Protocolo ARP

El protocolo ARP tiene un papel clave entre los protocolos de capa de Internet relacionados con el protocolo TCP/IP, ya que permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP. Por eso se llama Protocolo de Resolución de Dirección (en inglés ARP significa Address Resolution Protocol).

Cada equipo conectado a la red tiene un número de identificación de 48 bits. Éste es un número único establecido en la fábrica en el momento de fabricación de la tarjeta. Sin embargo, la comunicación en Internet no utiliza directamente este número (ya que las direcciones de los equipos deberían cambiarse cada vez que se cambia la tarjeta de interfaz de red), sino que utiliza una dirección lógica asignada por un organismo: la dirección IP.

Para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya. Si alguno de ellos se identifica con esta dirección, el equipo responderá al ARP, que almacenará el par de direcciones en la tabla de búsqueda, y, a continuación, podrá establecerse la comunicación.

Tablas ARP

Esta taba es un cache en el cual se guardan por un tiempo limitado el numero de ip de una maquina enlazado con su dirección Mac.(Para pedir la tabla utilizamos en cmd el comando arp–a)

Funcionamiento

Primer Funcionamiento

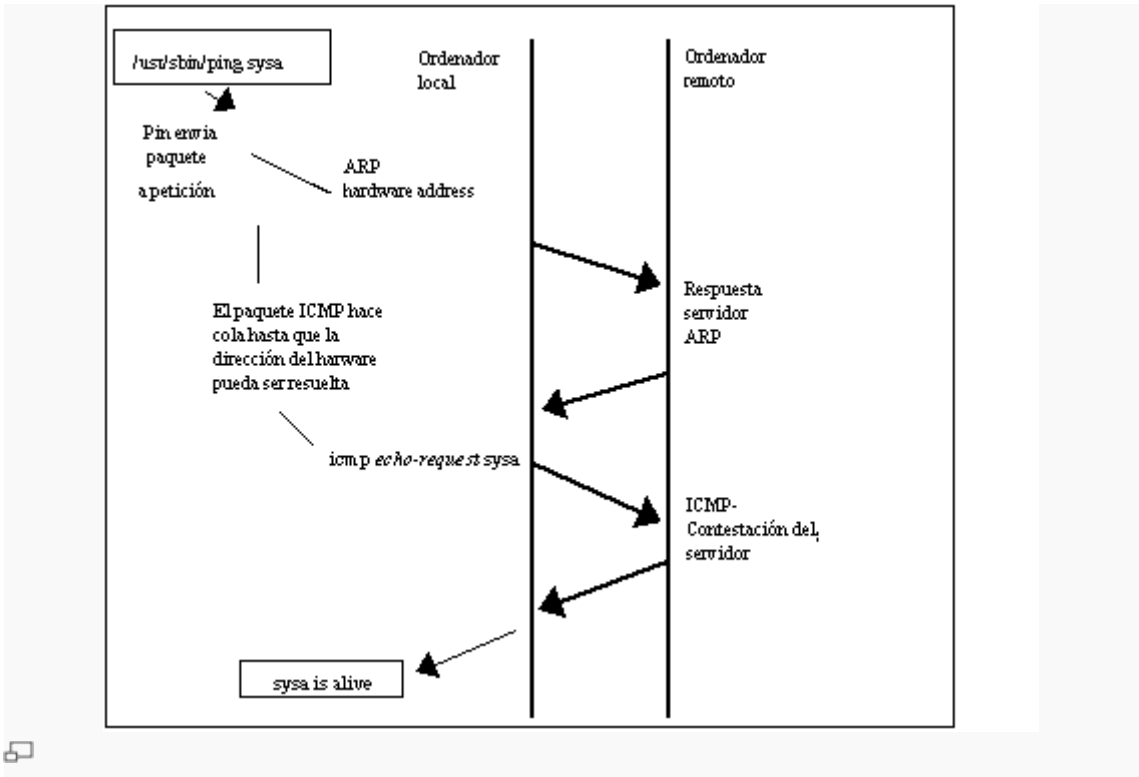
Si A quiere enviar una trama a la dirección IP de B (misma red), mirará su tabla ARP para poner en la trama la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos la trama, no tendrán que deshacerla para comprobar si el mensaje es para ellos, sino que se hace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

Segundo Funcionamiento

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.

Una vez en el router, éste consultará su tabla de encaminamiento(tabla ARP), 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 .



Estructura del paquete

El Protocolo de resolución de direcciones utiliza un formato simple mensaje 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 o. 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 y la respuesta .

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

Tipo de hardware (HTYPE) : Este campo especifica el tipo de protocolo de red. Ejemplo: Ethernet.

Tipo de protocolo (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. El tamaño de direcciones Ethernet es 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.) El tamaño de la dirección de IPv4 es 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.

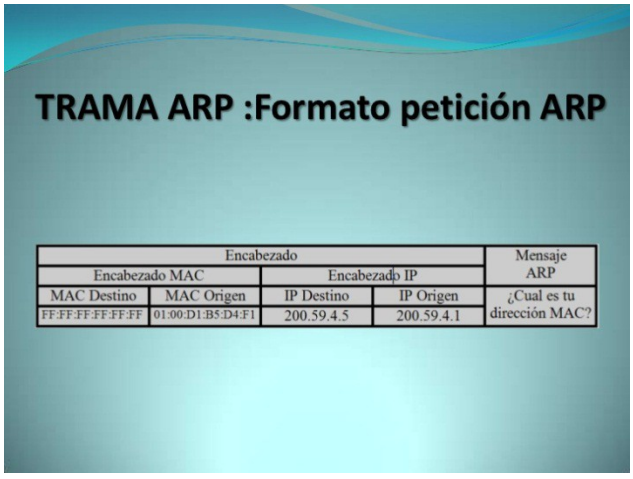
Remitente dirección de protocolo (SPA) : dirección de la interconexión del remitente.

Dirección de hardware de destino (THA) : dirección de los medios de comunicación del receptor previsto. Este campo se ignora en las solicitudes.

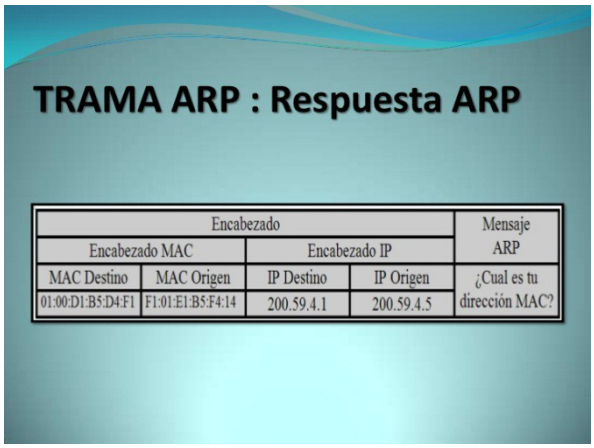
Target dirección de protocolo (TPA) : dirección de la interconexión del receptor previsto.

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

Paquete del emisor



Paquete de Respuesta



Ejemplo

Así que para saber la MAC de otro equipo no hay más que comunicarse con él (haciendo un ping por ejemplo) y luego mirar la tabla arp de nuestro equipo.

Así que si nosotros tenemos la dirección IP: 192.168.1.136, y nuestra impresora tiene la dirección IP 192.168.1.99 tenemos que:

Paso 0)

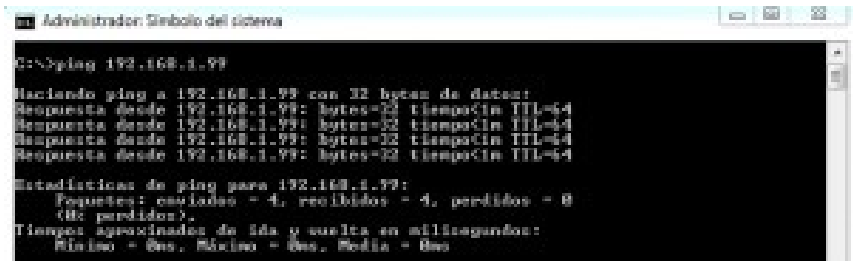
Ver si la dirección MAC de la impresora ya ha sido resuelta por el protocolo ARP. Si es así, ya habremos terminado. Ésto ocurrirá siempre que en la sesión actual hayamos conectado con ella, por ejemplo enviando un documento para imprimir.

En nuestro caso no está, por lo que pasamos al paso 1)

Paso 1)

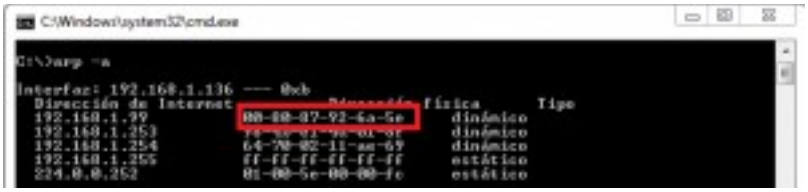
Comunicarnos con la impresora para asegurarnos que el protocolo arp resuelve su dirección MAC

Realizamos un ping a 192.168.1.99 y esperamos la respuesta.



Paso 2)

Luego miramos la tabla ARP de nuestro equipo con el comando: arp -a



ARP PROBE

Un ARP Probe es una petición construida con una dirección IP del remitente de todo ceros. El término es utilizado específicamente en direcciones IPv4 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 Probe.

ARP SPOOFING

El ***ARP Spoofing***, también conocido como ***ARP Poisoning*** o ***ARP Poison Routing***, es una técnica usada para infiltrarse en una red ethernet conmutada (basada en *switches* y no en *hubs*), que puede permitir al atacante leer paquetes de datos en la LAN (red de área local), modificar el tráfico, o incluso detenerlo.

El principio del *ARP Spoofing* es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. Normalmente la finalidad es asociar ladirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada (gateway). Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). El atacante puede incluso lanzar un ataque de tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

El ataque de ARP Spoofing puede ser ejecutado desde una máquina controlada (el atacante ha conseguido previamente hacerse con el control de la misma: intrusión), o bien la máquina del atacante está conectada directamente a la LAN Ethernet.

Como sucede desde el lado del atacante

El envenenamiento de las tablas ARP consiste básicamente en inundar la red con paquetes ARP indicando que la nuestra es la MAC asociada a la IP de nuestra víctima y que nuestra MAC está también asociada a la IP del router (puerta de enlace) de nuestra red. De este modo, todas las máquinas actualizaran sus tablas con esta nueva información maliciosa. Así cada vez que alguien quiera enviar un paquete a través del router, ese paquete no será recogido por el router, sino por nuestra máquina, pues se dirige a nuestra dirección MAC, y cada vez que el router u otra máquina envíe un paquete a nuestra víctima sucederá lo mismo. Como nuestra máquina sabe que "está haciendo trampas" no se auto envenenará y sí conocerá las MACs reales de todas sus víctimas, por lo que la podremos configurar para que reenvíe esos paquetes a su verdadero destinatario, así nadie notará que nos hemos metido en medio (Man-in-the-middle)

Ahora que todos los paquetes que nos interesan pasan por nuestra máquina podremos usar una aplicación analizadora de paquetes (sniffer) como Wireshark para ver su contenido y usarlo con buenos o malos propósitos.

Defensa de ARP Spoofing

Un método para prevenir el **ARP Spoofing**, es el uso de tablas ARP estáticas, es decir añadir entradas estáticas ARP, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP. Sin embargo, esta no es una solución práctica, sobre todo en redes grandes, debido al enorme esfuerzo necesario para mantener las tablas ARP actualizadas: cada vez que se cambie la dirección IP de un equipo, es necesario actualizar todas las tablas de todos los equipos de la red.

Por lo tanto, en redes grandes es preferible usar otro método: el DHCP snooping. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC que están conectadas a cada puerto, de modo que rápidamente detecta si se recibe una suplantación ARP. Este método es implementado en el equipamiento de red de fabricantes comoCisco, Extreme Networks y Allied Telesis.

Otra forma de defenderse contra el ARP Spoofing, es detectarlo. Arpwatch es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía correo electrónico al administrador de la red, cuando una entrada ARP cambia.

Comprobar la existencia de direcciones MAC clonadas (correspondientes a distintas direcciones IP) puede ser también un indicio de la presencia de ARP Spoofing, aunque hay que tener en cuenta, que hay usos legítimos de la clonación de direcciones MAC.

RARP ("Reverse ARP", o ARP inverso) es el protocolo usado para consultar, a partir de una dirección MAC, su dirección IP correspondiente. Si ante una consulta, RARP devuelve más de una dirección IP, significa que esa dirección MAC ha sido clonada.

PROXY ARP

El **Proxy ARP** es una técnica para usar el ARP para proporcionar un mecanismo de enrutamiento *ad hoc*.

Un dispositivo de varios puertos, como un router, que implemente Proxy ARP responderá a las peticiones de ARP en una interfaz como delegado o encargado de las direcciones de un dispositivo de otra interfaz. El dispositivo puede entonces recibir y remitir paquetes dirigidos a los demás dispositivos.

La ventaja del Proxy ARP sobre otros esquemas es la sencillez. Una red puede extenderse usando esta técnica sin que lo sepa el router de salida al exterior de la red.

Por ejemplo, supongamos que un host A quiere comunicarse con un host B de otra subred. Para ello, el host A enviará una solicitud ARP con la dirección IP de B en su paquete. El router que une ambas subredes responde a la petición de A con su dirección MAC en lugar de la dirección MAC auténtica de B, por lo tanto actúa como delegado del host B. A su debido tiempo, cuando A envíe al router un paquete que esté destinado en realidad a B, el router remitirá el paquete al host B. La comunicación entre A y B, se lleva a cabo sin que los hosts sepan que hay un router intermediario. Esto se debe a que el router responde con su propia dirección MAC a la petición ARP para una dirección IP, reemplazándola (proxying). A veces se denomina este proceso como "publicación" ("publishing").

Entre las desventajas del proxy ARP están la escalabilidad (de esta manera, la resolución ARP se necesita para cada dispositivo enrutado) y la fiabilidad (no está presente ningún mecanismo alternativo, y el enmascaramiento puede resultar confuso en algunos entornos). Nótese, sin embargo, que las técnicas de manipulación de ARP son la base de los protocolos que proveen redundancia en redes de difusión, como Ethernet, y más notablemente en el CARP y en el VRRP.

IETF standards documents (RFCs)

- RFC 826 - Ethernet Address Resolution Protocol, Internet Standard STD 37.
- RFC 903 - Reverse Address Resolution Protocol, Internet Standard STD 38.
- RFC 2390 - Inverse Address Resolution Protocol, draft standard
- RFC 5227 - IPv4 Address Conflict Detection, proposed standard