# Protocolo de resolución de direcciones

En red de computadoras, el protocolo (ARP) es un protocolo de comunicaciones de la capa de enlace de datos, responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto solo funciona si todas las máquinas lo soportan.  
En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas)

**Tablas ARP** Ejemplificando, para localizar al señor “X” entre 150 personas: preguntar por su nombre a todos, y el señor “X” debe responder. Cuando a **A** le llegue un mensaje con dirección origen IP y no tenga esa dirección en su caché de la tabla ARP, enviará su trama ARP a la dirección broadcast con la IP de la que quiere conocer su dirección física. El equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física.

**Reverse ARP (RARP):** Es un protocolo para obtener la dirección IP perteneciente a un determinado hardware electrónico que se encuentra en la mayoría de las veces en una red Ethernet. Las especificaciones del RARP se encuentran en RFC 903. RARP ya no es usado, fue reemplazado por BOOTP el cual fue tiempo más tarde sustituido por el Protocolo de Configuración Dinámica de Host (DHCP). RARP utiliza el mismo mecanismo que ARP

**ARP Proxy:** La técnica ARP Proxy consiste en que un host, generalmente un router, responde a peticiones ARP destinadas a un host que se encuentra fuera de la red local. Por fingir su identidad, el router es responsable de encaminar el paquete hacia su destino real. La técnica ARP Proxy permite a los hosts de una subred alcanzar subredes remotas sin la necesidad de configurar el enrutamiento o la puerta de enlace predeterminada   
**Ventajas:** La principal ventaja del uso de la técnica ARP Proxy es que se puede agregar a un solo enrutador en la red, permite que no se distorsione las tablas de encaminamiento de los otros enrutadores de la red. Es recomendable que el ARP Proxy sea utilizado en redes donde los hosts IP no se encuentren configurados con ninguna puerta de enlace predeterminada.

**Desventajas:**

Aumenta la cantidad de tráfico ARP en su segmento.

Posee grandes tablas ARP para manejar la asignación de dirección IP a MAC.

La seguridad puede ser expuesta. Un host puede simular ser otro host con el fin de interceptar los paquetes, esto es llamado “spoofing”.  
  
No funciona para redes que no utilicen el protocolo ARP para la resolución de direcciones.

**Exploración ARP:** Una exploración ARP es una petición construida con una dirección IP del remitente de todo ceros.  
Es utilizado específicamente en direcciones IPv4 de detección de conflictos. Antes de comenzar a utilizar una dirección IPv4, una serie implementara esta especificación que debe comprobar para ver si la dirección ya está en uso, mediante la transmisión de paquetes ARP exploración.

**Alcance de funcionamiento:** El protocolo de resolución de direcciones es una solicitud y un protocolo de respuesta que ejecuta encapsulado por el protocolo de línea. Se comunica dentro de los límites de una sola red, nunca encaminado a través de los nodos de interconexión de redes. Este establecimiento pone ARP en la capa de enlace del conjunto de protocolos de Internet; mientras que en la interconexión de sistemas abiertos normalmente se describe como residentes entre las capas 2 y 3, el ARP está rodeado por protocolos de capa 2, sin embargo, ARP no se desarrolló en el marco de OSI.