ARP

Teoría de las Comunicaciones

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

12.09.2017

Ethernet - MAC Address

- *Media Access Control Address*.

Ethernet - MAC Address

- *Media Access Control Address*.
- Identificador de una interfaz de red.

Ethernet - MAC Address

- *Media Access Control Address*.
- Identificador de una interfaz de red.
- 6 octetos

Ethernet - MAC Address

- *Media Access Control Address*.
- Identificador de una interfaz de red.
- 6 octetos
- 3 de OUI (Organization Unique Identifier) `standards.ieee.org/develop/regauth/oui/public.html`

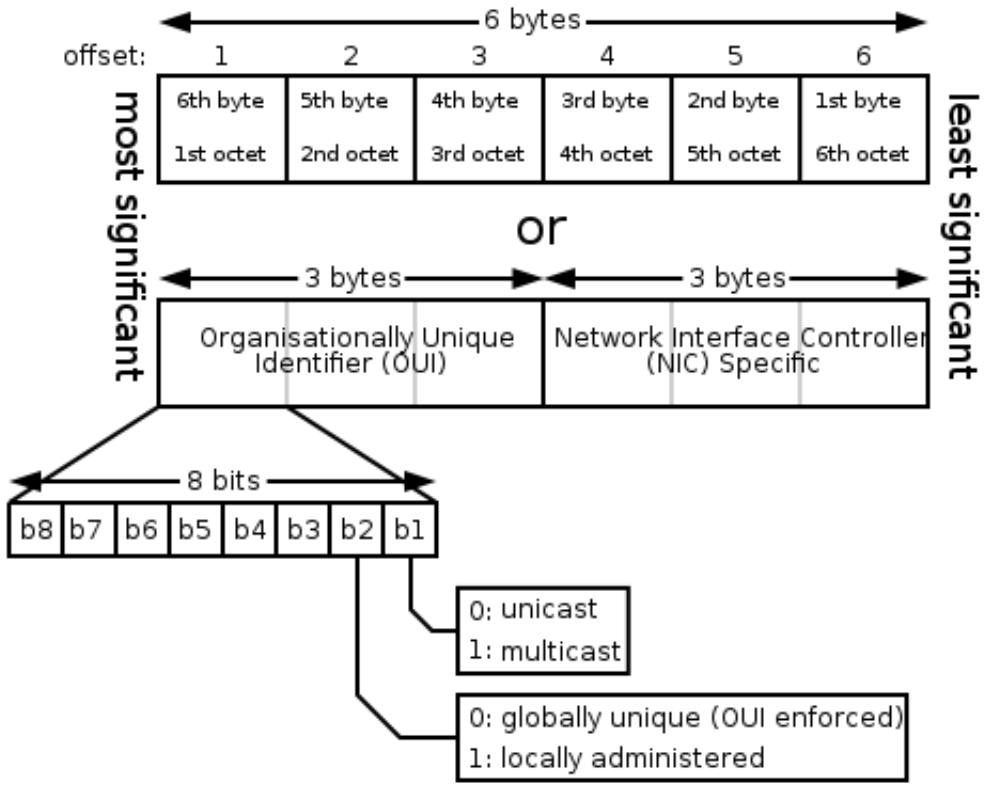
Ethernet - MAC Address

- *Media Access Control Address*.
- Identificador de una interfaz de red.
- 6 octetos
- 3 de OUI (Organization Unique Identifier) `standards.ieee.org/develop/regauth/oui/public.html`
- 3 de NIC (Network Interface Controller)

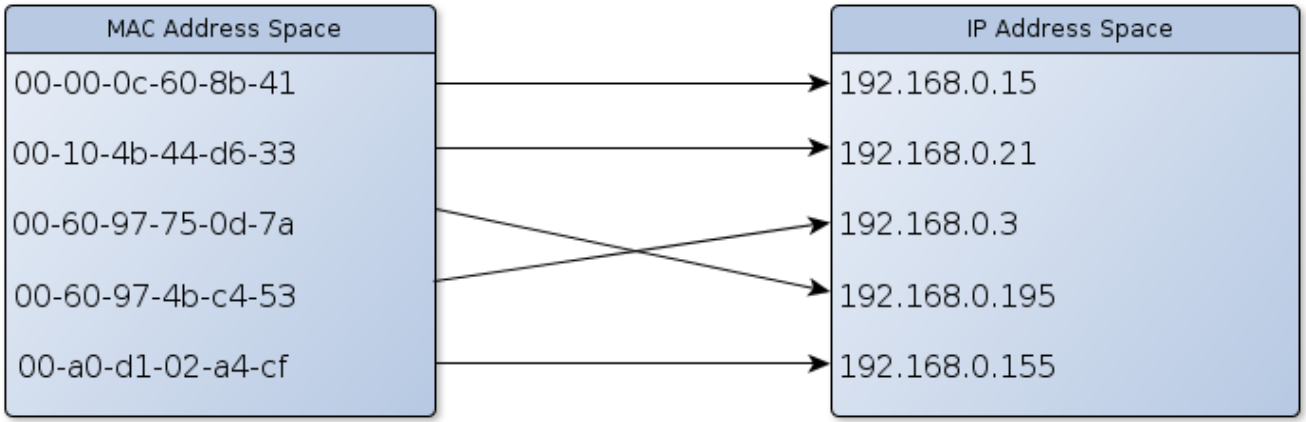
Ethernet - MAC Address

- *Media Access Control Address*.
- Identificador de una interfaz de red.
- 6 octetos
- 3 de OUI (Organization Unique Identifier) `standards.ieee.org/develop/regauth/oui/public.html`
- 3 de NIC (Network Interface Controller)
- Intel Corporate: 00:1c:c0:fa:55:cc

Ethernet - MAC Address cont.



Navegando entre dos mundos



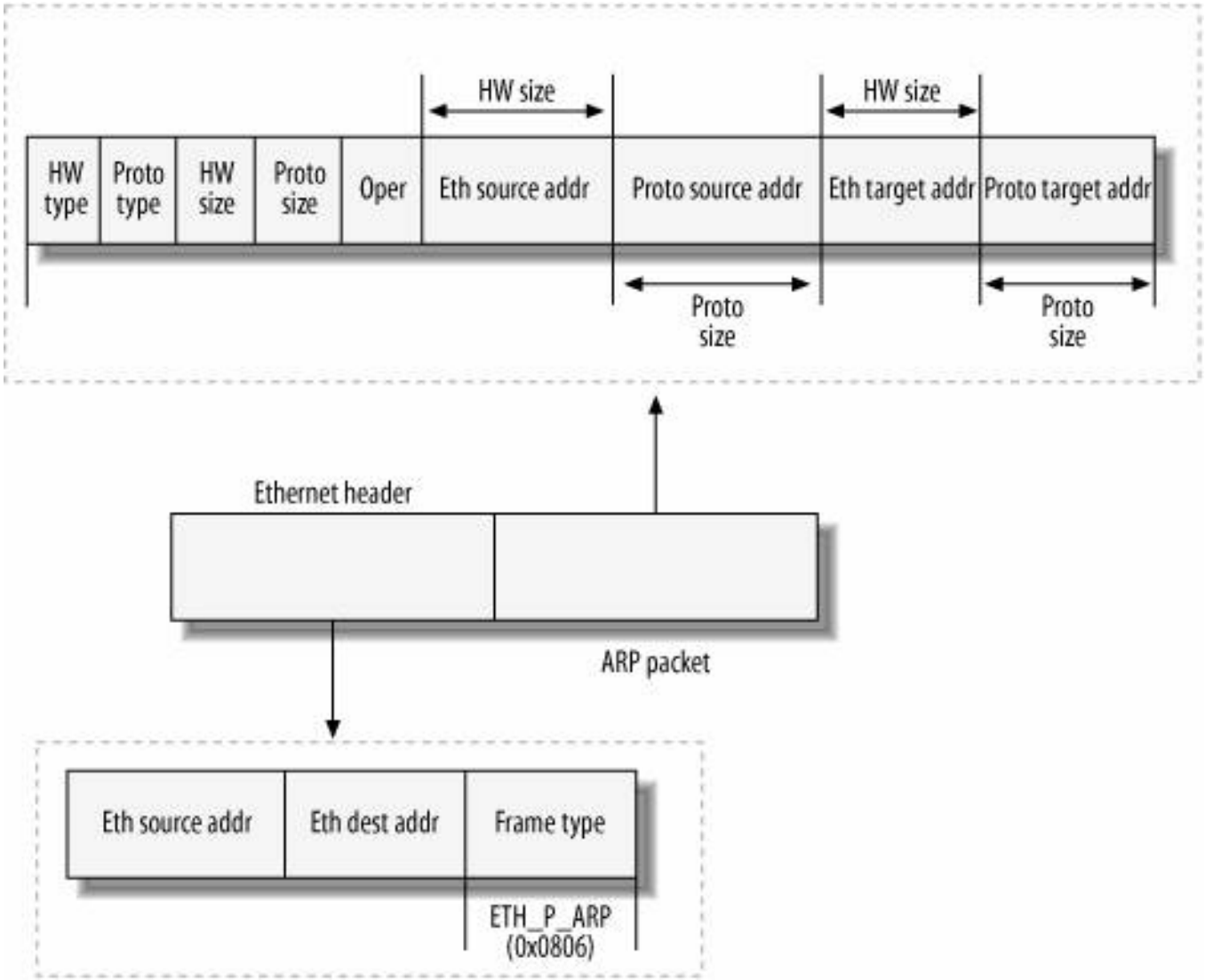
¿Qué es ARP?

- La sigla: *Address Resolution Protocol*.
- Es un protocolo que, en esencia, permite mapear direcciones de nivel de red a direcciones físicas.
- Clave e indispensable en el funcionamiento de las redes modernas.
- Especificado en el RFC 826 (circa 1982).
- No está limitado a IP + Ethernet: la especificación es general.

Tecnicismos varios

- La pregunta ARP consiste en un mensaje **broadcast** sobre la red local.
  - Recordar que no se propaga más allá de la red local!
- La respuesta, en cambio, es **unicast**.
- Optimización: se implementa una caché para guardar las direcciones resueltas (o conocidas).
  - Las entradas se agregan al resolver o bien al observar un pedido de otra máquina.
  - Cada entrada tiene un tiempo de expiración para evitar problemas.

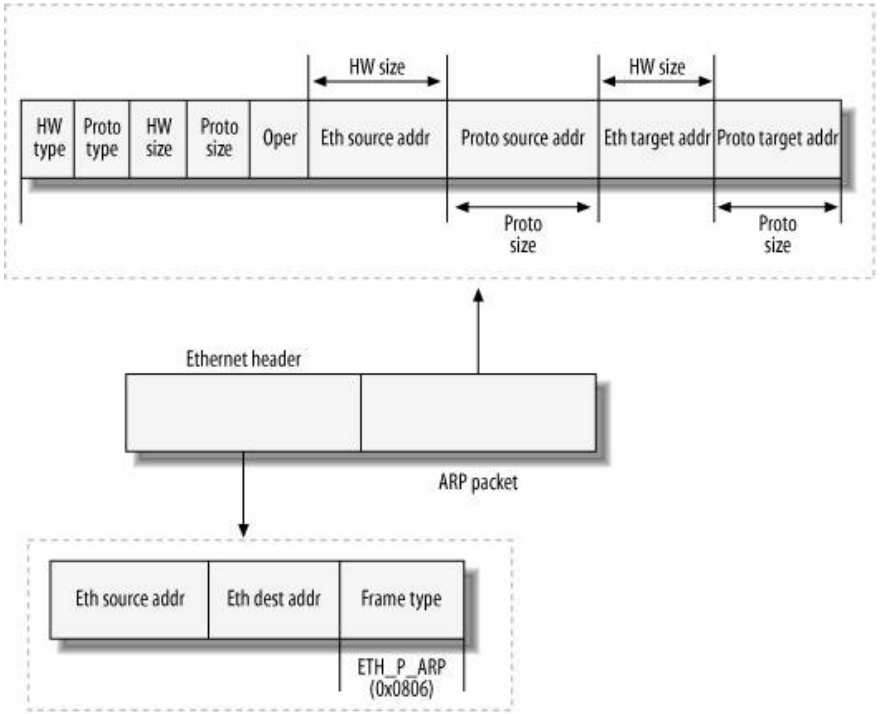
Pormenores del paquete



Pormenores del paquete (cont.)

- El campo **Oper** puede tomar los valores 1 (`who-has`) o 2 (`reply`).
- Observar que la cantidad de bits asingada a las direcciones depende del valor que tomen los campos **HW size** y **Proto size**.
- Dichos campos tienen un largo de 8 bits (i.e., direcciones con un máximo de $2^8 - 1 = 255$ bits).
- **HW type** y **Proto type** indican los protocolos de nivel de enlace y de nivel de red respectivamente involucrados en la comunicación.

¿Cómo funciona?



Otro uso interesante

- Cuando una máquina bootea o se levanta una de sus interfaces, muchos SOs envían automáticamente un pedido ARP *gratuito*.
- En él, **Proto source addr** == **Proto target addr**.
- Objetivos:
  - Detectar IPs duplicadas en la red local: esto ocurre si se recibe una respuesta.
  - Actualizar la caché ARP de los otros hosts.

...y otro uso más: ARP Spoofing

Spoofing

1. To deceive.
2. To do a spoof of; satirize gently.

- De lo anterior se desprende que ARP es un protocolo **sin estado** y **sin seguridad**.
- La técnica de ARP spoofing se apoya precisamente en estas características.
- Idea: una máquina envía de la nada una respuesta ARP mapeando una IP objetivo con su propia MAC.
- $\Rightarrow$ todo el tráfico destinado a dicha IP va a ser recibido por ella.