

---

---

# 無線通訊協定

中興大學資工系 曾學文

Tel : (04)22840497 ext 908

E-mail: [hwtseng@nchu.edu.tw](mailto:hwtseng@nchu.edu.tw)

---

# Outline

---

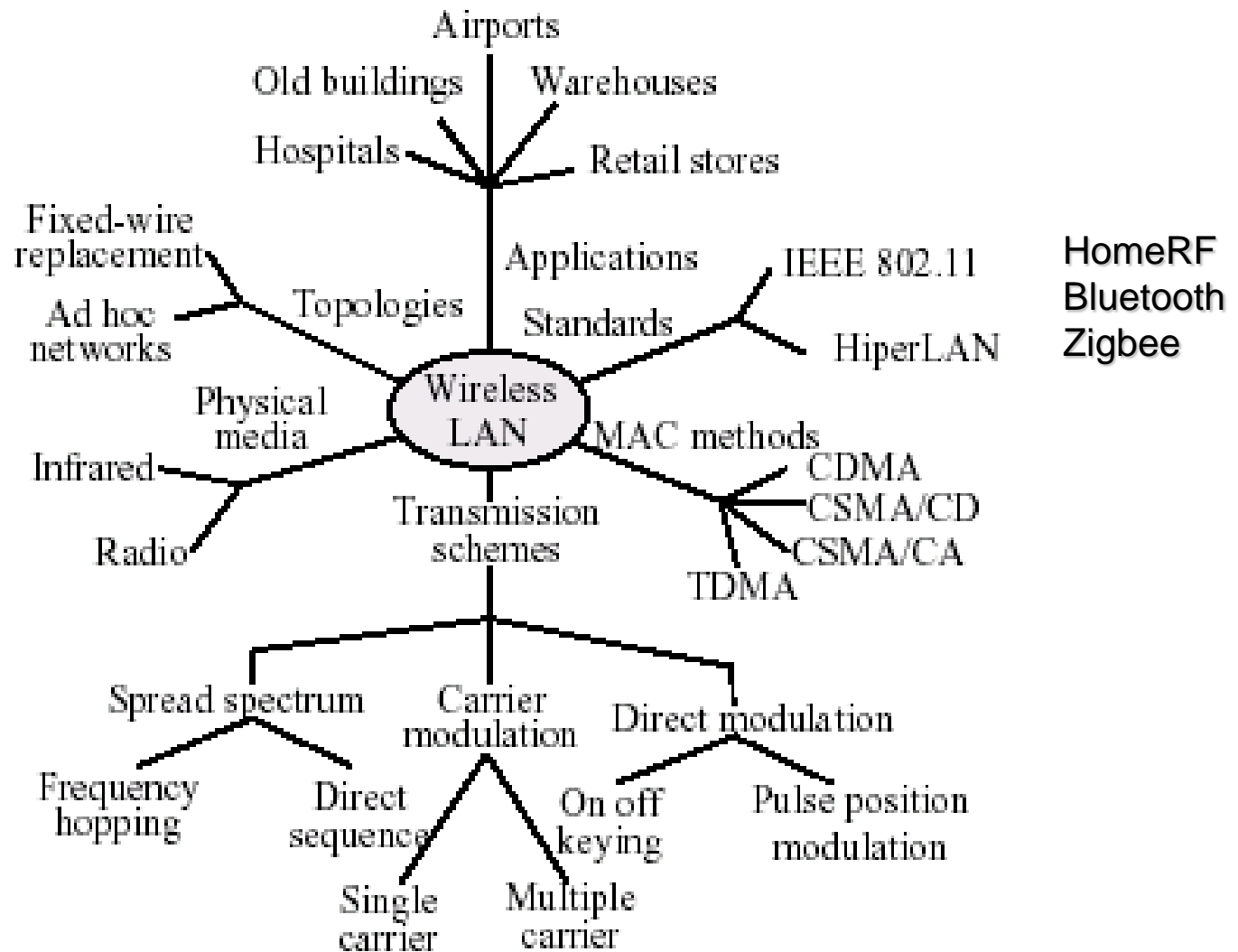
- 1. 802.11 Architecture and Overview**
- 2. Baseband Infrared (IR) Physical Layer Specification**
- 3. Direct Sequence Spread Spectrum (DSSS) Physical Layer Specification**
- 4. Orthogonal Frequency Division Multiplexing (OFDM) Physical Layer Specification**
- 5. IEEE 802.11g Extended Rate PHY (ERP) Specification**
- 6. Frequency Hopping Spread Spectrum PHY of the 802.11 Wireless LAN Standard**
- 7. IEEE 802.11 Wireless LAN MAC Standard**

---

---

# 1. 802.11 Architecture and Overview

# Technology Tree for Wireless LAN



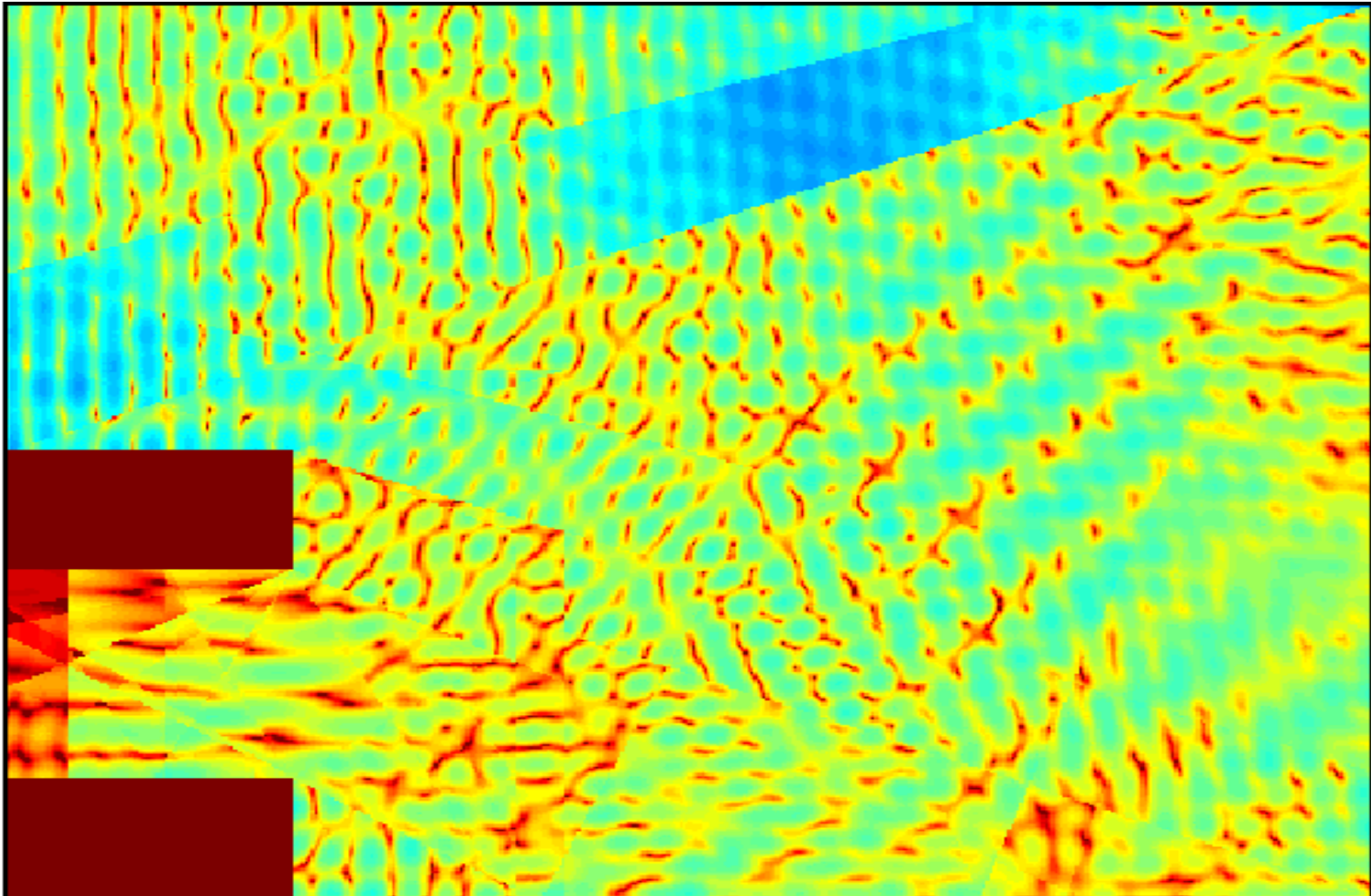
---

# What is unique about wireless?

---

- **Difficult media**
  - interference and noise
  - quality varies over space and time
  - shared with unwanted 802.11 devices
  - shared with non-802 devices (unlicensed spectrum: microwave ovens, bluetooth, Zigbee, etc.,)
- **Full connectivity cannot be assumed**
  - Hidden node problem
- **Multiple international regulatory requirements**

# Medium Variations



---

# Uniqueness of Wireless (continued)

---

- **Mobility**

- variation in link **reliability**
- **battery** usage: requires **power management**      **power control**
- want **seamless** connections      **???**

- **Security**

- no physical boundaries
- overlapping LANs

---

# Requirements

---

- **Single MAC to support multiple PHYs.**
  - Support single and multiple channel PHYs.
  - Different PHYs have different medium sense characteristics.
- **Should allow overlap of multiple networks in the same area and channel space.**
- **Need to be Robust for Interference?**
  - **ISM band** (Industry, Science and Medicine)
    - » 13.56 MHz, 27.55 MHz, 303 MHz, 315 MHz, 404 MHz, 433 MHz, 868 MHz (Europe), 915 MHz (North America), **2.45 GHz, 5.2 GHz (North America), 5.3 GHz, and 5.7 GHz (North America)**
    - » Microwave, other non-802.11 interferers.
    - » Co-channel interference.
- **Need mechanisms to deal with Hidden Nodes?**
- **Need provisions for **Time Bounded Services (real-time service)**.**



---

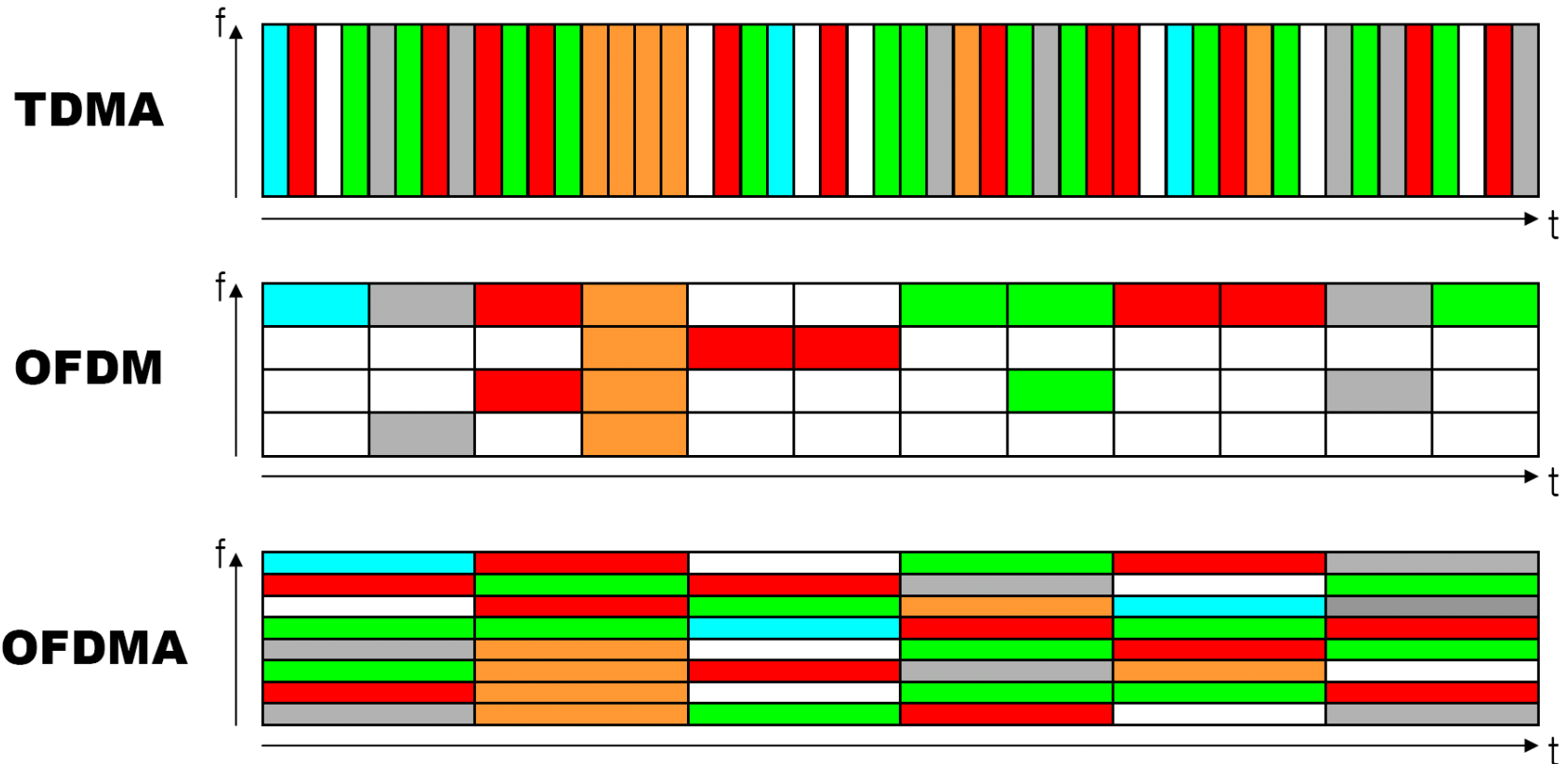
# Architecture Overview

---

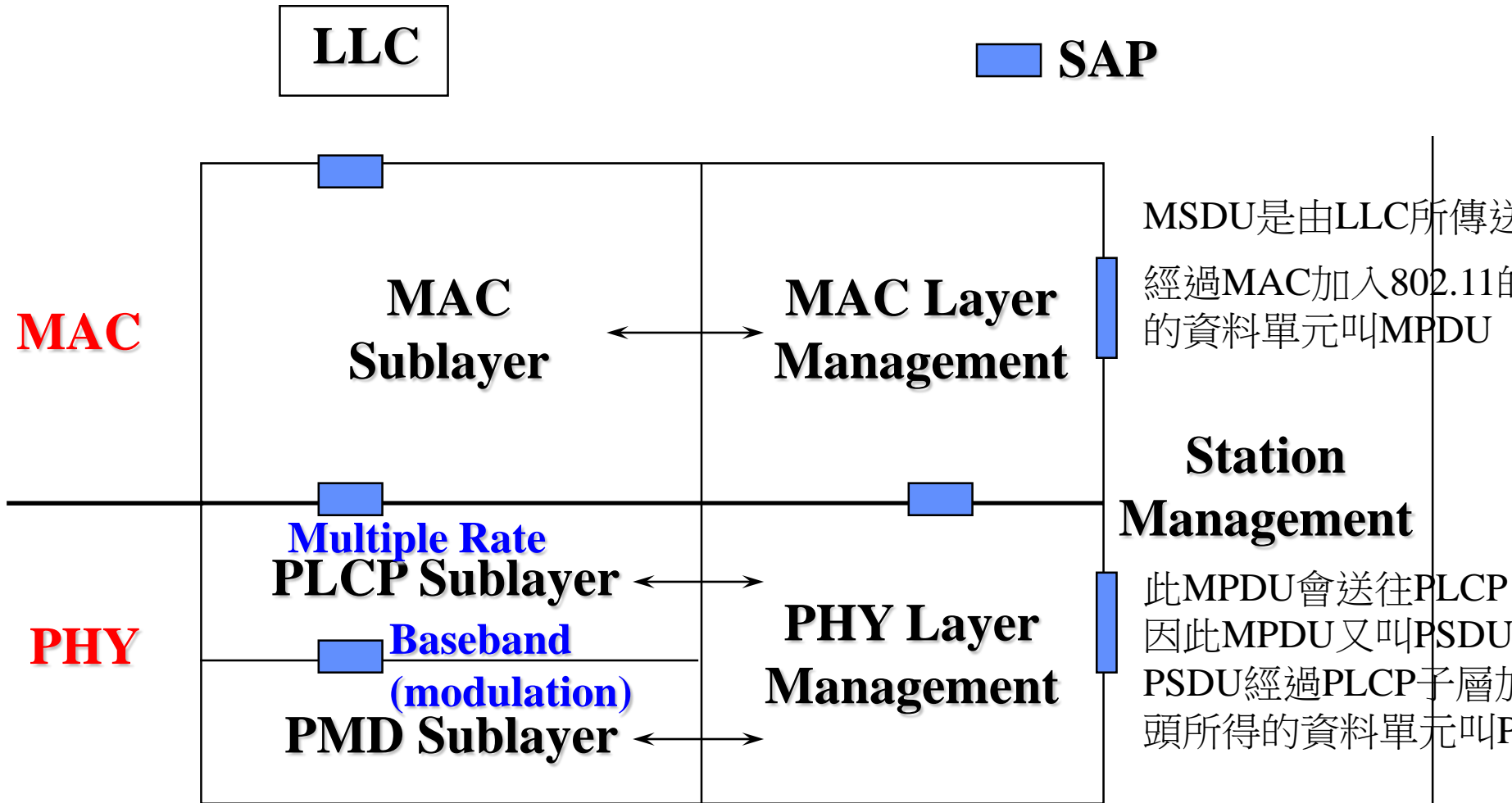
- **One MAC supporting multiple PHYs**
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum
  - Infrared
  - Orthogonal Frequency Division Multiplexing
  - Orthogonal Frequency Division Multiple Access (OFDMA)
  
- **Two configurations**
  - Independent (ad hoc) and Infrastructure
  - Hybrid configuration has being studied (802.11s)
  
- **CSMA/CA (collision avoidance) with optional Point Coordination Function (PCF)**

# TDMA/OFDM/OFDMA

## TDM / OFDM / OFDMA



# 802.11 Protocol Entities



---

## 802.11 Protocol Architecture

---

- **MAC Entity**
  - basic access mechanism
  - fragmentation/defragmentation
  - encryption/decryption
- **MAC Layer Management Entity**
  - synchronization
  - power management
  - roaming
  - MAC Management Information Base (MIB)
- **Physical Layer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)

---

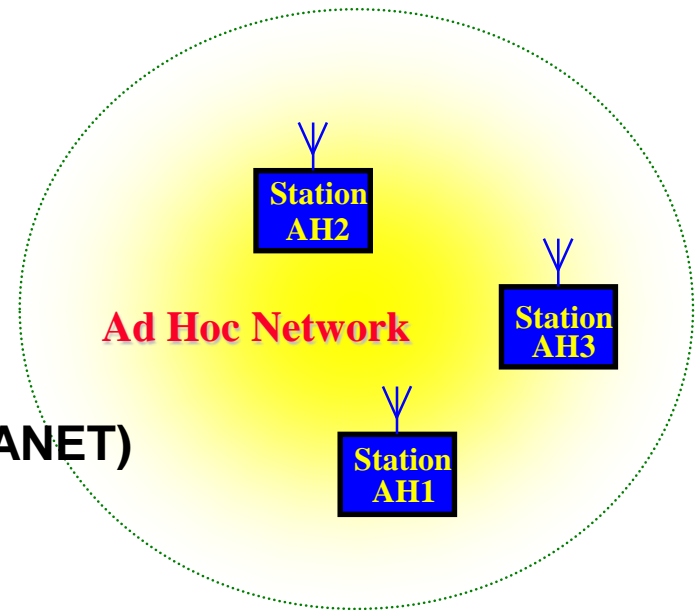
## 802.11 Protocol Architecture (cont.)

---

- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding (baseband)
  
- **PHY Layer Management**
  - channel tuning (channel switching delay : **224us** in 802.11b)
  - PHY MIB
  
- **Station Management**
  - interacts with both MAC Management and PHY Management

# 802.11 Configurations - Independent

- **Independent**
  - one **Basic Service Set (BSS)**
  - **Ad Hoc** network
  - direct communication
  - limited coverage area
- **Research topics**
  - Multi-Hop Routing (IETF MANET; VANET)
  - Multicasting
  - Multi-channel Access
  - Security
  - QoS ...



Mobile Station : **STA**

Vehicular Ad-Hoc Network (VANET)

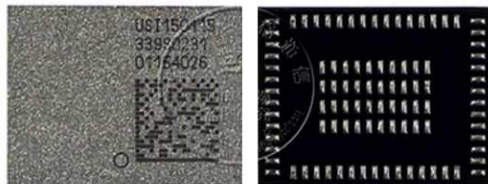
Mobile Ad Hoc Network (MANET)

# Commercial Products : WLAN Cards

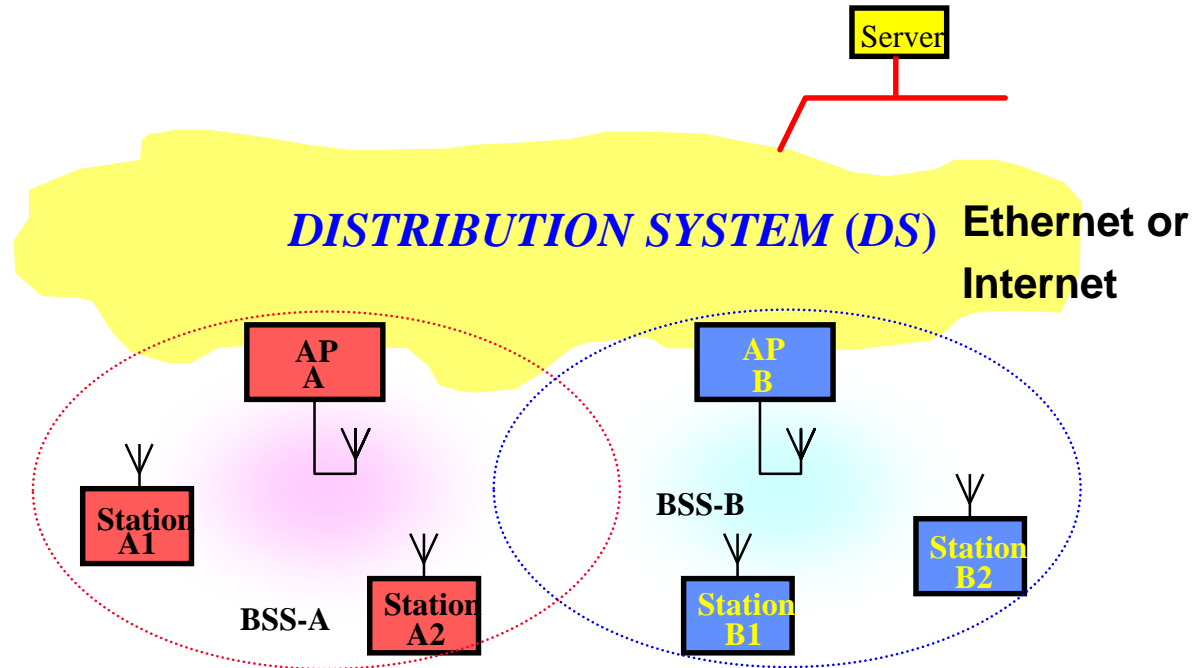
- One piece
- Two pieces



Pasadena Networks, LLC <http://www.pasadena.net>



# 802.11 Configurations - Infrastructure



- **Infrastructure**
  - Access Points (**AP**) and stations (**STA**)
- Distribution System interconnects Multiple Cells via Access Points to form a single Network.
  - extends wireless coverage area
- **Wireless bridge** application

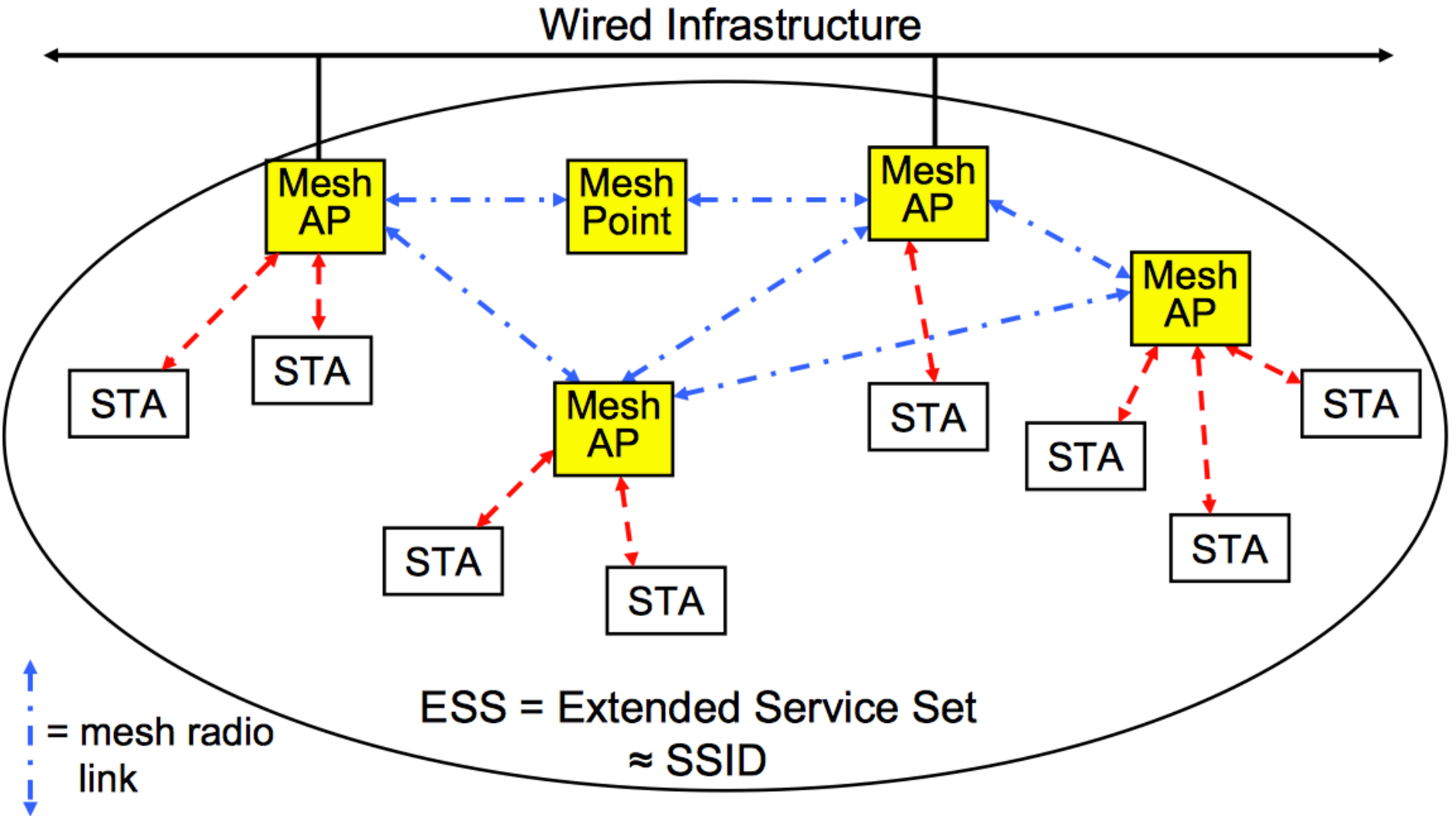


# Commercial Products : AP

## Access Points

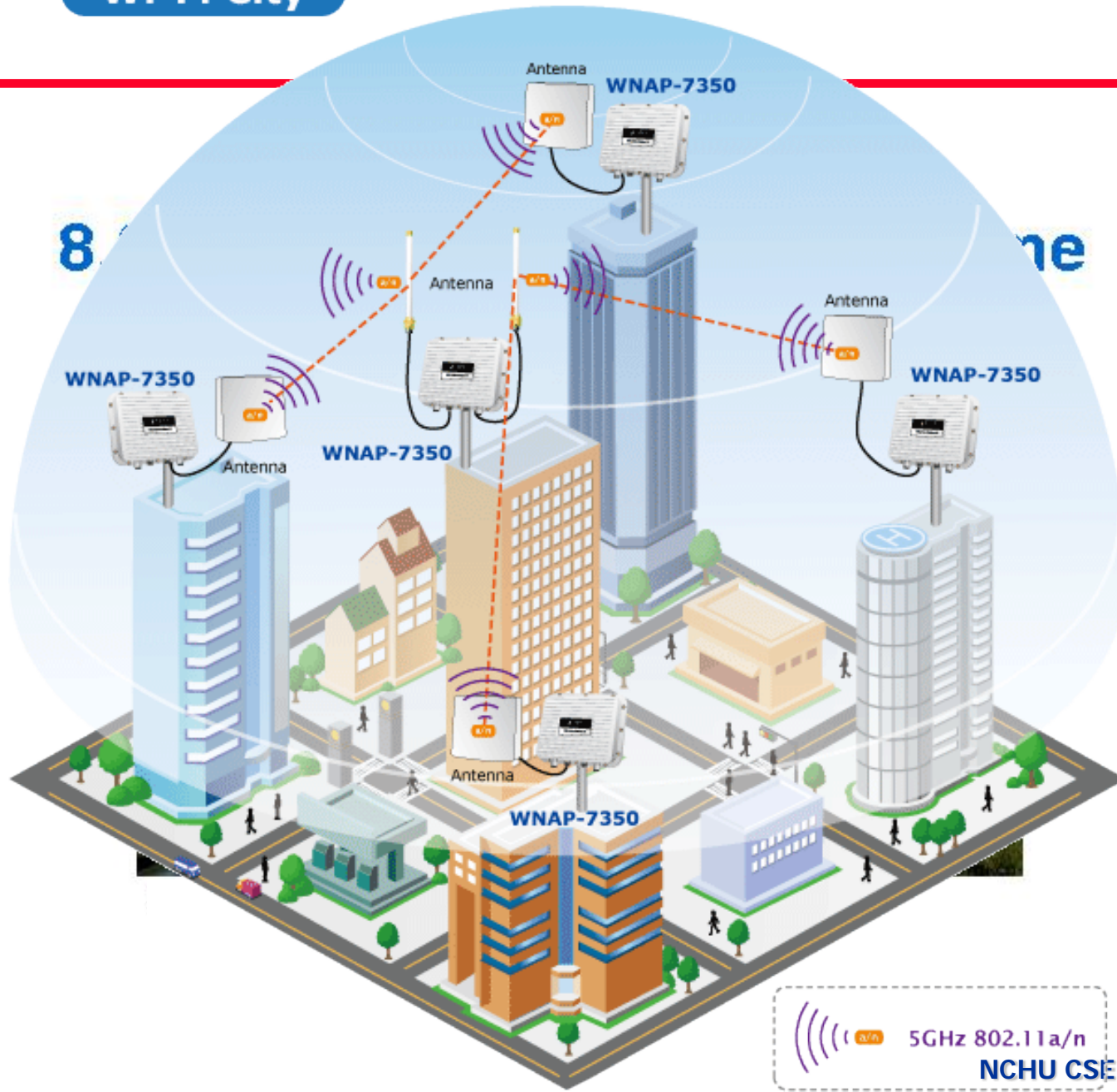


# Wireless Bridging



# Outdoor Application

## Wi-Fi City



5GHz 802.11a/n

# Outdoor Application - Antenna

## Antennas

Directional Antenna



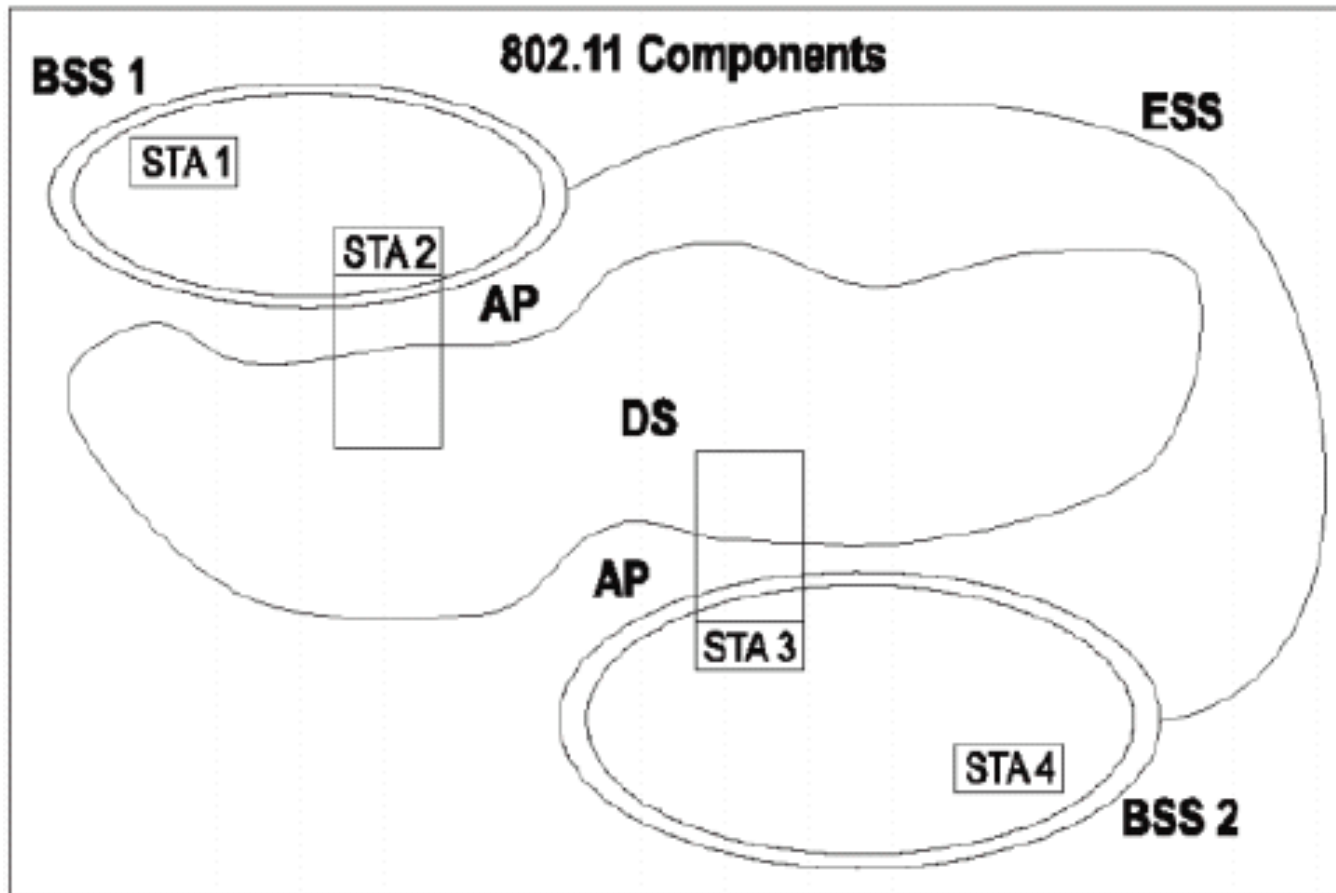
---

# Distribution System

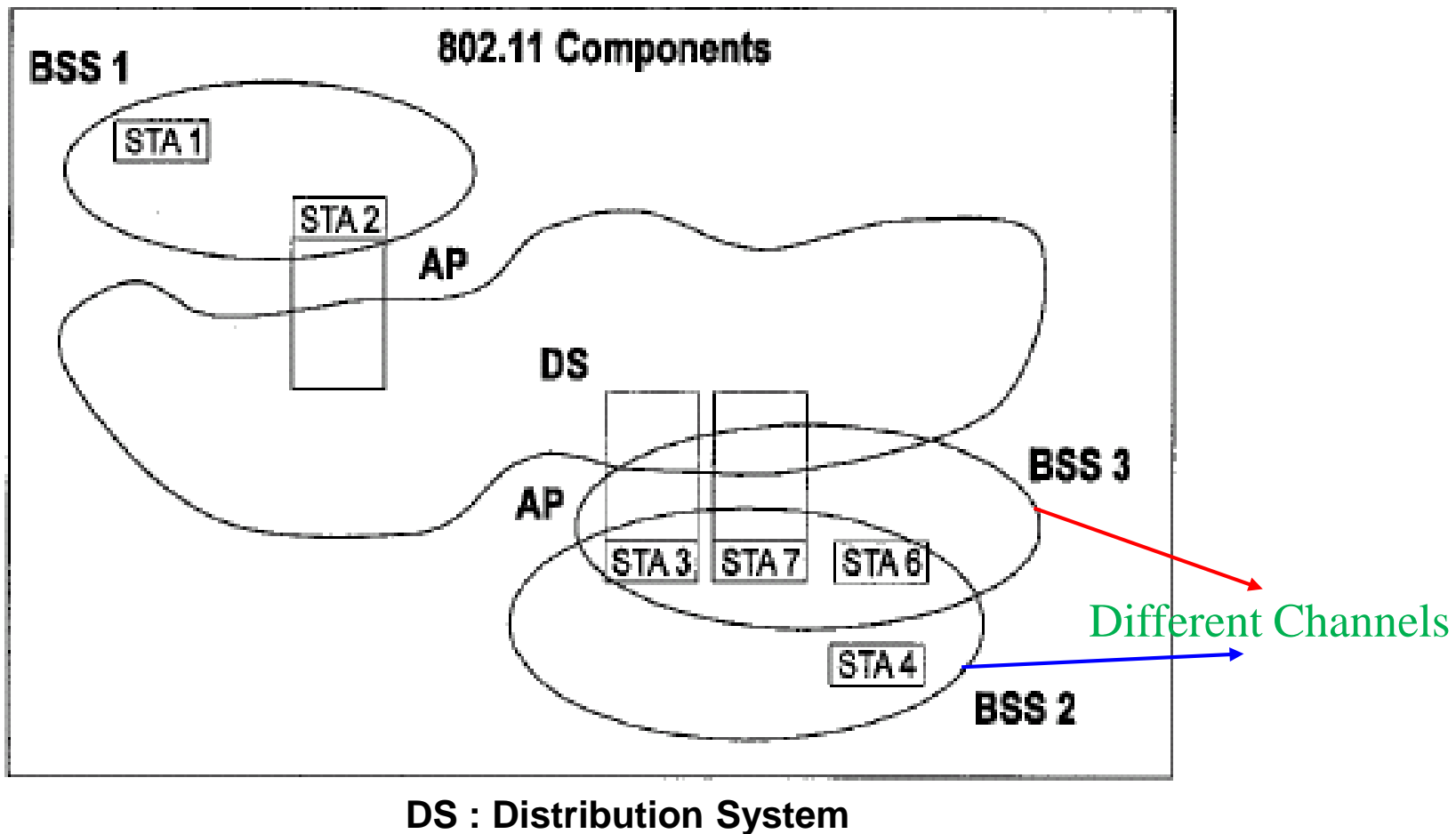
---

- **Used to interconnect wireless cells**
  - multiple BSS connected together form an **ESS (Extended Service Set)**
  - **Allows mobile stations to access fixed resources**
  
- **Not part of 802.11 standard**
  - could be bridged IEEE LANs, wireless, other networks
  - **Only Distribution System Services are defined**

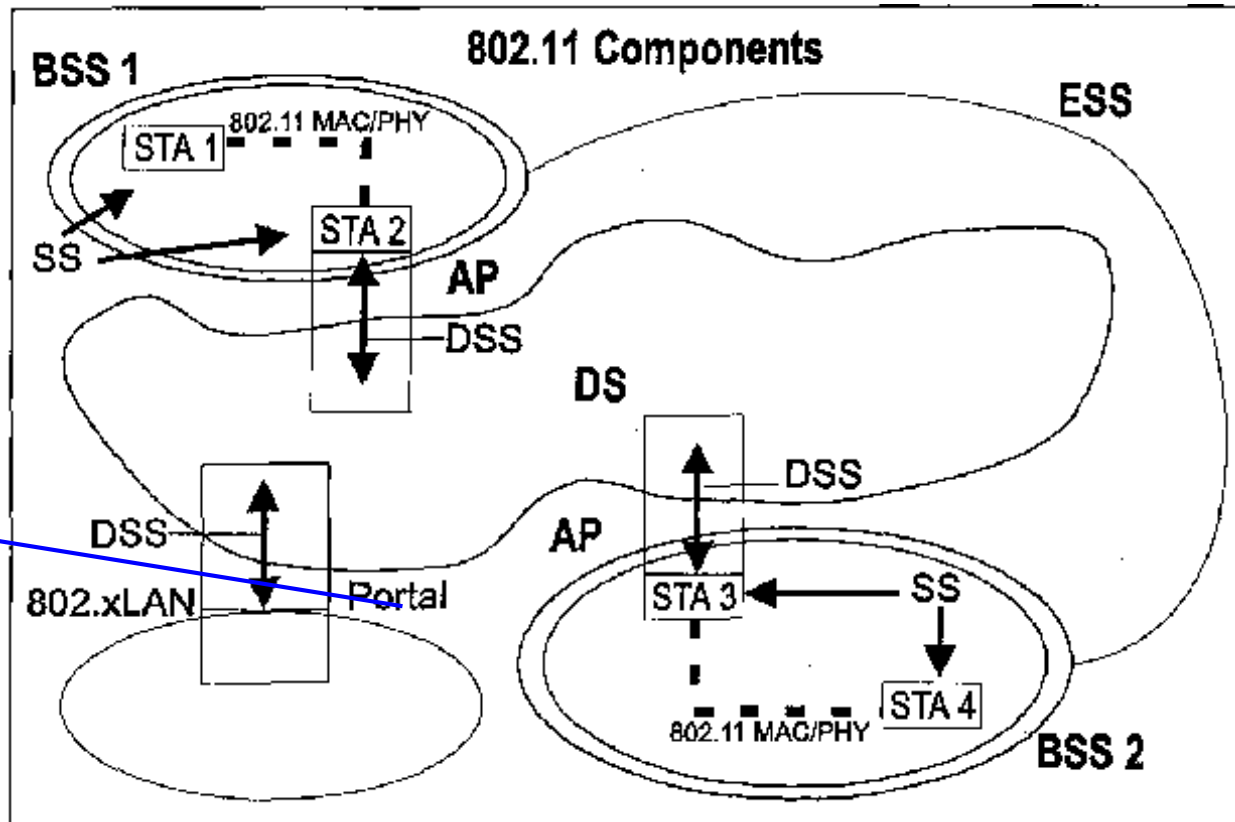
# BSS vs ESS



# Collocated Coverage Areas



# Complete Architecture



DSS : Distribution System Service



---

# Access Points

---

- Stations select an AP and **Associate** with it
- Support **roaming**
  - **IAPP (Inter Access Point Protocol) IEEE 802.11f (Layer 2)**
  - **Mobile IP (Layer 3; IETF)**
- Provide other functions
  - **time synchronization** (beaconing)
  - **power management** support (if any)
  - **point coordination function (PCF)** (if any)
- Traffic typically (but not always) flows through AP
  - direct communication possible (Ad-Hoc)

---

# Access Points

---

- **In an Infrastructure BSS, all mobile stations communicate with the AP**
  - quoted from “IEEE 802.11 Handbook”, Bob O’Hara and Al Petrick
  - Disadvantage :
    - » bandwidth is consumed **twice** than directional communication between STAs
    - » **more contentions** and more collisions
  - Advantage :
    - » easily solve **hidden terminal problem**
    - » provide **power saving** function
    - » meet the **AAA (authentication, authorized, accounting)** architecture
    - » **provide per flow bandwidth control, QoS guarantee (IEEE 802.11e)**

---

## 802.11 Defines the Airwaves IF

---

- **The airwaves interface between stations (including that between station and AP) is standardized**
  - PHY and MAC
- **No exposed MAC/PHY interface specified**
- **No exposed interface to Distribution System**
  - only required DS services are defined
- **Internals of Distribution System not defined**

---

# MAC Services

---

- **Asynchronous MSDU Data Delivery**
  - provided to **LLC (2304 octets maximum)**
- **Time Bounded Services**
  - optional point coordination function (**PCF**)
  - Existing in commercial products ?
    - » **Bandwidth is not enough for supporting real-time service**
    - » **Not necessary, CSMA/CA works well (likes Ethernet history)**
    - » **IEEE 802.11e enhances QoS**
- **Security Services**
  - confidentiality, **authentication**, access control
- **Management Services**
  - scanning, joining, roaming, **power management**

---

# MAC Functionality

---

- **Independent and Infrastructure configuration support**
  - Each BSS has a unique **48** bit address
  - Each ESS has a **variable** length address
- **CSMA with collision avoidance (CSMA/CA)**
  - MAC level **acknowledgment (positive acknowledgement)**
  - allows for **RTS/CTS** exchanges
    - » **hidden node protection** 41%
    - » **virtual carrier sense**
    - » **bandwidth saving**
  - MSDU fragmentation
  - Point Coordination Function (option)
    - » **AP polling**

---

## MAC Functionality (continued)

---

- **Roaming support within an ESS**
  - station **scans** for APs, **association** handshakes
- **Power management support**
  - stations may power themselves down
  - **AP buffering**, distributed approach for IBSS
- **Authentication and privacy**
  - Optional support of Wired Equivalent Privacy (**WEP**)
  - Key exchange
  - Authentication handshakes defined
  - **IEEE 802.1x** spec. enhances authentication control (EAP)
  - **IEEE 802.11i** enhances security (IEEE 802.11i over IEEE 802.1x)

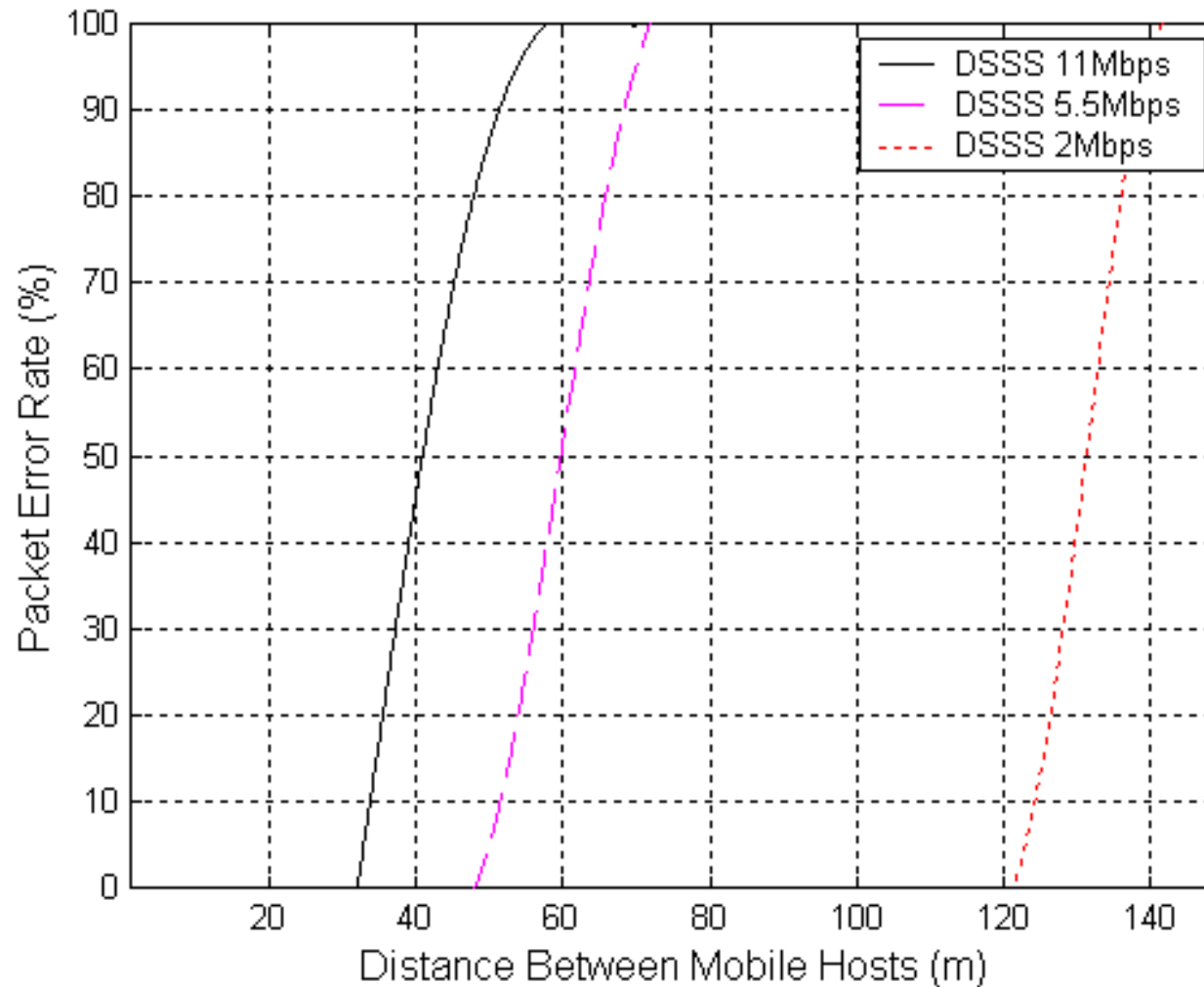
---

# PHY Layer Services

---

- **PHY\_DATA transfers**
  - multiple rates (1, 2, 5.5, 11Mbps)
  - extended rates (22, 33 or 6, 9, 12, 19, 24, 36, 48, 54Mbps)
  - The algorithm for performing rate switching is beyond the scope of the standard. (p6, 802.11b)
    - » Question : how to decide the proper data rate ?
- **Clear Channel Assessment (CCA)**
  - carrier sense
  - detect start frame delimiter
- **PHY Management**
  - channel tuning

# Data Rate vs. Range





---

# Four PHYs

---

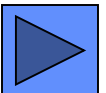
- **Frequency Hopping Spread Spectrum (FHSS)**
  - **2.4 GHz** band, **1** and **2** Mbps transmission
    - » 2GFSK, 4GFSK
    - » **2.5** hops/sec over **79 1MHz** channels (North America)
- **Direct Sequence Spread Spectrum (DSSS)**
  - **2.4 GHz** band, **1** and **2** Mbps transmission
    - » 11 chip Barker sequence
    - » DBPSK, DQPSK (Differential Binary/Quadrature Phase Shift Keying)
  - **2.4 GHz** band, **5.5** and **11** Mbps transmission
    - » CCK (Complementary Code Keying), PBCC (Packet Binary Convolutional Code)
    - » CCK : DQPSK(5.5Mbps, 11Mbps)
    - » PBCC : BPSK(5.5Mbps), QPSK(11Mbps) (optional)
    - » Sep. 1999 (**802.11b**)
  - **2.4 GHz** band, **22** and **33** Mbps transmission
    - » PBCC-22, PBCC-33

---

# Four PHYs

---

- **Baseband IR (Infrared)**
  - Diffuse infrared
  - **1** and **2** Mbps transmission, 16-PPM and 4-PPM
    - » PPM : Pulse Position Modulation
- **Orthogonal Frequency Division Multiplexing (OFDM)**
  - **2.4 GHz** band (IEEE 802.11g DSSS-OFDM, OFDM)
  - **5 GHz** band (IEEE 802.11a)
    - » Similar ETSI HIPERLAN/II PHY Spec.
  - **6, 9, 12, 18, 24, 36, 48** and **54** Mbps
    - » BPSK(6,9Mbps), QPSK(12,18Mbps), 16-QAM(24,36Mbps), 64-QAM(48,54Mbps)
    - » Convolutional Code with coding rates  $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}$ .
    - » **20MHz/64 subcarriers per channel**
      - 52 subcarriers occupy 16.6MHz
      - 12 additional subcarriers are used to normalized the average power of OFDM symbol
    - » Mandatory : **6, 12, 24** Mbps
    - » Extended (turbo mode 5-UP protocol): **72/108Mbps** (proposed by Atheros Corp.)



---

# Unlicensed Operation RF Bands

---

- **902MHz**
  - 26MHz BW (902-928MHz)
  - Crowded and Worldwide limited
  - IEEE 802.11 WLAN, IEEE 802.15.4 LR-WPAN, coreless phone, .etc.,
- **2.4GHz**
  - 83.5MHz BW (2400-2483.5MHz)
  - Available worldwide
  - IEEE 802.11(b/g) WLAN, Bluetooth, IEEE 802.15.4 LR-WPAN and IEEE 802.15.6 WBAN, etc.,
- **5.1GHz**
  - 300MHz (three 100MHz segments)
  - Unlicensed NII
  - **802.11a WLAN**
    - » OFDM / 6,12,18,24,36,48,54Mbps / BPSK,QPSK,16-QAM, 64-QAM
  - **HiperLAN I and HiperLAN II**
    - » 23.5Mbps/GMSK and 6-54Mbps/BPSK,QPSK,16-QAM, 64-QAM

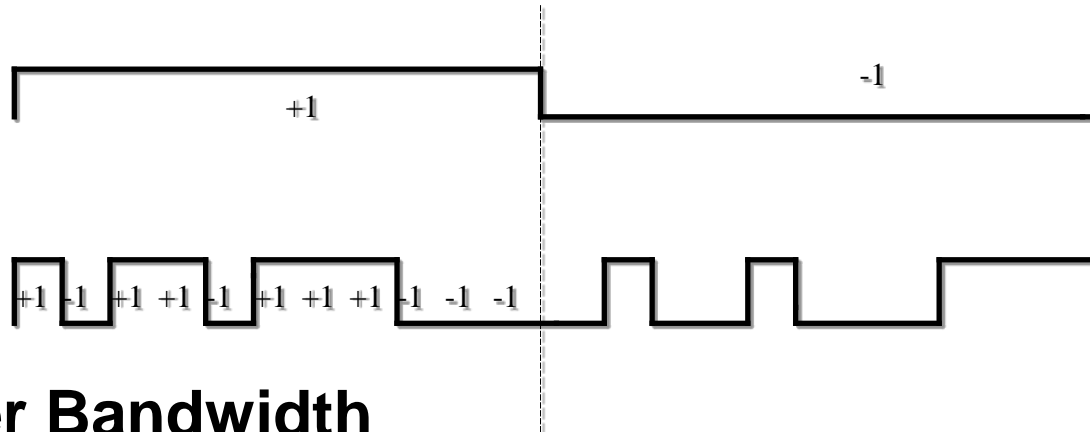
---

---

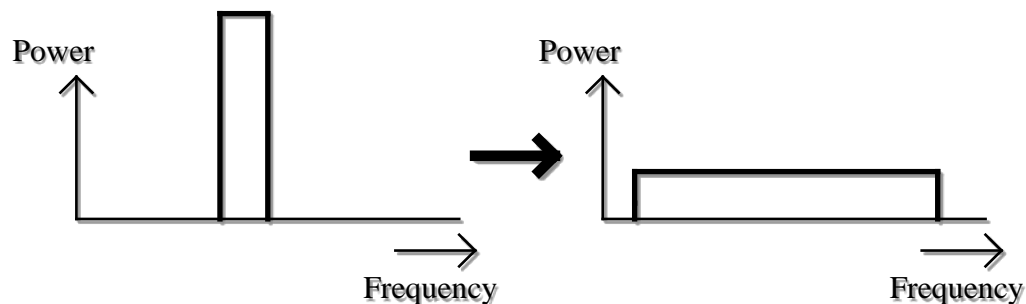
# 3. Direct Sequence Spread Spectrum (DSSS) Physical Layer Specification

# What is DSSS?

- Signal symbol is spread with a sequence

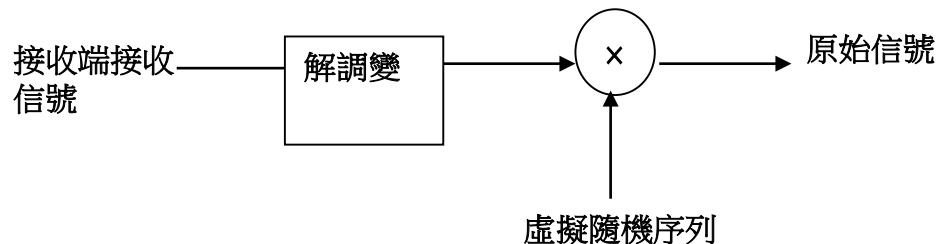
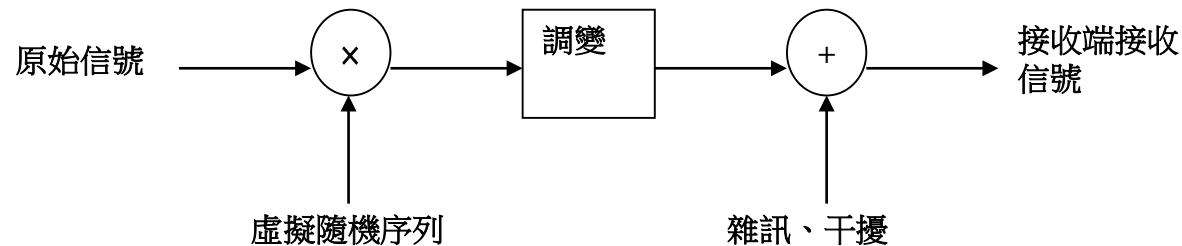


- Wider Bandwidth
- Less power density

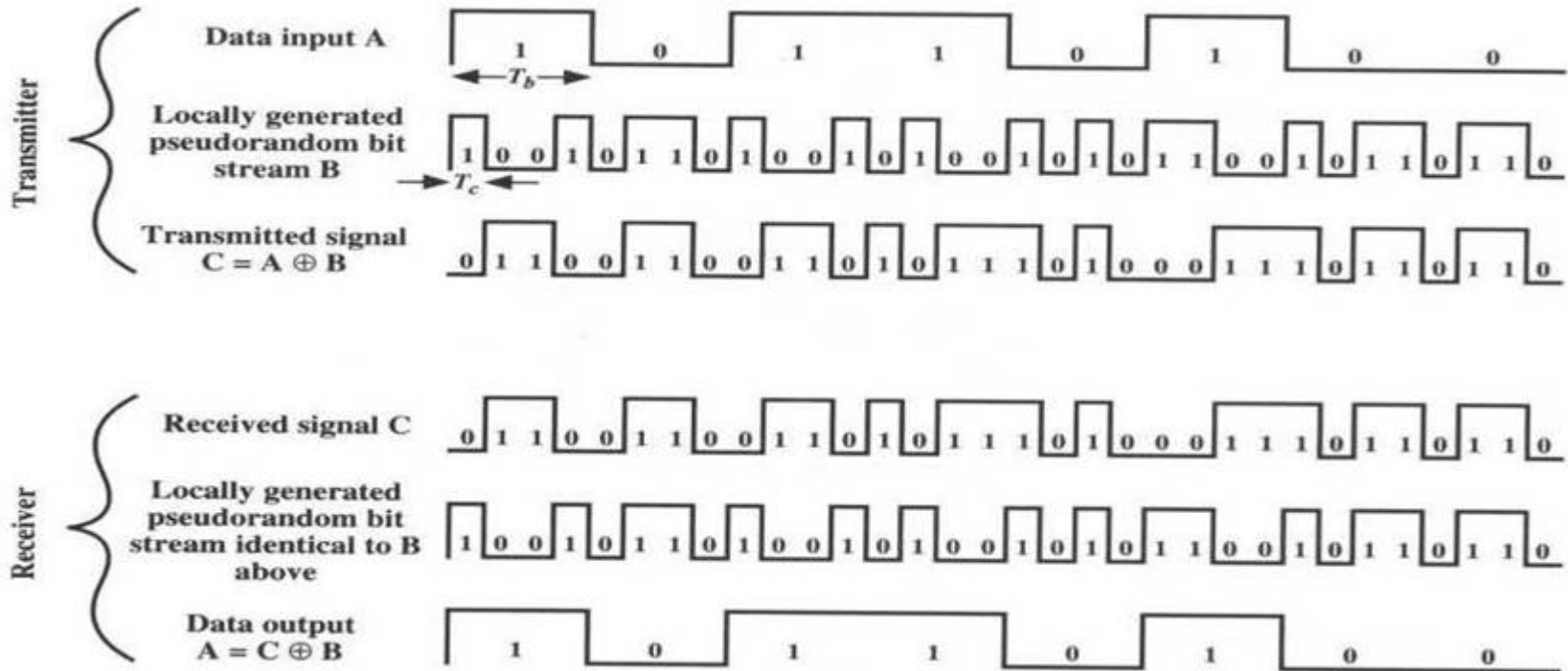


# 展頻技術-直接序列展頻

- 直接序列展頻技術（**Direct Sequence Spread Spectrum : DSSS**）是將原始信號乘上一虛擬隨機序列，再經過調變後送出去，當然在環境中會受到雜訊及干擾的影響，在接收端，會將接收到的信號經過解調變後，再乘上原本的虛擬隨機序列，最後就會將原始信號還原。



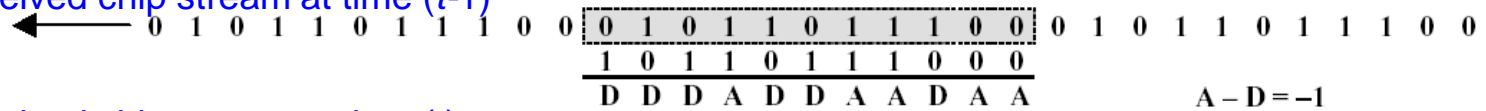
# DSSS



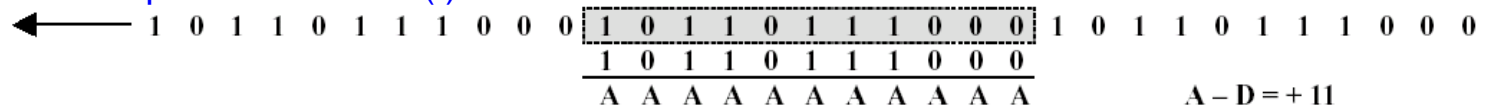
# 11 Chip BARKER Sequence

- Good **autocorrelation** properties
- **Minimal sequence** allowed by FCC
- **Coding gain 10.4 dB**

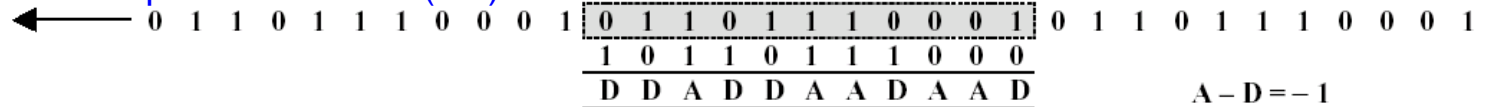
Received chip stream at time  $(t-1)$



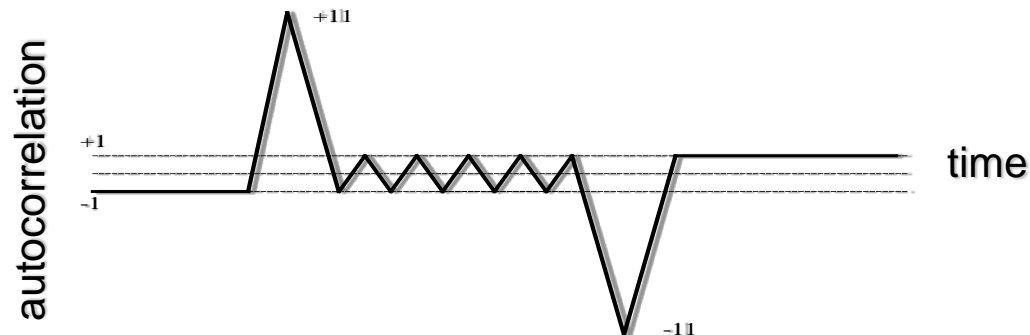
Received chip stream at time  $(t)$



Received chip stream at time  $(t+1)$



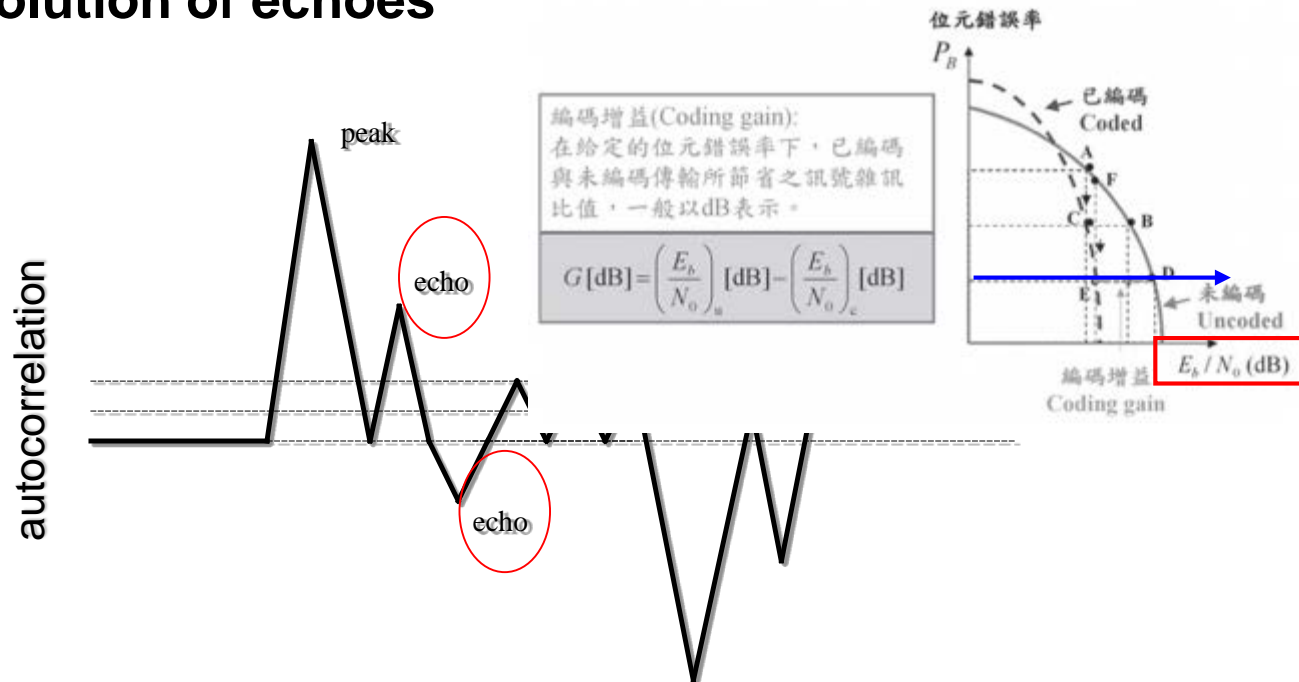
11-chip Barker sequence



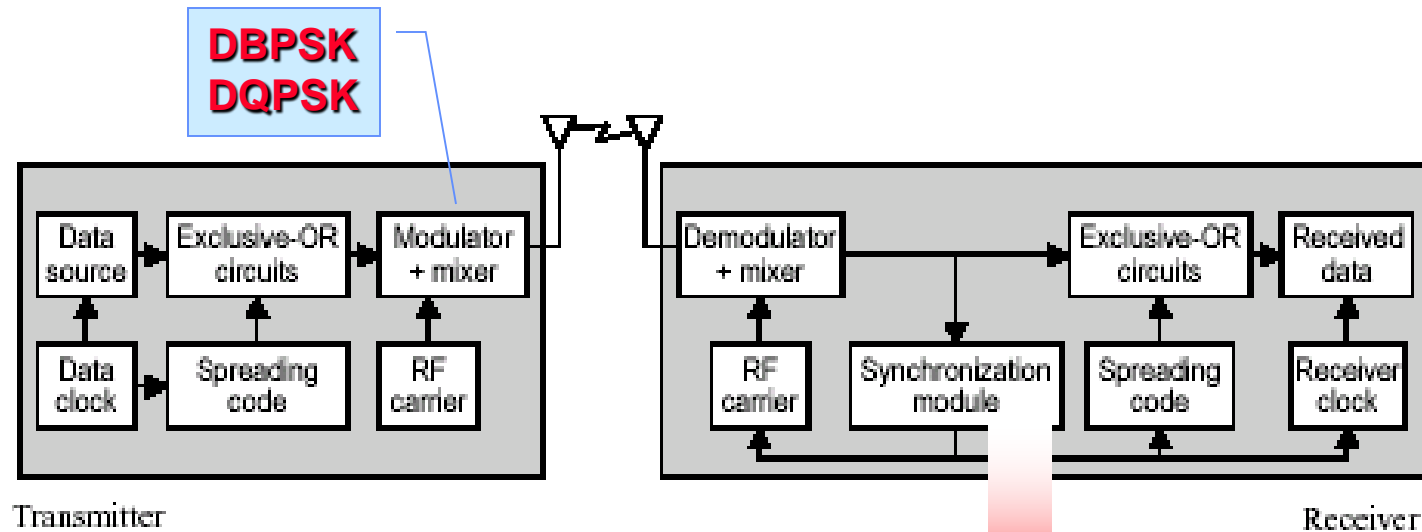


# DSSS Benefits

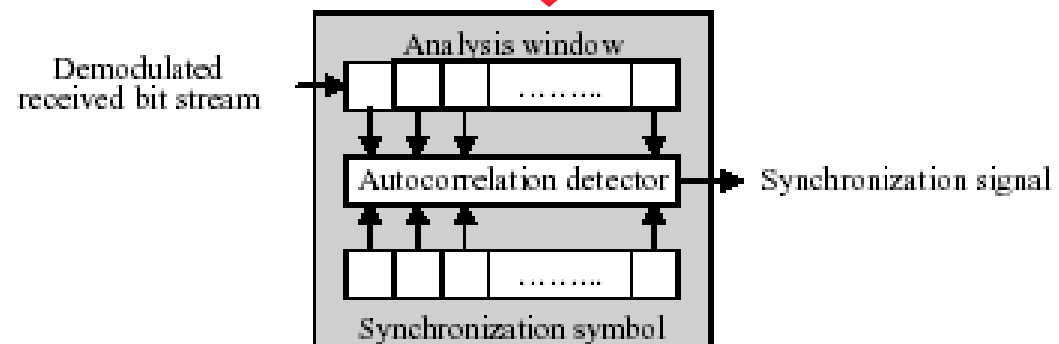
- 10 dB coding gain:
  - Robust against **interferers and noise** (10 dB suppression)
- Robust against **time delay spread**
  - Resolution of echoes



# DSSS Hardware Block Diagram



Transmitter and receiver schematic



Synchronization module schematic

---

# IEEE 802.11 DSSS PHY characteristics

---

- **2.4 GHz ISM band (FCC 15.247)**
- **1 and 2 Mb/s data rate**
  - DBPSK and DQPSK modulation
  - Chipping rate **11 MHz** with **11 chip Barker sequence**
- **5.5 and 11 Mbps (802.11b)**
  - **CCK** (QPSK, DQPSK modulations – mandatory)
  - **PBCC** (BPSK, QPSK modulations – optional)
- **22 and 33 Mbps (802.11g)**
  - **PBCC-22, PBCC-33** modulation (**TI proposal – optional**)
- **Multiple channels in 2.4 to 2.4835 GHz band**

# DSSS Channels

CHNL_ID	Frequencies	FCC Channel Frequencies	ETSI Channel Frequencies	Japan Frequency (MKK)	Japan Frequency (New MKK)
1	2412 MHz	X	X	-	X
2	2417 MHz	X	X	-	X
3	2422 MHz	X	X	-	X
4	2427 MHz	X	X	-	X
5	2432 MHz	X	X	-	X
6	2437 MHz	X	X	-	X
7	2442 MHz	X	X	-	X
8	2447 MHz	X	X	-	X
9	2452 MHz	X	X	-	X
10	2457 MHz	X	X	-	X
11	2462 MHz	X	X	-	X
12	2467 MHz	-	X	-	X
13	2472 MHz	-	X	-	X
14	2484 MHz	-	-	X	X

Table 1, DSSS PHY Frequency Channel Plan

- **FCC(US), IC(Canada) and ETSI(Europe) : 2.4GHz - 2.4835GHz**
- **Japan : 2.471GHz - 2.497GHz (MKK : channel 14; new MKK : channels 1-14)**
- **France : 2.4465GHz - 2.4835GHz (channels 10, 11, 12, 13)**
- **Spain : 2.445GHz - 2.475GHz (channels 10, 11)**
- **Adjacent cells using different channels :  $\geq 30\text{MHz}$  (25MHz in 802.11b)**
- **FCC pushes the unused unlicensed TV broadcasting band 3.65GHz-3.70GHz as WLAN band.**

---

## IEEE 802.11 PHY Terminology in Spec.(s)

---

- **1 Mbps : Basic Rate (BR)**
- **2 Mbps : Extended Rate (ER)**
- **5.5/11 Mbps : High Rate (HR)**
- **22~33/6~54 Mbps : Extended Rate PHY (ERP)**
- **150 Mbps : Multi-Input Multi-Output (MIMO); 11n**
- **500Mbps : IEEE 802.11ac**

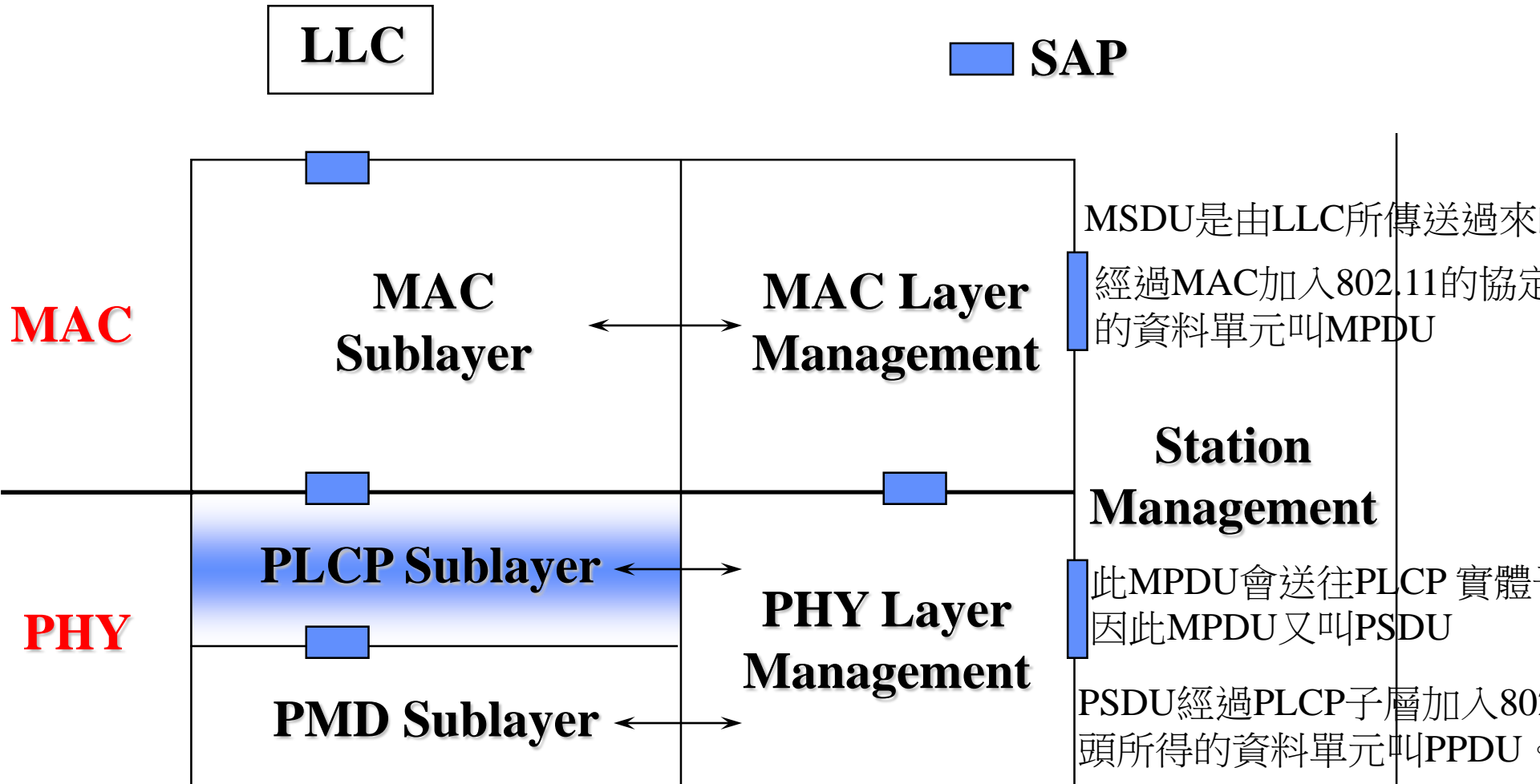
---

# PLCP Frame Formats in IEEE 802.11b

---

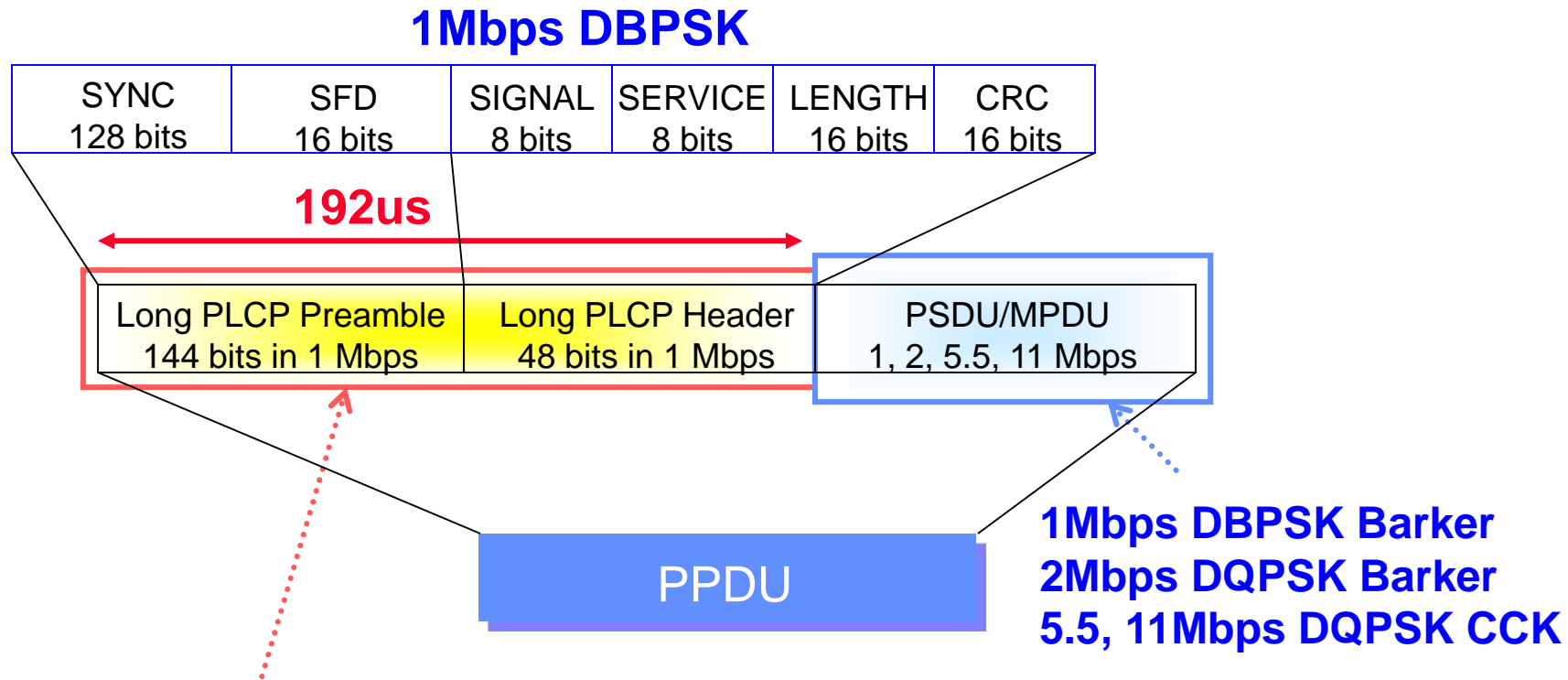
- Two different preamble and header formats
  - **Long PLCP PPDU format** (Mandatory in 802.11b)
    - » 144-bit preamble : 1Mbps DBPSK
    - » 48-bit header : 1Mbps DBPSK
    - » Spend 192us
    - » PSDU : 1, 2, 5.5, 11Mbps
    - » Compatible with 1 and 2 Mbps
  - **Short PLCP PPDU format** (Optional in 802.11b)
    - » Minimize overhead, maximize data throughput
    - » 72-bit preamble : 1Mbps DBPSK
    - » 48-bit header : 2Mbps DQPSK
    - » Spend 96us
    - » PSDU : 2, 5.5, 11 Mbps

# PLCP (PHY Convergence) Sublayer



# Long PLCP Frame Format

- Mandatory in 802.11b



**Preamble and Header always at 1Mb/s DBPSK Barker**



---

# Modulation

---

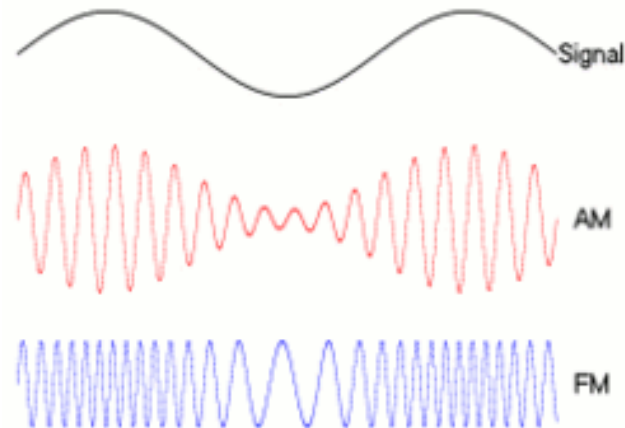
- **Modulation** is the process of varying one or more properties of a periodic waveform, called the carrier signal.
  - a modulating signal that typically contains information to be transmitted.
- Most radio systems in the 20th century used frequency modulation (FM) or amplitude modulation (AM) to make the carrier carry the radio broadcast.

---

# Modulation

---

- Modulation is a process of conveying message signal, for example, a digital bit stream or an analog audio signal, inside another signal that can be physically transmitted.
- Modulation of a sine waveform transforms a narrow frequency range baseband message signal into a moderate to high frequency range passband signal, one that can pass through a filter.



---

# Digital Modulation Methods

---

- Digital modulation methods can be considered as digital-to-analog conversion and the corresponding demodulation or detection as analog-to-digital conversion.
- The changes in the carrier signal are chosen from a finite number of **M** alternative symbols (the *modulation alphabet*).

---

## Example

---

- A telephone line is designed for transferring audible sounds, for example, tones, and not digital bits (zeros and ones).
- Computers may communicate over a telephone line by means of modems, which are representing the digital bits by tones, called symbols.
- If there are four alternative symbols (corresponding to a musical instrument that can generate four different tones, one at a time), the first symbol may represent the bit sequence 00, the second 01, the third 10 and the fourth 11.

---

## Example

---

- If the modem plays a melody consisting of 1000 tones per second, the symbol rate is 1000 symbols/second, or baud.
- Since each tone (i.e., symbol) represents a message consisting of two digital bits in this example, the bit rate is twice the symbol rate, i.e. 2000 bits per second.
  - This is similar to the technique used by dial-up modems as opposed to DSL modems.

---

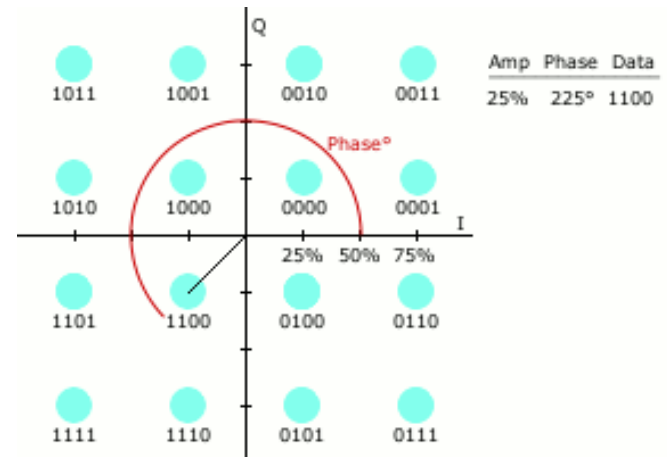
# Fundamental Digital Modulation Methods

---

- The most fundamental digital modulation techniques are based on keying:
  - PSK (phase-shift keying): a finite number of phases are used.
  - FSK (frequency-shift keying): a finite number of frequencies are used.
  - ASK (amplitude-shift keying): a finite number of amplitudes are used.
  - QAM (quadrature amplitude modulation): a finite number of at least two phases and at least two amplitudes are used.

# QAM

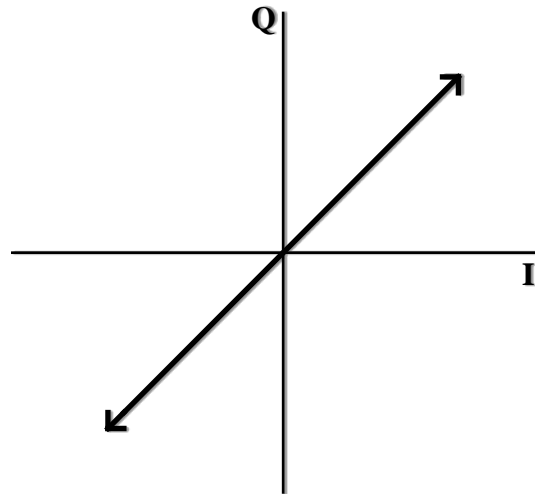
- An in-phase signal (or **I**, with one example being a cosine waveform) and a quadrature phase signal (or **Q**, with an example being a sine wave) are amplitude modulated with a finite number of amplitudes and then summed.
- It can be seen as a two-channel system, each channel using ASK. The resulting signal is equivalent to a combination of PSK and ASK.



---

# DBPSK Modulation

---

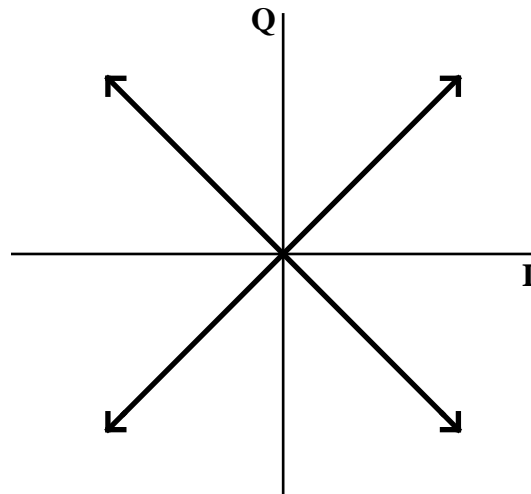


Bit Input	Phase Change ( $+j\omega$ )
0	0
1	$\pi$

Table 1, 1 Mb/s DBPSK Encoding Table.



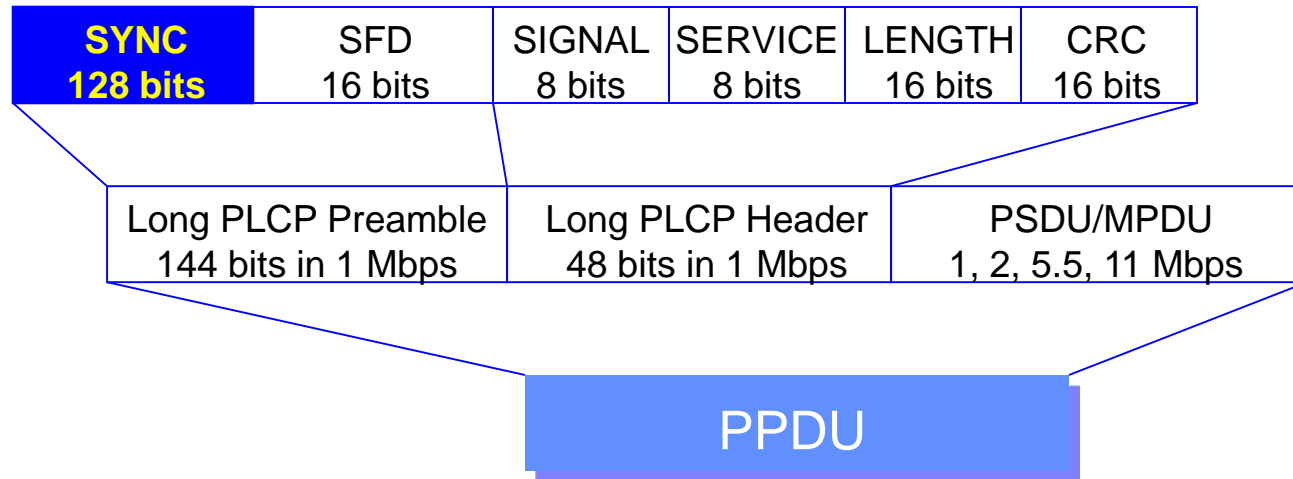
# DQPSK Modulation



Dibit pattern (d0,d1) d0 is first in time	Phase Change (+j $\omega$ )
00	0
01	$\pi/2$
11	$\pi$
10	$3\pi/2$ ( $-\pi/2$ )

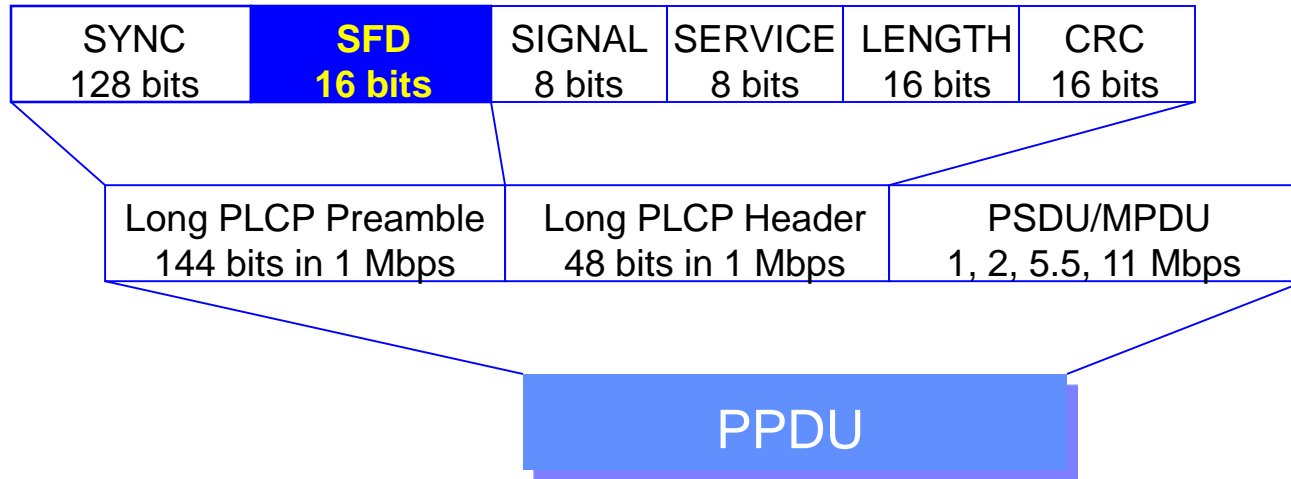
Table 1, 2 Mb/s DQPSK Encoding Table

# PLCP synchronization



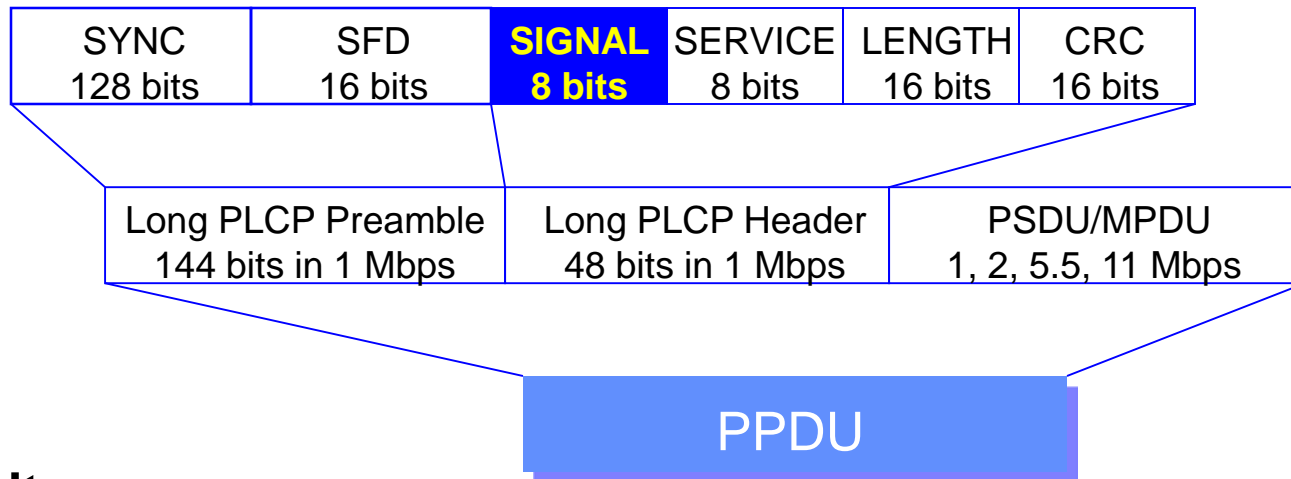
- **128** one bits ('1')
- **scrambled** by scrambler
- Used for receiver to clock on to the signal and to correlate to the PN (Pseudo Noise) code

# Start Frame Delimiter



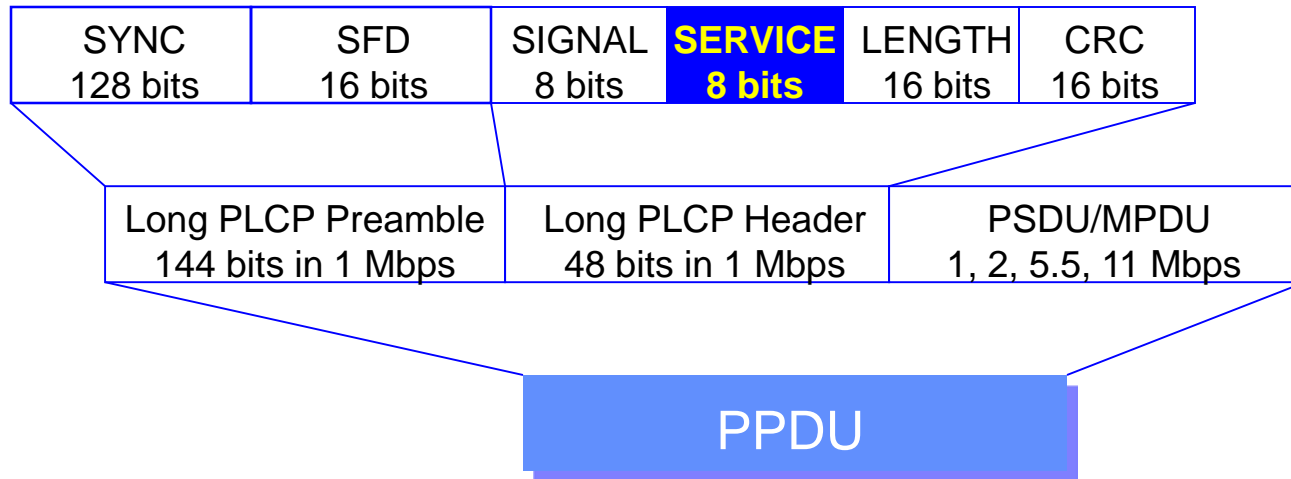
- **16 bit field (hF3A0)**
- **used for**
  - **bit synchronization**

# Signal Field



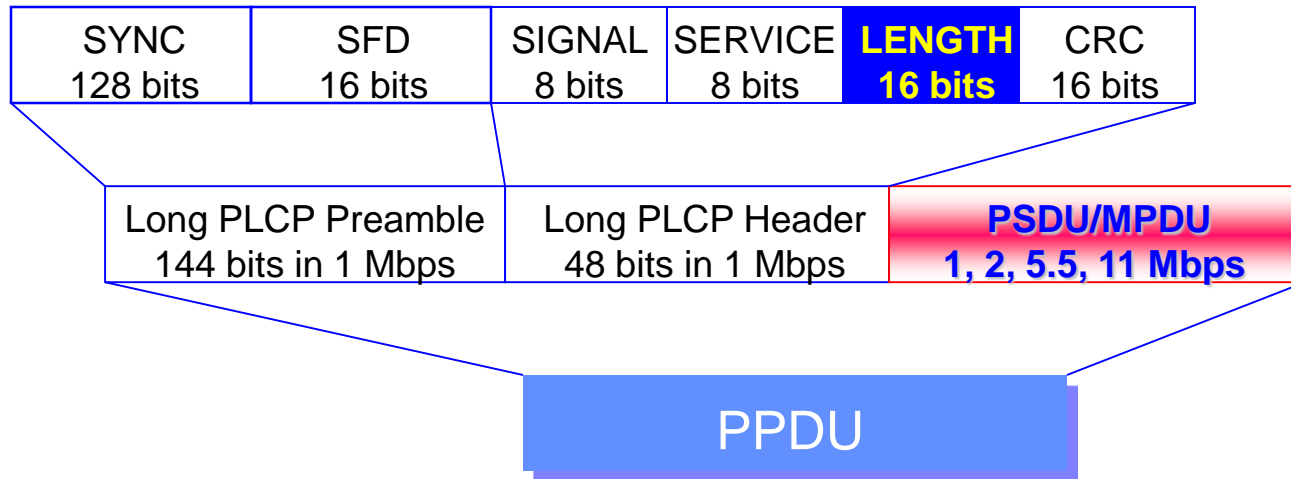
- **8 bits**
- **Rate indication**
  - **h0A** 1Mb/s DBPSK
  - **h14** 2Mb/s DQPSK
  - **h37** 5.5Mb/s CCK or PBCC
  - **h6E** 11Mbps CCK or PBCC
- **Other values reserved for future use (100 kb/s quantities)**

# Service Field



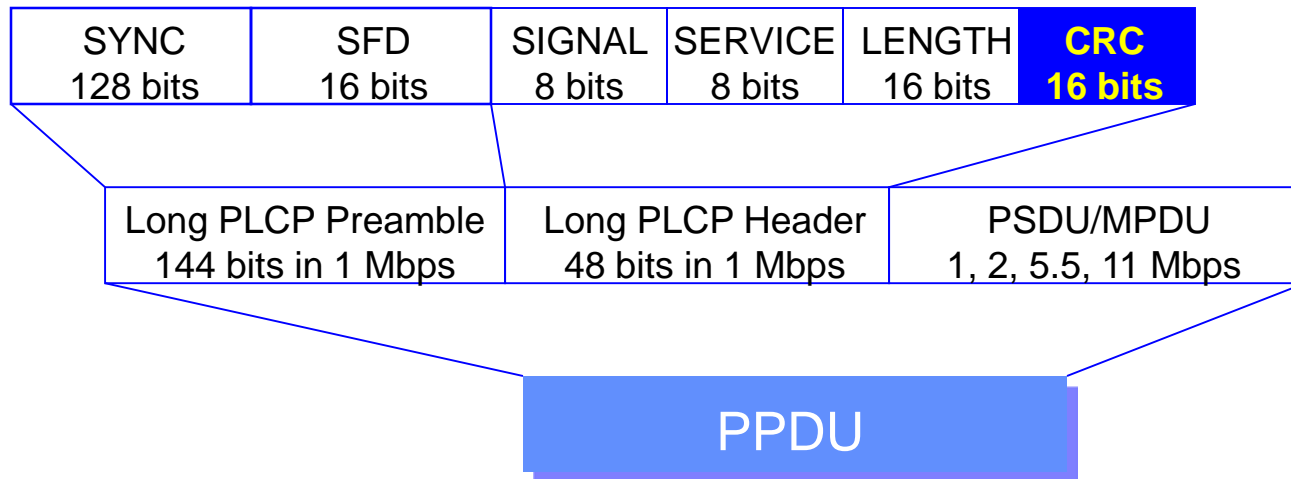
- **Reserved for future use**
  - **Bit 2 : locked clock bit**
    - » Indicate transmit freq. (mixer) & symbol clocks (baseband) derived from same oscillator
    - » **optional in 802.11b and mandatory in 802.11g**
  - **Bit 3 : modulation selection**
    - » 0 : CCK / 1 : PBCC
  - **Bit 7 : length extension bit (in the case datarate > 8Mbps)**
- **h00 signifies 802.11 compliant**

# Length Field



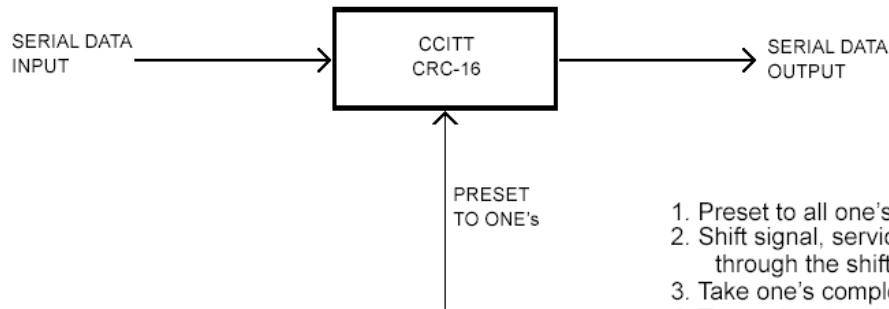
- Indicates number of **microseconds** to be transmitted in PSDU/MPDU
  - Decided by Length and datarate (in TXvector)
- Used for
  - End of frame detection
  - Perform Virtual Carrier Sense (for those with lower datarate)
  - MPDU CRC sync

# CRC field

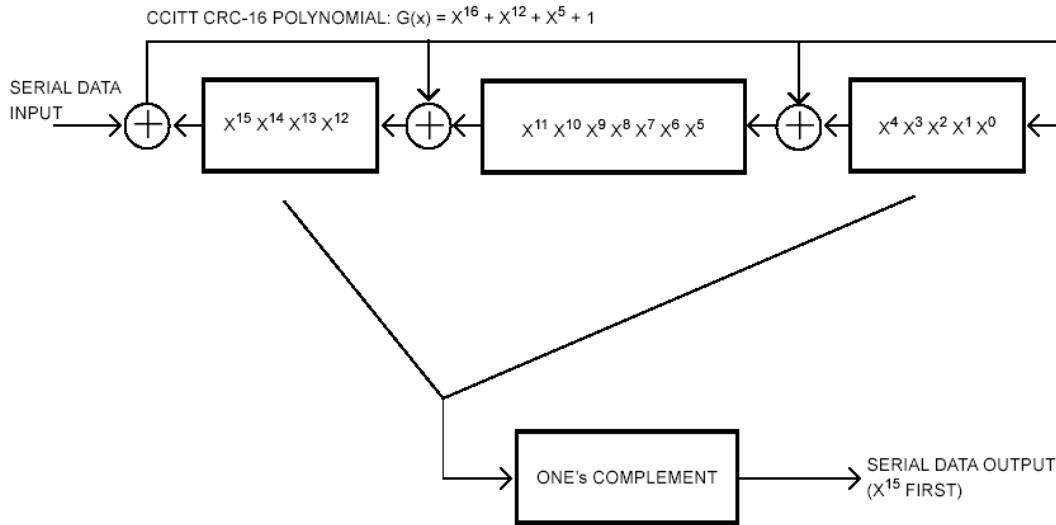


- **CCITT CRC-16**
- **Protects Signal, Service and Length Field**

# CRC Implementation



1. Preset to all one's
2. Shift signal, service length fields through the shift register
3. Take one's complement of the remainder
4. Transmit out serial  $X^{15}$  first



Data	CRC Registers
	msb                      lsb
	1111111111111111
0	1110111111101111
1	1101111111011110
0	1010111101011101
1	0101111010111010
0	1011110101110100
0	0110101011001001
0	1101010110010010
0	1011101100000101
0	0110011000101011
0	1100110001010110
0	1000100010001101
0	0000000100111011
0	0000001001110110
0	0000010011101100
0	0000100111011000
0	0001001110110000
0	0010011101100000
0	0100111011000000
0	1001110110000000
0	0010101100100001
0	0101011001000010
0	1010110010000100
1	0101100100001000
1	1010001000110001
0	0101010001000011
0	1010100010000110
0	0100000100101101
0	1000001001011010
0	0001010010010101
0	0010100100101010
0	0101001001010100
0	1010010010101000