reti locali senza fili, o con pochi fili

lo standard IEEE 802.11

g. di battista, m. patrignani

nota di copyright

- questo insieme di slides è protetto dalle leggi sul copyright
- il titolo ed il copyright relativi alle slides (inclusi, ma non limitatamente, immagini, foto, animazioni, video, audio, musica e testo) sono di proprietà degli autori indicati sulla prima pagina
- le slides possono essere riprodotte ed utilizzate liberamente, non a fini di lucro, da università e scuole pubbliche e da istituti pubblici di ricerca
- ogni altro uso o riproduzione è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori
- l'informazione contenuta in queste slides è fornita per scopi didattici e non può essere usata in progetti di reti, impianti, prodotti, ecc.
- gli autori non si assumono nessuna responsabilità per il contenuto delle slides, che sono comunque soggette a cambiamento
- questa nota di copyright non deve essere mai rimossa e deve essere riportata anche in casi di uso parziale

motivazioni

- edifici o locali nei quali non è possibile o economico realizzare un cablaggio
- uffici nei quali gli impiegati sono presenti occasionalmente
- aree pubbliche con utenti occasionali
  - aeroporti, stazioni, sale congressi, alberghi, caffè
- praticità di utilizzo
  - attualmente molti portatili non hanno Ethernet ed hanno solo la scheda di rete senza fili

problemi

- mezzo trasmissivo poco affidabile
- consumo energetico
  - se è comunque necessario avere un link con l'alimentazione, allora la praticità è ridotta
- area di copertura limitata
- salute
- aspetti legali sull'uso delle frequenze
- sicurezza
  - chiunque può ascoltare la rete

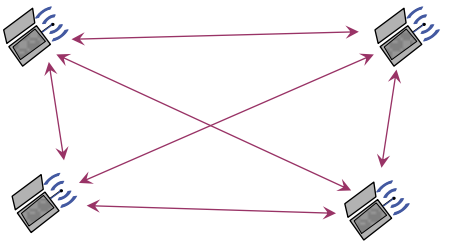
un po' di storia

- nel 1990 il comitato IEEE 802 forma il working group IEEE 802.11, dedicato alle wireless LAN
- il primo standard 802.11 ad affermarsi è stato 802.11b
- nel 1999 si forma il consorzio Wireless Ethernet Compatibility Alliance, successivamente denominato Wi-Fi (Wireless Fidelity) Alliance, per la certificazione dei prodotti 802.11

architetture

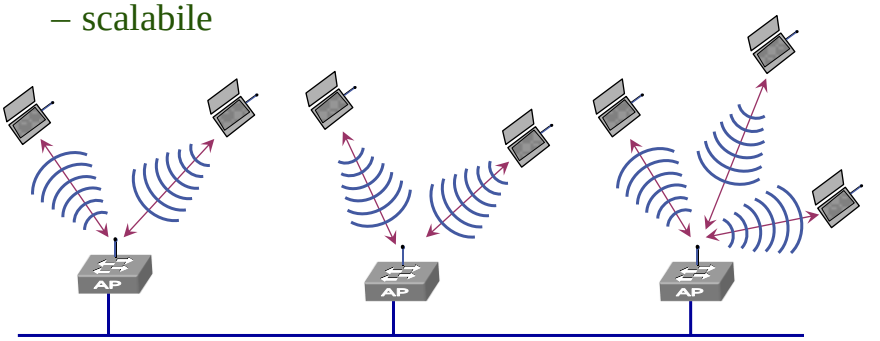
IEEE 802.11 – architetture

- reti *ad hoc*
  - le stazioni comunicano direttamente l'una con l'altra
  - pochi calcolatori in rete



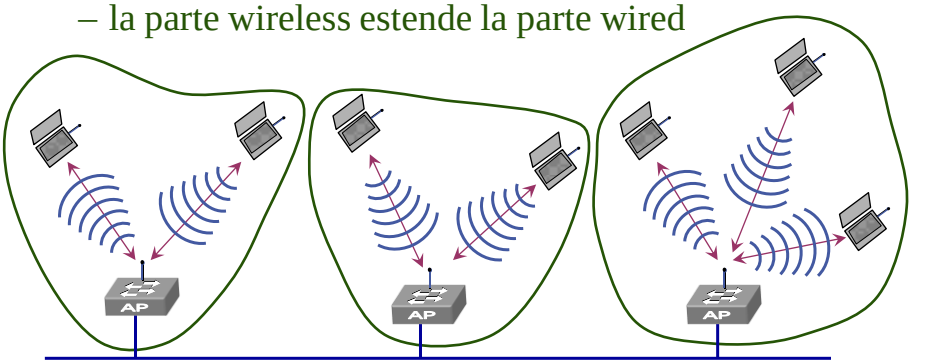
IEEE 802.11 – architetture

- reti strutturate
  - le stazioni comunicano l'una con l'altra solo mediante punti di accesso (Access Point o AP)
  - interconnessione con reti wired
  - scalabile



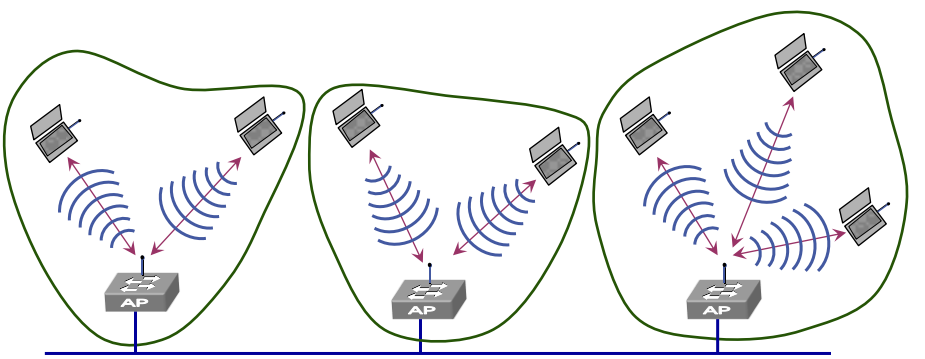
IEEE 802.11 – architetture

- reti strutturate
  - un AP ha il mac IEEE 802.11 e si comporta come un bridge
  - ciascun AP controlla un BSS (Basic Service Set)
  - la parte wireless estende la parte wired



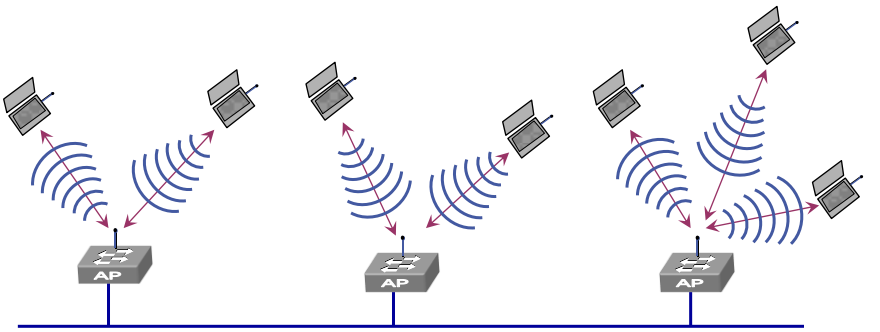
IEEE 802.11 – architetture

- reti strutturate
  - ogni BSS (Basic Service Set) ha un IDentifier (BSSID): ad es. l'indirizzo mac della scheda wireless dell'access point



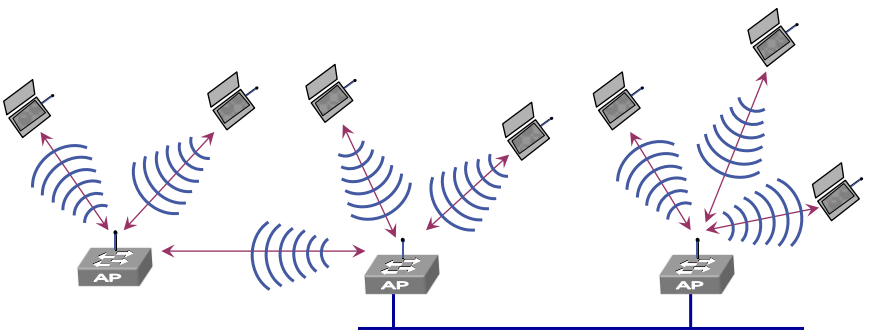
IEEE 802.11 – architetture

- reti strutturate
  - DS (Distribution System): rete wired di backbone



IEEE 802.11 – architetture

- reti strutturate
  - è previsto anche il caso in cui gli AP (tutti o alcuni) dialoghino wireless e non tramite l'infrastruttura wired

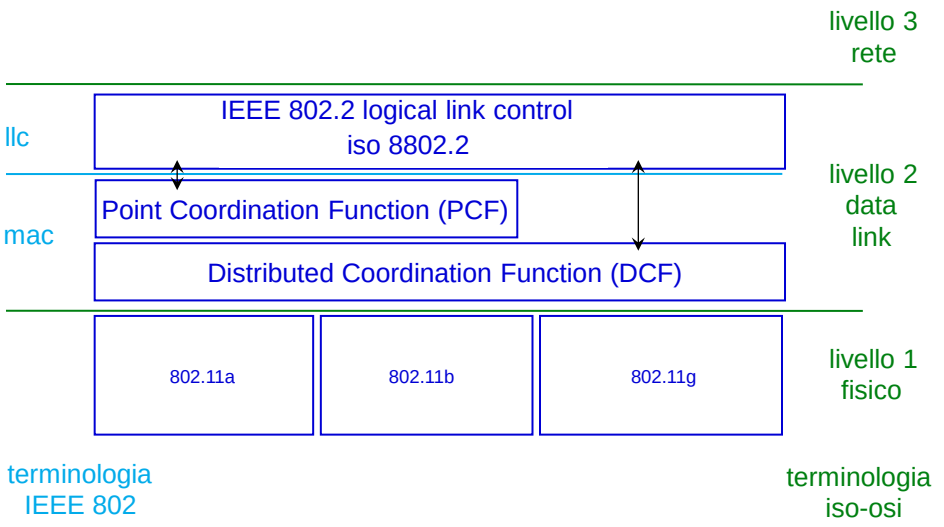


il mac

IEEE 802.11 – livello 2

- sottolivello llc
  - standard IEEE 802.2
- sottolivello mac
  - accesso al mezzo trasmissivo
  - spedizione affidabile delle pdu
  - sicurezza

IEEE 802.11 – mac e livelli vicini



due algoritmi per il mac

- accesso distribuito al mezzo trasmissivo, realizzato nel DCF – Distributed Coordination Function
  - ci occupiamo solo del DCF, ampiamente utilizzato
- accesso centralizzato al mezzo trasmissivo gestito da un gestore centralizzato, realizzato nel PCF – Point Coordination Function
  - implementato in pochi dispositivi e poco utilizzato

campi del pacchetto mac

- frame control: indica il tipo di pacchetto (controllo o dati) e fornisce informazioni di controllo
  - from e to DS
  - informazioni per la frammentazione
  - informazioni sulla riservatezza
- duration: indica il tempo necessario per la trasmissione
- indirizzi: fino a 4 indirizzi mac

campi del pacchetto mac

- sequence control: contiene informazioni utili per la frammentazione/riassemblaggio
- body: contiene una llc-pdu o informazioni di controllo del mac
- fcs: 32 bit di crc

indirizzamento

indirizzi mac

- analogamente alle normali schede di rete, ogni scheda wireless è dotata di un indirizzo mac
- il pacchetto viene raccolto da una scheda wireless se è diretto al suo indirizzo mac
  - due macchine che si scambiano pacchetti wireless devono conoscere i rispettivi indirizzi mac

indirizzamento

- nel pacchetto mac ci sono ben 4 indirizzi:
  - address 1, address 2, address 3 e address 4
- più due bit:
  - chiamati ToDS e FromDS
  - ToDS vale 1 quando il pacchetto è spedito all'AP per essere smistato sul DS
  - FromDS vale 1 quando il pacchetto è stato ricevuto dal DS

indirizzamento

- i quattro indirizzi sono usati secondo quanto specificato nella tabella

ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID	SA	DA	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

- address 1 è sempre l'indirizzo mac della scheda wireless cui è destinato il pacchetto
- address 2 è sempre l'indirizzo mac della scheda wireless che trasmette il pacchetto

ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID	SA	DA	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

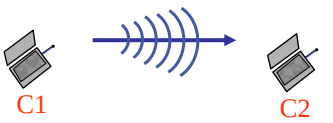
- address 3: se FromDS=1 contiene SA e se ToDS=1 contiene DA
- address 4 è usato solo nel caso di comunicazione wireless nel distribution system

ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID	SA	DA	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

- trasmissione diretta tra due stazioni

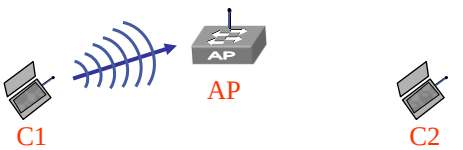


ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA=C2	SA=C1	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID	SA	DA	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

- trasmissione da una stazione all'AP

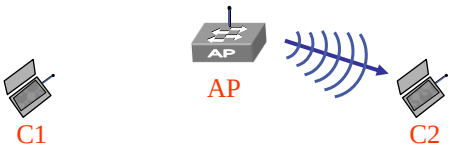


ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID=AP	SA=C1	DA=C2	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

- trasmissione dall'AP ad una stazione

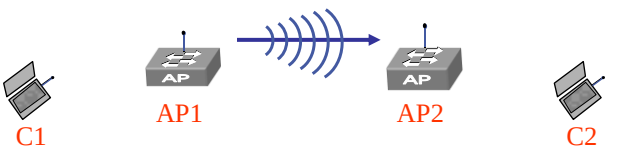


ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA=C2	BSSID=AP	SA=C1	_
1	0	BSSID	SA	DA	_
1	1	RA	TA	DA	SA

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

indirizzamento

- trasmissione dall'AP ad una stazione



ToDS	FromDS	address 1	address 2	address 3	address 4
0	0	DA	SA	BSSID	_
0	1	DA	BSSID	SA	_
1	0	BSSID	SA	DA	_
1	1	RA=AP2	TA=AP1	DA=C2	SA=C1

RA=recipient address (scheda ricevente), TA=transmitter address (scheda trasmittente), DA=destination address (destinatario finale), SA=sender address (sorgente del pacchetto)

DCF – Distributed Coordination Function

requisiti del DCF mac

- evitare interferenze tra trasmissioni simultanee
  - consentendo il maggior numero possibile di trasmissioni
  - in modo tale che il canale trasmissivo sia gestito con ragionevole equità
- nessun controllo centralizzato
- nessun clock
  - trasmissioni completamente asincrone

DCF utilizza csma/ca

- variante di csma/cd
- carrier sense multiple access / collision avoidance
  - se una stazione ha un pacchetto da spedire ascolta il mezzo trasmissivo
  - se il mezzo trasmissivo è inutilizzato allora trasmette
  - altrimenti attende che la trasmissione corrente sia stata completata

DCF utilizza csma/ca

- non si fa collision detection
  - inefficace nelle reti wireless: è difficile distinguere pacchetti in arrivo (in collisione con la propria trasmissione) dal rumore
- si fa collision avoidance
  - si cerca, per quanto possibile, di evitare collisioni
  - strumenti utilizzati: backoff, acknowledgement, Request To Send / Clear To Send (RTS/CTS)

DCF e inter-packet gap

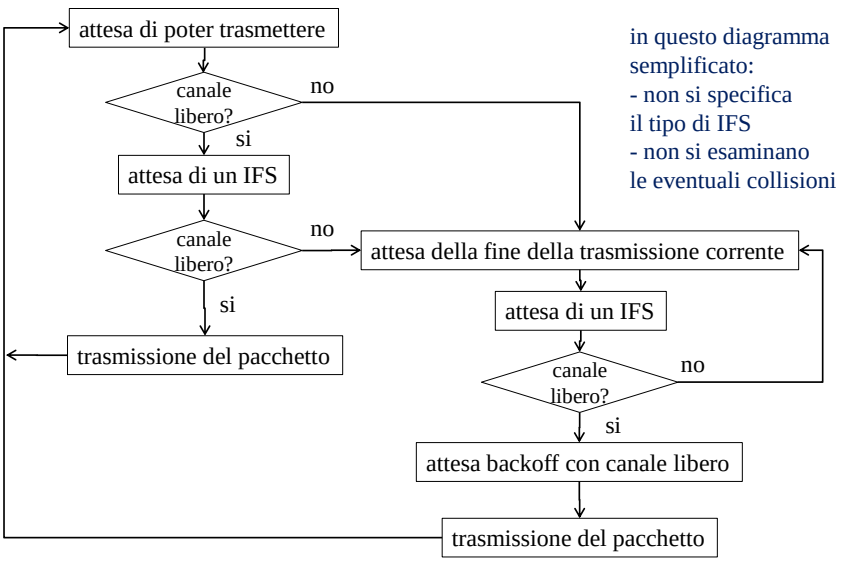
- DCF sfrutta i ritardi tra pacchetti consecutivi come strumento per gestire delle priorità
- due tipi principali di inter-packet gap (Inter-Frame Space, IFS)
  - DIFS: DCF Inter-Frame Space
  - SIFS: Short Inter-Frame Space (SIFS < DIFS)
- ci sono altri tipi di IFS

DCF senza RTS/CTS

per cercare di evitare collisioni

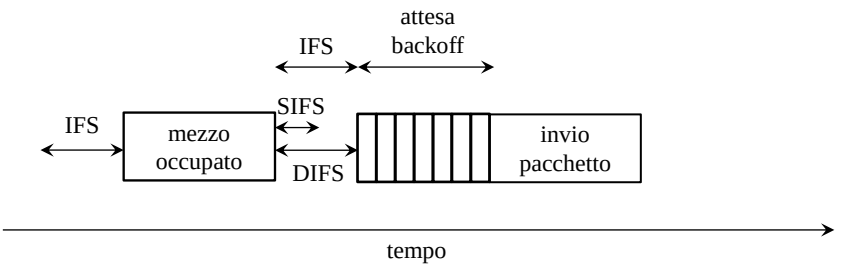
- quando una stazione vuole trasmettere ma il canale è occupato sceglie un numero random di backoff nell'intervallo [0, cw] ed inizializza un timer
  - decrementa il timer di backoff quando il canale è libero
  - quando il canale è occupato il decremento è sospeso
  - quando il timer raggiunge 0 la trasmissione può avvenire
- quando una stazione rileva una collisione duplica cw
  - rimane da stabilire in cosa consista una collisione e come si possa rilevare senza collision detection
  - cw è limitato superiormente da cw_{max}
- se un pacchetto è inviato con successo si pone $cw=cw_{min}$
- valori ragionevoli per cw_{min} e cw_{max} sono 7/../31 e 255/../1023

spedizione di un pacchetto



in questo diagramma semplificato:
- non si specifica il tipo di IFS
- non si esaminano le eventuali collisioni

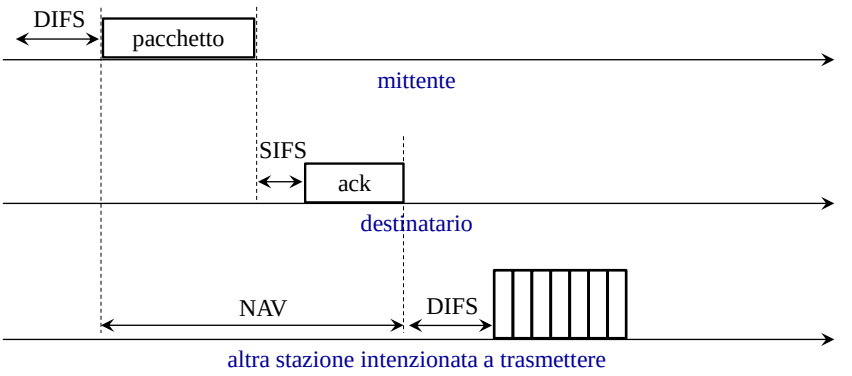
trasmissione senza uso di RTS/CTS



trasmissione senza uso di RTS/CTS

- in un pacchetto spedito è specificata la durata (campo duration) della trasmissione
- la durata viene memorizzata, da ogni stazione in ascolto, nel proprio NAV (Network Allocation Vector)
- il NAV viene utilizzato per sincronizzare le stazioni
  - ogni stazione decrementa il suo NAV con il passare del tempo
  - una stazione può trasmettere solo quando il proprio NAV è a zero

trasmissione senza uso di RTS/CTS



trasmissione senza uso di RTS/CTS

- nella spedizione di un acknowledgement si attende SIFS, più breve di DIFS
- ciò implica priorità rispetto a qualunque altra trasmissione

carrier sense

- il mac IEEE 802.11 usa due strumenti per fare carrier sense
  - fisico: informazione di canale libero dal livello fisico
  - logico: il NAV
- il canale è ritenuto libero quando entrambe le seguenti condizioni sono vere:
  - il livello fisico segnala canale libero
  - il NAV è arrivato a zero

ack e collisioni

- quando una stazione inizia a trasmettere un pacchetto non si interrompe fino alla fine
- la trasmissione del pacchetto dati è sempre terminata da un riscontro (acknowledgement – ack)
- collisione = pacchetto che non ottiene ack
  - è il momento in cui si duplica il valore di cw nel backoff

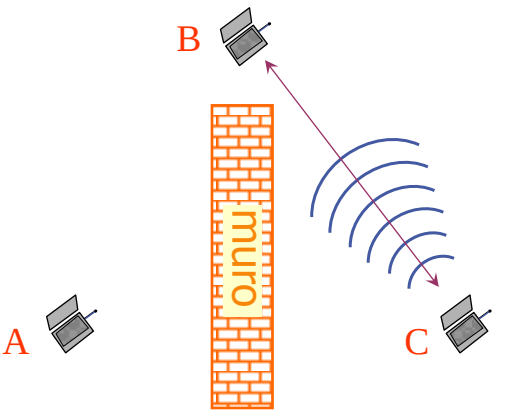
DCF con RTS/CTS

due problemi

- se il pacchetto su cui si verifica una collisione è molto grande si perde molto tempo prima che la collisione sia riscontrata
- mentre su una rete Ethernet ogni stazione "vede" ogni altra stazione, nelle reti wireless non è così
- per tentare di risolvere questi problemi il protocollo viene complicato ulteriormente

il problema della stazione nascosta

A ascolta il canale e pensa di poter trasmettere a B perché non può accorgersi del fatto che B sta già ricevendo da C



trasmissione con uso di RTS/CTS

- meccanismo di prenotazione del canale
  - quando una stazione vuole trasmettere spedisce un breve frame al destinatario, chiedendo l'autorizzazione alla trasmissione
  - se il destinatario è disponibile emette un breve frame di conferma
  - alle stazioni vicine è richiesto di non interferire per l'intera durata della trasmissione che sta per avvenire
    - la durata (residua) della trasmissione, viene dichiarata nel campo duration di ogni pacchetto scambiato tra le due stazioni

trasmissione con uso di RTS/CTS

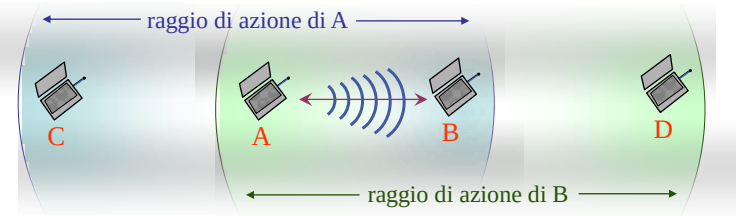
- meccanismo di prenotazione del canale
  - A vuole trasmettere a B ed il canale è libero
  - A manda un RTS (Request To Send) a B
  - B è libero quindi manda un CTS (Clear To Send) a A
    - tutte le stazioni che ricevono il CTS inviato da B e/o l'RTS inviato da A, ora sanno che B ed A stanno trasmettendo
    - le stazioni che vogliono trasmettere ad A o B dovranno aspettare un tempo pari alla "duration" specificata nei pacchetti inviati da A o B
  - A trasmette a B

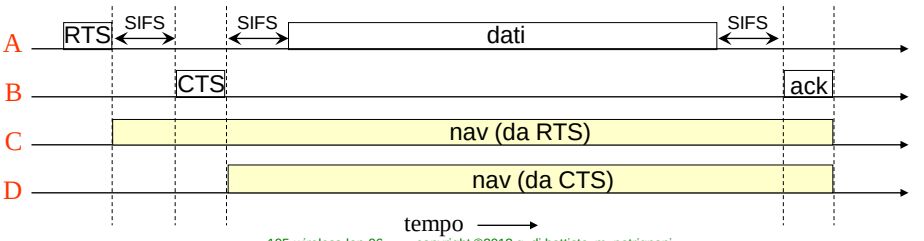
trasmissione con uso di RTS/CTS

- la duration viene memorizzata da ogni stazione in ascolto nel suo NAV (Network Allocation Vector)
- il NAV viene utilizzato per sincronizzare le stazioni
  - ogni stazione decrementa il suo NAV con il passare del tempo
  - quando il NAV è a zero la stazione può trasmettere
- le uniche collisioni possibili sono dovute all'invio simultaneo da parte di due stazioni dell'RTS

trasmissione con uso di RTS/CTS

- esempio di trasmissione senza collisioni





RTS/CTS e collisioni

- percezione della collisione
  - la collisione viene rilevata quando la stazione trasmittente non riceve il CTS del destinatario

algoritmo backoff – sintesi

- algoritmo di backoff del mac 802.11
  - una stazione che rileva una collisione o che trova il canale occupato sceglie un numero a caso tra 0 e cw
  - il numero viene moltiplicato per un tempo chiamato slot-time e viene inizializzato il timer di attesa per backoff
  - ad ogni nuova collisione sullo stesso pacchetto l'estremo superiore della cw viene raddoppiato fino ad un massimo di cw_{max}
  - per ogni slot-time che il canale rimane libero, il timer viene decrementato di uno slot-time
    - a differenza di csma/cd, il valore viene decrementato solamente se il canale è libero (cioè se il NAV della stazione è pari a zero)
  - quando il timer è a zero la stazione può trasmettere
  - quando una trasmissione ha successo cw è riportato a cw_{min}

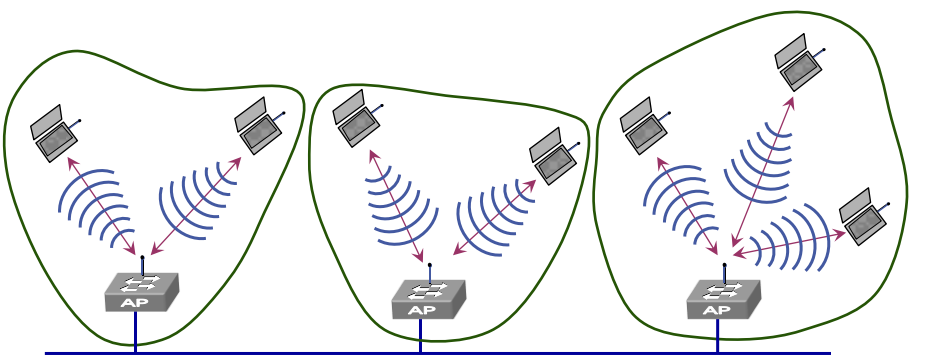
uso di RTS/CTS nella pratica

- nelle stazioni è definita una soglia *s* che stabilisce per quali pacchetti utilizzare RTS/CTS
  - si usa RTS/CTS per tutti i pacchetti il cui campo dati ha dimensione superiore ad *s*
- molto spesso *s* ha il valore della dimensione massima di un pacchetto (1.500 bytes)
  - l'effetto è quello di disabilitare RTS/CTS per la totalità dei pacchetti

altri aspetti del mac

IEEE 802.11 – handshaking

- l'insieme delle stazioni di un BSS cambia continuamente
  - i computer vengono accesi, spenti, entrano nel range di un AP e ne escono

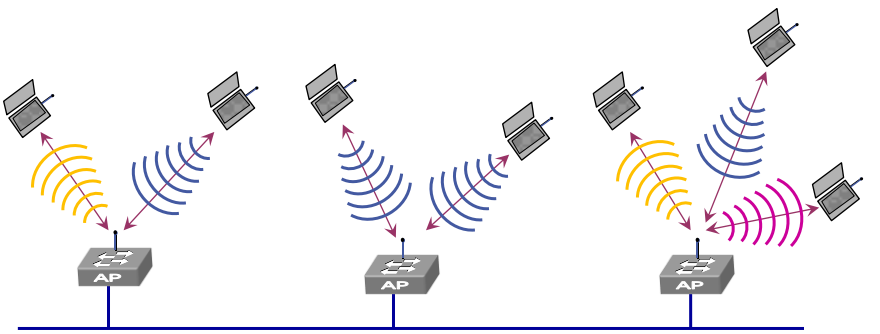


IEEE 802.11 – handshaking

- una stazione che vuole accedere ad un BSS deve scambiare informazioni di *handshaking* con l'AP di quel BSS
  - AP e stazione presentano i propri indirizzi mac
- due possibilità per l'accesso ad un BSS
  - utilizzo di pacchetti "beacon" inviati dall'AP
    - ogni AP annuncia la sua presenza inviando un pacchetto di riconoscimento broadcast, denominato "beacon frame"
  - utilizzo di pacchetti di "probe" inviati dalla stazione
    - la stazione esplora l'esterno inviando pacchetti di "probe request"
    - la stazione aspetta un pacchetto di "probe response"

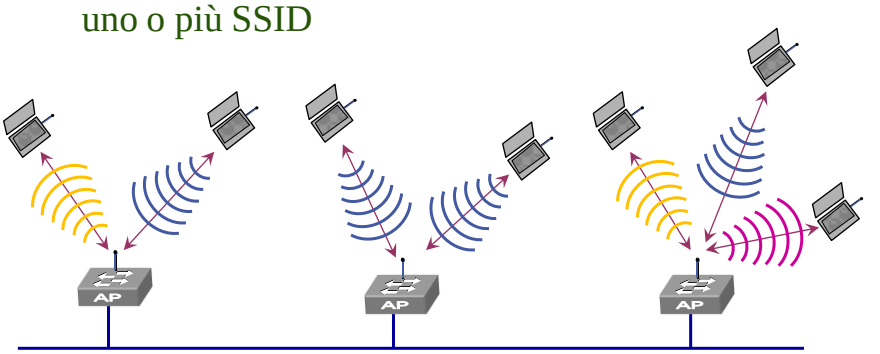
ieee 802.11 – torniamo all'architettura

- un amministratore può definire varie reti logiche sulla stessa rete fisica
  - ciascuna identificata da un Service Set ID – SSID
  - es: studenti, professori, ospiti



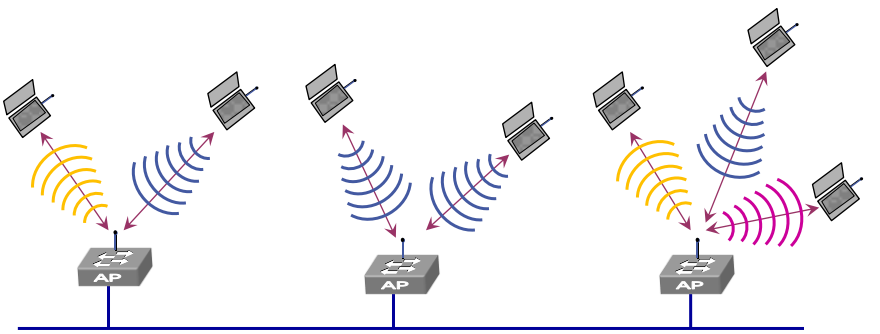
ieee 802.11 – torniamo all'architettura

- un amministratore può definire varie reti logiche sulla stessa rete fisica
  - un AP con un BSSID può, attraverso i suoi annunci, dirsi disponibile a far passare il traffico di uno o più SSID



ieee 802.11 – torniamo all'architettura

- solo chi ha gli opportuni permessi può entrare nella rete che corrisponde a un certo SSID
  - la trattazione sull'autenticazione è fuori dagli obiettivi del corso



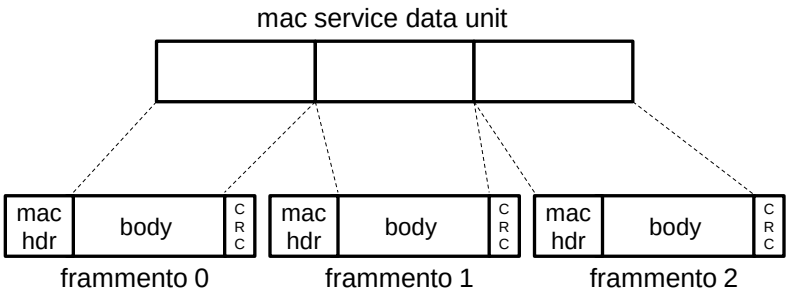
ieee 802.11 – torniamo all'architettura

- Extended Service Set – ESS
  - insieme delle stazioni appartenenti ai BSS di una rete e con lo stesso SSID
- le stazioni, pur rimanendo nello stesso ESS, si possono muovere cambiando BSS

IEEE 802.11 – frammentazione

- il livello mac può decidere di frammentare un pacchetto
  - in tal caso si occupa anche del riassemblaggio
- perché frammentare?
  - nelle wlan può essere utile avere pacchetti di dimensioni inferiori rispetto a quelli delle lan cablate
  - per ridurre l'overhead in caso di ritrasmissione del pacchetto
  - per ridurre la probabilità di errore nella trasmissione

IEEE 802.11 – frammentazione



ciascun frammento viene trattato come pacchetto e viene riscontrato singolarmente

IEEE 802.11 – frammentazione

- il mac ricevente riassembla i frammenti ricostruendo il pacchetto
- gli strati superiori e gli altri mac coinvolti nella spedizione del pacchetto non si accorgono della frammentazione
  - es. un pacchetto che viene frammentato dal mac IEEE 802.11 di un computer per la spedizione attraverso un AP verso il DS viene riassemblato sull'AP e spedito al DS intero

IEEE 802.11 – rapporto tra llc e mac

- si noti come il mac si occupi in questo caso degli acknowledgement anche se nello stesso livello 2 IEEE 802 il livello llc potrebbe fare la stessa cosa
  - essenzialmente il mac realizza un servizio di trasferimento dati con conferma
  - nel mac IEEE 802.11 gli ack sono parte fondamentale del meccanismo di riconoscimento delle collisioni

trasmissioni verso l'indirizzo mac broadcast

- nel caso in cui ToDS=0 non si usano ack e non si usano RTS/CTS
  - eventuali collisioni non sono rilevate
- nel caso in cui ToDS=1 si usano ack ed eventualmente RTS/CTS
  - i pacchetti vanno verso l'AP
- è possibile configurare un AP in modo tale che un pacchetto broadcast ricevuto sia o meno inviato a tutto il BSS

