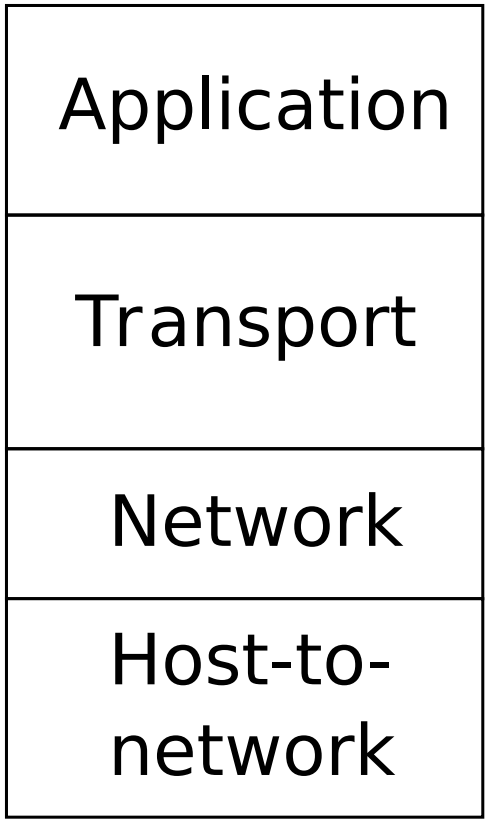
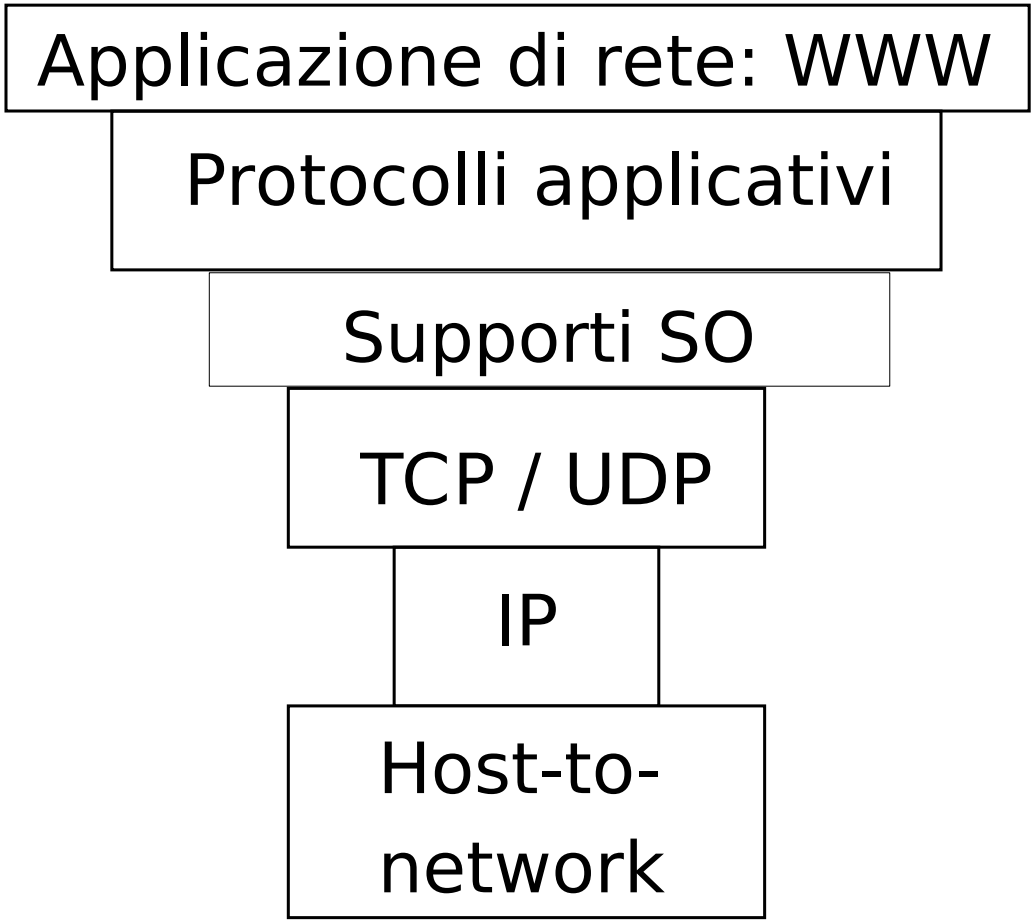
PARTE 3

LIVELLO HOST-TO-NETWORK (H2N)

Modulo 1:
H2N: introduzione

Livello H2N


Application
Transport
Network
Host-to-network


Applicazione di rete: WWW
Protocolli applicativi
Supporti SO
TCP / UDP
IP
Host-to-network

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

- **Modalità di interconnessione e protocolli per la trasmissione dati tra host interconnessi sono strettamente dipendenti tra loro**

  → 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, ac, ...)
- **Mediante modem**
  - SLIP
  - PPP

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
  - Lo strato di rete deve essere in grado di compiere il suo lavoro end-to-end in presenza di differenti set di servizi forniti da specifici protocolli h2n

Possibili servizi H2N

- **Livello 1 (“fisico”)**
  - Connessione di host secondo diversi mezzi trasmissivi (doppino, cavo coassiale, fibra ottica, trasmissione radio)

Possibili servizi H2N

- **Livello 2 (“data link”)**
  - Framing (incapsulamento in *frame*)
  - Accesso al link (es., CSMA/CD)
  - Recapito affidabile (acknowledgement e ritrasmissione)
  - Controllo di flusso
  - Ricerca di errori
  - Correzione degli errori
  - Half-duplex o Full-duplex

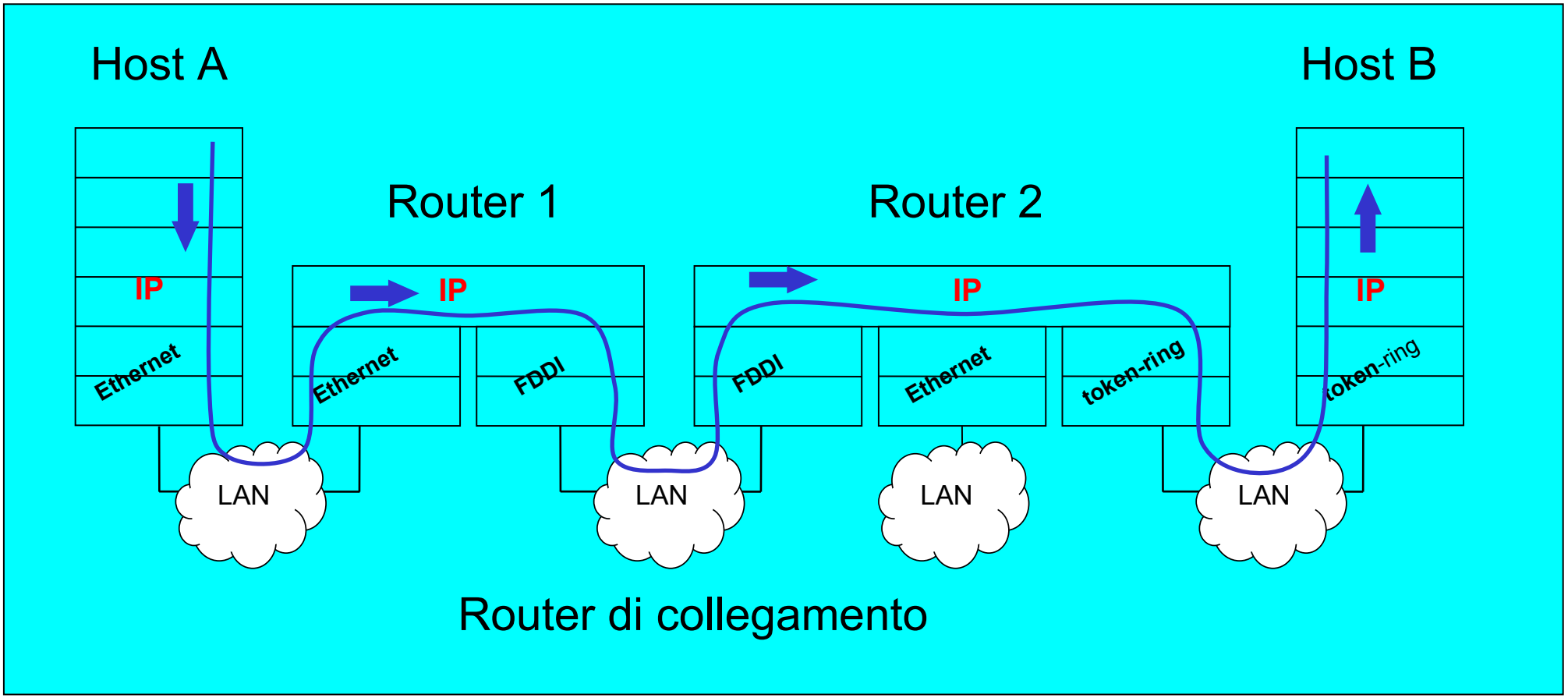
NOTA: Questi servizi sono solo possibili, non è detto che siano presenti in tutte le tecnologie

Differenze con il livello trasporto

- **La similitudine con alcuni servizi del protocollo di trasporto (soprattutto TCP) non deve trarre in inganno:**
  - → Il livello h2n opera a livello di singolo link (host interconnessi)
  - → Il livello trasporto opera a livello di host end-to-end

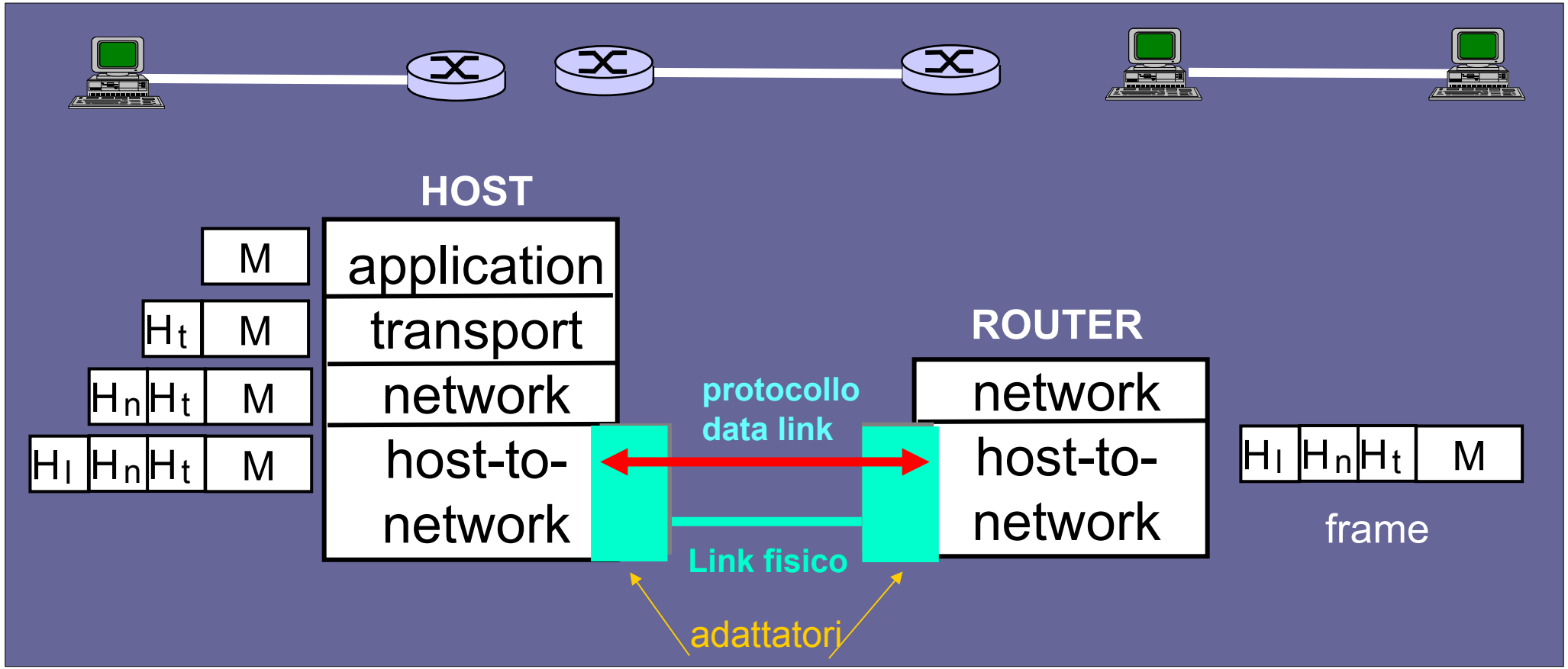
Differenze con il livello IP

- Il livello data link consegna pacchetti solo all'interno di una stessa LAN
- Il livello network (IP) consegna pacchetti ovunque su Internet



Collegamenti dell'H2N

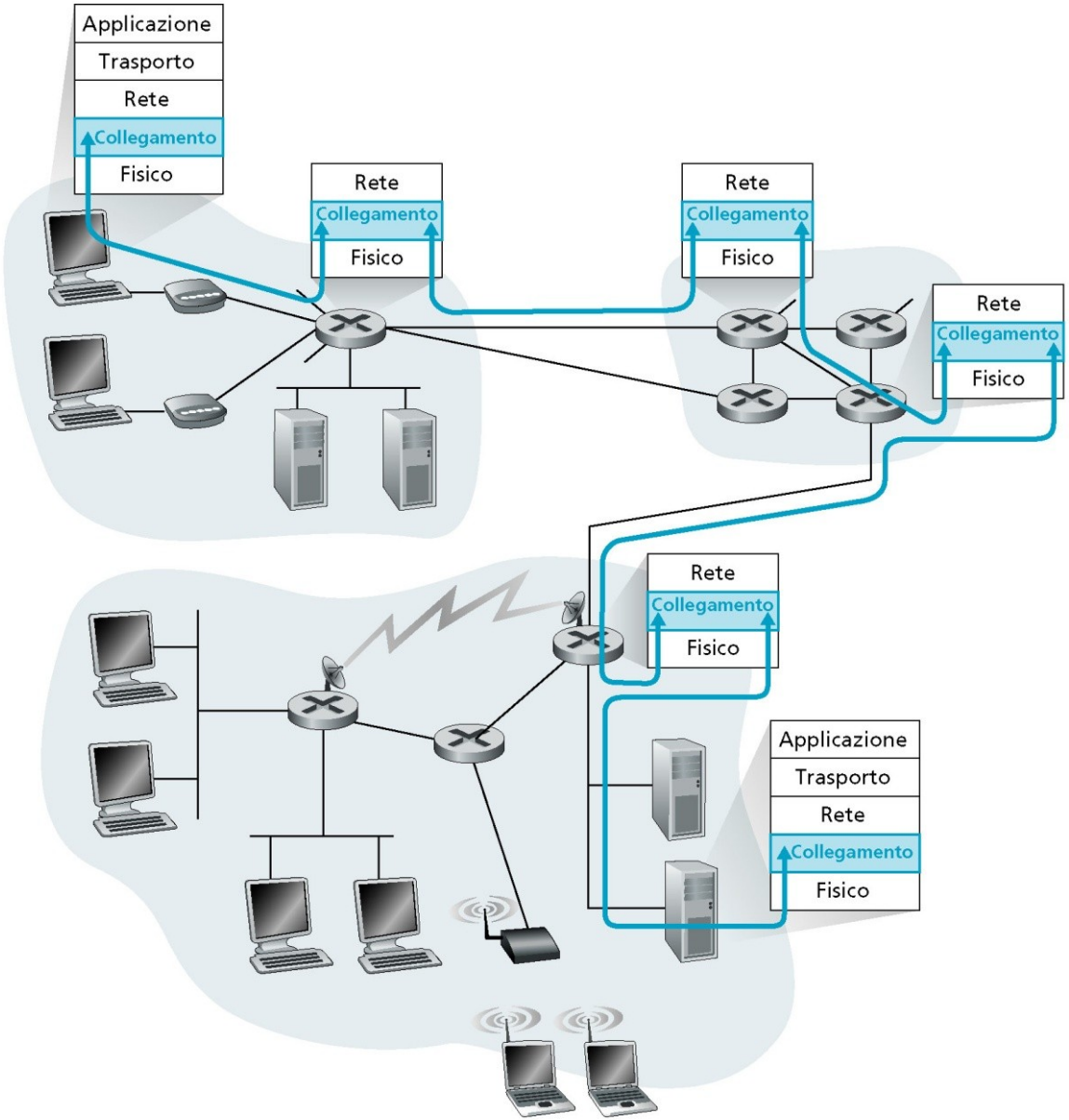
- **Due dispositivi connessi fisicamente: *host-router*, *router-router*, *host-host***
- **Unità di dato trasmesso: *frame***



Funzionamento dell'H2N

Si collegano:

- **host con host**
- **host con router**
- **router con router**



Definizioni: Tipi di collegamento

- **Collegamento broadcast**
  - Molti host connessi ad uno stesso canale di comunicazione
  - E’ necessario un protocollo di accesso al mezzo per coordinare le trasmissioni e per evitare le collisioni
  - Sono comuni nelle LAN, Wireless LAN, 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 ed il router dell’ISP

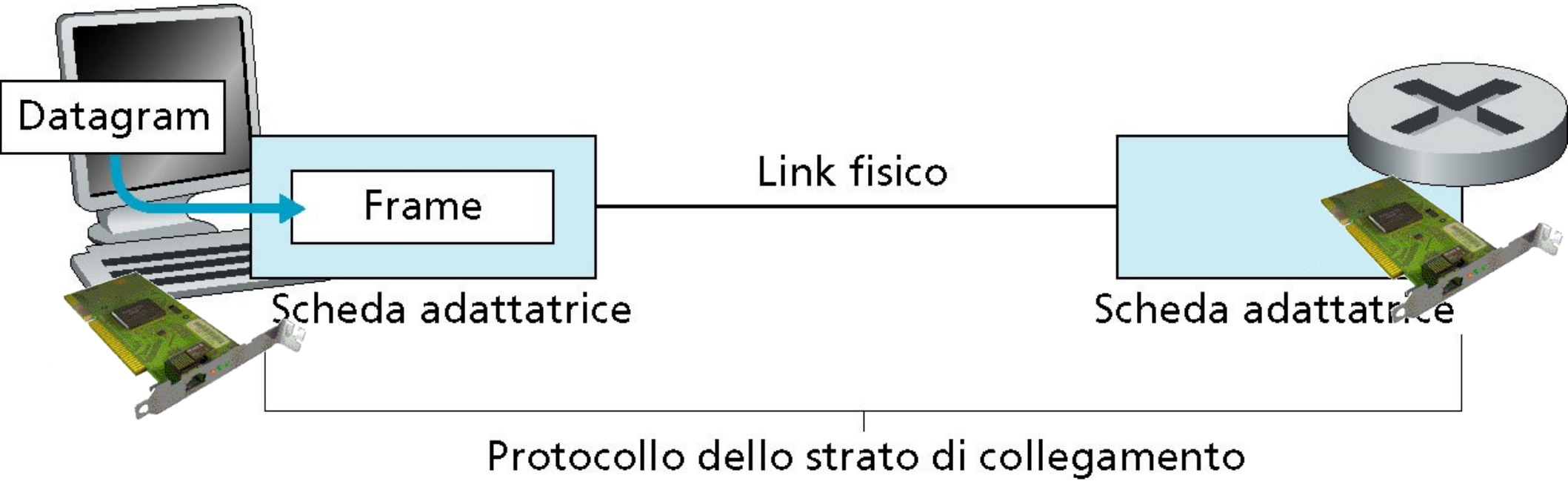
Definizioni: Modalità di trasmissione

- **Unicast: comunicazione fra un singolo mittente ed un singolo ricevente**
- **Multicast: comunicazione fra un singolo mittente ed 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**

Modulo 2: Tecnologie per interconnettere host alla rete

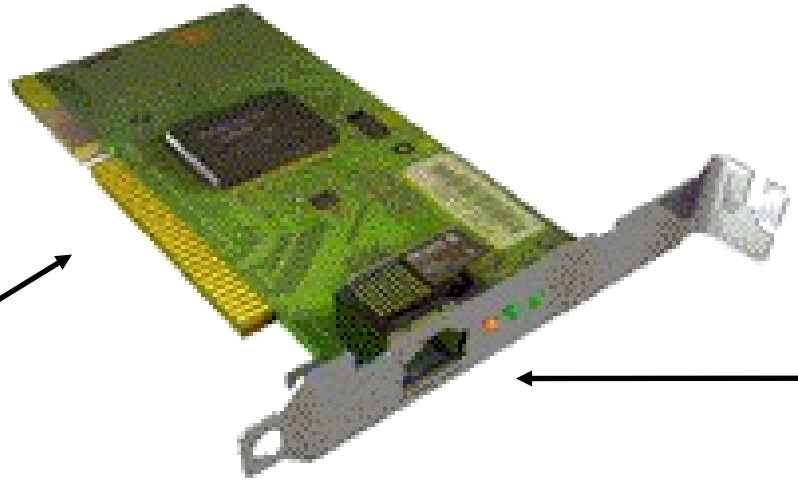
Adattatori per la comunicazione

- Il protocollo h2n è implementato in 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



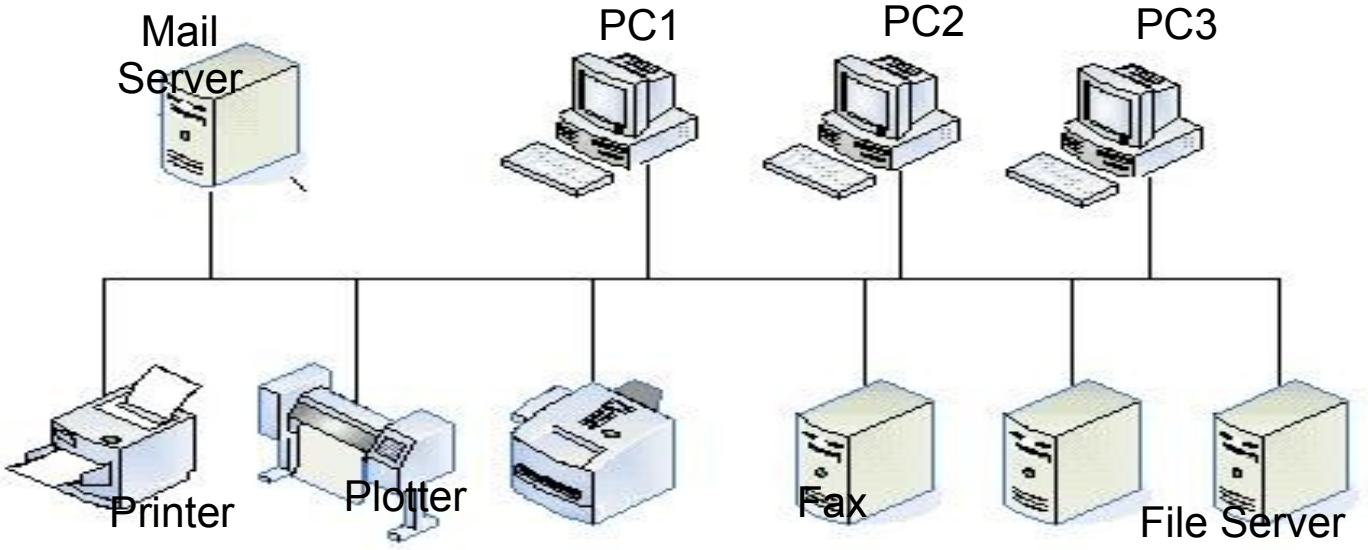
Network Interface Card (NIC)

- **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 all'host in cui risiede**



Local Area Network

- **Rete di host collegati tra loro all'interno di un'area fisica limitata (es., l'interno di un edificio, di un complesso ospedaliero o di un campus universitario) che non superi la distanza di qualche chilometro**
- **Basata su una rete di trasmissione condivisa a bit rate elevato (LAN storiche a 10 Mbps, successive a 100 Mbps, attuali a 1-10 Gbps)**

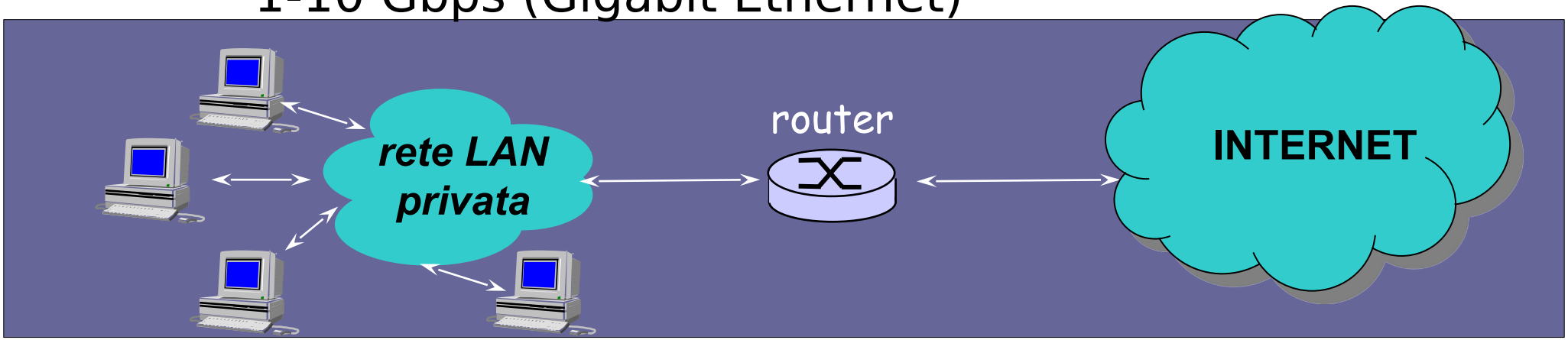


Tecnologie per LAN

- **Differenti classi di tecnologie per LAN (Standard IEEE 802)**
- **LAN wired:**
  - Ethernet (LAN 802.3) → standard de facto
  - Token Ring
  - FDDI
  - Frame relay
- **LAN wireless:**
  - WLAN (LAN 802.11x, con x = a, b, ...)

Accessi da una propria rete LAN

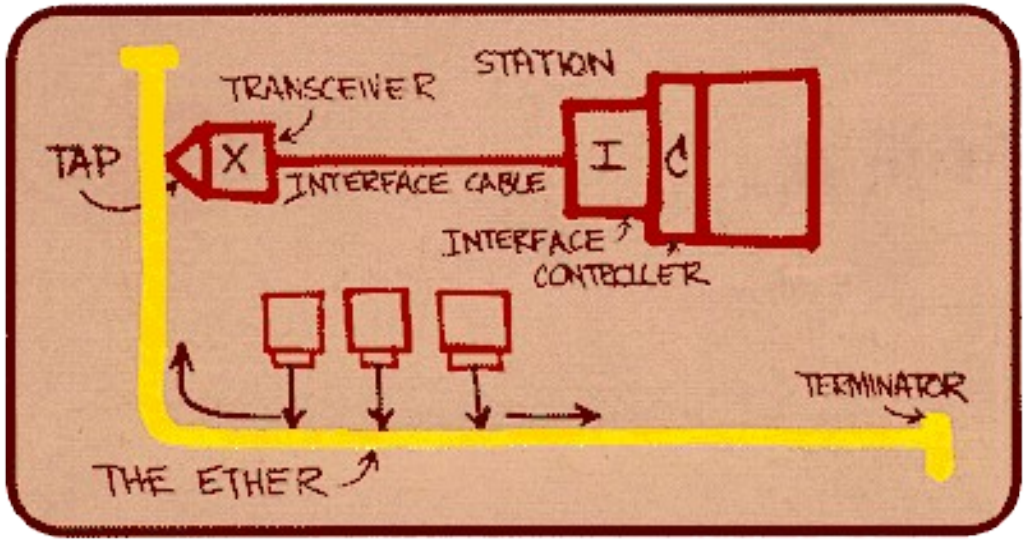
- **La rete locale (LAN) dell'università o azienda viene collegata ad un router di Internet**
- **Un cavo dedicato o condiviso collega i computer della LAN e questi, mediante bridge e switch, al router**
- **Tipiche bande di trasmissione della LAN privata più diffusa (Ethernet):**
  - 10 Mbps (Ethernet)
  - 100 Mbps (Fast Ethernet)
  - 1-10 Gbps (Gigabit Ethernet)



Modulo 3: Ethernet

Ethernet

- **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 per connettere i nodi**



Motivi del successo di Ethernet

- **Relativamente poco costosa**
- **Si presta all'uso con diverse:**
  - Topologie (modo di connettere gli host della rete)
  - Tecnologie (tecnologia del mezzo trasmissivo usato per le connessioni)
- **La rapida diffusione iniziale ha ostacolato l'uscita di successive tecnologie concorrenti (FDDI, ATM)**
- **Ampiamente adottata perché funziona bene ed è poco costosa (cosa rara…)**
- **Si adatta bene con l'utilizzo dei protocolli TCP/IP**

Caratteristiche Ethernet

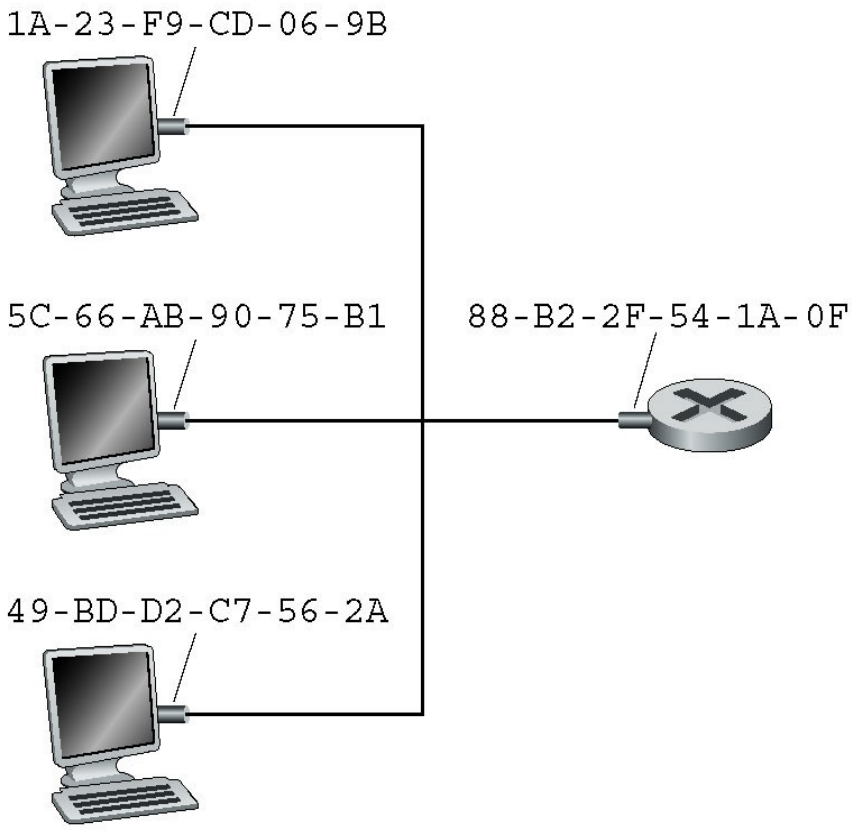
- **Tipo di collegamento**
  - Canale di broadcast (non punto-punto): molti host connessi ad uno stesso canale di comunicazione
- **Modalità di trasmissione**
  - Broadcast: comunicazione fra un singolo mittente e tutti gli altri nodi
- **Gli host di una LAN si scambiano dati su un canale broadcast: Quando un host trasmette un pacchetto sulla LAN, TUTTI gli host collegati lo ricevono**

Indirizzi MAC

- **Gli host utilizzano un indirizzo hardware o indirizzo MAC (Media Access Control) per capire chi è il destinatario del dato**
  - Quando un host vuole trasmettere un pacchetto, vi inserisce l'indirizzo MAC del destinatario e lo immette nella LAN (canale di broadcast)
  - Se l'indirizzo di destinazione del pacchetto corrisponde all'indirizzo MAC dell'host ricevente, l'host accetta il pacchetto e lo passa verso l'alto nella pila protocollare
  - Se l'indirizzo di destinazione non corrisponde all'indirizzo MAC dell'host ricevente, l'host scarta il pacchetto

Indirizzi MAC (2)

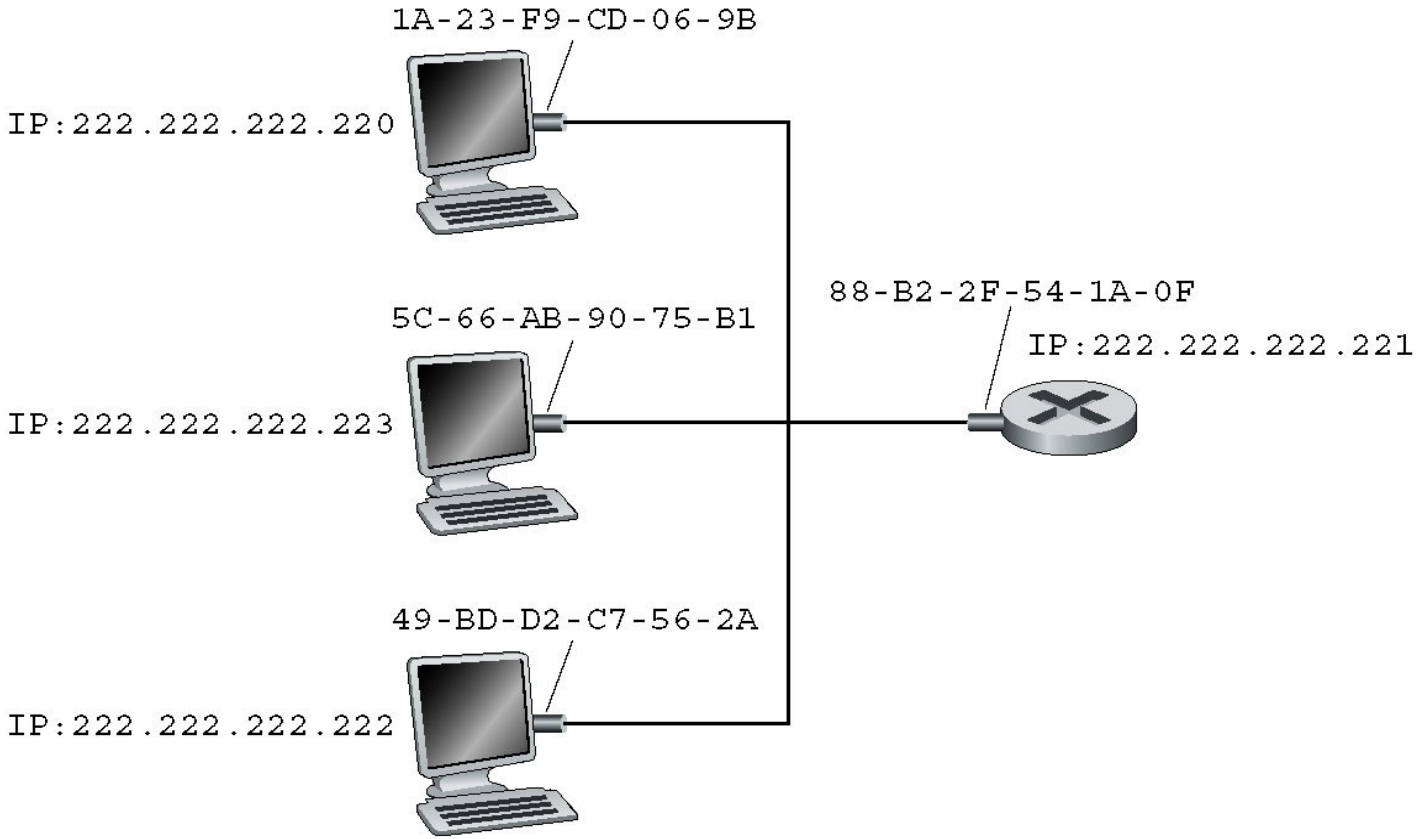
- **In realtà non è l'host a possedere l'indirizzo MAC, ma è il NIC dell'host**
- **Ogni NIC ha un indirizzo LAN univoco di 48 bit**
- **L'indirizzo MAC di un adattatore è permanente: incorporato nella ROM al momento della fabbricazione**
- **Gli indirizzi sono assegnati ai produttori di NIC (Network Interface Card) da un'autorità centrale: la IEEE**



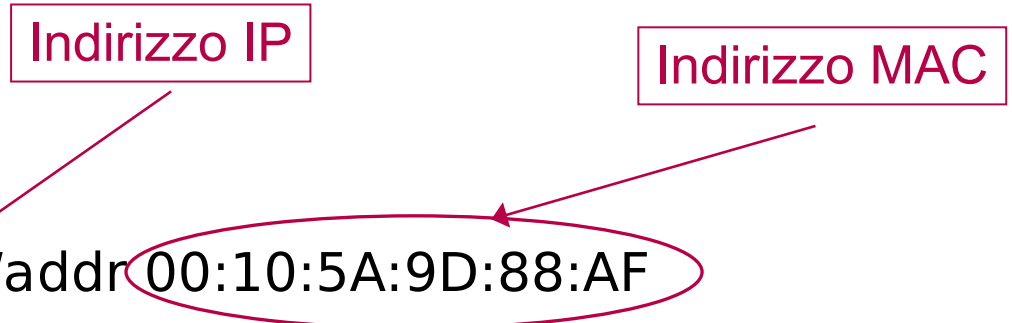
L'indirizzo broadcast è
FF-FF-FF-FF-FF-FF
(tutti i bit settati a 1)

Indirizzi di un host

Ciascun host di una LAN ha almeno una NIC. Ciascun dispositivo di rete ha un indirizzo MAC cui si associa un indirizzo IP



Esempio



 # ifconfig eth0

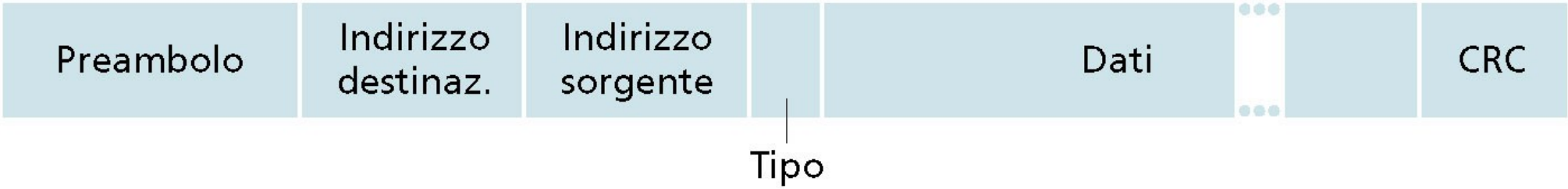
```
eth0   Link encap:Ethernet  HWaddr 00:10:5A:9D:88:AF
       inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:92 errors:0 dropped:0 overruns:0 frame:0
       TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
       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 "neutri" indirizzi MAC:**
  - non sarebbero in grado di supportare facilmente altri protocolli di rete differenti da IP
  - gli indirizzi IP dovrebbero essere registrati nella RAM del NIC → riconfigurati ad ogni spostamento o riaccensione
- **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

- **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 prembolo (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 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 adattatore 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 dello strato di rete.**
- **Gli host possono supportare protocolli dello strato di rete diversi da IP (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
  - Esiste un dimensione alternativa di 9000 byte (Jumbo frame)

Dati (e dimensione)

- **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)**

CRC

- **Quando un host riceve il frame ricalcola il CRC utilizzando la stessa funzione e vede se corrisponde**
  - Se corrisponde, sa che non c’è stato errore
  - Se non corrisponde? …

Modulo 4: Protocolli ARP

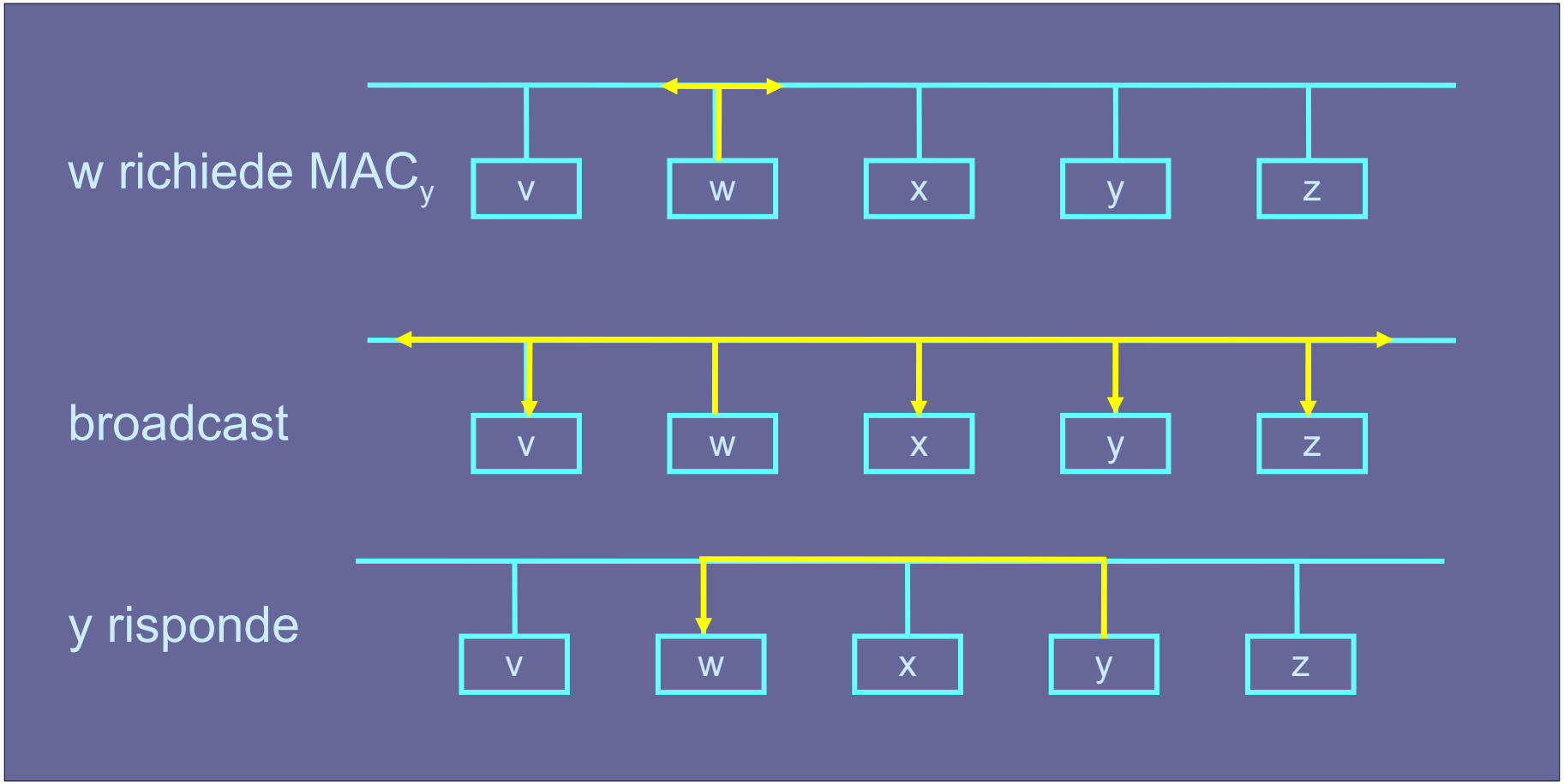
Protocollo per la risoluzione degli indirizzi

- **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 trasformare l'indirizzo IP di un host della stessa LAN nel corrispondente indirizzo MAC

- **Il protocollo ARP è incluso nella suite di protocolli TCP/IP**

Protocollo ARP



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**

Messaggio 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 propria tabella di instradamento**

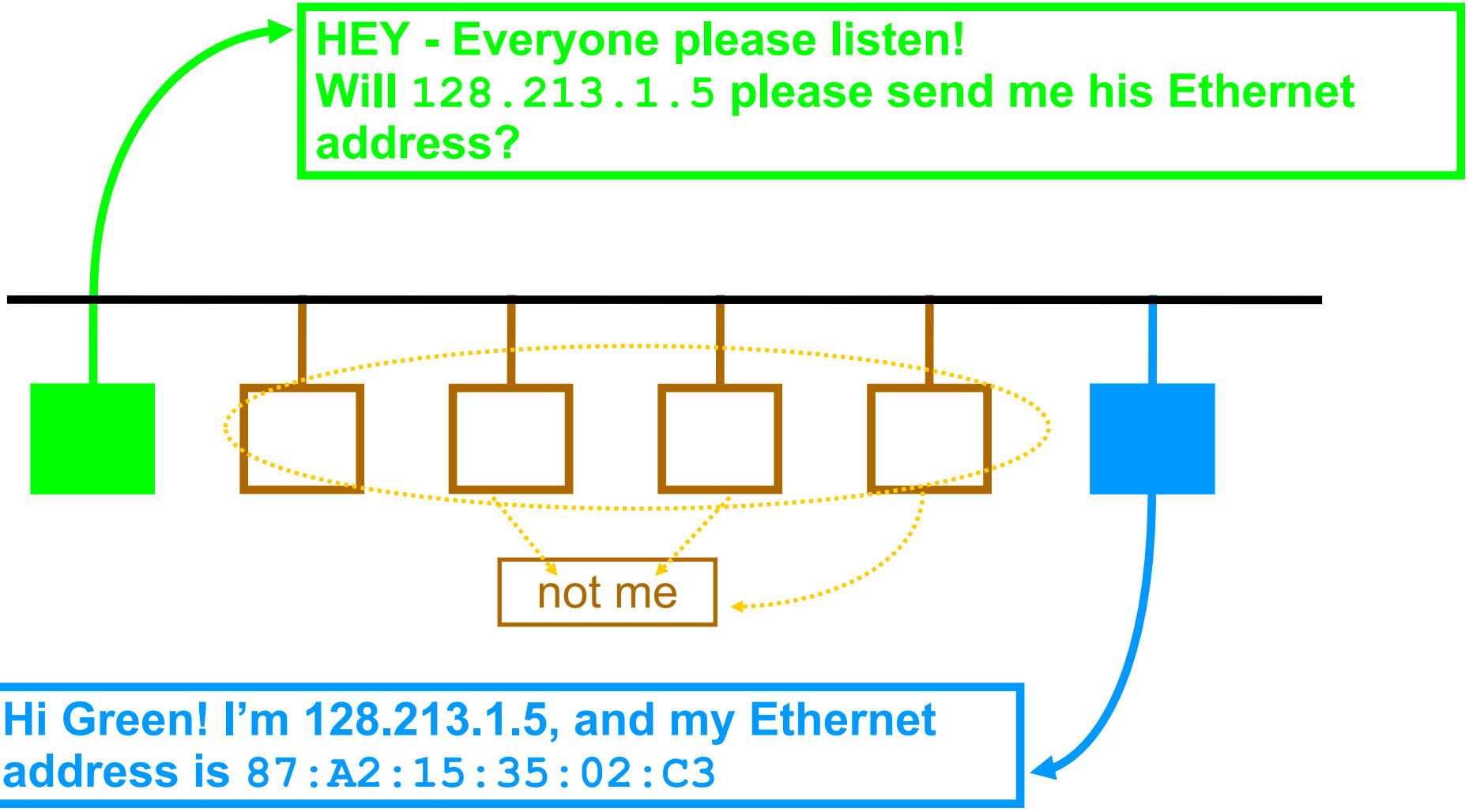
Indirizzo IP	Indirizzo MAC	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

- **Ottimizzazione: il mittente inserisce nella richiesta la corrispondenza fra il proprio indirizzo IP e quello MAC**

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
```

Conversazione ARP



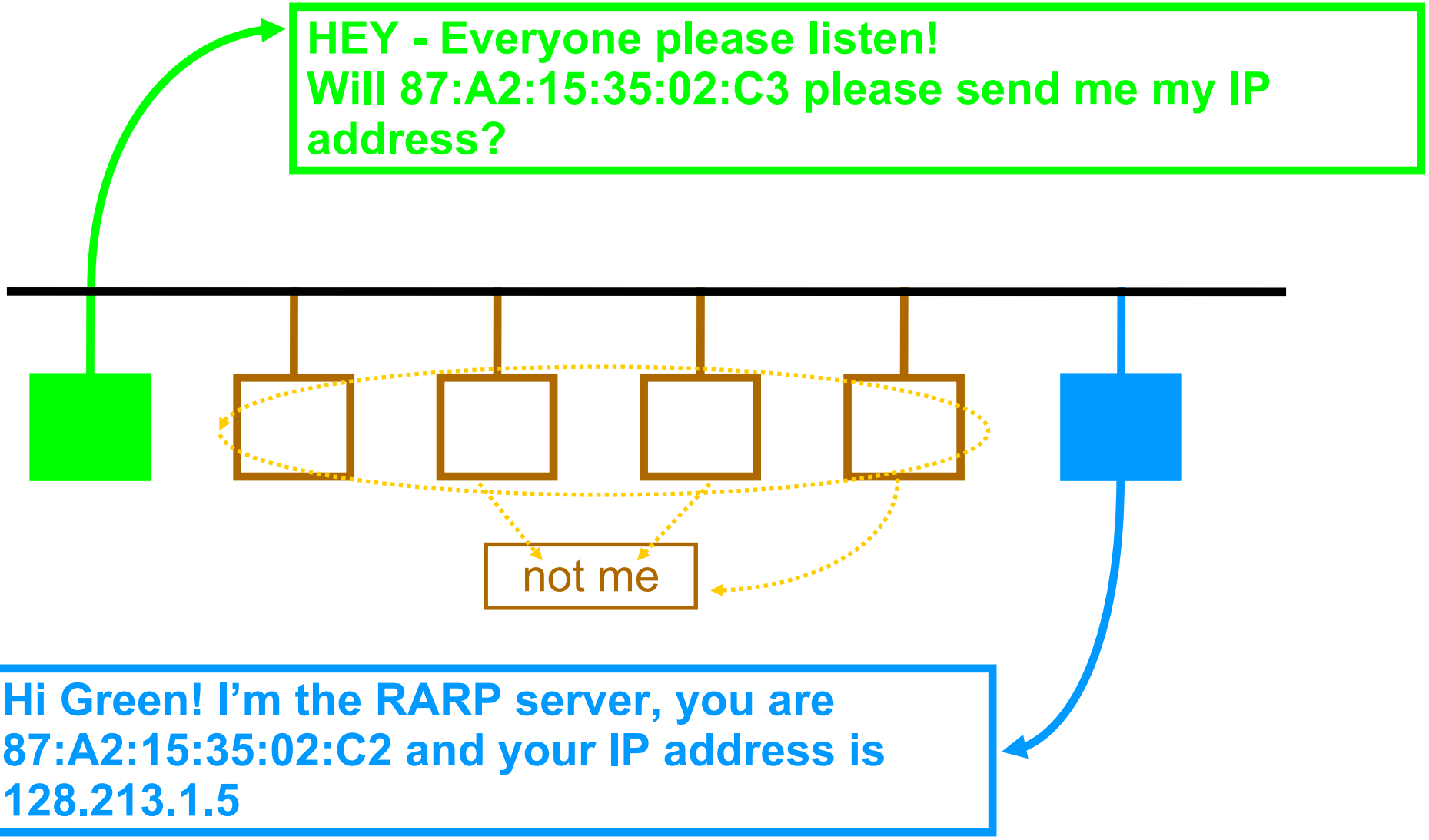
Protocollo RARP

- **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 uguale al protocollo ARP

Protocollo RARP

- **Utilizzato 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 bytes**
- **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 comune: IP su Ethernet

- **Sender HW address**
- **Sender net address**
- **Receiver HW address**
- **Receiver net address**

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

Modulo 5: Interconnessione di LAN

Interconnettere LAN

- **Perché non creare un'unica grande LAN quando vi sono da interconnettere molti host?**
- **Motivazioni**
  - Sarebbe possibile supportare una quantità limitata di traffico: su una singola LAN, tutte gli host devono condividere la stessa larghezza di banda
  - Lunghezza limitata: lo standard 802.3 specifica la massima lunghezza del cavo
  - Ci sarebbe un unico grande "dominio di collisione" (ciascun host può collidere con molti host)

Apparati di rete

- **Esistono diversi apparati di rete dipendenti da:**
  - topologia di interconnessione degli host
  - numero degli host collegati
  - efficienza delle comunicazioni (anche in funzione del traffico previsto)

Tipi di apparati di rete

- **Hub**
- **Bridge**
- **Switch**
- ***Switch di livello 3***

Vantaggi degli hub

- **Dispositivi semplici ed estremamente economici**

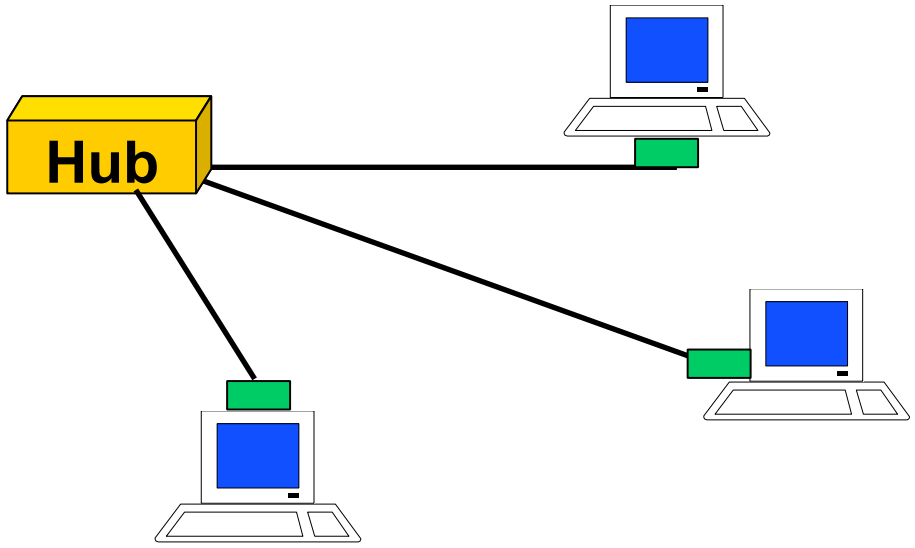
  → Inizialmente fa era la tecnologia migliore per piccole LAN con poco traffico (SOHO)
- **Estende la massima distanza fra coppie di nodi** (con doppino: 100m fra host e hub
  → 200m tra due host)
- **Trasparente: non necessita di alcun cambiamento agli adattatori LAN degli host**
- **Confinamento dei guasti: un guasto su un segmento di LAN non impedisce il traffico sugli altri segmenti**

Hub

- **Dispositivo di livello fisico dotato di due o più interfacce.** Essenzialmente, è un ripetitore che opera a livello di singoli bit:

  → **ripete i bit ricevuti su una interfaccia a tutte le altre interfacce**

- **Ogni nodo connesso costituisce un segmento di LAN**



Svantaggi degli hub

- **Gli hub non isolano il dominio delle collisioni (non implementano la rilevazione della portante):**

  → il traffico di un host può collidere con il traffico di ogni altro host che risieda in un qualsiasi segmento della LAN collegato all'hub
- **In pratica, dal punto di vista del traffico, una LAN collegata mediante hub è equivalente ad una topologia a bus** (non è equivalente per i guasti a livello di segmento)

Limiti (generali) di Ethernet

- **Ciascuna tecnologia Ethernet ha limitazioni relative a:**
  - numero massimo di host consentiti in un dominio di collisione
  - massima distanza fra due host in un dominio di collisione
  - massimo numero di livelli in uno schema multi-livello
- **Queste caratteristiche limitano sia il massimo numero di host collegabili, sia il raggio di azione geografico di una LAN multilivello**

Bridge

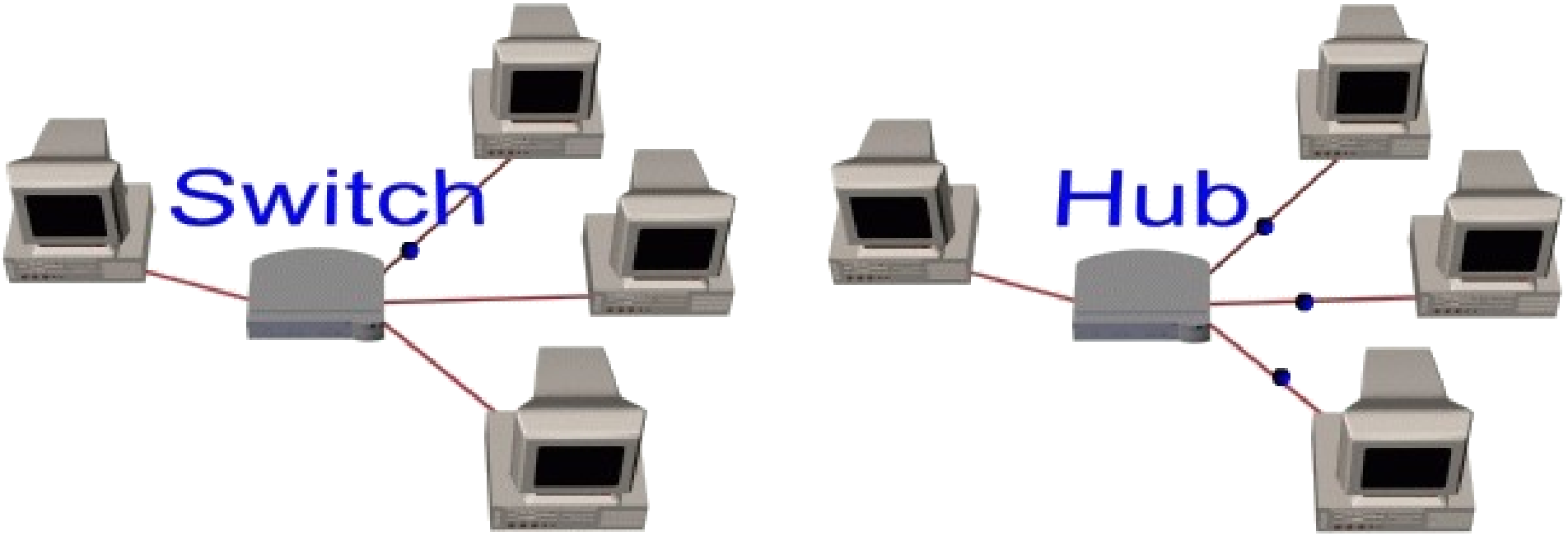
- **Dispositivo di livello 2 (link layer)**
- **Opera a livello di frame Ethernet, esaminando l'header dei frame ed inoltrandoli selettivamente, sulla base dell'indirizzo MAC della loro destinazione**
- **Quando un frame deve essere inoltrato su un segmento di LAN, il bridge usa il protocollo CSMA/CD (con attesa esponenziale) per trasmettere**

Bridge e Hub

- **Un bridge è “più intelligente” di un hub perché è in grado di andare a leggere l’indirizzo del destinatario all’interno di un frame che gli arriva**

- **Un bridge svolge funzioni di filtraggio: dato che è in grado di capire il MAC address del destinatario, manda il pacchetto solo sulla porta di uscita su cui sa che c’è il destinatario**

Bridge e Hub



Vantaggi dei bridge

- **Isola i domini di collisione producendo un aumento del massimo throughput totale, e non limita il numero degli host, né la copertura geografica**

- **Può connettere tipi diversi di Ethernet dal momento che è un dispositivo store-and-forward**

- **Trasparente: non necessita di alcun cambiamento agli adattatori LAN degli host**

Filtraggio ed inoltro dei frame

- **Filtraggio dei frame**
  - I frame destinati ad host dello stesso segmento non sono inoltrati sugli altri segmenti della LAN
  - Il meccanismo di filtraggio consente di aumentare sensibilmente il traffico sulla rete: se, ad esempio, in ciascun segmento di LAN il traffico è prevalentemente locale, la capacità complessivamente disponibile è pari a quella di ciascun segmento moltiplicata per il numero dei segmenti
- **Inoltro dei frame**
  - Come si fa a sapere qual è il segmento di LAN su cui deve essere inoltrato un frame?

Metodi di filtraggio e inoltro

- **I bridge imparano quali host possono essere raggiunti attraverso quali interfacce**
  - Mantengono delle tabelle di filtraggio costruite automaticamente senza bisogno dell'intervento di amministratori di rete
  - Quando viene ricevuto un frame, il bridge "impara" la locazione del mittente
  - Registra la locazione del mittente nella tabella di filtraggio

Metodi di filtraggio e inoltro

- **Record per la tabella di filtraggio:**
  - Indirizzo MAC dell'host, Interfaccia del Bridge, Time-To-Live (TTL) che è il periodo di validità delle informazioni memorizzate nella tabella di filtraggio
  - Record vecchi nella tabella di filtraggio vengono scartati (TTL può essere configurato a 60 minuti)

Procedura di filtraggio

if (destinazione è sulla LAN dalla quale il frame è stato ricevuto)

then elimina il frame;

else

{ guarda nella tabella di filtraggio;

if (trovi un record per la destinazione)

then inoltra il frame sull'interfaccia indicata;

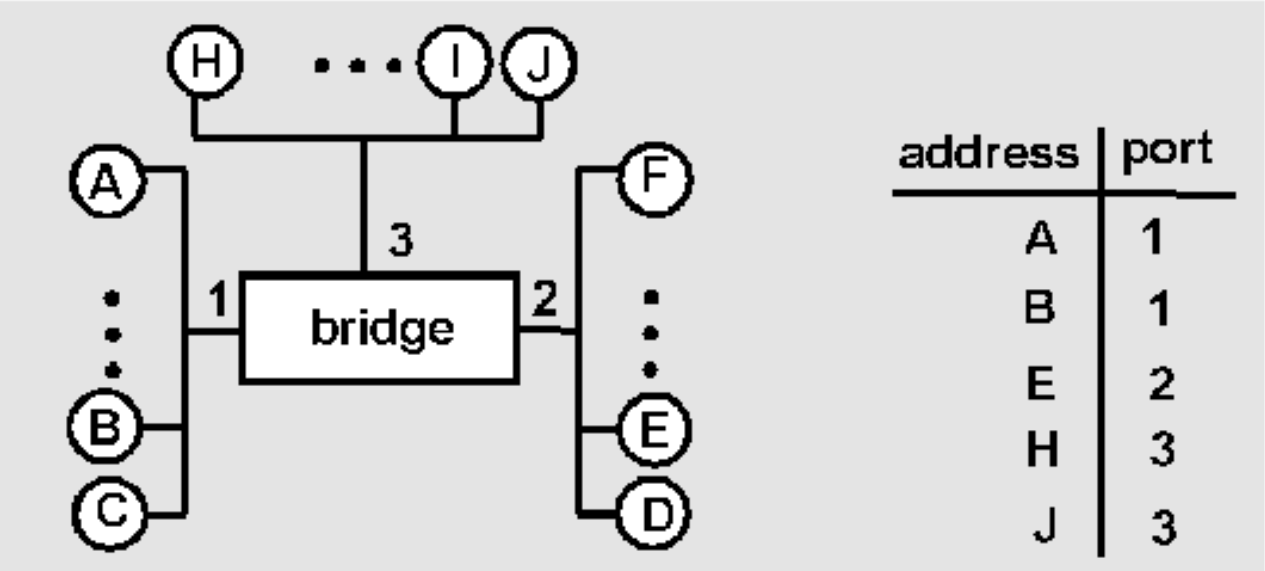
else flooding;

/* inoltra il frame a tutte le interfacce tranne quella da cui è arrivato*/

}

Autoapprendimento: esempio

Si supponga che C mandi un frame a D e D risponda con un frame a C

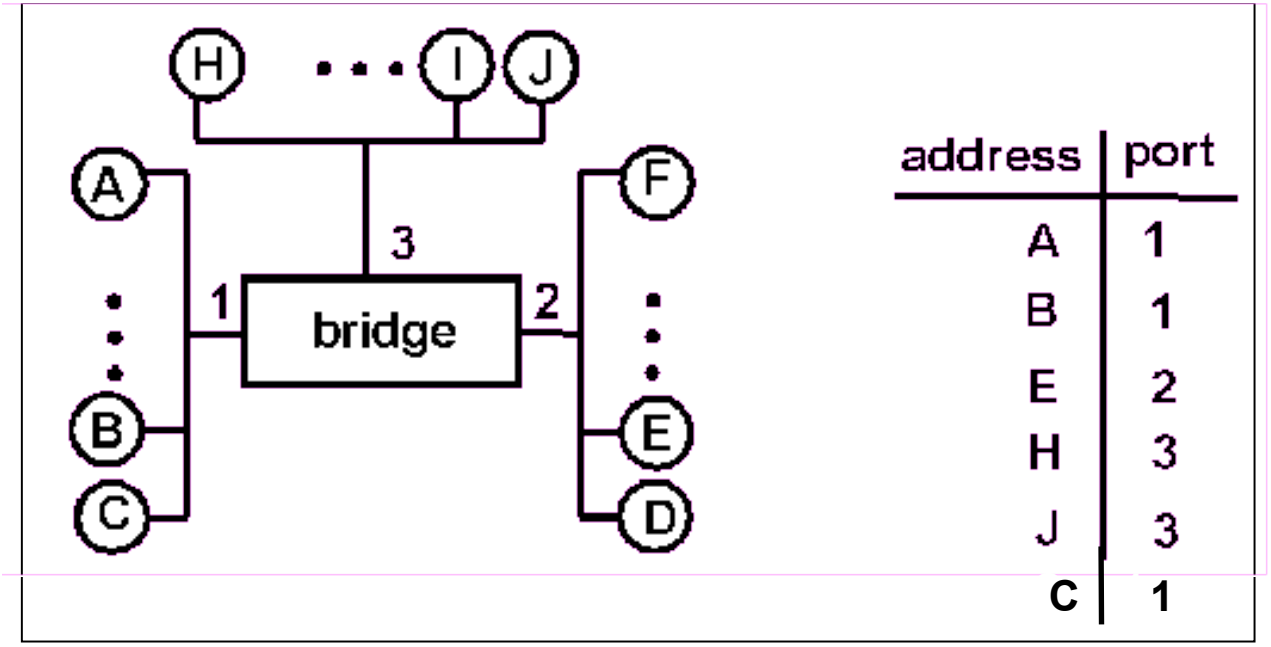


address	port
A	1
B	1
E	2
H	3
J	3

C manda un frame, il bridge non ha informazioni su D, così inoltra su entrambe le LAN 2 e 3

- Il bridge nota che C è sulla porta 1
- Il frame è ignorato nella LAN 3
- Il frame è ricevuto da D

Autoapprendimento: esempio

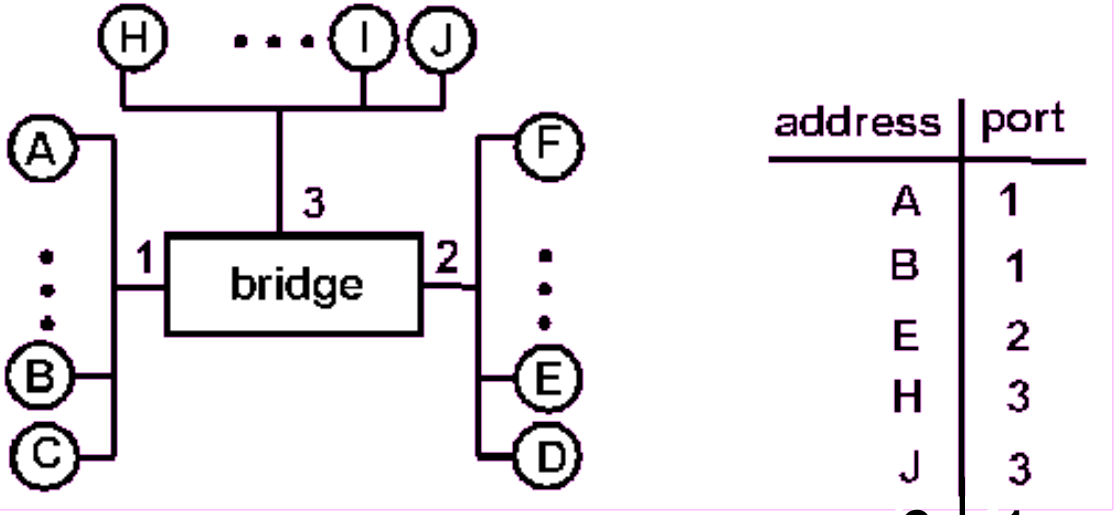


D genera la risposta per C, manda il suo frame

- Il bridge vede un frame da D
- Il bridge nota che D è sull'interfaccia 2
- Il bridge sa che C è sull'interfaccia 1, così inoltra selettivamente il frame attraverso l'interfaccia 1

Autoapprendimento: svantaggio

- **Se si sposta l'host A dalla LAN 1 alla LAN 3, su quale interfaccia lo switch inoltra i frame?**
  - I frame sono inoltrati sul segmento di LAN sbagliato (1) fino a quando l'host A non invia il primo frame (modifica tabella di filtraggio) o fino allo scadere del TTL per la entry relativa ad A (cancellazione della entry dalla tabella)

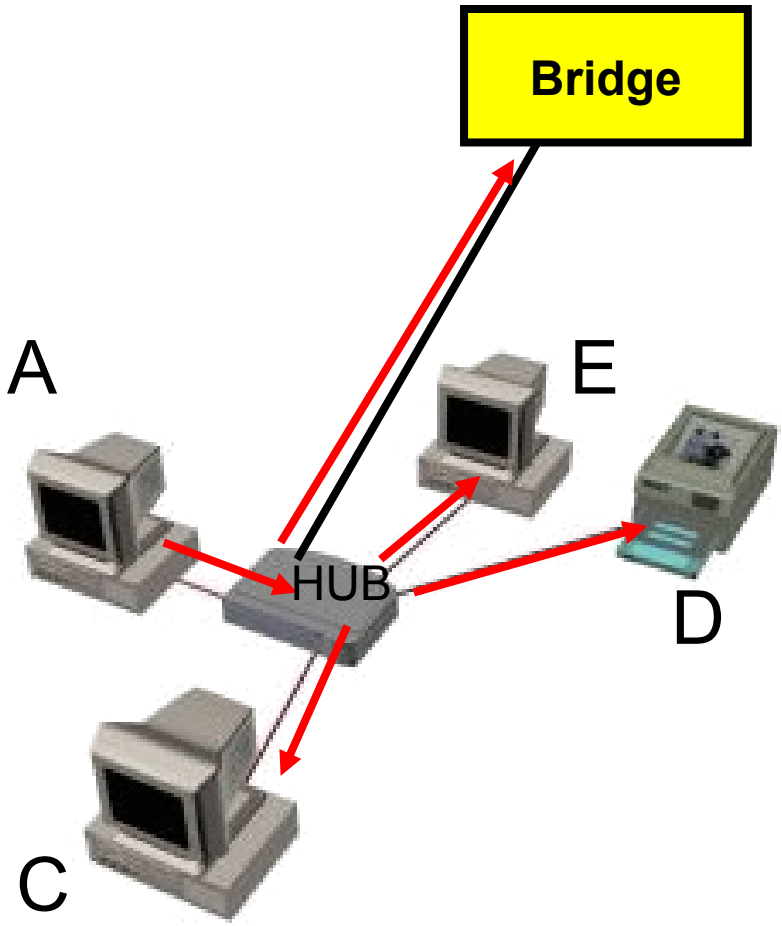


address	port
A	1
B	1
E	2
H	3
J	3
C	1

Di solito (es., nei sistemi Windows) ogni host che si collega alla rete manda un frame per avvisare della sua presenza

Esempio

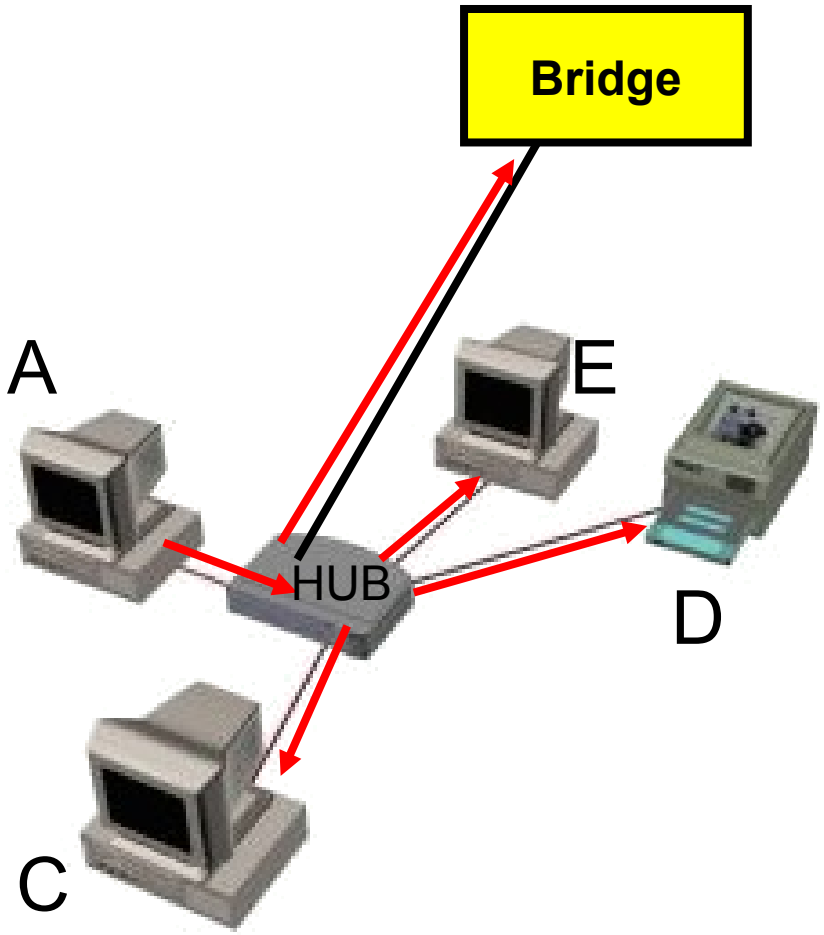
- Il nodo A spedisce all'HUB un pacchetto destinato a B
- L'HUB rispedisce il pacchetto che gli arriva da A su tutte le altre porte
- Il pacchetto arriva quindi ai nodi C, D, E e al BRIDGE



Matematica

Esempio

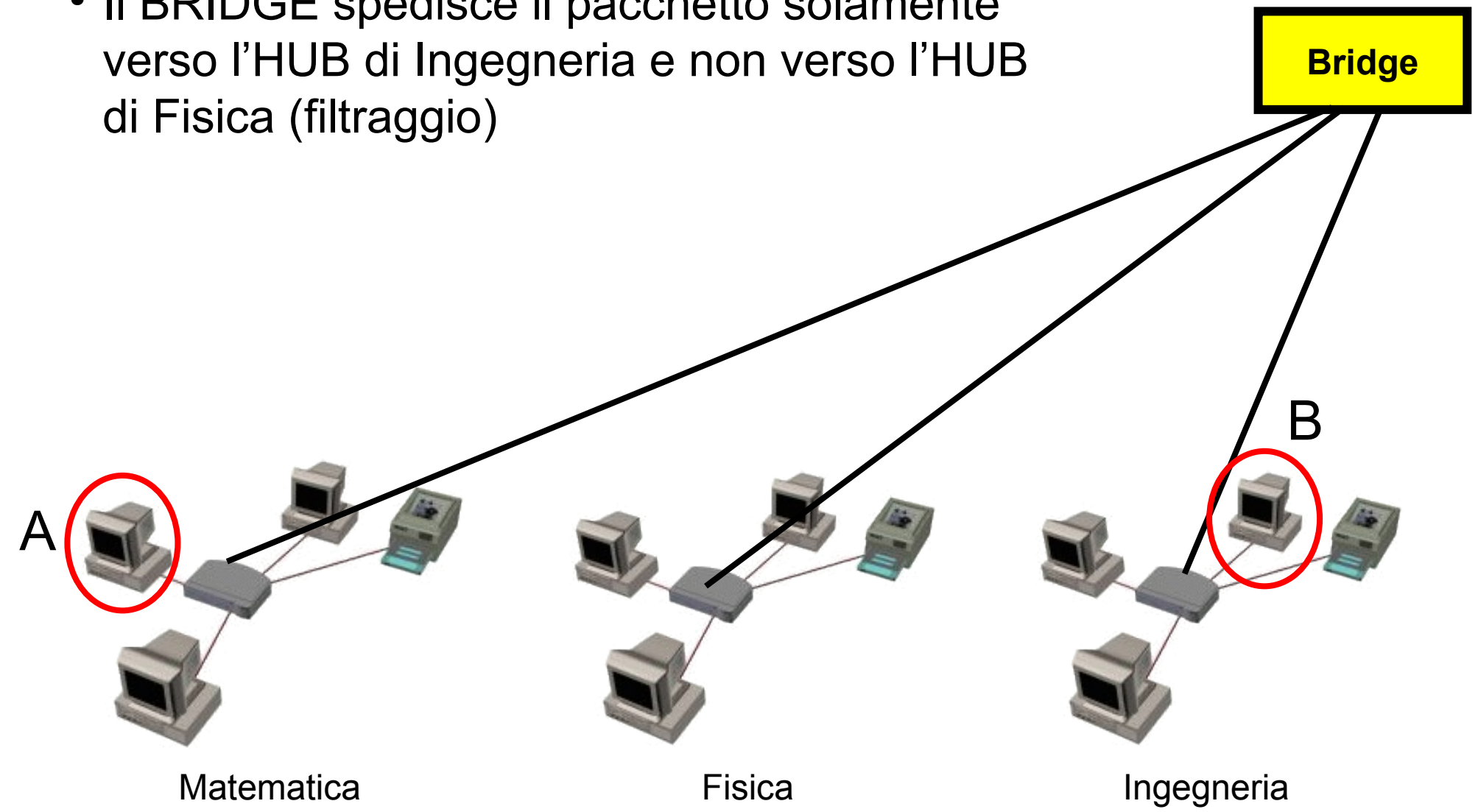
- Tutti i nodi guardano il MAC address del destinatario
- I nodi C, D ed E vedono che il pacchetto non è per loro e lo scartano
- Il BRIDGE invece capisce che quel pacchetto è per un nodo della LAN di Ingegneria



Matematica

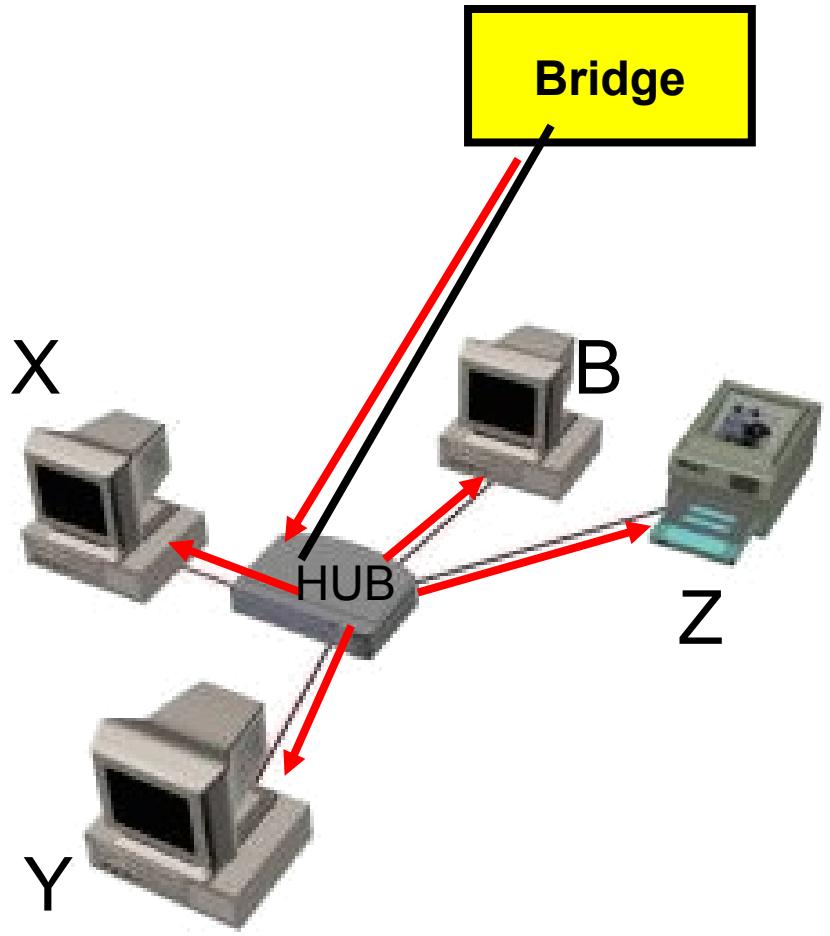
Esempio

- Il BRIDGE spedisce il pacchetto solamente verso l'HUB di Ingegneria e non verso l'HUB di Fisica (filtraggio)



Esempio

- L'HUB di Ingegneria manda il pacchetto a tutti i nodi di Ingegneria
- Il pacchetto arriva quindi ai nodi X, Y, Z ed al nodo B
- Il nodo B capisce che il pacchetto è per lui e lo legge
- Tutti gli altri nodi vedono che il pacchetto non è per loro e lo scartano



Ingegneria

Affidabilità delle LAN

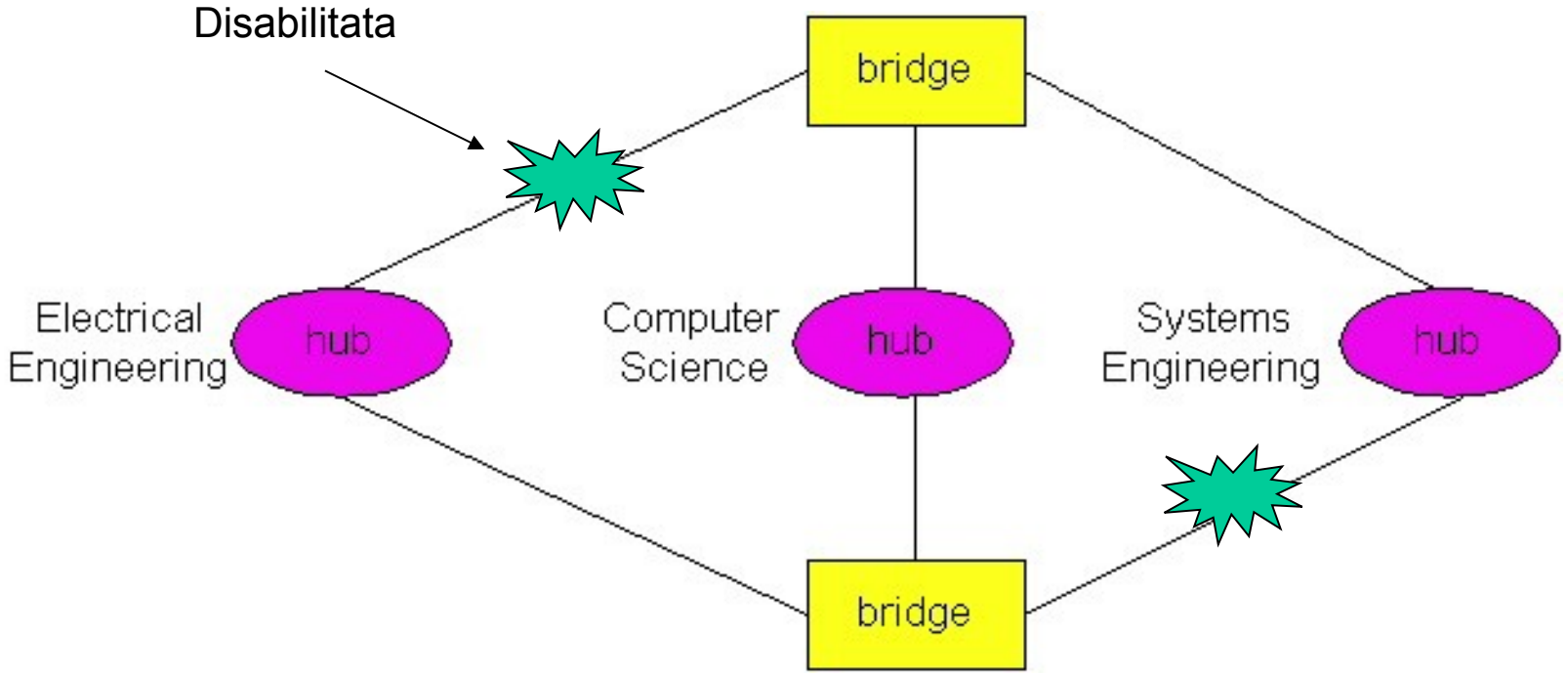
- **Per aumentare l'affidabilità di una rete, è desiderabile avere ridondanza ovvero cammini alternativi dalla sorgente alla destinazione**

- **Però, con cammini multipli possono crearsi dei cicli e conseguentemente i bridge potrebbero moltiplicare e inoltrare frame**

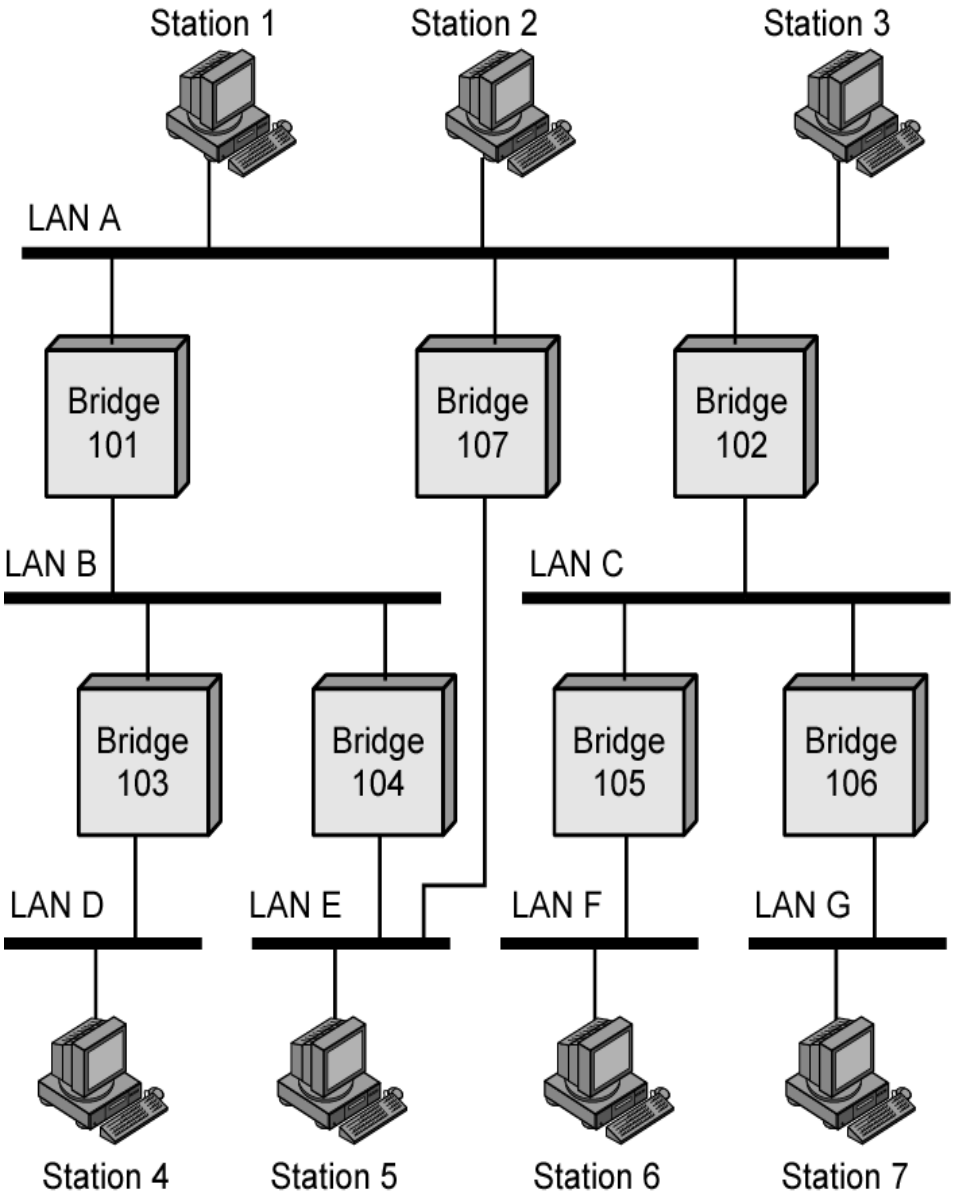
- **Soluzione → Spanning tree**

Spanning tree

- **Lo spanning tree è un sottoinsieme della topologia originaria che non contiene cicli**
- **Si può organizzare l'architettura di bridge e hub in uno spanning tree disabilitando un sottoinsieme di interfacce**
- **La riattivazione, in caso di necessità, è una semplice operazione di riconfigurazione software**



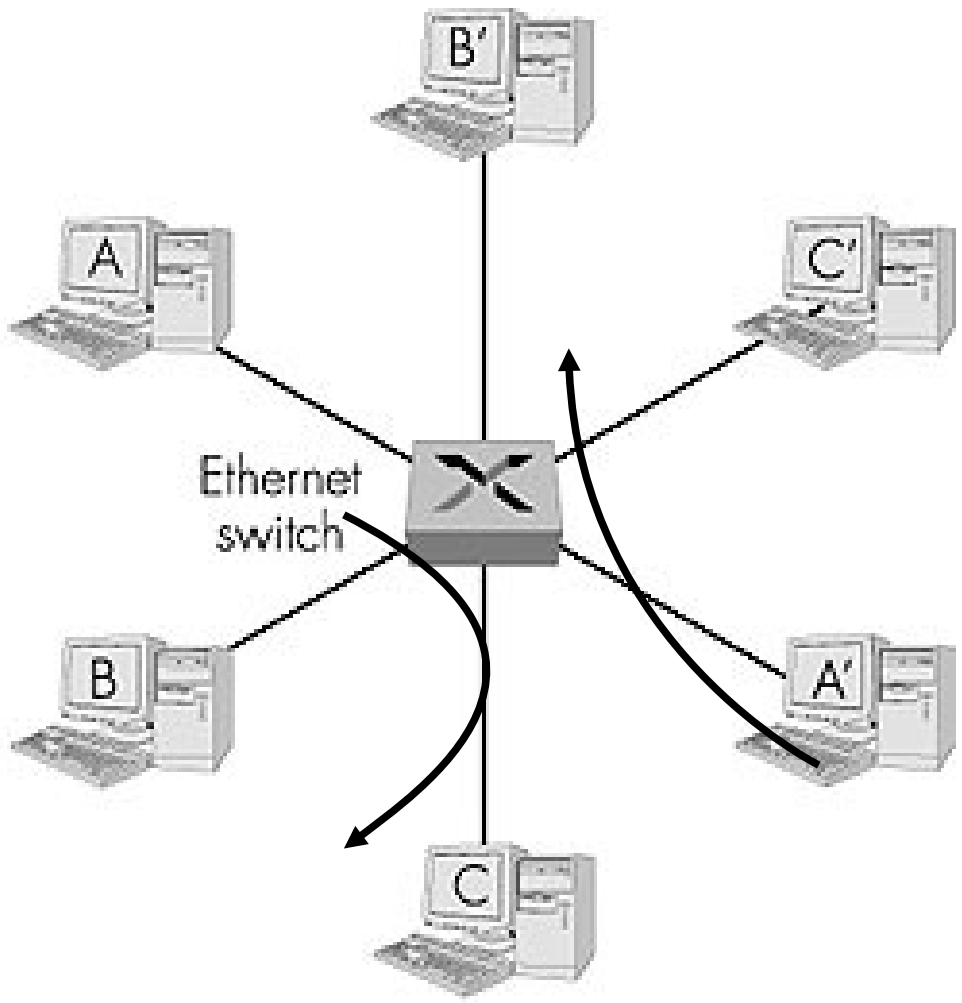
LAN con percorsi alternativi



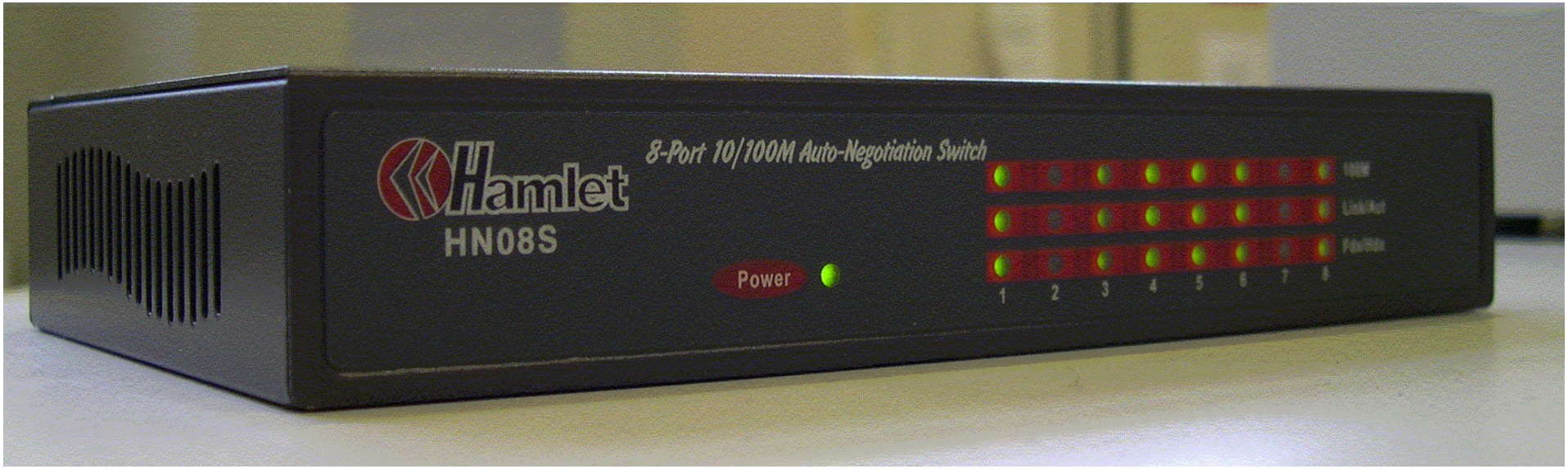
- **Lo spanning tree è un sottoinsieme della topologia originaria che non contiene cicli**
- **Si può organizzare l'architettura di bridge e hub in uno spanning tree disabilitando un sottoinsieme di interfacce**

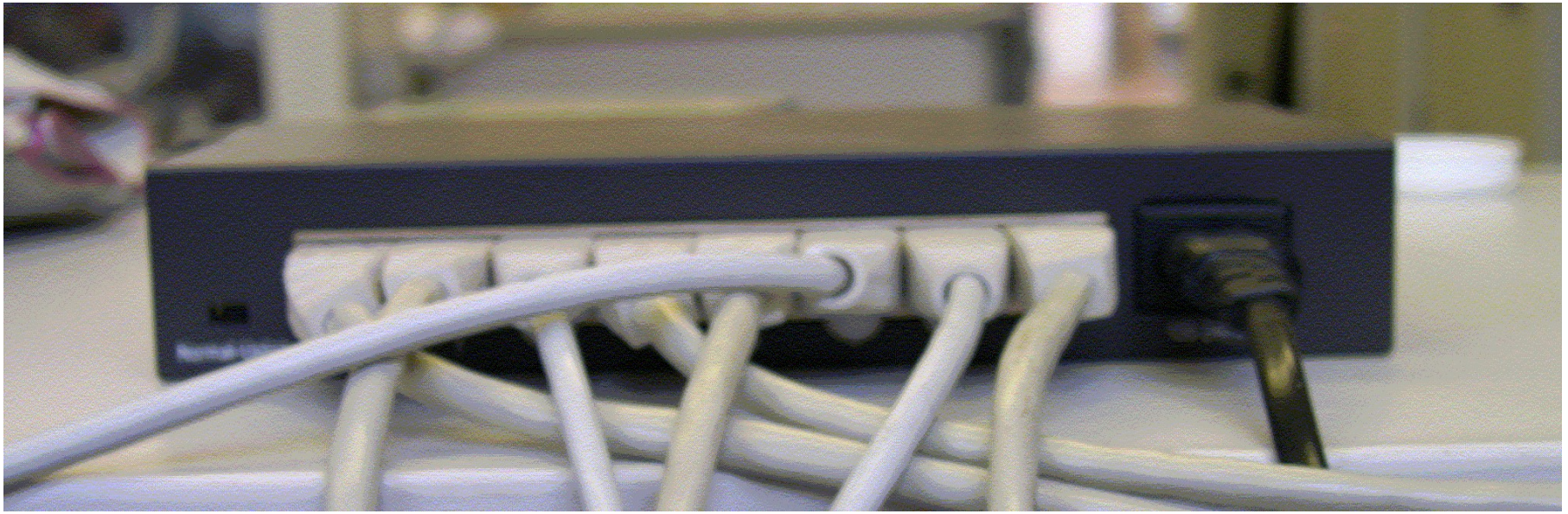
Switch

- **Sono in pratica dei bridge ad alte prestazioni con molte interfacce (e.g., 8-48)**
  - Inoltro di frame a livello 2
  - Filtraggio utilizzando indirizzi MAC
- **Spesso lo switch è usato con singoli host con gli host interconnessi a stella mediante lo switch (in alternativa all'uso di un hub)**



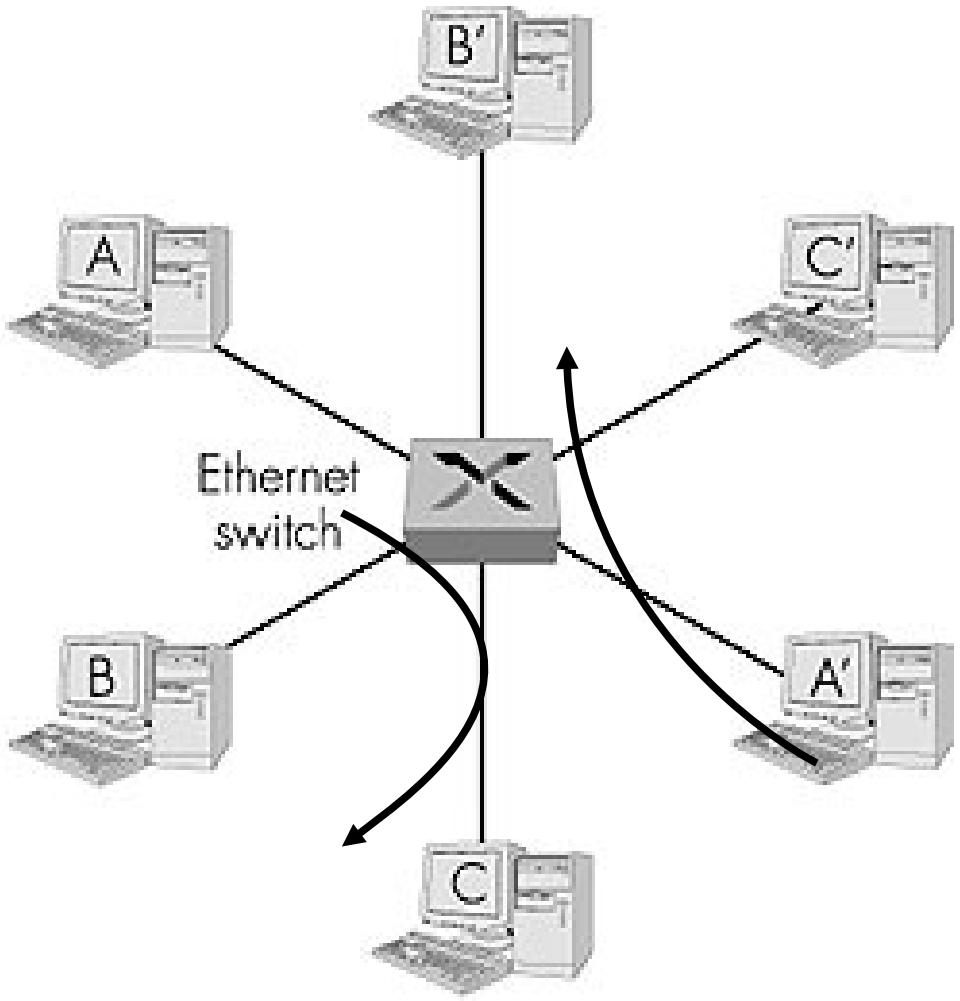
Dispositivo switch 10/100





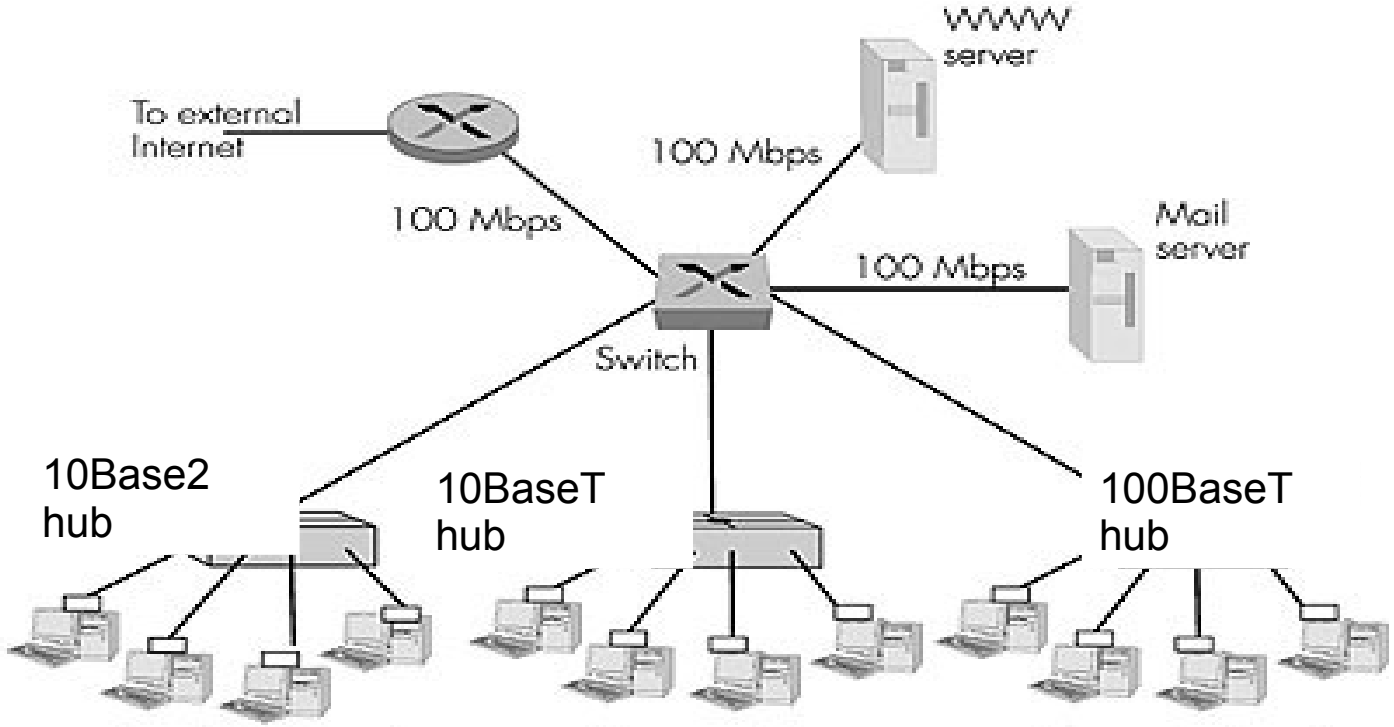
Switch: vantaggi

- **Come nel caso dei bridge, a differenza del caso degli hub, consentono un'architettura Ethernet senza collisioni (accesso dedicato e full duplex)**
- **Esempio di switching:**
  - Traffico tra A-B e tra A'-B' simultaneo, senza collisioni



Switch: vantaggi

- **Consentono la combinazione di interfacce eterogenee (10/100/1000 Mbps) condivise (shared) e dedicate**
- **Consentono la realizzazione di architetture abbastanza complesse**



Tipi di commutazione per switch

- **Switch con commutazione store-and-forward**
  - Quando un frame è instradato attraverso un commutatore store-and-forward, è raccolto e immagazzinato nella sua totalità prima che il commutatore inizi a trasmetterlo sulla linea di uscita

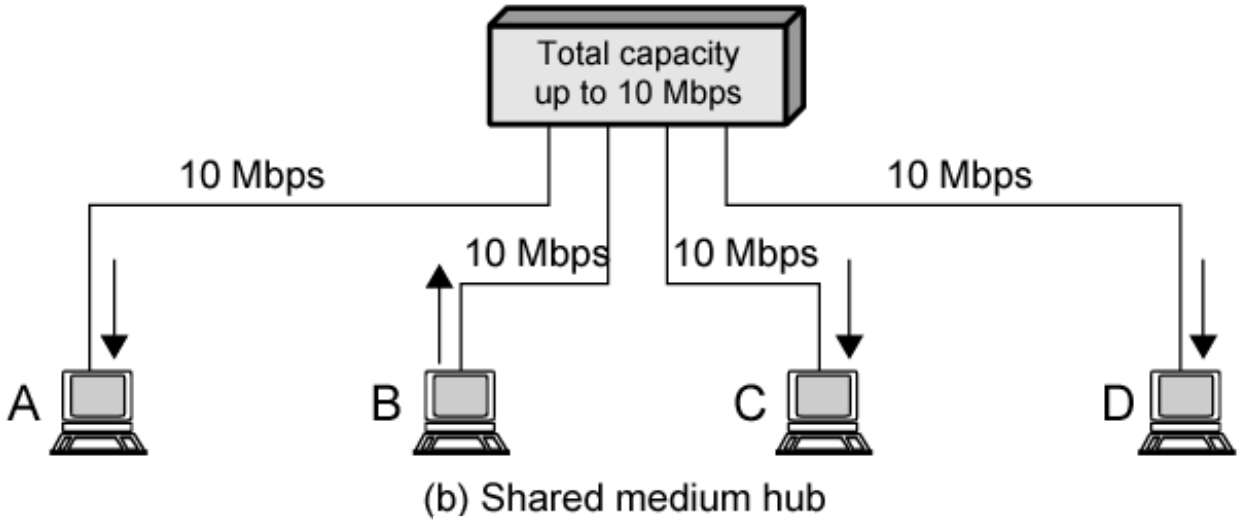
Tipi di commutazione per switch

- **Switch con commutazione cut-through**
  - Il frame è inoltrato dalla porta di input dello switch a quella di output senza aspettare che tutto il frame sia arrivato al commutatore
  - E' sufficiente che sia giunta la parte del frame contenente l'indirizzo di destinazione e che il canale di uscita sia libero

→ **PRO: miglioramento delle prestazioni**

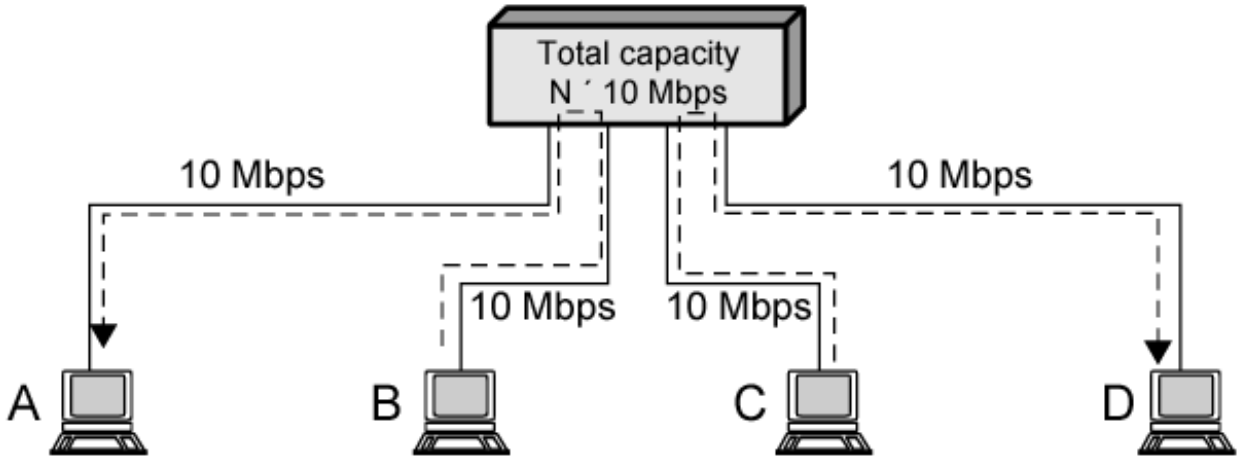
→ **CONTRO: possibile inoltro di frame corrotti (non c'è possibilità di verificare la correttezza del byte di controllo)**

Hub e switch



(b) Shared medium hub

Hub (mezzo condiviso)



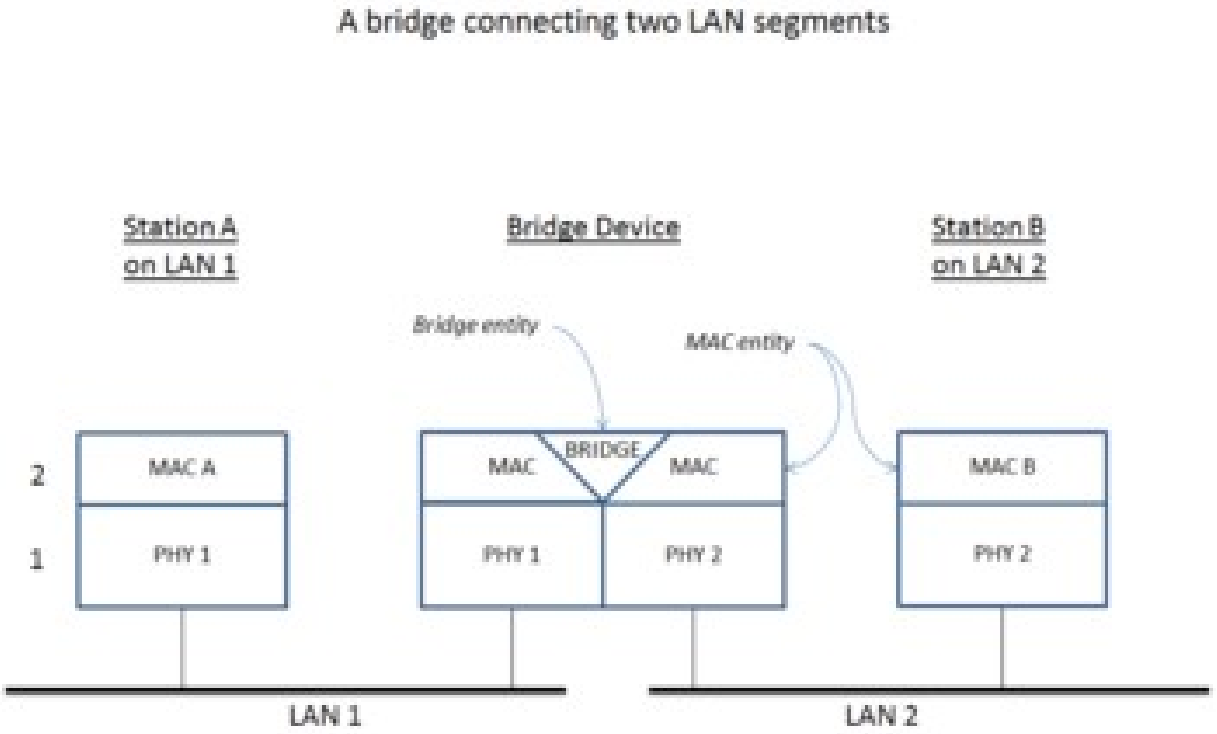
(c) Layer 2 switch

Bridge e switch

- **Apparati concettualmente identici**
- **Tipico scenario di riferimento**
  - Switch → apparato hardware
  - Bridge → sistema software
- **Dove si usano i bridge?**
  - Nelle VM (Tra VM/con host)
  - Nei container (Docker/Kubernetes)
  - Nei server per collegare più porte fisiche (a livello H2N)
  - Per separare tecnologie trasmissive diverse (es Wired/Wireless)

Bridge tra due porte fisiche

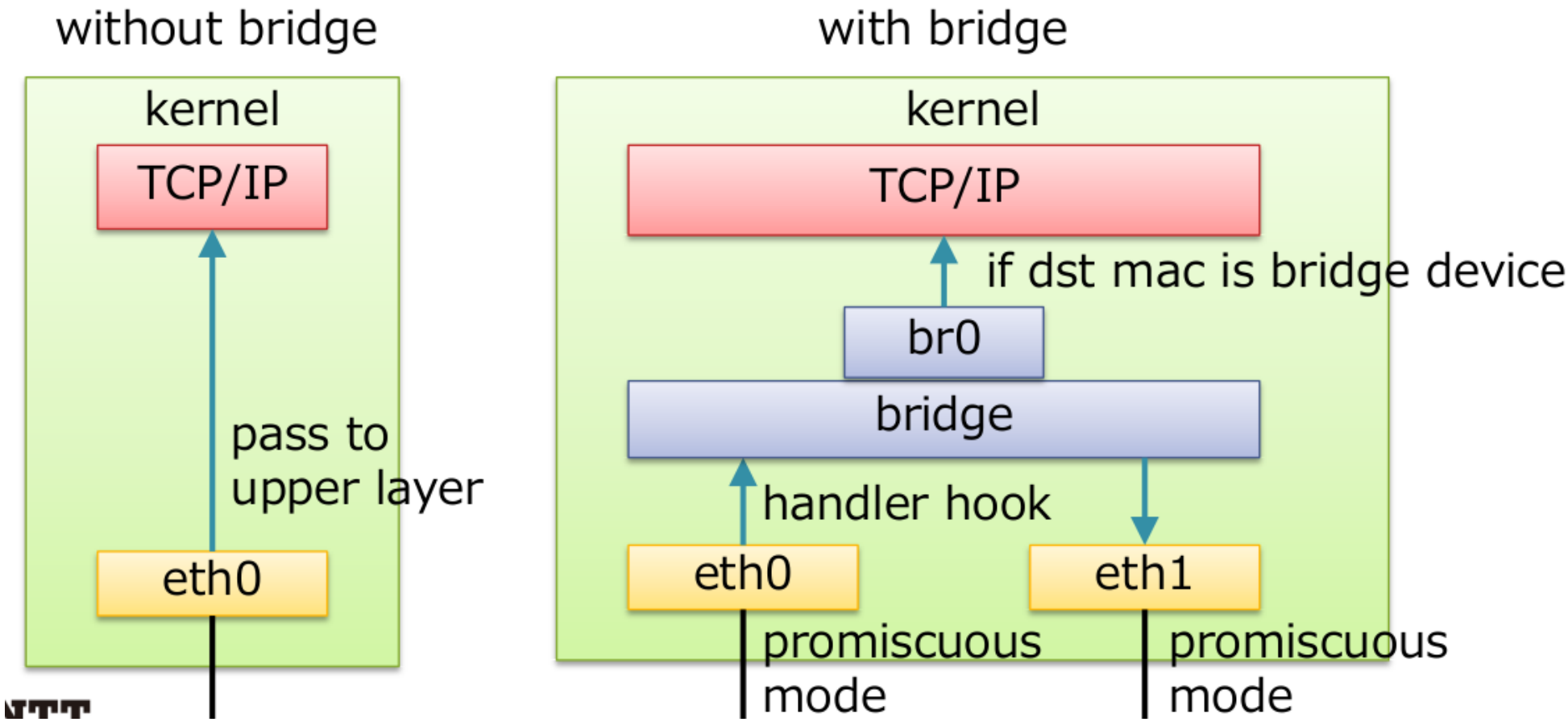
- **Bridge con un host connesso a due segmenti di LAN**



Bridge in Linux

- **All'interno di un sistema Linux è possibile collegare tra loro più interfacce di rete**
  - Vincolo: indirizzi hardware di 6 byte
  - Le interfacce possono essere aggiunte e rimosse in ogni momento
- **Un bridge Linux permette di ottenere la semplicità di inoltro di uno switch Ethernet insieme a funzionalità più avanzate di controllo del traffico. Ad esempio:**
  - Filtering
  - Traffic shaping

Bridge in Linux



Da Linux Conference Japan - 2014

Comandi di riferimento

- **Creazione di un bridge**
  - `brctl addbr <bridge>`
  - `ip link add <bridge> type bridge ...`
- **Aggiungere interfacce al bridge**
  - `brctl addif <bridge> <iface>`
  - `ip link set <iface> master <bridge>`
- **Visualizzazione dei bridge attualmente configurati**
  - `brctl show <bridge>`

Comandi di riferimento

- **Visualizzare la lista degli indirizzi MAC conosciuti dal bridge**
  - `brctl showmacs nomebridge`

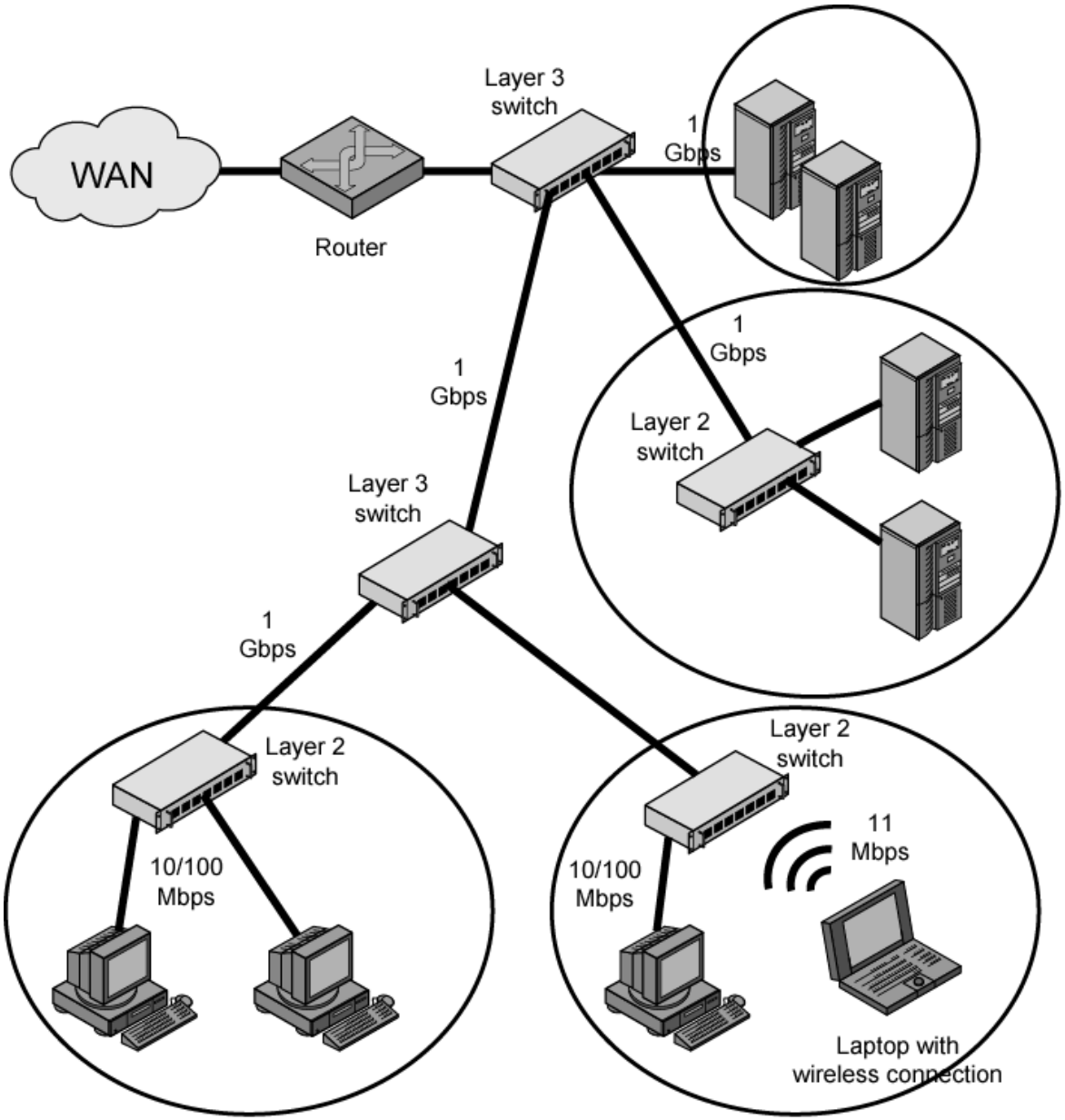
- **Alcuni parametri configurabili**
  - forward delay (default: 30)
  - ageing degli indirizzi
  - STP
  - hairpin mode

Configurazione persistente

- **Riferimento: Linux Debian**
- **Come una interfacce di rete,**
  - Bridge può essere configurato col file /etc/network/interfaces
- **Esempio:**

```
auto br0
iface br0 inet static
    bridge_ports <iface1> <iface2> ...
    address <ip-address>
    ...
```

Tipica architettura dipartimentale



Modulo 6: Virtual LAN

Le virtual LAN

- **Lo standard 802.1Q (2003) definisce le specifiche che permettono di definire più reti locali virtuali (VLAN) distinte, utilizzando una stessa infrastruttura fisica**
- **Ciascuna VLAN si comporta come se fosse una rete locale separata dalle altre**
  - i pacchetti broadcast sono confinati all'interno della VLAN
  - la comunicazione a livello 2 è confinata all'interno della VLAN
  - la connettività tra diverse VLAN può essere realizzata solo a livello 3, attraverso routing
- **Lo standard è definito nell'ambito del protocollo 802.1D (bridging) che in generale riguarda la comunicazione tra diversi standard 802 attraverso bridge**
  - gli switch ethernet sono sostanzialmente bridge monoprotocollo

Scopo delle VLAN

- **L'utilizzo delle Virtual LAN permette di realizzare**
  - risparmio: non è necessario realizzare una nuova infrastruttura di rete locale con apparati e linee dedicate per creare una nuova LAN parallela entro lo stesso ambiente della LAN preesistente
  - aumento di prestazioni: il confinamento del traffico broadcast permette di evitare la propagazione di frame verso destinazioni che non hanno necessità di riceverlo
  - aumento della sicurezza: una utenza connessa ad una VLAN non ha modo di vedere il traffico interno alle altre VLAN
  - flessibilità: lo spostamento fisico di una utenza all'interno dei locali raggiunti dalla infrastruttura di rete può essere realizzato senza modifiche della topologia fisica, ma logicamente attraverso la opportuna riconfigurazione degli apparati di rete (switch o bridge)

Requisiti sui bridge

- **Per realizzare VLAN è necessario che gli switch ed i bridge della infrastruttura di rete siano capaci di distinguere le diverse VLAN**
- **Gli apparati devono quindi osservare lo standard 802.1Q**
- **Vi sono diversi modi per realizzare VLAN**
  - VLAN port based (o private VLAN)
  - VLAN tagged (802.1Q)
- **In ogni caso entro il bridge devono essere definite le VLAN, con nome e numero identificativo per distinguerle una dall'altra**

Funzioni del bridge in 802.1Q

- **Sostanzialmente esistono tre funzioni che i bridge devono saper svolgere per poter gestire più reti virtuali**
  - ingress: il bridge deve essere in grado di capire a quale VLAN appartenga un frame in ingresso da una porta
  - forwarding: il bridge deve conoscere verso quale porta deve essere inoltrato il frame verso destinazione, in funzione della VLAN di appartenenza
  - egress: il bridge deve poter trasmettere il frame in uscita in modo che la sua appartenenza alla VLAN venga correttamente interpretata da altri bridge a valle

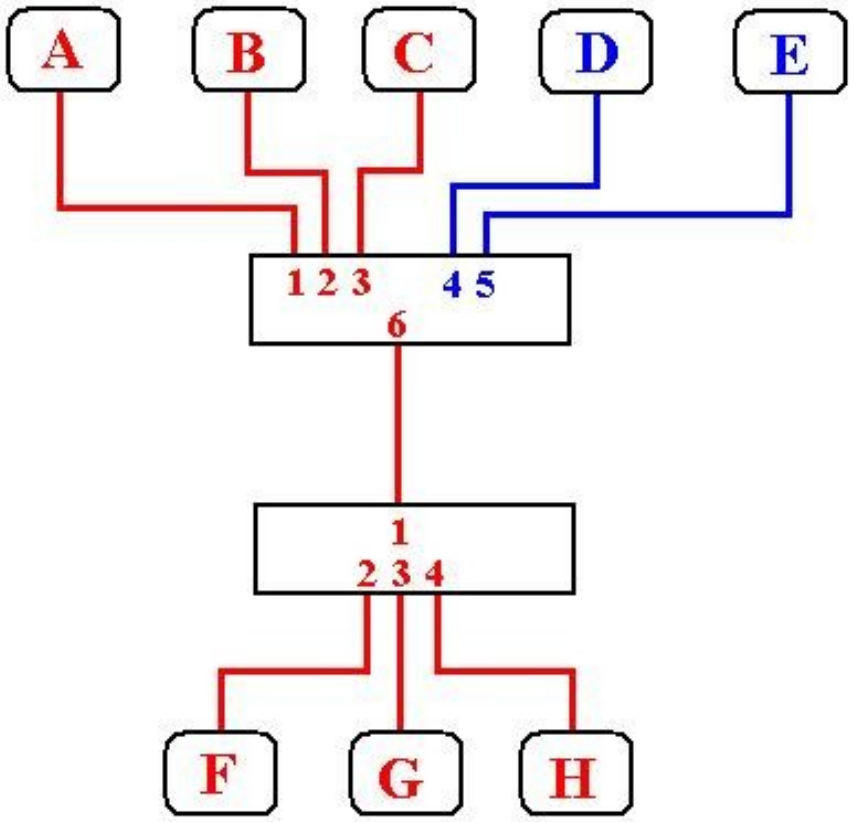
Port based VLAN (untagged)

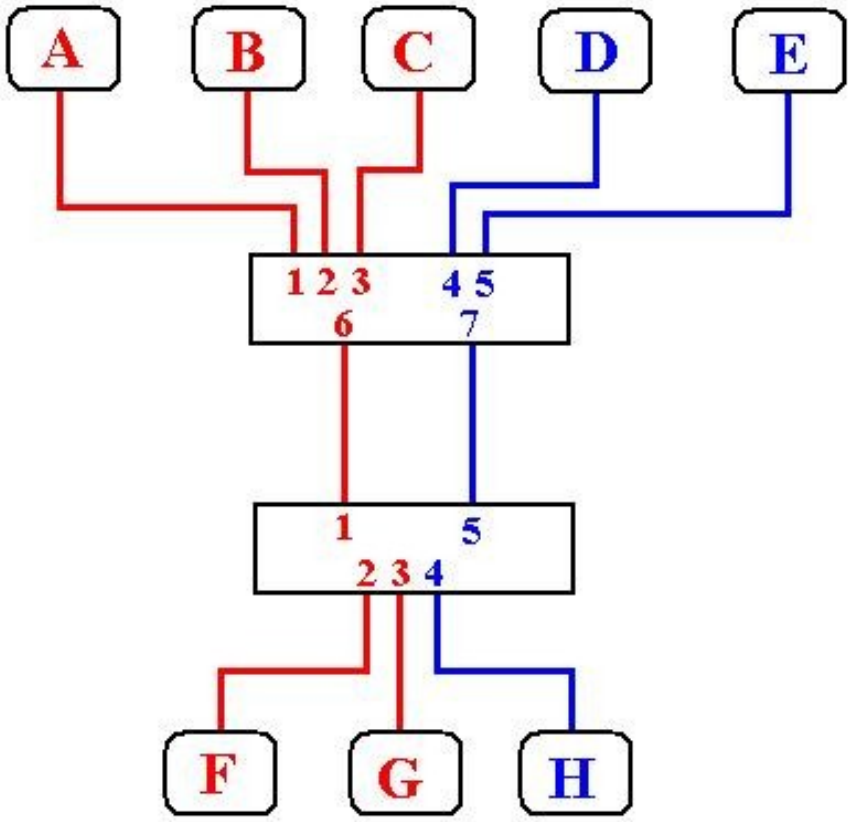
- **Questa tecnica prevede l'assegnazione statica di ciascuna porta del bridge ad una VLAN (definita sul bridge)**
  - porte diverse possono essere assegnate a VLAN differenti
- **Di fatto in questo modo si realizza un partizionamento del bridge in due o più bridge logici**

Port based VLAN (untagged)

- **ingress: un frame in ingresso appartiene alla VLAN a cui è assegnata la porta**
  - non c'è bisogno di utilizzare indicatori di appartenenza sul frame
- **forwarding: il frame potrà essere inoltrato solo verso porte appartenenti alla stessa VLAN a cui appartiene la porta di ingresso**
  - il bridge mantiene un forwarding database distinto per ogni VLAN: nessuna stazione appartenente ad una VLAN potrà essere vista attraverso una porta assegnata ad una VLAN differente
- **egress: una volta determinata la porta (o le porte) attraverso cui deve essere trasmesso il frame, questo può essere trasmesso così com'è**
- **Le VLAN untagged (dette anche private) non richiedono l'osservanza dello standard 802.1Q, ma solo che lo switch ne supporti la configurabilità**

Esempi di VLAN port based



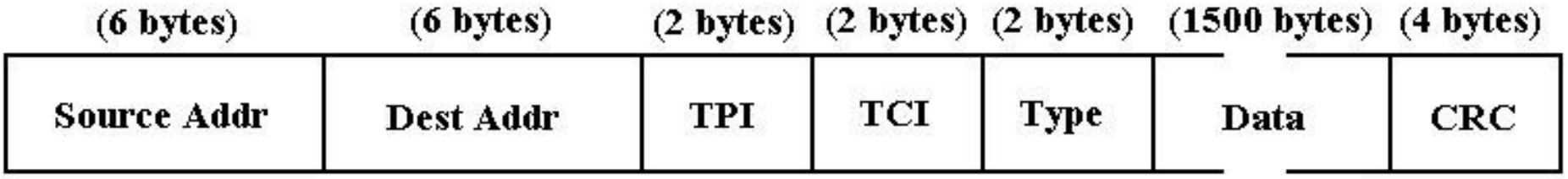


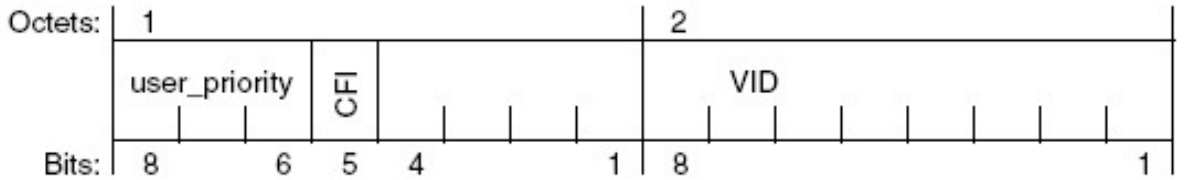
VLAN 802.1Q (tagged VLAN)

- **Lo standard 802.1Q viene utilizzato per poter condividere lo stesso link fisico tra VLAN differenti**
- **Per poter fare ciò il bridge deve poter distinguere la VLAN di appartenenza del frame in arrivo**
- **Lo standard definisce una modifica del formato del frame ethernet aggiungendo 4 byte che trasportano le informazioni sulla VLAN (ed altro)**
- **Poiché tutti i bridge devono concordare sulla VLAN di appartenenza di un frame, l'identificativo (VLAN tag) della VLAN deve essere uguale per tutti i bridge**

Frame (Ethernet) 802.1Q

- **Il formato del frame Ethernet secondo lo standard 802.1Q continene i campi aggiuntivi:**
  - TPI (Tag Protocol Identifier): due bytes di valore 81 00 che identificano il frame come frame 802.1Q
  - TCI (Tag Control Information): due bytes che trasportano le informazioni sulla tag
    - i primi tre bit (user priority) indicano l'eventuale livello di priorita' del frame
    - il quarto bit (CFI) vale 1 se il frame proviene da una LAN token ring
    - i restanti 12 bit (VID) trasportano la VLAN tag (da 0 a 4095)
      - i valori 0 e 4095 sono riservati e non vanno utilizzati come VLAN ID





Considerazioni sul frame

- **Il frame così costituito rappresenta una violazione dello standard Ethernet, in quanto può eccedere la dimensione massima di 1518 bytes**
  - tutti i bridge che osservano lo standard devono poter accettare frame con 2 byte in più
- **Il campo TPI ha un valore che non è utilizzato come "protocol type" nei frame Ethernet ordinari**
  - questo permette di identificare immediatamente se un frame è di tipo 802.1Q
  - una scheda Ethernet non conforme allo standard 802.1Q scarterebbe il frame

Porte tagged ed untagged

- **In un bridge 802.1Q tutte le porte devono essere associate ad una o più VLAN**
  - se la porta è associata ad una VLAN “port based” (untagged) i frame ricevuti da quella porta non trasporteranno TAG, nè dovranno trasportarla i frame in uscita
    - il link attestato su tali porte si dice access link
  - in caso contrario la porta sarà associata ad una o più VLAN in modalità tagged, ed i frame trasporteranno le informazioni di tag
    - il link associato a tali porte si dice trunk link
    - la VLAN di appartenenza del frame è definito dal valore inserito nella TAG

Porte ibride

- **Lo standard richiede che una porta possa essere associata ad una VLAN in modalità untagged, e ad altre VLAN in modalità tagged**
  - il link attestato su tali porte si dice hybrid link
  - l'appartenenza del frame ricevuto ad una VLAN è definito univocamente
    - se non ha il TAG, il frame appartiene alla VLAN a cui la porta è associata in modalità untagged
    - se ha il TAG, la VLAN di appartenenza è definita dal valore trasportato dalla TAG
  - la VLAN a cui la porta è associata in modalità untagged viene anche detta PVID (Private Vlan ID)

Funzioni ingress e forwarding in 802.1Q

- **ingress: quando viene ricevuto un frame il bridge deve identificare la VLAN di appartenenza**
  - se il frame è untagged, la VLAN di appartenenza è identificata con la VLAN a cui la porta è associata in modalità untagged
  - se il frame è tagged, la VLAN di appartenenza viene identificata dal TAG
- **forwarding: una volta identificala la VLAN di appartenenza vengono applicate le regole di forwarding e viene identificata la porta di uscita**
  - la o le porte in uscita devono essere associate alla VLAN di appartenenza del frame

egress: inserimento e rimozione di TAG

- **La funzione egress può richiedere la modifica del frame ricevuto:**
  - se il frame in ingresso è di tipo 802.1Q e la porta in uscita è associata alla VLAN di appartenenza in modalità tagged, il frame viene inoltrato senza modifiche
  - se il frame in ingresso è untagged e la porta in uscita è associata alla VLAN di appartenenza in modalità untagged, il frame viene inoltrato senza modifiche
  - se il frame in ingresso è di tipo 802.1Q e la porta di uscita è in modalità untagged, il TAG deve essere rimosso
  - se il frame in ingresso è di tipo 802.3 e la porta di uscita è associata alla VLAN di appartenenza in modalità tagged, deve essere inserito il TAG
  - negli ultimi due casi, il bridge deve ricalcolare il valore del CRC

Coesistenza con apparati non 802.1Q

- **Gli apparati che non osservano lo standard 802.1Q saranno connessi su porte del bridge associate esclusivamente ad una VLAN in modalità untagged**
  - questo garantisce che
    - ogni frame ricevuto sarà associato ad una VLAN
    - nessun frame di tipo 802.1Q sarà inoltrato verso l'apparato a valle, in quanto il TAG deve essere rimosso
- **Questo permette di inserire in una rete locale apparati 802.1Q senza dover sostituire l'hardware preesistente**

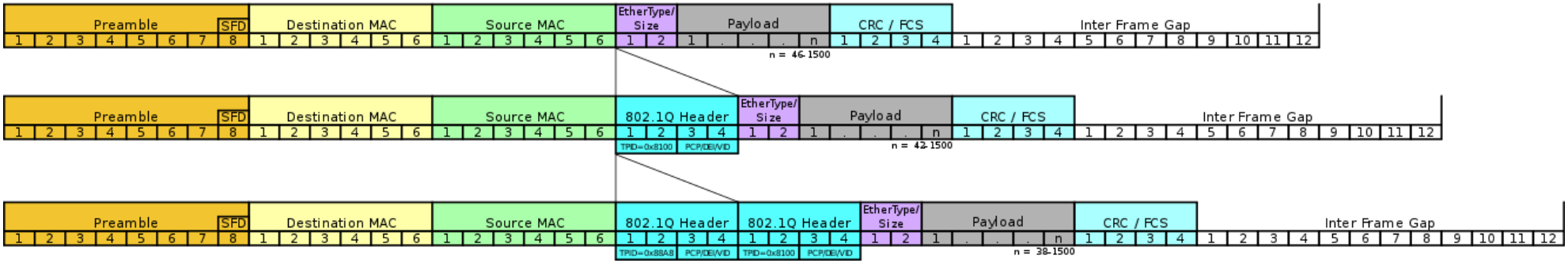
Coesistenza con apparati non 802.1Q

- **Solitamente le interfacce di rete degli host connessi alla LAN non sono compatibili con lo standard 802.1Q**
  - la possibilità di utilizzare 802.1Q su una interfaccia di rete dipende sia dalla scheda che dal driver del sistema operativo
  - tutte le schede moderne installate sui server possono lavorare in modalità 802.1Q
  - tutte le recenti versioni di linux hanno driver che permettono di utilizzare 802.1Q sulle schede che possono farlo
  - su Windows non sempre è possibile

Doppia codifica

- **Ulteriore standard**
  - IEEE 802.1AD
- **Usata da ISP**
- **Due livelli di VLAN**
  - Utente (C-Tag)
  - ISP (S-Tag)
- **S-Tag gestito solo da ISP**
  - Non viene mai visto sulle VLAN del cliente
- **Viene tuttavia preservata la doppia definizione delle VLAN**

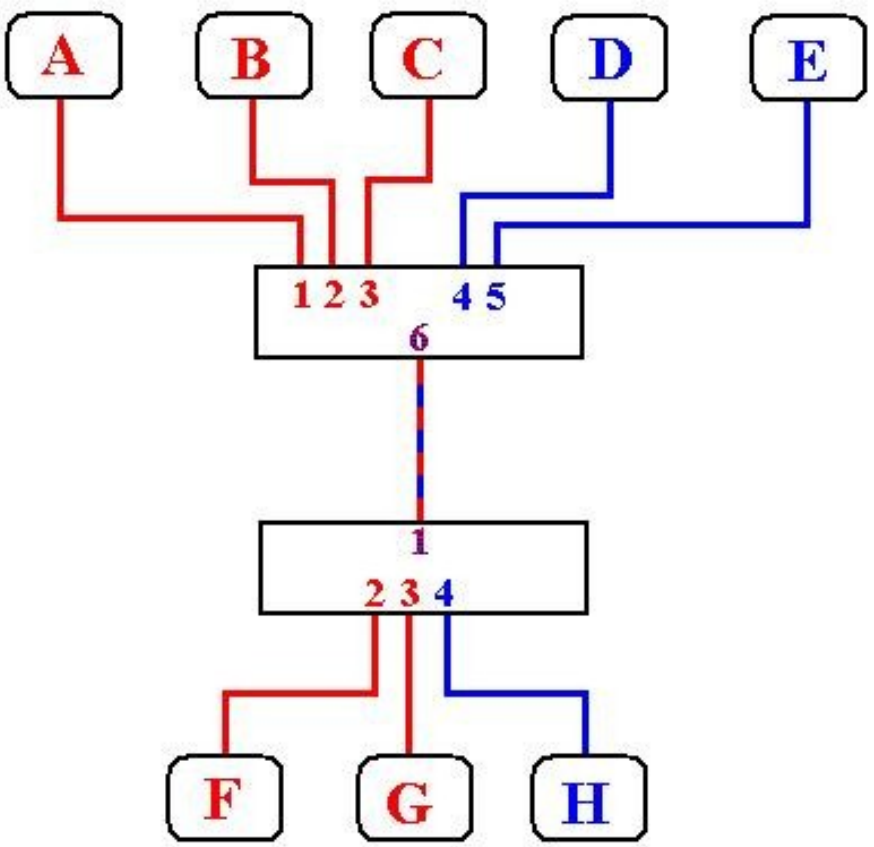
Evoluzione del frame



- **In presenza di doppio tag**
  - Cambia TPID per S-Tag
  - C-Tag resta come in 802-1Q classico

Esempio di topologia 802.1Q

- **Nell'esempio il link tra i due switch è di tipo trunk e trasporta frame di entrambe le VLAN**
- **I frame ricevuti dalle stazioni entrano privi di tag**
- **I bridge devono inserire il tag per trasmettere i frame verso l'altro bridge**
- **I bridge dovranno rimuovere il tag prima di inoltrare i frame verso la stazione di destinazione**
- **Nessun frame appartenente ad una VLAN può raggiungere stazioni connesse su porte associate ad un'altra VLAN**
  - per realizzare una comunicazione tra stazioni appartenenti a VLAN differenti i dati devono essere inoltrati a livello di rete da un router



Protocol based VLAN

- **L'assegnazione di un frame ad una VLAN può essere effettuata dinamicamente, in funzione di diversi parametri**
  - le regole di assegnazione devono essere configurate nei bridge opportunamente
  - non tutti i bridge 802.1Q sono in grado di effettuare l'assegnazione dinamica, anche se osservano lo standard 802.1Q
  - l'applicazione di queste regole viene definita packet filtering
- **I parametri possono essere**
  - indirizzo IP del mittente (se il frame trasporta un pacchetto IP)
  - protocol type del frame Ethernet (IP, NETBios…)
  - indirizzo Ethernet della stazione mittente

Protocol based VLAN

- **Queste regole di assegnazione possono anche convivere con una assegnazione statica, che avrà priorità maggiore**
  - se però il frame ha già un tag, questo ha la precedenza sulle altre regole
- **Alcuni bridge o switch supportano protocolli proprietari che permettono di configurare le regole di assegnazione dinamica centralmente, su uno o più server dai quali lo switch importa le configurazioni**
- **Un esempio tipico è la assegnazione definita dal MAC address: nessuna stazione può accedere ad una VLAN se il suo MAC address non è registrato opportunamente dall'amministratore della rete, indipendentemente dalla porta a cui si connette**

Default VLAN

- **Gli switch 802.1Q vengono venduti con una VLAN predefinita, detta default VLAN,**
  - questa configurazione permette di inserire lo switch in una LAN che non utilizza 802.1Q in modo trasparente
- **Alla default VLAN è assegnato il TAG 1**
- **Tutte le porte appartengono alla default VLAN in modalità untagged (PVID = 1)**

VLAN di management

- **Tutti gli switch 802.1Q sono gestibili in remoto via TCP/IP**
  - l'indirizzo IP viene assegnato ad una VLAN, e lo switch sarà raggiungibile via TCP/IP solo all'interno della VLAN a cui è assegnato l'indirizzo IP (o via routing)
  - gli switch layer 2 hanno generalmente la possibilità di avere un solo indirizzo IP
  - gli switch layer 3 possono avere piu' indirizzi IP assegnati a VLAN differenti, ed eventualmente possono fare routing tra le VLAN
- **E' consigliabile per motivi di sicurezza creare una VLAN dedicata al management degli apparati di rete**