Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# Práctica 5 – Análisis de tramas Ethernet. ARP

## 1- Objetivos

Análisis de tramas Ethernet correspondientes a protocolos de nivel de red; ICMP, IP y nivel de enlace; ARP.

## 2- Avisos generales

En esta práctica hará uso de la cuenta de nombre `arss` y password `telemat` en los PCs A, B y C.

Los ficheros creados o modificados durante una sesión de prácticas serán borrados diariamente de forma automática. Si quieren conservar cualquier fichero entre sesiones guárdenlo en un pendrive.

## 3- ARP (Address Resolution Protocol)

En este apartado vamos a estudiar las características de ARP, protocolo de nivel de enlace. Recuerde que el protocolo ARP es el mecanismo que utiliza el nivel de red para determinar la dirección hardware de un determinado interfaz, y viceversa. Como, dada la configuración de las redes actuales, Ethernet e IP son los protocolos más extendidos, ARP, principalmente se encarga de la traducción de direcciones IP a EthernetMAC y viceversa. Para ello mantiene en cada equipo una tabla/caché de pares IP-MAC. En Linux, el comando `arp` nos permite visualizar y manipular el contenido de dicha tabla, pero no hay que confundir ARP con `arp`; son cosas totalmente diferentes, ya que `arp` es un COMANDO que nos permite visualizar y manipular el contenido de la tabla ARP, y ARP es un PROTOCOLO que define el formato y significado de los mensajes enviados y recibidos, y qué acciones han de tomarse en la transmisión y recepción de dichos mensajes.

Vamos a ver qué hay en la tabla ARP de nuestro ordenador:

- ✓ Abrimos una consola de comandos en PCA.
- ✓ Tecleamos `arp -n -a` (consulte el manual `man arp`)

¿Qué observa? ¿Por qué está vacía? ¿Cómo puede ver las interfaces que están activas?

Lo primero que haremos será activar y configurar una de las cuatro interfaces de red de las que dispone PCA.

Conecte una de las tarjetas Ethernet de PCA(por ejemplo: `eth0`) al punto C de su mesa. Este punto le lleva a la red del laboratorio. *Para efectuar dicha conexión utilice uno de los puntos del panel de parcheo R9-R12 (consulte la documentación de los armarios).*

Asigne una dirección ip y una máscara de red a dicha tarjeta de red:

```
sudo ifconfig eth0 10.3.17.armario netmask 255.255.240.0
```

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Añada una puerta de enlace a la tabla de rutas del kernel de linux:

```
sudo route add default gw 10.3.16.1
```

Abra un navegador y compruebe que tiene conexión a Internet. Probablemente necesite configurar su servidor de nombres de dominio (DNS). Para ello añadan la siguiente línea en el archivo `/etc/resolv.conf` que estará vacío (verifíquelo con un `cat /etc/resolv.conf`)

```
echo nameserver 10.1.1.253 > /etc/resolv.conf
```

Ahora debería poder acceder a Internet sin problemas.

Vuelva a teclear el comando `arp` ¿Qué diferencias encuentra? Anote el contenido de la tabla ARP de tu ordenador. ¿Cuál es el significado de los valores de cada columna?

A continuación vamos a observar una típica secuencia de mensajes ARP; para ello borramos la tabla ARP del ordenador, y así le forzamos a enviar una petición ARP.

- ✓ Desde una consola de comandos tecleamos (como supersusuario) `arp -d *` (-d para darle la orden delete y * para indicarle que ha de ejecutar la orden con todas las entradas de la tabla). Es posible que necesite indicarle específicamente la entrada que desea borrar de la tabla arp, consulte para ello el manual del comando `arp` (`man arp`).

Una vez vacía la tabla ARP:

- ✓ Vaciamos la caché de nuestro navegador.
- ✓ Iniciamos Wireshark y comenzamos la captura.

Descargamos la página: http://www.faqs.org/rfcs/rfc826.html (RFC 826 - RFC de arp)

- ✓ Detenemos la captura.
- ✓ Pinchamos en Analyze > Enabled Protocols. Verifique que todos están seleccionados.
- ✓ Pulsamos OK.

¿Cuáles son los valores hexadecimales de las direcciones fuente y destino en la trama Ethernet que contiene el mensaje ARP Request? ¿Qué indican?

Checkpoint 5.1: Muestre al profesor de prácticas el valor hexadecimal del campo que ha permitido al analizador determinar el tipo de trama Ethernet capturada. Considerando dicha trama, ¿En qué nivel de la pila de protocolos diría que se encuentra ARP? Justifíquelo.

### 3.1- Escenario 1

Este primer escenario constará de tres ordenadores conectados a través del hub cuyos puertos se encuentran parcheados en el panel de parcheo de su armario (*consulte la documentación de los armarios*). Además deberá configurar una tarjeta de red Ethernet en cada equipo.

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Asignen una dirección ip a cada uno de los PCs A, B y C dentro de la red 10.3.armario.0/24.

Para comprobar el funcionamiento de ARP deberemos borrar antes la caché de arp de cada PC.

Lance un ping entre PCA y PCB. Para capturar los paquetes intercambiados entre ambos ordenadores utilice `tcpdump` en cada uno de los PCs, de tal manera que un terminal se esté permanentemente capturando sólo tramas `arp`, mientras que en un segundo terminal se realiza el envío de paquetes ICMP entre PCs.

Simultáneamente en PC C lance wireshark y capture sólo mensajes ICMP y ARP.

Observe las entradas de las tablas `arp` en los PCs A y B y analice lo que está pasando. ¿Se corresponde la captura con `tcpdump` en los PCs A y B con la realizada en PCC mediante `wireshark`, ¿Por qué?

Lance ahora un ping de PCB a PCA ¿Ha cambiado algo en las tablas `arp` de ambos PCs?¿Por qué?

Detenga ahora los `pings` y modifique la dirección ip de PCA asignándole una nueva, pero dentro del espacio de direcciones 10.3.armario.0/24. Vuelva a lanzar un ping entre PCA y PCB. Compruebe nuevamente las caches `arp` de ambos PCs, ¿Qué ha ocurrido?

¿Qué ocurriría si en lugar de cambiar la dirección ip de PCA le cambiase la dirección MAC a su tarjeta de red y a continuación lanzara un ping entre PCA y PCB? Compruébelo con:

```
sudo ifconfig eth0 down hw ether 00:11:22:33:44:55
```

Verifique siempre cualquier cambio que realice. Para este caso basta con un simple:

```
ifconfig eth0
```

Checkpoint 5.2: Muestre al profesor de prácticas el mecanismo de ARP apoyándose en las capturas realizadas.

Detenga el ping y las capturas de tcpdump y wireshark y pase al escenario 2.

### 3.2- Escenario 2

Conecte ahora los PCA, PCB y PCC a través de un switch, utilice el switch0 de su armario(*consulte la documentación de los armarios*). Mantenga la configuración ip de los tres PCs y borre la caché `arp` de éstos.

Abra `wireshark` en todos los ordenadores y haga un ping de PCA a PCB. ¿Qué es lo que ocurre?

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Checkpoint 5.3: Muestre al profesor de prácticas qué es lo que ha cambiado respecto del escenario 1 y justifíquelo.

A la vista de los resultados obtenidos debería ser capaz de responder a preguntas del tipo:

1. Nuestro PC, con IP 150.214.142.100 y máscara de red 255.255.255.0, tiene la caché ARP vacía. De repente generamos varios paquetes IP destinados a los equipos 150.214.144.250, 150.214.143.250, 150.214.142.250 ¿Cuántas peticiones ARP hemos tenido que realizar?
2. ¿Es necesario que las peticiones ARP sean transportadas en una trama con destino BROADCAST?
3. ¿Se le ocurre algún motivo para enviar una petición ARP dentro de una trama con destino UNICAST? ¿De qué tipo son las respuestas ARP? ¿Por qué?
4. ¿Qué tiempo de vida tienen las entradas en la caché ARP?
5. ¿Cada cuánto tiempo se actualiza la caché ARP? ¿Sería capaz de demostrarlo con una captura?

Checkpoint 5.4: Capturen un caso de petición ARP UNICAST e indique a qué se debe.