ARP

Address Resolution Protocol

# Definición

Es un protocolo de comunicaciones de la capa de enlace de datos (2), responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

Es **imprescindible** para la **transmisión de datos en redes Ethernet** por dos razones:

* las tramas de datos (también **tramas Ethernet) de los paquetes IP** solo pueden enviarse con **ayuda de una dirección de hardware** a los hosts de destino, pero el protocolo de Internet no puede obtener estas direcciones físicas por sí mismo.
* debido a su limitada longitud, el protocolo **IPv4 carece de la posibilidad de almacenar las direcciones de los dispositivos**.

Con un mecanismo de caché propio, el protocolo ARP también es, aquí, la solución más adecuada. IPv6, por su parte, adopta las funciones del Neighbor Discovery Protocol (NDP).

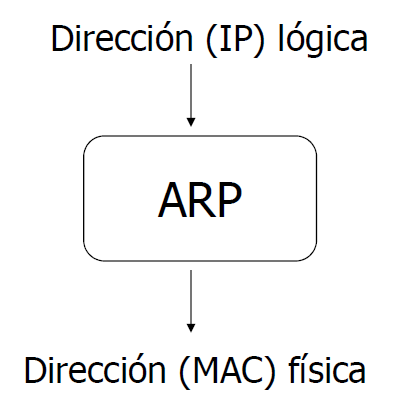
# Problema que resuelve

Problemas:

* Las aplicaciones de alto nivel solo trabajan con direcciones IP.
  + Ilusión de una única red virtual.
  + La comunicación es realizada por redes físicas, reales.
* Los datagramas IP son encapsulados en tramas MAC → se necesitan direcciones de hardware MAC.

Resolución

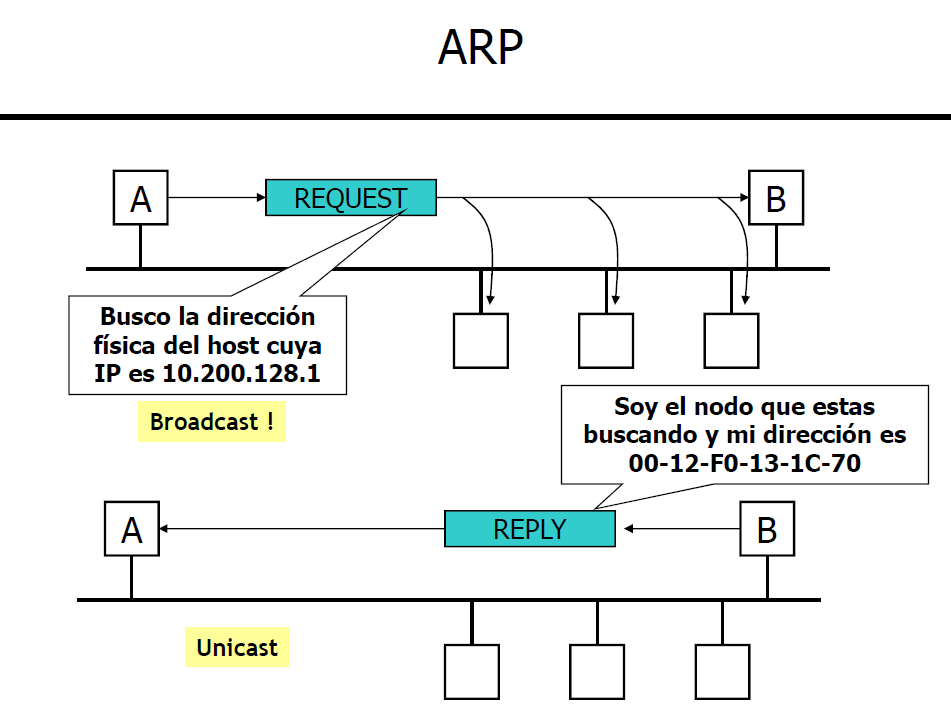
* Mapear direcciones IP de alto nivel a direcciones MAC físicas.



**Ejemplos concretos:**

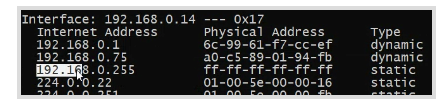
* Para enviar un mensaje a la impresora, necesito saber su mac address. Esto lo necesito para mandarle una trama Ethernet.
* Para enviar un mensaje a Gmail via browser, necesito saber el mac address del router.

# Cómo funciona



A trata de conectarse con B.

1. Envía un mensaje tipo **broadcast** a toda la red (sólo los vecinos, miembros de esa red) preguntando quién tiene la dirección MAC de B.
2. B le responde a A con un **unicast**, diciendo: “esa MAC es mía”
3. Esta info nueva se almacena en un cache que tiene una duración. La info es efímera.



## Para asignar direcciones por medio del ARP:

* **Revisión de la máscara de subred** para **distinguir si la dirección IP del host de destino** se encuentra en la **misma red local o en otra subred.**
  1. Si la IP se encuentra **en la** **red local**, el primer paso es **controlar si ya existe una entrada** para ella en la **caché del ARP.**
     1. Si una **dirección IP ya tiene asignada una dirección física**, se usa ésta para el direccionamiento.
     2. En **caso contrario:**
        1. El remitente **envía una solicitud ARP (ARP Request)** con la dirección IP de destino **a todos los hosts de la red**. Para eso, el emisor usa la dirección de broadcast de ARP: FF:FF:FF:FF:FF:FF como dirección del destinatario.
        2. **Cada una de las estaciones compara la dirección IP indicada en la petición con las suyas propias** y rechaza la solicitud si no hay coincidencia. Si una estación percibe que **se trata de la dirección propia**, reacciona con una **respuesta ARP (ARP Reply**) en la que, entre otros datos, también **transmite la dirección MAC**. Ambas partes pueden **incorporar la dirección MAC y la IP de la otra parte en la memoria caché**, sentando las bases para el intercambio de datos.
* Si el host de destino **no se encuentra en la misma subred**, el remitente se dirige a la puerta de enlace estándar (en la mayoría de los casos un router).
  1. Puede acceder a ella mediante la combinación de dirección MAC e IP, por lo que aquí también se necesita el Address Resolution Protocol.
  2. Una vez resueltas las direcciones, la puerta de enlace recibe el paquete de datos y a continuación lo envía al host de destino. Para ello esta pasarela de enlace analiza la cabecera IP para obtener los datos necesarios.
  3. El proceso se repite tantas veces como sea necesario hasta que el paquete de datos llegue a su destino o hasta que el campo TTL (Time to Live) haya adoptado el valor 0 en la cabecera IP.

## Entregas

### Entrega directa o unicast

Caso en el que busca una única dirección MAC.

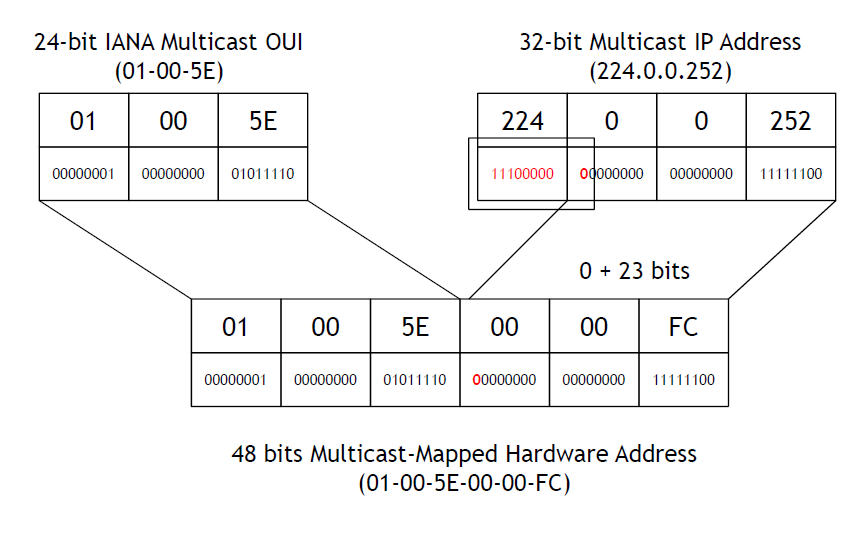
### Entrega broadcast

Caso en el que se envía un broadcast. No se hace la ARP request, la dirección IP todos los host, se mapea a la dirección MAC todos los dispositivos (la de broadcast).

### Entrega multicast

Caso en el que el **mensaje va dirigido a un grupo destino** (las direcciones de clase D).

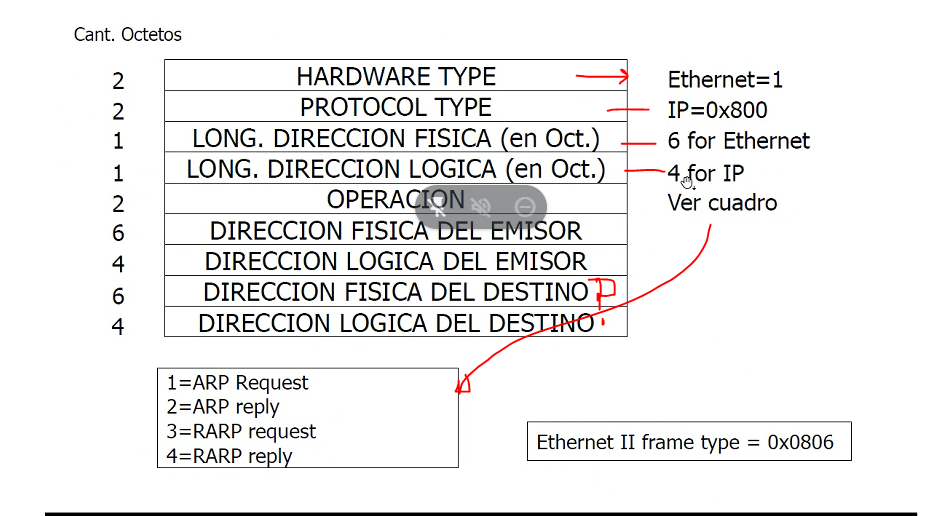
**No se hace la ARP request.** Se encapsula el datagrama IP con dirección destino multicast en una trama Ethernet cuya dirección **MAC destino se confecciona a partir de la información de grupo de multicast.** Entonces las estaciones que pertenezcan a ese grupo de multicast van a identificar esa dirección MAC y van a procesar los mensajes. Quienes no pertenezcan lo van a ignorar.



Se **combina la IANA multicast OUI** (identificador único de organización, es un prefijo de la MAC address para grupos) **con la dirección IP multicast** que identifica el grupo (todos los octetos menos el 224 que identifica a multicast en si), **está combinación conforma la dirección MAC destino.**

# Formato de datagrama

El datagrama va a ir encapsulado en una trama Ethernet cuyo EtherType es 0x0806.



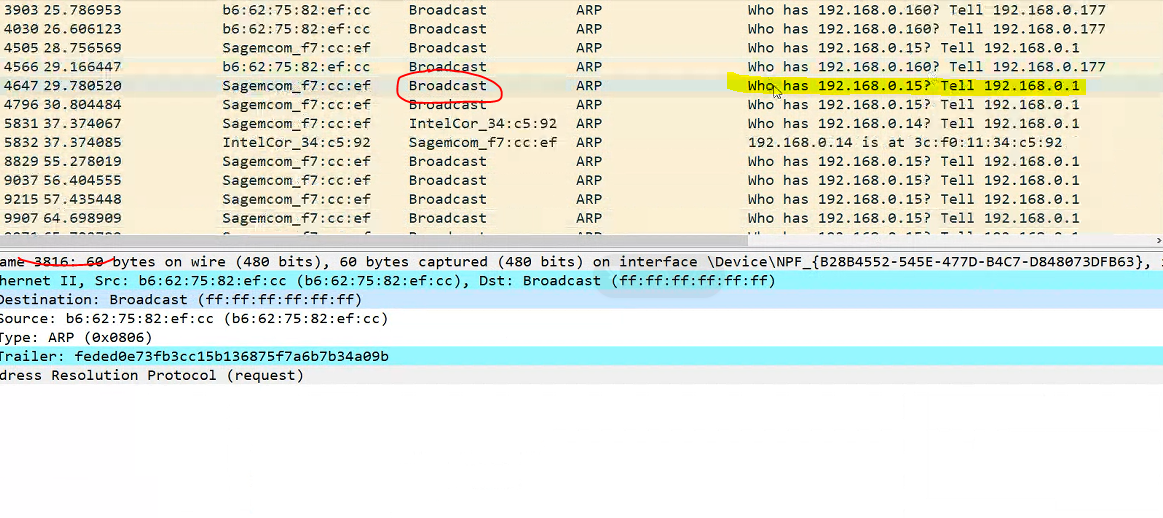
# Caso real en wireshark

Se busca averiguar la dir física del destino.

Tiene un **formato dinámico**, porque **se adecua a varios tipos** (hardware/protocolo).

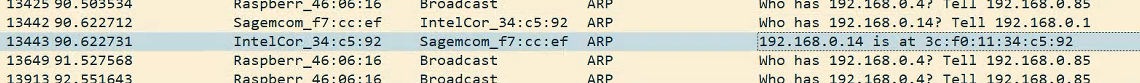
En longitud de dirección, el 6 y el 4 es la cantidad de bytes que se utilizan.

En la **request**, la **dirección física del destino va en 0** porque es lo que queremos averiguar.

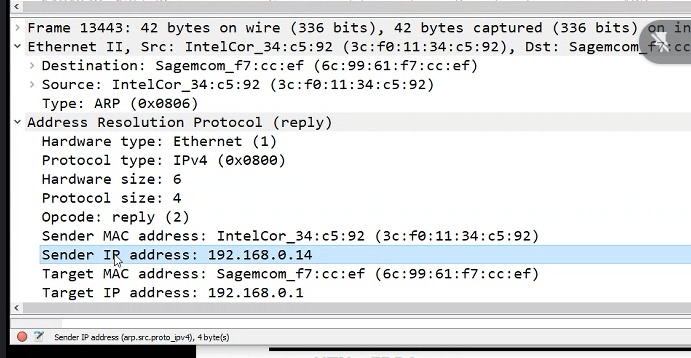


Este msj se manda una y otra vez como broadcast porque no encuentra a ese IP.

Reply:

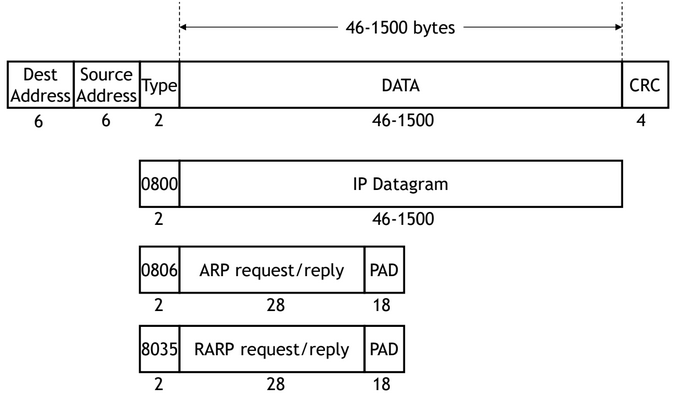


Envia unicast al router.



El router lo olvida bastante rápido (segundos) y vuelve a preguntar.

# Estructura de la trama Ethernet para ARP



Como son solo 28 bytes el ARP request/reply y la cantidad mínima de un campo de datos es 46, se rellena con 18 bytes.

# Gratuitous ARP

Antes de activar la interfaz con cualquier dirección IP lo que va a hacer el host es enviar un ARP request gratuito. Lo llamamos gratuito porque el host pregunta por sí mismo (la dirección IP asignada), si alguien responde, hay un conflicto. De esta manera el host detecta si existe alguien con su misma IP.

Es una variante del ARP. Son útiles por las siguientes razones:

* Permiten detectar conflictos en IP (principal utilidad, por ejemplo cuando sale el “la dirección IP está en uso).
* Actualizan el contenido del cache ARP.
* Informan a los switches el MAC del cliente conectado.
* Sucede a cada cambio de estado de la interfaz, por lo que indica si hay problemas.

Resumen Koval de Gratuitous: consiste en preguntar por mi mismo. X pide X (misma dir entre target y quién pregunta). Esto permite detectar dirs IP duplicadas.

Esto se manda antes de guardar una configuración manual de una IP estática, para verificar que n oesté repetida.