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 ICMP, IP y ARP.

2- Login

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

3- ARP (Address Resolution Protocol)

Con el predominio de Ethernet e IP en las redes actuales, ARP, principalmente se encarga de la traducción de direcciones IP a Ethernet-MAC 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.

A continuación comprobará el contenido de la tabla ARP de su ordenador. Además como ejercicio de repaso, inspeccionará la tabla de rutas del mismo:

Nota: antes de hacer nada,reinicien su PCA para conseguir una configuración limpia del mismo.

- Abra una consola de comandos.
- Teclee `arp`. ¿Qué observa? ¿Por qué está vacía?
- ¿Cómo puede ver las interfaces Ethernet que están activas? ¿Y la tabla de rutas de PCA? Ejecute los comandos:

```
$ ifconfig

$ route -n
```

Lo primero que hará 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
```

Compruebe ahora la tabla de rutas de PCA ¿Qué ha cambiado?

Añada una puerta de enlace por defecto a la tabla de rutas del kernel de linux(PCA):

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

Vuelva a comprobar la tabla de rutas de PCA e identifique la ruta estática que acaba de añadir. ¿Cuál es la red destino a la que podemos acceder mediante la puerta de enlace `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 10.1.1.193 > /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 teclee (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:

- Vacíe la caché de su navegador.
- Inicie Wireshark y comience la captura.

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

- Detenga la captura.
- Pinche en Analyze > Enabled Protocols. Verifique que todos están seleccionados.
- Pulse 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.

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

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.

Para asegurarse una configuración limpia en sus equipos, reinicie los tres PCs A, B y C.

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.

Ponga wireshark a capturar tramas Ethernet en sus tres PCs. Capture sólo mensajes ICMP y ARP.

Lance un ping entre PCA y PCB.

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

Haga 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?

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

¿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`

¿Qué ha ocurrido al cambiar la MAC? Necesitará activar la interfaz: `sudo ifconfig eth0 up`

Detenga el ping y las capturas de 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 todos ellos. Ponga wireshark a capturar tramas en sus tres PCs y haga un ping de PCA a PCB. ¿Qué es lo que ocurre?

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

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

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? Seguro que ha visto este tipo de tramas en alguna de sus capturas.
4. ¿Diría que las respuestas ARP son de tipo BROADCAST? ¿Por qué?

Checkpoint 5.4: Utilizando uno de los mensajes ARP request o ARP reply, capturados mediante wireshark, complete en notación hexadecimal el siguiente formato de trama ARP:

0 8 16 24 31 bits

Hardware type		Protocol type
HardSize	ProtSize	Operation
Sender Ether (octects 0-3)		
Sender Ether (4-5)		Sender IP (0-1)
Sender IP (2-3)		Target Ether (0-1)
Target Ether (octects 2-5)		
Target IP (octects 0-3)		

0 8 16 24 31 bits
