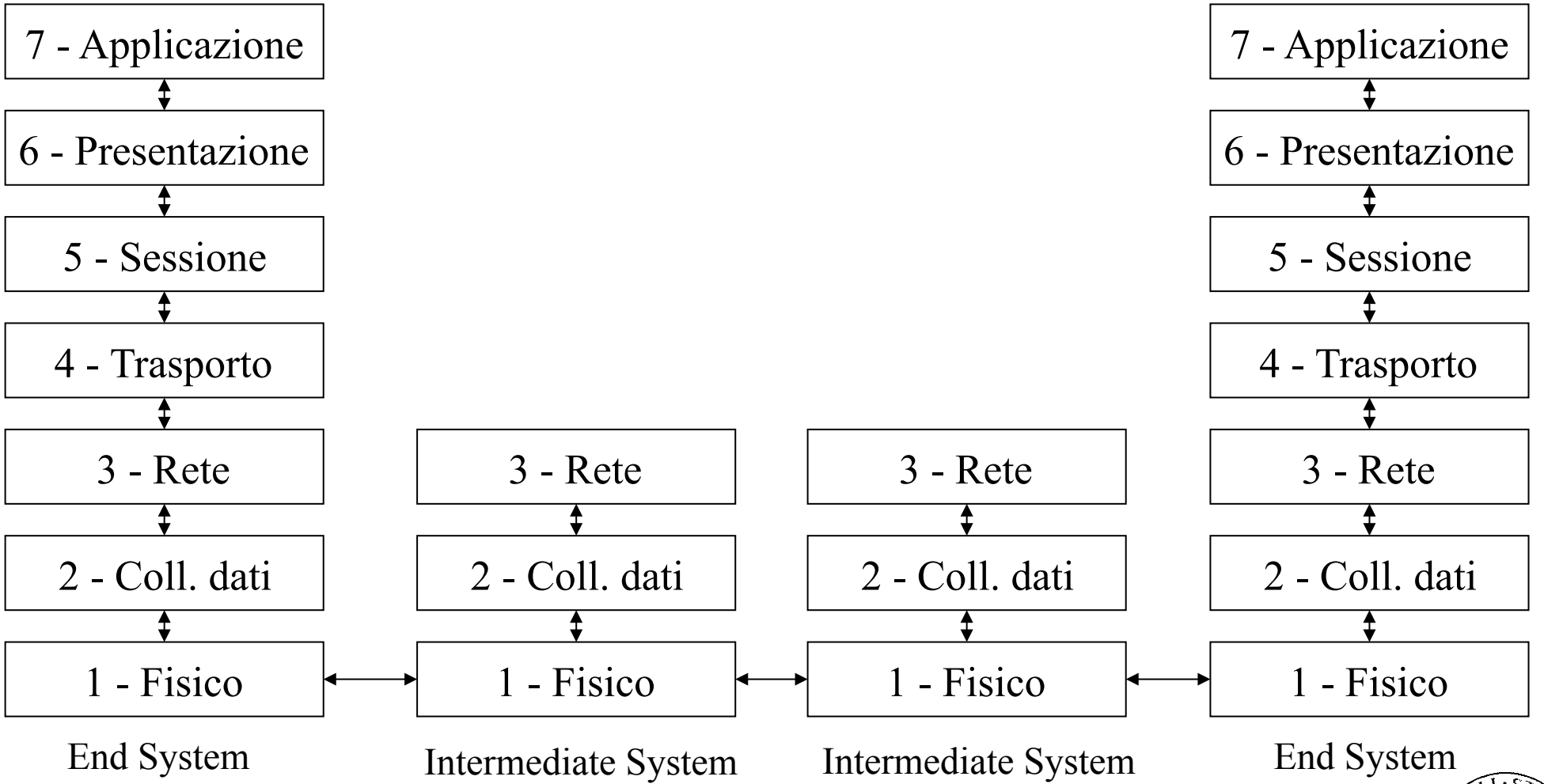
# Reti di Calcolatori


## Il livello Data Link

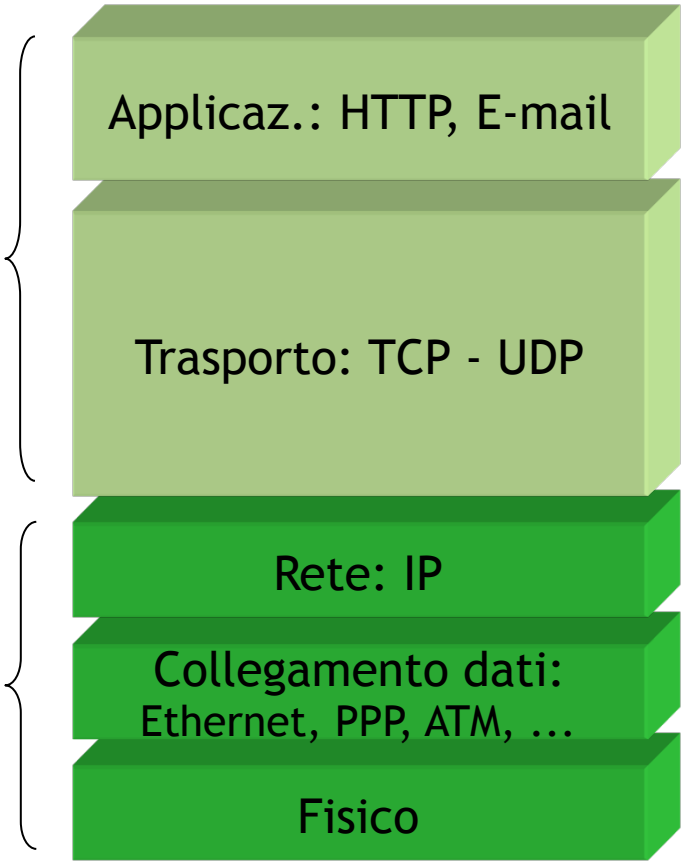
Universtità degli studi di Verona
Facoltà di Scienze MM.FF.NN.
A.A. 2010/2011
Laurea in Informatica

# Modello a strati



# Stack OSI...


# ...e Stack TCP/IP



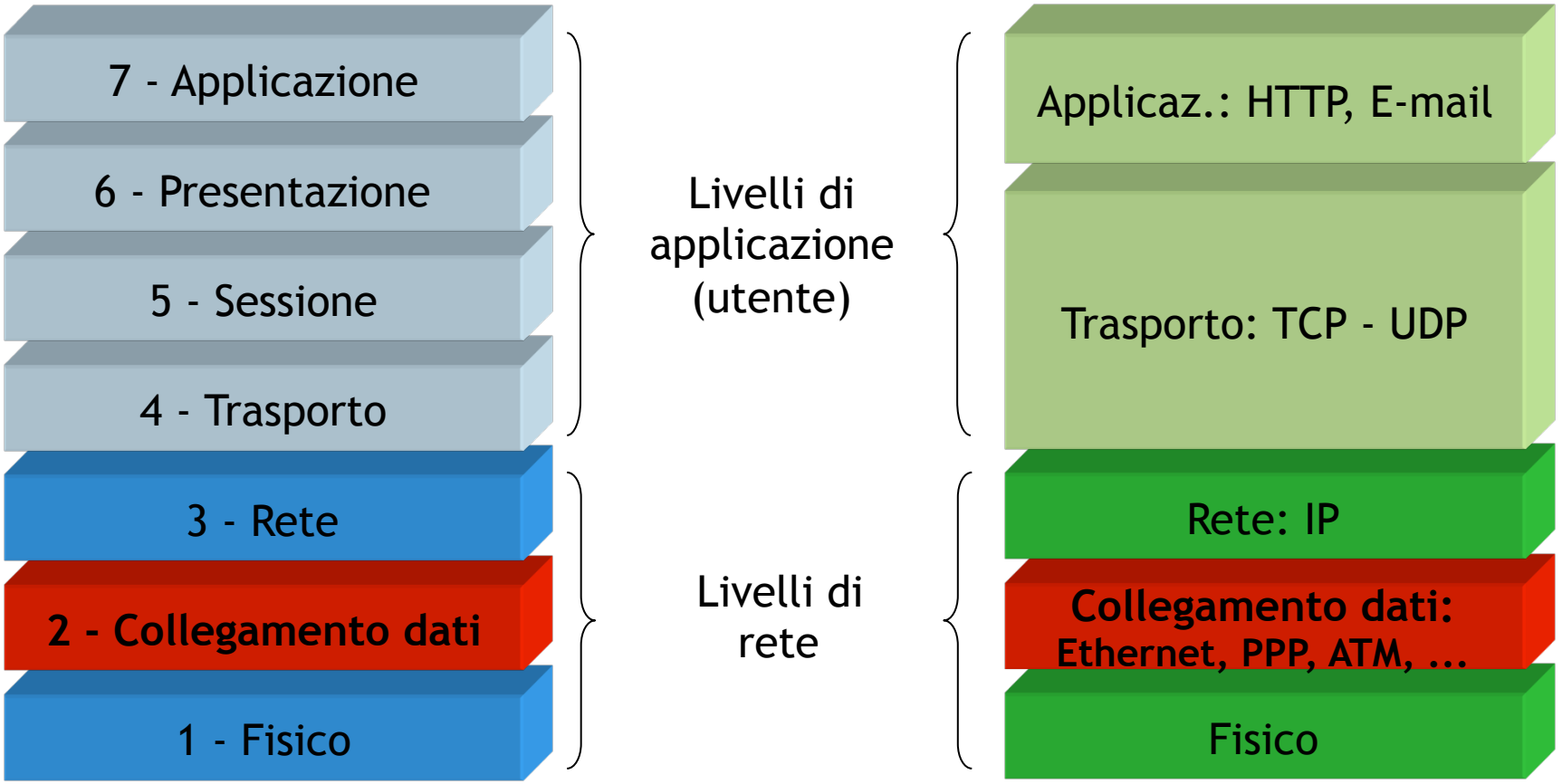

Livelli di applicazione (utente)

Livelli di rete

# Indice

- Il livello Data Link: funzionalità
- Il sotto livello MAC
- Protocolli di Livello 2
- Verifica Contenuti

# Livello Data Link



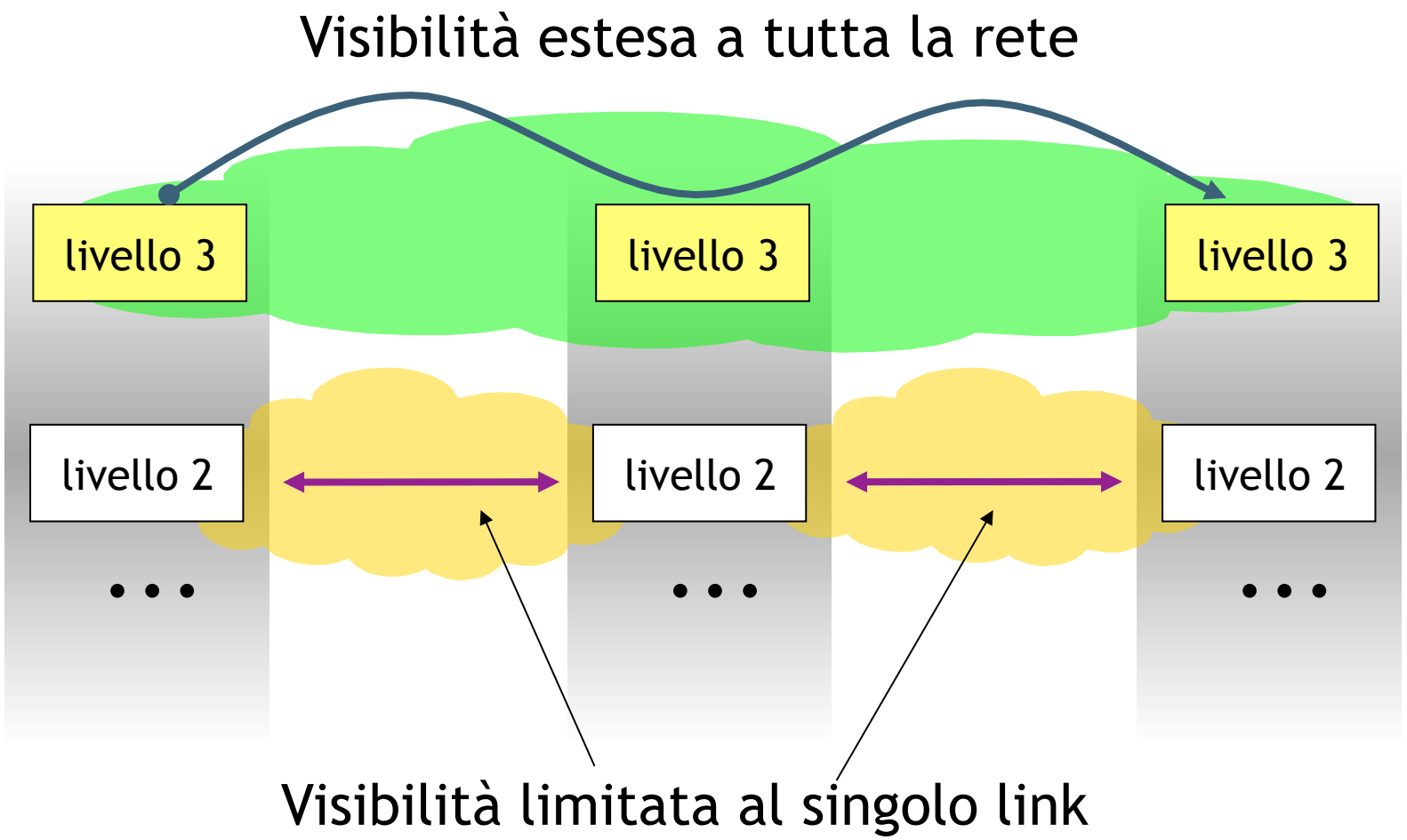
# Livello Data Link

- Obiettivo principale: fornire al livello di rete di due macchine adiacenti un ***canale di comunicazione*** il più possibile affidabile.
  - macchine adiacenti → fisicamente connesse da un canale di comunicazione (es. un cavo coassiale, doppino telefonico)
  - canale di comunicazione → "tubo digitale", ovvero i bit sono ricevuti nello stesso ordine in cui sono inviati
- Per compiere questo obiettivo, come tutti i livelli OSI, il livello 2 offre dei servizi al livello superiore (livello di rete) e svolge una serie di funzioni
- Problematiche: il canale fisico non è ideale
  - errori di trasmissione tra sorgente e destinazione
  - necessità di dover gestire la velocità di trasmissione dei dati
  - ritardo di propagazione non nullo

# Tipologia di servizi offerti al livello superiore

- Servizio connectionless senza acknowledge
  - non viene attivata nessuna connessione
  - invio delle trame senza attendere alcun *feedback* dalla destinazione
    - Se una trama viene persa non ci sono tentativi per recuperarla, il compito viene lasciato ai livelli superiori
  - ***la maggior parte delle LAN utilizzano questa tipologia di servizio***
- Servizio connectionless con acknowledge
  - non viene attivata nessuna connessione
  - ogni trama inviata viene "riscontrata" in modo individuale
- Servizio connection-oriented con acknowledge
  - viene attivata una connessione e, al termine del trasferimento, essa viene abbattuta
  - ogni trama inviata viene "riscontrata" in modo individuale

# Visibilità della rete del livello 2



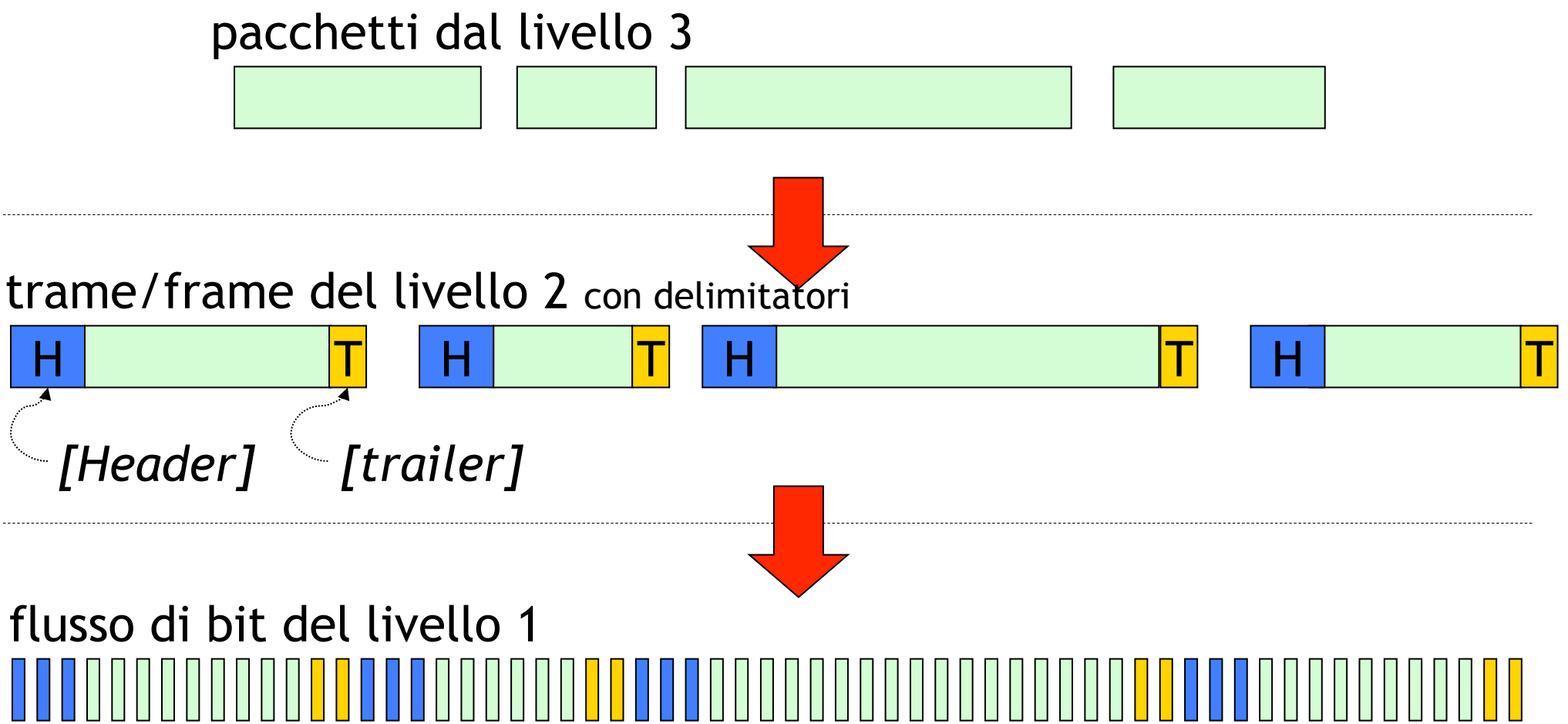
# Funzioni di competenza del livello 2

- Le principali funzioni svolte dal livello 2 sono:
  - framing
    - delimitazione delle trame
  - rilevazione/gestione errori
    - controlla se la trama contiene errori ed eventualmente gestisce il recupero
  - controllo di flusso
    - gestisce la velocità di trasmissione

# Framing

- Il livello 2 riceve dal livello superiore (rete) dei pacchetti
- Considerando che:
  - la lunghezza dei pacchetti (di livello 3) e delle corrispondenti trame (livello 2) è variabile
  - i sistemi non sono sincronizzati tra loro, ovvero non hanno un orologio comune che segna la stessa ora per tutti
  - il livello 1 tratta solo bit, e quindi non è in grado di distinguere se un bit appartiene ad una trama o a quella successiva
- ... nasce il problema della ***delimitazione delle trame***
- La funzionalità di *framing* (frame = trama) è dunque di rendere distinguibile una trama dall'altra attraverso l'utilizzo di opportuni codici all'inizio e alla fine della trama stessa

# Esempio

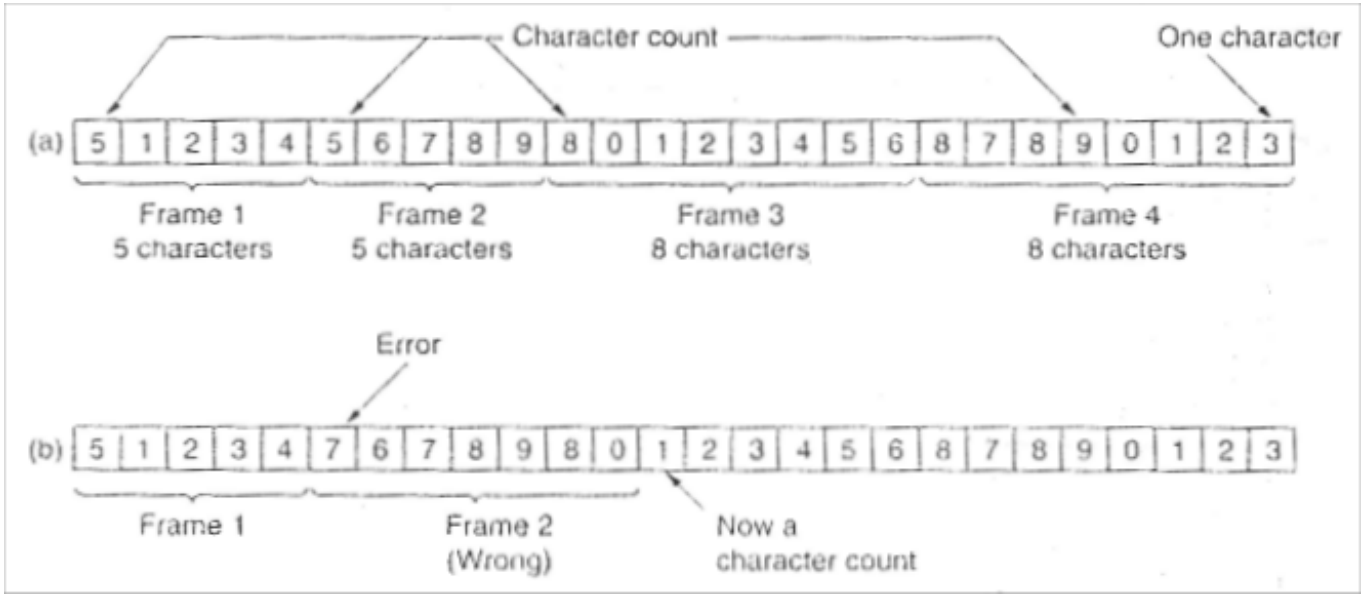

pacchetti dal livello 3
trame/frame del livello 2 con delimitatori
H
T
[Header]
[trailer]
flusso di bit del livello 1

# Modalità di Framing

- Esistono diverse tecniche per implementare il framing:
  - inserire intervalli temporali fra trame consecutive
    - problema: per natura intrinseca le reti di telecomunicazione non danno garanzie sul rispetto delle caratteristiche temporali delle informazioni trasmesse
    - gli intervalli inseriti potrebbero essere espansi o ridotti generando problemi di ricezione
  - marcare inizio e termine di ogni trama
    1. Character count
    2. Character stuffing
    3. Starting and ending flags (bit stuffing)
    4. Physical layer coding violations

# Framing: Character Count

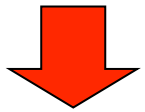
- Un campo nell'header del frame indica il numero di 'caratteri' nel frame stesso




*(fonte A.Tanenbaum, Computr Networks)*

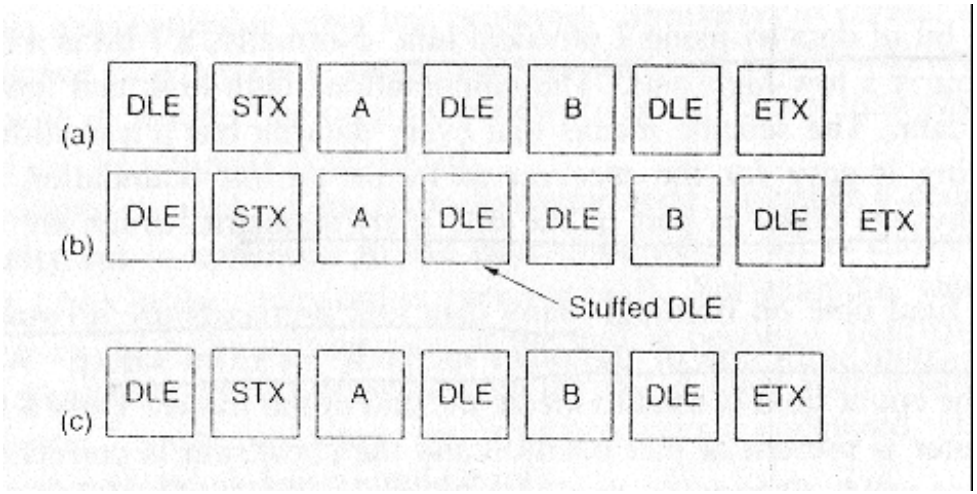
# Framing: Character stuffing (1)

- Ogni trama inizia e termina con una sequenza di caratteri ASCII ben definita
  - DLE (Data Link Escape) + STX (Start of TeXt)
  - DLE (Data Link Escape) + ETX (End of TeXt)
- Se nella trasmissione di dati binari, una sottosequenza di bit corrisponde ai caratteri speciali...



- ...la sorgente duplica il carattere DLE
  - **character stuffing**

# Framing: Character Stuffing (2)




*(fonte A.Tanenbaum, Computr Networks)*

- Svantaggio principale: soluzione legata al modulo base dei caratteri ad 8 bit e alla codifica ASCII

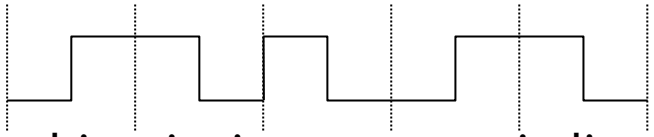
# Framing: Bit Stuffing

- Ogni trama può includere un numero arbitrario di bit
- Ogni trama inizia e termina con uno speciale pattern di bit, 01111110, chiamato **byte di flag**
- In trasmissione se la sorgente incontra 5 bit “1” consecutivi, aggiunge uno “0”
  - **bit stuffing**
  - es. la sequenza “01111110” è trasmessa come “011111010”

# Framing: Physical medium coding violations

- E’ una tecnica basata su sistemi che utilizzano ridondanza a livello fisico
  - es. ogni bit di informazione viene trasmesso utilizzando una combinazione di due bit a livello fisico
    - ‘1’ ⇨ ’10’
    - ‘0’ ⇨ ’01’

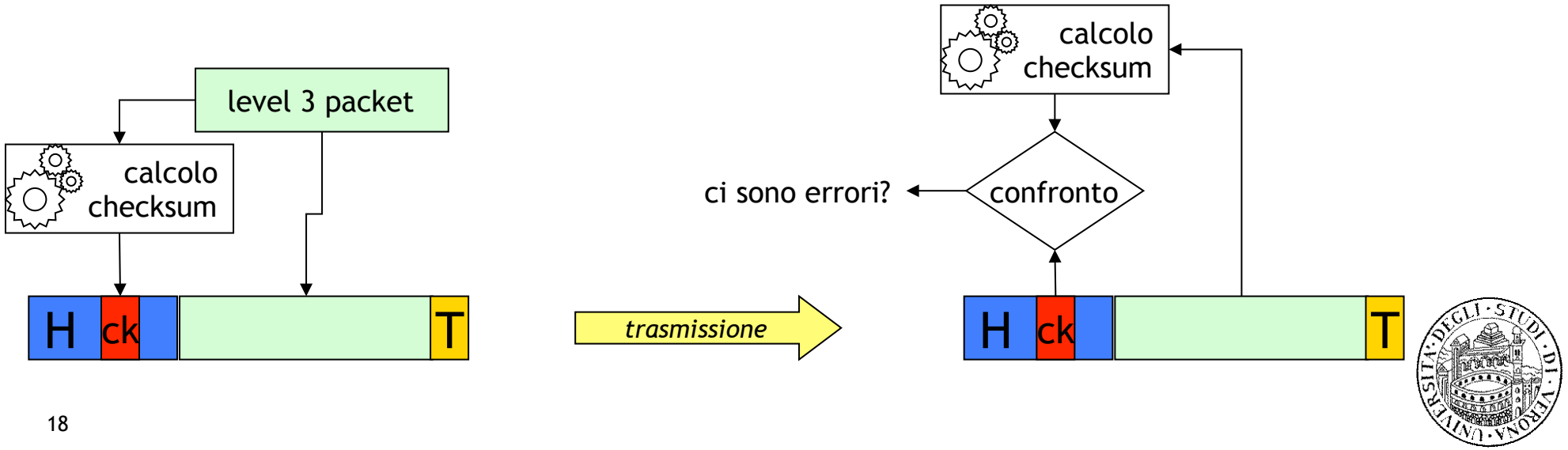
“01101” ⇨



  - determinate combinazioni non sono quindi usate per i dati e possono essere quindi utilizzate per il framing
    - ’00’ e ’11’

# Rilevazione dell'errore

- Il livello fisico offre un canale di trasmissione ***non privo di errori***
  - errori sul singolo bit
  - replicazione di bit
  - perdita di bit
- Per la rilevazione di tali errori, nell'header di ogni trama il livello 2 inserisce un campo denominato **checksum**
  - il checksum è il risultato di un calcolo fatto utilizzando i bit della trama
  - la destinazione ripete il calcolo e confronta il risultato con il checksum: se coincide la trama è corretta



# Gestione del flusso

- Problema: la sorgente trasmette le trame ad una velocità superiore di quella che la destinazione utilizza per accettare l'informazione
  - conseguenza: congestione del nodo destinazione
- Soluzione: implementare il **controllo di flusso**
- Il controllo della velocità di trasmissione della sorgente è basato su feedback inviati alla sorgente dalla destinazione indicando
  - di bloccare la trasmissione fino a comando successivo
  - la quantità di informazione che la destinazione è ancora in grado di gestire
- I feedback possono essere
  - nei servizi con riscontro, gli ack stessi
  - nei servizi senza riscontro, dei pacchetti appositi

# Gestione del flusso e recupero degli errori

- La principale tecnica di gestione del flusso è chiamata “controllo di flusso a finestra scorrevole”
  - possono essere trasmessi solo i pacchetti all’interno della finestra
  - quando il feedback è positivo, la finestra scorre e nuovi pacchetti possono essere trasmessi
- Contemporaneamente vengono definite delle tecniche di recupero degli errori
  - stop and wait
  - go-back-N
  - selective repeat
- Nelle reti TCP/IP (la maggior parte delle reti dati è di questo tipo) il controllo di flusso e il recupero degli errori è demandato ai livelli superiori
  - a livello 2 non vi sono feedback della destinazione per cui la sorgente trasmette le trame indipendentemente
  - viene controllata la presenza di errori e, in caso di errore, la trama viene semplicemente scartata senza gestire il recupero

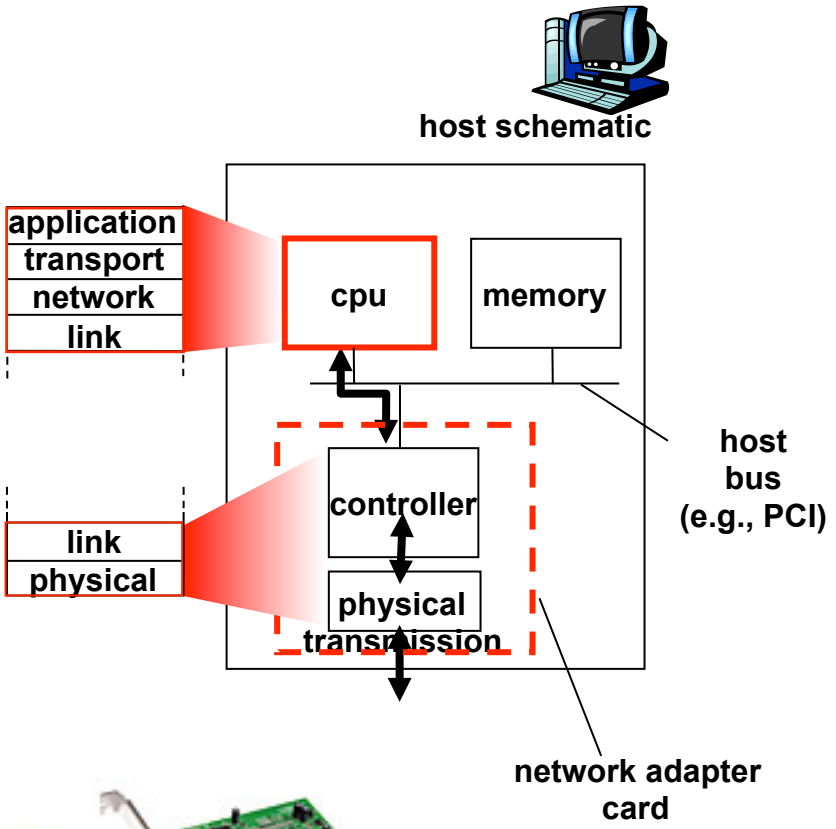
# Il sotto-livello MAC

# Introduzione di un nuovo sotto-livello

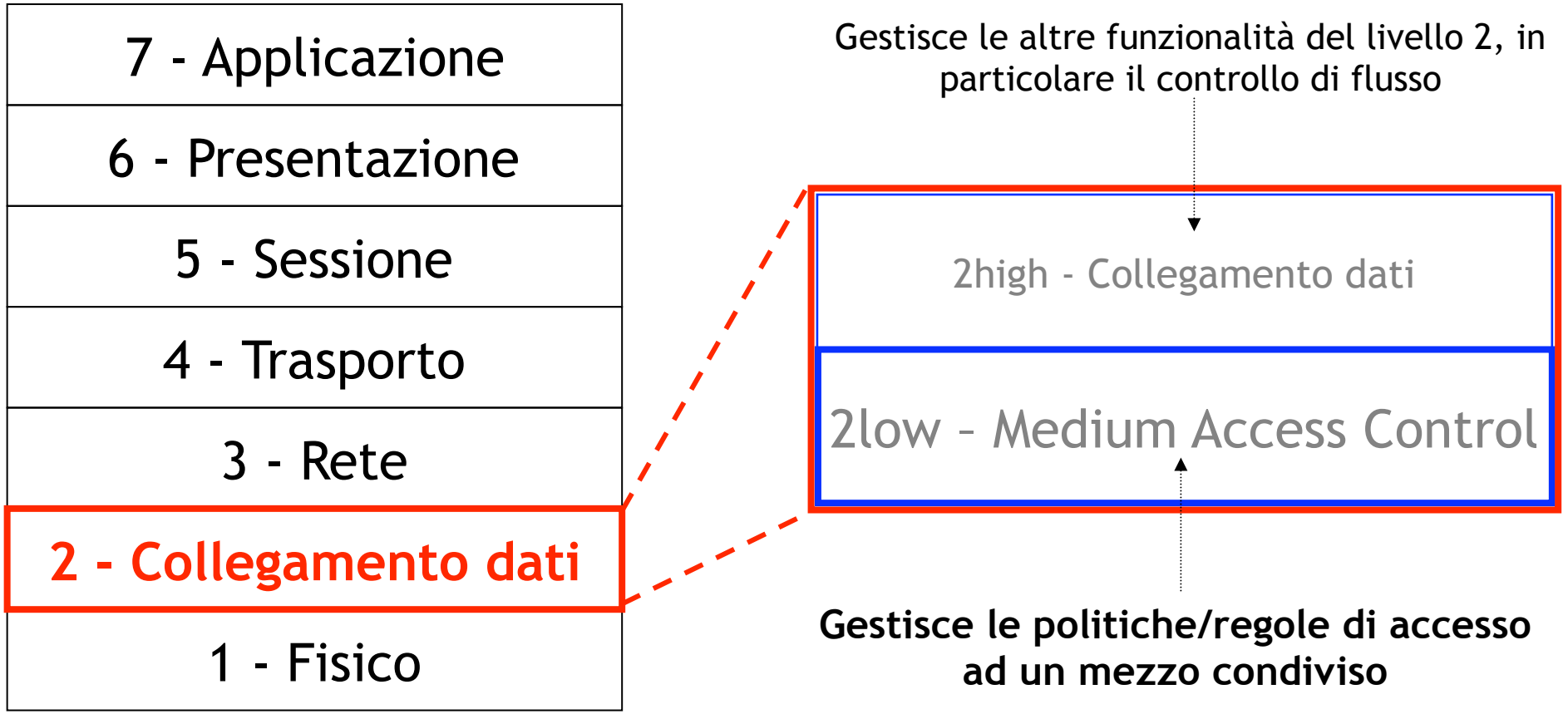
- Abbiamo visto che il livello 2 gestisce un insieme di problematiche svolgendo le funzioni di framing, rivelazione degli errori, controllo di flusso
- Bisogna considerare però che il livello 2 ha a che fare con il livello 1, ovvero il livello fisico (direttamente collegato al mezzo fisico)
- Il mezzo fisico può essere:
  - dedicato (reti punto-punto)
  - condiviso (reti broadcast)
- Se il mezzo fisico è condiviso, nascono una serie di problematiche relative all'accesso a tale mezzo
  - selezione dell'host che ha il diritto di trasmettere sul mezzo condiviso
  - situazione di competizione per la risorsa trasmissiva
- Viene introdotto un sotto-livello al livello 2 che gestisce queste problematiche
  - **MAC (Medium Access Control)**

# Where is the link layer implemented?

- in each and every host
- link layer implemented in "adaptor" (aka *network interface card* NIC)
  - Ethernet card, PCMCI card, 802.11 card
  - implements link, physical layer
- attaches into host's system buses
- combination of hardware, software, firmware




# Livello MAC




NOTA: anche se in linea di principio il livello MAC gestisce *l'accesso al mezzo* e il livello "high" gestisce le altre funzionalità, nella pratica il livello MAC gestisce anche il framing e il controllo di errore, mentre il livello 2 "high" si occupa del *controllo di flusso*. Nello stack TCP/IP ove il livello 2 non fa controllo di flusso, il livello 2 "high" è completamente assente o, se c'è, non svolge nessuna funzione

# Definizione del problema

- Per mezzo ***condiviso*** si intende che un unico canale trasmissivo può essere usato da più sorgenti
  - esempio: stanza piena di persone che vogliono parlare tra di loro
    - se tutti parlano contemporaneamente, non potrà esserci scambio di informazione
    - l'opposto è avere un mezzo dedicato per ogni coppia di persone che vuole parlare (ad esempio un tubo o una coppia di walkie-talkie)
- E' necessario definire una serie di regole per poter utilizzare il mezzo (tecniche di allocazione del canale)
  - se due sorgenti parlano contemporaneamente vi sarà collisione è l'informazione andrà persa

# Tecniche di allocazione del canale

- Esistono due categorie in cui rientrano le tecniche di allocazione del canale trasmissivo
  - allocazione statica
    - il mezzo trasmissivo viene “partizionato” e ogni porzione viene data alle diverse sorgenti
    - il partizionamento può avvenire in base:
      - al tempo: ogni sorgente ha a disposizione il mezzo per un determinato periodo
      - alla frequenza: ogni sorgente ha a disposizione una determinata frequenza (si pensi alle stazioni radiofoniche ove il canale trasmissivo è l’aria...)
  - allocazione dinamica
    - il canale viene assegnato di volta in volta a chi ne fa richiesta e può essere utilizzato una volta che questi ha finito di usarlo e lo libera

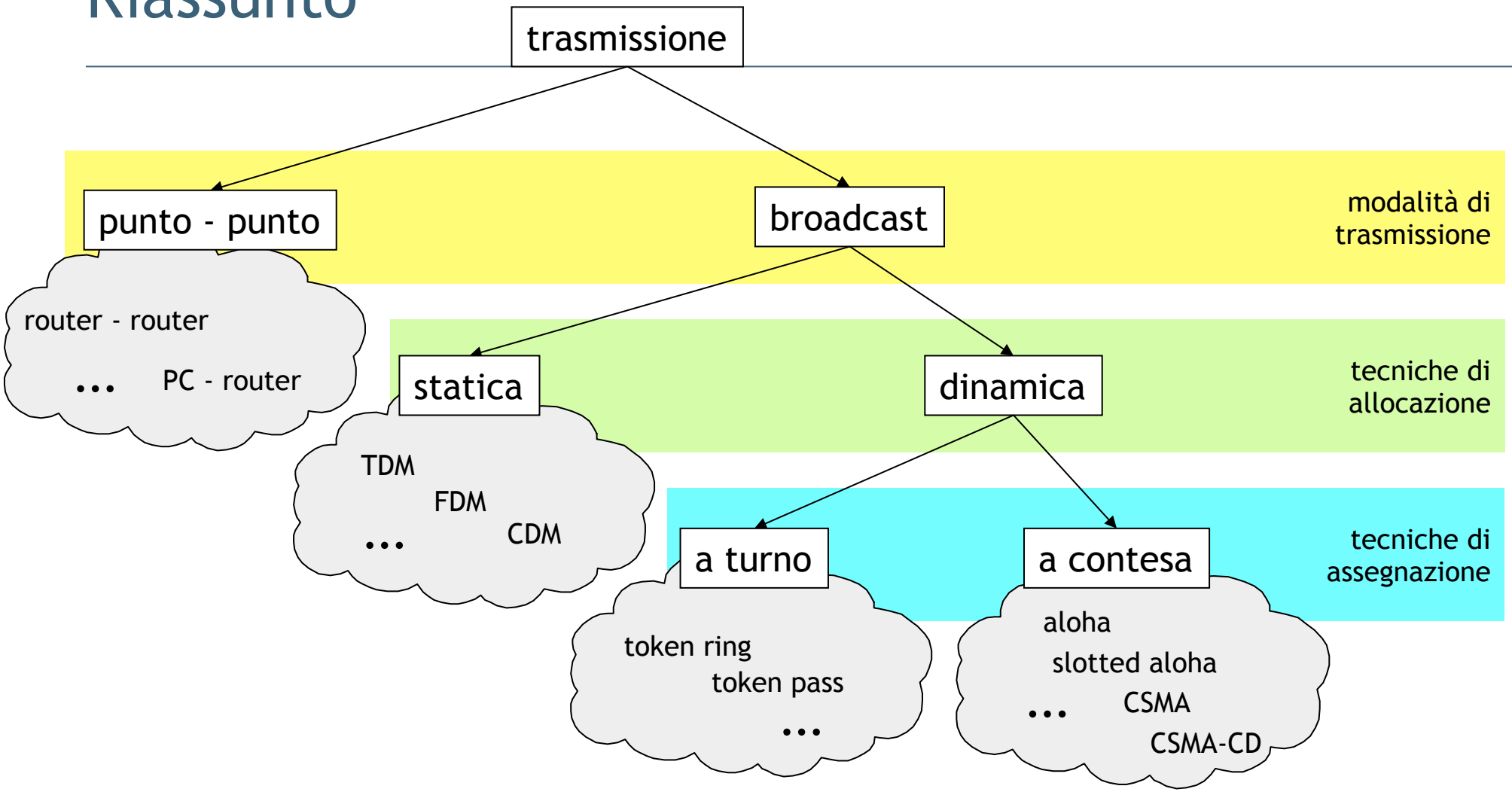
# Allocazione statica

- Soluzioni “tradizionali” (Protocolli a suddivisione del canale)
  - Frequency Division Multiplexing
  - Time Division Multiplexing
- Buona efficienza in situazioni di ***pochi utenti con molto carico costante nel tempo***
- Meccanismi di semplice implementazione (FDM)
- Tuttavia...
  - molti utenti
  - traffico discontinuo
- ...generano una scarsa efficienza di utilizzo delle risorse trasmissive
  - le risorse dedicate agli utenti “momentaneamente silenziosi” sono perse

# Allocazione dinamica

- Il canale trasmissivo può essere assegnato:
  - a turno (“Taking turns” o a rotazione)
    - viene distribuito il “permesso” di trasmettere; la durata viene decisa dalla sorgente
  - a contesa (Protocolli ad accesso casuale)
    - ciascuna sorgente prova a trasmettere indipendentemente dalle altre
- Nel primo caso si presuppone la presenza di meccanismi per l’assegnazione del permesso di trasmettere
  - overhead di gestione
- Nel secondo caso non sono previsti meccanismi particolari
  - sorgente e destinazione sono il più semplici possibile
- I protocolli che gestiscono la trasmissione a contesa sono generalmente i più utilizzati

# Riassunto




**In generale**: se le risorse sono scarse rispetto alle esigenze delle stazioni (tante stazioni con molti dati), un accesso statico (*multiplazione*) è preferibile; viceversa, ovvero con tante risorse rispetto alle necessità delle stazioni e traffico generato discontinuo, l'allocazione dinamica (*accesso multiplo*) risulta più efficiente

# Allocazione dinamica con contesa: ipotesi

- Analizziamo in dettaglio le prestazioni ottenibili da protocolli (protocollo: insieme di regole...) progettati per gestire l'allocazione dinamica del canale con contesa della risorsa. Seguono una serie di ipotesi per semplificare il problema

1. **Single channel assumption**
   - unico canale per tutte le comunicazioni
2. **Station model**
   - *N* stazioni indipendenti ognuna delle quali è sorgente di trame di livello 2
   - le trame sono generate secondo la distribuzione di Poisson con media **S**
   - la lunghezza delle trame è fissa, ovvero il tempo di trasmissione è costante e pari a **T** (tempo di trama)
   - una volta generata una trama, la stazione è bloccata fino al momento di corretta trasmissione
3. **Collision assumption**
   - due trame contemporaneamente presenti sul canale generano collisione
   - non sono presenti altre forme di errore
4. **Tempo...**
   - continuo: la trasmissione della trama può iniziare in qualunque istante
   - *slotted*: la trasmissione della trama può iniziare solo in istanti discreti
5. **Ascolto del canale...**
   - *carrier sense*: le stazioni sono in grado di verificare se il canale è in uso prima di iniziare la trasmissione di una trama (questo equivale a dire che il tempo di propagazione t è =< T)

# Protocolli di accesso multiplo

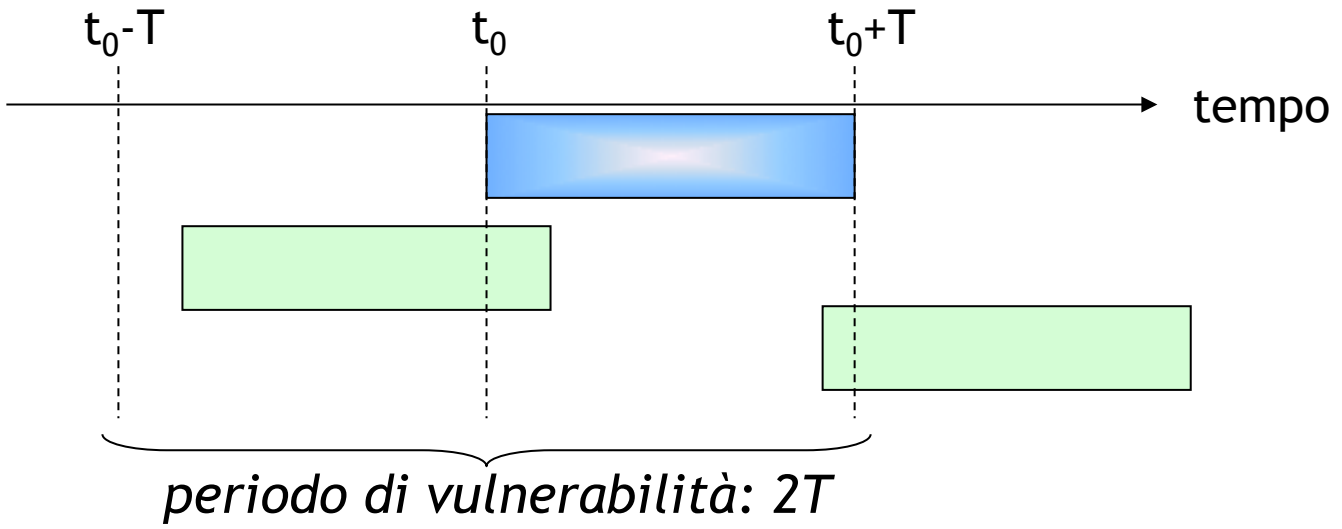
- In letteratura sono disponibili molti algoritmi di accesso multiplo al mezzo condiviso con contesa
- Principali algoritmi (utilizzati dai protocolli):
  - ALOHA
    - Pure ALOHA
    - Slotted ALOHA
  - Carrier Sense Multiple Access Protocols
    - CSMA
    - CSMA-CD (con rilevazione della collisione)

# Pure ALOHA

- Definito nel 1970 da N. Abramson all'università delle Hawaii
- Algoritmo:
  - una sorgente può trasmettere una trama ogniqualvolta vi sono dati da inviare *(continuous time)*
  - la sorgente rileva, ascoltando il canale, l'eventuale collisione
  - collisione ⇨ la sorgente aspetta un tempo casuale e ritrasmette la trama
    - un tempo deterministico porterebbe ad una situazione di collisione all'infinito

# Periodo di vulnerabilità

- Si definisce “periodo di vulnerabilità” l’intervallo di tempo in cui può avvenire una collisione che invalida una trasmissione
- Detto T il tempo di trama e $t_0$ l’inizio della trasmissione da parte di una sorgente, il periodo di vulnerabilità è pari al doppio del tempo di trama
  - nel momento in cui inizia a trasmettere ($t_0$), nessuna altra sorgente deve aver iniziato la trasmissione dopo l’istante di tempo $t_0$ -T e nessuna altra sorgente deve iniziare la trasmissione fino a $t_0$ +T



# Prestazioni

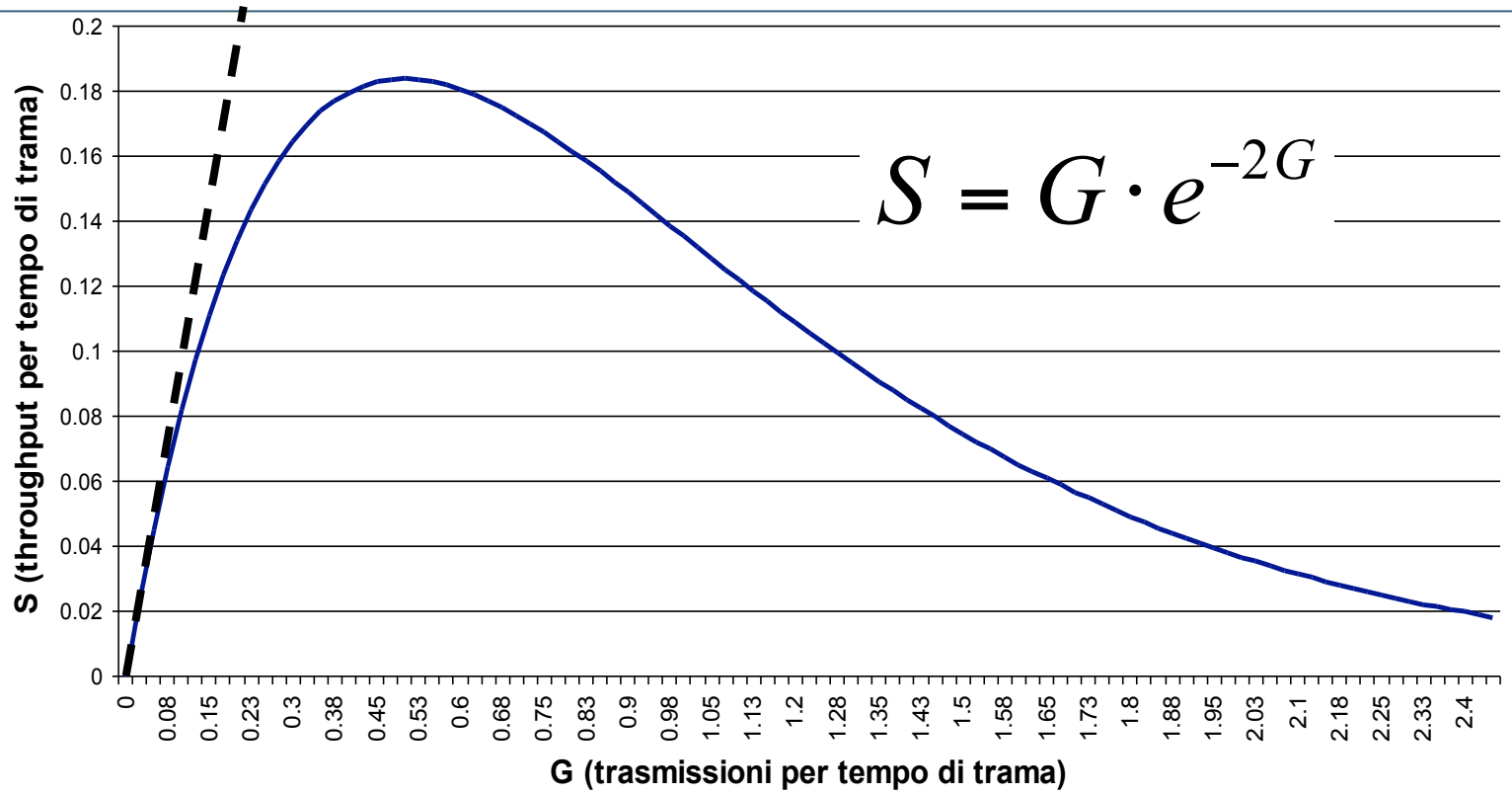
- Ipotesi
  - trame di lunghezza fissa
  - tempo di trama: tempo necessario per trasmettere una trama
  - popolazione ∞ che accede ad un mezzo condiviso
- Traffico generato (numero di trame per tempo di trama) segue la distribuzione di Poisson con media G
  - G ingloba anche il numero di ri-trasmissioni dovuto a collisioni
- Il throughput reale è dato da
  - numero medio di trasmissioni * probabilità che non ci siano trasmissioni per tutto il periodo di vulnerabilità (2 tempi di trama consecutivi)

    → S = G*P[0 trasmissioni per 2T], ovvero

$$S = G \cdot e^{-2G}$$

G = numero medio di trame trasmesse nel tempo di trama
S = numero medio di trame trasmesse con successo (throughput)

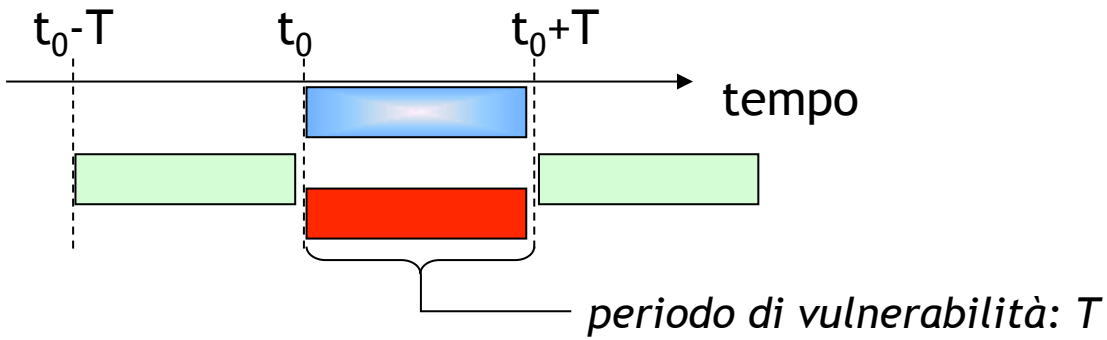
# Prestazioni




- ALOHA permette al massimo di sfruttare il 19% degli slot liberi (nel caso in cui mediamente vengono generati 0.5 trasmissioni per tempo di trama)

# Slotted ALOHA

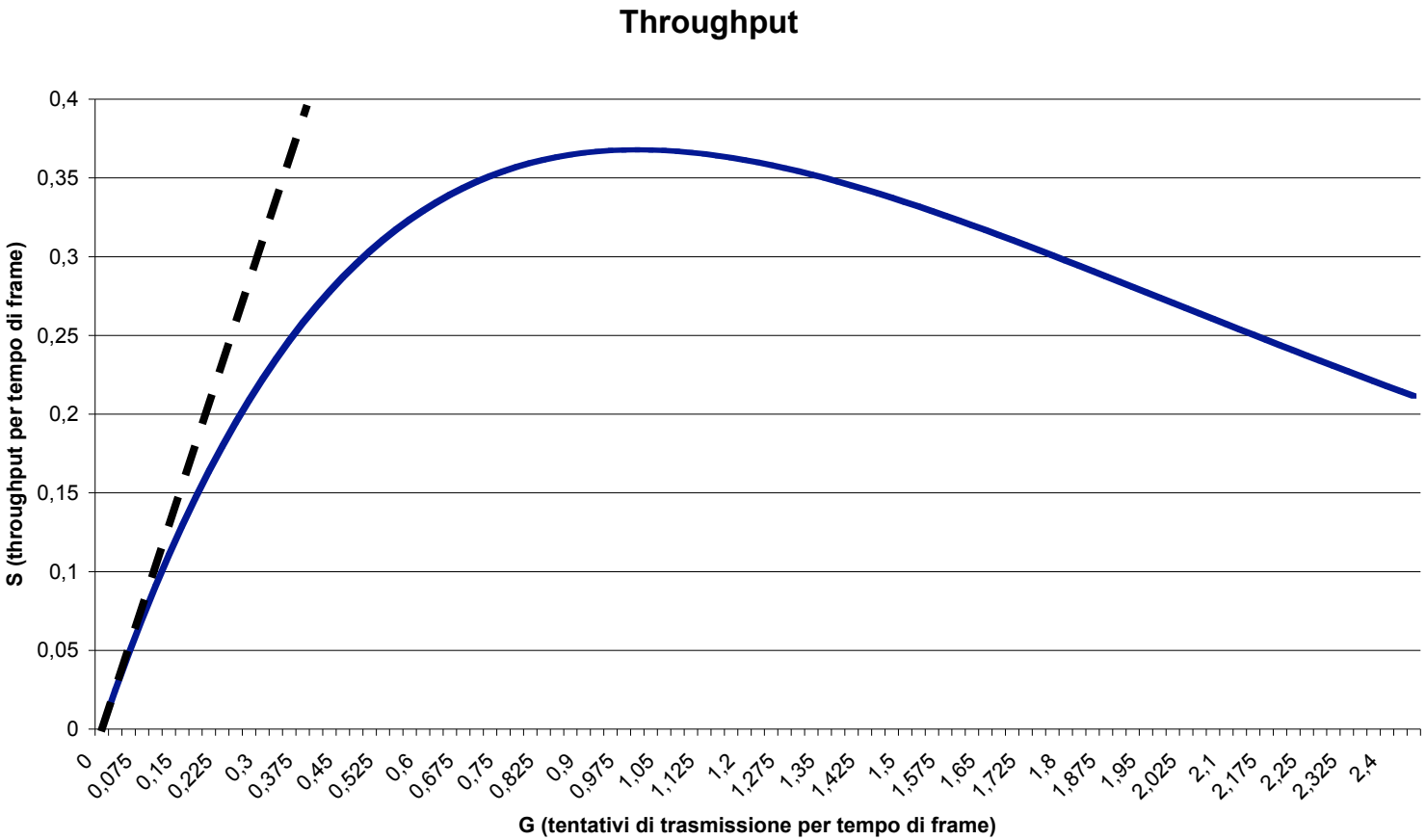
- Proposto nel 1972 da Roberts per duplicare la capacità di Pure ALOHA
- Basato su ipotesi di *slotted time* (tempo suddiviso ad intervalli discreti)
- Algoritmo:
  - Pure ALOHA
  - la trasmissione di una trama può iniziare solo ad intervalli discreti
  - necessaria sincronizzazione tra stazioni
- Periodo di vulnerabilità: T (tempo di trama)



# Prestazioni

- Il periodo di vulnerabilità è dimezzato, quindi il throughput reale è dato da

$$S = G \cdot e^{-G}$$




- Slotted ALOHA permette al massimo di sfruttare il 37% degli slot liberi (nel caso in cui mediamente viene generata 1 trasmissione per tempo di trama)

# Carrier Sense Multiple Access (CSMA)

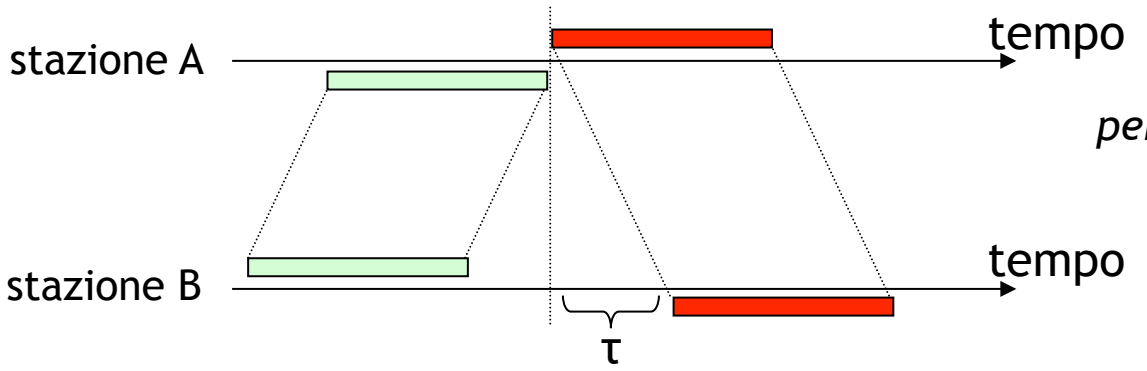
- Ambito LAN: le stazioni possono monitorare lo stato del canale di trasmissione (ritardi bassi)
- Le stazioni sono in grado di "ascoltare" il canale *prima di iniziare a trasmettere* per verificare se c'è una trasmissione in corso
- Algoritmo
  - se il canale è libero, si trasmette
  - se è occupato, sono possibili diverse varianti
    - non-persistent
      - rimanda la trasmissione ad un nuovo istante, scelto in modo casuale
    - persistent
      - nel momento in cui si libera il canale, la stazione inizia a trasmettere
  - se c'è collisione, come in ALOHA, si attende un tempo casuale e poi si cerca di ritrasmettere

# CSMA: modalità p-persistent

- Il tempo viene suddiviso in intervalli
  - la lunghezza degli intervalli è uguale alal periodo di vulnerabilità
    - *round trip propagation delay* $2\tau$
- Algoritmo
  1. ascolta il canale
     - se il canale è libero
       - si trasmette con probabilità p;
       - se si è deciso di trasmettere, si passa al punto 2
       - se non si è deciso di trasmettere, si attende un intervallo di tempo e si torna al punto 1
     - se è occupato, si attende un intervallo di tempo e si torna al punto 1
  2. se c'è collisione
     - si attende un tempo casuale e poi si torna al punto 1

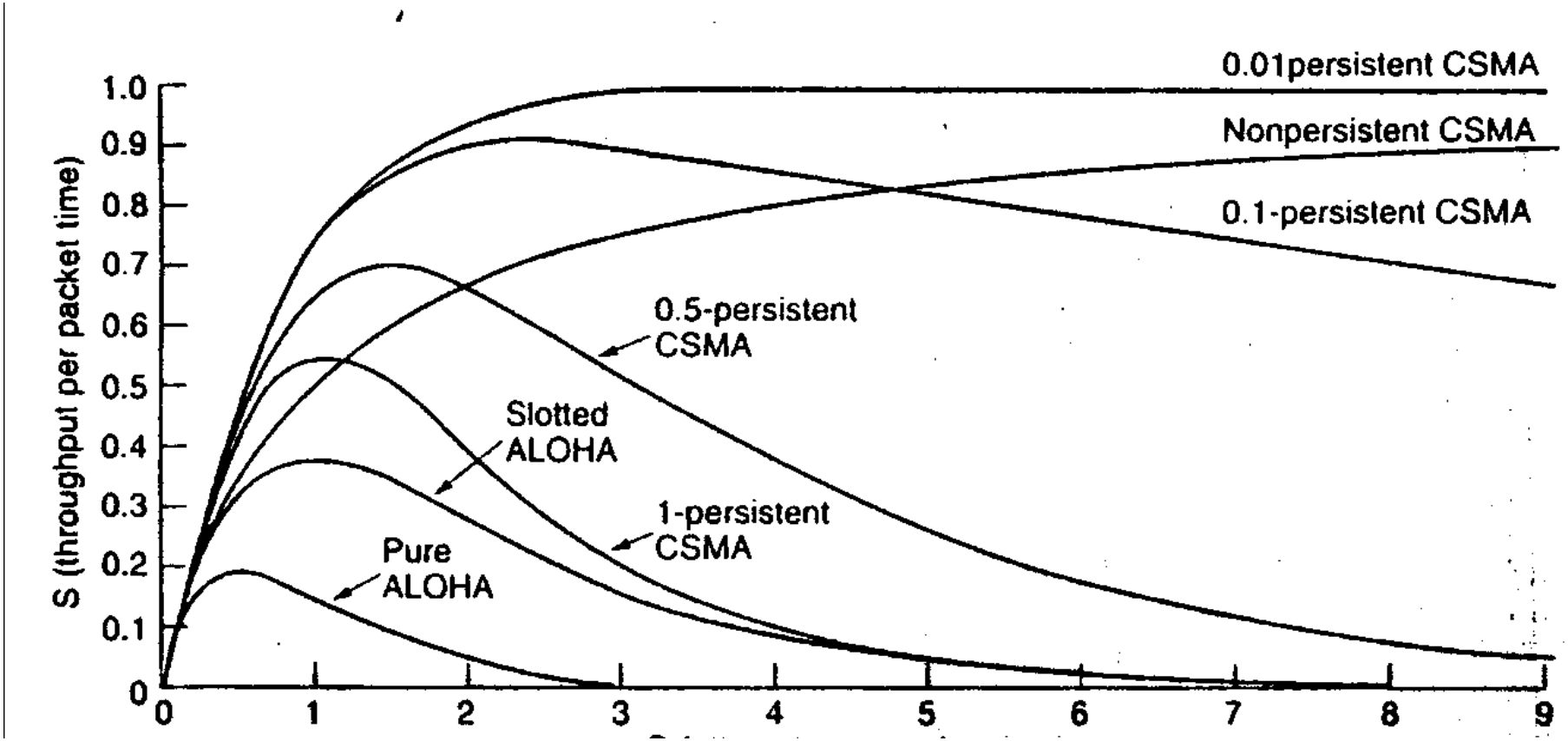
# Periodo di vulnerabilità

- In questo caso il periodo di vulnerabilità è legato al ritardo di propagazione del segnale (τ)
  - se una stazione ha iniziato a trasmettere, ma il suo segnale non è ancora arrivato a tutte le stazioni, qualcun altro potrebbe iniziare la trasmissione
  - periodo di vulnerabilità → 2τ
- A seconda del ritardo di propagazione, se questi risulta paragonabile al tempo si trama o meno, si hanno prestazioni differenti
- In generale, il CSMA viene usato in reti in cui il ritardo di propagazione τ è << di T (tempo di trama)




*periodo di vulnerabilità*: 2τ

# Confronto efficienza algoritmi




(fonte: A. Tanenbaum, Computer Networks)

# CSMA con Collision Detection (CSMA-CD)

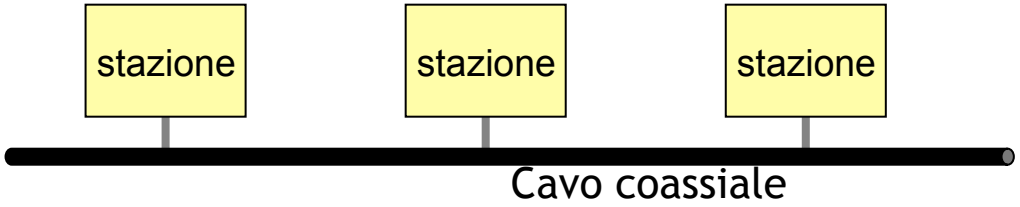
- Miglioramento
  - se la stazione che sta trasmettendo rileva la collisione, interrompe immediatamente
- In questo modo, una volta rilevata collisione, non si spreca tempo a trasmettere trame già corrotte
- Inoltre, per far sentire a tutte le stazioni che vi è stata collisione, si trasmette una particolare sequenza, detta di jamming

# Riassunto

- Finora abbiamo visto
  - tecniche di trasmissione
    - punto-punto
    - broadcast
  - tra queste, esistono varie tecniche di allocazione del canale comune
    - statiche → TDM, FDM, ... usate per le comunicazioni radiomobili, in cui il mezzo condiviso è l'aria
    - dinamiche
  - tra queste, esistono varie tecniche di assegnazione del canale
    - a contesa → Aloha, Slotted-Aloha, CSMA, CSMA-CD; quest'ultima, nella versione 1 persistent, è quella più diffusa nelle reti locali (LAN Ethernet)
    - a turno
      - tra queste ultime, esistono alcune importanti tecniche basate sul token (= gettone; solo chi possiede il token in quel momento può trasmettere)
        - » Token Ring, token bus

# LAN estese

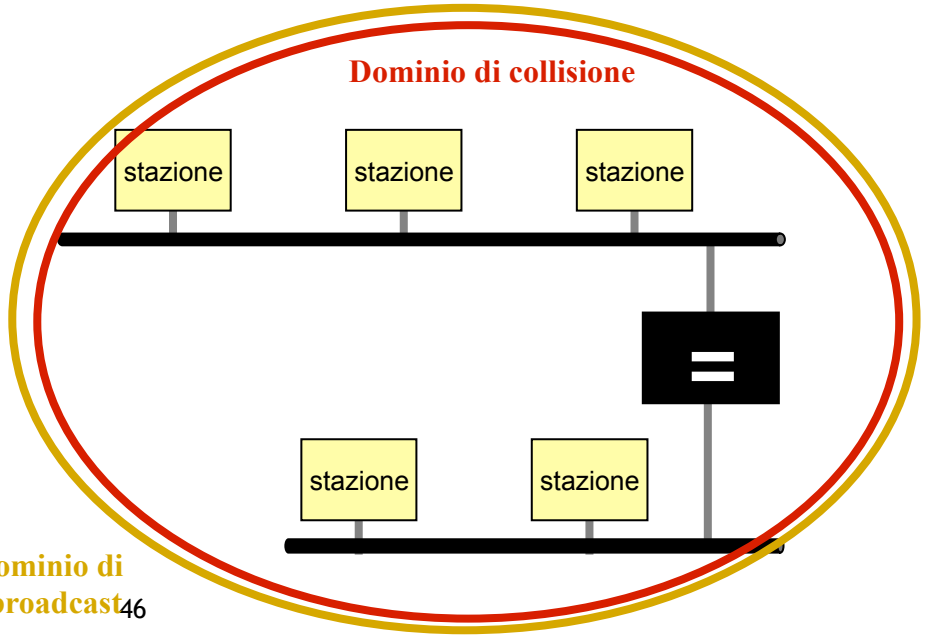
# Introduzione

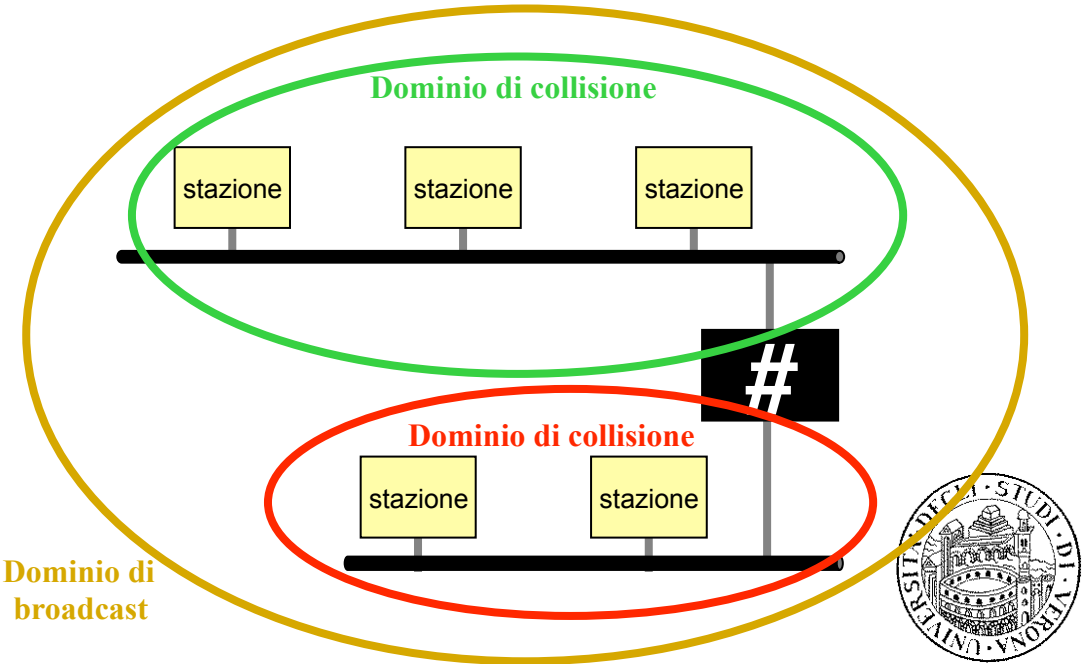



- La scelta di utilizzare mezzi condivisi per l'accesso al canale di trasmissione è stata fatta sia per necessità (ad es. trasmissioni wireless) sia motivi economici
- Grazie proprio agli aspetti economici, tale tecnologia è stata utilizzata e si è diffusa particolarmente nelle *reti locali* (Local Area Networks, LAN)
- La rappresentazione tipica di una LAN è una serie di stazioni (PC) connesse ad un segmento di cavo (bus)
- Poiché il segmento non può essere troppo lungo...
  - attenuazione del segnale
  - disposizione spaziale delle stazioni all'interno di un edificio (ad es.: su più piani)
- ... nasce il problema di come estendere le LAN
- Esistono 3 tipi di apparati, in ordine crescente di complessità:
  - Repeater o Hub
  - Bridge
  - Switch

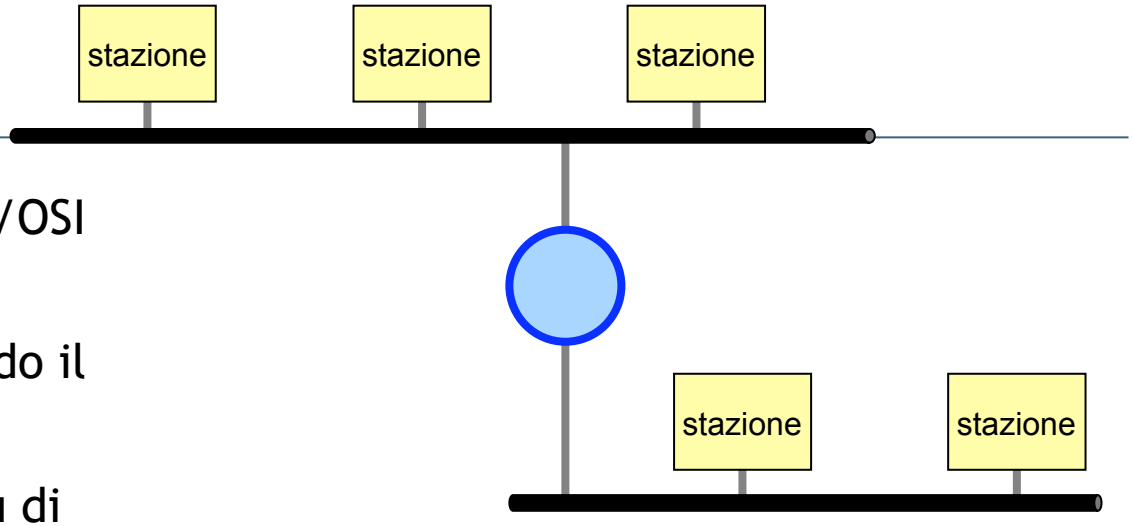
# Dominio di collisione – Dominio di broadcast

- Dominio di collisione
  - parte di rete per cui, se due stazioni trasmettono dati contemporaneamente, il segnale ricevuto dalle stazioni risulta danneggiato
- Dominio di broadcast (detto anche *Segmento data-link)*
  - parte di rete raggiunta da una trama con indirizzo broadcast (a livello 2)
- Stazioni appartenenti alla medesima rete di livello 2 condividono lo stesso dominio di broadcast
  - gli apparati che estendo le LAN possono solo influire sul dominio di collisione

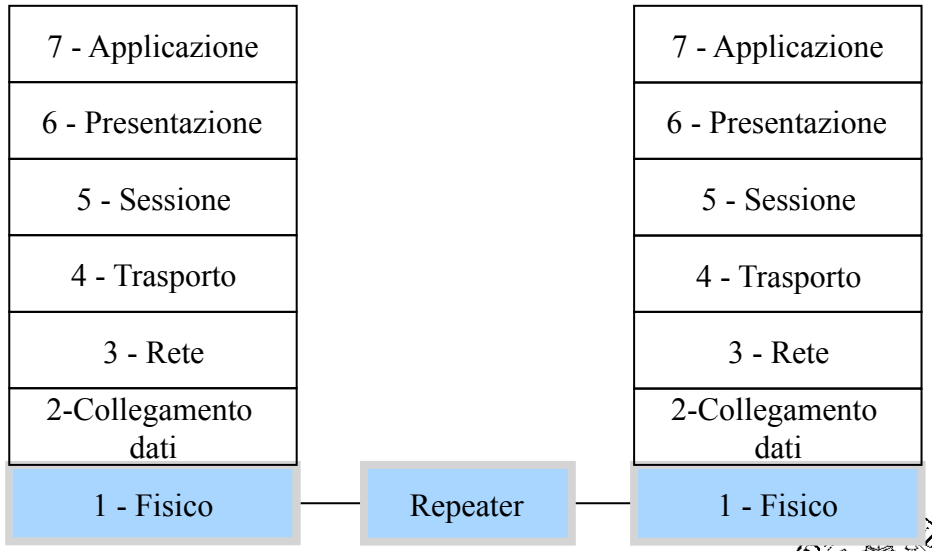


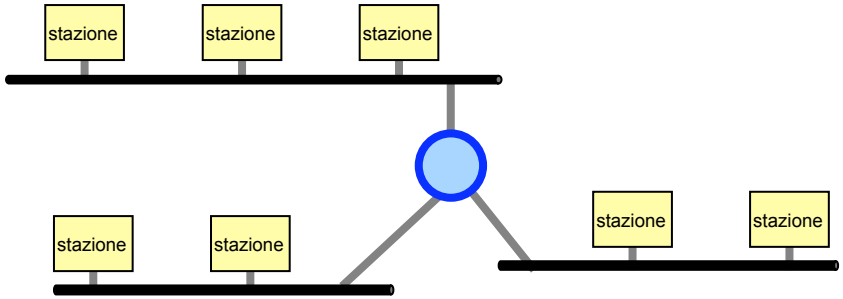
# Repeater e Hub

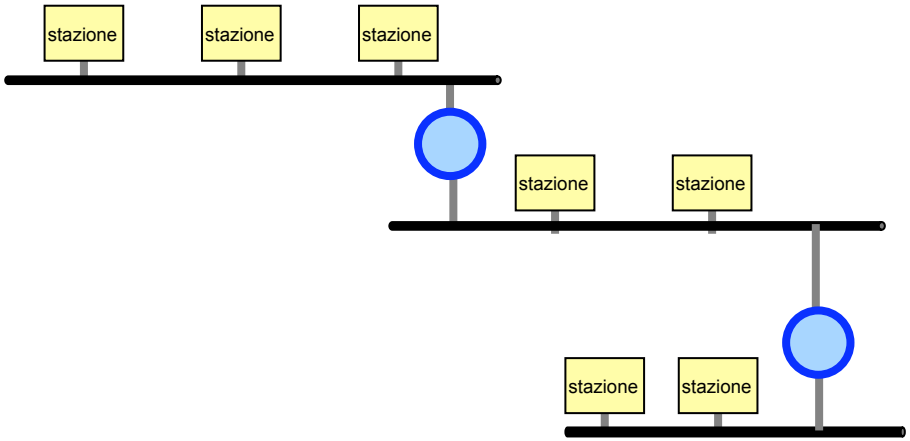


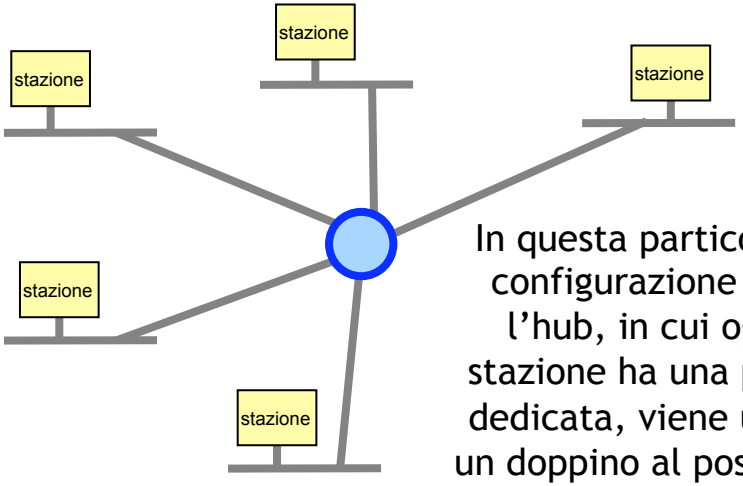

- Interviene solo a livello fisico ISO/OSI
- Replica le trame in arrivo da un segmento ad un altro, amplificando il segnale
- I repeater possono connettere più di due segmenti
  - in questo caso di parla di ***Hub***
    - copia le trame che riceve su una porta su tutte le altre porte
  - il segnale trasmesso da una stazione viene propagato a tutte le uscite
- Non ci possono essere più di 4 repeater in cascata tra due stazioni
- Il dominio di collisione coincide con il dominio di broadcast



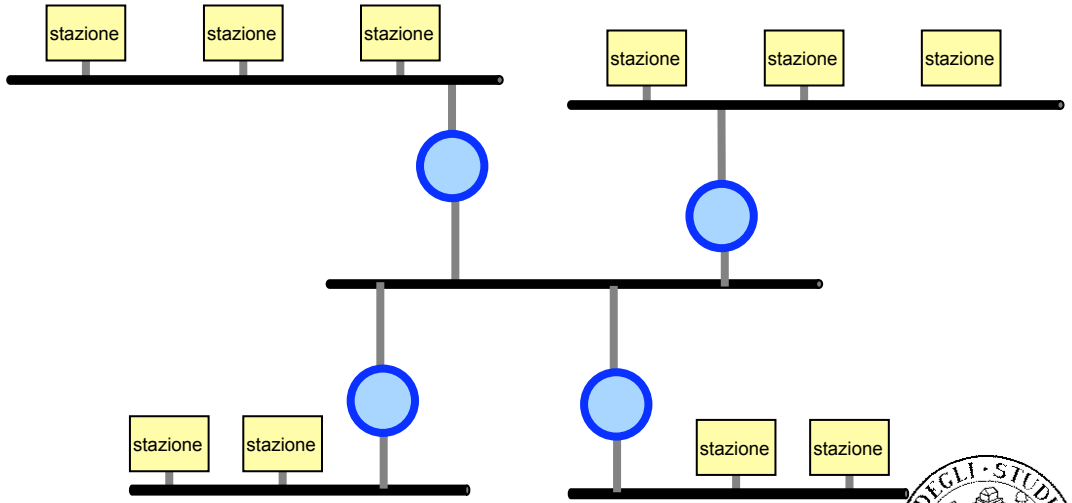
# Alcune possibili combinazioni



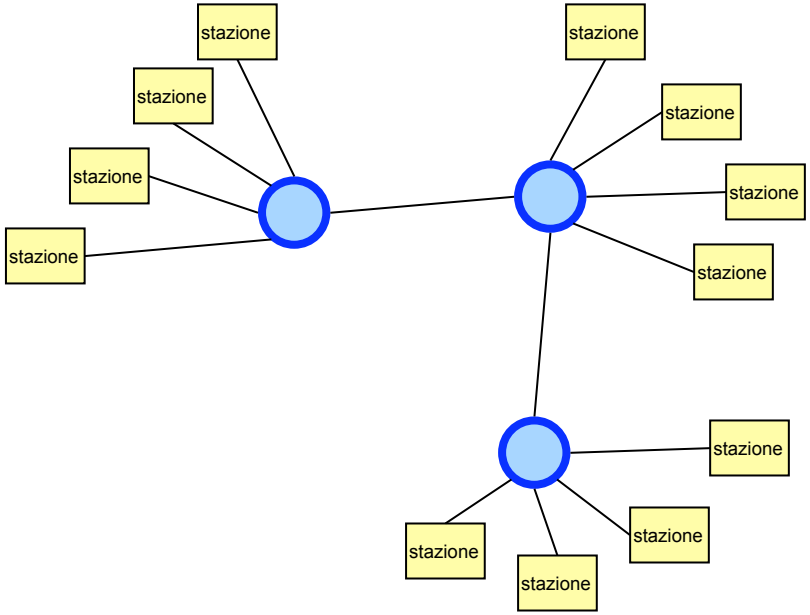



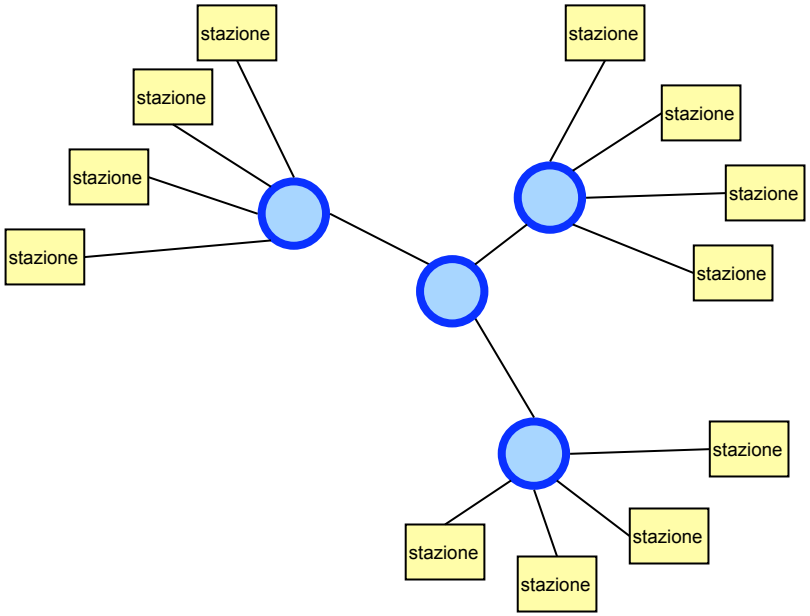




In questa particolare configurazione con l'hub, in cui ogni stazione ha una porta dedicata, viene usato un doppino al posto del cavo coassiale



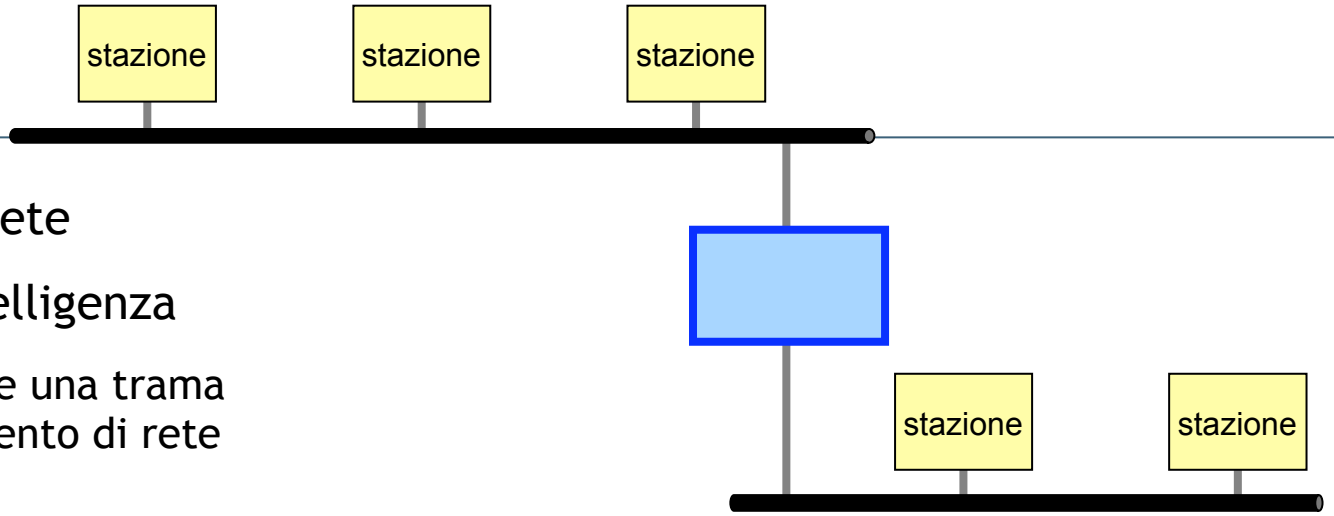
# e ancora...



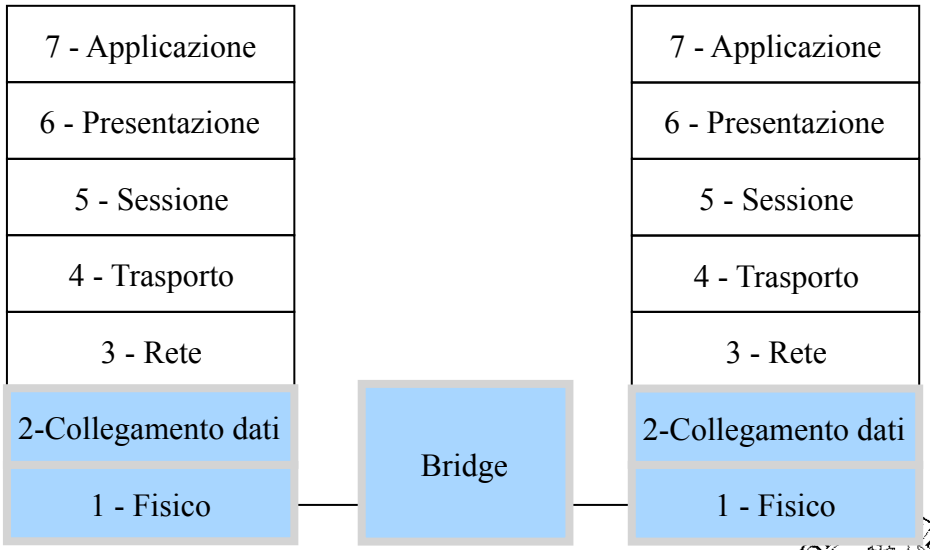




- Il problema legato a questo tipo di configurazioni è l'eccessiva estensione del dominio di collisione
  - con i repeater è come se tutte le stazioni condividessero lo stesso mezzo fisico

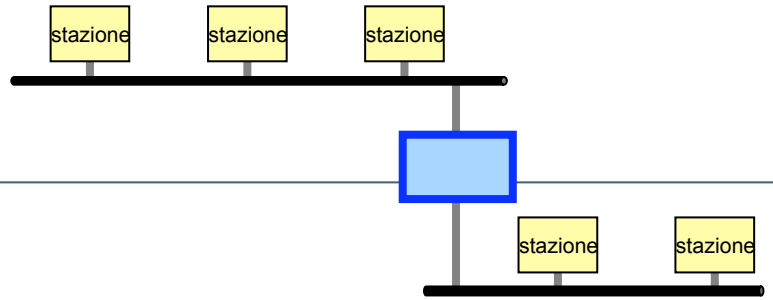
# Bridge

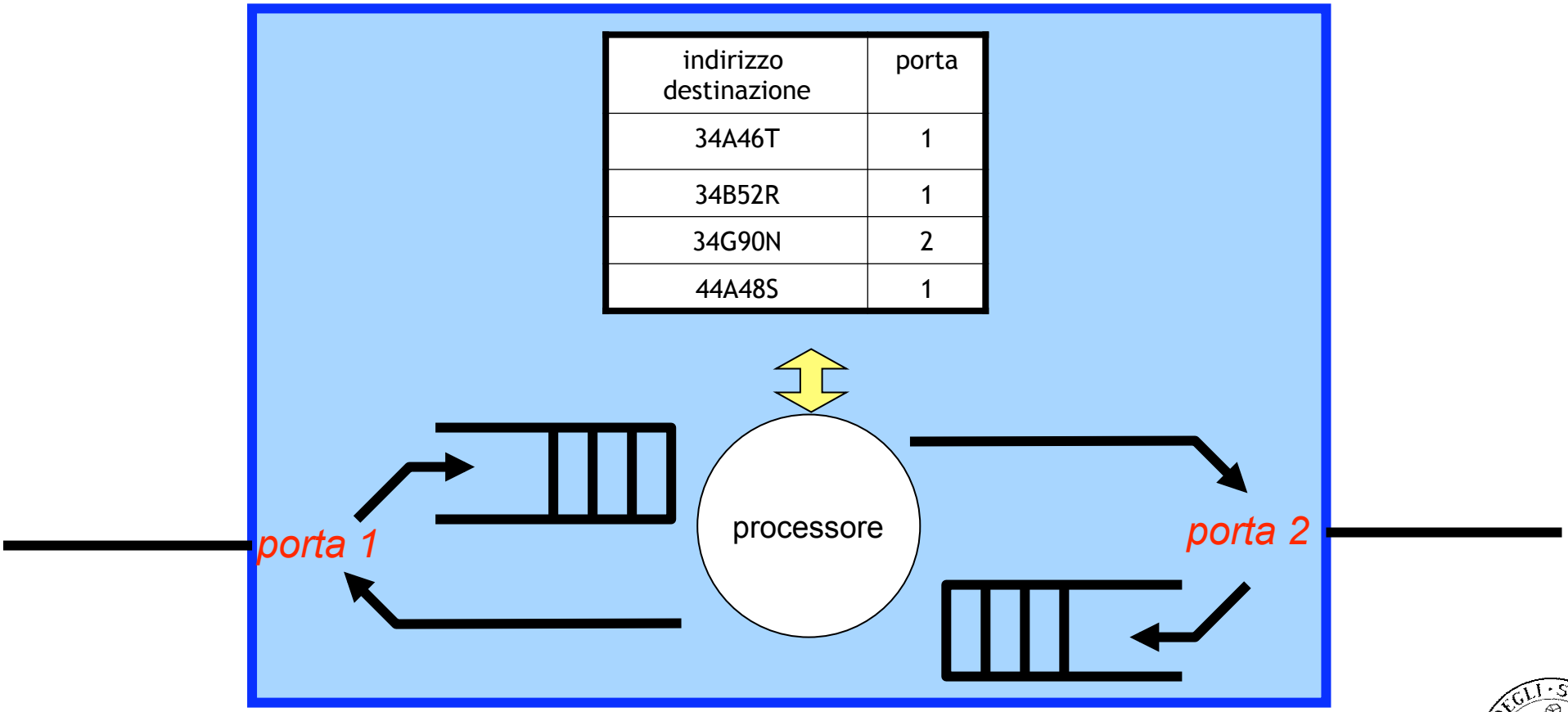



- Collega 2 segmenti di rete
- Apparato dotato di intelligenza
  - seleziona se ripetere una trama generata da un semento di rete sull'altro segmento
  - la selezione avviene in base ad una tabella che esso mantiene
  - in tale tabella c'è scritto quali stazioni fanno parte di ciascun segmento di rete
  - quando viene generata una trama, il bridge legge l'indirizzo di destinazione e in base alla propria tabella decide se propagare la trama nell'altro segmento di rete
- Spezza il dominio di collisione



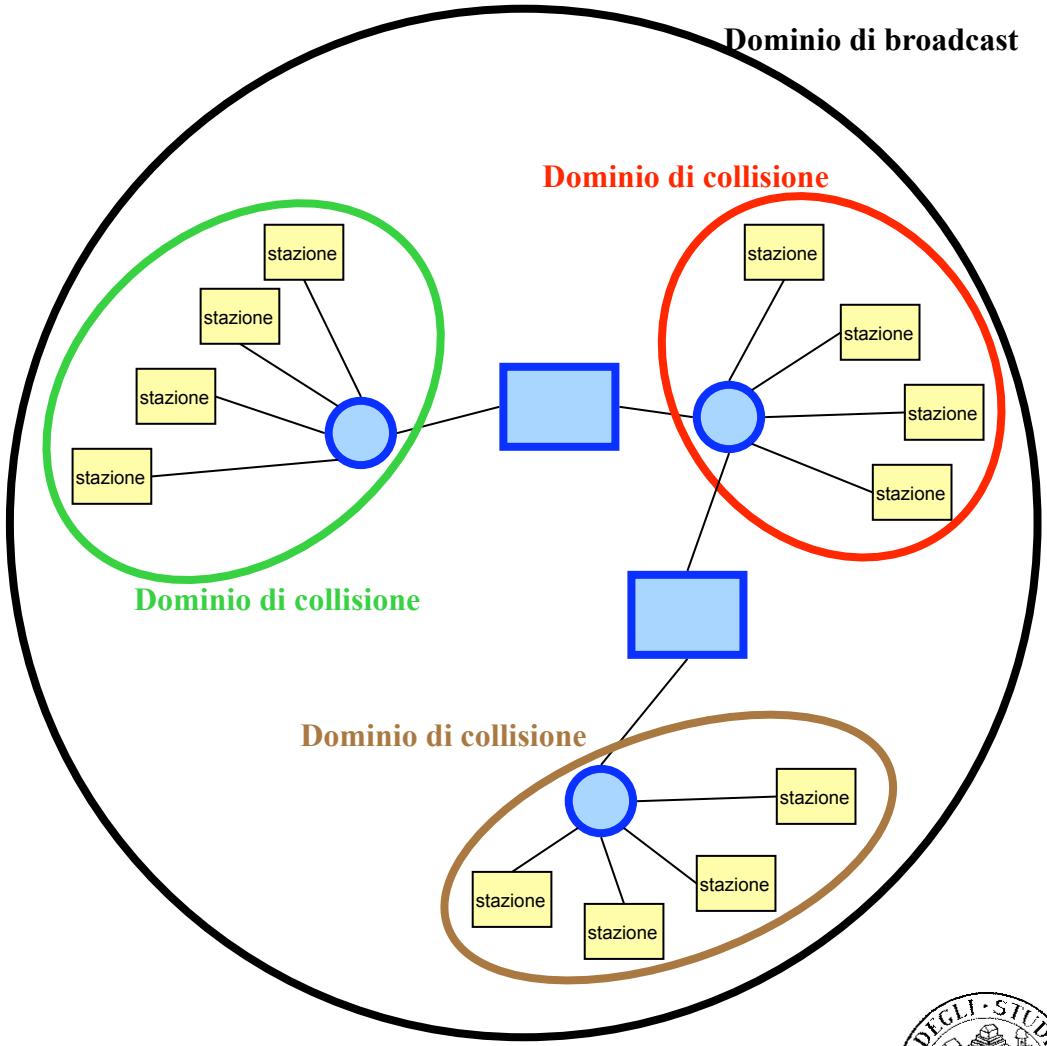
# Schema di un bridge



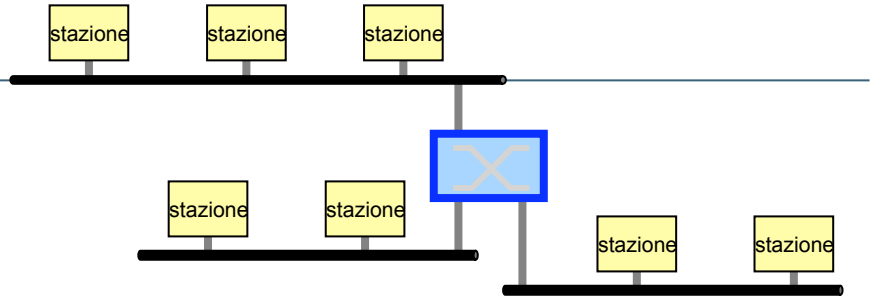



# Bridge: esempio di configurazione

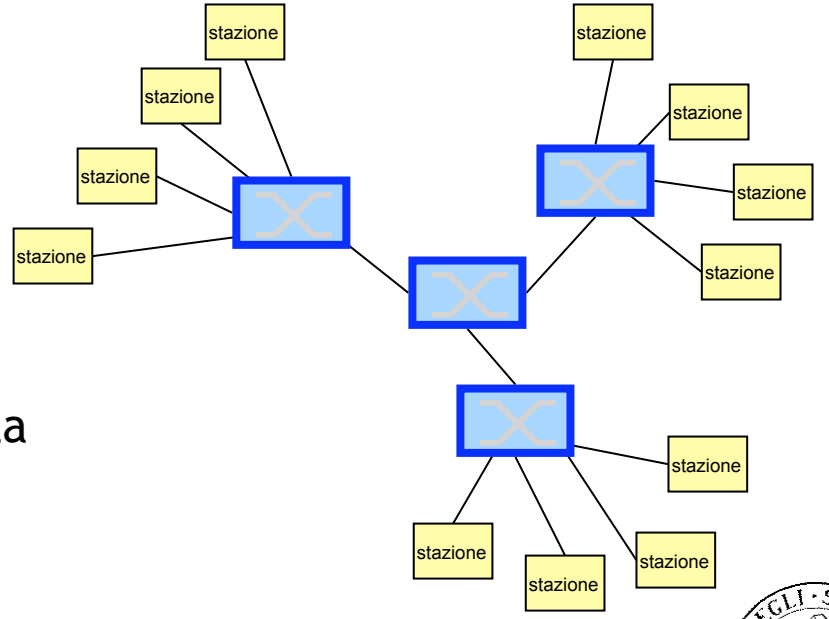
- Spezza il dominio di collisione, ovvero ciascun segmento di rete è conteso solo da chi è attestato sull'hub
- Gli hub vedono il bridge come una stazione qualsiasi che genera trame
- La trama è propagata dal bridge solo se il destinatario è attestato su un hub diverso da quello di origine
- Il concetto di *segmento data-link* viene preservato: ogni frame indirizzata ad un indirizzo broadcast di livello 2 viene ricevuta da tutti i nodi del segmento, anche se separati da diversi bridge



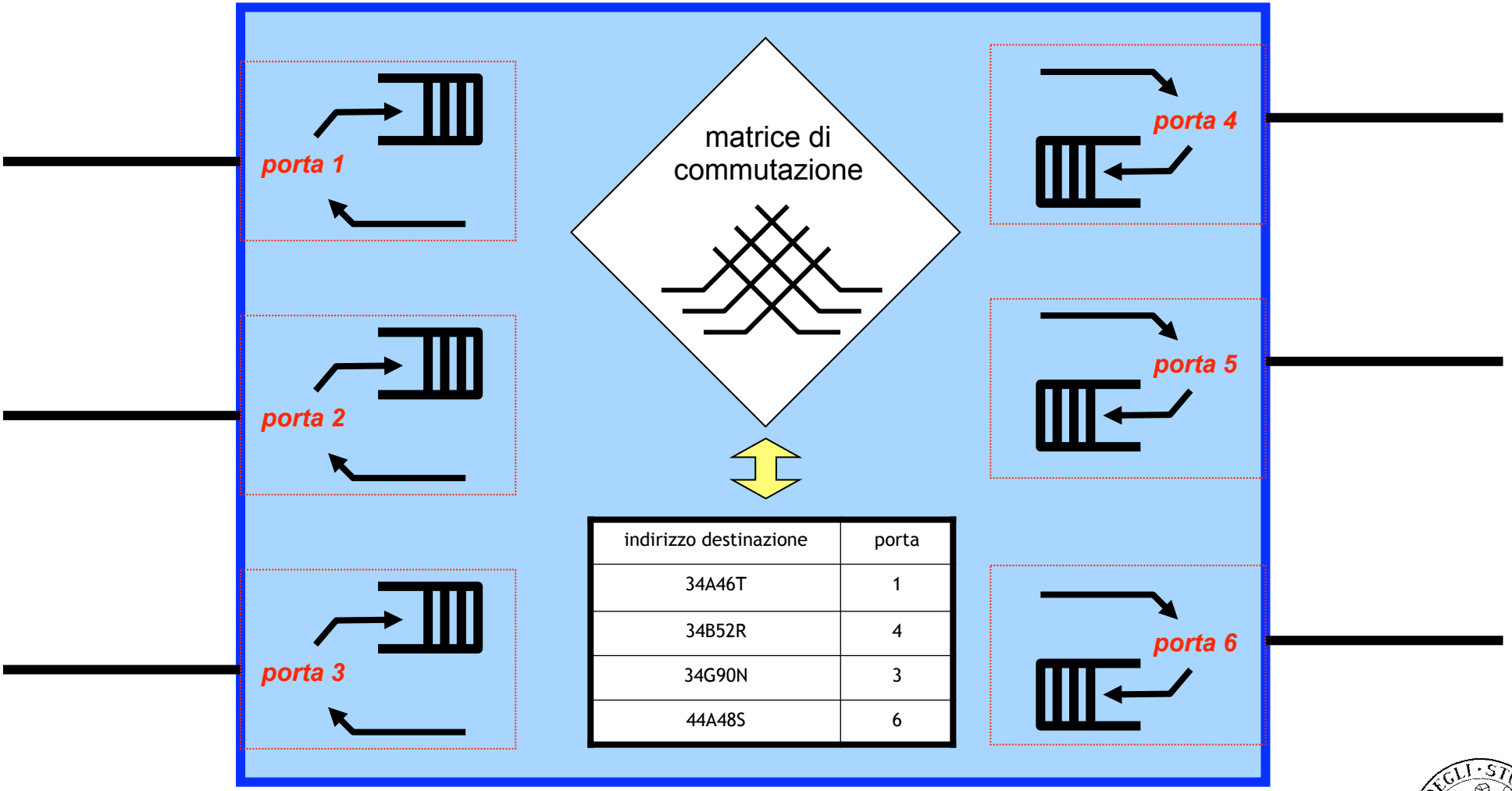
# Evoluzione: Layer 2 Switch




- Il bridge ha solo 2 porte
- Lo switch è un bridge multiporta
  - mantiene una tabella in cui sono associati indirizzi di livello 2 e segmenti di rete di appartenenza
- Spesso ogni porta è connessa ad un'unica stazione (invece che ad un segmento di rete)
  - realizza un accesso dedicato per ogni nodo
  - elimina le collisioni e dunque aumenta la capacità
  - supporta conversazioni multiple contemporanee



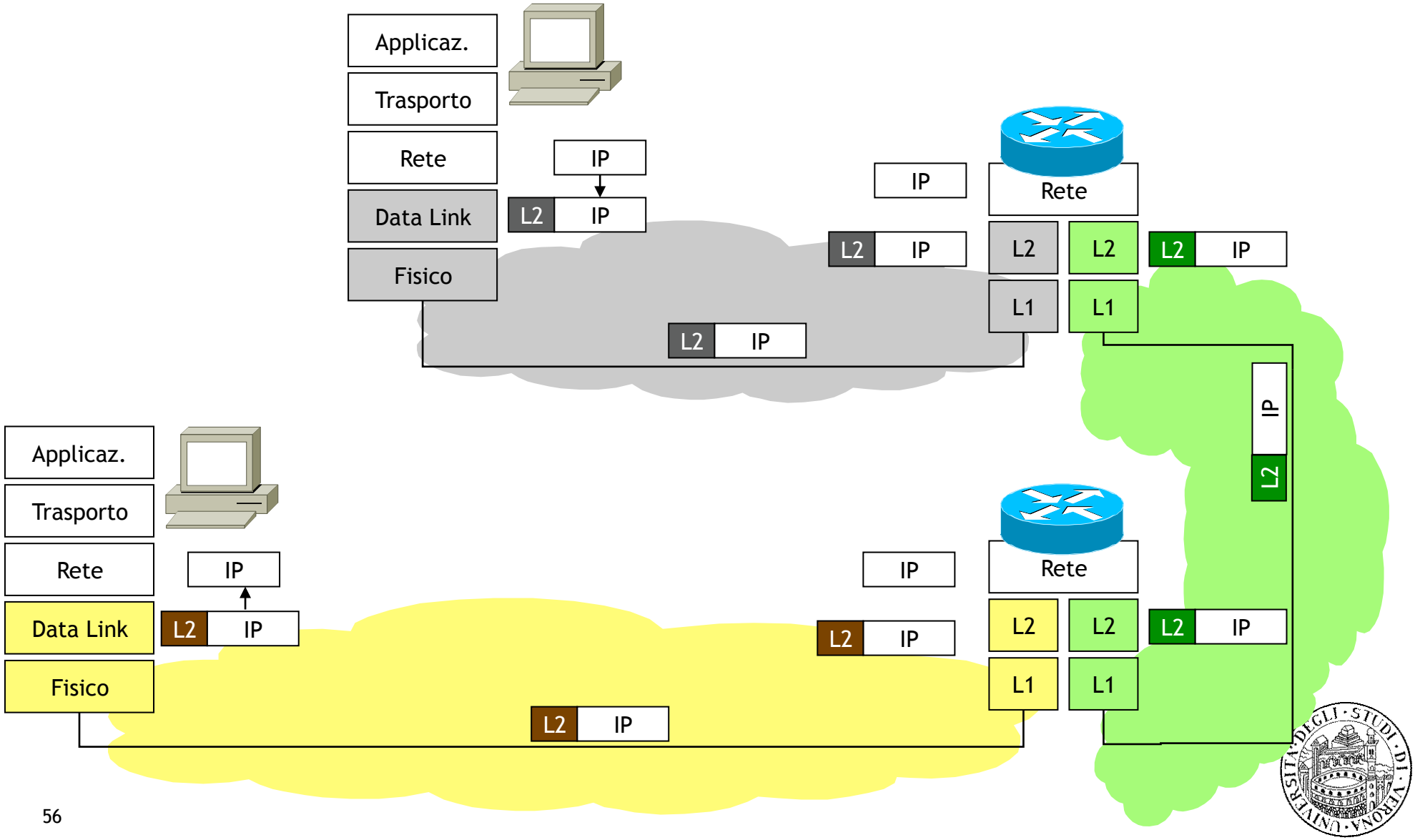
# Schema di uno switch




| indirizzo destinazione | porta |
|---|---|
| 34A46T | 1 |
| 34B52R | 4 |
| 34G90N | 3 |
| 44A48S | 6 |

# Protocolli di livello 2 (incapsulamento di IP)

# Visione d'insieme



# Introduzione

- Il livello 2 svolge una serie di funzionalità che consentono il trasferimento hop-by-hop
  - funzionalità del livello 2
    - framing, rilevazione errori, controllo flusso
  - in caso di mezzo condiviso, è necessaria la presenza di un sotto livello di accesso al mezzo
- Le funzionalità sono implementate dai protocolli di livello 2
  - insieme di regole e formato dei messaggi che regolano la comunicazione tra entità peer
- Ogni hop può avere un protocollo di livello 2 che può essere differente dall'hop successivo

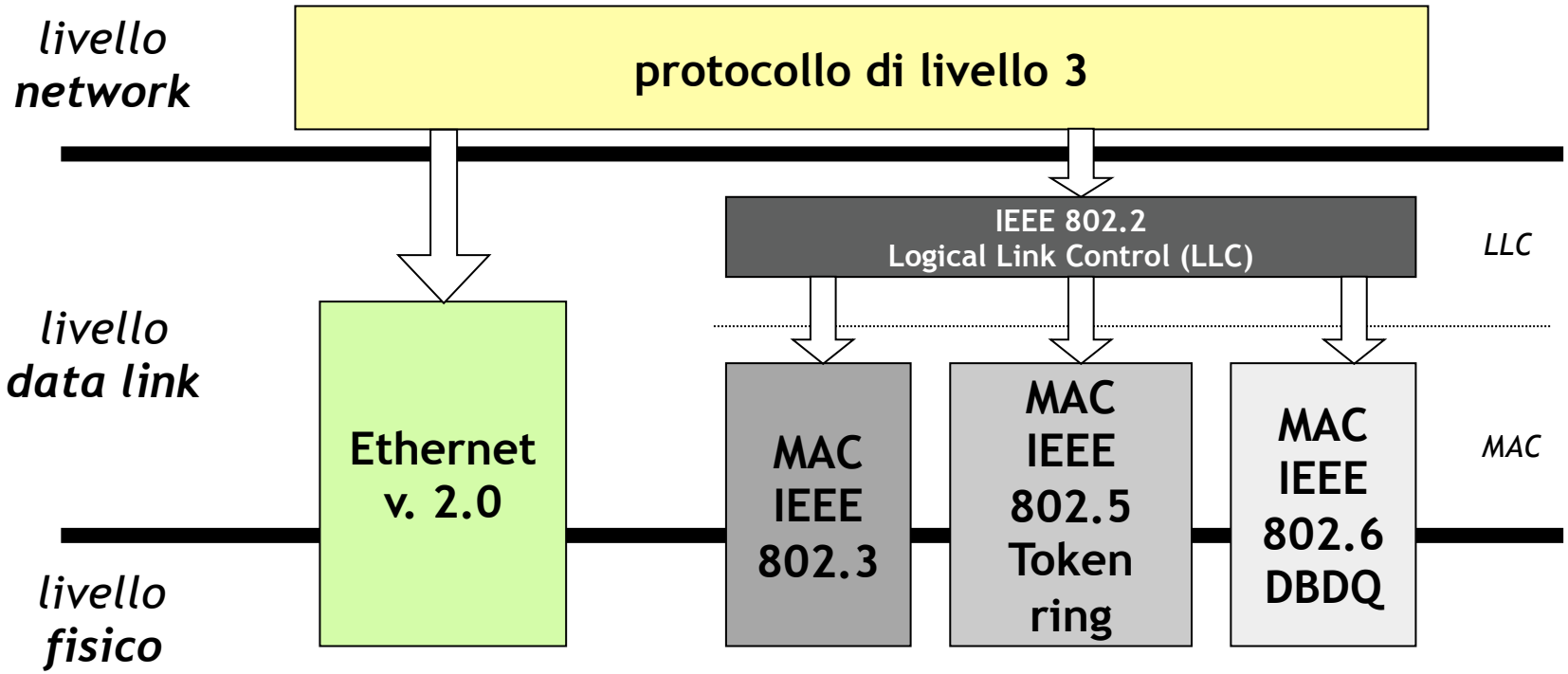
# Introduzione

- L'elemento unificante è il protocollo di Rete
  - il livello 3 ha visibilità end-to-end
- Esistono dunque diverse modalità di incapsulamento dei pacchetti IP
  - ovvero esistono diversi protocolli di livello 2
- Alcuni modalità di incapsulamento dei pacchetti IP
  - soluzioni utilizzate prevalentemente per l'accesso
    - ethernet e IEEE 802.3
    - PPP
      - PPP con modem
      - PPP con ADSL
  - soluzioni utilizzate prevalentemente per il backbone
    - Frame Relay
    - ATM
    - soluzioni su SDH

# Ethernet e Standard IEEE 802.3
# Caratteristiche e prestazioni

- Ambito di utilizzo
  - reti locali (LAN)
    - uffici, campus universitari, ...
- Tecnologia economica
  - facilità di installazione e manutenzione
- Si interfaccia direttamente e gestisce il livello fisico
- Sopporta un carico medio del 30% (3 Mb/s) con picchi del 60% (6 Mb/s)
- Sotto carico medio
  - Il 2-3% dei pacchetti ha una sola collisione
  - Qualche pacchetto su 10,000 ha più di una collisione
- Principale differenza tra Ethernet e 802.3
  - 802.3 definisce un'intera famiglia di sistemi CSMA/CD con velocità 1-10Mbps
  - Ethernet è solamente a 10Mbps

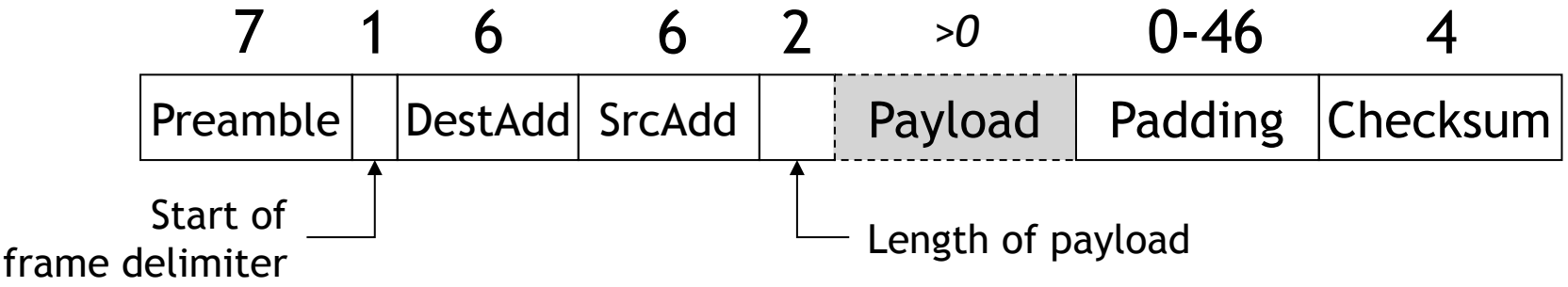
# Ethernet e Standard IEEE 802.3
# Posizionamento nello stack



# Ethernet e Standard IEEE 802.3
# Algoritmi implementati

- Gli standard Ethernet e 802.3 implementano un livello MAC di tipo CSMA/CD *1-persistent*
- In caso di collisione, l'istante in cui ritrasmettere viene calcolato utilizzando un algoritmo di **binary exponential backoff**
  - dopo *i* collisioni, l'host attende prima di ri-iniziare la procedura di trasmissione un tempo casuale nell'intervallo [0, 1, ..., $2^i$-1]
  - vincoli
    - dopo 10 collisioni il tempo di attesa è limitato all'intervallo [0, 1, ..., 1023]
    - dopo 16 collisioni viene riportata una *failure* al sistema operativo

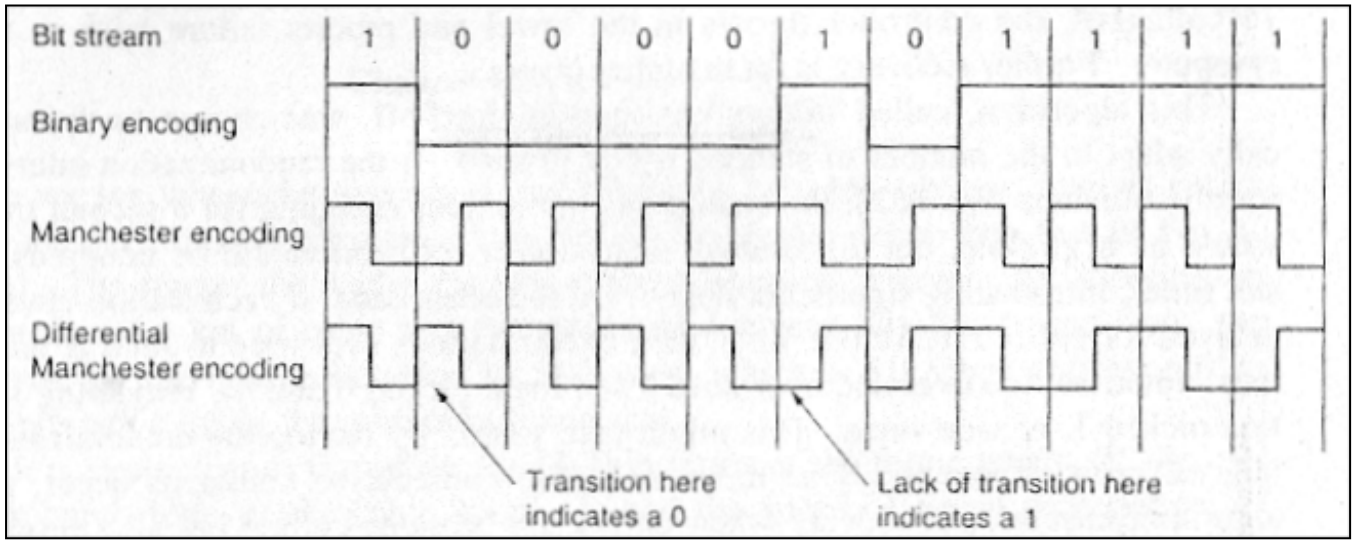
# Ethernet e Standard IEEE 802.3
# Formato della trama




- Preambolo (7 byte)
  - sequenza di byte “10101010” utilizzata per sincronizzare il ricevitore
- Start of frame (1 byte)
  - flag di inizio della trama “10101011”
- Addresses (6 byte)
  - indirizzi destinazione e sorgente della trama
- Length (2 byte)
  - lunghezza in byte della trama (0-1500)
  - se > 1500 indica Protocol Type
- Payload
  - informazione trasmessa
- Checksum
  - codice per rilevazione di errore

# Ethernet e Standard IEEE 802.3
# Interfacciamento col mezzo fisico

- Viene utilizzata la codifica Manchester
  - Tradizionale
    - ogni periodo di bit è suddiviso in due sottoperiodi
      - "0" ⇨ basso,alto
      - "1" ⇨ alto basso
  - Differenziale
    - ogni periodo di bit è diviso in 2 sottoperiodi
      - "1" assenza di transizione all'inizio del periodo di bit
      - "0" transizione all'inizio del periodo di bit



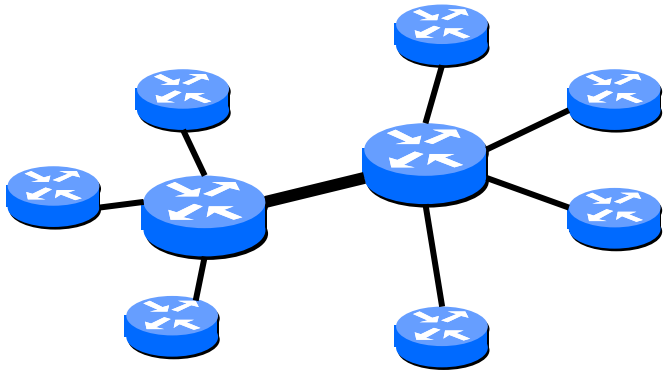
# Ethernet e Standard IEEE 802.3
# Evoluzione di Ethernet

- Fast Ethernet
  - Ethernet a velocità di 100Mbps
- Gigabit Ethernet
  - formato e dimensione dei pacchetti uguale a Ethernet/802.3
  - velocità di 1 Gbps (in corso di standardizzazione anche 10 Gbps)
  - Offre i vantaggio tipici di Ethernet:
    - Semplicità di accesso al mezzo CSMA/CD
    - Alta scalabilità tra le diverse velocità di trasmissione
  - Permette di velocizzare le moltissime LAN Ethernet e FastEthernet già presenti con costi contenuti tramite sostituzione apparati di rete (Hub, Switch, interfacce)

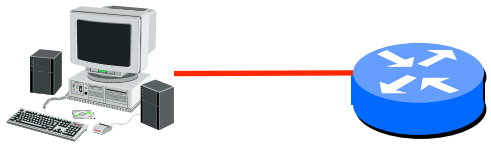
# PPP
# Caratterisitiche

- E’ un protocollo di livello 2 utilizzato sia nell’accesso e che nel backbone
- Caratteristiche principali:
  - character oriented
  - character stuffing per il framing
  - identificazione degli errori
  - supporta vari protocolli di livello superiore (rete)
  - negoziazione dinamica degli indirizzi IP
  - autenticazione del “chiamante”

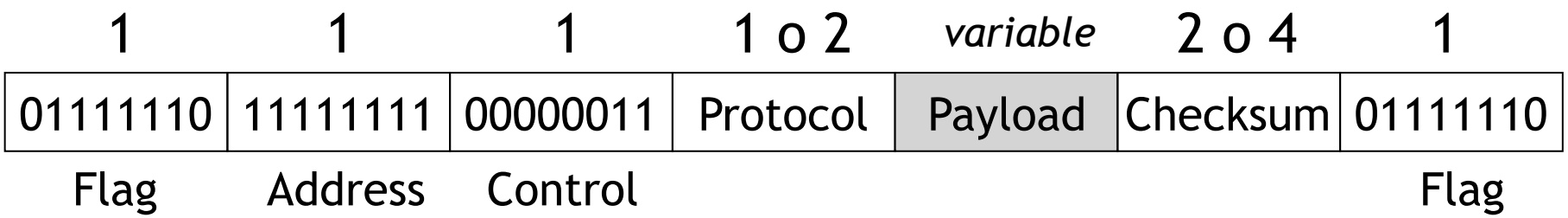
*collegamento punto-punto tra router*



*collegamento punto-punto dial-up tra un PC e un router*



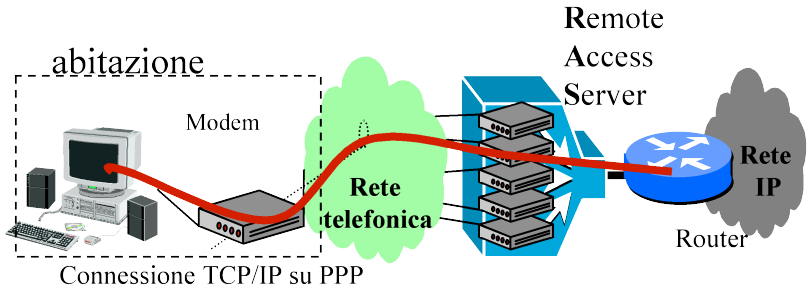
# PPP
# Formato della trama

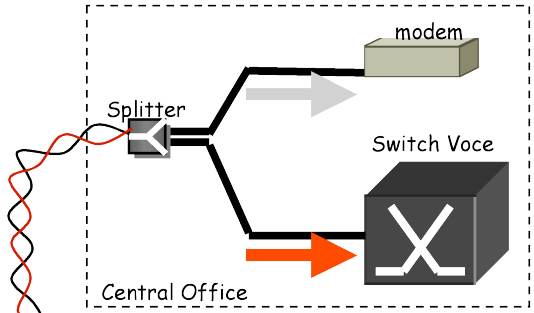


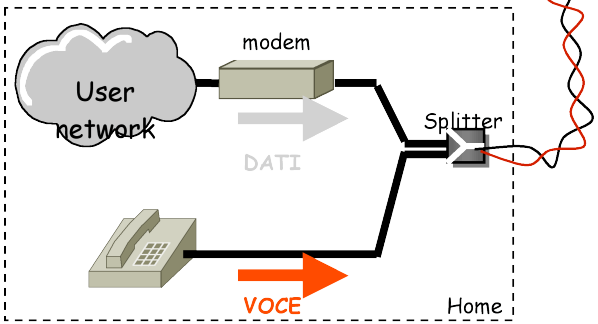

- Flag (1 byte)
  - identifica inizio e fine della trama ("01111110")
- Address (1 byte)
  - utilizzato in configurazione "tutti gli host"
- Control (1 byte)
  - valore predefinito "00000011" ⇨ *unnumbered*
  - di default non fornisce un servizio affidabile: richiesta di ritrasmissione e rimozione replicazioni sono lasciate ai livelli superiori
    - è disponibile un'estensione per reti con alto BER (wireless) ad un servizio connection oriented (RFC1663)
- Protocol (1 o 2 byte)
  - identifica il tipo di livello di frame (LCP, NCP, IP, IPX, ...)
- Payload (>0 byte)
  - informazione trasmessa
- Checksum (2 o 4 byte)
  - identificazione dell'errore

# PPP
# accesso con modem e ADSL

- Modem (es.: V.90)
  - utilizza la banda telefonica per inviare i segnali
  - ha limite estremo superiore 56 Kbps
- xDSL (Digital Subscriber Line)
  - famiglie di tecnologie che permette di utilizzare la banda disponibile del doppino telefonico
  - si possono distinguere in sistemi simmetrici e asimmetrici
    - es: ADSL
      - Sistema asimmetrico su singola coppia
      - Rate adaptive:
        - » 640 – 8200 kb/s downstream
        - » Fino a 512 kb/s upstream
      - Strato di trasporto di livello 2: PPP su ATM
      - Distanze: a seconda del bit-rate



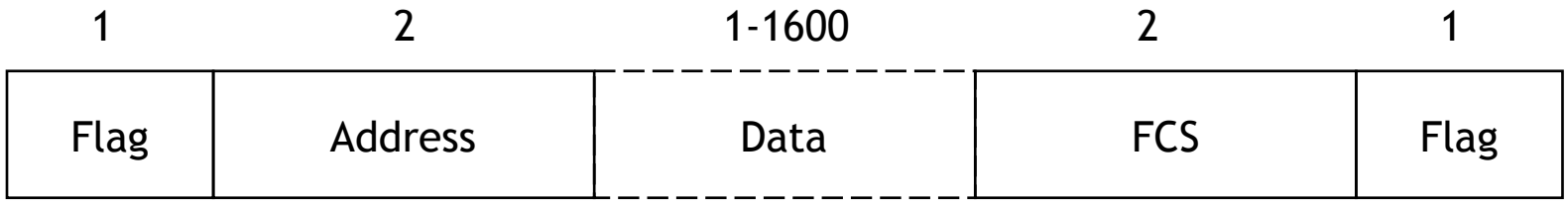



# Frame Relay
# Caratteristiche

- Progettato inizialmente per essere utilizzato su ISDN, è stato poi usato in diversi altri contesti, soprattutto WAN
- Caratteristiche principali:
  - offre servizi di comunicazione ***connection oriented***
    - utilizzo di circuiti virtuali (VC) bidirezionali
      - Switched Virtual Circuit (SVC)
        - » Stati operativi: Call Setup, Data Transfer, Idle, Call Termination
      - Permanent Virtual Circuit (PVC)
        - » Stati operativi: Data Transfer, Idle
  - implementa meccanismi di ***notifica della congestione***
    - rispetto al controllo di flusso (azione preventiva), la notifica di congestione avviene come azione di reazione
  - possiede un meccanismo per la rilevazione di errori
    - non viene implementato la funzionalità di correzione degli errori

# Frame Relay
# Formato della trama

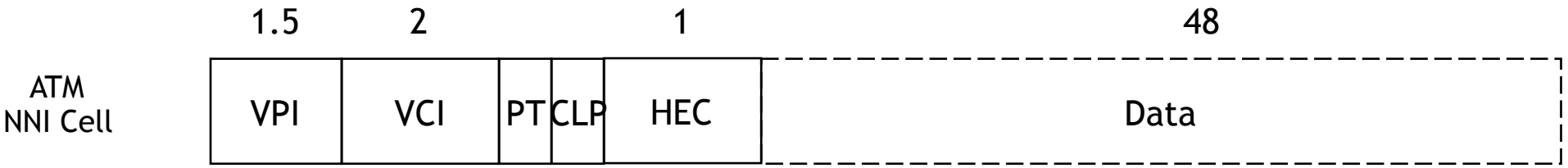



- Flag (1 byte)
  - sequenza di byte “01111110” utilizzata per delimitare la trama
- Address (2 byte)
  - contiene i seguenti campi:
    - DLCI (10 bit): Data Link Connection Identifier
    - EA (1 bit): extended address
    - C/R (1 bit): Command/Response
    - Congestion control (3 bit)
- Data (1-1600 byte)
  - contiene i dati provenienti dal livello 3
- FCS (2 byte)
  - Frame Check Sequence, per la verifica dell’integrità della trama
- Flag (1 byte)
  - sequenza di byte “01111110” utilizzata per delimitare la trama

# Asynchronous Transfer Mode (ATM) Caratteristiche

- Sistema progettato come tecnologia per il trasferimento di dati, voce e video a bit-rate elevato
  - oggi: impiegato principalmente nei backbone
- Caratteristiche principali
  - trame, dette **celle**, di lunghezza fissa (53 Kbyte)
    - i pacchetti di livello 3 vengono suddivisivi in N celle e ricomposti alla destinazione
  - multiplazione statistica delle celle
  - offre una gamma di servizi prevalentemente connection oriented con diverse qualità del servizio disponibili
    - utilizzo di Virtual Circuit e Virtual Path
      - Switched Virtual Circuit (SVC)
      - Permanent Virtual Circuit (PVC)
  - offre una serie di funzionalità ai bordi della rete (traffic shaping, gestione delle code)
    - controllo di flusso
    - controllo della congestione
  - possiede un meccanismo per la rilevazione di errori

# ATM
# Formato delle celle

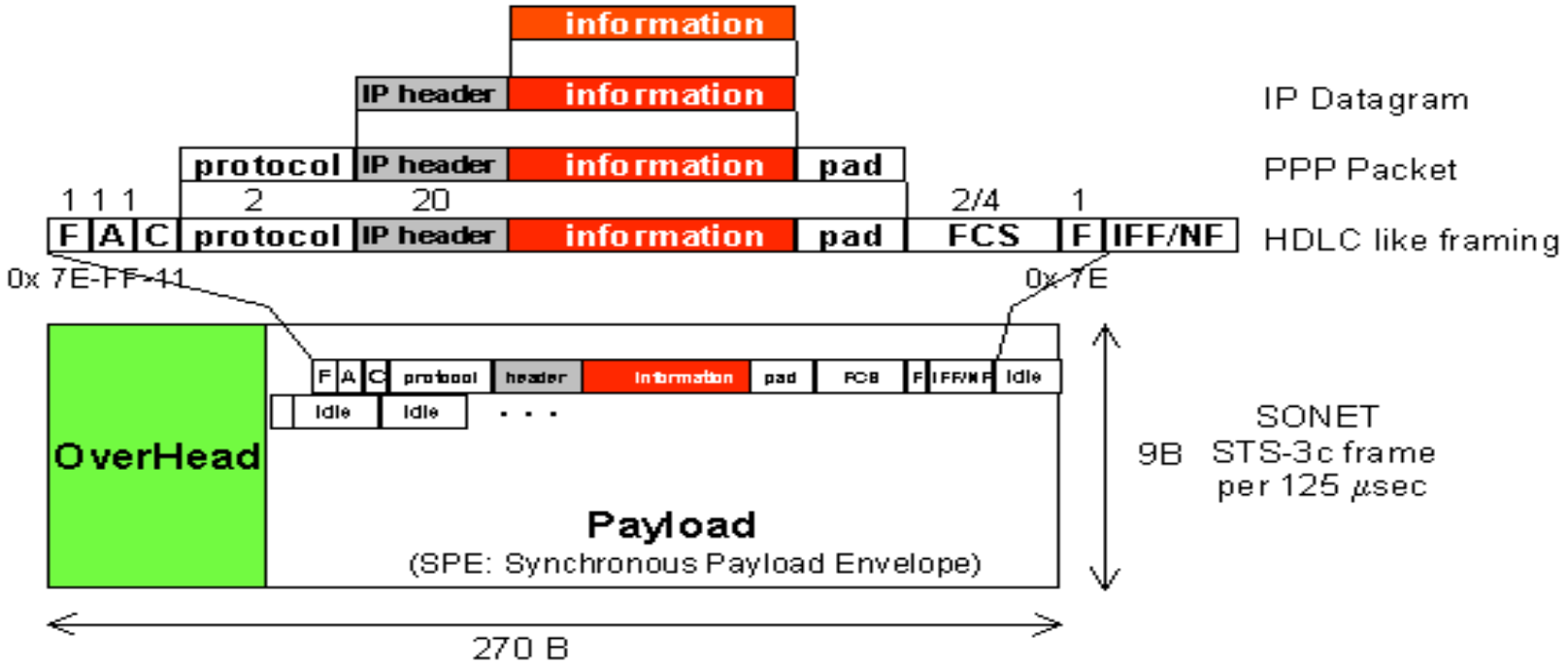



- VPI (1.5 byte)
  - Virtual Path Identifier
- VCI (2 byte)
  - Virtual Circuit Identifier
- PT (3 bit)
  - Payload Type
    - primo bit: indica se la cella contiene dati utente o dati di controllo
    - secondo bit: utilizzato per indicare se c'è congestione
    - terzo bit: indica se la cella contiene la fine di un pacchetto
- CLP (1 bit)
  - Cell Loss Priority
    - indica se la cella, in caso di congestione, può essere scartata
- HEC
  - Header Error Control
    - checksum del solo header
    - è in grado di correggere un bit di errore

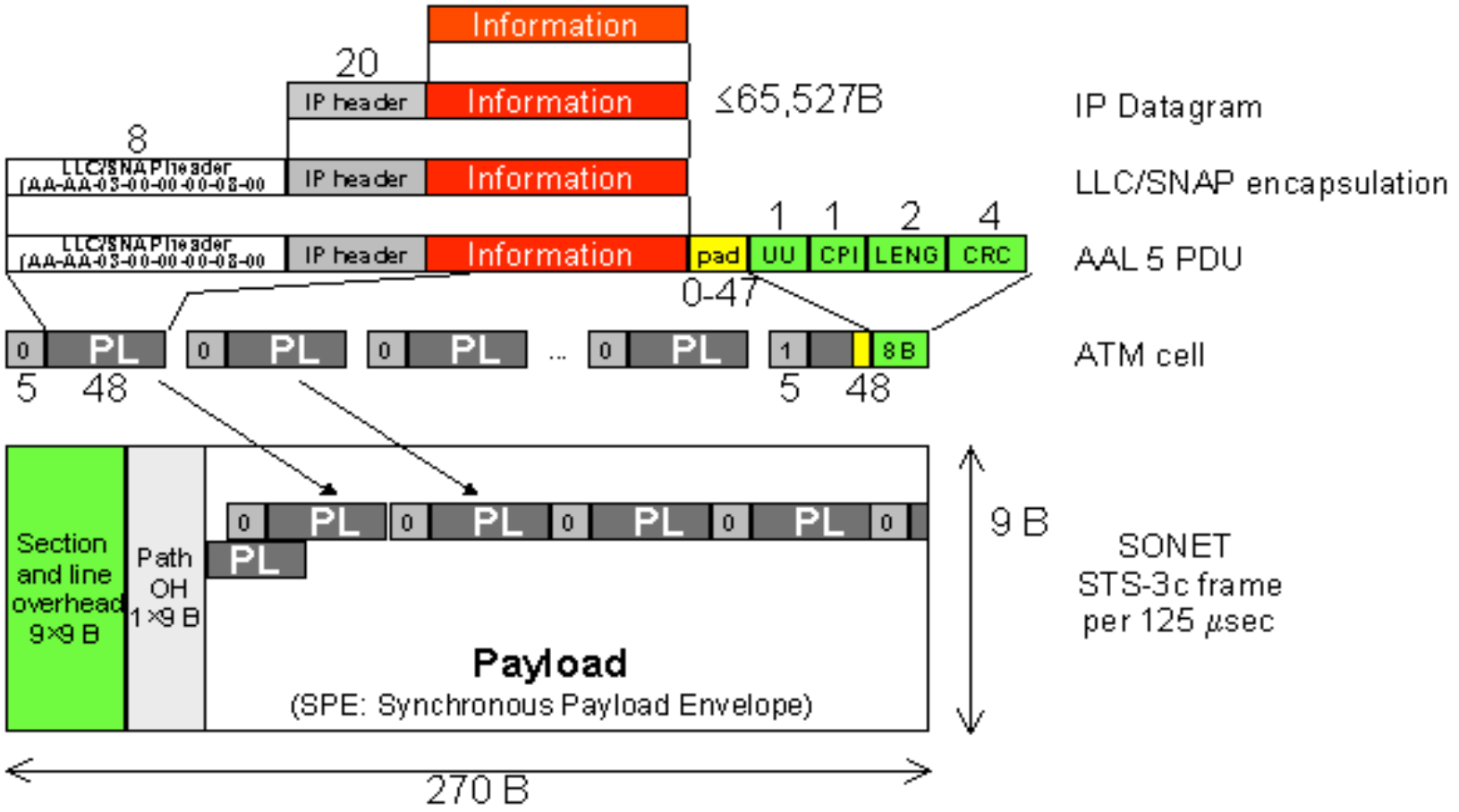
# SDH

- Tecnologia di trasporto di livello ISO-OSI 1 (fisico) ad alta velocità basata su multiplazione TDM (ottimizzata per la voce)
- Nasce come evoluzione della gerarchia PDH
  - PDH: standard di riferimento per le reti numeriche
    - definito dalla Raccomandazione G.702 ITU-T
    - normalizza a livello mondiale due diversi standard generalmente noti come standard PCM europeo ed PCM americano.
    - la versione europea prevede:
      - un flusso di base a 64 kb/s, che è multiplato con una trama sincrona entro un flusso primario a 2048 kb/s, comunemente nominato flusso a 2 Mb/s;
      - flussi di ordine superiore, a 8448 kb/s, 34368 kb/s (34 Mb/s) e 139264 kb/s (140 Mb/s)
- Scopo della gerarchia SDH è stato quello di superare le limitazioni delle gerarchie plesiocrone
  - coesistenza con la gerarchia PDH
  - funzioni di gestione avanzate
  - funzioni di allarme e gestione in-band
  - funzioni e architetture di protezione del traffico
  - definizione di molteplici architetture di rete e di elementi funzionali

# Soluzioni per il trasporto di pacchetti IP su SDH: IP su SDH (PoS)



# Soluzioni per il trasporto di pacchetti IP su SDH: IP su ATM su SDH



# Verifica contenuti

# Domande generali

- Che differenza c'e' tra commutazione di pacchetto a datagramma e a circuito virtuale?
- Quali sono le principali funzioni del livello 2?
- Che cosa si intende per framing? Si dia un esempio di come viene realizzato
- Che cosa gestisce il sottolivello MAC?
- Perché le tecniche di allocazione statica non vengono utilizzate (nella trasmissione dei dati)
- Qual'è il periodo di vulnerabilità del protocollo Aloha? E del protocollo S-Aloha? E del CSMA?
- Che cosa si intende per CSMA 0.2 persistent?
- Che cosa è un hub? E un bridge?
- Cosa succede se una stazione invia una trama su un segmento di rete mentre su un altro segmento di rete, collegato al primo tramite uno switch, un'altra stazione sta trasmettendo? Avviene collisione?