Protocolo de resolución de direcciones

En red de computadoras, el **protocolo de resolución de direcciones** (**ARP**, del inglés *Address Resolution Protocol*) es un protocolo de comunicaciones de la capa de enlace de datos, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (*ARP request*) a la dirección de difusión de la red (*broadcast*, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (*ARP reply*) 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.

ARP está documentado en el RFC 826. El protocolo RARP realiza la operación inversa y se encuentra descrito en el RFC 903.

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). Para realizar esta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

ARP se utiliza en cuatro casos referentes a la comunicación entre dos *hosts*:

1. Cuando dos *hosts* están en la misma red y uno quiere enviar un paquete a otro.
2. Cuando dos *hosts* están sobre redes diferentes y deben usar un *gateway* o *router* para alcanzar otro *host*.
3. Cuando un *router* necesita enviar un paquete a un *host* a través de otro *router*.
4. Cuando un *router* necesita enviar un paquete a un *host* de la misma red.

1 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* (física = FF:FF:FF:FF:FF:FF), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física. En este momento, A ya puede agregar la entrada de esa IP a la caché de su tabla ARP.

Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (por ejemplo: si se estropea una tarjeta de red y hay que sustituirla, o simplemente algún usuario de la red cambia de dirección IP).

2 *Reverse ARP* (RARP)

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 (protocolo de red que es usado para obtener una dirección IP de un servidor), el cual fue tiempo más tarde sustituido por el **Protocolo de Configuración Dinámica de *Host*** (DHCP).

RARP utiliza el mismo mecanismo que ARP. La respuesta que se devuelve de una solicitud es la dirección de protocolo de la estación origen, no la dirección de la estación destino de la solicitud.

Para poder usar RARP, todas las direcciones MAC deben estar configuradas en un servidor central para que transfiera una dirección IP.

El RARP además de encontrarlo en las redes Ethernet, está disponible en otras redes de área local como lo son la Interfaz de Fibra de Distribución de Datos y las redes LAN Token Ring, entre otras.

3 *Inverse ARP* (InARP)

La función del InARP es traducir las direcciones de la capa de red (capa 3) a direcciones de la capa de enlace de datos (capa 2).

Es mas efectivo que usar el envió de mensaje ARP en cada circuito virtual para cada dirección que desee resolver, y más flexible porque no depende de una configuración estática.

InARP no envía solicitudes porque conoce la dirección

de la estación destino.

InARP sucede cada 60 segundos predeterminadamente en los circuitos virtuales que se encuentran activos.

Cuando se envía un mensaje completo de información llamado *full status message* se puede conocer si un circuito está activo. Cuando el *router* reconoce que se encuentra un circuito activo, en el circuito virtual, envía un *Inverse ARP*, en caso de que no haya sido ya ejecutado con el comando *frame-relay map*.

InARP es implementada como una extensión del protocolo ARP, la cual utiliza el mismo formato de paquete como el ARP, difiere porque usa el código de operación distinto.

4 *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 (*gateway)*.

ARP Proxy se define en RFC 1027.

4.1 Usos

Uno de los usos de la técnica *ARP Proxy* es cuando en una implementación más antigua de IPv4, no puede deducir si el *host* destino se encuentra en la misma red lógica que el *host* de origen. En estos casos, el ARP envía solicitudes de ARP para la dirección IPv4 de destino.

Si en la interfaz del *router* se desactiva el *Proxy ARP*, entonces los *hosts* no podrán comunicarse fuera de la red local.

Otro caso en donde se utiliza el *ARP Proxy* es cuando un *host* cree estar conectado directamente a la misma red lógica del *host* de destino. Esto sucede cuando se configura el *host* con una máscara de red inapropiada.

Otro uso que se puede dar a la técnica *ARP Proxy* es cuando se trata de un *host* que no está configurado con una *gateway* predeterminada.

El *ARP Proxy* permite que los dispositivos de una red accedan a subredes remotas sin tener que configurar el enrutamiento o la *gateway* predeterminada.

4.2 Ventajas

La principal ventaja del uso de la técnica ARP Proxy es que se puede agregar a un solo enrutador en la red, esto 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.

4.3 Desventajas

Los anfitriones (*hosts*) no tienen ni idea de los detalles físicos de la red y suponen que es una red plana la cual llega a cualquier destino con tan solo hacer una solicitud ARP.

ARP tiene las desventajas siguientes:

- 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.

5 Exploración ARP

Una exploración ARP es una petición construida con una dirección IP del remitente de todo ceros.

El término es utilizado específicamente en direcciones IPv4 de detección de conflictos (RFC 5227). Antes de comenzar a utilizar una dirección IPv4 (si recibió de configuración manual, DHCP, o de cualquier otra manera), una serie implementara esta especificación que debe comprobar para ver si la dirección ya está en uso, mediante la transmisión de paquetes ARP exploración.

6 Alcance de funcionamiento

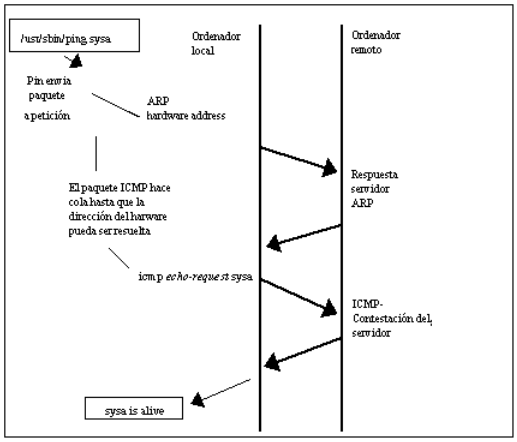
El protocolo de resolución de direcciones es una solicitud y un protocolo de respuesta que ejecuta encapsulado por el protocolo de línea. Se comunica dentro de los límites de una sola red, nunca encaminado a través de los nodos de interconexión de redes. Este establecimiento pone ARP en la capa de enlace del conjunto de protocolos de Internet; mientras que en la interconexión de sistemas abiertos (OSI), 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.

6.1 Funcionamiento I

Si A quiere enviar una trama a la dirección IP de B (misma red), mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos la trama, no tendrán que deshacerla para comprobar si el mensaje es para ellos, sino que se hace con la dirección física.

6.2 Funcionamiento II

Si A quiere enviar un mensaje a C (un nodo que no esté en la misma red), el mensaje deberá salir de la red. Así, A envía la trama a la dirección física de salida del *router*. Esta dirección física la obtendrá a partir de la IP del *router*, utilizando la tabla ARP. Si esta entrada no está en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.



Ejemplo Address Resolution Protocol *(ARP).*

Una vez en el *router*, este consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por la interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último *router*, que es el que comparte el medio con el *host* destino. Aquí el proceso cambia: la interfaz del *router* tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP, y en caso de no existir la entrada correspondiente a la IP, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.

7 Estructura del paquete

El ARP utiliza un formato de mensaje simple que contiene una solicitud de resolución de dirección o respuesta.

El tamaño del mensaje ARP depende de la capa superior y menor tamaño de dirección de capa, que se da por el tipo de protocolo de red (por lo general IPv4) en uso y el tipo de capa de enlace virtual que el protocolo de capa superior se ejecuta en el hardware.

El encabezado del mensaje especifica estos tipos, así como el tamaño de las direcciones de cada uno. El encabezado del mensaje se completa con el código de operación para la solicitud (1) y la respuesta (2).

La carga útil del paquete consta de cuatro direcciones, el hardware y la dirección de protocolo del remitente y el receptor *host*.

- Tipo de hardware o *Hardware Type* (**HTYPE**): este campo especifica el tipo de protocolo de red. Ejemplo: Ethernet es 1.
- Tipo de protocolo o *Protocol Type* (**PTYPE**): este campo especifica el protocolo de interconexión de redes para las que se destina la petición ARP. Para IPv4, esto tiene el valor 0x0800. Los valores permitidos pType comparten un espacio de numeración con los de EtherType.
- Longitud Hardware (**HLEN**): longitud (en octetos) de una dirección de hardware. En Ethernet el tamaño de direcciones es de 6.
- Longitud del Protocolo (**PLEN**): longitud (en octetos) de direcciones utilizadas en el protocolo de capa superior. El protocolo de capa superior especificado en PTYPE. IPv4 tamaño de la dirección es de 4.
- Operación: especifica la operación que el emisor está realizando: **1** para la petición, **2** para la respuesta.
- Dirección de hardware del remitente (**SHA**): dirección de medios de comunicación del remitente.
- Remitente dirección de protocolo ('*SPA*): dirección de la interconexión del remitente.
- Dirección de hardware de destino (**THA**): dirección de los medios de comunicación del receptor previsto. Este campo se ignora en las solicitudes.
- Dirección de protocolo *target* (**TPA**): dirección de la interconexión del receptor previsto.

Valores de los parámetros del protocolo ARP se han normalizado y se mantienen por la Autoridad de Números Asignados de Internet (IANA).

7.1 Generación del paquete ARP

Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio *host* de destino o un "*router*") y el dispositivo hardware al que se debería enviar.

Si se trata de una red 802.3./4/5, deberá consultarse al módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un *broadcast* de red para una solicitud ARP.

7.2 Recepción del paquete ARP

Cuando un host recibe un paquete ARP (bien un *broadcast* o una respuesta punto a punto), el dispositivo receptor le pasa el paquete al módulo ARP.

7.3 Ejemplo

Las computadoras Matterhorn y Washington están en una oficina, conectados entre sí en una red de área local de la oficina mediante cables Ethernet y conmutadores de red, sin *gateways* o *routers* intermedios.

Matterhorn quiere enviar un paquete a Washington. A través de otros medios, se determina que la dirección IP de Washington es 192.168.0.55, pero para enviar el mensaje también tiene que saber la dirección MAC de Washington.

En primer lugar, Matterhorn utiliza una tabla caché ARP para buscar 192.168.0.55 en todos los registros existentes la dirección MAC de Washington (00: eb: 24: B2: 05: ac).

Si el caché no ha dado ningún resultado para 192.168.0.55, Matterhorn envía un mensaje *ARP broadcast* (destino FF: FF: FF: FF: FF: FF de dirección MAC, que es aceptada por todos los equipos), solicitando una respuesta para 192.168.0.55.

Washington responde con su dirección MAC (y su IP). Washington puede insertar una entrada para Matterhorn en su propia tabla ARP para su uso futuro.

La información de la respuesta se almacena en caché en la tabla ARP del Matterhorn y el mensaje que se puede enviar.

8 Véase también

- RARP

9 Referencias

- «ARP» (en inglés). Consultado el 3 de julio de 2013.
- «ARP» (en inglés). Consultado el 3 de julio de 2013.

10 Enlaces externos

- RFC 826
- RFC 826 (español)
- RFC 903
- RFC 826
- RFC 903
- RFC 1027
- RFC 5227

11 Origen del texto y las imágenes, colaboradores y licencias

11.1 Texto

- **Protocolo de resolución de direcciones** *Fuente:* https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones?oldid=85791739 *Colaboradores:* Pilaf, Tano4595, Barcex, Gchain, Taichi, RobotQuistnix, Yrbot, BOT-Superzerocool, Vitamine, YurikBot, Icvav, GermanX, JRGL, BOTpolicia, CEM-bot, Jjvaca, JosepabloULE, Thijs!bot, PabloCastellano, TXiKiBoT, Juckar, Gustronico, Rei-bot, Cinevoro, VolkovBot, Matdrodes, Synthebot, Barri, AlleborgoBot, Muro Bot, Gerakibot, SieBot, Ironfisher, Carmin, Macarse, Er conde, Manwë, Marcecoro, A20002174, HUB, Tonchizerodos, Alexbot, BodhisattvaBot, AVBOT, MarcoAurelio, Diegusjaimes, Bethan 182, Arjuno3, L18r4, Dangelin5, ArthurBot, MartinDM, Felix.rivas, Xqbot, SassoBot, Dreitmen, AdrianLois, PatruBOT, EmausBot, Savh, Zchumager, Pequetrefe, Chapito69, MerlIwBot, KLBot2, TeleMania, AvocatoBot, Gonzalo0089, Alsan1228, Sebc, Alba10, Crystallizedcarbon, BenjaBot, Gloix01, Juanga983 y Anónimos: 80

11.2 Imágenes

- **Archivo:Arp_v1.PNG** *Fuente:* https://upload.wikimedia.org/wikipedia/commons/c/c5/Arp_v1.PNG *Licencia:* Public domain *Colaboradores:* ? *Artista original:* ?

11.3 Licencia del contenido

- Creative Commons Attribution-Share Alike 3.0