Instituto Politécnico Nacional

Escuela Superior de Cómputo

Unidad de Aprendizaje

Redes de Computadoras

Alumno

Alejandro Hernandez Gomez

Profesor

Moreno Cervantes Axel Ernesto

Practica ARP

**Protocolo de resolución de direcciones (ARP)**

ARP es un protocolo de comunicaciones de la capa de enlace, 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 de resolución de direcciones inverso (RARP) realiza, obviamente, 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.

**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).

**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.

**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.

**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.

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.

**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 enlace. 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.

**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.

**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.

**El código**

Basandonos en el código visto en clase, la parte con la que se trabajó es la siguiente

PcapPacketHandler<String> jpacketHandler = new PcapPacketHandler<String>() {

int i=0;

String ip;

Scanner leer = new Scanner(System.in);

public void nextPacket(PcapPacket packet, String user) {

if(i==0){

System.out.println("Ingresa la direccion ip");

ip = leer.nextLine();

System.out.println("IP a buscar: "+ip);

}

int operacion = (packet.getUByte(20)==0)?packet.getUByte(21):(packet.getUByte(20)\*256)+packet.getUByte(21);

String ipp="";

//System.out.println("Direccion IP: ");

for(int i=38;i<42;i++){

int a = packet.getUByte(i) &255;

if(i==41)

ipp += a;

else

ipp+=a+".";

//System.out.printf("%02X ",packet.getUByte(i));

//System.out.println(a);

}

System.out.println("ip a comparar: "+ipp+" y operacion: "+operacion);

//String operacion2 = Integer.toBinaryString(packet.getUByte(21));

//System.out.println("operwcion : "+operacion);

//int operacion = Integer.parseInt(operacion);

//&& ip.equals(ipp)

if(ip.equals(ipp) && operacion == 2){

System.out.printf("\nReceived packet at %s caplen=%-4d len=%-4d %s\n",

new Date(packet.getCaptureHeader().timestampInMillis()),

packet.getCaptureHeader().caplen(), // Length actually captured

packet.getCaptureHeader().wirelen(), // Original length

user // User supplied object

);

System.out.println("ip a comparar: "+ipp);

System.out.println("numero: "+i);

//if(packet.getUByte(21))

/\*\*\*\*\*\*Desencapsulado\*\*\*\*\*\*\*\*/

System.out.println("MAC destino:");

for(int i=0;i<6;i++){

System.out.printf("%02X ",packet.getUByte(i));

}

System.out.println("");

System.out.println("MAC origen:");

for(int i=6;i<12;i++){

System.out.printf("%02X ",packet.getUByte(i));

}

System.out.println("");

System.out.println("Tipo:");

for(int i=12;i<14;i++){

System.out.printf("%02X ",packet.getUByte(i));

}

int tipo = (packet.getUByte(12)==0)?packet.getUByte(13):(packet.getUByte(12)\*256)+packet.getUByte(13);

System.out.printf("Tipo= %d",tipo);

System.out.println("");

/\*System.out.println("Direccion IP: ");

for(int i=38;i<42;i++){

int a = packet.getUByte(i) &255;

//System.out.printf("%02X ",packet.getUByte(i));

System.out.println(a);

}

System.out.println("\n\n");\*/

//String operacion1 = Integer.toBinaryString(packet.getUByte(20));

//String operacion2 = Integer.toBinaryString(packet.getUByte(21));

for(int i=0;i<packet.size();i++){

System.out.printf("%02X ",packet.getUByte(i));

if(i%16==15)

System.out.println("");

}

//System.out.println("\n\nEncabezado: "+ packet.toHexdump());

System.out.println("\n\n");

}

i++;

}

};

pcap.loop(200, jpacketHandler, "");

al encontrar coincidencia con la ip y el número de operación (2) el programa realiza la impresión en consola de la información que es de nuestro interés:

Received packet at Wed Dec 14 02:44:03 CST 2016 caplen=42 len=42

ip a comparar: 192.168.15.4

numero: 23

MAC destino:

48 5A B6 0E 08 71

MAC origen:

52 02 71 62 36 E7

Tipo:

08 06 Tipo= 2054

48 5A B6 0E 08 71 52 02 71 62 36 E7 08 06 00 01

08 00 06 04 00 02 52 02 71 62 36 E7 C0 A8 0F 01

48 5A B6 0E 08 71 C0 A8 0F 04