

Livello di Rete: Broadcast, Multicast  
Livello di collegamento: introduzione

Gaia Maselli  
maselli@di.uniroma1.it

Queste slide sono un adattamento delle slide fornite dal libro di testo e pertanto protette da copyright.  
All material copyright 1996-2007 J.F Kurose and K.W. Ross, All Rights Reserved

# Livello di rete

Introduzione

Reti a circuito virtuale e  
a datagramma

Che cosa si trova  
all'interno di un  
router?

Protocollo Internet (IP)

- Formato dei datagrammi
- Indirizzamento IPv4
- ICMP
- IPv6

Algoritmi di  
instradamento

- Stato del collegamento
- Vettore distanza
- Instradamento gerarchico

Instradamento in  
Internet

- RIP
- OSPF
- BGP

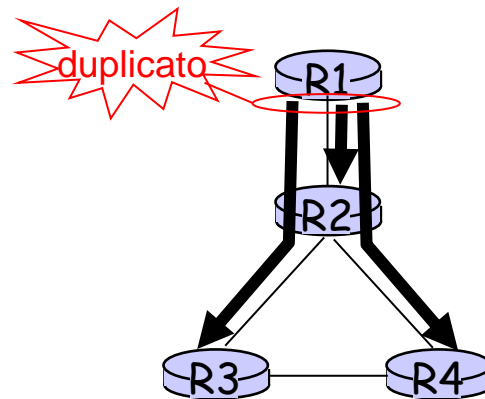
Instradamento  
broadcast e multicast

# Unicast, broadcast, multicast

- ❑ UNICAST: comunicazione punto-punto in cui un nodo sorgente invia un pacchetto a una destinazione SINGOLA
  - Comunicazione 1 a 1
  
- ❑ BROADCAST: invio di un pacchetto da un nodo sorgente a TUTTI i nodi della rete
  - Comunicazione 1 a N, N: tutti I nodi della rete
  
- ❑ MULTICAST: invio di un pacchetto da un nodo sorgente ad ALCUNI nodi della rete
  - Comunicazione 1 a M,  $M < N$  (M: gruppo di nodi della rete)

# Instradamento broadcast: Unicast a N vie

- ❑ Consegna di un pacchetto spedito da un nodo origine a TUTTI gli altri nodi della rete.
- ❑ Può essere realizzato mediante unicast a N vie
  - ❑ Spedizione unicast verso ogni destinatario: all'origine viene creata una copia del pacchetto per ogni destinatario (N copie)

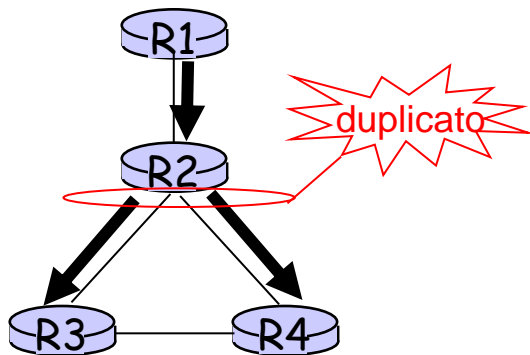


Duplicazione  
All'origine

- ❑ Inefficiente
- ❑ Necessità di conoscere gli IP di tutti i nodi della rete

# Intradamento broadcast: flooding incontrollato

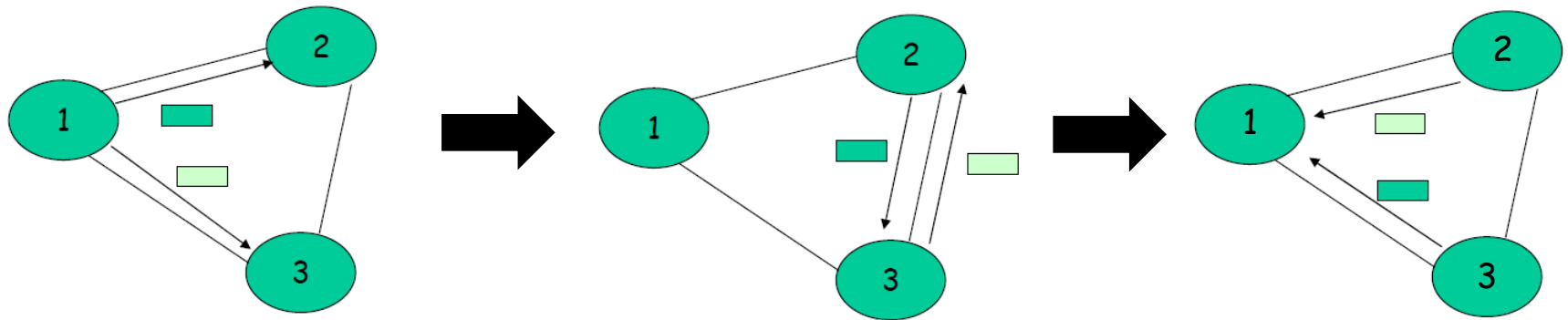
- ❑ Flooding (inondazione): quando un nodo riceve un pacchetto di broadcast ne crea una copia per ogni vicino e glielo invia (escluso il nodo da cui ha ricevuto il pacchetto)



Duplicazione  
interna alla rete

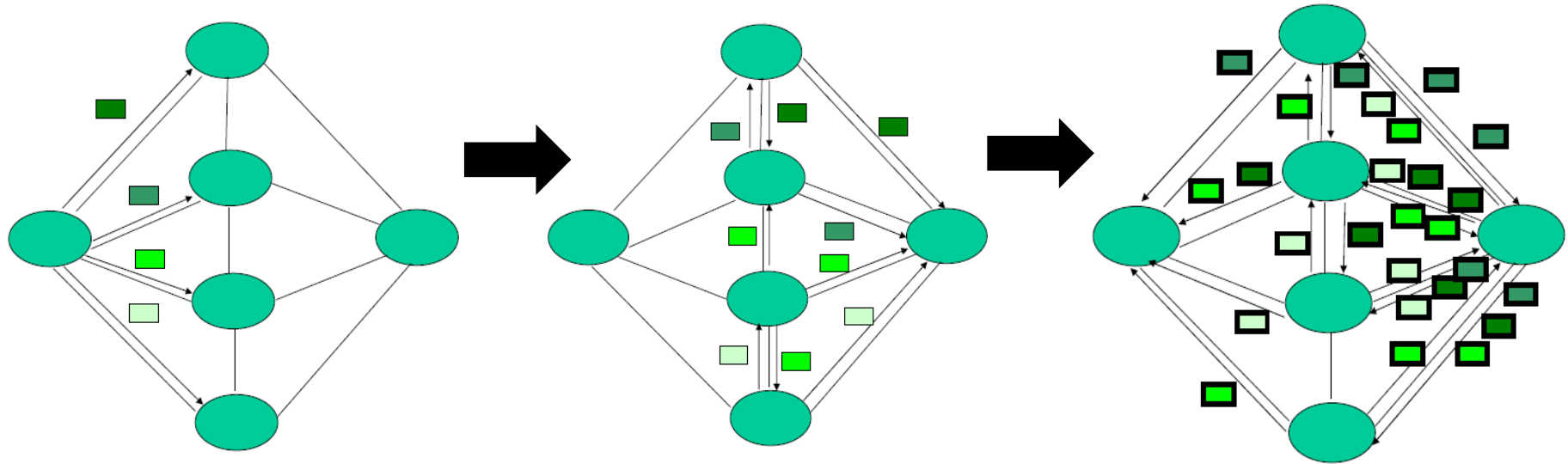
- ❑ Inefficiente
  - ❑ Cicli nella rete
  - ❑ Broadcast storm

# Problema dei cicli nel flooding incontrollato



- ❑ Più copie di un pacchetto broadcast continueranno a percorrere quel ciclo
- ❑ Per evitare cicli bisogna saper distinguere tra quando mandiamo un nuovo messaggio e quando stiamo ritrasmettendo qualcosa che abbiamo già visto
  - Numeri di sequenza!

# Problema del broadcast storm nel flooding incontrollato



- ❑ Il numero di pacchetti in rete cresce significativamente quando il numero di vicini è elevato
- ❑ Ogni nodo riceve svariate copie dello stesso pacchetto

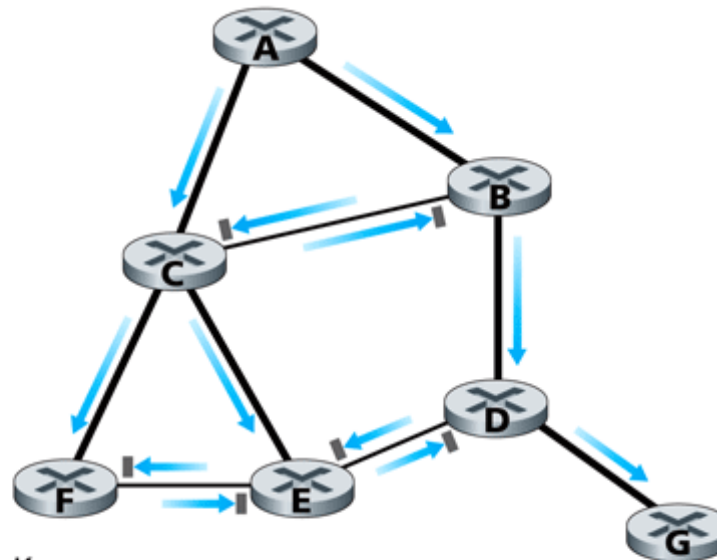
# Flooding controllato (1)

- ❑ Flooding controllato con numero di sequenza
- ❑ Il nodo origine pone il proprio indirizzo ed il numero di sequenza nei pacchetti che invia in broadcast
- ❑ Ciascun nodo mantiene una lista di (ID origine, SEQN) per i broadcast inviati
- ❑ Se riceve un pacchetto broadcast per prima cosa verifica se  $\langle \text{ID}, \text{SEQN} \rangle$  compare nella lista dei pacchetti già gestiti
  - Se si  $\rightarrow$  scarta
  - Altrimenti  $\rightarrow$  riinvia a tutti i vicini escluso quello da cui ha ricevuto il pacchetto



# Flooding controllato (2)

- ❑ Inoltro su percorso inverso
- ❑ Quando un router riceve un pacchetto di broadcast lo trasmette a tutti i suoi vicini (escluso quello da cui è stato ricevuto il pacchetto) solo se è pervenuto attraverso il percorso unicast più breve tra il router e l'origine



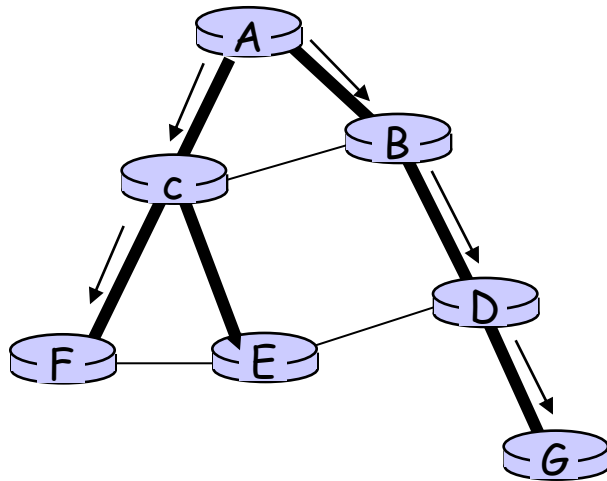
Key:

→ pkt will be forwarded

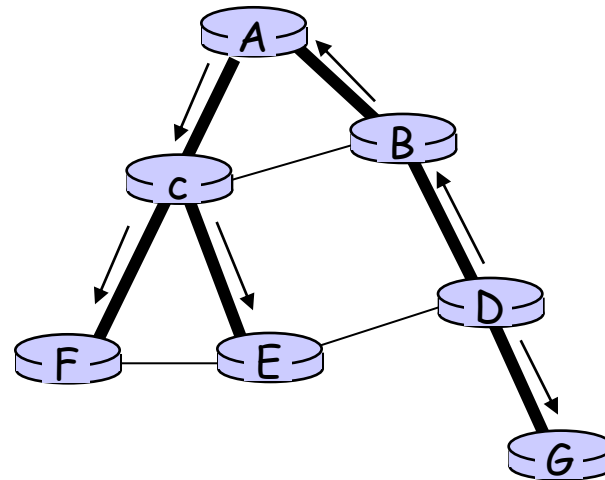
→| pkt not forwarded beyond receiving router

# Broadcast con Spanning tree

1. Creare l'albero di copertura (spanning tree): Albero ricoprente di un grafo, che contiene tutti i nodi e non contiene cicli
2. Ogni nodo invia un pacchetto broadcast solo sui collegamenti che appartengono all'albero di copertura.



(a) Broadcast iniziato presso A

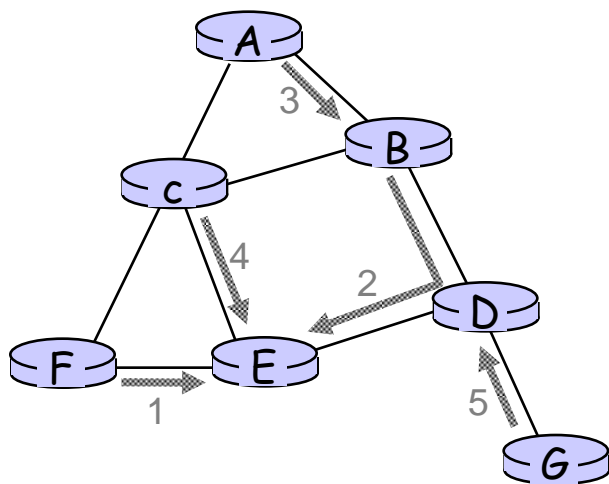


(b) Broadcast iniziato presso D

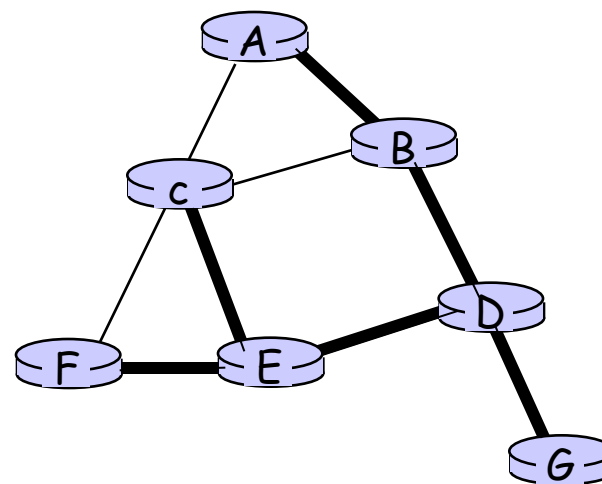
- Elimina completamente pacchetti ridondanti !!!

# Determinazione dell'albero di copertura

- Si definisce un nodo centrale (nell'esempio E).
- I nodi inoltrano al nodo centrale il messaggio di adesione.
  - Il messaggio prosegue fino a quando raggiunge un router che già appartiene all'albero di copertura o arriva al nodo centrale.



(a) Costruzione passo passo dell'albero di copertura



(b) Albero di copertura risultante

# perchè il broadcast

- ❑ Usato al livello di applicazione da protocolli come Gnutella per trasmettere richieste di dati tra i propri peer
  - Flooding a campo limitato: flooding controllato con numeri di sequenza, e TTL per limitare il numero di hop
- ❑ Algoritmi link state come OSPF
  - Flooding controllato con numeri di sequenza

# Instradamento multicast

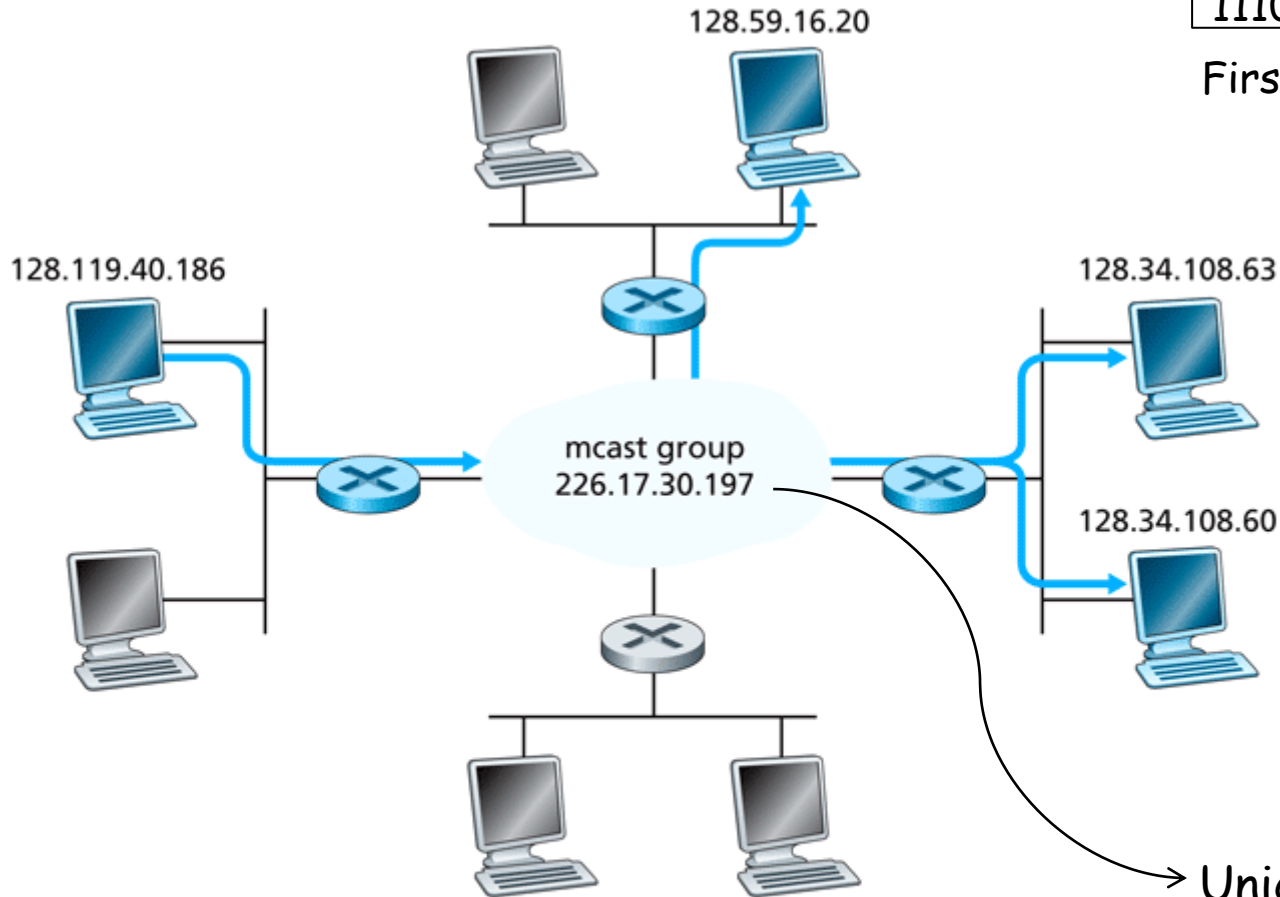
- Molte applicazioni richiedono il trasferimento di pacchetti da uno o più mittenti ad un gruppo di destinatari
  - trasferimento di un aggiornamento SW su un gruppo di macchine
  - streaming (audio/video) ad un gruppo di utenti o studenti
  - applicazioni con dati condivisi (lavagna elettronica condivisa da più utenti)
  - aggiornamento di dati (andamento di borsa)
  - giochi multi-player interattivi

# Gruppo multicast


Indirizzi multicast:


1110	group identifier
------	------------------

First byte: 224 to 239



Key:

 Router with attached group member

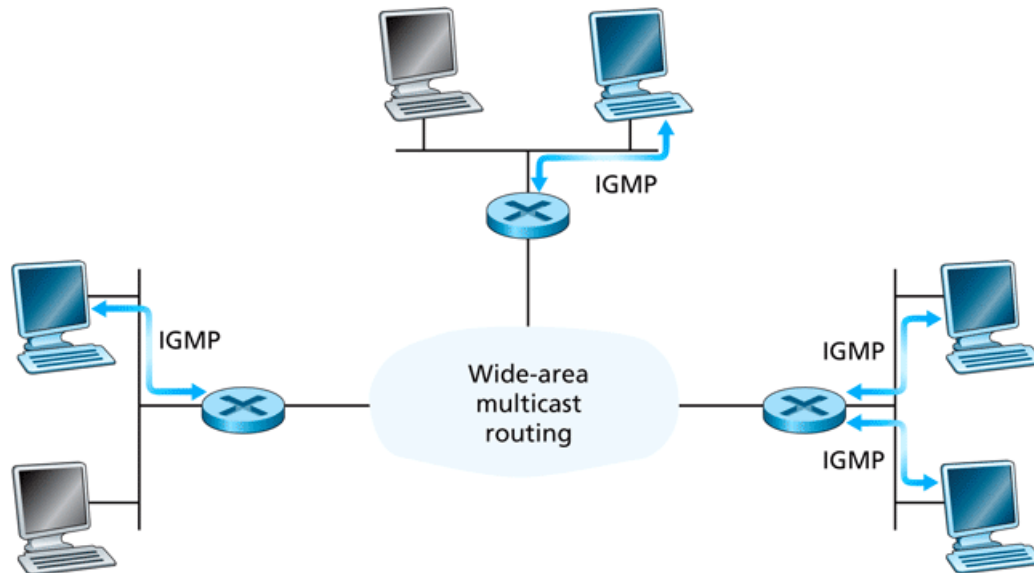
 Router with no attached group member

Unico indirizzo IP a cui sono associati più host

I router devono sapere quali host sono associati a un gruppo multicast !!!

# Internet Group Management Protocol (IGMP)

- ❑ Lavora tra un **host** e il **router** che gli è direttamente connesso
- ❑ Offre agli host il mezzo di informare i router ad essi connessi del fatto che un'applicazione in esecuzione vuole aderire ad uno specifico gruppo multicast
- ❑ È necessario un protocollo che coordini i router multicast in Internet



# IGMP

- ❑ Messaggi incapsulati in datagrammi IP, con IP protocol number 2
  - Mandati con TTL a 1
- ❑ Messaggi IGMP
  - **Membership query**: router → host, per determinare quali host hanno aderito a un gruppo su ogni interfaccia
  - **Membership report**: host → router per informare il router su un'adesione, anche non inseguito a una query (al momento dell'adesione)
  - **Leave group**: host → router, quando si lascia un gruppo
- ❑ Il leave group è opzionale: il router può capire che non ci sono più host associati a un gruppo quando non riceve report in risposta a query

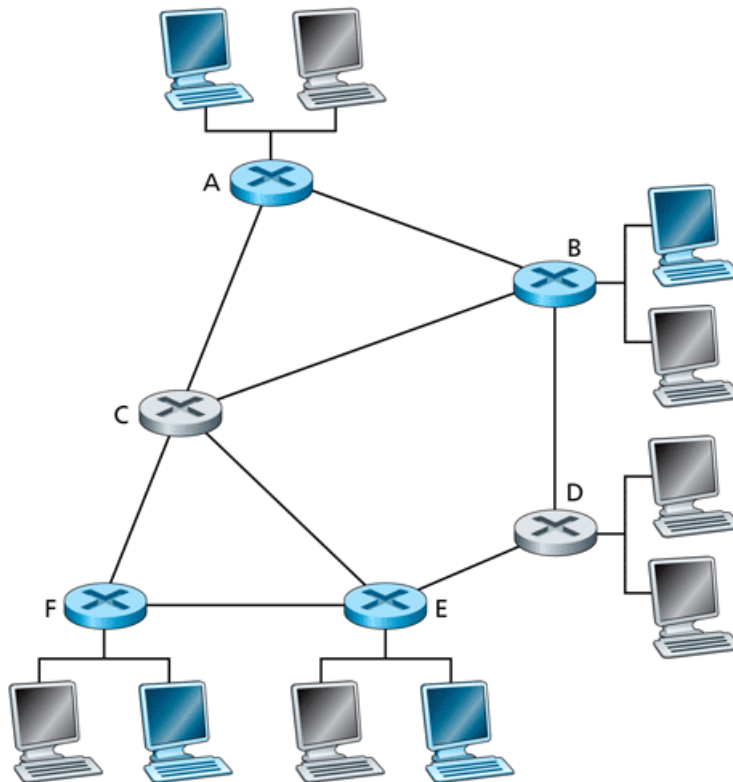


# IGMP

- Un router multicast tiene una lista per ciascuna sottorete dei gruppi multicast (multicast group membership → almeno un elemento del gruppo fa parte della sottorete) con un timer per membership
  - la membership deve essere aggiornata da report inviati prima della scadenza del timer
  - può essere anche aggiornata tramite messaggi di leave espliciti

# Problema dell'instradamento multicast

- Fra la popolazione complessiva di router solo alcuni (quelli collegati a host del gruppo multicast) dovranno ricevere traffico multicast

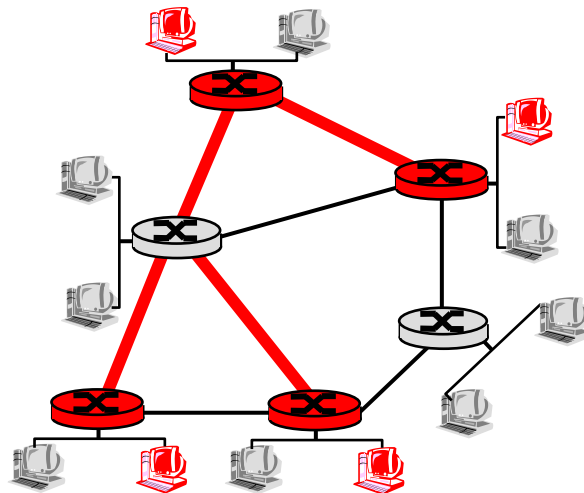


A,B,E,F sono router che devono ricevere traffico multicast

***Obiettivo:*** trovare un albero che colleghi tutti i router connessi ad host che appartengono al gruppo multicast. I pacchetti verranno instradati su questo albero

# Approcci per determinare albero d'instradamento multicast

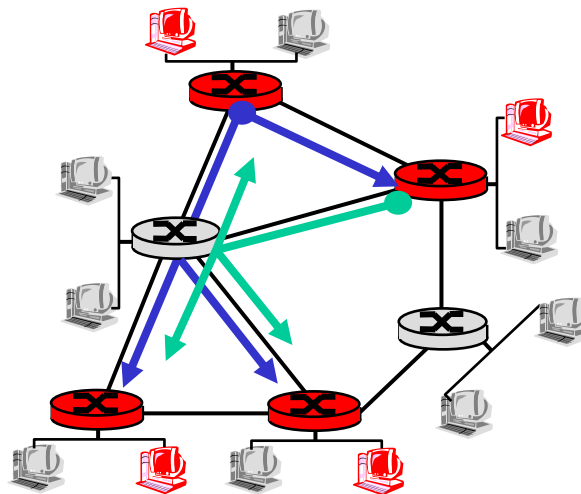
- Albero condiviso dal gruppo: viene costruito un singolo albero d'instradamento condiviso da tutto il gruppo multicast
  - Se il mittente del traffico multicast non è il centro, allora esso invierà il traffico in unicast al centro, e il centro provvederà a inviarlo al gruppo
  - Per la costruzione: Algoritmi di scelta del centro + messaggi unicast verso il centro come nel caso del broadcast



Albero condiviso dal gruppo

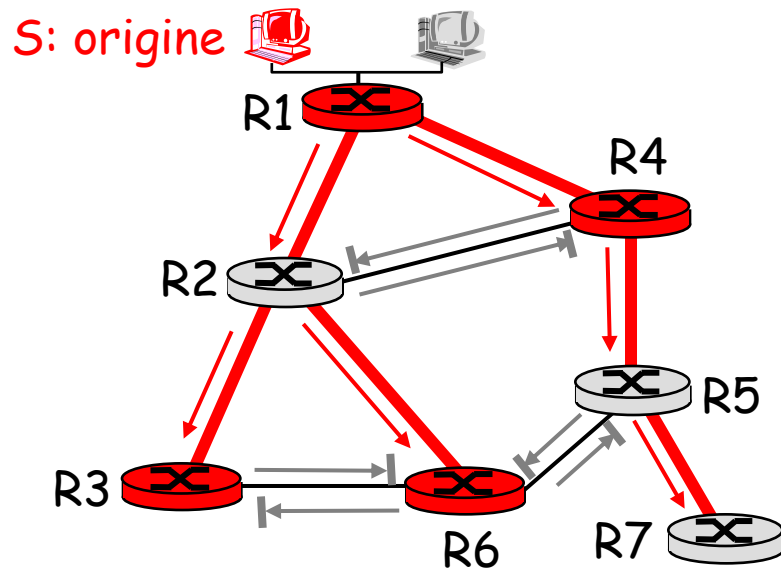
# Approcci per determinare albero d'instradamento multicast

- Albero basato sull'origine: viene creato un albero per ciascuna origine nel gruppo multicast
  - Ci sono tanti alberi quanti sono i mittenti del gruppo unicast
  - Per la costruzione si usa un algoritmo basato su inoltro su percorso inverso, con pruning (potatura)



Albero basato sull'origine

# Inoltro su percorso inverso (RPF): un esempio



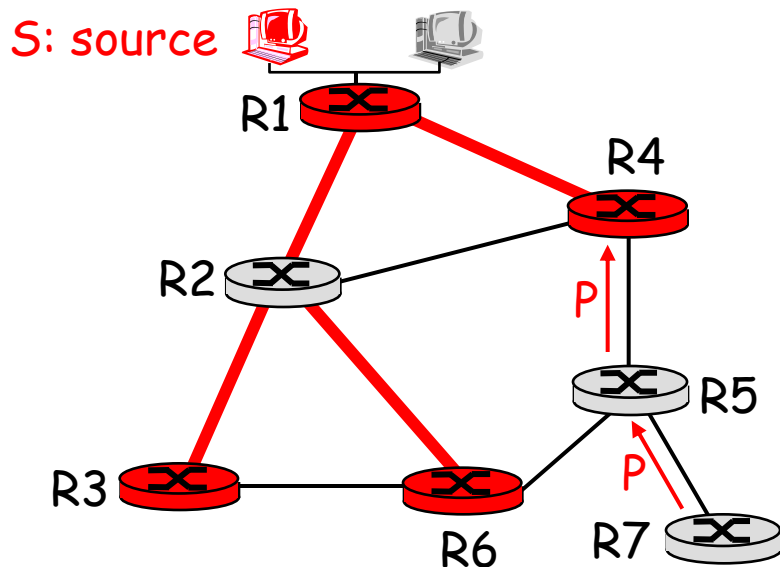
## LEGENDA

-  Router con membro di gruppo collegato
-  Router senza membri di gruppo collegati
-  Il pacchetto sarà inoltrato
-  Il pacchetto non sarà inoltrato oltre il router di ricezione

- Il risultato è un *reverse* SPT relativo all'origine

# Inoltro su percorso inverso: potatura

- È la soluzione per evitare di ricevere pacchetti multicast non desiderati.
  - Un router multicast che riceve pacchetti multicast e non è connesso a host aderenti al gruppo invierà un messaggio di potatura al proprio router di upstream.
  - Se un router riceve questi messaggi da tutti i suoi router di downstream (nell'albero creato), può inoltrare il messaggio di potatura in upstream.



## LEGENDA



Router con membro di gruppo collegato



Router senza membri di gruppo collegati



Messaggio di potatura



Collegamenti che ricevono pacchetti multicast

# Instradamento multicast in Internet

## **Intra-dominio multicast** (interno a un sistema autonomo)

- DVMRP: distance-vector multicast routing protocol
- MOSPF: multicast open shortest path first
- PIM: protocol independent multicast

## **Inter-dominio multicast** (tra sistemi autonomi)

- MBGP: multicast border gateway protocol

# Riassunto

- Introduzione
- Reti a circuito virtuale e a datagramma
- Che cosa si trova all'interno di un router?
- Protocollo Internet (IP)
  - Formato dei datagrammi
  - Indirizzamento IPv4
  - ICMP
  - IPv6
- Algoritmi di instradamento
  - Stato del collegamento
  - Vettore distanza
  - Instradamento gerarchico
- Instradamento in Internet
  - RIP
  - OSPF
  - BGP
- Instradamento broadcast e multicast



# Livello di collegamento e reti locali

## Obiettivi:

- ❑ Comprendere i principi per implementare i servizi di trasmissione dati:
  - Rilevazione e correzione dell'errore
  - Condivisione di un canale broadcast: accesso multiplo
  - Indirizzamento a livello di collegamento
  - Trasferimento affidabile dei dati, controllo del flusso: *già visto!*
- ❑ Istanziamento e implementazione delle varie tecnologie a livello di link.

# Livello di collegamento e reti locali

Livello di collegamento: introduzione e servizi

Tecniche di rilevazione e correzione degli errori

Protocolli di accesso multiplo

Indirizzi a livello di collegamento

Ethernet

Switch a livello di collegamento

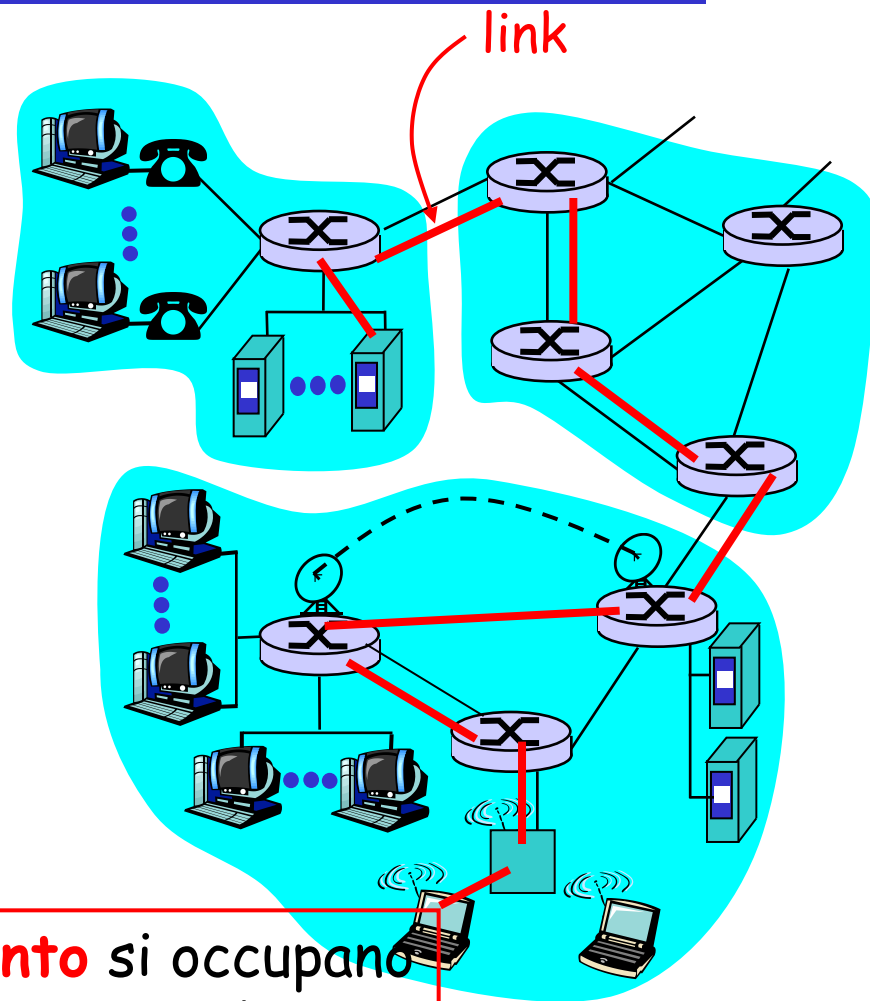
PPP: protocollo punto-punto

Canali virtuali: una rete come un livello di link

# Livello di collegamento: introduzione

## Alcuni termini utili:

- ❑ host e router sono i **nod**i
- ❑ 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**.



**I protocolli a livello di collegamento** si occupano del trasporto di datagrammi lungo un singolo canale di comunicazione.

# Livello di collegamento

- ❑ 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:

- ❑ Agente di viaggio = **protocollo di routing**
- ❑ Viaggio da Princeton a Losanna pianificato nel seguente modo:
  - taxi: da Princeton all'aeroporto JFK
  - aereo: dal JFK a Ginevra
  - treno: da Ginevra a Losanna
- ❑ Turista = **datagramma**
- ❑ Ciascuna tratta del trasporto = **collegamento**
- ❑ Tipologia del trasporto = **protocollo di link**

# 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"
  - ⑩ Diversi rispetto agli indirizzi IP!

## □ Consegna affidabile:

- Basata su ACK come nel trasporto
- 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 collegamento

## ❑ **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
  - ⑩ è possibile grazie all'inserimento, da parte del nodo trasmittente, di bit di controllo di errore all'interno del frame.

## ❑ **Correzione degli errori:**

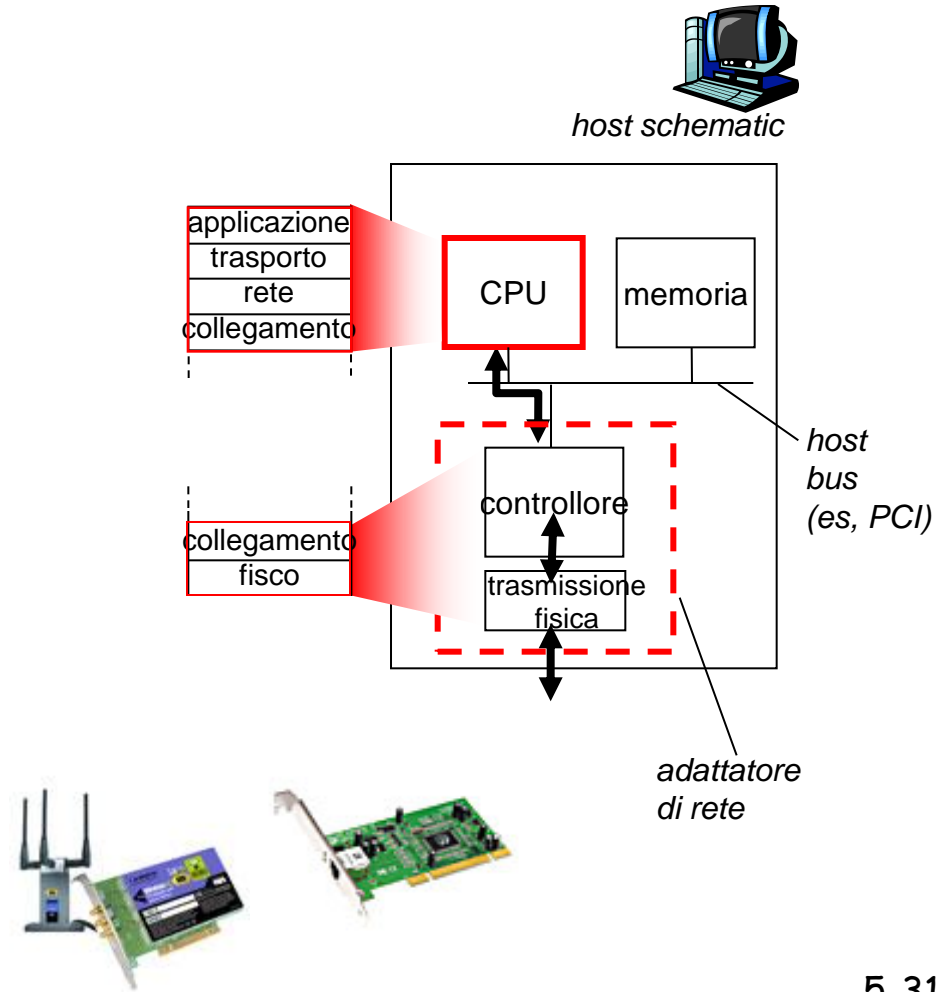
- Il nodo ricevente determina anche il punto in cui si è verificato l'errore, e lo corregge.

## ❑ **Half-duplex e full-duplex**

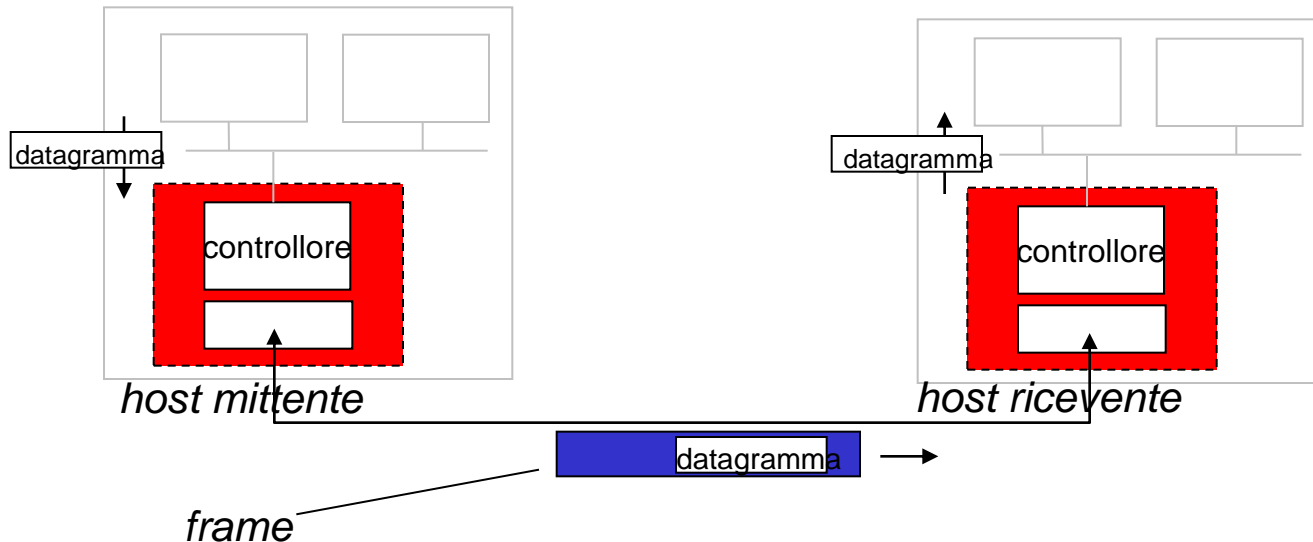
- Nella trasmissione full-duplex gli estremi di un collegamento possono trasmettere contemporaneamente: non in quella half-duplex.

# Dove è implementato il livello di collegamento?

- in tutti gli host
- È realizzato in un adattatore (NIC, *network interface card*)
  - scheda Ethernet, PCMCIA, 802.11
  - Implementa il livello di collegamento e fisico
- è una combinazione di hardware, software e firmware



# Adattatori



## □ Lato mittente:

- 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



# Livello di collegamento e reti locali

Livello di collegamento: introduzione e servizi

Tecniche di rilevazione e correzione degli errori

Protocolli di accesso multiplo

Indirizzi a livello di collegamento

Ethernet

Switch a livello di collegamento

PPP: protocollo punto-punto

Canali virtuali: una rete come un livello di link

# Tecniche di rilevazione degli errori

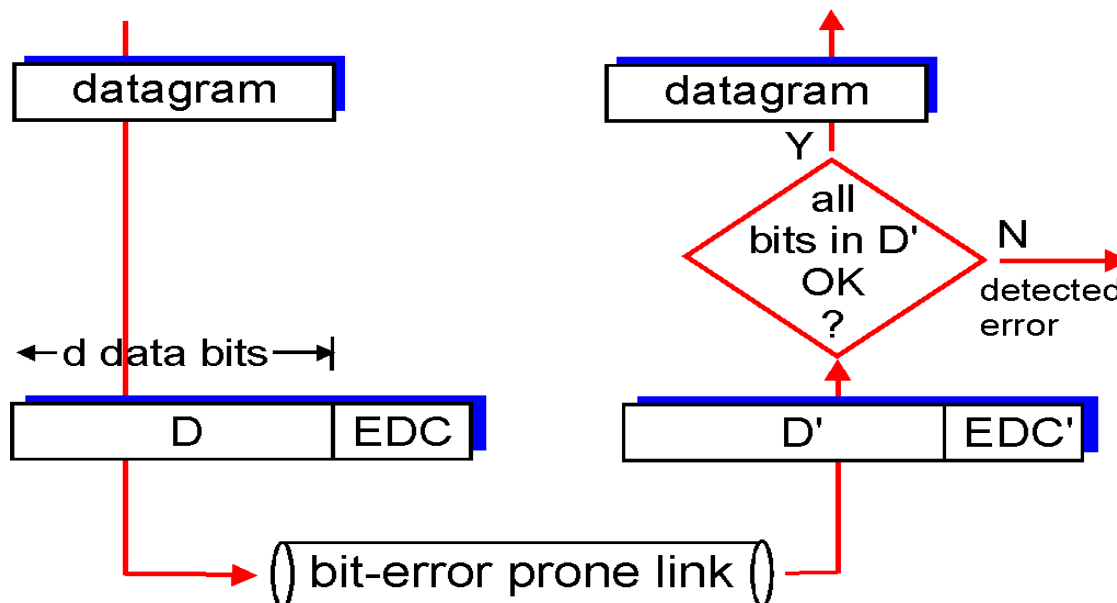
Gli errori sono dovuti a interferenze (che possono cambiare la forma del segnale)

EDC= *Error Detection and Correction*

D = Dati che devono essere protetti da errori e ai quali vengono aggiunti dei bit EDC.

La rilevazione degli errori non è attendibile al 100%!

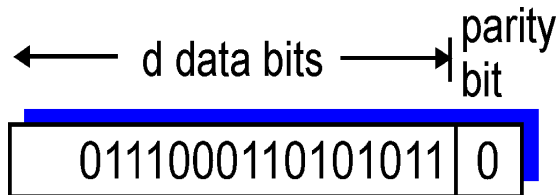
- è possibile che ci siano errori non rilevati
- per ridurre la probabilità di questo evento, le tecniche più sofisticate prevedono un'elevata **ridondanza**



# Controllo di parità

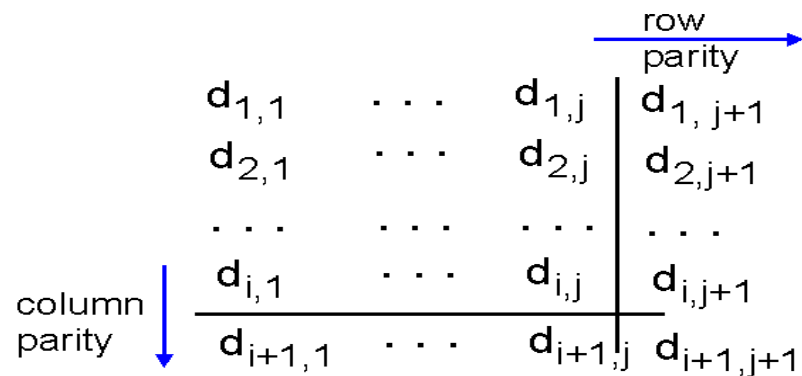
## Unico bit di parità:

Si è verificato almeno un errore in un bit



## Parità bidimensionale:

Individua e *corregge* il bit alterato



101011	1
111100	0
011101	1
001010	0

*no errors*

101011	1
<del>1</del> 1100	0
011101	1
001010	0

parity error

*correctable  
single bit error*

# Checksum di Internet

Obiettivi: rileva gli errori ma viene usata *solo* a livello di trasporto

## 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:

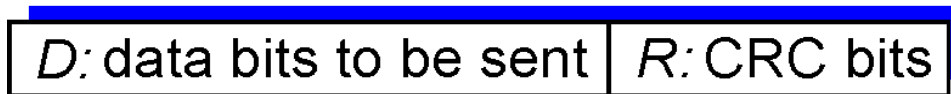
- ❑ Il ricevente controlla la checksum.
- ❑ Calcola il complemento a 1 della somma dei dati ricevuti e verifica che i bit del risultato siano 1:
  - **NO**, non lo sono: segnala un errore
  - **SÌ** lo sono: non sono stati rilevati errori.

*Ciononostante, ci potrebbero essere altri errori?*

Lo scopriremo in seguito ...

# Controllo a ridondanza ciclica

- Esamina i dati, **D**, come numeri binari.
- Origine e destinazione si sono accordati su una stringa di  $r+1$  bit, conosciuta come generatore, **G**.
- 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!



*bit  
pattern*

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

*mathematical  
formula*

*Vogliamo:*

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

*Quindi:*

se dividiamo  $D \cdot 2^r$  per  $G$ , otteniamo il valore  $R$ .

*Ovvero:*

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