
Wireless Medium Access Control

Una discussione sui problemi e possibili soluzioni.

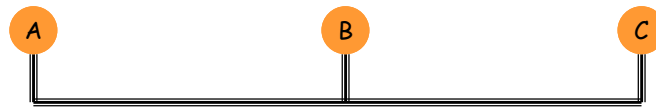
Wired Vs Wireless Media Access

Entrambe usano un mezzo condiviso.

Quindi, quali sono le differenze significative?

L'accesso al mezzo in un canale wired

- Diversi nodi condividono lo stesso canale

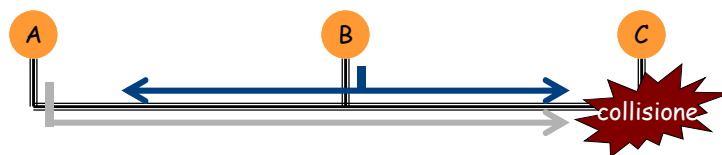


- La comunicazione avviene di solito fra coppie di nodi
 - La comunicazione simultanea non è però possibile

- MAC Protocols
 - Suggestiscono come organizzare la comunicazione
 - **Massimizzano** il numero di comunicazioni
 - Garantiscono la **fairness** fra i vari trasmettitori

Corso di Reti per Automazione Industriale 3

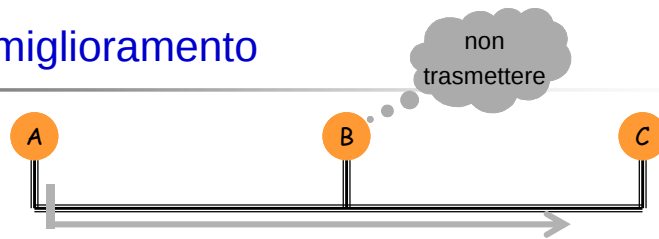
La soluzione più banale



- Trasmetti e prega
 - Abbondanza di collisioni --> il Throughput è basso con carico elevato

Corso di Reti per Automazione Industriale 4

Un miglioramento



Possano ancora verificarsi collisioni?

■ Trasmetti e prega

- Abbondanza di collisioni --> il Throughput è basso con carico elevato

■ Ascolta prima di trasmettere

- Carrier sense multiple access (CSMA)
- Rimanda la trasmissione se il canale è occupato

Corso di Reti per Automazione Industriale

5

CSMA e collisioni

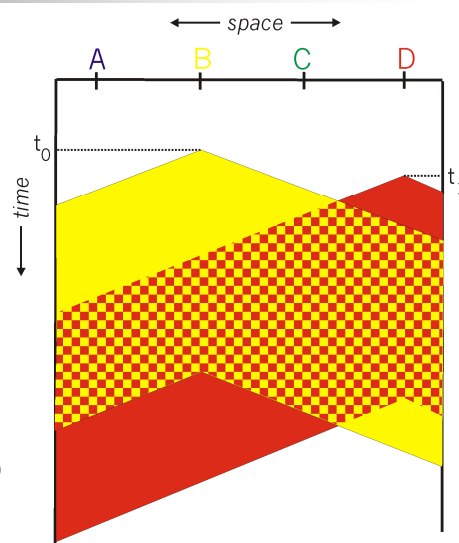
Collisioni possono ancora verificarsi:

A causa del ritardo di propagazione fra i nodi

In caso di collisione:

Sprechiamo il tempo di trasmissione di un pacchetto

nota: La probabilità di collisione dipende dalla distanza e dal ritardo di propagazione

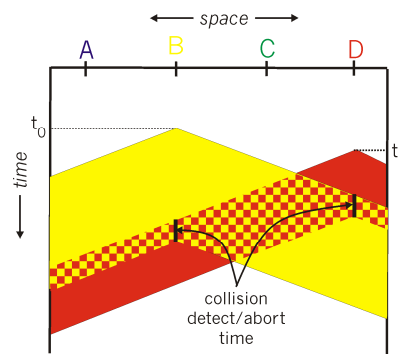


Corso di Reti per Automazione Industriale

6

CSMA/CD (Collision Detection)

- Ascoltiamo il canale
 - Durante la trasmissione



- If (Transmitted_Signal $\neq$ Sensed_Signal)
 - Il Sender capisce che c'è una **Collisione**
 - **ABORT**

Due osservazioni sul CSMA/CD

- Il transmitter può **send/listen** contemporaneamente
 - If (Transmitted - Sensed = null)? Then **successo**
- Il segnale ha la stessa intensità nel Tx e in Rx
 - Non-spreca banda



Il trasmettitore può rivelare se e quando si verifica una collisione

Sfortunatamente ...

Entrambe le osservazioni non valgono per i sistemi wireless

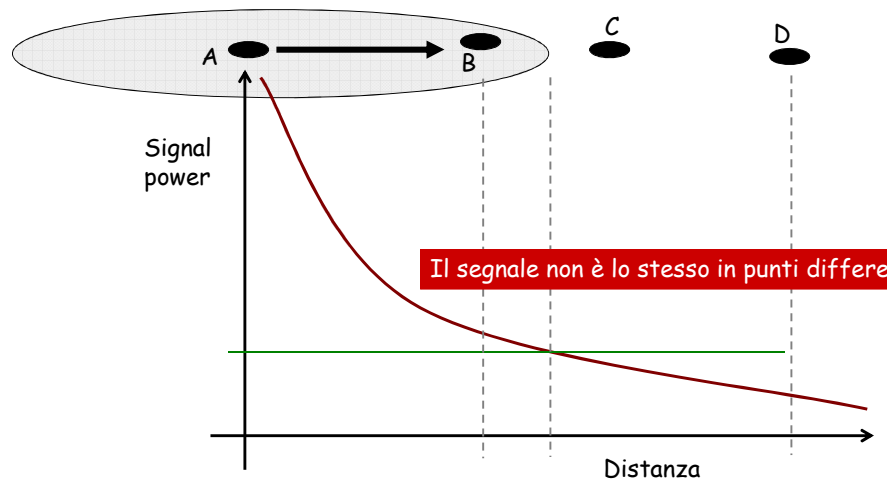
perchè ...

Corso di Reti per Automazione Industriale

9

Il mezzo wireless Disperde Energia

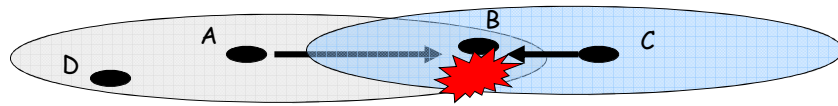
A non può trasmettere ed ascoltare in parallelo



Corso di Reti per Automazione Industriale

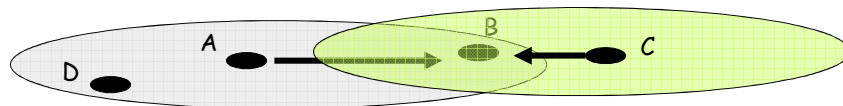
10

Difficoltà nella rivelazione di collisioni



- La ricezione del segnale è basata su SINR
 - Il Transmitter può solo ascoltare sè stesso
 - Non è possibile determinare la qualità del segnale al ricevitore

Come si calcola SINR



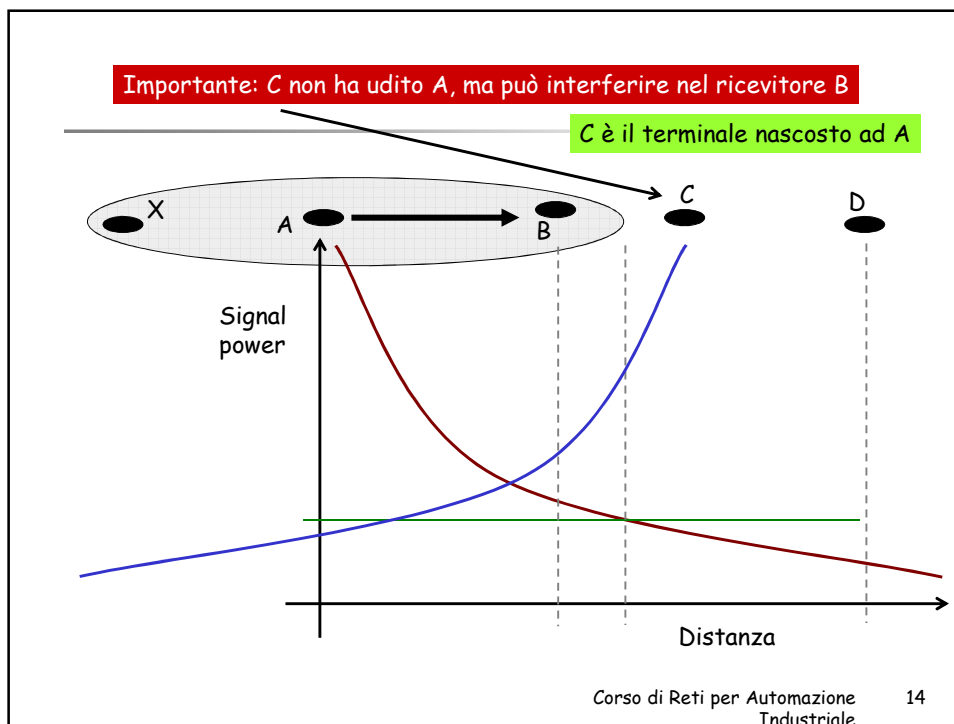
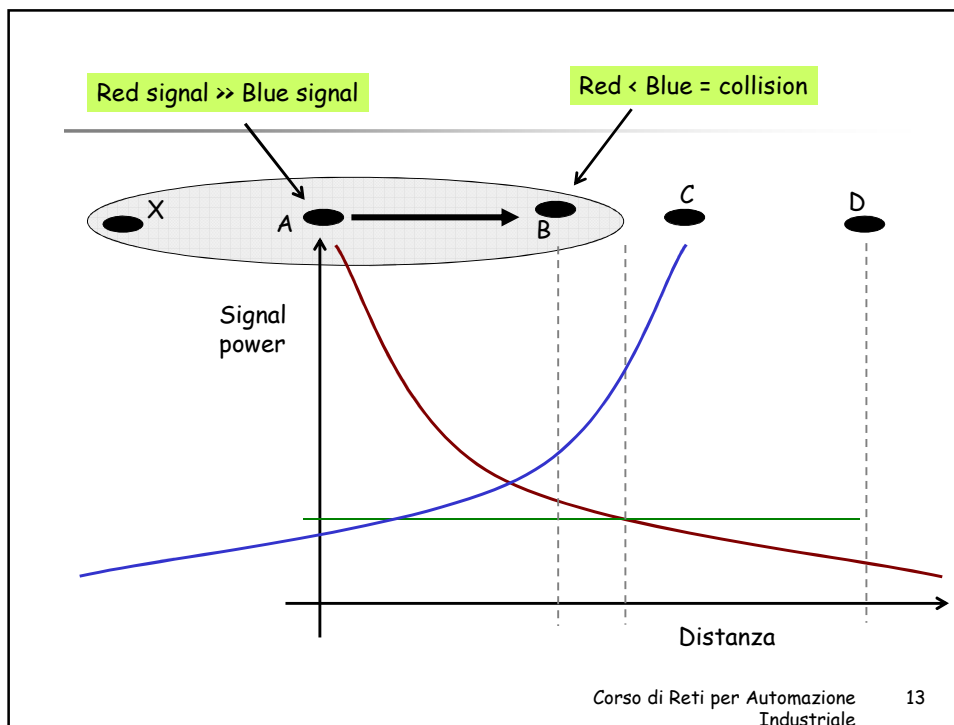
$$SINR = \frac{SignalOfInterest(SoI)}{Interference(I) + Noise(N)}$$

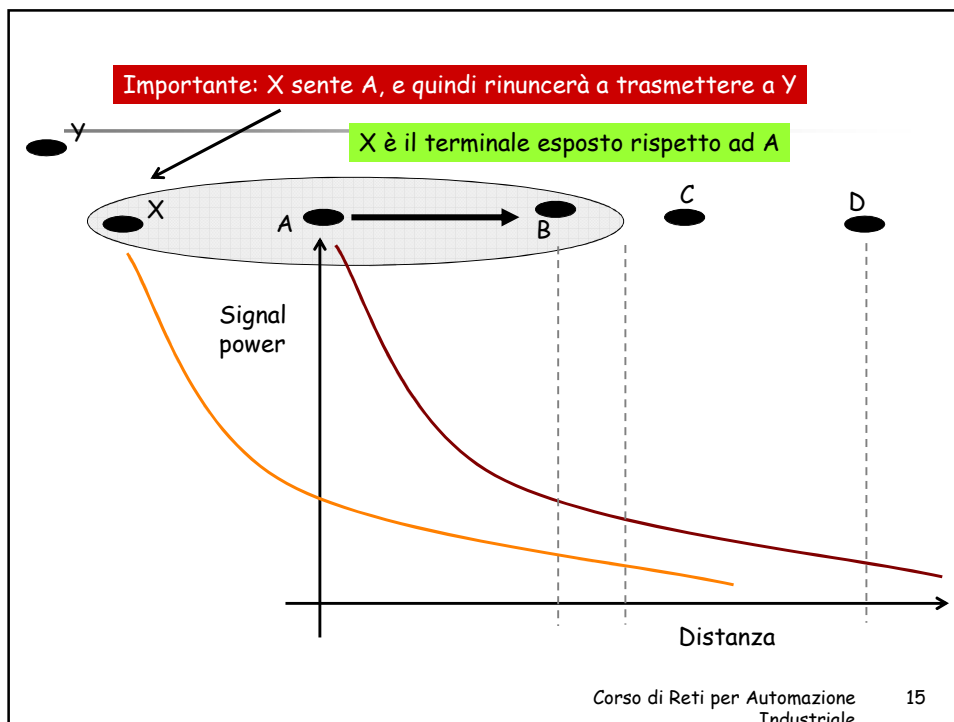
$$SoI_B^A = \frac{P_{transmit}^A}{d_{AB}^\alpha}$$

$$I_B^C = \frac{P_{transmit}^C}{d_{CB}^\alpha}$$



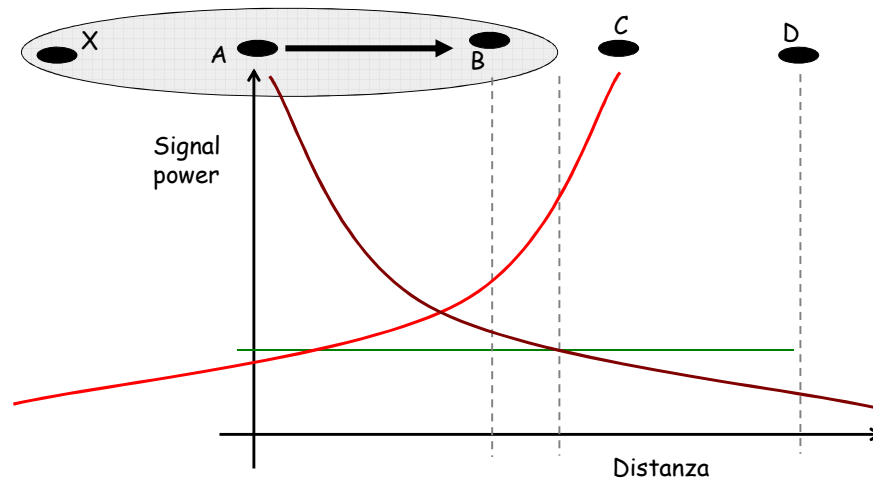
$$SINR_B^A = \frac{\frac{P_{transmit}^A}{d_{AB}^\alpha}}{N + \frac{P_{transmit}^C}{d_{CB}^\alpha}}$$





E quindi, come possiamo gestire il problema del terminale nascosto/esposto?

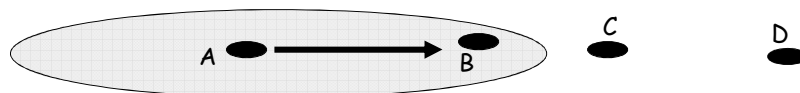
Come impedire a C di trasmettere?



Corso di Reti per Automazione Industriale

17

Una idea!

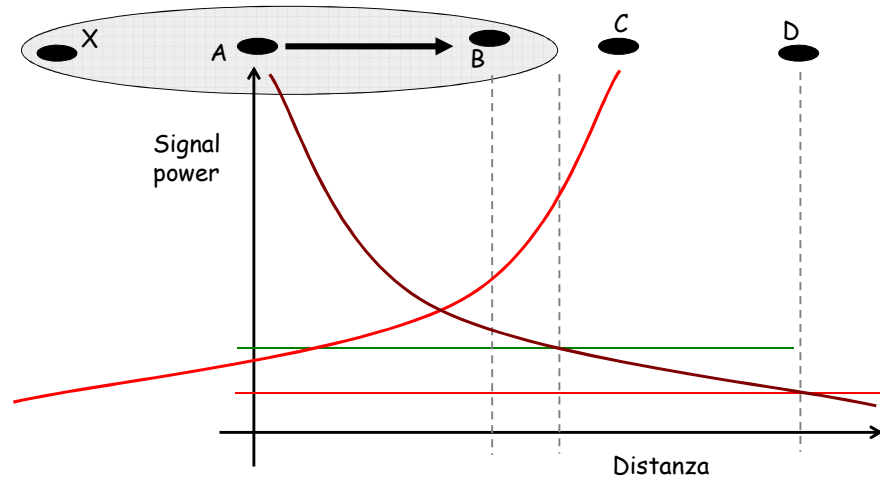


- Un nodo decide di scegliere una opportuna soglia T
Carrier sensing threshold (T)
- Il nodo ascolta il canale
 - If signal > T, then il nodo non trasmette
 - If signal < T, then il nodo trasmette
- E' Possibile garantire l'assenza di collisioni?

Corso di Reti per Automazione Industriale

18

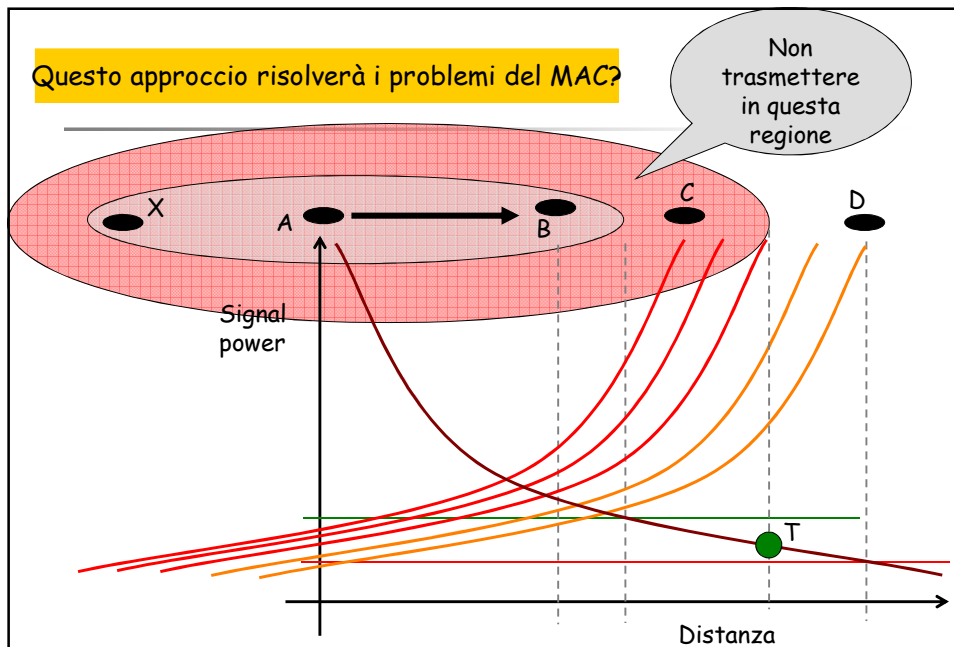
Una idea!



Corso di Reti per Automazione Industriale

19

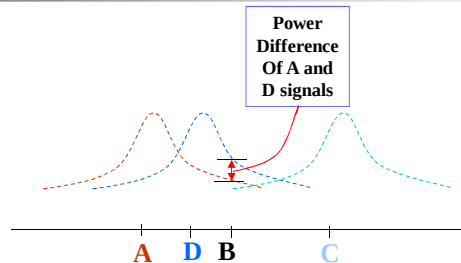
Questo approccio risolverà i problemi del MAC?



Corso di Reti per Automazione Industriale

20

L'effetto di cattura



- Un ulteriore problema è l'effetto di cattura.
- A e D trasmettono simultaneamente a B, l'intensità del segnale che B riceve da D è molto maggiore di quella ricevuta da A. Pertanto la trasmissione di D può essere ricevuta senza errori.
- Ciò produce una suddivisione unfair della banda.

Corso di Reti per Automazione Industriale

La nascita di MACA, MACAW, & 802.11

- Si è visto come il MAC Wireless non possa essere banale
- 1992 - research by Karn (MACA)
- 1994 - research by Bhargavan (MACAW)
- Hanno portato alla IEEE 802.11 committee
 - Lo standard è stato ratificato nel 1999

Corso di Reti per Automazione Industriale

22

MACA

- Obiettivi:

- Superare il problema del terminale nascosto e di quello esposto.

- L'idea:

Riservare il canale prima di mandare i pacchetti dati.
Minimizzare il costo delle collisioni (il pacchetto di controllo è molto minore dei pacchetti dati)

Principali contributi:

Un protocollo MAC con three-way handshake : MACA

CSMA/CA

MA/CA

MACA

Corso di Reti per Automazione Industriale

Principali assunzioni di MACA

- Simmetria

- A può sentire B $\Leftrightarrow$ B può sentire A

- Nessun effetto di cattura

- Assenza di fading nel canale

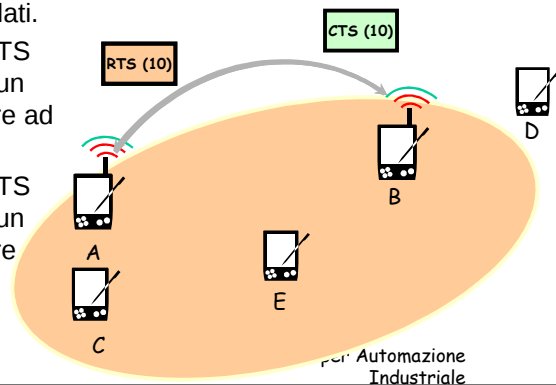
- Packet error solo a causa di collisioni

- Data packets e control packets sono trasmessi sullo stesso canale.

Corso di Reti per Automazione Industriale

Three-Way Handshake in MACA

- **A** invia la Ready-to-Send (RTS)
- **B** risponde con Clear-to-Send (CTS)
- **A** spedisce il DATA PACKET
- RTS e CTS annunciano la durata del trasferimento dati.
- I Nodi che ascoltano la RTS rimangono silenziosi per un certo tempo per consentire ad **A** di ricevere la CTS
- I Nodi che ascoltano la CTS rimangono silenziosi per un certo tempo per consentire **B** di ricevere il pacchetto dati.

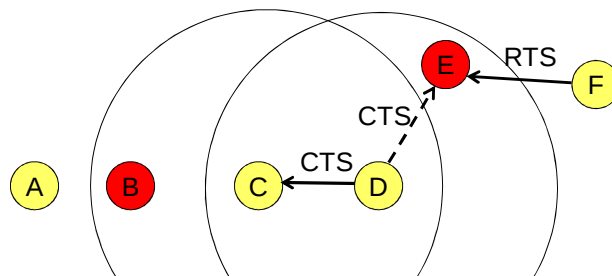


Ma è sufficiente?

RTS/CTS

■ Risolve il problema del terminale nascosto ?

- Assumiamo che la carrier sensing zone = communication zone



E non sente la RTS inviata da C e parlerà con F mentre D invia la CTS. La comunicazione fra E ed F interferirà con D. Il problema del terminale nascosto, persiste.

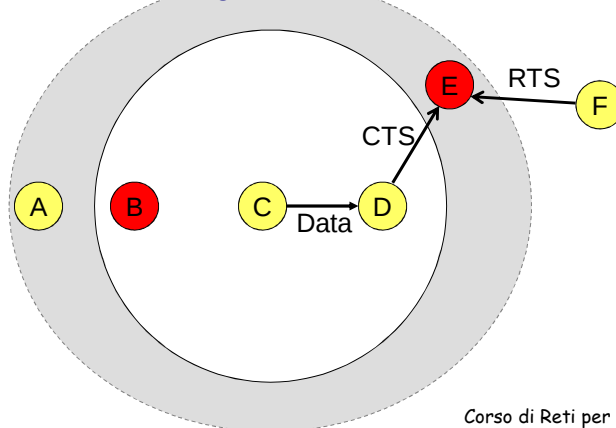
Corso di Reti per Automazione Industriale

27

Il problema del terminale nascosto

■ E se aumentassimo il carrier sense range ??

- E sentirà la RTS inviata da C ed eviterà di rispondere alla RTS che gli sta inviando F. Si evita la collisione!

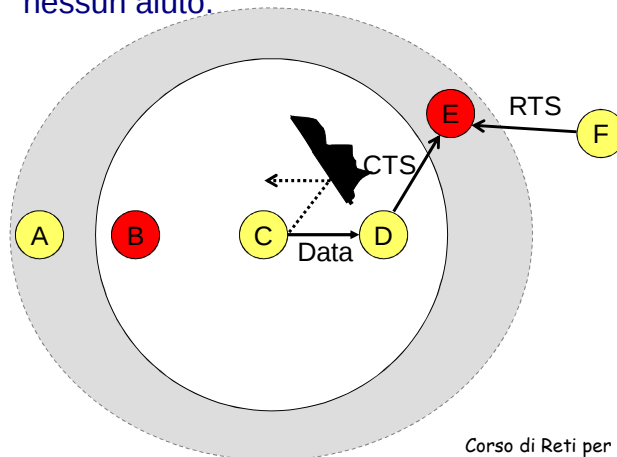


Corso di Reti per Automazione Industriale

28

Il problema del terminale nascosto

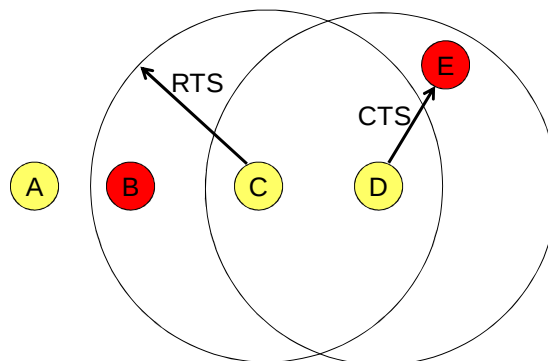
- Cosa succede se ci sono barriere/ostruzioni ??
 - E non potrà sentire C: il Carrier sensing non è di nessun aiuto.



Corso di Reti per Automazione Industriale 29

Il problema del terminale esposto

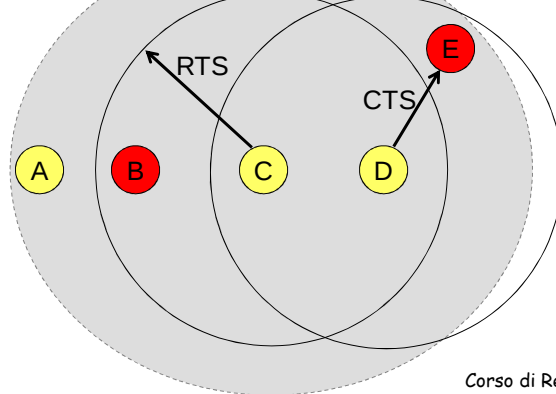
- B dovrebbe poter trasmettere ad A dato che non è coinvolto nella comunicazione con C
 - RTS non lo consente



Corso di Reti per Automazione Industriale 30

Il problema del terminale esposto

- **B** dovrebbe poter trasmettere ad **A** dato che non è coinvolto nella comunicazione con **C**
 - Ampliare la **Carrier sensing area** peggiora ulteriormente la situazione.

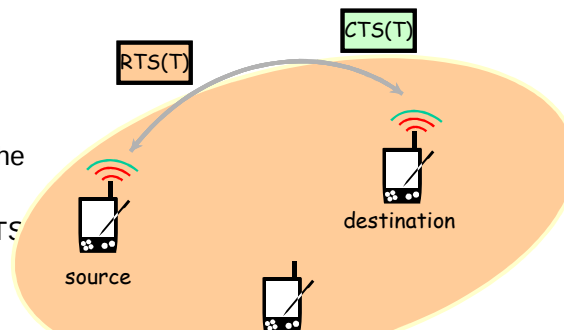


Corso di Reti per Automazione Industriale

31

Four-Way Handshake in MACAW

- Il Sender invia una Ready-to-Send (RTS)
- Il Receiver risponde con la Clear-to-Send (CTS)
- Il Sender invia il DATA PACKET
- Il ricevitore risponde con un ACK
- RTS e CTS contengono anche la durata della trasmissione
- I Nodi che ascoltano RTS/CTS rimangono silenziosi per quella durata
- Il Sender ritrasmette la RTS se non riceve un ACK.



Corso di Reti per Automazione Industriale

MACAW : le fasi

- Tutti i nodi scelgono un numero random
 - $R = \text{rand}(0, CW_min)$
- Ciascun nodo conta all'indietro partendo da R
 - Continua il carrier sensing durante il counting down
 - Appena rivela una portante, congela il countdown
- Chiunque raggiunge ZERO trasmette **RTS**
 - I vicini bloccano il countdown, e decodificano la RTS
 - RTS contiene la durata $(CTS + DATA + ACK) = T_comm$
 - I vicini settano il $NAV = T_comm$
 - Rimangono silenziosi per un tempo contenuto nel NAV.

MACAW : Le fasi

- Il ricevitore replica con CTS
 - Contiene anche la durata $(DATA + ACK)$.
 - I vicini aggiornano il NAV I nuovo.
- Tx invia i DATI, Rx conferma con un ACK
 - Dopo l'ACK, ognuno riparte col rimanente countdown
 - Tx sceglie un nuovo $R = \text{rand}(0, CW_min)$
- Se RTS o i DATI collidono (cioè non torna un CTS/ACK)
 - Viene rivelata la collisione
 - RTS sceglie un nuovo random $R1 = \text{rand}(0, 2 * CW_min)$
 - Si usa un **Exponential Backoff** $Ri = \text{rand}(0, 2^i * CW_min)$
 - Se la trasmissione ha successo, resetta a $\text{rand}(0, CW_min)$

Confronto senza Ack e con Ack

Error Rate	RTS-CTS-DATA	RTS-CTS-DATA-ACK
0	40.41	36.76
0.001	36.58	36.67
0.01	16.65	35.52
0.1	2.48	9.93

La tabella confronta il Throughput, in pacchetti al secondo, ottenuto da un singolo flusso TCP, fra due nodi, in presenza di rumore.

Si evidenziano i miglioramenti che l'uso di un ACK introduce.

MACAW è stata la base per 802.11

ne
Industriale

Alcune riflessioni !

- 802.11 non riesce a risolvere in maniera completa il problema del nodo nascosto/esposto
 - Però alleggerisce il problema mediante l'uso della RTS/CTS e consiglia l'uso di CS zone più ampie.
- Però CS zone più ampie peggiorano il problema del terminale esposto.
 - L'uso di CS più piccole migliora lo Spatial reuse e riduce il problema del nodo esposto: occorre un compromesso
 - I pacchetti RTS/CTS consumano banda.
 - Anche il meccanismo di back-off mechanism consuma banda.

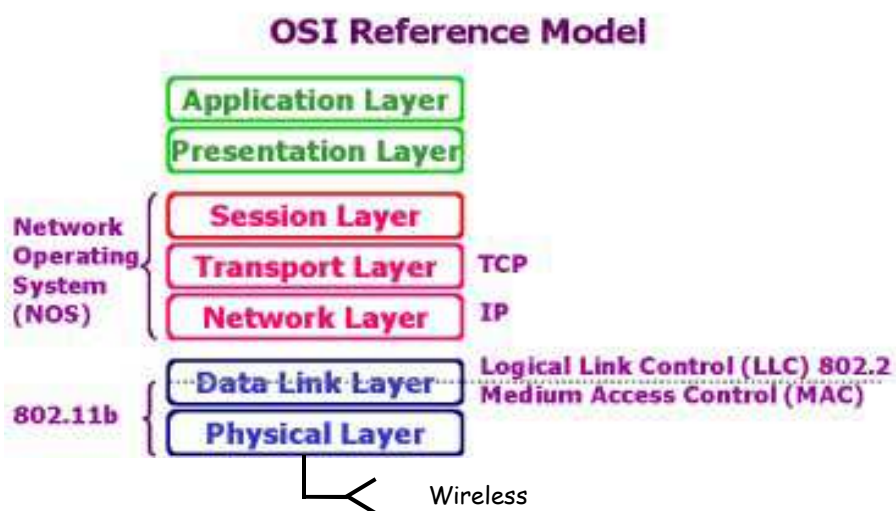
La ricerca del miglior MAC protocol è ancora in corso.

In questi anni 802.11 è stato continuamente migliorato, anche se una soluzione definitiva non è stata ancora trovata.

IEEE 802.11 – An overview

Corso di Reti per Automazione Industriale 37

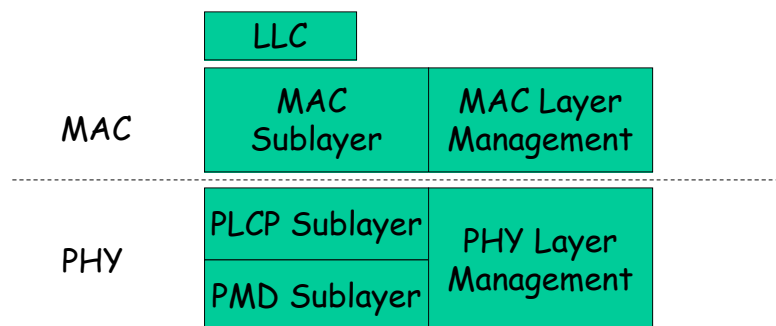
IEEE 802.11 in OSI Model



Corso di Reti per Automazione Industriale 38

802.11 Scope & Modules

To develop a **MAC** and **PHY** spec for wireless connectivity for fixed, portable and moving stations in a local area



Applications

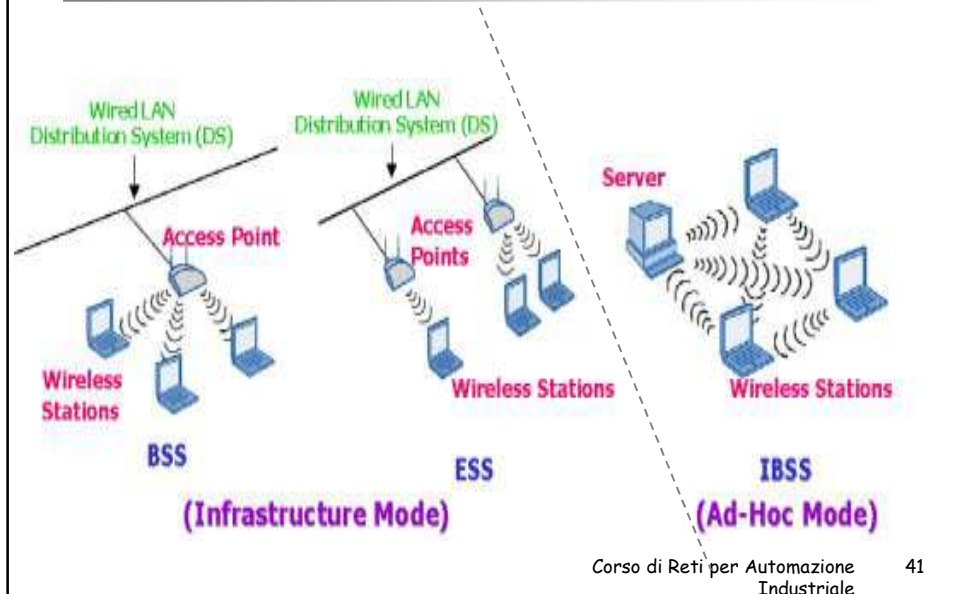
Single Hop

- Home networks
- Enterprise networks (e.g., offices, labs, etc.)
- Outdoor areas (e.g., cities, parks, etc.)

Multi-hops

- Adhoc network of small groups (e.g., aircrafts)
- Balloon networks (SpaceData Inc.)
- Mesh networks (e.g., routers on lamp-posts)

802.11 Architecture – Two modes



802.11 PHY Technologies

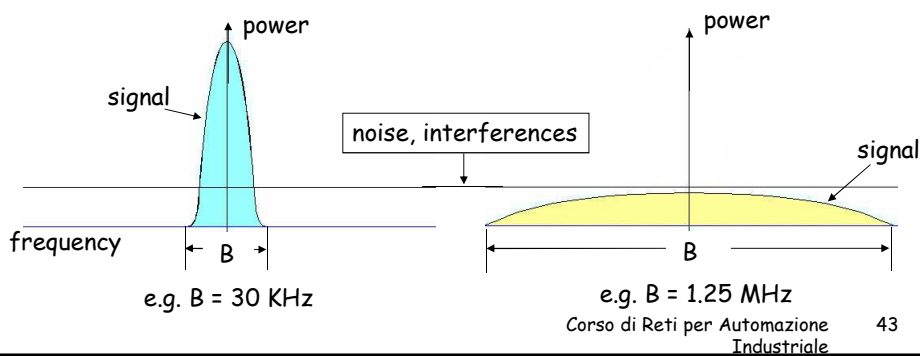
- Two kinds of radios based on
 - “Spread Spectrum”
 - “Diffused Infrared”
- Spread Spectrum radios based on
 - Frequency hopping (FH)
 - Direct sequence (DS)

Radio works in 2.4GHz ISM band --- license-free by FCC (USA), ETSI (Europe), and MKK (Japan)

- 1 Mbps and 2Mbps operation using FH
- 1, 2, 5.5, and 11Mbps operation using DSSS (FCC)

Why Spread Spectrum ?

- $C = B \cdot \log_2(1 + S/N)$... [Shannon]
- To achieve the same channel capacity C
 - Large S/N, small B
 - Small S/N, large B
 - Increase S/N is inefficient due to the logarithmic relationship



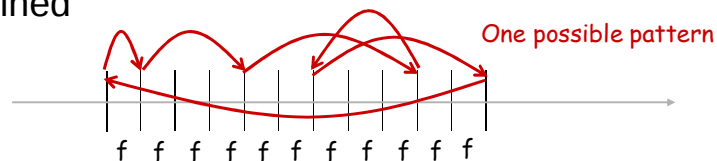
Spread Spectrum

Methods for spreading the bandwidth of the transmitted signal over a frequency band (spectrum) which is **wider than the minimum bandwidth** required to transmit the signal.

- Reduce effect of jamming
 - Military scenarios
- Reduce effect of other interferences
- More "secure"
 - Signal "merged" in noise and interference

Frequency Hopping SS (FHSS)

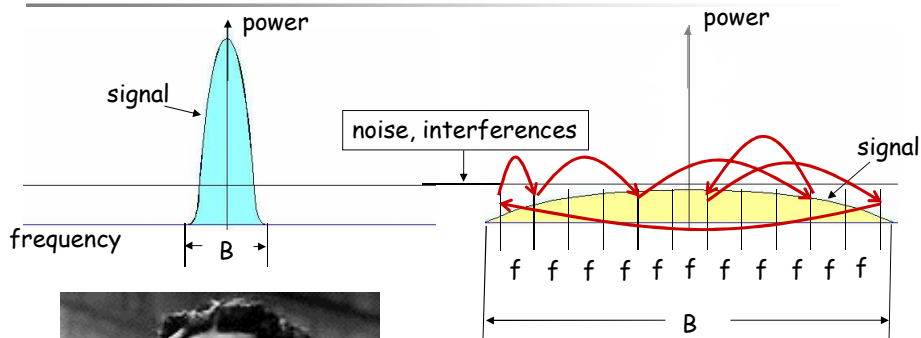
- 2.4GHz band divided into 75 1MHz subchannels
- Sender and receiver agree on a hopping pattern (pseudo random series). 22 hopping patterns defined



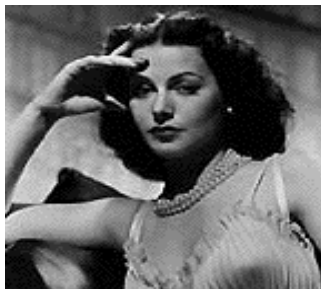
- Different hopping sequences enable co-existence of multiple BSSs
- Robust against narrow-band interferences

Corso di Reti per Automazione Industriale 45

FHSS due to [Lamarr1940]



Simple radio design with FHSS
Data rates ~ 2 Mbps



Invented by Hedy Lamarr (Hollywood film star) in 1940, at age of 27, with musician George Antheil

Corso di Reti per Automazione Industriale 46

Direct Sequence SS

- Direct sequence (DS): **most prevalent**
 - Signal is spread by a wide bandwidth pseudorandom sequence (code sequence)
 - Signals appear as wideband noise to unintended receivers
- Not for intra-cell multiple access
 - Nodes in the same cell use same code sequence

IEEE 802.11b DSSS

- ISM unlicensed frequency band **(2.4GHz)**
- Channel bandwidth: $f_{\text{high}} - f_{\text{low}} = \mathbf{22\text{ MHz}}$
- 1MHz guard band
- Direct sequence spread spectrum in each channel
- **3 non-overlapping channels**

Channel	f_{low}	f_{high}
1	2.401	2.423
2	2.404	2.428
3	2.411	2.433
4	2.416	2.438
5	2.421	2.443
6	2.426	2.448
7	2.431	2.453
8	2.436	2.458
9	2.441	2.463
10	2.446	2.468
11	2.451	2.473

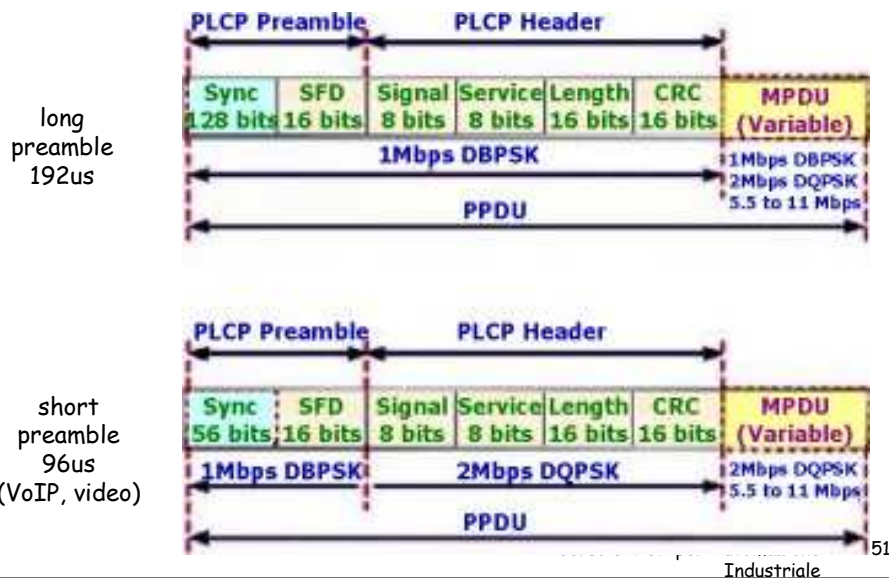
Diffused Infrared

- Wavelength range from 850 – 950 nm
- For indoor use only
- Line-of-sight and reflected transmission
- 1 – 2 Mbps

PHY Sublayers

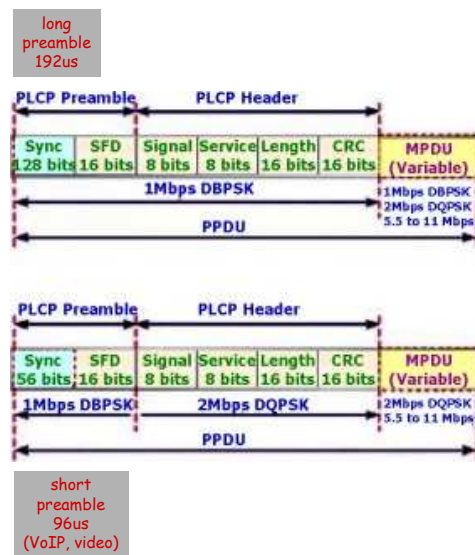
- **Physical layer convergence protocol (PLCP)**
 - Provides common interface for MAC
 - Offers carrier sense status & CCA (Clear channel assesment)
 - Performs channel synchronization / training
- **Physical medium dependent sublayer (PMD)**
 - Functions based on underlying channel quality and characteristics
 - E.g., Takes care of the wireless encoding

PLCP (802.11b)



Industriale

PLCP (802.11b)



Note:

To send **even one bit payload** reliably, you will have to form a packet with the PLCP preamble and the PLCP header.

This constraints protocol design

You cannot arbitrarily exchange control messages.

What are the control messages in IEEE 802.11 ?

Corso di Reti per Automazione
Industriale

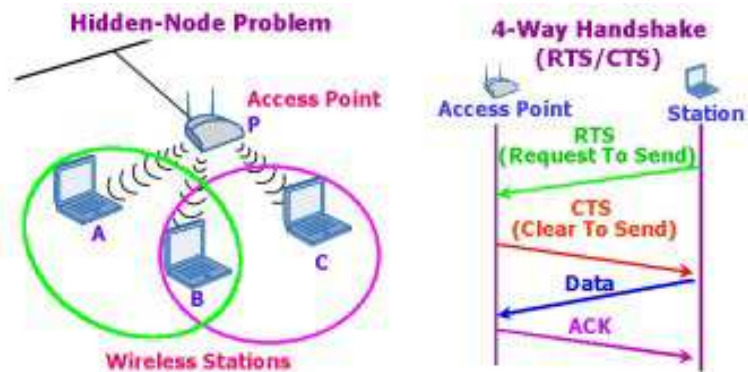
52

IEEE 802.11 MAC

802.11 MAC (DCF)

- **CSMA/CA based protocol**
 - Listen before you talk
 - CA = Collision avoidance (prevention is better than cure !!)
- **Robust for interference**
 - Explicit acknowledgment requested from receiver
 - for unicast frames
 - Only CSMA/CA for Broadcast frames
- **Optional RTS/CTS offers Virtual Carrier Sensing**
 - RTS/CTS includes duration of immediate dialog
 - Addresses hidden terminal problems

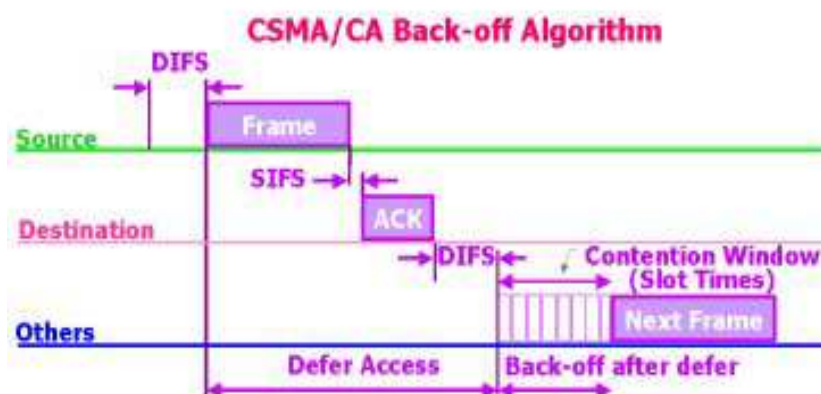
802.11 MAC (DCF)



Corso di Reti per Automazione Industriale

55

Physical Carrier Sense & Backoff



Corso di Reti per Automazione Industriale

56

MAC Management Layer

■ Synchronization

- Finding and staying with a WLAN
 - Uses TSF timers and beacons

■ Power Management

- Sleeping without missing any messages
 - Periodic sleep, frame buffering, traffic indication map

■ Association and Reassociation

- Joining a network
- Roaming, moving from one AP to another
- Scanning

Corso di Reti per Automazione Industriale 57

Synchronization

■ Timing Synchronization Function (TSF)

- Enables synchronous waking/sleeping
- Enables switching from DCF to PCF
- Enables frequency hopping in FHSS PHY
 - Transmitter and receiver has identical dwell interval at each center frequency

■ Achieving TSF

- All stations maintain a local timer.
- AP periodically broadcasts beacons containing timestamps, management info, roaming info, etc.
 - Not necessary to hear every beacon
- Beacon synchronizes entire BSS
 - Applicable in infrastructure mode ONLY
- Distributed TSF (for Independent BSS) more difficult

Corso di Reti per Automazione Industriale 58

Power management

- **Battery powered devices require power efficiency**
 - LAN protocols assume idle nodes are always ON and thus ready to receive.
 - Idle-receive state key source of power wastage
- **Devices need to power off during idle periods**
 - Yet maintain an active session – tradeoff power Vs throughput
- **Achieving power conservation**
 - Allow idle stations to go to sleep periodically
 - APs buffer packets for sleeping stations
 - AP announces which stations have frames buffered when all stations are awake – called **Traffic Indication Map (TIM)**
 - TSF assures AP and Power Save stations are synchronized
 - TSF timer keeps running when stations are sleeping
- **Independent BSS also have Power Management**
 - Similar in concept, distributed approach

Corso di Reti per Automazione Industriale 59

Roaming & Scanning

- **Stations switch (roam) to different AP**
 - When channel quality with current AP is poor
- **Scanning function used to find better AP**
 - Passive Scanning → Listen for beacon from different Aps
 - Active Scanning → Exchange explicit beacons to determine best AP
- **Station sends Reassociation Request to new AP**
 - If Reassociation Response successful → Roaming
- **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

Corso di Reti per Automazione Industriale 60

MAC management frame

- **Beacon**
 - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
 - Traffic Indication Map
- **Probe**
 - ESSID, Capabilities, Supported Rates
- **Probe Response**
 - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
 - same for Beacon except for TIM
- **Association Request**
 - Capability, Listen Interval, ESSID, Supported Rates
- **Association Response**
 - Capability, Status Code, Station ID, Supported Rates

MAC Management Frame

- **Reassociation Request**
 - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address
- **Reassociation Response**
 - Capability, Status Code, Station ID, Supported Rates
- **Disassociation**
 - Reason code
- **Authentication**
 - Algorithm, Sequence, Status, Challenge Text
- **Deauthentication Reason**

Security

- **Range of attacks huge in wireless**
 - Easy entry into the network
 - Jamming, selfish behavior, spatial overhearing
- **Securing the network harder than wired networks**
 - Especially in distributed environments
- **WEP → symmetric 40 or 128-bit encryption**
- **WPA: Wi-Fi protected access**
 - Temporal key integrity protocol (TKIP) – better
 - User authentication
- **IEEE 802.11i – Efforts toward higher security**