



*Corso di Laurea Triennale in Informatica  
Università degli Studi della Basilicata*

# Reti di Calcolatori

Docente: Ugo Erra

*ugo.erra+reti@unibas.it*

13° Lezione – Livello di collegamento – I° parte

# Sommario



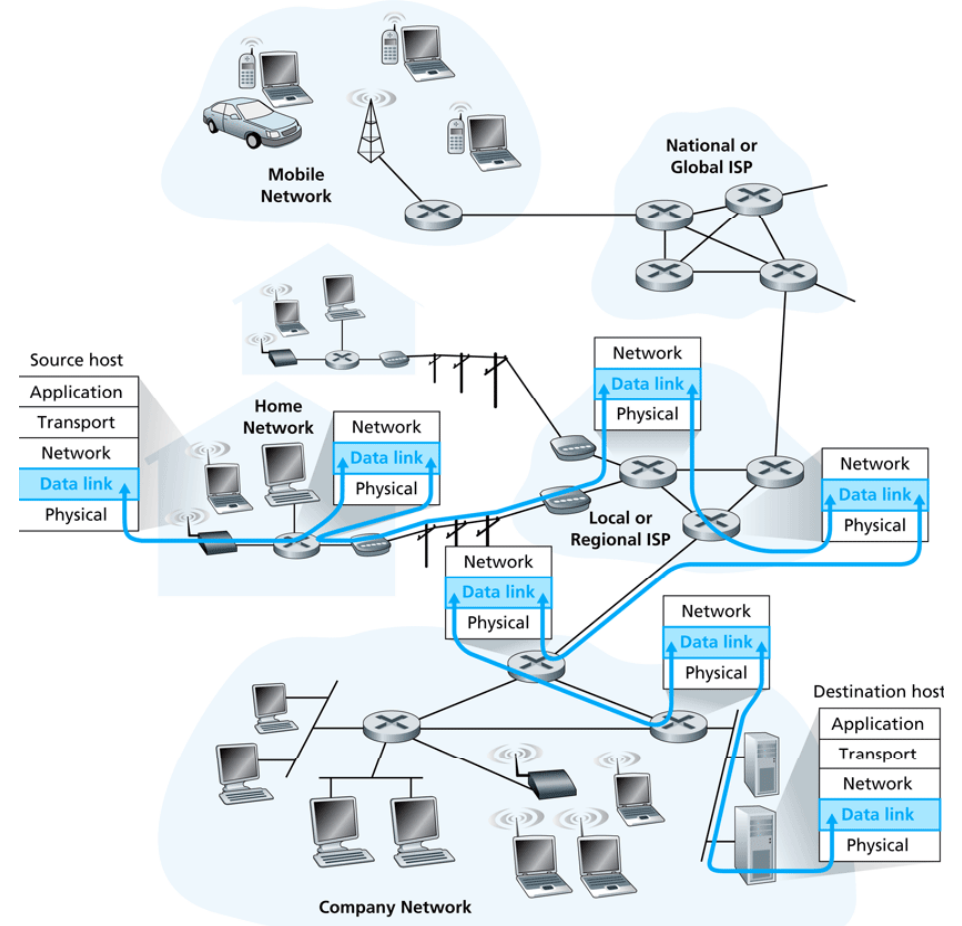
- **Livello di link: introduzione e servizi**
- Tecniche di rilevazione e correzione degli errori
- Protocolli di accesso multiplo

# Dove ci troviamo?



# Introduzione

- I **protocolli a livello di collegamento** si occupano del trasporto di datagrammi lungo un singolo canale di comunicazione
- Alcuni termini utili
  - ▣ Host e router sono i **nodi**
  - ▣ I canali di comunicazione che collegano nodi adiacenti lungo un cammino sono i **collegamenti (link)**
    - Collegamenti cablati
    - Collegamenti wireless
    - LAN
- Le unità di dati scambiate dai protocolli a livello di link sono chiamate **frame**



# Livello di link

- Un datagramma può essere gestito da diversi protocolli, su collegamenti differenti:
  - ▣ Es., un datagramma può essere gestito da Ethernet sul primo collegamento, da PPP sull'ultimo e da un protocollo WAN nel collegamento intermedio
- Anche i servizi erogati dai protocolli del livello di link possono essere differenti:
  - ▣ Ad esempio, non tutti i protocolli forniscono un servizio di consegna affidabile

## *Analogia con un tour operator:*

- Un viaggio da Potenza a New York:
  - ▣ Taxi: da Potenza a Salerno
  - ▣ Treno: da Salerno a Napoli
  - ▣ Aereo: da Napoli a New York
- Turista = **datagramma**
- Ciascuna tratta del trasporto = **collegamento**
- Tipologia del trasporto = **protocollo di link**
- Agente di viaggio = **protocollo di rete**

# Servizi offerti dal livello di link

## □ Framing

- I protocolli incapsulano i datagrammi del livello di rete all'interno di un frame a livello di link
- Il protocollo MAC controlla l'accesso al mezzo
- Per identificare origine e destinatario vengono utilizzati indirizzi "MAC"
- Diversi rispetto agli indirizzi IP!

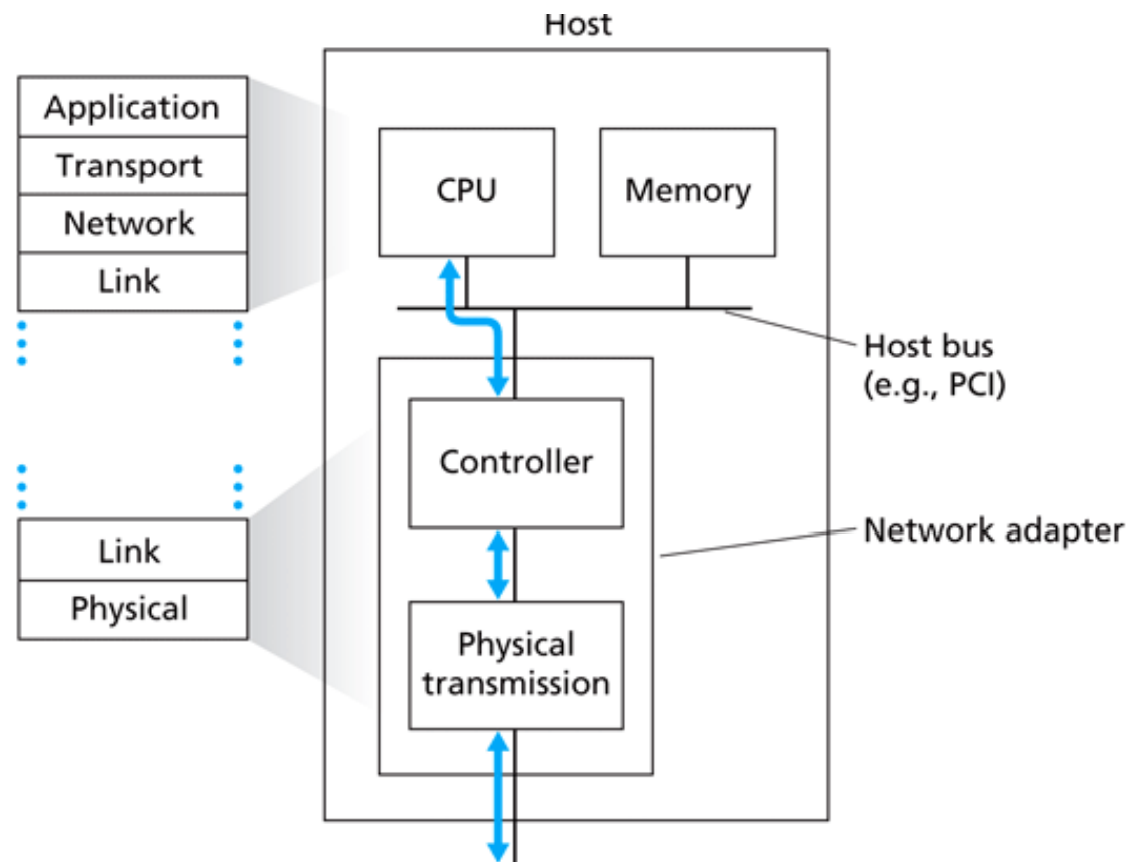
## □ Consegna affidabile

- Come avviene, lo abbiamo già studiato nel Capitolo 3
- È considerata non necessaria nei collegamenti che presentano un basso numero di errori sui bit (fibra ottica, cavo coassiale e doppino intrecciato)
- È spesso utilizzata nei collegamenti soggetti a elevati tassi di errori (es.: collegamenti wireless)

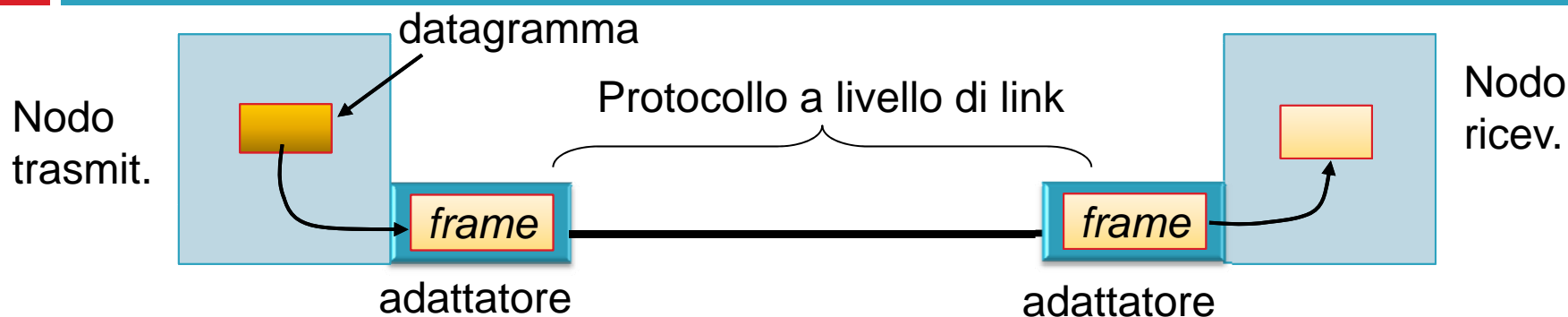
# Servizi offerti dal livello di link

- **Controllo di flusso**
  - Evita che il nodo trasmittente saturi quello ricevente
- **Rilevazione degli errori**
  - Gli errori sono causati dall'attenuazione del segnale e da rumore elettromagnetico
  - Il nodo ricevente individua la presenza di errori
    - Attraverso l'inserimento, da parte del nodo trasmittente, di un bit di controllo di errore all'interno del frame
- **Correzione degli errori**
  - Il nodo ricevente determina anche il punto in cui si è verificato l'errore, e lo corregge
- **Half-duplex e full-duplex**
  - Nella trasmissione full-duplex gli estremi di un collegamento possono trasmettere contemporaneamente: non in quella half-duplex

# Chi si occupa del livello di link?



# Adattatori



- Il protocollo a livello di link è realizzato da un adattatore (NIC, scheda di interfaccia di rete)
  - ▣ Adattatori Ethernet, adattatori PCMCIA e adattatori 802.11
- Lato trasmittente:
  - ▣ Incapsula un datagramma in un frame
  - ▣ Imposta il bit rilevazione degli errori, trasferimento dati affidabile, controllo di flusso, etc.
- Lato ricevente:
  - ▣ Individua gli errori, trasferimento dati affidabile, controllo di flusso, etc.
  - ▣ Estrae i datagrammi e li passa al nodo ricevente
- L'adattatore è un'unità semi-autonoma
- Si occupa del livello di link e fisico

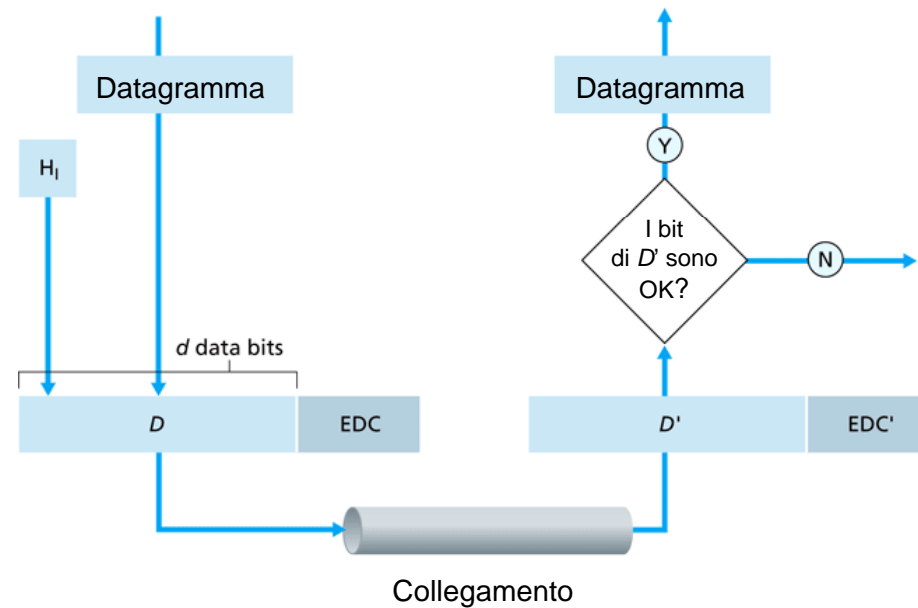
# Sommario



- Livello di link: introduzione e servizi
- **Tecniche di rilevazione e correzione degli errori**
- Protocolli di accesso multiplo

# Tecniche di rilevazione degli errori

- Supponiamo di avere  $D$  bit di dati da trasmettere
- Per poter rilevare eventuali errori vengono aggiunti dei bit **EDC** (*Error Detection and Correction*)
- La rilevazione degli errori non è attendibile al 100%!
  - E' possibile che ci siano errori non rilevati
  - Per ridurre la probabilità di questo evento, le tecniche più sofisticate prevedono un'elevata ridondanza



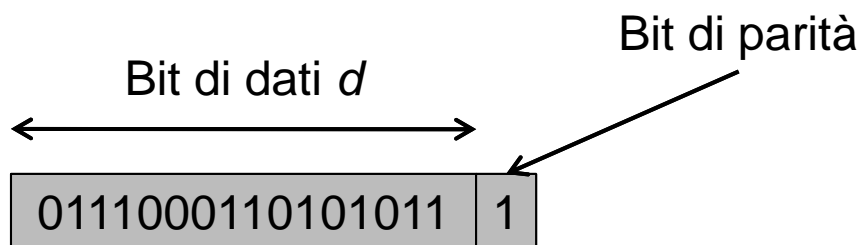
# Tecniche per la rilevazione degli errori



- Tecniche per rilevare errori nei dati trasmessi
  - ▣ Controllo di parità
  - ▣ Metodo della somma di controllo
  - ▣ Controllo a ridondanza ciclica

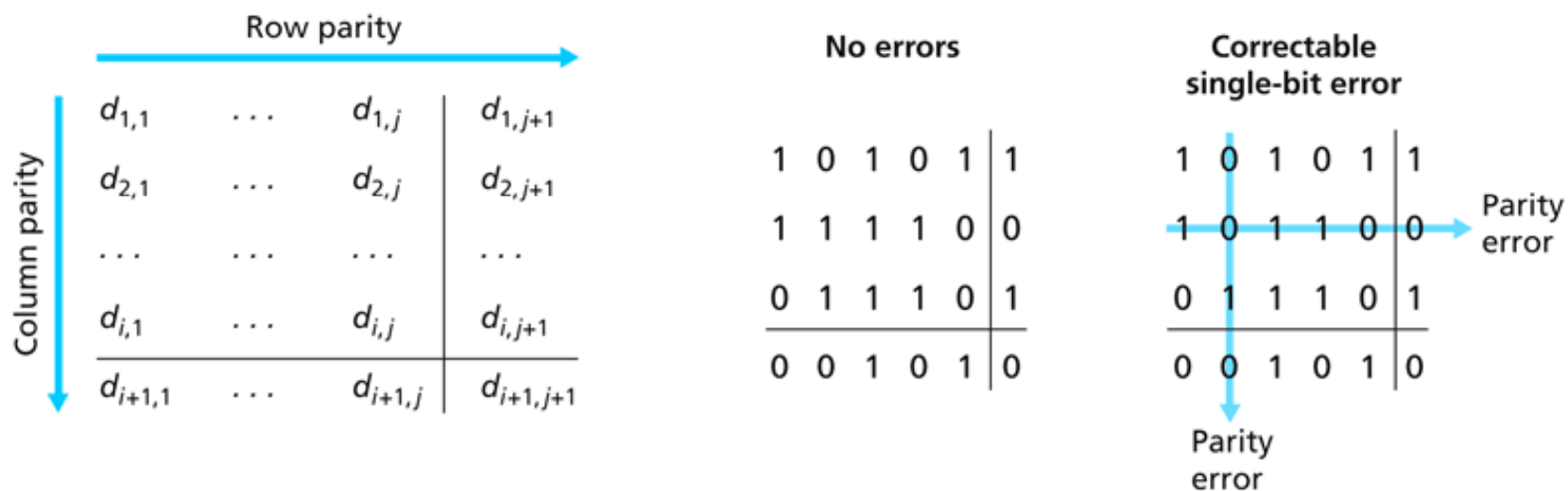
# Controllo di parità - 1

- Supponiamo che le informazioni  $D$  da inviare siano composte da  $d$  bit
- L'aggiunta di un **bit di parità** permette di rilevare un eventuale errore
- Nella parità pari il mittente include un bit 1 nella posizione  $d+1$  in modo da rendere pari il numero di bit ad 1 trasmessi
- Nella parità dispari il mittente include un bit 1 nella posizione  $d+1$  in modo da rendere dispari il numero di bit ad 1 trasmessi
- Cosa avviene se si verifica un numero di errori pari nei bit?



# Controllo di parità - 2

- La **parità bidimensionale** permette di estendere questo schema per fornire un semplice approccio alla correzione dell'errore



# Somma di controllo

- Il metodo della **somma di controllo** o **checksum** rileva gli errori ma viene usata solo a livello di trasporto
  - ▣ Il livello di trasporto è implementato via software nel sistema operativo quindi il checksum si adatta bene poichè è semplice e veloce
- Mittente
  - ▣ I dati sono trattati come interi da 16 bit e sommati
  - ▣ Checksum: è il complemento a 1 di questa somma
  - ▣ Il mittente inserisce il valore della checksum nell'intestazione dei segmenti
- Destinatario:
  - ▣ Il ricevente controlla la checksum
  - ▣ Calcola il complemento 1 della somma dei dati ricevuti e verifica che i bit del risultato siano 1:
    - NO, non lo sono: segnala un errore
    - SÌ lo sono: non sono stati rilevati errori

# Controllo a ridondanza ciclica - 1

- Esamina i dati,  $D$ , come numeri binari
- Origine e destinazione si sono accordati su una stringa chiamata generatore  $G$  di  $r+1$  bit
  
- Obiettivi: scegliere  $r$  bit addizionali  $R$ , in modo che:
  - ▣  $\langle D, R \rangle$  siano esattamente divisibili per  $G$  (modulo 2)
  - ▣ Il destinatario conosce  $G$ , e divide  $\langle D, R \rangle$  per  $G$ . Se il resto è diverso da 0 si è verificato un errore!
  - ▣ CRC può rilevare errori a raffica inferiori a  $r+1$  bit
- Nella pratica è molto usato (ATM, HDCL)

# Come calcoliamo $R$ ?

- Vogliamo:

$$D \cdot 2^r \text{ XOR } R = nG$$

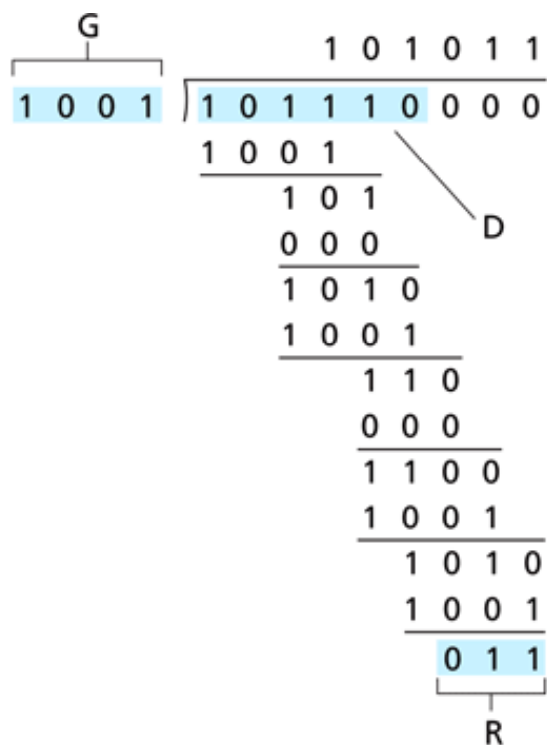
- Ovvero:

$$D \cdot 2^r = nG \text{ XOR } R$$

- Quindi dividiamo  $D \cdot 2^r$  per  $G$ , otteniamo il valore  $R$

$$R = \frac{D \cdot 2^r}{G}$$

# Esempio CRC



- $D=101110$
- $d=6$
- $G=1001$
- $r=3$
- I nove bit da trasmettere sono 101110011

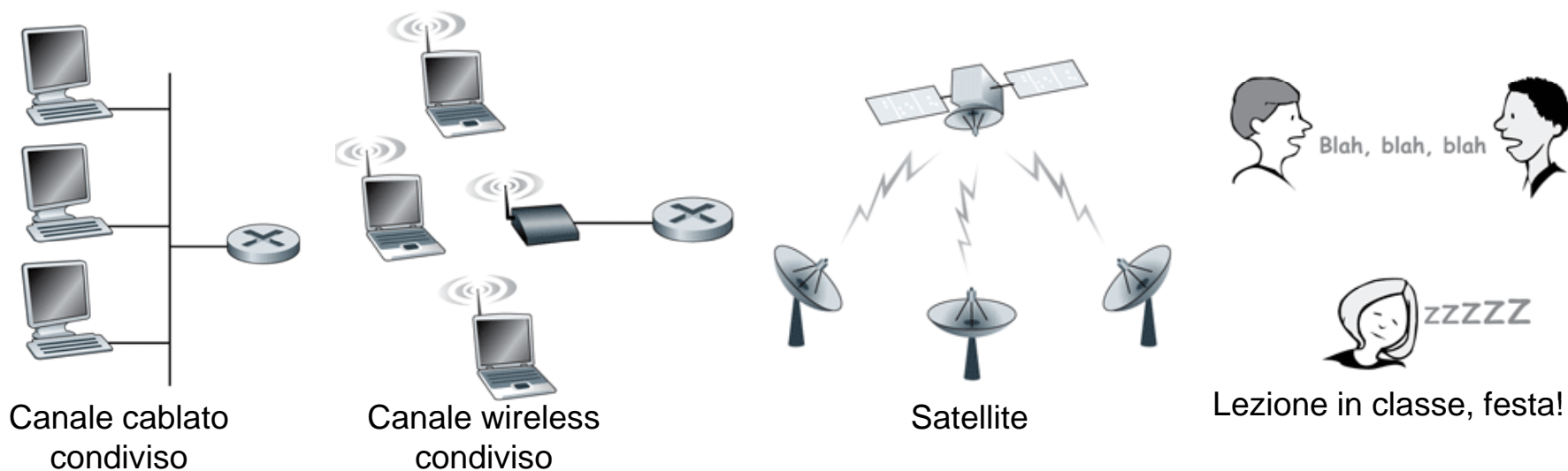
# Sommario



- Livello di link: introduzione e servizi
- Tecniche di rilevazione e correzione degli errori
- **Protocolli di accesso multiplo**

# Protocolli di accesso multiplo

- Esistono due tipi di collegamenti di rete:
  - ▣ Collegamento punto-punto (PPP)
    - Impiegato per connessioni telefoniche
    - Collegamenti punto-punto tra Ethernet e host
  - ▣ Collegamento broadcast (cavo o canale condiviso)
    - Ethernet tradizionale
    - HFC in upstream
    - Wireless LAN 802.11



# Protocolli ad accesso multiplo

- Connessione a un canale broadcast condiviso
- Centinaia o anche migliaia di nodi possono comunicare direttamente su un canale broadcast
  - ▣ Si genera una **collisione** quando i nodi ricevono due o più frame contemporaneamente
- I **protocolli di accesso multiplo** sono adoperati nei canali broadcast
  - ▣ Protocolli che fissano le modalità con cui i nodi regolano le loro trasmissioni sul canale condiviso
  - ▣ La comunicazione relativa al canale condiviso deve utilizzare lo stesso canale!
    - Non c'è un canale “out-of-band” per la coordinazione

# Protocolli di accesso multiplo ideali

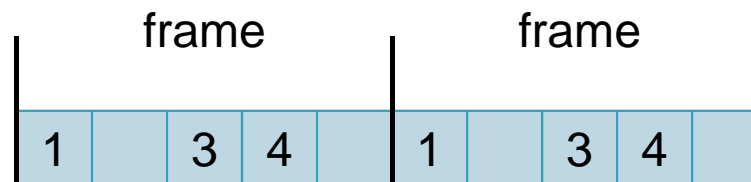
- Idealmente un canale broadcast con velocità di  $R$  bit/sec dovrebbe avere le seguenti caratteristiche:
  1. Quando un nodo deve inviare dati, questo dispone di un tasso trasmissivo pari a  $R$  bps
  2. Quando  $M$  nodi devono inviare dati, questi dispongono di un tasso trasmissivo pari a  $R/M$  bps
  3. Il protocollo è decentralizzato:
    - Non ci sono nodi master
    - Non c'è sincronizzazione dei clock
  4. Il protocollo deve essere semplice

# Protocolli di accesso multiplo

- Si classificano in una di queste tre categorie:
  - ▣ **Protocolli a suddivisione del canale** (*channel partitioning*)
    - Suddivide un canale in “parti più piccole” (slot di tempo, frequenza, codice)
  - ▣ **Protocolli ad accesso casuale** (*random access*)
    - I canali non vengono divisi e si può verificare una collisione
    - I nodi coinvolti ritrasmettono ripetutamente i pacchetti
  - ▣ **Protocolli a rotazione** (*taking-turn*)
    - Ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi

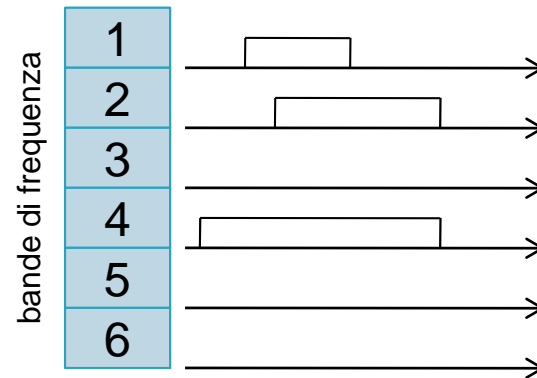
# Protocolli a suddivisione del canale: TDMA

- TDMA: accesso multiplo a divisione di tempo
  - ▣ Suddivide il canale condiviso in *intervalli di tempo*
  - ▣ Gli slot non usati rimangono inattivi
    - Esempio: gli slot 1, 3 e 4 hanno un pacchetto, 2, 5 e 6 sono inattivi



# Protocolli a suddivisione del canale: FDMA

- FDMA: accesso multiplo a divisione di frequenza
  - ▣ Suddivide il canale in bande di frequenza
  - ▣ A ciascuna stazione è assegnata una banda di frequenza prefissata
    - Esempio: gli slot 1, 3 e 4 hanno un pacchetto, 2, 5 e 6 sono inattivi



# Protocolli ad accesso casuale

- Quando un nodo deve inviare un pacchetto:
  - ▣ Trasmette sempre alla massima velocità consentita dal canale, cioè  $R$  bps
  - ▣ Non vi è coordinazione a priori tra i nodi
- Se due o più nodi trasmettono contemporaneamente si verifica una **collisione**
- Il protocollo ad accesso casuale definisce:
  - ▣ Come rilevare un'eventuale collisione
  - ▣ Quando ritrasmettere se si verifica una collisione
  - ▣ Esempi di protocolli ad accesso casuale:
    - Slotted ALOHA
    - ALOHA
    - CSMA, CSMA/CD, CSMA/CA

# Slotted ALOHA - 1



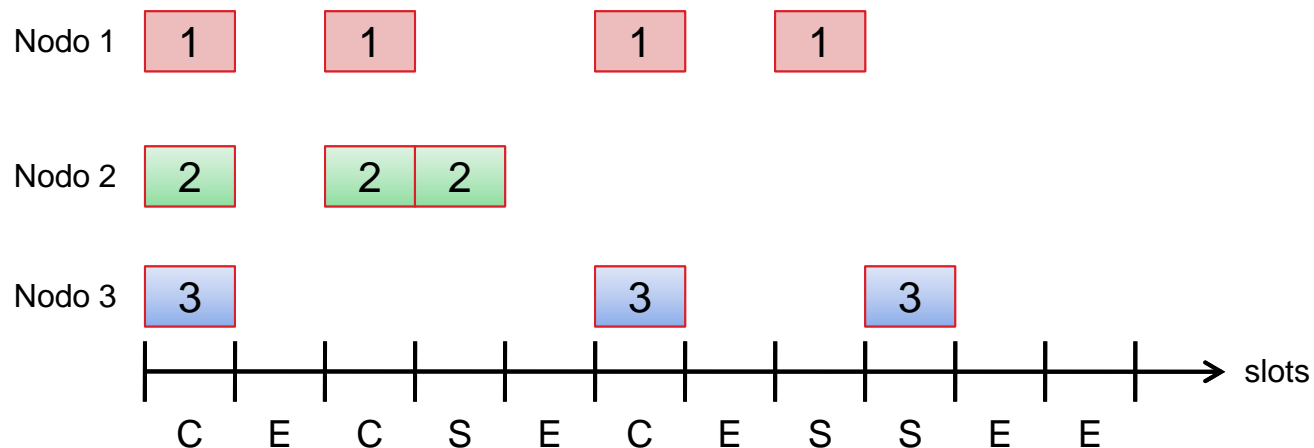
- Assumiamo che:
  - ▣ Tutti i pacchetti hanno la stessa dimensione
  - ▣ Il tempo è suddiviso in slot; ogni slot equivale al tempo di trasmissione di un pacchetto
  - ▣ I nodi iniziano la trasmissione dei pacchetti solo all'inizio degli slot
  - ▣ I nodi sono sincronizzati
  - ▣ Se in uno slot due o più pacchetti collidono, i nodi coinvolti rilevano l'evento prima del termine dello slot

# Slotted ALOHA - 2



- Operazioni possibili:
  - Quando a un nodo arriva un nuovo pacchetto da spedire, il nodo attende fino all'inizio dello slot successivo
  - Se non si verifica una collisione: il nodo può trasmettere un nuovo pacchetto nello slot successivo
  - Se si verifica una collisione: il nodo la rileva prima della fine dello slot e ritrasmette con probabilità  $p$  il suo pacchetto durante gli slot successivi

# Slotted ALOHA - 3



## *Pro*

- Consente a un singolo nodo di trasmettere continuamente pacchetti alla massima velocità del canale
- È fortemente decentralizzato, ciascun nodo rileva le collisioni e decide indipendentemente quando ritrasmettere
- È estremamente semplice

## *Contro*

- Una certa frazione degli slot presenterà collisioni e di conseguenza andrà "sprecata"
- Un'alta frazione degli slot rimane vuota, quindi inattiva

# Efficienza dello slotted ALOHA - 1

- L'**efficienza** è definita come la frazione di slot vincenti in presenza di un elevato numero di nodi attivi, che hanno sempre un elevato numero pacchetti da spedire
- Consideriamo  $N$  nodi con pacchetti da spedire
- Ogni nodo trasmette i pacchetti in uno slot con probabilità  $p$ 
  - ▣ Un nodo non trasmetterà con probabilità  $(1-p)$
- La probabilità di successo di un dato nodo è

$$p(1-p)^{N-1}$$

- La probabilità che un nodo arbitrario abbia successo

$$Np(1-p)^{N-1}$$

# Efficienza dello slotted ALOHA - 2

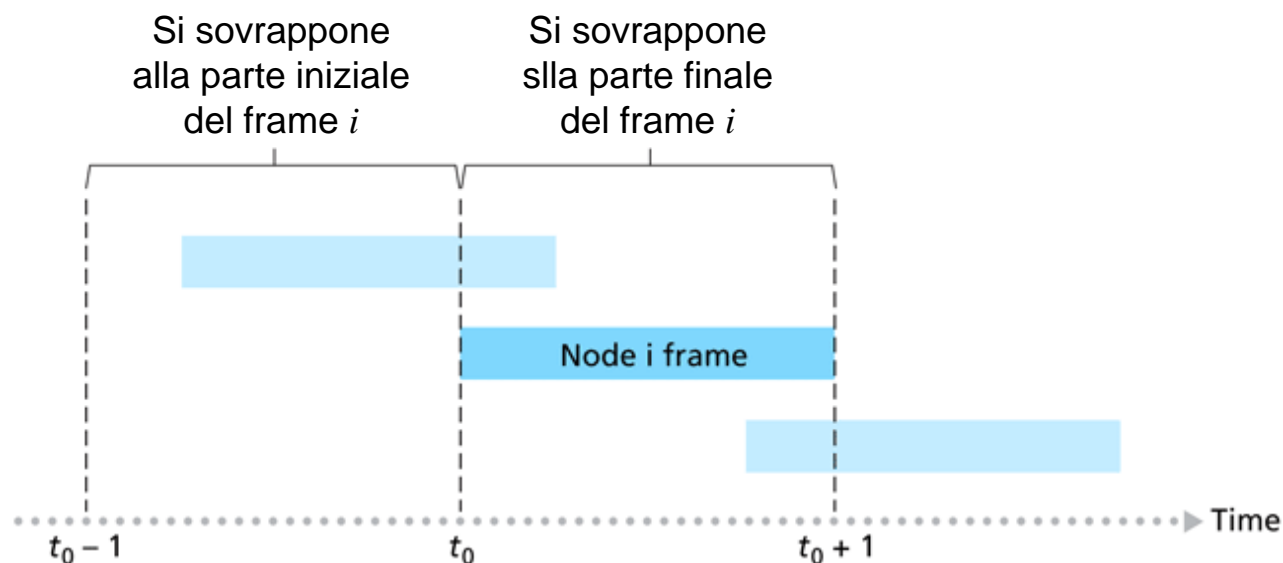
- Per ottenere la massima efficienza con  $N$  nodi attivi, bisogna trovare un valore  $p^*$  che massimizza

$$Np(1-p)^{N-1}$$

- Per un elevato numero di nodi, ricaviamo il limite di  $Np^*(1-p^*)^{N-1}$  per  $N$  che tende all'infinito, e otterremo  $1/e = 0,37$
- Nel caso migliore: solo il 37% degli slot compie lavoro utile

# ALOHA puro

- ALOHA puro è più semplice ed è non sincronizzato
- Quando arriva il primo pacchetto:
  - ▣ Lo trasmette immediatamente e integralmente nel canale broadcast
- Elevate probabilità di collisione:
  - ▣ Il pacchetto trasmesso all'istante  $t_0$  si sovrappone con la trasmissione dell'altro pacchetto inviato in  $[t_0 - 1, t_0 + 1]$
- L'efficienza di ALOHA pure è di 0.18...peggio si slotted ALOHA

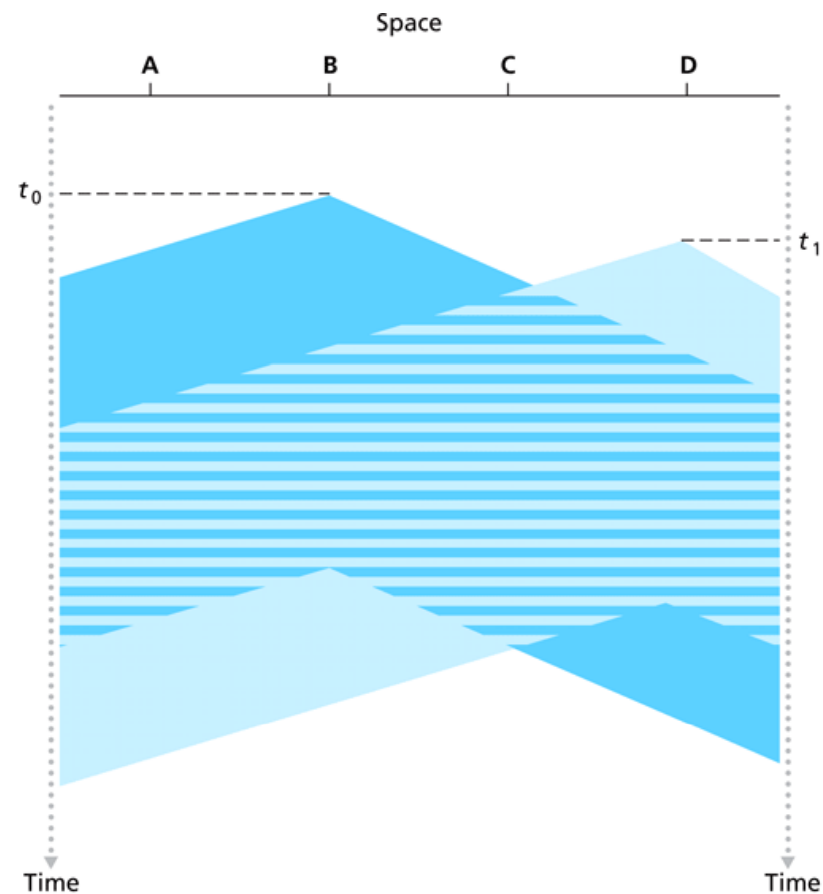


# Accesso multiplo a rilevazione della portante (CSMA)

- Nella versione **CSMA** (*carrier sense multiple access*) si ascolta il canale prima di trasmettere
  - ▣ Se rileva se il canale è libero e si trasmette l'intero pacchetto
  - ▣ Se il canale sta già trasmettendo, il nodo aspetta un altro intervallo di tempo
- Analogia: se qualcun altro sta parlando usa l'educazione aspettate fino a quando non ha finito!

# CSMA con trasmissioni in collisione

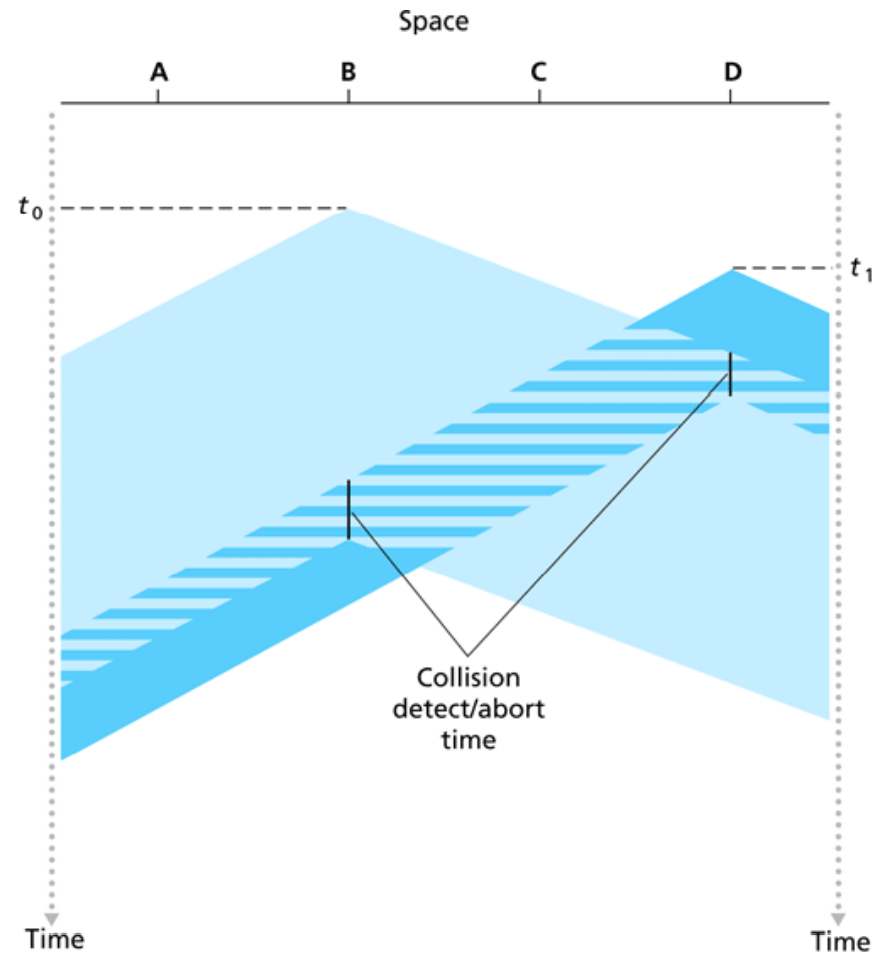
- Le collisioni possono ancora verificarsi:
  - Il ritardo di propagazione fa sì che due nodi non rilevino la reciproca trasmissione
- Quando si verifica una collisione un nodo termina immediatamente la trasmissione
- La distanza e il ritardo di propagazione giocano un ruolo importante nel determinare la probabilità di collisione



# CSMA/CD (rilevazione di collisione)

- CSMA/CD: rilevamento della portante differito, come in CSMA:
  - Rileva la collisione in poco tempo
  - Annulla la trasmissione non appena si accorge che c'è un'altra trasmissione in corso
- Rilevazione della collisione:
  - Facile nelle LAN cablate
  - Difficile nelle LAN wireless
- Il nodo è un interlocutore educato

# CSMA/CD (rilevazione di collisione)



# Protocolli a rotazione



- Protocolli a suddivisione del canale:
  - ▣ Condividono il canale equamente ed efficientemente con carichi elevati
  - ▣ Inefficienti con carichi non elevati
- Protocolli ad accesso casuale:
  - ▣ Efficiente anche con carichi non elevati: un singolo nodo può utilizzare interamente il canale
  - ▣ Carichi elevati: eccesso di collisioni
- Protocolli a rotazione
  - ▣ Prendono il meglio dei due protocolli precedenti!

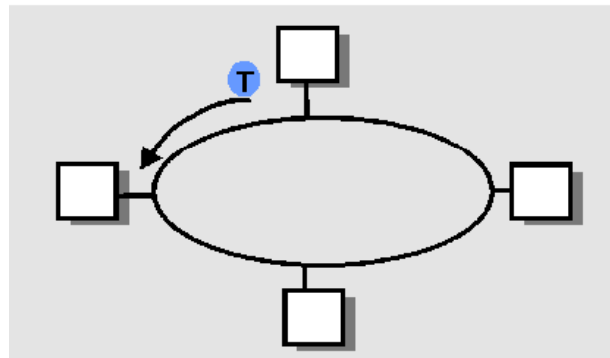
# Protocolli a rotazione

## □ Protocollo polling:

- Un nodo principale sonda “a turno” gli altri.
- In particolare:
  - Elimina le collisioni
  - Elimina gli slot vuoti
  - Ritardo di polling

## □ Protocollo token-passing:

- Un messaggio di controllo circola fra i nodi seguendo un ordine prefissato
- Messaggio di controllo (**token**)
- In particolare:
  - Decentralizzato
  - Altamente efficiente
  - Il guasto di un nodo può mettere fuori uso l'intero canale



# Protocolli: riepilogo

- Cosa si può fare con un canale condiviso?
  - ▣ Suddivisione del canale per: tempo, frequenza, codice.
    - TDM, FDM
  - ▣ Suddivisione casuale (dinamica).
    - ALOHA, S-ALOHA, CSMA, CSMA/CD
    - Rilevamento della portante: facile in alcune tecnologie (cablate), difficile in altre (wireless)
    - CSMA/CD usato in Ethernet
    - CSMA/CA usato in 802.11
  - ▣ A rotazione.
    - Polling con un nodo principale; a passaggio di testimone.

# Tecnologie LAN

- Fin qui, il livello di link:
  - ▣ Servizi, rilevamento/correzione dell'errore, accesso multiplo
- Andiamo avanti: tecnologie LAN
  - ▣ Indirizzamento
  - ▣ Ethernet
  - ▣ Hub, switch
  - ▣ PPP

