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

Práctica2 - Analizadores de red: Ethereal y tcpdump. ARP

1- Objetivos

Comprender los conceptos básicos del monitoreo de tráfico de red mediante el uso del analizador de protocolos Ethereal y del sniffer tcpdump.

Análisis de tramas Ethernet correspondientes a protocolos de nivel de transporte; TCP y de nivel de red; 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)

En este apartado vamos a estudiar las características de ARP, protocolo de nivel de red. 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`.

¿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 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 está conectado a la red del laboratorio. Para efectuar dicha conexión utilice uno de los puntos del panel de parcheo R9-R13 (*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
```

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

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

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

Abra un navegador y compruebe que tiene conexión a Internet. Vuelva a teclear el comando `arp` ¿Qué diferencias encuentra ahora? Anote el contenido de la tabla ARP de tu ordenador. ¿Cuál es el significado de los valores de cada columna?

A continuación vamos a analizar 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 Ethereal y comenzamos la captura.
- Descargamos la página: http://www.faqs.org/rfcs/rfc826.html (RFC 826 - RFC de ARP)
- Detenemos la captura.

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

Checkpoint 2.4: 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 (*consulte la documentación de los armarios*). Además deberá configurar una tarjeta de red Ethernet en cada equipo.

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 `ethereal` y capture sólo mensajes ICMP y ARP.

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

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 `ethereal`, ¿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 siempre 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 2.5: Muestre al profesor de prácticas el resultado obtenido y explique el mecanismo de ARP apoyándose en las capturas realizadas.

Detenga el `ping` y las capturas de `tcpdump` y `ethereal` 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*). Mantenemos la configuración ip de los tres PCs y borramos la caché ARP de éstos.

Abra `ethereal` en todos los ordenadores y haga un `ping` de PCA a PCB.

¿Qué es lo que ocurre?

Checkpoint 2.6: 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. ¿Se le ocurre alguna utilidad al hecho de que un ordenador, al arrancar, genere una petición ARP en la que el campo “TARGET PROTOCOL ADDRESS” tenga el valor de la IP de ese ordenador?
5. Imagine que usamos el comando “`arp -s`” en nuestro PC para añadir a la caché ARP todas las entradas correspondientes a todos los equipos con los que podemos intercambiar tramas Ethernet directamente. ¿Evitaría esto que nuestro equipo generase tráfico ARP?

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 2.7: Utilizando uno de los mensajes ARP request o ARP reply, capturados mediante ethereal, complete en *notación hexadecimal* el formato de trama ARP:

0 8 16 24 31

Hardware type		Protocol type
Hlen	Plen	Operation
Sender HA (octects 0-3)		
Sender HA (4-5)		Sender IP (0-1)
Sender IP (2-3)		Target HA (0-1)
Target HA (octects 2-5)		
Target IP (octects 0-3)		

0 8 16 24 31
