

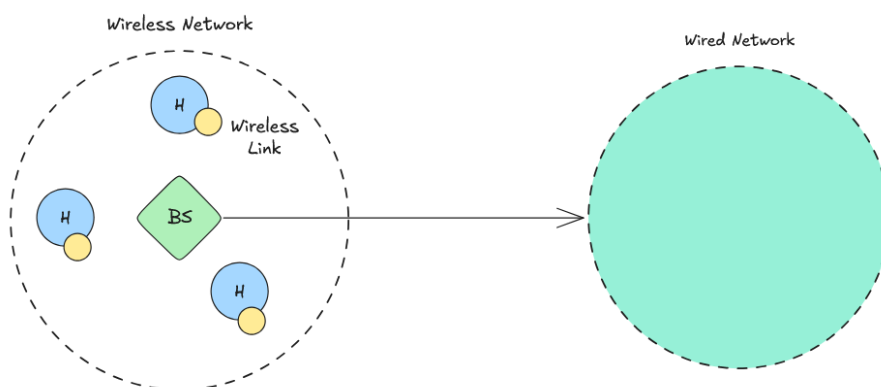
Wireless

Le principali sfide di una connessione senza fili sono:

- **Wireless:** dobbiamo gestire comunicazioni basate sul wireless
- **Mobilità:** gestire utenti che si muovono da un'area a un'altra.

Elementi di una rete wireless

- **Wireless host:** eseguono applicazioni e possono essere mobili o no.
- **Base station:** tipicamente connessa a una wired network responsabile di inviare pacchetti tra la wired network e i wireless host vicini.
- **Wireless link:** servono per connettere gli host alle base station. Un protocollo di accesso multiplo coordina l'accesso al collegamento, vengono supportate diverse velocità e frequenze di trasmissione tra gli host e la base station.



Modalità infrastruttura

Le base station sono collegate fisicamente a una rete, che poi si collega a un ISP, ogni base station copre una determinata area dopo la quale se la rete è ben strutturata avviene un **handoff** ovvero che se il cellulare dell'utente era connesso alla BS1 ora è sotto la copertura della BS2 e così via.

Modalità ad hoc

Non abbiamo un punto di connessione centrale ma ogni dispositivo funge da base station, ovvero che copre una determinata area e il segnale passa da questa copertura, se un dispositivo si allontana troppo interrompe il collegamento.

Tipo di rete	Single Hop	Multiple Hops
Con infrastruttura	L'host si connette a una stazione base (WiFi, cellulare), che a sua volta è connessa a Internet.	L'host deve inoltrare i dati attraverso più nodi wireless per raggiungere Internet (mesh networks).
Senza infrastruttura	Non c'è una stazione base e non c'è connessione a Internet. Esempi: Bluetooth, reti ad hoc .	Non c'è una stazione base né connessione a Internet. Esempi: VANET (Vehicular Ad hoc Networks) .

Caratteristiche dei collegamenti wireless

Abbiamo delle differenze sostanziali dai collegamenti con cavo, dove i dati viaggiavano su un canale fisico, tra cui vediamo principalmente:

- **Forza del segnale ridotta:** il segnale radio si va ad attenuare mentre si propaga. (**path loss**)

- **Interferenze da altre sorgenti:** abbiamo le stesse frequenze usate da dispositivi diversi.
- **Propagazione multipath:** il segnale radio si riflette sugli oggetti, arrivando a destinazione con tempi diversi.

Queste complicazioni rendono la comunicazione più difficile nonostante sia **Point-to-Point** e quindi diretta con la destinazione.

SNR e BER

Il **SNR (Signal-to-Noise Ratio)** misura la qualità del segnale rispetto al rumore, mentre il **BER (Bit Error Rate)** indica la percentuale di errori nella trasmissione: all'aumentare del SNR, il BER diminuisce, ma trasmissioni più affidabili richiedono mezzi più costosi, creando un trade-off tra qualità e costo. Un SNR maggiore permette una estrazione del segnale dal noise migliore.

Problemi con le reti wireless

Ci sono due problemi principali, il primo è quello del **terminale nascosto**, il secondo è **l'attenuazione del segnale**.

- **Problema del terminale nascosto:** si verifica quando due dispositivi (ad esempio **A** e **C**) **non riescono a rilevare** la presenza reciproca, ma entrambi interferiscono su un terzo dispositivo (**B**).
- **Attenuazione del segnale:** il segnale wireless si attenua man mano che la distanza tra i dispositivi aumenta. Questo porta a problemi di comunicazione.

Code Division Multiple Access (CDMA)

CDMA è un **una modalità di accesso al canale** usa un codice assegnato a ogni utente. Tutti gli utenti **condividono la stessa frequenza** ma ognuno ha la propria **sequenza di chipping** per codificare i dati così da far coesistere più utenti contemporaneamente e avere interferenze minime.

1. **Encoding** (Codifica): ogni utente codifica i propri dati moltiplicando il **dato originale** per la **chipping sequence**.
2. **Decoding** (Decodifica): al ricevitore, il segnale viene **decodificato** con i dati ricevuti e la **chipping sequence** del mittente. Il destinatario è in grado di **estrarre il segnale del destinatario specifico**, ignorando quelli degli altri utenti.

La vera utilità si vede in questa situazione, ovvero **quando due** (o più dispositivi) **inviano** dati alla **stessa destinazione** ma la **destinazione** vuole solo **leggere** i dati di un **dispositivo** in quel momento, utilizza il **suo codice** per **estrarre** solo i suoi dati.

802.11 Architettura LAN

Gli host wireless comunicano con la **base station** (che fa da access point) e sono all'interno di una **BSS** (Base Service Set) in modalità **infrastruttura** che contiene gli **host** wireless e la **base station**. Una **BSS in ad hoc** mode invece **contiene solo gli host**.

Associazione di canali

Lo **spettro delle reti Wi-Fi** è diviso in frequenze diverse, scelte da colui che implementa la BSS, quando un nuovo host entra nella BSS accade:

- Esegue una scansione dei canali in ascolto dei **beacon frame** ovvero frame inviati **dall'AP** che contengono il **SSID** (nome della rete) e il **MAC dell'AP**.
- Dato che le BSS possono sovrapporsi in alcuni punti l'host sceglie la migliore in base alla potenza di segnale.
- Si **autentica** se l'AP richiede delle credenziali.
- **Richiede un IP** tramite DHCP Discovery da cui riceve le informazioni, il server DHCP può essere interno o esterno alla BSS.

802.11 Scanning attivo e passivo

Scanning passivo

1. I **beacon frame** sono **inviati dall'AP**.
2. **Host** invia una **richiesta** di associazione con Association Request.
3. L'AP risponde con l'accettazione della richiesta con Association Response .

Scanning attivo

1. L'host invia in **broadcast** un **Probe Request**
2. **Gli AP rispondono** con un **Probe Response**.
3. **Host** invia una **richiesta** di associazione con Association Request.
4. L'AP risponde con l'accettazione della richiesta con Association Response .

802.11 Accesso multiplo

Bisogna evitare le collisioni a tutti i costi quando due o più nodi trasmettono allo stesso dispositivo, 802.11 utilizza un protocollo CSMA ovvero "ascolta prima di trasmettere" tuttavia non c'è una collision detection nelle reti 802.11 perchè è difficile accorgersi della collisione. Abbiamo attenuazione del segnale oppure c'è un altro nodo di cui non rilevo la trasmissione.

802.11 CSMA/CA

Lato mittente

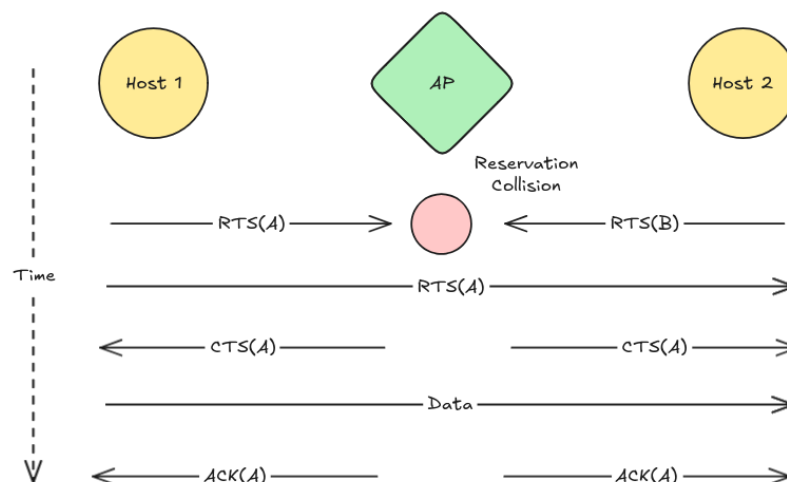
1. Se il canale è inattivo (idle) per il tempo di attesa DIFS (Distributed Inter-Frame Space), trasmette tutto il frame senza fare CD.
2. Se il canale è attivo (busy) inizializza un timer randomico di backoff, che si decrementa solo quando il canale è idle, trasmette quando si azzera e se non riceve ACK incrementa il backoff e ripete questo punto.

Lato destinatario

- Se il frame ricevuto è OK ritorna un ACK dopo un SIFS (Short Inter-Frame Space), al mittente serve per capire se il suo frame è stato letto a causa del terminale nascosto non sa se altri stanno inviando al suo destinatario.

Per evitare collisioni (CA) possiamo riservare il canale usando il **reservation packet**:

- Il sender prima manda un piccolo pacchetto **request-to-send** (RTS) alla base station (BS) usando CSMA, i pacchetti RTS possono collidere tra loro ma dura per poco tempo.
- La base station manda in broadcast un **clear-to-send** (CTS) come risposta a tutti gli host. Così il sender invia e gli altri aspettano.



802.11 Frame Addressing

Un frame **802.11 Wi-Fi** include fino a **4 indirizzi MAC**, a seconda della modalità di trasmissione.



- **Address 1:** Indirizzo MAC del dispositivo che **deve ricevere i dati**.
- **Address 2:** Indirizzo MAC del dispositivo che **sta inviando i dati**.
- **Address 2:** Indirizzo MAC dell'**interfaccia del router** a cui è collegato l'AP.
- **Address 4:** Utilizzato solo quando **due dispositivi comunicano direttamente senza AP**.
- **Frame control:** Indica il **tipo di frame** (es. RTS, CTS, ACK, DATA).
- **Duration:** Indica **per quanto tempo il canale è riservato** con RTS.
- **Sequenze control:** serve per il trasferimento affidabile, ritrasmissione in caso di perdita.
- **Payload:** Contiene i **dati effettivi** trasmessi tra mittente e destinatario.
- **CRC:** Campo per il **controllo degli errori**, per l'integrità.

Mobilità dentro la stessa subnet

Se un host si sposta tra più AP nella stessa rete, il suo **IP non cambia** perché la subnet è definita dal router non dalla BSS. Lo **switch aggiorna automaticamente** la porta associata al MAC dell'host grazie al meccanismo di **self-learning**.

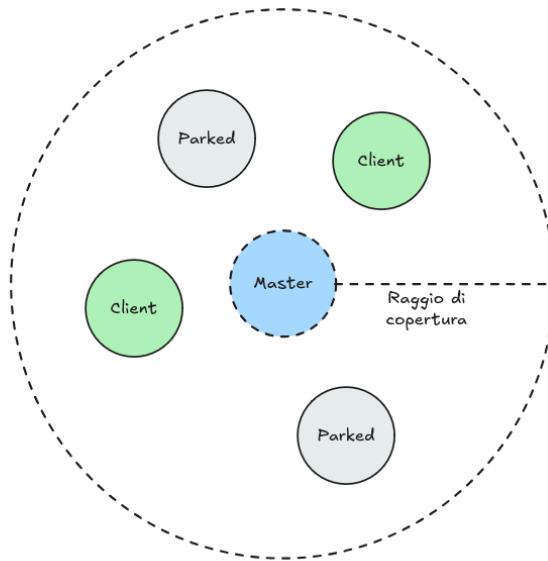
802.11 Abilità avanzate

- **Rate Adaptation:**
 - La **Base Station (BS)** e i dispositivi mobili **adattano la velocità di trasmissione** in base alla qualità del segnale.
 - Se lo **SNR diminuisce**, il **BER aumenta**, indicando un peggioramento del segnale.
 - Se il **BER diventa troppo alto**, la rete riduce la velocità di trasmissione per migliorare l'affidabilità.
- **Power Management:**
 - Il nodo può comunicare all'**AP** che entrerà in **sleep mode** fino al prossimo **Beacon Frame**.
 - L'AP sa quindi che **non deve trasmettere** dati al nodo finché non si risveglia.
 - Il **Beacon Frame** contiene la lista dei dispositivi con dati in attesa.
 - Il nodo si sveglia solo se ci sono frame per lui, altrimenti resta in sleep fino al successivo Beacon Frame.

Il **Beacon Frame** è un pacchetto inviato periodicamente dagli **Access Point (AP)** per annunciare la loro presenza e trasmettere informazioni di rete ai dispositivi Wi-Fi.

Area personale Bluetooth

Il **Bluetooth** copre circa **10 metri** ed è usato per sostituire cavi in dispositivi come **mouse, tastiere e cuffie**. Funziona in modalità **ad hoc**, con un **master controller** che gestisce i dispositivi **client (slave)**. Utilizza **TDM** con slot da **625 µs** e **FDM** su **79 frequenze** per ottimizzare la trasmissione. I client possono entrare in **Parked Mode** per risparmiare energia e riattivarsi quando necessario. Grazie al **bootstrapping**, si connettono automaticamente alla **piconet** in modalità **plug & play**.

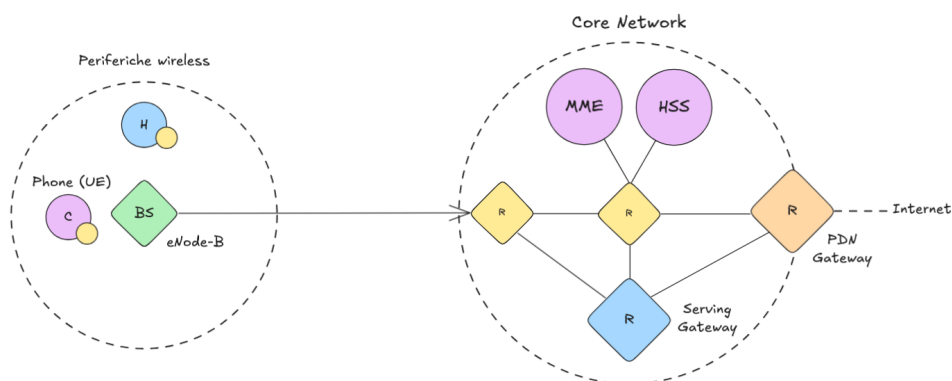


Rete cellulare

La rete cellulare 4G/5G presenta delle **similitudini** con la rete internet cablata.

- **Similitudini:** stessi protocolli, rete di reti, periferiche che fanno capo a una core.
- **Differenze:** connessione wireless, mobilità delle periferiche, gli utenti si sottoscrivono a un fornitore di servizi cellulari.

Elementi di una rete cellulare 4G LTE



- **Mobile Device:** dispositivi che supportano il 4G, id univoco ovvero il **IMSI** (International Mobile Subscriber Identity) salvata sulla SIM card. Si chiama **UE** (User Equipment) in LTE.
- **Base Station:** Nodo all'**edge** della rete mobile. Chiamato **eNode-B** in LTE.
- **Home Subscriber Service (HSS):** Memorizza le informazioni sui device se sono Home network, lavora assieme al MME per l'autenticazione. Questo è un database con le informazioni da servire al MME quando necessario.
- **Mobility Management Entity (MME):** Autenticazione dei dispositivi con HSS della Home network, gestisce il **tracking** del dispositivo per sapere la cella e l'**handover** ovvero lo spostamento tra esse. Prende la posizione attuale dal HSS quando ad esempio il UE si trova in una visited e in oltre gestisce i tunnel.
- **Serving Gateway (S-GW) e PDN Gateway (P-GW):**

- **S-GW:** Smista i dati tra il dispositivo mobile e la rete core.
- **P-GW:** Funziona come gateway verso Internet, applica NAT e assegna IP ai dispositivi mobili.

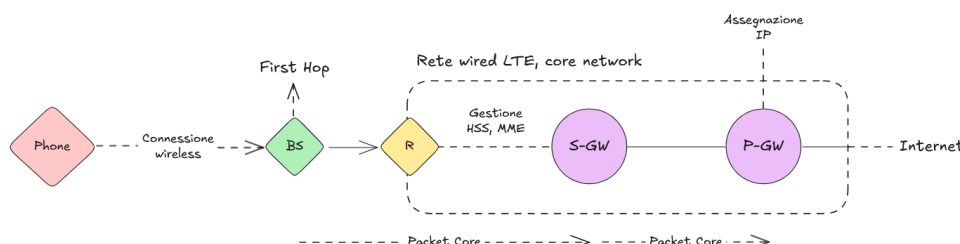
Standard LTE

Lo standard LTE prevede la divisione del data plane e control plane dentro i router:

- **Data Plane:** nuovi protocolli per la mobilità, sicurezza e autenticazione.
- **Control Plane:** nuovi protocolli per il trasporto collegamento e link si usa il tunneling per facilitare la mobilità.

Possiede diverse specifiche per la gestione dei canali e risorse:

- **Canale Downstream (da rete a dispositivo)**
 - Dentro ogni canale di frequenza **OFDM**, si usa **FDM (Frequency Division Multiplexing)** e **TDM (Time Division Multiplexing)**.
- **Canale Upstream (da dispositivo a rete)**
 - Funziona in modo simile al downstream, con **FDM/TDM** e una variante di OFDM per ottimizzare la trasmissione.
- **Assegnazione delle risorse**
 - Ogni dispositivo attivo riceve **slot temporali** da 0,5ms su 12 frequenze.
 - **L'algoritmo di scheduling** (che decide chi trasmette e quando) non è standardizzato, dipende dall'operatore.



LTE First Hop

LTE suddivide il livello collegamento in tre fasi principali:

1. **Packet Data Convergence (PDC):** Compressione degli header per ridurre l'overhead e cifratura.
2. **Radio Link Control (RLC): Frammentazione e riassemblaggio,** Garantisce un **trasferimento dati affidabile**.
3. **Medium Access:** Gestisce il **richiesta/assegnazione degli slot di trasmissione**.

LTE Packet core

Il **packet core** di LTE utilizza il **tunneling** per trasportare i dati dal eNode fino alla rete. Questo avviene attraverso una serie di incapsulamenti, garantendo efficienza e continuità della connessione anche in mobilità.

- **Tunneling dei dati:** I **datagrammi mobili** ricevuti dal eNode vengono **incapsulati usando il GPRS Tunneling Protocol (GTP)**. Sono inseriti in **datagrammi UDP** e inviati al **S-GW**. Il **S-GW re-incapsula** i pacchetti e li inoltra al **P-GW**, che li connette alla rete Internet.
- **Mobilità:** Quando un utente si sposta tra le celle, **cambiano solo gli endpoint del tunnel**, senza interrompere la trasmissione dei dati.

Connessione a una Base Station (BS)

Quando un telefono vuole connettersi a una **Base Station (BS)** in LTE, deve completare questi passaggi:

1. Trasmissione dei segnali di sincronizzazione:

- Ogni **5ms**, la BS trasmette un **primary sync signal** su tutte le frequenze disponibili.
- Più stazioni base possono trasmettere questi segnali contemporaneamente.

2. Individuazione e decodifica dei segnali:

- Il telefono rileva il **primary sync signal** e poi trova il **second sync signal** sulla stessa frequenza, ricevendo informazioni fondamentali.

3. Selezione della stazione base:

- Il dispositivo sceglie a quale **BS associarsi** in base a criteri comuni come la potenza.

4. Autenticazione e configurazione della connessione dati:

- Dopo aver scelto la BS, il dispositivo deve ancora **autenticarsi** e **stabilire il collegamento dati** con il core network.

Solo dopo questi passaggi, il dispositivo può avviare il "first hop" e poi accedere al packet core per raggiungere Internet e comunicare.

LTE Modalità Sleep

I dispositivi LTE possono mettere le onde radio in sleep per risparmiare la batteria:

- **Light sleep:** dopo 100ms si riattiva automaticamente per controllare eventuali trasmissioni in arrivo (**downstream check**).
- **Deep sleep:** dopo 5-10s di inattività si può pensare che il dispositivo abbia cambiato BS durante il deep sleep quindi bisogna associare nuovamente il UE.

Connessione 5G

Quello che otteniamo con il 5G rispetto al 4G sono bit-rate maggiori, latenze ridotte e la capacità di traffico migliorata, ma lavoriamo su distanze più corte e non è uno standard uniforme:

- **EMBB** (Enhanced Mobile Broadcast): Fornisce più bandwidth per download e upload, quindi più veloce e una riduzione moderata della latenza. Serve per le "Rich media" come realtà virtuale, risoluzione 4K o video streaming 360*.
- **URLLC** (Ultra Reliable Low-Latency Communications): Destinato per applicazioni sensibili a cambi di latenza, come automazioni di macchinari in fabbrica o guida autonoma.
- **mMTC** (Massive Machine Type Communications): Questo protocollo utilizza bande strette, ovvero una piccola larghezza per le frequenze, per applicazioni di rilevamento, misurazione o monitoraggio. Principalmente usato nel mondo dei dispositivi IoT, serve anche per ridurre il consumo di energia dei dispositivi.

Dato che il 5G utilizza frequenze più precise, hanno un range minore perché come sappiamo le onde si disperdono più sono lunghe le distanze, quindi bisogna mettere BS con densità maggiore.