ARQUITECTURA DE REDES
1º Ingeniería Informática

Práctica 5

Analizador de protocolos Ethereal/Wireshark

Objetivo

Estudiar los formatos de trama y algunos de los distintos protocolos estudiados en la asignatura a través de una herramienta de análisis de protocolos.

Material

Para la realización de la presente práctica se utilizará el software Ethereal, disponible para su descarga en Moodle. Alternativamente, se puede emplear su versión más actual bajo el nombre WireShark. Asimismo, las distintas capturas de tramas con las que se realizará la práctica se encuentran en el fichero `Capturas.zip`, también disponible en Moodle.

Ejercicio 1

Abrir el fichero `Spanning_tree.cap`. Cada línea representa una trama capturada. Al seleccionar una trama pueden verse los campos que la componen en la zona inferior de la pantalla.

Responder las siguientes preguntas relativas a la trama 1:

a) ¿Qué protocolo se emplea en la subcapa MAC? ¿Cuál es el formato de trama? ETHERNET II

b) Anotar las direcciones origen y destino. ¿Qué diferencias se observan entre ellas?
Primeros y segundos 12 bytes. Destino es broadcast y la otra es conocida (origen)

c) ¿Cuál es el fabricante de la tarjeta de origen? Localizar otra trama con el mismo fabricante, pero distinta dirección MAC.
CISCO. En la trama 6, por ejemplo

d) ¿Qué indica el campo Type? ¿Y el campo Trailer/Padding?
Protocolo capa red . Relleno + codificación de errores.

Responder las siguientes preguntas relativas a la trama 3:

a) ¿Qué valor tiene ahora el campo Type?
IPv4

b) ¿Por qué no aparece el campo Trailer/Padding en esta trama?
Trama completa sin relleno

Responder las siguientes preguntas relativas a la trama 6:

a) ¿Qué protocolo se emplea en la subcapa MAC? ¿Cuál es el formato de trama? ¿Qué diferencias se observan con el formato de la trama 1?
IEE 802.3. Destino, Origen, Tamaño y padding . No se manda por la capa red, si no directamente por MAC.

Ejercicio 2

Abrir el fichero `Captura_LLC.cap`. Responder a las siguientes preguntas:

a) Observar la trama 1. ¿Qué direcciones se identifican en la cabecera 802.11?
Destino Broadcast y origen conocido

b) Observar los flags de la cabecera. ¿Van encriptados los datos?
Si, tiene la Protected Flag

c) En la trama 5, dentro del campo de control de LLC, ¿qué indican los campos N(S), N(R) y Frame type?
Numero ventana sender y numero ventana receiver, frame type indica ventana deslizante

Práctica 5

Analizador de protocolos Ethereal/Wireshark

Ejercicio 3

Abrir el fichero `Descarga_google.cap`. Responder a las siguientes preguntas:

a) En relación a las tramas 1 y 5:

```
Source Address: 192.168.1.34
Destination Address: 80.58.61.250
```

```
Source Address: 192.168.1.34
Destination Address: 64.233.183.104
```

a.1) Clasificar las distintas direcciones IP origen y destino.

a.2) Observar en la trama 1 las direcciones de destino en la subcapa MAC y en la capa IP. ¿Identifican a la misma máquina?

b) Representar las pilas de protocolos que generan, respectivamente, las tramas 4 y 14.

Ethernet II -> IPv4 -> UDP -> DNS

Ethernet II -> IPv4 -> TCP -> HTTP

Ejercicio 4

Abrir el fichero `Captura_arp.cap`. Responder a las siguientes preguntas sobre el protocolo ARP:

a) ¿Qué estación realiza la solicitud? ¿A quién dirige dicha solicitud?

```
Sender MAC address: Intel_13:54:a7 (00:a0:c9:13:54:a7)
Sender IP address: 192.168.1.55
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.69
```

b) ¿Quién se encarga de dar respuesta a la anterior solicitud?

```
Sender MAC address: BellTechnolo_00:4a:ae (00:00:1c:00:4a:ae)
Sender IP address: 192.168.1.69
Target MAC address: Intel_13:54:a7 (00:a0:c9:13:54:a7)
Target IP address: 192.168.1.55
```

Ejercicio 5

Responder a las siguientes preguntas sobre el protocolo ICMP:

a) ¿Quién realiza la solicitud y quién da la respuesta en `Captura_ping.cap`?

b) ¿Qué ocurre si el destino no es alcanzable? Compruébese en `Captura_ping2.cap`.

```
Source Address: 192.168.1.34
Destination Address: 192.168.1.1
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.34	150.214.112.100	ICMP	74	Echo (ping) request id=0x0200, seq=2304/9, ttl=128 (no response found!)
2	5.356884	192.168.1.34	150.214.112.100	ICMP	74	Echo (ping) request id=0x0200, seq=2560/10, ttl=128 (no response found!)
3	10.364089	192.168.1.34	150.214.112.100	ICMP	74	Echo (ping) request id=0x0200, seq=2816/11, ttl=128 (no response found!)
4	15.371285	192.168.1.34	150.214.112.100	ICMP	74	Echo (ping) request id=0x0200, seq=3072/12, ttl=128 (no response found!)