Tarea 14 y 15

PROTOCOLO ARP. Address Resolution Protocol

Claudio Acuña, Cristian Garrido, José Acuña, Guillermo Rojas, Leonardo Jofre.

January 8, 2014

¿Cómo opera?

ARP es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware, es decir la dirección MAC que corresponde a una determinada dirección IP.

Para ello se envía un paquete a la dirección de difusión de la red, es decir la dirección de broatcast(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 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 sólo funciona si todas las máquinas lo soportan.

Explique el Contexto de operación.

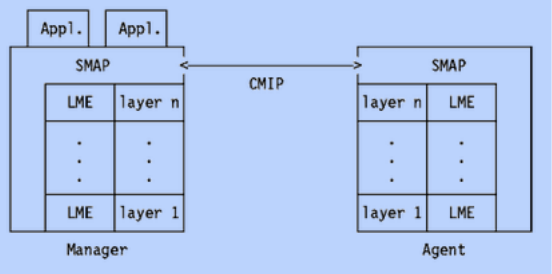
El protocolo ARP es el encargado de "traducir" las direcciones IP de 32 bits a las correspondientes direcciones de hardware, las cuales suelen tener 48 bits.. En una sola red, los hosts individuales se conocen a través de su dirección física, los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (en este caso la dirección IP), cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w,x,y,z, el manejador de dispositivo no la entiende, en consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a las dirección física del host de destino; esta utiliza una tabla (llamada a veces caché ARP) para realizar la traducción. Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red con un formato especial llamado petición de ARP, si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una respuesta a ARP al host que la solicitó, la cual contendrá la dirección física del hardware así como información de direccionamiento (si el paquete ha atravesado puentes durante su trayecto). Tanto esta dirección como la ruta se almacenan en la caché del host solicitante y todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el manejador de dispositivo para mandar el datagrama a la red.

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

- Dos host están en la misma red y uno quiere enviar un paquete a otro.
- Dos host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
- Un router necesita enviar un paquete a un host a través de otro router.
- Un router necesita enviar un paquete a un host de la misma red.

¿Cómo opera la conversión en la subida y en la bajada?

Generación de paquetes ARP Si una aplicación desea enviar datos a cierta dirección de destino IP, el mecanismo de enrutamiento IP primero determina la dirección IP del "próximo salto" del paquete (puede ser el propio host de destino, o un router) y el dispositivo hardware al cual se debería enviar. Si se trata de una red IEEE 802.3/4/5, el módulo ARP se debe consultar para hacer corresponder el <tipo de protocolo, la dirección del protocolo de destino> con una dirección física. El módulo ARP intenta encontrar la dirección en esta caché ARP. Si encuentra la pareja correspondiente, devuelve la correspondiente dirección física de 48 bits al que lo llamó (el driver del dispositivo) que entonces transmite el paquete. Si no encuentra la pareja en su tabla, descarta el paquete (assumption is that a higher-level protocol will retransmit) y generates a network broadcast of an ARP request.



donde:

espacio de direcciones hardware

Especifica el tipo de hardware; ejemplo de ello son Ethernet o Red de Radio por Paquetes.

espacio de direcciones del protocolo

Especifica el tipo de protocolo, igual que el campo EtherType en la cabecera IEEE 802 (IP o ARP).

longitud de direcciones hardware

Especifica la longitud (en bytes) de las direcciones hardware en este paquete. Para IEEE 802.3 y IEEE 802.5 será 6.

longitud de direcciones del protocolo

Especifica la longitud (en bytes) de las direcciones del protocolo en este paquete. Para IP será 4.

código de operación

Especifica si es una petición ARP (1) o una respuesta (2).

dirección hardware origen/destino

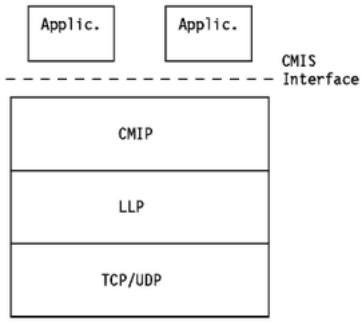
Contiene las direcciones hardware de red física. Para IEEE 802.3 son direcciones de 48 bits.

dirección del protocolo origen/destino

Contiene las direcciones del protocolo. Para TCP/IP son direcciones de IP de 32 bits. Para el paquete de petición ARP, la dirección hardware de destino es el único campo no definido en el paquete.

Recepción de paquetes ARP

Cuando un host recibe un paquete ARP (una petición de broadcast o una respuesta punto a punto), el driver del dispositivo receptor pasa el paquete al módulo ARP que lo trata como se muestra en la figura.



El host solicitante recibirá esta respuesta ARP y seguirá el mismo algoritmo para tratarlo. Como resultado de esto, se añadirá la tripleta <tipo de protocolo, dirección de protocolo, dirección hardware> para el host deseado a su tabla de búsqueda (cahé ARP). La próxima vez que una protocolo de más alto nivel quiera enviar un paquete a ese host, el módulo ARP encontrará la dirección hardware de destino y se enviará el paquete a ese host.

Explique en qué consiste el 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.

Explique por qué NAT.

Una dirección IPv4 consta de 32 bits. Esto hace que la cantidad de direcciones a usar sea bastante limitada (4,294,567,295 direcciones ip). Desde que se generalizó el uso de internet, su tamaño ha aumentado exponencialmente, por lo que sobre 1992 la IETF implementó algunos cambios para permitir que no se agotarán las direcciones. Estos fueron NAT y CIDR. Con el uso de NAT (o PAT) varios equipos de una misma localización, empresa o domicilio, comparten una única dirección ip pública. Hay que tener en cuenta que actualmente usamos televisiones, consolas, equipos portátiles, de sobremesa, teléfonos, etc que pueden conectarse a internet, por lo que los cuatro mil millones de direcciones representables con 32 bits de dirección (232) se están agotando. Actualmente ya se usan direcciones IPv6 que usan 128 bits para cada dirección de hosts. IPv6 proporciona aproximadamente 640 sextillones de direcciones.

Enumere la situación que requieren uso de IP.

1. Cualquier dispositivo que se conecte a una red cableada, como un computador
2. Cualquier dispositivo que se conecte a una red inalámbrica, como un un celular
3. Servidores

¿Por qué no IPV6 ahora EN CHILE?

IPv6 es la sexta versión de los protocolos IP, creado para resolver los problemas de infraestructura de Internet, asociados al inminente agotamiento del patrón actualmente vigente, provisto por el protocolo IPv4. Desarrollado de manera abierta y colaborativa a lo largo de 15 años, IPv6 mantiene como base los principios de IPv4, supliendo además las carencias presentadas por su antecesor. Su mayor diferencia estriba en una mayor capacidad de direccionamiento, que pasa de 32 a 128 bits, con lo que dispone de un enorme espacio de direcciones, en torno a los sextillones de números disponibles (340.282.366.920.938.000.000.000.000.000.000.000.000) que permite afirmar que toda necesidad actual y futura de direcciones estará asegurada.

La versión 6 del Protocolo de Internet, coexiste con el estándar IPv4 pero lo reemplazará en algunos años más, estimándose que dos terceras partes de las direcciones IPv4 ya se encuentran asignadas, en cambio, en el caso del IPv6 se maneja una cifra de 340 sextillones de direcciones disponibles, una cantidad prácticamente "ilimitada".

Asumimos que esta es la principal razón. Aún existen plazas disponibles. No obstante ya existen servidores ISP que ya tienen implementado ipv6 como VTR, y ciertas fundaciones como Universidades y GNU Chile.

¿Qué representa una dirección/16?

El «/16» significa que los primeros 16 dígitos binarios constituyen la dirección de red, o en otras palabras, «1.2.» es la parte de la red (recuerde: cada dígito representa 8 binarios). Esto significa que cualquier dirección IP que comience por «1.2» es parte de la red: «1.2.3.4» y «1.2.3.50» lo son, y «1.3.1.1» no.

Para hacer la vida más fácil, solemos usar redes que acaban en «/8», «/16» y «/24». Por ejemplo, «10.0.0.0/8» es una gran red que contiene las direcciones desde la 10.0.0.0 a la 10.255.255.255 (¡alrededor de 24 millones de direcciones!). 10.0.0.0/16 es más pequeña, y sólo contiene las direcciones IP de la 10.0.0.0 a la 10.0.255.255. 10.0.0.0/24 es aún más pequeña, y sólo contiene las direcciones 10.0.0.0 a 10.0.0.255.

Explique NAT.

NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

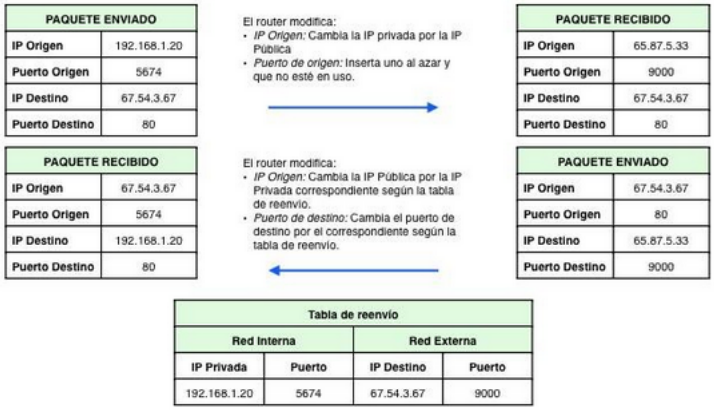
¿Cuáles son lo rangos de direcciones IP privadas?

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- Clase B: 172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Cuando la información vuelve sobre la dirección IP externa y es cambiada a la dirección IP interna, ¿cómo sabe a cuál máquina está asociada la respuesta?

La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública. Para poder hacer esto el router hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.



Explique brevemente las objeciones que se hacen a esta solución (NAT).

El propósito principal de IP - enmascaramiento NAT es que ha sido una solución práctica para el agotamiento inminente del espacio de direcciones IPv4 . Incluso las grandes redes se pueden conectar a Internet con tan poco como una única dirección IP .

El arreglo más común es tener máquinas que requieren conectividad de extremo a extremo se suministra con una dirección IP enrutable , al tiempo que las máquinas que no prestan servicios a usuarios fuera detrás de NAT con sólo unas pocas direcciones IP utilizadas para permitir el acceso a Internet , sin embargo, este trae algunos problemas, se describen a continuación .

Algunos también han llamado a esta función exacta de un gran inconveniente , ya que retrasa la necesidad de la implementación de IPv6 :

" Es posible que su uso generalizado [de NAT] retrasará significativamente la necesidad de desplegar IPv6. Es probablemente seguro decir que las redes estarían mejor sin NAT"

Ejércitos detrás de routers compatibles con NAT no tienen conectividad de extremo a extremo y no pueden participar en algunos protocolos de Internet. Los servicios que requieren el inicio de las conexiones TCP desde la red exterior, o protocolos sin estado como los que usan UDP, se pueden interrumpir . A menos que el router NAT hace un esfuerzo específico para apoyar este tipo de protocolos , los paquetes entrantes no pueden llegar a su destino . Algunos protocolos pueden acomodar a una instancia de NAT entre hosts participantes (FTP " modo pasivo " , por ejemplo) , a veces con la ayuda de una puerta de enlace de nivel de aplicación (ver más abajo) , pero fallan cuando ambos sistemas se separan de la Internet mediante NAT. El uso de NAT también complica protocolos de túnel , tales como IPsec porque NAT modifica los valores en los encabezados que interfieren con las comprobaciones de integridad realizado por IPsec y otros protocolos de túnel .

La conectividad de extremo a extremo ha sido un principio fundamental de la Internet , con el apoyo , por ejemplo, por la Junta de Arquitectura de Internet . Documentos

actuales de arquitectura de Internet señalan que NAT es una violación del principio de extremo a extremo , pero que NAT tiene un papel válido en el diseño cuidadoso. No es considerablemente más preocupación con el uso de NAT IPv6 , y muchos arquitectos IPv6 creen IPv6 fue diseñado para eliminar la necesidad de NAT .

Debido a la naturaleza efímera de las tablas de traducción con estado en los routers NAT , los dispositivos de la red interna pierden conectividad IP típicamente dentro de un período muy corto de tiempo, a menos que se implementen mecanismos de NAT keep-alive accediendo frecuencia hosts externos. Esto reduce drásticamente las reservas de energía en los dispositivos portátiles que funcionan con baterías y se ha frustrado un despliegue más generalizado de este tipo de dispositivos habilitados para Internet IP nativas. [Cita requerida]

Algunos proveedores de servicios de Internet (ISP), especialmente en la India , Rusia, partes de otras regiones "en desarrollo" Asia y ofrecer a sus clientes sólo con direcciones IP "locales" , debido a un número limitado de direcciones IP externas asignadas a dichas entidades [cita requerida] . Así, estos clientes deben acceder a los servicios externos a la red del ISP a través de NAT . Como resultado, los clientes no pueden lograr una verdadera conectividad de extremo a extremo , en violación de los principios básicos del Internet según lo indicado por el Consejo de Arquitectura de Internet.

Escalabilidad - Una implementación que sólo controla los puertos se puede agotar rápidamente las aplicaciones internas que utilizan múltiples conexiones simultáneas (por ejemplo, una solicitud HTTP para una página web con muchos objetos incrustados) . Este problema puede ser mitigado mediante el seguimiento de la dirección IP de destino , además del puerto (compartiendo así un solo puerto local con muchos hosts remotos) , a expensas de la complejidad de la implementación y los recursos de CPU / memoria del dispositivo de traducción.

Complejidad Firewall - Debido a que las direcciones internas están todos disfrazados detrás de una dirección de acceso público, es imposible para los servidores externos para iniciar una conexión a un host interno particular, sin necesidad de configuración especial en el firewall para reenviar conexiones a un puerto en particular. Las aplicaciones como VoIP, videoconferencia y otras aplicaciones peer -to-peer deben utilizar técnicas de NAT transversal para funcionar.

¿En qué se diferencian de los Routers?

Una pasarela, puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

En red de comunicaciones, un gateway es un nodo de la red equipado para hacer de interfaz con otra red que usa un protocolo diferente:

Como hardware, un gateway puede contener dispositivos como traductores de protocolos, dispositivos de adaptación de impedancias, conversores de ratio, aisladores de errores o traductores de señales, necesarios para proveer de interoperabilidad al sistema.

También es requerido un establecimiento de aceptación mutua entre ambas redes.

Como software, un protocolo gateway de traducción/mapeo que interconecte redes con diferentes protocolos de red, realizando las conversiones de protocolos requerida. Por extensión, una computadora gateway, es una computadora configurada para realizar tareas de un gateway.

El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

¿Qué pasa con la seguridad de los datos que van el túnel?

Se conoce como túnel al efecto de la utilización de ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

Túnel SSH

El protocolo SSH (secure shell) se utiliza con frecuencia para tunelizar tráfico confidencial sobre Internet de una manera segura. Por ejemplo, un servidor de ficheros puede compartir archivos usando el protocolo SMB (Server Message Block), cuyos datos no viajan cifrados. Esto permitiría que una tercera parte, que tuviera acceso a la conexión (algo posible si las comunicaciones se realizan en Internet) pudiera examinar a conciencia el contenido de cada fichero transmitido.

Para poder montar el sistema de archivo de forma segura, se establece una conexión mediante un túnel SSH que encamina todo el tráfico SMB al servidor de archivos dentro de una conexión cifrada SSH. Aunque el protocolo SMB sigue siendo inseguro, al viajar dentro de una conexión cifrada se impide el acceso al mismo. Por ejemplo, para conectar con un servidor web de forma segura, utilizando SSH, haríamos que el cliente web, en vez de conectarse al servidor directamente, se conecte a un cliente SSH. El cliente SSH se conectaría con el servidor tunelizado, el cual a su vez se conectaría con el servidor web final. Lo atractivo de este sistema es que hemos añadido una capa de cifrado sin necesidad de alterar ni el cliente ni el servidor web.