UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Metodología para la evaluación del rendimiento de red en tecnologías Inalámbricas WLAN

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Maldonado Jiménez Pablo Enrique **(ORCID:** 0000-0003-1724-3247)

ASESOR:

Dra. Rodríguez Baca Liset Sulay **(ORCID:** : 0000-0003-1850-615X)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de servicios de redes y comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Tecnologías de la Información y comunicación

LIMA – PERÚ

2022

DEDICATORIA

A Dios Padre, a mis abuelos Norma y Herminio por su apoyo incondicional, a mi mama Marleni que estando lejos siempre me motivo a seguir adelante, a mi padre por enseñarme a ser fuerte y a mis hermanos y toda mi familia que fue participe de mi desarrollo universitario.

AGRADECIMIENTO

A mi casa de estudio y los profesores que fueron parte de mi desarrollo profesional, a su nivel de exigencia y toda la experiencia depositada en conocimientos, a todas las personas que me ayudaron a desempeñarme en el ámbito laboral.

Índice de contenidos

Índice de tablas

Índice de Figuras

Tabla de Anexos

RESUMEN

El trabajo de investigación fue desarrollado con el objetivo de implementar una metodología para evaluar el rendimiento de red en las tecnologías inalámbricas Wlan, así mismo se instaló dos tecnologías PLC y Wifimesh para un caso de estudio en la pyme BNC Servicios generales. Se elaboró la metodología TROUDEJINISE como parte de la investigación, para su desarrollo se hizo una revisión de libros y revistas respecto a los procesos para la implementación y la evaluación del rendimiento de una red. La metodología TROUDEJINISE está compuesta por las siguientes fases: (1) Diseño e Implementación, (2) Pruebas de Rendimiento, (3) Nivel de Seguridad y (4) Pruebas de Fuerza Bruta .Los resultados demostraron que el retardo extremo a extremo se redujo en 6.8 ms , el porcentaje de paquetes pedidos disminuyo en un 0.10 %, la tasa de datos promedio incremento en 2.31 Mbps, la variación de tiempo de transmisión disminuyo en 2.2 ms y la cantidad de ataques bloqueados fue 1115667 aplicando prueba de fuerza bruta. Por último, se recomienda utilizar nuevos indicadores y someter otras tecnologías inalámbricas a prueba.

Palabras Clave: Rendimiento de red, wifimesh, PLC, tecnologías inalámbricas, seguridad de red.

ABSTRACT

The research work was developed with the objective of implementing a methodology to evaluate network performance in WLAN wireless technologies, likewise two PLC and Wifimesh technologies were installed for a case study in the SME BNC General Services. The TROUDEJINISE methodology was developed as part of the research, for its development a review of books and magazines was made regarding the processes for the implementation and evaluation of the performance of a network. The TROUDEJINISE methodology is composed of the following phases: (1) Design and Implementation, (2) Performance Testing, (3) Security Level and (4) Brute Force Testing. The results showed that the end-to-end delay was reduced in 6.8 ms, the percentage of requested packets decreased by 0.10%, the average data rate increased by 2.31 Mbps, the transmission time variation decreased by 2.2 ms and the number of attacks blocked was 1115667 applying brute force testing. Finally, it is recommended to use new indicators and put other wireless technologies to the test.

Keywords : Network performance, wifimesh, PLC, wireless technologies y network security.

I INTRODUCCIÓN

Las redes WLAN ocupan un lugar importante en todos los sectores, siendo de gran impacto en los últimos años, por la coyuntura actual muchas tecnologías de conexión a red se han desarrollado para servir de buenas alternativas, generando mayor satisfacción a los usuarios finales. García Castaño, Mosquera Taborda y Pérez Múnera (2018). Las conexiones inalámbricas están surgiendo cada vez más en la vida cotidiana, a medida que esto incremente también nace la necesidad de sostener en estos entornos (Wireless) los mismos programas que se desempeñan en redes cableadas (Tavara 2016). Por otro lado, las redes WLAN de hoy son aceptadas y utilizadas para la trasmisión de información, en el rol de expansión de las redes de conexión local, esto genera menores costos de implementación, disponibilidad y rendimiento (Skendzic, Kovacic y Ljubicic 2020).

Actualmente existen metodologías para implementar, diseñar y analizar el estado y estructura de una red, siendo estas favorables en su enfoque. El propósito de Top-Down Network Design, es ayudar a diseñar redes que cumplan con objetivos comerciales y técnicos de un cliente. Esta metodología cuenta con procesos y herramientas comprobados para entender la circulación de tráfico de red, el comportamiento del protocolo y el trabajo de internet (CISCO 2011).

MARIN, Antonio (2014) Indica que el rendimiento de una red se enfoca a la calidad de distribución que se pueda emplear, así mismo se encuentra relacionada con ciertas métricas de desempeño QoS (Quality of Service). Así mismo el rendimiento de una red depende de varios componentes, incluido la cantidad de datos, el medio de transmisión, las capacidades del hardware y la eficiencia del software (Sreenivasulu, T. Shaheen, H. Himabindu y E. Rajasekar 2018).

La conexión inalámbrica ha evolucionado el mundo de forma exponencial de tal manera que es difícil ver cuán especialmente está cambiando la industria. Al fomentar el crecimiento económico y la mejora de estas tecnologías atraen más beneficios en los diferentes sectores no solo en las comunicaciones, cada día más las industrias aprovechan las conexiones inalámbricas trazando nuevos

horizontes, convirtiéndose en más eficaces y establecer un potencial para un amplio desarrollo (Deloitte 2017).

En Latinoamérica desde fines de marzo del 2020, las estadísticas del tráfico de información de 125 millones de router wifi indican un incremento del 80% en las cargas de ordenadores hacia la nube, tal como los picos generados por los servicios streaming. Esto produce saturación de las bandas 2.4 Ghz y 5g Ghz en su mayoría (CEPAL 2020).

Según los analistas del Instituto Nacional de Estadísticas e Informática (INEI), en el Perú se ha visto un crecimiento a gran escala en el acceso a internet. A diferencia en el año 2011, el 16.4% de hogares contaban con internet, llegando al 44.2% con acceso a internet en el 2020 (INEI 2020), esto a raíz de la pandemia que ha obligado a centrarse en un mundo más virtualizado y altamente demandado.

En lo mencionado se observa un incremento de uso de las tecnologías de redes inalámbricas a nivel Latinoamérica como también a nivel nacional, de la misma manera es importante saber cuál de ellas se adaptan mejor hacia las necesidades que se presentan en los usuarios de acuerdo al uso y al alcance que se requiera dar, por lo tanto, es necesario también contar con una metodología que permita evaluar el rendimiento que brindan actualmente las nuevas tecnologías de redes inalámbricas, de esta manera se propone una metodología que tenga un enfoque general hacia las métricas de rendimiento establecidas por estudios que han sido comprobados y procesos que definan cómo obtener los mejores resultados de comparación entre una y otra para poder ayudar a seleccionar la tecnología indicada.

Así mismo el estudio cuenta con justificación tecnológica debido a que se propone evaluar diferentes tecnologías de redes inalámbricas, entre ellas la tecnología WifiMesh, una tecnología que se ha vuelto muy demanda hacías las redes wifi puesto que cuenta con una tecnología en malla para garantizar la cobertura y estabilidad de toda la red. MUHENDRA, Rifky y ARZI, Yudha (2017) mencionaron que las ventajas que brindan las redes de malla es la conexión de distancia transmisión, lo mismo que esta reduce cierto grado de pérdida de datos,

y cuenta con una red sostenible entre sí, en caso un nodo falle los otros restantes puedes mantener el enlace formando una red y enviar paquete de datos. De la misma manera Power Line Comunications, el objetivo de usar esta tecnología es que la red eléctrica tiene mayor cobertura y es predominante ante otras conexiones como redes LAN o WIFI, puesto que la mayoría de equipos van conectados a toma de corriente y esto genera un valor agregado (Motta y Gonzales 2019).

Se propone la metodología TROUDEJINISE para diferenciar el rendimiento que brindan cada una de estas tecnologías, de la misma forma estarán basadas en ciertas métricas propuestas por parte de la metodología que se implementará en este proyecto.

La justificación metodológica, se propone implementar una metodología con las buenas prácticas de investigaciones y antecedentes para la evaluación del rendimiento de las redes, puesto que actualmente no existe una como tal. Skendzic, KOVACIC, A. y LJUBICIC, B. (2020) mencionaron que la medición del rendimiento de una red brinda información del estado y permite ver respuestas sobre mejora hacia las necesidades con el propósito de sostener la calidad del servicio, especialmente rapidez, disponibilidad y seguridad.

El problema general de la investigación es cuál es el resultado de implementar una metodología para evaluar el rendimiento de red en tecnologías inalámbricas wlan. Así mismo los problemas específicos:

P1: Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Throughput en un sistema PLC y WifiMesh.

P2 Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Jitter en un sistema PLC y WifiMesh.

P3: Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Delay en un sistema PLC y WifiMesh.

P4: Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Nivel de seguridad en un sistema PLC y WifiMesh.

De la misma manera se definió el objetivo general Implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan, así pues, los objetivos específicos planteados son:

OE1: Aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Throughput de un sistema PLC y WifiMesh.

OE2: Aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Jitter de un sistema PLC y WifiMesh.

OE3 Aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Delay de un sistema PLC y WifiMesh.

OE4: Aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Nivel de seguridad de un sistema PLC y WifiMesh.

La Hipótesis general del proyecto de investigación es: La implementación de una metodología permite la evaluación del rendimiento de red en tecnologías inalámbricas wlan.

HE1: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el troughput de un sistema PLC con Wifimesh.

HE2: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Jitter de un sistema PLC con Wifimesh.

HE3: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Retardo extremo a extremo de un sistema PLC con Wifimesh.

HE4: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Nivel de Seguridad de un sistema PLC con Wifimesh.

II. MARCO TEÓRICO

Para este capítulo se recopiló información de los artículos y tesis de investigaciones anteriores relacionadas a las tecnologías a la cual serán sometidas en nuestra metodología así mismo se detallará las variables e indicadores con su marco conceptual de cada una de ellas.

AGURTO, Fernando , HERNANDEZ, Mario y LOPEZ, Heber (2016) propusieron en su investigación implementar red mesh para video vigilancia y ampliar la cobertura de wifi. (Agurto, Hernandez y Lopez 2016) seleccionó una muestra de estudio de un total de 66 personas que conforman el personal del área. Obtuvo como resultado que la Tasa de transferencia fue de 18 Mbps y carga 54 Mbps, la Tasa de transferencia del streaming de video fue de 3 Mbps promedio y la Tasa de transferencia del servicio de acceso a internet se vio limitada siento 4 Mbps. De la misma manera Agurto, Hernandez y Lopez (2016) recomiendan que para que el sistema sea más robusto y se puedan soportar enlaces de mejor calidad, se debe utilizar interfaces con el protocolo 802.11AC y antenas direccionales para soportar la red Mesh.

AYON, Michel (2020) planteó en su investigación mostrar los beneficios e implementar la red mesh para el campus universitario . La metodología usada fue mixta. AYON, Michel (2020) seleccionó una muestra de 269 personas que conforman la plana estudiantil. En la encuesta aplicada post-implementación se obtuvo como resultado que, el 60% tal vez conocen acerca de los beneficios que ofrece la tecnología Mesh, el 30% conocen y el otro 10% mencionó no conocer. AYON, Michel (2020) recomienda que el equipo de red más recomendable es el UniFi UAP-AC Mesh, debido a su compatibilidad con los dispositivos ya existentes dentro del complejo universitario UNESUM.

BENITES, Maria (2018) llevó a cabo el Diseño E Implementación De Un Piloto De Red Wireless Mesh Basada En Firmware Libre Utilizando Nodos

802.11. BENITES, Maria (2018) Mencionó que se instaló un firmware de acuerdo a la tecnología de los equipos, para analizar el tráfico se utilizó herramienta wireshark, también se midió el tiempo de convergencia entre router y viabilidad de la red las cuales se utilizó software iperf para el diagnóstico de ciertas métricas de red como delay y jitter. Se obtuvo de resultado que el retardo y el jitter son proporcionales al número de saltos obteniendo una variación de 0.639 ms y 0.896 ms, mientras que la tasa de transmisión es inversamente proporcional. BENITES, Maria (2018) recomendó realizar un estudio sobre el impacto en el retardo y jitter a través de Access Point, así mismo determinar las métricas que se utilizó en el trabajo de investigación.

MENDOZA, Christian (2021) propuso un diseño de red inalámbrica para una compañía del sector minero. El autor propuso en su investigación el uso de la frecuencia de la tecnología mesh en la banda de 5Ghz para la red wifi al determinar que no existe una buena calidad de cobertura y velocidad para transmisión de datos en el lugar de estudio. MENDOZA, Christian (2021) destacó como resultado que la cobertura de señal estaba por -45 dm promedio hasta el último piso, ya que lo recomendable para calidad de servicio es mínimo -55, con respecto a la velocidad se demostró que se puede alcanzar 4.8 Gbps en la frecuencia de 5 GHz. MENDOZA, Christian (2021) recomendó contar con un plan beta para probar el diseño y así mismo generar retroalimentación para entomizar mejor el sistema de conexión inalámbrica.

HERRERA, Hector (2018) implementó un Modelo De Optimización De Rendimiento En Redes 802.11ac Utilizando Programación Multi-Objetivo. HERRERA, Hector (2018) Aplicó un modelo propuesto programación matemática multi-objetivo la cual permitió a partir de dos funciones objetivo, analizar y evaluar en más detalle el rendimiento de redes wlan 802.11ac. Se obtuvo como resultado que después de 66 iteraciones se optimiza el rendimiento de las redes inalámbricas WLAN utilizando tecnología 802.ac, obteniendo retardos con un valor decimal cero. HERRERA, Hector (2018) recomendó para futuras investigaciones tener más funciones objetivas, con otros parámetros que pueda garantizar mejor optimización del rendimiento de las redes wlan.

CEDEÑO, Carlos (2018) implementó la tecnología PLC para transmisión de internet en zonas rurales Guayas - Ecuador. La metodología empleada fue experimental y descriptiva. El objetivo propuesto fue implementar PLC para distribuir la señal de internet del mismo modo que se realizó comparativas con otras tecnologías alternas comprendiendo las ventajas y limitaciones de cada una. CEDEÑO, Carlos (2018) destacó los resultados que brinda PLC puesto que permite transición de velocidades de hasta 300 Mbps y el alcance que tiene hacia las zonas rurales puesto que resalta que es un 34.9 % de población rural que accede a internet en espacios públicos, del tal modo que PLC pueda cubrir el resto. CEDEÑO, Carlos (2018) indicó que PLC no sirve de reemplazo de otras tecnologías, sino que esta se pueda usar de complemento para ahorrar en costos y tener mayor alcance.

PONCE, David y SANTILLAN, Sergio (2016) propusieron en su investigación el Diseño e implementación de un sistema de transferencias de datos a través de Labview-arduino y tecnología PLC. La metodología que utilizaron en su proyecto fue método inductivo y deductivo. Demostraron que se pueden interconectar las dos tecnologías para servir como alternativas de transferencia de datos puesto que usan la red eléctrica de baja tensión, resaltan la efectividad de la conexión, el ahorro de infraestructura y el trabajo en espacios estrechos. Así mismo PONCE, David y SANTILLAN, Sergio (2016) recomiendan hacer un análisis de la red eléctrica y tomacorrientes donde se requiera implementar PLC para evitar contratiempos en la ejecución del proyecto.

MONTOYA, Moises (2017) ejecutó la evaluación de los diferentes tipos de modulaciones para sistemas PLC empleados en las Smart Grids. La metodología empleada fue exploratoria y descriptiva. MONTOYA, Moises (2017) propuso evaluar las características de los parámetros de modulación para PLC de tal modo que se pueda especificar mejor el desempeño para transferir información. A través de las pruebas sometidas concluyó que OFDM resulta ser la modulación más eficiente para reducir interferencias en transmisión por potencia eléctrica.

URIBE, Maria y GARCIA, Jorge (2016) llevaron a cabo la Transmisión de datos a través de redes eléctricas PLC. El objetivo de la investigación fue

proponer una solución inHome por medio de PLC. El resultado del estudio que se obtuvo fue que PLC brinda un mejor rendimiento en trayectos que no superan los 100mtrs, del mismo modo que comparte compatibilidad magnética puesto que se transmite por una red eléctrica de potencia baja, demostrando así que pueda ser empleada en lugares como casas, oficinas, residencias entre otras. URIBE, Maria y GARCIA, Jorge (2016) recomendaron que esta tecnología a futuro tendrá mayor impacto y habrá interés de inversión para comercializar del mismo modo que disminuirán los costos de adquisición y será más accesible hacia los hogares.

CABRERA, Byron (2016) diseñó una red multiservicio para una institución cuyo objetivo fue agilizar los procesos administrativos y mejorar la calidad de enseñanza. La metodología empleada fue Top Down Network Desing. CABRERA, Byron (2016) concluyó que Top down permitió establecer un sistema por fases como análisis, diseño lógico, físico y las pruebas en marcha, esto facilitó un mejor análisis para la implementación de la red. Del mismo modo recomienda que es importante mantener una documentación de toda la red para facilitar la escalabilidad y mantenimiento de la red.

RAMIREZ, Maria (2020) diseñó una red de datos aplicando metodología PDDIO de Cisco para mejorar la eficiencia conexión y transferencia de la red en una empresa. Se empleó una metodología de investigación descriptiva no experimental. La muestra seleccionada fue de 23 usuarios de red, en el grado de satisfacción con la red actual el 78.26% mostró inconformidad además el 100% sostuvo en implementar una nueva red. Concluyó que la metodología empleada ayudo a mejorar la conectividad y permitió el uso compartido de recursos más rápida y efectiva. Del mismo modo recomienda mantener un personal capacitado para el mantenimiento y estabilidad de la red.

CHAUCA, Juan (2016) diseñó una red convergente para transferencia de voz y datos en una empresa. La metodología para el diseño y análisis de red fue James Mccabe. Como resultado se concluyó con cada fase dentro de la metodología, 1era la recopilación de información que requiere la empresa, la 2da fase el análisis y diseño de red, 3era fase soluciones y cambios para mejorar el

rendimiento y la 4ta fase los costos en equipamiento y estructura de red propuesta. CHAUCA, Juan (2016) recomendó la implementación de un sistema de monitoreo de red para detectar posibles fallas que puedan presentarse.

CHUQUICONDOR, Yuri (2017) propuso una metodología para la gestión y evaluación del ancho de banda de una red en un campus universitario. Se realizó un estudio experimental, se tomó una muestra de 100 personas donde el 0% muestra inconformidad con el servicio de red dado y una necesidad de propuesta de mejora el 100%, estos datos demostraron la necesidad de implementar una metodología para la red del campus. Después de la implementación se concluyó que resultó beneficioso la metodología puesto que permitió trabajar e ingresar más rápido en los diferentes sistemas de la universidad, así como también la mejora de velocidad y disponibilidad de red wifi y LAN. CHUQUICONDOR, Yuri (2017) recomienda la adquisición de equipos de nueva tecnología para crear políticas de seguridad hacia internet dentro del campus universitario.

GARCIA, Deysi y MORAN, Lidia (2016) realizaron un estudio para la comparación de redes inalámbricas en base al rendimiento de redes IEEE 802.11ac Y 802.11n. El tipo de investigación desarrollada fue bibliográfica con diseño no experimental, para la participación se tomó una muestra de 75 estudiantes. Se concluyó que el estándar 802.11 ac utiliza menos energía además difiere de interferencias o ruidos puesto que opera en banda de 5Ghz. GARCIA, Deysi y MORAN, Lidia (2016) recomendaron evaluar las tecnologías que brindan los proveedores ISP para aprovechar mejor el rendimiento del estándar en bandas 5Ghz.

ERAZO, Pablo (2016) realizaron una comparación de metodologías para implementar proyectos de redes. Utilizó como muestra las metodologías de redes existentes como Top Down, PDDIOD, CISCO entre otras. ERAZO, Pablo (2016) concluyo que cada metodología brinda información de los procesos para cada fase, pero no proveen un modelo para desarrollarlo. De lo anterior el autor recomienda mantener una base documental que facilite la ejecución y mantenimiento de la red.

En esta sección se detallan las teorías en relación al proyecto de investigación. La tecnología WifiMesh, están siendo utilizadas en la mayoría de conexiones de red wifi puesto que ha optimizado mejor la conectividad inalámbrica. Las ventajas que brindan una red mesh es la adicción de distancia y transmisión, de la misma forma que reduce la pérdida de paquetes, y brinda una comunicación de enrutamiento de datos de forma automática en caso falle la conexión (Muhendra y Arzi 2017).

Del mismo modo DENG, et al. (2017) mencionaron que las redes malla superan los problemas de infraestructura inalámbrica, los enrutadores están interconectados entre sí, estos actúan también como servidores de acceso a red a clientes en malla, presenta mayor escalabilidad hacia las redes inalámbricas puesto que una WNM (Wireless Network Mesh) puede comunicarse con otros enrutadores o a otro nodo de internet para ampliar la cobertura y mejorar el rendimiento de una red.

MUHENDRA et al. (2017) resaltó que esta tecnología se adiciona a los diferentes estándares de redes Inalámbricas puesto que está formado de una red con topología de malla, el enrutador es un dispositivo el cual funciona como enlace entre varias redes para transferir datos entre una y otra de tal manera que si un nodo no funciona el resto aún pueden comunicarse de forma de directa o a través de un nodo intermedio. Por otra parte DENG, et al. (2017) indicaron que esta tecnología ha tomado importancia para implementar en las Smart Grid (SG) puesto que facilita la recopilación de datos y control remoto además que permite ahorrar en equipos de red e incrementa el rendimiento.

Power Line Comunications (PLC) es una tecnología que permite transportar la red de datos por alimentación eléctrica, es una opción hacia la variedad de conectividad que se pueda emplear de tal manera que complementa con las redes inalámbricas Wifi. ARROYO, Xavier, et al. (2017) mencionaron que es una tecnología prometedora puesto que no requiere de mucha infraestructura para emplearla además requiere de una tensión eléctrica media o baja.

Así mismo la principal ventaja que presenta es la amplia cobertura a diferencia de una red wifi común, puesto que permite llegar hacia los puntos ciegos de una red permite velocidades de hasta 1gbps del mismo modo que garantiza mayor seguridad (Vlachou, Henri y Thiran 2016) .

VLACHOU Christina, HENRI. Sebastien y THIRAN, Patrick (2016) demostraron que Power Line Comunications (PLC), proporciona mayor rendimiento, puesto que logra 18 veces mayor que Wifi (40.1 para a diferencia de wifi 2.2 Mbps). El ancho de banda 12 veces (46.3 frente a 3.8 Mbps), para estos resultados sometieron dichas tecnologías a ciertas métricas propuestas en su artículo.

Para la evaluación del rendimiento de una red es importante primero el diseño e implementación de la misma, por tal modo existen diferentes metodologías y guías para diseñar e implementar, estas se encuentran formadas por diferentes fases y procedimientos el cual sirven de apoyo para llevar a cabo un proyecto, así mismo mencionaremos las existentes.

Metodología MacCabe esta metodología está estructurada para seguir el desarrollo lógico del análisis y validación de requisitos para formar una red de tal manera que permita seleccionar la estructura tecnología que se desea emplear. MCCABE, James (2007) mencionó que los prendimientos que ofrece en su metodología están basados de contribuciones y experiencia de arquitectos y diseñadores de redes. El objetivo de la metodología se basa en determinar el enrutamiento, seguridad, rendimiento y gestión de una red, del mismo modo que apoya a desarrollar la trazabilidad de requerimientos y diseños de arquitectura además de determinar cómo aplicar los mecanismos de desempeño de una red la calidad de servicio el nivel de acuerdo y políticas de la red.

Por otra parte, la Metodología Top Down para el diseño y estructura de red propuesta por CISCO, permite analizar el flujo de tráfico y la conducta de los protocolos y conexión de diferentes tecnologías de redes. Consta de 5 fases para la implementación y diseño de una red, la primera fase identificación de requisitos, la segunda diseño lógico la tercera diseño físico y la última fase testing optimización y documentación de la red.

El rendimiento de una red puede ser explicado de diferentes puntos de vista de tal manera que permite incorporar diferentes maneras de evaluación. Entre los parámetros para evaluar se mencionan throughput, latencia, jitter y el porcentaje de paquetes perdidos (Ferreira, Granados y Vesga 2016), estas métricas están relacionadas con las QoS (Quality of service) para las redes de información resaltaron (Caiza y Lara 2019) de tal modo que permite clarificar los resultados de la evaluación. La QoS garantiza la transferencia de información en ciertos parámetros que ya están definidos por diferentes organismos que controlan los servicios inalámbricos, algunos de los requisitos es que el retardo extremo a extremo no exceda al tiempo específico así mismo asegure un mayor ancho de banda (Olivera y Alvarez 2018).

Jperf es una herramienta de software libre el cual permite analizar el rendimiento de una red, se puede realizar las pruebas correspondientes para conexiones de red inalámbricas como por cable. Aviles y Pachacama (2015) mencionaron que Jperf es una herramienta que permite crear flujo de datos UDP y TCP, desarrollada por DAST (Distributed Applications Support Team) y está desarrollada en c++, entre las funcionas que permite medir esta herramienta son latencia, Jitter, pérdida de datagramas, pérdida de paquetes, Throughput, retardo y bandwicth.

PRGT Network Monitor esta herramienta permite monitorear la red de tal manera que supervisa la disponibilidad y uso de red, es un software de licencia Freeware compuesto con 100 sensores. Naranjo (2016) indicó que esta herramienta cuenta con una interfaz interactiva de tal manera que no es necesario tener conocimientos técnicos puesto que muestra resultados en gráficos de tiempo real y reportes customizados, se desempeña en entorno Windows, permite medir los siguientes indicadores Throughput, pérdida de paquetes y bandwitch.

El nivel de seguridad de red es de suma importancia para cualquier tipo de infraestructura y tecnología con la cual se trabaje, es indispensable proporcionar planes estrictos para cada detalle o vulnerabilidad de la red.

RODRIGUES et al. (2018) mencionaron que el nivel de seguridad está relacionado con el control de contingencias para asegurar la protección a los dispositivos finales en una red, del mismo modo en salvaguardar la información que transita en ella. El objetivo de la seguridad es identificar las vulnerabilidades y contrarrestar los posibles ataques o instrucciones que puedan presentarse, del mismo modo MUKHERJEE, Aditya (2020) mencionó que para la seguridad de una red se debe tener en cuenta protocolos de seguridad, inspección SSL, motor de prevención de amenazas, análisis de ataques y saber entender la eficacia de los productos para garantizar mayor seguridad.

Existen diferentes herramientas para automatizar pruebas de penetración e identificar vulnerabilidades dentro de una red, en ella especificaremos las siguientes para someter a las tecnologías que se evaluarán en el proyecto de investigación. MUKHERJEE, Aditya (2020) resaltó Kali Linux, es un sistema operativo el cual contiene 300 herramientas de pruebas de penetración, las aplicaciones con las que cuenta el sistema es lo necesario para la fase de explotación si se requiere vulnerar una red.

Del mismo modo MUKHERJEE, Aditya (2020) mencionó WireShark como una de las plataformas de seguridad de red más utilizada, esta permite capturar datos en vivo en la red y analizar los paquetes de datos. Proporciona para la investigación realizar inspecciones profundas y permite utilizar soporte de descifrado como IPSec, ISAKMP, Kerberos, SSL / TSL y WPA / WPA2, entre otros.

Si se habla de ataques a una red inalámbrica podemos mencionar entre ellas el ataque de Fuerza Bruta, este ataque consiste en generar aleatoriamente todas las posibles claves de acceso hacia una red en un cierto tamaño basado en un determinado conjunto de caracteres. VEGA, Edgar (2020) mencionó que dado suficiente tiempo y poder de procesamiento, todas las contraseñas pueden ser vulneradas por un ataque de fuerza bruta, analistas y atacantes usan sucesivamente varios algoritmos para calcular en paralelo el algoritmo de craqueo, reduciendo plenamente los tiempos de ejecución de la prueba.

III. MÉTODO

En este capítulo se describe el tipo enfoque y diseño de la investigación además las variables e indicadores. Se considerará también una muestra de estudio para la investigación de tal manera que se utilizaran técnicas y herramientas para la recolección de datos el método el análisis y finalmente el aspecto ético de acuerdo al vicerrectorado de la universidad.

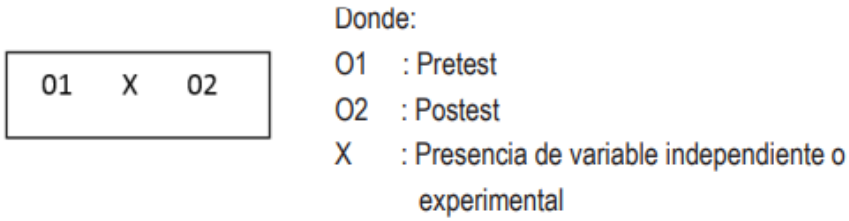
3.1 Tipo y diseño de investigación

PIMIENTA, Julio y DE LA ORDEN HOZ, Arturo (2017) " El tipo de investigación es aplicada porque su principal objetivo es ampliar y profundizar en los conocimientos acerca de la realidad, se enfoca en la construcción de generalizaciones como hipótesis teorías entre otros, así mismo permite entender los objetos o fenómenos de estudio " (p.9). En relación con la investigación es directamente porque el objetivo es evaluar el rendimiento de red en las tecnologías inalámbricas WLAN por medio de la metodología TROUDEJINISE, del mismo modo que se desarrollará a cabo de las investigaciones y publicaciones existentes.

La investigación tiene un enfoque cuantitativo puesto que se estimó las magnitudes o impacto de los objetos de estudio para comprobar la hipótesis. "El enfoque cuantitativo utiliza la recolección de datos y el análisis para contestar preguntas de investigación y probar hipótesis formuladas previamente, así mismo confía en la medición de variables e instrumentos de investigación " (Ñaupas et al. 2018 p.140).

El diseño de la investigación es experimental puesto que se aplicará una metodología para evaluar el rendimiento de red en tecnologías inalámbricas WLAN. HERNANDEZ, Roberto y MENDOZA, Christian (2018) indicaron "Lo que efectúas en una investigación experimental es manipular las variables denominadas (variables independientes) para observar los efectos sobre otras variables dependientes " (p.152), del mismo modo el tipo de diseño pre experimental ya que se realizará un post-test y un pre-test para determinar los resultados correspondientes a los indicadores. Así mismo SÁNCHEZ, Hugo y

REYES, Carlos y MEJIA, Katia (2018) mencionaron que en un diseño pre-experimental con un solo grupo permite el efecto de una variable independiente



infiere de la dependencia entre el pretest y el postest.

Figura 1: Diseño pretest y postest con un solo grupo

3.2 Variables y operacionalización

Las variables utilizadas para el proyecto fueron la metodología para la evaluación y el rendimiento de red Wlan. Las dimensiones utilizadas fueron las siguientes (1) Jitter, (2) Throughput, (3) Delay (4) Nivel de Seguridad. El rendimiento de la red se medirá a través de los indicadores a) Tasa de Datos Promedio b) Variación de tiempo de transmisión, c) Retardo Extremo a Extremo, d) Porcentaje de paquetes perdidos e) Cantidad de vulnerabilidades y f) Ataques bloqueados. (Ver Anexo Nº1).

Throughput se define como el paquete de información útil por segundo transmitido a través de canales de enlace, se mide en bits por segundo. (Ferreira, Granados y Vesga 2016)

Tasa de Datos Promedio

$$\boldsymbol{Throughtput} = \frac{TransferSize}{TransferTime}$$

Dónde:

TransferSize: Cantidad de datos

Transfer Time: Tiempo (en segundos)

(Petterson y Bruce 2003)

Jitter se define por la variación de latencia, es calculado cogiendo la diferencia de retrasó del paquete vigente y del anterior.

$$\Delta \boldsymbol{t_i} = t_i - t_{i-1}\,, donde\ i = 1, 2 \ldots . N$$

Fórmula:

Δt_i : Variación de Tiempo de transmisión

t_i : Tiempo de transmisión de paquete

(Petterson y Bruce 2003)

Delay o retardo consiste en el tiempo que demora en llegar un paquete de un lugar a otro (Caiza y Lara 2019). Así mismo Rayes y Salam (2020) mencionan que puede definirse como el retardo extremo a extremo el cual indica que es la cantidad de tiempo (en milisegundos) que toma un paquete para llegar hacia su destino.

Fórmula:

$$\boldsymbol{DT} = dp + de + dt + dy$$

Donde:

DT: Demora total

dp: Demora de Procesamiento.

de: Demora de espera

dt: Demora de Transmisión

dy: Demora de Propagación

(Rayes y Salam 2020)

Porcentaje de Paquetes Perdidos son las partes de todos los paquetes que no llegaron a su destino (Granizo y Tacuri 2017) , se generan debido al canal de transmisión, puesto que una red puede ser afectada por interferencias por dispositivos aledaños que comparten acceso al mismo canal de transmisión o se encuentren en las mismas frecuencias (Caiza y Lara 2019).

Fórmula:

$$PLR = \frac{Total\ number\ of\ paquets\ loss}{Total\ number\ of\ paquets\ sent}\ x100\%$$

(Sarangapani 2007)

Donde:

PLR: Porcentaje de Paquetes Perdidos

3.3 Población, muestra y muestreo

La población está compuesta por 30 registros de rendimiento que emplean las tecnologías inalámbricas WLAN, así mismo se evaluarán las métricas correspondientes a nuestra variable. PIMIENTA, Julio y DE LA ORDEN HOZ, Arturo (2017), resaltaron lo siguiente: “A dicho conjunto compuesto por la totalidad de los elementos, individuos o factores que forman parte de nuestro objeto de estudio y en un lugar y tiempo determinados poseen cualidades similares y observables se le denomina población” (p.84). Para los registros de rendimiento de las dos tecnologías se tomó los paquetes de datos (kilobytes) transmitidos durante las pruebas de ejecución en la red establecida. Se considerarán los siguientes criterios.

HERNANDEZ, Roberto y MENDOZA, Christian (2018) mencionaron que “La muestra es un subgrupo de la población de interés, de la que se obtendrán datos necesarios y será la forma más representativa de la población” (p.200). La muestra que se tomará para la investigación son 30 registros de rendimiento de red Power Line Comunications y WifiMesh. HERNANDEZ, Roberto y MENDOZA, Christian (2018) indicaron que “el muestreo es el procedimiento donde se selecciona el subconjunto de estudio de una población y/o universo de interés”(p.217) En la investigación el muestreo es no probabilístico por conveniencia debido a que los objetos de estudio que se tomarán sean accesibles . HERNANDEZ, Roberto y MENDOZA, Christian (2018) indicaron que “ el muestreo no probabilístico supone un procedimiento de selección orientado por las características y contexto de la investigación, más que por un criterio estadístico de generalización” (p.215).

3.4 Técnicas e instrumentos de recolección de datos

La técnica que se utilizo es la observación y como instrumento la ficha de registro. PIMIENTA, Julio y DE LA ORDEN HOZ, Arturo (2017) indicaron que "las técnicas de investigación son procedimientos diversos, esenciales para la investigación científica, por medio de las cuales es posible recabar y organizar la información" (p.86).

El instrumento ficha de registro permitió obtener la información correspondiente de las herramientas que se utilizaran para el desarrollo de la investigación como: Jperf, PRGT Network Monitor, TamoSoft, Kali Linux, Wifi App, Commad Pront. Las fichas permitirán recolectar información de acuerdo a los indicadores establecidos, Tasa de Datos Promedio, Variación de Tiempo de Transmisión, Retardo Extremo a Extremo (demora total), Porcentaje de Paquetes Perdidos, Cantidad de Vulnerabilidades y Ataques bloqueados. (Ver Anexo Nº3)

En esta investigación se aplicó la validez de contenido por juicio de expertos. ÑAUPAS, Humberto, et al. (2018) indicaron que "la validez de contenido se refiere al grado como un instrumento refleja dominio o contenido determinado" (p.274). Del mismo modo HERNANDEZ, Roberto y MENDOZA, Christian (2018) mencionaron que la validez del contenido se obtiene mediante las opiniones de expertos y al asegurarse que las dimensiones medidas por el instrumento sean representativas de dimensiones de las variables de interés.

La confiabilidad de un instrumento se refiere al grado en que su ejecución repetida al mismo individuo, caso o muestra produce resultados iguales (Hernandez y Mendoza 2018).

3.5 Procedimientos

Para ejecutar el proyecto se llevó a cabo la metodología TROUDIJENISE, así mismo está compuesta por los siguientes procesos: 1) Diseño e Implementación, 2) Ejecutar Pruebas de Mejor Esfuerzo, 3) Ejecutar Prueba de Fuerza Bruta 4) Documentar Resultados, con el objetivo de evaluar el rendimiento en las dos

tecnologías WifiMesh y PLC mediante las dimensiones propuestas Jitter, Delay, Throughput y nivel de seguridad. Se explicará el detalle en la sesión de anexos las partes compuestas de nuestra metodología (Ver Anexo 4). Los procedimientos son los siguientes:

A) Diseñar e Implementar la Red

- Establecer topología de red
- Diseño lógico
- Diseño físico
- Implementar equipos y dispositivos finales

B) Ejecutar Pruebas de Rendimiento

- Pruebas para determinar el Throughput
- Pruebas para determinar la Perdida de paquetes
- Pruebas para determinar el Jitter
- Pruebas para determinar el Retardo Extremo a Extremo

C) Evaluar el nivel de seguridad

- Planificación
- Especificación
- Ejecución
  - ✓ Identificar vulnerabilidades
- Caracterización de vulnerabilidades

D) Ejecutar Pruebas de Fuerza Bruta

Etapa de Descubrimiento

Etapa de Exploración

Etapa de Evaluación

Etapa de Intrusión

- ✓ Ataques Bloqueados

Del mismo modo para la recolección de datos se puso a prueba dos tecnologías plc y wifimesh, donde se implementó una red para la prueba piloto de ambas tecnologías, evaluando los indicadores variación de tiempo de transmisión, tasa de datos promedio, porcentaje de paquetes perdidos, retardo extremo a extremo, cantidad de vulnerabilidades identificadas y ataques bloqueados. Se hicieron pruebas de rendimiento a través de softwares Iperf3, Tamosoft, PGRT Monitor,

Kali Linux, para obtener los resultados de cada indicador y procesarlo por software estadístico para procesar resultados de la investigación. De igual forma para comprobar la metodología se realizó un estudio de caso aplicando todas las fases que corresponde a la metodología propuesta para evaluar el rendimiento de red inalámbrica con sistema plc y wifimesh en una pyme. Se aplicó las pruebas pretest y postest para la evaluación y se obtuvieron los resultados para las fichas de registro y posteriormente realizar el análisis estadístico.

3.6 Método de análisis de datos

GALLARDO, Eliana (2017) mencionó que el análisis de datos consiste en diferenciar los elementos básicos de la información y examinarlos, con el objetivo de contestar a las distintas interrogantes planteadas en la investigación. Para la investigación se desarrollará un análisis cuantitativo puesto que se revisará los datos números obtenidos en las fichas de registro para cada indicador de nuestra variable. Así mismo se efectuará el análisis inferencial puesto que permite estimar parámetros y comprobar las hipótesis." (Ñaupas et al. 2018) mencionó que "La estadística Inferencial permite probar la hipótesis general y especificas mediante técnicas de análisis paramétricas.

Se utilizó la prueba de Shapiro-Wilk para especificar si las distribuciones acumuladas de las muestras fueron normales o no normales. SALDAÑA, Manuel (2016) indico que la prueba de kolmogorov-Smirnov se emplea cuando el tamaño muestral es mayor de 50. Del mismo modo menciona que cuando el tamaño muestral es igual o menor a 50 la se aplica la prueba de shapiro-wiks.

Para la comprobación de hipótesis se empleó la prueba T Student. GUTIERREZ, Eduardo y VLADIMIROVNA, Olga (2016) mencionaron que "la prueba de T student consiste en establecer el contraste de hipótesis a probar y fijar el nivel de significancia" (p.307). De la misma forma HERNANDEZ, Roberto y MENDOZA, Christian (2018) señalaron que la prueba T permite evaluar si dos grupos difieren entre sí de manera significativa con respecto a sus medias y distribuciones en una variable.

3.7 Aspectos éticos

La tesis muestra originalidad de acuerdo a los lineamientos seguidos para citar los artículos y documentos de investigación, de tal manera que se cumple con lo concertado por el artículo 9 “la Política Anti Plagio” del Código De Ética En La Investigación De La Universidad César Vallejo 2020, así mismo se cumplió con las normas establecidas del CONCYTEC en el Código nacional de la integridad científica, “Sobre La Conducta Científica Y Sujetos Del Procedimiento Sancionador”.

Para la redacción de los conceptos bibliográficos y citas de los documentos plasmados para nuestra investigación, se desarrolló siguiendo la normativa del ISO 690-2, también usó de manera responsable los conceptos teóricos y bibliográficos de otros autores respetando el Decreto Legislativo N° 822 – Ley Sobre el Derecho de Autor.

Del mismo modo las técnicas realizadas para la metodología y los procedimientos para el desarrollo del proyecto, se ejecutaron respetando las políticas de la universidad, cumpliendo con el artículo 18 del Código de Ética del Colegio de Ingenieros del Perú, que hace referencia a obedecer las leyes, ordenanzas y disposiciones vigentes, de la misma forma ejercer los principios de honradez y moralidad.

IV. RESULTADOS

En este capítulo se presentan los resultados de la investigación en cuanto a los indicadores de rendimiento de red en las tecnologías Wifimesh y PLC, para: variación de tiempo de transmisión, tasa de datos promedio, porcentaje de paquetes perdidos, retardo extremo a extremo, cantidad de vulnerabilidades identificadas y ataques bloqueados. Del mismo modo se presentan los procesos de los datos obtenidos mediante la aplicación de la metodología TROUDEJINISE, estos datos fueron procesados mediante software estadístico para la validación correspondiente de cada indicador e hipótesis planteadas.

Análisis Descriptivo

Delay – Retardo Extremo a Extremo

Los resultados obtenidos para retardo extremo a extremo se representan en la figura 2 y se describen en la tabla 1.

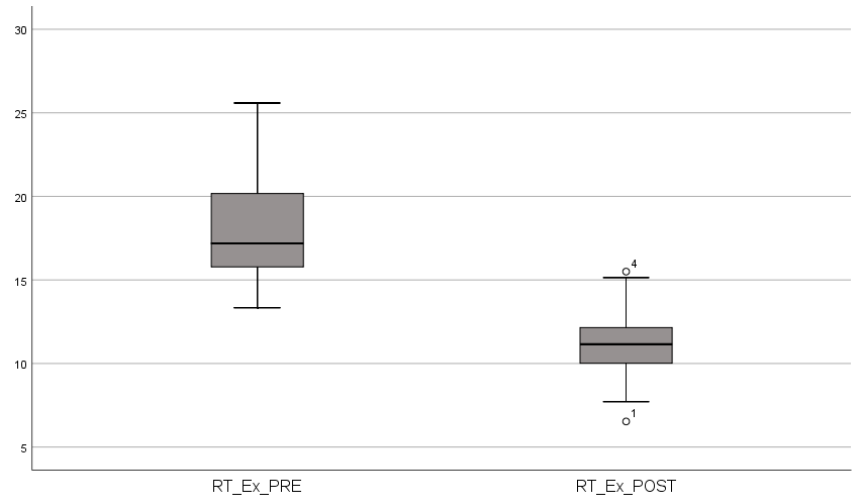


Figura 2: Retardo extremo a extremo

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
RT_Ex_PRE	30	13,33	25,59	18,0563	2,96122
RT_Ex_POST	30	6,53	15,50	11,2570	2,14480
N válido (por lista)	30				

Tabla 1: Estadísticos descriptivos - Retardo extremo a extremo

Se describe el indicador retardo extremo a extremo de las pruebas realizadas, donde el promedio obtenido en un pretest fue 18.056 y en el post test resulto un promedio de 11.257, se concluye que el retardo extremo a extremo vario en 6.799 ms considerando una mejora después de las tecnologías implementadas y la evaluación del indicador dado por la metodología.

Prueba de normalidad

Para el indicador retardo extremo a extremo puesto que la cantidad de la muestra es menor a 50 se aplicó la prueba de Shapiro-Wilk. Los resultados se muestran en la tabla 2.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
RT_Ex_PRE	0,145	30	0,111	0,947	30	0,143
RT_Ex_POST	0,107	30	0,200*	0,973	30	0,638

Tabla 2: Prueba de normalidad - Retardo extremo a extremo

En cuanto a los resultados obtenidos los valores de significancia 0.143 y 0.638 fueron mayor a 0.05, así mismo se deduce que los datos siguen una distribución normal.

Delay – Porcentaje de Paquetes Perdidos

Los resultados obtenidos para porcentaje de paquetes perdidos se representan en la figura 3 y se describen en la tabla 3.

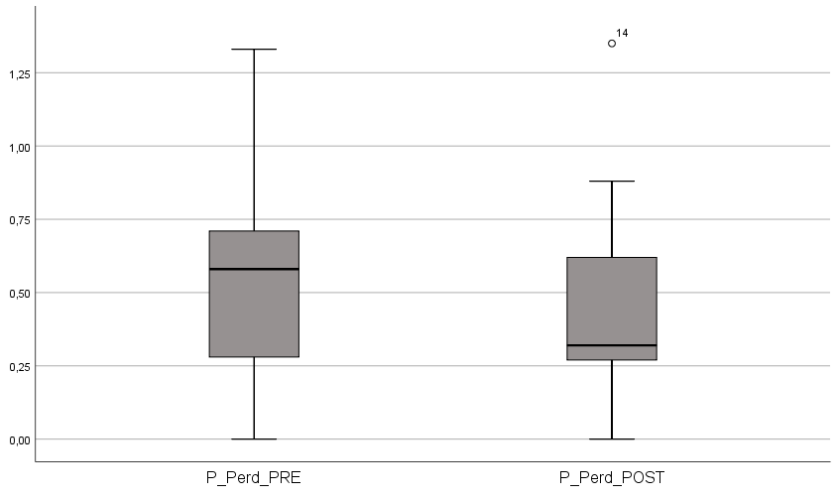


Figura 3: Porcentaje de paquetes perdidos

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
P_Perd_PRE	30	,00	1,33	,5100	0,37834
P_Perd_POST	30	,00	1,35	,3860	0,31817
N válido (por lista)	30				

Tabla 3: Estadísticos descriptivos - Porcentaje de paquetes perdidos

Se describe el indicador porcentaje de paquetes perdidos de las pruebas realizadas, donde el promedio obtenido en un pretest fue 0.51 y en el post test resulto un promedio de 0.38 se concluye que porcentaje de paquetes perdidos vario en 0.13 % considerando una mejora después de las tecnologías implementadas y la evaluación del indicador dado por la metodología.

Prueba de normalidad

Para el indicador porcentaje de paquetes perdidos puesto que la cantidad de la muestra es menor a 50 se aplicó la prueba de Shapiro-Wilk. Los resultados se muestran en la tabla 4.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
P_Perd_PRE	0,121	30	0,200*	0,927	30	0,041
P_Perd_POST	0,191	30	0,007	0,893	30	0,006

Tabla 4: Prueba de normalidad – Porcentaje de paquetes perdidos

En cuanto a los resultados obtenidos los valores de significancia 0.041 y 0.006 fueron menor a 0.05, así mismo se deduce que los datos no siguen una distribución normal.

Troughput – Tasa de datos promedio

Los resultados obtenidos para tasa de datos promedio se representan en la figura 4 y se describen en la tabla 5.

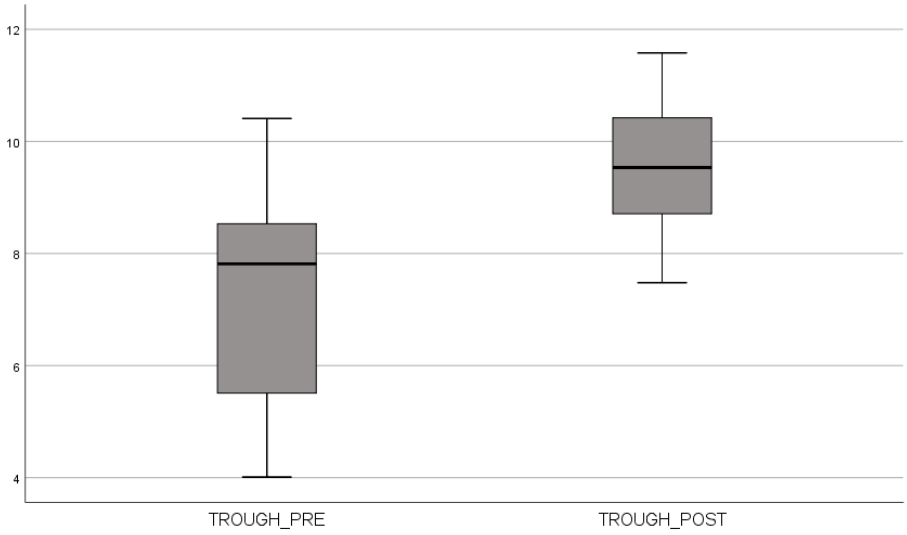


Figura 4: Tasa de datos promedio

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
TROUGH_PRE	30	4,01	10,41	7,2387	1,77882
TROUGH_POST	30	7,48	11,58	9,5530	1,15958
N válido (por lista)	30				

Tabla 5: Estadísticos descriptivos - Troughput

Se describe la tasa de datos promedio de las pruebas realizadas, donde el promedio obtenido en un pretest fue 7.23 y en el post test resulto un promedio de 9.55 se concluye que la tasa de datos promedio incremento en 2.32 considerando una mejora después de las tecnologías implementadas y la evaluación del indicador dado por la metodología.

Prueba de normalidad

Para el indicador tasa de datos promedio puesto que la cantidad de la muestra es menor a 50 se aplicó la prueba de Shapiro-Wilk. Los resultados se muestran en la tabla 6.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
TROUGH_PRE	0,157	30	0,057	0,935	30	0,068
TROUGH_POST	0,095	30	0,200*	0,970	30	0,531

Tabla 6: Prueba de normalidad - Troughput

En cuanto a los resultados obtenidos los valores de significancia 0.068 y 0.531 fueron mayor a 0.05, así mismo se deduce que los datos siguen una distribución normal.

Jitter – Variación de Tiempo de Transmisión

Los resultados obtenidos variación de transmisión para se representan en la figura 5 y se describen en la tabla 7.

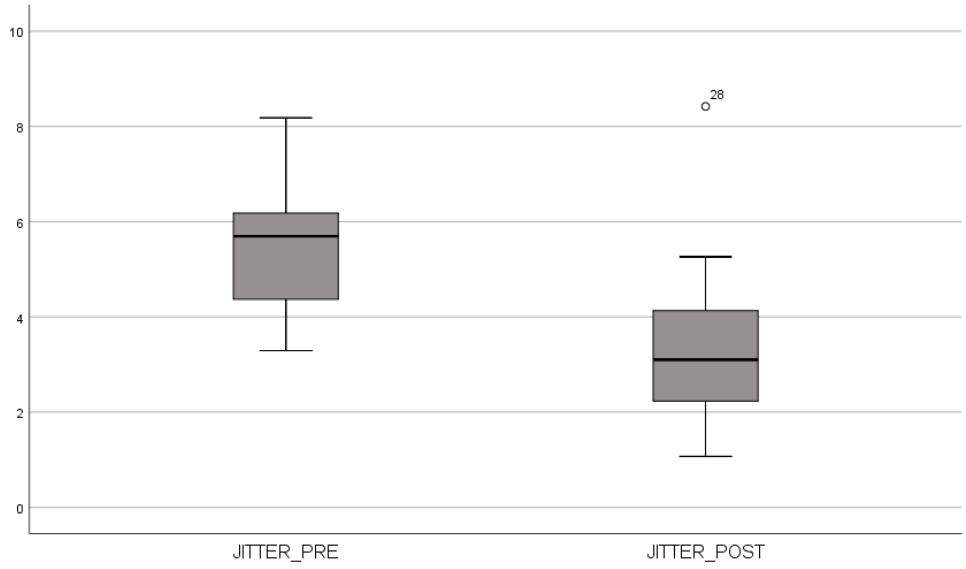


Figura 5: Variación de tiempo de transmisión

Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
JITTER_PRE	30	3,29	8,18	5,4513	1,19163
JITTER_POST	30	1,07	8,42	3,2490	1,45577
N válido (por lista)	30				

Tabla 7: Estadísticos descriptivos - Jitter

Se describe variación de transmisión de las pruebas realizadas, donde el promedio obtenido en un pretest fue 5.45 y en el post test resulto un promedio de 3.24 se concluye que la tasa de datos promedio disminuyó en 2.21 considerando una mejora después de las tecnologías implementadas y la evaluación del indicador dado por la metodología.

Prueba de normalidad

Para el indicador tasa de datos promedio puesto que la cantidad de la muestra es menor a 50 se aplicó la prueba de Shapiro-Wilk. Los resultados se muestran en la tabla 8.

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
JITTER_PRE	,116	30	,200*	0,974	30	0,647
JITTER_POST	,130	30	,200*	0,894	30	0,601

Tabla 8: Prueba de normalidad - Jitter

En cuanto a los resultados obtenidos los valores de significancia 0.647 y 0.601 fueron mayor a 0.05, así mismo se deduce que los datos siguen una distribución normal.

Prueba de Hipótesis

Hipótesis especifica 1

HE1o: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan no mide el Troughput de un sistema PLC con Wifimesh.

HE1a: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Troughput de un sistema PLC con Wifimesh.

Prueba T

Se utilizó la prueba de T debido a que la cantidad de registros fueron menor a 30. (Ñaupas,2018) menciono que para aplicar la prueba T student se requiere que la muestra no sea mayor a 30. Los resultados que se obtuvieron para la hipótesis especifica 1 se muestran en la siguiente tabla 9.

Prueba de muestras Emparejadas								
Diferencias emparejadas								
				95% de intervalo de confianza de la diferencia		t	gl	Sig (bilateral)
	Media	Desviación	Desv. Error Promedio	Inferior	Superior			
TROUGH_PRE TROUGH_POST	-2,31433	2,09039	0,38165	-3,090490	-1,53377	-6,064	29	0,000

Tabla 9: Prueba T - Troughput

Se obtuvieron de los resultados el nivel de significancia 0,000 que fue menor a 0.05, por lo tanto, se rechaza la hipótesis nula **H1o** y se acepta la hipótesis alternativa **H1a**.

Hipótesis especifica 2

HE2o: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan no mide el Jitter de un sistema PLC con Wifimesh.

HE2a: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Jitter de un sistema PLC con Wifimesh.

Prueba T

Se utilizó la prueba de T debido a que la cantidad de registros fueron menor a 30. Los resultados que se obtuvieron para la hipótesis especifica 2 se muestran en la siguiente tabla 10.

Prueba de muestras Emparejadas								
Diferencias emparejadas								
				95% de intervalo de confianza de la diferencia		t	gl	Sig (bilateral)
	Media	Desviación	Desv.Error Promedio	Inferior	Superior			
JITTER_PRE JITTER_POST	2,20233	2,04797	0,37391	1,43761	2,96706	5,890	29	0,000

Tabla 10: Prueba T - Jitter

Se obtuvieron de los resultados el nivel de significancia 0,000 que fue menor a 0.05, por lo tanto, se rechaza la hipótesis nula **H2o** y se acepta la hipótesis alternativa **H2a**.

Hipótesis especifica 3

HE3o: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan no mide el Retardo extremo a extremo de un sistema PLC con Wifimesh.

HE3a: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Retardo extremo a extremo de un sistema PLC con Wifimesh.

Prueba T

Se utilizó la prueba de T debido a que la cantidad de registros fueron menor a 30. Los resultados que se obtuvieron para la hipótesis especifica 3 se muestran en la siguiente tabla 11,

Prueba de muestras Emparejadas								
Diferencias emparejadas								
				95% de intervalo de confianza de la diferencia		t	gl	Sig (bilateral)
	Media	Desviación	Desv.Error Promedio	Inferior	Superior			
RT_Ex_PRE RT_Ex_POST	6,79933	3,04955	0,55677	5,66061	7,93805	12,212	29	0,000

Tabla 11: Prueba T - Retardo extremo a extremo

Se obtuvieron de los resultados el nivel de significancia 0,000 que fue menor a 0.05, por lo tanto, se rechaza la hipótesis nula **H3o** y se acepta la hipótesis alternativa **H3a**.

Hipótesis especifica 4

HE4o: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan no mide el Nivel de Seguridad de un sistema PLC con Wifimesh.

HE4a: La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Nivel de Seguridad de un sistema PLC con Wifimesh.

Prueba T

Se utilizó la prueba de T debido a que la cantidad de registros fueron menor a 30. Los resultados que se obtuvieron para la hipótesis especifica 3 se muestran en la siguiente tabla 12.

Prueba de una muestra						
Valor de prueba=0						
		95% de intervalo de confianza de la diferencia		t	gl	Sig (bilateral)
	Dif. De Medias	Inferior	Superior			
A_BLOQUEADOS	11566,70000	7590,1832	15543,2168	6,580	9	0,000

Tabla 12: Prueba T - Ataques bloqueados

Se obtuvieron de los resultados el nivel de significancia 0,000 que fue menor a 0.05, por lo tanto, se rechaza la hipótesis nula **H4o** y se acepta la hipótesis alternativa **H4a**.

V. DISCUSION

Después del desarrollo de la investigación y el análisis estadístico, en este capítulo se discute los resultados obtenidos para la evaluación del rendimiento de red en base a los indicadores propuestos, de igual forma se procede con la comparación de investigaciones anteriores que fueron especificadas en nuestro marco teórico.

A través de los resultados se midió el troughput aplicando la metodología propuesta, se comprobó que al implementar tecnología PLC con Wifimesh en una red demostró un incremento en el valor del indicador tasa de datos promedio considerando una diferencia de 2.31 Mbps (megabits por segundo). Estos resultados se asemejan a los presentados por Bahamonde y Segundo (2020), quienes indicaron que PLC demostró un troughput que vario de 0.05 kbs a 0.45 kbs en la aplicación de esta tecnología para mejorar el desempeño de una red en la clínica Quirós Sonar Diagnostico. Cabe resaltar también que PLC proporciona una mejora significativa a toda red ya que es una tecnología que no requiere de mucha infraestructura para emplearla, por otra parte, esta tecnología se desempeña por una tensión eléctrica media o baja. ARROYO, Xavier, et al. (2017) mencionaron que la principal ventaja que presenta plc es mejorar una red wifi común permitiendo velocidades de hasta 1gbps.

Por otra parte, se pudo medir el Jitter a través de la metodología, puesto que se especifica el proceso y el uso del software iperf3 para procesar las pruebas y registrar los valores de medición, así mismo se demostró que al implementar tecnologías plc con wifimesh en una red según nuestro caso de prueba en la empresa bnc servicios generales, se pudo evidenciar una mejora en la variación del tiempo de transmisión mostrando una diferencia de 2 ms (milisegundos). Estos resultados resultan congruentes con la investigación que realizo Benítez (2018), quien demostró en las pruebas que obtuvo para VoIP mediante software Wireshark, que el Jitter es proporcional al número de saltos, del mismo modo represento una variación de 0.639 ms y 0.896 ms en la implementación de un piloto de red wifimesh utilizando nodos en el

A.E.I.R.N.N.R. de la Universidad Nacional de Loja, Ecuador. Es importante mencionar algunas de las ventajas que presenta la tecnología wifimesh entre ellas la continuidad de red y la cobertura que proporciona a una red inalámbrica wlan. MUHENDRA et al. (2017) resaltó que esta tecnología adiciona diferentes estándares de red inalámbrica, también mencionó que los dispositivos de una red wifimesh funcionan como enlace entre varias redes, esto permite que los datos se trasfieran de una y otra de tal manera que si un nodo no funciona el resto mantenga la red disponible sin necesidad de interrumpir la conexión de red inalámbrica.

De igual importancia se logró medir el delay aplicando la metodología y el uso del commandPromt de windows entre otras herramientas. Se obtuvieron resultados favorables demostrando que la implementación de tecnologías PLC y wifimesh en una red mejora el desempeño a través del indicador retardo extremo a extremo, el resultado vario en 6.8 ms (milisegundos), también para el indicador de porcentaje de paquetes perdidos, se obtuvo una diferencia del 0.10 % en las pruebas realizadas pre y postest .En este caso el resultado se asemeja a los presentados por Bahamonde y Segundo (2020), quienes mencionaron en su investigación que el retardo que mostro PLC en la implementación para mejorar el desempeño de una red fue de 18.27 ms a 11.42 ms, demostrando que PLC brinda menor retardo en la transmisión de datos extremo a extremo.

Finalmente, en cuanto al nivel de seguridad se hizo una prueba con ambas tecnologías aplicando la metodología propuesta para demostrar cuál de ellas muestra mayor valor, se pudo diferenciar que PLC mostro mayor significancia en cuanto a los indicadores evaluados cantidad de vulnerabilidades y ataques bloqueados. Estos resultados fueron semejantes a lo mencionado por Motta y Gonzales (2019) quienes indicaron que PLC incluye funciones de seguridad que permite que los usuarios detecten la señal como un ruido por potencia eléctrica, del mismo modo Gómez (2018) resalto que los circuitos son independientes y el acceso a la información se da estando dentro de la propia red eléctrica. Por otra parte, se aplicó también la metodología para evaluar el nivel de seguridad en el caso de estudio en la empresa bcn servicios generales, donde se ejecutó la prueba de fuera bruta a través de Kali Linux y diccionarios para vulnerar la red

inalámbrica, se aplicó más de 1 500 000 solicitudes para penetrar la red mostrando esta una cantidad de 115 667 ataques bloqueados. MUKHERJEE, Aditya (2020) resalto que Kali Linux, es un sistema operativo el cual permite hacer pruebas de penetración ya que cuenta con más de 300 herramientas y las aplicaciones necesarias si se requiera vulnerar una red. Del mismo modo VEGA, Edgar (2020) menciona que el ataque de fuerza bruta muestra un poder de procesamiento el cual permite que las contraseñas puedan ser vulneradas a través de algoritmos.

VI. CONCLUSIONES

A través de los resultados que se obtuvieron del desarrollo del proyecto de investigación se concluyó lo siguiente:

1.Para el primer indicador Retardo extremo a extremo en el pretest resulto 18.06 ms (milisegundos) y después se obtuvo una reducción de retardo a 11.26 ms.

2.En cuanto al indicador porcentaje de paquetes perdidos, mostró una variación del 0.49 a 0.39 %, teniendo como resultado una reducción del 0.10 % de porcentaje de paquetes perdidos.

3.De la igual manera para el troughput la tasa de datos promedio resulto de 7.24 Mbps a 9.55 Mbps, mostrando una diferencia de 2.31 Mbps.

4.En relación al Jitter para el indicador variación de transmisión mejoro de 5.45 ms a 3.25 ms, mostrando una diferencia de 2 milisegundos.

5.Por último, se evaluó el nivel de seguridad en la red inalámbrica de la empresa, aplicando fuerza bruta con un total de 1 500 000 solicitudes se obtuvieron 115 6667 ataques bloqueados, identificando también las vulnerabilidades descritas en la tabla 16.

Finalmente se concluyó que al Implementar la metodología TROUDEJINISE para la evaluación del rendimiento de red en tecnologías inalámbricas WLAN, permitió hacer una evaluación de la red wifi de la empresa BNC Servicios Generales a través de los indicadores retardo extremo, porcentaje de paquetes perdidos, variación de transmisión, tasa de datos promedio, cantidad de vulnerabilidades identificadas y ataques bloqueados, implementando a su vez dos tecnologías inalámbricas PLC y wifimesh, demostrando mejoras en toda la red del negocio.

VII. RECOMENDACIONES

1. Con respecto a la metodología desarrollada se recomienda implementar más indicadores que permitan un análisis más profundo de una red inalámbrica.
2. Se recomienda hacer pruebas con nuevas tecnologías inalámbricas entre ellas LiFi, la tecnología Lifi permite trasferencia de datos a través de la luz.
3. Profundizar más en el nivel de seguridad para implementar nuevos indicadores del mismo modo se pueda auditar redes con soporte tecnológico más avanzado y robustas a su vez.
4. Implementar la metodología en pymes del sector minorista, ya que la metodología especifica cada paso a seguir para identificar las vulnerabilidades más comunes que se puedan encontrar y así evitar la violación de seguridad o perdida de activos.
5. Por ultimo para poder aplicar la metodología en una empresa macro se recomienda agregar nuevos indicadores para el nivel de seguridad así mismo se pueda considerar una evaluación más compleja aplicando un sistema de seguridad de la información SGSI utilizando ISO 27001.

REFERENCIAS

AGURTO, J., HERNANDEZ, M. y HEBER, L., 2016. Aplicación de redes mesh en el área de videovigilancia y ampliación de zonas Wi-Fi en el municipio de San José las Flores, Chalatenango. [en línea], pp. 1-224. Disponible en: https://ri.ues.edu.sv/id/eprint/10356/.

ARROYO RODRÍGUEZ, X., OLIVARES ROJAS, J.C., REYES ARCHUNDIA, E., GUTIERREZ GNECCHI, J.A. y MÉNDEZ PATIÑO, A., 2017. Estudio Comparativo de protocolos de comunicacion de banda estrecha en lineas de potencia. *Academia Journals* [en línea], vol. 9, no. 6, pp. 388-601. Disponible en: http://www.academiajournals.com/publicaciones-celaya/.

AVILES, J. y PACHACAMA, C., 2015. Guía para la Evaluación del Rendimiento de una Red de Datos con Tecnología Ethernet. [en línea], pp. 102. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/11046.

AYON, B., 2020. Universidad Estatal Del Sur De Manabí Facultad De Ciencias Técnicas. [en línea], no. 261, pp. 1-108. Disponible en: http://repositorio.unesum.edu.ec/bitstream/53000/2671/1/CASTRO LINO LUCIA JOSELYN.pdf.

BAHAMONDE, N. y SEGUNDO, R., 2020. *Influencia de Power Line Communications en el desempeño de una red LAN en la clinica Quiros Sonar Diagnostico, La Molina - 2020* [en línea]. S.l.: s.n. ISBN 0000000310. Disponible en: https://hdl.handle.net/20.500.12692/57347.

BARON, S. y PAREDES, G., 2015. MODELO PARA EVALUAR EL RENDIMIENTO DE UNA RED LAN SOBRE PLC EN LA TRANSMISIÓN DE VIDEO BAJO. , vol. 3, no. 7, pp. 59-78.

BENITES, M., 2018. Diseño E Implementación De Un Piloto De Red Wireless Mesh Basada En Firmware Libre Utilizando Nodos 802.11 En El A.E.I.R.N.N.R. De La Universidad Nacional De Loja. [en línea], pp. 1-130. Disponible en: https://dspace.unl.edu.ec/jspui/handle/123456789/20752.

CABRERA, B., 2016. “ANÁLISIS Y DISEÑO DE UNA RED BACHILERATO MIGUEL SÁNCHEZ ASTUDILLO. [en línea], pp. 1-181. Disponible en: https://dspace.unl.edu.ec/jspui/handle/123456789/17208.

CAIZA, C. y LARA, R., 2019. Evaluación del desempeño de la tecnología wifi en concordancia con los estándares IEEE 802.11 b/g/n en el interior de una cámara anecoica para la banda de 2.4 GHz / Performance evaluation of technology Wi-Fi in conformance with IEEE 802.11 b/g/n into an a. *RECI Revista Iberoamericana de las Ciencias Computacionales e Informática*, vol. 8, no. 15, pp. 22-44. ISSN 2007-9915. DOI 10.23913/reci.v8i15.92.

CEDEÑO, C., 2018. Propuesta de implementación de tecnología plc para transmisión de datos de internet en zonas rurales para la provincia del guayas. [en línea], pp. 1-25. Disponible en: http://biblioteca.uteg.edu.ec:8080/handle/123456789/83.

CEPAL, 2020. La Digitalización En América Latina Frente Al Covid-19. *Cepal Caf Elac*, pp. 2-33.

CHAPMAN, C., 2016. *Traffic performance testing in the network*. S.l.: s.n. ISBN 9780128035849.

CHAUCA, J., 2016. Diseño de una red convergente de comunicaciones de voz y datos para la empresa agroindustrial AVOCADO PACKING COMPANY S.A. - sede CHAO. *Universidad Privada Antenor Orrego* [en línea], ISSN T046_70821784T. Disponible en: http://repositorio.upao.edu.pe/handle/upaorep/3668.

CHUQUICONDOR, Y., 2017. “PROPUESTA METODOLÓGICA PARA LA GESTIÓN Y ADMINISTRACIÓN DEL ANCHO DE BANDA DE COMUNICACIONES EN EL CAMPUS DE LA UNIVERSIDAD NACIONAL DE PIURA – 2016. ,

CISCO, 2011. *Top-Down Network Design*. S.l.: s.n. ISBN 9781587202834.

DELOITTE, 2017. Wireless Connectivity Fuels Industry Growth and Innovation. , no. January.

DENG, X., HE, T., HE, L., GUI, J. y PENG, Q., 2017. Performance Analysis for IEEE 802.11s Wireless Mesh Network in Smart Grid. *Wireless Personal Communications*, vol. 96, no. 1, pp. 1537-1555. ISSN 1572834X. DOI 10.1007/s11277-017-4255-7.

DOMÍNGUEZ, H., MAYA, E., PELUFFO, D. y CRISANTO, C., 2017. Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple "Contraseñas", pruebas de concepto con software libre y su remediación. *Maskana*, vol. 7, no. Supl., pp. 87-95. ISSN 2477-8893.

ERAZO GUERRA, P., 2016. "Propuesta De Metodología Para La Implementación De Proyectos De Redes – Caso De Estudio Institución Financiera Local. , pp. 258.

FERREIRA, J.C., GRANADOS, G. y VESGA, J.A., 2016. Evaluación del rendimiento de una red LAN sobre power line communications para la transmisión de VOIP. *Iteckne*, vol. 13, no. 1, pp. 83-95. ISSN 1692-1798. DOI 10.15332/iteckne.v13i1.1385.

GALLARDO, E., 2017. Metodología de la Investigación. Manual Autoformativo Interactivo I. *Universidad Continental* [en línea], vol. 1, pp. 98. Disponible en: https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf.

GARCÍA CASTAÑO, D.A., MOSQUERA TABORDA, G.M. y PÉREZ MÚNERA, M.Y., 2018. Modelo de optimización de la red Wifi en el politécnico Grancolombiano sede Medellín. [en línea], pp. 1-51. Disponible en: http://hdl.handle.net/10823/1397.

GARCIA, D. y MORAN, L., 2016. REDES INALÁMBRICAS; ESTUDIO DEL COMPORTAMIENTO, RENDIMIENTO Y MIGRACIÓN DEL ESTÁNDAR DE COMUNICACIÓN 802.11AC. , no. PROYECTO DE FACTIBILIDAD TÉCNICA, ECONÓMICA Y FINANCIERA DEL CULTIVO DE OSTRA DEL PACÍFICO EN LA PARROQUIA MANGLARALTO, CANTÓN SANTA ELENA, PROVINCIA DE SANTA ELENA, pp. 136.

GOMEZ, J., 2018. Definición y Aplicación de PJON-PLC para Redes de Sensores. *ASEE Annual Conference and Exposition, Conference Proceedings*,

GRAJALES, H., 2019. Diseño de red inalámbrica para la Escuela de Artes y Comunicaciones basada en la metodología Top-Down Network Design. ,

GRANIZO, A. y TACURI, A., 2017. Guía referencial para el manejo de QoS en redes WLAN prioritizando tráfico. *Maskana*, vol. 7, no. Supl., pp. 65-77. ISSN 2477-8893.

HERNANDEZ, R. y MENDOZA, C., 2018. *Metodología De La Investigación : Las Rutas Cuantitativa* , [en línea]. S.l.: s.n. ISBN 9781456260965. Disponible en: https://www.academia.edu/43711980/METODOLOGÍA_DE_LA_INVESTIGACIÓN_LAS_RUTAS_CUANTITATIVA_CUALITATIVA_Y_MIXTA.

HERRERA, H., 2018. Modelo de optimización de rendimiento en redes 802.11ac utilizando programación multi-objetivo. [en línea], pp. 97. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/14493/1/HerreraHerreraHectorManuel2019.pdf.

LI, K., WANG, R., LI, H. y HAO, Y., 2021. A Network Attack Blocking Scheme based on Threat Intelligence. *2021 IEEE 6th International Conference on Intelligent Computing and Signal Processing, ICSP 2021*, no. Icsp, pp. 976-980. DOI 10.1109/ICSP51882.2021.9408916.

MARÍN, A., 2014. Evaluación experimental de QoE / QoS en redes inalámbricas 802.11. , pp. 90.

MCCABE, J.D., 2007. *Network Analysis, Architecture, and Design, Third Edition* [en línea]. S.l.: s.n. ISBN 0123704804. Disponible en: http://www.amazon.com/dp/0123704804.

MENDOZA, C., 2021. Diseño de red inalámbrica para una compañía del sector minero. [en línea], pp. 1-119. Disponible en: https://ri.ues.edu.sv/id/eprint/10356/.

MONTOYA, M., 2017. Evaluación de los diferentes tipos de modulaciones para sistemas PLC empleados en las redes energéticas inteligentes (Smart Grids). , pp. 1-23.

MOTTA, A. y GONZALES, D., 2019. Implementación de un sistema de comunicación por líneas de potencia (PLC) para su uso en redes inteligentes de distribución. [en línea], Disponible en: https://ciencia.lasalle.edu.co/ing_electrica.

MOTTA, A. y GONZALEZ, D., 2019. Implementación de un sistema de comunicación por líneas de potencia (PLC) para su uso en redes inteligentes de distribución. [en línea], Disponible en: https://ciencia.lasalle.edu.co/ing_electrica.

MUHENDRA, R. y ARZI, Y.H., 2017. Development of street lights controller using wifi mesh network. *Proceeding of 2017 International Conference on Smart Cities,*

Automation and Intelligent Computing Systems, ICON-SONICS 2017, vol. 2018-Janua, pp. 105-109. DOI 10.1109/ICON-SONICS.2017.8267830.

MUHENDRA, R., RINALDI, A., BUDIMAN, M. y KHAIRURRIJAL, 2017. Development of WiFi Mesh Infrastructure for Internet of Things Applications. *Procedia Engineering* [en línea], vol. 170, pp. 332-337. ISSN 18777058. DOI 10.1016/j.proeng.2017.03.045. Disponible en: http://dx.doi.org/10.1016/j.proeng.2017.03.045.

MUKHERJEE, A., 2020. *Network Security Strategies*. BIRMINGHAM - MUMBAI: 2020. ISBN 9781789806298.

NARANJO, J., 2016. Estudio comparativo de factibilidad del uso de herramientas de Control de Dispositivos y Servicios de Red de Datos mediante el Protocolo SNMP y Software Libre . Previa a la obtención del Título de : INGENIERO EN NETWORKING Y TELECOMUNICACIONES AUTOR : JOR. , pp. 149.

ÑAUPAS, H., PALACIOS, J., VALDIVIA, M. y ROMERO, H., 2018. *Metodologia de la investigacion*. S.l.: s.n. ISBN 9789587628760.

OLIVERA, R. y ALVAREZ, F., 2018. Basado En Tiempos De Contención Quality of Service in Wlan Networks Using Medium Access. , vol. 17, no. 3, pp. 55-64.

PEREIRA, A., 2017. Propuesta De Optimizacion De La Infrastructura De Telecomunicaciones Corporativa Basada En La Metodologia Top-Down De Cisco Juliette. *Journal of Chemical Information and Modeling*, vol. 1, no. 9, pp. 71. ISSN 1098-6596.

PETTERSON, L. y BRUCE, D., 2003. *Computer Network - A System Approach*. S.l.: s.n. ISBN 155860832X.

PONCE, D. y SANTILLAN, S., 2016. Diseño E Implementacion De Un Sistema De Transferencia De Datos a Través De La Red Electrica De Baja Tension Con La Interfaz Labview-Arduino Empleando La Tecnologia Power Line Communications (Plc). , pp. 214.

PRIETO, J. y DE LA ORDEN HOZ, A., 2017. Metodología de la investigación. [en línea], pp. 216. Disponible en: https://issuu.com/maiquim.floresm./docs/259310380-metodologia-de-la-investi.

QUIROZ, S. y MACIAS, D., 2017. Seguridad en informática: consideraciones. *Dominio de las Ciencias*, vol. 3, no. 3, pp. 676-688. ISSN 2477-8818.

QUISPE, A., CALLA, K., YANGALI, J. y RODRÍGUEZ, J., 2019. *Estadística no paramétrica aplicada a la investigación científica c on software SPSS , MINITAB Y EXCEL Enfoque práctico*. S.l.: s.n. ISBN 9789585203099.

RAMIREZ, M., 2020. *PROPUESTA DE IMPLEMENTACIÓN DE LA RED DE DATOS EN LA EMPRESA M3 INGENIERÍA PERÚ S.A.C. - AREQUIPA; 2020.* [en línea]. S.l.: s.n. ISBN 9789586991285. Disponible en: http://repositorio.unan.edu.ni/2986/1/5624.pdf.

RAYES, A. y SALAM, S., 2020. *Internet of Things: from hype to reality*. S.l.: s.n. ISBN 9783319995151.

REGES BESSA, C.D., SOARES SEMENTE, R., CAVALCANTE BENJAMIM, X., CORREIA DE MELO, T.A., MENDONÇA DE OLIVEIRA, F.D., HOLANDA NORONHA, D., EDUARDO DE MORAIS SILVA, A., LAURINDO MAITELLI, A. y ORTIZ SALAZAR, A., 2016. Performance Evaluation Analysis of Wireless Sensor Networks Routing Protocols in Smart Grids. *Revista Cientifica TECNIA*, vol. 26, no. 1, pp. 17. ISSN 0375-7765. DOI 10.21754/tecnia.v26i1.2.

RODRIGUES, O., DUTARI, R., CEDEÑO, E. y NORBERTO, H., 2018. Nivel de seguridad de las redes de área local en algunas instituciones públicas que funcionan en la ciudad de Santiago , provincia de Veraguas . Security level of local area networks in some public institutions operating in the Head District of Santiago ,. , vol. 2, no. 1, pp. 1-15.

SALDAÑA, M., 2016. Pruebas de bondad de ajuste a una distribución normal. *Enfermería del Trabajo*, vol. 6, no. 3, pp. 105-114. ISSN 2174-2510.

SARANGAPANI, J., 2007. *Wireless Ad Hoc and Sensor*. S.l.: s.n. ISBN 9780824726751.

SKENDZIC, A., KOVACIC, B. y LJUBICIC, L., 2020. Performance analysis of aruba wireless local network in croatian pension insurance institute. *2020 43rd International Convention on Information, Communication and Electronic Technology, MIPRO 2020 - Proceedings*, pp. 1397-1401. DOI 10.23919/MIPRO48935.2020.9245371.

SREENIVASULU, T. SHAHEEN, H. HIMABINDU, E. RAJASEKAR, R., 2018. *Data Comunications and Computer Networks*. S.l.: s.n. ISBN 9789387610170.

TAVARA, J.C., 2016. ANALISIS DE CALIDAD DE SERVICIO EN REDES IPv6. *Revista Cientifica TECNIA*, vol. 26, no. 1, pp. 7. ISSN 0375-7765. DOI 10.21754/tecnia.v26i1.1.

URIBE, M. y GARCIA, J., 2016. Transmicion de Datos a traves de Redes PLC. ,

VEGA, E., 2020. *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking*. S.l.: s.n. ISBN 9788412145946.

VLACHOU, C., HENRI, S. y THIRAN, P., 2016. Electri-Fi your data: Measuring and combining power-line communications with WiFi. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, vol. 2016-Octob, pp. 325-338. DOI 10.1145/2815675.2815689.

YUNQUERA, J.J., 2015. Diseño de una Red WI-FI para la E.S.I. *Universidad de Sevilla* [en línea], pp. 36-51. Disponible en: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCapítulo+3.pdf+%7C.

ZAPATA, A., 2016. MAESTRÍA EN REDES DE COMUNICACIÓN TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE : MASTER EN REDES DE COMUNICACIÓN TEMA : MIROSLAVA ARACELY ZAPATA RODRÍGUEZ DIRECTOR : MsC . Francisco Chafla . Quito , Marzo 2016 Dedicatoria. ,

ANEXOS

Anexo 1. Matriz De Operacionalización de Variables

Metodología TROUDEJINISE para la evaluación del rendimiento de red en tecnologías Inalámbricas WLAN

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	INSTRUMENTO	ESCALA DE MEDICIÓN
Rendimiento de red	La cantidad del trabajo realizado en una unidad de tiempo se conoce como rendimiento. El rendimiento de una red se puede determinar considerando algunos factores como tiempo de tránsito, tiempo de respuesta y retraso. **(ITL Education Solutions Limited, Dorling Kindersley (2016)**	Entre los parámetros para la evaluación del rendimiento de una red se mencionan Throughput, latencia, jitter y el porcentaje de paquetes perdidos **(Vesga, Granados y Barrera, 2016)**	Jitter	Variación de Tiempo de transmisión **(Petterson y Bruce 2003)**	Ficha de Registro	De Razón
			Throughput	Tasa de Datos Promedio **(Petterson y Bruce 2003)**	Ficha de Registro	De Razón
			Delay	Porcentaje de Paquetes Perdidos **(Sarangapani 2007)**	Ficha de Registro	De Razón
				Retardo de extremo a extremo **(Rayes y Salam 2020)**	Ficha de Registro	De Razón
			Nivel de Seguridad	Cantidad de Vulnerabilidades Identificadas **(Vega 2020)**	Ficha de Registro	De Razón
				Ataques Bloqueados **(Li et al. 2021)**	Ficha de Registro	De Razón

Anexo 2. Matriz De Consistencia de Variables

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES	METODOS Y TECNICAS DE INVESTIGACION
PROBLEMA GENERAL Cuál es el resultado de implementar una metodología para evaluar el rendimiento de red en tecnologías inalámbricas wlan. **PROBLEMAS ESPECIFICOS** **1.** Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Throughput en un sistema PLC con WifiMesh **2.** Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Jitter en un sistema PLC con WifiMesh **3.** Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Delay en un sistema PLC con WifiMesh **4.** Cuál es la influencia de implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Nivel de Seguridad en un sistema PLC con WifiMesh	**OBJETIVO GENERAL** Implementar una metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan. **OBJETIVOS ESPECIFICOS** 1. Determinar la influencia al aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Throughput de un sistema PLC con WifiMesh 2. Determinar la influencia al aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Jitter de un sistema PLC con WifiMesh 3. Determinar la influencia al aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Delay de un sistema PLC con WifiMesh 4. Determinar la influencia al aplicar la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan en función al Nivel de seguridad de un sistema PLC con WifiMesh	**HIPÓTESIS GENERAL** La implementación de una metodología permite la evaluación del rendimiento de red en tecnologías inalámbricas wlan. **HIPÓTESIS ESPECIFICOS** **H1:** La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el troughput de un sistema PLC con WifiMesh **H2:** La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Jitter de un sistema PLC con Wifimesh **H3:** La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el retardo extremo a extremo de un sistema PLC con Wifimesh **H4:** La aplicación de la metodología para la evaluación del rendimiento de red en tecnologías inalámbricas wlan mide el Nivel de Seguridad de un sistema PLC con Wifimesh	**VARIABLE** **V. Rendimiento de red** **D1. Jitter** **D2. Throughput** **D3. Delay** **D4. Nivel de Seguridad** Indicadores: **D1.** Jitter 1. Variación de Tiempo de Transmisión **D2.** Throughput 2. Tasa de Datos Promedio 3. **D3.** Delay Porcentaje de paquetes perdidos Retardo extremo a extremo 4. **D4.** Nivel de Seguridad Cantidad de Vulnerabilidades Identificadas Ataques Bloqueados	**Métodos:** **Tipo:** Aplicada **Enfoque:** Cuantitativo **Diseño:** Experimental– Pre Experimental **Población:** **30 registros de rendimiento** Que emplean tecnologías inalámbricas WLAN **Muestra:** **30 registros de rendimiento WifiMesh y PLC**

Anexo 3. Instrumento de recolección de datos

Ficha de Registro			
Investigadores	Maldonado Jiménez Pablo Enrique	**Prueba**	**Pretest**
Herramientas	commandPront Windows.		
Motivo de Estudio	**Retardo Extremo a Extremo**		
Fecha de Inicio	**09/ 06 / 2021**	**Fecha Final**	**09/ 06 / 2022**

Variable	Indicador	Simbología de Formula	Formula
Rendimiento de la Red	**Retardo Extremo a Extremo**	DT: Demora total dp: Demora de Procesamiento. de: Demora de espera dt: Demora de Transmisión dy: Demora de Propagación	$DT = dp + de + dt + dy$

Ítem	Hora	Demora de Procesamiento	Demora de Espera	Demora de Transmisión	Demora de Propagación	Formula
1	10:05 am	3	5.20	3.54	7.20	18.94
2	10:10 am	2	4.07	4.45	6.70	17.22
3	10:15 am	2	4	2.36	6.70	15.06
4	10:20 am	3	3.30	6.75	8.60	21.65
5	10:25 am	3	3.40	8.63	6.60	21.63
6	10:30 am	3	3.60	9.42	6.20	22.22
7	10:35 am	3	5.80	6.32	8.20	23.32
8	10:40 am	2	5.75	5.75	7.20	21.7
9	10:45 am	2	3.35	4.73	5.20	15.28
10	10:50 am	3	2.24	2.55	7.80	14.59
11	10:55 am	2	3.65	7.32	6.20	20.17
12	11:00 am	2	3.35	6.40	5.20	16.95
13	11:05 am	2	3.63	5.65	5.50	16.78
14	11:10 am	3	2.25	4.23	6.30	15.78
15	11:15 am	2	6.85	8.14	8.60	25.59
16	11:20 am	3	3.25	7.34	6.60	20.19
17	11:25 am	2	3.15	6.25	7.20	18.6
18	11:30 am	3	3.20	5.85	5.60	17.65
19	11:35 am	3	3.25	3.20	6.80	16.25
20	11:40 am	2	5.20	4.55	6.20	17.95
21	11:45 am	2	3.50	3.45	8.20	17.15
22	11:50 am	3	4.85	2.85	8.60	19.3
23	11:55 am	3	3.54	2.68	6.10	15.32
24	12:00 pm	2	2.58	3.15	5.60	13.33
25	12:05 pm	1	3.45	3.23	7.00	14.68
26	12:10 pm	2	3.10	4.80	6.20	16.1
27	12:15 pm	3	2.65	5.65	4.60	15.9
28	12:20 pm	2	5.35	3.25	5.10	15.7
29	12:25 pm	3	6.24	4.45	6.20	19.89
30	12:30 pm	3	2.00	3.70	8.10	16.8
	PROMEDIO TOTAL					**18.06 ms**

Ficha de Registro			
Investigador	Maldonado Jiménez Pablo Enrique	**Prueba**	**Pre Test**
Herramientas	Iperf, commandPront Windows.		
Motivo de Estudio	**Porcentaje de Paquetes Pedidos**		
Fecha de Inicio	**09 /06 / 2021**	**Fecha Final**	**09/ 06 / 2022**

Variable	Indicador	Simbología de Formula	Formula
Rendimiento de la Red	**Porcentaje de Paquetes Pedidos**	**PLR:** Porcentaje de paquetes perdidos	$PLR = \frac{\text{total number of packets loss}}{\text{total number of packets sent}} \times 100\%$

Ítem	Hora	Total de Paquetes Perdidos	Total de Paquetes Enviados	Formula
1	10:05 am	0.0	389	0.00 %
2	10:10 am	3.0	244	1.22 %
3	10:15 am	1.0	329	0.30 %
4	10:20 am	3.0	225	1.33 %
5	10:25 am	2.0	284	0.70 %
6	10:30 am	0.0	317	0.00 %
7	10:35 am	1.0	272	0.36 %
8	10:40 am	4.0	323	1.23 %
9	10:45 am	1.0	384	0.26 %
10	10:50 am	0.0	281	0.00 %
11	10:55 am	1.0	336	0.29 %
12	11:00 am	2.0	305	0.65 %
13	11:05 am	3.0	365	0.82 %
14	11:10 am	2.0	282	0.70 %
15	11:15 am	3.0	354	0.84 %
16	11:20 am	2.0	278	0.71 %
17	11:25 am	2.0	360	0.55 %
18	11:30 am	1.0	345	0.28 %
19	11:35 am	0.0	365	0.00 %
20	11:40 am	2.0	327	0.61 %
21	11:45 am	1.0	289	0.34 %
22	11:50 am	2.0	315	0.63 %
23	11:55 am	3.0	368	0.81 %
24	12:00 pm	0.0	348	0.00 %
25	12:05 pm	2.0	298	0.67 %
26	12:10 pm	2.0	304	0.65 %
27	12:15 pm	1.0	298	0.33 %
28	12:20 pm	0.0	278	0.00 %
29	12:25 pm	1.0	345	0.28 %
30	12:30 pm	2.0	268	0.74 %
TOTAL PROMEDIO				**0.49 %**

Ficha de Registro			
Investigadores	Maldonado Jiménez Pablo Enrique	**Prueba**	**Pre Test**
Herramientas	Iperf, commandPront Windows.		
Motivo de Estudio	**Jitter**		
Fecha de Inicio	**09 /06 / 2022**	**Fecha Final**	**09/ 06 / 2022**

Variable	Indicador	Simbología de Formula	Formula
Rendimiento de la Red	**Jitter**	Δt_i : Variación de Tiempo de transmisión t_i : Tiempo de transmisión de paquete	$\Delta t_i = t_i - t_{i-1}, donde\ i = 1, 2 \ldots . N$

Ítem	Hora	Tiempos de Transmisión (Ti) ms	Tiempo de Transmisión (Ti-1) ms	Formula
1	10:05 am	28.654	22.325	6.33
2	10:10 am	30.420	22.244	8.18
3	10:15 am	27.542	21.456	6.09
4	10:20 am	26.543	20.142	6.40
5	10:25 am	25.123	19.541	5.58
6	10:30 am	28.146	23.871	4.28
7	10:35 am	25.456	20.487	4.97
8	10:40 am	26.542	21.984	4.56
9	10:45 am	28.654	22.471	6.18
10	10:50 am	27.244	21.812	5.43
11	10:55 am	29.342	23.644	5.70
12	11:00 am	25.554	21.465	4.09
13	11:05 am	23.244	18.862	4.38
14	11:10 am	23.689	17.246	6.44
15	11:15 am	26.145	19.174	6.97
16	11:20 am	25.354	20.985	4.37
17	11:25 am	27.952	23.684	4.27
18	11:30 am	28.347	22.453	5.89
19	11:35 am	25.341	19.546	5.80
20	11:40 am	24.213	19.210	5.00
21	11:45 am	25.345	20.985	4.36
22	11:50 am	30.458	24.687	5.77
23	11:55 am	26.741	20.648	6.09
24	12:00 pm	25.574	19.795	5.78
25	12:05 pm	25.456	18.679	6.78
26	12:10 pm	30.542	22.987	7.56
27	12:15 pm	29.213	23.325	5.69
28	12:20 pm	28.987	25.697	3.29
29	12:25 pm	27.648	23.795	3.85
30	12:30 pm	26.745	23.287	3.46
	TOTAL	**Jitter PROMEDIO**		**5.45 ms**

Ficha de Registro			
Investigador	Maldonado Jiménez Pablo Enrique	**Prueba**	**Pre Test**
Herramientas	Iperf, commandPront Windows.		
Motivo de Estudio	**Throughput**		
Fecha de Inicio	**09 /06 / 2022**	**Fecha Final**	**09/06 / 2022**

Variable	Indicador	Simbología de Formula	Formula
Rendimiento de la Red	**Throughput**	**TransferSize:** Cantidad de datos (en Mbts) **Transfer Time:** Tiempo (en segundos)	$\boldsymbol{Throughtput} = \frac{TransferSize}{TransferTime}$

Ítem	Hora	Cantidad de Datos (Mbts)	Tiempo (Segundos)	Formula
1	10:05 am	2530.20	300	8.43
2	10:10 am	2825.10	300	9.42
3	10:15 am	2720.35	300	9.07
4	10:20 am	2540.20	300	8.47
5	10:25 am	1504.20	300	5.01
6	10:30 am	1897.10	300	6.32
7	10:35 am	2340.30	300	7.80
8	10:40 am	2468.10	300	8.23
9	10:45 am	1464.35	300	4.88
10	10:50 am	2560.25	300	8.53
11	10:55 am	1320.15	300	4.40
12	11:00 am	1203.30	300	4.01
13	11:05 am	2350.20	300	7.83
14	11:10 am	2152.40	300	7.17
15	11:15 am	1785.20	300	5.95
16	11:20 am	1435.15	300	4.78
17	11:25 am	2456.30	300	8.19
18	11:30 am	2235.60	300	7.45
19	11:35 am	2843.40	300	9.48
20	11:40 am	1654.30	300	5.51
21	11:45 am	2624.20	300	8.75
22	11:50 am	2513.65	300	8.38
23	11:55 am	1745.20	300	5.62
24	12:00 pm	1550.45	300	5.17
25	12:05 pm	2650.20	300	8.83
26	12:10 pm	3124.10	300	10.41
27	12:15 pm	2354.20	300	7.85
28	12:20 pm	1540.15	300	5.13
29	12:25 pm	2137.35	300	7.13
30	12:30 pm	2687.20	300	8.96
Promedio				**7.24 Mbps**

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE RENDIMIENTO DE RED

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: Variación de Tiempo de transmisión	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	$\Delta t_i = t_i - t_{i-1}$, $donde\ i = 1, 2 \ldots . N$	X		X		X		
	INDICADOR: Tasa de Datos Promedio	**Si**	**No**	**Si**	**No**	**Si**	**No**	
2	$\boldsymbol{Throughtput} = \frac{TransferSize}{TransferTime}$	X		X		X		
	INDICADOR: Porcentaje de Paquetes Perdidos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	$PLR = \frac{Total\ number\ of\ paquets\ loss}{Total\ number\ of\ paquets\ sent}\ x100\%$	X		X		X		
	INDICADOR: Retardo de extremo a extremo	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	$\boldsymbol{DT} = dp + de + dt + dy$	X		X		X		
	INDICADOR : Cantidad de Vulnerabilidades	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	$\boldsymbol{Number\ of\ Vulnerabilities} = V.Logical + V.Physical$	X		X		X		

Observaciones (precisar si hay suficiencia): -------, existe suficiencia en el instrumento

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. .....Daniel Angeles Pinillos.....

Especialidad del validador.....Gestión de Tecnologías de Información.....

30 de mayo del 2022

[1]**Pertinencia:**El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE RENDIMIENTO DE RED

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	INDICADOR: Variación de Tiempo de transmisión	Si	No	Si	No	Si	No	
1	$\Delta t_i = t_i - t_{i-1}$, $donde\ i = 1, 2 \ldots . N$	x		x		x		
	INDICADOR: Tasa de Datos Promedio	Si	No	Si	No	Si	No	
2	$\boldsymbol{Throughtput} = \frac{TransferSize}{TransferTime}$	x		x		x		
	INDICADOR: Porcentaje de Paquetes Perdidos	Si	No	Si	No	Si	No	
3	$PLR = \frac{Total\ number\ of\ paquets\ loss}{Total\ number\ of\ paquets\ sent}\ x100\%$	x		x		x		
	INDICADOR: Retardo de extremo a extremo	Si	No	Si	No	Si	No	
4	$\boldsymbol{DT} = dp + de + dt + dy$	x		x		x		
	INDICADOR : Cantidad de Vulnerabilidades	Si	No	Si	No	Si	No	
5	$\boldsymbol{Number\ of\ Vulnerabilities} = V.Logical + V.Physical$	x		x		x		

Observaciones (precisar si hay suficiencia): -------, existe suficiencia en el instrumento

Opinión de aplicabilidad: **Aplicable [...x.....]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Mg. MENENDEZ MUERAS ROSA

Especialidad del validador Ingeniería de sistemas

25 de Junio del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Ficha de Registro			
Investigadores	Maldonado Jiménez Pablo Enrique	Prueba	Post Test
Herramientas	Kali Linux – Aircrack-ng		
Indicador	Ataques Bloqueados		
Fecha	16/06/2022	Proceso	Ataque por Fuerza Bruta

Ítem	Hora	Cantidad de Solicitudes	Red Wifi Ataques bloqueados
1	13:00 pm	150 000	18541
2	13:30 pm	150 000	21456
3	14:00 pm	150 000	12524
4	14:30 pm	150 000	8541
5	15:00 pm	150 000	10543
6	15:30 pm	150 000	10874
7	16:00 pm	150 000	7982
8	16:30 pm	150 000	4233
9	17:00 pm	150 000	5432
10	17:30 pm	150 000	15541
TOTAL	4hrs 30 min	1 500 000	115667

Anexo 4. Metodologías para Desarrollo de la Metodología Propuesta

A continuación, se mostrará los métodos que se usaron para formar la metodología propuesta para la evaluación de las tecnologías inalámbricas.

1 Metodología para el Diseño e Implementación de Redes TOP DOWN

La metodología Top Down se enfoca en el diseño e implementación de un proyecto de red LAN o inalámbrica. (Grajales 2019) " Mencionó que Top Down Network Desing permite centrarse en las necesidades y peticiones de las redes de comunicación el cual deben tenerse en cuenta antes de la selección de los equipos para implementar una red física" (p.5). (Pereira 2017) Indico el propósito de esta metodología es colaborar en el diseño de redes que cumplan con los objetivos empresariales y técnicos de diferentes áreas o instituciones. Brinda procesos y herramientas para cumplir con las condiciones técnicas en cuanto a la funcionalidad, disponibilidad, escalabilidad, accesibilidad y seguridad.

Del mismo modo (CISCO 2011) menciono que "cuando un cliente solicita una respuesta inmediata de un diseño de red se puede emplear la metodología de redes siempre y cuando los objetivos y requisitos estén bien definidos"(p.4) , sin embargo, la mayoría de diseñadores de red piensan que comprenden los requerimientos del cliente solo por propia experiencia, después de instalar la red se percatan de no haber captado las necesidades más importantes, a lo largo que la red abarque más usuarios empiezan a aparecer los problemas de escalabilidad y rendimiento.

Esta metodología propone cuatro fases para el diseño e implementación de una red 1) Identificación de Necesidades, 2) Diseño Lógico, 3) Diseño Físico, 4) Documentación de la red.

Primera Fase: En esta fase se identifica los requisitos y necesidades del cliente o negocio del mismo modo las limitaciones.(CISCO 2011)

- Análisis de Objetivos y Requisitos del Negocio
- Objetivos técnicos y Limitaciones
- Características de la Red
- Características del tráfico de Red

Segunda Fase: En esta Fase se determina la topología de red, el direccionamiento además se selecciona los protocolos de conexión hacia los dispositivos interconectados. (CISCO 2011)

- Topología de la red
- Modelo de direccionamiento y Nombramiento
- Selección de Protocolos
- Estrategias de Gestión de red

Tercera Fase: En esta fase se selecciona las tecnologías y equipos con el cual se implementará la red que cumplan con los requerimientos técnicos de acuerdo al diseño lógico propuesto.(CISCO 2011)

- Cableado Estructurado
- Tecnologías LAN, WLAN, entre otras.
- Dispositivos finales (HOST)

Cuarta Fase: Esta fase abarca la documentación del diseño y estructura de red además de la respuesta hacia los requerimientos del cliente u organización.

METODOLOGIAS PARA DISEÑO E IMPLEMENTACION DE RED			
FASES	**TOP DOWN**	**PDDIOD**	**JAMES MACCABE**
Análisis	Analizar Requerimientos	Fase de Planificación	Análisis de Situación Actual
Diseño	Desarrollar Diseño Lógico y Diseño Físico	Fase de Diseño	Determinar Requerimientos
Implementación	Probar y documentar red	Fase de Implementación	Análisis de Necesidades de Sistema
Desarrollo	Implementar y probar	Fase de Operación	Construcción
Control	Monitorear y Optimizar	Fase de Optimización	-
Rendimiento y Seguridad	-	-	-

Tabla 13. Metodologías para el diseño e implementación de red

En la tabla 12 se visualiza las diferentes metodologías que existen para la implementación y diseño de una red entre las más recientes encontramos a TOP DOWN propuesta por CISCO, consta de 5 fases y es la más completa para diseñar e implementar una red. Se puede evidenciar que entre las metodologías estudiadas carecen de una fase que permita evaluar el rendimiento y seguridad, por ello se propone la metodología “TROUDEJINISE” que considera implementar las pruebas correspondientes para el rendimiento, pruebas para cantidad de vulnerabilidades, cantidad de ataques bloqueados y fuerza bruta.

2 Pruebas de Rendimiento de Red

Las pruebas de rendimiento de una red consisten en medir los parámetros que implican para garantizar una transición de datos de forma segura y efectiva. El rendimiento de una red está relacionado con la seguridad en la forma de reducir los riesgos y ataques que se encuentre expuesta, del mismo modo a la calidad de la experiencia del usuario (Chapman 2016). El rendimiento de la red implica varios indicadores. (Reges Bessa et al. 2016) indicaron los siguientes:

Perdida de Paquetes: La pérdida de paquetes consiste en la cantidad de paquetes que no llegan hacia su destino, en las redes inalámbricas el causante principal son las interferencias que existes en el medio de trasmisión o saturación de los canales en las frecuencias 2.4 Ghz o 5GHz.

Throughput: Para determinar el Troughput se mide en términos de éxitos entrega de paquetes de datos dentro de un tiempo límite (Reges Bessa et al. 2016), esto se mide utilizando el número de bits del paquete recibido por unidad de tiempo en segundos.

Delay: Este parámetro se utiliza para medir el rendimiento con el tiempo que tarda un paquete en viajar a través de la red desde un nodo inicial hasta el nodo destino, evalúa la latencia entre datos.

Jitter: Se define como la variación de retardos de paquetes. (Caiza y Lara 2019) resaltaron que el retraso de paquetes sucesivos es constante, entonces no hay

daño, pero si los paquetes se reciben en intervalos de tiempo irregulares entre ellos el resultado puede ser inaceptable.

3 Metodología para Evaluaciones de Seguridad

Cuando se hace referencia a procesos de evaluación de seguridad es indispensable llevar a cabo una selección de procedimientos completos que permitan identificar los objetivos, garantizar la afinidad y estructura de la evaluación, disminuir los riesgos y comunicar adecuadamente los resultados.

(Vega 2020) Mencionó que la metodología a utilizar tiene que contemplar aspectos que hagan referencia a las siguientes Etapas:

a) **Planificación y Preparación:** En esta fase se lleva a cabo las entrevistas reuniones laborales en el cual se determinan los objetivos y propósitos así mismo se trazan las expectativas y se presenta al equipo de trabajo.

- Definición de Objetivos
- Horarios y medidas de contingencias
- Equipo de Trabajo

b) **Especificación de una Evaluación de Seguridad:** Según la definición de objetivos y posición en la que se ubiquen los analistas de seguridad, se podrán emplear diferentes técnicas (Vega 2020).También resalto que se debe considerar si se desea analizar la infraestructura, las aplicaciones, una base de datos o todo en general. Se considera los siguientes puntos:

- Evaluación de la red
- Evaluación de equipos o host
- Evaluación de la seguridad física
- Análisis de Vulnerabilidades
- Pruebas de Intrusión

c) **Ejecución de Tareas:** (Vega 2020) Indico para esta etapa los siguientes puntos a considerar:

- Reconocimiento
- Técnicas y Herramientas
- Escaneo de Puertos

- Escaneo de Servicios

d) Caracterización de Vulnerabilidades: "El objetivo de esta etapa es determinar las posibles rutas que tendría un intruso malicioso para atacar. Como resultado se obtendrá una lista de las vulnerabilidades asociadas a los sistemas y procedimientos, que puedan ser explotadas por fuentes de amenaza".(Vega 2020)(p.70). Se comprende por vulnerabilidad una característica o circunstancia de debilidad de un recurso informático la cual es expuesta de ser explotada por una amenaza (Quiroz y Macias 2017).

Se considera los siguientes puntos:

- Identificación de Vulnerabilidades
- Clasificación de Vulnerabilidades
- Lista de requerimientos
- Herramientas automáticas
- **Explotación de Vulnerabilidades:** El principal objetivo es comprobar o refutar el impacto potencial de las vulnerabilidades detectadas. Se considera a) Generalidades, b) Ejecución (Vega 2020).

e) Informe de Evaluación de Seguridad: (Vega 2020)Resalto que en esta fase se consolida el proceso sistemático, planificado y técnicamente bien ejecutado por el coordinador profesional, puesto que la documentación constituye la relación entre los resultados de las fases anteriores.

- Resumen y Análisis General
- Riesgos detectados y clasificados
- Evidencias y documentos Generados

4 Prueba de Fuerza Bruta

En la prueba de fuerza bruta se prepara el ataque para descifrar las claves de acceso a una red inalámbrica considerando la permutación de varios caracteres en rápida sucesión esto es posible por un algoritmo que es simple y limitado en probar las diferentes combinaciones (Yunquera 2015).

Los procesos considerados para la técnica de ataque por fuerza bruta según (Domínguez et al. 2017) mencionaron las siguientes:

a) **Etapa de Descubrimiento:** En esta etapa se enfoca en reconocer los riesgos asociados al negocio del mismo modo que se obtiene información como segmentos de redes y rangos de direcciones IPs
b) **Etapa de Exploración:** En esta etapa se aplican técnicas no invasivas para identifica los blancos potenciales del segmento de red.
c) **Etapa de Evaluación:** En esta etapa se analizan los datos identificados para mostrar las posibles vulnerabilidades asociadas a las tecnologías o servicios asociados a la red.
d) **Etapa de Intrusión:** En esta etapa se empieza a violar la seguridad de los servicios encontrados, puede que no se cumpla con el objetivo en el primer intento, pero se buscan alternativas o variantes que permitan cumplir con el propósito.

Anexo 5. Metodología TROUDEJINISE

En la siguiente parte se describe los procedimientos correspondientes para el desarrollo de nuestra metodología. Del mismo modo se mencionan las fases de cada proceso objetivo, alcance entrada, proceso y salida.

Descripción y soporte de la solución

Se desarrollará la metodología para la evaluación del rendimiento de las tecnologías inalámbricas WifiMesh y PLC (Power Line Comunications), no existe un marco metodológico para dicha evaluación, del mismo modo que la propuesta de la metodología se basa en función a las métricas para evaluar el rendimiento de una red. (Caiza y Lara 2019) Mencionaron las siguientes Throughput, Delay, Jitter y Paquetes Perdidos. La evaluación del rendimiento de una red es importante puesto que permite identificar sus alcances y límites de la arquitectura de red y tecnología implementada, del mismo modo ayuda a identificar y solucionar los cuellos de botella de una red, revisar el nivel de seguridad, evitar las vulnerabilidades de la red, identificar las áreas en la red que no cuenten con recursos o cuentan con equipos reutilizados.

Según (Zapata 2016) para analizar el rendimiento de red es recomendable considerar los siguientes puntos:

a) Planificación: Se debe comprender los requerimientos y necesidades del servicio que se desea emplear en cada área dentro de una organización o entorno local.
b) Diseño: Considerar las configuraciones correspondientes en un entorno donde pueda ser seguro y se puedan solucionar los errores.
c) Despliegue: Implementar las pruebas correspondientes estableciendo fases en cada función para identificar las métricas de estudio.
d) Seguimiento y Análisis: Monitorear el comportamiento de red para la documentación correspondiente y análisis.

Plan de Proyecto

Las actividades para realizar la propuesta de metodología son las siguientes:

1. Recaudar información y documentación de artículos marcos de trabajo y metodologías para el diseño, implementación y evaluación del rendimiento de red.
2. Desarrollar la metodología propuesta para evaluar las tecnologías WifiMesh y PLC a través de las revisiones bibliográficas anteriores.
3. Aplicar la metodología para evaluar el rendimiento de red en las tecnologías de estudio.
4. Reporte de indicadores.

Proceso de Desarrollo de Metodología

Los procesos que tendrá la metodología son:

- Diseño e Implementación de red considerando las fases de la metodología Top Down (CISCO 2011) para evaluar las tecnologías de estudio.
- Ejecutar las pruebas de rendimiento de red considerando los indicadores de estudio (Reges Bessa et al. 2016).
- Ejecutar los tres últimos procesos correspondientes de la metodología para la evaluación de la seguridad (Vega 2020), para identificar las vulnerabilidades de la red usando las dos tecnologías de estudio.
- Ejecutar los cuatro procesos de pruebas de fuerza bruta (Domínguez et al. 2017), para medir la seguridad de la red de las dos tecnologías de estudio.

Arquitectura

Se presenta en la siguiente figura la representación de la arquitectura de la metodología TROUDEJINISE que se utilizara para evaluar el rendimiento de las dos tecnologías de estudio

Figura 2. Arquitectura De La Metodología TROUDEJINISE

Enfoque Metodológico

Para el desarrollo de la metodología propuesta, se utilizarán pruebas y metodologías para evaluar el rendimiento y seguridad a través de softwares, estas mismas se detallarán en lo siguiente:

- ✓ Para el diseño e implementación de la red donde se realizarán las pruebas de rendimiento se utilizará la Metodología Top Down. Esta metodología apoyara a montar la red y las tecnologías a evaluar en este caso PLC y WifiMesh.

- ✓ Pruebas de Rendimiento: Consiste en cuantificar los parámetros que permitan un mejor transporte de datos. Las pruebas que se realizarán estarán enfocadas con los indicadores para determinar el rendimiento de cada tecnología, cabe especificar perdida de paquetes, Throughput, Delay y Jitter, cumpliendo con los objetivos del proyecto.

- ✓ Metodología para Evaluación de Seguridad: Consiste en 5 procesos para llevar a cabo la evaluación del nivel de seguridad en cada tecnología. Planificación y preparación, Especificación de una evaluación de seguridad, ejecución de tareas, caracterización de vulnerabilidades e Informe de evaluación.

- ✓ Prueba de Fuerza Bruta: Pruebas para medir las vulnerabilidades de las redes de datos, se basa en algoritmos para atacar la red con diccionarios esto permite descifrar la clave de acceso a una red inalámbrica wifi.

Objetivo

El objetivo de la metodología es evaluar el rendimiento de red en tecnologías inalámbricas WLAN.

Alcance

- ✓ Dirigida hacia las micro y pequeñas empresas.
- ✓ Conocimiento básico en tecnologías y redes.
- ✓ Cada fase especifica los pasos necesarios para la evaluación de una red.
  1. Diseñar e implementar red.
  2. Ejecutar pruebas de rendimiento.
  3. Evaluar nivel de seguridad.
  4. Ejecutar prueba de fuerza bruta.

Entradas

Se refiere a los equipos que están instalados dentro de la red y las herramientas que se usaran para la evaluación.

- ➢ Definir equipos y herramientas necesarias para cada proceso de prueba.

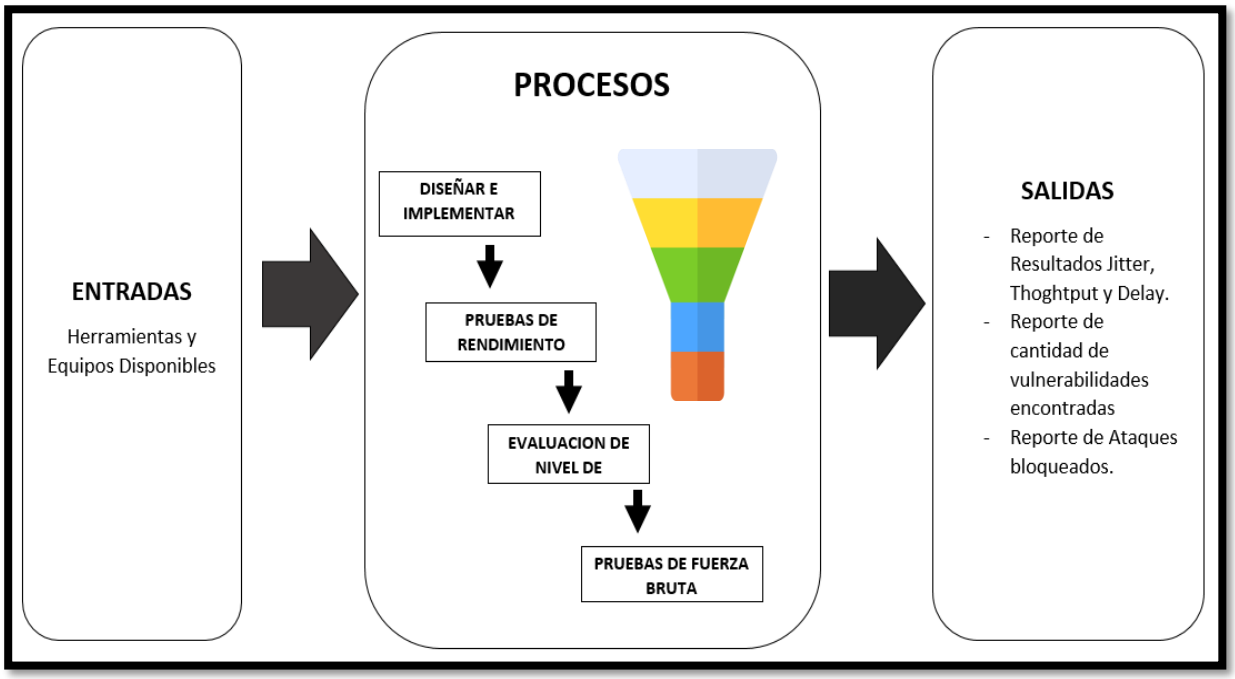


Figura 6. Diagrama de Proceso de TROUDEJINISE

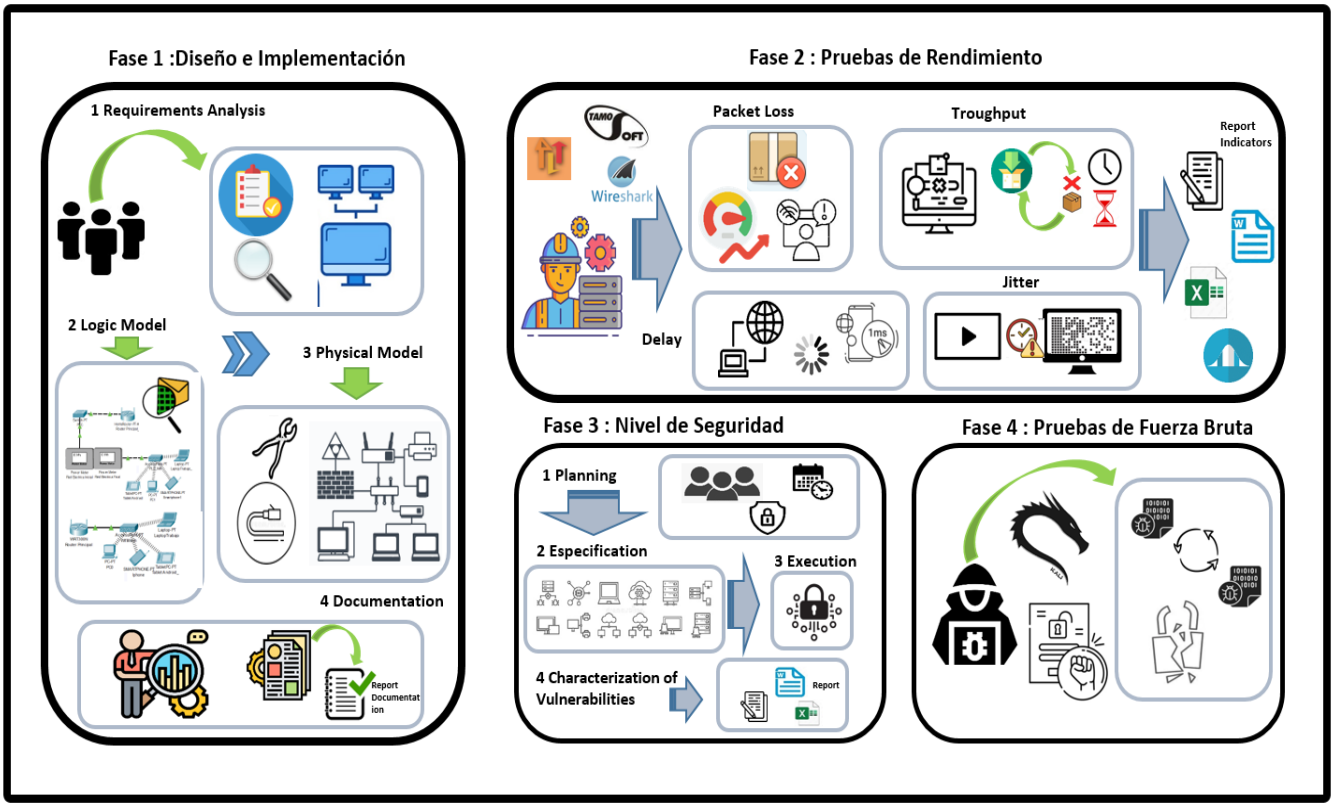


Figura 7. Procesos de la Metodología TROUDEJINISE

Salidas

- Fichas de registro resultados Troughput, Jitter y Delay
- Fichas de registro resultados de Cantidad de vulnerabilidades encontradas y ataques bloqueados

Anexo 6.Desarrollo de la Metodología TROUDEJINISE

FASE 1: Diseño e Implementación

Análisis de objetivos y Requisitos

Se busca medir el rendimiento de dos tecnologías de red inalámbrica, del mismo modo que permitan identificar las diferencias entre las mismas a nivel de cada indicador establecido en la metodología, throuhgput, delay, jitter, y nivel de seguridad. Cabe resaltar que se escogieron las dos tecnologías por disponibilidad en el mercado y alcance financiero del investigador.

Requisitos para el diseño de red a prueba

Compuesto por materiales a nivel de software y equipos que se usaran para la implementación y las pruebas de rendimiento que se realizaran.

Identificación de Aplicaciones

Los programas que se usaran para ejecutar los procesos de la metodología son los siguientes:

Software	Tipo	Valor	Detalle
Windows 10	Sistema Operativo	Necesario	Sistema operativo instalado en laptop o pc.
Packet Tracer	Software CISCO	Necesario	Software para diseño lógico de redes.
ISO Kali Linux	Sistema Operativo	Necesario	Sistema operativo para pruebas de seguridad.
VMWare	Software de virtualización	Necesario	Sistema para simular S.O

TamoSoft	Software para Test de Red	Necesario	Software para calcular métricas de rendimiento
Google Chrome	Navegador	Necesario	Software navegador de internet
Packet Loss Test	Aplicativo	Necesario	Software tester de red

Tabla 14. Identificación de Aplicaciones

Identificación de Equipos

Los equipos que se utilizaran para armar la red donde se llevara la prueba de rendimiento son los está compuesto por lo siguiente:

Hardware	Tipo	Valor	Detalle
Reuter Askey TCG220-46	Reuter Principal	Necesario	Enrutador Principal
PLC TP-Link	Extensor de Red	Necesario	Equipo de red para prueba
WifiMesh TP-Link	Extensor de Red	Necesario	Equipo de red para prueba
Patch Core Cat6	Cable de Red	Necesario	Cable de red LAN
Pc	Equipo de computo	Necesario	Computador de escritorio
Laptop	Equipo Portátil	Necesario	Computador portátil
Celulares	Dispositivo Móvil	Necesario	Host para red

Tabla 15. Identificación de Equipos

Diseño Lógico

Se muestra la estructura de la red donde se implementarán los equipos inalámbricos para la prueba de rendimiento. Los equipos adquiridos los medios de transmisión, señal banda 2.4 GHz para ambas tecnologías. Gateway con dirección IPv4 192.168.0.1. Direccionamiento para Host por DHCP.

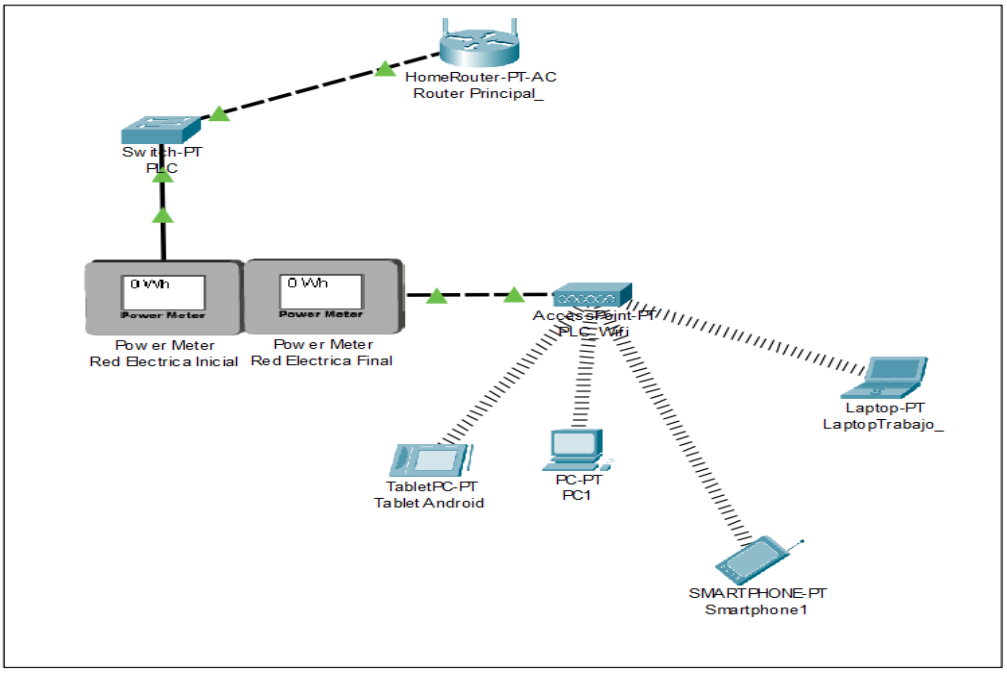


Figura 8. Topología de para pruebas de red PLC

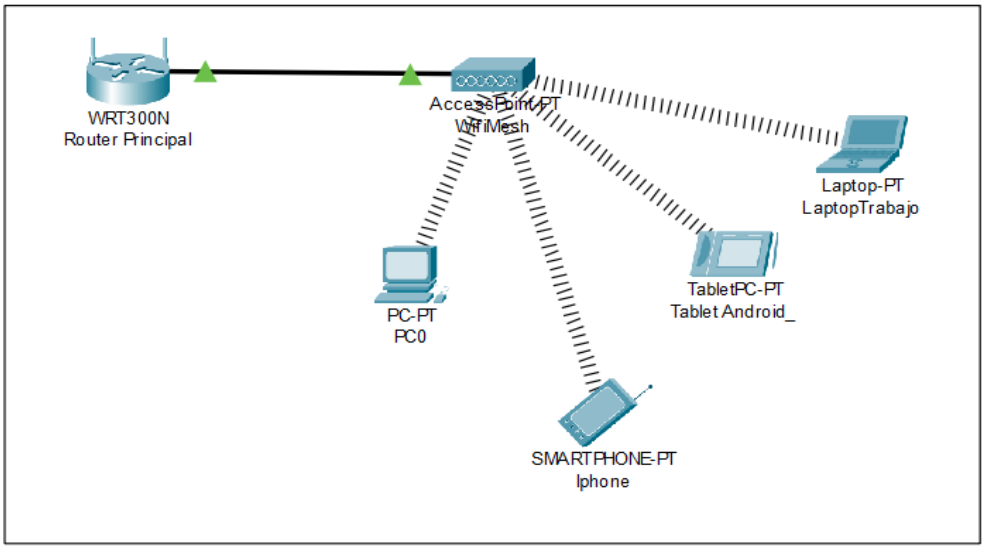


Figura 9. *Topología para Pruebas de red WifiMesh*

Diseño Físico

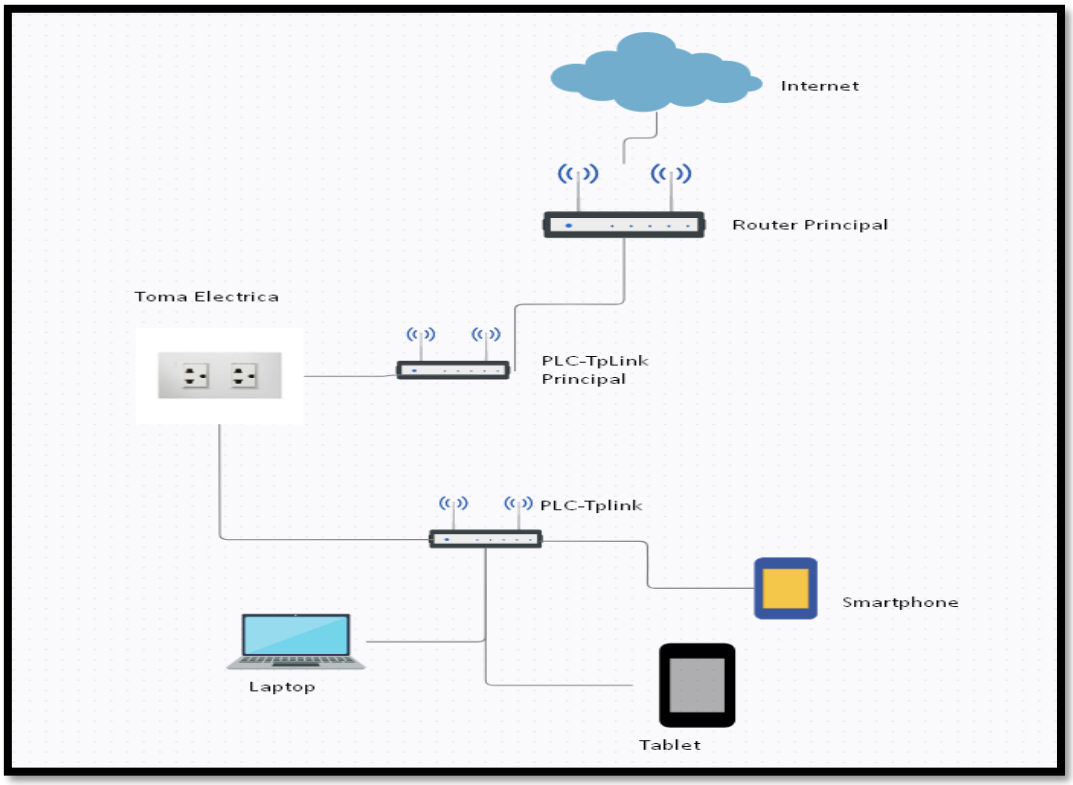


Figura 10. Dispositivos implementados para Red PLC

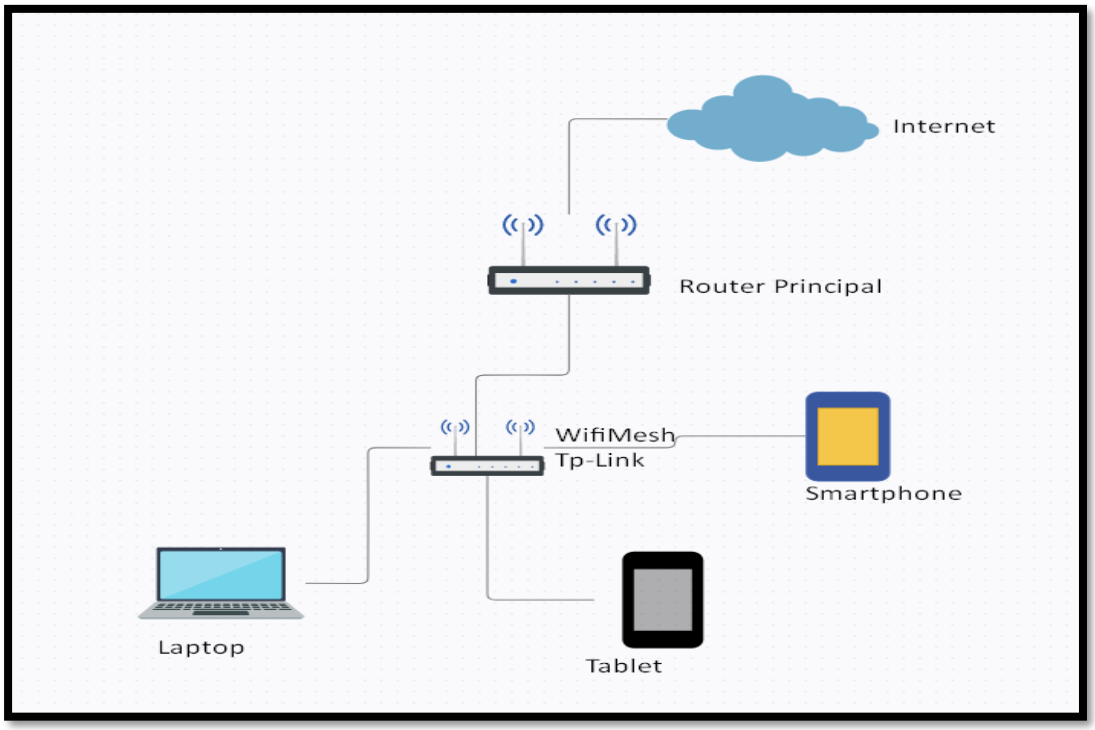


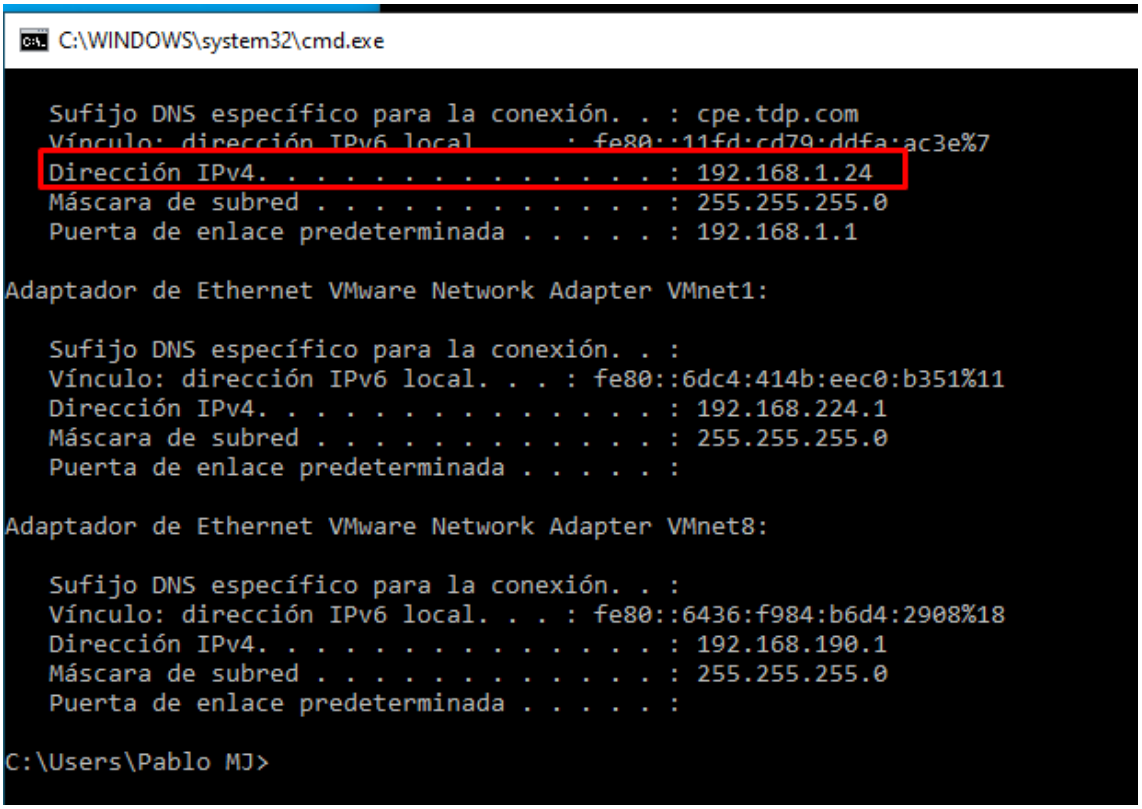
Figura 11. Dispositivos implementados para Red WifiMesh

FASE2: Pruebas de Rendimiento

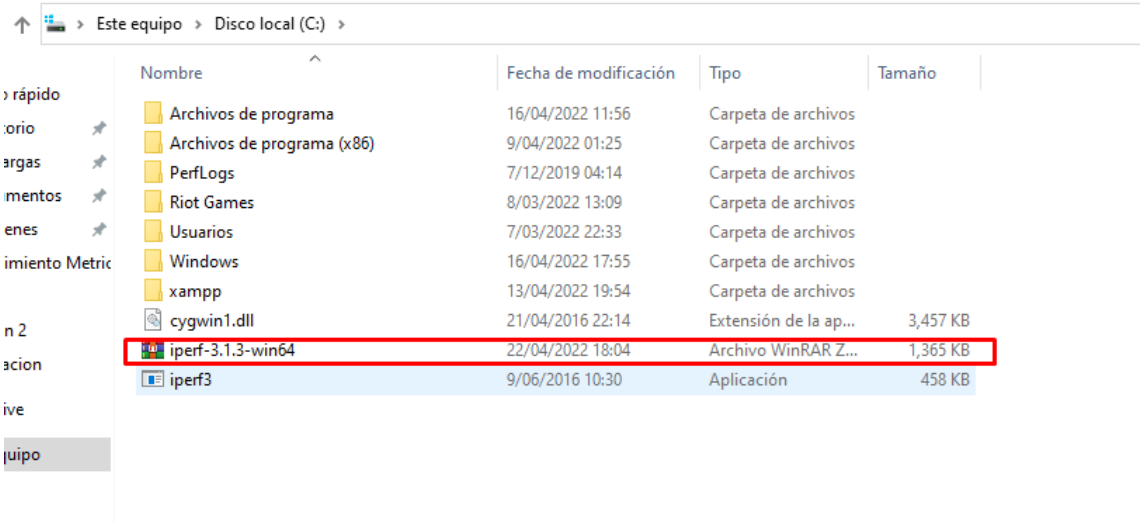
Software IPERF: Implementación en el Modo Servidor

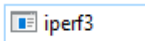
En el pc A tenemos de dirección Ip 192.168.1.24, en donde implantaremos el servidor para hacer las pruebas de Jiiter Delay Throuput

Configuración del Servidor para pruebas de rendimiento

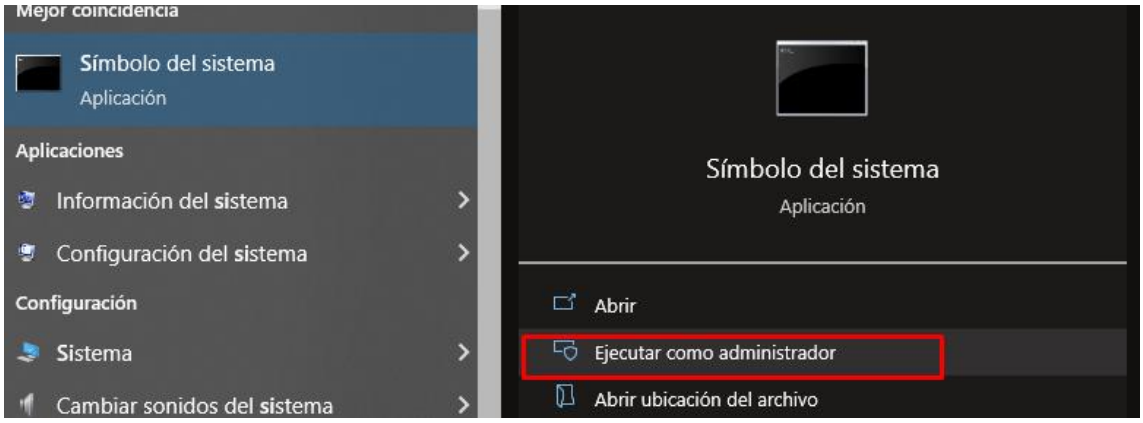


Para ello instalaremos el paquete Iperf3 en la unidad C de arranque del sistema para poder ingresar con los comandos del símbolo de sistema

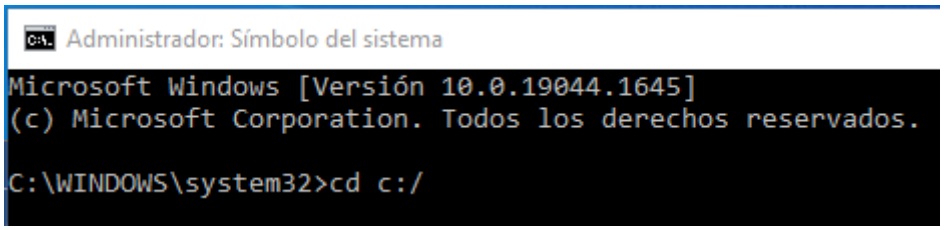


1. Se Descomprime el archivo iperf-3.13-win64.rar
2. Mantenemos el archivo 

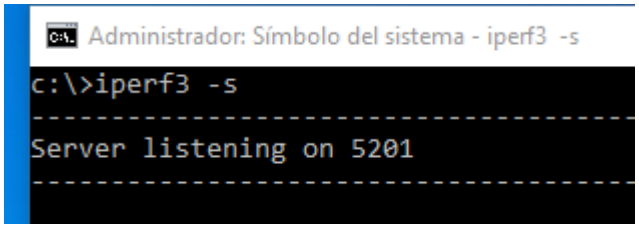
iperf3.exe un archivo ejecutable que nos permitirá acceder en modo servidor desde la PC A



3. Ejecutamos el CommandPront de Windows con permiso de administrador
4. Ejecutamos los siguientes comandos en el CommanPront **cd c:/** este comando nos permitirá acceder a la carpeta de destino donde se almaceno el archivo **iperf3.exe**



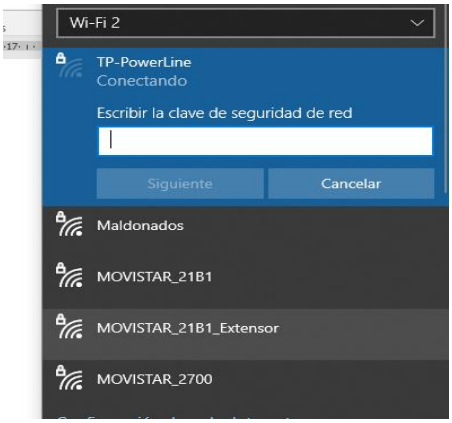
5. Una vez dentro de la carpeta, iperf3.exe ejecutamos el siguiente comando **iperf3 -s**, para asignar el pc A como Modo Servidor. Por defecto se asignará un puerto lógico donde podamos escuchar o enrutar hacia el servidor desde cualquier Host.

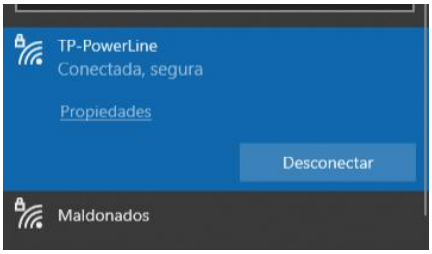


Software IPERF: Implementación en el Modo Cliente

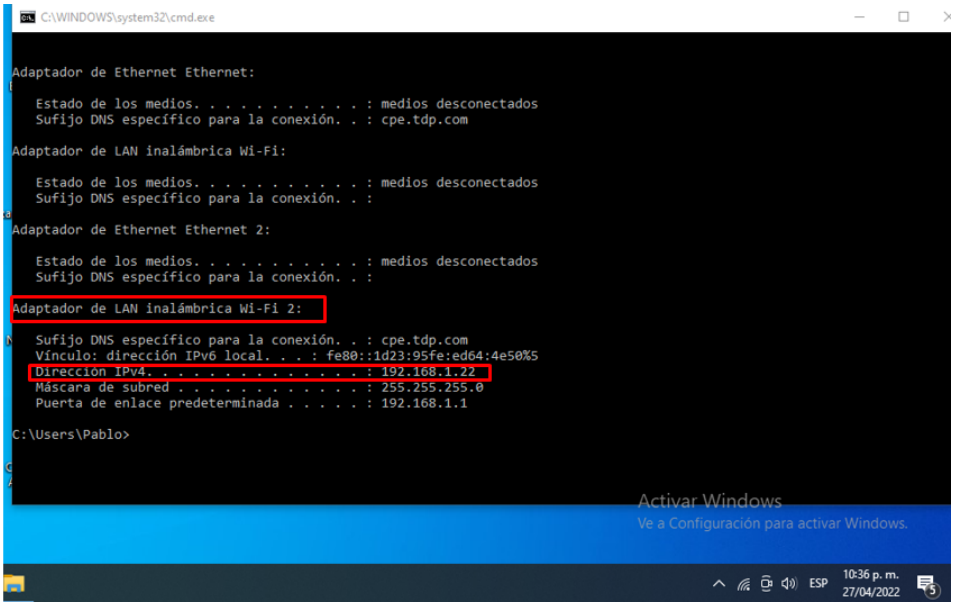
Para el Modo Cliente se usará una laptop PC B con dirección ip 192.168.1.22, conexión inalámbrica por Red PLC para ejecutar las pruebas de rendimiento para ello se implementarán los siguientes pasos.

1. Conectar a la red inalámbrica con la red PLC / WifiMesh



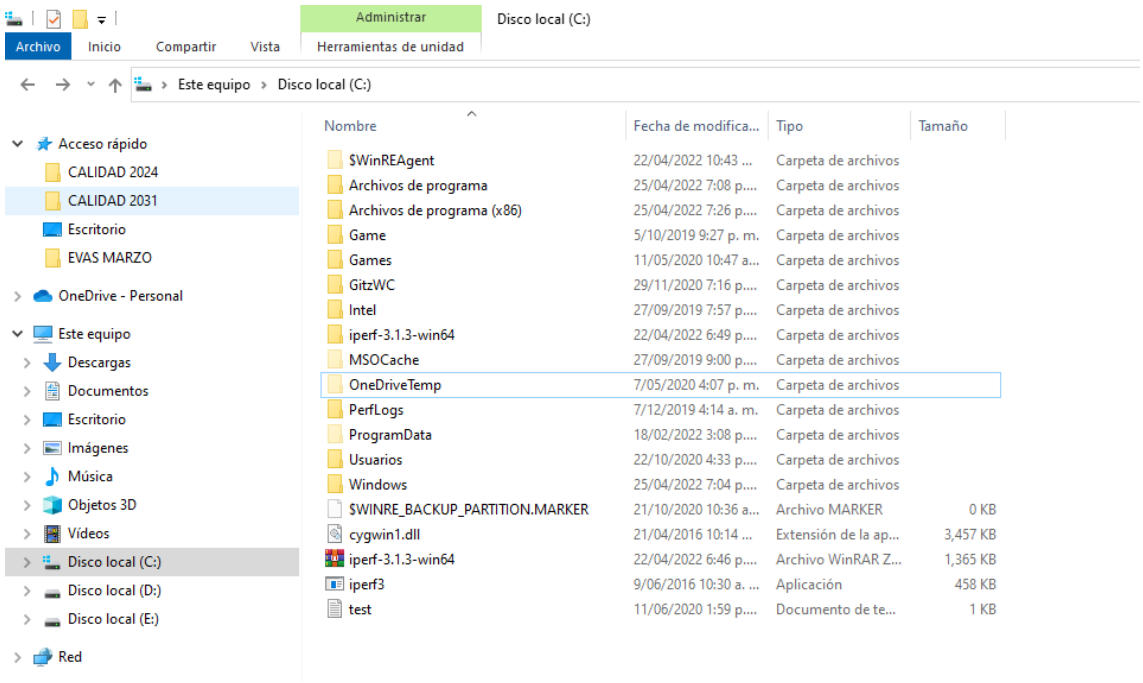


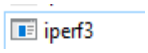
2. Se muestra la dirección de la Pc B – Cliente



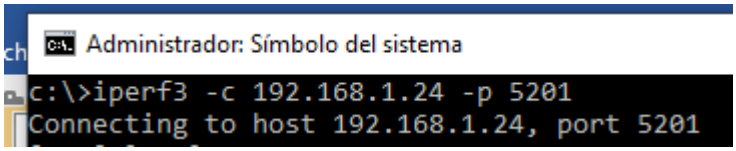
3. Instalar el paquete Iperf3 en la unidad C de arranque del sistema para poder ingresar por medio del CommandPront de Windows

4. Descomprimir el archivo iperf-3.13-wind64.rar

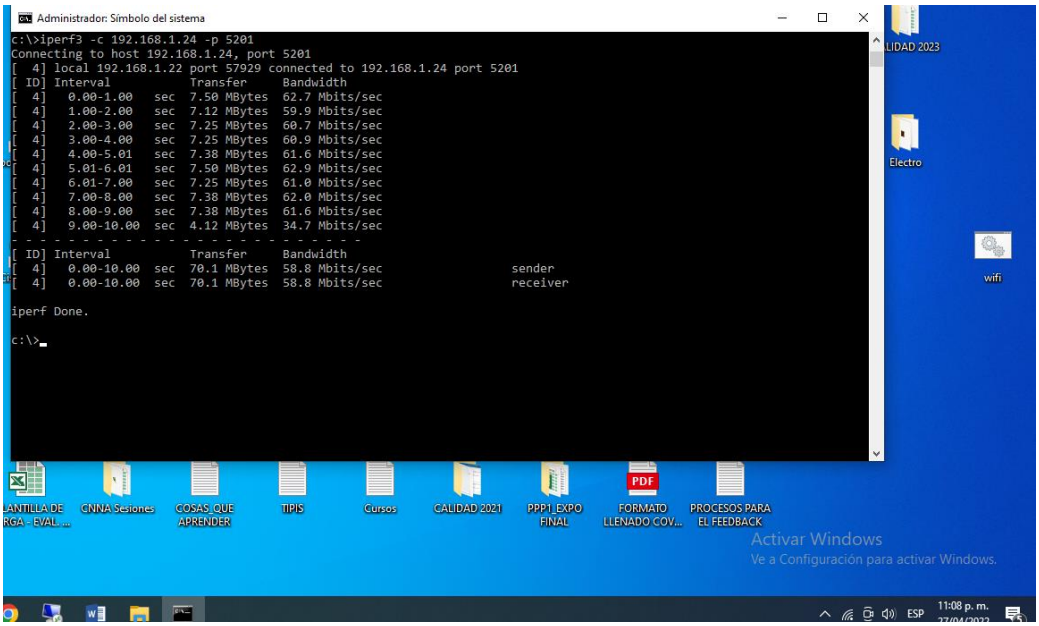


5. Mantenemos el archivo **ipef3.exe** un archivo 

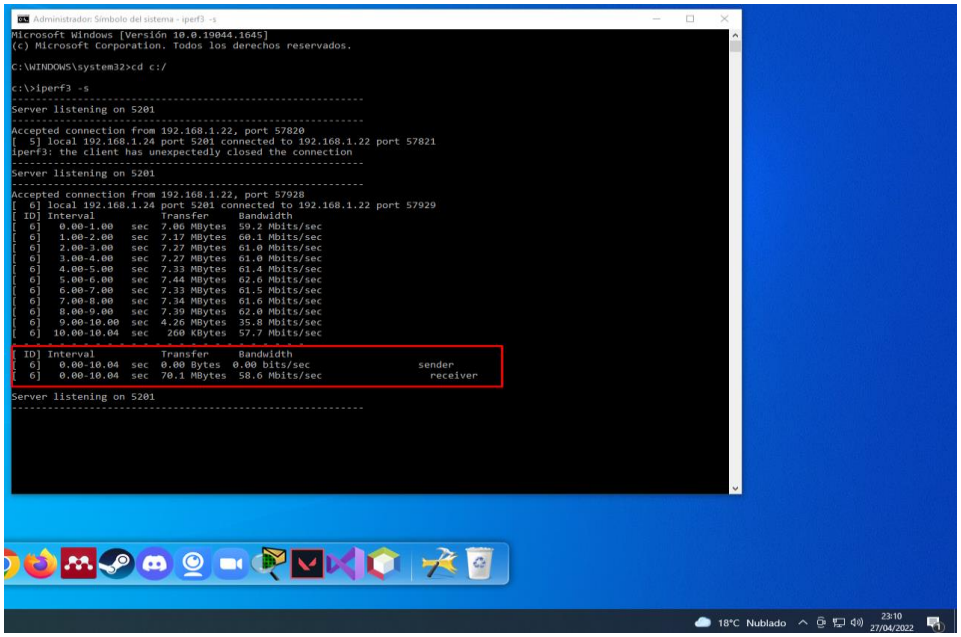
ejecutable que nos permitirá configurar como Modo Usuario la PC B.
6. Ejecutamos el CommandPront de Windows con permiso de administrador
7. Ejecutamos el siguiente comando **cd c:/** para acceder a la carpeta destino donde se almaceno el archivo **iperf3.exe**
8. Una vez dentro de la carpeta, iperf3.exe ejecutamos el siguiente comando **iperf3 -c**, para asignar el pc B como PC Cliente y concatenamos la dirección ip **192.168.1.24** del servidor a la cual se conectará y el puerto de escucha, de la siguiente manera:



9. Por defecto el sistema ejecuta dentro de 10 segundos envió de paquetes para confirmar la conexión de servidor y cliente.
10. La Pc B – Cliente muestra lo siguiente conexión



11. Mientras La Pc A – Servidor muestra la escucha que hizo al pc Cliente en el siguiente gráfico.

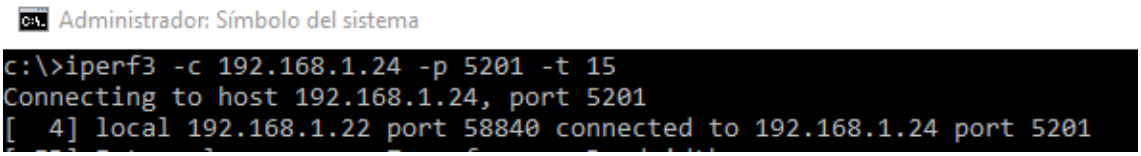


12. Se Confirma la conexión Cliente-**Servidor** para ejecutar las pruebas de rendimiento.

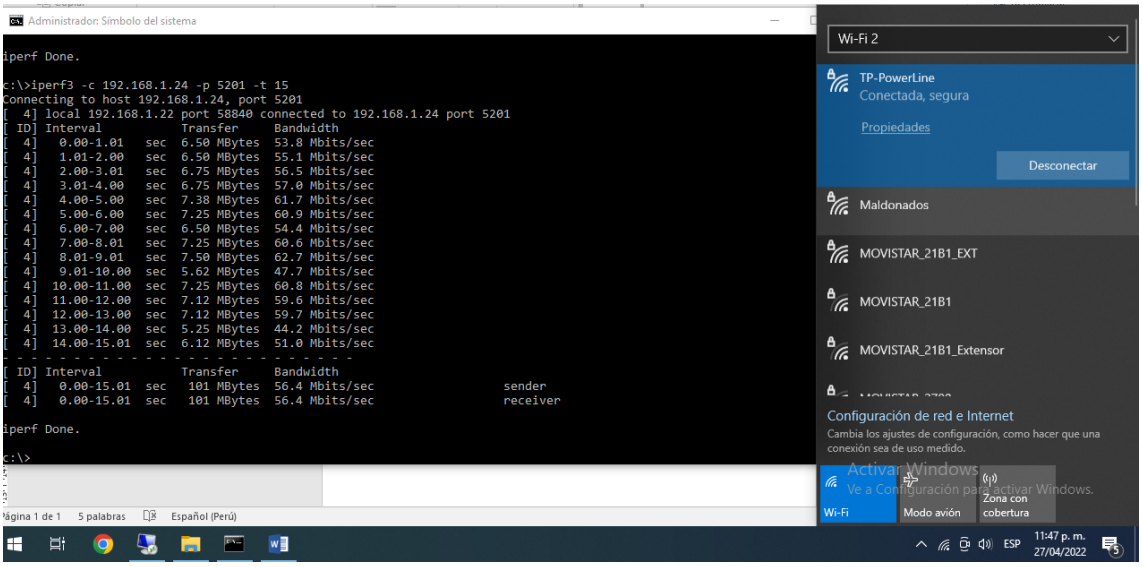
Pruebas para Trouhgput - Tecnología PLC / WifiMesh

Trouhgput: Se define como el paquete de información útil por segundo transmitido a través de canales de enlace, se mide en bits por segundo. (Ferreira, Granados y Vesga 2016).

1. Para medir la Tasa de trasferencia, primero nos conectamos a la red inalámbrica PLC.
2. Ejecutamos el CommandPront de Windows con permiso de administrador.
3. Accedemos a la carpeta donde se encuentra iperf3.exe y empezamos a ejecutamos el siguiente comando: **iperf3 –c 192.168.1.24 –p 5201 –t 15**



4. Se especifica en lo comandos anteriores el modo cliente (-c) la dirección ip de la misma el puerto por donde nos conectaremos hacia el servidor para enviar paquetes en un tiempo de 15 segundos, de la misma manera nos proyecte los siguientes parámetros: **intervalo** (segundos) y **tasa de trasferencia** (Mbytes).

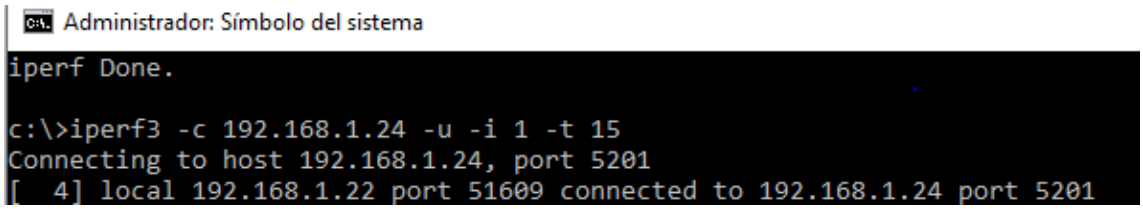


5. Se toman las muestras correspondientes para anotar en las fichas de registro.

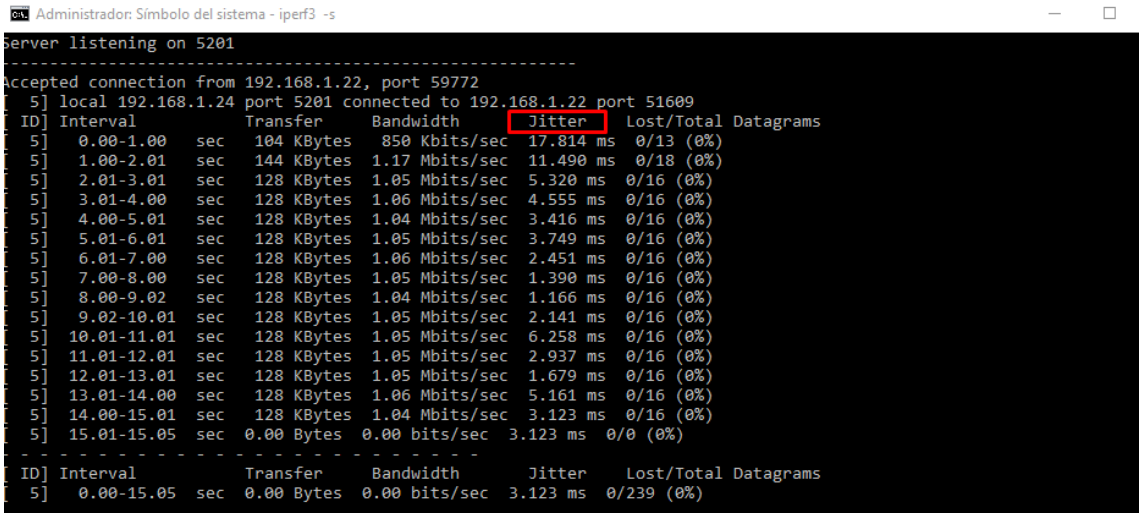
Pruebas para Jitter - Tecnología PLC / WifiMesh

Jitter se define por la variación de latencia, es calculado cogiendo la diferencia de retrasó del paquete vigente y del anterior

1. Para medir el Jitter, primero nos conectamos a la red inalámbrica PLC / WifiMesh.
2. Ejecutamos el CommandPront de Windows con permiso de administrador.
3. Accedemos a la carpeta donde se encuentra iperf3.exe y empezamos a ejecutamos el siguiente comando: **iperf3 – c 192.168.1.24 –u –i 1 –t 15**



4. Se especifica en lo comandos anteriores el modo cliente **-c** la dirección ip de la misma, el comando **–u** porque se verá un tráfico más detallado par eso se utiliza paquetes Udp, el comando **–i** para indicar el intervalo de 1segundo y -**t** para asignar el tiempo de prueba en 15 segundos. El resultado proyectara un detalle de la variación de latencia (Jitter).

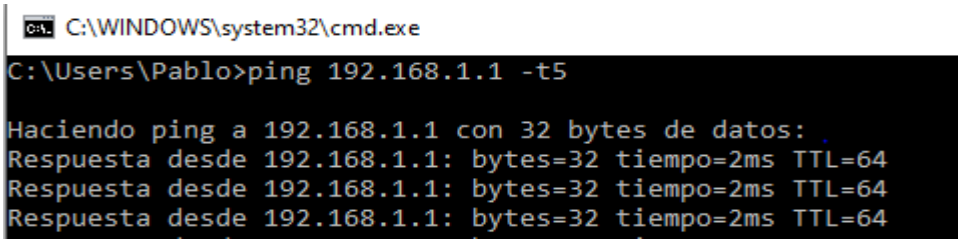


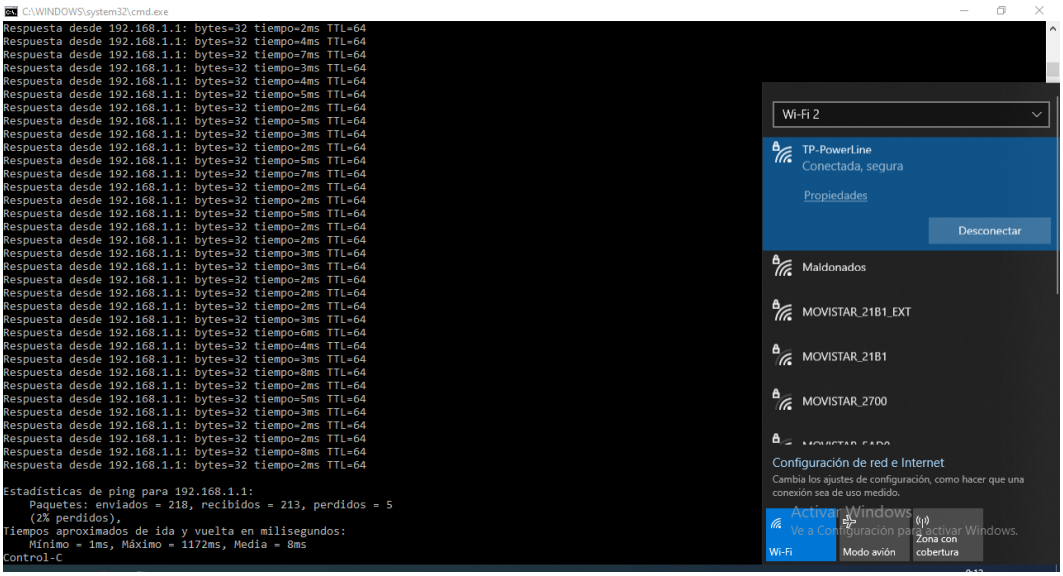
5. Se toman las muestras correspondientes para anotar en las fichas de registro.

Prueba para Porcentaje de Paquetes Perdidos PLC / WifiMesh

Porcentaje de paquetes perdidos son las partes de todos los paquetes que no llegaron a su destino (Granizo y Tacuri 2017), se generan debido al canal de transmisión, puesto que una red puede ser afectada por interferencias por dispositivos aledaños que comparten acceso al mismo canal de transmisión o se encuentren en las mismas frecuencias (Caiza y Lara 2019).

1. Conectarse a la red inalámbrica PLC / WifiMesh.
2. Ejecutar el CommandPront de Windows con permiso de administrador.
3. Se ejecuta el siguiente comando ping **192.168.1.1 –t 5**, el comanda **–t** permite asignar el tiempo de escucha en este caso de 5 minutos para cada intervalo de 1hra para la prueba.



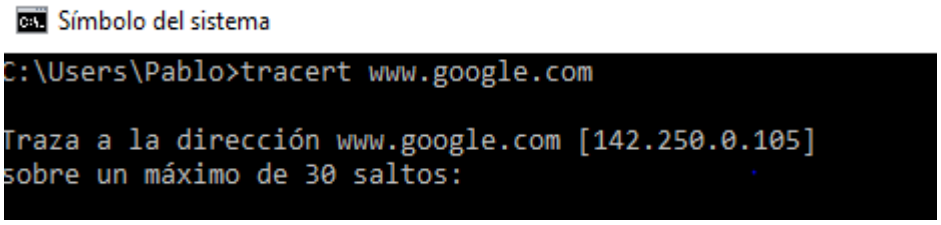


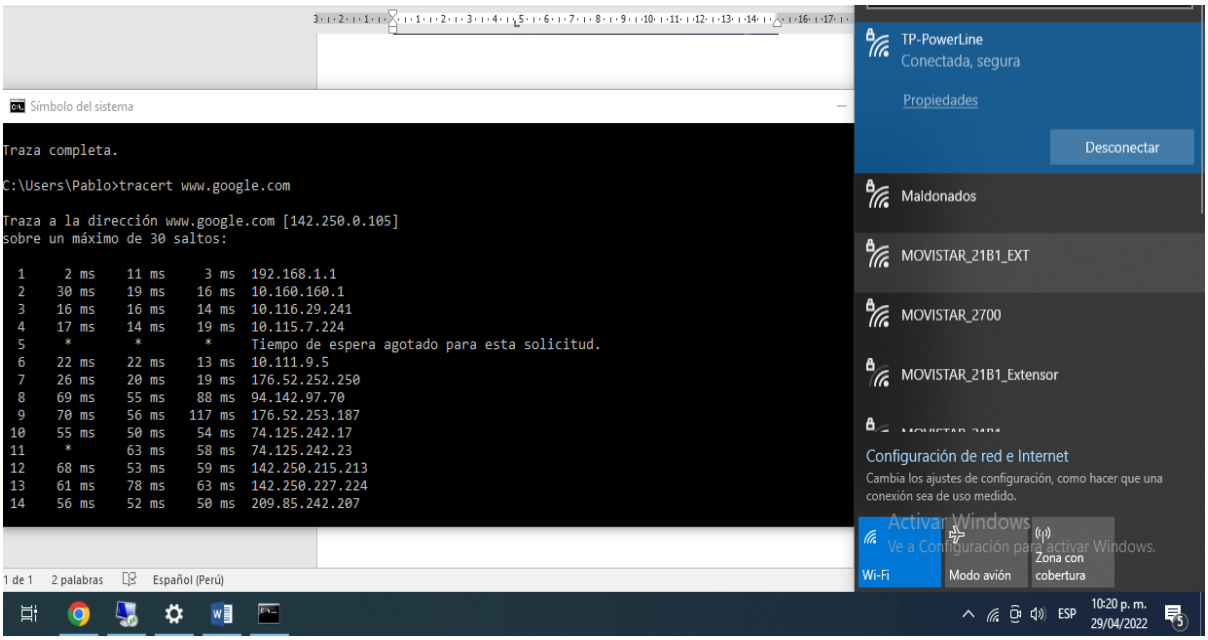
4. Se toman las muestras correspondientes para anotar en las fichas de registro.

Prueba para Retardo Extremo a Extremo PLC

Rayes y Salam (2020) mencionan que puede definirse como el retardo extremo a extremo la cantidad de tiempo (en milisegundos) que toma un paquete para llegar hacia su destino.

1. Para medir el retardo extremo a extremo primero conectarse a la red inalámbrica
2. Ejecutamos el CommandPront de Windows con permiso de administrador.
3. Se ejecuta el siguiente comando **tracert 192.168.1.1 –t 5**, el comanda **–t** permite asignar el tiempo de escucha en este caso de 5 minutos para cada intervalo de 1hra para la prueba. El comando tracert permite ver la traza que viaja un paquete hasta llegar hacia su destino.





4. Se toman las muestras correspondientes para anotar en las fichas de registro.

FASE 3: Nivel de Seguridad

1 Planificación:

Se determinan los objetivos y propósitos de las evaluaciones del mismo modo se establece el alcance que se tendrá con el equipo de trabajo.

Definición de objetivos:

- Identificar vulnerabilidades Físicas
- Identificar Vulnerabilidades Lógicas
- Describir las características de los dispositivos o tecnologías involucradas

Equipo de Trabajo:

Tester	Objetivo
Pablo E. Maldonado Jiménez (Estudiante Hacking Wifi - Academia de Ciber Seguridad Hacker Mentor)	Evaluar la seguridad de red de los equipos inalámbricos WifiMesh y PLC

Tabla 16: Equipo de Trabajo

2 Especificación:

Descripción de dispositivos involucrados para las pruebas de seguridad.

Evaluación de la Red y Equipos

Equipos / Host	Tecnología	Características
WifiMesh/ AC1200 -	TpLink-Wireless Adapter	Dual Band 2.4 / 5 GHz Seguridad WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC.
PLC / TLWPA-4220	TpLink-Wireless Adapter	Dual Band 2.4 / 5 GHz Seguridad WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC.
TL – WN722N V.1	Adapter USB - TPLink	Antena desmontable 4dBI – 150Mpbs Soporte WEP 64/128 bits, WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC. Soporta Modo Monitor

Reuter TCG220-46	Askey Reuter	Band 2.4GHZ 300Mbps Soporte WEP 64/128 bits, WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC.
PC-Desktop SCNM98P	S.O Windows10	Core i5-10400 CPU 2.90Ghz RAM 16 GB – SSD 500
PC2	S.O. KaliLinux – Kernel 5.15.	Core i5-10400 CPU 2.90Ghz RAM 8 GB – SSD 100

Tabla 17: Evaluación de la Red y Equipos

3 Ejecución:

Técnicas y Herramientas:

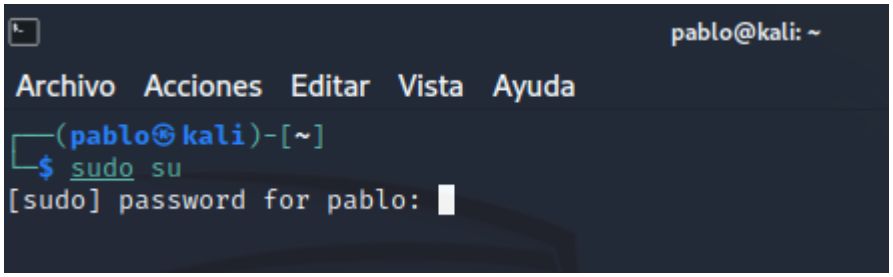
Se entiende por técnicas a algoritmos o códigos para aplicar mediante un software e iniciar los ataques, de la misma manera herramientas al uso de software o hardware que sean necesarios para las pruebas.

Nombre de Herramienta	Característica
Nmap	Aplicación de multiplataforma, permite analizar las redes y extraer información acerca de los servicios y sistemas operativos de los dispositivos dentro de una red.
Hpig3	Esta herramienta se utiliza en Kali Linux desde la terminar para el análisis y ensamblado de paquetes TCP.
Aircrack – ng	Software con un paquete detector, permite rastrear paquetes WEP y WPA/WPA2 –PSK. Analizador de redes LAN e Inalámbricas.
Airmong-ng	Este escript permite habilitar el modo monitor del adaptador de red para hacer escucha al tráfico de redes inalámbricas.
Airodump-ng	Este escript permite capturar paquetes inalámbricos además acumula vectores de inicialización.
Aireplay-ng	Este script permite inyectar fotogramas, genera tráfico para su uso posterior y descifrar claves WEP y WPA-PSK.

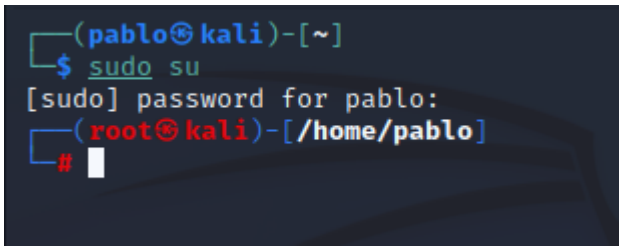
Tabla 18: Técnicas y Herramientas:

➢ Escaneo de Puertos:

1. Inicializamos el Sistema Kali Linux
2. Abrimos el terminal e inicializamos en modo administrador con el comando **sudo su**

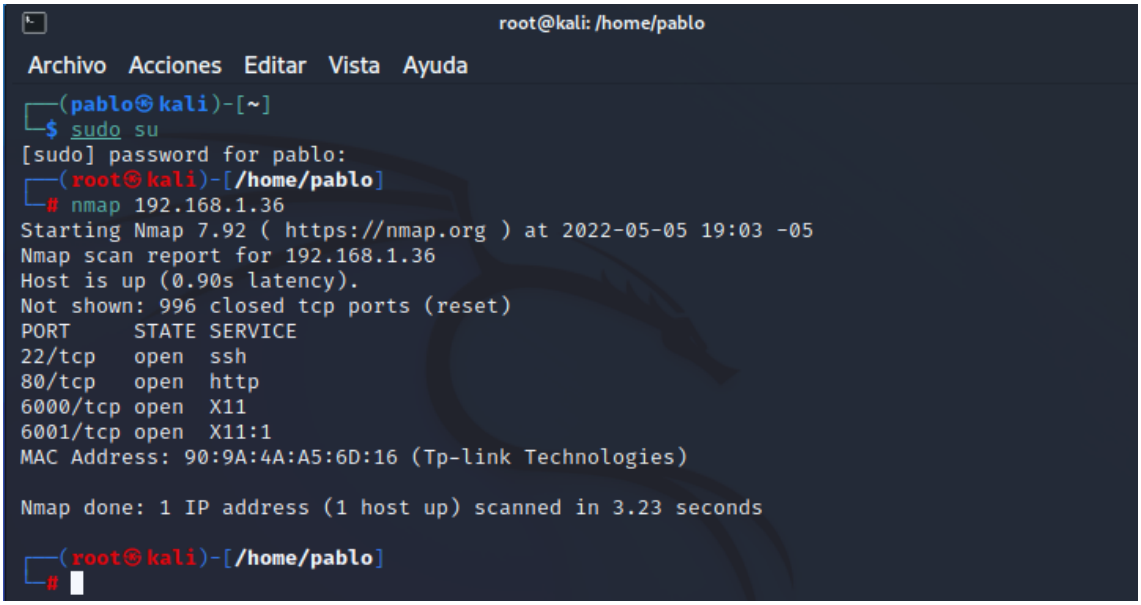


3. Ingresamos la clave de acceso como administrador



4. Antes de escanear los puertos del host a prueba, tenemos que obtener la dirección ip asignada del dispositivo, para esta prueba lo vemos en el mismo terminal del hardware

5. Empezamos a hacer el escaneo de puerto con el siguiente comando **nmap 192.168.1.36**



Se puede visualizar en la figura anterior el escaneo de 1000 puertos en una velocidad que ofrece el terminal de 0.90 segundos, se identifica en el host WifiMesh 4 puertos habilitados por donde se puedan vulnerar la red.

- Identificación de Vulnerabilidades:

Se describen las siguientes vulnerabilidades que cuenta cada tecnología WifiMesh / PLC.

TECNOLOGIA	WIFIMESH	PLC
Vulnerabilidades Lógicas		
Puertos TCP Abiertos	4	1
Protocolos de Encriptación	-	-
DHCP	1	1
Vulnerabilidades Físicas		
Puertos LAN libres	-	1
Por conducto Eléctrico	-	Energía eléctrica estandarizada
Filtrado Mac	-	-
SSID	1	1

Tabla 19: Vulnerabilidades PLC y WifiMesh

4 Caracterización de Vulnerabilidades

Se especifican y describen las vulnerabilidades encontradas en cada tecnología que se puso a prueba.

- Los puertos abiertos en un equipo de red son un foco importante si se quiere vulnerar la seguridad. Se describen los siguientes puertos abiertos.

PUERTO	ESTADO	SERVICIO	CARACTERISTICAS
22/TCP	Abierto	SSH	Este puerto permite hacer conexiones seguras hacia Servidores. Así mismo administrar equipos de forma remota
80/TCP	Abierto	HTTP	Puerto web para conexión hacia servidores. Se puede hacer ataque de inyección XSS y SQL entre otros.
6000/TCP	Abierto	X11	Puerto X, sistema de ventanas.
6001/TCP	Abierto	X11:1	Puerto que de control de transmisión permite garantizar la entrega de paquetes en el mismo orden de envió.

Tabla 20: *Descripción de Vulnerabilidades – Puertos*

DESCRIPCIÓN DE VULNERABILIDADES		PERMISOS
Puertos TCP Port 22 Port 80 Port 6000 Port 6001	Los puertos TCP abiertos se pueden aprovechar para dar acceso hacia otros dispositivos mediante los servicios, así mismo conectarse directamente y vulnerar la red que se requiera.	**Servicio SSH:** permite hacer trasferencia de archivos SSH, SFTP y SCP. **Servicio HTTP :** Permite administrar la conexión hacia un servidor
Protocolo Cliente / Servidor **DHCP**	Protocolo de configuración dinámica, permite brindar la configuración automáticamente a un host.	Brinda la configuración automática en primera instancia.

Puertos LAN	Puertos ethernet habilitado. Puerta de enlace para conectar cualquier equipo mediante cable UTP	Conexión directa hacia la red.
Nombre de Red SSID	Identificador de red inalámbrica.	Permite identificar la red, para vulnerar mediante el modo monitor e identificar el nombre físico del dispositivo (MAC).

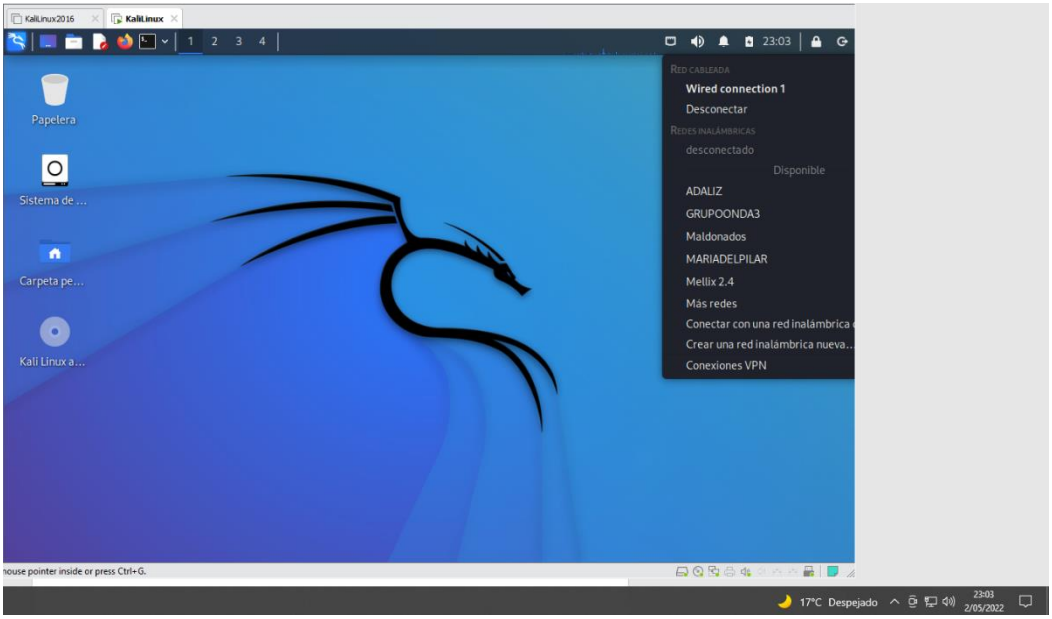
Tabla 21: Descripción de Vulnerabilidades

FASE 4: Prueba de Fuerza Bruta

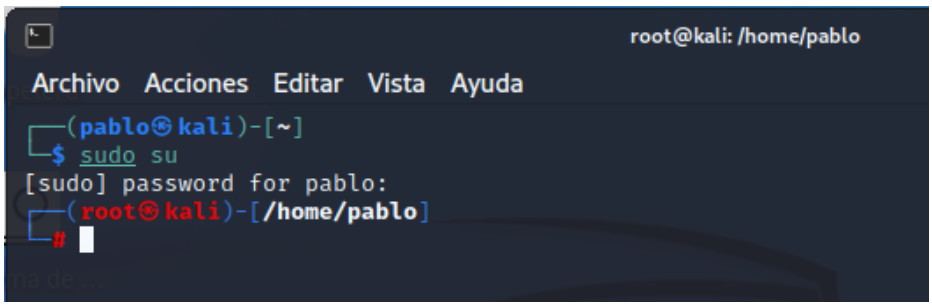
- Etapa de Descubrimiento:

En esta etapa se enfoca en reconocer los riesgos asociados a la red del mismo modo que se obtiene información como segmentos de redes y rangos de direcciones IP´s

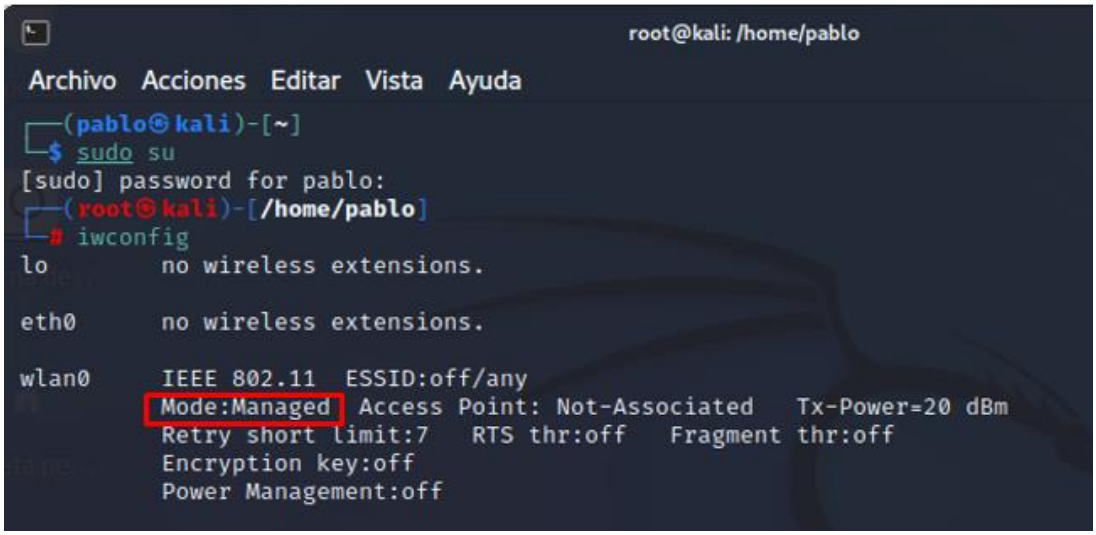
1. Conectar adaptador de red Wifi



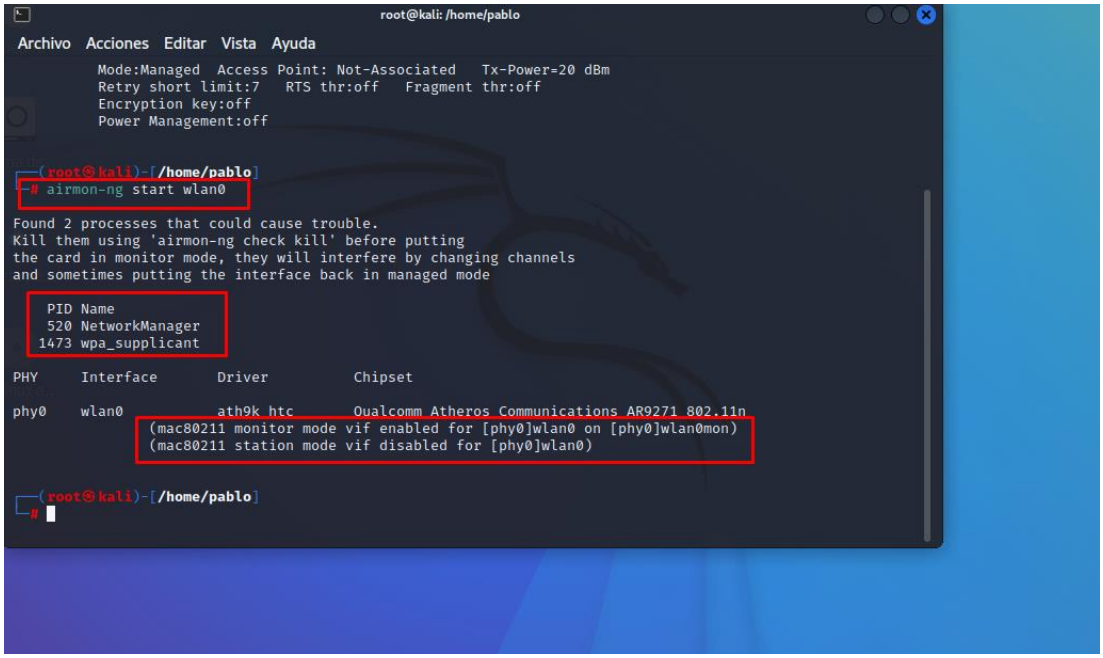
2. Abrir el terminal en modo administrador con el comando **sudo su**, ingresamos la clave de usuario



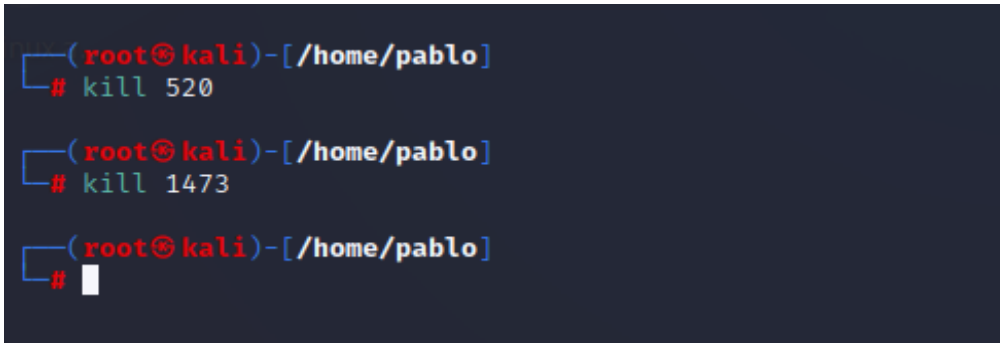
3. Ingresamos el siguiente comando **iwconfig** para ver que el sistema acepte al adaptador de red, como podemos ver esta en mode administrador. Tenemos que cambiar a mode monitor para hacer escucha de red.



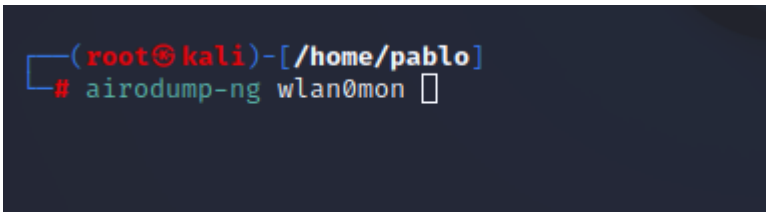
4. Ejecutamos el comando **airmon-ng start wlan0** para habilitar el mode monitor del adaptador inalámbrico.



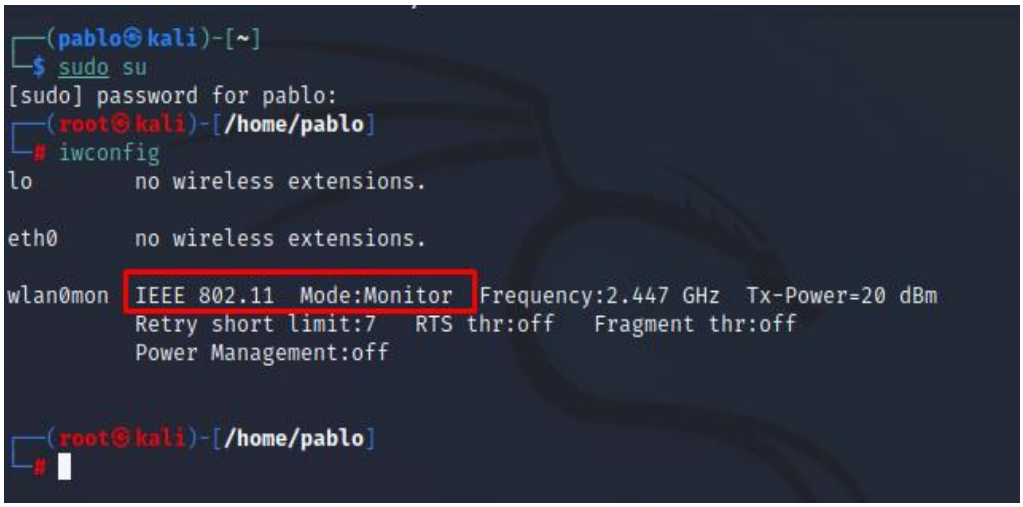
5. Para que se habilite el mode monitor del adaptador de red tenemos que matar los procesos con el siguiente comando **kill**



6. Escribir el comando **airodump-ng** wlan0mon para activar el mode monitor

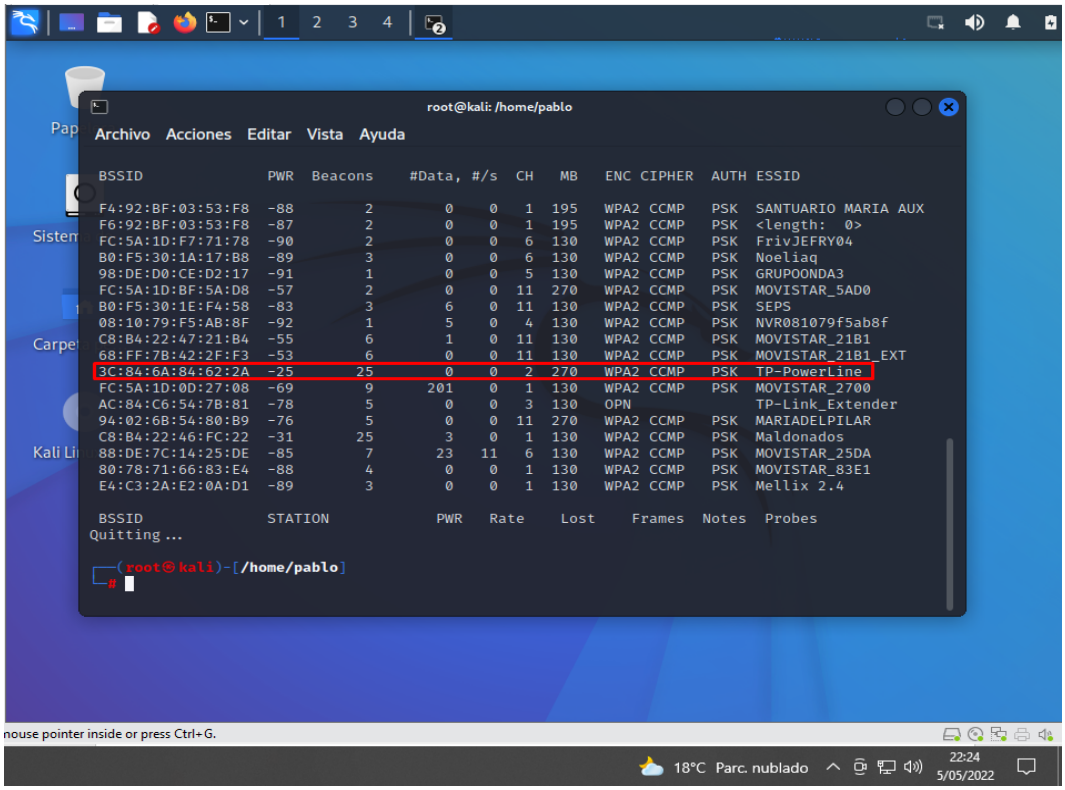


7. Ingresamos por consola el comando iwconfig y visualizamos que el adaptador ya está en mode monitor, listo para empezar el ataque.

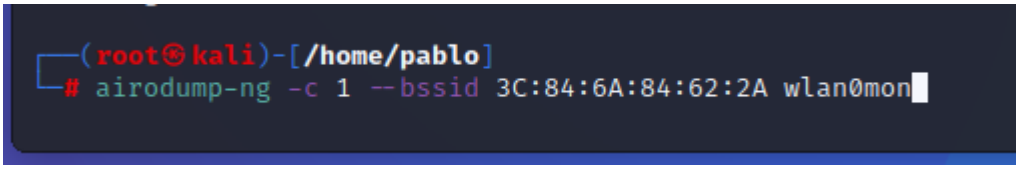


Etapa de Exploración

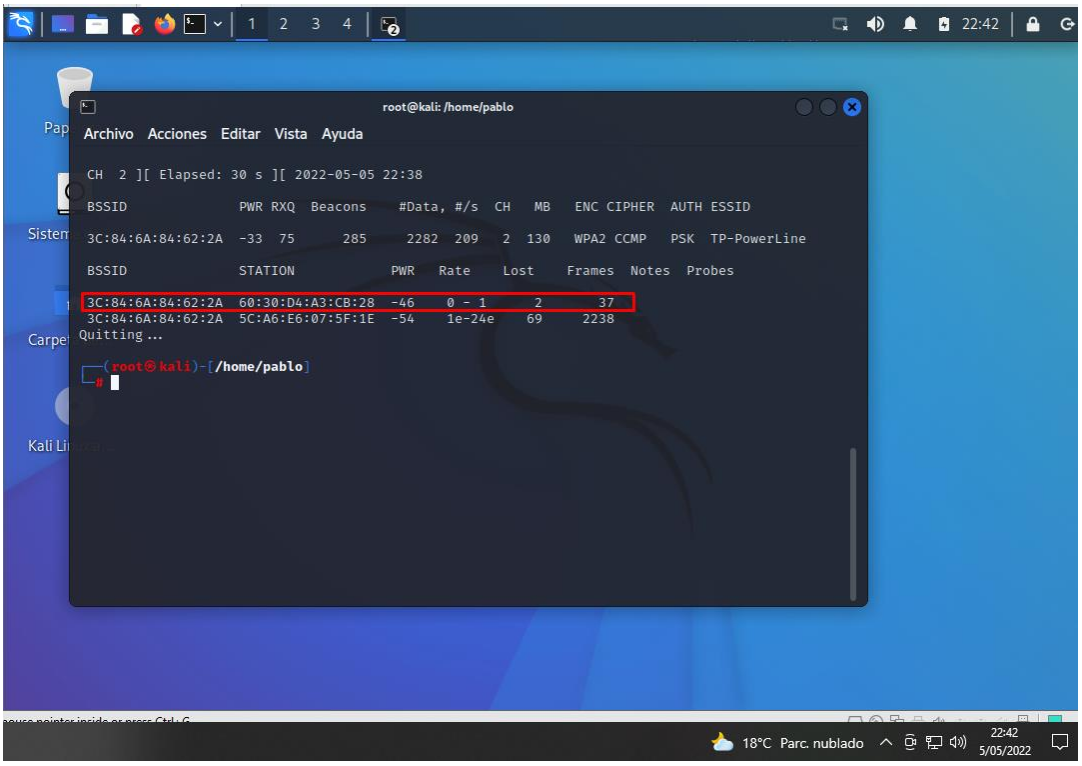
1. Ejecutar el comando **aerodump-ng wlan0mon,** empieza la etapa de exploración donde se hace escucha a las redes inalámbricas, identificamos el nombre de la red con la MAC y el canal por el cual se desempeña.



2. Ingresamos el siguiente comando **airodump-ng –c 1 -–bssid** 3C:84:6A:84:62:2A **wlan0mon** para escanear la red a la cual atacaremos.

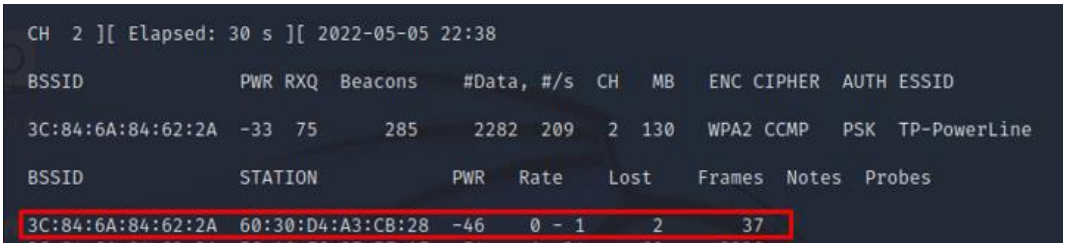


3. Después de escanear la red, se mostrarán los dispositivos conectados hacia la red inalámbrica y por el cual se intercederá para iniciar el ataque.



Etapa de Evaluación

1. Identificamos el dispositivo conectado a la red por el cual se capturará la clave autenticada. Seleccionaremos la serie Mac para identificarlo.

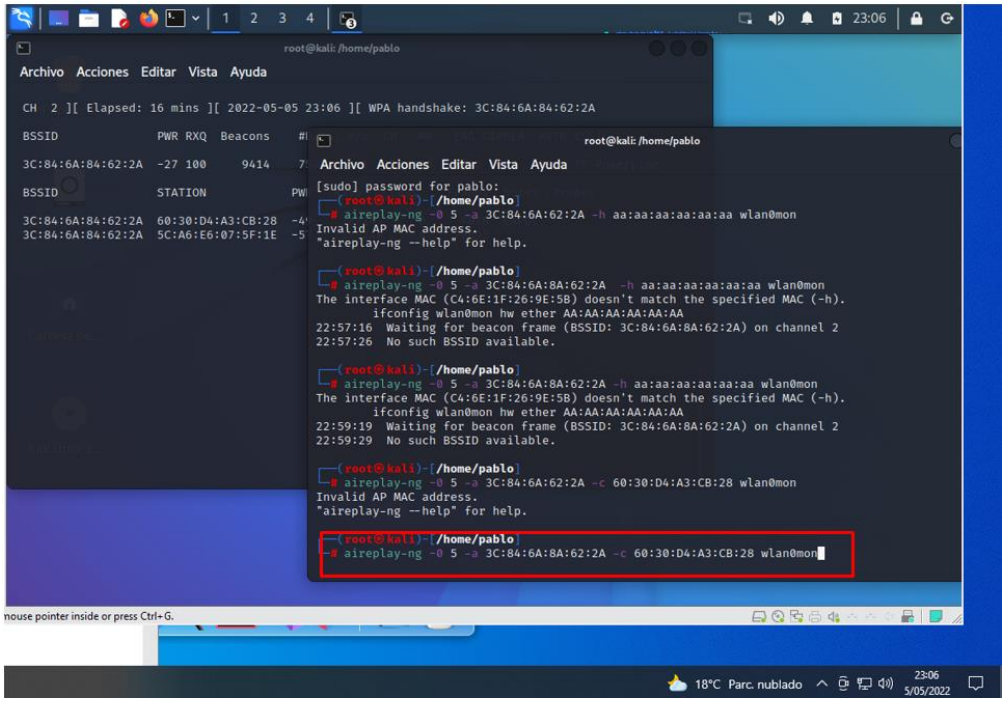


2. Ejecutamos el siguiente comando: **aireplay-ng -0 5 –a 3C:84:6A:8A:62:2A –c 60:30:D4:A3:CB:28 wlan0mon.**

Se describe lo siguiente:

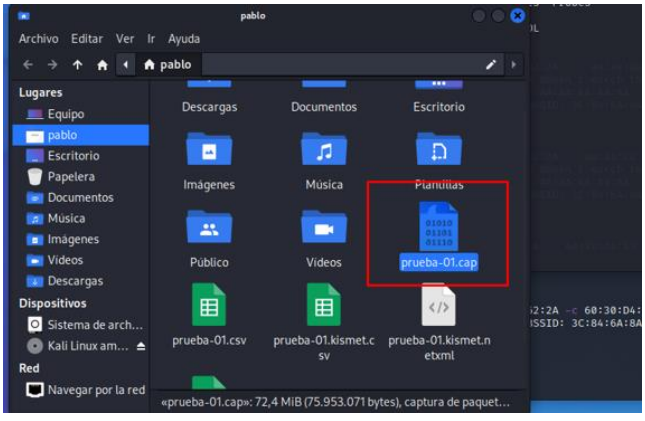
- aireplay-ng -0 5 –a (MAC dispositivo conectado). Este comando permitirá des-autenticar 5 veces al dispositivo para capturar la clave.

- -c (MAC de equipo de Red inalámbrica) wlan0mon. Hace referencia al equipo que atacaremos haciendo escucha por mode monitor del adaptador de red inalámbrica.



3. Una vez ejecutado el comando verificamos en la primera terminal del paso n° 1, que la ejecución fue exitosa se llegó hacer **handshake**, se visualiza en la siguiente imagen.

4. Se llega a capturar el paquete de encriptación de la clave de red y se almacena en un formato **.cap**



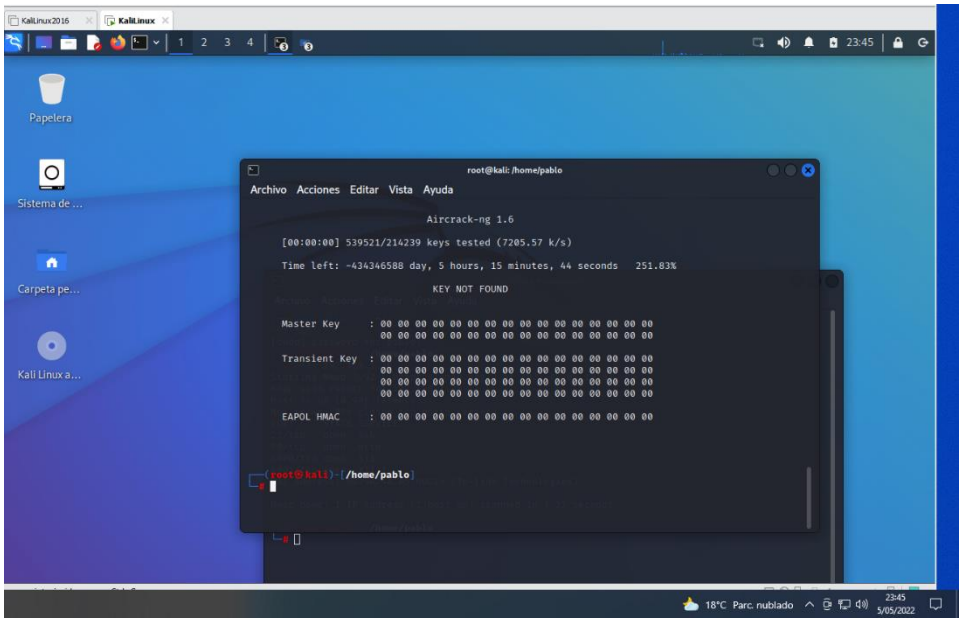
Etapa de Intrusión

1. Identificar la ruta del archivo Prueba-01.cap.
2. Ejecutamos el siguiente comando aircrack-ng
3. Con el enlace –w, se direccionará hacia el archivo donde se encuentra la clave encriptada.
4. Ejecutamos el siguiente comando y inicializamos el ataque por fuerza bruta.

```
┌──(root㉿kali)-[/home/pablo]
└─# aircrack-ng -w /usr/share/wordlists/rockyou.txt.gz  prueba-01.cap
```

Wordlists / rockyou.txt.gz son diccionarios con diferentes combinaciones de caracteres para vulnerar la red inalámbrica, es un script propiamente de kali Linux, de acuerdo a la versión puede almacenar hasta millones de combinaciones que permutaran para descifrar la clave.

5. En la siguiente imagen se visualiza el ataque por fuerza bruta que se realizara con un script de **539521** combinaciones.



Anexo 7.Herramientas para evaluar el rendimiento y nivel de seguridad de red de las tecnologías inalámbricas WLAN

TamoSoft

Esta herramienta permite enviar consecutivamente flujos de datos TCP y UDP a través de la red en el cual permite calcular métricas como valores del rendimiento ascendente y descendente, perdida de paquetes de una trama hacia otra, los resultados se muestran en representaciones gráficas y numéricas. Las pruebas de rendimiento de TamoSoft admite conexiones Ipv4 e IPv6 además permite evaluar los parámetros de calidad QoS para una red, lo más resaltante de este software es que permite como herramienta usar dos componentes con un servidor y cliente. Funciona de la siguiente manera, el cliente se conecta con el servidor que está escuchando las conexiones. Una vez que se realiza la conexión, el cliente y el servidor intercambian datos en ambas direcciones y la parte cliente de la aplicación calcula y muestra las métricas de la red.

La parte del **servidor** cuenta con dos herramientas configurables: a) el puerto en que escucha las conexiones entrantes y b) el protocolo de red que se utilizara, por default el servidor escucha en el puerto 27100 y usa IPV4, como detallamos en la siguiente figura:

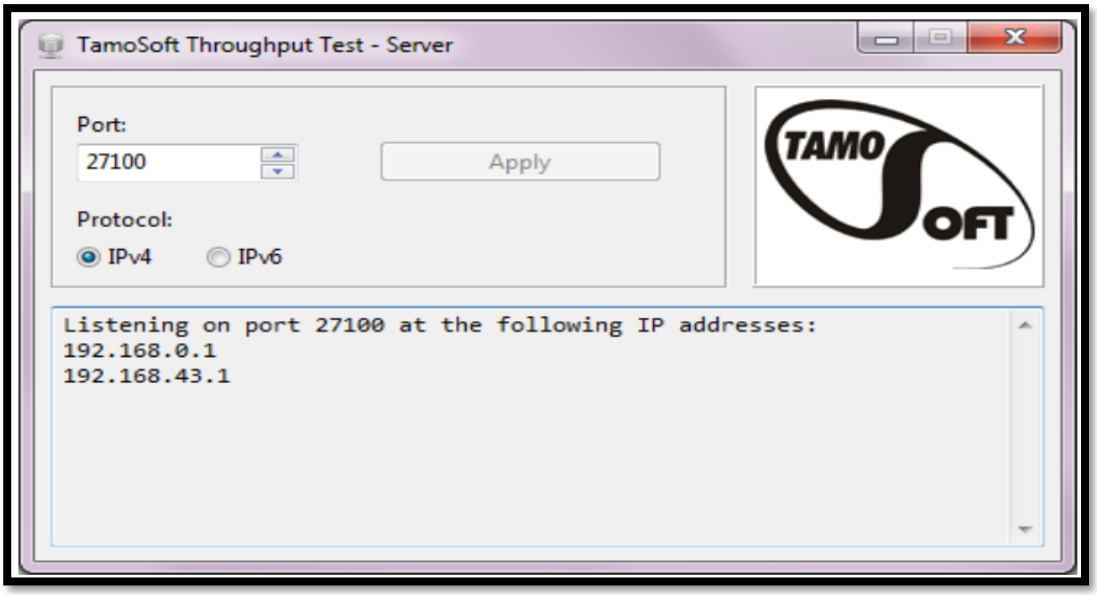


Figura 12. ventana de Configuración Servidor por TamoSoft.

En el Cliente solo especificamos el número de puerto que se utilizara para conectarnos al servidor. Para empezar a generar las pruebas es necesario configurar el servidor y el cliente en diferentes computadoras para poder realizar el test correspondiente y obtener los parámetros por cada indicador como se muestra en la siguiente figura.

***Figura 13*. Ventana de Configuración Cliente por TamoSoft.**

Packet Loss Test

Es un aplicativo online diseñado para generar pruebas de transmisión de datos, de tal manera que permite obtener parámetros sobre la cantidad de paquetes perdidos en una red. Para hacer la prueba primero se genera los ajustes seleccionando la cantidad de paquetes (en bytes) que se puedan enviar en un determinado tiempo (en segundos) y estableciendo puntos de retrasos aceptable en milisegundos. Ver los siguientes gráficos.

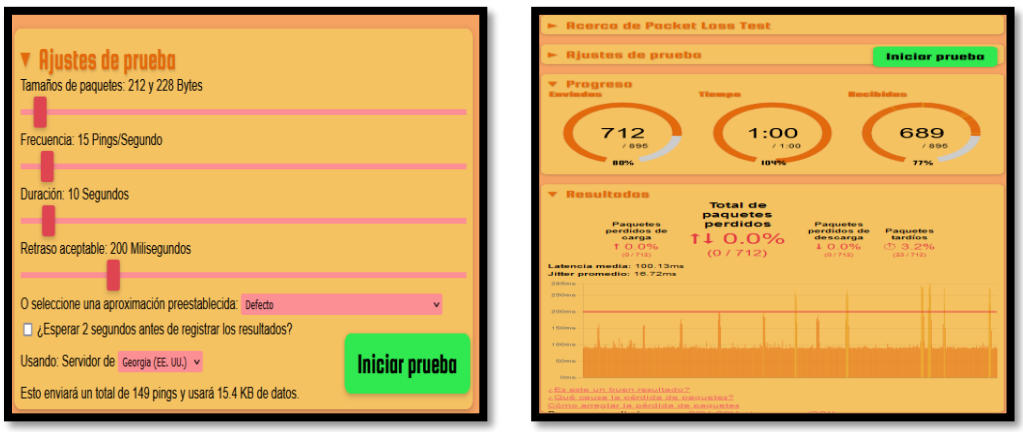


Figura 14. Prueba por Packet Loss Test

JPerf

Este software permite hacer la medición de la red por capacidad de trafico dentro de un mismo segmento de red. Este permite realizar pruebas para ayudar a realizar un diagnóstico de la red, validando si existen problemas de congestión, degradación fisca de alguno de los componentes de la red. Para ejecutar JPerf se requiere dos pcs para configurar el rol independientemente a cada una. Después de haber seleccionado el rol de cada equipo se debe instalar el software Jperf en cada uno. Requisito indispensable Java para completar la ejecución.

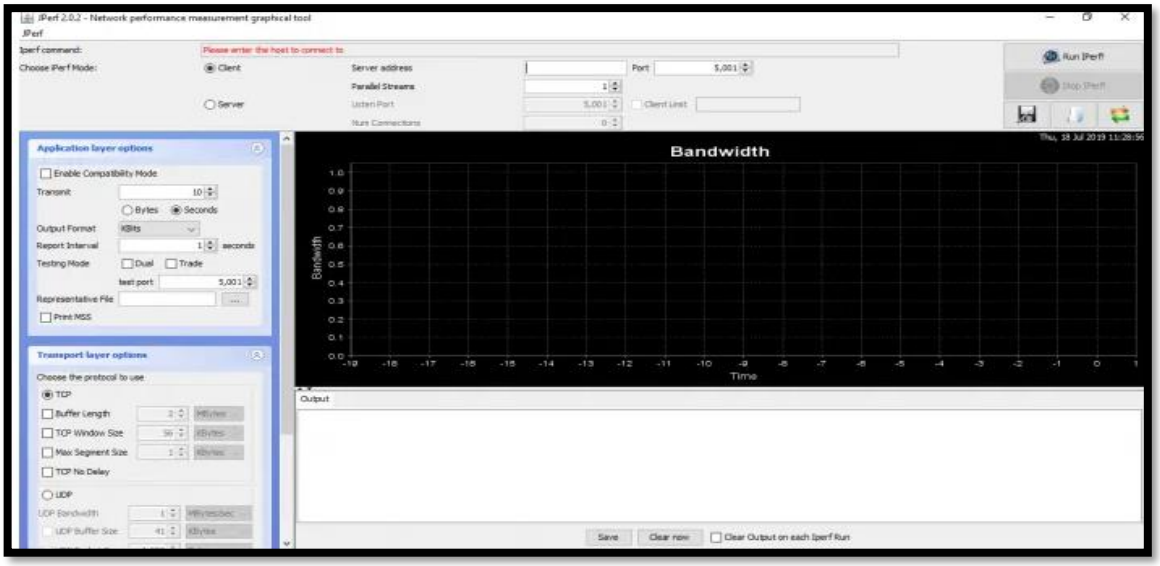


Figura 15. Ventana de Consola del Software Jperf.

Configurar Modo Servidor

Para iniciar la configuración en el equipo modo servidor se tiene que elegir “Chosse Ipef mode: Server” en la máquina seleccionada para ejecutar como servidor. Se puede usar diferentes comandos de acuerdo a las configuraciones que se debe realizar.

Listen Port: Es el puerto de escucha de donde recibirá los paquetes para realizar la medición, se recomienda dejarlo por defecto, si tienes inconvenientes puedes usar otro puerto que no esté bloqueado, para verificar el estado de tus puertos puedes usar la herramienta nmap.

Num Connectios: Permite colocar el número máximo de conexiones que soportará el servidor, por defecto se deja en 1.

Report Interval: permite configurar el intervalo de muestras que se tomarán para realizar el gráfico de capacidad de tráfico. Luego de establecer estos parámetros ejecutamos el programara JPerf.

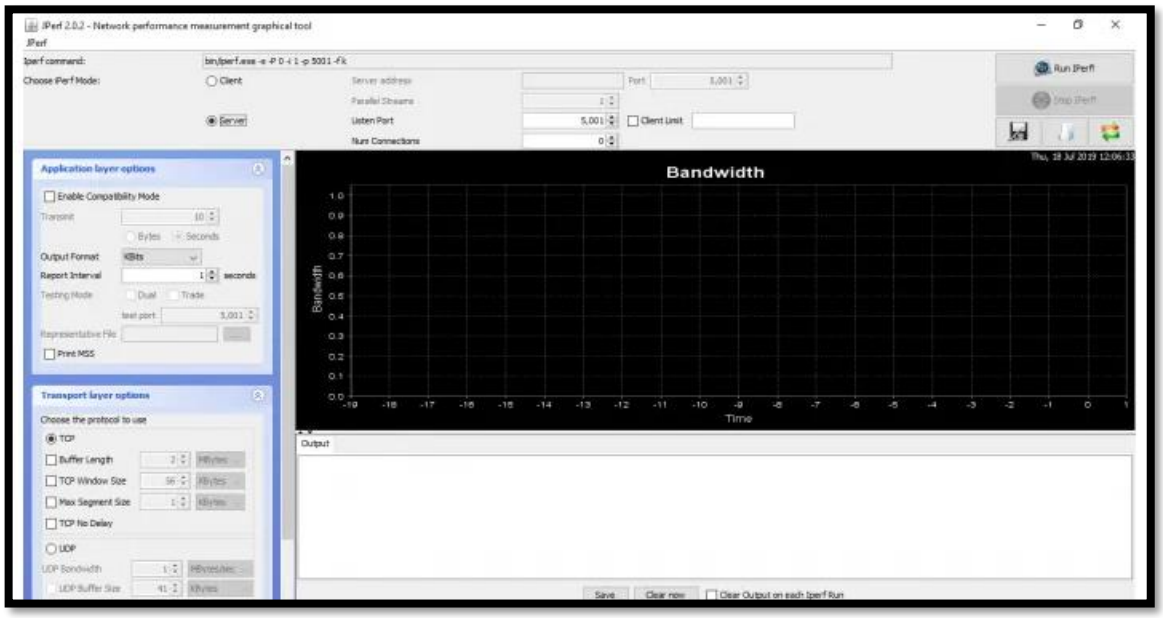


Figura 16. Configurar modo servidor por Jperf.

Configuración Modo Cliente

Para configurar el modo se debe elegir “Chosee IPerf mode: Client” en la máquina seleccionada para ejecutar como cliente. Luego, se coloca la dirección IP del servidor en “Server Address”, además colocamos el puerto a donde se enviarán el flujo de prueba y el número de flujos de prueba para este cliente.

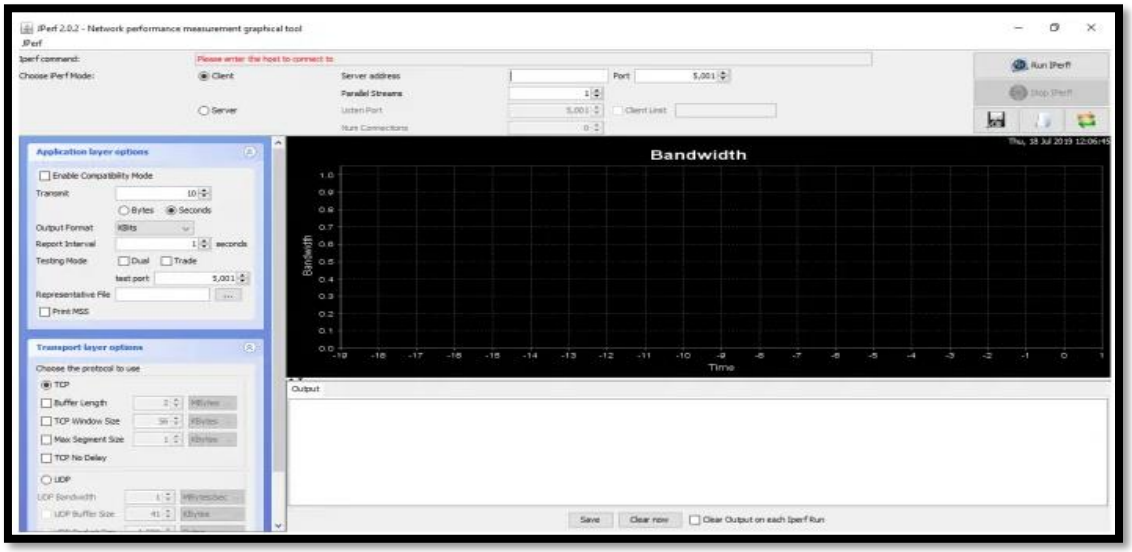


Figura 17. Configurar Modo Cliente por Jperf.

Con esto se inicia la prueba de rendimiento en JPerf usando la configuración predeterminada, después de ejecutar la prueba durante 10 segundos. Una vez que aparezcan los gráficos quiere decir que la ejecución fue correctamente.

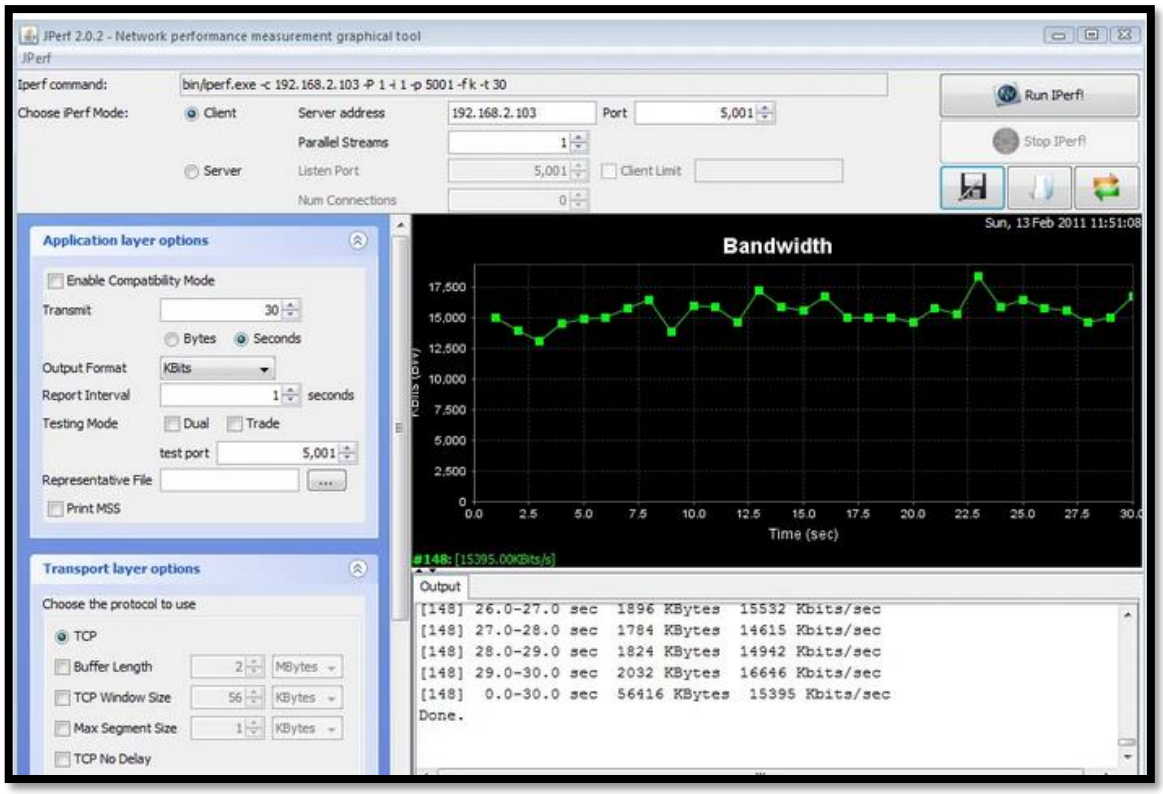
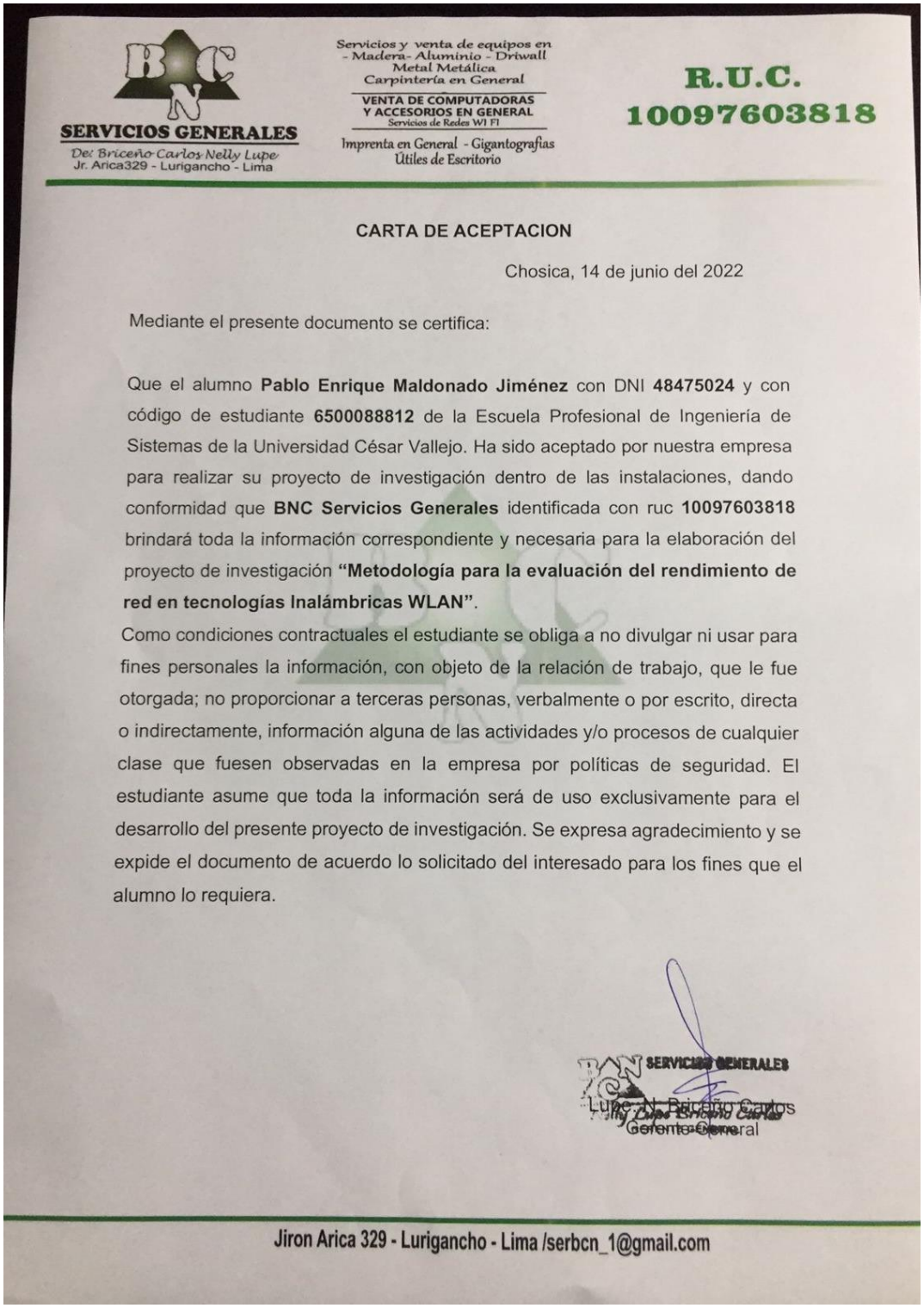


Figura 18. Prueba de Rendimiento por Jperf

Anexo 8: Carta de Aceptación BNC Servicios Generales



SERVICIOS GENERALES
De: Briceño Carlos Nelly Lupe
Jr. Arica329 - Lurigancho - Lima

Servicios y venta de equipos en
- Madera- Aluminio - Driwall
Metal Metálica
Carpintería en General
VENTA DE COMPUTADORAS
Y ACCESORIOS EN GENERAL
Servicios de Redes WI FI
Imprenta en General - Gigantografías
Útiles de Escritorio

R.U.C.
10097603818

CARTA DE ACEPTACION

Chosica, 14 de junio del 2022

Mediante el presente documento se certifica:

Que el alumno **Pablo Enrique Maldonado Jiménez** con DNI **48475024** y con código de estudiante **6500088812** de la Escuela Profesional de Ingeniería de Sistemas de la Universidad César Vallejo. Ha sido aceptado por nuestra empresa para realizar su proyecto de investigación dentro de las instalaciones, dando conformidad que **BNC Servicios Generales** identificada con ruc **10097603818** brindará toda la información correspondiente y necesaria para la elaboración del proyecto de investigación **"Metodología para la evaluación del rendimiento de red en tecnologías Inalámbricas WLAN"**.

Como condiciones contractuales el estudiante se obliga a no divulgar ni usar para fines personales la información, con objeto de la relación de trabajo, que le fue otorgada; no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la empresa por políticas de seguridad. El estudiante asume que toda la información será de uso exclusivamente para el desarrollo del presente proyecto de investigación. Se expresa agradecimiento y se expide el documento de acuerdo lo solicitado del interesado para los fines que el alumno lo requiera.

SERVICIOS GENERALES
Lupe N. Briceño Carlos
Gerente General

Jiron Arica 329 - Lurigancho - Lima /serbcn_1@gmail.com

Anexo 9: Caso de Estudio - Aplicación de TROUDEJINISE en BNC Servicios Generales

FASE 1: Diseño e Implementación

1.1 Análisis de objetivos y Requisitos

BNC Servicios Generales es un negocio de imprenta con ruc 10097603818 dedicada a prestar servicios de ventas de artículos de oficina, elaboración de recuerdos accesorios, agente de pagos y trabajos de imprenta en general. La red está compuesta con los equipos del proveedor Movistar, computadoras y dispositivos inalámbricos interconectados.

El objetivo es mejorar el rendimiento de red inalámbrica dentro del negocio en función al throughput, delay, jitter, y nivel de seguridad. A través de la implementación de dos tecnologías inalámbricas PLC y Wifimesh.

Requisitos para el diseño de red

- Plano del negocio y ubicación de puestos de trabajo

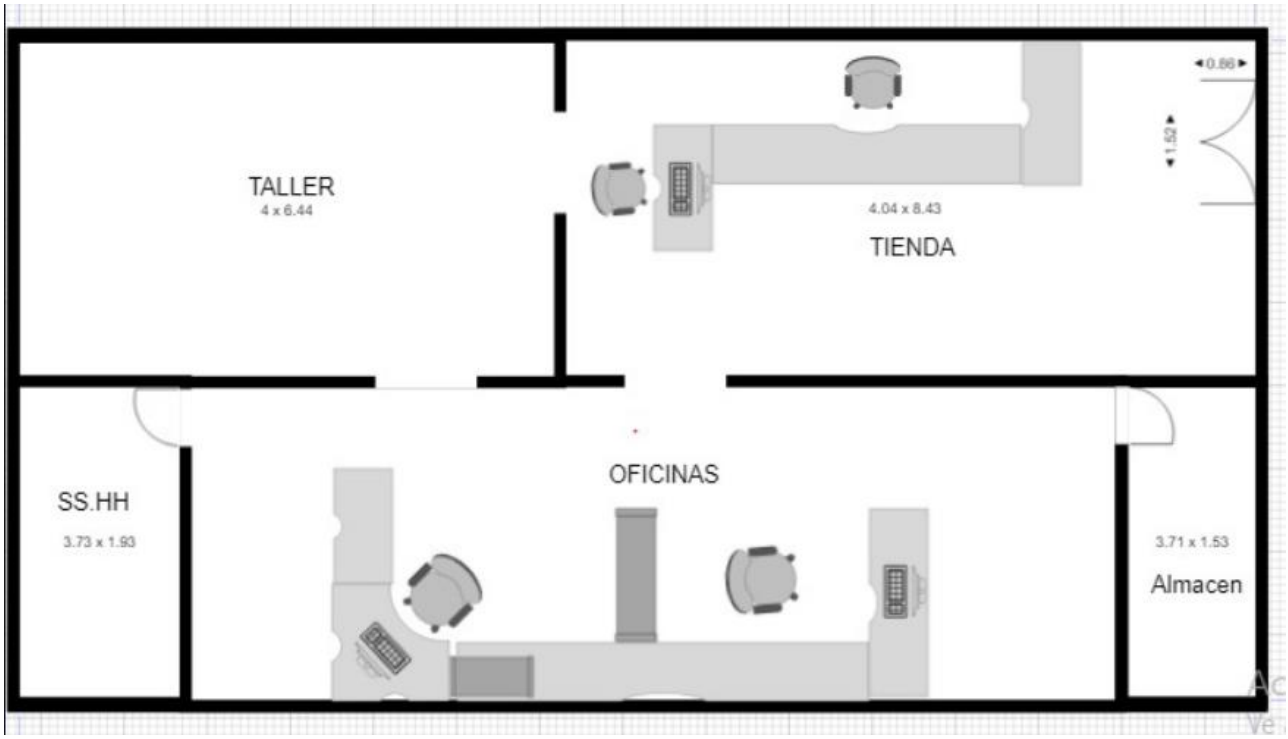


Figura 19: Elaboración propia - Plano de BNC Servicios Generales

- Total, de equipos que componen la red LAN y Wifi.

Equipos	Descripción	Cantidad
Computadoras y Laptops	PC de escritorio con S.O. Windows 10	4
Celulares	Dispositivos Android	6
Patch Core	Cableado ethernet cat6	2
Reuter	Equipo de proveedor Movistar	1
PLC y WifiMesh	Equipos de red inalámbrica	2
TOTAL		15

Tabla 22: Equipos de red BNC Servicios Generales

- Software para el diseño lógico y físico de la red.

Cisco Packet Tracert: Programa de simulación de redes, tiene como principal objetivo diseñar y estructurar una red virtual para someter a pruebas de enrutamiento de paquetes, creación de subredes, configuración de dispositivos principales y finales, etc.

Identificación de Aplicaciones

Los programas que se usaran para ejecutar los procesos de la metodología son los siguientes:

Software	Tipo	Valor	Detalle
Windows 10	Sistema Operativo	Necesario	Sistema operativo instalado en laptop o pc.
ISO Kali Linux	Sistema Operativo	Necesario	Sistema operativo para pruebas de seguridad.

VMWare	Software de virtualización	Necesario	Sistema para simular S.O
Iperf	Software para Test de Red	Necesario	Software para calcular métricas de rendimiento
Google Chrome	Navegador	Necesario	Software navegador de internet
Packet Loss Test	Aplicativo	Necesario	Software tester de red

Tabla 23: Identificación de aplicaciones – Red BNC Servicios Generales

1.2 Identificación de Equipos

Se describen los equipos con el cual está compuesto la red LAN e inalámbrica del negocio así mismo los equipos que también se implementarán donde se realizarán las pruebas de rendimiento.

Hardware	Tipo	Valor	Detalle
Reuter Askey TCG220-46	Reuter Principal	Necesario	Enrutador Principal
PLC TP-Link	Extensor de Red	Necesario	Equipo de red para prueba
WifiMesh TP-Link	Extensor de Red	Necesario	Equipo de red para prueba
Patch Core Cat6	Cable de Red	Necesario	Cable de red LAN
Pc	Equipo de computo	Necesario	Computador de escritorio
Laptop	Equipo Portátil	Necesario	Computador portátil
Celulares	Dispositivo Móvil	Necesario	Host para red

Tabla 24: Identificación de Equipos – Red BNC Servicios Generales

Diseño Lógico – BNC Servicios Generales

Se muestra la red estructurada de la Pyme BNC, el enrutamiento por las diferentes interfaces y los equipos PLC y Wifimesh implementados para ejecutar las pruebas de rendimiento. Direccionamiento por DHCP para cada Host. Puerta de enlace 192.168.0.1.

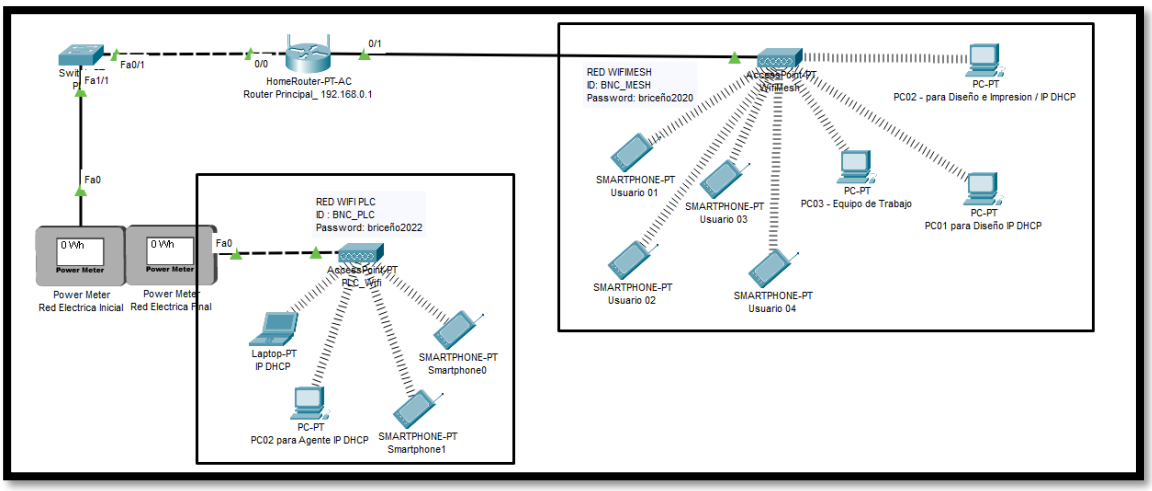


Figura 20: Diseño Lógico - Red BNC Servicios Generales

Diseño Físico – BNC Servicios Generales

Se muestra la ubicación de los equipos que forman la red así mismo los equipos PLC y Mesh para ejecutar la prueba de rendimiento.

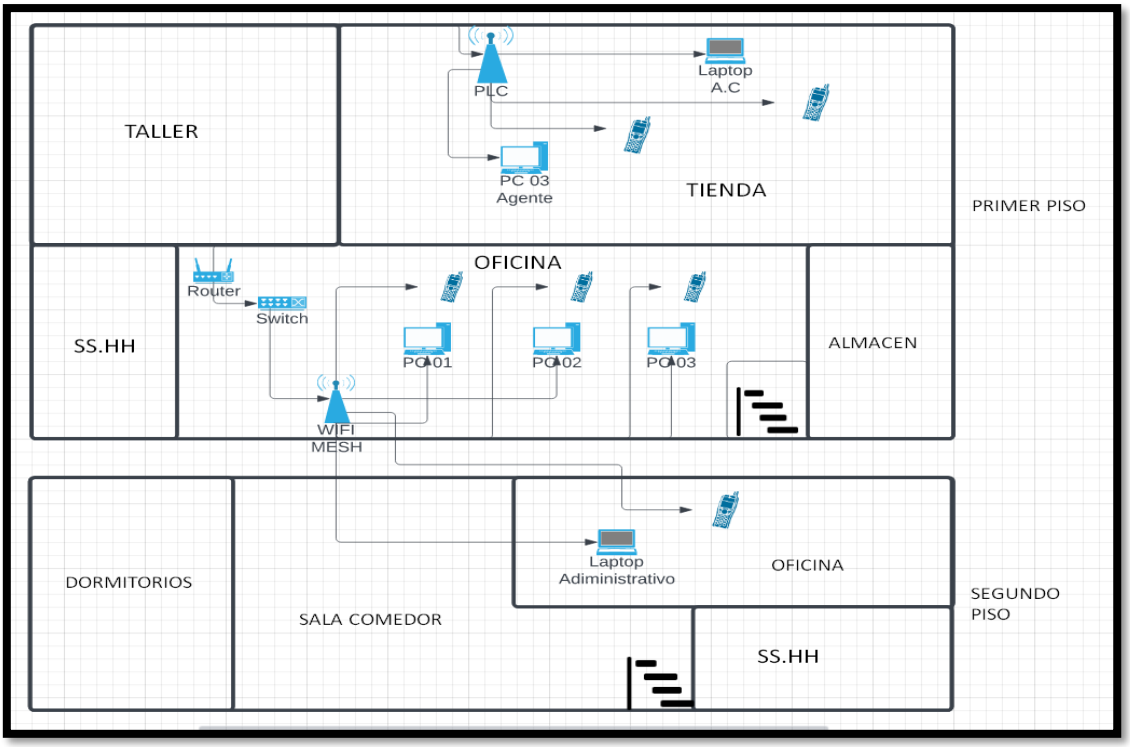


Figura 21: Diseño Físico - Red BNC Servicios Generales

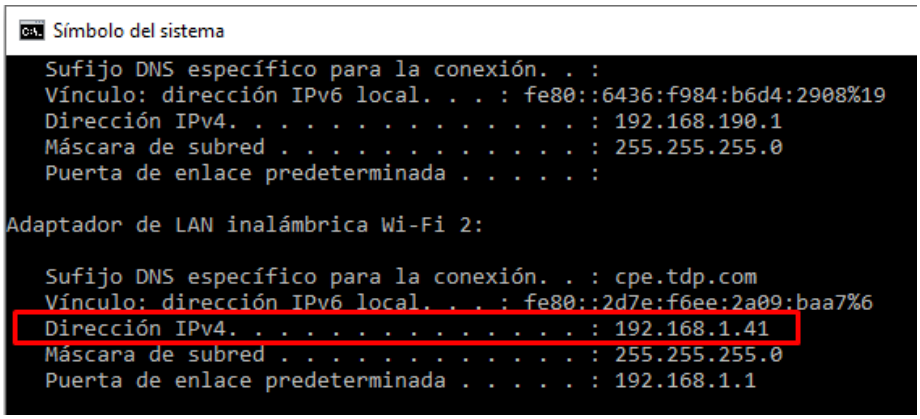
FASE 1: Pruebas de Rendimiento

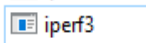
Después de haber instalado los equipos PLC y Wifimesh, a continuación, ejecutaremos las pruebas de rendimiento implementando la herramienta Iperf, en un pc principal que actuara como Modo servidor y otra en Modo Cliente.

Instalación de Herramienta Iperf – Modo Servidor

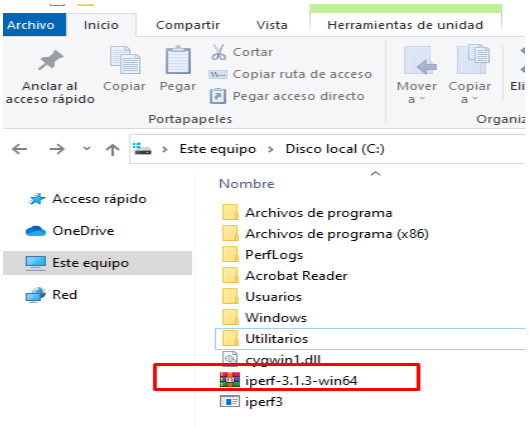
En el pc principal tenemos de dirección Ip **192.168.1.41**, en donde implantaremos el servidor para hacer las pruebas de Jiiter Delay Througput.

- **Configurando Modo servidor**

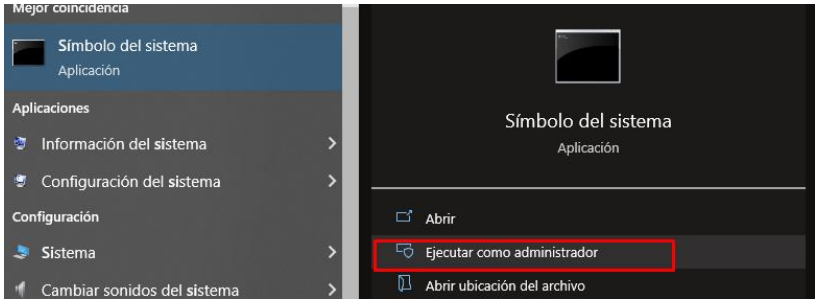


1. Instalar la herramienta Iperf3 en la unidad C.
2. Descomprimir el archivo iperf-3.3.13-win64.rar.
3. El archivo iperf3.exe 

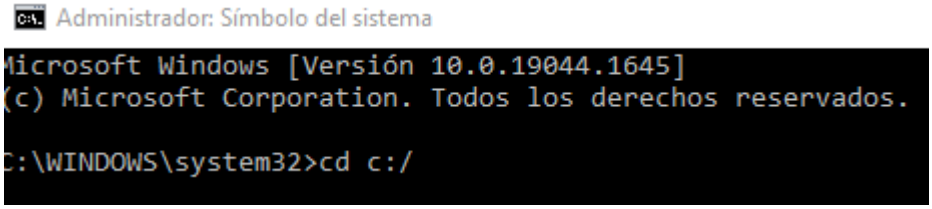
es un formato ejecutable para ejecutar los comandos desde el commandPromt de Windows para realizar las pruebas en modo servidor y cliente.



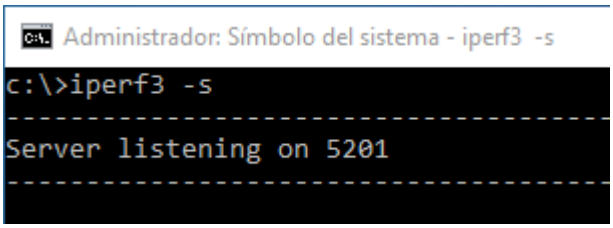
4. Ejecutar el CommandPromt de Windows con permiso administrador.



5. Accedemos a la herramienta iperf3 desde la consola con el siguiente comando: **cd c:/**.



6. Ejecutamos el comando iperf3 –s, este comando asignará la computadora en modo servidor y por defecto asigna el puerto 5201 por donde hará escucha desde cualquier host.

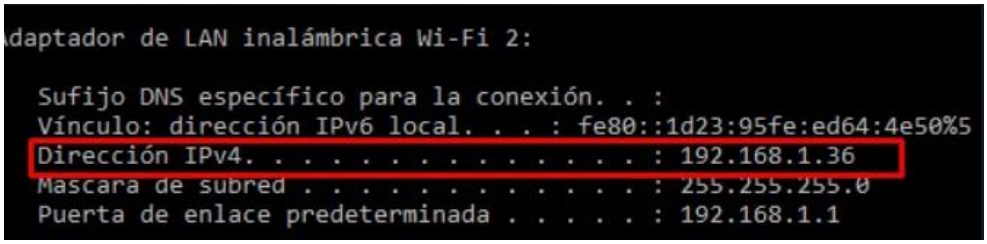


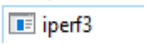
7. Finalmente, el equipo está configurado en modo servidor.

- **Configurando Modo Cliente**

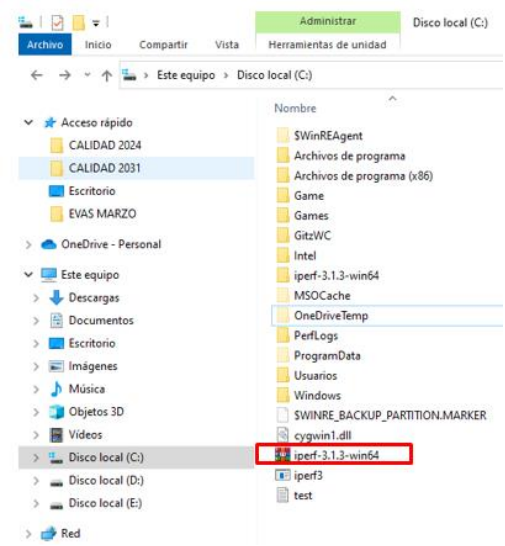
Usaremos una laptop para el Modo Cliente, la dirección **ip 192.168.1.36**, se conectará a la red inalámbrica PLC / Wifimesh para ejecutar las pruebas de rendimiento.

1. Conectar a la red inalámbrica PLC / Wifimesh.
2. Ejecutar el comando **ipconfig** desde el **command promt** de Windows en modo servidor para obtener la ip asignada a la laptop.

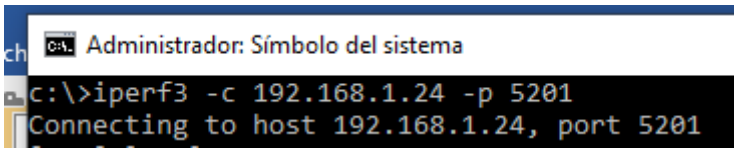


3. Instalar la herramienta Iperf3 del mismo modo que se ejecutó para el modo servidor, unidad c.
4. Descomprimir el archivo y mantener el ejecutable 

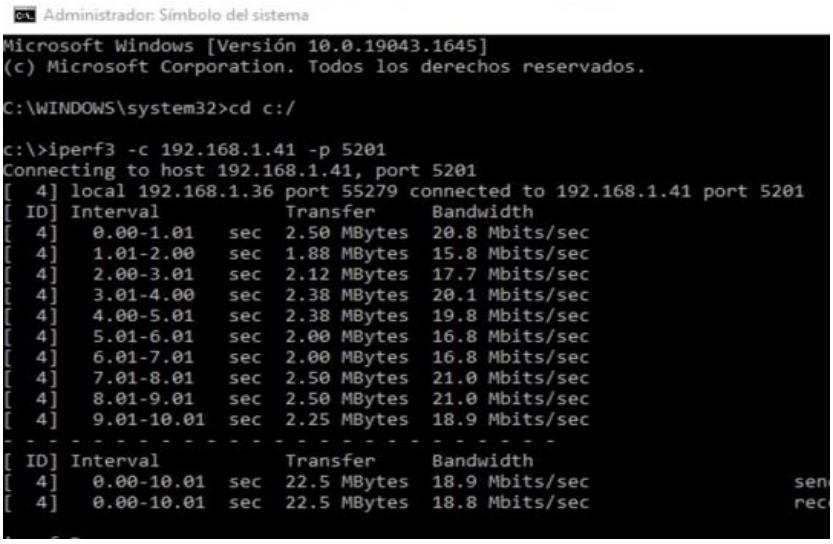
iperf3.exe



5. Abrir el CommandPromt de Windows con permiso de administrador.
6. Ejecutar el comando **cd c:/**, para acceder a la herramienta iperf3.
7. Ejecutar el comando **iperf3 –c 192.168.1.41 –p 5201**.



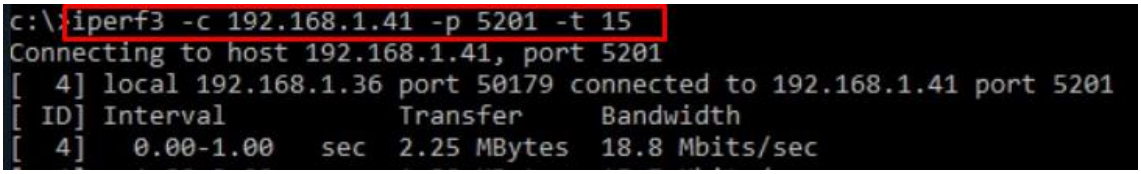
8. Se confirmará la conexión de PC cliente a PC Servidor una vez ejecutado el comando anterior se muestra en la siguiente figura la respuesta del servidor con una muestra de 10 segundos.



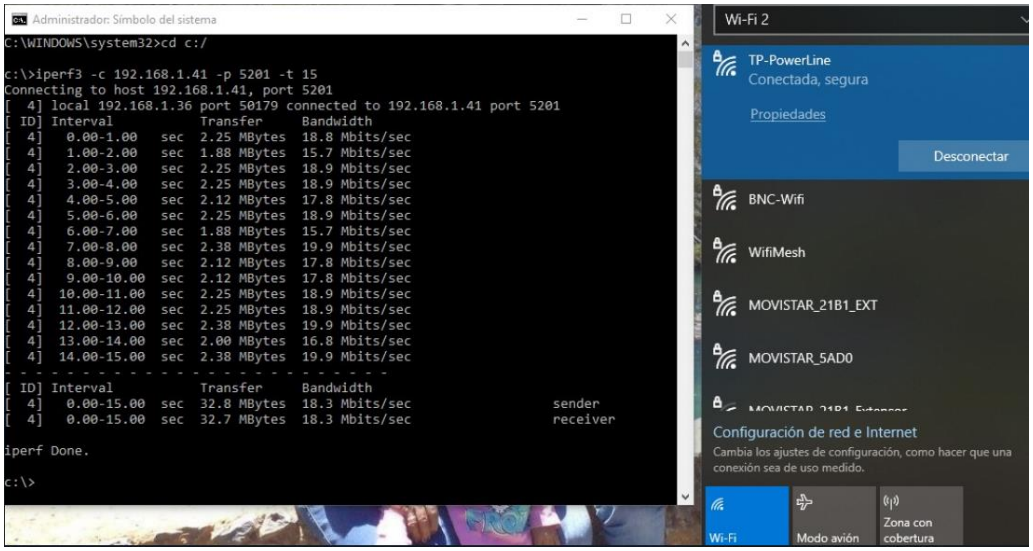
9. Conexión establecida PC cliente con PC Servidor.

Pruebas para Trouhgput – Implementando PLC con WifiMesh

6. Para medir la Tasa de trasferencia, primero nos conectamos a la red inalámbrica PLC.
7. Ejecutamos el **CommandPromt** de Windows con permiso de administrador. Accedemos a la carpeta donde se encuentra iperf3.exe y ejecutamos el siguiente comando: **iperf3 –c 192.168.1.41 –p 5201 –t 15.**

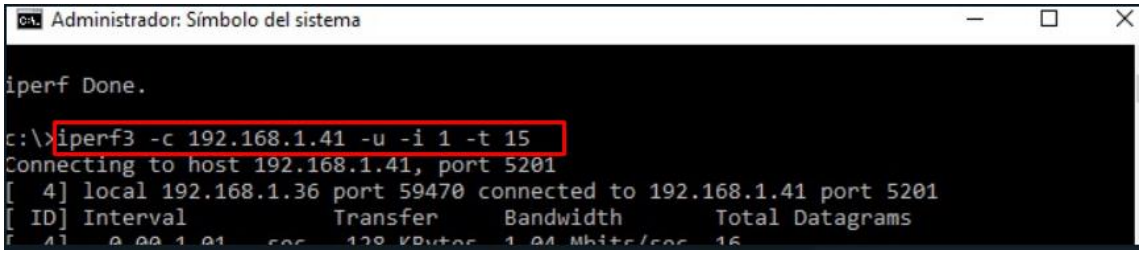


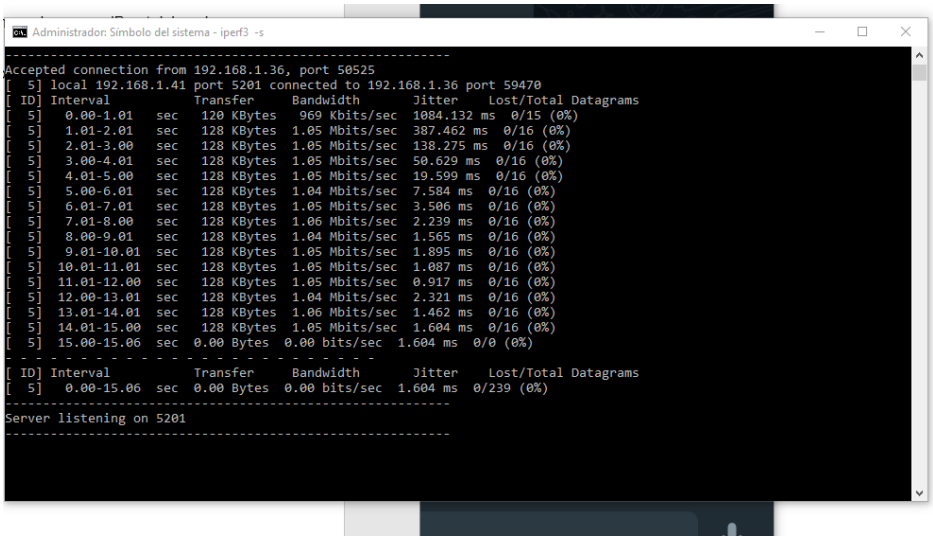
8. Se ejecuta y se obtienen los resultados para tasa de transferencia.



Pruebas para Jitter – Implementando PLC con WifiMesh

6. Para medir el Jitter para variación de tiempo de transmisión, primero conectar a la red inalámbrica PLC / WifiMesh.
7. Ejecutamos el CommandPront de Windows con permiso de administrador.
8. Acceder a la carpeta donde se encuentra iperf3.exe y empezar a ejecutar el siguiente comando: **iperf3 – c 192.168.1.41 –u –i 1 –t 15**
9. Las mediciones de jitter se expresarán en el commandPront del modo servidor.
10. Se capturan los valores del commandPromt del pc **modo servidor** y se registra en las fichas.

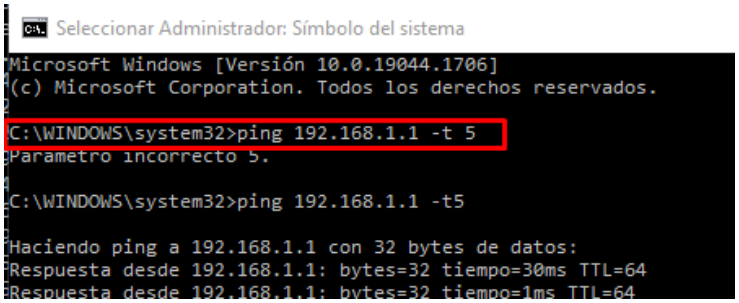


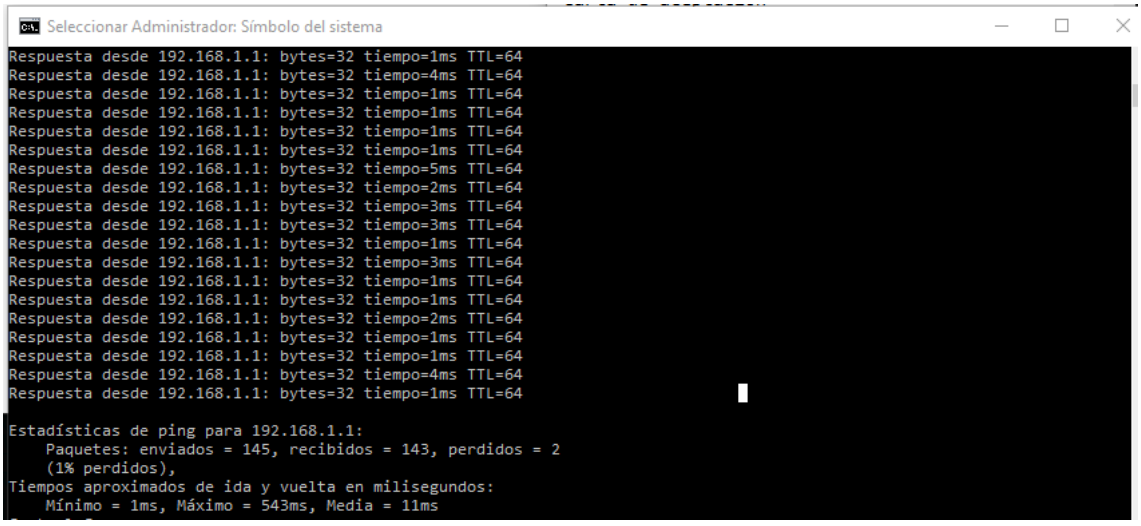


Prueba para Delay PLC con WifiMesh

✓ Porcentaje de paquetes perdidos

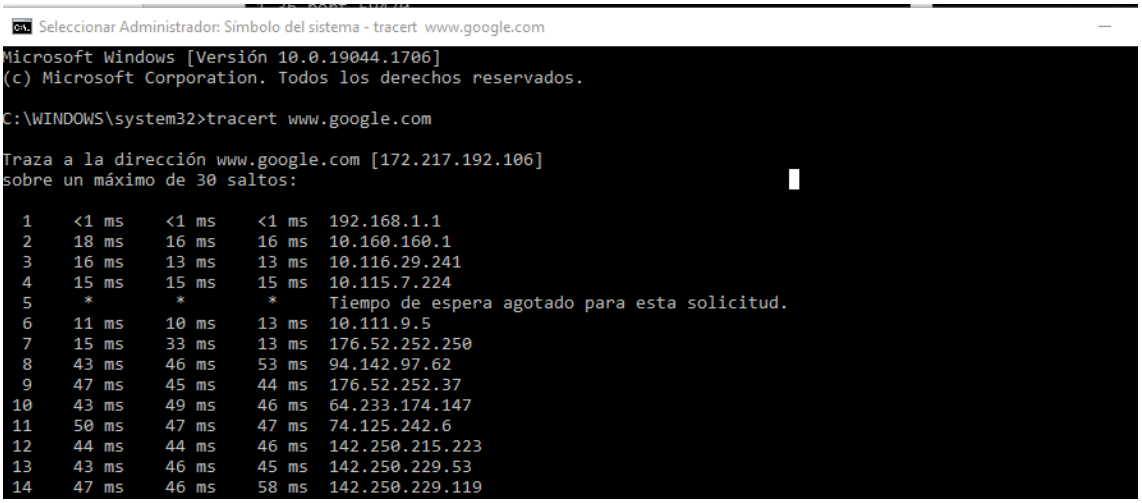
5. Conectarse a la red inalámbrica PLC / WifiMesh.
6. Ejecutar el CommandPront de Windows con permiso de administrador.
7. Se ejecuta el siguiente comando ping **192.168.1.1 –t 5**, el comanda **–t** permite asignar el tiempo de escucha en este caso de 5 minutos para cada intervalo de 1hra para la prueba.





✓ Retardo extremo a extremo

1. Para medir el retardo extremo a extremo primero conectarse a la red inalámbrica
2. Ejecutamos el CommandPront de Windows con permiso de administrador.
3. Se ejecuta el siguiente comando **tracert 192.168.1.1 –t 5**, el comanda **–t** permite asignar el tiempo de escucha en este caso de 5 minutos para cada intervalo de 1hra para la prueba. El comando tracert permite ver la traza que viaja un paquete hasta llegar hacia su destino.



4. Se capturan los valores del commandPromt y se registra en las fichas.

FASE 3: Nivel de Seguridad - BCN Servicios Generales

Planificación

Se determinan los objetivos y propósitos de las evaluaciones del mismo modo se establece el alcance que se tendrá con el equipo de trabajo.

Definición de objetivos:

- ✓ Identificar vulnerabilidades Físicas
- ✓ Identificar Vulnerabilidades Lógicas
- ✓ Describir las características de los dispositivos o tecnologías involucradas

Equipo de Trabajo:

Tester	Objetivo
Pablo E. Maldonado Jiménez (Estudiante Hacking Wifi - Academia de Ciber Seguridad Hacker Mentor)	Evaluar la seguridad de red de la empresa **BNC Servicios Generales**

Tabla 25: Equipo de trabajo para red BNC Servicios Generales

Especificación

Se describen los equipos que forman parte de la infraestructura de red y seguridad del negocio.

- ✓ **Evaluación de la red y Equipos**
  - Equipos del Negocio BNC Servicios Generales

Equipos / Host	Tecnología	Características
Reuter TCG220-46	Askey Reuter (Proveedor Movistar)	Band 2.4GHZ 300Mbps Soporte WEP 64/128 bits, WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC.
Switch	Tp-Link	SG108 8 Puertos 10/100/1000 Mbps

PC1	Sistema Operativo Windows 10	Core i3-3220 CPU 2.90Ghz RAM 4 GB – Disco 1TB
PC2	Sistema Operativo Windows 10	Core i3-3220 CPU 2.90Ghz RAM 4 GB – Disco 500 GB
PC3	Sistema Operativo Windows 10	Core i3-3220 CPU 2.90Ghz RAM 4 GB – Disco 500 GB
PC4	Sistema Operativo Windows 10	Core i3-3220 CPU 2.90Ghz RAM 4 GB – Disco 500 GB
Laptop	Sistema Operativo Windows 10.	Core i5-6500 CPU 3.02Ghz RAM 4 GB – Disco 500 GB

Tabla 26: Equipos de red BNC Servicios Generales

- Equipos para evaluar la red del Negocio BNC Servicios Generales

Equipos / Host	Tecnología	Características
TL – WN722N V.1	Adapter USB - TPLink	Antena desmontable 4dBI – 150Mpbs Soporte WEP 64/128 bits, WPA-PSK/WPA2-PSK, Filtrado inalámbrico de MAC. Soporta Modo Monitor
PC-Desktop SCNM98P	S.O Windows10	Core i5-10400 CPU 2.90Ghz RAM 16 GB – SSD 500
PC-Virtual VMWARE	S.O. KaliLinux – Kernel 5.15.	Core i5-10400 CPU 2.90Ghz RAM 8 GB – SSD 100

Tabla 27: Equipos para evaluar la red BNC Servicios Generales

Ejecución

Técnicas y Herramientas:

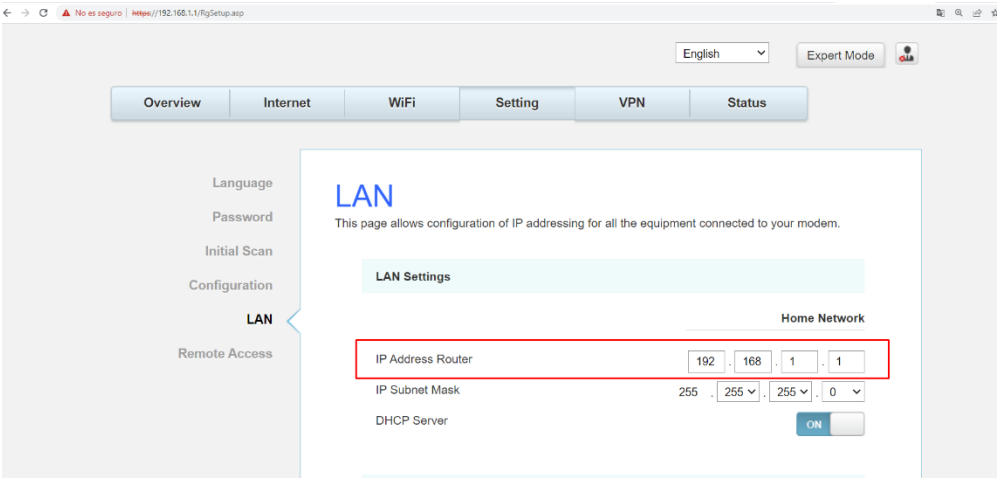
Se entiende por técnicas a algoritmos o códigos para aplicar mediante un software e iniciar los ataques, de la misma manera herramientas al uso de software o hardware que sean necesarios para las pruebas.

Nombre de Herramienta	Característica
Nmap	Aplicación de multiplataforma, permite analizar las redes y extraer información acerca de los servicios y sistemas operativos de los dispositivos dentro de una red.
Hpig3	Esta herramienta se utiliza en Kali Linux desde la terminar para el análisis y ensamblado de paquetes TCP.
Aircrack – ng	Software con un paquete detector, permite rastrear paquetes WEP y WPA/WPA2 –PSK. Analizador de redes LAN e Inalámbricas.
Airmong-ng	Este escript permite habilitar el modo monitor del adaptador de red para hacer escucha al tráfico de redes inalámbricas.
Airodump-ng	Este escript permite capturar paquetes inalámbricos además acumula vectores de inicialización.
Aireplay-ng	Este script permite inyectar fotogramas, genera tráfico para su uso posterior y descifrar claves WEP y WPA-PSK.

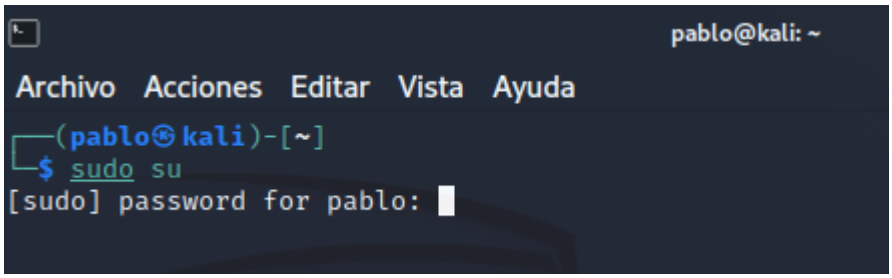
Tabla 28: *Técnicas y herramientas para evaluar red BNC Servicios Generales*

- Escaneo de Puertos:

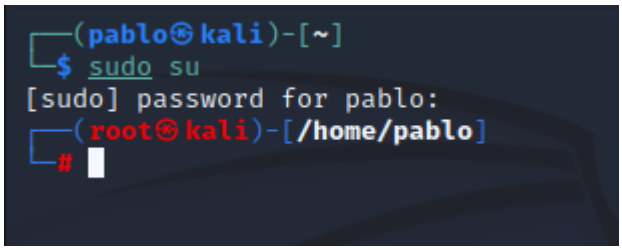
1. Identificar dirección Ip del equipo principal de red Reuter TCG220-46, ip 192.168.1.1.



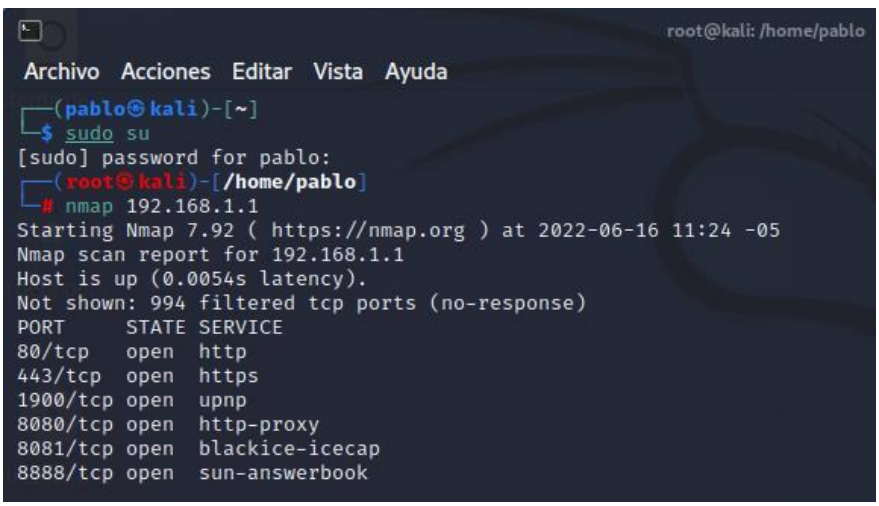
2. Inicializamos el Sistema Kali Linux
3. Abrimos el terminal e inicializamos en modo administrador con el comando **sudo su**



4. Ingresamos la clave de acceso como administrador



5. Empezamos a hacer el escaneo de puerto con el siguiente comando **nmap 192.168.1.1**



Se visualiza en la figura anterior el escaneo de 1000 puertos en una velocidad que ofrece el terminal de 0.0054 segundos, se identifica en la red inalámbrica **6** puertos lógicos abiertos.

- Identificación de Vulnerabilidades:

Se describen las siguientes vulnerabilidades identificadas en el nivel lógico y físico de la red inalámbrica **BNC Servicios Generales**

- ✓ Vulnerabilidades Lógicas: Red Lan/wlan BNC Servicios Generales

Red Inalámbrica **BNC Servicios Generales**	Reuter Askey – Proveedor Movistar
Puertos TCP Abiertos	6
Servicios	6
Mode-Encryptacion	WPA2-AES

Tabla 29: Vulnerabilidades Lógicas de equipo Wifi BNC Servicios Generales

Vulnerabilidades por Equipos	**Antivirus**	**Sistema Operativo**	**Windows Defender Firewall**	**Actualizaciones de S.O**	**Contraseñas**
PC 01	No	No activo	Deshabilitado	Pendiente	No
PC 02	No	No activo	Deshabilitado	Pendiente	No
PC 03	No	No activo	Deshabilitado	Pendiente	No
PC 04	Si / Vencido	Activo	Habilitado	Pendiente	No
Laptop	Si / vencido	No activo	Habilitado	Pendiente	No

Tabla 30: Vulnerabilidades por host de la red BNC Servicios Generales

- Vulnerabilidades Físicas: Red Lan/wlan BNC Servicios Generales

Vulnerabilidades por Equipos	Puertos USB
PC 01	Habilitados
PC 02	Habilitados
PC 03	Habilitados
PC 04	Habilitados
Laptop	Habilitados

Tabla 31: Vulnerabilidades Físicas red BCN Servicios Generales

Caracterización de Vulnerabilidades

Se especifican y describen las vulnerabilidades encontradas en la red wlan del negocio.

- Los puertos abiertos en un equipo de red son un foco importante si se quiere vulnerar la seguridad. Se describen los siguientes puertos abiertos.

PUERTO	ESTADO	SERVICIO	CARACTERISTICAS
80 / TCP	Abierto	HTTP	Puerto web para conexión hacia servidores. Se puede hacer ataque de inyección XSS y SQL entre otros.
443 / TCP	Abierto	HTTPS	Puerto por default para utilizar Hypertex Tranfers Protocol Secure.
1900 / TCP	Abierto	UPNP	Garantiza la entrega de paquetes de datos en la misma orden, en que fueron mandados.
8080 / TCP	Abierto	HTTP-PROXY	Se usa mayormente para proxy y puerto de almacenamiento en cache trafico http.
8081 / TCP	Abierto	BLACKICE-ICECAP	Blackice-ICap Puerto aperturado por software para administración de firewall.
8888 / TCP	Abierto	SUN-ANSWERBOOK	Utilizado como puerto alternativo http para algunas aplicaciones

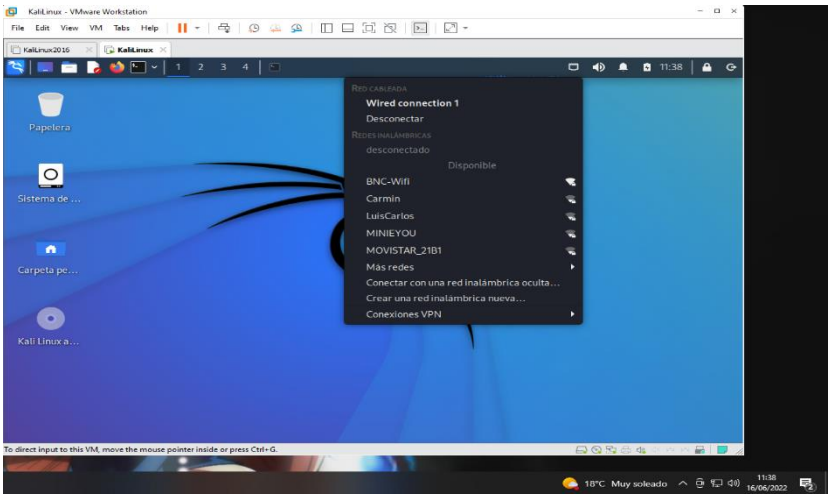
Tabla 32: Caracterización de Vulnerabilidades red BCN Servicios Generales

Prueba de Fuerza Bruta – Red BNCWifi

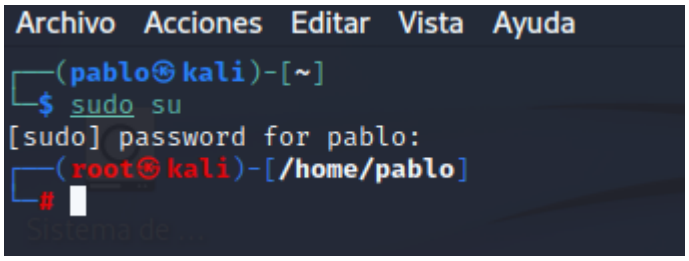
Etapa de Descubrimiento:

En esta etapa se enfoca en reconocer los riesgos asociados a la red del mismo modo que se obtiene información como segmentos de redes y rangos de direcciones IP´s

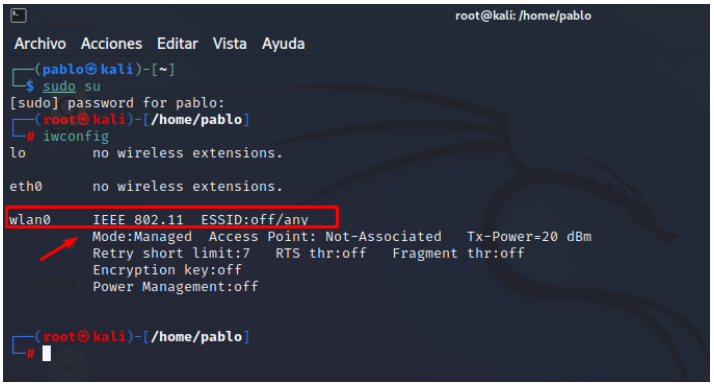
1. Conectar adaptador de red Wifi



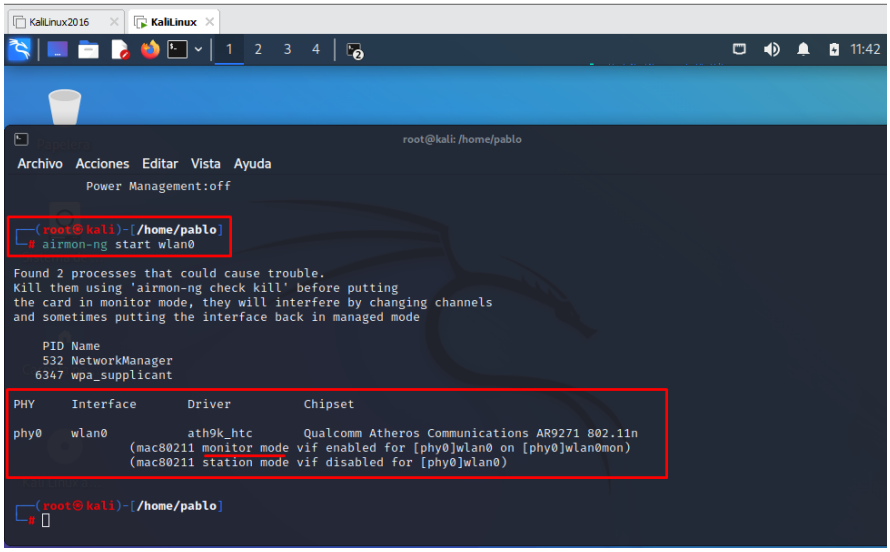
2. Abrir el terminal en modo administrador con el comando **sudo su**, ingresamos la clave de usuario



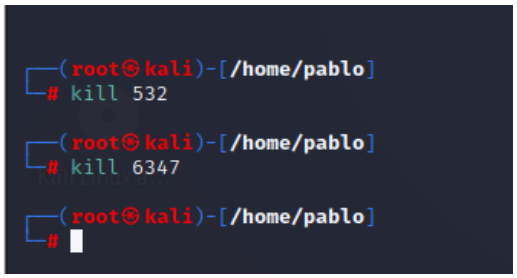
3. Ingresamos el siguiente comando **iwconfig** para ver que el sistema acepte al adaptador de red, como podemos ver esta en **Mode Managed**. Tenemos que cambiar a **Mode monitor** para hacer escucha de red.



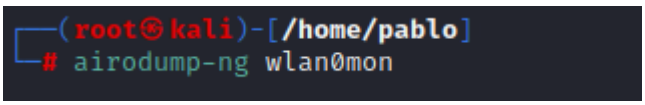
4. Ejecutamos el comando **airmon-ng start wlan0** para habilitar el **mode monitor** del adaptador inalámbrico.



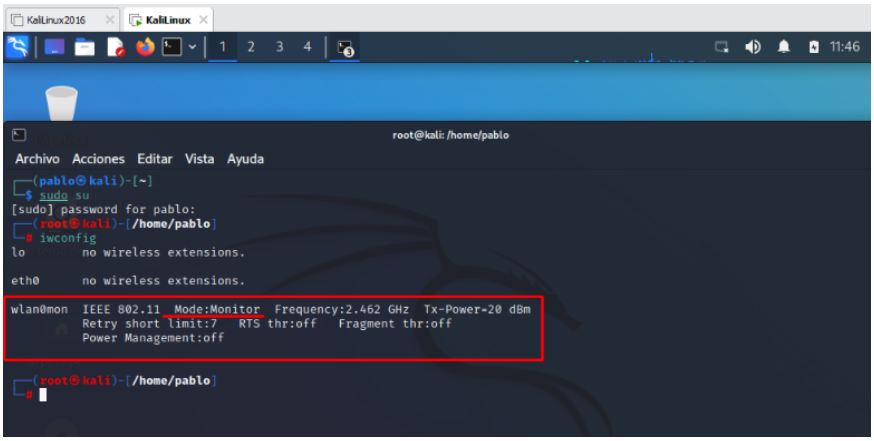
5. Para que se habilite el mode monitor del adaptador de red tenemos que matar los procesos con el siguiente comando **kill.**



6. Escribir el comando **airodump-ng** wlan0mon para activar el mode monitor

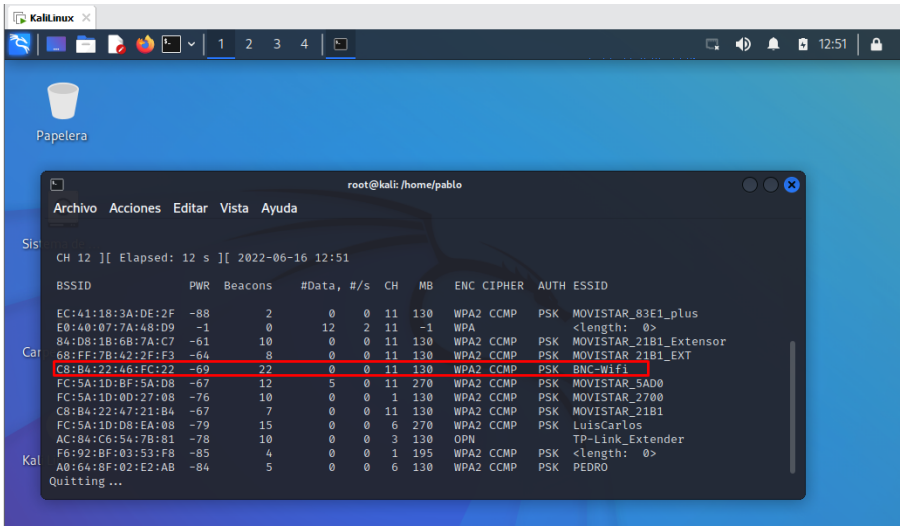


7. Ingresamos por consola el comando iwconfig y visualizamos que el adaptador ya está en mode monitor, listo para empezar el ataque.

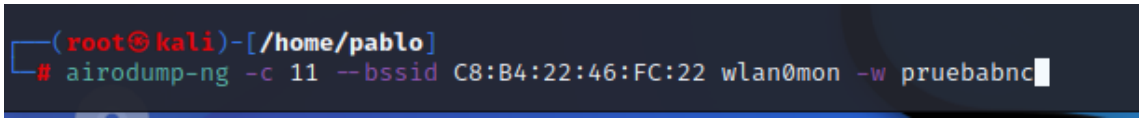


Etapa de Exploración:

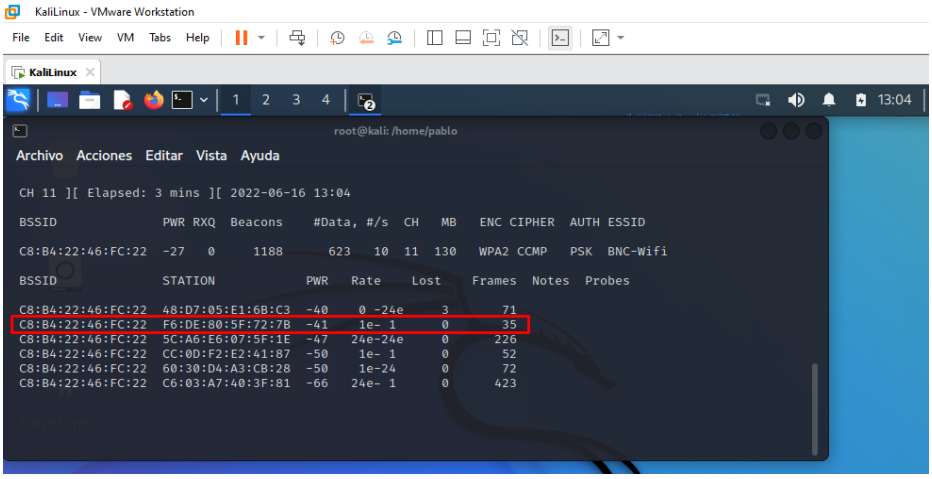
1. Ejecutar el comando **airodump-ng wlan0mon,** empieza la etapa de exploración donde se hace escucha a las redes inalámbricas, identificamos el nombre de la red **BNC-Wifi** con la MAC y el canal por el cual se desempeña.



2. Ingresamos el siguiente comando **airodump-ng –c 1 -–bssid** C8:B4:22:46:FC:22 **wlan0mon –w** pruebabnc para escanear la red a la cual atacaremos, del mismo modo crearemos un archivo **pruebabnc** donde se almacenará el paquete después de hacer handshake.

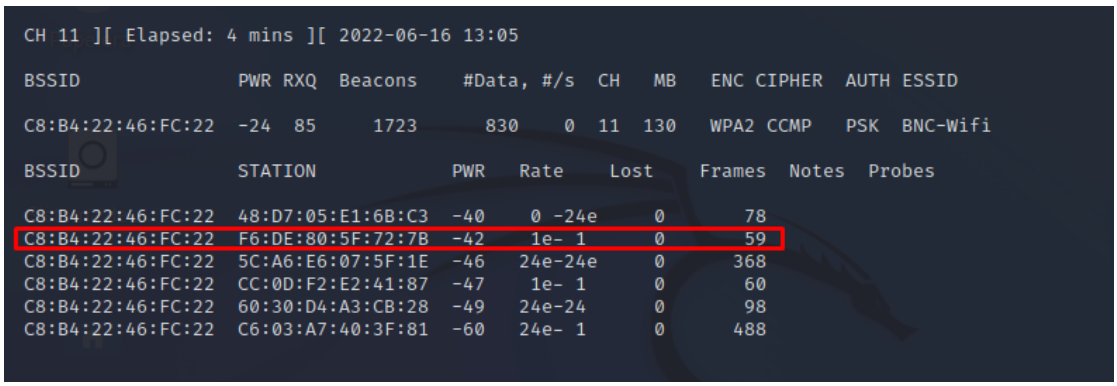


3. Después de escanear la red, se mostrarán los dispositivos conectados hacia la red inalámbrica, por el cual se intercederá para iniciar el ataque.

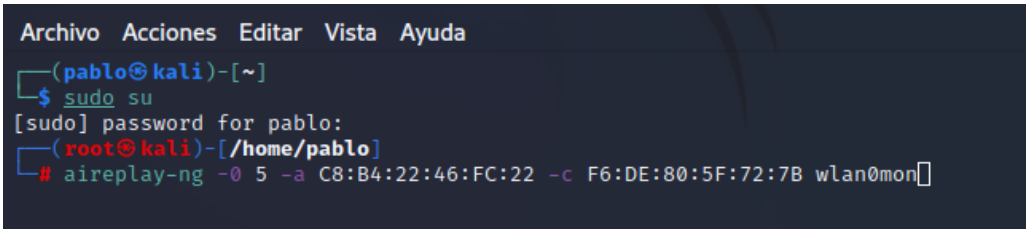


Etapa de Evaluación:

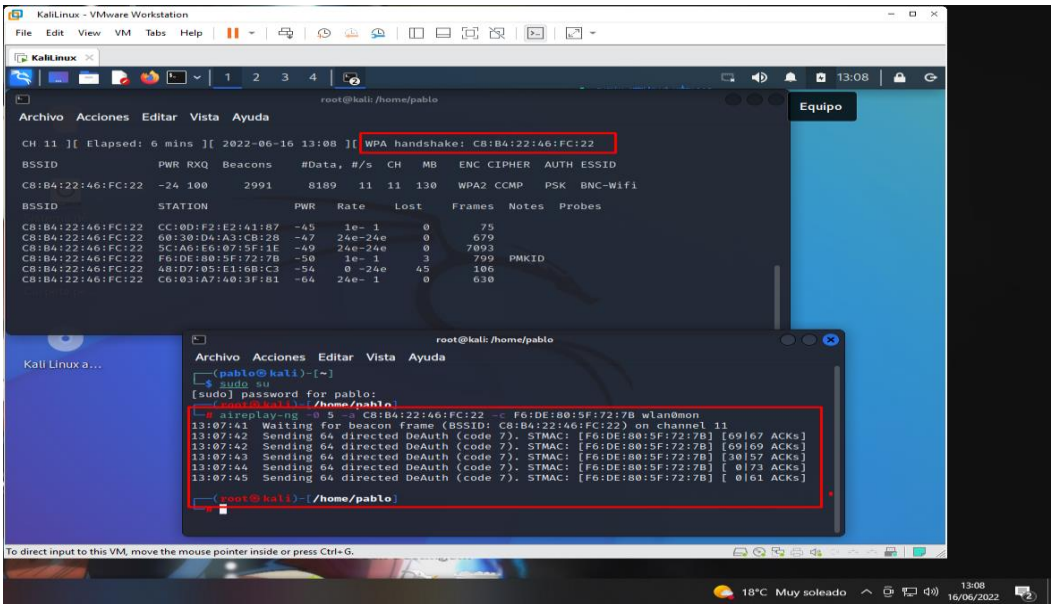
5. Identificamos el dispositivo conectado a la red por el cual se capturará la clave autenticada. Seleccionaremos la serie Mac para identificarlo.



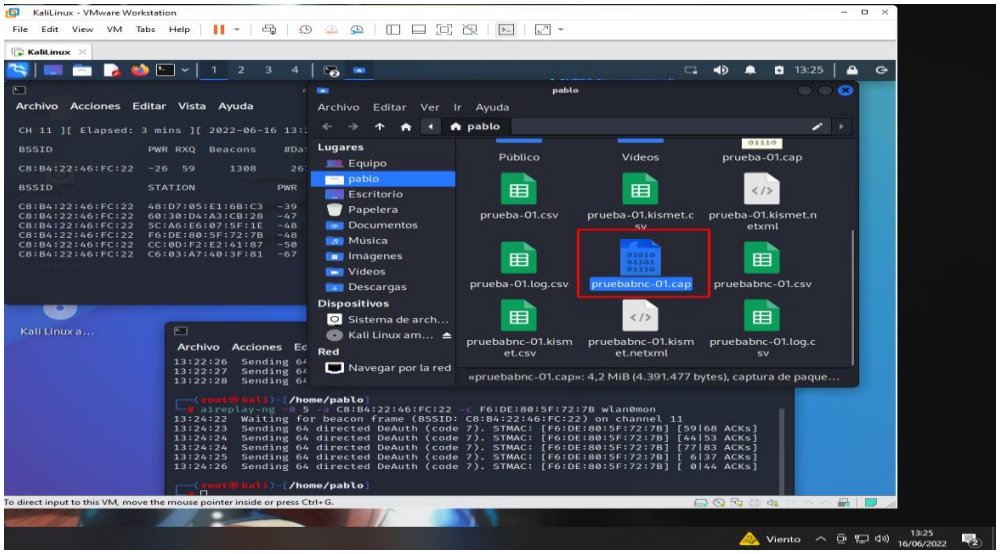
6. Ejecutamos el siguiente comando: **aireplay-ng -0 5 –a** C8:B4:22:46:FC:22 **–c** F6:DE:80:5F:72:7B **wlan0mon.**



7. Después de ejecutar el comando del paso n°2 verificamos que se captura el paquete donde contiene el descifrado de clave, haciendo handshake.

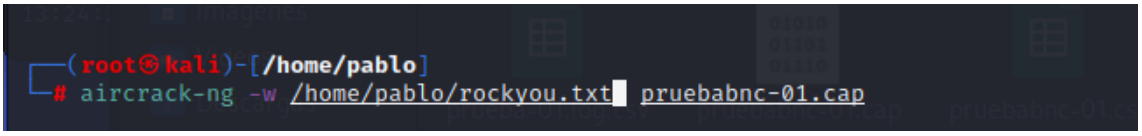


8. Se genera la captura del paquete de encriptación de clave de red y se almacena en un formato **.cap**, **pruebabnc.cap**.

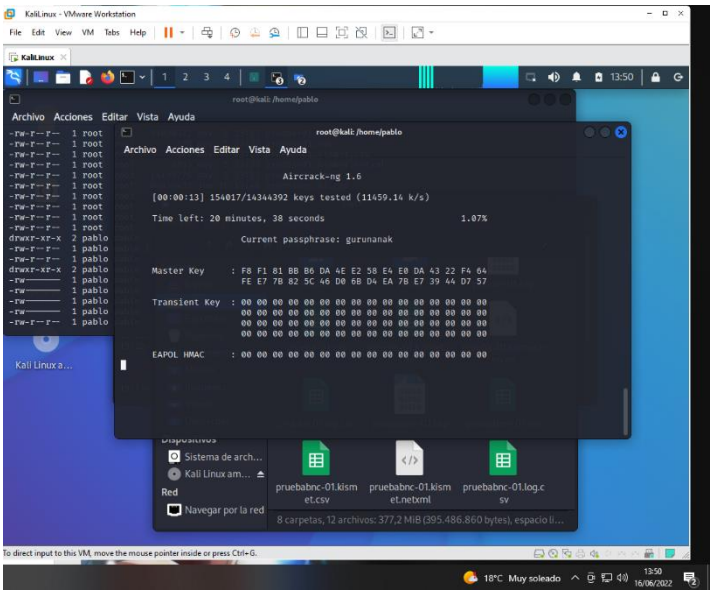


Etapa de Intrusión:

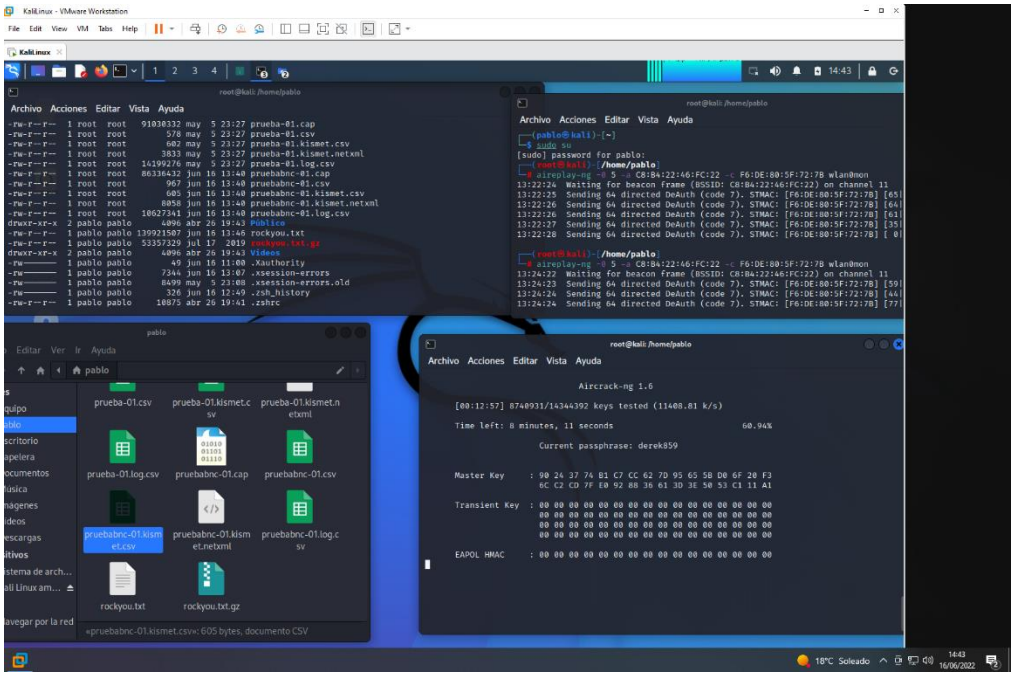
6. Identificar la ruta del archivo **pruebabnc.cap.**
7. Ingresar al terminal con permiso administrador, **sudo su.**
8. Ejecutamos el siguiente comando **aircrack-ng –w /usr/share/wordlists/rockyou.txt pruebabnc-01.cap.**



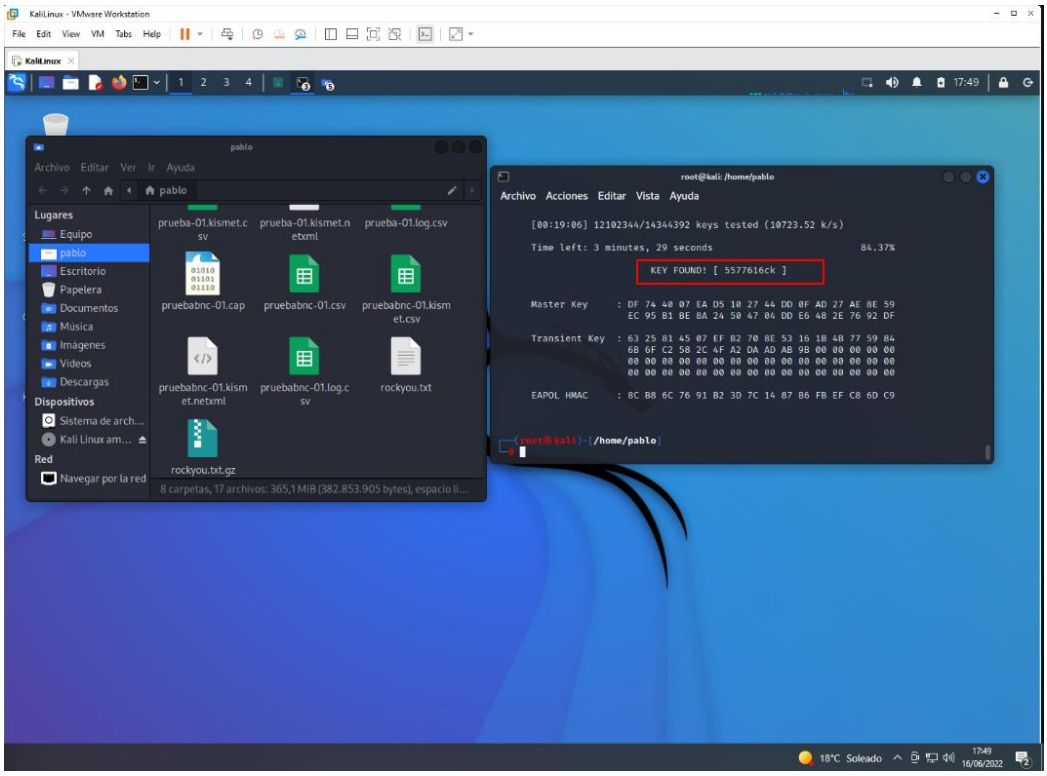
9. Se inicializa el ataque por fuerza bruta por diccionario rockyou.



El ataque por fuerza bruta depende de los diccionarios que se usen puesto que puedan contener más de 2 millones de claves y permutaciones.



Después de más de 3hrs en ataque hacia la red inalámbrica se llega a vulnerar la red. Se muestra la clave descifrada en la siguiente figura.



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, RODRIGUEZ BACA LISET SULAY, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "METODOLOGÍA PARA LA EVALUACIÓN DEL RENDIMIENTO DE RED EN TECNOLOGÍAS INALÁMBRICAS WLAN", cuyo autor es MALDONADO JIMENEZ PABLO ENRIQUE, constato que la investigación cumple con el índice de similitud establecido, y verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 07 de Julio del 2022

Apellidos y Nombres del Asesor:	**Firma**
RODRIGUEZ BACA LISET SULAY **DNI:** 41353210 **ORCID** 0000-0003-1850-615X	Firmado digitalmente por: LRODRIGUEZB14 el 12-07-2022 17:32:02

Código documento Trilce: TRI - 0325665

INVESTIGA UCV