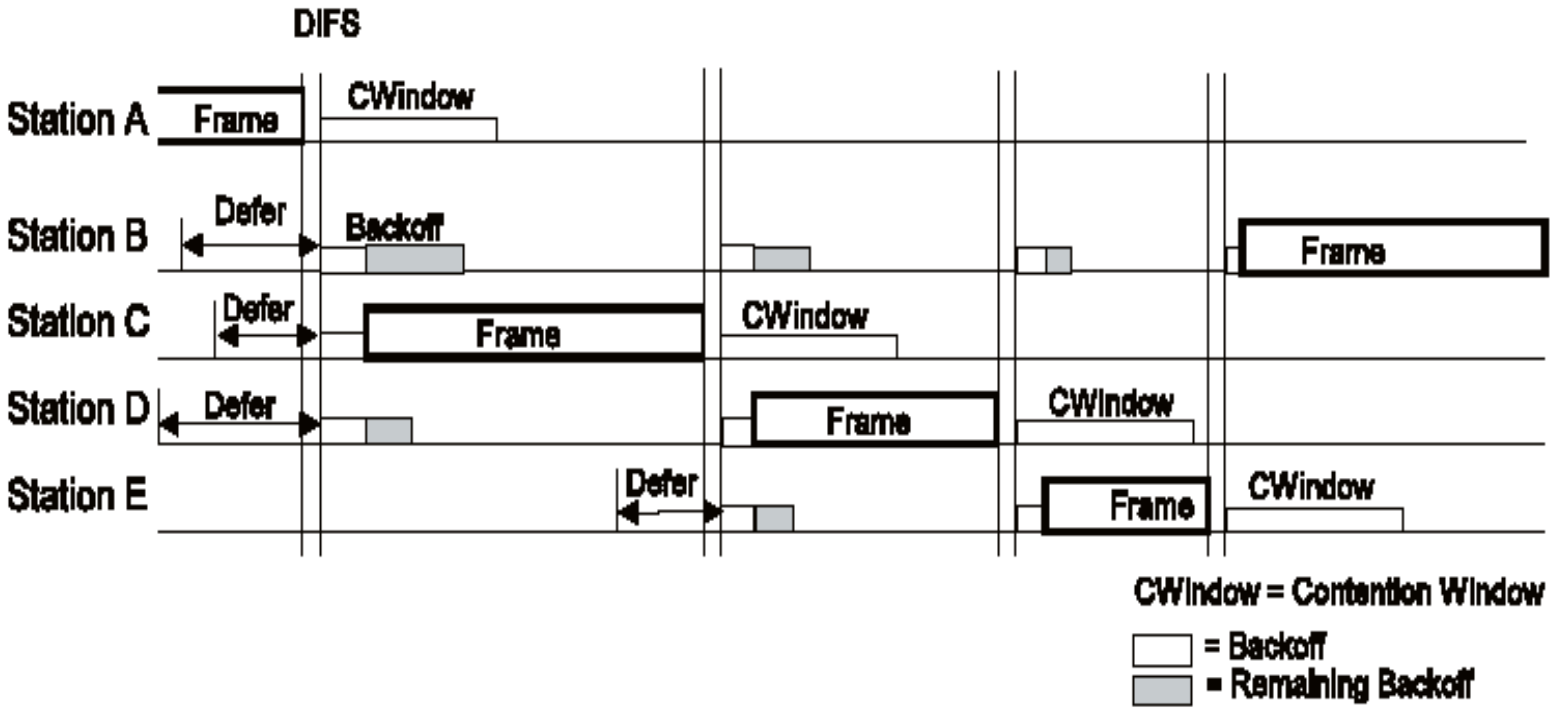


Figure 52—Backoff procedure

802.11 RTS/CTS(Optional)

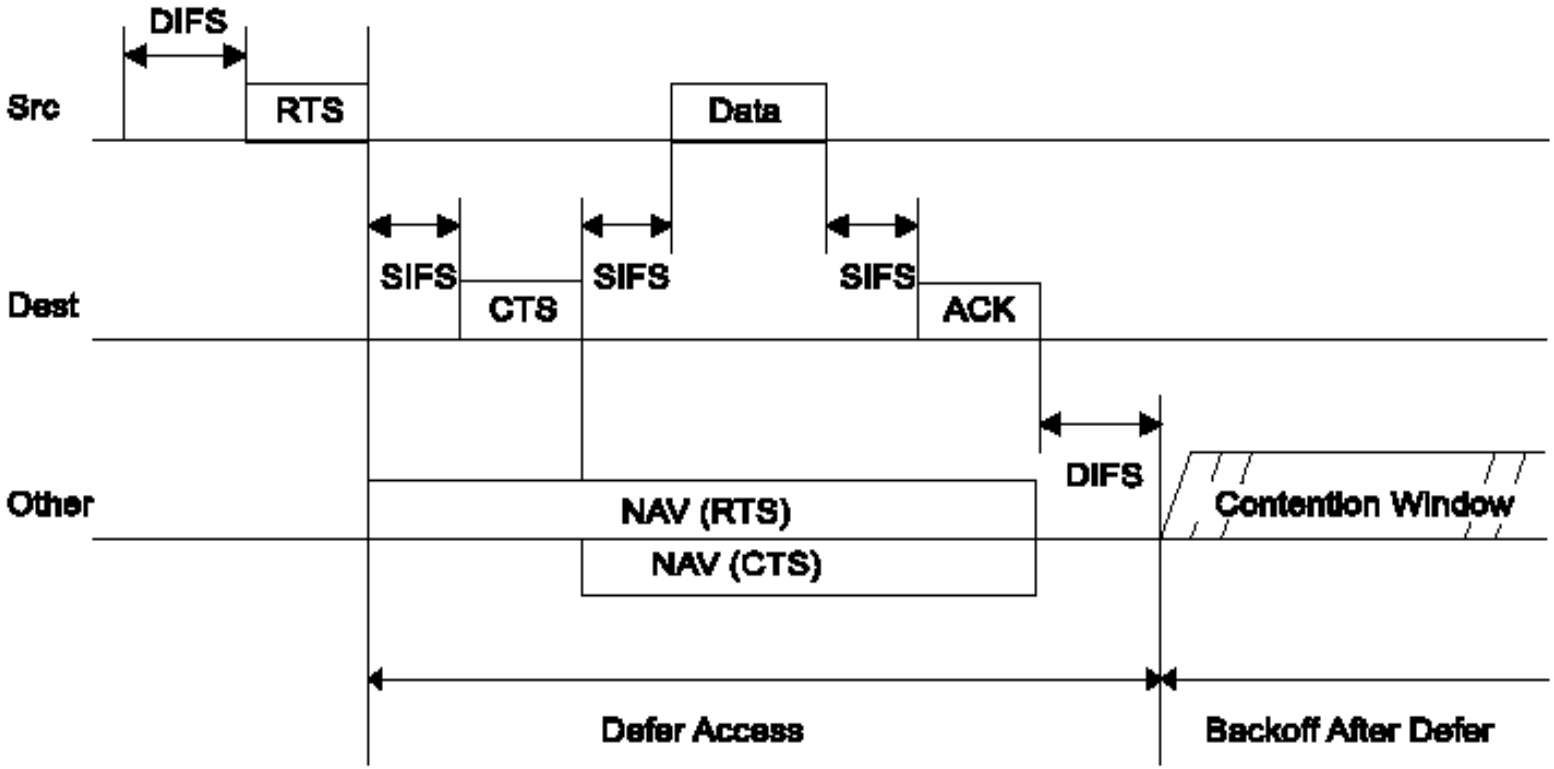
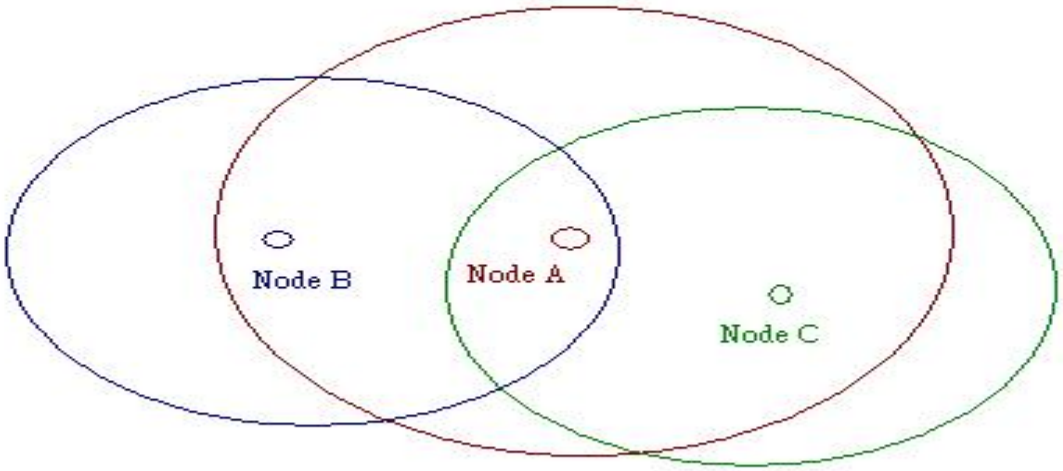


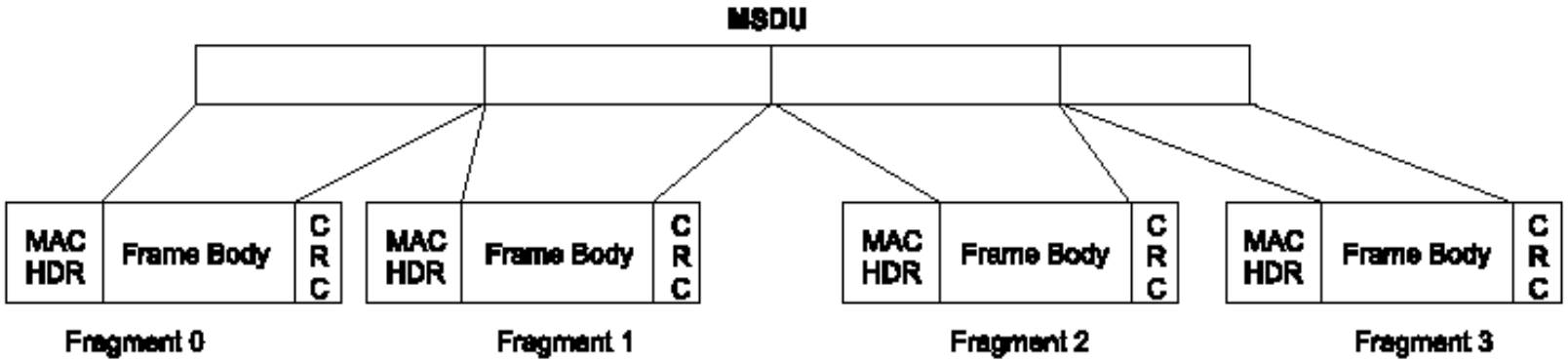
Figure 53—RTS/CTS/data/ACK and NAV setting

Hidden sender problem



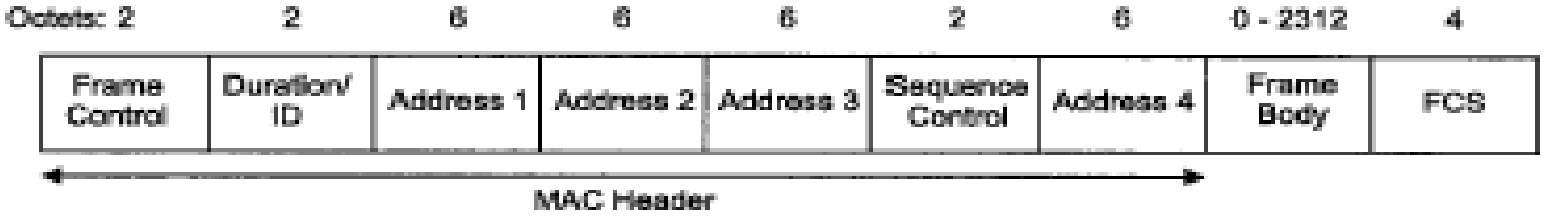
802.11 MSDU/MPDU

- MSDU: Mac Service Data Unit
- MPDU: Mac Protocol Data Unit

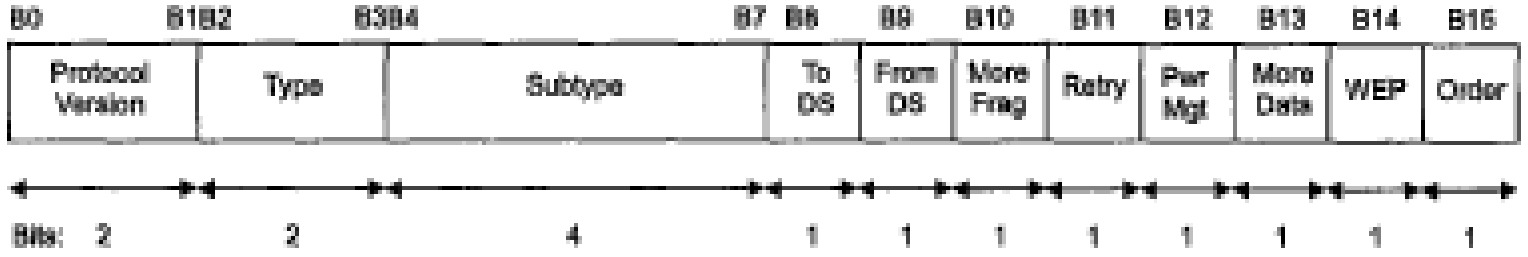


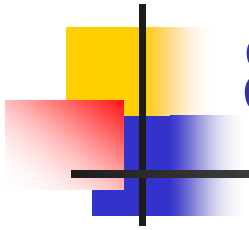
802.11 Mac Frame Format

- Mac frame format



- Frame Control field

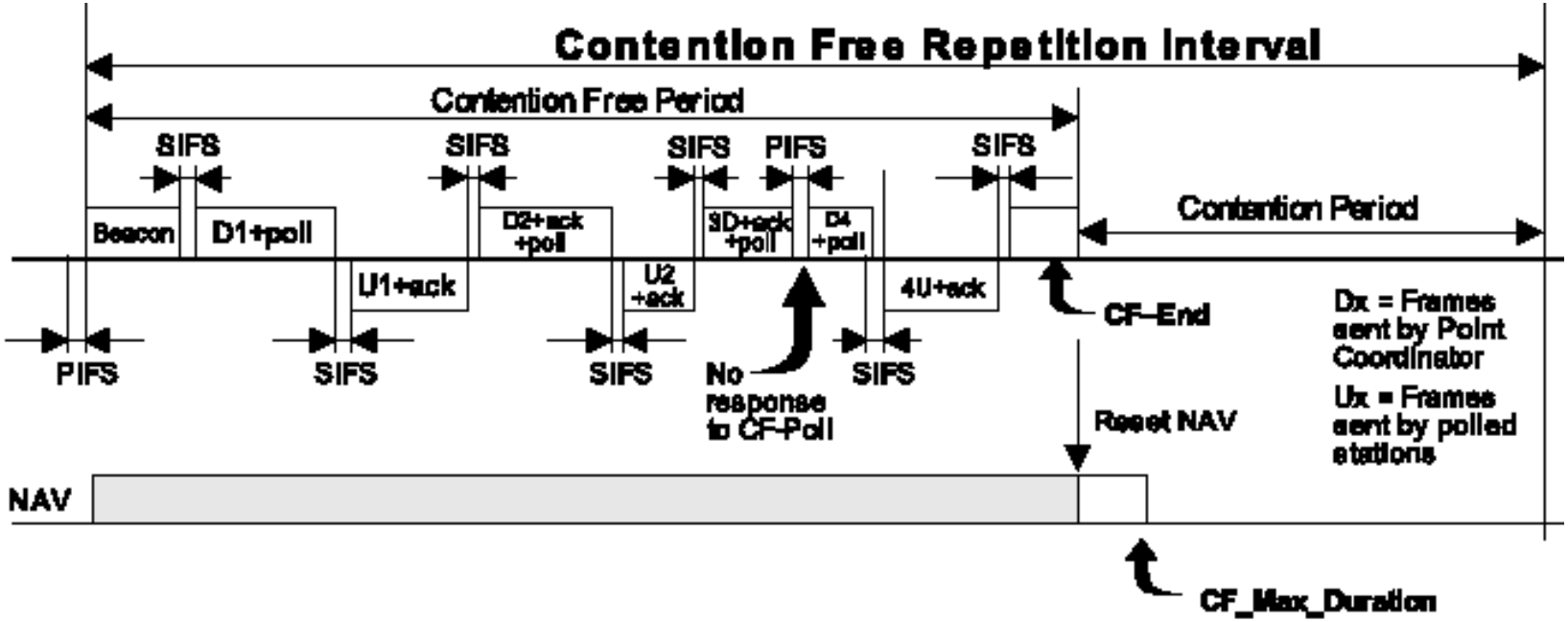




802.11 Mac Frame Type

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

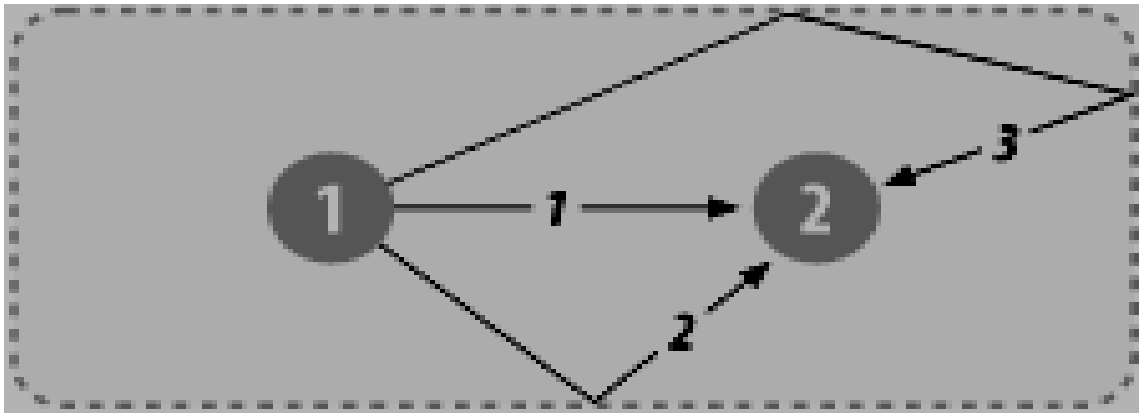
802.11 PCF Transfer Procedure



802.11 DSSS vs. FHSS

	DSSS	FHSS
Systems Collocation	3	26(15)
Noise and Interference Immunity	X	O
Multipath Immunity	X	O
Throughput	O	X
Form Factor	X	O
Power Consumption	X	O
Cost	X	O

802.11 Multipath Problem(1)



2.4GHz ≈7.4cm wavelength

5GHz ≈3.8cm wavelength

* **Inter-Symbol Interference**
* ***Out-of-phase impulses garble signal***

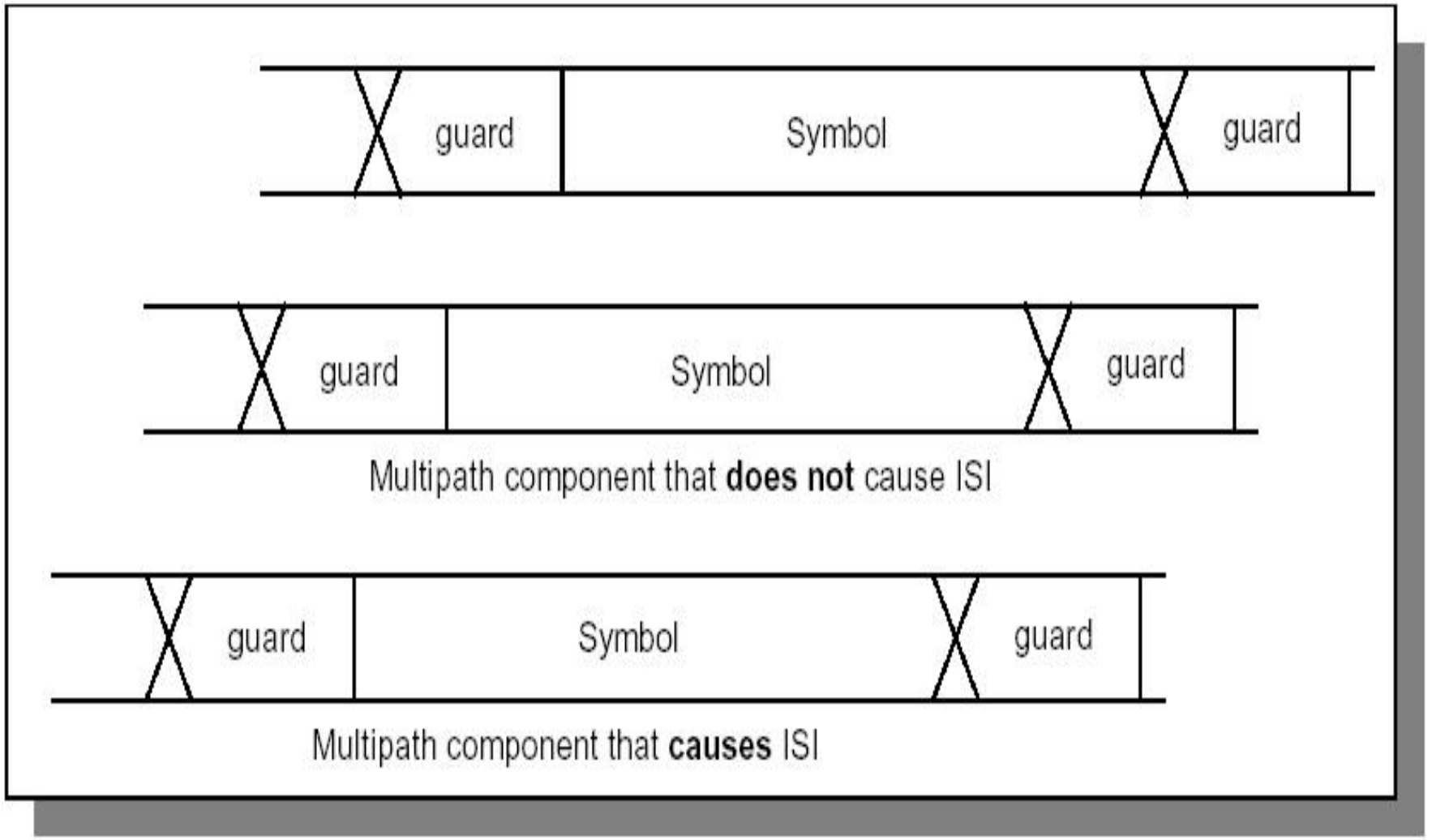
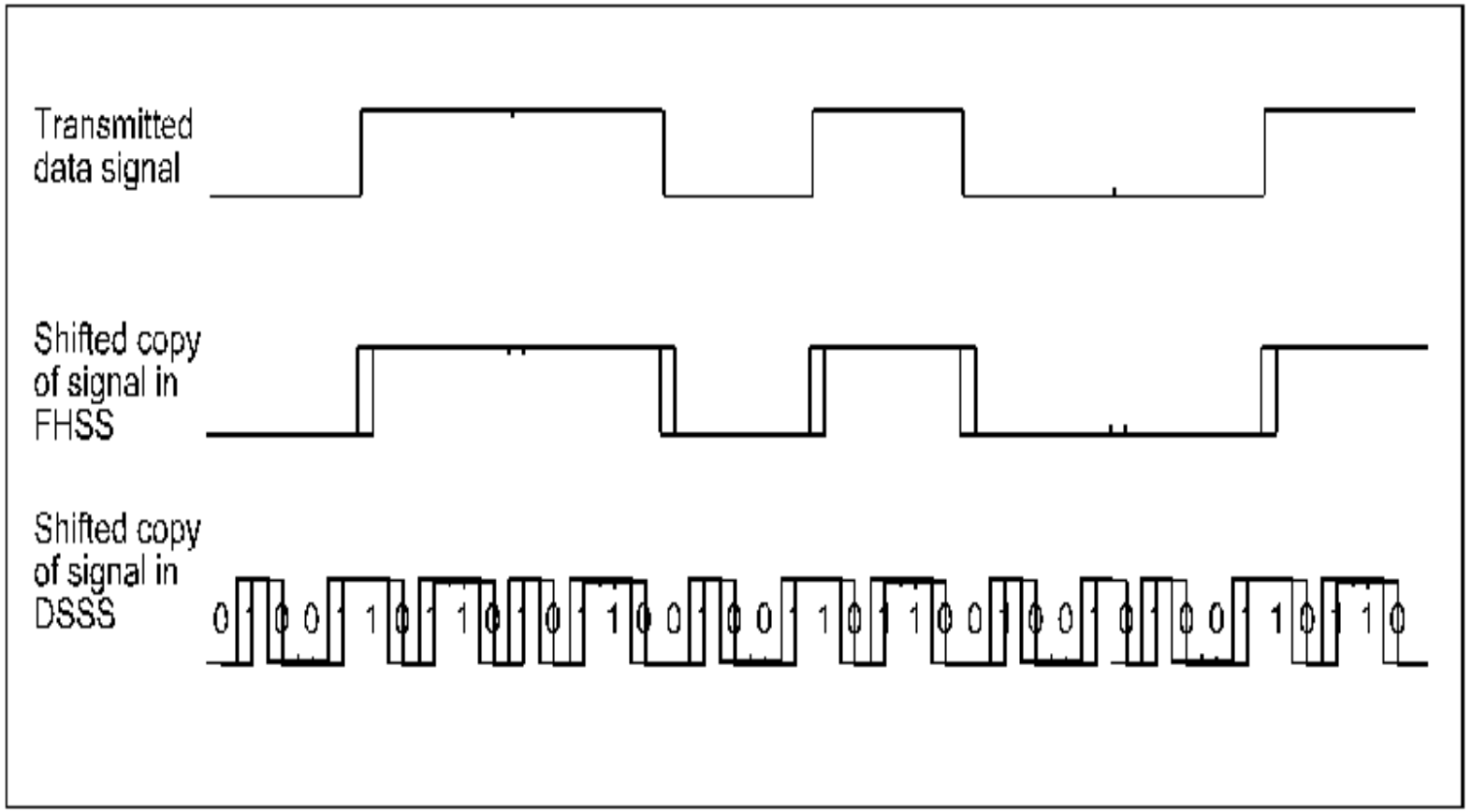


Figure 4 : Guard Time and Cyclic Extension - Effect of Multipath

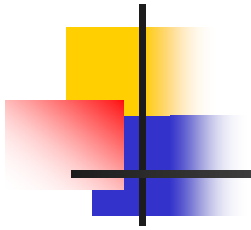
802.11 Multipath Problem(2)



Hot spot problem?

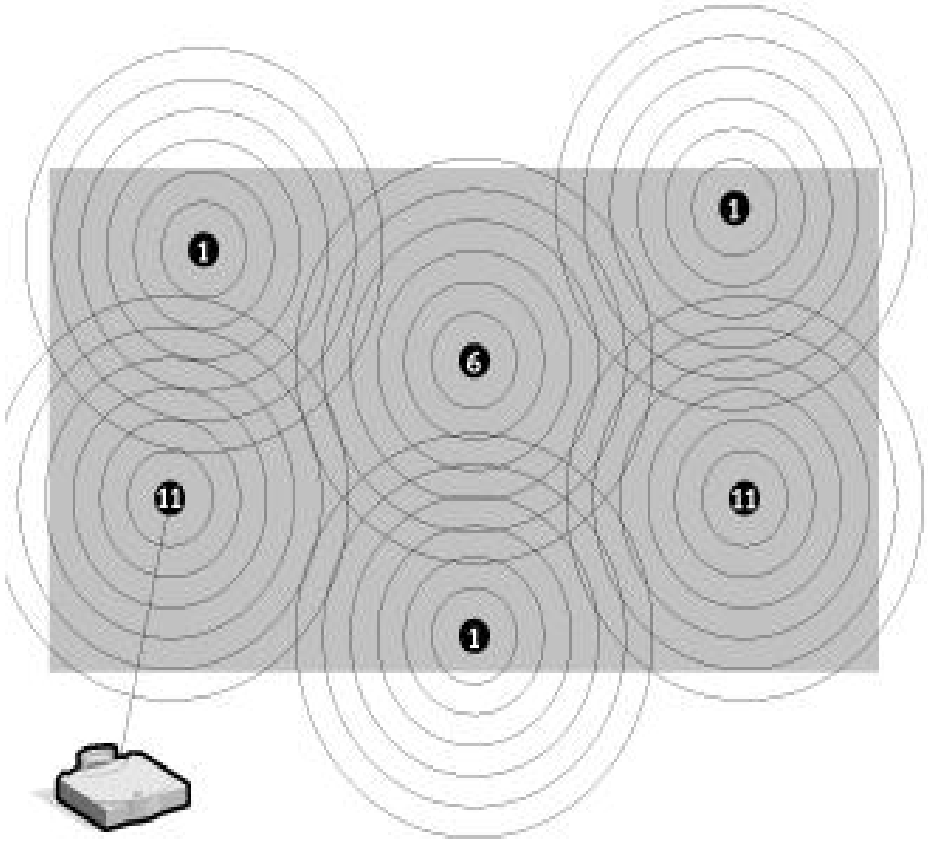
- 一間教室同時有60個人上網,三台ap是否可解決問題?
- Solution 1: maximum users =20/ap ?
- Solution 2: access management system is controlled by switch =>load balance , =>deassociation, deauthentication
- traffic balance or user balance?

Approaches to Noise and Interference

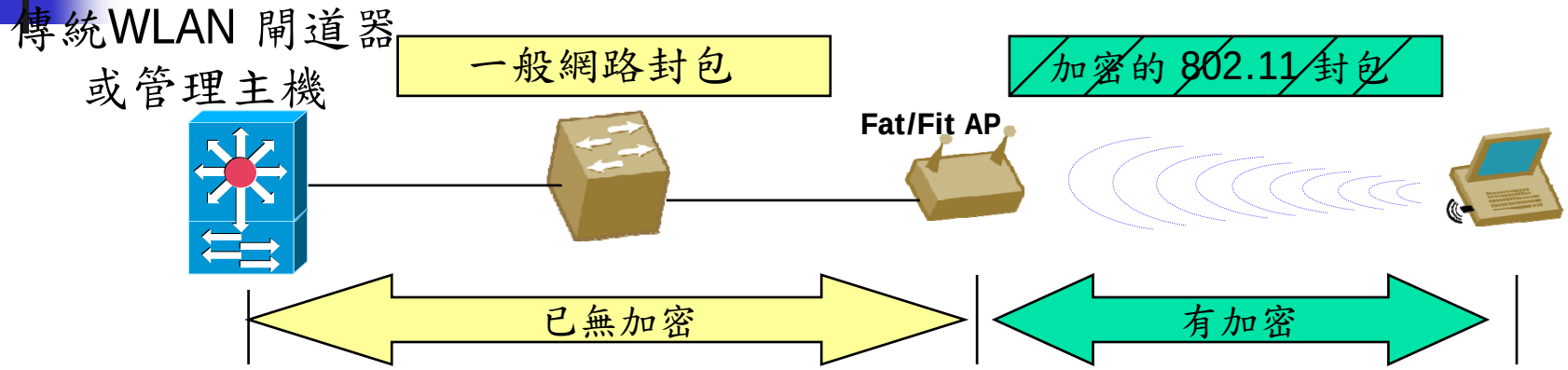


- Idea: Send stronger signals
- But . . .
  - Signal strength capped by government
  - Everyone raises their voice
  - Noise can be *really* strong
  - Requires more power

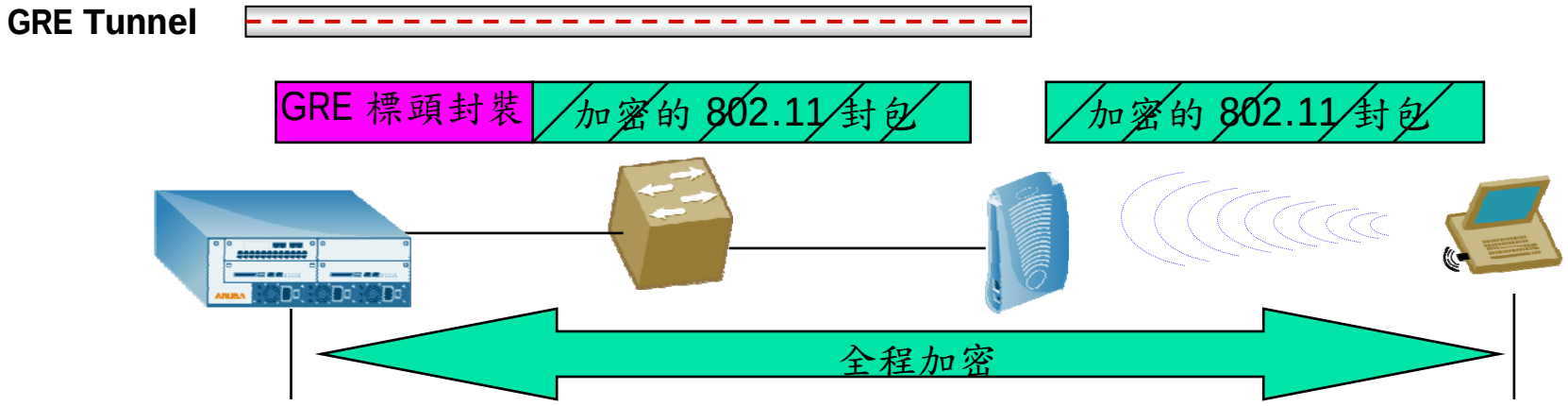
802.11 DSSS (Frequency usage example)



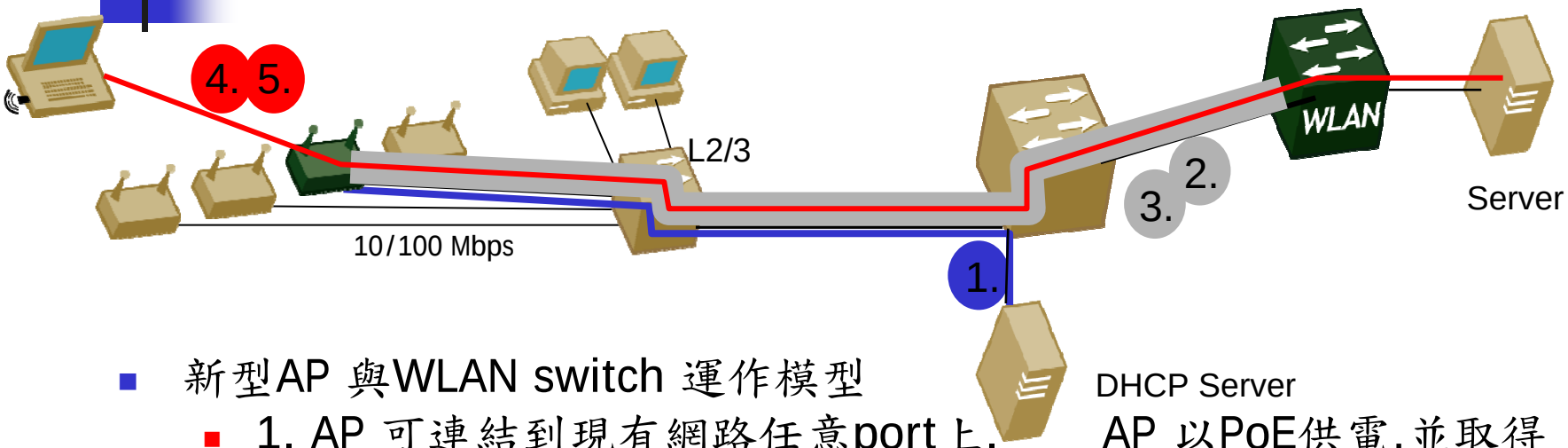
新世代無線網路安全與管理整體解決方案(1)



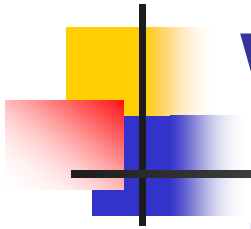
新一代WLAN的邏輯：



新世代無線網路安全與管理整體解決方案(2)



- 新型AP 與WLAN switch 運作模型
  - 1. AP 可連結到現有網路任意port上. AP 以PoE供電,並取得DHCP address (或是預先設定皆可).
  - 2. AP 主動聯繫 WLAN switch 的位置 (以 DNS 或 IP皆可)
  - 3. AP 從WLAN switch 取得 OS 以及設定檔,在AP與WLAN switch之間建立GRE tunnel.
  - 4. 所有的 client 端通訊將透過AP以GRE封裝直接送達switch上,可以不受LAYER2 或 LAYER3 甚至WAN的限制
  - 5. AP斷電或是離線,內部設定立即消失,無法竊取



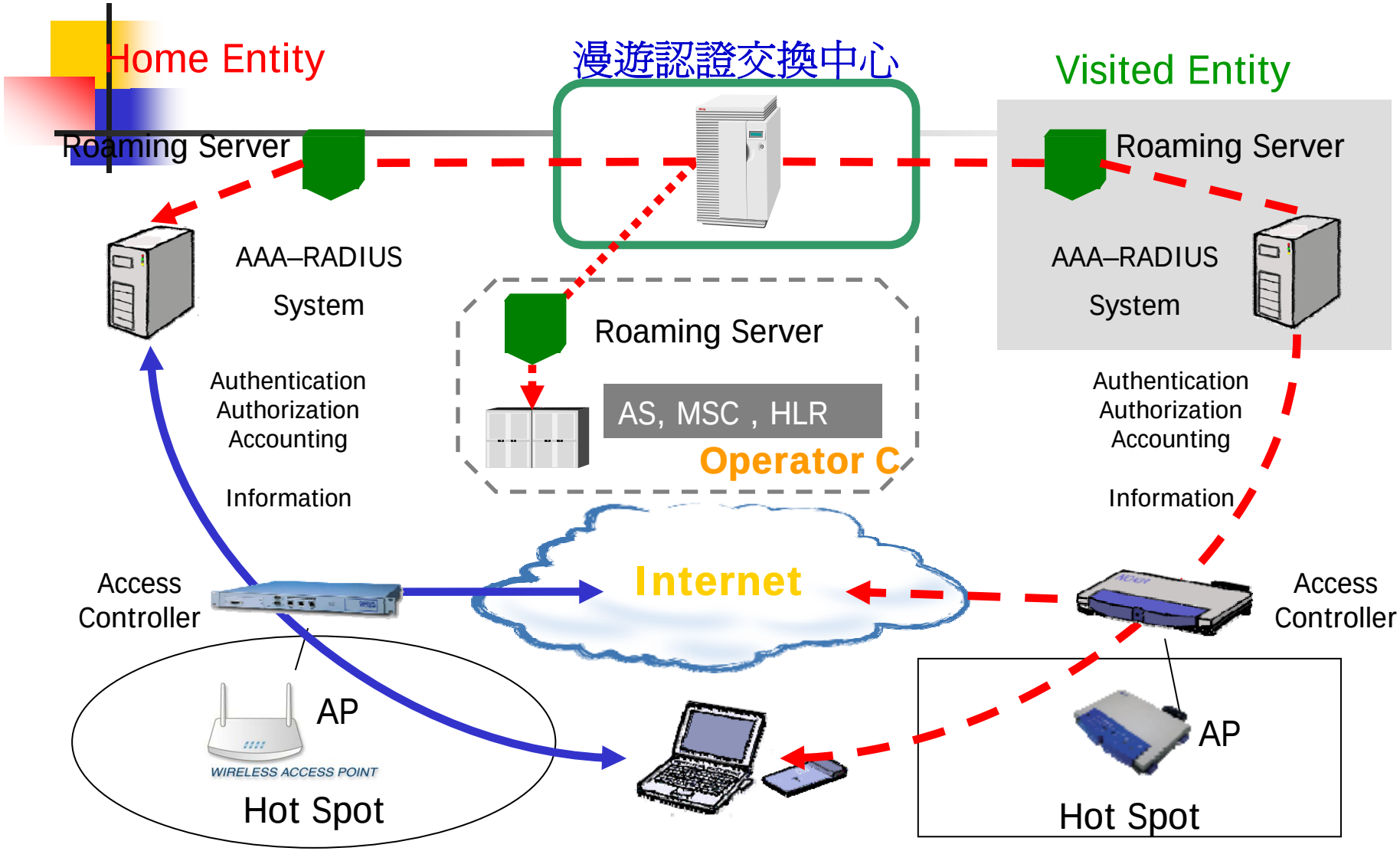
Wireless Setup Notes

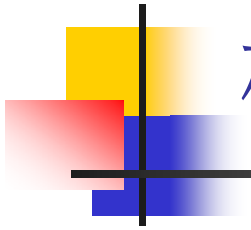
- Login/Logout pages
- PAP/CHAP(RFC1994)/EAP(RFC2284)/Radius(accounting)/LDAP
- IPSec(DE3,3DES,AES) ⇔ avoid hacker
- CA replacement
- 802.11g speed pull down by 802.11b
- AP supports 802.1x/Outdoor or indoor/POE?
- 802.11a backbone// 802.11b/g access
- Fat AP / thin AP+controller(location mobility..)

802.11b/g exp

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

7Mbps up to 17Mbps.


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

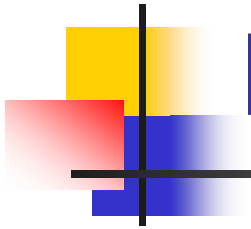


校園導覽系統

- http://guide.cc.ntu.edu.tw
- SNMP to find user connected AP
- Precision: 50m
- In NTU wireless login pages
- Don’t need authentication

Login page


歡迎光臨台灣大學校園無線網路服務
1 輸入計中帳號密碼
《WiFi登入》
請輸入帳號和密碼
帳號：
b90123456
密碼：
登入
重置
2 按登入
欲登入無線網路的服務，您必須要有經過計中認證確認後的帳號及密碼
You need NTU CC account and password
台大校園導覽系統(NTU Campus Tour)

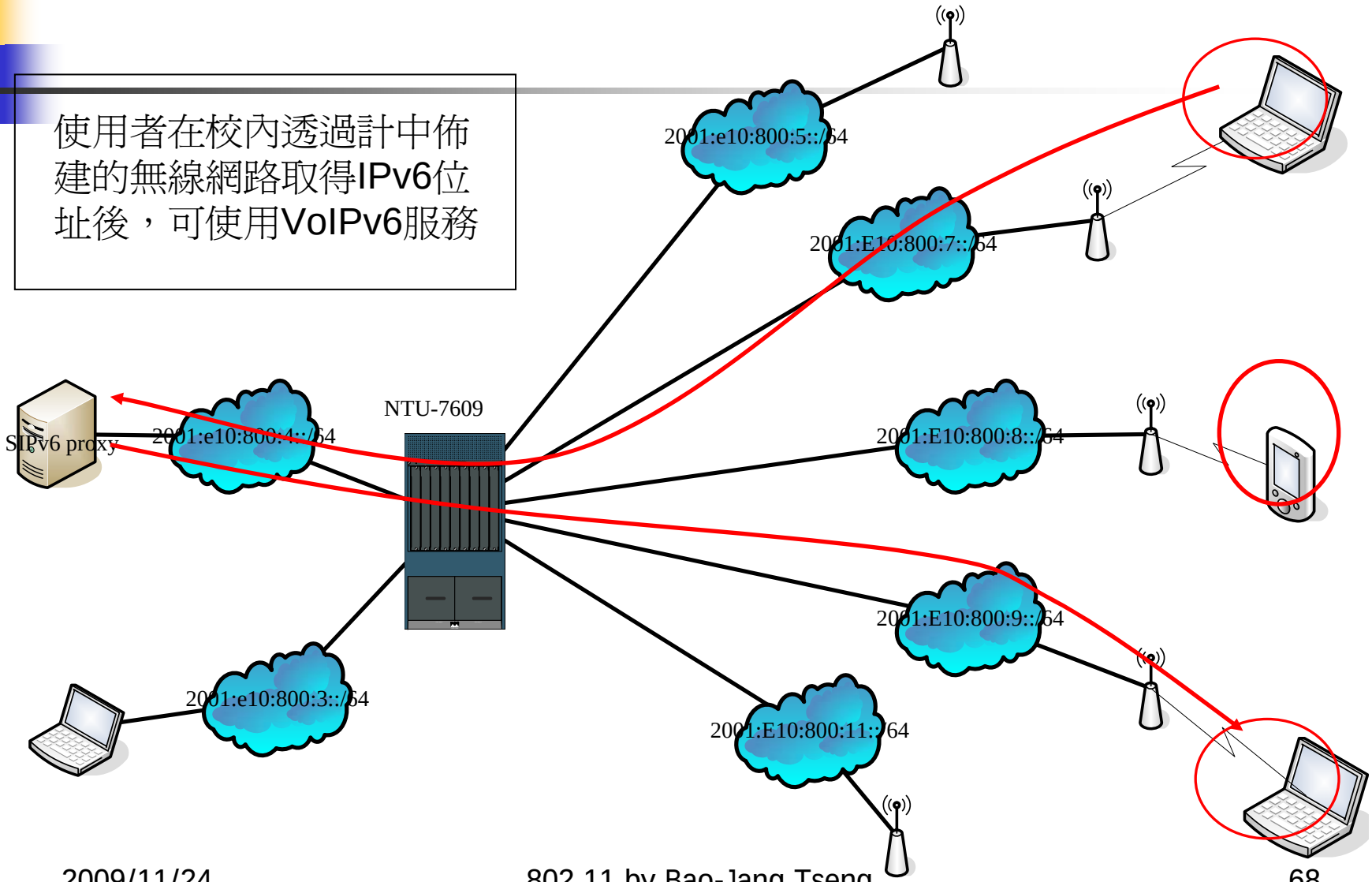


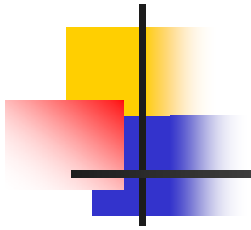
Future working

- MIMO :Multiple-Input Multiple-Output
  - 802.11n
- WiFi phone:
  - NAT,Authentication,Quality problem
- GIS system.
- Roaming between different GATEWAY or lan.

Pure IPv6 wireless VoIP communication

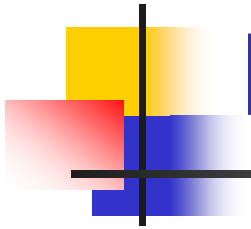
使用者在校內透過計中佈建的無線網路取得IPv6位址後，可使用VoIPv6服務





為何需要單一認證主機

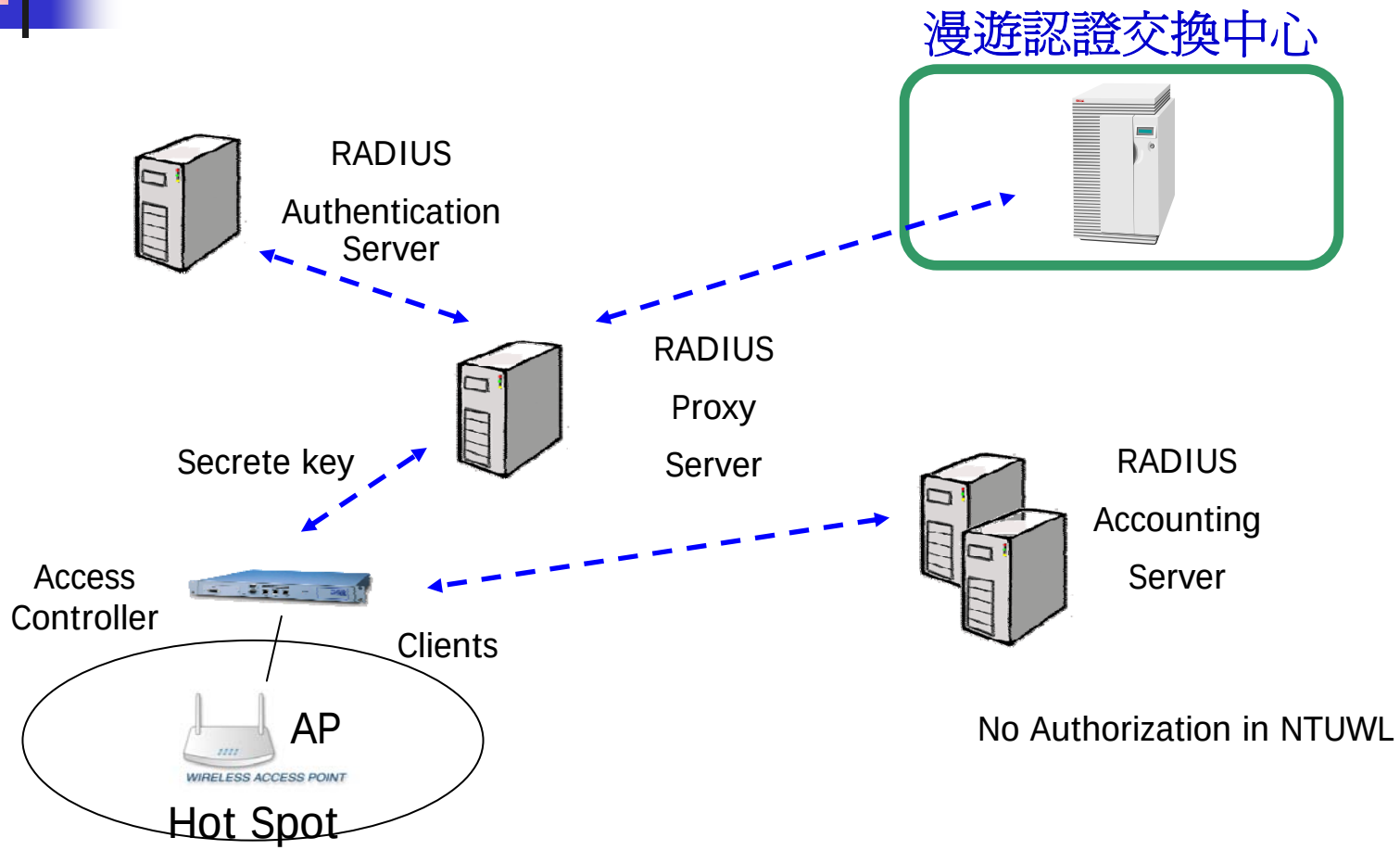
- 主要的認證主機協定有: AD(Active Directory,Microsoft), LDAP(Lightweight Directory Access Protocol,SUM), RADIUS
- Mail、FTP、File system、Wireless Lan、Single Sign-On 、VPN 及電腦教室等帳號管理

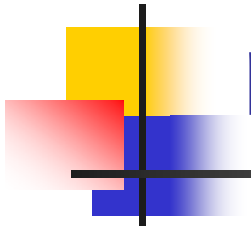


Free Radius

- 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



radiusd.conf

- Define the following
- Ports for authentication/accounting are 1812/1813
- PAP/CHAP/UNIX/EAP/MSCHAP/LDAP..
- digest for SIP
- Directory definition: sysconfdir, raddbdir,

proxy.conf & client.conf

```
realm ntu.edu.tw {
        type            = radius
        authhost        = ntuRadius:1812
        accthost        = ntuRadius:1813
        secret          = abcd
}

realm NULL {
        type            = radius
        authhost        = ntuRadius:1812
        accthost        = ntuRadius:1813
        secret          = efgh
}

realm DEFAULT {
        type            = radius
        authhost        = RoamingCenter:1812
        accthost        = RoamingCenter:1813
        secret          = ijkl
        nostrip
}
```

```
client NTU_NAS{
        secret          = abcd
        shortname       = NTU_NAS
}
```

sql.conf & eap.conf

- sql {
- server = "localhost"
- login = “abc"
- password = “def"

- # Database table configuration
- radius_db = "radius"

```
 tls {
private_key_password = whatever
private_key_file = ${raddbdir}/certs/demo1.pem
certificate_file = ${raddbdir}/certs/demo1.pem
#  Trusted Root CA list
CA_file = ${raddbdir}/certs/demo2.pem
```

測試是否安裝成功,請用debug mode: radiusd -X