Livello Collegamento

Protocolli Mac

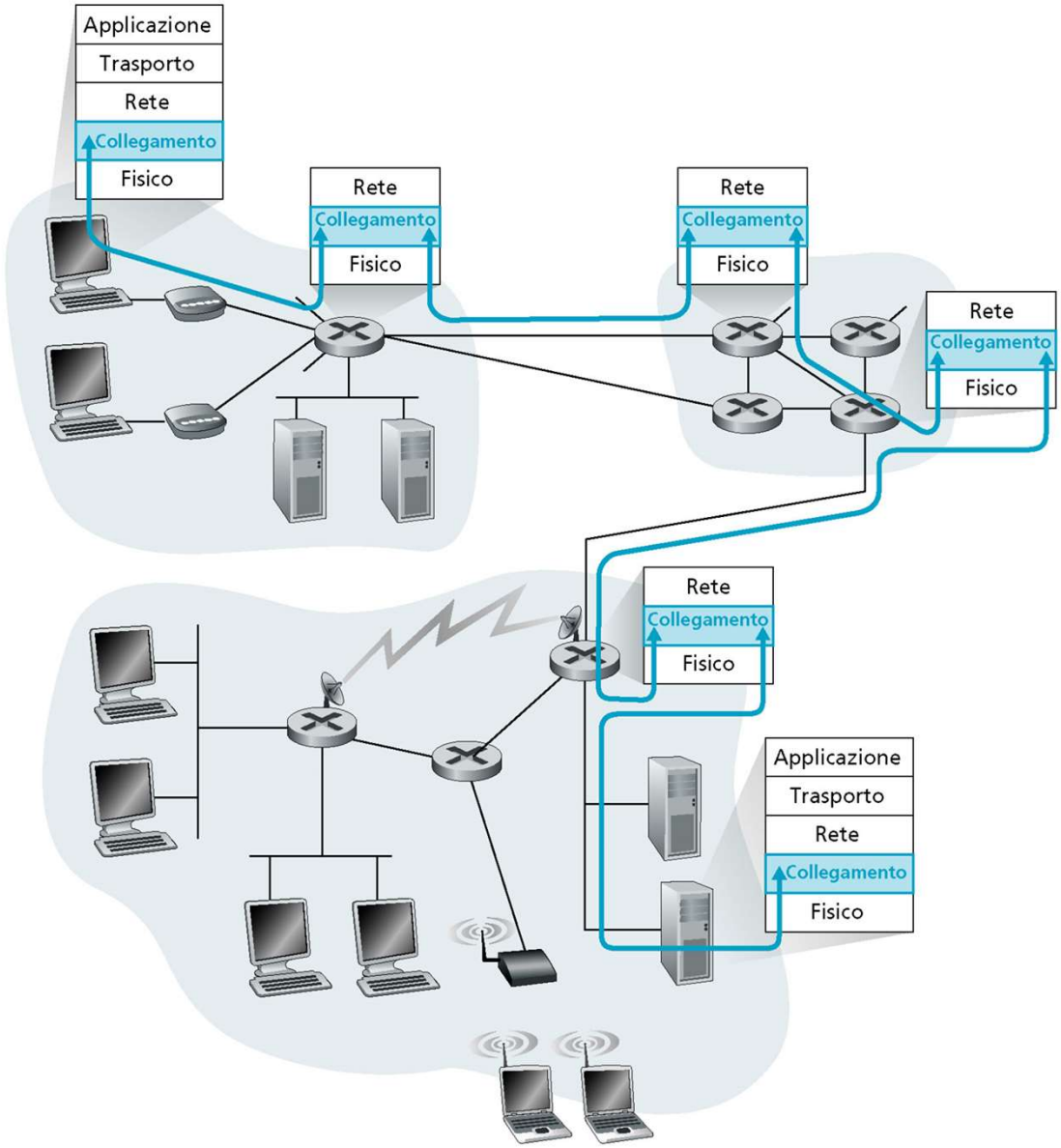
Indirizzamento

ARP

Reti di Calcolatori

Federica Paganelli

Il livello Collegamento muove i datagrammi da un nodo al nodo adiacente su un singolo link di comunicazione

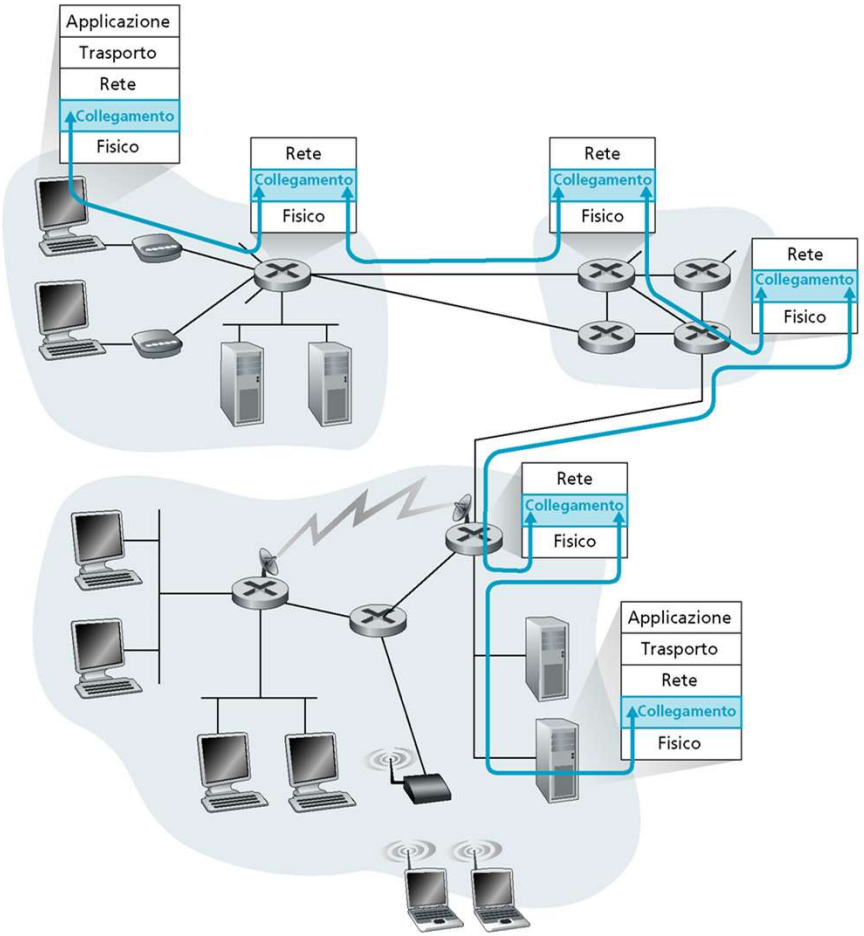


Livello collegamento

Terminologia

- host e router: nodi
- canali di comunicazione che collegano nodi adiacenti lungo un cammino sono collegamenti (link)
  - Collegamenti cablati
  - Collegamenti wireless

- unità dati di livello 2: frame (trama)
  - Incapsula un datagramma



Livello collegamento

- Un datagramma può essere gestito da diversi protocolli,
  - su collegamenti differenti:
  - Es., un datagramma può essere gestito da Ethernet sul primo collegamento, da un collegamento wireless 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.

Livello collegamento

- Collegamenti
  - Punto-punto: collegamento dedicato a due soli dispositivi
    - Collegamenti WAN, Switched LAN Ethernet,…
  - Broadcast: collegamento condiviso tra più dispositivi. Quando un nodo trasmette un frame, il canale lo diffonde e tutti gli altri nodi ricevono una copia
    - Wireless LAN, reti satellitari, Ethernet…

Servizi offerti

- Framing
  - I protocolli incapsulano i datagrammi del livello di rete all'interno di un frame a livello di link.
  - Frame: campo dati, intestazione e eventuale trailer
  - Il framing separa i vari messaggi durante la trasmissione da una sorgente a una destinazione
  - Per identificare origine e destinatario sono utilizzati indirizzi di livello collegamento (diversi rispetto agli indirizzi IP!)
- Consegna affidabile
  - È considerata non necessaria nei collegamenti che presentano un basso numero di errori sui bit (es. fibra ottica, cavo coassiale e doppino intrecciato)
  - È spesso utilizzata nei collegamenti soggetti a elevati tassi di errori (es.: collegamenti wireless)

Servizi offerti

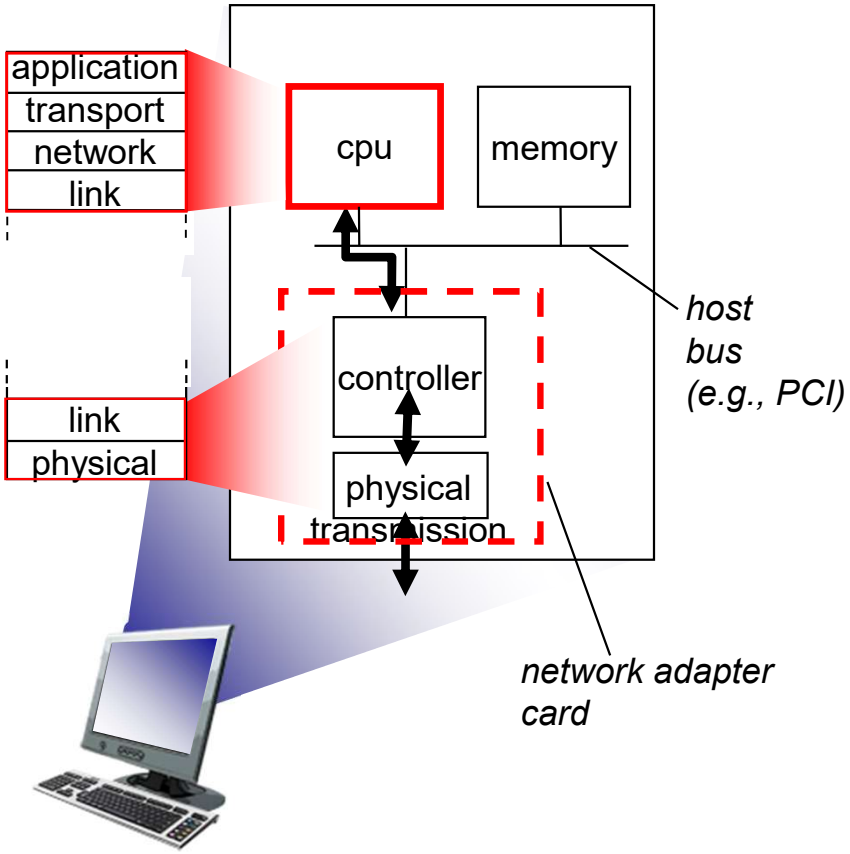
- Controllo di flusso
  - Evita che il nodo trasmittente saturi quello ricevente.
- Rilevazione degli errori
  - Gli errori sono causati dall'attenuazione del segnale e da rumore elettromagnetico.
  - Il nodo ricevente individua la presenza di errori
  - è possibile grazie all'inserimento, da parte del nodo trasmittente, di 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.

Livello collegamento

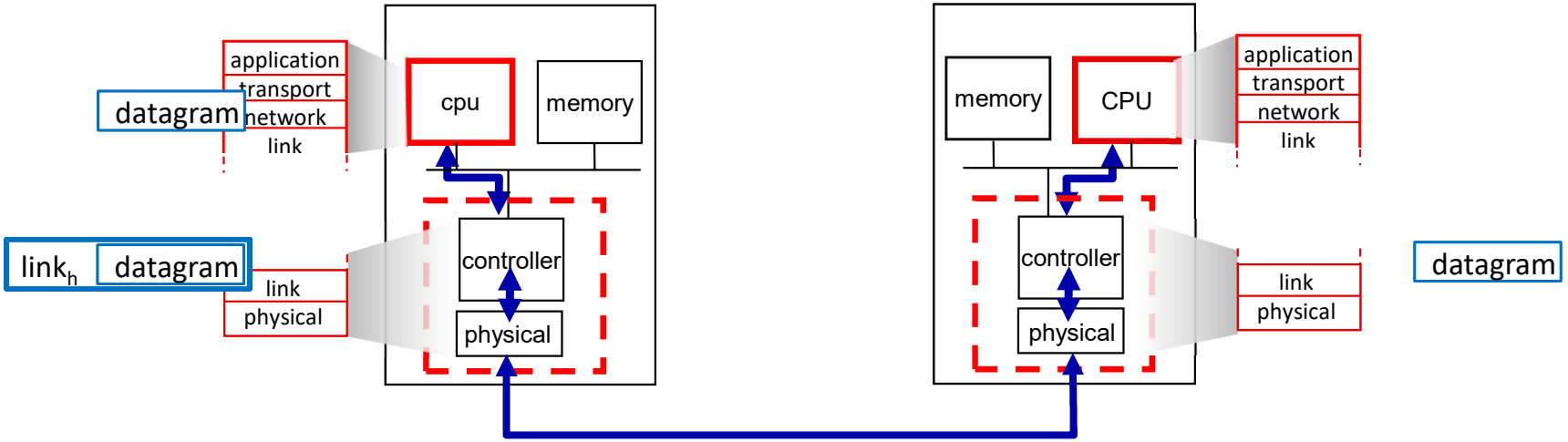
- Suddivisibile in due sottolivelli
- Data-Link Control:
  - Framing
  - Flow and Error Control
- Medium Access Control
    - Accesso al mezzo (in canali broadcast rischio collisione)
    - Regole per accedere al mezzo

Dove è implementato il livello collegamento?

- Presente in ogni host
- link layer implementato in un "adaptor" o scheda di rete (*network interface card* NIC)
  - Ethernet card, 802.11 card;
  - Implementazione dei livelli link e fisico
- Collegato al system bus dell'host
- Combinazione di hardware and software
  - Operazioni in software eseguite dalla CPU
    - Mittente: assemblaggio delle informazioni di indirizzamento; attivazione del controller
    - Ricevente: risponde agli interrupt del controller, gestione degli errori, passaggio del datagramma a livello di rete



Comunicazione tra adaptor



Lato mittente:

- Incapsula il datagramma in un frame
- aggiunge error checking bits, rdt, flow control, etc

Lato destinatario

- controllo errori, rdt, flow control, etc.
- Estrae il datagramma, lo passa al livello superiore

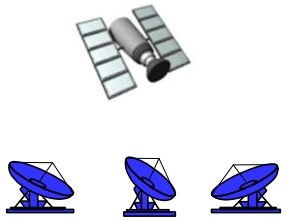
Collegamenti ad accesso multiplo

Due tipi di "link":

- point-to-point
  - PPP per accesso dial-up
  - Collegamento point-to-point link tra switch Ethernet e host
- *broadcast (cavo o mezzo condiviso)*
  - old-fashioned Ethernet
  - 802.11 wireless LAN

shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Protocolli ad accesso multiplo

- Canale di broadcast singolo e condiviso
- Due o più trasmissioni simultanee dai nodi: interferenza
  - *collisione* se un nodo riceve due o più segnali nello stesso istante

Protocollo ad accesso multiplo

- algoritmo distribuito che determina come i nodi condividono il canale, i.e., determina quando il nodo può trasmettere
- La comunicazione per la condivisione del canale deve usare il canale stesso!

Un protocollo di accesso multiplo ideale

dato: canale broadcast con rate R bps

desiderata:

1. Quando un solo nodo trasmette, può inviare dati con un rate di R bps.
2. quando M nodi vogliono trasmettere, ciascuno trasmette ad un rate medio R/M
3. decentralizzato
   - Non ci sono nodi speciali che coordinano la trasmissione
4. semplice

Protocolli MAC

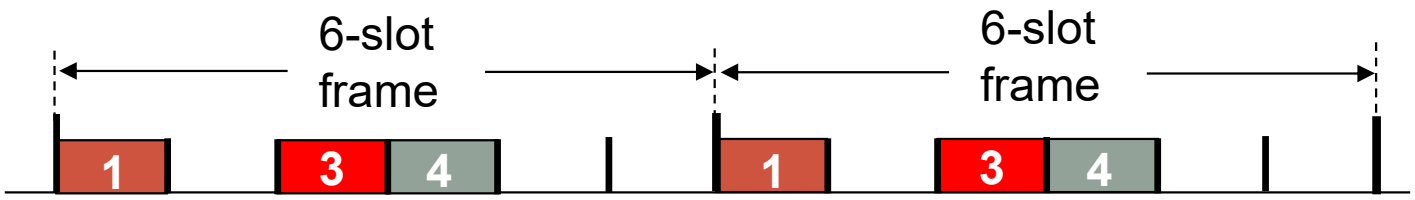
Tre classi principali di protocolli:

- *a suddivisione del canale*
  - Dividono il canale in "pezzi" (risorse) più piccoli (time slot, frequenza, codice)
  - La risorsa è allocata al nodo in modo esclusivo
- *ad accesso random*
  - Il canale è condiviso, possono esserci collisioni
  - meccanismi per "recuperare" da eventi di collisione
- *a rotazione*
  - Rotazione tra i nodi

Channel partitioning MAC protocols: TDMA

TDMA: time division multiple access

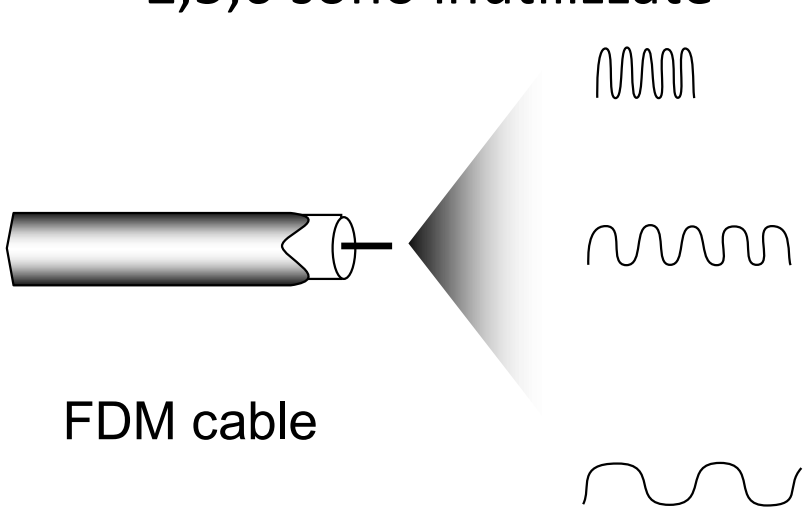
- Accesso al canale in “intervalli di tempo"
- Ciascun intervallo di tempo è suddiviso in time slot
- Ogni stazione ha a disposizione un time slot di lunghezza fissa (length = packet transmission time) in ogni intervallo
- Gli slot non utilizzati sono sprecati
  - esempio: 6-stazioni LAN, 1,3,4 hanno dati da inviare, slots 2,5,6 non utilizzati

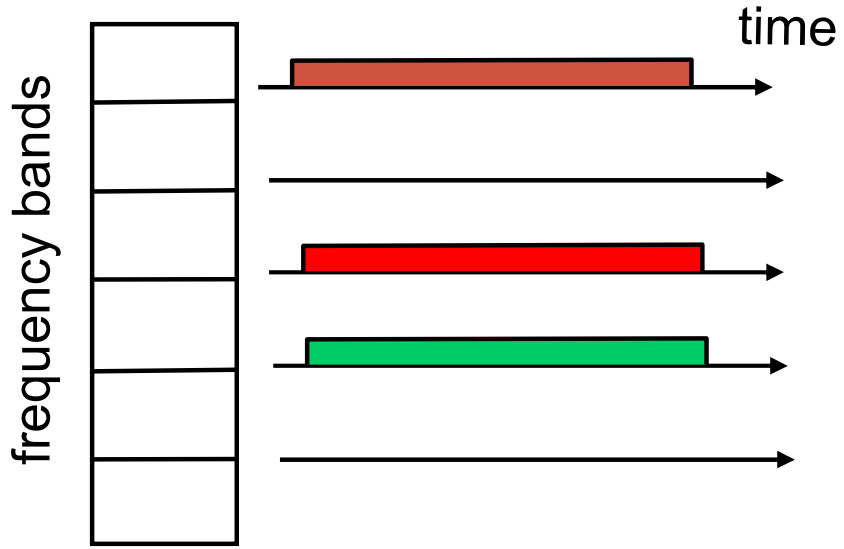


Channel partitioning MAC protocols: FDMA

FDMA: frequency division multiple access

- Spettro del canale diviso in bande di frequenza
- Ad ogni stazione è assegnata una banda di frequenza fissa
- Se ci sono stazioni che non trasmettono, le rispettive bande di frequenza non sono utilizzate
- esempio: 6-station LAN, 1,3,4 inviano dati, le bande di frequenza 2,5,6 sono inutilizzate





Protocolli ad accesso random

- Quando un nodo deve inviare dati
  - trasmette al massimo rate del canale R.
  - non c'è coordinamento *a priori* tra i nodi
- Due o più nodi trasmettono simultaneamente ➜ "collisione",
- Un protocollo MAC ad accesso random specifica:
  - Come rilevare le collisioni
  - Come recuperare dopo le collisioni (e.g., con ritrasmissioni ritardate)
- esempi
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

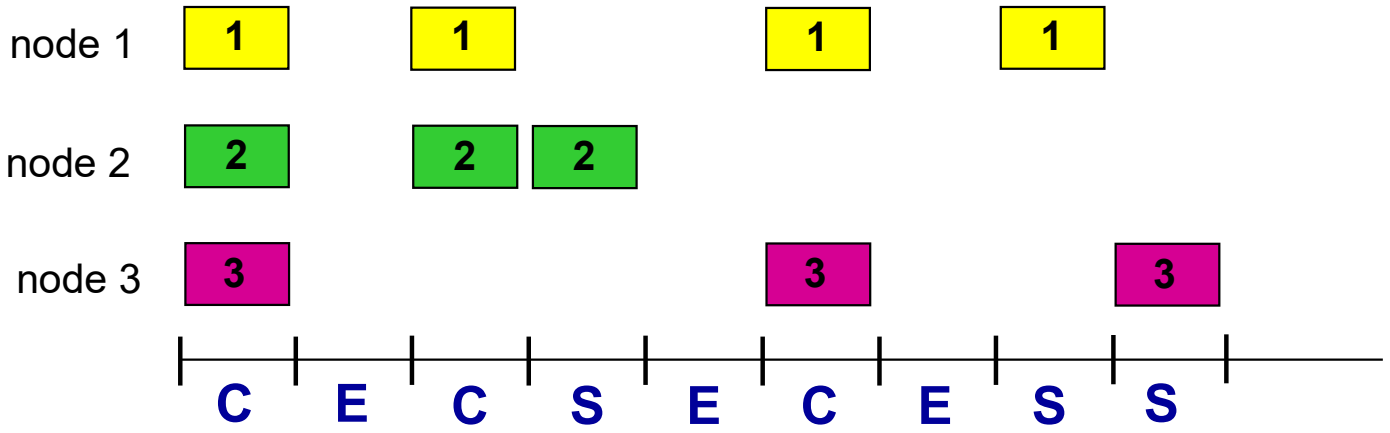
assunzioni:

- time diviso in slot uguali e fissi
- I nodi iniziano a trasmettere all'inizio dello slot
- I nodi sono sincronizzati
- se 2 o più nodi trasmettono, ogni nodo rileva la collisione

funzionamento:

- Quando il nodo deve trasmettere un frame, comincia a trasmetterlo all'inizio dello slot successivo
  - *Se non ci sono collisioni:* il nodo può inviare un nuovo frame nello slot successivo
  - *Il nodo rileva una collisione:* il nodo ritrasmette con probabilità *p* il frame nello slot successivo finché la trasmissione non ha successo

Slotted ALOHA



Pros:

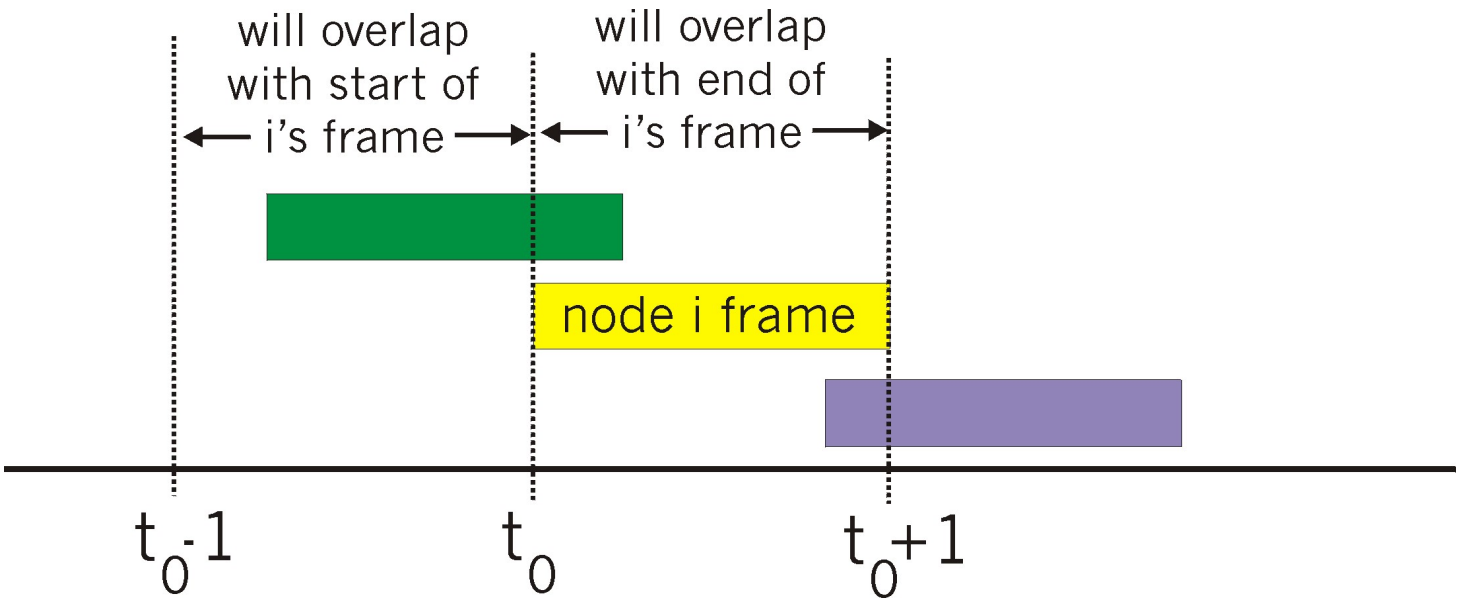
- Il singolo nodo attivo può trasmettere alla massima velocità consentita dal canale
- Fortemente decentralizzato: devono essere sincronizzati solo gli slot
- semplice

Cons:

- collisioni, spreco di slot
- Se c'è un gran numero di nodi attivi canale usato con successo solo il 37% del tempo

ALOHA puro (unslotted)

- Più semplice: non serve la sincronizzazione
- Quando il nodo ha dati da inviare
  - li trasmette immediatamente
- Probabilità di collisione maggiore rispetto allo slotted Aloha
  - Un frame inviato a t_0 collide con altri frame inviati nell'intervallo $[t_0-1,t_0+1]$



CSMA (carrier sense multiple access)

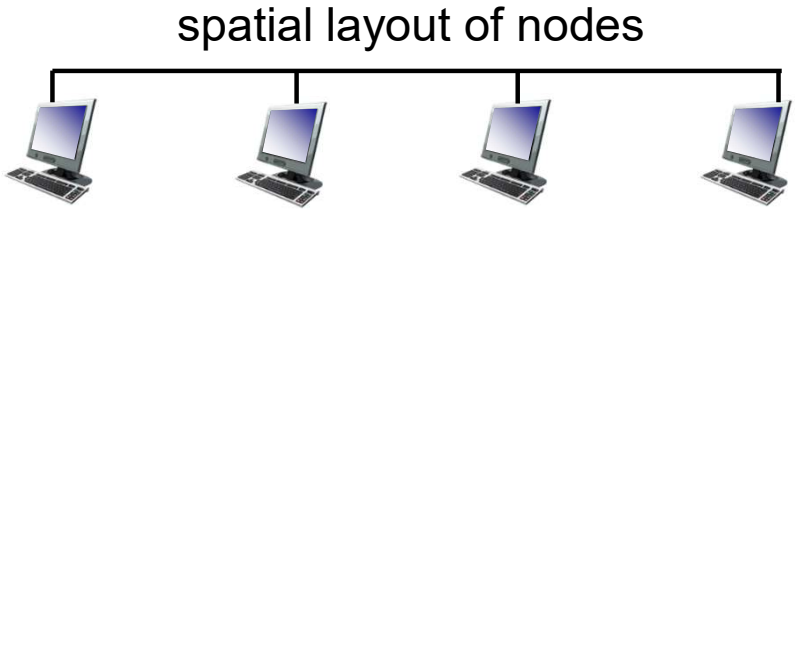
CSMA: ascoltare prima di parlare:

Se il canale è libero: trasmette l'intero frame

- Se il canale è occupato, ritarda la trasmissione

Non interrompere qualcuno che sta parlando!

CSMA: collisioni



- Le collisioni *possono ancora avvenire*: a causa del ritardo di propagazione due nodi potrebbero non rilevare le comunicazioni reciproche
- collisione: tempo di trasmissione del pacchetto sprecato
  - La distanza e il ritardo di propagazione influiscono sulla probabilità di rilevare collisioni

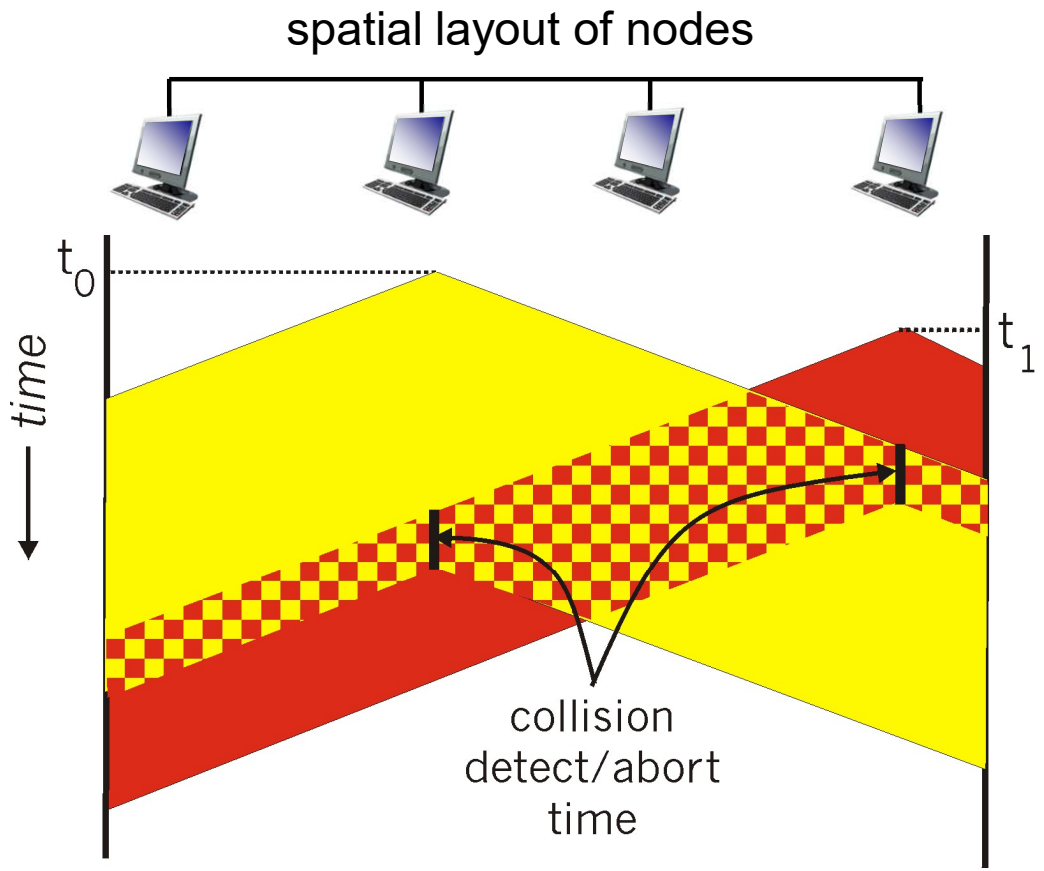
CSMA/CD (collision detection)

CSMA/CD: carrier sensing

- Le transmissioni che collidono vengono abortite, minori perdite

- collision detection:
  - facile in LAN cablate
  - difficile in LAN wireless

CSMA/CD (collision detection)



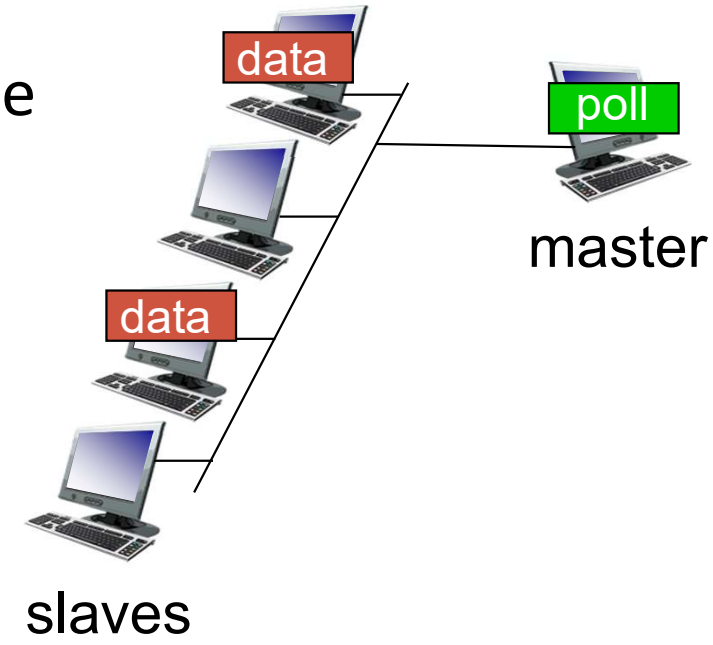
Ethernet CSMA/CD algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame!
4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. After aborting, NIC enters *binary (exponential) backoff:*
   - after *m*th collision, NIC chooses *K* at random from $\{0,1,2, \ldots, 2^m-1\}$. NIC waits $K \cdot 512$ bit times, returns to Step 2
   - longer backoff interval with more collisions

Protocolli MAC a "rotazione"

polling:

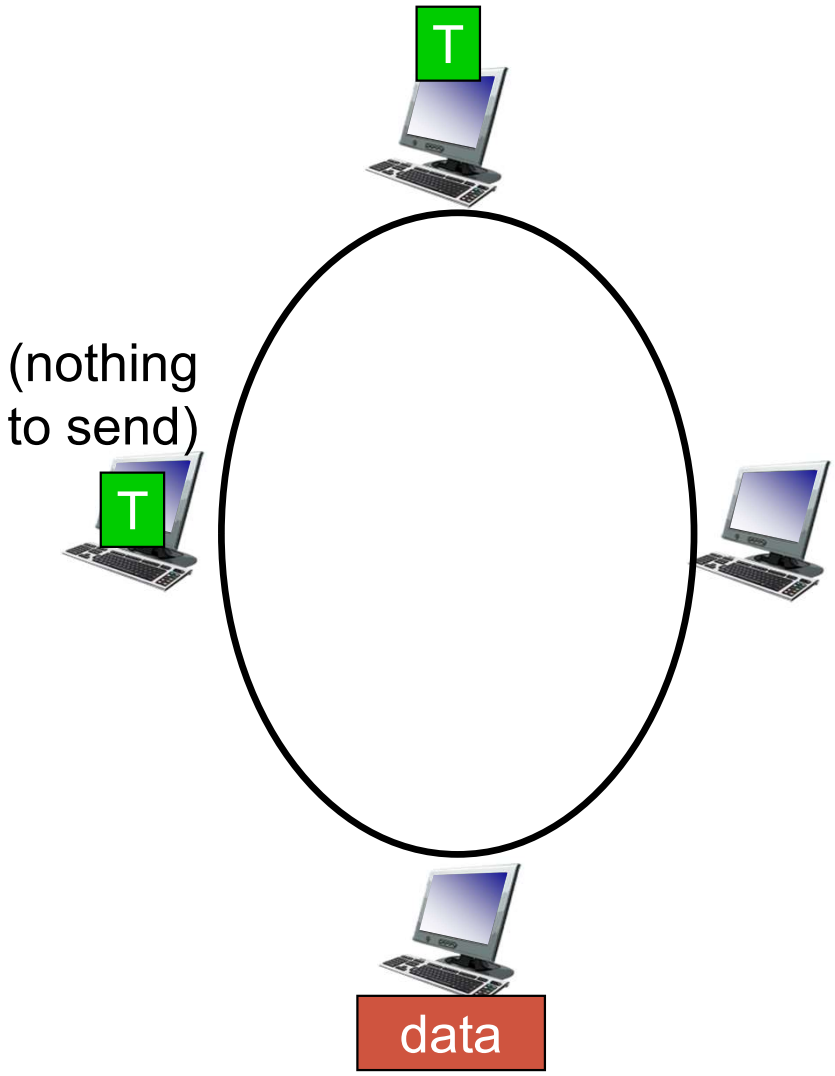
- Il nodo master "invita" i nodi slave a trasmettere a rotazione
- Usato tipicamente con dispositive slave "dumb"
- svantaggi:
  - polling overhead
  - latenza
  - single point of failure (master)



Protocolli MAC a "rotazione"

token passing:

- *token* passato da nodo a nodo.
- token message
- svantaggi
  - token overhead
  - latenza
  - single point of failure (token)



Sintesi

- *Suddivisione del canale*
  - Time Division, Frequency Division
- *random access* (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD in Ethernet
  - CSMA/CA in 802.11
- *rotazione*
  - polling from central site, token passing
  - Bluetooth, FDDI, token ring

Indirizzi a livello collegamento

- Un indirizzo del livello collegamento
  - è associato alla scheda di rete, non al nodo, ed è tipicamente permanente (anche se è possibile modificarlo);
  - è detto indirizzo fisico o indirizzo LAN o indirizzo MAC (Media Access Control);
  - per le LAN Ethernet e IEEE 802.11 è lungo sei byte (2^{48} possibili indirizzi) ed è espresso in notazione esadecimale (12 cifre esadecimali).
    - Esempio: 1A-63-F9-BD-06-9B
  - Come viene garantita l'univocità?
    - IEEE definisce ed assegna i primi 24 bit (OUI – Organization Unique Identifier), mentre i rimanenti 24 bit vengono gestiti dalle aziende ed assegnati a livello locale.
    - Quando una società vuole costruire adattatori, compra un blocco di spazio di indirizzi (univocità degli indirizzi).

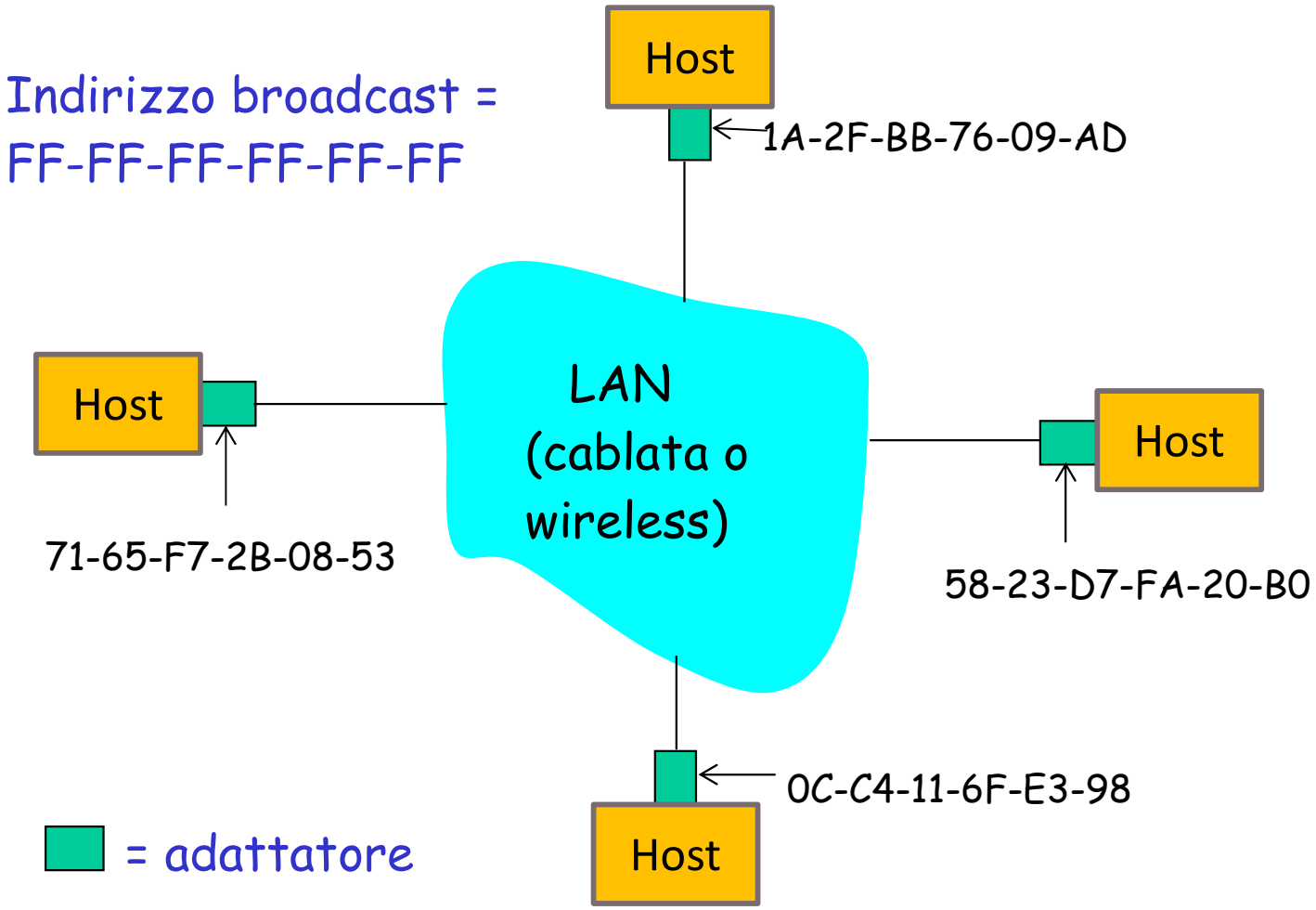
Indirizzi MAC e ARP

- Indirizzo MAC (o LAN o fisico o Ethernet):
  - Struttura piatta
  - Analogo al numero di codice fiscale di una persona: ha una struttura «piatta» e non varia a seconda del luogo in cui la persona si trasferisce.
  - Indirizzo a 48 bit (per la maggior parte delle LAN) .

- 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 (rete).

Indirizzi LAN

Ciascun adattatore di una LAN ha un indirizzo MAC univoco



un adattatore inserisce l'indirizzo MAC di destinazione per spedire un frame

- In LAN broadcast il frame sarà ricevuto ed elaborato da tutti gli adattatori della LAN.
- Ogni scheda controlla se l'indirizzo MAC corrisponde al proprio.
- In caso positivo estrae il datagramma e lo passa al livello superiore.
- In caso negativo scarta il datagramma

Indirizzamento

- Quando un adattatore spedisce un frame, vi inserisce l'indirizzo MAC della scheda di destinazione.
- Nel caso di reti LAN Broadcast, tutti gli adattatori attestati sulla rete controllano l'indirizzo destinazione e passano i dati allo strato superiore solo se riconoscono il proprio indirizzo MAC nell'intestazione.
- Se un adattatore trasmittente vuole che tutte le schede di rete passino i dati agli strati superiori, immette nel campo indirizzo destinazione: FF-FF-FF-FF-FF-FF, ovvero l'indirizzo broadcast

Risoluzione degli indirizzi

- Problema

- Normalmente all'accensione una macchina conosce:
  - il suo indirizzo MAC
  - il suo indirizzo IP (e la rete locale a cui appartiene)
  - il suo indirizzo alfanumerico

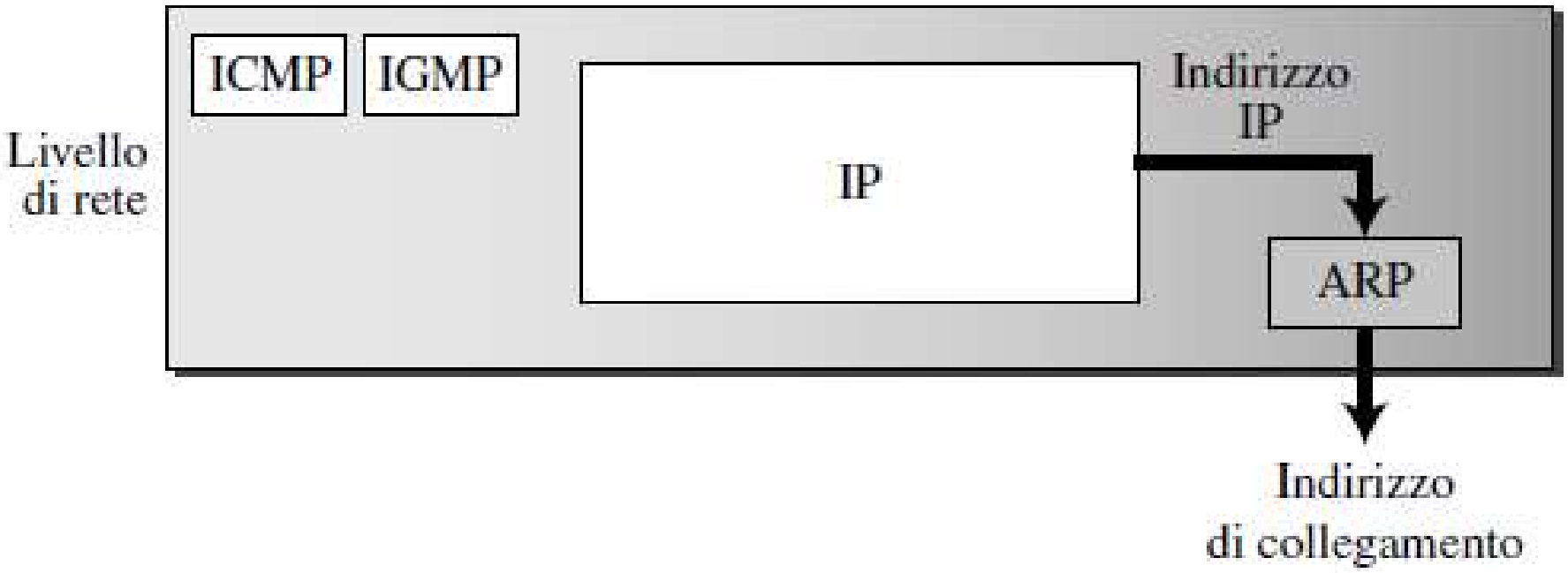
- NON sa:
  - chi ha attorno (macchine "visibili" direttamente)

Risoluzione degli indirizzi

ARP: Address Resolution Protocol

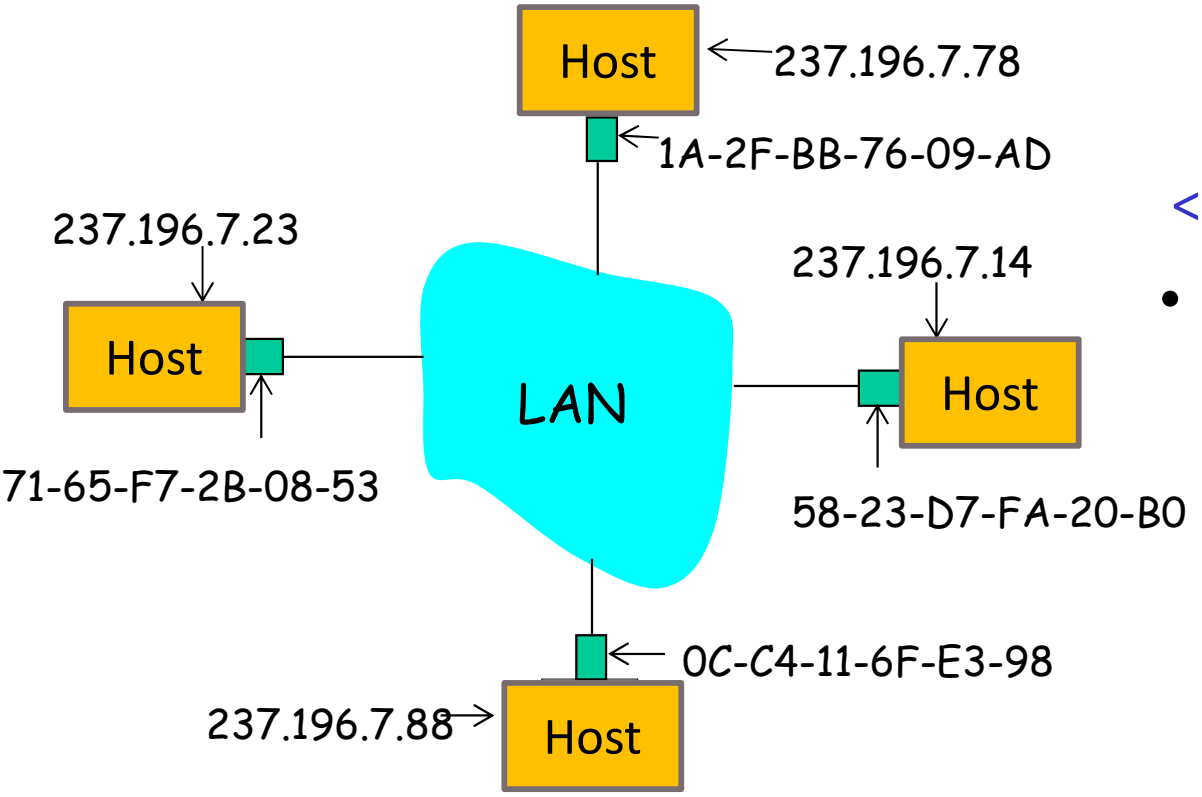
ARP: IP-> ind. MAC

ARP: Address Resolution Protocol



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>

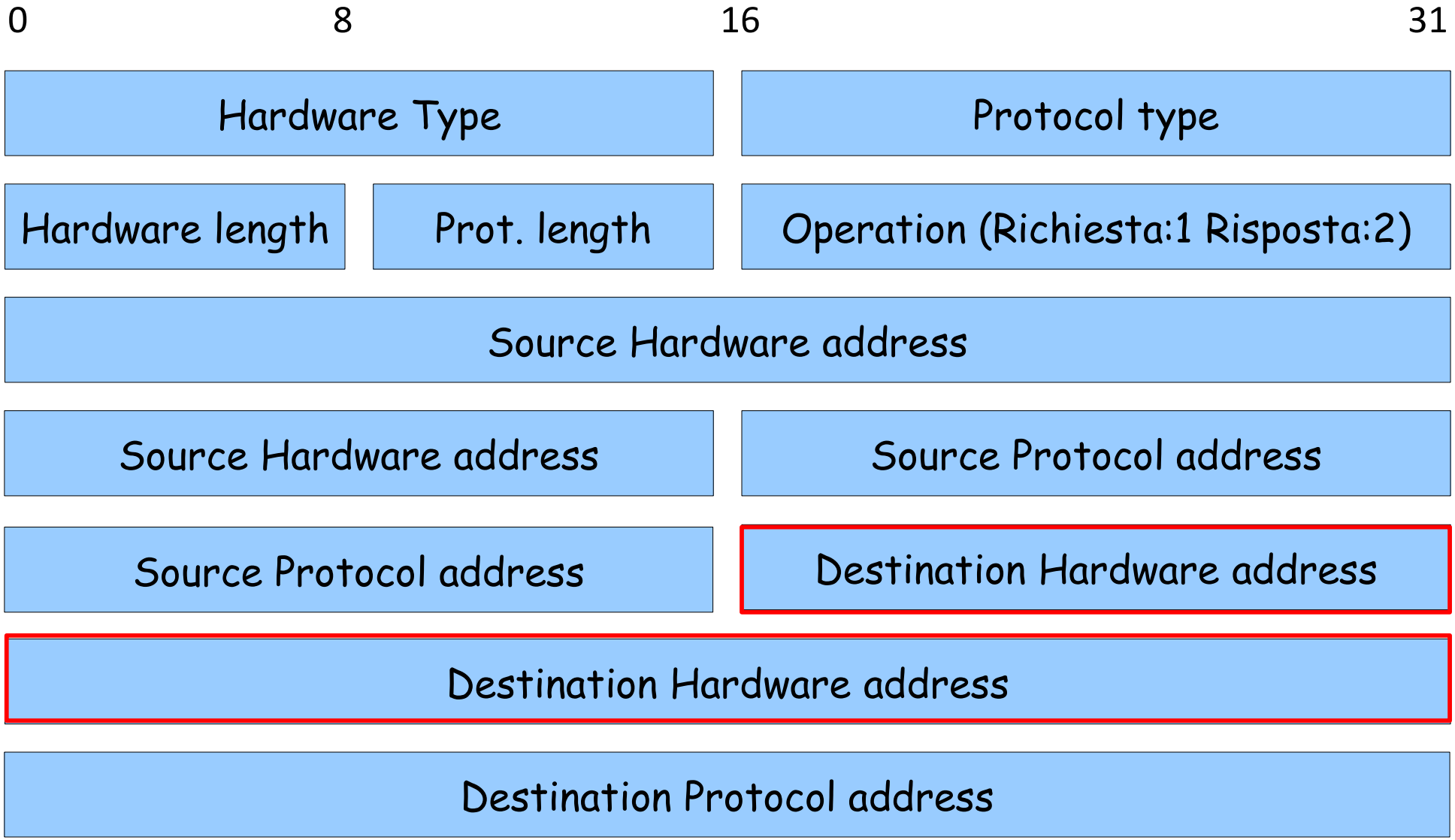
- TTL (tempo di vita): valore che indica quando bisognerà eliminare una data voce nella tabella (il tempo di vita tipico è di 20 min)

Tabella ARP

- Poiché ARP risolve gli indirizzi IP solo per i nodi della stessa LAN, le tabelle ARP contengono la corrispondenza fra indirizzi IP e indirizzi MAC per i nodi della stessa sottorete.
- La tabella non contiene necessariamente le corrispondenze per tutti i nodi della sottorete.

Indirizzo IP	Indirizzo LAN	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

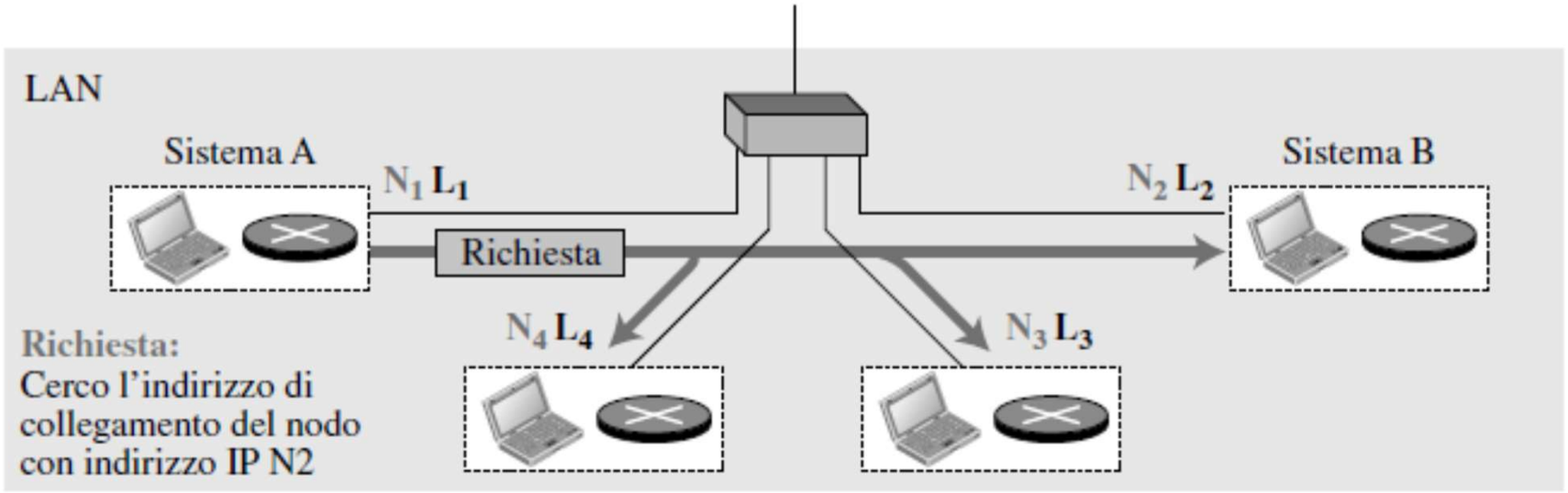
Pacchetto ARP



Pacchetto ARP

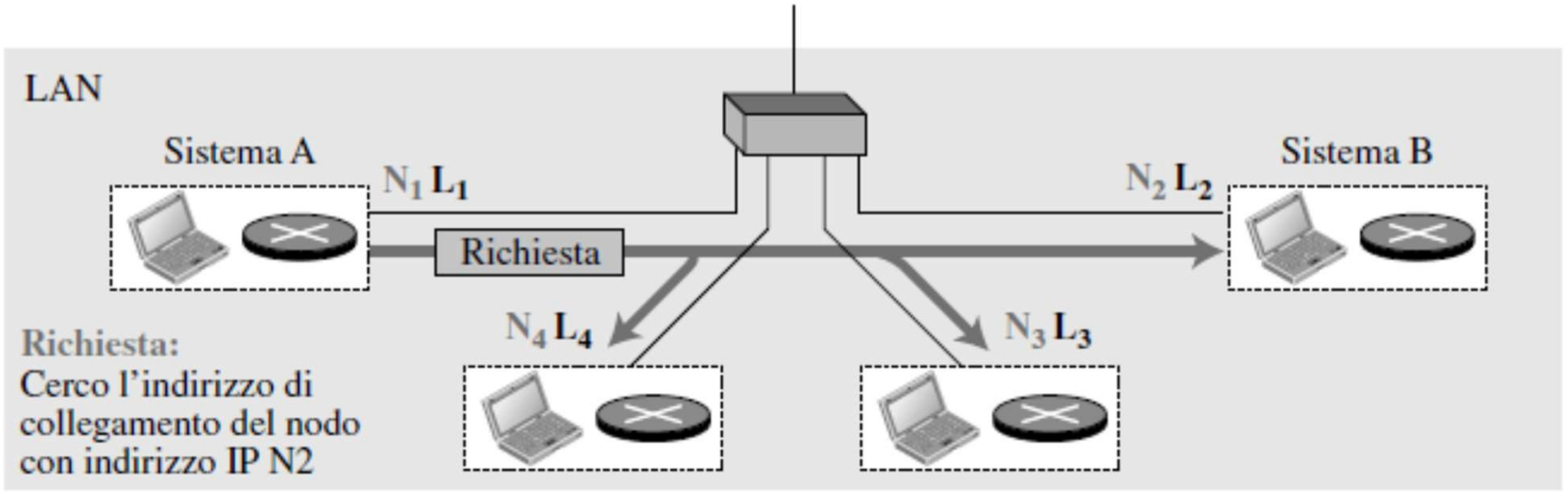
- *Hardware Type*: protocollo a livello di collegamento (es. Ethernet 1)
- *Protocol Type*: protocollo di livello superiore (es. IP)
- *Source hardware address* e *source protocol address*: indirizzi del nodo mittente a livello link e superiore. Lunghezza variabile. Campi Hard. Length e prot. Length
- *Destination hard. Address* (vuoto nelle richieste) e *destination protocol address*.

ARP: funzionamento

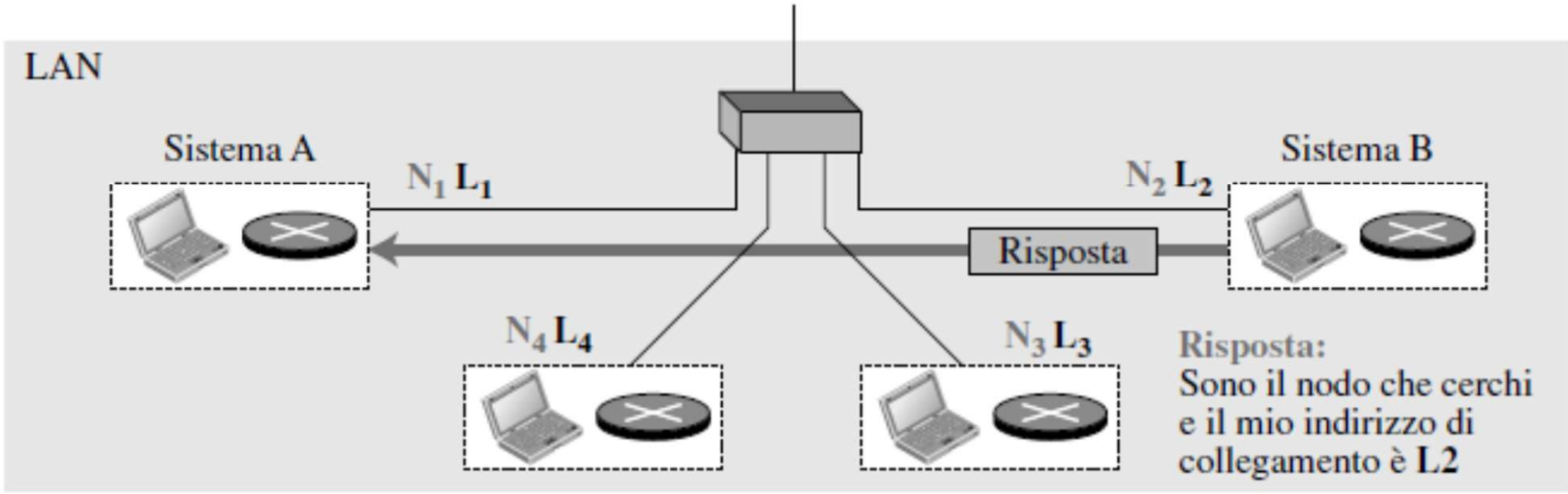


a. La richiesta ARP è inviata in broadcast

ARP: funzionamento



a. La richiesta ARP è inviata in broadcast



b. La risposta ARP è inviata in unicast

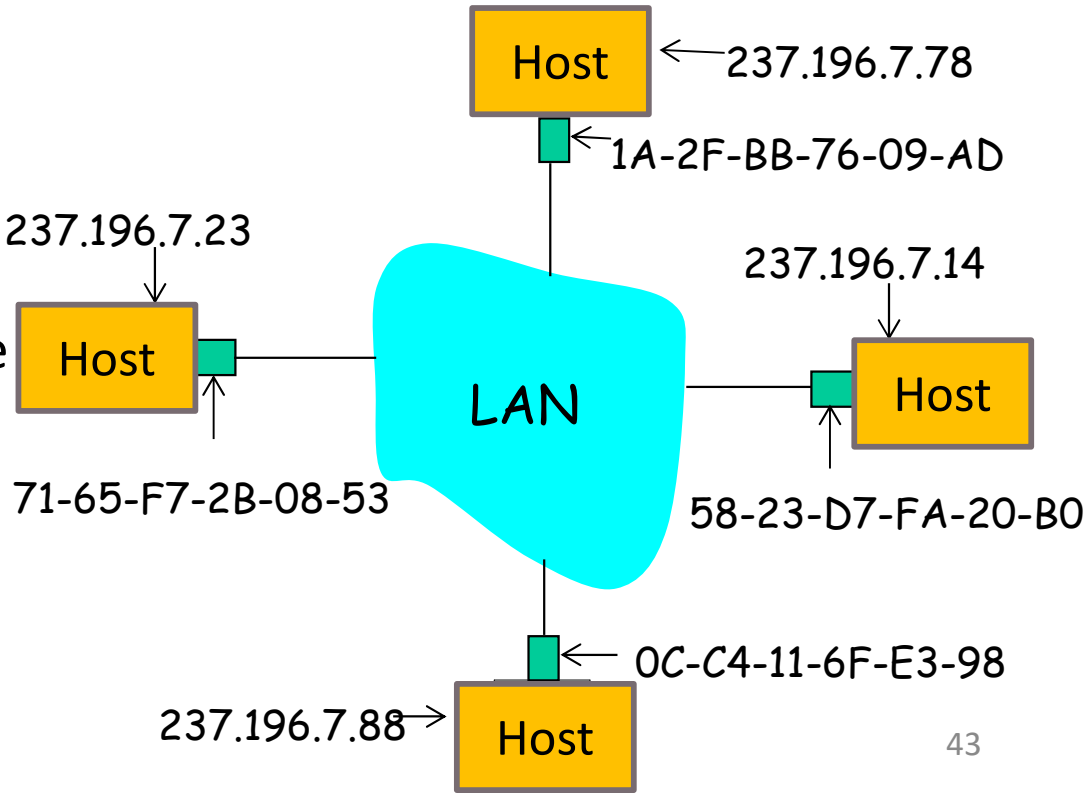
Pacchetto ARP

- Il protocollo ARP interagisce direttamente con il livello collegamento
- Il pacchetto ARP viene incapsulato in un frame e spedito in broadcast sulla rete
- L'header del frame di livello 2 specifica che il frame contiene un pacchetto ARP
- Ogni nodo nella rete locale riceve ed elabora il pacchetto di richiesta ARP.
- Il nodo che riconosce il proprio indirizzo IP restituisce un pacchetto di risposta ARP che contiene il proprio indirizzo IP e indirizzo MAC. Il pacchetto di risposta viene inviato in modalità unicast al nodo originario

Esempio per Forwarding diretto

- 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.

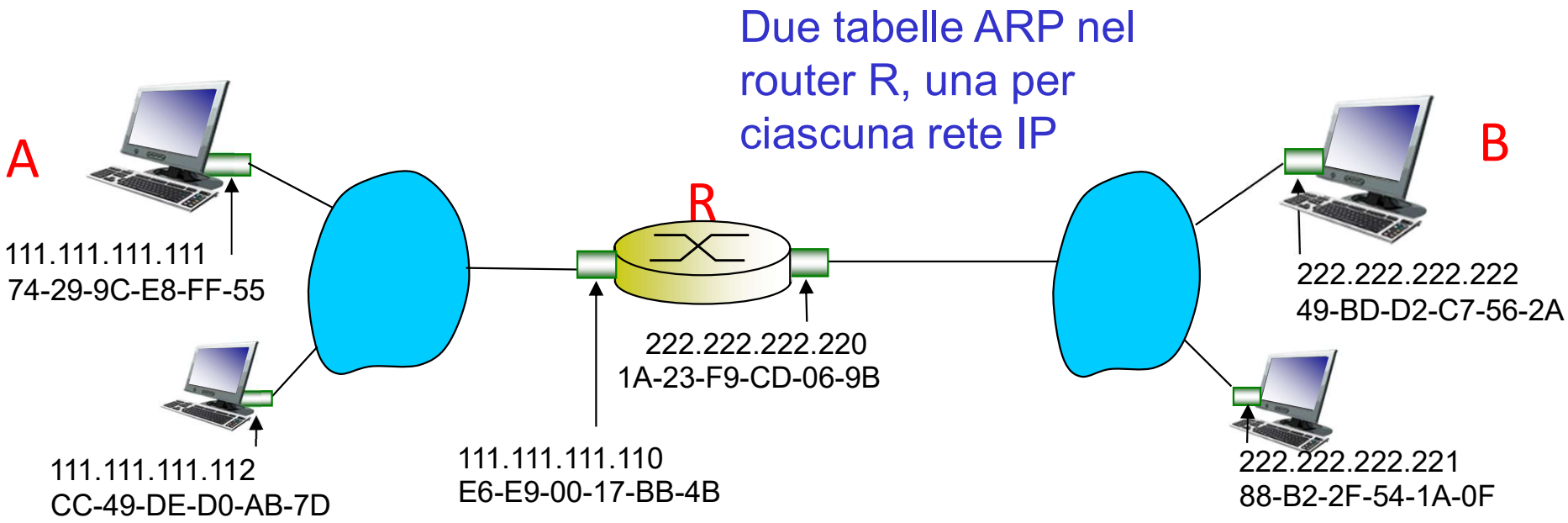
- ARP è "plug-and-play":
- La tabella ARP di un nodo si costituisce automaticamente e non deve essere configurata dall'amministratore del sistema.



Forwarding indiretto

caso: invio di un datagramma con mittente Ip di A e destinatario IP di B

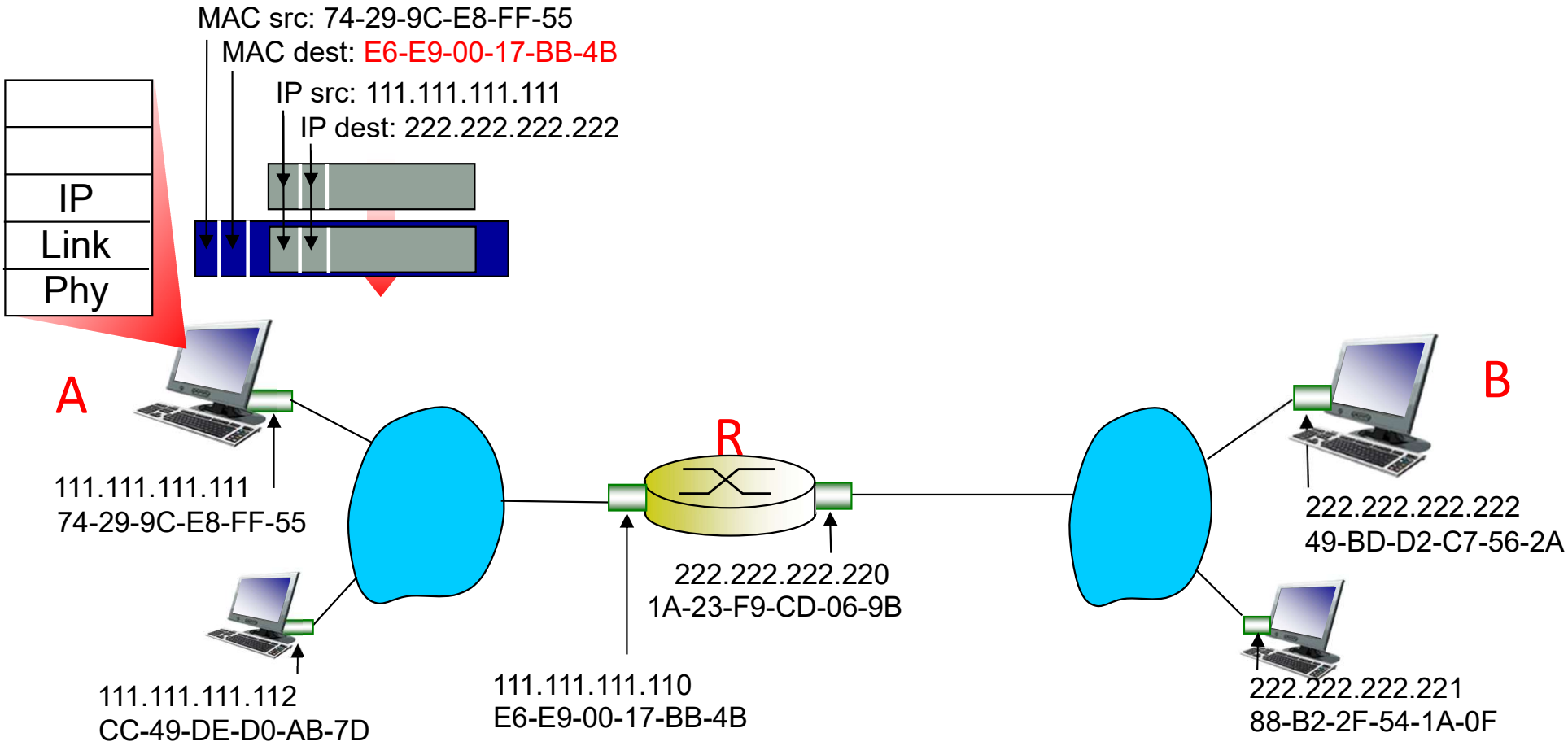
- Attenzione su indirizzamento IP (datagramma) e MAC (frame)
- Ipotesi
  - A conosce l'indirizzo IP di B
  - A conosce l'indirizzo IP del primo router (come fa?)
  - A conosce l'indirizzo MAC di R (come fa?)



LAN con tecnologia Ethernet

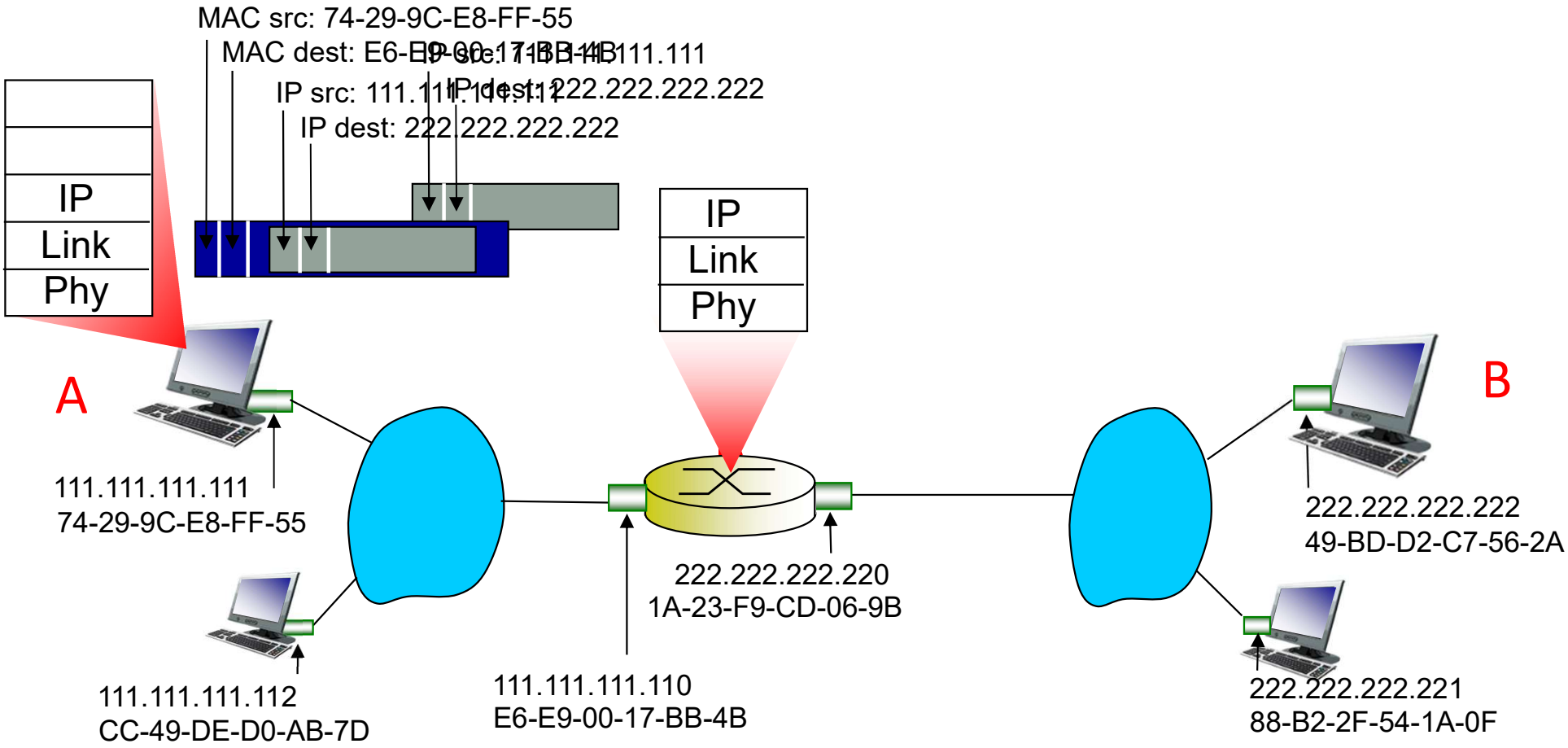
Forwarding indiretto

- A crea un datagramma IP con IP sorgente A, destinazione B
- A crea un frame con indirizzo MAC destinazione il MAC address di R, il frame incapsula il datagramma IP (A-to-B)



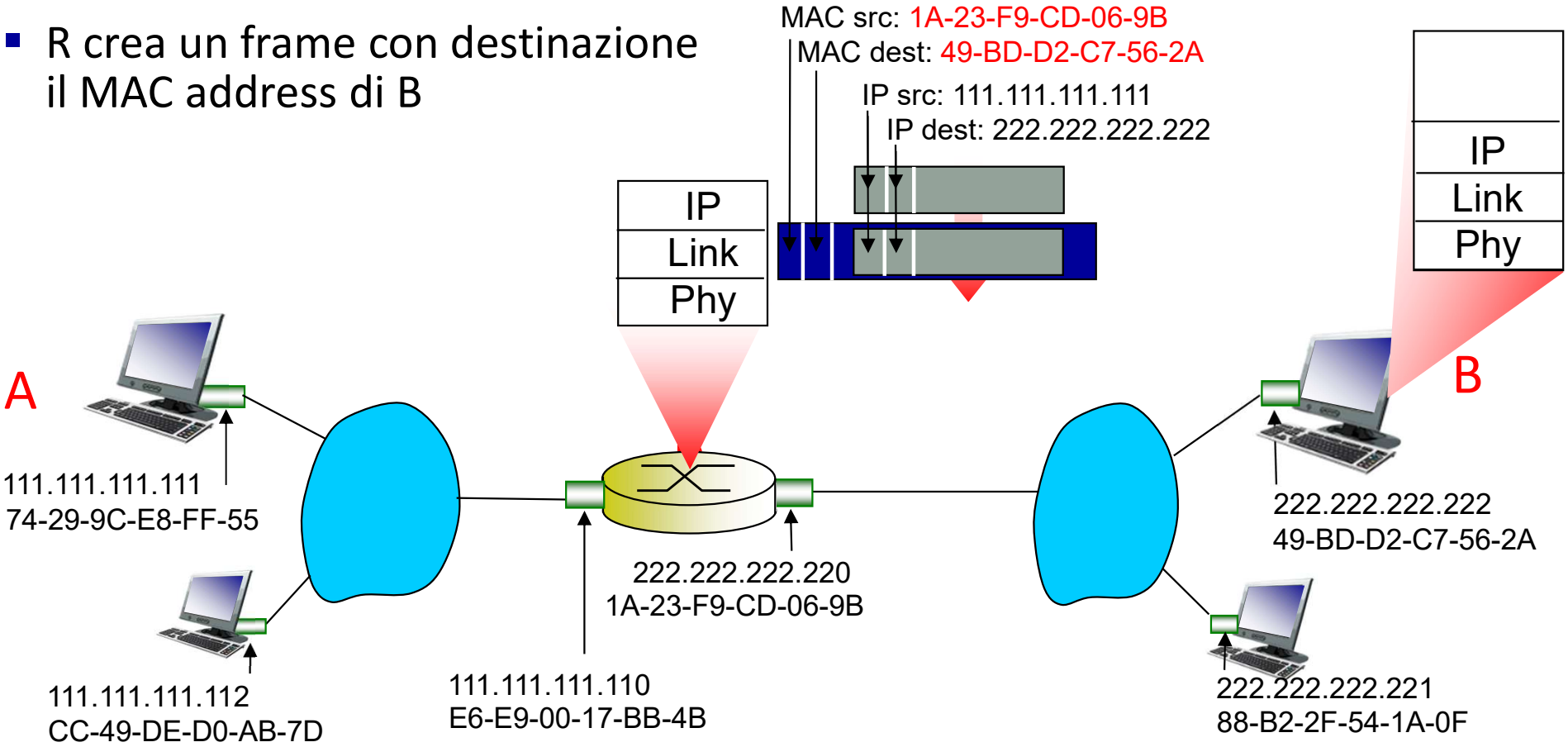
Forwarding indiretto

- frame inviato da A a R
- frame ricevuto da R, decapsulato, il datagramma passa al livello IP



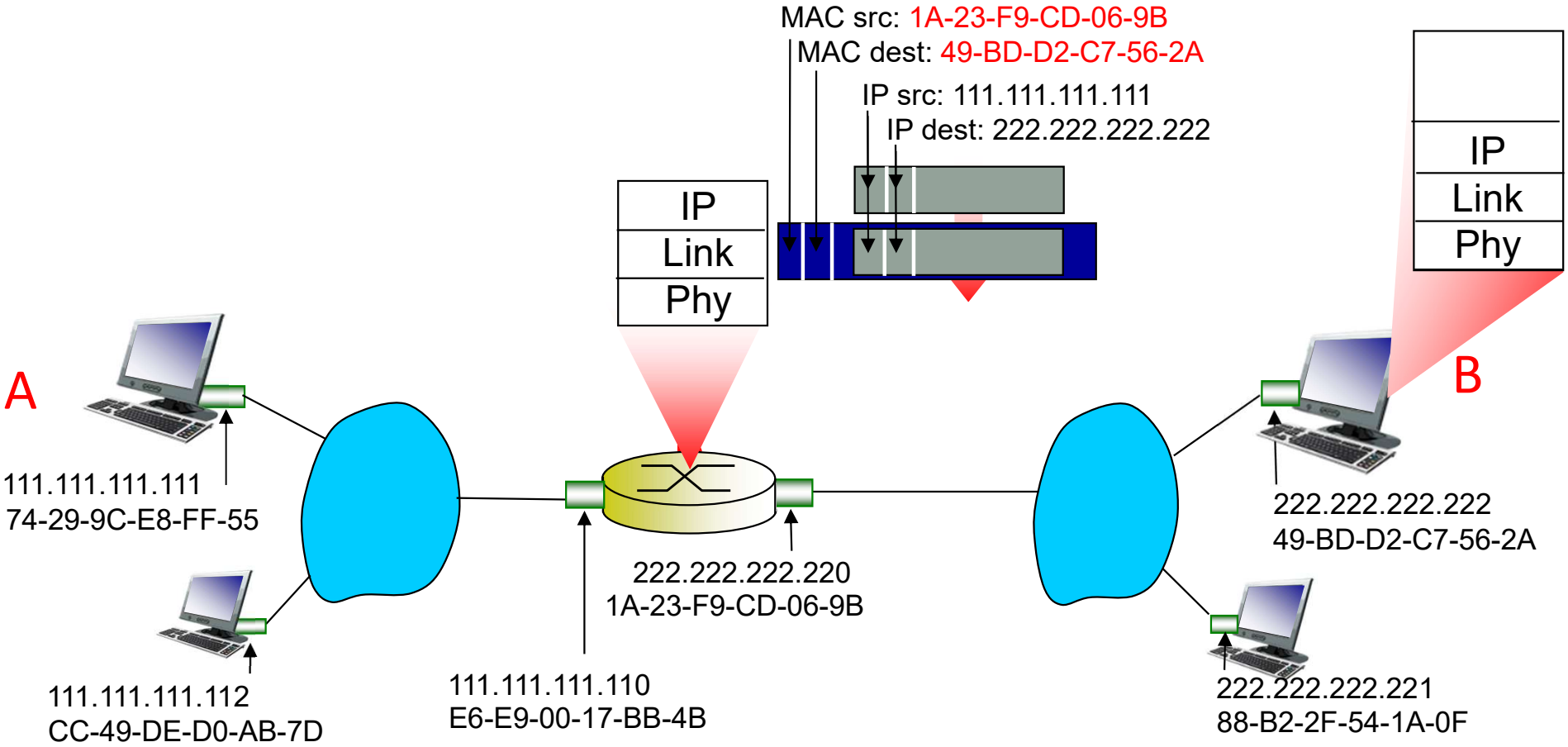
Forwarding indiretto

- R estrae il datagramma IP dal frame Ethernet, e vede che la sua destinazione è B.
- R inoltra il datagramma con IP sorgente A, destinazione B
- R usa ARP per ottenere l'indirizzo MAC di B
- R crea un frame con destinazione il MAC address di B

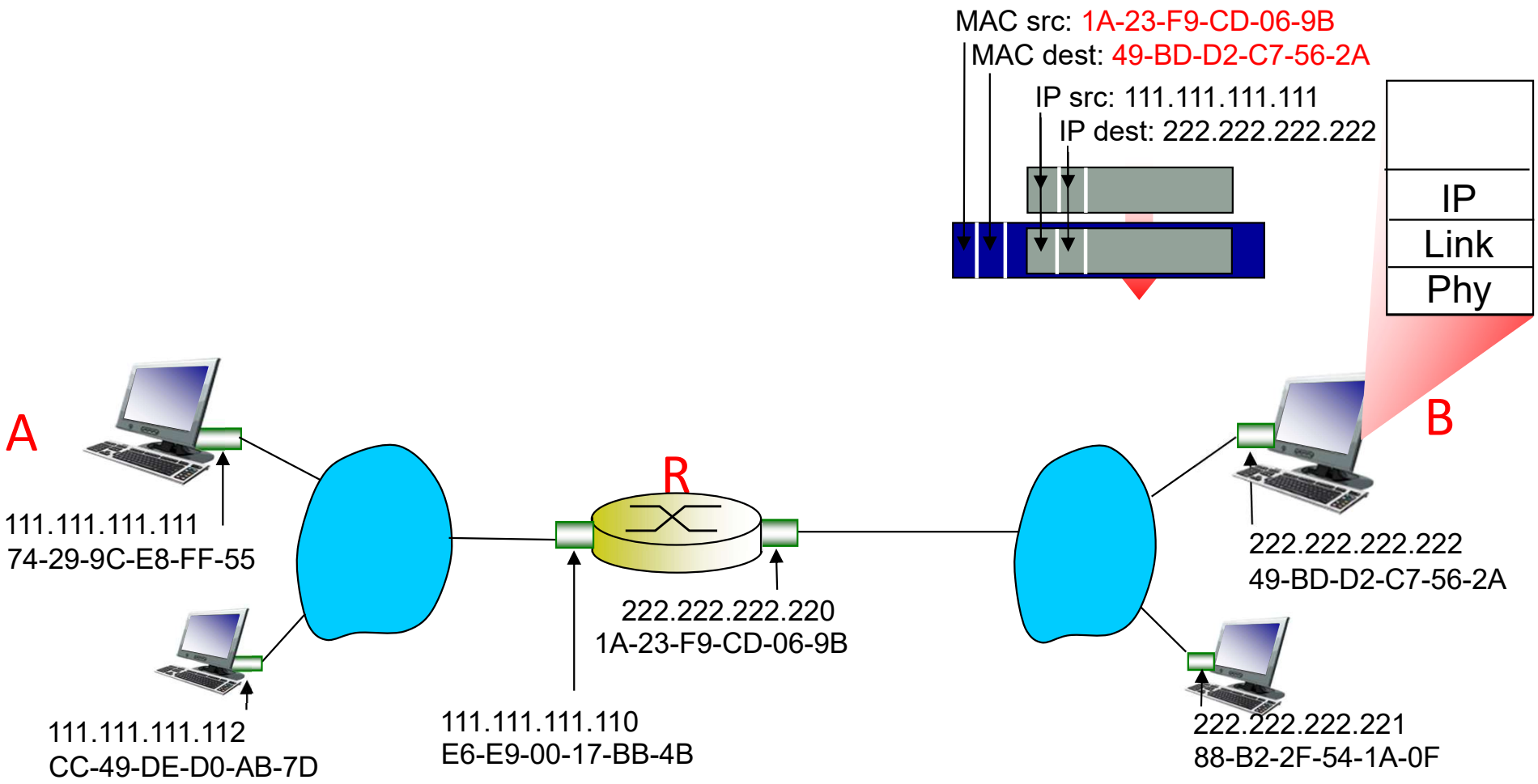


Forwarding indiretto

- R inoltra il datagramma con IP sorgente A, destinazione B
- R crea un frame con destinazione il MAC address di B



Forwarding indiretto

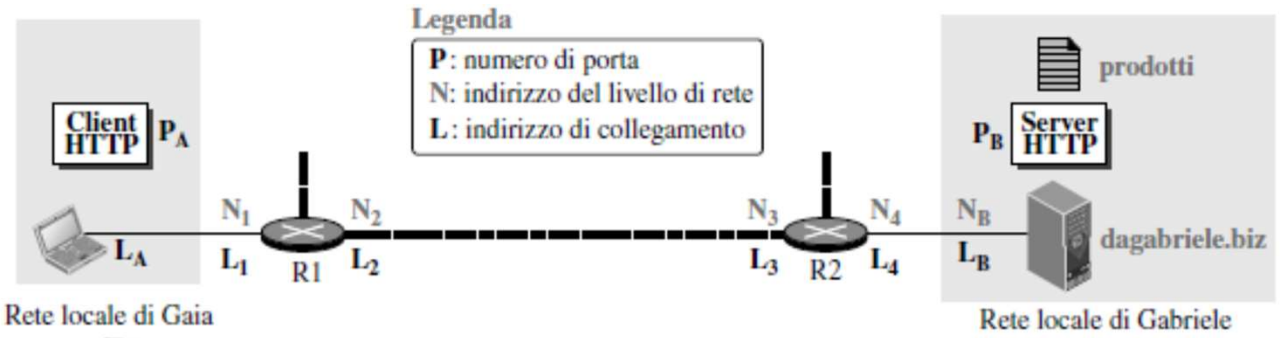


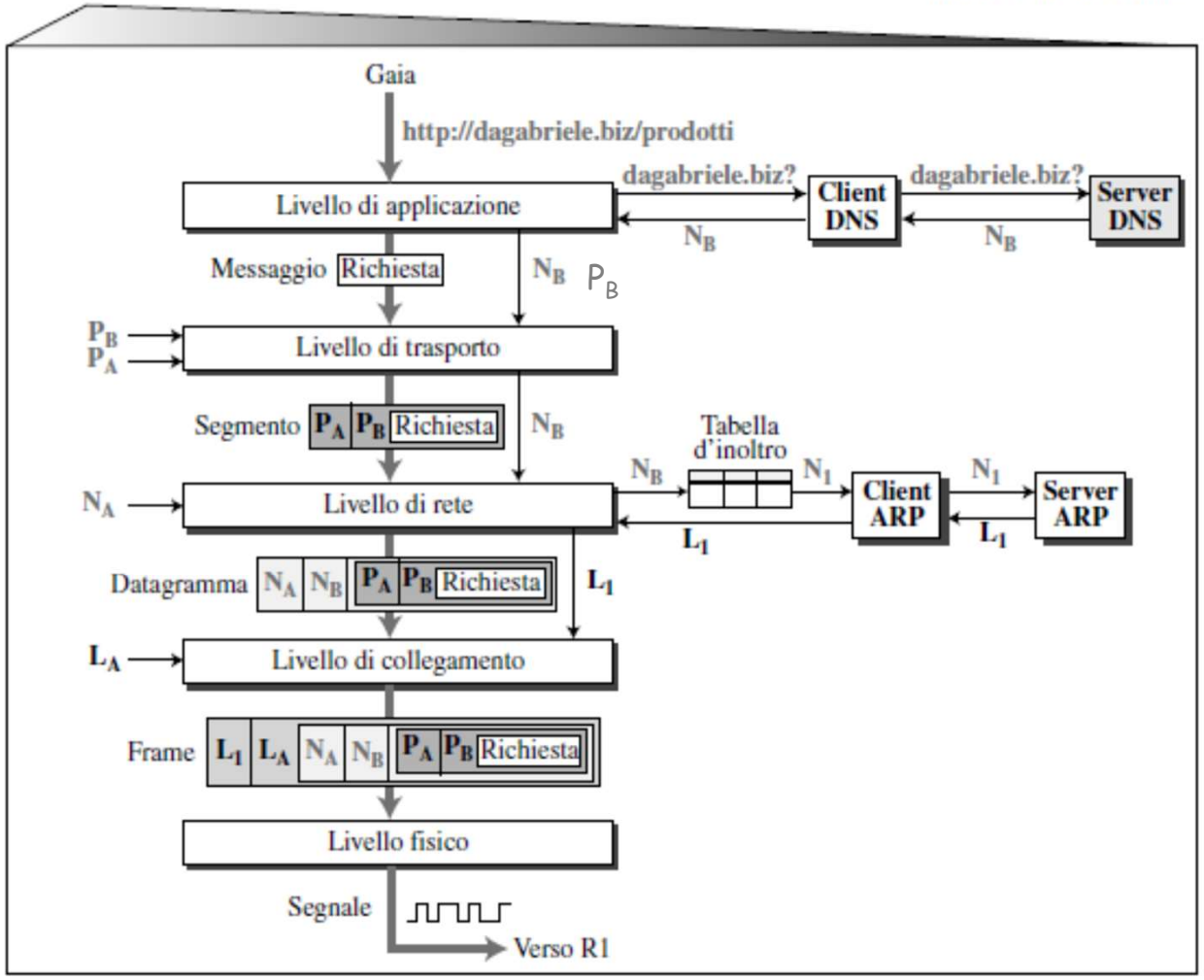
ARP Poisoning/Spoofing

- ARP è stato progettato in modo tale da essere il più possibile efficiente.
  - Vulnerabilità che possono essere sfruttate (e vengono di fatto utilizzate) per sferrare attacchi.
  - Risposte MAC con dati alterati
  - Scopo:
    - man in the middle attack: i pacchetti che hanno un certo host destinatario vengono redirezionati verso un host malevolo e da lì verso il destinatario;
    - Denial of service: i pacchetti non arrivano al destinatario

- Alterando l'indirizzo MAC associato ad un determinato IP di un dispositivo connesso alla rete, tutti i pacchetti dati vengono automaticamente inviati al sistema che ha lanciato l'attacco *ARP poisoning*. I dati possono essere a questo punto analizzati, eventualmente modificati e quindi inviati al reale destinatario.

Indirizzi: esempio (1/3)





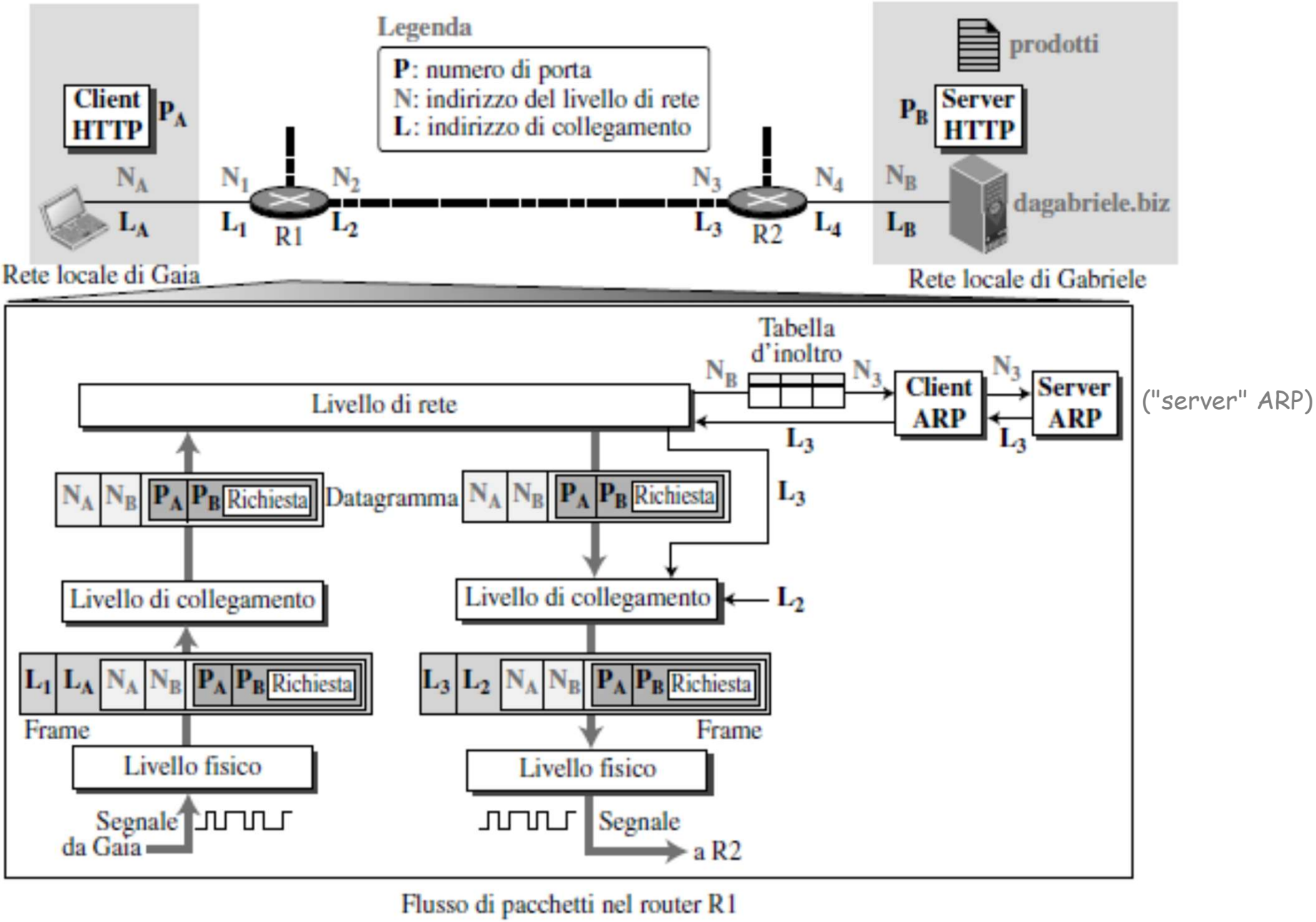
Flusso di pacchetti nel computer di Gaia

(DNS usa UDP ...)

(hp: connessione "già stabilita")

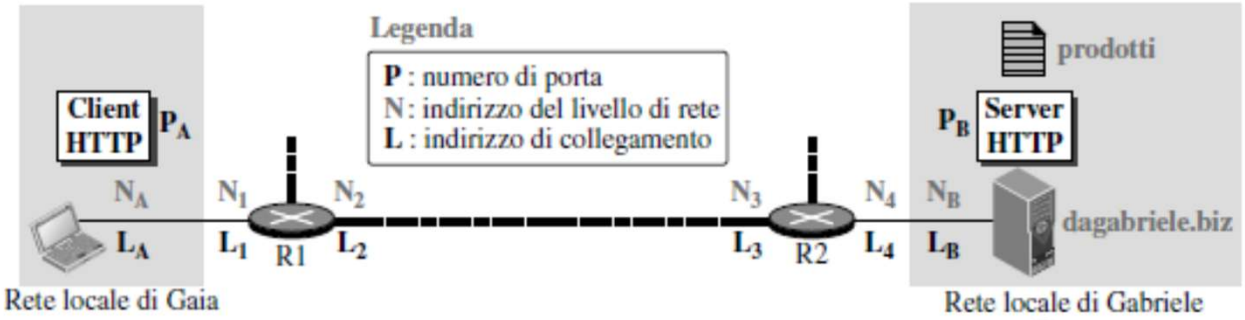
("server" ARP)

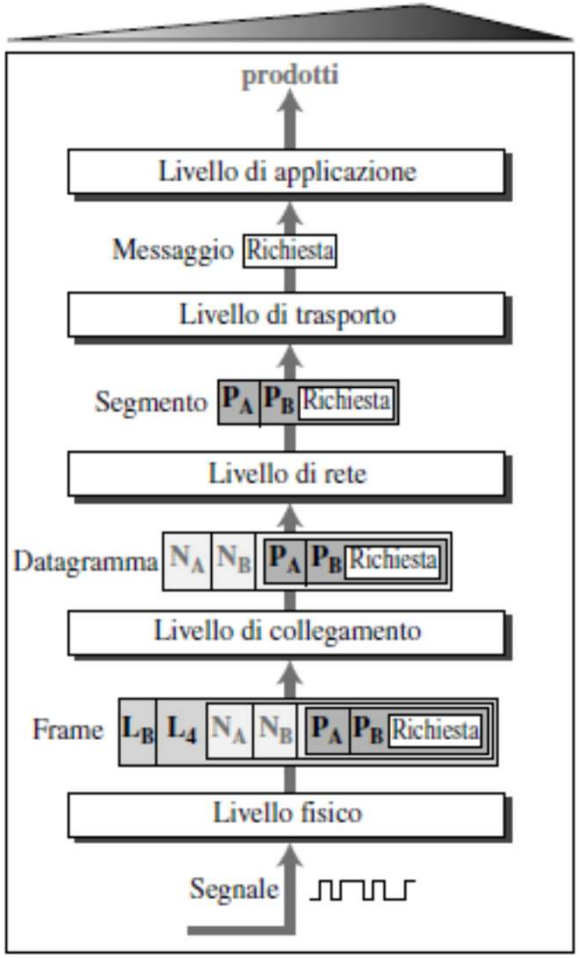
Indirizzi: esempio (2/3)



Flusso di pacchetti nel router R1

Indirizzi: esempio (3/3)





Flusso di pacchetti nel computer di Gabriele

(Liv. trasporto riceve anche N_A e N_B)