

Arquitectura de Internet

Ejercicios de Evaluación P1: Protocolos y Ethernet



Universidad
Rey Juan Carlos



Curso
2020-2021

Marzo de 2021

Profesores: Felipe Ortega y Juan González

Contenido

1. Análisis de ficheros de captura de tráfico
2. Generación de tráfico Ethernet y análisis de la captura de tráfico

Ejercicios de Evaluación. P1: Protocolos y Ethernet

- **Envío:** El envío se realizará a través del espacio de entrega habilitado en el apartado **Evaluación** de la página de la asignatura en Aula Virtual.
- **Herramientas software:** Utiliza NetGUI, Wireshark así como las herramientas Linux que se han ido introduciendo en las Prácticas 0 y 1 para contestar las preguntas de cada apartado.
- **Formato:** Puedes enviar tus respuestas en un fichero de procesador de textos (LibreOffice u OpenOffice) o en formato PDF. También es válido componer un documento con una herramienta de notas para tables, siempre que el envío se realice **en formato PDF**.

- **⚠ Advertencia:** Incluye claramente en el documento de tu respuesta tus datos personales, así como **toda la información solicitada** en cada pregunta (pantallazos, comandos, justificaciones, etc.). De lo contrario, la respuesta no puntuará.
-  **Fecha tope de entrega:** xxxxx-xxx-xxxx.

Descargas

- **Guion de la práctica en PDF:** TODO (opcional) (es lo mismo de esta wiki)

Ficheros que debes **descargar** para realizar los ejercicios:

- **Captura 1:** [evp1-captura1.cap](#)
- **Escenario de red:** [ev-p1.zip](#)

1. Análisis de ficheros de captura de tráfico

Abre el fichero de captura con [Wireshark](#) y responde a las siguientes preguntas:

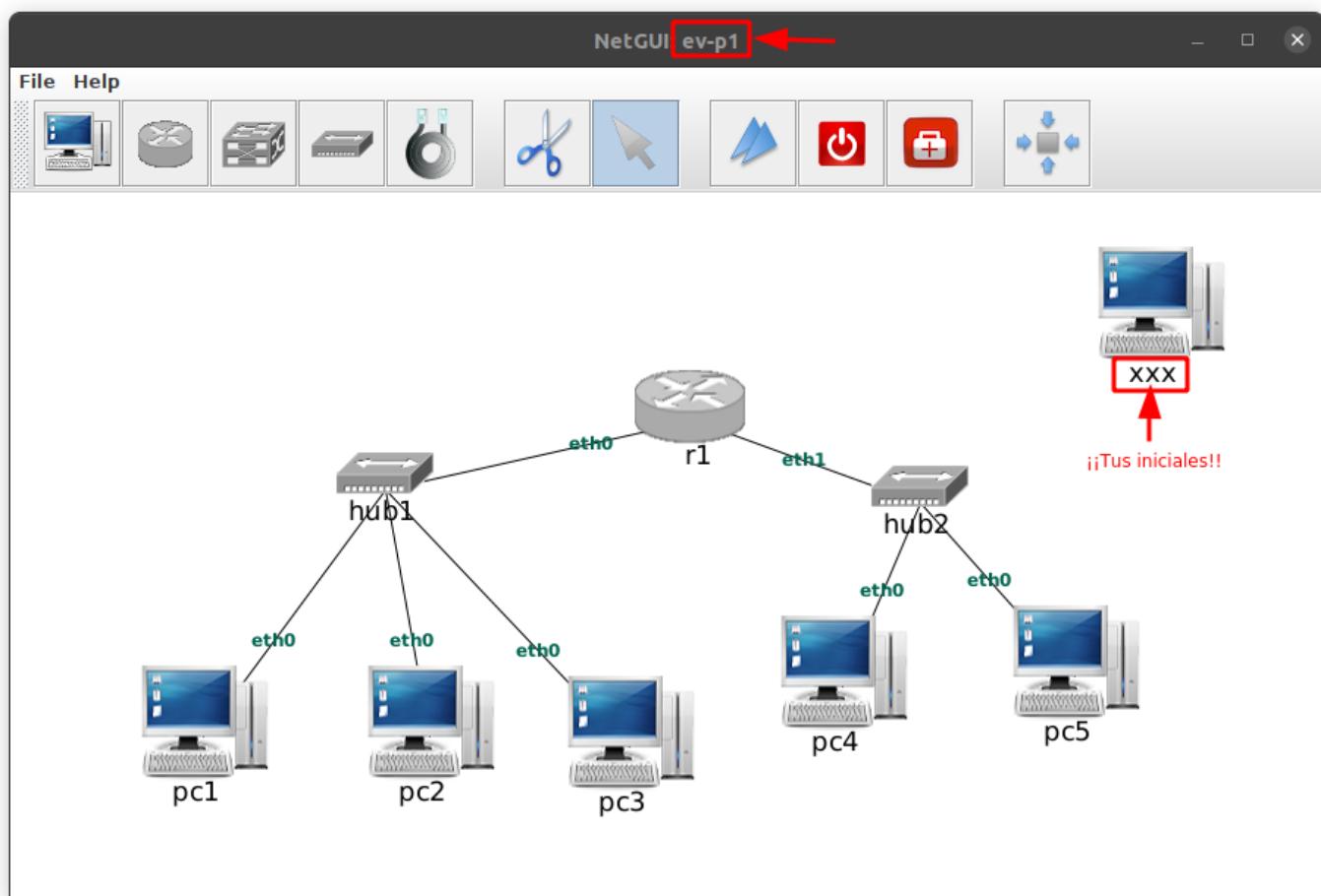
1. ¿Cuántas tramas se han capturado en total?
2. Accede a la trama capturada a los **14.711630** segundos. Indica qué **protocolos** se usan y a **qué nivel de la arquitectura TCP/IP** corresponden
3. Seguimos con la misma trama anterior, capturada a los **14.711630** segundos y responde a las siguientes preguntas:
 - 3.1: ¿Cuántos bytes se envía por el cable físico? (Sin contar el preámbulo y el CRC)
 - 3.2. ¿Y contando el CRC?
 - 3.3. ¿Cuántos bytes tiene la cabecera del protocolo Ethernet?
 - 3.4. ¿Cuántos bytes tiene la cabecera del protocolo IP? (si lo usa)
 - 3.5. ¿Cuántos bytes tiene la cabecera del protocolo TCP? (si lo usa)
4. Usando la misma trama anterior, responde las siguientes preguntas:
 - 4.1: ¿Cuál es la dirección física de la máquina que recibe la trama?
 - 4.2: ¿Cuál es la dirección física de la máquina que envía la trama?
 - 4.3: ¿Cuál es el valor del campo *Type* de esta trama ethernet?
5. Analiza **todas** las tramas y escribe todos los protocolos diferentes que veas que se están usando, y clasifícalos según niveles según la **arquitectura TCP/IP**
6. Analiza la trama número 8
 - 6.1: ¿Cuántos datos útiles (bytes) se transportan en el protocolo de último nivel?
 - 6.2: ¿Qué mensaje se está enviando?

7. Analiza todas las tramas. Localiza todas las máquinas que hay e indica para cada una de ellas su dirección física y su dirección de red

2. Generación de tráfico Ethernet y análisis de la captura de tráfico

Abre el escenario proporcionado con **NetGUI**. Se trata de un escenario que **ya está configurado**, y que sólo contiene un único ordenador: pc1

1. **Completa el escenario** para que sea igual al mostrado en la figura, PERO cambia el nombre del PC **xxx** por **tus iniciales**. Así, si tu nombre fuese Antonio Gonzalez Martinez este PC debería llamarse **agm**. **No arranques** ninguna máquina hasta que no termines de hacer el dibujo. Una vez finalizado haz una **captura de pantalla** de NETGUI con tu escenario y **adjúntala** como solución a este apartado



2. **Arranca** todas las máquinas, y **adjunta otro pantallazo** de tu escritorio en el que se pueda ver NETGUI y todas las consolas abiertas a su alrededor
3. Obtén la dirección física de la interfaz de red de PC1. Muestra un pantallazo del terminal con el comando que has usado e indica exactamente dónde se puede ver esta dirección
4. Haz una **tabla** con las direcciones físicas de TODAS las interfaces de red que aparecen en el escenario
5. Indica si existe alguna máquina que tenga más de una dirección física
6. Captura el tráfico que ven los ordenadores PC3 y PC4. Utiliza el comando necesario para que se empiece la captura en dichos ordenadores y se guarde en los ficheros **evp1-cap-pc3.cap** y **evp1-**

pc4.cap en el **directorio personal** de tu ordenador. Adjunta una captura de los terminales de pc3 y pc4 una vez que se ha iniciado la captura

7. Desde PC1 usa el comando `arping -c 1 <dir ethernet pc2>`, donde `<dir ethernet pc2>` es la **dirección física** de la interfaz de red de PC2. Muestra un pantallazo del terminal con el resultado de su ejecución
8. Interrumpe las capturas de pc3 y pc4. Abre los ficheros evp1-cap-pc3.cap y evp1-cap-pc4.cap con wireshark y envía una captura de pantalla de cada uno de ellos, donde se pueden ver el resultado que has obtenido
9. **Analiza las tramas Ethernet** que aparecen en ambas capturas. Para cada paquete indica:
 - (a) Dirección Ethernet origen
 - (b) Dirección Ethernet destino
10. Explica lo que ocurre en la captura de pc4
11. Analiza la captura desde PC3
 - (a) Indica qué máquinas reciben la primera trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior
 - Indica qué máquinas reciben la segunda trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior
 - Si la primera trama lleva como dirección destino **ff:ff:ff:ff:ff:ff** indica qué máquinas recibirían dicha trama y qué máquinas se la entregarían al protocolo de nivel superior
12. Indica qué ocurre si se envía una trama Ethernet de pc4 a pc5 y se capturara el tráfico en las siguientes interfaces: pc1(eth0) y r1(eth1)
13. Indica qué ocurriría si se envía una trama Ethernet de pc1 a pc4 y se capturara el tráfico en pc2(eth0) y en pc5(eth0)