Reti di Calcolatori
A.A. 2011-2014

Livello Data-Link

L. Vetrano

Capitolo 5

Livello di collegamento e reti locali

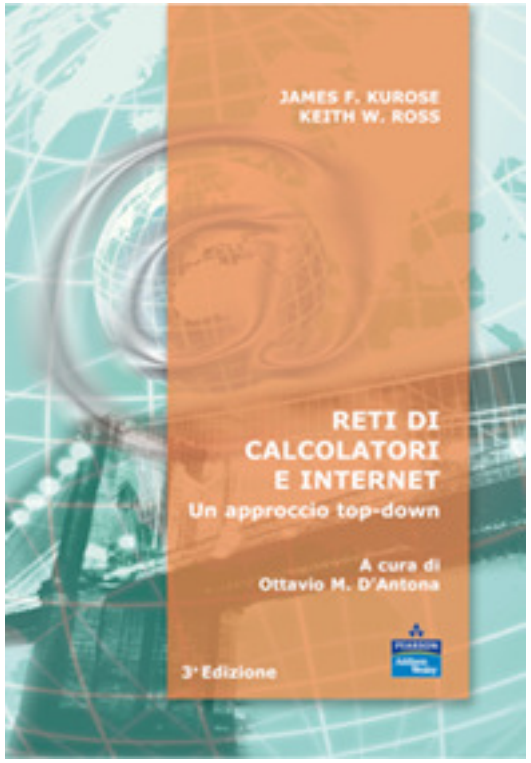
Nota per l'utilizzo:

Abbiamo preparato queste slide con l'intenzione di renderle disponibili a tutti (professori, studenti, lettori). Sono in formato PowerPoint in modo che voi possiate aggiungere e cancellare slide (compresa questa) o modificarne il contenuto in base alle vostre esigenze.
Come potete facilmente immaginare, da parte nostra abbiamo fatto *un sacco* di lavoro. In cambio, vi chiediamo solo di rispettare le seguenti condizioni:

- se utilizzate queste slide (ad esempio, in aula) in una forma sostanzialmente inalterata, fate riferimento alla fonte (dopo tutto, ci piacerebbe che la gente usasse il nostro libro!)
- se rendete disponibili queste slide in una forma sostanzialmente inalterata su un sito web, indicate che si tratta di un adattamento (o che sono identiche) delle nostre slide, e inserite la nota relativa al copyright.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2005
J.F Kurose and K.W. Ross, All Rights Reserved



Reti di calcolatori e Internet: Un approccio top-down

3ª edizione
Jim Kurose, Keith Ross
Pearson Education Italia ©2005

Livello di collegamento e reti locali

Obiettivi:

- Comprendere i principi dei servizi di trasmissione dati a livello data-link:
  - Rilevazione e correzione dell'errore
  - Condivisione di un canale broadcast: accesso multiplo
  - Indirizzamento a livello di link
  - Trasferimento affidabile dei dati
  - Controllo del flusso
- Implementazione delle varie tecnologie a livello di link.

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

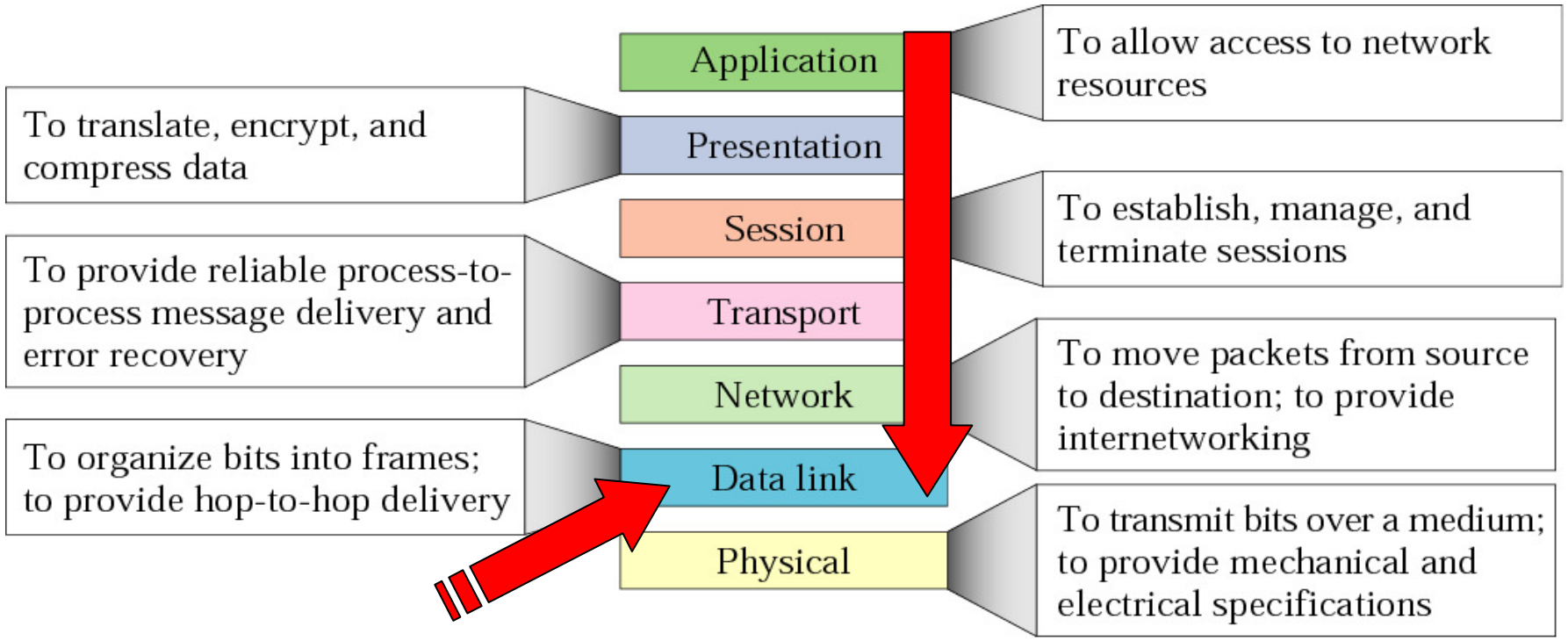
5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

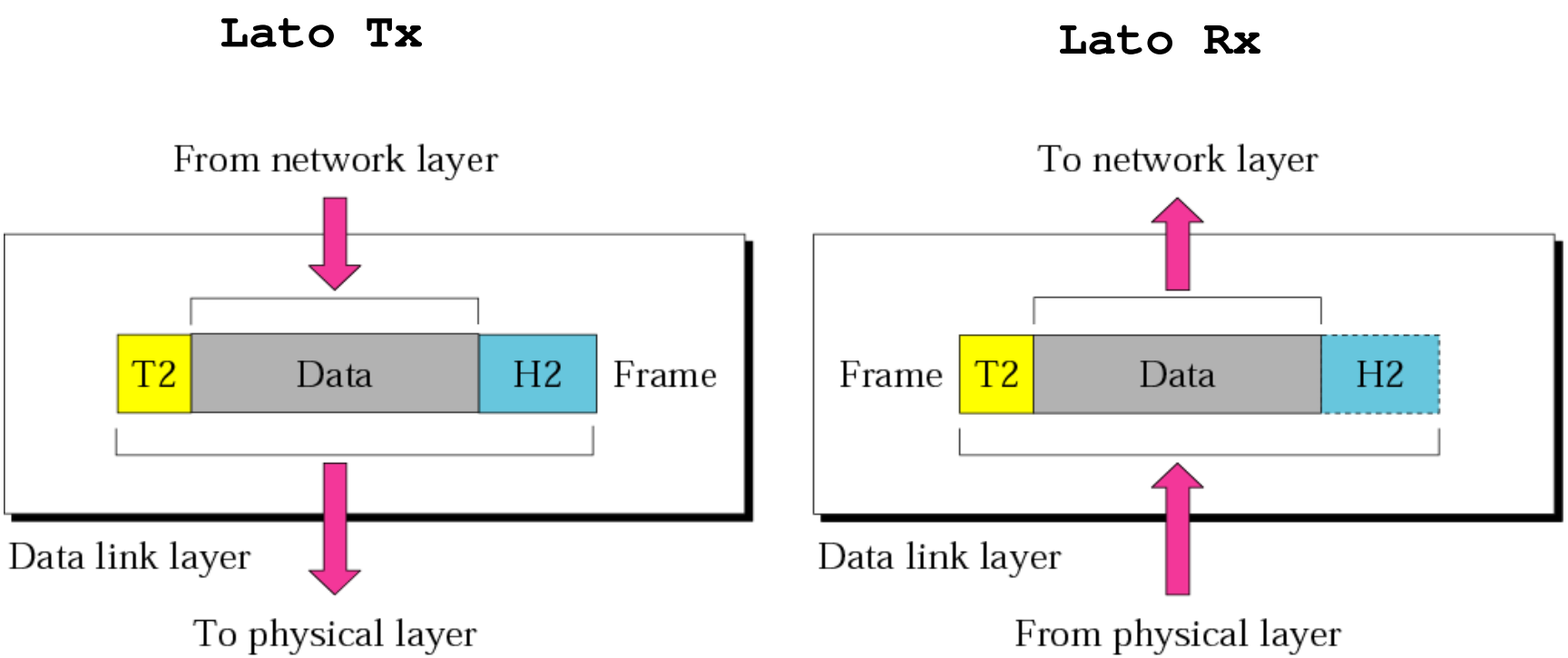
5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

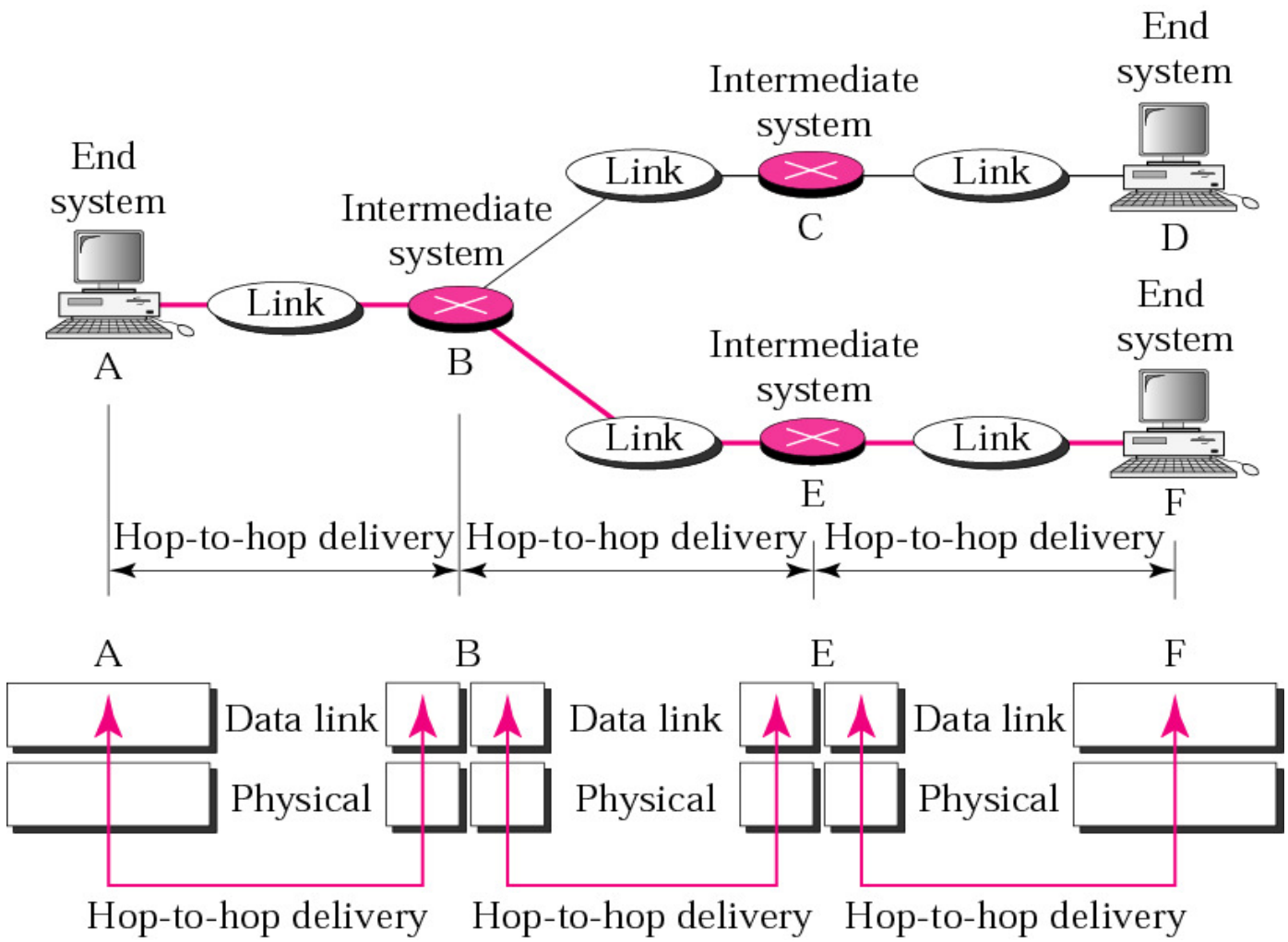
Sommario dei layers



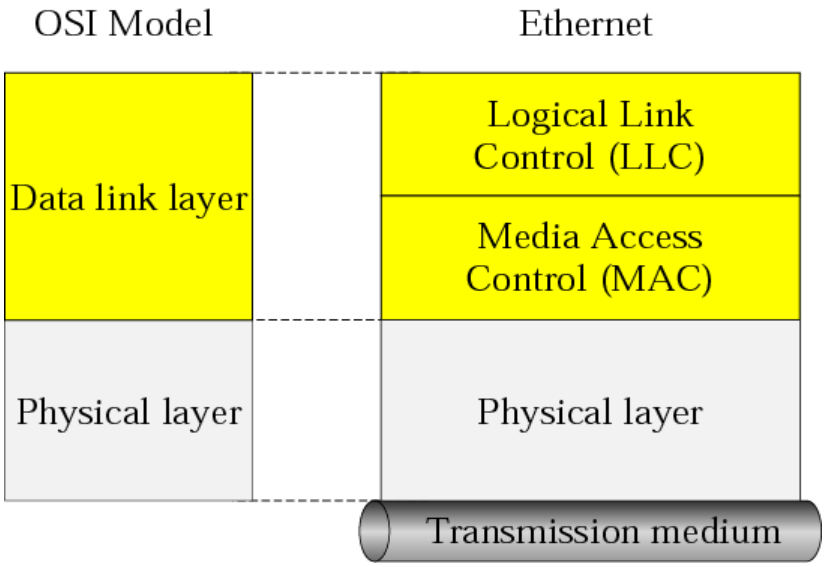
Data link layer



Hop-to-hop delivery



Dove siamo ?

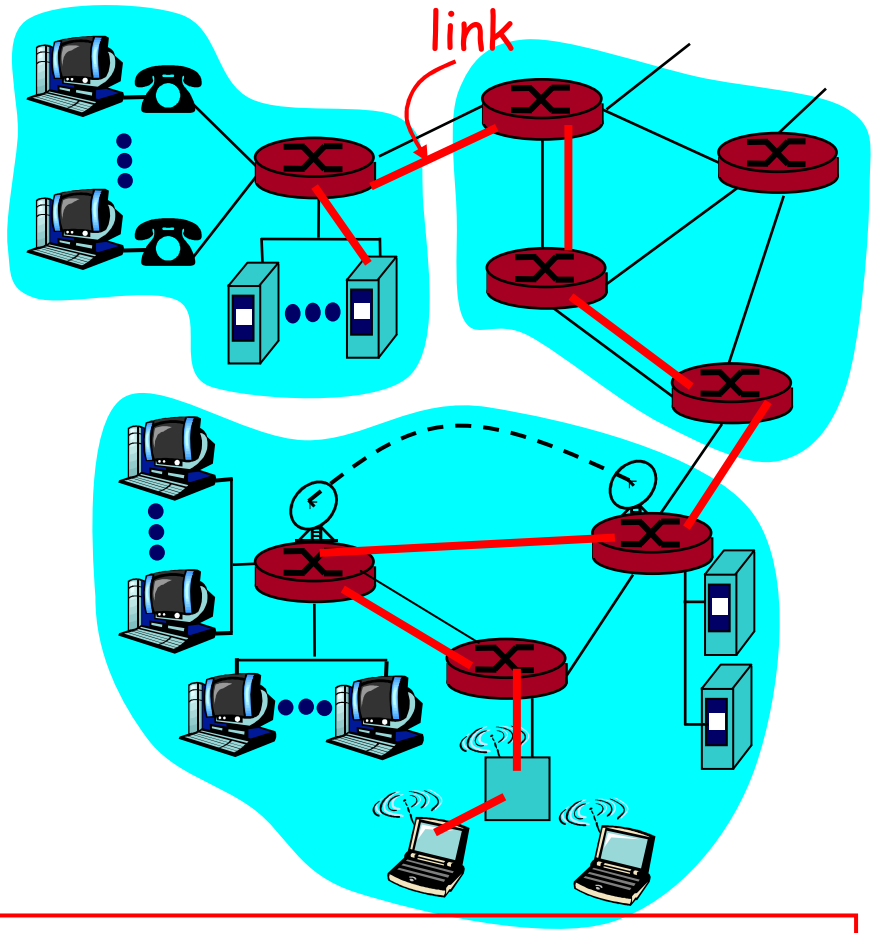


- LLC è comune a tutte le LAN ed è l'interfaccia verso il livello network.
  - I servizi e i protocolli di questo sottolivello sono descritti nello standard IEEE 802.2
- MAC è specifico per ogni LAN e risolve il problema della condivisione del mezzo trasmissivo.
  - Esistono vari tipi di MAC: ad allocazione di canale fissa o dinamica, deterministici o statistici, ecc.

Livello di link: introduzione

Alcuni termini utili:

- host e router sono i **nodi** (nel senso che per il DL layer sono indistinguibili)
- 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 link si occupano del trasporto di **frames** lungo un **singolo** canale di comunicazione.

Livello di link

- Un frame può essere gestito da diversi protocolli, su collegamenti differenti:
  - Es.: 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 L'Aquila a Losanna:
  - ARPA da L'Aquila a Roma Tiburtina
  - taxi: da Roma all'aeroporto Leonardo Da Vinci
  - aereo: dal LdV a Ginevra
  - treno: da Ginevra a Losanna
- Turista = frame
- Ciascuna tratta del trasporto = collegamento
- Tipologia del trasporto = protocollo di link
- Agente di viaggio = protocollo di routing

Protocolli a Livello di link

- Tra i protocolli a livello di link possiamo citare :
  - Ethernet
  - 802.11 Wireless LAN (Wi-Fi)
  - Token Ring
  - PPP
  - ATM*
  - Frame Relay
  - X.25
  - HDLC
  - FDDI

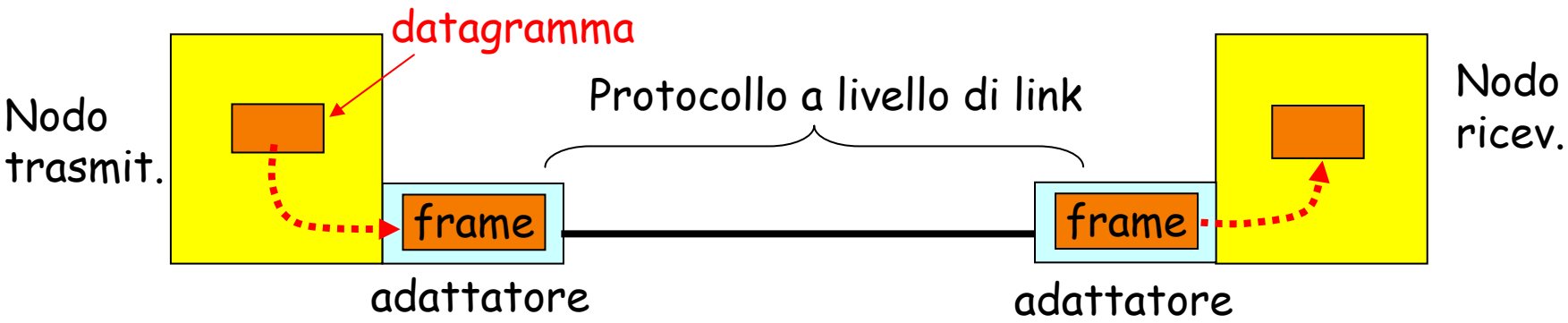
Servizi offerti dal livello di link

- Framing:
  - I protocolli incapsulano i datagrammi del livello di rete all'interno di un frame a livello di link.
- Accesso al collegamento: il protocollo MAC controlla l'accesso al mezzo
  - Per identificare origine e destinatario vengono utilizzati indirizzi "MAC" [00:01:02:03:04:05]
    - Diversi rispetto agli indirizzi IP ! [1.2.3.4]
- Consegna affidabile:
  - Come avviene ? lo abbiamo già imparato 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)
- Nota: la consegna affidabile in TCP è di tipo end-to-end, adesso stiamo parlando di una consegna affidabile hop-by-hop. Lo stesso vale per il controllo di flusso !!

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
    - è possibile grazie all'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 implementa il DL Layer ?



- 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 che lavora a livello di link e fisico.

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

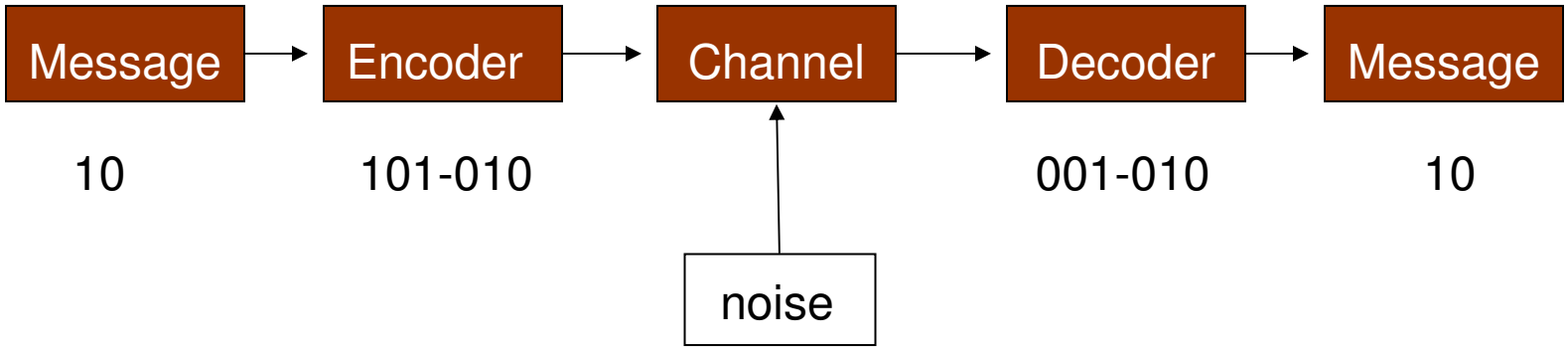
5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

Spedire un messaggio



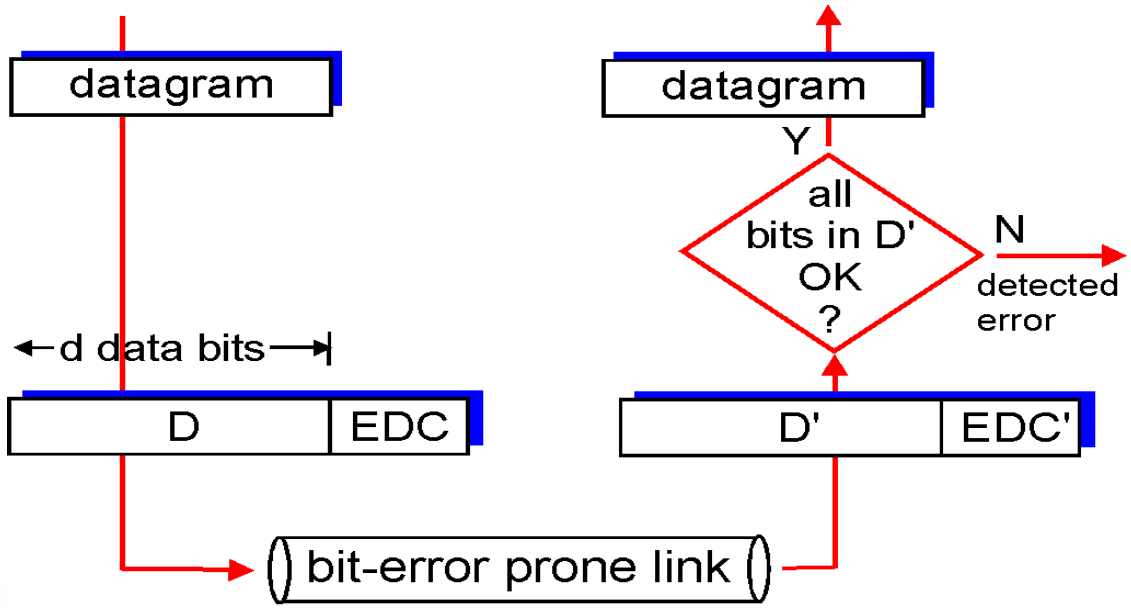
TechnoLabs

Tecniche di rilevazione degli errori

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



Tecniche di rilevazione degli errori

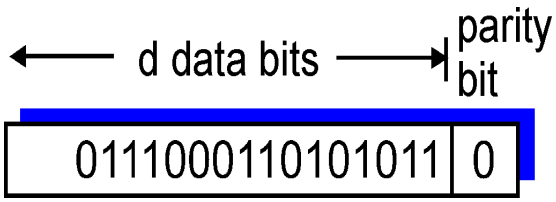
Tre tecniche per rilevare gli errori nei dati trasmessi:

1. Controllo di parità (parity check)
2. Controllo basato sulla Checksum
3. Controllo a Ridondanza Ciclica (CRC)

Controllo di parità

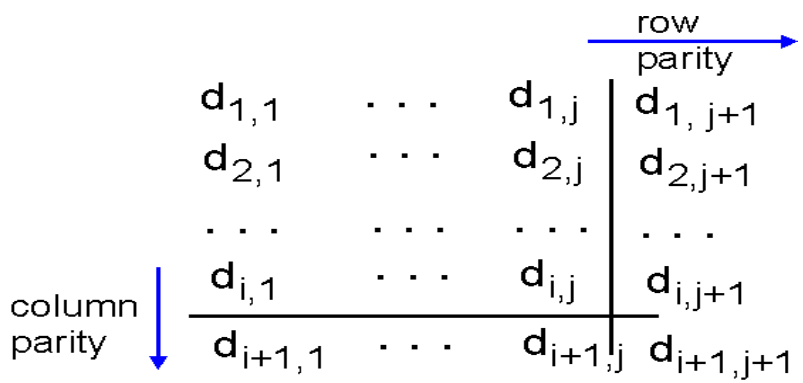
Unico bit di parità:

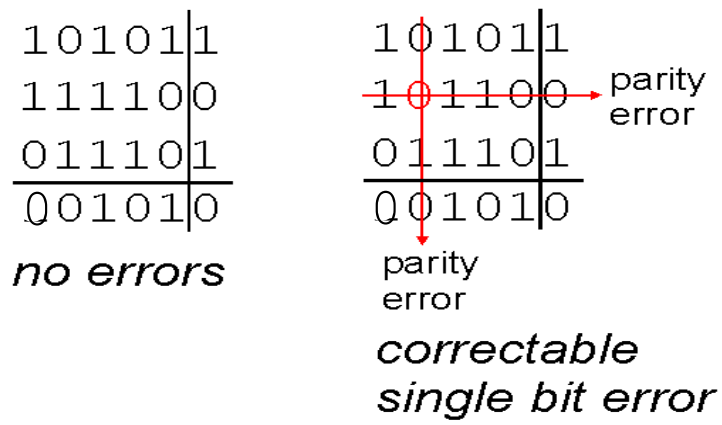
Si è verificato almeno un errore in un bit



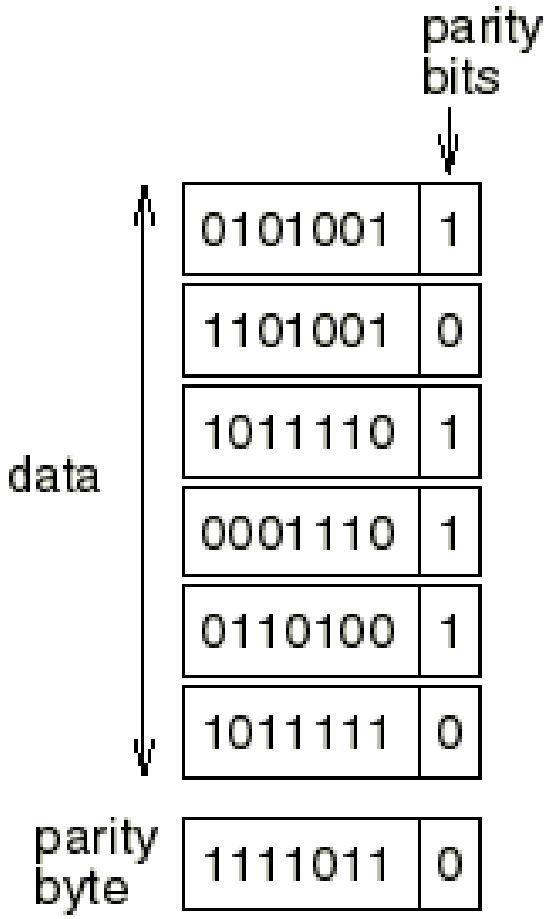
Parità bidimensionale:

Individua e *corregge* il bit alterato





Parità Bi-Dimensionale



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 ...

Checksum di Internet

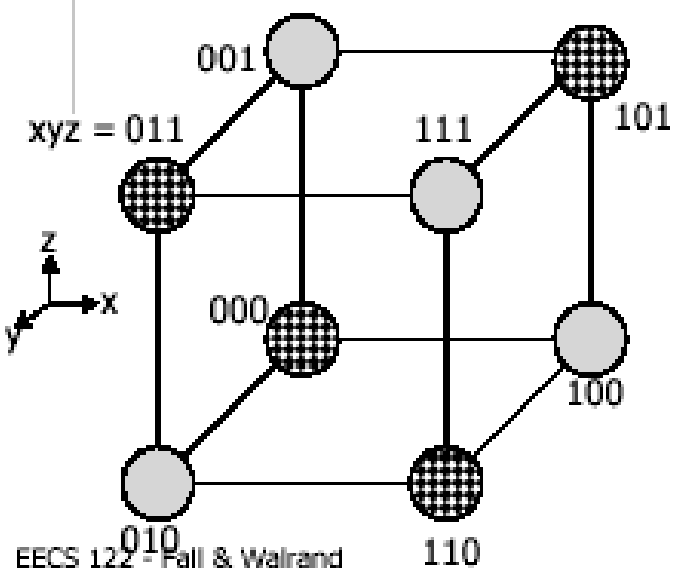
```
u_short cksum(u_short *buf, int count)
{
   register u_long sum = 0;

   while (count--)
   {
      sum += *buf++;
      if (sum & 0xFFFF0000)
      {
         /* carry occurred, so wrap around */
         sum &= 0xFFFF;
         sum++;
      }
   }
   return ~(sum & 0xFFFF);
}
```

Codici

Error Control Codes

How Codes Work: Words and Codewords

- Code = subset of possible words: Codewords
- Example:
  - 3 bits => 8 words; codewords: subset



Words:
000, 001, 010, 011
100, 101, 110, 111

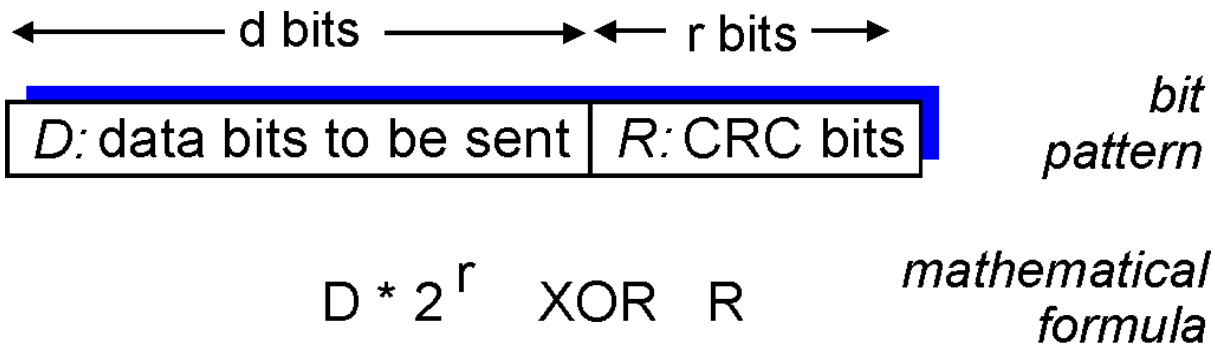
Code:
000, 011, 101, 110

Send only codewords

TechnoLabs

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:
  - <**D,R**> sia esattamente divisibile per **G** (modulo 2)
  - Il destinatario conosce **G**, e divide <**D,R**> 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).



Esempio di CRC

Vogliamo:

$D \cdot 2^r$ XOR R = nG

Ovvero:

$D \cdot 2^r$ = nG XOR R

Quindi:

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

$$R = \text{resto di } \left[\frac{D \cdot 2^r}{G} \right]$$

D=101110 G=1001 r=3

```
                101011
1001 ) 101110000
G      1001          D
        101
        000
         1010
         1001
          110
          000
           1100
           1001
            1010
            1001
             011
R
```

Esempio

- Tutti I messaggi leciti (legali) li scegliamo divisibili per 3
- Se vogliamo trasmettere il messaggio **10**
  - Prima moltiplichiamo per 4 e otteniamo **40**
  - Aggiungiamo 2 e lo rendiamo divisibile per 3 = **42**
  - Trasmettiamo **42**
- Quando il dato viene ricevuto ..
  - Dividiamo per 3, se non c'è resto non c'è errore
  - Se non c'è errore, si divide per 4 e si ottiene il messaggio trasmesso
- Se riceviamo 43, 44, 41, 40, rileviamo un errore
- Purtroppo la ricezione di 45 non sarà riconosciuta come un errore

Polinomi di uso comune:

CRC	$C(x)$
CRC-8	$x^8+x^2+x^1+1$
CRC-10	$x^{10}+x^9+x^5+x^4+x^1+1$
CRC-12	$x^{12}+x^{11}+x^3+x^2+x^1+1$
CRC-16	$x^{16}+x^{15}+x^2+1$
CRC-CCITT	$x^{16}+x^{12}+x^5+1$
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+$ $x^8+x^7+x^5+x^4+x^2+x+1$

TechnoLabs

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

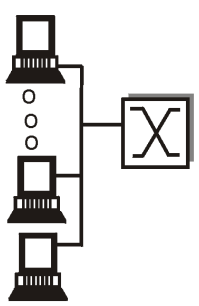
5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

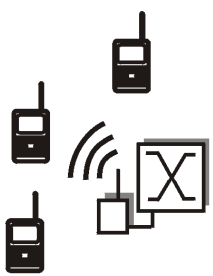
Protocolli di accesso multiplo

Esistono due tipi di collegamenti di rete:

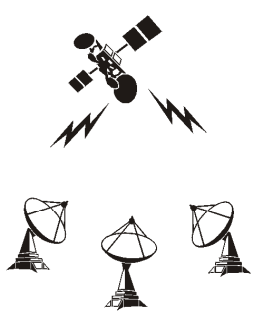
- Collegamento punto-punto (PPP)
  - Impiegato per connessioni telefoniche.
  - Collegamenti punto-punto tra Ethernet e host.
- Collegamento broadcast (cavo o canale condiviso)
  - Ethernet tradizionale
  - HFC in upstream
  - Wireless LAN 802.11



shared wire
(e.g. Ethernet)



shared wireless
(e.g. Wavelan)



satellite

cocktail party

Protocolli di accesso multiplo

Contesto di 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 frames contemporaneamente.

Protocolli di accesso multiplo

- Protocolli che fissano le modalità con cui i nodi regolano le loro trasmissioni sul canale condiviso.
- La segnalazione relativa al canale condiviso deve utilizzare lo stesso canale!
  - non c'è un canale "out-of-band" per la coordinazione

Desiderata da Protocolli di accesso multiplo

Canale broadcast con velocità di *R* bit al sec:

1. Quando un solo nodo deve inviare dati deve disporre di un tasso trasmissivo pari a *R* bps.
2. Quando *M* nodi devono inviare dati devono disporre di un tasso trasmissivo pari a *R/M* bps.
3. Il protocollo deve essere decentralizzato:
   - non ci sono nodi master
   - non c'è sincronizzazione dei clock
4. Il protocollo deve essere semplice.

Protocolli di accesso multiplo

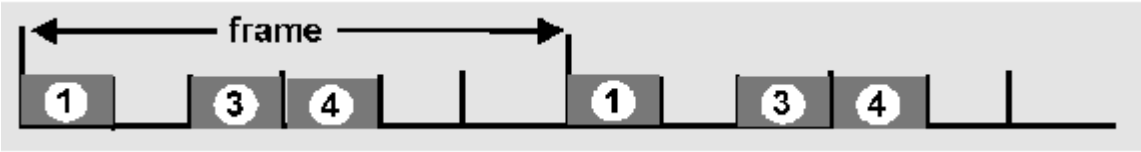
Si possono classificare in una di queste tre categorie:

- 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: accesso multiplo a divisione di tempo.

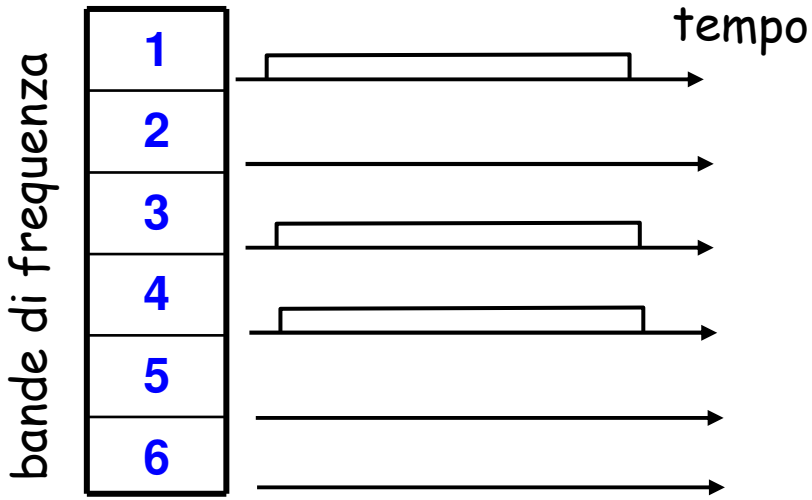
- Suddivide il canale condiviso in *intervalli di tempo.*
- Gli slot non usati rimangono inattivi
- Esempio: gli slot 1, 3 e 4 hanno un pacchetto, 2, 5 e 6 sono inattivi.



Protocolli a suddivisione del canale

FDMA: 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
- Due o più nodi trasmittenti ➜ "collisione"
- Il protocollo ad accesso casuale definisce:
  - Come rilevare un'eventuale collisione.
  - Come ritrasmettere se si è verificata una collisione.
- Esempi di protocolli ad accesso casuale:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

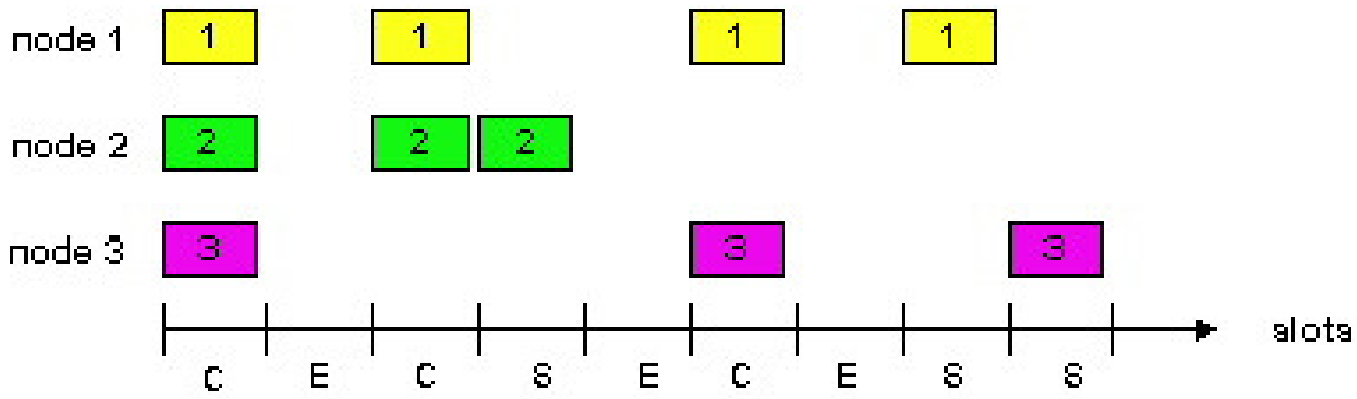
Assumiamo che:

- 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.

Operazioni:

- 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



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.

L'efficienza di Slotted Aloha

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 di pacchetti da spedire.

- Supponiamo N nodi con pacchetti da spedire, ognuno trasmette i pacchetti in uno slot con probabilità *p*.
- La probabilità di successo di un dato nodo = $p(1-p)^{N-1}$
- La probabilità che un nodo arbitrario abbia successo

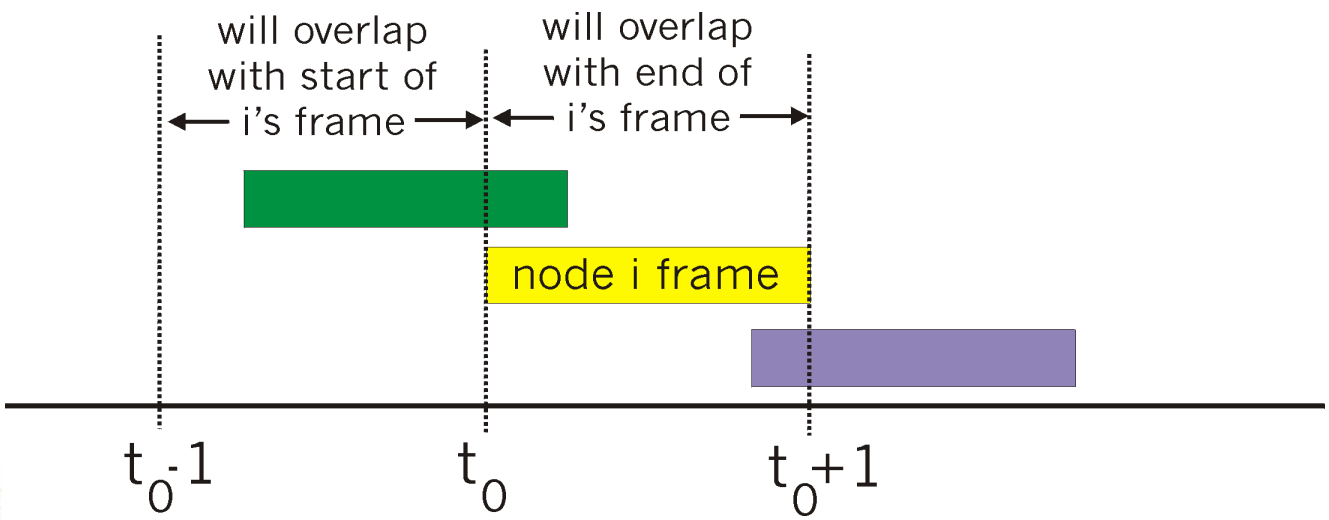
  = $Np(1-p)^{N-1}$

- Per ottenere la massima efficienza con N nodi attivi, bisogna trovare il 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: più semplice, non sincronizzato.
- Quando arriva il primo pacchetto:
  - lo trasmette immediatamente e integralmente nel canale broadcast.
- Elevate probabilità di collisione:
  - Il pacchetto trasmesso a t_0 si sovrappone con la trasmissione dell'altro pacchetto inviato in $[t_0-1,t_0+1]$.



L'efficienza di Aloha puro

P(trasmissione con successo da un dato nodo) =

P(il nodo trasmette)·

P(nessun altro nodo trasmette in $[t_0-1,t_0]$ ·

P(nessun altro nodo trasmette in $[t_0,t_0+1]$

$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$

$= p \cdot (1-p)^{2(N-1)}$

… scegliendo p migliore e lasciando N → infinito …

= 1/(2e) = 0,18

Peggio di prima !

Aloha puro

- In generale il protocollo avrà una buona probabilità di riuscita quando il traffico è molto basso (poche stazioni, e trasmissioni rarefatte)
- In caso di alti carichi, le collisioni cresceranno, e con esse le ritrasmissioni, fino a rendere la trasmissione di fatto impossibile
- Il calcolo della capacita' di trasporto (S) del canale in funzione del numero di tentativi di trasmissione per tempo di frame (G) e'

$$S = Ge^{-2G}$$

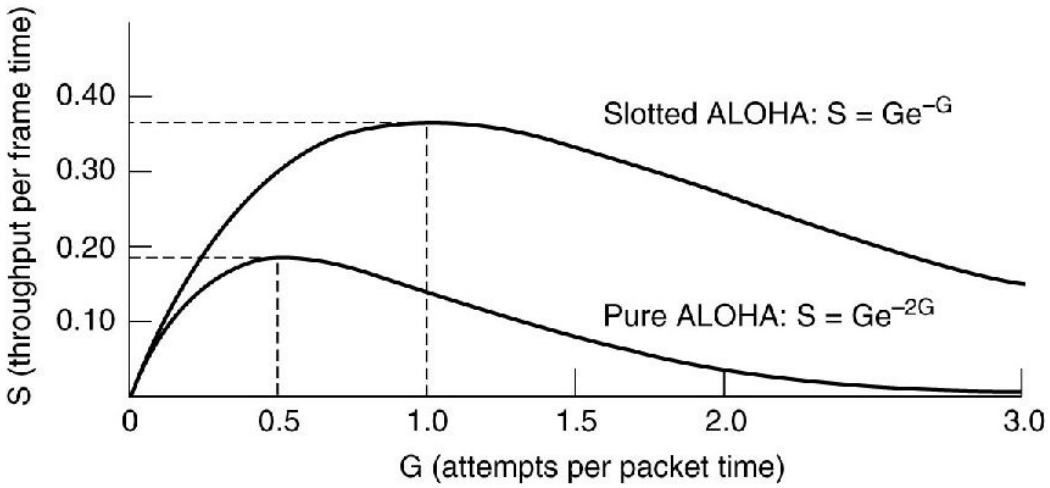
- Il protocollo ha quindi una efficienza massima quando per ogni tempo di frame ci sono G = 0.5 tentativi di trasmissione; in questa condizione l'efficienza di utilizzo del canale e' pari circa al 18%

Aloha a slot temporali

- L'efficienza dell'utilizzo del canale con questo protocollo e' data da

$$S = Ge^{-G}$$

e per G = 1 raggiunge il suo valore massimo (37%) che e' doppio rispetto ad aloha puro



Protocolli con rilevamento della portante

- Una delle maggiori inefficienze dei protocolli aloha è determinata dal fatto che la trasmissione viene fatta senza controllare prima se il canale è libero
- Vediamo ora una classe di protocolli che migliora la situazione: protocolli con rilevamento della portante (CSMA: Carrier Sense Multiple Access)
  - in questo contesto il termine portante indica in generale il livello del segnale presente sul mezzo trasmissivo
  - il segnale non è necessariamente un segnale costituito dalla modulazione di una portante, ma anche, ad esempio, un segnale in banda base

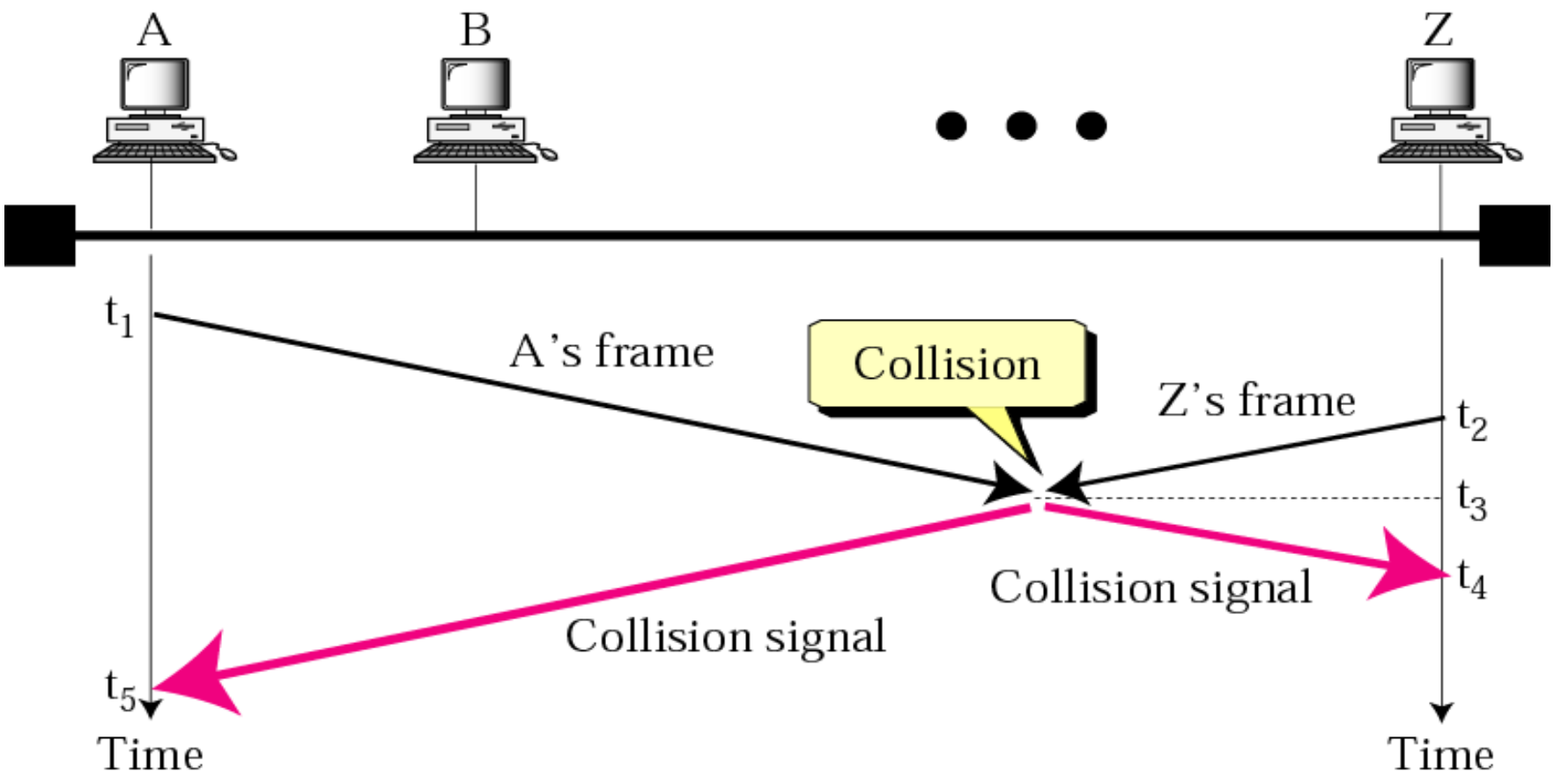
Accesso multiplo a rilevazione della portante

CSMA: si pone in ascolto prima di trasmettere

- Se rileva che il canale è libero, trasmette l'intero pacchetto.
- Se il canale sta già trasmettendo, il nodo aspetta un altro intervallo di tempo.

- Analogia: se qualcun altro sta parlando, aspettate finché abbia concluso!

Collisione


A
B
Z
t1
A's frame
Collision
Z's frame
t2
t3
t4
Collision signal
Collision signal
t5
Time
Time

CSMA con trasmissioni in collisione

Le collisioni *possono* ancora verificarsi:

Il ritardo di propagazione fa sì che due nodi non rilevino la reciproca trasmissione

collisione:

Quando un nodo rileva una collisione, cessa immediatamente la trasmissione.

nota:

La distanza e il ritardo di propagazione giocano un ruolo importante nel determinare la probabilità di collisione.

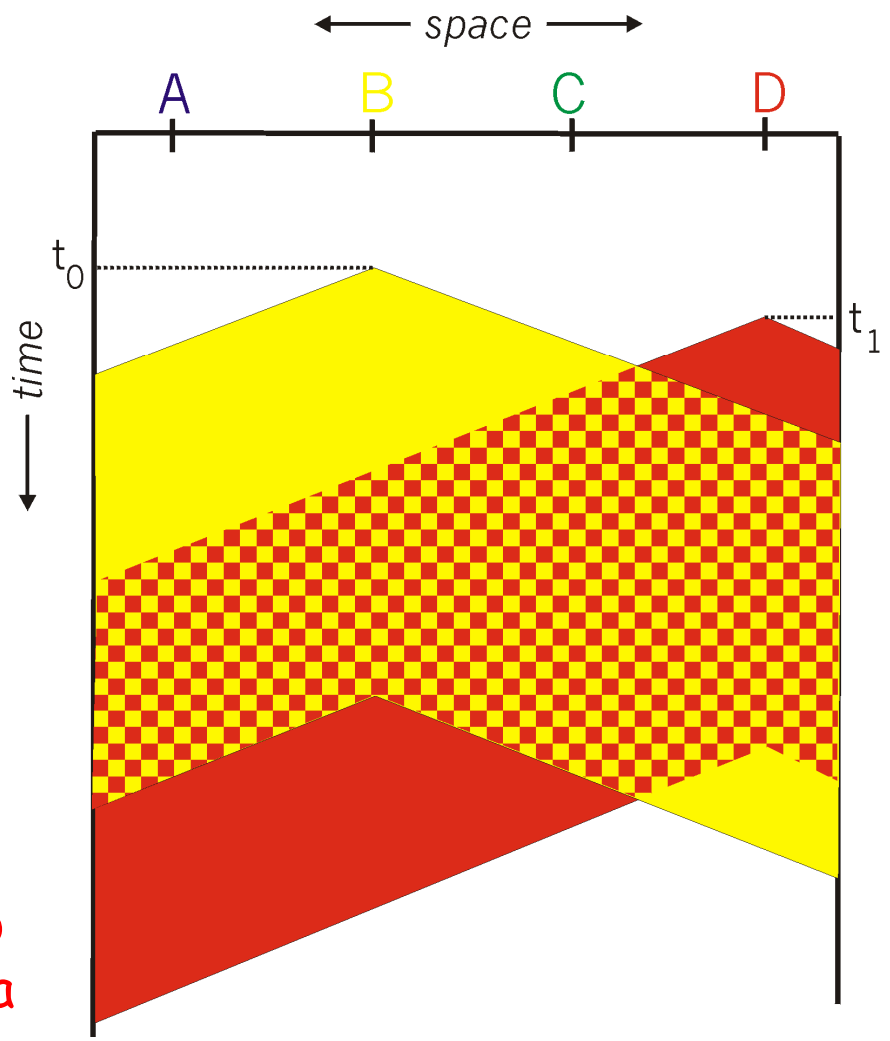


Diagramma spazio tempo

TechnoLabs

CSMA/CD (rilevazione di collisione)

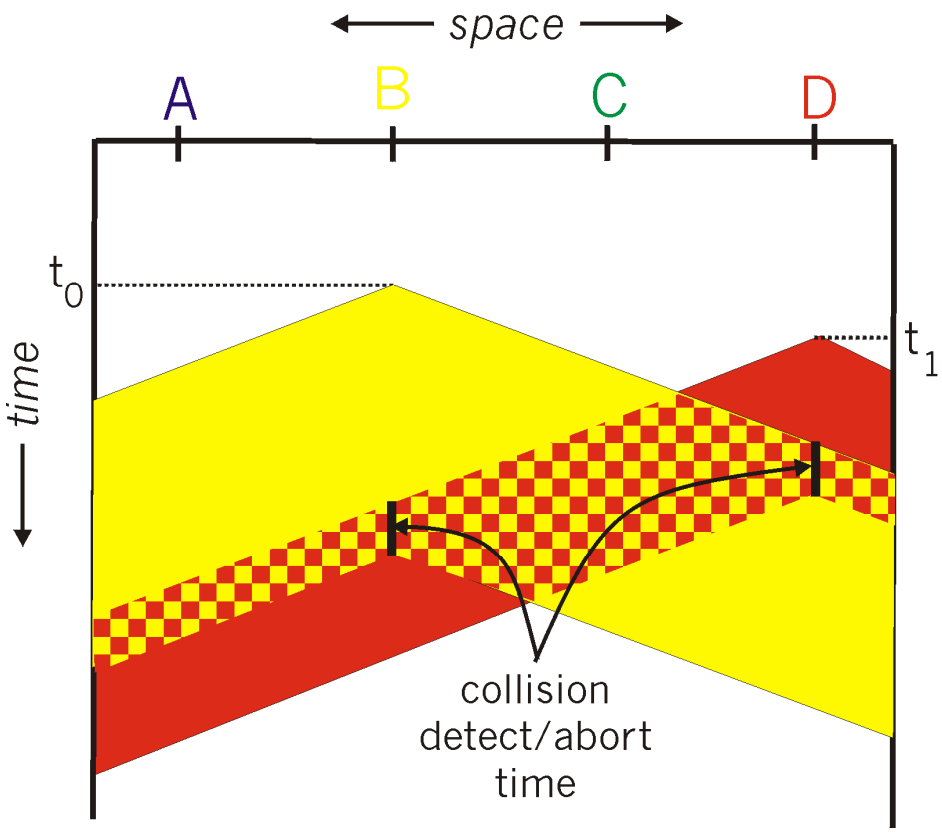
CSMA/CD: rilevamento della portante differito, come in CSMA:

- Rileva la collisione in poco tempo.
- Annulla la trasmissione non appena si accorge che c'è un'altra trasmissione in corso.

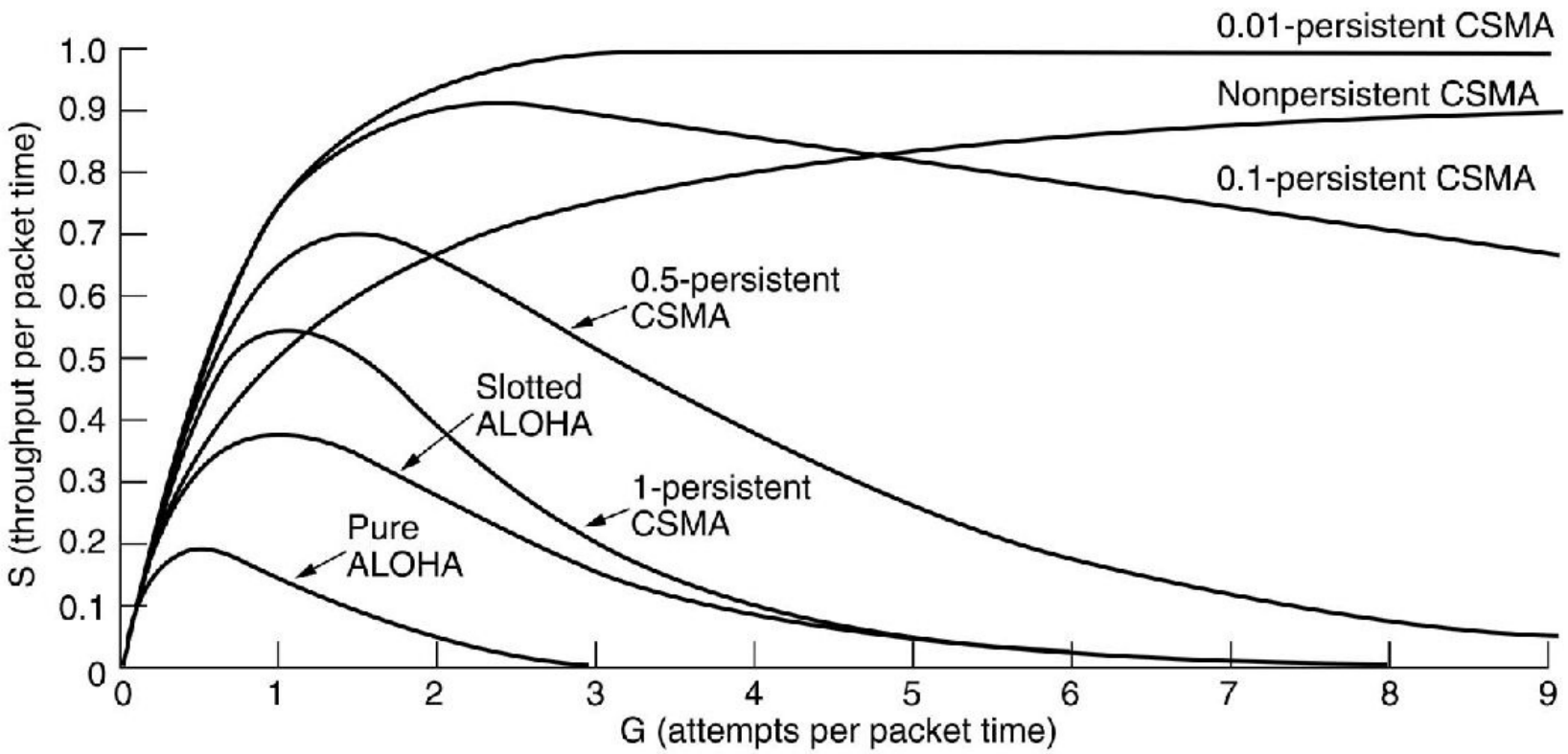
- Rilevazione della collisione:
  - facile nelle LAN cablate.
  - difficile nelle LAN wireless.

- Analogia: un interlocutore educato.

CSMA/CD (rilevazione di collisione)



Confronto tra protocolli CSMA



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!

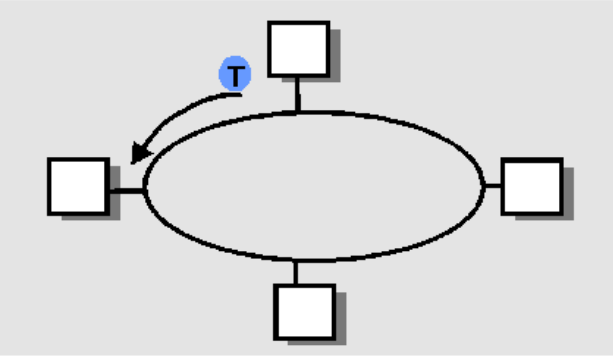
Protocolli a rotazione

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



Protocollo round robin: token ring

- Token ring (standard IEEE 802.5)
  - questo protocollo prevede l'utilizzo di una topologia ad anello
  - sull'anello circola un piccolo frame, detto token (gettone) che le stazioni ricevono da una parte e ritrasmettono dall'altra in continuazione
  - una stazione e' autorizzata a trasmettere dati solo quando e' in possesso del token
    - la stazione riceve il token, lo trattiene ed inizia a trasmettere dati
    - terminata la trasmissione, ritrasmette il token in coda ai frame di dati
  - esistono specifiche a 4 e 16 Mbps
- Esiste una versione modificata del token ring standardizzata per trasmissione su doppio anello in fibra ottica, detto FDDI (Fiber Distributed Data Interface) a 100 Mbps
- L'IEEE ha sviluppato uno standard molto simile, dedicato alle topologie a bus (token bus: IEEE 802.4)
  - in questo protocollo il problema aggiuntivo è determinato dalla necessita' di configurare un ordine sequenziale delle stazioni, che viene fatto in una fase di inizializzazione del protocollo

Protocollo round robin: token ring

- Il protocollo token ring (come tutti quelli a turno) è poco efficiente in condizioni di basso carico
  - la stazione che deve trasmettere deve attendere di ricevere il token (o in generale deve attendere il suo turno) prima di poterlo fare, anche se il canale non è occupato
- In condizioni di carico elevato, quando tutti vogliono trasmettere, l'efficienza del protocollo sfiora il 100%
  - il solo overhead è dovuto alla necessita' che ha una stazione di identificare il token prima di poter trasmettere
  - in questi protocolli il token è scelto in modo opportuno per minimizzare l'overhead
- Una importante caratteristica di questo genere di protocolli e' la possibilita' di valutare un tempo massimo di ritardo per le trasmissioni
  - una stazione che desidera trasmettere dovra' attendere al piu' N tempi di trasmissione (uno per stazione, nel caso tutti debbano trasmettere) prima che tocchi nuovamente ad essa
  - questo permette l'utilizzo del protocollo in situazioni in cui i tempi di risposta possono essere determinanti (ad esempio una catena di montaggio)

Protocolli: riepilogo

- Cosa si può fare con un canale condiviso?
  - Suddivisione del canale per: tempo, frequenza, codice.
    - TDM, FDM, CDMA.
  - 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

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

5.7 PPP: protocollo punto-punto

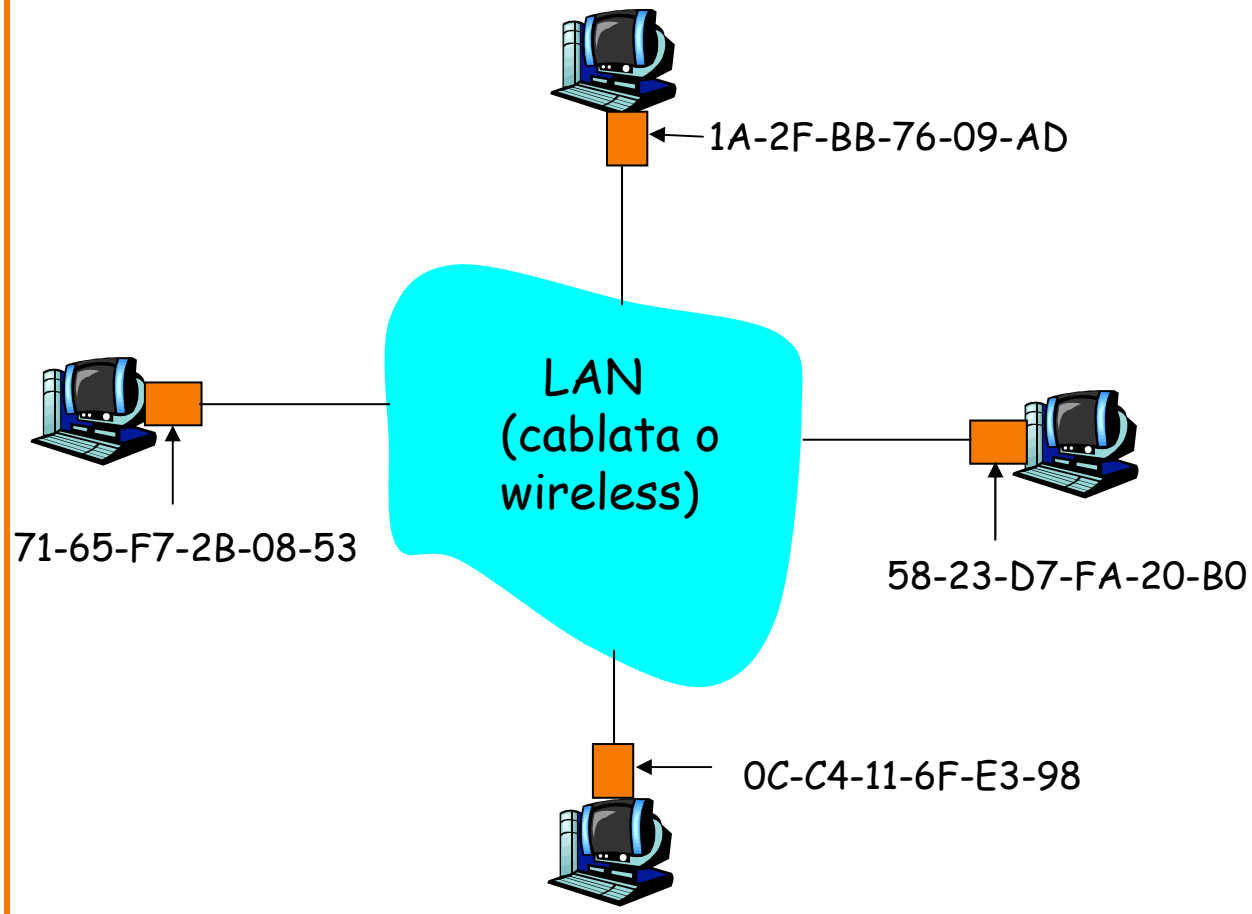
5.8 Canali virtuali: una rete come un livello di link

Indirizzi MAC

- Indirizzo IP a 32 bit:
  - Indirizzo a *livello di rete.*
  - Analogo all'indirizzo postale di una persona: hanno una struttura gerarchica e devono esser aggiornati quando una persona cambia residenza.
- Indirizzo MAC (o LAN o fisico o Ethernet):
  - Analogo al numero di codice fiscale di una persona: ha una struttura orizzontale e non varia a seconda del luogo in cui la persona si trasferisce.
  - Indirizzo a 48 bit (per la maggior parte delle LAN) .

Indirizzi MAC (LAN)

Ciascun adattatore di una LAN ha un indirizzo MAC (LAN) univoco .



Indirizzo broadcast =
FF-FF-FF-FF-FF-FF

= adattatore

Indirizzi MAC

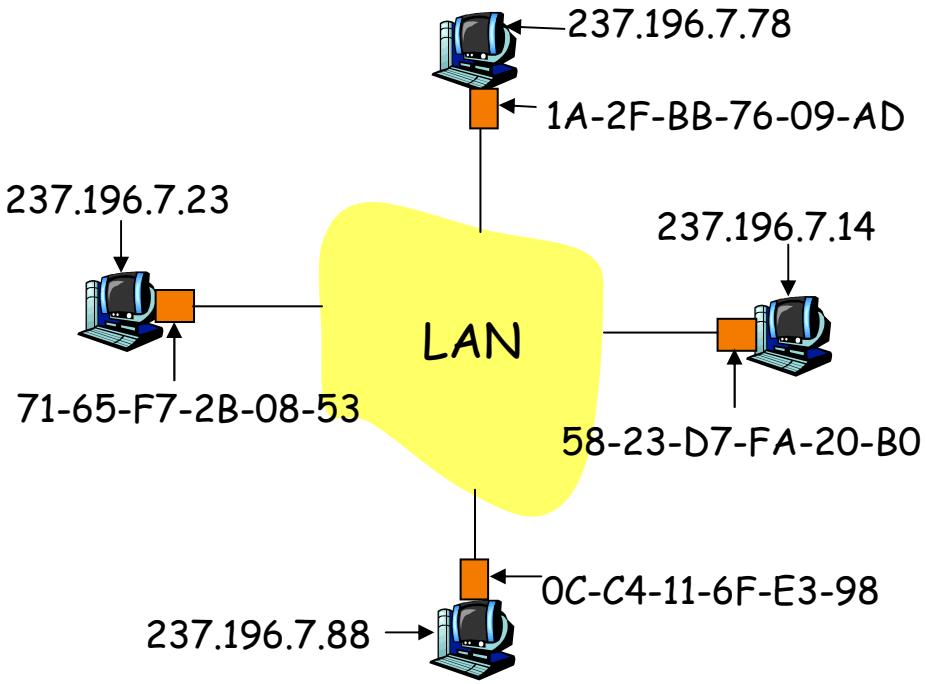
- La IEEE sovrintende alla gestione degli indirizzi MAC.
- Quando una società vuole costruire adattatori, compra un blocco di spazio di indirizzi (unicità degli indirizzi).
- Analogia:

  (a) Indirizzo MAC: analogo al codice fiscale di una persona.

  (b) Indirizzo IP: analogo all'indirizzo postale di una persona.
- Indirizzo orizzontale MAC ➜ portabilità
  - È possibile spostare una scheda LAN da una LAN ad un'altra.
- Gli indirizzi IP hanno una struttura gerarchica e devono essere aggiornati se spostati.
  - dipendono dalla sottorete IP cui il nodo è collegato.

Protocollo per la risoluzione degli indirizzi (ARP)

Domanda: come si determina l'indirizzo MAC di B se si conosce solo l'indirizzo IP di B?



- Ogni nodo IP (host, router) nella LAN ha una tabella ARP.
- Tabella ARP: contiene la corrispondenza tra indirizzi IP e MAC.

<Indirizzo IP; Indirizzo MAC; TTL>

– TTL (tempo di vita): valore che indica quando bisognerà eliminare una data voce nella tabella (il tempo di vita tipico è di 20 min).

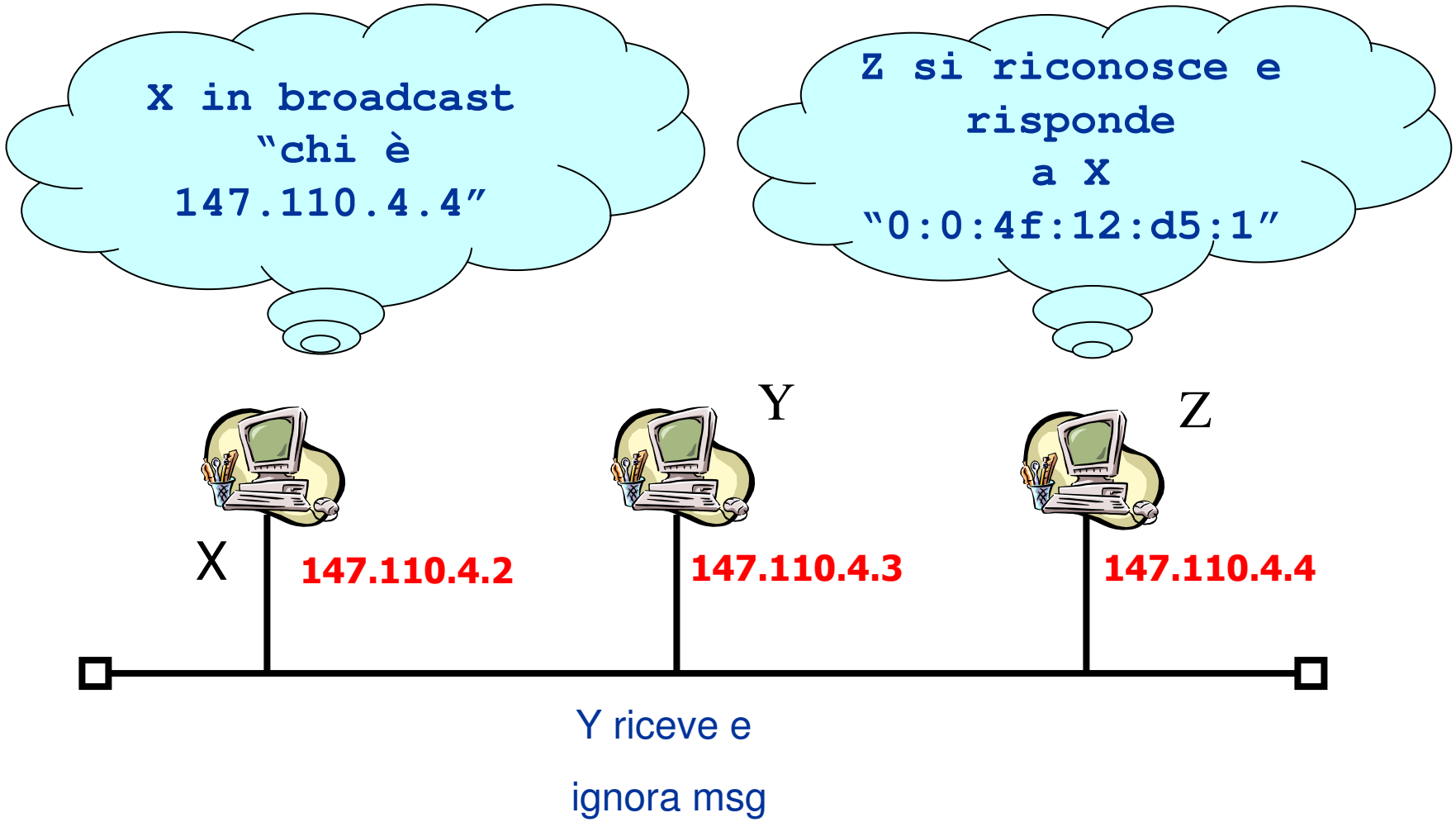
Tabella ARP

```
C:\Luigi> arp -a
  Interface: 192.168.35.222 --- 0x3
  Internet Address      Physical Address      Type
  192.168.35.2          00-0a-b7-78-ad-00     dynamic
  192.168.35.12         00-30-05-ae-f0-ce     dynamic
  192.168.35.27         00-30-05-21-16-29     dynamic
  192.168.35.31         00-30-05-7a-c9-78     dynamic
C:\Luigi> ping 192.168.35.56
  Pinging 192.168.35.56 with 32 bytes of data:
  Reply from 192.168.35.56: bytes=32 time<1ms TTL=128
  ^C
C:\Luigi> arp -a
  Interface: 192.168.35.222 --- 0x3
  Internet Address      Physical Address      Type
  192.168.35.2          00-0a-b7-78-ad-00     dynamic
  192.168.35.12         00-30-05-ae-f0-ce     dynamic
  192.168.35.27         00-30-05-21-16-29     dynamic
  192.168.35.31         00-30-05-7a-c9-78     dynamic
  192.168.35.56         00-30-05-84-9d-7d     dynamic
```

Protocollo ARP nella stessa sottorete

- *A* vuole inviare un datagramma a *B*, e l'indirizzo MAC di *B* non è nella tabella ARP di *A.*
- A trasmette in un pacchetto broadcast il messaggio di richiesta ARP, contenente l'indirizzo IP di B.
  - Indirizzo MAC del destinatario = FF-FF-FF-FF-FF-FF
  - Tutte le macchine della LAN ricevono una richiesta ARP.
- *B* riceve il pacchetto ARP, e risponde ad *A* comunicandogli il proprio indirizzo MAC.
  - il frame viene inviato all'indirizzo MAC di A.
- Il messaggio di richiesta ARP è inviato in un pacchetto broadcast mentre il messaggio di risposta ARP è inviato in un pacchetto unicast.
- ARP è "plug-and-play":
  - La tabella ARP di un nodo si costituisce automaticamente e non deve essere configurata dall'amministratore del sistema.

ARP in funzione



ARP datagram (caso Ethernet)

Frame hdr	ARP/RARP Message	CRC

Hardware type		Protocol type
Hw len	Prot len	ARP Operation
Sender MAC address (byte 0-3)		
Sender MAC add(byte 4-5)		Sender IP add (byte 0-1)
Sender IP add (byte 2-3)		Dest MAC add (byte 0-1)
Destination MAC address (byte 2-5)		
Destination IP address (byte 0-3)		

Esempio di Header (caso Ethernet)

- Nell'header del frame ethernet il campo "type" è ARP (=0x806)
- Nel messaggio ARP il campo "hardware type" è Ethernet (= 1)
- Protocol type IP = 0x800
- Hw len Ethernet = 6 byte
- Prot len IP = 4 byte
- ARP Operation
  - ARP req = 1, ARP reply = 2
  - RARP req = 3, RARP reply = 4

Come funziona ARP

- X spedisce msg in broadcast
- Ciascuna macchina
  - Esamina campo “operazione”
  - Se (op=risposta) ok
  - Se (op=richiesta)
    - Se (IND PROT DEST == proprio indirizzo prot.)
      - Inverte ind. Fisico e di protocollo mittente con dest.
      - Inserisce proprio indirizzo MAC nel campo mittente
      - Imposta tipo operazione = risposta
      - Estrae ind. MAC mittente e lo memorizza in cache

ARP - continua

- **Ottimizzazioni**
  - Utilizzo cache
  - Destinatario memorizza MAC mittente

Reverse ARP - RARP

- Mappa indirizzo MAC in indirizzo IP
- Utilizzato da dispositivi come workstation senza disco rigido
  - Immagine OS uguale per tutti
- Necessita di server con tabella RARP
- Stesso formato frame
  - 0x0835 Ethernet RARP request

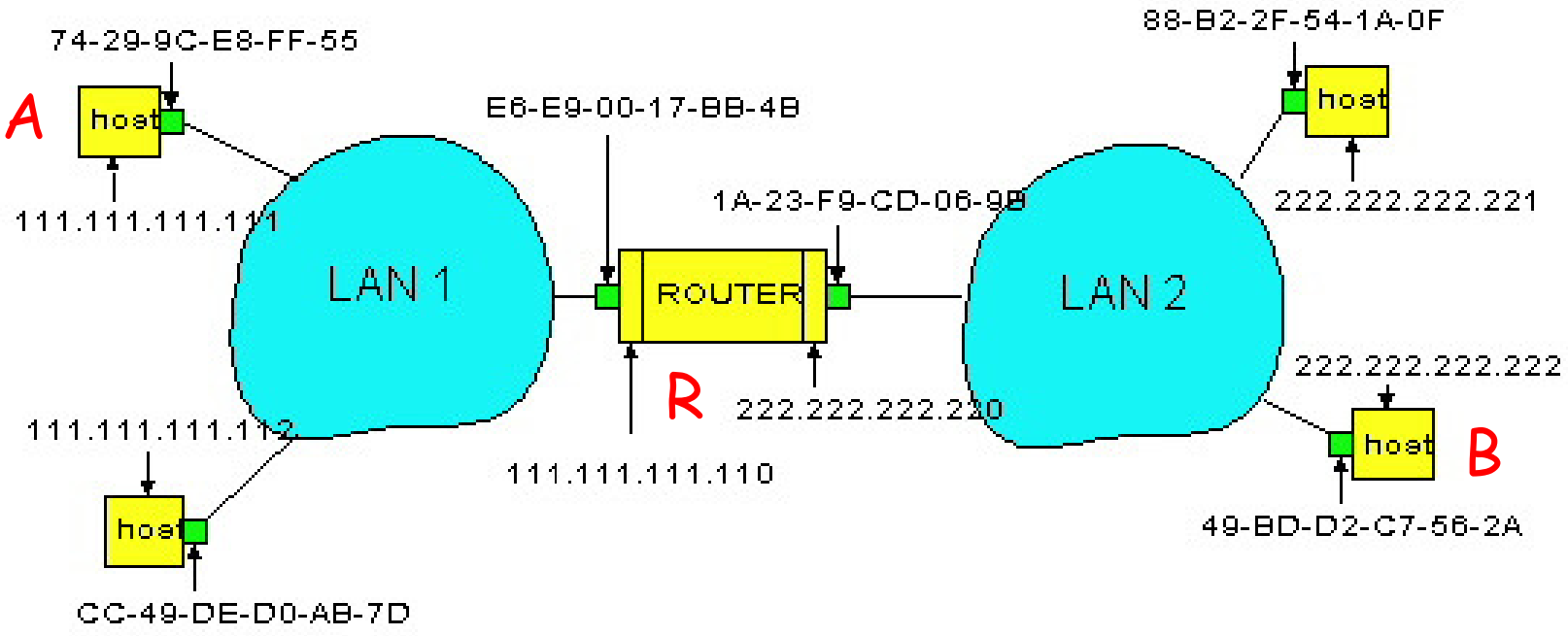
Reverse ARP - RARP

- **Primary server assegnato a ciascun host**
  - Host spedisce richiesta in broadcast
  - Solo il primary risponde, gli altri memorizzano richiesta
  - Se no risposta, rinnova richiesta
  - Uno degli altri risponde
- **In alternativa...**
  - Ciascun RARP server aspetta per un certo tempo prima di rispondere
  - Limito collisioni

Invio verso un nodo esterno alla sottorete

Invio di un datagramma da A a B attraverso R

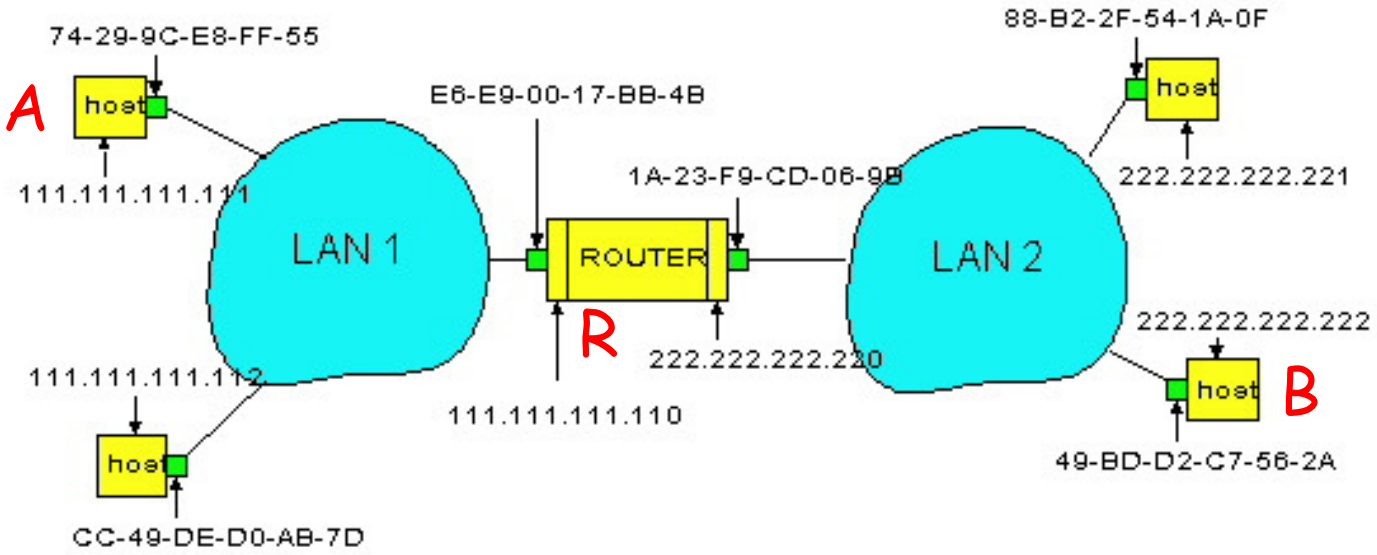
A conosce l'indirizzo IP di B.



Due tabelle ARP nel router R, una per ciascuna rete IP (LAN).

Invio verso un nodo esterno alla sottorete

- A crea un datagramma con origine A, e destinazione B.
- A usa ARP per ottenere l'indirizzo MAC di R.
- A crea un collegamento a livello di rete con l'indirizzo MAC di destinazione di R, il frame contiene il datagramma IP da A a B.
- L'adattatore di A invia il datagramma.
- L'adattatore di R riceve il datagramma.
- R estrae il datagramma IP dal frame Ethernet, e vede che la sua destinazione è B.
- R usa ARP per ottenere l'indirizzo MAC di B.
- R crea un frame contenente il datagramma IP da A a B IP e lo invia a B.



Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

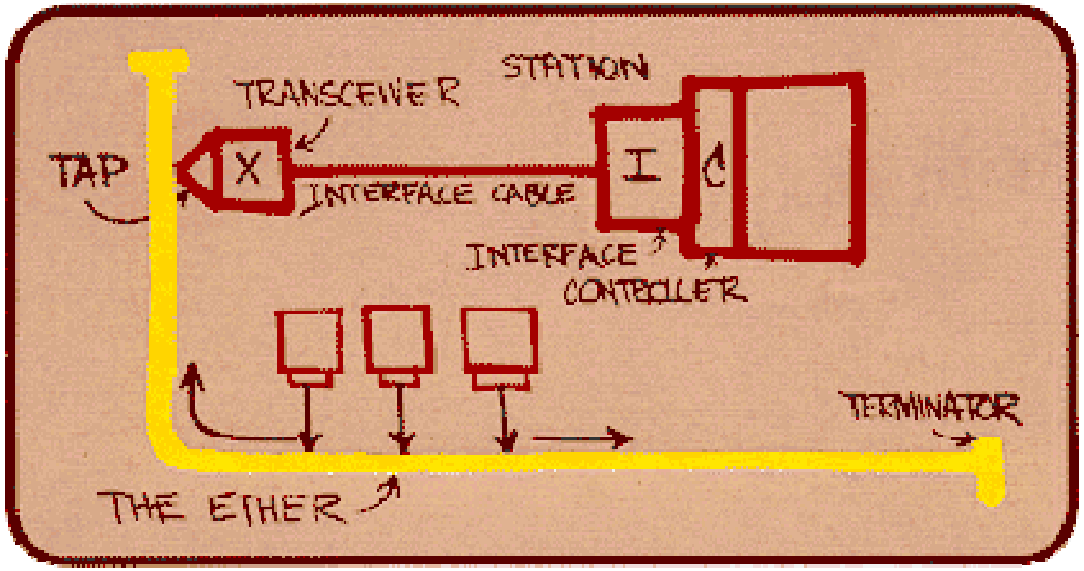
5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

Ethernet

Posizione dominante nel mercato delle LAN cablate.

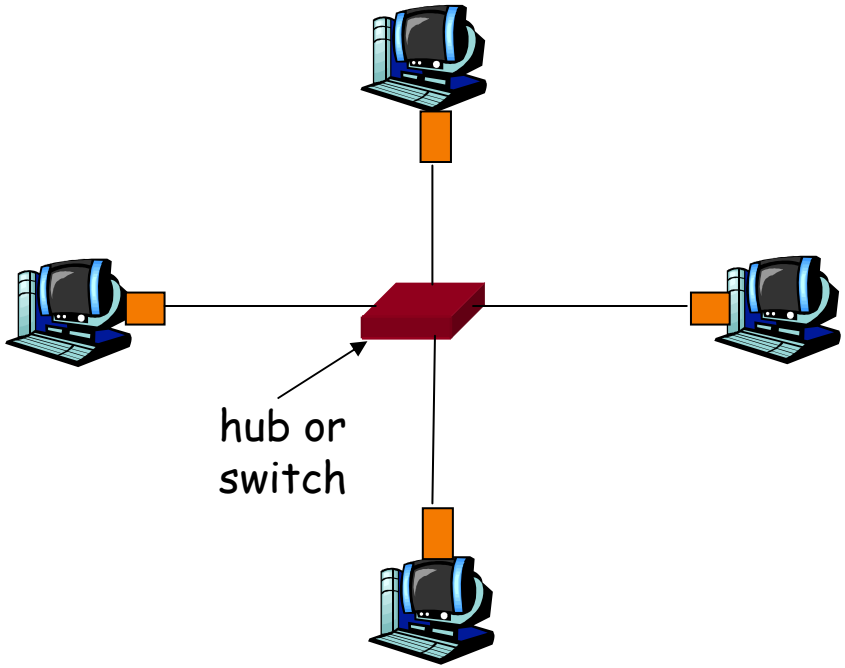
- È stata la prima LAN ad alta velocità con vasta diffusione.
- Più semplice e meno costosa di token ring, FDDI e ATM.
- Sempre al passo dei tempi con il tasso trasmissivo.



Il progetto originale di Bob Metcalfe che portò allo standard Ethernet.

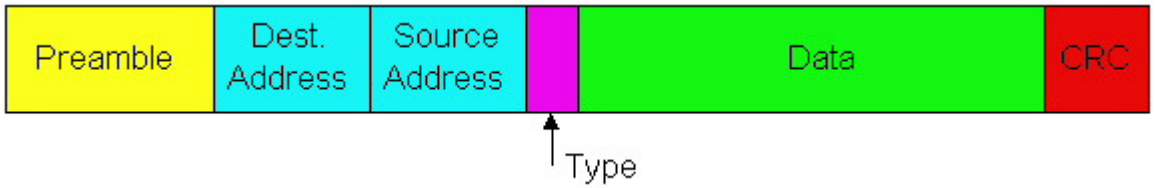
Topologia a stella

- La topologia a bus era diffusa fino alla metà degli anni 90.
- Quasi tutte le odierne reti Ethernet sono progettate con topologia a stella.
- Al centro della stella è collocato un hub o commutatore (*switch*).



Struttura dei pacchetti Ethernet

L'adattatore trasmittente incapsula i datagrammi IP in un pacchetto Ethernet.

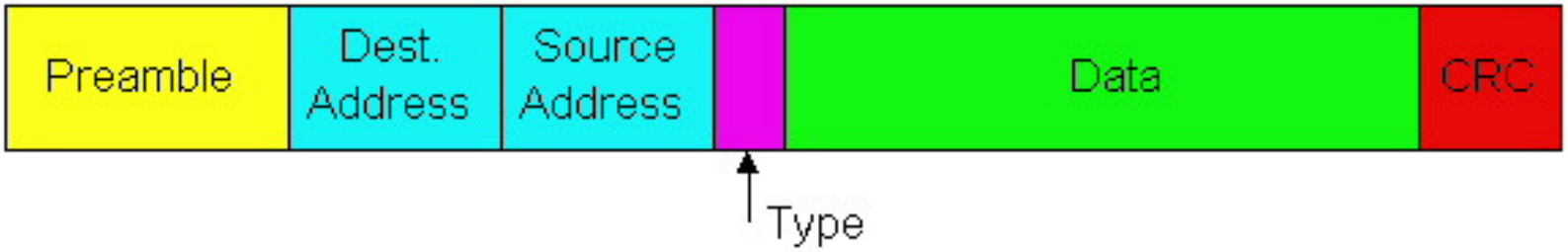


Preambolo:

- I pacchetti Ethernet iniziano con un campo di otto byte: sette hanno i bit 10101010 e l'ultimo è 10101011.
- Servono per "attivare" gli adattatori dei riceventi e sincronizzare i loro orologi con quello del trasmittente.

Struttura dei pacchetti Ethernet

- Indirizzo di destinazione: 6 byte
  - Quando un adattatore riceve un pacchetto contenente l'indirizzo di destinazione o con l'indirizzo broadcast (es.: un pacchetto ARP), trasferisce il contenuto del campo dati del pacchetto al livello di rete.
  - I pacchetti con altri indirizzi MAC vengono ignorati.
- Campo tipo: consente a Ethernet di supportare vari protocolli di rete (in gergo questa è la funzione di "multiplexare" i protocolli).
- Controllo CRC: consente all'adattatore ricevente di rilevare la presenza di un errore nei bit del pacchetto.



Servizio senza connessione non affidabile

- Senza connessione: non è prevista nessuna forma di handshake preventiva con il destinatario prima di inviare un pacchetto.
- Non affidabile: l'adattatore ricevente non invia un riscontro né se un pacchetto supera il controllo CRC né in caso contrario.
  - Il flusso dei datagrammi che attraversano il livello di rete può presentare delle lacune.
  - L'applicazione può rilevare le lacune se viene impiegato TCP.
  - Altrimenti, potrebbe accusare problemi a causa dell'incompletezza dei dati.

Ethernet utilizza il protocollo CSMA/CD

- Non utilizza slot.
- Non può trasmettere un pacchetto quando rileva che altri adattatori stanno trasmettendo: rilevazione della portante.
- Annulla la propria trasmissione non appena rileva che un altro adattatore sta trasmettendo: rilevazione di collisione.
- Prima di ritrasmettere, l'adattatore resta in attesa per un lasso di tempo stabilito arbitrariamente.

Fasi operative del protocollo CSMA/CD

1. L'adattatore riceve un datagramma di rete dal nodo cui è collegato e prepara un pacchetto Ethernet.
2. Se il canale è inattivo, inizia la trasmissione. Se il canale risulta occupato, resta in attesa fino a quando non rileva più il segnale.
3. Verifica, durante la trasmissione, la presenza di eventuali segnali provenienti da altri adattatori. Se non ne rileva, considera il pacchetto spedito.
4. Se rileva segnali da altri adattatori, interrompe immediatamente la trasmissione del pacchetto e invia un segnale di disturbo (jam).
5. L'adattore rimane in attesa. Quando riscontra l'n-esima collisione consecutiva, stabilisce un valore k tra {0,1,2,…,2m-1}. L'adattatore aspetta un tempo pari a K volte 512 bit e ritorna al Passo 2.

Protocollo CSMA/CD di Ethernet

Segnale di disturbo (*jam*): la finalità è di avvisare della collisione tutti gli altri adattatori che sono in fase trasmissiva; 48 bit.

Tempo di Bit : corrisponde a 0,1 microsec per Ethernet a 10 Mbps; per K=1023, il tempo di attesa è di circa 50 msec.

Attesa esponenziale:

- *Obiettivo*: l'adattatore prova a stimare quanti siano gli adattatori coinvolti.
  - Se sono numerosi il tempo di attesa potrebbe essere lungo.
- Prima collisione: sceglie K tra {0,1}; il tempo di attesa è pari a K volte 512 bit.
- Dopo la seconda collisione: sceglie K tra {0,1,2,3}…
- Dopo dieci collisioni, sceglie K tra {0,1,2,3,4,…,1023}.

Efficienza di Ethernet

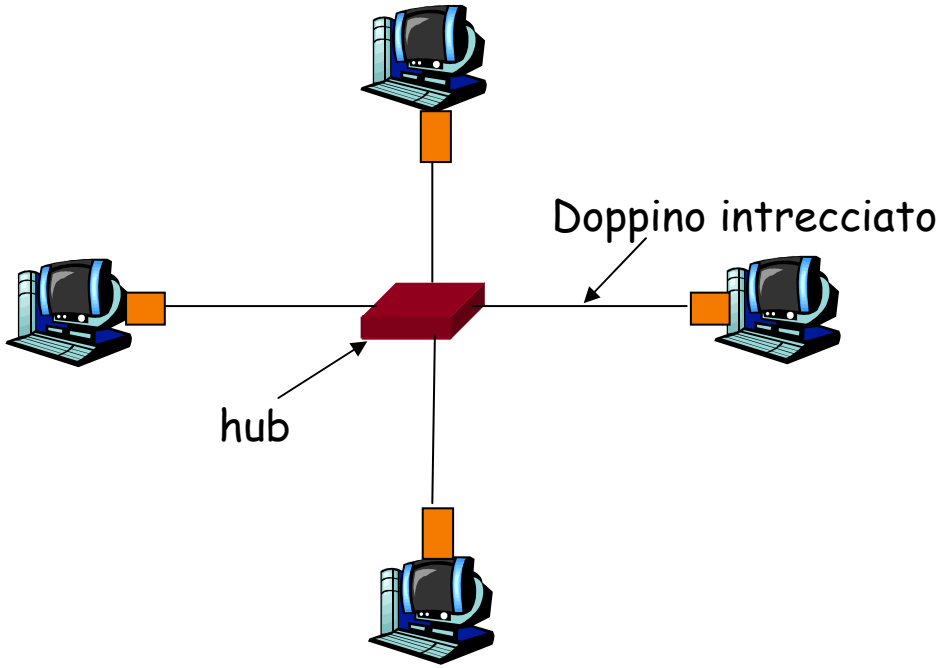
- T_{prop} = tempo massimo che occorre al segnale per propagarsi fra una coppia di adattatori.
- t_{trasm} = tempo necessario per trasmettere un pacchetto della maggior dimensione possibile.

$$\text{efficienza} = \frac{1}{1 + 5t_{prop} / t_{trasm}}$$

- Si evince che quando t_{prop} tende a 0, l'efficienza tende a 1.
- Al crescere di t_{trasm}, l'efficienza tende a 1.
- Molto meglio di ALOHA, ma ancora decentralizzato, semplice, e poco costoso.

Tecnologie 10BaseT e 100BaseT

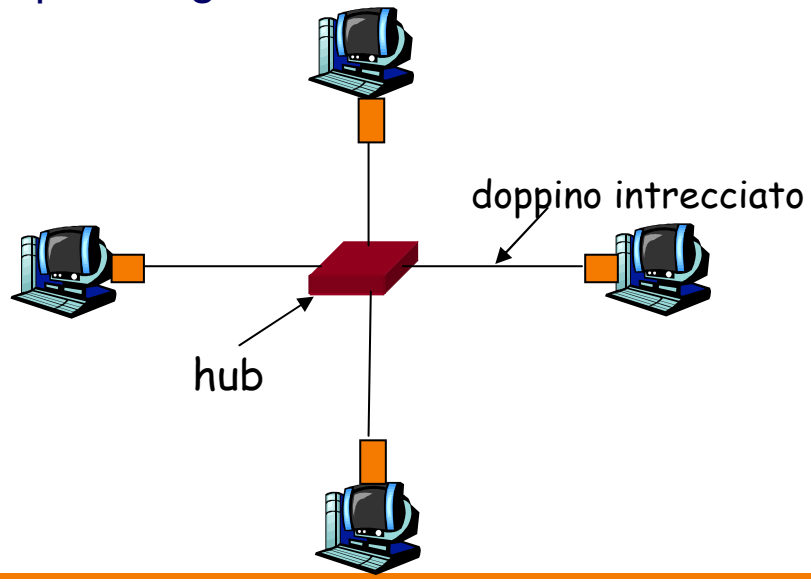
- Attualmente, molti adattatori Ethernet sono a 10/100 Mbps; possono quindi utilizzare sia 10BaseT sia 100BaseT
- La lettera T è l'iniziale di Twisted Pair (doppino intrecciato).
- Ogni nodo ha una diretta connessione con l'hub (topologia a stella); la massima distanza tra un adattatore e il centro stella è di 100m.



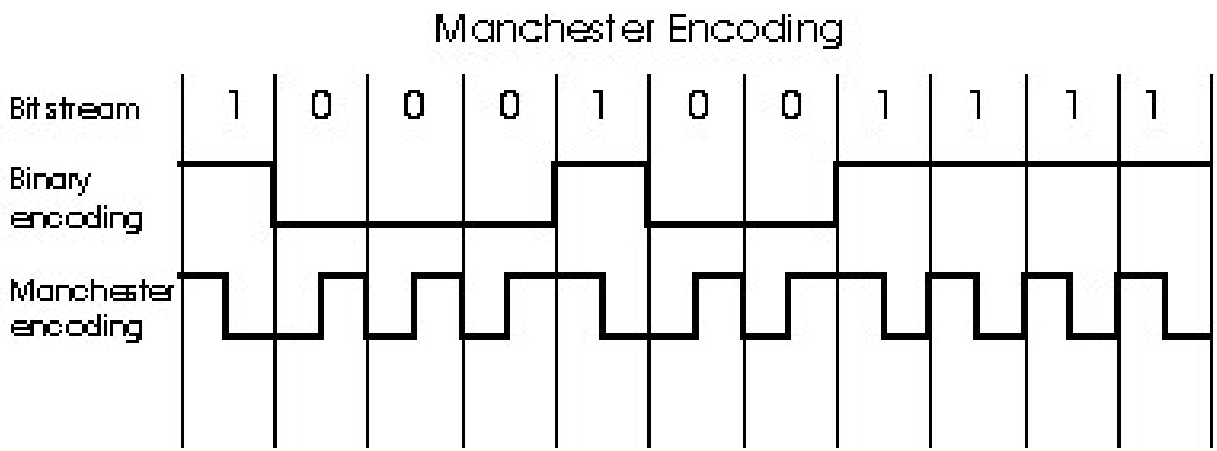
Hub

L'hub (ripetitore) è un dispositivo che opera sui singoli bit:

- all'arrivo di un bit, l'hub lo riproduce incrementandone l'energia e lo trasmette attraverso tutte le sue altre interfacce.
- non implementa la rilevazione della portante né CSMA/CD
- ripete il bit entrante su tutte le interfacce uscenti anche se su qualcuna di queste c'è un segnale
- trasmette in broadcast, e quindi ciascun adattatore può sondare il canale per verificare se è libero e rilevare una collisione mentre trasmette
- fornisce aspetti di gestione di rete.



Codifica Manchester



- Durante la ricezione di ciascun bit si verifica una transizione.
- Permette di sincronizzare gli orologi degli adattatori trasmittenti e riceventi.
  - Non c'è bisogno di un clock centralizzato e globale tra i nodi!
- La codifica Manchester è un'operazione del livello fisico!

Gigabit Ethernet

- Utilizza il formato del pacchetto standard di Ethernet.
- I canali punto-punto utilizzano commutatori, mentre i canali broadcast utilizzano hub.
- Utilizza CSMA/CD per i canali broadcast condivisi; è necessario limitare la distanza tra i nodi per ottenere un livello accettabile di efficienza.
- Gli hub sono definiti “distributori bufferizzati”.
- Impiegando i canali punto-punto si può operare in full-duplex a 1000 mbps.
- Attualmente 10 Gbps!

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

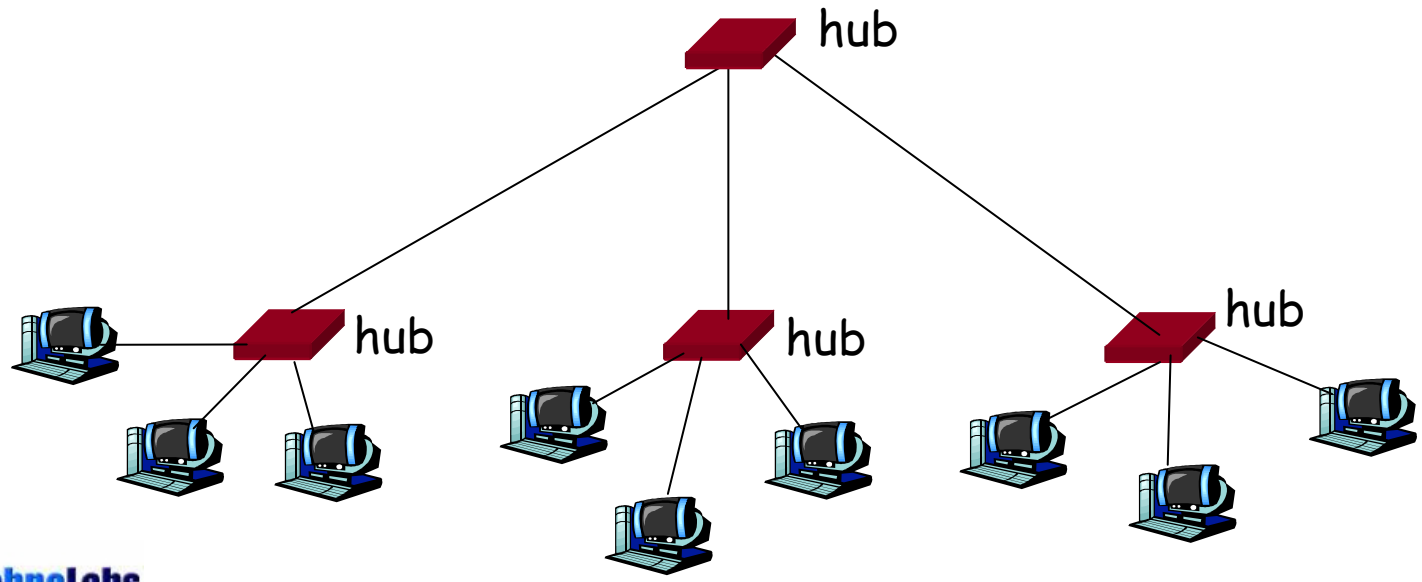
5.6 Interconnessioni: hub e commutatori

5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

Interconnessioni: hub e commutatori

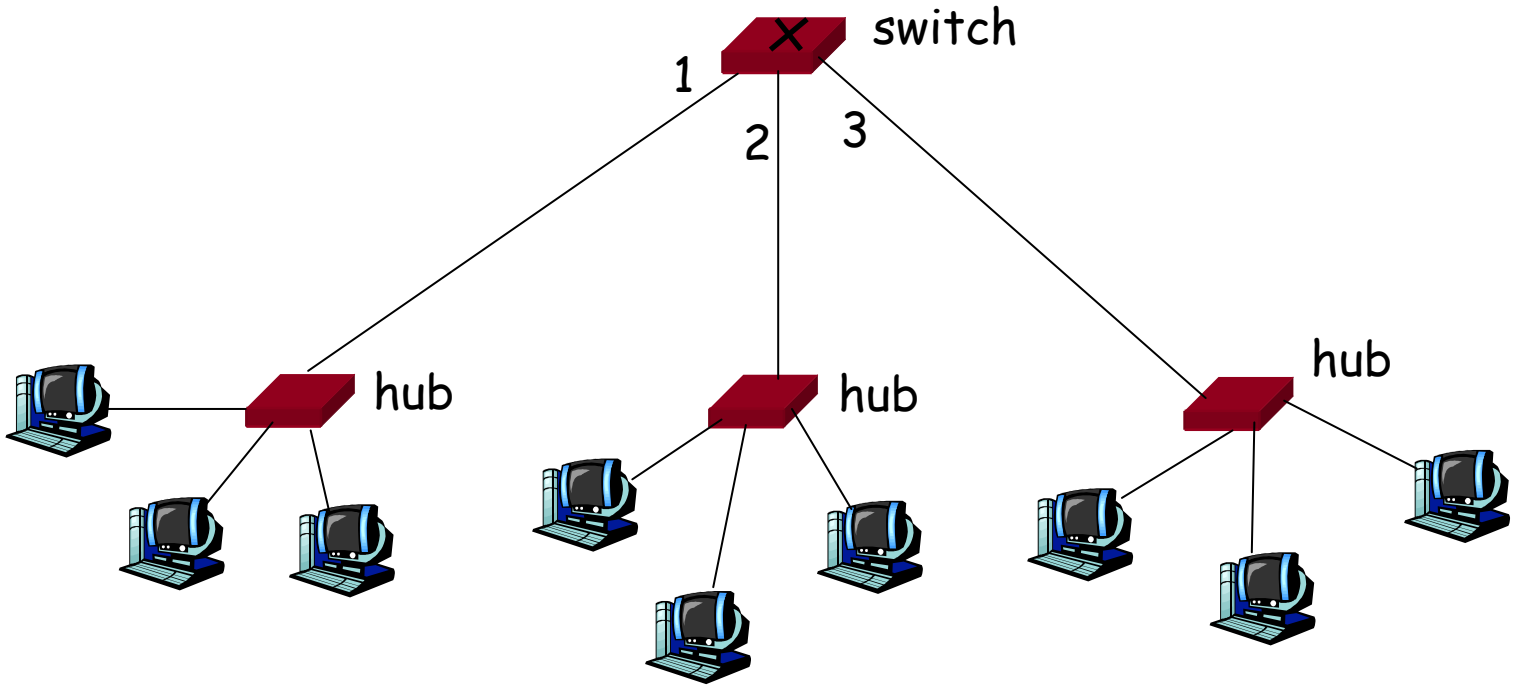
- Utilizzare hub è il modo più semplice per interconnettere le LAN.
- Permette di incrementare la distanza tra i nodi.
- Quando un hub dipartimentale manifesta un funzionamento non conforme, l'hub della dorsale rileva il problema e lo disconnette dalla LAN.
- Impossibile interconnettere 10BaseT e 100BaseT.



Switch

- Dispositivo del livello di link:
  - Filtra e inoltra i pacchetti Ethernet.
  - Esamina l'indirizzo di destinazione e lo invia all'interfaccia corrispondente alla sua destinazione.
  - Quando un pacchetto è stato inoltrato nel segmento, usa CSMA/CD per accedere al segmento.
- Trasparente
  - Gli host sono inconsapevoli della presenza di switch.
- Plug-and-play (autoapprendimento)
  - Gli switch non hanno bisogno di essere configurati.

Inoltro (forwarding)



- Come si individua l'interfaccia verso cui un pacchetto deve essere diretto?
- Sembra proprio un problema d'instradamento…

Auto apprendimento

- Le operazioni sono eseguite mediante una tabella di commutazione.
- Lo switch archivia nelle proprie tabelle:
  - l'indirizzo MAC, l'interfaccia e il momento dell'arrivo.
  - Se lo switch non riceve pacchetti da un determinato indirizzo sorgente, lo cancella (tempo di invecchiamento, TTL = 60 min)
- Lo switch *apprende* quali nodi possono essere raggiunti attraverso determinate interfacce
  - quando riceve un pacchetto, lo switch "impara" l'indirizzo del mittente
  - registra la coppia mittente/indirizzo nella sua tabella di commutazione

Filtraggio e inoltro

Quando uno switch riceve un pacchetto:

(gli switch utilizzano indirizzi MAC)

if entry found for destination
then{

if dest on segment from which frame arrived
then drop the frame

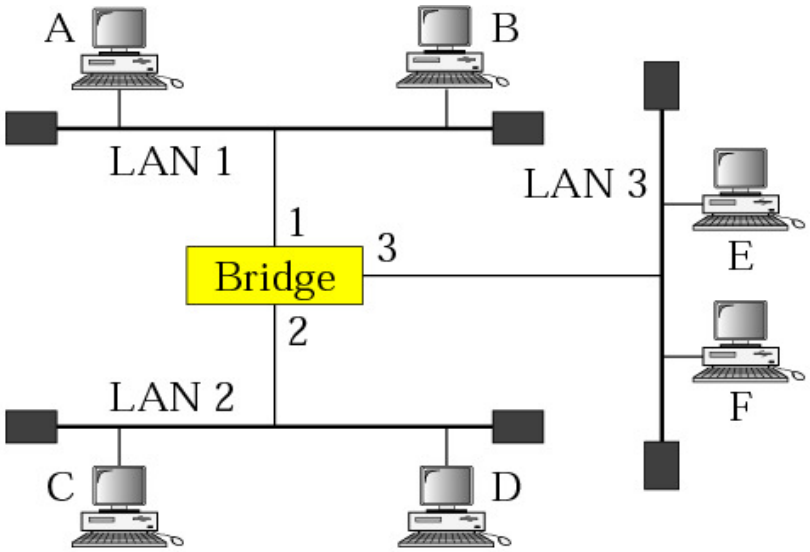
else forward the frame on interface indicated

}

else flood

Lo inoltra a tutti tranne all'interfaccia dalla quale è arrivato il pacchetto

Switch: esempio



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

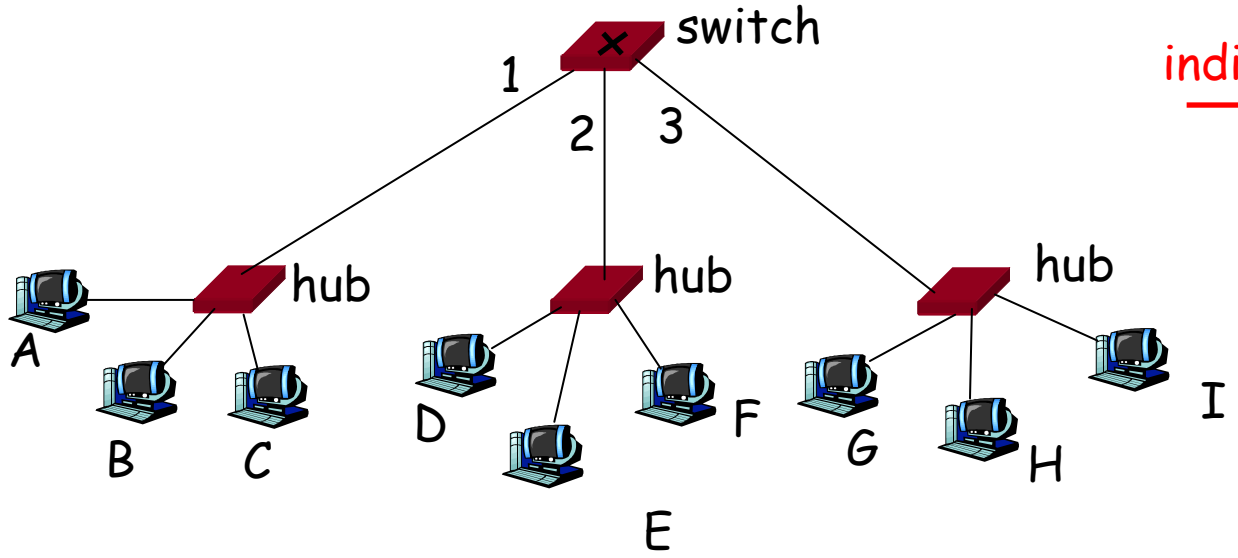
c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

Switch: esempio

Supponiamo che C invii un pacchetto a D

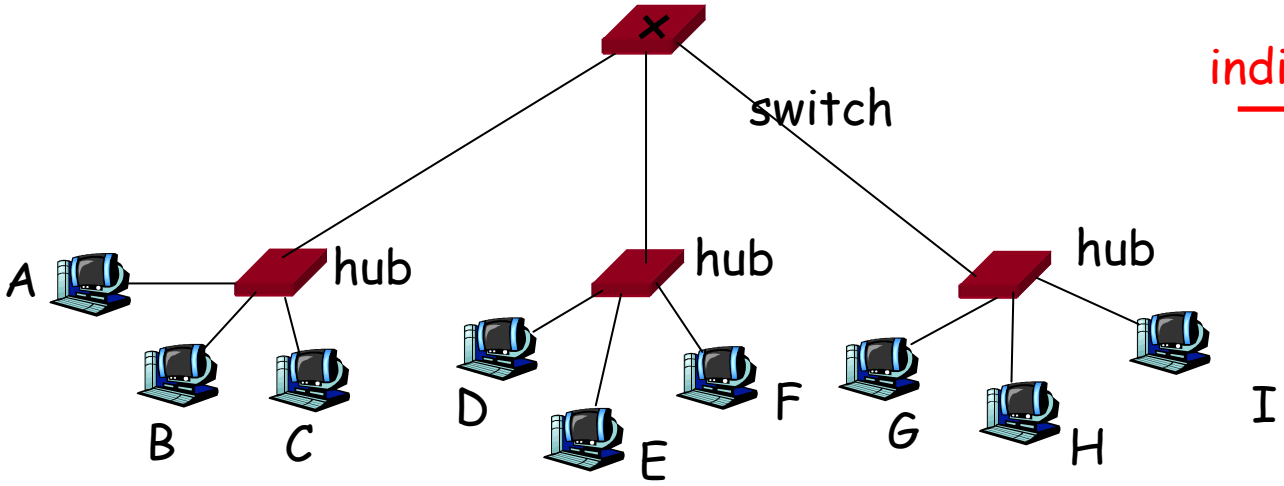


indirizzo	interfaccia
A	1
B	1
E	2
G	3

- **Lo switch riceve il pacchetto da C:**
  - **annota nella tabella di commutazione che C si trova nell'interfaccia 1.**
  - **Poiché D non è presente nella tabella, lo switch inoltra il pacchetto alle interfacce 2 e 3.**
- **Il pacchetto viene ricevuto da D.**

Switch: esempio

Supponiamo che D risponda a C con l'invio di un pacchetto.



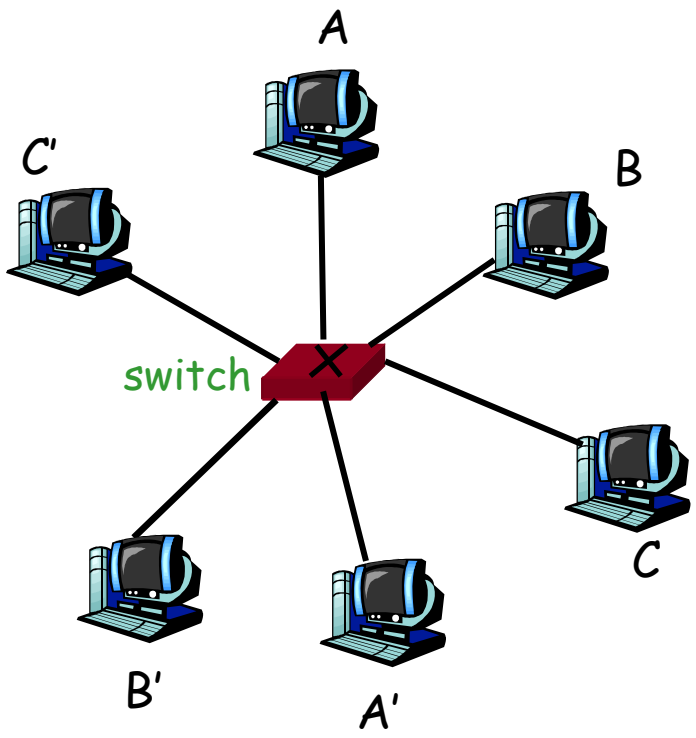
indirizzo	interfaccia
A	1
B	1
E	2
G	3
C	1

- **Lo switch riceve il pacchetto da D:**
  - **annota nella tabella di commutazione che D si trova nell'interfaccia 2**
  - **poiché C si trova già nella tabella, lo switch inoltra il pacchetto solo all'interfaccia 1.**
- **Il pacchetto viene ricevuto da C.**

Switch: accesso dedicato

- Switch con molte interfacce.
- Gli host hanno una connessione diretta con lo switch.
- Esclude qualsiasi possibilità di collisione; opera in modalità full duplex.

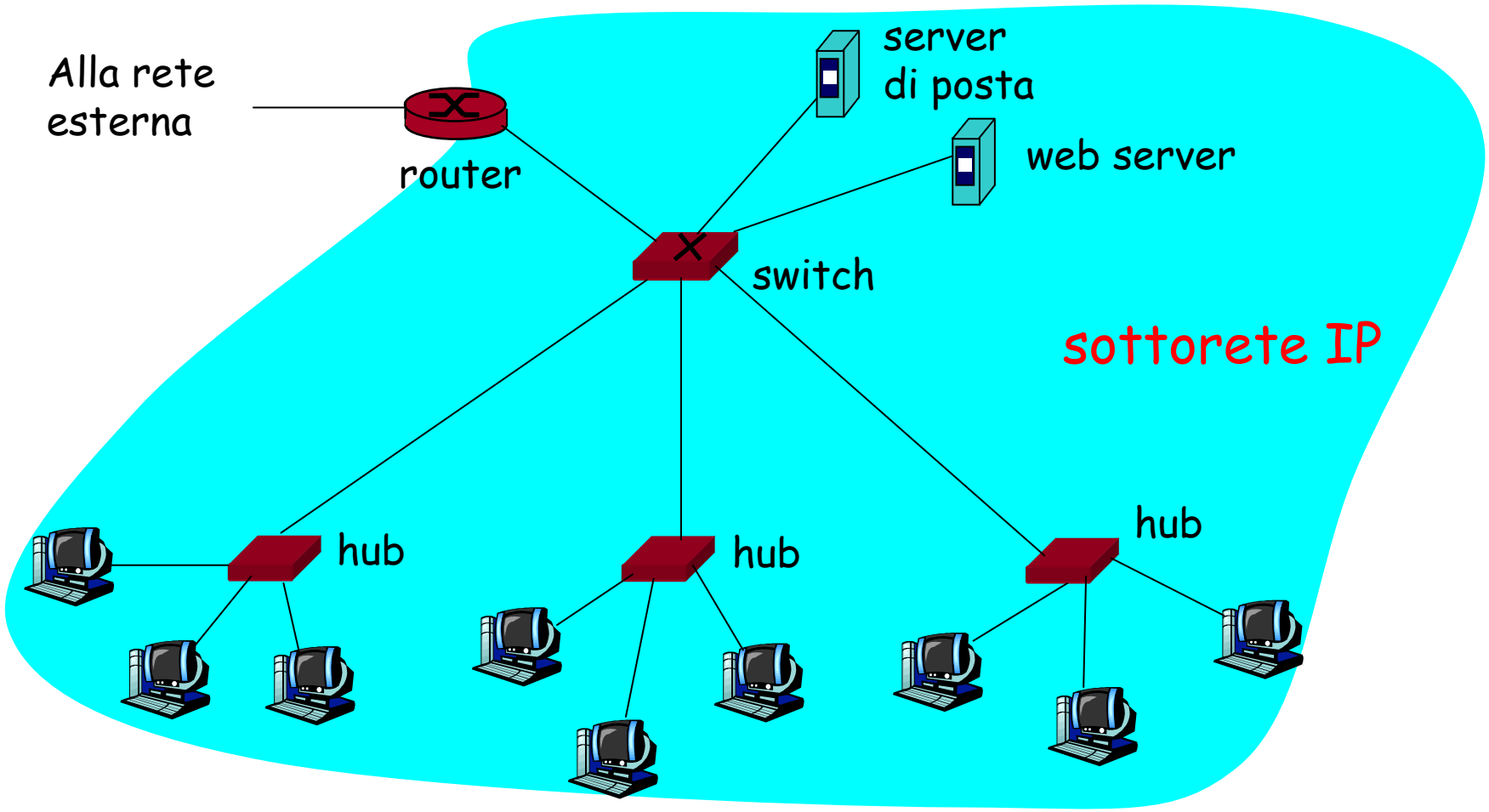
Commutazione: A-a-A' e B-a-B' simultaneamente, senza collisioni.



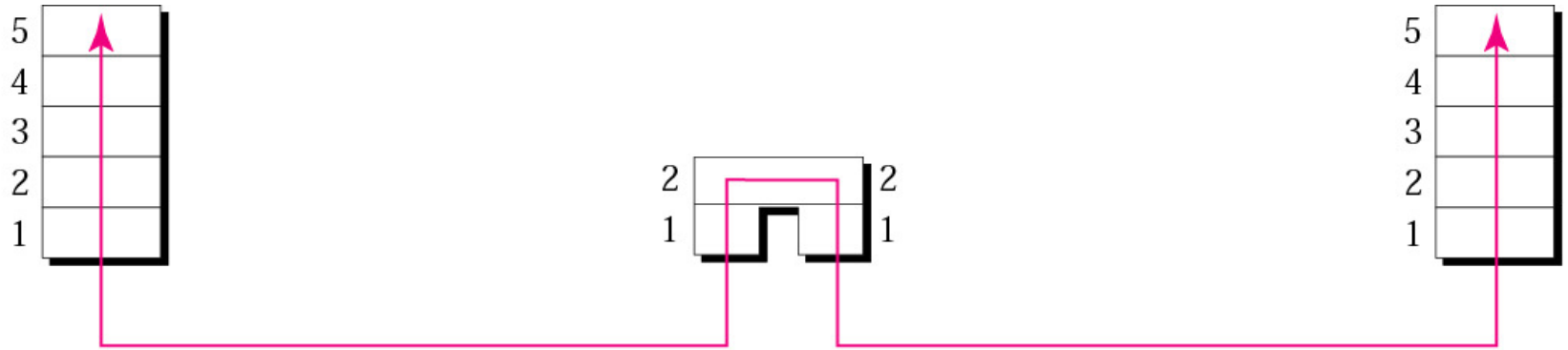
Ancora sugli switch

- Commutazione cut-through: lo switch inizia la trasmissione della parte iniziale del pacchetto anche se questo non è pervenuto integralmente.
- Lo switch cut-through riduce il ritardo solamente di un tempo compreso tra 0,12 e 1,2 ms, ed esclusivamente con carichi leggeri del collegamento in uscita. Un vantaggio piuttosto limitato…

Esempio di rete di un'istituzione

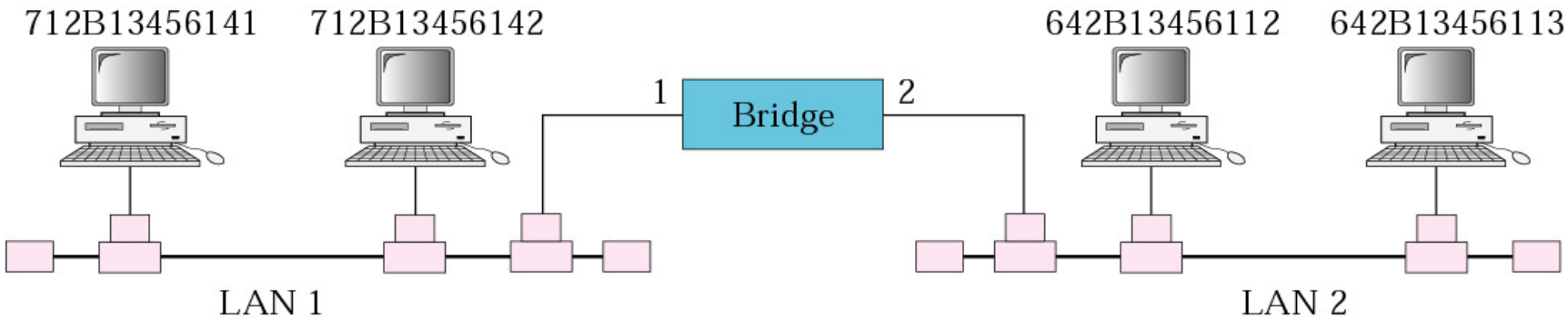


Switch e router a confronto



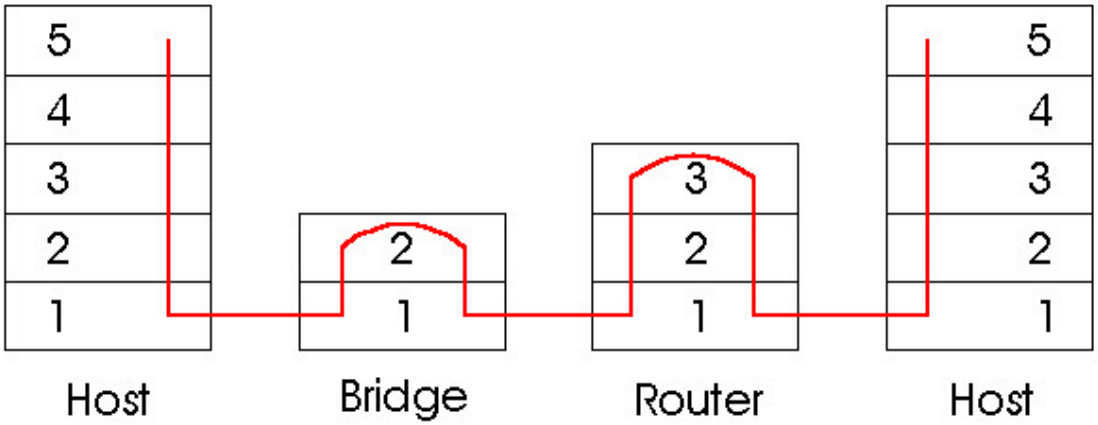
Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

Bridge table

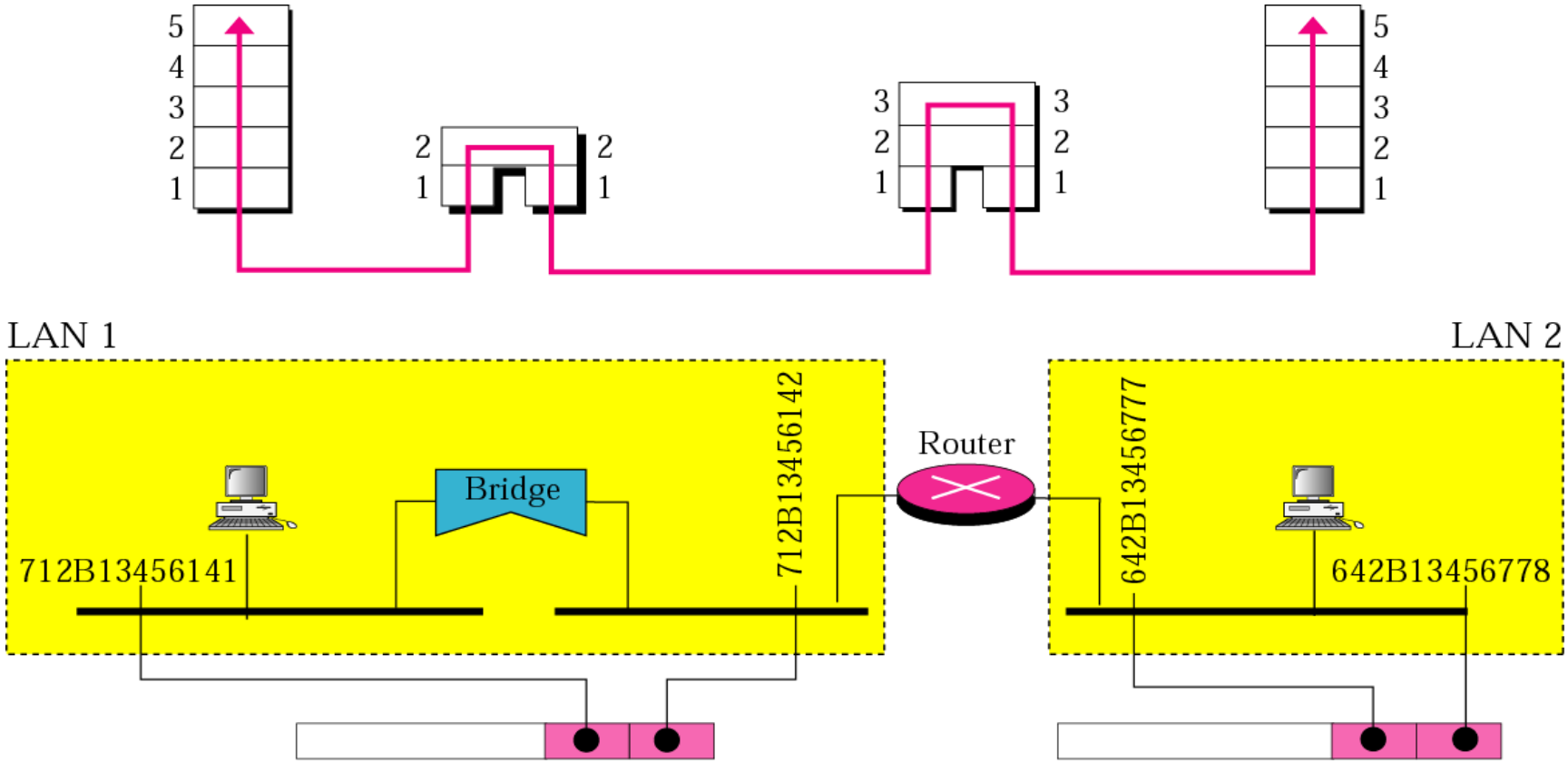


Switch e router a confronto

- **Entrambi sono dispositivi store-and-forward**
  - **router: dispositivi a livello di rete**
  - **switch: dispositivi a livello di link**
- **I router mantengono tabelle d'inoltro e implementano algoritmi d'instradamento**
- **Gli switch mantengono tabelle di commutazione e implementano il filtraggio e algoritmi di autoapprendimento**



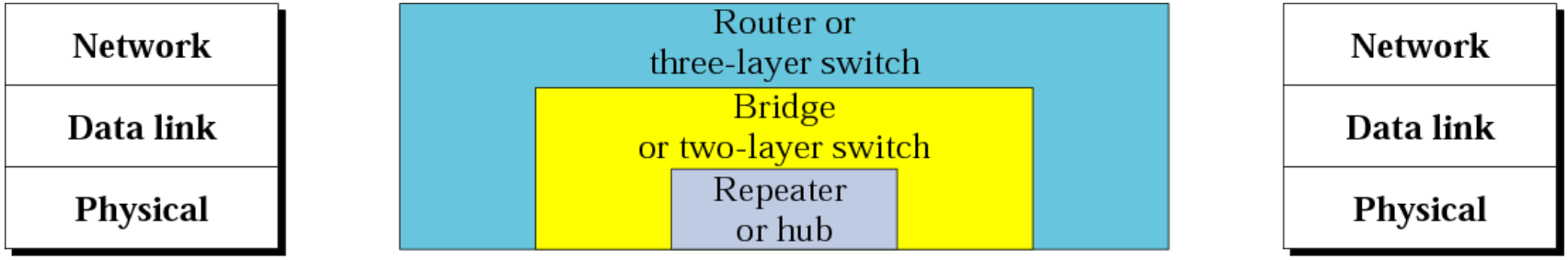
Switch e router a confronto



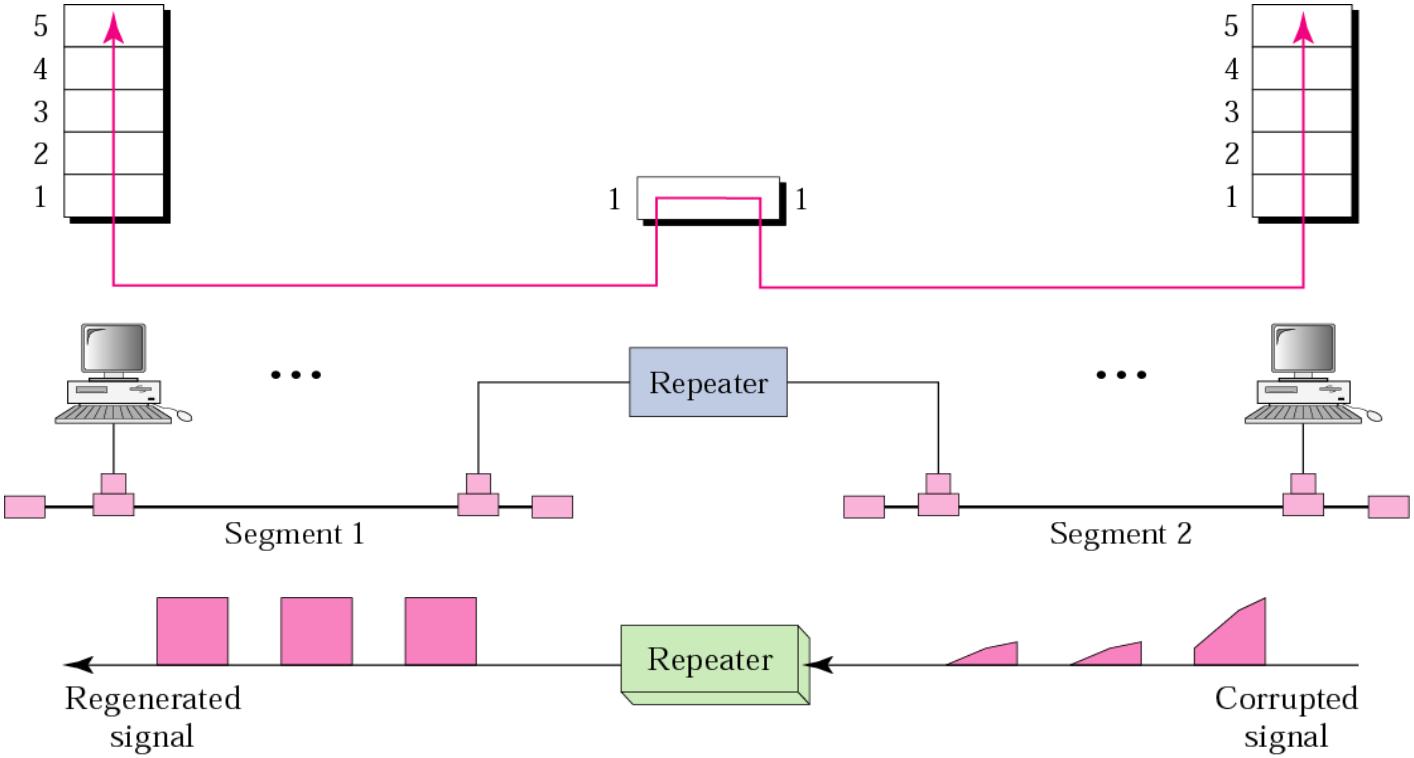
Nota: Trasparenza

Un bridge NON cambia MAI l'indirizzo fisico (MAC) in una frame.

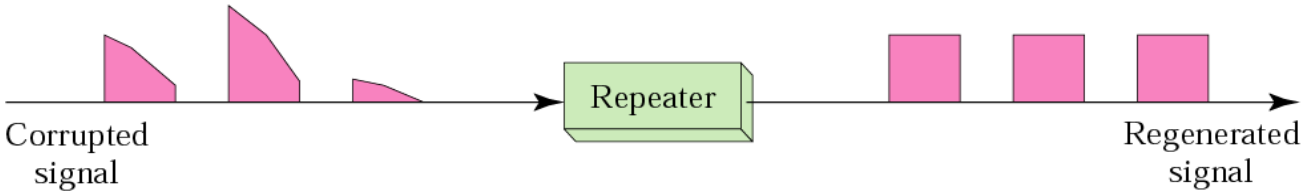
Connecting devices



Repeater



a. Right-to-left transmission.



b. Left-to-right transmission.

Sintesi delle caratteristiche

	hub	router	commutatore
Isolamento del traffico	no	sì	sì
Plug and play	sì	no	sì
Instradamento ottimale	no	sì	no
Cut-through	sì	no	sì

Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

Protocollo punto-punto

- Un mittente, un destinatario, un collegamento: estremamente semplice.
  - non c'è protocollo di accesso al mezzo (MAC)
  - non occorre indirizzamento MAC esplicito
  - il collegamento potrebbe essere una linea telefonica seriale commutata, un collegamento SONET/SDH, una connessione X.25 o un circuito ISDN
- Protocolli punto-punto DLC più diffusi:
  - PPP (*point-to-point protocol*)
  - HDLC (*high-level data link control*)

Requisiti IETF per il PPP [RFC 1547]

- Framing dei pacchetti: il protocollo IP del mittente incapsula un pacchetto a livello di rete all'interno del pacchetto PPP a livello di link.
- Trasparenza: il protocollo PPP non deve porre alcuna restrizione ai dati che appaiono nel pacchetto a livello di rete.
- Rilevazione degli errori (ma non la correzione)
- Disponibilità della connessione: il protocollo deve rilevare la presenza di eventuali guasti a livello di link e segnalare l'errore al livello di rete.
- Negoziazione degli indirizzi di rete: PPP deve fornire un meccanismo ai livelli di rete comunicanti per ottenere o configurare gli indirizzi di rete.

Requisiti che PPP non deve implementare

- Correzione degli errori.
- Controllo di flusso.
- Sequenza (non deve necessariamente trasferire i pacchetti al ricevente mantenendo lo stesso ordine).
- Collegamento multipunto (es., polling).

Correzione degli errori, controllo di flusso,
ri-ordinamento dei pacchetti
sono delegati ai livelli superiori!

Formato dei pacchetti dati PPP

- Flag: ogni pacchetto inizia e termina con un byte con valore 01111110
- Indirizzo: unico valore (11111111)
- Controllo: unico valore; ulteriori valori potrebbero essere stabiliti in futuro
- Protocollo: indica al PPP del ricevente qual è il protocollo del livello superiore cui appartengono i dati incapsulati

1	1	1	1 or 2	variable length	2 or 4	1
01111110	11111111	00000011	protocol	info	check	01111110
flag	address	control				flag

Formato dei pacchetti dati PPP

- informazioni: incapsula il pacchetto trasmesso da un protocollo del livello superiore (come IP) sul collegamento PPP.
- checksum: utilizzato per rilevare gli errori nei bit contenuti in un pacchetto; utilizza un codice a ridondanza ciclica HDLC a due o a quattro byte.

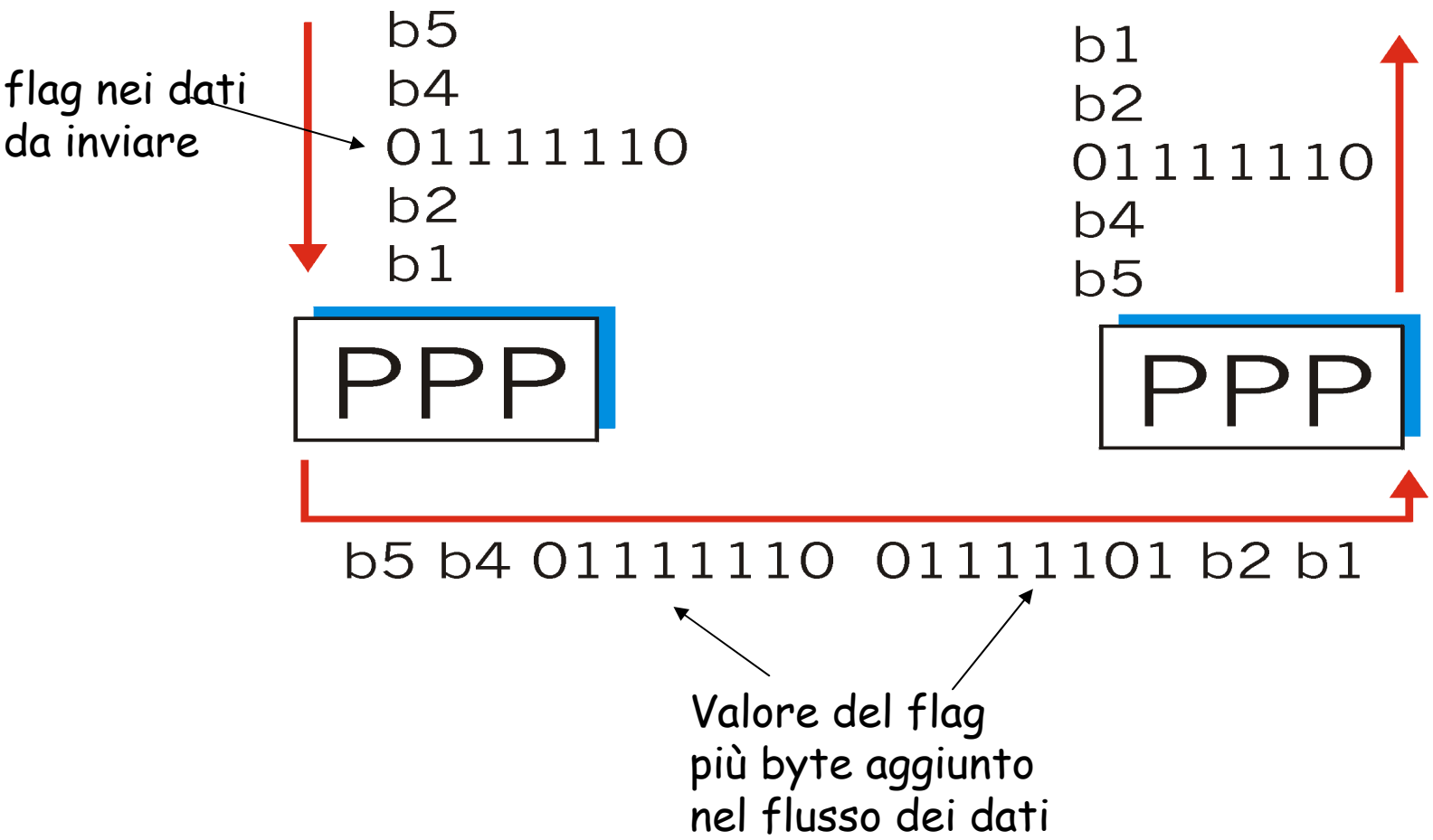
1	1	1	1 or 2	variable length	2 or 4	1
01111110	11111111	00000011	protocol	info	check	01111110
flag	address	control				flag

Riempimento dei byte (Byte stuffing)

- Requisito di trasparenza: nel campo informazioni deve essere possibile inserire una stringa <01111110>
  - D: se compare <01111110> come fa il ricevente a rilevare in modo corretto la fine del frame PPP?

- Mittente: aggiunge ("stuff") un byte di controllo <01111110> prima di ogni byte di dati <01111110>
- Destinatario:
  - Due byte 01111110: scarta il primo e continua la ricezione dei dati.
  - Singolo 01111110: valore di flag

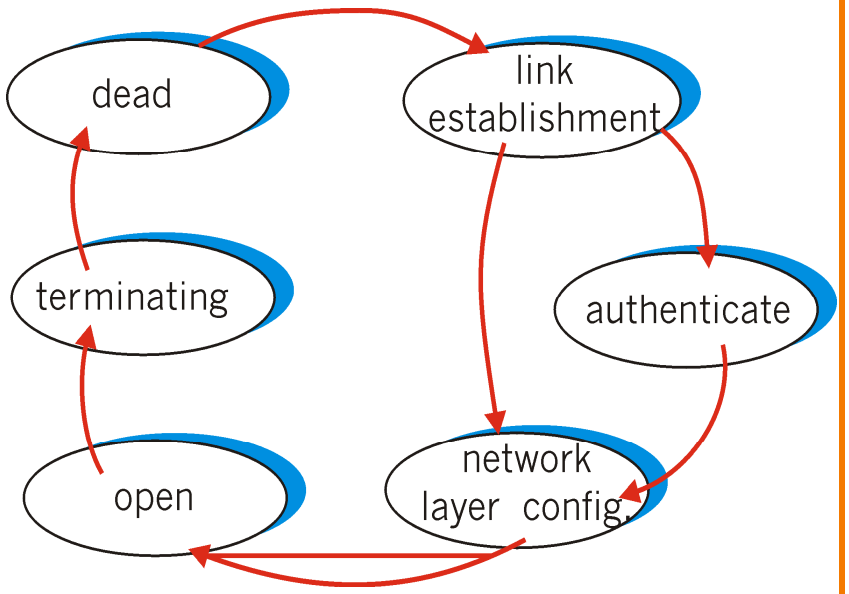
Byte stuffing



Protocollo di controllo del collegamento e protocolli di rete

Prima di avviare lo scambio di dati, i due peer devono configurare il collegamento:

- **Configurazione del collegamento PPP (massima dimensione del pacchetto, autenticazione).**
- **Scambio dei pacchetti di controllo propri del livello di rete**
  - **per IP: viene utilizzato il protocollo di controllo IP (IPCP) e i dati IPCP sono inseriti in un pacchetto PPP (il cui campo protocollo contiene 8021) in modo analogo a quello in cui i dati LCP sono inseriti in un pacchetto PPP**



Livello di collegamento e reti locali

5.1 Livello di link: introduzione e servizi

5.2 Tecniche di rilevazione e correzione degli errori

5.3 Protocolli di accesso multiplo

5.4 Indirizzi a livello di link

5.5 Ethernet

5.6 Interconnessioni: hub e commutatori

5.7 PPP: protocollo punto-punto

5.8 Canali virtuali: una rete come un livello di link

Virtualizzazione delle reti

Virtualizzazione delle risorse: una potente astrazione nell'ingegneria dei sistemi

- Esempi nell'informatica: memoria virtuale, dispositivi virtuali
  - macchine virtuali: es. Java
  - Sistema operativo IBM VM tra gli anni '60 e '70

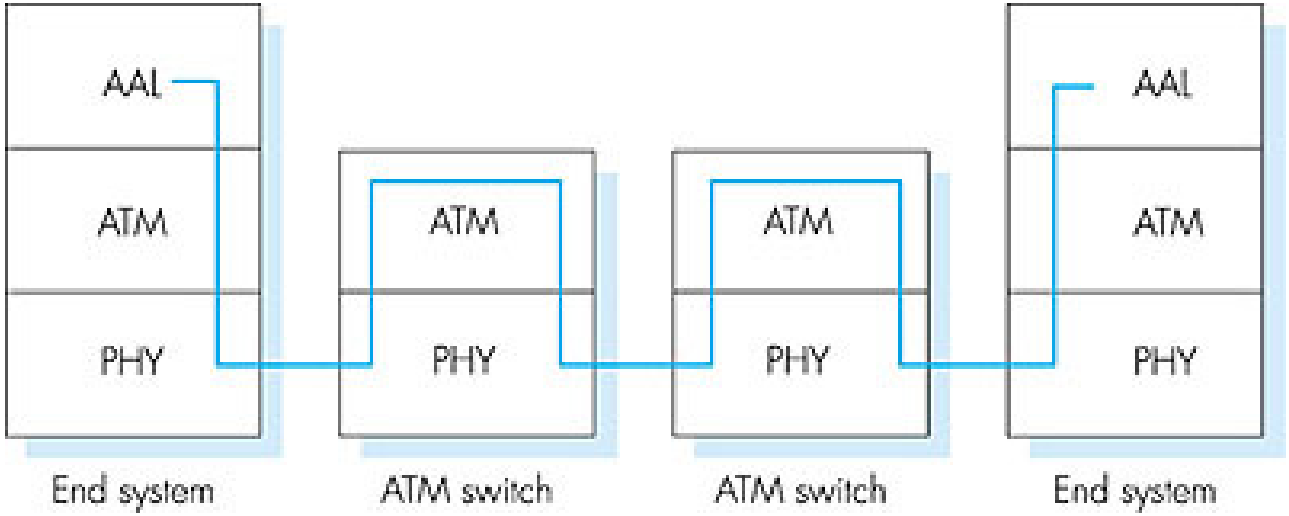
ATM e MPLS

- ATM, MPLS utilizzano la commutazione a pacchetto e sono reti a circuito virtuale.
  - hanno propri formati di pacchetto e propri metodi d'invio.
- Dal punto di vista di Internet sono al pari di un qualunque collegamento che interconnette dispositivi IP.
  - come una rete telefonica e una Ethernet commutata
- ATM, MPSL: vedremo come queste reti forniscono connessione ai dispositivi IP

Trasferimento asincrono: ATM

- **Gli standard per ATM cominciarono a essere sviluppati alla metà degli anni ’80 dall’ATM Forum e dall’ITU; in pratica fu utilizzata principalmente all’interno di reti telefoniche e IP servendo, per esempio, come tecnologia dei collegamenti che connettono router IP.**
- **<u>Obiettivo:</u>** ***progettare reti in grado di trasportare file audio e video in tempo reale, oltre a testo, e-mail e file di immagini***
  - **Rispondenza ai requisiti di tempo/QoS per voce e video (rispetto al modello best-effort di Internet)**
  - **Telefonia di ultima generazione**
  - **Commutazione di pacchetto usando circuiti virtuali**

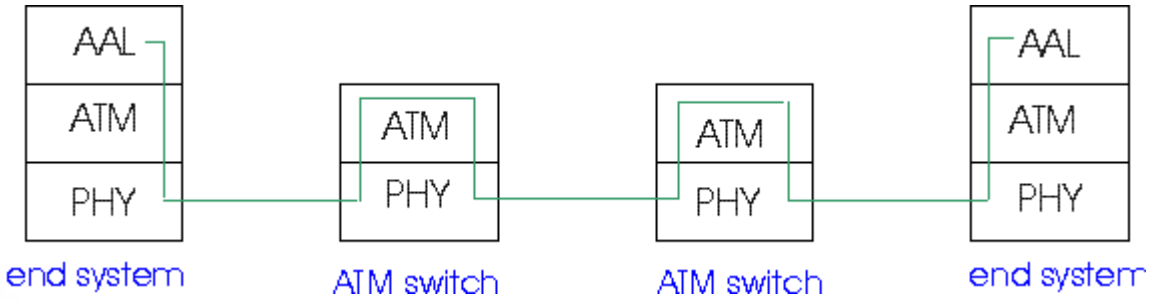
Architettura di ATM



- **AAL (ATM *adaptation layer*) è presente solo nei dispositivi alla periferia della rete ATM:**
  - **Segmentazione e riassemblaggio dei pacchetti**
  - **Simile al livello di trasporto in Internet**
- **Livello ATM: "livello di rete"**
  - **Definisce la struttura della cella ATM e il significato dei suoi campi**
- **Livello fisico**

AAL: ATM Adaptation Layer

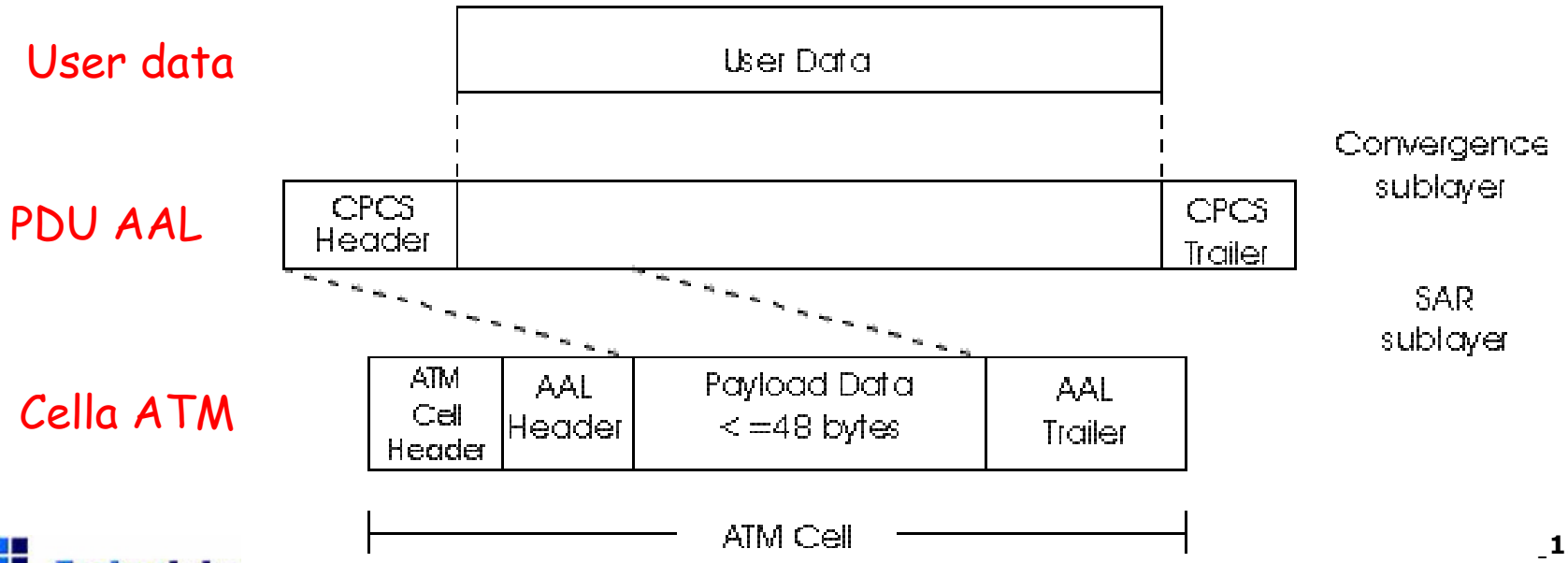
- *ATM* ***Adaptation Layer*** (AAL): “adatta” i livelli superiori (IP o applicazioni ATM native) al sottostante livello ATM.
- AAL è presente **solo nei sistemi terminali** e non nei commutatori.
- Segmento di livello AAL frammentato su più celle ATM
  - Analogia: segmenti TCP in vari pacchetti IP.



AAL: ATM Adaptation Layer

Differenti versioni di livelli AAL, in base alla classe di servizio ATM:

- **AAL1: per il servizio a tasso costante, CBR (*Constant Bit Rate*), es. emulazione di circuito.**
- **AAL2: per il servizio a tasso variabile, VBR (*Variable Bit Rate*), es. video MPEG.**
- **AAL5: per il servizio dati (es., datagrammi IP).**



Livello ATM

Servizio: trasporto di celle attraverso la rete ATM.

- Analogo al livello di rete IP.
- I servizi sono molto differenti dal livello di rete IP.

Architettura della rete	Modello di servizio	Garanzie				Feedback congestione
		Larghezza di banda	Perdita	Ordine	Timing	
Internet	best effort	nessuna	no	no	no	no (dedotta se c'è perdita)
ATM	CBR	Tasso costante	sì	sì	sì	non c'è congestione
ATM	VBR	Tasso garantito	sì	sì	sì	non c'è congestione
ATM	ABR	Minimo garantito	no	sì	no	sì
ATM	UBR	nessuna	no	sì	no	no

Livello ATM: canale virtuale (VC)

- Canale virtuale: percorso che consiste in una sequenza di collegamenti fra sorgente e destinazione.
  - Impostazione della chiamata, prima di avviare la trasmissione dati
  - Ciascun pacchetto ha un identificatore del circuito virtuale (VCI)
- Canale virtuale permanente (PVC, *permanent VC*)
  - Per connessioni di lunga durata
  - Le celle ATM sono instradate dal punto d'ingresso a quello d'uscita
- Canale virtuale dinamico (SVC, *switched VC*):
  - Creato o cancellato dinamicamente, su richiesta

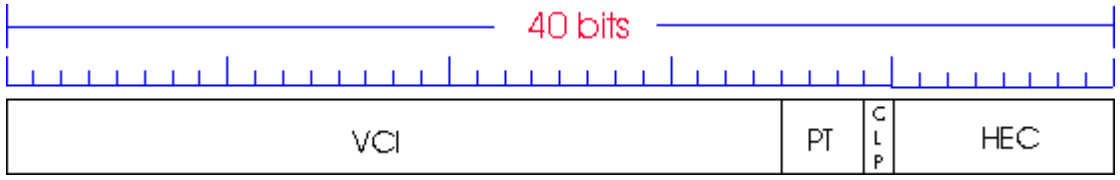
Canali virtuali ATM

- Vantaggi:
  - Prestazioni e QoS sono garantite (ampiezza di banda, ritardo/perdita, jitter)
- Svantaggi:
  - Inadeguato supporto al traffico dei pacchetti
  - Un PVC tra ciascuna coppia sorgente/destinatario: problemi di scalabilità
  - Eccesso di elaborazione per connessioni di breve durata

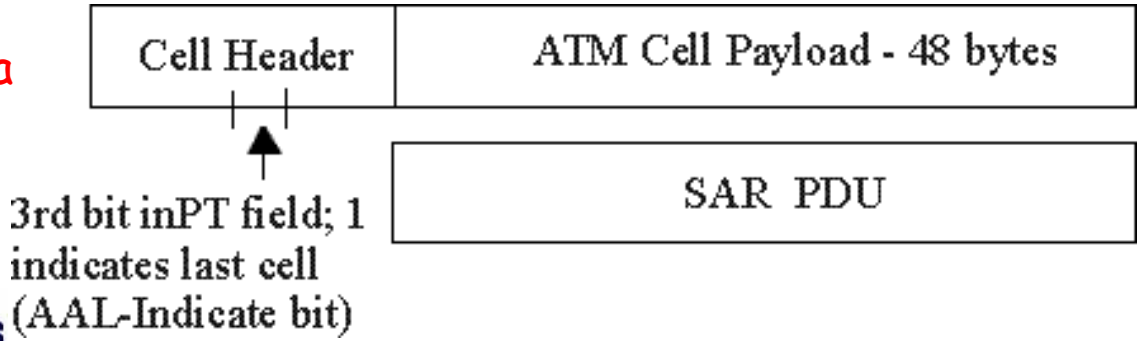
Livello ATM: cella ATM

- Intestazione: 5-byte
- Carico utile: 48-byte
  - Perché?: se il carico utile è piccolo ➔ piccolo ritardo per voce digitalizzata
  - A metà strada tra 32 e 64 (compromesso!)

Intestazione cella

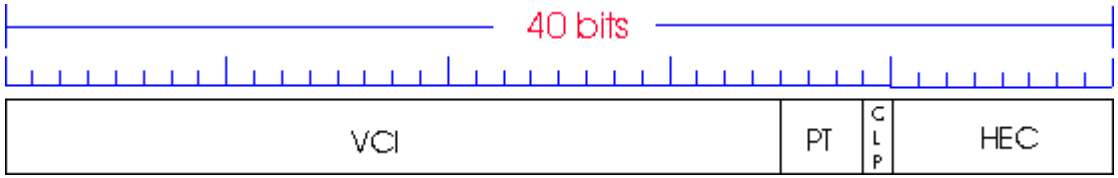


Formato cella



Campi della cella ATM (intestazione)

- **VCI:** identificatore del canale virtuale.
  - Il VCI di una cella varia da collegamento a collegamento.
- **PT:** tipo di carico utile
  - Indica il tipo di carico che la cella contiene
- **CLP:** bit di priorità sulla perdita di cella.
  - CLP = questo bit può essere usato per scegliere le celle da scartare se si verifica una congestione.
- **HEC:** byte d'errore nell'intestazione.
  - I bit per il rilevamento e la correzione dell'errore che proteggono l'intestazione della cella.



Livello fisico ATM

Esistono *due* classi generali del livello fisico:

- Transmission Convergence Sublayer (TCS): adatta il livello ATM al livello PMD sottostante
- Physical Medium Dependent: dipende dal mezzo fisico utilizzato

Livello fisico ATM

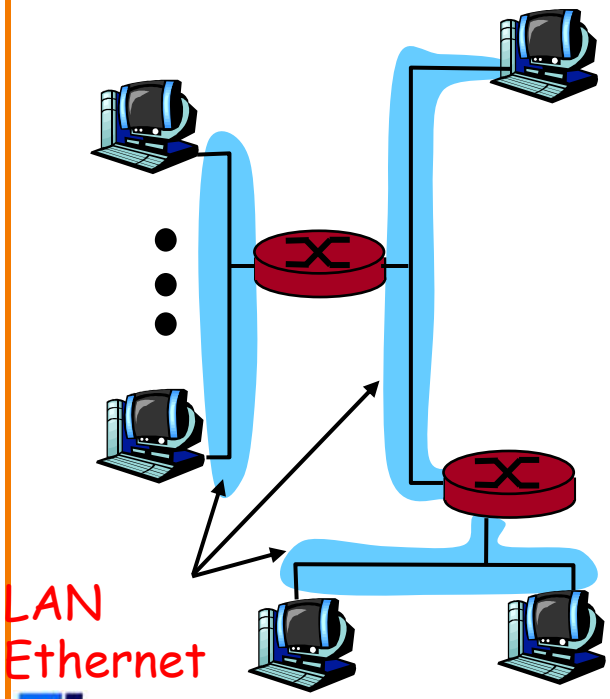
Alcuni possibili livelli fisici includono:

- **SONET/SDH**: (*synchronous optical network/ synchronous digital hierarchy*, reti ottiche sincrone/gerarchia digitale sincrona)
  - sincronizzazione dei bit
  - suddivisione di banda
  - differenti velocità: OC3 = 155.52 Mbps; OC12 = 622.08 Mbps; OC48 = 2.45 Gbps, OC192 = 9.6 Gbps
- **T1/T3**: su fibra, microonde e cavo: 1.5 Mbps/ 45 Mbps
- **Basati su cella senza frame.** In questo caso, la temporizzazione al ricevente è derivata da un segnale trasmesso.

IP su ATM

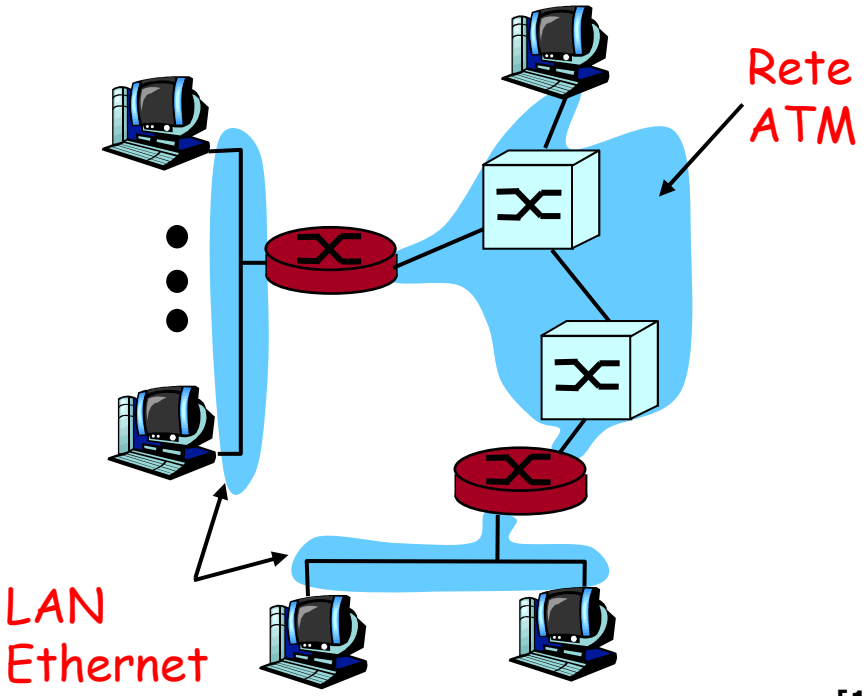
Solo IP

- 3 “reti” (es., segmenti LAN).
- MAC (802.3) e indirizzi IP.

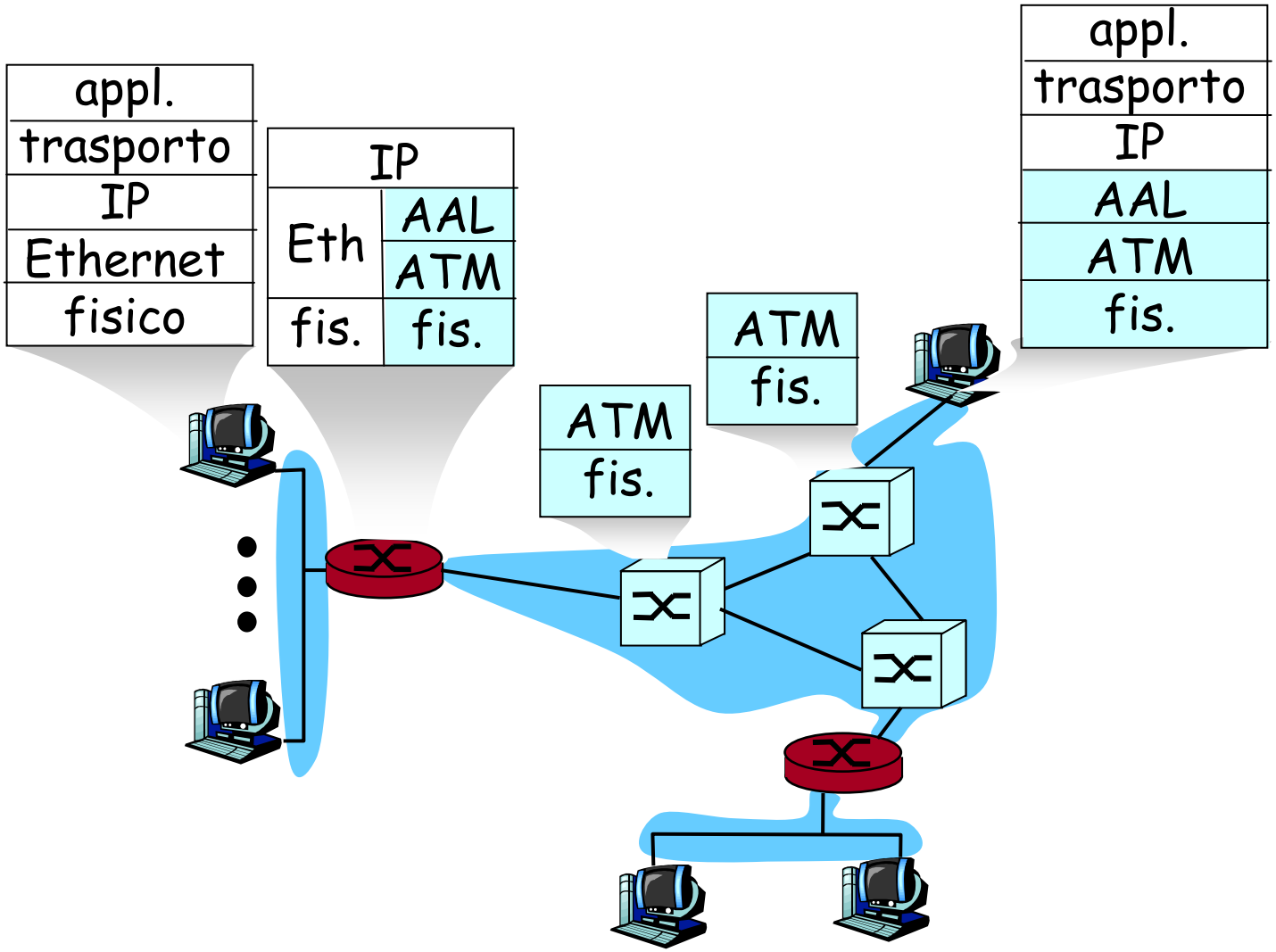


IP su ATM

- Sostituisce “le reti” (es., segmento LAN) con la rete ATM .
- Indirizzi ATM e indirizzi IP.



IP su ATM

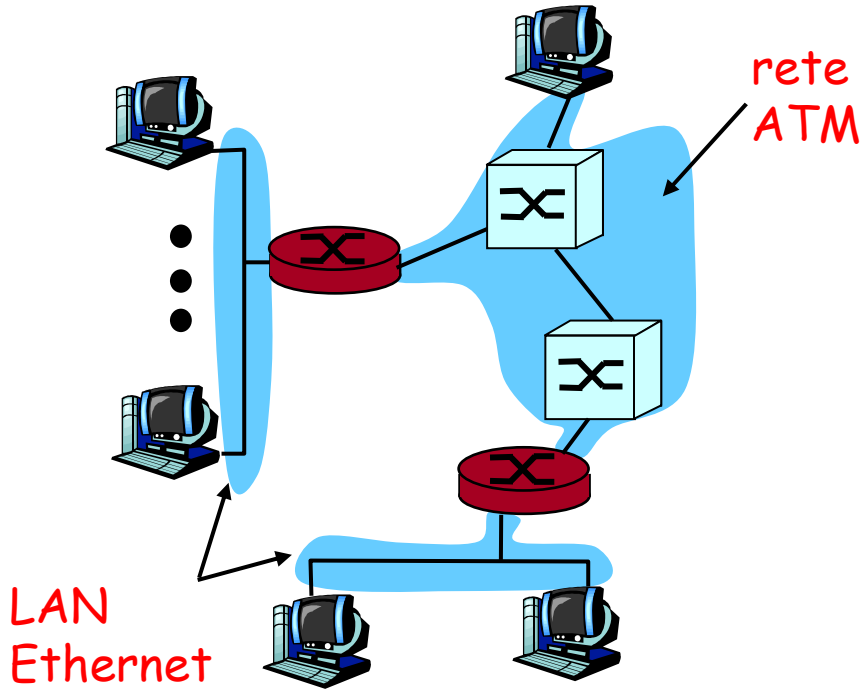

appl.
trasporto
IP
Ethernet
fisico
IP
Eth
AAL
ATM
fis.
fis.
ATM
fis.
ATM
fis.
appl.
trasporto
IP
AAL
ATM
fis.

Viaggio di un datagramma in IP su ATM

- Router d'ingresso:
  - Esamina l'indirizzo di destinazione, indicizza la tabella d'instradamento e determina l'indirizzo IP del router successivo sul percorso del datagramma.
  - Per determinare l'indirizzo fisico del router del prossimo hop, utilizza ARP (nel caso dell'interfaccia ATM, il router d'ingresso indicizza una tabella ATM ARP con l'indirizzo IP del router d'uscita e ne determina l'indirizzo ATM.
  - L'IP nel router d'ingresso trasferisce il datagramma e l'indirizzo ATM del router di uscita al livello di link sottostante, cioè ad ATM.
- Rete ATM: trasporta le celle al ricevente lungo il VC.
- Router di uscita:
  - AAL5 riassembla le celle nel datagramma originale.
  - Se CRC è OK, il datagramma è passato a IP.

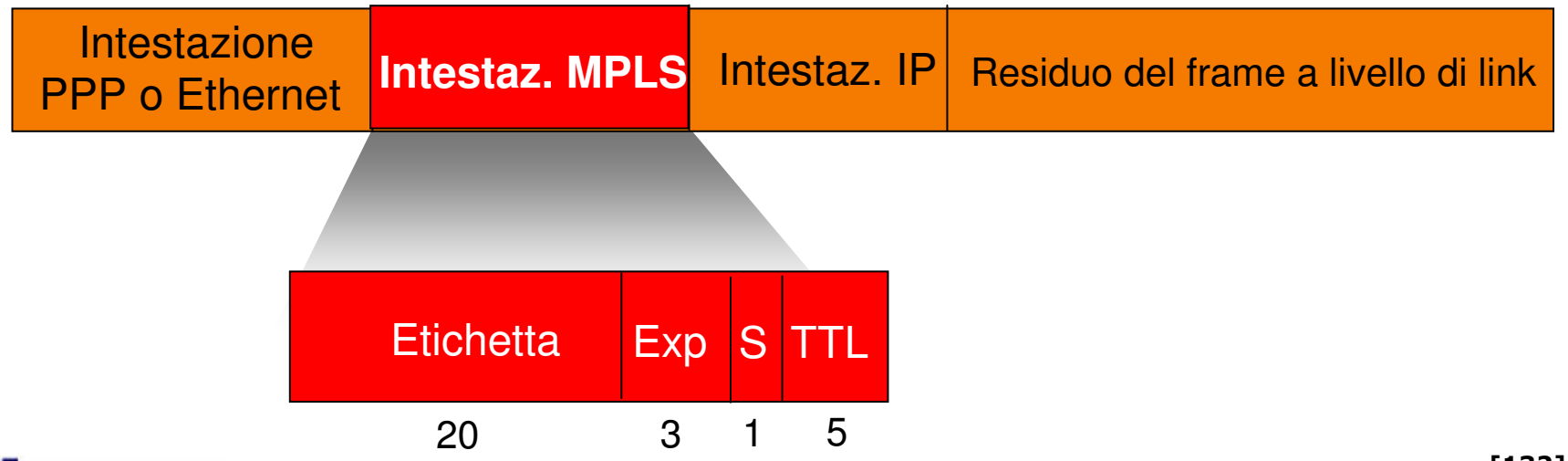
IP su ATM

- Datagrammi IP nelle PDU ATM AAL5
- Da indirizzo IP a indirizzo ATM
  - Proprio come da indirizzi IP a indirizzi MAC 802.3!



Multiprotocol label switching (MPLS)

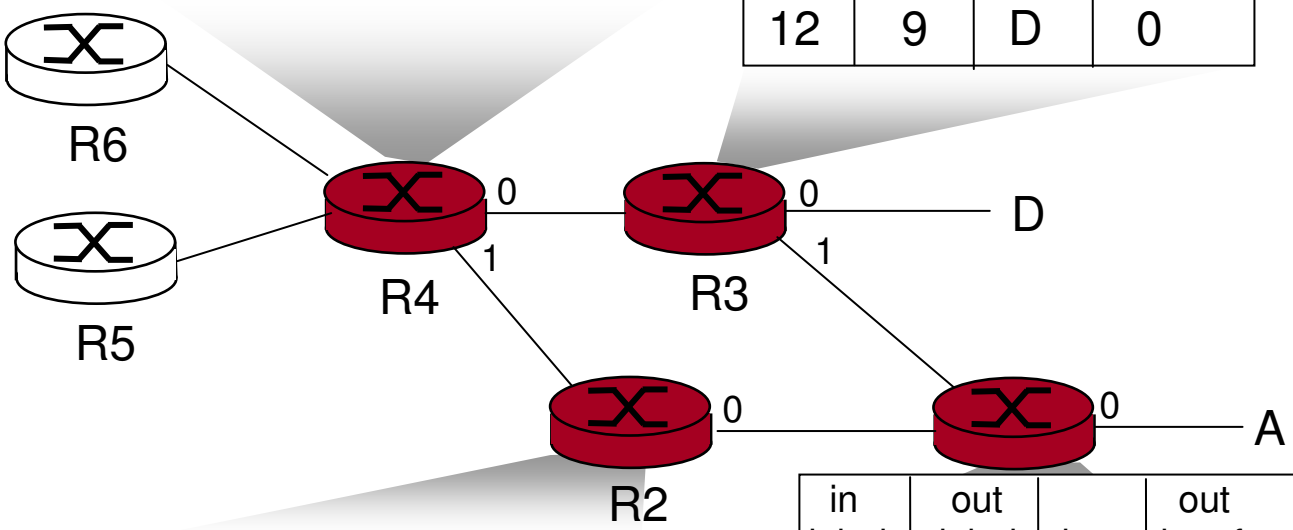
- Obiettivo iniziale: velocizzare l'inoltro IP usando un'etichetta di lunghezza stabilita (invece degli indirizzi di destinazione IP)
  - L'idea viene presa a prestito dall'approccio del VC
  - Ma i datagrammi IP mantengono ancora l'indirizzo IP!



Router MPLS: router a commutazione di etichetta

- Detti anche “label-switched router”
- Inviano i pacchetti MPLS analizzando l’etichetta MPLS nella tabella d’instradamento, passando immediatamente il datagramma all’appropriata interfaccia
  - Tabelle d’instradamento MPLS ≠ Tabelle d’instradamento IP
- Necessità di un protocollo utilizzato per distribuire etichette tra i router MPLS
  - RSVP-TE, un’estensione del protocollo RSVP
  - Consente l’invio di pacchetti lungo rotte che non potrebbero essere utilizzate con i protocolli d’instradamento IP standard!!
  - utilizza MPLS per il “traffic engineering”
- Devono coesistere con i router “solo-IP”

Tabelle d'instradamento MPLS



in label	out label	dest	out interface
	10	A	0
	12	D	0
	8	A	1

in label	out label	dest	out interface
10	6	A	1
12	9	D	0

in label	out label	dest	out interface
8	6	A	0

in label	out label	dest	out interface
6	-	A	0

Rappresentazione polinomiale e bits

Slides Informative

Rappresentazione polinomiale di sequenze di bit

- Una sequenza di N bit puo' essere rappresentata tramite un polinomio a coefficienti binari, di grado pari a N-1, tale che i suoi coefficienti siano uguali ai valori dei bit della sequenza
- Il bit piu' a sinistra rappresenta il coefficiente del termine di grado N-1, mentre il bit piu' a destra rappresenta il termine noto (di grado 0)
- Ad esempio, la sequenza 1001011011 puo' essere rappresentata dal polinomio

$$x^9 + x^6 + x^4 + x^3 + x + 1$$

- Il grado del polinomio e' determinato dal primo bit a sinistra di valore 1 presente nella sequenza

Aritmetica dei polinomi in modulo 2

- L'aritmetica dei polinomi a coefficienti binari si gestisce con le regole della aritmetica modulo 2:
  - le somme e le sottrazioni non prevedono riporti; sono pertanto coincidenti ed equivalenti all'OR esclusivo:

$$\begin{array}{r} 10011011\ + \\ 11001010\ = \\ \hline 01010001 \end{array} \qquad \begin{array}{r} 00110011\ + \\ 11001101\ = \\ \hline 11111110 \end{array}$$

  - le divisioni sono eseguite normalmente, tranne che le sottrazioni seguono la regola sopra detta; in questi termini, il divisore "sta" nel dividendo quando il dividendo ha grado maggiore o uguale al divisore, mentre non si puo' dividere quando il dividendo ha grado inferiore al divisore

Divisione binaria di polinomi

- Ad esempio:

$$\frac{x^6 + x^3 + x^2 + 1}{x^2 + x} =$$

$$x^4 + x^3 + x^2 + 1$$

con resto $x + 1$

```
1 0 0 1 1 0 1 | 1 1 0
1 1 0         |-------
≠ 1 0 1       | 1 1 1 0 1
  1 1 0       |
  ≠ 1 1 1     |
    1 1 0     |
    ≠ 0 1 0   |
      0 0 0   |
      ≠ 1 0 1 |
        1 1 0 |
        ≠ 1 1 |
```

risultato

resto

TechnoLabs

Codifica polinomiale (CRC)

- La tecnica consiste nel considerare i dati (m bit) da inviare come un polinomio di grado m-1
- Trasmettitore e ricevitore si accordano sull'utilizzo di un polinomio generatore G(x) di grado r
- Il trasmettitore aggiunge in coda al messaggio una sequenza di bit di controllo (CRC) in modo che il polinomio associato ai bit del frame trasmesso, costituito dall'insieme di dati e CRC, sia divisibile per G(x)
  - e' sempre possibile trovare tale polinomio
- In ricezione si divide il polinomio associato ai dati ricevuti per G(X)
  - se la divisione ha resto nullo, si assume che la trasmissione sia avvenuta senza errori
  - se la divisione ha resto non nullo, sono certamente avvenuti errori

Codifica polinomiale (cont.)

- Dal punto di vista logico, la generazione del codice CRC avviene nel seguente modo:
  - Sia M(x) il polinomio associato agli m bit di dati
  - Sia G(x) il polinomio generatore di grado r
  - Si aggiungono r bit a valore 0 in fondo ai bit di dati; il polinomio associato all'insieme di m+r bit è quindi $x^r M(x)$
  - Si calcola il resto della divisione $x^r M(x)/G(x)$, che sara' un polinomio R(x) di grado inferiore ad r, quindi rappresentativo di una sequenza di r bit
  - Si costruisce la sequenza di bit associata al polinomio $T(x) = x^r M(x)-R(x)$, che equivale ad aggiungere i bit corrispondenti a R(x) in coda ai dati da inviare: vanno riportati tutti gli r bit associati ad R(x), quindi anche eventuali zeri in testa al resto; questa e' una sequenza di m+r bit
  - E' evidente che il polinomio T(x) risultera' divisibile per G(x) con resto nullo

Esempio di calcolo di CRC

- Supponiamo di voler trasmettere con CRC la sequenza 1101011011, utilizzando il polinomio generatore

$$x^4 + x + 1$$

  equivalente alla sequenza di bit 10011
- Si costruisce la sequenza 11010110110000, e la si divide per 10011
- Il resto della divisione è 1110
- Il frame che verrà trasmesso sarà quindi 11010110111110
- In ricezione si divide la sequenza ricevuta per lo stesso polinomio, e si verifica che il resto sia nullo

Caratteristiche del polinomio generatore

- Le caratteristiche del polinomio generatore determinano quali errori saranno rilevabili e quali invece potranno passare inosservati
- Detto T(x) il polinomio associato al frame trasmesso, il polinomio associato al frame ricevuto puo' essere espresso come T(x)+E(x), dove E(x) avrà coefficiente 1 per ogni bit che è stato modificato da errori trasmissivi
- Risulta chiaro che un errore passerà inosservato solo se T(x)+E(x) sarà divisibile per G(x), ma essendo per definizione T(x)/G(x) = 0, l'errore passerà inosservato se E(x) sarà divisibile per G(x)

Polinomi standard

- Viste le caratteristiche dei polinomi, si sono identificati diversi polinomi opportuni per rendere molto improbabile la mancata rilevazione di errori
- I più comuni a 16 bit sono

$$x^{16} + x^{15} + x^{2} + 1 \qquad \textbf{CRC - 16}$$
$$x^{16} + x^{12} + x^{5} + 1 \qquad \textbf{CRC - CCITT}$$

- Un polinomio standard a 32 bit utilizzato in molte applicazioni (tra cui IEEE 802) e' il CRC-32:

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

Capitolo 5: riassunto

- Principi per implementare i servizi di trasmissione dati:
  - Rilevazione e correzione dell'errore
  - Condivisione di un canale broadcast: accesso multiplo
  - Indirizzamento a livello di link
- Implementazione di varie tecnologie al livello di link:
  - Ethernet
  - LAN commutate
  - PPP
  - Reti virtuali: ATM, MPLS