UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN
Redes II Ciclo I 2018
Ing. Manuel Flores Villatoro

Actividad Protocolo ARP

Índice de contenido

Índice de ilustraciones

El material

Los materiales que se necesitarán para el laboratorio son:

- Dos o mas computadoras
- 1 switch
- Tener wireshark, tcpdump, arping instalado.

Los Equipos

Los equipos de laboratorio con los que deberá contar serán:

- Una computadora con Debian GNU/Linux o Ubuntu.
- Una o mas computadoras con cualquier Sistema operativo para configurarle una IP dinámica.

La práctica de laboratorio consistirá en manipular las tablas ARP de una computadora para poder entender su funcionamiento.

Se crearán grupos de trabajo de **dos** personas **máximo**, los cuales deberán tener los materiales y equipos antes mencionado.

La calificación del laboratorio se basará en:

1. 50% funcionamiento del ARP con Debian (Capturas de pantalla de todo lo realizado).
2. 50% las respuestas del cuestionario al final del documento.

Teoría

Protocolo ARP

ARP (del inglés ***A**ddress **R**esolution **P**rotocol* o, en español, *Protocolo de resolución de direcciones*) es un protocolo de la capa de enlace de datos responsable de **encontrar la dirección 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

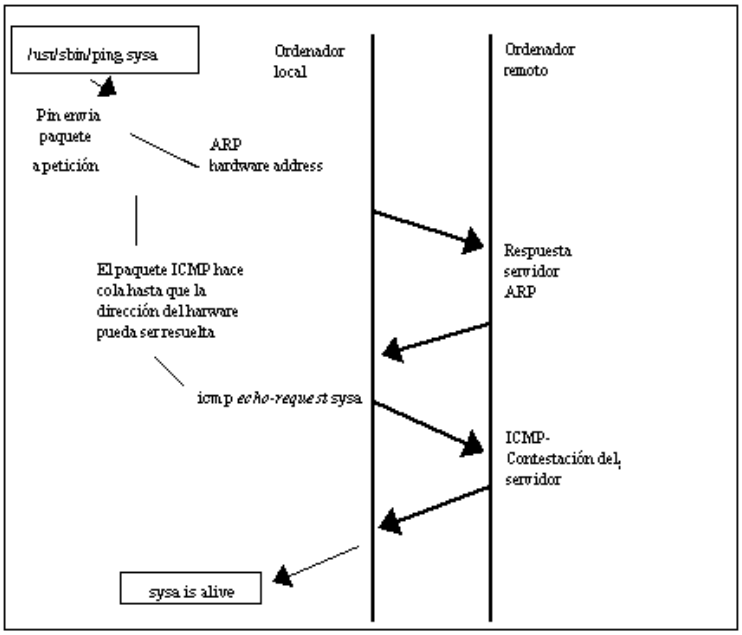

Ilustración 1: Mensajes ARP

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.

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 4 casos referentes a la comunicación entre 2 hosts:

1. Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
2. Cuando 2 host están sobre redes diferentes y deben usar un gateway/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

La filosofía es la misma que tendríamos para localizar al señor "X" entre 150 personas: preguntar por su nombre a todo el mundo, y el señor "X" nos responderá. Así, 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 (Ej: si se estropea una tarjeta de red y hay que sustituirla, o simplemente algún usuario de la red cambia de dirección IP).

Funcionamiento de ARP

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.

Una vez en el router, éste 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.

Diagrama de Red del Laboratorio

El diagrama de red a implementar en el laboratorio es el siguiente:

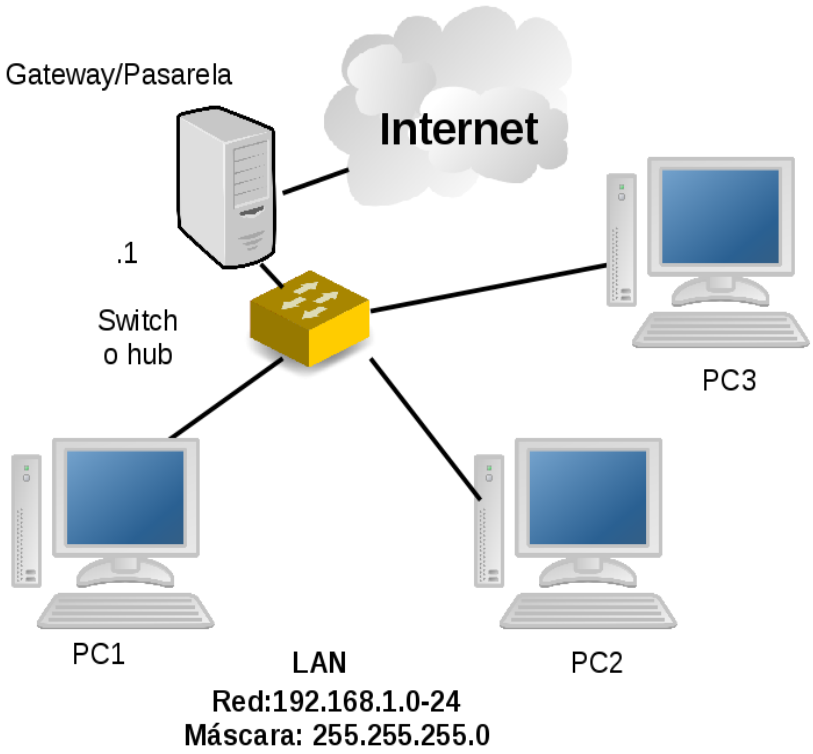

Ilustración 2: Diagrama de red

Nota: Para los ejemplos de comandos se utilizará la red 192.168.99.0/24 que puede no coincidir con la red que usando de local. El documento deberá contener la descripción de las redes usadas, direcciones MAC de cada uno de los hosts y capturas de pantallas de los pasos realizados con su descripción así como respuestas del cuestionario.

Manipulación de tablas ARP

Instalación

Antes de armar la red y de realizar cualquier cambio, deberemos instalar los programas necesarios para el laboratorio.

Los programas que se instalarán serán wireshark (examinador de paquetes), arping (ping sobre arp) y tcpdump (examinador de paquetes en shell). Para instalarlo en un debian, se debe hacer:

```
// Instalación del wireshar, tcpdump y arping
      aptitude install wireshark tcpdump arping
```

Verificación de la tabla

Para verificar la tabla caché de ARP ejecutamos el siguiente comando como root:

```
arp -a
```

El cual nos mostrará algo como:

```
? (192.168.99.228) at 08:00:27:19:a5:b5 [ether] on eth0
? (192.168.99.237) at f0:4d:a2:dc:34:2e [ether] on eth0
? (192.168.99.156) at a4:ba:db:fe:ef:5e [ether] on eth0
```

Ejercicio #1 tabla ARP

Verificar la conexión con otra computadora dentro de la red que no este listada en la tabla caché ARP. Luego verificar la tabla ARP verificando que se ha agregado el registro. ¿Cuales son las direcciones que agrego?

Después de haber terminado el ejercicio, seguir con lo siguiente. No olvidarse de realizar **capturas de pantalla.**

En caso de necesitar borrar un registro de nuestra tabla arp, podemos hacerlo con el comando

```
arp -d 192.168.99.20
```

En este caso borra un registro de la tabla que coincide con la dirección IP 192.168.99.20.

Mensajes ARP

Los mensaje ARP son enviados antes de realizar cualquier comunicación dentro de la red LAN. Así que cuando se comienza una comunicación con una computadora dentro de la red, si no esta en la tabla ARP, ésta se agrega. Ahora verificaremos cuales son estos mensajes. Para ver los mensajes podemos usar dos herramientas examinadoras de paquetes:

1. **tcpdump** en modo consola
2. **wireshark** en modo gráfico

El ejemplo que se seguirá será en modo consola, aunque se recomienda tambien utilizar el modo gráfico.

Pasos:

Verificamos nuestra tabla ARP

```
arp -a
```

Asumiendo que nuestra interfaz de red es la eth0 , en otra consola ejecutamos como usuario root :

```
tcpdump  -n -i eth0
ó
tcpdump  -n -i eth0 | grep ARP
```

Después aparecerán todos los mensajes que pasan por nuestra interfaz. El segundo comando filtra los mensajes para mostrar solo los datos del protocolo ARP.

Los mensajes seran parecidos a:

```
18:34:37.677044 ARP, Request who-has 192.168.99.238 tell 192.168.99.228,
length 28
18:34:37.677423 ARP, Reply 192.168.99.238 is-at 00:0e:08:d6:0a:4b,
length 46
18:32:23.647373 IP 192.168.99.228 > 192.168.99.238: ICMP echo request,
id 16663, seq 1, length 64
18:32:23.647823 IP 192.168.99.238 > 192.168.99.228: ICMP echo reply, id
16663, seq 1, length 64
```

La información que no muestra es: fecha y hora, protocolo, mensaje del protocolo.

Ejercicio #2 Mensajes ARP

Verificar la conexión con otra computadora dentro de la red que no este listada en la tabla caché ARP. Registrar los mensajes ARP que entra y salen de la computadora con tcpdump. ¿Cuales son los tipos de mensajes ARP que envía y recibe?

Después de haber terminado el ejercicio, seguir con lo siguiente. No olvidarse de realizar **capturas de pantalla.**

Pueden verificar los mensajes con wireshark ejecutando desde la consola como usuario normal:

Darle permisos a todos los usuarios para puedan ejecutar una aplicaciones gráficas.

```
xhost +
```

Ingresar como root

```
su
```

Abrir wireshark

```
wireshark
```

Ejecutar en el menú (asumiendo que nuestra interfaz es la eth0) *capture->interfaces->eth0*

IPs Duplicadas

Uno de los casos mas comunes en que es útil el conocimiento del funcionamiento del protocolo ARP es cuando se tiene una IP duplicada en la red. En este caso utilizaremos una aplicación (arping) que envia solicitudes de ARP y leer las respuestas.

Pasos:

En la segunda computadora deberán asignar la misma IP que la PC1

Antes de la duplicación de la IP verificar el resultado del comando con arping, ejemplo:

```
arping 192.168.99.238
```

Lo cual mostrará un resultado como

```
60 bytes from 00:0e:08:d6:0a:4b (192.168.99.238): index=0 time=356.749
usec
60 bytes from 00:0e:08:d6:0a:4b (192.168.99.238): index=1 time=624.381
usec
```

Luego duplicar la IP y verificar los resultados.

Ejercicio #3 IP Duplicada

Contestar ¿Cuales son los mensajes que se muestran? ¿Que significa?

Después de haber terminado el ejercicio, seguir con lo siguiente. No olvidarse de realizar **capturas de pantalla.**

Acceso a Internet

Verifique las tablas ARP cuando accede hacia algún recurso en Internet.

Ejercicio #4 Tabla ARP a Internet

Verificar los mensajes que se reciben al realizar alguna comunicación hacia:

8.8.8.8 y 168.232.49.178 .

Deberá mostrar la tabla ARP de la computadora y el comando arping. Luego contestar las siguiente preguntas: ¿Qué sucedió? ¿Por qué muestra esos mensajes? Explicar.

No olvidarse de realizar **capturas de pantalla.**

Referencias:

- **http://es.wikipedia.org/wiki/Address_Resolution_Protocol**
- **http://en.wikipedia.org/wiki/Address_Resolution_Protocol**
- **http://linuxgnublog.org/envenamiento-de-las-tablas-arp-arp-spoofing/**
- http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html
- **http://blog.desdelinux.net/como-cambiar-tu-mac-address-en-linux/**
- **http://www.portalhacker.net/b2/como-evitar-ataques-envenenamiento-arp-by-fnix/70466/**
- **http://www.maestrosdelweb.com/editorial/sniffers/**
- **http://wiki.wireshark.org/Gratuitous_ARP**

UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN
Redes II Ciclo I 2018
Ing. Manuel Flores Villatoro

Actividad Protocolo ARP

Integrantes: _____ Carnet:_____
_____ Carnet:_____

Resumen de Preguntas .

1. Ejercicio #1 Tabla ARP (25%)

   ¿Cuales son las direcciones que agrego?

   MAC:_____ IP:_____

2. Ejercicio #2 Mensajes ARP (25%)

   ¿Cuales son los tipos de mensajes ARP que envía y recibe?

   _____

   _____

   _____

3. Ejercicio #3 IP Duplicada (25%)

   ¿Cuales son los mensajes que se muestran?

   _____

   _____

   _____

   _____

   ¿Que significa?_____

   _____

   _____

   _____

4. Ejercicio #3 Tabla ARP a Internet (25%)

   ¿Qué sucedió? _____

   _____

   _____

   _____

   ¿Por qué no muestra la dirección MAC de 8.8.8.8 y de 168.232.49.155 ?

   _____