

Università degli Studi di Roma "Tor Vergata"
Laurea in Informatica

Sistemi Operativi e Reti
(modulo Reti)
a.a. 2024/2025

Wireless e Reti Mobili (parte1)

dr. Manuel Fiorelli

manuel.fiorelli@uniroma2.it

<https://art.uniroma2.it/fiorelli>

Basate sulle slide del libro di testo:

https://gaia.cs.umass.edu/kurose_ross/ppt.php

Introduction: 1-1

Wireless e reti mobili: contesto

- più abbonati alla telefonia wireless (mobile) che alla telefonia fissa (via cavo) (10 a 1 nel 2019)!
- più dispositivi connessi alla banda larga mobile che dispositivi connessi alla banda larga fissa (5 a 1 nel 2019)!
 - le reti cellulari 4G/5G abbracciano ora lo stack di protocolli Internet, compreso SDN
- due sfide importanti (ma diverse)
 - **wireless:** comunicazione su collegamento wireless
 - **mobilità:** gestione dell'utente mobile che cambia punto di aggancio alla rete

Sommario

■ Introduzione

Wireless

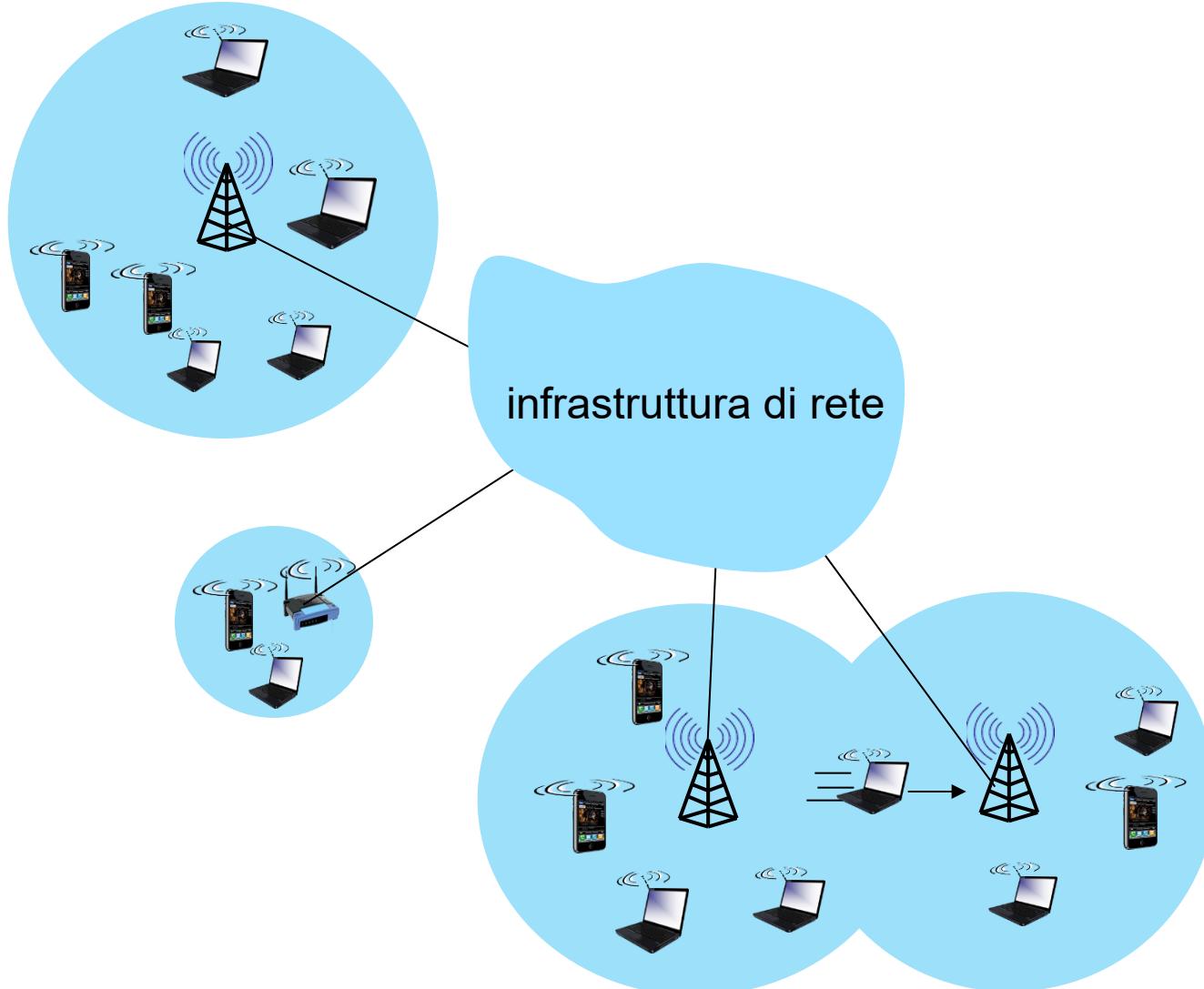
- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth

Mobilità

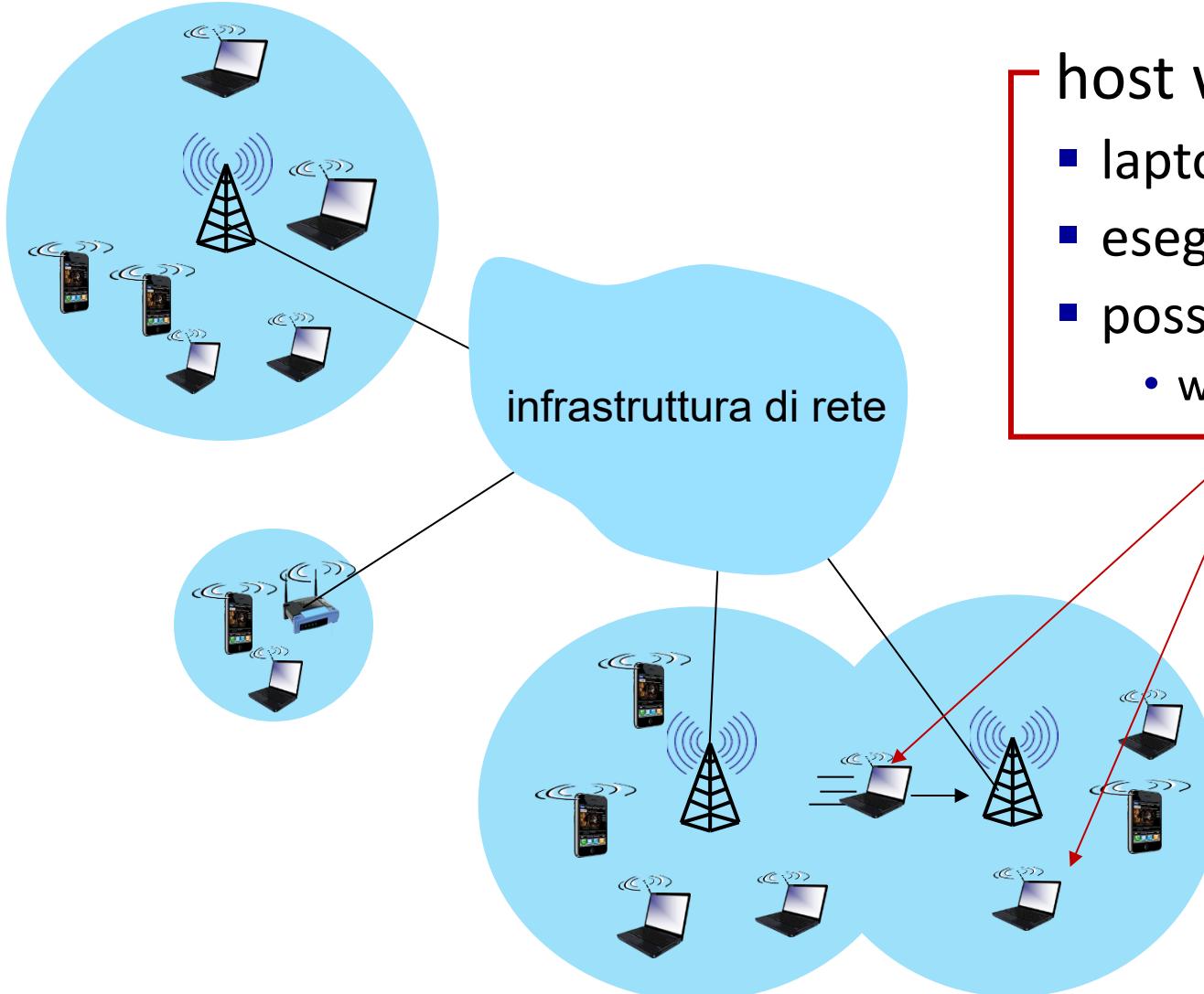
- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore



Componenti di una rete wireless



Componenti di una rete wireless

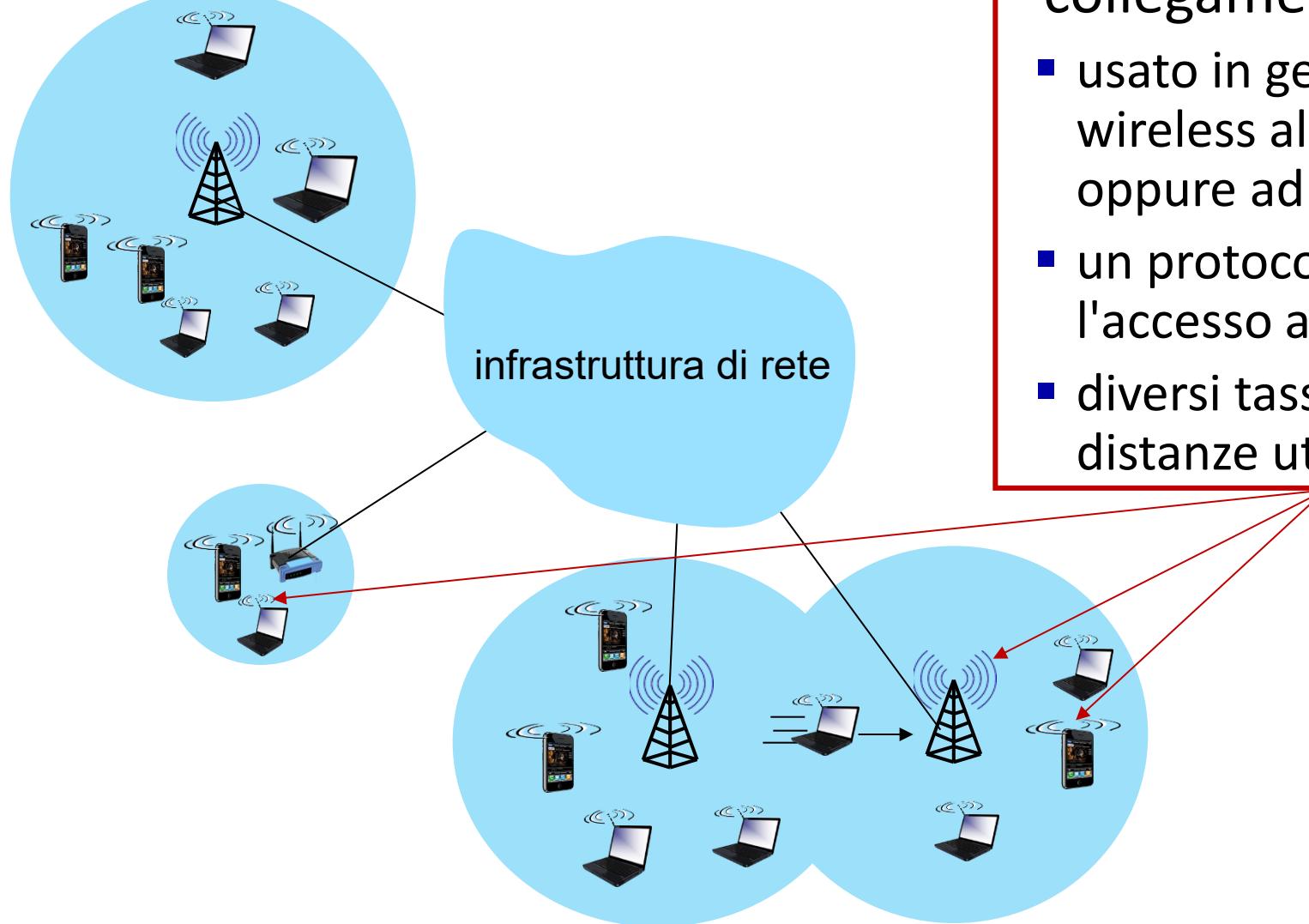


host wireless

- laptop, smartphone, IoT
- eseguono le applicazioni
- possono essere fissi (stazionari) o mobili
 - wireless *non* significa necessariamente mobilità!



Componenti di una rete wireless

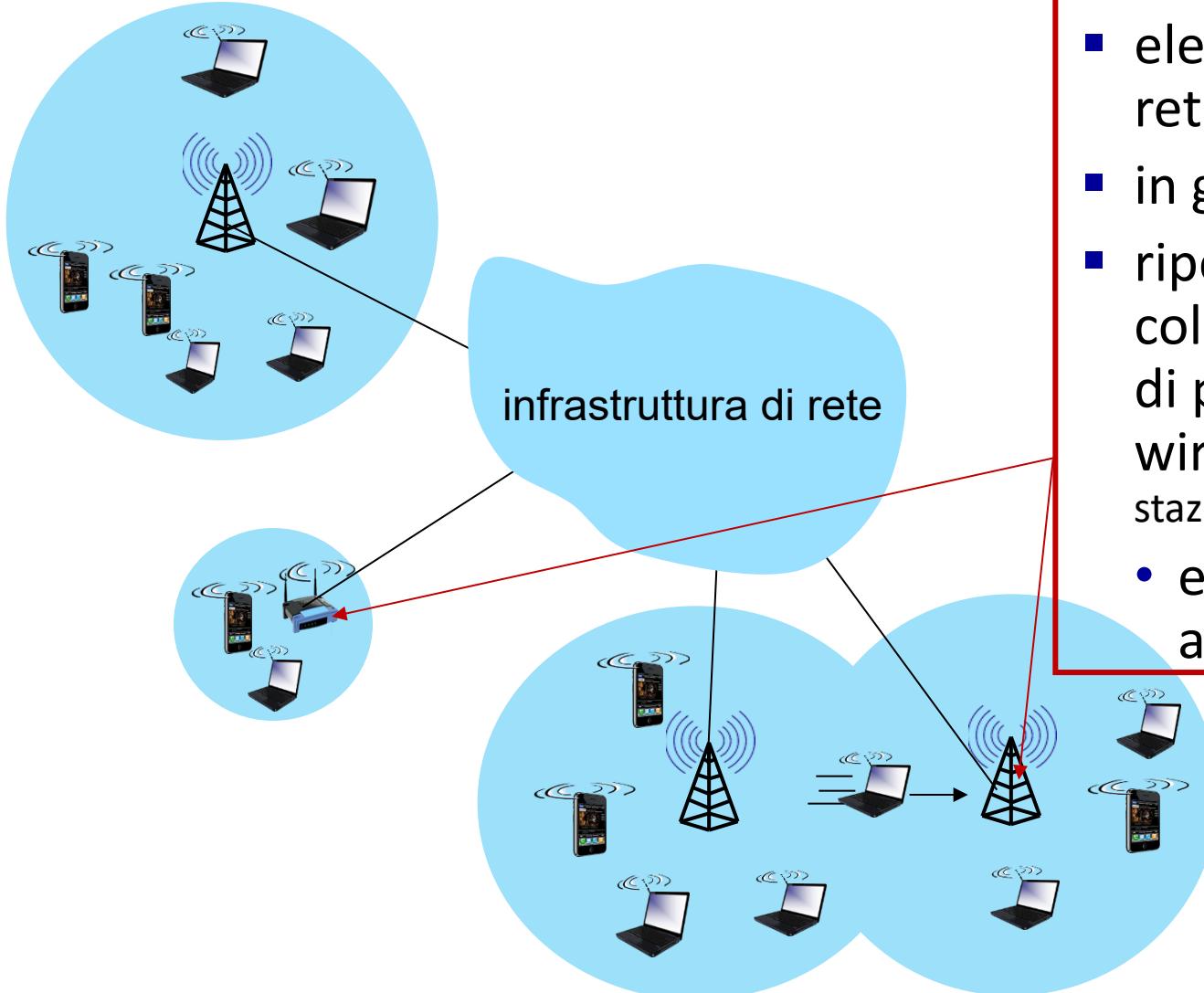


collegamento wireless

- usato in genere per collegare un host wireless alla stazione base (vedi dopo) oppure ad un altro host wireless
- un protocollo ad accesso multiplo regola l'accesso al collegamento
- diversi tassi trasmissivi e massime distanze utile, diverse bande di frequenza



Componenti di una rete wireless

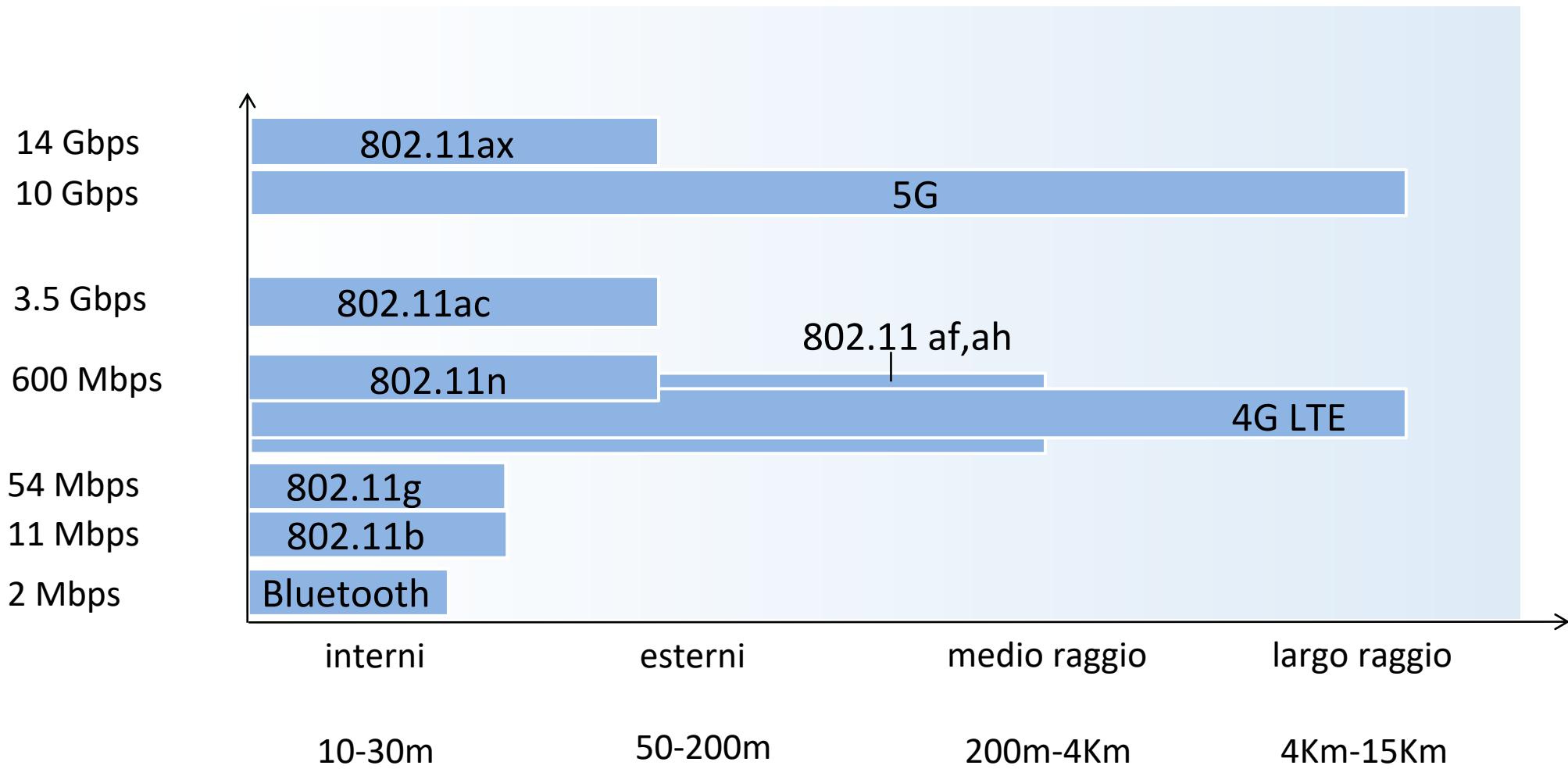


stazione base

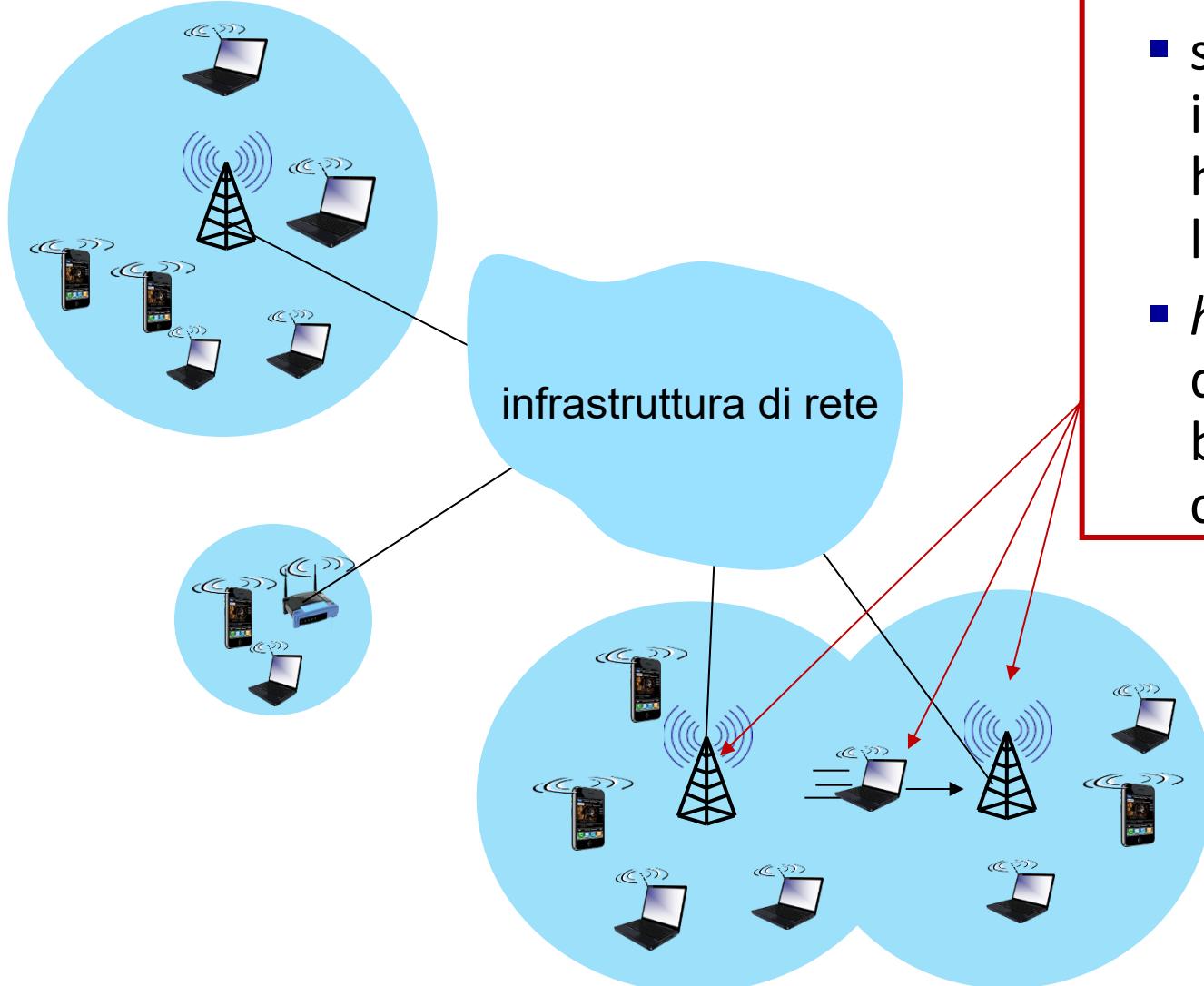


- elemento chiave dell'infrastruttura di rete wireless
- in genere connessa a una rete cablata
- ripetitore (*relay*) a livello di collegamento – responsabile dell'invio di pacchetti tra reti cablate e host wireless nella sua "area" (associati alla stazione base)
- es. cell tower nelle reti cellulari, access point nelle LAN 802.11

Caratteristiche dei collegamenti wireless selezionati



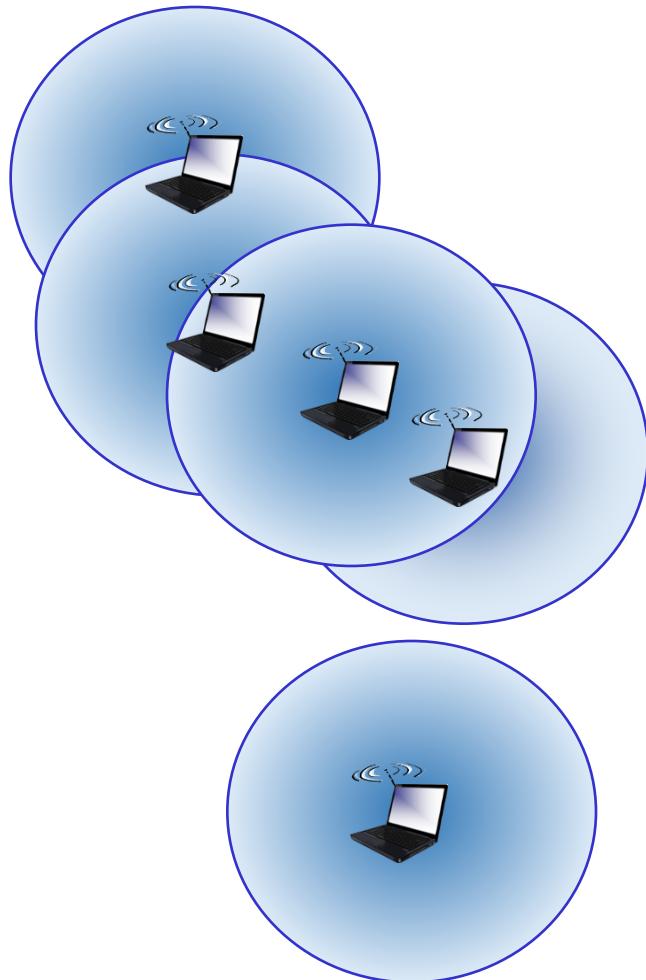
Componenti di una rete wireless



modalità infrastruttura

- servizi di rete (es. indirizzamento, instradamento) forniti dalla rete cui gli host wireless sono connessi attraverso la stazione base
- *handoff*: quando l'host si sposta dall'area di copertura di una stazione base a un'altra cambia il suo punto di collegamento con la rete più ampia

Componenti di una rete wireless



reti ad hoc

- non ci sono stazioni base
- gli host wireless possono trasmettere solo a altri nodi entro la copertura del collegamento
- gli host stessi provvedono ai servizi d'instradamento, di assegnazione degli indirizzi, traduzione dei nomi simil-DNS

Tassonomia delle reti wireless

	hop singolo	hop multipli
infrastruttura (es., stazione base)	I'host si collega a una stazione base, che lo collega al resto della rete: <i>Wi-Fi, rete cellulare</i>	c'è una stazione base collegata al resto della rete. Tuttavia, un host può dover ritrasmettere (<i>relay</i>) la propria comunicazione attraverso altri nodi wireless per comunicare con la stazione base: <i>alcune reti di sensori e Wi-Fi mesh</i>
<i>nessuna infrastruttura</i>	senza stazione base, uno dei nodi può coordinare la trasmissione degli altri: <i>Bluetooth</i>	nessuna stazione base, i pacchetti possono dover essere ritrasmessi attraverso diversi nodi wireless prima di giungere a destinazione: <i>mobile ad hoc networks (MANETs) e vehicular ad hoc network (VANET)</i>

Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth



Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

Caratteristiche dei collegamenti wireless: attenuazione

- le radiazioni elettromagnetiche si attenuano (attenuation) quando attraversano determinati ostacoli (es., a causa dell'assorbimento e della diffusione)
- anche nello spazio libero l'intensità del segnale si attenua al crescere della distanza percorsa, per effetto della *dispersione* del segnale: attenuazione di spazio libero (*free space path loss*)

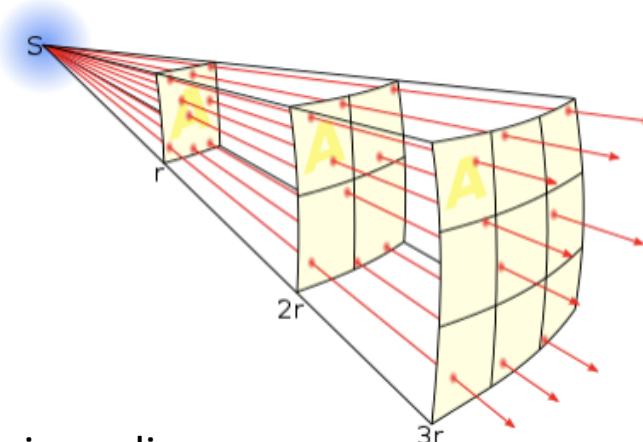
attenuazione di spazio libero $\sim (fd)^2$

f : frequenza

d : distanza

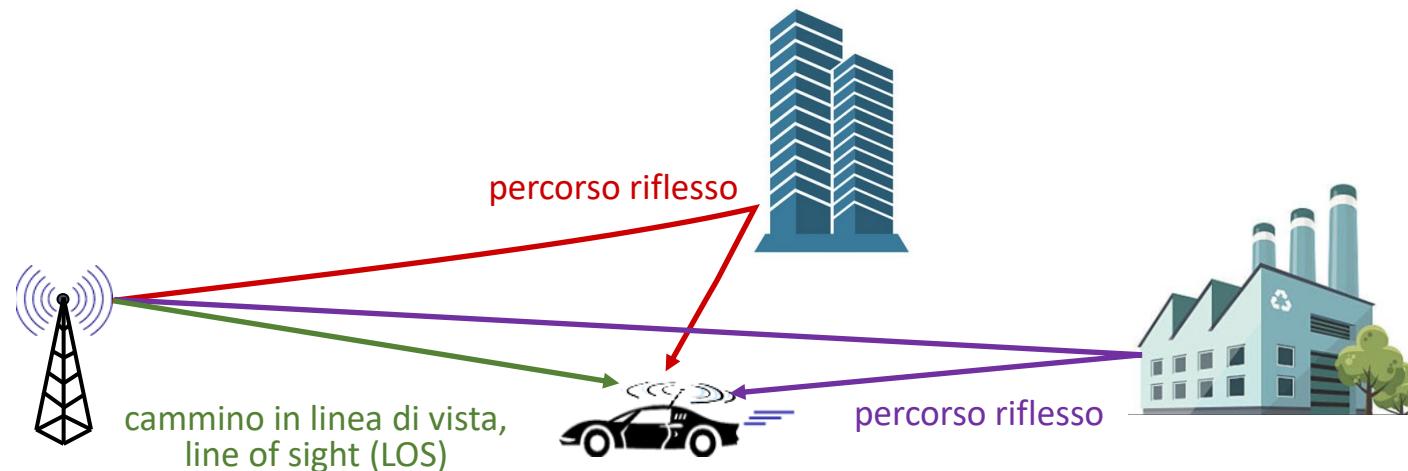
frequenza più alta o
distanza maggiore

maggior attenuazione di
spazio libero



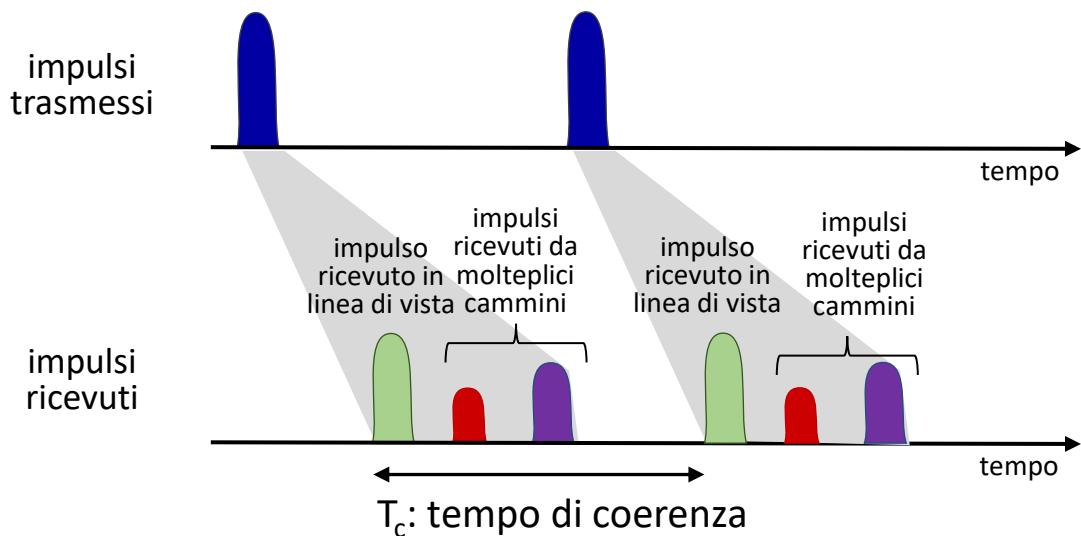
Caratteristiche dei collegamenti wireless: propagazione su più cammini

Propagazione su più cammini (multipath propagation): una parte del segnale si riflette su oggetti e sul terreno, giungendo a destinazione attraverso percorsi di lunghezza differente e quindi arrivando in momenti leggermente differenti.



Caratteristiche dei collegamenti wireless: propagazione su più cammini

Propagazione su più cammini (multipath propagation): una parte del segnale si riflette su oggetti e sul terreno, arrivando a destinazione in momenti leggermente diversi



Tempo di coerenza

- quantità di tempo in cui il bit è presente nel canale per essere ricevuto
- influenza la massima velocità di trasmissione possibile, poiché i tempi di coerenza non possono sovrapporsi

Caratteristiche dei collegamenti wireless: interferenze da parte di altre sorgenti

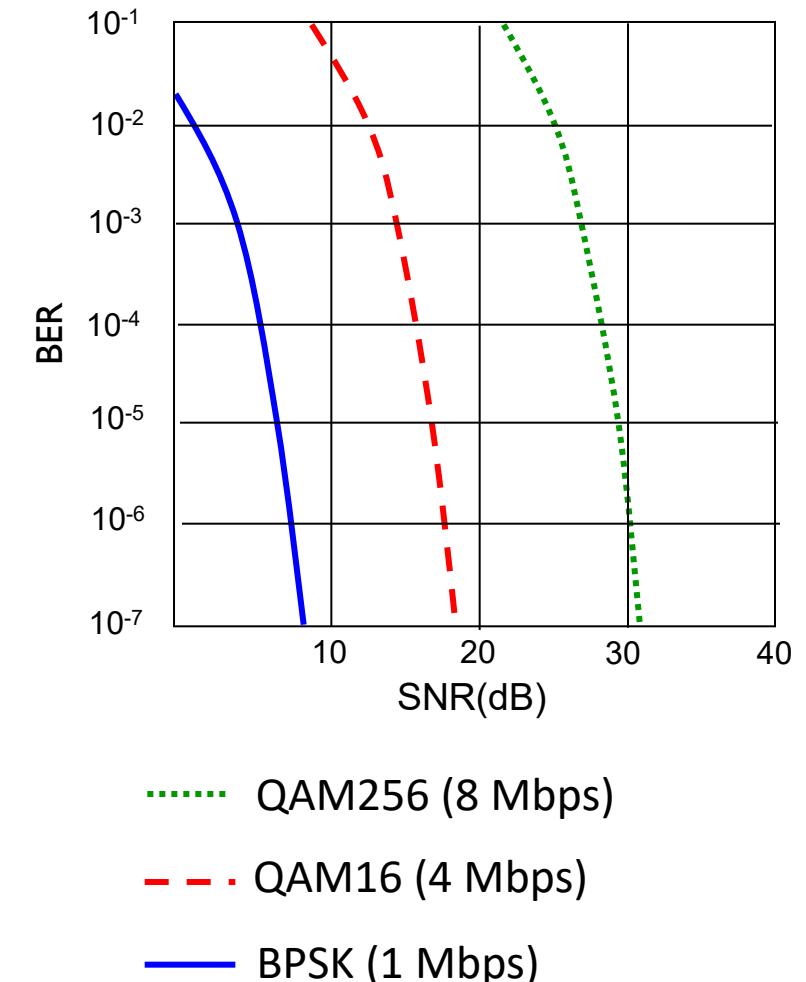
- frequenze wireless standard (es. 2,4 GHz usata da Wi-Fi e Bluetooth) condivise da altri dispositivi (es. telefoni cordless)
- rumore elettromagnetico ambientale (es. prodotto da motori, forni a microonde)
- per evitare queste interferenze, standard 802.11 recenti usando banda 5 GHz

Caratteristiche dei collegamenti wireless: interferenze da parte di altre sorgenti

- **rapporto segnale-rumore (signal-to-noise ratio, SNR)**
 - un SNR più grande facilita il ricevente nell'estrazione del segnale trasmesso (ma ricevuto degradato per l'attenuazione e i cammini molteplici) dal rumore di fondo
- **tasso di errore sui bit (Bit error rate, BER)**
 - semplificando: probabilità che un bit sia ricevuto in errore

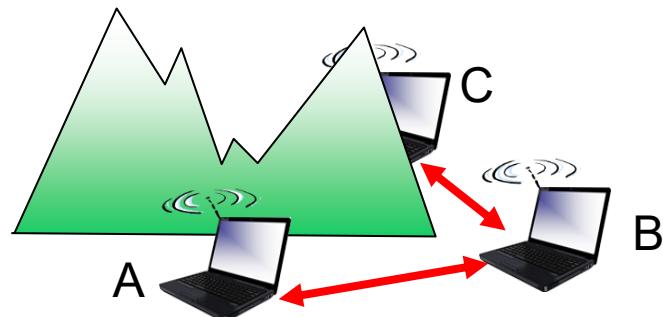
Caratteristiche dei collegamenti wireless: interferenze da parte di altre sorgenti

- Bilanciamento di SNR e BER
 - *per un dato schema di modulazione:* aumentare la potenza -> aumentare lo SRN
-> diminuisce il BER
 - trasmissioni a potenza maggiore implicano un maggiore consumo di energia (critico per dispositivi a batteria) e possono andare a interferire con altre trasmissioni
 - per un dato SNR, una tecnica di modulazione con più elevato tasso di trasmissione dei bit avrà un BER più alto
 - lo SNR può cambiare con la mobilità: adattare dinamicamente il livello fisico (tecnica di modulazione, tasso di trasmissione)



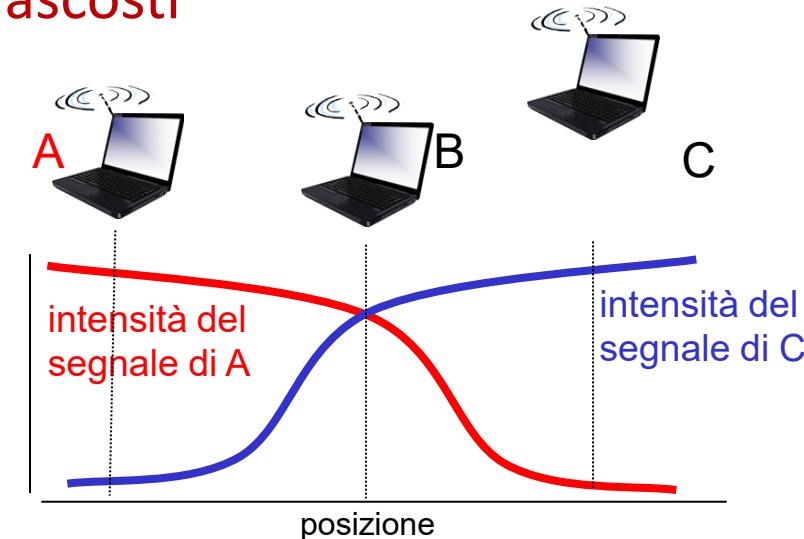
Caratteristiche dei collegamenti wireless: terminali nascosti

Problema del terminale nascosto



- B, A possono comunicare
- B, C possono comunicare
- A, C non possono comunicare tra loro ma possono causare (senza saperlo!) interferenza presso la destinazione B

Anche l'attenuazione causa “terminali nascosti”



- B, A possono comunicare
- B, C possono comunicare
- A, C non possono comunicare ma causano interferenza presso B

Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth



Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

Accesso multiplo a divisione di codice (Code Division Multiple Access, CDMA)

- Un "codice" unico viene assegnato a ciascun utente (*code set partitioning*)
 - tutti gli utenti condividono la stessa frequenza, ma ciascun utente ha una propria sequenza "chipping" (cioè il "codice") per codificare i dati
 - consente a più utenti di "coesistere" e trasmettere simultaneamente con un'interferenza minima (se i codici sono "ortogonali", cioè con prodotto scalare nullo, ovvero $\vec{c}^1 \cdot \vec{c}^2 = 0$)

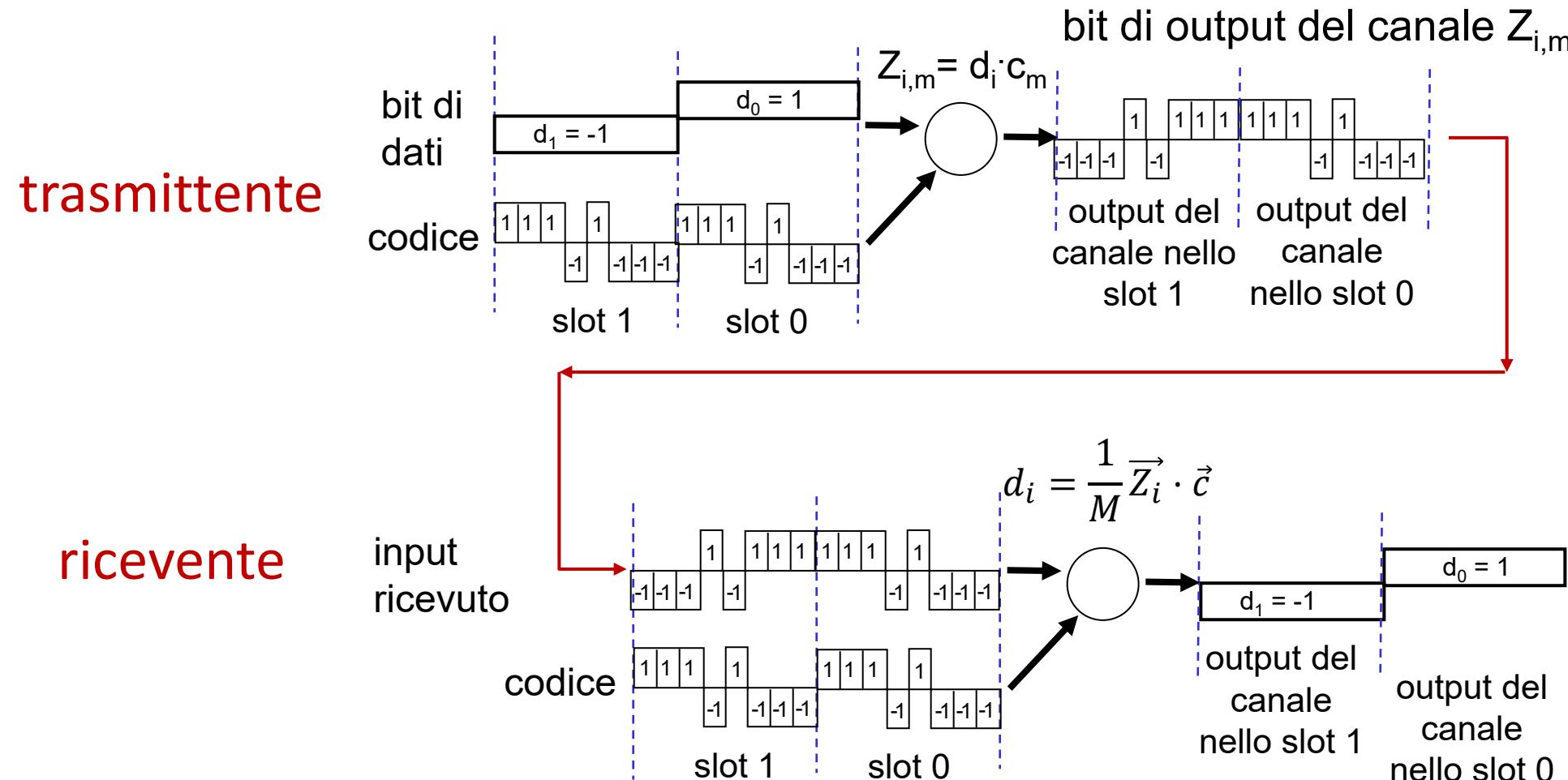
Tratteremo CDMA in maniera "semplificata", facendo una serie di assunzioni:

- rappresentare i bit 0 e 1 rispettivamente con i valori -1 e +1
- segnali provenienti dai diversi mittenti ricevuti con la stessa intensità
- sincronizzazione

Sotto queste assunzioni:

- **codifica:** il bit di dati d_i viene codificato come $d_i \vec{c}$: un singolo bit di dati viene codificato con M bit quanto è lungo il codice. Pertanto, il segnale codificato ha un tasso maggiore del segnale di dati originale.
- **decodifica:** raggruppa i bit ricevuti a M a M, quindi calcola il prodotto scalare tra ciascun gruppo e il codice del mittente di interesse, successivamente diviso per M

CDMA codifica/decodifica

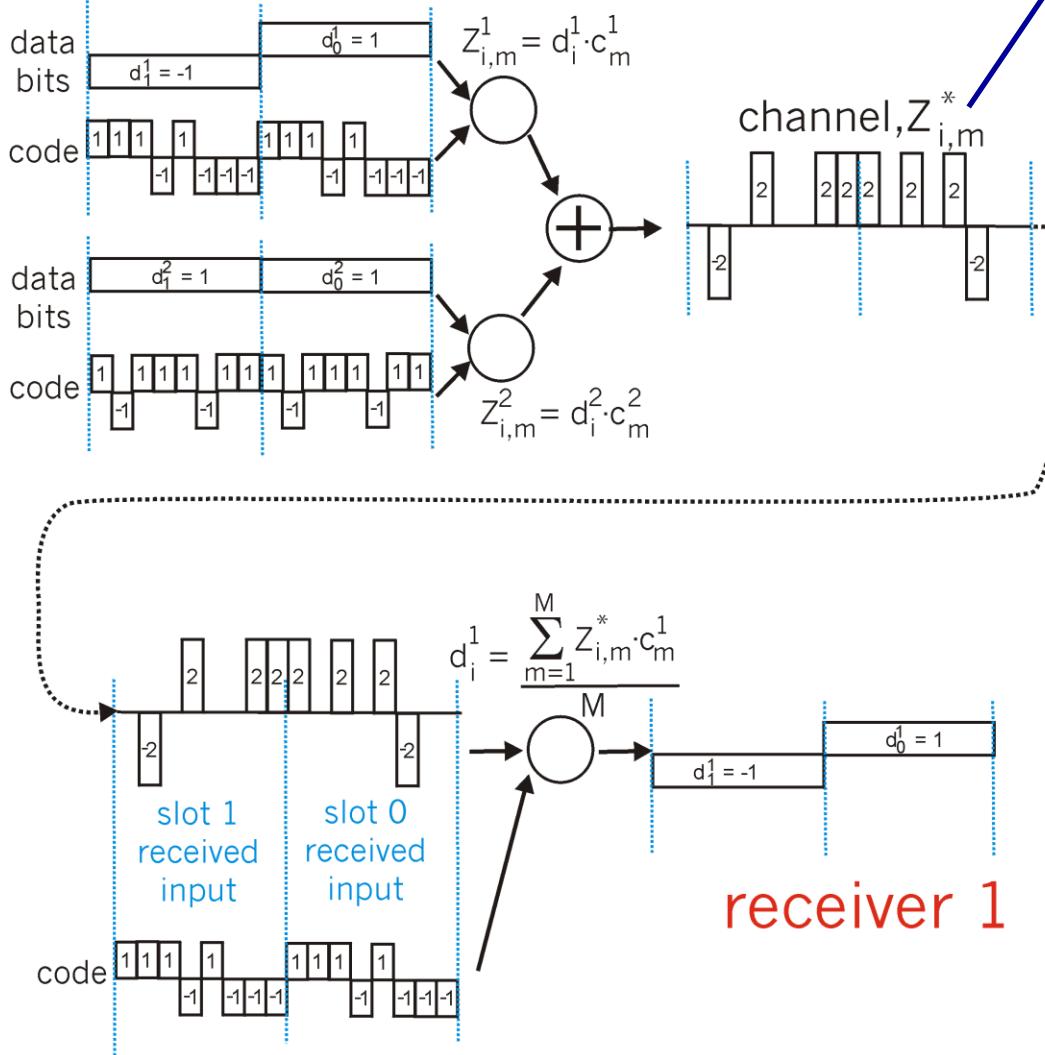


... cosa accade se due nodi trasmettono simultaneamente?

CDMA: due trasmittenti

trasmittente 1

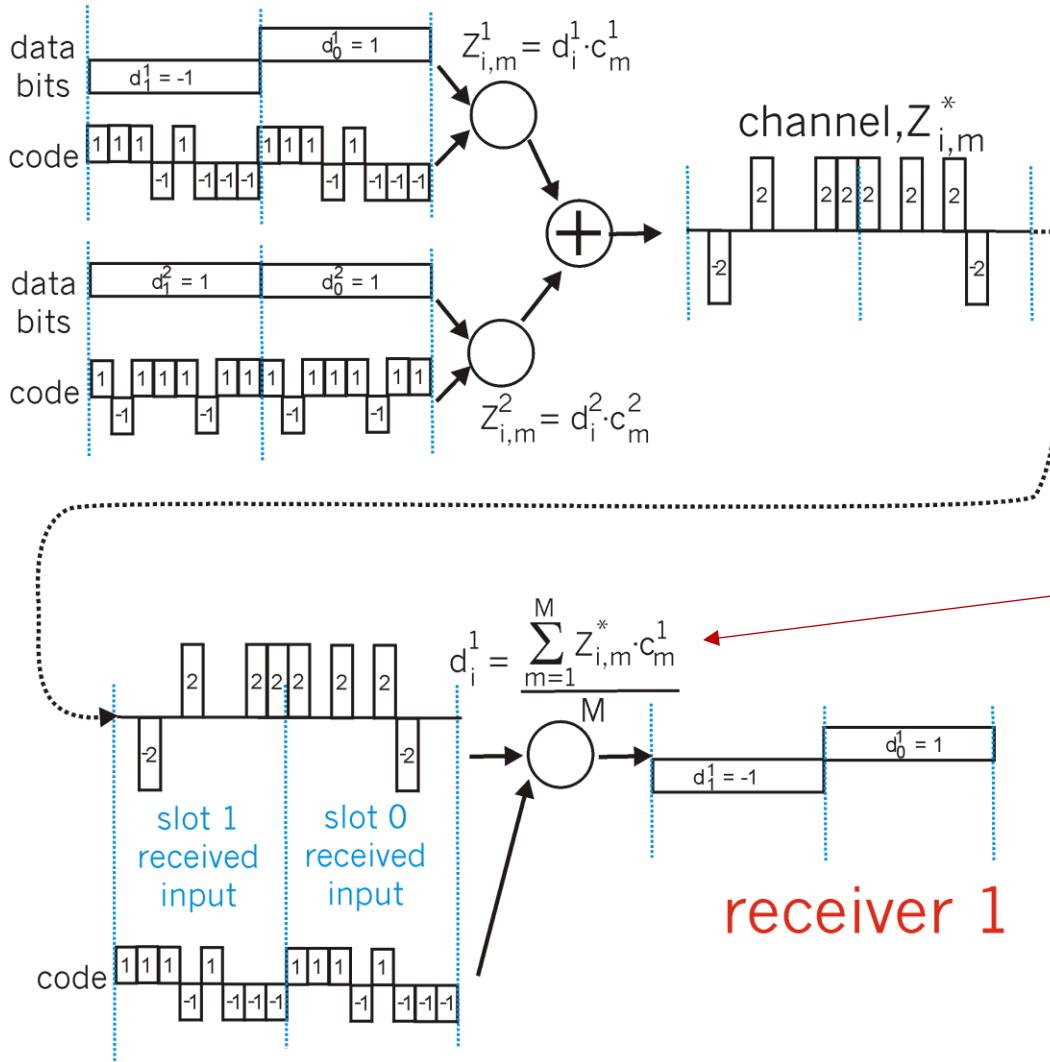
trasmittente 2



CDMA: due trasmittenti

trasmittente 1

trasmittente 2



Perché funziona?

$$\begin{aligned}
 & \frac{1}{M} \vec{Z}_i^* \cdot \vec{c}^1 \\
 &= \frac{1}{M} \left(\left(d_i^1 \cdot \vec{c}^1 \right) + \left(d_i^2 \cdot \vec{c}^2 \right) \right) \cdot \vec{c}^1 \\
 &= \frac{1}{M} \left(\left(d_i^1 \cdot \vec{c}^1 \right) \cdot \vec{c}^1 + \left(d_i^2 \cdot \vec{c}^2 \right) \cdot \vec{c}^1 \right) \\
 &= \frac{1}{M} \left(d_i^1 \cdot \left(\vec{c}^1 \cdot \vec{c}^1 \right) + d_i^2 \cdot \left(\vec{c}^2 \cdot \vec{c}^1 \right) \right) \\
 &= \frac{1}{M} \left(d_i^1 M + d_i^2 0 \right) = d_i^1
 \end{aligned}$$

Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth



Mobilità

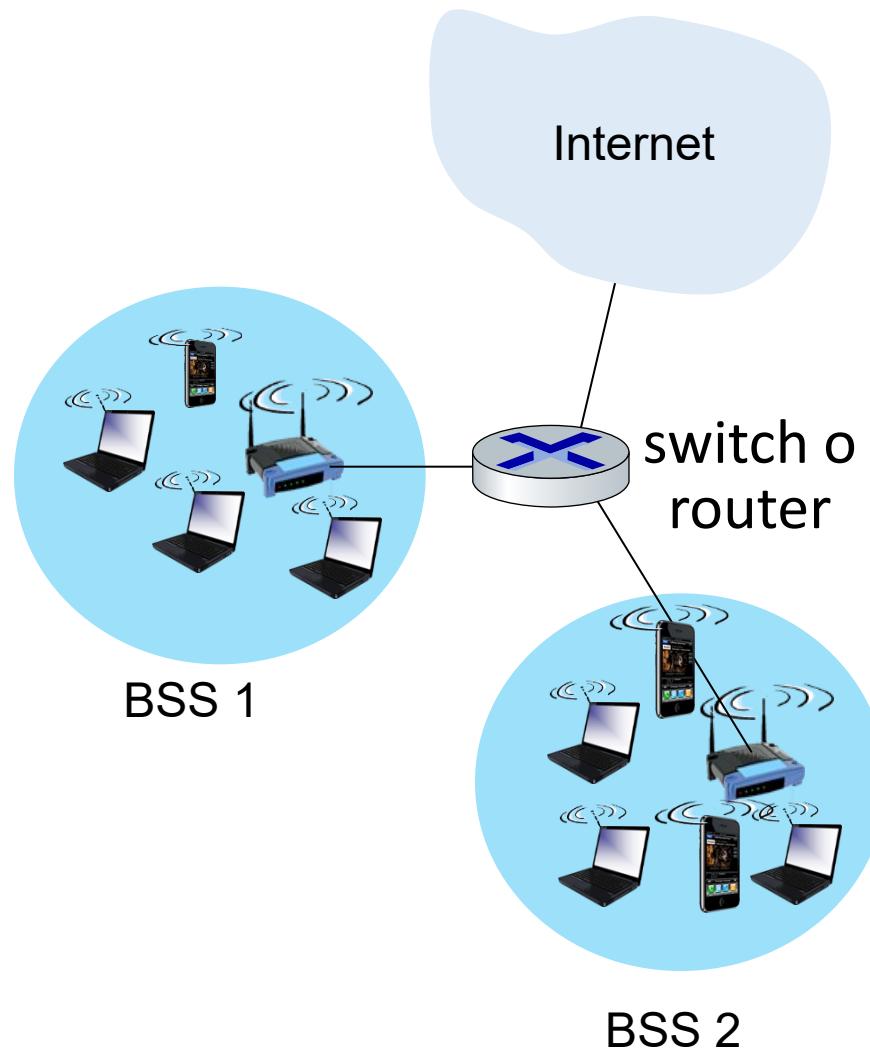
- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Anno	Max data rate	Raggio	Frequenza
802.11b	1999	11 Mbps	30 m	2.4 GHz
802.11g	2003	54 Mbps	30m	2.4 GHz
802.11n (WiFi 4)	2009	600 Mbps	70m	2.4, 5 GHz
802.11ac (WiFi 5)	2013	3.47Gbps	70m	5 GHz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 GHz
802.11af	2014	35 – 560 Mbps	1 Km	Bande televisive inutilizzate (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 MHz

- Tutti usano CSMA/CA per l'accesso multiplo ed hanno versioni con stazione base e rete ad hoc

Architettura delle LAN 802.11

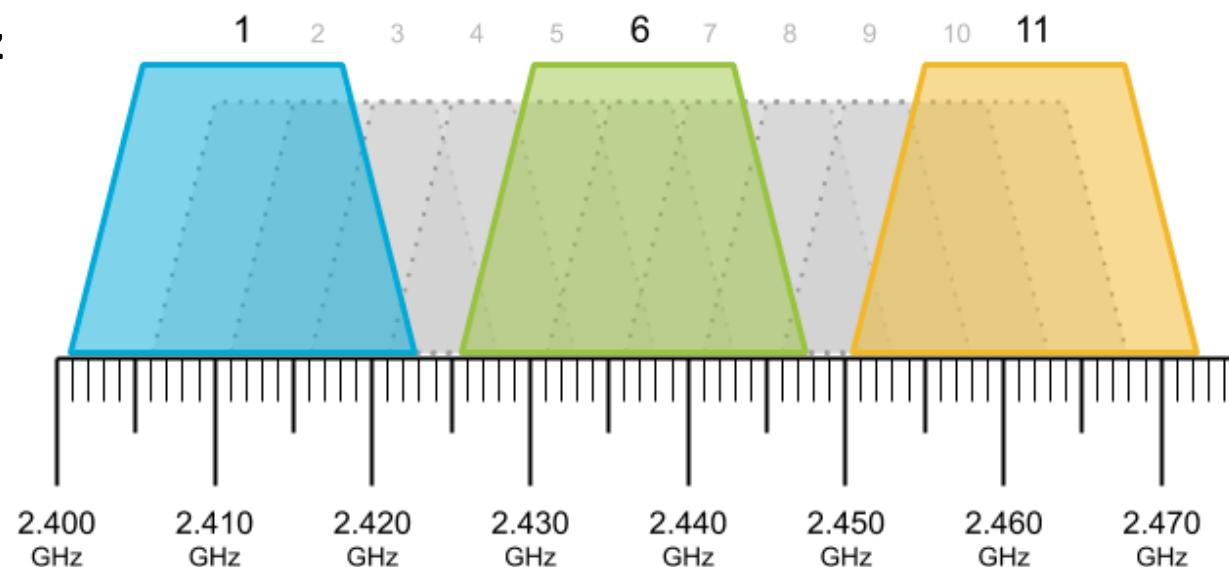


- Gli host wireless comunicano con la stazione base
 - stazione base = punto di accesso, access point (AP)
- **Basic Service Set (BSS)** (detto anche “cella”) in modalità infrastruttura contiene:
 - host wireless
 - punto di accesso (AP): stazione base
 - modalità ad hoc: solo host

802.11: Canali

- spettro **diviso in canali** a frequenze differenti
 - AP admin sceglie le frequenze per il punto di accesso
 - possibili interferenze: il canale può essere lo stesso scelto dall'AP vicino!

Esempio: 2.4 GHz



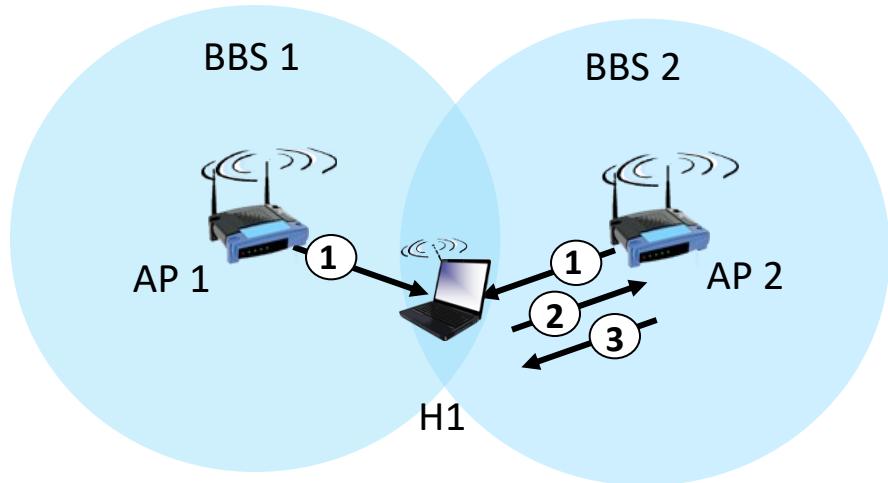
- Canali non sovrapposti: separati da 4 o più canali
- Ne esistono 3
- Possibilità di installare 3 AP nello stesso posto per avere un tasso aggregato pari al triplo del tasso di trasmissione nominale

802.11: Associazione

- host in arrivo: deve essere **associato** con un AP
 - scansiona i canali, in ascolto per i *frame beacon* inviati periodicamente dall'AP e contenenti il nome dell'AP (SSID) e l'indirizzo MAC
 - sceglie l'AP con cui associarsi
 - può autenticarsi
 - quindi tipicamente invia un messaggio di richiesta DHCP nella sottorete attraverso l'AP per ottenere un indirizzo IP nella sottorete

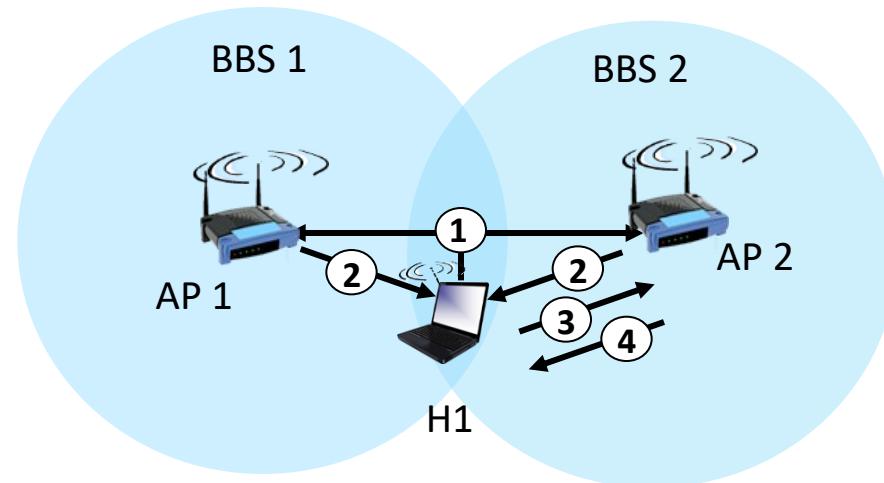


802.11: scansione passiva e attiva



scansione passiva:

- (1) frame beacon inviati dagli AP
- (2) invio di un frame di richiesta di associazione da H1 all'AP selezionato
- (3) invio di un frame di risposta di associazione dall'AP selezionato a H1

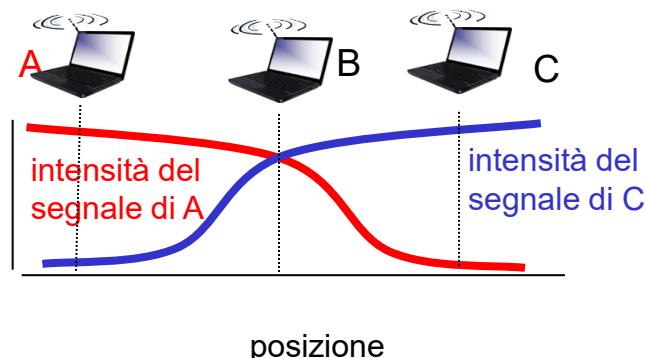


scansione attiva:

- (1) frame sonda di richiesta inviato in broadcast da H1
- (2) frame sonda di risposta inviato dagli AP
- (3) invio di un frame di richiesta di associazione da H1 all'AP selezionato
- (4) invio di un frame di risposta di associazione dall'AP selezionato a H1

IEEE 802.11: accesso multiplo

- evitare collisioni: 2⁺ nodi che trasmettono simultaneamente
- 802.11: CSMA – ascolta il canale prima di trasmettere
 - non si verifica una collisione con la trasmissione rilevata di un altro nodo in corso
- 802.11: *non rileva le collisioni!*
 - difficile rilevare le collisioni: intensità del segnale trasmesso, debolezza del segnale ricevuto a causa dell'attenuazione
 - in ogni caso, non potrebbe rilevare tutte le collisioni: terminale nascosto, attenuazione
 - obiettivo: *evitare le collisioni:* CSMA/[CollisionAvoidance](#)



IEEE 802.11 Protocollo MAC: CSMA/CA

802.11 mittente fisicamente o in modo virtuale usando i valori di duration (vedi dopo)

1 se percepisce il canale inattivo per **DIFS** (Distributed Inter-frame Space) allora

trasmette il frame per intero (no CD)

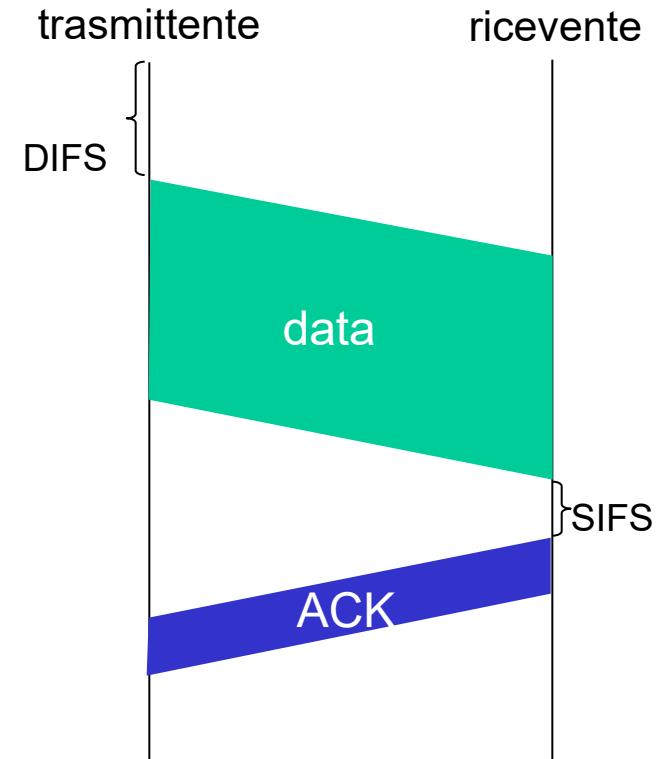
2 altrimenti, la trasmissione deve essere differita

- sceglie un valore di ritardo casuale, usando *binary exponential backoff*
- finché il timer non è zero:
 - aspetta che il canale sia libero per DIFS
 - decrementa il timer, al termine di uno slot in cui il canale è libero
- quando il timer raggiunge zero (può accadere solo se il canale è libero), trasmette il frame per intero
- se non riceve un ACK, incrementa l'intervallo di backoff, ripete il punto 2
- se riceve un ACK e ha altri dati trasmettere*, resetta l'intervallo di backoff e ripete il punto 2

802.11 destinatario

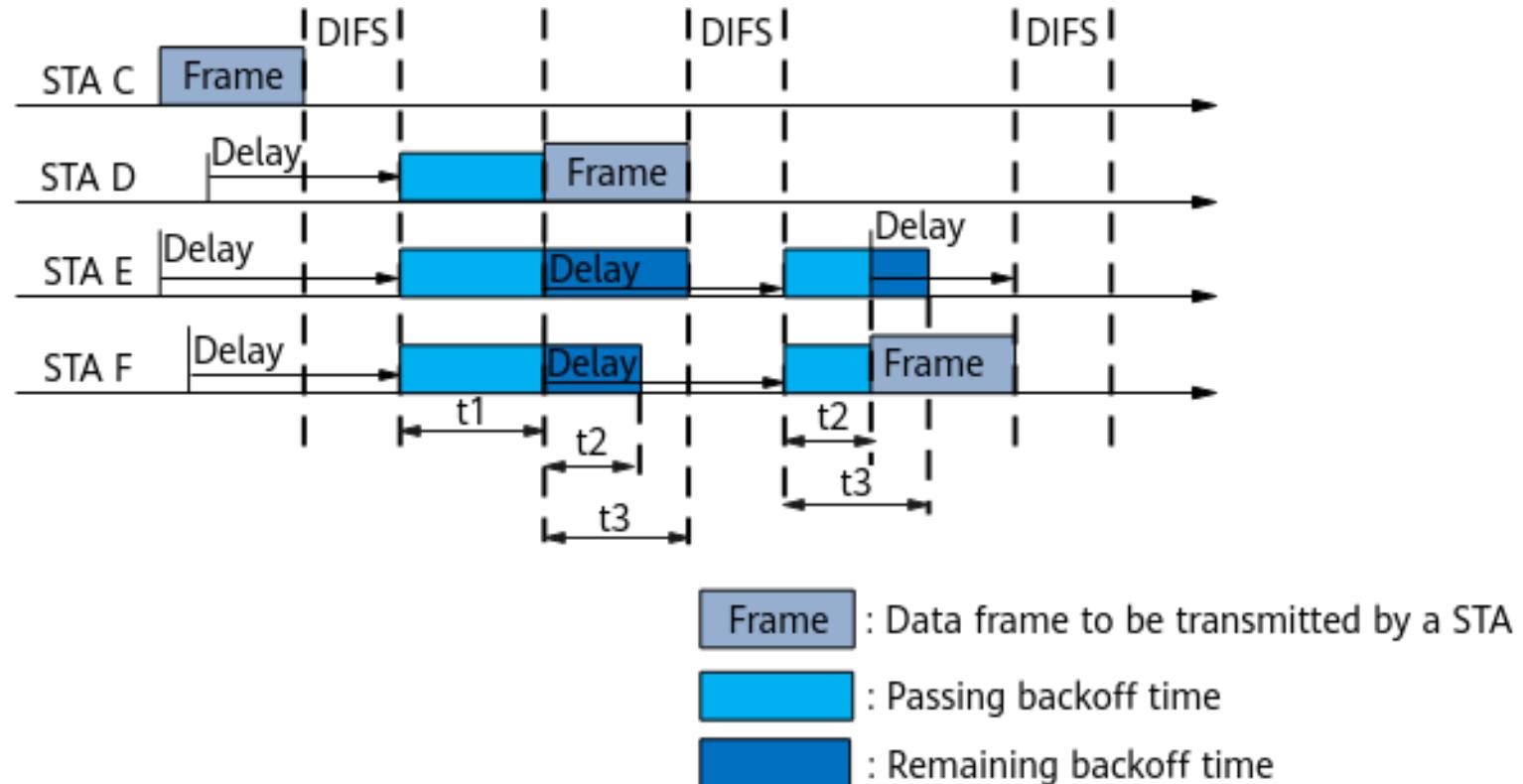
se il frame ricevuto è OK

invia un ACK (necessario a causa del problema del terminale nascosto) dopo **SIFS** (Short Inter-frame Spacing)



*può trasmettere una raffica di frammenti ciascuno dopo SIFS (entro un certo limite)

IEEE 802.11 Protocollo MAC: CSMA/CA



Fonte: <https://support.huawei.com/enterprise/en/doc/EDOC1100410096/25772fc2>

IEEE 802.11 Protocollo MAC: CSMA/CA

Si supponga che due nodi abbiano frame da trasmettere, ma che entrambi percepiscano il canale occupato dalla trasmissione di un terzo nodo.

In CSMA/CD, i due nodi iniziano a trasmettere non appena percepiscono il canale libero, collidendo...ma il rilevamento delle collisioni interromperebbe presto entrambe le trasmissioni, riducendo lo spreco.

Quando non è possibile implementare il rilevamento delle collisioni, CSMA/CA cerca di evitarle: pertanto, i due nodi entrano in un processo di attesa casuale, che permette a uno dei due nodi iniziare a trasmettere, dando tempo all'altro di rilevarne il segnale e, quindi, congelare il proprio timer (in attesa che il canale diventi nuovamente libero).

Puttropo, le collisioni sono ancora possibili:

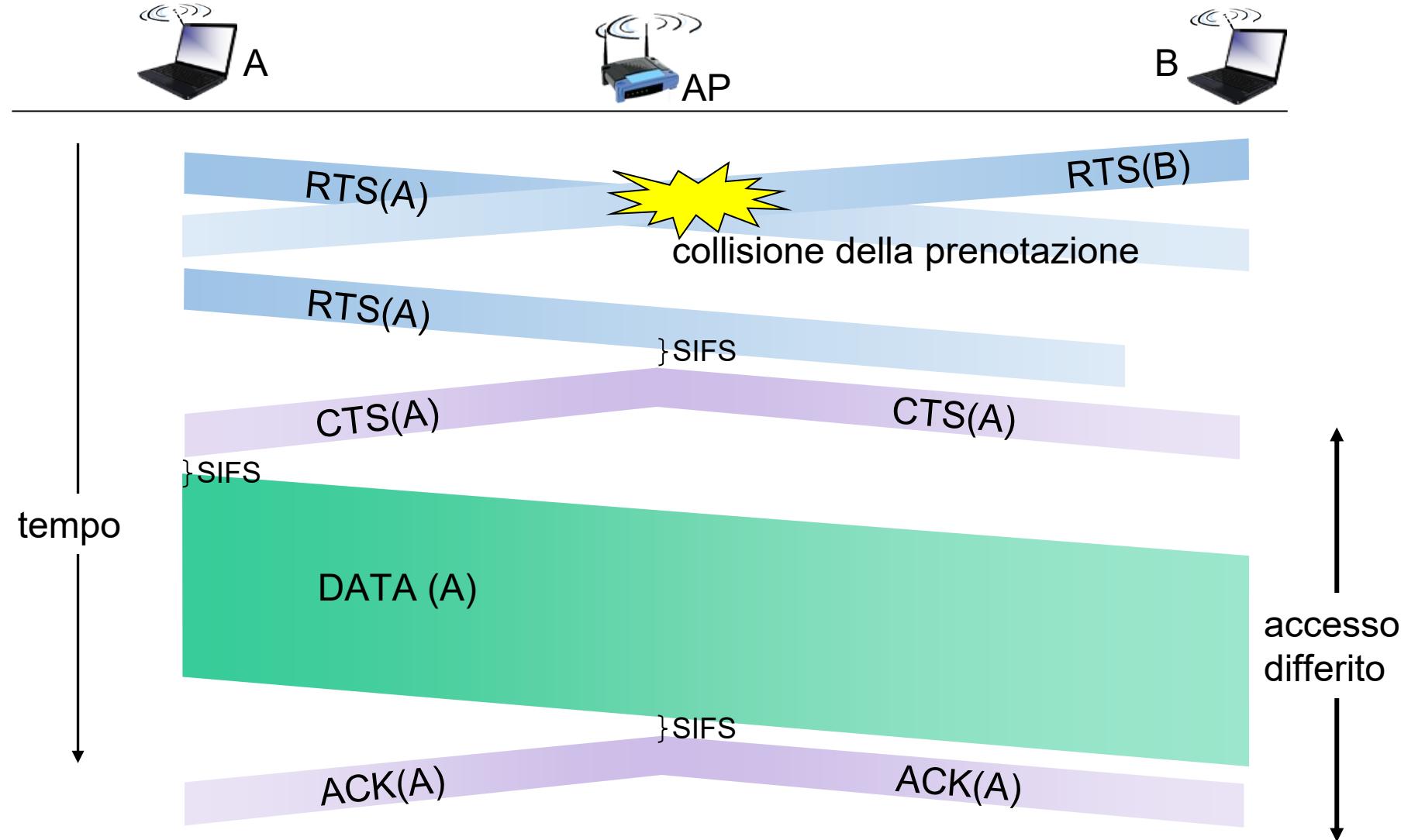
- terminale nascosto
- i tempi di attesa scelti dai due nodi sono sufficientemente vicini, per cui il segnale dell'uno non raggiunge l'altro nodo quando questo inizia a trasmettere perché anche il proprio timer si è azzerato

Evitare le collisioni (di più)

idea: consentire al mittente di "prenotare" il canale: si evitano così le collisioni anche durante l'invio di lunghi pacchetti di dati (opzionale, non viene sempre usato)

- il mittente invia prima un *piccolo* pacchetto request-to-send (RTS) all'AP usando CSMA
 - possono verificarsi collisioni tra i pacchetti RTS (ma sono comunque molto piccoli)
- AP risponde (dopo un SIFS) diffondendo in broadcast il pacchetto clear-to-send CTS in risposta al pacchetto ricevuto
- Il pacchetto CTS è ricevuto da tutti i nodi
 - il mittente invierà (dopo un SIFS) il pacchetto
 - gli altri nodi rimanderanno eventuali trasmissioni

Evitare le collisioni: scambio di pacchetti RTS-CTS



802.11 frame: indirizzamento

2	2	6	6	6	2	6	0 - 2312	4
controllo del frame	durata	indirizzo 1	indirizzo 2	indirizzo 3	numero di sequenza	indirizzo 4	payload (carico utile)	CRC

Indirizzo 1: indirizzo MAC dell'host wireless o AP che deve ricevere il frame (può non essere il destinatario finale)

Indirizzo 2: indirizzo MAC dell'host wireless o AP che trasmette il pacchetto (può non essere il mittente iniziale)

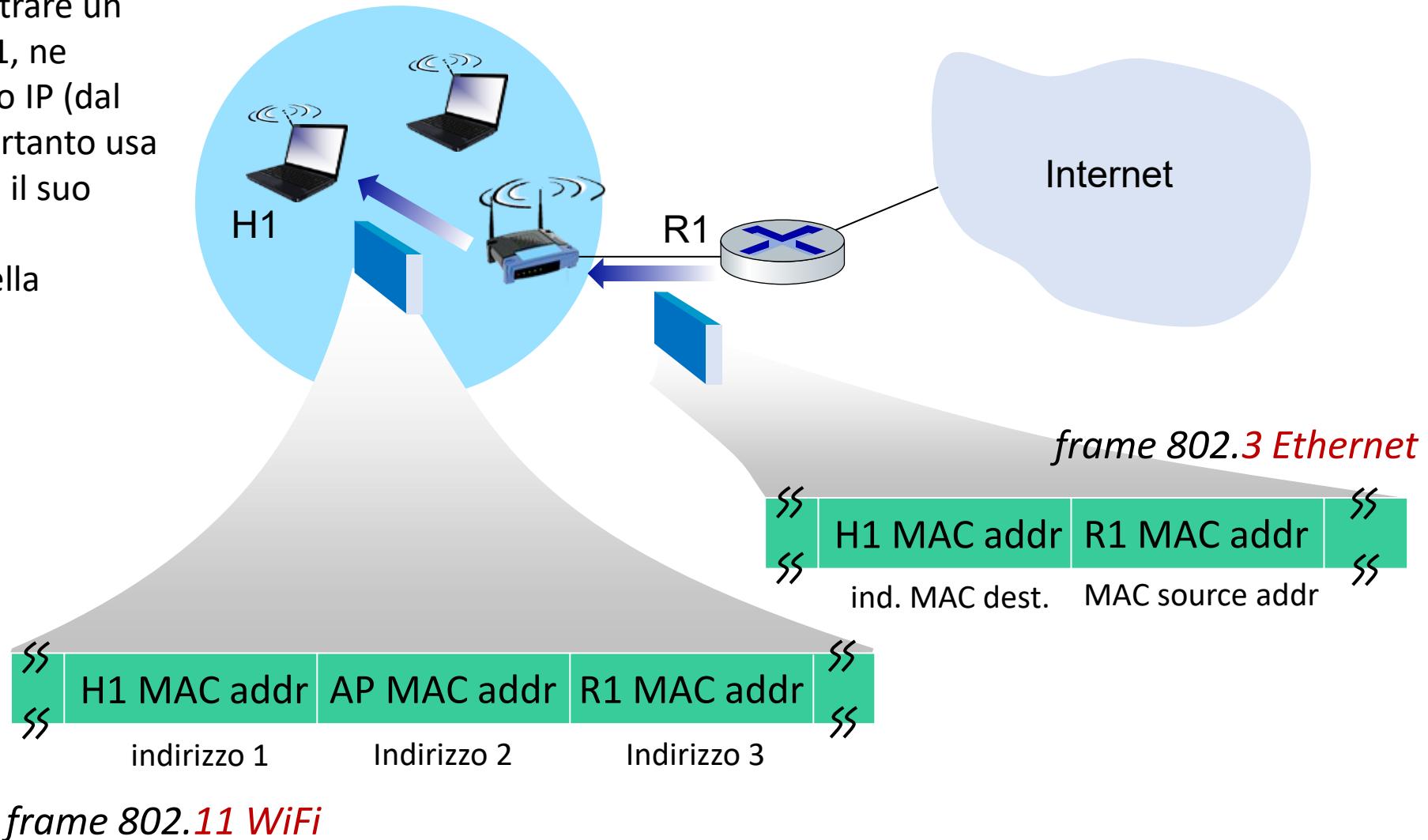
Indirizzo 4: usato solo in modalità ad hoc

Indirizzo 3: indirizzo MAC dell'interfaccia router cui l'AP è collegato

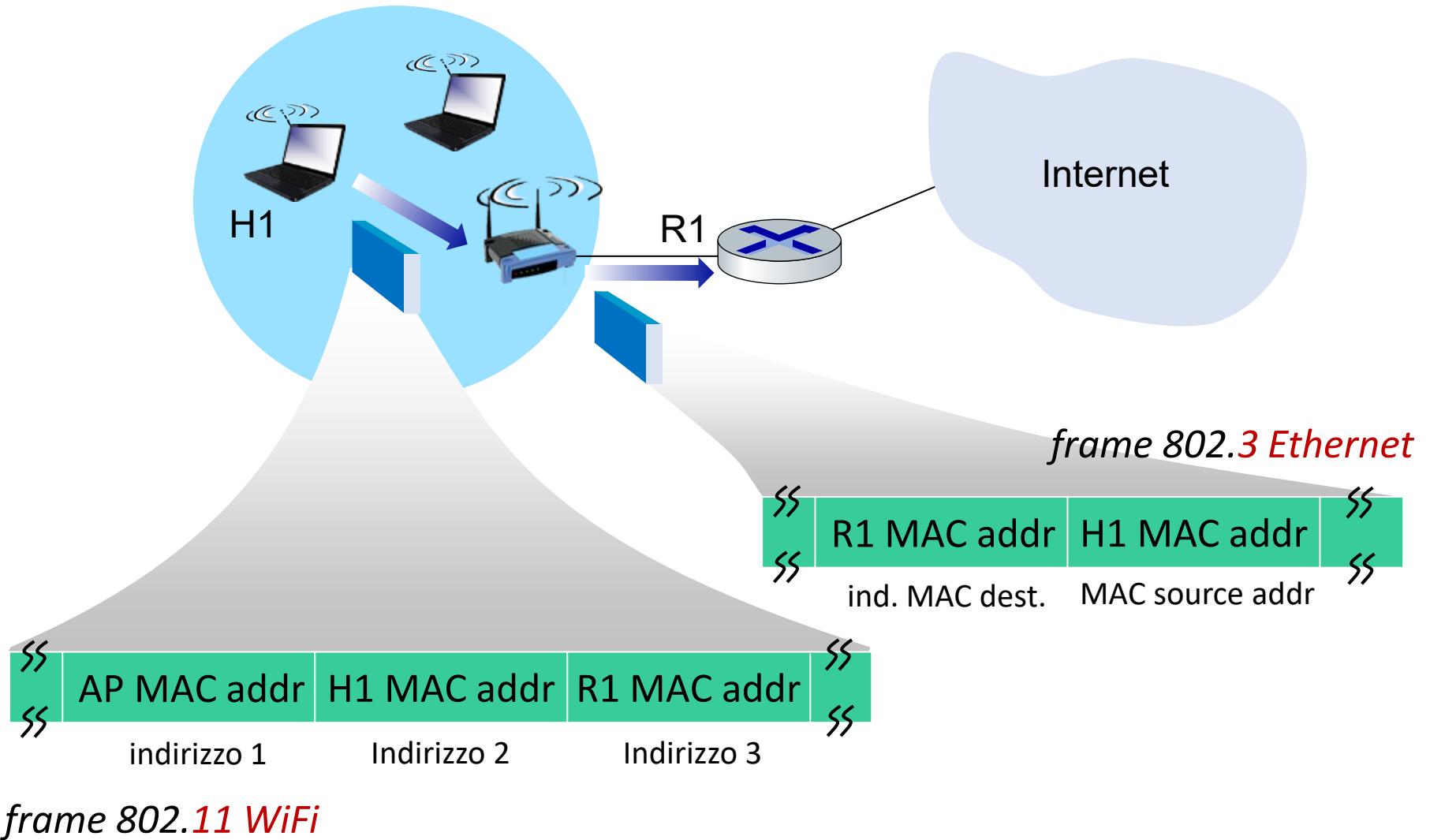
Indirizzo 3 gioca un ruolo cruciale nell'internetworking tra un BSS e una LAN cablata

802.11 frame: indirizzamento

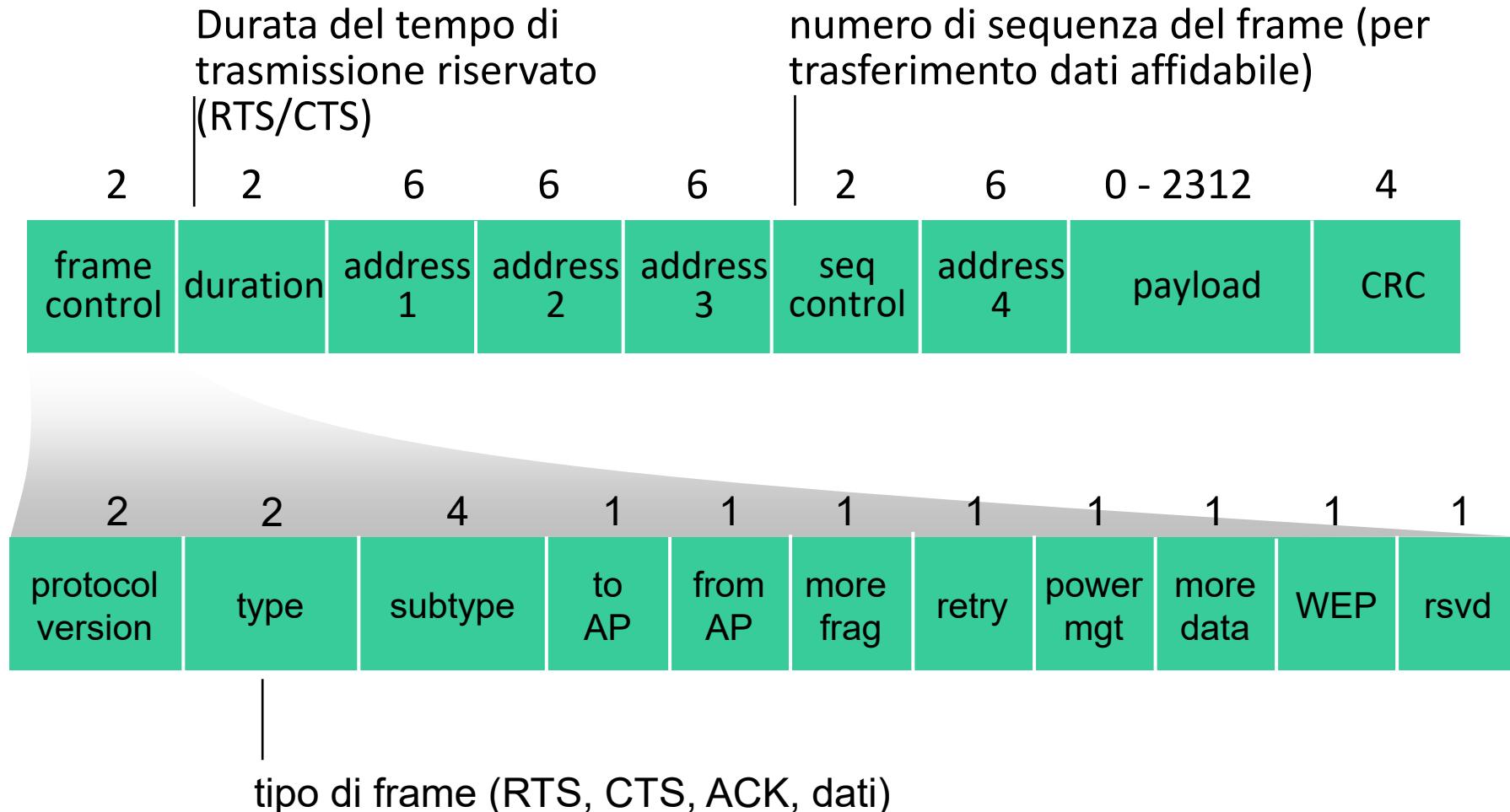
R1, che deve inoltrare un datagramma a H1, ne conosce l'indirizzo IP (dal datagramma), pertanto usa ARP per ottenere il suo MAC address: inconsapevole della presenza dell'AP



802.11 frame: indirizzamento

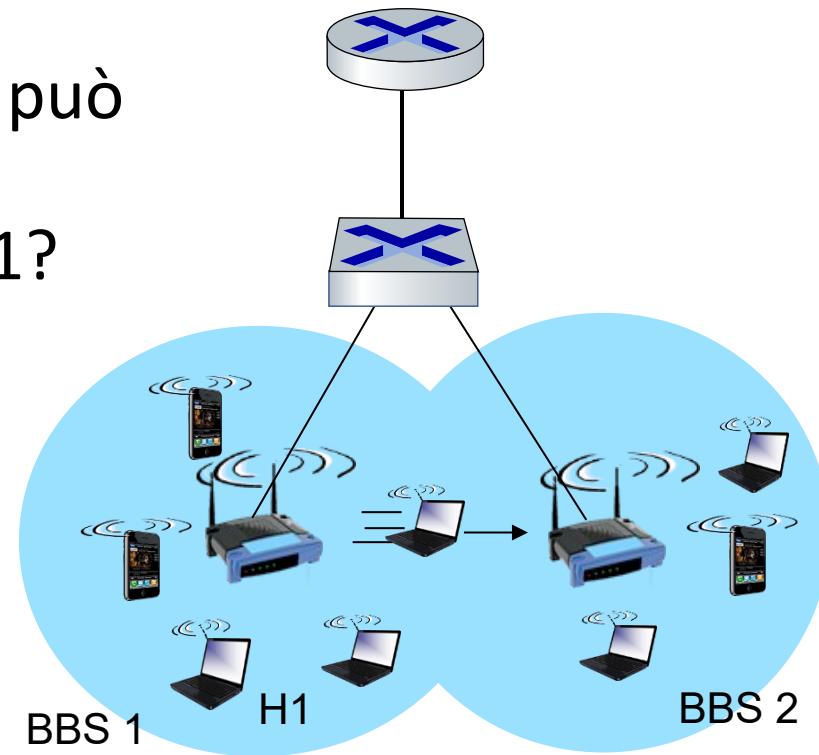


802.11 frame: indirizzamento



802.11: mobilità all'interno della stessa sottorete

- siccome i due AP sono connessi da uno switch (anziché da un router), H1 rimane nella stessa sottorete: l'indirizzo IP può rimanere lo stesso
- switch: con quale AP è associato H1?
 - auto-apprendimento: lo switch vedrà frame da H1 e "ricorderà" quale porta può essere usata per raggiungere H1
 - Il nuovo AP può inviare un frame Ethernet broadcast con mittente H1, affinché lo switch apprenda la nuova porta per raggiungere H1
 - Lo standard 802.11f definisce un protocollo inter-AP che affronta questo e altri problemi

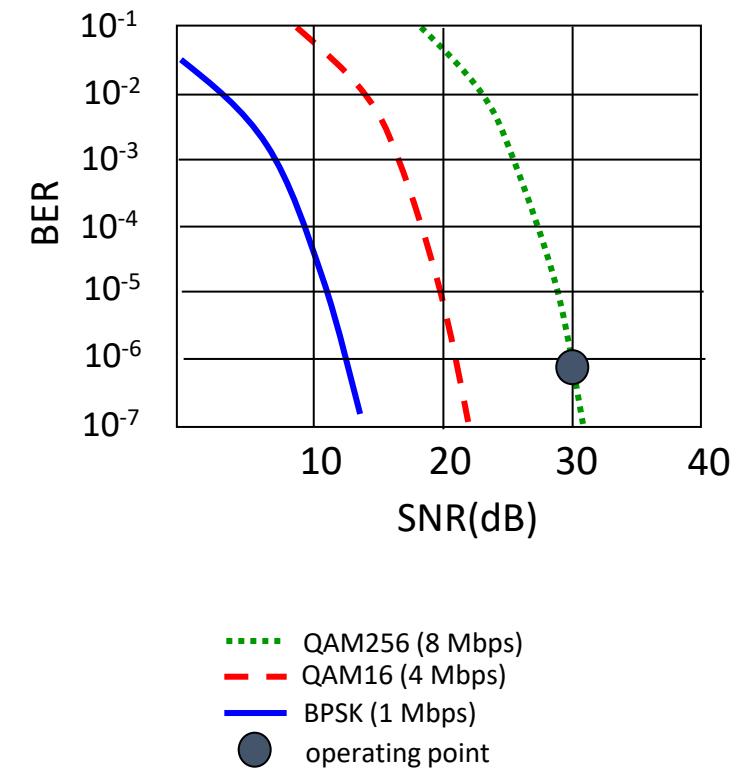


802.11: funzionalità avanzate

Adattamento del tasso trasmittivo

- La stazione base e la stazione mobile cambiano dinamicamente il tasso trasmittivo (tecnica di modulazione a livello fisico) come la stazione mobile si sposta e di conseguenza cambia l'SNR

1. SNR cala BER aumenta quando il nodo si allontana dalla stazione base
2. Quando il BER diventa troppo alto, passa un tasso trasmittivo inferiore ma con BER inferiore



802.11: funzionalità avanzate

Gestione dell'energia

- Nodo ad AP: “Sto per diventare inattivo fino al prossimo frame beacon”
 - AP sa che non deve trasmettere frame a questo nodo
 - il nodo si riattiva prima del successivo frame beacon
- frame beacon: contiene la lista dei nodi che devono ricevere frame in attesa sull'AP
 - il nodo rimane sveglio se devono essere inviati frame da AP a mobile; altrimenti dorme di nuovo fino al prossimo frame beacon

Università degli Studi di Roma "Tor Vergata"
Laurea in Informatica

Sistemi Operativi e Reti
(modulo Reti)
a.a. 2023/2024

Wireless e Reti Mobili (parte2)

dr. Manuel Fiorelli

manuel.fiorelli@uniroma2.it

<https://art.uniroma2.it/fiorelli>

Basate sulle slide del libro di testo:

https://gaia.cs.umass.edu/kurose_ross/ppt.php

Introduction: 1-44

Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth

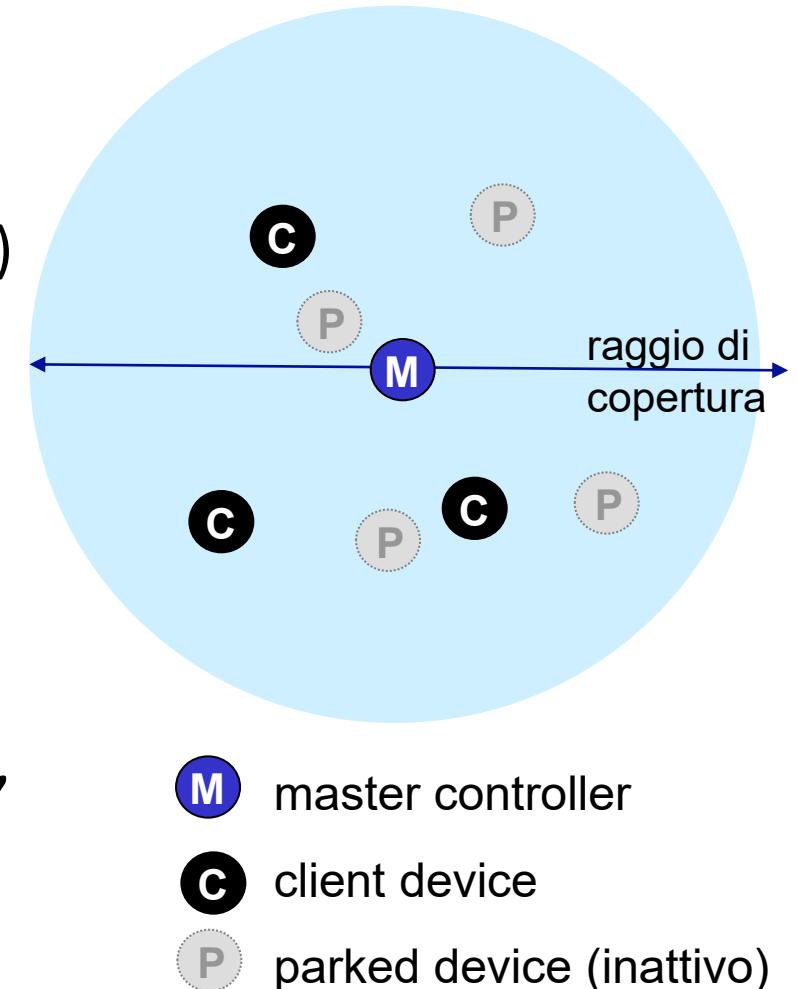


Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

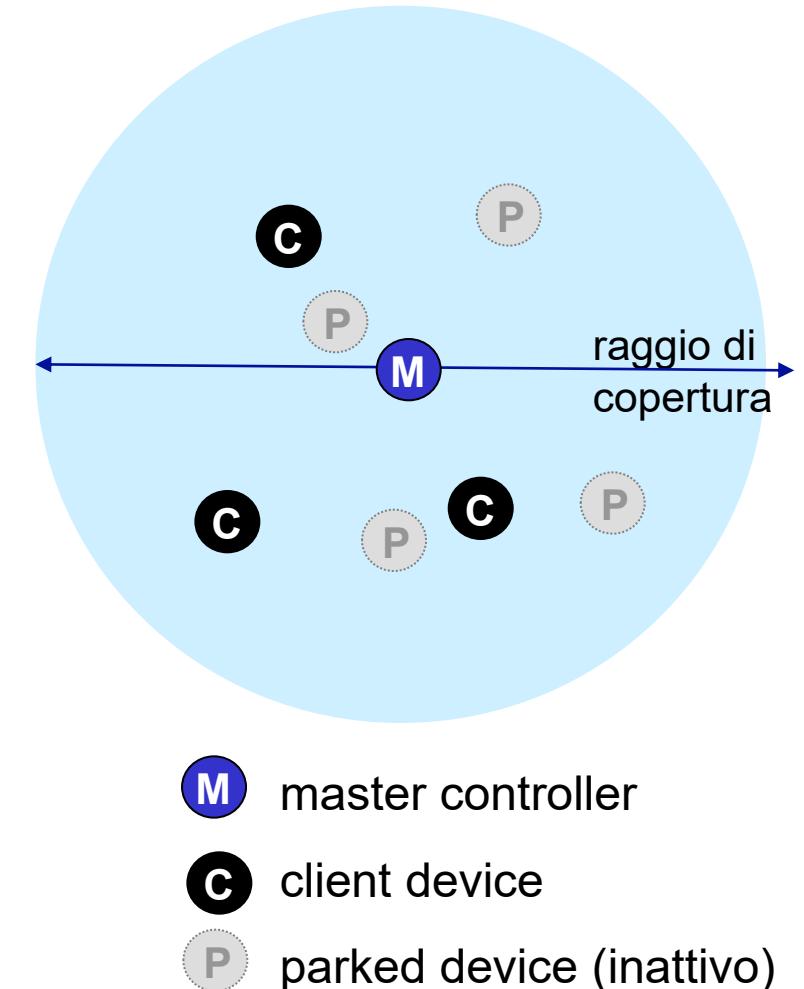
Bluetooth: Personal area network

- meno di 10 m di diametro
- sostituzione dei cavi (mouse, tastiera, cuffie)
- *wireless personal area network* (WPAN) [connette dispositivi nell'area di lavoro di una persona] o *piconet*
- 2.4-2.5 GHz ISM radio band, fino a 3 Mbps: essendo usata da molti altri dispositivi, Bluetooth deve tenere in particolare considerazione le interferenze



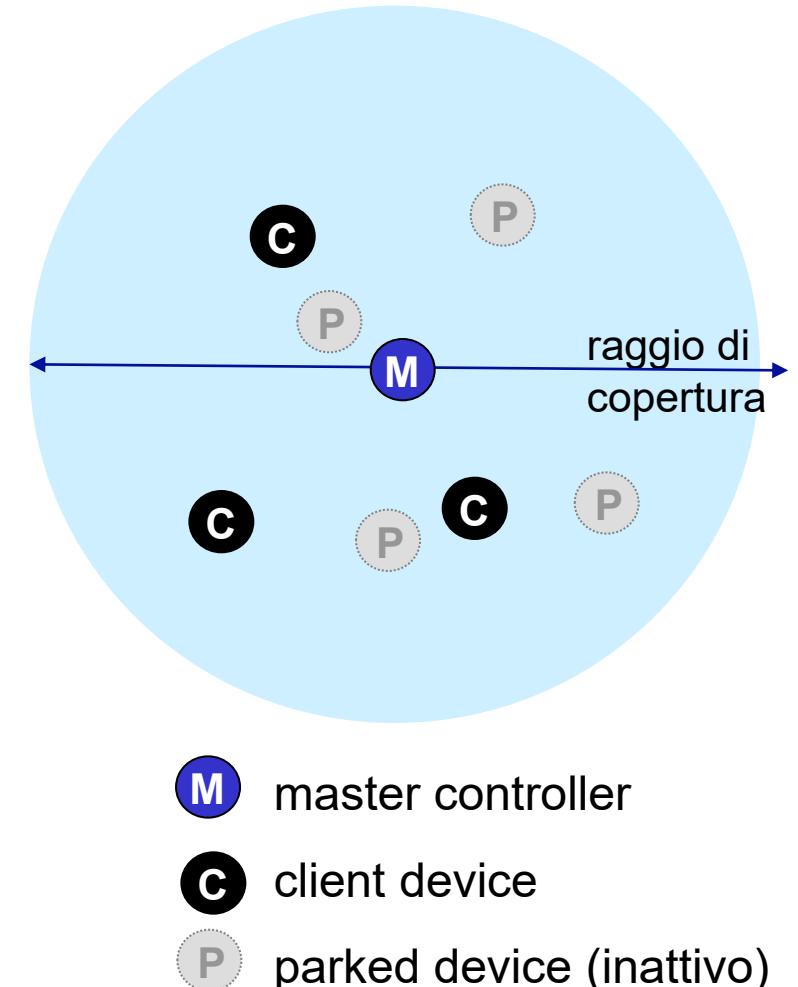
Bluetooth: Personal area network

- TDM, slot di 625 μ sec
- FDM: il mittente usa 79 canali di frequenza in un ordine conosciuto, pseudo-casuale da slot a slot (*frequency-hopping spread spectrum, FHSS*)
 - altri dispositivi/apparecchiature non nella piconet interferiscono solo in alcuni slot



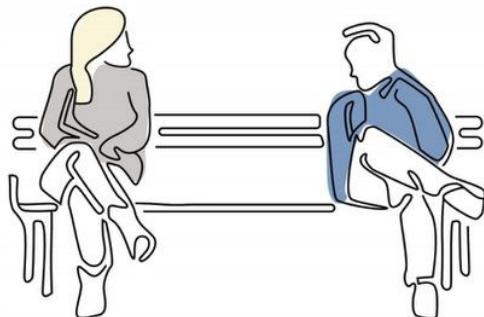
Bluetooth: Personal area network

- ad hoc: nessuna infrastruttura
- fino a 8 dispositivi attivi: un master e dispositivi client:
 - il master stabilisce il "clock", decide la sequenza dei salti tra le frequenze, controlla la potenza di trasmissione, esegue il polling dei client
- **parked mode** (fino a 255): i client possono “andare a dormire” (park) e risvegliarsi successivamente (per preservare la batteria)
- **bootstrapping**: i nodi si autoassemblano (plug and play) in una piconet
 - **neighbor discovery**: il master invia (ripetutamente) messaggi *inquiry* in broadcast su ciascun canale di frequenza, cui i dispositivi (in ascolto su un determinato canale) rispondono dopo un ritardo casuale (per evitare collisioni)
 - **paging**: il master manda a ciascun singolo dispositivo un invito: quando riceve un ACK, il master invia al dispositivo del pattern per il frequency hopping, il clock e un indirizzo

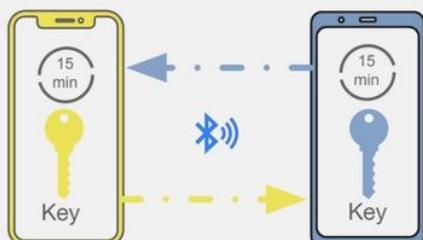


Pandemia + Bluetooth

Alice and Bob meet each other for the first time and have a 10-minute conversation.



Their phones exchange anonymous identifier beacons (which change frequently).



A few days later...

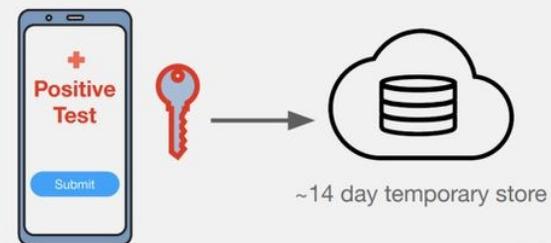


Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.



With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

Apps can only get more information via user consent



Apple | Google

Pandemia + Bluetooth

Alice continues her day unaware she had been near a potentially contagious person.



Alice's phone periodically downloads the broadcast beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with the Bob's anonymous identifier beacons.



Anonymous identifier keys are downloaded periodically



A match is found



Sometime later...

Alice sees a notification on her phone.



Alice's phone receives a notification with information about what to do next.



Additional information is provided by the health authority app or website



Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth



Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

Reti cellulari 4G/5G

- *la soluzione per Internet mobile in wide-area*
- disiegamento/uso diffuso:
 - Più dispositivi mobili che fissi connessi alla banda larga (5 a 1 nel 2019)!
 - Disponibilità del 4G: 97% del tempo in Korea (90% negli US)
- tassi di trasmissione fino a centinaia di Mbps
- standard tecnici: 3rd Generation Partnership Project (3GPP)
 - www.3gpp.org
 - 4G: Long-Term Evolution (LTE)standard

Reti cellulari 4G/5G

similarità con Internet cablato

- Distinzione periferia/nucleo, ma entrambi appartengono allo stesso *carrier*
- Rete cellulare globale: una rete di reti
- Uso diffuso di protocolli: HTTP, DNS, TCP, UDP, IP, NAT, separazione tra piano di controllo e piano di dati, SDN, Ethernet, tunneling
- Interconnessione a Internet cablato

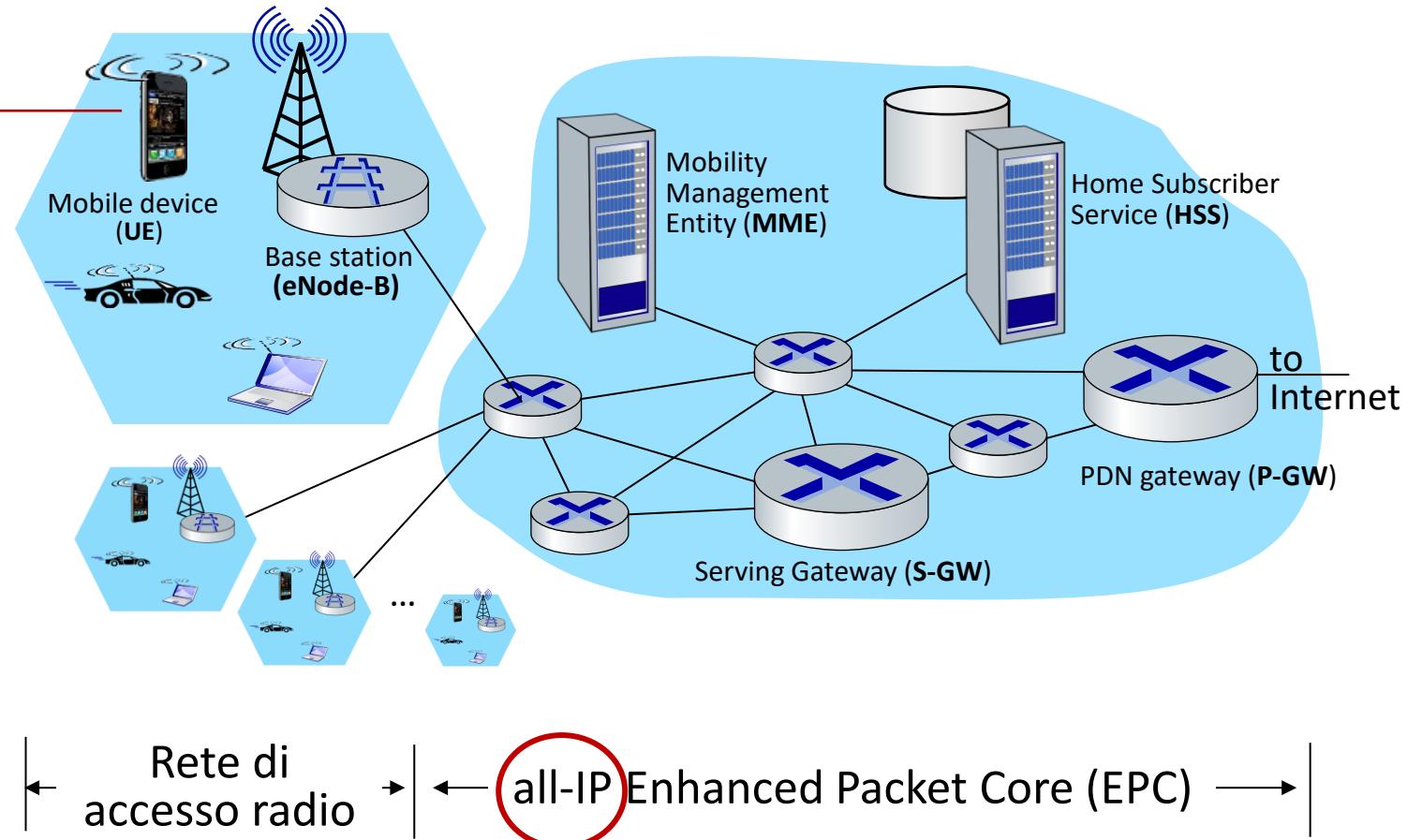
Differenze con Internet cablato

- Differenti protocolli livello di collegamento wireless
- Mobilità come servizio di 1° classe
- "identità" dell'utente (attraverso la SIM card)
- modello di business: gli utenti si abbonano a un operatore di telefonia mobile
 - forte nozione di "home network", contrapposta al roaming in una "visited network"
 - accesso globale, con infrastruttura di autenticazione, e accordi tra operatori

Elementi dell'architettura 4G

Mobile device:

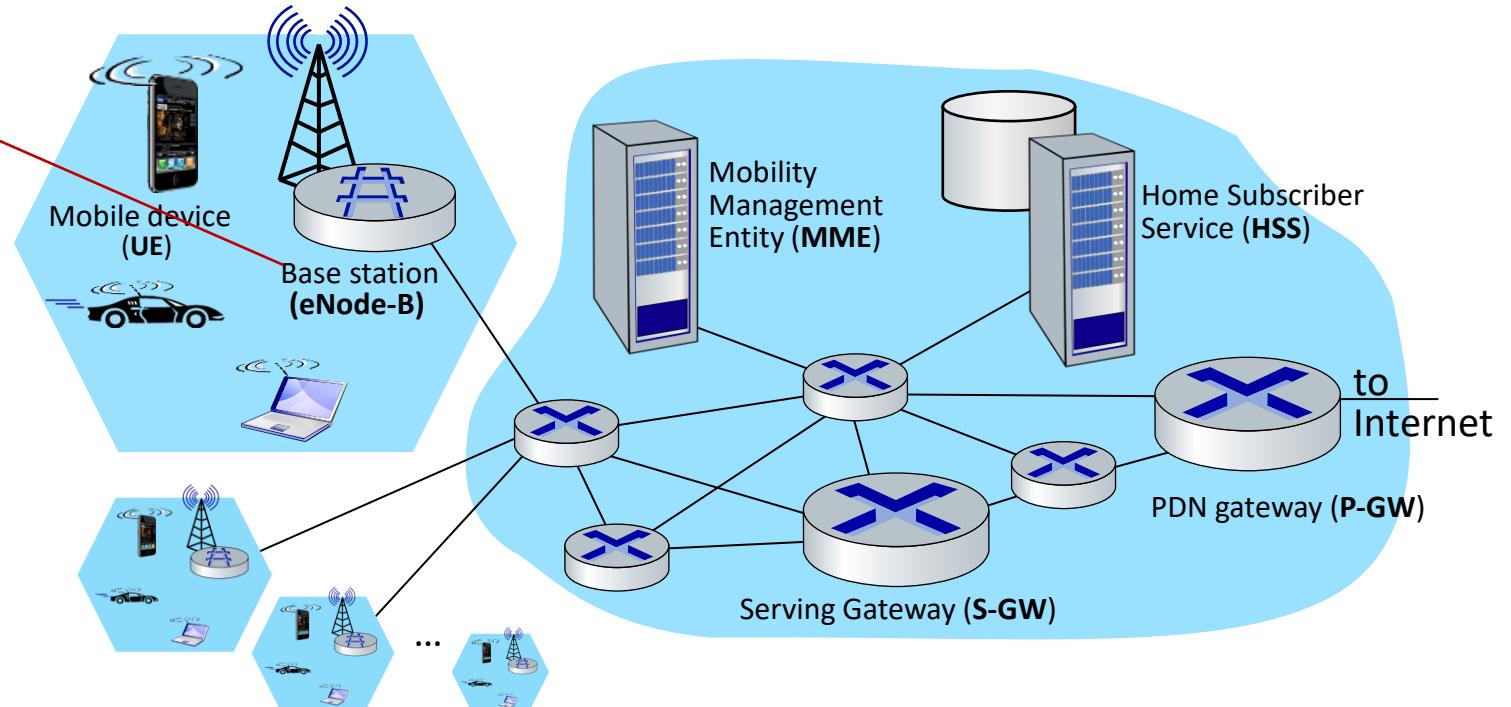
- smartphone, tablet, laptop, IoT, ... con radio 4G LTE
- International Mobile Subscriber Identity (IMSI) a 64-bit, memorizzato sulla SIM (Subscriber Identity Module) card
- Gergo LTE: User Equipment (UE)



Elementi dell'architettura 4G

Base station (stazione base):

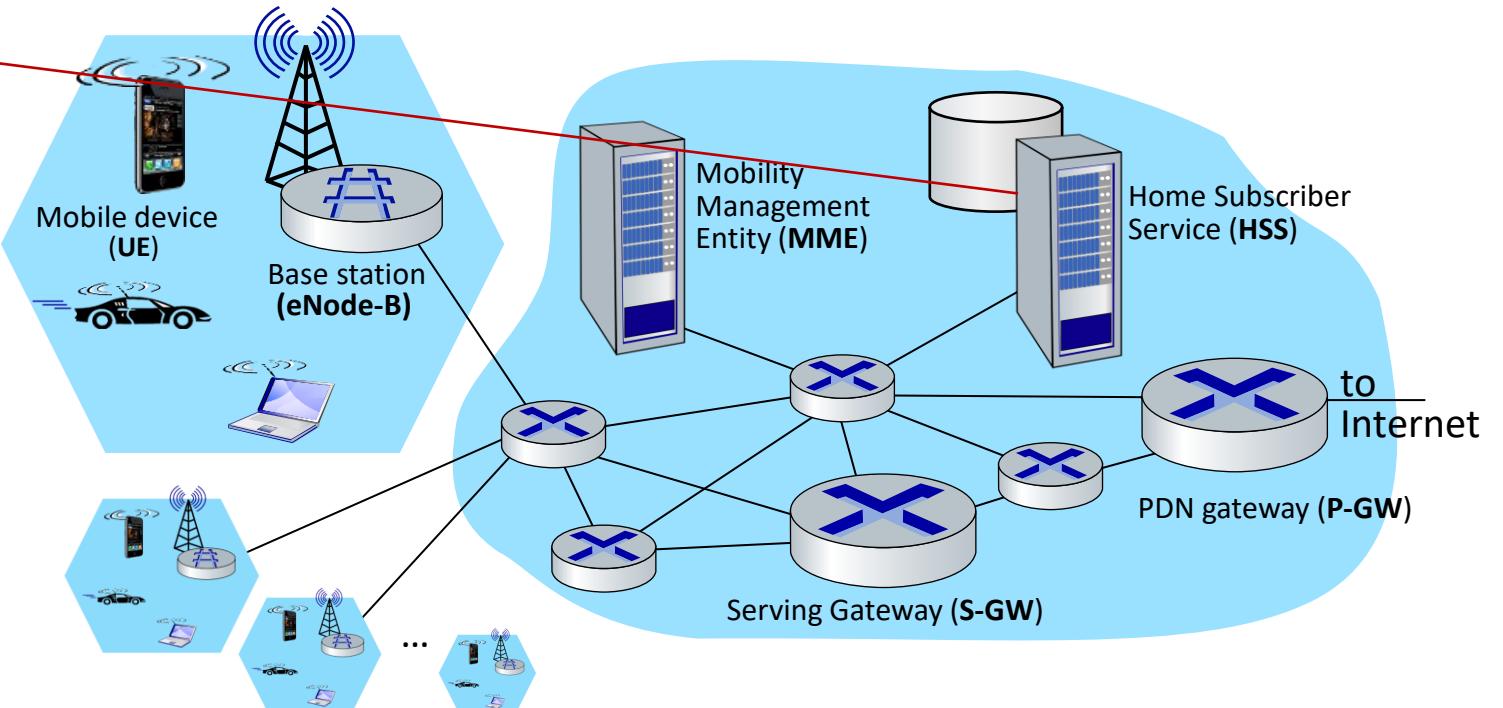
- alla “periferia” della rete dell'operatore
- gestisce le risorse radio, per i mobile device nella propria area di copertura (“cella”)
- coordina l'autenticazione del dispositivo con altri elementi
- simile all'AP WiFi ma:
 - ruolo attivo nella mobilità degli utenti
 - si coordina con quasi tutte le base station per ottimizzare l'uso della radio
- Gergo LTE: eNode-B



Elementi dell'architettura 4G

Home Subscriber Service

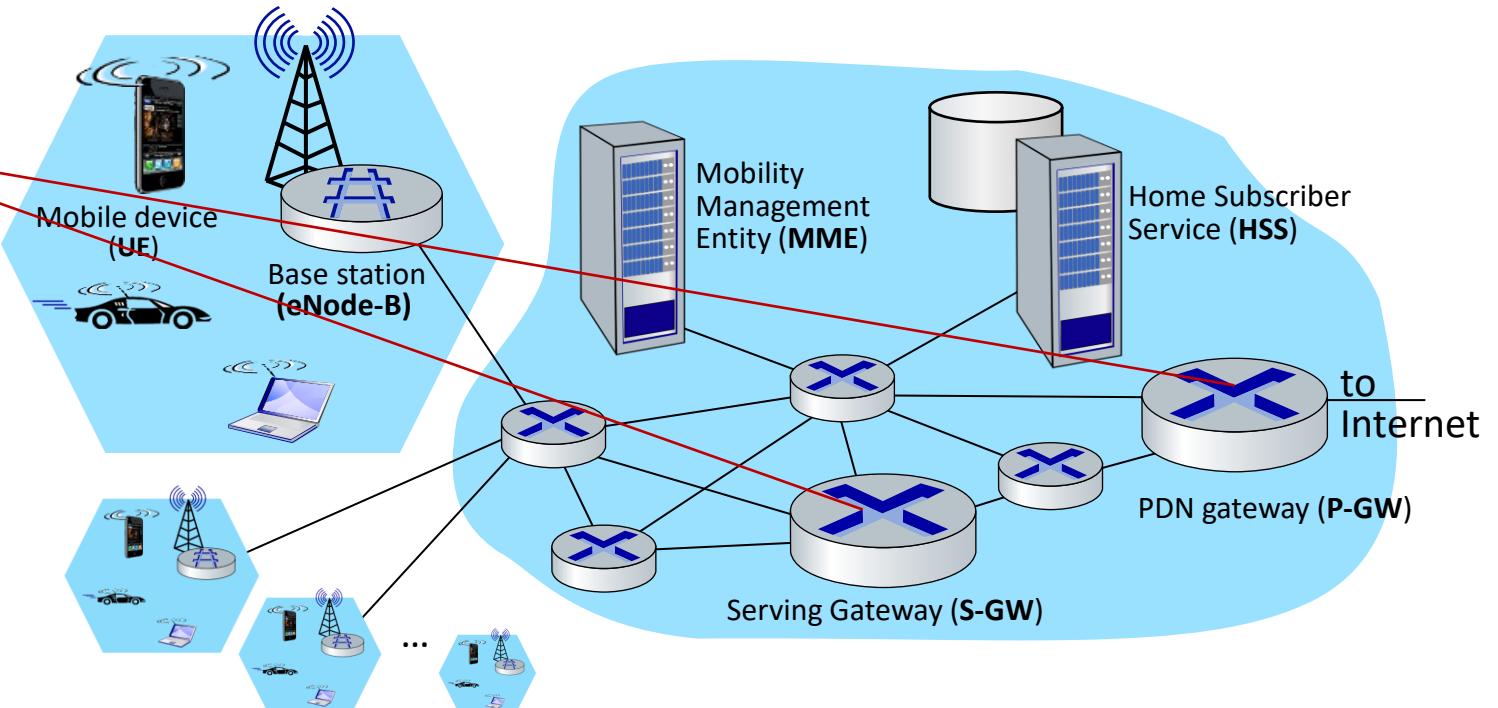
- memorizza informazioni sui mobile device per i quali la rete dell'HSS è la loro "home network"
- lavora con l'MME per l'autenticazione dei dispositivi



Elementi dell'architettura 4G

Serving Gateway (S-GW), PDN Gateway (P-GW)

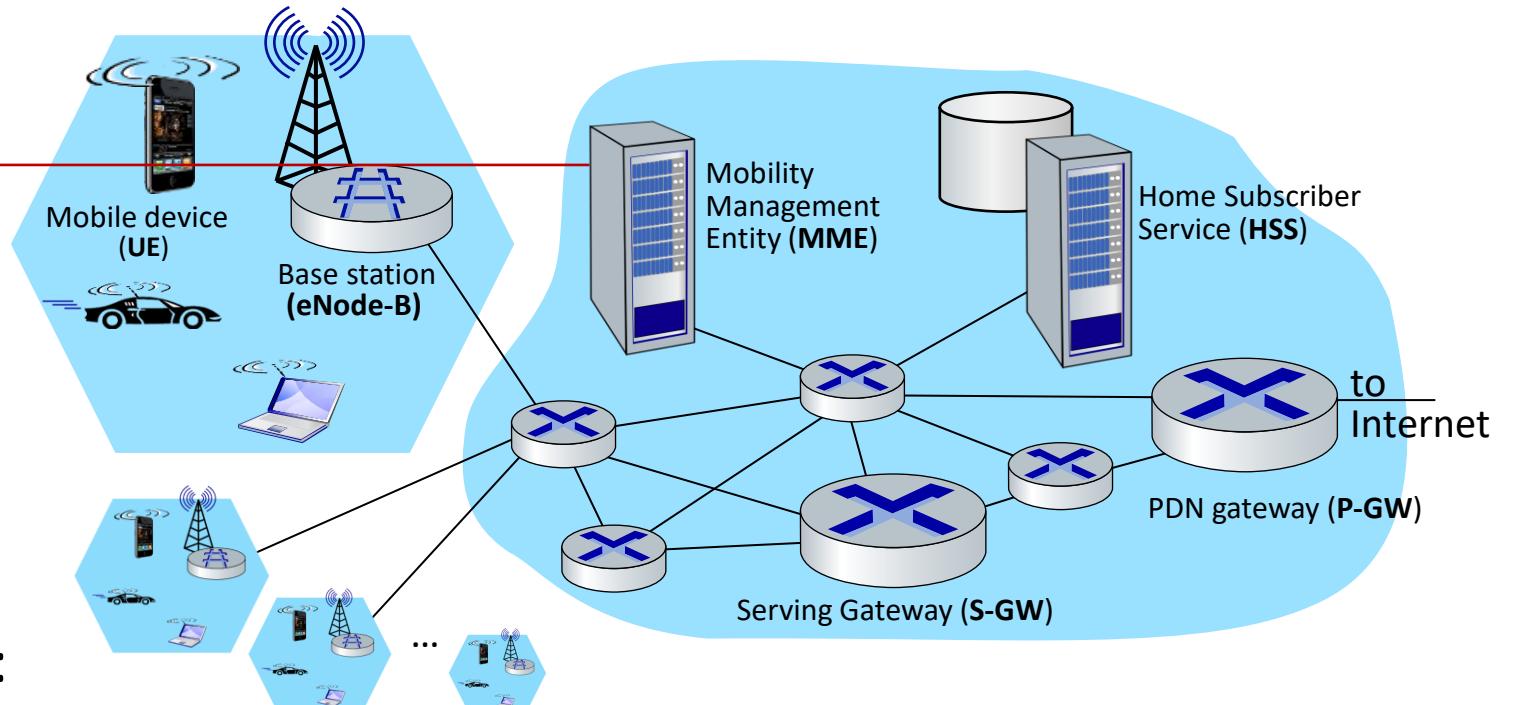
- situati lungo il percorso dei dati tra Internet e il mobile device
- P-GW
 - gateway per la rete mobile cellulare
 - appare come qualunque altro router di Internet
 - fornisce servizi NAT
- altri router:
 - uso estensivo di tunneling



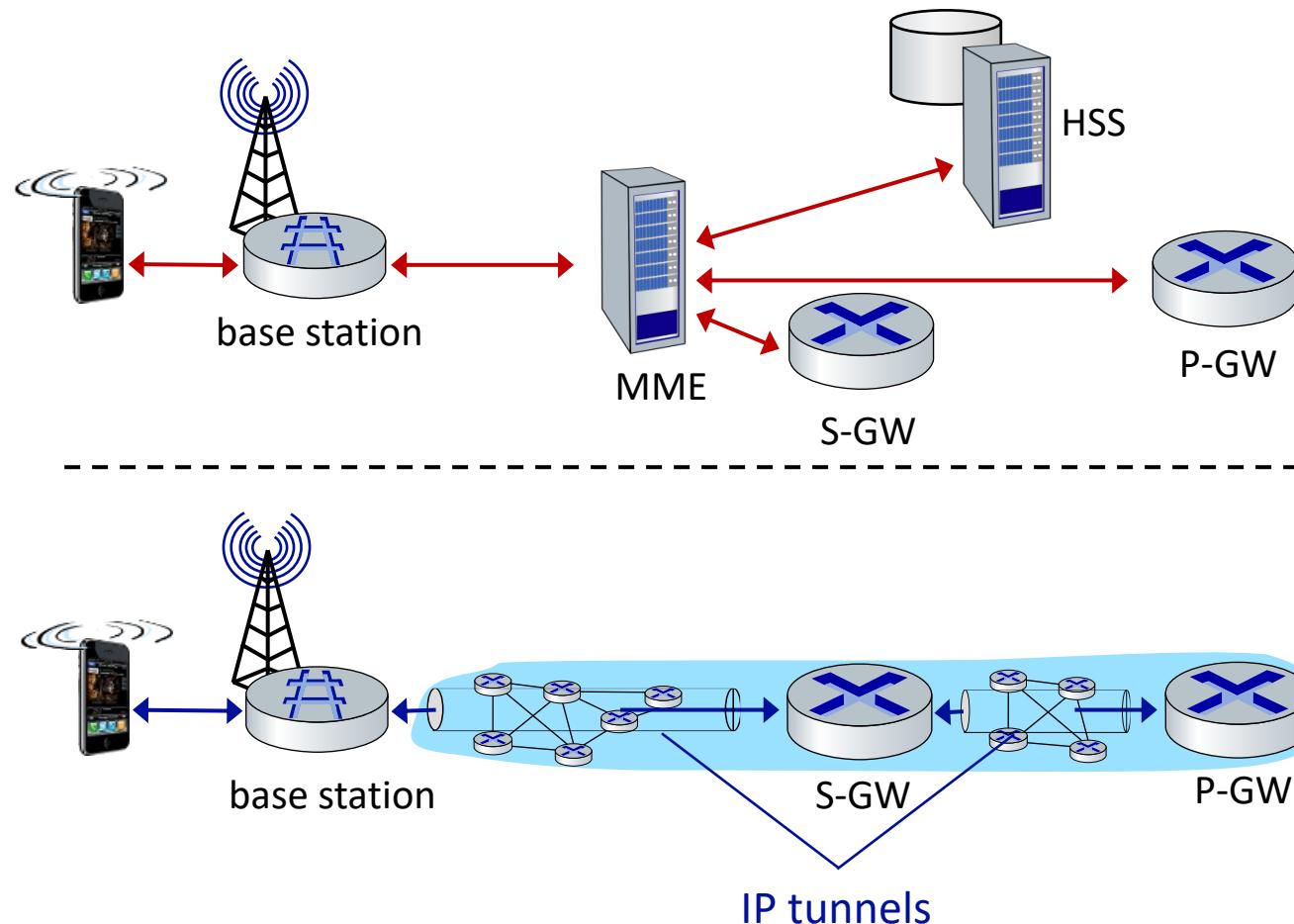
Elementi dell'architettura 4G

Mobility Management Entity

- Autenticazione dei device (device-to-network, network-to-device) coordinata con l'HSS della home network HSS del dispositivo mobile
- gestione dei dispositivi mobili:
 - handover dei device tra celle
 - tracking/paging della posizione dei device
- setup del percorso (tunneling) dal mobile device e il P-GW



LTE: separazione del piano dei dati e di controllo



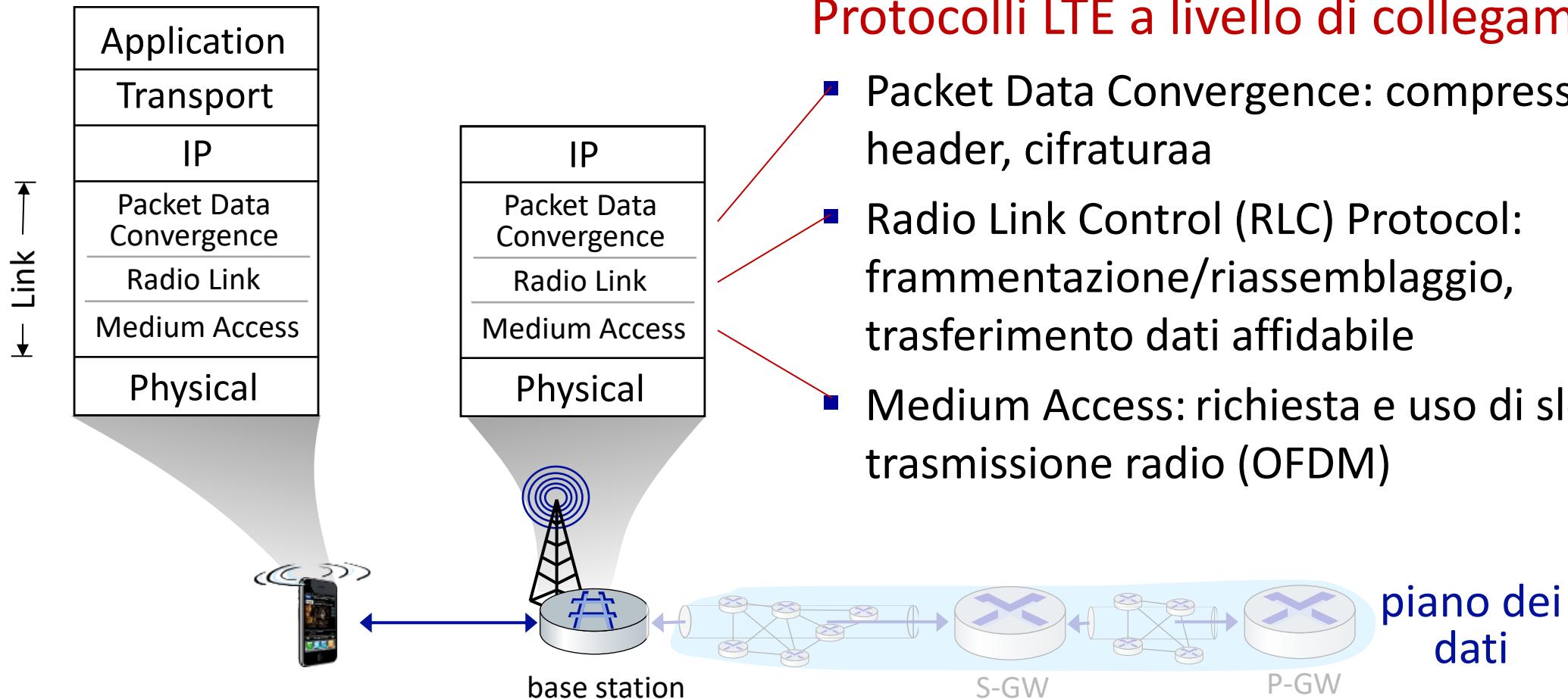
piano di controllo

- Nuovi protocolli per la gestione della mobilità, la sicurezza e l'autenticazione

piano dei dati

- nuovi protocolli a livello fisico e di collegamento
- uso estensivo di tunnel per gestire la mobilità

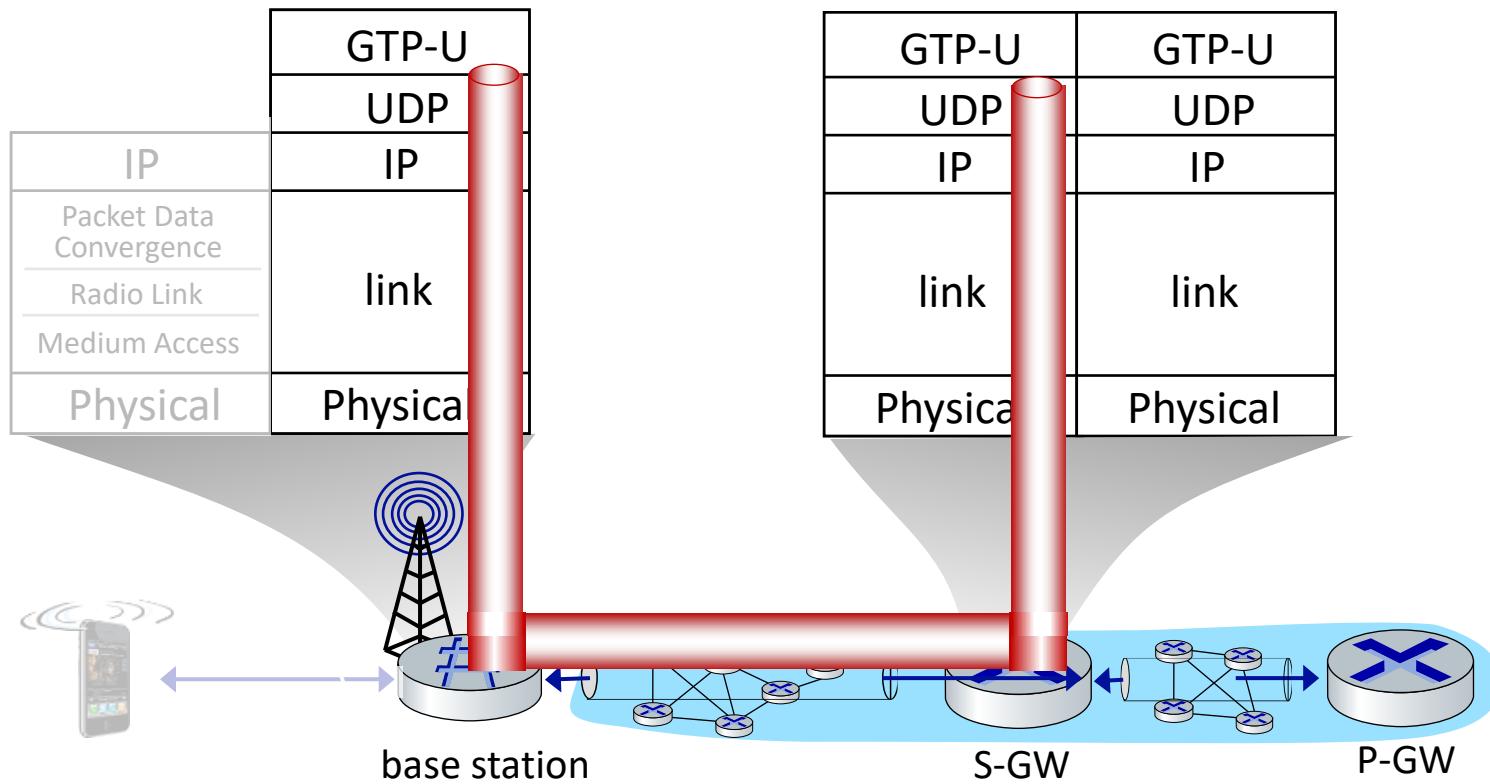
Pila protocollare del piano dei dati LTE: first hop



Protocolli LTE a livello di collegamento:

- Packet Data Convergence: compressione degli header, cifratura
 - Radio Link Control (RLC) Protocol: frammentazione/riassembaggio, trasferimento dati affidabile
 - Medium Access: richiesta e uso di slot per la trasmissione radio (OFDM)

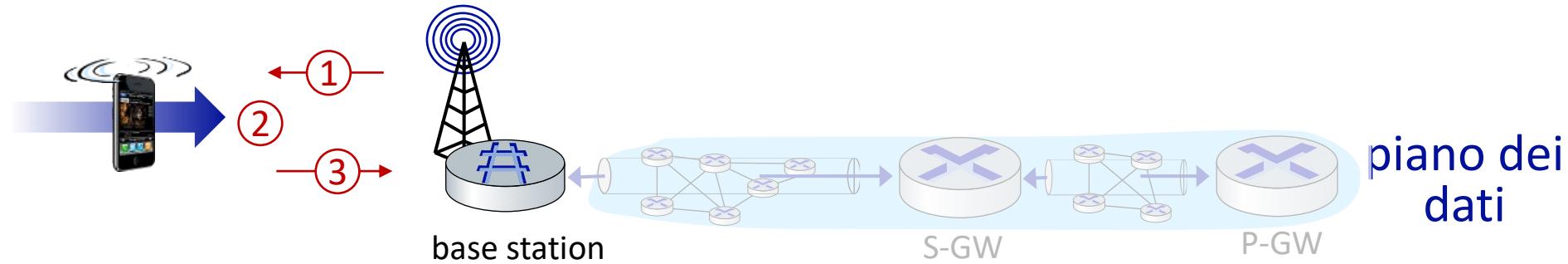
Pila protocollare del piano dei dati LTE: packet core



tunneling:

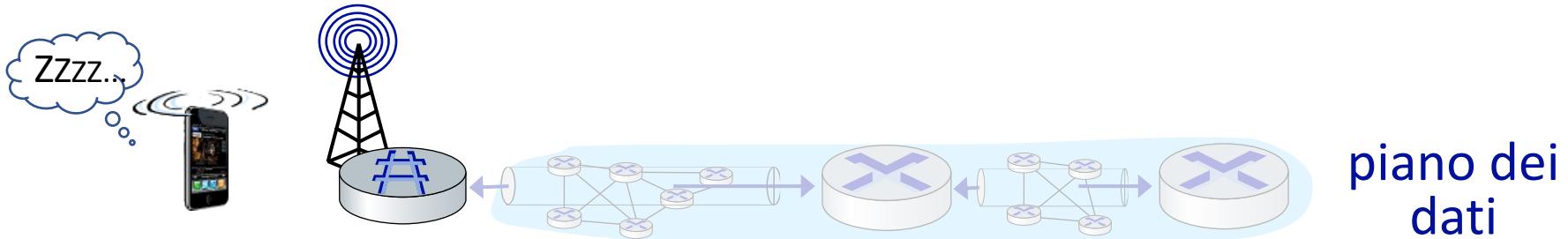
- datagrammi mobile incapsulati usando GPRS Tunneling Protocol (GTP), inviati dentro datagrammi UDP all'S-GW
- S-GW reinvia i datagrammi al P-GW tramite un altro tunnel
- supporta la mobilità: solo gli endpoint del tunnel cambiano quando l'utente mobile si sposta

Piano dei dati LTE: associazione con una BS



- ① BS invia in broadcast un segnale di sincronizzazione primario ogni 5 ms su tutte le frequenze
 - BS di più carrier possono inviare in broadcast segnali di sincronizzazione
- ② Il mobile node trova un segnale di sincronizzazione primario, quindi individua il secondo segnale di sincronizzazione su questa frequenza.
 - il mobile node trova quindi le informazioni trasmesse dalla BS: larghezza di banda del canale, configurazioni, informazioni sul vettore cellulare della BS.
 - il mobile node può ricevere informazioni da più stazioni di base, più reti cellulari
- ③ il mobile node sceglie con quale BS associarsi (ad esempio, preferendo la rete dell'operatore d'origine)
- ④ sono necessari altri passaggi per l'autenticazione, la creazione dello stato e la configurazione del piano dati.

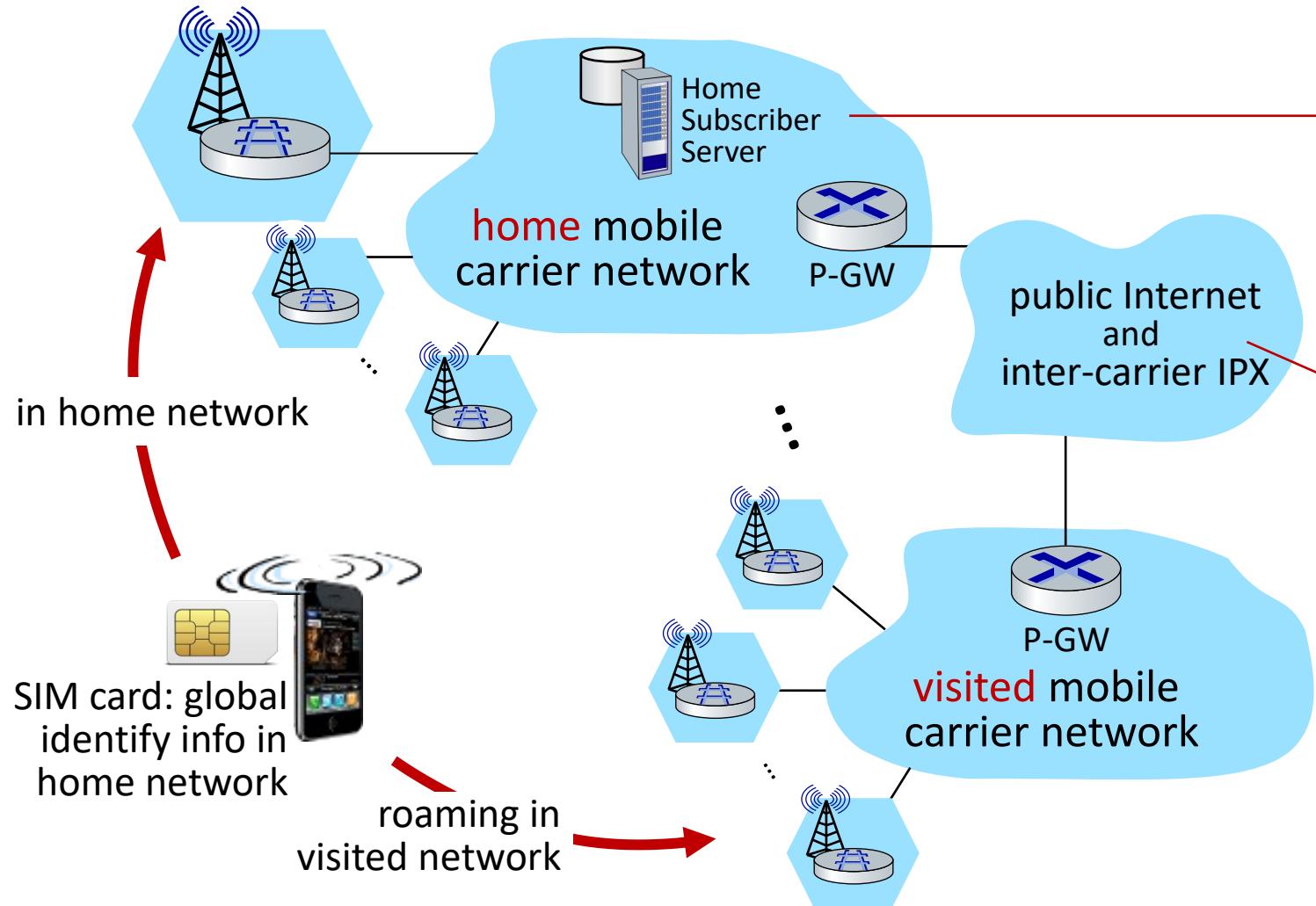
LTE: sleep modes



come in WiFi, Bluetooth: i mobile node LTE possono mettere la radio a “dormire” per preservare la batteria:

- **light sleep:** dopo centinaia di millisecondi di inattività
 - si svelga periodicamente (centinaia di ms) per controllare le trasmissioni downstream
- **deep sleep:** dopo 5-10 secondi of inattività
 - la mobilità può cambiare le celle durante il sonno profondo: è necessario ristabilire l'associazione.

Rete cellulare globale: una rete di reti IP



home network HSS:

- informazioni sull'identificazione e sui servizi, mentre si è nella rete domestica e in roaming

all IP:

- gli operatori si interconnettono tra di loro e on l'internet pubblico nei punti di scambio
- legacy 2G, 3G: non tutto IP, gestito altrimenti

Passaggio al 5G: motivazione

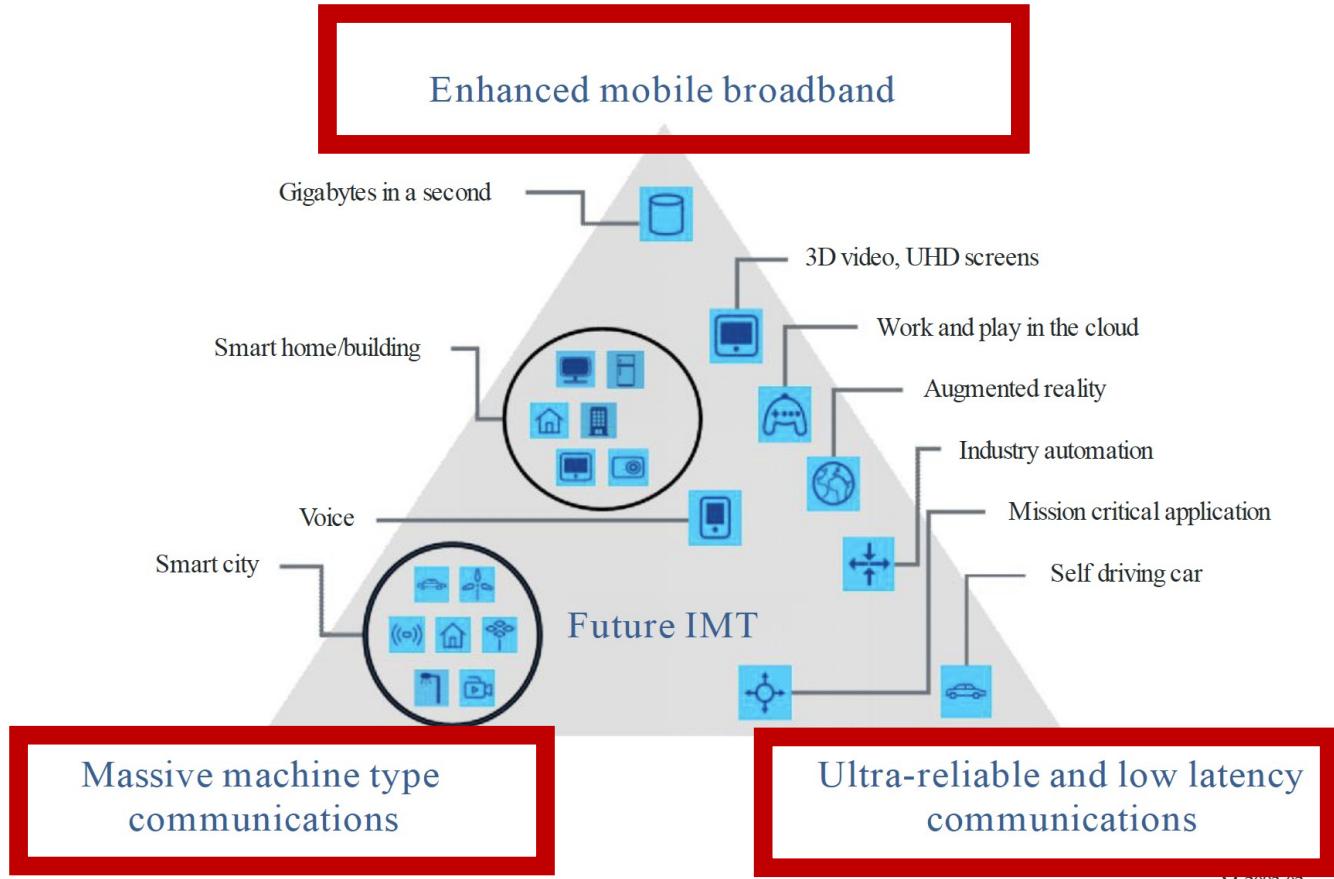


Figure: from Recommendation ITU-R M.2083-0 (2015)

“initial standards and launches have mostly focused on **enhanced Mobile Broadband**, 5G is expected to increasingly enable new business models and countless new use cases, in particular those of **massive Machine Type Communications** and **Ultra-reliable and Low Latency Communications**.”

Passaggio al 5G: motivazione

- **obiettivo:** incremento di 10x del bitrate di picco, riduzione di 10x della latenza, aumento di 100x della capacità di traffico rispetto 4G
- **5G NR (new radio):**
 - due bande di frequenza: FR1 (450 MHz–6 GHz) and FR2 (24 GHz–52 GHz): frequenze delle onde millimetriche
 - non è retrocompatibile con il 4G
 - MIMO: antenne multiple direzionali
- **frequenze delle onde millimetriche:** velocità di trasmissione dei dati molto più elevate, ma su distanze più brevi
 - pico-cell: diametro: 10-100 m
 - necessaria distribuzione massiccia e densa di nuove stazioni di base

Sommario

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth

Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore



Cos'è la mobilità?

- spettro della mobilità, dal punto di vista del **livello di rete**:

nessuna mobilità

alta mobilità

il dispositivo si sposta tra le reti di accesso, ma è spento durante lo spostamento.

all'interno di una sola base station, non c'è neanche mobilità a livello di collegamento

il dispositivo si sposta entro la stessa rete di accesso wireless, in una sola rete di fornitore

il dispositivo si sposta tra reti di accesso in una singola rete di fornitore, mantenendo connessioni in corso

Il dispositivo si sposta tra reti di fornitori differenti, mantenendo connessioni in corso

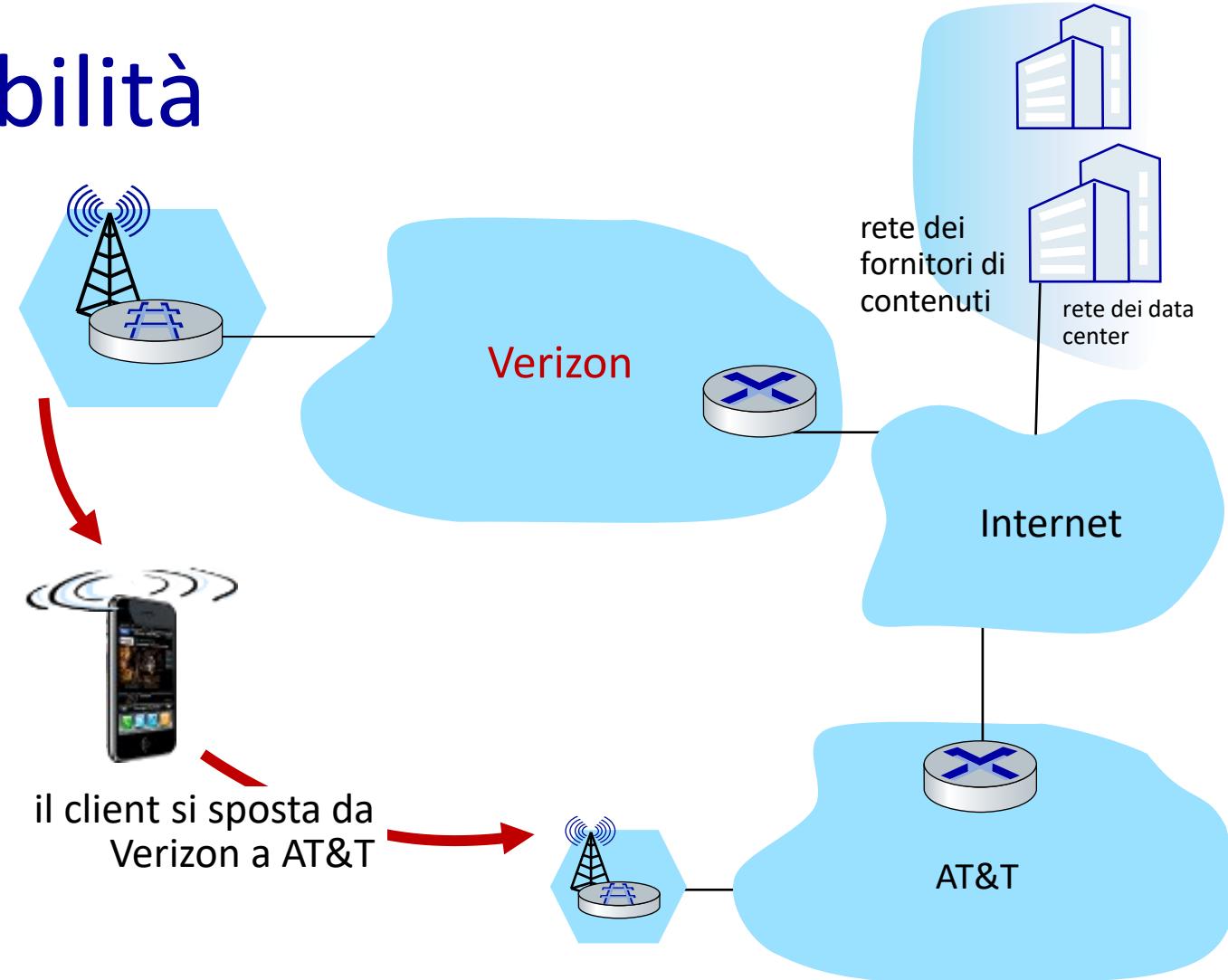
Siamo interessati a questi!



Il problema della mobilità

Se un dispositivo si sposta da una rete all'altra:

- Come farà la “rete” a sapere che deve inoltrare i pacchetti alla *nuova rete*?



Approcci alla mobilità

- **lasciare che sia la rete (i router) a gestirla:**
 - i router annunciano il nome, l'indirizzo IP permanente del nodo mobile in visita tramite lo scambio della tabella di routing
 - quando un dispositivo mobile abbandona una *visited network*, questa ritira la rotta
 - il routing di Internet potrebbe già farlo *senza* alcuna modifica! Le tabelle di routing indicano la posizione di ogni nodo mobile tramite la corrispondenza del prefisso più lungo!

Mobility approaches

- lasciare che sia la rete (i router) a gestirla:
 - i router annunciano il nome e l'indirizzo IP permanente del nodo mobile in visita tramite lo scambio di routing
 - quando un dispositivo mobile entra in una rete visitata, questa ritira la rotta
 - il routing di Internet potrebbe funzionare *senza alcuna modifica!* Le tabelle di routing indicano la posizione di ogni cellulare tramite la corrispondenza del prefisso più lungo!
- **lasciare che siano gli end-system a gestirla:** funzionalità nella "periferia"
 - *instradamento indiretto (indirect routing)*: la comunicazione dal corrispondente al dispositivo mobile attraverso la rete home, viene quindi inoltrata al dispositivo mobile nella rete visitata
 - *instradamento diretto (direct routing)*: il corrispondente ottiene l'indirizzo del dispositivo mobile nella rete visitata, invia direttamente al dispositivo mobile



non
scalabile per
miliardi di
dispositivi

Contattare un amico

Considerate un amico che cambia spesso
domicilio, come lo trovate?

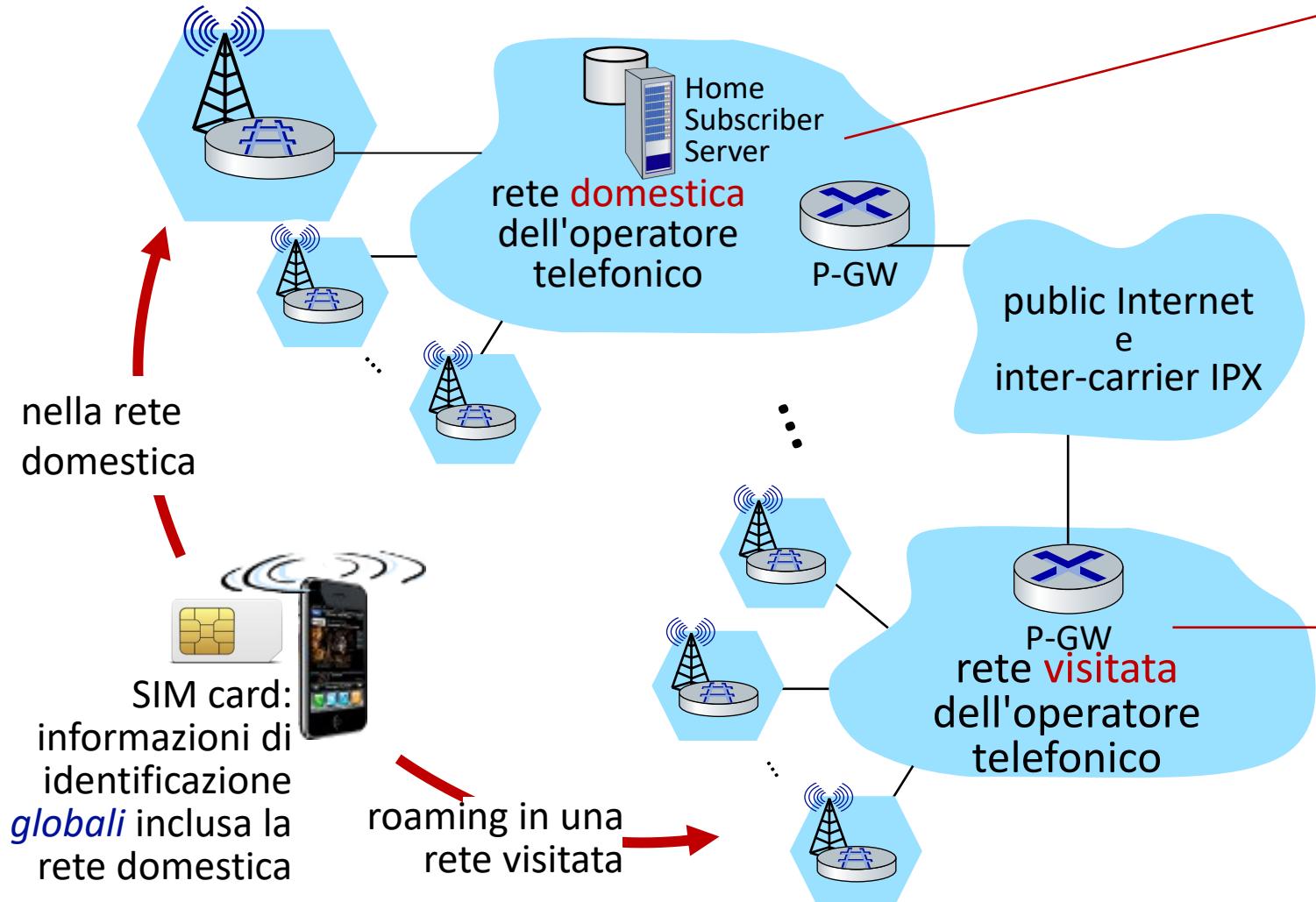
- cercate in tutti gli elenchi telefonici?
- vi aspettate che vi faccia sapere dove sta?
- chiamate i suoi genitori?
- Facebook!

L'importanza di avere una "casa":

- una fonte di informazioni definitive su di voi
- un posto dove le persone possono trovare dove vi trovate



Rete domestica, rete visitata: 4G/5G



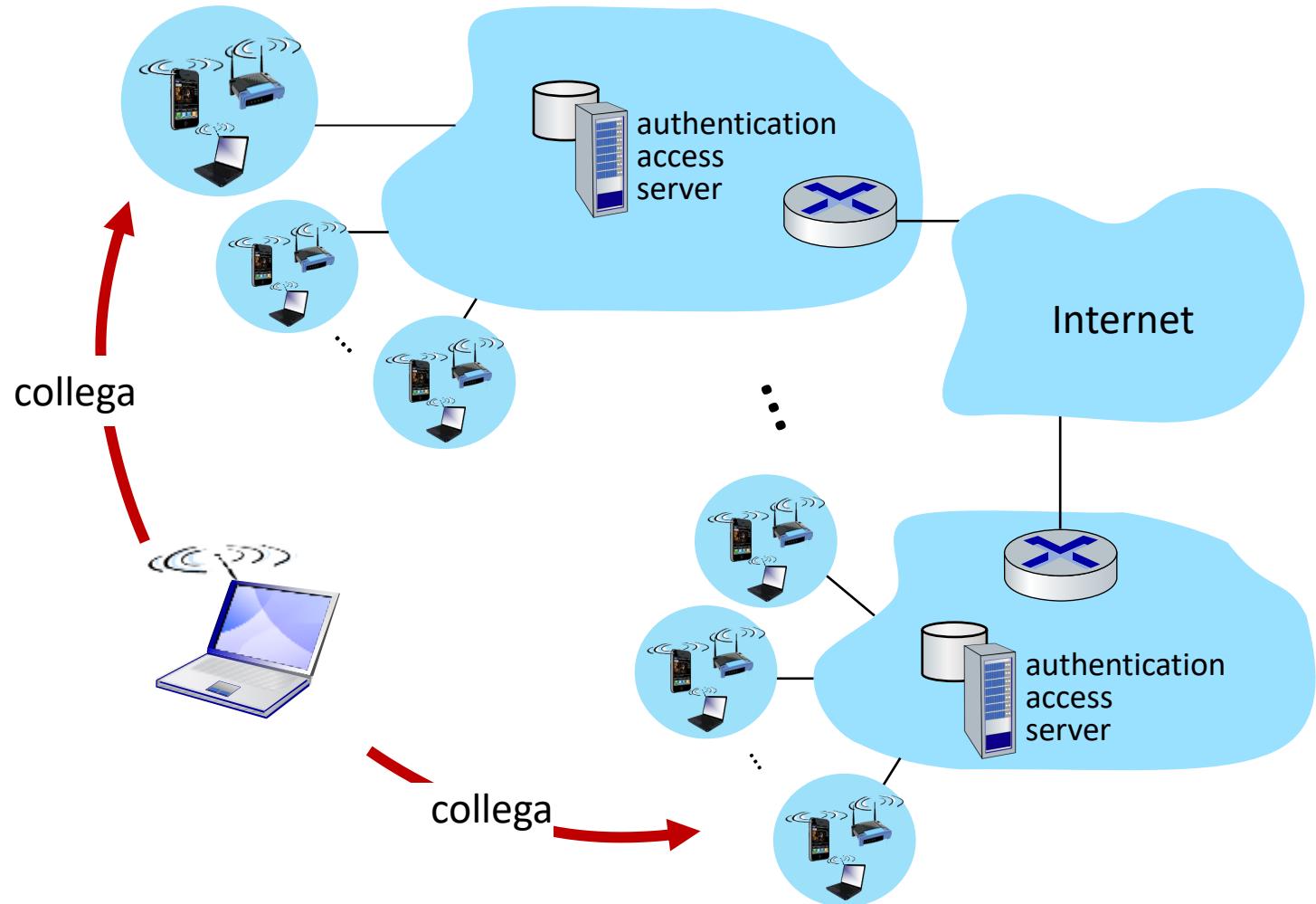
home network (rete domestica):

- piano di servizio (a pagamento) con un operatore di telefonia mobile
- L'HSS della rete domestica memorizza le informazioni circa l'identità e i servizi

visited network (rete visitata):

- qualsiasi altra rete diversa dalla tua rete domestica
- accordo di servizio con altre reti: per fornire l'accesso alla telefonia mobile in visita

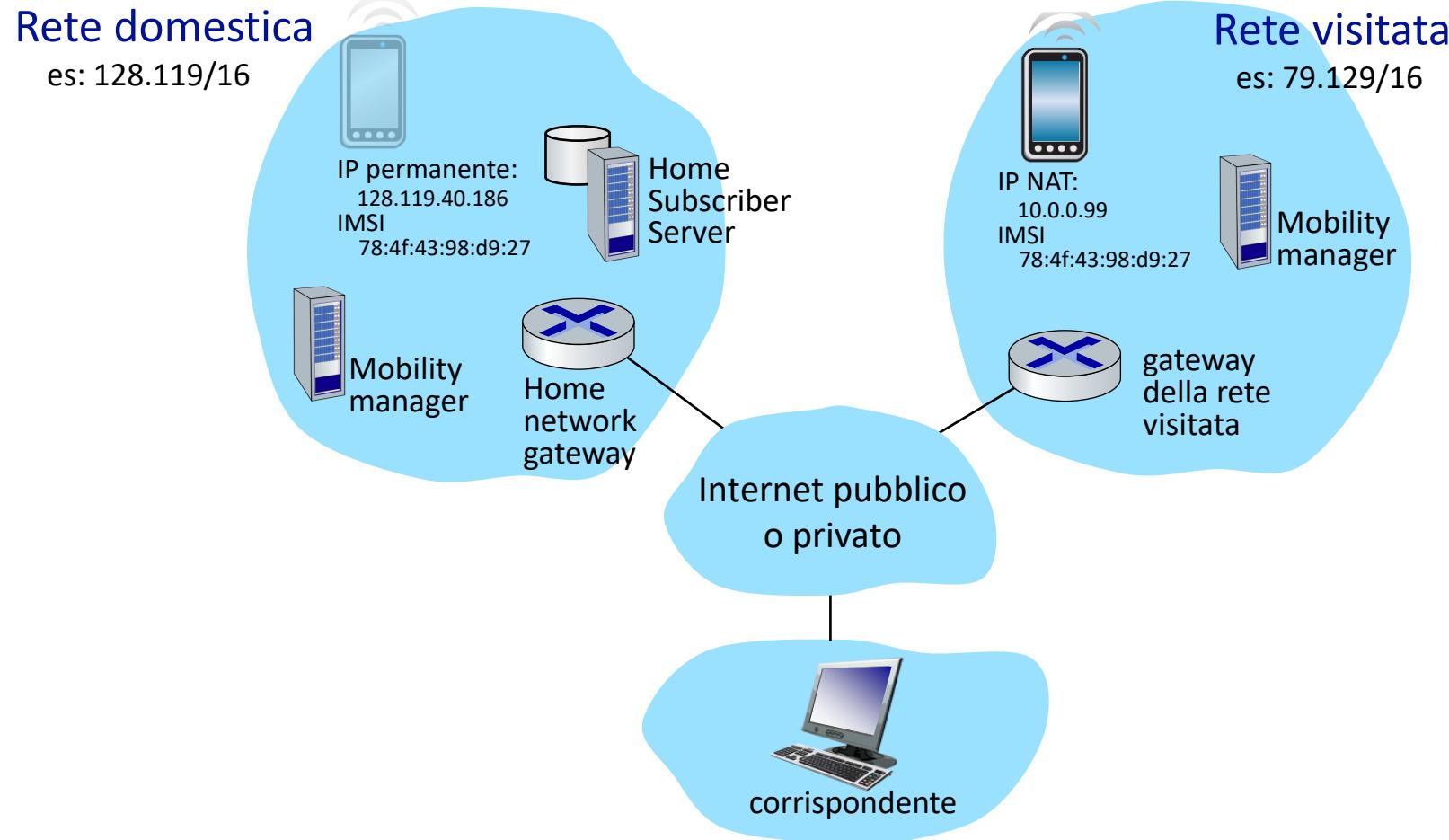
Rete domestica, rete visitata: ISP/WiFi



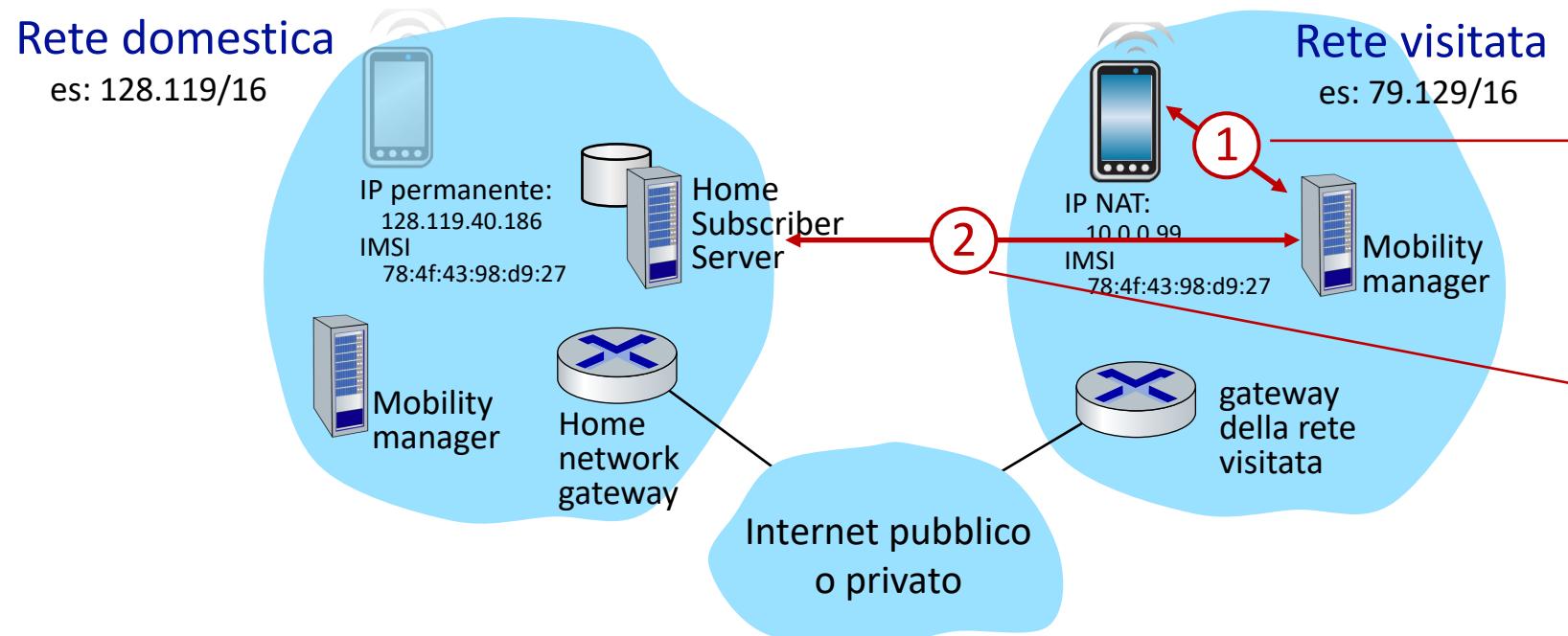
ISP/WiFi: nessuna nozione di "casa"

- credenziali dell'ISP (ad esempio, nome utente, password) memorizzate sul dispositivo o presso l'utente
- gli ISP possono avere una presenza nazionale o internazionale
- reti differenti: credenziali differenti
 - alcune eccezioni (es., eduroam)
 - Esistono architetture (IP mobile) per la mobilità di tipo 4G, ma non sono utilizzate.

Rete domestica, rete visitata: visione generica



Registrazione: casa deve sapere dove stai!



il nodo mobile *si associa* al mobility manager visitato

il mobility manager visitato *registra* la posizione del dispositivo mobile nell'HSS della rete domestica

Risultato finale:

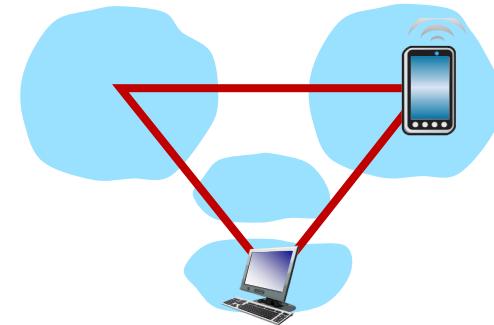
- il mobility manager visitato sa del dispositivo mobile
- l'HSS domestico sa la posizione del dispositivo mobile

Mobilità con routing indiretto

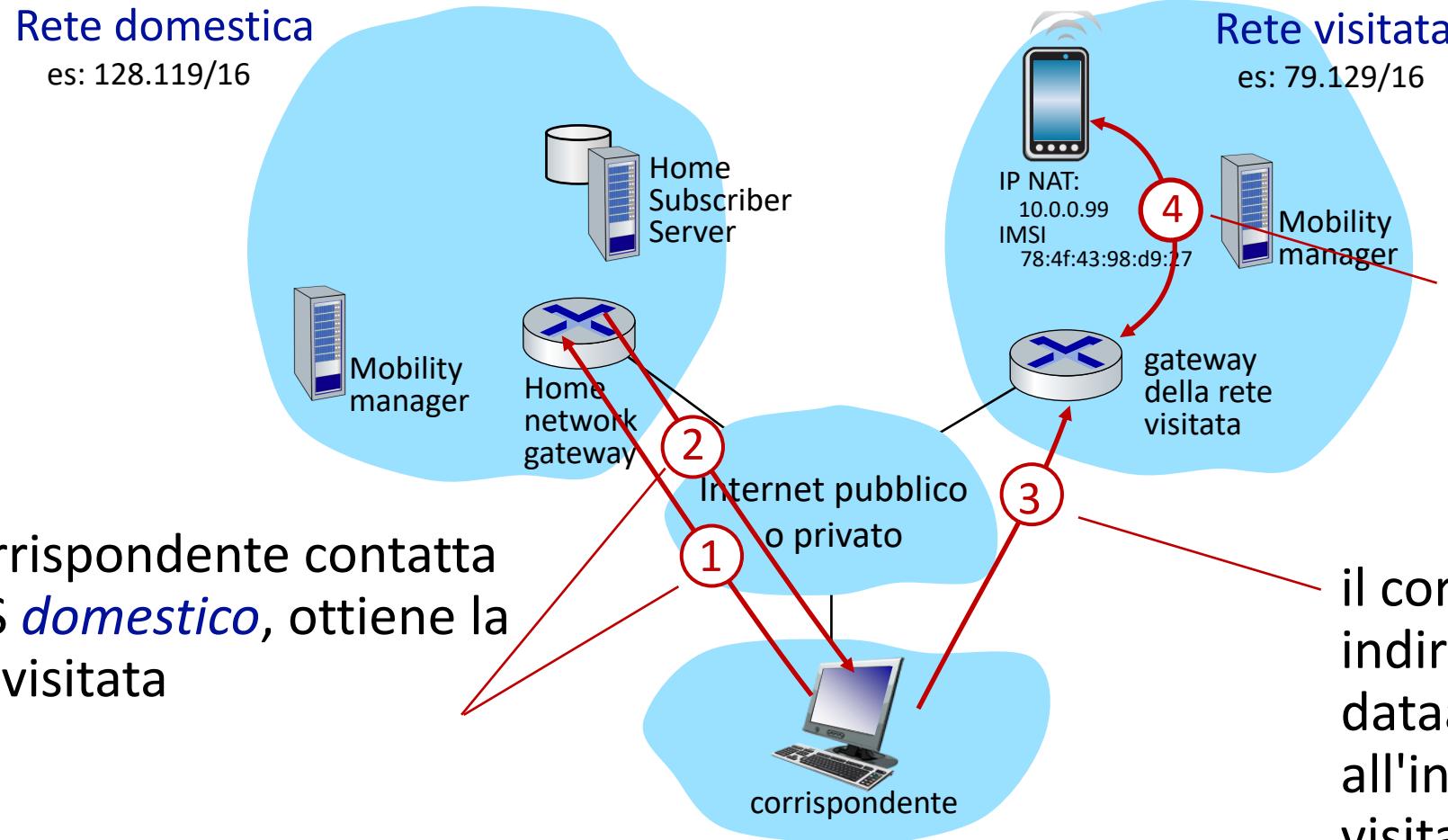


Mobilità con routing indiretto: commenti

- instradamento triangolare (triangular routing):
 - inefficiente se il corrispondente e il dispositivo mobile sono nella stessa rete
- Il dispositivo mobile si sposta tra reti visitate: trasparente al corrispondente!
 - si registra in una nuova rete visitata
 - la nuova rete visitata si registra presso l'HSS domestico
 - i datagrammi continuano a essere inoltrati dalla rete domestica al dispositivo mobile nella nuova rete
 - *connessioni (es., TCP) in corso tra il corrispondente e il dispositivo mobile possono essere mantenute!*



Mobilità con routing diretto



Il corrispondente contatta l'HSS *domestico*, ottiene la rete visitata

Il router gateway visitato inoltra al dispositivo mobile

il corrispondente indirizza il dataagramma all'indirizzo della rete visitata

Mobilità con routing diretto: commenti

- supera le inefficienze dell'instradamento triangolare
- *non-transparente al corrispondente*: il corrispondente deve ottenere l'indirizzo care-of (nella rete vistata) dall'agente domestico
- che succede se il dispositivo mobile cambia rete?
 - può essere gestito, ma aggiunge complessità

Sommario

- Introduzione

Wireless

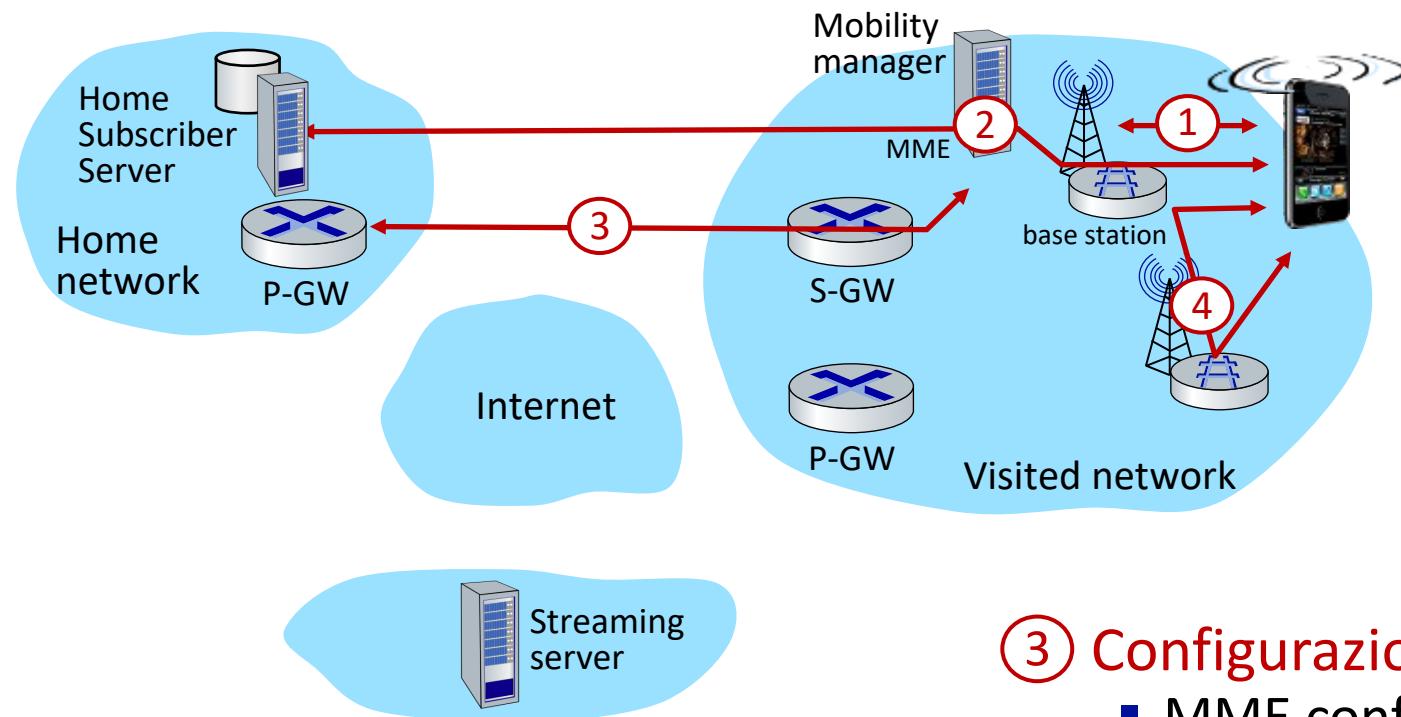
- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth

Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore



Mobilità nelle reti 4G: compiti di mobilità principali



④ mobile handover:

- il dispositivo mobile cambia il proprio punto di aggancio nella rete visitata

① associazione alla stazione base:

- il dispositivo mobile fornisce l'IMSI – identificando se stesso e la home network

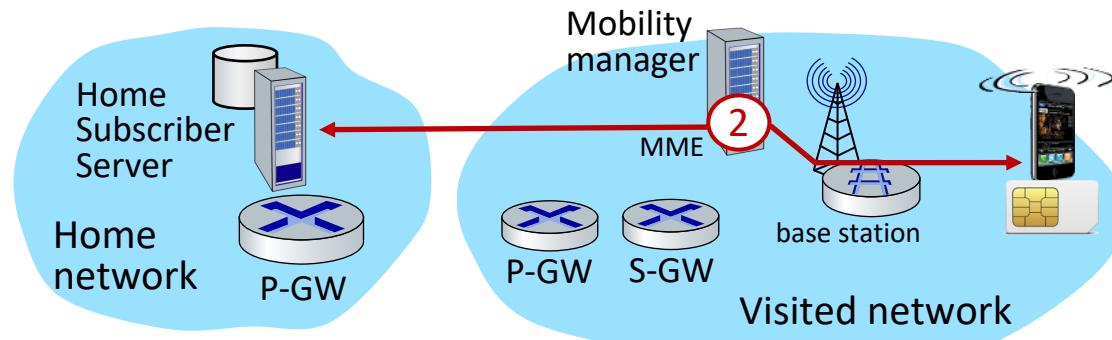
② Configurazione del piano di controllo:

- MME, home HSS stabiliscono lo stato del piano di controllo - il mobile device è nella visited network

③ Configurazione del piano di dati:

- MME configura tunnel di inoltro per il dispositivo mobile
- la visited network e la home network stabiliscono tunnel da home P-GW a cellulare

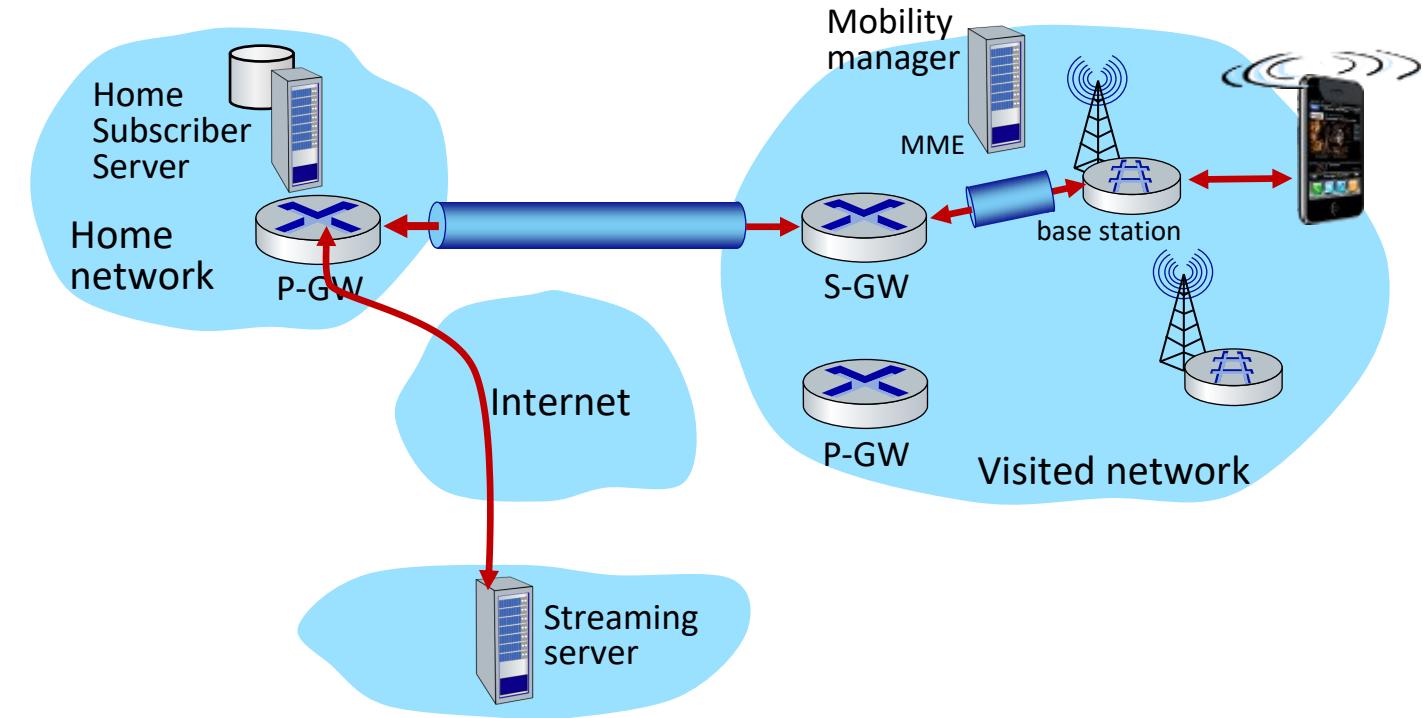
Configuring LTE control-plane elements



- Il dispositivo mobile comunica con l'MME locale attraverso il canale del piano di controllo con la BS
- l'MME usa l'informazione sull'IMSI del dispositivo mobile per contattare l'HSS della home network del dispositivo
 - Recupera informazioni per l'autenticazione, la cifratura e i servizi di rete
 - L'HSS nella home network sa ora che il dispositivo mobile è residente nella visited network
- La BS e il dispositivo mobile selezionano i parametri per il canale radio tra BS e dispositivo mobile nel piano di dati

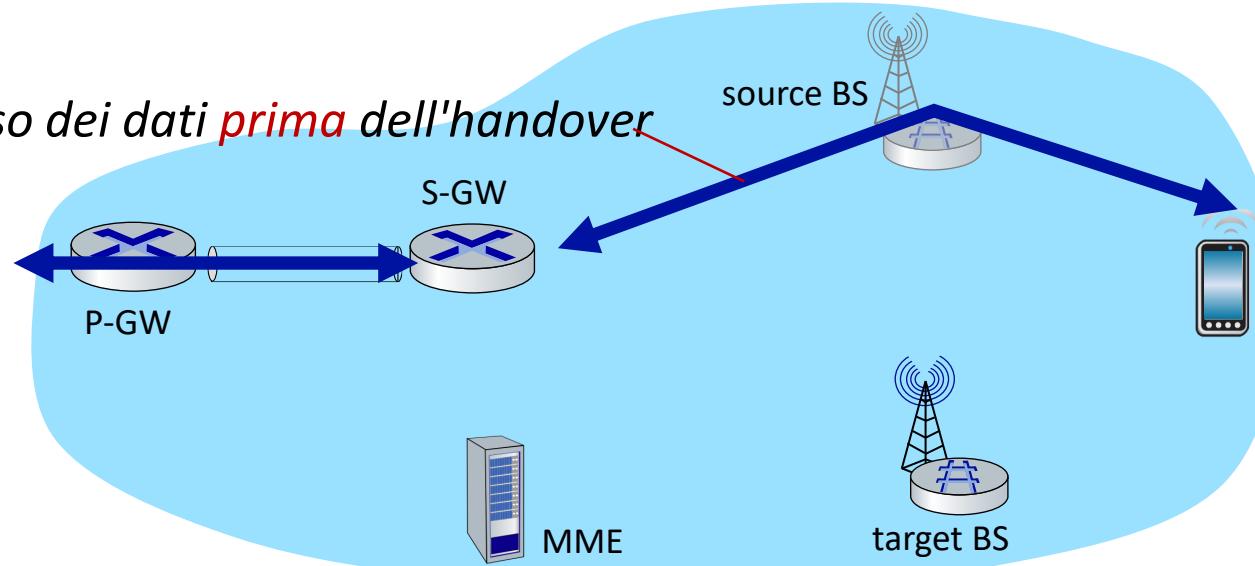
Configurazione dei tunnel del piano dati per un cellulare

- **tunnel da S-GW a BS:**
quando il dispositivo mobile cambia stazione base, semplicemente cambia l'indirizzo IP dell'estremità del tunnel
- **tunnel da S-GW a home P-GW tunnel:**
implementazione dell'instradamento indiretto
- **tunneling attraverso GTP (GPRS tunneling protocol):** il datagramma del dispositivo mobile al server di streaming incapsulato utilizzando GTP all'interno di UDP, all'interno del datagramma

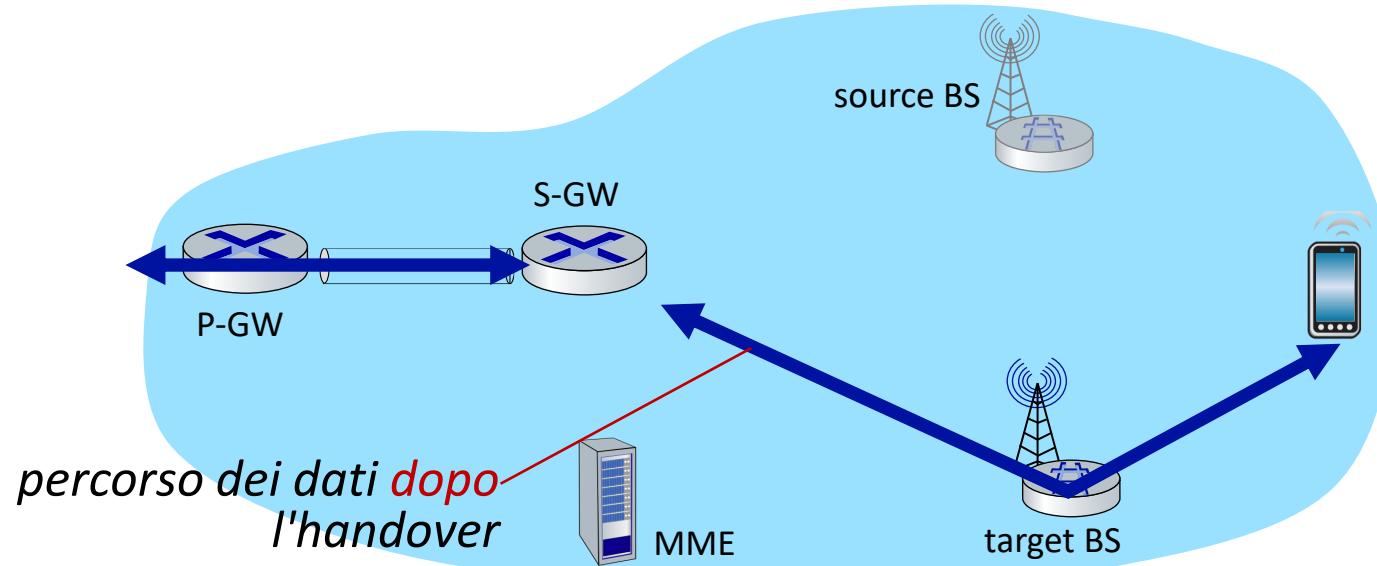


Handover tra BS nella stessa rete cellulare

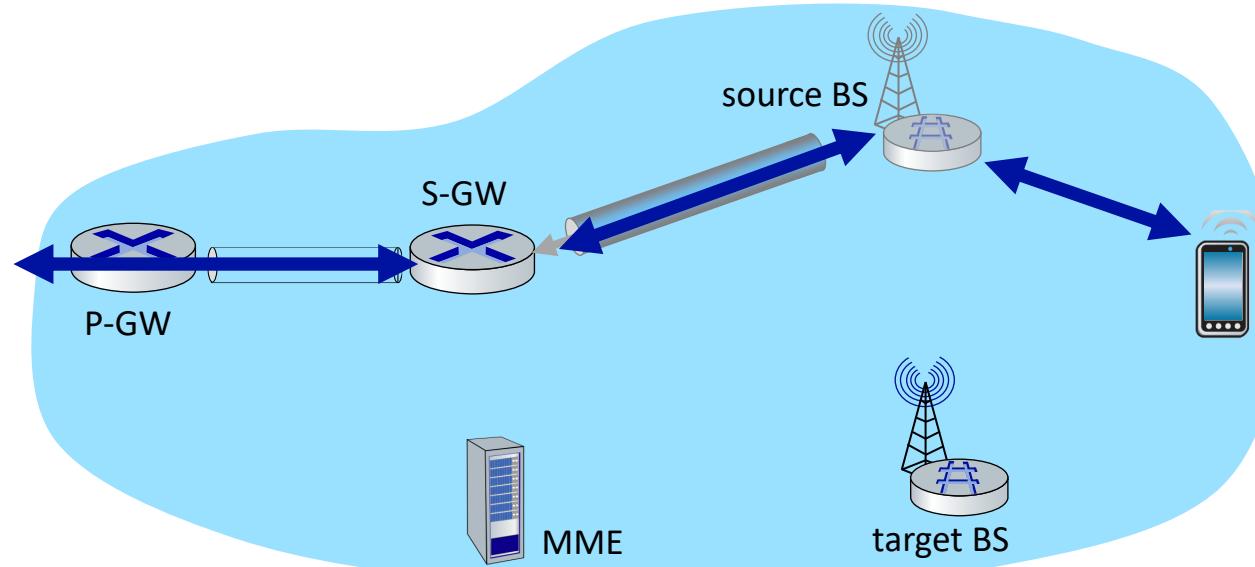
percorso dei dati prima dell'handover



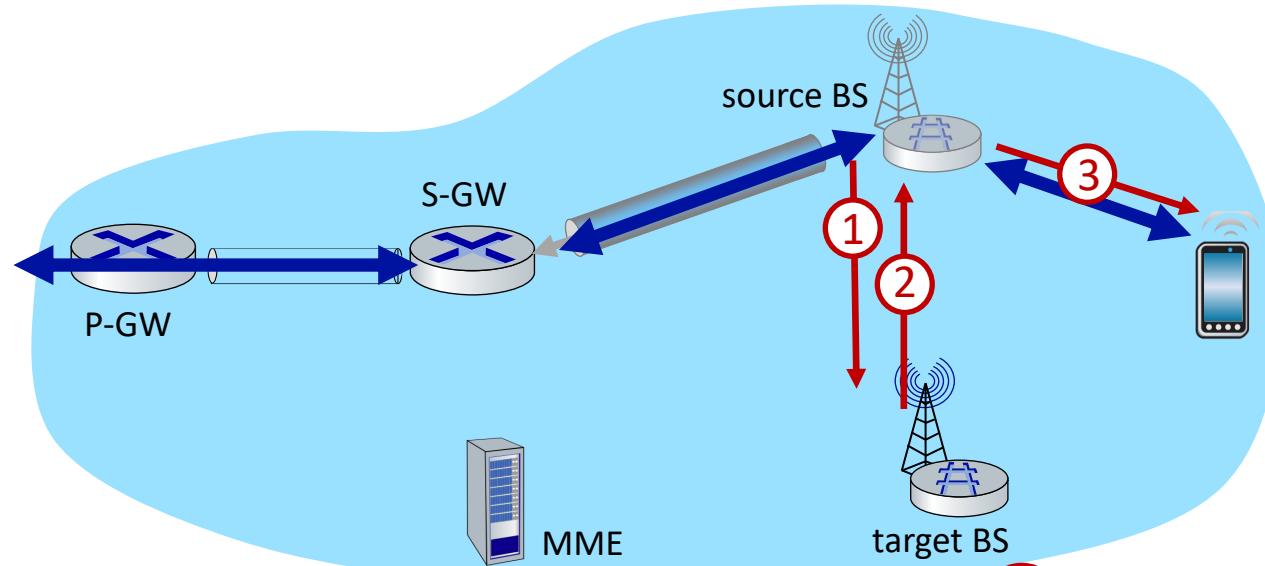
Handover tra BS nella stessa rete cellulare



Handover tra BS nella stessa rete cellulare

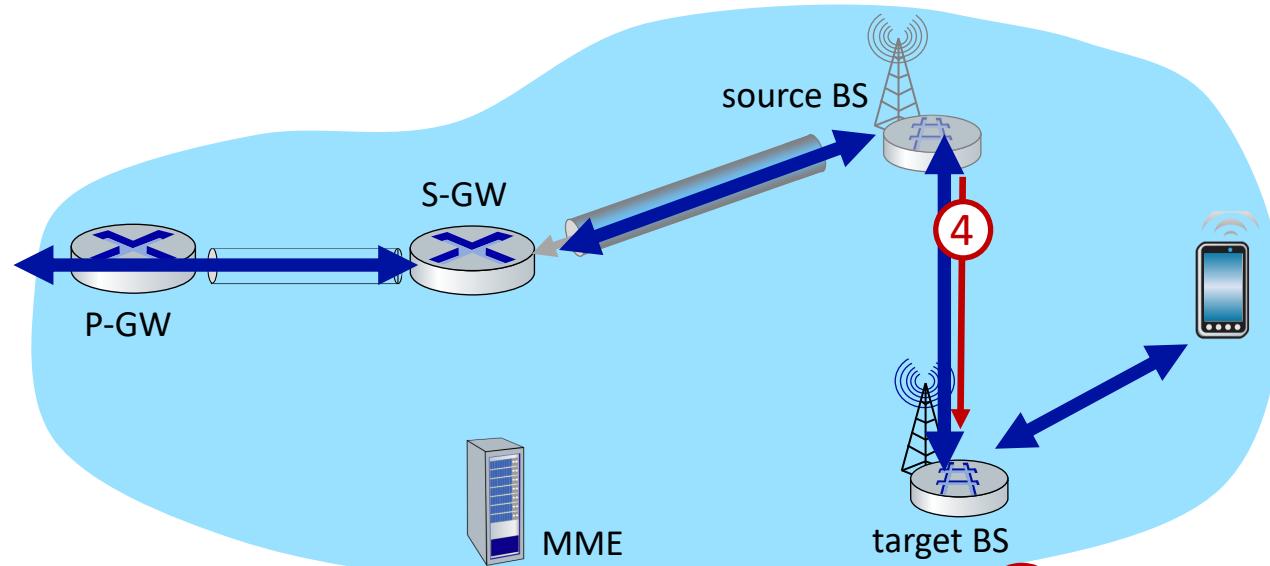


Handover tra BS nella stessa rete cellulare



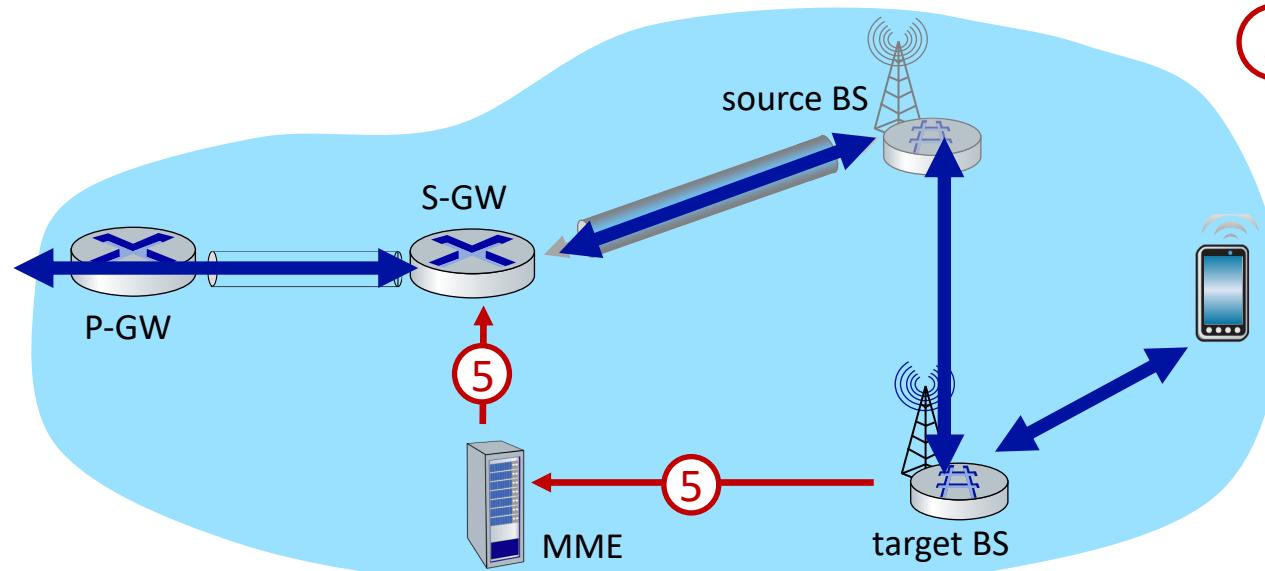
- ① la BS corrente (source) seleziona il BS target, invia un messaggio di *Richiesta di Handover* al BS target
- ② la BS target pre-alloca slot temporali nel canale radio, risponde con un ACK con informazioni necessarie al dispositivo mobile per associarsi alla nuova BS
- ③ la BS source informa il dispositivo mobile della nuova stazione base
 - il dispositivo mobile può ora inviare attraverso la nuova BS - handover *appare* completo al dispositivo mobile

Handover tra BS nella stessa rete cellulare



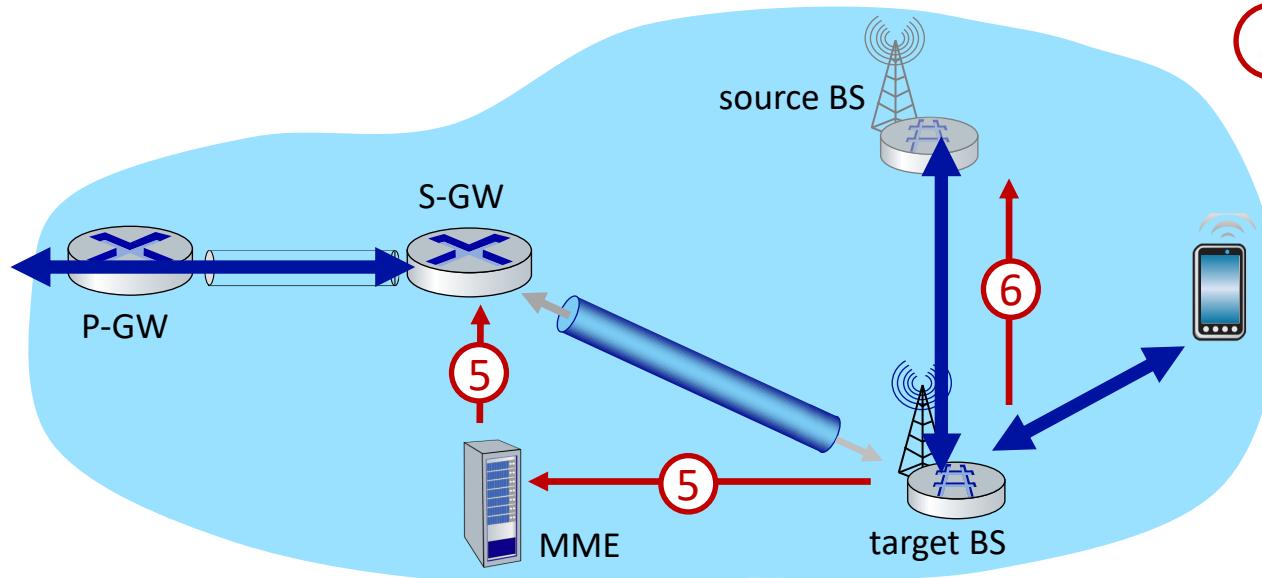
- ① la BS corrente (source) seleziona il BS target, invia un messaggio di *Richiesta di Handover* al BS target
- ② la BS target pre-alloca slot temporali nel canale radio, risponde con un ACK con informazioni necessarie al dispositivo mobile per associarsi alla nuova BS
- ③ la BS source informa il dispositivo mobile della nuova stazione base
 - il dispositivo mobile può ora inviare attraverso la nuova BS - handover *appare* completo al dispositivo mobile
- ④ la BS source smette di inviare datagrammi al cellulare, inoltra invece alla nuova BS (che inoltra al dispositivo mobile attraverso il canale radio)

Handover tra BS nella stessa rete cellulare



- ⑤ la BS target informa l'MME che è la nuova BS per il dispositivo mobile
- l'MME istruisce l'S-GW per cambiare l'estremità del tunnel alla (nuova) BS target

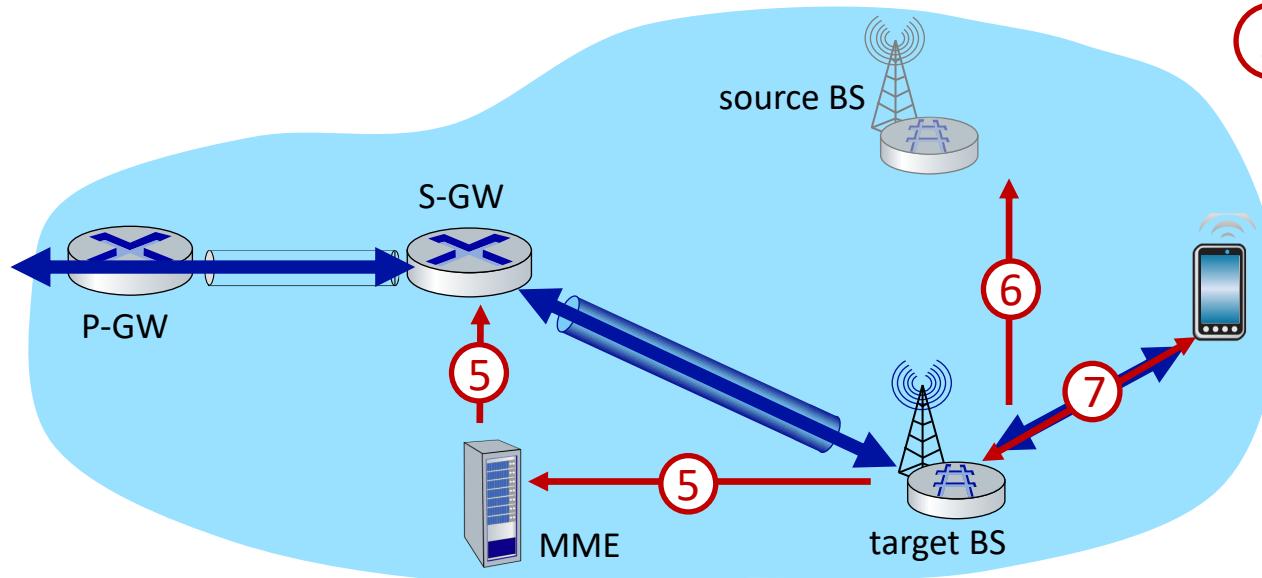
Handover tra BS nella stessa rete cellulare



- ⑤ la BS target informa l'MME che è la nuova BS per il dispositivo mobile
- l'MME istruisce l'S-GW per cambiare l'estremità del tunnel alla (nuova) BS target

- ⑥ la BS target manda un ACK indietro alla BS source: handover completo, la BS source può rilasciare le risorse

Handover tra BS nella stessa rete cellulare



- ⑤ la BS target informa l'MME che è la nuova BS per il dispositivo mobile
- l'MME istruisce l'S-GW per cambiare l'estremità del tunnel alla (nuova) BS target

- ⑥ la BS target manda un ACK indietro alla BS source: handover completo, la BS source può rilasciare le risorse
- ⑦ i datagrammi del dispositivo mobile ora fluiscano attraverso il nuovo tunnel dal BS target all'S-GW

Mobile IP

- L'architettura di mobile IP standardizzata ~20 anni fa [RFC 5944]
 - Molto prima degli smartphone ubiqi e del supporto del 4G ai protocolli di Internet
 - Non ha visto un grande dispiegamento/uso
 - forse WiFi per Internet, e cellulari 2G/3G per la voce erano “sufficientemente buoni” al tempo
- architettura di mobile IP:
 - routing indiretto al nodo (attraverso la home network) usando tunnel
 - mobile IP home agent: combina i ruoli dell'HSS e dell'home P-GW in 4G
 - mobile IP foreign agent: combina i ruoli dell'MME e dell'S-GW in 4G
 - Protocolli per agent discovery nelle visited network, registrazione della posizione visitata nella home network attraverso estensioni di ICMP

Wireless, mobilità: impatto sui protocolli di livello superiore

- logicamente, l'impatto *dovrebbe* essere minimo...
 - il modello di servizio best effort service model resta inalterato
 - TCP e UDP possono girare (e in effetti lo fanno) sul wireless e il mobile
- ... ma dal punto di vista delle prestazioni:
 - perdita/ritardo di pacchetti a causa di errori sui bit (pacchetti scartati, ritardi a causa di ritrasmissioni a livello di collegamento), e perdite di handover
 - TCP interpreta le perdite come congestione, riducendo la finestra di congestione senza motivo. Soluzioni:
 - recupero locale (infatti Wi-Fi implementa il trasferimento di dati affidabile)
 - consapevolezza del mittente dei collegamenti wireless (es. distinguendo le perdite causate dal wireless dalle perdite per congestione)
 - split connection (la connessione end-to-end divisa in una connessione da un capo all'access point wireless e una connessione dall'access point wireless all'altro capo)
 - traffico in tempo reale danneggiato dai ritardi
 - data la natura condivisa del canale wireless, occorre che le applicazione considerino la larghezza di banda come una risorsa scarsa

Riassunto

- Introduzione

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G
- Bluetooth

Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore



Riassunto

Wireless

- Collegamenti wireless e caratteristiche della rete
- WiFi: 802.11 wireless LAN
- Reti cellulari: 4G e 5G

Mobilità

- Gestione della mobilità: principi
- Gestione della mobilità: pratica
 - Reti 4G/5G
 - Mobile IP
- Mobilità: impatto sui protocolli di livello superiore

