

CDAR - PRACTICO III

Aplicaciones – Segunda Parte

- 1- Considere el siguiente texto de caracteres ASCII generados cuando un browser envía un mensaje HTTP GET y explique el significado de los distintos parámetros. Los caracteres <cr><lf> representan el salto de línea en el comando

```
GET /cs453/index.html HTTP/1.1<cr><lf>
Host: gaia.cs.umass.edu<cr><lf>
User-Agent: Mozilla/5.0 (U; Windows NT 5.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax) <cr><lf>
Accept:ext/xml,application/xml,application/xhtml+xml;q=0.9, text/plain ;q=0.8,image/png,*/*;q=0.5 <cr><lf>
Accept-Language: en-us,en;q=0.5<cr><lf>
Accept-Encoding: zip,deflate<cr><lf>
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7<cr><lf>
Keep-Alive: 300<cr><lf>
Connection:keep-alive<cr><lf>
<cr><lf>
```

- 2- DNS en Wireshark

En la captura *dns-ethereal-trace-1* Examine el mensaje de consulta DNS en el paquete DNS enviado por el cliente.

- a. ¿Qué campo indica si el mensaje es una consulta o una respuesta?
- b. ¿Qué información lleva en el cuerpo de la consulta?
- c. ¿Cuál es el ID de la transacción consulta?
- d. Identificar los campos que llevan el tipo y clase de la consulta.

• Consideremos ahora el paquete que transporta la respuesta DNS a la consulta anterior.

- e. ¿Cuál debe ser la de Ethernet y las direcciones IP para este paquete? Comprueba si estas direcciones son como se esperaba.
- f. ¿Cuál es el tamaño del paquete IP y UDP que llevan la respuesta? ¿Es más largo que la consulta?
- g. Compruebe que el ID de transacción en el mensaje de respuesta es correcto.
- h. ¿Cuántas respuestas están dentro del mensaje de respuesta? Comparar la respuestas y sus valores de TTL.

En la captura *dns-ethereal-trace-4*

- i. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es esta la dirección IP de un servidor DNS local por defecto? Si no es así, ¿a qué corresponde esa dirección IP?
- j. Examine el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es? ¿El mensaje de consulta contiene algunas "respuestas"?
- k. Examine el mensaje de respuesta de DNS. ¿Cuántas "respuestas" se proveen? ¿Qué contiene cada una de estas respuestas?

- 3- Considerando la red del ejercicio 2 de la primera parte del práctico y que el equipo en el cual reside el web cache también tienen un servidor DNS Responda:

- a. Que tiempo se debe considerar si se tiene una consulta típica a un DNS de manera iterativa.
- b. Que tiempo se debe considerar si se tiene una consulta típica a un DNS de manera recursiva.
- c. Cambian estos tiempos si se hacen dos consultas iguales consecutivas. Justifique.
- d. Realice un ejemplo de los mensajes generados en el inciso a) especificando los campos más importantes.