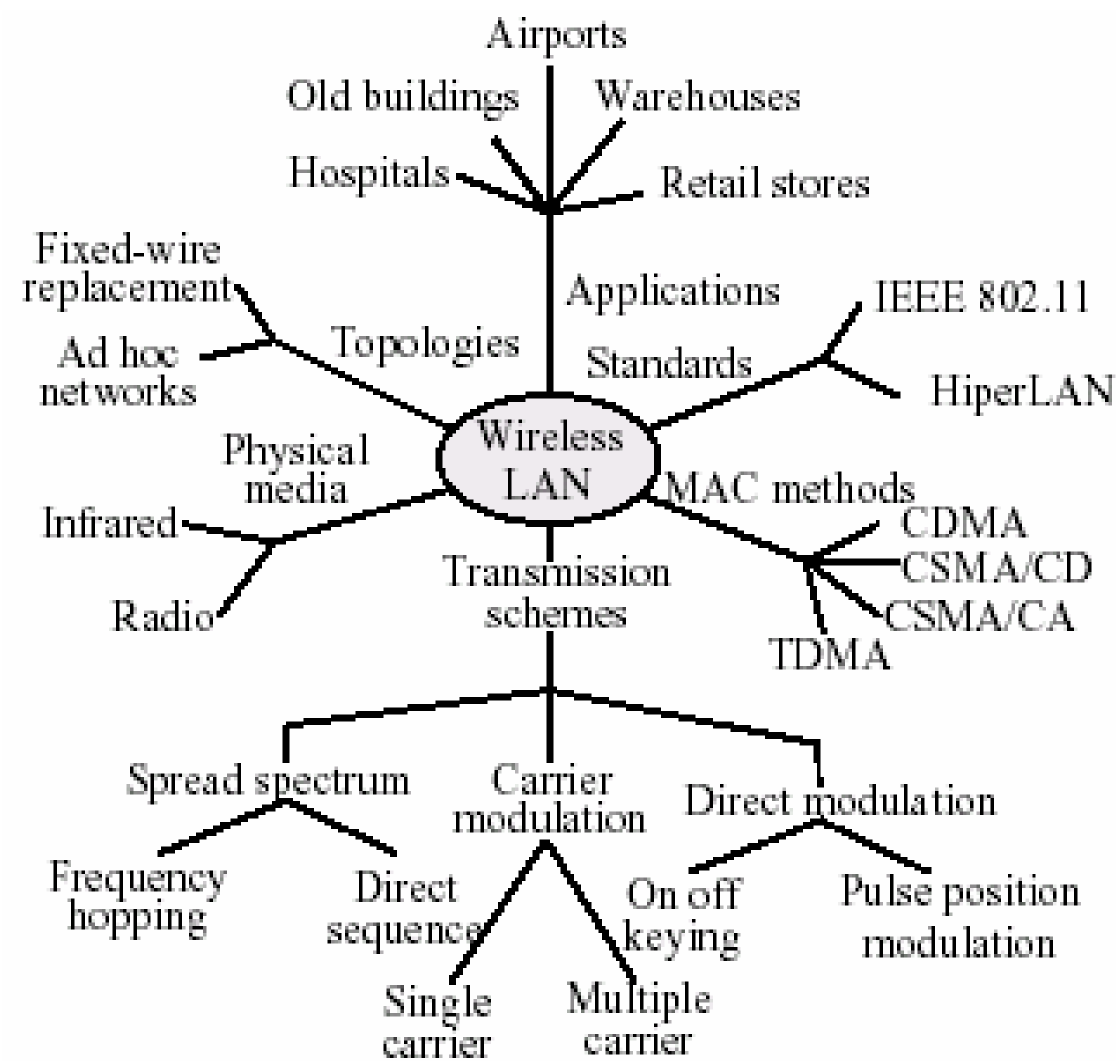
無線通訊協定

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

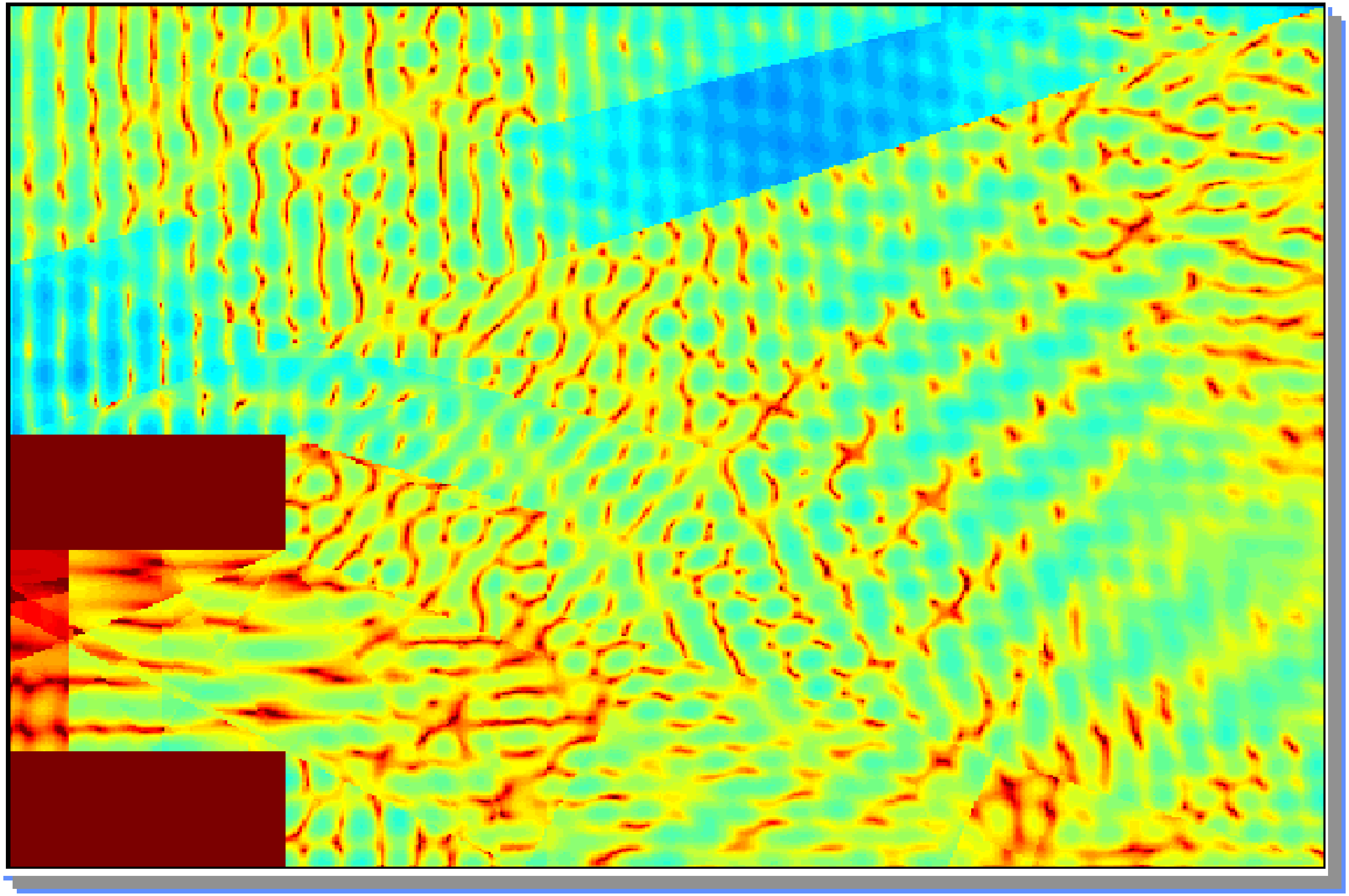


HomeRF
Bluetooth

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, 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
  - want seamless connections

- **Security**
  - no physical boundaries
  - overlapping LANs

Requirements

- Single MAC to support multiple PHYs.
  – Support single and multiple channel PHYs.
  – PHYs with 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.

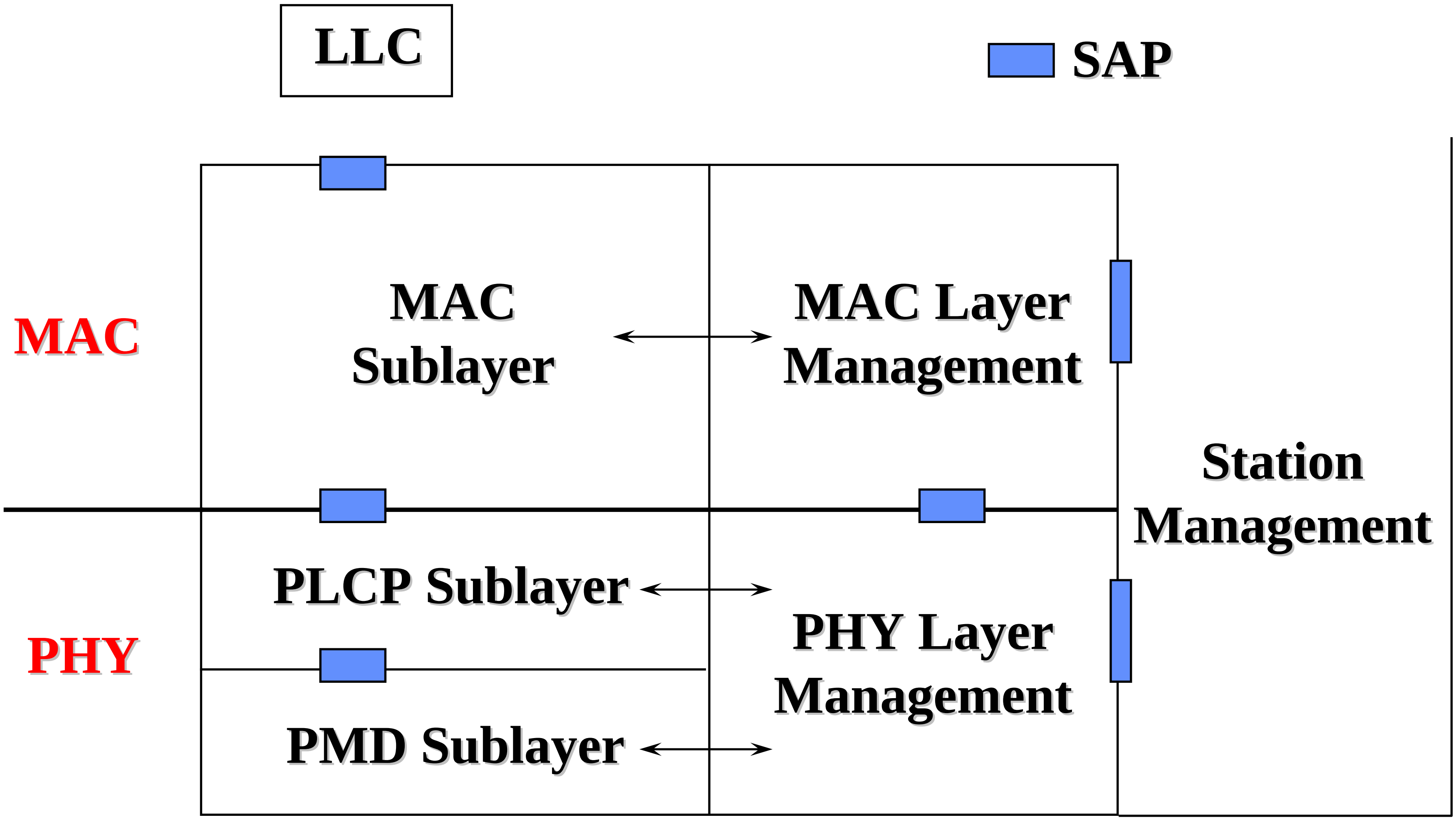
Architecture Overview

- **One MAC supporting multiple PHYs**
  - **Frequency Hopping Spread Spectrum**
  - **Direct Sequence Spread Spectrum**
  - **Infrared**
  - **Orthogonal Frequency Division Multiplexing**

- **Two configurations**
  - **Independent (ad hoc) and Infrastructure**
  - Hybrid configuration has being studied

- **CSMA/CA (collision avoidance) with optional Point Coordination Function (PCF)**

802.11 Protocol Entities



802.11 Protocol Architecture

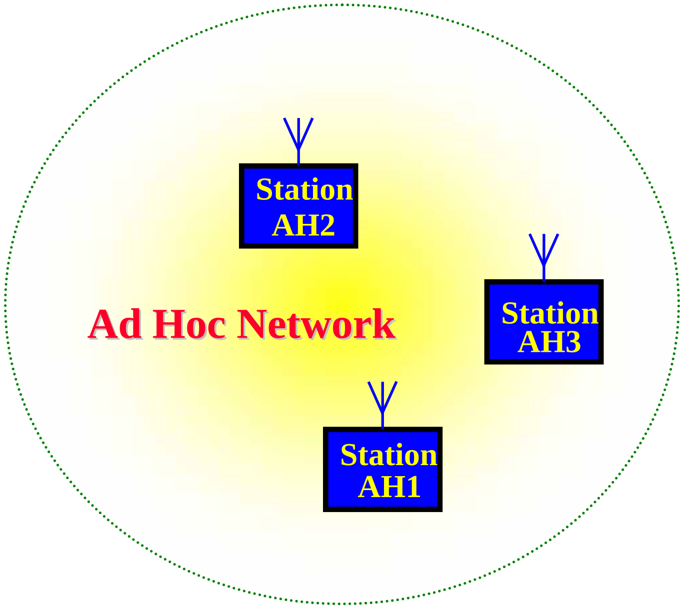
- **MAC Entity**
  - basic access mechanism
  - fragmentation/defragmentation
  - encryption/decryption
- **MAC Layer Management Entity**
  - synchronization
  - power management
  - roaming
  - MAC MIB
- **Physical Layer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides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

802.11 Protocol Architecture (cont.)

- **Physical Medium Dependent Sublayer (PMD)**
  - **modulation and encoding**
- **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
- **Current research topics**
  - Multi-Hop Routing (IETF MANET)
  - Multicasting
  - Multi-channel Access
  - Security
  - QoS ...

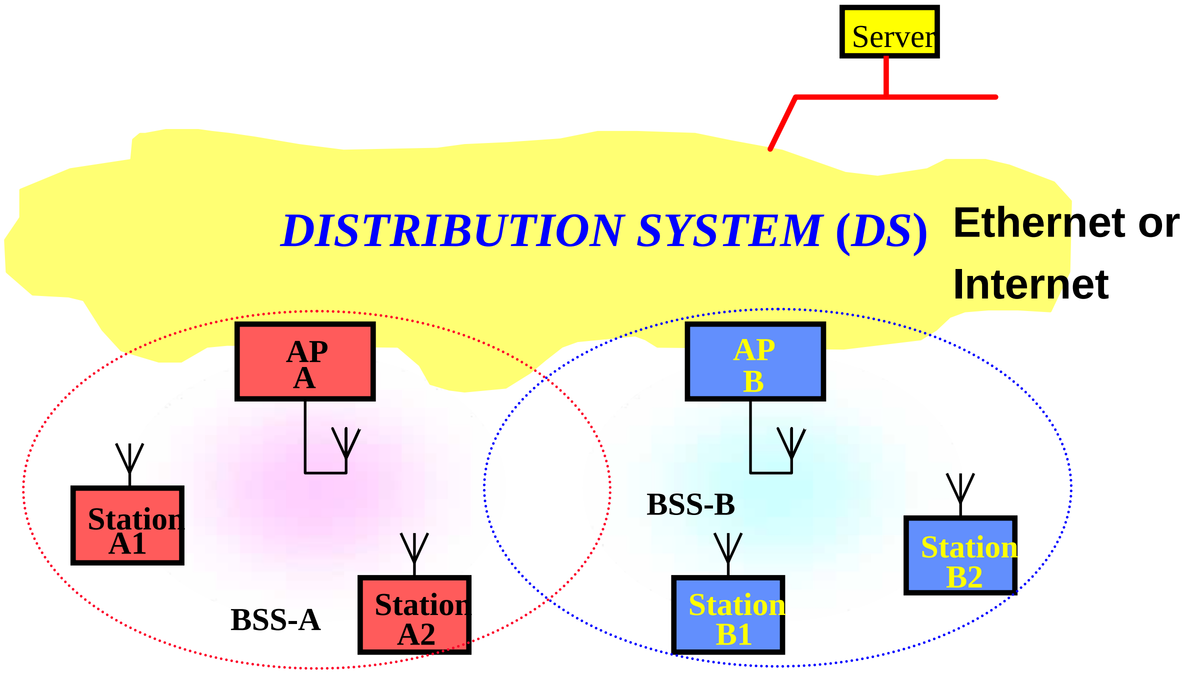


Mobile Station : STA

Commercial Products : WLAN Cards

- **One piece**
- **Two pieces**

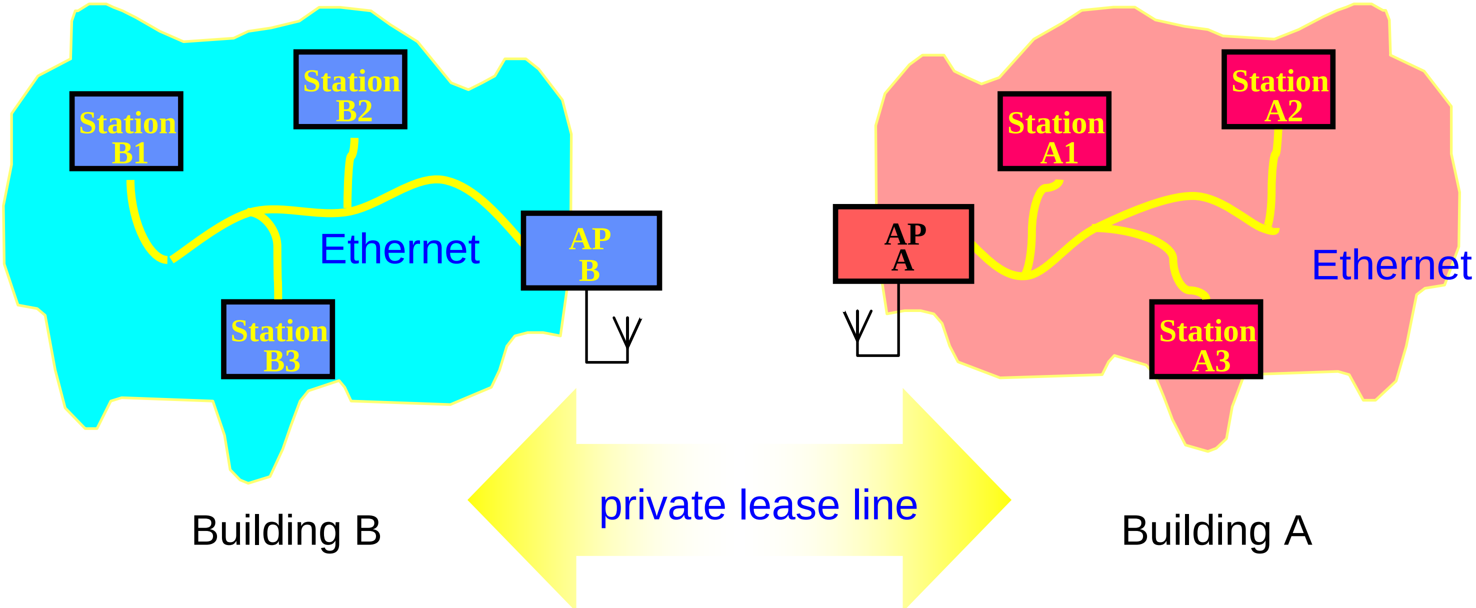
802.11 Configurations - Infrastructure



- **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

Wireless Bridging



Data Rate
Cost ?
Legal ?
Security ?
Range ?

Outdoor Application

8.6 Mile 802.11 Link using home built antenna's

Outdoor Application - Antenna

Antennas

Outdoor Application

Antennas

6.5 Miles distance. Average speed 2- 3 Mbps.

Long Distances

- **Security Issue :**
  - **The transmission distance can be up to**

    25Miles

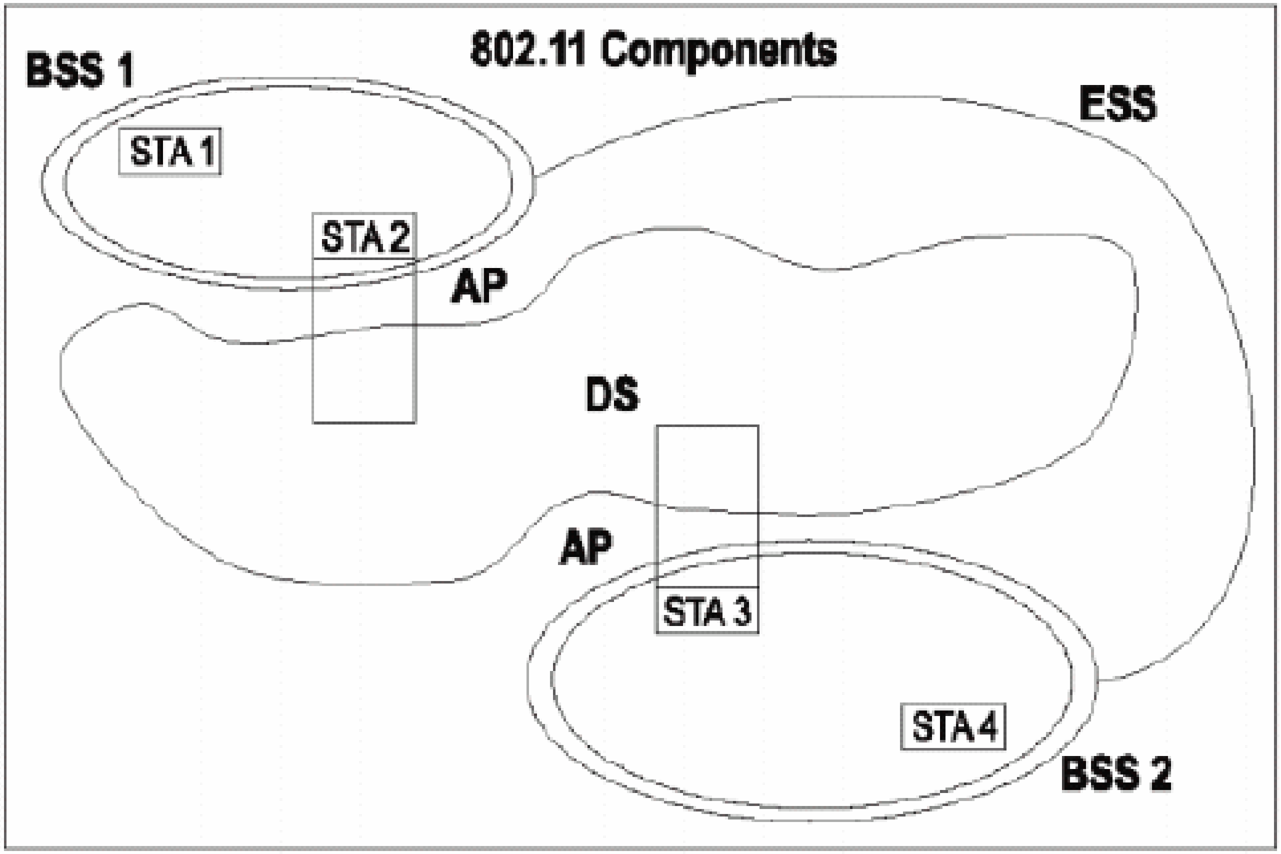
  - **If the AP is distanced from the street or on a high floor of a building, users will be safe from network trespassers.**

Distribution System

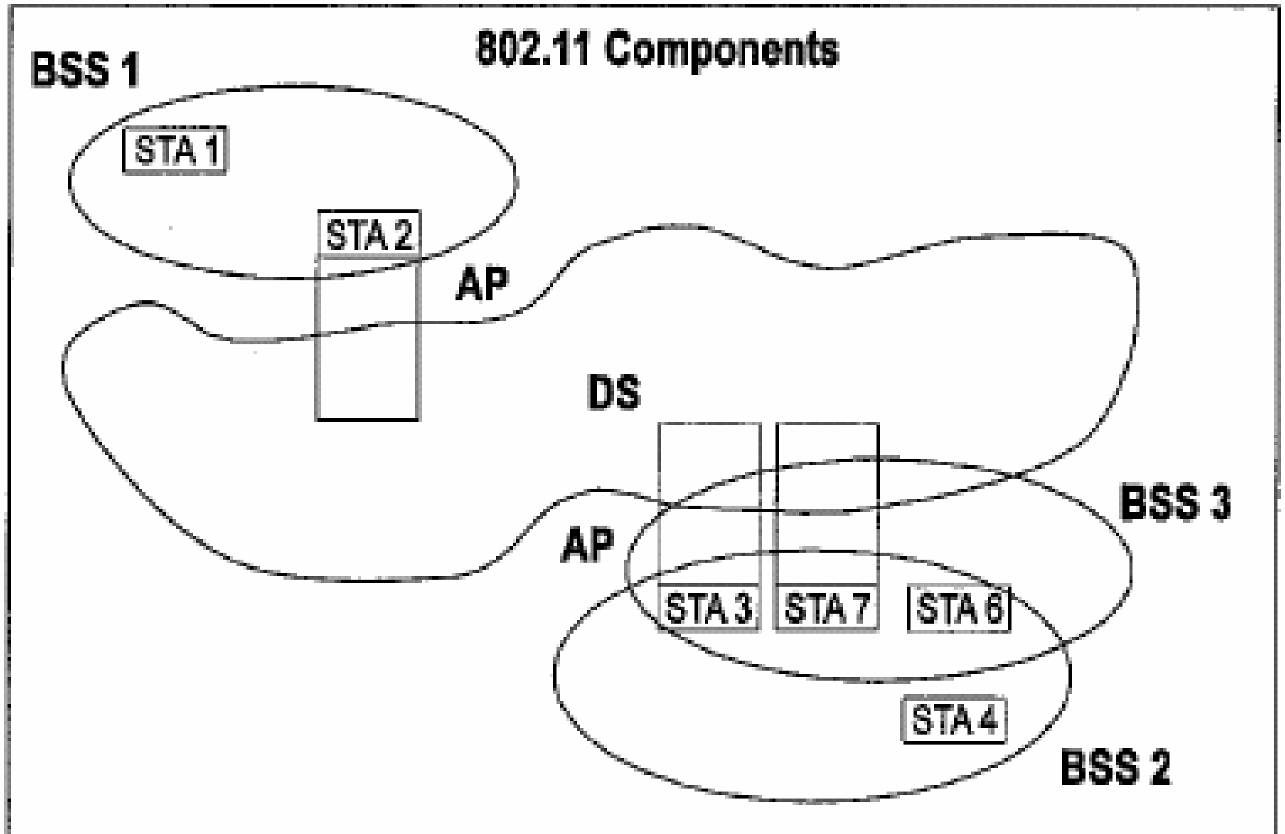
- **Used to interconnect wireless cells**
  - **multiple BSS connected together form an ESS (Extended Service Set)**
  - **Allows mobile stations to access fixed resources**

- **Not part of 802.11 standard**
  - **could be bridged IEEE LANs, wireless, other networks**
  - **Only Distribution System Services are defined**

BSS vs ESS

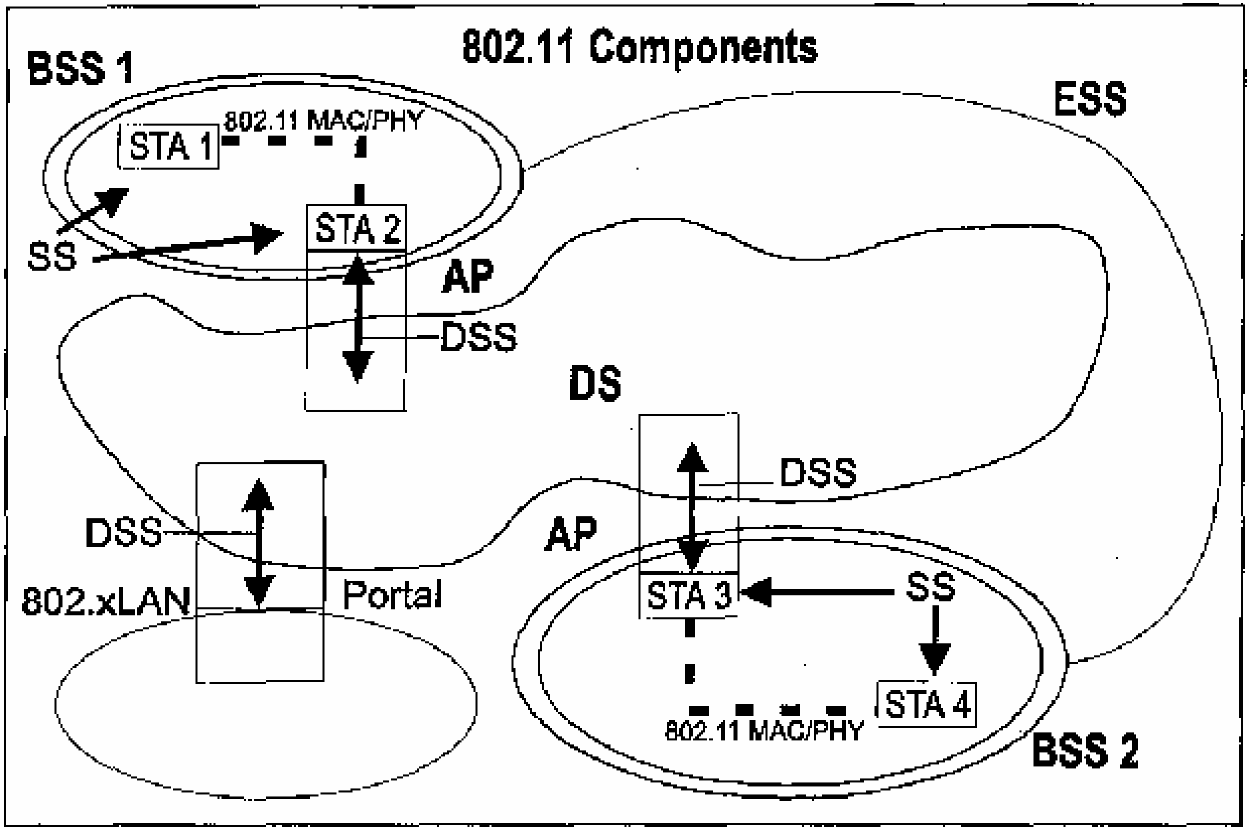


Collocated Coverage Areas



DS : Distribution System

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
  - Mobile IP
- 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

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 (in the near future)

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)**
    - » **Digitalocean Corp. “Starfish II” AP.**
    - » **IEEE 802.11e draft 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
    - » virtual carrier sense
    - » bandwidth saving
  - MSDU fragmentation
  - Point Coordination Function option
    - » AP polling

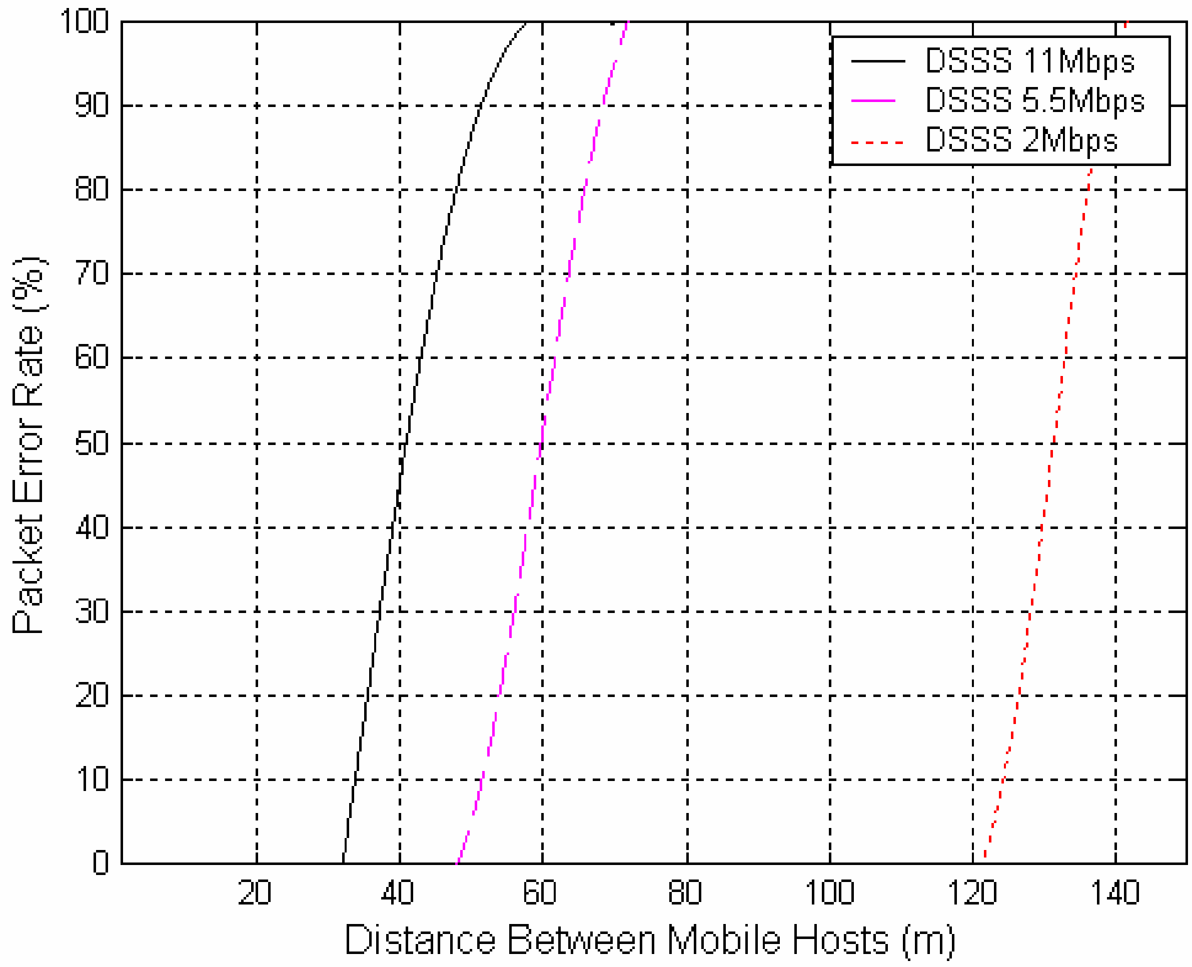
MAC Functionality (continued)

- **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
  - IEEE 802.11i draft enhances security

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
    - » Jan. 2002 (802.11g D2.1 - optional)

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 D2.1 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 ½,2/3,¾.
    - » 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.)

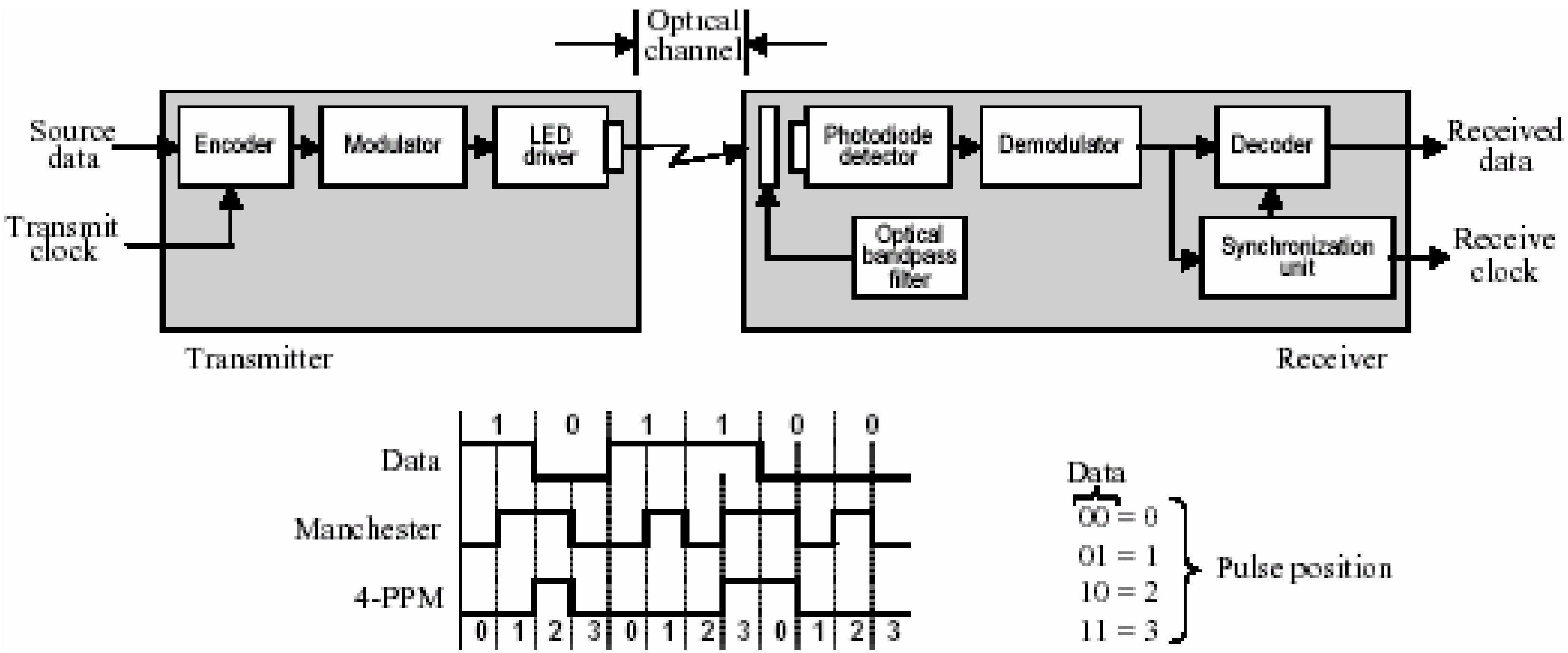
Unlicensed Operation RF Bands

- **902MHz** **ps. 27MHz**
  - 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 HomeRF, 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

2. Baseband Infrared (IR) Physical Layer Specification

PPM Modulation

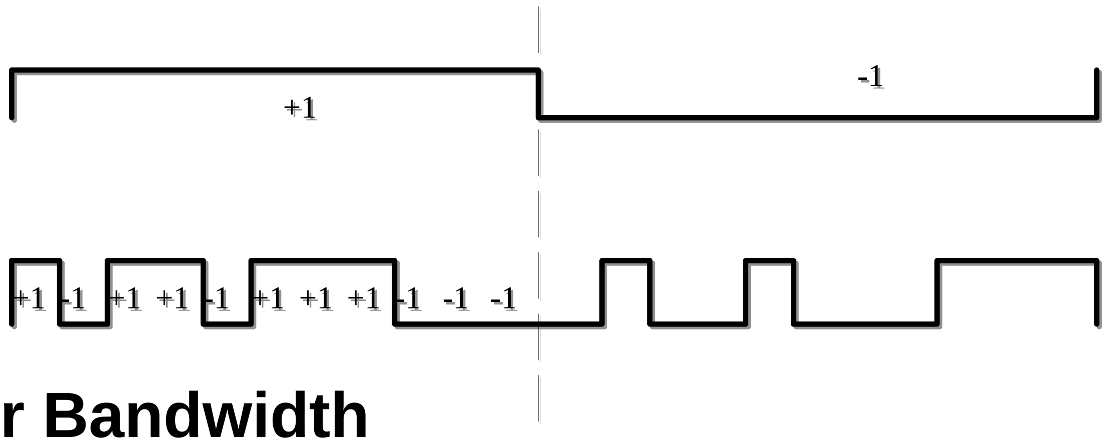
- **OOKPPM :**
  - **Reduce the optical power**



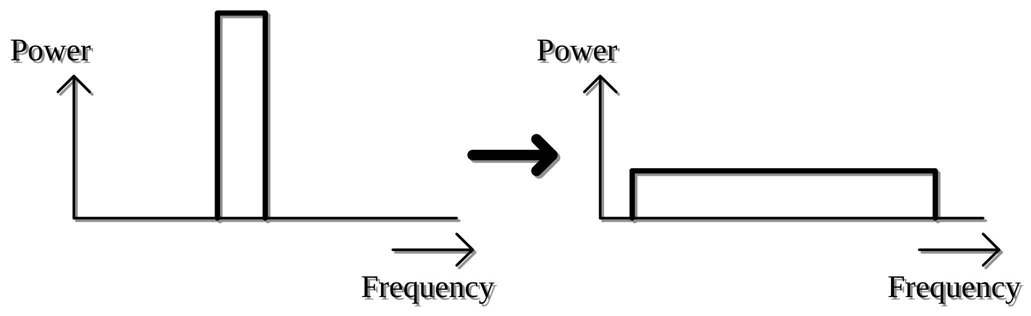
3. Direct Sequence Spread Spectrum (DSSS) Physical Layer Specification

What is DSSS?

- Signal symbol is spread with a sequence

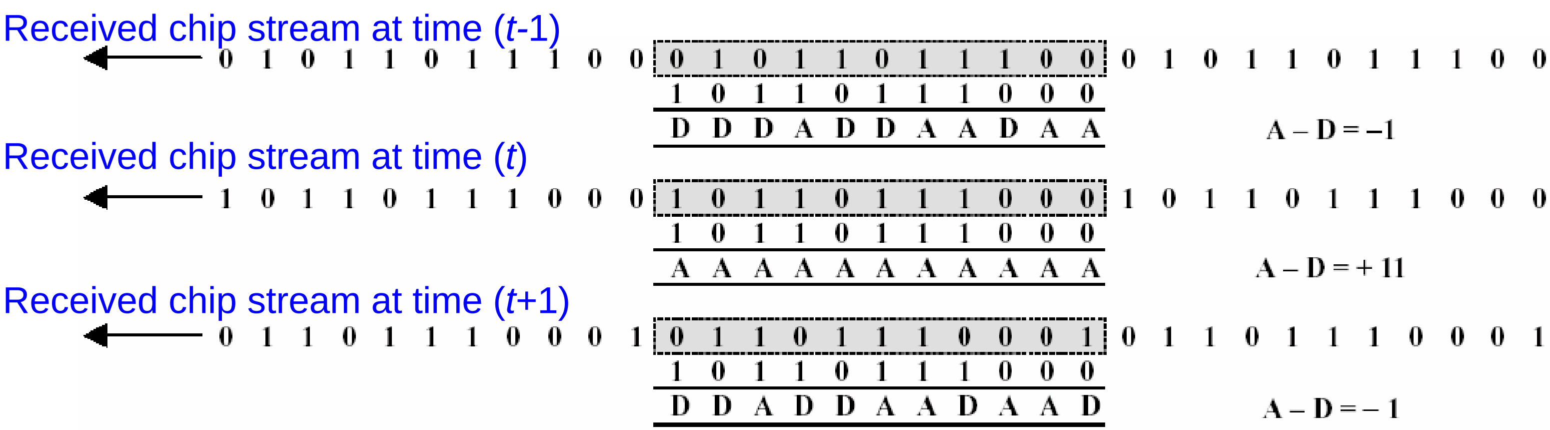


- Wider Bandwidth
- Less power density

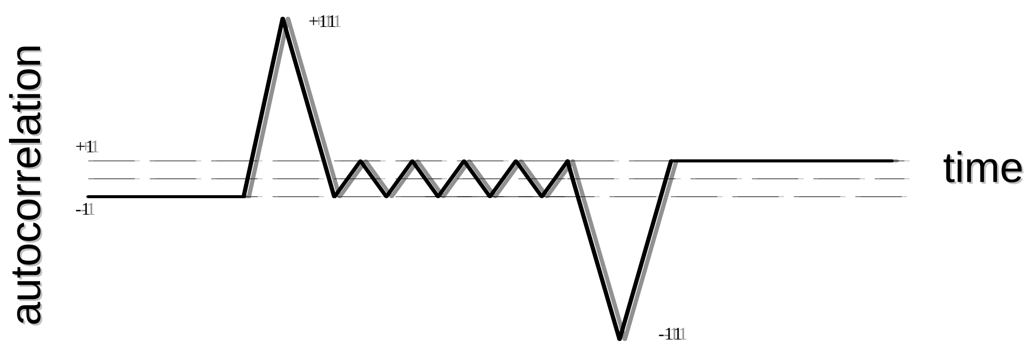


11 chip BARKER sequence

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

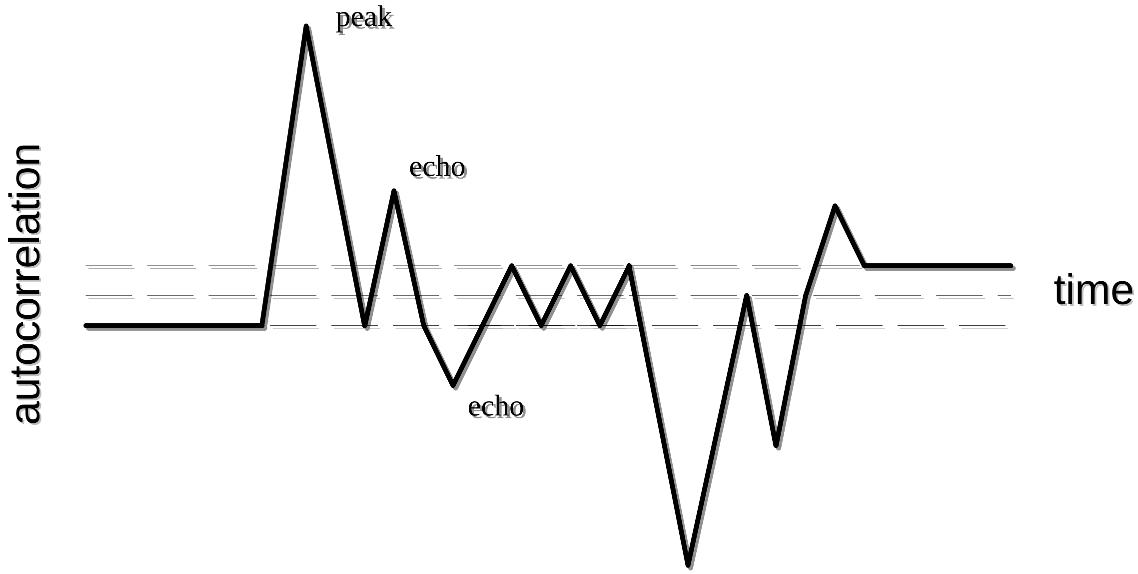


11-chip Barker sequence

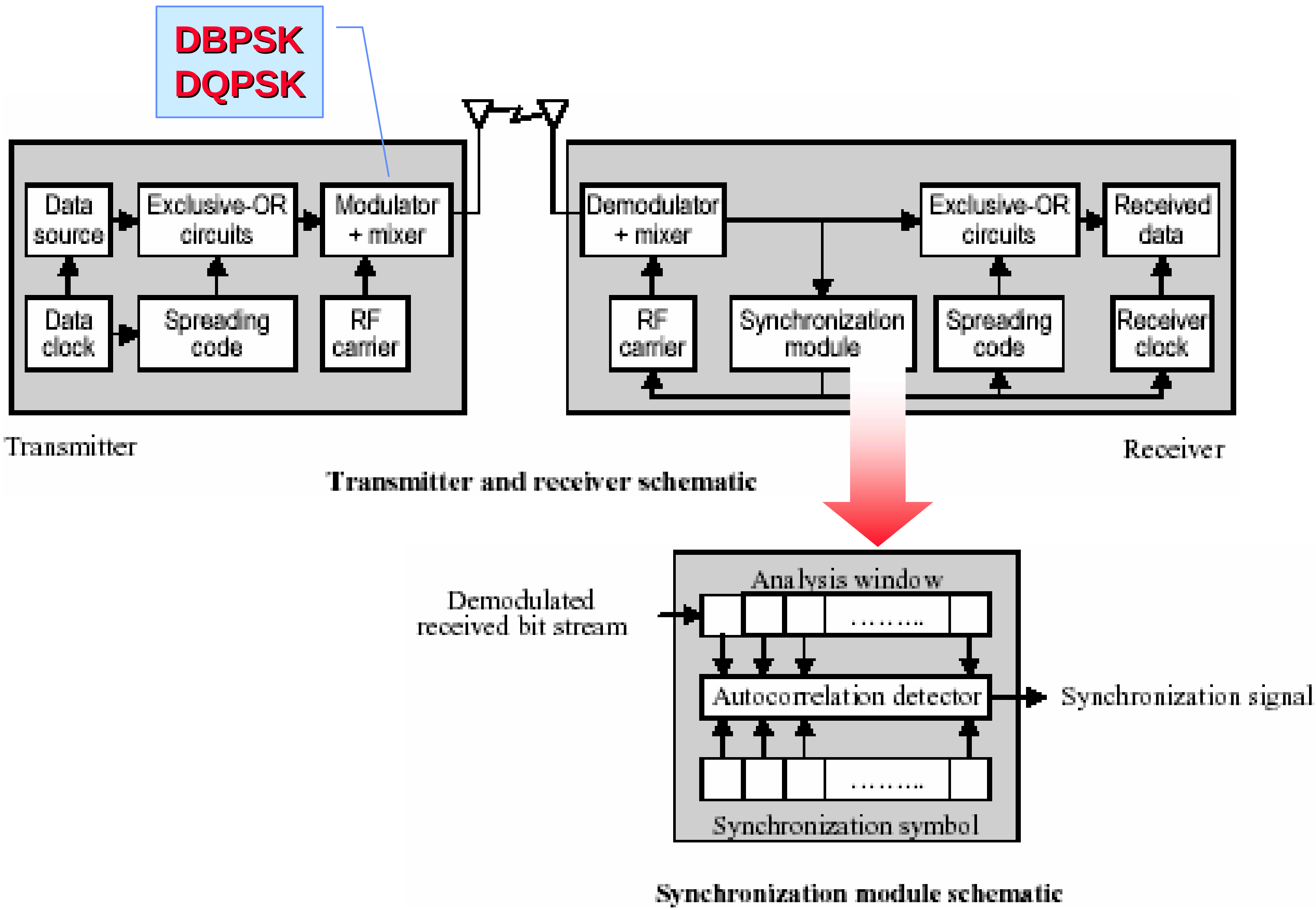


DSSS benefits

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



DSSS hardware block diagram



IEEE 802.11 DSSS PHY characteristics

- **2.4 GHz ISM band (FCC 15.247)**
- **1 and 2 Mb/s datarate**
  - DBPSK and DQPSK modulation
  - Chipping rate 11 MHz with 11 chip Barker sequence
- **5.5 and 11Mbps (802.11b)**
  - CCK (QPSK, DQPSK modulations – mandatory)
  - PBCC (BPSK, QPSK modulations – optional)
- **22 and 33Mbps (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 : ≥ 30MHz (25MHz in 802.11b)**
- FCC pushes the unused unlicensed TV broadcasting band 3.65GHz-3.70GHz as WLAN band.

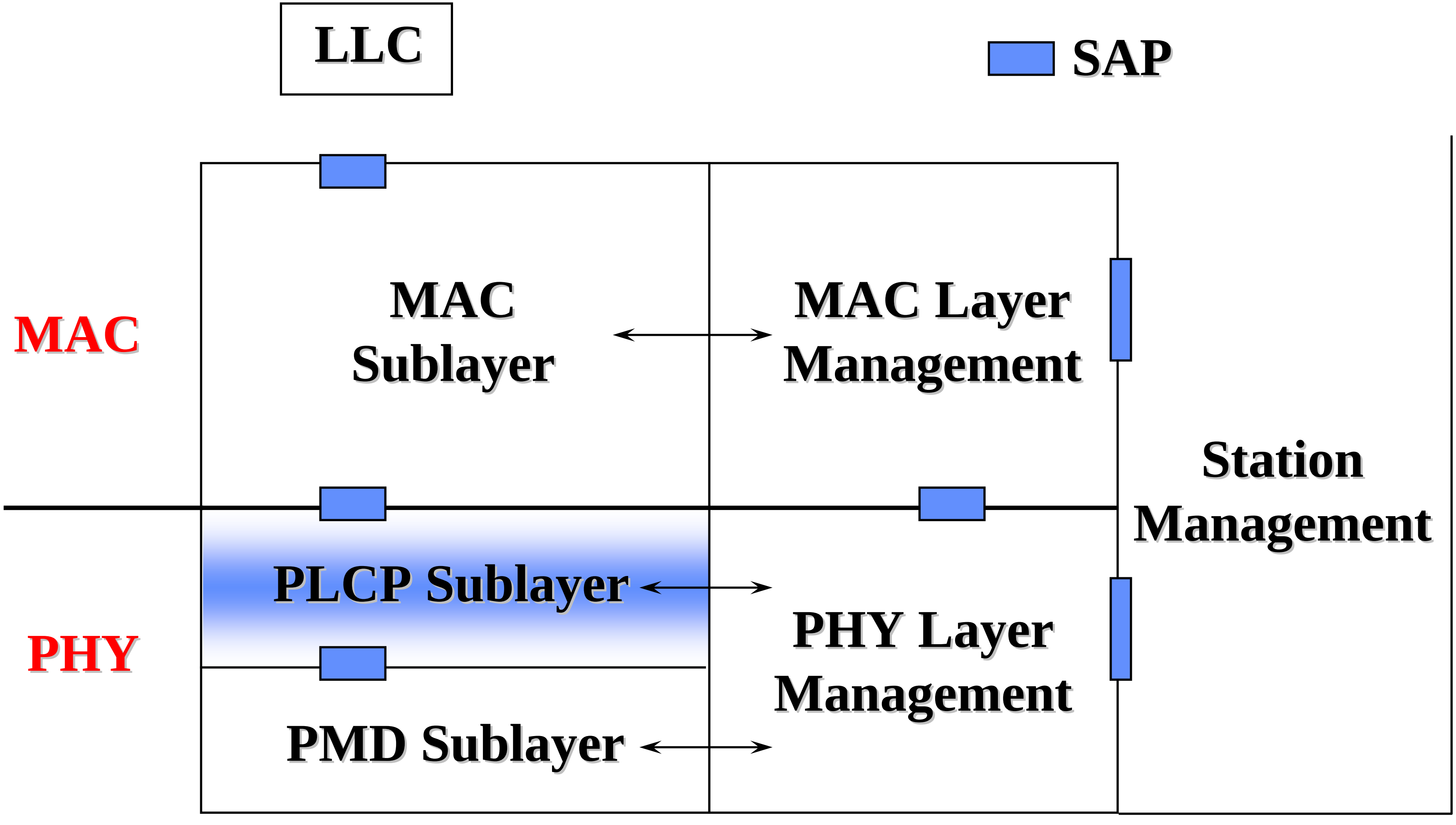
IEEE 802.11 PHY Terminology in Spec.(s)

- **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)**

PLCP Frame Formats in IEEE 802.11b

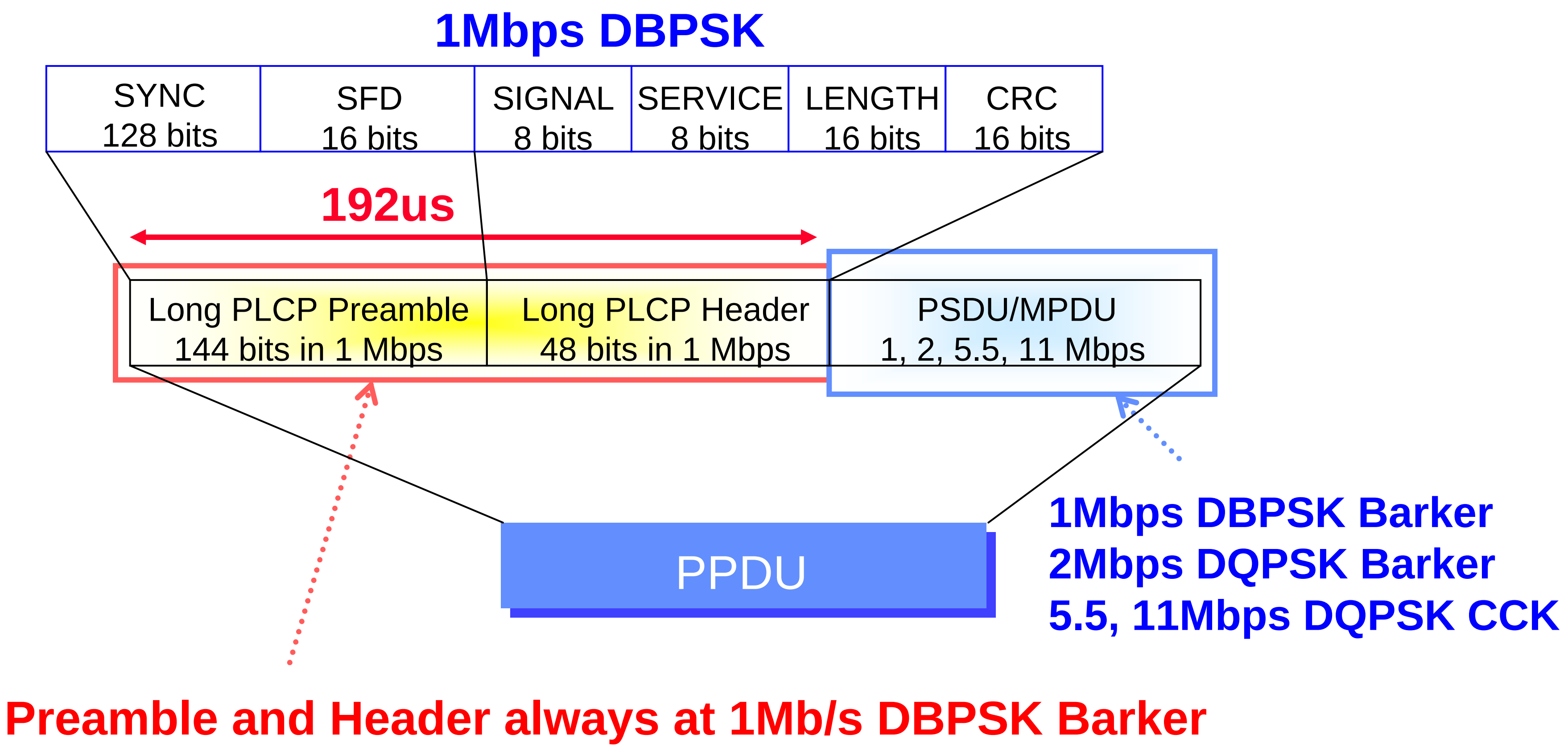
- **Two different preamble and header formats**
  - **Long PLCP PPDU format (Mandatory in 802.11b)**
    - » **144-bit preamble : 1Mbps DBPSK**
    - » **48-bit header : 1Mbps DBPSK**
    - » **Spend 192us**
    - » **PSDU : 1, 2, 5.5, 11Mbps**
    - » **Compatible with 1 and 2 Mbps**
  - **Short PLCP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

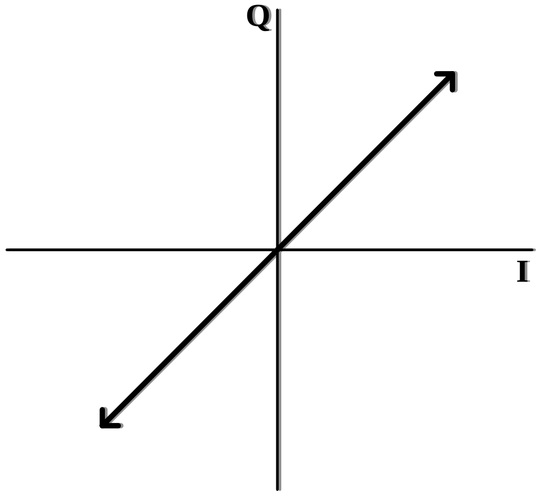


Long PLCP Frame Format

- **Mandatory in 802.11b**



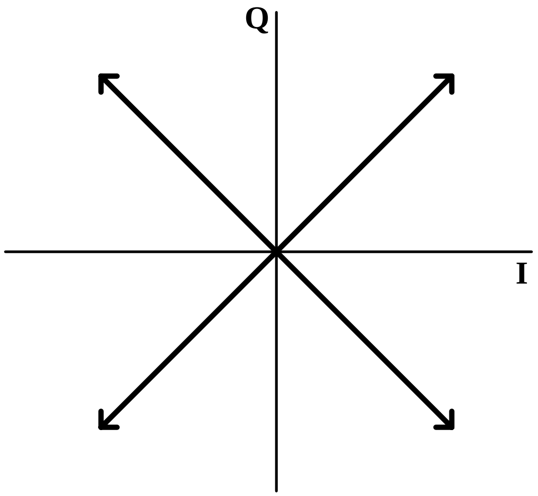
DBPSK Modulation



Bit Input	Phase Change (+jω)
0	0
1	π

Table 1, 1 Mb/s DBPSK Encoding Table.

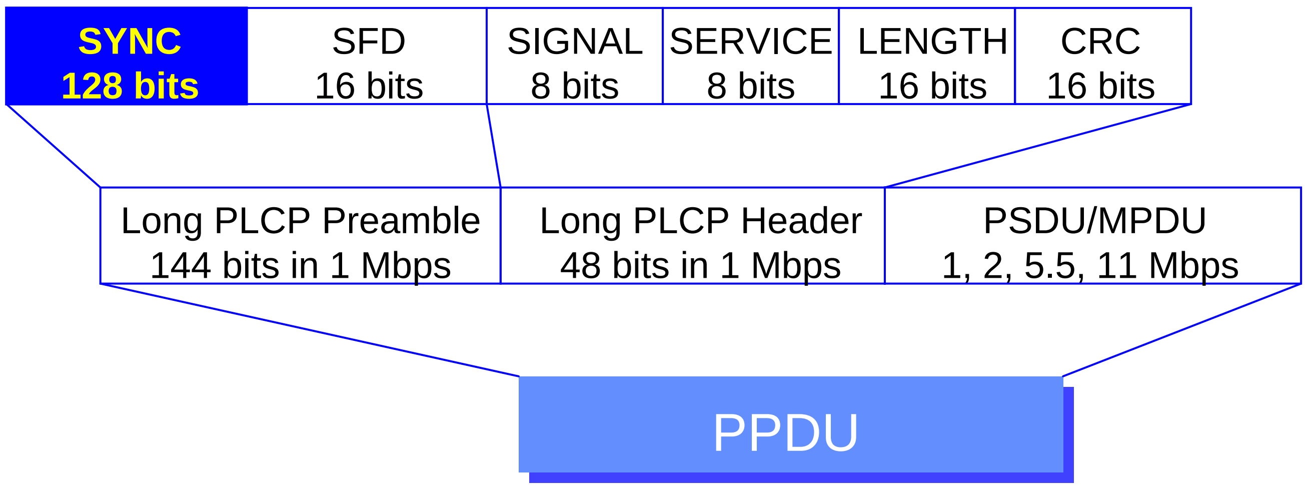
DQPSK Modulation



Dibit pattern (d0,d1) d0 is first in time	Phase Change (+jω)
00	0
01	π/2
11	π
10	3π/2 (-π/2)

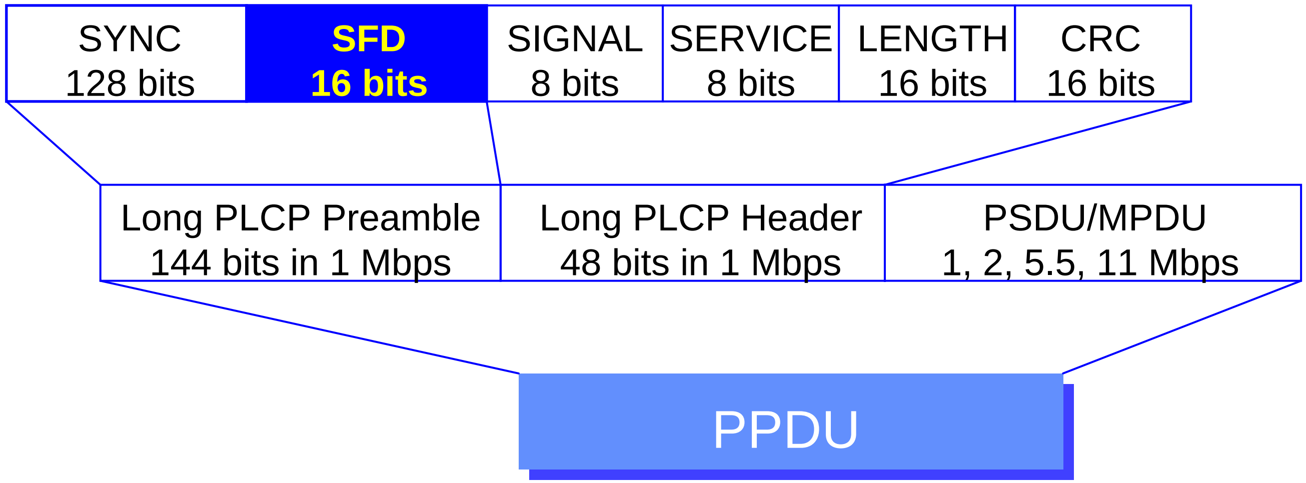
Table 1, 2 Mb/s DQPSK Encoding Table

PLCP synchronization



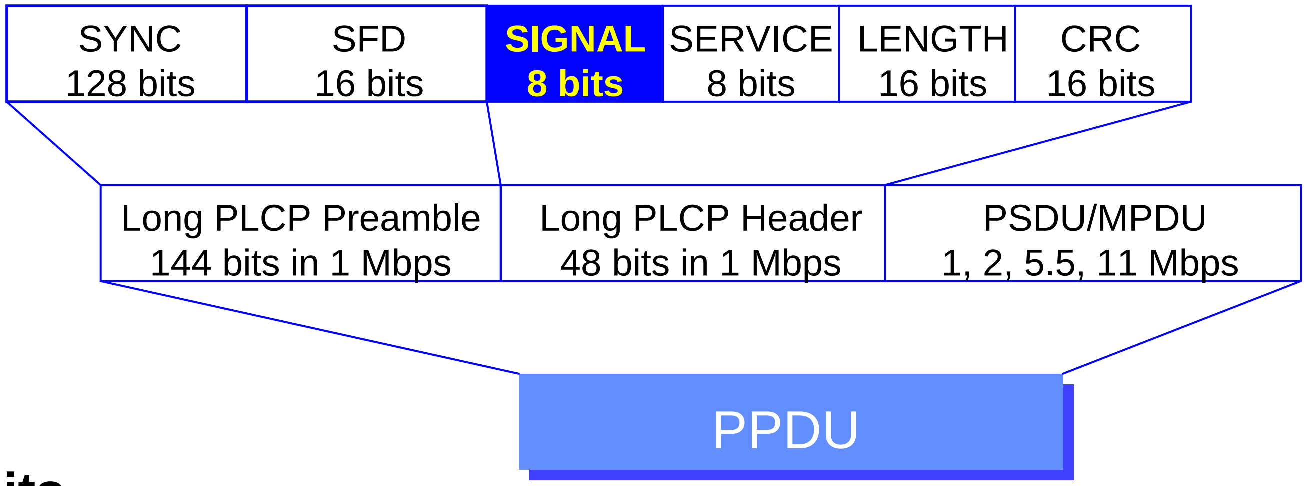
- **128 one bits ('1')**
- **scrambled by scrambler**
- **Used for receiver to clock on to the signal and to correlate to the PN code**

Start Frame Delimiter



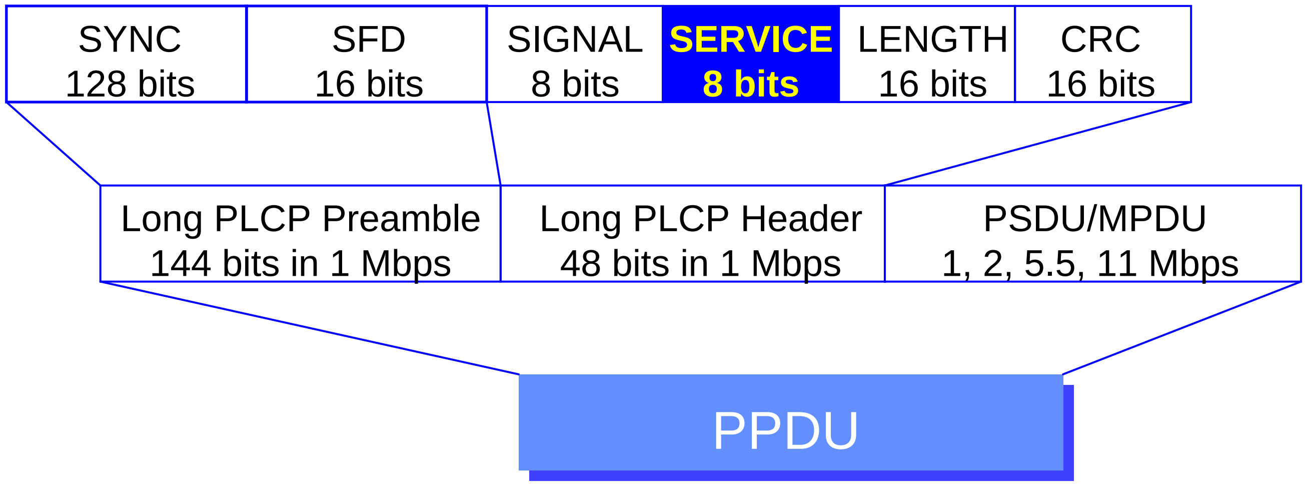
- **16 bit field (hF3A0)**
- **used for**
  - **bit synchronization**

Signal Field



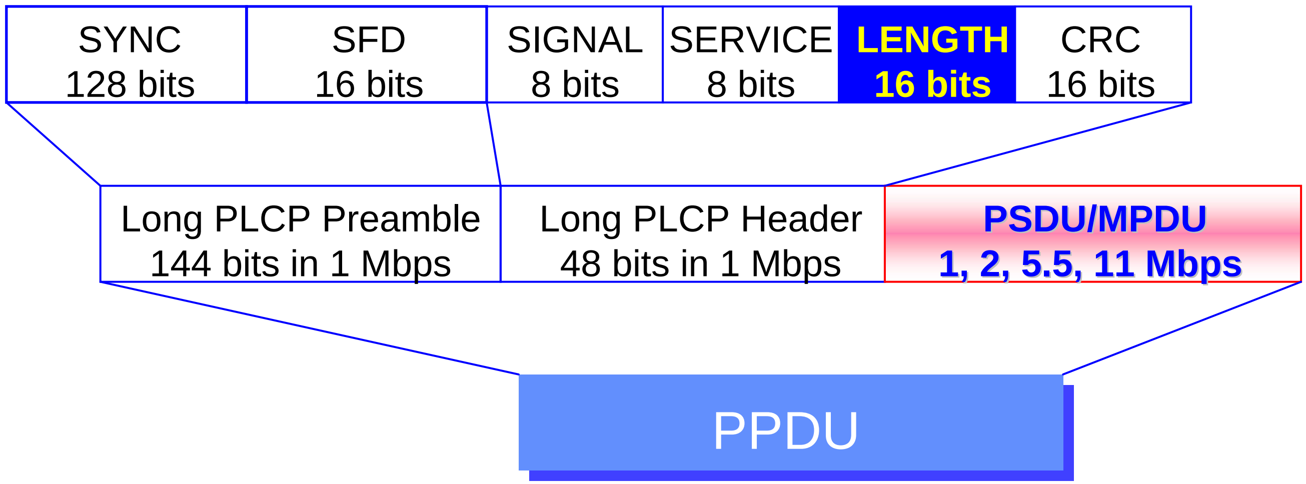
- **8 bits**
- **Rate indication**
  - **h0A 1Mb/s DBPSK**
  - **h14 2Mb/s DQPSK**
  - **h37 5.5Mb/s CCK or PBCC**
  - **h6E 11Mbps CCK or PBCC**
- **Other values reserved for future use (100 kb/s quantities)**

Service Field



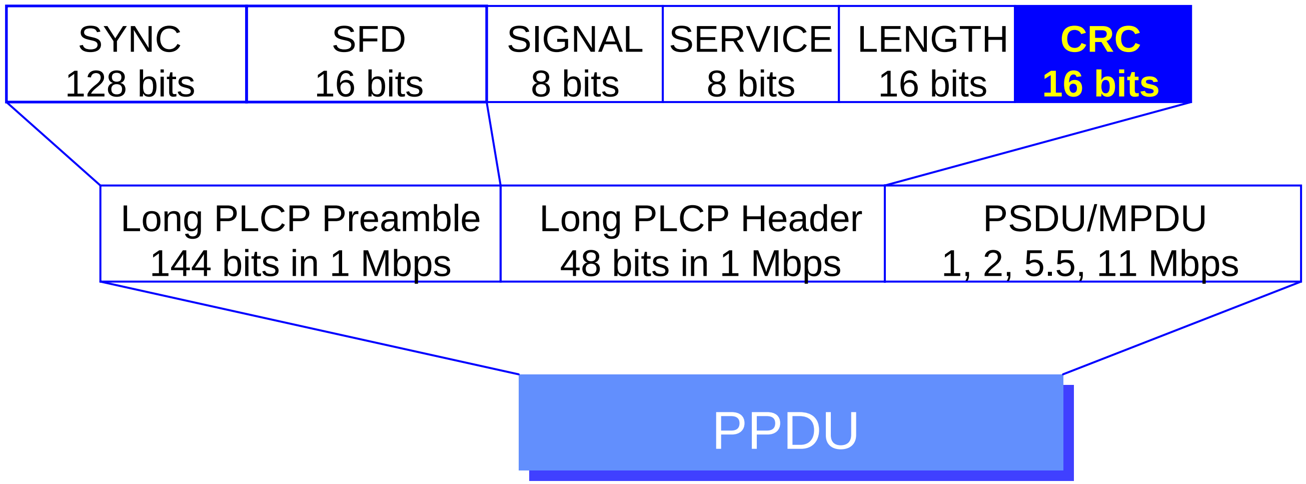
- **Reserved for future use**
  - **Bit 2 : locked clock bit**
    - » **Indicate transmit freq. (mixer) & symbol clocks (baseband) derived from same oscillator**
    - » **optional in 802.11b and mandatory in 802.11g**
  - **Bit 3 : modulation selection**
    - » **0 : CCK / 1 : PBCC**
  - **Bit 7 :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

Length Field



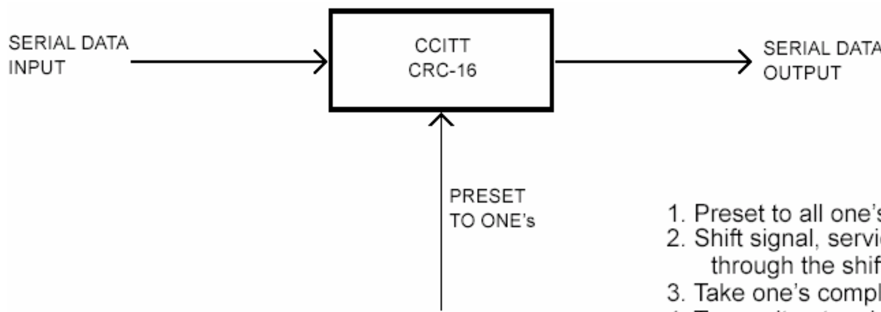
- **Indicates number of micosceonds to be transmitted in PSDU/MPDU**
  - **Decided by Length and datarate (in TXvector)**
- **Used for**
  - **End of frame detection**
  - **Perform Virtual Carrier Sense (for those with lower datarate)**
  - **MPDU CRC sync**

CRC field

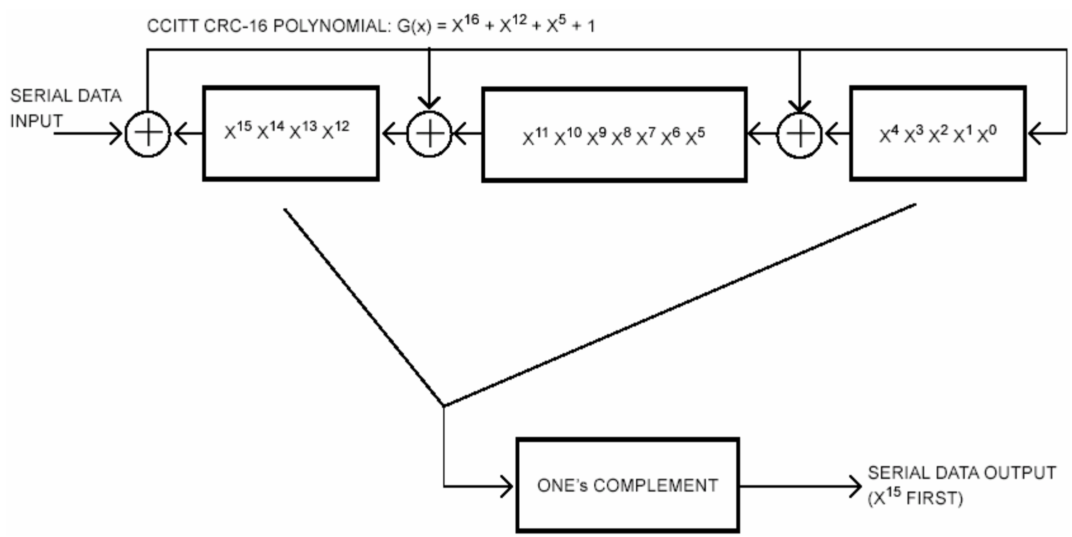


- **CCITT CRC-16**
- **Protects Signal, Service and Length Field**

CRC Implementation



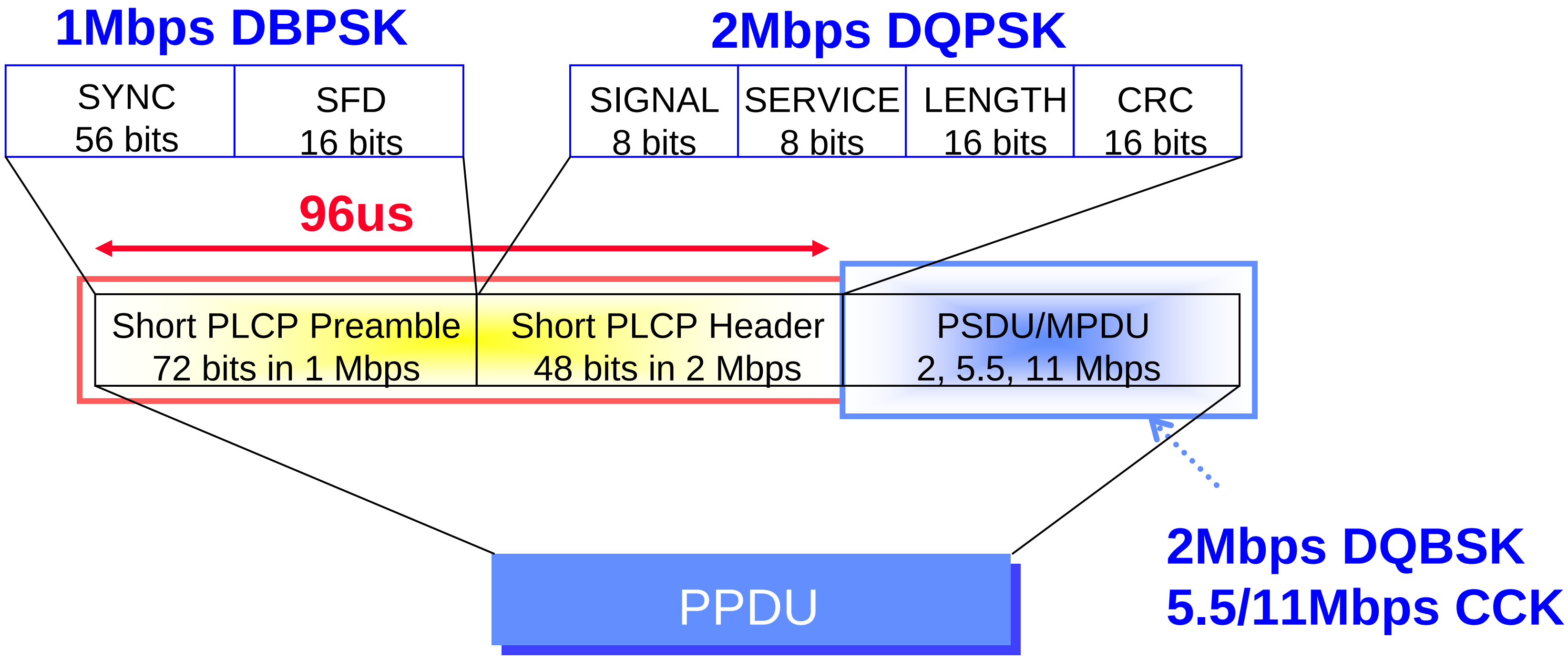
1. Preset to all one's
2. Shift signal, service length fields through the shift register
3. Take one's complement of the remainder
4. Transmit out serial X^{15} first



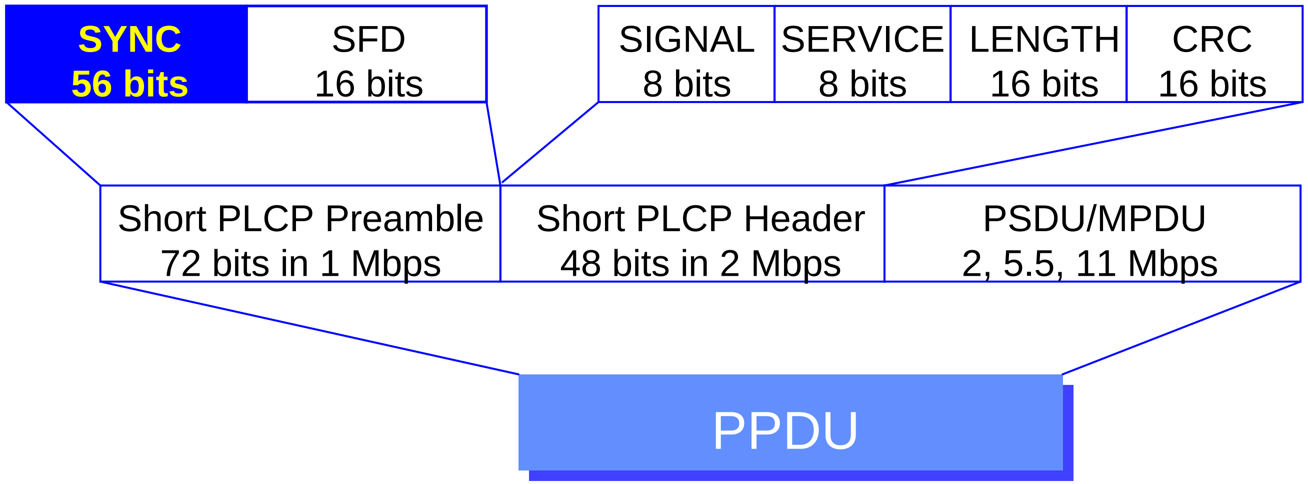
Data	CRC Registers msb lsb
	1111111111111111
0	1110111111011111
1	1101111110111110
0	1010111101011101
1	0101111010111010
0	1011110101110100
0	0110101011001001
0	1101010110010010
0	1011101100000101
0	0110011000101011
0	1100110001010110
0	1000100010001101
0	0000000100111011
0	0000001001110110
0	0000010011101100
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

Short PLCP Frame Format in 802.11b

- **Optional in 802.11b**

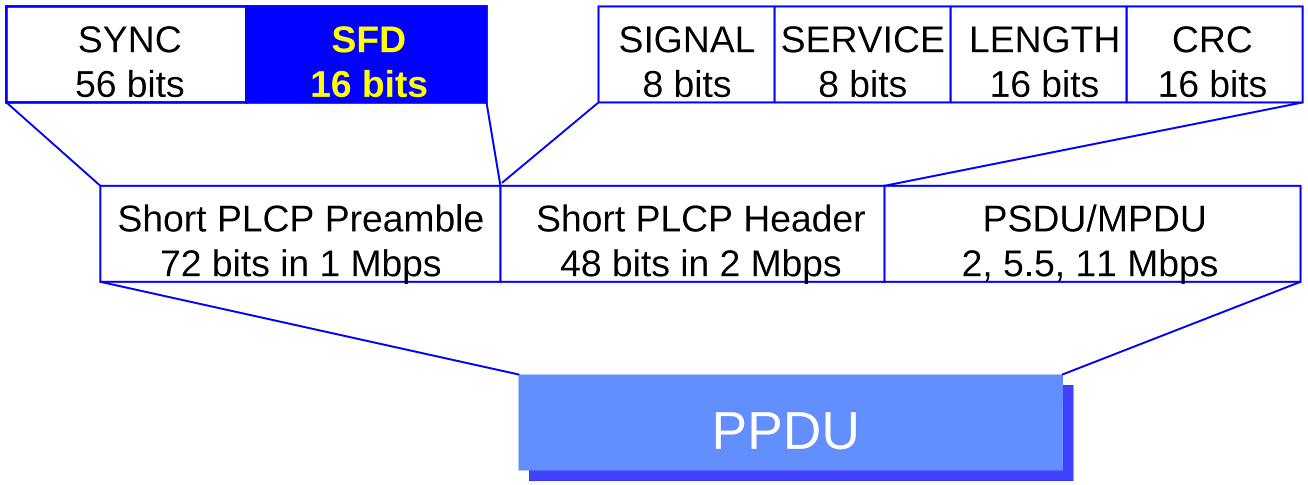


PLCP synchronization



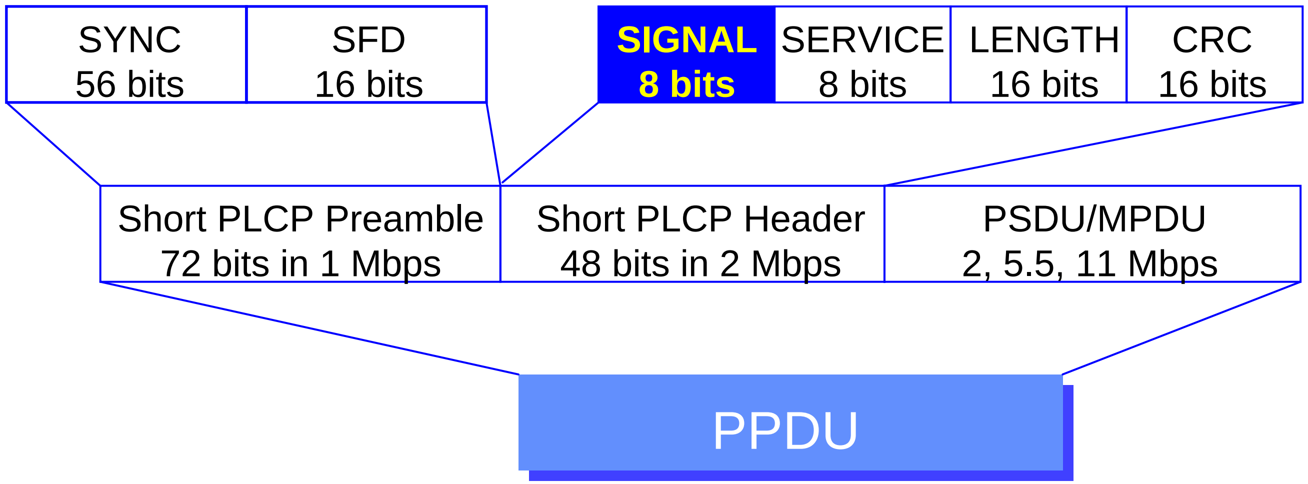
- 56 zero bits (‘0’)
- scrambled by scrambler with seed ‘0011011’
- Used for receiver to clock on to the signal and to correlate to the PN code

Start Frame Delimiter



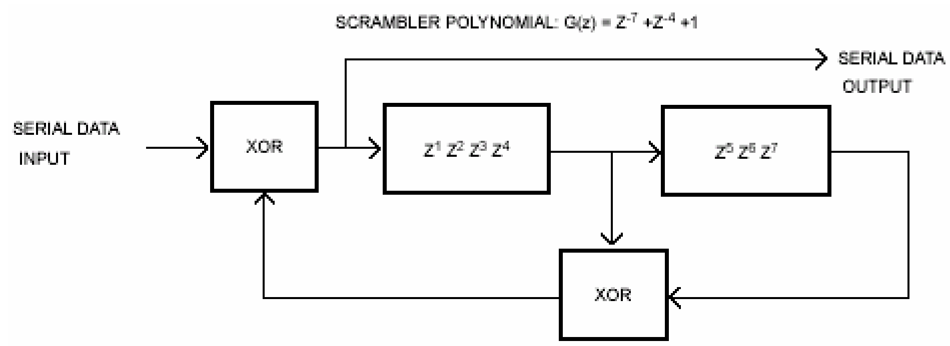
- **16 bit field (h05CF)**
- **used for**
  - **bit synchronization**

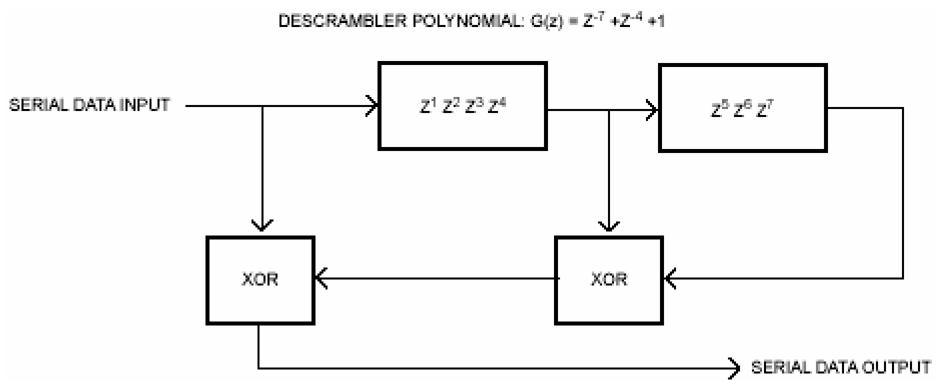
Signal Field



- **Rate indication**
  - **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)**

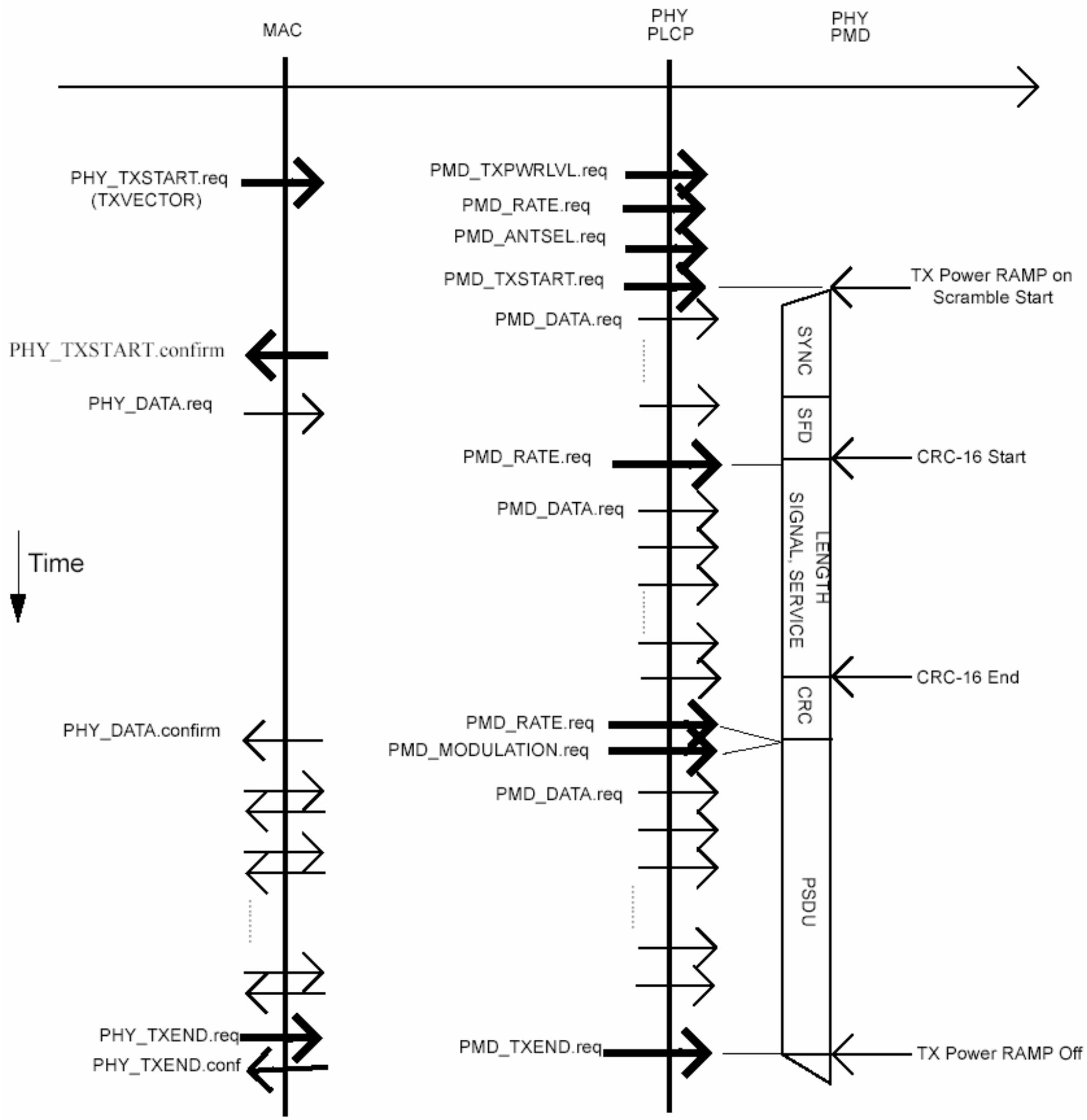
Data Scrambler/Descrambler



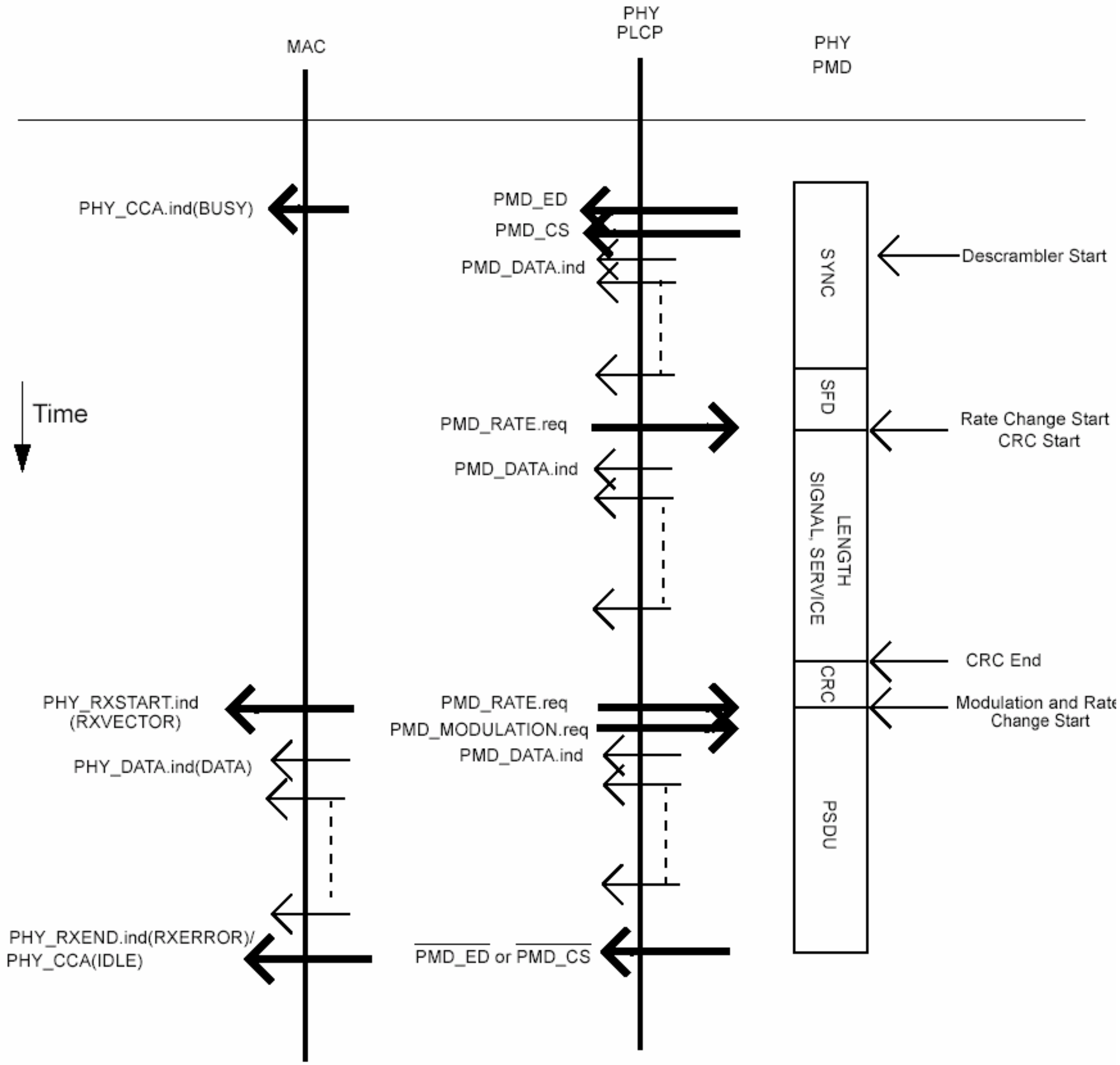


- **ALL bits transmitted/received by the DSSS PHY are scrambled/descrambled**

PLCP Transmit Procedure

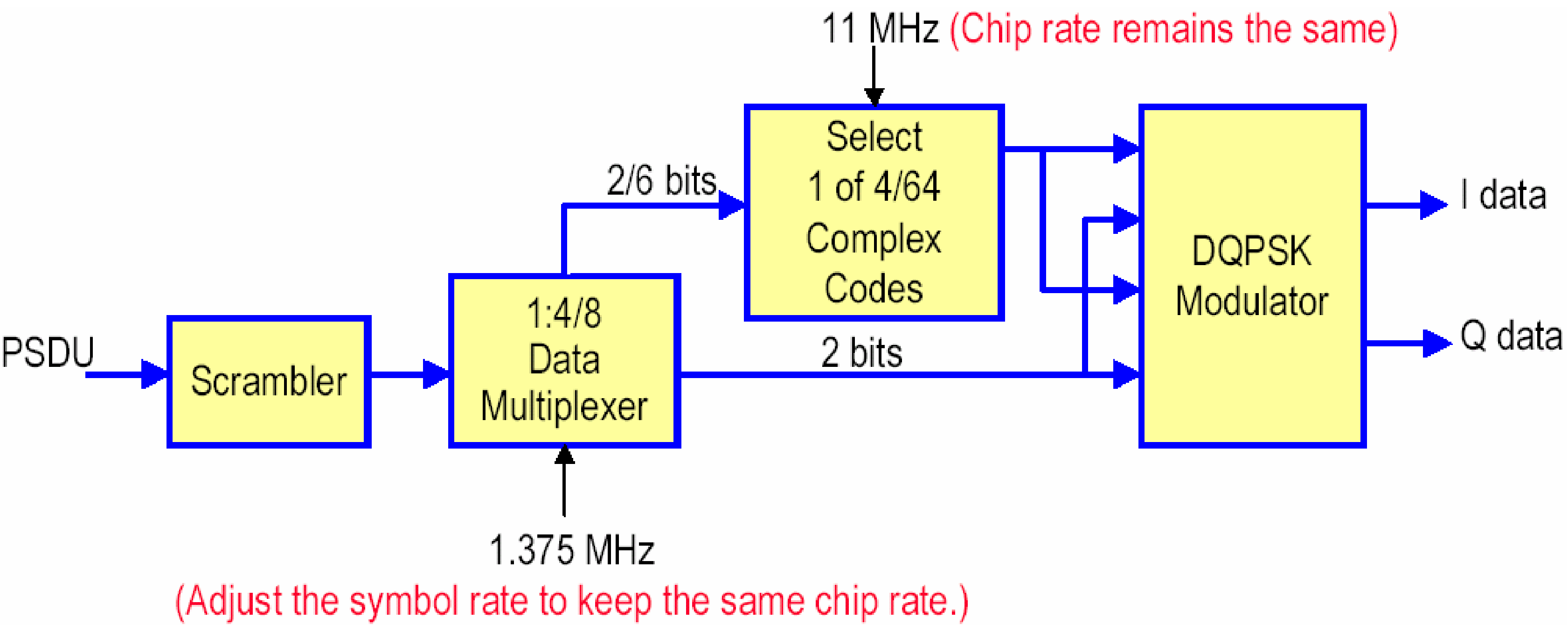


PLCP Receive Procedure



Complementary Code Keying (CCK)

- **HR/DSSS adopts 8-chip CCK as the modulation scheme with 11MHz chipping rate**
- **It provides a path for interoperability with existing 1,2 Mbps Spec.**



8-chip*1.375MHz = 11MHz chipping rate

Complementary Code Keying (CCK)

- **Spreading code length = 8, c={c0-c7} and**

$$c = \{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)},$$
$$-e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1}\}$$

where φ_1 is added to all code chips,

φ_2 is added to all odd code chips,

φ_3 is added to all odd pairs of code chips, and

φ_4 is added to all odd quads of code chips.

Cover code : c4 and c7 chips are rotated 180° (with **-**) by a cover sequence to optimize the sequence correlation properties and minimize dc offsets in the codes.

Complementary Code Keying (CCK) 5.5Mbps

- **At 5.5Mbps CCK, 4 data bits (d0,d1,d2,d3) are transmitted per symbol**
  - **(d0,d1) is DQPSK modulated to yield $\varphi 1$, which the information is bear on the "phase change" between two adjacent symbols**
  - **(11/8)*(4 data bits per symbol)*1Mbps = 5.5Mbps**

Table 108—DQPSK encoding table

Dibit pattern (d0, d1) (d0 is first in time)	Even symbols phase change (+jω)	Odd symbols phase change (+jω)
00	0	π
01	$\pi/2$	$3\pi/2$ ($-\pi/2$)
11	π	0
10	$3\pi/2$ ($-\pi/2$)	$\pi/2$

Complementary Code Keying (CCK) 5.5Mbps

- (d2,d3) encodes the basic symbol, where

$$\begin{cases} \varphi_2 = d_2 \times \pi + \pi / 2; \\ \phi_3 = 0; \\ \phi_4 = d_3 \times \pi; \end{cases}$$

Table 109—5.5 Mbit/s CCK encoding table

d2, d3	c1	c2	c3	c4	c5	c6	c7	c8
00	1j	1	1j	–1	1j	1	–1j	1
01	–1j	–1	–1j	1	1j	1	–1j	1
10	–1j	1	–1j	–1	–1j	1	1j	1
11	1j	–1	1j	1	–1j	1	1j	1

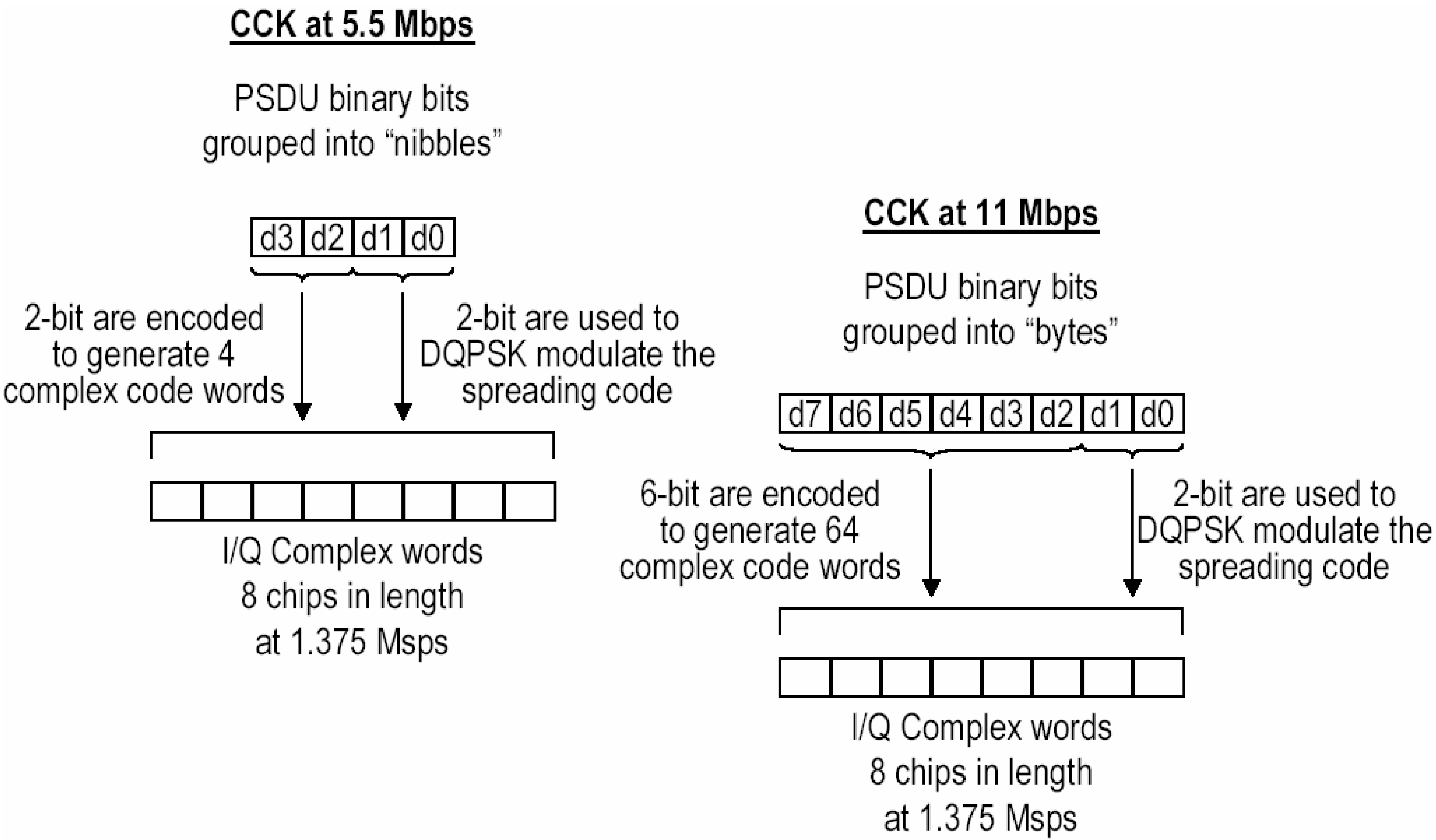
Complementary Code Keying (CCK) 11Mbps

- **At 11Mbps CCK, 8 data bits (d0-d7) are transmitted per symbol**
  - **(d0,d1) is DQPSK modulated to yield φ1, which the information is bear on the "phase change" between two adjacent symbols**
  - **(d2,d3),(d4,d5),(d6,d7) encode φ2, φ3, φ4, respectively, based on QPSK**
  - **(11/8)*(8 data bits per symbol)*1Mbps = 11Mbps**

Table 110—QPSK encoding table

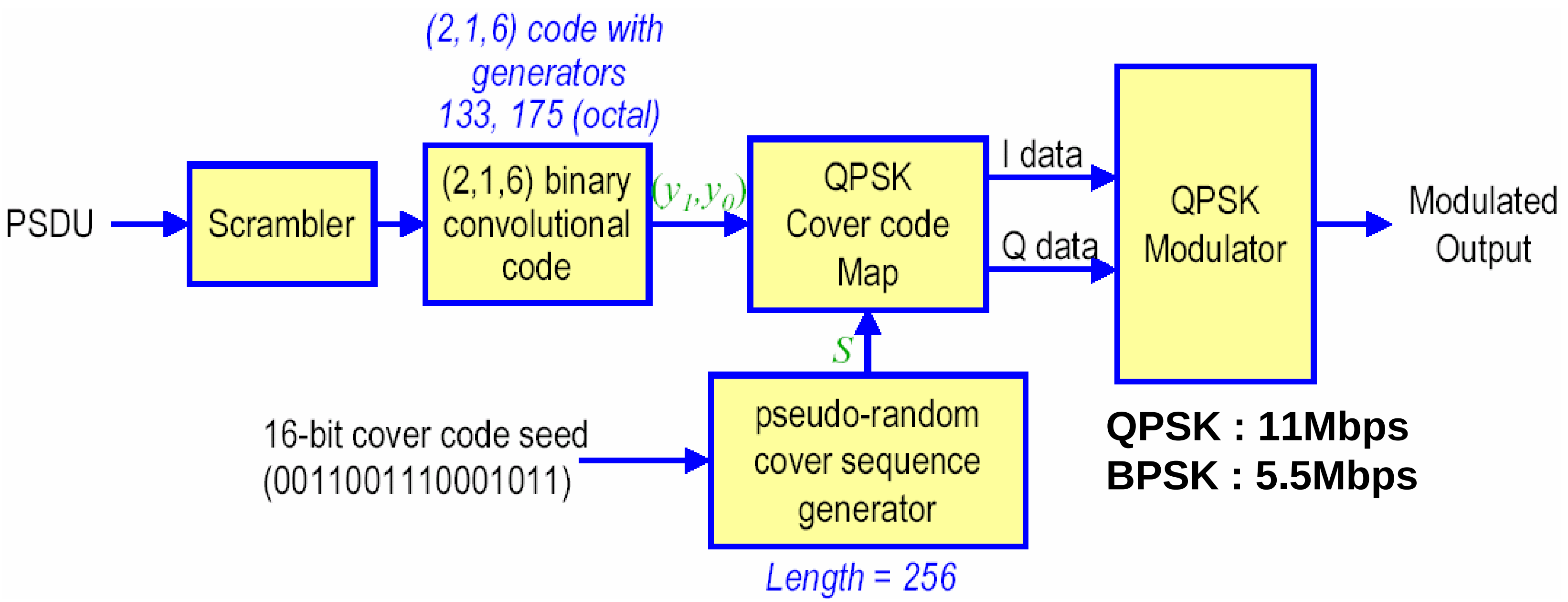
Dibit pattern [di, d(i+1)] (di is first in time)	Phase
00	0
01	π/2
10	π
11	3π/2 (−π/2)

Complementary Code Keying (CCK)



Packet Binary Convolutional Code (PBCC)

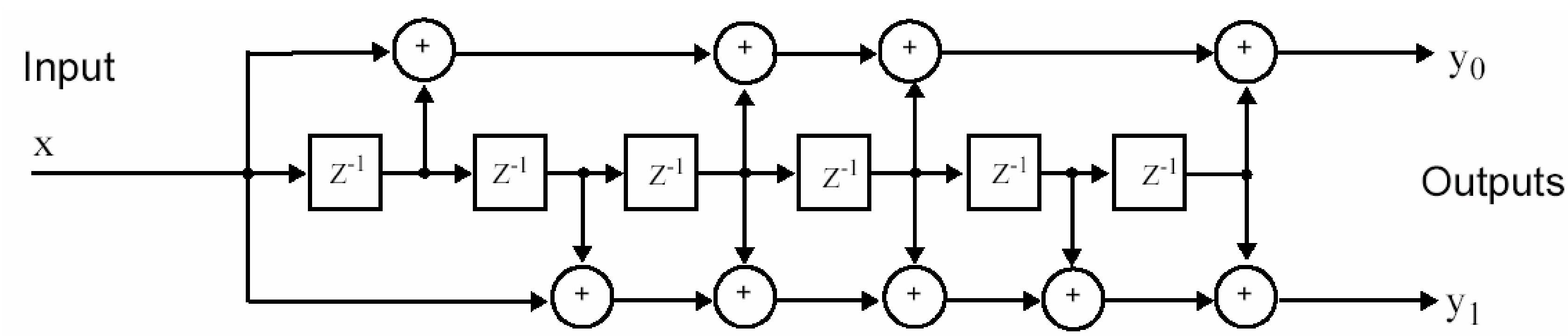
- **64-state BCC**



QPSK : 11Mbps
BPSK : 5.5Mbps

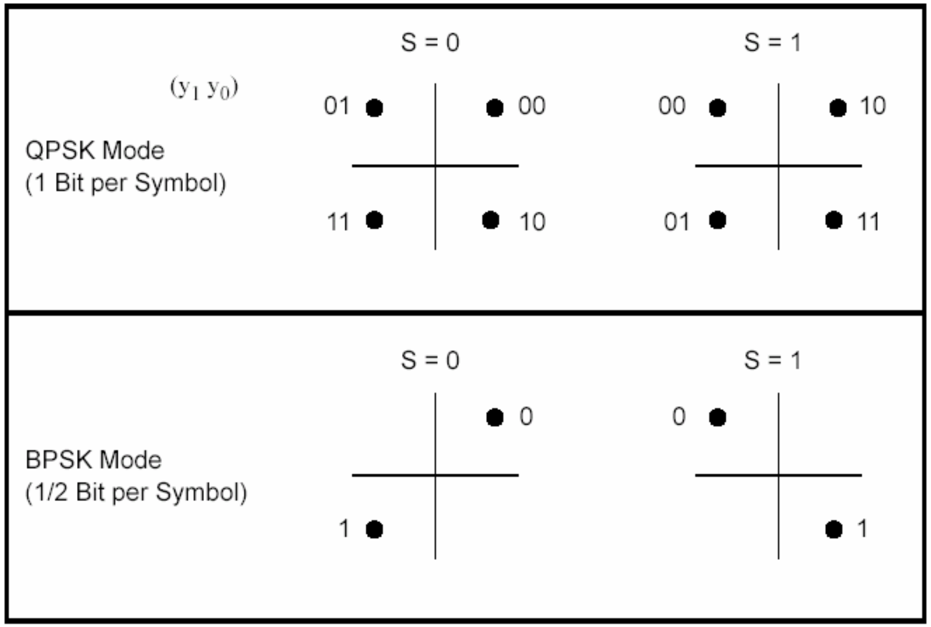
Packet Binary Convolutional Code (PBCC)

- **PBCC convolutional encoder**
  - **Provide encoder the “known state”**
    - » **6 memory elements are needed and**
    - » **one octet containing all zeros is appended to the end of the PPDU prior to transmission**
      - **One more octet than CCK**
  - **For every data bit input, two output bits are generated**



Packet Binary Convolutional Code (PBCC)

- **For 11Mbps, two output bits (y0,y1) produce one symbol via QPSK**
  - **one data bit per symbol**
- **For 5.5Mbps, each output bit (y0 or y1) produces two symbols via BPSK**
  - **One-half a bit per symbol**

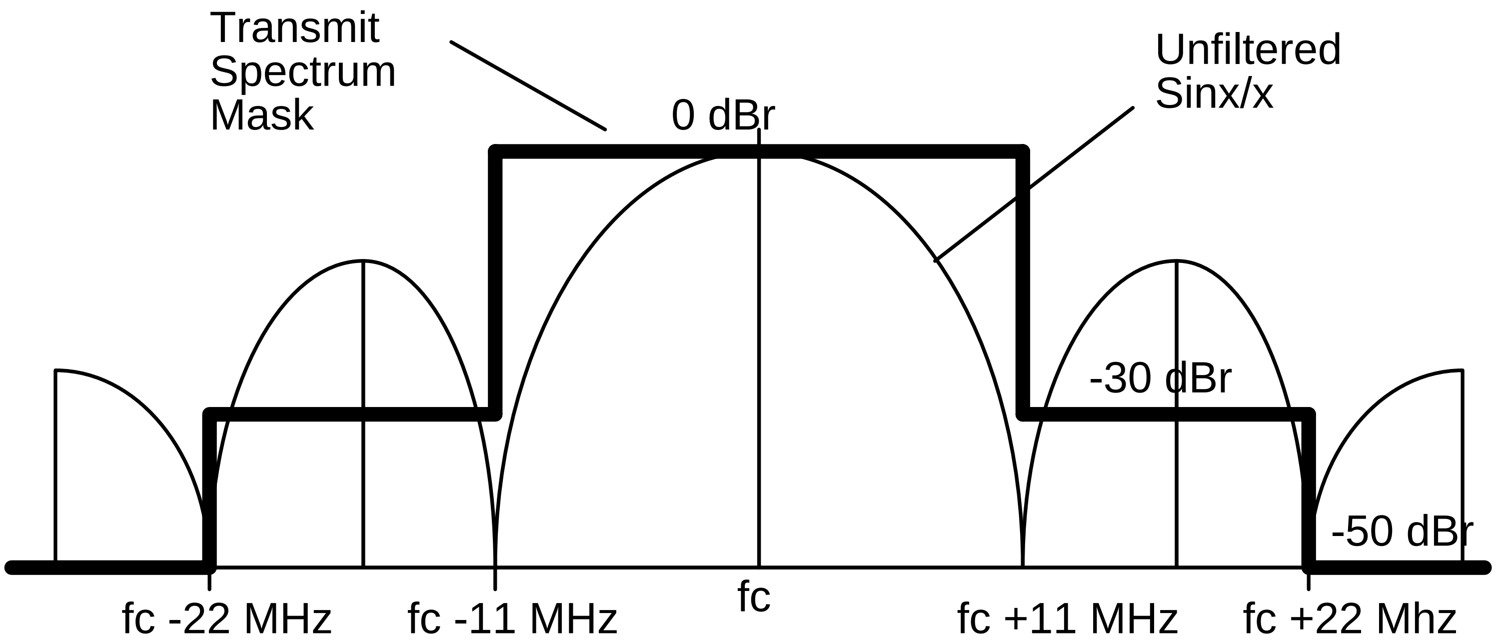


Packet Binary Convolutional Code (PBCC)

- **Pseudo-random cover sequence**
  - use 16-bit seed sequence (0011001110001011)
  - to generate 256-bit pseudo-random cover sequence

c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15
c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2
c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3 c4 c5
c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8
c12 c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11
c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14
c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1
c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3 c4
c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7
c11 c12 c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10
c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13
c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0
c4 c5 c6 c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3
c7 c8 c9 c10 c11 c12 c13 c14 c15 c0 c1 c2 c3 c4 c5 c6
c10 c11 c12c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9
c13 c14 c15 c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 c10 c11 c12

Transmit Spectrum Mask



Clear Channel Assessment

- Five methods:
  - CCA mode 1: Energy above threshold (detect energy) (11b-HR, 11g-ERP)
  - CCA mode 2: Carrier sense only (detect DSSS signal)
  - CCA mode 3: Carrier sense with energy above threshold (2Mbps)
  - CCA mode 4: Carrier sense with timer (11b-HR)
    - 3.65ms is the duration of the longest possible 5.5Mbps PSDU
  - CCA mode 5: Carrier sense (detect DSSS signal) with energy above threshold (5.5Mbps, 11Mbps) (11b-HR, 11g-ERP)
- Energy detection function of TX power in modes 1 & 3
  - Tx power > 100mW: -80 dBm (-76dBm in mode 5)
  - Tx power > 50mW : -76 dBm (-73dBm in mode 5)
  - Tx power <= 50mW: -70 dBm (-70dBm in mode 5)
- Energy detect time : 15 μs
- Correct PLCP header --> CCA busy for full (intended) duration of frame as indicated by PLCP Length field

DSSS Specification Summary

- **Slottime** **20 us**
- **TX to Rx turnaround time** **10** us
- **Rx to Tx turnaround time** **5** us
- **Operating temperature range**
  - » **type 1: 0 - 40 ^{o}C**
  - » **type 2: -30 - 70 ^{o}C**
- **Tx Power Levels**
  - » **1000 mW** **USA (FCC 15.274)**
  - » **100 mW** **Europe (ETS 300-328) (=20dbm)**
  - » **10 mW/MHz** **Japan (MPT ordinance 49-20)**
- **Minimum Transmitted Power 1 mW**
- **Tx power level control required above 100 mW**
  - **four power levels**

DSSS Specification Summary (cont)

• Tx Center Frequency Tolerance	+/- 25 ppm
• Chip Clock Frequency Tolerance	+/- 25 ppm
• Tx Power On Ramp	2 μs
• Tx Power Down Ramp	2 μs
• RF Carrier suppression	15 dB
• Transmit modulation accuracy	test procedure
• Rx sensitivity	-80 dB (-76dbm) @ 0.08FER (1024 Bytes) <@ 0.10FER (1000 Bytes) in 11g
• Rx max input level	-4 dB (-10dbm)
• Rx adjacent channel rejection	>35 dB @ > 30(25) MHz separation between channels

4. Orthogonal Frequency Division Multiplexing (OFDM) Physical Layer Specification

IEEE 802.11a PLCP

- **TxVector / RxVector**
  - **length 1-4095 octets**
  - **Mandatory data rates : 6, 12, 24 Mbps**
  - **8 power levels**

Table 76—TXVECTOR parameters

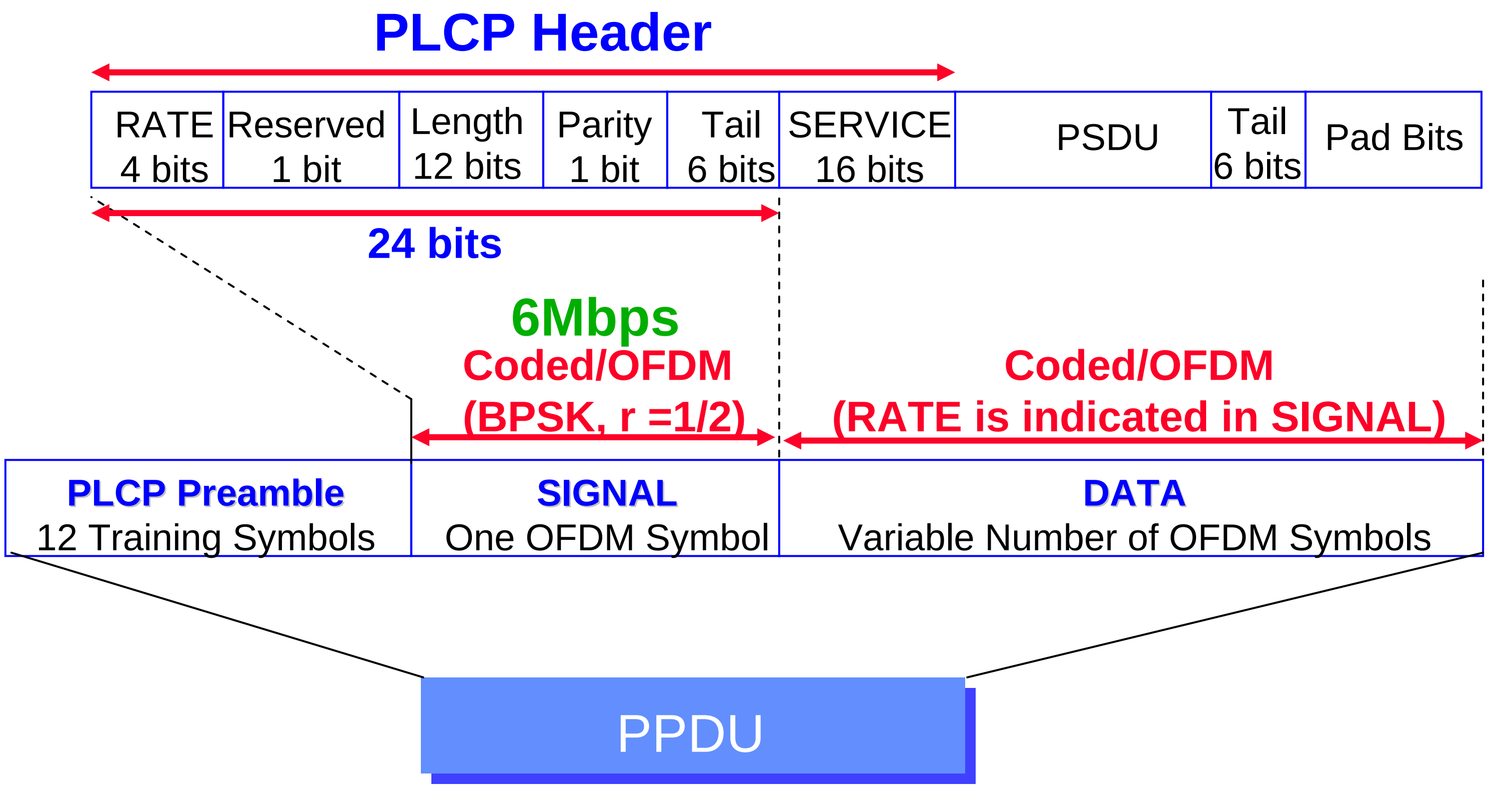
Parameter	Associate primitive	Value
LENGTH	PHY-TXSTART.request (TXVECTOR)	1–4095
DATATRATE	PHY-TXSTART.request (TXVECTOR)	6, 9, 12, 18, 24, 36, 48, and 54 (Support of 6, 12, and 24 data rates is mandatory.)
SERVICE	PHY-TXSTART.request (TXVECTOR)	Scrambler initialization; 7 null bits + 9 reserved null bits
TXPWR_LEVEL	PHY-TXSTART.request (TXVECTOR)	1–8

IEEE 802.11a PLCP

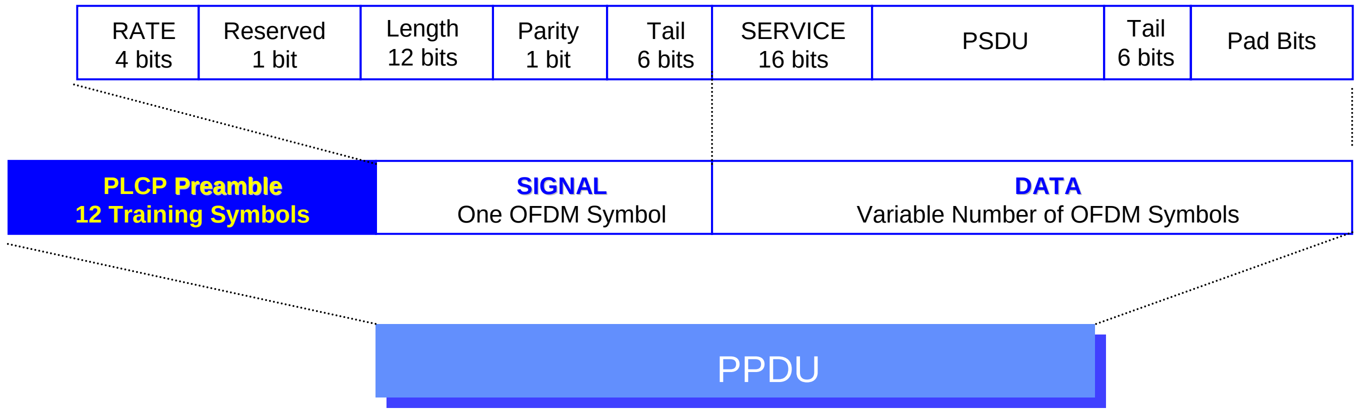
Table 77—RXVECTOR parameters

Parameter	Associate primitive	Value
LENGTH	PHY-RXSTART.indicate	1–4095
RSSI	PHY-RXSTART.indicate (RXVECTOR)	0–RSSI maximum
DATARATE	PHY-RXSTART.request (RXVECTOR)	6, 9, 12, 18, 24, 36, 48, and 54
SERVICE	PHY-RXSTART.request (RXVECTOR)	Null

IEEE 802.11a PLCP frame format

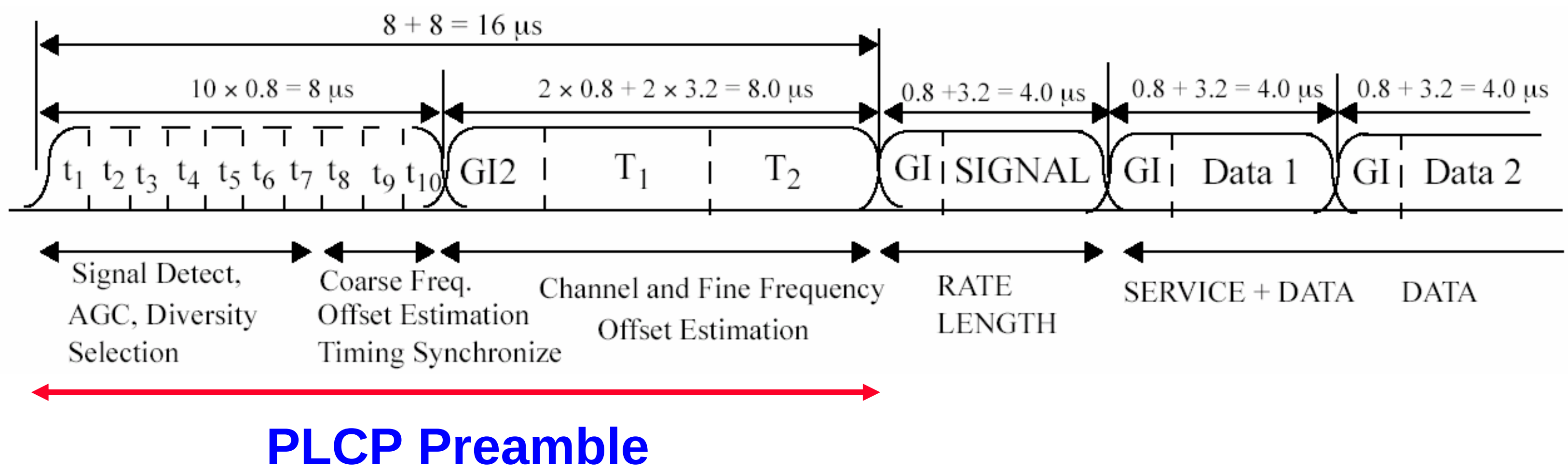


PCLP Preamble

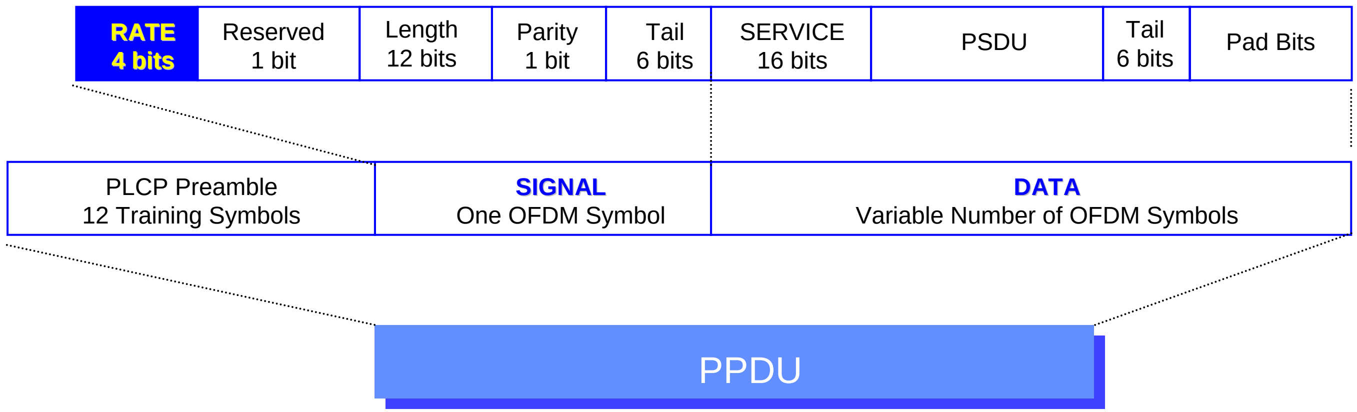


1. **preamble field contains**
   - **10 short training sequence**
     - » used for AGC convergence, diversity selection, timing acquisition, and coarse frequency acquisition in the receiver
   - **2 long training sequence**
     - » used for channel estimation and fine frequency acquisition in the receiver
   - **and a guard interval (GI)**

PCLP Preamble



PCLP Rate/Length



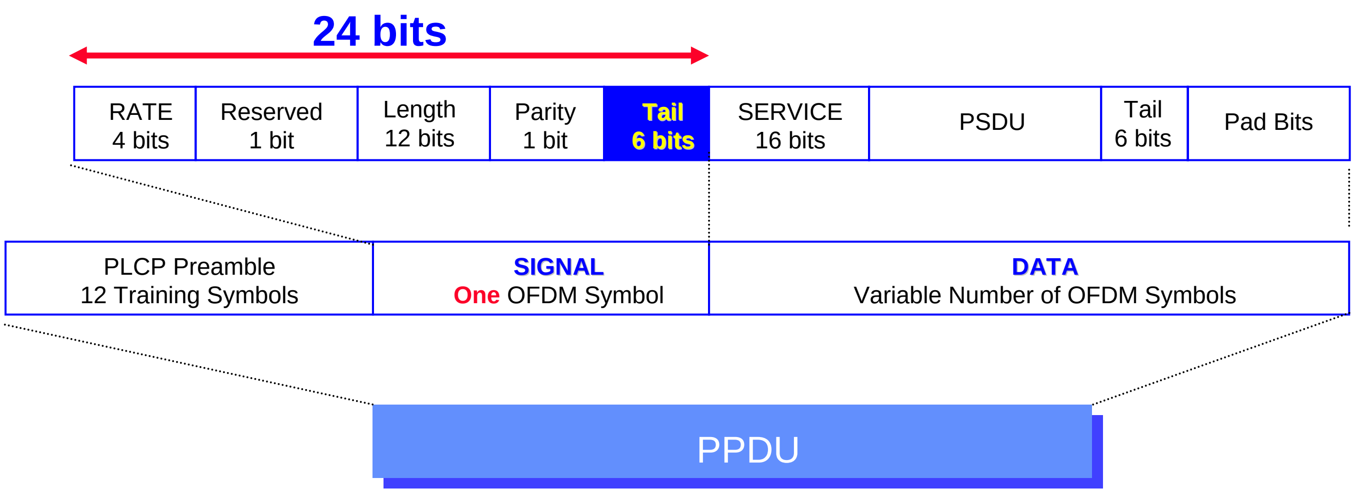
- **Data Rates (<u>determined from TXVECTOR</u>)**
  - **1101 : 6Mbps (M)**
  - **1111 : 9Mbps**
  - **0101 : 12Mbps (M)**
  - **0111 : 18Mbps**
  - **1001 : 24Mbps (M)**
  - **1011 : 36Mbps**
  - **0001 : 48Mbps**
  - **0011 : 54Mbps**

Rate-dependent Parameters

Table 78—Rate-dependent parameters

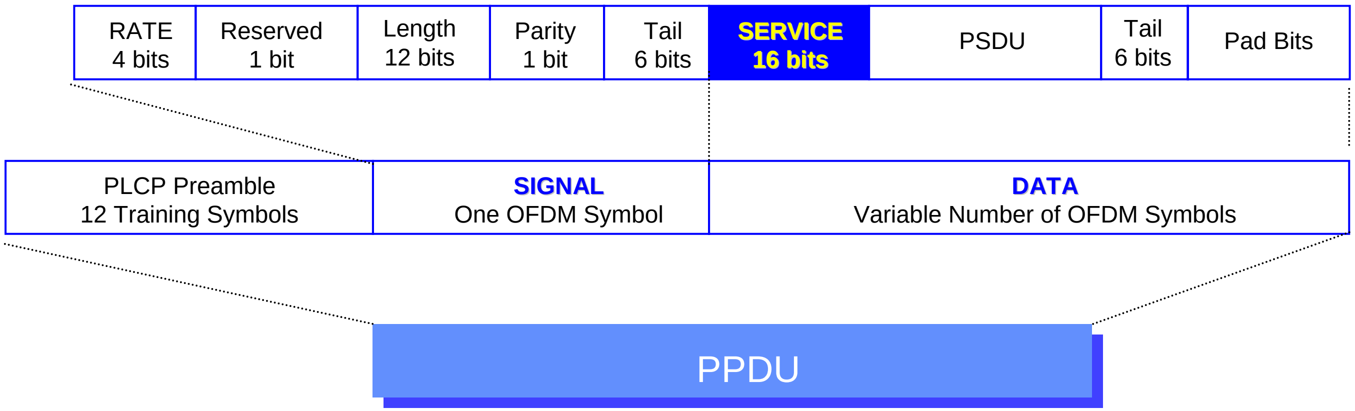
Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})	
6	BPSK	1/2	1	48	24	**(for SIGNAL field)**
9	BPSK	3/4	1	48	36	
12	QPSK	1/2	2	96	48	
18	QPSK	3/4	2	96	72	
24	16-QAM	1/2	4	192	96	
36	16-QAM	3/4	4	192	144	
48	64-QAM	2/3	6	288	192	
54	64-QAM	3/4	6	288	216	

PCLP Tail Subfield

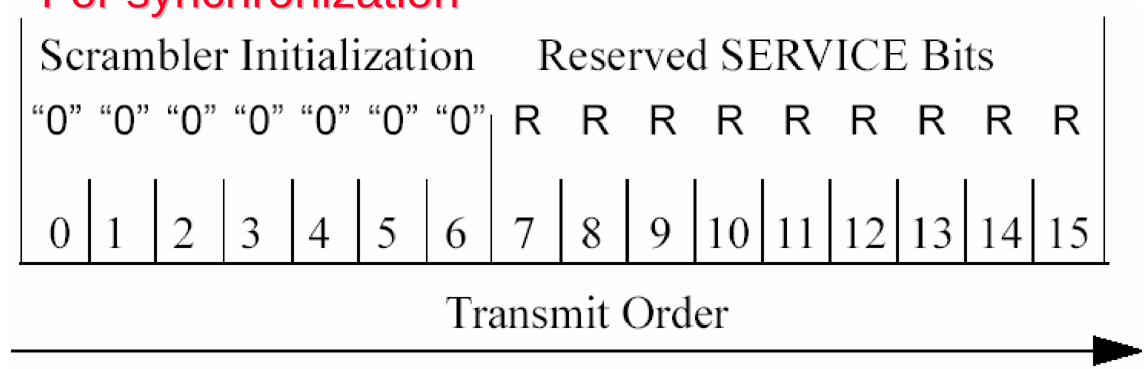


- **6 'zero' bit**
- **to make the length of SIGNAL field to be 24 bits (for the N_{DBPS}=24 in 6Mbps mode)**
- **to facilitate a reliable and timely detection of the RATE and LENGTH fields**

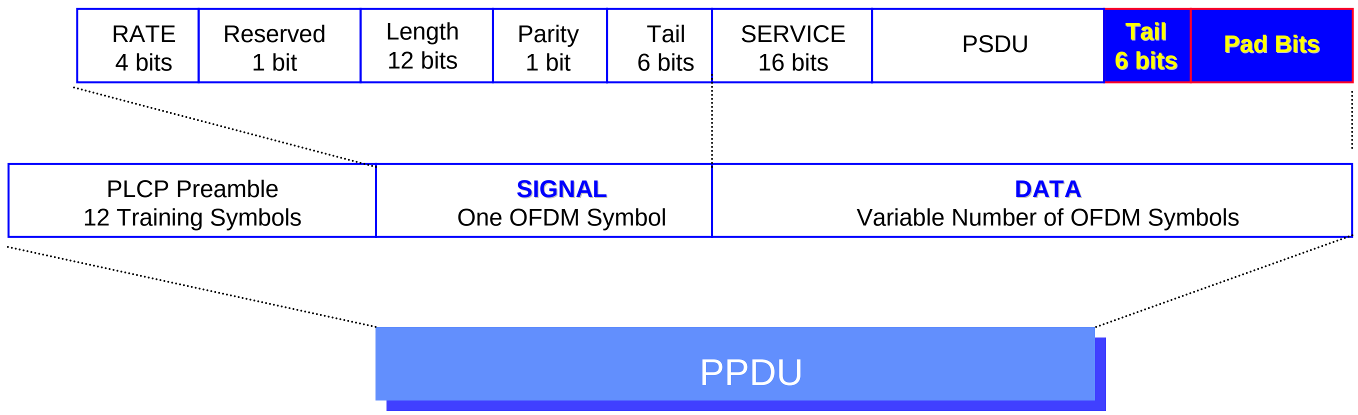
PCLP Service



For synchronization

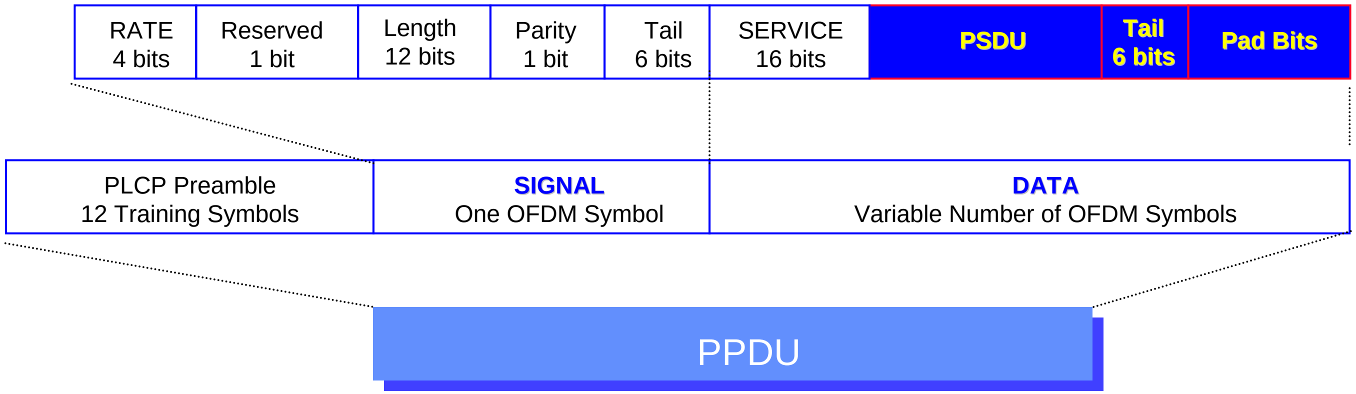


PCLP PSDU tail



- Append **6** non-scrambled tail bits for PSDU to return the convolutional code to the "zero state"
- Add pad bits (with "zero" and at least 6 bits) such that the length of DATA field is a multiple of N_{DBPS}

PCLP DATA encoding



1. encode data string with convolutional encoder (include punctured coding)
2. divide encoded bit string into groups of N_{CBPS} bits
3. within each group, perform data interleaving
4. For each of the groups, convert bit string group into a complex number according to the modulation tables (see next page)
5. divide the complex number string into groups of **48** complex numbers, each such group will be associated with one OFDM symbol
   - map to subcarriers –26~-22, -20~-8, -6~-1, 1~6, 8~20, 22~26
   - **4** sucarriers –21, -7, 7, 21 are used for pilot
   - subcarrier 0 is useless
6. convert subcarriers to time domain using inverse Fast Fourier transform (IFFT)
7. append OFDM symbols after SINGNAL and un-convert to RF freq.

Modulation Tables

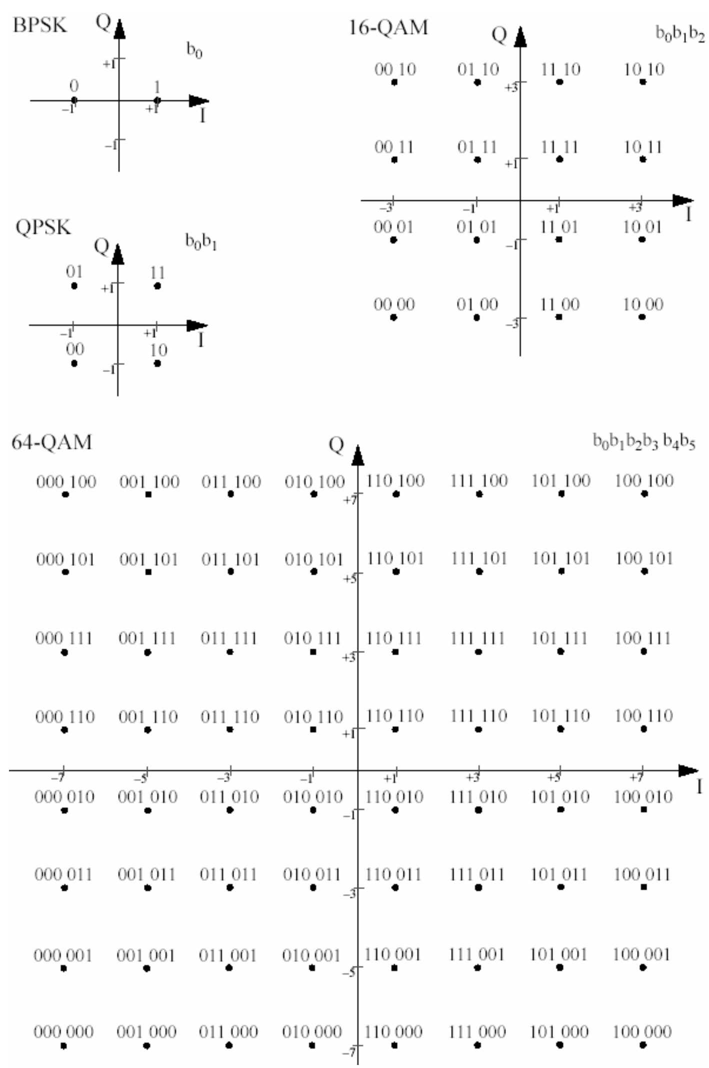


Table 82—BPSK encoding table

Input bit (b_0)	I-out	Q-out
0	–1	0
1	1	0

Table 83—QPSK encoding table

Input bit (b_0)	I-out
0	–1
1	1

Input bit (b_1)	Q-out
0	–1
1	1

Table 84—16-QAM encoding table

Input bits (b_0 b_1)	I-out
00	–3
01	–1
11	1
10	3

Input bits (b_2 b_3)	Q-out
00	–3
01	–1
11	1
10	3

Table 85—64-QAM encoding table

Input bits (b_0 b_1 b_2)	I-out
000	–7
001	–5
011	–3
010	–1
110	1
111	3
101	5
100	7

Input bits (b_3 b_4 b_5)	Q-out
000	–7
001	–5
011	–3
010	–1
110	1
111	3
101	5
100	7

Convolutional Encoder

- use the industry-standard generator polynomials,
  - $g0 = 133_8$ and $g1 = 171_8$, of rate $R = 1/2$,

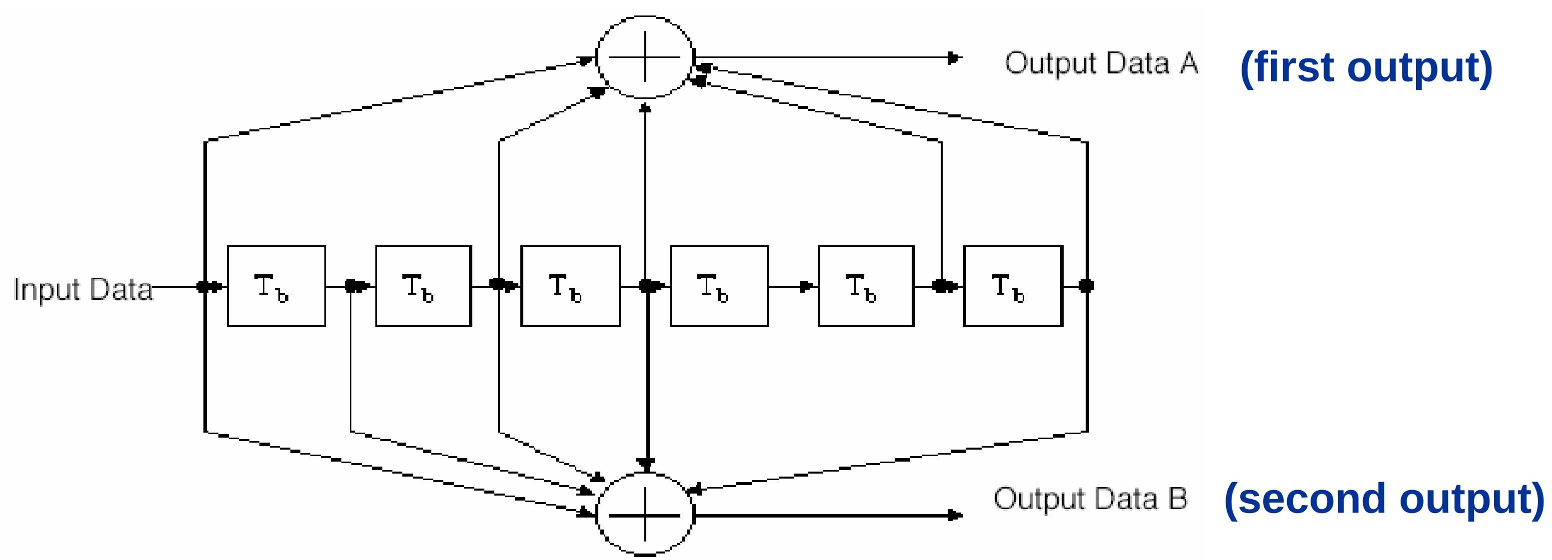
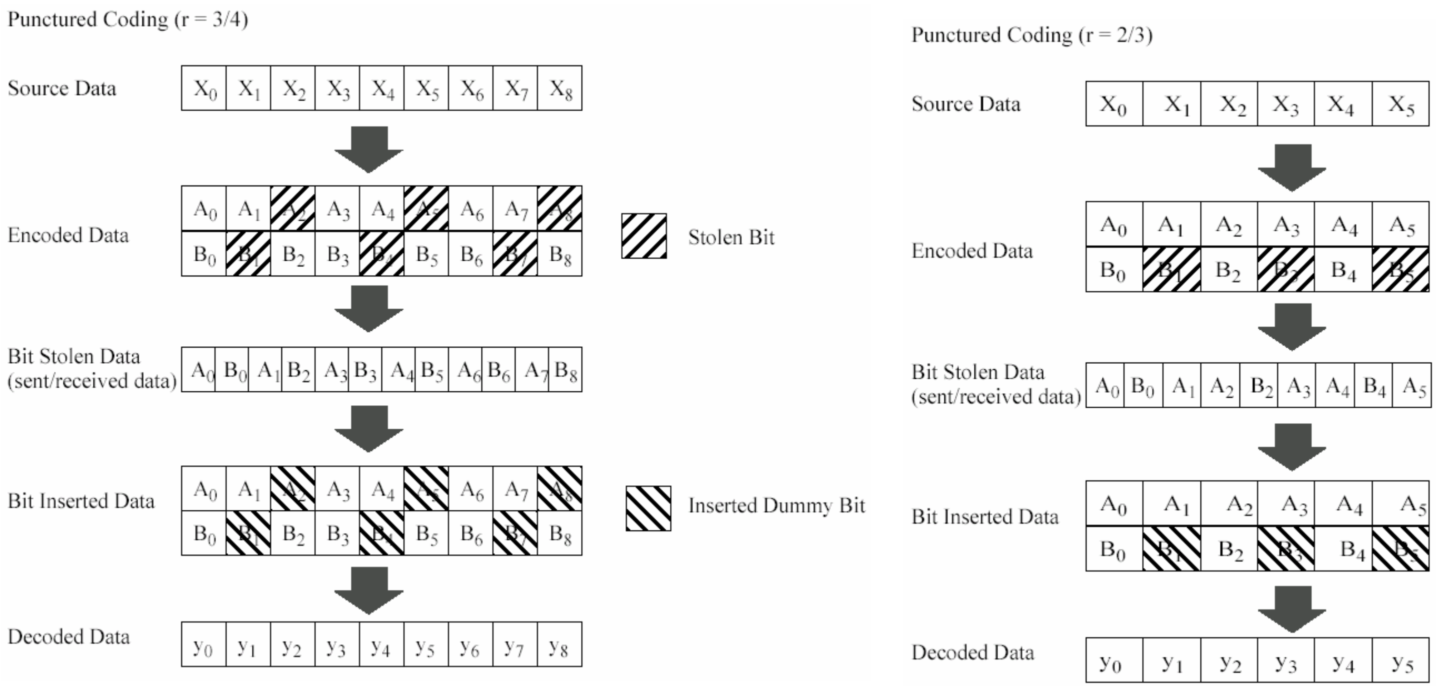


Figure 114—Convolutional encoder (k = 7)

Punctured Coding

- **to omit some of the encoded bits in the transmitter**
  - thus reducing the number of transmitted bits and increasing the coding rate
  - inserting a dummy "zero" metric into the convolutional decoder on the receive side
  - decoding by the Viterbi algorithm is recommended.



Timing-related Parameters

Table 79—Timing-related parameters

Parameter	Value
N_{SD}: Number of data subcarriers	48
N_{SP}: Number of pilot subcarriers	4
N_{ST}: Number of subcarriers, total	52 ($N_{SD} + N_{SP}$)
Δ_F: Subcarrier frequency spacing	0.3125 MHz (=20 MHz/64)
T_{FFT}: IFFT/FFT period	3.2 μs ($1/\Delta_F$)
$T_{PREAMBLE}$: PLCP preamble duration	16 μs ($T_{SHORT} + T_{LONG}$)
T_{SIGNAL}: Duration of the SIGNAL BPSK-OFDM symbol	4.0 μs ($T_{GI} + T_{FFT}$)
T_{GI}: GI duration	0.8 μs ($T_{FFT}/4$)
T_{GI2}: Training symbol GI duration	1.6 μs ($T_{FFT}/2$)
T_{SYM}: Symbol interval	4 μs ($T_{GI} + T_{FFT}$)
T_{SHORT}: Short training sequence duration	8 μs ($10 \times T_{FFT}/4$)
T_{LONG}: Long training sequence duration	8 μs ($T_{GI2} + 2 \times T_{FFT}$)

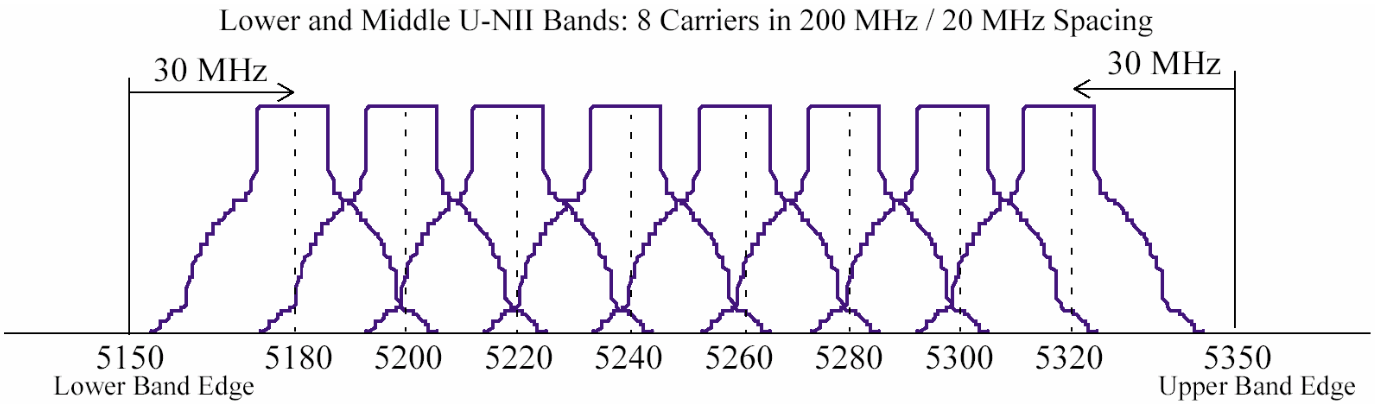
- **Slot time : 9us**
- **CCA detect time < 4us**

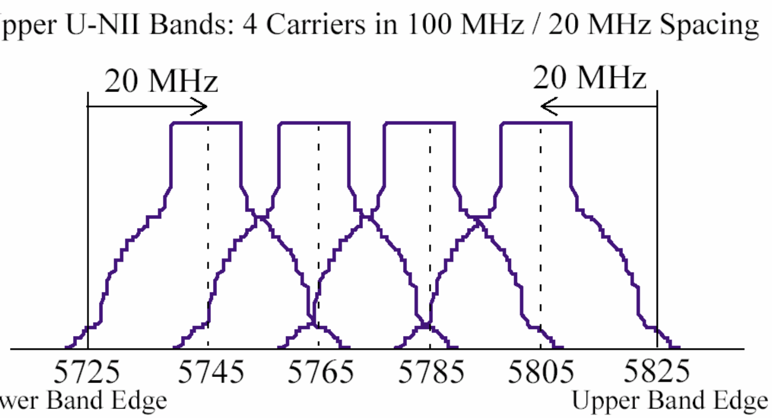
OFDM PHY Characteristics

- **OFDM**
- Slottime 9 us
- SIFS 16 us (6us for decoder)
- CCA Time < 4 us
- TX to Rx turnaround time < 10 us
- Rx to Tx turnaround time < 5 us
- Preamble Length 16 us
- PLCP Header Length 4 us
- MPDUmax Length 4095
- aCWmin 15
- aCWmax 1023

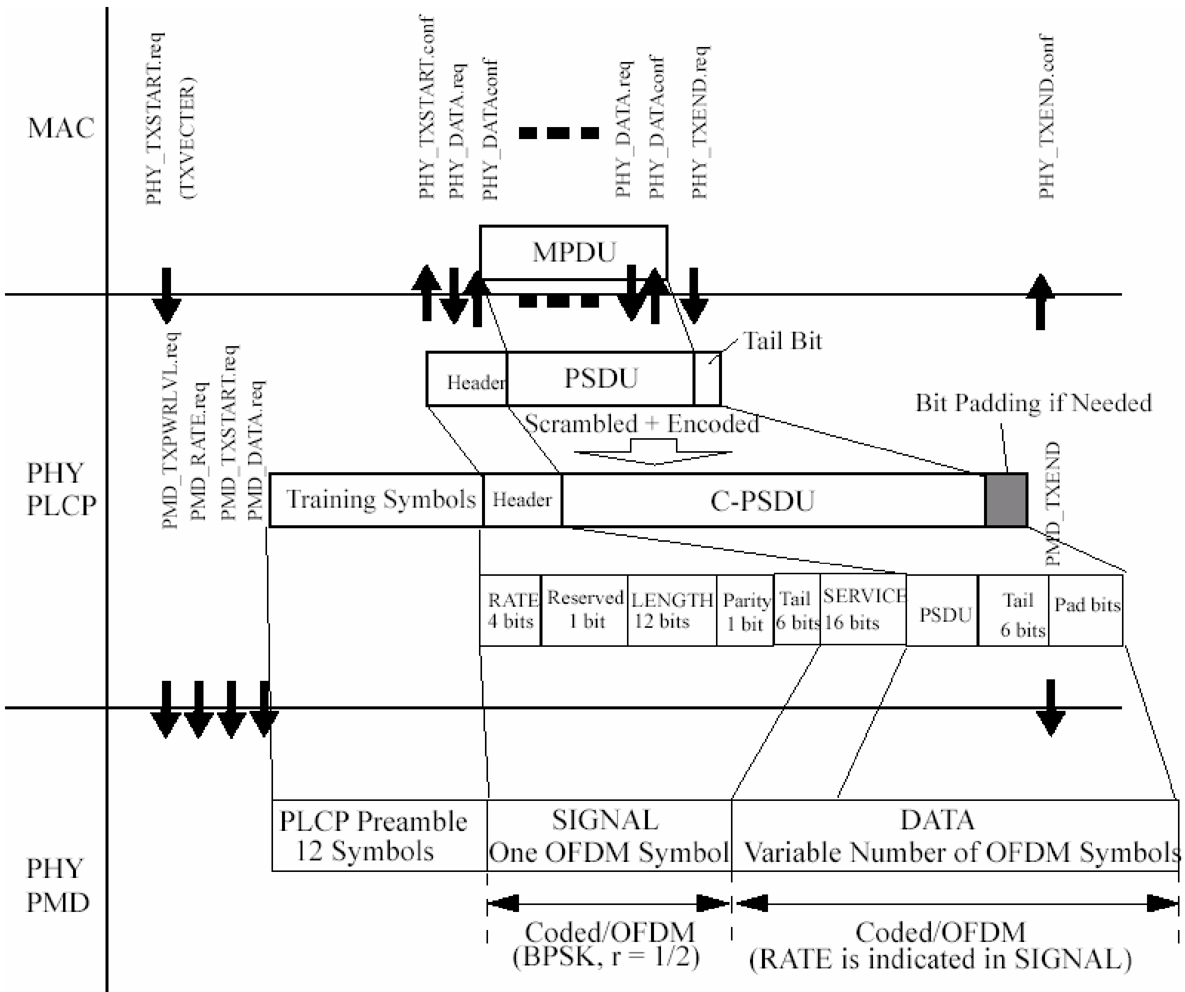
Channelization

- **8 independent channels in 5.15GHz-5.35GHz**
- **4 independent channels in 5.725-5.825GHz**

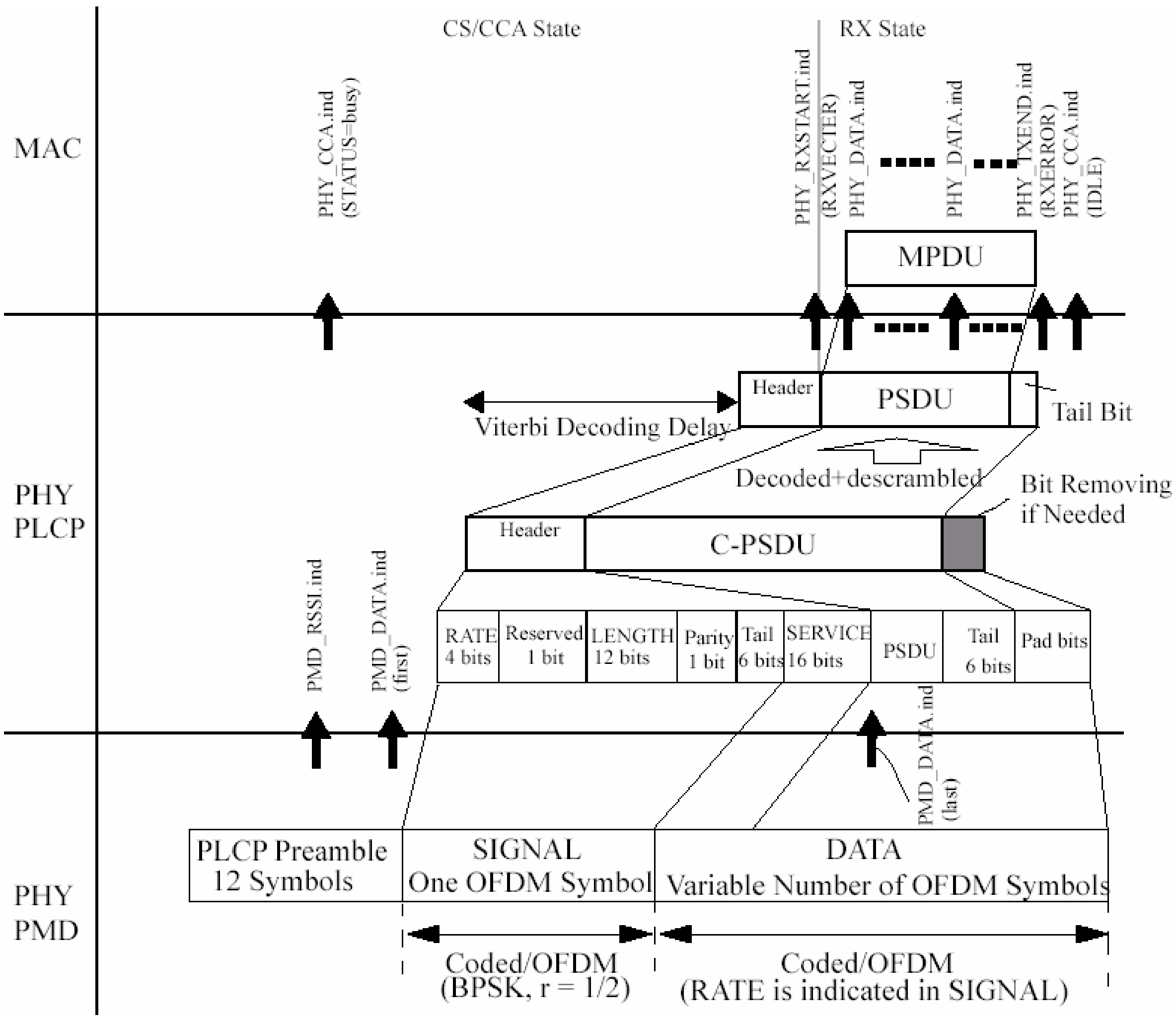




PCLP Transmit Procedure

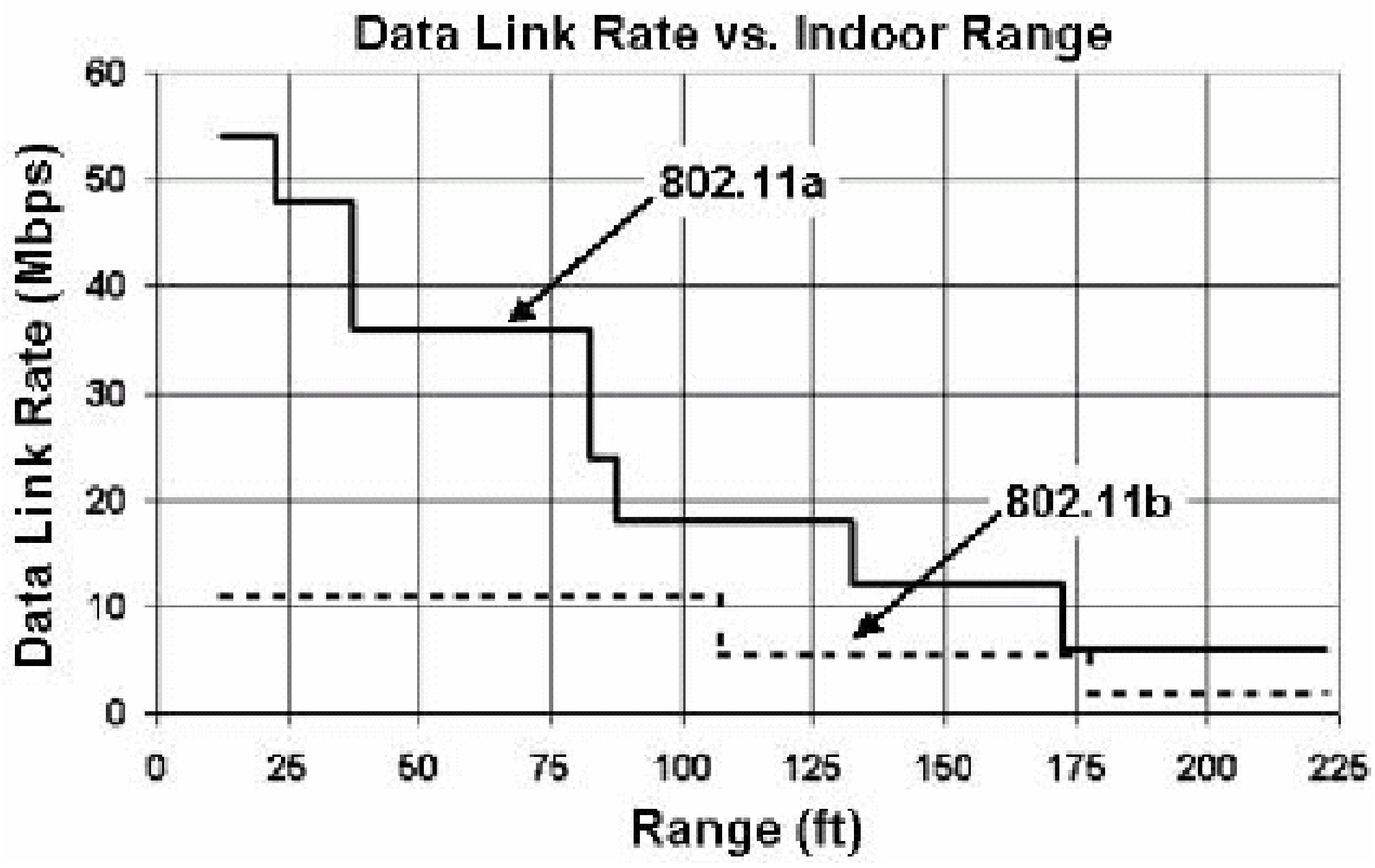


PCLP Receive Procedure



IEEE 802.11a vs IEEE 802.11b (max.)

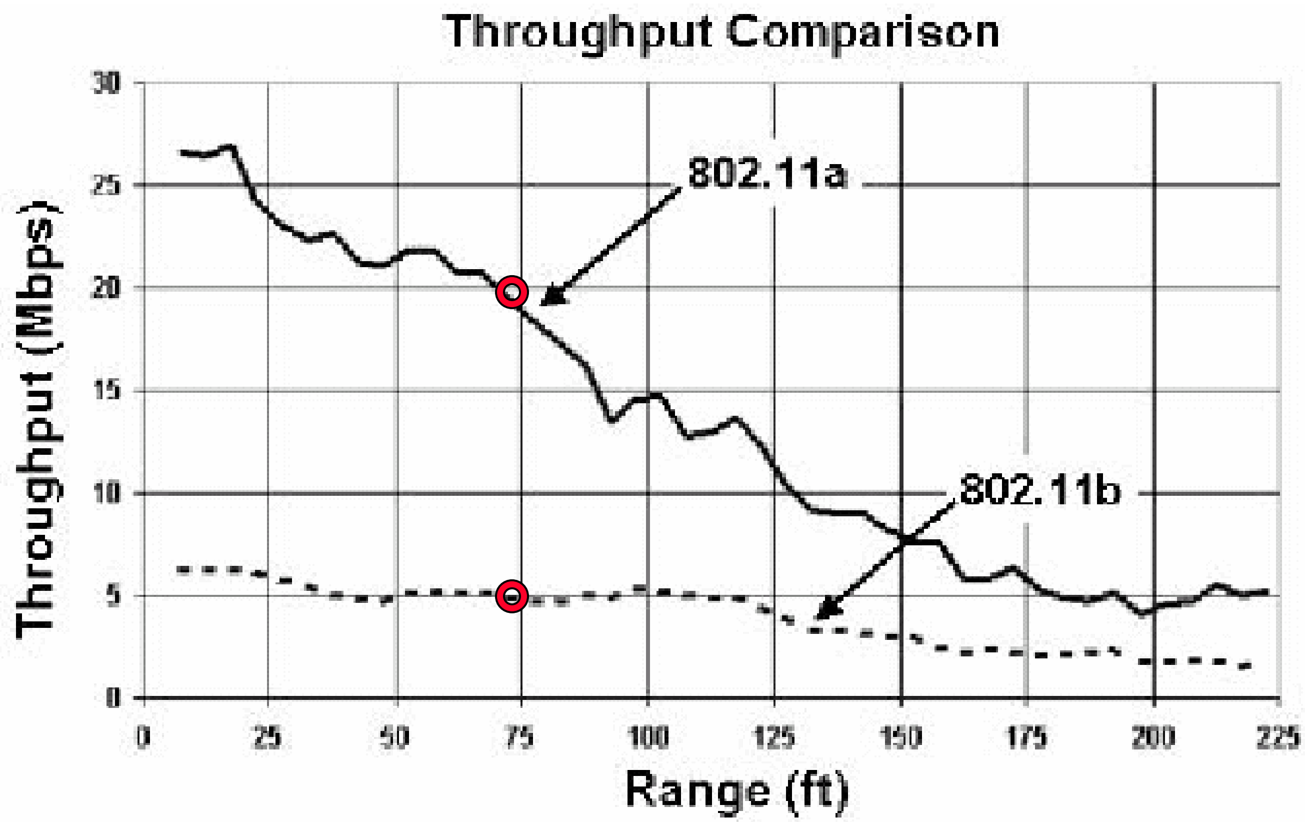
1500 bytes per frame



Refer from "AtherosRangeCapacityPaper.pdf"

IEEE 802.11a vs IEEE 802.11b (average)

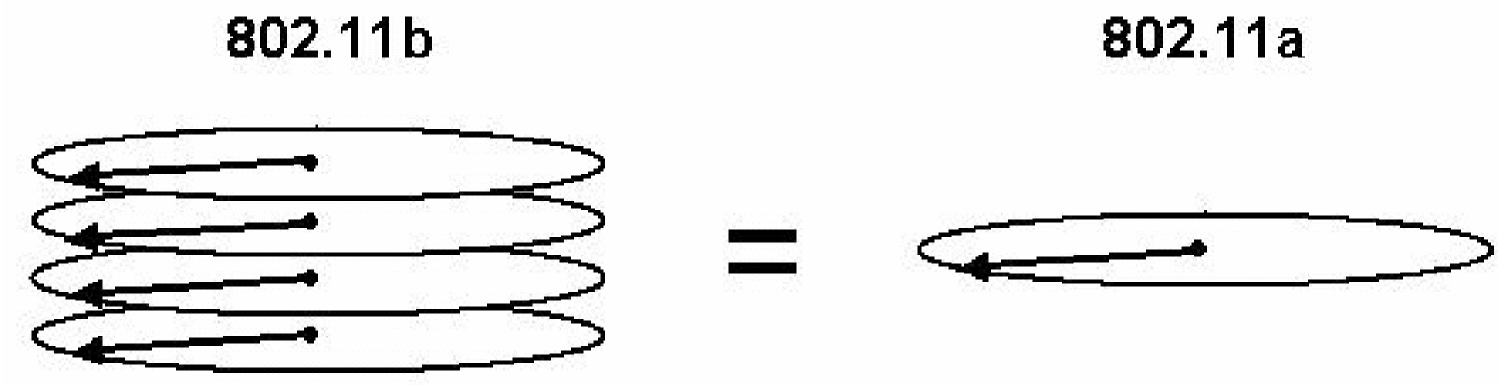
1500 bytes per frame



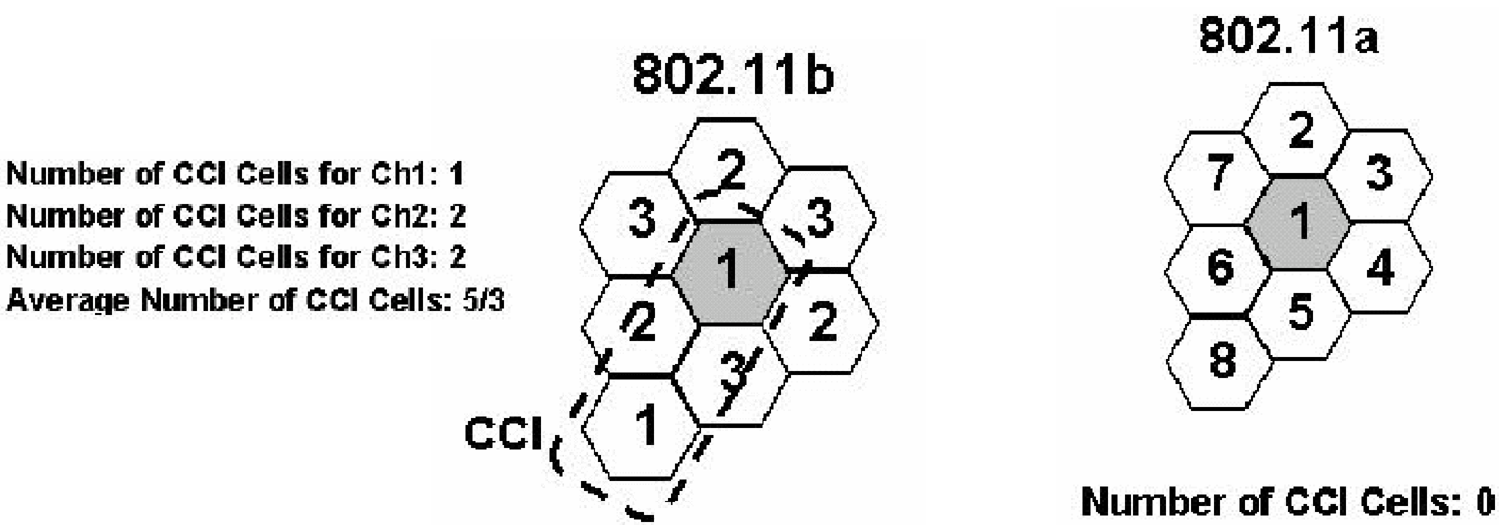
Refer from “AtherosRangeCapacityPaper.pdf”

IEEE 802.11a vs IEEE 802.11b (average)

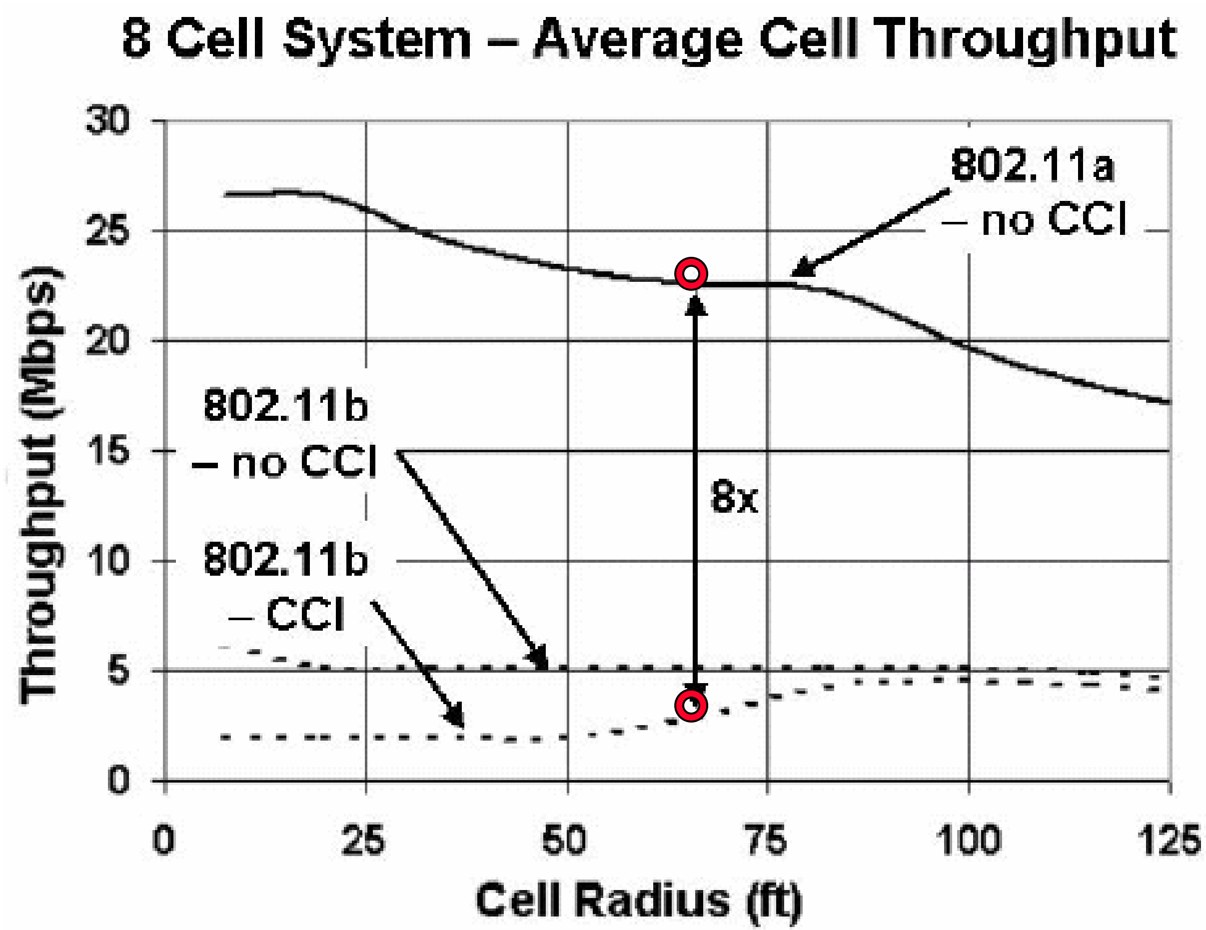
for a cell radius of 65 feet



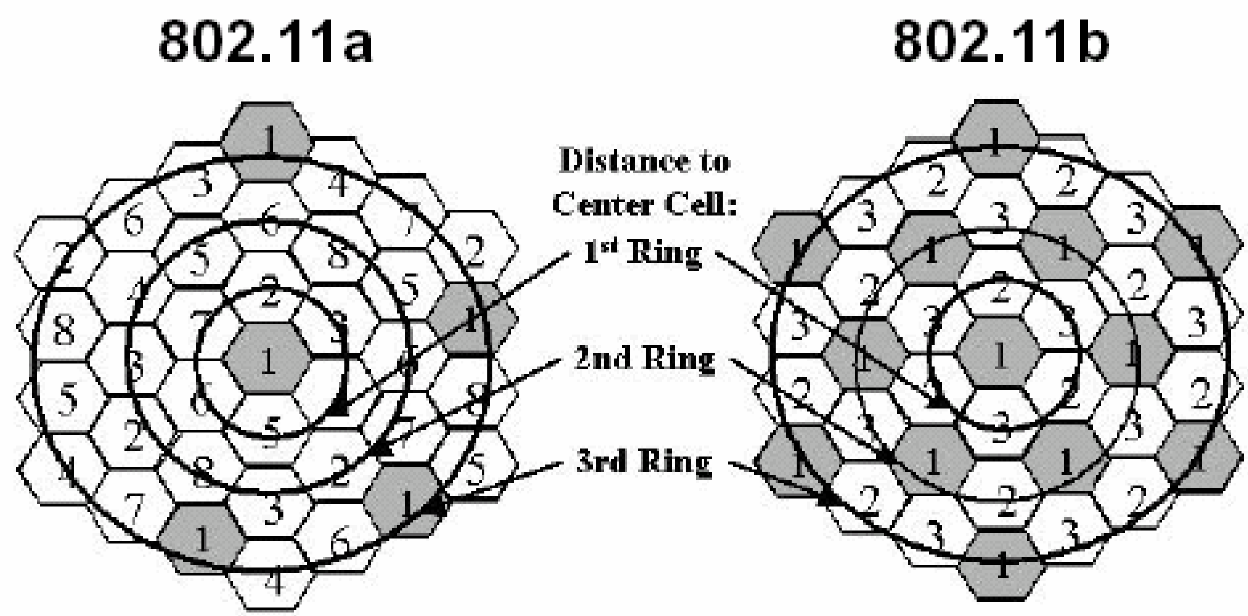
Cell allocation



IEEE 802.11a vs IEEE 802.11b (average)



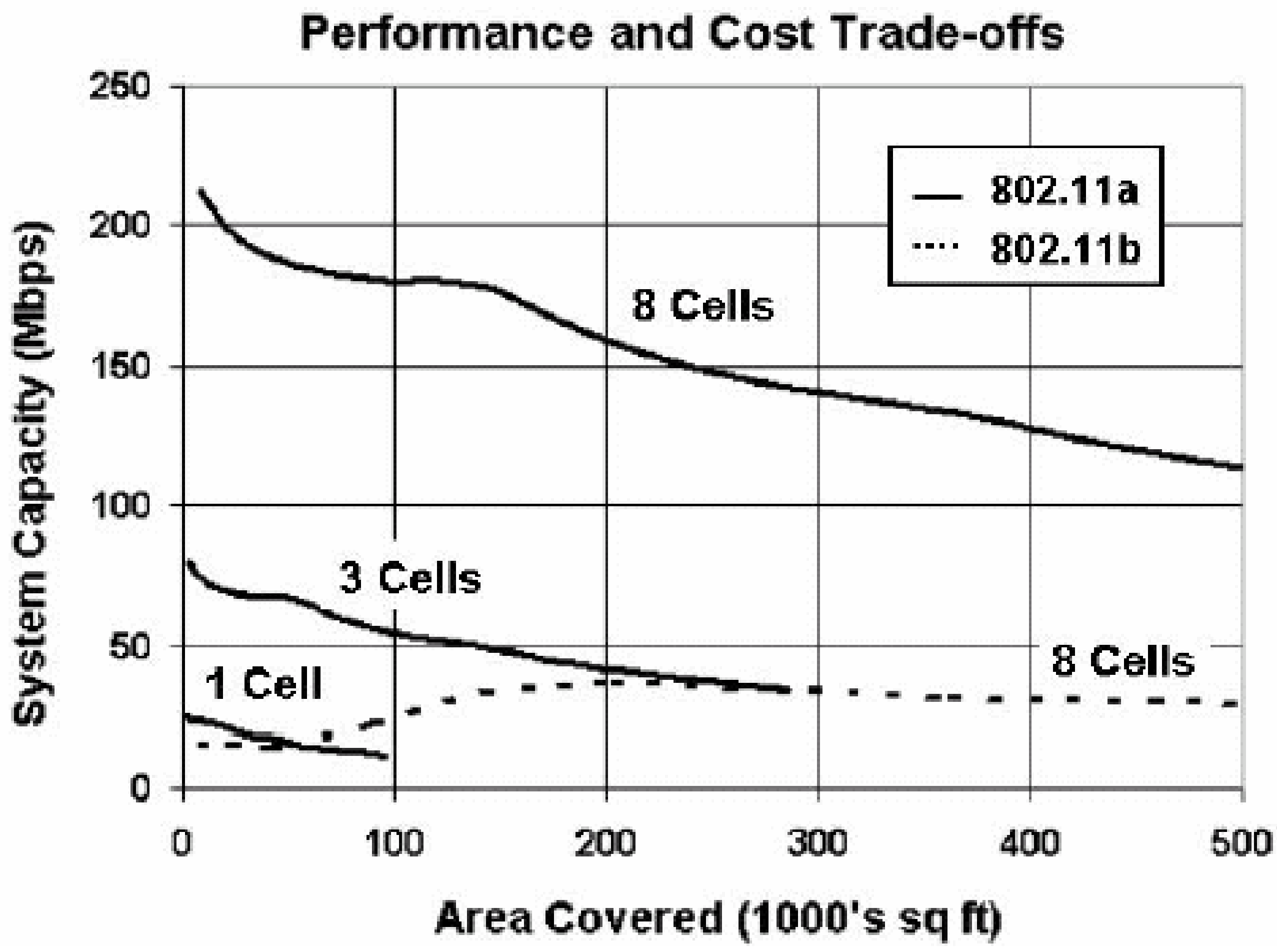
IEEE 802.11a vs IEEE 802.11b (average)



Number of CCI cells in 1st Ring: 0
Number of CCI cells in 2nd Ring: 0
Number of CCI cells in 3rd Ring: 4

Number of CCI cells in 1st Ring: 0
Number of CCI cells in 2nd Ring: 6
Number of CCI cells in 3rd ring: 12

IEEE 802.11a vs IEEE 802.11b (average)



5. IEEE 802.11g Extended Rate PHY (ERP) Specification

IEEE 802.11g

- **Extended Rate PHY (ERP) Goal :**
  - **coexists with 802.11b (.....?)**
  - **enhances the ability of interference protection**
- **ERP-DSSS/CCK (Mandatory) (1,2,5.5,11 Mbps)**
  - **short PLCP PPDU is mandatory**
  - **transmit center frequency and symbol clock frequency shall refer the same oscillator (locked oscillator, mandatory)**
- **ERP-OFDM (Mandatory) (6,9,12,18,24,36,48,54 Mbps)**
  - **Optional 9 us slot time when the BSS consists of only ERP devices**
- **ER-PBCC (Optional) (5.5,11,22,33 Mbps)**
  - **256-state binary convolutional code**
- **ERP-DSSS-OFDM (Optional) (6,9,12,18,24,36,48,54 Mbps)**
  - **Hybrid modulation**
  - **DSSS : for preamble and header**
  - **OFDM : for data payload**

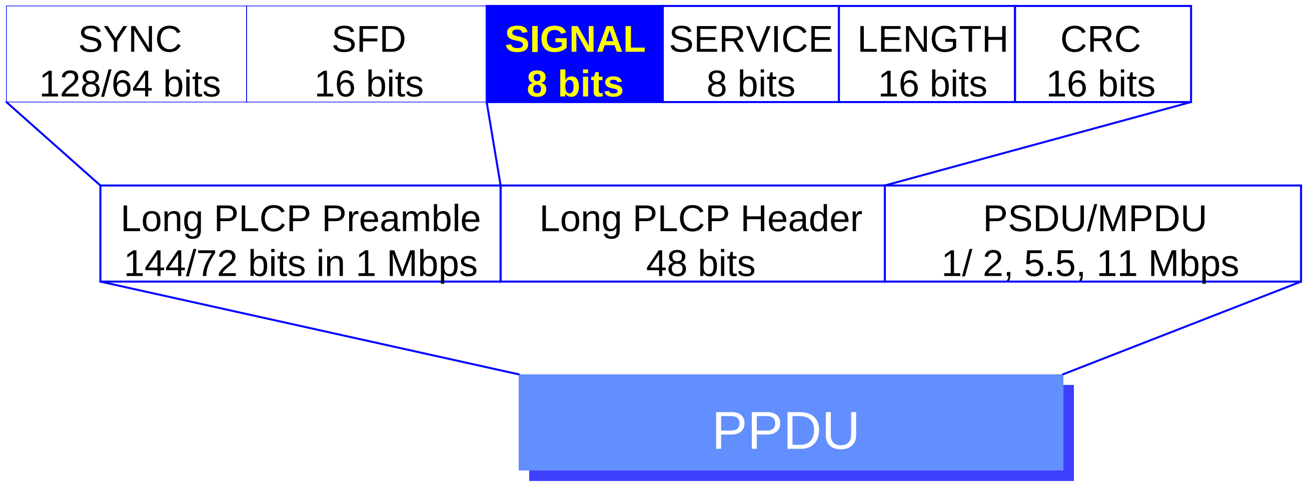
IEEE 802.11g PCLP

- **Three different mandatory PLCP PPDU format**
  - **Long Preamble and header (same as 11b) (for DSSS-OFDM and ERP-PBCC)**
  - **Short Preamble and header (same as 11b) (for DSSS-CCK)**
    - **Differences in SERVICE field**
      - **Diff 1 : a bit in SERVICE field is used to indicate DSSS-OFDM**
      - **Diff 2 : two bits in SERVICE field are used to resolve the length ambiguity for PBCC-22 and PBCC-33**

b0	B1	b2	b3	b4	b5	b6	b7
Modulation selection 0 = Not DSSS-OFDM 1 = DSSS-OFDM	Reserved	Locked Clock Bit 0 = not locked 1 = locked	Modulation Selection 0 = CCK 1 = PBCC	Reserved	Length Extension Bit (PBCC)	Length Extension Bit (PBCC)	Length Extension Bit

  - **OFDM preamble and header (similar as 11a) (for ERP-OFDM)**

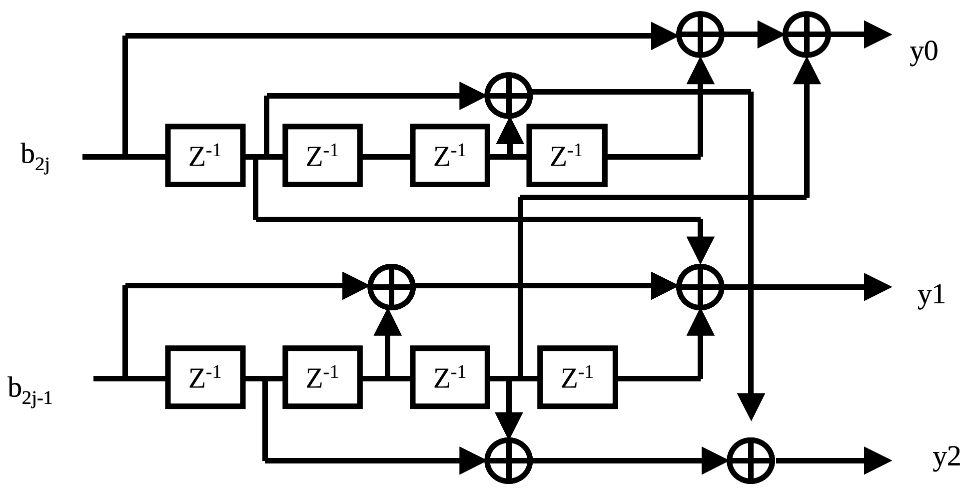
Long/Short PLCP for PBCC-22 and PBCC-33



- **Rate indication**
  - **h0A 1Mb/s DBPSK (for long only)**
  - **h14 2Mb/s DQPSK**
  - **h37 5.5Mb/s CCK or PBCC**
  - **h6E 11Mbps CCK or PBCC**
  - **hDC 22Mbps PBCC-22**
  - **h21 33Mbps PBCC-33**

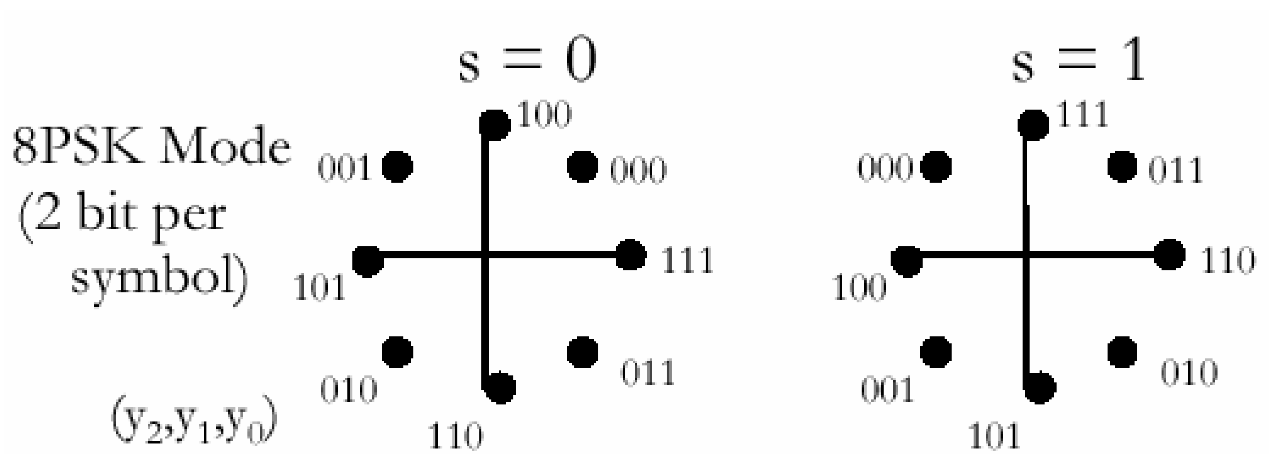
PBCC-22 in 802.11g

- **256-state binary convolutional code of rate R=2/3**
- **PBCC-22 convolutional encoder**
  - **Provide encoder the "known state"**
    - » **4 memory elements are needed and**
    - » **one octet containing all zeros is appended to the end of the PPDU prior to transmission**
      - **One more octet than CCK**
  - **For every pair of data bits input, three output bits are generated (R=2/3)**



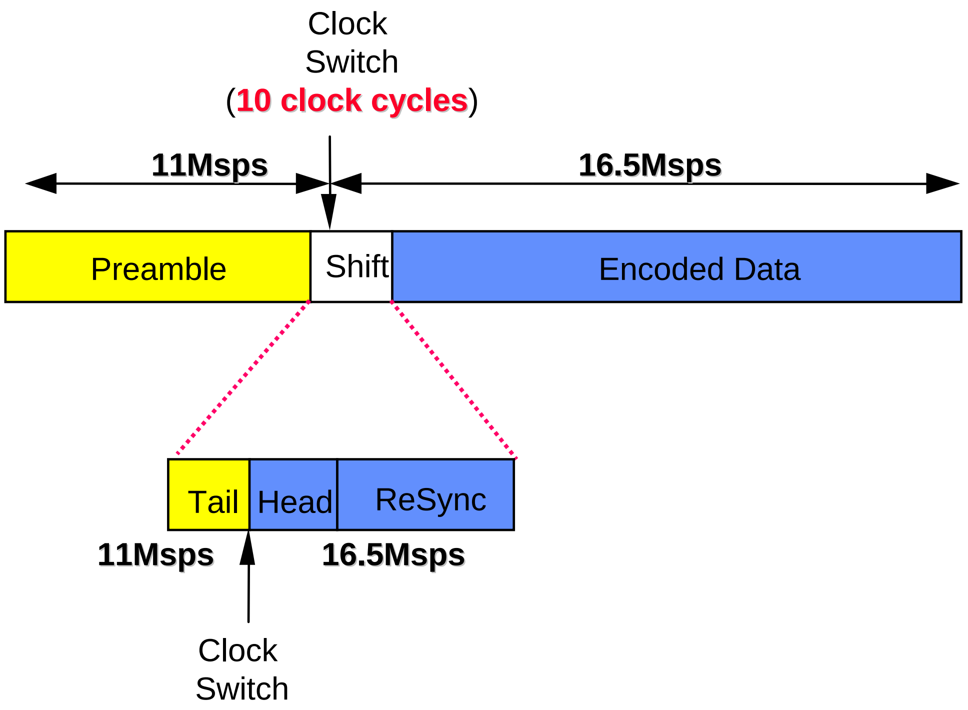
PBCC-22 in 802.11g

- For **22Mbps**, three output bits (y0,y1,y2) produce one symbol via **8-PSK**
  - two data bits per symbol

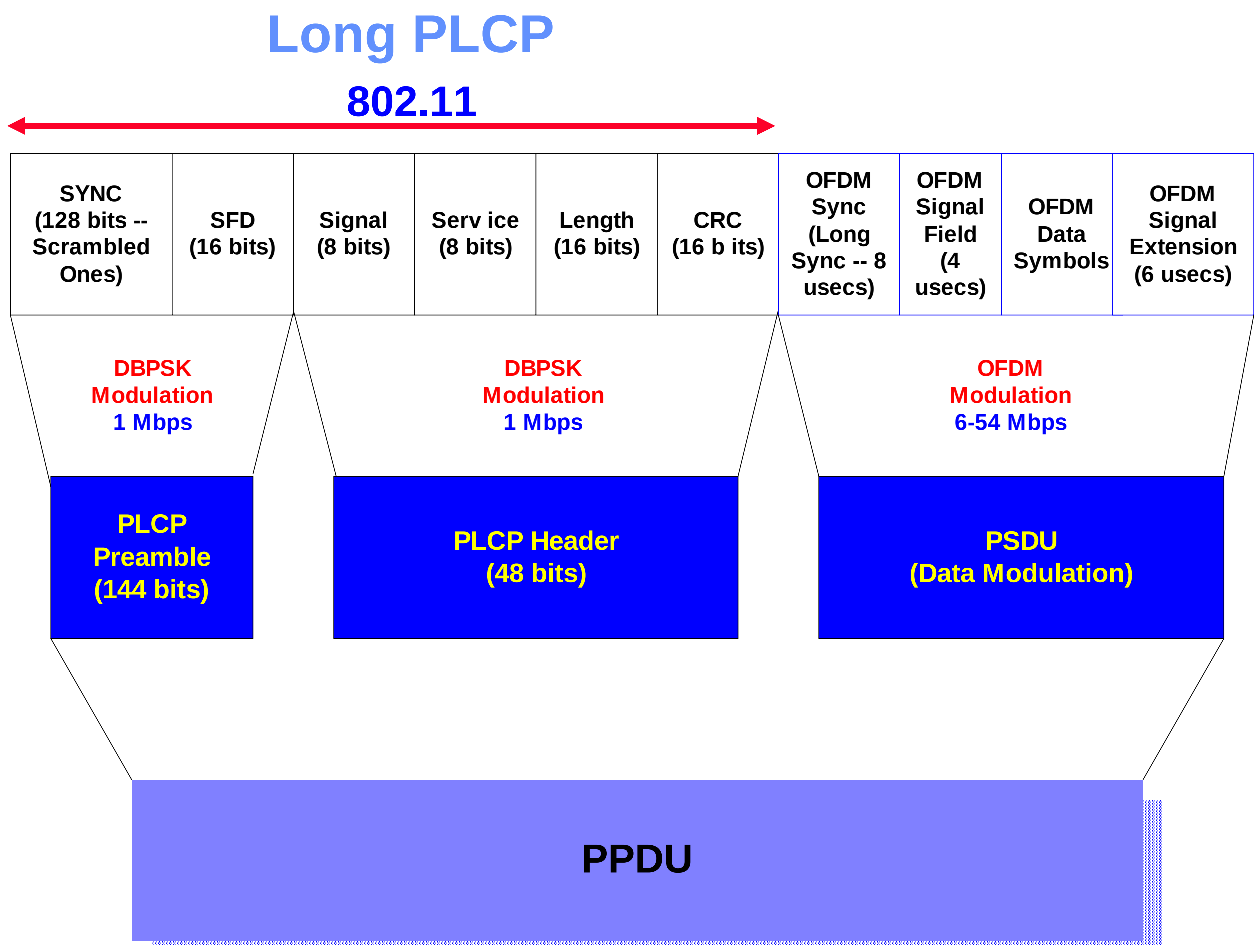


PBCC-33 in 802.11g

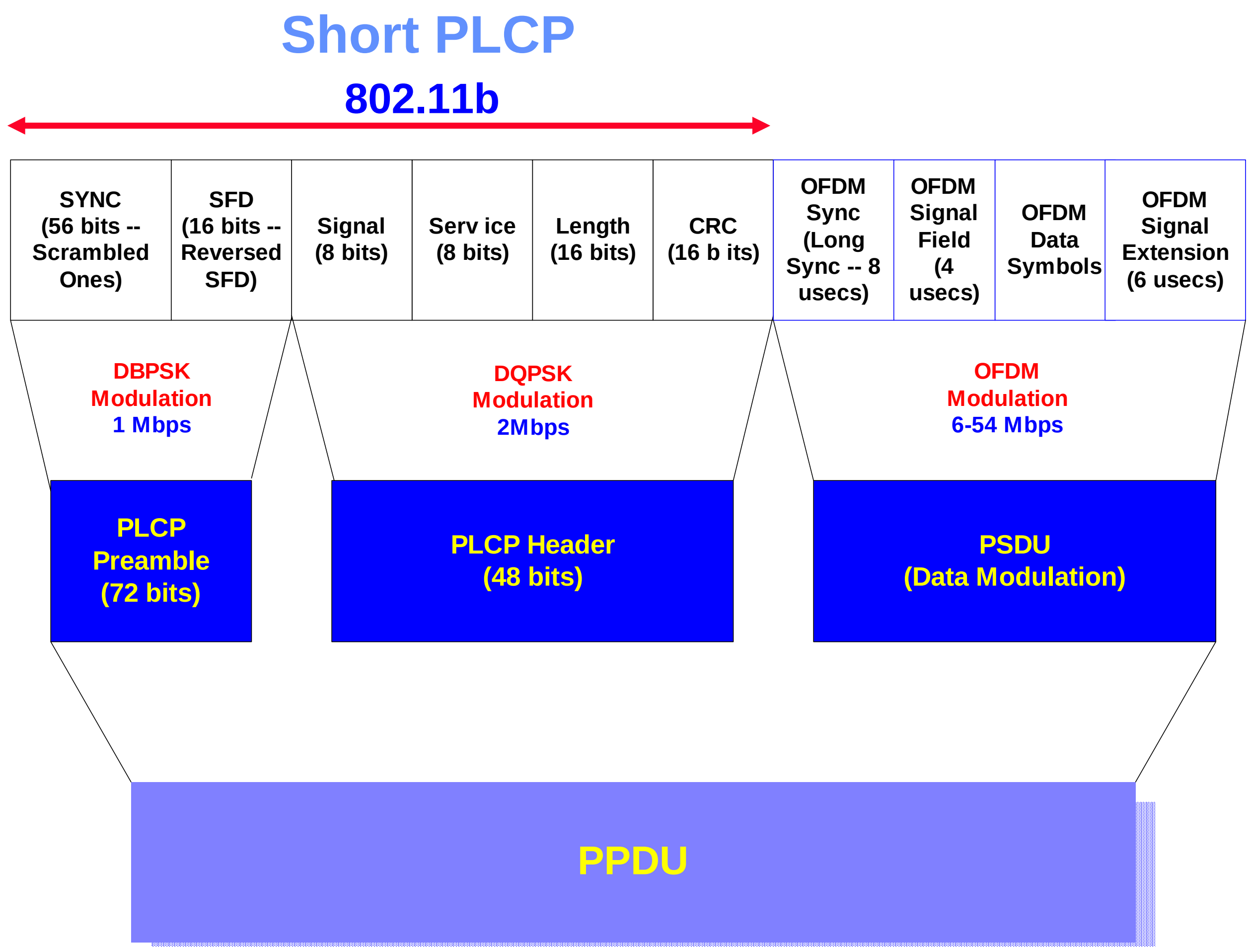
- Upgrade the 802.11b 11Msps (in 20MHz bandwidth) as 16.5Msps
  - by using pulse shaping and adaptive equalization
  - enhance 50% data rate



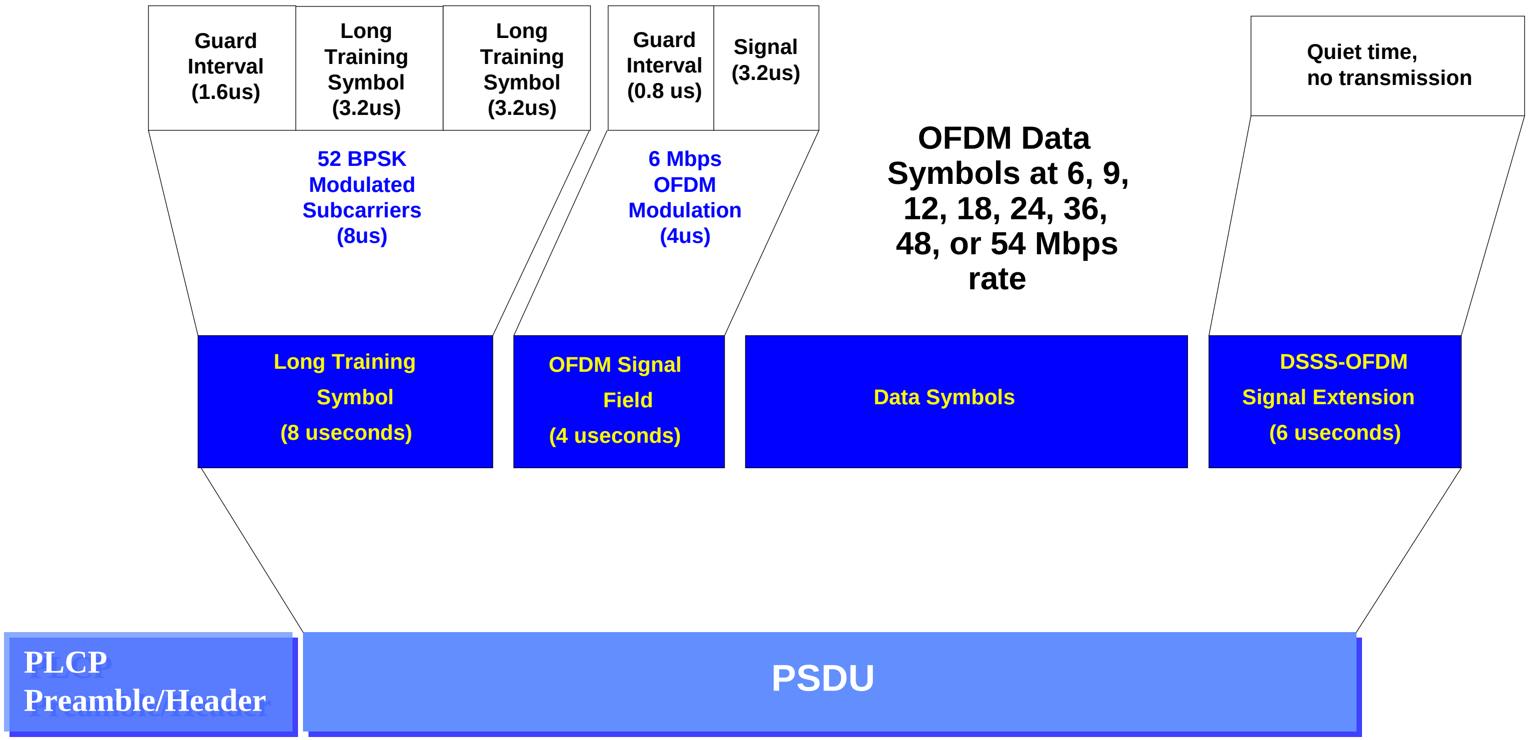
Long PLCP for 802.11g DSSS-OFDM



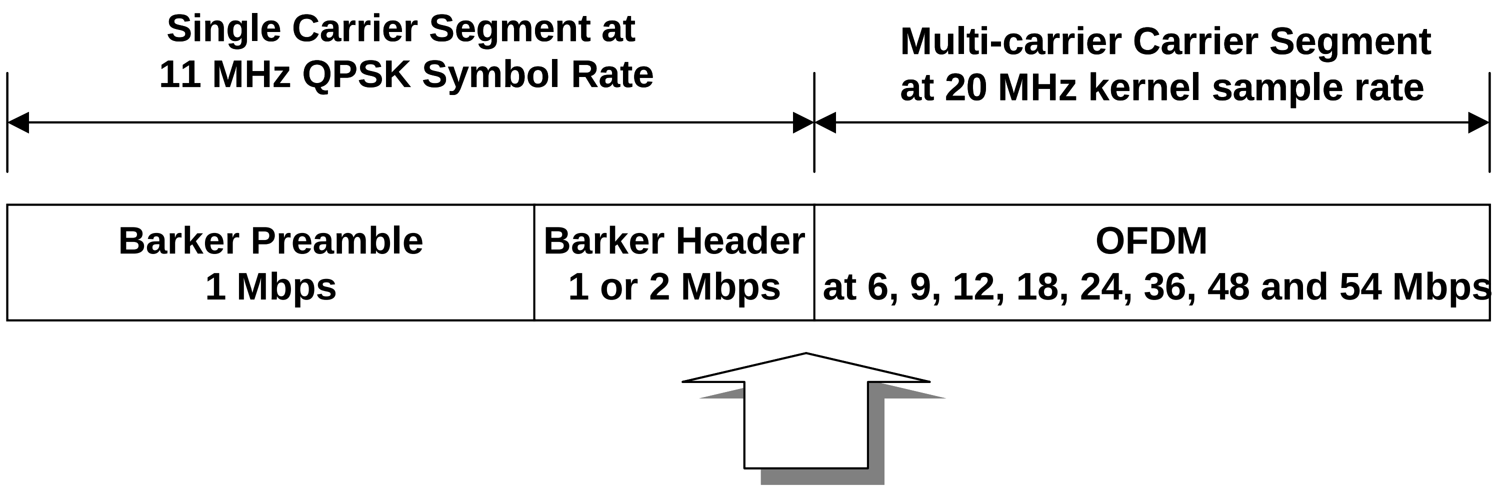
Short PLCP for 802.11g DSSS-OFDM



DSSS-OFDM PLCP PSDU Encoding



Single-Carrier to Multi-carrier transition

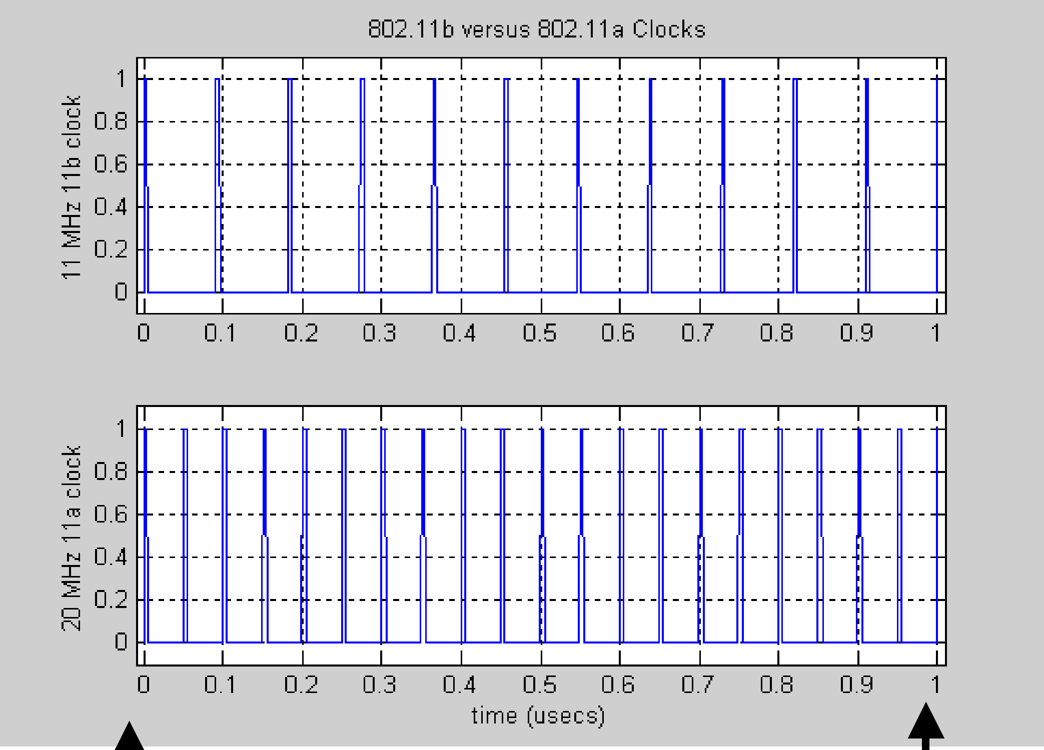


Ideal Transition Specification

- **Constant Power**
- **Constant Spectrum**
- **Constant Frequency and Phase**
- **Constant Timing**

Single-Carrier to Multi-carrier transition

- **The signals are easily aligned by first aligning the 11 MHz clock and the 20 MHz clock on 1 us boundaries**



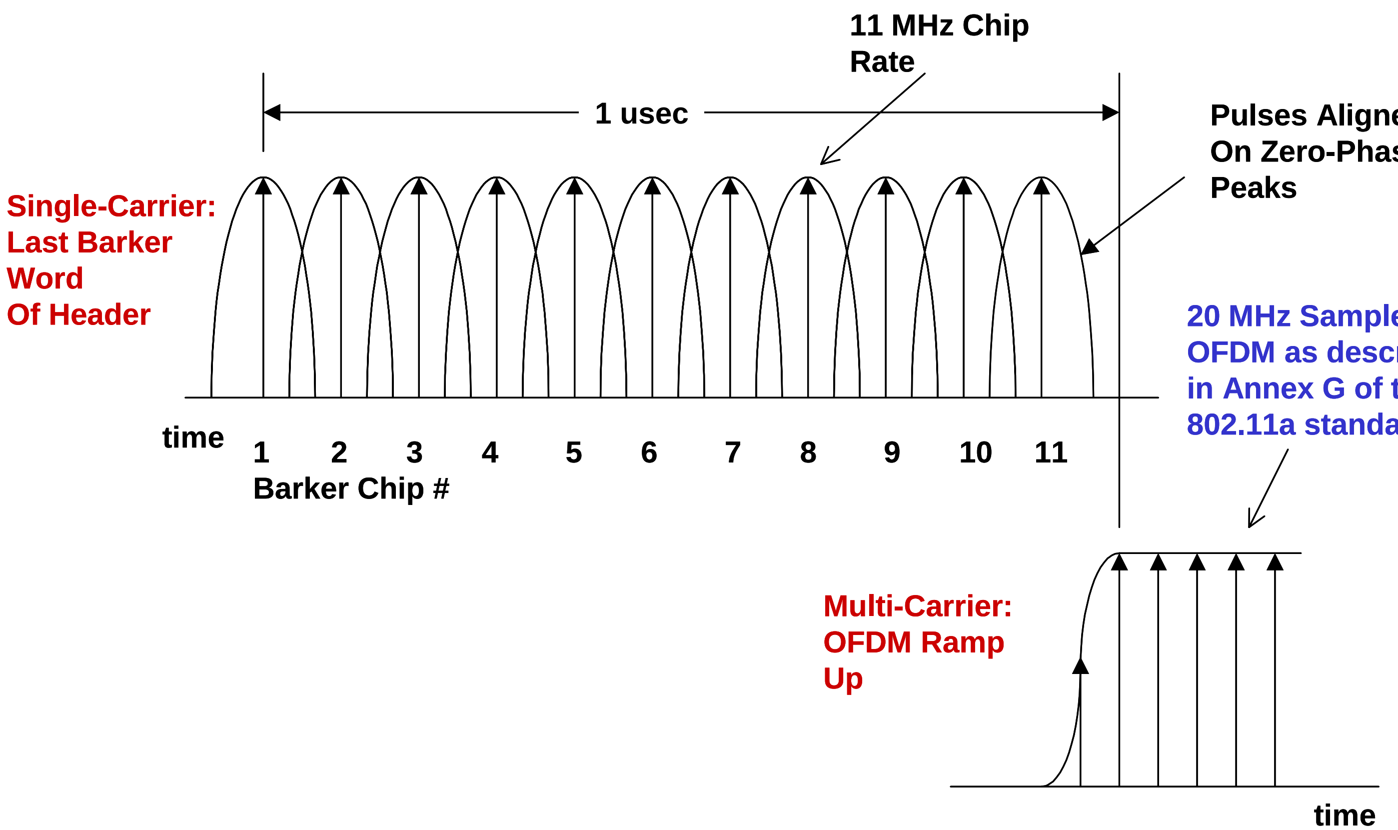
1/11 vs. 1/20

Alignment Epoch

Alignment Epoch

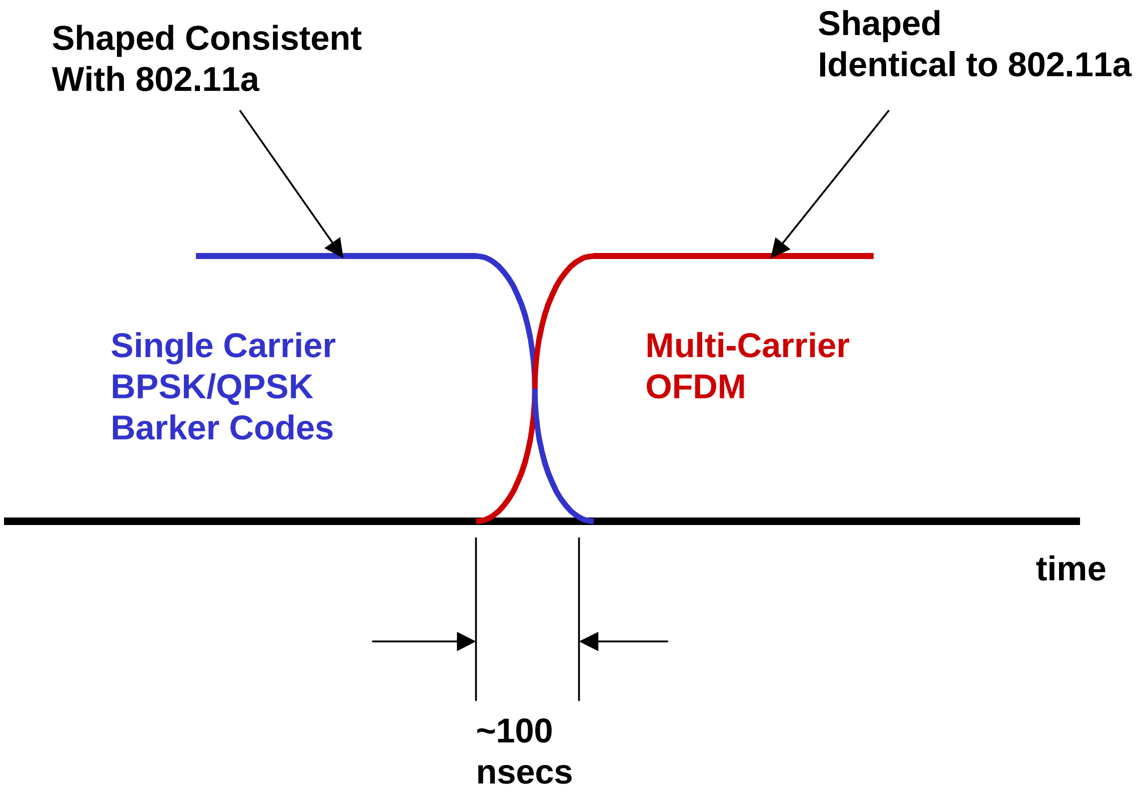
Single-Carrier to Multi-carrier transition

- The signals are easily aligned by first aligning the 11 MHz clock and the 20 MHz clock on 1 us boundaries



Single-Carrier to Multi-carrier transition

- **The single carrier segment of a packet should terminate in nominally 0.1 us (100ns)**



Extended Rate PHY Characteristics

- **ERP-OFDM**

• **Slottime**	**Long: 20 us (DSSS)** **Short: 9 us** (OFDM)
SIFS	10/16 us
• **CCA Time**	**Long: < 15 us** **Short: < 4 us**
• **TX to Rx turnaround time**	**< 10** us
• **Rx to Tx turnaround time**	**< 5** us
• **Preamble Length**	**20 us**
• **PLCP Header Length**	**4 us**
• **MPDUmax Length**	**4095**
• **aCWmin(0)**	**31 (for 11b)**
• **aCWmin(1)**	**15 (for 11g OFDM)**
• **aCWmax**	**1023**

6. Frequency Hopping Spread Spectrum PHY of the 802.11 Wireless LAN Standard

Why Frequency Hopping?

- Frequency Hopping is one of the variants of Spread Spectrum- a technique which enables coexistence of multiple networks (or other devices) in same area
- FCC recognizes Frequency Hopping as one of the techniques withstanding Fairness requirements for unlicensed operation in the ISM bands.
- 802.11 Frequency Hopping PHY uses 79 nonoverlapping frequency channels with 1 MHz channel spacing.
- FH enables operation of up to 26 collocated networks, enabling therefore high aggregate throughput.
- Frequency Hopping is resistant to multipath fading through the inherent frequency diversity mechanism

Regulatory requirements for FH

- North America (CFR47, Parts 15.247, 15.205, 15.209):
  - Frequency band: 2400-2483.5 MHz
  - At most 1 MHz bandwidth (at -20 dB re peak)
  - At least 75 hopping channels, pseudorandom hopping pattern
  - At most 1 W transmit power and 4 W EIRP (including antenna)
- Europe (ETS 300-328, ETS 300-339):
  - Frequency band: 2400-2483.5 MHz
  - At least 20 hopping channels
  - At most 100 mW EIRP
- Japan (RCR STD-33A):
  - Frequency band: 2471-2497 MHz
  - At least 10 hopping channels

802.11 FH PHY vs. Regulations

- 1 MHz Bandwidth
- 79 hopping channels in North America and Europe; pseudorandom hopping pattern. (2.402-2.480GHz)
- 23 hopping channels in Japan. (2.473-2.495GHz)
- At most 1 W power; devices capable of more than 100 mW have to support at least one power level not exceeding 100 mW.

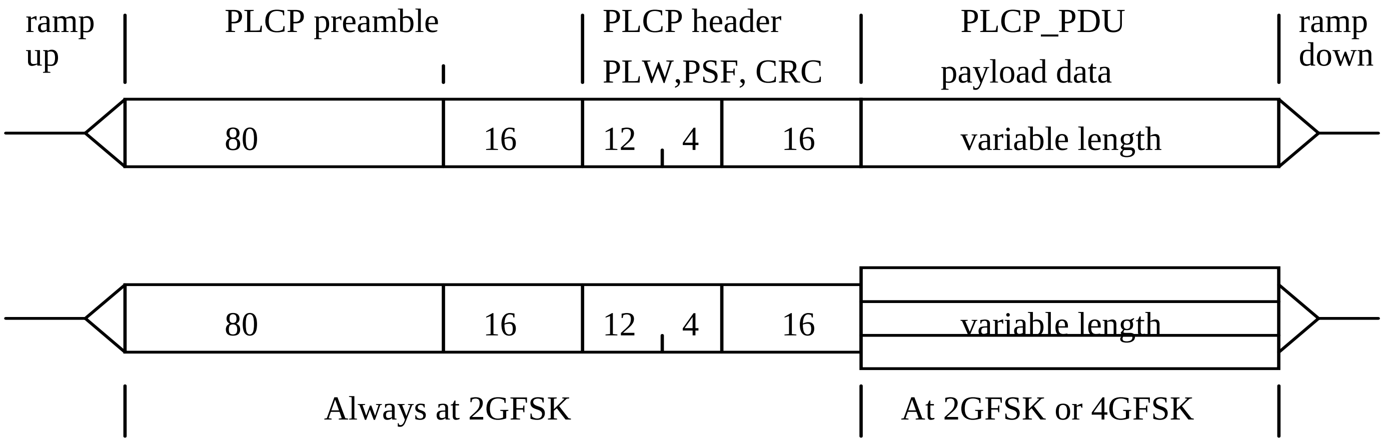
802.11 FHSS Modulation Objectives

- Achieving at least 1 Mbit/sec rate
- Familiar, field proven, low cost technology - FSK
  - Constant Envelope- Saturated Amplifiers
  - Limiter-Discriminator detection
- Multichannel operation transmit signal shaping to reduce adjacent channel interference

802.11 FHSS Modulation

- **Gaussian shaped FSK** (GFSK) at F_{clk} = 1 Msymbol/sec
  - NRZ data is filtered with BT=0.5 low-pass Gaussian filter (500 KHz bandwidth at 3 dB) and then FM modulates a carrier
- 1 or 2 Mbit/sec with multilevel GFSK
  - 1 Mbit/sec: 2 level GFSK h_2=0.34
  - 2 Mbit/sec: 4 level GFSK h_4=0.45h_2=0.15
- 1 Mbit/sec operation mandatory; 2 Mbit/sec-optional
  - facilitates production of interoperable lower-rate/lower-cost and higher-rate/higher-cost equipment

802.11 FHSS Frame Format



- **PHY header indicates payload rate and length; CRC16 protected**
- **Data is whitened by a synchronous scrambler and formatted to limit DC offset variations**
- **Preamble and Header always at 1 Mbit/sec; Data at 1 or 2 Mbit/sec**

PLCP Preamble

- PLCP preamble starts with 80 bits
  - 0101 sync pattern
  - detect presence of signal
  - to resolve antenna diversity
  - to acquire symbol timing
- Follows 16 bit Start Frame Delimiter (SFD)
  - h0CBD
  - the SFD provides symbol-level frame synchronization
  - the SFD pattern is balanced

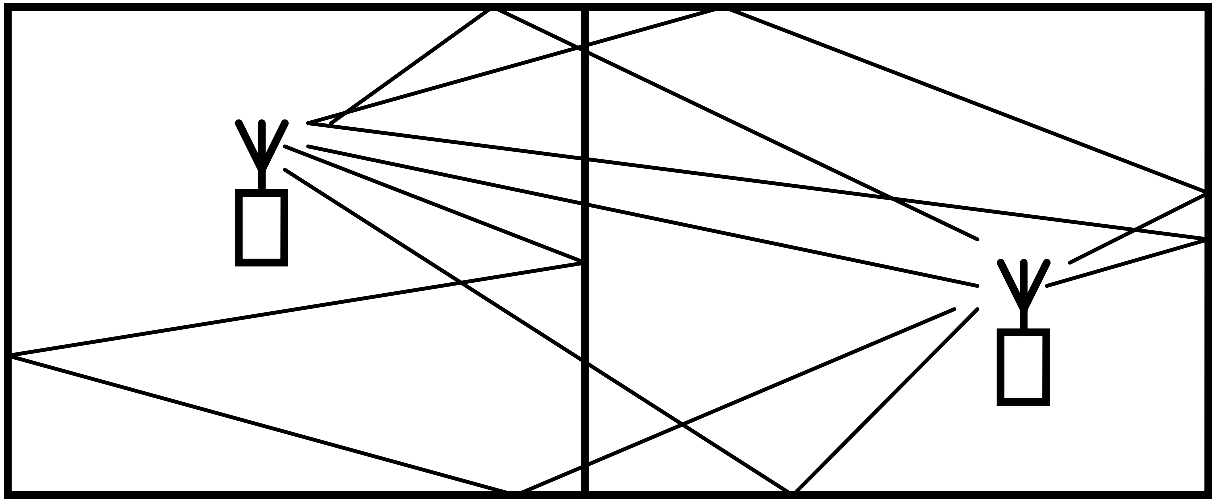
PLCP Header

- A 32 bit PLCP header consists of
  - PLW (PLCP_PDU Length Word) is 12 bit field
    - » indicating the length of PLCP_PDU in octets, including the 32 bit CRC at the PLCP_PDU end, in the range 0 .. 4095 (the same as IEEE 802.11a)
  - PSF (PLCP Signaling Field) is 4 bit field,
    - » Bits 0 is reserved
    - » Bit 1-3 indicates the PLCP_PDU data rate
      - (1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5 Mbit/s)
  - HEC is a 16 bit CRC

PLCP_PDU Formatting

- **Dividing serial bit stream into symbols:**
  - **at 1 Mbps, each bit is converted into 2FSK symbol**
  - **at 2 Mbps, each 2 bits are encoded into 4FSK symbol using Gray mapping**

Indoor Environment - Multipath Fading



- **Multiple propagation paths, interfering with each other, create a frequency selective fading.**
- **The fades are correlated at adjacent frequencies and get decorrelated after few megahertz in an indoor environment**

Frequency Hopping Sequences (1)

- **Design Criteria:**
  - **Assured minimum hop distance for multipath diversity performance (6 channels in North America and Europe, 5 channels in Japan)**
  - **Minimizing hits and adjacent channel hits between different hopping patterns**
  - **Minimizing consecutive hits between different hopping patterns**
- **FCC 15.247 requirement: Pseudorandomly ordered frequency list**

Frequency Hopping Sequences (2)

- Hop Sequence :
  - 1&2Mbps : hopping patterns are divided into three sets
    - » 26 sequences per set for North America and Europe
    - » 4 sequences per set for Japan
  - High rate (channel agility in 802.11b): hopping patterns are divided into two sets
    - » first set uses non-overlapping frequency channels
      - minimize interference degradation
      - 25/30MHz center frequency spacing for North America/Europe
      - 3 sequences per set for North America and Europe
    - » second set uses half overlapping frequency channels
      - 10MHz center frequency spacing
      - 6/7 sequences per set for North America/Europe
      - interoperability with 1&2Mbps FH systems

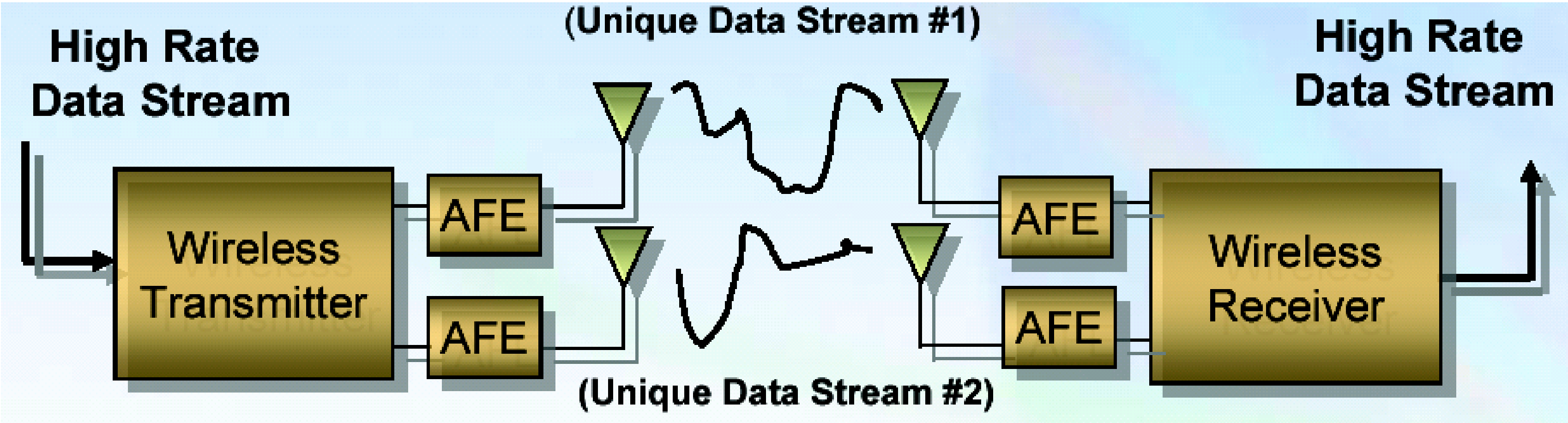
7. IEEE 802.11n Next Generation WLAN

IEEE 802.11n

- Next Generation Wireless LAN expectations
  - Over 100Mbps
  - Maybe standardized in 2007-2008
- Increasing channel size
  - Spectrally - Wider bandwidth channels
    - 40MHz per channel (vs. 20MHz)
  - Spatially - MIMO Smart Antenna spatial streams
- Improving channel utilization
- Industry activities

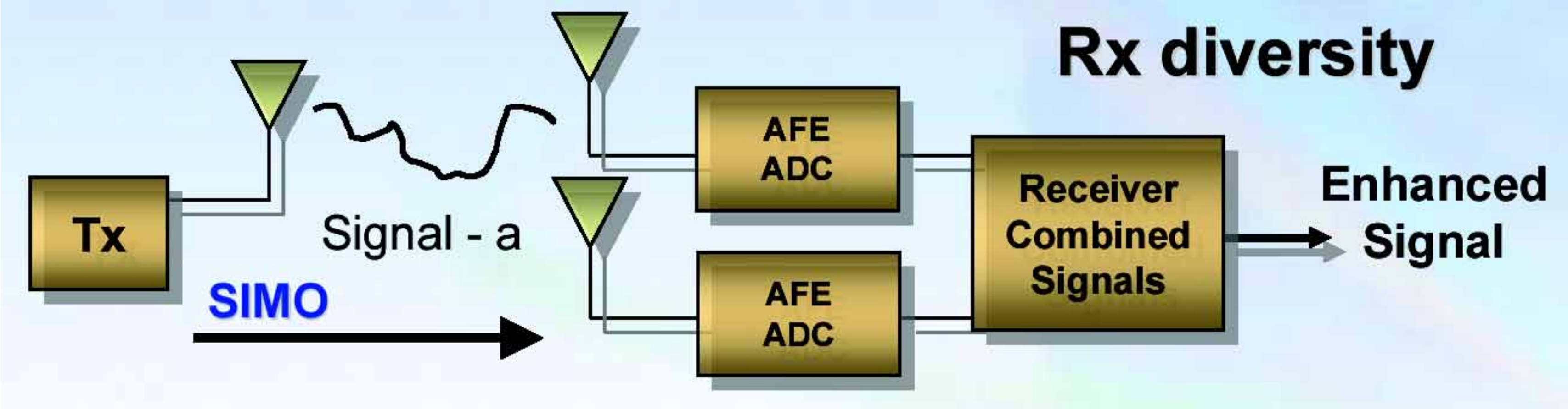
MIMO - Smart Antenna Multiplexing

- Use **multiple antennas** to digitally process multiple signals
- Distinct spatial streams simultaneously transfer unique data
- **Theoretical performance increases linearly with number of antennas**



Smart Antenna - Spatial Diversity

- Digital Maximal Ratio Combining (MRC)
- Signals coherently combined (unlike noise) to improve signal gain
- Diversity can incrementally enhance spatial multiplexing and wider bandwidth channels
- Spatial differences between antennas enable recombining



MRC can improve range up to 1.4 times

100 Mbps Implementation Comparisons

$(108*54/48)\times 2=243$

	4x4 MIMO @ 20 MHz Ch	2X2 MIMO @ 40 MHz Ch
Peak Rate to meet 100Mb	216 Mbps OTA, requires 4 non-correlated streams	243 Mbps OTA (Over the Air) (108 tones)
Range	Longer, 1x4 @ 6 Mbps	Shorter, 1x2 @ 13.5 Mbps
RF Cost	Higher, 4 x RF chains	Lower, 2 x RF chains
Digital Cost	Higher, 4 digital filters	Lower, 2 digital filters but 128 vs. 64 point FFT
Coexistence	Simple, RTS.CTS, i.e.11g	Challenge, support 20 & 40
Freq. reuse	U-NII, 7 freq. reuse	U-NII, 3-4 freq. reuse
Future	Limited, FF & complexity	Path beyond 100 Mbps @ MAC SAP (200Mbps)

7. IEEE 802.11 Wireless LAN MAC Standard

Wireless LAN Architecture

- **Major differences between Wireless LAN and Wired LANs:**
  - **Destination Address Does not Equal Destination Location.**
    - » **In wired LANs an address is equivalent to a physical address. In 802.11 the addressable unit is a station (STA). The STA is a message destination, but not a fixed location.**
  - **The Media Impacts the Design**
    - » **The PHY layers used in 802.11 are fundamentally different from wired media. 802.11 PHYs:**
      - **Have limited physical point to point connection ranges.**
      - **Use a medium shared.**
      - **Are unprotected from outside signals.**
      - **Are significantly less reliable than wired PHYs.**
      - **Have dynamic topologies.**

Wireless LAN Architecture

- Impact of Handling Mobile Stations
  - A portable station is one that is moved from location to location, but is only used while at a fixed location.
  - Mobile stations actually access the LAN while in motion.
  - Propagation effects blur the distinction between portable and mobile stations.
- Interaction With Other 802 Layers
  - 802.11 is required to appear to higher layers (LLC) as a current 802 style LAN. Station mobility has to be handled within the MAC layer.

802.11 Wirelss LAN Characteristics

- **1, 2, 5.5, 11, 22, 33, 6, 9, 12, 18, 24, 36, 48, 54 Mbps**
- **IEEE 802.11 CSMA/CA Frame**
- **Transmission Medium: Radio**
- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) Protocol**
  - **Provides priority scheme**
- **Provides delay guaranteed transmission service. CSMA/CA avoids most of the collisions so that the transmission delay can be guaranteed.**
- **Bandwidth Fairness is not guaranteed. By employing the CSMA/CA protocol, the bandwidth employed by each station may be different.**
  - Needs load sharing scheme in the near future ?

802.11 Wirelss LAN Characteristics

- **Changes and additions to IEEE Std. 802.11-1999:**

- **(1). IEEE Std 802.11a-1999--High-speed Physical Layer Extension in the 5 GHz Band:**
  - **Frequency range: 5.15-5.25, 5.25-5.35, and 5.725-5.825 GHz.**
  - **System: orthogonal frequency division multiplexing (OFDM).**
  - **Data payload communication capability: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.**

- **(2). IEEE Std 802.11b-1999--High-speed Physical Layer Extension in the 2.4 GHz Band:**
  - **Frequency range: 2.4 - 2.4835 GHz.**
  - **System: Direct Sequence Spread Spectrum (DSSS).**
  - **Data payload communication capability: 1, 2, 5.5, and 11Mbps.**

802.11 Wirelss LAN Characteristics

- (3). IEEE Std 802.11g-2003—Further Higher-Speed Physical Layer Extension in the 2.4GHz Band
  - Frequency range: 2.4 GHz.
  - System: hybrid DSSS and OFDM.
  - Data payload communication capability: 22, 33 / 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
- (4). IEEE Std 802.11e-2003—Medium Access Control (MAC) Enhancements for Quality of Services (QoS)
- (5). IEEE Std 802.11i-2003—Enhanced Security
  - WEP
  - TKIP
  - WRAP
  - CCMP

802.11 Architecture Components

- **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 Services (SS):**
  - The set of services that support transport of MSDUs (MAC Service Data Units) between Stations within a BSS.
- **Basic Service Set (BSS):**
  - A set of STAs controlled by a single CF (Co-ordination Function).
  - The BSS is the basic building block of an 802.11 LAN. The members of a BSS can communicate to each other directly.
  - If a station moves out of it's BSS coverage area, it can no longer directly communicate with other members of the BSS.
- **The Independent BSS as an Ad-Hoc Network**
  - This mode of operation is possible when 802.11 LAN stations are close enough to form a direct connection (without pre-planning).

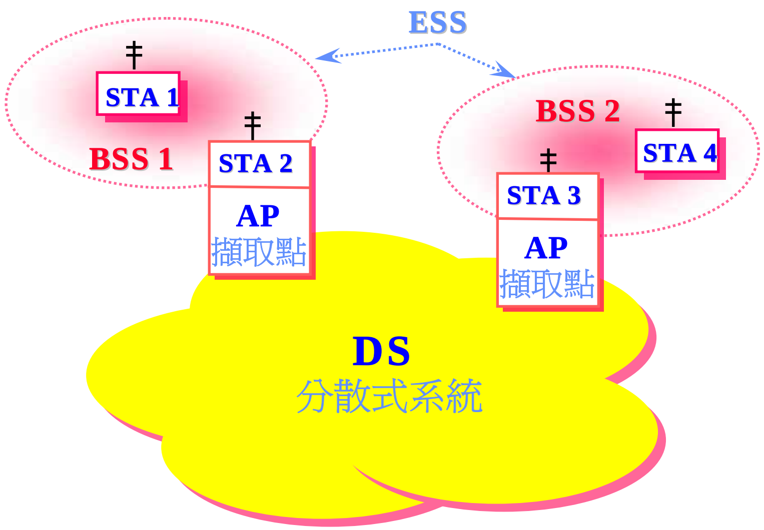
802.11 Architecture Components

- **Distribution System (DS):**
  - **A system used to interconnect a set of BSSs to create an ESS.**
  - **Used in Infrastructure Network**

- **Distribution System Medium (DSM):**
  - **The medium used by a DS (for BSS interconnections)**
  - **802.11 logically separates the WM from the DSM. Each logical medium is used for different purposes, by a different component of the architecture.**
  - **The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.**

802.11 Architecture Components

- **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.
  - figure



802.11 Architecture Components

- **STA to AP Association is Dynamic**
  - **The association between a station and a BSS is dynamic (STAs turn on, turn off, come within range and go out of range).**
  - **To become a member of an infrastructure BSS a station must become Associated.**

- **Distributed System Concepts:**
  - **Extend an 802.11 network with multiple BSSs named as ESS.**
  - **The architecture component used to interconnect BSSs is the Distributed System.**

802.11 Architecture Components

- **ESS: The large coverage network**
  - **The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity.**

- **Extended Service Set (ESS):**
  - **A set of interconnected BSSs which appears as a single BSS.**
  - **The ESS network appears the same to an LLC layer as an independent BSS network.**
  - **Stations within an ESS can communicate and mobile stations may move from one BSS to another (within the same ESS) transparently to LLC.**

- **Basic Service Area (BSA):**
  - **The area within which members of a BSS can communicate.**

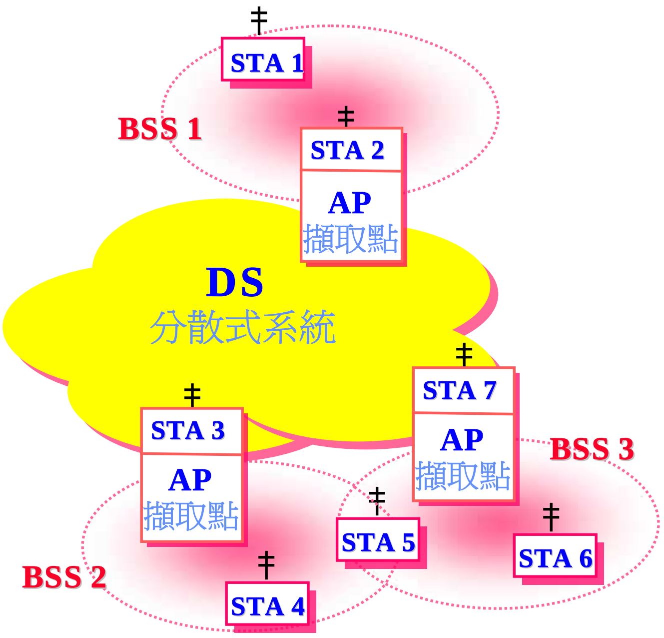
- **Extended Service Area (ESA):**
  - **The area within which members of a ESS can communicate. An ESA is larger than or equal to a BSA.**

802.11 Architecture Components

- The following are possible
  - The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.
  - The BSSs could be physically disjoint.
  - The BSSs may be physically collocated.
    This might be done to provide redundancy.

- Max number of overlapping BSSs
  - 3 in DSSS 2.4GHz
  - 26 in FHSS 2.4GHz
  - 12 in OFDM 5GHz

- **Question : Is it possible for a single BSS to utilizes multiple channels ?**

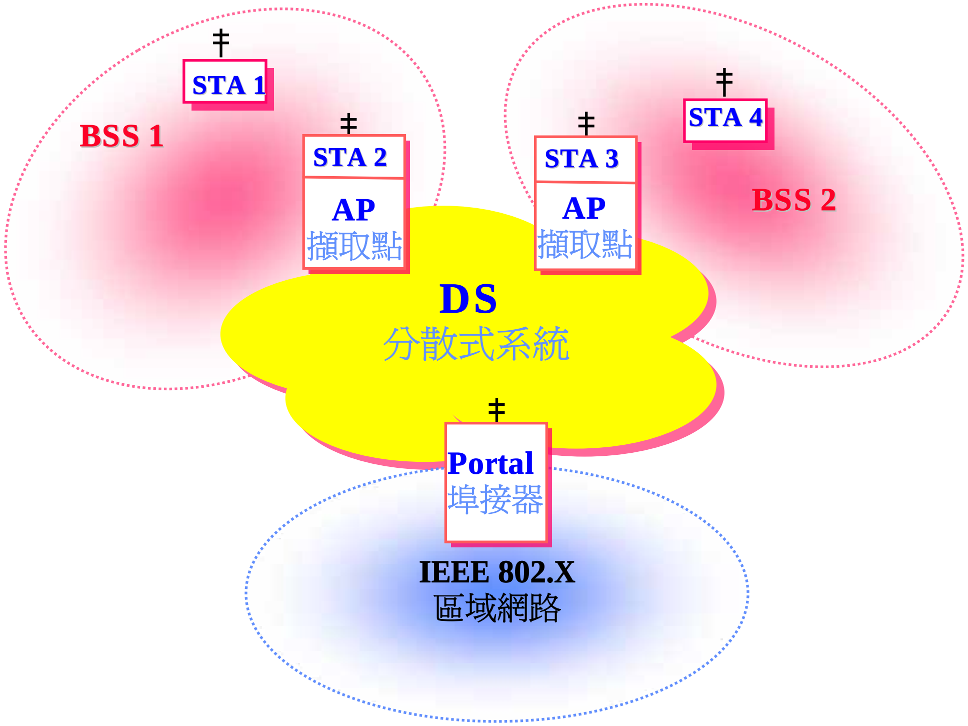


802.11 Architecture Components

– One (or more) independent BSS, or ESS networks may be physically present in the same space as one (or more) ESS networks.
  - » An ad-hoc network is operating in a location which also has an ESS network.
  - » Physically adjacent 802.11 networks have been set up by different organizations.

Integration with Wired LANs

- **To integrate the 802.11 architecture with a traditional wired LAN, a logical architecture component (Portal) is introduced.**
- **All data from non-802.11 LANs enters the 802.11 architecture via a portal.**



Portals and Bridges

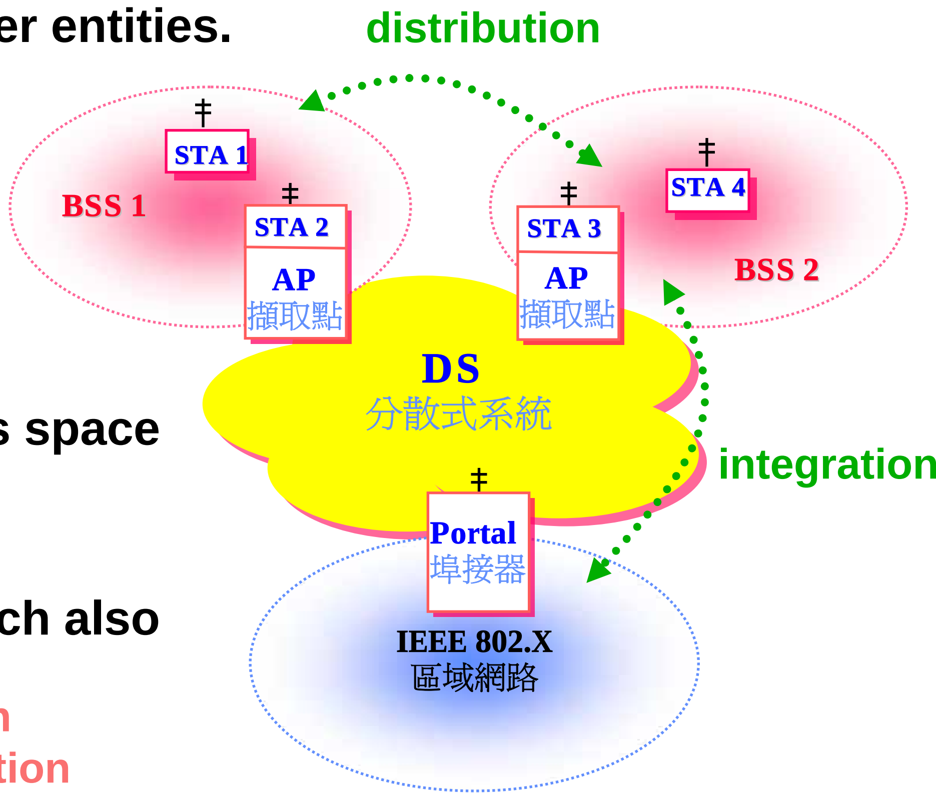
- Bridges were originally designed to provide range extension between like-type MAC layers.
- In 802.11, arbitrary range (coverage) is provided by the ESS architecture (via the DS and APs) making the PHY range extension aspects of bridges unnecessary.
- Bridges are also used to interconnect MAC layers of different types. Bridging to the 802.11 architecture raises the questions of which logical medium to bridge to; the DSM or the WM ?
- The portal must also consider the dynamic membership of BSSs and the mapping of address and location required by mobility.
- Physically, a portal may, or may not, include bridging functionality depending on the physical implementation of the DS.

Logical Service Interface

- The DS may not be identical to an existing wired LAN and can be created from many different technologies including current 802.x wired LANs.
- 802.11 does not constrain the DS to be either Data Link or Network Layer based. Nor constrain a DS to be either centralized or distributed.
- 802.11 specifies services instead of specific DS implementations. Two categories of services are defined: Station Service (SS) and Distribution System Service (DSS).
- The complete set of 802.11 architectural services are:
  1. Authentication
  2. Association
  3. Disassociation
  4. Distribution
  5. Integration
  6. Reassociation
  7. Deauthentication
  8. Privacy
  9. MSDU delivery

Logical Service Interface

- **Station Service (SS):**
  - Present in every 802.11 station, including APs.
  - Are specified for use by MAC layer entities.
  - The SS subset is:
    - » Authentication
    - » Deauthentication
    - » Privacy
    - » MSDU delivery
- **Distribution System Services**
  - Used to cross media and address space logical boundaries.
  - Provided by the DS.
  - They are accessed via a STA which also provides DSS.
  - The DSS subset is:
    - »Association
    - »Disassociation
    - »Distribution
    - »Integration
    - »Reassociation



Multiple Logical Address Spaces

- **The WM, DSM, and an integrated wired LAN may all be different physical media. Each of these components may be operating within different address spaces.**
- **802.11 only uses and specifies the use of WM address space.**
- **Each 802.11 PHY operates in a single medium: WM.**
- **802.11 has chosen to use the IEEE 802 48-bit address space.**
- **A multiple address space example is one where DS uses network layer addressing. In this case the WM address space and the DS address space would be different.**

Overview of the Services

- There are nine services specified by 802.11. Six to support MSDU delivery between stations, and three to control 802.11 access and confidentiality.
- Each of the services is supported by one or more MAC frames.
- Some of the services are supported by MAC Management messages and some by MAC Data messages.
- 802.11 MAC layer uses three types of messages:
  - Data : handled via the MAC data service path.
  - Management: handled via the MAC Management Service data path.
  - Control
- The following examples assume an ESS network environment.

Distribution of Message Within a DS

- Distribution:
  - The service which (by using Association information) delivers MSDUs within the DS.
- Consider a data message being sent from STA1 to STA4 via STA2 (Input AP) and STA3 (Output AP). The input AP gives the message to the Distribution Service of the DS.
- How the message is delivered within the DS is not specified by 802.11.
- All 802.11 is required is to provide the DS with enough information for the DS to be able to determine the "output" point which corresponds to the desired recipient. The necessary information is provided to the DS by the three Association related services.
  - Association
  - Reassociation
  - Disassociation

Distribution of Message Within a DS

- **Integration:**
  - **The service which enables delivery of MSDUs between the DS and an existing network.**
- **If the Distribution Service determines that the intended recipient of a message is a member of an integrated LAN, the "output" point would be a Portal instead of an AP.**
- **Messages which are distributed to a Portal cause the DS to invoke the Integration service (conceptually after the Distribution Service).**
- **The Integration service is responsible for accomplishing whatever is needed to deliver a message from the DSM to the integrated LAN media, including any required media or address translation.**

Distribution Services (1/4)

- The information required for the Distribution service to operate is provided by the Association services.
- Before a data message can be handled by the Distribution service, a STA must be "Associated".
- Mobility types:
  - No-transition
    - » Static - no motion
    - » Local movement - movement within a Basic Service Area
  - BSS-transition: movement from one BSS in one ESS to another BSS within the same ESS.
  - ESS-transition: movement from one BSS in one ESS to another BSS in an independent ESS.
- Different Association services support the different categories of mobility.

Distribution Services (2/4)

- **Association**:
  - The service which establishes an initial Association between a station and an access point.
- Before a STA is allowed to send via an AP, it must first become associated with the AP.
- At any given time, a mobile STA may be associated with no more than one AP. This ensures that the DS can determine which AP is serving a specified STA.
- An AP may be associated with many mobile STAs at one time.
- A station learns what APs are present and requests to establish an association by invoking the Association service.
- Association is always initiated by the mobile STA.
- Association is sufficient to support no-transition mobility.
- Association is necessary, but not sufficient, to support BSS-transition mobility.

Distribution Services (3/4)

- **Reassociation:**
  - **The service which enables an established Association (of a STA) to be transferred from one AP to another AP (within an ESS).**
- **The Reassociation Service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS.**
- **Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP.**
- **Reassociation is always initiated by the mobile STA.**

Distribution Services (4/4)

- **Disassociation**:
  - The service which deletes an existing Association.
- The Disassociation Service is invoked whenever an existing Association must be terminated, and can be invoked by either party to an Association (mobile STA or AP).
- Disassociation is a notification (not a request) and can not be refused by either party to the association.
- APs might need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.
- STAs are encouraged to Disassociate whenever they leave a network.

Access and Confidentiality Control Services (1/2)

- Wired LAN design assume the closed, non-shared nature of wired media. The open, shared medium nature of an 802.11 LAN violates those assumptions.
- Two services are required for 802.11 to provide functionality equivalent to that which is inherent to wired LANs.
  - Authentication : used instead of the wired media physical connection.
    - » Now be further enhanced with IEEE 802.1x port-based authentication
  - Privacy : used to provide the confidential aspects of closed wired media.
    - » Now be further extended IEEE 802.11i enhanced sceurity
- Authentication:
  - The service used to establish the identity of Stations to each other.

Access and Confidentiality Control Services (2/2)

- **In a wired LAN, access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN.**
- **An equivalent ability to control LAN access is provided via the Authentication service, which is used by all stations to establish their identity with stations they wish to communicate with.**
- **If a mutually acceptable level of authentication has <u>not</u> been established between two stations, an association shall not be established.**

Authentication Service

- 802.11 supports a general authentication ability which is sufficient to handle authentication protocols ranging from unsecured to public key cryptographic authentication schemes. (OPEN system and Shared Key)
- 802.11 provides link level (not end-to-end or user-to-user) authentication between 802.11 stations.
- 802.11 authentication is simply used to bring the wireless link up to the assumed physical standards of a wired link. If desired, an 802.11 network can be run without authentication.
- 802.11 provides support for challenge/response (C/R) authentication. The three steps of a C/R exchange are:
  - Assertion of identity
  - Challenge of Assertion
  - Response to Challenge

Authentication Service

- Examples of a C/R exchange are:
- An open system example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Null.
  - (c) Response: Null.
  - (d) Result: Station becomes Authenticated.
- A password based example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Prove your identity.
  - (c) Response: Here is my password.
  - (d) Result: If password OK, station becomes Authenticated.
- A Cryptographic challenge/response based example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Here is some information (X) I encrypted with your public key, what is it ?
  - (c) Response: The contents of the challenge is X (only station 4's private key could have recovered the challenge contents).
  - (d) Result: OK, I believe that you are station 4.

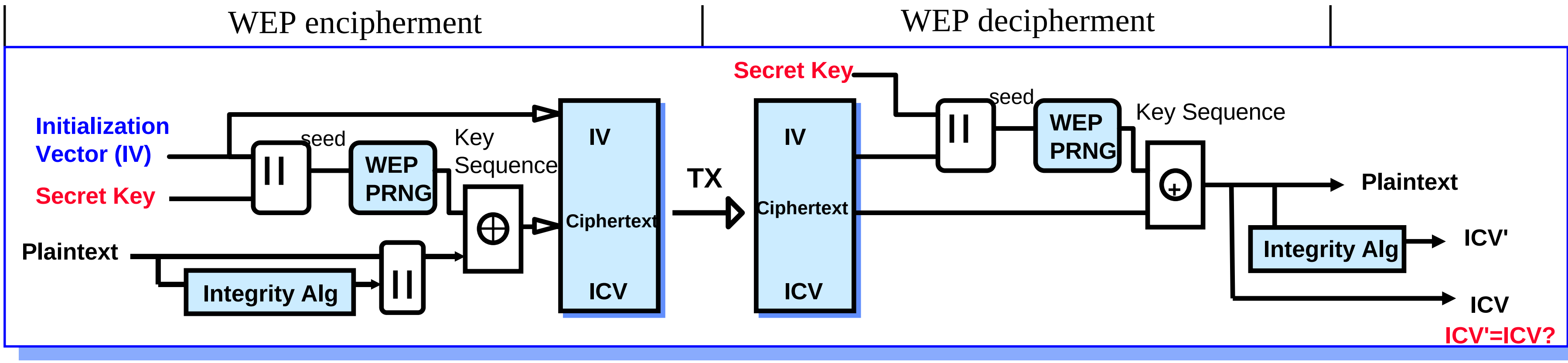
Authentication Service

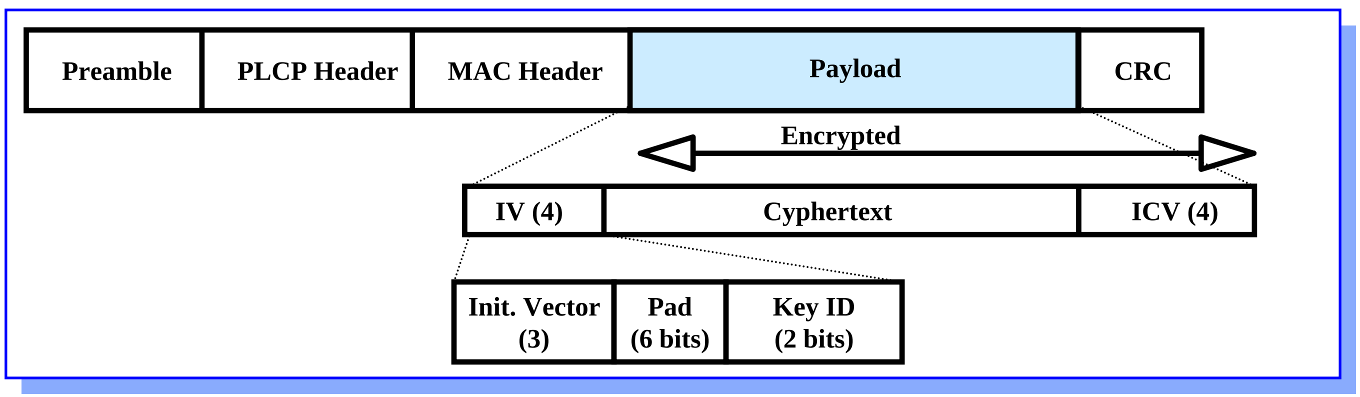
- 802.11 uses 802.10 services to perform the actual challenge and response calculations. A Management Information Base (MIB) function is provided to support inquires into the authentication algorithms supported by a STA.
- 802.11 requires mutually acceptable, successful, bi-directional authentication.
- A STA can be authenticated with many other STAs (and hence APs) at any given instant.
- The Authentication service (could be time consuming) can be invoked independently of the Association service.
- Pre-authentication is typically done by a STA while it is already associated with an AP which it previously authenticated with.
- 802.11 does not require that STAs pre- authenticate with APs.
- However, Authentication is required before an Association can be established. Thus, pre-authentication can speedup the reassociation process.

Privacy and Access Control

- Goal of 802.11 is to provide Wired Equivalent Privacy (WEP)
  - Usable worldwide
- 802.11 provides for an Authentication mechanism
  - To aid in access control.
  - Has provisions for OPEN Shared Key or proprietary authentication extensions.
- Optional (WEP) Privacy mechanism defined by 802.11.
  - Limited for Station-to-Station traffic, so not "end to end".
    - » Embedded in the MAC entity.
  - Only implements Confidentiality function.
  - Uses RC4 PRNG algorithm based on:
    - » a 40-bit secret key (No Key distribution standardized)
      - by external key management service
    - » and a 24-bit IV that is send with the data.
    - » 40+24 = 64-bit PRNG seed (new 128, 152 bits - performane)
    - » includes an ICV to allow integrity check.
  - Only payload of Data frames are encrypted.
    - » Encryption on per MPDU basis.

Privacy Mechanism





- **WEP bit** in Frame Control Field indicates WEP used.
  - Each frame can have a new IV, or IV can be reused for a limited time.
  - If integrity check fails then frame is ACKed but discarded.

Privacy Service (1/2)

- **Privacy**:
  - The service used to prevent the contents of messages from being reading by other than the intended recipient.
- In a wired LAN only those stations physically connected to the wire can hear LAN traffic. This is not true for the 802.11 wireless LAN.
- 802.11 provides the ability to encrypt the contents of messages.
- IEEE 802.10 SDE clause 2 is used to perform the encryption. A MIB function is provided to inquire the encryption algorithms supported by a station.
- A mutually acceptable privacy algorithm must be agreed upon before an Association can be established.

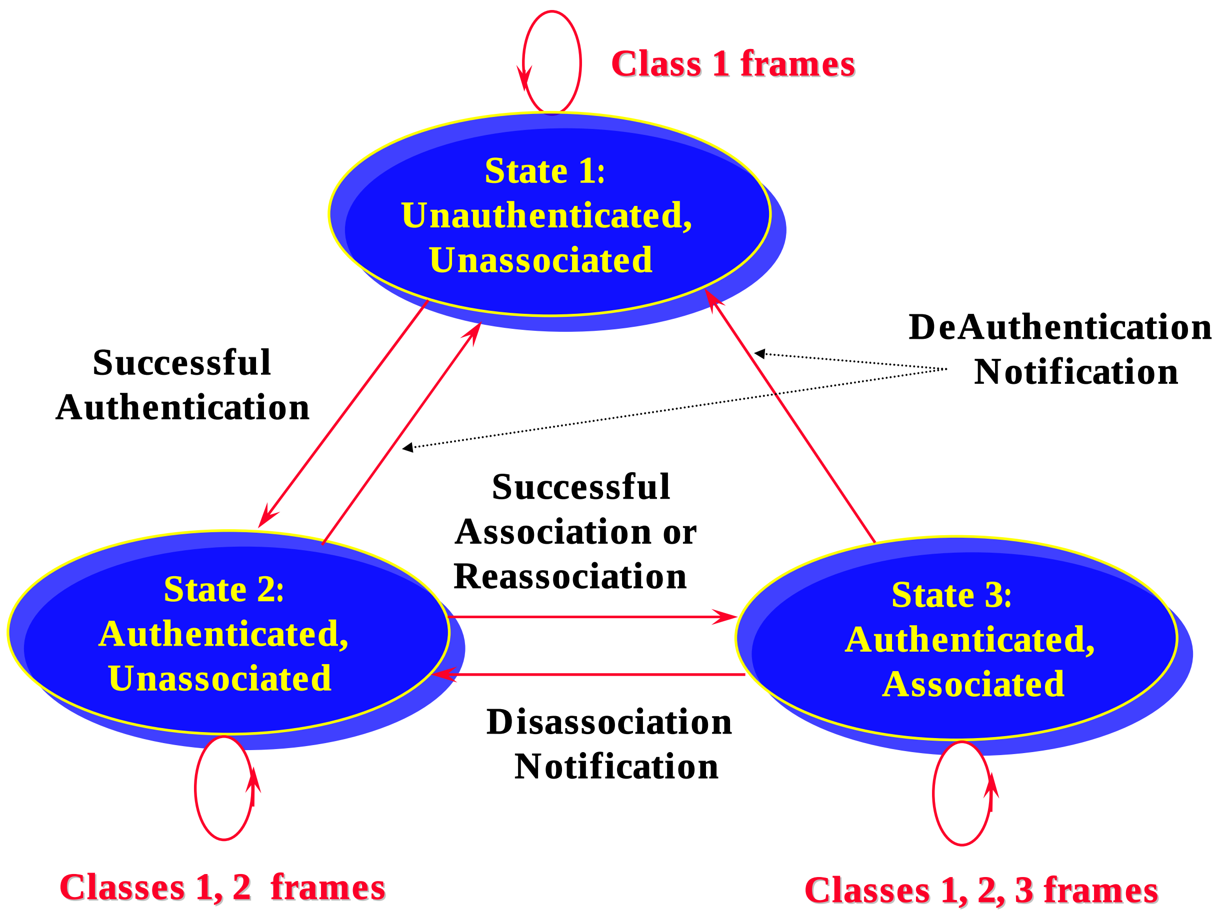
Privacy Service (2/2)

- The default privacy algorithm for all 802.11 stations is <u>in the clear.</u> If the privacy service is not invoked to set up a privacy algorithm, all messages will be sent unencrypted.
- If a privacy algorithm is set up, then the algorithm will be used for all subsequent transmissions.
- Even if an Association is successful, a later Reassociation may be refused.
- 802.11 specifies an optional privacy algorithm that is designed to satisfy the goal of wired LAN "equivalent" privacy.

Relationship Between Services

- For a station, two state variables are required to keep track:
  - Authentication State : Unauthenticated and Authenticated
  - Association State : Unassociated and Associated
- Three station states are possible:
  - State 1 : Initial start state, Unauthenticated, Unassociated.
  - State 2 : Authenticated, not Associated.
  - State 3 : Authenticated and Associated
- These states determine the 802.11 frame types (grouped into classes) which may be sent by a station.
  - State 1 : Only Class 1 frames are allowed.
  - State 2 : Either Class1 or Class 2 are allowed.
  - State 3 : All frames (Class 3) are allowed.

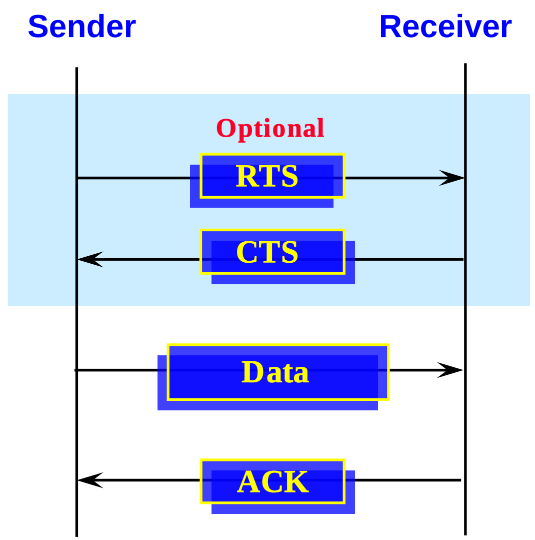
Relationship Between State Variables and Services



Frame Types

- Class 1 frames
  - Control Frames
    - (1) RTS
    - (2) CTS
    - (3) ACK
    - (4) CF-End+ACK
    - (5) CF-End
  - Management Frames
    - (1) Probe Request/Response
    - (2) Beacon
    - (3) Authentication
      - » Successful association enables Class 2 frames.
      - » Unsuccessful association leaves STA in State 1.
    - (4) Deauthentication

      Return State 1.
    - (5) Announcement traffic indication message (ATIM)
  - Data Frames
    - (1) In IBSS, direct data frames only (FC control bits "To DS and from DS" both false)



Frame Types

- **Class 2 Frames**
  - **Data Frames**

    (1) Asynchronous data. Direct data frames only (FC control bits "To DS and from DS" both false)
  - **Management Frames**

    (1) Association Request/Response
      - » **Successful association enables Class 3 frames.**
      - » **Unsuccessful association leaves STA in State 2.**

    (2) Reassociation request/response
      - » **Successful association enables Class 3 frames.**
      - » **Unsuccessful association leaves STA in State 2.**

    (3) Disassociation

    Return State 2.

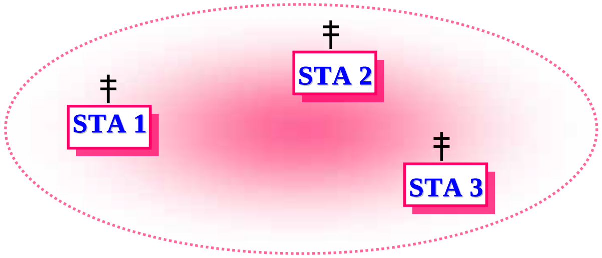
PS. When STA A receives a non-authenticated frame from STA B, STA A sends a deauthentication to STA B

Frame Types

- Class 3 Frames
  - Data Frames
    (1) Asynchronous data. Indirect data frames allowed (FC control bits "To DS and from DS" may be set to utilize DS Services)
  - Management Frames
    (1) Deauthentication
      » Return state 1
  - Control Frames
    (1) PS-Poll

Differences Between ESS and Independent BSS LANs

- An independent BSS (IBSS) is often used to support an "Ad-Hoc" network, in which a STA communicates directly with one or more other STAs.
- IBSS is a logical subset of an ESS and consists of STAs which are directly connected.
- Since there is no physical DS, there cannot be a Portal, an integrated wired LAN, or the DS Services.
- In an IBSS, only class 1 frames are allowed since there is no DS in an IBSS.
- The services which apply to an IBSS are the Station Services.



IBSS

Frame and MPDU Formats

- Each frame should consist of three basic components:
  - A MAC Header, which includes control information, addressing, sequencing fragmentation identification, duration and QoS information.
  - A variable length Frame Body, which contains information specify to the frame type.
  - A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

Frame Formats

Octets:

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order / rsrv

Frame Control Field

- MAC Header format differs per Type:
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames
- Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.

Address Field Description

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- **Addr 1 = All stations filter on this address.**
- **Addr 2 = Transmitter Address (TA)**
  - **Identifies transmitter to address the ACK frame to.**
- **Addr 3 = Dependent on *To* and *From DS* bits.**
- **Addr 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames.**
  - **BSSID**
    - **infrastructure : AP MAC address**
    - **Ad Hoc : 01 + 46-bit random number (may set as ‘1’)**

Frame Fields

- Frame Control Field :
  - Protocol Version: the value of the protocol version is zero.

    A device that receives a frame with a higher revision level than it supports will discard the frame without indication to the sending STA or to LLC.
  - Type and Subtype: used to identify the function of the frame.
  - To DS: is set to 1 in data type frames destined for the DS via AP.
  - From DS: is set to 1 in data type frames existing the DS.
  - More Fragment: is set to 1 if there has another fragment of the current MSDU or MMSDU.
  - Retry : Indicates that the frame is a retransmission of an earlier frame. A station may use this indication to eliminate duplicate frames.
  - Power Management : Indicates power management mode of a STA. A value of 1 indicates that the STA will be in power-save mode. A value of 0 indicates that the STA will be in active mode. This field is always set to 0 in frames transmitted by an AP.

Frame Fields

  - **More Data: is used to indicate to a STA in power-save mode that more MSDUs, or MMSDUs are buffered for that STA at the AP; or indicate that at least one additional MSDU buffered at STA available for transmission in response to a subsequent CF-Poll**
  - **WEP: It is set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm.**
  - **Order: is set to 1 in any data type frame that contains an MSDU, or fragment, which is being transferred using the Strictly Ordered service class.**
- **Duration or Connection ID : Used to distribute a value (us) that shall update the Network Allocation Vector (NAV) in stations receiving the frame.**

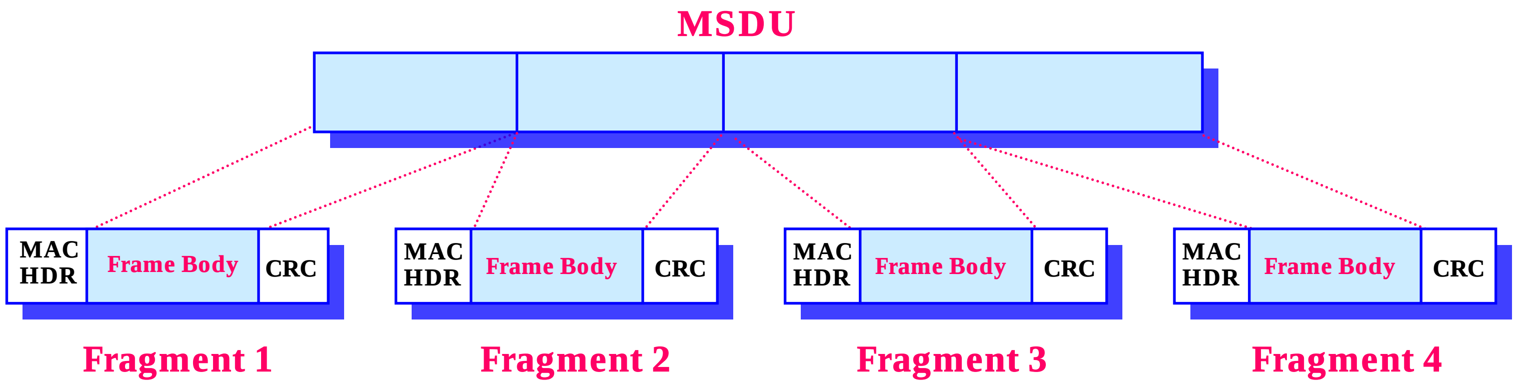
Duration/ID Field

- In PS-Poll control frame, Duration/ID carries association ID (AID) with the 2 MSB set as 1 (AID range 1-2007)
- other types carries duration in us.
- Transmitted frames in CFP, duration is set as 32768.

Bit 15	Bit 14	Bits 13-0	Usage
0	0-32767		Duration (us)
1	0	0	Fixed value within frames transmitted during the CFP
1	0	1-16383	Reserved
1	1	0	Reserved
1	1	1-2007	AID in PS-Poll frames
1	1	2008-16383	Reserved

Frame Fields

- **Address Fields : Indicate the BSSID, SA, DA, TA (Transmitter address), RA (Receiver address), each of 48-bit address.**
- **Sequence Control**
  - **Sequence Number (12-bit): An incrementing value. The same value shall be used for all fragments of the same MSDU.**
  - **Fragment Number (4-bit): Indicates the number of each individual fragment.**
- **Frame Body: 0 – 2312(2310) bytes.**
- **CRC (4 octets)**



Format of Individual Frame Types

- **Control Frames**
  - ***Immediately previous frame*** **means a frame, the reception of which concluded within the prior SIFS interval.**
- **RTS Frame Format**
  - **In an infrastructure LAN, the DA shall be the address of the AP with which the station is associated. In an ad hoc LAN, the DA shall be the destination of the subsequent data or management frame.**
- **CTS Frame Format**
  - **The DA shall be taken from the source address field of the RTS frame to which the CTS is a response.**
- **ACK Frame Format**
  - **The DA shall be the address contained in the Address 2 field of the immediately previous Data or Management frame.**
- **PS-Poll Frame Format**
  - **The BSS ID shall be the address of the AP. The AID shall be the value assigned by the AP in the Association Response frame. The AID value always has its two significant bits set to 1.**

Format of Individual Frame Types (control frames)

Bit : 7654
Subtype: 1011

MAC Header

Frame Control	Duration	RA	TA	FCS

RTS Frame

Subtype: 1100

MAC Header

Frame Control	Duration	RA	FCS

CTS Frame

Subtype: 1101

MAC Header

Frame Control	Duration	RA	FCS

ACK Frame

Subtype: 1010

MAC Header

Frame Control	AID	BSSID	TA	FCS

PS-Poll Frame

Format of Individual Frame Types (control frames)

Bit: 7654
Subtype:1110

MAC Header				
Frame Control	Duration	RA	BSSID	FCS

CF-End Frame

Subtype:1111

MAC Header				
Frame Control	Duration	RA	BSSID	FCS

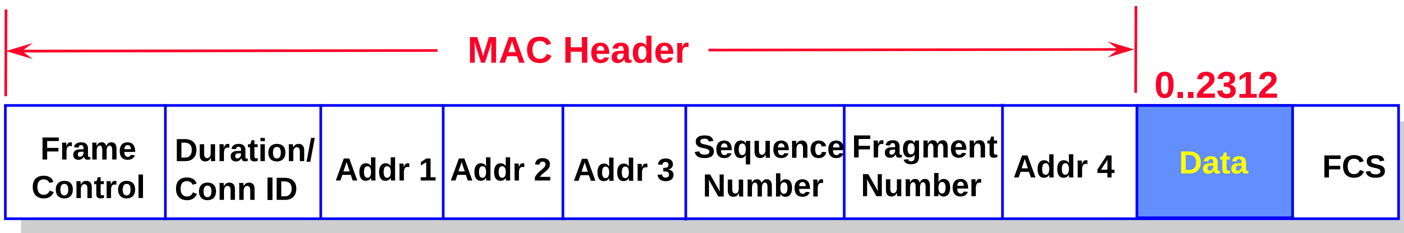
CF-End+CF-Ack Frame

- **The BSSID is the address of the STA contained in the AP.**
- **The RA is the broadcast group address.**
- **The Duration field is set to 0.**

Format of Individual Frame Types

- **Data Frames**
  - **The contents of the Address fields shall be dependent upon the values of the To DS and From DS bits.**
  - **A station shall use the contents of Address 1 to perform address matching for receive decisions.**
  - **The DA shall be the destination of the frame (MSDU).**
  - **The RA shall be the address of the AP in the wireless DS that is the next immediate intended recipient of the frame.**
  - **The TA shall be the address of the AP in the wireless DS that is transmitting the frame.**
  - **The BSSID**
    - **The AP address, if the station is an AP or associated with an AP.**
    - **The BSS ID of the ad hoc LAN, if the station is a member of an ad hoc LAN.**
  - **The frame body is null(0 octets in length) in data frames of subtype null function (no data), CF-Ack (no data), CF-Poll (no data), and CF-Ack+CF-Poll (no data).**

Data Frames



To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Frame Exchange Sequences

- **The following frame sequences are possible:**
  - **Data**
  - **Data - ACK**
  - **RTS - CTS - Data - ACK**
  - **Data - ACK - Data - ACK (Fragmented MSDU)**
  - **RTS - CTS - Data - ACK - Data - ACK (Fragmented MSDU)**
  - **Poll - Data - ACK**
  - **Poll - Data - ACK - Data - ACK (Fragmented MSDU)**
  - **Poll - ACK (No data)**
  - **ATIM – ACK**
  - **Request (management : Probe Request)**
  - **Request - ACK (management)**
  - **Response - ACK (management)**
  - **CTS - Data (11g)**
  - **CTS - Management (11g)**
  - **CTS - Data - ACK (11g)**
  - **CTS - Data - ACK - Data - ACK (Fragmented MSDU) (11g)**

Format of Individual Frame Types

- **Management Frames**
  - **The BSSID**
    - » **The AP address, if the station is an AP or associated with an AP.**
    - » **The BSS ID of the ad hoc LAN, if the station is a member of an ad hoc LAN.**
  - **The Frame body shall be the *information elements*:**

MAC Header							
Frame Control	Duration/ AID	DA	SA	BSSID	Sequence Control	Frame Body	CRC

Management Frames (Frame Body)

- **BEACON Frame**: Time stamp, beacon interval,Capability information, SSID, supported rates, FH Parameter Set, DS parameter Set, CF Parameter Set, IBSS Parameter Set, and TIM. (the parameter sets are present only when the functions are used)
  - In 802.11g, new "ERP Information Element" and "Extended Supported Rates Element"are added.
- **ATIM Frame**: Null
- **Disassociation Frame**: Reason code.
- **Association Request Frame**: Capability information, Listen Interval, SSID, and Supported Rates.
- **Association Response Frame**: Capability information, Status code, Association ID (AID), and the supported rates.
- **Reassociation Request Frame**: Capability information, Listen Interval, Current AP address, SSID, and Supported Rates.
- **Reassociation Response Frame**: Capability information. status code, Association ID (AID), and supported rates.
- **Deauthentication**: Reason code.

Management Frames (Frame Body)

- **Probe Request Frame**: **SSID and The supported rates.**
- **Probe Response Frame**: **Time stamp, beacon interval, capability information, supported rates, and parameter sets.**
  - » **Omit “TIM” field.**
  - » **In 802.11g, new “ERP Information Element” and “Extended Supported Rates Element”are added.**
- **Authentication Frame**: **Authentication algorithm number (0:Open system 1: Shared Key), Authentication transaction sequence number, Status code (if reserved, set to 0), and Challenge text.**

Authentication algorithm	Authentication Transaction sequence number	Status code	Challenge text
Open System	1	Reserved	Not present
Open System	2	Status	Not present
Shared Key	1	Reserved	Not present
Shared Key	2	Status	Present
Shared Key	3	Reserved	Present
Shared Key	4	Status	Not present

Capability Information field 1

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		
						802.11b				802.11g		802.11g		

- **APs** set the ESS subfiled to 1 and IBSS subfield to 0 within transmitted Beacon or Probe Response management frame.
- **STAs** within an IBSS set the ESS subfield to 0 and IBSS subfield to 1 in transmitted Beacon or Probe Response management frame.
- Bit 10 is used to indicate 9us slot time is used. (IEEE 802.11g)
- Bit 13 is used to indicate the new option of DSSS-OFDM. (IEEE 802.11g)

Capability Information field 2

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		

801.11g

- **STAs** set the CF-Pollable and CF-Poll Request subfields in **Association Request** and **Reassociation Request** management frames according to

CF-Pollable	CF-Poll request	Meaning
0	0	STA is not CF-Pollable
0	1	STA is CF-Pollable, not requesting to be placed on the CF-Polling list
1	0	STA is CF-Pollable, requesting to be placed on the CF-Polling list
1	1	STA is CF-Pollable, requesting never to be Polled

Capability Information field 3

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		

801.11g

- **APs** set the CF-Pollable and CF-Poll Request subfields in **Beacon**, **Probe Response** and **Association Response**, **Reassociation Response** management frames according to

CF-Pollable	CF-Poll request	Meaning
0	0	No point coordinator at AP
0	1	Point coordinator at AP for delivery only
1	0	Point coordinator at AP for delivery and polling
1	1	Reserved

Capability Information field 4

2 octets

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10		B13		B15
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility			Short Slot time	…	DSSS-OFDM		

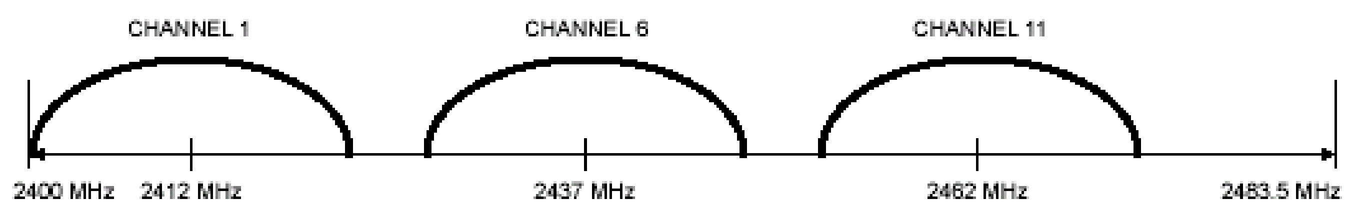
801.11g

- Optional frequency hopping for solve the shortcoming of static channel assignment in DSSS.
  - **Example : Tone jammer**
- Goal : without added cost
- Interoperability with 802.11 FHSS 1/2Mbps
  - Use same frequency hopping patterns
- (Ref. Page 121.)

Channel Agility (optional)

- Two Sets for frequency hopping patterns (**224us per hop**)
  - North American

Set	Number of Channels	HR/DSSS Channel Number
1	3	1,6,11
2	6	1,3,5,7,9,11



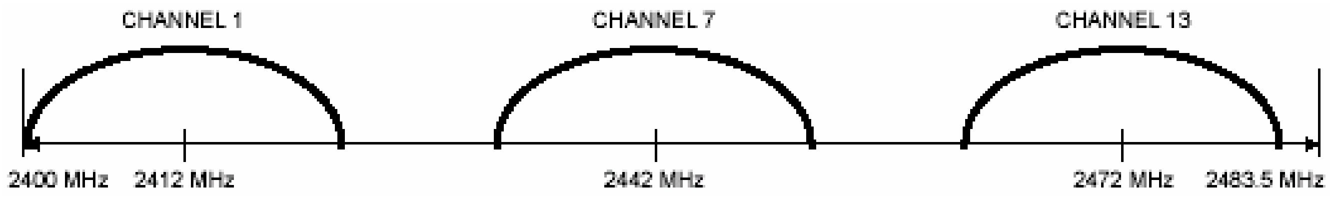
Non-overlapping Channels Selection (25MHz gap)

Half-overlapping Channels Selection (10MHz gap)

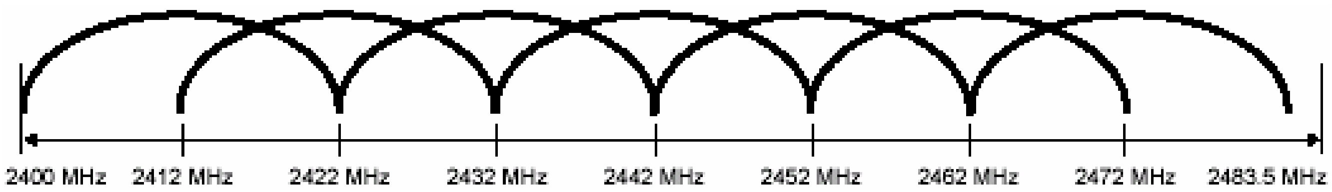
Channel Agility (optional)

- Two Sets for frequency hopping patterns
  - Europe (except Spain and France)

Set	Number of Channels	HR/DSSS Channel Number
1	3	1,7,13
2	7	1,3,5,7,9,11,13



Non-overlapping Channels Selection (30MHz gap)



Half-overlapping Channels Selection (10MHz gap)

Information Element

octets

1	1	length
Element ID	Length	Information

Information Element	Element ID
SSID	0
Supported rates	1
FH Parameter Set	2
DS Parameter Set	3
CF Parameter Set	4
TIM	5
IBSS Parameter Set	6
Country	7
Legacy Indication (11g)	8
Reserved	9-15
Challenge Text	16
Reserved for challenge text extension	17-31
Reserved	32-255

Elements

SSID

octets	1	1	0-32
	Element ID	Length	SSID

Supported Rate

octets	1	1	1-8
	Element ID	Length	Supported Rates

FH Parameter Set

octets	1	1	2	1	1	1
	Element ID	Length	Dwell time	Hop Set	Hop Pattern	Hop Index

DS Parameter Set

octets	1	1	1
	Element ID	Length	current channel

CF Parameter Set

octets	1	1	1	1	2	2
	Element ID	Length	CF Count	CF Period	CFP Maxduration	CFP DurRemaining

TIM

octets	1	1	1	1	1	1-251
	Element ID	Length	DTIM Count	DTIM Period	Bitmap Control	Partial Virtual Map

SSID Elements

SSID Indication

octets	1	1	0-32
	Element ID	Length	SSID

- indicates the identity of an ESS or IBSS
- a ‘0’ length information field indicates the broadcast SSID

Supported Rate Elements

802.11 (a, b only)

octets	1	1	1-8
	Element ID	Length=1	Supported rates

802.11g Extended supported rate

octets	1	1	1-255
	Element ID	Length=1	Extended Supported rates

- The number of supported rates is **14** (a/b/g).
- Each supported rate belonging to the BSSBasicRateSet is encoded as an octet with the msb (bit 7) set to 1
  - e.g., a 1 Mbit/s rate is encoded as X'82' (in 500kbps)
- Rates not belonging to the BSSBasicRateSet are encoded with the msb set to 0
  - e.g., a 2 Mbit/s rate is encoded as X'04'.

ERP Information Elements

NonERP Indication

octets	1	1				1				
	Element ID	Length=1	b0	b1	r	r	r	r	r	r

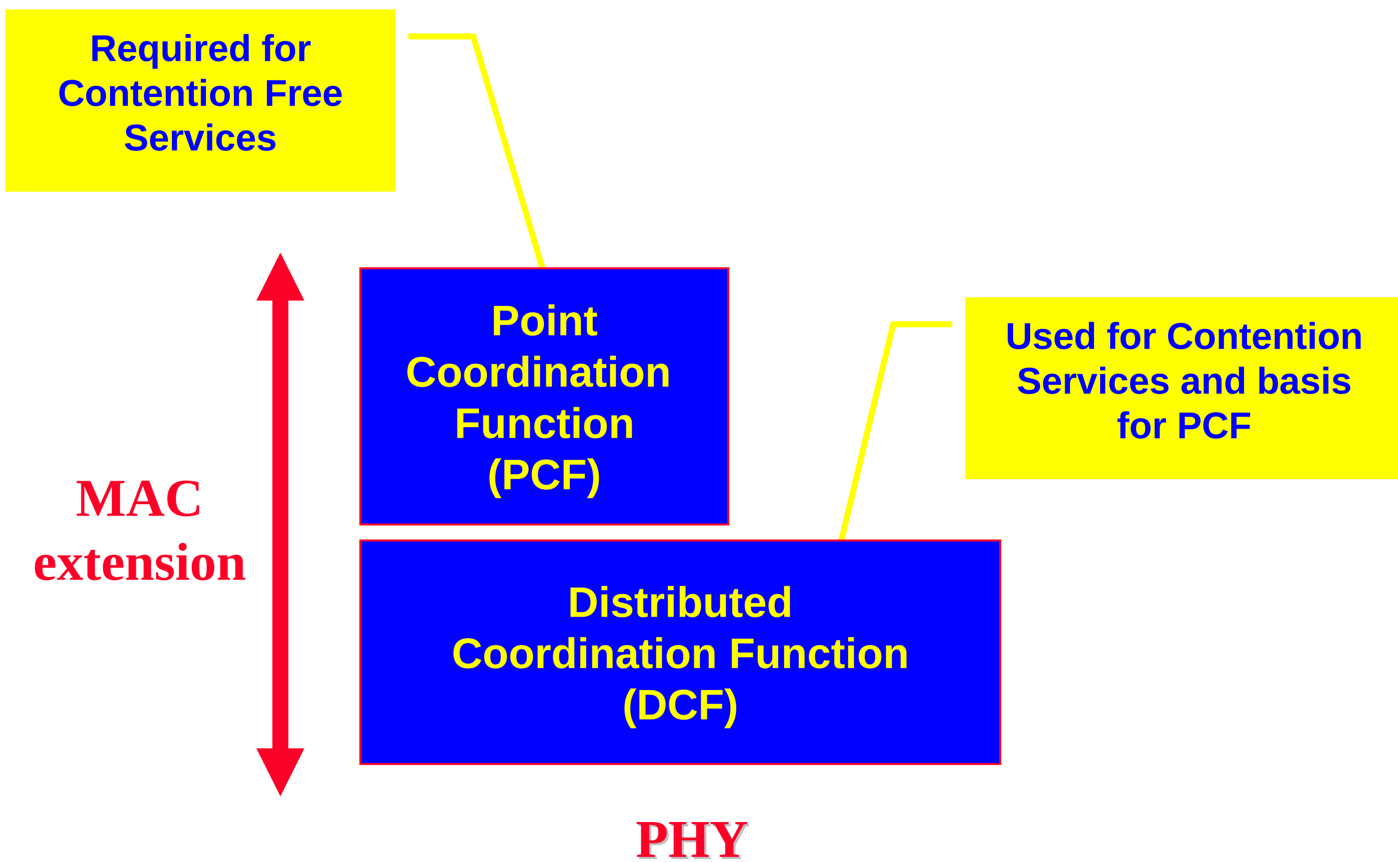
Bit b0	**NonERP_Present**
0	No NonERP stations are within the BSS
1	There are NonERP stations within the BSS

Bit b1	**Use_Protection**
0	STAs with an ERP should not use protection mechanisms for MPDUs transmitted at one of the ERP-OFDM rates.
1	STAs with an ERP shall use protection mechanisms for MPDUs transmitted at one of the ERP-OFDM rates.

- transmitted from AP in BSS or STA in IBSS
- defined in IEEE 802.11g
- **Protection mechanism**

  Use CTS frame to update the NAV of all receiving STAs prior to the transmission of a frame that may or may not be understood by receivers. The updated NAV period shall be longer than or equal to the total time required to send the data and any required response frames.

MAC Architecture



MAC Architecture

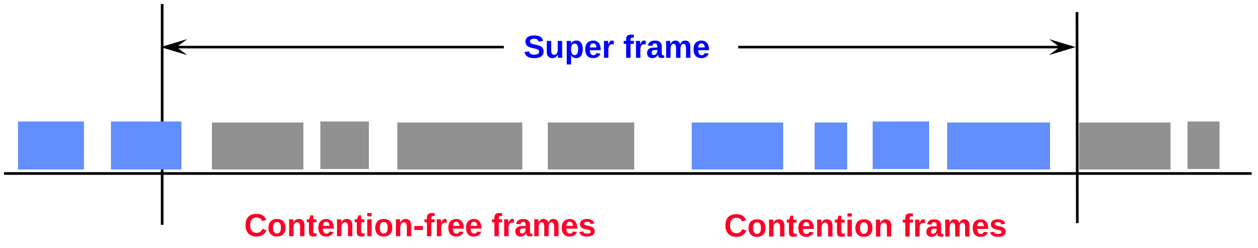
- **Distributed Coordination Function (DCF)**
  - **The fundamental access method for the 802.11 MAC, known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).**
  - **Shall be implemented in all stations and APs.**
  - **Used within both ad hoc and infrastructure configurations.**
- **Point Coordination Function (PCF)**
  - **An alternative access method**
  - **Shall be implemented on top of the DCF**
  - **A point coordinator (polling master) is used to determine which station currently has the right to transmit.**
  - **Shall be built up from the DCF through the use of an access priority mechanism.**
  - **Different accesses of traffic can be defined through the use of different values of IFS.**
  - **Shall use a Point IFS (PIFS) < Distributed IFS (DIFS)**

MAC Architecture

– Point coordinated traffic shall have higher priority to access the medium, which may be used to provide a *contention-free* access method.

– The priority access of the PIFS allows the point coordinator to seize control of the medium away from the other stations.

- Coexistence of DCF and PCF
  - – Both the DCF and PCF shall coexist without interference.
  - – They are integrated in a superframe in which a contention-free burst occurs at the beginning, followed by a contention period.



Distributed Coordination Function

- Allows for automatic medium sharing between similar and dissimilar PHYs through the use of CSMA/CA and a random backoff time following a busy medium condition.
- All directed traffic uses immediate positive ack (ACK frame) where retransmission is scheduled by the sender if no ACK is received.
- Carrier Sense shall be performed both through *physical* and *virtual* mechanisms.
- The virtual Carrier Sense mechanism is achieved by distributing medium busy reservation information through an exchange of special small RTS and CTS frames (contain a duration field) prior to the actual data frame. Unicast only, not used in multicast/broadcast.
- The use of RTS/CTS is under control of RTS_Threshold (payload length, under which without any RTS/CTS prefix).
- All stations are required to be able to receive any frame transmitted on a given set of rates, and must be able to transmit at (at least) one of these rates. This assures that the Virtual Carrier Sense mechanism still works on multiple rates environments.

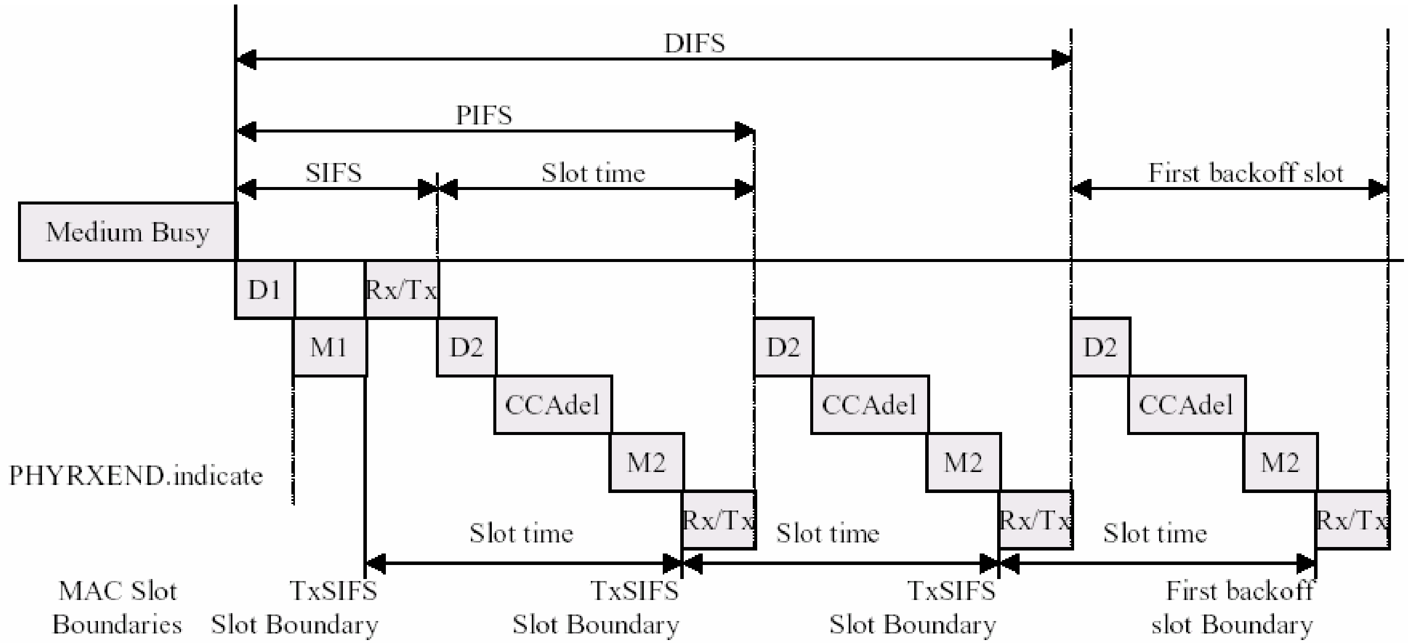
Distributed Coordination Function

- **Physical Carrier Sense Mechanism**
  - **A physical carrier sense mechanism shall be provided by the PHY.**
- **Virtual Carrier Sense Mechanism**
  - **Provided by the MAC, named Net Allocation Vector (NAV), which maintains a prediction of future traffic based on duration information announced in RTS/CTS frames.**
- **MAC-Level Acknowledgments (Positive Acknowledgment)**
  - **To allow detection of a lost or errored frame an ACK frame shall be returned immediately following a successfully received frame. The gap between the received frame and ACK frame shall be SIFS.**
  - **The frame types should be acknowledged with an ACK frame:**
    - » **Data**
    - » **Poll**
    - » **Request**
    - » **Response**
  - **The lack of an ACK frame means that an error has occurred.**

Distributed Coordination Function -- Inter-Frame Space (IFS)

- **A station shall determine that the medium is free through the use of carrier sense function for the interval specified.**
- **Three different IFS's are defined to provide priority levels.**
- **Short-IFS (SIFS)**
  - **Shall be used for an ACK frame, a CTS frame, by a station responding to any polling. It may also be used by a PC for any types of frames during the CFP.**
  - **Any STA intending to send only these frame types shall be allowed to transmit after the SIFS time has elapsed following a busy medium.**
- **PCF-IFS (PIFS)**
  - **Shall be used only by the PCF to send any of the Contention Free Period frames.**
  - **The PCF shall be allowed to transmit after it detects the medium free for the period PIFS, at the start of and during a CF-Burst.**
- **DCF-IFS (DIFS)**
  - **Shall be used by the DCF to transmit asynchronous MPDUs.**
  - **A STA using the DCF is allowed to transmit after it detects the medium free for the period DIFS, as long as it is not in a backoff period.**
- **Extended IFS (EIFS)**

Time Intervals SIFS/PIFS/DIFS



D1 = aRxRFDelay + aRxPLCPDelay (referenced from the end of the last symbol of a frame on the medium)
D2 = D1 + Air Propagation time
Rx/Tx = aRXTXTurnaroundTime (begins with a PHYTXSTART.request)
M1 = M2 = aMACPrcDelay
CCAdel = aCCATime – D1

EIFS

- The EIFS shall begin following indication by the PHY that the medium is idle after detection of the erroneous frame, without regard to the virtual carrier-sense mechanism.
- The EIFS is defined to provide enough time for another STA to acknowledge what was, to this STA, an incorrect received frame before this STA commences transmission.
- EIFS = aSIFSTime + (8$\times$ACKsize) + aPreambleLength + PLCPHeaderLength + DIFS,

  where ACKsize is computed based on 1Mbps data rate.

Distributed Coordination Function -- Random Backoff Time

- **Before transmitting asynchronous MPDUs, a STA shall use the carrier sense function to determine the medium state. If busy, the STA shall defer until after a DIFS gap is detected, and then generate a random backoff period for an additional deferral time (resolve contention).**

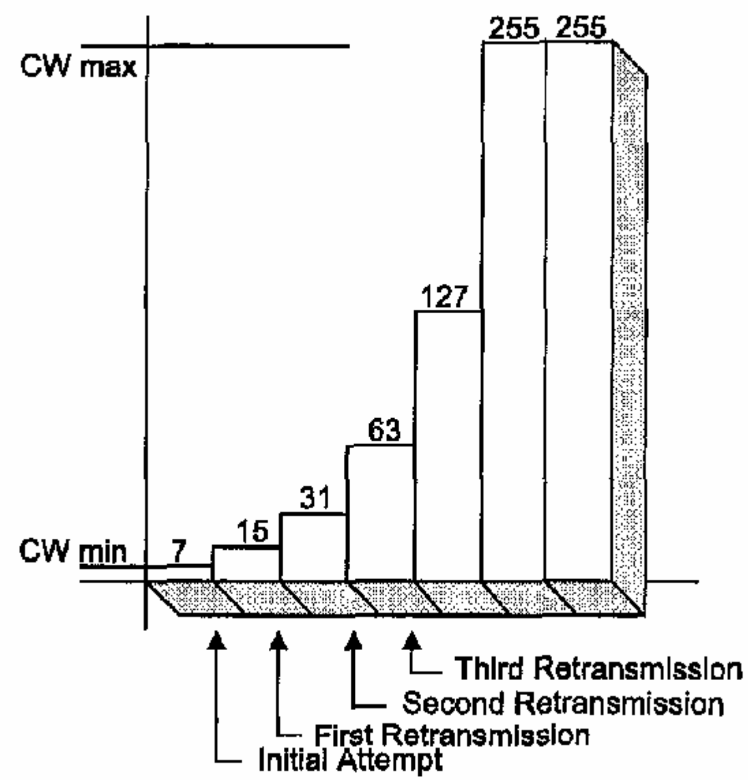
Backoff time = Random() * Slot time **where**

Random() = Pseudorandom integer drawn from a uniform distribution over the interval [0, CW].

CW = An integer between CWmin and CWmax

Slot Time = Transmitter turn-on delay +
medium propagation delay +
medium busy detect response time

Binary Exponentional Backoff Window



15~1023 for FHSS PHY
Source: IEEE Std 802.11-1997
14.8.2 FH PHY attributes: Table 49

63~1023 for IR PHY
Source: IEEE Std 802.11-1997
16.4 PHY attributes: Table 74

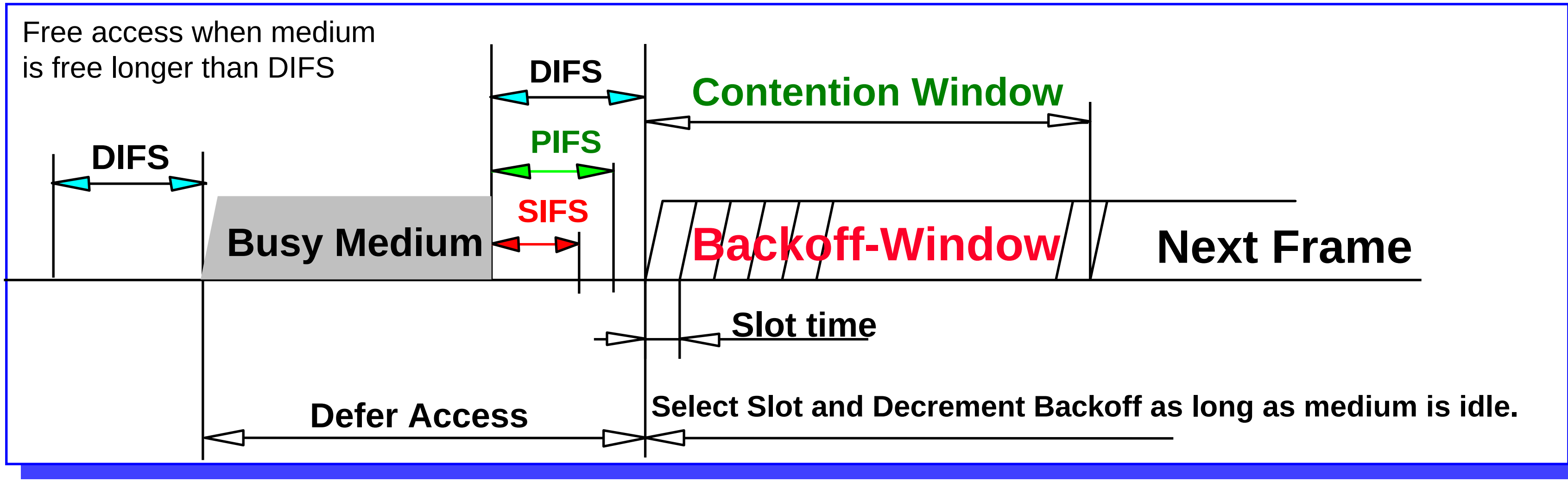
31~1023 for DSSS PHY
Source: IEEE Std 802.11-1997
15.3.2 DSSS PHY MIB: Table 58

15~1023 for DSSS ERP PHY (>20Mb/s)
31 ~1023 for DSSS ERP PHY (≤20Mb/s)
Source: IEEE Std 802.11g-2001
19.4.3.8.5 PHY Page 12

Basic Access Protocol Features

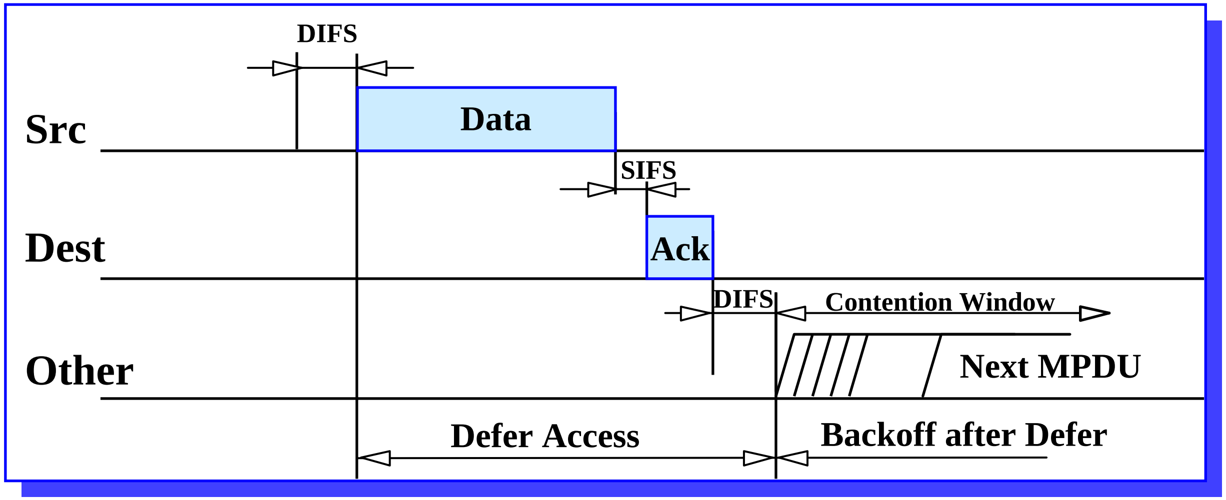
- **Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions.**
  - **Use CSMA with Collision Avoidance derivative.**
  - **Based on *Carrier Sense* function in PHY called *Clear Channel Assessment* (CCA).**
- **Robust for interference (use positive acknowledge).**
  - ***CSMA/CA + ACK* for unicast frames, with MAC level recovery.**
  - **CSMA/CA for Broadcast frames.**
- **Parameterized use of RTS / CTS to provide a *Virtual Carrier Sense* function to protect against *Hidden Nodes*.**
  - ***Duration* information is distributed by both transmitter and receiver through separate RTS and CTS Control Frames.**
- **Includes fragmentation to cope with different PHY characteristics.**
- **Frame formats to support the access scheme**
  - **For Infrastructure and Ad-Hoc Network support**
  - **and *Wireless Distribution System*.**

CSMA/CA Explained



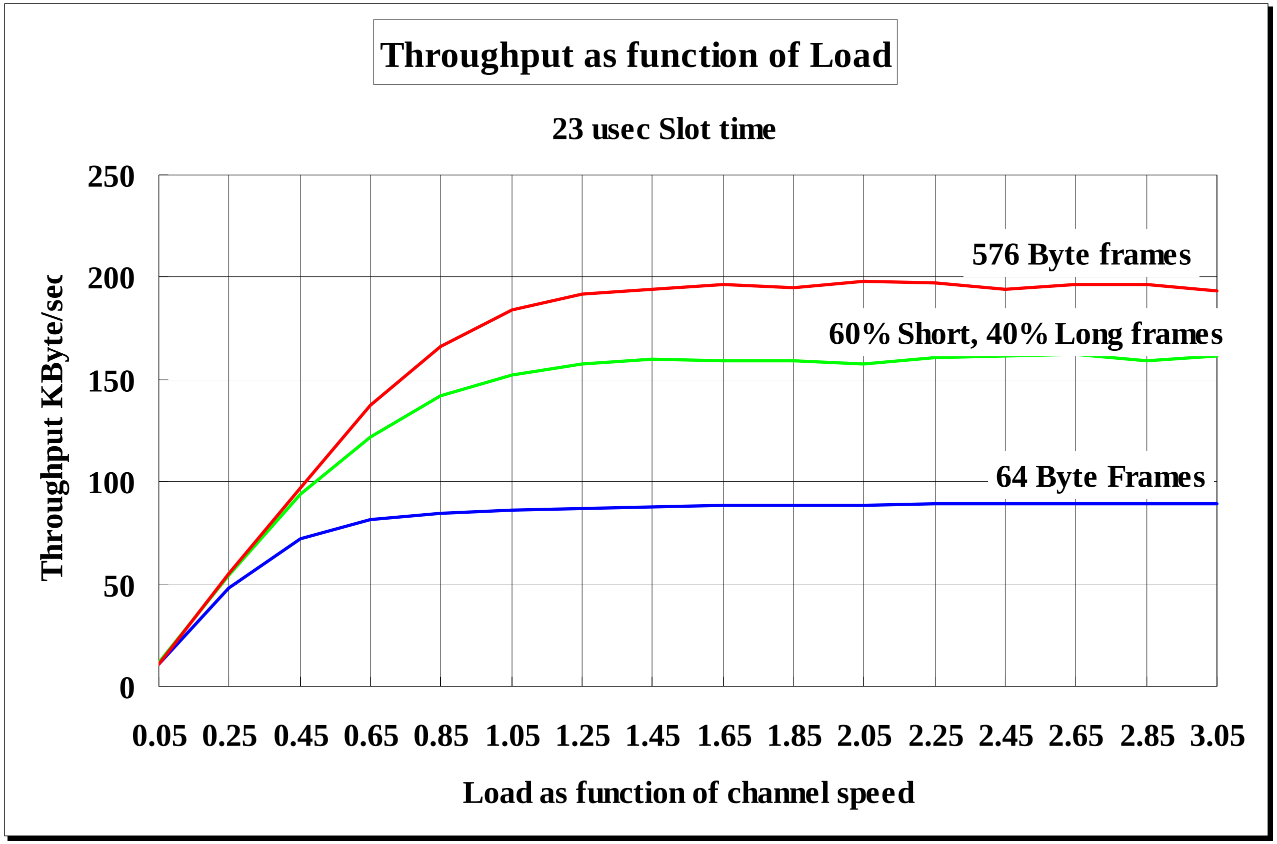
- **Reduce collision probability where mostly needed.**
  - **Stations are waiting for medium to become free.**
  - **Select Random Backoff after a Defer, resolving contention to avoid collisions.**
- **Efficient Backoff algorithm stable at high loads.**
  - **Exponential Backoff window increases for retransmissions.**
  - **Backoff timer elapses only when medium is idle.**
- **Implement different fixed priority levels.**
  - **To allow immediate responses and PCF coexistence.**

CSMA/CA + ACK protocol



- **Defer access based on *Carrier Sense*.**
  - **CCA from PHY and *Virtual Carrier Sense* state.**
- **Direct access when medium is sensed free longer then DIFS, otherwise defer and backoff.**
- **Receiver of directed frames to return an ACK immediately when CRC correct.**
  - **When no ACK received then retransmit frame after a random backoff (up to maximum limit).**

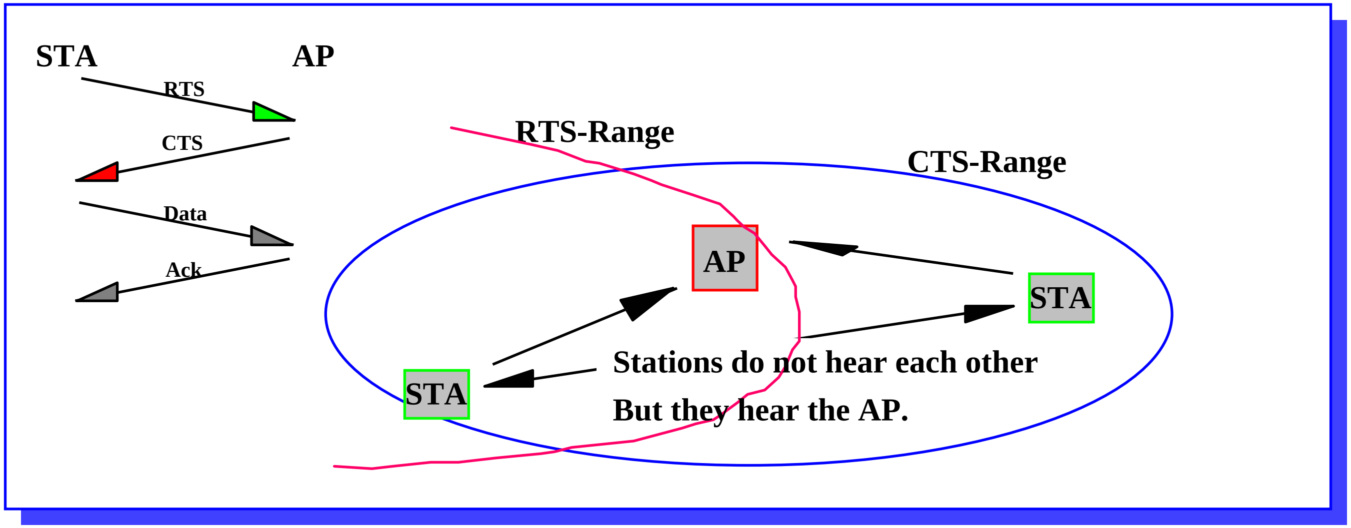
Throughput Efficiency



- **Efficient and stable throughput.**
  - **Stable throughput at overload conditions.**
  - **To support Bursty Traffic characteristics.**

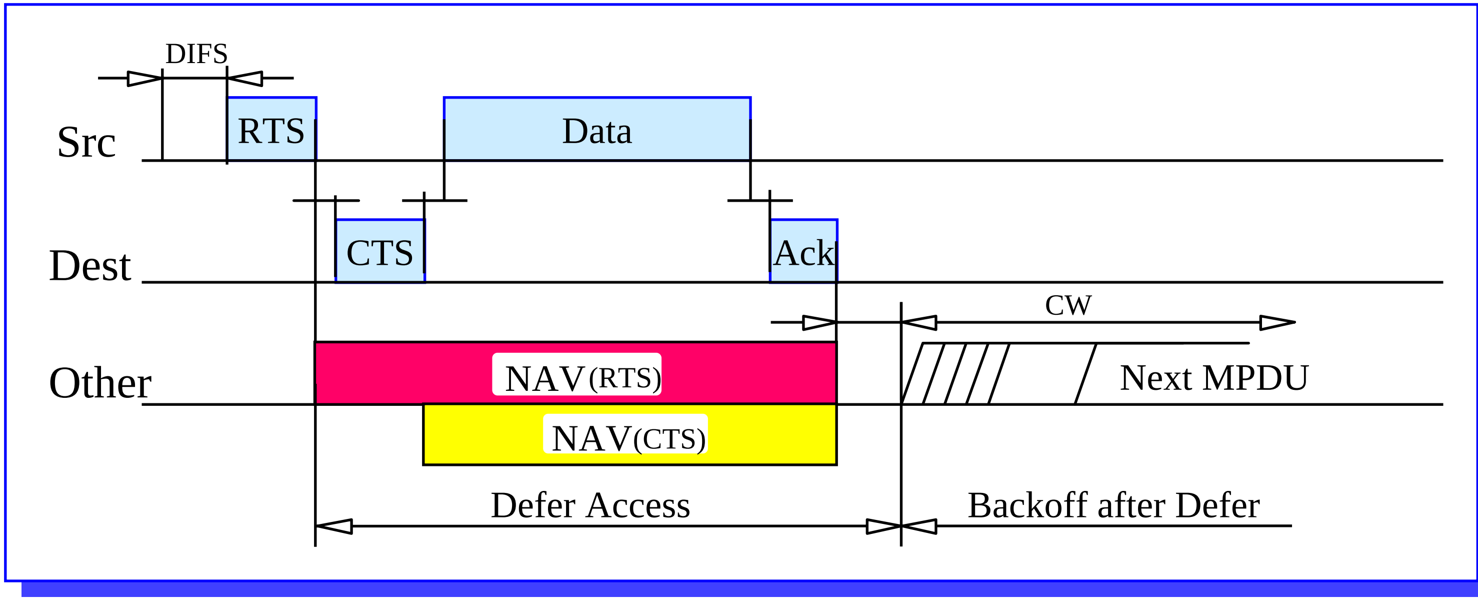
Hidden Node Problem

- **Transmitters contending for the medium may not *"Hear each other"* as shown below.**



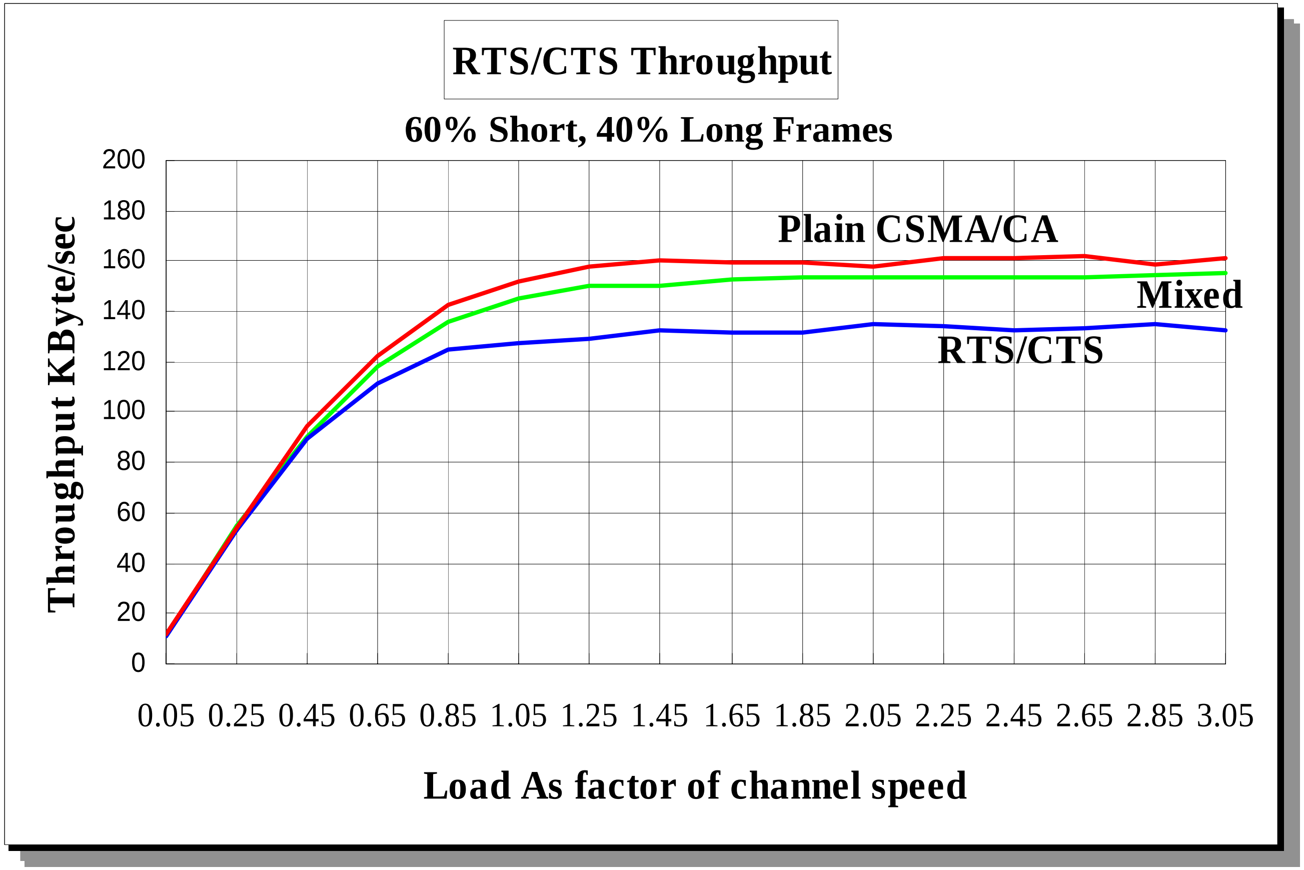
- **Separate Control frame exchange (RTS / CTS) between transmitter and receiver will *Reserve the Medium* for subsequent data access.**
  - ***Duration* is distributed around both Tx and Rx station.**

Hidden Node Provisions



- ***Duration*** **field in RTS and CTS frames distribute** ***Medium Reservation*** **information which is stored in a** ***Net Allocation Vector (NAV)*****.**
- **Defer on either NAV or "CCA" indicating** ***Medium Busy*****.**
- **Use of RTS / CTS is optional but must be implemented.**
- **Use is controlled by a** ***RTS_Threshold*** **parameter per station.**
  - **To limit overhead for short frames. (200 bytes)**

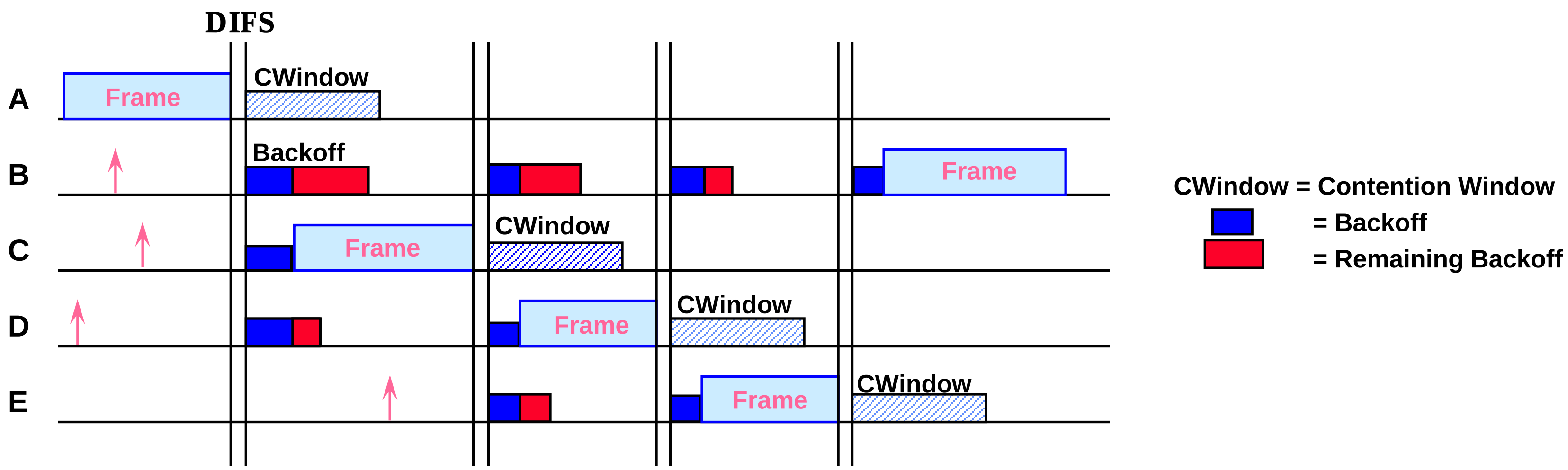
RTS/CTS Overhead Impact



Good mixed Throughput (long inbound frames) efficiency.

Distributed Coordination Function -- DCF Access Procedure

- **Backoff Procedure**
  - A backoff time is selected first. The Backoff Timer shall be frozen while the medium is sensed busy and shall decrement only when the medium is free (resume whenever free period > DIFS).
  - Transmission whenever the Backoff Timer reaches zero.
  - A STA that has just transmitted a frame and has another frame ready to transmit (queued), shall perform the backoff procedure (fairness concern).
  - Tends toward fair access on a FCFS basis.

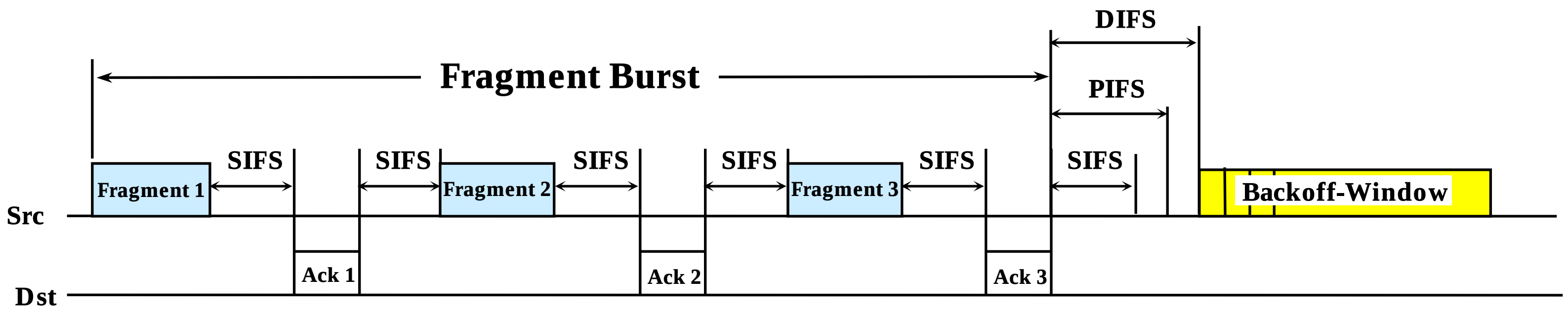


Distributed Coordination Function -- DCF Access Procedure

- RTS/CTS Recovery Procedure and Retransmit Limits
  - After an RTS is transmitted, if the CTS fails in any manner within a predetermined CTS_Timeout (T1), then a new RTS shall be generated (the CW shall be doubled).
  - This procedure shall continue until the RTS_Re-Transmit_Counter reaches an RTS_Re-Transmit_Limit.
  - The same backoff mechanism shall be used when no ACK is received within a predetermined ACK_Window(T3) after a directed DATA frame has been transmitted.
  - This procedure shall be continue until the ACK_Re-Transmit_Counter reaches an ACK_Re-Transmit_Limit.
  - STAs shall maintain a short retry count (for MAC frame <= RTS_Threshold) and a long retry count (for MAC frame > RTS_Threshold) for each MSDU and MMPDU awaiting transmission. These counts are incremented and reset independently of each other.

Distributed Coordination Function -- DCF Access Procedure

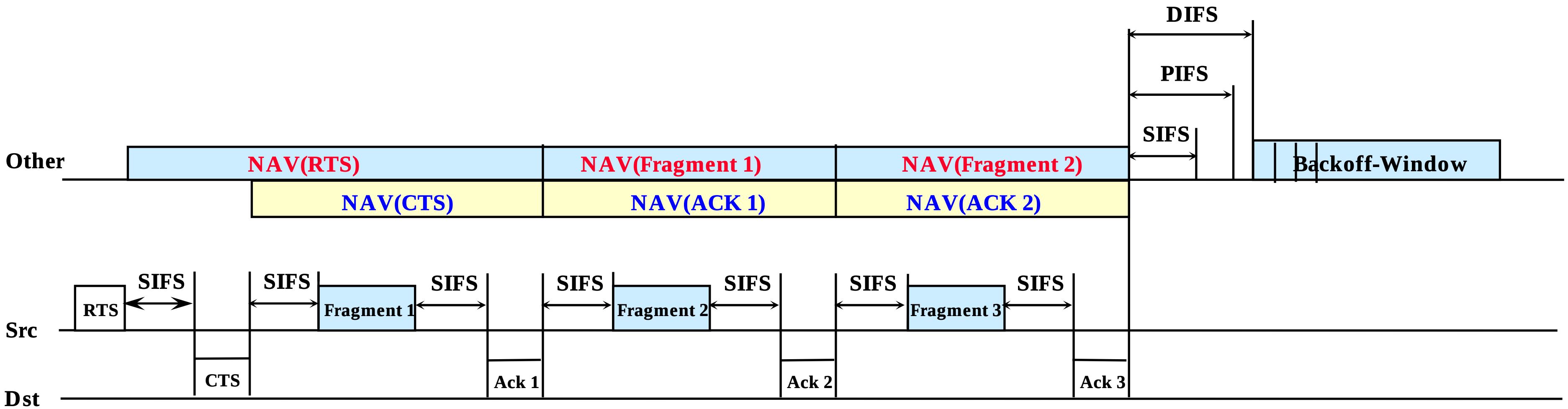
- Control of the Channel
  - The IFS is used to provide an efficient MSDU delivery mechanism.
  - Once a station has contended for the channel, it will continue to send fragments until either all fragments of a MSDU have been sent, an ack is not received, or the station can not send any additional fragments due to a dwell time boundary.
  - If the source station does not receive an ack frame, it will attempt to retransmit the fragment at a later time (according to the backoff algorithm). When the time arrives to retransmit the fragment, the source station will contend for access in the contention window.

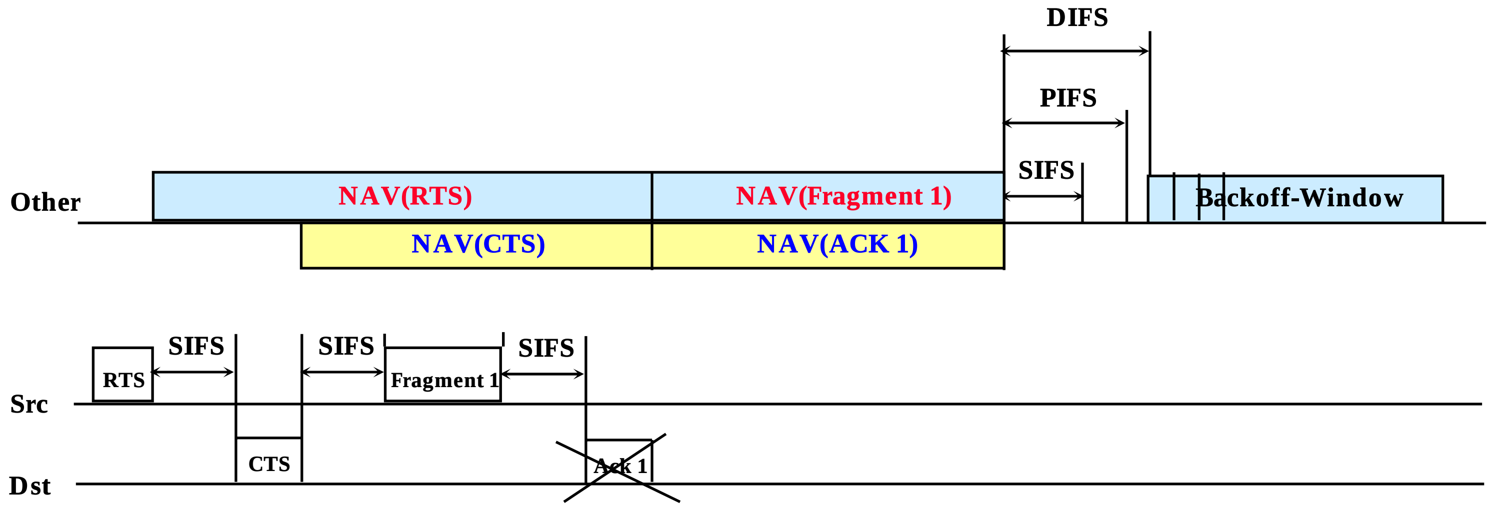


Distributed Coordination Function -- DCF Access Procedure

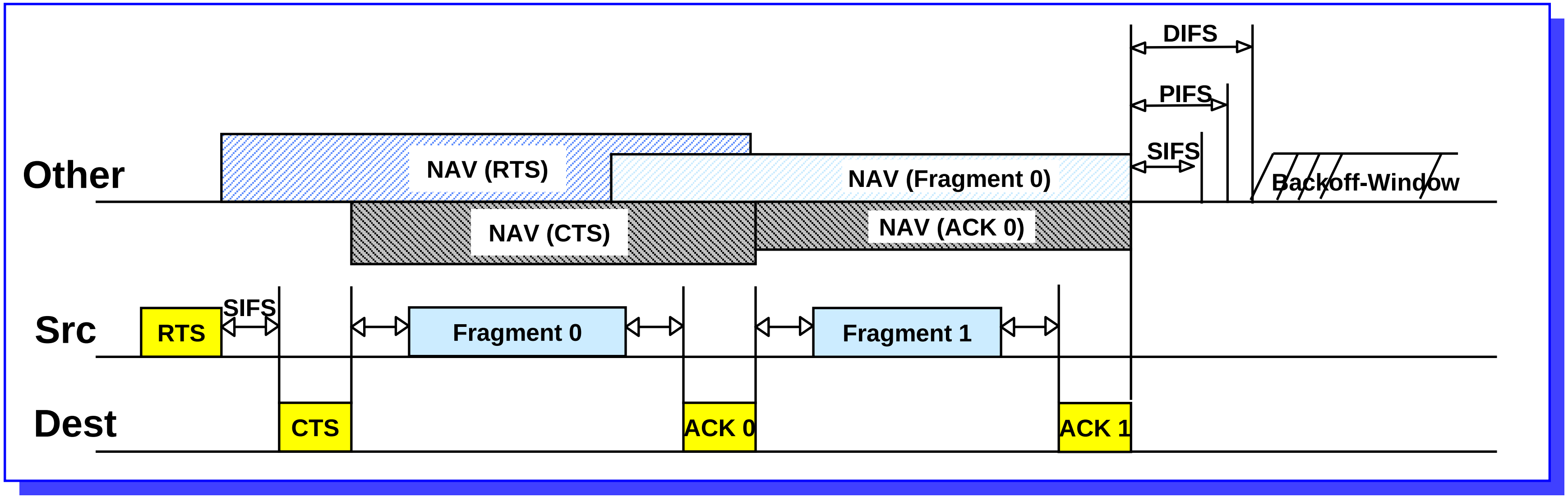
- **RTS/CTS Usage with Fragmentation**
  - **The RTS/CTS frames define the duration of the first frame and ack. The duration field in the data and ack frames specifies the total duration of the next fragment and ack.**
  - **The last Fragment and ACK will have the duration set to zero.**
  - **Each Fragment and ACK acts as a virtual RTS and CTS.**
  - **In the case where an ack is not received by the source station, the NAV will be marked busy for next frame exchange. This is the worst case situation.**
  - **If the ack is not sent by the destination, stations that can only hear the destination will not update their NAV and be free to access the channel.**
  - **All stations that hear the source will be free to access the channel after the NAV from Fragment 1 has expired.**
  - **The source must wait until the NAV (Fragment 1) expires before attempting to contend for the channel after not receiving the ack.**

RTS/CTS Usage with Fragmentation





Fragmentation (1/2)



- Burst of Fragments which are individually acknowledged.
  - For Unicast frames only.
- Random backoff and retransmission of failing fragment when no ACK is returned.
- *Duration* information in data fragments and Ack frames causes NAV to be set, for medium reservation mechanism.

Fragmentation (2/2)

- The length of a fragment MPDU shall be an equal number of octets for all fragments except the last, which may be smaller.
- The length of a fragment MPDU shall always be an even number of octets, except for the last fragment.
- The length of a fragment shall never be larger than aFragmentationThreshold unless WEP is invoked for the MPDU. Because the MPDU shall be expanded by IV and ICV.
- The sequence number shall remain the same for all fragments of a MSDU or MMPDU.
- The fragments shall be sent in order of lowest fragment number to highest fragment number (start at zero, and increased by one).
- More Fragments bit is used to indicate the last (or only) fragment of the MSDU or MMPDU.

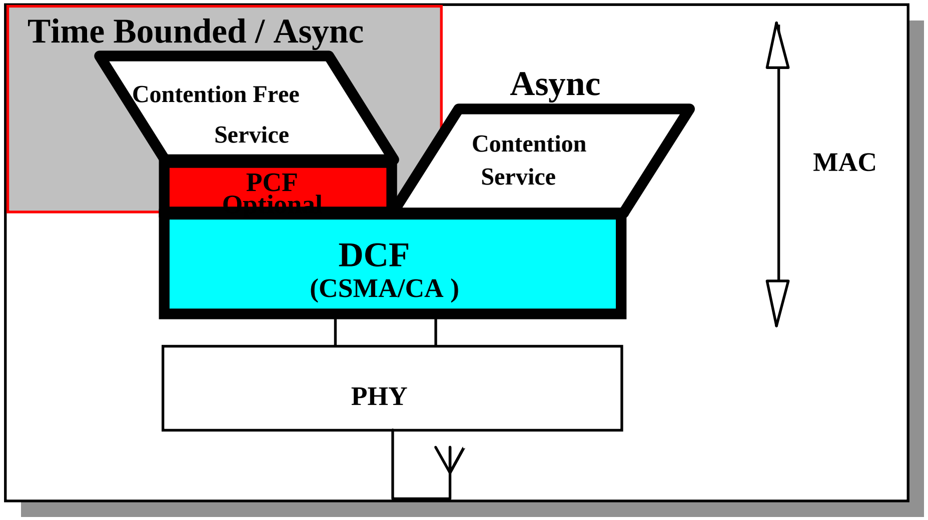
Defragmentation

- The header of each fragment contains the following information that is used by the destination STA to reassemble the MSDU or MMPDU.
  - Frame type.
  - Address of the sender.
  - Destination address.
  - Sequence Control field.
- More Fragments indicator. If WEP has been applied, it shall be decrypted before the defragmentation.
- All STAs shall support the concurrent reception of fragments of at least three MSDUs or MMPDUs.
- All STAs shall maintain a Receive Timer for each MSDU or MMPDU. If the a timer is not maintained, all the fragments belong to the part of an MSDU or MMPDU are discarded.
- If the receive MSDU timer exceeds aMaxReceiveLifetime, then all received fragments of this MSDU or MMPDU are discarded.

Distributed Coordination Function -- DCF Access Procedure

- **Broadcast and multicast MPDU transfer procedure**
  - In the absence of a PCF, when broadcast or multicast MPDUs are transferred from a STA with the ToDS bit clear, only the basic access procedure shall be used. Regardless of the length of the frame, no RTS/CTS exchange shall be used.
  - In addition, no ACK shall be transmitted by any of the recipients of the frame.
  - Any broadcast or multicast MPDUs transferred from a STA with a ToDS bit set shall obey the rules for RTS/CTS exchange, because the MPDU is directed to the AP.
  - The broadcast/multicast message shall be distributed into the BSS, so the STA originating the message will also receive the message. Therefore, all STAs must filter out broadcast/multicast messages that contain their address as the source address.
  - Broadcast/multicast MSDUs shall be propagated throughout the ESS.
  - This no MAC-level recovery on broadcast or multicast frames, except for those frames sent with ToDS bit set.

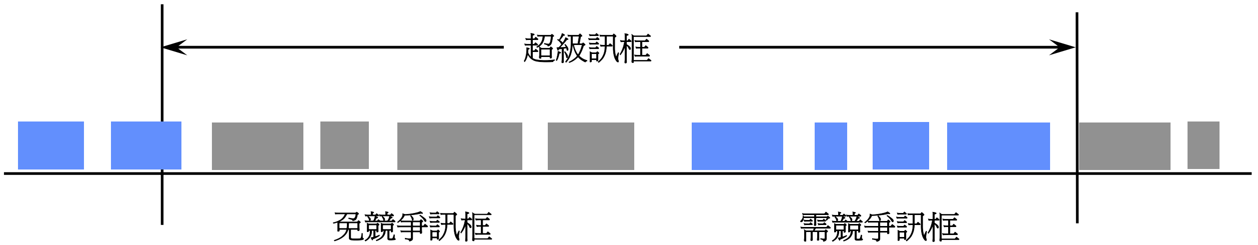
Optional Point Coordination Function (PCF)



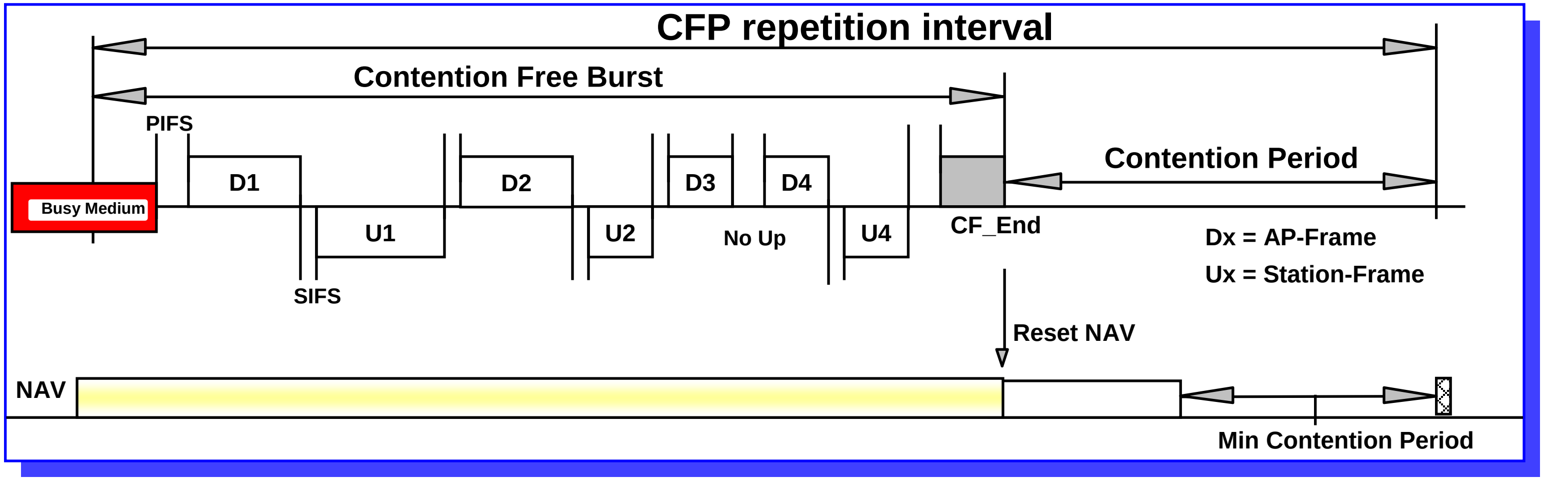
- **Contention Free Service uses Point Coordination Function (PCF) on a DCF Foundation.**
  - **PCF can provide lower *transfer delay* variations to support *Time Bounded Services*.**
  - **Async Data, Voice or mixed implementations possible.**
  - **Point Coordinator resides in AP.**
- **Coexistence between Contention and optional Contention Free does not burden the implementation.**

Point Coordination Function(PCF)

- **The PCF provides contention free services.**
- **It is an option for a station to become the Point Coordinator(PC), which generates the Superframe (SF).**
- **The PC shall reside in the AP.**
- **The SF consists of a Contention Free (CF) period and a Contention Period.**
- **The length of a SF is a manageable parameter and that of the CF period may be variable on a per SF basis.**



PCF Burst



- CF-Burst by Polling bit in CF-Down frame.
- Immediate response by Station on a CF_Poll.
- Stations to maintain NAV to protect CF-traffic
- Responses can be variable length.
- Reset NAV by last (CF_End) frame from AP.
- "ACK Previous Frame" bit in Header. (piggyback)

Valid Type/Subtype combinations 1/2

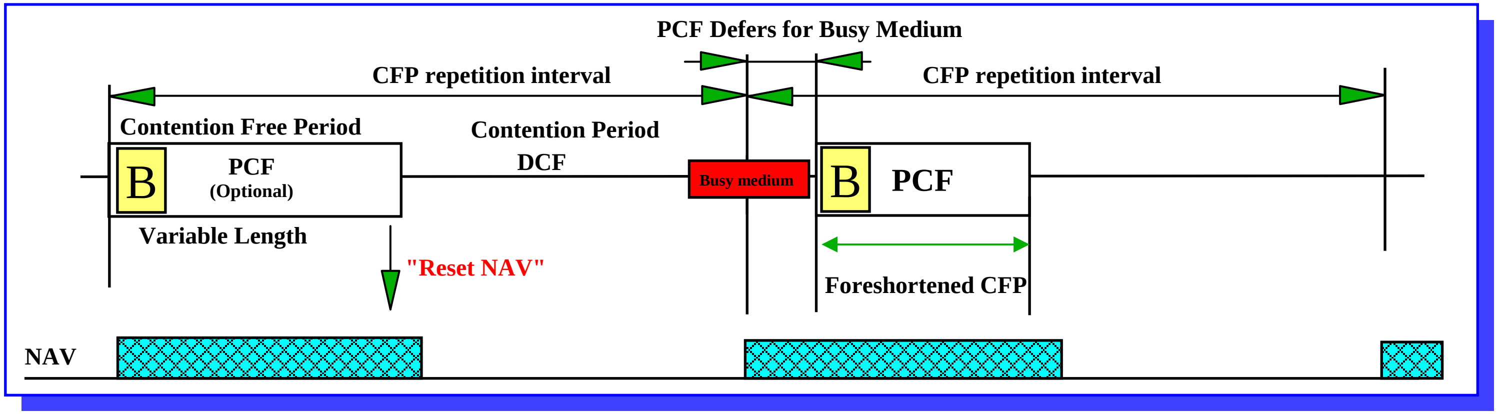
Type value b3 b2	Type description	Subtype Value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved

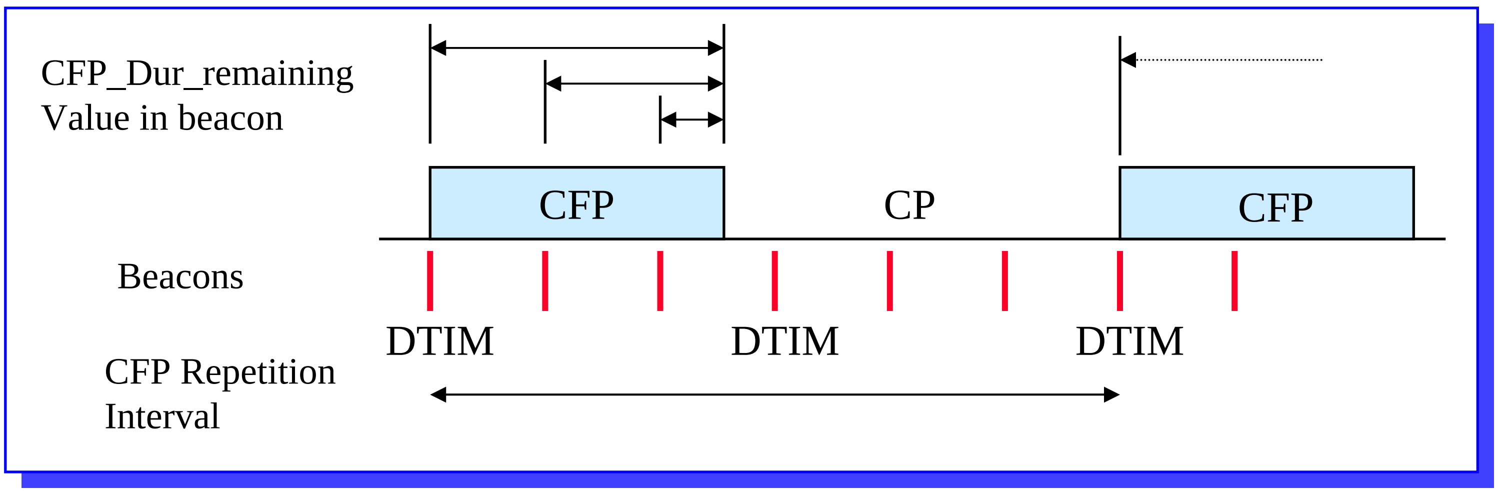
Valid Type/Subtype combinations 2/2

Type value b3 b2	Type description	Subtype Value b7 b6 b5 b4	Subtype description
01	Control	000-1001	Reserved
01	Control	1010	Power Save (PS-Poll)
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

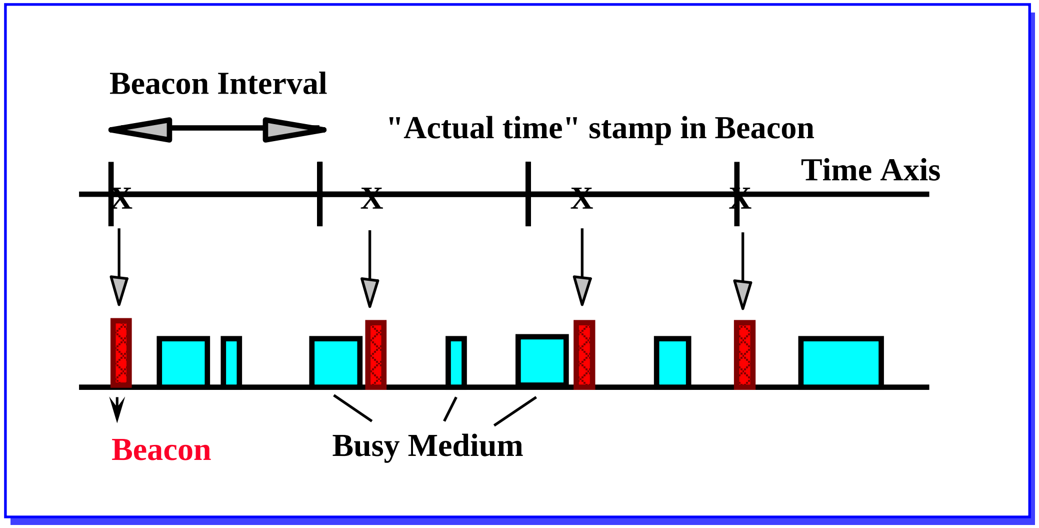
Point Coordination Function
-- CFP structure and timing (1/2)

- The PC generates CFPs at the contention-free repetition rate (CFPRate), which is defined as a number of DTIM intervals.





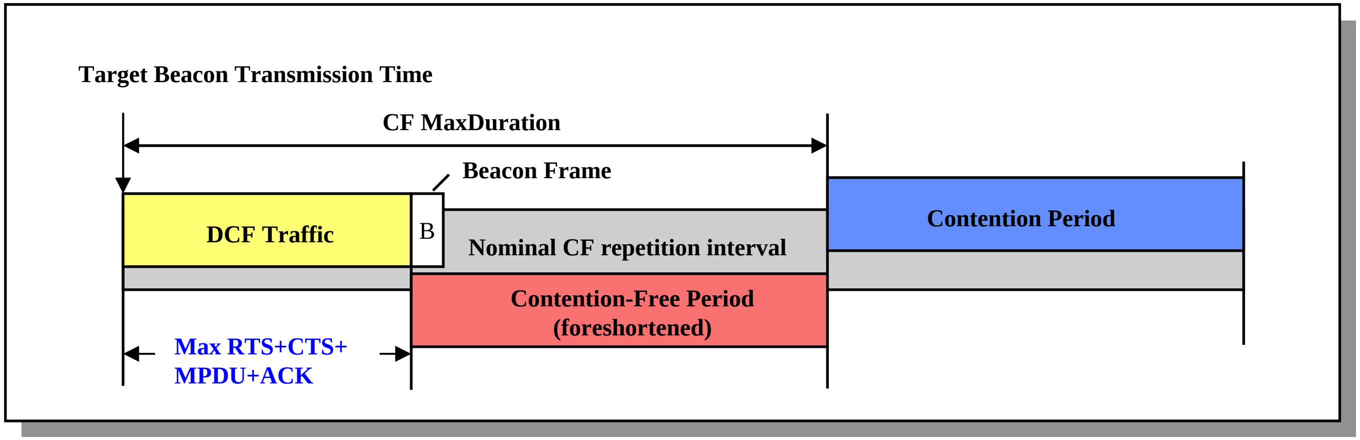
Infrastructure Beacon Generation



- APs send Beacons in infrastructure networks.
- Beacons scheduled at Beacon Interval .
- Transmission may be delayed by CSMA deferral.
  - subsequent transmissions at expected Beacon Interval
  - not relative to last Beacon transmission
  - next Beacon sent at Target Beacon Transmission Time
- Timestamp contains timer value at transmit time.

Point Coordination Function
-- CFP structure and timing (2/2)

- The length of the CFP is controlled by the PC, with maximum duration specified by the value of the CFP-MaxDuration Parameter Set at the PC. (broadcast by Beacon & probe response)
- Because the transmission of any beacon may be delayed due to a medium busy, a CFP may be foreshortened by the amount of the delay.
- The CFPDurRemaining value in the beacon shall let the CFP end time no later than TBTT plus the value of CF MaxDuration.



Point Coordination Function -- PCF Access Procedure (1/2)

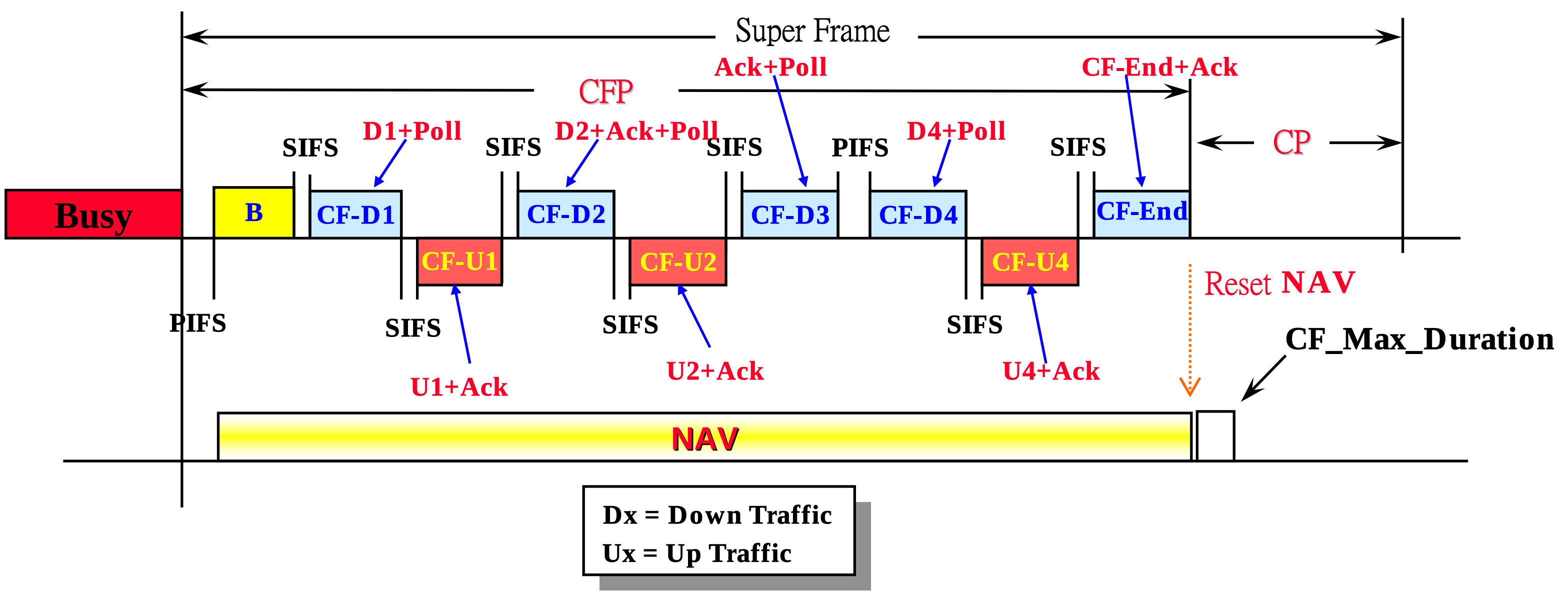
- The PCF protocol is based on a polling scheme controlled by one special STA per BSS called the Point Coordinator.
- The PC gains control of the medium at the beginning of the CF and maintains control for the entire CF period by waiting a shorter time between transmissions.
- At the beginning of the CF, the PCF shall sense the medium. If it is free the PCF shall wait a PIFS time and transmit
  - a Data frame with the CF-Poll Subtype bit set, to the next station on the polling list, or
  - a CF-End frame, if a null CF period is desired.

Point Coordination Function -- PCF Access Procedure (2/2)

- The PCF uses the PCF priority level of the CSMA/CA protocol. The shorter PIFS gap causes a burst traffic with inter-frame gaps that are shorter than the DIFS gap needed by stations using the Contention period.
- Each station, except the station with the PCF, shall preset it's NAV to the maximum CF-Period length at the beginning of every SF. The PCF shall transmit a CF-End or CF-End+Ack frame, at the end of the CF-Period, to reset the NAV of all stations in the BSS.

Point Coordination Function
-- PCF Transfer Procedure

- **PCF Transfers When the PCF Station is Transmitter or Recipient**
  - **Stations shall respond to the CF-Poll immediately when a frame is queued, by sending this frame after an SIFS gap. This results in a burst of Contention Free traffic (CF-Burst).**
  - **For services that require MAC level ack, the ack is preferably done through the CF-Ack bit in the Subtype field of the responding CF-Up frame.**



MAC Management Layer

- **Synchronization**
  - finding and staying with a WLAN
  - Synchronization functions
    - » TSF Timer, Beacon Generation
- **Power Management**
  - sleeping without missing any messages
  - Power Management functions
    - » periodic sleep, frame buffering, Traffic Indication Map
- **Association and Reassociation**
  - Joining a network
  - Roaming, moving from one AP to another
  - Scanning
- **Management Information Base**

Synchronization in 802.11

- Timing Synchronization Function (TSF)

- Used for Power Management
  - Beacons sent at well known intervals
  - All station timers in BSS are synchronized
- Used for Point Coordination Timing
  - TSF Timer used to predict start of Contention Free burst
- Used for Hop Timing for FH PHY
  - TSF Timer used to time Dwell Interval
  - All Stations are synchronized, so they hop at same time.

Synchronization Approach

- All stations maintain a local timer.
- Timing Synchronization Function
  - keeps timers from all stations in synch
  - AP controls timing in infrastructure networks
  - distributed function for Independent BSS
- Timing conveyed by periodic Beacon transmissions
  - Beacons contain Timestamp for the entire BSS
  - Timestamp from Beacons used to calibrate local clocks
  - not required to hear every Beacon to stay in synch
  - Beacons contain other management information
    - » also used for Power Management, Roaming

Beacon Generation (*)

- **In Infrastructure**
  - **AP defines the *aBeaconPeriod* for transmitting beacons**
  - ***aBeaconPeriod* is broadcast by beacon and probe response**
  - **may delayed by CSMA/CA**
- **In IBSS**
  - **all members participate in beacon generation**
  - **The IBSS initiator defines the *aBeaconPeriod***
  - **At each TBTT, STA shall**
    - » **suspend the decrementing backoff timer for any non-beacon or non-ATIM transmission**
    - » **calculate a random delay from [0, 2*(CWmin*Slot_time)]**
    - » **backoff the selected random delay**
    - » **If a beacon is detected, give up sending beacon and decrementing backoff timer**
    - » **otherwise, transmit beacon**

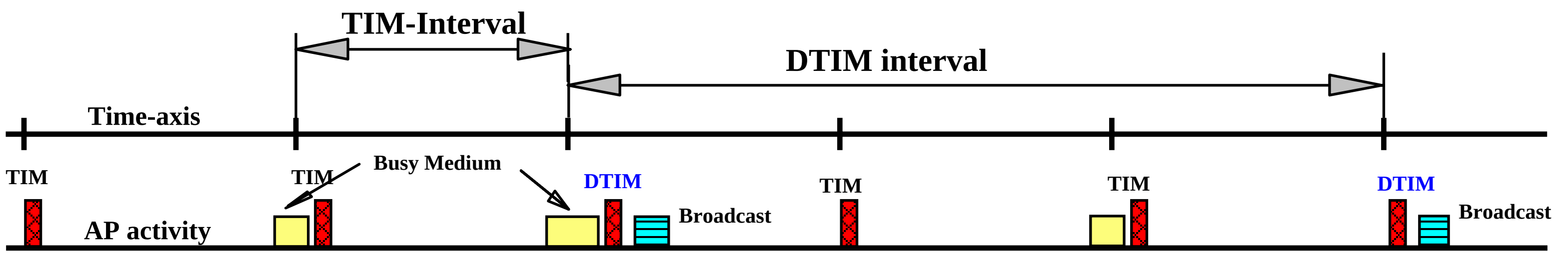
Power Management

- **Mobile devices are battery powered.**
  - ***Power Management* is important for mobility.**
- **Current LAN protocols assume stations are always ready to receive.**
  - **Idle receive state dominates LAN adapter power consumption over time.**
- **How can we power off during idle periods, yet maintain an active session?**
- **802.11 Power Management Protocol:**
  - **allows transceiver to be off as much as possible**
  - **is transparent to existing protocols**
  - **is flexible to support different applications**
    - » **possible to trade off throughput for battery life**

Power Management Approach

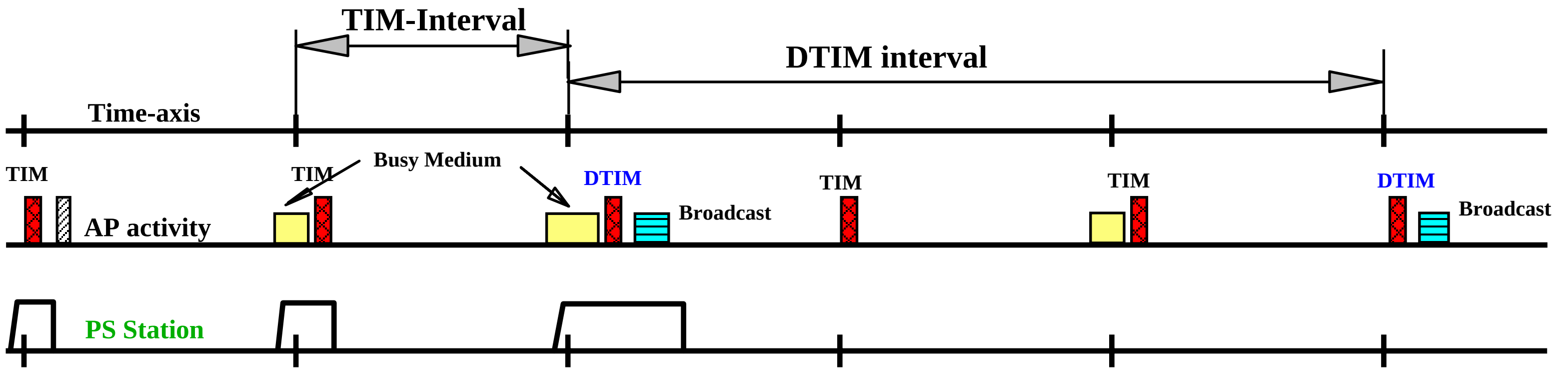
- Allow idle stations to go to sleep
  - station power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF assures AP and Power Save stations are synchronized
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- Independent BSS also have Power Management
  - similar in concept, distributed approach

Infrastructure Power Management



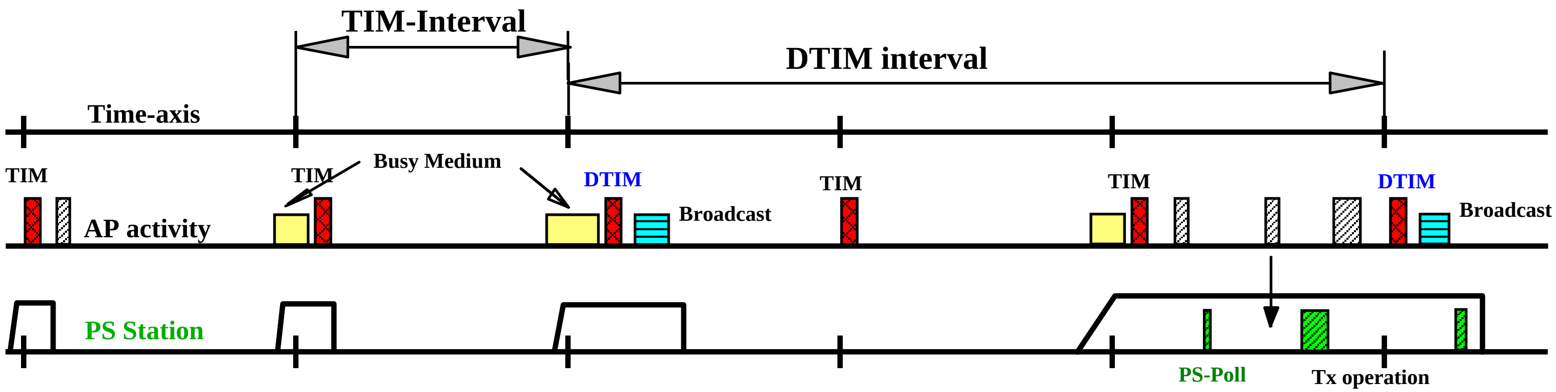
- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
    - » DTIM : Delivery Traffic Indication Message
  - DTIM interval is a multiple of TIM interval

Infrastructure Power Management



- **Broadcast frames are also buffered in AP.**
  - **all broadcasts/multicasts are buffered**
  - **broadcasts/multicasts are only sent after DTIM**
  - **DTIM interval is a multiple of TIM interval**
- **Stations wake up prior to an expected (D)TIM.**

Infrastructure Power Management

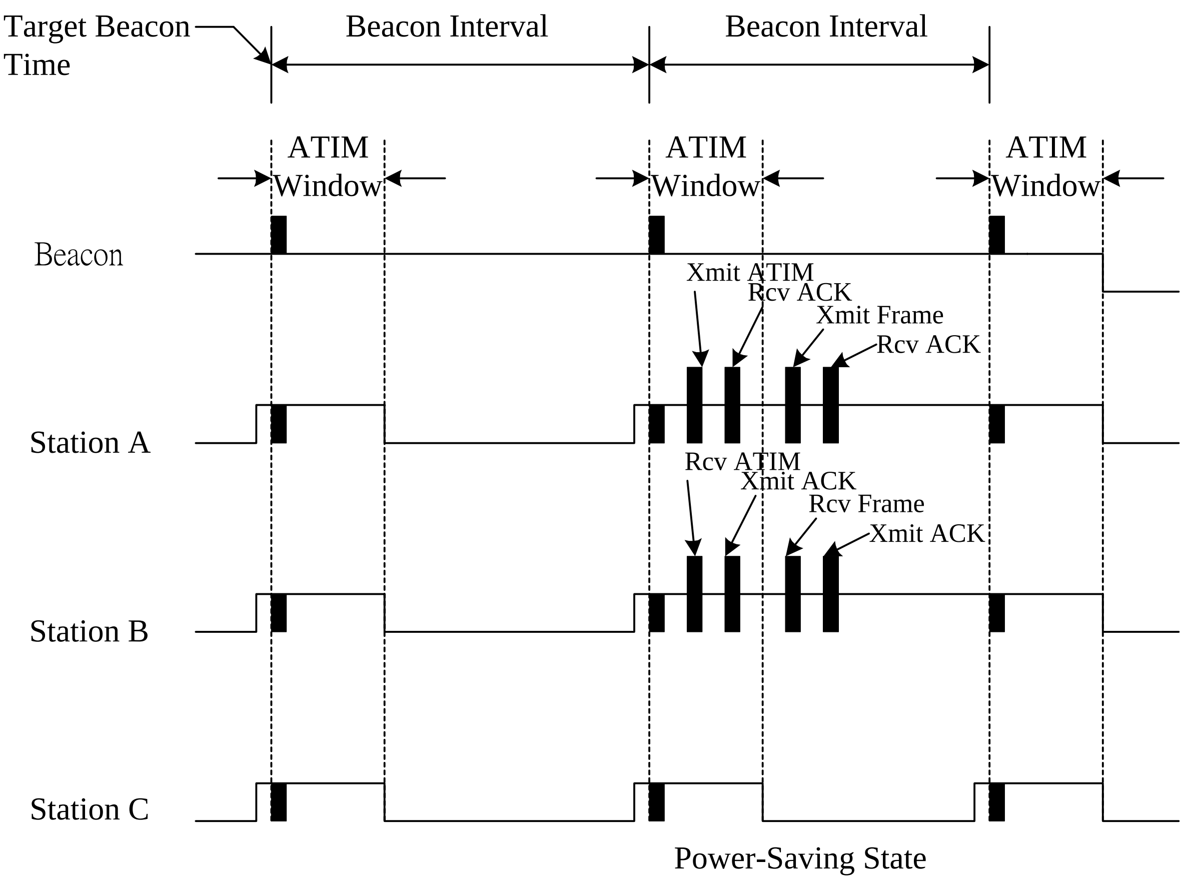


- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
  - DTIM interval is a multiple of TIM interval
- Stations wake up prior to an expected (D)TIM.
- If TIM indicates frame buffered
  - station sends PS-Poll (with AID) and stays awake to receive data
  - else station sleeps again

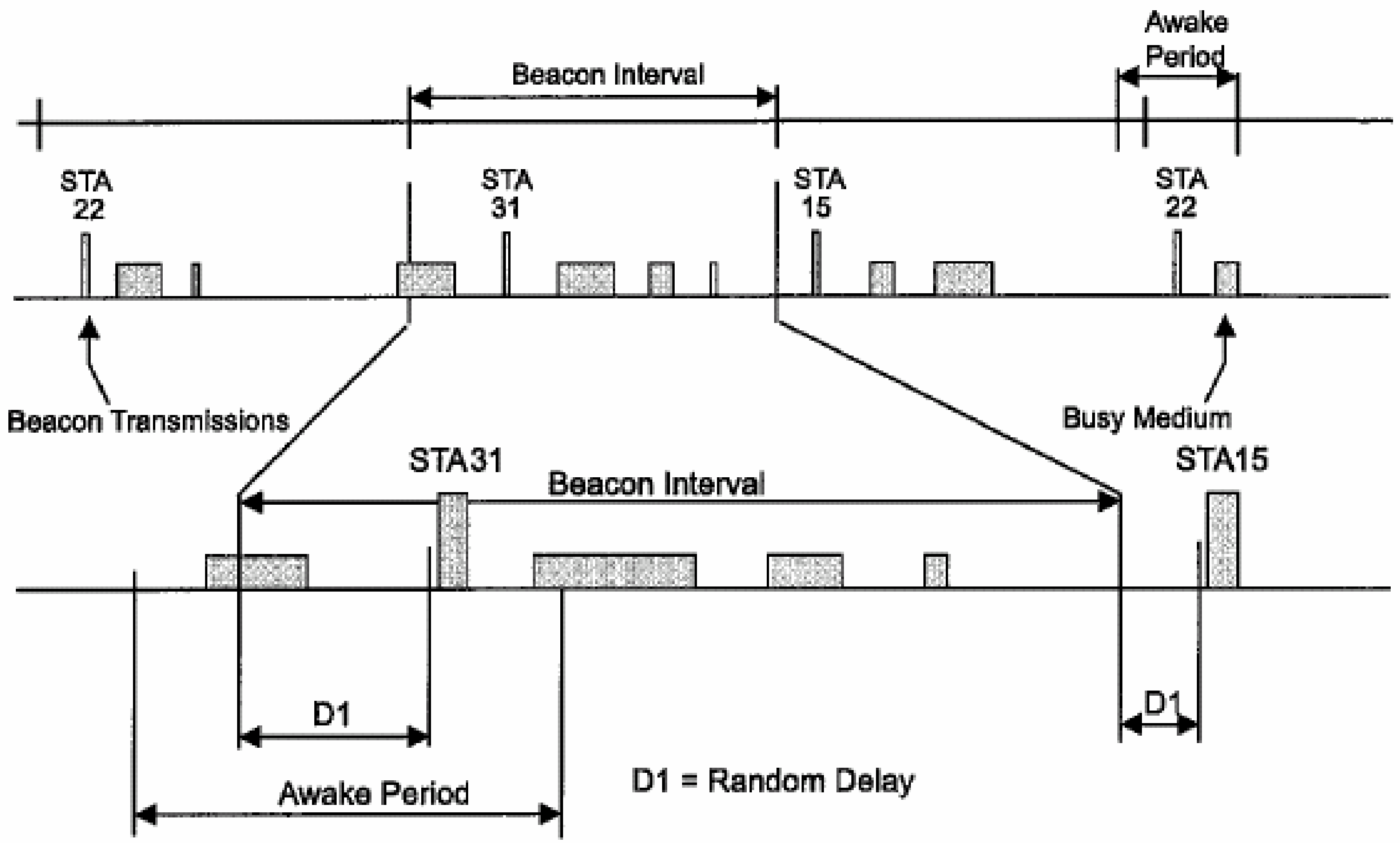
IBSS Power Management

- **ATIM: Ad Hoc (Announced) Traffic Indication Message.**
- **If a STA is PS, it shall enter the Awake state prior to each TBTT.**
- **If received a ATIM, a STA shall remain in the Awake state until the end of the next ATIM window.**
- **If a STA transmits a Beacon or an ATIM management frame, it shall remain in the Awake state until the end of the next ATIM window.**
- **Use RTS/CTS to detect if a STA is in PS-mode.**
- **A STA shall transmit no frame types other than RTS, CTS, and ACK Control frames, and Beacon, ATIM management frames in ATIM window.**
- **Transmission is begin following the ATIM window, backoff, DCF is used.**

IBSS Power Management



IBSS Beacon Transmission



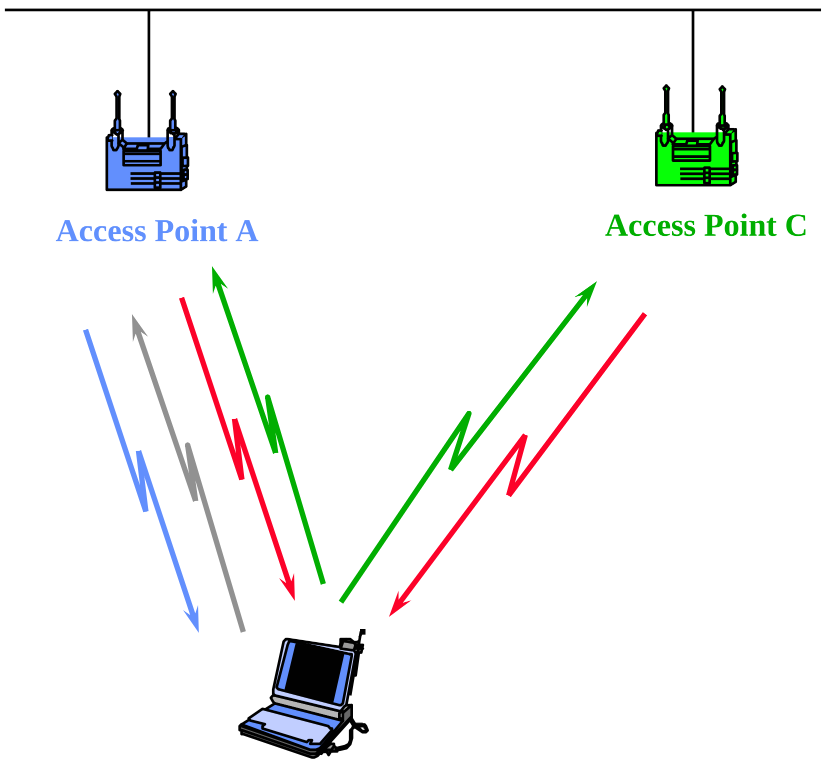
Scanning

- Scanning required for many functions.
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- 802.11 MAC uses a common mechanism for all PHY.
  - single or multi channel
  - passive or active scanning
- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel
    - » Send a Probe, Wait for a Probe Response
- Beacon or Probe Response contains information necessary to join new network.

Channel Scanning

- **A STA shall operate in either a Passive Scanning mode or an Active Scanning mode.**
- **For Passive scanning, the STA shall scan for Beacon frames containing the desired SSID (or broadcast SSID). The STA shall listen to each channel scanned for no longer than a maximum duration defined by the ChannelTime parameter.**
- **For Active scanning, the STA shall transmit Probe request containing the desired SSID (also can use broadcast SSID).**
- **If a STA's scanning does not result in finding a BSS with the desired SSID, or does not result in finding any BSS, the STA may start an IBSS .**
- **A STA may start its own BSS without first scanning for a BSS to join.**

Active Scanning Example



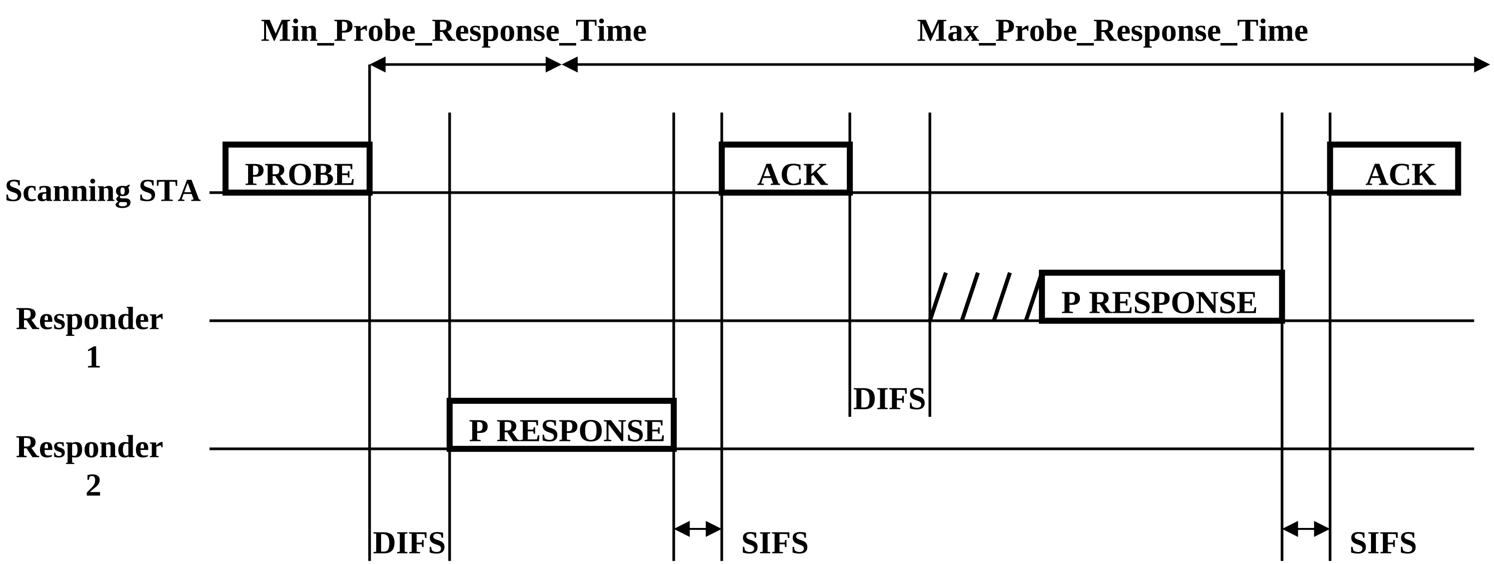
Steps to Association:

- Station sends Probe Request.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

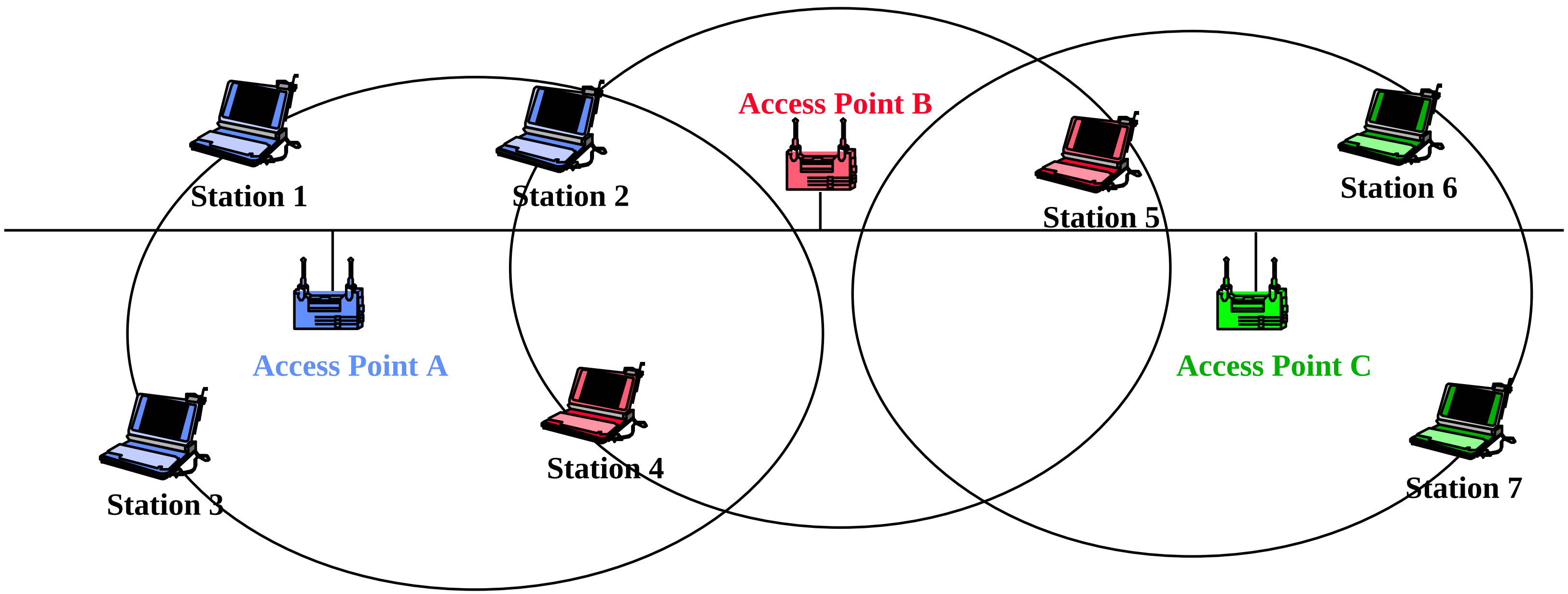
Initial connection to an Access Point
- Reassociation follows a similar process

Active Scanning

- For each channel to be scanned,
  - Send a Probe request with the broadcast destination, SSID, and broadcast BSSID.
  - Start a ProbeTimer.
  - If the response has not been received before the *Min_Probe_Response_time*, then clear NAV and scan the next channel, else when ProbeTimer reaches *Max_Probe_response_time*, process all received probe responses and scan the next channel.

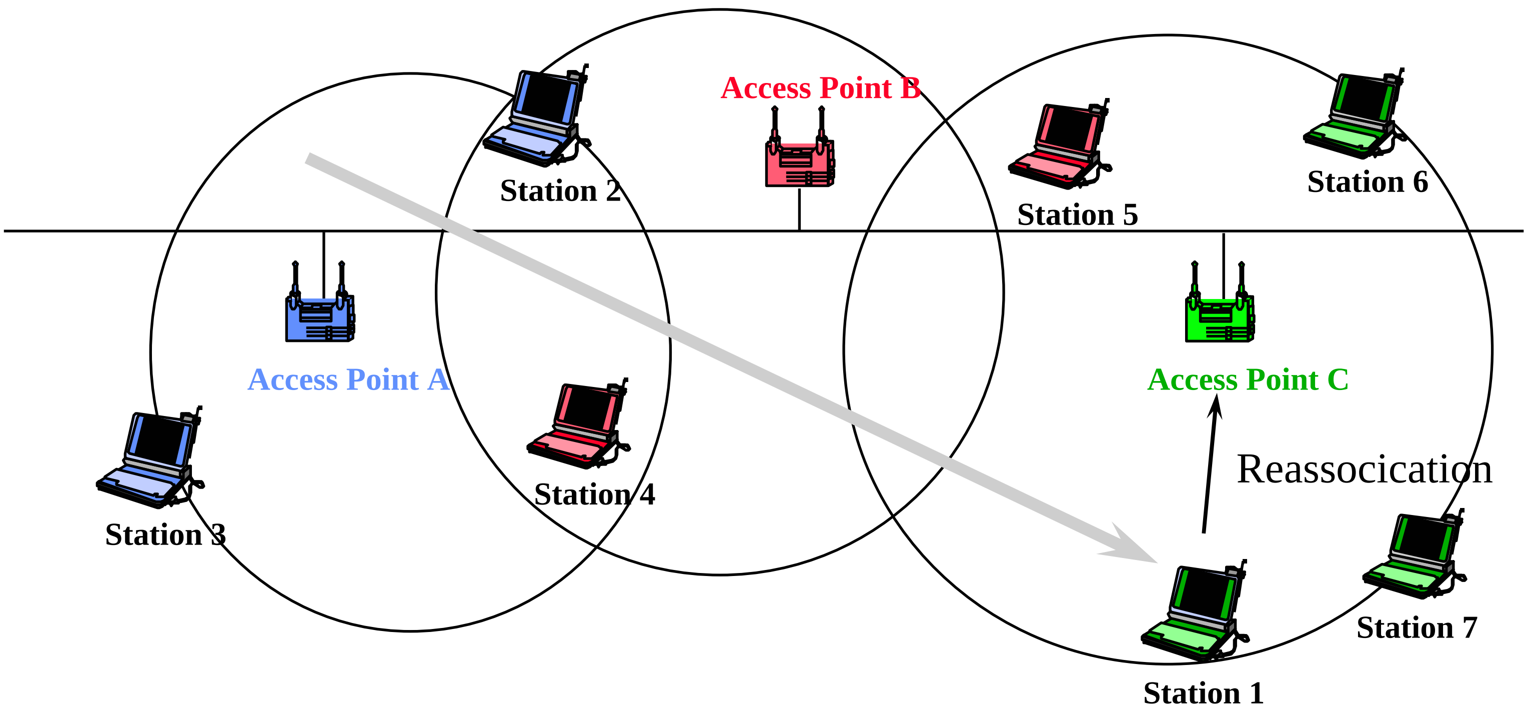


Wireless LAN Infrastructure Network



- **Each Station is Associated with a particular AP**
  - **Stations 1, 2, and 3 are associated with Access Point A**
  - **Stations 4 and 5 are associated with Access Point B**
  - **Stations 6 and 7 are associated with Access Point C**

Roaming



- **Mobile stations may move**
  - **beyond the coverage area of their Access Point**
  - **but within range of another Access Point**
- **Reassociation allows station to continue operation**

Roaming Approach

- Station decides that link to its current AP is poor
- Station uses scanning function to find another AP
  – or uses information from previous scans
- Station sends Reassociation Request to new AP
- If Reassociation Response is successful
  – then station has roamed to the new AP
  – else station scans for another AP
- If AP accepts Reassociation Request
  – AP indicates Reassociation to the Distribution System
  – Distribution System information is updated
  – normally old AP is notified through Distribution System