



Wireless-LAN & IEEE 802.11 standard

Pietro Nicoletti
Piero[at]studioreti.it



Copyright note

- These slides are protected by copyright and international treaties. The title and the copyrights concerning the slides (inclusive, but not only, every image, photograph, animation, video, audio, music and text) are the author's (see Page 1) property.
- The slides can be copied and used by research institutes, schools and universities affiliated to the Ministry of Public Instruction and the Ministry of University and Scientific Research and Technology, for institutional purpose, not for profit. In this case there is not requested any authorization.
- Any other complete or partial use or reproduction (inclusive, but not only, reproduction on discs, networks and printers) is forbidden without written authorization of the author in advance.
- The information contained in these slides are believed correct at the moment of publication. They are supplied only for didactic purpose and not to be used for installation-projects, products, networks etc. However, there might be changes without notice. The authors are not responsible for the content of the slides.
- In any case there can not be declared conformity with the information contained in these slides.
- In any case this note of copyright may never be removed and must be written also in case of partial use.



Wireless-LAN IEEE standard

■ 802.11

- Main/first standard operate at 2,4 GHz with 1 & 2 Mbps data rate
- Physical layer specify 2 transmission techniques:
 - DSSS = Direct Sequence Spread Spectrum
 - FHSS = Frequency-Hopping Spread Spectrum

■ 802.11b

- 802.11 extension, specify HR/DSSS (High Rate DSSS) transmission technique operating at 2,4 GHz with 5.5 & 11 Mbps data rate



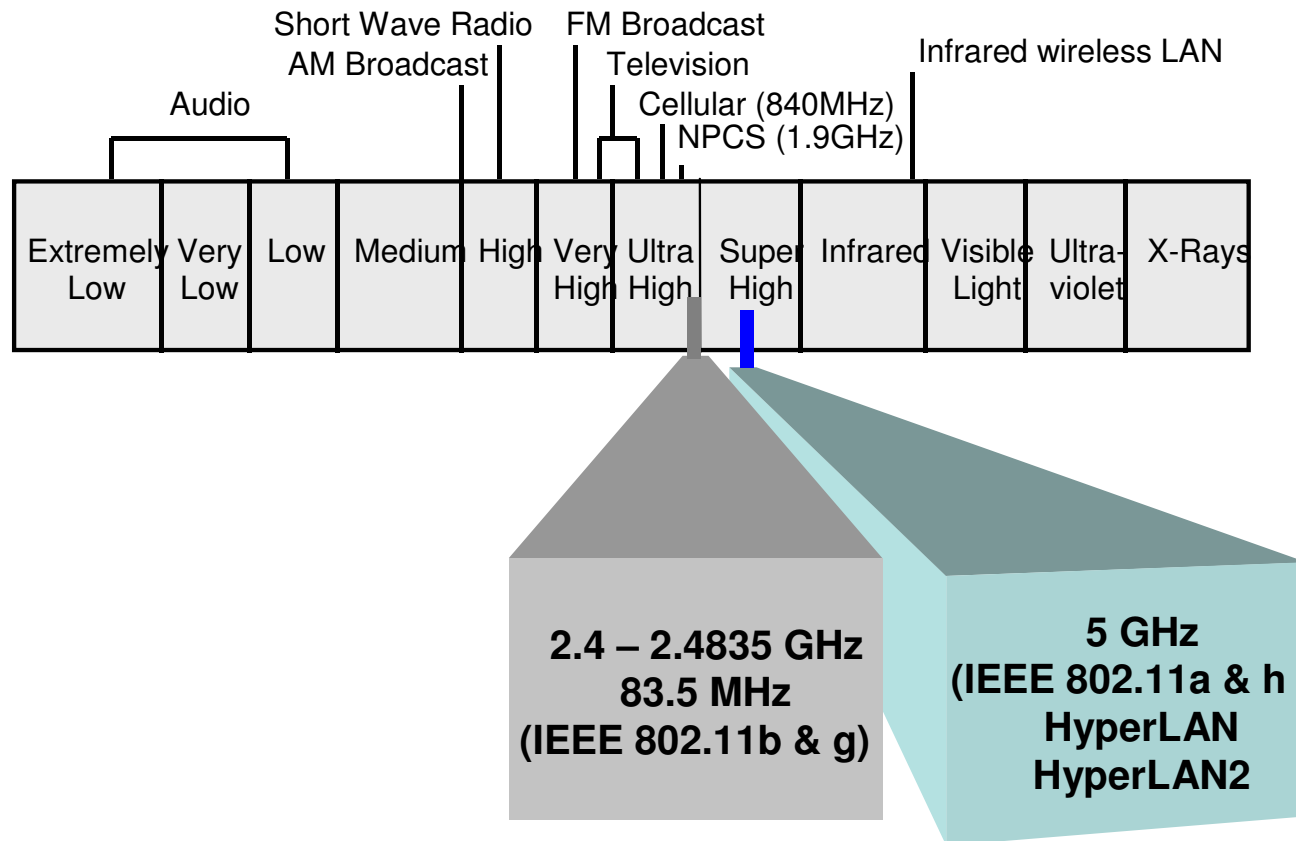
Wireless-LAN IEEE standard

■ 802.11a

- 802.11 standard extension operating at 5 GHz with different data rate up to 54 Mbps
- Physical layer specify OFDM (Orthogonal Frequency Division Multiplexing) modulation technique
- The frequency range is not conform to ETSI European normative



Wireless-LAN IEEE standard





IEEE 802.11 standard evolution

- Increase transmission speed
- 802.11g approved and published in June 2003
 - Operate at 2,4 GHz as 802.11b
 - Increase the speed up to 54 Mb/s
 - 802.11b backward compatibility
- 802.11h approved and published in September 2003
 - opera at 5 GHz as 802.11a, but with different frequency range conforming to ETSI European normative



802.11g speed

- IEEE 802.11 may operate:
 - In 802.11 compatibility mode
 - 1 & 2 Mb/s
 - In 802.11b compatibility mode
 - 5,5 & 11 Mb/s
 - 802.11g speed
 - 6, 9, 18, 22, 24, 33, 36, 48, 54 Mb/s

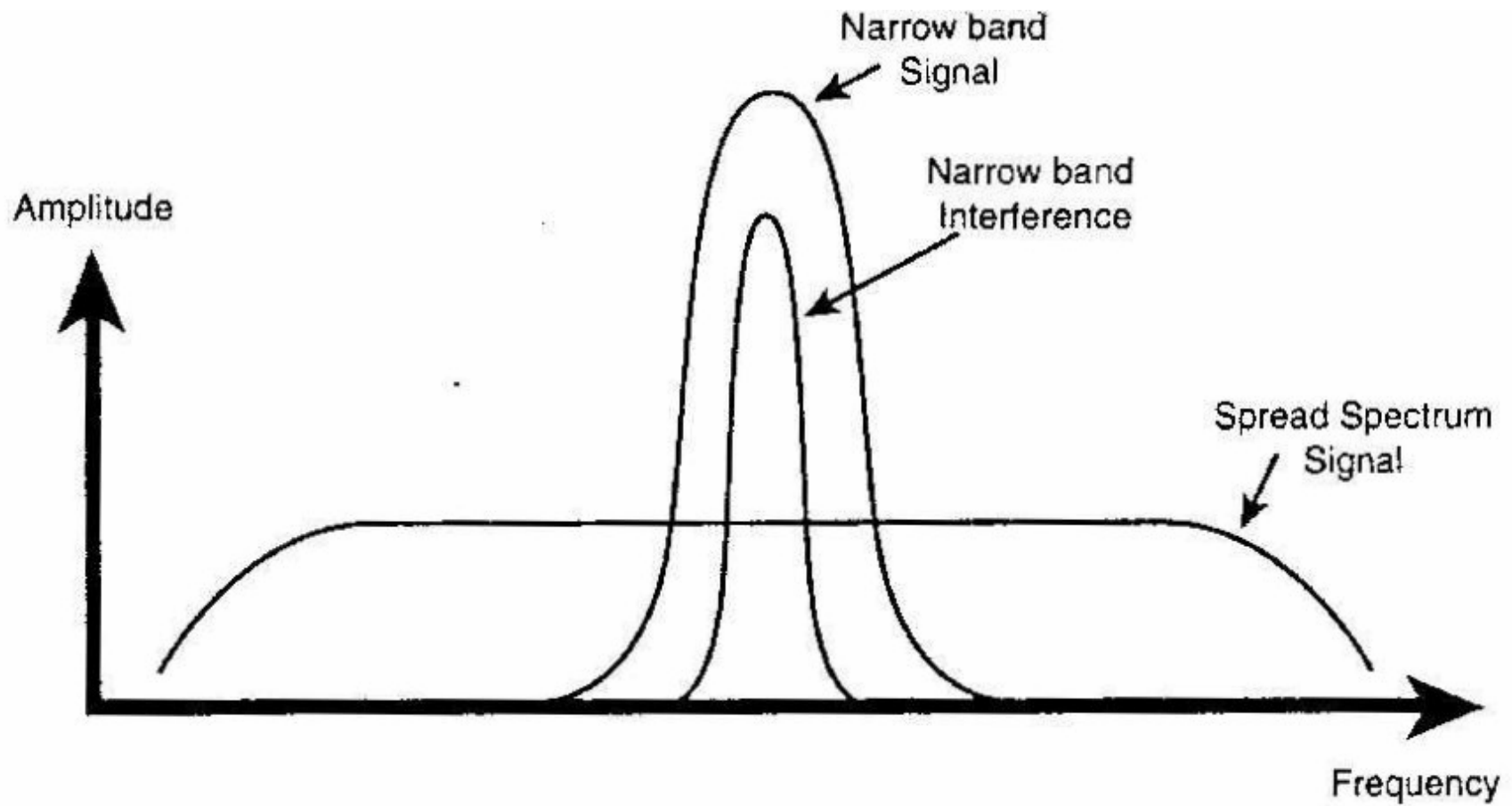


Spread Spectrum modulation

- Goals:
 - Increase transmission data rate
 - Reduce the SNR (Signal to Noise Ratio)
- Spread radio power over wide frequency range
 - Spread Spectrum Modulation reduce probability and effects of interference
- Spread Spectrum Modulation techniques:
 - frequency hopping
 - direct sequence



Spread Spectrum vs. Narrow Band





Frequency-Hopping Spread Spectrum

- The signal is modulated over a carrier which hops continuously frequency by frequency over a wide frequency range, following a ***hopping pattern***.
- Data rate:
 - 1 Mb/s with 2-level GFSK modulation
 - 2 Mb/s with 4-level GFSK modulation
- Hopping sequence and channel to use depending by the country
 - 79 hopping set for USA and Europe except Spain and France
 - 23 hopping set for Japan
 - 27 hopping set for Spain
 - 35 hopping set for France



Frequency-Hopping Spread Spectrum - Timing

- Channel switching/settling time = 224 μ s
- Dwell time on the channel
 - max dwell time 390 TU = 400 ms
 - Recommended dwell time value = about 19 ms
 - Increasing too much dwell time increases the interference probability
- In case of excessive Noise the signal will be retransmitted on the next hop frequency

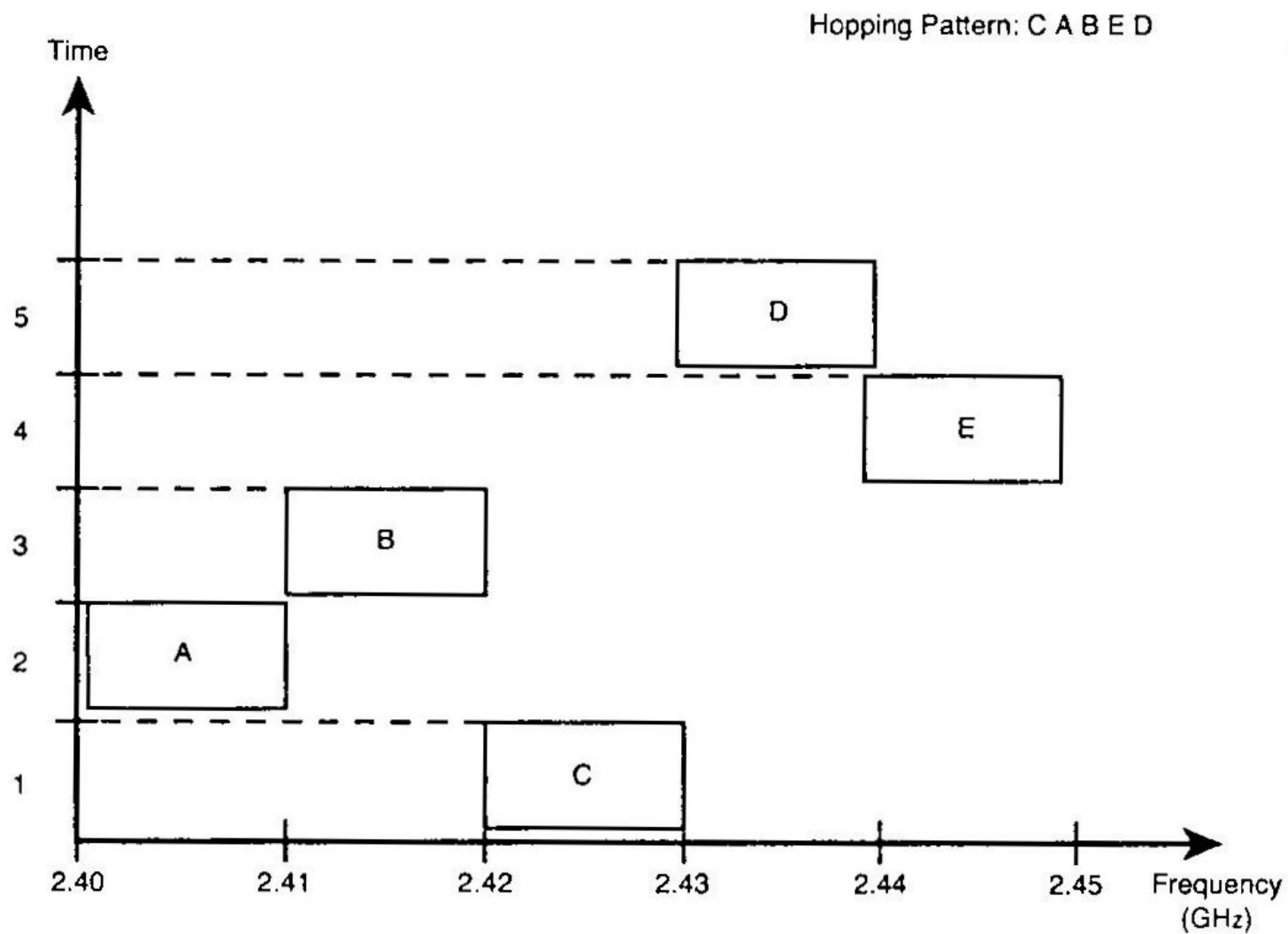


HOP sequence

- Hop sequences chosen to have more networks on the same area
 - 3 set of 26 sequence for USA and Europe except France and Spain
 - Any sequence use 26 different frequencies or channels
 - Set 1: $x =$
{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
 - Set 2: $x =$
{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
 - Set 3: $x =$
{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}



Hopping sequence example





802.11: Hopping channels for USA & Europe (1 MHz increment) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
2	2.402	28	2.428	54	2.454
3	2.403	29	2.429	55	2.455
4	2.404	30	2.430	56	2.456
5	2.405	31	2.431	57	2.457
6	2.406	32	2.432	58	2.458
7	2.407	33	2.433	59	2.459
8	2.408	34	2.434	60	2.460
9	2.409	35	2.435	61	2.461
10	2.410	36	2.436	62	2.462
11	2.411	37	2.437	63	2.463
12	2.412	38	2.438	64	2.464



802.11: Hopping channels for USA & Europe (1 MHz increment) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
13	2.413	39	2.439	65	2.465
14	2.414	40	2.440	66	2.466
15	2.415	41	2.441	67	2.467
16	2.416	42	2.442	68	2.468
17	2.417	43	2.443	69	2.469
18	2.418	44	2.444	70	2.470
19	2.419	45	2.445	71	2.471
20	2.420	46	2.446	72	2.472



802.11: Hopping channels for USA & Europe (1 MHz increment) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
21	2.421	47	2.447	73	2.473
22	2.422	48	2.448	74	2.474
23	2.423	49	2.449	75	2.475
24	2.424	50	2.450	76	2.476
25	2.425	51	2.451	77	2.477
26	2.426	52	2.452	78	2.478
27	2.427	53	2.453	79	2.479
—	—	—	—	80	2.480



DSSS = Direct Sequence Spread Spectrum

■ DSSS Technique

- A bit flow is converted in a symbol flow
 - symbol represent a different bit number depending by coding technique
 - Symbol is converted in signal that is conveyed to spreader
- spreader combine input signal with Pseudo-Noise sequence called *chip sequence*
 - 11-chip Barker sequence on 802.11
 - CCK (complementary code keying) on 802.11b
- Combination result is a signal spreaded on a wider frequency band

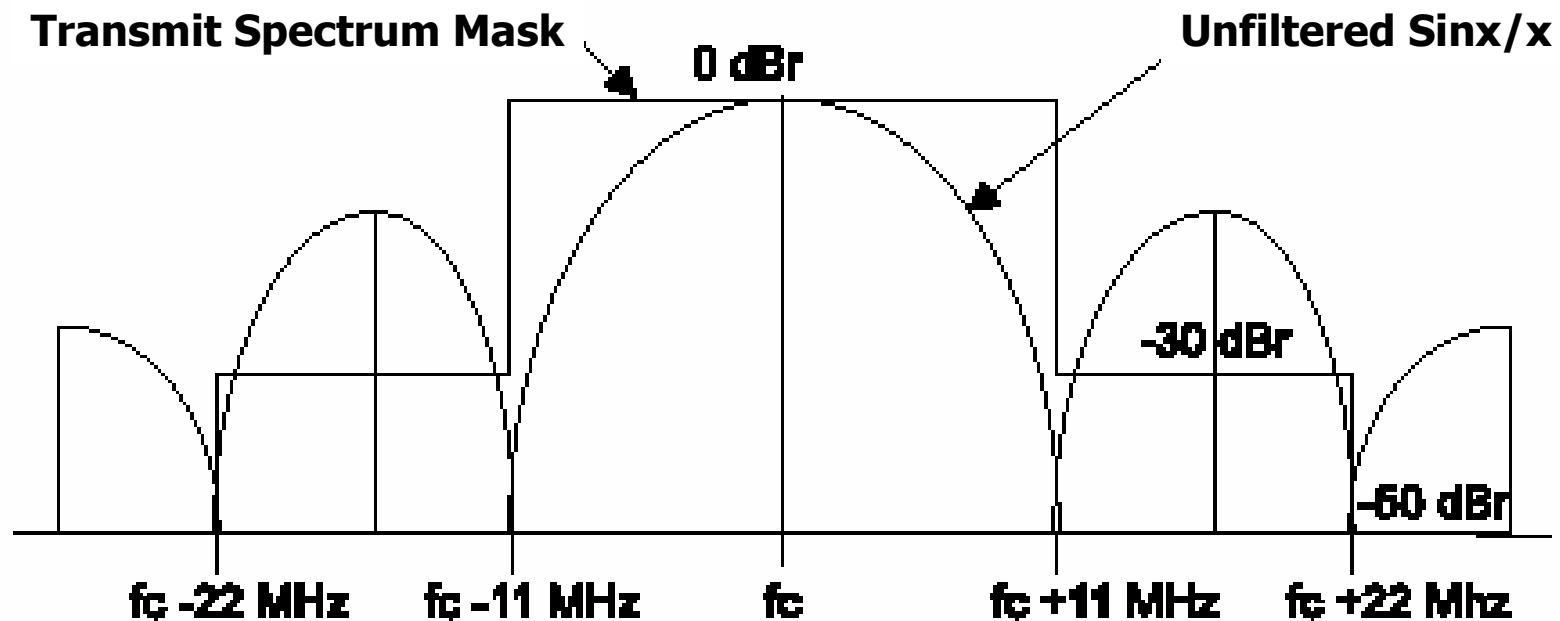


802.11 DSSS

- Operate at 1 or 2 Mb/s
 - 1 Mb/s with Differential Binary Phase Shift Keying (DBPSK) modulation
 - 2 Mb/s with Differential Quadrature Phase Shift Keying (DQPSK) modulation
- 14 channels available:
 - Frequency range 2,412 GHz - 2,484 GHz
 - 5 MHz channel distance between channels except channel 14 dedicated for Japan
 - Channel use depending by country normative
 - a channel cover a frequency spectrum of 22 MHz



802.11 DSSS: theoretical spectrum mask





802.11b: extension speed up to 11Mb/s

- Adopt HR/DSSS (High Rate DSSS) modulation technique
- Operate at 2,4 GHz with 1, 2, 5.5 e 11 Mbps data rate
 - Differential Binary Phase Shift Keying (DBPSK) modulation for 1 & 5,5 Mbps transmission speed
 - Differential Quadrature Phase Shift Keying (DQPSK) modulation for 2 & 11 Mbps transmission speed
- Adopt CCK (Complementary Code Keying) coding scheme for Pseudo-Noise sequence for speed 5,5 Mb/s & 11 Mb/s instead 11-chip Barker sequence



Overlapping channels

- Not overlapped channels
 - Minimum 25 MHz distance from central frequency
 - May operate in the same cell/area without interference
- Overlapping channels
 - Operate in adjacent cell/areas partially overlapped;
 - Minimum 15 MHz distance from central frequency
 - Signal interference ratio
 - minimum 6 dB over interference signal at 2 Mb/s
 - minimum 12 dB over interference signal at 11 Mb/s



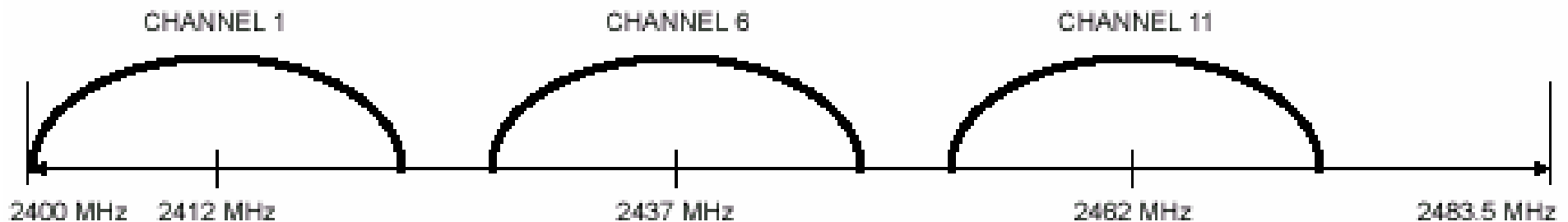
DSSS & channels to be used in different country

CHNL_ID	Frequency	Regulatory domains					
		X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' 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	X	X	—
11	2462 MHz	X	X	X	X	X	—
12	2467 MHz	—	—	X	—	X	—
13	2472 MHz	—	—	X	—	X	—
14	2484 MHz	—	—	—	—	—	X



USA: DSSS not overlapped & overlapping channels

- 3 not overlapped channels may be used on the same cell/area
 - 1,6,11

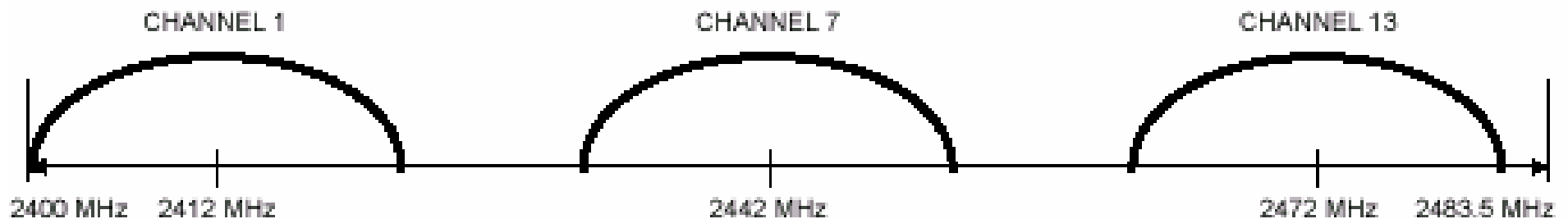


- 4 overlapping channels may be used on adjacent cell/area partially overlapped
 - 1, 4, 7, 11



Europe: DSSS not overlapped & overlapping channels

- 3 not overlapped channels may be used on the same cell/area
 - 1, 7, 13

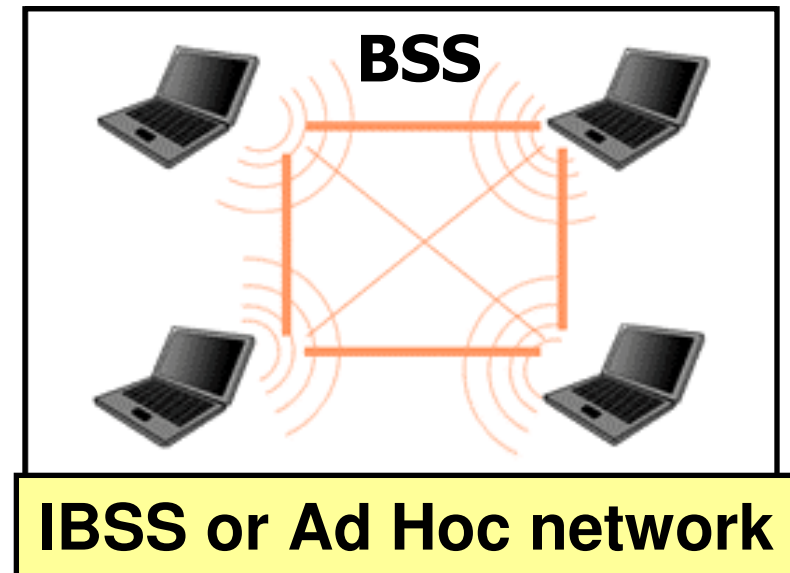


- 5 overlapping channels may be used on adjacent cell/area partially overlapped
 - 1, 4, 7, 10, 13



802.11 - IBSS network topology

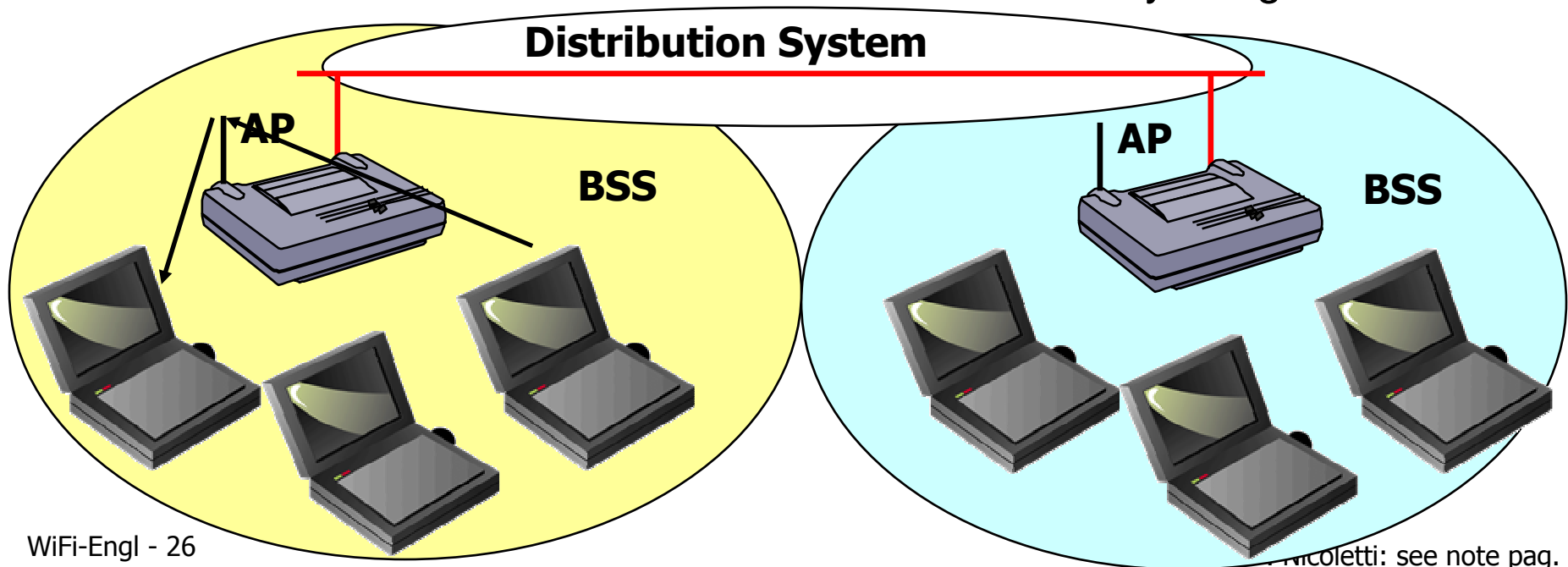
- Independent Basic Service Set (IBSS) called *Ad Hoc Network*
 - Station (STA) group located in the same area (BSA=Basic Service Area) that form an assembly called Basic Service Set (*BSS*)
 - In Ad Hoc network the communication model is peer-to-peer between stations
 - WLAN use a ether shared transmission media called *Wireless Medium*
 - **No access Point needed**





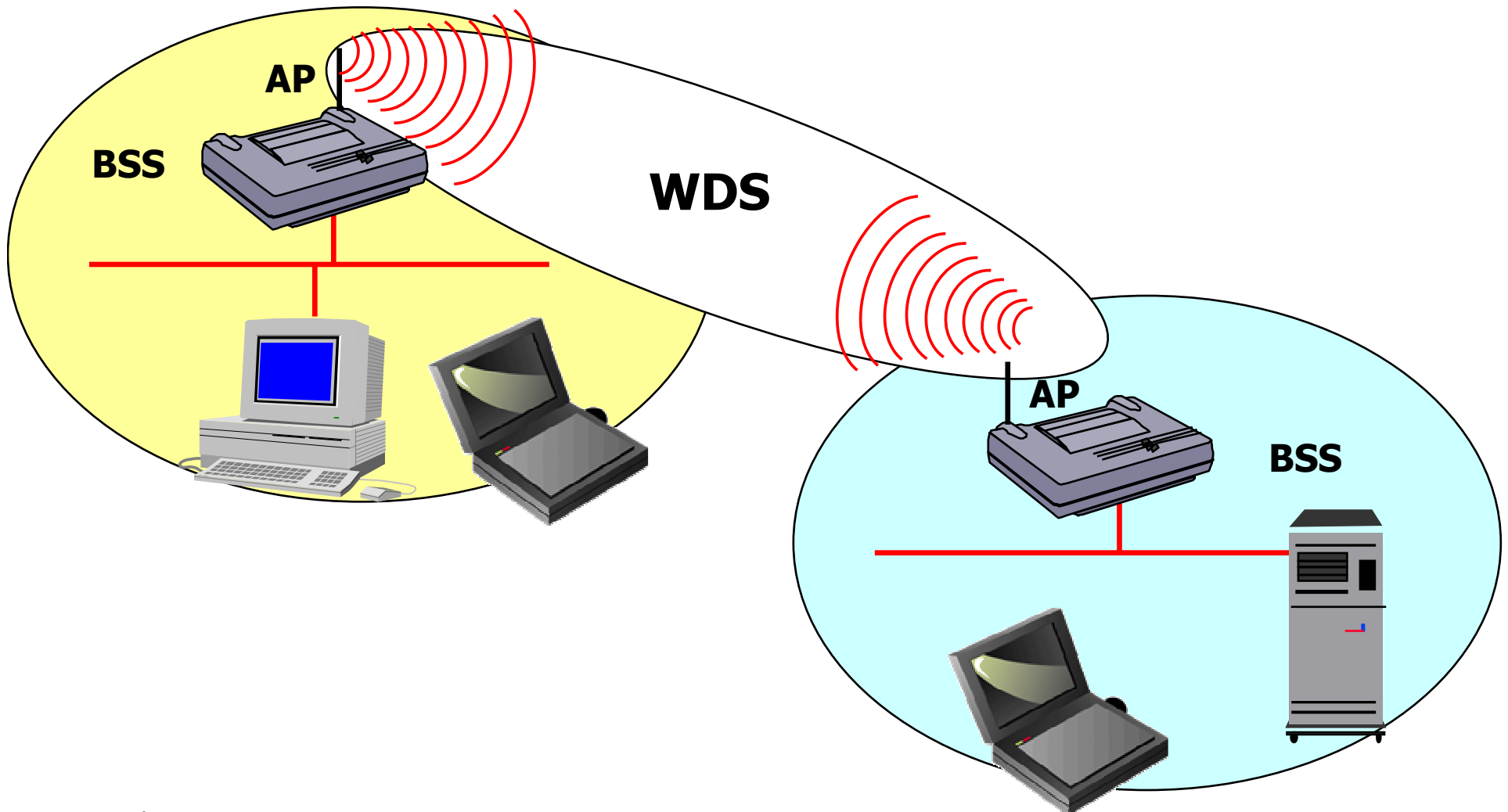
802.11 – ESS network topology

- ESS network topology called *Infrastructure Network*
- Extended Service Set (ESS):
 - A LAN form a Distribution System witch connect one or more BSS via Access Point (AP)
 - Frame are sent e received from/to AP
 - Station on the same BSS communicate only trough AP





802.11 - ESS with Wireless Distribution System (WDS)





Coordination Function

- All stations located in the Basic Service Area are under control of coordination function that can be:
 - Distributed
 - DCF = Distributed Coordination function
 - DCF is implemented in every station
 - Concentrated, based on Master/slave concept
 - PCF = Point Coordination Function
 - Master poll periodically every station
- Coordination function establish if the station can participate at BSS and can communicate in the BSA trough WM (WM=Wireless Medium)



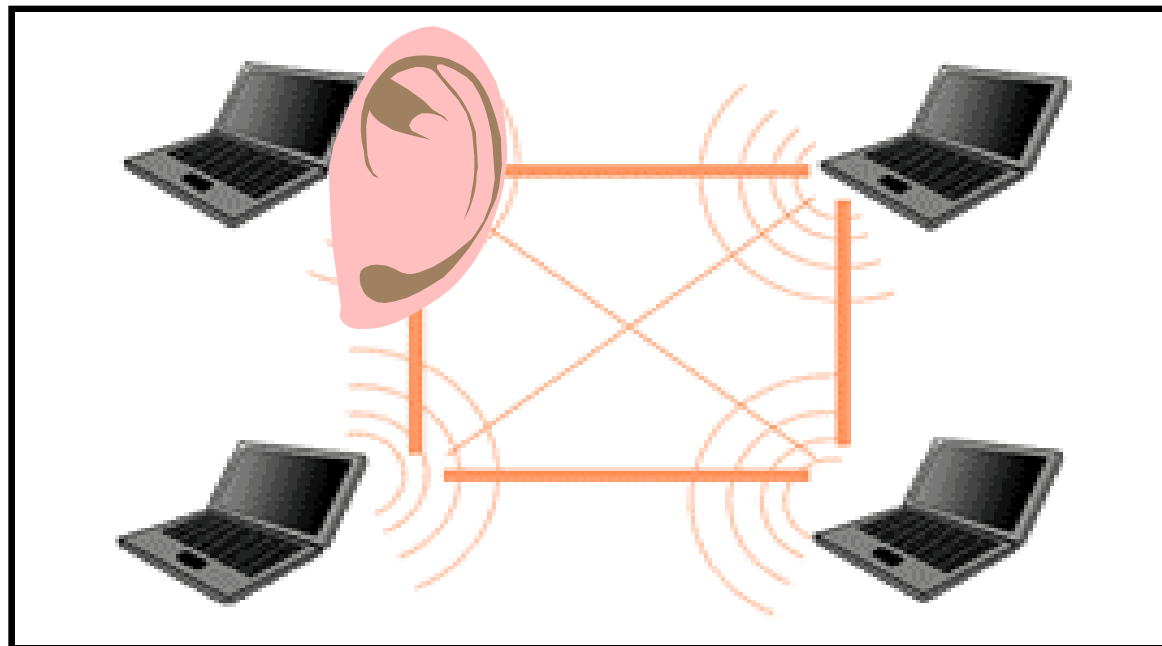
Station insertion in a BSS on Ad Hoc Network topology

- Station that want participate at BSS need to tune and synchronize with other stations
 - In Ad Hoc network station perform a ***passive-scanning***



Passive scanning

- Scan all possible channels listening for a short time looking for a *beacon*
 - When receive a beacon compare SSID contained on it with own SSID, if the contents is the same can communicate on that IBSS





Beaconing

- Beacon is a management frame containing information like:
 - Service Set ID (SSID) and timestamp necessary to synchronize stations
- In Ad Hoc network all stations participate to beacon frame generation



Active scanning

- Possible only in Infrastructured Network (ESS topology)
 - Access Point (AP) permit and control station association to that BSS using an handshaking protocol based on probe/association request/response management frames



Active Scanning

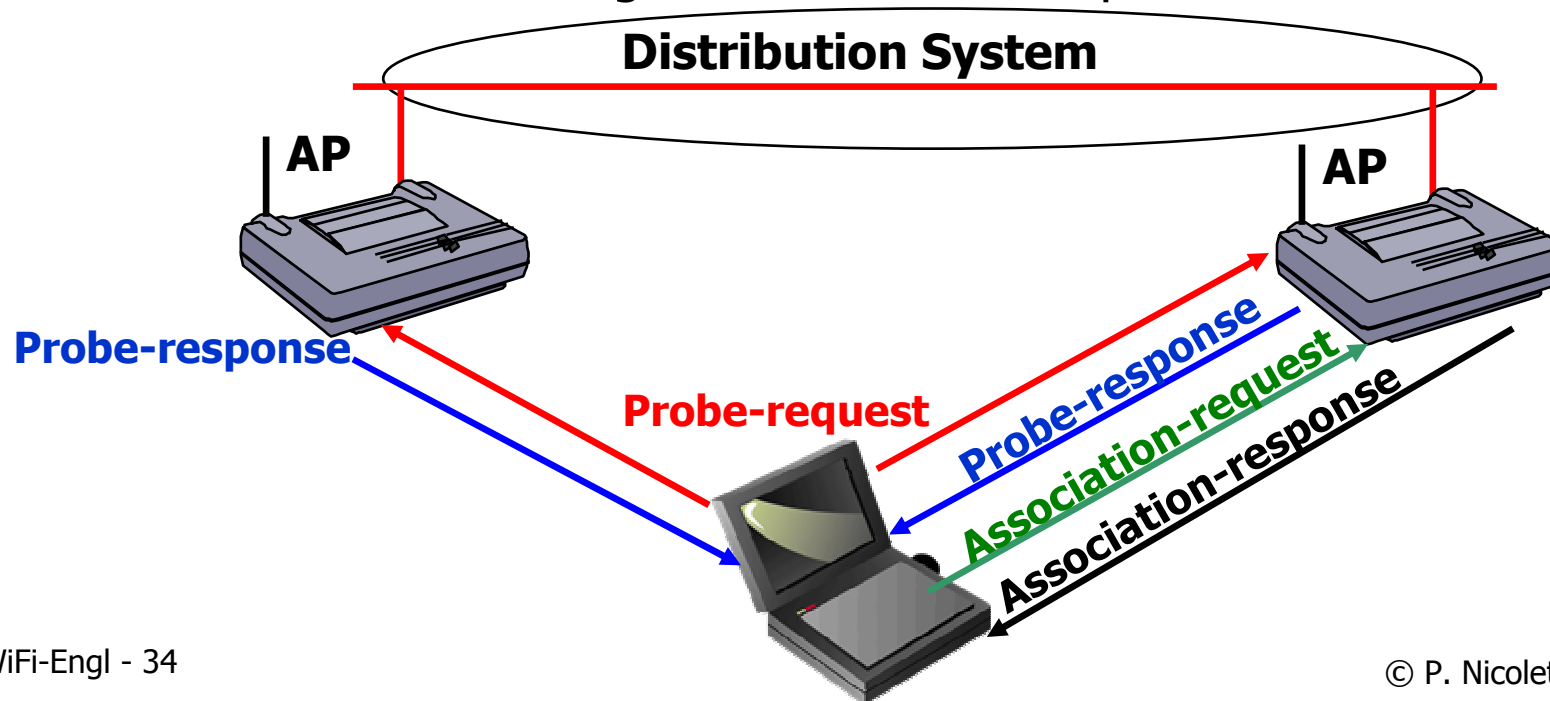
- Station that want to participate to a BSS:
 - Send a Management *Probe-Request* frame in broadcast
 - Wait for a short time expecting to receive a *Probe-Response* frame from Access Point
 - If do not receive *Probe-Response* frame try in an other channel



Active Scanning & association

■ Procedure

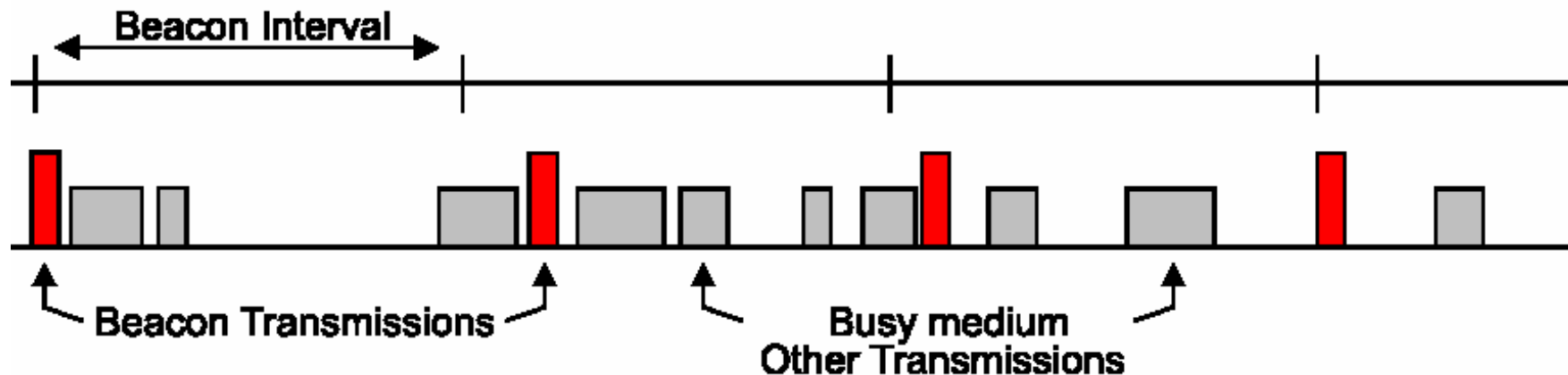
- Station send Probe-Request frame
- One or more AP may answer with Probe-Response frame
- Station select best AP (better signal & SNR) and send an Association-Request frame
- AP answer sending an Association-Response frame





Beacon in unfractured network

- Any Target Beacon Transmssion Time (TBTT) Access Point prepare a Beacon frame. If the WM is free transmit Beacon if WM is busy Access Point delay Beacon frame Transmission.



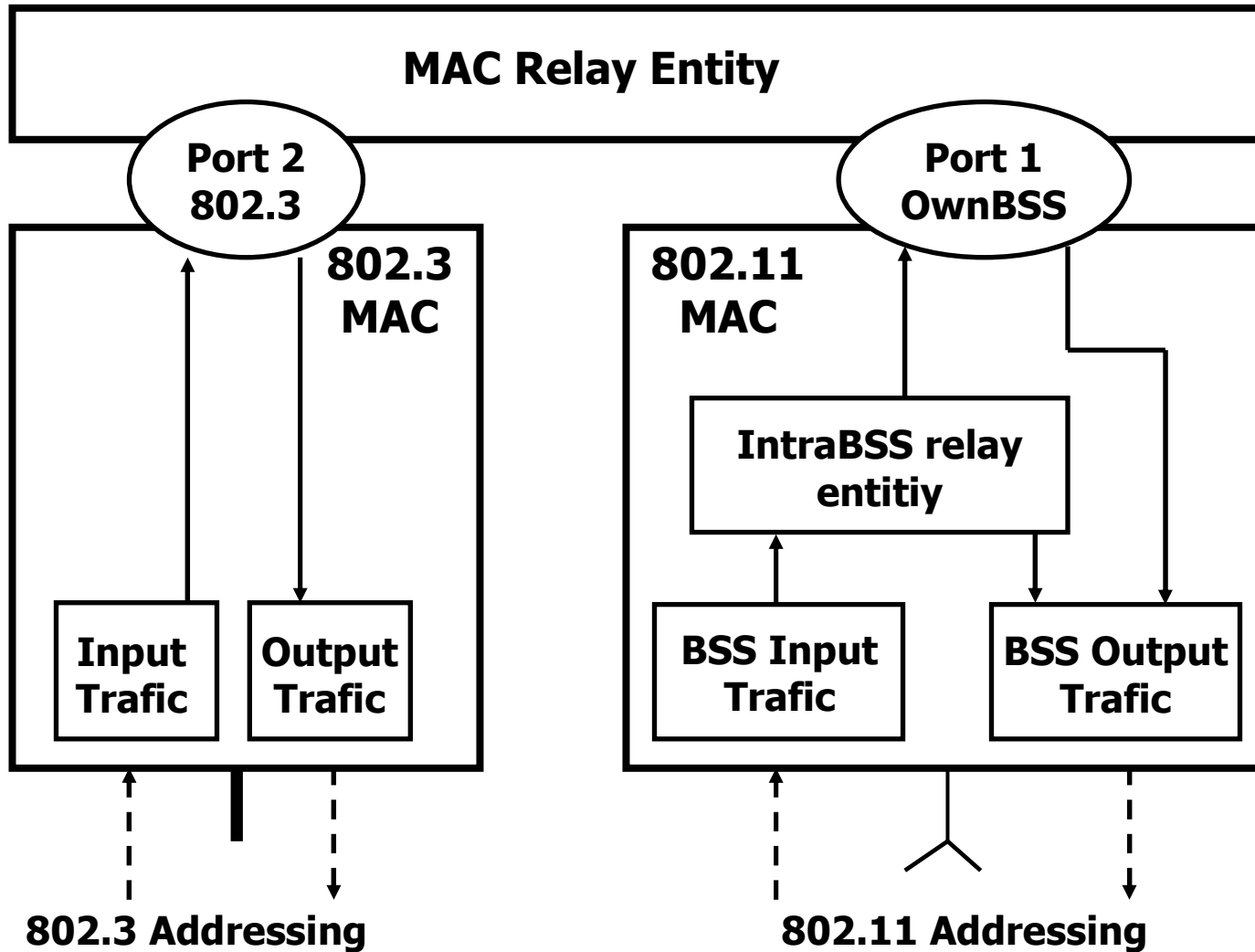


Access Point (AP)

- Access Point is an entity which permit MAC Services distribution via Wireless Medium for the associated stations with it.
 - It work as a local bridge with limited bridging functions:
 - Have a table containing only MAC Addresses of associated wireless stations
 - Forward and filter packet between Wireless and Wired LAN.
 - Cover a certain area, depending on AP and Station characteristics
 - Permit roaming between BSS (or cell)
 - Can work in repeater mode
 - The bridging function realize translation between Ethernet and Wireless frame and buffering.
 - It work with a concept of Default Route for the data destined to wired LAN



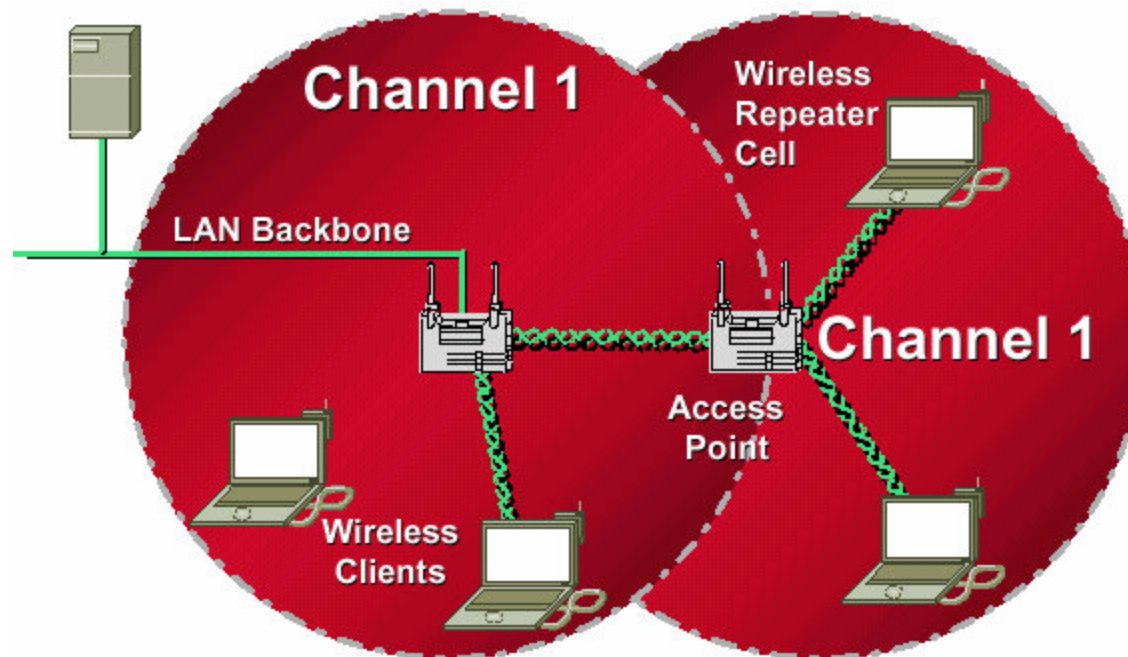
AP transparent bridged architecture





L'Access Point working in Repeater mode

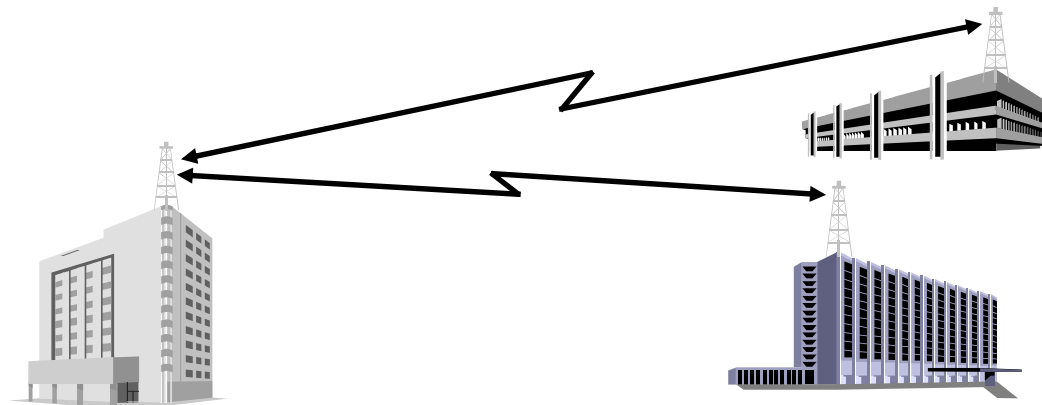
- Access Point can work as Repeater in the WM:
 - Use same channel than Root-AP
 - Retransmit frame on the Cell
 - The station in the overlapped cell area chose the AP with better signal
 - AP as Repeater increase the traffic and reduce the transmission efficiency





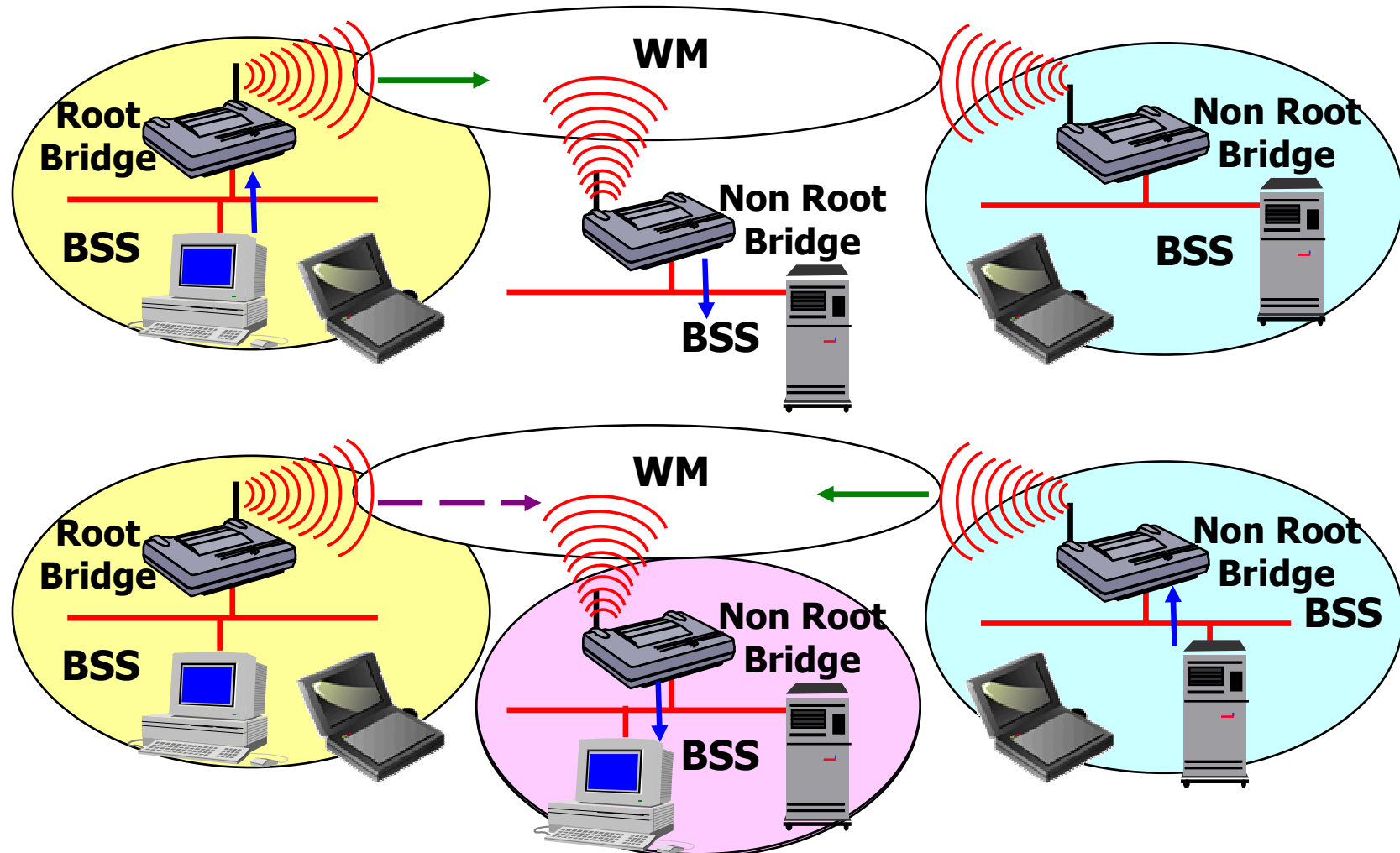
Wireless Bridge

- Normally used to bridge Wired LAN via Wireless Medium
 - Full bridging functions
 - One Bridge in the WM must be configured as Root-Bridge, other bridge must be configured as Non-Root-Bridge
 - Non-Root-Bridge can't communicate directly, they can communicate through Root-Bridge





Wireless Bridge Transmission cases





802.11 MAC

- 2 Medium Access methods
 - DCF (Distributed Coordination function) which implement CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) with Acknowledgement ACK Medium Access method
 - PCF (Point Coordination Function) based on polling realized Access Point to enable station to transmit data
 - Ideal for real-time applications



CSMA-CA: Carrier Sense Multiple Access Collision Avoidance

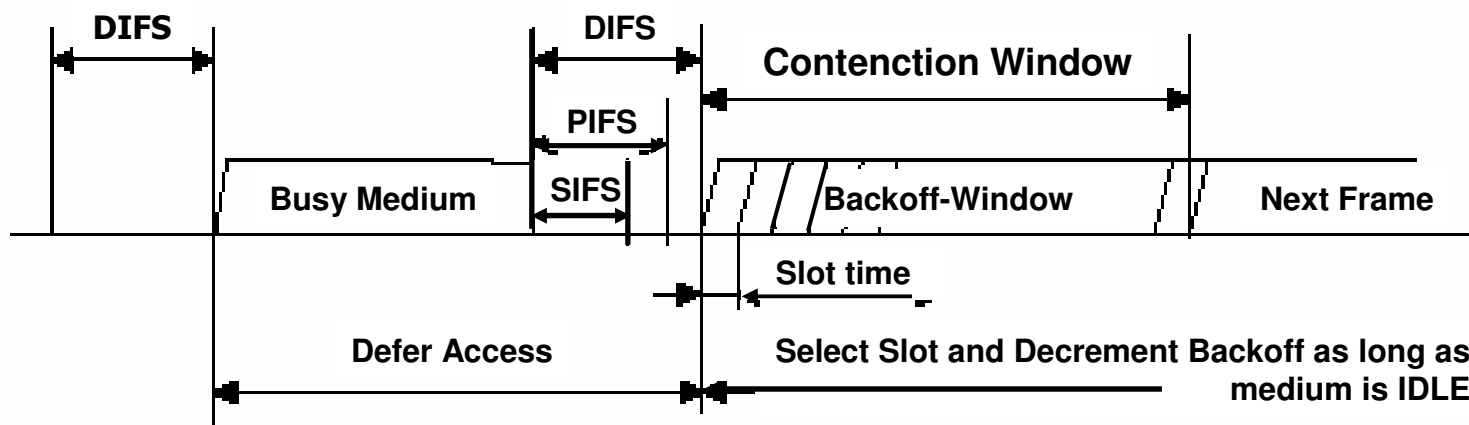
- Wireless LAN differ from Ethernet LAN because the station can't listen during transmission instead of Ethernet witch *listen while talking*. For that reason Wireless Station can't detect collision and need to avoid collision.
 - Station "listen" WM (Carrier Sense) before transmit il WM (listen before talking).
 - If WM is free for a time higher than DIFS (Distributed (coordination function Interframe Space) STA transmit, otherwise wait for end of transmission and compute a backoff time using a random (exponential random backoff) function to prevent collision.
 - Station with smaller back-off time value win the WM contention.



CSMA-CA: Inter Frame Spacing & contention

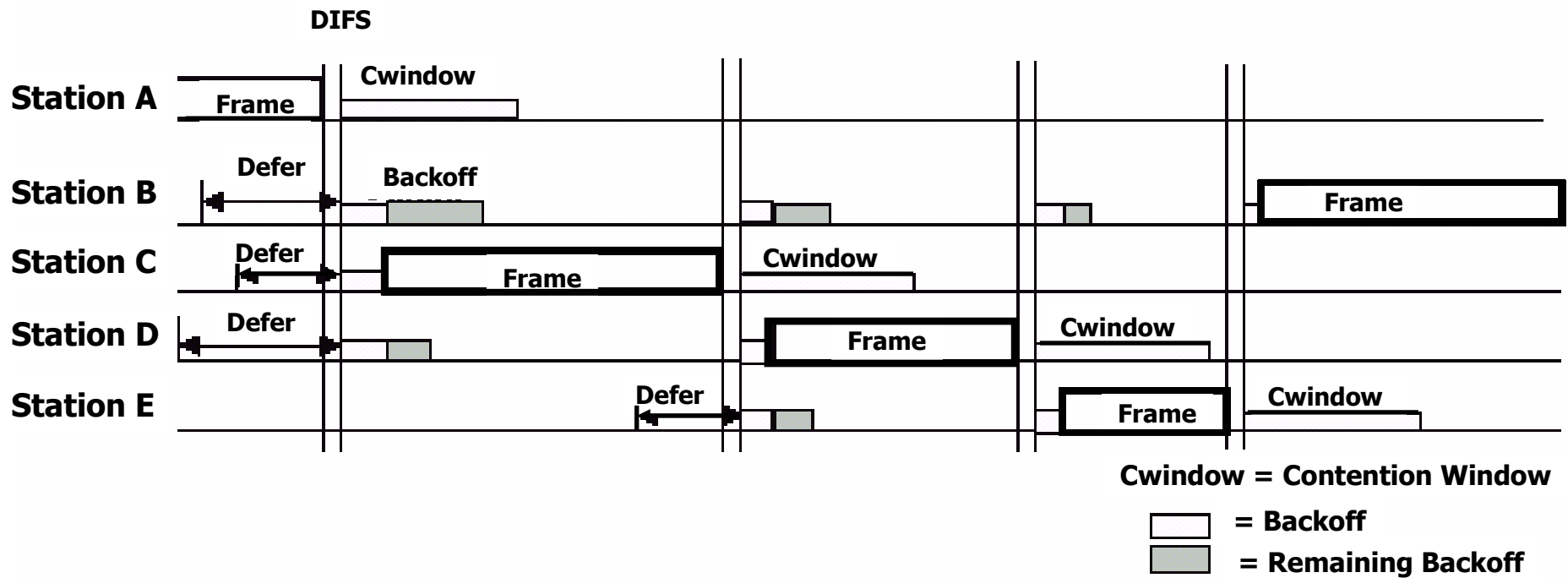
- Inter Frame Spacing types:
 - DIFS: DCS Inter Frame Space
 - PIFS: PCF Inter Frame Space
 - SIFS: Short Inter Frame Space
- BackoffTime = Random()*SlotTime

Immediate access when medium is free \geq DIFS





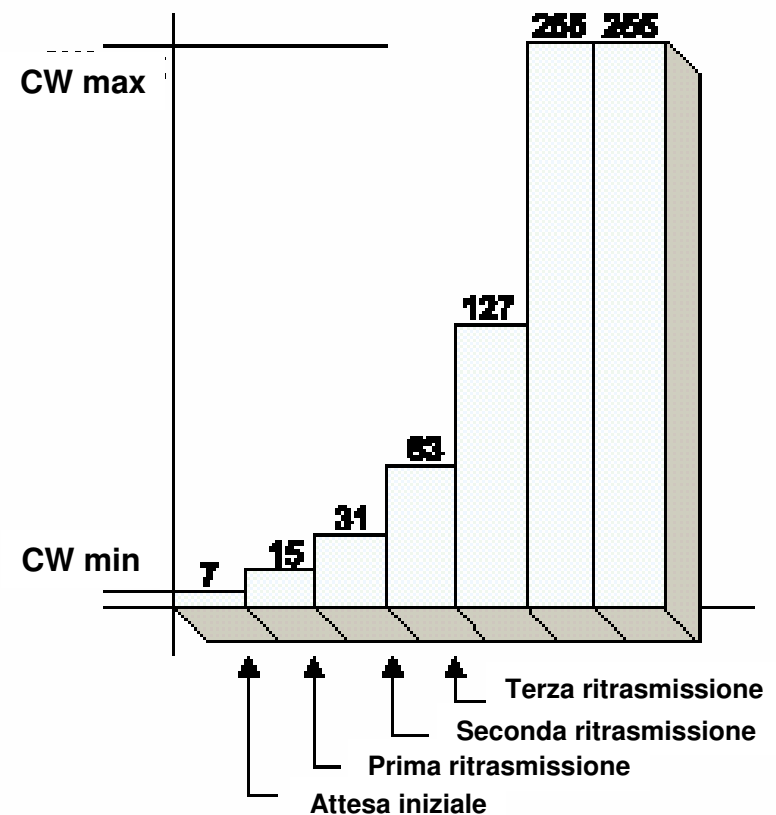
Backoff procedure





CSMA-CA: Exponential Random Backoff

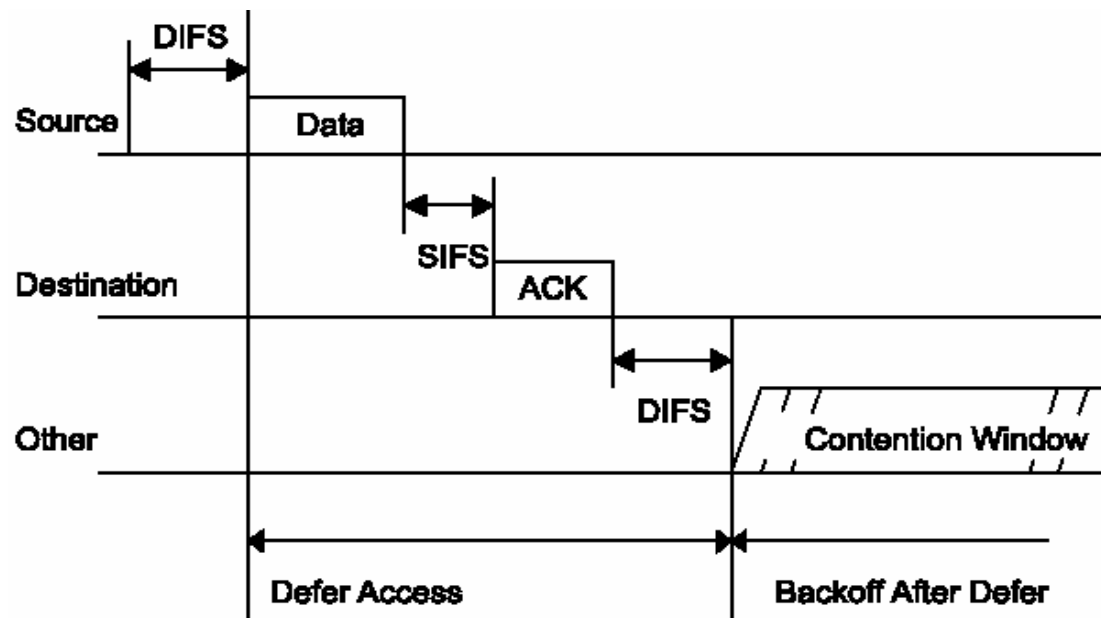
- Used when:
 - STA want to transmit but WM is busy;
 - Before any retransmission;
 - After any MPDU transmission with success;
 - BackoffTime = Random()*SlotTime
 - Random value chosen between values CWmin (Collision window min) e CWmax
 - $CWmin \leq CW \leq CWmax$





CSMA-CA with Acknowledgement ACK

- Acknowledgement ACK: is a Control Frame used to confirm a correct frame reception (correct CRC)
 - Receiving station wait for a time SIFS (Short Inter Frame Spacing) before send ACK
 - If Source station do not receive ACK within timeout set l'Exponential Random Backoff and retransmit frame.





CSMA-CA with Acknowledgement ACK

- Acknowledgement is not sent as answer for Multicast or Broadcast frame
- If the frame sent by transmitting station in the WM is designated to Distribution System (DS) Access Point is responsible to send ACK in case of correct frame reception.
- If the frame is coming from DS and is designated to a Station in the WM, (AP forward frame to WM), destination station send ACK in case of correct frame reception.
 - IF Access Point do not receive ACK, within certain time, set Exponential Random Backoff and retransmit frame.



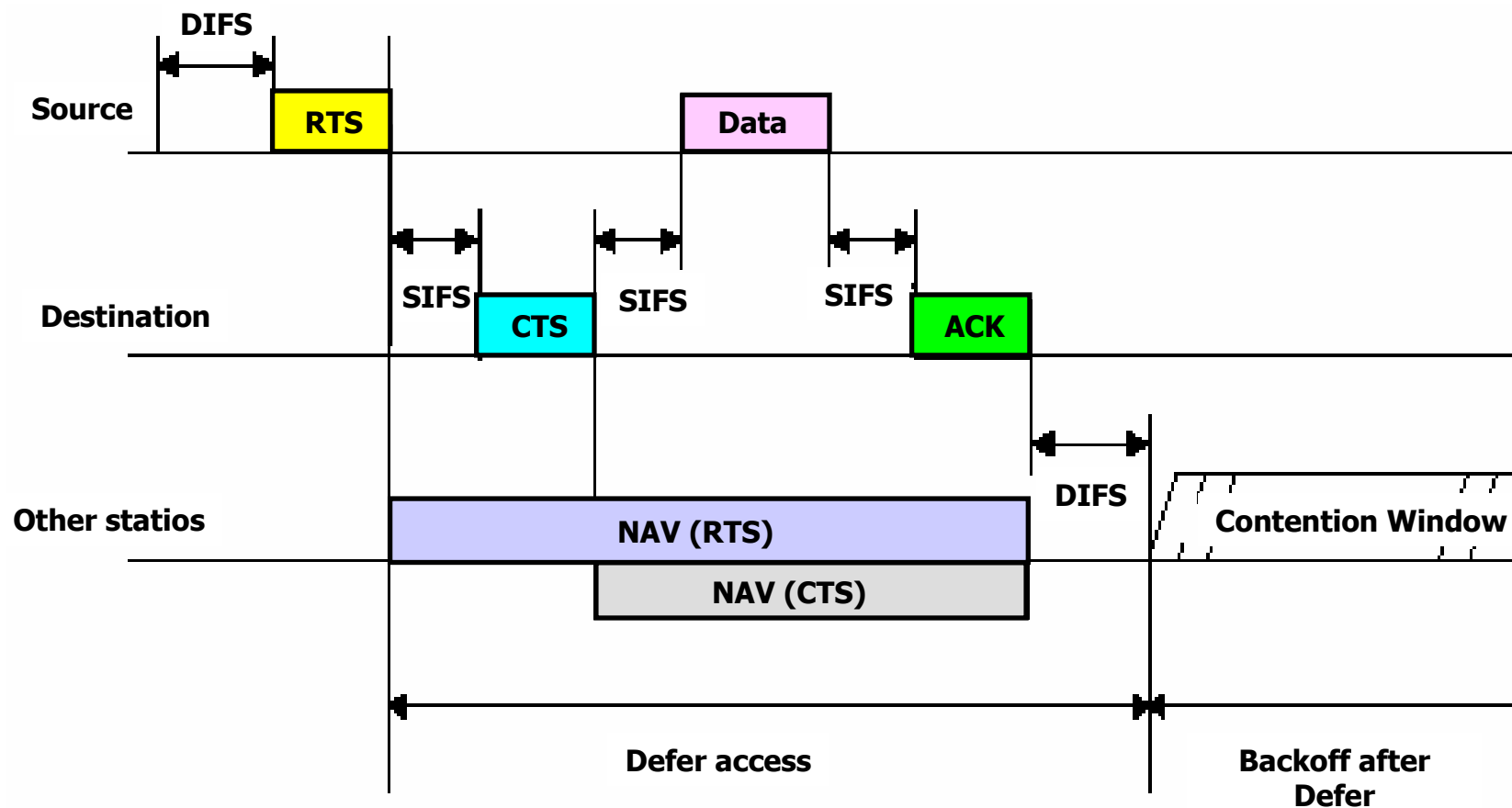
RTS/CTS & virtual carrier sense

- During transmission Station can't detect collision because is not able to hear own transmission.
- For better collision prevention AP realize virtual carrier sense by using **RTS** and **CTS** control frame witch contain information about next transmission duration
 - Stations for witch the frame is not designated load information about next transmission duration in **NAV** (Network Allocation Vector) register
 - For the time loaded in NAV register station can't transmit frames

Note: RTS = Request To Send, CTS = Clear To Send



Transmission procedure with RTS & CTS





Frame fragmentation

- Fragmentation is optional, frame reassembly is mandatory
 - Fragmentation may improve transmission performance in noising environment were the quality signal is poor
 - Shorter frame are more immune at noising
 - Fragmentation create an overhead consuming bandwith



Roaming

- 802.11 standard support roaming through scanning and reassociation functions
- Roaming use scanning function, or previous data obtained by previous scanning, to find another AP.
- When station detects a poor quality signal (attenuation and bad SNR):
 - Send an Reassociation Request control frame to new AP.
 - If the new AP sends an Reassociation Response Station is associated to new AP otherwise look for another AP.
- If AP accepts Reassociation Request:
 - Inform DS about Reassociation
 - Old AP is informed about new reassociation through DS



Power Management on Infrastructured network (ESS)

- A station may be in 3 different state:
 - *Transmit*
 - *Awake*: Station is continuously powered.
 - *Doze*: Station is not enable to transmit and receive frame. Low power consumption.
- Station may work in 2 way:
 - Active Mode (AM).
 - Power Save mode (PS).



Power Management - Active Mode

- Station may receive frame at any time.
- Station is always in Awake state.



Power Management – Power Save Mode (PS)

- Station listen for Beacons
- If one of the beacon received contain TIM (Traffic Indication Map) identifying the STA for which traffic is pending and buffered in the AP. The Station understand that AP have data to be transmitted
 - Station transmit a PS-Poll control frame to AP, than AP transmit data to the station
- Station in PS mode still remain doze status except to hear Beacons, transmit PS-Poll, receiver buffered data from AP
- Station entering in Power Save send inform AP PwrMgt bit in the del Frame Control



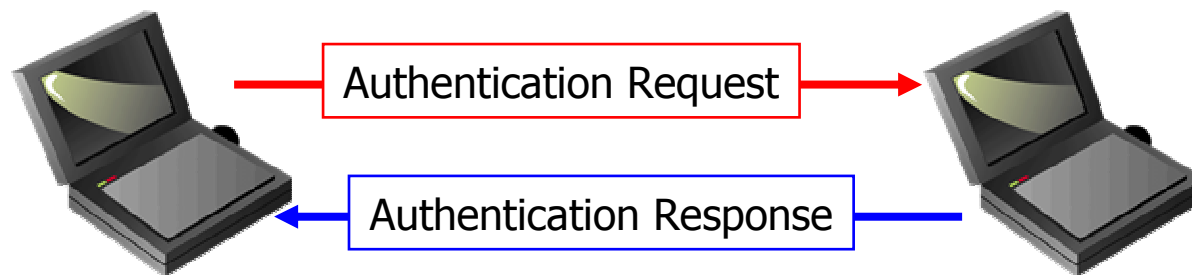
Authentication

- Authentication is the service used to establish the identity of one station as a member of the set of stations authorized to associate with another station.
 - Open System.
 - Shared Key.
- Between AP and STA in infrastructured network, between 2 STAs in Ad Hoc network.



“Open System” authentication

- Default configuration on AP and interfaces
 - Dangerous configuration if are not implemented other authentication systems



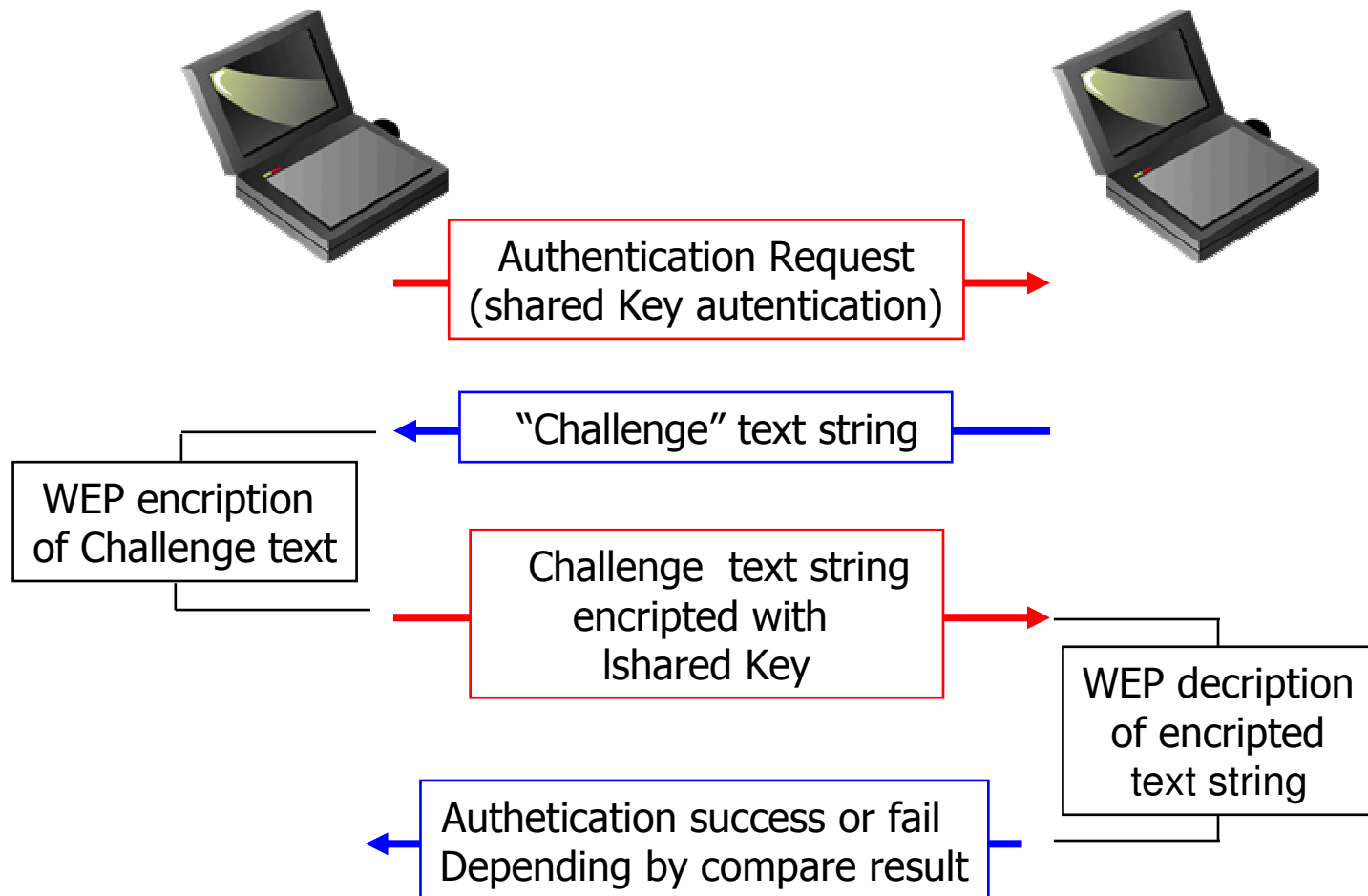


WEP & “Shared Key”

- WEP (Wired Equivalent Privacy) 2 main functions:
 - Authentication
 - Data encryption
- “Shared Key” Authentication implemented in 802.11 with WEP adoption
 - Every station and AP must have the same key (shared)



WEP Authentication steps





Wireless users mobility

- Goal: hold connection of users moving cell by cell
- Implemented with IAPP (Interaccess Point Protocol)
 - Draft 802.11F
 - 2 protocols developed to permit user mobility: Announce Protocol and Handover Protocol



IAPP protocols

■ Announce Protocol

- Access Point coordination
- Inform other AP about activity of one AP
- Inform AP about new network configuration

■ Handover Protocol

- Inform Access Point when a station is reassocated to an other Access Point
- Old AP send frame designated to station to new AP via Distribution System
- New AP modify the filtering data base to send data to new station