Redes de Comunicaciones I – Prácticas 2020
Práctica 3: Análisis de tráfico

Turno y pareja: 1302, 07.

Integrantes:

Leandro García Ortiz,

Fabián Alejandro Gutiérrez Peña.

Fecha de entrega: 13 de diciembre de 2020.

Contenido

1 Introducción

Las redes de comunicaciones, indudablemente, son parte fundamental del mundo actual. Cada avance en estas ha supuesto a lo largo de la historia la ampliación de los horizontes de la humanidad, tanto en el ámbito personal con la aparición de servicios que van desde el mero entretenimiento o la comunicación directa entre personas hasta el acceso a información virtualmente infinita, como en el ámbito profesional, pues cosas como la colaboración entre personas de distintos continentes en un mismo proyecto, la difusión masiva de noticias en tiempo real o, *simplemente*, fotografiar un agujero negro serían impensables hace un siglo.

El amplio uso de las redes de comunicaciones supone que han de ser de la mejor calidad posible. Un buen diseño y correcto mantenimiento son cruciales para que el desempeño de las redes sea óptimo. De aquí la importancia de la monitorización de las redes, bien sea activa o pasiva, ya que permite detectar problemas o ineficiencias, incluso ataques, que puedan tener graves impactos en la red y en los equipos conectados a esta.

Por tanto, esta práctica tiene como objetivo realizar una monitorización pasiva del tráfico de una red y, en consecuencia, adquirir conocimientos y capacidades de las que un gestor de redes debe disponer. Específicamente, se realizarán distintas mediciones sobre una traza que simula el tráfico entre dos routers: los porcentajes que representan los distintos protocolos en el tráfico, las direcciones o puertos con más bytes o paquetes enviados o recibidos, la evolución temporal del ancho de banda consumido, y un análisis estadístico de los tamaños y tiempo entre llegadas de los paquetes mediante el cálculo de funciones de distribución acumulada empíricas.

2 Realización de la práctica

1. Análisis de protocolos.

   Obtener los porcentajes de paquetes IP y NO IP (entendemos como **NO-IP** aquellos paquetes que no son ni **ETH|IP** ni **ETH|VLAN|IP**)

% Paquetes IP	% Paquetes NO-IP
99,34%	0,66%

Filtro utilizado[1]: 'ip'.

Se observa que prácticamente todos los paquetes capturados en la traza son datagramas IPv4 en nivel de red. En particular, los datagramas IPv6 suponen a lo más un 0,66% de los paquetes capturados, con lo que IPv4 sigue siendo el protocolo de nivel de red hegemónico pese a estar limitado a direcciones de 32 bits.

   Obtener los porcentajes de paquetes UDP, TCP y OTROS sobre los que son IP (igualmente entienda, un paquete IP como aquel que cumpla la pila **ETH|IP** o **ETH|VLAN|IP**).

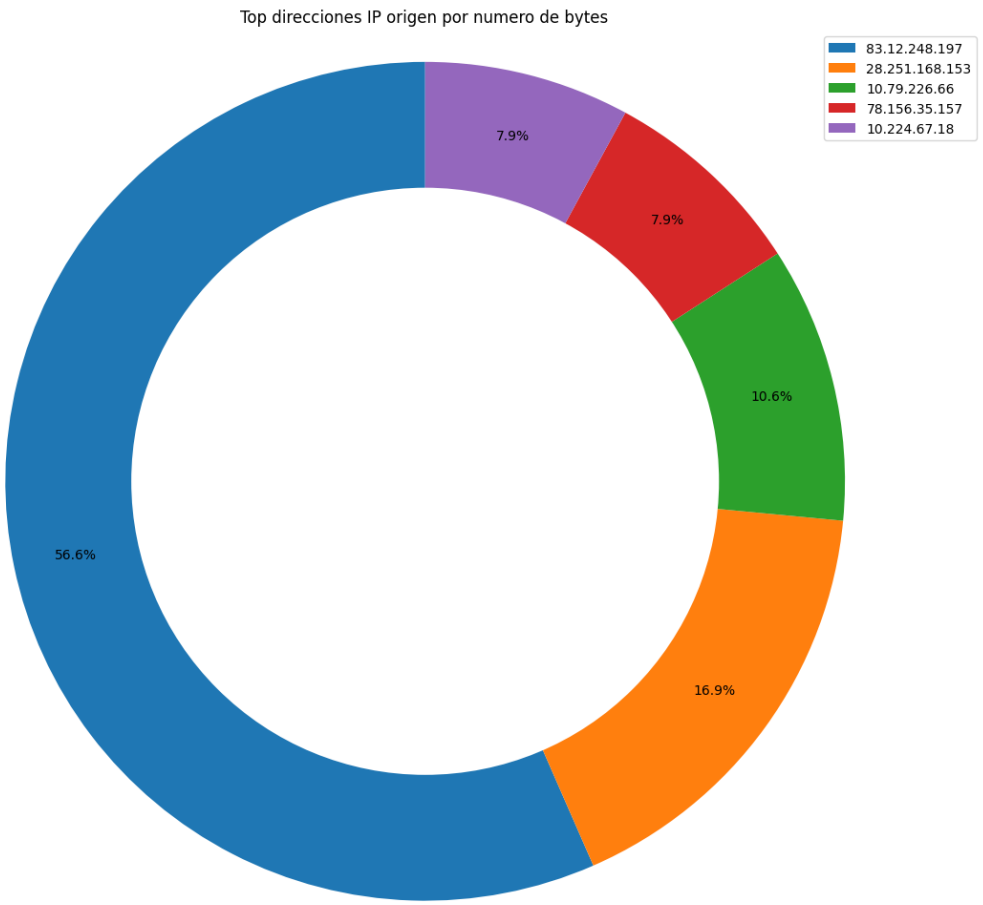
% Paquetes TCP	% Paquetes UDP	% Paquetes OTROS
59,76%	6,01%	34,23%

Filtros utilizados: 'tcp and ip and (not icmp)' para la captura de paquetes TCP y 'udp and ip and (not icmp)' para la de paquetes UDP.

El protocolo a nivel de transporte más común es el TCP, presente en más de la mitad de los paquetes IP. Esto puede deberse al funcionamiento del protocolo, pues se envían paquetes para la apertura y cierre de la conexión, además de paquetes de reconocimiento y retransmisiones cuando corresponde. Por otra parte, UDP, con poco más del 6%, tiene muy poca presencia entre los paquetes restantes.

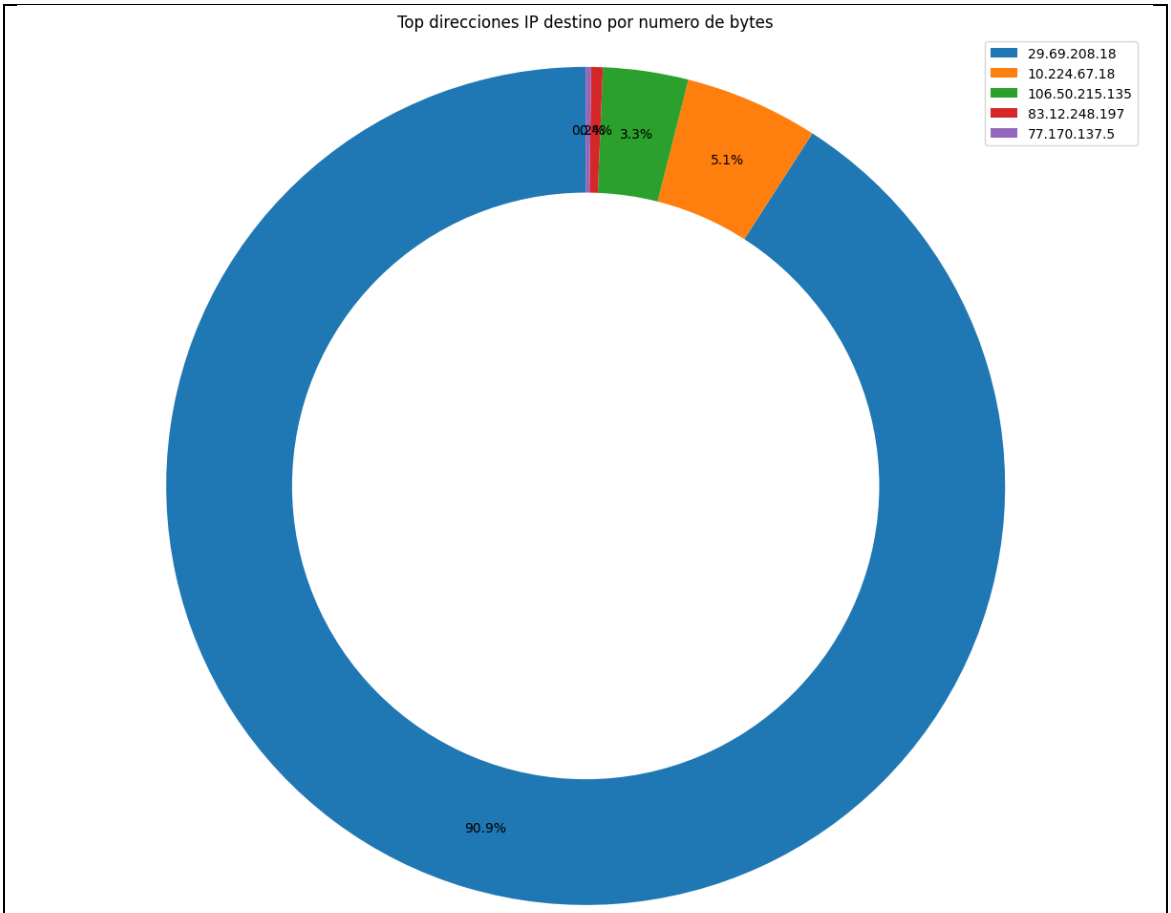
[1] Se indica el filtro utilizado en el comando de Tshark, mas no el comando completo. Los últimos pueden consultarse en el script de Python adjunto.

2. Obtención de top 5 de direcciones IP.



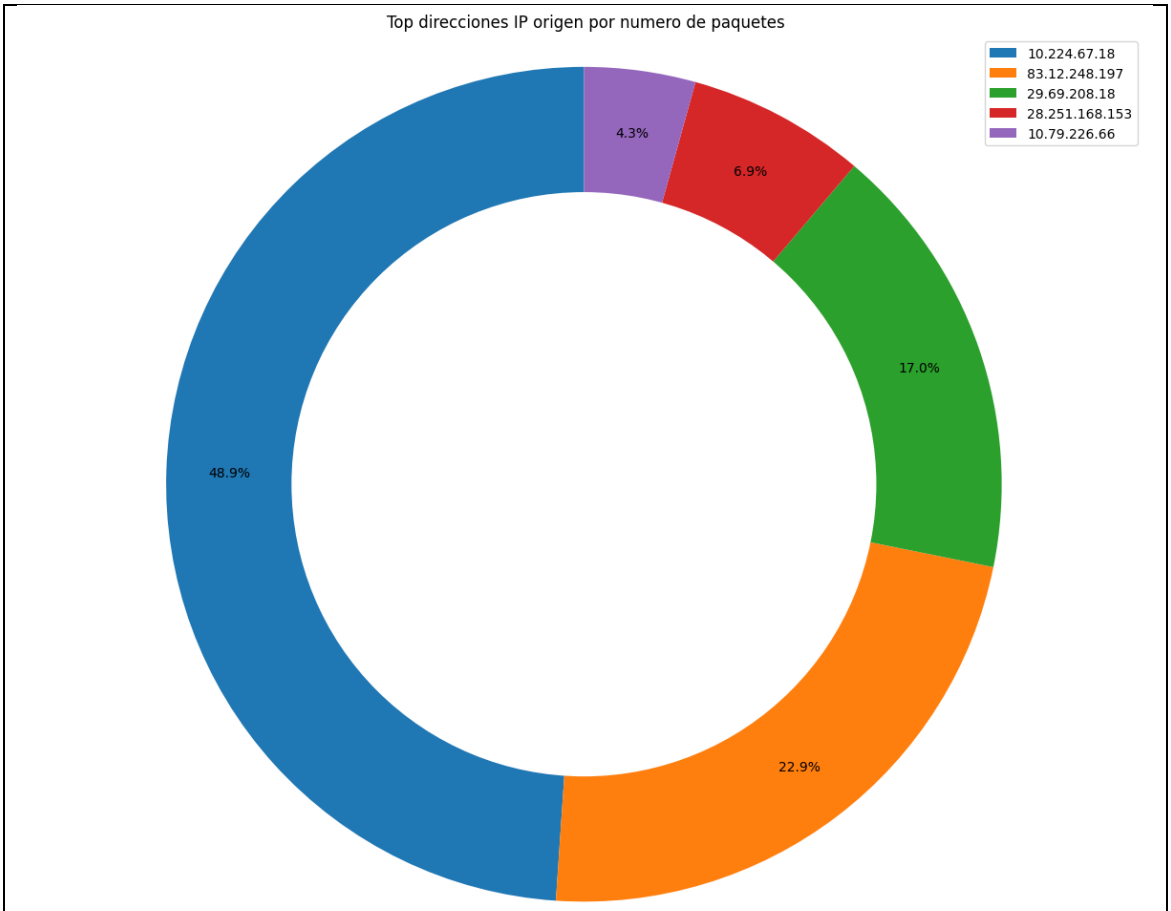
Filtro utilizado: 'ip'.

En esta gráfica se puede observar una evidente mayoría de bytes con origen en la IP 83.12.248.197, siendo estos más de la mitad de los representados. El resto de direcciones, por el contrario, se distribuyen de forma más equitativa.



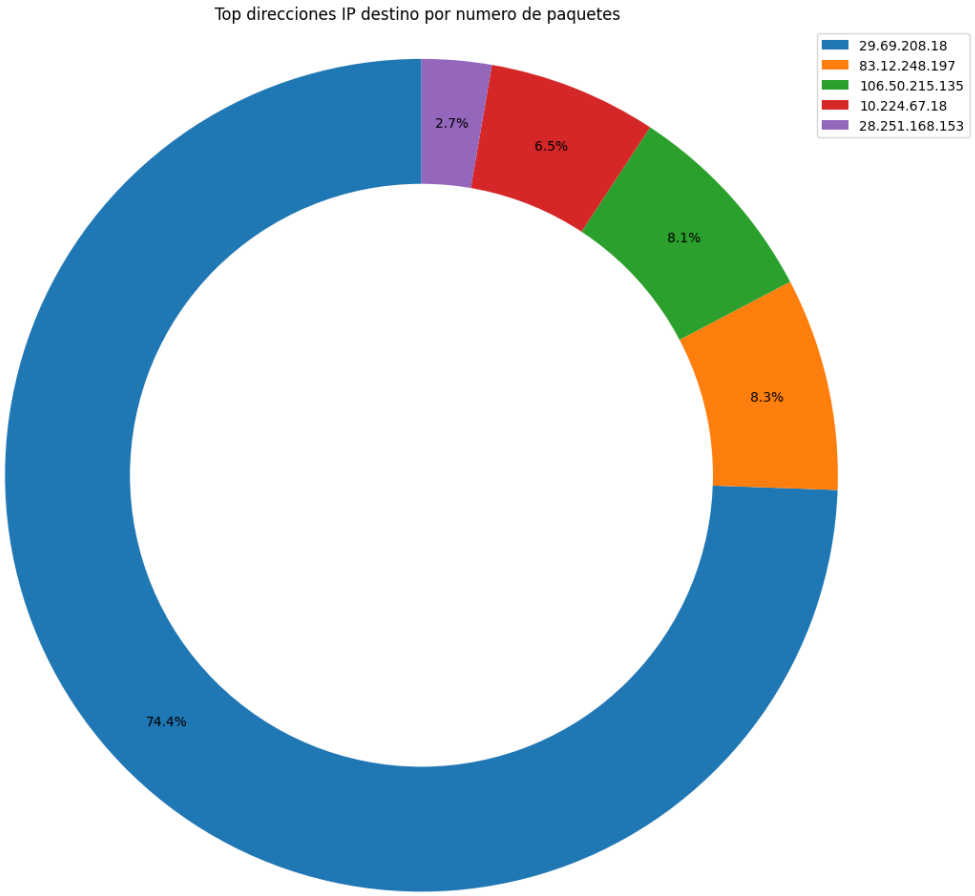
Filtro utilizado: ‘ip’.

En lo que respecta al número de bytes recibidos, se observa que la IP 29.69.208.18 monopoliza este ámbito con un 90.9% del total de bytes. Cabe destacar que la IP que anteriormente envió mayor número de bytes se encuentra en el top pero no alcanza el 1% del total.



Filtro utilizado: ‘ip’.

Aquí se puede ver como la IP con más paquetes enviados es la 10.224.67.18 con casi la mitad de los paquetes. En segundo lugar, la 83.12.248.197, que anteriormente apareció con la mayor cantidad de bytes enviados. Se puede deducir de aquí que esta última, pese a enviar menos paquetes, estos fueron de mayor tamaño.

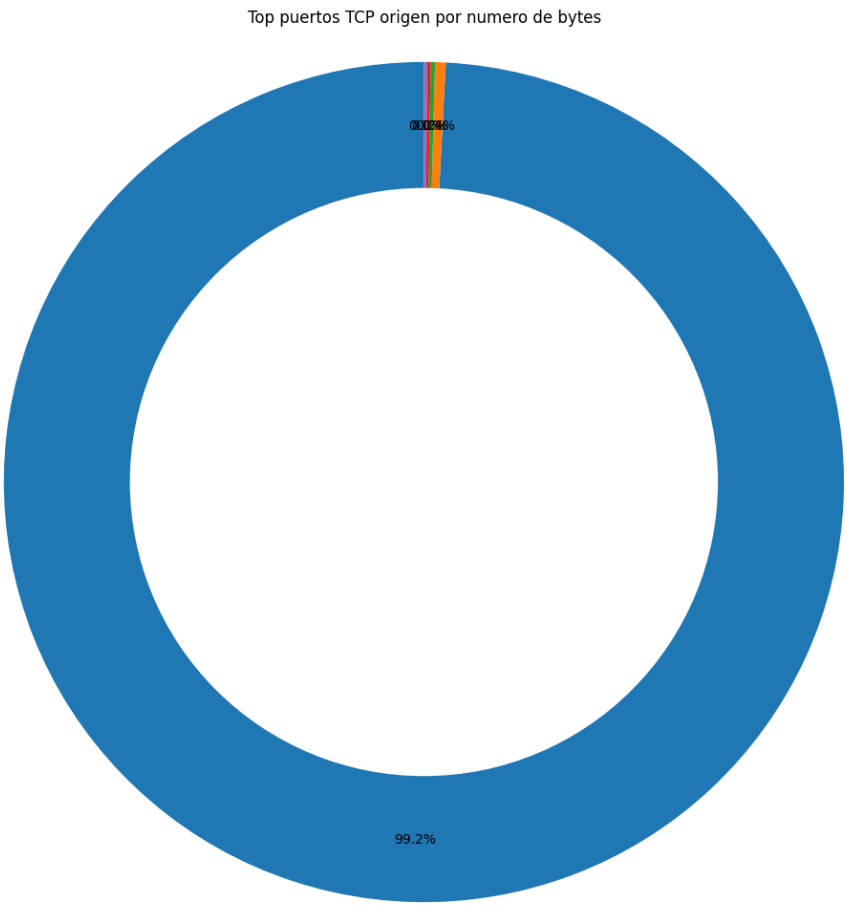


Filtro utilizado: ‘ip’.

En esta ocasión, al igual que en anterior top, la dirección que recibe más paquetes no es a la que más bytes le llegan, pese a tener un 74,4% de paquetes. Aquella con más bytes recibidos (más de un 90%) lo hace con tan solo un 8,3% de los paquetes, mostrándose así que son mucho mayorees que los demás.

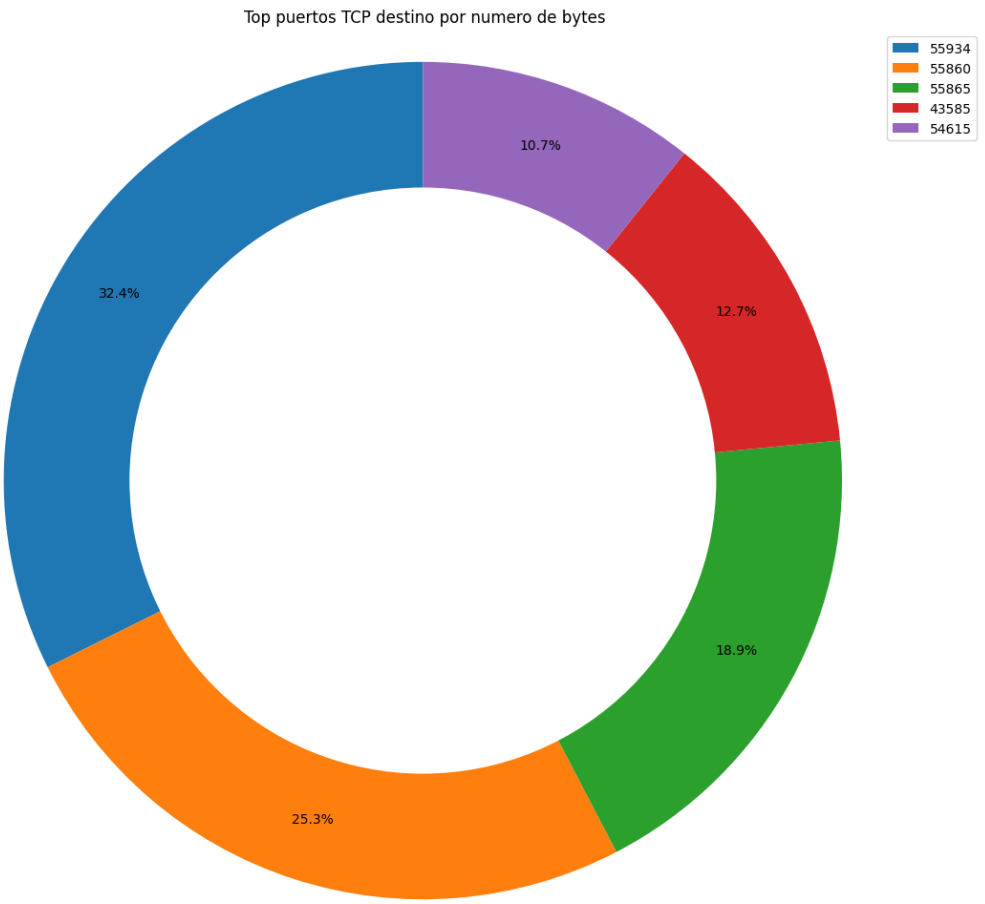
3. Obtención de top 5 de puertos:

TCP:



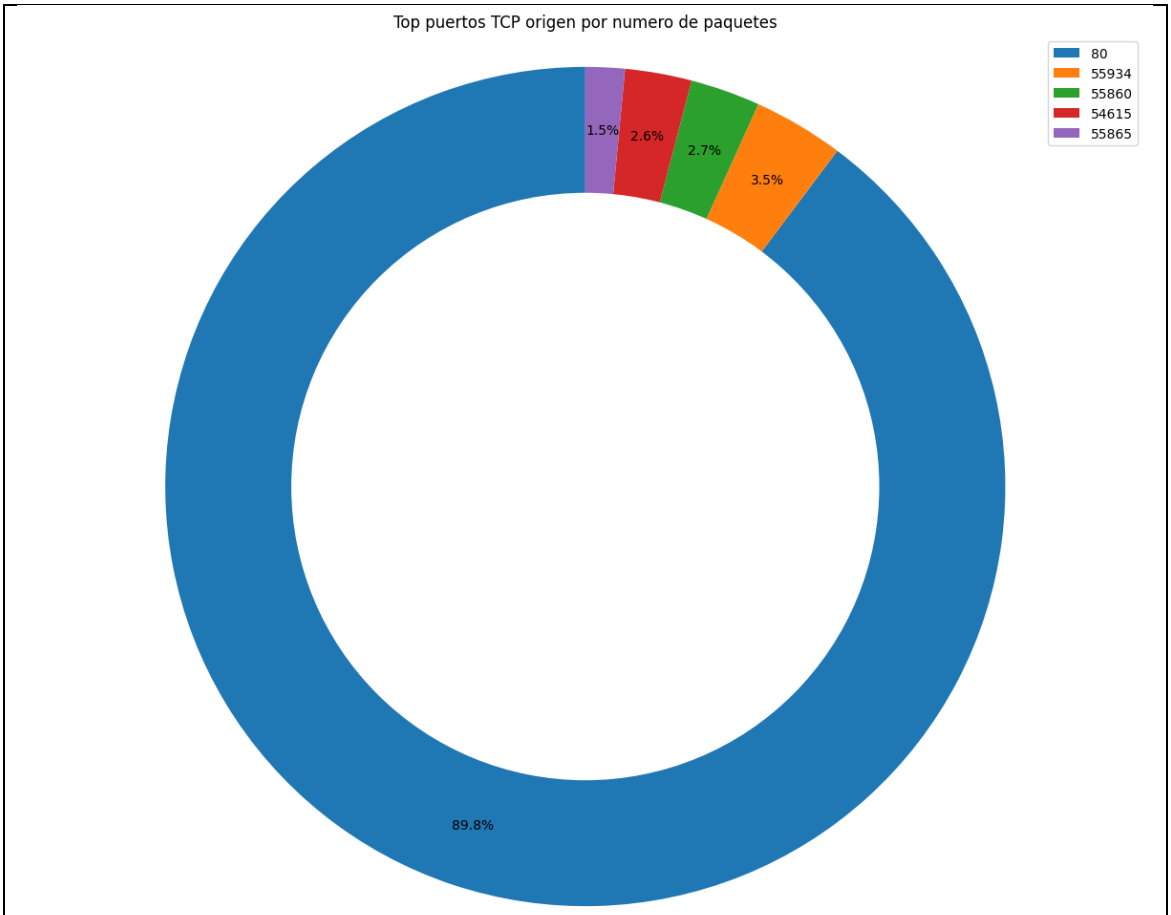
Filtro utilizado: ‘tcp and (not icmp)’.

De esta gráfica se obtiene que más del 99% de los bytes de TCP son enviados por el puerto 80.



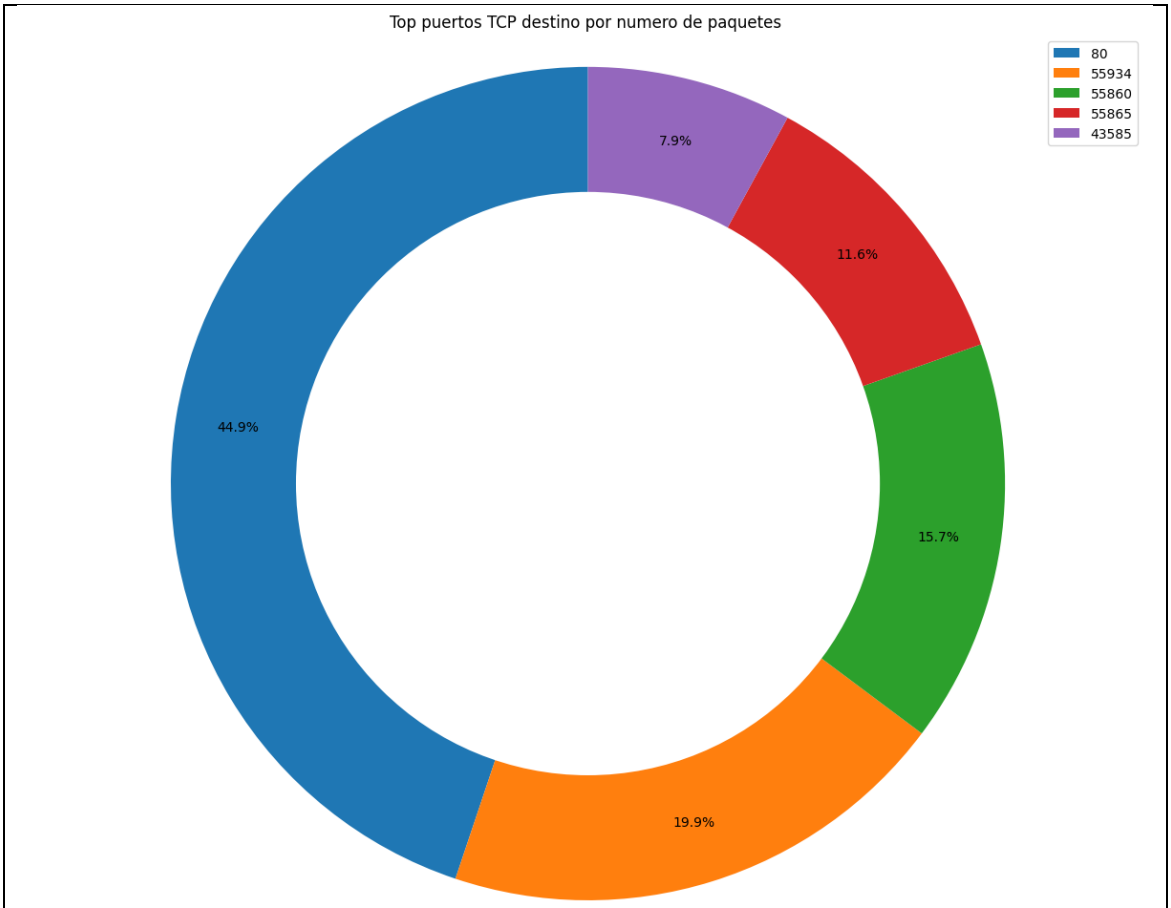
Filtro utilizado: ‘tcp and (not icmp)’.

La distribución de los bytes recibidos es mucho más equitativa, destacando los puertos 55934 y 55860 en primer y segundo lugar, respectivamente.



Filtro utilizado: ‘tcp and (not icmp)’.

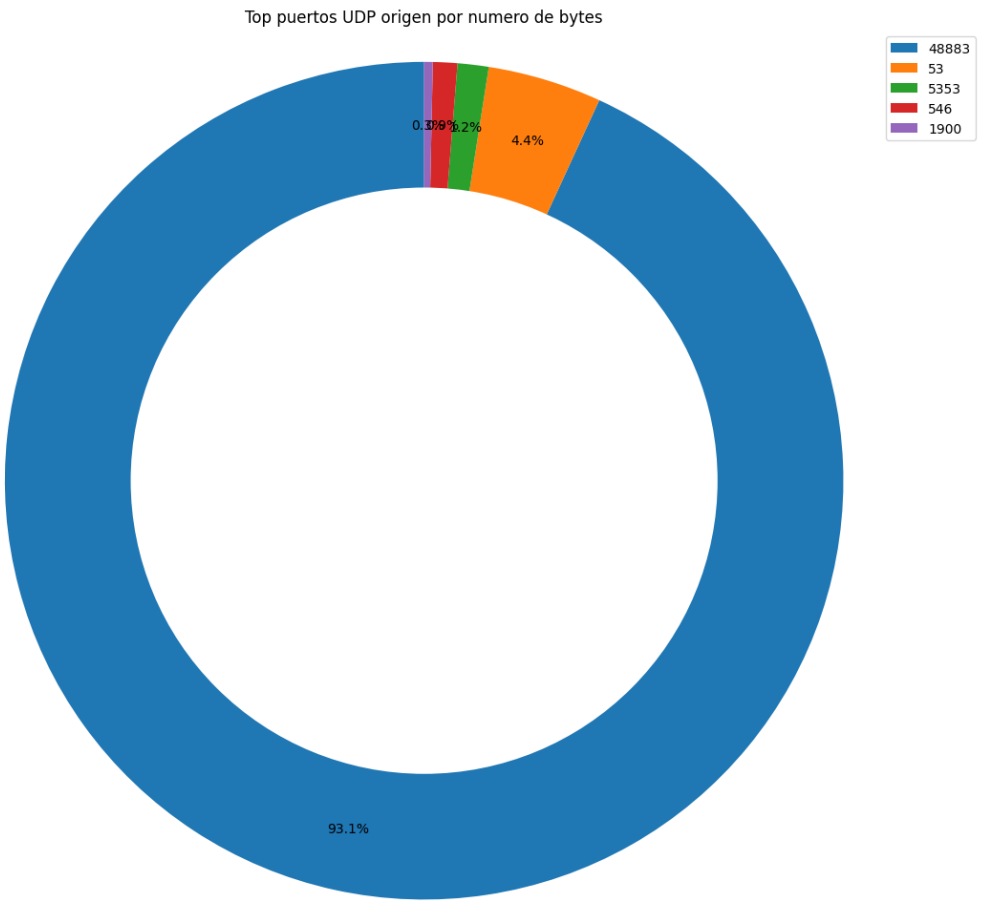
En el caso de contabilizar el número de paquetes, el puerto 80 es también el que más envía con una amplia diferencia.



Filtro utilizado: ‘tcp and (not icmp)’.

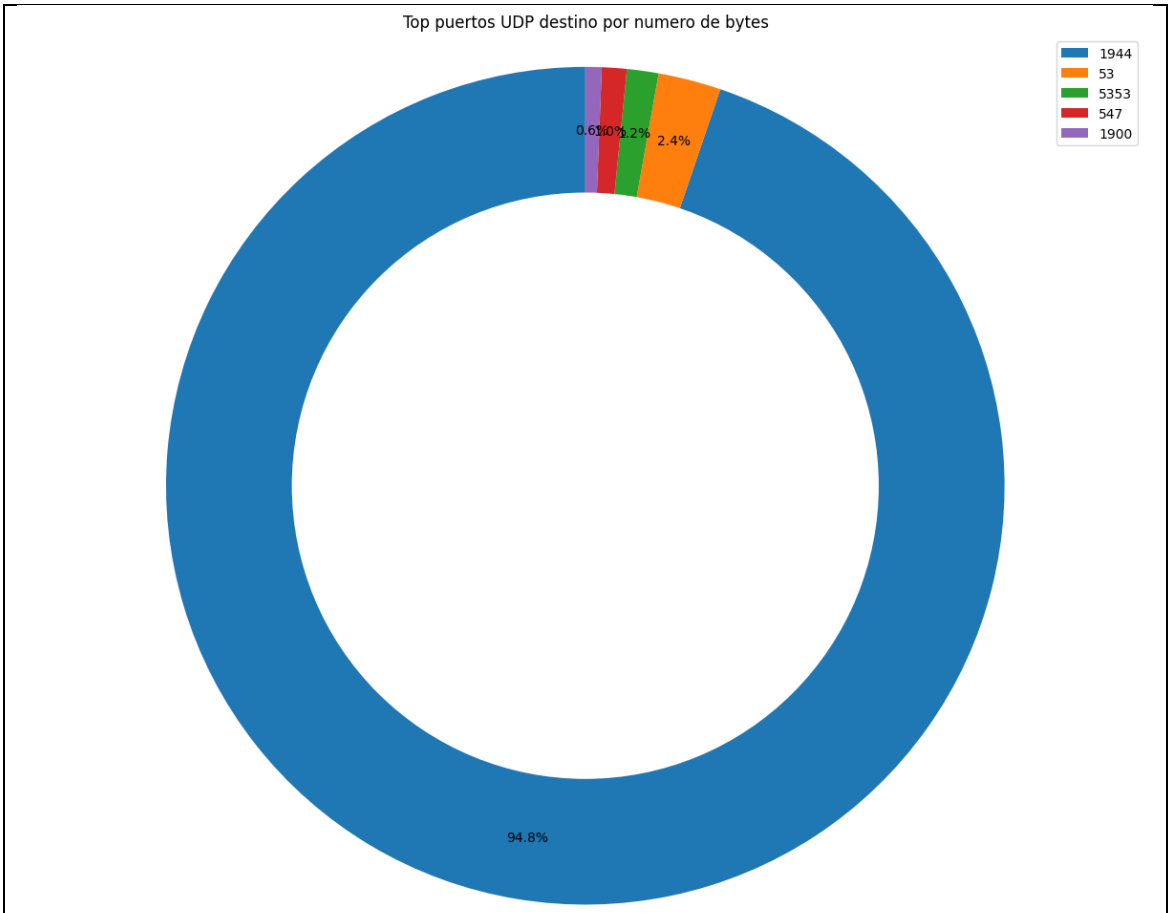
En el número de paquetes TCP recibidos aparece el puerto 80 como más relevante, que no se encontraba en el top de bytes recibidos. Esto indica que este puerto recibe muchos paquetes de muy pequeño tamaño.

UDP:



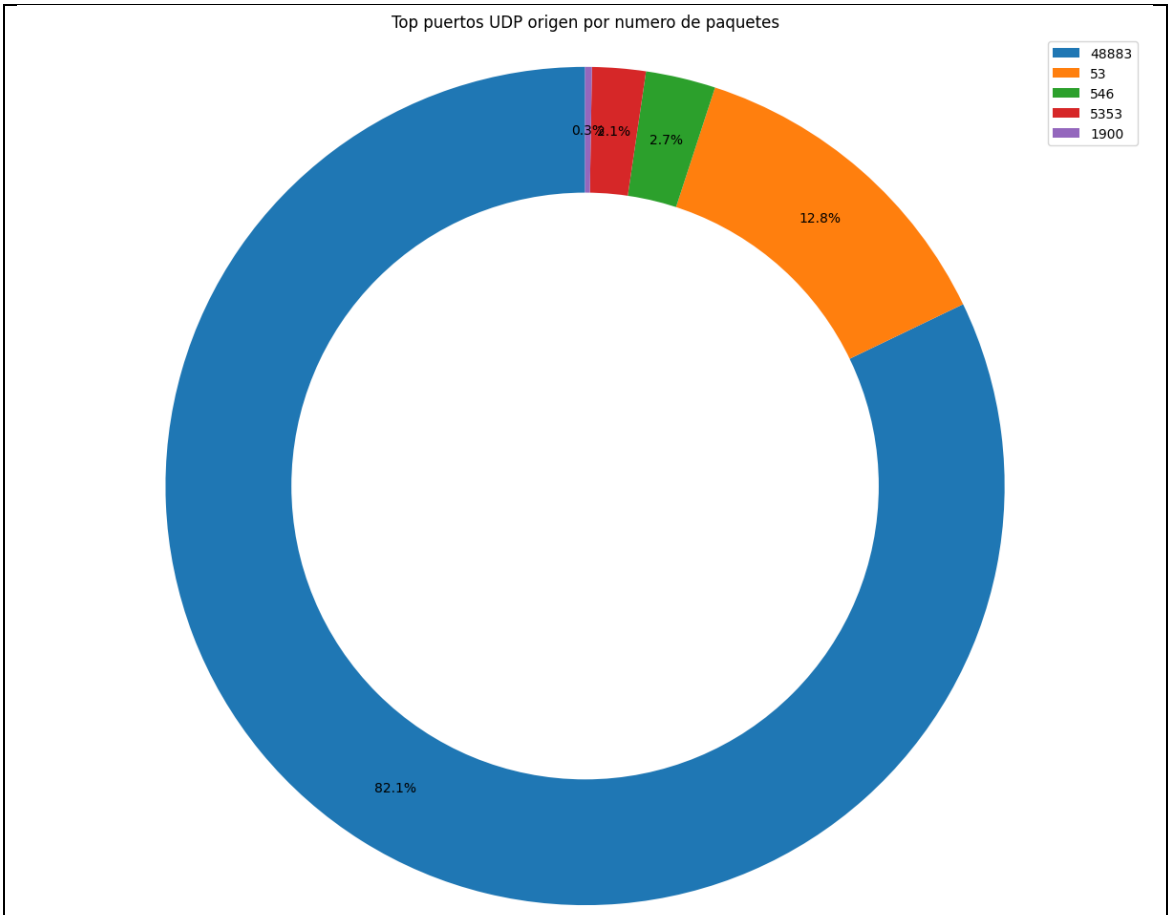
Filtro utilizado: ‘udp and (not icmp)’.

El puerto 48883 aparece en el gráfico de sectores como la mayor cantidad de bytes enviados por protocolo UDP con un 93,1%.



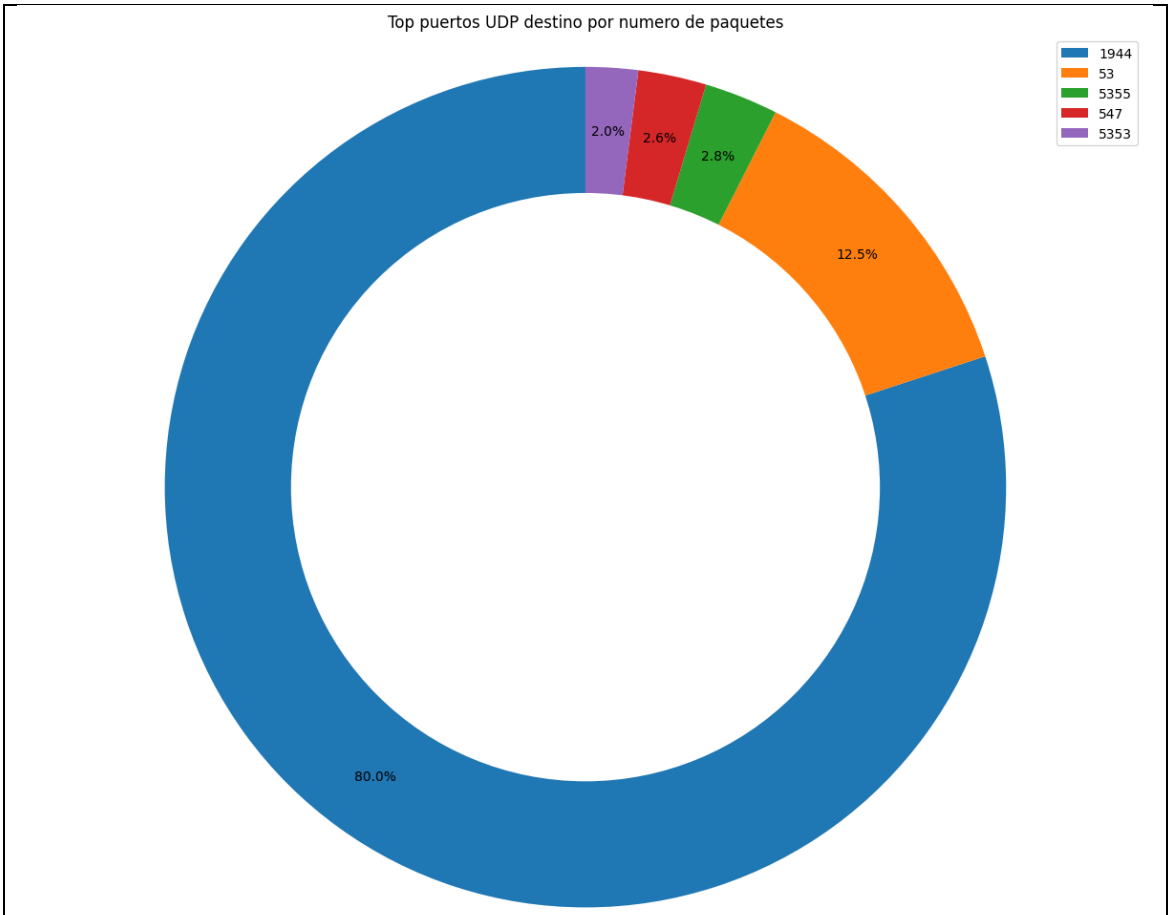
Filtro utilizado: ‘udp and (not icmp)’.

EL puerto 1944, con más de un 94% domina los bytes recibidos por UDP.



Filtro utilizado: ‘udp and (not icmp)’.

En cuanto a paquetes UDP se mantiene un orden muy similar al obtenido por cantidad de bytes para este protocolo.

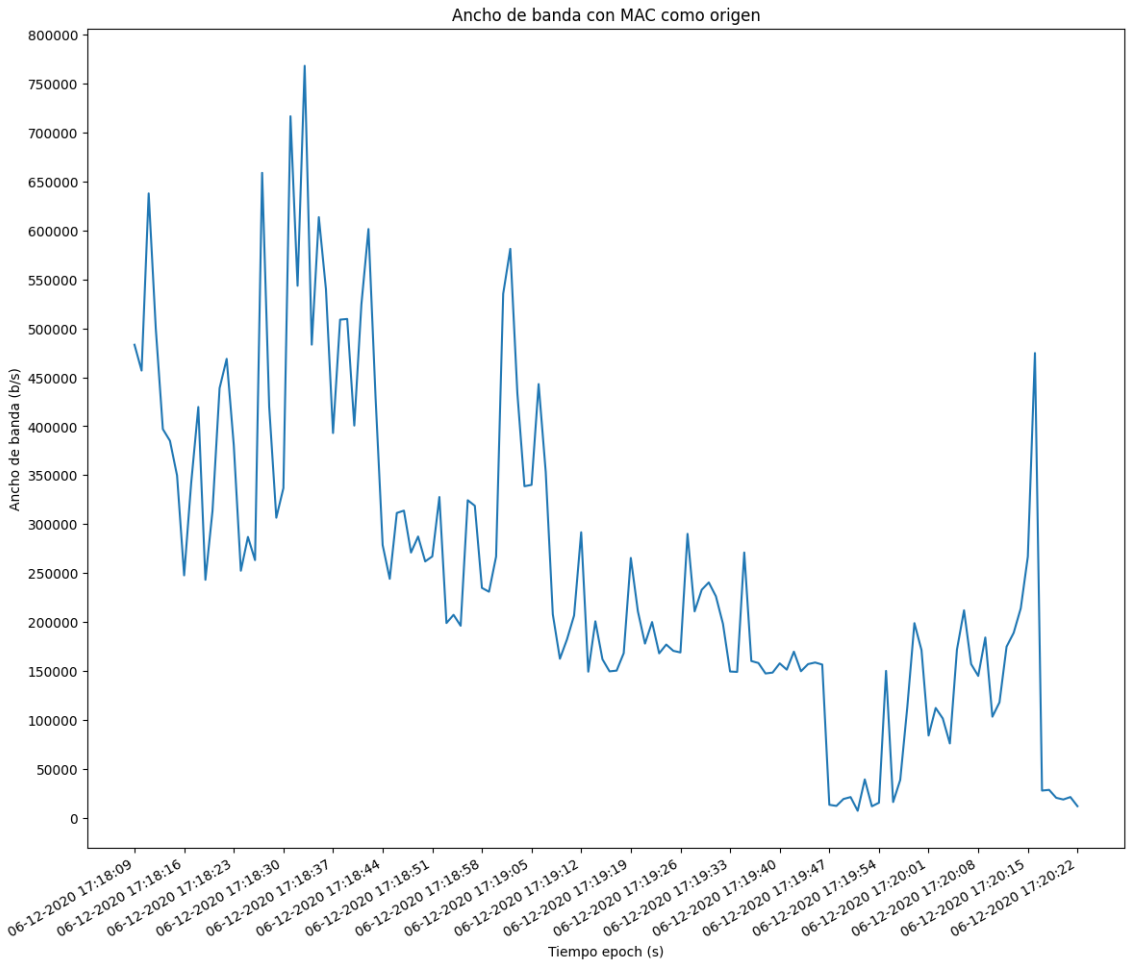


Filtro utilizado: ‘udp and (not icmp)’.

Por último, se ve en esta gráfica que se vuelve a mantener un resultado similar entre la proporción de bytes y la de paquetes en las primeras posiciones (pese a una reducción del porcentaje del puerto en primer lugar). Esto hace pensar, junto con los resultados anteriores, que el protocolo UDP forma paquetes con un tamaño más regular que otros protocolos como TCP.

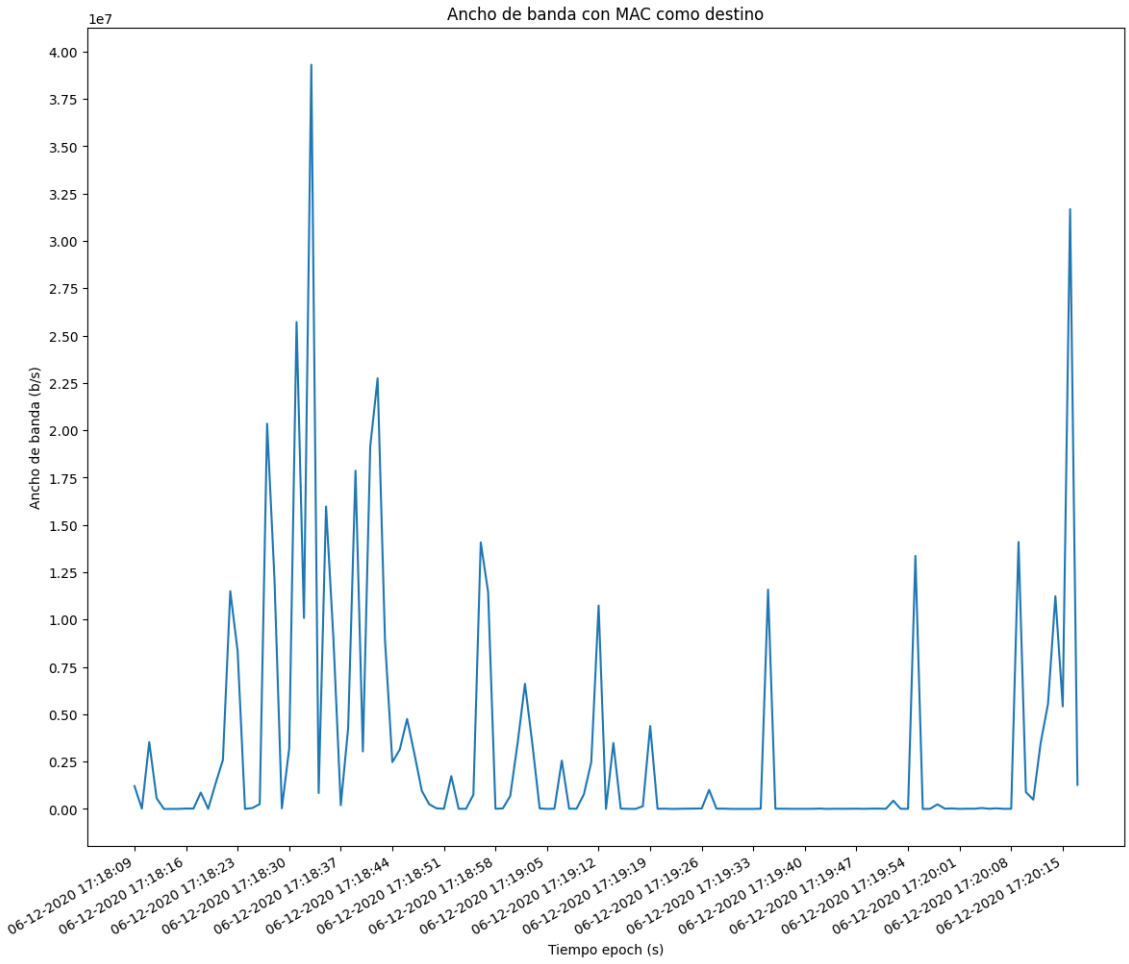
4. Series temporales de ancho de banda/tasa/caudal:

Dirección MAC: 00:11:88:CC:33:FC



Filtro utilizado: 'eth.src eq 00:11:88:CC:33:FC'.

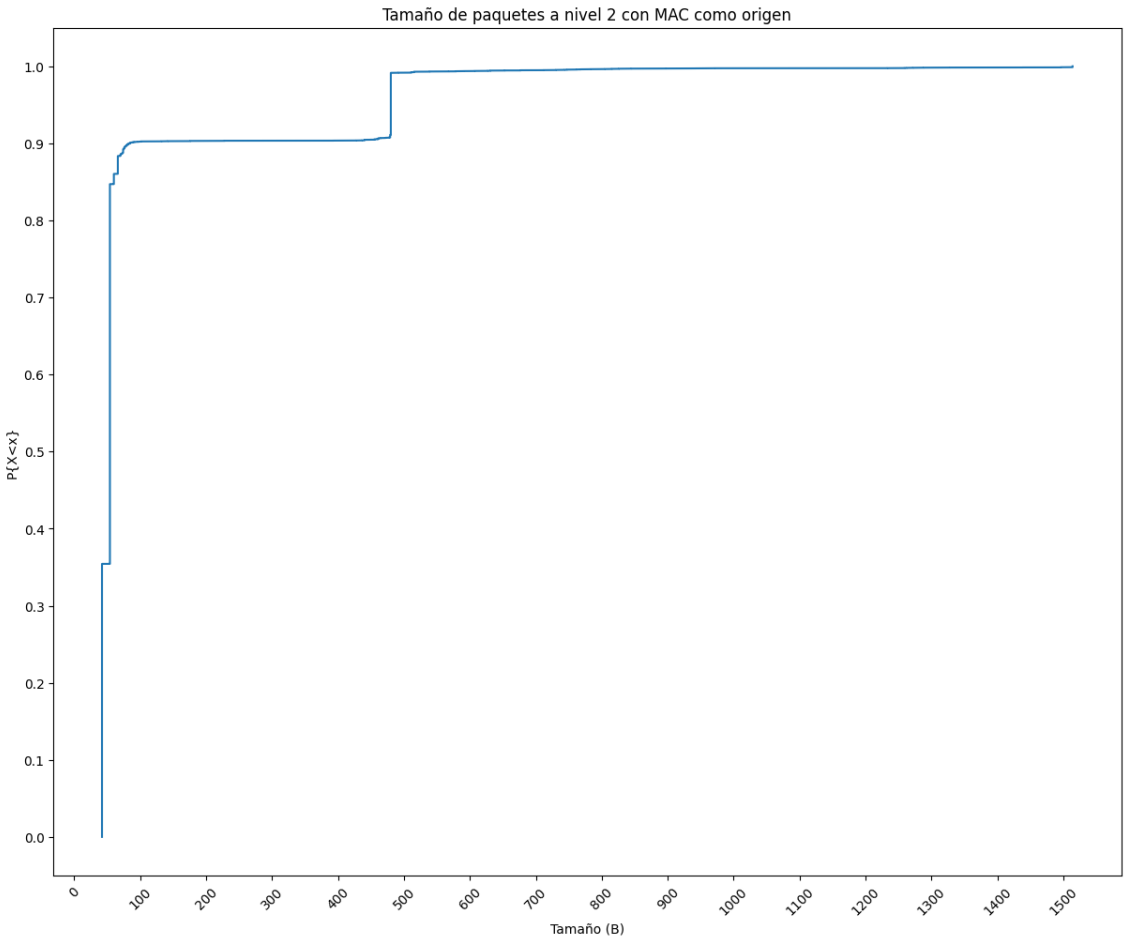
Se puede observar una tendencia descendente en el ancho de banda de salida de la MAC dada por el generador de trazas. Pese a ser bastante irregular, se aprecia claramente como con el tiempo los picos de mayor emisión son cada vez más bajos. Cabe destacar que el máximo ancho de banda consumido ronda los 775 kbps.



Filtro utilizado: ‘eth.dst eq 00:11:88:CC:33:FC’.

En cuanto al ancho de banda de llegada a nivel 2, hay irregularidades mucho mayores. Durante la mayoría del tiempo la gráfica toma valores relativamente bajos; sin embargo, se alcanzan picos con una tasa de b/s bastante mayor a la observada en el caso de salida. Esta irregularidad dificulta la observación de otros matices, ya que la escala hace imposible valorar correctamente los datos más pequeños. En este caso, el máximo ancho de banda consumido es de casi 4 Mbps, unas 5 veces mayor que el máximo ancho de banda de salida.

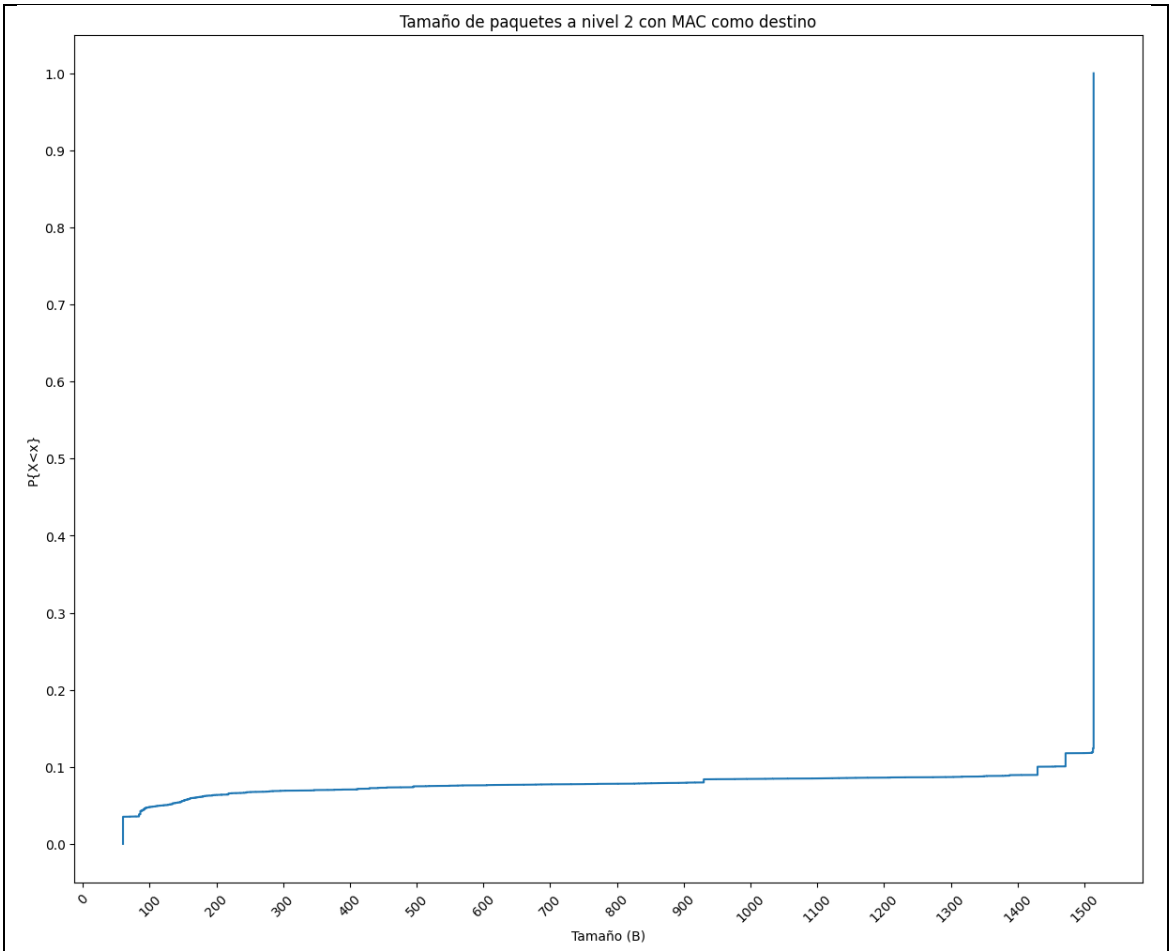
5. ECDFs de los tamaños de los paquetes



Filtro utilizado: ‘eth.src eq 00:11:88:CC:33:FC’.

Se aprecia que la probabilidad se concentra en los menores tamaños de paquete: cerca del 90% ocupan menos de 200 bytes. Los 2 tamaños más frecuentes (los “peldaños” más altos) son menores que 100 bytes y se corresponden aproximadamente al 85% de las tramas capturadas. Destaca el menor de estos, 60 bytes, pues es el tamaño mínimo de las tramas ethernet y esto supone que todos los paquetes de menos de 60 bytes de carga útil (más la cabecera ethernet) sean rellenados hasta este tamaño mínimo, como se había estudiado en la práctica 2.

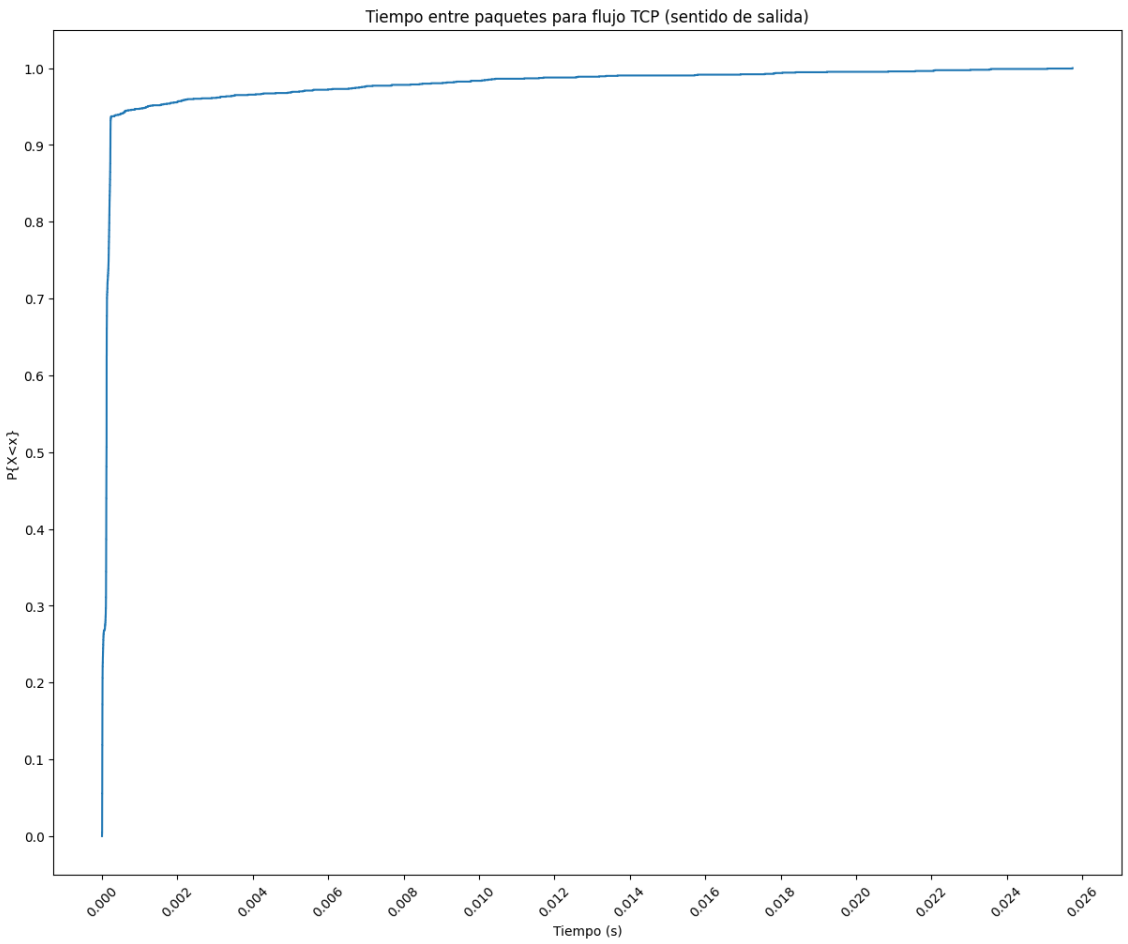
También resaltan los paquetes de en torno a 500 bytes al ser el tercer tamaño más frecuente. Prácticamente la totalidad de los paquetes tienen un tamaño menor o igual a 500 bytes.



Filtro utilizado: ‘eth.dst eq 00:11:88:CC:33:FC’.

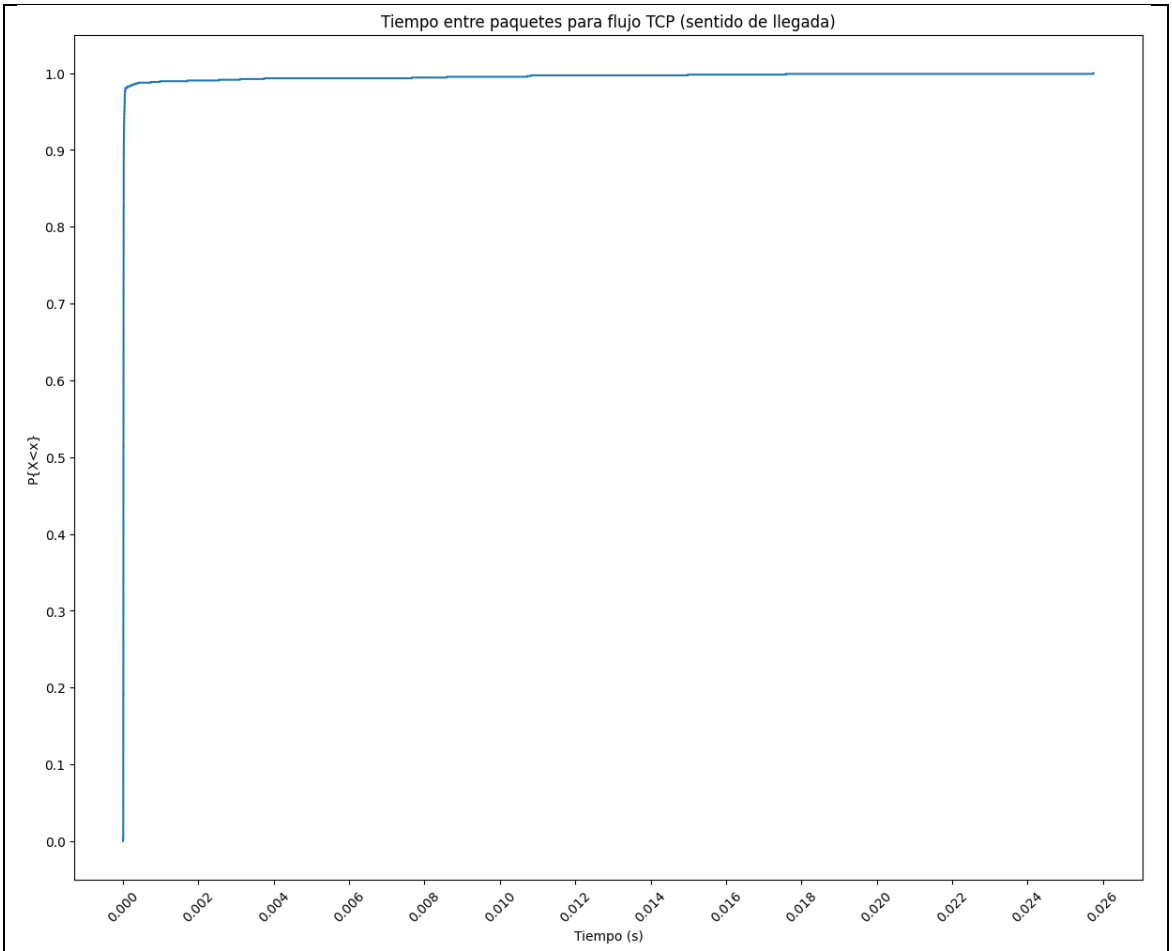
En esta gráfica se observa más claramente que en la anterior que el tamaño mínimo capturado está en torno a los 60 bytes y el máximo en torno a 1514 bytes, precisamente los tamaños mínimo y máximo de tramas ethernet estudiados en la práctica anterior. Se observa también que estos tamaños son los más frecuentes, particularmente las tramas de 1514 bytes representan más del 80% del total.

6. ECDF tiempos entre paquetes



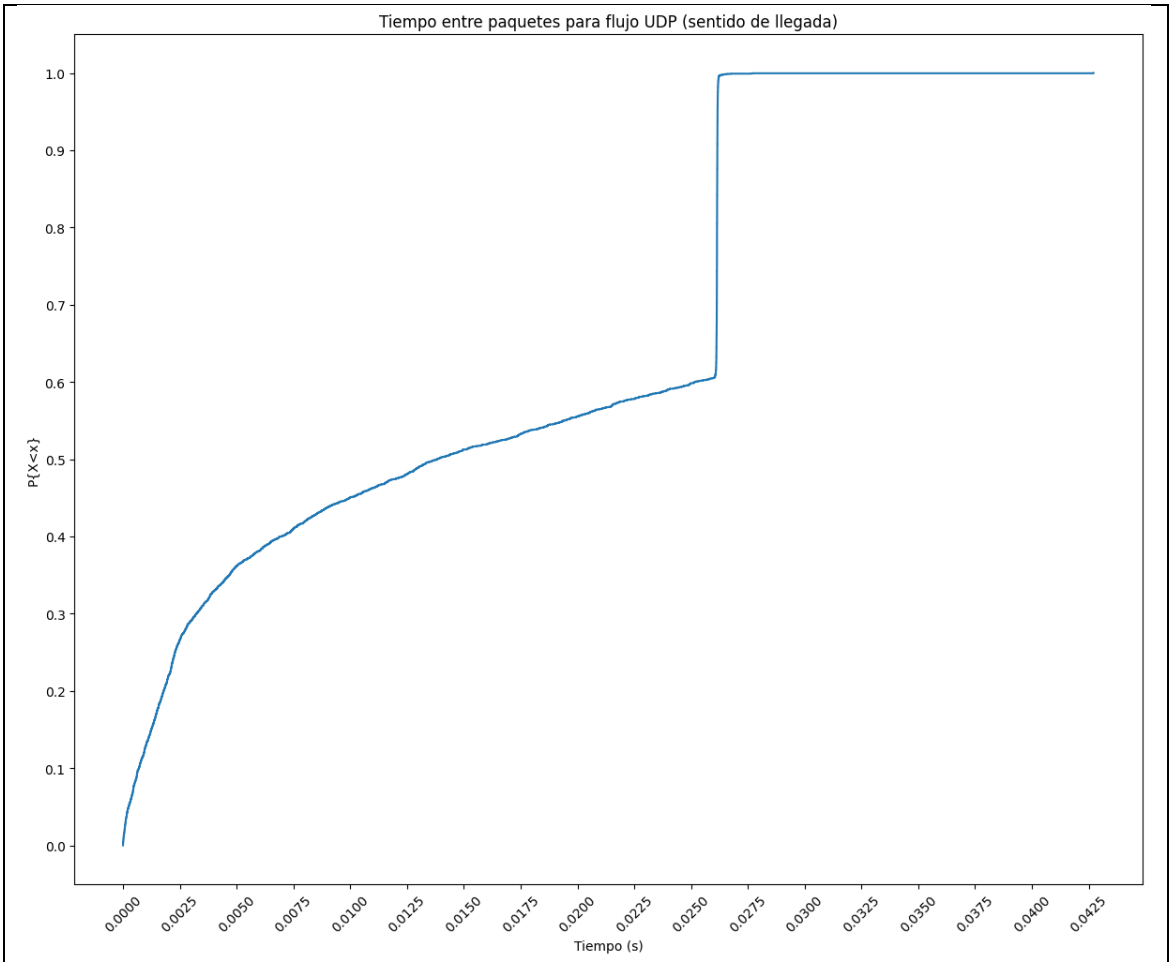
Filtro utilizado: 'ip.src eq 53.59.245.211 and (not icmp)'.

Se observa que poco menos del 95% de los *interarrivals* de los paquetes TCP que parten de la dirección IP dada son menores a un milisegundo. Este comportamiento se puede corresponder con el arranque lento de TCP, ya que consiste en aumentar la tasa de envío de forma exponencial, con lo que los *interarrivals* disminuyen rápidamente.



Filtro utilizado: 'ip.dst eq 53.59.245.211 and (not icmp)'.

De forma similar que en la gráfica anterior, poco más del 95% de los *interarrivals* de los paquetes TCP que parten de la dirección IP dada son menores a un milisegundo. De nuevo, esto puede ser producto del arranque lento de TCP visto desde el destino del tráfico.



Filtro utilizado: 'udp.srcport eq 1944 and (not icmp)'.

En la gráfica se aprecia que aproximadamente el 60% de los *interarrivals* de los paquetes UDP que llegan al puerto dado son menores a 25 milisegundos. Este 60% presenta valores bastante heterogéneos; la concavidad de este trozo de la curva indica que los menores tiempos entre llegadas son más frecuentes. Por otra parte, el 40% restante está concentrado casi totalmente en torno a los 26,5 milisegundos.

En definitiva, se observa que los *interarrivals* de los paquetes UDP tienden a ser mayores que los de los paquetes TCP. Esto puede deberse al nulo control de congestión que realiza UDP, o simplemente a que solo un 6% (aproximadamente) de los paquetes capturados son UDP, con lo que en general son más raros.

Cabe destacar que los datos referentes al flujo UDP que parte del puerto dado no se incluyen porque no hay paquetes UDP tales en la traza proporcionada. Esto concuerda con que, como se discutió anteriormente, el puerto 1944 sea el que más tráfico UDP haya recibido y que no figure en el top de puertos que más tráfico UDP hayan enviado.

3 Conclusiones

Tras haber realizado la práctica, se llega a conclusiones que pueden inscribirse en dos grupos.

En cuanto a la traza analizada, se observan varias diferencias entre los protocolos analizados (TCP y UDP). En primer lugar, la IP dada para analizar el flujo TCP es la 53.59.245.211, que se ha comprobado mediante un mayor análisis de la traza que se corresponde con el puerto 80. Este aparece en los análisis realizados como el que más bytes envía, pero no está entre los que más recibe. También es el que más paquetes envía y recibe. Sabiendo esto, parece razonable pensar que desde este puerto se transmite algún tipo de información a otro equipo (lo que supondría una gran cantidad de paquetes de tamaño sustancial), como podría ser algún tipo de contenido audiovisual. Como TCP es un protocolo con enlace bidireccional, en el que se envían paquetes para distintas funciones, desde aquí se envían y reciben un gran número de estos. Sin embargo, los paquetes recibidos son de menor tamaño, lo que podría ser debido a paquetes para control de error o solicitud de información y explicaría la ausencia de este puerto entre los que más bytes reciben. Adicionalmente, se ha comprobado mediante Wireshark que la dirección MAC empleada en las series temporales se corresponde con la IP que se comunica con el puerto 80. Las series temporales muestran una recepción de paquetes de gran tamaño y emisión de paquetes más pequeños. Este resultado es coherente con la hipótesis anterior, ya que este equipo recibiría la información retransmitida desde el puerto 80 y tan solo enviaría solicitudes y control de errores.

Por otra parte, el puerto UDP 1944, cuyo flujo se ha analizado previamente, figura como el mayor receptor de bytes y paquetes, pero no aparece en ningún caso como emisor. Esto se trata de un claro ejemplo del concepto de UDP. Este protocolo no establece enlaces y no recibe ninguna respuesta, es unidireccional. Esto se refleja claramente en que el puerto recibe información pero no responde. El hecho de no producirse una “conversación” entre dos terminales con paquetes de tamaños claramente distintos (como se ha visto en TCP) refuerza la idea de una mayor uniformidad en los tamaños de paquetes UDP, como ya se comentó en apartados anteriores.

Finalmente, cabe comentar respecto al nivel de red la predominancia casi total del protocolo IPv4 frente a IPv6. Si la traza analizada es representativa de la internet entera, se observa que el uso de direcciones IP de tan solo 32 bits (2^{32} direcciones) sigue siendo ampliamente común pese a haber más equipos en la red que direcciones disponibles. Esto explica los incentivos que ofrecen organizaciones como la ICANN a los ISPs que apoyen la transición a IPv6, que cuenta con un número de direcciones a asignar suficiente para suplir la demanda actual (con direcciones de 128 bits, existen 2^{128} direcciones IPv6). De hecho, la ICANN prevé que IPv6 será más longevo que IPv4, es decir, dentro de unos 30 años habrá aún direcciones IPv6 disponibles.

En cuanto al trabajo realizado, queda en evidencia que la monitorización pasiva tiene una amplia utilidad en la gestión de redes y que está lejos de ser una labor trivial, pues el valor de los datos, mediciones y estadísticas radica precisamente en su análisis e interpretación, que finalmente desembocan en la identificación y corrección de errores y en general en un mejor funcionamiento de las redes.