PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2333 — Sistemas Operativos y Redes — 1/2021

# Tarea 4

7 de junio, 2021

**Fecha de entrega:** 7 de julio, hasta las 20:59
**Fecha de ayudantía:** 30 de junio, 2021
**Composición:** en parejas (2 personas)

## 1. Objetivos

En esta tarea deberán monitorear y analizar paquetes de datos de la red a través del programa Wireshark. La tarea consiste de distintos casos que les permitirán familiarizarse con el programa y conocer más sobre los dispositivos conectados a la red y protocolos de red.

## 2. Caso 1: Servidor UDP (10 puntos)

Junto con este enunciado se les entregó un archivo ejecutable: `broadcast_OS`, en donde `OS` corresponde a su sistema operativo. Este archivo permite correr un servidor UDP que hace **broadcast** de mensajes constantemente. Deberán correr este servidor y mientras esté corriendo deben encontrar y analizar los paquetes correspondientes usando el programa Wireshark. En específico, deberán realizar lo siguiente:

- Ejecuten el archivo `broadcast_OS` a través del siguiente comando en consola:

  ```
  $ ./broadcast_OS <numero_de_alumno_sin_digito_verificador>
  ```

  Esto ejecutará el servidor UDP, el cual comenzará a hacer broadcast de mensajes.

- Usando Wireshark, notarán que aparecen muchos paquetes de tipo UDP. Cree un filtro de forma que solo se capturen paquetes cuya IP de destino sea `255.255.255.255` y que el protocolo sea UDP. ¿Cuál es este filtro?

- ¿Cuál es el tamaño en bytes del paquete completo? ¿Cuántos de estos corresponden a UDP? ¿A qué se debe esta diferencia?

- ¿Cuál es el mensaje que emite el servidor? ¿Cuál es su largo en bytes en el paquete?

- Adjunten un archivo de captura con Wireshark de nombre `server_PDU.pcapng` en donde se pueda ver el mensaje recibido.

## 3. Caso 2: Conexión a SIDING (10 puntos)

En está sección deberán analizar, usando Wireshark, lo que ocurre cuando se conectan a la plataforma **SIDING** y navegan por ella a través de su *browser* de preferencia. Deberán hacer lo siguiente:

- Identificar la IP de la plataforma. Esto lo pueden lograr observando los paquetes capturados por Wireshark cuando se conectan a la página y navegan en ella. ¿Cuál es esta IP?

- Crear un filtro en Wireshark, de forma que solo se capturen paquetes cuyo origen o destino es la IP de la plataforma SIDING. ¿Cuál es este filtro?

- Con el filtro activado y el visor de paquetes capturados vacío, realizar la conexión a la página del curso a través de su navegador web de preferencia. Debiesen aparecer 6 paquetes capturados. ¿Qué es lo que está ocurriendo? ¿A qué corresponden estos paquetes?
- Si espera unos momentos sin hacer nada en su navegador comenzará a recibir paquetes de tipo **TCP Keepalive**. ¿Qué significan estos paquetes? ¿Por qué se envían?
- Al navegar por la plataforma, observarán que Wireshark detecta paquetes del protocolo TCP de tipo **RST**. ¿A qué se deben estos paquetes? ¿Qué está ocurriendo? Creen un filtro de Wireshark de forma que solo muestre estos paquetes. ¿Cuál es este filtro?
- Expliquen qué es el protocolo **TSL** y para qué se usa. Describan además el **Handshake Protocol** de TSL. ¿Tiene sentido que aparezcan paquetes de este protocolo al conectarse a la plataforma SIDING? ¿Por qué?

# 4. Caso 3: Red Local y Diagnóstico de Red (10 puntos)

En esta sección deberán analizar, usando Wireshark, distintos mensajes que pueden ocurrir dentro de sus redes privada o mensajes relacionados con diagnóstico de red.

- Determinen las IPs públicas de sus redes locales. En consola ejecuten un test **traceroute**[1] desde uno de sus equipos a la IP pública del compañero. Observen lo que ocurre en Wireshark. ¿Qué está pasando? ¿En qué consiste este test?
- Adjunten un archivo de captura de Wireshark con nombre `traceroute.pcapng` en donde se puedan ver los paquetes capturados que apoyen su respuesta de la pregunta anterior.
- Describan qué es el protocolo **ICMP** y para qué se usa generalmente.
- Si no utilizan ningún filtro, cada cierto tiempo van a recibir un paquete de protocolo **ARP**. ¿Cuál es la finalidad de este protocolo?
- Indiquen utilizando Wireshark si el servicio **DHCP** está habilitado en sus redes locales. Esto lo pueden comprobar observando lo que ocurre en Wireshark cuando se conectan a sus redes locales. Describan lo que realizaron para llegar a su respuesta.
- Adjunten un archivo de captura de Wireshark con nombre `dhcp.pcapng` en donde se puedan ver los paquetes capturados que apoyen su respuesta de la pregunta anterior.
- En consola ejecuten un test **nslookup**[2] hacia la IP de la plataforma SIDING. ¿Qué está ocurriendo? ¿Qué objetivo tiene este test? Respondan a partir de lo que aparece en Wireshark al ejecutar el test.

# 5. Entrega y formalidades

Deberán subir un archivo comprimido `.zip` a la carpeta `T4` de su directorio en el servidor del curso. Este archivo comprimido deberá contener el archivo `respuestas.pdf` con sus respuestas a todas las preguntas de los puntos anteriores, junto con las capturas pedidas en el enunciado.

El nombre del archivo debe tener el siguiente formato: `t4_[numalumno_1]_[numalumno_2].zip`. Por ejemplo, si el número de alumno del integrante 1 es `12345678` y el del integrante 2 es `22446688`, su archivo a subir tendrá por nombre `t4_12345678_22446688.zip`.

Además, pueden subir un `README` en caso de que lo estimen necesario.

[1] https://es.wikipedia.org/wiki/Traceroute
[2] https://es.wikipedia.org/wiki/Nslookup

## 6. Nota final y atraso

La nota final de la tarea entregada a tiempo se calcula de la siguiente manera:

$$N = 1 + \frac{\sum_i p_i}{5}$$

Se puede hacer entrega de la tarea con un máximo de cuatro días de atraso. La fórmula a seguir es la siguiente:

$$N_{atraso} = \text{mín}(N; 7 - 0{,}75 \cdot a)$$

Siendo $p_i$ el puntaje obtenido en el ítem $i$, $a$ la cantidad de días de atraso y $\text{mín}(x; y)$ la función que retorna el valor mas pequeño entre $x$ e $y$.