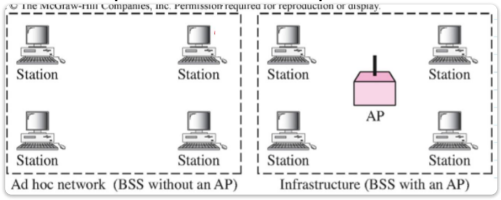
RETI WIRELESS

- Dipositivi collegati senza filo

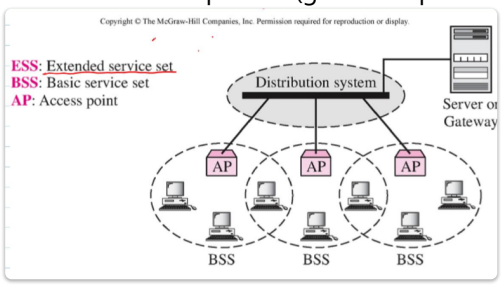
MODALITA' DI COMUNICAZIONE

- *Infrastrutturata*: i terminali wireless non sono direttamente collegati tra loro - esiste un access point il quale permette di gestire le richieste (sistema centralizzato)

- *Rete Ad-Hoc*: non è presente l'access point - i terminali possono collegarsi direttamente tra loro
  - Più impegnativo per la rete
  - Utilizzato in aree piuttosto ridotte
  - I segnali vengono talvolta potenziati grazie ai dispositivi della rete per arrivare in tratte più lunghe



- *Extended Service Set* (ESS): rete infrastrutturata in cui i diversi access point sono connessi in rete - esiste un server che gestisce gli indirizzi → si può effettuare comunicazioni tra più reti (gli access point sono in comunicazione tra loro)



STANDARDIZZAZIONE

- Wi-Fi Alliance
  - Certifica apparati e sviluppa standard di rete
  - Gli apparati che hanno questo riconoscimento rispondono allo standard IEEE 802.11

ANALISI SWOT

Punti di forza (strenghts)

- Connettività obiqua
- Accesso in mobilità
- Facilità di installazione
- Servizio Standardizzato (cfr. Wi-Fi Alliance)

Debolezze (weaknesses)

- Banda di accesso (velocità accesso) inferiore alle reti cablate (wired)
- Sensibilità ai disturbi (possibili interferenze)
- Delay quando si utilizzano servizi a grandi latenze

Opportunità (opportunities)

- Nuove applicazioni facilmente sviluppabili (standardizzato)

- Costi ridotti (standardizzato)
- Convergenza - far colloquiare reti wireless con reti di tecnologia diverse

Minacce (threats)

- Sicurezza (potenziale man-in-the-middle)
- Riservatezza (privacy bassa)

LIVELLO MAC

- Si basa sulla metodologia di tecniche CSMA. Data tuttavia la specificità dell'ambiente wireless, le tecniche già note non sono efficaci
  - Ad esempio, le tecniche CSMA semplici (non CD) la rilevazione delle collisioni avveniva una volta completata la fase di accesso rimanendo in ascolto per un tempo adeguato per comprendere se nel canale c'era sempre attività
  - Questa modalità nel contesto wireless non è sempre efficiente: essendo il canale radio soggetto a disturbi/interferenze esterne può capitare che durante la fase di ascolto successiva alla fine della trasmissione si rilevino ancora segnali con sufficiente potenza da far credere che ci sia ancora attività sul canale (quando in realtà sono solo disturbi)
  - La tecnica CSMA/CD non si può applicare in wireless perché (causa problemi radio), un dispositivo può tramite l'apposito collegamento all'antenna o trasmettere o ricevere (non entrambi contemporaneamente)

  Pertanto, si utilizza la tecnica

$$\text{CSMA/CA}$$

- Dove CA indica *collision avoidance* (evitare collisioni)
  - Si cerca cioè di **prevenire** le collisioni (non risolverle poi)

CSMA/CA

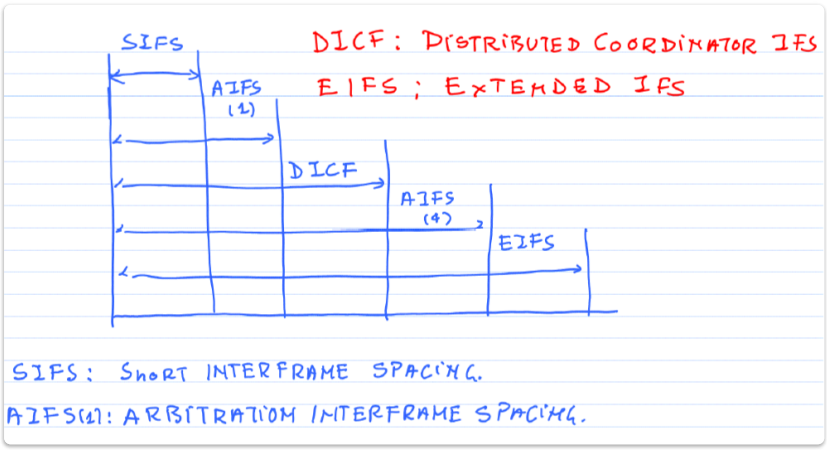
È un protocollo di accesso multiplo

Metodo:

- Si introducono appositi ritardi nell'invio di un frame per evitare collisioni. In generale: { ritardo basso $\longleftrightarrow$ azione con priorità alta }

  Il ritardo suddetto prende il nome di

$$\text{INTER FRAME SPACING (IFS)}$$



  Si nota come:
  - S: short (ritardo più piccolo possibile)
  - A: arbitration (accesso coordinato - ritardo immediatamente più grande)
  - D: distributed (ritardo per fase di accesso casuale)
  - (A: aritration 2) (non sempre prevista)
  - E: extended (ritardo più grande)

Un terminale quindi che vuole accedere in modalità casuale:

- Ascolta il canale e attende almeno un tempo SIFS (short)

- Se per ora è libero, attende anche un ulteriore intervallo AIFS per capire se nel frattempo si è provato a collegare qualcuno
- Attende quindi un ulteriore tempo fino a completare la fase DIFS (detta anche DICS)
- Se è ancora libero, accede e inizia trasmettere il proprio pacchetto
    - Per capire se è andato tutto bene, si prepara a ricevere nell'istante successivo (entro il tempo SIFS) il messaggio di Ack (che quindi ha la massima priorità)
        - L'invio dell'Ack ha una doppia funzione: far capire se è andato o meno tutto bene; dar la possibilità esclusiva a chi riceve Ack di inviare subito un nuovo pacchetto (quindi appena chiusa la fase DIFS e dopo aver atteso un tempo SIFS viene subito mandato un nuovo pacchetto se va tutto bene) $\rightarrow$ si riducono tempi di latenza
        - Se c'è stato qualche problema, si attiva il meccanismo di risoluzione delle collisioni (quello già visto)

RITARDO ESPONENZIALE (EXPONENTIAL BACK-OFF)

Nota: tanto più è lungo l'intervallo in termini di tempo entro cui si sceglie l'istante per il nuovo tentativo, tanto più piccola è la probabilità che supponendo due client che hanno colliso scelgano lo stesso istante (probabilità uniforme)

- Però tanto più lungo è questo intervallo e più ritardo si impone ai nuovi tentativi (quindi dobbiamo cercare di minimizzare con criterio il ritardo)
- È stato perciò creato un *algoritmo* che adatta la lunghezza di un intervallo temporale in cui si va a ritrasmettere alla relativa necessità di farlo (ovvero al numero di collisioni che vengono rilevate, cioè: si parte da un valore piccolo - se abbiamo collisione si raddoppia - se abbiamo ancora collisione si raddoppia - etc... - fino a un valore massimo (poi viene cancellato))

L'aumento progressivo dell'intervallo prende il nome di *exponential-back-off*

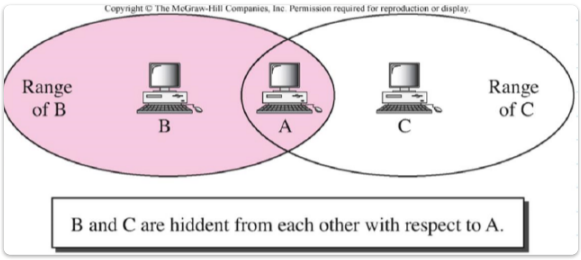
Matematicamente:

- Cerchiamo di esprimere con $Cw_{(i)}$ l'ampiezza dell'intervallo di back-off alla iterazione i-esima (cioè dopo i collisioni). È dato dal doppio del valore dell'istante precedente e il valore massimo In formule:

$$Cw_{(i)} = \min\{2Cw_{(i-1)}, Cw_{MAX}\}$$

TERMINALE NASCOSTO

La tecnica CSMA/CA presenta un problema noto con il nome di $terminale\ nascosto$



- Specifico per reti Ad-Hoc (la rete infrastrutturata non presenta questo problema)
- Abbiamo tre terminali
- Ciascun ellisse è il raggio di copertura, ovvero la distanza entro la quale il segnale emesso dal terminale che è al centro può essere ricevuto in maniera comprensibile (senza problemi)
    - Al di fuori, il segnale arriva solo come rumore di fondo
    - Si nota come il terminale A è situato nella sovrapposizione delle due: può ricevere quindi sia da B che da C

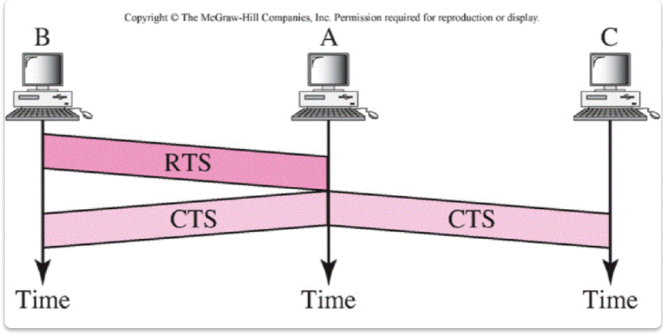
Supponiamo che B voglia dialogare con A e al contempo anche $\mathrm{C} \rightarrow \mathrm{A}$:

- C ascolta il canale, e non trovando niente trasmette
    - In realtà però avviene una *collisione* con il segnale $\mathrm{B} \rightarrow \mathrm{A}$

HANDSHAKE

Si è risolto questo problema con l'**handshake**

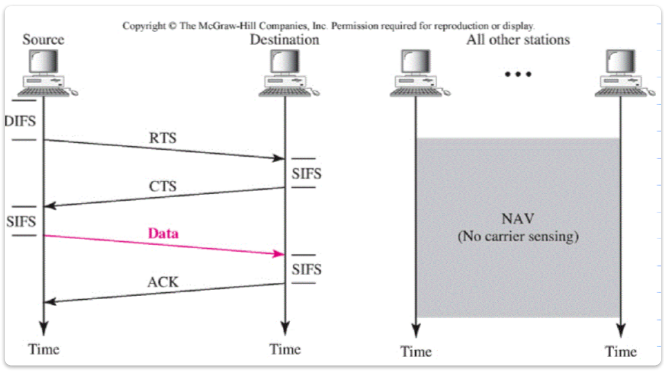
- Si mandano messaggi specifici per rendere tutti i terminali (anche quelli non in copertura radio tra loro) consapevoli della situazione della rete (in questo caso quindi C si accorgerebbe che non può dialogare con A)



- RTS: Request To Send ("sono pronto al collegamento")
- CTS: Clear To Send ("state zitti, parla solo l'autorizzato")

FASI

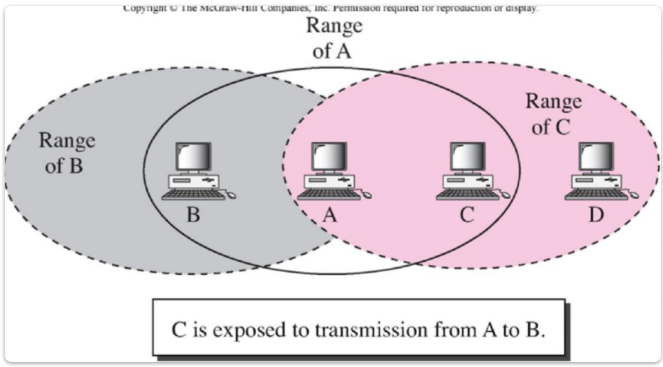
- B chiede ad A la sua disponibilità, attraverso il messaggio RTS che arriva solo ad A come detto prima
- A accetta l'invio inviando un messaggio CTS a tutti i terminali nel raggio di copertura (quindi nel caso nostro sia a B che a C)
- B interpreta il messaggio come autorizzazione all'invio dei pacchetti (abilitazione); viceversa C comprende che non potrà procedere (inibizione)



- NAV (Network Allocation Vector): specifica per quanto tempo la connessione è stata prenotata tramite il messaggio RTS
  - Utile per non far consumare energia inutile ai terminali che non son riusciti a entrare in collegamento (tempo di letargo)
  - È come se fosse un countdown che parte da una cifra indicata in RTS e scende a zero via via

TERMINALE ESPOSTO

È un altro problema della tecnica CSMA/CA



- Abbiamo 4 terminali stavolta

Il terminale A si suppone in collegamento con B

- C ha capito questa situazione quindi viene fermato, inibito (non manda nulla anche se magari vorrebbe)
  Durante questo tempo, B vuole trasmettere a C
- B non è nel raggio radio di A (nonostante dalla figura non sia ben chiaro), quindi potenzialmente può fare questa operazione
- Non lo può tuttavia fare perché C è inibito a qualsiasi azione sulla rete

Questo è un *problema che non si risolve*: se vogliamo risolvere il terminale nascosto, il terminale esposto si può presentare come problema (non si possono risolvere entrambi)
Quindi B deve aspettare il periodo di NAV prima di trasmettere

> *Se abbiamo una rete infrastrutturata non c'è problema né di terminale nascosto né di terminale esposto*

FRAMMENTAZIONE

- Per contrastare la vulnerabilità agli errori d'integrità si cerca di trasmettere pacchetti composti da pochi bit
  Ciò è permesso dalla frammentazione
- Nota: il canale dovrà restare aperto finché non si completa l'invio di tutti i frames

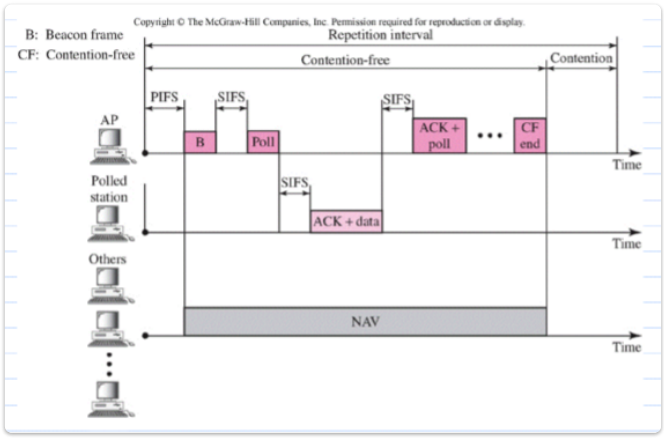
IN RETI INFRASTRUTTURATE (CON ACCESS POINT)

La fase di accesso casuale è anticipata da una fase di *accesso coordinato* (senza contesa)

- Questa modalità è detta PCF (Point Coordinator Function)

Durante questo tempo di accesso senza contesa, l'access point aspetta un tempo detto PIFS per poi avvisare tutti che inizierà la fase di accesso ordinato, mandando un segnale di riferimento che fa capire l'inizio di questo periodo (segnale detto Beacon $\{B\}$) - chi deve mandare manda, chi non deve far niente sta fermo $\rightarrow$ valore NAV per tutti quelli che non partecipano

- Si procede quindi con un POLLING (interrogazione diretta): l'Access Point manda l'autorizzazione a un terminale della lista, riceve il riscontro e quindi continua con gli altri
- Alla fine viene mandato un messaggio di fine attività detto $\mathrm{CF\ END}$



Conclusioni finali: MONOPOLIZZAZIONE ACCESSO

Sappiamo che un terminale che acquisisce l'accesso, con la modalità SIFS può gestirlo finché ne non ha concluso il suo periodo di necessità.
Si nota quindi: se un terminale che acquisisce il diritto di accesso ha bisogno continuo di accedere al canale, egli lo monopolizza

Soluzione: TXOP

La soluzione è quella di assegnare a ciascun terminale **un tempo massimo di accesso consecutivo**. Prende il nome di TXOP