

Università di Roma Tor Vergata  
Corso di Laurea triennale in Informatica  
**Sistemi operativi e reti**  
A.A. 2017-18

Pietro Frasca

Parte II: Reti di calcolatori  
Lezione 21 (45)

Martedì 29-05-2018

# Controllo a ridondanza ciclica (CRC)

- Una tecnica di rilevazione dell'errore molto usata nelle reti di calcolatori è basata sui codici di controllo a ridondanza ciclica (**CRC, *Cyclic Redundancy Check***).
- I codici CRC sono chiamati anche **codici polinomiali**, poiché è possibile vedere la stringa dei bit da controllare come un polinomio i cui coefficienti sono valori 0 e 1.
- Ad esempio, la sequenza **10101101** può essere rappresentata dal polinomio

$$x^7 + x^5 + x^3 + x^2 + 1$$

- Per descrivere il funzionamento dei codici CRC consideriamo una sequenza ***D***, costituita di ***d*** bit che il nodo mittente invia al nodo ricevente.



- Il mittente appende alla stringa ***D*** di lunghezza ***d*** bit, una stringa ***R*** di ***r* bit**, in modo che la stringa risultante di ***d + r*** bit sia esattamente divisibile per un polinomio ***G*** di ***r+1*** bit detto ***polinomio generatore***.
- Trasmettitore e ricevitore utilizzano uno stesso polinomio generatore ***G*** di grado ***r+1***, ed eseguono le operazioni con l'aritmetica modulo 2.



- Il ricevitore divide i  **$d + r$**  bit ricevuti per **G**.
- Se il resto della divisione è diverso da zero, il ricevitore capisce che si è verificato un errore; altrimenti i dati sono accettati come corretti.
- Tutti i calcoli CRC sono eseguiti in **aritmetica modulo 2** senza riporti e resti in addizione e sottrazione.



- Questo significa che addizione e sottrazione sono operazioni identiche, e che entrambe equivalgono all'**operazione di OR esclusivo (XOR)** bit a bit degli operandi.

**Tabella della verità XOR**

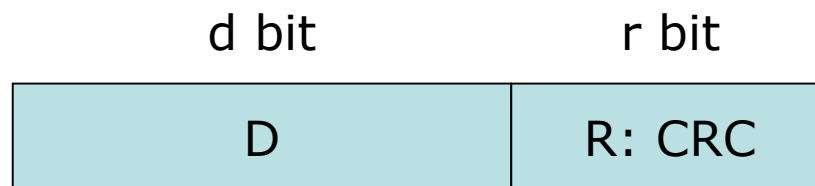
x1	x2	Y
0	0	0
0	1	1
1	0	1
1	1	0

- Allora, per esempio,

1011 XOR 0101 = 1110

1001 XOR 1101 = 0100

- Moltiplicazione e divisione sono le stesse dell'aritmetica in base 2. La moltiplicazione per  $2^r$  provoca lo slittamento (shift) a sinistra dei bit di  $r$  posizioni. Quindi, dati  $D$  e  $R$ , la quantità  **$D \cdot 2^r \text{ XOR } R$**  fornisce una stringa di  **$d + r$**  bit.



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

- Il **mittente** calcola  **$R$**  in modo che  **$D \cdot 2^r \text{ XOR } R$**  sia divisibile per  **$G$**  senza avere resto:

$$(D \cdot 2^r \text{ XOR } R) / G = n =$$

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

Se eseguiamo l'operazione XOR di **R** con entrambi i membri dell'equazione sopra, otteniamo

$$\mathbf{D \cdot 2^r XOR R = n \cdot G}$$

$$\begin{aligned}\mathbf{D \cdot 2^r XOR R XOR R} &= \mathbf{n \cdot G XOR R} = \\ \mathbf{D \cdot 2^r XOR (R XOR R)} &= \mathbf{n \cdot G XOR R} = \\ \mathbf{D \cdot 2^r XOR 0} &= \mathbf{n \cdot G XOR R} = \\ \mathbf{D \cdot 2^r} &= \mathbf{n \cdot G XOR R}\end{aligned}$$

- Questa equazione ci dice che se dividiamo  **$D \cdot 2^r$**  per **G**, il valore del resto è precisamente **R**.
- In altre parole, possiamo calcolare **R** come

$$\mathbf{R = resto (D \cdot 2^r / G)}$$

# Esempio di calcolo CRC

Eseguiamo il calcolo del CRC nel caso in cui

$$D = 101110 \ (d = 6)$$

$$G = 1001, \ r = 3.$$

I nove bit trasmessi in questo caso sono **101110 011**.



**D·2<sup>3</sup>**

1	0	1	1	1	0	0	0	0
1	0	0	1					
<hr/>								
0	0	1	0	1	0			
		1	0	0	1			
<hr/>								
	0	0	1	1	0	0		
			1	0	0	1		
<hr/>								
		0	1	0	1	0		
			1	0	0	1		
<hr/>								
			0	0	1	1		

**R**

**G**

1	0	0	1		
1	0	1	0	1	1

1 0 1 1 1 0 0 1 1

Esempio di calcolo di CRC al mittente

<b>D'</b>	<b>G</b>
1 0 1 1 1 0 0 1 1	1 0 0 1
1 0 0 1	1 0 1 0 1 1
0 0 1 0 1 0	
1 0 0 1	
0 0 1 1 0 1	
1 0 0 1	
0 1 0 0 1	
1 0 0 1	
0 0 0 0	
<b>R</b>	

Esempio di calcolo di CRC al ricevitore

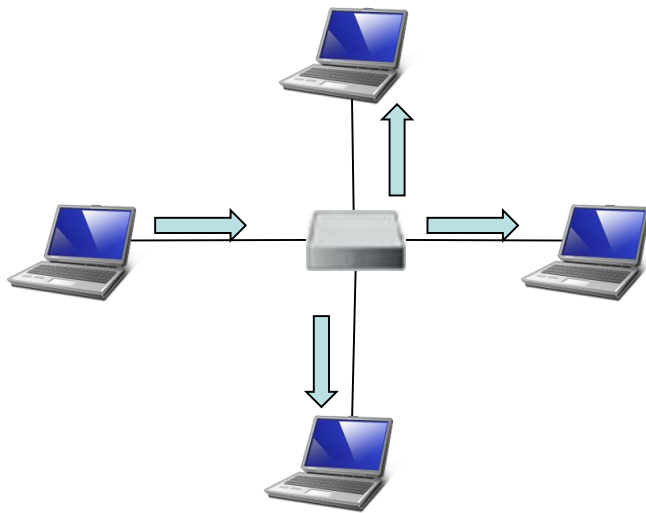
- Sono stati definiti standard internazionali per **generatori G** di 8, 12, 16 e 32 bit. Lo standard CRC-32 a 32 bit, che è stato adottato in numerosi protocolli IEEE dello strato di collegamento, usa un generatore di

$$\mathbf{G_{CRC-32} = 100000100110000010001110110110111}$$

- Ciascuno dei CRC standard può rilevare errori a raffica inferiori a  $r + 1$  bit.
- Inoltre, ciascuno dei CRC standard può rilevare qualsiasi numero dispari di errori.

# Protocolli di accesso multiplo

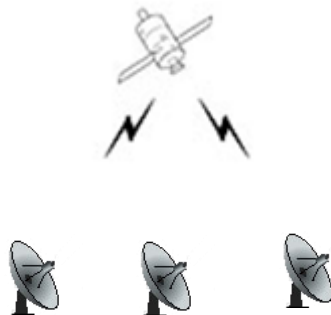
- Molti protocolli dello strato di collegamento, come ad esempio il PPP, sono stati progettati per i link **punto-punto**, in grado di connettere solo due nodi.
- Il tipo di link **broadcast**, invece, può avere più nodi collegati allo stesso canale condiviso.
- Nel link broadcast un frame trasmesso da un nodo è ricevuto da tutti gli altri nodi connessi allo stesso canale.
- **Ethernet, LAN wireless e le reti satellitari** sono esempi di tecnologia a link broadcast.
- Prima di descrivere le caratteristiche dei protocolli dello strato di collegamento ethernet e wi-fi, parleremo di un importante problema per lo strato di collegamento: **il problema dell'accesso multiplo** consistente in come coordinare l'accesso al canale condiviso da parte di più nodi.



Canale cablato condiviso  
(esempio Ethernet)



Canale wireless condiviso  
(esempio WiFi)



Satellite



Lezione in classe

## Diversi canali condivisi ad accesso multiplo

- Poiché il canale è condiviso, è possibile che più di due nodi possano trasmettere frame nello stesso istante causando una **collisione** dei frame trasmessi.
- Quando si verifica una collisione, i segnali relativi ai frame trasmessi producono un segnale risultante distorto, non comprensibile ai nodi che lo ricevono.
- Pertanto, durante il tempo di collisione il canale broadcast condiviso è inutilizzato.
- È evidente che, se molti nodi trasmettono con una elevata frequenza, molti frame collideranno, e la larghezza di banda del canale broadcast si ridurrà.
- E' necessario quindi limitare al massimo le collisioni coordinando le trasmissioni dei nodi.
- Il compito di coordinare le trasmissioni è svolto dai **protocolli di accesso multiplo**.

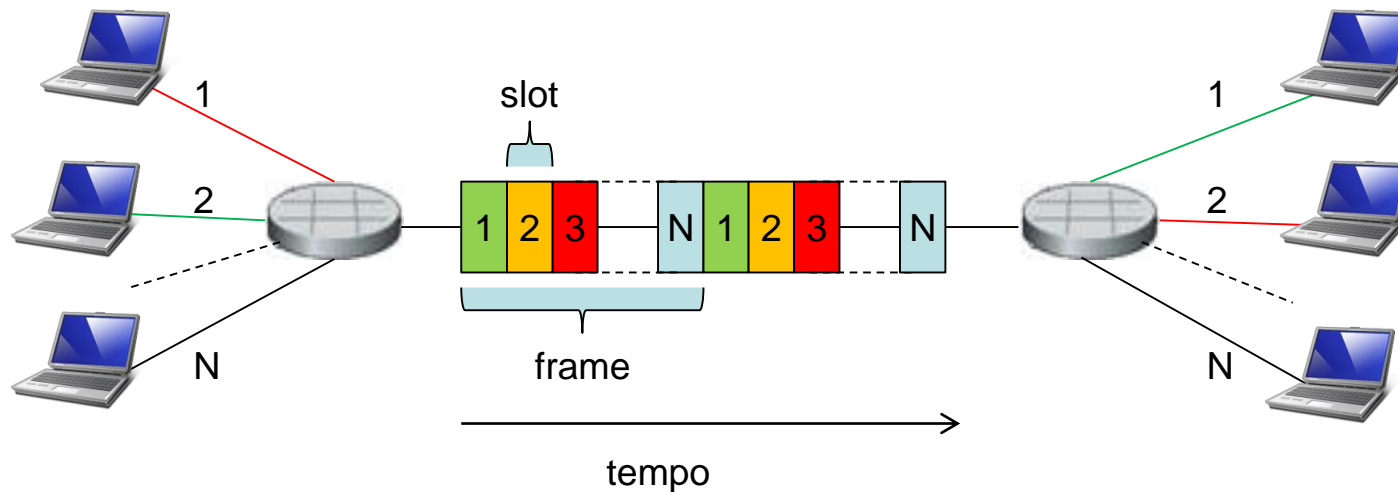
- Negli ultimi decenni, sono stati progettati numerosi protocolli ad accesso multiplo e, attualmente, la ricerca è molto attiva soprattutto nel campo delle reti **Wireless**.
- Schematicamente, possiamo classificare i protocolli di accesso multiplo in tre classi:
  - **protocolli a suddivisione di canale** (*channel partitioning protocol*),
  - **protocolli ad accesso casuale** (*random access protocol*) e
  - **protocolli a turni (rotazione)** (*taking-turns protocol*).

# Protocolli a suddivisione del canale

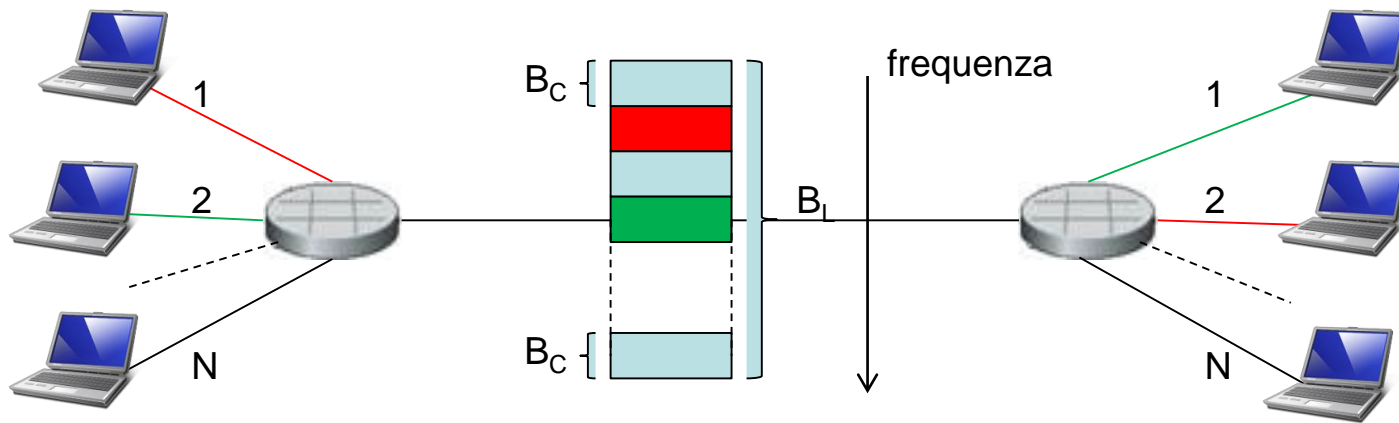
- Ricordiamo che il **multiplexing a divisione di tempo** (**TDM**, *Time Division Multiplexing*), e il **multiplexing a divisione di frequenza** (**FDM**, *Frequency Division Multiplexing*), sono due tecniche che possono essere usate per suddividere la larghezza di banda di un canale tra tutti i nodi che condividono quel canale.
- Ad esempio, supponiamo che il canale sia condiviso da  **$N$**  nodi e che la velocità di trasmissione del canale sia  **$R$**  bit/s.
- Il TDM divide il tempo in **intervalli di tempo** (o frame) e poi divide ciascun frame in  $N$  blocchi (**slot**) di tempo. Ciascuno slot è quindi assegnato a uno degli  $N$  nodi. Ogni volta che un nodo ha un frame da spedire, esso trasmette i bit del frame durante lo slot di tempo a esso assegnato nel frame TDM a rotazione.



- Di solito, le dimensioni del frame (tempo) sono scelte in modo che durante uno slot di tempo possa essere trasmesso un singolo frame (pacchetto). La figura mostra un semplice esempio di TDM a N nodi.



- Il TDM elimina le collisioni e ciascun nodo ottiene una velocità di trasmissione dedicata di  $R/N$  bit/s durante ciascun frame di tempo.
- Il TDM ha due evidenti svantaggi:
  - un nodo può trasmettere alla velocità media di  $R/N$  bit/s anche quando è l'unico nodo che ha frame da inviare.
  - un nodo per trasmettere deve sempre attendere il suo turno anche se è l'unico nodo che ha frame da spedire.
- L'FDM invece, divide il canale a  $R$  bit/s in differenti frequenze (ciascuna con larghezza di banda di  $R/N$ ) e assegna ciascuna frequenza a uno degli  $N$  nodi.
- L'FDM quindi suddivide il canale di  $R$  bit/s in  $N$  canali più piccoli di  $R/N$  bit/s.
- L'FDM condivide sia vantaggi sia svantaggi con il TDM. Evita le collisioni e divide la larghezza di banda fra gli  $N$  nodi. Tuttavia, l'FDM condivide anche il principale inconveniente con il TDM: un nodo utilizza una larghezza di banda di  $R/N$ , anche quando è il solo nodo che ha frame da trasmettere.



# Protocolli di accesso casuale

- Una seconda classe di protocolli ad accesso multiplo è costituita dai protocolli ad **accesso casuale** (***random access protocols***).
- In un protocollo ad accesso casuale, un nodo trasmette i dati sempre alla massima velocità del canale, cioè a  $R$  bit/s.
- Quando si verifica una collisione, ciascun nodo ritrasmette ripetutamente il suo frame finché questo passa senza collisioni. Più precisamente, ogni nodo coinvolto nella collisione, non ritrasmette subito il suo frame ma ***attende un ritardo casuale indipendente***. Poiché i ritardi sono scelti indipendentemente, è probabile che uno dei nodi scelga questo ritardo abbastanza piccolo, rispetto a quello degli altri nodi in collisione, tale da consentire al suo frame di attraversare il canale senza collisioni.

# CSMA (Carrier Sense Multiple Access, accesso multiplo a rilevazione di portante)

- I protocolli **CSMA (Carrier Sense Multiple Access, accesso multiplo a rilevazione di portante)** e **CSMA/CD (CSMA with Collision Detection, CSMA con rilevazione di collisione)** basano il loro funzionamento su due fondamentali operazioni che un nodo deve eseguire per trasmettere su un canale condiviso:
  - ***Verificare se il canale è libero prima di trasmettere. (rilevazione di portante)***: un nodo ascolta il canale prima di trasmettere. Se il canale è occupato da un frame di un'altra trasmissione, il nodo allora attende un intervallo di tempo casuale dopo di che ascolta di nuovo il canale. Se rileva che il canale è libero il nodo inizia a trasmettere. In caso contrario, il nodo aspetta un altro intervallo di tempo casuale e poi ripete la procedura.
  - ***Interrompere la trasmissione se qualche altro nodo sta trasmettendo (rilevazione di collisione)***: un nodo che sta trasmettendo continua ad ascoltare il canale mentre trasmette.

Se rileva che un altro nodo sta trasmettendo un frame che interferisce, termina la trasmissione e attende un intervallo di tempo casuale prima di ricominciare a trasmettere.

- E' da notare che nonostante il CSMA esegua l'operazione di **rilevazione di portante prima di trasmettere** è sempre possibile che si verifichino collisioni. Per chiarire questo facciamo riferimento alla figura seguente che mostra un **diagramma spazio-tempo** in cui quattro nodi A, B, C, e D sono collegati a un canale broadcast.
- All'istante  **$t_0$** , il **nodo B** rileva che il canale è libero, e quindi inizia a trasmettere. La propagazione del frame di B richiede un intervallo di tempo **non nullo**, nonostante il frame si propaghi ad una velocità prossima a quella della luce.
- All'istante  **$t_1$  ( $t_1 > t_0$ )**, il **nodo D sonda il canale e**, sebbene il nodo B stia ancora trasmettendo, al tempo  $t_1$  i bit trasmessi da B non hanno ancora raggiunto il nodo D, per cui in base al protocollo CSMA, D inizia a trasmettere. Dopo un breve tempo, la trasmissione di B comincia a interferire con quella di D.

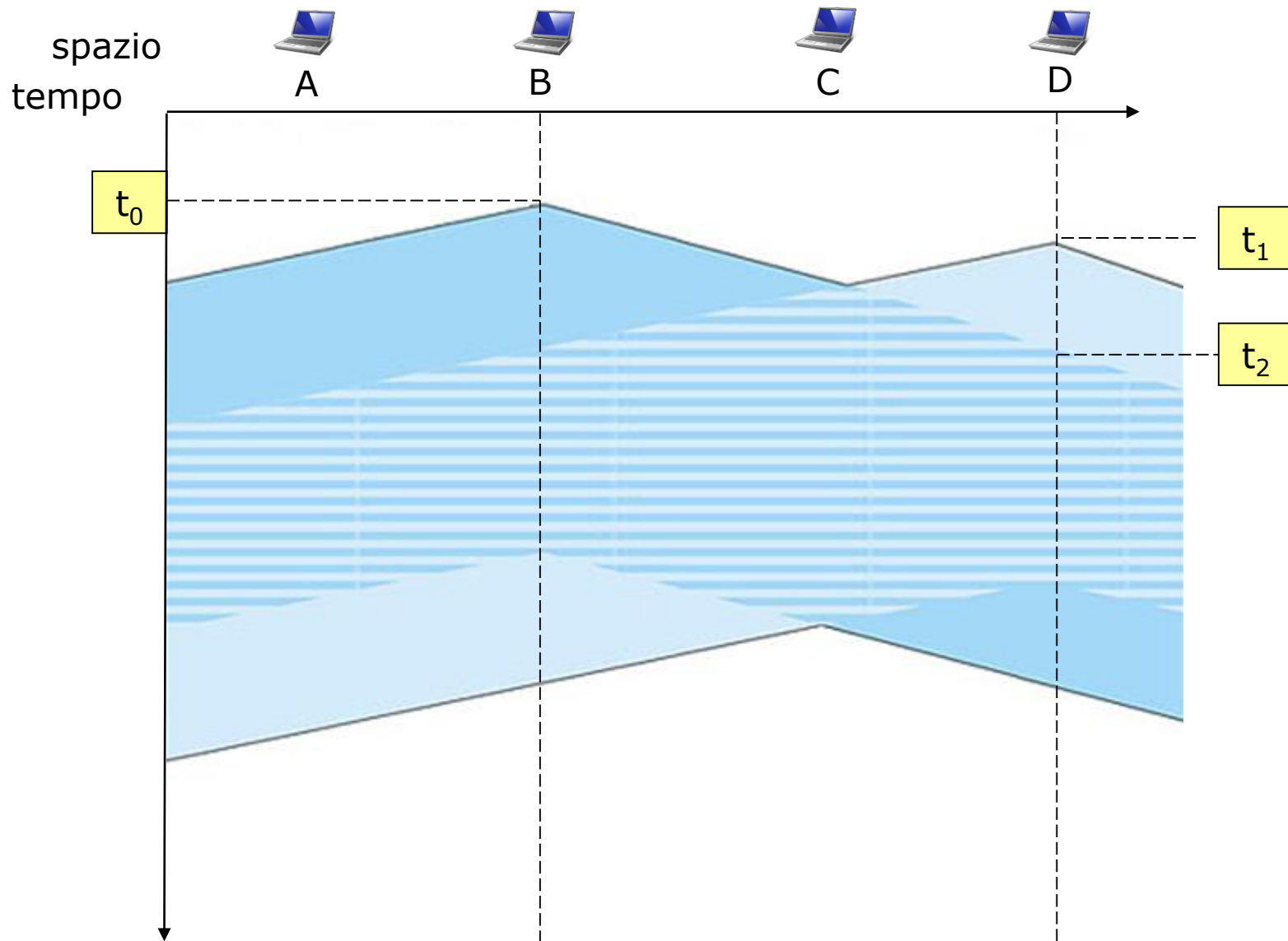
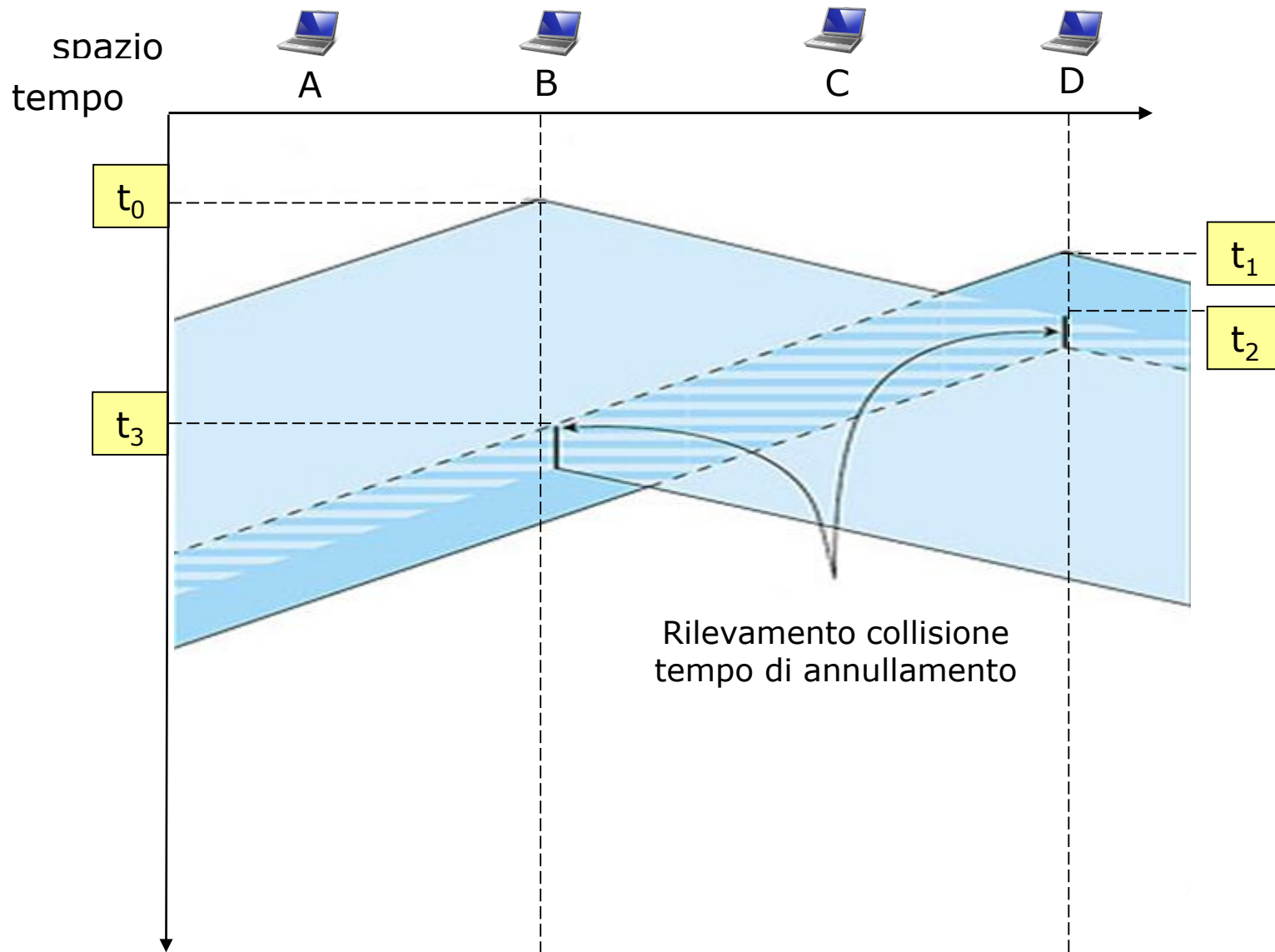


Diagramma spazio-tempo di due nodi CSMA con trasmissione in collisione.

- Dalla figura risulta evidente che il tempo richiesto da un segnale per propagarsi da un estremo all'altro del canale avrà una importanza fondamentale per valutare le prestazioni del canale. Infatti, maggiore è questo tempo di propagazione, maggiore sarà la probabilità che un nodo non sia in grado di rilevare una trasmissione che è già iniziata da parte di un altro nodo.
- Nella figura precedente, i nodi **non eseguono la rilevazione delle collisioni**; B e D continuano entrambi a trasmettere i loro frame nella loro interezza anche se si è verificata una collisione.
- Quando invece un nodo esegue l'operazione di **rilevazione di collisione**, esso **cesserà la trasmissione** immediatamente dopo averla rilevata. La figura seguente mostra la stessa scena della figura precedente, ma ora i due nodi eseguono l'operazione di rilevazione di collisione.





CSMA con controllo di collisione.

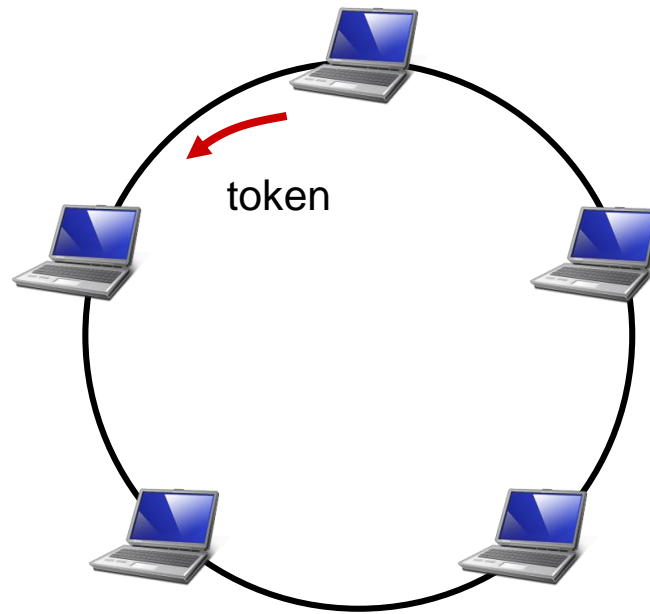
- E' evidente che l'uso della rilevazione di collisione a un protocollo di accesso multiplo migliorerà le prestazioni del protocollo evitando l'inutile trasmissione completa del frame danneggiato (dall'interferenza con un frame di un altro nodo).
- **Il protocollo Ethernet utilizza il CSMA/CD.**

# Protocolli a turno (rotazione)

- Sono stati progettati vari protocolli a turno.
- Due dei protocolli più importanti sono il **protocollo a sondaggio (polling protocol)** e il **protocollo a passaggio del testimone (token-passing protocol)**.
- Nel protocollo a sondaggio uno dei nodi funziona come nodo master (principale) che ha il compito di interrogare a rotazione ciascuno dei nodi.
- Inizialmente, il nodo master invia un messaggio al nodo 1, abilitandolo a trasmettere un certo numero massimo di frame. Dopo che il nodo 1 ha trasmesso i suoi frame, il nodo master ripete la stessa procedura con il nodi successivi.
- Il nodo master può determinare quando un nodo ha terminato di inviare i suoi frame rilevando l'assenza di un segnale nel canale.

- Il protocollo a sondaggio elimina le collisioni che costituiscono il punto debole dei protocolli di accesso casuale e quindi può avere un'efficienza più alta.
- Tuttavia presenta anche qualche svantaggio. Il primo è dovuto al fatto che il protocollo produce un **ritardo di sondaggio** dovuto al tempo richiesto per abilitare un nodo alla trasmissione. Ad esempio, se è attivo solo un nodo, allora il nodo trasmetterà a una velocità inferiore a  $R$  bit/s, poiché il master deve sondare ciclicamente tutti i nodi inattivi tutte le volte che il nodo attivo ha terminato l'invio del suo numero massimo di frame.
- Il secondo svantaggio, potenzialmente più grave, è che se un nodo master si guasta, l'intero canale non è più funzionante.
- Il secondo protocollo a rotazione è il **protocollo a passaggio del testimone**, o del gettone (***token-passing protocol***).

- Il protocollo del passaggio del token è decentralizzato, in quanto non esiste un nodo master.
- I nodi si scambiano un piccolo frame detto **token** (gettone), in un ordine prefissato. Per esempio, il nodo 1 spedisce il token al nodo 2, il nodo 2 lo spedisce al nodo 3, il nodo  $N$  spedisce il token al nodo 1.
- Quando un nodo riceve il token e non deve trasmettere, rinvia il token al nodo successivo. Se invece in nodo deve trasmettere, esso invia il numero massimo consentito di frame e poi passa il token al nodo seguente.
- Questo protocollo ha un'alta efficienza, ma risulta poco robusto. Infatti basta che un solo nodo si guasti per mettere fuori servizio l'intera rete.



Protocollo a passaggio del testimone

# Reti di area locale (LAN)

- Una rete di area locale (LAN, *Local Area Networks*) è una rete di calcolatori cablata in un'area limitata come la superficie di uno o più edifici.
- Negli anni '80 e nei primi anni '90, erano diffuse principalmente due classi di tecnologie LAN.
- La prima classe era costituita dalle LAN **Ethernet (IEEE 802.3)** basate sull'accesso casuale e la seconda classe era quella a **passaggio del token**, tra cui la **token ring (IEEE 802.5)** e la **FDDI (*interfaccia dati distribuita su fibra, Fiber Distributed Data Interface*)**.
- Le tecnologie basate sul passaggio del token hanno avuto un'importanza minore rispetto alla grande diffusione di Ethernet.
- Attualmente, la velocità di trasmissione *delle* LAN Ethernet è di 10 Mbit/s, 100 Mbit/s, 1 Gbit/s e di 10 Gbit/s.
- Tipicamente, la LAN è connessa a Internet attraverso un router, come mostrato nella figura seguente.

