

# Práctica 3

## Redes de computadores

Enrique Cabrerizo Fernández      Guillermo Ruiz Álvarez

14/11/2013

## Índice

<b>1. Introducción</b>	<b>3</b>
<b>A. Manual de utilización del programa</b>	<b>4</b>
A.1. Compilación . . . . .	4
A.2. Ejecución . . . . .	4

## 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 4).

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\_rc1lab.pcap*

Las funciones que realizará el programa son las siguientes:

- Mostrar por pantalla los porcentajes de paquetes IP, NO 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).
- Calcule el ECDF de la variable *tamaño de paquete leído*.
- Calcule

## 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*

### 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.