Corso di Laurea in Ingegneria Informatica

Corso di Reti di Calcolatori
(a.a. 2011/12)

Roberto Canonico (roberto.canonico@unina.it)
Giorgio Ventre (giorgio.ventre@unina.it)

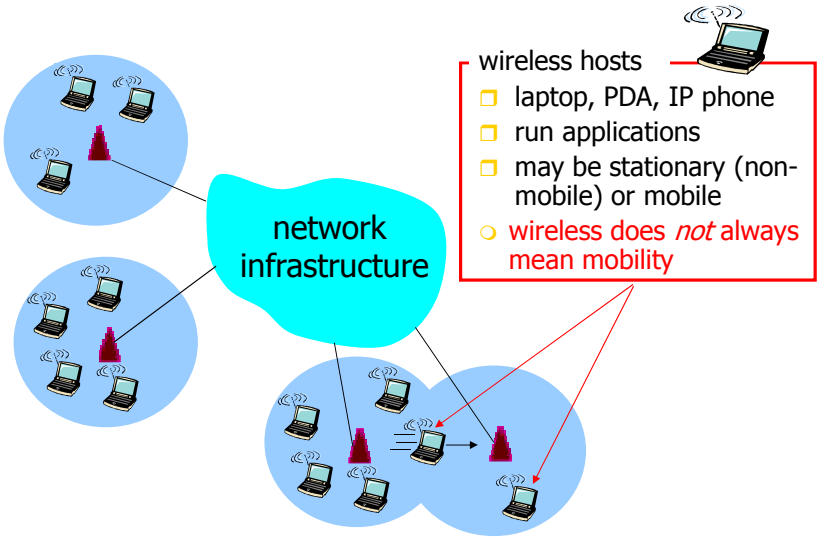
Reti wireless

5 dicembre 2011

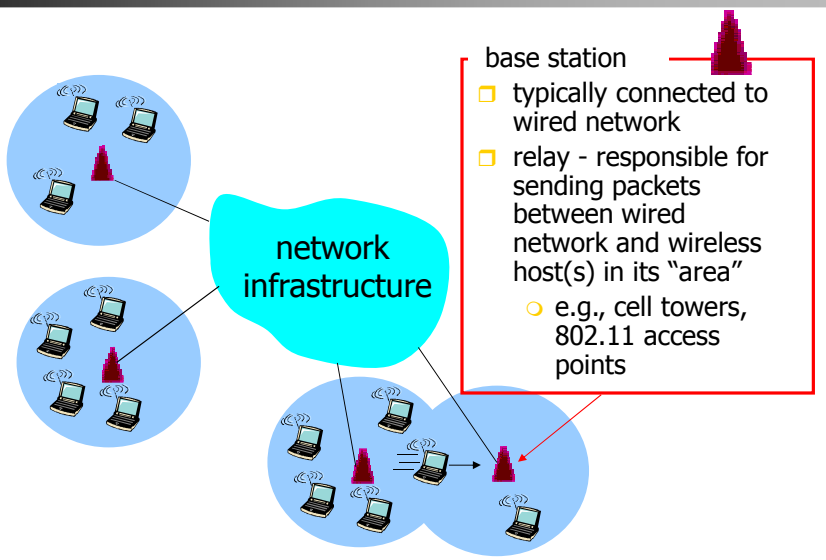
I lucidi presentati al corso sono uno strumento didattico
che NON sostituisce i testi indicati nel programma del corso
I lucidi sono adattati dagli originali di J. Kurose e K. Ross e fanno riferimento al testo
Reti di calcolatori e Internet - Un approccio top-down (4a ed.)

Nota di copyright per le slide COMICS

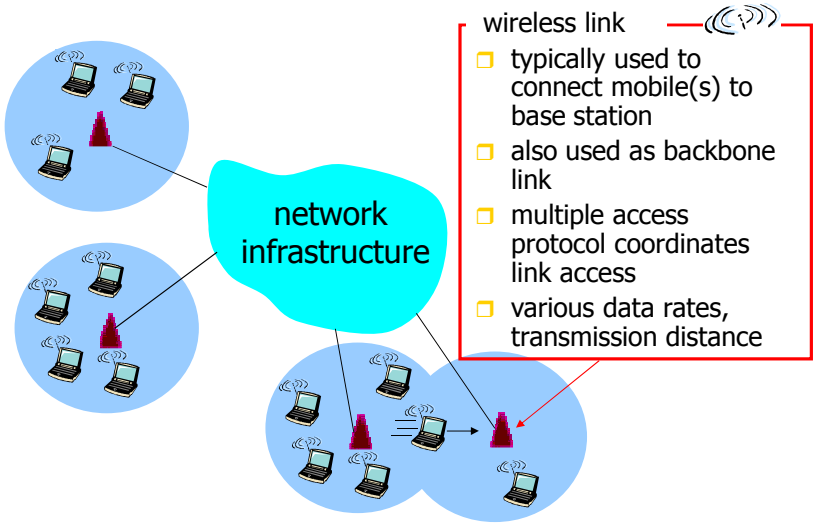
Elements of a wireless network



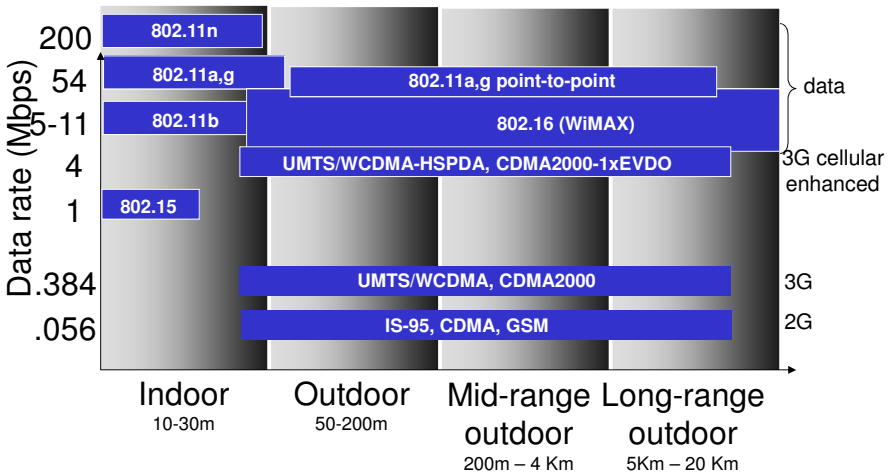
Elements of a wireless network



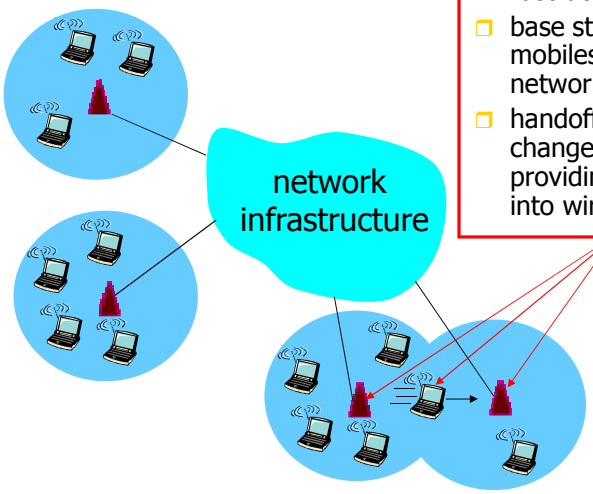
Elements of a wireless network



Characteristics of selected wireless link standards



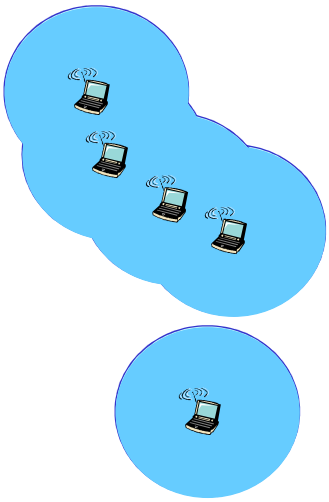
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics

Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

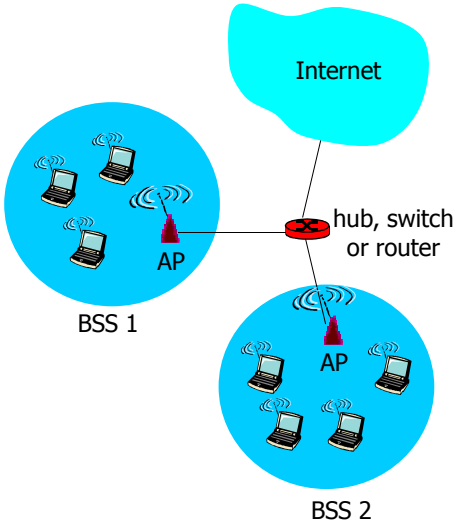
…. make communication across (even a point to point) wireless link much more “difficult”

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)

11

802.11 LAN architecture



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

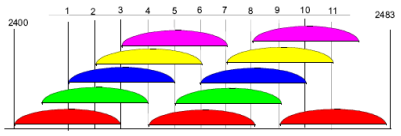
WLAN/802.11: livello fisico

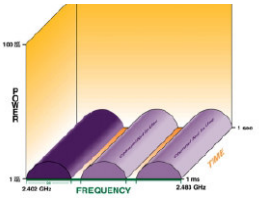
- 802.11 è progettato per trasmettere dati usando tre tecniche differenti:
  - *frequency hopping*
  - *direct sequence*
  - *diffused infrared*
- Le prime due tecniche sfruttano il range di frequenza intorno ai 2.4 GHz e sono tecniche del tipo *"spread spectrum":*
  - L'obiettivo di tali tecniche è 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

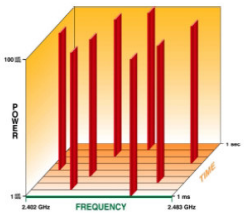
13

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

14

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

15

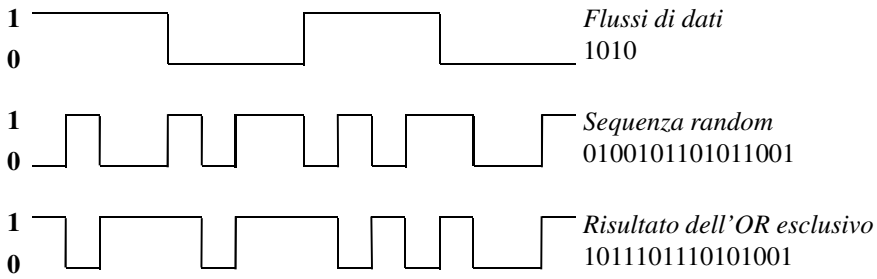
WLAN/802.11: direct sequence

- 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

16

WLAN/802.11: direct sequence

- Un esempio: chipping sequence a 4 bit



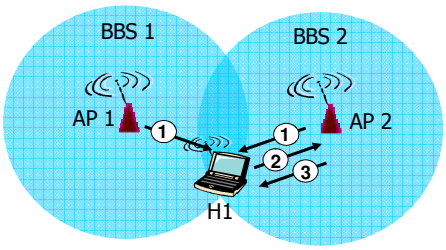
17

802.11: Canali ed associazione ad un Access Point

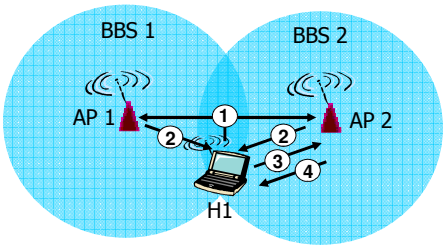
- 802.11b: 2.4GHz-2.485GHz
  - Lo spettro è diviso in 11 canali a differenti frequenze
    - Solo 3 canali risultano non sovrapposti
  - All'atto dell'installazione di un AP, l'amministratore di rete sceglie il canale da utilizzare per la trasmissione
  - Possibilità di interferenza nel caso in cui due 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

18

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

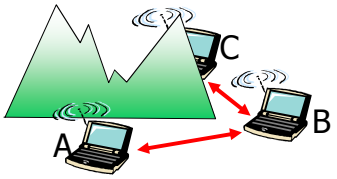
WLAN/802.11: Medium Access Control

- 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 determina due tipi di problemi:
    - Problema del *nodo nascosto (Hidden node problem)*
    - Problema del *nodo esposto (Exposed node problem)*

20

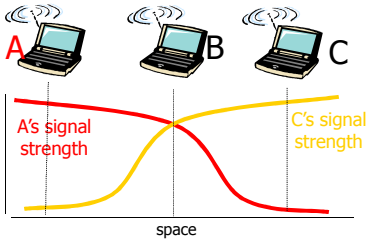
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B

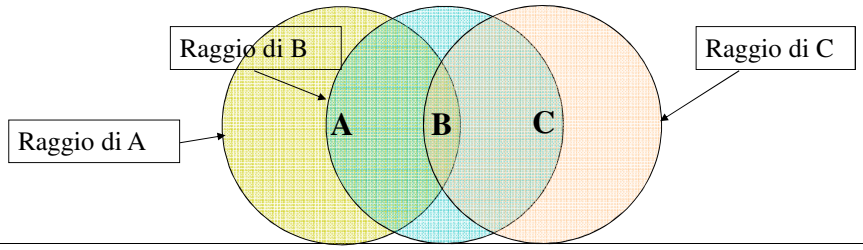


Signal attenuation:
- B, A hear each other
- B, C hear each other
- A, C can not hear each other

interfering at B

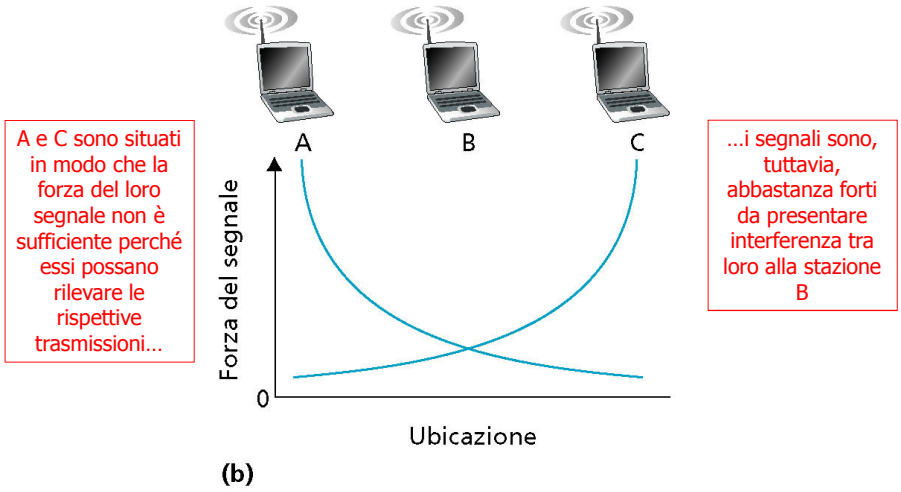
WLAN/802.11: Hidden nodes problem

- 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 *nodi nascosti* (l'uno rispetto all'altro)



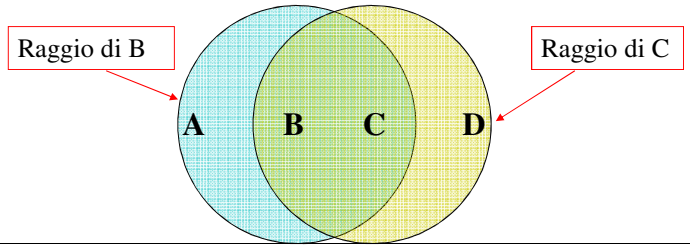
22

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



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



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
- Obiettivo: *evitare le collisioni:* CSMA/C(ollision)A(voidance)

25

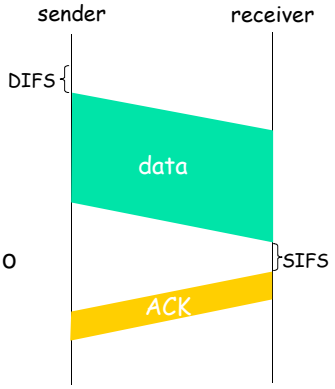
Protocollo CSMA/CA

802.11 sender

- se il canale è inattivo per un tempo pari a **DIFS** (Distributed Inter Frame Space) allora
  - Trasmette un'intera frame (senza CD)
- 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

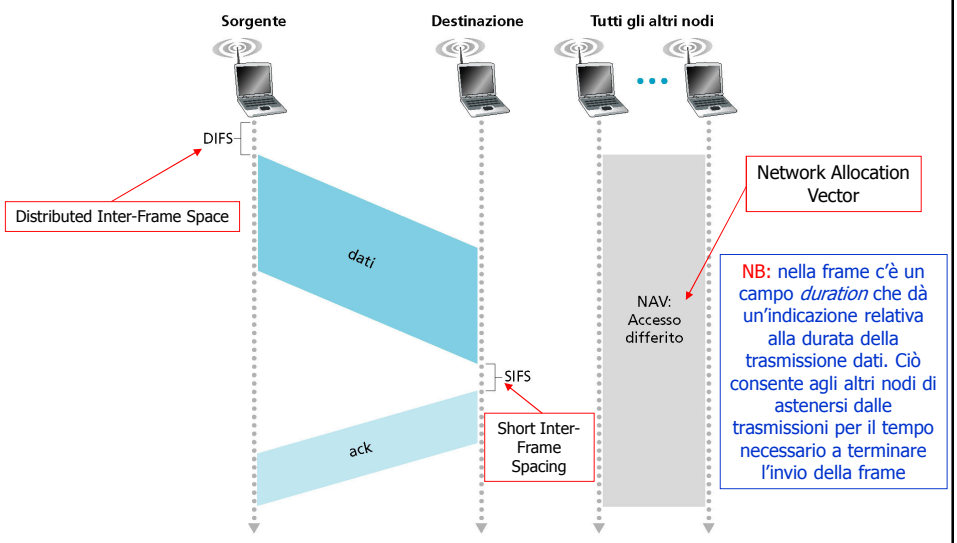
802.11 receiver

- se la frame è ricevuta in maniera corretta
  - restituisce un ACK dopo un tempo **SIFS** (Short Inter Frame Space)



26

WLAN/802.11: gestione dell'accesso

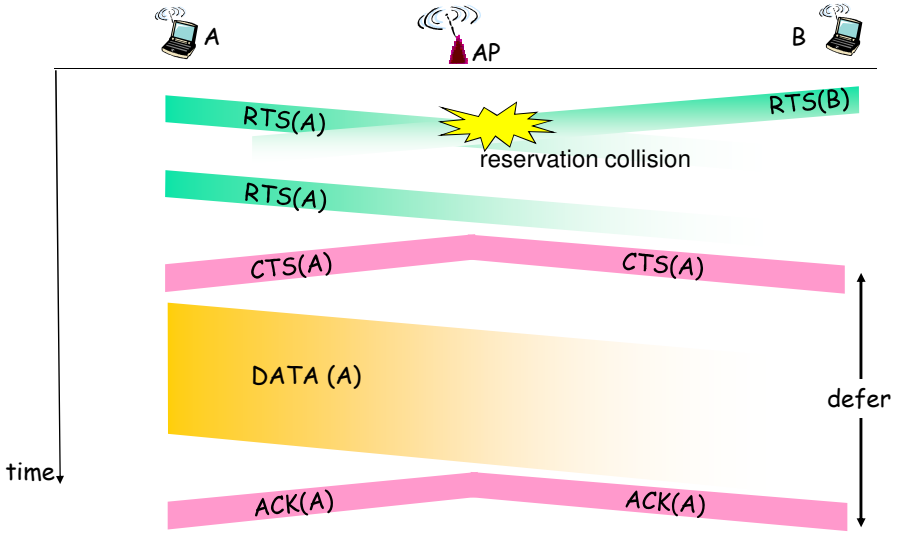


Collision Avoidance: RTS/CTS

- *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) all'AP, usando il CSMA
  - 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

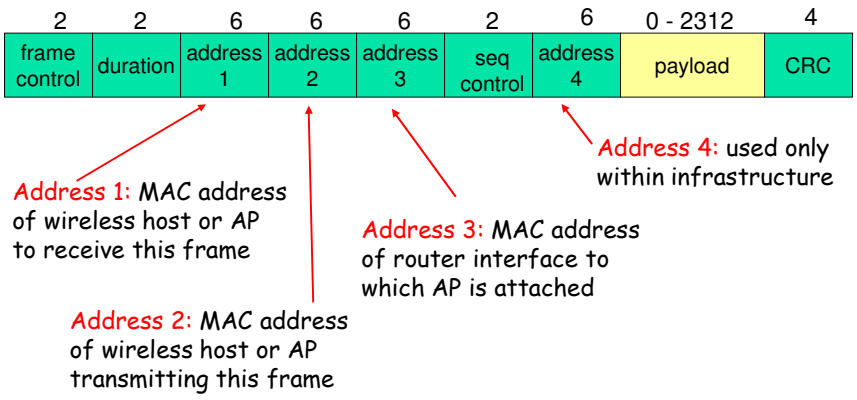
Si evitano completamente le collisioni sui dati, usando piccoli pacchetti di prenotazione!

Collision Avoidance: RTS-CTS exchange



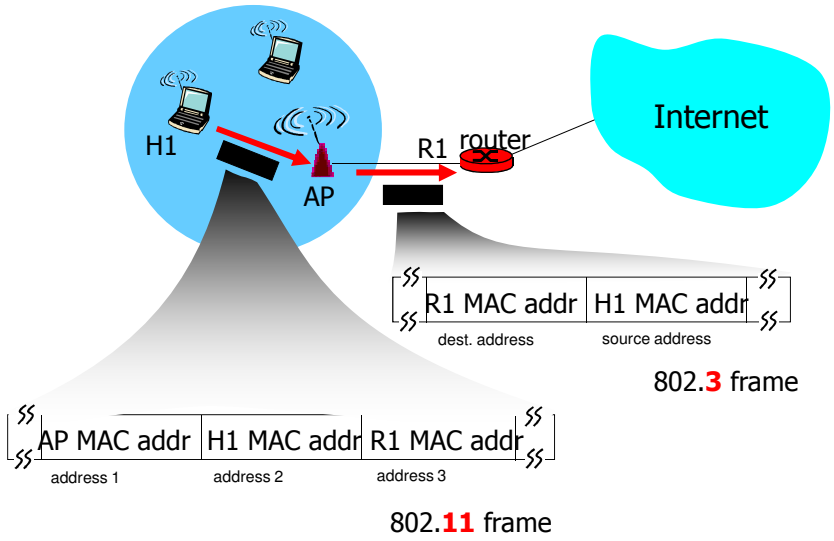
29

802.11 frame: addressing

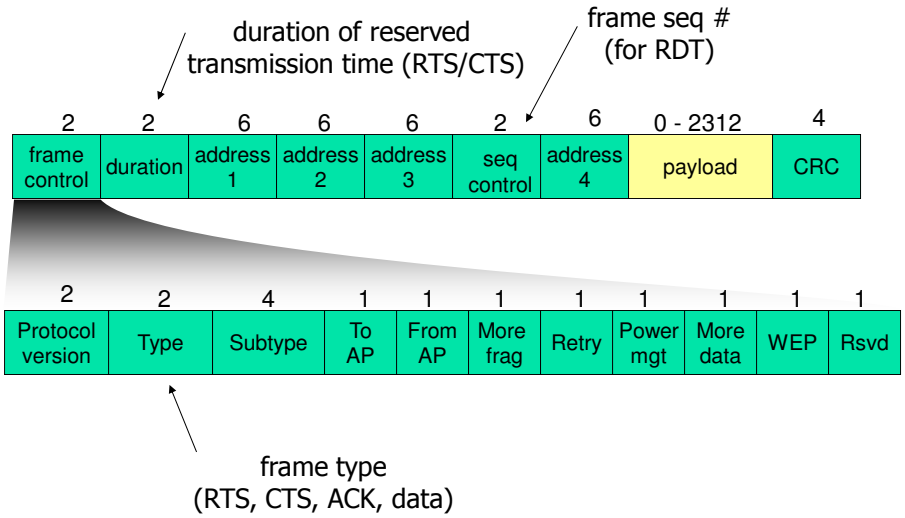


30

802.11 frame: addressing



802.11 frame: altri dettagli



WLAN/802.11: collision avoidance (1/2)

- Lo standard 802.11 risolve i due problemi precedenti introducendo l'algoritmo CSMA/CA visto in precedenza
- 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

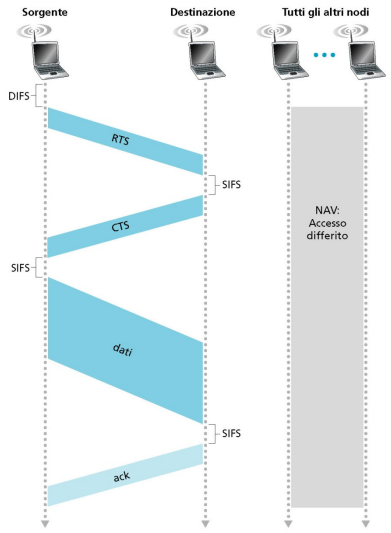
33

WLAN/802.11: 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

34

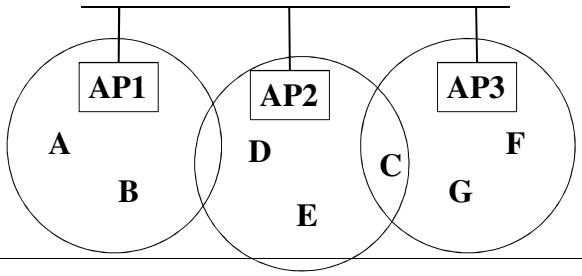
WLAN/802.11: il CSMA/CA in funzione



35

WLAN/802.11: Distribution system (1/4)

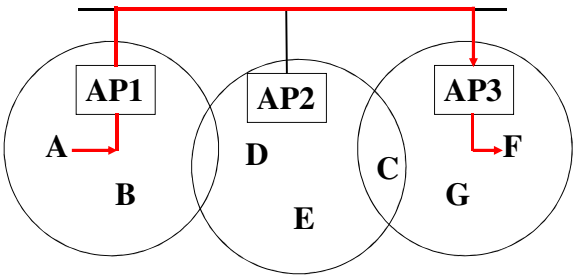
- Per fornire il supporto alla mobilità e la connessione ad altre reti (prima tra tutte, la rete Internet), si utilizzano dei nodi speciali:
  - Access Point (AP):
    - Si tratta di nodi connessi ad un'infrastruttura di rete fissa, chiamata *Distribution System*



36

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



37

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*

38

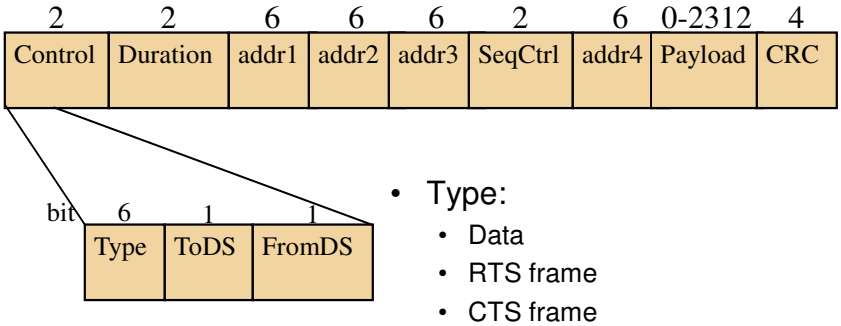
WLAN/802.11: Distribution system (4/4)

- 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*

39

WLAN/802.11: framing

Domanda: perché ci sono 4 campi indirizzo?



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

40

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

41

IEEE 802.11 security

- *war-driving:* drive around Bay area, see what 802.11 networks available?
  - More than 9000 accessible from public roadways
  - 85% use no encryption/authentication
  - packet-sniffing and various attacks easy!
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - current attempt: 802.11i

Wired Equivalent Privacy (WEP):

- authentication as in protocol *ap4.0*
  - host requests authentication from access point
  - access point sends 128 bit nonce
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- no key distribution mechanism
- authentication: knowing the shared key is enough

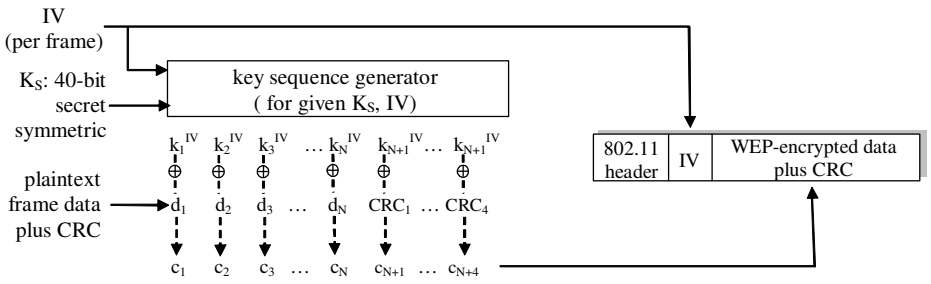
WEP data encryption

- host/AP share 40 bit symmetric key (semi-permanent)
- host appends 24-bit initialization vector (IV) to create 64-bit key
- 64 bit key used to generate stream of keys, k_i^{IV}
- k_i^{IV} used to encrypt ith byte, d_i, in frame:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

802.11 WEP encryption



Sender-side WEP encryption

Breaking 802.11 WEP encryption

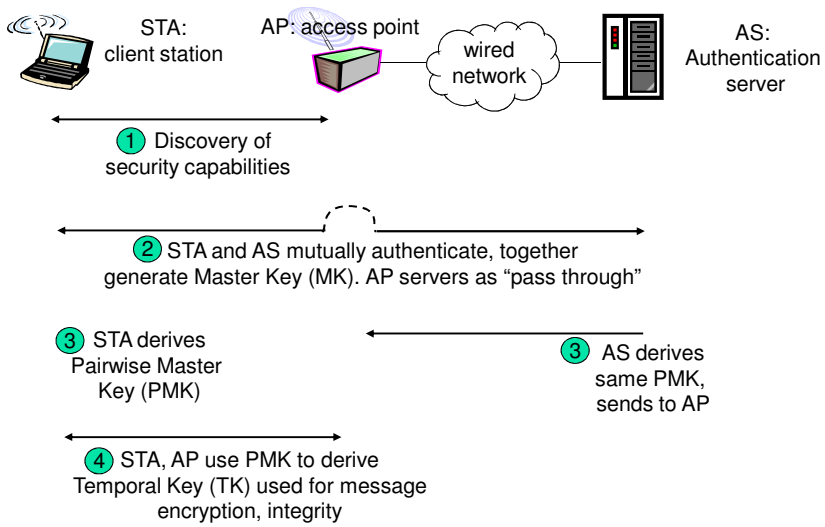
security hole:

- 24-bit IV, one IV per frame, -> IV's eventually reused
- IV transmitted in plaintext -> IV reuse detected
- attack:
  - Trudy causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
  - Trudy sees: $c_i = d_i$ XOR k_i^{IV}
  - Trudy knows c_i d_i, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time IV is used, Trudy can decrypt!

802.11i: improved security

- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

802.11i: four phases of operation



EAP: extensible authentication protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate “links”
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)