Análisis de tráfico con Wireshark

Álvaro González Sotillo

4 de octubre de 2021

Índice

1. Objetivos de la práctica

En esta práctica se espera que el alumno se familiarice con:

- La encapsulación de los protocolos de nivel n en los protocolos $n-1$.
- Utilización de la herramienta **Wireshark**, incluidos sus filtros.
- Búsqueda autónoma de información en Internet.
- La correspondencia entre los niveles ISO/OSI y los protocolos de una red real.

La última versión de este documento está disponible en el aula virtual.

2. Tramas de *broadcast*

Las tramas de *broadcast* son las que tienen la dirección del nivel de enlace `FF:FF:FF:FF:FF:FF`.

- Monitoriza la red durante uno o dos minutos y determina qué tramas de las recibidas son de *broadcast*.
- Haz una lista de las pilas de protocolos (desde nivel de enlace hasta nivel de aplicación) que viajan sobre tramas de *broadcast*, e incluye al menos 3 pantallazos de estas pilas como ejemplo.
- ¿Para qué se utilizan esos protocolos de nivel de aplicación?

Pila de protocolos

Una pila de protocolos es la lista de todos los protocolos, desde el físico hasta el más alto.

3. ¿Qué protocolos viajan sobre el nivel de enlace?

Más de un protocolo puede utilizar el nivel de enlace para enviar sus datos. En esos casos, el nivel de enlace debe apuntar a qué protocolo se le entregarán los datos en el ordenador de destino.

Segundo nivel/nivel de enlace

No hablamos del segundo nivel en **wireshark**, sino del nivel de enlace en ISO/OSI.
Es posible que un nivel de enlace ISO/OSI aparezca en segundo o tercer nivel en el **wireshark**.

Captura el tráfico de la red durante uno o dos minutos. Haz una lista de los protocolos que viajen sobre los niveles de enlace que encuentres, y crea una tabla con el nombre de protocolo y su código. Como ejemplo:

- Hay tramas *Ethernet* que llevan *IP*. Hay que apuntar `0x0800`
- Pero no apuntes el *Transmission Control Protocol*, porque no va directamente sobre el nivel de enlace (*Ethernet II*) sino dentro de un nivel de red

4. Conversación `ping`

- Captura el tráfico mientras haces un `ping` al servidor de DNS de Google `8.8.8.8`
- Usa un filtro de Wireshark para mostrar solo esa Conversacióm
- Incluye en el trabajo el pantallazo de la conversación y el filtro utilizado.

5. Qué se valorará

- La corrección técnica
- Que esté correctamente redactado (ortografía, gramática)
- La apariencia profesional:
  - Estética
  - Organización
  - Homogeneidad de formatos y estilos

6. Instrucciones de entrega

- El ejercicio se realizará y entregará de manera individual.
  - Solo se admiten trabajos en pareja, si en clase es necesario compartir ordenador.
  - En este caso, todos los integrantes del grupo deben subir el trabajo al aula virtual, y el trabajo debe especificar todos sus autores.
- Los trabajos pueden entregarse:
  - En formato `DOC` o `DOCX`.
  - En formato `ODT`.
  - En formato `PDF`.
  - Como una entrada en un `blog`, por ejemplo en blogger o en wordpress.
- La entrega se realizará en la tarea correspondiente del aula virtual. Si se entrega un fichero, este se subirá directamente. Si es una entrada de blog, se subirá un fichero de texto con la URL de dicha entrada.