

Università degli Studi di Trieste

Corso di Laurea Magistrale in
INGEGNERIA CLINICA



**UNIVERSITÀ
DEGLI STUDI
DI TRIESTE**

Dipartimento di
Ingegneria e Architettura

Reti di calcolatori: Livello Fisico e Datalink

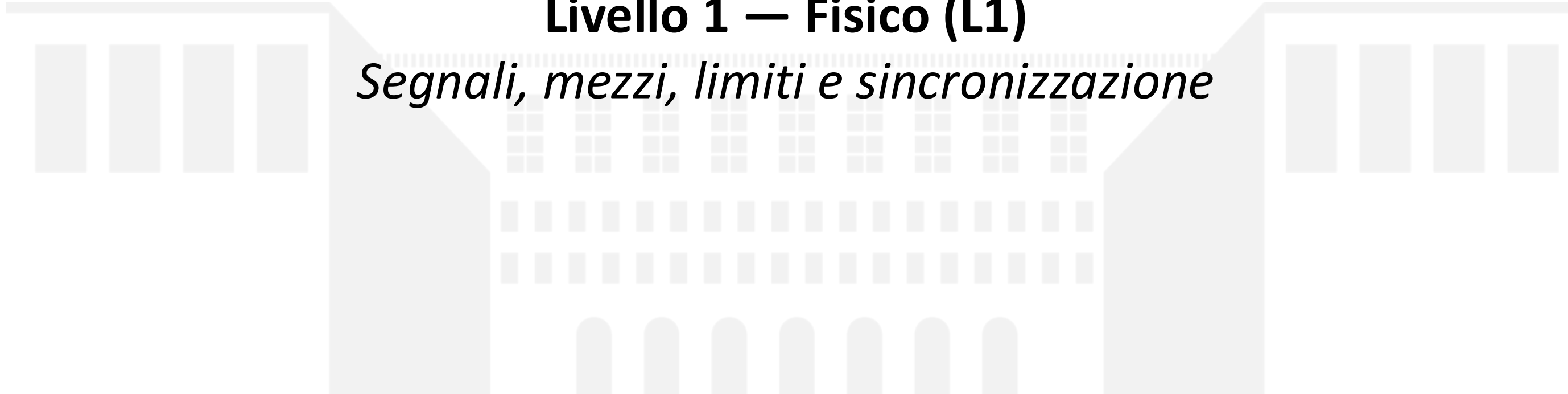
Corso di Informatica Medica

Docente: Aleksandar Miladinović

Questa presentazione è stata realizzata, in parte o interamente, basandosi sulle slide fornite dal Prof. Francesco Brun.

Livello 1 — Fisico (L1)

Segnali, mezzi, limiti e sincronizzazione



- Si occupa della **trasmissione di bit "grezzi" su un canale** di comunicazione
- Gli aspetti di progetto riguardano prevalentemente le **caratteristiche meccaniche, elettriche del mezzo fisico** (ad esempio cavo o antenna)
- E' a questo livello che ad esempio è necessario determinare:
 - ✓ tensioni elettriche scelte per rappresentare 0 ed 1
 - ✓ durata (in microsecondi) di un bit
 - ✓ trasmissione simultanea in due direzioni oppure no
 - ✓ forma dei connettori

Cosa fa il livello fisico?



- **Bit → segnali sul mezzo** — i bit (0/1) diventano variazioni fisiche: tensione/corrente (rame), luce (fibra), onde radio (wireless).
- **Connettori, codifica e temporizzazione** — standard fisici (es. RJ-45/LC), schemi di line coding e regole di clock per sapere quando inizia/finisce un bit.
- **Half/Full-duplex** — half-duplex = si trasmette a turni; full-duplex = invio e ricezione contemporanei sullo stesso collegamento.
- **Niente indirizzi né consegna end-to-end** — L1 non garantisce l'arrivo dei dati: fornisce solo il trasporto fisico dei bit.

Banda (Hz) — intervallo di frequenze che il canale trasporta senza distorsione eccessiva; più banda ⇒ più simboli al secondo.

Throughput (bit/s) — velocità effettiva di dati utili (dipende da bitrate nominale, overhead e condizioni del canale).

Latenza (s) — tempo tra invio e ricezione (trasmissione + propagazione + code + elaborazione).

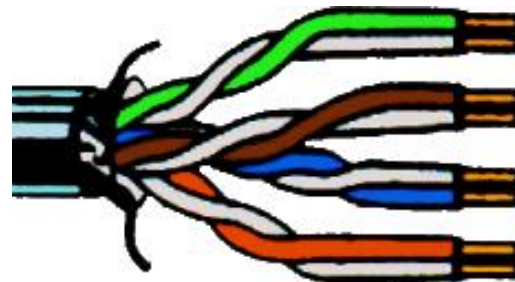
Jitter — variabilità della latenza tra pacchetti consecutivi (critica per voce/video real-time).

Baud (simboli/s) — numero di simboli al secondo; non coincide con bit/s se un simbolo rappresenta più bit.

Rame (UTP/STP) — economico e diffuso, ma soggetto a attenuazione/interferenze; tratte Ethernet tipiche ~100 m.

Fibra ottica (SM/MM) — lunga distanza, immunità EMI; single-mode per distanze elevate, multi-mode per tratte più brevi.

Wireless (Wi-Fi/5G) — trasmissione via radio su canali condivisi; occorre gestire potenza, canali e interferenze.



Attenuazione — perdita di ampiezza del segnale con distanza/frequenza; limita la lunghezza utile della tratta.

Rumore & SNR — il rumore è disturbo casuale; rapporto segnale/rumore alto \Rightarrow meno errori di bit.

Diafonia (crosstalk) — accoppiamento indesiderato tra coppie di fili nel rame che introduce interferenza.

Dispersione (fibra) — allargamento degli impulsi luminosi (modale/cromatica) che limita bitrate e distanza.

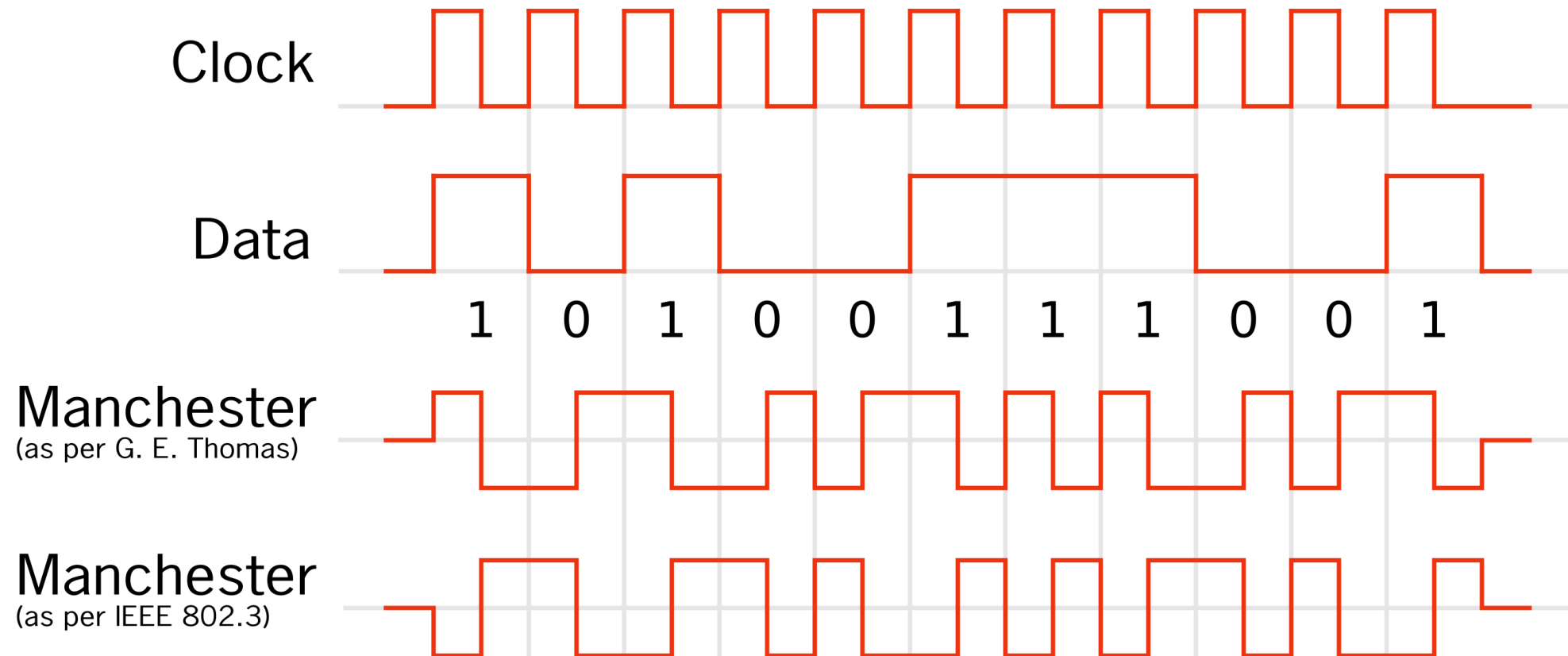
Trade-off fisici — velocità, distanza e affidabilità sono legate: aumentare il bitrate richiede mezzi migliori, distanze minori o rigenerazione.

Line coding (baseband) — mappa i bit in forme d'onda su banda base (es. NRZ, Manchester) spesso includendo informazione di sincronismo.

Modulazione (passband) — varia ampiezza/frequenza/fase di una portante per trasportare l'informazione (es. ASK/FSK/PSK in radio).

Modem (esempio) — dispositivo che modula/demodula i segnali per adattarli a un canale nato per altro (storiche linee telefoniche).

Manchester line coding



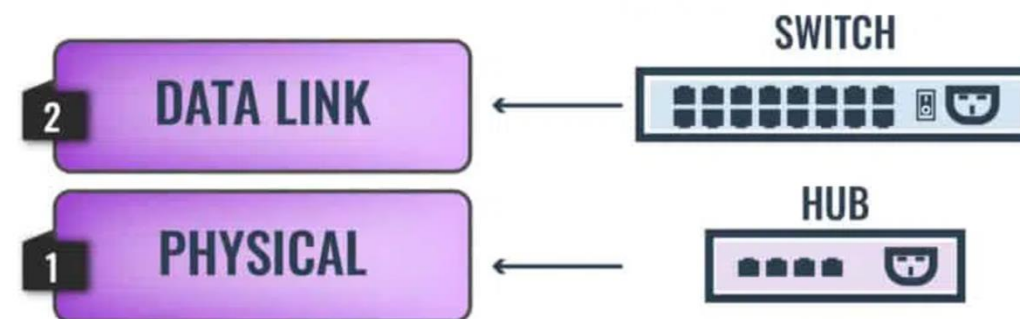
Video: <https://youtu.be/SJE2IFR5utM?si=8rq2nvYTIIPhcuph>

Half-duplex — una direzione alla volta; semplice ma meno efficiente (tipico dei vecchi hub/mezzi condivisi).

Full-duplex — invio e ricezione simultanei sullo stesso link; elimina collisioni e aumenta il throughput.

Hub vs Switch (contesto) — l'hub ripete segnali a tutti (mezzo condiviso); lo switch commuta per porta (collegamenti indipendenti, full-duplex).

→ Un **hub** è un dispositivo semplice che replica i segnali e invia i dati a tutte le porte connesse



Niente instradamento — L1 non interpreta indirizzi e non sceglie percorsi; ciò avviene in L2/L3.

Errori gestiti sopra — L1 non corregge; L2 rileva corruzioni con CRC/FCS e scarta; le ritrasmissioni spettano agli strati superiori.

Affidabilità end-to-end — ordine e consegna garantita sono compito dei protocolli di trasporto (es. TCP), non del livello fisico.

L1 = mezzo + segnale + sincronismo — lo strato che realizza fisicamente la trasmissione dei bit.

Prestazioni legate al mezzo — distanza/velocità/affidabilità dipendono da attenuazione, SNR, diafonia/dispersione.

Il resto sta sopra — indirizzi, controllo/ritrasmissione errori e consegna end-to-end sono responsabilità di L2/L4.

Parte 1 — Segnali e misure

Bit → segnale (rame/fibra/radio), banda vs baud, throughput, latenza e jitter

SNR e BER: qualità del link, attenuazione e diafonia

Tempo di trasmissione vs tempo di propagazione (stima rapida)

Link: https://www.youtube.com/live/YXcC6QoaEPw?si=7FdeeeAH_AsFI_Tf

Parte 2 — Mezzi trasmissivi e qualità

Rame (UTP/STP), fibra (SM/MM), wireless (Wi-Fi/5G): quando scegliere cosa

Distanze tipiche, EMI, dispersione (modale/cromatica), posa e raggi di curvatura

Connettori (RJ-45, LC/SC), note pratiche su cablaggio e PoE

Link: <https://youtu.be/TMAcaygaTjM?si=bJHtdeseKVRXOLyO>

Parte 3 — Sincronizzazione e accesso al mezzo

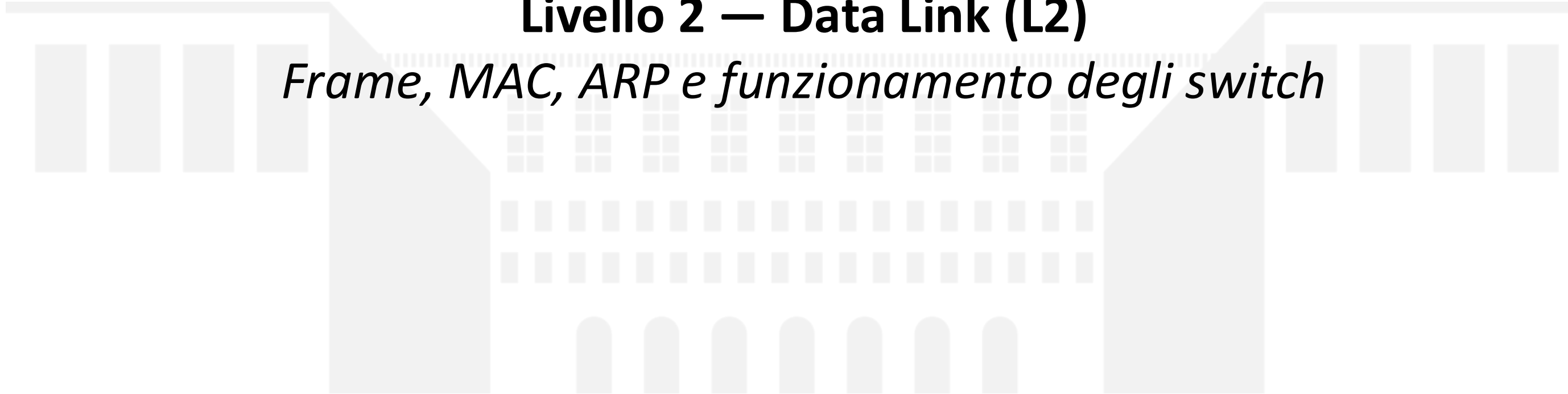
Preambolo e clock recovery; line coding (NRZ, Manchester) e modulazione (ASK/FSK/PSK/QAM)

Half-duplex vs full-duplex; impatto su collisioni (contesto CSMA/CD) e switch moderni

Link: <https://www.youtube.com/live/qbOuP2X1mcc?si=TqGF9f9MSjGfkC9a>

Livello 2 — Data Link (L2)

Frame, MAC, ARP e funzionamento degli switch



Incapsula i dati in frame — aggiunge intestazioni e controllo d'errore per il collegamento locale.

Indirizza gli host adiacenti con MAC — i MAC servono a raggiungere il “prossimo nodo” sul link, non l'intera Internet.

Consegna hop-by-hop — il frame vale solo sul tratto locale; lungo il percorso i MAC cambiano a ogni hop, l'IP resta.

Rileva errori locali, non ritrasmette — se il frame è corrotto viene scartato; eventuali ritrasmissioni avvengono ai livelli superiori.

Indirizzo MAC (Media Access Control)

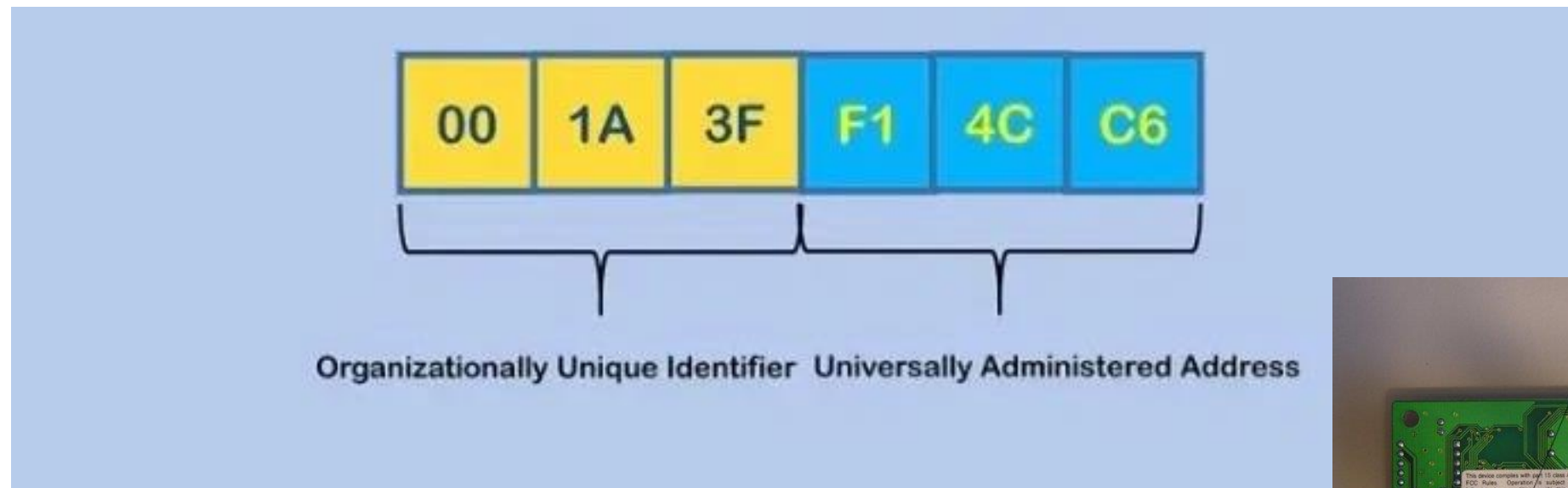


UNIVERSITÀ
DEGLI STUDI
DI TRIESTE

Cos'è — Identifica l'interfaccia di rete sul link locale; serve al recapito **hop-by-hop** dei frame.

Lunghezza e formato — **48 bit** (MAC-48/EUI-48), scritto in esadecimale: es. 00:1A:2B:3C:4D:5E.

Struttura — **OUI** (primi 24 bit, produttore) + **NIC** (ultimi 24 bit, seriale dell'interfaccia).

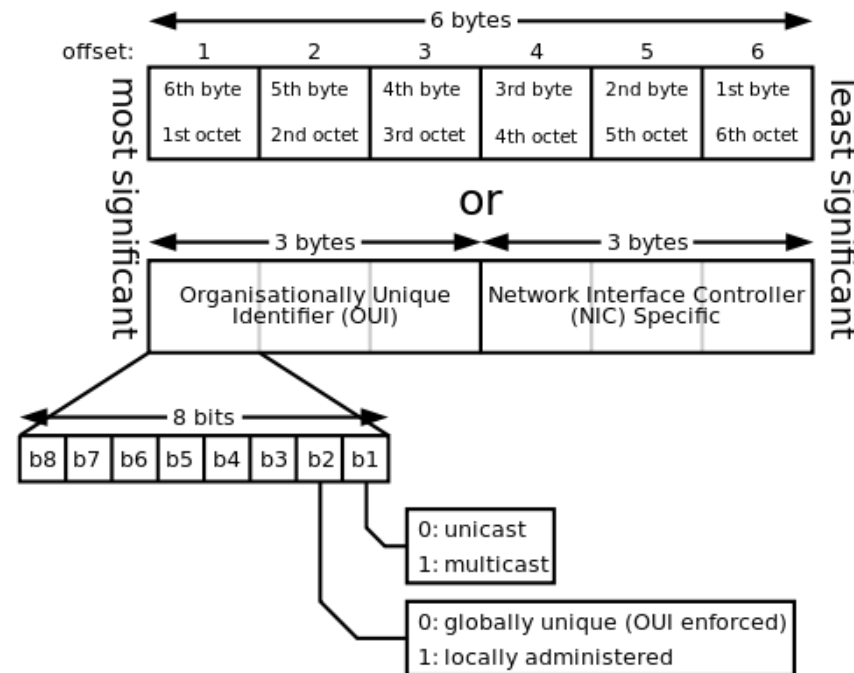


Indirizzo MAC (Media Access Control)



Flag nel 1° byte — bit **I/G**: 0 unicast, 1 multicast • bit **U/L**: 0 universale (vendor), 1 **locally administered** (configurato a software).

Tipi di destinazione — **Unicast** (un host), **Multicast** (gruppo), **Broadcast** ff:ff:ff:ff:ff:ff (tutti sulla LAN).



È il **“pacchetto” del Livello 2** che viaggia sul collegamento locale (cavo o Wi-Fi).

Serve per **recapitare i dati** dal mittente al **prossimo** destinatario sullo stesso tratto (hop-by-hop).

È pensato per essere **veloce da filtrare** (guardando subito l'indirizzo MAC) e **semplice da verificare** (CRC).

MAC destinazione → a chi è diretto sul link.

MAC sorgente → chi lo ha inviato sul link.

Dati (payload) → il contenuto da consegnare allo strato superiore.

FCS/CRC (4 byte) → controllo d'integrità del frame.

(Dimensioni tipiche: minimo 64 B, massimo 1518 B; basta ricordare: c'è un minimo e un massimo.)

Ethernet (802.3) Frame Format

| 7 bytes | 1 byte | 6 bytes | 6 bytes | 2 bytes | 42 to 1500 bytes | 4 bytes | 12 bytes |
|----------|--------------------------|--------------------------------|---------------------------|---------|------------------|---------|-----------------|
| Preamble | Start of Frame Delimiter | Destination MAC Address | Source MAC Address | Type | Data (payload) | CRC | Inter-frame gap |



For TCP/IP communications, the payload for a frame is a

Cosa succede quando arriva un frame

Prima Ethernet (coassiale, “porta vampiro”)

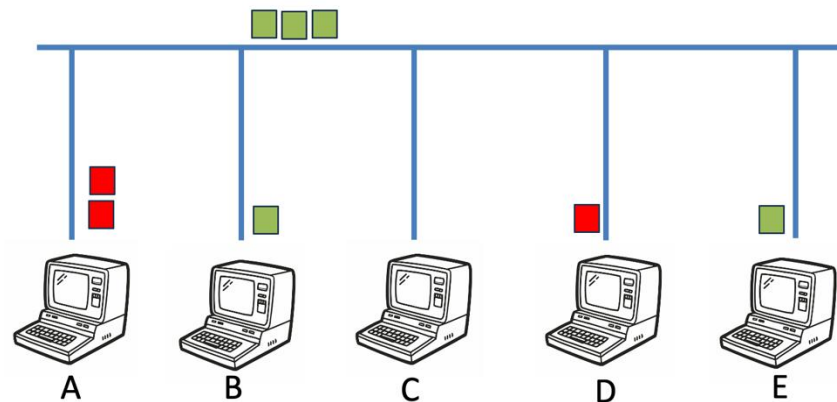
10BASE5/10BASE2: un **unico cavo coassiale in bus**; ogni trasmissione **viaggia su tutto il mezzo**.

Tutte le schede “vedono” ogni frame e leggono subito il MAC di destinazione:

se è il **proprio** (o **broadcast**) → proseguono;

se è **di altri** → **scartano**.

(Contesto) Mezzo condiviso ⇒ servivano regole per **non parlare insieme**; comunque la logica “vedo-MAC-mio?” resta la stessa.



NOTA: Oggi (Ethernet su switch, punto-punto) Il frame unicast non va più “a tutti”: lo switch lo **inoltra solo** verso la **porta** del destinatario.

Cosa succede quando arriva un frame (2)



Ordine semplice di elaborazione (host o switch)

1) Guarda MAC di destinazione

mio/broadcast → **accetto** (host) / **inoltrato** (switch);

non mio → **scarto** (host) / **inoltrato verso porta corretta** (switch).

Controlla il CRC (FCS)

OK → il frame è integro, si **consegna** il contenuto allo strato superiore;

Errore → **scarto!!!**

Se “scarto”, chi gestisce la perdita?



A L1–L2 si **scarta e basta**: niente ritrasmissioni automatiche qui.

La **perdita** viene gestita dai **livelli superiori** (software): possono **ritentare**, **riordinare**, oppure **tollerare** la perdita se l'applicazione lo consente.

Idea chiave delle reti di calcolatori:

anche con collegamenti **non affidabili** (collisioni, errori) si può ottenere un **servizio affidabile** grazie a **meccanismi software end-to-end**.

Intuizione storica (**ALOHAnet**): invece di coordinare rigidamente “chi parla quando”, si **accetta il rischio di collisioni** e si risolve con **strategie semplici lato terminali** (attesa casuale e ritento).

Questo principio ha reso le reti **scalabili, robuste ed economiche**, favorendo l'**esplosione** della comunicazione a pacchetto!!!

Collisioni (contesto storico, mezzo condiviso)

Su Ethernet coassiale/hub due stazioni possono **trasmettere insieme** → i segnali si **sovrappongono** → il frame si **corrompe** → **CRC errato** → **scarto**.

Altre cause:

Degrado del segnale sul mezzo

- Interferenze (EMI/RFI), diafonia: disturbi esterni o accoppiamento tra coppie.
- Riflessioni/terminazioni (coassiale storico), cablaggi scadenti, connettori ossidati, raggi di curvatura (fibra).

Mismatch e incoerenze di link

- Duplex mismatch (uno half, l'altro full) → late collisions, FCS errors, prestazioni pessime.
- Velocità/MTU non allineate → “runts/giants”, scarti o frammentazioni a valle.

Wireless (cenno)

- Interferenza di canale, hidden node, multipath → ritrasmissioni e perdita; non è un errore “di filo”, ma l'effetto è lo stesso: frame non valido o perso.

Congestione di buffer (non errore di bit, ma perdita)

- Switch/host saturi scartano frame validi per mancanza di spazio → i livelli superiori vedono perdita e reagiscono.

Collisioni e CSMA/CD (Ethernet coassiale “storica”)

Scenario storico (10BASE5/10BASE2, porta vampiro + cavo coassiale in bus)

Tutte le stazioni condividono **lo stesso mezzo**: quando una trasmette, **tutte** “sentono”.

Due stazioni **possono iniziare insieme** (propagazione \neq istantanea) \Rightarrow i segnali si **sovrappongono** \Rightarrow **collisione**.

CSMA/CD: come si convive col mezzo condiviso

- >**Carrier Sense (CS)** — prima di parlare, **ascolto**: se il mezzo è occupato, **attendo**.
- >**Multiple Access (MA)** — **tutti** hanno diritto di accesso, senza ordine prefissato.
- >**Collision Detection (CD)** — mentre trasmetto, **controllo**: se rilevo una collisione (livelli elettrici anomali), **invio un “jam”** (breve sequenza che rende evidente la collisione a tutti), **mi fermo**, aspetto un **ritardo casuale** (backoff) e **ritento**.

Backoff binario esponenziale (idea chiave)

Al 1° tentativo fallito, scelgo a caso 0 o 1 “slot” di attesa;

al 2° fallito, scelgo tra 0..3; poi 0..7, ecc. (cresce l’intervallo per **decongestionare**).

Dopo **16 tentativi** falliti: **rinuncio** e segnalo errore ai livelli superiori.

Perché funziona

È **semplice** (tutto lato stazione, niente coordinatore centrale) e **scalabile** (principio ereditato da ALOHAnet): si **accettano** collisioni occasionali ma le si **risolvono** con regole locali e ritenti casuali.

Cos'è un link (collegamento L1/L2)

Collegamento tra due interfacce adiacenti che possono scambiarsi **frame direttamente** (senza passare per un router).

Fisco o logico: cavo rame/fibra (fisico) oppure mezzo radio **Wi-Fi** (logico sull'aria); in entrambi i casi è il "tratto" su cui valgono **MAC** e incapsulamento di **L2**.

Tipologie: **punto-punto** (es. PC ↔ switch) e **mezzo condiviso** (hub/Wi-Fi: il link è logico verso l'AP).

Proprietà chiave del link: mezzo, **duplex** (half/full), **bitrate/throughput**, **MTU**, **latenza** e **BER** (errori).

Domini L2: un link appartiene a un **dominio di collisione** (storico) e a un **dominio di broadcast** (segmento/VLAN); i broadcast restano nel dominio L2, un **router** li interrompe.

Confini del link: termina su un'interfaccia; superare un **router** crea un **nuovo link** e richiede **nuovo incapsulamento** (e spesso **ARP** verso il prossimo hop).

Esempi rapidi: cavo **PC↔switch** = link p-p; **client↔AP** = link logico Wi-Fi; una **VLAN** definisce un segmento L2: più link fisici possono trasportarla su trunk **802.1Q**.

Consegna hop-by-hop: il MAC cambia per tratto

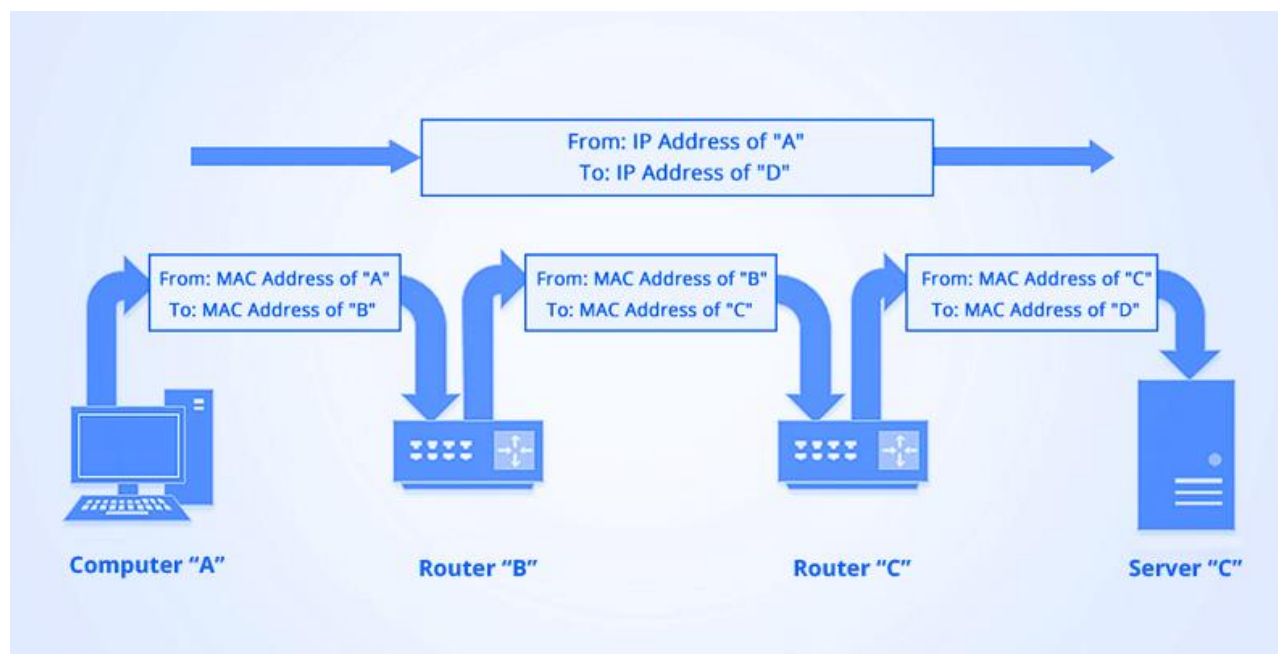
IP è end-to-end, MAC è locale al link — l'header L2 (MAC sorgente/destinazione) vale solo sul **tratto fisico** corrente; a ogni salto **L3 (router)** viene riscritto.

Dentro la stessa LAN (solo switch) — il **MAC destinazione** resta quello dell'host finale lungo tutti gli switch; gli switch **non** riscrivono i MAC.

Attraverso un router — il router **decapsula a L2**, inoltra a L3, poi **ricapsula con nuovi MAC**:

MAC sorgente = interfaccia di uscita del router

MAC destinazione = **MAC del next hop** (host target nella stessa subnet di uscita, oppure l'interfaccia del router successivo)



Nota operativa: prima di ogni invio su un tratto, chi trasmette deve conoscere il **MAC del next hop** (ARP se nella stessa subnet; i router usano ARP sulle proprie interfacce verso la rete di uscita).

ARP (Address Resolution Protocol)



A cosa serve — risolve **IP** → **MAC** nella stessa subnet; se la destinazione è fuori subnet, si risolve il **MAC** del gateway.

Come funziona:

Request (broadcast): “Chi ha IP X? Dica a IP Y” → inviato a ff:ff:ff:ff:ff:ff

Reply (unicast): “IP X è a MAC Z” → inviato direttamente al richiedente.

La mappatura viene salvata in **cache ARP** per un periodo breve.

Quando si attiva — prima di inviare il **frame** verso l’host (stessa subnet) o verso il **gateway** (fuori subnet). Anche i **router** usano ARP sulle **loro interfacce** verso il *next hop*.

Tabella ARP — elenco IP↔MAC temporaneo, visibile con `arp -a`; le voci scadono se non usate e si rinnovano automaticamente.

```
(base) aleksandarmiladinovic@MacBook-Air-M1 ~ % arp -a
? (169.254.53.108) at a8:42:e3:53:6c:34 on en0 [ethernet]
? (169.254.105.246) at a8:42:e3:53:f6:68 on en0 [ethernet]
? (169.254.141.121) at a8:42:e3:53:79:8c on en0 [ethernet]
```

Stessa subnet — invio il frame al **MAC dell'host destinatario**.

Fuori subnet — invio al **MAC del gateway**; sarà il router a incapsulare di nuovo per il prossimo hop.

MAC cambia, IP no — i MAC vengono riscritti ad ogni tratto; gli IP restano quelli della sorgente/destinazione finali.

Il **default gateway** è l'**indirizzo IP del router** della tua rete locale.

->È “la porta d'uscita”: se vuoi parlare con un IP che **non appartiene** alla tua sottorete, **spedisci al gateway** e sarà lui a instradare oltre.

Decisione: locale o fuori?

Il tuo host confronta **IP_dest & mask** con **IP_mio & mask**.

Se uguali ⇒ **stessa sottorete** ⇒ invia **direttamente** al destinatario (ARP sul suo IP, MAC del destinatario).

Se diversi ⇒ **fuori sottorete** ⇒ invia al **default gateway** (ARP sul **gateway**, MAC del gateway).

Cos'è uno switch (L2) e perché è diverso da un hub



Hub (ripetitore L1)

- Dispositivo “stupido”: **ripete** i segnali elettrici **su tutte le porte**.
- Tutti sono sul **mezzo condiviso** → un **solo dominio di collisione**.
- Tipicamente **half-duplex**; servono meccanismi tipo **CSMA/CD** (storico).
- **Nessuna** tabella MAC, **nessuna** decisione: zero selettività, banda **condivisa** tra tutte le porte.

Switch (commutatore L2)

- Dispositivo “intelligente”: **legge l'header L2**, guarda il **MAC di destinazione** e **inoltra solo** dove serve.
- Ogni porta è un **dominio di collisione separato** → collegamenti punto-punto, di norma **full-duplex**.
- Usa **buffer** e, di solito, modalità **store-and-forward** (controlla il CRC prima di inoltrare); alcuni modelli supportano **cut-through** (bassa latenza).
- Mantiene una **tabella MAC** per decidere rapidamente **su quale porta** inviare i frame.

Come decide uno switch (quattro comportamenti chiave)

Learning

Quando vede un frame **provenire** dal **MAC X sulla porta P**, memorizza (o aggiorna) in tabella: **MAC X → porta P**.

Effetto: “so dov’è X se devo spedirgli qualcosa”.

Flooding

Se **non sa** dove si trova il **MAC destinazione** (*unknown unicast*), oppure se il frame è **broadcast**, **replica** il frame su **tutte le porte** della stessa rete (VLAN/segmento), **tranne** quella d’ingresso.

Effetto: il destinatario, dovunque sia in quel segmento, lo riceverà.

Forwarding / Filtering

Se **conosce** la porta del **destinatario**, **inoltra solo lì** (forwarding) e **non** sulle altre (filtering).

Effetto: meno traffico inutile, più banda disponibile per tutti.

Aging

Le voci **MAC → porta** scadono dopo un certo **tempo** se non vengono più viste.

Effetto: la tabella **rimane aggiornata** e non cresce con dispositivi non più presenti.

Mini-scenario (come si “popola” la tabella)



PC-A → PC-B (prima volta)

Lo switch **impara**: “MAC(A) è sulla porta 3” (learning dalla sorgente).

Non conosce MAC(B) → **flooding** su tutte le altre porte.

PC-B risponde a PC-A

Lo switch **impara**: “MAC(B) è sulla porta 7”.

Ora le prossime comunicazioni **A↔B** saranno **unicast** punto-punto (**forwarding**) solo tra porta 3 e 7.

Risultato: meno traffico inutile, **zero collisioni** tra porte, banda **dedicata** per ciascun link.

Nota operativa: i **broadcast** (es. ARP) vengono comunque replicati a tutti nel segmento; per evitare tempeste in presenza di **anelli** fisici servono meccanismi anti-loop (es. STP/RSTP) — tema che puoi citare più avanti.

- **Unità di L2 = frame:** “pacchetto” locale che viaggia solo sul tratto fisico corrente (hop-by-hop).
- **Indirizzi MAC (48 bit):** servono a raggiungere il prossimo nodo sul link; IP resta end-to-end.
- **Ordine logico sul frame** (semplificato): MAC destinazione → MAC sorgente → dati → FCS/CRC.
- **Primo controllo:** si guarda il **MAC destinazione**; se è mio/broadcast accetto, altrimenti scarto (lo switch inoltra alla porta giusta).
- **Secondo controllo: CRC/FCS;** se non torna, il frame è corrotto ⇒ scarto.
- **ARP** risolve **IP** → **MAC** nella stessa subnet; se la destinazione è fuori rete, si risolve il **MAC del gateway**.
- **Switch L2:** imparano la mappa MAC→porta (learning), inoltrano unicast noto, fanno flooding se ignoto/broadcast.
- **Hop-by-hop:** attraversando un router i **MAC cambiano** a ogni tratto; gli **IP non cambiano**.
- **Errori e perdite:** a L2 si scarta e basta; l’affidabilità/ritrasmissione è compito degli strati superiori (idea chiave delle reti a pacchetto).
- **Contesto storico:** su mezzo condiviso (coassiale/hub) c’erano **collisioni** gestite con **CSMA/CD**; con switch full-duplex le collisioni spariscono.

1. Che cos'è un **frame** e perché è diverso da **pacchetto IP**.
2. A cosa servono i **MAC** e perché cambiano a ogni **hop** mentre l'**IP** resta lo stesso.
3. Come funziona **ARP** (request broadcast → reply unicast) e quando si usa il **gateway**.
4. Cosa fa uno **switch** (learning, forwarding, flooding) e perché i **broadcast** arrivano a tutti.
5. Perché si **scarta** un frame (MAC non mio, **CRC** errato) e chi gestisce la perdita.
6. Perché storicamente serviva **CSMA/CD** e perché oggi non serve più.
7. Perché in una LAN con solo switch il **MAC destinazione** non cambia "in mezzo", ma attraversando un router sì?
8. Quando mando a **8.8.8.8** da 192.168.1.10/24, quale **MAC** uso nel frame e perché?
9. Che succede a L2 se il **CRC** è errato? Chi si occupa di ritrasmettere eventualmente?