

Corso di Laurea in Ingegneria Informatica

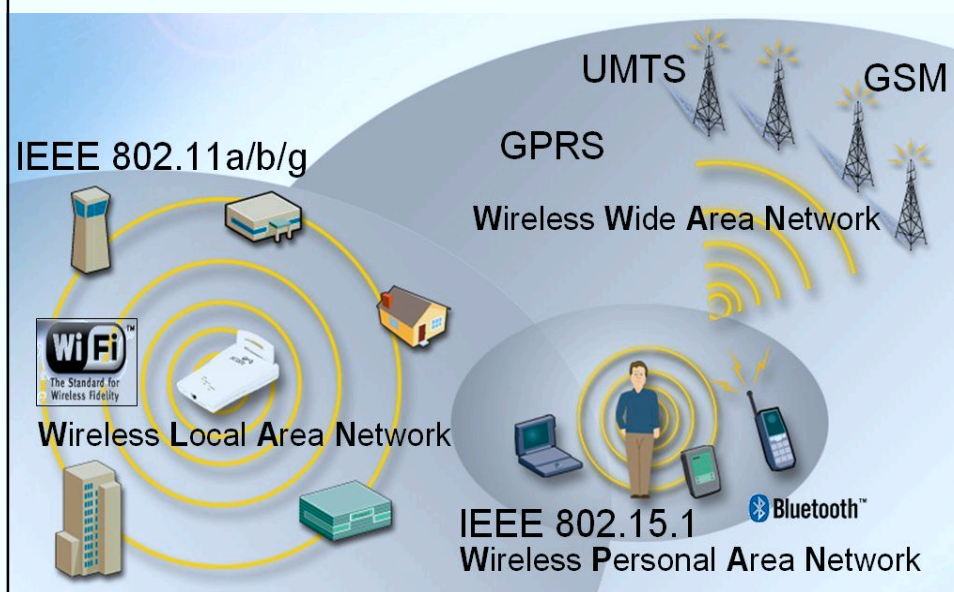


Corso di Reti di Calcolatori
a.a. 2009/10

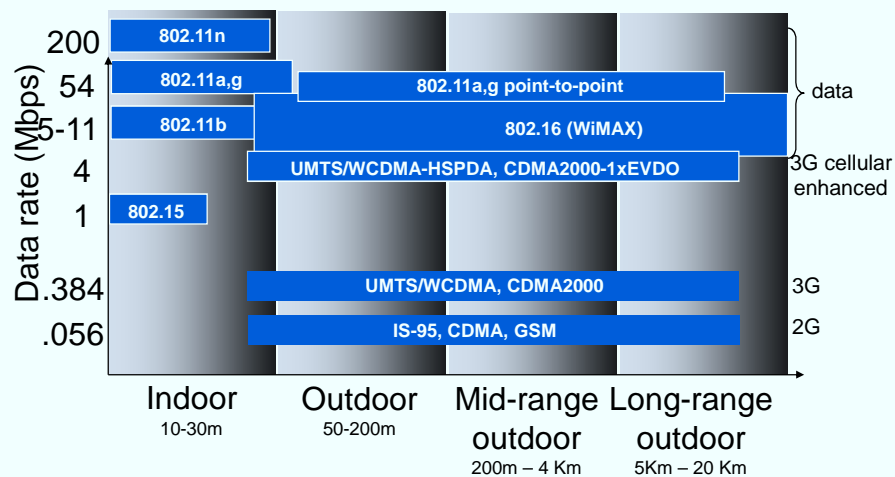
Roberto Canonico (roberto.canonico@unina.it)
Antonio Pescapè (pescapè@unina.it)

Wireless LAN

Le tecnologie wireless



Characteristics of selected wireless link standards



Le tecnologie per le WLAN



- IEEE 802.11 (1a Generazione)
 - 2.5 GHz
 - Velocità di 1-2Mb/s
- IEEE 802.11b (2a Generazione)
 - Velocità 11Mb/s
- IEEE 802.11g (3a Generazione)
 - Velocità 54Mb/s
- IEEE 802.11a
 - 5GHz
 - Fino a 54 Mbit/s

Wireless LAN: 802.11



- Le reti wireless rappresentano una tecnologia in rapida evoluzione per la connessione di computer
- In una rete locale wireless, i dispositivi non sono collegati fisicamente, ma, per comunicare, usano onde elettromagnetiche che si propagano nello spazio
- Come altre tecnologie LAN, l'802.11 è progettato per un impiego in aree geografiche limitate ed ha lo scopo principale di "fare da mediatore" nell'accesso ad un mezzo condiviso di comunicazione (in questo caso, una frequenza radio)

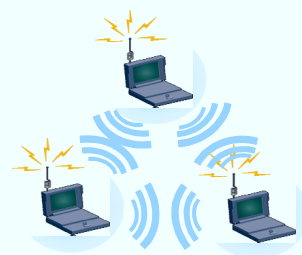
5

Rete "Ad hoc"



Gli host comunicano tra loro stabilendo delle comunicazioni punto-punto

- E' adatta per:
 - Piccolo gruppo di lavoro
 - Host vicini tra loro
 - Nessuna necessità di fornire l'accesso ad altre risorse
- Le schede di rete devono supportare la modalità



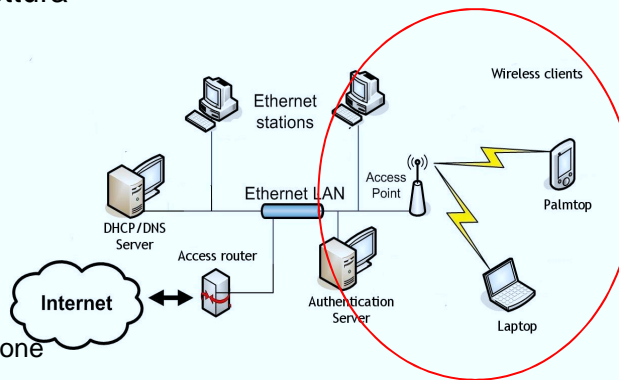
Rete "infrastructured"

- Elementi dell'architettura necessari:

- Access Points
- Clienti wireless

- Elementi opzionali:

- DNS/DHCP
- Router di accesso
- LAN
- Server di autenticazione
- Monitoraggio/Gestione Wireless LAN



WLAN/802.11: livello fisico

- 802.11 è progettato per trasmettere dati usando tre tecniche differenti:

- *frequency hopping*
- *direct sequence*
- *diffused infrared*

- Le prime due tecniche sfruttano il range di frequenza intorno ai 2.4 GHz e sono tecniche del tipo "spread spectrum":

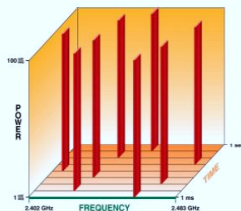
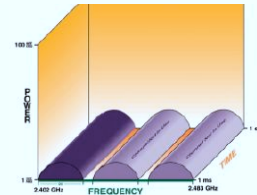
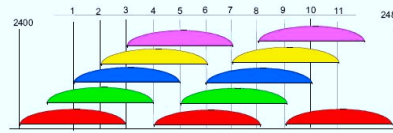
- L'obiettivo di tali tecniche è quello di diffondere il segnale su di un intervallo di frequenza ampio, in modo tale da minimizzare l'effetto dell'interferenza da parte di altri dispositivi

Spread spectrum



- Direct sequence

- 11 canali stazionari da 22 MHz
- data rate = 11 Mbps
- 3 canali non sovrapposti
- codifica del bit in una stringa di bit:
 - chipping sequence
 - ridondanza in cambio di robustezza al rumore
- trasmissione delle chipping sequence su un range di frequenze
- cambio di canale in caso di interferenza



- Frequency hopping

- 79 canali ciascuno ampio 1 MHz
- cambio di frequenza (hop) almeno ogni 0.4 secondi
- richiede sincronizzazione
- ridotta sensibilità alle interferenze
- un pacchetto perso viene trasmesso al successivo hop

9

WLAN/802.11: frequency hopping



- Il segnale è trasmesso su una sequenza “random” di frequenze
- Tale sequenza è in realtà calcolata in maniera algoritmica, tramite un generatore di numeri pseudo-casuali
- Il ricevitore:
 - utilizza il medesimo algoritmo del mittente
 - inizializzazione con il medesimo *seme*
 - è dunque in grado di “saltare” le frequenze in maniera sincronizzata con il mittente, per ricevere correttamente le frame

10

WLAN/802.11: direct sequence



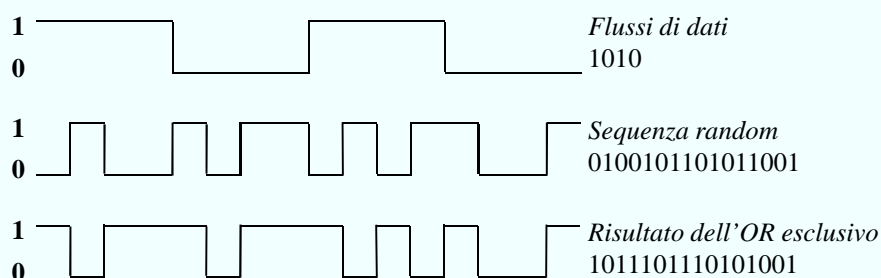
- Ogni bit di una frame è rappresentato da molteplici bit nel segnale trasmesso
 - Il mittente invia, in effetti, il risultato dell'OR esclusivo di tale bit e di n bit scelti in maniera casuale
 - Come nel caso del *frequency hopping*, la sequenza di bit casuali è generata da un generatore di numeri "pseudo-casuali" nota sia al mittente che al ricevitore
 - I valori trasmessi sono noti come *chipping sequence* (come nel caso del CDMA)
 - L'802.11 utilizza una chipping sequence a 11 bit

11

WLAN/802.11: direct sequence



- Un esempio: chipping sequence a 4 bit



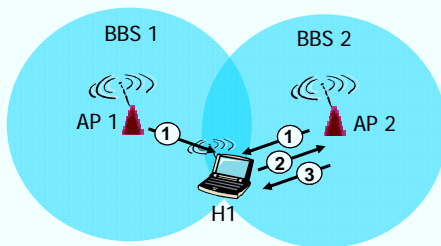
12

802.11: Canali ed associazione ad un Access Point

- 802.11b: 2.4GHz-2.485GHz
 - Lo spettro è diviso in 11 canali a differenti frequenze
 - Solo 3 canali risultano non sovrapposti
 - All'atto dell'installazione di un AP, l'amministratore di rete sceglie il canale da utilizzare per la trasmissione
 - Possibilità di interferenza nel caso in cui due AP vicini utilizzino lo stesso canale
- Un host deve *associarsi* ad un AP
 - Controlla i vari canali ascoltando le cosiddette *beacon frame*, contenenti MAC address ed identificativo (SSID – Service Set Identifier) dell'AP
 - Seleziona l'AP cui associarsi ed inizia la procedura di associazione (che può prevedere anche una fase di autenticazione)
 - Al termine di tale procedura, tipicamente effettuerà una richiesta DHCP per ottenere un indirizzo IP nella subnet dell'AP

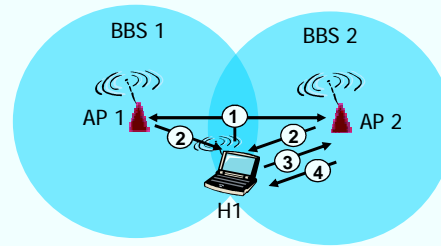
13

802.11: passive/active scanning



Passive Scanning:

- (1) beacon frames sent from APs
- (2) association Request frame sent: H1 to selected AP
- (3) association Response frame sent: H1 to selected AP



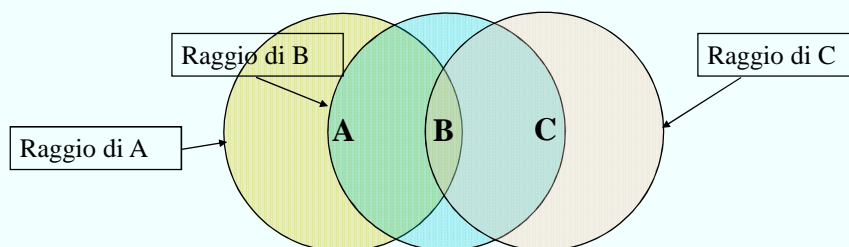
Active Scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probes response frame sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent: H1 to selected AP

WLAN/802.11: Hidden nodes problem

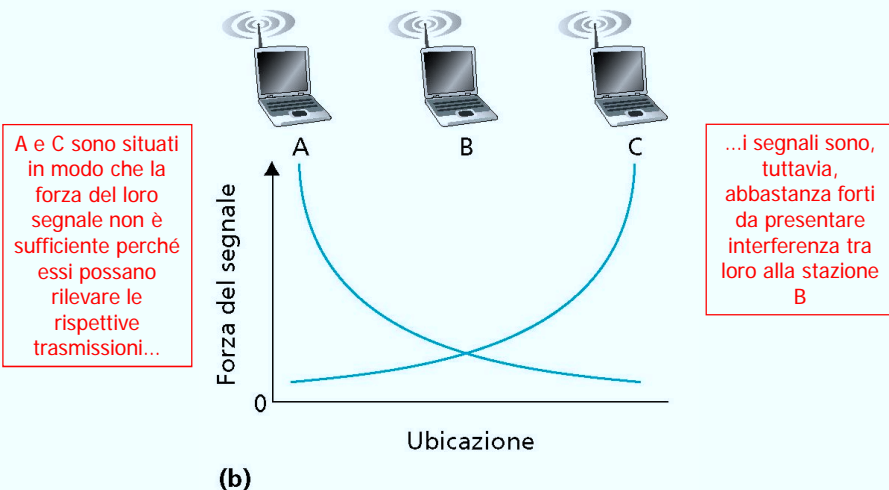


- Le trasmissioni di A non sono ascoltate da C (e viceversa)
- A e C possono inviare dati simultaneamente verso B causando una collisione in ricezione
- Né A né C sono in grado di rilevare la collisione
- A e C sono detti *nodì nascosti* (l'uno rispetto all'altro)



15

WLAN/802.11: attenuazione del segnale (*fading*)

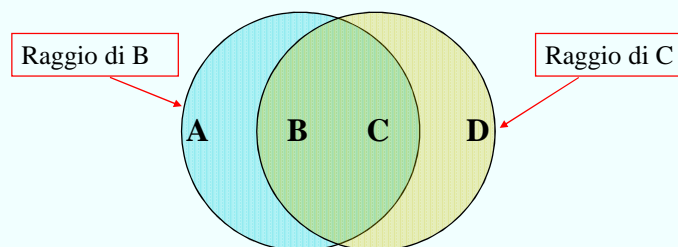


16

WLAN/802.11: Exposed nodes problem



- B invia dati ad A
- C è al corrente di tale comunicazione perché ascolta le trasmissioni di B:
 - È un errore per C concludere di non poter trasmettere a nessuno
 - Ad esempio, C potrebbe inviare frame a D senza interferire con la capacità di A di ricevere dati da B



17

IEEE 802.11: accesso multiplo



- Come Ethernet, usa il CSMA:
 - Accesso random
 - carrier sense: si evitano collisioni con eventuali trasmissioni in corso
- A differenza di Ethernet:
 - Non effettua *collision detection*
 - Tutte le frame sono trasmesse nella loro interezza
 - Usa gli *acknowledgment*
 - Conferma di avvenuta ricezione
- Perché non si effettua la *collision detection*?
 - Difficoltà a ricevere durante la trasmissione, a causa della debolezza dei segnali ricevuti (fading)
 - Impossibile in alcuni casi accorgersi delle collisioni:
 - Stazione nascosta (hidden terminal)
 - Fading (evanescenza)
- Obiettivo: **evitare le collisioni**: CSMA/C(ollision)A(voidance)

18

Protocollo CSMA/CA



802.11 sender

1 se il canale è inattivo per un tempo pari a **DIFS** (Distributed Inter Frame Space) allora

- Trasmette un'intera frame (senza CD)

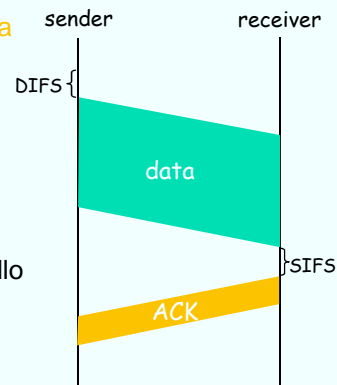
2 se il canale è occupato

- Sceglie un *backoff time* casuale
- Il timer viene decrementato mentre il canale è inattivo
- Allo scadere del timer, trasmette una frame
- Se non riceve ACK, incrementa l'intervallo di backoff casuale, torna al passo 2

802.11 receiver

Se la frame è ricevuta in maniera corretta

- restituisce un ACK dopo un tempo **SIFS** (Short Inter Frame Space)



19

Collision Avoidance: RTS/CTS

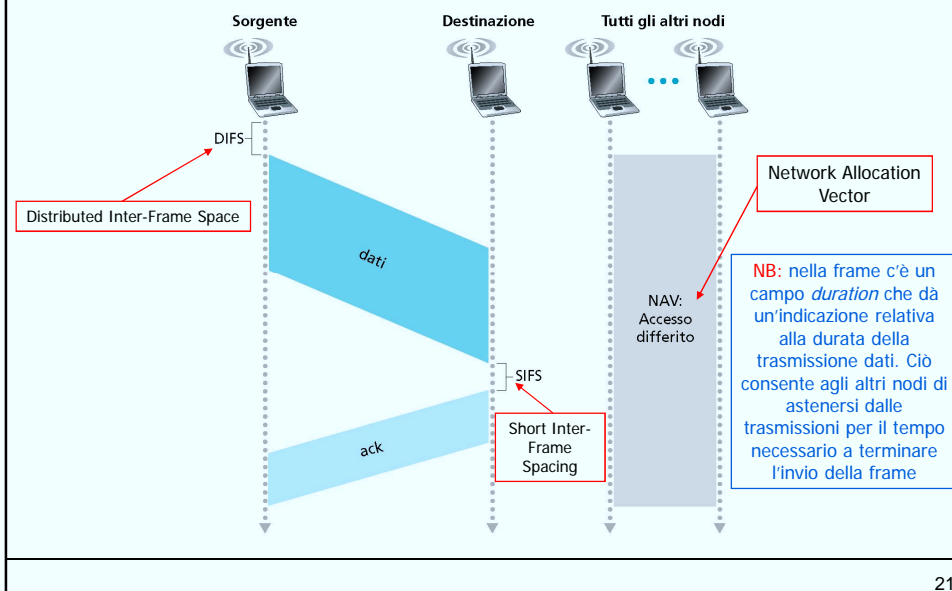


- **Idea:** consentire al mittente di "prenotare" il canale
 - Evitare collisioni per le frame di dati "lunghe"
- Soluzione opzionale
- Il mittente trasmette prima una piccola frame request-to-send (RTS) a tutti (anche all'AP), usando il CSMA, indicando il tempo totale richiesto per trasmettere la frame DATI
 - Le frame RTS possono collidere (ma sono piccole...)
- L'AP invia in broadcast una frame clear-to-send CTS in risposta alla frame RTS
- La frame CTS è ascoltata da tutti i nodi
 - Il mittente trasmette la frame dati
 - Le altre stazioni differiscono le loro trasmissioni

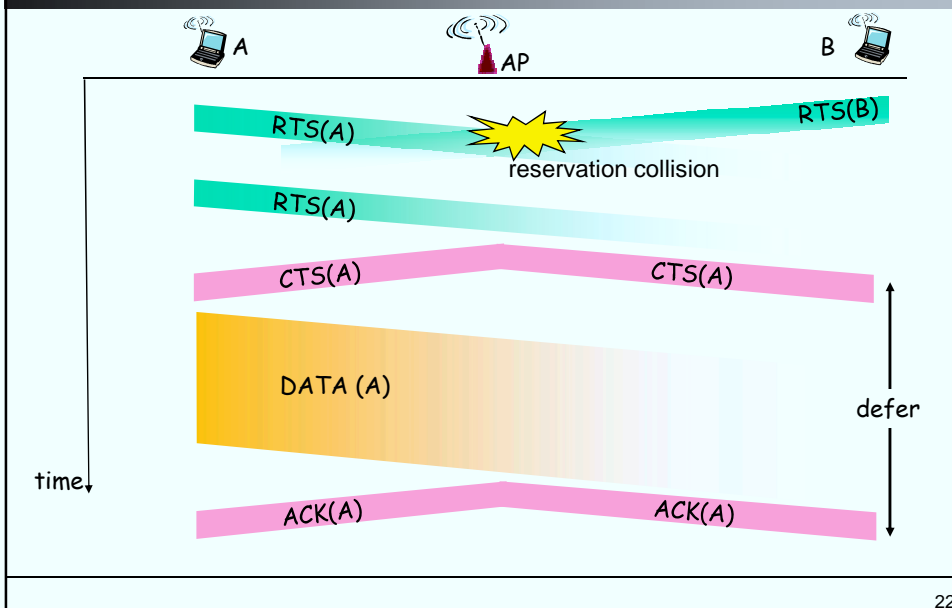
Si evitano completamente le collisioni sui dati, usando piccoli pacchetti di prenotazione!

20

WLAN/802.11: gestione dell'accesso



Collision Avoidance: RTS-CTS exchange



Ricapitolando: collision avoidance (1/2)



- Prima di inviare i dati, il mittente trasmette una frame di “richiesta di trasmissione”:
 - Request to Send (RTS):
 - In tale frame è presente anche un campo che indica la lunghezza della frame dati da trasmettere
- Il ricevitore risponde con una frame di “permesso di trasmissione”:
 - Clear to Send (CTS)
 - In tale frame viene replicato il valore relativo alla lunghezza dei dati, annunciato dal mittente

23

Ricapitolando: collision avoidance (2/2)



- Un nodo che vede la frame CTS sa di essere vicino al ricevitore:
 - Esso non può trasmettere per tutto il tempo necessario ad inviare la frame dati (la cui lunghezza è stata specificata nella frame RTS)
- Un nodo che vede la frame RTS, ma non quella CTS, non è abbastanza vicino al ricevitore per interferire con esso e può quindi trasmettere senza attendere
- Il ricevitore invia un ACK dopo aver ricevuto una frame
- I nodi non rilevano le collisioni:
 - Se due nodi inviano una frame RTS in contemporanea, queste frame collideranno
 - I nodi assumono che vi sia stata una collisione se non ricevono una frame CTS di risposta

24

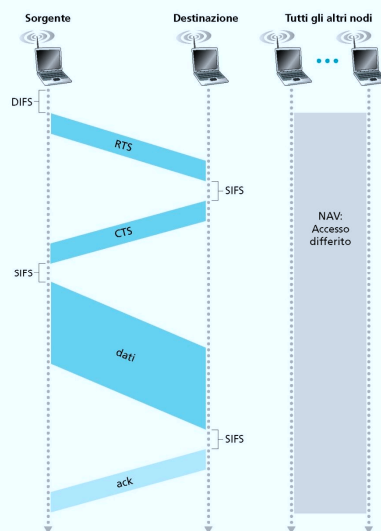
WLAN/802.11: Medium Access Control



- Il metodo di accesso è simile ad Ethernet:
 - Prima di trasmettere, si attende finché il canale diventa libero
 - In caso di collisione:
 - algoritmo del *binary exponential backoff*
- Tuttavia, bisogna tenere in considerazione il fatto che non tutti i nodi sono sempre alla portata l'uno dell'altro
 - Ciò impone due tipi di problemi:
 - Problema del *nodo nascosto* (*Hidden node problem*)
 - Problema del *nodo esposto* (*Exposed node problem*)

25

WLAN/802.11: il CSMA/CA in funzione

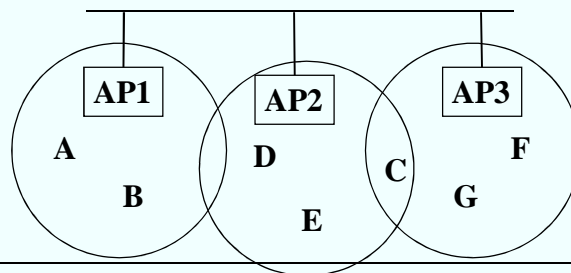


26

WLAN/802.11: Distribution system (1/4)



- Per fornire il supporto alla mobilità e la connessione ad altre reti (prima tra tutte, la rete Internet), si utilizzano dei nodi speciali:
 - Access Point (AP):
 - Si tratta di nodi connessi ad un'infrastruttura di rete fissa, chiamata *Distribution System*

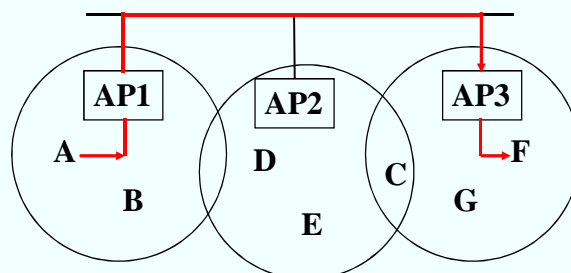


27

WLAN/802.11: Distribution system (2/4)



- Ogni nodo si associa ad un particolare *access point*
- Se A vuole comunicare con F:
 - A invia una frame al suo access point (AP1)
 - AP1 inoltra ad AP3 la frame attraverso il *distribution system*
 - AP3 trasmette la frame ad F



28

WLAN/802.11: Distribution system (3/4)



- La tecnica per selezionare un Access Point è detta *scanning* e prevede quattro passi:
 1. Il nodo invia una frame di *probe*
 2. Tutti gli AP alla portata del nodo rispondono con una frame di *risposta al probe*
 3. Il nodo seleziona uno degli AP (tipicamente quello con la migliore qualità del segnale ricevuto), e gli invia una frame di *richiesta di associazione*
 4. L'AP selezionato risponde con una frame di *conferma di associazione*

29

WLAN/802.11: Distribution system (4/4)



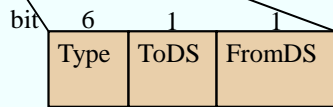
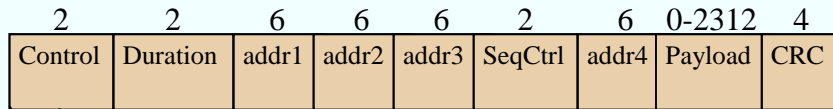
- Il protocollo descritto è utilizzato:
 - Quando il nodo si unisce alla rete
 - Quando il nodo diventa "scontento" dell'attuale AP utilizzato
 - Questo avviene, per esempio, perché il segnale ricevuto da tale AP risulta indebolito a causa del fatto che il nodo si sta allontanando da esso
- Durante lo spostamento, un nodo potrebbe preferire un nuovo AP ed inviargli una richiesta di associazione:
 - Il nuovo AP invia una notifica del cambiamento al vecchio AP, attraverso il *distribution system*

30

WLAN/802.11: framing



Domanda: perché ci sono 4 campi indirizzo?

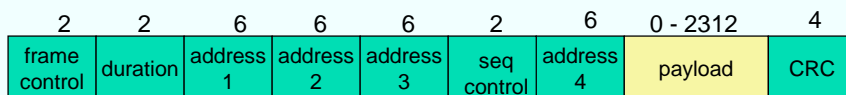


• Type:

- Data
- RTS frame
- CTS frame
- Used by scanning algorithm

31

802.11 frame: addressing



Address 1: MAC address of wireless host or AP to receive this frame

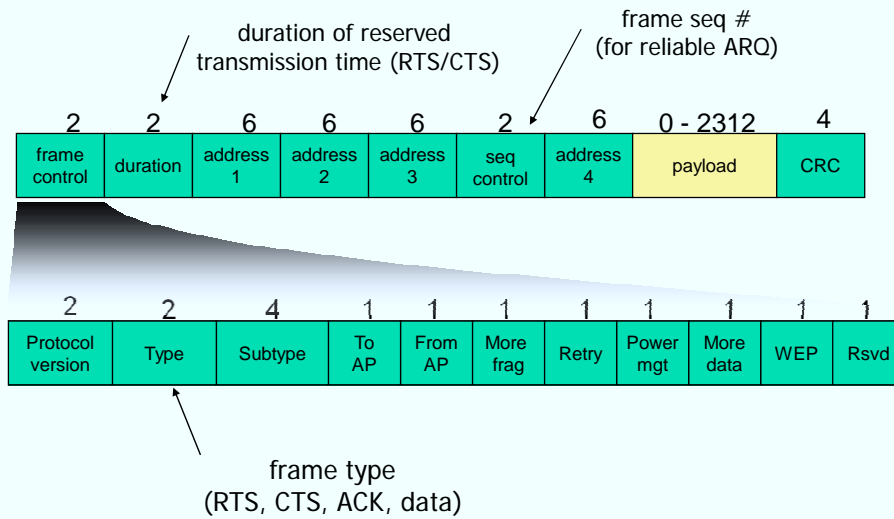
Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

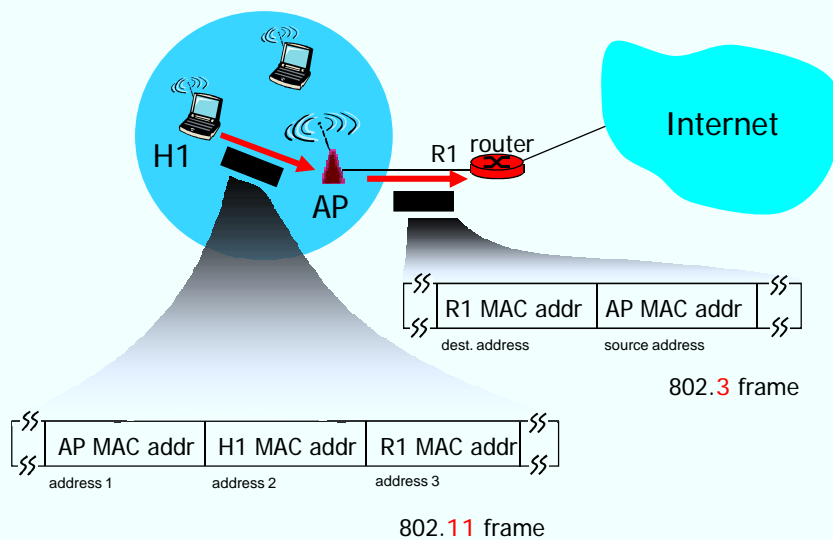
Address 4: used only within infrastructure

32

802.11 frame: more



802.11 frame: addressing



I valori degli indirizzi



| scenario | to DS | from DS | address 1 | address 2 | address 3 | address 4 |
|-----------------------------------|-------|---------|-----------|-----------|-----------|-----------|
| ad-hoc network | 0 | 0 | DA | SA | BSSID | - |
| infrastructure network, from AP | 0 | 1 | DA | BSSID | SA | - |
| infrastructure network, to AP | 1 | 0 | BSSID | SA | DA | - |
| infrastructure network, within DS | 1 | 1 | RA | TA | DA | SA |

- SA = Source Address
- DA = Destination Address
- BSSID = Indirizzo dell'AP
- TA = Transmitter Address
- RA = Receiver Address