



# Reti di Calcolatori

Prof. Roberto Canonico

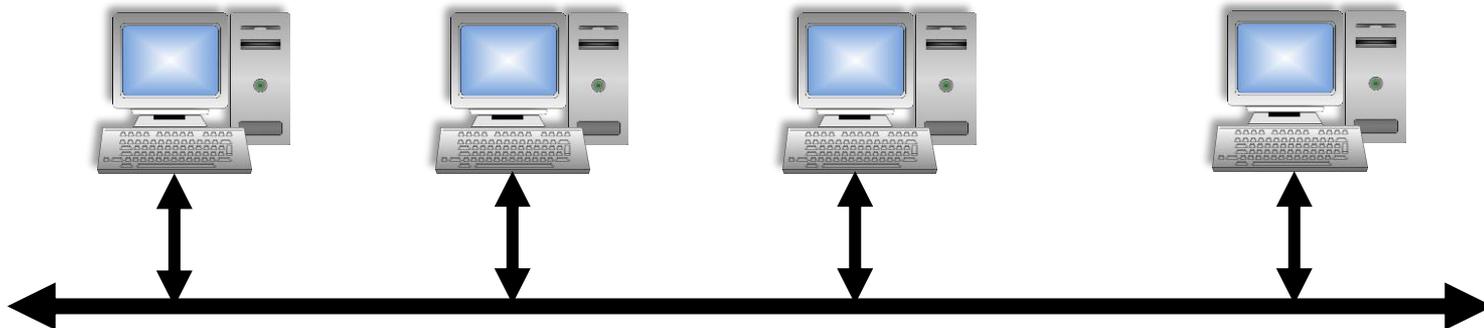
Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Corso di Laurea in Ingegneria Informatica

**Trasmissione di datagrammi IP in reti locali Ethernet**

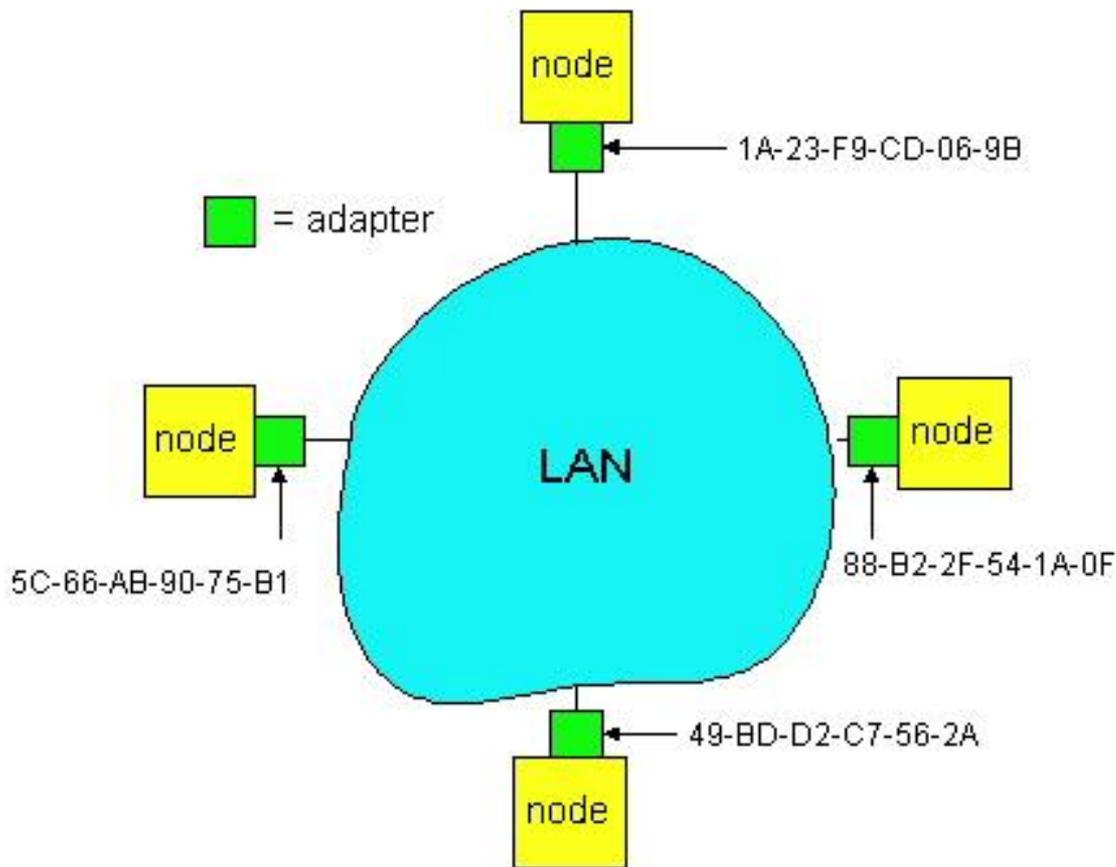
**Il protocollo ARP**

- Quasi tutte le tecnologie di rete locale realizzano, in modi diversi, l'equivalente logico di un bus
- La trasmissione di una stazione può arrivare direttamente ad una delle rimanenti  $N-1$  stazioni
- Ciascuna stazione è collegata alla rete mediante una scheda (NIC, *Network Interface Card*) identificata univocamente da un indirizzo MAC di 48 bit configurato dal costruttore nell'hardware della scheda



# Indirizzi MAC

Ogni scheda di rete in una LAN ha un indirizzo MAC (di 48 bit) univoco cablato nell'hardware della scheda dal costruttore



# Struttura della frame Ethernet

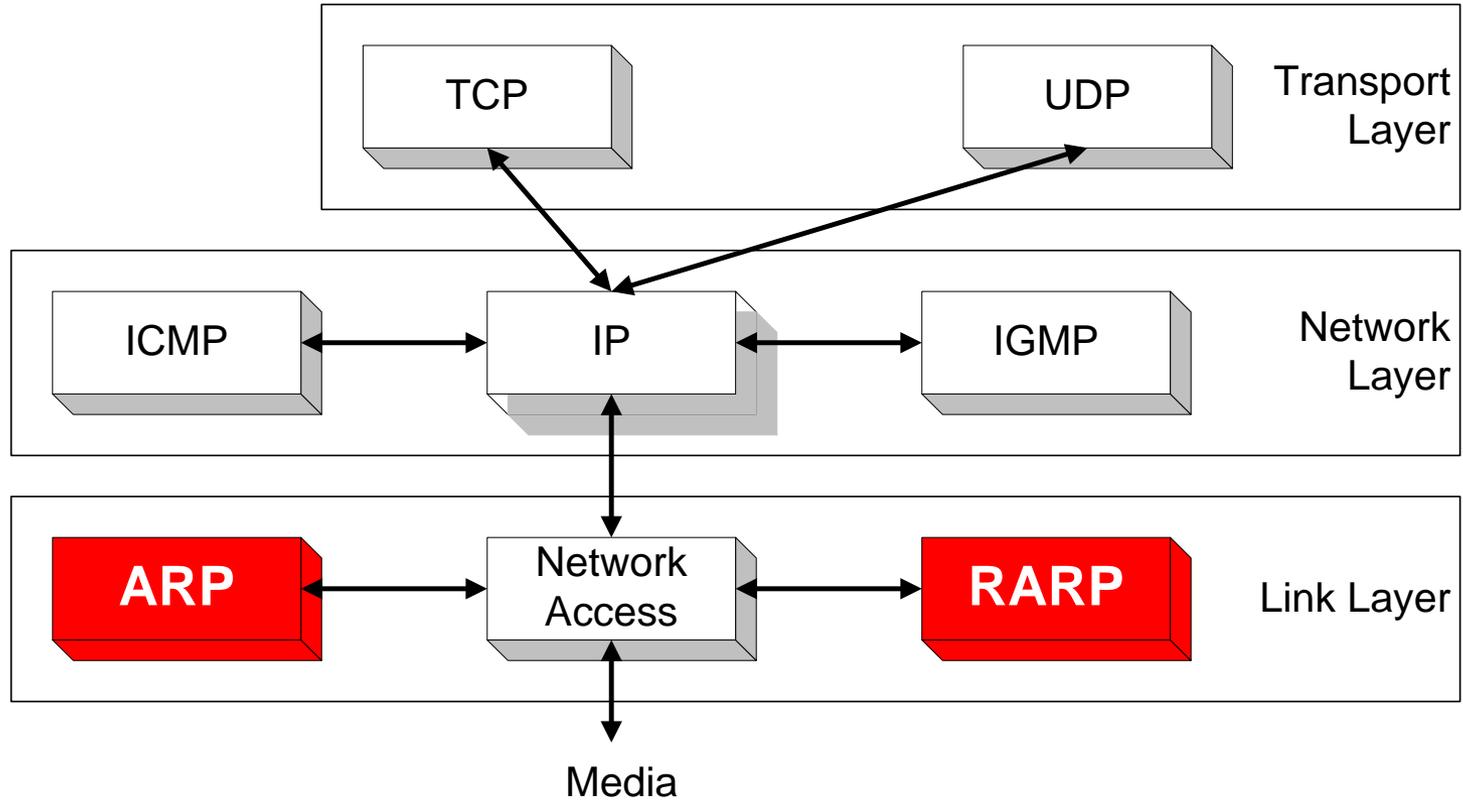


- Una PDU di livello 2 (frame) Ethernet presenta nell'header:
  - SA: indirizzo MAC di 48 bit che identifica la scheda che ha trasmesso la frame
  - DA: indirizzo MAC di 48 bit che identifica la destinazione della frame
    - La destinazione può essere:
      - **Unicast** – una specifica scheda collegata nella rete locale
      - **Broadcast** – tutte le schede collegate alla rete locale
      - **Multicast** – un sottoinsieme di schede collegate alla rete locale
- Gli indirizzi MAC sono rappresentati comunemente in notazione esadecimale

L'indirizzo MAC destinazione FF:FF:FF:FF:FF:FF indica una frame trasmessa in **broadcast**: tutti i sistemi collegata alla rete locale (inclusi i router) ricevono il pacchetto

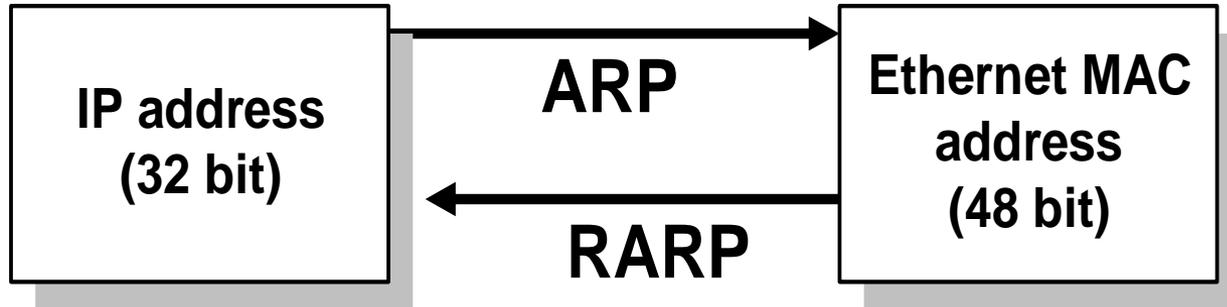
- Il campo **Type** (2 byte) indica il protocollo del pacchetto trasportato dalla frame nella parte **Data** (di lunghezza variabile)
  - Type = 0x0800           indica il protocollo IPv4
  - Type = 0x86DD           indica il protocollo IPv6
  - Type = 0x0806           indica il protocollo ARP (*Address Resolution Protocol*)
  - Cfr.: <https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml>

# TCP/IP: protocolli ausiliari del livello 2



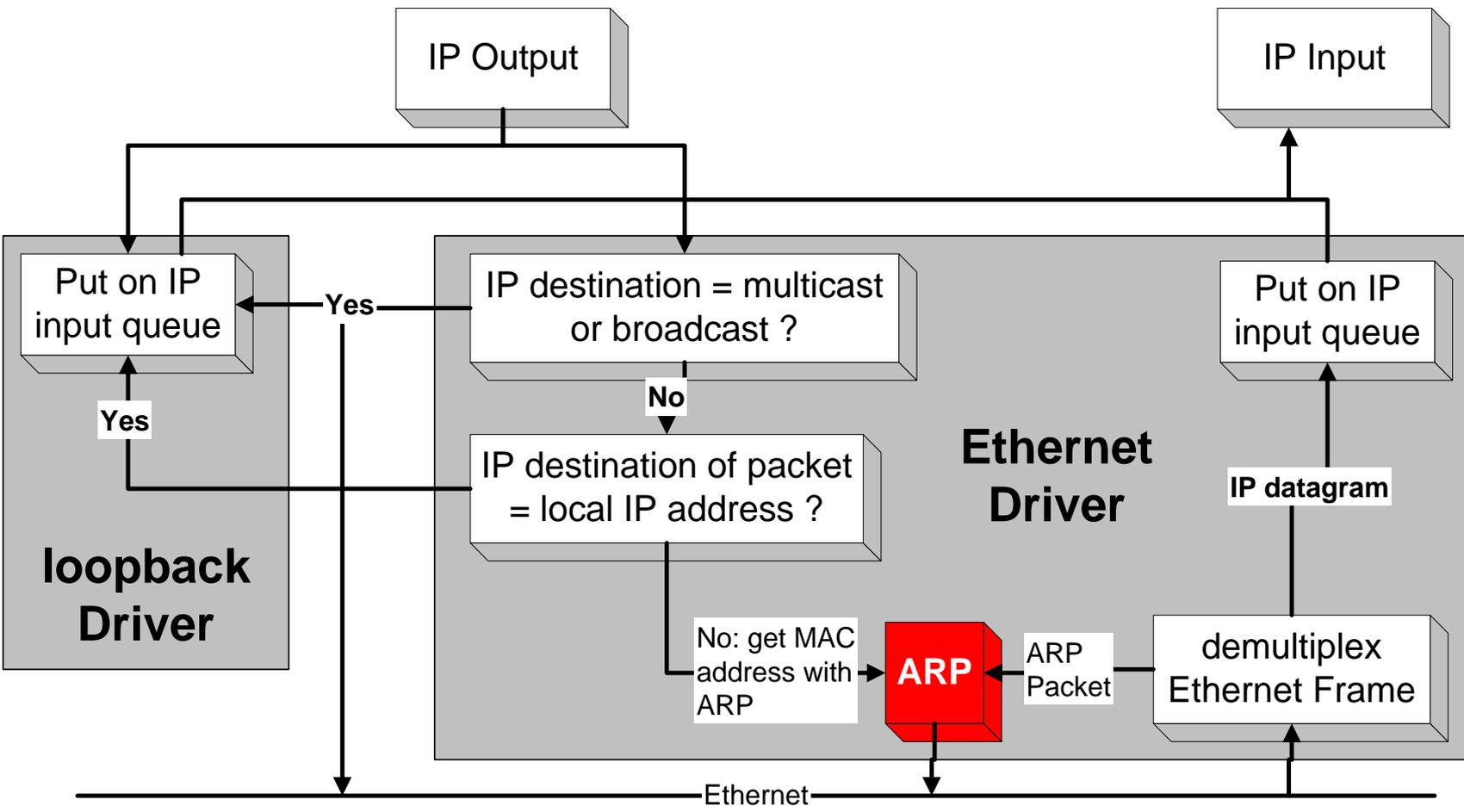
- I protocolli ARP e RARP svolgono funzioni ausiliarie a supporto della trasmissione di datagrammi IP (ed in generale di un protocollo di livello rete) in reti locali con capacità di trasmissione broadcast (come, ad esempio, le LAN Ethernet)

# ARP e RARP



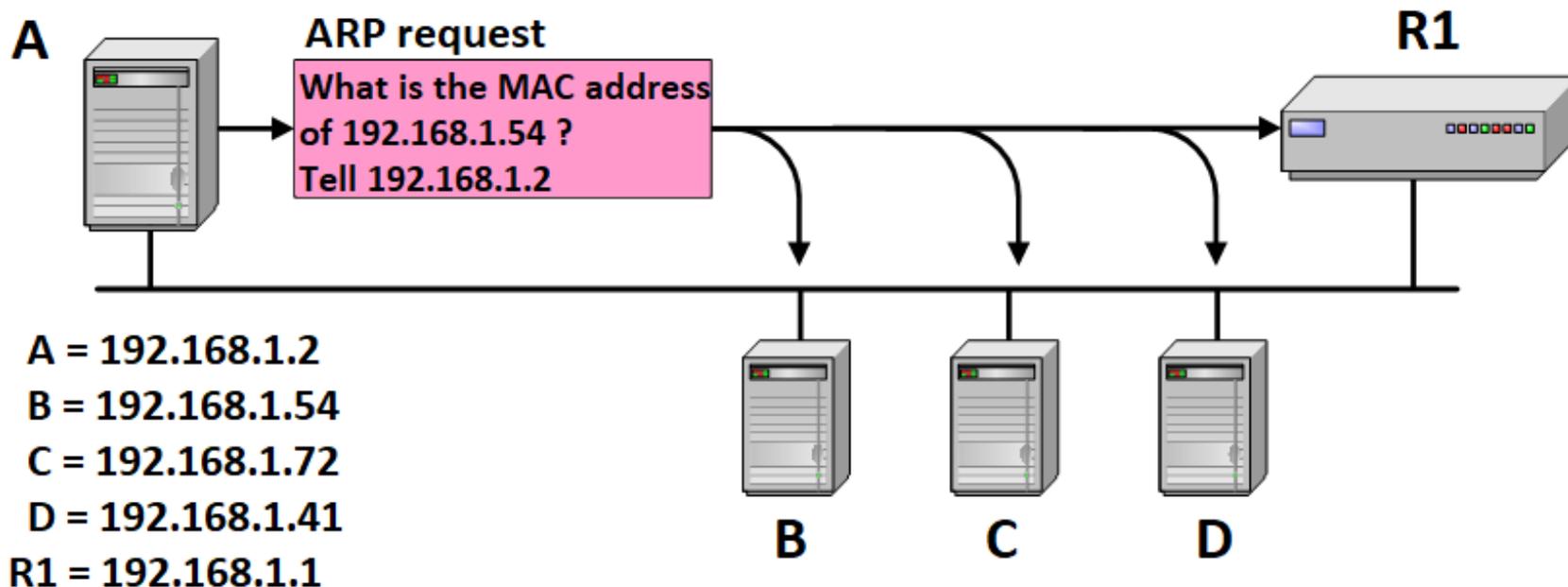
- Il protocollo ARP serve ad associare un indirizzo di rete (es. IP) al corrispondente indirizzo MAC
  - La sua funzione è necessaria quando un host vuole trasmettere un pacchetto IP ad una certa destinazione presente sulla rete locale e non ne conosce il corrispondente indirizzo MAC
  - La conoscenza dell'indirizzo MAC è necessaria a costituire la frame secondo la struttura vista nella slide precedente
  - ARP è definito in RFC 826
- Il protocollo RARP serve ad associare un indirizzo MAC al corrispondente indirizzo di rete (es. IP)
  - Questa esigenza si presenta in circostanze particolari

# Elaborazione di un pacchetto svolta dal driver



# Uso di ARP : richiesta (primo scenario)

**Primo scenario: A vuole trasmettere un pacchetto IP a B**

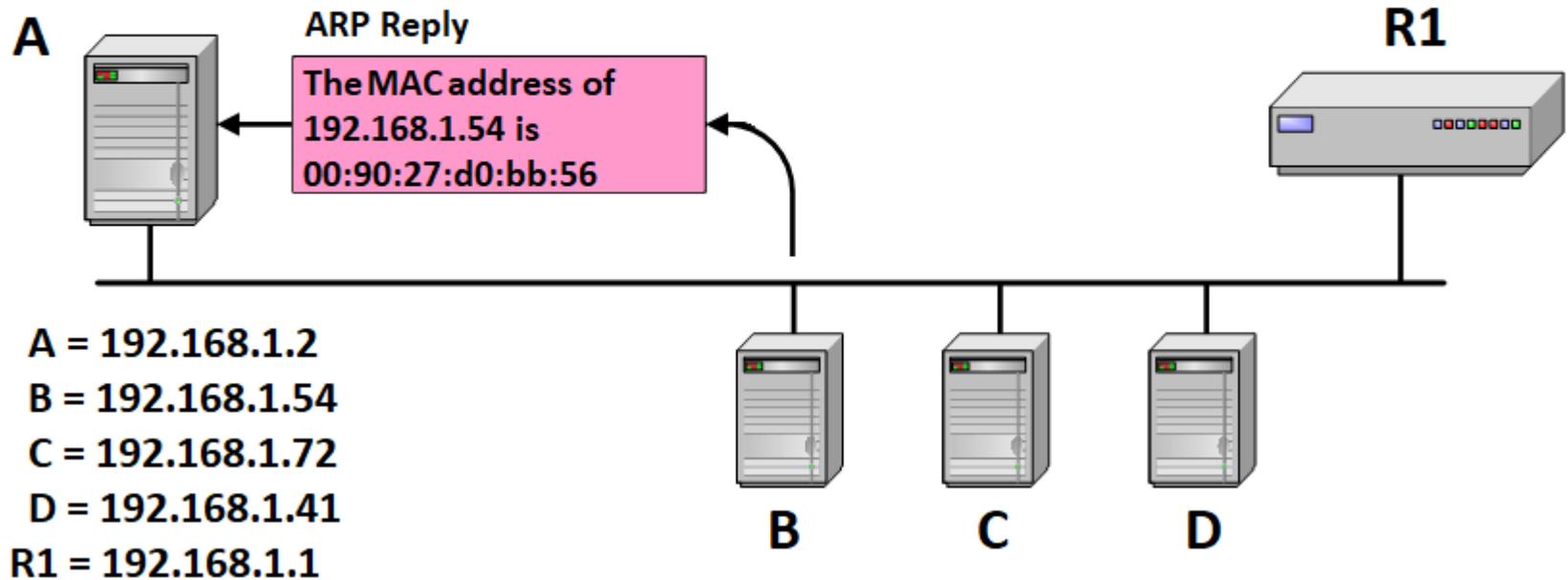


**Primo scenario:** la destinazione è nella stessa LAN (subnet IP) del mittente

- A chiede mediante ARP di conoscere il MAC address associato alla destinazione B (*target IP*) direttamente raggiungibile
- La richiesta ARP è trasmessa in una frame con indirizzo MAC destinazione broadcast FF:FF:FF:FF:FF:FF

# Uso di ARP : risposta (primo scenario)

**Primo scenario: A vuole trasmettere un pacchetto IP a B**

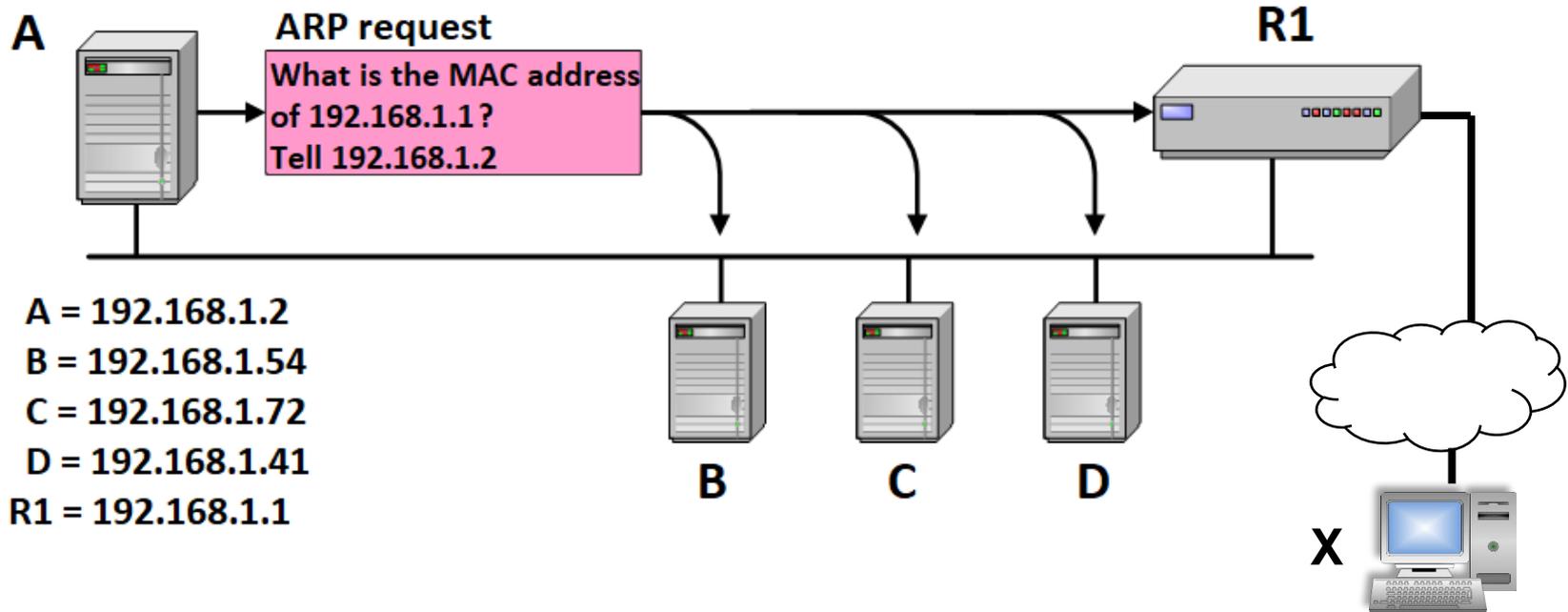


**Primo scenario:** la destinazione è nella stessa LAN (subnet IP) del mittente

- La risposta ARP è inviata da B direttamente ad A

# Uso di ARP : richiesta (secondo scenario)

**Secondo scenario: A vuole trasmettere un pacchetto IP a X**

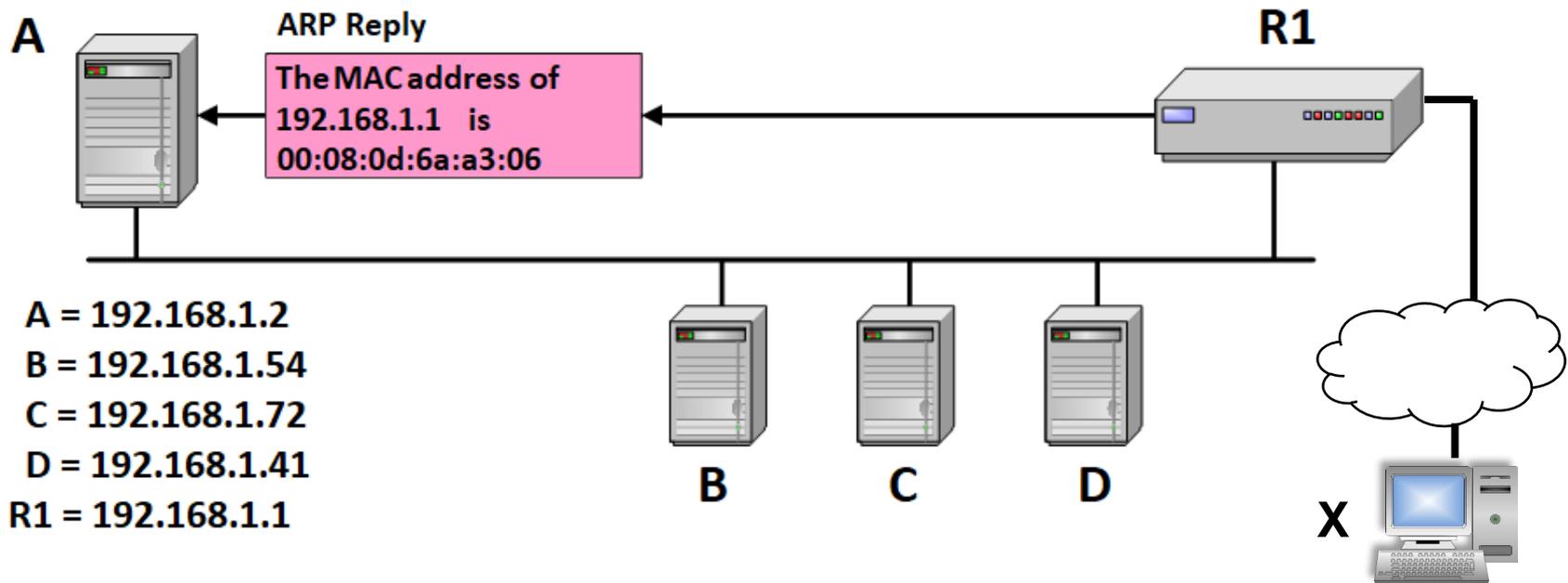


**Secondo scenario:** la destinazione è fuori dalla LAN (subnet IP) del mittente

- In base alla sua tabella di routing, A determina l'indirizzo R1 del gateway associato alla destinazione X
- A chiede mediante ARP di conoscere il MAC address associato al gateway R1 (*target IP*) direttamente raggiungibile
- La richiesta ARP è trasmessa in una frame con indirizzo MAC destinazione broadcast FF:FF:FF:FF:FF:FF

# Uso di ARP : risposta (secondo scenario)

**Secondo scenario: A vuole trasmettere un pacchetto IP a X**



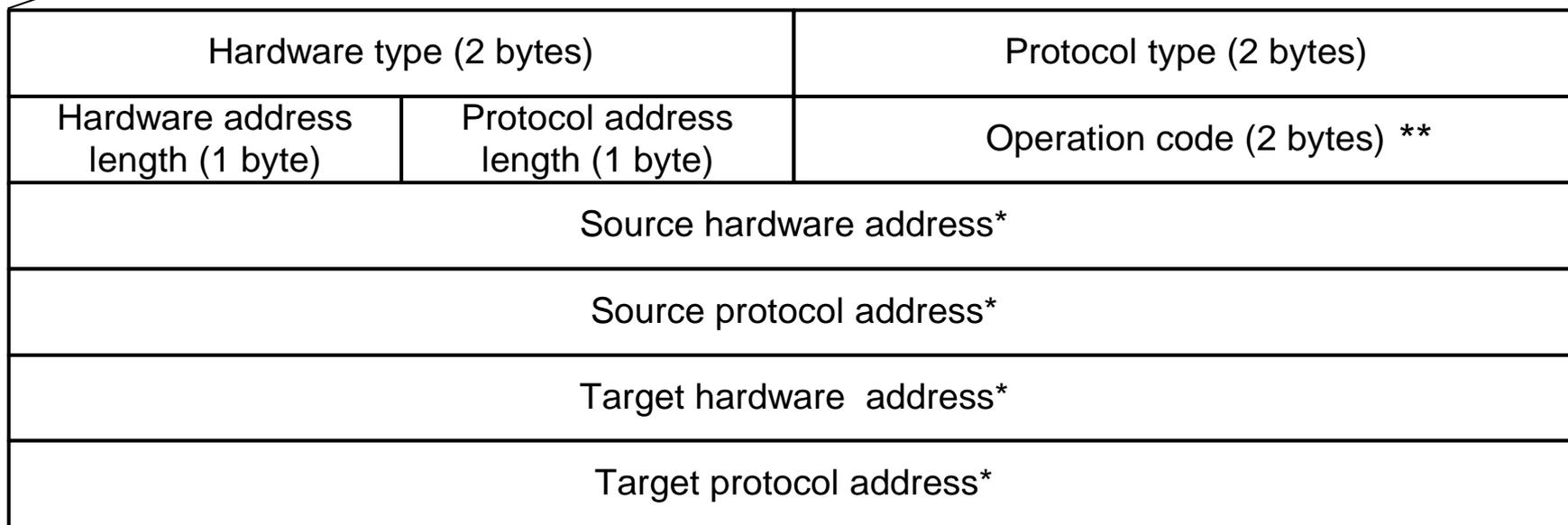
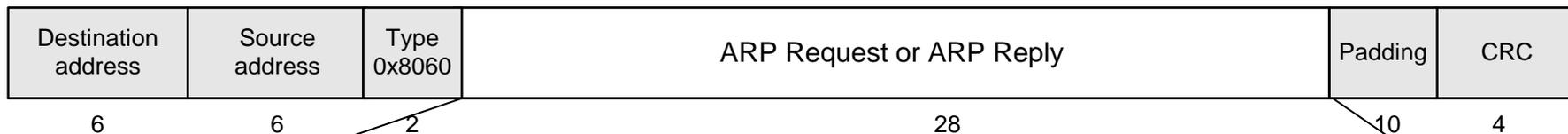
**Secondo scenario:** la destinazione è fuori dalla LAN (subnet IP) del mittente

- La risposta ARP è inviata dal gateway R1 direttamente ad A



# ARP Packet Format

← Ethernet II header →



\* Note: The length of the address fields is determined by the corresponding address length fields

\*\* *OpCode* = 0x0001 → *request*

*OpCode* = 0x0002 → *reply*



- La denominazione dei campi dei messaggi ARP usa i termini:
- **Protocol** per riferirsi a indirizzi di rete (layer-3)
  - tipicamente IPv4 a 32 bit (4 byte)
- **Hardware** per riferirsi ad indirizzi fisici (layer-2)
  - tipicamente MAC a 48 bit (6 byte)
- **Source** per riferirsi al mittente del messaggio ARP
- **Target** per riferirsi al destinatario del messaggio ARP
- Complessivamente, un messaggio ARP contiene 4 indirizzi:
  1. Source hardware
  2. Source protocol
  3. Target hardware
  4. Target protocol



- Il campo **Operation Code** discrimina tra due tipi di messaggi:
  - *ARP request* con *OpCode* = 0x0001
  - *ARP reply* con *OpCode* = 0x0002
- In un contesto nel quale ARP si usa per la risoluzione di indirizzi MAC rispetto ad indirizzi IP:
  1. **source hardware address** specifica il MAC address dell'host mittente
  2. **source protocol address** specifica l'indirizzo IP del mittente
  3. **target hardware address** contiene:
    - FF:FF:FF:FF:FF:FF in una richiesta ARP "normale"
    - 00:00:00:00:00:00 nei messaggi ARP Probe ed ARP Announcement
    - l'indirizzo MAC del destinatario in una risposta
  4. **target protocol address** contiene:
    - l'indirizzo IP di cui si desidera conoscere il MAC in una richiesta
    - l'indirizzo IP del destinatario in una risposta



## ARP caching

- Per ridurre il traffico sulla rete e ridurre il tempo necessario all'invio di nuovi pacchetti IP, ogni host mantiene in una cache le corrispondenze tra indirizzi logici e fisici precedentemente apprese
- Ciascuna corrispondenza viene mantenuta per un tempo limitato (alcuni minuti) e poi eliminata allo scadere di un timeout
- Per rinnovare le corrispondenze prossime alla scadenza, un host può inviare una richiesta ARP unicast al MAC address associato all'indirizzo IP
  - Questo comportamento è definito "Unicast Poll" nella sezione 2.3.2.1 ARP Cache Validation di [RFC 1122](#)
  - In questo modo si evita la trasmissione di una richiesta in broadcast

## Il comando `arp`

- In quasi tutti i sistemi operativi, il comando `arp` consente di consultare le corrispondenze MAC-IP già presenti nella cache ARP dell'host
- Il comando `arp -f` elimina tutte le corrispondenze presenti in cache (operazione di *flush*)
- Esempio di output del comando `arp` su un sistema Windows

```
Interfaccia: 192.168.1.123 --- 0x15
  Indirizzo Internet      Indirizzo fisico      Tipo
  192.168.1.1            20-b0-01-1d-70-b0    dinamico
  192.168.1.195          22-b0-01-1d-70-b9    dinamico
  192.168.1.218          82-69-d7-6f-43-dd    dinamico
  192.168.1.240          3c-52-82-08-ef-c2    dinamico
  255.255.255.255       ff-ff-ff-ff-ff-ff    statico
```

- Si osservi che l'indirizzo IP speciale `255.255.255.255` usato per inviare un pacchetto IP in broadcast nella propria rete è associato al MAC address broadcast `FF:FF:FF:FF:FF:FF`
  - Questa associazione è considerata *statica* in quanto non ottenuta tramite ARP

# Gratuitous ARP

- Un "*gratuitous ARP*" (o GARP) è un messaggio *ARP reply*:
  - Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF
- con:
  1. ***source hardware address*** dell'host mittente
  2. ***source protocol address*** dell'host mittente
  3. ***target hardware address*** FF:FF:FF:FF:FF:FF
  4. ***target protocol address*** dell'host mittente

```
▼ Address Resolution Protocol (reply/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  [Is gratuitous: True]
  Sender MAC address: 00:53:ff:ff:bb:bb
  Sender IP address: 10.0.0.22
  Target MAC address: ff:ff:ff:ff:ff:ff
  Target IP address: 10.0.0.22
```

## Gratuitous ARP: perché?

- Un GARP è un messaggio di risposta ARP *unsolicited* cioè **non** generato per effetto di una precedente richiesta
- Messaggi GARP possono essere generati se:
  - L'host desidera popolare le ARP cache degli altri host della rete locale
    - Questo effetto potrebbe non essere raggiunto in quanto un host non è obbligato ad inserire le corrispondenze apprese mediante GARP
  - L'host ha modificato il proprio indirizzo IP oppure ha subito una disconnessione dalla rete e desidera aggiornare del cambiamento gli altri host (e switch) della rete locale

# ARP Probe

- Un "*ARP Probe*" è un messaggio *ARP request*:
  - Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF
- con:
  1. **source hardware address** dell'host mittente
  2. **source protocol address** 0.0.0.0
  3. **target hardware address** 00:00:00:00:00:00
  4. **target protocol address** indirizzo oggetto del "probe"

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:50:56:c0:00:01
  Sender IP address: 0.0.0.0
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.174.111
```



## ARP Probe: perché?

- Un ARP Probe può essere usato per verificare che nella rete locale non ci siano altri host con lo stesso indirizzo IP target
  - L'eventuale ricezione di una risposta al probe è sintomo che un altro host nella rete locale è già configurato con l'indirizzo IP target
  - Usando un ARP Probe, anziché un Gratuitous ARP, si evita di inserire una entry duplicata nelle cache degli altri host della rete locale, cioè si evita il verificarsi del problema della duplicazione di un indirizzo IP

# ARP Announcement

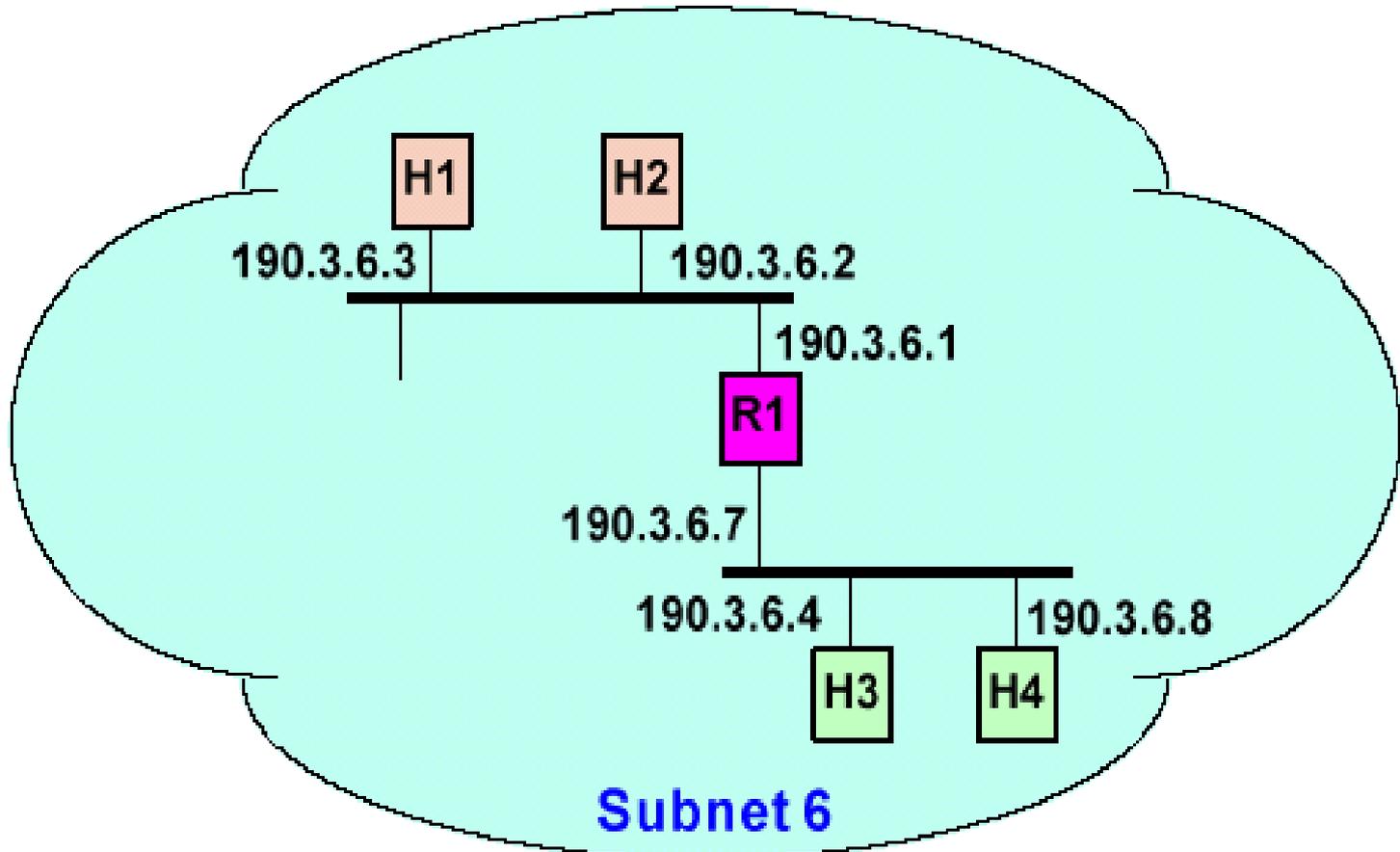
- Un "*ARP Announcement*" è un messaggio *ARP request*.
  - Trasmesso in una frame con MAC destinazione FF:FF:FF:FF:FF:FF
- con:
  1. **source hardware address** dell'host mittente
  2. **source protocol address** dell'host mittente
  3. **target hardware address** 00:00:00:00:00:00 oppure FF:FF:FF:FF:FF:FF
  4. **target protocol address** dell'host mittente

```
▼ Address Resolution Protocol (request/gratuitous ARP)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is gratuitous: True]
  Sender MAC address: 00:50:56:c0:00:01
  Sender IP address: 192.168.174.111
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.174.111
```

## ARP Announcement: perché?

- Un *ARP Announcement* è simile ad un *gratuitous ARP* perché:  
***source protocol address == target protocol address***  
con la differenza di essere un messaggio di richiesta
- A differenza di un ARP Probe, un ARP Announcement trasmette una associazione completamente definita tra un indirizzo MAC sorgente ed un indirizzo IP sorgente
  - Gli host della rete locale che ricevono l'announcement possono aggiornare le proprie ARP cache
- I messaggi ARP announcement vengono usati con le stesse finalità dei messaggi gratuitous ARP
- Anche un ARP Announcement può essere usato per verificare che nella rete locale non ci siano altri host con lo stesso indirizzo IP target
  - L'eventuale ricezione di una risposta è sintomo che un altro host nella rete locale è già configurato con l'indirizzo IP target

- Permette di usare la stessa subnet su due o più reti fisiche diverse





- Il protocollo RARP svolge il ruolo opposto ad ARP
  - Indirizzo fisico (MAC) → indirizzo logico (IP)
- Usato per sistemi diskless:
  - X terminal, diskless workstation
  - Al boot non conoscono il loro indirizzo IP
- Presuppone l'esistenza nella rete locale di un server RARP che risponde alla richiesta
- Questo protocollo è oggi superato da DHCP che, oltre ad assegnare un indirizzo IP, consente di fornire all'host ulteriori parametri di configurazione (netmask, default gateway, server DNS locale, ecc.)