Práctica 3
Redes de computadores

Enrique Cabrerizo Fernández Guillermo Ruiz Álvarez

14/11/2013

Índice

1. Introducción

En esta prática 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 8).

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_rc1lab.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: 0 (0.00%)
        Total NO TCP-UDP: 6423 (12.15%)
        Total que pasan el filtro: 46449 (87.85%)
```

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 Eth-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
                 130.206.193.15         4657
                 74.125.216.180         2906
                 74.125.168.19   2188

        Destino:
                IP Destino              N.Paquetes.
                 192.168.128.133        34986
                 130.206.193.12         3881
                 130.206.193.15         1273
                 74.125.216.180         983
                 130.206.193.14         666

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
                 130.206.193.12         249160
                 173.194.41.229         115206
                 130.206.193.15         79229
                 173.194.34.197         76301
```

Figura 2: Popularidad de direcciones IP.

La razón por la cual las clasificaciones por paquetes no coinciden con las clasificaciones por tamaños es que muchos de los paquetes enviados o recibidos por algunas direcciones o puertos son asentimientos (ACK). Por tanto, aunque una dirección o puerto pueda recibir o enviar muchos paquetes, si un porcentaje elevado de estos son asentimientos sólo ocuparan 54 bytes (el tamaño mínimo de una trama ethernet), es decir, que se habrán enviado o recibido muchos paquetes pero de poco tamaño.

```
Popularidad de puertos por paquetes (TOP 5):
        Origen:
                Puerto   N.Paquetes
                 80      34757
                 55934   1423
                 55860   1096
                 55865   617
                 43585   607

        Destino:
                Puerto   N.Paquetes
                 80      11296
                 55934   5486
                 55860   4313
                 55865   3204
                 43585   2188

Popularidad de puertos por bytes (TOP 5):
        Origen:
                Puerto   Bytes
                 80      50127403
                 443     217800
                 55934   88065
                 55860   67367
                 55865   40574

        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 ha un histograma y un ECDF de dicha variable sobre la traza. (Véase figura XXXXXXXXXXXXX).

2.4. Ancho de banda a nivel 2

Se analizará 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.

2.5. Tiempo entre llegadas de paquetes de un flujo

Para analizar los tiempos entre llegadas de paquetes de un flujo, se asumirá el flujo UDP con puertos de origen y destino 24704 y 27088 respectivamente. Dicho análisis se llevará a cabo con la ayuda de Wireshark dado que la pila de protocolos usada no es Eth-IP, sino VLAN.

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.