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

Turno y pareja: 1391, P05

Integrantes:

Ángel Casanova Bienzobas

Rodrigo Juez Hernández

Fecha de entrega: 14/12/2020

Contenido

1 Introducción

En esta práctica hemos desarrollado el trabajo de gestores de red, analizando una traza. Para poder comentar el comportamiento de la red, hemos elaborado varios gráficos donde mostramos el uso más concurrente que realizan los usuarios de esta red.

A continuación, comentáremos los resultados obtenidos en cada campo analizado

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
98.96928353090286	1.0307164690971433

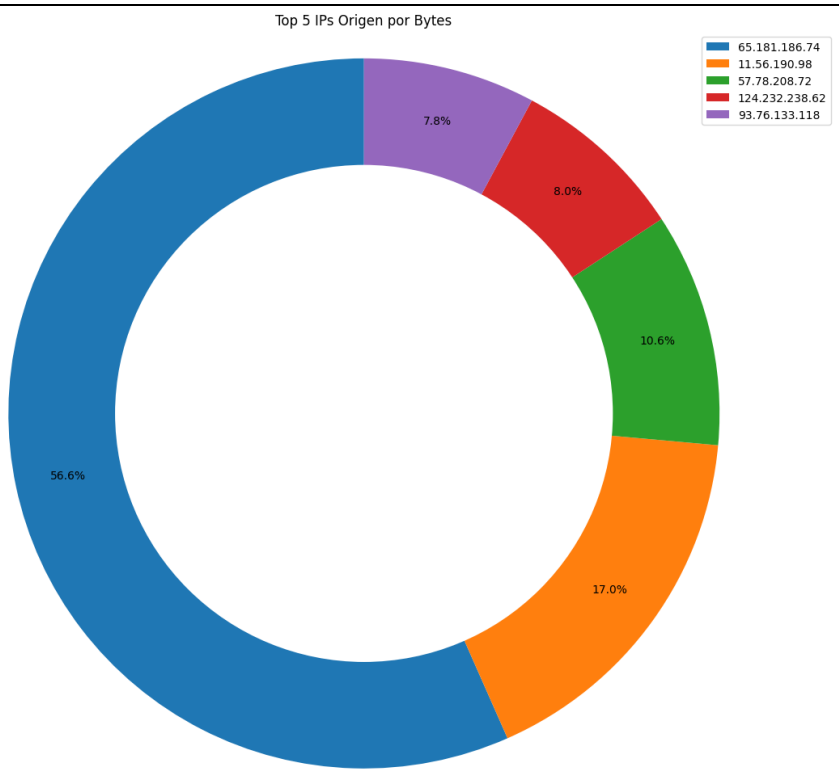
Para obtener los paquetes IP hemos usado 'ip' Para obtener los paquetes NO IP hemos usado 'ip'

   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
92.99233507222358	5.565076555114032	1.4425883726623852

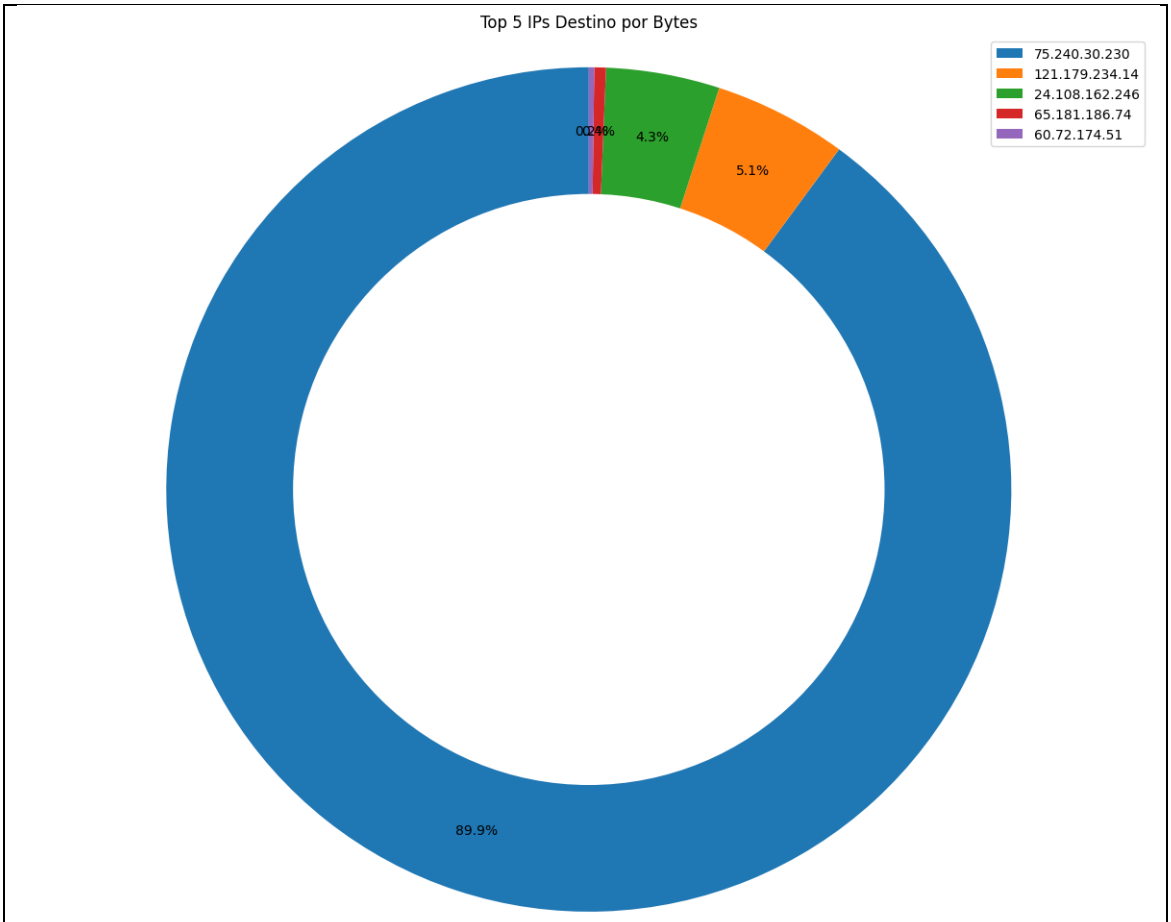
Para obtener los paquetes IP/TCP hemos usado '(ip) && (ip.proto eq TCP)'. Para obtener los paquetes IP/UDP hemos usado '(ip) && (ip.proto eq UDP)'. Para obtener todos los paquetes que, siendo IP, no eran ni TCP ni UDP, sencillamente hemos restado 100 - (porcentaje de TCP + porcentaje UDP).

2. Obtención de top 5 de direcciones IP



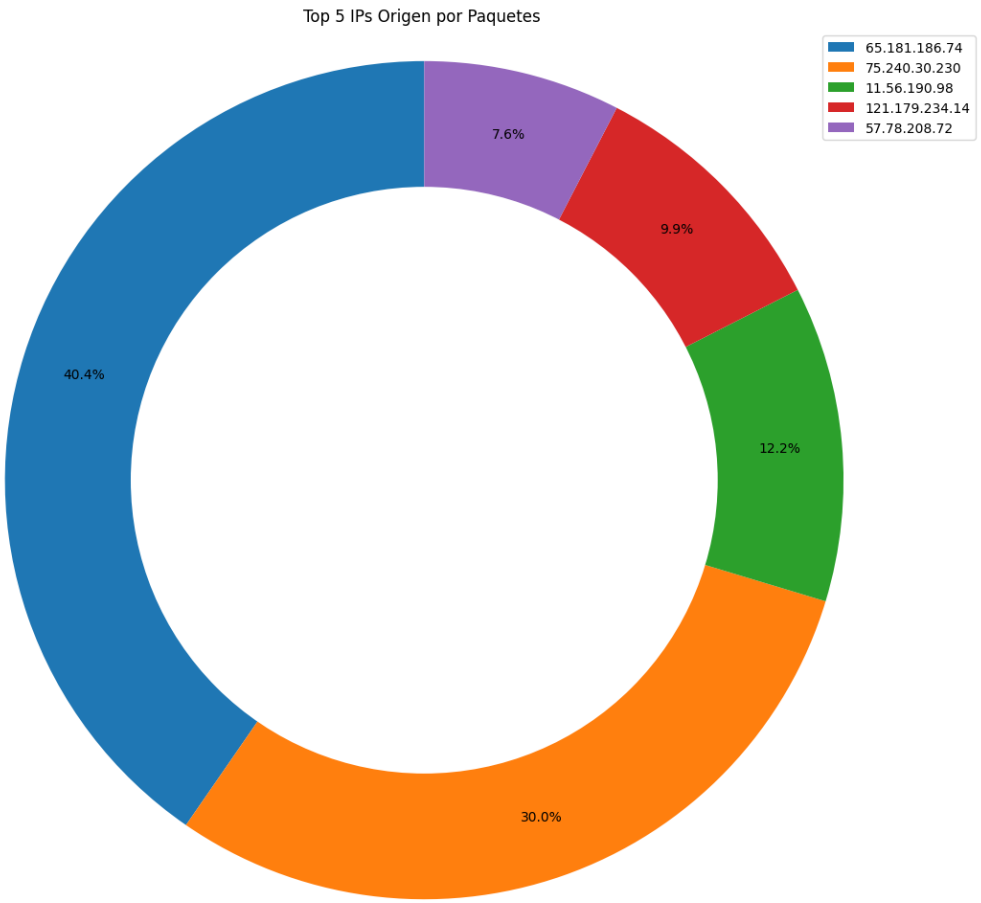
tshark -T fields -e ip.src -e frame.len -Y 'ip'

En esta grafica podemos observar que la ip 65.181.186.74, es la dirección ip origen que más volumen de datos genera, por lo tanto, es la que más hace uso de la subida, puede que este subiendo un archivo, o emitiendo un streaming.



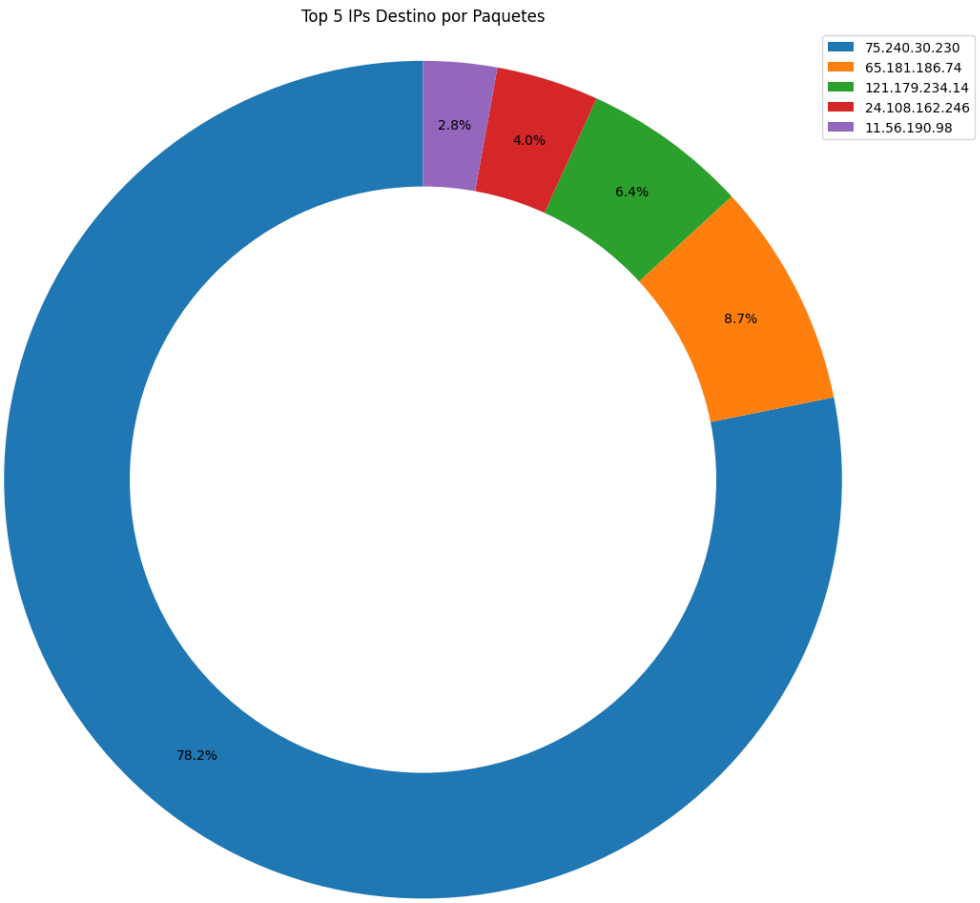
tshark -T fields -e ip.dst -Y ' ip '

La ip **75.240.30.230** es la que más bytes genera como destino, esto podría ser porque este viendo una película en una plataforma, o descargando un archivo muy grande.



tshark -T fields -e ip.src -e frame.len -Y ' ip '

Ahora, comparando las ip’s más usadas por número de paquetes en lugar de por bytes enviados, podemos ver que hay una cierta similitud entre las tartas, aunque no tendría que ser necesariamente así, ya que un usuario podría mandar muchos paquetes pequeños como, por ejemplo, paquetes para confirmar la recepción de un contenido mientras que otro usuario podría estar descargando un fichero de varios GiB que generarían tráfico de paquetes de 1514B (que es máximo)



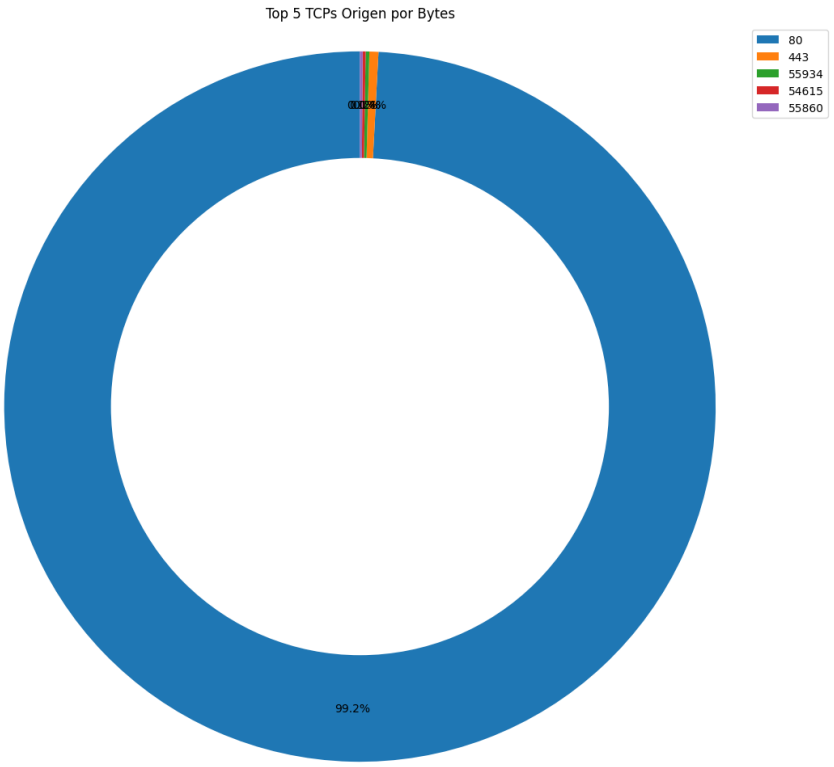
tshark -T fields -e ip.dst -e frame.len -Y ' ip '

Al igual que en grafico de origen, podemos observar una similitud entre el tráfico por bytes y por paquetes, lo que significa que la mayoría de los paquetes recibidos por ip tienen que tener un tamaño similar.

El hecho de que una ip destino, ocupe una gran tasa del espacio total de direcciones, no es preocupante, ya que puede tratarse de una página web grande usada por múltiples usuarios como (Amazon, gmail ...) o a una descarga masiva donde un usuario a pedido muchos paquetes a la misma página.

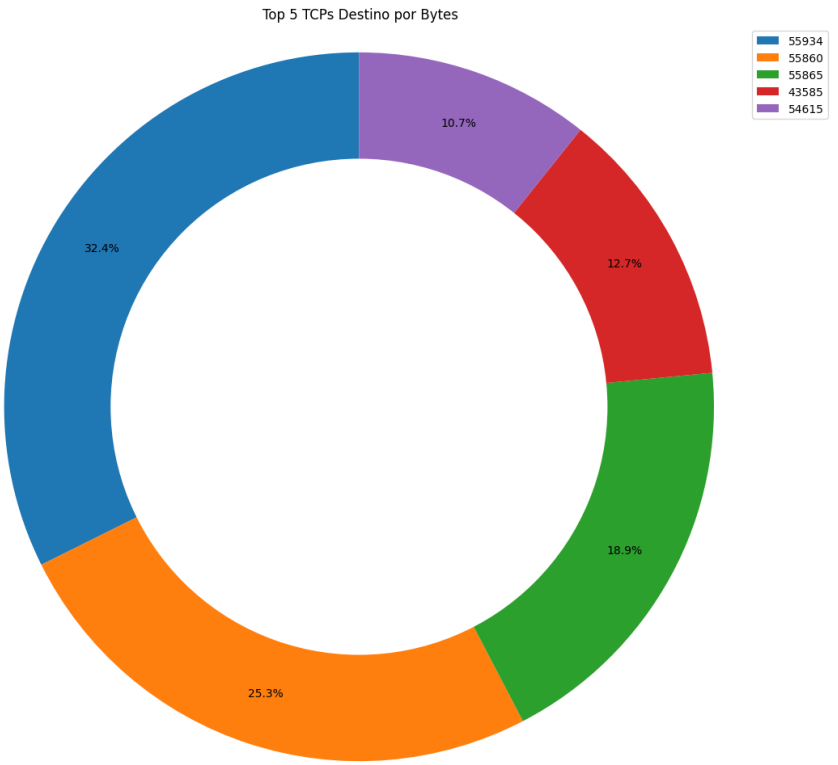
3. Obtención de top 5 de puertos:

TCP:



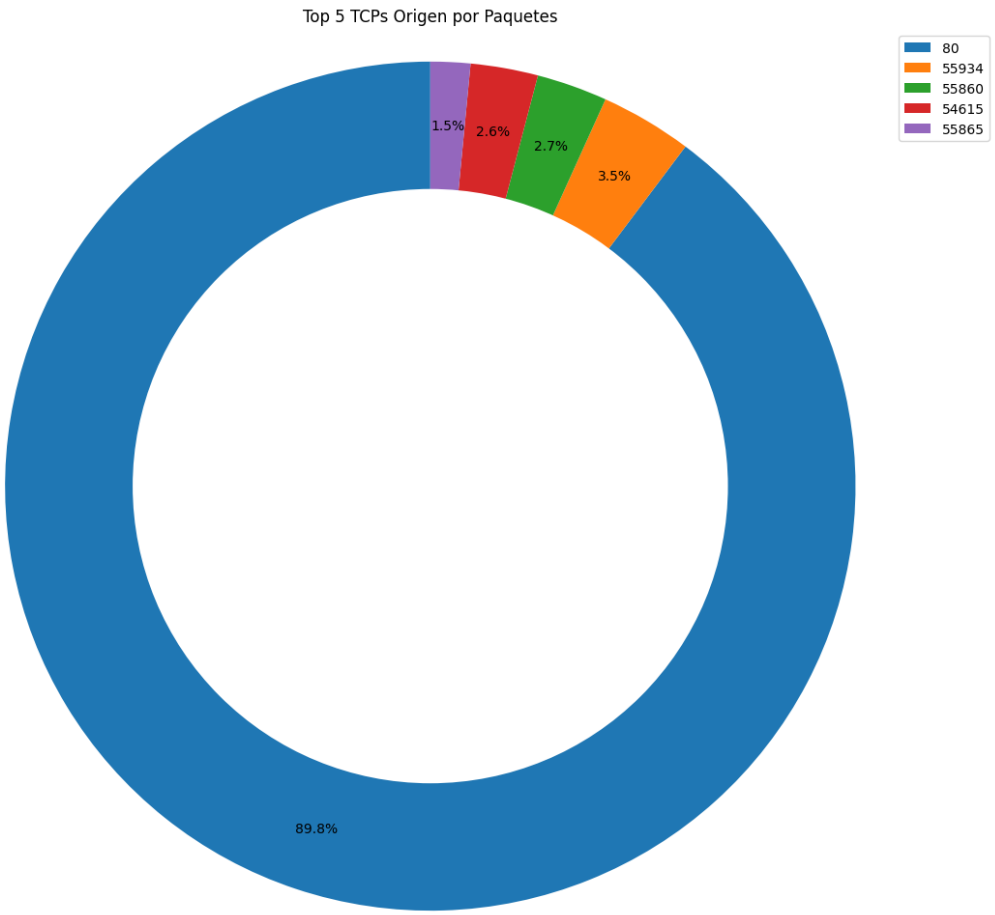
tshark -T fields -e tcp.srcport -e frame.len -Y '(ip) && (ip.proto eq TCP)'

El puerto 80 es prácticamente el único que se usa, probablemente esto se deba a que estamos analizando una red que solo se usa para sitios web, ya que el puerto 80 es el que utiliza el protocolo http.



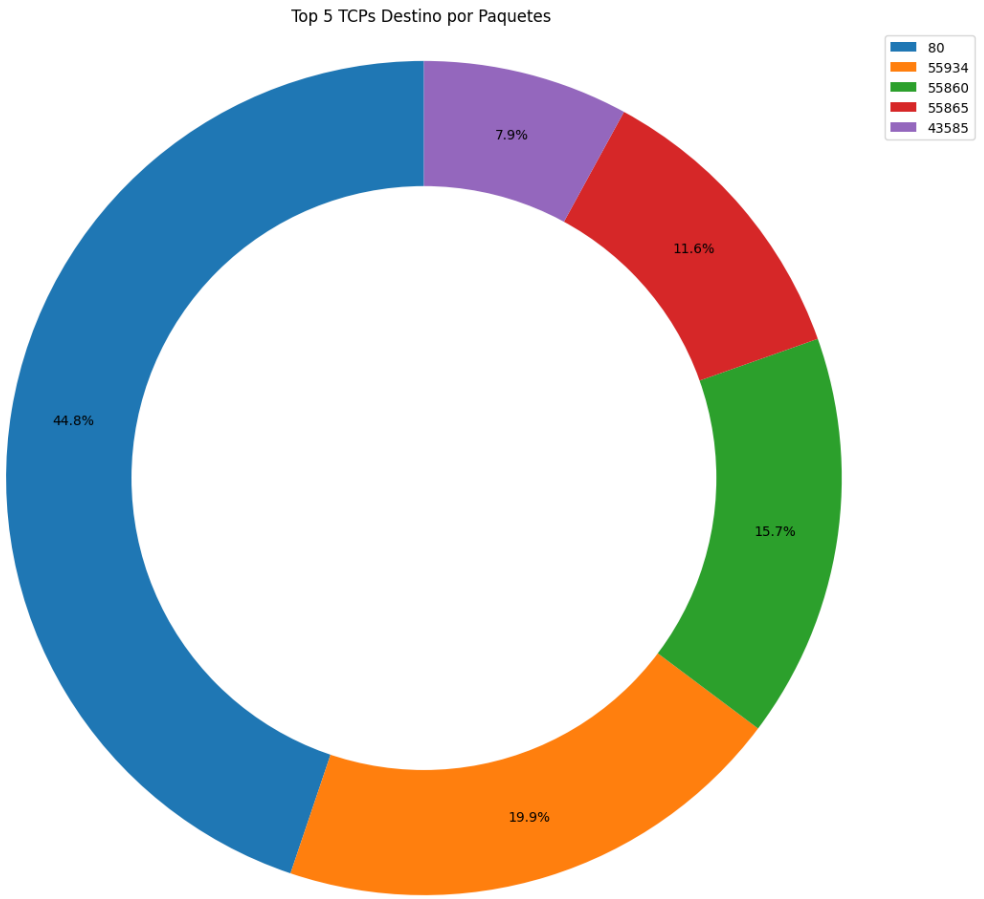
tshark -T fields -e tcp.dstport -e frame.len -Y '(ip) && (ip.proto eq TCP)'

Los puertos de destino TCP a diferencia de los Ip, son bastante heterogéneos, esta diferencia se debe a que los diversos usuarios han hecho un uso distinto de la red, conectándose a diferentes entornos de internet, por ejemplo, uno de los puertos podría ser utilizado por una videoconsola y otro de ellos el de algún servicio de televisión diferido (Netflix, Hbo ...). Este enfoque explica que el tráfico TCP este tan repartido.



tshark -T fields -e tcp.srcport -e frame.len -Y '(ip) && (ip.proto eq TCP)'

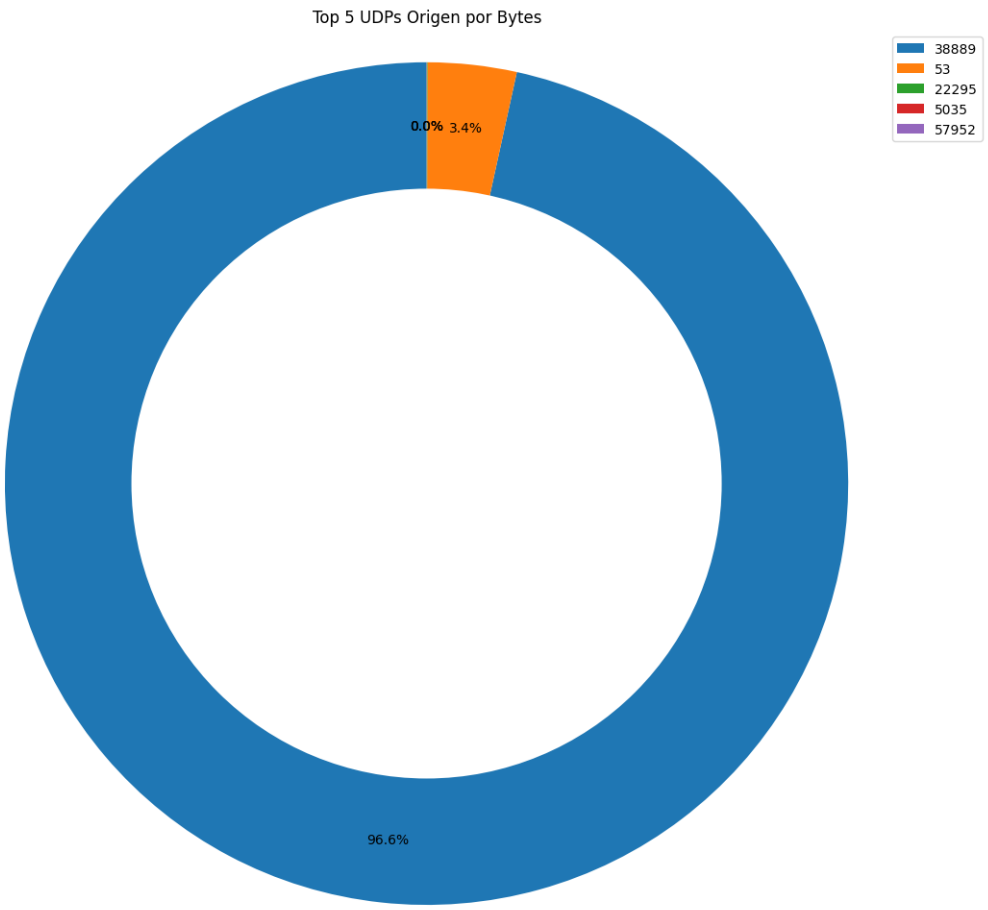
Al igual que el top 5 por bytes, el puerto 80 es el más solicitado por los usuarios de la red, lo que nuevamente podemos confirmar que prácticamente el 90% de los paquetes, pertenecen a paquetes enviados por usuarios, lo que confirma que el estado de la red es satisfactorio.



tshark -T fields -e tcp.dstport -e frame.len -Y '(ip) && (ip.proto eq TCP)'

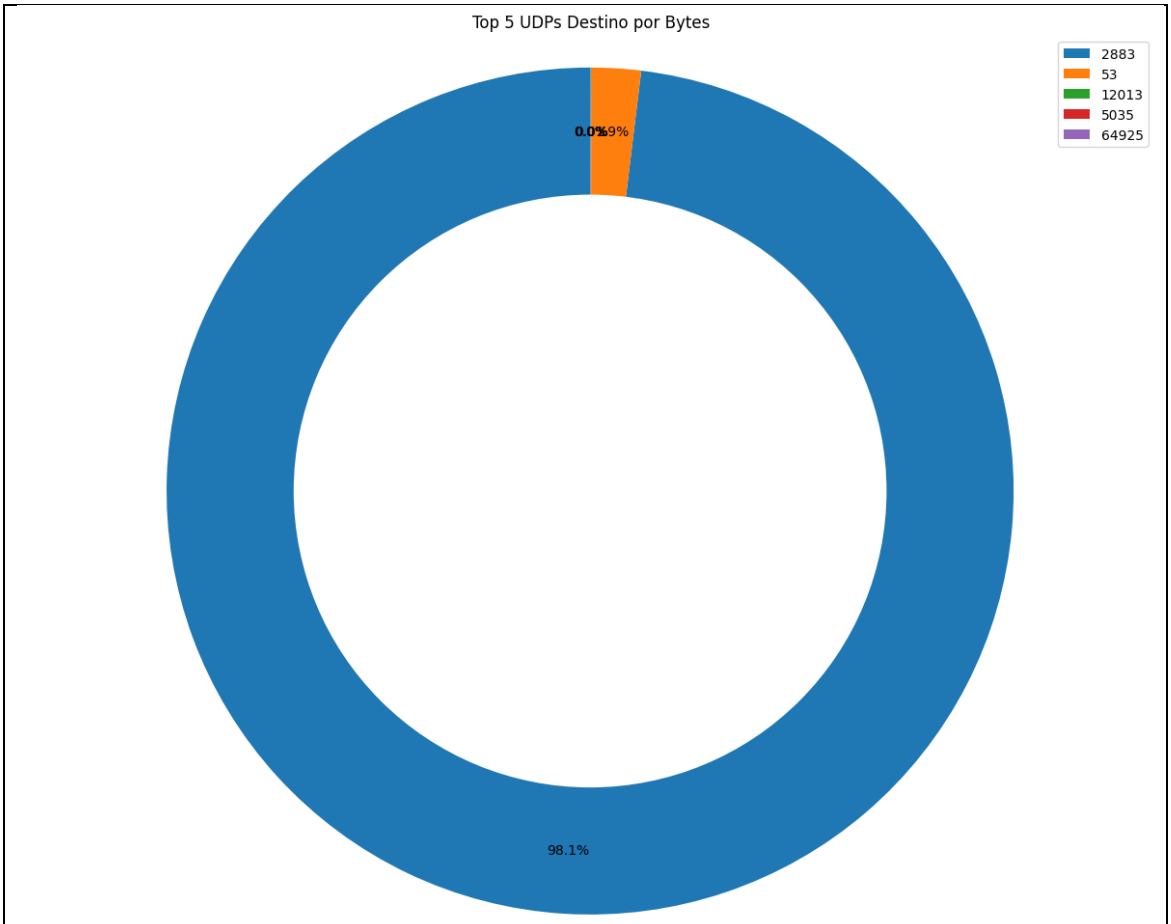
Aunque debido a su importancia en la web, el puerto 80 siga manteniendo su hegemonía, podemos observar que, si nos referimos a destinos, el uso de la red es más amplio, ya que cada vez más aplicaciones hacen uso de puertos propios a través de internet, pero sin usar la web como tal.

UDP:



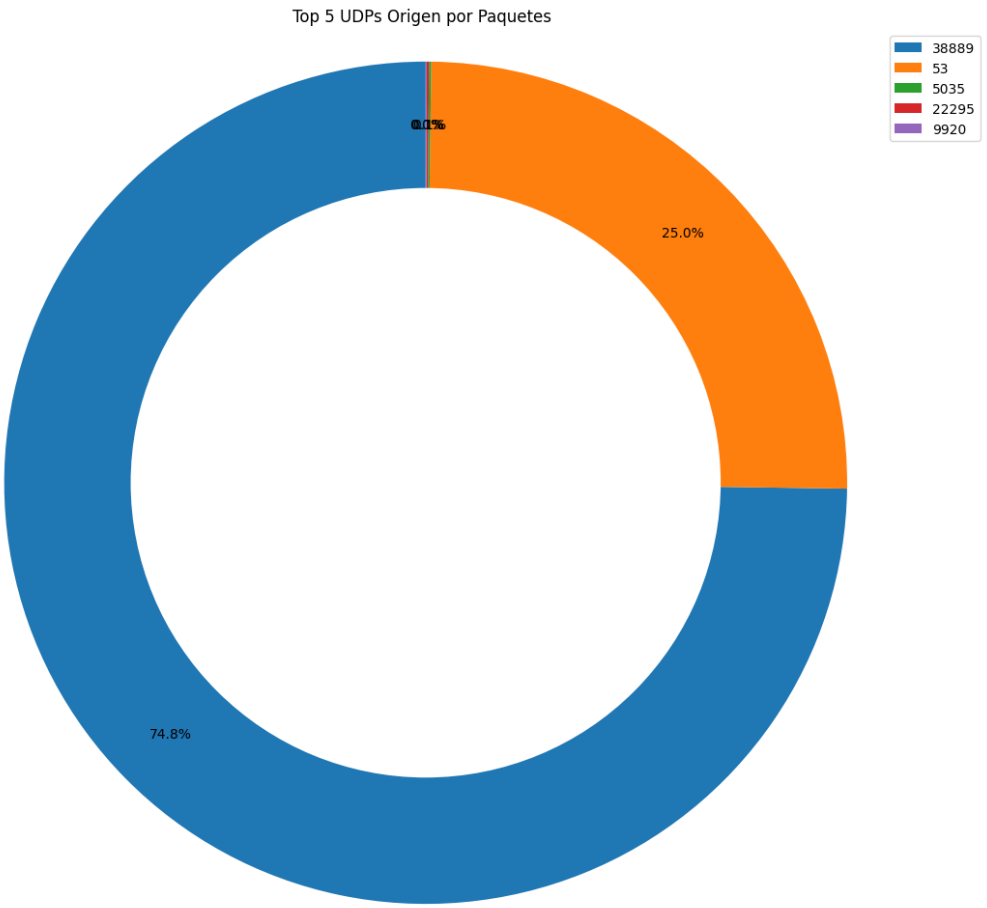
tshark -T fields -e udp.srcport -e frame.len -Y '(ip) && (ip.proto eq UDP)'

El puerto más usado es el 38889, este puerto es usado por paquetes VLAN, esto es debido a que esta misma gráfica, pero sin incluir paquetes VLAN (es decir sustituyendo el filtro ip por eth.type eq 0x8000) da que 53 es el más usado. El 53 es el DNS así que tiene sentido que este entre los más usados.
No hemos podido identificar ningún uso para ese puerto (38889) en internet, por lo que podría asociarse a cualquier servicio.



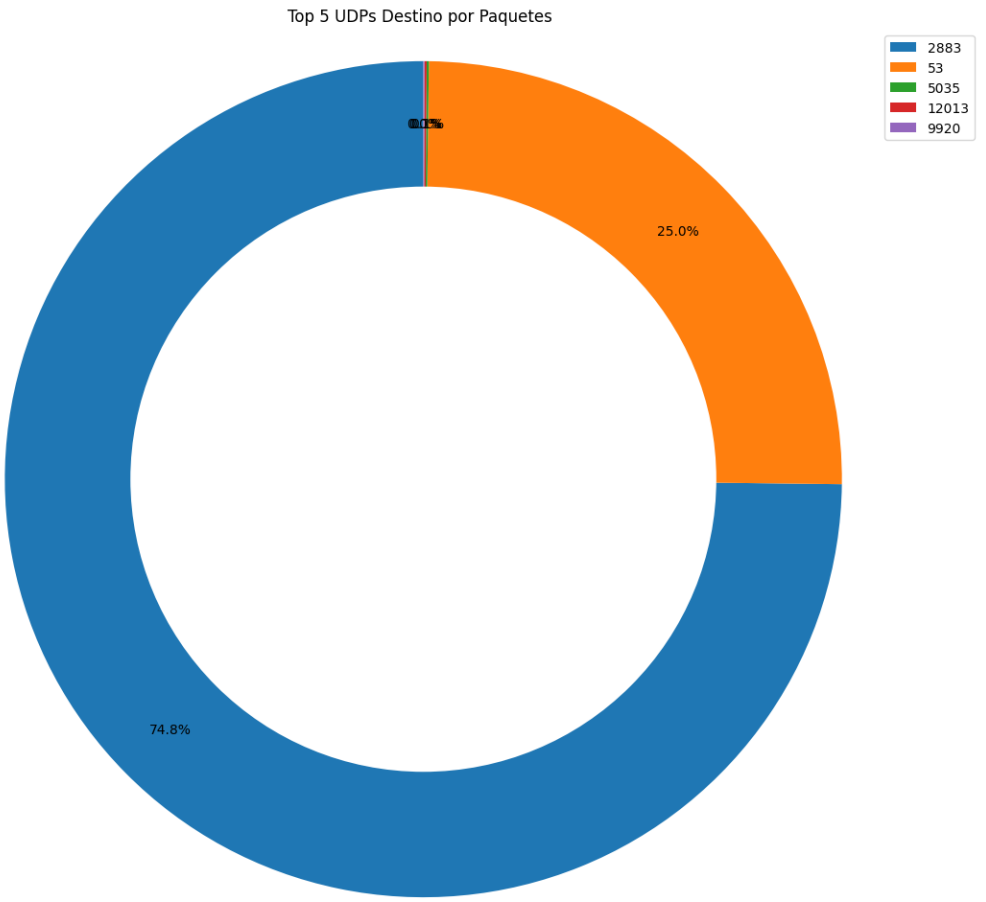
tshark -T fields -e udp.dstport -e frame.len -Y '(ip) && (ip.proto eq UDP)'

De nuevo se puede observar que se navega mucho por internet en esta red puesto que la DNS está en el top, sin embargo, el 2883 monopoliza las entradas en esta red. De nuevo hemos buscado si algún servicio usa este puerto, pero no lo hemos encontrado.



tshark -T fields -e udp.srcport -e frame.len -Y '(ip) && (ip.proto eq UDP)'

Se puede ver que hay un 25% de paquetes al puerto 53, esto es porque como son peticiones al DNS, sin embargo, el grueso de los paquetes, lo usa el puerto 38889, que como hemos comentado anteriormente, concentraba la mayoría de los paquetes VLAN.

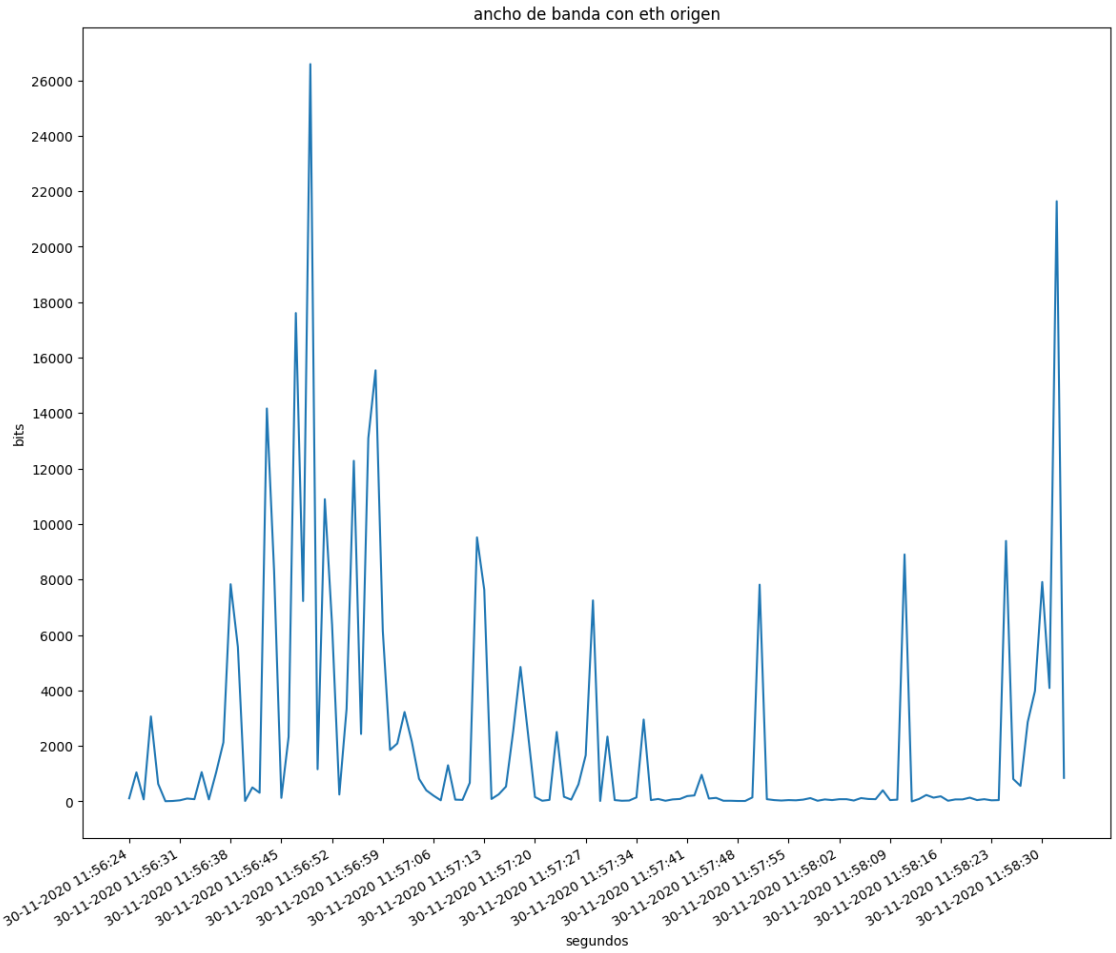


tshark -T fields -e udp.dstport -e frame.len -Y '(ip) && (ip.proto eq UDP)'

Al igual que en el tráfico por origen, aquí también se utiliza la misma cantidad de veces el puerto destinado al DNS, y el 2883, que es por donde se están recibiendo la mayoría de los paquetes UDP, se corresponde con paquetes VLAN.

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

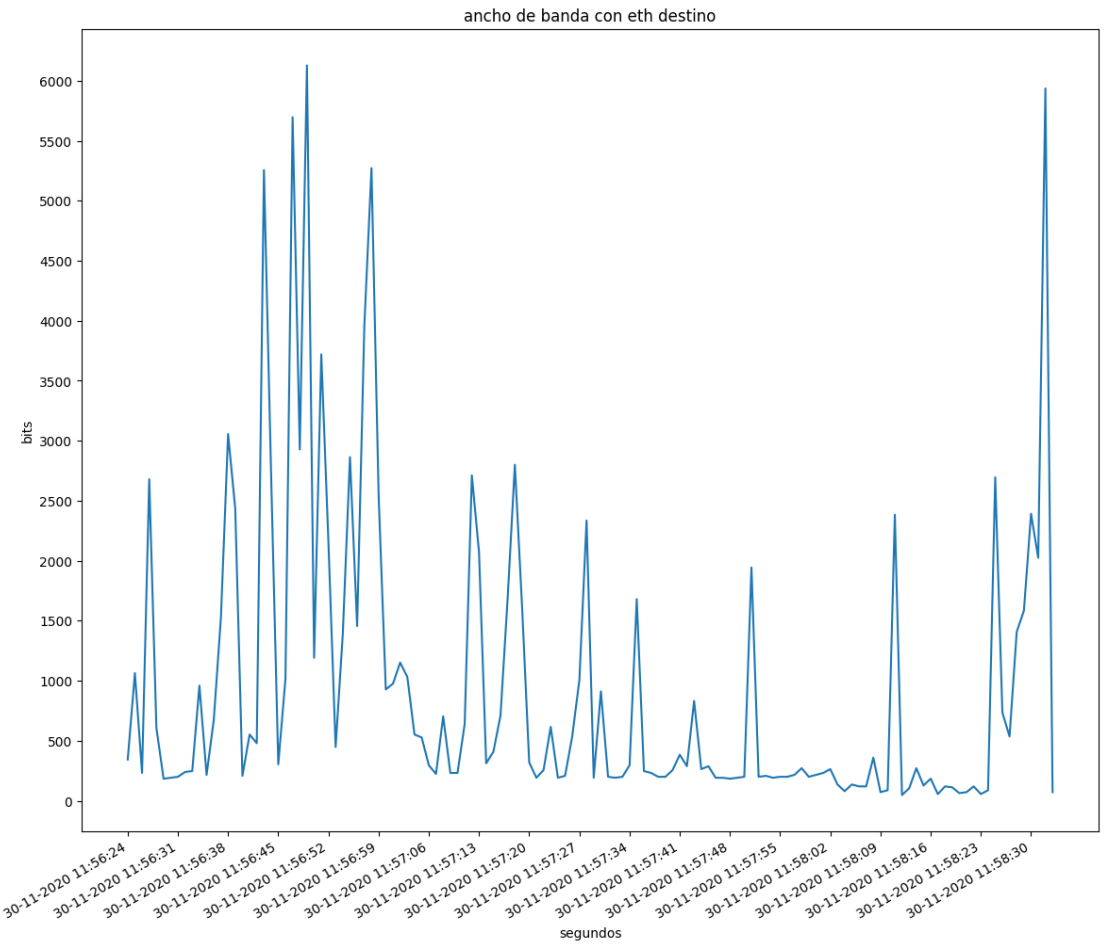
00:11:88:CC:33:15



tshark -Y “eth.scr eq 01:11:88:CC:33:15” -w --> tempfile.pcap -F pcap, genera una traza nueva donde aparecen solo las direcciones eth que son de interés

tshark -r tempfile.pcap -qz io,stat,1 --> Una vez filtradas las MAC’s hacemos una estadística con intervalos de un segundo

Como se puede observar el bando de ancha utilizado por este dispositivo, varia bastante según transcurre el tiempo, esto es debido, a que posiblemente la red que estamos analizando sea una red domestica donde el usuario de esta MAC concentra el tráfico en unos segundos y en otros no utiliza la red, no se puede apreciar demasiado ya que esta traza solo dura 2m y no es suficientemente representativa.

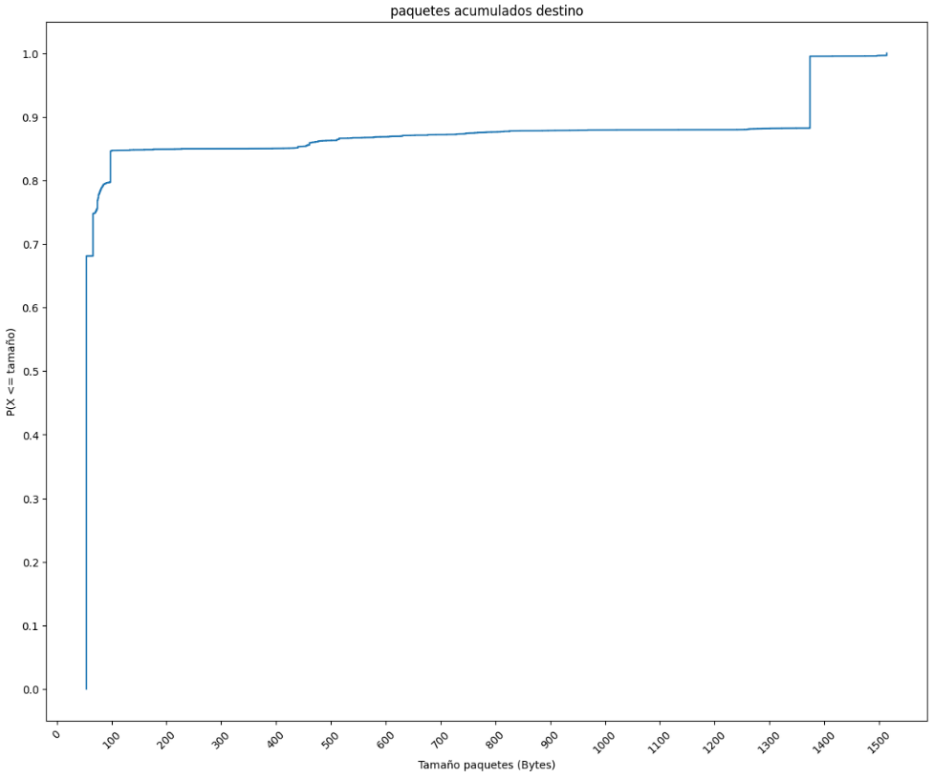


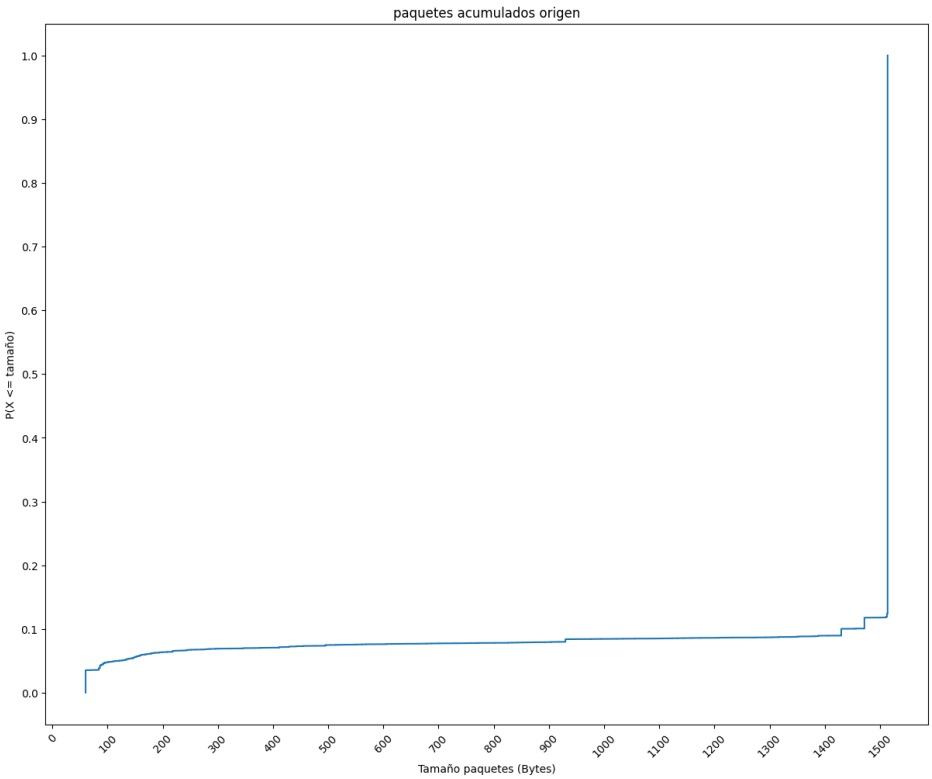
tshark -Y “eth.dst eq 01:11:88:CC:33:15” -w tempfile.pcap -F pcap --> genera una traza nueva donde aparecen solo las direcciones eth que son de interés

tshark -r tempfile.pcap -qz io,stat,1 --> Una vez filtradas las MAC’s hacemos una estadística con intervalos de un segundo

En el caso del ancho de banda de bajada, se aprecia de forma muy significativa el usuario de esta MAC está subiendo a la red mucho más contenido del que se están bajando, puesto que el pico aquí está en 6000 y en el anterior en 26000, este fenómeno se podría dar, por ejemplo, si el dispositivo sube un documento a Moodle, para navegar se requiere poca descarga, pero para subir el documento habrá un pico.

5. ECDFs de los tamaños de los paquetes

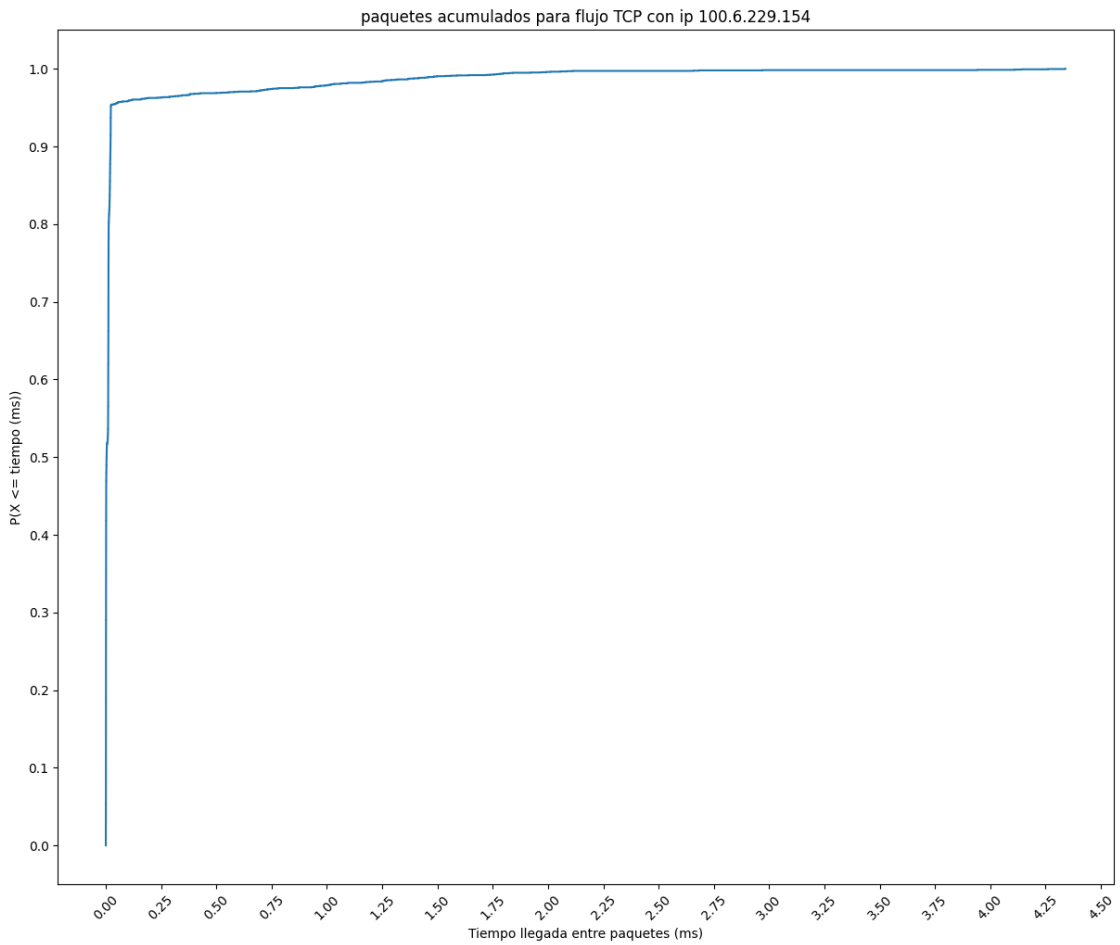




tshark -Y 'eth.src == 00:11:88:CC:33:15 -r traza.pcap -T fields -e frame.len
tshark -Y 'eth.dst == 00:11:88:CC:33:15 -r traza.pcap -T fields -e frame.len

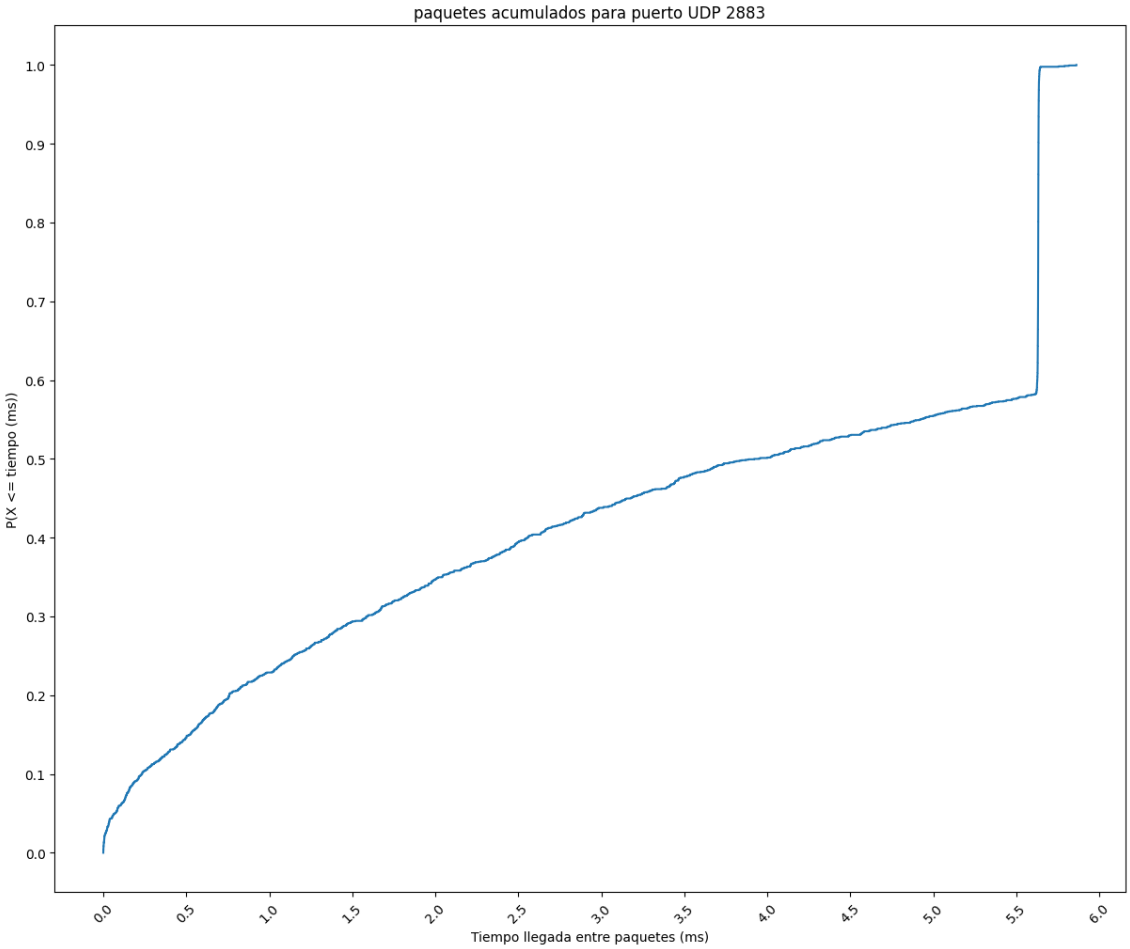
Comparando ambas gráficas, podemos llegar a la conclusión de que los paquetes de origen tienen una probabilidad mucho más elevada que los de destino de ser grandes, en concreto el máximo permitido (1514B).
Esto respalda la hipótesis comentada en las gráficas del ancho de banda, en la que apostamos por que, en el momento de capturar esta traza de la red, el usuario de la MAC origen, estaba subiendo algo a la red mientras que no realizaba ninguna descarga significativa.

6. ECDF tiempos entre paquetes



tshark -Y '(ip.addr == 100.6.229.154) && (ip.proto eq TCP)' -r traza.pcap -T fields -e frame.time_delta

Esta ip concretamente está incluida en el top 5 ip's destino por paquetes, lo que indica que tiene un peso considerable en la red. Cabe destacar que el tiempo de llegada entre los distintos paquetes que nos indica este grafico es muy probablemente ínfimo, es decir, los paquetes llegan muy juntos unos de otros.



tshark -Y '(udp.port == 2883) && (ip.proto eq UDP)' -r traza.pcap -T fields -e frame.time_delta

Para este puerto se puede observar que el tiempo entre paquetes varía bastante, excepto que hay muchos paquetes que les separan alrededor de 5.6 segundos, puede que el usuario tenga un servicio que cada 5.6 segundos usa el puerto 2883, por ejemplo, una aplicación de mensajería puede que compruebe el servidor cada cierto tiempo a través de ese puerto.

3 Conclusiones

Como conclusión podemos observar que el 98% del tráfico es IP, lo que probablemente nos da a entender de que es tráfico de usuario. Y de ese tráfico la mayor parte (92%) se lo lleva TCP, esto tiene sentido dado que en la navegación web es el más usado, UDP se usa mucho menos salvo para transmisión de video, audio… puesto que es más rápido, por lo tanto, esta red no se usa tanto para consumo de media.

El uso de puertos TCP es bastante claro: de subida, el más usado es el 80 en cuanto a número de paquetes, esto quiere decir que se están enviando muchas peticiones http, por lo que nos incita a pensar, que hay una gran parte del tráfico web. En cuanto a descarga, no hay ningún puerto que destaque sobre los demás en cuanto a cantidad de datos, el 80 vuelve a aparecer en cantidad de paquetes, pero al ser pequeños no entra en el top de tamaño.

En cuanto al uso de puertos UDP, se ve claramente como el 38889 y el 2883 de salida y entrada respectivamente son los más usados, no hemos podido averiguar para que se usaban estos puertos, sin embargo, su uso era bastante intensivo tanto por número de paquetes como por tamaño, podríamos imaginar que son usados por servicios de streaming, videojuegos… dado que es el uso típico de UDP. En específico el puerto 2883 tiene una naturaleza periódica (como se puede observar en el ECDF). También es muy importante (25% de uso) el puerto 53 que se usa para DNS, lo cual corrobora la tesis de que el tráfico web es muy alto.

En las mediciones del ancho de banda, filtradas por la MAC origen, hemos visto que uno de los equipos estaba subiendo contenido a la red y que por tanto el ancho de banda de subida ha sido más alto que el de bajada. Esta información se contrasta con las gráficas ECDF posteriores que nos indican que probabilidad de que los paquetes de subida sean de 1514B es muy alta, mientras que los paquetes que nos descargamos de la red, tenemos más posibilidades de que sean más pequeños. Por tanto, concluimos que la medición de la traza se realizó mientras el equipo de la MAC origen, subía contenido a la red.

Respecto al flujo de TCP, como ya hemos comentado en la gráfica, el tiempo entre paquetes es ínfimo, esto resalta que la red está en un buen estado ya que la latencia será mínima.

Tras haber analizado esta traza de red, hemos concluido que esta se encuentra en un buen estado, es decir, no hemos encontrado ninguna peculiaridad en el tráfico medido que nos incite a pensar que haya algún problema con esta red.