

# Práctica 3

## Redes de computadores

Enrique Cabrerizo Fernández      Guillermo Ruiz Álvarez

14/11/2013

## Índice

|  |           |
|--|-----------|
| <b>1. Introducción</b>                                       | <b>3</b>  |
| <b>2. Análisis de la traza</b>                               | <b>3</b>  |
| 2.1. Porcentajes de protocolos . . . . .                     | 3         |
| 2.2. Popularidad de direcciones IP y puertos . . . . .       | 4         |
| 2.3. Tamaños de los paquetes . . . . .                       | 5         |
| 2.4. Ancho de banda a nivel 2 (Throughput) . . . . .         | 7         |
| 2.5. Tiempo entre llegadas de paquetes de un flujo . . . . . | 8         |
| <b>A. Manual de utilización del programa</b>                 | <b>10</b> |
| A.1. Compilación . . . . .                                   | 10        |
| A.2. Ejecución . . . . .                                     | 10        |

## 1. Introducción

En esta práctica se va a implementar un programa que analizará y caracterizará una captura de paquetes de red. Para ello, utilizará un fichero \*.pcap que contenga una traza o directamente una interfaz especificada, dependiendo del argumento utilizado (véase sección A, página 10).

Las funciones que realizará el programa son las siguientes:

- Mostrar por pantalla los porcentajes de paquetes IP, no ETH-IP, TCP, UDP y no TCP-UDP.
- Mostrar por pantalla el top de 5 direcciones IP activas y el top de 5 puertos activos (ambos por paquetes y tamaño en bytes).
- Almacene en fichero y calcule el ECDF de la variable *tamaño de paquete capturado*.
- Almacene en fichero el ancho de banda a nivel 2 cada segundo por sentido.
- Almacene en fichero y calcule el ECDF de la variable *tiempo entre llegadas de los paquetes de un flujo entre un par de puertos*.

Adicionalmente se calcularán histogramas de las variables en las que se pide calcular un ECDF para así disponer de más información para analizar los datos.

De forma particular, el análisis que se va a llevar a cabo consistirá en mostrar la funcionalidad de la herramienta sobre el fichero proporcionado con el enunciado de la práctica: *practica3\_rcllab.pcap*

## 2. Análisis de la traza

### 2.1. Porcentajes de protocolos

En la **Figura 1** se muestran los porcentajes de los paquetes IP, no Eth-IP, UDP, TCP y no UDP-TCP.

```
Recuento de paquetes:
Total capturado: 52872 (100%)
Total IP: 46449 (87.85%)
Total NO IP: 6423 (12.15%)
Total TCP: 46449 (87.85%)
Total UDP: 6423 (12.15%)
Total NO TCP-UDP: 0 (0.00%)
Total que pasan el filtro: 52872 (100.00%)
```

Figura 1: Recuento y porcentajes de protocolos de paquetes.

Se puede observar que el 12,15 % de los paquetes (6423 paquetes) no son Eth-IP. Un análisis posterior con Wireshark nos dirá que su tipo de ethernet corresponde a *802.1Q Virtual LAN (0x8100)*.

El resto de paquetes son todos TCP/IP, los dos protocolos más importantes del conjunto de protocolos de internet.

El campo *Total que pasan el filtro* cuenta aquellos paquetes que pasan el filtro especificado mediante los argumentos. El filtro básico, para el que no se utiliza ningún argumento adicional, es que el paquete sea IP (tanto Eth-IP como VLAN-IP).

## 2.2. Popularidad de direcciones IP y puertos

En la **Figura 2** se muestra el top 5 de direcciones IP activas y en la **Figura 3** se muestra el top 5 de puertos activos, ambos clasificados por *número de paquetes, tamaño en bytes, origen y destino*.

|  |             |  |
|--|-------------|--|
| Popularidad de IPs por paquetes (TOP 5): |             |  |
| Origen:                                  |             |  |
| IP Origen                                | N.Paquetes. |  |
| 130.206.193.12                           | 15454       |  |
| 192.168.128.133                          | 11463       |  |
| 123.212.11.229                           | 6423        |  |
| 130.206.193.15                           | 4657        |  |
| 74.125.216.180                           | 2906        |  |
| Destino:                                 |             |  |
| IP Destino                               | N.Paquetes. |  |
| 192.168.128.133                          | 34986       |  |
| 123.212.13.223                           | 6423        |  |
| 130.206.193.12                           | 3881        |  |
| 130.206.193.15                           | 1273        |  |
| 74.125.216.180                           | 983         |  |
| Popularidad de IPs por bytes (TOP 5):    |             |  |
| Origen:                                  |             |  |
| IP Origen                                | Bytes.      |  |
| 130.206.193.12                           | 23098523    |  |
| 130.206.193.15                           | 6918040     |  |
| 74.125.216.180                           | 4344112     |  |
| 74.125.168.19                            | 3245100     |  |
| 130.206.193.14                           | 3193577     |  |
| Destino:                                 |             |  |
| IP Destino                               | Bytes.      |  |
| 192.168.128.133                          | 50345203    |  |
| 123.212.13.223                           | 1400214     |  |
| 130.206.193.12                           | 249160      |  |
| 173.194.41.229                           | 115206      |  |
| 130.206.193.15                           | 79229       |  |

Figura 2: Popularidad de direcciones IP.

Como se puede observar, la popularidad en paquetes y en bytes no tiene por qué coincidir. Esto es obvio dado que se pueden enviar o recibir paquetes de distintos tamaños, particularmente, de entre 54 y 1514 bytes. Por ejemplo, si una dirección o puerto envía diez asentimientos (ACK) estará enviando diez paquetes de 54 bytes (el tamaño mínimo de la trama ethernet), que será menor en tamaño que un paquete de 1514 bytes.

|  |        |            |
|--|--------|------------|
| Popularidad de puertos por paquetes (TOP 5): |        |            |
| Origen:                                      |        |            |
|  | Puerto | N.Paquetes |
|  | 80     | 34757      |
|  | 24704  | 6423       |
|  | 55934  | 1423       |
|  | 55860  | 1096       |
|  | 55865  | 617        |
| Destino:                                     |        |            |
|  | Puerto | N.Paquetes |
|  | 80     | 11296      |
|  | 27088  | 6423       |
|  | 55934  | 5486       |
|  | 55860  | 4313       |
|  | 55865  | 3204       |
| Popularidad de puertos por bytes (TOP 5):    |        |            |
| Origen:                                      |        |            |
|  | Puerto | Bytes      |
|  | 80     | 50127403   |
|  | 24704  | 1400214    |
|  | 443    | 217800     |
|  | 55934  | 88065      |
|  | 55860  | 67367      |
| Destino:                                     |        |            |
|  | Puerto | Bytes      |
|  | 55934  | 8236507    |
|  | 55860  | 6437994    |
|  | 55865  | 4808618    |
|  | 43585  | 3245100    |
|  | 33896  | 2707440    |

Figura 3: Popularidad de puertos.

### 2.3. Tamaños de los paquetes

Para analizar la variable *tamaño del paquete capturado* se han realizado un histograma (**Figura 4**) y un ECDF (**Figura 5**) de dicha variable sobre la traza.

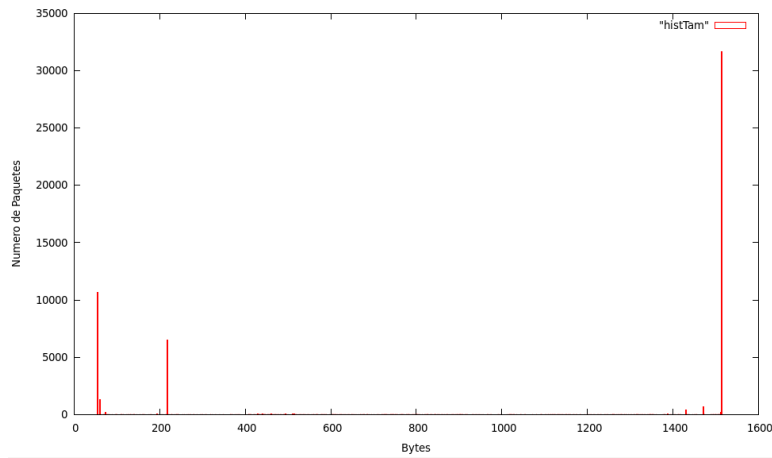


Figura 4: Histograma de tamaños de paquetes.

En el histograma puede observarse que la mayoría de paquetes tienen un tamaño de 54, 218 o 1514 bytes.

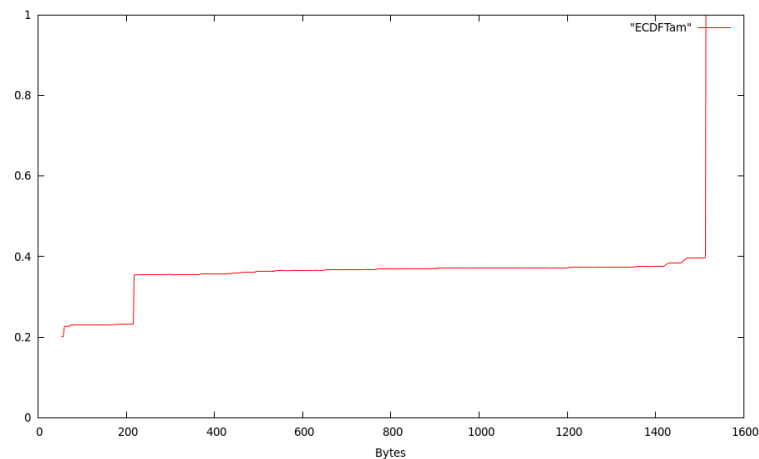


Figura 5: ECDF de tamaños de paquetes.

El ECDF nos muestra una información similar, se puede comprobar que las subidas en el mismo corresponden con los tamaños 54, 218 y 1514 bytes vistos en el histograma.

Este resultado se obtiene porque los paquetes de la traza corresponden a asentimientos, tráfico UDP y segmentos de datos.

Los paquetes de 54 bytes se corresponden con asentimientos, que se utilizan para confirmar la recepción de un mensaje (dado que 54 bytes es el tamaño mínimo de una trama ethernet). Por otro lado, los paquetes de 218 bytes corresponden a paquetes de tráfico UDP de esta traza. Y finalmente,

los paquetes de 1514 bytes son segmentos de datos, es decir, cuando se quiere enviar una cantidad de datos, se segmentan en varios paquetes ocupando varios de 1514 bytes (el tamaño máximo de una trama ethernet) y el resto de la información se colocará en un paquete del tamaño necesario.

En conclusión, hay una cantidad considerable de paquetes que son asentimientos o tráfico UDP y la gran mayoría del resto de datos que se quieren enviar han sido fragmentados en paquetes de 1514 bytes y en paquetes de tamaño variable que contienen el resto de dicha fragmentación.

## 2.4. Ancho de banda a nivel 2 (Throughput)

Tras el ancho de banda a nivel 2 cada segundo por sentido asumiendo que la dirección Ethernet origen es `00:55:22:af:c6:37` y descartando el tráfico broadcast obtenemos una figura con la representación del throughput (**Figura 6**)

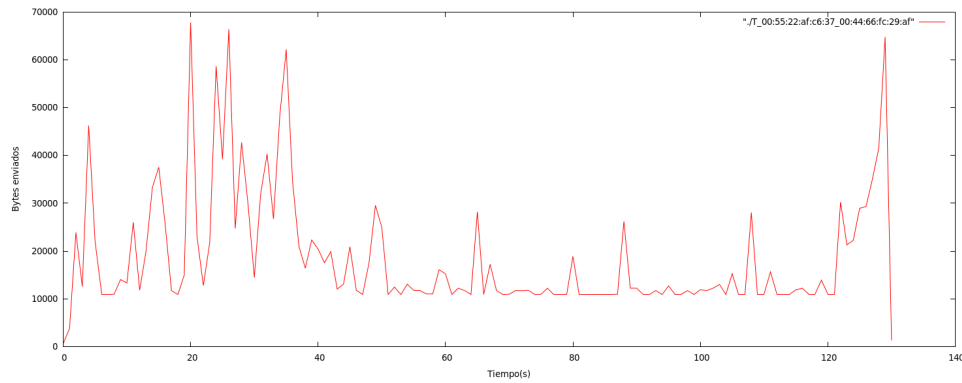


Figura 6: Ancho de banda cada segundo.

En la gráfica puede observarse que hay una base de tasa de envío de unos 10900 bytes cada segundo, que se corresponden a envíos constantes de paquetes UDP de 218 bytes cada 0,02 segundos aproximadamente ( $\frac{218B}{0,02s} = 10900 B/s$ ).

El resto de los saltos de la gráfica pueden deberse a lo que se haya decidido enviar en cada momento, tanto segmentos de datos como asentimientos. El caudal de datos por segundo no sigue una distribución fija pues depende de los paquetes que se envían y del momento en el que se envían, sin embargo, ofrece una visión generalizada de la cantidad de información que se envía en cada momento, así como de las tasas constantes de envío, como en este caso el tráfico UDP.

## 2.5. Tiempo entre llegadas de paquetes de un flujo

Para analizar los tiempos entre llegadas de paquetes de un flujo, se asumió el flujo UDP con puertos de origen y destino 24704 y 27088 respectivamente. Se obtienen en este caso el histograma (**Figura 7**) y el ECDF (**Figura 8**) correspondientes.

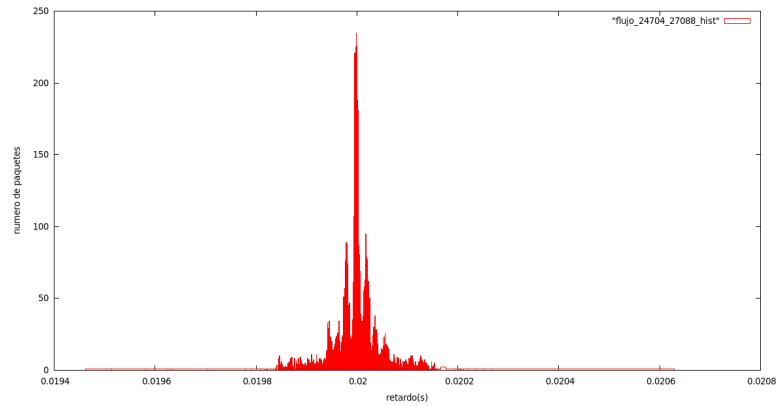


Figura 7: Histograma del tiempo entre llegadas de paquetes del flujo.

El histograma muestra como el tiempo de llegadas entre paquetes se concentra en 0,02 segundos.

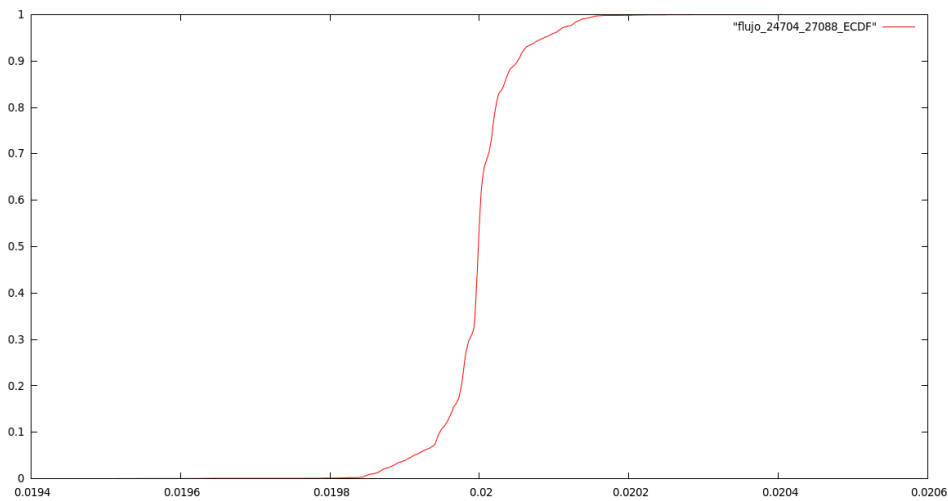


Figura 8: ECDF del tiempo entre llegadas de paquetes del flujo.

En el ECDF se observa como el salto en el valor 0,02 de los segundos es muy pronunciado, lo que indica una baja dispersión con respecto a este valor.



En conclusión, en el flujo analizado, se obtiene un tiempo de llegadas entre paquetes centrado y muy próximo a 0,02 segundos en todos los casos, lo que podría atribuirse a una tasa de recibo muy constante y por tanto un Jitter bajo. En los casos en los el Jitter fuera alto, la tasa de recibo no sería constante, sino que sufriría altibajos y el tiempo entre llegadas de paquetes se dispersaría más de su media.

## A. Manual de utilización del programa

En esta sección se ofrece una breve explicación sobre la utilización del programa implementado.

### A.1. Compilación

Para compilar el programa se proporciona un fichero Makefile, existen tres opciones equivalentes para la compilación del mismo utilizando el programa make:

- **make all** compila el programa y le da el nombre *practica3*
- **make practica3** compila el programa y le da el nombre *practica3*
- **make main** compila el programa y le da el nombre *main*

Para limpiar los archivos generados por la compilación, basta con ejecutar **make clean**.

### A.2. Ejecución

Para ejecutar el programa se utiliza la siguiente estructura:

**./practica3 INTERF [<filtro> <dato a filtrar>]**

Donde:

**INTERF** es el fichero pcap o interfaz ethernet (ethX con  $X \in [0, 9]$ ).

[<filtro> <dato a filtrar>] : puede ser:

- ipo x.x.x.x : filtro de IP de origen x.x.x.x ( $x \in [0, 255]$ )
- ipd x.x.x.x : filtro de IP de destino x.x.x.x ( $x \in [0, 255]$ )
- po x : filtro de puerto de origen x ( $x \in [0, 65536]$ )
- pd x : filtro de puerto de destino x ( $x \in [0, 65536]$ )
- etho xx:xx:xx:xx:xx:xx : filtro de MAC origen ( $xx \in [00, FF]$ )
- ethd xx:xx:xx:xx:xx:xx : filtro de MAX destino ( $xx \in [00, FF]$ )

Se pueden aplicar varios filtros a la vez y el orden de los mismos no se tiene en cuenta. Si un filtro IP es 0.0.0.0, un filtro de puertos es 0, o un filtro ethernet es 00:00:00:00:00:00 se considerará inexistente, es decir, no se aplicará dicho filtro.