PLANIFICACIÓN Y EXPLOTACIÓN DE REDES Y SERVICIOS,
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS DE LA TELECOMUNICACIÓN

Análisis de la Eficiencia de las VPNs en el Acceso Global a Servidores Web

Javier Linzoain Pedraza
javierlinzoain@correo.ugr.es
27/05/2024

***Abstract*— El objetivo de este caso de estudio es analizar la eficiencia de las VPNs a la hora de acceder a servidores web localizados en cualquier parte del mundo. Para ello, se medirá el rendimiento de la red. En este estudio se compara el retardo que supone acceder a servidores localizados en Australia, Estados Unidos y España a través de una VPN frente a no utilizarla. Se ha diseñado un script en bash que realiza de forma automatizada las medidas de los parámetros a estudiar (*delay*, *jitter* y *throughput*) aleatorizando la medida a distintos servidores. Se ha mantenido un registro que contiene información de los servidores relativa a cada medida. Se ha utilizado "nslookup" para conseguir la IP asociada a un dominio, "IPinfo" (API) para conseguir la localización de dicha IP, "expressVPN" (mediante línea de comandos) para conectarnos a la VPN deseada, ping para medición del retardo y *jitter* y "*yt-dlp*" para medir el *throughput*. Para analizar la influencia en mayor o menor grado de los factores y la relación entre ellos se ha usado ANOVA.**

***Index Terms*: VPN, gettec.com, aipg-tx.org y …, *delay*, *jitter*, *throughput*,**

I. DESCRIPCIÓN DE MÉTRICAS Y FUNCIONES A MEDIR

En este estudio se persigue comprobar la implicación que tienen las VPN en la conexión a servidores web localizados en lugares remotos. Concretamente, se estudiarán las implicaciones en el *delay*, *jitter* y *throughput*. Para entender la influencia de estos, es necesario conocer qué son:

- ***Delay***: tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino a través de la red. En el contexto de este trabajo, se considerará el *delay* como el tiempo que tarda un paquete de datos en ir y volver (*round-trip-time, RTT* por sus siglas en inglés), ya que es el retardo proporcionado por la herramienta ping.
- ***Jitter***: es una medida de la variabilidad en el retardo entre paquetes de datos enviados a través de una red. El *jitter* se expresa típicamente en términos de la desviación estándar del retardo de los paquetes. Dicha medida también es proporcionada por la herramienta ping.
- ***Throughput***: esta métrica se refiere a la cantidad de datos que pueden ser transferidos exitosamente a través de la red en un periodo de tiempo determinado. La herramienta se explicará en el siguiente apartado.

II. DISCUSIÓN SOBRE TÉCNIAS PASIVAS Y ACTIVAS

El objetivo o función OAM (Operations, Administration and Maintenance, por sus siglas en inglés) de este trabajo es el "Monitoreo del Rendimiento" (*Performance monitoring*) de una red [1]. Éste se consigue mediante la medición del retardo y el rendimiento a través del *delay*, *jitter* y *throughput.*

En cuanto a la fuente de medición OAM, se trata de la medición de los paquetes y estadísticas de protocolos (ICMP para *ping*, HTTPS para *yt-dlp*).

Herramientas empleadas:

Para la medición de las métricas se van a utilizar dos herramientas: *ping* y *yt-dlp*.

- ***Ping:*** es una utilidad de red utilizada para verificar la accesibilidad y calidad de la conexión a un host o dispositivo.
- ***Yt-dlp***: es una herramienta de línea de comandos utilizada para descargar vídeos de sitios web como YouTube. Esta herramienta permite seleccionar el tipo de formato a descargar, lo que permite establecer el mismo formato de video para todas las medidas. Además, proporciona información detallada sobre la velocidad media de descarga en MB/s, lo que la hace ideal para la medición del *throughput*.

TABLE I. DETALLE DEL CONJUNTO DE TÉCNICAS DE MEDICIÓN

Métrica	***Herramienta***	***Técnica***	***Medida***	***Fuente***
delay	*ping*	Activa *continuity-check*	Agregada	ICMP
jitter	*ping*	Activa *continuity-check*	Agregada	ICMP
throughput	*yt-dlp*	Activa *Performance monitoring*	Agregada	HTTPS

Como estrategia de medición del *throughput*, se va a utilizar una estrategia activa y agregada. Activa porque se va a generar tráfico hacia el servidor objetivo cada vez que se utilice *yt-dlp*, y agregada porque el resultado proporcionado por *yt-dlp* es un resultado final de la descarga del video durante un tiempo, pudiendo variar la velocidad de descarga al principio y al final de la descarga. Cada vez que se ejecuten la herramienta se obtiene una medida agregada del *throughput.*

El *delay* y el *jitter* se medirán a partir del *RTT* obtenido mediante la herramienta *ping*, que realizará un *"Continuity Check"*. Las medidas de estas métricas son agregadas porque se considera la media y la desviación típica observada en la serie temporal de 20 pings enviados durante 30 segundos.

III. DISEÑO DEL EXPERIMENTO: DESCRIPCIÓN DE RESPUESTAS, FACTORES Y NIVELES

SIGUIENDO la Tabla 2, se tiene un total de 3 variables respuesta o métricas:

- *Delay.*
- *Jitter.*
- *Throughput.*

Las 3 variables serán medidas considerando varios factores:

- **Factor 1: Día de la semana**. Trataremos este factor como cualitativo y fijo. Se trata de un factor estorbo "*nuisance"* ya que el sistema debe funcionar para cualquier día de la semana, no controlable. Este factor tiene 5 niveles, correspondientes a los 5 días laborables de la semana: lunes, martes, miércoles, jueves y viernes.
- **Factor 2: Hora del día**. También es un factor "*nuisance"* por la misma justificación, se quiere que el sistema funcione a cualquier hora. Se considera cualitativo y fijo. Este factor tendrá 2 niveles: 12:30, 23:30.
- **Factor 3: Servidor objetivo**. Este factor se trata del destino al que se pretende acceder con o sin VPN para monitorear el rendimiento de la red. Se considerarán 3 niveles, que serán los servidores objetivo cuyos dominios son: "*gettec.es", "aipg-tx.org"* y *"bmgs",* se considera este factor cualitativo y fijo. Es un factor "*nuisance"* ya que no se puede controlar la ubicación de los servidores.
- **Factor 4: Conexión VPN**. El último factor se trata de la conexión VPN. Se consideran 3 niveles: conexión VPN mediante *expressvpn* a Australia-Sydney, conexión mediante *expressvpn* a Atlanta-EEUU y sin conexión VPN, accediendo desde Granada. Este factor se considera cualitativo y fijo y se trata de un factor estorbo debido a que no se puede controlar la conexión VPN, esta viene impuesta por la herramienta *expressvpn.*

TABLE II. DETALLE DE RESPUESTAS, FACTORES, NIVELES Y REPLICATES

Métrica	***Herramienta***	***Factores***	***Niveles***	***Replicates***
Delay	*ping*	F1: Dia/sem. F2: Hora/Dia F3: servidor objetivo F4: VPN	F1: lunes-viernes F2: 12:30, 23:30 F3: Gettec, Aipg, Bmgs F4: sin VPN, con VPN	40 reps.
Jitter	*ping*	F1: Dia/sem. F2: Hora/Dia F3: servidor objetivo F4: VPN	F1: lunes-viernes F2: 12:30, 23:30 F3: Gettec, Aipg, Bmgs F4: sin VPN, con VPN	40 reps.
Through put	*Yt-dlp*	F1: Dia/sem. F2: Hora/Dia F4: VPN	F1: lunes-viernes F2: 12:30, 23:30 F4: sin VPN, con VPN	40 reps.

Para la toma de medidas únicamente se disponía de 2 semanas, por lo que no es relevante comparar la diferencia entre los días de la semana. Es decir, no merece la pena comparar si existen diferencias significativas entre el primer lunes y el segundo, además de que, si se considerase el tipo de día de la semana como factor, solamente existirían 2 *replicates*. Para conseguir un mayor número de *replicates* se aprovechó la ventaja de que los pings generan muy poco tráfico en la red, por lo que, esperando 10 segundos entre medida y medida es suficiente para garantizar la independencia de los *replicates.* Por otro lado, para conseguir aleatoriedad en las medidas, en el script de *bash* se aleatorizó el acceso a los distintos servidores. De esta forma, para cada configuración de factores se midieron 20 *replicates* aleatorizados, por lo que, si se tienen dos semanas, correspondieron 10 *replicates* por día.

IV. EJECUCIÓN DEL EXPERIMENTO

Se desea comprobar el detrimento del rendimiento al usar VPNs frente al hecho de no hacerlo realizando pruebas de conexión a las IPs asociadas a los dominios de 3 empresas de geotecnia. Cada una de estas empresas está situada en un continente. La primera de ellas *"gettec.es"* se encuentra en Granada (Europa), la segunda *"aipg-tx.org"*, en Utah (USA) y la tercera, *"bmgs.com.au"*, en New-South Wales (Australia). A priori, únicamente se conocen los dominios de estas páginas web.

Las pruebas se realizaron a las IPs asociadas a estos dominios. Para averiguar las IPs, se utilizó *nslookup*. Una vez conocida la IP, mediante la API de *ipinfo.io* se extrajo información de la localización del servidor que contenía dicha IP, como la región del país en el que se encontraba, incluso las coordenadas. En la Fig. 1 se puede ver a partir de las coordenadas extraídas las localizaciones de los distintos servidores.

Fig. 1 Localizaciones de los servidores.

A lo largo de todo el proceso se medida, se realizó un registro de la información asociada a cada dominio, como la IP, ubicación, coordenadas, día y hora con el fin de verificar que en ningún momento ninguna IP cambió. Este fichero se encuentra adjunto en el repositorio de github asociado al proyecto.

Para llevar a cabo la ejecución del experimento, se ha diseñado un script en *Bash* que realiza la toma de medidas a los distintos servidores y VPNs de forma automatizada. El orden de ejecución seguido en el script de *Bash* para una medida a una hora, en un día concreto, se muestra en la Fig. 2.

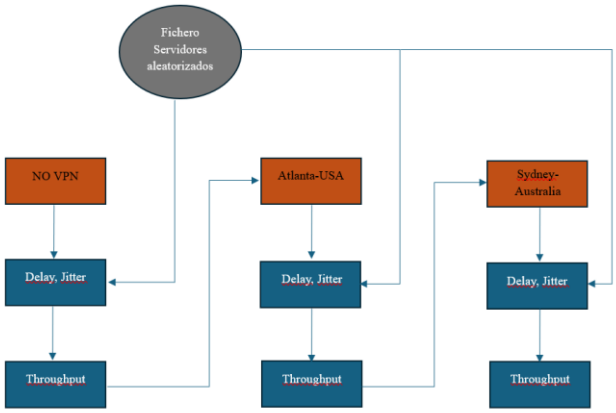

Fig. 2 Flujo de una medida realizada a una hora concreta y un día concreto mediante el script de Bash.

El flujo de la Fig. 2 es el siguiente:

1. Se crea un fichero de texto con 60 líneas, cada línea únicamente contiene un nombre de dominio del servidor a acceder. En total aparece el nombre de cada servidor 20 veces, para que se puedan tener 20 replicates. El orden en el que aparecen los dominios es aleatorio. Esto es crucial para evitar efectos de correlación entre medidas.
2. Se genera un bucle *for* que va leyendo los valores de cada fila del fichero. Se comprueba que el dominio sea correcto, se realiza la medida de *delay* y *jitter* para el dominio considerado. Para las medidas de *delay* y *jitter*, el intervalo entre medida y medida es de 10 segundos, para garantizar independencia entre *pings.*
3. Tras haber realizado las medidas de *delay* y *jitter* 10 veces a cada servidor de forma aleatoria, se pasa a la medición del *throughput.* Las medidas para la respuesta *throughput* solamente dependían de 3 factores: VPN, día y hora. De estos 3, el único factor aleatorizable es la conexión VPN. Sin embargo, por limitaciones técnicas temporales no se consideró su aleatorización, por lo que las medidas del *throughput* para cada VPN se realizaron de manera seguida, manteniendo un tiempo de espera entre medida y medida de 10 segundos para garantizar la independencia entre medidas.

Todos los pasos anteriores se realizan en primer lugar, sin VPN, en segundo lugar, con conexión VPN a Atlanta y se establece una espera de 5 minutos para estabilización de la nueva conexión. Se hace lo mismo para la conexión VPN a Sydney. Habría sido ideal aleatorizar este factor. Sin embargo, por motivos de limitaciones técnicas temporales explicadas en el apartado siguiente apartado, se optó por no aleatorizar este factor.

LIMITACIONES Y MEJORAS DEL SCRIPT

A la hora de implementar el código *Bash* se realizaron las medidas de forma secuencial. Este código se puede encontrar en el repositorio del proyecto en github [2]. No obstante, en esta implementación se encontraron 2 puntos de mejora.

En primer lugar, no había separación temporal entre las medidas de *delay* y *jitter* realizadas, por lo que era muy posible que existiese correlación entre 10 *replicates* medidos secuencialmente al mismo servidor. En segundo lugar, se realizaban todas las medidas al mismo servidor. Una vez terminadas, se cambiaba de servidor y así sucesivamente. Esto podía suponer un aumento de la correlación entre medidas. Para solventar estos defectos, se desarrolló una nueva versión del script de Bash que es el que se ha utilizado finalmente. En esta nueva versión, la conexión a los servidores se realizó de forma aleatoria, evitando la posible correlación entre medidas consecutivas. Además, se estableció un tiempo de espera de 10 segundos entre medida y medida, para garantizar que un ping no afectase al resto. De esta manera se consigue una separación entre medidas que garantiza que una no influye sobre las adyacentes y se aleatoriza el Factor 3, consiguiendo una mejor independencia entre las medidas.

A pesar de haber solventado los dos obstáculos anteriores, el diseño del experimento tiene un punto de mejora, la aleatorización del Factor 4. En el diseño del experimento se optó por no aleatorizar el Factor 4 (VPN) por exceso en el tiempo de medida, ya que cada vez que se realiza el cambio de conexión de una VPN a otra, se establece un tiempo de espera de 5 minutos para que la conexión se estabilice. Si el acceso a los distintos servidores (Factor 3) se aleatorizase entre conexiones VPN (Factor 4), el número de intercambio de conexión VPN aumentaría, aumentando el tiempo de medida 5 min. por cada intercambio VPN, lo que haría la medida bastante más extensa. Por ello, se ha optado por medir primero sin conexión VPN, y después realizar únicamente dos cambios, uno a la VPN de EEUU y otro a la VPN de Australia.

V. ANÁLISIS DE DATOS

Una vez presentado el procedimiento de medida, las respuestas y los factores que influyen en éstas, en esta sección se realiza un análisis de las medidas tomadas, trabajando en Matlab. Concretamente, se realiza un Análisis de Varianza (ANOVA, por sus siglas en inglés) mediante el que se determinará cual es el factor más influyente en las respuestas, y su nivel de significancia. Antes de ello, se presentarán los gráficos *boxplot* que nos dan información sobre la distribución de las medidas para los distintos niveles de cada factor.

Para poder realizar estos análisis, se han formateado los datos obtenidos para que puedan ser interpretables por Matlab.

V.I. DELAY

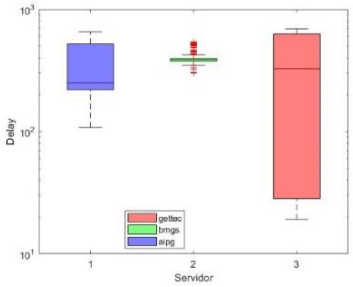

Fig. 3 *Boxplot* factor "servidor".

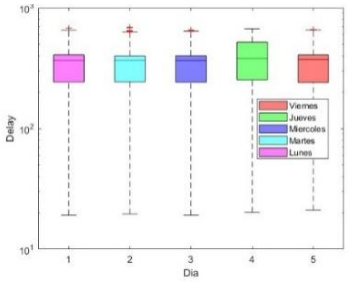

Fig. 4 *Boxplot* factor "día".

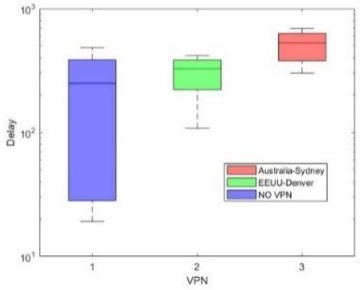

Fig. 5. *Boxplot* factor "VPN"

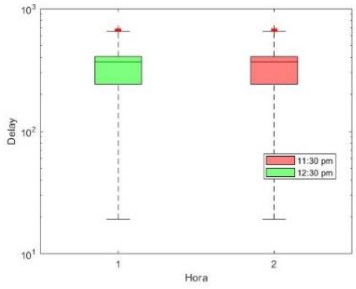

Fig. 6 *Boxplot* factor "hora".

En primer lugar, consideramos la métrica *delay*.
En las Fig. [3-6] se representan los *boxplot* correspondientes a los 4 factores para el *delay*. De estos, se puede extraer que el *delay* en función del día únicamente varía para el nivel "jueves" (Fig. 5), mientras que para la hora (Fig. 6) no varía significativamente. El factor VPN (Fig. 5), muestra que se observa una mayor variabilidad del *delay* para las medidas realizadas desde Granada, sin conexión VPN. Como hipótesis razonable, se puede suponer que ciertos días la red del hogar se encontraba más congestionada que otros, ya que dos de esos días, durante las medidas, se encontraban varios dispositivos consumiendo contenido multimedia. En cuanto al factor "servidor" (Fig. 3), es interesante observar la poca dispersión de los datos asociados al servidor *bmgs*, donde se observa que el 50% de los datos (contenidos en el *box*) se encuentran muy concentrados alrededor de la mediana, por lo que el *delay* es bastante consistente y se observan varios valores atípicos. Sin embargo, todavía no estamos en condiciones de considerarlos *outliers*.

Ahora pasamos a realizar un análisis ANOVA. Todos los ANOVAs realizados en este trabajo incluyen los modelos con interacciones directamente. No se tendrán en cuenta ANOVA de efectos principales por ser menos reveladores que los modelos con interacciones.

El primer paso en un análisis ANOVA es determinar la normalidad de los residuos, ya que este hecho verificará la validez de nuestro experimento. Primeramente, se realizó un análisis sin transformaciones, obteniéndose unos valores bastante alejados de los deseados. Posteriormente, con el objetivo de conseguir una mejor normalidad de los residuos, se probaron diferentes tipos de transformaciones, siendo la transformación *rank* la escogida por ser la que ofrecía mejores valores de *sk* y *k* (Tabla III).. En la Fig. 7, se puede observar la normalidad de los residuos de nuestros datos una vez aplicada la transformación.

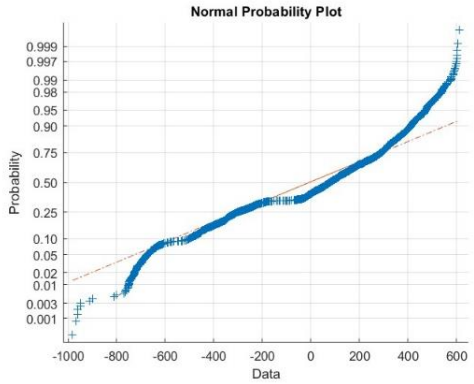

Fig. 7 ANOVA con transformación Rank.

TABLE III. VALORES DE KURTOSIS Y SKEWNESS PARA ANOVA DELAY

Transformación	*sk (Skewness)*	*K (Kurtosis)*
Sin transformación	-0.4833	2.0393
Rank	-0.518	2.2763

Se puede ver que con la transformación Rank se consiguen mejores valores de *sk* y *k*, con el compromiso de una modificación de los datos. Aceptamos esta modificación de los datos y nos centraremos en los datos obtenidos en la tabla ANOVA para la transformación *rank* (Fig. 8)

En la Fig. 8 se puede observar que prácticamente todas las interacciones presentan un efecto significativo en la respuesta. Sin embargo, nos vamos a centrar en aquellos que tengan un

mayor valor de Mean Squares (MS). Un valor elevado de MS para una interacción explica una mayor cantidad de variabilidad de los datos, es decir, las diferencias en los niveles de los factores que están interactuando producen efectos más significativos en la variable dependiente (Delay).

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Servidor	1339828.7	2	669914.3	1501.64	0
VPN	27919636.9	2	13959818.4	31291.53	0
Dia	59138.3	4	14784.6	33.14	0
Hora	996.2	1	996.2	2.23	0.1353
Servidor:VPN	21728507.1	4	5432126.8	12176.34	0
Servidor:Dia	62862.4	8	7857.8	17.61	0
Servidor:Hora	21543.6	2	10771.8	24.15	0
VPN:Dia	48704.4	8	6088	13.65	0
VPN:Hora	4002.4	2	2001.2	4.49	0.0114
Dia:Hora	20959.6	4	5239.9	11.75	0
Error	785619.7	1761	446.1		
Total	52022923.2	1798			

Fig. 8 Tabla resultados ANOVA considerando interacciones.

De la misma manera que para el test ANOVA sin interacciones, se realiza una transformación *Rank* porque es la que ofrece mejores valores de *sk* y *k*. Concretamente *sk*=

Una vez obtenidos los factores e interacciones que tienen un efecto significativo en la respuesta, se realiza un análisis *Post-Hoc* con el que se trata de determinar la influencia de dichos factores en la respuesta. Este análisis nos permite observar qué niveles del factor son significativamente diferentes, así como la influencia de estos en la respuesta. Además, muestran los intervalos de confianza mediante líneas horizontales que cruzan los puntos que representan las medias marginales. Por ejemplo, en el caso del servidor, qué servidor supone un mayor retardo. En un gráfico *Post-Hoc*, cada punto representa la media marginal estimada y las líneas horizontales alrededor de cada punto representan los intervalos de confianza (IC) de esas medias. Si en un gráfico *Post-Hoc* los IC no se solapan, esto significa que hay una diferencia significativa entre las medias.

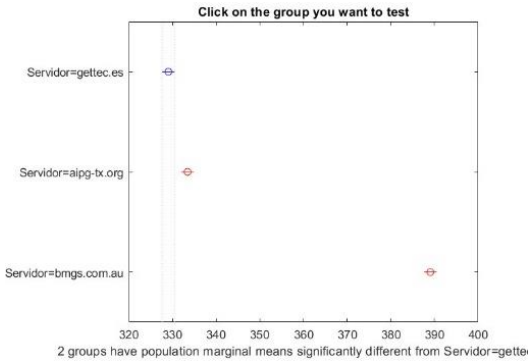

Fig. 9 Gráfico Post-Hoc factor servidor

- **Factor Servidor**: en la Fig. 11 se puede observar que el servidor que presenta un menor delay es "gettec.es" y el mayor, "bmgs.com.au". Esto es lógico ya que "bmgs.com.au" es el que está más alejado, y "gettec.es" el más cercano.

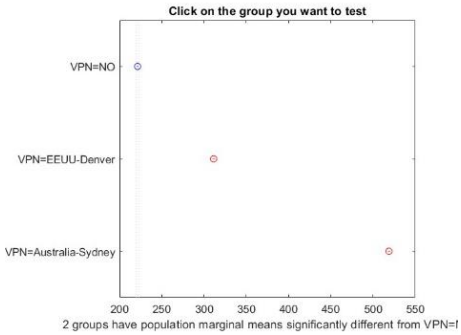

Fig. 10 Post-Hoc factor VPN.

- **Factor VPN**: en la Fig. 12 se observa que el hecho de usar VPN supone un incremento del retardo. Esto tiene sentido ya que, por ejemplo, para acceder a un servidor de Australia, mediante la VPN de EEUU, primero hay que enviar los paquetes al servidor en EEUU, los descifra y los envía al destino final.

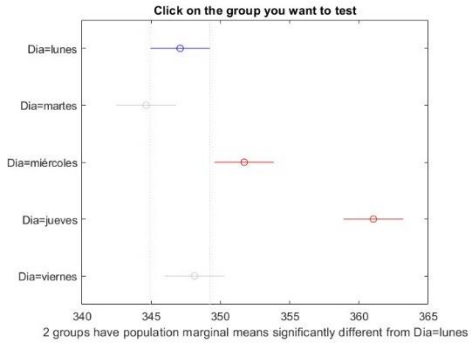

Fig. 11. Post-Hoc para factor Dia

- **Factor Dia**: en Fig. 13 se observa que hay diferencias significativas entre lunes, martes y viernes con respecto al jueves, mostrando este un retardo mayor. Esto puede ser por el hecho que se comentó antes de que había varios dispositivos consumiendo contenido multimedia a la hora que se realizó la medida.

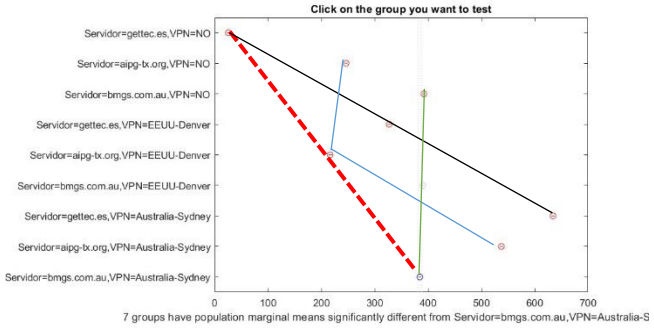

Fig. 12 Post-Hoc interacción servidor-VPN. En rojo la tendencia del menor retardo para cada servidor. En azul, la tendencia del retardo para el servidor "aipg-tx.org", en negro, la del servidor "gettec.es" y en verde la del servidor "bmgs.com.au".

- **Interacción Servidor-VPN**: en Fig. 14 se muestra la interacción con el mayor valor de F, por lo que es la interacción que más afecta a la respuesta. Esta es la interacción más importante ya que nos muestra cómo

influye el hecho de la distancia a la que se encuentran los servidores en relación con la VPN. Se puede ver que el menor retardo tiene lugar para el servidor "gettec.es" (España), sin conexión VPN (acceso desde Granada). El retardo a este servidor aumenta conforme aumenta la distancia a la que se encuentra la VPN a la que nos conectamos. En cuanto al servidor "aipg-tx.org" se observa que el menor retardo se tiene cuando la conexión se realiza mediante la VPN de EEUU en Denver, y el mayor para la conexión VPN más alejada del servidor (Australia). Por último, el servidor "bmgs.com.au" apenas presenta diferencias significativas en función de la VPN utilizada. Aun así, el menor retardo se obtiene cuando la conexión VPN es Australia-Sydney.

De todo lo observado, se pueden extraer las siguientes conclusiones:

1. El menor retardo para acceder a un servidor en cualquier parte del mundo se consigue mediante una conexión VPN cercana a ese servidor (al menos para los servidores estudiados en este proyecto, habría que hacer una prueba a otros continentes para verificar esta hipótesis. Este hecho se representa mediante la línea punteada en rojo en Fig. 14.
2. Es ineficiente utilizar VPN si no se pretende acceder a servicios cercanos a esa VPN. Por ejemplo, sería ineficiente utilizar una VPN para acceder a la plataforma "prado" o a páginas web de administración pública de España.
3. A medida que aumenta la distancia del servidor al que se pretende acceder, influye menos usar una conexión VPN u otra. Se ve que para el servidor "gettec.es" que es el más cercano a nosotros, influye mucho el hecho de usar una VPN u otra. En cambio, para el servidor en EEUU, esta diferencia del retardo se ve disminuida, siendo esta incluso sin diferencias significativas para el servidor de Australia.

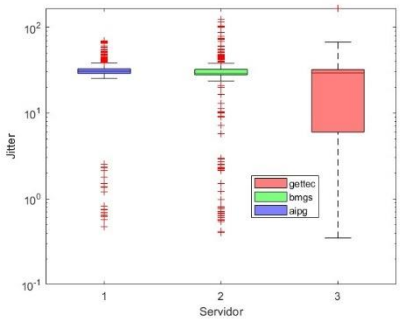

Fig. 13 *Boxplot* factor "servidor"

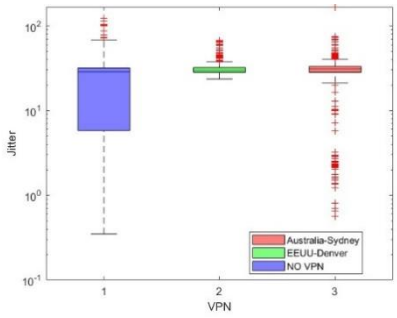

Fig. 14 *Boxplot* factor "VPN"

V.II. JITTER

Tras haber realizado una descripción detallada del procedimiento de análisis para la métrica *delay*, en este apartado se prescindirá de explicar el significado de conceptos como "factor MS", "valor p", interpretación de los gráficos de ANOVA, y solamente nos centraremos en extraer conclusiones a partir de los resultados obtenidos y la interpretación de estos. Tampoco se considerará el test ANOVA sin interacciones, directamente se pasará al test con interacciones.

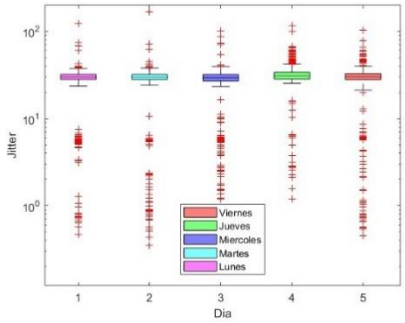

Fig. 15 *Boxplot* factor "día"

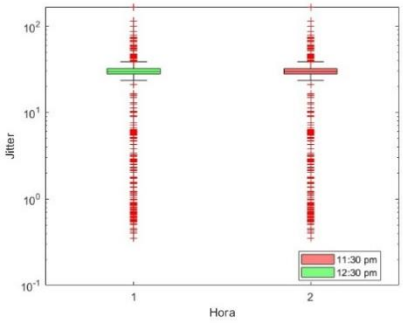

Fig. 16 *Boxplot* factor "hora"

En primer lugar, se muestran los *boxplot* correspondientes a los diferentes factores que afectan al *Jitter*. En ellos, se puede observar que los niveles del factor

En los *Boxplot* de las Fig. 16-19 se puede ver lo siguiente. En primer lugar, la variabilidad del *Jitter* para el servidor "gettec.es" es mayor que para los otros dos servidores, conteniendo todos los valores dentro de los bigotes, en cambio, para el resto de servidores se pueden ver bastantes *outliers.* En cuanto al factor VPN, la conexión que presenta más variabilidad es la que no se usa VPN.

El comportamiento observado para el servidor y la conexión VPN puede estar determinado por la conexión VPN, que presenta una menor variabilidad. Sin embargo, se pueden observar bastantes *outliers* para el servidor de Australia.

En cuanto a los factores "día" y "hora" también se puede observar una gran cantidad de *outliers* lo que indica que será necesario realizar una filtración de *outliers.*

ANÁLISIS ANOVA

A continuación, se realiza el análisis ANOVA. Para esta métrica, se trabajará directamente con el análisis con interacciones, ya que es en definitiva el que nos interesa. Para ello, en primer lugar, se realiza el análisis considerando los outliers, y sin realizar ninguna transformación, donde los valores de *skewness* y *kurtosis* se muestran en la Tabla 4. Se puede ver que la normalidad de los residuos se aleja bastante del modelo teórico y los valores de *sk* y *k* están muy lejos de los deseados. Por lo tanto, se realiza en primer lugar un filtrado de los *outliers*. Se eliminan todos los valores de *jitter* superiores a 80 ms. Los valores de *sk* y *k* parecen en la Tabla IV. Para conseguir unos valores *sk* y *k* más cercanos a los deseados, realizamos una transformación *rank* obteniendo la siguiente curva ANOVA en la que se ve como los residuos se ajustan mucho mejor a la línea del modelo teórico (Fig. 22).

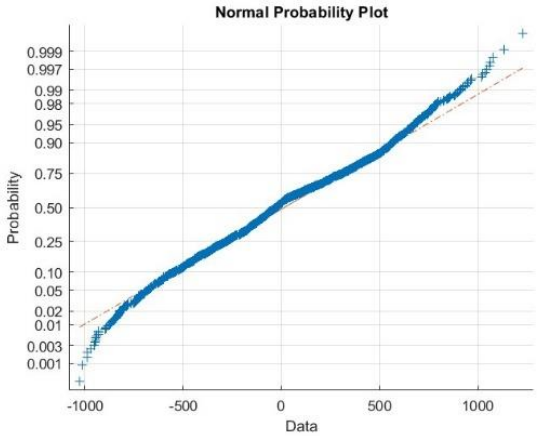

Fig. 17 Representación ANOVA con filtrado y transformación rank para Jitter.

TABLE IV. VALORES DE KURTOSIS Y SKEWNESS PARA ANOVA JITTER

Transformación	*sk (Skewness)*	*K (Kurtosis)*
Sin transformación	2.2529	25.1462
Filtrado de outliers	-0.7356	8.0067
Rank + filtrado	0.0661	2.5123

A partir de los resultados observados en Tabla 4 se observa la gran mejora que supone realizar el filtrado de *outliers.* Si a este filtrado se le incorpora la transformación *rank*, se obtienen valores casi ideales de *sk* y *k*, muy cercanos a 0 y a 3, respectivamente. Trabajaremos con esta transformación.

Los resultados del test ANOVA con interacciones, para los datos habiendo filtrado *outliers* y con transformación *rank*, se muestran en Fig. 23:

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
Servidor	19122211.5	2	9561105.7	54.83	0
VPN	25778564.6	2	12889282.3	73.92	0
Dia	10489652	4	2622413	15.04	0
Hora	1117471.4	1	1117471.4	6.41	0.0114
Servidor:VPN	86975099.9	4	21743775	124.7	0
Servidor:Dia	4755018.6	8	594377.3	3.41	0.0007
Servidor:Hora	96507.5	2	48253.8	0.28	0.7583
VPN:Dia	3687088.1	8	460886	2.64	0.007
VPN:Hora	3686564.8	2	1843282.4	10.57	0
Dia:Hora	3064864.5	4	766216.1	4.39	0.0015
Error	302005928.9	1732	174368.3		
Total	462102476.5	1769			

Fig. 18 Tabla ANOVA para filtrado de outliers y transformación rank, para Jitter.

Se puede ver que hay 3 efectos (factores) significativos y 4 interacciones significativas, y que todos los efectos principales aparecen en alguna interacción significativa, por lo que no se van a considerar los efectos principales por separado. Cuando un efecto principal está presente en una estadísticamente significativa, se estudia la interacción, no los factores por separado. Por lo tanto, nos centramos únicamente en las interacciones. A continuación, se muestran los gráficos *Post-Hoc* que muestran las diferencias entre sus niveles y la influencia en la respuesta.

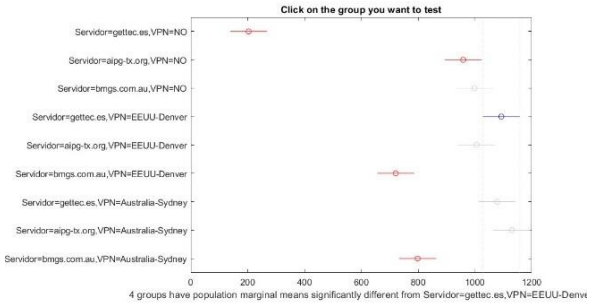

Fig. 19 Post-Hoc interacción Servidor-VPN para Jitter.

- **Interacción Servidor-VPN**: se observa que no existen diferencias significativas entre los servidores "gettec.es" y "aipg-tx.org" cuando se utiliza conexión

VPN, pero si se observan para el servidor "bmgs.com.au"

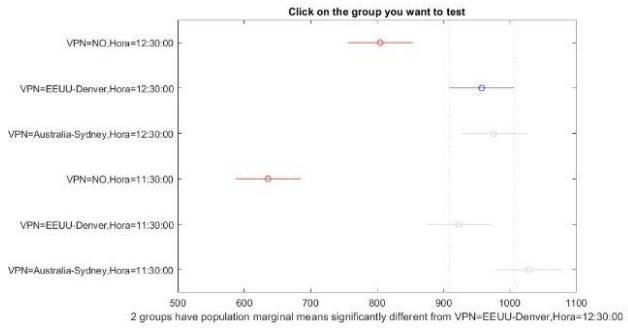

Fig. 20 Post-Hoc interacción VPN-Hora para Jitter.

- **Interacción VPN-Hora**: se puede ver en Fig. 27 que no existen diferencias significativas entre las conexiones VPN a EEUU y Australia a ninguna hora, ya que aparecen solapados los intervalos de confianza. Sin embargo, sí que existen para el caso en el que la conexión no es mediante VPN. Esto significa que el *jitter* medido es menor a cualquier hora del día siempre que no haya conexión VPN. Este resultado es muy interesante ya que confirma que el *jitter* depende de la conexión VPN y no de la franja horaria en la que se realicen las medidas.

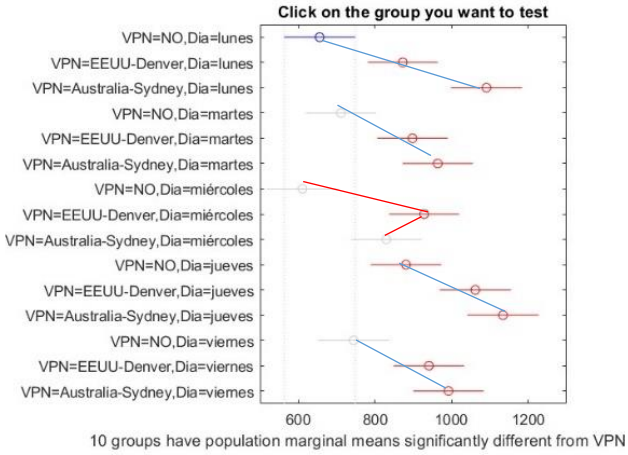

Fig. 21 Post-Hoc interacción VPN-día para Jitter.

- **Interacción VPN-Día**: en Fig. 28 se observa un patrón que se cumple para todos los días excepto para el jueves. Este patrón indica que el *jitter* aumenta a medida que nos conectamos a una nueva VPN. En azul, aparecen representadas las tendencias que confirman este patrón para todos los días menos para el jueves, que aparece en rojo indicando la excepción.

V.III. THROUGHPUT

Por último, analizamos la respuesta del *throughput*. Para esta métrica, no se van a tener en cuenta los servidores destino ya que no tiene sentido. El objetivo de esta métrica es comprobar como varía el *throughput* en función de la conexión VPN, el día y la hora, por lo que solamente se consideran 3 factores.

Por lo tanto, al igual que las dos métricas anteriores, se muestran los gráficos *boxplot* (Fig. 27-31). De los *Boxplots* se pueden extraer las siguientes conclusiones. En primer lugar. Aparentemente los factores Día y Hora presentan la misma variabilidad en cuanto al Throughput, por lo que a priori, no parece que tengan significancia en la respuesta. En cambio, para el factor VPN, se puede observar que cuando no estamos conectados a una VPN, tenemos el máximo Throughput, con velocidades por encima de 10 Mbps. A medida que la VPN se "aleja" del origen (Granada), el Throughput disminuye. Tarda más en descargarse un video de Youtube a través de una VPN que sin ella, y dentro de las VPNs, la velocidad disminuye en función de la distancia a la que se encuentre la VPN a la que se accede.

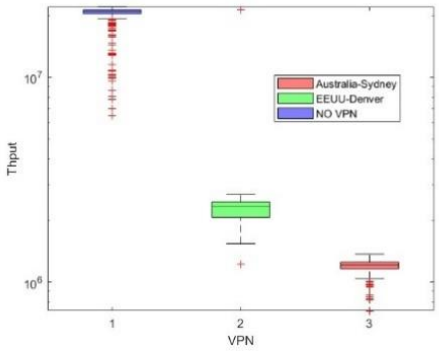

Fig. 22 *Boxplot* factor VPN para Throughput

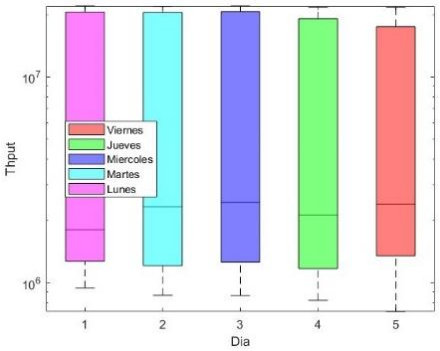

Fig. 23 *Boxplot* factor VPN para Throughput

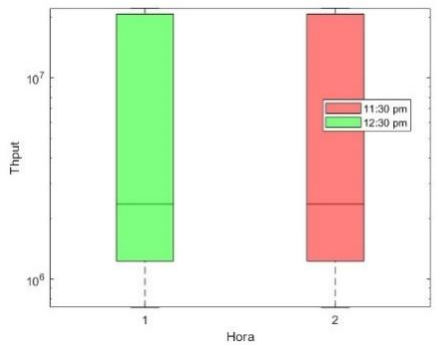

Fig. 24 *Boxplot* factor VPN para Throughput

ANÁLISIS ANOVA

A continuación, se realiza el análisis ANOVA. Al igual que para el resto de las respuestas, únicamente se muestra el gráfico de ANOVA para el modelo final, con filtrado de outliers y transformación Rank. El filtrado de outliers está debidamente justificado porque la magnitud del outlier era 4 veces mayor en el eje X. Además, aplicando una transformación *Rank*, se obtiene una adaptación de los residuos muy buena al modelo teórico. Esto se observa en Fig. 29.

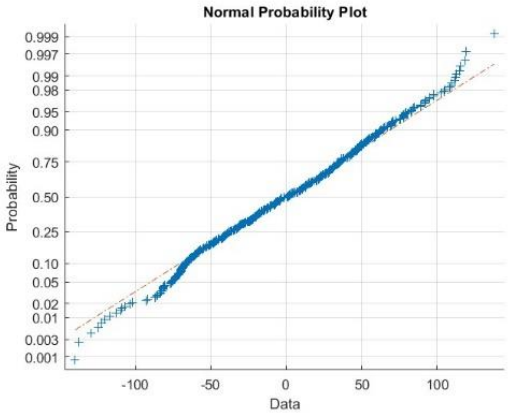

Fig. 25 Representación ANOVA habiendo filtrado outliers y con transformación de los datos.

TABLE V. VALORES DE KURTOSIS Y SKEWNESS PARA ANOVA THROUGHPUT

Transformación	*sk (Skewness)*	*K (Kurtosis)*
-	-1.794	26.9746
Rank + filtrado	-0.014	2.6254

Atendiendo a los resultados de la Tabla V, trabajaremos con la transformación *rank*. La tabla ANOVA con los datos asociados a dicho modelo se representan en Fig. 30.

Source	Sum Sq.	d.f.	Mean Sq.	F	Prob>F
VPN	15888082.2	2	7944041.1	3047.65	0
Dia	254828.1	4	63707	24.44	0
Hora	1450.4	1	1450.4	0.56	0.456
VPN:Dia	160041.4	8	20005.2	7.67	0
VPN:Hora	49102	2	24551	9.42	0.0001
Dia:Hora	48689.2	4	12172.3	4.67	0.001
Error	1504013.6	577	2606.6		
Total	17906143.5	598			

Fig. 26 Tabla ANOVA para la transformación Rank de los datos y filtrado de outliers.

En la Fig. 30 se puede ver que el día y la VPN son factores que afectan significativamente a la respuesta, así como las interacciones VPN-Dia, VPN-Hora, Dia-Hora.

Pasamos a realizar un análisis *Post-Hoc* únicamente de las interacciones y para el efecto principal "Factor VPN"

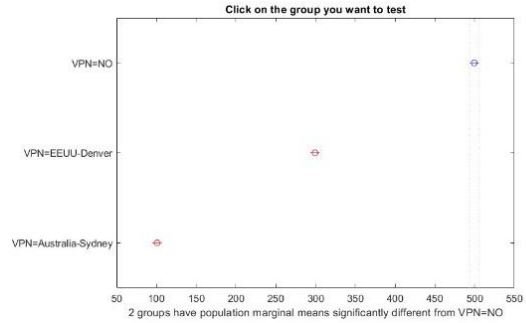

Fig. 27 Gráfico Post-Hoc para el factor Día para Throughput.

- **Factor VPN**: en Fig. 36 se puede ver que todos los niveles del factor Día presentan diferencias significativas, por lo que este factor tiene una influencia significativa en la respuesta.

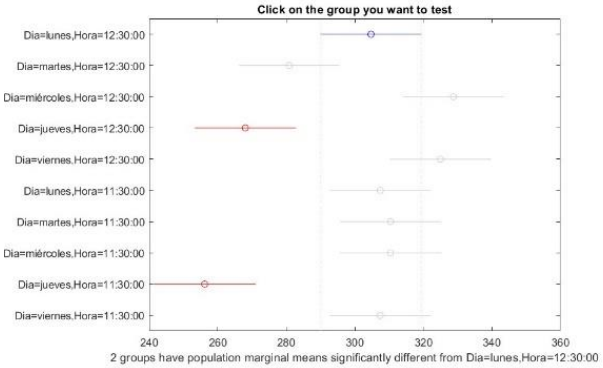

Fig. 28 Gráfico Post-Hoc para la interacción Día-Hora.

- **Interacción Día-Hora**: se puede ver que las dos horas del jueves presentan diferencias significativas respecto al resto de días y horas.

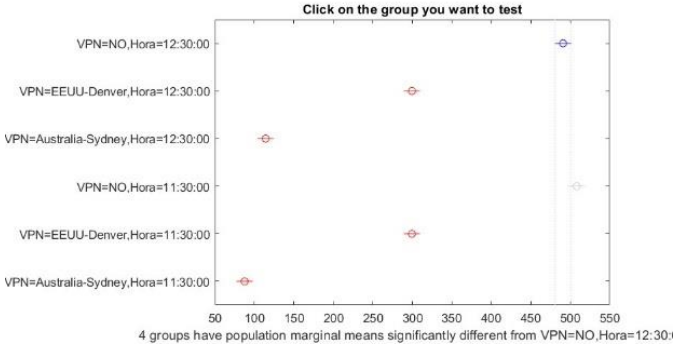

Fig. 29 Gráfico Post-Hoc para la interacción VPN-Hora.

- **Interacción VPN-Hora**: se observa en Fig. 33 que no hay diferencias significativas entre las horas para la misma VPN pero sí para distintas VPNs.

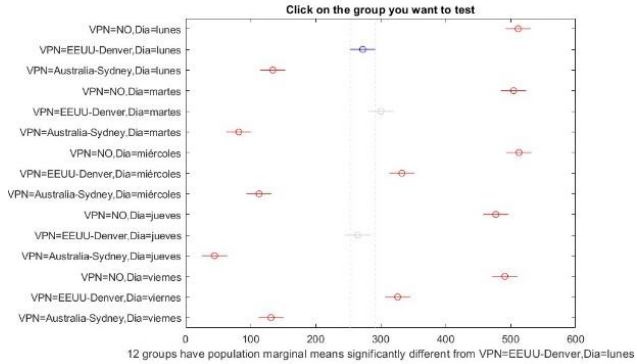

Fig. 30 Gráfico Post-Hoc para la interacción VPN-Hora.

- **Interacción VPN-Dia**: se puede ver en Fig. 34 que existen diferencias significativas, en distintos días, para la misma conexión VPN. Se puede comprobar que estos dos factores no están tan correlados como la interacción VPN-Hora.

VI. Conclusión

Finalmente, teniendo en cuenta todo el trabajo realizado, los resultados obtenidos y los análisis ANOVA realizados, se pueden extraer como conclusiones principales las siguientes:

1. Se ha comprobado que el hecho de filtrar *outliers* y aplicar transformación a los datos, consigue que los datos puedan ser fiables para realizar un test ANOVA sobre ellos. Mediante estas transformaciones, tanto el valor de *kurrtosis* como se *skewness* mejoraban.
2. El menor retardo para acceder a un servidor en cualquier parte del mundo se consigue mediante una conexión VPN cercana a ese servidor. Este hecho se representa mediante la línea punteada en rojo en Fig. 14.
3. Es ineficiente utilizar VPN si no se pretende acceder a servicios cercanos a esa VPN. Por ejemplo, sería ineficiente utilizar una VPN externa a España para acceder a la plataforma “prado” o a páginas web de administración pública de España.
4. A medida que aumenta la distancia del servidor al que se pretende acceder, influye menos usar una conexión VPN u otra. Se ve que para el servidor “gettec.es” que es el más cercano a nosotros, influye mucho el hecho de usar una VPN u otra. En cambio, para el servidor en EEUU, esta diferencia del retardo se ve disminuida, siendo esta incluso sin diferencias significativas para el servidor de Australia.
5. El *jitter* aumenta a medida que nos conectamos a una nueva VPN
6. A medida que la VPN se “aleja” del origen (Granada), el Throughput disminuye.

En resumen, las VPNs, son una gran solución que proporciona seguridad, acceso a contenidos restringidos, protección en redes públicas… No obstante, el hecho de usarlas puede hacer que la conexión a un servicio sea muy ineficiente debido al retardo introducido por la conexión VPN.

Por lo tanto, si se desea utilizar VPNs, y se desea hacerlo de la manera más eficiente posible, sin experimentar problemas de retardo, hay que tener muy presente la elección de la VPN a utilizar. El retardo puede quedar muy reducido mediante la elección de la VPN correcta a la que conectarnos.

Todo esto se ha demostrado midiendo 3 respuestas o métricas de rendimiento de una red, considerando hasta 4 factores, y viendo cuál de estos era más significativo. La conclusión a la que se llega es que el factor determinante en el rendimiento de una red de todos los factores considerados es el factor VPN.

References

[1] AN OVERVIEW OF OPERATIONS, ADMINISTRATION, AND MAINTENANCE (OAM) TOOLS RFC 7276 https://datatracker.ietf.org/doc/rfc7276/

[2] Operations, administration, and maintenance (oam) for deterministic networking (detnet) with the mpls data plane RFC 9546. https://datatracker.ietf.org/doc/rfc9546/

[3] IPInfo https://ipinfo.io/developers

[4] ExpressVPN https://www.expressvpn.com/es

Javier Linzoain Pedraza (Estudiante MUIT) es Graduado en Ingeniería de Tecnologías de Telecomunicación por la Universidad de Granada (UGR) habiendo realizado una estancia Erasmus+ en la Universidad Tecnológica de Praga (CVUT). Trabajó en el grupo S.W.A.T como investigador con cargo a proyecto. Actualmente trabaja en Accenture. Sus intereses profesionales son el Desarrollo de aplicaciones seguras y el conocimiento de la ciberseguridad en todos sus ámbitos.