Universidad Autónoma

Redes de Comunicaciones I

Práctica 3

Memoria

Autores:
Adrián Fernández
Santiago González-Carvajal

13 de noviembre de 2017

Índice

1. Introducción

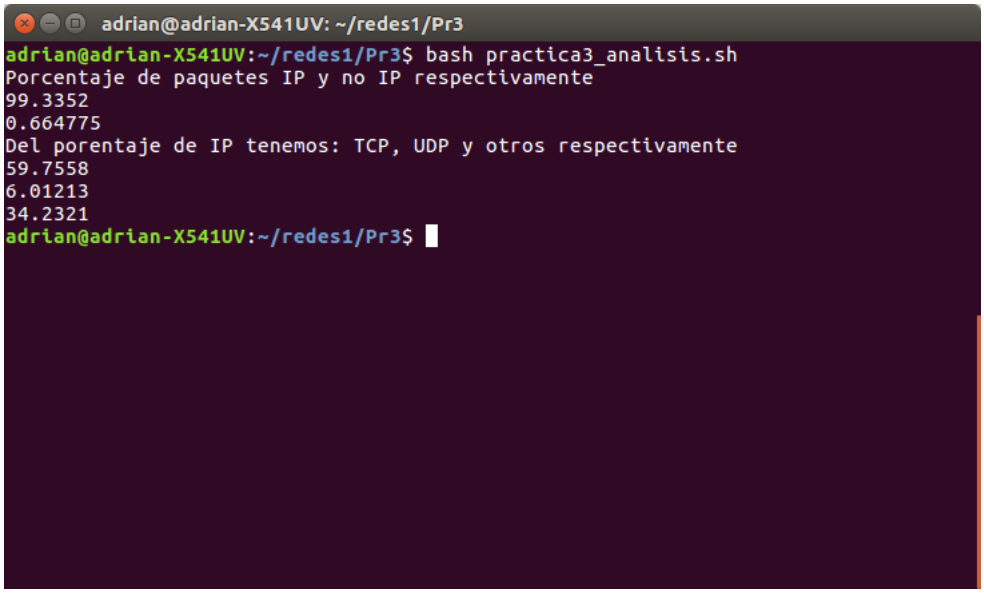
Con motivo de la practica 3 de Redes de Comunicaciones I, debemos utilizar scripts para analizar una traza que simula el trafico de una red real.

En concreto, debemos distinguir los paquetes IP y los no IP, y analizar varios parámetros de los IP, como las direcciones IP destino y origen o, en el caso en el que se trate de paquetes TCP o UDP, los puertos destino y origen. También deberemos analizar el ancho de banda de cierta dirección MAC y la diferencia temporal en la emisión y recepción de los paquetes que cumplen unas características determinadas.

Una vez recopilados estos datos, debemos representarlos en ECDF's mediante scripts y explicar los resultados obtenidos.

2. Porcentajes de paquetes

Captura de la ejecución:



Porcentajes:

IP: 99.3352 % - Filtro: (eth.type eq 0x0800 || vlan.etype eq 0x0800)

No IP: 0.664775 % - Filtro: ((eth.type ne 0x0800&&eth.type ne 0x8100)|| (eth.type eq 0x8100&&vlan.etype ne 0x0800))

Dentro de los IP (contados con awk):

TCP: 59.7558 % - Filtro: (ip.proto == 6)

UDP: 6.01213 % - Filtro: (ip.proto == 17)

Otros: 34.2321 % - Filtro: paquetes restantes

Como podemos ver, casi todos los paquetes son de tipo IP, y entre ellos, la mayoría son TCP.

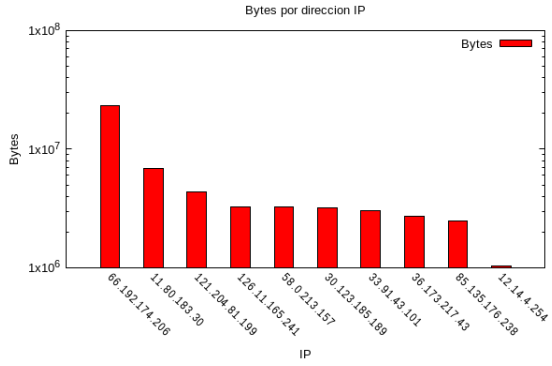
3. Top 10 de direcciones IP y puertos (TCP y UDP)

Nótese que el eje vertical está en escala logarítmica para que se puedan apreciar las direcciones IP o puertos que tienen menos tráfico. Las barras sin altura implican que esa dirección o puerto solo ha estado implicado en la transmisión de un paquete.

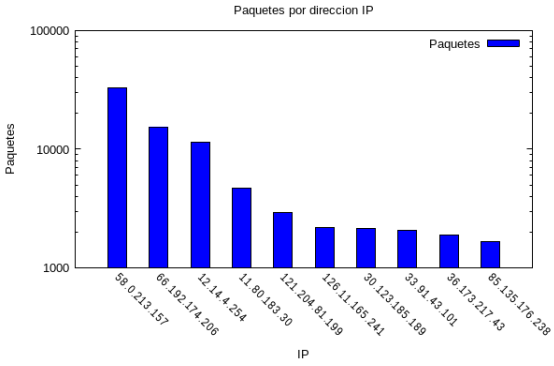
Cabe remarcar que las gráficas de bytes y las de paquetes están relacionadas pero no son idénticas. Esto se debe a que los paquetes transmitidos varían en tamaño. La relación evidente entre las gráficas es que cuantos más paquetes se envían, más Bytes se están enviando

Direcciones IP origen:

Por bytes:

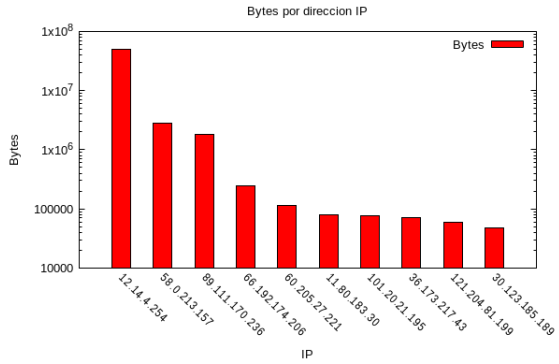


Por paquetes:

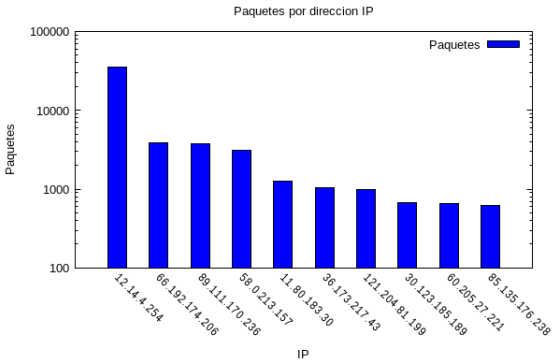


Direcciones IP destino:

Por bytes:



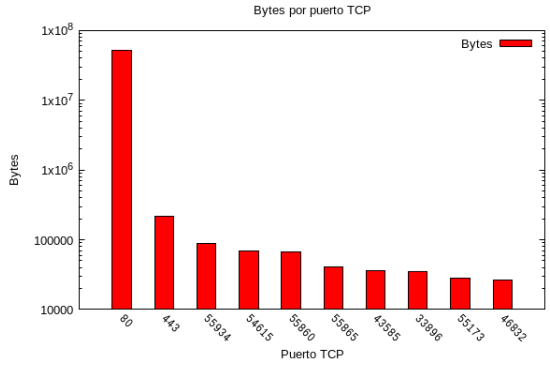
Por paquetes:



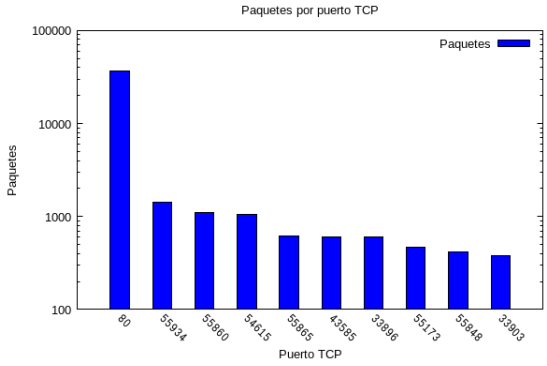
Como podemos apreciar, estas gráficas representan un elevado número de Bytes y de paquetes debido al gran porcentaje tan elevado de paquetes IP que tiene la traza generada.

Puertos TCP origen:

Por bytes:

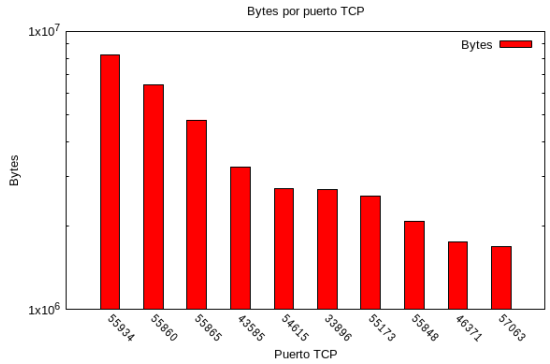


Por paquetes:

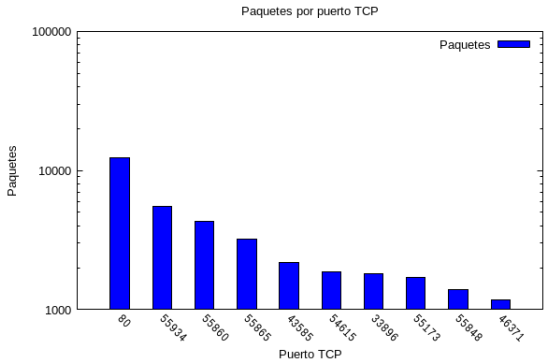


Puertos TCP destino:

Por bytes:



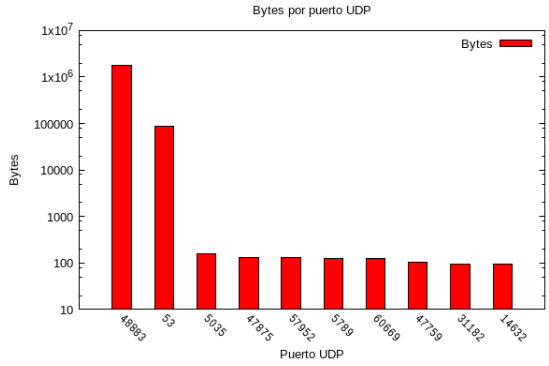
Por paquetes:



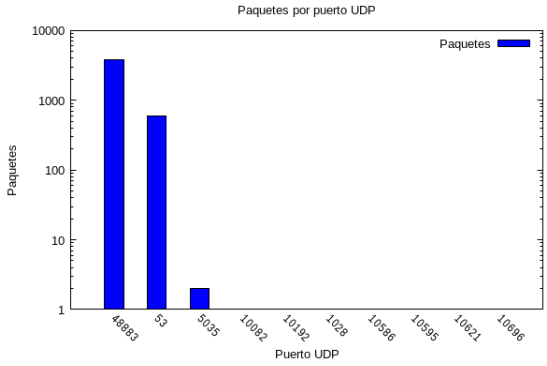
Como podemos observar, estos valores son menores que los obtenidos en las gráficas para paquetes IP, lo cual se debe a que componen un a porción de los paquetes IP. Sin embargo los valores son mayores los de UDP, puesto que el porcentaje de paquetes TCP es mayor que el de UDP.

Puertos UDP origen:

Por bytes:

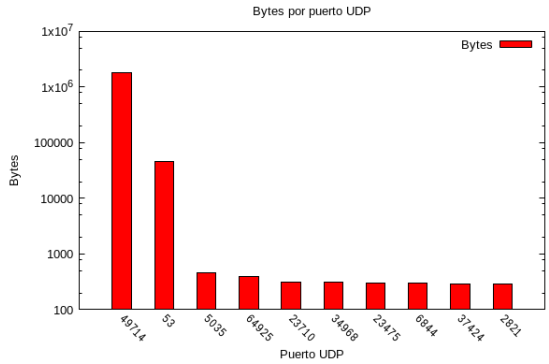


Por paquetes:

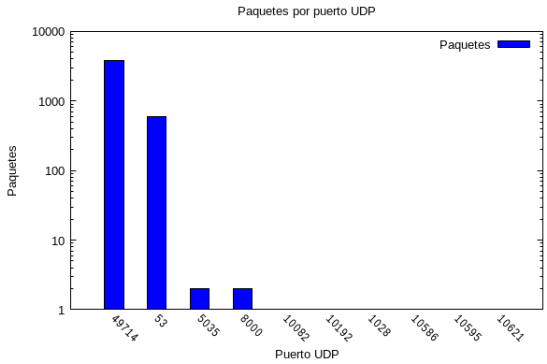


Puertos UDP destino:

Por bytes:



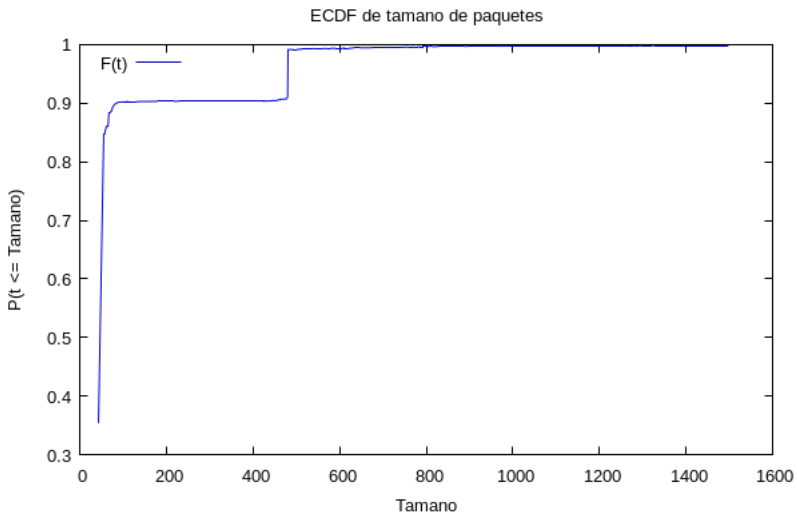
Por paquetes:



En estas gráficas podemos relacionar los valores bajos al limitado número de paquetes UDP. La gran mayoría de los puertos están involucrados e la trnsmisión de uno o ningún paquete UDP.

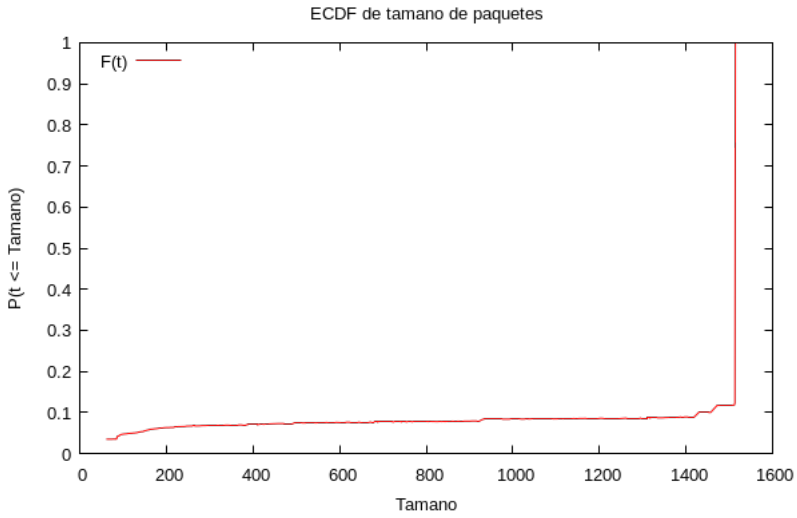
4. ECDFs de tamaños de paquetes a nivel 2

ECDF de tamaños a nivel 2 de paquetes (origen):



Esta ECDF nos dice que los paquetes enviados desde la dirección MAC indicada en el generador de trazas pueden tener un tamaño de entre 50 y 100 Bytes (con una probabilidad muy elevada), o bien entre 450 y 500 Bytes (con una probabilidad bastante menor que la anterior) y que rara vez se dan casos de paquetes con tamaño distinto.

ECDF de tamaños a nivel 2 de paquetes (destino):

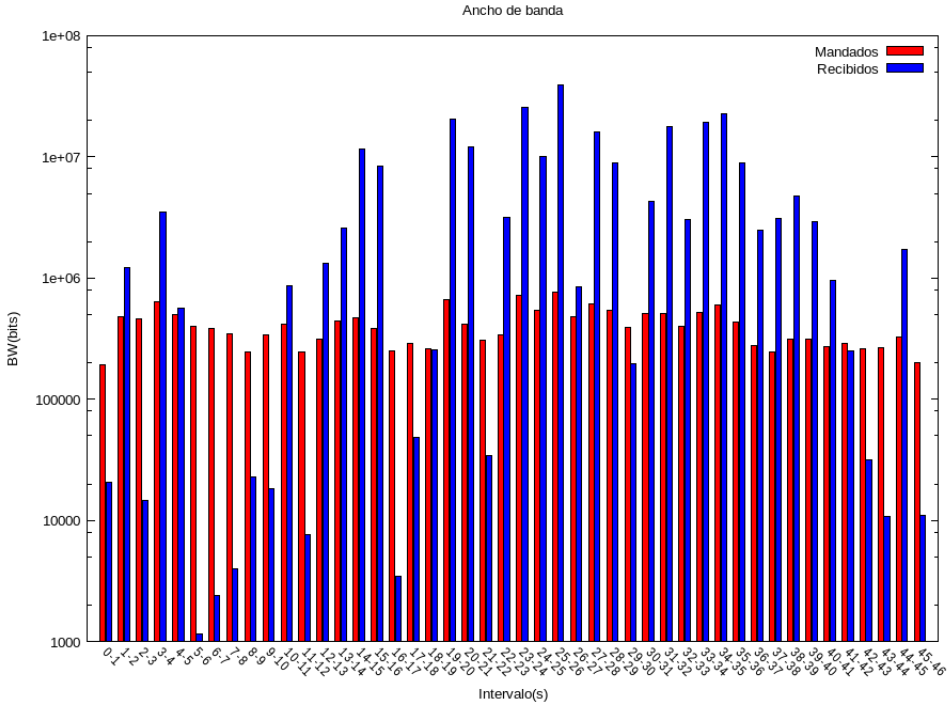


En cambio, los recibidos tienen, en general, un tamaño de entre 1500 y 1550 Bytes (aunque algunos paquetes tienen tamaños menores, pero la probabilidad de obtenerlos muy inferior).

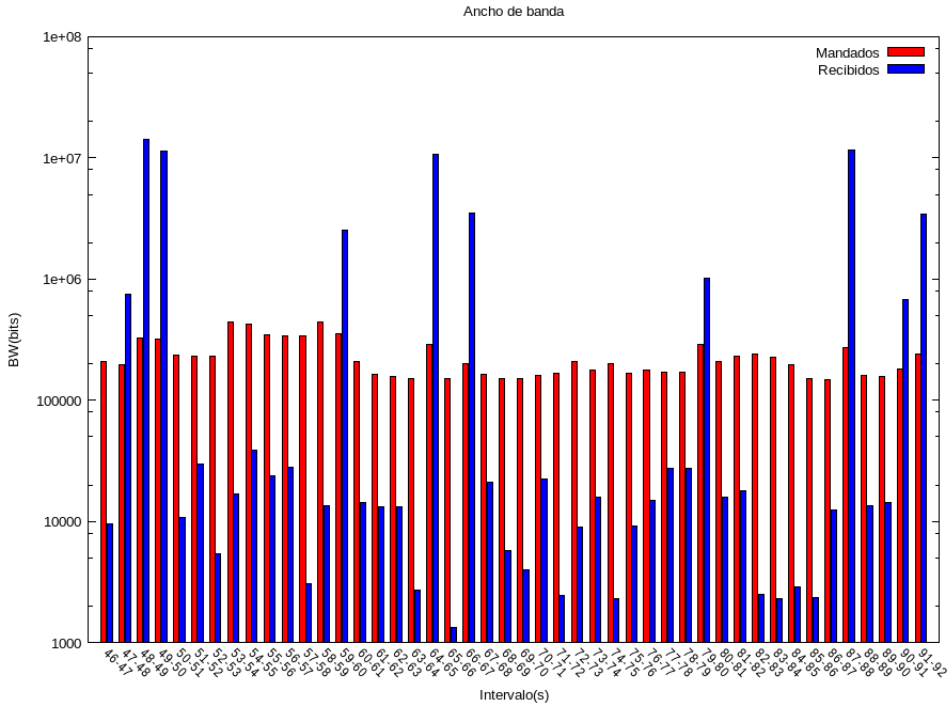
5. Ancho de banda

Nótese que el eje vertical está en escala logarítmica para que se pueda apreciar el ancho de banda de los bits mandados.

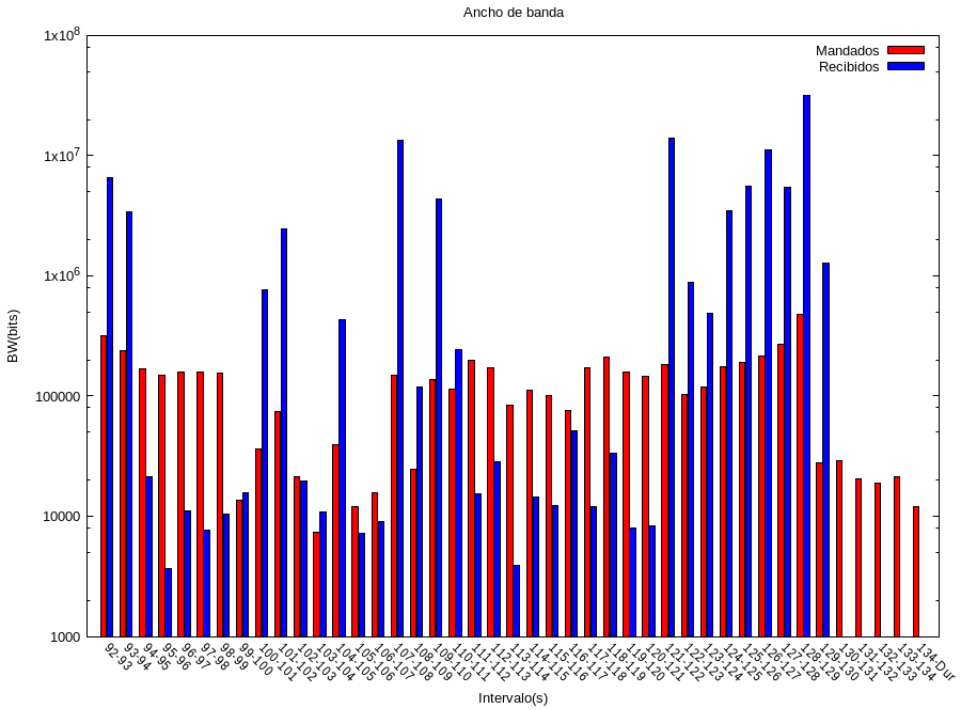
BW en los primeros 46 segundos:



BW en los segundos 46 - 92:



BW en los últimos segundos:



Estas gráficas muestran el ancho de banda con granularidad de 1 segundo. Podemos observar que el ancho de banda de los paquetes enviados desde la dirección MAC proporcionada se mantiene estable en líneas generales (los valores no cambian más de 40K b/s), salvo en los últimos segundos donde hay una bajada considerable.

En cambio, los valores de los recibidos son poco uniformes. Podemos observar que en los primeros segundos (hasta el segundo 20 aproximádamente) los valores son muy bajos, luego se disparan (hasta el segundo 42), y a partir de ese momento los valores son bajos en general con algunas subidas puntuales (que no se mantienen) hasta el segundo 92. De ahí en adelante los valores oscilan en gran medida hasta los últimos 5 segundos, donde no existe tráfico en este sentido.

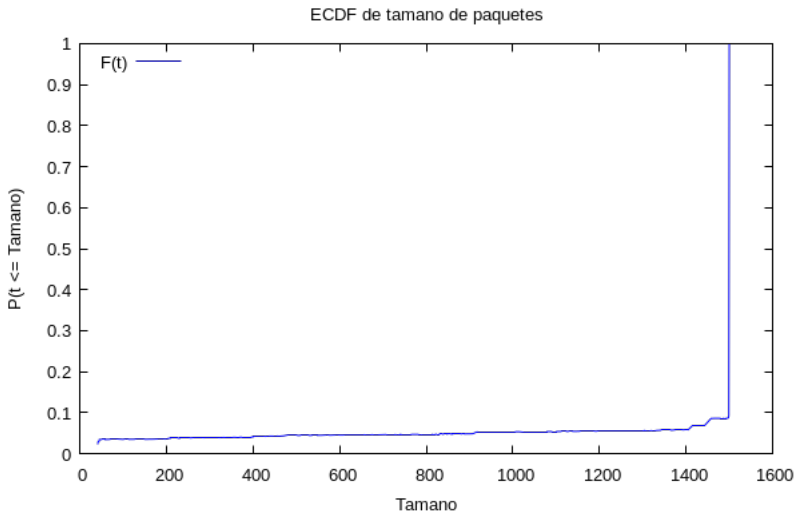
De estas observaciones podemos concluir que la emisión de paquetes requiere de muy poco ancho de banda en comparación con la recepción de

paquetes y que mientras la emisión es muy uniforme en el tiempo, la recepción es errática.

6. ECDFs de los tamaños de paquete a nivel 3

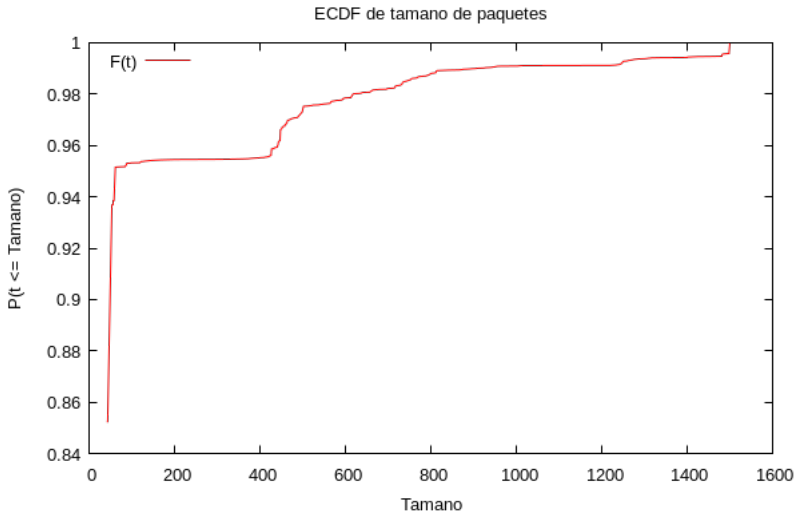
ECDF de los tamaños a nivel 3 de los paquetes DNS de la traza (una por sentido a nivel 4). Entenderemos como DNS todos aquellos paquetes que usen el puerto 53 de UDP en origen o destino.

ECDF de tamaños a nivel 3 (http origen):



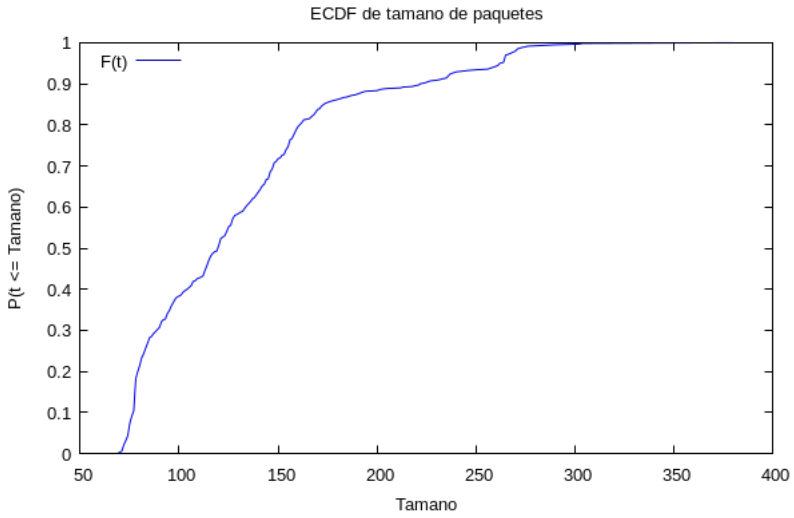
Aquí podemos observar que casi todos los paquetes HTTP de origen tienen un tamaño de unos 1500 Bytes.

ECDF de tamaños a nivel 3 (http destino):



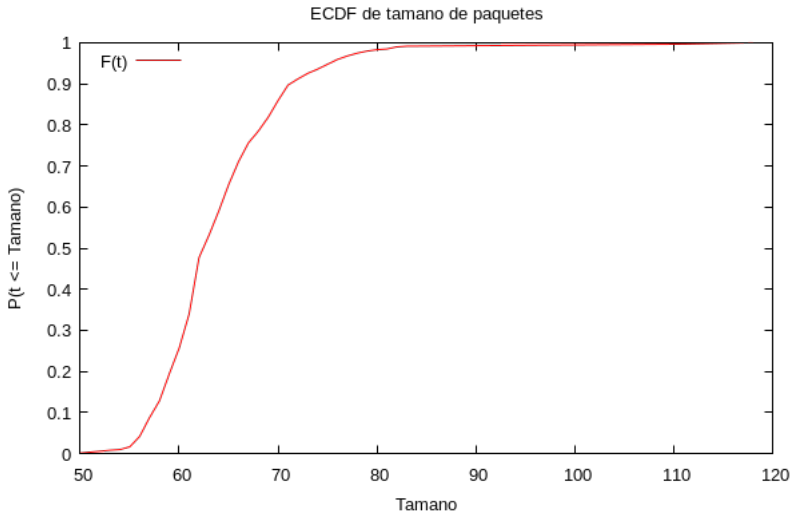
En cambio, en esta gráfica podemos observar que el tamaño de los paquetes HTTP destino cambia. El valor predominante es 50 Bytes aproximadamente, y abundan paquetes de entre 400 y 1500 Bytes (aunque estos últimos con menor probabilidad).

ECDF de tamaños a nivel 3 (dns origen):



Podemos apreciar que el tamaño de este tipo de paquetes oscila (en general) entre 75 y 275 Bytes, tomando los valores más bajos del intervalo con más frecuencia que los altos.

ECDF de tamaños a nivel 3 (dns destino):

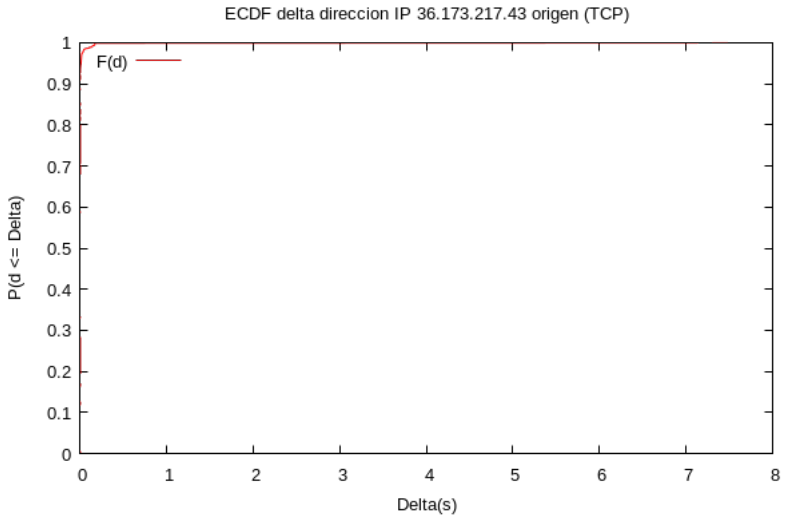


Podemos observar que los valores del tamaño de estos paquetes oscilan (en general) entre 55 y 80 Bytes tomando valores más pequeños del intervalo con mayor frecuencia que los mayores.

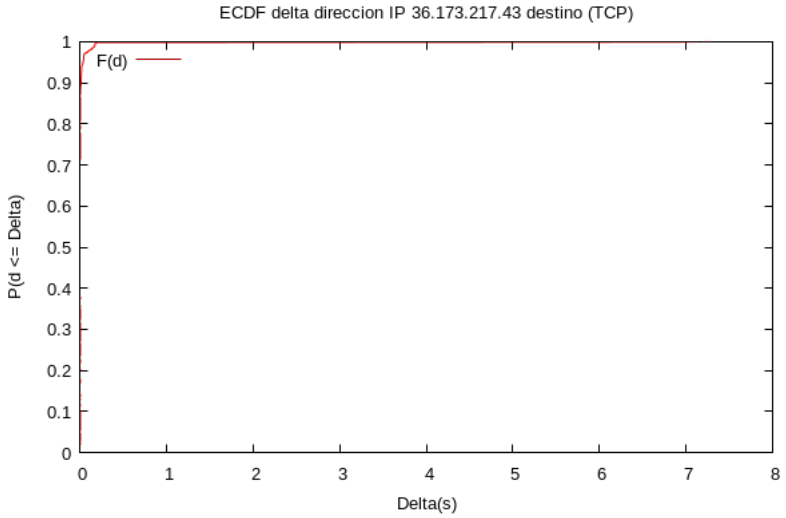
7. ECDFs de los tiempos entre llegadas (TCP)

ECDF de los tiempos entre llegadas del flujo TCP indicado por el generador de la traza (una por sentido a nivel 4).

ECDF de los tiempos entre llegadas de paquetes del flujo tcp (origen):



ECDF de los tiempos entre llegadas de paquetes del flujo tcp (destino):



El parecido entre ambas gráficas hace que las conclusiones obtenidas sean las mismas para las dos.

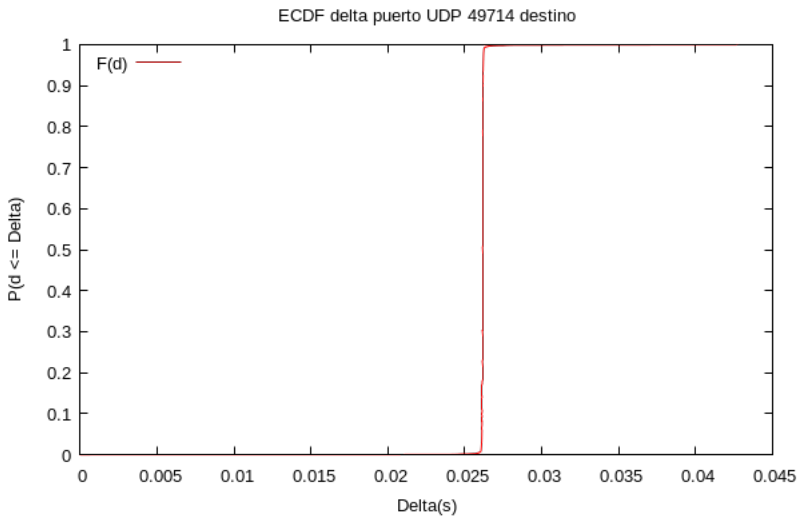
Podemos observar que los tiempos entre llegadas de paquetes de estos flujos son muy cercanos a 0, es decir, estos paquetes están llegando a un ritmo muy rápido en general. Aunque existen excepciones, como paquetes que llegan unos 7 segundos después, que causan que en la gráfica generada con gnuplot se muestre hasta el valor 8 en el eje x, y por consiguiente, que no se aprecie el crecimiento de la función.

8. ECDFs de los tiempos entre llegadas (UDP)

ECDF de los tiempos entre llegadas del flujo UDP indicado por el generador de la traza (una por sentido a nivel 4).

Nótese que solo hay gráfica para el flujo udp pedido con el puerto dado como destino, ya que no hay ningún paquete con dicho puerto como origen y por lo tanto no hay datos para generar la gráfica.

ECDF de los tiempos entre llegadas de paquetes del flujo udp (destino):



Podemos observar que los tiempos entre llegada de paquetes de este flujo son muy cercanos a 0 en general. Es decir, el tiempo máximo no llega en ningún caso a 0.5 segundos y el delta predominante es de aproximadamente 0.025 segundos, con una frecuencia de cerca del 100 %.

9. Conclusión

Esta práctica a requerido obtener parámetros básicos de una red mediante el uso de scripts con comandos de las herramientas tshark y awk. También ha sido útil el uso de gnuplot como herramienta para generar gráficas a partir de los datos obtenidos mediante tshark, y así facilitar el análisis de los mismos.

En concreto, la representación de los datos en forma de ECDF nos permite representar de una manera rápida e intuitiva la distribución estadística de los parámetros analizados y así comprender el comportamiento de la red.