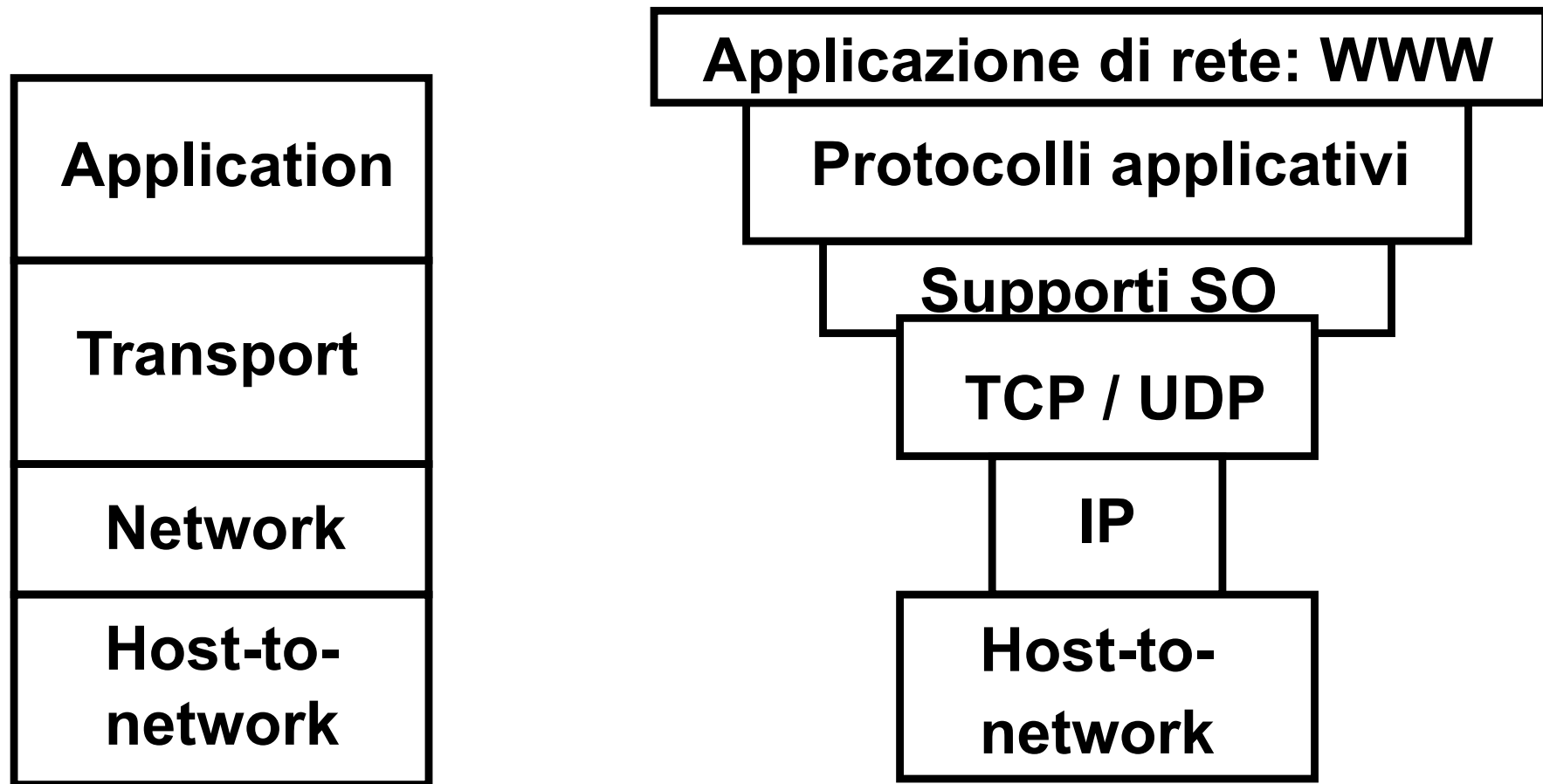


LIVELLO HOST-TO-NETWORK (H2N)

Ethernet

Livello h2n



Scopo del livello h2n

- Il livello host-to-network affronta le problematiche di:
 - **interconnessione** tra due o più host
 - **trasmissione dati** tra host direttamente connessi
 - **connessione** di un host a Internet
- Nello stack TCP/IP (non nello stack ISO/OSI), la modalità di interconnessione, la relativa tecnologia e i protocolli per la trasmissione dati tra host interconnessi sono tra loro **strettamente dipendenti**
→ **la scelta dell'uno implica la scelta dell'altro**

Esempi

- **LAN wired**
 - *Ethernet* (standard de facto)
 - *Token-ring*
 - *FDDI*
 - *Frame relay*
- **LAN wireless**
 - *802.11x* ($x = a, b, g, n, c, \dots$)
- **PAN**
 - *Bluetooth*
 - *ZigBee*
- **Mediante modem**
 - *SLIP*
 - *PPP*
- **WAN wireless**
 - *GSM*
 - *UMTS*
 - *LTE*

Premessa importante per protocolli h2n

- **I servizi offerti da differenti protocolli h2n possono essere diversi**
 - Un protocollo può garantire l'affidabilità della consegna del pacchetto e un altro no
 - Il livello network, quindi, deve essere in grado di compiere il suo lavoro *end-to-end* in presenza di differenti insiemi di servizi forniti da specifici protocolli h2n

Definizioni: *Modalità di trasmissione*

- **Unicast:** comunicazione fra un singolo mittente e un singolo ricevente
- **Multicast:** comunicazione fra un singolo mittente e un gruppo di riceventi
- **Anycast:** comunicazione fra un singolo mittente ed almeno un ricevente in un gruppo
- **Broadcast:** comunicazione fra un singolo mittente e tutti gli altri nodi

Definizioni: *Tipi di collegamento*

- **Collegamento broadcast / condiviso**
 - Molti host connessi a uno stesso canale di comunicazione
 - E' necessario un protocollo di accesso al mezzo per coordinare le trasmissioni e per evitare le collisioni (chi può trasmettere?), ovvero per risolvere le eventuali collisioni
 - Sono comuni nelle LAN, WirelessLAN, reti satellitari
- **Collegamento punto-punto**
 - Costituito da un unico trasmittente a un'estremità del collegamento e da un unico ricevente all'altra estremità
 - E' il tipico collegamento fra due router o fra un modem di un accesso residenziale e il router dell'*Internet Service Provider* (ISP o *Provider*)

Collegamenti punto-punto half- e ful-duplex

- **Collegamento Half-Duplex**

- Collegamento che permette solo a un partecipante di comunicare sul mezzo fisico in un istante di tempo
- Quasi sempre inteso in modo ancora più stringente come comunicazione unidirezionale

- **Collegamento Full-Duplex**

- Possibilità per il mittente e il destinatario di comunicare in modo indipendente l'uno dall'altro
- Ad esempio, collegamento punto-punto con collegamenti interni dedicati per le due direzioni di trasferimento

Attenzione

Attenzione a distinguere le modalità di trasmissione e le caratteristiche del mezzo trasmissivo

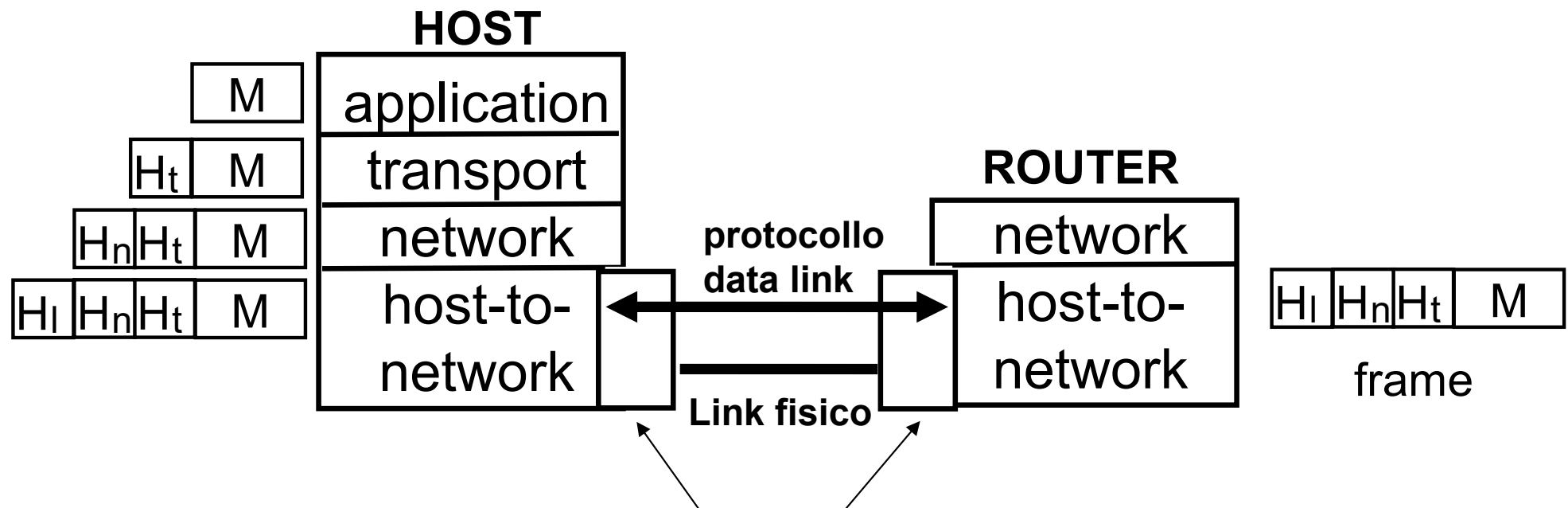
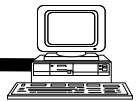
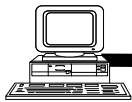
- Il protocollo H2N è solitamente progettato per un particolare mezzo trasmissivo, che potrebbe essere intrinsecamente broadcast o unicast
- A prescindere dal mezzo, il protocollo può prevedere molteplici modalità di trasmissione: broadcast, multicast, unicast, ...
- A breve discuteremo un esempio con Ethernet

Possibili servizi offerti dal livello h2n

- **Livello 1 (“fisico”)**
 - *Connessione di host secondo diversi mezzi trasmissivi (doppino, cavo coassiale, fibra ottica, trasmissione radio, modem)*
- **Livello 2 (“data link”)**
 - Framing (*incapsulamento in frame*)
 - Accesso multiplo al link (es., CSMA/CD)
 - Recapito affidabile (acknowledgement e ritrasmissione)
 - Controllo di flusso
 - Ricerca di errori
 - Correzione degli errori
 - Half-duplex o Full-duplex

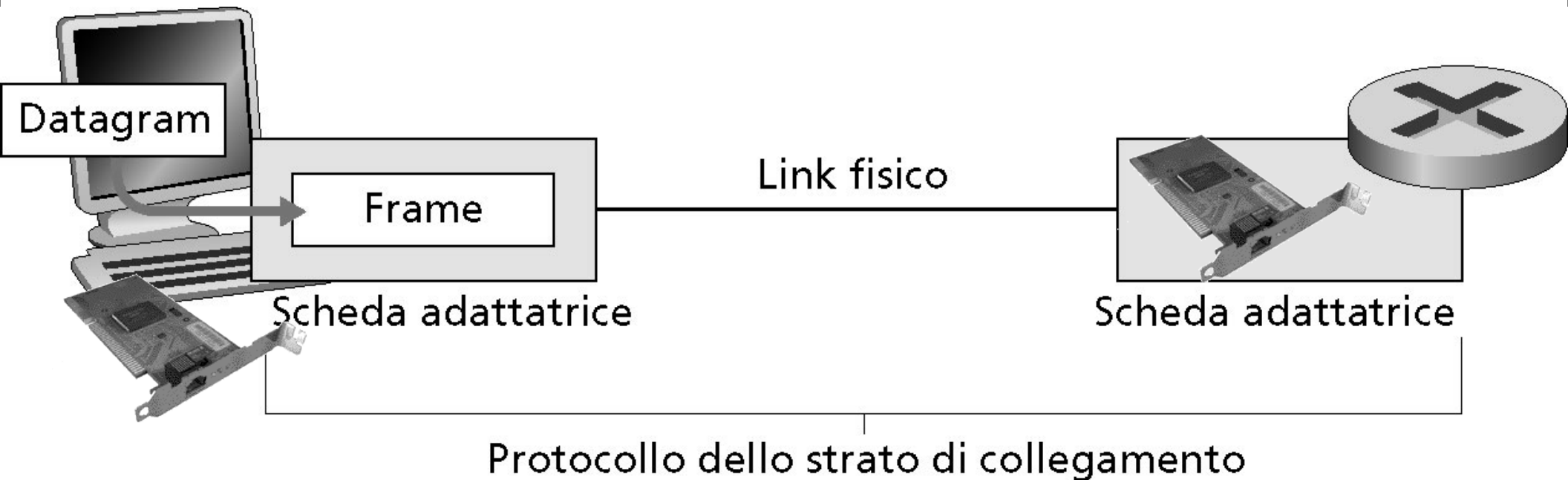
Collegamenti del livello h2n

- Due dispositivi connessi “fisicamente”:
host-router/switch, router/switch-router/switch, host-host
- Unità di dato trasmesso: frame



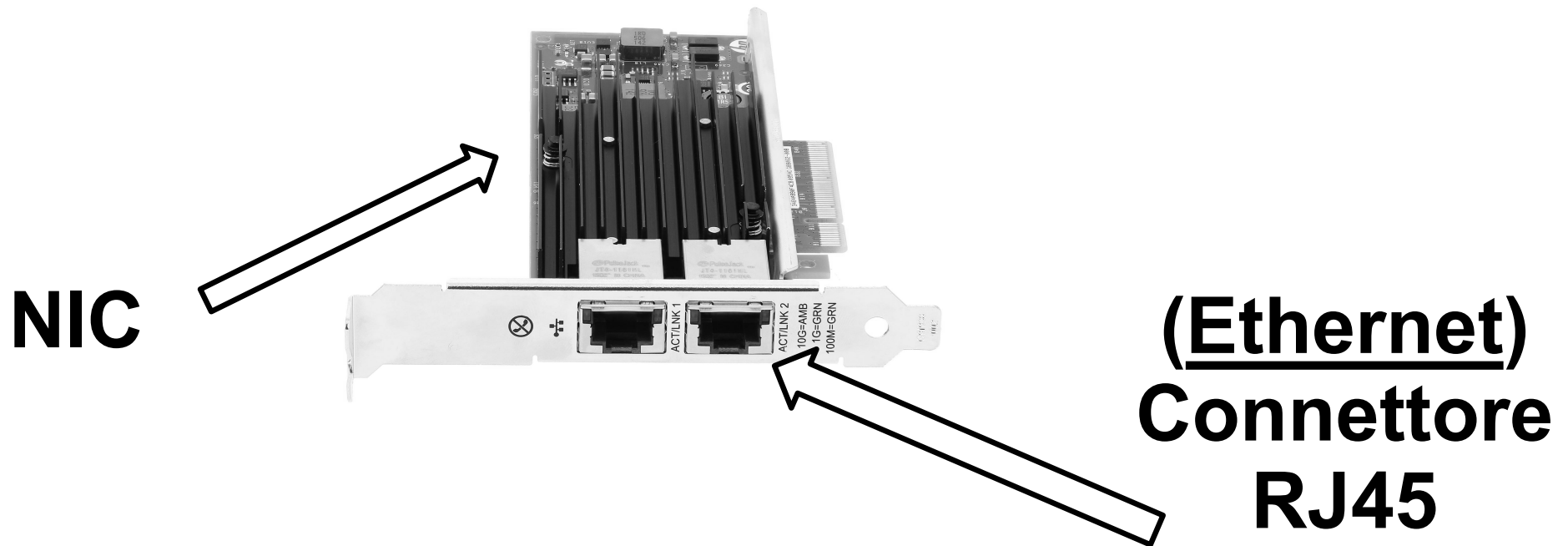
Adattatori per la comunicazione H2N

- Il protocollo h2n è solitamente implementato all'interno di una **scheda adattatrice**, conosciuta anche col nome di **Network Interface Card** o **NIC**
- Tutti i dispositivi (host, router, altri dispositivi di rete), per poter essere utilizzati in una rete LAN, devono essere dotati di una scheda di rete



Network Interface Card (NIC)

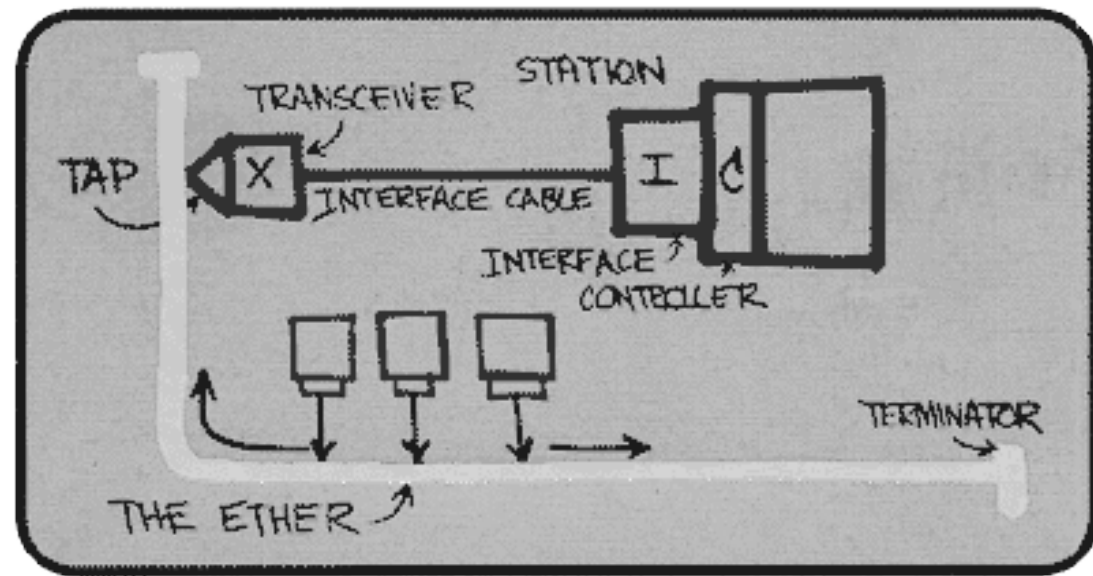
- Dispositivo generalmente costituito da una RAM, un **DSP** (Digital Signal Processor), un'interfaccia bus/host e un'interfaccia di collegamento alla rete
- **Entità semi-autonoma** rispetto al sistema in cui risiede
- Può essere sia integrata sulla scheda madre, oppure presente come dispositivo dedicato



Ethernet

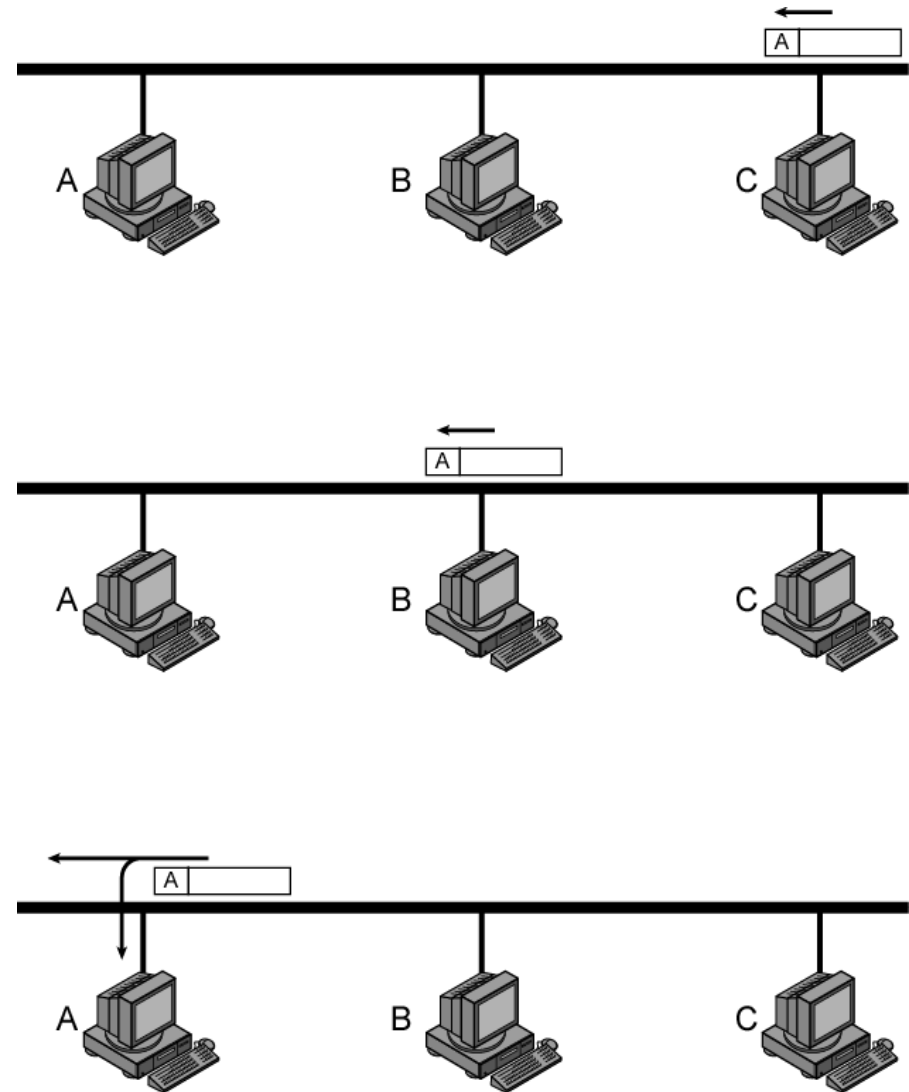
Ethernet: *standard de facto*

- Oggi posizione dominante sul mercato
- Inventata a metà degli anni '70 da **Metcalfe** che propone ***Ethernet*** nella sua tesi di PhD
- Il disegno originale prevedeva **un solo canale di tipo *bus*** per connettere i nodi



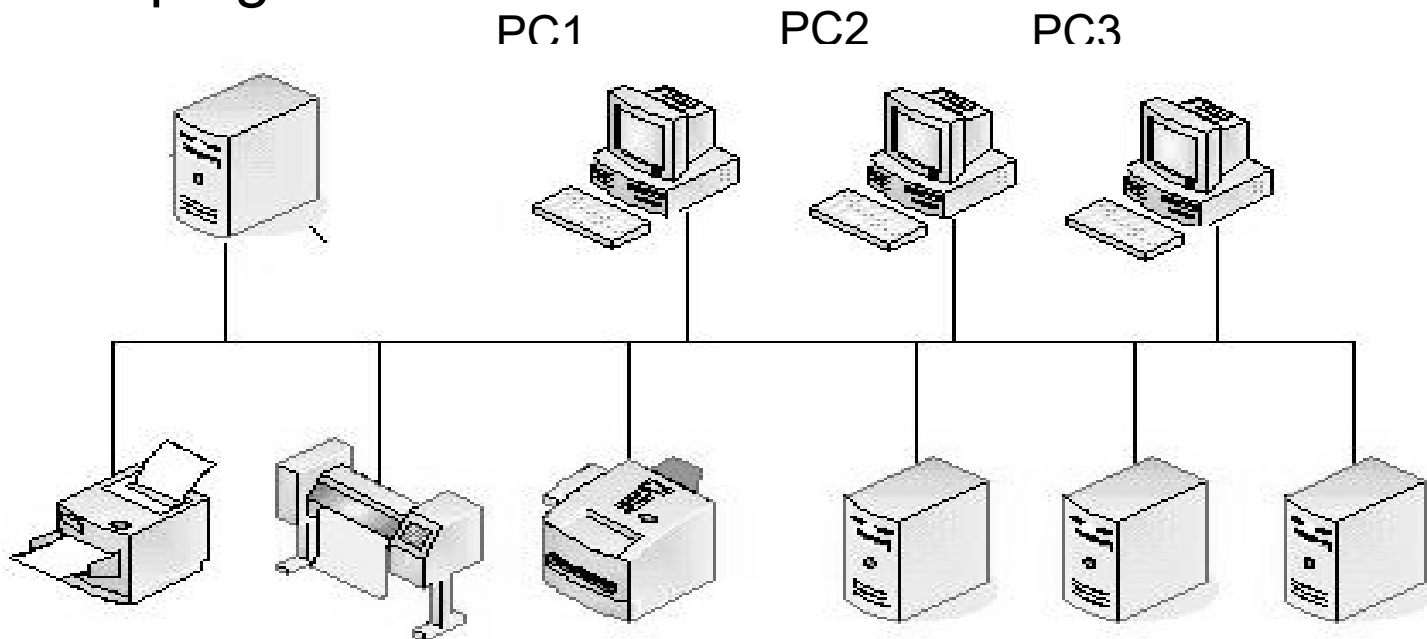
Modalità per trasmissione su bus

1. L'host C si appresta a spedire un frame a A
2. L'host B riceve il frame, ma non essendo diretto a lui, lo ignora
3. L'host A riceve il frame e non lo ignora (frame passato ai livelli superiori dello stack). Il frame continua comunque a viaggiare sul bus



LAN Ethernet

- Ethernet è stato pensato **in origine** per
 - topologia a bus
 - velocità 1-10Mbps
- **Attualmente** utilizzato
 - quasi sempre in topologia a stella tramite l'impiego di ulteriori dispositivi di rete (bridge e switch)
 - supporta velocità differenti (anche decine di Gb/s) a seconda dell'HW impiegato



Reti Ethernet e Tipologie di Cavo

- Il supporto a determinate velocità di Ethernet dipende dalle interfacce di rete, ma anche dal **tipo di collegamenti**
 - Per le reti Ethernet ancora più veloci o per distanze più ampie si passa all'uso di fibra ottica

Ethernet Cable Comparison Chart			
Category	Shielded	Max. Transmission	Max. Bandwidth
Cat 3	No	10 Mbps at 100m	16 MHz
Cat 5	No	10/100 Mbps at 100m	100 MHz
Cat 5e	No	1 Gbps at 100m	100 MHz
Cat 6	Yes & No	1 Gbps at 100m	250 MHz
Cat 6a	Yes	10 Gbps at 100m	500 MHz
Cat 7	Yes	10 Gbps at 100m	600 MHz
Cat 7a	Yes	10 Gbps at 100m	1000 MHz
Cat 8	Yes	25 Gbps/40 Gbps	2000 MHz at 30m

Motivi del successo di Ethernet

- Relativamente **poco costosa** (soprattutto rispetto ad altre tecnologie proprietarie)
- Funziona bene e si integra perfettamente con i protocolli IP e TCP
- E' molto flessibile e si presta a diverse:
 - ***topologie (modo di connettere gli host della rete)***
 - ***tecnologie (tecnologia del mezzo trasmissivo usato per le connessioni)***
- La **rapida diffusione iniziale** di Ethernet ha ostacolato l'uscita di successive tecnologie concorrenti (FDDI, ATM)

Caratteristiche Ethernet

- **Tipo di collegamento**

- Usa un ***Canale di broadcast*** (non punto-punto): molti host connessi ad uno stesso canale di comunicazione
- Quando un host trasmette un pacchetto sulla LAN, TUTTE le interfacce degli host collegati lo ricevono

- **Modalità di trasmissione**

- Permette comunicazioni ***Unicast*** fra host
- Alcuni messaggi “speciali”, necessari per il corretto funzionamento del protocollo, sono di tipo ***Broadcast***

Sommario

Ethernet

- a. Indirizzi Ethernet: MAC
- b. Frame Ethernet
- c. Protocollo ARP
- d. Accesso al mezzo condiviso
(Protocollo CSMA/CD)

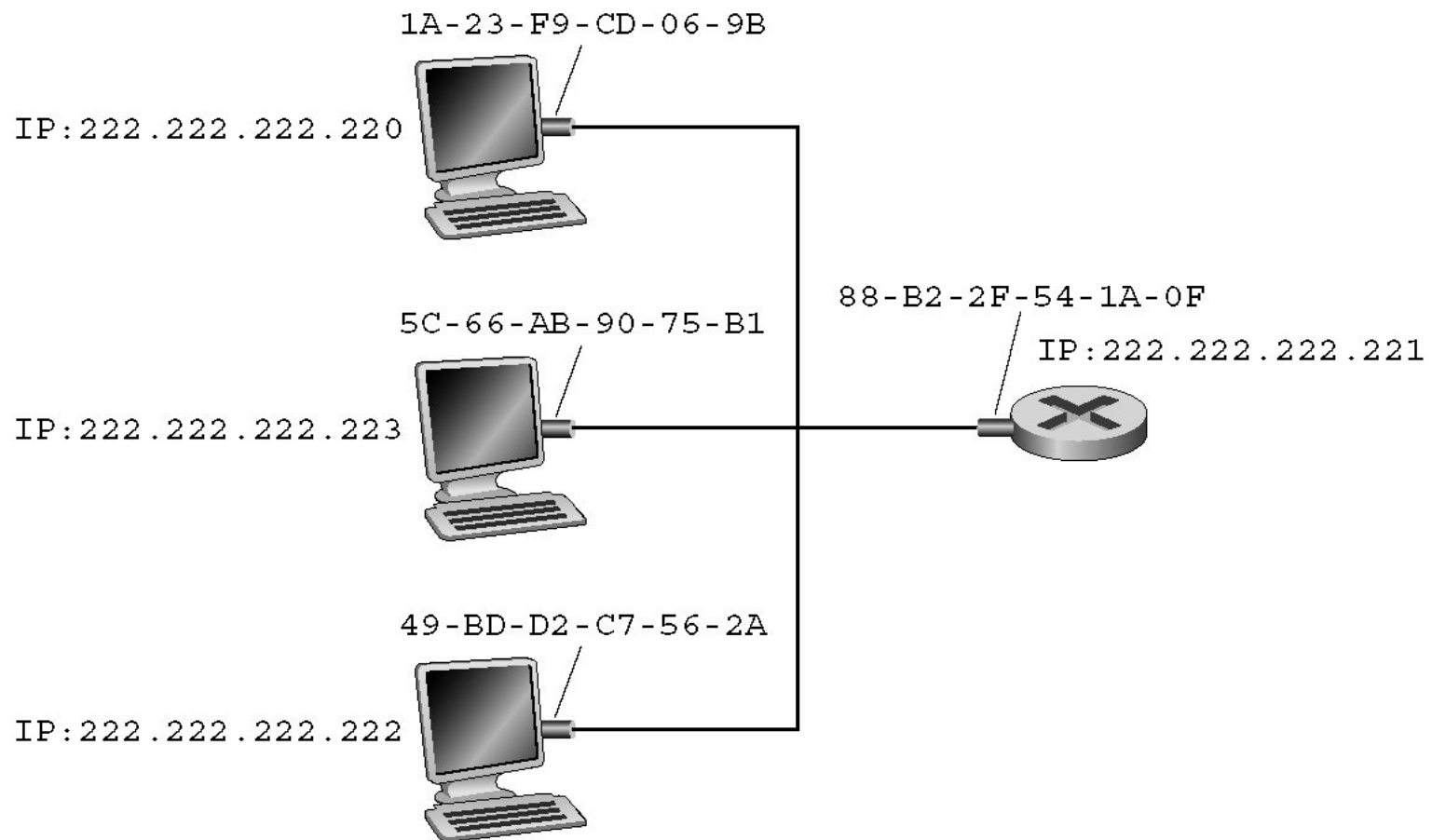
Indirizzi Ethernet: MAC

Indirizzi MAC

- A livello Ethernet, gli host utilizzano un **indirizzo hardware** o **indirizzo MAC** (*Media Access Control*)
- In realtà, l'indirizzo MAC non si riferisce all'host, ma al **NIC** (**Network Interface Card**) dell'host. Ogni NIC ha un indirizzo LAN **univoco** di 48 bit, tipicamente rappresentato da 6 coppie di numeri esadecimali. Es., **81:F4:A3:AA:9C:49**
- L'indirizzo broadcast è FF-FF-FF-FF-FF-FF (tutti i bit a 1)
- L'indirizzo MAC di un NIC è **univoco** e **permanente**:
 - è chiamato anche *hardware address* perché incorporato nella ROM al momento della fabbricazione (però è meglio non fidarsi dell'autenticazione di un computer basandosi sul MAC ...)
 - univoco in quanto assegnato ai produttori di NIC (Network Interface Card) dall'autorità centrale IEEE (però, certi produttori taiwanesi non si preoccupano di chiedere e pagare l'IEEE...)

Indirizzi di un host

Ciascun host di una LAN ha un indirizzo IP e il NIC di ciascun host e dispositivo di rete ha un indirizzo MAC



Utilizzo indirizzo MAC

- Quando un host vuole trasmettere, inserisce nel frame l'indirizzo MAC del destinatario e lo immette nella LAN (che è un canale di broadcast)
- Se l'indirizzo di destinazione del frame corrisponde all'indirizzo MAC dell'host ricevente, il NIC dell'host accetta il frame e lo passa al sistema operativo dell'host che gestisce gli altri livelli dello stack TCP/IP
- Se l'indirizzo di destinazione del frame non corrisponde all'indirizzo MAC del NIC, il NIC scarta il pacchetto senza coinvolgere il sistema operativo (*a meno che sull'host non sia caricato un software di sniffing*)

Esempio

Indirizzo IP

Indirizzo MAC

```
# ifconfig eth0
```

```
eth0 Link encap:Ethernet HWaddr 00:10:5A:9D:88:AF
```

```
inet addr:192.168.1.3 Bcast:192.168.1.255
```

```
Mask:255.255.255.0
```

```
UP BROADCAST RUNNING MULTICAST MTU:1500
```

```
Metric:1
```

```
RX packets:92 errors:0 dropped:0 overruns:0 frame:0
```

```
TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
```

```
RX bytes:14162 (13.8 KiB) TX bytes:6744 (6.5 KiB)
```

```
Interrupt:9 Base address:0xfc00
```

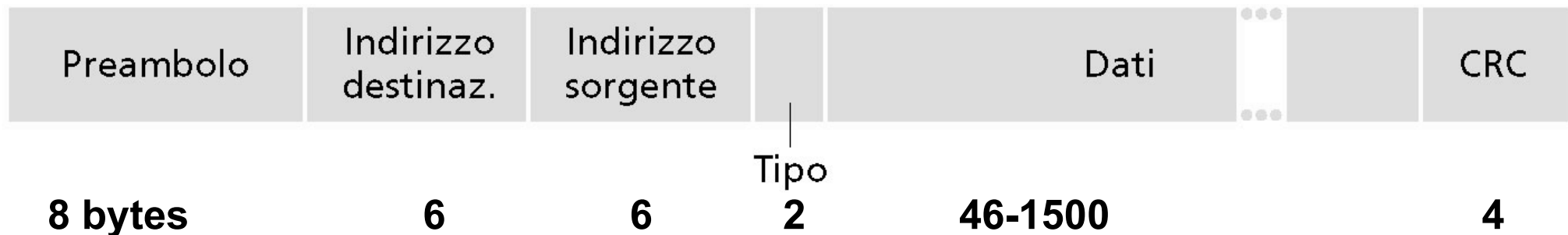
Perché l'indirizzo IP non basta?

- **Se i NIC usassero indirizzi IP invece che indirizzi MAC “indipendenti”:**
 - non sarebbero in grado di supportare altri protocolli di rete differenti da IP
 - gli indirizzi IP dovrebbero essere registrati nella memoria del NIC → riconfigurati ad ogni spostamento dell'host in un'altra rete
- **Se i NIC non utilizzassero alcun indirizzo:**
 - ogni pacchetto ricevuto verrebbe passato dal NIC all'host su cui risiede per verificare la concordanza dell'indirizzo IP
→ i sistemi operativi degli host sarebbero interrotti da ogni pacchetto in transito sulla LAN anche se non diretto a loro!

Frame Ethernet

Frame Ethernet

- I pacchetti scambiati a livello h2n vengono detti **frame**
- Indipendentemente dalla topologia, dai mezzi trasmissivi e dalla velocità di trasmissione, tutte le tecnologie Ethernet fanno uso dello stesso formato per il frame che trasmettono (**Frame Ethernet**)



Preambolo

- Campo **preambolo** (8 byte)
- I primi 7 byte hanno valore 10101010
- L'ultimo byte ha valore 10101011
- I primi 7 byte servono per “attivare” gli adattatori dei riceventi e sincronizzare i loro orologi con quello del mittente (sincronizzazione necessaria a causa dei tassi di trasmissione diversi da quelli nominali)
- I due 1 consecutivi nell'ultimo byte avvisano l'adattatore del ricevente che la fase di sincronizzazione è terminata e sta arrivando il contenuto vero e proprio del frame

Indirizzo destinazione e sorgente

- **Campi indirizzo di destinazione (6 byte) e indirizzo sorgente (6 byte)**
- Contengono l'indirizzo MAC di sorgente e destinazione
- Quando un NIC riceve un frame Ethernet con indirizzo di destinazione diverso dal proprio indirizzo MAC, o dall'indirizzo broadcast della LAN, lo scarta. Altrimenti, passa il contenuto del campo dati allo strato di rete

Tipo

- Campo **tipo** (2 byte)
- Permette a Ethernet di **multiplexare** i protocolli del livello di rete
- Gli host potrebbero supportare protocolli dello strato di rete diversi da IP (es., Novell IPX, AppleTalk)
- Gli host supportano i protocolli ARP e RARP
- Il campo tipo serve all'adattatore per sapere a quale dei protocolli dello strato di rete debba essere passato il campo dati di ciascun frame ricevuto

Dati (e dimensione)

- Contiene i dati reali (**datagramma IP**)
- L'unità massima trasferibile (**MTU - Maximum Transfer Unit**) per Ethernet è 1500 byte
 - Se i dati superano i 1500 byte, devono essere frammentati (si vedrà in seguito)
- La dimensione minima del campo dati è 46 byte
 - Se la dimensione dei dati è inferiore a 46 byte, il campo dati deve essere “completato” (**stuffing**) fino a 46 byte con byte di riempimento (che verranno rimossi all'atto della ricezione)

CRC

- **CRC = Controllo a Ridondanza Ciclica** (4 byte)
- **Scopo** = permettere all'adattatore che riceve i dati di rilevare la presenza di un errore nei bit del frame ricevuto
- Quando un host trasmette il frame calcola un campo CRC, che ottiene dalla correlazione degli altri bit del frame (escluso il preambolo)
- Quando un host riceve il frame ricalcola il CRC utilizzando la stessa funzione e vede se corrisponde
 - Se no corrisponde, sa che c'è stato errore
 - Se corrisponde? Assume che il frame sia corretto

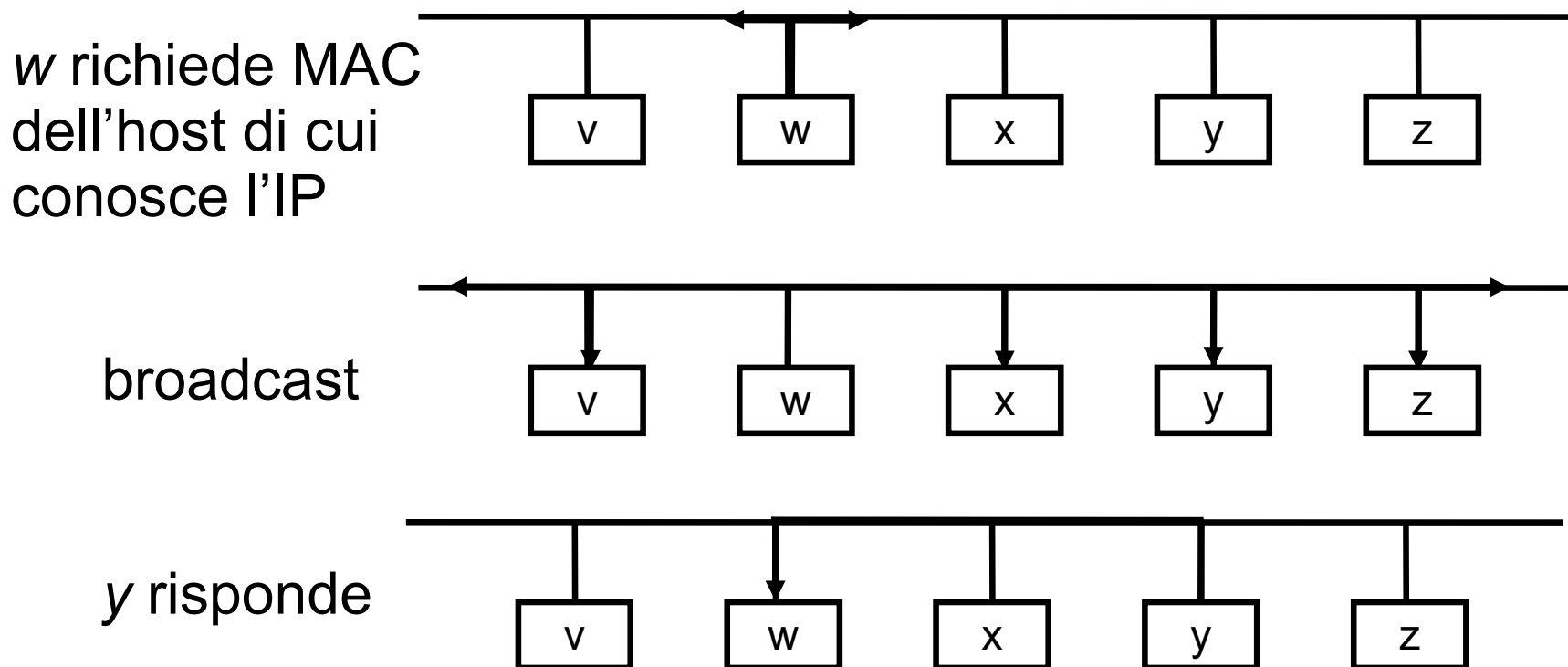
Protocollo ARP

Protocollo per la risoluzione indirizzi

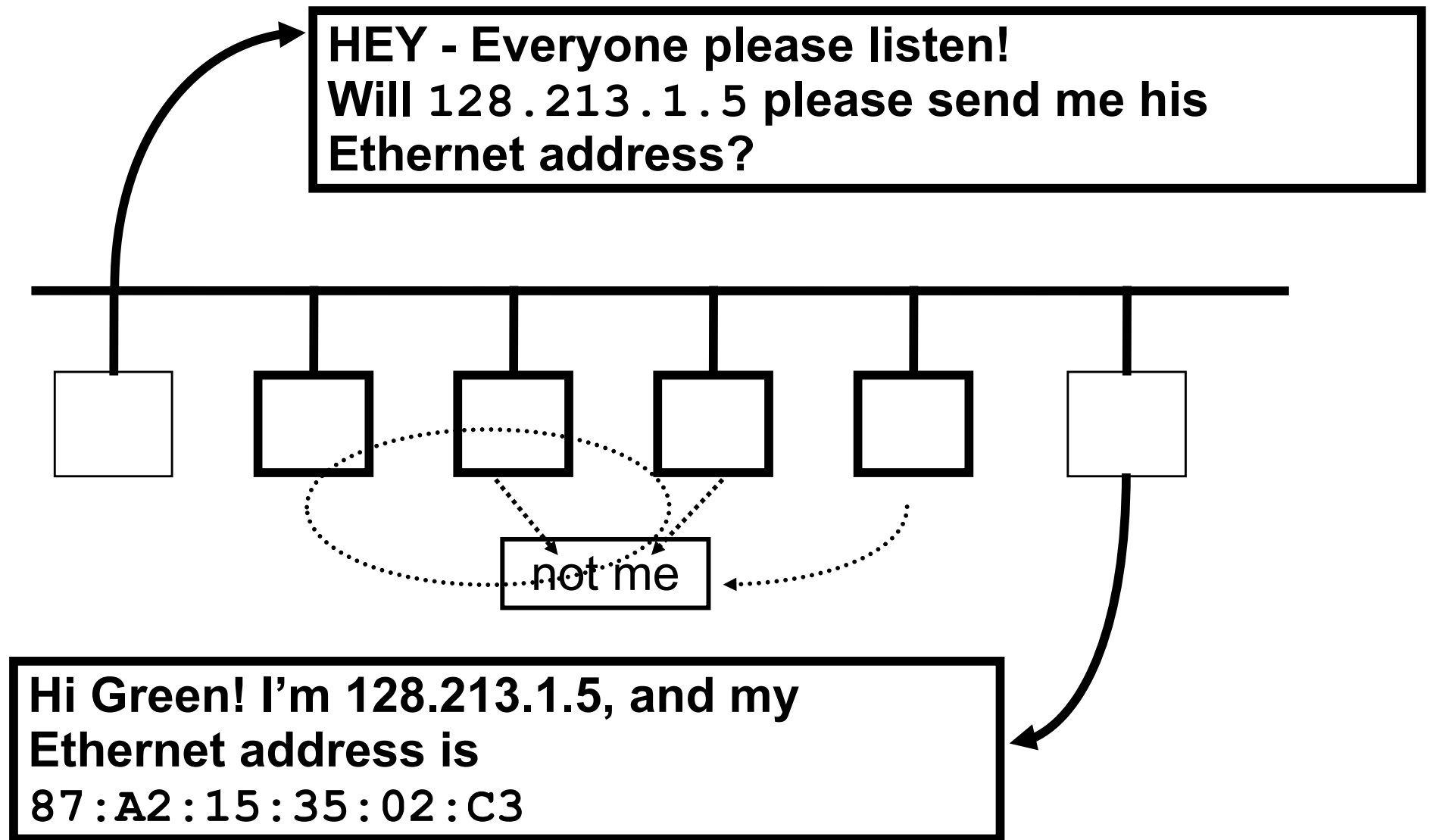
- Gli indirizzi IP non sono riconosciuti dall'hardware
 - Se conosciamo l'indirizzo IP di un host, come si può determinare il corrispondente indirizzo MAC?
- ➔ **L'Address Resolution Protocol (ARP)** si occupa di individuare l'indirizzo MAC di un host della stessa LAN di cui conosce l'indirizzo IP
- Il protocollo ARP è incluso nella suite di protocolli TCP/IP

Protocollo ARP

- Utilizza due tipi di messaggi ARP:
 - **richiesta** contenente l'indirizzo IP del destinatario
 - **risposta** contenente il corrispondente indirizzo MAC
- ARP utilizza il **broadcast della richiesta**



Conversazione ARP



Migliorare le prestazioni di ARP

- **Cache ARP:** per ridurre il traffico sulla rete causato dallo scambio di messaggi ARP:
 - ciascun host effettua un caching temporaneo delle risoluzioni IP/MAC nella sua **tabella di instradamento**
 - il mittente inserisce nella richiesta la corrispondenza fra il proprio indirizzo IP e quello MAC

Indirizzo IP	Indirizzo MAC	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Time To Live (per quanto tempo è valido)

Cache ARP

```
riccardo@chrysophylax:~$ sudo arp
```

Address	HWtype	Hwaddress	Flags	Mask	Iface
ns1.ing.unimo.it	ether	00:01:03:11:6B:63	C		eth0
info-gw.ing.unimo.it	ether	00:0A:57:05:A0:00		C	eth0

```
riccardo@chrysophylax:~$ ping brandy.ing.unimo.it
```

```
[...]
```

```
riccardo@chrysophylax:~$ sudo arp
```

Address	HWtype	Hwaddress	Flags	Mask	Iface
brandy.ing.unimo.it	ether	00:11:11:5A:EB:41	C		eth0
ns1.ing.unimo.it	ether	00:01:03:11:6B:63	C		eth0
info-gw.ing.unimo.it	ether	00:0A:57:05:A0:00	C		eth0

Ricordare il flusso di funzionamento di Ethernet

- Se l'input è l'indirizzo IP (come solito):
 1. Controllare se IP in tabella ARP locale
 2. Se assente o TTL scaduto, eseguire protocollo ARP per ottenere MAC address destinatario
 - Se scade timeout, assumo che il destinatario non sia presente nella rete Ethernet (non c'è una risposta esplicita negativa)
 3. Uso il MAC address ottenuto nel payload della risposta ARP come MAC address destinazione dei frame da inviare nella comunicazione
 - Periodicamente, il sistema esegue ARP per verificare la corrispondenza IP-MAC

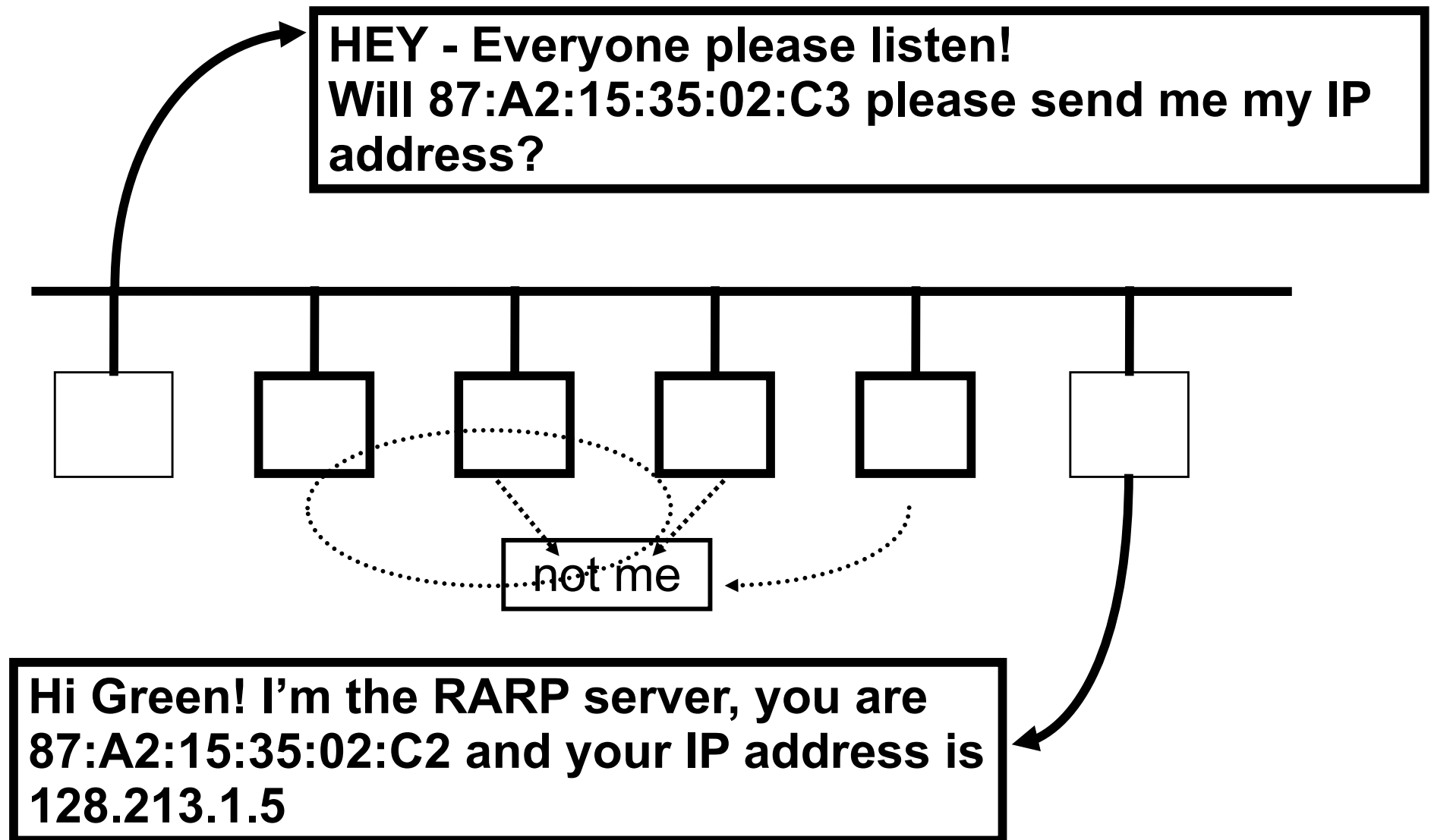
Note sul funzionamento di Ethernet

- Alcuni strumenti di debug possono fornire direttamente l'indirizzo MAC a cui inviare i frame Ethernet (in questi casi ovviamente non serve ARP)
- Durante una comunicazione con Ethernet, il SO solitamente esegue periodicamente il protocollo ARP «in parallelo» per aggiornare il TTL della entry del destinatario nella tabella ARP
- Nei sistemi reali è possibile modificare il comportamento di Ethernet, ad esempio:
 - Inserire manualmente delle entry permanenti nella tabella ARP
 - Disattivare completamente il protocollo ARP

Protocollo RARP (deprecato)

- **Reverse Address Resolution Protocol**
- Funzione opposta al protocollo ARP → Dato un indirizzo MAC, ricava l'indirizzo IP corrispondente
- Meccanismo analogo ad ARP
 - Broadcast di una richiesta
 - Solo l'host interessato risponde (in questo caso, il server RARP)
 - Struttura dei messaggi analoga a quella del protocollo ARP
- Utilizzabile anche in sistemi con host senza disco che conoscono soltanto il proprio indirizzo MAC
 - Quando un host senza disco entra in servizio chiede il proprio indirizzo IP
 - Un server RARP mantiene le coppie di indirizzi IP-MAC per gli host associati

Conversazione RARP



Pacchetti ARP/RARP

- Payload di 28 byte
- Hardware type (ht) tipo di protocollo livello fisico
 - Ethernet=1
- Network protocol type (pt) tipo di protocollo livello rete
 - IP=0x800
- Hardware address size (hs)
- Network protocol address size (ps)

- Operation (op)
 - 1 ARP richiesta
 - 2 ARP risposta
 - 3 RARP richiesta
 - 4 RARP risposta

Caso tipico: **IP su Ethernet**

- Sender hardware address (MAC)
- Sender network address (IP)
- Receiver hardware address
- Receiver network address

ht	pt	hs	ps	op	snd hw add	snd net	rcv hw add	rcv net
2	2	1	1	2	6 bytes	4	6 bytes	4

Accesso al mezzo trasmissivo (Protocollo CSMA/CD)

Protocollo di accesso multiplo

- I frame Ethernet vengono trasmessi dagli host collegati allo stesso segmento di LAN su un canale **condiviso broadcast** a bit rate elevato (**modalità di accesso multiplo**)
 - La spedizione contemporanea di più frame causa rischi di **collisione**
- ➔ E' necessario un **protocollo di accesso al mezzo** per coordinare le trasmissioni sul canale condiviso e evitare, se possibile, collisioni ovvero gestirle nel caso in cui non sia stato possibile evitarle

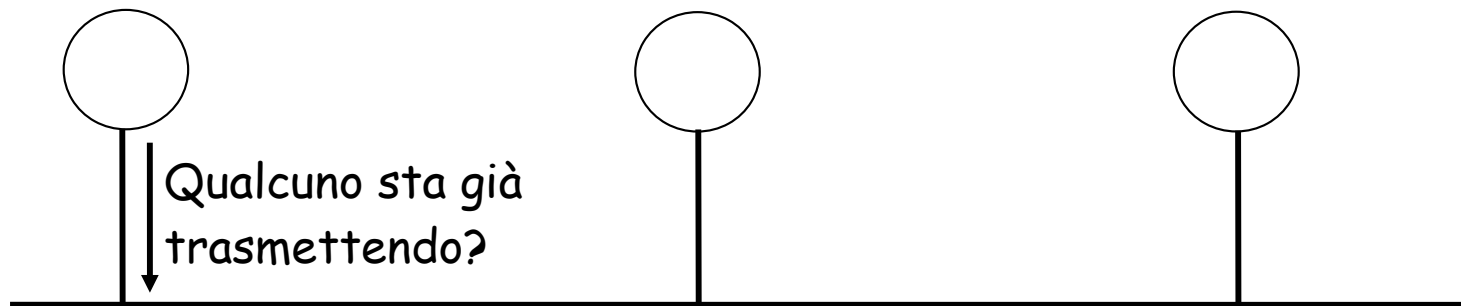
Protocollo CSMA/CD

Protocollo CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

- Protocollo ad **accesso casuale**
- Protocollo completamente **decentralizzato**
- Quando un host deve trasmettere, “ascolta” il canale (*carrier sense*)
- Quando un host trasmette, lo fa alla massima velocità consentita dal canale
- Quando un host rileva una collisione, ritrasmette il frame fino a quando la trasmissione non ha successo
- La ritrasmissione non è immediata, ma l’host attende un periodo di tempo calcolato in modo pseudo-casuale

CSMA/CD: Carrier Sense

- **CS=Carrier Sense** (rilevazione della portante)
- Ogni host che deve trasmettere ascolta il bus e decide di trasmettere solo se lo trova libero (*listen before talking*)

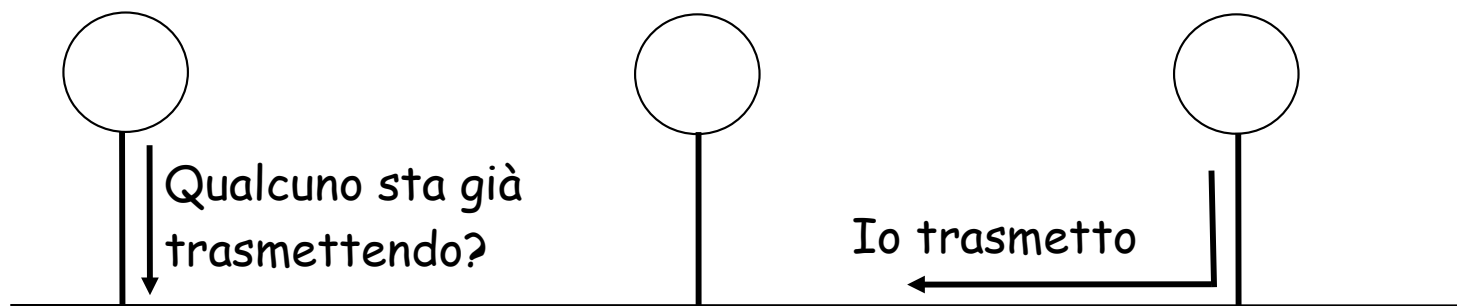


Inter Frame Gap

- Due frame consecutivi vengono sempre distanziati per un tempo che corrisponde alla lunghezza del pacchetto dati più piccolo (es., 9.6 microsecondi per reti a 10 Mbps)
- Questo intervallo è detto **Inter Frame Gap (IFG)**
- IFG serve a garantire agli host in ascolto sulla rete di poter distinguere la fine della trasmissione di un frame dall'inizio della trasmissione successiva
- Prima di iniziare la trasmissione del primo frame, un host deve riscontrare che il canale sia libero per la durata di un IFG

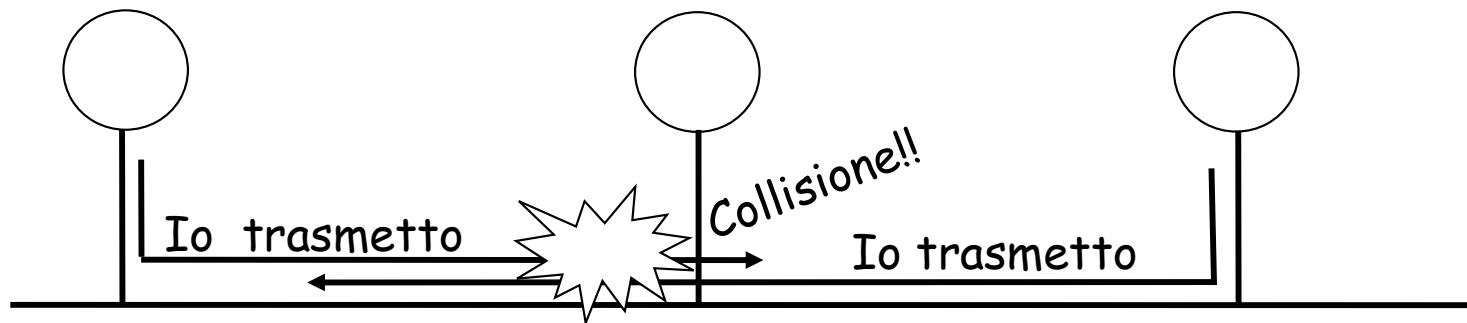
CSMA/CD: Multiple Access

- **MA=Multiple Access** (accessi multipli)
- Nonostante la funzione di *carrier sense*, essendo un protocollo decentralizzato, due host potrebbero decidere di trasmettere in contemporanea
- Essendo il tempo di propagazione del segnale sulla rete non nullo, un host può presumere che il mezzo sia libero ***anche se un altro ha già iniziato a trasmettere***



CSMA/CD: Collision Detection

- **CD=Collision Detection** (rilevamento della collisione)
- Se si verifica una sovrapposizione di trasmissioni si ha una collisione
- Per rilevare una collisione, ogni host mentre trasmette ascolta i segnali sul mezzo, confrontandoli con quelli da esso generati (**listen while talking**)
- Se viene rilevata una collisione, l'host **interrompe la trasmissione**



CSMA/CD: collisioni

A seguito di una collisione:

- Ogni host sospende la trasmissione e trasmette un segnale di **JAMMING** (disturbo) per avvisare della collisione tutti gli host. Il disturbo è composto tipicamente da 48 bit
- Il segnale di JAMMING assicura che ogni host rilevi la collisione anche nel caso in cui la collisione sia stata di breve durata (sovrapposizione di pochi bit)
- Gli host trasmittenti ripetono il tentativo di trasmissione dopo un ritardo (pseudo-)casuale, determinato mediante un **algoritmo di exponential back-off**, fino a un massimo di 16 ritrasmissioni

Binary Exponential Back-off (BEB)

- Il ritardo è $K \times 512$ intervalli di tempo (bit), dove K dipende dal numero di collisioni già rilevate
- Algoritmo di exponential back-off \rightarrow la cardinalità dell'insieme da cui è scelto K cresce esponenzialmente col numero delle collisioni
 - $K \leftarrow [0, 2^{n-1}]$
- Ethernet usa un approccio “calmierato” quando $n = 10$
 - 1 collisione: scegli K tra $\{0, 1\}$;
 - n -esima collisione: scegli K tra $\{0, 1, \dots, 2^{n-1}\}$
 - (dove $m = \min\{n, 10\}$)
 - Da 10 collisione a 15 : scegli K tra $\{0, \dots, 1023\}$
 - 16 collisione: RINUNCIA

BEB: Calcolo di K

- 2 collisione, $n=2$, $m=\min(2,10)=2$, K scelto da $\{0,1,2,3\}$
- 3 collisione, $n=3$, $m=\min(3,10)=3$, K scelto da $\{0,1,\dots,6,7\}$
- 4 collisione, $n=4$, $m=\min(4,10)=4$, K scelto da $\{0,1,\dots,14,15\}$
- 5 collisione, $n=5$, $m=\min(5,10)=5$, K scelto da $\{0,1,\dots,30,31\}$
- 6 collisione, $n=6$, $m=\min(6,10)=6$, K scelto da $\{0,1,\dots,62,63\}$
- 7 collisione, $n=7$, $m=\min(7,10)=7$, K scelto da $\{0,1,\dots,127\}$
- 8 collisione, $n=8$, $m=\min(8,10)=8$, K scelto da $\{0,1,\dots,255\}$
- 9 collisione, $n=9$, $m=\min(9,10)=9$, K scelto da $\{0,1,\dots,511\}$
- 10 collisione, $n=10$, $m=\min(10,10)=10$, K scelto da $\{0,1,\dots,1023\}$
- Per tutti i tentativi successivi, fino a 15, K è scelto da $\{0,1,\dots,1023\}$

BEB: attesa esponenziale

- Scopo: si cerca di stimare il livello di carico della rete per adattare i successivi tentativi di ritrasmissione
- Tramite l'incremento esponenziale delle dimensioni dell'insieme dei valori tra cui si sceglie il ritardo di attesa, l'host riesce ad adattare la ritrasmissione alle diverse situazioni di traffico:
 - - Basso ritardo quando pochi host collidono,
 - - Ritardo di attesa maggiore in presenza di
 - sovraccarico

Riassunto: Algoritmo CSMA/CD

A: controlla il canale, **if** libero

then { trasmetti e controlla il canale;

if scopri un'altra trasmissione

then { // c'è stata una collisione

smetti e manda il segnale di disturbo;

incrementa il numero di collisioni;

ritarda quanto determinate dall'algoritmo BEB;

goto A

}

else { // non c'è stata collisione

quando hai finito di trasmettere il frame, setta il numero di collisioni a zero

attendi un intervallo pari a Inter Frame Gap

goto A}

}

else { aspetta finché la trasmissione corrente è finita; goto A}