# Reti di Telecomunicazioni


## Livello Data Link

## Wireless

# Autori

Queste slides sono state scritte da

Michele Michelotto:

michele.michelotto@pd.infn.it

che ne detiene i diritti a tutti gli effetti

# Copyright Notice

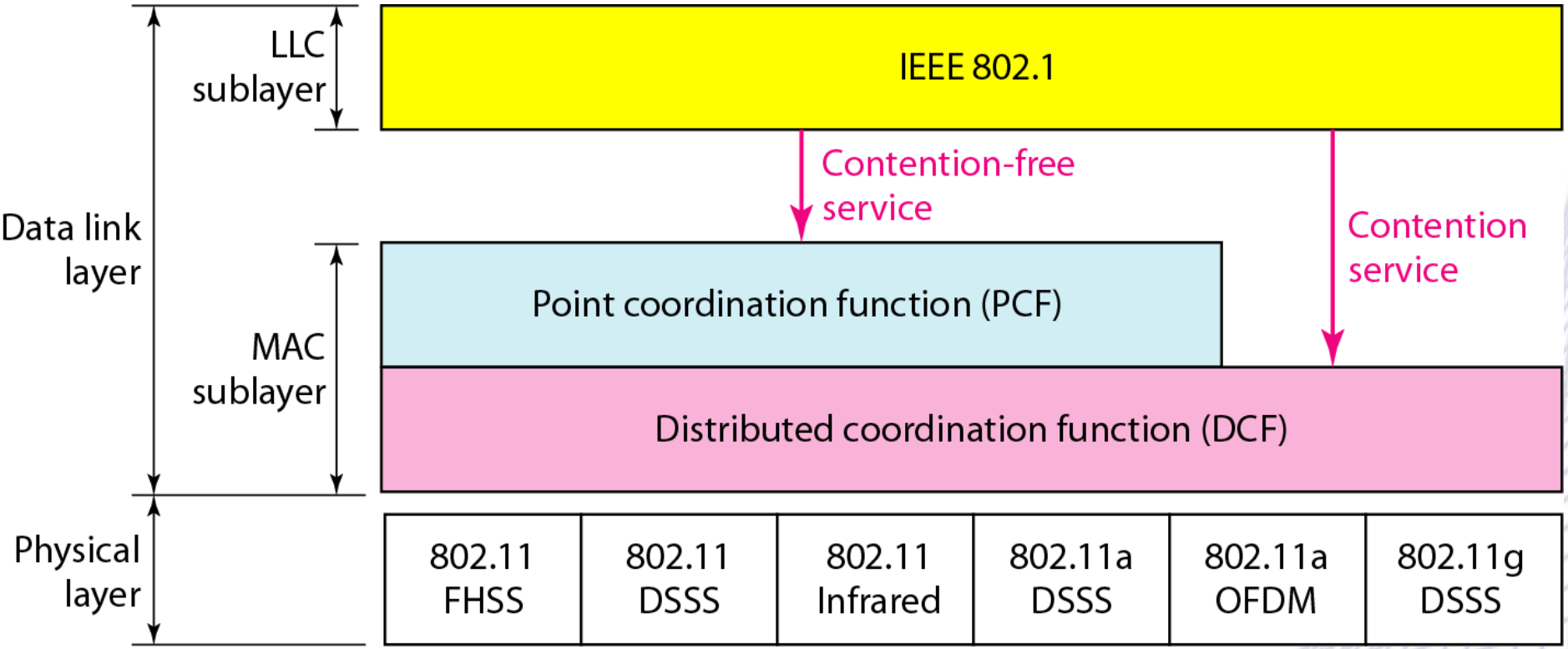
# Wireless


- Vedremo in queste slides alcune famiglie di protocolli wireless
- 802.11 Wireless LAN
- 802.16 Wireless MAN
- 802.15 Bluetooth, Wireless PAN

# 802.11 e WiFi

- 1997: 802.11.y (Legacy)
  - Infrarosso: Come il telecomando del TV, poi elimitata per scarso successo commerciale
  - Uso di bande radio ISM (Industrial Scientifical Medical)
  - 802.11 a 2.4 GHz con tecniche FHSS e DSSS, (interferiscono con forno a microonde, telecomando del cancello e telefoni cordless) Operano a 1 o 2 Mbps a bassa potenza
- 1999: Tecniche OFDM e HR-DSSS operano a 54 e 11Mbps
- 2001 una nuova modulazione OFDM  a 5 GHz

# Stack 802.11


LLC sublayer
IEEE 802.1
Contention-free service
Contention service
Data link layer
MAC sublayer
Point coordination function (PCF)
Distributed coordination function (DCF)
Physical layer
802.11 FHSS
802.11 DSSS
802.11 Infrared
802.11a DSSS
802.11a OFDM
802.11g DSSS

# Infrarosso

- Usa trasmissione diffusa (non a linea visiva) a 0.85µm o 0.95µm
  - Non penetra i muri, ottimo isolamento ma sensibile a illuminazione solare
- A 1Mbps
  - un gruppo di 4 bit viene codificato come una codeword a 16bit con 15 **“0”** e un singolo **“1”** (**Gray code**)
  - Un piccolo errore di sincronizzazione porta ad un errore a singolo bit nell’output
- A 2 Mbps:
  - 2 bit producono una codeword da 4 bit con un singolo “1” (0001, 0010, 0100, 1000)

# FHSS

- **Frequency Hopping Spread Spectrum**: usa 79 canali da 1 MHz partendo da 2.4 GHz
- Un generatore pseudorandom produce la sequenza di salti, le stazioni che usano lo stesso seed restano sincronizzate
- Il tempo in una certa frequenza (**dwell**) si può scegliere ma deve rimanere sotto i 400msec.
- Difficile da sniffare se non si conosce la sequenza di hopping o il dwell time
- Buona resistenza al **multipath fading** che potrebbe dare problemi su lunghe distanze

# DSSS

- Direct Sequence Spread Spectrum
  - Anche questo solo fino a 1 o 2 Mbps
  - Usa tecnologia CDMA
  - Usa Phase Shift Modulation
    - 1 bit per baud a 1 Mbps
    - 2 bit per baud a 2 Mbps

# High Speed Wireless

- 802.11a
  - ODFM nella banda più larga a 5GHz
  - max 54 Mbps
- 802.11b
  - HR-DSSS nella banda a 2.4 GHz
  - max 11 Mbps
  - Non deriva da 802.11a anzi è stata approvata per prima ed è arrivata sul mercato per prima
- 802.11g
  - Miglioramento di 802.11b a 2.4 GHz ma usa ODFM come 802.11a
  - Arriva fino a 54 Mbps

# HR-DSSS (802.11b)

- High Rate Direct Sequence Spread Spectrum fino a 11 Mbps nella banda a 2.4 GHz
  - Supporta 1,2,5.5 e 11 Mbps
  - Una gran parte della banda viene sacrificata per l'overhead di CSMA per cui al massimo ottengo 5.9 Mbps (TCP)  o 7.1 Mbps (UDP)
  - 1 e 2 Mbps a 1 Mbaud come DSSS per compatibilità
  - A 5.5 e 11 Mbps usa 1,375 Mbaud con 4 e 8 bits/baud usando codici Complementary Code Keying (CCK)
  - Cambia dinamicamente secondo il rumore tra le quattro velocità.
  - Pur essendo più lento di 802.11a ha un range di 7 volte superiore

# 802.11g

- Versione migliorata di **802.11b** ratificata nel 2003
  - usa OFDM come **802.11a** ma opera nella banda stretta a 2.4 GHz insieme a **802.11b**
  - Il data rate massimo è 54 Mbps (24.7 netto)
  - Altri data rate 6,9,12,18,36 e 48 oppure scende a 5.5 e 11Mbps di 802.11b
  - Soffre delle interferenze della banda a 2.4 (forni a microonde e cordless)
  - Alcuni produttori hanno varianti non standard che raddopiano la velocità accoppiando due canali

# Canali a 2.4 GHz

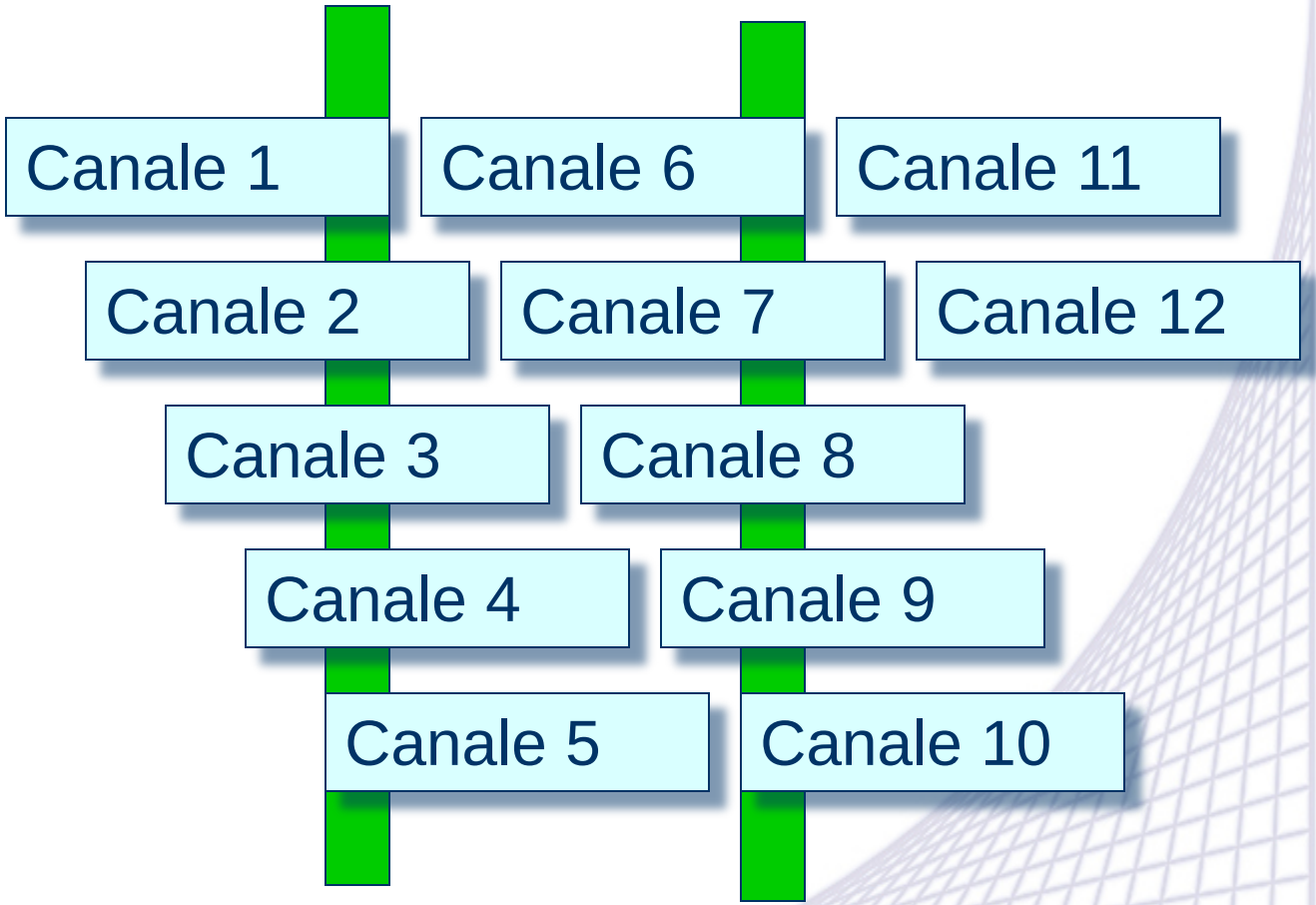
- 802.11b e 802.11g si dividono lo spettro in 14 canali da 22 MHz l'uno
- I canali sono parzialmente sovrapposti quindi tra due canali consecutivi c'è molta interferenza
- 2 gruppi di canali (1,6,11) e (2,7,12) sono completamente separati e vengono usati quando ci sono diverse reti wireless
- Solo i canali 10 e 11 sono utilizzabili ovunque perché per esempio in Spagna non sono utilizabili i canali da 1 a 9 e molte nazioni hanno solo i primi 11 canali

# Aspetti pratici

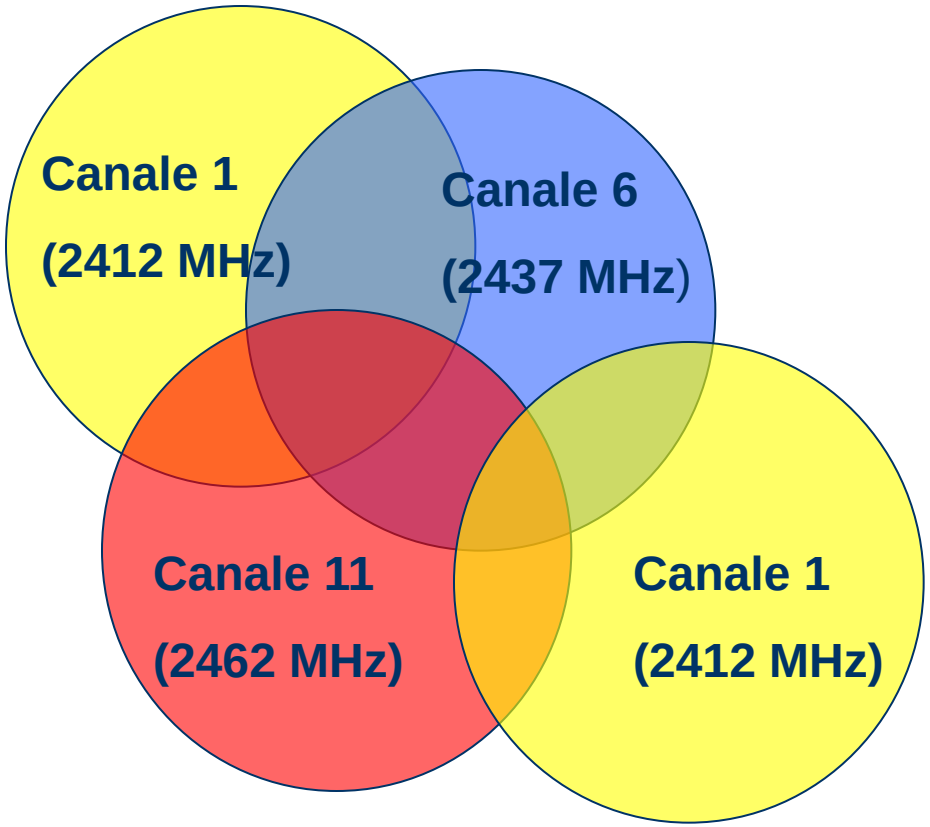
- La banda netta è inferiore a quella nominale per l'overhead di 802.11
- La banda con un singola stazione cala molto con l'aumentare della distanza dall'AP
- **La banda viene condivisa dai diversi client**
- Meglio non mettere più di una decina di client nella stessa frequenza
- Se si vogliono servire più utenti usare diversi terminali ma attenzione agli overlap di banda

# Canali sovrapposti

- Vediamo come i canali siano da 1 a 5 siano sovrapposti
- Anche **ch1** e **ch5** hanno un leggero overlap
- Solo il **ch6** è completamente separato da **ch1** e di nuovo il **ch11**



# Riuso dei canali




Spostando gli AP e lavorando sulle potenze dei canali posso fare in modo che i canali della stessa frequenza non si sovrappongano

I canali 1, 6 e 11 posso sovrapporsi nello spazio dal momento che sono completamente separati in frequenza

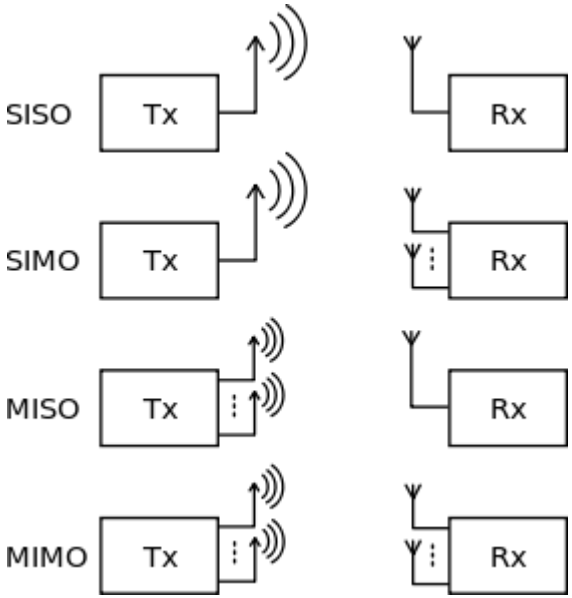
# OFDM 802.11a

- Orthogonal FDM
  - Fornisce 54 Mbps nella banda a 5 GHz, ho 12 canali non sovrapposti
  - Scende se necessario a 48,36,24,18,12,9  e 6 Mbps
  - Non è interoperabile con 802.11b a meno di apparati dual standard
  - Opera in una banda a 5GHz più libera rispetto a quella ISM ma in pratica richiede linea visiva perché viene assorbita maggiormente dai muri
  - In pratica arrivo a 20 Mbps netti
  - Schema complesso di encoding con phase-shift modulation fino a 18 Mbps e QAM al di sopra.
  - A 54 Mbps 216 bits di dati sono codificati in simboli di 288 bits

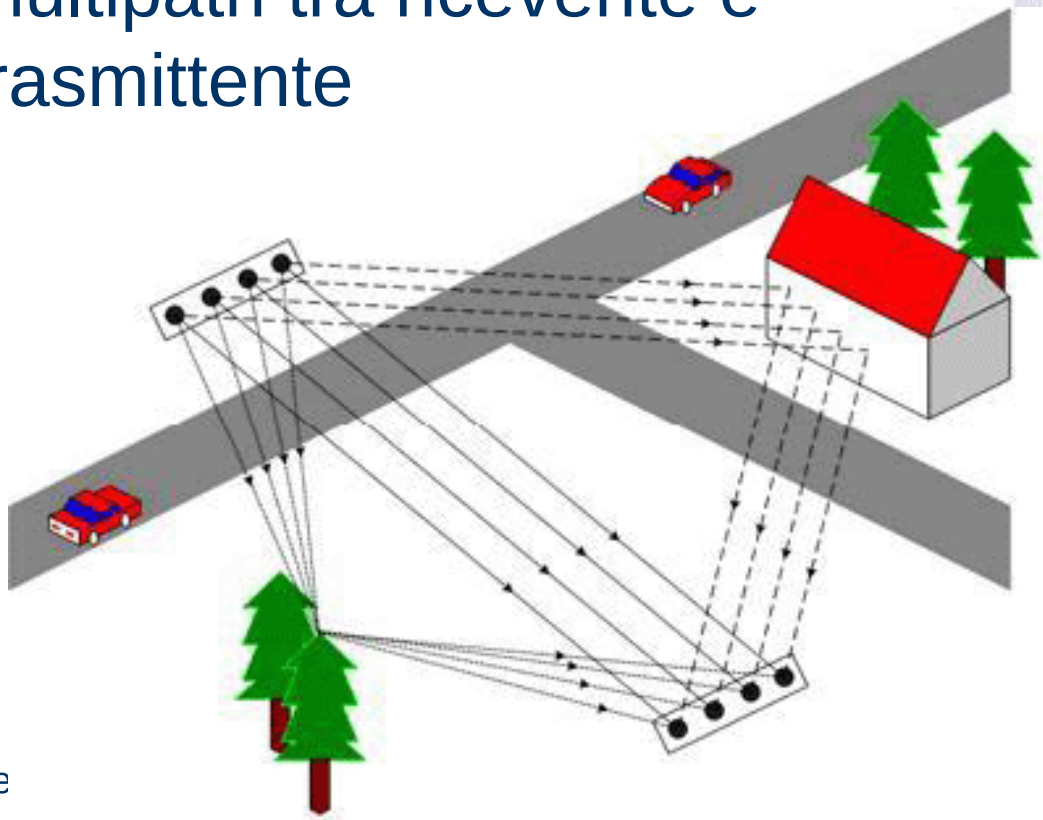
# 802.11n

- Modifica allo standard 802.11
  - Studi iniziati nel 2004, Draft 2.0 a inizio 2007 publicato il draft 3.0. Standard finale nel 2009
  - Data rate attorno a 100 – 2000 Mbps (fino a 250 – 600 Mbps a livello fisico)
  - Opera a 2.4 e 5.0 Ghz con range da 70m indoor a 250m outdoor
- Può usare MIMO (Multiple Input, Multiple Output) a livello fisico
  - In pratica diverse antenne riceventi e trasmittenti per aumentare il throughput usando multiplexing spaziale e codici evoluti
  - Le antenne possono cambiare il guadagno in certe direzioni

# MIMO




- I canali MIMO funzionano bene quando ci sono multipath tra ricevente e trasmittente



# 802.11y

- Proposta di estensione allo standard 802.11 su bande soggette a licenza (3650-3700 MHz) negli USA
- Può usare potenze molto elevate per operare fino a 5km
- Servono meccanismi di prenotazione per gestire la contention
- Potrebbe essere esteso per operare anche a 4.9, 5, 10 o 20 GHz

# Formati proprietari

- Oltre gli standard IEEE molti produttori hanno annunciato prodotti che sfruttano tecnologie proprietarie
- Chiaramente vanno usati anche client proprietari
- Esempi
  - SuperG di Atheros fino a 108 Mbps
  - Afterburner di Broadcom
  - Turbo mode (Texas Instruments) 125 Mbps
  - Nitro Extreme (Prism) 140 Mbps

| STANDARD | 802.11b | 802.11a | 802.11g | 802.11a/g | 802.11n |
|---|---|---|---|---|---|
| Primi prodotti | 1999 | 2001 | 2003 | 2003 | 2006 |
| Costo AP | 55-180 | 100-130 | 130-200 | 300 | 300 |
| Costo Card | 30-90 | 100 | 80-130 | 100 | 100 |
| Freq (GHz) | 2.4 | 5.0 | 2.4 | 2.4 e 5 | 2.4 e 5 |
| Mbps teorico | **11** | **54** | 54 | 54 | 600 |
| Throughput 7-20m | **4** | **23** | 19 | 15-20 | 70-300 |
| Range outdoor (m) | **50** | **35** | 50 | 50 | 70 |
| Modulazione | Dsss | Ofdm | Ofdm | Ofdm | MIMO |
| Compatibile | 802.11g | | 802.11b | 802.11 abg | N.d. |
| Max users | 32 | 64 | 64 | 128 | N.d. |
| note | diffuso | USA | diffuso | Poco diff. | attuale |
| Canali non sovrap. | **3** | **12** | 3 | 12 | |

# 802.11n

- Come arriviamo da 54 a 600 Mbps?
- Aumenta le sottoportati OFDM da 48 a 52 (con questo andiamo da 54 a 58.5 Mbps)
- FEC Max Forward Error Correction da 3/4 a 5/6 ci porta da 58.5 a 65 Mbps
- Intervallo di guardia da 800ns a 400ns da 65 a 72 Mbps
- MIMO. Riesco ad aumentare il throughput con il numero di antenne (con 2 raddoppio, con 3 triplico, fino a ad un massimo di 4). 4 streams da 72 mi danno 288.9
- Canali da 40 MHz invece che 20 (optional mode, non sempre usabile). Sottoportanti da 52 a 108)

# 802.11n real throughput

- Ma il throughput raw non ci dice molto.
- 802.11a/g fornisce 54 Mbps ma poi l'overhead a livello MAC lo fa scendere a 26 Mbps oltre il 50% viene perso !
- Con 802.11n invece perdo solo Il 25% per cui da 65 Mbps scendo solo a 50 Mbps
- NB. Queste sono le top speed, ma ci sono poi vari schemi di modulazione quando le condizioni non sono perfette. Per minimizzare questo 802.11n ha vari trucchetti per aggirarli

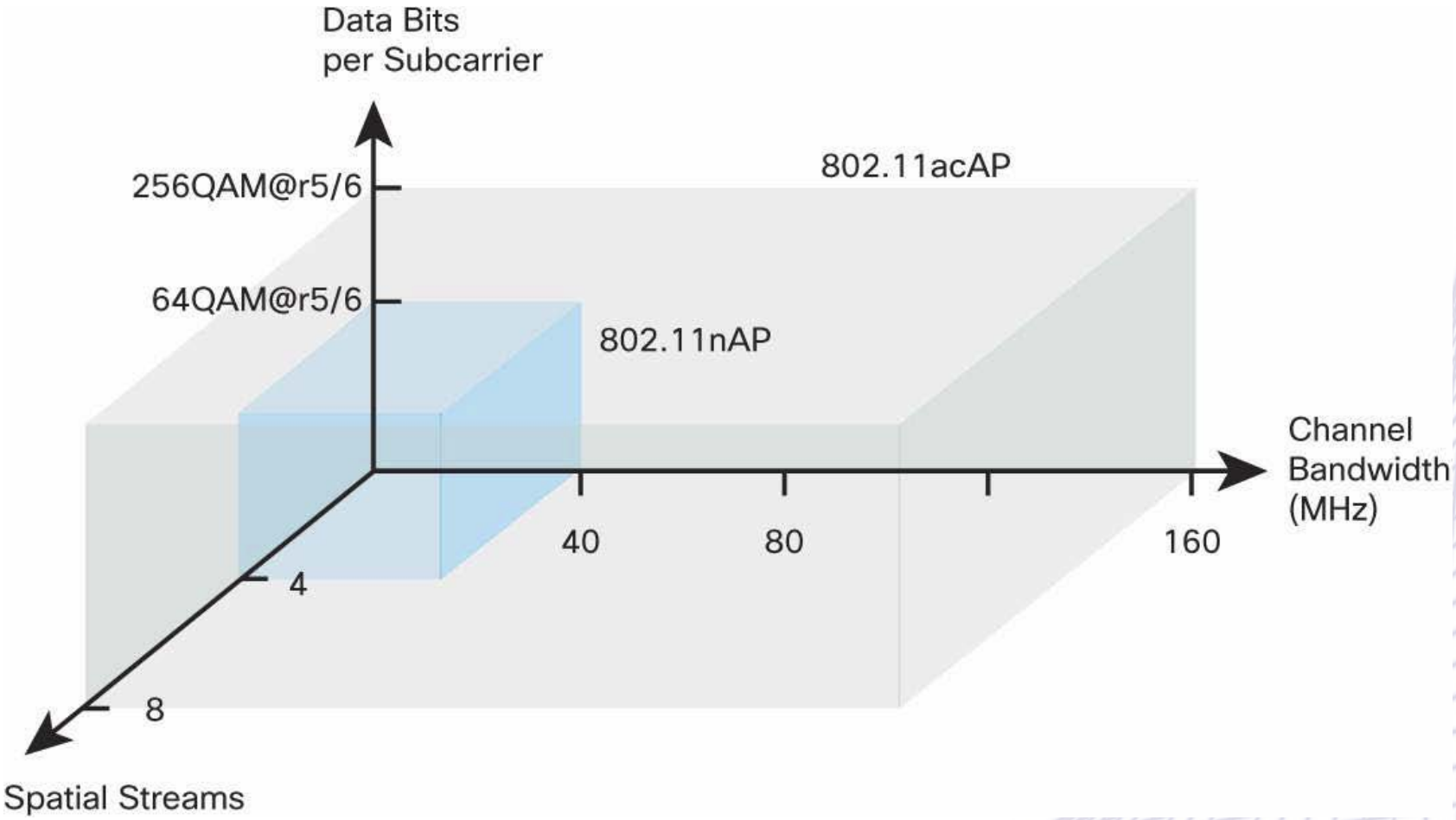
| MCS index | Spatial streams | Modulation type | Coding rate | Data rate (Mbit/s) | | | |
|---|---|---|---|---|---|---|---|
| | | | | 20 MHz channel | | 40 MHz channel | |
| | | | | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI |
| 0 | 1 | BPSK | 1/2 | 6.50 | 7.20 | 13.50 | 15.00 |
| 1 | 1 | QPSK | 1/2 | 13.00 | 14.40 | 27.00 | 30.00 |
| 2 | 1 | QPSK | 3/4 | 19.50 | 21.70 | 40.50 | 45.00 |
| 3 | 1 | 16-QAM | 1/2 | 26.00 | 28.90 | 54.00 | 60.00 |
| 4 | 1 | 16-QAM | 3/4 | 39.00 | 43.30 | 81.00 | 90.00 |
| 5 | 1 | 64-QAM | 2/3 | 52.00 | 57.80 | 108.00 | 120.00 |
| 6 | 1 | 64-QAM | 3/4 | 58.50 | 65.00 | 121.50 | 135.00 |
| 7 | 1 | 64-QAM | 5/6 | 65.00 | 72.20 | 135.00 | 150.00 |
| 8 | 2 | BPSK | 1/2 | 13.00 | 14.40 | 27.00 | 30.00 |
| 9 | 2 | QPSK | 1/2 | 26.00 | 28.90 | 54.00 | 60.00 |
| 10 | 2 | QPSK | 3/4 | 39.00 | 43.30 | 81.00 | 90.00 |
| 11 | 2 | 16-QAM | 1/2 | 52.00 | 57.80 | 108.00 | 120.00 |
| 12 | 2 | 16-QAM | 3/4 | 78.00 | 86.70 | 162.00 | 180.00 |
| 13 | 2 | 64-QAM | 2/3 | 104.00 | 115.60 | 216.00 | 240.00 |
| 14 | 2 | 64-QAM | 3/4 | 117.00 | 130.00 | 243.00 | 270.00 |
| 15 | 2 | 64-QAM | 5/6 | 130.00 | 144.40 | 270.00 | 300.00 |
| 16 | 3 | BPSK | 1/2 | 19.50 | 21.70 | 40.50 | 45.00 |
| 17 | 3 | QPSK | 1/2 | 39.00 | 43.30 | 81.00 | 90.00 |
| 18 | 3 | QPSK | 3/4 | 58.50 | 65.00 | 121.50 | 135.00 |
| 19 | 3 | 16-QAM | 1/2 | 78.00 | 86.70 | 162.00 | 180.00 |
| 20 | 3 | 16-QAM | 3/4 | 117.00 | 130.00 | 243.00 | 270.00 |
| 21 | 3 | 64-QAM | 2/3 | 156.00 | 173.30 | 324.00 | 360.00 |
| 22 | 3 | 64-QAM | 3/4 | 175.50 | 195.00 | 364.50 | 405.00 |
| 23 | 3 | 64-QAM | 5/6 | 195.00 | 216.70 | 405.00 | 450.00 |
| 24 | 4 | BPSK | 1/2 | 26.00 | 28.80 | 54.00 | 60.00 |
| 25 | 4 | QPSK | 1/2 | 52.00 | 57.60 | 108.00 | 120.00 |
| 26 | 4 | QPSK | 3/4 | 78.00 | 86.80 | 162.00 | 180.00 |
| 27 | 4 | 16-QAM | 1/2 | 104.00 | 115.60 | 216.00 | 240.00 |
| 28 | 4 | 16-QAM | 3/4 | 156.00 | 173.20 | 324.00 | 360.00 |
| 29 | 4 | 64-QAM | 2/3 | 208.00 | 231.20 | 432.00 | 480.00 |
| 30 | 4 | 64-QAM | 3/4 | 234.00 | 260.00 | 486.00 | 540.00 |
| 31 | 4 | 64-QAM | 5/6 | 260.00 | 288.80 | 540.00 | 600.00 |

- Tutti i possibili data rate di 802.11n

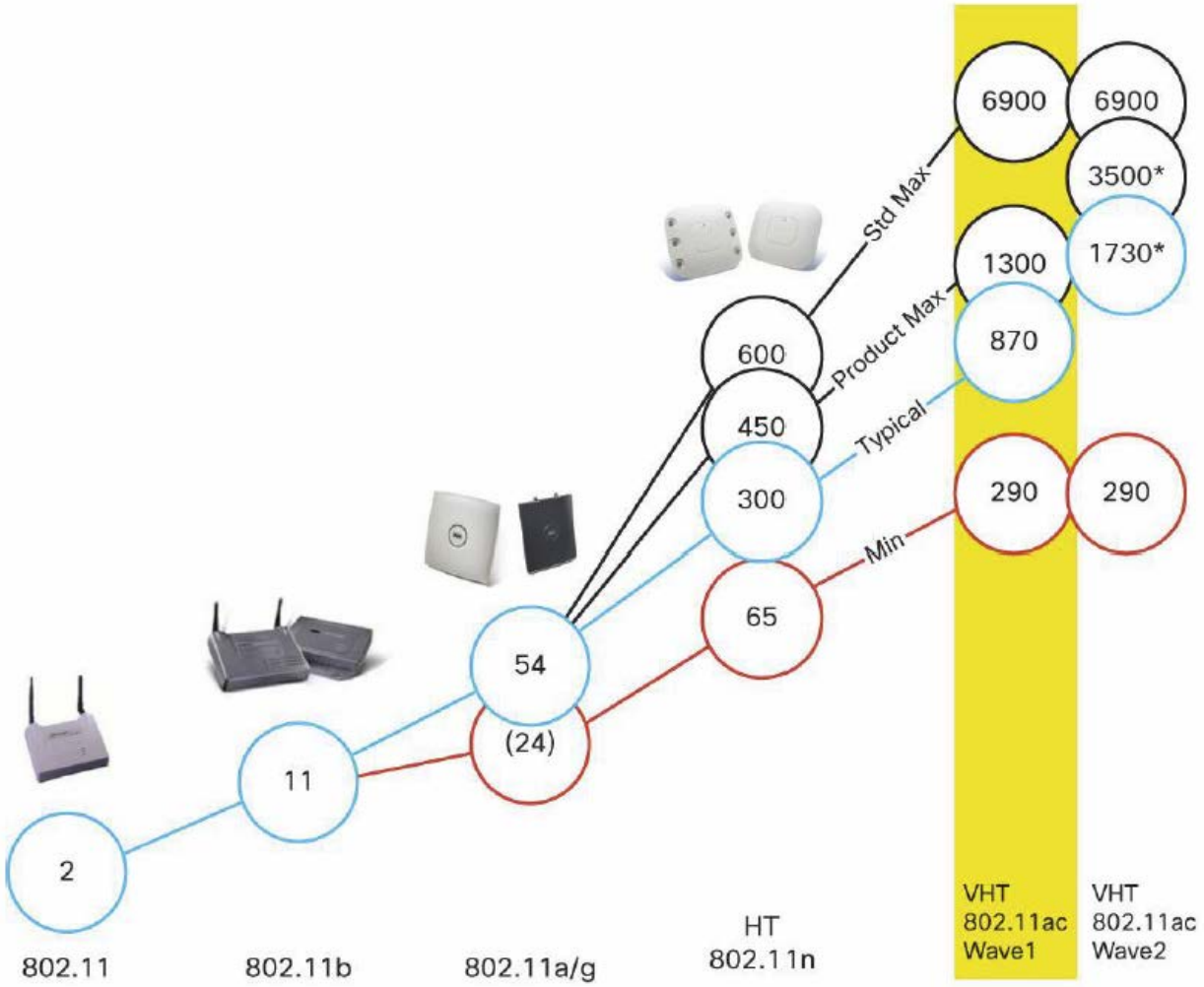
# 802.11ac

- Ulteriore incremento di raw speed
  - Canali anche da 40 MHz fino a 80 MHz e 160 MHz
  - Modulazioni molto dense dai 64 QAM a 256 QAM
  - MIMO da 4 stream fino a 8 stream
- Primi prodotti da 433 Mbps (low end) a 867 o 1300 Mbps (high end)
- 802.11ac usa solo la banda a 5GHz quindi la banda a 2.4 viene usata da 802.11n
- MU-MIMO – Multiuser MIMO
  - 802.11n viene usato come un HUB, un frame a tutte le porte, ma le prossime generazione potrebbero permettere l'accesso a diversi client su porte diverse alla stessa frequenza come fosse uno switch

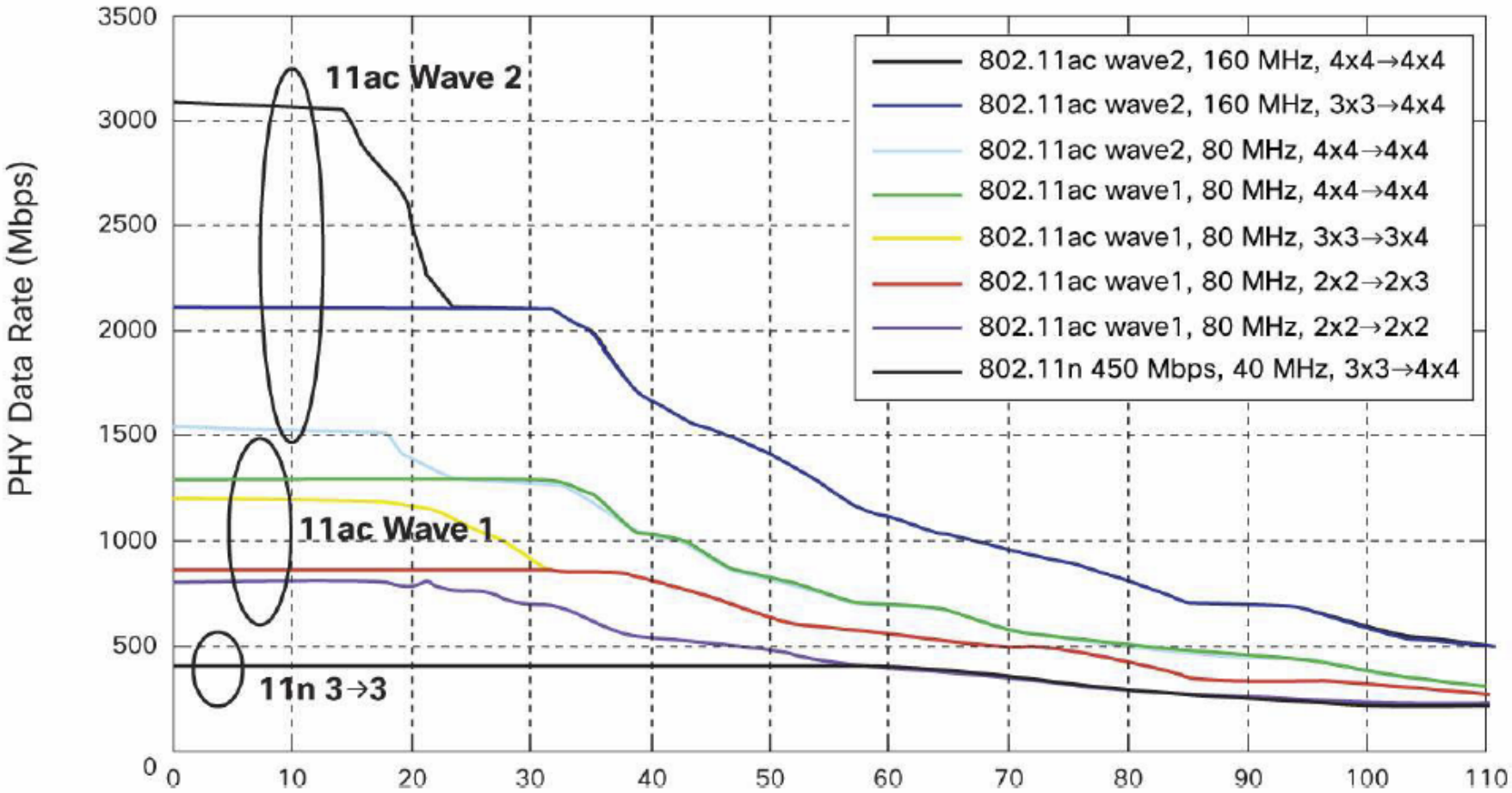
# 802.11ac vs 802.11n



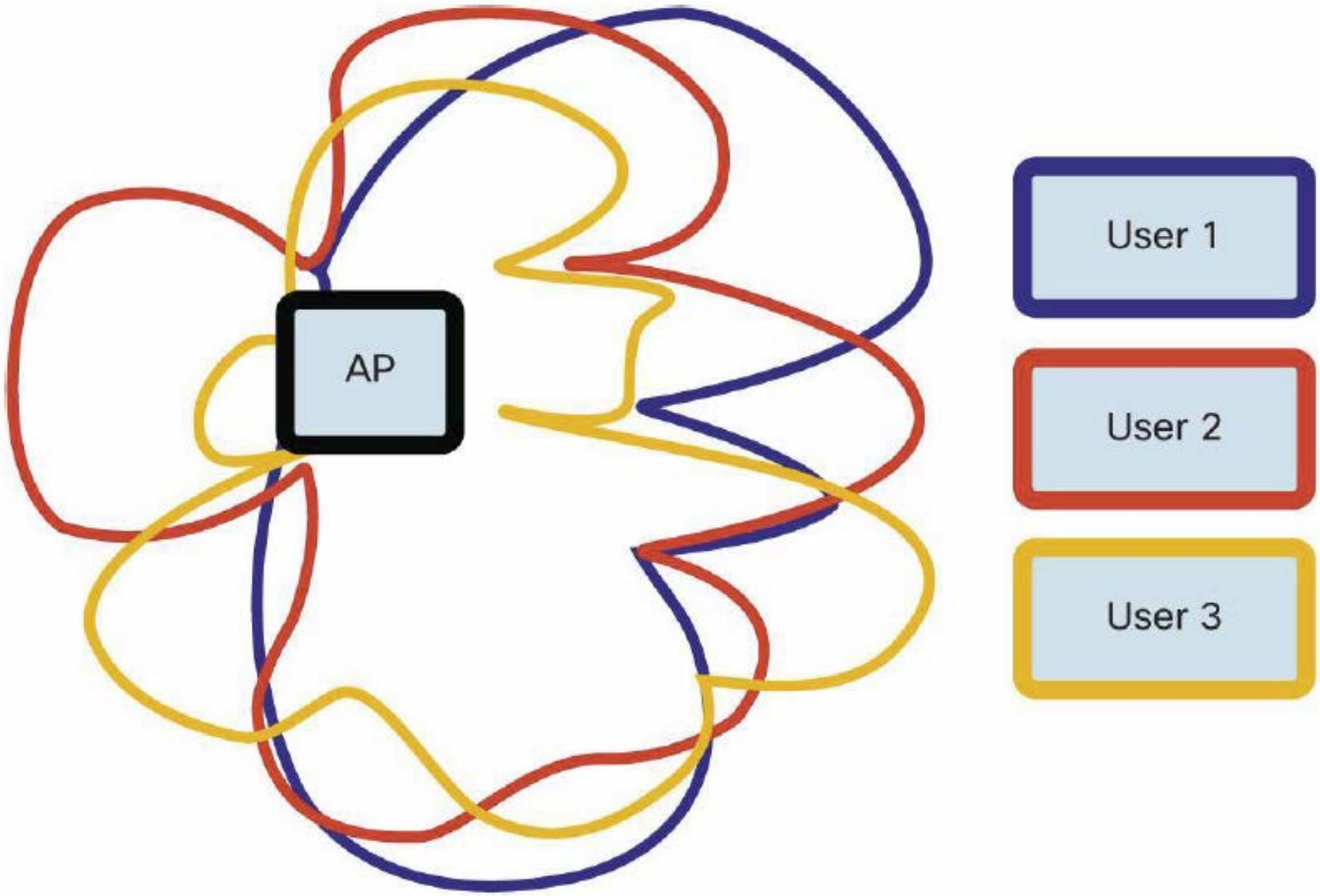
# Evoluzione del layer fisico



# Range – Simulazione



# MU-MIMO



# 802.11ac data rate 1x1

| Theoretical throughput for single Spatial Stream (in Mb/s) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| MCS index | Modulation type | Coding rate | 20 MHz channels | | 40 MHz channels | | 80 MHz channels | | 160 MHz channels | |
| | | | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI |
| 0 | BPSK | 1/2 | 6.5 | 7.2 | 13.5 | 15 | 29.3 | 32.5 | 58.5 | 65 |
| 1 | QPSK | 1/2 | 13 | 14.4 | 27 | 30 | 58.5 | 65 | 117 | 130 |
| 2 | QPSK | 3/4 | 19.5 | 21.7 | 40.5 | 45 | 87.8 | 97.5 | 175.5 | 195 |
| 3 | 16-QAM | 1/2 | 26 | 28.9 | 54 | 60 | 117 | 130 | 234 | 260 |
| 4 | 16-QAM | 3/4 | 39 | 43.3 | 81 | 90 | 175.5 | 195 | 351 | 390 |
| 5 | 64-QAM | 2/3 | 52 | 57.8 | 108 | 120 | 234 | 260 | 468 | 520 |
| 6 | 64-QAM | 3/4 | 58.5 | 65 | 121.5 | 135 | 263.3 | 292.5 | 526.5 | 585 |
| 7 | 64-QAM | 5/6 | 65 | 72.2 | 135 | 150 | 292.5 | 325 | 585 | 650 |
| 8 | 256-QAM | 3/4 | 78 | 86.7 | 162 | 180 | 351 | 390 | 702 | 780 |
| 9 | 256-QAM | 5/6 | N/A | N/A | 180 | 200 | 390 | 433.3 | 780 | 866.7 |

Note: A second stream doubles the theoretical data rate, a 3rd 3x, etc.

# 802.16 WiMax

- Broadband Wireless per fornire il Wireless Local Loop
- Simile a 802.11 ma pensati per risolvere problemi diversi
- 802.16 offre servizi a edifici a utenti non mobili, che quindi non migrano di cella in cella
- 802.16 copre distanze di km con grandi variazioni di potenze, rumore e problemi di sicurezza maggiori
- Ogni cella ha più utenti, quindi deve offrire maggior bandwidth, quindi poter operare a bande oltre fino a 66 GHz
- Queste sono onde millimetriche, sensibili all'acqua (pioggia, neve, nebbia) e che si diffondono in linea retta (802.11 omnidirezionale)

# 802.11 vs 802.16

- Entrambi per servizi wireless ad alta velocità
- Entrambi della famiglia 802
- 802.11 si occupa di reti privati di utenti con apparecchi potenzialmente mobili, transizione di celle e piccole distanze (circa 30m, max 100m, decine di utenti) e basse potenze (banda ISM, massima potenza 20bB, all'interno di proprietà private)
- 802.16 si occupa di reti pubbliche e grandi distanze (10-50km, centinaia di utenti)
- 802.16d in particolare verso antenne fisse (edifici che contengono molti computer) di qualità migliore dei notebook, magari direzionali, non gestisce le transizioni di celle
- 802.16e è la versione mobile, quindi sempre a grandi distanze ma deve gestire la transizione tra diverse base station

# 802.16 vs cellulari

- 802.11 rivolto agli utenti Ethernet mobili
- 802.16 rivolto a utenti residenti (per gestire l'ultimo miglio e ridurre il digital divide) e che vogliono tv wireless oltre i dati e la voce
- Con GSM si forniscono solo servizi voce a utenti molto mobili
- Con UMTS (o CDMA2000 negli SU) sono previsti servizi video ma non si prevedono le bande del 802.16
- Es 802.16 ha bande 2.5 volte superiori a HSDPA

# Convergenza futura?

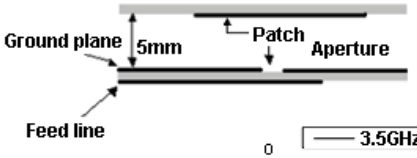
- I telefoni di 4ª generazione
  - Progettati per banda larga, bassa latenza, e completamente basate su IP anche per il traffico voce
  - Es i progetti 3GPP Long Term Evolution e Ultra Mobile Bradband
  - Dovrebbero avere una Air interface basate su OFDMA per downlink e OFDM per uplink , permettendo un internet più veloce di WiMax
  - Possibilità di convergenza con 802.16m

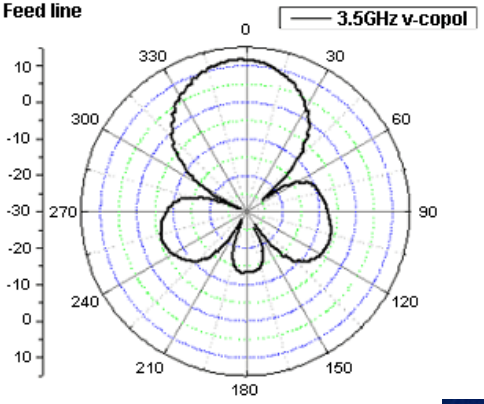
# Usi 802.16

- Connettività “last mile” a data rate elevati (altrimenti si deve usare wireless punto a punto, cavo o DSL)
- Connessione di Hot spot WiFi
- Connettività nomadica
- Accesso a Internet in caso di calamità (Tsunami in Indonesia, Uragano Katrina)
- Business Continuity (link di backup, in alternativa a provider fissi)

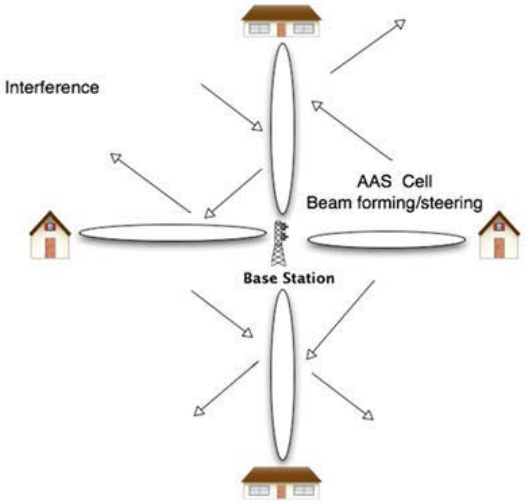
# Antenne

- A destra antenne 802.16d per utenti, fisse, molto direzionali
- Sotto antenne del provider
- In basso  a sx antenne per utenti 802.16e



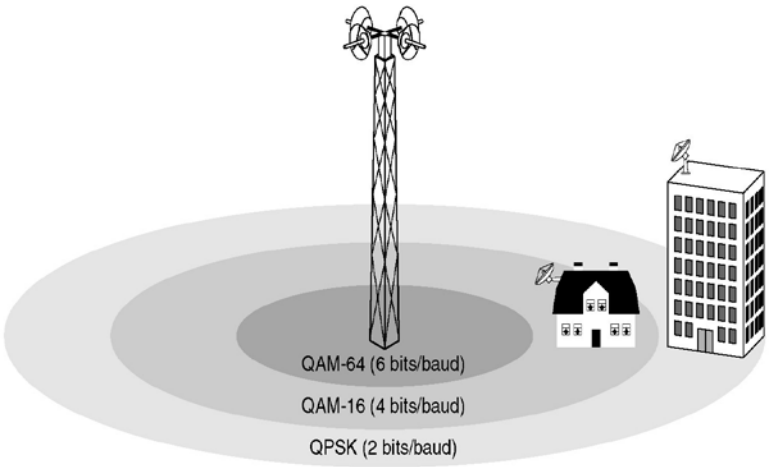



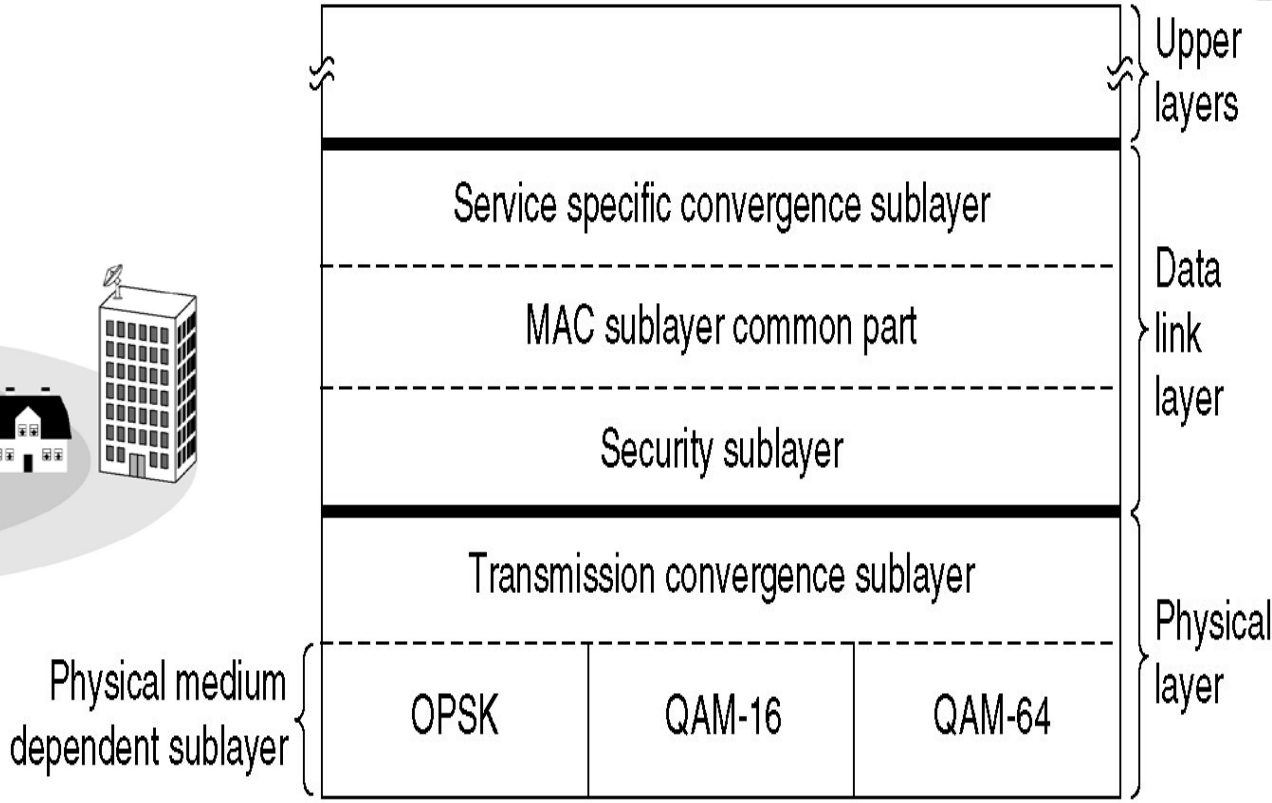

Antenna Gain = 14 dbi
F/R = 24.89 dB




# Stack 802.16

- QAM-64 offre 150 Mbps , QAM-16 100 Mbps e QPSK 50 Mbps su bande tipiche di 25 MHz



# Livello MAC

- WiFi:
  - tutte le stazioni che vogliono mandare frame sono in competizione per avere l'attenzione del Access Point in modo random
  - Le stazioni lontane sono spesso interrotte da stazioni vicine riducendo il throughput e soprattutto complicando la QOS per applicazioni Real Time
  - Gestisce male sovraccarichi
- WiMax:
  - Usa un algoritmo di scheduling. Una stazione deve compere una sola volta per entrare nella rete, poi gli viene allocato uno slot che può crescere o diminuire ma rimane sempre allocato alla stazione (insomma nessun altro lo può usare)
  - Questo permette stabilità in caso di sovraccarico o oversubscription e migliore sfruttamento della banda passante

# Livello Fisico

- Originariamente (2001) solo in linea di visibilità da 10 a 66 GHz
- 802.16a (2004) aggiunge range 2 – 11 GHz e senza necessibilità di linea di visibilità
  - 256 sottoportanti (di cui 200 usate) con Orthogonal FDM (OFDM)
- 802.16e (2005)
  - Usa SOFDMA (Scalable Orthogonal FD Multiple Access) e supporto ad antenne multiple MIMO
  - Canali da 1.25 a 20 MHz con fino a 2048 sottoportanti
  - Permette Mobilità completa
- Il maggior interesse commerciale è in  frequenze basse
  - (2.3, 2.5 e 3.5 GHz) che offrono range maggiori e possono penetrare gli edifici ma anche 5 GHz nella banda libera
  - Possibilità di avere terminali dual standard (WiFi +  WiMax) o (Cellulare + WiMax)

# Sviluppi

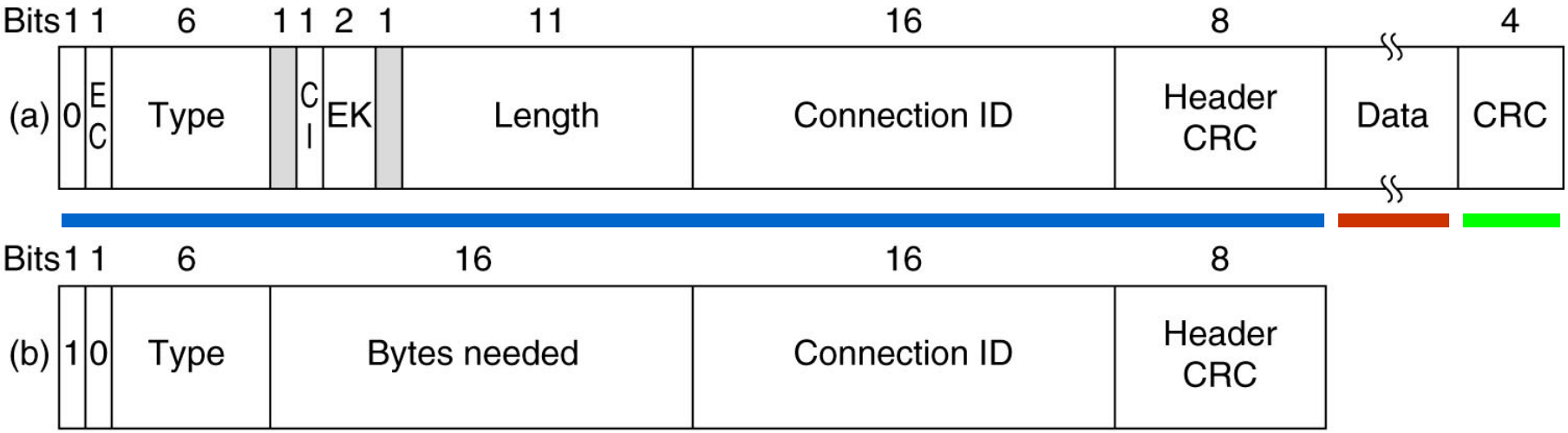
- In fase di sviluppo:
  - 802.16j Multihop relay (architetture mesh)
- In fase di pre-draft
  - 802.16m Advanced air interface: Fino a 100 Mbps mobile e fino a 1 Gbps fisso, cellulare, micro e macro celle, senza restrizioni alle bande di RF (sopra i 20 MHz)

# Limitazioni

- WiMax non offre 70 Mbps a 50 Km.
  - Si arriva a 50km ma con bit error rate elevati per cui si deve andare a data rate bassi A basse distanze invece si possono avere range più alti
  - Impianti fissi hanno antenne direzionali con buoni range e throughput
  - Impianti mobili hanno antenne omnidirezionali con minor guadagno ma più portabili (in pratica al massimo 10 Mbps su 2 km se l'antenna è in linea di visibilità)
  - Le prestazioni calano se ci sono molti utenti attivi che condividono una certa banda radio (es 2, 4, 6, 8, 10 o 12 Mbps)

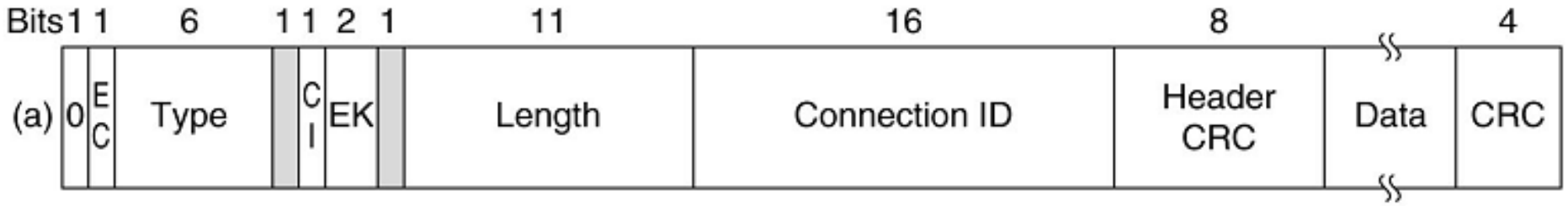
# Frame 802.16

- Frame 802.16
  - cominciano con un header generico di 6 Byte
  - seguito da un payload opzionale (a); non serve nei frame di controllo (b)
  - 1 Byte checksum CRC (opzionale, non serve se viene fatto error correction a livello fisico)



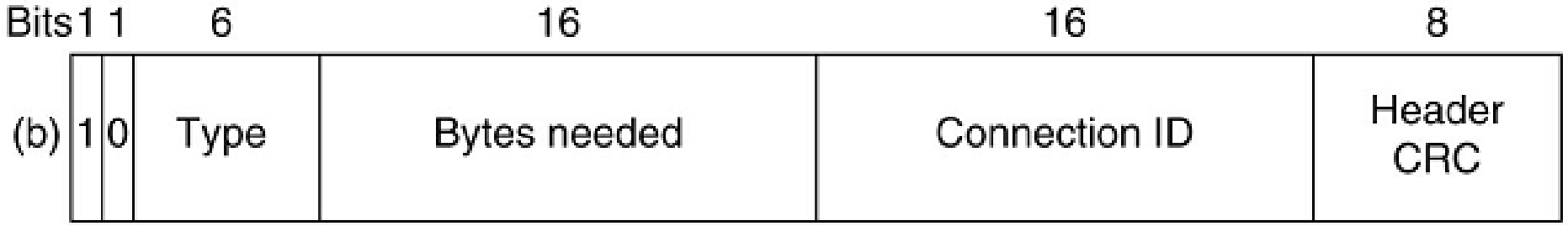
# Frame 802.16

- **Primo bit a 0**
- Il campo **EC** dice se il payload è encrypted
- **Type** identifica il tipo di frame (fragmentation etc)
- **CI** indica presenza o meno di Checksum
- **EK** fornisce la lunghezza del frame compreso l'header
- **Connection ID** indica a quale connessione appartengono i frame
- **CRC** dell'header
- Poi i dati



# Bandwidth request

- Il secondo tipo di frame per richiesta di banda
- Comincia con un **bit 1** invece che **bit 0**
- è simile al precedente a parte il **secondo** e **terzo** byte che formano un numero a 16 bit per indicare la banda richiesta per trasportare un certo numero di byte (**Byte needed**)



# Sperimentazioni recenti

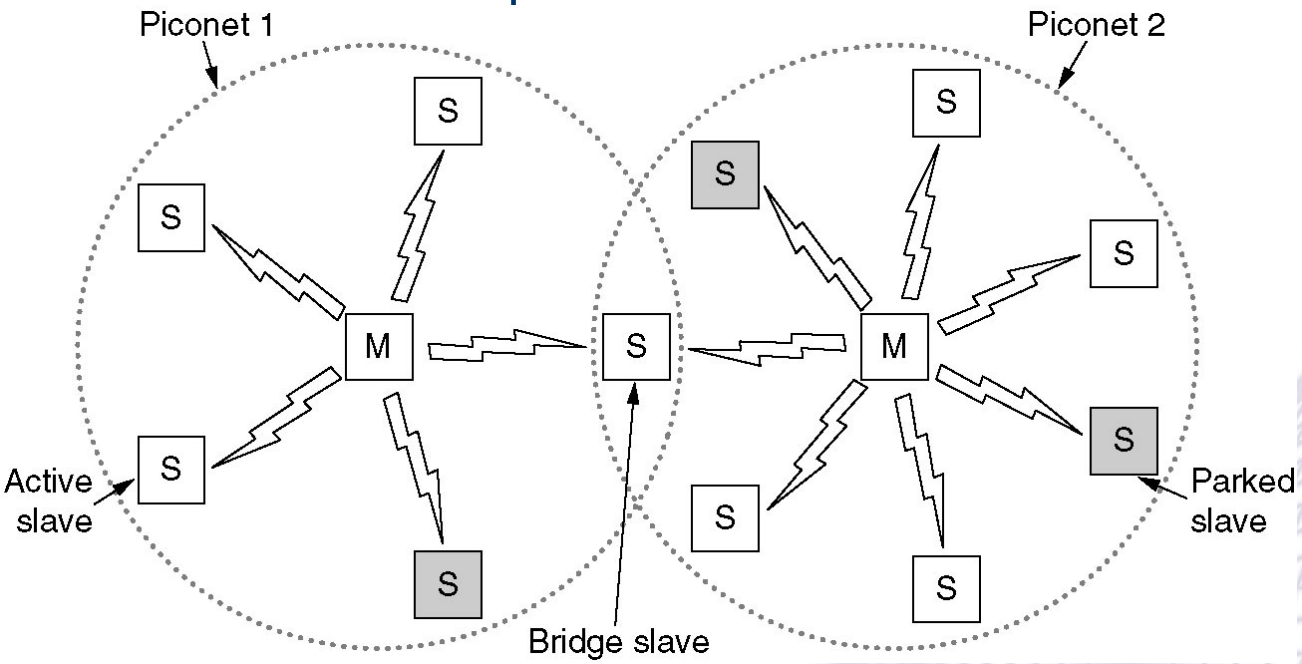
- IEEE 802.16d-2004 permette accesso a 74 Mbps fino a 54 km dall'hot spot su frequenze tra 3.4 e 3.6 GHz
- In ITALIA
  - Sperimentazioni partite a Luglio 2005 con IEEE 802.16d che permette accesso a 74 Mbps fino a 54 km dall'hot spot su frequenze tra 3.4 e 3.6 GHz
  - Ritardo dovuto alle bande usate dai militari
  - Bando per l'asta delle licenze a Ottobre 2007, con concessioni decennali a livello provinciale o regionale
  - Bandite solo due bande di 35 MHz invece dei 200 Mhz previsti
- In altri paesi europei ci sono già offerte commerciali (in Francia ci sono 44 licenze WiMax da almeno un paio di anni)

# 802.16e

- WiMax mobile che funziona con veicoli fino a 140 km/h
- In Corea esiste uno standard simile al WiMax mobile che si chiama WiBro sperimentato da Samsung alle Olimpiadi di Torino 2006
- Questo standard non funziona molto bene sulle frequenze di WiMax sopra i 3 GHz. Sarebbe meglio poter usare frequenze televisive liberate con il passaggio alla tv digitale.

# Bluetooth 802.15

- Base: **Piconet**, nodo master e fino a 7 slave entro 10 metri (e fino a 255 “parked nodes”
- Diverse Piconet nella stessa stanza si connettono con un bridge e formano una **scatternet**
- Il master ha l’intelligenza e gestisce in TDM gli slaves che sono molto stupidi (il chip deve costare meno di 5 Euro)
- Comunicazione slave-slave impossibile



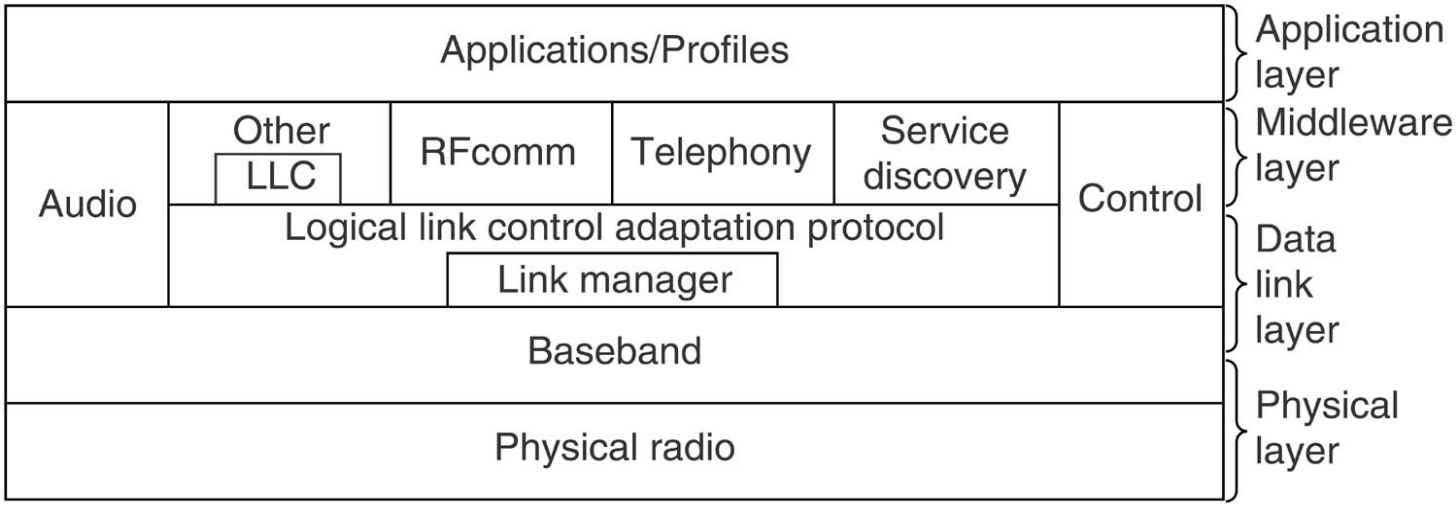
# Applicazioni Bluetooth

- 802.11 non dice come usare il wireless (leggere e-mail o navigare sul web)
- 802.15 invece specifica le applicazioni dette anche profili

| Name | Description |
|---|---|
| Generic access | Procedures for link management |
| Service discovery | Protocol for discovering offered services |
| Serial port | Replacement for a serial port cable |
| Generic object exchange | Defines client-server relationship for object movement |
| LAN access | Protocol between a mobile computer and a fixed LAN |
| Dial-up networking | Allows a notebook computer to call via a mobile phone |
| Fax | Allows a mobile fax machine to talk to a mobile phone |
| Cordless telephony | Connects a handset and its local base station |
| Intercom | Digital walkie-talkie |
| Headset | Intended for hands-free voice communication |
| Object push | Provides a way to exchange simple objects |
| File transfer | Provides a more general file transfer facility |
| Synchronization | Permits a PDA to synchronize with another computer |

# Stack Bluetooth

- Livello applicazioni/profili
- Livello middleware con mix di protocolli, tra cui 802LLC per compatibilità con altre reti 802
- Il link manager gestisce i canali logici tra i devices (power, autenticazione, Qos) e il LLC Adaptation Protocol (**L2CAP**) che scherma i layer superiori dai dettagli della tramissione (è un po' come 802 LLC sublayer)
- Baseband è equivalente al livello MAC
- Infine sotto il livello fisico come nei modelli OSI e 802, gestisce trasmissione radio e modulazione



# Bluetooth Radio Layer

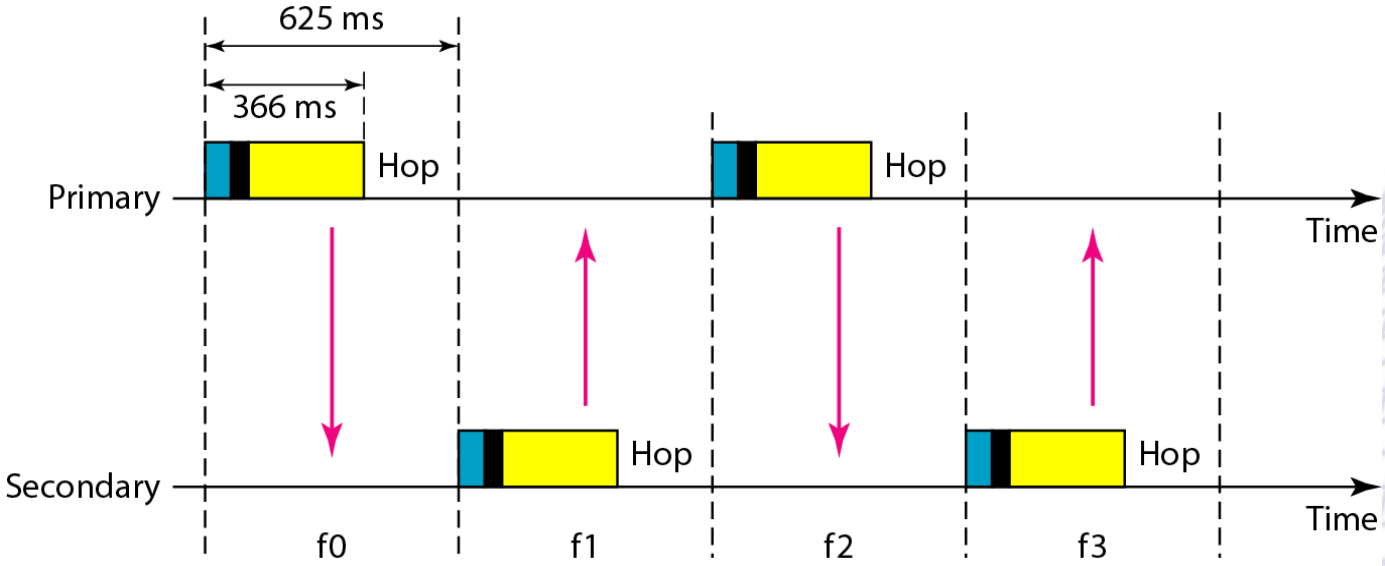
- Sistema a bassa potenza con range di 10 metri nella banda ISM a 2.4 GHz
- La banda si divide in 79 canali da 1 MHz con circa 1bit/Hz → 1 Mbps in gran parte usato per overhead
- Usa Frequency Hopping con 1600 hops/sec e 625 µsec di dwell time
- Bluetooth è nella stessa frequenza di 802.11 e di solito il primo disturba il secondo

# Bluetooth Baseband Layer

- Simile al MAC Sublayer
  - Converte i bit in frames
  - Nella forma più semplice il master di ogni piconet definisce una serie di time slots di 625 μs
  - Il master trasmette negli slot pari e gli slaves in quelli dispari
  - I frames possono essere lunghi 1, 3 o 5 slot
  - Il timing del frequency hopping permette di avere 250 μs per slot per permettere ai circuiti radio di stabilizzarsi.

# Payload

- Frame single slot
  - Dopo la stabilizzazione restano 366 bit su 625
  - di questi: 126 sono per un codice di accesso nell'header per cui rimangono solo 240 bit per i dati
  - Se ho 5 slot insieme ho un'unica stabilizzazione quindi ho 5*625 bit in 5 slot di cui 2781 buoni per i dati
  - Ogni frame viene trasmesso su un canale logico detto link di cui ne esistono due tipi: ACL E SCO



# ACL

- ACL: Asyncronous Connection-less link per dati packet switched  disponibili a intervalli irregolari
- Questi dati arrivano dal L2CAP layer e vengono mandati “best-effort” al L2CAP layer del ricevente.
- Essendo best-effort non c’è garanzia di consegna, se i frame vengono persi vanno ritrasmessi
- Ogni slave può avere un solo link ACL verso il suo master

# SCO

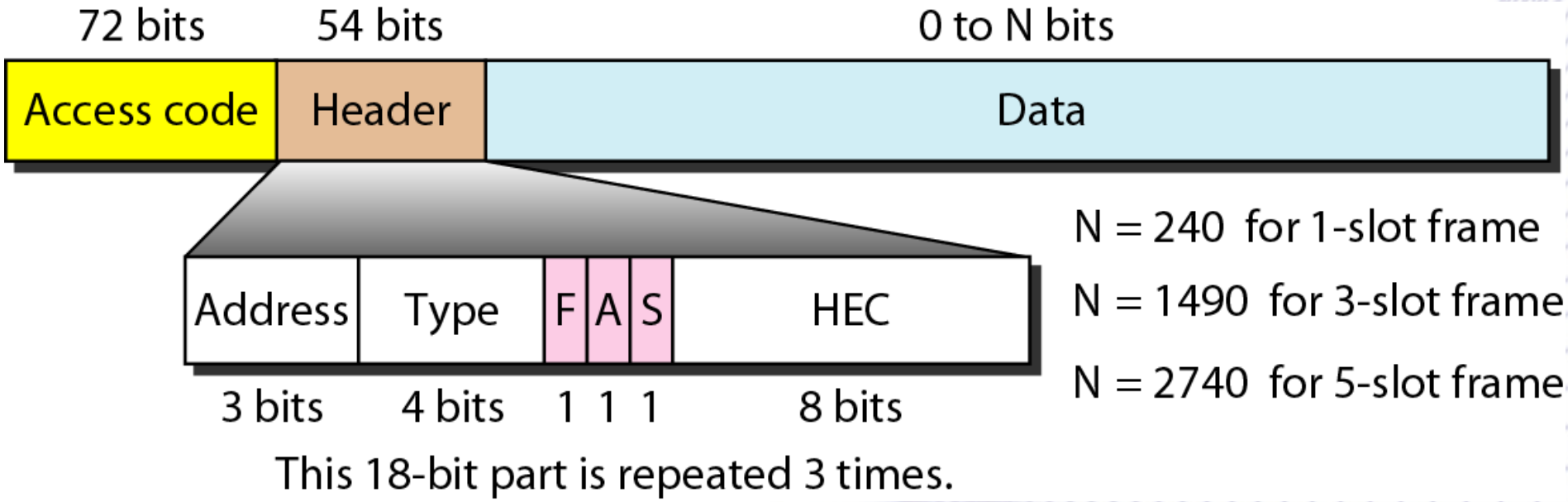
- SCO: Syncronous Connction Oriented link per trasmissioni real time come per esempio le comunicazioni telefoniche
- Viene allocato un singolo slot in ogni direzione
- Frame persi non vengono ritrasmessi per esigenze di real time ma si può usare Forward Error Correction
- Uno slave può avere fino a 3 link SCO con il suo master
- Ogni SCO link può trasmettere  un canale PCM a 64 kbps.

# Blutooth L2CAP layer

- Ha 3 funzioni principali
  - Accetta pacchetti fino a 64 KB dai layer superiori e li rompe in frame per la trasmissione
  - Gestisce multiplexing e demultiplexing da diverse sorgenti di pacchetti. Quando un pacchetto viene riassemblato L2CAP decide a quale protocollo di livello superiore deve consegnarlo
  - Gestisce la richieste di QoS sia quando vengono stabiliti i links che nelle normali operazioni. Vengono anche contrattati il massimo payload size, perché non tutti i dispositivi sanno gestire i pacchetti massimi di 64 KB

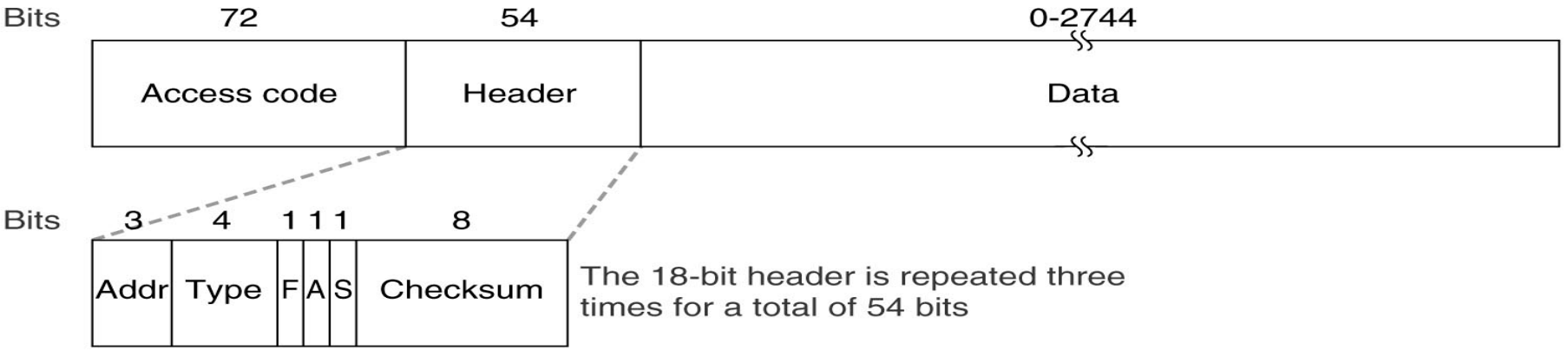
# Bluetooth frame

- Ci sono diversi tipi di frame ma il più importante è quello in figura
- C'è un codice di accesso che identifica il master (se uno slave è nel range di due master)
- Un header a 54 bit con i tipici campi di un sublayer MAC
- Poi 2744 bit per una trasmissione cn frames da 5 slot ( 240 per uno slot, 1490 per slot a 3 frames)



# Bluetooth header

- Address indica quale degli 8 dispositivi attivi deve ricevere il frame
- Type identifica il tipo di frame e il tipo di error correction
- Flow bit viene alzato dallo slave quando ha il buffer pieno
- ACK bit usato per mandare indietro un ACK in un frame di dati in direzione opposta (piggybacking)
- Sequence bit per numerare i frame per rivelare ritrasmissioni (stop and wait, quindi ne basta uno)
- Poi c'è un checksum a 8 bit
- Il tutto viene ripetuto 3 volte per fare 54 bit (stiamo usando elettronica economica e a bassa potenza 2.5 mW)



# Bluetooth data field

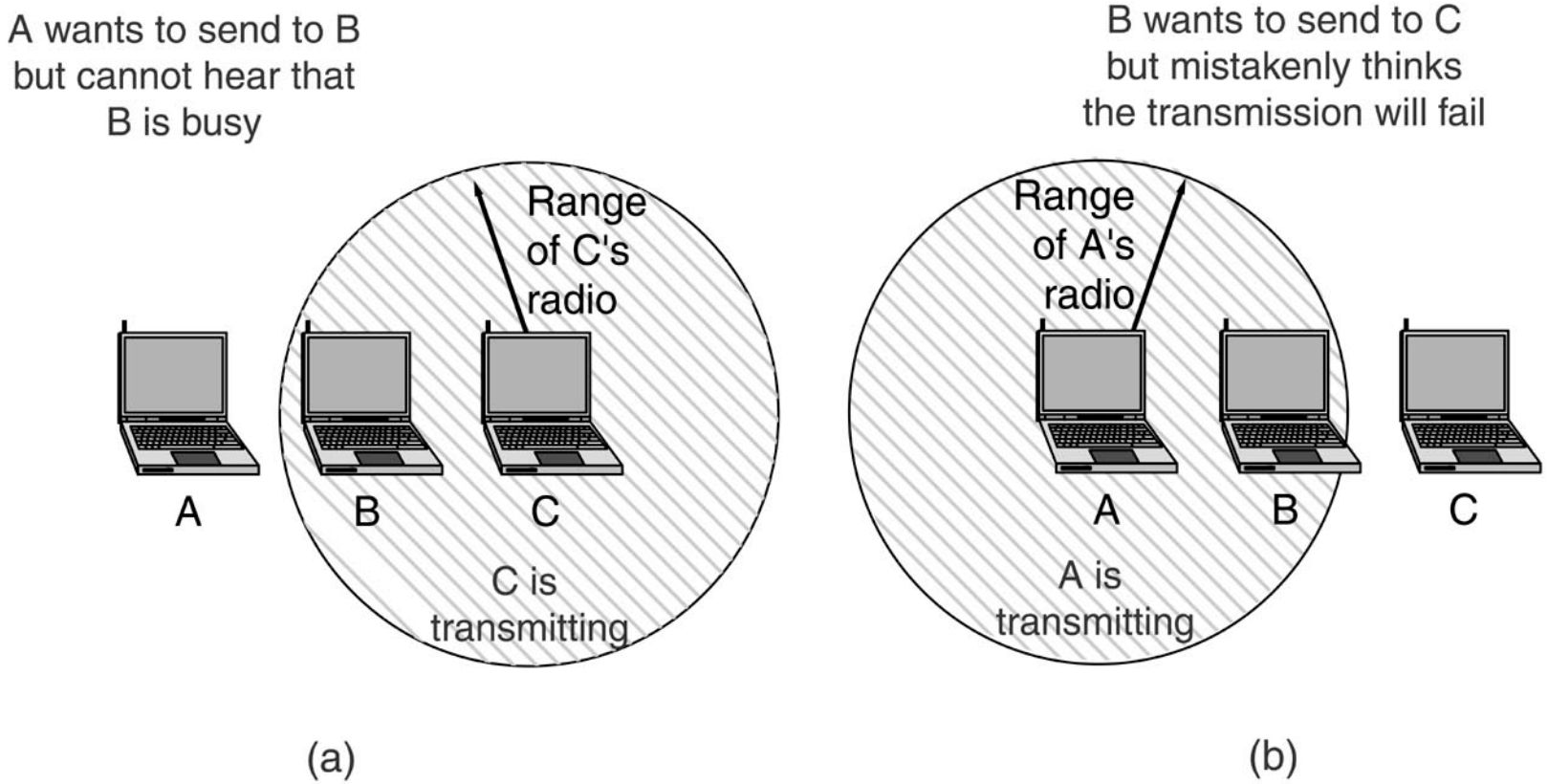
- Uno slave può usare solo i campi dispari, quindi al massimo 800 slot/sec (lo stesso il master sui pari)
- Se ho un payload di 80 bit allora ho 64000 bps come un canale voce PCM
- In pratica un canale voce full duplex di 64kbps in ogni direzione satura un canale a 1 Mbps
- Per varianti meno affidabili 240 bit/slot senza ridondanza posso avere 3 canali alla volta, da cui il limite di 3 SCO link

# 802.11 MAC sublayer


- Torniamo al livello MAC: In Ethernet se trasmetto un pacchetto e non mi arriva un noise burst dovuto ad una collisione nei primi 64bytes posso stare tranquillo, infatti tutti sentono tutto
- In 802.11 c'è il problema del range radio

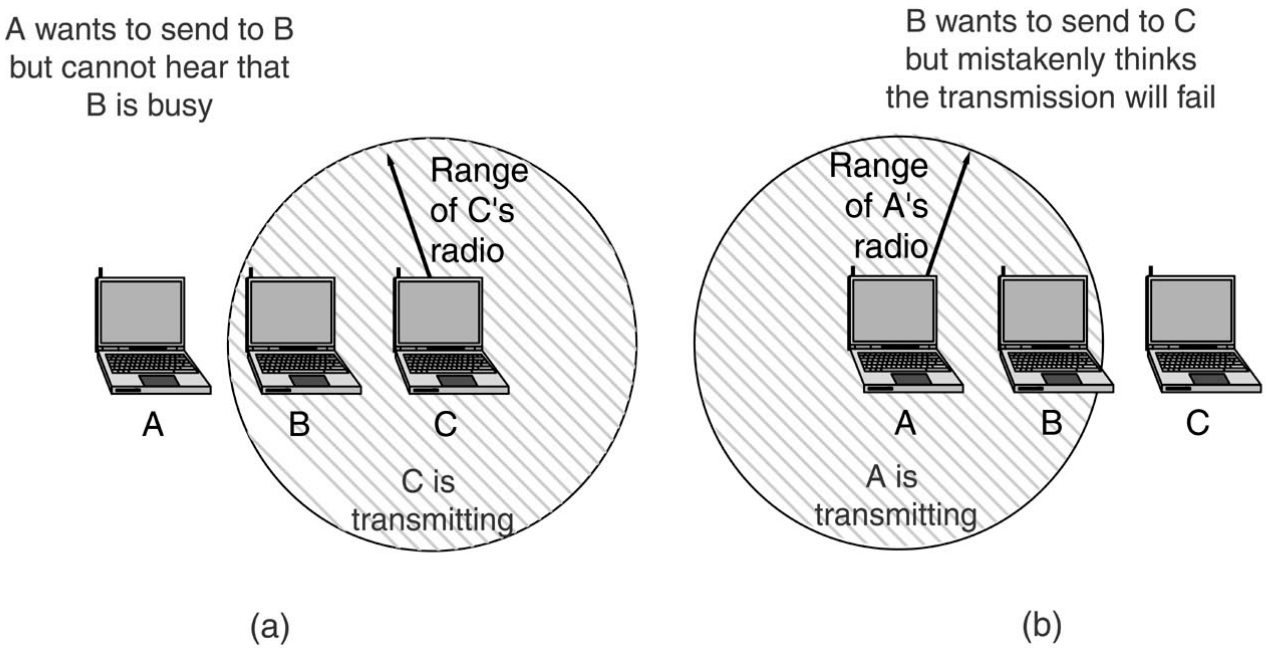
# 802.11 MAC

- Il livello MAC di 802.11 è diverso da quello Ethernet per i problemi della stazione nascosta e della stazione esposta



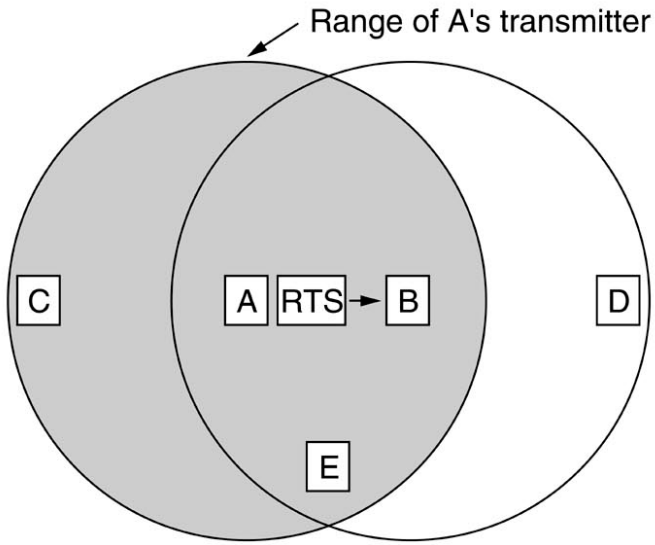
# 802.11 MAC

- Dal momento che non tutte le stazioni si sentono tra di loro
  - (a) C trasmette a B, A non se ne accorge via sensing e quindi erroneamente pensa di poter trasmettere a B
  - (b) A trasmette a B. B erroneamente pensa di non poter trasmettere a C, pensando che la trasmissione potrebbe essere disturbata da A (che magari sta parlando con D)

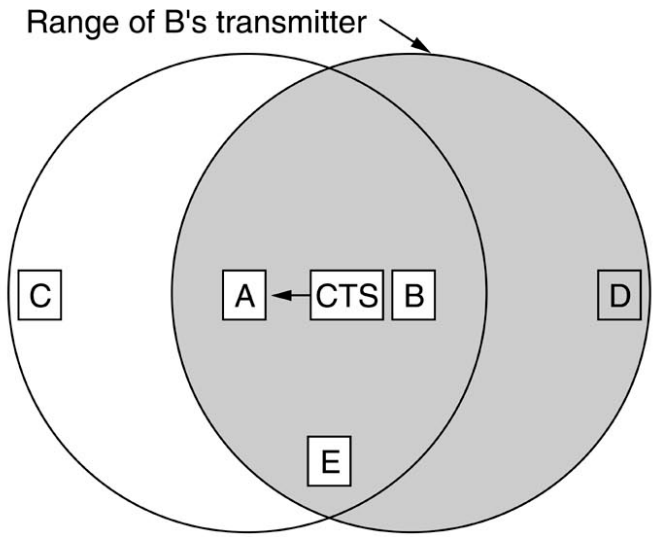


# MACA e MACAW

- MACA: protocollo in cui A manda un piccolo RTS di 30 byte con la lunghezza del vero frame che si vuole trasmettere, B risponde con un CTS di nuovo con la lunghezza in seguito al quale A trasmette
- Chi sente RTS o CTS sa che deve stare zitto per un periodo noto (dalla lunghezza dichiarata)
- MACAW: un MACA ottimizzato per Wireless




(a)

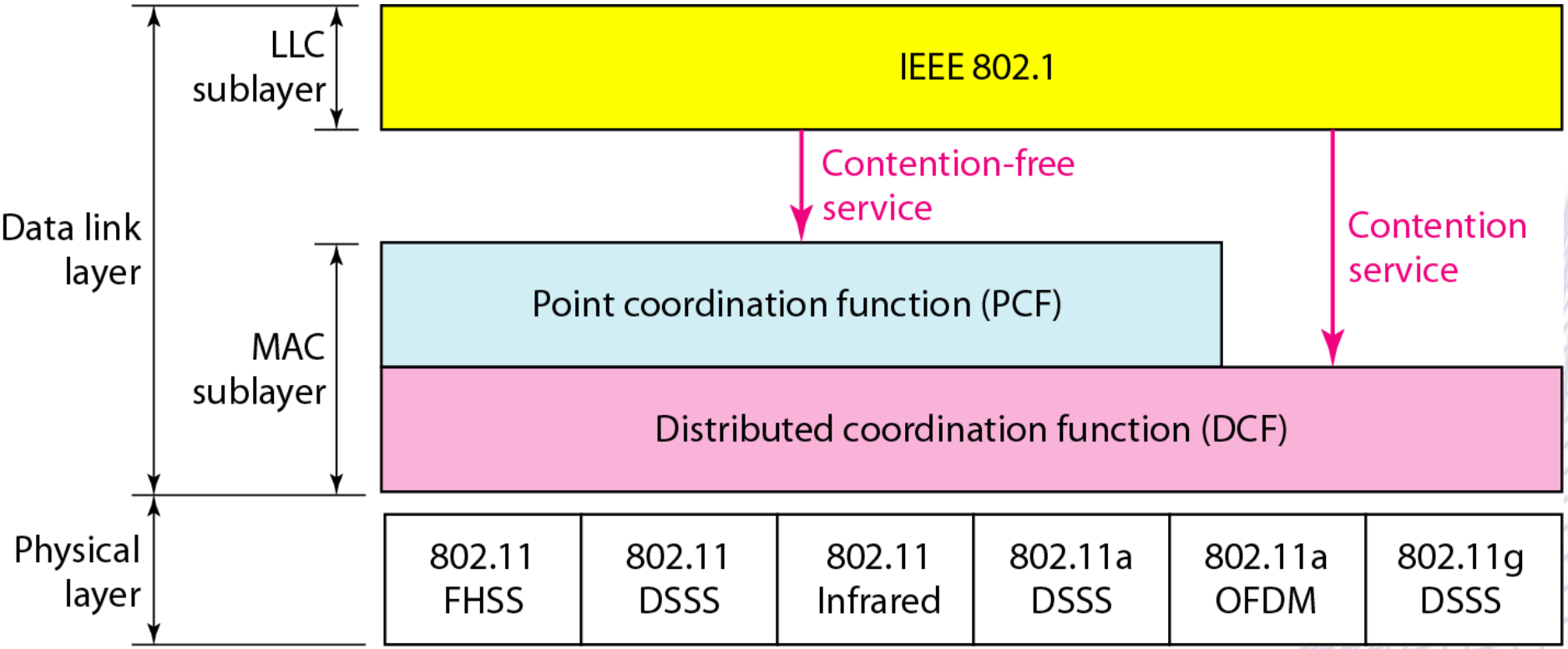



(b)

# DCF e PCF

- 802.11 quindi non usa CMSA/CD per superare i problemi a) e b) ma invece supporta due modi di operazione:
- DCF: Distributed Coordination Function, non usa alcuno tipo di controllo centrale, quindi in questo senso è simile a Ethernet
- PCF: Point Coordination Function usa una stazione base per controllare tutta l'attività nella cella
- Tutte le implementazioni devono supportare DCF mentre PCF è opzionale

# Stack 802.11

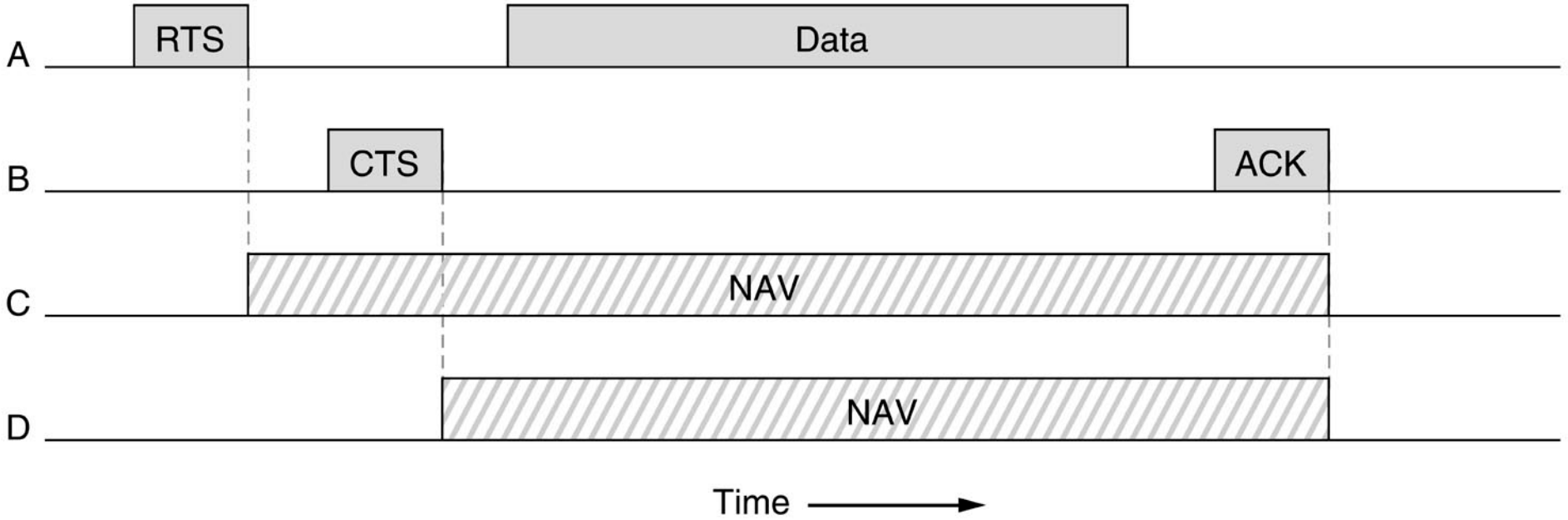

LLC sublayer
IEEE 802.1
Contention-free service
Contention service
Data link layer
MAC sublayer
Point coordination function (PCF)
Distributed coordination function (DCF)
Physical layer
802.11 FHSS
802.11 DSSS
802.11 Infrared
802.11a DSSS
802.11a OFDM
802.11g DSSS

# DCF

- Con DCF si usa un protocollo CSMA/CA (Collision Avoidance) con due metodi di operazione
  - Quando una stazione vuole trasmettere ascolta il canale
  - Se è idle trasmette, mentre trasmette non ascolta il canale ma emette il frame completo che potrebbe anche andare distrutto per interferenza con altri
  - Se invece sente traffico, rinvia la trasmissione fino a quando non torna idle
  - Se c'è una collisione, aspetta un tempo random usando l'algoritmo di backoff esponenziale di Ethernet

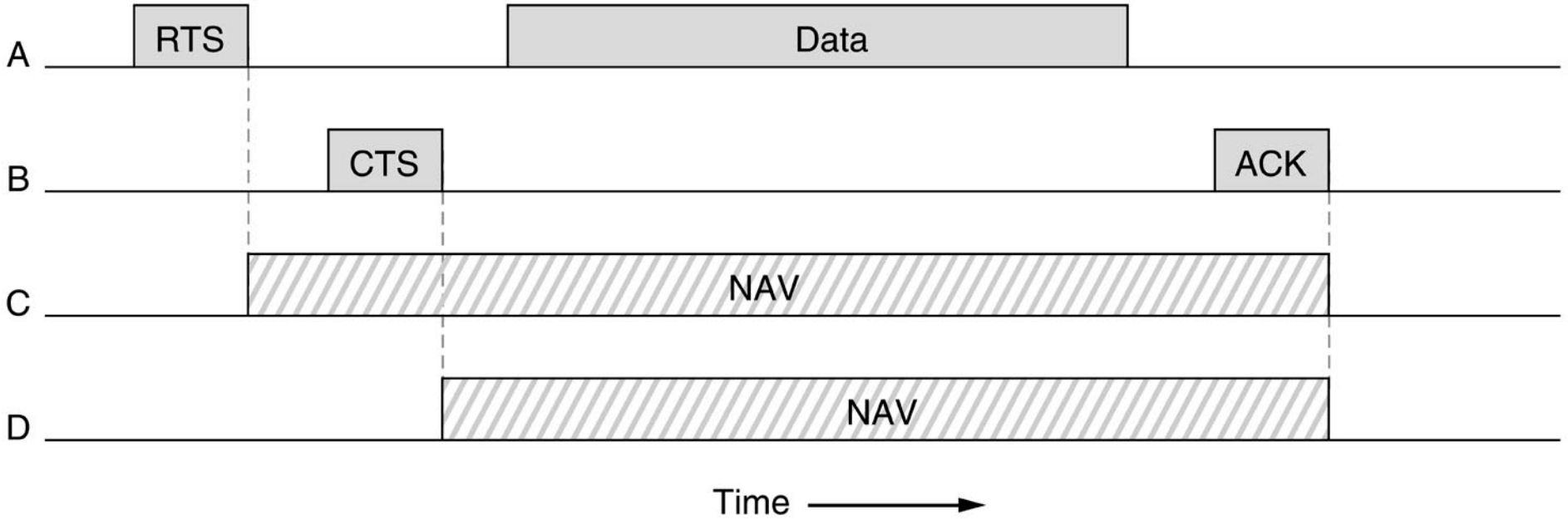
# DCF secondo metodo

- Il secondo metodo usa un MACAW con virtual channel sensing
- Es A vuole trasmettere a B, C è nel range di A (o anche di B ma non ci interessa) e D nel range di B ma non di A
- A manda un RTS a B che risponde con un CTS se vuole accettare il frame. Dopo di che A manda i dati e aspetta un ACK che B manderà. Se ACK arriva dopo un timeout di A il protocollo si ripete



# DCF secondo metodo

- Dal punto di vista di C: C è nel range di A quindi vede il RTS, stima la lunghezza richieste e mette sul suo canale virtuale un NAV (Network Allocation Vector) dichiarando il canale busy per se stesso, ma in realtà nulla viene trasmesso sul canale fisico, è come un promemoria per C
- La stessa cosa fa D quando sente il CTS di B

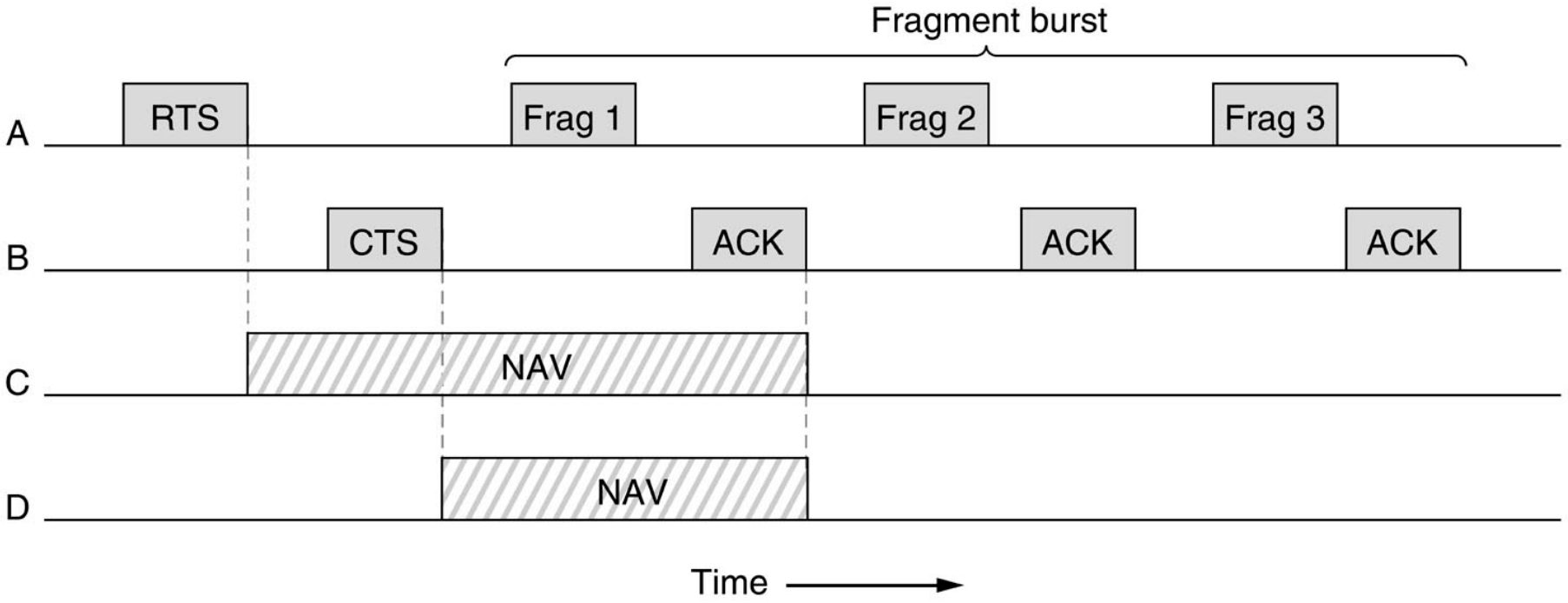


# Errori su canali noisy

- Al contrario delle reti wired, le reti wireless sono soggette a rumore e inaffidabili (altri apparati ISM, forni a microonde)
  - La probabilità che un frame riesca a passare diminuisce con la sua lunghezza
  - Se la probabilità che venga colpito un bit è **p**, la probabilità che un frame di **n** bit riesca a passare senza errori è $\mathbf{(1-p)^n}$
  - Se $\mathbf{p=10^{-4}}$ la probabilità di ricevere un frame Ethernet di 12144 bit senza errori è meno di 30%
  - Se $\mathbf{p=10^{-5}}$ un frame su 9 (oltre 10%) viene danneggiato
  - Se $\mathbf{p=10^{-6}}$ oltre 1% dei frame viene danneggiato, almeno 12 al secondo

# Fragment burst

- Per questo motivo in wireless i frame vengono frammentati in piccoli pezzi, ognuno con il suo checksum, ed ogni frammento deve ricevere il suo ACK prima che il frammento successivo possa essere trasmesso
- La frammentazione aumenta il throughput riducendo le ritrasmissioni ai frammenti cattivi e non a tutto il frame
- La lunghezza del frammento viene negoziata tra le stazioni



# PCF

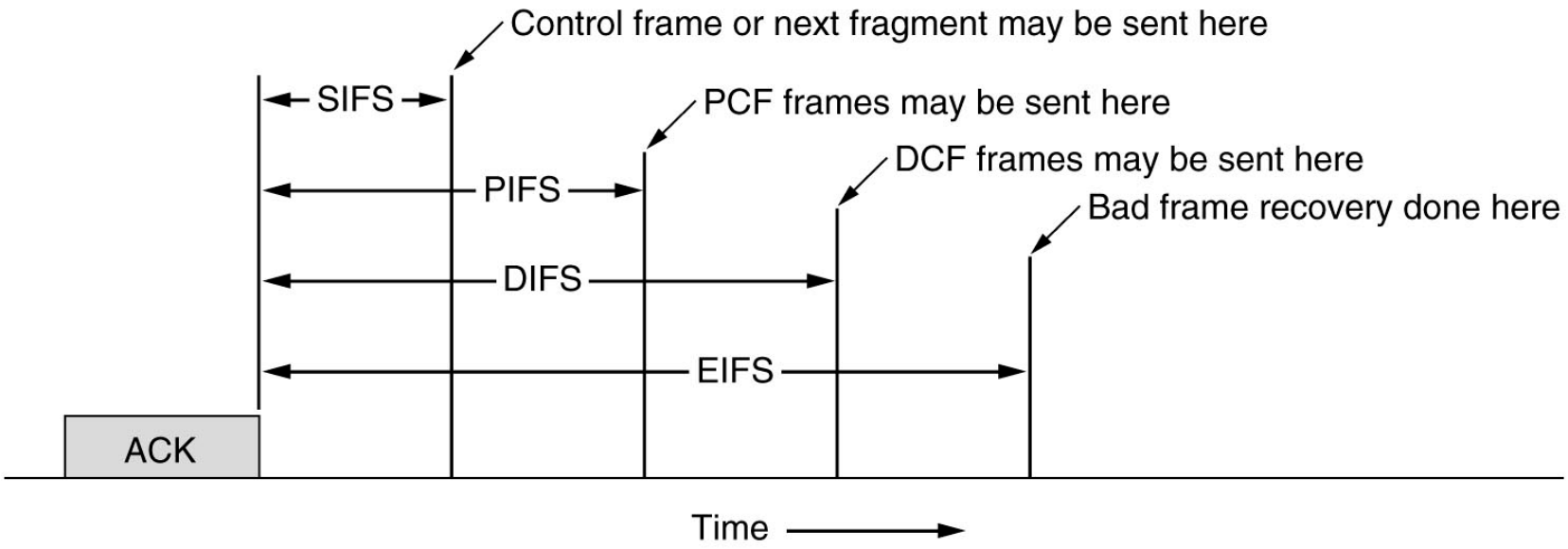
- Point Coordination Function: una stazione contatta periodicamente le altre chiedendo se devono trasmettere qualcosa.
- Questo permette di rimuovere le collisioni
- Lo standard non specifica la frequenza di polling o l'ordine di polling o se tutte le stazioni devono avere la stessa priorità
- Viene mandato in broadcast a tutte un **beacon frame** (da 10 a 100 volte al secondo), questo contiene parametri del sistema come la hopping sequence e dwell time (per FHSS), clock synchronization etc..
- Il beacon frame contiene anche l'invito a prenotare il servizio di polling

# PCF

- Quando una stazione si prenota ad un certo rate, le viene garantita una certa frazione della banda e quindi  si possono offrire servizi con QoS
- Problemi di consumo della batteria sono sempre sentiti in ambito wireless. La stazione base può dire ad una stazione di mettersi in sleep fino a quando non viene svegliato dalla stazione o dall'utente
- Tuttavia se mette una stazione in sleep, la stazione base deve bufferizzare qualsiasi frame diretto alla stazione in sleep

# PCF

- PCF e DCF possono coesistere in una cella. Questo è possibile definendo attentatamente l'intervallo interframe
- Quando un frame è stato spedito, deve passare un certo tempo morto prima che un'altra stazione possa trasmettere. Ci sono quattro diversi tipi di intervallo



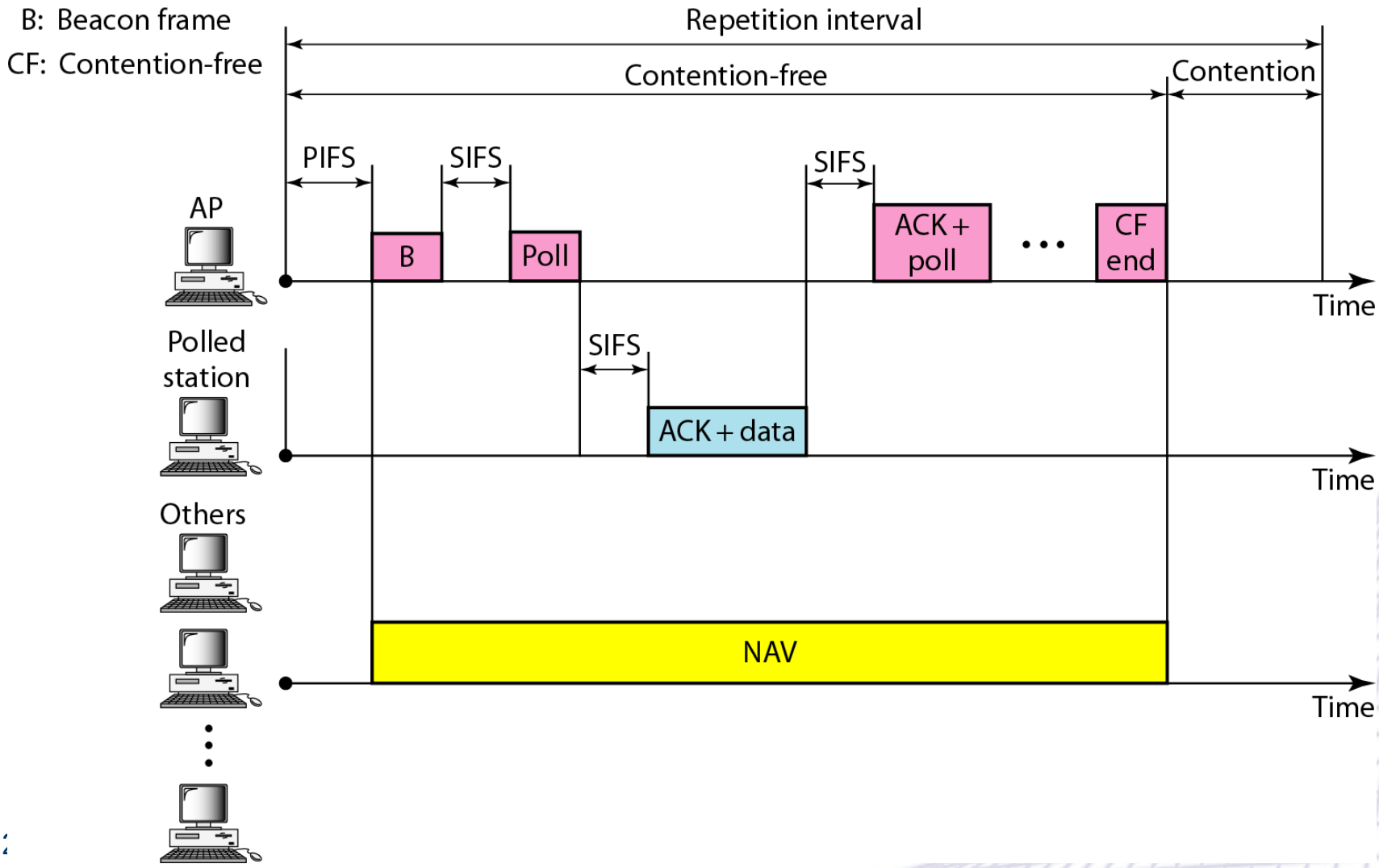
# intervalli

- SIFS: Shortest InterFrame Spacing
  - Permette a due stazioni in un singolo dialogo di avere la possibilità di partire per prime. Es CTS in risposta a RTS o ACK di un frame o di un frammento
- PIFS
  - Solo una stazione ha il diritto di rispondere in un SIFS, se se lo lascia scappare e passa un tempo PIFS (PCF Interframe Spacing) la stazione base può mandare un **poll frame** o un **beacon frame**.
  - In questo modo la stazione base ha la priorità ma non si mette in competizione all'interno di un dialogo esistente

# intervalli

- DIFS: DCF InterFrame Spacing
  - Se la stazione base non ha nulla da dire e passa un tempo DIFS, qualunque stazione può provare ad acquisire il canale per mandare un nuovo frame.
  - Solite regole di **contention** e **binary exponential backoff** in caso di collisione
- EIFS: Extended  InterFrame Spacing
  - Usabile solo da una stazione che ha appena ricevuto un frame rovinato. Questo evento ha la priorità più bassa dal momento che il ricevitore potrebbe non capire quello che sta succedendo è meglio che aspetti un po' prima di interferire in dialogo

# Intervallo di ripetizione

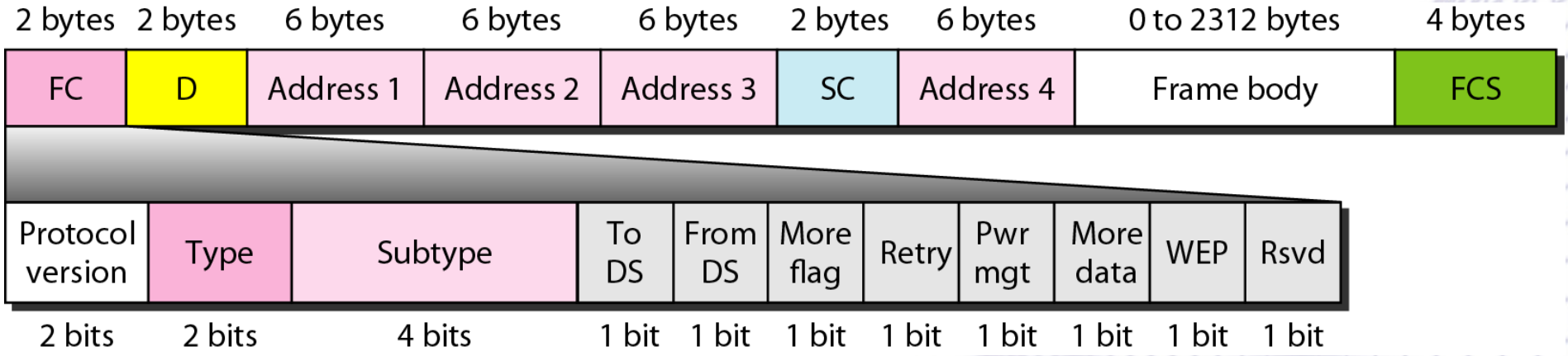


# Frame 802.11

- Tre tipi di frame
  - **Data**, **Control**, **Management**, ognuno con i suoi header con varietà di campi da usare nel sottolivello MAC
  - Inoltre ci sono alcuni header usati dal livello fisico che hanno a che fare con le tecniche di modulazione

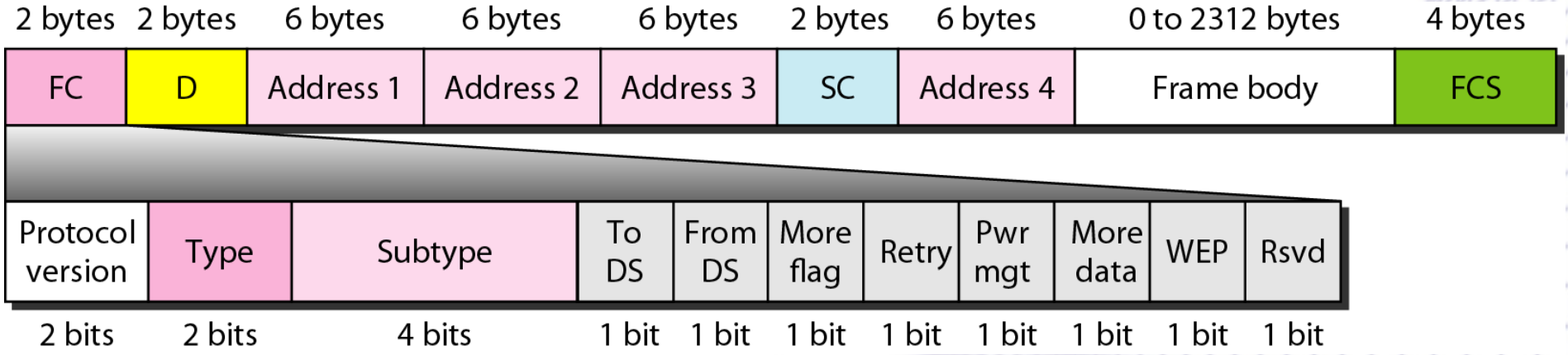
# Data Frame

- Frame Control Field ha 11 sottofield
  - **Protocol Version**: permette a due versione del protocollo di operare allo stesso momento nella stessa cella
  - **Type** (data, control, management)
  - **Subtype** (es. RTS, CTS)
  - **To DS**, **FromDS** per dire se il frame sta andando o venendo dall'intercell distribution system (es. Ethernet)



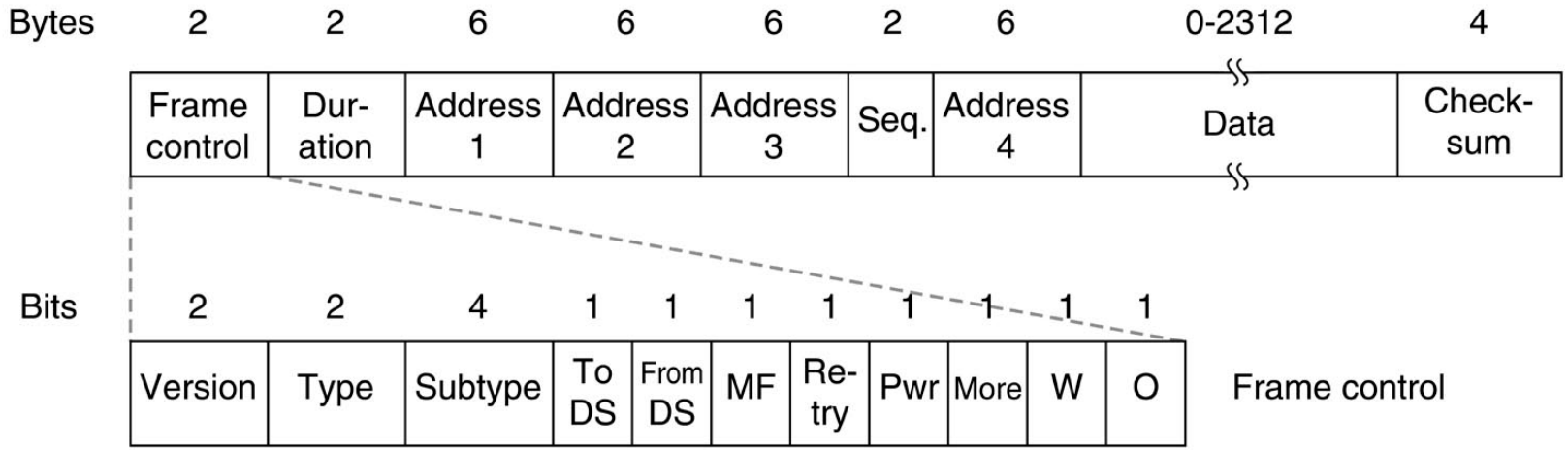
# Data Frame

- **MoreFlag** significa che altri frammenti sono in arrivo
- **Retry** bit significa che è una ritrasmissione di un frame già trasmesso prima
- **Power Management** serve alla stazione base per mettere una stazione in sleep o per svegliarla dallo stato di sleep
- **More data** significa che il mittente ha altri frame per il ricevente
- **WEP** indica che il body del frame è stato criptato WEP
- **O** indica al ricevente che una sequenza di bit con questo bit vanno processati strettamente in sequenza



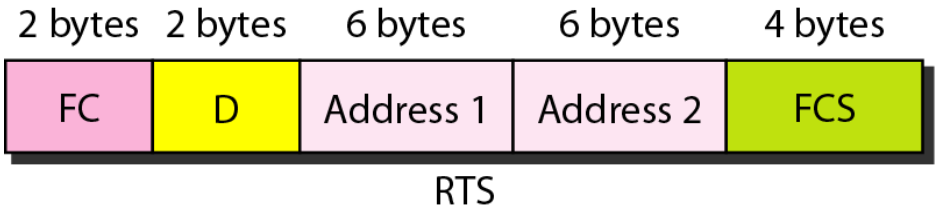
# Data Frame

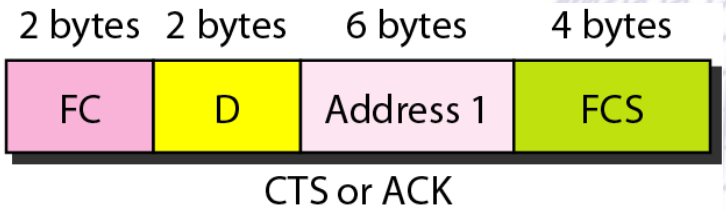
- **Duration** quanto a lungo il frame (e il suo ACK) occuperanno il canale. Questo campo è presente anche nei control frame ed è quello usato dalle altre stazioni di gestire il meccanismo NAV
- **Address** ci sono quattro indirizzi, tutti in formato IEEE 802. Ovviamente servono **Source** e **Destination**. A cosa servono gli altri? I frame entrano ed escono dalla cella attraverso una base station. Gli altri due sono usati come **source** e **destination** della base station
- **Sequence** permette di numerare i frammenti. Dei 16 bit, 12 identificano il frame e 4 identificano il frammento
- **Data** è il payload lungo fino a 2312 byte
- **Checksum**



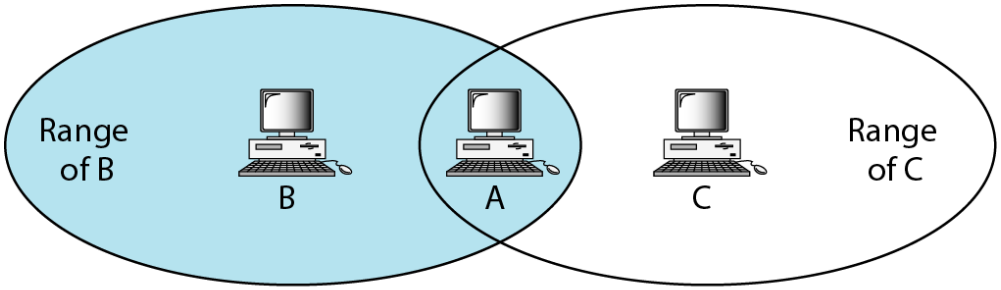
# Management e control frame

- **Management** Frame
  - Hanno un formato simile ai data frame ma non ha uno degli indirizzi delle base station, perché i management frame sono limitati ad una sola cella
- **Control** frame
  - Sono ancora più corti con solo uno o due indirizzi, nessun campo **Data**, e neppure campo **Sequence**.
  - Le informazioni chiave qui sono nel campo **Subtype** (di solito RTS, CTS, ACK)

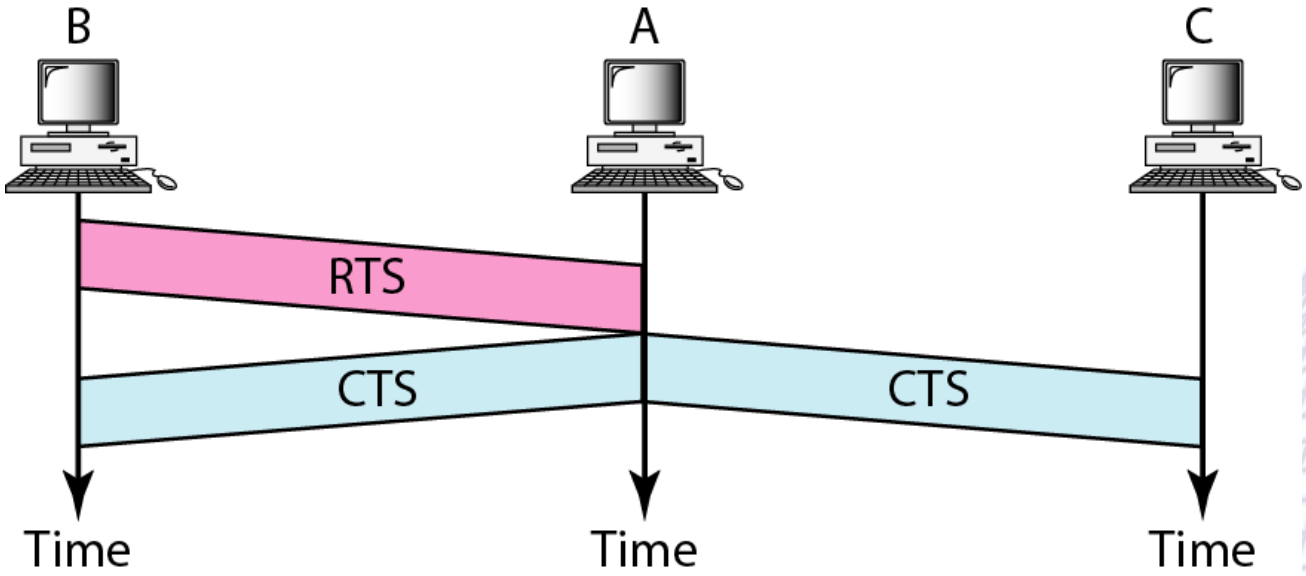


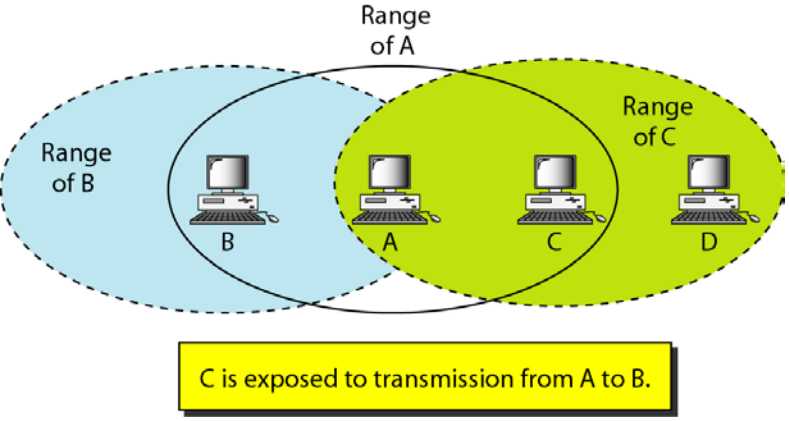
# Hidden station e RTS

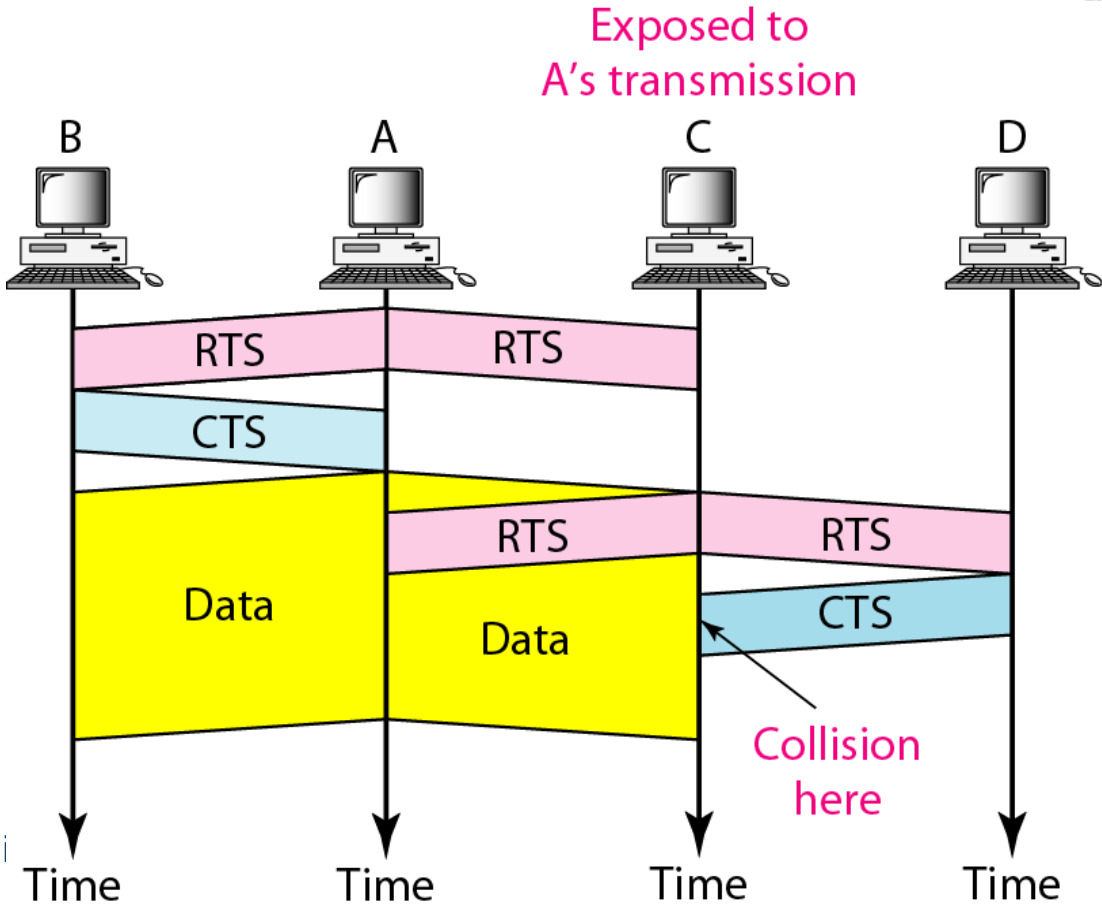



B and C are hidden from each other with respect to A.

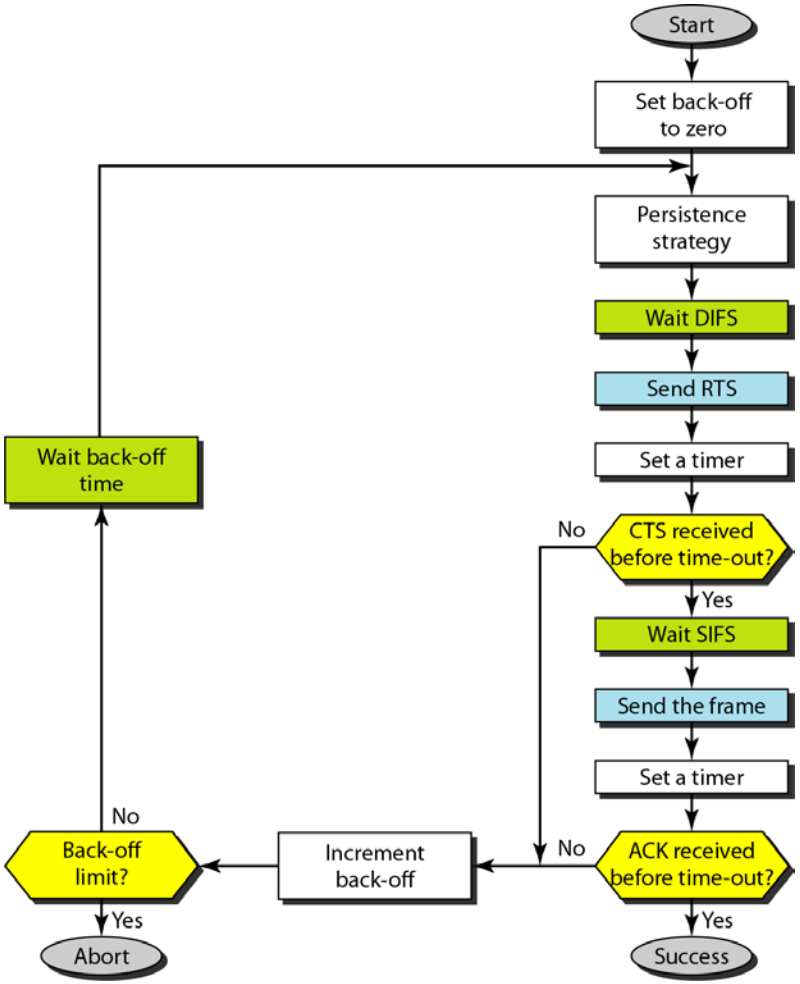


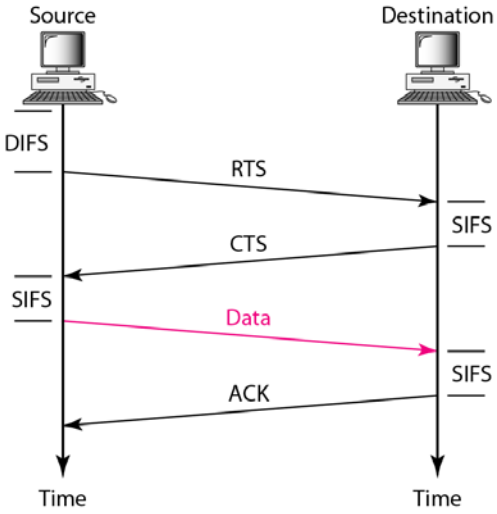
# Exposed station e RTS

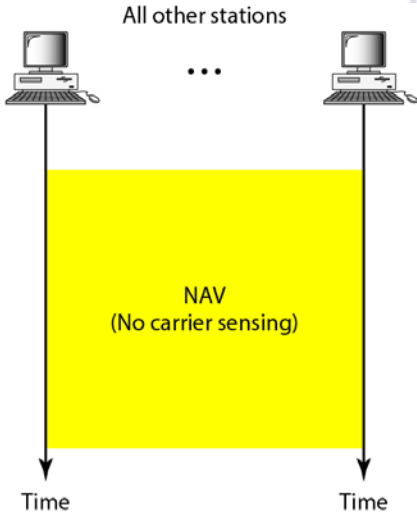


# Flowchart CSMA/CA



# Servizi

- Lo standard 802.11 stabilisce che una WLAN deve fornire 9 servizi, divisi in due categorie, 5 servizi di distribuzione e 4 servizi di stazione
- I primi sono legati alla gestione dei membri della cella e alle interazioni con le stazioni al di fuori della cella.
- I secondi sono legati alle attività all'interno di una singola cella.

# 5 distribution services

1) Associazione
   - Usato da una stazione mobile per connettersi alla stazione base non appena entra nel suo radio range
   - La stazione annuncia la sua identità e capacità (data rate, bisogno di PCF, power management)
   - La stazione base può accettare o rifiutare.
2) Disassociazione
   - La stazione o la base si possono disassociare e rompere la loro relazione.
3) Riassociazione
   - Una stazione può cambiare la stazione base preferita, per esempio spostandosi da una cella all'altra.
   - Se usata bene nessun dato dovrebbe andare perso (ma sappiamo che 802.11 come Ethernet è best effort)

# 5 distribution services

4) Distribuzione

Determina come ruotare i frame mandati ad una base station

Se la destinazione è locale alla base station si possono mandare via radio, altrimenti devono essere mandati via cavo

5) Integrazione

Se un frame deve essere mandato ad una rete non 802.11 con uno schema di indirizzamento o di framing diverso, questo servizio gestisce la traduzione richiesta dalla rete di destinazione

# 4 station services

1) Autenticazione

Una stazione deve autenticarsi per evitare che i frame arrivino a stazioni non autorizzate.

Quando una stazione è stata associata (accettata nella cella) la stazione base manda uno speciale frame di challenge per vedere se la stazione base conosce una chiave segreta.

La sfida è rimandare indietro il frame criptato con la chiave.

2) Deautenticazione

Quando una stazione vuole lasciare la rete viene deautenticata.

Dopo di che non appartiene più alla rete

# 4 station services

3) Privacy

Il wireless viene sniffato facilmente per cui deve essere criptato

Per esempio con algoritmo RC4 o AES

4) Data Delivery

Fornisce i servizi per trasmettere e ricevere i dati, come Ethernet, non c'è garanzia di consegna affidabile per cui i layer superiori devono rivelare e gestire gli errori