Desarrollo de una herramienta de monitoreo y detección de diferenciación de tráfico para verificar el cumplimiento de las políticas de neutralidad de red en proveedores de acceso a Internet del Ecuador

Marcillo Cerón, Kevin Roberto y Mosquera Barrazueta, Pablo Steven

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Trabajo de titulación, previo a la obtención del título de Ingeniero en Electrónica y Telecomunicaciones

Ing. Triviño Cepeda, Roberto Daniel MSc.

22 de Febrero, 2023

CERTIFICADO DE ANÁLISIS
magister

TESIS_MARCILLO_MOSQUERA

< 1% Similitudes

< 1% Texto entre comillas
< 1% similitudes entre comillas

1% Idioma no reconocido

Nombre del documento: TESIS_MARCILLO_MOSQUERA.pdf
ID del documento: b555afa78412c26cd0073dd0bc911050dd06d3b3
Tamaño del documento original: 6,21 Mo

Depositante: ANA VERÓNICA GUAMÁN NOVILLO
Fecha de depósito: 22/2/2023
Tipo de carga: interface
fecha de fin de análisis: 22/2/2023

Número de palabras: 25.694
Número de caracteres: 160.090

Ubicación de las similitudes en el documento:

Fuentes

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.itu.int https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html	< 1%		Palabras idénticas : < 1% (61 palabras)
2	repositorio.espe.edu.ec | Desarrollo de una aplicación que permita caracterizar tra... http://repositorio.espe.edu.ec:8080/bitstream/21000/23826/5/T-ESPE-044325.pdf.txt 2 fuentes similares	< 1%		Palabras idénticas : < 1% (27 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	es.wikipedia.org | Modelo OSI - Wikipedia, la enciclopedia libre https://es.wikipedia.org/wiki/Modelo_OSI	< 1%		Palabras idénticas : < 1% (30 palabras)
2	www.informatica-juridica.com | Ley Orgánica de Telecomunicaciones de 10 de febr... https://www.informatica-juridica.com/ley/ley-organica-telecomunicaciones-10-febrero-2015/	< 1%		Palabras idénticas : < 1% (24 palabras)
3	reunir.unir.net | La batalla por el «poder» en Internet https://reunir.unir.net/handle/123456789/5159	< 1%		Palabras idénticas : < 1% (12 palabras)
4	repositorio.flacsoandes.edu.ec | El principio de neutralidad de la red y el derecho a... http://repositorio.flacsoandes.edu.ec/bitstream/10469/16520/6/TFLACSO-2020GEM.pdf.txt	< 1%		Palabras idénticas : < 1% (13 palabras)
5	www.dspace.espol.edu.ec | Optimización de la red de un proveedor del servicio de i... http://www.dspace.espol.edu.ec//bitstream/123456789/1479/3/2829.pdf.txt	< 1%		Palabras idénticas : < 1% (11 palabras)

Fuente mencionada (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://cronicaglobal.elespanol.com/graficnews/horas-mas-conexiones

Firmado electrónicamente por: ROBERTO DANIEL TRIVIÑO CEPEDA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Certificación

Certifico que el trabajo de titulación **"Desarrollo de una herramienta de monitoreo y detección de diferenciación de tráfico para verificar el cumplimiento de las políticas de neutralidad de red en proveedores de acceso a Internet del Ecuador"** fue realizado por los señores **Marcillo Cerón, Kevin Roberto y Mosquera Barrazueta, Pablo Steven**, el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 22 de febrero de 2023

Firma

ROBERTO DANIEL TRIVIÑO CEPEDA

Ing. Roberto Daniel Triviño Cepeda, MSc.

C.C. 1712197522

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Responsabilidad de Autoría

Nosotros, **Marcillo Cerón, Kevin Roberto y Mosquera Barrazueta, Pablo Steven**, con cedula de ciudadanía n°0603941121 y 1716989403, declaramos que el contenido, ideas y criterio del trabajo de titulación: **Desarrollo de una herramienta de monitoreo y detección de diferenciación de tráfico para verificar el cumplimiento de las políticas de neutralidad de red en proveedores de acceso a Internet del Ecuador** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 22 de febrero de 2023

Firma

Marcillo Cerón, Kevin Roberto
C.C. 0603941121

Mosquera Barrazueta, Pablo Steven
C.C. 1716989403

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Ingeniería en Electrónica y Telecomunicaciones

Autorización de Publicación

Nosotros, **Marcillo Cerón, Kevin Roberto y Mosquera Barrazueta, Pablo Steven**, con cedula de ciudadanía n°0603941121 y 1716989403, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Desarrollo de una herramienta de monitoreo y detección de diferenciación de tráfico para verificar el cumplimiento de las políticas de neutralidad de red en proveedores de acceso a Internet del Ecuador** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 22 de febrero de 2023

Firma

Marcillo Cerón, Kevin Roberto

C.C. 0603941121

Mosquera Barrazueta, Pablo Steven

C.C. 1716989403

Dedicatoria

Este trabajo de titulación está dedicado a mi familia, en especial a mi padre Roberto y a mi madre Cecilia, por ayudarme a ser la persona que soy, por guiarme, aconsejarme y apoyarme incondicionalmente en toda la carrera y a lo largo de toda mi vida, sin ustedes nada de esto hubiera sido posible, también a mi hermana Carolina por siempre creer en mí, nunca dejar de animarme y apoyarme a culminar con mi formación universitaria.

Kevin Roberto Marcillo Cerón

Dedicatoria

Este trabajo, con el que culmino una de las etapas más importantes de mi vida, fruto de años de esfuerzo, esmero y compuesto de muchos logros y sacrificios, se lo dedico a dos seres que han estado junto a mí en todo momento.

A mi padre: principal pilar en mi vida, fuente de inspiración, modelo a seguir. Gracias por demostrarme que frente a todo siempre has estado y estarás. Gracias por darme el apoyo incondicional y palabras para perseverar. Gracias porque sin ti no podría haber llegado a ser la persona que soy. Gracias por estar conmigo ayer, mañana y en especial hoy.

Gracias padre, por ser mi padre.

A mi felino Nino: quien me ha dejado una marca imborrable, quien me ha ayudado a encontrar el equilibrio y la paz, por estar a mi lado siempre.

Pablo Steven Mosquera Barrazueta

Agradecimiento

En primer lugar, doy gracias a Dios por darme la vida, por la oportunidad de estudiar en esta universidad y por las bendiciones que me ha dado en el transcurso de toda mi carrera universitaria.

Quiero además agradecer a mis padres por su amor incondicional, su apoyo y sacrificios que han hecho, ya que esto me permitió llegar a este momento. A mi padre Roberto por ser mi ejemplo académico y profesional, y siempre inculcarme el estudio y los valores de esfuerzo y dedicación, a mi madre Cecilia por ser mi apoyo emocional a lo largo de toda mi vida y mi carrera universitaria, por ser siempre comprensiva y siempre brindarme palabras de aliento y levantarme cuando me pensaba derrotado.

A mi hermana también agradecerle por siempre orar por mí y darme consejos para todos mis problemas, sus palabras de aliento nunca faltaron y pese a la distancia siempre acordarse de mí.

A mi novia Andrea que es y fue mi apoyo constante en el transcurso de la mayor parte de la carrera, por darme fuerzas en los momentos difíciles, por animarme todos los días a concluir este proyecto de titulación y sobre todas las cosas por llegar a mi vida y formar parte de este logro.

Quisiera también extender un agradecimiento especial al tutor de este trabajo, al Ing. Daniel Triviño, por la guía, ayuda, dedicación, paciencia y tiempo que nos brindó para concluir de mejor manera con este proyecto.

Finalmente agradezco a todos los compañeros y amigos que tuve a lo largo de la carrera universitaria, por todo lo enseñado y aprendido en cada una de las materias, además a mi compañero Pablo Mosquera, ya que sin la dedicación que emprendimos juntos en los últimos semestres y en este trabajo no hubiese sido posible llegar a la tan anhelada meta.

Kevin Roberto Marcillo Cerón

Agradecimiento

Agradezco a toda mi familia: a mi padre por ser la mejor persona que conozco en este mundo, que ha sido capaz de entregar tiempo y esfuerzo en todos y cada uno de sus días, no puedo ni imaginarme el no poder compartir contigo momentos como este de mi vida. A mis hermanas, con quienes he compartido muchos momentos, con quienes espero poder caminar de la mano todo lo que esté por venir, a quienes llevo en mi corazón en cada momento. A mi madre, quien me inculcó valores y enseñó sobre la vida, gracias a quien me encuentro en este momento tan especial, agradezco tu esfuerzo.

A mi mejor amiga, con quien he contado a lo largo de tantos años, la distancia será una ventaja para poder viajar y conocer parte del mundo juntos.

A mis amigos y compañeros de universidad, con quienes a lo largo de los años hemos compartido y vivido juntos, que me han ayudado a sobrellevar las dificultades y a disfrutar al máximo los buenos momentos. A mis tres hermanos (Joel Gallo, Kevin Marcillo y Steven Calahorrano) con quienes espero recordar momentos como estos por muchos años a venir.

Expresar un agradecimiento especial al Ingeniero Daniel Triviño, de quien tuve la oportunidad de observar como profesor y tutor. Su dedicación, esfuerzo y esmero se ven reflejados en su profesión y trayectoria académica, por brindarnos su guía, conocimiento, ayuda y tiempo.

A todas y cada una de las personas que han aportado en mi desarrollo personal y profesional, quiero expresarles mi más sincero agradecimiento. Gracias por sus consejos, su apoyo y su ejemplo, que me han permitido crecer y mejorar día a día.

Y a esas personas que ya no se encuentran conmigo, les agradezco por todo lo que han aportado en mí.

Pablo Steven Mosquera Barrazueta

Índice de Contenido

Índice de tablas

Índice de figuras

Resumen

La Internet es aprovechada por más de 5 billones de personas en todo el mundo, convirtiéndose en la infraestructura de comunicaciones más utilizada y es parte fundamental del crecimiento económico de muchos países y diferentes organizaciones. Por lo tanto, preservar un ecosistema de Internet justo, equitativo y abierto, fomenta la innovación, la competencia leal y da libertad de elección a los usuarios, siendo esta la base fundamental de la Neutralidad de red (NR). La NR establece que todo el tráfico de Internet debe ser tratado por igual, sin importar su origen, destino y/o contenido. Esto significa que ningún proveedor de servicios de Internet (ISP's) o gobierno puede bloquear, limitar o priorizar ciertos tipos de tráfico en detrimento de otros. Muchos países alrededor del mundo han implementado políticas, normas y estatutos en sus marcos regulatorios para garantizar la NR, con ayuda de herramientas de monitoreo de red, para garantizar la integridad de este principio por parte de los ISP's. El presente trabajo de titulación realiza el desarrollo de una herramienta de monitoreo e inyección de tráfico activa, para detectar diferenciación de tráfico en la red y verificar el cumplimiento de las políticas de NR en los ISP's del Ecuador. Al inyectar tráfico en la red, la herramienta permite detectar posibles abusos por parte de los ISP's, a través de la comparación de latencia y pérdida de paquetes entre diferentes tipos de servicios de video, como Netflix, YouTube y Google Meet, y observar la existencia de discriminación de unos frente a otros. Con los datos obtenidos por la herramienta desarrollada, a lo largo de un periodo de pruebas, se realiza el análisis de manera que se obtengan evidencias empíricas sobre el cumplimiento de las políticas de neutralidad de red en los principales ISP's fijos y móviles en el país.

Palabras clave: Diferenciación de tráfico, herramienta de monitoreo, inyección de tráfico, latencia, neutralidad de red, pérdida de paquetes.

Abstract

The Internet is used by more than 5 billion people worldwide, making it the most used communications infrastructure and a fundamental part of the economic growth of several countries and different organizations. Therefore, preserving a fair, equitable and open Internet ecosystem promotes innovation, fair competition and user choice, which is the fundamental basis of Network Neutrality (NN). The NN establishes that all Internet traffic should be treated equally, regardless of its origin, destination and/or content. This means that no Internet Service Provider (ISP) or government can block, limit, or prioritize certain types of traffic above others. Many countries around the world have implemented policies, rules and statutes in their regulatory frameworks to guarantee NN, with the help of network monitoring tools, to guarantee the integrity of this principle by ISP's. This degree work carries out the development of an active traffic injection and monitoring tool to detect traffic differentiation in the network and verify compliance with NN policies in Ecuadorian ISP's. With the injection of traffic into the network, the tool allows the detection of possible abuses by the ISPs through the comparison of latency and packet loss between different types of services, such as Netflix, YouTube and Google Meet, and observing the existence of prioritization of some above others. With the obtained data by the developed tool throughout a testing period, an analysis is performed in order to obtain empirical evidence on the compliance with network neutrality policies in the main fixed and mobile ISPs in the country.

Keywords: Latency, monitoring tools, net neutrality, packet loss, traffic differentiation, traffic injection.

Capítulo I

Introducción

Antecedentes

Aproximadamente el 62.5% de la población mundial utiliza la Internet, son aproximadamente 4.95 billones de personas, convirtiéndose en la infraestructura de comunicaciones más utilizada (Kemp, 2022). Conforme crece, aumenta la demanda de ancho de banda y empiezan a surgir desafíos de carácter técnico, económico y social.

Al ser una plataforma abierta, convergente y fuertemente relacionada con las redes, la tecnología y los medios, se han desarrollado una gran variedad de aplicaciones y servicios que demandan gran cantidad de ancho de banda y no funcionarían bajo el principio *best effort* (mejor esfuerzo) (Molina, 2011). Además, debido a la carga sobre la red y el gasto en la infraestructura, los proveedores de servicios de Internet (ISP, del inglés *Internet Service Provider*) emplean prácticas de gestión de red como parte de sus procesos de operación y mantenimiento, pero también podrían estar aplicando prácticas discriminatorias injustificadas para la gestión de su tráfico al bloquear, reducir la velocidad y favorecer o priorizar ciertas aplicaciones o contenidos, obteniendo ventajas frente a su competencia (Garret, Setenareski, Peres, & Erpen, 2018).

El éxito de Internet se debe a su naturaleza ideológicamente abierta (Triviño, Franco, & Ochoa, 2020), donde los datos han sido tratados de igual manera sin discriminación, esto es lo que se conoce como el principio de la neutralidad de la red (NR), que desde su introducción hace casi dos décadas siempre ha sido objeto debate alrededor del mundo. El principio fundamental manifiesta que todos los paquetes de datos en Internet deben ser tratados de la misma manera sin importar su origen, destino y/o contenido (Easley, Guo, & Kraemer, 2017). Pero debido a las características de las aplicaciones y contenidos actuales sensibles al ancho de banda, la aplicación de prácticas de gestión de tráfico se ha vuelto inevitable, haciendo uso de diferenciación de tráfico (DT). Aspecto que además podría ser usado para discriminar datos, aplicaciones o servicios de manera injustificada, atentando en

contra del Internet abierto, la innovación, la competencia leal y libertad de elección por parte de los usuarios (Garret, Setenareski, Peres, & Erpen, 2022).

La DT podría ser usada por ISP's por diferentes razones, entre ellas, el control de la congestión (cuando afecte la operación de la red), limitando el ancho de banda para ciertas aplicaciones como: archivos P2P, transmisión de audio y video, entre otras. También existen otras razones como acuerdos comerciales con proveedores de contenido o servicios para utilizar priorización pagada para beneficiar a los grandes servicios ya establecidos, perjudicando nuevos servicios, soluciones similares y la competencia justa.

Las autoridades gubernamentales de regulación alrededor del mundo se han visto obligadas a analizar las condiciones entregadas por los ISP's y las responsabilidades que tienen con sus clientes y la libre competencia (Triviño, et al, 2020). Por lo cual, la NR ha avanzado de una propuesta regulatoria a la implementación actual en varios países como Chile, Brasil, Japón, India, Corea del Sur, Canadá, EEUU, México y la Unión Europea, que ya han implementado regulaciones para cumplir con los principios de NR. Sin embargo, estudios sobre su implementación provienen mayormente del Norte Global. Por otro lado, en Latinoamérica, hay pocos estudios sobre el incumplimiento o faltas a las políticas de NR por parte de las agencias nacionales de regulación y control; Y particularmente en Ecuador no hay análisis al respecto, a pesar que la Ley Orgánica de Telecomunicaciones - LOT 2015 en su capítulo 3 y 4 establece la Neutralidad de Red, siendo un tema incipiente, y sin una normativa legal para aplicación y control establecida (Cordero, 2019).

Actualmente, el cumplimiento de las regulaciones por parte de los proveedores de servicios de Internet (fijo o móvil) no puede ser controlada en su totalidad, debido al aumento en la demanda de ancho de banda y calidad de servicio por parte de los usuarios. Además, la pandemia originada por el SAR-CoV-2 obligó a las personas a realizar todas sus actividades académicas y profesionales de manera virtual, se ha incrementado el número de usuarios que necesitan acceso a Internet y tráfico de datos. Esto ha ocasionado gran presión sobre las redes de los ISP's obligándolos a adaptarse a la demanda de tráfico y

garantizar el servicio, ha ocasionado una posible aplicación de prácticas discriminatorias injustificadas que pueden atentar con el principio de NR (Triviño, Franco, & Ochoa, 2021),

Conforme a lo anterior, en este trabajo de titulación se desarrolla una herramienta de software que para monitorear y detectar la diferenciación de tráfico para ciertos tipos de aplicaciones o servicios (datos y video) en las redes de los proveedores de acceso a Internet (fijo y móvil), a través de la inyección de tráfico activo desde equipos de usuario.

La herramienta de software de generación de tráfico activo se desarrolla para: 1) proveedores fijos como una aplicación de escritorio, y 2) para proveedores móviles con una aplicación para teléfonos inteligentes. Estas permiten el envío de diferentes tipos de paquetes de datos con el mismo contenido (datos, audio o video), pero con la posibilidad de incluir también bits aleatorios en su cabecera *Differentiated Service Code Point* (DSCP) de tal manera prevengan la categorización general de los paquetes por parte del ISP.

Las pruebas del software de monitorización se realizan en ambientes de laboratorio y posteriormente sobre las redes de los operados desde el lado del usuario final. De los resultados obtenidos, se identifican posibles bloqueos, reducción de velocidad o priorización de datos y de esta forma verificar o no la existencia de una discriminación que pueda afectar el cumplimiento del principio de NR en los operadores principales del Ecuador. Para ello, como unidades de análisis se monitorea a los operadores de acceso a Internet fijo (CNT y Netlife) y móviles (Claro, CNT y Movistar) de tal forma que se determine si existe aplicación de medidas discriminatorias en la gestión de tráfico y el cumplimiento del principio de NR para el servicio que brindan a los usuarios finales.

Justificación

La Internet se ha convertido en un importante medio de comunicación, así como un instrumento de investigación, innovación y entretenimiento para la sociedad (Dogruer, Eyyam, & IpekMenevis, 2011). Ha contribuido al desarrollo de diferentes aplicaciones y servicios por su estructura abierta, alcanzando el 62.5% de la población mundial (Kemp,

2022). Este exitoso fenómeno ha sido factible por la naturaleza abierta de Internet (Triviño, Franco-Crespo, & Ochoa-Urrego, 2021), un ambiente con las mismas oportunidades de acceso, uso y libertad de expresión (Triviño, et al, 2020).

Desde el 2015 hasta la actualidad, el número de personas conectadas ha aumentado alrededor de 1.5 billones a nivel mundial. En el caso particular de Latinoamérica, pasó de tener una penetración de Internet de 43,4% a 71,5%, sobrepasando incluso el promedio mundial actual (Soto, 2022). Además, la concentración de dispositivos, aplicaciones, redes y plataformas basados en Internet impactan positivamente en el crecimiento económico.

En América Latina, se ha masificado la difusión de nuevas tecnologías, y se ha acelerado la transición hacia economías digitales, reformando los procesos de negociación e impulsando el desarrollo regional e internacional de la industria del software y aplicaciones (CEPAL, 2010).

La forma en que Internet se gobierna es crucial; la gestión de este recurso global interfiere directamente sobre las oportunidades económicas y sociales presentes y futuras, por lo que necesita ser cuidada para garantizar su sostenibilidad y conservar su apertura (Internet Society, 2015). Posiblemente el problema más relevante en políticas de Internet, en torno a todo lo que involucra su desarrollo y regulación, en la última década, es el principio de Neutralidad de la Red (Triviño, et al, 2021), introducido por Tim Wu en 2003.

La NR establece que todos los paquetes de datos en Internet deben ser tratados de la misma manera sin importar origen, destino y/o contenido (Easley, et al, 2017). Pero, debido a las características de ciertas aplicaciones y contenidos que son sensibles al ancho de banda, la aplicación de prácticas de gestión de tráfico se ha vuelto común. Así, el debate sobre NR, con casi 20 años en desarrollo, se basa en cuatro aspectos principales: restricciones arbitrarias de ciertas aplicaciones, contenidos y servicios por parte de los ISP,

priorización de aplicaciones, contenidos y servicios, y falta de transparencia y monopolización de ISP's fijos y móviles (Molina, 2011)

La DT puede ser aplicada por los ISP's por diferentes motivos, entre ellos el control de la congestión, que bloquea o limita el consumo de ancho de banda de ciertas aplicaciones (archivos P2P, transmisión de audio y video, entre otras) (Garret, et al, 2018). La priorización pagada de determinado tráfico también es común o a su vez la obtención de una ventaja competitiva mediante la cual un ISP prioriza el tráfico de sus propios servicios y degrada (o incluso bloquea) el tráfico de los competidores. Esto amenazaría los tres conceptos que son considerados esenciales para el éxito de Internet: innovación, competencia leal y libertad de elección del consumidor (Garret, et al, 2018)

En Ecuador, la ley (LOT) de 2015 en el Título 1, Capítulo 1 "Consideraciones Preliminares", en su Artículo 4 "Principios" establece que: "La provisión de los servicios públicos de telecomunicaciones responderá a los principios constitucionales de obligatoriedad, ...uso eficiente de la infraestructura y recursos escasos, neutralidad tecnológica, neutralidad de red y convergencia." (Asamblea Nacional, 2015). Sin embargo, la Ley no define su concepto, o normativa de aplicación, dejando a consideración de los ISP lo que puede o no considerarse como una práctica discriminatoria, las acciones que podría realizar al brindar el servicio, así como la transparencia en cuanto a prácticas de DT que permitan garantizar el principio de NR (Cordero, 2019). Por otro lado, el análisis del cumplimiento de las políticas de NR en Sudamérica se ha pronunciado únicamente en Chile y Brasil, pero para el resto de países es escaso y no se tiene mayores evidencias empíricas sobre las transgresiones que los ISP's podrían estar cometiendo.

En base a lo mencionado, y con el fin de aportar información sobre las prácticas de diferenciación de tráfico en los servicios que ofrecen los proveedores de acceso a Internet fijo y móvil, este proyecto está enfocado principalmente al desarrollo y uso de una herramienta de software activo para el monitoreo y detección de DT, a través de la inyección de cierto tipo de tráfico que permita identificar prácticas discriminatorias y así

verificar el cumplimiento del principio de NR, en los principales proveedores de acceso a Internet fijos y móviles del Ecuador. De esta manera aportar con evidencia empírica sobre el tema, que no solo sirva para aumentar la bibliografía existente, sino que pueda ser usada por entes de regulación, proveedores o usuarios para determinar el cumplimiento de las políticas de NR.

Alcance

La metodología que se siguió para la realización de este trabajo es de tipo mixta: con un componente cualitativo y cuantitativo junto con un componente de tipo teórica/experimental y de tipo hipotético/deductivo.

En la primera parte se utilizó la metodología cualitativa con el fin de buscar información relevante al principio de Neutralidad de Red (NR) y al desarrollo de herramientas de monitoreo. De esta forma se pretende levantar el estado del arte en base a la búsqueda de palabras clave como: *net neutrality*, neutralidad de red, monitoring tools, *traffic differentiation detection*, en bases de datos (Scopus, IEEEXplorer, Springer, etc) y la selección de artículos relevantes para el estudio. Además, se pretende identificar, analizar y verificar la implementación de políticas de NR en el Ecuador de acuerdo a lo establecido en la Ley Orgánica de Telecomunicaciones (LOT 2015).

Para la segunda parte, el método experimental, se desarrolló una aplicación activa de inyección y monitoreo de tráfico para ISP fijos (CNT y Netlife) (aplicación de escritorio) y móviles (Claro, CNT y Movistar) (aplicación para smartphones). Las aplicaciones deberán realizar 1) el envío de paquetes de tráfico de aplicaciones, contenido o servicios populares (streamings de audio y video), 2) medición de: TTL, latencia y pérdida de paquetes en respuesta al tráfico de las aplicaciones, contenido o servicios populares inyectados a la red del ISP, 3) envío de paquetes con el mismo contenido de servicios populares, pero con bits aleatorios en sus cabeceras (DSCP) que prevengan la categorización de los paquetes por parte del ISP y 4) medición de: TTL, latencia y pérdida de paquetes con bits aleatorios en las cabeceras. El método experimental será puramente cuantitativo, ya que se va a emplear

pruebas de ensayo y error para verificar el funcionamiento de la herramienta de acuerdo a los parámetros establecidos.

Dentro de la parte dos, además, se implementó el protocolo de pruebas. Donde: 1) Las pruebas en ambiente de laboratorio permitirán validar las herramientas desarrolladas además de verificar el tráfico que estas generen, tanto en escenarios de alto y bajo tráfico, durante tiempo largo o corto, de manera sostenida o pausada y considerando parámetros y valores como latencia, encriptación, posible procesamiento y otros. Para esto se utilizaron herramientas como *sniffers* y equipos de red que realicen DT y permitan validar esta información una vez obtenida del tráfico generado.

En la tercera parte, se estableció el protocolo de pruebas en campo, considerando un muestreo de operadores por conveniencia tanto para el escenario fijo (CNT y Netlife) y el escenario móvil (Claro, CNT y Movistar). Así se determinó la existencia de las prácticas de diferenciación de tráfico, y verificó la vulneración del principio de Neutralidad de red por parte de los ISP’s. Las pruebas tanto en fijo como en móvil fueron realizadas por un periodo diario en el transcurso de 4 semanas, con enfoque en dos horarios, las horas de mayor demanda (con mayor densidad de tráfico) y una hora de poco uso, ya que en horas de mayor demanda se tiene mayor probabilidad y una posible necesidad de implementar reglas arbitrarias de gestión de tráfico para asegurar el servicio.

Finalmente, se analizaron los datos obtenidos/recabados para determinar si existe o no violación al principio de NR por parte de los proveedores de servicio de Internet en el Ecuador, emitiendo conclusiones y recomendaciones sobre las pruebas realizadas y los resultados obtenidos

Objetivos

Objetivo General

Desarrollar una herramienta de monitoreo y detección de diferenciación de tráfico para verificar el cumplimiento de las políticas de neutralidad de red en proveedores de acceso a Internet (fijo y móvil) del Ecuador.

Objetivos Específicos

- Desarrollar el estado del arte sobre la neutralidad de la red y las especificaciones necesarias de las herramientas de monitoreo de tráfico.
- Analizar las políticas de neutralidad de red, con énfasis en el Ecuador.
- Desarrollar una herramienta de software para computadoras que permita la inyección de tráfico activo de red para monitoreo y detección de diferenciación de tráfico en redes de acceso a Internet fijo.
- Desarrollar una herramienta de software para teléfonos inteligentes que permita la inyección de tráfico activo de red para monitoreo y detección de diferenciación de tráfico en redes de acceso a Internet móvil.
- Establecer y validar el protocolo de pruebas de las herramientas de monitoreo y detección de diferenciación de tráfico en laboratorio y campo.
- Analizar los resultados del monitoreo de proveedores de acceso a Internet fijo y móvil.
- Determinar y discutir el cumplimiento de las políticas de neutralidad de red y el uso de prácticas discriminatorias.

Descripción General

Este proyecto de investigación desarrolla una herramienta de inyección de tráfico activa para el monitoreo y detección de diferenciación de tráfico para verificar posibles incumplimientos de las políticas de neutralidad de red en proveedores de acceso a Internet del Ecuador.

En el capítulo 2, se hace uso de la metodología cualitativa con el fin de construir el estado del arte y el marco teórico acerca del Internet y la Neutralidad de Red (NR) y proporcionar así una base de datos sólida sobre su historia, estructura, funcionamiento y gobernanza, obteniendo el contexto de la investigación. Luego se analizan las iniciativas y políticas implementadas por los gobiernos y las organizaciones de regulación en diferentes países del mundo sobre la NR, y su diferencia con las del Ecuador. Seguido se incluye un estudio sobre las diferentes técnicas y herramientas de monitoreo/inyección para diferenciación de tráfico (DT) utilizadas para garantizar el cumplimiento del principio de NR, incluyendo una revisión de los diferentes enfoques y tecnologías disponibles, así como su efectividad y limitaciones.

Una vez comprendida la NR y las herramientas de monitoreo/inyección de tráfico para DT, en el capítulo 3 se menciona el proceso creación de una herramienta para la inyección y monitoreo de tráfico. Se inicia con la definición de los requerimientos funcionales de la herramienta, y los pasos necesarios para construir paquetes sintéticos. A continuación, se realiza el diseño de la aplicación de inyección y monitoreo de tráfico (fija y móvil). Después, se desarrolla un servidor que permitirá a las aplicaciones realizar solicitudes de inyección de tráfico. Luego, se llevan a cabo las pruebas de laboratorio con su correspondiente protocolo de pruebas, con el objetivo de validar la herramienta creada. Posteriormente, se realizan pruebas de campo con su respectivo protocolo de pruebas, que servirá para recopilar los datos a lo largo de un plazo establecido para su posterior análisis. Finalmente, se crea una página web que muestra gráficas de los resultados de las pruebas de campo realizadas.

En el capítulo 4 se muestran los resultados obtenidos tanto del diseño de las aplicaciones (fija y móvil), como de las pruebas realizadas. Los resultados de diseño muestran los paquetes sintéticos creados de cada servicio establecido, la interfaz de la aplicación fija y de la móvil, cada una desde su dispositivo de uso (computadora, teléfono inteligente). Los resultados obtenidos de las pruebas de laboratorio y campo, muestran

tanto para el escenario fijo, como para el móvil, el comportamiento de la herramienta y su validez. En el caso de las pruebas realizadas en campo se consideran las pruebas realizadas diariamente en un transcurso de 4 semanas, las cabeceras DSCP con diferentes valores, y la comparación entre servicios de manera que se observe el tratamiento de los ISP's a los tráficos de los servicios en cada uno de los escenarios.

En el capítulo 5 se realiza el análisis de resultados a través de las comparaciones de los datos obtenidos en el capítulo anterior con la realizada en estudios relacionados, de manera que se pueda brindar juicio sobre el tratamiento del tráfico realizado por los ISP a través de las evidencias empíricas que respaldan esta investigación.

Finalmente, en el capítulo 6 se realizan las conclusiones y recomendaciones del proyecto de investigación. Se realizará el análisis de los datos obtenidos por las herramientas para determinar si existe o no diferenciación en el tratamiento de los datos de los diferentes servicios probados, y por ende una posible transgresión al principio de NR por parte de los ISP en el Ecuador.

Capítulo II

Estado del Arte

Internet y gobernanza

La Internet es una super red mundial de miles de computadoras personales y servidores interconectados. La Internet está compuesto por redes informáticas y de telecomunicaciones más pequeñas alrededor del mundo las cuales se conectan y comunican entre sí y mediante la transferencia de datos (Rahman, 2003).

ARPANET (*Advanced Projects Agency Net*) fue una red interestatal, creada por el Ministerio de Defensa de los EEUU, a inicios de los años 60, esta red estaba destinada a cumplir con ciertos propósitos como: proteger las comunicaciones en caso de desastres naturales o guerras, permitir la incorporación de nuevos elementos y usar un lenguaje/protocolo entendible por cualquier ordenador (De La Cuadra, 1996).

Los orígenes de la Internet tienen diversos eventos de inicio, entre los que destacan: La llamada “Red Galáctica” que imaginó Licklider en 1962, que consistía en un conjunto de computadoras interconectadas globalmente a través de las cuales todos pudieran acceder rápidamente a datos y programas desde cualquier lugar (algo muy parecido al concepto de Internet de hoy en día). La teoría de la conmutación de paquetes en Kleinrock (1964) fue también un gran paso en el camino hacia las redes informáticas. Otro evento importante fue la comunicación entre dos computadoras en 1965, Merrill y Roberts conectaron dos computadoras, la TX-2 ubicada en Massachusetts y la Q-32 en California con una línea telefónica de marcación de baja velocidad creando la primera red informática de área amplia de la historia.

A fines de 1966, Roberts fue a DARPA para desarrollar el concepto de red informática y rápidamente armó su plan para “ARPANET”, publicándose en 1967. Ya en 1972, ARPANET se extendió por el mundo con 23 nodos ubicados en diferentes países. En 1969, cuatro computadoras host se conectaron juntas a la ARPANET inicial, y la Internet comenzó a despegar (Leiner, Cerf, & Clark, 2009). La Internet global se inició en los años

80 cuando la ARPA comenzó a convertir las máquinas conectadas a sus redes de investigación a los nuevos protocolos. Pronto ARPANET se convirtió en el Backbone de la nueva Internet y se utilizó para muchos de los primeros experimentos con TCP/IP. La transición a la tecnología de Internet concluyó a inicios de 1983 cuando por orden del secretario de Defensa todas las computadoras conectadas a redes de larga distancia debían usar TCP/IP.

En 1985, la *National Science Foundation* (NSF), tomó la decisión de que TCP/IP sería obligatorio para NSFNET. En 1993, el European Organization for Nuclear Research (CERN) anunció que la *World Wide Web* (WWW) sería gratuita para que todas las personas tuvieran la oportunidad de usar y desarrollar esta plataforma, un factor clave en el impacto que tendría esta red en el mundo. La política de privatización de NSF terminó en abril de 1995 con la desfinanciación de NSFNET Backbone. En menos de 9 años, Backbone había crecido de seis nodos con enlaces de 56 Kbps a 21 nodos con múltiples 45 Mbps. La Internet había crecido a más de 50,000 redes en los siete continentes y el espacio exterior.

Tal fue el peso del programa NSFNET (200 millones de dólares, 1986-1995) y la calidad de los propios protocolos que, en 1990, cuando ARPANET finalmente se desmanteló, TCP/IP había suplantado a la mayoría de los demás sistemas informáticos de área amplia, protocolos de red en todo el mundo, e IP se encaminaba a convertirse en el servicio portador para la Infraestructura de Información Global (Leiner, Cerf, & Clark, 2009)

Aspectos como la operación y gestión, sociales y de comercialización en la Internet fueron muy importantes en la transición eficaz, ya que llevaron a esta red a convertirse en una infraestructura de información ampliamente implementada y disponible, que hoy en día por su gran impacto a nivel mundial se considera como una tecnología de propósito general.

Tecnología de propósito general

Una tecnología se define como una Tecnología de Propósito General (GPT) cuando tiene efecto o impacto sobre la economía de un país o del mundo. También se puede

considerar una GPT cuando puede ser aplicada sobre productos o industrias con bajos costos de adaptación, implicando un beneficio, innovación o cambio en mercados o industrias completas y desencadenan beneficios indirectos para todo el sector (Gambardella & Giarratana, 2016).

Los países que invierten e integran tecnologías/servicios de telecomunicaciones (entre ellos la Internet) se benefician en innumerables aspectos, particularmente en industrias reduciendo tiempos, mejorando su eficiencia, alcanzando mayores niveles de escalabilidad, mejores alcances a masas, etc. (Clarke, Zhenwei, & Colin, 2015)

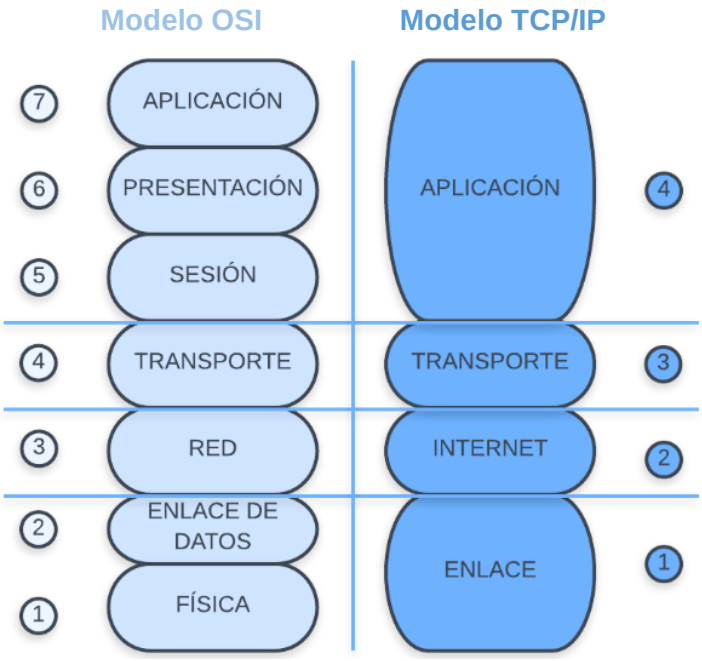
Clarke, Zhenwei y Lixin, en su estudio “The Internet as a general-purpose technology: Firm-level evidence from around the world” concluyen que la Internet es una GPT, puesto que, con información a nivel de empresas y corporaciones a nivel mundial, demuestran que el uso de servicios de Internet en general y el uso de la web por negocios locales particularmente, establecen una relación fuerte y directa con la productividad y crecimiento de la empresa o corporación. Este estudio encuentra además que aquellos países que manejan tecnologías/servicios de telecomunicaciones tienen un crecimiento más acelerado debido a los beneficios ya mencionados.

Por otro lado, parte del éxito del Internet también fue la creación de modelos de comunicación para el control de las redes y la transmisión de datos, y para el desarrollo de redes heterogéneas, compatibles con cualquier sistema, se estandarizaron diversos modelos, siendo ampliamente OSI y TCP/IP los más aplicados.

Modelos de comunicación de redes

Figura 1

Comparación de los modelos de comunicación de redes.



Modelo OSI: A principios de la década de 1980 se existieron grandes aumentos en el número y el tamaño de las redes, ya que muchos notaron las ventajas de utilizar la tecnología de red. A mediados de los 80s, las empresas comenzaron a tener problemas debido a la rápida expansión, ya que era muy difícil el intercambio de información para las redes que usaban diferentes especificaciones e implementaciones. El mismo problema ocurrió con las empresas que desarrollaron tecnologías de redes privadas o propietarias. Las tecnologías de red que seguían estrictamente reglas de propiedad no podían comunicarse con tecnologías que seguían reglas de propiedad diferentes (Salim, Mohammed, & Yahya, 2020).

Para solucionar este problema de incompatibilidad de las redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de redes como DECnet, SNA y TCP/IP para encontrar el conjunto de reglas generales de aplicación para todas las redes. La ISO creó un modelo de red para ayudar a los proveedores a crear redes compatibles con otras redes, y este fue el modelo de referencia de interconexión de sistemas abiertos (OSI).

Este modelo proporcionó a los proveedores un conjunto de estándares que garantizaron una mayor compatibilidad e interoperabilidad entre varias tecnologías de red producidas por empresas de todo el mundo (Salim, Mohammed, & Yahya, 2020). Las capas de este modelo son:

Aplicación: Es la capa del modelo más cercano al usuario, es la única capa del modelo que no brinda servicio a ninguna otra capa, sino únicamente a aplicaciones fuera del modelo OSI.

Presentación: Es la capa que garantiza que la información que se dirige a la capa de aplicación de un sistema este en un formato en común.

Sesión: Esta capa se encarga de establecer, administrar y finalizar las sesiones entre dos hosts que se comunican, además sincroniza el diálogo entre las capas de presentación de los dos anfitriones y gestiona el intercambio de datos

Transporte: Es la capa encargada de la segmentación de los datos del sistema del host emisor y vuelve a ensamblar los datos en un flujo de datos en el sistema del host receptor

Las capas superiores, de aplicación, presentación y sesión se ocupan de los problemas de la aplicación, mientras que las capas inferiores se ocupan de los problemas en la transferencia de datos.

Red: Es la capa encargada de proporcionar conectividad y selección de rutas entre dos sistemas host que pueden estar ubicados en redes separadas geográficamente.

Enlace de datos: es la capa encargada de garantizar una transmisión confiable de datos a través de un enlace físico. Se ocupa del direccionamiento físico, la topología de la red, el acceso a la red, la notificación de errores, la entrega ordenada de tramas y el acceso a los medios de control.

Física: La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas finales (Salim, Mohammed, & Yahya, 2020).

Modelo TCP/IP: El Departamento de Defensa de EEUU creó el modelo de referencia TCP/IP con el propósito de obtener una transmisión de paquetes ininterrumpida y bajo cualquier condición. TCP/IP se desarrolló como un estándar abierto, lo que ayudó a acelerar el desarrollo de este modelo como estándar. TCP/IP posee las siguientes capas: acceso a la red, internet, transporte y aplicación (Salim, Mohammed, & Yahya, 2020).

Aplicación: La capa de aplicación permite que las aplicaciones se comuniquen entre sí y brinda acceso a los servicios de las capas inferiores del modelo. En comparación con el modelo OSI, realiza la función de las capas de sesión, presentación y aplicación (Ver Figura 1).

Transporte: En inglés también se la conoce como 'Host to host layer', esta capa se encarga de gestionar el transporte y establecer la conexión entre hosts para el intercambio de datos. También es la responsable de crear los canales de comunicación entre la capa de aplicación y las capas inferiores del modelo. En comparación con el modelo OSI esta capa se asocia con la capa de transporte de dicho modelo.

Los principales protocolos TCP/IP que actúan en esta capa son:

- Protocolo de Control de Transmisión (TCP): TCP ofrece una mayor fiabilidad a la hora de transportar datos que la que ofrece UDP, ya que la aplicación hace el envío de datos recibe una confirmación de que los datos fueron recibidos.
- Protocolo de datagramas de usuario (UDP): UDP no proporciona un transporte de datos confiable. No se transmiten reconocimientos o confirmaciones.

Internet: Esta capa se encarga del empaquetado, direccionamiento y enrutamiento de los datos, en comparación con el modelo OSI, esta capa guarda relación con la capa de red.

Los principales protocolos TCP/IP que operan en la capa de Internet son:

- Protocolo de resolución de direcciones (ARP)
- Protocolo de Internet (IP)
- Protocolo de mensajes de control de Internet (ICMP)
- Protocolo de administración de grupos de Internet (IGMP)

***Enlace*:** Esta capa supervisa el intercambio de datos que se da entre el host y la red, se encarga de la supervisión del direccionamiento MAC y define los protocolos para la transmisión física de datos (Kabir, 2020).

El hardware que se conecta a esta interfaz de red es:

- El medio de red: Puede ser cableado coaxial, de par trenzado o fibra óptica. Actualmente la tecnología inalámbrica se ha vuelto una alternativa muy utilizada.
- Tarjeta de interfaz de red (NIC): la NIC tiene las siguientes direcciones:
  - Dirección MAC (dirección física)
  - Dirección IP (una dirección lógica)

Algo que también se ha ido aplicando a los modelos de redes con el paso del tiempo es el principio de extremo a extremo, que surge por la necesidad de obtener comunicaciones fiables en los entornos inestables o poco fiables.

Principio de extremo a extremo

Después de que Arpanet empezara a utilizar el protocolo TCP/IP, Saltzer, Reed y Clark escribieron el artículo "End-to-end arguments in system design", que se convertiría en la base del concepto de Internet. Este artículo trata acerca de los sistemas de comunicaciones, sobre lo que ocurre mientras se realiza la transmisión entre los dos extremos del sistema, como, recuperación de errores de bits, seguridad a través de cifrado, supresión de mensajes duplicados, recuperación de fallas del sistema, y la confirmación de la recepción del mensaje. Además, se da una justificación para mover las funciones en un

sistema de capas hacia la aplicación o capa que requiere la función, esto para mejorar la organización y modularidad del sistema (Saltzer, Reed, & Clark, 1984).

Extremo a extremo en redes: En redes este concepto se refiere a una red que no posee clientes ni servidores con roles fijos, sino, se forma por diferentes equipos con la capacidad de actuar como clientes y como servidores con respecto al resto de equipos que conforman la red. Visto de otra manera el concepto de extremo a extremo iría en contra del modelo cliente-servidor que ha existido desde los comienzos del Internet.

En cuanto a arquitectura la Internet desde sus inicios se manejó de tres formas, las cuales son: centralizada, descentralizada y mixta. Actualmente con la evolución del Internet las arquitecturas son solo descentralizadas o mixtas.

Descentralizada: Esta arquitectura no posee “servidor” central, todos los nodos tienen la misma importancia, conceptualmente es el que más se acerca a la definición de las redes de extremo a extremo, ya que cada equipo puede comportarse como servidor y como cliente en la misma red. La característica principal de esta arquitectura es el uso del TTL (tiempo de vida máximo), que se utiliza para evitar las trasmisiones infinitas, además de garantizar el envío de información ya puede optar por múltiples caminos para llevar a destino cualquier mensaje, sin importar que algún nodo deje de funcionar (Hernández, 2017).

Mixta: Esta es una mezcla entre la arquitecturas centralizada y descentralizada, aquí algunos equipos de la red funcionan como “servidores” centrales, los cuales se encargan de gestionar el tráfico hacia el resto de equipos.

Las redes de extremo a extremo pueden soportar las siguientes aplicaciones:

- Sistemas para transmisión y difusión de contenido multimedia por Internet
- Sistemas de datos distribuidos
- Sistemas de comunicación directa entre equipos y mensajería instantánea
- Sistemas de intercambio de archivos

- Sistemas para el trabajo
- Sistemas de telefonía por Internet basados en VoIP

El principio de extremo a extremo posee un enfoque arquitectónico, mediante el cual se puede reutilizar redes de servicios ya existentes (audio, video, etc.) como redes de comunicación de datos, mediante el cual los nodos finales se encarguen del reenvío de paquetes en ‘mejor esfuerzo’, particularmente en el transporte fiable de datos, o aplicaciones específicas, mediante la reorganización dependiendo de los resultados esperados en la comunicación, sin necesidad de una coordinación global o de modificar el diseño de sus redes subyacentes

Al tener esta libertad y adaptabilidad para reutilizar cualquier tipo de infraestructura de cualquier tecnología de transmisión, Internet no está sujeta a una tecnología de datos predeterminada, y parte de esto se debe a su infraestructura ideológicamente abierta, para cualquier persona, sea consumidor, proveedor de servicios, académico, etc. y es esto lo que le permite a esta red de redes estar en constante evolución (Internet Society, 2020).

Internet abierto

Según Lessig (1999) para comprender el Internet abierto, primero se debe conocer y relacionar conceptos, como el movimiento de software libre y el movimiento de software de código abierto. Ambos señalan que el software fundamental (el código) que gobierna Internet sea un software “abierto”, es decir que su fuente esté disponible para todos, para tomarlo, modificarlo y lo mejorarlo. Al ser de código abierto ha podido ser mejorado, y ahora es más robusto, eficiente y confiable.

Un ejemplo claro es el sistema operativo de GNU/Linux, ya que diferentes personas editaron su núcleo y lo convirtieron en un sistema operativo, considerado en muchas ocasiones como la mayor amenaza de Microsoft. Sin embargo, esta idea, de software de código abierto no se limita a sistemas operativos, se extiende a muchas de las tecnologías centrales que hacen funcionar la red. La mayor parte de Internet es código abierto, y la

mayor parte de su crecimiento y alcance se debe a esta característica particular (Lessig, 1999).

Según Cerf (2009), la Internet se considera como una plataforma abierta que abraza la libertad y la innovación de los usuarios, a pesar de ser una plataforma de propósito general, no se diseñó para alguna aplicación en particular, sino, es neutral con respecto a las aplicaciones que admite, ya que son los usuarios finales los que poseen el control del contenido y las aplicaciones que consumen y crean por lo que mantener la apertura del Internet es fundamental y se considera uno de los principales objetivos de la política de la banda ancha.

Para comprender por qué es importante la apertura de Internet, se deben observar diferentes puntos de vista: qué, dónde, cómo y por qué de la Red (Cerf, 2009).

1. La naturaleza en capas de Internet describe su arquitectura, como se observó en los modelos OSI y TCP/IP. Las capas crean estabilidad y brindan la capacidad a largo plazo para adaptarse a las nuevas tecnologías y admitir nuevas aplicaciones.
2. El principio de diseño de extremo a extremo describe dónde se implementan las aplicaciones en Internet, ya que esta red se diseñó para que las aplicaciones residieran principalmente en los "bordes" o nodos finales de la red, en lugar del núcleo, y da el poder y la funcionalidad de la red a los usuarios finales y los proveedores de contenido y aplicaciones.
3. El diseño del Protocolo de Internet (IP) separa las redes subyacentes de los servicios que se encuentran sobre ellas. IP fue diseñado para ser un estándar abierto, sin considerar a las redes físicas subyacentes que transportan paquetes como a la información de las diferentes aplicaciones y dispositivos que se transporta dentro de dichos paquetes. Internet enruta los datos por igual, sin favorecer a proveedores de contenido o aplicaciones particulares sobre otros, y de esta manera no está diseñado para ningún uso en particular.
4. Las aplicaciones y el contenido tienen éxito en función de los intereses de los usuarios, no por intervención de intermediarios.

La naturaleza abierta del Internet ha generado grandes beneficios sociales y económicos convirtiéndose hoy en día en la infraestructura esencial más utilizada, que sirve como enlace hacia múltiples actividades siendo uno de los pilares del crecimiento económico global (Cerf, 2009).

Los nuevos contenidos y aplicaciones de Internet generan mayor demanda de los usuarios de conexiones de banda ancha, por lo que este recurso empieza a volverse indispensable. Según Raúl Katz (2022) una mayor penetración en la banda ancha fija y móvil genera un impacto económico y social; económico debido al aumento en el PIB per cápita y social al impulsar la inclusión financiera, además de reducir la brecha digital al brindar conectividad a muchos más usuarios. Debido a la relevancia socioeconómica del Internet, en la región, se debe conocer la gobernanza del Internet y la importancia que tienen los marcos regulatorios y fiscales en el crecimiento de la economía digital (Katz, 2022).

Gobernanza del Internet

Después de que la Internet tomara la forma comercial actual, en la década de los 90s, su gobernanza aún no se consideraba como un tema de política importante. La gobernanza de Internet comenzó con dos formas relevantes, las cuales son: La gobernanza de Internet para desarrollar y operar Internet y la gobernanza de Internet para abordar la actividad en Internet (Solum, 2008).

A medida que Internet comenzó a globalizarse, el gobierno de Estados Unidos creó la Corporación de Internet para la Asignación de Nombres y Números (ICANN) sin fines de lucro para operar los DNS. ICANN se estableció como una entidad de múltiples partes interesadas con aportes de los gobiernos, la comunidad técnica, los usuarios comerciales y no comerciales y la sociedad civil (Solum, 2008).

Es así que la gobernanza de Internet se planteó oficialmente por primera vez a nivel internacional durante la Cumbre Mundial sobre la Sociedad de la Información (CMSI)

acordada por la Unión Internacional de Telecomunicaciones (UIT) bajo el patrocinio del entonces secretario general de las Naciones Unidas, Kofi Annan. La primera fase se llevó a cabo en Ginebra en 2003 y la segunda fase en Túnez en 2005. Se acordó abordar la creciente brecha digital entre países con respecto al acceso a las Tecnologías de la Información y la Comunicación (TIC), en particular, Internet (Kende, 2020).

Las primeras diferencias de la gobernanza del Internet se dieron debido al papel que estaba desempeñando el gobierno de los EEUU. Varios gobiernos se opusieron a que los DNS, una parte clave del Internet, estén a cargo de la ICANN, una entidad privada, con la supervisión del gobierno de los EEUU, entonces presionaron por una mayor participación de los gobiernos internacionales.

La solución a este problema fue la creación del Grupo de Trabajo sobre la Gobernanza de Internet (WGIG) entre las dos fases de la CMSI. WGIG incorporó un modelo de gobernanza de Internet de múltiples partes interesadas, en el que las partes participan en los debates y el desarrollo de políticas, asumiendo diferentes roles de acuerdo al tema y el foro (Kende, 2020). Finalmente se definió a la Gobernanza del Internet como la gestión multilateral democrática y transparente del Internet con la participación completa de los gobiernos, sector privado, sociedad civil y organizaciones internacionales, para garantizar una distribución justa de los recursos, permitir el acceso de todos y asegurar el funcionamiento constante y seguro de Internet (CMSI, 2005).

El modelo de gobernanza de Internet de múltiples partes interesadas que surgió de la CMSI refiere que ninguna organización es propietaria o están encargadas del Internet. La cumbre de Internacional Ginebra 2003 sobre la Internet tuvo un papel muy importante en la gobernanza de Internet, además alberga algunos de los problemas internacionales más relevantes relacionados con la gobernanza (Kende, 2020).

Estos problemas incluyen cerrar la brecha digital y ayudar a desarrollar una economía digital en todos los países. Además, hoy en día se ha vuelto muy importante

garantizar la ciberseguridad y la confianza en las actividades en línea, como también, garantizar la aplicación de los derechos humanos en estas actividades en línea (Kende, 2020)

En el congreso de Túnez 2005 se reafirmaron los principios enunciados en la fase de Ginebra de la CMSI, en 2003, de que Internet se ha convertido en un servicio mundial disponible para el público y su gobernanza debe constituir un tema central de la agenda de la Sociedad de la Información (SI). La gestión internacional de Internet debe ser multilateral, transparente y democrática, con la total participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Debe garantizar una distribución equitativa de los recursos, facilitar el acceso para todos y garantizar un funcionamiento estable y seguro de Internet, teniendo en cuenta el multilingüismo (CMSI, 2005)

En otras palabras, el desarrollo social del Internet, se debe en gran parte a la gobernanza, pero existe un criterio que en ocasiones tiende a convertirse en una problemática, para dicho desarrollo, este se denomina neutralidad de la red.

Neutralidad de la red

La NR es un principio que establece que todo el contenido que pasa a través de Internet, debe tener un trato igualitario, dando apertura a la libre circulación de información, sin discriminar, sin importar origen, uso o aplicación, dando la potestad única a los proveedores del servicio de garantizar acceso y conexión a los usuarios sin restricciones de los contenidos que atraviesan la red (Wu, 2003). Este principio tiene como objetivo principal proteger la competencia leal, la innovación, y garantizar la elección de los consumidores. De acuerdo con los principios de NR los ISP’s no pueden bloquear, limitar o priorizar ningún tráfico de manera arbitraria. Sin embargo, existen excepciones en virtud de restricciones técnicas específicas (por ejemplo, requisitos de calidad del servicio) o administrativas (por ejemplo, enrutamiento en emergencias) (Garret, Setenareski, Peres, & Erpen, 2022).

Autores como Schulzrinne (2018) y Bauer, Knieps (2018) mencionan que un menor control sobre cómo los ISP administran sus redes produce un mercado más competitivo. En cambio, otros autores como Yiakoumis, Katti y McKeown (2016), afirman que deberían ser los consumidores quienes opinen sobre cómo se está gestionando su tráfico (Garret, Setenareski, Peres, & Erpen, 2022).

El término de Neutralidad de red fue introducido por Tim Wu (2003), a pesar de que la idea tiene sus indicios en el movimiento de acceso abierto de Lawrence Lessig (2001) (Jan Krämer, 2013), y precisamente son ellos en el año 2003 quienes enviaron una carta a la Comisión Federal de Comunicaciones (FCC) con la propuesta hacia una Internet neutral. Lo más destacado de esta carta era una solución regulatoria que permita a los operadores de infraestructura regularse a sí mismos, y así promover la competencia justa entre las aplicaciones en las redes de banda ancha (Garret, et al, 2022)

Según académicos, abogados e ingenieros, el término "neutralidad de la red" puede referirse a tres entendimientos diferentes, pero que funcionan simultáneamente. El primero se refiere a los principios de NR teóricos, principalmente a aquellos que se deben proteger, como la innovación, la libertad de expresión y la competencia leal en Internet. El segundo, abarca el conjunto de reglas y políticas legales presentes en los marcos regulatorios de cada país y que deben hacerse cumplir por el ente de control a cargo en cada uno de ellos. Finalmente, se refiere también a los protocolos de red y a la arquitectura de Internet, en el nivel técnico, y cómo los ISP discriminan entre contenido, servicios o aplicaciones (Madhvapaty & Goyal, 2014).

Cabe mencionar que el principio de la neutralidad de red se aplica principalmente al Internet público, con el objetivo de garantizar que todos los usuarios tengan acceso al mismo contenido y servicios en Internet sin restricciones o discriminaciones, independientemente de su proveedor de servicios de internet (ISP) o su ubicación geográfica. Sin embargo, el concepto de neutralidad de la red también se puede aplicar a

otras redes, como las redes privadas o las redes empresariales, pero en esos casos las regulaciones pueden variar o no existir (Van Schewick, 2010).

La llegada de nuevas tecnologías como 5G e IoT, aumentan los retos en el debate sobre NR, ya que al ser tecnologías de alta demanda de ancho de banda, llegan con nuevos métodos de gestión de red, un ejemplo es el 'slicing', el cual consiste en crear redes virtuales personalizadas, sobre el ancho de banda otorgado, las cuales funcionan de acuerdo a las necesidades determinadas por aplicaciones, servicios, operadores y clientes (por ejemplo, velocidades de datos y latencia), y usar este 'slicing' quebranta los principios estrictos de NR, ya sea con priorización, discriminación, y degradando o mejorando la configuración de QoS. En algunos países existen ciertas regulaciones de NR para admitir la diferenciación del tráfico en el caso de aplicaciones que poseen estrictos requisitos de QoS, por ejemplo, en la UE se definen como servicios especiales y no son parte del Internet público (Garret, et al, 2022).

Entre los principales debates sobre políticas de NR se puede mencionar a:

Estados Unidos: En EEUU los procesos de regulación comenzaron en el 2008, con la ley HR5353 o "Ley de Preservación de la Libertad en Internet". Para el 2010 la FCC presentó tres reglas para la preservación del Internet como una plataforma abierta orientada a la innovación, inversión, crecimiento económico, competencia leal y la libertad de expresión, las cuales eran: transparencia, no bloqueo y ninguna discriminación irrazonable. Dichas reglas fueron puestas a debate por la Corte de apelaciones de Columbia en 2014. Posteriormente en 2015 la FCC reclasificó los servicios de banda ancha como "servicios de telecomunicaciones", con el fin de conseguir medios legales para implementar reglas para preservar y proteger una Internet abierta.

Estados Unidos:En EEUU los procesos de regulación comenzaron en el 2008, con la ley HR5353 o "Ley de Preservación de la Libertad en Internet". Para el 2010 la FCC presentó tres reglas para la preservación del Internet como una plataforma abierta orientada

a la innovación, inversión, crecimiento económico, competencia leal y la libertad de expresión, las cuales eran: transparencia, no bloqueo y ninguna discriminación irrazonable. Dichas reglas fueron puestas a debate por la Corte de apelaciones de Columbia en 2014. Posteriormente en 2015 la FCC reclasificó los servicios de banda ancha como “servicios de telecomunicaciones”, con el fin de conseguir medios legales para implementar reglas para preservar y proteger una Internet abierta.En 2017 se derogó la normativa de 2015, entrando en vigencia durante 2018 y en 2019 se presentó un proyecto de ley para restablecer la regulación derogada, y fue la “Ley Salvemos Internet”, la cual fue aprobada por la Cámara de Representantes, actualmente está a la espera de su aprobación por parte del senado. Cabe mencionar que, en ciertos estados, como California, tomaron iniciativas propias para un restablecimiento total o parcial sobre las reglas de NR derogadas en el 2017 (Garret, Setenareski, Peres, & Erpen, 2022).

Unión Europea (UE): La Unión Europea (UE) tuvo varios intentos para implementar políticas de NR entre 2009 y 2014. El primero intento se dio en 2009, cuando la Comisión Europea (ECOM) creó 12 reformas para garantizar derechos de los consumidores, una Internet abierta, un mercado único europeo de telecomunicaciones y alta velocidades de conexión a Internet para todo usuario final, además del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (BEREC). En 2011, el Parlamento Europeo (PE) concluyó que ya no serían necesarias más medidas regulatorias y exigió a los ISP transparencia respecto sus prácticas de gestión del tráfico. Ya en 2014, ECOM presentó un informe que recogía la situación de NR en cada país de la UE los años anteriores.

Finalmente, en 2015, los diferentes organismos de regulación y control (EP, ECL y ECOM) aprobaron la “Regulación de Internet Abierta”, estableciendo las regulaciones del Mercado Único de Telecomunicaciones (TSM) para los 28 países miembros de ese entonces. Tim Berners-Lee dijo que dicho reglamento era débil, ya que daba oportunidad a los ISP de tomar las denominas ‘vías rápidas’, tarifas de zero-rating, definir clases de servicio y reducir la velocidad del tráfico en cualquier instante que este considere necesario

hacerlo. Entonces en 2016, BEREC definió cómo las agencias reguladoras de los países de la UE deben implementar las reglas de NR y cómo se deben tratar los casos específicos.

Finalmente, en 2019, se actualizaron las directrices de 2016 y cuya versión final de las se publicó en 2020. Con cambios en la inclusión de una “metodología de evaluación de ofertas zero-rating y similares”, que fueron puestas a revisión en 2021, para una consulta pública sobre un nuevo borrador con las Directrices de Internet Abierta para 2022 (Garret, Setenareski, Peres, & Erpen, 2022).

Chile: Chile se convirtió en el primer país a nivel mundial en aplicar una ley para la Neutralidad de red. La ley 20.453 de 2010, establece que los ISP:

- No pueden bloquear, interferir, discriminar, impedir o restringir arbitrariamente el derecho de cualquier usuario a acceder, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet.
- No pueden limitar el derecho de los usuarios a hacer uso o introducir cualquier tipo de dispositivo en la red.
- Deben prestar (a los usuarios que soliciten), servicios de control parental de los contenidos que atenten contra las leyes o la moral.
- Deben publicar en su sitio web toda la información relativa a las características de los servicios de Internet que ofrecen, tales como velocidad, calidad y garantías del servicio, distinguiendo entre conexiones nacionales e internacionales.

En 2014, Subsecretaría de Telecomunicaciones (SUBTEL) exigió a los ISP eliminar las ofertas de tarifa cero (Redes Sociales Libres), ya que esto beneficia el uso de servicios específicos, y va en contra de la ley de NR. El reglamento menciona que no se puede bloquear, interferir, discriminar, ni restringir arbitrariamente cualquier tipo de contenido, aplicación o servicio legal a través de Internet, en otras palabras, se debe ofrecer al usuario un servicio de conectividad que neutral (Subsecretaría de Telecomunicaciones, 2014).

Actualmente la tecnología 5G, ya se encuentra operando en Chile, y lo que se busca es darle flexibilidad a la ley de NR en cuanto al ‘slicing’, ya que, si bien la SUBTEL estaría en contra de este método de gestión de tráfico, la FNE (Fiscalía Nacional Económica) buscaría que se admita cierta diferenciación de tráfico por razones técnicas, de modo que pueda existir armonía entre las redes virtuales personalizadas y una Internet neutral (Johannsen, 2022).

Ecuador: En 2012 en Ecuador, el Consejo Nacional de Telecomunicaciones (CONATEL) emitió el: “Reglamento Abonados Servicios Telecomunicaciones y Valor Agregado”, que en su Art. 41. menciona que “Los prestadores de servicios de telecomunicaciones y servicios de valor agregado no pueden bloquear, priorizar, restringir o discriminar de forma injustificada aplicaciones, contenidos o servicios, sin consentimiento del usuario o por orden de la autoridad competente”. Sin embargo, estas normas sí consentían las prácticas de gestión de tráfico, pero solo para garantizar la QoS y sin que se perjudique a ningún usuario (CONATEL, 2012).

Con la eliminación del CONATEL y la creación del ARCOTEL en 2015, el reglamento de 2012 formó parte de la Ley Orgánica de Telecomunicaciones de 2015 (LOT 2015), pero ya con mención directa al principio de NR, en los objetivos del Art. 3, principios del Art. 4 y 66, y en el artículo 22, numeral 18, como derechos de los clientes, usuarios o abonados (Cordero, 2019). En los que básicamente se establece que los proveedores de servicios (ISP), no podrán bloquear, limitar, discriminar, ni restringir los derechos de sus usuarios a utilizar, enviar o recibir cualquier contenido, aplicación o servicio a través de Internet (AsambleaNacional, 2015).

Pese a esto, la LOT realiza ciertas omisiones, como: definición de la NR, ya que usa el concepto de la ITU, que es confuso y difícil de aplicar. También el Art. 66 de la ley, que permite a los ISP establecer planes de tarifas constituidos por servicios o productos en particular. De igual manera, los conceptos de no discriminación de reglamentos anteriores como los de 2012, no fueron incluidos; dejando todos los aspectos que atentan contra la NR

y vulnerando a los usuarios frente a los abusos que podrían incurrir los proveedores de servicio. Tal es el caso de los servicios de Zero Rating (ZR), con las redes sociales libres, en donde se ofrecen servicios ilimitados de ciertas aplicaciones, pero con limitaciones en ciertas funcionalidades lo que va en contra de la NR, y a pesar de esto aún en el país las operadoras móviles siguen ofertando este tipo de servicio (Triviño, Franco, & Ochoa, 2020).

En el siguiente cuadro se puede observar un resumen de las políticas públicas de ciertos países en base a la neutralidad de red.

Tabla 1

Comparativa de las políticas de NR de diferentes países

País	Nivel de la política de NR	Detalle de la política
Estados Unidos (California, Oregon, Washington)	Fuerte (Kang, 2018), (Lee, 2018), (ACLU, 2018)	Las leyes SB-822 (California), SB 844 (Oregón) y House Bill 2282 (Washington), estas leyes se consideran fuertes ya que han sido aprobadas en la legislación de cada estado y dispuesto un organismo de control para llevar a cabo su cumplimiento, como: California Consumer Privacy Act (CCPA), Departamento de Servicios Públicos de Oregon (OPUC), Comisión de Servicios Públicos de Washington
Unión Europea	Fuerte (Berners-Lee, 2015)	En la legislación de la UE se encuentra en rigor el Reglamento (UE) 2015/2120, es la ley vigente sobre el Internet abierto y la NR, las normas se rigen a través del Parlamento Europeo (PE) y se considera una ley fuerte ya que ha sido reforzada, además dispone de un ente de control encargado de hacer cumplir este reglamento, y es la Agencia Europea para las Comunicaciones Redes y Tecnologías de la Información (BEREC).
Chile	Fuerte	La ley N° 20.453 (2010) se encuentra en el marco legislativo del país, y habla sobre las políticas que deben seguir los ISP con respecto a la NR.

País	Nivel de la política de NR	Detalle de la política
	(Garret, et al, 2022) (CRC, 2021)	Se considera fuerte ya que está bien definida en la legislación, y está bien aplicada, además, posee un organismo de control, la SUBTEL.
Brasil	Fuerte (Garret, et al, 2022) (CRC, 2021)	La legislación sobre la NR en este territorio es fuerte, ya que tiene La ley 12965 (2014) en efecto y un decreto 8771 (2016). Existe un ente encargado de hacer cumplir estas leyes conocido como Agencia Nacional de Telecomunicaciones (ANATEL).
Ecuador	Débil (Garret, et al, 2022) (CRC, 2021)	La ley vigente es la LOT 2015, y el organismo de regulación y control para esta ley es la ARCOTEL, se considera débil primeramente porque no está bien definida la NR, no se dispone de una legislación acorde a todo lo que desencadena garantizar una internet neutral o abierta, además su ente de control es limitado, no dispone de los recursos para poder monitorizar a los IPS y verificar que se esté cumpliendo con este principio.
Argentina	Débil (Garret, et al, 2022) (CRC, 2021)	La ley vigente se es la 27.078 (2014), se encuentra en el marco regulador de las telecomunicaciones, y está regulado por el Ente Nacional de Comunicaciones (ENACOM), pese a esto se considera débil ya que su definición no es muy clara, por ende, su regulación tampoco.

Tal como se menciona en la tabla 1, existen diferentes políticas de Neutralidad de Red (NR) en todo el mundo, algunas son más fuertes que otras. Países como Estados Unidos, la Unión Europea, Chile y Brasil han trabajado en fortalecer sus marcos regulatorios y cuentan con leyes más sólidas, algunos definen los casos especiales en donde se permite que los ISP realicen DT o gestión razonable de su tráfico, se mencionan los casos sobre los servicios especializados, las tarifas de zero-rating (Garret, Setenareski, Peres, & Erpen, 2022), tethering (CRC, 2021), la transparencia del tráfico en cuanto a la NR.

Sin embargo, países como Ecuador, Argentina, entre otros poseen leyes o estatutos que hablan sobre la NR, pero al tener un mal concepto sobre el término, falta de claridad sobre las políticas y la falta de presión a los organismos de control por parte de las autoridades desencadenan las posibles violaciones al principio por parte de los proveedores de servicio de Internet (CRC, 2021).

El debate sobre la Neutralidad de la Red se ha intensificado debido a la congestión actual en Internet, así como a la pandemia COVID-19 que ha llevado a las personas a trabajar y aprender desde sus hogares. El aumento del tráfico en línea ha llevado a los proveedores de servicios de Internet (ISP) a implementar prácticas de gestión de tráfico para mantener el buen funcionamiento de su servicio. Esto ha generado una mayor controversia sobre la importancia de garantizar la Neutralidad en la Red y proteger la igualdad de acceso a Internet para todos los usuarios (Triviño, Franco, & Ochoa, 2021).

Existen excepciones a la NR, como la gestión y la diferenciación de tráfico, que permiten a los ISP optimizar y administrar sus redes de manera eficiente, siempre y cuando no vayan en contra del objetivo general de la NR (Garret, Setenareski, Peres, & Erpen, 2018). La gestión de tráfico permite a los proveedores de servicios de Internet equilibrar la demanda en su red. Por otro lado, la diferenciación de tráfico ofrece diferentes niveles de servicio a diferentes usuarios o tipos de tráfico, como voz o video. Por lo tanto, identificar posibles violaciones al principio de Neutralidad de la Red (NR) a través de prácticas de diferenciación de tráfico puede ser muy útil para garantizar la igualdad de acceso a Internet para todos los usuarios.

Diferenciación de tráfico

Las técnicas de gestión de la red deben ser transparentes, proporcionales, razonables y no discriminatorias, basadas en diferencias técnicas objetivas, de acuerdo con las disposiciones legales vigentes en algunos países (Triviño, Franco, & Ochoa, 2021), siendo así, la diferenciación de tráfico puede verse como una técnica de gestión beneficiosa o perjudicial según cómo aplique.

Se considera beneficiosa cuando se usa para mejorar el rendimiento y la calidad de servicio en la red, siempre y cuando se sigan consideraciones éticas y legales al implementarla y se considera perjudicial o incluso ilegal si se utiliza para bloquear o limitar el acceso a ciertas aplicaciones o servicios atentando contra el principio de NR (Molina, 2011). La diferenciación de tráfico injusta afecta los tres conceptos clave en el éxito del Internet (innovación, competencia leal, y libertad de elección del consumidor) (Garret, Setenareski, Peres, & Erpen, 2018).

El tráfico puede discriminarse de acuerdo al protocolo, origen, destino, carga útil, etc. De igual forma se pueden emplear diversas técnicas con el mismo propósito, como:

- Throttling: Controla el volumen del tráfico que pasa por la red en un determinado tiempo, y encola o elimina paquetes cuando existe congestión.
- Shaping: Realiza un control exhaustivo en el volumen del tráfico, tasa de transferencia, entre otros, siendo más completo que el 'Throttling'.
- De acuerdo al consumo umbral: Se basa en el control del consumo que tiene un usuario en un determinado tiempo (usualmente es un mes) hasta llegar a un valor umbral y a partir de este se empieza a reducir la velocidad de conexión, esta práctica es utilizada por los ISP móviles, lo que les permite estimar valores de consumo por usuario y planificar su red.
- Basada en bloqueo: Esta técnica permite realizar un bloqueo de tráfico hacia las aplicaciones que utilicen o consuman un alto ancho de banda (archivos P2P, videos, etc.).
- Basadas en aplicación: Esta técnica utiliza un conjunto de reglas y algoritmos para asegurar que diferentes tipos de tráfico reciban un tratamiento adecuado en función de las necesidades de ciertas aplicaciones y servicios.
- Basada en usuario: consiste en repartir el ancho de banda a todos los usuarios por igual, para ser eficaz, esta práctica debe ser medida en periodos de tiempo cortos, ya que de lo contrario no podría combatir la congestión en la red. A diferencia de la

técnica basada en la aplicación, esta estrategia proporciona al operador una herramienta importante para mantener una calidad de servicio media constante, respetando la NR (Molina, 2011).

Por otro lado, las prácticas de diferenciación de tráfico (DT) deben ser transparentes, ya que afectan directamente a los usuarios finales, proveedores de contenido y servicios. Las regulaciones que existen actualmente en muchos países no son suficientemente fuertes para garantizar la neutralidad de la red por parte de los proveedores de servicios de Internet. Por lo tanto, es importante monitorear la red para detectar posibles prácticas discriminatorias (Garret, et al, 2018).

Herramientas de monitoreo de red: Las herramientas de monitoreo de red han evolucionado significativamente a lo largo de la historia. En las primeras décadas las herramientas de monitoreo eran muy limitadas si se las compara con las que se tienen actualmente, se utilizaban principalmente para detectar problemas de conectividad. Con el tiempo, las redes se volvieron más complejas y se desarrollaron herramientas más avanzadas para monitorizar y diagnosticar problemas en la red.

En la década de 1980 y principios de los 90, surgieron las primeras herramientas de monitoreo de red basadas en SNMP (Simple Network Management Protocol) para recopilar datos de los dispositivos de red. A medida que las redes se volvieron más complejas y se introdujeron nuevos protocolos y tecnologías, las herramientas de monitoreo evolucionaron para incluir capacidades de análisis de tráfico en tiempo real, detección de problemas y generación de alertas (Edwards, 2020).

En la década de 2000, con la popularidad de las redes de área amplia (WAN) y las redes privadas virtuales (VPN), las herramientas de monitoreo se volvieron más importantes que nunca para garantizar la disponibilidad y rendimiento de las aplicaciones críticas. Con el aumento de la movilidad y el Internet de las cosas (IoT), las herramientas de monitoreo de

red se han adaptado para monitorear y gestionar dispositivos móviles y dispositivos IoT (Zidek, Magdina, & Alkhalaf, 2022).

En la actualidad, las herramientas de monitoreo de red se han vuelto cada vez más sofisticadas y se utilizan para no solo detectar problemas, sino también para analizar el tráfico, mejorar el rendimiento, garantizar la seguridad, cumplir con las regulaciones y tomar decisiones adecuadas, esto se puede realizar a través de dos tipos de mediciones:

- Monitoreo pasivo: esta técnica permite evaluar el rendimiento y la condición de la red sin requerir modificaciones en el tráfico existente. Se realiza mediante el uso de protocolos integrados en componentes de red como enrutadores, conmutadores, entre otros. La medición se realiza de manera periódica y se determina el estado y rendimiento de la red a partir de las métricas recolectadas.
- Monitoreo activo: Este tipo de medición se implementa a través de la inyección de tráfico a la red monitoreada, parámetros como: el tiempo de ida y vuelta (RTT), la tasa de pérdida promedio, el ancho de banda de la conexión y el rendimiento del paquete ayudan a determinar con gran precisión el flujo del tráfico (Zidek, Magdina, & Alkhalaf, 2022).

Monitoreo activo: Este tipo de medición se implementa a través de la inyección de tráfico a la red monitoreada, parámetros como: el tiempo de ida y vuelta (RTT), la tasa de pérdida promedio, el ancho de banda de la conexión y el rendimiento del paquete ayudan a determinar con gran precisión el flujo del tráfico (Zidek, Magdina, & Alkhalaf, 2022). Existen diferentes herramientas de monitoreo activo y pasivo, cada una con diferentes especificaciones y diferentes métricas a considerar, cada una con el mismo propósito, encontrar DT y cumplimiento de NR. Entre las herramientas más conocidas se detallan en la siguiente tabla.

Tabla 2

Herramientas de monitoreo activo y pasivo para DT (Obtenido de: **(Castoreo, Maillé, & Tuffin, 2020)***)*

Herramienta	Diferenciación	Tráfico	Métricas	Medición	Tipo de prueba
Switzerland	Integridad del paquete	Cualquiera	Hashing de paquetes	Pasiva	Comparación
NetPolice	Tipo/basado en enrutamiento	HTTP, BitTorrent, SMTP, PPLive, VoIP	Tasa de pérdida de paquetes	Activa	Kolmogorov-Smirnov con Jackknife
Nano	Basado en tipos	Cualquiera	Throughput	Pasiva	Inferencia causal
Glasnost	Basado en tipos	BitTorrent (se pueden añadir más)	Throughput	Activa	Comparación de rendimiento máximo
DiffProbe	Basado en tipos	Skype, Vonage	Throughput	Activa	Kullback-Leiber
POPI	Basado en tipos	ICMP, FTP, Telnet, POP3, BGP, HTTPS, Fasttrack, Donkey, Gnutella, BitTorrent	Tasa de pérdida de paquetes, delay	Activa	Clasificación, promedio y agrupación
Packsen	Basado en tipos	BitTorrent	Tasa de pérdida de paquetes	Activa	Mann-Whitney U

Herramienta	Diferenciación	Tráfico	Métricas	Medición	Tipo de prueba
OONI Probe	Basado en tipos	web, DNS, Tor, messaging applications	Resolución DNS, conexión exitosa	Activa	Comparación
ChkDiff	Basado en tipos	Cualquiera	Tasa de pérdida de paquetes, delay	Activa	Kolmogorov-Smirnov
Wehe	Basado en tipos	Cualquiera	Tasa de pérdida de paquetes, throughput, delay	Activa	Personalizado inspirado en Kolmogorov-Smirnov
CONNEcT	Basado en tipos	Cualquiera	Tasa de pérdida de paquetes	Pasiva	Sin análisis

Muchas de las herramientas mencionadas fueron únicamente implementadas por proyectos de investigación, y, por consiguiente, no se han hecho públicas o de libre acceso. Las únicas herramientas de acceso público y disponibles al momento de esta investigación son dos, Wehe y OONIProbe (Castoreo, Maillé, & Tuffin, Weaknesses and Challenges of Network Neutrality Measurement Tools, 2020).

Wehe: como se muestra en la tabla 2, es una herramienta de medición activa, utilizada principalmente en terminales móviles. Esta herramienta se conecta a servidores y replica el tráfico de aplicaciones específicas (Netflix, Facebook, Disney+, etc.) a través de una VPN. El tráfico es enviado sin encriptar, y se reproduce encriptado, esto para detectar diferencias potenciales en términos de rendimiento, asumiendo que el tráfico cifrado no está diferenciado, utilizando una variante de la regla de Kolmogorov-Smirnov (esta regla permite

verificar si una muestra proviene de una determinada distribución teórica o no) (Castoreo, Maillé, & Tuffin, Weaknesses and Challenges of Network Neutrality Measurement Tools, 2020).

Wehe como se muestra en la tabla 2, es una herramienta de medición activa, utilizada principalmente en terminales móviles. Esta herramienta se conecta a servidores y replica el tráfico de aplicaciones específicas (Netflix, Facebook, Disney+, etc.) a través de una VPN. El tráfico es enviado sin encriptar, y se reproduce encriptado, esto para detectar diferencias potenciales en términos de rendimiento, asumiendo que el tráfico cifrado no está diferenciado, utilizando una variante de la regla de Kolmogorov-Smirnov (esta regla permite verificar si una muestra proviene de una determinada distribución teórica o no) (Castoreo, Maillé, & Tuffin, Weaknesses and Challenges of Network Neutrality Measurement Tools, 2020).OONI Probe es también una herramienta de medición activa, su objetivo principal es detectar el bloqueo de tráficos web, aplicaciones de mensajería, entre otros., mediante el DNS.

OONI Probe: es también una herramienta de medición activa, su objetivo principal es detectar el bloqueo de tráficos web, aplicaciones de mensajería, entre otros., mediante el DNS. Primero se hace una prueba de conectividad hacia el servicio, y se compara la resolución de DNS con la DNS neutral (servidores de Google) asumiendo que no hay manipulación de DNS durante este proceso. En caso de fallar la conexión se concluye que existe bloqueos a nivel de TCP. En caso de funcionar la conexión, la herramienta pasa a solicitar un recurso, en caso de abortar la solicitud el bloqueo está a nivel de HTTP. Con esto el usuario conoce en qué nivel se produce el bloqueo y puede buscar la manera de usarlo (Castoreo, Maillé, & Tuffin, Weaknesses and Challenges of Network Neutrality Measurement Tools, 2020).

Uno de los problemas en ciertas herramientas como menciona Castoreo, Maille y Tuffin (2020) es la réplica de los paquetes de un servicio en específico en ciertas herramientas de inyección, por lo que el uso de técnicas como la Inspección Profunda de

paquetes (DPI) pueden ser de mucha ayuda, ya que es una técnica utilizada para analizar el tráfico de red a nivel de paquetes, inspecciona y analiza los paquetes más allá de las cabeceras, en un punto de la red diferente a la de los extremos puede ser utilizado para detectar y medir la DT, ya que, puede incluso analizar el contenido del mismo paquete (DeRose, 2010).

La DPI se desarrolla por la necesidad de conocer la información sobre el protocolo y la aplicación que transporta un paquete. Esto se realiza mediante la búsqueda de firmas (identificadores) que los desarrolladores de DPI entregan en la búsqueda de un protocolo o aplicación. DPI también puede clasificar protocolos en tiempo real, llegando a analizar la información del usuario de ser necesario, en comparación con técnicas empleadas por otras herramientas DPI es la más completa (Molina, 2011).

DPI supera a otras herramientas de monitoreo de red o sniffers como Wireshark, ya que proporciona a profundidad el detalle de los paquetes, incluso llegando a analizar tipos de tráfico encriptado, por lo que se puede decir que nada está oculto cuando se hace este tipo de inspección. Las principales herramientas que realizan DPI son: PACE, nDPI, NBAR, Qosmos ixEngine, Netify Agent (Netifyd), NetFort LANGuardian, SolarWinds Network Performance Monitor, ManageEngine NetFlow Analyzer, entre otros (Wilson, 2022).

Capítulo III

Diseño e Implementación

Con lo visto en el capítulo anterior, el diseño y desarrollo de la herramienta de inyección y monitoreo de tráfico, se realizó considerando cinco aspectos fundamentales:

- Protocolo de Internet IPv4.
- Tipo de medición (activa o pasiva).
- Servicios o aplicaciones a simular (streaming de video, videoconferencias, etc.), cuyo correcto funcionamiento es sensible a la latencia y ancho de banda.
- Métricas a obtener (latencia, pérdida de paquetes) considerando aquellas obtenidas por herramientas ya existentes y disponibles públicamente (throughput por Wehe y restricción/bloqueo por OONI Probe).
- Tipo de conexión (fija y móvil).

IPv4 se mantiene como el protocolo predominante a pesar de que IPv6 ha estado disponible por varios años, pero su adopción ha sido limitada, además de que la transición de IPv4 a IPv6 presenta múltiples retos, desafíos y riesgos (Šimon & Ladislav, 2019). Otro punto a considerar es la diferencia en características de red de IPv6, pues este introduce varios cambios en las cabeceras y en el manejo de los paquetes (Ordabayeva, G, et al, 2020). Es por esto que enfocando el estudio a IPv4 se tiene una mayor relevancia en la actualidad (Carisimo, Esteban, et al, 2019).

Para un monitoreo activo es necesario la captura, replicación, generación e inyección de tráfico a la red monitoreada, misma que simule el uso de servicios o aplicaciones ya conocidas (Castoreo, Maillé, & Tuffin, 2020).

Los servicios o aplicaciones elegidos, cuyo tráfico se simuló, son Netflix, YouTube y Google Meet, los dos primeros siendo las aplicaciones más populares de video entretenimiento y el tercero entre los más populares de comunicación (Curry, 2023) (Cisco, 2021). Estos en conjunto producen la mayor cantidad de carga a las redes de telecomunicaciones, por lo que podrían ser objeto de prácticas discriminatorias.

Las dos herramientas de inyección de tráfico para detectar DT que se encuentran disponibles públicamente en la actualidad se enfocan en una característica en particular. La herramienta Wehe usa ‘throughput’, que es la cantidad de información en un periodo de tiempo o comúnmente conocido como ‘velocidad’ (10, 50, 100 Mbps), para detectar potenciales diferencias en términos de rendimiento. En cambio, la herramienta OONI Probe se enfoca en la conexión o acceso, esto para detectar la restricción directa o bloqueo hacia una aplicación, servicio, contenido o servidor específico.

Es así que, para el caso de este trabajo de investigación, se optó por un enfoque hacia la latencia (*round-trip time*, o RTT) y la pérdida de paquetes (*packet loss*). Latencia o RTT es el tiempo desde que un paquete de información es enviado (desde el host o usuario hacia el servidor de una aplicación o servicio) y la llegada de su respuesta (desde el servidor hacia el host), generalmente, siendo el segundo aquel que contiene la mayor cantidad de información en la comunicación. La pérdida de paquetes es la cantidad de paquetes perdidos en la comunicación, es decir que no llegaron a su destino final, generalmente se da por congestión en la red, problemas o fallos en dispositivos finales o intermedios (terminal, servidores, enrutadores, antenas, etc.) o problemas del medio. En este caso, puede darse una de las técnicas de DT conocida como throttling, que es la ralentización o entorpecimiento hacia una determinada aplicación, servicio o tipo de tráfico (Molina, 2011).

Otro aspecto a considerar es el tipo de conexión. Los ISP’s fijos proporcionan una red de tipo fijo, que utiliza una conexión de transmisión como cable de cobre o fibra óptica, proporcionando una estabilidad robusta y altas velocidades, además de datos teóricamente ilimitados. Sin embargo, están limitados a una ubicación especifica, por lo que no pueden ser portátiles o moverse hacia otra ubicación fácilmente (Hallahan, 2022).

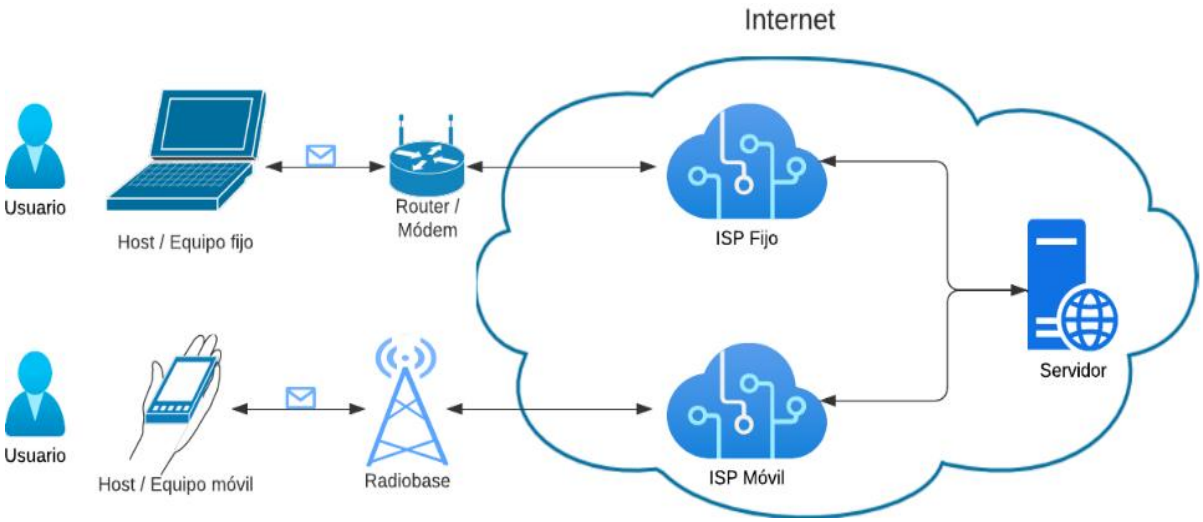
Por otro lado, los ISP’s móviles proporcionan una red de tipo móvil, que utiliza múltiples y diversas tecnologías inalámbricas como WiFi, 4G, 5G, etc., posibilitando la movilidad y portabilidad siempre y cuando exista cobertura de la red, pero tanto su

velocidad como estabilidad son variables (Hallahan, 2022), además de que generalmente el ISP establece límites en la cantidad de datos a utilizar junto con un costo predeterminado.

El diagrama de red de las herramientas de inyección y monitoreo de tráfico se muestra en la figura 2, considerando ISP's de conexión fija y móvil.

Figura 2

Diagrama general de la red

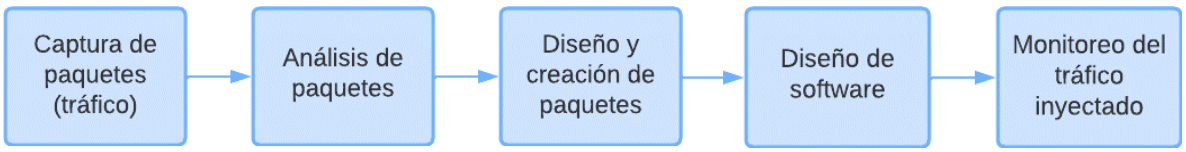


Los datos parten desde un equipo terminal de usuario (host) hacia un servidor en específico alojado en Internet, a través de la red del ISP, la cual está compuesta de diferentes equipos (antenas, enrutadores, conmutadores, etc.).

El diagrama general de diseño de software que se siguió se muestra en la figura 3.

Figura 3

Diagrama general del diseño



Este inicia con la captura de los paquetes o tráfico de las aplicaciones elegidas anteriormente para su análisis. Una vez extraída y obtenida la información relevante, se procede con el diseño de los paquetes de manera que simule y replique, en medida de lo posible, los paquetes y tráficos originales. Con el tráfico sintético recreado, se procede al

diseño de la herramienta y, finalmente, se analizará y validará el mismo haciendo uso de herramientas de análisis.

Requerimientos de diseño

En base a los aspectos detallados al inicio de este capítulo y considerando el estándar IEEE 830-1998 "*Recommended Practice for Software Requirements Specifications*" (IEEE, 1998), que establece la definición de requisitos de software, se plantea como requerimientos funcionales para el desarrollo de la aplicación de inyección y monitoreo de tráfico:

- Capacidad de creación de paquetes de tipo TCP y UDP: TCP ya que una de las técnicas de DT es la censura o bloqueo y ambas se pueden lograr mediante el reseteo o terminación de una conexión TCP con paquetes RST, y UDP ya que las aplicaciones que utilizan este protocolo se pueden considerar como menos criticas o importantes por lo tanto podría recibir un trato diferente frente a otros protocolos como TCP (Castoreo, Maillé, & Tuffin, 2020).
- Capacidad de replicar tráfico de servicios o aplicaciones elegidos: Netflix como streaming de video, YouTube como servicio de video y Google Meet como servicio de videoconferencia.
- Capacidad de inyección de tráfico y medición activa: ya que permite medir exactamente lo que se necesita, incluso cuando se puedan presentar varios desafíos en comparación con las mediciones pasivas que ofrecen capacidades limitadas e ineficientes en cuanto a la observación y análisis del estado de la red (Castoreo, Maillé, & Tuffin, 2020).
- Capacidad de monitorear latencia y pérdida de paquetes: La latencia es un indicador importante de la velocidad y eficiencia de una red, afecta la experiencia de usuario en aplicaciones de tiempo real y es uno de los atributos a los que son sensibles varios tipos de servicios. Mientras que la pérdida de paquetes puede ocasionar problemas como retrasos y aumento de latencia (Molina, 2011).

- Capacidad de uso en dispositivos fijos (computadoras) y móviles (teléfonos inteligentes): ya que se pretende monitorear tanto ISP’s fijos como móviles.

Construcción de paquetes

Captura de paquetes y tráfico real

Para la generación del tráfico que simule un tipo de servicio o aplicación, primero es necesario la captura y análisis de tráfico real a replicar (Netflix, YouTube y Google Meet). Para esto se hizo uso de sniffers y herramientas de análisis de paquetes y tráfico de red detalladas a continuación:

- Wireshark: Es un sniffer, ayuda en el análisis de paquetes, es gratuito y de código abierto, presenta ventajas al momento de analizar el tráfico como: interfaz personalizable, capacidad de monitoreo en tiempo real, compatibilidad con diferentes sistemas operativos, amplia gama de protocolos y capacidad de filtrado de paquetes, convirtiéndose en una herramienta muy útil. Además, se puede descomponer los paquetes capturados y mostrar información detallada sobre los encabezados de cada capa y los datos contenidos en ellos (Adams, 2013).
- ntopng: es una herramienta de análisis/monitoreo de tráfico de red, de código abierto, que se utiliza para visualizar y analizar el tráfico de red en tiempo real. Sin embargo, ntopng tiene algunas características adicionales que lo diferencian de Wireshark, como su interfaz más dinámica, una serie de herramientas avanzadas para la clasificación de tráfico basada en criterios de direcciones IP, puertos, throughput, análisis de información (capa de aplicación) haciendo uso de tecnología ntop DPI y la detección de amenazas de seguridad (ntop, 2023).

Con la ayuda de estas herramientas se realizó 10 capturas por aplicación, un total de 30, con el objetivo de identificar información interna de los paquetes de dichos servicios.

A continuación, se muestra un ejemplo de Netflix en la figura 4 y de Google Meet en la figura 5 y, posteriormente, el análisis respectivo haciendo énfasis en los parámetros distintivos del tráfico y paquetes:

Figura 4

Captura de paquetes con Wireshark – tráfico de Netflix

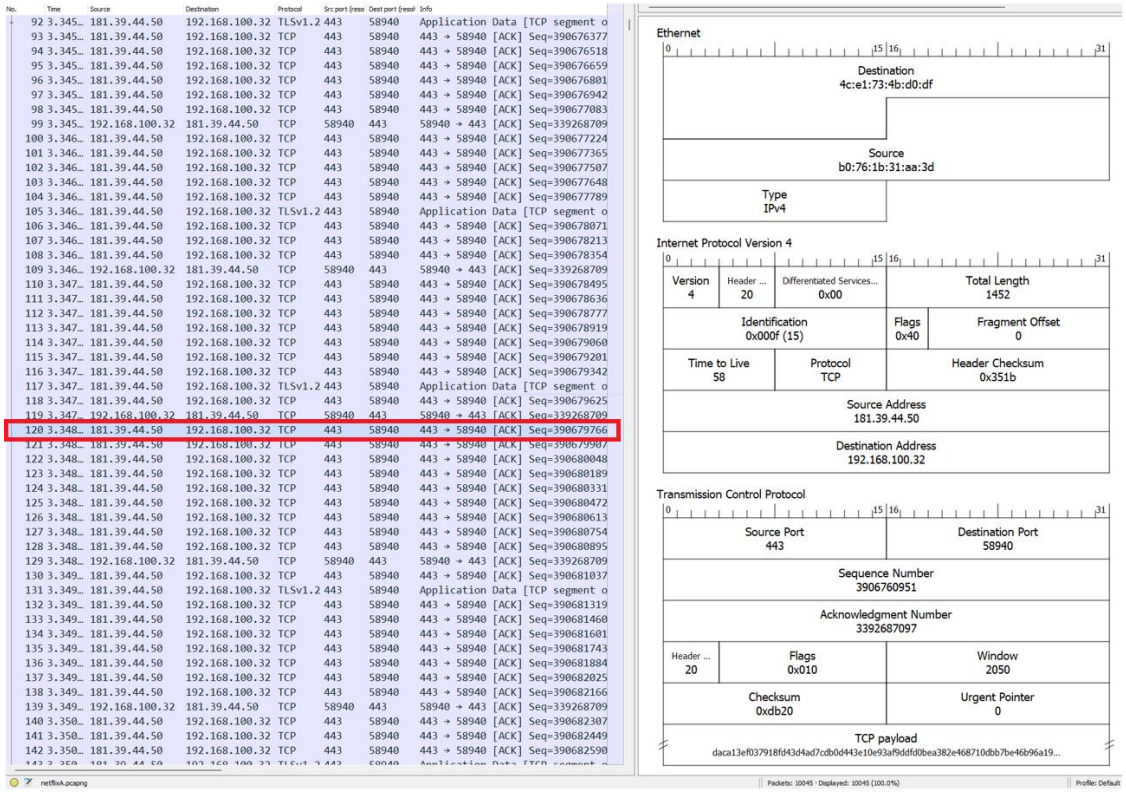
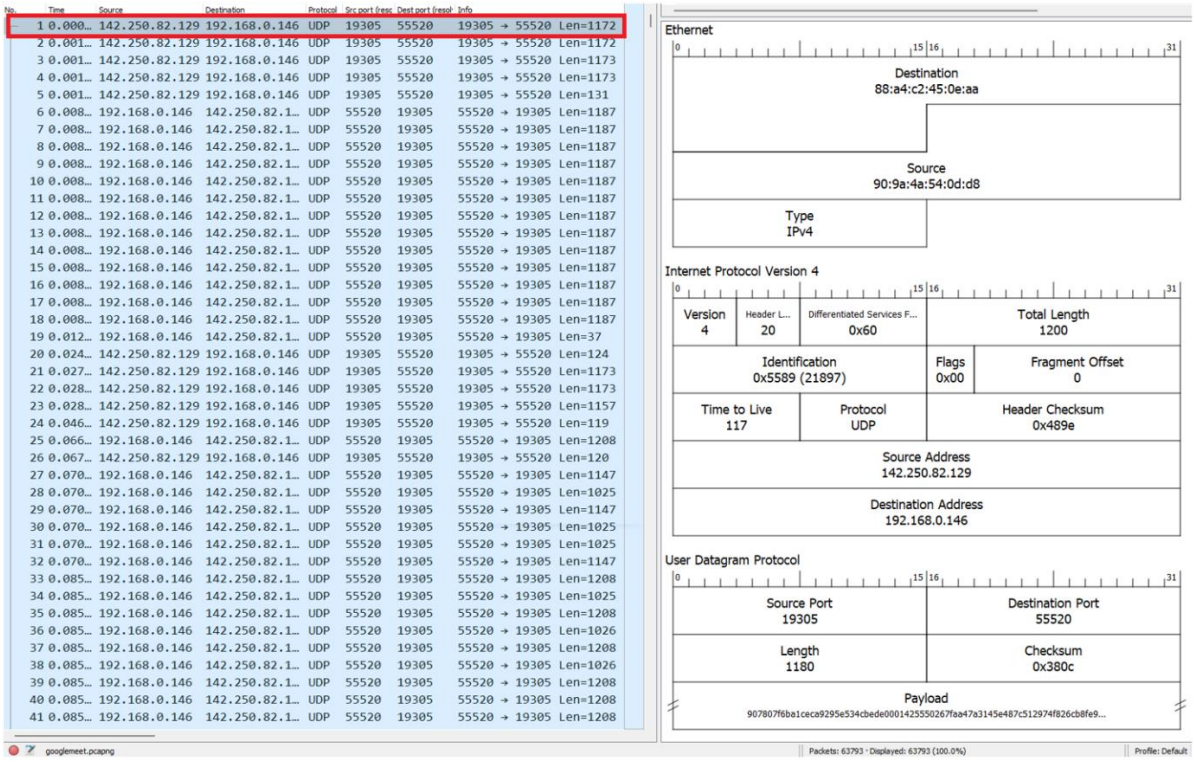


Figura 5

Captura de paquetes con Wireshark - tráfico de Google Meet



Tal como se vio en el capítulo anterior, se presentó el modelo TCP/IP, mismo que está conformado por 4 capas y son: aplicación, transporte, Internet y enlace, cada una con sus funciones correspondientes. Es necesario considerar este modelo, pues cada uno maneja cabeceras con valores específicos y se usaron para el análisis de los paquetes y tráfico real.

Se detallan estas capas y sus cabeceras más relevantes en la tabla 3 a continuación (IBM, 2023):

Tabla 3

Capas y cabeceras de un paquete

Capa	Cabecera	Descripción
Enlace / Ethernet	MAC Destino	Identificador único del dispositivo que recibe
	MAC Fuente	Identificador único del dispositivo que envía
	Tipo	IPv4 o IPv6
Internet	Versión	IPv4 o IPv6
	DSCP	Tipo de tratamiento de tráfico solicitado
	Protocolo	TCP o UDP
	IP Fuente	Dispositivo que envía
	IP Destino	Dispositivo que recibe
Transporte	Puerto fuente	Puerto en uso por la aplicación que envía
	Puerto destino	Puerto en uso por la aplicación que recibe
Aplicación	Payload	Carga útil / Información/ Data

Las cabeceras más relevantes para este trabajo de investigación son: ‘tipo’ (capa enlace), ‘versión’, ‘DSCP’ y ‘protocolo’ (capa Internet), puertos fuente y destino (capa transporte) y payload (capa aplicación).

Las cabeceras ‘tipo’ y ‘versión’ indican la versión del protocolo de Internet en uso y, como se mencionó anteriormente, se enfocará este estudio a IPv4.

La cabecera ‘protocolo’ indica si la capa Internet maneja protocolo TCP o UDP, el primero maneja envío con acuse de recibo (asegurando que los paquetes lleguen a su destino mediante retransmisiones en el caso de pérdida) y el segundo orientado a la velocidad incluso si se pierden varios paquetes en el envío.

Una cabecera importante para este trabajo de investigación es la de ‘DSCP’ (Differentiated Services Code Point por sus siglas en inglés), el cual puede ser considerado una solicitud del paquete para un tratamiento prioritario.

Esta cabecera es un mecanismo utilizado para clasificar tráfico en las redes, al encontrarse en la capa 3, permite mantener la misma solicitud de prioridad a lo largo de su trayecto hasta llegar a su destino (Nvidia, 2020), los valores más importantes que puede tomar se detallan en la tabla a continuación:

Tabla 4

Cabecera DSCP - descripción y valores

Nombre	Precedencia IP	Uso / Descripción	Hexadecimal
CS7	7	Control de Red	0xe0
CS6	6	Control de Internet	0xc0
EF	**5**	**Crítico**	**0xb8**
CS5	5	Crítico	0xa0
CS4	4	Flash Override	0x80
CS3	3	Flash	0x60
CS2	2	Inmediato	0x40
CS1	1	Prioridad	0x20
BE	**0**	**Normal**	**0x00**

El payload, carga útil o data, es la información misma que busca enviar una aplicación desde un punto en la red hacia otro. Esta puede llamarse ‘carga tcp’ o ‘tcp payload’ en el caso de utilizar TCP como protocolo de transporte o simplemente ‘carga’, ‘payload’ o ‘data’ en el caso de UDP.

Otros valores como ‘longitud de cabecera’, ‘longitud total’ (capa IP), ‘checksum’ (capas IP y transporte), ‘secuencia’ y ‘acknowledgment’ (capa transporte) entre otros, son cabeceras que manejan valores variables en todo momento y que su relevancia no es considerable para casos de análisis de paquetes y herramientas de monitoreo de DT (Li & al, 2019).

Análisis de paquetes y tráfico real

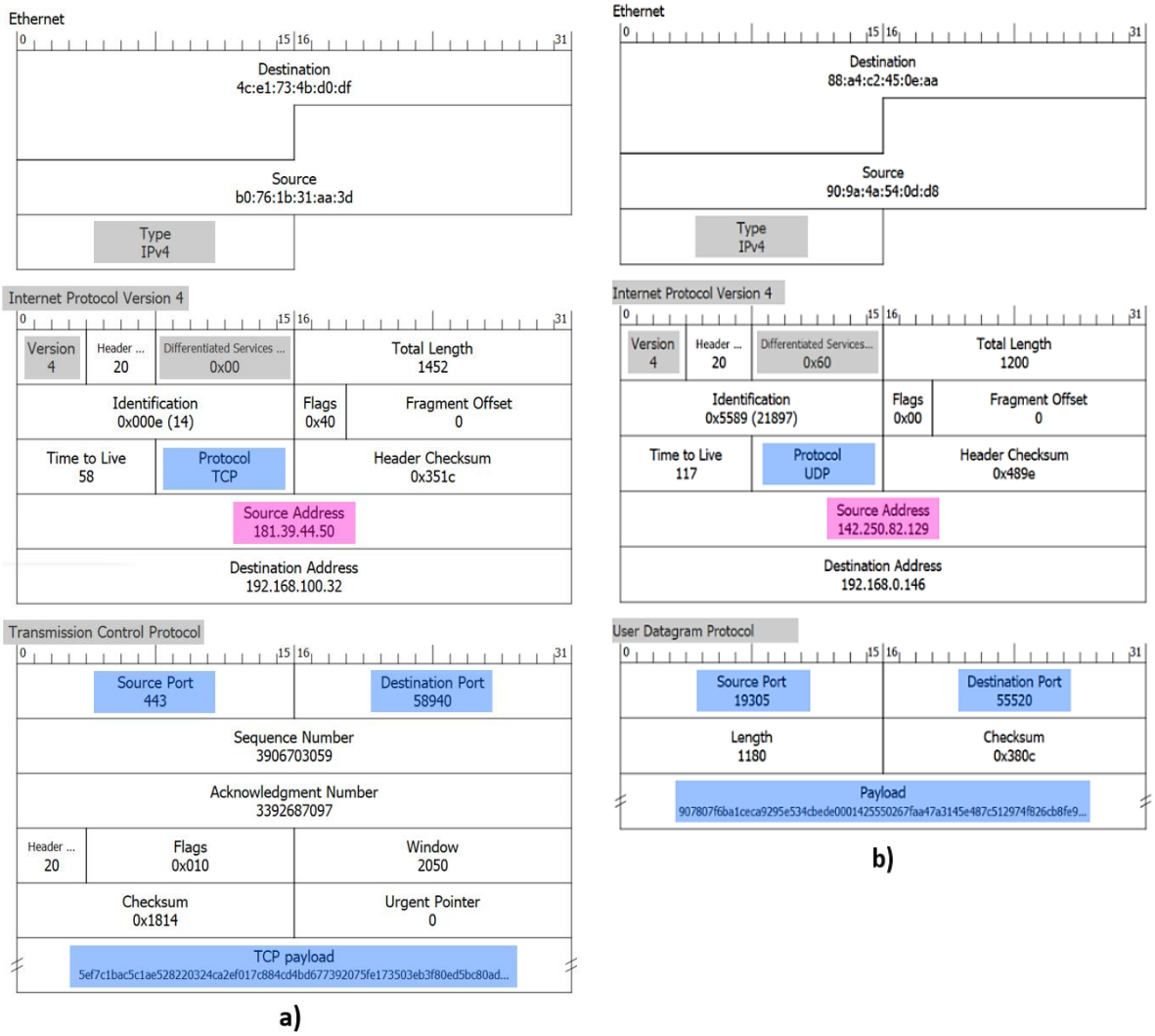
Para el análisis de los paquetes capturados se consideró los 4 puntos principales para identificar el tipo de servicio de un tráfico, mismos que se encuentran en todo paquete de datos (sea este TCP o UDP) y que son: puertos origen y destino, direcciones origen y destino (IP y MAC), protocolos y payload (carga útil / capa de aplicación) (Molina, 2011).

Para el análisis de los paquetes capturados se consideró los 4 puntos principales para identificar el tipo de servicio de un tráfico, mismos que se encuentran en todo paquete de datos (sea este TCP o UDP) y que son: puertos origen y destino, direcciones origen y destino (IP y MAC), protocolos y payload (carga útil / capa de aplicación) (Molina, 2011).

Cabe recalcar que no es posible replicar las direcciones fuente IP o MAC de los servicios que se usaron para el análisis, por lo que se descartó este parámetro.

Figura 6

Diagrama de paquetes - capas enlace, Internet, transporte, aplicación a) Netflix y b) Google Meet



A continuación, en la figura 6, se muestran 2 ejemplos de servicios capturados, Netflix y Google Meet respectivamente. Se resaltan las cabeceras revisadas anteriormente, en color rosa la dirección IP de origen (no replicable), en color gris las poco relevantes (pero igual consideradas) y en color azul las principales para identificar el tipo de servicio y en las que se basó para el diseño de los paquetes que fueron replicados.

Por lo tanto, se procedió con el análisis de las distintas capturas, con lo que se obtuvo la siguiente tabla resumen de las 30 capturas realizadas de todos los servicios:

Tabla 5

Parámetros considerados y analizados para la replicación de paquetes de acuerdo al servicio

	Puerto origen	Puerto destino	Protocolo	Payload
Netflix	443	49152-65535	TCP	Encriptación TLS y HTTPS, tamaño 1412 bytes.
YouTube	443	49152-65535	TCP	Encriptación TLS y HTTPS, tamaño 1412 bytes.
Google Meet	19294-19305	49152-65535	UDP	Encriptación HTTPS, tamaño 1200 bytes

Diseño y creación de paquetes sintéticos

Considerando los parámetros extraídos de la captura de los paquetes de los diferentes servicios expuestos en la tabla 5, para el diseño de paquetes los parámetros que se escogieron son:

- Puertos: se utilizaron los puertos en el rango de 61200-61300, dentro del rango de puertos utilizados por las aplicaciones analizadas.
- Protocolos: TCP en el caso de Netflix y YouTube, UDP en el caso de Google Meet.
- Payload: se ha extraído y utilizado el payload sin alteraciones correspondientes a cada uno de los servicios, para poder crear paquetes idénticos a los capturados.

Adicional a estos valores, se hace uso también del campo DSCP o ‘Differentiated Services Code Point’ en la cabecera IP con dos valores distintos para su tratamiento y reenvío, el primero servicio BE o best effort (hexadecimal 0x00), indicando prioridad normal, y el segundo EF o expedited forwarding (hexadecimal 0xb8), indicando alta prioridad.

Al realizar la inyección de tráfico replicado y para una mejor comparación o contraste entre las aplicaciones elegidas, es necesario considerar la idea de un tráfico neutral (suponiendo que este no es diferenciado), por lo que un cuarto tipo de tráfico será

generado, este con bits aleatorios o una serie de caracteres para su posterior reconstrucción y verificación de la integridad en la comunicación. Se lo denominó tráfico aleatorio o referencia y se observa sus parámetros en la tabla 6 a continuación:

Tabla 6

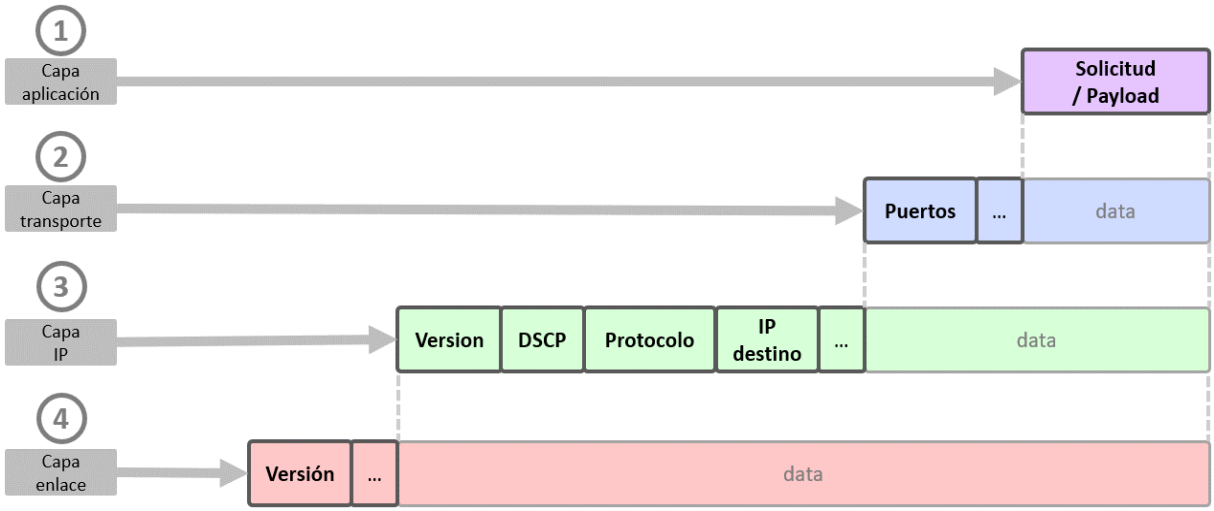
Parámetros considerados para el tráfico aleatorio / referencia

	Puerto origen	Puerto destino	Protocolo	Payload
Aleatorio / Referencia	443	61200-61300	TCP	Codificación ASCII, tamaño 1400 bytes

Los 4 tipos de paquetes (tráfico Netflix, YouTube, Meet y Aleatorio) se crean mediante un proceso denominado encapsulamiento que agrega la información correspondiente capa a capa hasta tener un paquete completo (la información junto con la cabecera de una capa, se vuelve información en la capa inferior (Molina, 2011)). Los 4 tipos de paquetes (Netflix, YouTube, Meet y Aleatorio) se crean mediante un proceso llamado encapsulamiento que agrega la información correspondiente capa a capa hasta tener un paquete completo (la información junto con la cabecera de una capa, se vuelve información en la capa inferior (Molina, 2011)). Este proceso (y los principales parámetros para esta investigación) se observan en la figura 7 a continuación:

Figura 7

Creación de paquetes por capas – 1) aplicación, 2) transporte, 3) IP y 4) enlace

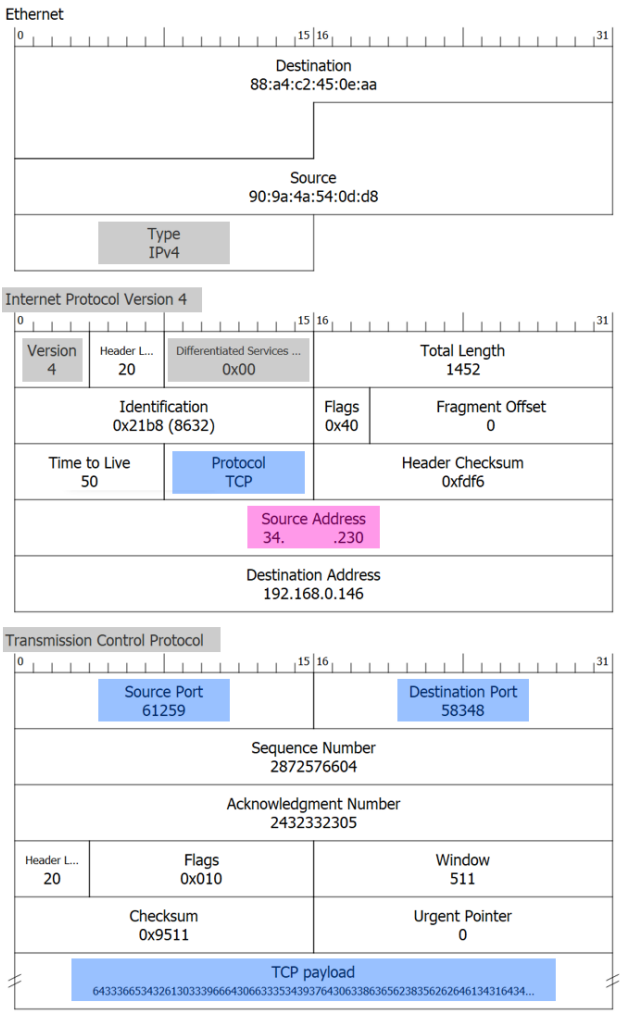


1. Capa aplicación: en el campo de ‘TCP Payload’ se tiene el payload extraído anteriormente de tráfico original que está enviando el servidor al host. Debe tomarse en cuenta la codificación y/o decodificación de la información.
2. Capa transporte: se observa principalmente el puerto fuente, es decir el puerto en el servidor correspondiente al ISP y servicio: 61259, puerto que está enviando la respuesta a la solicitud.
3. Capa IP: se ingresa la versión a utilizar (IPv4), DSCP BE (en hexadecimal 0x00), Protocolo (TCP)y finalmente IP del host (192.168.0.146).
4. Capa enlace: se especifica la versión a utilizar (IPv4).

En la figura 8 se detalla un ejemplo de paquete capturado del tráfico Netflix sintético:

Figura 8

Captura tráfico Netflix sintético



Se puede observar los parámetros considerados en la tabla 4 (color azul) para este tipo de tráfico (resaltado en color rosado la dirección IP del servidor, suprimida una parte por motivos de seguridad).

Adicionalmente se muestra en la figura 9, el payload del tráfico aleatorio, que es un tipo de ‘arte ASCII’ que forma la imagen de un dibujo o marioneta, compuesto de caracteres de todo tipo (números, letras minúsculas y mayúsculas, símbolos y especialmente espacios), de manera que no se observe manipulación o supresión de los mismos y verificar, como ya se mencionó la integridad en la comunicación.

Figura 9

Tráfico Aleatorio / Referencia - Payload

Diseño de aplicación de inyección de tráfico y monitoreo

Descripción

Al tener dos escenarios (fijo y móvil), las aplicaciones se desarrollaron siguiendo el mismo principio y funcionamiento (inyección de tráfico y monitoreo), una para equipos de escritorio como computadores y laptops y la otra para equipos o dispositivos móviles como teléfonos inteligentes o tablets, al tratarse de la misma herramienta pero en plataformas distintas, se pretende que ambas posean la misma interfaz de usuario, pese a su desarrollo en distintas IDEs (ambiente de desarrollo integrado o Integrated Development Environment por sus siglas en inglés).

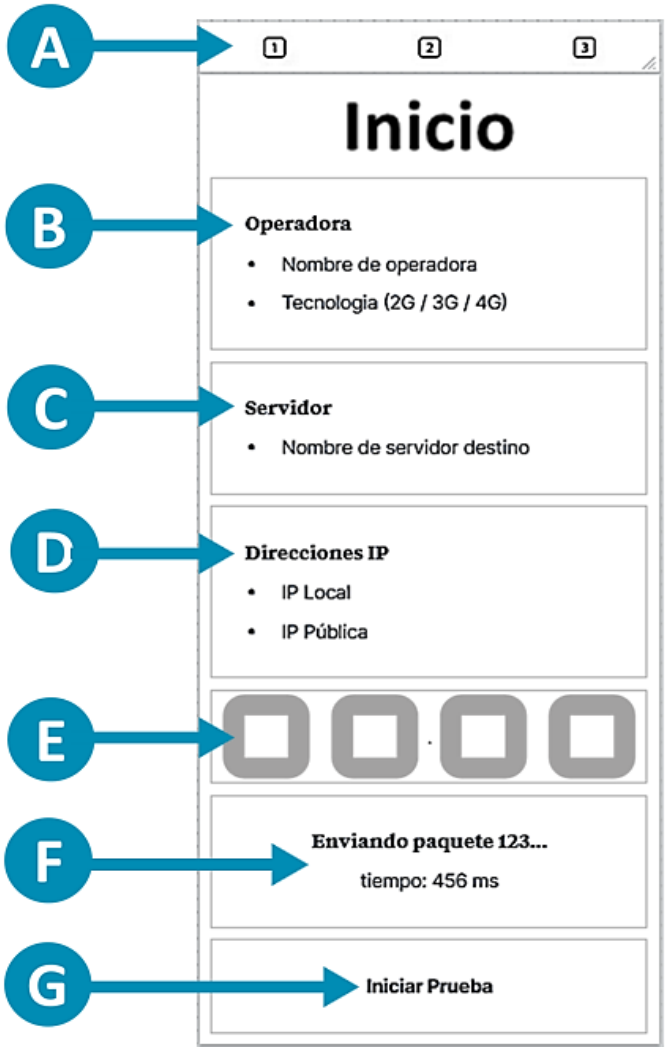
Interfaz

La interfaz de usuario se creó de manera que se pueda iniciar y empezar la prueba completa, también tener el control de las pruebas de inyección de tráfico y finalmente la visualización de los resultados obtenidos de la prueba junto con su identificador o nombre y envío de los resultados para su registro en servidor y visualización en la página web:

- Pestaña 1 – Inicio: En esta pestaña (figura 10) se tiene: a) sección de pestañas, b) operadora y tecnología, c) nombre de servidor, d) direcciones IP (local y pública), e) íconos de servicios replicados, f) estado de prueba (servicio en curso y latencia de paquete actual) y g) botón de inicio de prueba.

Figura 10

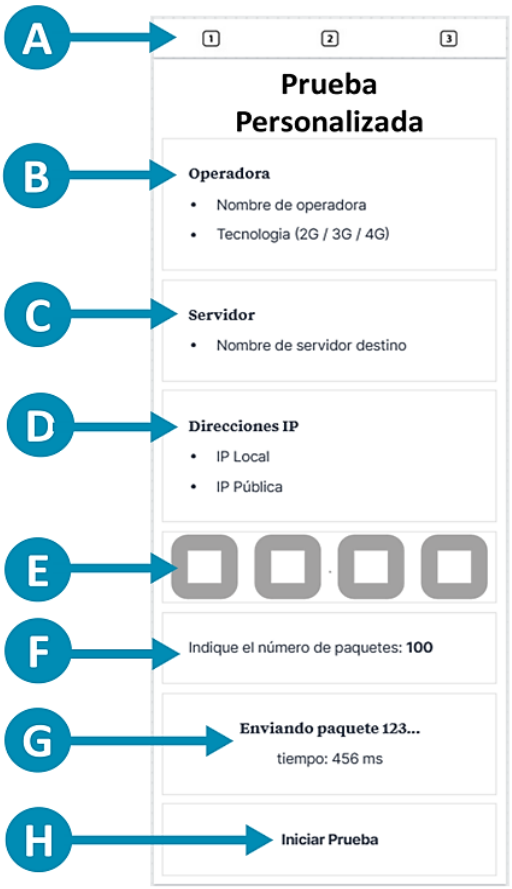
Diseño de la interfaz de la aplicación de escritorio (pestaña 1)



- Pestaña 2 – Prueba personalizada: (figura 11) similar a la pestaña anterior (puntos a, b, c, d, g y h) y adicionalmente: e) se puede elegir (activar/desactivar) los servicios y f) digitar el número de paquetes a inyectar por servicio.

Figura 11

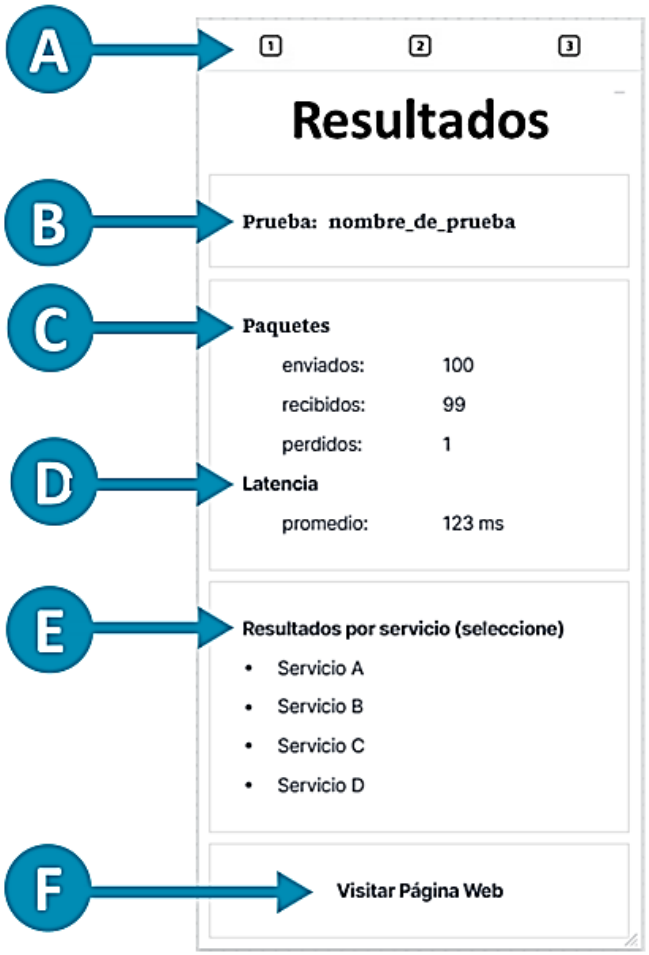
Diseño de la interfaz de la aplicación de escritorio (pestaña 2)



- Pestaña 3 – Resultados: Esta pestaña (figura 12) se encuentra dividida por bloques de la siguiente manera: a) sección de pestañas, b) nombre de prueba (fecha, hora, ISP y, en el caso de móviles, tecnología (WiFi, HSPA+, LTE, etc.)), c) resultado total de los paquetes enviados, recibidos y perdidos, d) latencia promedio general de la prueba concluida, e) resultados individuales por servicio/aplicación (paquetes enviados, recibidos, perdidos y latencia promedio) y f) botón de redirección a página web de los resultados obtenidos en el estudio.

Figura 12

Diseño de la interfaz de la aplicación de escritorio (pestaña 3)



Storyboard

En el storyboard de la figura 13 y 14, ambas aplicaciones reciben al usuario en la pantalla de inicio (1), desde aquí el usuario puede iniciar la prueba, ir a la página de resultados (2) y posteriormente visitar la página web (3). De manera opcional se puede navegar desde inicio (1) hacia la pestaña de prueba personalizada (1.2) para activar o desactivar servicios a monitorear y digitar el número de paquetes a inyectar por servicio.

Al manejar una interfaz de pestañas, se puede interactuar entre ellas libremente (inicio hacia resultados, inicio hacia prueba personalizada, etc.).

Figura 13

Storyboard – Aplicación de escritorio

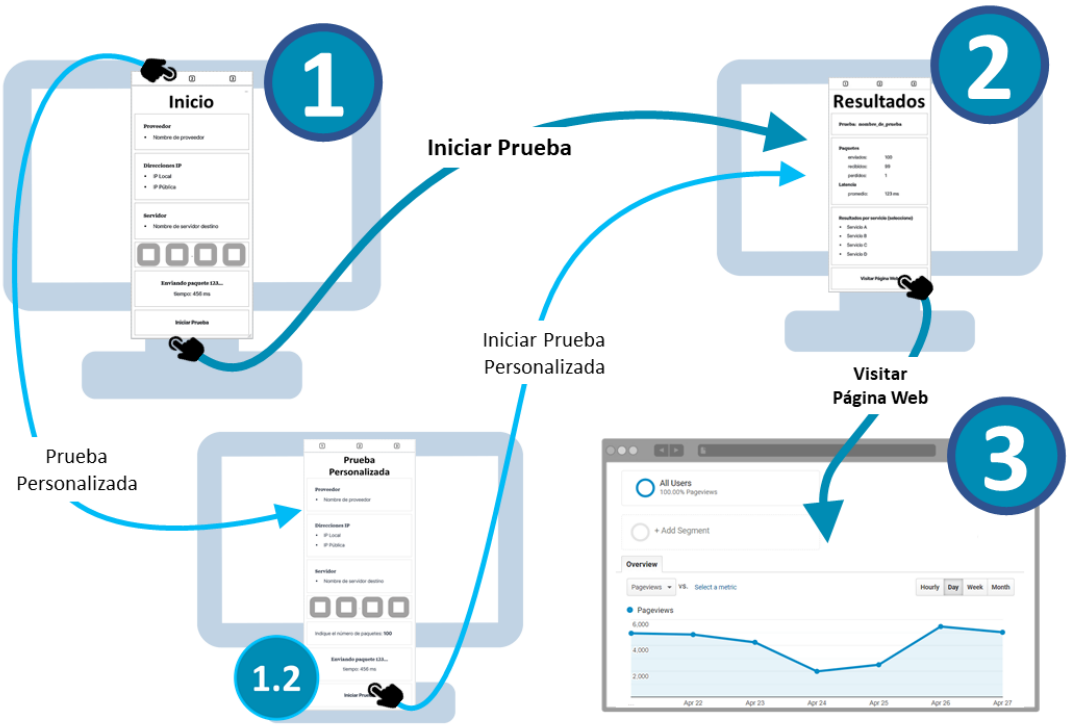


Figura 14

Storyboard – Aplicación móvil

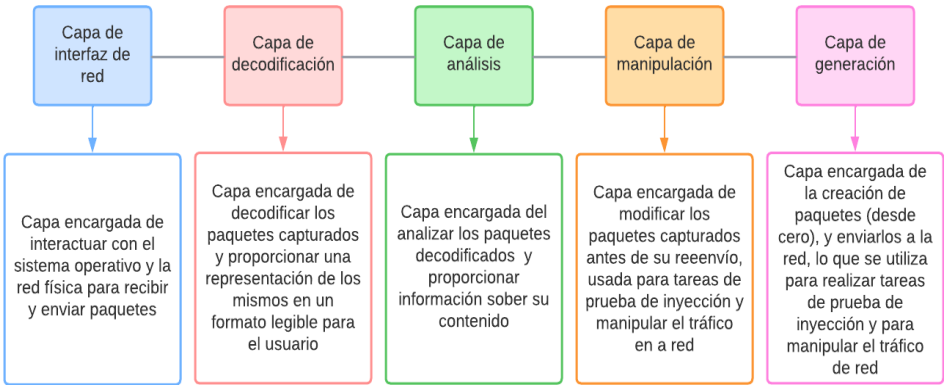
Programación y desarrollo

Aplicación de escritorio: Esta aplicación se desarrolló en Python v3.9, lenguaje sumamente versátil y de propósito general, además de su gran escalabilidad y gran variedad de librerías y frameworks. Como IDE se utilizó Pycharm de JetBrains, ambiente de desarrollo de gran ayuda gracias a su interfaz de usuario adaptable y personalizable, gran depurador, control de versiones, compatibilidad y demás.

La librería Scapy, de código abierto y uso libre, permite la fácil extracción y manipulación del payload y cabeceras específicas de las capturas realizadas a través de Wireshark, esto para la creación de los paquetes a inyectar (Gómez, 2020). El funcionamiento de Scapy posee diversas capas de funcionamiento, cada una con una función específica y se detallas en la figura 15.

Figura 15

Diagrama de bloques por capas del funcionamiento de Scapy

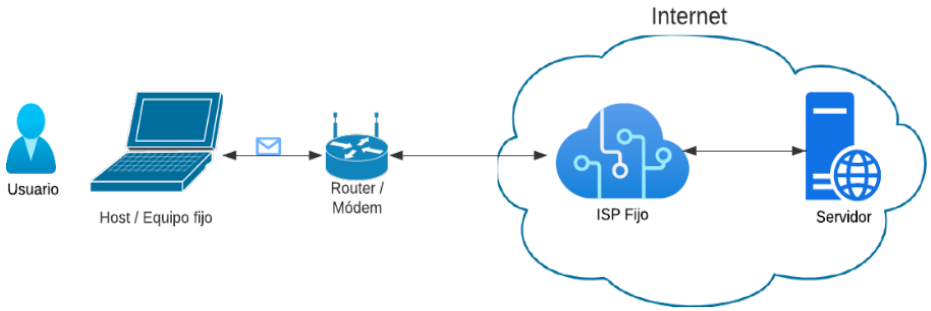


La función '*rdpcap('captura.pcapng')*' fue utilizada para leer las capturas resumidas en la tabla 5, archivos de tipo pcapng (captura de Wireshark) para la modificación de cabeceras en las capas de enlace (direcciones MAC), de transporte (direcciones IP) y nuevos valores en cabeceras como 'chksum', 'length' y otros que varían acorde a los bits en el paquete y que no son relevantes para su contenido pero si para la integridad del paquete en cuestión, de manera que se pueda comparar entre tráfico generado y tráfico original. Los resultados de este paso se analizan más adelante en el capítulo de resultados.

Es importante considerar el escenario en el que se va a trabajar (figura 2), por lo que se presenta la figura 16, como topología de una red de conexión fija y uso de la aplicación en un ordenador (de escritorio o portátil):

Figura 16

Escenario herramienta de fija (escritorio)



Aplicación móvil: Esta aplicación se desarrolló en Java 19, lenguaje orientado a objetos, capacidad de hilos y con gran repertorio de librerías y herramientas útiles, Java SDK 33. Como IDE se utilizó Android Studio Electric Eel 2022.1.1 y Runtime v11.

Las librerías utilizadas fueron Java.Net, Java.IO y Java.Util, ya que prestan las capacidades necesarias para iniciar la comunicación y manipular el campo DSCP (java.net.Socket - setTrafficClass), para especificar prioridades BE y EF.

Es importante considerar nuevamente el escenario en el que se va a trabajar, por lo que se presenta la topología de una red de conexión móvil y uso en teléfonos inteligentes en la figura 17:

Figura 17

Escenario herramienta móvil

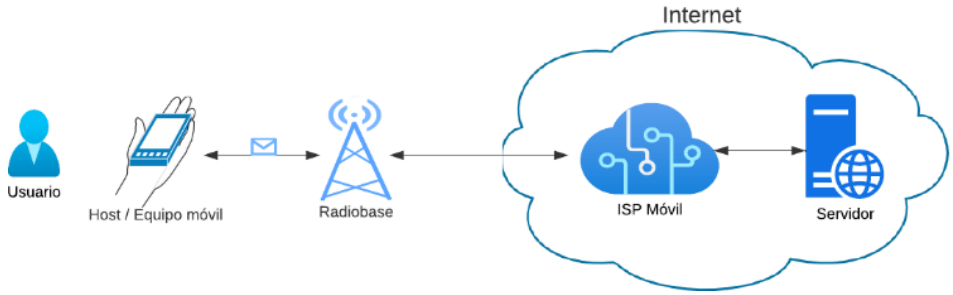


Diagrama de flujo

Aplicación de escritorio: Al iniciar la aplicación de escritorio, se cargan las librerías Scapy (lectura, creación, manipulación y envío de paquetes), socket (interacción con la interfaz de red), json (lectura de archivos tipo json), requests (interacción con API web), PIL (imágenes e iconos) y customtkinter (interfaz gráfica) y se crea la interfaz. Luego se carga la información principal como es la dirección IP del servidor junto con los puertos para cada servicio y operador, donde cada operador dispone de un rango de puertos y cada servicio un puerto respectivo.

Una vez cargada la información, se selecciona el tipo de tráfico a inyectar y se inicia el proceso de inyección de tráfico, este revisa que servicios han sido activados o seleccionados (en el caso de prueba personalizada), carga la información para cada servicio y llama al subproceso ‘envío/recepción’.

El subproceso ‘envío/recepción’ consiste en el envío de 150 paquetes de solicitud con DSCP BE y 100 paquetes con DSCP EF. Las respuestas con sus payloads y sus respectivos tiempos se almacenan en variables.

Terminado el subproceso de ‘envío/recepción’ del primer servicio, se procede a elegir el siguiente con su respectivo tipo de tráfico y se repite el subproceso y el almacenamiento de respuestas y tiempos para los servicios siguientes.

Terminado el proceso de inyección de tráfico, se calculan promedios de tiempos por servicios y DSCP, latencia y pérdida de paquetes para su presentación en la pestaña de resultados.

Una vez en la pestaña de resultados, se puede visualizar los valores generales, por servicio y la redirección hacia la página web haciendo uso del botón.

En la figura 18 se puede observar el diagrama de flujo de la herramienta de escritorio y en la figura 19 el proceso de inyección de tráfico y subproceso de ‘envío/ recepción’:

Figura 18

Diagrama de flujo - aplicación de escritorio

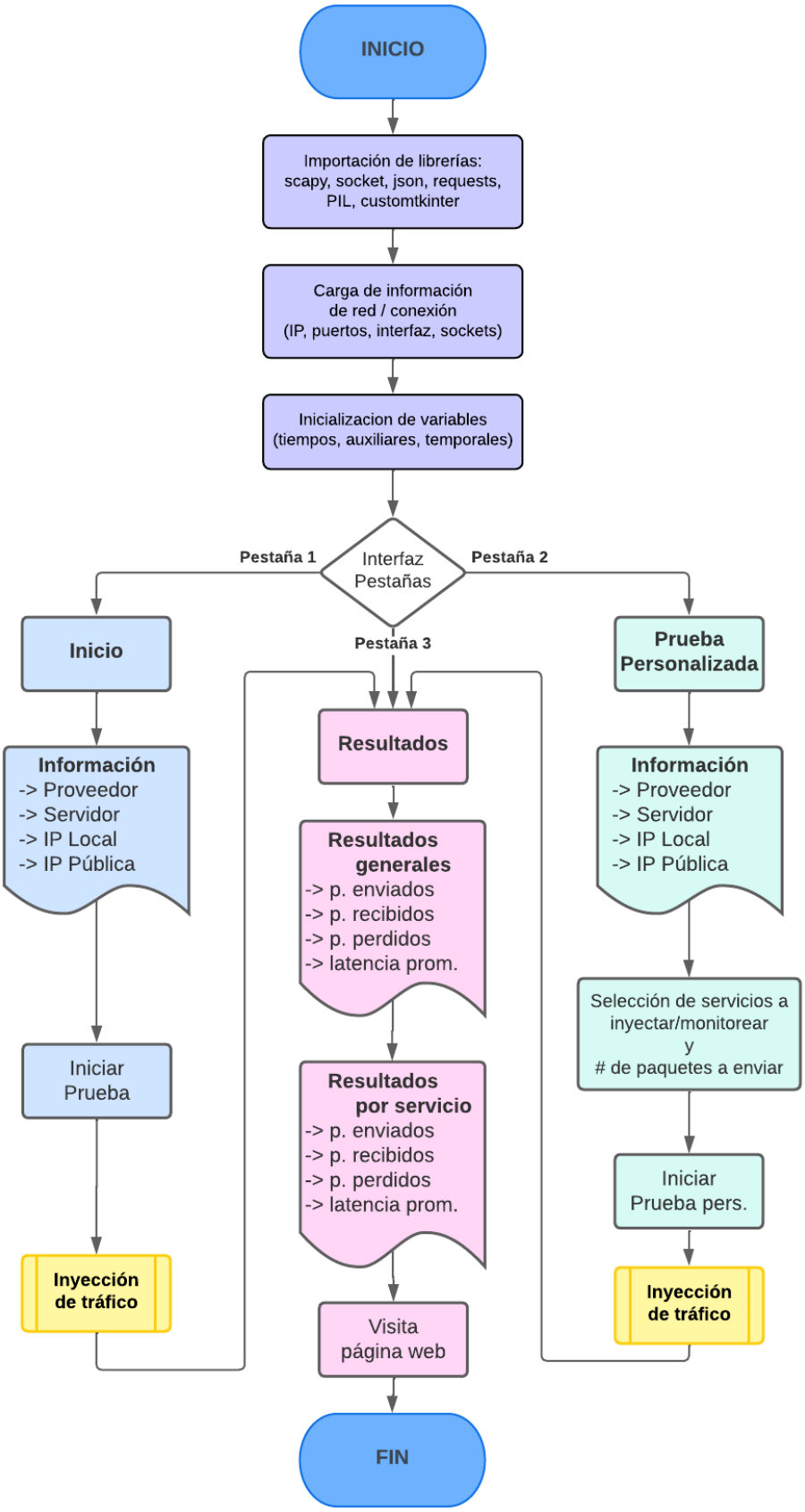
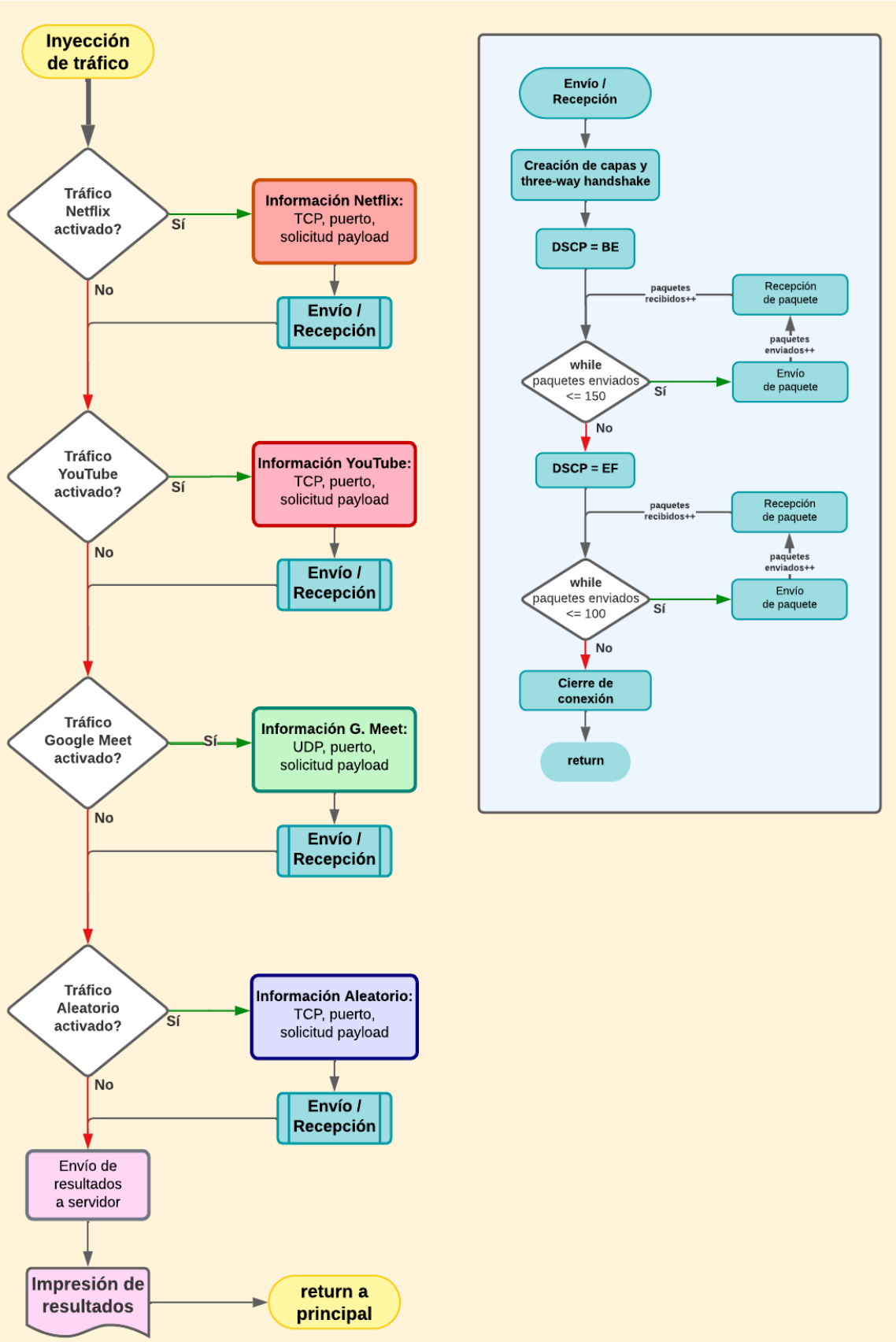


Figura 19

Diagrama de flujo – Aplicación de escritorio – subprocesos



Aplicación móvil: El proceso de la aplicación móvil es similar al de la aplicación fija, pero obteniendo información adicional de la red móvil como es el nombre de operadora y tecnología (3G – HSPA, HSPA+, UMTS o 4G – LTE). Se cargan los paquetes originales con sus respectivos payloads, se carga la información principal como es la dirección IP del servidor junto con los puertos para cada servicio y operador. Cada operador tiene un rango de puertos y cada servicio un puerto respectivo.

Una vez cargada la información, se selecciona el tipo de tráfico a inyectar y se inicia el proceso de inyección de tráfico, este revisa que servicios han sido activados o seleccionados (en el caso de prueba personalizada), carga la información para cada servicio y llama al subproceso 'envío/recepción'.

El subproceso 'envío/recepción' consiste en la creación de socket con puerto respectivo, envío de 150 paquetes de solicitud con DSCP BE y 100 paquetes con DSCP EF y cierre de socket. Las respuestas y tiempos se almacenan en variables.

Terminado el subproceso de 'envío/recepción' del primer servicio, se procede a elegir el siguiente con su respectivo tipo de tráfico y se repite el subproceso y el almacenamiento de respuestas y tiempos para los servicios siguientes.

Terminado el proceso de inyección de tráfico, se calculan promedios de tiempos por servicios y DSCP, latencia y perdida de paquetes para su presentación en la pestaña de resultados. Adicional al proceso de la herramienta fija, se envía al servidor la información de operadora y tecnología.

Una vez en la pestaña de resultados, se puede visualizar los valores generales, por servicio y la redirección hacia la página web haciendo uso del botón.

En la figura 20 se puede observar el diagrama de flujo de la herramienta móvil y en la figura 21 el proceso de inyección de tráfico y subproceso de 'envío/ recepción':

Figura 20

Diagrama de flujo - aplicación móvil

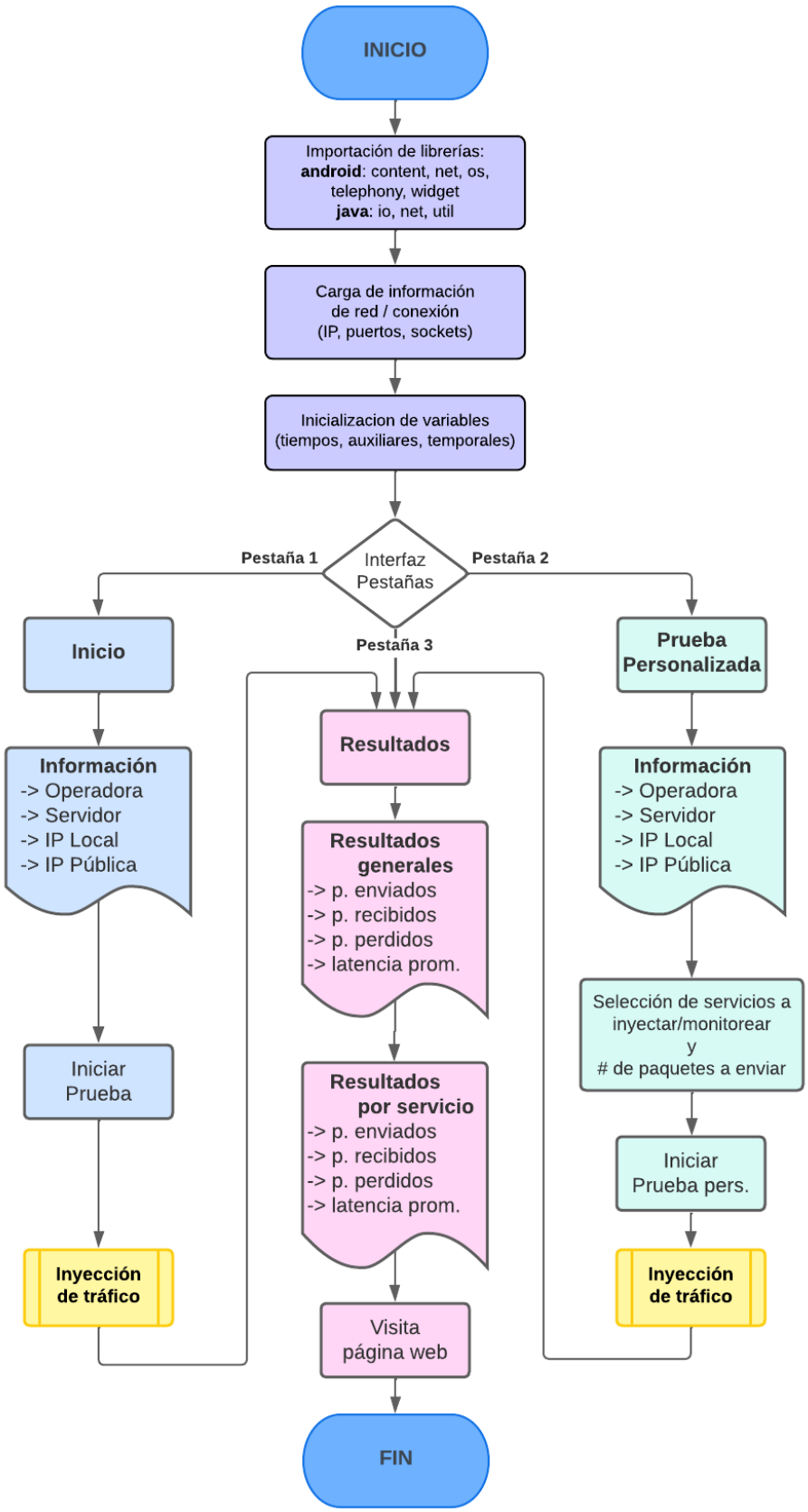
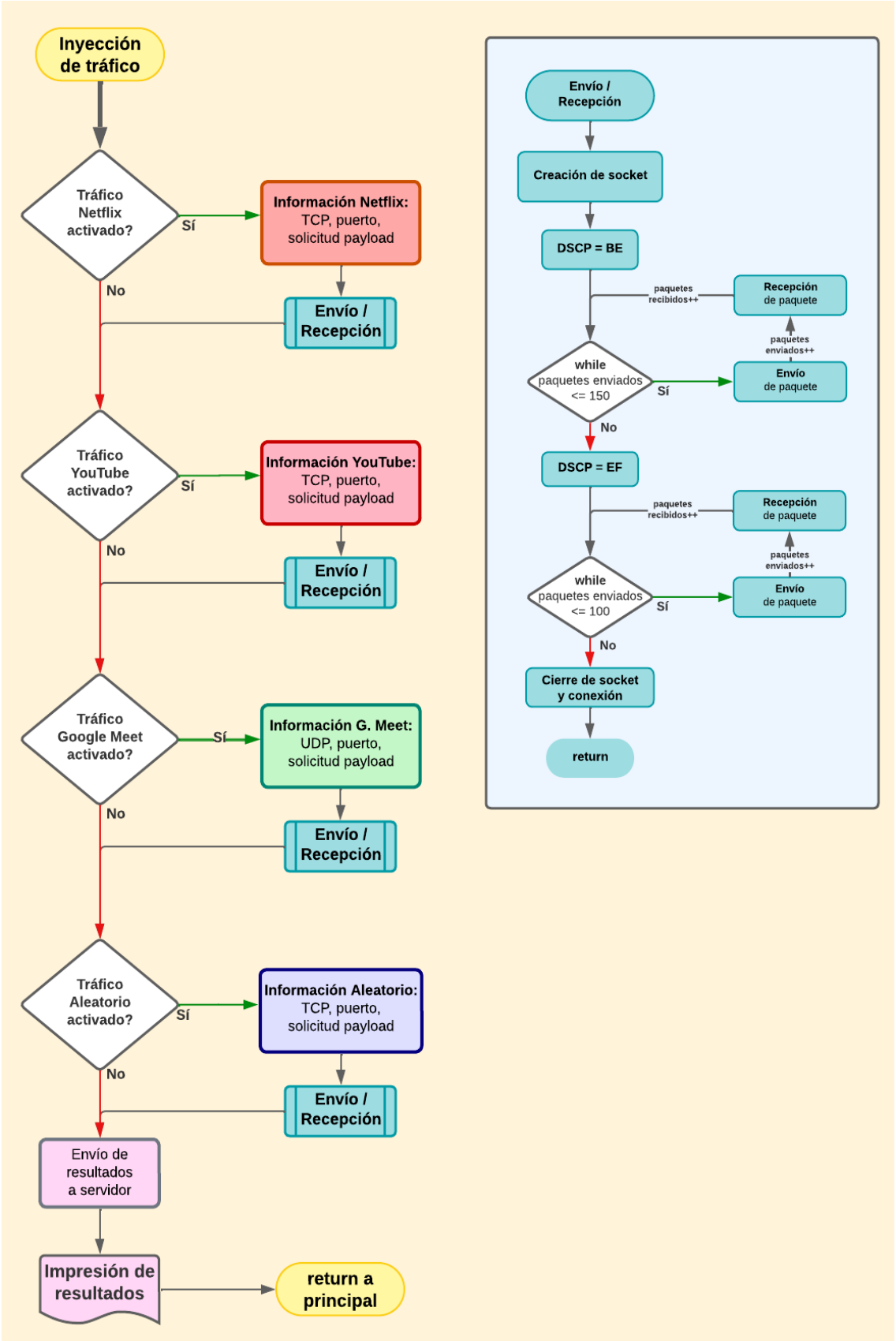


Figura 21

Diagrama de flujo - Aplicación móvil - subproceso envío/recepción



Desarrollo de servidor

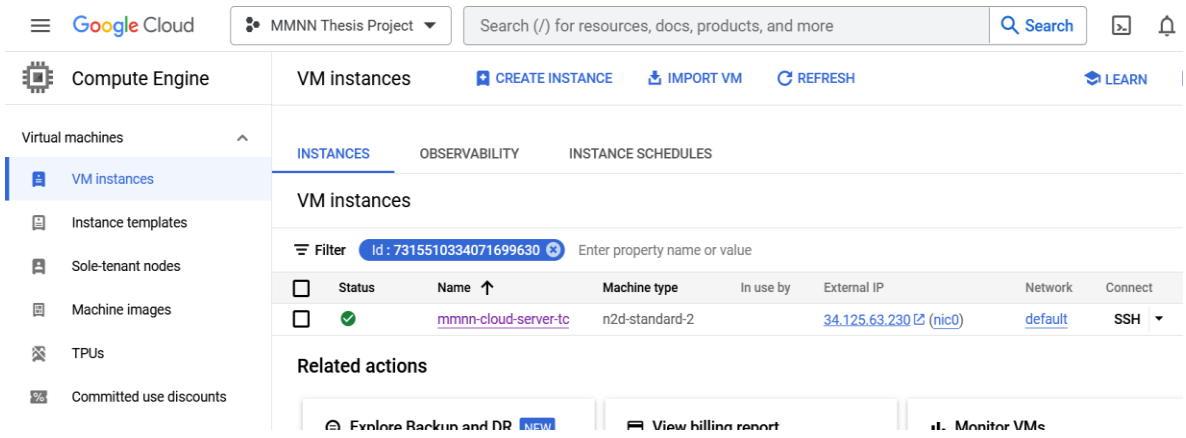
Considerando los requerimientos ya establecidos en las secciones anteriores, también es necesario establecer los requerimientos funcionales del servidor, mismo que debe encontrarse en un punto neutral de la red (suponiendo que el proveedor del mismo no implemente técnicas de DT), en este caso se optó por el uso de *Google Cloud Platform* o GCP. Esta plataforma ofrece múltiples servicios a grandes escalas y capacidades. Además, ofrece acceso gratuito y un periodo de 90 días en sus servicios de paga como es el hosting de máquinas virtuales junto con direcciones IP públicas, aspectos esenciales requeridos para esta investigación.

La máquina virtual creada dentro del servidor dispone de las siguientes características físicas dedicadas (para su funcionamiento ininterrumpido, alta capacidad de procesamiento y rápida respuesta): 2 núcleos dedicados de CPU tipo AMD Rome con arquitectura x86/64, 8GB de RAM y disco sólido, sistema operativo Ubuntu 22.04 LTS.

Se observa la plataforma de GCP con el servidor creado en la figura 22:

Figura 22

Consola Google Cloud (servidor)

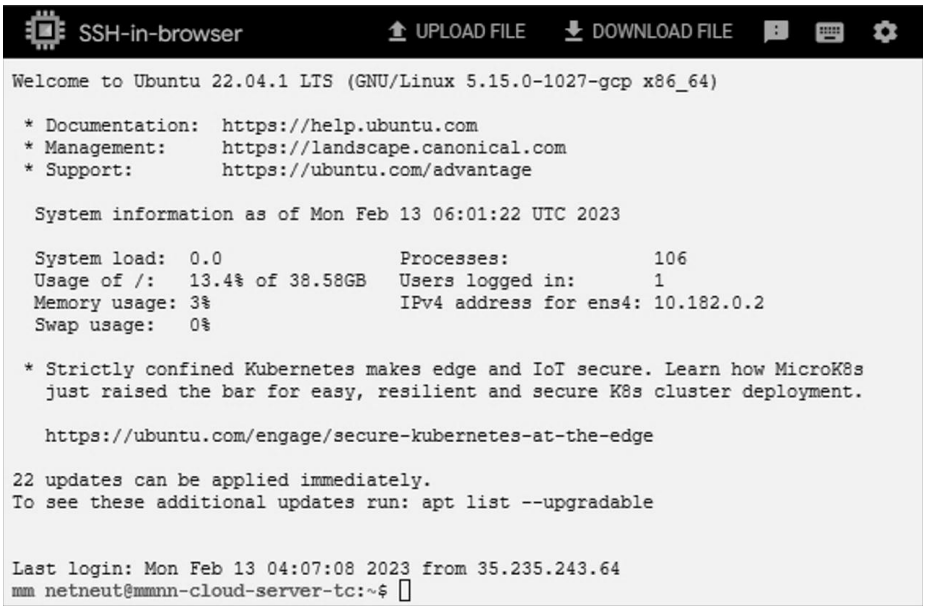


Para la configuración, programación y desarrollo de script de servidor se utilizó una conexión de SSH, misma que la plataforma GCP configura al momento de crear cada VM o máquina virtual, una característica adicional de GCP es la subida y descarga de archivos hacia o desde la VM.

Se observa la conexión al servidor por conexión SSH en la figura 23 a continuación:

Figura 23

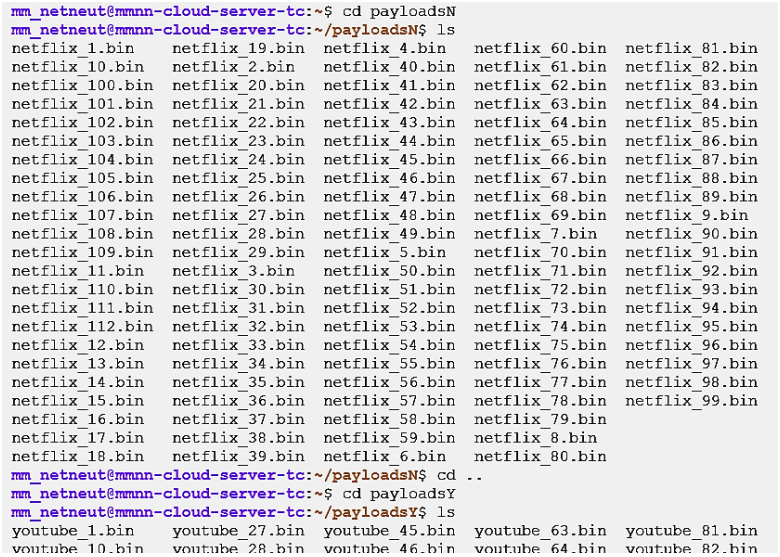
Conexión SSH a Servidor



Se establece entonces como requerimientos funcionales del servidor: Capacidad de recepción y envío de paquetes de respuesta inmediata y capacidad de acceso remoto. Los paquetes de respuesta del servidor contienen los payloads de las diferentes capturas realizadas y de cada servicio, se los puede observar en la figura 24:

Figura 24

Archivos payloads en servidor



Programación y desarrollo

La programación del servidor se basa en un script tipo bash utilizando *Port Listeners* (escuchador de puertos), en este se definen 4 funciones (‘*serve_file’*), una para cada tipo de servicio. Cada función dispone de 2 variables que son carpeta (*folder*) y puerto (*port*), además de un *loop while*, en este se elige un archivo aleatorio de una carpeta especificada correspondiente al tipo de servicio (archivo que contiene el *payload*) para su posterior envío. El código principal netcat crea un PL (*Port Listener*) y, cuando este reciba una solicitud de conexión, se establezca la misma y se envíe un paquete con el payload previamente elegido. En el caso de Google Meet, que utiliza UDP en lugar de TCP, se añade ‘-ulp’ en el comando para especificar conexiones de tipo UDP.

Esta estructura de funciones *‘serve_file’* permite la llamada y creación de 4 instancias al mismo tiempo, una para cada servicio. Se muestra a continuación una función ejemplo en la figura 25 y la instanciación con un puerto en la figura 26:

Figura 25

Código servidor - función serve_file_N()

```
serve_file_N() {
 folder=$1
 port=$2

 for i in {1..10}
 do
  file=$(ls $folder | sort -R | head -n 1)
  cat $folder/$file /home/mm_netneut/end.txt > /home/mm_netneut/tempN.bin
  nc -lp $port < /home/mm_netneut/tempN.bin
 done
}
```

Figura 26

Código servidor - script bash principal (puerto 61259)

```
serve_file_N "/home/mm_netneut/payloadsN" 61259
```

Al finalizar la prueba, se reciben los valores calculados (número de paquetes enviados, recibidos, perdidos y latencias) por parte de la aplicación, para su almacenamiento en base de datos ‘registros’ y representación gráfica en la página web.

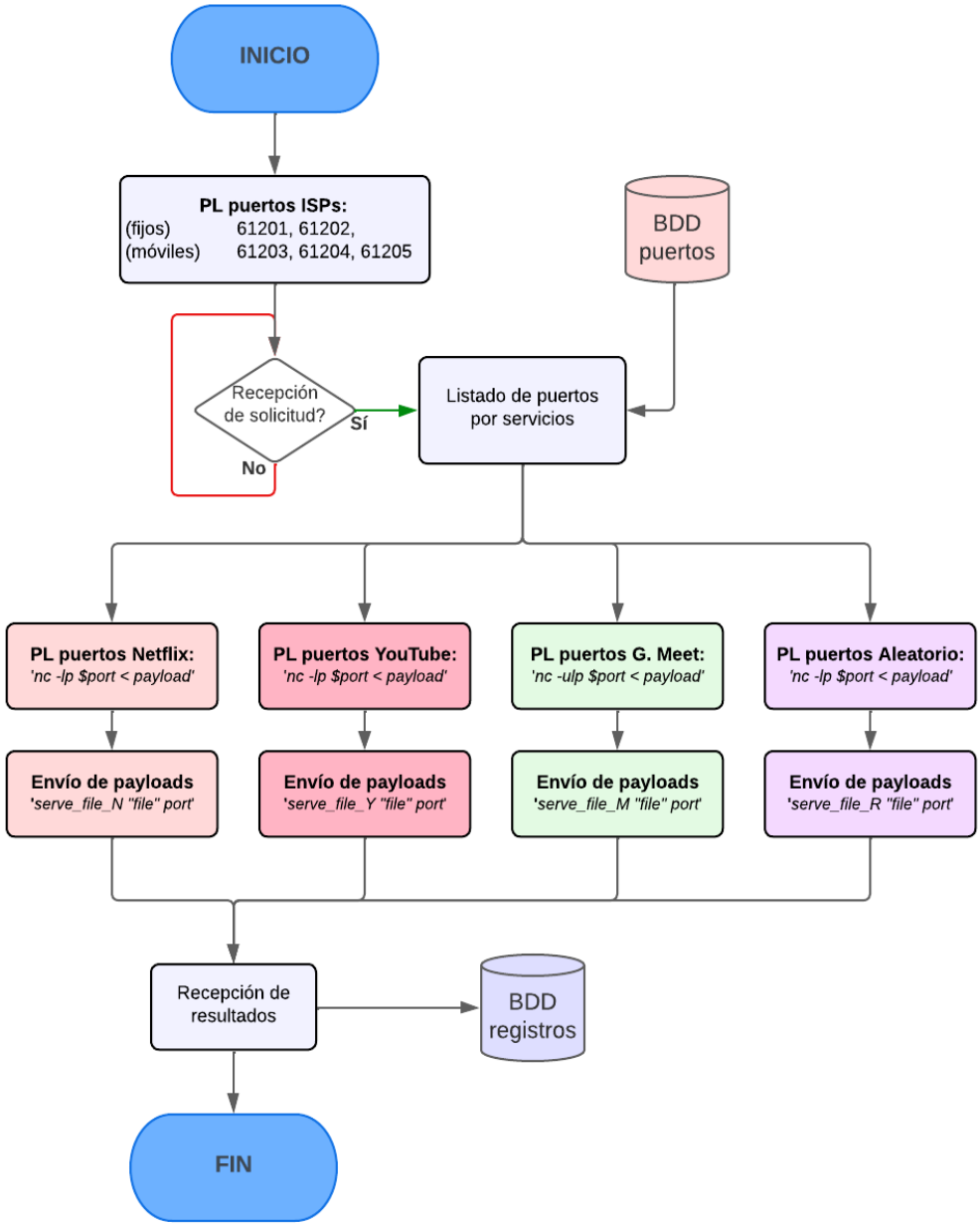
El desarrollo de la página web se realizó utilizando código HTML y PHP y se detalla posteriormente.

Diagrama de flujo

Se esquematiza el código y funcionamiento del servidor en el diagrama de flujo presentado a continuación en la figura 27. Se describe la función con ejemplo de código en el caso de PL (*Port Listener*) y envío de payloads con la función '*serve_file'*:

Figura 27

Diagrama de flujo – servidor



Una vez vistos los puntos de diseño de aplicación (3.3) y desarrollo de servidor (3.4) se indica el diagrama de tecnologías para aplicación de escritorio en la figura 28 y móvil en la figura 29.

Figura 28

Diagrama de tecnologías - Frontend (aplicación de escritorio) y Backend (Servidor)

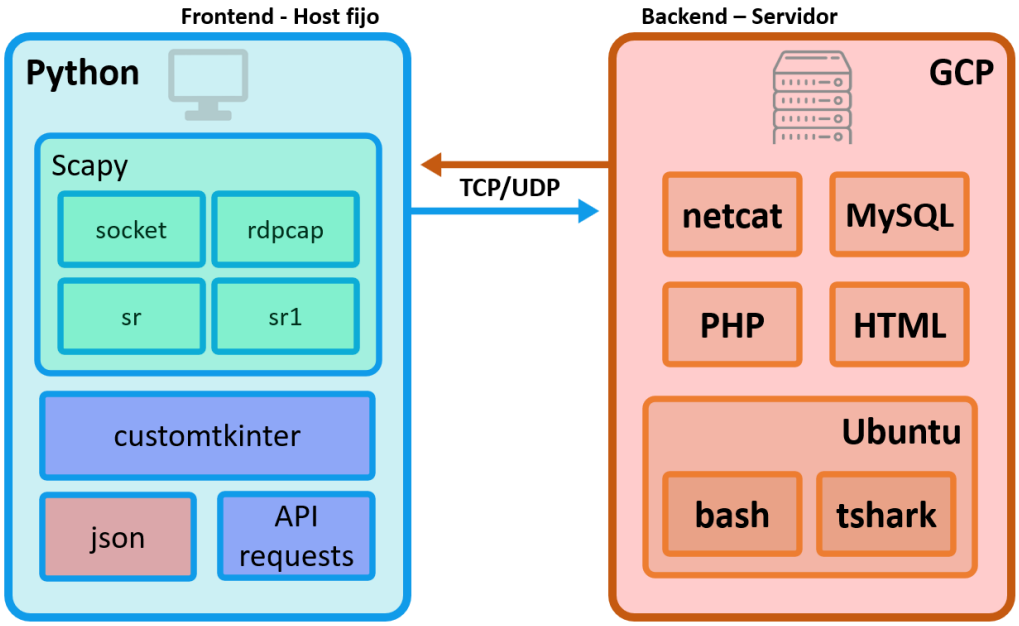
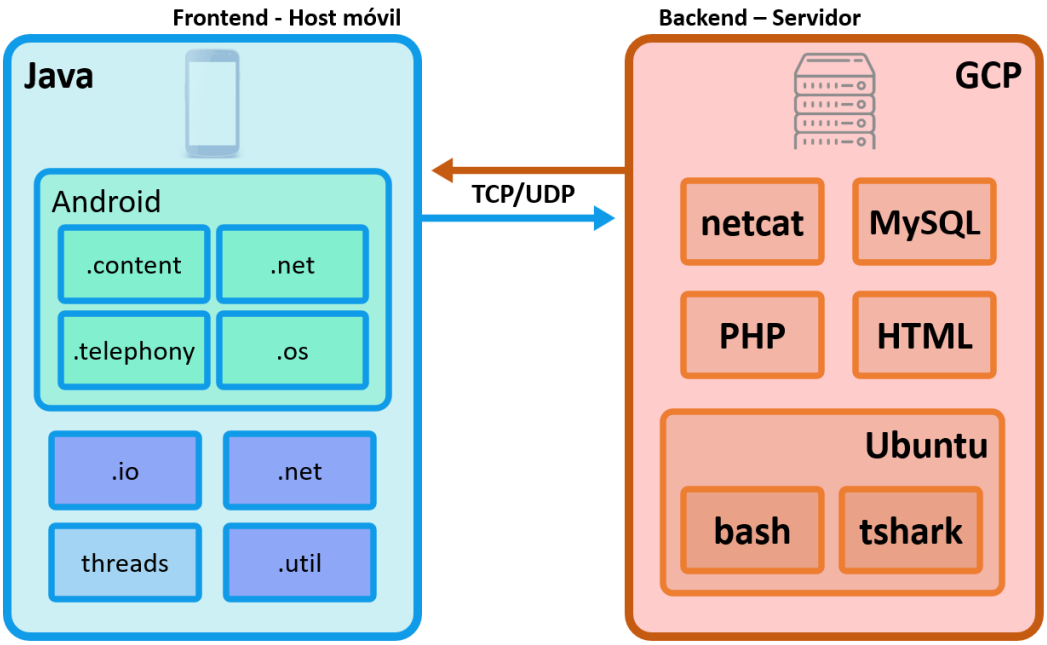


Figura 29

Diagrama de tecnologías - Frontend (aplicación móvil) y Backend (Servidor)



Protocolos de pruebas

Definir protocolos de pruebas brinda beneficios en trabajos de investigación, los más importante son: replicabilidad (posibilidad de realizar los mismos pasos y obtener resultados similares), objetividad (reflejar de mejor manera los efectos reales de las variables que se están evaluando), fiabilidad (minimizar variabilidad en la recopilación de datos) y validación (demostrar que los resultados obtenidos son válidos y confiables) (Rout & Aldous, 2016).

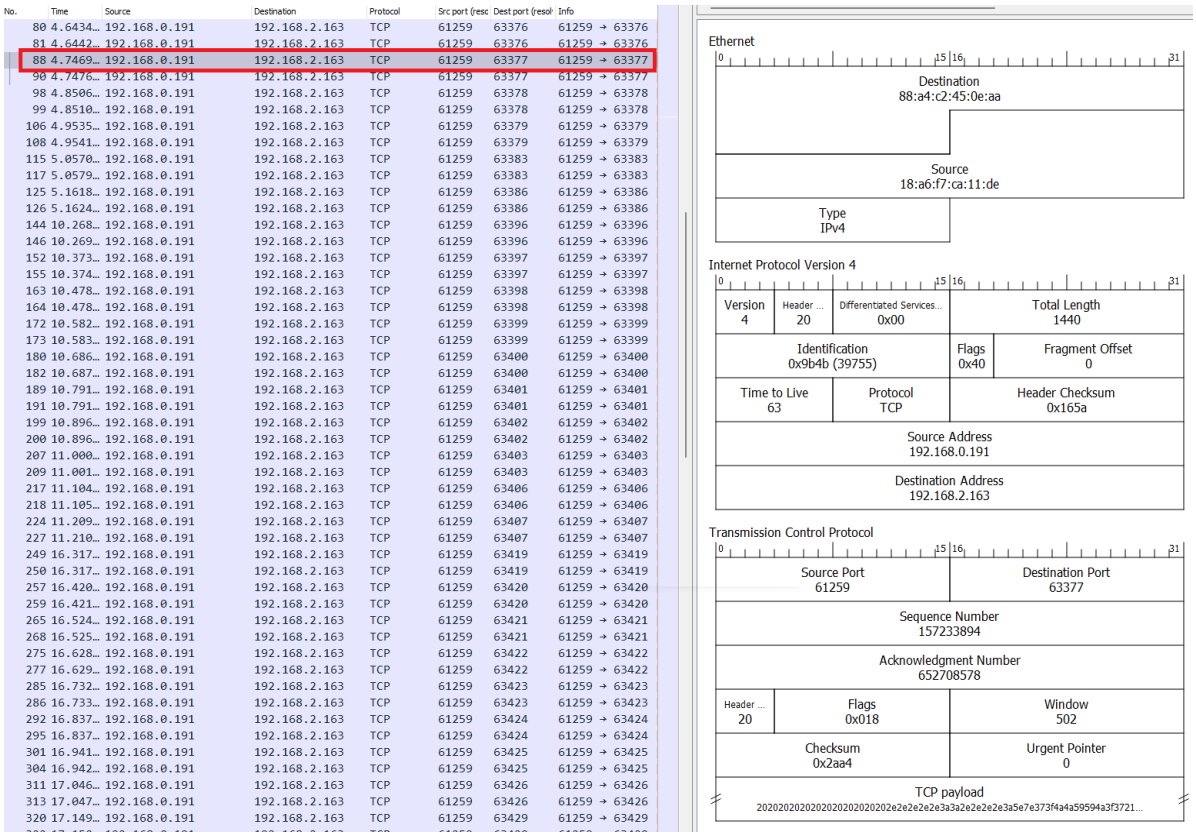
Pruebas de aplicación

Estas pruebas, junto con la captura y posterior análisis del tráfico generado (por las aplicaciones fija y móvil), validan el mismo y el correcto funcionamiento de la aplicación.

Aplicación de escritorio: Se observan las capturas del tráfico generado por la aplicación de escritorio en la figura 30, más adelante se muestran los paquetes y sus campos relevantes para la replicación de cada tipo de tráfico o servicio.

Figura 30

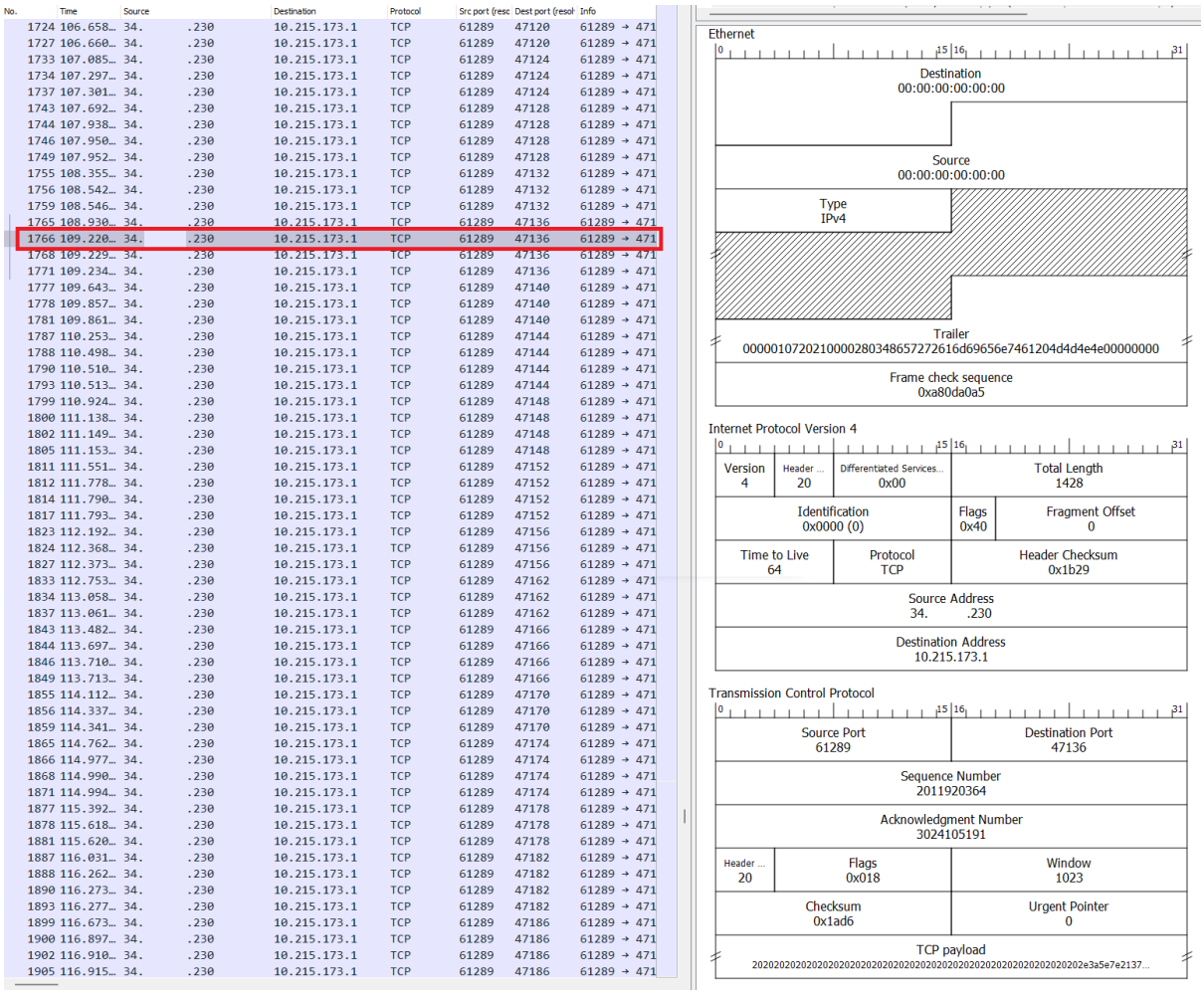
Prueba de aplicación de escritorio



Aplicación móvil: Al igual que en el punto anterior, se observan las capturas del tráfico generado por la aplicación móvil en la figura 31 y más adelante se analizan los paquetes.

Figura 31

Prueba de aplicación móvil



Pruebas de laboratorio

Estas pruebas ayudarán a validar el funcionamiento, conexión y tráfico de red generado entre las aplicaciones y el servidor local, además de los requerimientos de diseño, entre ellos el monitoreo de paquetes y latencia en un ambiente controlado.

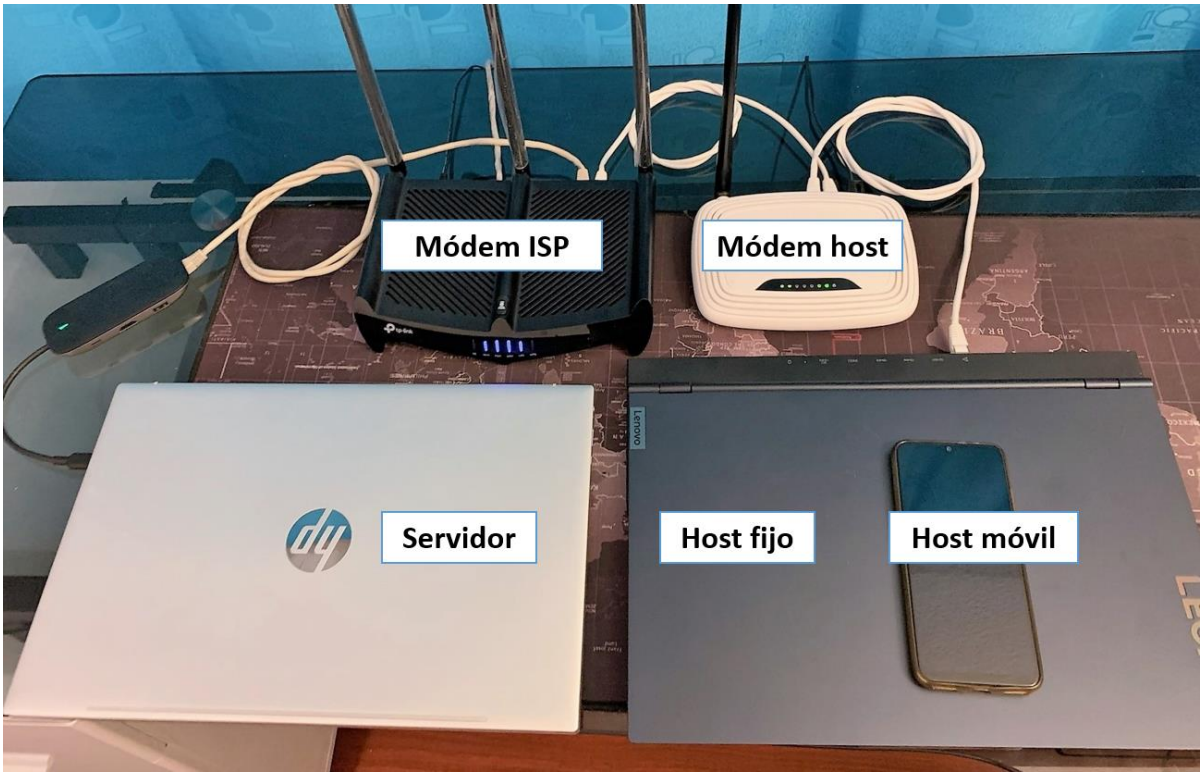
Se realizaron pruebas en 3 escenarios de reglas de tráfico: sin DT, con DT hacia 1 aplicación o servicio y con DT hacia varias aplicaciones o servicios

Estas pruebas se realizaron con 2 equipos routers (TP-Link), 1 computador portátil como servidor, 1 equipo portátil como host fijo y 1 teléfono inteligente como host móvil. Las conexiones servidor-router ISP y router ISP-router host se realizaron mediante cable ethernet, simulando en medida de lo posible la topología de ambos escenarios.

Se presenta a continuación en la figura 32 una fotografía de estas conexiones:

Figura 32

Pruebas de laboratorio – fotografía conexiones de red



- **Red primaria** **192.168.0.0 /24**
  - Servidor 192.168.0.191
  - Módem ISP 192.168.0.1
  - Módem host 192.168.0.102
- **Red secundaria** **192.168.2.0 /24**
  - Módem host 192.168.2.1
  - Host fijo 192.168.2.170
  - Host móvil 192.168.2.161

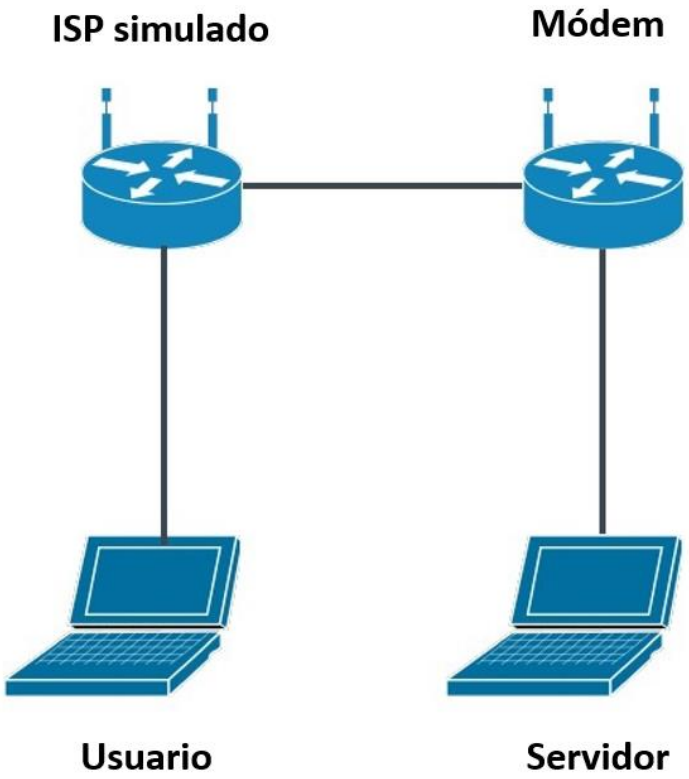
La red primaria simula la Internet y la red del ISP, aquí se encuentra el servidor (dirección IP reservada que simula una pública), y se puede acceder al mismo desde cualquiera de las dos redes (primaria y secundaria). La red secundaria simula la red local del host, aquí se encuentran los hosts fijo y móvil.

El módem host utiliza al módem ISP como Gateway o DNS, por lo que los paquetes que lleguen a este, será redireccionados hacia el servidor. Las conexiones se verificaron desactivando firewalls y utilizando los comandos ‘ping’, ‘tracert’ y ‘traceroute’ más adelante.

Aplicación de escritorio: En el escenario de conexión fija y aplicación de escritorio, se utilizó conexión por cable ethernet entre módem host y equipo de usuario como se indica en la figura 33.

Figura 33

Prueba laboratorio - escenario fijo



1. Prueba de conexión (haciendo uso del comando tracert y ping) desde el host (computadora de usuario) hacia el servidor local (figura 34).

Figura 34

Prueba de conexión fija (usuario – servidor local)

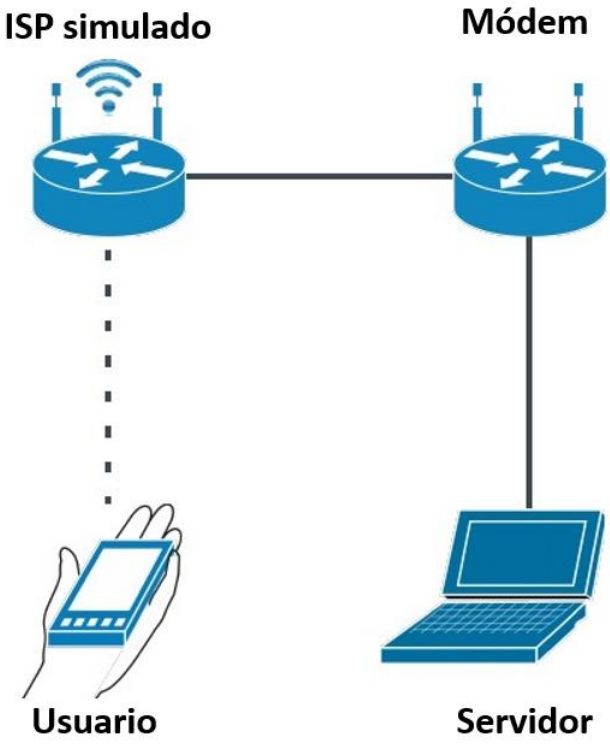
```
C:\Users\steve>tracert 192.168.0.191

Tracing route to 192.168.0.191 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2     1 ms    <1 ms     1 ms  192.168.0.191

Trace complete.

C:\Users\steve>ping 192.168.0.191

Pinging 192.168.0.191 with 32 bytes of data:
Reply from 192.168.0.191: bytes=32 time<1ms TTL=63
Reply from 192.168.0.191: bytes=32 time=1ms TTL=63
Reply from 192.168.0.191: bytes=32 time=1ms TTL=63
Reply from 192.168.0.191: bytes=32 time=1ms TTL=63

Ping statistics for 192.168.0.191:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\steve>
```

2. Correr comando de servidor local (netcat / serve_file) listo para recibir solicitudes y enviar paquetes con payloads a los puertos respectivos.
3. Inicio de aplicación de escritorio.
4. Inicio de prueba, duración aproximada de 2 a 3 minutos (dependiendo del estado y velocidad de la red).
5. Impresión y registro de resultados.
6. Repetir desde el paso 4 hasta alcanzar los requerimientos y consideraciones necesarias para la validación de la herramienta.
7. Verificación y validación del tráfico generado.

Aplicación móvil: En el escenario de conexión y aplicación móvil, se utilizó conexión por Wi-Fi 2.4GHz a menos de 1 metro de distancia entre módem host y equipo de usuario como se indica en la figura 35.

Figura 35

Red móvil - laboratorio



1. Prueba de conexión (haciendo uso del comando traceroute y ping) desde el host (equipo móvil de usuario) hacia el servidor local (figura 36).

Figura 36

Prueba de conexión móvil (usuario – servidor local)

```
$ ifconfig
Warning: cannot open /proc/net/dev (Permission denied). Limited output.
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)

rmnet_data2: flags=65<UP,RUNNING>  mtu 1500
        inet 100.80.76.211  netmask 255.255.255.248
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.161  netmask 255.255.255.0  broadcast 192.168.2.255
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 3000  (UNSPEC)

$ traceroute 192.168.0.191
 1?: [LOCALHOST]                      pmtu 1500
 1:  192.168.2.1                                           5.877ms
 1:  192.168.2.1                                           5.275ms
 2:  192.168.0.191                                         2.790ms reached
     Resume: pmtu 1500 hops 2 back 2
$
```

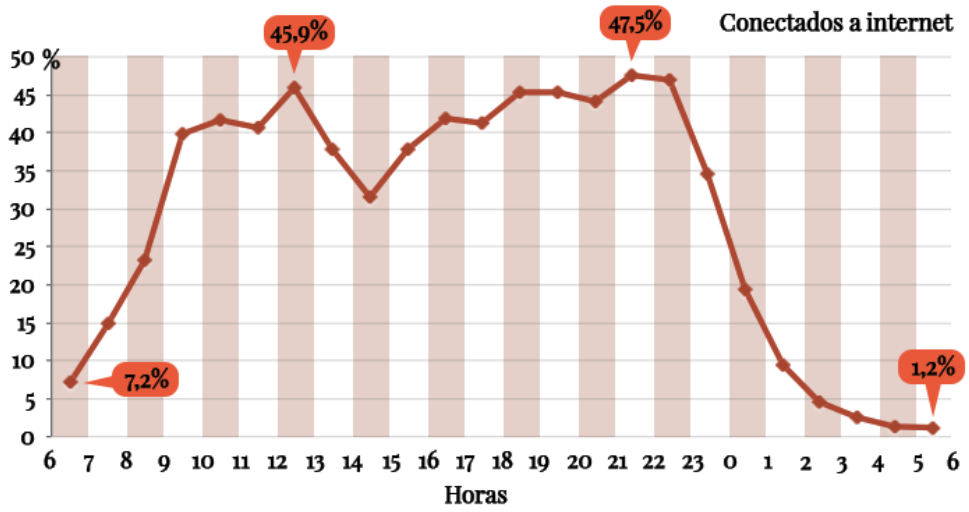
2. Ejecutar el comando de servidor (netcat / serve_file) listo para recibir solicitudes y enviar paquetes con payloads a los puertos respectivos.
3. Inicio de aplicación de escritorio.
4. Inicio de prueba, duración aproximada de 3 a 5 minutos.
5. Impresión y registro de resultados.
6. Repetir desde el paso 4 hasta alcanzar los requerimientos y consideraciones necesarias para la validación de la herramienta.
7. Verificación y validación del tráfico generado.

Pruebas de campo

Para realizar las pruebas se establecieron parámetros de conexión, envío y recepción. Los horarios fueron escogidos por los autores, se hicieron en base a la figura 37, considerando las horas en las que existe una mayor demanda de tráfico.

Figura 37

Horas de mayor conexión a Internet



Nota. Tomado de *Crónica,* por Mateo, G, 2018, (https://cronicaglobal.elespanol.com/graficnews/horas-mas-conexiones-internet_127349_102.html)

Los horarios determinados por los autores con respecto al tráfico de Internet por horas se muestran en la tabla 7.

Tabla 7

Horarios establecidos para las pruebas de campo.

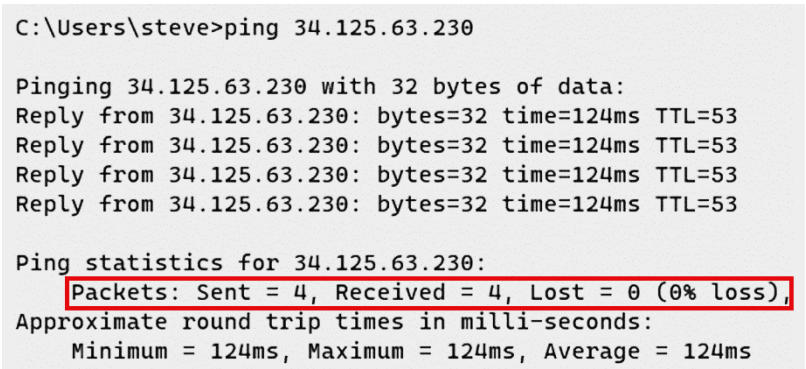
Horario	Horas
H1	23:00 – 03:00
H2	06:00 – 08:00
H3	11:00 – 13:00
H4	19:00 – 21:00

Aplicación de escritorio: Se aseguró una conexión por cable ethernet entre módem host y equipo de usuario (laptop) y corriendo únicamente la aplicación por la duración de las pruebas.

1. Prueba de conexión (haciendo uso del comando ping) desde el host (computadora de usuario) hacia el servidor en la nube (figura 38)

Figura 38

Prueba de conexión fija (usuario – servidor nube)



2. Correr comando de servidor en la nube (netcat / serve_file) listo para recibir solicitudes y enviar paquetes con payloads a los puertos respectivos.
3. Inicio de aplicación de escritorio.

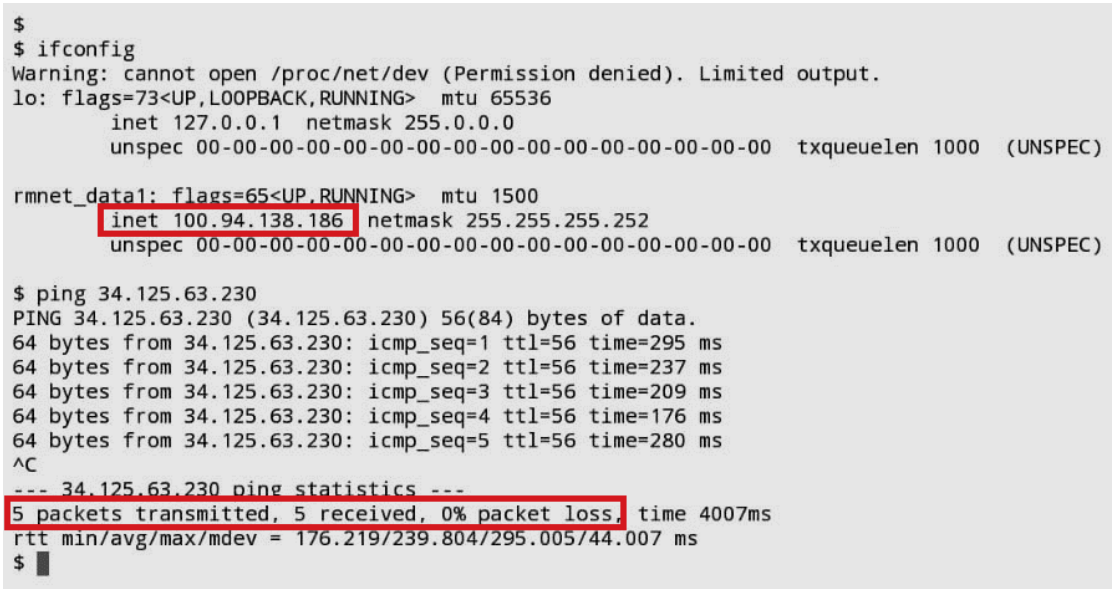
4. Inicio de prueba, duración aproximada de 2 a 3 minutos (dependiendo del estado y velocidad de la red).
5. Impresión y registro de resultados.
6. Repetir desde el paso 4 alternando horarios 1, 2, 3 y 4, de manera diaria y por 4 semanas.

Aplicación móvil: Se aseguró y verificó en todo momento conexión por 4G LTE en todos los ISP's móviles, con alta y constante señal en el equipo de usuario (móvil) y sin uso o manipulación física por la duración de las pruebas:

1. Prueba de conexión (haciendo uso del comando ping en) desde el host (equipo móvil de usuario) hacia el servidor local (figura 39)

Figura 39

Prueba de conexión móvil (usuario – servidor nube)



2. Ejecutar el comando de servidor (netcat / serve_file) listo para recibir solicitudes y enviar paquetes con payloads a los puertos respectivos.
3. Inicio de aplicación móvil.
4. Inicio de prueba, duración aproximada de 3 a 5 minutos (dependiendo del estado y velocidad de la red).
5. Impresión y registro de resultados.

6. Repetir desde el paso 4 alternando horarios 1, 2, 3 y 4, de manera diaria y por 4 semanas.

Los resultados obtenidos en las pruebas de campo se detallan y analizan en el siguiente capítulo.

Desarrollo de página web

Se desarrolló la página web HTML, de manera que se muestra el título del trabajo de investigación (figura 40) y resultados por ISP (figura 41).

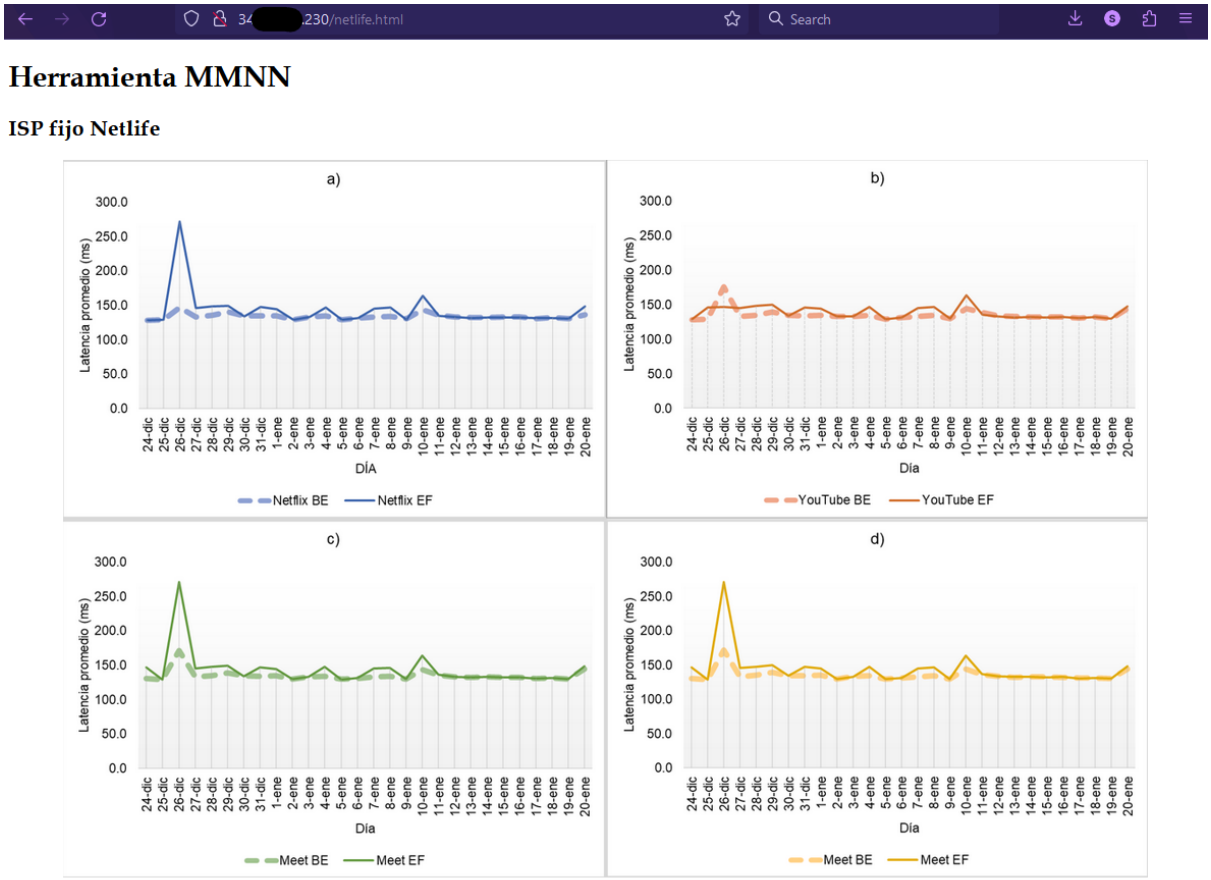
Figura 40

Página Web – Inicio

Se puede observar el redireccionamiento entre página principal a los resultados obtenidos del ISP Netlife, donde se representa las latencias de manera diaria y comparando servicios y tipos de tráfico con DSCP BE y EF.

Figura 41

Página web - Resultados ISP Netlife



Capítulo IV

Análisis y Resultados

Los resultados se obtuvieron a partir del diseño de las aplicaciones (fija y móvil) y de las pruebas realizadas tanto en campo como en laboratorio, cada una con su respectivo protocolo de pruebas, tal como se explicó en el capítulo anterior, las mismas fueron realizadas en un lapso de cuatro semanas, con los cuatro diferentes horarios definidos en los protocolos.

Resultados de diseño

Paquete creado

Se realiza la comparación en las figuras 42 y 43 entre paquetes original y sintético de los servicios de Netflix y Google Meet respectivamente, resaltando sus aspectos principales que son: protocolo, puertos y el mismo payload. Al utilizar una serie de paquetes sintéticos se logra un tráfico replicado en medida de lo posible.

Figura 42

Paquetes Netflix a) original y b) sintético.

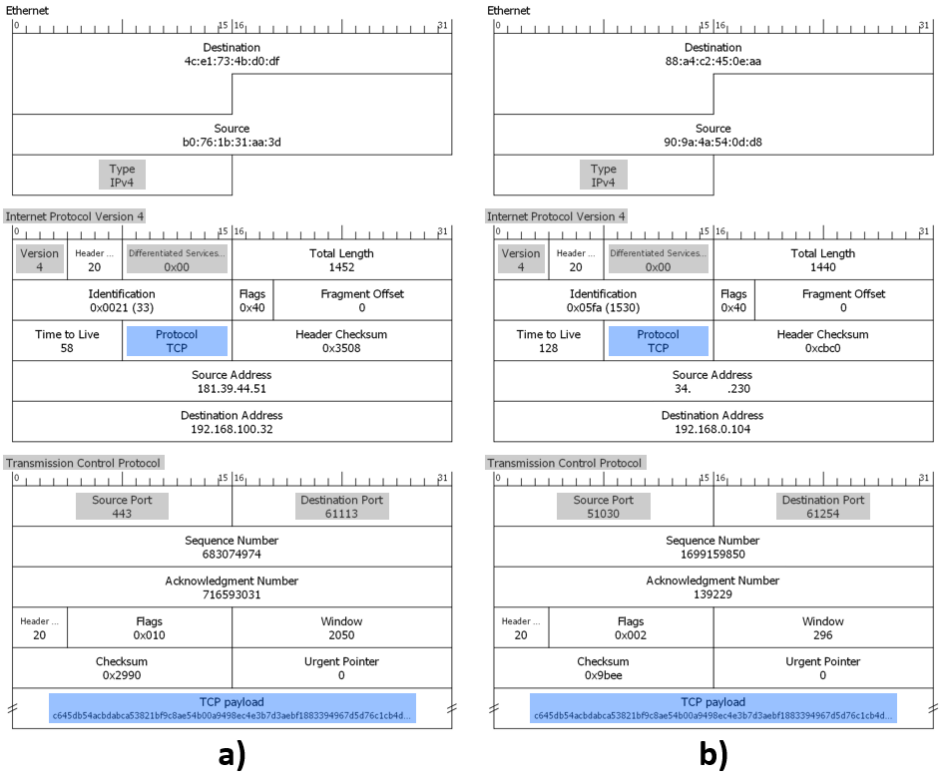
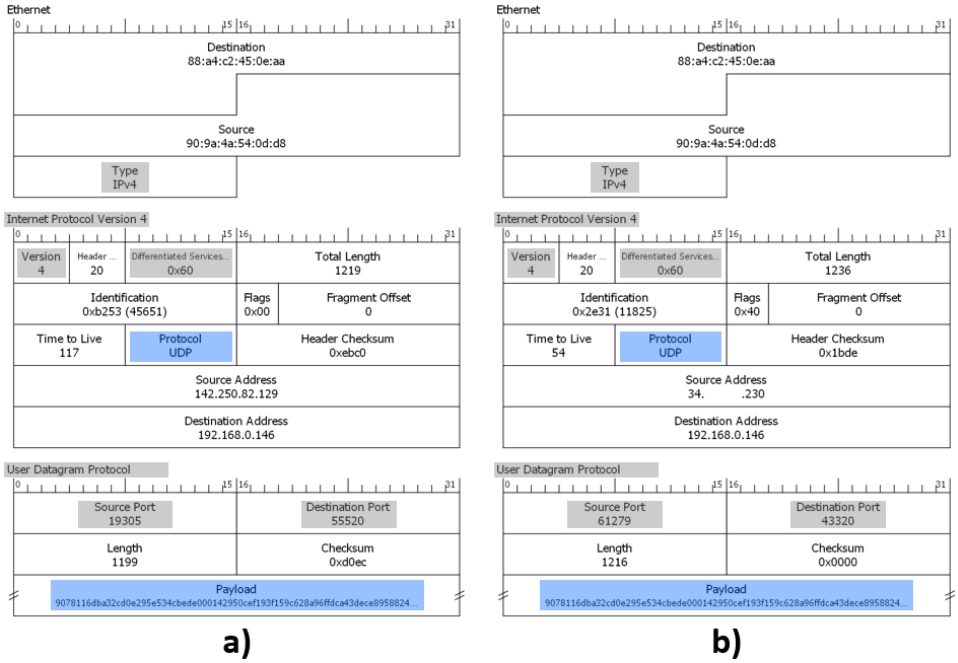


Figura 43

Paquetes Google Meet a) original y b) sintético

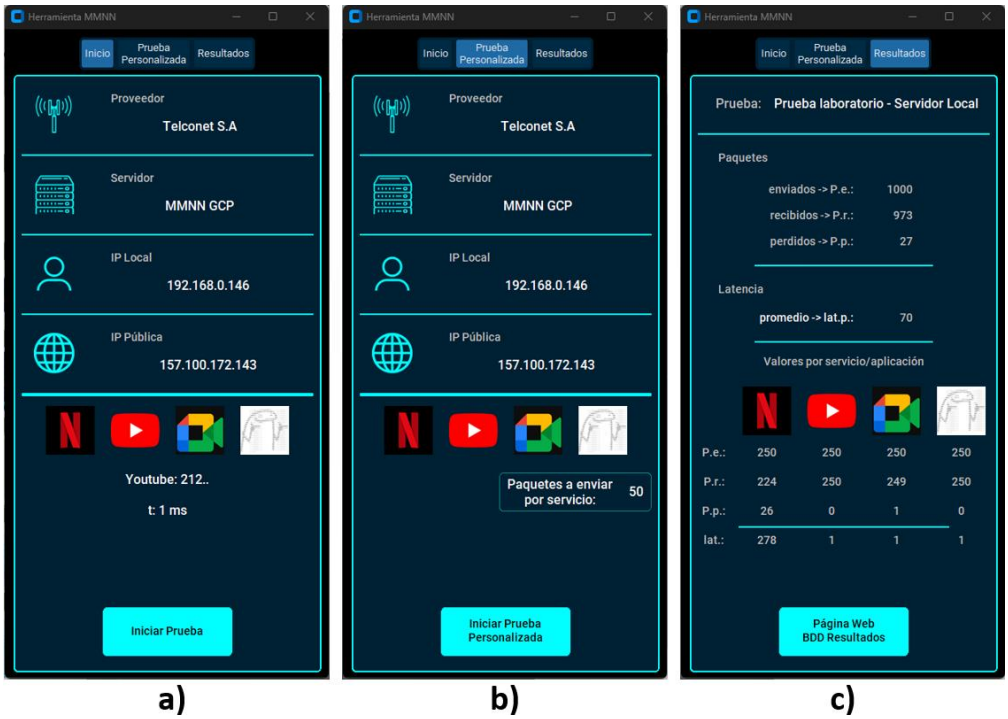


Aplicación fija

Se observa en la figura 44 y 45 las aplicaciones fija y móvil con sus 3 pestañas: inicio, prueba personalizada y resultados.

Figura 44

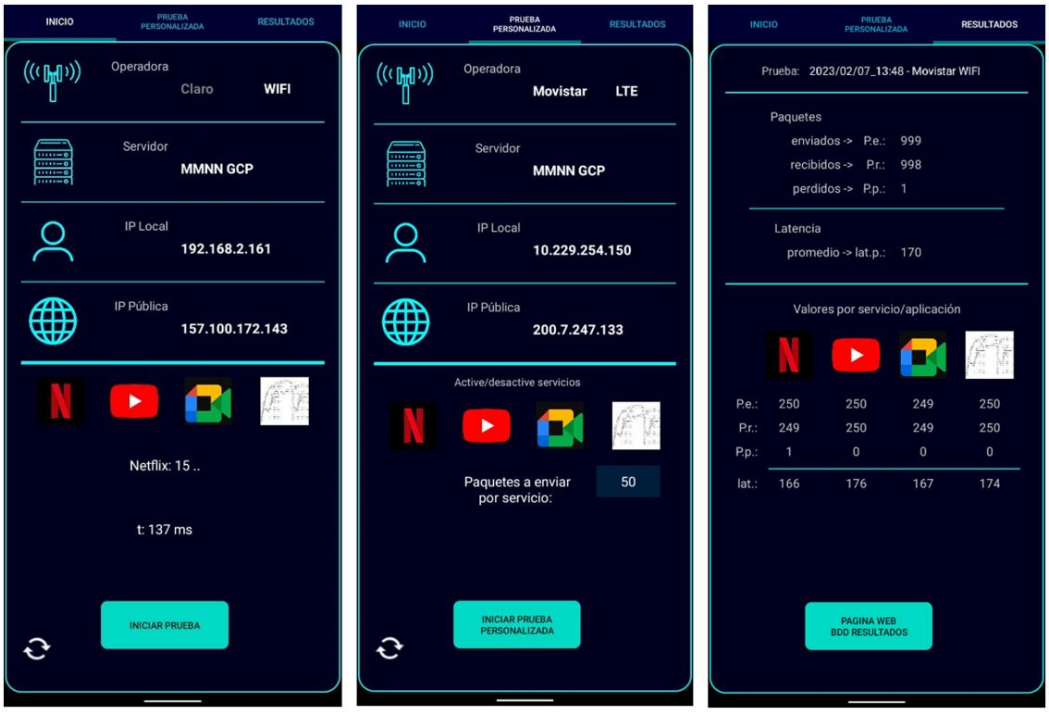
Resultados de diseño app escritorio - pestañas a) inicio, b) p. personalizada y c) resultados



Aplicación móvil

Figura 45

Resultados de diseño app móvil – pestañas a) inicio, b) prueba personalizada y c) resultados



Resultados de pruebas de laboratorio

Aplicación de escritorio

Se realizaron pruebas en 2 escenarios, sin DT y con DT hacia la aplicación Netflix. Para esto se utilizó un módem con capacidad de aplicar reglas de tráfico por direcciones IP y puertos, se muestra en la tabla con las reglas de tráfico en la figura 46 a continuación:

Figura 46

Reglas de tráfico por direcciones IP y puertos.

Bandwidth Control Rule List

ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
1	192.168.2.161 - 192.168.2.164/61250 - 61260	200	400	20	40	☑	Modify Delete
2	192.168.2.161 - 192.168.2.164/61261 - 61270	200	400	10	20	☑	Modify Delete
3	192.168.2.161 - 192.168.2.164/61271 - 61280	200	400	200	400	☑	Modify Delete
4	192.168.2.161 - 192.168.2.164/61281 - 61290	200	400	200	400	☑	Modify Delete

Primer escenario – Sin DT: Para el primer escenario no se activó reglas de tráfico, con tiempos de latencia host fijo-servidor (laboratorio) de menos de 1ms (como se muestra en la figura 34), se muestran los valores esperados y obtenidos en las tablas 8 y 9:

Tabla 8

Aplicación fija - Valores esperados – sin DT

	Netflix	**YouTube**	**Meet**	**Aleatorio**
P. enviados	250	250	250	250
P. recibidos	250	250	250	250
P. perdidos	0	0	0	0
Latencia prom.	<1 ms	<1 ms	<1 ms	<1 ms

Tabla 9

Aplicación fija - Valores obtenidos – sin DT

	Netflix	**YouTube**	**Meet**	**Aleatorio**
P. enviados	250	250	250	250
P. recibidos	250	250	250	250
P. perdidos	0	0	0	0
Latencia prom.	0.425 ms	0.271 ms	0.215 ms	0.374 ms

Los valores obtenidos coinciden con los esperados, una tasa de paquetes enviados-recibidos del 100% y un tiempo de latencia promedio de menos de 1ms, indicando el correcto y esperado funcionamiento de la herramienta de escritorio.

Segundo escenario – Con DT: Para el segundo escenario se activaron reglas de tráfico para el puerto 61259 en específico (mismo que utiliza Netflix en este caso), se muestran los valores esperados y obtenidos en las tablas 10 y 11:

Tabla 10

Aplicación fija - Valores esperados – con DT

	Netflix	**YouTube**	**Meet**	**Aleatorio**
P. enviados	250	250	250	250
P. recibidos	<250	250	250	250
P. perdidos	>0 ms	0 ms	0 ms	0 ms
Latencia prom.	>200 ms	<1 ms	<1 ms	<1 ms

Tabla 11

Aplicación fija - Valores obtenidos – con DT

	Netflix	YouTube	Meet	Aleatorio
P. enviados	250	250	250	250
P. recibidos	224	250	249	250
P. perdidos	26	0	1	0
Latencia prom.	278 ms	0.681 ms	0.484 ms	0.421 ms

Se puede observar que se obtienen los resultados esperados, con una pérdida de paquetes de aproximadamente 10% y un aumento en latencia promedio para ese servicio.

Aplicación móvil

Primer escenario – Sin DT: Se realizó esta prueba con las mismas reglas que el primer escenario de la aplicación fija, por lo que se pueden esperar tiempos parecidos con un aumento máximo de 10ms a través de todos los valores por la conexión inalámbrica host móvil-servidor (de laboratorio) de aproximadamente 8 ms (como se muestran en la figura 36), se muestran los valores esperados y obtenidos en las tablas 12 y 13:

Tabla 12

Aplicación móvil - Valores esperados – sin DT

	Netflix	YouTube	Meet	Aleatorio
P. enviados	250	250	250	250
P. recibidos	250	250	250	250
P. perdidos	0	0	0	0
Latencia prom.	<10 ms	<10 ms	<10 ms	<10 ms

Tabla 13

Aplicación móvil - Valores obtenidos – sin DT

	Netflix	YouTube	Meet	Aleatorio
P. enviados	250	250	250	250
P. recibidos	250	250	250	250
P. perdidos	0	0	0	0
Latencia prom.	9 ms	8 ms	4 ms	7 ms

Se observa que los valores esperados y obtenidos coinciden, esperando tiempos de menos de 10 ms en latencia y en todos los servicios y sin pérdida de paquetes.

Segundo escenario – Con DT: En este segundo escenario se utilizaron las mismas reglas que en aplicación fija, esperando valores similares. Se detallan los valores de latencia con reglas de tráfico (que se esperan en más de 200 ms) y los obtenidos en las tablas 14 y 15 respectivamente:

Tabla 14

Aplicación móvil - Valores esperados – con DT

	Netflix	**YouTube**	**Meet**	**Aleatorio**
P. enviados	250	250	250	250
P. recibidos	250	<250	<250	<250
P. perdidos	0	>0	>0	>0
Latencia prom.	>10 ms	>200 ms	>200 ms	>200 ms

Tabla 15

Aplicación móvil - Valores obtenidos – con DT

	Netflix	**YouTube**	**Meet**	**Aleatorio**
P. enviados	250	250	250	250
P. recibidos	250	241	246	239
P. perdidos	0	9	4	11
Latencia prom.	11 ms	267 ms	278 ms	251 ms

Resultados de pruebas de campo

Los resultados obtenidos con la aplicación de escritorio y aplicación móvil, se realizaron siguiendo los protocolos de pruebas de la herramienta en campo como se especificó en el capítulo anterior, estos son: los mismos horarios, la misma cantidad de paquetes inyectados, y procesando los datos para obtener la latencia promedio y la pérdida de paquetes.

Para el análisis de los resultados se consideraron dos estudios referentes a la herramienta de detección de DT Wehe.

El primero estudio (Li & al, 2019) es realizado por los desarrolladores de la aplicación, estos realizan un análisis del funcionamiento de la aplicación y como realiza el proceso de análisis de datos, de manera que, junto con los resultados obtenidos, se obtenga la capacidad de emitir juicios de valor y determinar o detectar la diferenciación de tráfico realizada por los ISP's para los servicios más populares.

En el segundo estudio (Castoreo, Maillé, & Tuffin, 2021) se analiza la herramienta Wehe poniéndola a prueba en un ambiente desarrollado y diseñado para buscar sus limitaciones y vulnerabilidades, para ofrecer alternativas adicionales (umbral de detección, detección vs impacto en la calidad percibida por el usuario y optimización de diferenciación) a las que utiliza Wehe (entre ellas la regla Kolmogorov-Smirnov), mediante las cuales se puede mejorar la detección de la existencia o no de DT por parte de los ISP.

Wehe utiliza una técnica de 'grabar y reproducir' para su inyección de tráfico, primero registra el tráfico de red generado por una aplicación y se incluye un seguimiento de tráfico a la misma. Cuando el usuario ejecuta la prueba en esta aplicación, Wehe reproduce este tráfico entre el dispositivo y un servidor Wehe, de manera que todo el tráfico que se intercambia sea idéntico al registrado (puertos, protocolo y payload) con la diferencia de las direcciones IP (Li & al, 2019).

Al ejecutar la aplicación se envía una solicitud al servidor de Wehe para iniciar una prueba. El servidor luego envía solicitudes de tráfico de prueba (replicado de los servicios más populares) al ISP en el que se encuentra el usuario. Una vez que el tráfico de prueba comienza a viajar a través de la red del ISP, la aplicación Wehe monitorea la calidad de la conexión y la velocidad de descarga para cada aplicación (Li & al, 2019).

Finalizadas las pruebas, Wehe realiza una combinación entre reglas estadísticas (como la de Kolmogorov-Smirno), estimadores de densidad de Kernel y la detección de puntos de cambio, con esto se obtiene una comparación entre un tráfico neutral (bits originales del payload invertidos) y uno de un servicio en específico, de manera que, si

ambos tráficos poseen la misma tendencia se concluye que no existe reglas de DT, pero en caso de no hacerlo se concluye que si existe DT (Li & al, 2019).

En el caso de la herramienta desarrollada en este trabajo de investigación y para el análisis de los datos no se puede seguir la regla de Kolmogorov-Smirnov, ya que no se generó un tráfico neutral del cual pueda compararse con el obtenido, solo se generó un tráfico aleatorio, adicional al de los servicios de video, y como se menciona en el estudio (Li, F, et al, 2017) los tráficos aleatorios si son propensos a activar la diferenciación, por lo que se consideró realizar un análisis por umbral de detección, el cual menciona que, para que un servicio de video sea deteriorado o se vea diferenciado, se debe tener una tasa de pérdida de paquetes de hasta el 4,6 %, o agregar menos de 55ms de retraso entre servicios (Castoreo, Maillé, & Tuffin, 2021).

Por lo tanto, los parámetros que se consideraron en los resultados de las pruebas para determinar la existencia de diferenciación de tráfico, tanto en los servicios de internet fijos como en los móviles son: latencia entre servicios, cabeceras con diferentes prioridades en los paquetes (DSCP) y pérdida de paquetes.

ISP Fijo - Netlife

Los resultados para este proveedor de servicios de Internet (ISP) se obtuvieron a través de las pruebas de campo y siguiendo su respectivo protocolo.

Los valores que se muestran a continuación (tabla 16), tienen el promedio de la latencia (unidades en milisegundos) por día, por cada uno de los servicios probados, y la diferencia de latencia entre estos (unidades en milisegundos).

En las columnas ‘Δt entre servicios’ se resaltaron los valores que exceden los 55ms, esto es consecuencia a la regla del umbral de detección, se resaltó de color naranja los que exceden este valor, y de color marrón los que exceden los 100ms, esto con el fin de verificar las posibles diferenciaciones de tráfico entre servicios.

Tabla 16

Latencia promedio por servicio y diferencia entre servicios (ISP NETLIFE)

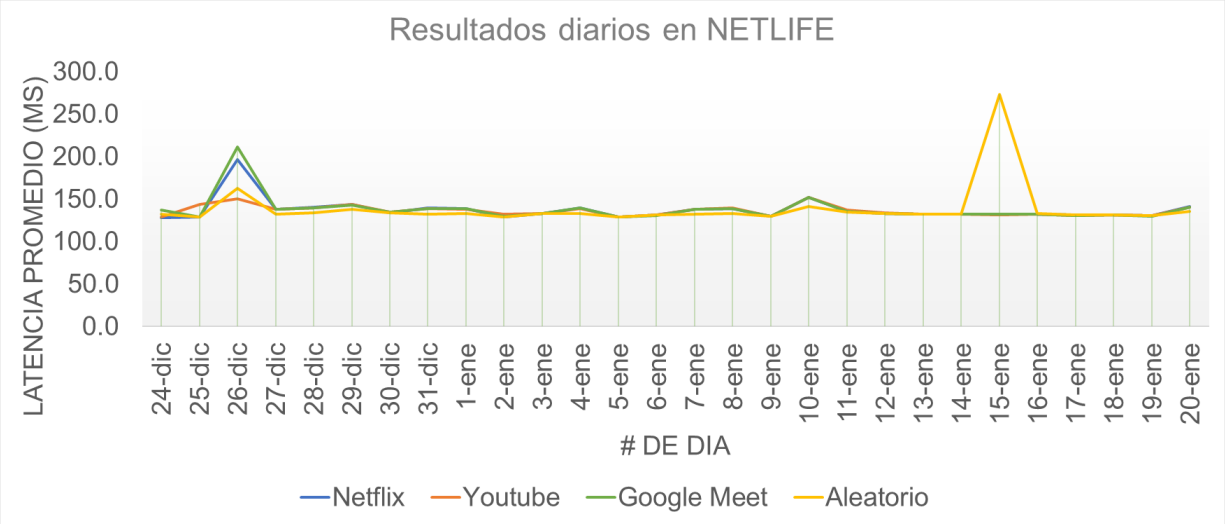
	Latencia promedio (ms)				ΔT entre servicios (ms)					
Día	**Netflix**	**YouTube**	**Google Meet**	**Aleatorio**	**Netflix - YouTube**	**Netflix - G. Meet**	**YouTube - G. Meet**	**Netflix - Aleatorio**	**YouTube - Aleatorio**	**G. Meet - Aleatorio**
24-dic	128.3	128.4	136.7	132.4	0.1	8.5	8.3	4.1	4.0	4.3
25-dic	128.5	143.5	128.5	128.4	15.0	0.0	15.0	0.2	15.2	0.2
26-dic	196.5	150.4	211.0	162.2	46.0	14.5	60.6	34.2	11.8	48.8
27-dic	137.8	137.7	137.6	131.7	0.1	0.2	0.1	6.1	6.0	5.9
28-dic	140.4	139.9	139.5	133.5	0.6	0.9	0.3	6.9	6.3	6.0
29-dic	144.0	143.7	143.1	137.9	0.3	0.9	0.6	6.0	5.8	5.1
30-dic	133.9	134.1	134.2	133.9	0.2	0.3	0.1	0.0	0.2	0.3
31-dic	139.3	138.5	139.0	132.1	0.7	0.2	0.5	7.2	6.4	6.9
1-ene	138.3	138.2	138.6	133.3	0.0	0.3	0.3	5.0	5.0	5.3
2-ene	128.9	132.3	129.2	129.2	3.4	0.3	3.1	0.3	3.1	0.0
3-ene	132.9	132.7	132.8	133.1	0.2	0.1	0.1	0.2	0.4	0.3
4-ene	139.3	139.0	139.3	133.1	0.3	0.0	0.3	6.2	5.9	6.2
5-ene	128.7	128.7	129.1	128.9	0.0	0.4	0.4	0.1	0.1	0.3
6-ene	131.3	131.0	130.7	131.0	0.2	0.6	0.3	0.2	0.0	0.3
7-ene	138.0	137.8	137.6	131.8	0.2	0.4	0.2	6.1	5.9	5.7
8-ene	138.7	139.1	138.7	132.9	0.4	0.1	0.5	5.8	6.2	5.7
9-ene	129.7	129.4	129.4	129.4	0.2	0.3	0.1	0.2	0.0	0.1

Día	Netflix	YouTube	Google Meet	Aleatorio	Netflix - YouTube	Netflix - G. Meet	YouTube - G. Meet	Netflix - Aleatorio	YouTube - Aleatorio	G. Meet - Aleatorio
10-ene	151.7	151.8	151.6	141.4	0.1	0.1	0.2	10.3	10.4	10.2
11-ene	135.1	137.3	135.6	134.9	2.2	0.5	1.6	0.2	2.4	0.7
12-ene	132.9	133.3	133.1	132.9	0.4	0.2	0.2	0.0	0.4	0.2
13-ene	132.0	132.2	131.9	132.3	0.2	0.1	0.3	0.3	0.1	0.4
14-ene	132.2	132.0	132.0	132.0	0.2	0.3	0.0	0.2	0.0	0.1
15-ene	132.2	131.5	132.0	272.9	0.8	0.2	0.5	140.6	141.4	140.9
16-ene	132.4	132.1	132.4	132.9	0.3	0.0	0.3	0.4	0.7	0.5
17-ene	130.9	130.3	130.4	131.4	0.6	0.4	0.1	0.5	1.1	0.9
18-ene	131.6	131.0	131.0	131.1	0.6	0.6	0.1	0.5	0.2	0.1
19-ene	130.3	130.0	129.8	130.8	0.3	0.6	0.2	0.4	0.8	1.0
20-ene	140.9	140.5	140.4	135.0	0.4	0.5	0.1	5.9	5.5	5.4

Los resultados de latencias por servicios de la tabla 16 se pueden apreciar de manera gráfica en la figura 47.

Figura 47

Latencia diaria promedio por servicio en NETLIFE

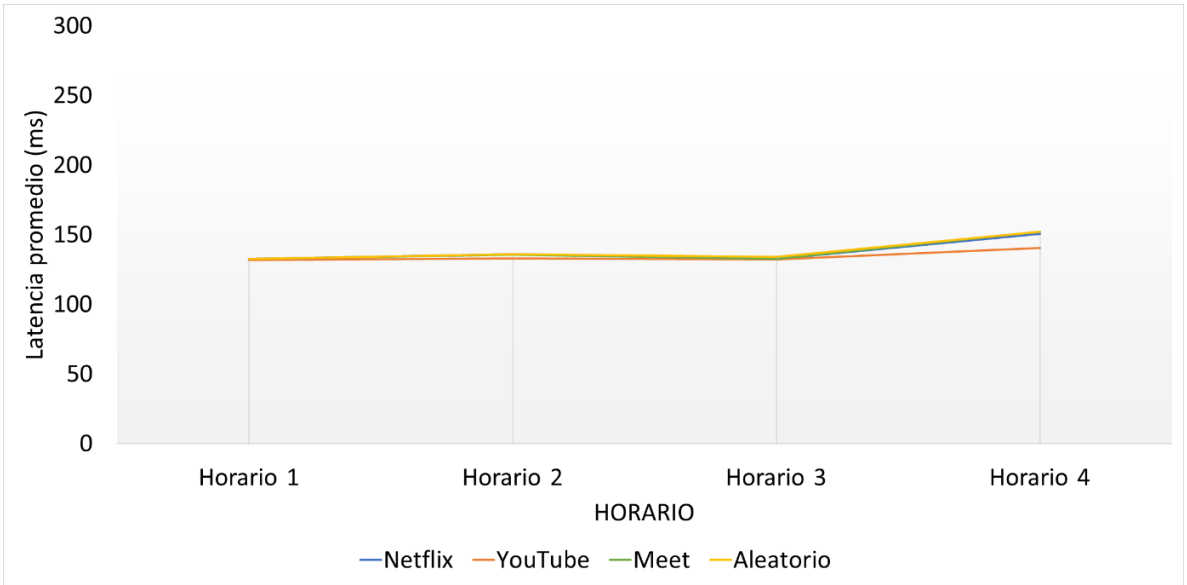


Se puede observar en la figura 47 que la latencia promedio de los servicios presenta una tendencia similar en la mayoría de días, exceptuando los días: 26-dic, donde se tiene una diferencia de latencia entre los servicios de Netflix y Google Meet (siendo estos los de mayor valor), y 15-ene, que presenta un comportamiento inusual, se puede apreciar un aumento significativo en la latencia del tráfico aleatorio, siendo más del doble del resto de servicios, y de acuerdo a la regla del umbral que se está considerando, podría existir DT.

Sin embargo, ya que estos valores inusuales no son repetitivos ni siguen un patrón en el transcurso de los días de pruebas, únicamente se resaltan en la tabla 8 dos ocasiones, por lo tanto, no podría afirmarse la existencia de DT. En este caso se puede atribuir los problemas de diferencia de latencia de estos servicios a la congestión que experimentó la red esos días, y de acuerdo con la figura 48, este aumento se encuentra en el horario 4 (19:00 – 21:00), que usualmente es el horario de mayor número de usuarios conectados a Internet según la figura 37.

Figura 48

Latencia promedio por horario y servicio (NETLIFE)



En las pruebas también se realizó la configuración del campo DSCP, donde se utilizaron dos valores: el primero es BE o ‘best effort’ y el segundo es EF o ‘expedited forwarding’; esto con el objetivo de comparar si los paquetes o el tráfico inyectado poseen un trato diferente al solicitar prioridad baja o alta.

En la figura 49, se observa cada uno de los servicios probados con los valores de DSCP mencionados anteriormente, en BE son los que presentan las líneas entrecortadas en cambio los de EF son los de líneas continuas. Es claro percibir que los valores de latencia en BE son menores en la mayor parte de los casos que en EF, pese a que estos últimos tienen el indicador de mayor prioridad.

Esto puede deberse a una sobrecarga de la red y el ISP podría estar utilizando técnicas de gestión de tráfico para evitar la congestión y garantizar que los paquetes más importantes, como los de control o de señalización, sean entregados con la menor latencia posible. En este caso, es posible que los paquetes con cabecera DSCP EF sean menos frecuentes frente a BE y por esto se esté experimentando mayor retraso.

Figura 49

Comparativa de servicios con DSCP 'BE' vs 'EF'

Los resultados obtenidos en pérdida de paquetes se observan en la tabla 17.

Tabla 17

Pérdida de paquetes en NETLIFE

Día	26-dic	4-ene	7-ene	8-ene	10-ene
Paquetes perdidos prom	0.25	0.25	0.25	0.25	0.25
% pérdida de paquetes	0.1	0.1	0.1	0.1	0.1

En la tabla 18 se puede notar que el promedio de pérdida es de 0.25, y esto se dio únicamente en 5 de los 28 días que duraron las pruebas. Lo que representa el 0.1% de tasa de pérdida en esos días, y de acuerdo a la regla del umbral de detección la pérdida de paquetes por día, y de acuerdo a la regla del umbral de detección no se debe superar el 4.6%; por lo que se puede inferir que, por pérdida de paquetes este ISP no está realizando prácticas discriminatorias o de DT.

ISP Fijo - CNT

Los resultados se obtuvieron siguiendo las mismas consideraciones del caso anterior. En la tabla 18 se presentan los valores de las latencias promedio por día y por servicio, además de la diferencia de latencia entre servicios y, tal como se puede apreciar, no existen valores resaltados por lo que es evidente que este ISP presenta una latencia promedio dentro del rango de la regla del umbral de detección.

Tabla 18

Latencia promedio por servicio y diferencia de servicios (CNT fijo)

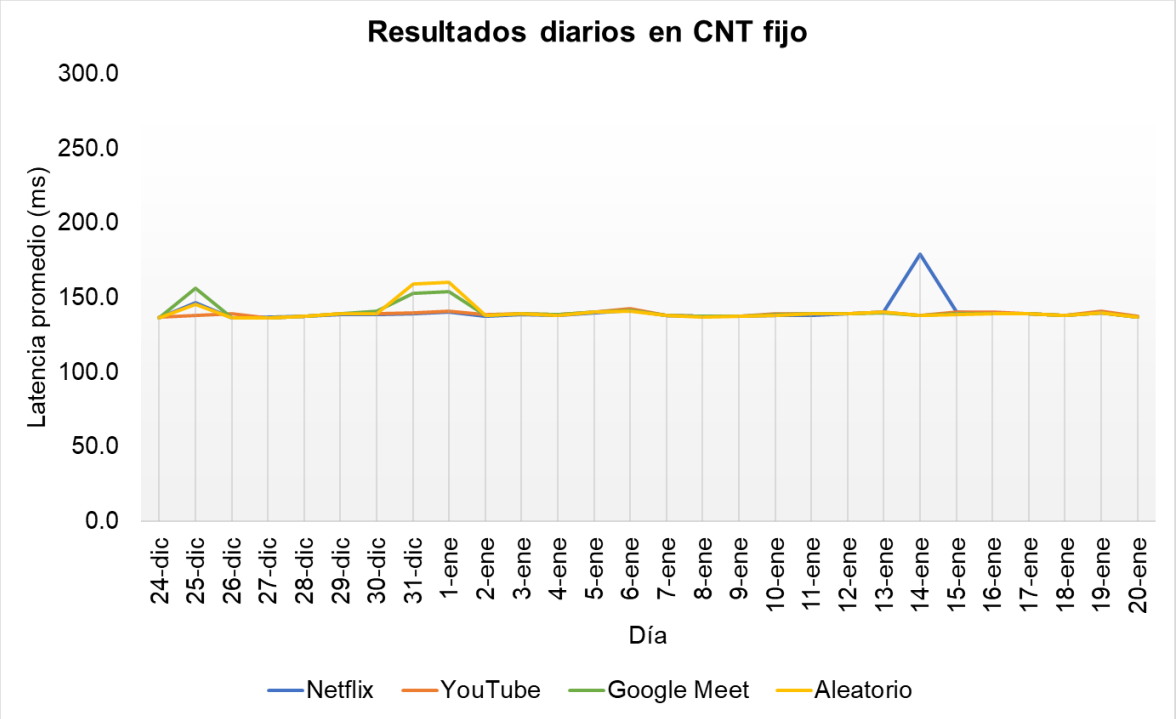
	Latencia promedio (ms)				ΔT entre servicios (ms)					
Día	**Netflix**	**YouTube**	**Google Meet**	**Aleatorio**	**Netflix - YouTube**	**Netflix - G. Meet**	**YouTube - G. Meet**	**Netflix - Aleatorio**	**YouTube - Aleatorio**	**G. Meet - Aleatorio**
24-dic	136.4	136.5	136.4	136.2	0.1	0.0	0.1	0.2	0.3	0.2
25-dic	146.6	137.8	156.0	145.1	8.8	9.4	18.2	1.5	7.4	10.8
26-dic	136.3	138.7	136.3	136.2	2.4	0.0	2.5	0.1	2.5	0.1
27-dic	136.5	136.1	136.2	136.2	0.3	0.3	0.0	0.3	0.1	0.0
28-dic	137.3	137.2	137.3	137.3	0.1	0.0	0.1	0.0	0.1	0.0
29-dic	138.6	138.8	138.8	138.9	0.2	0.2	0.0	0.3	0.1	0.0
30-dic	138.7	139.0	140.5	138.9	0.3	1.9	1.6	0.3	0.1	1.6
31-dic	138.0	138.1	138.1	138.0	0.1	0.1	0.0	0.0	0.1	0.1
1-ene	137.8	137.7	137.8	137.6	0.0	0.0	0.1	0.1	0.1	0.2
2-ene	137.5	138.6	137.6	137.7	1.1	0.1	1.0	0.1	1.0	0.1
3-ene	138.6	139.2	139.2	138.7	0.5	0.5	0.0	0.1	0.4	0.4

Día	Netflix	YouTube	Google Meet	Aleatorio	Netflix - YouTube	Netflix - G. Meet	YouTube - G. Meet	Netflix - Aleatorio	YouTube - Aleatorio	G. Meet - Aleatorio
4-ene	138.0	138.2	138.3	138.1	0.2	0.3	0.1	0.0	0.1	0.2
5-ene	139.8	140.1	140.1	139.9	0.3	0.4	0.1	0.1	0.2	0.3
6-ene	141.2	142.3	141.4	140.8	1.1	0.2	0.9	0.4	1.5	0.6
7-ene	137.8	137.9	137.9	137.9	0.1	0.1	0.0	0.2	0.1	0.0
8-ene	137.3	137.0	137.4	137.0	0.3	0.1	0.4	0.3	0.1	0.4
9-ene	137.3	137.2	137.3	137.0	0.1	0.0	0.1	0.3	0.1	0.3
10-ene	138.1	139.2	138.4	137.9	1.2	0.3	0.8	0.2	1.4	0.5
11-ene	178.7	138.9	139.1	138.8	39.8	39.6	0.2	39.9	0.1	0.3
12-ene	138.8	138.8	139.0	138.8	0.0	0.2	0.2	0.0	0.0	0.2
13-ene	139.9	140.0	139.7	139.9	0.1	0.2	0.2	0.0	0.1	0.1
14-ene	139.3	139.3	152.6	158.8	0.1	13.4	13.3	19.5	19.4	6.1
15-ene	140.2	139.9	139.2	138.7	0.2	1.0	0.8	1.5	1.2	0.5
16-ene	139.1	140.3	139.0	138.8	1.2	0.1	1.3	0.3	1.5	0.2
17-ene	138.9	138.9	138.9	139.0	0.1	0.0	0.1	0.1	0.2	0.1
18-ene	140.0	140.5	153.8	159.9	0.5	13.8	13.3	19.9	19.4	6.1
19-ene	139.6	140.8	139.6	139.6	1.3	0.0	1.2	0.1	1.2	0.1
20-ene	136.9	137.0	137.0	136.9	0.2	0.1	0.0	0.1	0.1	0.0

Representando los datos de la tabla de manera gráfica se obtiene la figura 50, y se puede apreciar que existe un comportamiento en la latencia similar en la mayoría de días, salvo los casos de diciembre (25 y 31) y enero (1 y 11), donde claramente existe una diferencia de latencia entre servicios.

Figura 50

Latencia diaria promedio por servicio en CNT

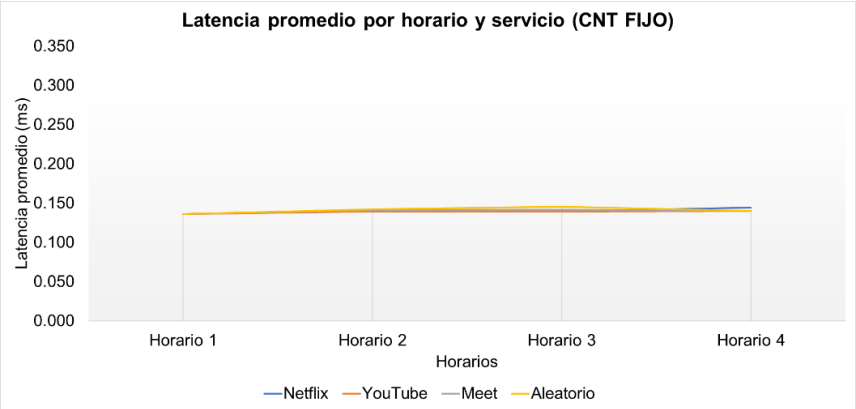


Pese a esta diferencia, los valores no exceden los 55ms de base del umbral de detección, por lo que no puede afirmarse una DT, la diferencia de latencia en los picos de la figura 50 pueden deberse a diferentes causas, como el de los días 25-dic, 31-dic y 1-ene que puede ser debido a la congestión que sufre usualmente de la red, por alta demanda de tráfico, múltiples dispositivos conectados y aumento en el consumo de medios digitales, congestión principalmente ocasionada en los feriados y fines de semana, como es el caso del 14-ene.

Se consideró la latencia promedio entre los diferentes horarios para buscar más patrones de diferenciación, donde se pudo observar (figura 51) que CNT fijo no muestra una variación significativa en sus valores de latencia entre servicios, sus respuestas siguen la misma tendencia en todos los horarios.

Figura 51

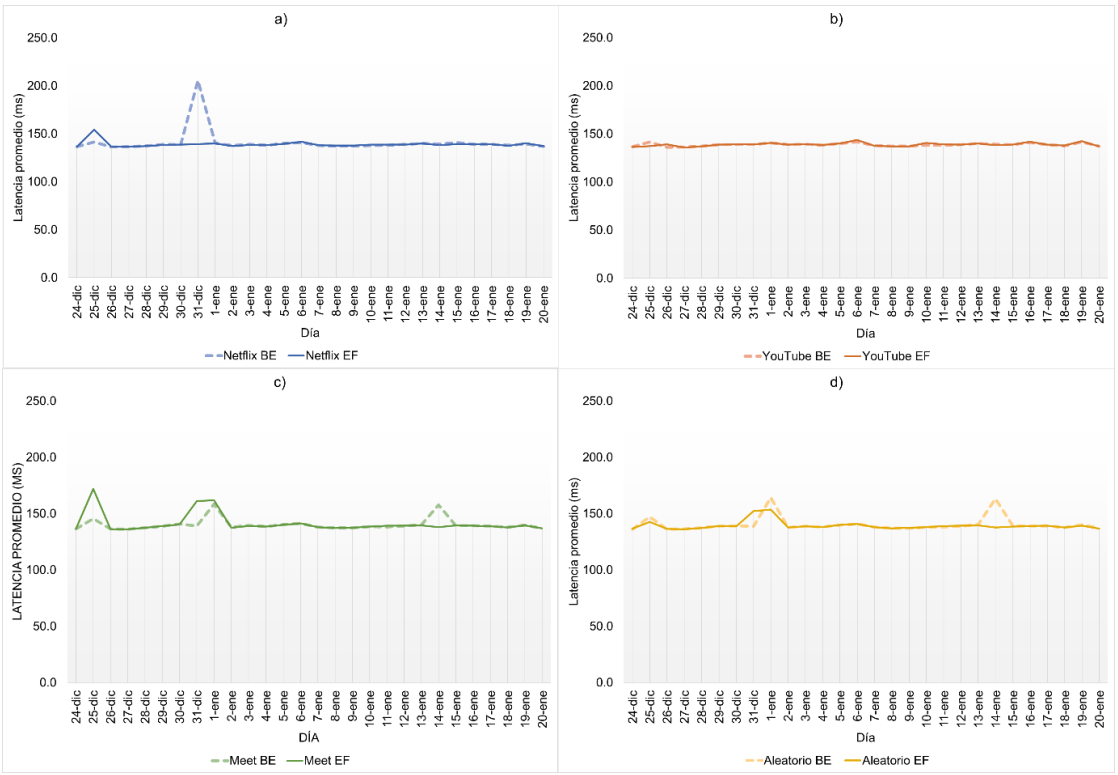
Comparación de latencias entre horarios y servicios



En cuanto a los resultados al cambiar las cabeceras DSCP, se puede observar (figura 52) que la mayor parte del tiempo no existe una diferencia entre BE y EF, y al enfocarse en los picos de las gráficas, en ocasiones el tráfico con DSCP BE es más lento (mayor latencia) que el tráfico con DSCP EF y viceversa, por lo que este parámetro no influye en este ISP para determinar prácticas de discriminación de tráfico.

Figura 52

Comparativa de servicios con DSCP 'BE' vs 'EF'



En cuanto a pérdida de paquetes para este ISP, no se obtuvo ningún caso en el transcurso de las pruebas, por lo que se puede decir que existió una tasa de paquetes recibidos del 100%.

Después de observar los resultados y los análisis de los ISP’s fijos se puede considerar que no existe una evidencia empírica de que estos realicen prácticas de DT. Un motivo de esto puede ser que en los planes que estos proveedores ofertan, se tienen las mismas altas velocidades de enlace tanto para subida como para bajada (uplink y downlink), esto posiblemente debido a que la capacidad de su red es mayor y no necesitan restringir el tráfico de ciertos servicios para gestionar el ancho de banda, es decir no poseen altos incentivos para realizar prácticas de DT.

ISP Móvil - Claro

Los datos presentados en la tabla 20, reflejan la latencia promedio por servicio y por día, de las pruebas realizadas para este ISP, además de la diferencia de latencias entre servicios, resaltando los valores que excedan los 55ms de color amarillo y de 100ms de color naranja, para conocer los valores que sobrepasan de la regla del umbral de detección que se está considerando para determinar la DT entre servicios.

Tabla 19

Latencia promedio por servicio y diferencia de servicios (CLARO)

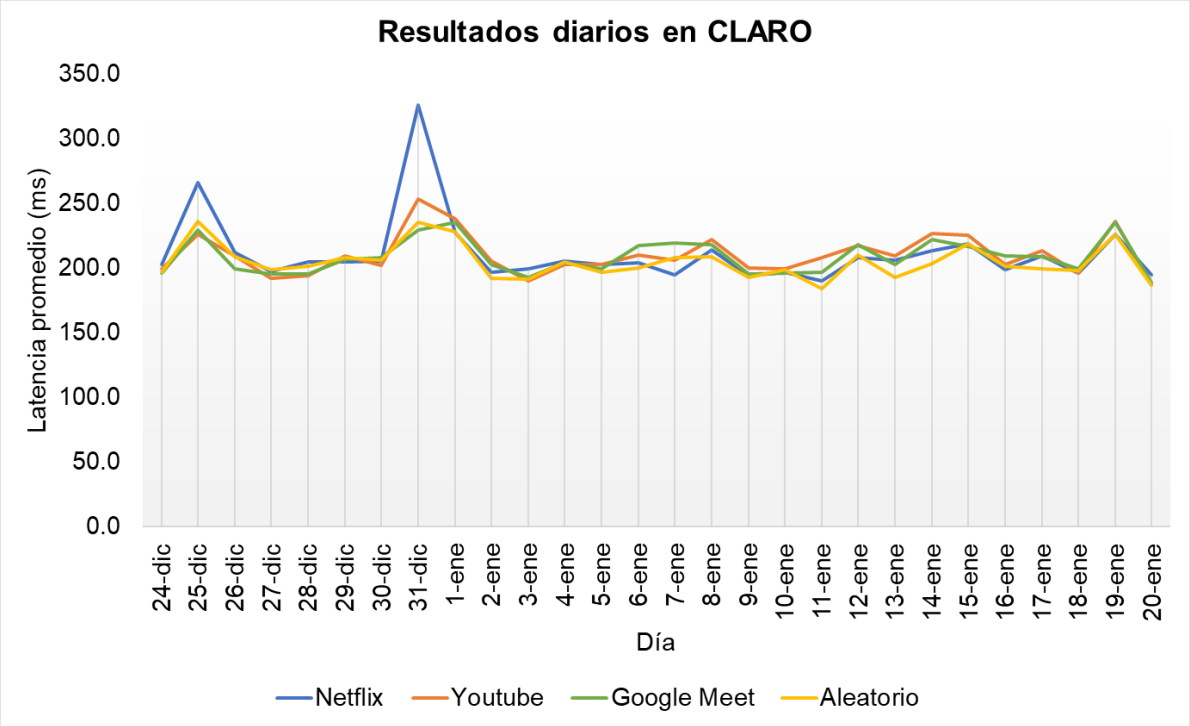
	Latencia promedio (ms)				ΔT entre servicios (ms)					
Día	**Netflix**	**YouTube**	**Google Meet**	**Aleatorio**	**Netflix - YouTube**	**Netflix - G. Meet**	**YouTube - G. Meet**	**Netflix - Aleatorio**	**YouTube - Aleatorio**	**G. Meet - Aleatorio**
24-dic	202.4	199.4	195.8	196.8	3.0	6.6	3.6	5.6	2.5	1.0
25-dic	265.8	225.8	229.1	236.2	39.9	36.7	3.3	29.6	10.4	7.1
26-dic	212.0	209.3	199.0	208.9	2.7	12.9	10.3	3.1	0.4	9.9
27-dic	197.5	192.1	195.3	198.7	5.4	2.3	3.2	1.1	6.5	3.4
28-dic	204.3	194.0	195.0	201.0	10.3	9.3	1.0	3.3	7.0	6.0
29-dic	204.6	209.3	206.5	208.0	4.7	1.9	2.8	3.4	1.3	1.5
30-dic	205.2	201.9	207.6	206.3	3.3	2.4	5.7	1.1	4.4	1.3
31-dic	194.8	187.4	188.3	186.4	7.5	6.5	1.0	8.4	0.9	1.9
1-ene	195.8	195.8	199.5	198.1	0.0	3.7	3.7	2.3	2.3	1.4
2-ene	190.2	208.2	196.4	184.0	18.0	6.2	11.9	6.2	24.2	12.3
3-ene	199.0	189.7	192.9	191.3	9.3	6.0	3.3	7.6	1.7	1.6
4-ene	205.2	202.7	203.7	204.9	2.5	1.6	0.9	0.3	2.2	1.2
5-ene	214.1	222.3	218.0	208.4	8.1	3.8	4.3	5.8	13.9	9.6
6-ene	204.3	209.9	217.4	199.9	5.7	13.1	7.5	4.4	10.1	17.5
7-ene	194.3	206.2	219.3	208.2	11.9	25.0	13.2	13.9	2.0	11.2
8-ene	202.3	202.5	199.1	196.6	0.2	3.2	3.4	5.7	5.9	2.5

Día	Netflix	YouTube	Google Meet	Aleatorio	Netflix - YouTube	Netflix - G. Meet	YouTube - G. Meet	Netflix - Aleatorio	YouTube - Aleatorio	G. Meet - Aleatorio
9-ene	193.8	199.7	195.6	192.6	5.8	1.8	4.0	1.2	7.0	3.0
10-ene	196.4	199.4	196.2	198.6	3.0	0.3	3.2	2.1	0.9	2.4
11-ene	218.3	225.1	216.7	218.4	6.8	1.7	8.5	0.1	6.7	1.8
12-ene	207.6	217.4	217.7	209.9	9.7	10.0	0.3	2.3	7.5	7.8
13-ene	213.4	226.5	222.1	203.5	13.0	8.7	4.3	10.0	23.0	18.7
14-ene	205.7	209.4	202.5	192.4	3.7	3.2	6.9	13.3	17.0	10.1
15-ene	196.5	205.1	202.8	192.0	8.6	6.3	2.2	4.4	13.0	10.8
16-ene	198.3	202.4	209.5	201.2	4.1	11.1	7.1	2.8	1.2	8.3
17-ene	209.6	213.1	208.4	199.4	3.5	1.2	4.7	10.2	13.7	9.0
18-ene	227.6	238.0	235.5	227.7	10.4	8.0	2.4	0.1	10.3	7.9
19-ene	226.1	235.7	235.6	226.2	9.7	9.6	0.1	0.2	9.5	9.4
20-ene	326.1	253.2	229.4	235.4	72.9	96.8	23.8	90.8	17.9	6.0

Se representa de manera grafica la tabla 20 en la figura 55, donde se puede apreciar el comportamiento de la latencia promedio en el transcurso de las 4 semanas.

Figura 53

Latencia promedio por servicio y por día del ISP CLARO



La figura 53 junto con la tabla 20 ofrecen información relevante y se presenta a continuación:

- Los valores de latencia promedio en comparación con los ISP's fijo son mayores, y más dispersos, no siguen una tendencia.
- Solo en un día se excede la regla del umbral de detección y es el 31 de diciembre, pese a esto otro día posee un comportamiento similar pese a no exceder dicho umbral y es el 25 de diciembre.
- Los otros picos de latencia se ubicaron en los fines de semana, en los días 7-8 de enero y 14-15 de enero.
- Existe un pico el día 19 de enero, día inusual puesto que es entre semana, pero su alza de latencia pudo también ocasionarse por una congestión en la red.

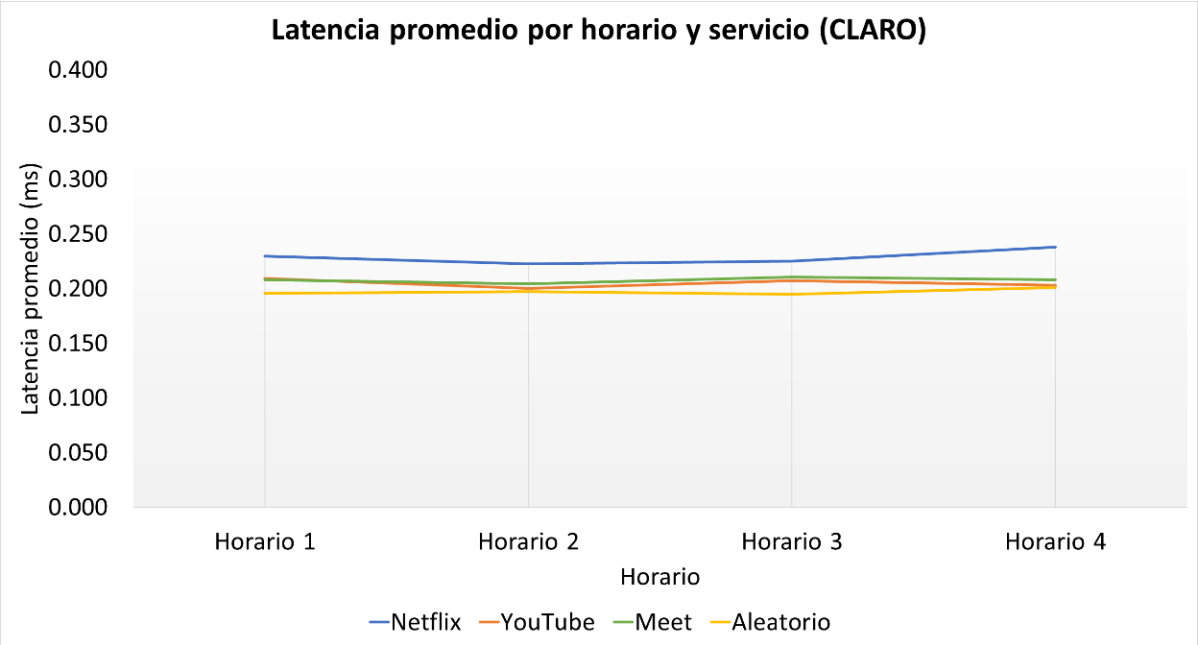
De los resultados mencionados anteriormente se puede deducir que, cuando existe una alta demanda en el tráfico de red, el servicio de Netflix es el más afectado, ya que es

retrasado mayormente respecto a los demás. Aun considerando este punto y al no existir un patrón de retrasos de este servicio en los fines de semana no se puede afirmar la existencia de discriminación de tráfico.

Las altas latencias de este servicio (particularmente en los días mencionados) pueden deberse a diferentes condiciones como: QoS (calidad de servicio, ya que la red puede estar configurada para asignar prioridades a diferentes tipos de tráfico), capacidad de la red (si la red se encuentra congestionada), capacidad del servidor de Netflix (si el servidor que proporciona el Netflix tiene una carga alta), la calidad de la conexión (si la conexión del usuario no es estable o tiene una baja velocidad) y ubicación geográfica del servidor de Netflix.

Figura 54

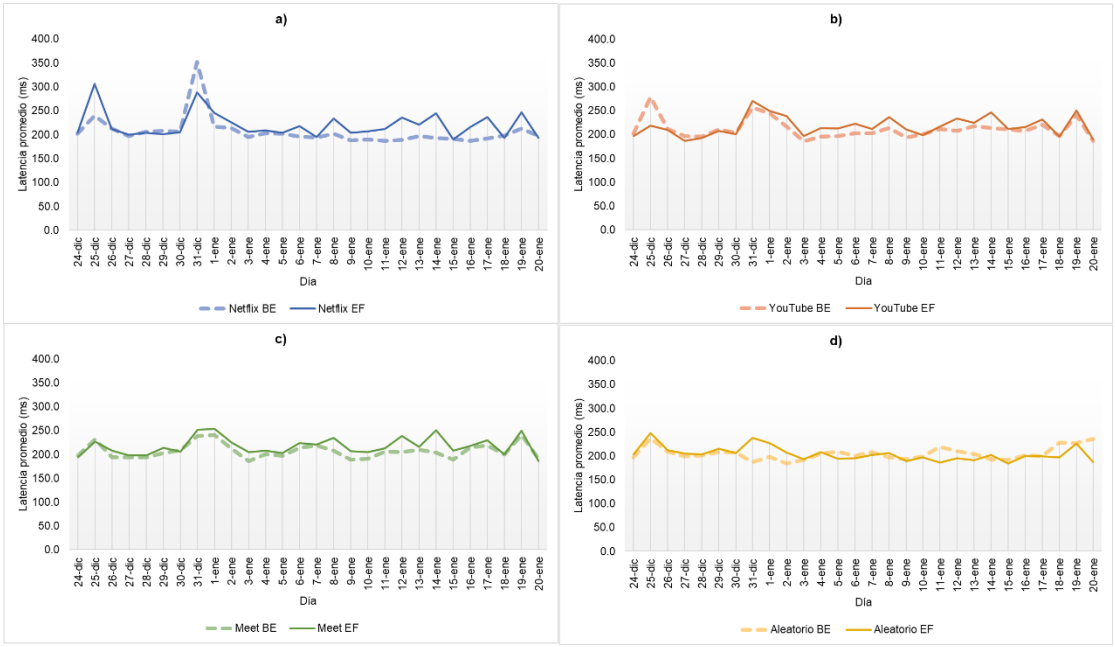
Comparación de latencias entre horarios y servicios



Se puede observar (figura 54) que la diferencia de latencias por horario no es significativa, pues existe únicamente un aumento en Netflix, pero los valores son menores a 30ms por lo que está en el margen del umbral de detección, por ende, no hay evidencia de discriminación de tráfico.

Figura 55

Comparativa de servicios con DSCP 'BE' vs 'EF'



Los resultados al considerar los valores del DSCP tanto en BE como en EF, vistos en la figura 56 y, como se observa, no poseen un comportamiento de diferenciación específica uno del otro, ya que en ocasiones la latencia de los servicios en BE es mayor que en EF, y en ocasiones ocurre lo contrario. Es por esto que el campo DSCP en las cabeceras no demuestra una priorización o entorpecimiento en el tratamiento del tráfico.

El último parámetro considerado para evaluar las prácticas de diferenciación en este ISP fue la pérdida de paquetes, después de realizadas todas las pruebas se obtuvo una pérdida únicamente en el segundo día, misma que se traduce en un promedio de 1.75 o 0.7% de paquetes perdidos (en ese día particularmente) y, considerando el valor umbral de 4.6%, se puede afirmar que no existió discriminación de tráfico acorde a este parámetro.

Tabla 20

Pérdida de paquetes en CLARO

Día	25-dic
Paquetes perdidos/día	1.75
%pérdida paquetes	0.7

ISP Móvil - Movistar

Los resultados de latencia promedio por servicio y la diferencia entre estos se muestra en la tabla 21.

Tabla 21

Latencia promedio por servicio y diferencia de servicios (MOVISTAR)

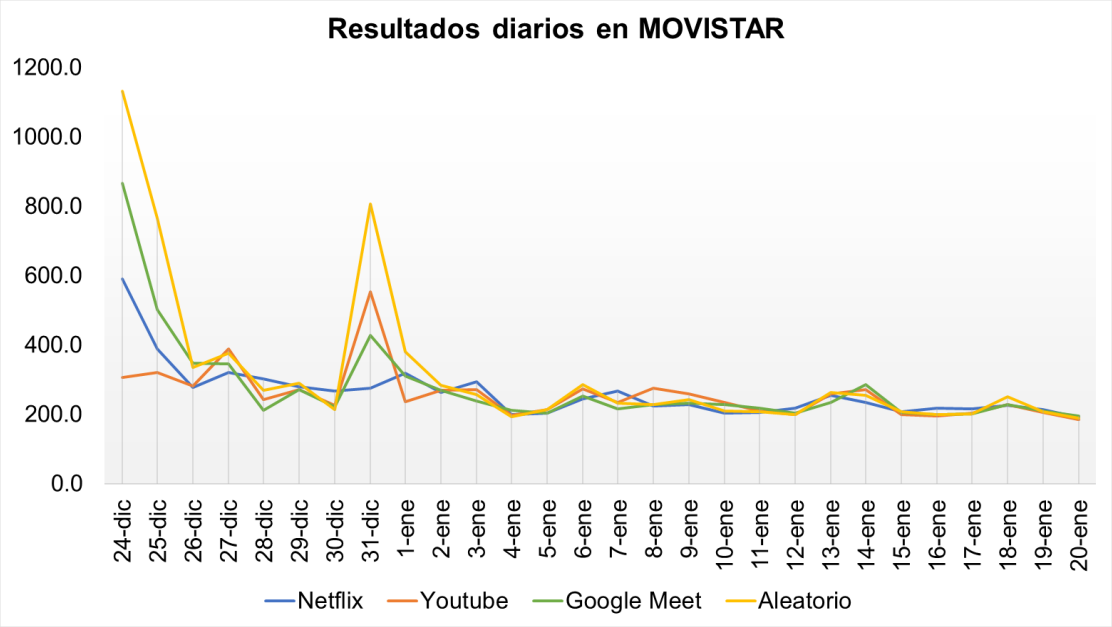
	Latencia promedio (ms)				ΔT entre servicios (ms)					
Día	**Netflix**	**YouTube**	**Google Meet**	**Aleatorio**	**Netflix - YouTube**	**Netflix - G. Meet**	**YouTube - G. Meet**	**Netflix - Aleatorio**	**YouTube - Aleatorio**	**G. Meet - Aleatorio**
24-dic	276.6	281.0	345.9	334.4	4.4	69.2	64.9	57.8	53.4	11.4
25-dic	388.4	320.0	501.7	764.6	68.3	113.4	181.7	376.2	444.6	262.9
26-dic	589.7	305.1	866.1	1131.2	284.5	276.4	560.9	541.6	826.1	265.1
27-dic	320.2	388.9	345.1	375.8	68.6	24.9	43.8	55.5	13.1	30.6
28-dic	302.1	242.4	211.1	269.5	59.7	91.1	31.4	32.7	27.1	58.4
29-dic	279.7	270.7	271.6	290.3	9.0	8.1	1.0	10.6	19.6	18.6
30-dic	266.2	225.2	220.3	213.9	41.0	45.9	4.9	52.3	11.3	6.4
31-dic	224.4	274.8	228.4	228.1	50.4	4.0	46.4	3.7	46.7	0.3
1-ene	262.3	268.4	268.8	282.9	6.1	6.6	0.4	20.7	14.5	14.1
2-ene	317.6	235.5	309.1	379.3	82.1	8.5	73.6	61.7	143.8	70.2
3-ene	294.4	271.3	237.4	256.4	23.1	57.0	33.9	38.1	15.0	19.0
4-ene	197.9	195.7	210.6	193.5	2.1	12.7	14.8	4.3	2.2	17.0
5-ene	202.1	213.4	203.0	212.1	11.3	0.8	10.4	10.0	1.3	9.2

Día	Netflix	YouTube	Google Meet	Aleatorio	Netflix - YouTube	Netflix - G. Meet	YouTube - G. Meet	Netflix - Aleatorio	YouTube - Aleatorio	G. Meet - Aleatorio
6-ene	243.7	273.4	253.1	285.2	29.7	9.3	20.4	41.4	11.8	32.1
7-ene	266.0	233.5	214.4	232.1	32.4	51.6	19.2	33.8	1.4	17.8
8-ene	275.8	553.8	427.7	805.3	278.0	151.9	126.1	529.5	251.5	377.6
9-ene	227.6	258.0	230.9	241.1	30.4	3.3	27.2	13.5	16.9	10.3
10-ene	202.7	233.0	226.9	208.3	30.3	24.2	6.1	5.6	24.7	18.5
11-ene	204.6	208.5	216.3	207.0	4.0	11.7	7.8	2.4	1.5	9.3
12-ene	216.7	197.8	202.5	197.8	18.9	14.2	4.7	18.9	0.0	4.7
13-ene	253.5	258.4	234.0	262.1	4.9	19.5	24.4	8.6	3.7	28.1
14-ene	233.7	270.3	285.1	254.7	36.6	51.5	14.8	21.0	15.6	30.5
15-ene	207.4	198.6	204.8	207.9	8.8	2.6	6.2	0.5	9.3	3.1
16-ene	216.8	194.8	199.5	199.5	22.0	17.3	4.7	17.3	4.7	0.0
17-ene	215.0	203.5	200.8	200.8	11.5	14.2	2.8	14.2	2.7	0.0
18-ene	224.8	226.8	226.7	250.8	2.0	1.9	0.0	26.0	24.1	24.1
19-ene	212.9	205.3	209.1	207.9	7.6	3.8	3.8	5.0	2.5	1.3
20-ene	189.8	185.2	195.5	188.9	4.7	5.7	10.4	0.9	3.7	6.6

Se puede observar en la tabla que existen diferencias de valores que exceden el umbral de 55ms y otros que exceden en más de 100ms, se encuentran resaltados de color amarillo y naranja respectivamente. Se representa estos datos de manera gráfica en la figura 56, a continuación:

Figura 56

Latencia promedio por servicio y por día del ISP MOVISTAR

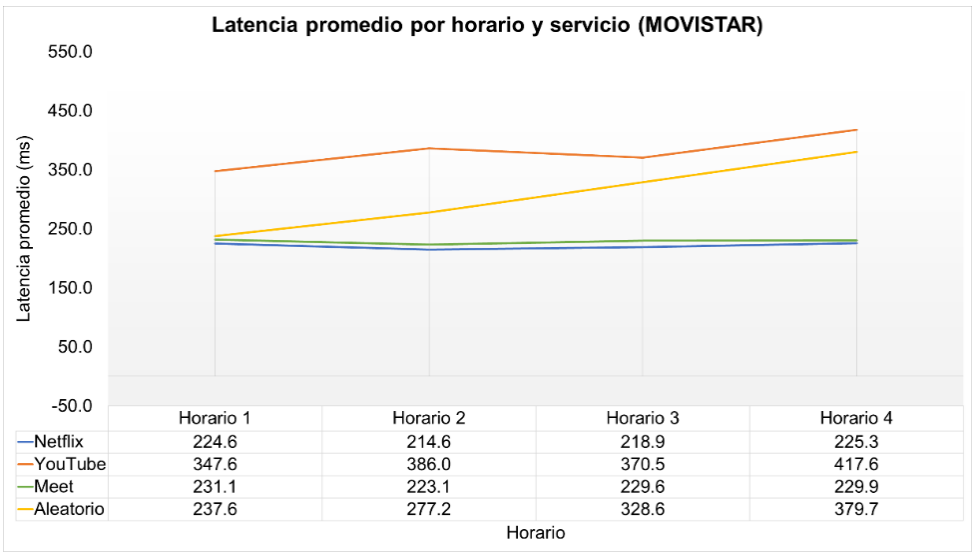


Tal como se puede observar, la tendencia de latencia promedio en la mayoría de días resulta similar, en múltiples días se encuentra que el umbral de detección fue superado, principalmente en los días 24, 25 y 31 de diciembre.

Por ende, al tener varios días, se procede a verificar si los valores de latencia también superan el umbral de detección al hacer el análisis de acuerdo a los horarios.

Figura 57

Comparación de latencias entre horarios y servicios.



Tal y como se observa en la figura 57, existen diferencias altas en el promedio de la latencia por horario, siendo YouTube el servicio de mayor latencia en todos los casos, su latencia excede en más de 55ms frente al resto de servicios, a excepción del aleatorio en el cuarto horario, mismo que, a partir del tercer horario comienza a supera el umbral, en relación a Netflix y Google Meet.

En cuanto a la pérdida de paquetes en este ISP se obtuvo la tabla 22:

Tabla 22

Pérdida de paquetes por día en MOVISTAR

Día	24-dic	25-dic	26-dic	27-dic	28-dic	31-dic	1-ene	3-ene	7-ene	14-ene	16-ene
PP	25	16.75	1.5	0.75	0.25	20	8.5	1.25	2.25	4.75	0.75
%PP	10	6.7	0.6	0.3	0.1	8	3.4	0.8	0.9	1.9	0.3

Se pueden observar resaltados los valores que exceden el porcentaje establecido por la regla del umbral de detección en los días 24-dic, 25-dic, y 31-dic, ya que esta admite una tasa máxima en la pérdida de paquetes del 4.6%,

Tras analizar todas las pruebas y evidencias y detectar valores que superan el umbral de detección, se puede concluir que la latencia elevada en este ISP no se debe a congestión de red, ya que se observa en días de bajo tráfico y se ha comparado mediante un promedio horario en todo el mes. Esto sugiere la posible existencia de una diferenciación y discriminación de tráfico por parte del ISP, que se dirige a servicios específicos y que ocurre con mayor frecuencia en dos horarios concretos, H3 y H4.

De igual manera se han realizado pruebas para evaluar la latencia al utilizar DSCP, en estas se observó una reducción en los valores de latencia al solicitar prioridad. Al analizar los resultados obtenidos en la figura 58, se observa que el tráfico aleatorio (d) y de YouTube (b) los valores de latencia con DSCP BE son mayores a los de EF. Sin embargo, en los paquetes de Netflix (a) y Google Meet (c) los valores de latencia en DSCP EF son mayores a los de BE. Estos resultados indican que la latencia puede variar dependiendo del

tipo de tráfico y del servicio utilizado, lo que sugiere una posible implementación de prácticas de discriminación de tráfico por parte de este ISP.

Figura 58

Comparativa de servicios con DSCP 'BE' vs 'EF'

ISP Móvil - CNT

Los resultados del último ISP se reflejan en la tabla 23, en una parte se encuentra la latencia promedio por día según el servicio, y en la otra parte la diferencia de latencia entre los mismos, resaltando los valores que excedan la regla del umbral de detección, de color amarillo los que exceden los 55ms y de color naranja los que exceden los 100ms.

Tabla 23

Latencia promedio por servicio y diferencia de servicios (CNT móvil)

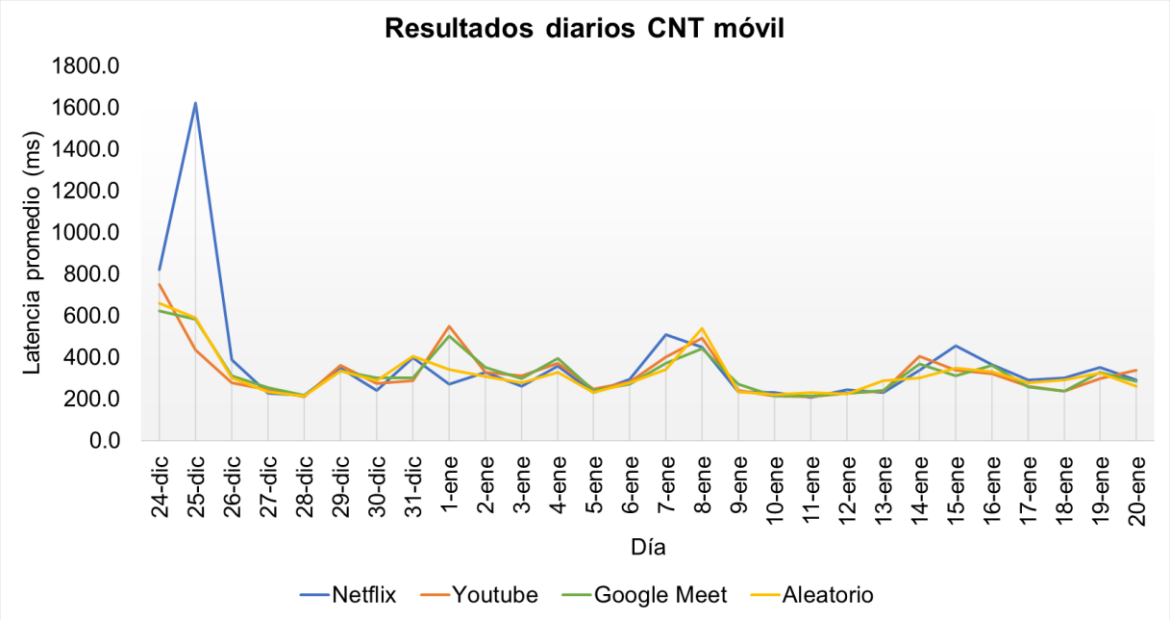
	Latencia promedio				ΔT entre servicios					
Día	**Netflix**	**YouTube**	**Google Meet**	**Aleatorio**	**Netflix-YouTube**	**N-GM**	**Y-GM**	**N-A**	**Y-A**	**GM-A**
24-dic	820.5	749.0	621.8	657.9	71.4	198.7	127.3	162.5	91.1	36.2
25-dic	1622.8	433.9	580.9	590.2	1188.9	1041.9	147.0	1032.6	156.3	9.3
26-dic	386.7	276.7	312.0	299.2	110.0	74.8	35.3	87.5	22.5	12.7
27-dic	225.8	244.2	253.4	232.1	18.4	27.6	9.2	6.3	12.1	21.3
28-dic	218.1	211.5	215.5	213.2	6.6	2.6	4.0	4.8	1.8	2.3
29-dic	347.4	359.3	333.0	335.8	11.9	14.4	26.3	11.6	23.5	2.8
30-dic	241.5	273.7	299.3	287.7	32.2	57.8	25.6	46.2	14.0	11.7
31-dic	396.7	287.9	299.0	403.6	108.7	97.6	11.1	6.9	115.6	104.5
1-ene	270.2	547.4	503.1	341.6	277.2	233.0	44.2	71.4	205.8	161.5
2-ene	326.0	327.9	350.3	307.4	1.9	24.3	22.4	18.7	20.5	42.9
3-ene	261.7	309.0	296.2	275.7	47.3	34.4	12.9	14.0	33.3	20.4
4-ene	358.9	370.4	393.5	326.9	11.6	34.6	23.1	32.0	43.5	66.6
5-ene	231.4	246.3	239.0	229.0	14.9	7.6	7.3	2.4	17.3	10.0
6-ene	292.6	280.7	269.3	277.8	11.8	23.3	11.5	14.8	2.9	8.6
7-ene	507.7	400.9	369.9	340.9	106.8	137.8	31.0	166.8	60.1	29.1
8-ene	449.2	492.7	441.1	537.5	43.5	8.1	51.6	88.2	44.7	96.4
9-ene	234.4	241.8	272.0	234.8	7.5	37.7	30.2	0.4	7.1	37.3

Día	Netflix	YouTube	Google Meet	Aleatorio	Netflix - YouTube	Netflix - G. Meet	YouTube - G. Meet	Netflix - Aleatorio	YouTube - Aleatorio	G. Meet - Aleatorio	
10-ene	231.4	213.8	214.6	220.5	17.6		16.8	0.9	11.0	6.7	5.8
11-ene	207.4	208.9	214.3	229.6	1.5		6.9	5.4	22.1	20.6	15.3
12-ene	242.3	227.4	225.6	222.1	14.8		16.6	1.8	20.1	5.3	3.5
13-ene	231.1	238.1	241.8	288.9	7.0		10.7	3.7	57.8	50.8	47.1
14-ene	338.6	405.2	367.3	301.9	66.6		28.7	37.9	36.7	103.3	65.4
15-ene	453.2	338.7	310.7	346.2	114.6		142.5	27.9	107.1	7.5	35.5
16-ene	363.5	321.2	361.2	331.4	42.4		2.3	40.0	32.1	10.3	29.7
17-ene	291.0	261.7	258.3	275.8	29.3		32.7	3.4	15.2	14.1	17.5
18-ene	302.1	237.9	236.9	291.4	64.2		65.1	1.0	10.6	53.5	54.5
19-ene	351.1	296.0	326.4	324.3	55.1		24.8	30.3	26.9	28.2	2.1
20-ene	292.1	336.2	283.0	260.4	44.0		9.1	53.2	31.8	75.8	22.6

Se representa de manera gráfica esta tabla en la figura 59.

Figura 59

Latencia promedio por servicio y por día del ISP CNT móvil.



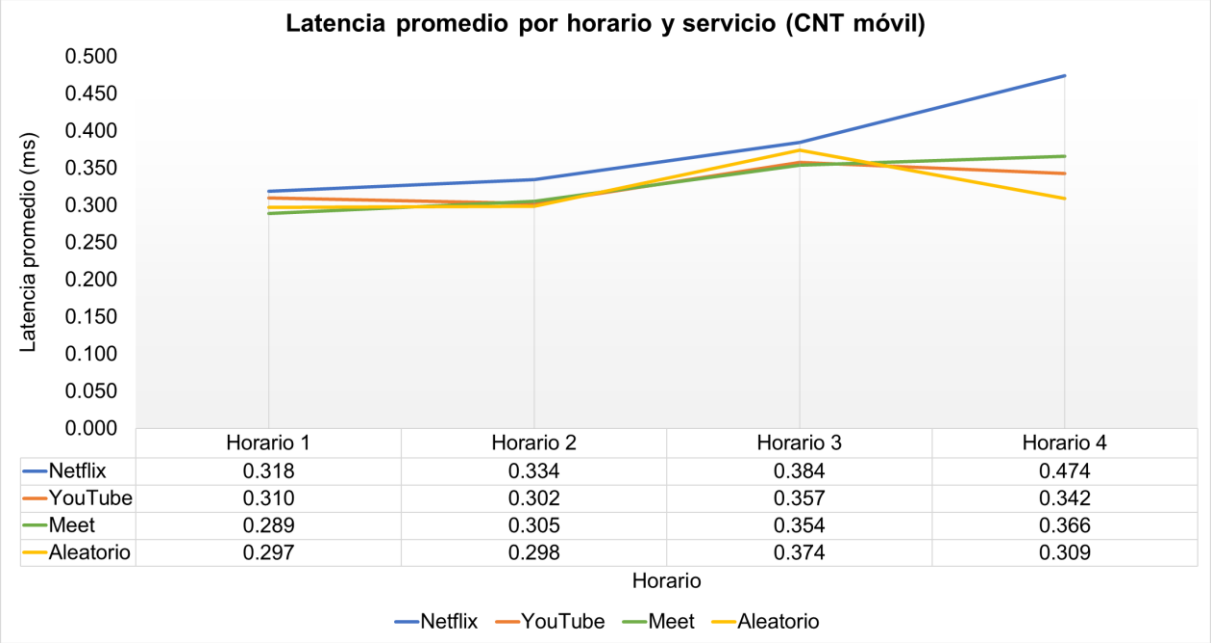
El comportamiento de latencia promedio diaria en este ISP es variable en ciertos días y se ve reflejado en la mayoría de valores picos, principalmente se nota en los días 24, 25 de diciembre, 1, 7, 8 y 15 de enero y de acuerdo con los valores de diferencia de servicios marcados en la tabla, en todos estos la regla del umbral de detección ha sido superada significativamente, lo que sugiere una posible diferenciación de tráfico discriminatorio.

De acuerdo a los valores vistos en la tabla 23, se tiene que, en 14 de los 28 días de pruebas existen valores de latencia que superan el umbral de 55ms de la regla utilizada, pero se debe considerar que los valores más altos corresponden a las fechas 24 y 31 de diciembre, posiblemente debido a la alta congestión que sufre la red en estos días, y los valores del 7, 8, 14 y 15 de enero posiblemente por la congestión en la red los fines de semana, pese a esto existen días de diferencia de latencias altas fuera de estas consideraciones, sugiriendo de igual manera posibles prácticas de DT discriminatoria por parte de este ISP o problemas en la red.

Representada la latencia promedio por horarios se obtiene la figura 60.

Figura 60

Latencia promedio por horario y por servicio del ISP CNT móvil



Se puede analizar que el comportamiento de la latencia en este ISP asciende de acuerdo al horario, es decir que conforme transcurre el día se aumentan los valores de latencia, siendo en las noches (horario 4) el de mayor valor, justificable por ser el de mayor uso por parte de usuario. Se puede denotar también que el umbral de detección se mantiene en el margen hasta el H3, pero en el H4 se observa un tratamiento distinto en el caso de Netflix, pues excede los 55ms en relación con el resto de servicios, sugiriendo una discriminación hacia este servicio.

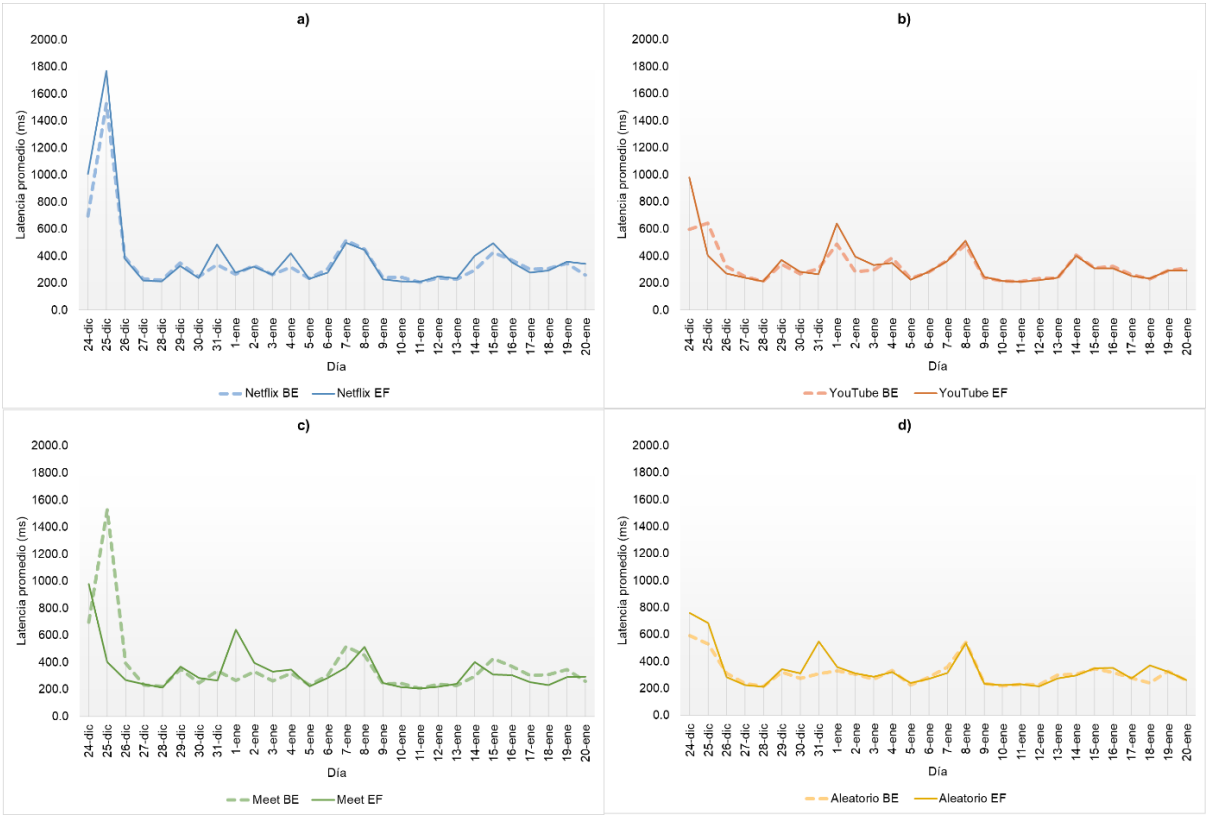
En el caso de considerar los valores BE y EF en la cabecera DSCP de los paquetes de cada uno de los servicios, se obtuvo la figura 61.

Se puede observar claramente que el comportamiento de latencia en el tráfico con solicitud de prioridad (EF) no es tan relevante, ya que en ocasiones el tráfico de los servicios con menor prioridad (BE) presenta menores tiempos de latencia.

Haciendo un énfasis en los días de alta congestión tampoco se puede concluir nada ya que en cada servicio la cabecera DSCP actúa de manera variable, en ocasiones los valores de latencia de EF son menores y en otros mayores.

Figura 61

Comparativa de servicios con DSCP 'BE' vs 'EF'.



El último parámetro considerado en este ISP es el porcentaje de pérdida de paquetes, reflejado en la tabla 24 y de la cual se puede concluir que, pese a existir pérdida de paquetes, no se excede el umbral de detección, por lo que en cuanto a este parámetro no se encuentran indicios de que se encuentran discriminando o bloqueando servicios.

Tabla 24

Pérdida de paquetes en CNT móvil

Días	1	11	15
Paquetes perdidos	0.5	1	2.75
% de pérdida	0.2	0.4	1.1

De acuerdo al comportamiento de la latencia promedio observado en las figuras 59 y 60, existe evidencia de altas posibilidades de prácticas de DT discriminatorio, sobre todo al servicio de Netflix, ya que en promedio presenta latencias sumamente mayores frente todos los otros servicios.

Conclusiones

El Internet es una tecnología de propósito general, una red global que depende de modelos de comunicación de redes, principio de extremo a extremo, una gobernanza efectiva para garantizar el principio de la neutralidad de red y un acceso equitativo y justo para todos los usuarios que la utilizan.

Visto el impacto de las políticas de NR en otros países, es claro que en el Ecuador se requiere de una normativa legal fuerte para proteger a los usuarios y garantizar el acceso libre y justo a Internet, sin importar origen, ubicación o poder adquisitivo. Asegurar que los proveedores de servicios de Internet cumplan con los principios de la neutralidad de la red y operen de manera transparente y responsable, fomenta la innovación en línea y la protección de los derechos de los usuarios de Internet.

Existen múltiples y diversas herramientas que realizan monitoreo activo, pero en el contexto de Neutralidad de la Red, la de mayor aporte para esta investigación fue Wehe, ya que se emuló un comportamiento similar en cuanto al monitoreo e inyección, con la diferencia del parámetro de análisis para determinar la diferenciación de tráfico, en el caso de Wehe se monitorea el throughput y en la herramienta desarrollada se monitorea la latencia.

Al llevar a cabo este estudio se logró el desarrollo, validación e implementación de una herramienta de inyección activa y monitoreo de tráfico de red, enfocada en la búsqueda de diferenciación de tráfico a través de la comparación de latencia y pérdida de paquetes entre diferentes tipos de servicios en las redes de ISP’s fijos y móviles.

Durante el desarrollo de las herramientas de inyección y monitoreo de proveedores de servicios de internet, se utilizaron diversas tecnologías de alta capacidad y versatilidad. Por un lado, para la herramienta de ISP’s fijos se emplearon Python y Scapy, lo que permitió la creación, manipulación, observación y análisis del tráfico generado, acorde a los servicios o aplicaciones requeridos. Por otro lado, en el desarrollo de la herramienta para

ISP’s móviles, se utilizaron principalmente tecnologías integradas en el entorno de desarrollo integrado (IDE) de Android Studio, una plataforma conocida por su alta capacidad y escalabilidad, herramienta ideal para la creación de una solución tan compleja como la desarrollada en este trabajo de investigación.

Es de suma importancia destacar que, en el contexto del desarrollo de herramientas de inyección y monitoreo de tráfico en redes de proveedores de servicios de Internet, resulta fundamental prestar atención a las características, desarrollo y scripts o código del servidor utilizado. Esto se debe a que es necesario asegurarse de que el servidor responda de manera rápida y precisa a los paquetes enviados, lo que permite reducir los valores de error en el punto medio de la medición. De esta manera, se garantiza una medición más confiable y precisa del tráfico en la red, lo que resulta esencial para mejorar su rendimiento y calidad en general.

Se realizó la construcción de paquetes sintéticos, logrando simular el comportamiento de servicios específicos (Netflix, YouTube y Google Meet), en cabeceras como puertos y payloads, lo que permitió evaluar cómo los ISP’s fijos y móviles manejan y priorizan el tráfico de estas aplicaciones, y llevar a cabo pruebas controladas y exhaustivas, para tener una mayor precisión en la detección de posibles casos de discriminación de tráfico.

Con los resultados obtenidos en los ISP’s fijos, se pudo inferir que no existen patrones de diferenciación en la gestión del tráfico ni por día, ni por horario (en latencia y pérdida de paquetes). Esto sugiere que dichos proveedores restringen el tráfico de los servicios de video, sensibles al ancho de banda, posiblemente debido a la amplia capacidad de su red, lo que les permite gestionar su tráfico sin necesidad de aplicar este tipo de prácticas diferenciadas o discriminatorias.

A través del análisis de resultados obtenidos en los ISP’s móviles se pudo concluir que, en Claro no existen las suficientes pruebas o patrones en los valores de latencia que

afirmen una DT, en el caso de CNT existen más evidencias de un tratamiento diferenciado y perjudicial hacia el tráfico de Netflix, y para Movistar se concluyó que sí existe diferenciación de tráfico, ya que es el único servicio que presenta diferencias de latencias por días y por horarios, diferente a los que son justificados por la alta congestión de tráfico de red (feriados y fines de semana), además es el único proveedor de servicio con valores de tasa de pérdida de paquetes que superan la regla del umbral de detección, coincidiendo con la base de datos de Wehe, donde en diferentes países este operador es el de mayor incidencia en prácticas de DT.

Las políticas de neutralidad de red en Ecuador son débiles, en el análisis de los proveedores Netlife, CNT fijo y Claro, se verificó el cumplimiento de las políticas de NR, pese a anomalidades observadas en ciertos días, en los casos de CNT móvil y Movistar se puede decir que no existe cumplimiento de las políticas de NR ya que se están dando tratos discriminatorios entre servicios, dando preferencia a unos sobre otros.

Recomendaciones

Si se requiere otro tipo de análisis para los datos (como la regla KS que utiliza Wehe), es necesario la implementación de un tráfico neutral, en lugar del aleatorio, para poder realizar comparaciones entre servicios de manera precisa, ya que en el estudio realizado por Fangfan Li (2017) se comprobó que los tráficos aleatorios son susceptibles a ser diferenciados.

Si se desean brindar juicios de valor con respecto a la Neutralidad de Red es recomendable tener un gran número de mediciones, por períodos de tiempo más largos y realizar un análisis a mayor profundidad para determinar si la diferenciación de tráfico se está llevando a cabo y si transgrede la NR.

Es fundamental mantener el equipo fijo sin uso y en lo posible sin aplicaciones trabajando en segundo plano, pues estas pueden interferir directamente en los parámetros de latencia que la herramienta pretende obtener y monitorear.

En el caso del dispositivo móvil es recomendable para la realización de las pruebas, que este se encuentre en un lugar de poca interferencia, sin manipulación ni uso. Además, se de asegurar que exista una conexión estable y con buena señal para una correcta toma de datos.

Las mediciones con la aplicación móvil pueden realizarse en tecnología 3G o 4G, pero una comparativa de resultados de ISP’s móviles debe ser realizada en una sola tecnología, es decir, si se realizaron las pruebas del ISP 1 en LTE, las pruebas del ISP 2 también en LTE.

Bibliografía

ACLU. (9 de Abril de 2018). *ACLU Oregon*. https://www.aclu-or.org/en/news/breaking-down-oregons-new-net-neutrality-law

Adams, M. (7 de Abril de 2013). *WireShark What is it & What is its purpose?* ResearchGate: https://www.researchgate.net/publication/236863534_Wire_Shark_What_is_it_What_is_its_purpose

AsambleaNacional. (2015). *Ley Orgánica de Telecomunicaciones.* Quito, Ecuador.

Berners-Lee, T. (2015). *World Wide Web Foundation*. Net Neutrality in Europe: A Statement From Sir Tim Berners-Lee: https://webfoundation.org/2015/10/net-neutrality-in-europe-a-statement-from-sir-tim-berners-lee

Castoreo, X., Maillé, P., & Tuffin, B. (2020). Weaknesses and Challenges of Network Neutrality Measurement Tools. *16th International Conference on Network and Service Management (CNSM).* Bordeaux: IEEE. https://doi.org/https://doi.org/10.23919/CNSM50824.2020.9269077

Castoreo, X., Maillé, P., & Tuffin, B. (2021). Analyzing the Wehe Network Neutrality Monitoring Tool. *GECON 2021 - 18th International Conference on the Economics of Grids, Clouds, Systems, and Services* (págs. 1-7). París: HAL open science. https://doi.org/10.1007/978-3-030-92916-9_13

CEPAL, N. (2010). *Las TIC para el crecimiento y la igualdad: renovando las estrategias de la sociedad de la información.* Santiago de Chile: CEPAL.

Cerf, V. (2009). The open Internet: What it is, and why it matters. *Telecommunications Journal of Australia, 59*, 1-10. https://doi.org/http://dx.doi.org/10.2104/tja09018

Cisco. (31 de Marzo de 2021). *Umbrella 1 Million*. Cisco: http://s3-us-west-1.amazonaws.com/umbrella-static/index.html

Clarke, G., Zhenwei, C., & Colin, L. (2015). The Internet as a general-purpose technology: Firm-level evidence from around the world. *Economics Letters, 135*, 24-27. https://doi.org/10.1016/j.econlet.2015.07.004.

CMSI. (2005). *Cumbre Mundial sobre la Sociedad de la Información Documentos Finales.* Túnez: ITU. https://www.itu.int/net/wsis/outcome/booklet-es.pdf

CONATEL. (2012). *Reglamento Abonados Telecomunicaciones y Valor Agregado.* Quito. https://www.arcotel.gob.ec/wp-content/uploads/2015/10/reglamento-para-los-abonados-clientes-sva.pdf

Cordero, X. (2019). *La neutralidad de la red y el desafío para el desarrollo de la normativa regulatoria en el Ecuador.* Quito: PUCE. http://repositorio.puce.edu.ec/handle/22000/16442

CRC, C. d. (2021). *Estudio del estado de la neutralidad de red en Colombia.* Bogotá: CRC. https://www.crcom.gov.co/es/biblioteca-virtual/estado-neutralidad-red-en-colombia-2021

Curry, D. (9 de Enero de 2023). *Most Popular Apps (2023)*. Business of Apps: https://www.businessofapps.com/data/most-popular-apps/

DeRose, M. (2010). *Deep Packet Inspection and its Effects On Net Neutrality.* Denver: Regis University. https://epublications.regis.edu/cgi/viewcontent.cgi?article=1355&context=theses#:~:text=DPI%20gives%20ISPs%20the%20ability,philosophy%20of%20a%20Free%20Internet.

Dogruer, N., Eyyam, R., & IpekMenevis. (2011). The use of the internet for educational purposes. *Procedia - Social and Behavioral Sciences, 28*(606-611), 606-611. https://doi.org/10.1016/j.sbspro.2011.11.115

Easley, R., Guo, H., & Kraemer, J. (2017). From Network Neutrality to Data Neutrality: A Techno-Economic Framework and Research Agenda. *SSRN*, 3-47. https://doi.org/10.2139/ssrn.2666217

Edwards, J. (26 de Octubre de 2020). *WhatsUp Gold*. A Brief History of Network Monitoring: https://www.whatsupgold.com/blog/a-brief-history-of-network-monitoring

Garret, T., Setenareski, L., Peres, L., & Erpen, L. (2018). Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection. *IEEE Communications Surveys & Tutorials, 20*(3), 2486-2517. https://doi.org/10.1109/COMST.2018.2812641.

Garret, T., Setenareski, L., Peres, L., & Erpen, L. (2022). A survey of Network Neutrality regulations worldwide. *Computer Law & Security Review, 44*, 46-88. https://doi.org/10.1016/j.clsr.2022.105654

Gerard, M. (15 de Marzo de 2018). *Cronica*. https://cronicaglobal.elespanol.com/graficnews/horas-mas-conexiones-internet_127349_102.html

Gómez, J. (1 de Julio de 2020). *Santander*. Guía: Uso de Scapy con Python: https://santandergto.com/guia-uso-de-scapy-con-python/#:~:text=Scapy%20es%20una%20librer%C3%ADa%20realizada,import%C3%A1ndola%20en%20programas%20de%20Python.

Hallahan, B. (31 de Marzo de 2022). *How to converge fixed and mobile networks to optimize your cable business*. Nokia: https://www.nokia.com/blog/how-to-converge-fixed-and-mobile-networks-to-optimize-your-cable-business/

Hernández, A. (2017). *Modelo algorítmico para limitar la congestión el protocolo TCP en redes de extremo a extremo.* Bogotá: UDISTRITAL. http://hdl.handle.net/11349/6403

IBM, C. (20 de Enero de 2023). *Transmission Control Protocol/Internet Protocol*. Networking: https://www.ibm.com/docs/en/aix/7.2?topic=networking

IEEE. (1998). Recommended Practice for Software Requirements Specifications. *IEEE Std 830-1998*, 1-40. https://doi.org/10.1109/IEEESTD.1998.88286

Internet Society. (30 de Octubre de 2015). https://www.internetsociety.org/es/policybriefs/internetgovernance/

InternetSociety. (9 de Septiembre de 2020). *Internet Society*. https://www.internetsociety.org/es/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/#_ftn1

Jan Krämer, L. W. (2013). Net neutrality: A progress report. *Telecommunications Policy, 37*(9), 794–813. https://doi.org/10.1016/j.telpol.2012.08.005

Johannsen, G. (16 de Febrero de 2022). *CeCo*. 5G y el Futuro de Internet: Un balance entre neutralidad y competencia: https://centrocompetencia.com/johannsen-5g-y-futuro-de-internet-balance-neutralidad-y-competencia/#_ftn5

Kabir, H. (2020). *Introduction to TCP/IP*. Researchgate: https://www.researchgate.net/publication/341326630_Introduction_to_TCPIP

Kang, C. (31 de Agosto de 2018). *The New York Times*. https://www.nytimes.com/2018/08/31/technology/california-net-neutrality-bill.html

Katz, R. (2022). *El papel de la economía digital en la recuperación económica de América Latina y el Caribe.* Telecom Advisory Services. https://www.millicom.com/media/5157/katz-informe-latam-completo-junio-2022.pdf

Kemp, S. (26 de Enero de 2022). *Digital 2022: Another year of bumper growth*. (we are social) Retrieved 17 de Febrero de 2022, from https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

Kende, M. (2020). *Internet Governance in international Geneva.* Ginebra: Fondation pour Genève. https://www.graduateinstitute.ch/sites/internet/files/2020-09/FPG_Bulletin%20Internet%20Governance-DIGITAL.pdf

Lee, T. (5 de Marzo de 2018). *Washington Governor*. Jay Inslee: https://www.governor.wa.gov/news-media/washington-becomes-first-state-pass-net-neutrality-protections-law

Leiner, B., Cerf, V., & Clark, D. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review, 39*(5), 22-31. https://groups.csail.mit.edu/ana/A%20brief%20history%20of%20the%20internet%20-%20p22-leiner.pdf

Lessig, L. (1999). Open code and open societies: values of Internet governance. *Chicago-Kent law review, 74*, 101-116. https://cyber.harvard.edu/works/lessig/final.PDF

Li, F., & al, e. (2019). A large-scale analysis of deployed traffic differentiation practices. *Association for Computing Machinery*, 130-144. https://doi.org/10.1145/3341302.3342092

Li, F., Razaghpanah, A., Molavi, A., Niaki, A., Choffnes, D., Gill, P., & Mislove, A. (2017). A Library for Exposing (Traffic-classification) Rules and Avoiding Them Efficiently. *Association for Computing Machinery*, 128-141. https://doi.org/10.1145/3131365.3131376

Madhvapaty, H., & Goyal, S. (2014). Net Neutrality – A Look at the Future of Internet. *IOSR Journal of Computer Engineering, 16*, 71-77. https://doi.org/10.9790/0661-16427177

Molina, J. (2011). *La Neutralidad de Red: Gestión de tráfico mediante DPI/DFI.* Barcelona: Universitat Politecnica de Catalunya. https://upcommons.upc.edu/bitstream/handle/2099.1/13900/pfc_memoria.pdf

ntop. (2023). *ntop*. https://www.ntop.org/products/traffic-analysis/ntop/

Nvidia. (23 de Junio de 2020). *Differentiated Services Code Point (DSCP)*. Ethernet Network: https://docs.nvidia.com/networking/pages/viewpage.action?pageId=30606673

Ordabayeva, G. K., & al, e. (2020). A Systematic Review of Transition from IPV4 To IPV6. *Proceedings of the 6th International Conference on Engineering & MIS 2020* (págs. 1-15). NY USA: Association for Computing Machinery. https://doi.org/10.1145/3410352.3410735

Rahman, S. (2003). Next Generation of Internet. *Proceedings of the International Workshop on Distributed Internet Infrastructure for Education and Research. 1*, págs. 17-26. Bangladesh: Dhaka. https://www.researchgate.net/publication/293168279_Next_Generation_of_Internet

Rout, C., & Aldous, C. (2016). How to write a research protocol. *Southern African Journal of Anaesthesia and Analgesia, 22*(4), 101-107. https://doi.org/10.1080/22201181.2016.1216664

Salim, H., Mohammed, A., & Yahya, O. (2020). *Introduction to Computer Network.* Bagdad: AL-MUTANABE. https://www.researchgate.net/publication/346108941_Introduction_to_Computer_Network

Saltzer, J., Reed, D., & Clark, D. (1984). *End-to-end arguments in system design.* Massachusetts: ACM Transactions. https://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf

Šimon, M., & Ladislav, H. (CSOC 2019). A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks. *Software Engineering Methods in Intelligent Algorithms, 984*, 109-118. https://doi.org/10.1007/978-3-030-19807-7_12

Solum, L. (2008). Models of Internet Governance. *U Illinois Law & Economics Research, 7*(25), 48-91. https://doi.org/https://ssrn.com/abstract=1136825

Soto, S. A. (13 de Noviembre de 2022). *La República*. Retrieved 20 de Febrero de 2022, from https://www.larepublica.co/especiales/la-industria-del-e-commerce/penetracion-de-internet-en-latinoamerica-supera-la-media-mundial-que-es-de-58-3088484

Subsecretaría de Telecomunicaciones, S. (27 de Mayo de 2014). *SUBTEL*. Ley de Neutralidad y Redes Sociales Gratis: https://www.subtel.gob.cl/ley-de-neutralidad-y-redes-sociales-gratis/

Triviño, R. D., Franco, A. A., & Ochoa, R. L. (2021). Internet and Net Neutrality in the Time of Covid-19: A Global Overview. *Eighth International Conference on eDemocracy & eGovernment (ICEDEG).* Sangolquí: IEEE. https://doi.org/10.1109/ICEDEG52154.2021.9530952.

Triviño, R., Franco, A., & Ochoa, L. (2020). Network Neutrality: The case of five South American countries. En M. Botto, H. Cruz, & A. Díaz, *Artificial Intelligence, Computer and Software Engineering Advances* (págs. 150-161). Springer International .

Triviño, R., Franco-Crespo, A., & Ochoa-Urrego, L. (2021). Convergencia y matices de la neutralidad en la red en América del Sur. *Scielo*(26), 30-40. http://dspace.ups.edu.ec/handle/123456789/20480

Van Schewick, B. (2010). The Public Internet and Net Neutrality. *Harvard Journal of Law & Technology*(402), 50-62. https://doi.org/10.2139/ssrn.1684677

Wilson, M. (12 de Diciembre de 2022). *PC & Network downloads*. https://www.pcwdld.com/deep-packet-inspection#wbounce-modal

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 141-179. https://scholarship.law.columbia.edu/faculty_scholarship/1281

Zidek, M., Magdina, P., & Alkhalaf, A. J. (2022). The History and Future of Network Monitoring. *International Journal of Engineering Research and Reviews, 10*(3), 29-32. https://doi.org/10.5281/zenodo.7060322