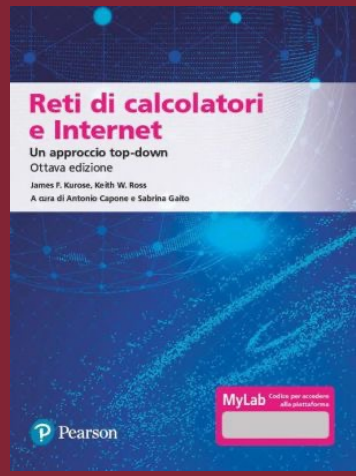
# Reti di Elaboratori

Reti Wireless – LAN Wireless




SAPIENZA
UNIVERSITÀ DI ROMA

Alessandro Checco
alessandro.checco@uniroma1.it

Thanks to prof. Gaia Maselli

Capitolo 7

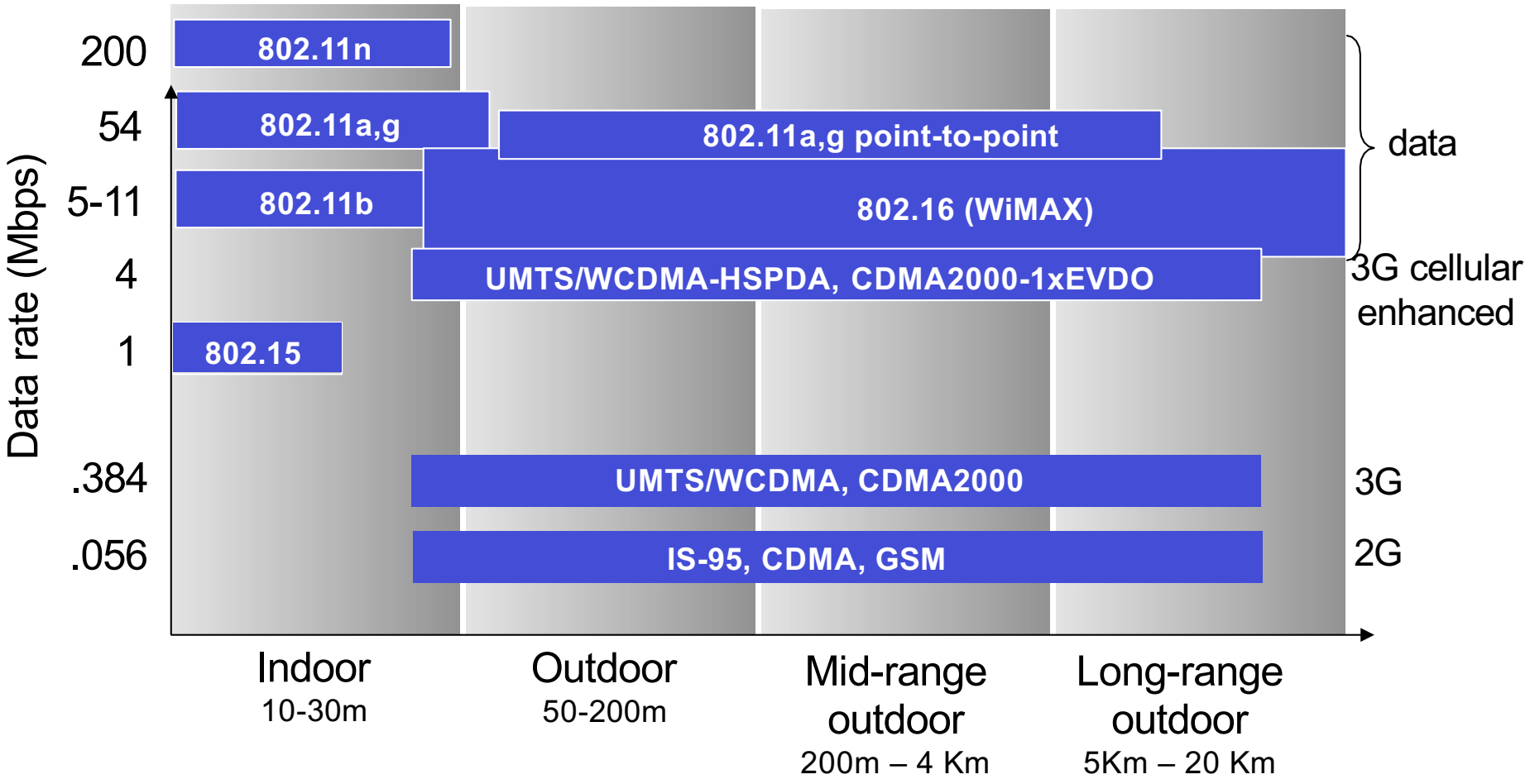
# Informazioni sul secondo esonero

- Solo chi ha superato il primo esonero può sostenere il secondo
- Il secondo esonero può essere sostenuto:
  - Il 6 Giugno al posto del primo appello
  - Il 3 Luglio al posto del secondo appello
- Il voto finale è la media dei due esoneri (se entrambi >=18)
- Chi non passa o non è contento del voto del secondo esonero deve rifare tutto l'appello
- Chi decide di sostenere l'intero appello perde i voti parziali (eventuali) degli esoneri
- Dal 3 Luglio in poi tutti i voti parziali non sono più validi

# Reti wireless

- LAN wireless
  - Disponibili in campus universitari, uffici, bar, aree pubbliche
- Reti cellulari
  - Il numero di abbonati alla telefonia mobile supera quello della telefonia fissa
- Bluetooth
- Reti di sensori, RFID, smart objects

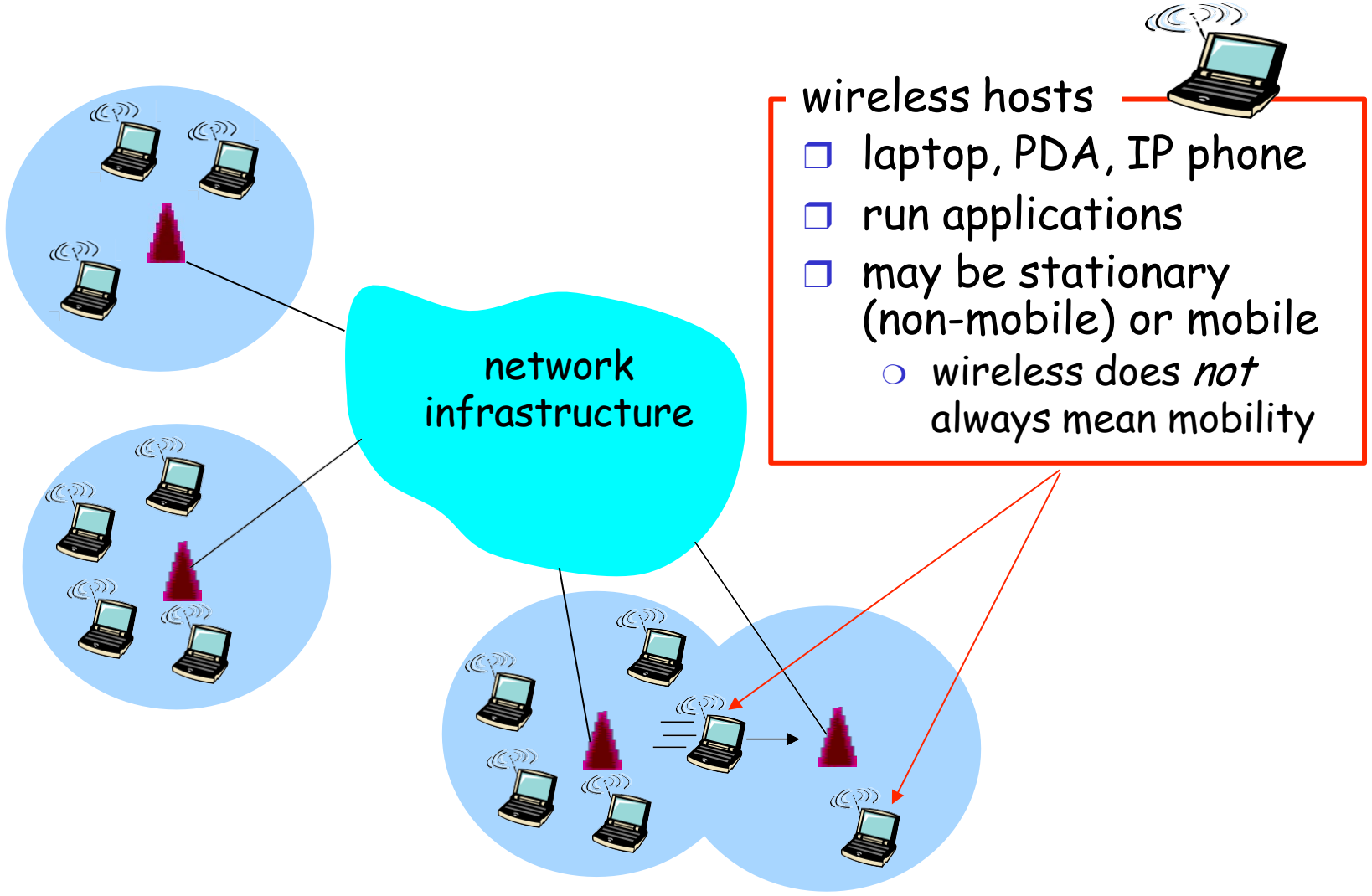
# Alcuni standard



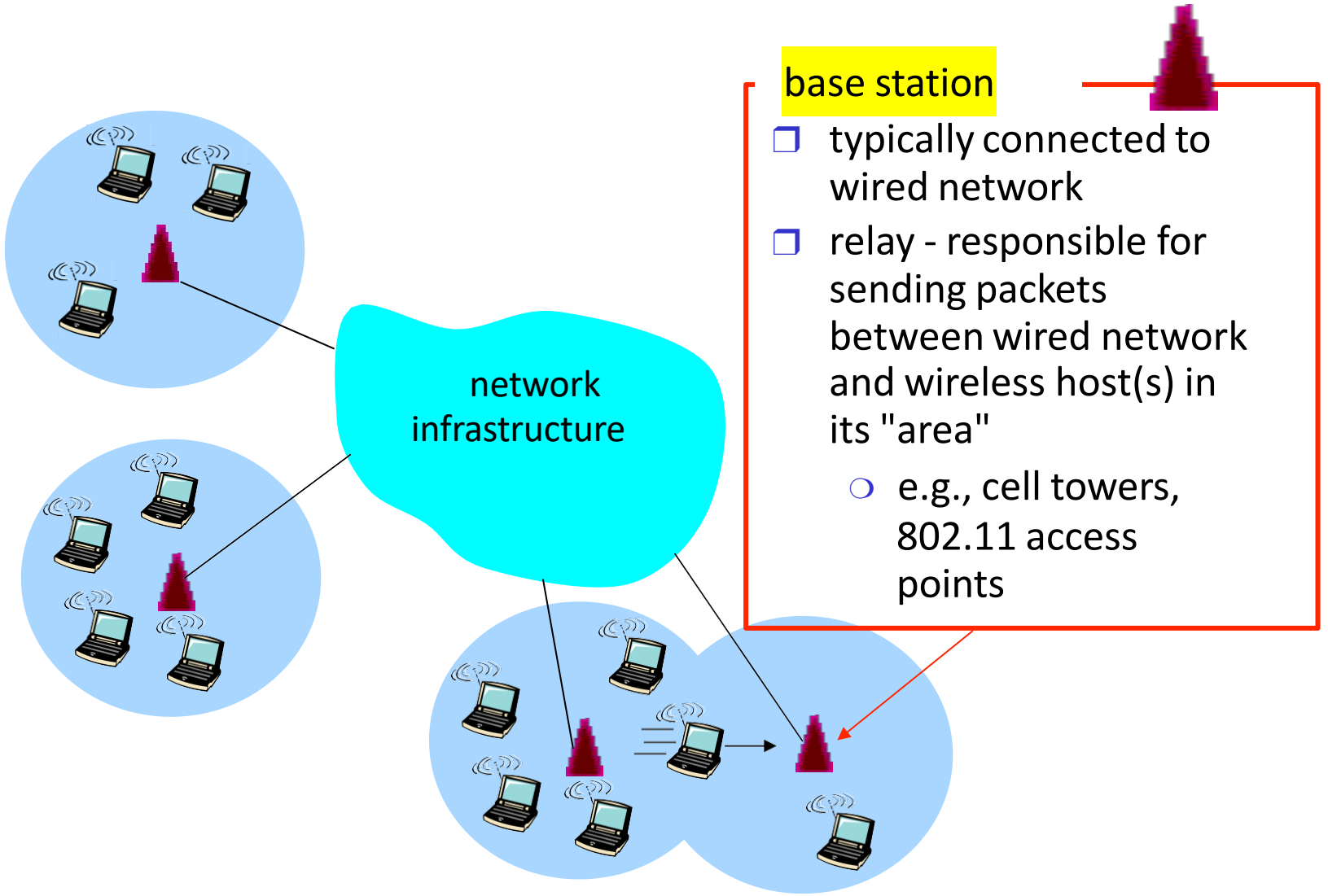
# Standard IEEE

| Protocol | Release Data | Freq. | Rate (typical) | Rate (max) | Range (indoor) |
|---|---|---|---|---|---|
| Legacy | 1997 | 2.4 GHz | 1 Mbps | 2Mbps | ? |
| 802.11a | 1999 | 5 GHz | 25 Mbps | 54 Mbps | ~30 m |
| 802.11b | 1999 | 2.4 GHz | 6.5 Mbps | 11 Mbps | ~30 m |
| 802.11g | 2003 | 2.4 GHz | 25 Mbps | 54 Mbps | ~30 m |
| 802.11n | 2008 | 2.4/5 GHz | 200 Mbps | 540 Mbps | ~50 m |

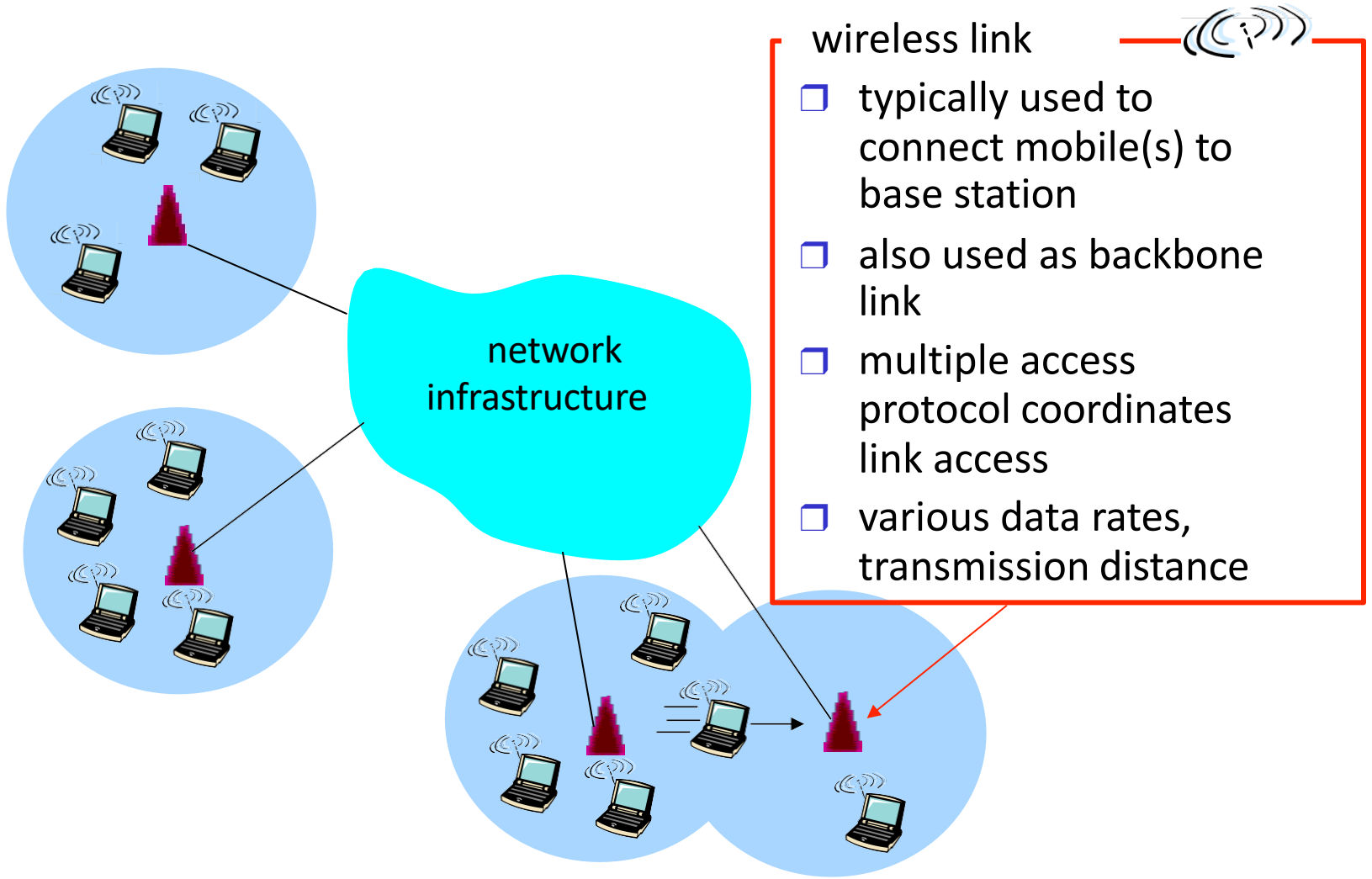
# LAN Wireless: elementi



# LAN Wireless: elementi

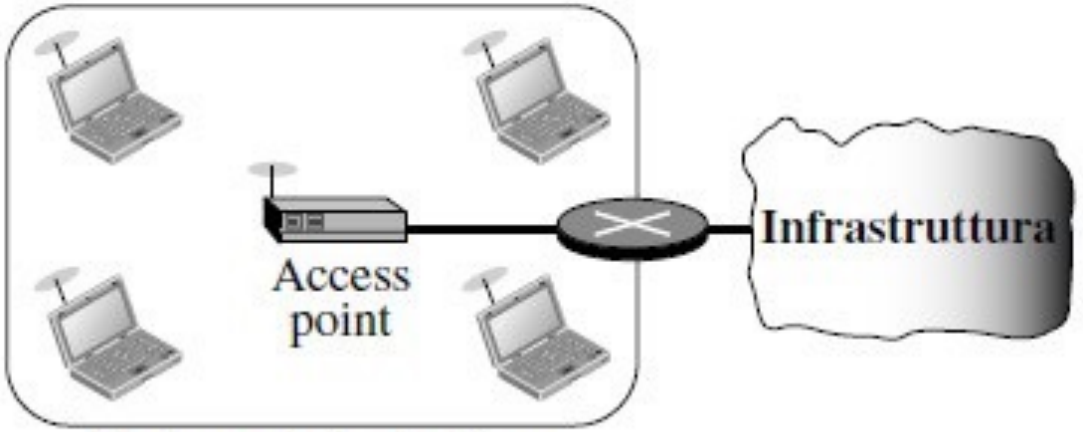


# LAN Wireless: elementi



# Caratteristiche LAN wireless

- Mezzo trasmissivo: aria, segnale broadcast, mezzo condiviso dagli host della rete
- Host wireless: non è fisicamente connesso alla rete e può muoversi liberamente
- Connessione ad altre reti: mediante una stazione base detta Access Point (AP) che unisce l'ambiente wireless all'ambiente cablato



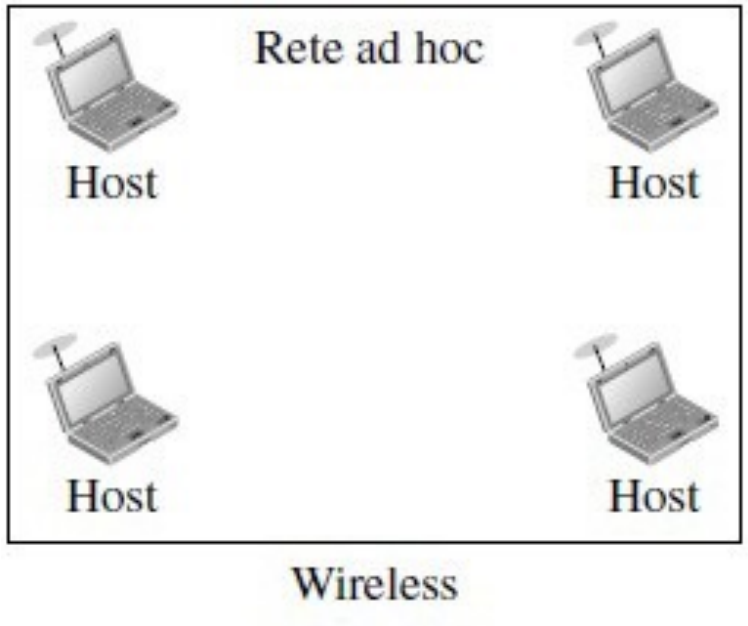
Rete con infrastruttura

# Migrazione dall'ambiente cablato al wireless

- Il funzionamento di una rete cablata o wireless dipende dai due sottolivelli inferiori dello stack protocollare (collegamento e fisico)
- Per migrare dalla rete cablata a quella wireless è sufficiente cambiare le schede di rete e sostituire lo switch di collegamento con un AP.
  - Gli indirizzi MAC cambiano mentre gli IP rimangono gli stessi

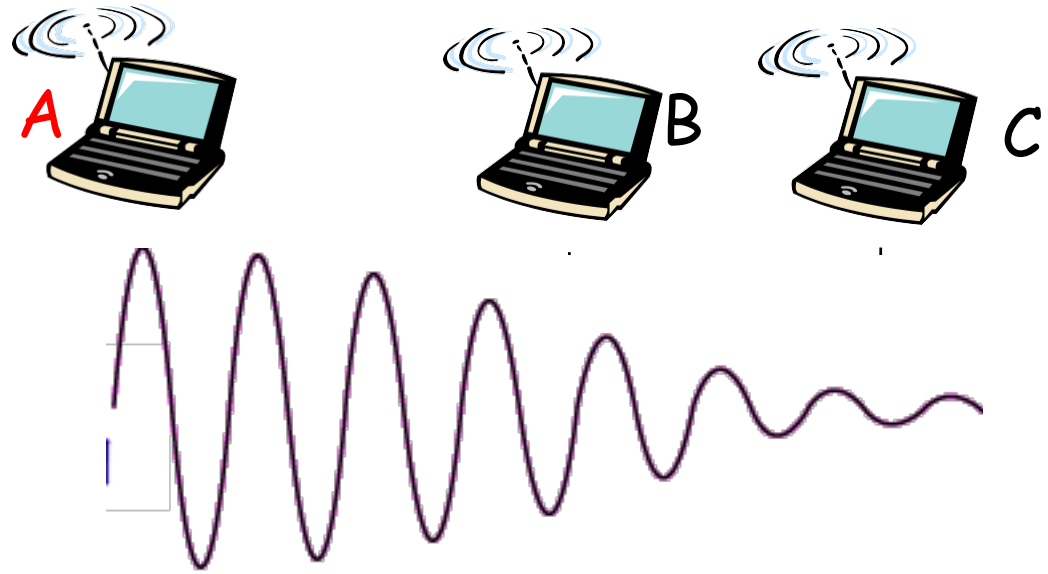
# Reti ad hoc (senza infrastruttura)

- Insieme di host che si auto-organizzano per formare una rete e comunicano liberamente tra di loro
  - Ogni host deve eseguire le funzionalità di rete quali network setup, routing, forwarding, etc.



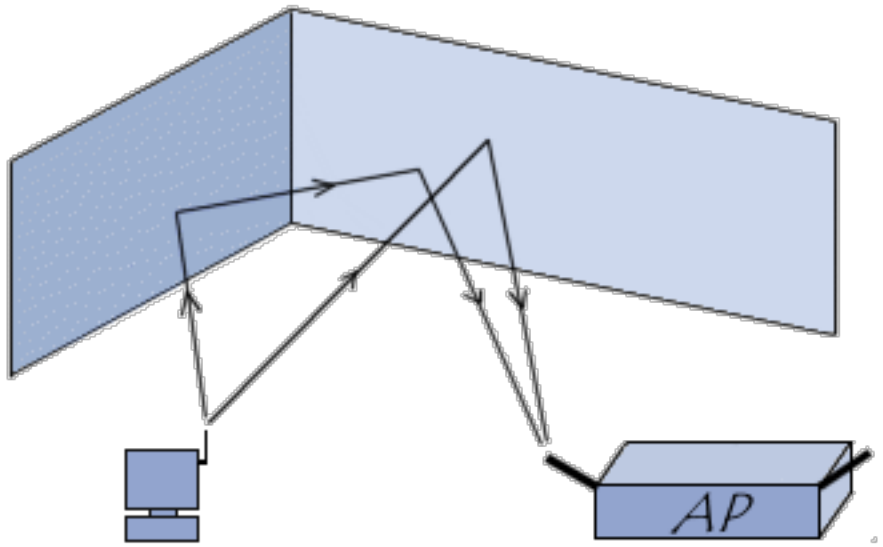
# Caratteristiche del link wireless

- Attenuazione del segnale
  - La forza dei segnali elettromagnetici diminuisce rapidamente all'aumentare della distanza dal trasmettitore in quanto il segnale si disperde in tutte le direzioni



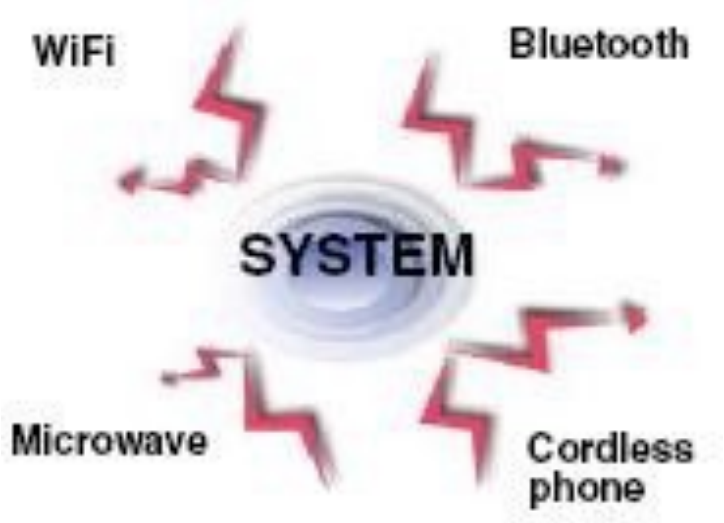
# Caratteristiche del link wireless

- Propagazione multi-path
  - Quando un'onda radio trova un ostacolo, tutta o una parte dell'onda è riflessa, con una perdita di potenza
  - Un segnale sorgente può arrivare, tramite riflessi successivi (su muri, terreno, oggetti), a raggiungere una stazione o un punto di accesso attraverso percorsi multipli



# Caratteristiche del link wireless

- Interferenze
  - Dalla stessa sorgente: Un destinatario può ricevere più segnali dal mittente desiderato a causa del multipath
  - Da altre sorgenti: altri trasmettitori stanno usando la stessa banda di frequenza per comunicare con altri destinatari



# Errori

- Le caratteristiche dei link wireless causano errori
- Signal to Noise Ratio (SNR) o rapporto segnale-rumore misura il rapporto tra il segnale buono e quello cattivo (segnale contro rumore)
  - Alto: il segnale è più forte del rumore, quindi può essere convertito in dati reali
  - Basso: il segnale è stato danneggiato dal rumore e i dati non possono essere recuperati

# Controllo dell'accesso al mezzo

- Mezzo condiviso (aria, stessa frequenza)
- Necessità di controllare l'accesso al mezzo per evitare le collisioni (trasmissioni che si sovrappongono)
- In Ethernet si usa CSMA/CD

D: Possiamo utilizzare CSMA/CD nel wireless?

R: No

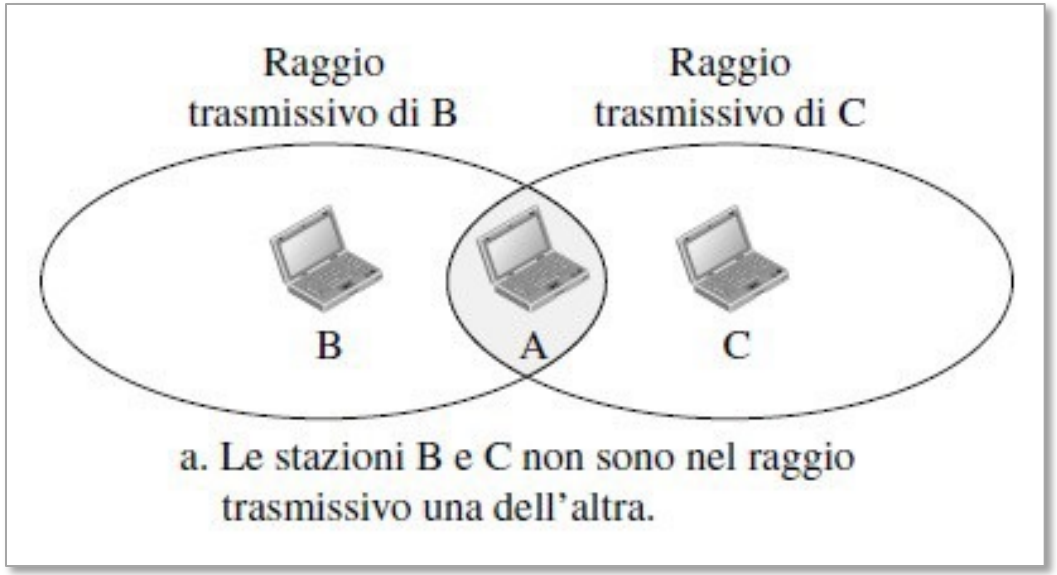
Vediamo perché..

# No collision detection

- Per rilevare una collisione un host deve poter trasmettere (il proprio frame) e ricevere (ascoltare il canale) contemporaneamente
- Poiché la potenza del segnale ricevuto è molto inferiore a quella del segnale trasmesso, sarebbe troppo costoso usare un adattatore di rete in grado di rilevare le collisioni (i dispositivi wireless hanno un'energia limitata fornita dalla batteria che non gli consente di usare tale dispositivi)
- Inoltre…

# Hidden terminal problem

- Un host potrebbe non accorgersi che un altro host sta trasmettendo e quindi non sarebbe in grado di rilevare la collisione (ascoltando il canale)




Problema di attenuazione del segnale

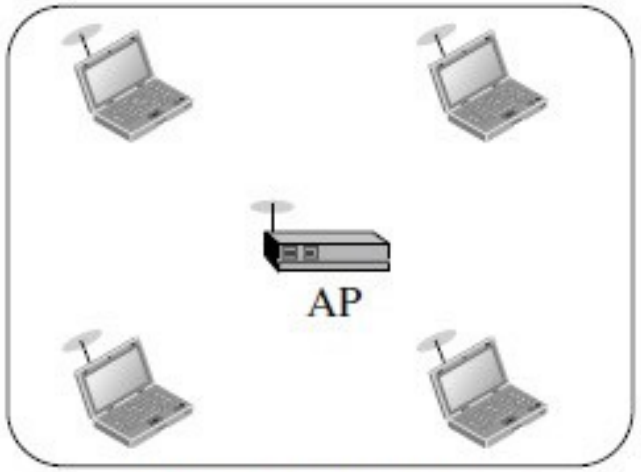
Problema di ostacoli

# IEEE 802.11

- IEEE ha definito le specifiche per le LAN wireless, chiamate 802.11, che coprono i livelli fisico e collegamento
- 802.11b
  - 11 Mbps
  - 2,4-2,5 GHz
- Wi-Fi (wireless fidelity) usato negli States
- Wi-Fi è una LAN wireless certificata dalla Wi-Fi Alliance, associazione (300 aziende) no profit che si occupa di promuovere la crescita delle LAN wireless

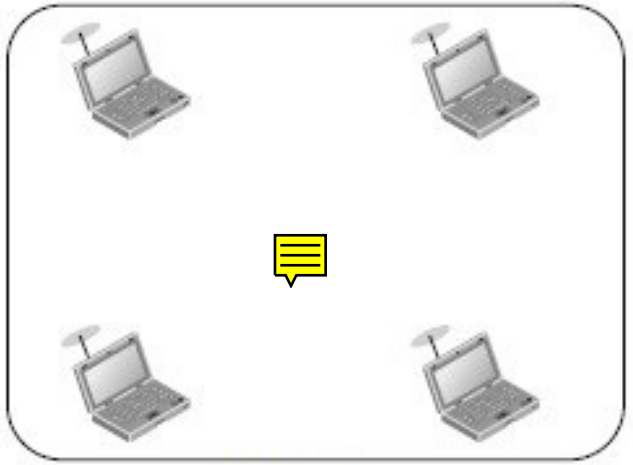
# Architettura: BSS

- Basic service set (BSS) è costituita da uno o più host wireless e da un access point




BSS con infrastruttura

- L'AP è collegato a un router
- Architettura più diffusa

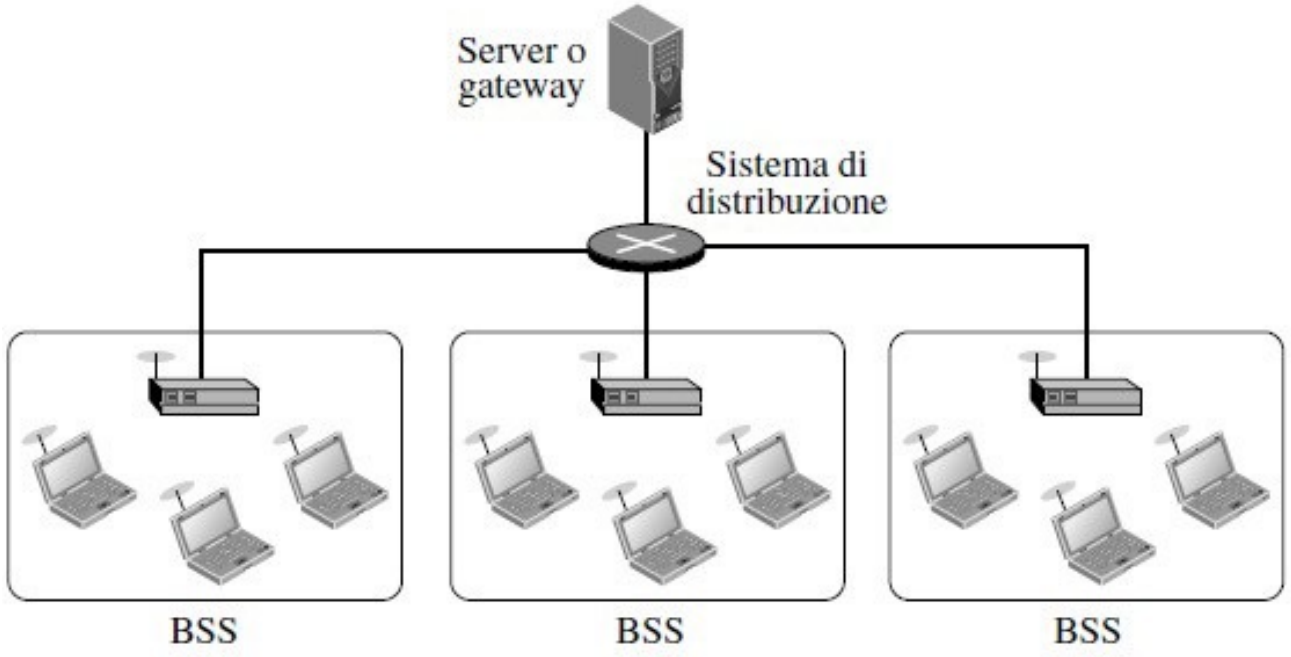


BSS ad hoc

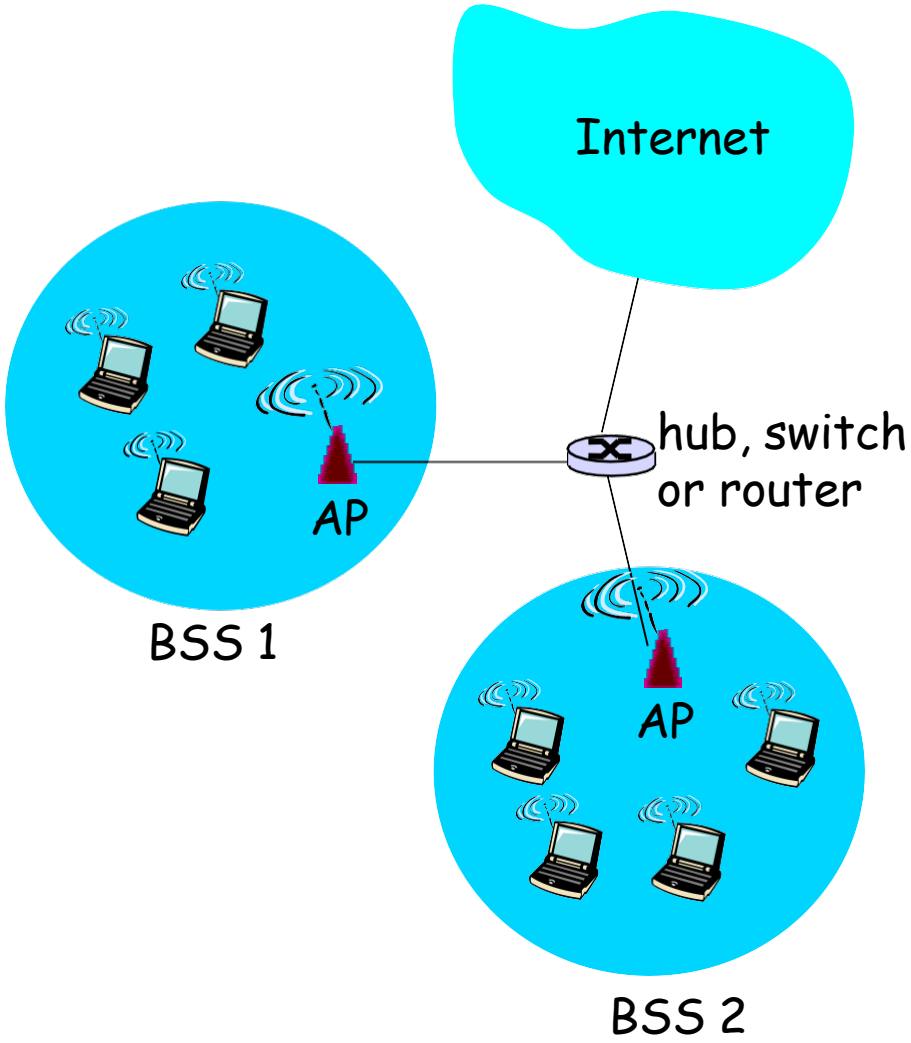
- Rete *standalone*

# Architettura: ESS

- Extended service set (ESS) è costituito da due o più BSS con infrastruttura
- I BSS sono collegati tramite un sistema di distribuzione che è una rete cablata (Ethernet) o wireless
- Quando i BSS sono collegati, le stazioni in visibilità comunicano direttamente mentre le altre comunicano tramite l'AP



# Architettura generale

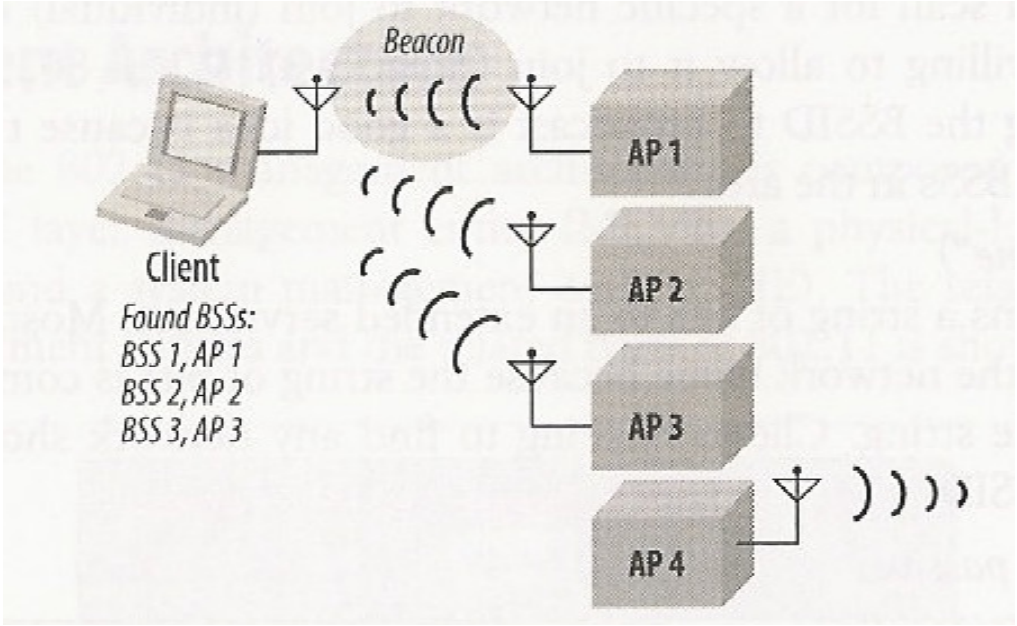



- BSS corrispondono alle **celle** delle reti cellulari

# Canali e Associazione

- Lo spettro 2.4GHz-2.485GHz è diviso in 11 canali parzialmente sovrapposti
  - L'amministratore dell'AP sceglie una frequenza
  - Sono possibili interferenze (stesso canale per AP vicini)
  - Il numero massimo di frequenza utilizzabili da diversi AP perevitare interferenze è 3 (usando i canali 1,6,11). I canali non interferiscono se separati da 4 o più canali

- L'architettura IEEE 802.11 prevede che una stazione wireless si associ a un AP per accedere a Internet



# Canali e Associazione

Associazione di una stazione a un AP

- E’ necessario conoscere gli AP disponibili in un BSS
- E’ necessario un protocollo di associazione
  - AP invia segnali periodici (beacon) che includono l’identificatore dell’AP (Service Set Identifier - SSID) e il suo indirizzo MAC
  - La stazione wireless che vuole entrare in un BSS scandisce gli 11 canali trasmissivi alla ricerca di frame beacon (passive scanning)
  - Alla fine della scansione la stazione sceglie l’AP da cui ha ricevuto il beacon con la maggiore potenza di segnale (o maggiore SSR) e gli invia un frame con la richiesta di associazione
  - L’AP accetta la richiesta con un frame di risposta associazione che permetterà all’host entrante di inviare una richiesta DHCP per ottenere un indirizzo IP
  - Può essere prevista un’autenticazione per eseguire l’associazione

# Protocollo MAC 802.11

- Più stazioni possono voler comunicare nello stesso momento
- 2 tecniche di accesso al mezzo:
  - Distributed Coordination Function (DCF) in cui i nodi si contendono l'accesso al canale
  - Point coordination function (PCF) in cui non c'è contesa e l'AP coordina l'accesso dei nodi al canale
- Vediamo DCF!

# CSMA/CA

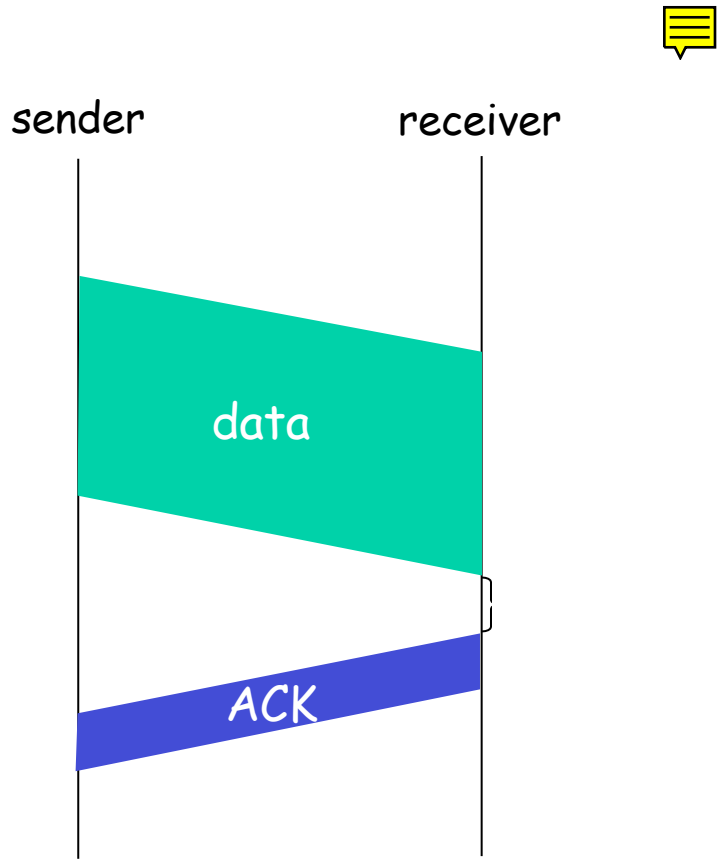
- Evitare le collisioni: due o più nodi che trasmettono simultaneamente
- Carrier sense: ascoltare il canale prima di trasmettere
- No collision detection per 3 motivi:
  - Impossibilità di trasmettere e ricevere contemporaneamente
  - Hidden terminal problem
  - Raggio di trasmissione limitato (difficile “sentire” tutte le trasmissioni)
- CSMA/Collision(C) Avoidance (A)

# CSMA/CA: ACK

- E’ necessario utilizzare riscontri positivi (ACK) e timer per capire se la trasmissione è andata a buon fine

# CSMA/CA: ACK

- No collision detection
- Necessità di riscontro per capire se una trasmissione è andata a buon fine (no collisione)
- ACK
- Carrier sense ascolta la presenza di
  - Dati
  - ACK
- Possibilità di collisione anche su ACK



# CSMA/CA: spazio interframe

- IFS (spazio interframe): Rilevata la portante, se il canale risulta libero, si rimanda la trasmissione per evitare che stazioni che hanno già iniziato a trasmettere collidano con la stazione che vuole trasmettere
  - SIFS: Short IFS realizza alta priorità
  - DIFS: Distributed IFS realizza bassa priorità

# CSMA/CA: spazio interframe

Mittente: ascolta il canale

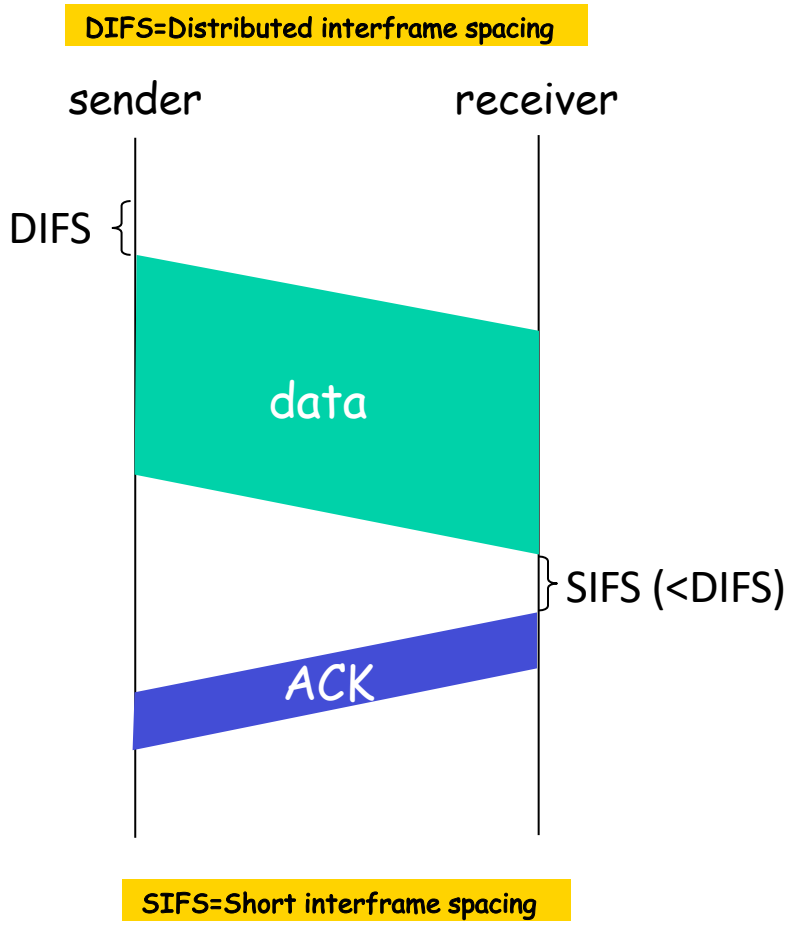
- Se libero per DIFS tempo allora trasmette
- DIFS: DCF Interframe Space

Ricevente

- Se frame ricevuto correttamente allora invia ACK dopo SIFS tempo
- SIFS: Short Interframe Space

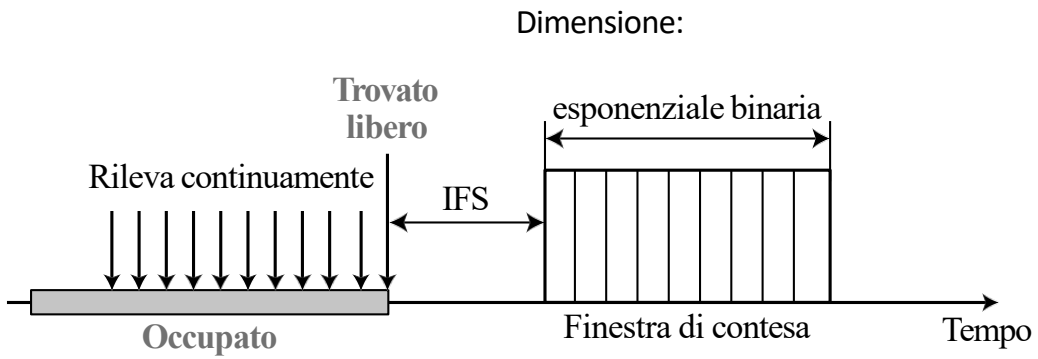
  = sense + inizio trasmissione

- DIFS > SIFS per dare priorità alle comunicazioni già iniziate (priorità ad ACK)



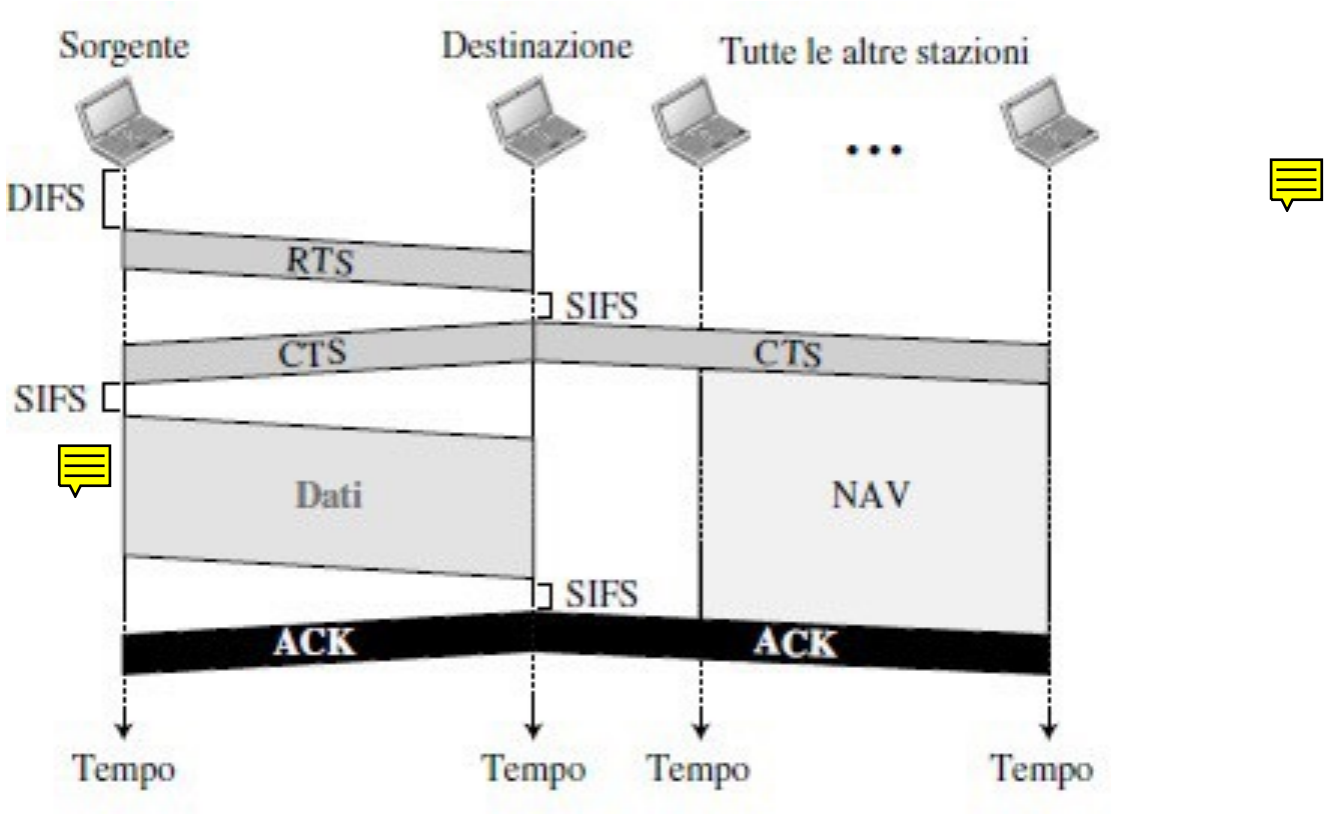
# CSMA/CA: finestra di contesa

- Dopo aver atteso un tempo DIFS, se il canale è ancora inattivo, la stazione attende un tempo di contesa (non succede per il SIFS)
- Finestra di contesa (Contention window): lasso di tempo (backoff) per cui deve sentire il canale libero prima di trasmettere (il tempo è suddiviso in slot e a ogni slot si esegue il sensing del canale)
  - Scegli R random in [0,CW]. (CW dipende da collissioni precedenti)
  - While R>0
    - ascolta il canale per uno slot
    - Se il canale è libero per la durata dello slot → R:= R-1, altrimenti attende: interrompe il timer e aspetta che il canale si liberi (e riavvia il timer)



# CSMA/CA: RTS/CTS

- Il problema dell'hidden terminal non viene risolto con gli IFS e finestra di contesa
- È necessario un meccanismo di prenotazione del canale: Request-to-send (RTS) Clear-to-send (CTS)



# Evitare collisioni sul destinatario

- Come fanno le stazioni che non sono coinvolte nella comunicazione (ma sono nel raggio di trasmissione della destinazione) a sapere per quanto tempo devono astenersi dal trasmettere?

(ascoltando il canale non sono in grado di rilevare la trasmissione)

# Network Allocation Vector (NAV)

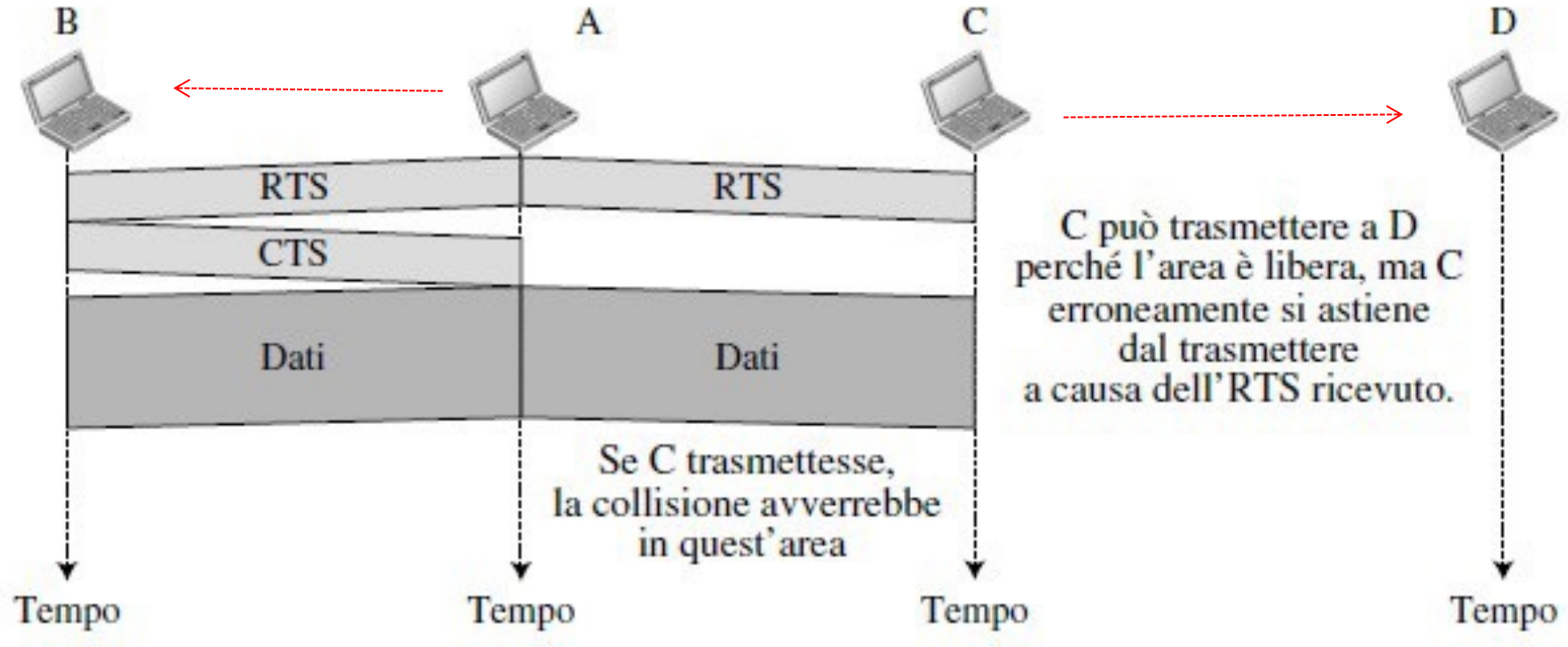
- Quando una stazione invia un frame RTS include la durata di tempo in cui occuperà il canale per trasmettere il frame e ricevere l'ack
- Questo tempo viene incluso anche nel CTS
- Le stazioni che sono influenzate da tale trasmissione avviano un timer chiamato NAV che indica quanto tempo devono attendere prima di eseguire il sensing del canale
- Ogni stazione prima di ascoltare il canale verifica il NAV

# Collisioni durante l’handshaking

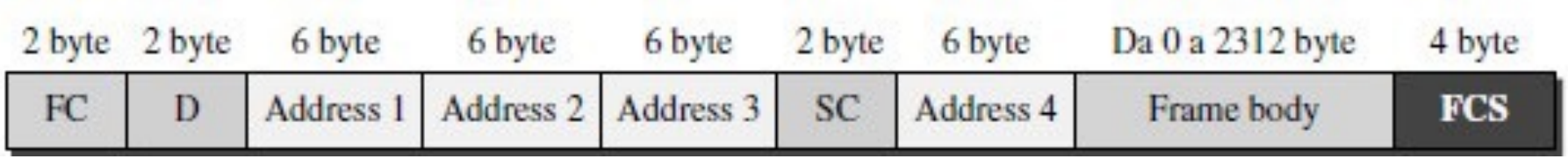
- Cosa succede se avviene una collisione durante la trasmissione di RTS o CTS?
- Se il mittente non riceve CTS allora assume che c’è stata collisione e riprova dopo un tempo di backoff

# Problema della stazione esposta

- Una stazione (nell'esempio C) si astiene dall'usare il canale anche se potrebbe trasmettere (C è la stazione esposta)
- Per questo esiste RTS threshold: per pacchetti piccoli non si usa RTS/CTS
  - RTS/CTS si può anche abilitare/disabilitare

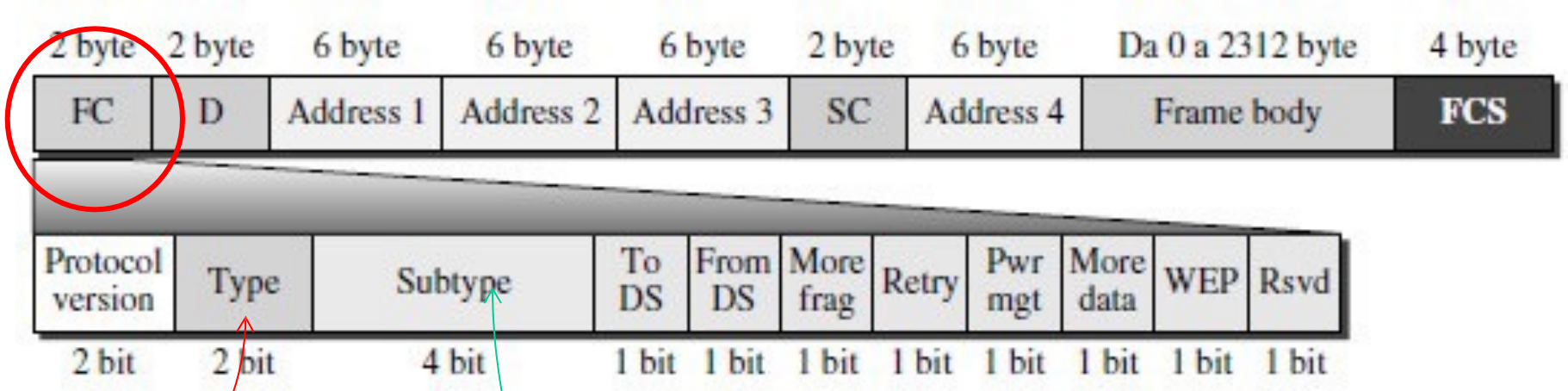


# Formato del frame



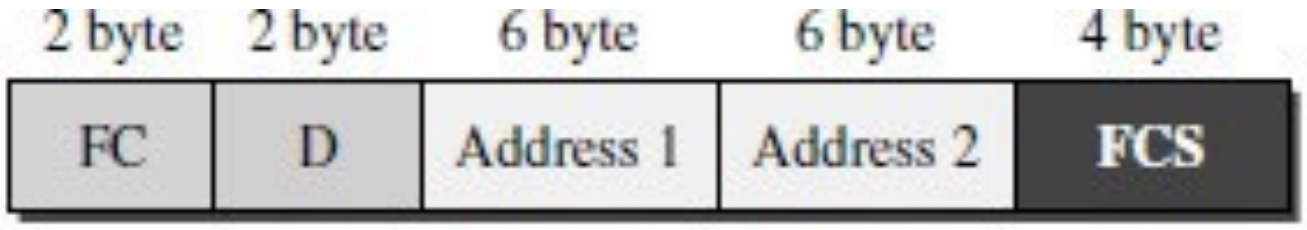

- Frame Control (FC) tipo di frame e alcune informazioni di controllo
- D: durata della trasmissione, usata per impostare il NAV (Impostata sia per DATA che per RTS, CTS frame)
- Indirizzi: indirizzi MAC (descritti inseguito)
- SC: informazioni sui frammenti (# frammento e # sequenza). Il numero di sequenza serve per distinguere frame ritrasmessi come nel livello trasporto (ACK possono andare perduti)
- Frame Body: payload
- FCS: codice CRC a 32 bit

# Formato del frame

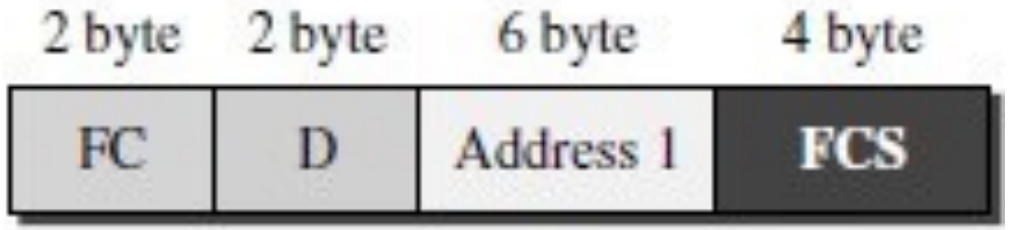



- Una LAN wireless ha 3 categorie di frame: gestione, controllo e dati
- 00: Frame di gestione: usati per le comunicazioni iniziali tra stazioni e punti di accesso
- 01: Frame di controllo: si usano per accedere al canale e dare riscontro (1011: RTS, 1100: CTS, 1101: ACK)
- 10: Frame di dati: vengono usati per trasportare i dati

# Frame di controllo

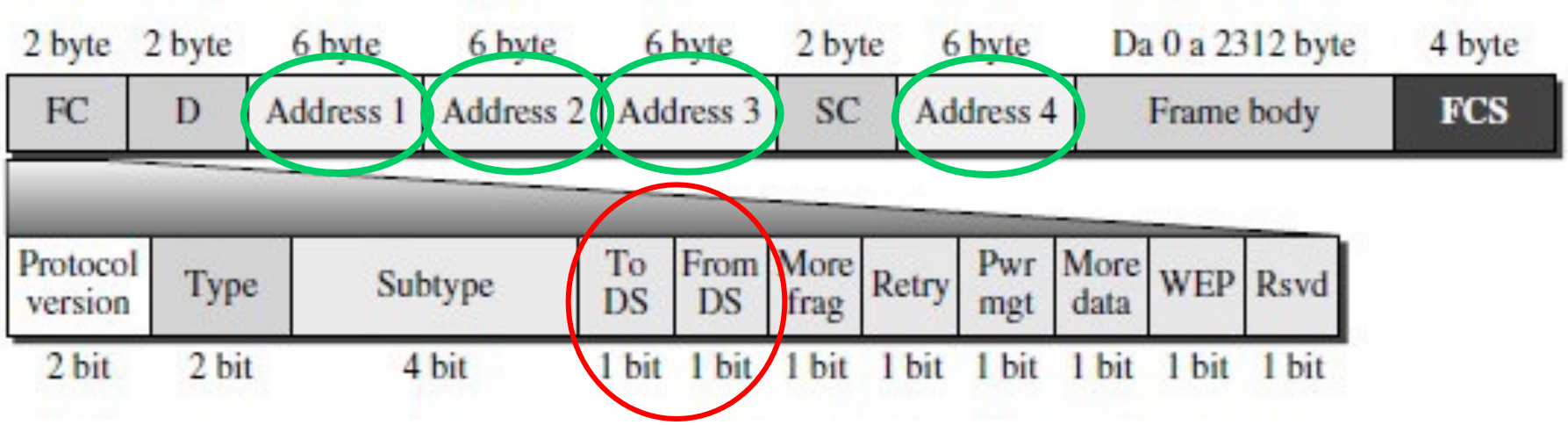



RTS




CTS o ACK

# Indirizzamento




DS: sistema di distribuzione

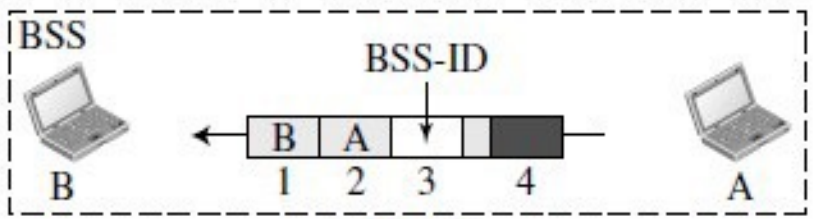
| *To DS* | *From DS* | *Address 1* | *Address 2* | *Address 3* | *Address 4* |
|---|---|---|---|---|---|
| 0 | 0 | Destinazione | Sorgente | BSS ID | N/A |
| 0 | 1 | Destinazione | AP mittente | Sorgente | N/A |
| 1 | 0 | AP ricevente | Sorgente | Destinazione | N/A |
| 1 | 1 | AP ricevente | AP mittente | Destinazione | Sorgente |

Indirizzo del dispositivo successivo a cui viene trasmesso il frame

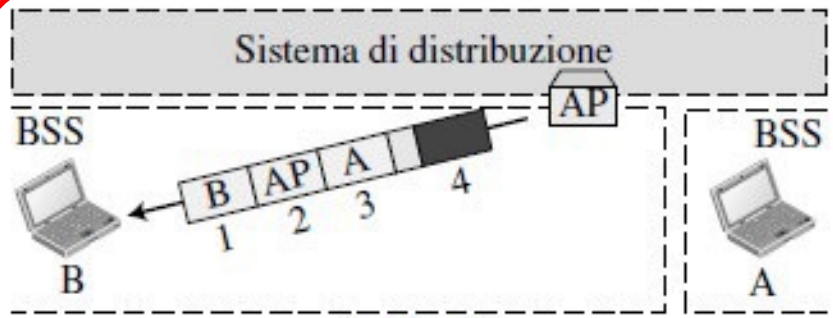
Indirizzo del dispositivo che il frame ha lasciato

# DS: sistema di distribuzione

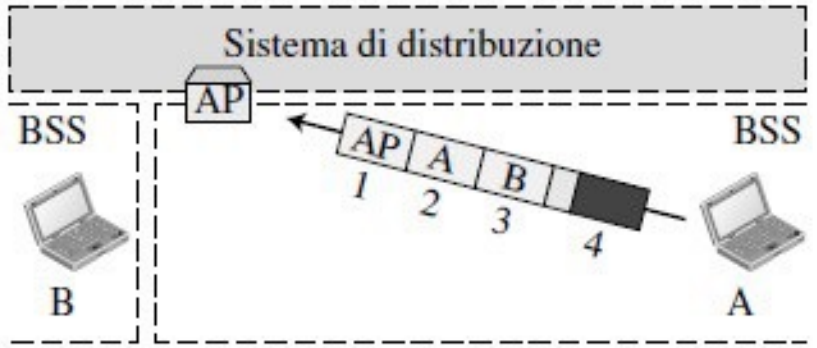
| *To DS* | *From DS* | *Address 1* | *Address 2* | *Address 3* | *Address 4* |
|---|---|---|---|---|---|
| 0 | 0 | Destinazione | Sorgente | BSS ID | N/A |
| 0 | 1 | Destinazione | AP mittente | Sorgente | N/A |
| 1 | 0 | AP ricevente | Sorgente | Destinazione | N/A |
| 1 | 1 | AP ricevente | AP mittente | Destinazione | Sorgente |



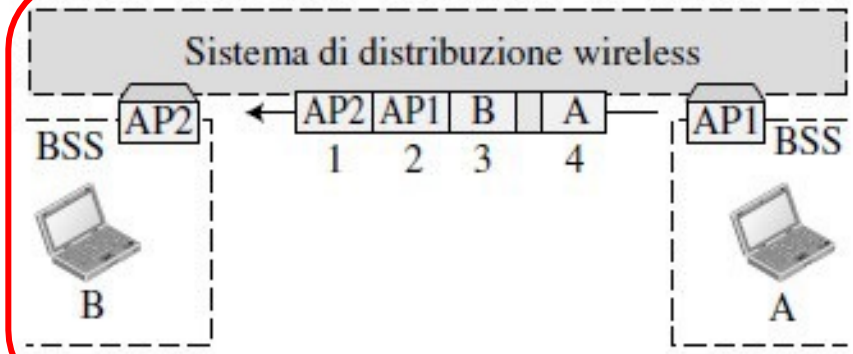
a. Caso 1



b. Caso 2



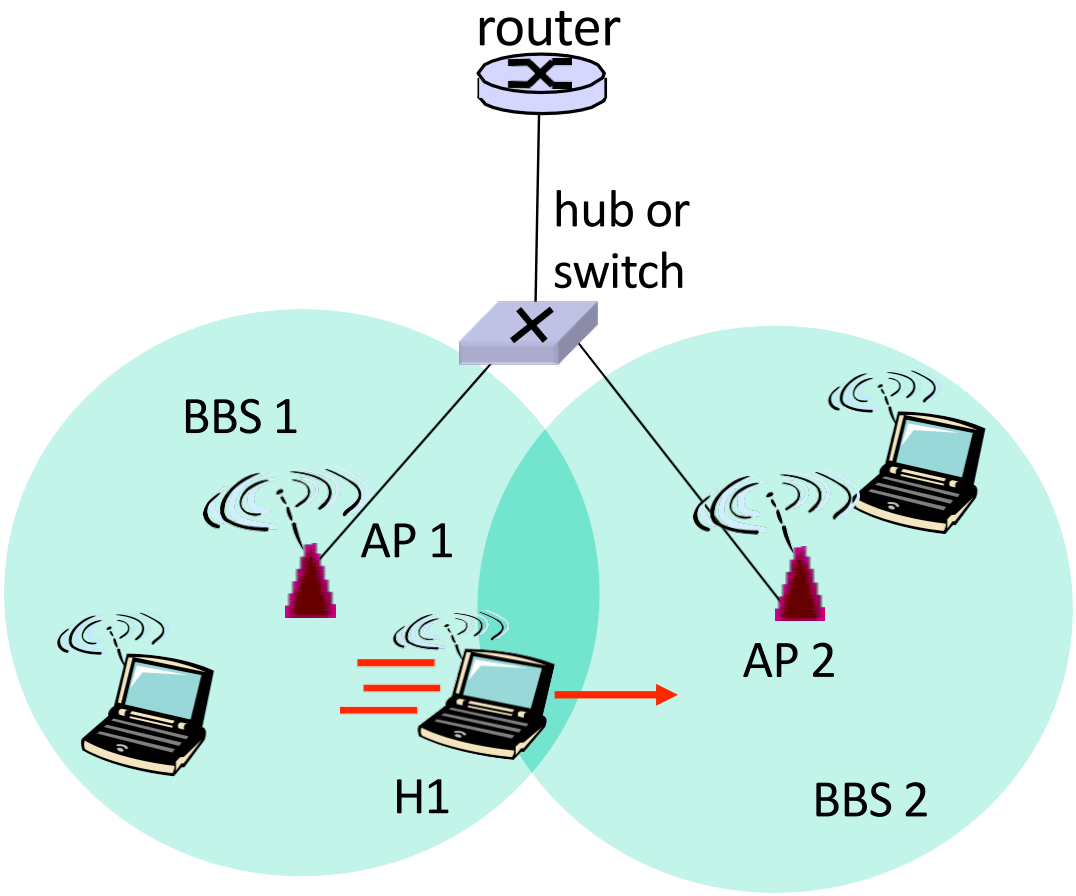
c. Caso 3



d. Caso 4

# Mobilità all'interno della stessa sottorete IP

- Semplice all'interno della stessa rete
- L'indirizzo IP rimane lo stesso
- Come avviene il cambio di AP mantenendo attive tutte le connessioni TCP?



# Mobilità (roaming)

- H1 sente che il segnale da AP1 si affievolisce e avvia una scansione per un segnale più forte
- H1 rileva AP2, si disassocia da AP1 e si associa a AP2, mantenendo lo stesso IP e sessioni TCP
- Come si comporta lo switch?
  - Autoimpara, ma non può supportare utenti con elevata mobilità
  - AP2 invia un frame broadcast allo switch con indirizzo mittente H1 e lo switch capisce che H1 è ora nel BSS2
- Un protocollo inter-AP è in via di sviluppo