+

UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE TELECOMUNICACIONES

Evaluación de la calidad de servicio de la red del Bloque A de la Facultad de Ingeniería, mediante el modelo de políticas y colas para determinar posibles falencias de la red y proponer una solución de mejora.

Trabajo de Titulación para optar al título de:
INGENIERO EN TELECOMUNICACIONES

Autor:
Mayra Andrea León León

Tutor:
Msc. José Luis Jinez Tapia

Riobamba, Ecuador. ***2025***

DECLARATORIA DE AUTORÍA

Yo, **MAYRA ANDREA LEÓN LEÓN**, con cédula de ciudadanía **0603953993-**, autor del trabajo de investigación titulado: **EVALUACIÓN DE LA CALIDAD DE SERVICIO DE LA RED DEL BLOQUE A DE LA FACULTAD DE INGENIERÍA, MEDIANTE EL MODELO DE POLÍTICAS Y COLAS PARA DETERMINAR POSIBLES FALENCIAS DE LA RED Y PROPONER UNA SOLUCIÓN DE MEJORA**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 10 de enero del 2025.

.

_____

Mayra Andrea León León
C.I:060395399-3

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, **José Luis Jinez Tapia** catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación titulado: **EVALUACIÓN DE LA CALIDAD DE SERVICIO DE LA RED DEL BLOQUE A DE LA FACULTAD DE INGENIERÍA, MEDIANTE EL MODELO DE POLÍTICAS Y COLAS PARA DETERMINAR POSIBLES FALENCIAS DE LA RED Y PROPONER UNA SOLUCIÓN DE MEJORA**, bajo la autoría de **Mayra Andrea León León**; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los 10 del mes de enero de 2025

Msc. José Luis Jinez Tapia
C.I: 0602899007

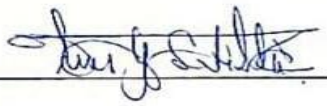
CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **EVALUACIÓN DE LA CALIDAD DE SERVICIO DE LA RED DEL BLOQUE A DE LA FACULTAD DE INGENIERÍA, MEDIANTE EL MODELO DE POLÍTICAS Y COLAS PARA DETERMINAR POSIBLES FALENCIAS DE LA RED Y PROPONER UNA SOLUCIÓN DE MEJORA** por **Mayra Andrea León León**, con cédula de identidad número **060395399-3**, bajo la tutoría Msc. José Luis Jinez Tapia; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

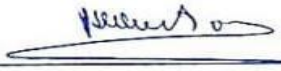
De conformidad a la normativa aplicable firmamos, en Riobamba 10 de enero del 2025

Alejandra Del Pilar Pozo Jara, /Mgs.
PRESIDENTE DEL TRIBUNAL DE GRADO

Luis Gonzalo Santillán Valdiviezo. /Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO



Klever Hernán Torres Rodríguez. / Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO



CERTIFICADO ANTIPLAGIO

C E R T I F I C A C I Ó N

Que, Mayra Andrea León León con CC: 0603953993, estudiante de la Carrera Telecomunicaciones, Facultad de INGENIERÍA; ha trabajado bajo mi tutoría el trabajo de investigación titulado " EVALUACIÓN DE LA CALIDAD DE SERVICIO DE LA RED DEL BLOQUE A DE LA FACULTAD DE INGENIERÍA, MEDIANTE EL MODELO DE POLÍTICAS Y COLAS PARA DETERMINAR POSIBLES FALENCIAS DE LA RED Y PROPONER UNA SOLUCIÓN DE MEJORA", cumple con el 8 %, de acuerdo al reporte del sistema Anti plagio **TURNITIN**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 16 de diciembre de 2024

Firmado electrónicamente por:
JOSE LUIS JINEZ TAPIA

Msc. José Luis Jinez Tapia
TUTOR

DEDICATORIA

Dedico mi Trabajo de Titulación a mis padres, Luis León y Marlene León, quienes desde un inicio me han bendecido cada día brindándome amor y apoyo incondicional, gracias a sus esfuerzos y sacrificios estoy logrando cumplir el sueño más anhelado.

A mi hija Aylin Valeska, por ser una fuente constante de inspiración y motivación para ir tomando cada paso en este camino, su alegría y amor incondicional han sido de mucho apoyo para seguir surgiendo, ya que este logro es por las dos.

Mayra Andrea León León

AGRADECIMIENTO

Quiero expresar un agradecimiento sincero a mi tutor de tesis, Msc. José Jinez, por su respeto, guía, paciencia y dedicación infinita. Su instrucción y destreza fueron fundamentales para el desarrollo de este proyecto de titulación.

Mi agradecimiento se extiende a Msc. Luis Santillán por su constante respaldo, comprensión y apoyo a lo largo de esta travesía, su tolerancia y animación fueron esenciales para superar los retos y alcanzar este resultado.

Finalmente, quiero expresar mi gratitud a todas las personas que, de una forma u otra, colaboraron al logro de este trabajo de titulación. Su contribución fueron de gran valor que dejaron huellas en este trabajo.

Mayra Andrea León León

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURA

RESUMEN

Este estudio analiza la calidad de servicio (QoS) de la red en el bloque A de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo. Mediante el uso de modelos de políticas y colas (FIFO, WFQ y CBWFQ), el estudio detecta problemas en la infraestructura de red vinculados con la ausencia de cobertura inalámbrica, escasez de puntos de acceso y un ancho de banda restringido. A través de técnicas experimentales y analíticas, se examinan factores cruciales como jitter, latencia, pérdida de paquetes y rendimiento, con el objetivo de entender su impacto en la eficacia de la red y las experiencias de los usuarios.

El estudio emplea instrumentos como GNS3 y Ostinato para replicar escenarios, creando tráfico realista y evaluando el desempeño de las configuraciones actuales. Los hallazgos indican que la implementación de políticas de calidad de servicio facilita la priorización del tráfico, la disminución de la congestión y la optimización de la distribución del ancho de banda, favoreciendo actividades fundamentales como el acceso a servicios académicos y administrativos. Las conclusiones proporcionan respuestas concretas para mejorar el desempeño de la red, que incluyen la puesta en marcha de configuraciones fundamentadas en CBWFQ con QoS para una administración eficaz del tráfico.

Palabras clave: Calidad de servicio (QoS), modelo de políticas y colas, jitter, latencia, throughput, simulación de red, CBWFQ, optimización de redes, gestión del tráfico.

ABSTRACT

This study analyzes the network's quality of service (QoS) in block A of the Faculty of Engineering of the Universidad Nacional de Chimborazo. Using policy and queuing models (FIFO, WFQ, and CBWFQ), the study detects problems in the network infrastructure linked to the absence of wireless coverage, scarcity of access points, and restricted bandwidth. It is essential to examine crucial factors such as jitter, latency, packet loss, and throughput through experimental and analytical techniques to understand their impact on network efficiency and user experiences.

This research employs tools such as GNS3 and Ostinato to replicate scenarios, create realistic traffic, and evaluate the performance of current configurations. The findings indicate that implementing QoS policies facilitates traffic prioritization, congestion reduction, and optimization of bandwidth allocation, favoring critical activities such as access to academic and administrative services. The findings provide concrete answers to improve network performance, including implementing CBWFQ-based configurations with QoS for effective traffic management.

Keywords: Quality of Service (QoS), policy and queuing model, jitter, latency, throughput, network simulation, CBWFQ, network optimization, traffic management.

Reviewed by:
Mgs. Jessica María Guaranga Lema
ENGLISH PROFESSOR
C.C. 0606012607

CAPÍTULO I

1. Introducción

En el mundo actual todas las acciones que realiza el ser humano están apoyadas en las redes de datos, en este entorno se utiliza ampliamente la expresión Calidad de Servicio (Quality of Service QoS), “no solo en el ámbito de las telecomunicaciones del cual procede, sino también en los servicios de banda ancha, inalámbricos y multimedia que usan IP” [1].

En el entorno de la Facultad de Ingeniería, el Bloque A se levanta como un núcleo de acciones académicas y administrativas, donde la efectividad de la conexión de red desempeña un papel importante. Es un ambiente cada vez más digitalizado, la calidad de servicio y la transmisión de datos se presentan como soporte fundamental para el desarrollo de las acciones diarias. Este estudio se profundiza en la evaluación de la red del Bloque A, empleando el modelo de políticas y colas como herramientas fundamentales para examinar su rendimiento, es por ello que la calidad de servicio es crucial, ya que puede generar fidelidad al superar expectativas a los usuarios [2], como benéficos nos permitirá manejar convenientemente los recursos de internet, realizando un uso más eficaz de los mismos, tener comprensión del para qué está siendo usada la red y así dar mejor servicio al tráfico más considerable [3].

Al emplear modelos determinísticos, buscamos no solo identificar posibles falencias, sino también comprender a fondo la dinámica de la red bajo diversas condiciones y cargas de trabajo. La importancia de esta investigación no radica solo en identificar los desafíos actuales, sino también en desarrollar soluciones específicas y adaptativas. La mejora continua de la calidad de los servicios de transmisión de datos no solo aumentará la eficiencia operativa del bloque A, sino que también contribuirá al desarrollo y éxito futuro de la Escuela de Ingeniería, mediante el estudio de la infraestructura de la red y el uso actual de los dispositivos digitales, este proyecto se ajusta a recomendaciones para mejorar la calidad de servicio suministrando el tráfico y afirmando una experiencia de beneficio ideal en todo momento.

1.1 Planteamiento del problema y justificación

La red de internet de la Facultad de Ingeniería enfrenta varios problemas, incluyendo falta de cobertura inalámbrica, escasos puntos de acceso para la cantidad de usuarios, y ancho de banda escaso tanto para conexiones cableadas como inalámbricas. Esto impide realizar actividades para estudiantes y docentes, el acceso limitado provoca discontinuidad y desconexiones, afectando la calidad del servicio.

Es determinante evaluar la calidad de servicio de la red de datos del bloque A, analizando la obstrucción con otras redes inalámbricas. Se deben considerar factores como el control de acceso, el tráfico de la red, aplicar modelos para comprender la relación entre la capacidad de la red, la demanda de servicio de los usuarios y el nivel de rendimiento. Esto asegurará una conexión eficiente y un ambiente de aprendizaje fluido para estudiantes y docentes [4].

La tasa de la red del Bloque A por medio del modelo de políticas y colas es sustancial para determinar posibles falencias en la infraestructura de red actual y proponer soluciones efectivas que mejoren su rendimiento. Es indispensable decidir si la distribución de ancho de banda, la priorización del tráfico y la gestión de colas están acorde con las necesidades de los usuarios y los requerimientos de las aplicaciones.

En la Facultad de Ingeniería, la calidad de servicio es crucial para las actividades de estudiantes, profesores y personal administrativo. Se ha investigado previamente la calidad de servicio en la distribución de puntos de acceso en laboratorios, aulas y dependencias administrativas [5]. Esta investigación se centra en identificar deficiencias en la infraestructura de red del Bloque A, utilizando un modelo de política y colas para un análisis cuantitativo preciso. La aplicación de este modelo se presenta como una inversión estratégica para mejorar la calidad de servicio y la transmisión de datos, beneficiando a la comunidad educativa [6].

1.2 Objetivos

1.2.1 Objetivo General

- Evaluar la calidad de servicio de la red del bloque A de la Facultad de Ingeniería, mediante el modelo de políticas y colas para determinar posibles falencias de la red y proponer una solución de mejora.

1.2.2 Objetivos Específicos

- Analizar la infraestructura de conexión por cable e inalámbrica del bloque A para determinar su situación actual.
- Estudiar el modelo a utilizar para la evaluación de la calidad de servicio y la transmisión en las redes de datos.
- Diseñar y simular la red de datos del bloque A para calcular los parámetros de QoS.
- Analizar y proponer alternativas de solución basándonos en los resultados estadísticos obtenidos en la simulación.

CAPÍTULO II

2. Fundamento Teórico

2.1 Estado el arte

Luego de indagar temas de investigación, encontré que la calidad de servicio (QoS) juega un papel crucial en las redes inalámbricas, por lo que a continuación se describe algunos de los resultados obtenidos en diferentes campos:

Los Sres. Carlos Erazo Prado, Juan Manuel Arana Mondragón, Iselin Meza Mejía y Sinhué Ezair Pérez Corella, en su proyecto investigativo: "Implantación de Calidad de Servicio (QoS) en redes inalámbricas wifi"[7], afirman que la tecnología en la actualidad es en demasiada, por lo que se recomienda la inserción de una calidad de servicio para usar totalmente los bienes que nos ofrece el internet, dando como resultado una mejoría en la administración y control.

El Ingeniero Diego Mauricio Llerena Delgado en su proyecto investigativo: "Algoritmos de Calidad de Servicio (QoS) y la congestión en los enlaces de comunicación de los usuarios de la empresa Uniplex Systems de la ciudad de Quito"[8], confirmaron que la solución a los problemas de tráfico de la red podría solucionarse añadiendo un sistema de distribución con políticas propias, lo que sin duda accedería a ajustar la topología para cubrir las modificaciones de tráfico que se encuentran en la red.

La Ingeniera Tatiana Paola Zambrano Valverde, en su proyecto investigativo: "Modelos de Configuración de Calidad de Servicio (QoS) en el tráfico de Voz y su impacto en el sistema de telefonía de la empresa Cemento Chimborazo C.A"[9], afirma que al implementar la Calidad de Servicio (QoS) en VoIP, se realizaron mejorías a través de pruebas internas y apoyadas por WRED&CBWFQ y el manejo de las propias tecnologías, como IP, RTP y LLQ, resultando mejoras entre diferentes departamentos y otros.

Laura Alejandra Torres Robayo, en su proyecto de investigación; "Aplicación De La Teoría De Colas En Una Central De Servicios Asistenciales Para Minimizar El Tiempo De Espera De Los Clientes En Línea"[10], El tiempo que debe esperar en la cola está continuamente relacionado con el crecimiento en el porcentaje de abandono llegando a influir así los grados de servicio y atención.

Zapata en la tesis titulada, "Evaluación De Parámetros De Calidad De Servicio (Qos) Para El Diseño De Una Red Vpn Con Mpls " [11], La investigación se realizó debido a la colectividad del diseño de redes orientadas al soporte de voz, video y datos. El objetivo de la tesis consistió en elaborar una red VPN/MPLS en el ambiente del laboratorio (Simulación) con la ayuda de la evaluación de parámetros de QoS para asegurar la disponibilidad de la red. La tecnología VPN MPLS permite a una empresa incorporar voz, video y datos en una plataforma con seguridad de calidad de servicio que es necesario

en la actualidad, ya que el tráfico de red es muy distinto y cada tipo de tráfico tiene diferentes peticiones como ancho de banda, jitter, delay y disponibilidad. Llegando a la conclusión: el mecanismo DiffServ permite distribuir el tráfico en clases, manejando la porción de tráfico que cada cliente envía a la red y prefiriendo el envío a través de políticas de clasificación corrigiendo la red.

Peña, Sanatana, Contreras en la tesis titulado "Diseño E Implementación De Una Red Mpls Para El Sistema De Comunicación De Editorial Océano Dominicana, En Santo Domingo Y Zona Metropolitana De Santiago" [12], la implementación del protocolo de comunicación MPLS tiene mejoría el rendimiento de la red de Editorial Océano Dominicana, ya que los paquetes son sustituidos con base a etiquetas evitando la lectura de las cabeceras IP, también facilita el reacomodo de mecanismos de balanceo de carga para librarse de la congestión con la Ingeniería de Tráfico y posibilidad de ofrecer servicios de VPN's a través de túneles virtuales quitando los inconvenientes de las VPN's tradicionales.

2.1.1 Calidad de Servicio

La calidad de servicio (QoS) de una red se determina por la capacidad de la red para equilibrar un nivel aceptable de rendimiento en términos de algunos parámetros, como la velocidad de transferencia de datos, latencia, la pérdida de paquetes y la disponibilidad.

Para lograr buena calidad de servicio, las redes suelen construir políticas de gestión de tráfico, de asignación de ancho de banda, de priorización de paquetes y otras herramientas que afirmen el desempeño para diversos tipos de tráfico. También es importante controlar y gestionar la red para encontrar y solucionar problemas que puedan afectar la QoS.
Sus dos aspectos esenciales son: clasificación y políticas de colas.

2.1.2 Funcionamiento

QoS emplea retardando paquetes sin importancia, o en los casos de tráfico extremo de la red eliminándole totalmente, así liberando espacios para que los paquetes importantes lleguen a su destino [13].

a) **Clasificación de tráfico**
   La clasificación en QoS se basa en principios de aplicación, en protocolos de transporte, en la prioridad de los datos y la sensibilidad al retardo, [14].
b) **Priorización**
   Al ser clasificado el tráfico se asignan niveles prioritarios a cada categoría de tráfico en función de los requisitos de calidad de servicio.
c) **Control de Congestión**
   La calidad de servicio evita la congestión de la red para asegurar un flujo de datos ligero con esto se puede incluir el uso de métodos que limite el acceso de flujo de

datos a la red cuando este al borde de la capacidad máxima que regule la transferencia de datos para evitar que se saturen los enlaces.

2.2 Elementos para deteriorar el QoS

2.2.1 Perdida de Paquetes

La pérdida ocurre cuando los paquetes que transmiten en una red IP, no llegan al destino y su motivo de la perdida de los paquetes se debe a la degradación de la señal al pasar por el medio, al congestionar la red los paquetes erróneos se rechazan durante la transmisión, falla el hardware de red como se muestra en la figura 1. La pérdida de paquetes se debe a problemas de la red, los paquetes perdidos causan problemas de rendimiento, fallas notables, la perdida de paquetes no necesariamente es malo como cuando es utilizada para equilibrar la latencia.
Se estima que la perdida de paquetes entre el 5% y el 10% del tráfico de datos llega a ser notorio, al estar la red congestionada libera el paquete para ello los protocolos de red como TCP tienen control de congestión conocido como inicio lento lo que impide que el rendimiento reenvié la información, para evitar las caídas de red no se reciben antes los paquetes perdidos.

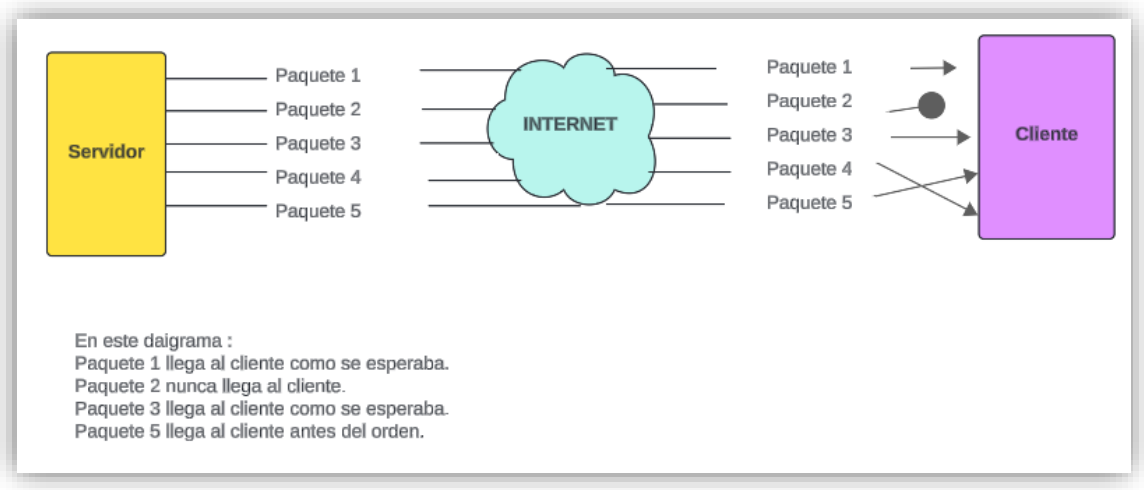


Figura 1. Pérdida de Paquetes
Fuente: [15]

2.2.2 Demora / Jitter

La demora del Jitter es definida como la modificación en el tiempo de llegada al punto de recepción que va afectando a los paquetes sucesivos, los paquetes llegan con espacios entre sí para garantizar una conversión a voz analógica. La medición del itter se completan en segundos y denotan distorsión en el modelo original de datos enviados como se muestra en la figura 2. El jitter tiene sentido al ser medido a un set de datos y no uno por uno.

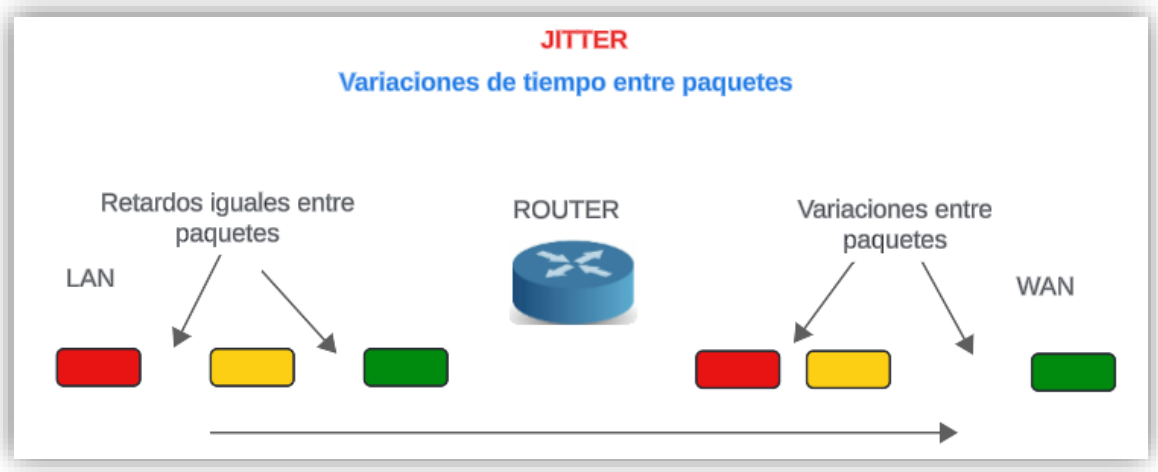


Figura 2: Jitter en redes Lan/ Wan
Fuente: [16]

2.2.3 Retraso o Latencia (Delay)

El retraso o latencia es el tiempo que transcurre cuando un paquete viaja hasta llegar a su destino; el retraso se da debido a varios factores como la separación física entre los dispositivos, la acumulación en la red, duración en el transcurso de los dispositivos de la red. La latencia afecta en aplicaciones sensibles al tiempo, como la transmisión de videos en tiempo real o juegos online; mientras menos sea la latencia, más efectiva es la respuesta de la red.

2.3 Mecanismos de Colas

2.3.1 Gestión de colas

El encolamiento de paquetes en el internet es el mecanismo de almacenar temporalmente los paquetes en una cola a través de un dispositivo de red, como puede ser en un enrutador o en un conmutador, antes de ser enviados al destino. Este proceso es esencial para el tráfico en la red para garantizar un flujo de datos ordenados y justos [17].
La causa de la congestión en interfaces es la distinción de velocidad existente entre ellas, como se lo representa en la figura 3.

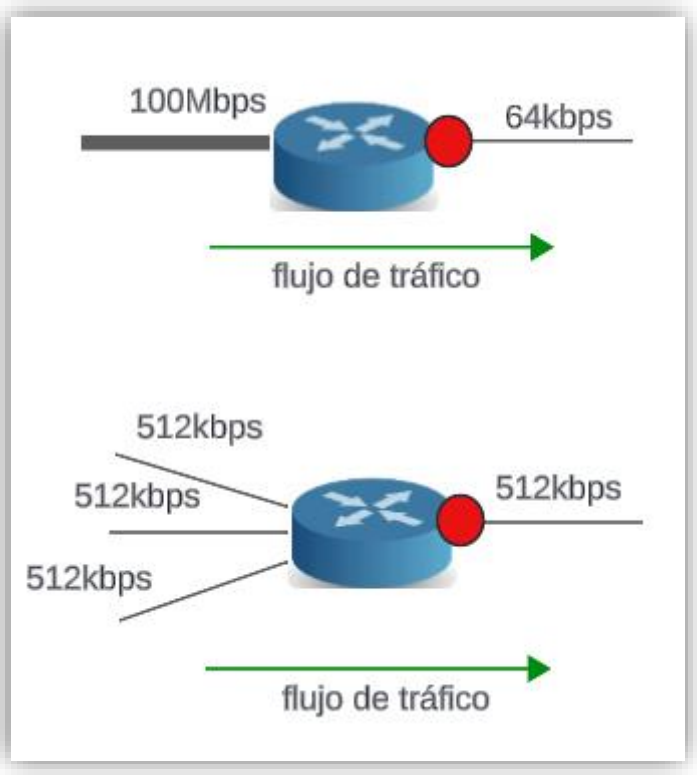


Figura 3: Gestión de colas
Fuente: [17]

Si la red MPLS y el cliente al no usar QoS (Calidad de Servicio) no tendrán problemas hasta que se origine aglomeración en la red. Al no producirse la aglomeración, actúa el encolamiento por hardware (FIFO), una sola cola. Si hay aglomeración, actúan los encolamientos por software para el uso de las colas, y lo primero que se afecta es la telefonía IP, seguido de la videoconferencia y los datos decisivos. Conforme a la aplicación que se esté utilizando, se debe determinar cuál encolamiento es más adecuado.

2.3.1.1 Política y Colas

El modelo de políticas y colas en una red es utilizado para manejar el tráfico de datos de modo eficiente y mejorar el rendimiento de la red. Este modelo conlleva aplicar políticas específicas para manejar y priorizar los paquetes de datos en las colas de enrutadores, conmutadores y otros dispositivos de red.

2.3.1.2 Notación de Kendall

La notación de Kendall es una abreviatura que utiliza símbolos para representar las particularidades características de una cola [18].

2.3.1.3 Modelos de Colas

a) **Modelo M/M/1:** El sistema de espera se determina porque los tiempos de llegada y los tiempos de servicio se reparten de manera exponencial con un único servidor o nodo [19]. Es importante saber que este modelo es simplificado y puede ser que no capture algunas complejidades del sistema.

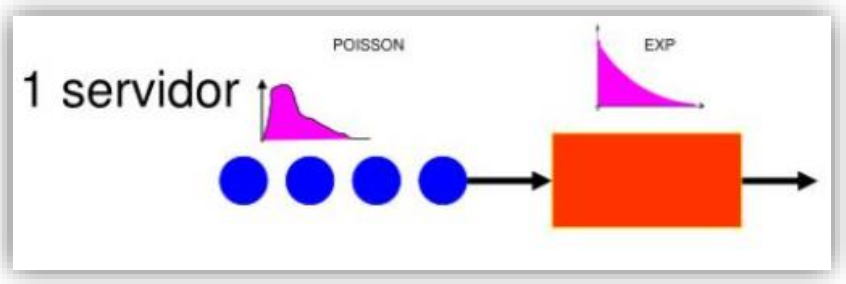


Figura 4: Modelo M/M/1
Fuente:[20]

b) **Modelo M/M/c:** Analiza los sistemas de colas con varios servidores y puede facilitar información valiosa sobre la efectividad del sistema y la obligación de recursos adicionales [21].

2.3.1.4 Métrica y análisis en la teoría de colas

Se utilizan distintas métricas y técnicas para calcular el rendimiento y la efectividad de los sistemas de colas, son sustanciales para comprender cómo se conlleva un sistema de colas y reconocer áreas de mejora [22].
Se describe algunas métricas y técnicas:

a) **Tasa de llegada (ʎ):** Es el número promedio que llegan los clientes por una unidad de tiempo.
b) **Tasa de servicio (μ):** Indica el número promedio de clientes que el servidor pueda considerar por unidad de tiempo [22].
c) **Factor de utilización (p):** Indica el tiempo que ha estado ocupando el servidor.
d) **Tiempo medio de espera en la cola (Wq):** Tiempo que un cliente espera en fila antes de que lo atiendan.
e) **Número medio de clientes en el sistema (L):** Es el número promedio de clientes en un sistema implicando a los que están en espera y a los que están siendo atendidos por el servidor.

2.3.2 Evaluación de la calidad de servicio de la red

La evaluación de la calidad de servicio de una red garantiza el rendimiento eficaz para los usuarios.

a) **Definir los parámetros de calidad de servicio (QoS)**: Se incluye la velocidad, latencia, pérdida de paquetes, etc. Es importante verificar qué aspectos son necesarios para la ejecución de la red y el requerimiento de los usuarios [23].
b) **Medición de parámetros**: Se utilizan resoluciones para medir los parámetros, como las herramientas para controlar la red, medir velocidad, latencia y pérdida de paquetes.
c) **Análisis de datos**: Una vez reunidos los datos, se va analizando e identificando posibles problemas en la red, se pueden comparar los resultados con mediciones anteriores [24].
d) **Identificación de problemas y áreas de mejora:** Con base en los análisis de los datos, identificar algún problema de desempeño o zonas donde la calidad de servicio
no cumple con las condiciones definidas, también podría incluir los cuellos de botella, congestión de red, etc.
e) **Implementación de soluciones**: Al identificar los problemas, se deben buscar soluciones para el mejoramiento del servicio; esto ayuda a la optimización de la red, actualización de los equipos, entre otros.
f) **Monitorización continua**: Es importante monitorear la red de forma graduada para afirmar que se mantenga un rendimiento eficaz y así poder detectar cualquier problema que pueda existir [25].

2.4.2.1 Requerimientos de calidad de servicio en una red E-MAN

Al caracterizar la calidad de servicios, se han tomado algunas iniciativas como IPMM (métricas de rendimiento de IP) [26], que define al conjunto de métricas que pueden ser utilizadas para caracterizar la calidad de servicio, el rendimiento de los ratos que son transmitidos a través de la red IP. Las métricas se definen como enlace, retardo y perdida de paquetes, reorganización de paquetes.

En la figura 5 se muestran los modos de los usuarios finales donde es impredecible crear políticas para la organización, etiquetado de paquetes y el control del ancho de banda de

tal manera que es necesario establecer un método de señalización y enrutamiento para la calidad de servicio

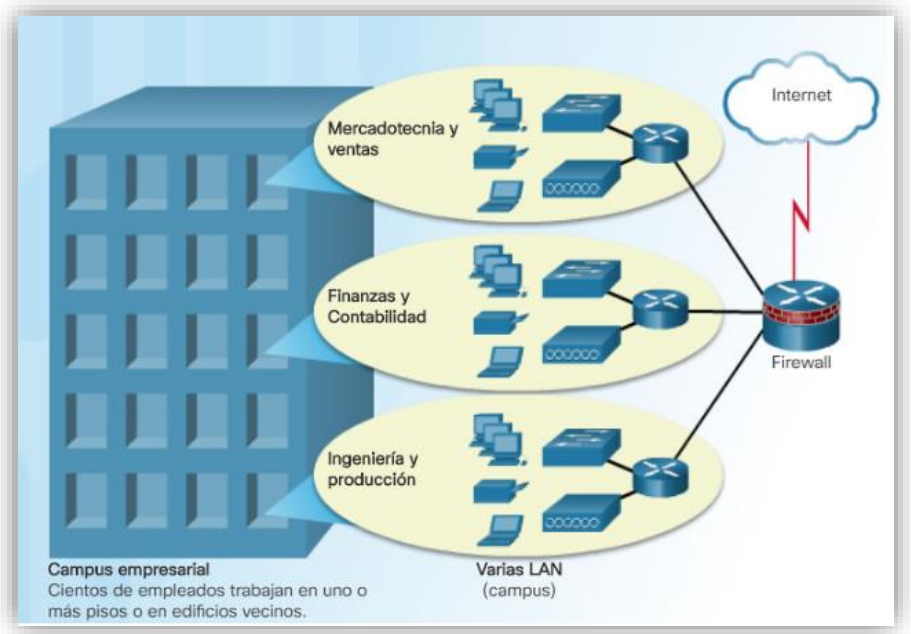


Figura 5: Conexión de una red de campus
Fuente:[27]

.

2.4.2.2 Métricas de calidad de servicio por obtener de extremo a extremo

Se califica en dos tipos: el QoS Relativa/Suave, que establece mecanismos conocidos de la IETF (Grupo de trabajo de ingeniería de Internet) para una edificación de servicios diferenciados; otro mecanismo es la IP DiffServ (Servicios Diferenciados) IEEE 802.1p con MPLS (cambio de etiquetas multiprotocolo), que son expuestos enérgicamente para definir políticas de QoS a través del ancho de la red de datos [28].

CAPÍTULO III

3. Metodología

3.1 Tipo de investigación

El tipo de investigación de este proyecto de titulación es de carácter descriptivo, ya que lo principal es estudiar la situación actual de la infraestructura de conexión en el bloque A. Se busca entender y documentar cómo está configurada y funcionando actualmente la red. La investigación implica el análisis de componentes específicos, como cables, dispositivos de red, puntos de acceso inalámbrico, switches, routers, entre otros.
Los datos se procesarán mediante estudios cuantitativos, se determina el grado de confiabilidad de la red en el tiempo mediante el diseño y simulación en un entorno de prueba y se determina cualitativamente el nivel y madurez de la información.

3.2 Método de investigación

3.2.1 Método Analítico

Se centra en el análisis detallado de los componentes clave que influyen en la calidad de la red. Ppara este método se identifican los parámetros clave que afectan la calidad de servicio, como latencia, ancho de banda, pérdida de paquetes, jitter.
Este enfoque analítico proporciona una base sólida para comprender, analizar y mejorar la calidad de servicio y la transmisión de datos en una red, utilizando políticas de colas para obtener una visión detallada de los factores clave que influyen en el rendimiento de la red.

3.2.2 Método Experimental

El método experimental en el contexto de calidad de servicio (QoS) y transmisión de datos implica la manipulación de variables específicas en un entorno controlado para observar y medir los efectos resultantes en el rendimiento de la red.
Este enfoque experimental brinda la oportunidad de realizar evaluaciones precisas y controladas de la calidad de servicio y la transmisión de datos, permitiendo la identificación de relaciones causa-efecto en un entorno controlado y la obtención de información valiosa para la mejora de la red.

3.3 Procedimiento y análisis

A continuación, se detallan las etapas para el análisis:

ETAPA 1: Se realizará un relevamiento preliminar de todos los trabajos relacionados con el tema y, utilizando asesoramiento técnico, trabajos de investigación y recursos bibliográficos, se seleccionará la información relevante para contribuir a la investigación.
ETAPA 2: Se analizará la infraestructura de conexión por cable e inalámbrica del bloque A y se determinará su situación actual.

ETAPA 3: Se estudiará el modelo a utilizar para evaluar la calidad de servicio (QoS) de la red de datos, lo que implica comprender las técnicas y políticas que se basan en el modelo para garantizar el rendimiento de la red.
ETAPA 4: Se diseñará y simulará la red de datos del bloque A con el objetivo de calcular los parámetros de calidad de servicio (QoS), implica utilizar herramientas de simulación para modelar el comportamiento de la red en diferentes escenarios.
ETAPA 5: La quinta etapa será la evaluación de los resultados con los cambios y mejoras respectivas.

En la Figura 6 muestra las etapas en las cual se desarrollará este proyecto.

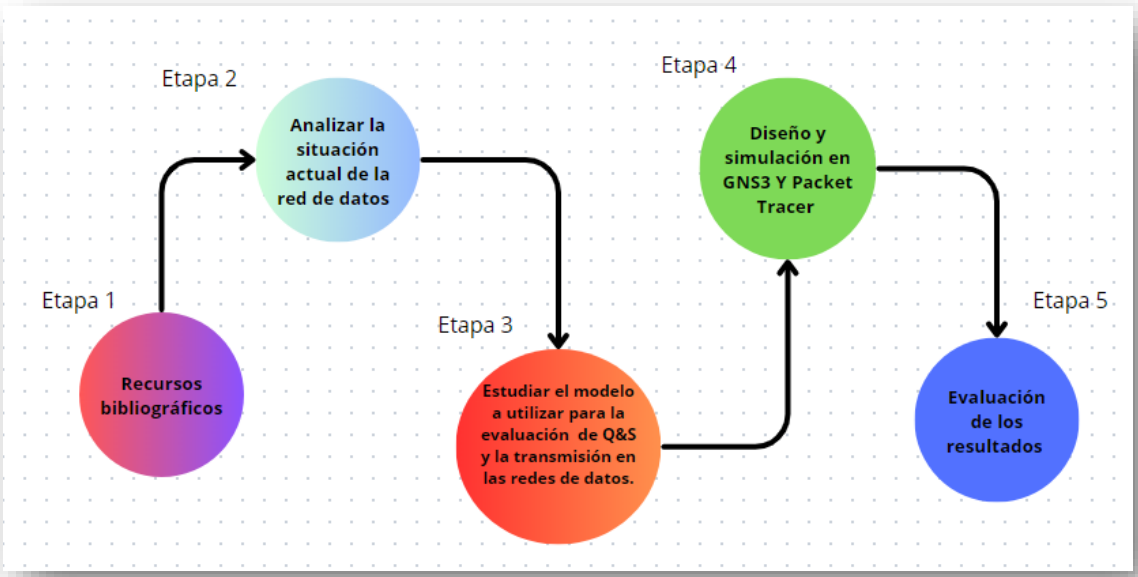


Figura 6: Proceso para el diseño de investigación
Fuente: Autor.

3.4 Población y muestra

3.4.1 Población

La población que se considera para el análisis y evaluación de la red de datos toma las variables de estudio en torno a la infraestructura de red. Se realiza un estudio cuantitativo que implica la cantidad de datos obtenidos sobre el escenario de pruebas con la finalidad de medir el nivel de la calidad de servicio en la que se encuentra.

3.4.2 Muestra

Se obtuvo la muestra del conjunto de datos definidos en la población mediante un proceso de selección aleatorio de datos sobre el escenario de pruebas de la red. El tamaño de

muestra que respalde validez se basa en consideraciones estadísticas para lograr un equilibrio entre la precisión y eficiencia de los resultados.
El tamaño de la muestra se extraerá de un subconjunto de datos de la población considerados de forma aleatoria, para medir la calidad de servicio en base al modelo de políticas y colas, y determinar las falencias y problemas que tiene la red actual.

3.5 Operación de variables

Analizar variables requiere conocer las variables independientes que producen los resultados y las variables dependientes que representan los valores que miden esos resultados.

Tabla 1. Operacionalización de variables

Variable	Descripción	Indicadores	Método e Instrumentos
	INDEPENDIENTE		
Evaluación de la calidad de servicio de la red del bloque A de la Facultad de Ingeniería	La red de dato permite la conexión alámbrica e inalámbrica entre los dispositivos y equipos de red mediante la aplicación de diferentes tipos de técnicas.	-Re direccionamiento de la red. -Configuración de los diferentes equipos para la comunicación. -Diseño de la red de comunicación (voz, datos, video).	Fortinet Packet Tracer GNS-3 MATLAB
	DEPENDIENTE		
Optimización de la red de datos	El rendimiento de la red representa los parámetros que se van a evaluar para posteriormente dar un punto de vista sobre su estado.	-Pérdida de Paquetes -Calidad de servicio QoS.	Utilizar herramientas de monitoreo de red para medir retrasos en la transmisión de datos y registrar tiempos promedio , aplicaciones para medir el tráfico de una red inalámbrica.

Fuente: Autor.

3.6 Métodos de análisis, y procesamiento de datos

Para estudio e identificación de los dispositivos de la topología de red, utiliza herramientas de simulación GNS3, Packet Tracer para descubrir, escanear vulnerabilidades, captura y análisis de tráfico, simulación de eventos en base a los modelos de QoS, evaluando la configuración y proporcionando información valiosa para fortalecer la infraestructura.

3.7 Estado actual de la red

Mediante una entrevista con el analista de DTIC se obtiene información para el análisis de la red inalámbrica de Facultad de Ingeniería que se detalla a continuación.

Tabla 2. Información Facilitada por DTIC.

Información proporcionada por DTIC	
Switch de Core	Catalyst 6500
Switch de Distribución	Catalyst 3750x
Puntos de Acceso	Juniper
Nombre de red	Estudiantes Unach en Movimiento.
Almacenamiento de Información de Usuarios	Base de Datos SICOA.
Servidor de Autenticación	Servidor Radius.
Autenticación y Autorización	802.1x para intercambio de mensajes entre el Servidor Radius y el dispositivo de red mediante el protocolo PEAP.
Encriptación de Datos	WPA2 Enterprise.
Clase de Dirección IP	Clase B
Asignación de Claves	DHCP en el switch de core
Gestión de Claves	Usuario: usuario SICOA Contraseña: número de C.I.
Firewalls	Filtros de Contenido Adulto
Monitoreo y Registro	Realiza a diario para detectar y prevenir posibles amenazas de dispositivos no autorizados.
Segmentación de Red	VLANs para cada tipo de privilegios • Estudiantes VLAN 56 con mascara de red /21. • Unach en movimiento VLAN 96 con mascara de red /20.
Control de Acceso	Un dispositivo por estudiante

Fuente: Autor

3.8 Levantamiento de Información

Con la información reunida se comienza a elaborar la topología de red, como se muestra en la Figura 7, con la información de la cantidad de PCs por aula, puntos de acceso y localización de ellos en cada piso del edificio del bloque A de la Facultad de Ingeniería.

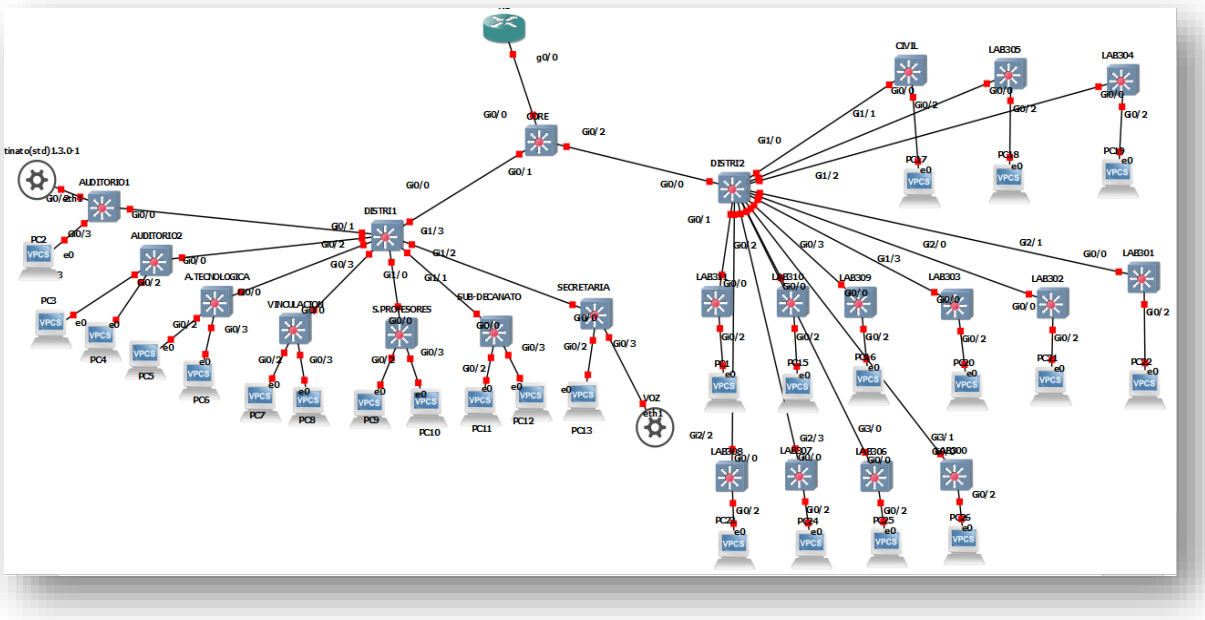


Figura 7: Topología de Red del bloque A de la Facultad Ingeniería
Fuente: Autor

En la Tabla 3 se especifican los dispositivos que forman parte de la red LAN.

Tabla 3.Detalle de dispositivos de la red Lan

Equipo	Modelo	Cantidad
Switch Core	Catalyst 6500	1
Switch de Distribución	Catalyst 3750X	2
Puntos de acceso	AP JUNIPER A32 AP JUNIPER A63	22

Fuente: Autor

3.8.1 Bloque A

En la Tabla 4 muestra el número de puntos de acceso por cada planta del Bloque A de la Facultad de Ingeniería.

Tabla 4. Número de Puntos de Acceso del Bloque A.

Número de Plantas	Puntos de Acceso
Planta Baja	2
Primera Planta	5
Planta Alta	2
Total	9

Fuente: Autor

En la Tabla 5 muestra la distribución por aula de PC, puntos de red y puntos de acceso en la planta baja del Bloque A de la Facultad de Ingeniería.

Tabla 5. Distribución de la red en la Planta Baja-Bloque A

Nombre	PC	PR	AP
Lab A100	1	1	
A 110	1	1	
A 109	1	1	
A 108	1	1	
A 107	1	1	
A 106	1	1	
A 105	1	1	
A 104	1	1	
A 103	1	1	
A 102	1	1	
A 101	1	1	
PASILLO I			1
PASILLO II			1

Fuente: Autor

La Figura 8 nos muestra el plano de cómo están asignados e instalados los puntos de acceso (AP), puntos de red (PR) y computadoras (PC) en cada aula de la planta baja del Bloque A de la Facultad de Ingeniería. Esta información es importante para comprender la infraestructura de la red.

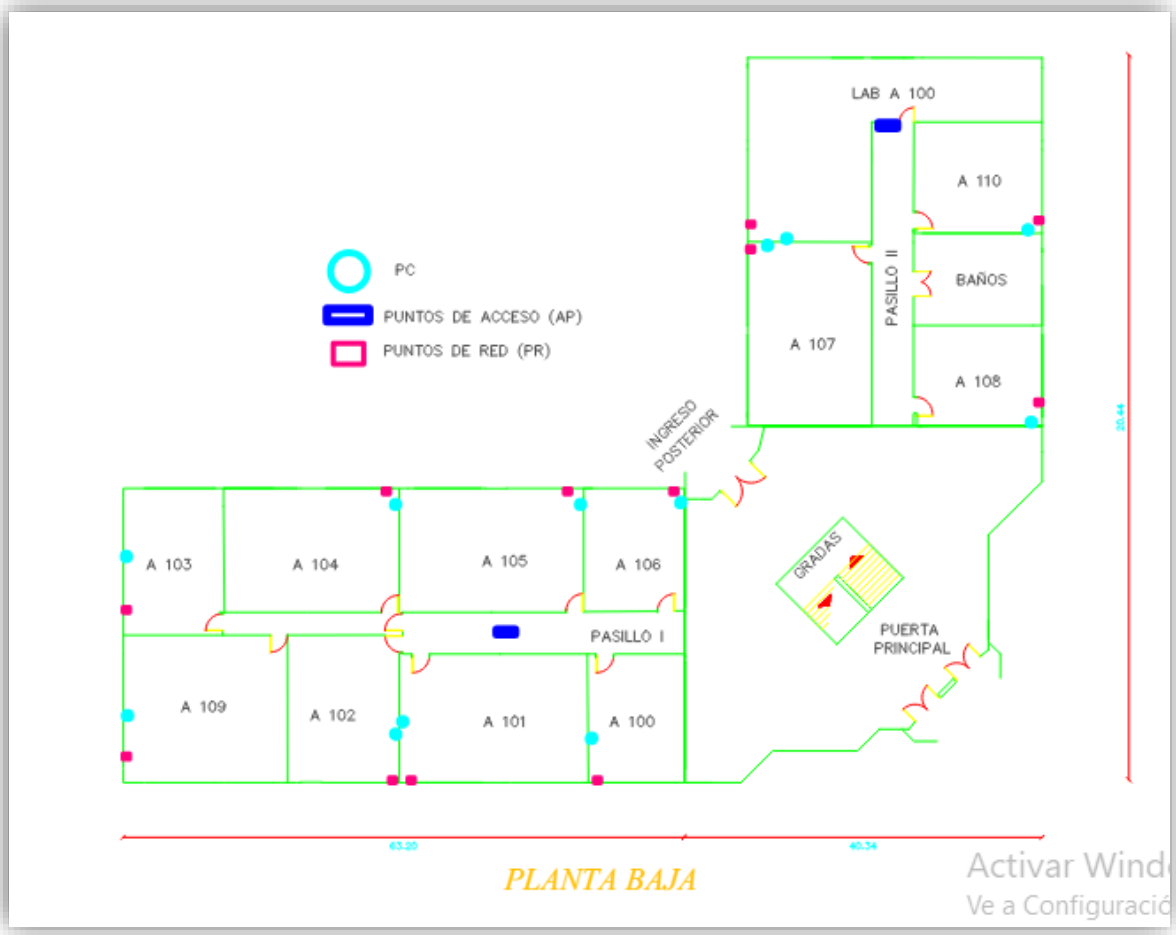


Figura 8: Planta Baja del Bloque A-Facultad de Ingeniería
Fuente: Autor

En la Tabla 6 muestra la distribución por aula de PC, puntos de red y puntos de acceso en la primera planta del Bloque A de la Facultad de Ingeniería.

Tabla 6.Distribución de la red en la Primera Planta-Bloque A

Nombre	PC	PR	AP	Teléfono
Auditorio I	1	1	1	
Auditorio II	1	1	1	
A 200	1	1		
A 201	1	1		
Área de Tecnología	9	9		
Vinculación	7	7		
Sala de Docentes	14	14		

Subdecanato	2	2		2
Decanato	3	3		2
Secretaria Académica	14	14		14
PASILLO I			2	
Gradas		1	1	

Fuente: Autor

La Figura 9 muestra el plano de cómo está ubicada e instalada la red de la Primera Planta del Bloque A de la Facultad de Ingeniería.

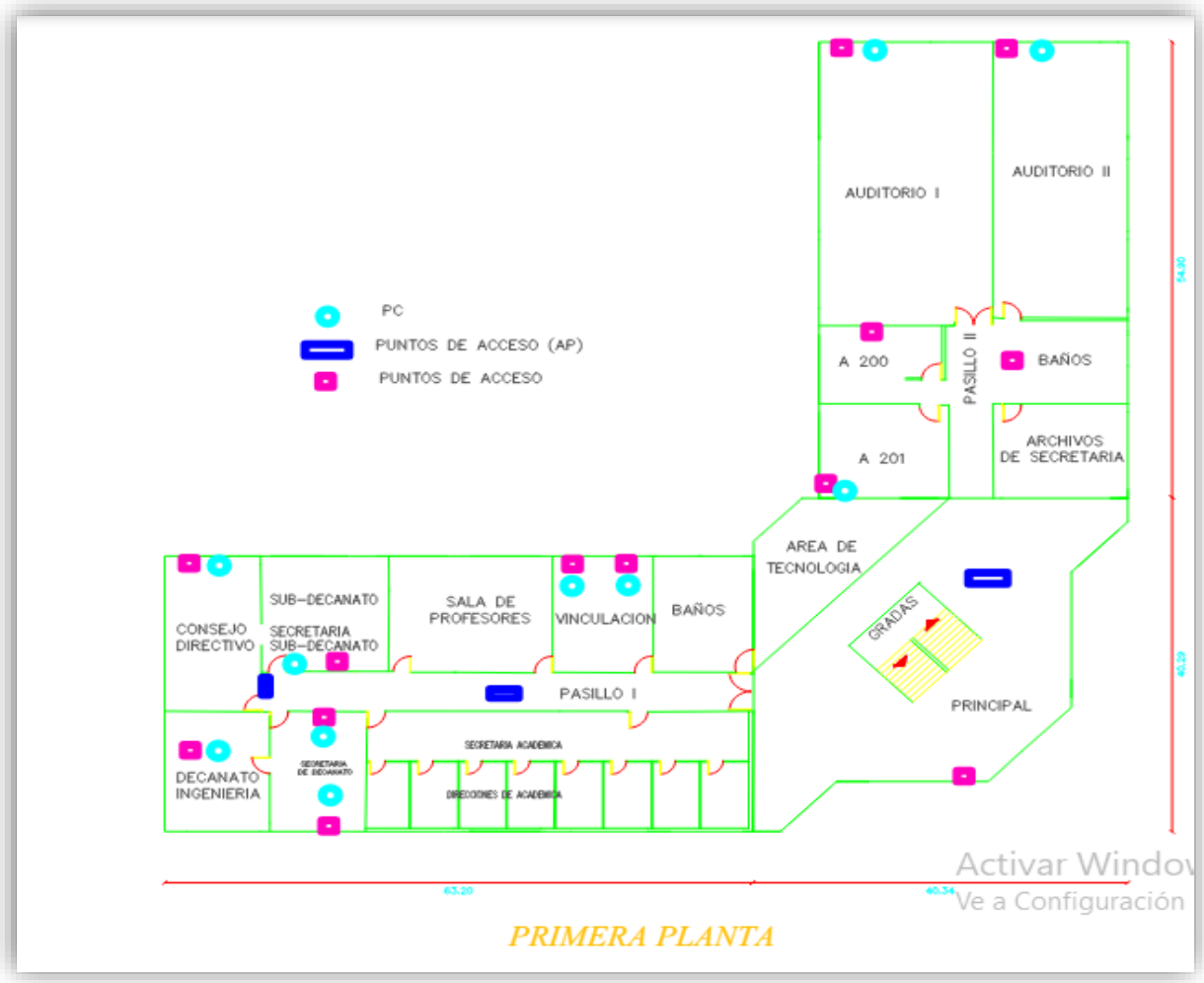


Figura 9: Plano de la Primera Plata del Bloque A-Facultad de Ingeniería
Fuente: Autor

En la Tabla 7 muestra la distribución por aula de PC, puntos de red y puntos de acceso de la planta alta del Bloque A de la Facultad de Ingeniería.

Tabla 7.Distribución de la red en la Planta Alta-Bloque A

Nombre	PC	PR	AP
Lab A 311	10	10	
Lab A 310	20	20	
Lab A 309	40	40	
Lab A 308	2	2	
Lab A 307	21	21	
Lab A 306	3	3	
Ingeniería Civil	3	5	
Lab A 305	10	1	
Lab A 304	21	21	
Lab A 303	20	20	
Lab A 302	1	1	
Lab A 301	3	1	
Lab A 300	23	23	
Pasillo I		2	1
Pasillo II		1	1

Fuente: Autor

En la Figura 10 se muestra el plano y como están la localizados los puntos de acceso de la planta alta de Bloque A de la Facultad de Ingeniería.

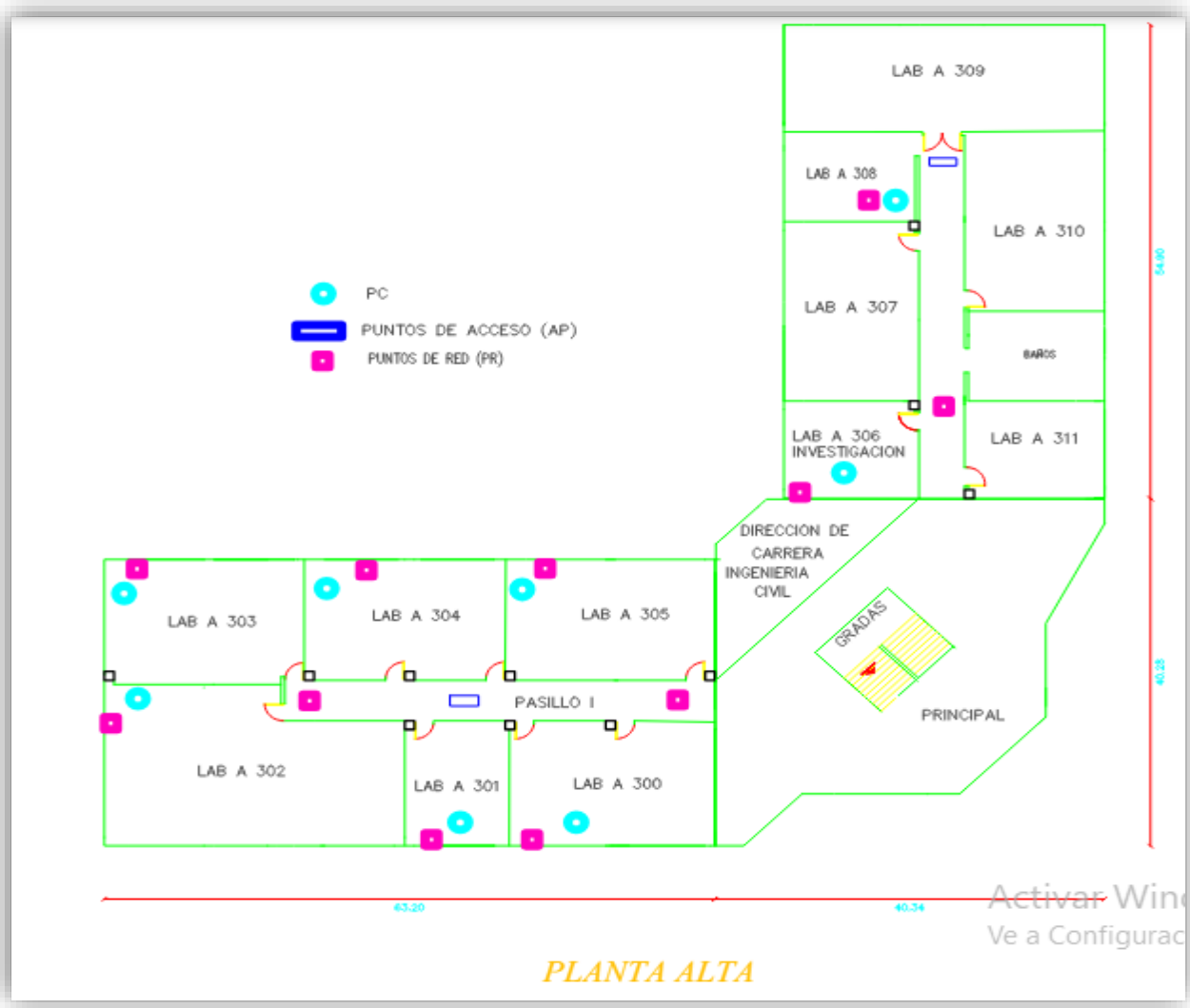


Figura 10: Plano de la Plata Alta del Bloque A-Facultad de Ingeniería
Fuente: Autor

3.9 Modelos de políticas y colas QoS

Los modelos de políticas y colas QoS (Calidad de Servicio) son fundamentales en la gestión de redes para confirmar el rendimiento efectivo a continuación, se explicará dos modelos esenciales.

3.9.1 FIFO (Primero en entrar y primero en salir)

Se utiliza principalmente en la misión de colas y paquetes que aguardan ser transmitidos o procesados en un router o switch; no tiene prioridad ni clase de tráfico, ya que existe una sola cola y así todos los paquetes se transmiten por igual. Los paquetes se envían a la salida en el orden en que llegaron, como se muestra en la figura 11.

Figura 11: Encolamiento FIFO
Fuete:[29]

3.9.2 WFQ (Mecanismo de Cola Equitativo Ponderado)

Da prioridad a cierto tipo de tráfico utilizando varios factores; para ello lo clasifica en conversaciones o flujo. El enrutador va determinando cuáles son sensibles al retardo, dando prioridad al flujo más alto, que es puesto al final de la cola, y los flujos más bajos sensibles al retardo son puestos al principio de la cola. En la figura 12 se muestra el encolamiento WFQ.

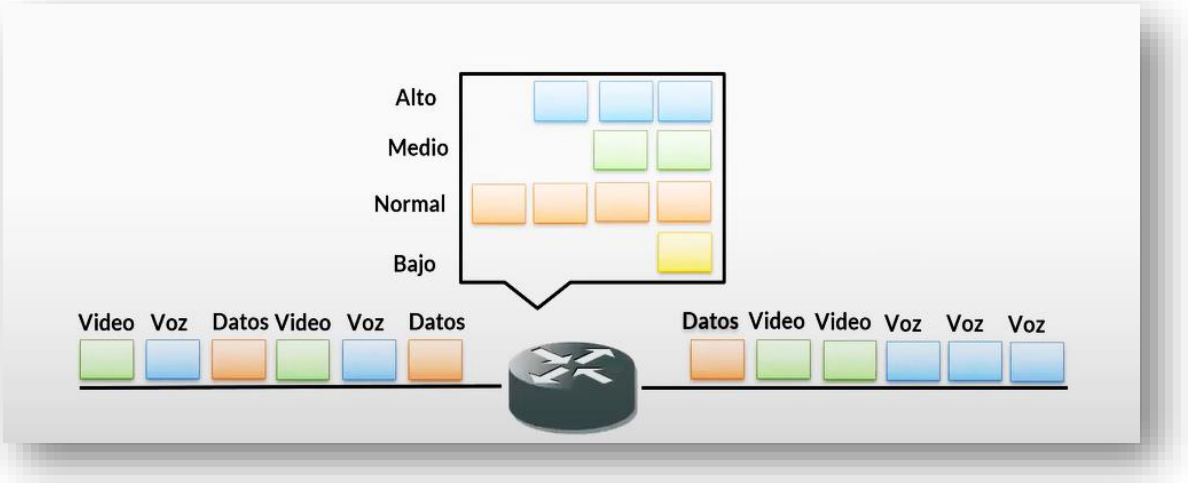


Figura 12: Encolamiento WFQ
Fuente: [29]

Al clasificar cada paquete y ponerlo en la cola, el servidor va calculando y colocando un tiempo de fin a cada paquete, cuando el servidor WFQ suministra sus colas, selecciona el paquete con el tiempo de finalización menor como el siguiente paquete a transmitir por el puerto de salida [30].

3.9.2.1 Características

- WFQ utiliza clasificación automática.

- Disminuye el ancho de banda muy considerable entre las conversaciones o los flujos.
- Las conversaciones o flujos con mayor peso adquieren mayor ancho de banda
- Se puede ajustar a diferentes tipos de tráfico, garantizando un adecuado rendimiento.
- Usa un número establecido de colas [31].

3.9.3 CBWFQ (Mecanismo de Cola Equitativo Ponderado basado en Clases)

Este mecanismo está basado en clases, fue desarrollado para evitar restricciones y desplegar la funcionalidad del algoritmo WFQ, permitiendo la agregación de clases dadas por el usuario, dando así un control al tráfico y ancho de banda. Se definen las clases de los tráficos basándose en emparejamiento, incluyendo protocolos, listas de control de accesos y protocolos de entrada. Al ser definida la clase, se pueden asignar características a la clase, límite de paquetes máximos, como se muestra en la figura 13[32].

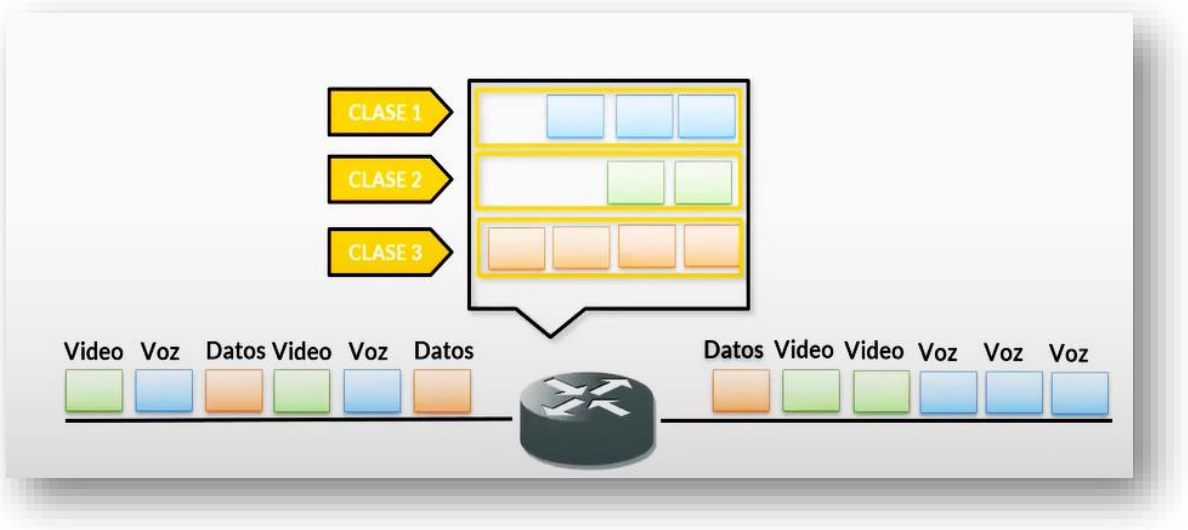


Figura 13: Encolamiento CBWFQ
Fuente:[29]

3.9.3.1 Características

- El tráfico es ordenado en diferentes clases basadas en algunos aspectos como tipo de aplicación, dirección IP, etc.
- Las clases se definen por el peso que determina el ancho de banda estipulado.
- La distribución es muy equitativa del ancho de banda entre distintas clases de tráfico.

3.9.4 WRED (Detección temprana aleatoria ponderada)

Utilizado para salvar la congestión en la red y evitar la pérdida de paquetes en los dispositivos, se basa en red, pero aplica políticas de descarte acordes al tipo de flujo [33]. Una de sus características esenciales es evitar la congestión, ya que en vez de esperar que la cola se encuentre llena y descartar paquetes numerosos (lo que puede causar la caída del rendimiento), por tal razón WRED ejecuta antes reduciendo la congestión.

3.10 Generador de Trafico

Ostinato es el generador de tráfico empleado para generar flujos de paquetes, ya que puede manejar diferentes tipos de flujos de tráfico como (TCP, UDP, ICMP).

Figura 14: Generador de Tráfico
Fuente: [34]

CAPÍTULO IV

4. Resultados y discusión

4.1 Escenario de pruebas

El escenario de pruebas de la figura 15 utiliza dispositivos físicos como también máquinas virtuales utilizando el software de Virtual Box, ofreciendo un medio controlado que incluye routers, base de datos, firewall. Por otro lado, los dispositivos físicos como los puntos de acceso y dispositivos de usuarios son parte del ambiente real. Con esto se lleva a cabo la simulación de algunos elementos y configuraciones del diseño de red.

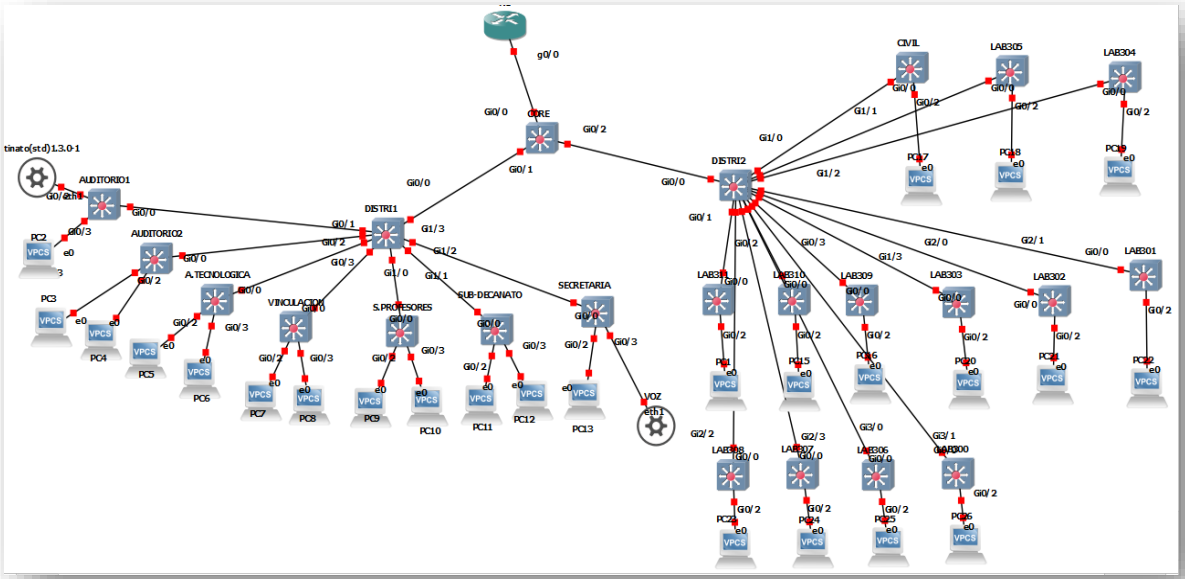


Figura 15: Topología del escenario
Fuente: Autor

La configuración de los dispositivos virtuales simplifica la evaluación de la calidad de servicio implementada en el entorno de la red, como se muestra en la figura 16.

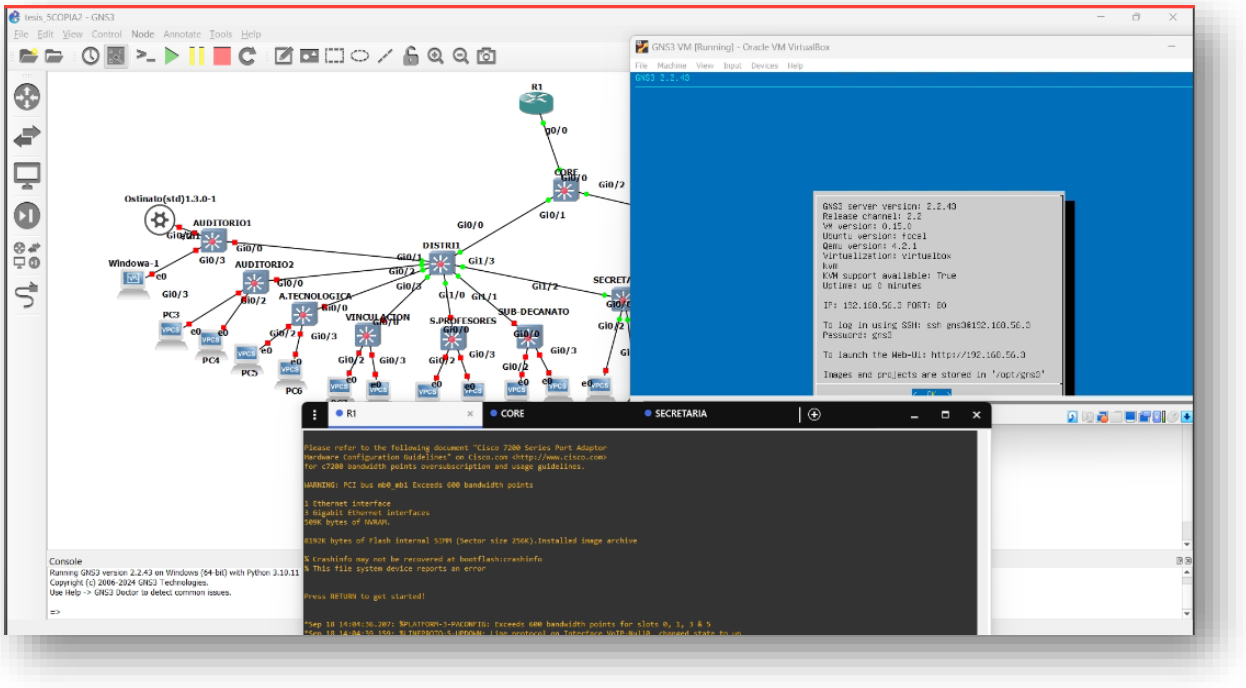


Figura 16: Acceso a los routers, máquinas virtuales, servidores
Fuente: Autor

En la tabla 8 muestra el direccionamiento IP del escenario de pruebas.

Tabla 8. Tabla de Direccionamiento IP

Red	Direccionamiento IP
Router	DHCP de proveedor de servicio de (Internet)
Vlan Inalámbrica de Estudiantes (Vlan 10)	172.16.0.0/19
Vlan Inalámbrica de Docentes (Vlan 20)	172.16.30.0/21
Vlan de Aulas (Vlan 30)	172.16.40.0/24
Vlan de teléfonos (Vlan 40)	172.16.41.0/25
Vlan de secretarias y Administrativos (Vlan 50)	172.16.41.128/26

Fuente: Autor

4.2 Hardware y Software del escenario de pruebas

Para la puesta de funcionamiento del escenario virtual se implementó con el siguiente hardware y software como se muestra en la tabla 9 y 10.

Tabla 9. Hardware del escenario de red

Nombre	Especificación	Descripción
1 laptop	ASUS TUF CAMING A5	Computadora personal para la implementación
Router	VM / 1GB RAM	Router Principal
Puntos de Acceso	TP-LINK TL-WR840N	Puntos de Acceso

Fuente: Autor

Tabla 10. Sofware del escenario de red

Nombre	Descripción
S.O Windows	Sistema Operativo utilizado por el equipo del usuario Laptop.
GNS3	Sistema Operativo utilizado para realizar la topología a estudiar.
Packet tracer	Sistema Operativo utilizado para diseño de la red
VirtualBox	S.O. utilizado para crear entornos de red más completos y a su vez incluir máquinas virtuales.
Ostinato	S.O. utilizado para la generación de tráfico hacia la red en tiempo real.
Wireshark	S.O. utilizado para capturar el tráfico de los paquetes.

Fuente: Autor

4.3 Procedimiento de evaluación de la calidad de servicio QoS

Para evaluar la calidad de servicio se realiza una serie de procedimientos que se detallan a continuación.

- Análisis de la red del bloque A de la facultad de Ingeniería para identificar puntos de acceso y dispositivos de usuarios: En el escenario de pruebas, mediante el uso de la herramienta GNS3, se realiza un escaneo para identificar los SSID de los puntos de acceso y los dispositivos que están conectados a cada uno de ellos.
- Identificar los dispositivos inalámbricos: Con la herramienta GNS3 se realiza un escaneo para identificar los dispositivos que están conectados a los puntos de acceso.
- Pruebas para evaluar la calidad de servicio QoS de la red: Se utilizan las herramientas de simulación Ostinato y Wireshark para analizar el tráfico cursado por la red.
- Evaluación de los modelos de QoS: Realizamos las simulaciones de los 3 modelos de QoS con las herramientas de simulación Ostinato y Wireshark.

- Generación de reporte del mejor modelo de QoS: Se realizan tablas de acuerdo a los criterios de evaluación para determinar el modelo de QoS que mejor se adapte a la red de la Facultad de Ingeniería UNACH.

4.4 Configuración

4.4.1 Configuración del Router (R1)

La figura 17 muestra la configuración del router con direcciones DHCP para diferentes segmentos de la red, configurando la dirección de red, el gateway y el servidor DNS tanto para las VLAN de docentes, estudiantes, aulas, teléfonos y secretarias mostrados en la figura 17.

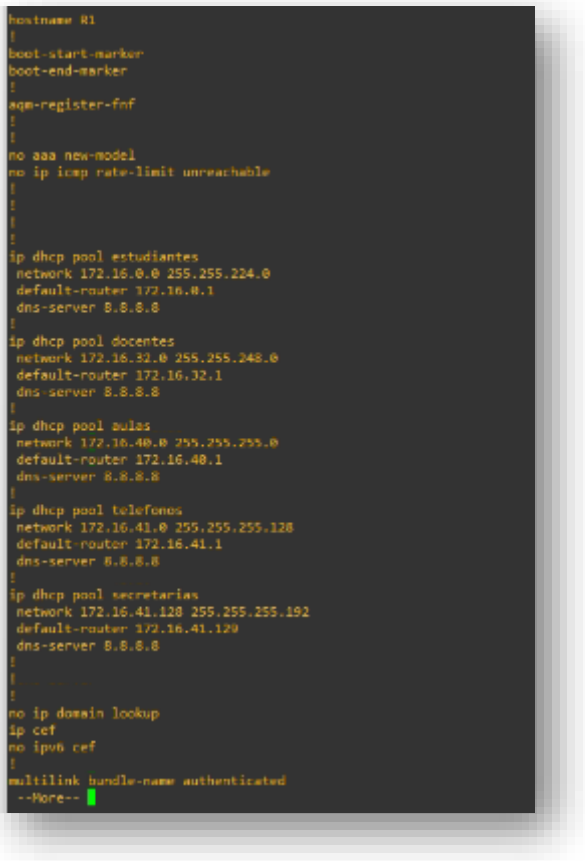
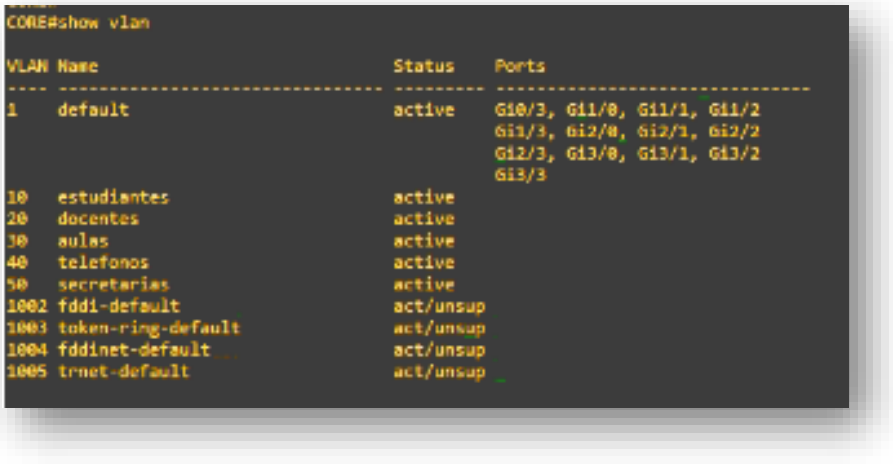


Figura 17: Configuración del router (R1)
Fuente: Autor

4.4.2 Configuración de Switch Core

La figura 18 muestra la configuración en la que se han creado varias VLAN para dividir la red por distintos departamentos, como son estudiantes, docentes, aulas, teléfonos,

secretarias, lo que permite dividir el tráfico de la red efectivamente y mejorar el rendimiento, y se encuentran asignadas a diferentes puertos del switch.



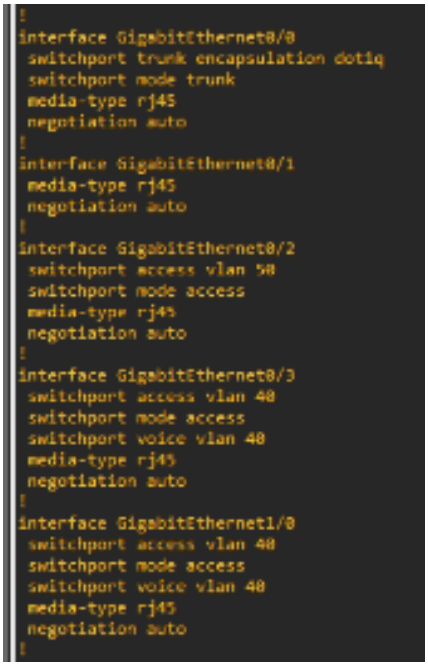
```
CORE#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
10   estudiantes                      active
20   docentes                         active
30   aulas                            active
40   telefonos                        active
50   secretarias                      active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 18: Configuración del Switch CORE
Fuente: Autor

4.4.3 Configuración de Switch de Distribución

La figura 19 muestra la configuración de la troncalización y acceso al puerto de la interfaz G0/0. Este puerto está distribuido como troncal y así varias VLAN lo usan y los demás puertos están configurados para acceso y redistribuidos a las VLAN específicas.
Esta configuración es clásica en donde se requiera segmentar la red para distintos tipos de dispositivos o usuarios y así permitir que las interfaces manejen tráfico de VLANs.



```
!
interface GigabitEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 switchport access vlan 50
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 40
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/0
 switchport access vlan 40
 switchport mode access
 switchport voice vlan 40
 media-type rj45
 negotiation auto
!
```

Figura 19: Configuración del Switch de Distribución
Fuente: Autor

4.4.4 Configuración de Software Ostinato

En los flujos generados se configuran algunos parámetros como las direcciones IP, tanto de origen como de destino, las direcciones MAC, tanto de origen como de destino, valores de los flujos y el contenido de los paquetes, ya sea TCP o UDP.
Los puertos son seleccionados por el que se quiera transmitir flujos, como se muestra en la figura 20.
Este software, a su vez, permite recibir los paquetes creados desde otro Ostinato y ser mostrados en GNS3 con el programa Wireshark la información de los paquetes recibidos.

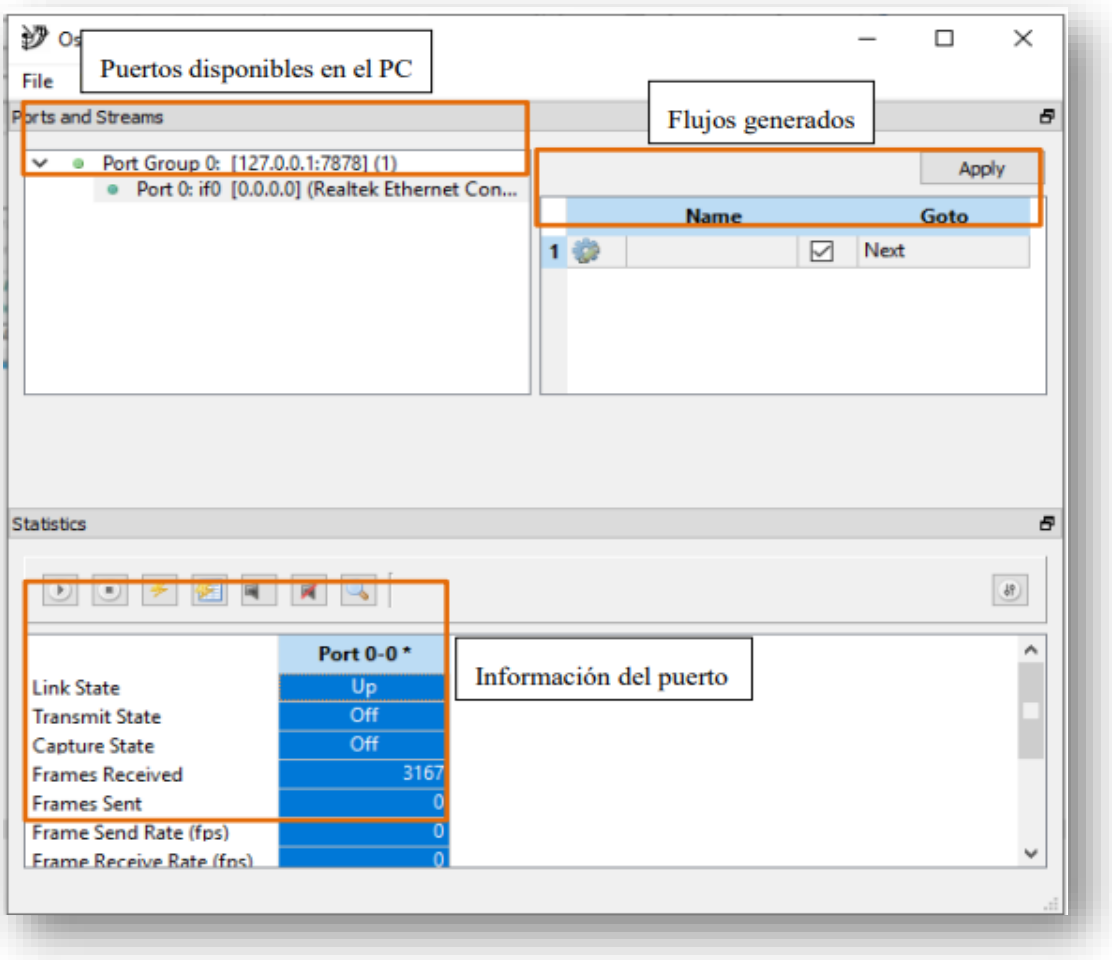


Figura 20: Ventana principal del software ostinato
Fuente: [35]

En la figura 21 se configuran los protocolos que van a componer los paquetes del flujo elegido como (ICMP, IGMP, TCP, UDP, MLD), como también se puede configurar el tamaño de los paquetes para que sea de valor fijo, como también vayan aumentando de un tamaño mínimo a un máximo o disminuyendo de un tamaño máximo a un mínimo. En este caso, configure cada PC de forma que el PC33 envíe tráfico TCP sobre IPv4. De igual manera, se configuró el tamaño de los paquetes para que sea aleatorio entre el mínimo y máximo que sujeta cada protocolo para simular tráfico real.

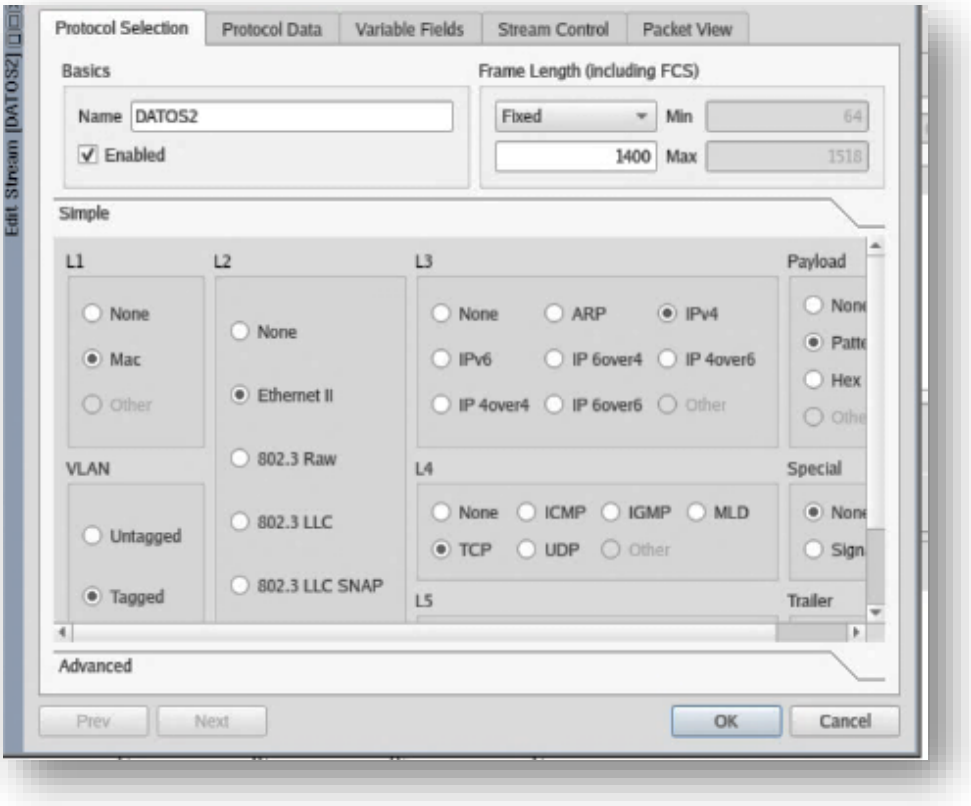


Figura 21: Selección de protocolo y tamaño de los paquetes
Fuente: Autor

En la figura 22 se configuran tanto los parámetros de las cabeceras de los protocolos como también el contenido de los paquetes.
Las direcciones MAC de origen y destino de los paquetes pueden ser tanto fijas como crecientes o decrecientes. En este caso se configuraron las direcciones MAC de cada PC para que generen tráfico y que sean las mismas que las del PC; para la dirección MAC destino se utilizó la dirección MAC del puerto G0/0 del router (R1).

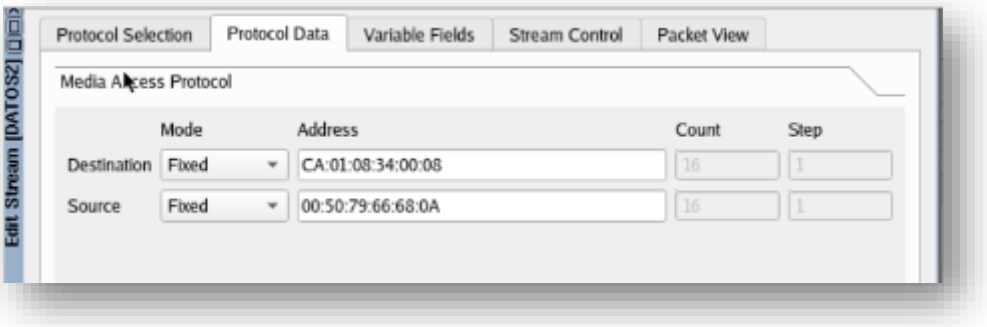


Figura 22: Configuración del protocolo y direcciones MAC
Fuente: Autor

La figura 23 muestra al seleccionar el puerto y crear los streams configurados con sus respectivas MAC de origen, destino y los paquetes, tanto TCP como UDP. En Transmit le ponemos Iniciar para que se ejecute el software con lo solicitado.

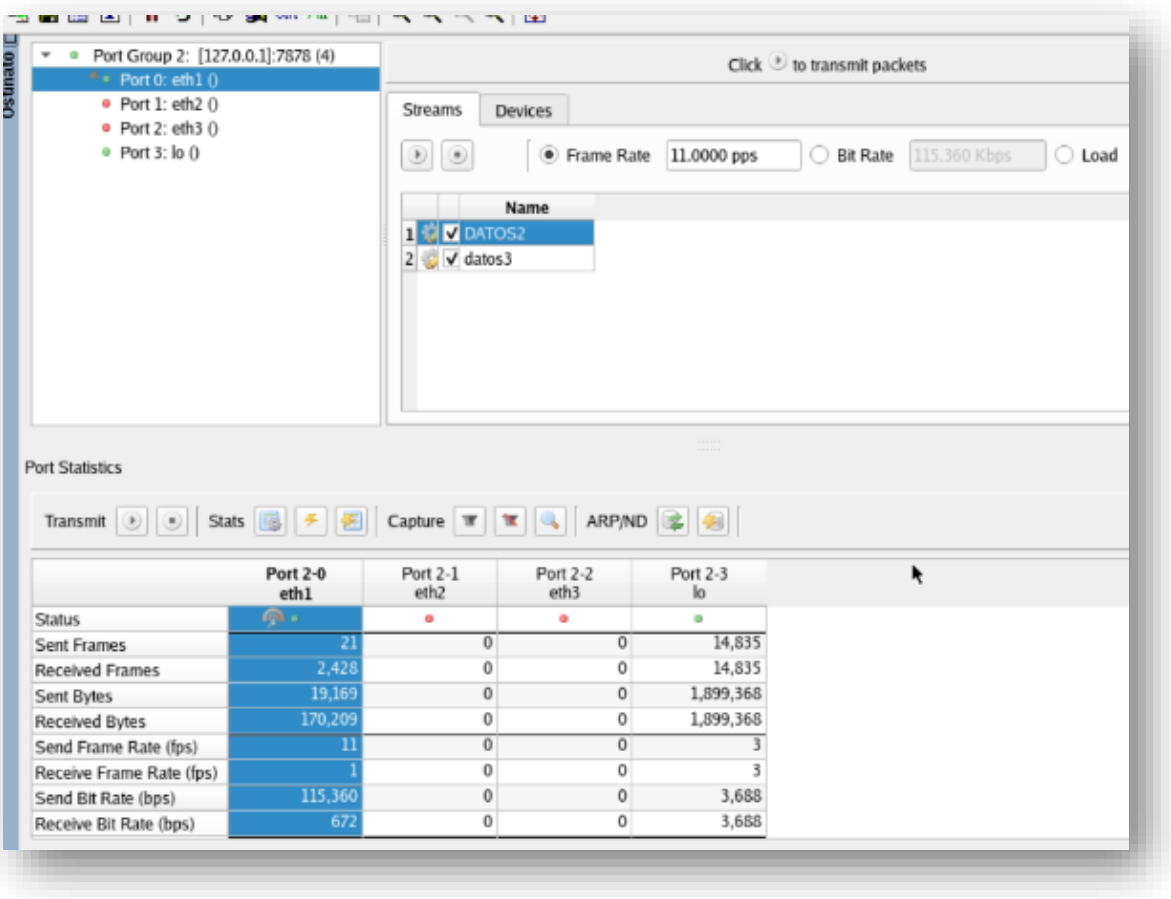


Figura 23: Selección del puerto para correr el software ostinato
Fuente: Autor

La figura 24 muestra que han llegado paquetes TCP y UDP y a su vez se puede observar que el tamaño de los paquetes va variando, por lo tanto, su simulación mejora el tráfico real que va por la red.

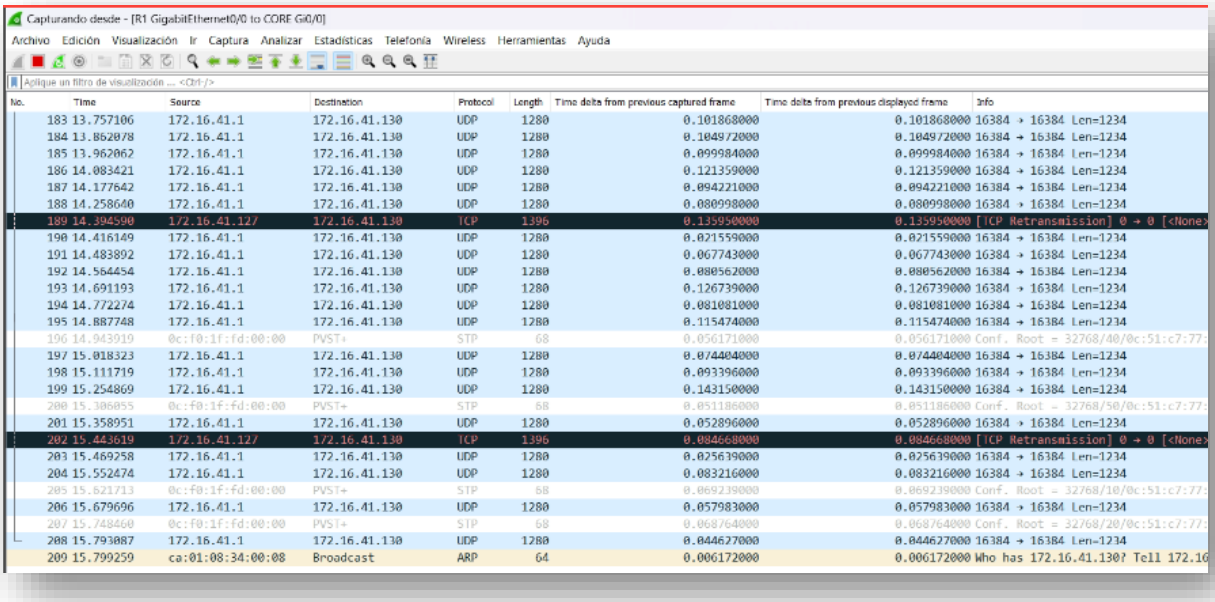


Figura 24: Paquetes generados y recibidos en Wireshark
Fuente: Autor

4.5 Cálculo de Jitter

Jitter se encarga de la medición del tiempo de llegada de los paquetes.
Se usan los valores del Time delta from previous captured frame, ya que estos valores muestran el tiempo entre la llegada de los paquetes consecutivos y para calcular el jitter realizamos la diferencia entre los valores, como se muestra en la figura 25.

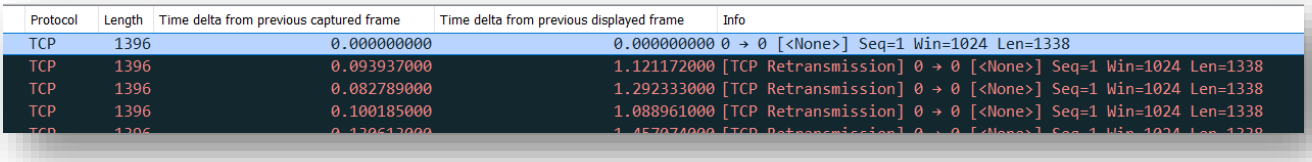


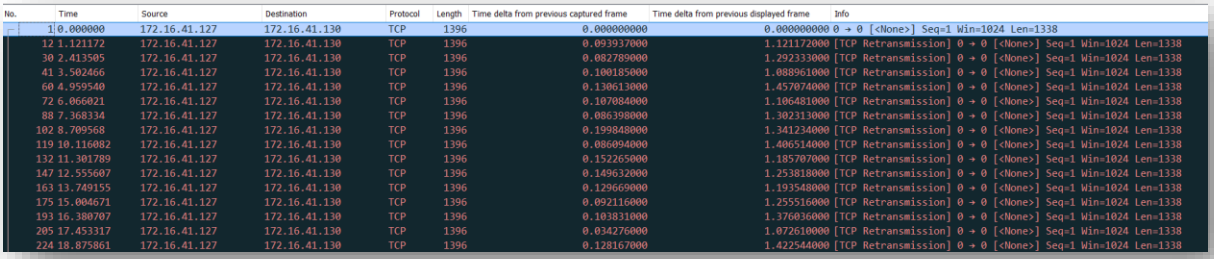
Figura 25: Valores a tomar para el cálculo del Jitter
Fuente: Autor

4.6 Configuración sin calidad de servicio (QoS)

4.6.1 FIFO

En la cola FIFO, los paquetes son analizados en el orden de llegada; el primero en llegar es el primero en ser analizado, ya que no prioriza el tráfico. El tráfico se gestionará de

dos maneras: TCP a la red y UDP para visualizar cómo afecta el tráfico no bueno en la configuración. En la figura 26 nos muestra la captura del tráfico TCP sin calidad de servicio, observando los tiempos que van variando para posteriormente irles analizando.



No.	Time	Source	Destination	Protocol	Length	Time delta from previous captured frame	Time delta from previous displayed frame	Info
1	0.000000	172.16.41.127	172.16.41.130	TCP	1396	0.000000000	0.000000000	0 → 0 [<None>] Seq=1 Win=1024 Len=1338
12	1.121172	172.16.41.127	172.16.41.130	TCP	1396	0.093937000	1.121172000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
30	2.413505	172.16.41.127	172.16.41.130	TCP	1396	0.082789000	1.292333000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
41	3.502466	172.16.41.127	172.16.41.130	TCP	1396	0.100185000	1.088961000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
60	4.959540	172.16.41.127	172.16.41.130	TCP	1396	0.130613000	1.457074000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
72	6.066021	172.16.41.127	172.16.41.130	TCP	1396	0.107084000	1.106481000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
88	7.368334	172.16.41.127	172.16.41.130	TCP	1396	0.086398000	1.302313000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
102	8.709568	172.16.41.127	172.16.41.130	TCP	1396	0.199848000	1.341234000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
119	10.116082	172.16.41.127	172.16.41.130	TCP	1396	0.086094000	1.406514000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
132	11.301789	172.16.41.127	172.16.41.130	TCP	1396	0.152265000	1.185707000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
147	12.555607	172.16.41.127	172.16.41.130	TCP	1396	0.149632000	1.253818000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
163	13.749155	172.16.41.127	172.16.41.130	TCP	1396	0.129669000	1.193548000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
175	15.004671	172.16.41.127	172.16.41.130	TCP	1396	0.092116000	1.255516000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
193	16.380707	172.16.41.127	172.16.41.130	TCP	1396	0.103831000	1.376036000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
205	17.453317	172.16.41.127	172.16.41.130	TCP	1396	0.034276000	1.072610000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
224	18.875861	172.16.41.127	172.16.41.130	TCP	1396	0.128167000	1.422544000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338

Figura 26: Captura de tráfico TCP sin QoS con FIFO
Fuente: Autor

4.6.2 FIFO CON WRED

La figura 27 muestra la configuración de la cola FIFO con WRED, ya que evita que se llene totalmente FIFO y así ayuda a que los paquetes se descarten de manera aleatoria, lo que reduce la saturación y el rendimiento, mejorando la estabilidad de la red.
Se crea una política y dentro de ella una clase predeterminada; posteriormente se habilita la detección aleatoria (random-detect), que es utilizada para evitar la congestión de la red. Luego asignamos la política a la interfaz g0/0 como política saliente.

```
R1(config)#no policy-map politica_fifo
R1(config)#policy-map fifo_wred
R1(config-pmap)#class
R1(config-pmap)#class class-default
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#exit
R1(config)#interface g0/0
R1(config-if)#service
R1(config-if)#service-policy ou
R1(config-if)#service-policy output fifo_wred
R1(config-if)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Figura 27: Configuración de FIFO con WRED sin QoS
Fuente: Autor

En la figura 28 se observa la captura de tráfico TCP utilizando la configuración de colas FIFO con WRED donde:

- Time: Es el tiempo que se capturo al paquete.

- Fuente: Es la IP de origen.
- Destino: Es la IP de destino.
- Protocolo: Es el protocolo que se está utilizando en este caso el TCP.
- Longitud: Medida en bytes del paquete.
- Info: Información sobre el paquete.

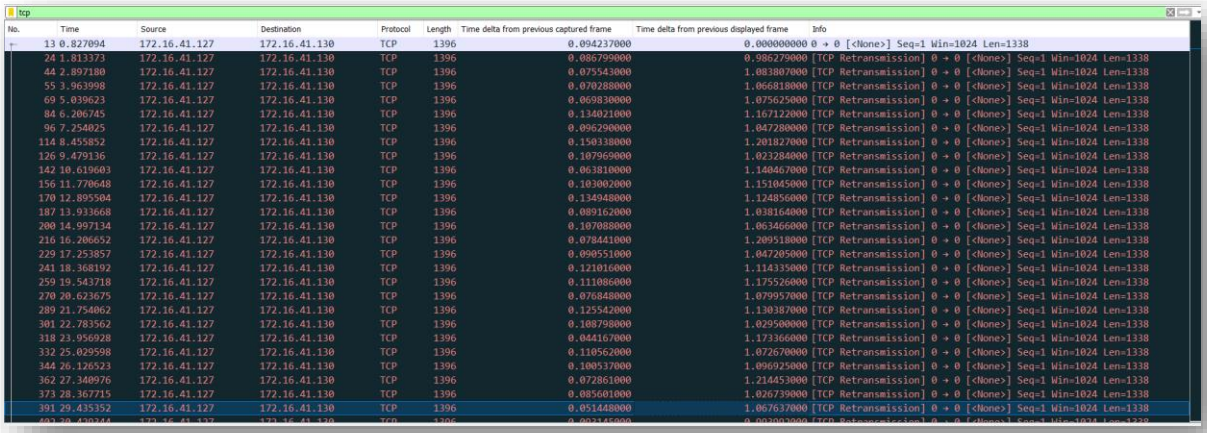


Figura 28: Captura de tráfico TCP sin QoS de FIFO con WRED
Fuente: Autor

4.6.3 WFQ

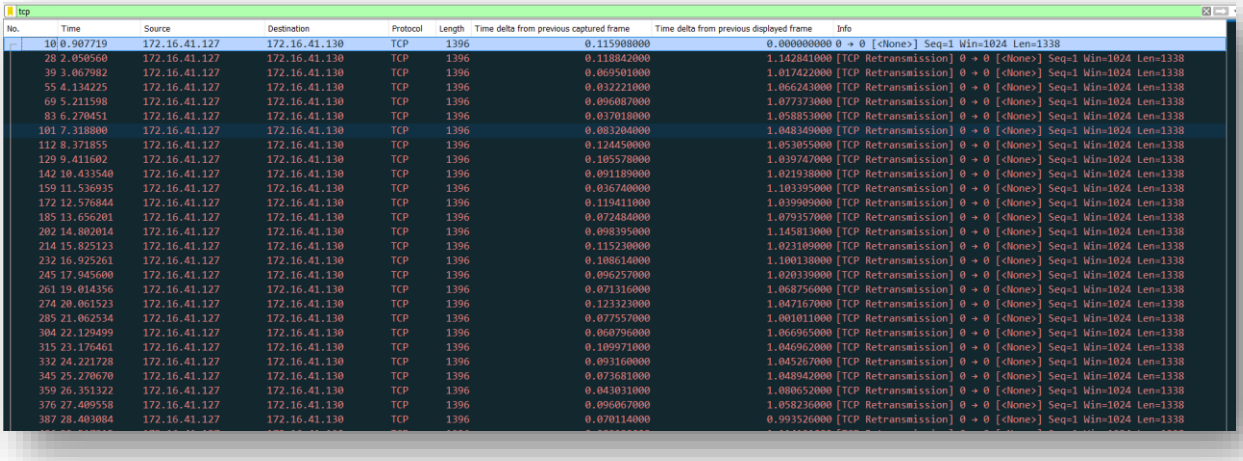
La figura 29 muestra la configuración en el router creando una clase llamada cola_wfq, y asignando a la g0/0 la política, ya que con WFQ distribuye el ancho de banda de manera equitativa entre todas las colas activas y así sus paquetes más importantes se priorizan automáticamente y esto es beneficioso para aplicaciones en tiempo real.

```
R1(config)#class-map match-any cola_wfq
R1(config-cmap)#mat
R1(config-cmap)#match any
R1(config-cmap)#pol
R1(config-cmap)#policy
R1(config-cmap)#policy-map politica_wfq
R1(config-pmap)#class colas_wfq
class map colas_wfq not configured
R1(config-pmap)#band
R1(config-pmap)#bandwidth percent 30
                  ^
% Invalid input detected at '^' marker.

R1(config-pmap)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy ou
R1(config-if)#service-policy output politica_wfq
R1(config-if)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Figura 29: Configuración de WFQ sin QoS
Fuente: Autor

En la figura 30 muestra la captura de tráfico TCP con el protocolo WFQ sin calidad de servicio y la variación de los tiempos de los paquetes que serán analizados estadísticamente.



No.	Time	Source	Destination	Protocol	Length	Time delta from previous captured frame	Time delta from previous displayed frame	Info
10	0.907719	172.16.41.127	172.16.41.130	TCP	1396	0.115908000	0.000000000	0 → 0 [<None>] Seq=1 Win=1024 Len=1338
28	2.050560	172.16.41.127	172.16.41.130	TCP	1396	0.118842000	1.142841000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
39	3.067982	172.16.41.127	172.16.41.130	TCP	1396	0.069501000	1.017422000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
55	4.134225	172.16.41.127	172.16.41.130	TCP	1396	0.032221000	1.066243000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
69	5.211598	172.16.41.127	172.16.41.130	TCP	1396	0.096087000	1.077373000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
83	6.270451	172.16.41.127	172.16.41.130	TCP	1396	0.037018000	1.058853000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
101	7.318800	172.16.41.127	172.16.41.130	TCP	1396	0.083204000	1.048349000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
112	8.371855	172.16.41.127	172.16.41.130	TCP	1396	0.124450000	1.053055000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
129	9.411602	172.16.41.127	172.16.41.130	TCP	1396	0.105578000	1.039747000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
142	10.433540	172.16.41.127	172.16.41.130	TCP	1396	0.091189000	1.021938000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
159	11.536935	172.16.41.127	172.16.41.130	TCP	1396	0.036740000	1.103395000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
172	12.576844	172.16.41.127	172.16.41.130	TCP	1396	0.119411000	1.039909000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
185	13.656201	172.16.41.127	172.16.41.130	TCP	1396	0.072484000	1.079357000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
202	14.802014	172.16.41.127	172.16.41.130	TCP	1396	0.098395000	1.145813000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
214	15.825123	172.16.41.127	172.16.41.130	TCP	1396	0.115230000	1.023109000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
232	16.925261	172.16.41.127	172.16.41.130	TCP	1396	0.108614000	1.100138000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
245	17.945600	172.16.41.127	172.16.41.130	TCP	1396	0.096257000	1.020339000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
261	19.014356	172.16.41.127	172.16.41.130	TCP	1396	0.071316000	1.068756000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
274	20.061523	172.16.41.127	172.16.41.130	TCP	1396	0.123323000	1.047167000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
285	21.062534	172.16.41.127	172.16.41.130	TCP	1396	0.077557000	1.001011000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
304	22.129499	172.16.41.127	172.16.41.130	TCP	1396	0.060796000	1.066965000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
315	23.176461	172.16.41.127	172.16.41.130	TCP	1396	0.109971000	1.046962000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
332	24.221728	172.16.41.127	172.16.41.130	TCP	1396	0.093160000	1.045267000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
345	25.270670	172.16.41.127	172.16.41.130	TCP	1396	0.073681000	1.048942000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
359	26.351322	172.16.41.127	172.16.41.130	TCP	1396	0.043031000	1.080652000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
376	27.409558	172.16.41.127	172.16.41.130	TCP	1396	0.096067000	1.058236000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
387	28.403084	172.16.41.127	172.16.41.130	TCP	1396	0.070114000	0.993526000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338

Figura 30: Captura de tráfico TCP de WFQ sin QoS
Fuente: Autor

4.6.4 WFQ con WRED

WRED es un proceso de control de congestión, ya que con WFQ progresa mejor el rendimiento de la red y evita la congestión antes de que pase, rechazando cuidadosamente paquetes de colas, y es muy necesario para las redes TCP y así vayan reduciendo la congestión en la red.

La figura 31 muestra la configuración, ya que primero creamos una política que incluye colas y a la interfaz g0/0 le aplicamos la política creada.

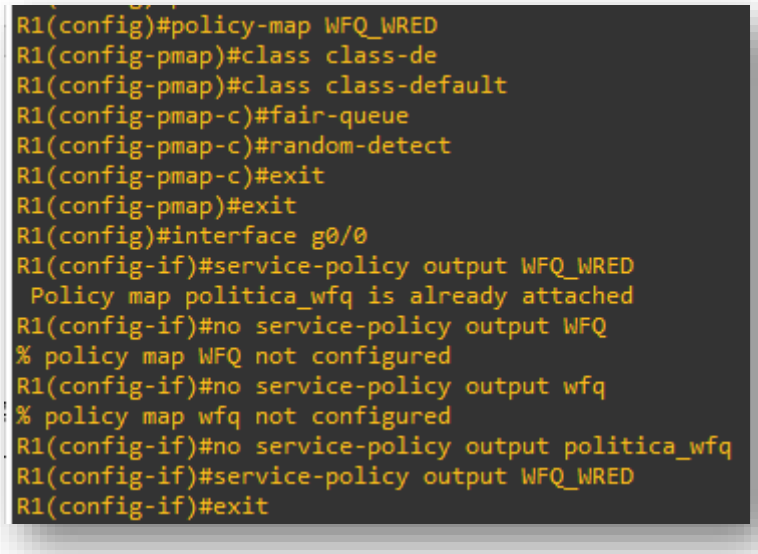


Figura 31: Configuración de WFQ con WRED sin QoS
Fuente: Autor

En la figura 32 muestra de lo que se va capturando el tráfico TCP con el protocolo WFQ con WRED sin calidad de servicio (QoS) con sus variaciones de tiempos.

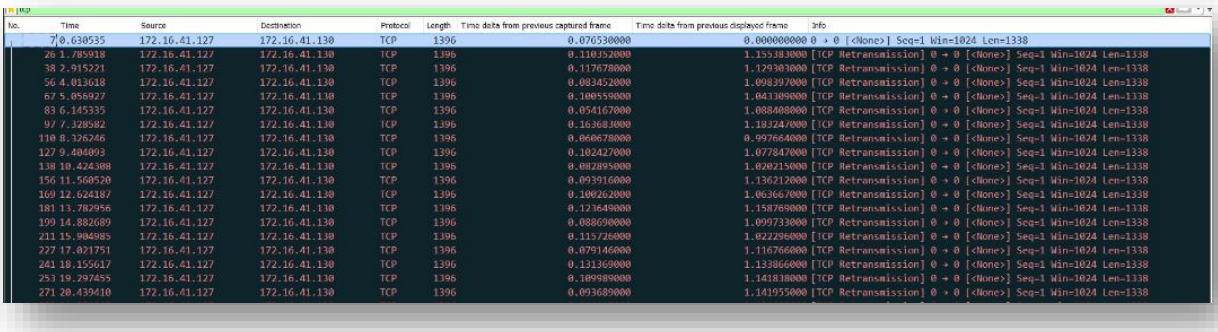


Figura 32: Captura de tráfico TCP de WFQ con WRED sin QoS
Fuente: Autor

4.6.5 CBWFQ

CBWFQ brinda un control más riguroso al conceder que los usuarios agrupen el tráfico en clases basado en diferentes normas, como protocolos o direcciones IP.
En la figura 33 se define las clases simples que agrupan cierta forma de tráfico como tenemos las creadas una para tráfico web y otra para el resto. A continuación, se asigna el ancho de banda a cada clase utilizando el comando bandwidth para determinar el

número de ancho de banda que se asigna a las clases, por último, se aplica la política de colas a la interfaz g0/0.

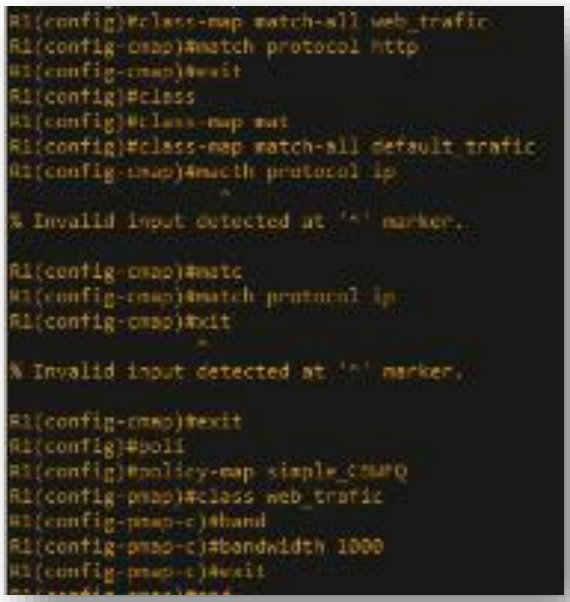


Figura 33: Configuración de CBWFQ sin QoS
Fuente: Autor

En la figura 34 muestra la captura de tráfico TCP con el protocolo CBWFQ sin calidad de servicio con los tiempos variados para el estudio estadístico.

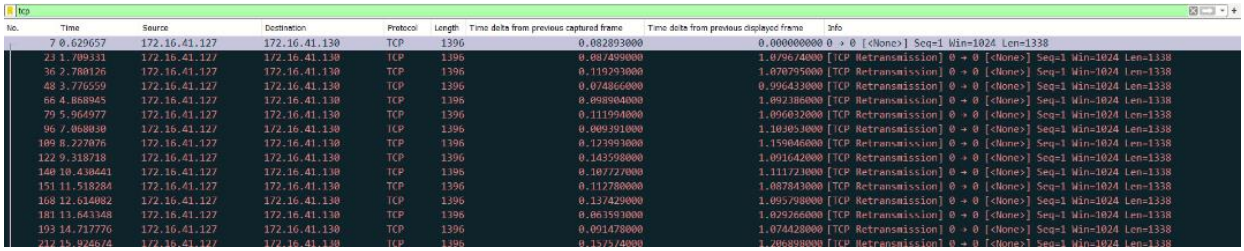


Figura 34: Captura de tráfico TCP de CBWFQ sin QoS
Fuente: Autor

4.6.6 CBWFQ con WRED

WRED evita la congestión eliminando algunos paquetes de forma específica al momento que las colas empiecen a llenarse.
En la figura 35 se crean las clases de tráfico para la agrupación de algunos tipos de paquetes; a continuación, se crean dos clases, una para el tráfico HTTP y otra para el tráfico sobrante. Por siguiente, se crea la política de colas y la atribución del ancho de banda a cada clase; al poner WRED en las colas, irá ayudando con la congestión.

```
R1(config)#class-map match-all web_trafic
R1(config-cmap)#mat
R1(config-cmap)#match protocol http
R1(config-cmap)#exit
R1(config)#class-map match-all default_trafic
R1(config-cmap)#match protocol ip
R1(config-cmap)#exit
R1(config)#poli
R1(config)#policy-map cbwfq_wred
R1(config-pmap)#class web_trafic
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 1000
R1(config-pmap-c)#rand
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#class default_trafic
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 500
R1(config-pmap-c)#rand
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#exit
R1(config)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy out
R1(config-if)#service-policy output cbwfq_wred
 Policy map WFQ_RED is already attached
R1(config-if)#po
R1(config-if)#poli
R1(config-if)#exit
R1(config)#polic
R1(config)#policy-map
R1(config)#no policy-map WFQ_RED
R1(config)#interface g0/0
R1(config-if)#service-policy output cbwfq_wred
R1(config-if)#
*Oct 17 14:09:02.319: %QOS-4-QLIMIT_HQUEUE_VALUE_SY

R1(config-if)#exit
```

Figura 35: Configuración de CBWFQ con WRED sin QoS
Fuente: Autor

En la figura 36 muestra lo que va capturando el tráfico TCP con el protocolo CBWFQ con WRED sin calidad de servicio y variando sus valores para las pruebas estadísticas.

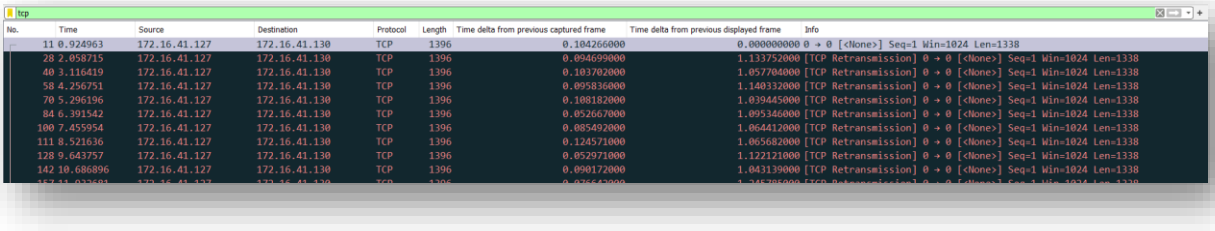


Figura 36: Captura de tráfico TCP de CBWFQ con WRED sin QoS
Fuente: Autor

4.7 Configuración con calidad de servicio (QoS)

4.7.1 FIFO

En la figura 37 describimos las clases de tráfico que se gestionarán con calidad de servicios, en este caso una clase para el tráfico HTTP y otra clase para el tráfico predeterminado. Se continúa creando política de calidad de servicio que asigna anchos de

banda definidos a cada clase de tráfico, ya que utilizamos FIFO; no se dará prioridad ni se arreglarán los paquetes, solo se fijarán límites o asignación de ancho de banda.

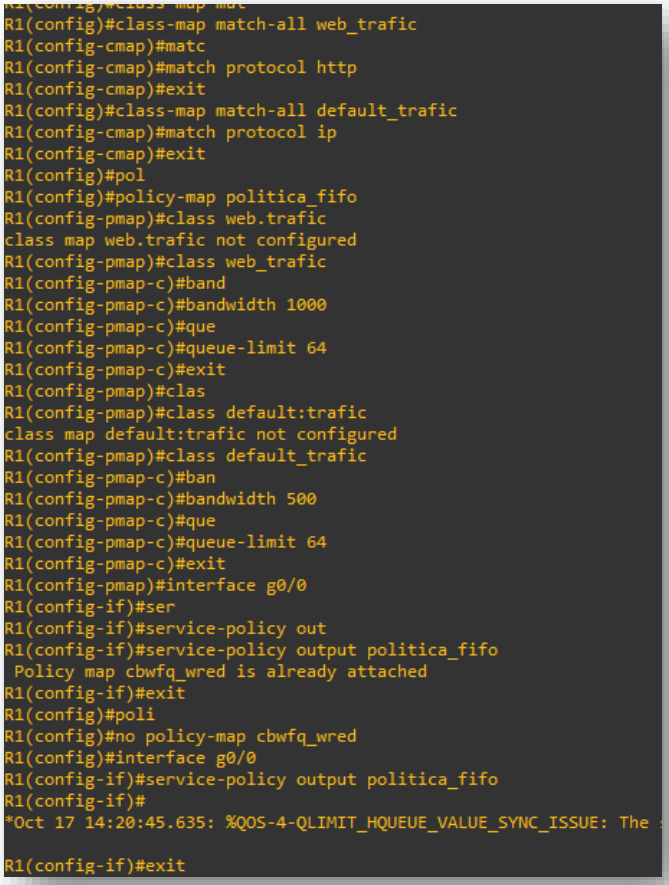


Figura 37: Configuración de FIFO con QoS
Fuente: Autor

En la figura 38 al aplicar QoS en una cola FIFO asegura que ciertos tipos de tráfico reciban un ancho de banda mínimo sin anteponer un tráfico sobre otro, y así recortar el tamaño de las colas para impedir congestiones.

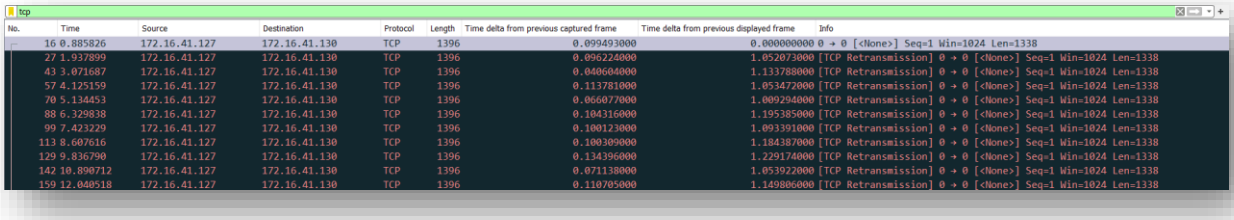


Figura 38: Captura de tráfico TCP de FIFO con QoS
Fuente: Autor

4.7.2 FIFO con WRED

En la figura 39 se coloca una clase para la voz y otra clase para un tráfico general y uno por defecto para lo sobrante, utilizamos también una política para agrupar las clases con

el tráfico, definimos el ancho de banda en cada clase y usamos WRED para gestionar la congestión.

```
R1(config)#class-map match-any trafico_voz
R1(config-cmap)#mat
R1(config-cmap)#match protocol rtp
R1(config-cmap)#class-map match-any trafico_dato
R1(config-cmap)#match protocol http
R1(config-cmap)#pol
R1(config-cmap)#poli
R1(config-cmap)#exit
R1(config)#poli
R1(config)#policy-map fifo_wred_qs
R1(config-pmap)#class trafico_voz
R1(config-pmap-c)#prio
R1(config-pmap-c)#priority 128
R1(config-pmap-c)#class trafico_datos
class map trafico_datos not configured
R1(config-pmap)#class trafico_dato
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 256
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class class-default
R1(config-pmap-c)#fai
R1(config-pmap-c)#fair-queue ran
R1(config-pmap-c)#fair-queue
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy out
R1(config-if)#service-policy output fifo_wred_qs
 Policy map politica_fifo is already attached
R1(config-if)#exit
R1(config)#pol
R1(config)#no policy-map politica_fifo
R1(config)#interface g0/0
R1(config-if)#service-policy output fifo_wred_qs
R1(config-if)#
*Oct 17 14:36:36.795: %QOS-4-QLIMIT_HQUEUE_VALUE_SYNC_ISS

R1(config-if)#exit
```

Figura 39: Configuración de FIFO con WRED y QoS
Fuente: Autor

En la figura 40 muestra la captura de tráfico TCP con el ancho de banda asignado ya que QoS prioriza tráfico como voz y video.

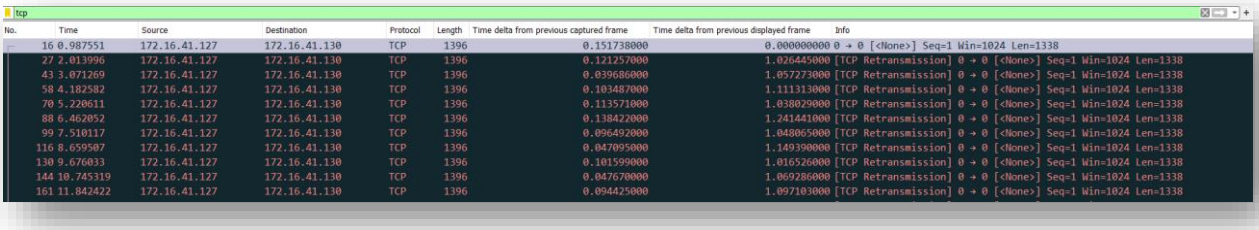


Figura 40: Captura de tráfico TCP de FIFO con WRED y QoS
Fuente: Autor

4.7.3 WFQ

En la figura 41 se definen las clases de tráfico que se van a priorizar y se lo realiza mediante class-maps, el cual va determinando qué tipos de tráfico afectan a cada clase. Configuramos la política WFQ y a su vez el ancho de banda de cada clase de tráfico; por último, aplicamos la política a la interfaz, en nuestro caso a la g0/0, para que QoS utilice el tráfico que pasa por la interfaz. Esta configuración asegura que el tráfico reciba el ancho de banda apropiado y eficiente utilizando WFQ en conjunto con QoS.

```
R1(config)#class-map match-any trafico_voz
R1(config-cmap)#mat
R1(config-cmap)#match protocol rtp
R1(config-cmap)#class-map match-any trafico_dato
R1(config-cmap)#match protocol http
R1(config-cmap)#class-map match-any trafico_video
R1(config-cmap)#match protocol rtsp
R1(config-cmap)#exit
R1(config)#poli
R1(config)#policy-map WFQ_qos
R1(config-pmap)#class trafico_voz
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 128
R1(config-pmap-c)#class trafico_dato
R1(config-pmap-c)#ba
R1(config-pmap-c)#bandwidth 256
R1(config-pmap-c)#class trafico_video
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 512
R1(config-pmap-c)#clas
R1(config-pmap-c)#class class_default
class map class_default not configured
R1(config-pmap)#class class-default
R1(config-pmap-c)#fa
R1(config-pmap-c)#fair-queue
R1(config-pmap-c)#exit
R1(config-pmap)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy ou
R1(config-if)#service-policy output wfq_qos
% policy map wfq_qos not configured
R1(config-if)#exit
R1(config)#pol
R1(config)#no policy-map fifo_wred_qs
R1(config)#interface g0/0
R1(config-if)#service-policy output wfq_qos
% policy map wfq_qos not configured
R1(config-if)#service-policy output WFQ_qos
R1(config-if)#
*Oct 17 14:52:02.051: %QOS-4-QLIMIT_HQUEUE_VALUE_SYN
```

Figura 41: Configuración de WFQ con QoS
Fuente: Autor

En la figura 42 muestra la captura de tráfico TCP con el protocolo WFQ aplicado con calidad de servicio QoS y con sus variaciones de tiempos.

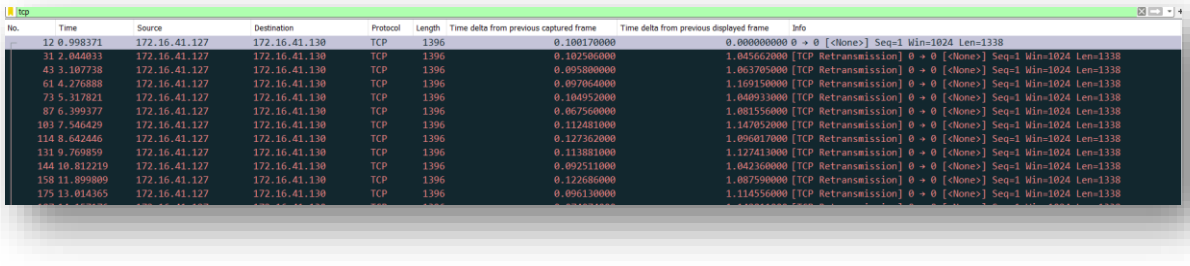


Figura 42: Captura de tráfico TCP de WFQ y QoS
Fuente: Autor

4.7.4 WFQ con WRED

En la figura 43 tenemos la configuración creamos clases de tráfico para voz, datos y video, configuramos la política y se van asignando anchos de banda, se activa WFQ para el tráfico por defecto y el random-detect activa el WRED para evitar congestión por último se aplica a la política a la interfaz g0/0 y sea manejado por QoS.

```
R1(config)#class-map match-any trafico_voz
R1(config-cmap)#mat
R1(config-cmap)#match protocol rtp
R1(config-cmap)#class-map match-any trafico_dato
R1(config-cmap)#match protocol http
R1(config-cmap)#class-map match-any trafico_video
R1(config-cmap)#match protocol rtsp
R1(config-cmap)#exit
R1(config)#pol
R1(config)#policy-map wfq_wred_qs
R1(config-pmap)#class trafico_voz
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 128
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class trafico_dato
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 256
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class trafico_video
R1(config-pmap-c)#bandwidth 512
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class class-default
R1(config-pmap-c)#fa
R1(config-pmap-c)#fair-queue
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy ou
R1(config-if)#service-policy output wfq_wred_qs
 Policy map WFQ_qos is already attached
R1(config-if)#exiy
             ^
% Invalid input detected at '^' marker.

R1(config-if)#exit
R1(config)#pol
R1(config)#no policy-map WFQ_qos
R1(config)#interface g0/0
R1(config-if)#service-policy output wfq_wred_qs
R1(config-if)#
```

Figura 43: Configuración de WFQ con WRED y QoS
Fuente: Autor

La figura 44 muestra la captura del tráfico TCP generado con el protocolo WFQ con WRED aplicando calidad de servicio QoS como es visible disminuyen los intervalos de tiempos y serán estudiados estadísticamente.

tcp

No.	Time	Source	Destination	Protocol	Length	Time delta from previous captured frame	Time delta from previous displayed frame	Info
6	0.321653	172.16.41.127	172.16.41.130	TCP	1396	0.060087000	0.000000000	0 → 0 [<None>] Seq=1 Win=1024 Len=1338
20	1.402443	172.16.41.127	172.16.41.130	TCP	1396	0.113726000	1.080790000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
32	2.418221	172.16.41.127	172.16.41.130	TCP	1396	0.097280000	1.015778000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
49	3.472762	172.16.41.127	172.16.41.130	TCP	1396	0.098429000	1.054541000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
60	4.530766	172.16.41.127	172.16.41.130	TCP	1396	0.075428000	1.058004000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
80	5.685779	172.16.41.127	172.16.41.130	TCP	1396	0.132869000	1.155013000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
91	6.803767	172.16.41.127	172.16.41.130	TCP	1396	0.103765000	1.117988000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
108	7.944083	172.16.41.127	172.16.41.130	TCP	1396	0.030166000	1.140316000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338
121	8.954536	172.16.41.127	172.16.41.130	TCP	1396	0.099835000	1.010453000	[TCP Retransmission] 0 → 0 [<None>] Seq=1 Win=1024 Len=1338

Figura 44: Captura de tráfico TCP de WFQ con WRED y QoS
Fuente: Autor

4.7.5 CBWFQ

La figura 45 muestra la configuración del protocolo, el CBWFQ asigna prioridades y garantiza los tipos específicos de tráfico, como es voz, video o datos, reciban los recursos apropiados. Al combinar CBWFQ con QoS genera una solución flexible para ejecutar el tráfico en redes empresariales, afirmando que cada tipo de tráfico reciba adecuados recursos y el rendimiento general de la red sea satisfactorio y equilibrado.

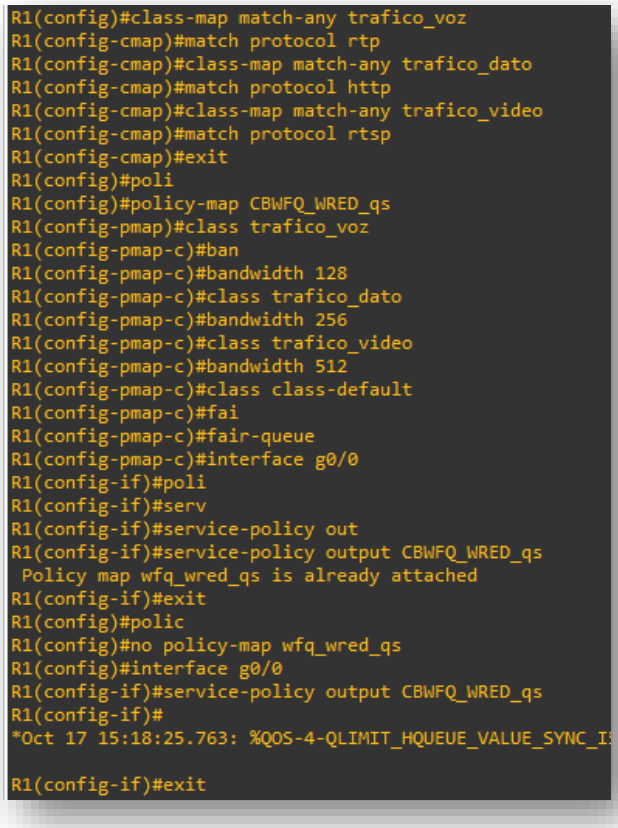


Figura 45: Configuración de CBWFQ y QoS
Fuente: Autor

En la figura 46 muestra la captura de los paquetes del protocolo TCP con la dirección IP de origen y destino también muestra los retrasos entre la captura de los paquetes y entre la visualización de los mismos.

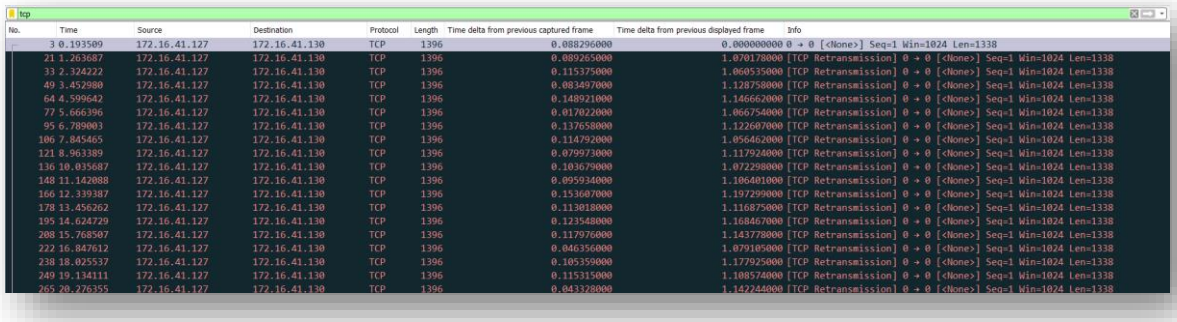


Figura 46: Captura de tráfico TCP de CBWFQ con QoS
Fuente: Autor

4.7.6 CBWFQ con WRED

Esta configuración de CBWFQ con WRED y QoS permite gestionar el tráfico de manera satisfactoria, confirmando el ancho de banda necesario para cada tipo de tráfico impidiendo la congestión a través de la gestión de colas. Esto es fundamental para mantener un rendimiento excelente en redes donde hay tráfico delicado como voz y video.

```
R1(config)#class-map match-any trafico_voz
R1(config-cmap)#match protocol rtp
R1(config-cmap)#class-map match-any trafico_dato
R1(config-cmap)#match protocol http
R1(config-cmap)#class-map match-any trafico_video
R1(config-cmap)#match protocol rtsp
R1(config-cmap)#exit
R1(config)#poli
R1(config)#policy-map CBWFQ_WRED2_qs
R1(config-pmap)#class trafico_voz
R1(config-pmap-c)#ban
R1(config-pmap-c)#bandwidth 128
R1(config-pmap-c)#ran
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class trafico_dato
R1(config-pmap-c)#bandwidth 256
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class trafico_dato
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class trafico_video
R1(config-pmap-c)#bandwidth 512
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#class class-default
R1(config-pmap-c)#fa
R1(config-pmap-c)#fair-queue
R1(config-pmap-c)#ra
R1(config-pmap-c)#random-detect
R1(config-pmap-c)#exit
R1(config-pmap)#interface g0/0
R1(config-if)#ser
R1(config-if)#service-policy ou
R1(config-if)#service-policy output CBWFQ_WRED2_qs
 Policy map CBWFQ_WRED_qs is already attached
R1(config-if)#exit
R1(config)#pol
R1(config)#no policy-map CBWFQ_WRED_qs
R1(config)#interface g0/0
R1(config-if)#service-policy output CBWFQ_WRED2_qs
R1(config-if)#
*Oct 17 15:34:34.615: %QOS-4-QLIMIT_HQUEUE_VALUE_SYNC_ISSUE: The sum

R1(config-if)#exit
R1(config)#do wr
Building configuration...
```

Figura 47: Configuración de CBWFQ con WRED y QoS
Fuente: Autor

En la figura 48 muestra la captura de tráfico TCP con sus distintas variaciones de tiempo

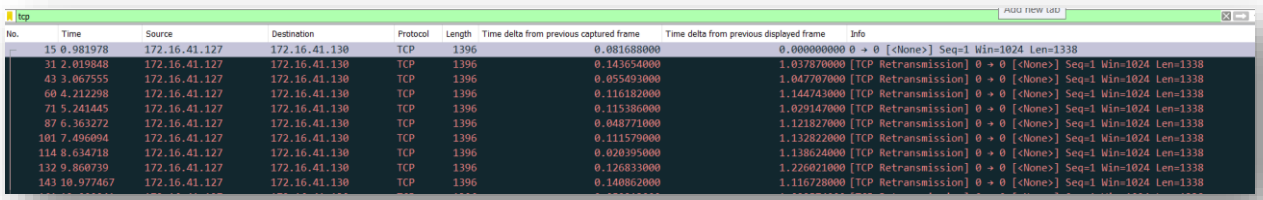


Figura 48: Captura de tráfico TCP de CBWFQ con WRED y QoS
Fuente: Autor

4.8 Resultados

4.8.1 FIFO – JITTER

La tabla 11 presenta el análisis de desempeño de la red tomando en consideración la calidad de servicio (QoS).
Se tiene una métrica principal que es el JITTER y es evaluado en diferentes escenarios que son: con QoS, sin QoS , WRED sin QoS y WRED con QoS, para cada caso se considera 150 datos como muestra, lo que equivale al 100% sin tener perdidas.

Tabla 11. Resumen del proceso de casos

	FIFO	Válido			
		N	Porcentaje	Porcentaje	Porcentaje
JITTER	QoS	150	100,0%	0,0%	100,0%
	sin QoS	150	100,0%	0,0%	100,0%
	WRED -sin QoS	150	100,0%	0,0%	100,0%
	WRED QoS	150	100,0%	0,0%	100,0%

Fuente: Autor

4.8.1.1 Histogramas

La figura 49 ilustra la asignación de los valores de jitter en el protocolo QoS:
El valor 1.02110 representa la media de los valores de jitter que se han medido, para mayoría de servicios de red, un promedio cercano a 1.0 ms de jitter es bastante aceptable, aunque sería más conveniente que sea inferior a 1 ms en aplicaciones de baja latencia.

El valor 0.09113 ilustra la variabilidad de los datos en comparación con la media, la reducida desviación estándar señala que las fluctuaciones en el jitter son mínimas lo que constituye un indicador positivo para la estabilidad de la red.
El histograma revela una elevada concentración de valores que oscilan entre 0.9 y 1.1 ms, lo que implica que la red proporciona un jitter estable en la mayoría de los casos.
No obstante, existen valores atípicos (de 0.0 a 0.3 ms) que podrían indicar variaciones en el tráfico o fallos ocasionales.
Los valores en el intervalo de 0.2 ms podrían ser atribuibles a:

- **Desorden en la red:** Sí, la red sufre un tráfico desmedido en determinados instantes.
- **Cuestiones de hardware:** Como un enrutador o interruptor defectuoso que a veces provoca demoras.
- **Configuraciones deficientes**: Incorrectas configuraciones de priorización para paquetes o políticas de QoS.
- **Interferencias provenientes del exterior:** Especialmente en redes sin cables donde las señales pueden verse alteradas por el ambiente.

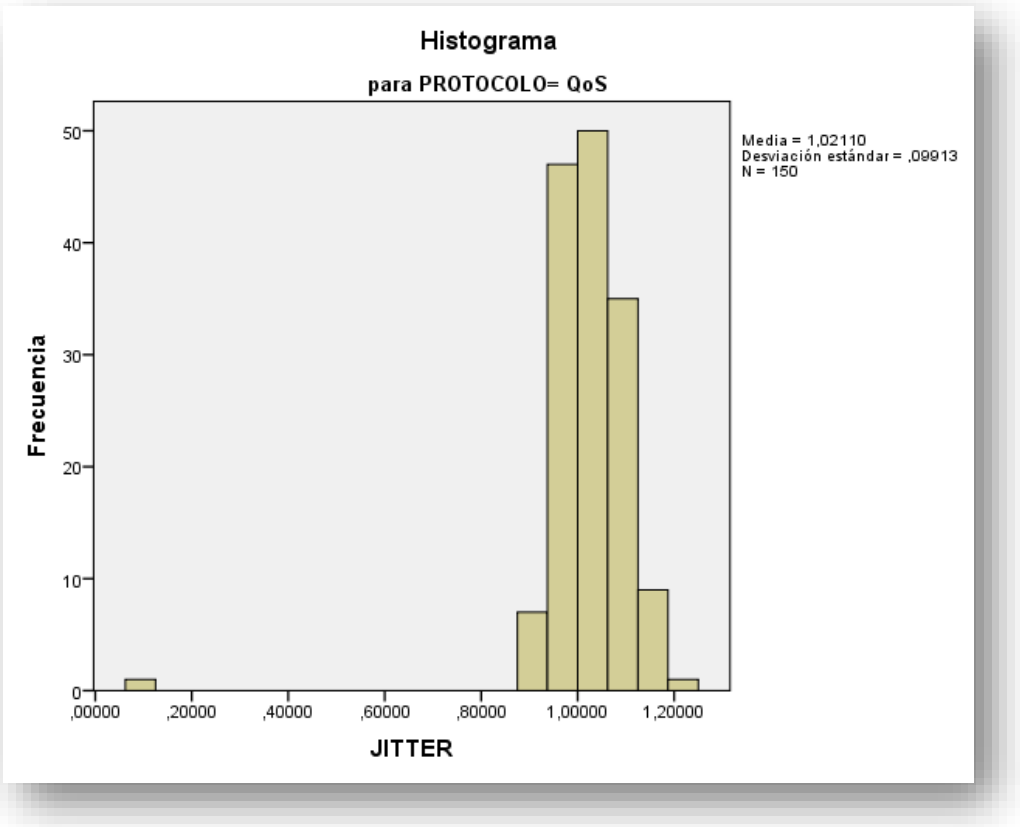


Figura 49: Histograma de FIFO-QoS
Fuente: Autor

En la figura 50 se ilustra la distribución de los valores de jitter en un contexto en el que no se implementa el protocolo QoS.

La media con el valor 0.90290 indica que el jitter es un poco inferior al del caso con QoS (1.02110).
Si no se aplica QoS, la desviación estándar supera a la que se aplica (0.11827 en lugar de 0.09113). Esto evidencia que los valores de jitter son menos uniformes y coherentes.
A pesar de que la media es inferior sin QoS, una desviación estándar más alta sugiere una calidad de servicio menos constante. Esto podría provocar dificultades en aplicaciones que se rigen por el jitter, como la VoIP o la transmisión de video.

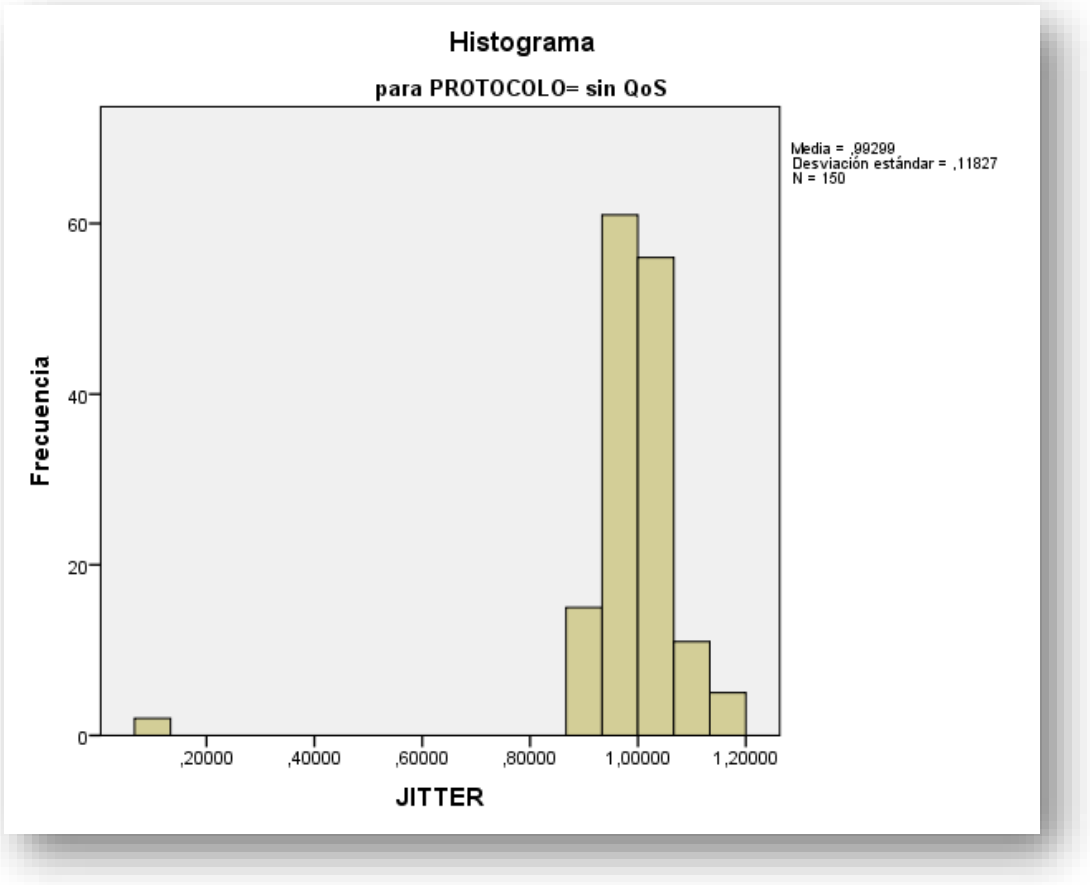


Figura 50: Histograma de FIFO-sin QoS
Fuente: Autor

La figura 51 corresponde al análisis de jitter con el protocolo WRED sin QoS y se detalla el análisis:
La media de jitter supera la media en el ambiente sin QoS estándar (0.90290 ms), y también sobrepasa la media con QoS (1.02110 ms).
El valor 0.16229 ms señala que la variabilidad de los datos es superior en comparación de sin QoS (0.11827 ms) y con QoS (0.09113 ms). Esto muestra una menor uniformidad en la distribución de paquetes.
La mayor parte de los valores de jitter se sitúan entre 0.9 y 1.2 ms, aunque existen algunos que llegan a 1.4 ms, expandiendo el espectro en relación con los histogramas anteriores.
WRED sin QoS presenta una distribución más extensa, lo que indica una dispersión superior en los valores de jitter, lo que indica un control del tráfico menos eficaz.

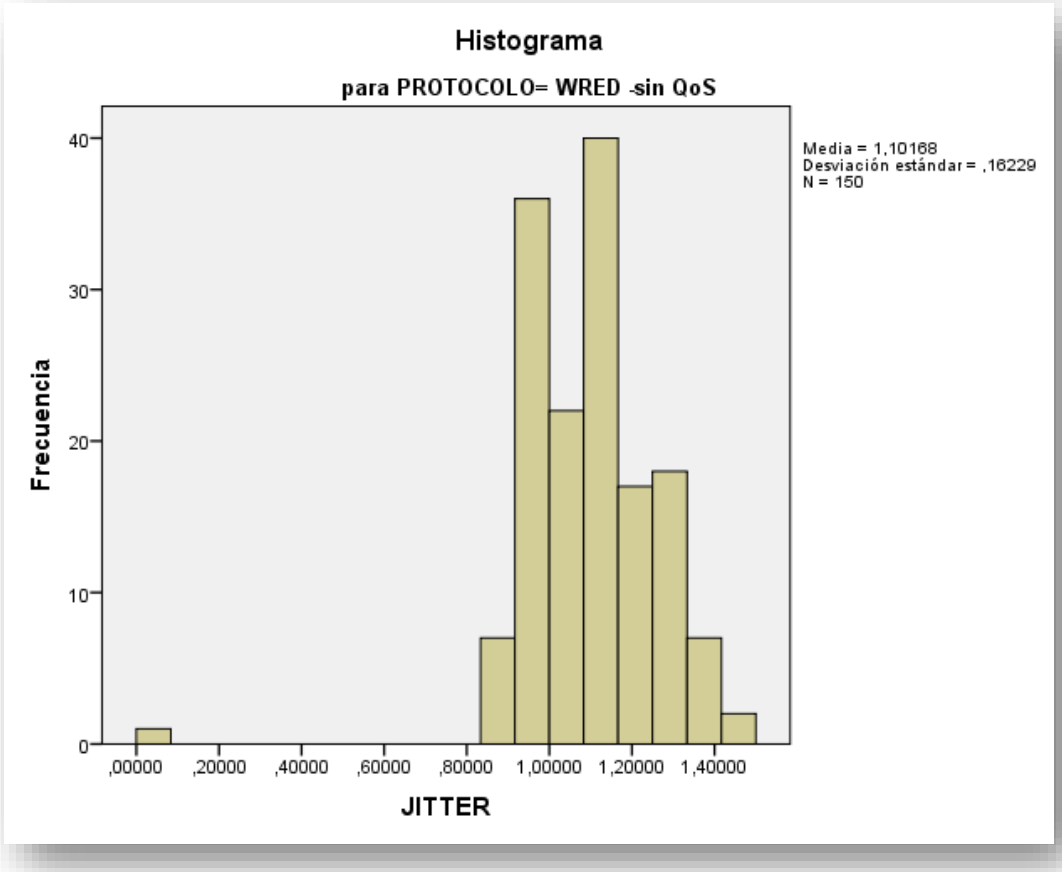


Figura 51: Histograma de FIFO-WRED sin QoS
Fuente: Autor

La figura 52 muestra la repartición de los valores de jitter en una red que emplea el protocolo WRED con QoS:
El valor de la media es de 1.01841 lo que señala que, en términos generales, el valor de jitter en la red se sitúa cerca de 1 unidad. Esto indica que la variación en el retraso de los paquetes de datos es aproximadamente estable.
La desviación estándar es de 0.0945, lo que sugiere que los valores de jitter se encuentran ubicados cerca del promedio con una variabilidad reducida. Esto es un indicador fiable de estabilidad, dado que una dispersión reducida implica que la red conserva un jitter bastante uniforme, esto resulta beneficioso en aplicaciones en tiempo real, en las que una reducida variación en el tiempo de entrega de los paquetes contribuye a mejorar la calidad de servicios susceptibles a los retrasos, como las videollamadas y el streaming.

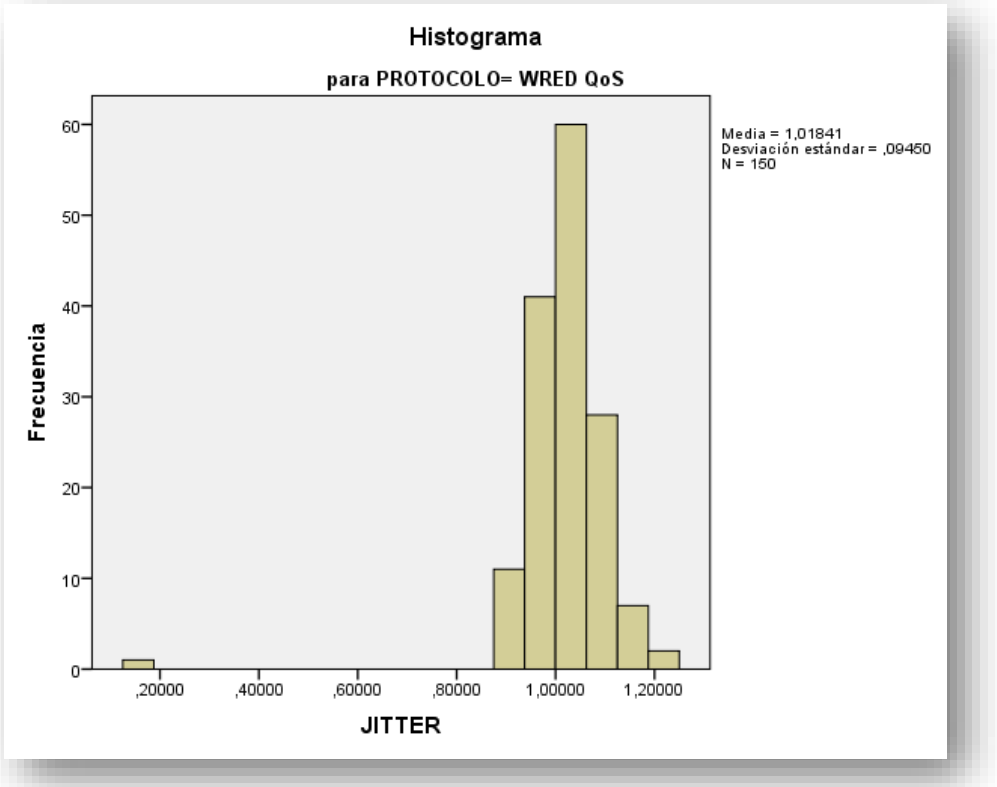


Figura 52: Histograma de FIFO – Wred con QoS
Fuente: Autor

En la figura 53 muestra un diagrama de caja, que contrasta los valores de jitter bajo distintas configuraciones de red con y sin calidad de servicio.

- La opción "WRED - sin QoS" presenta una variabilidad en el jitter más alta, lo que podría resultar menos agradable en aplicaciones en tiempo real debido a la incoherencia en el retraso.
- Al combinar de WRED con QoS disminuye la variabilidad de jitter, pero no en la misma medida que las configuraciones de QoS sin WRED.
- Las configuraciones "QoS" y "sin QoS" presentan los valores de jitter más regulados, con una dispersión y un número reducidos de outliers.

En conclusión, para un jitter más estable y predecible, las configuraciones con QoS presenta resultados superiores, mientras que la utilización de WRED aporta más variabilidad al jitter, aunque su combinación con QoS puede reducir parte de dicha variabilidad.

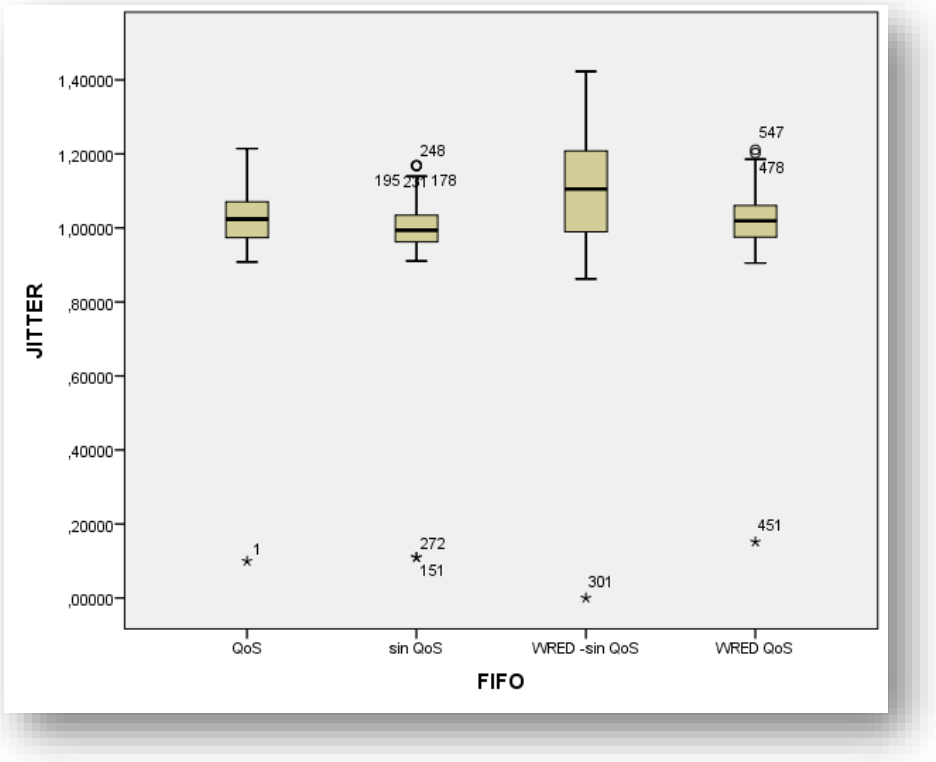


Figura 53: Diagrama de cajas de FIFO con los protocolos
Fuente: Autor

En la tabla 12 muestra el análisis de la varianza con la variable Jitter, el coeficiente de significancia es 0.000 (comúnmente reportado como p < 0.001). Este valor señala que hay una variación de relevancia estadística entre los grupos, dado que el p-valor es inferior al nivel de significancia normal de 0.05.

Tabla 12. Análisis de la varianza ANOVA

ANOVA					
JITTER					
	Suma de cuadrados	Gl	Media cuadrática	F	Sig.
Entre grupos	1,001	3	,334	22,580	,000
Dentro de grupos	8,803	596	,015		
Total	9,804	599			

Fuente: Autor

En la tabla 13 señalan que los grupos sin QoS, WRED QoS y QoS conforman un conjunto uniforme, con medios parecidos a JITTER.

La configuración WRED - sin QoS presenta un valor JITTER notablemente superior, distinguiéndose de los demás grupos, esto indica que las configuraciones con WRED junto con la falta de QoS impactan de manera negativa en la variabilidad de JITTER en comparación con las demás configuraciones.

Tabla 13. Resultados de la prueba post hoc Tukey

JITTER			
HSD Tukey			
FIFO	N	Subconjunto para alfa = 0.05	
		1	2
sin QoS	150	,9929916	
WRED QoS	150	1,0184103	
QoS	150	1,0211046	
WRED - sin QoS	150		1,1016773
Sig.		,188	1,000

Fuente: Autor

En la figura 54 presenta el estudio de la media del jitter basándose en la utilización del protocolo FIFO bajo diversas configuraciones.
El estudio indica que la implementación de QoS y su conexión con WRED disminuyen el jitter y potencian la estabilidad del tiempo de transmisión en la red. En cambio, la configuración sin QoS o con WRED sin QoS suele provocar más inestabilidad en la demora de los paquetes.

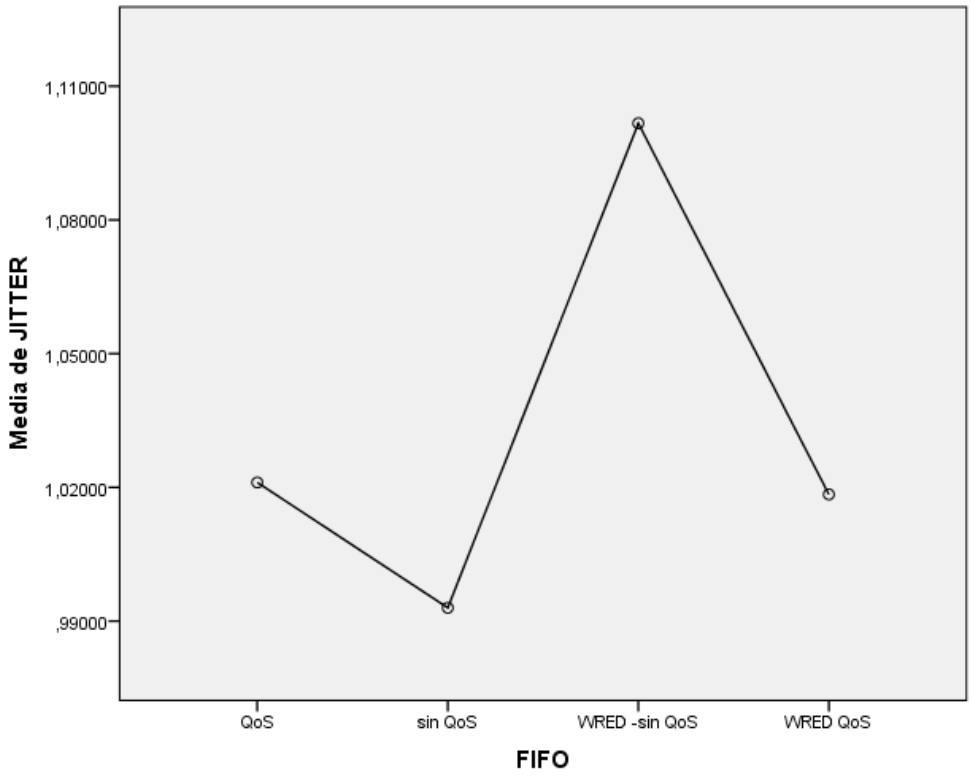


Figura 54: Gráfica de medias del protocolo FIFO
Fuente: Autor

4.8.2 WFQ – JITTER

En la figura 55 muestra la distribución del parámetro Jitter utilizando WFQ con QoS.
La distribución presenta un giro positivo (asimetría hacia la derecha), debido a que existen ciertos valores inferiores (<0,4) que se registran con escasa frecuencia, mientras que la mayoría de los datos se encuentran cerca de 1.
La concentración más elevada se produce en los intervalos [0,9 - 1,1], donde la frecuencia llega a un máximo pico de cerca de 60. Este tipo de protocolo entrega un ancho de banda moderado a diversos flujos de información, un jitter bajo indica que el protocolo está manejando de manera efectiva la asignación temporal de los paquetes.

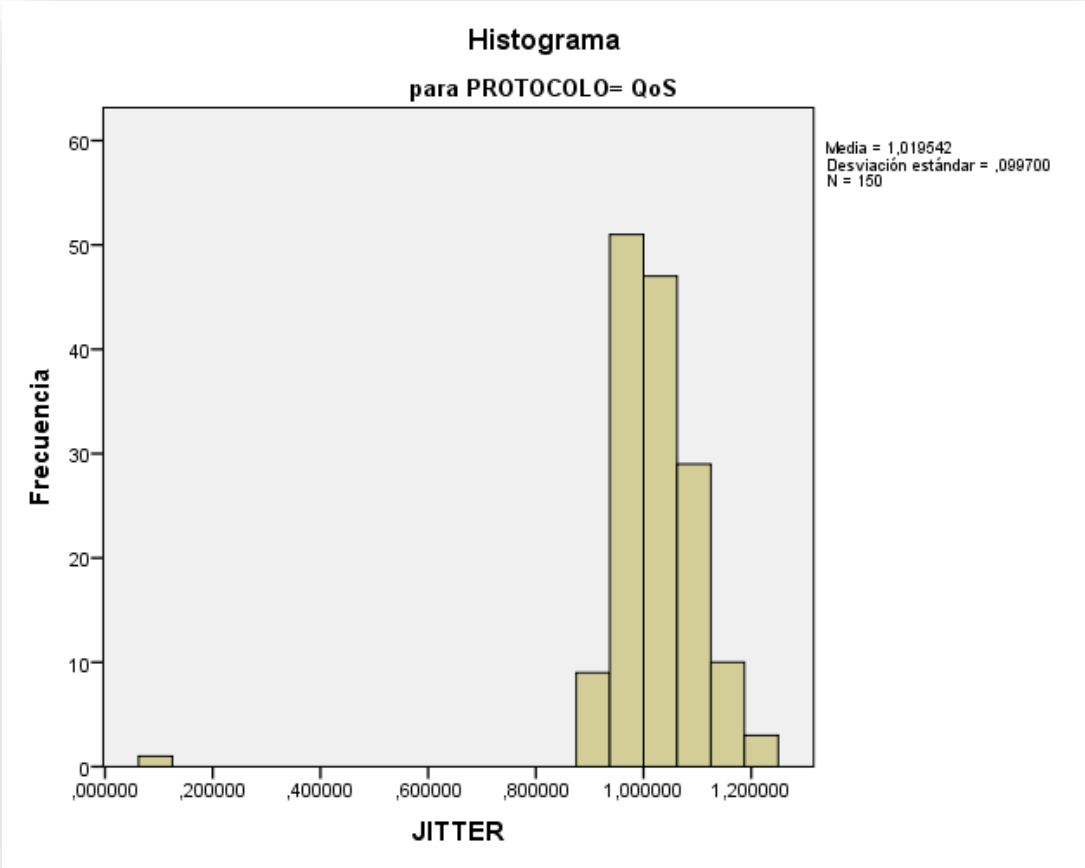


Figura 55: Histograma Jitter WFQ con QoS
Fuente: Autor

La figura 56 muestra el cálculo del Jitter con el protocolo WFQ sin QoS.
El valor 1,1231444 en este esquema supera la media observada con (WFQ con QoS), cuya media era 1,019542. Este aumento indica un incremento en la inestabilidad de la demora de entrega de los paquetes.
El valor 0.150203. señala que los valores de jitter muestran una variabilidad superior a la del protocolo WFQ con QoS (0,089700), lo que sugiere que los tiempos de entrega no son tan uniformes.
La falta de QoS provoca un efecto contrario en el desempeño de la red, demostrado por un jitter más elevado y menos consistente. Esto indica la importancia de establecer protocolos como WFQ para mejorar la gestión del tráfico en redes.

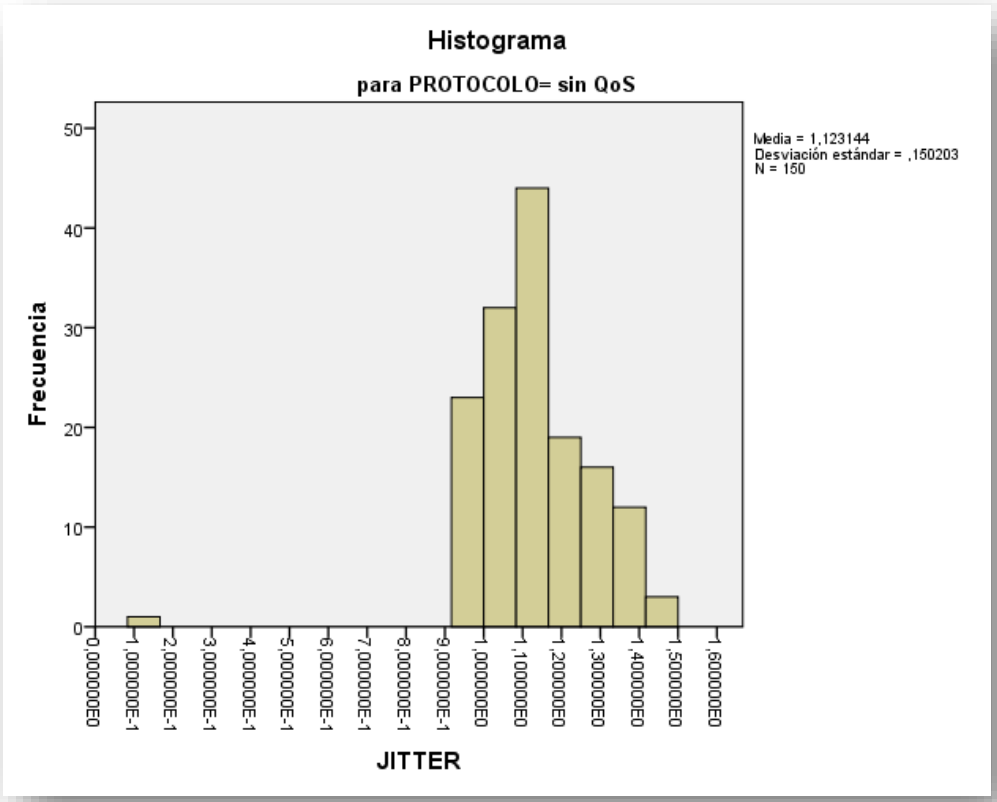


Figura 56: Histograma Jitter-WFQ sin QoS
Fuente: Autor

La figura 57 muestra la variable del jitter con el protocolo WFQ con WRED sin implantación de QoS.
Si la red no establece QoS, no otorga prioridad a tipos específicos de tráfico, la estabilidad demostrada por el protocolo indica que la pérdida de paquetes a causa de la política de descarga aleatoria no impacta de manera significativa en el jitter promedio.

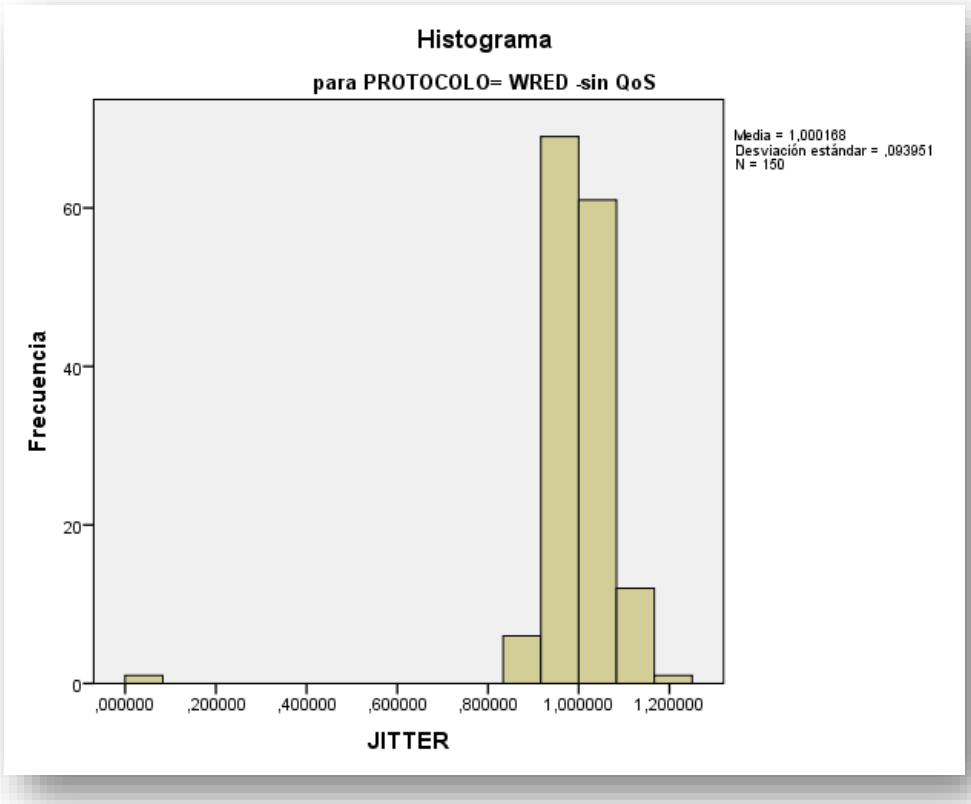


Figura 57: Histograma Jitter-WFQ-Wred sin QoS
Fuente: Autor

La figura 58 muestra los detalles del jitter aplicando el protocolo WFQ con QoS.
El valor 1,020800 señala el promedio del jitter es ligeramente superior a 1, lo que muestra más reducido y consistente debido a la utilización de WRED con QoS por lo que consigue un balance apropiado entre la regulación del tráfico y la consistencia con valores de jitter bastante reducidos y un control adecuado de la variabilidad. Este procedimiento es óptimo para redes combinadas que requieren rendimiento y eficiencia.

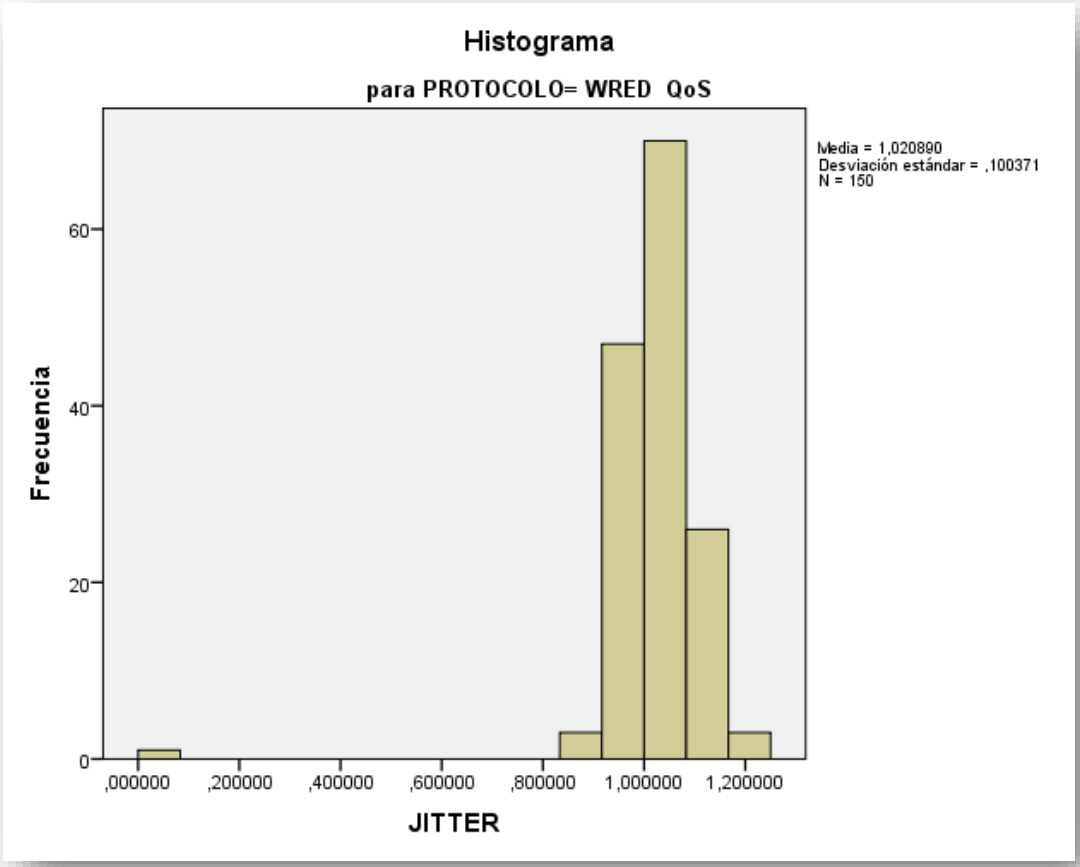


Figura 58: Histograma Jitter-WFQ-Wred con QoS
Fuente: Autor

La figura 59 muestra el diagrama de cajas para el parámetro de Jitter, analizando su reacción en diferentes situaciones de configuración del protocolo WFQ.

- La aplicación de QoS estabiliza el jitter, disminuyendo tanto la variabilidad como la cantidad de valores extremadamente altos.
- La falta de QoS aumenta la variabilidad del jitter, dejando al sistema expuesto a valores extremos y comportamientos menos previsibles.
- La incorporación de WRED ayuda a mejorar un poco la estabilidad, sin embargo, sin QoS se mantiene un nivel considerable de dispersión y valores extremos.
- Al combinar WRED y QoS ofrece la mayor gestión del jitter, minimizando la variabilidad y los valores irregulares.

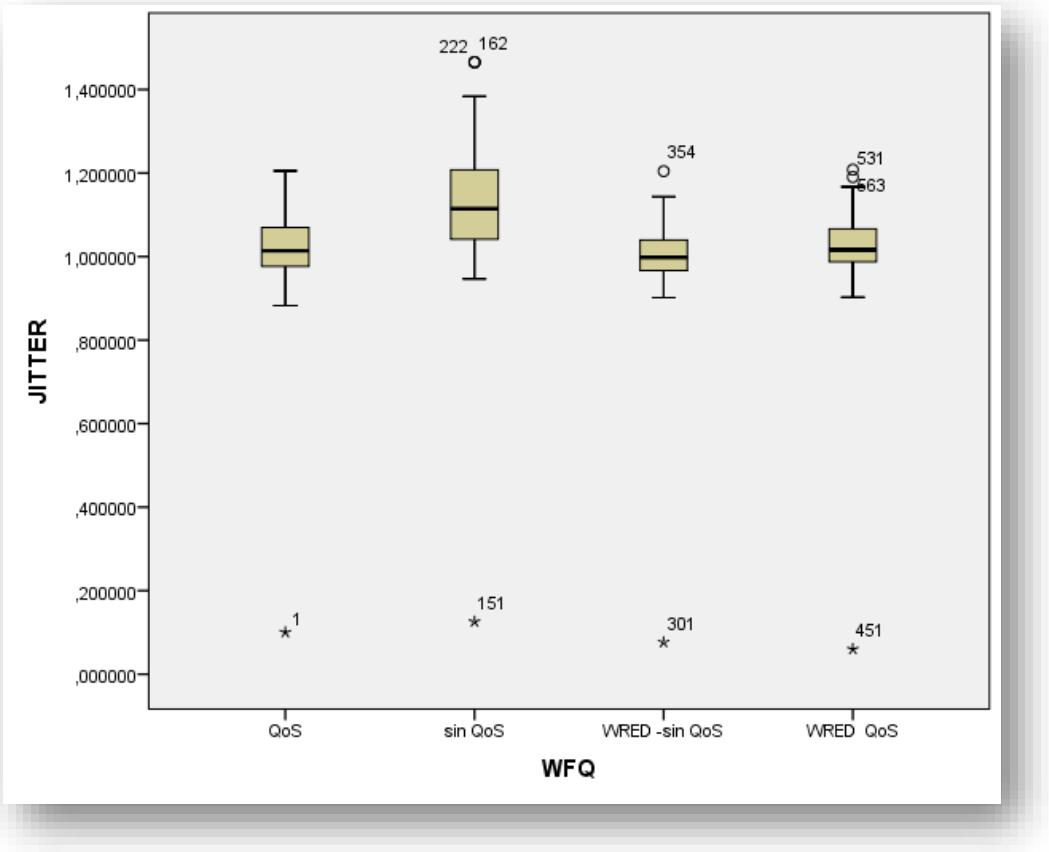


Figura 59: Diagrama de cajas del protocolo WFQ
Fuente: Autor

La tabla 15 muestra el análisis de varianza (ANOVA) se aplica a los valores de Jitter en distintas configuraciones del protocolo WFQ, utilizando diferentes valores de Jitter.

- Suma de cuadrados (7.659): Simboliza la variabilidad residual, que podría deberse a discrepancias individuales o elementos que no se tomaron en cuenta en el estudio.
- Media cuadrática (0.013): Muestra una variabilidad bastante reducida en los grupos, lo que sugiere que los valores de jitter en cada configuración son bastante uniformes.
- En esta situación, un F de 36.107 es considerablemente elevado, lo que indica diferencias de importancia estadística entre las configuraciones.
- El grado de significancia de 0.000 (< 0.05) corrobora que las variaciones detectadas entre las configuraciones poseen significación estadística. Esto significa que las configuraciones de WFQ ejercen un verdadero efecto en los valores de jitter.

Tabla 14. Análisis de la varianza con WFQ

ANOVA					
JITTER					
	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	1,392	3	,464	36,107	,000
Dentro de grupos	7,659	596	,013		
Total	9,051	599			

Fuente: Autor

La tabla 16 muestra el análisis de Tukey a los valores de jitter bajo distintas configuraciones del protocolo WFQ.

Esto indica que las configuraciones WRED - sin QoS, QoS y WRED con QoS no muestran diferencias notables en el jitter, aunque la configuración sin QoS es notablemente distinta a las demás.

El estudio muestra que la aplicación de QoS (ya sea con o sin WRED) tiene un efecto beneficioso en la disminución del jitter, dado que los medios se encuentran en el subgrupo con los valores más reducidos. Sin QoS, el jitter es superior y distinto, subrayando la relevancia de instaurar mecanismos como QoS para potenciar la calidad del servicio en redes.

Tabla 15. Análisis de Tukey aplicado a los valores de jitter

JITTER			
HSD Tukey[a]			
WFQ	N	Subconjunto para alfa = 0.05	
		1	2
WRED -sin QoS	150	1,00016793	
QoS	150	1,01954159	
WRED QoS	150	1,02088959	
sin QoS	150		1,12314406
Sig.		,389	1,000

Fuente: Autor

En la figura 60 muestra la media del jitter en redes se calcula utilizando el protocolo WFQ bajo diversas configuraciones vinculadas al QoS.
El protocolo WFQ más adecuado, fundamentado en los resultados, es WRED con QoS. A pesar de que la media de jitter (1,04) no es la más baja en absoluto, esta configuración consigue:

- Un balance entre la estabilidad (jitter reducido), la eficacia en la administración de la congestión (WRED) y la priorización del tráfico esencial (QoS).
- Un rendimiento seguro para redes con aplicaciones en tiempo real y tráfico variado.

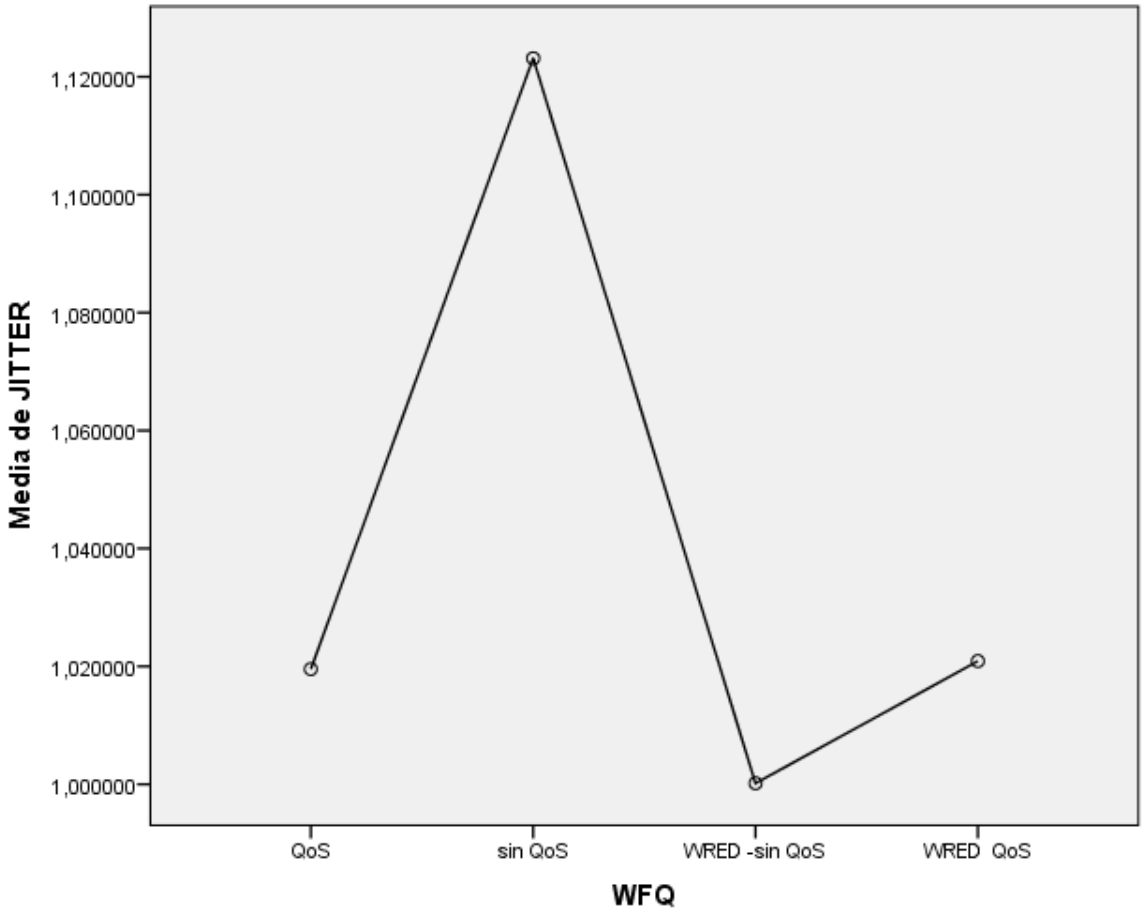


Figura 60: Gráfica de medias de jitter con el protocolo WFQ
Fuente: Autor

4.8.3 CBWFQ – JITTER

En la figura 61 muestra los hallazgos del "jitter" logrado mediante el uso del protocolo CBWFQ con QoS.

El histograma revela que la concentración más alta de datos se encuentra alrededor del promedio (1 ms), con una distribución altamente sesgada hacia valores más altos e inferiores.

Hay escasos valores extremos (outliers) que sean inferiores a 0,75 ms y superiores a 1,25 ms, lo que indica que el protocolo CBWFQ maneja el jitter de forma eficaz en la mayoría de las situaciones.

Bajo las circunstancias estudiadas, el protocolo CBWFQ evidencia su eficacia para reducir el jitter, ofreciendo un desempeño estable y predecible para flujos de datos que respaldan el QoS.

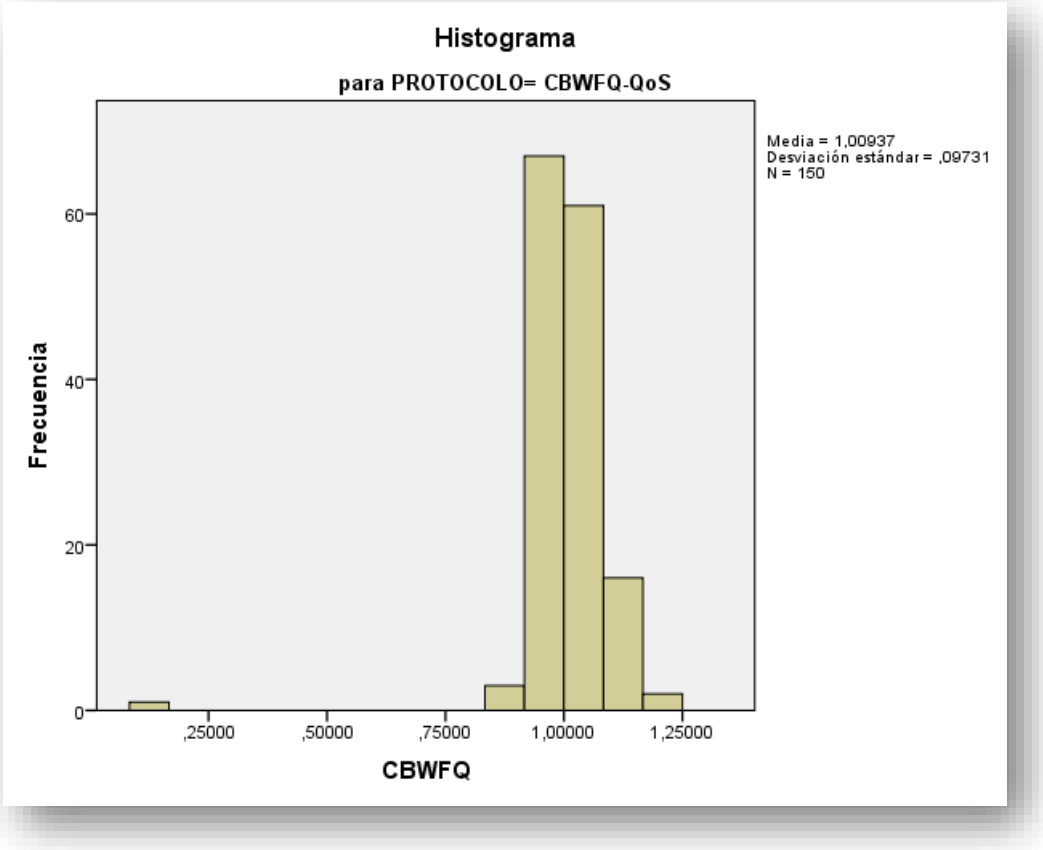


Figura 61: Histograma del Jitter – CBWFQ con QoS

Fuente: Autor

En la figura 62 presenta los resultados del jitter obtenidos al emplear el protocolo CBWFQ sin aplicar QoS:

La mayor parte de las mediciones de jitter se encuentran en un rango cercano al promedio, aproximadamente 1 ms, aunque con un pequeño incremento de dispersión en relación con el caso de QoS.

Hacia la izquierda se observan valores atípicos (outliers), en valores bajos, cerca de 0,2 ms o incluso menos, lo que sugiere inconsistencias en la gestión del jitter cuando no se implementa QoS.

El protocolo CBWFQ, sin la implementación de QoS, proporciona un rendimiento aceptable en cuanto a jitter, aunque presenta controles inferiores en comparación con su implementación con QoS. Esto podría generar problemas para aplicaciones

esenciales como videoconferencias o transmisión de voz, donde incluso variaciones mínimas pueden perjudicar la calidad.

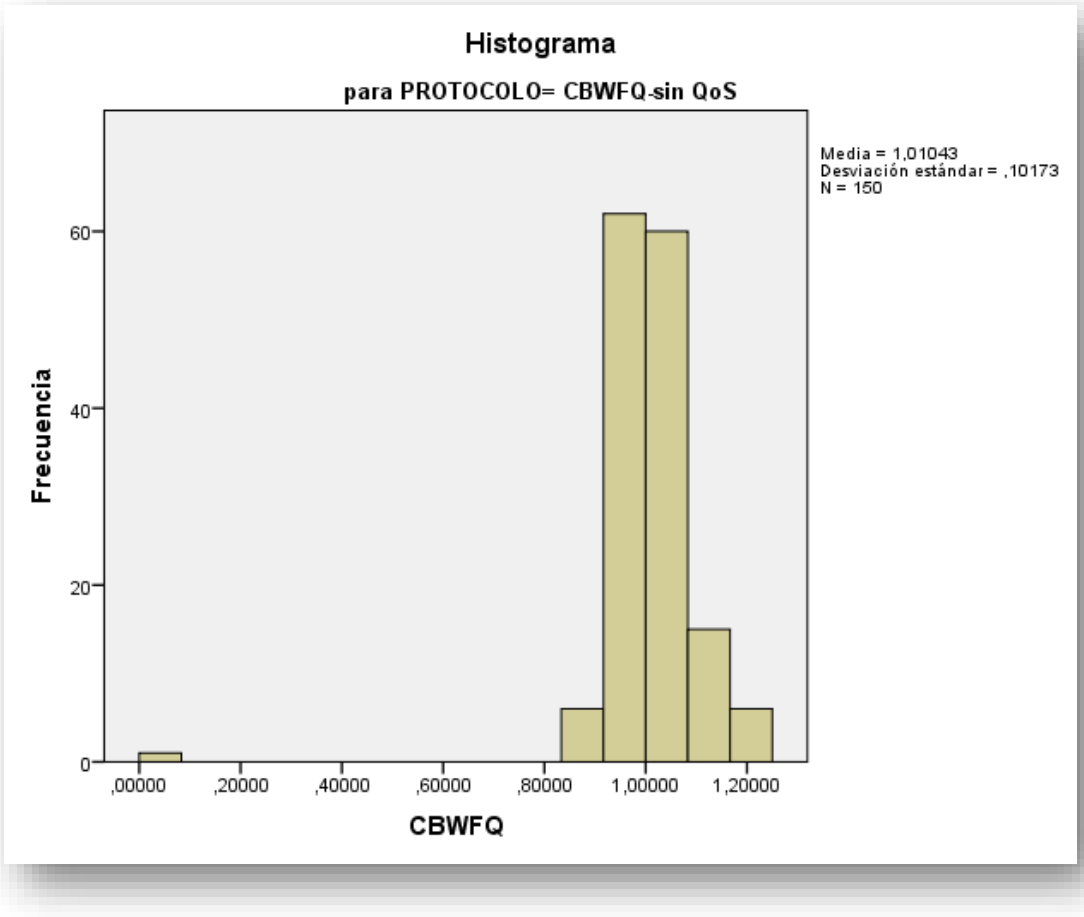


Figura 62: Histograma del Jitter – CBWFQ sin QoS
Fuente: Autor

En la imagen 63 muestra el cálculo del jitter con el protocolo CBWFQ con WRED sin QoS.

La mayor parte de los valores de jitter se ubican cerca del promedio (cerca de 1,00 a 1,05), con una frecuencia que llega a 60 observaciones en el rango más elevado. Esto evidencia que el desempeño bajo estas circunstancias es homogéneo en la mayoría del tiempo.

Existen algunos valores que sobrepasan el 1,25 hacia la derecha, a pesar de ser escasos, esto señala que a veces se producen variaciones más elevadas en el jitter.

La leve variabilidad detectada en los valores elevados podría generar un efecto notable en servicios que requieren latencia, como la voz sobre IP o las videoconferencias, especialmente si los valores máximos suceden de manera constante.

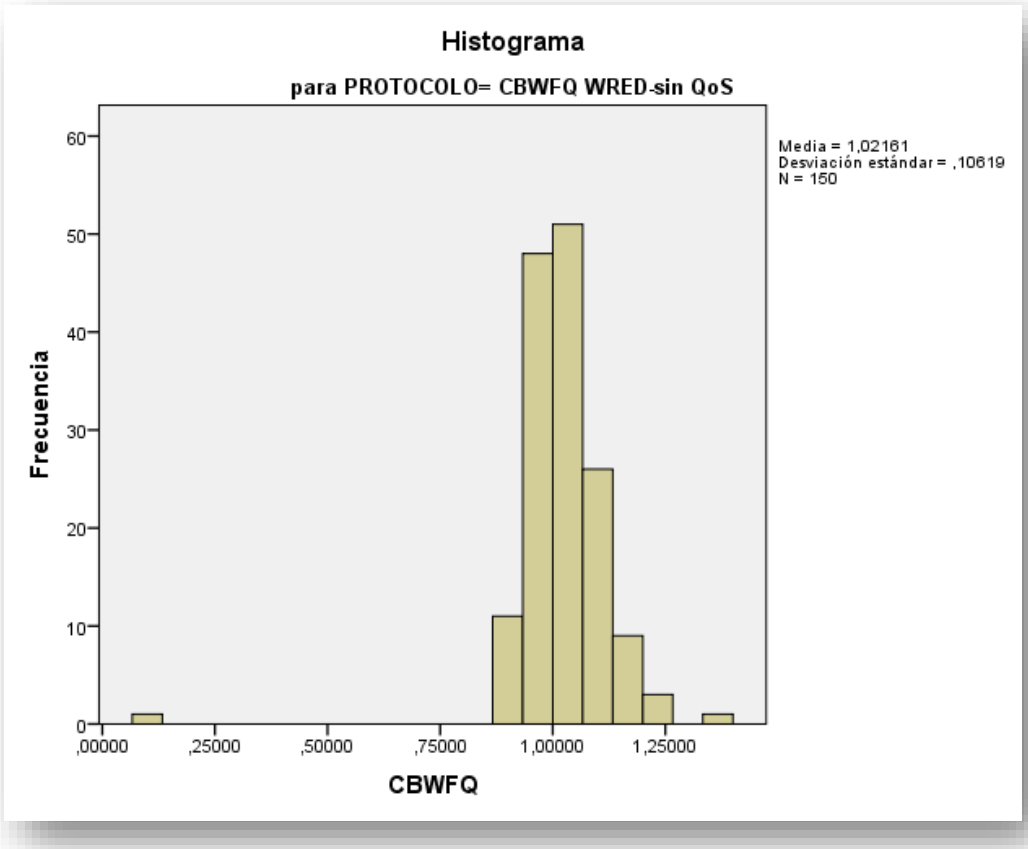


Figura 63: Histograma del Jitter – CBWFQ-WRED sin QoS
Fuente: Autor

En la figura 64 muestra los resultados logrados al determinar el jitter mediante el protocolo CBWFQ utilizando WRED y QoS.

El jitter medio es de 1,08286, lo que señala un ligero aumento en relación con el histograma del caso sin QoS (media de 1,02161). Este incremento está vinculado con calidad de servicio (QoS), que intentan dar prioridad a determinados tipos de tráfico.

El valor es de 0,15006, lo que evidencia una dispersión superior en comparación con el escenario sin QoS (que contaba con 0,10619). Esto sugiere que en esta situación los valores de jitter son más variables, posiblemente debido a la gestión de prioridades del protocolo QoS.

La aplicación de QoS en el protocolo CBWFQ con WRED consigue un jitter promedio bastante bajo y estable, este comportamiento es dado por QoS ya que reasigna los recursos de red para dar prioridad a determinados tipos de tráfico, lo que podría provocar variaciones en el desempeño de los flujos menos esenciales.

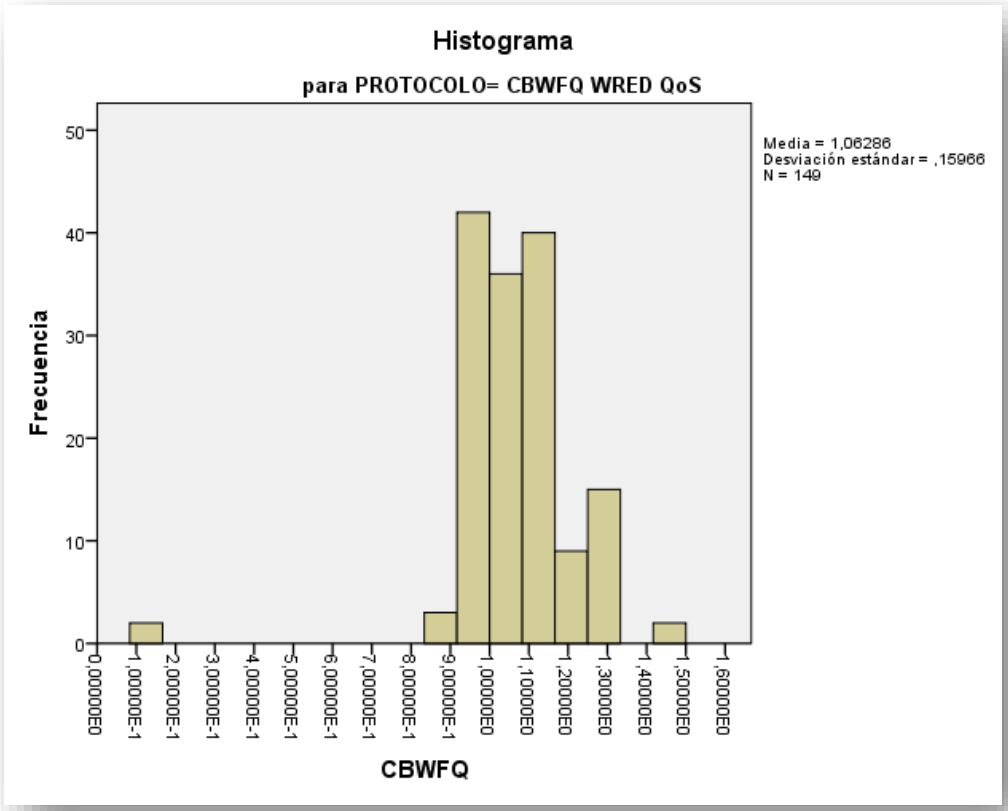


Figura 64: Histograma del Jitter – CBWFQ-WRED con QoS
Fuente: Autor

En la figura 65 muestra el diagrama de cajas que contrasta la comparación del jitter en distintas configuraciones del protocolo CBWFQ.

- En redes con tráfico sensible al jitter, es esencial establecer QoS para garantizar la correcta priorización.
- La mezcla de CBWFQ con QoS (sin WRED) resulta ser la alternativa más estable ya que proporciona el óptimo balance entre un jitter bajo, una variabilidad reducida y escasos valores atípicos. Es perfecto para usos esenciales como la VoIP o la videoconferencia.
- Si se emplea WRED, es necesario tener en cuenta la probabilidad de una mayor variabilidad y valores irregulares. Es más conveniente fusionarlo con QoS para atenuar sus impactos adversos en aplicaciones delicadas.

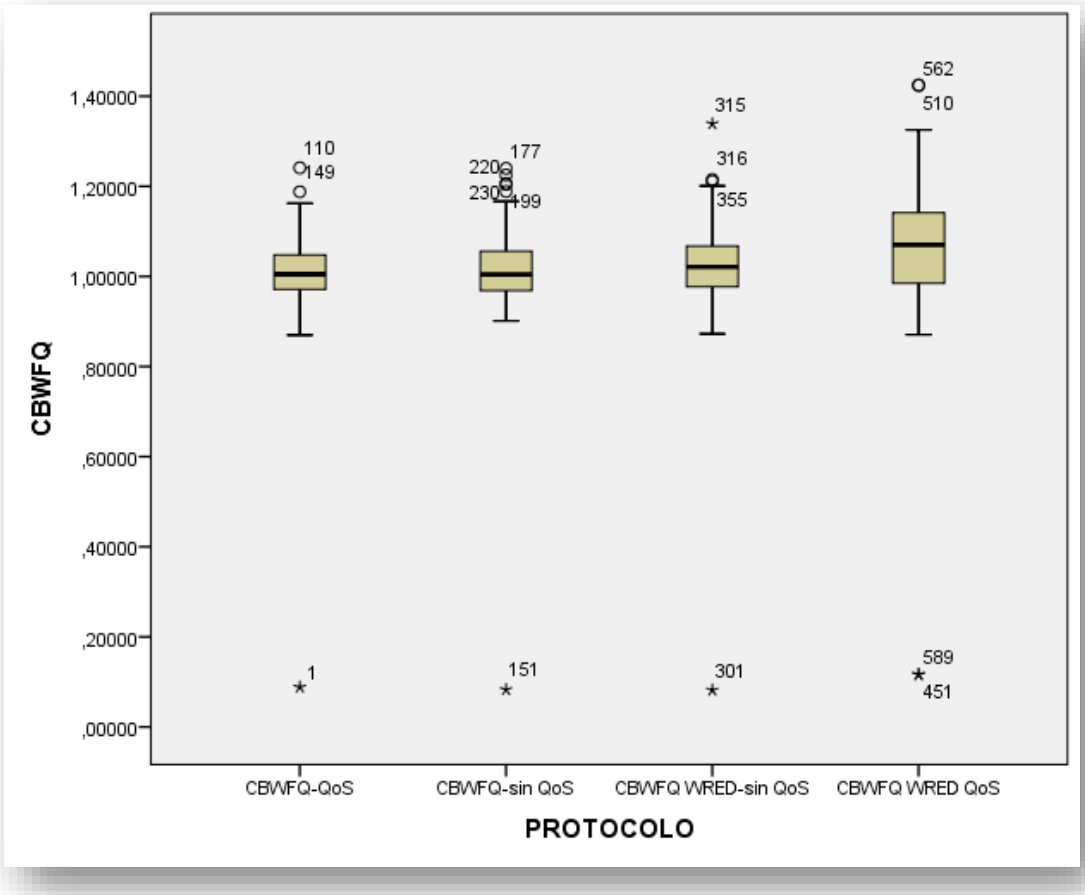


Figura 65: Diagrama de cajas de Jitter con el protocolo CBWFQ
Fuente: Autor

En la tabla 17 muestra el análisis de la varianza con el protocolo CBWFQ.
Considerando que sig=0.000, existen diferencias considerables entre las medias de los grupos evaluados. Esto significa que los grupos varían considerablemente de acuerdo con la variable estudiada en el protocolo CBWFQ.
La mayoría de la variación total (8.689) se deriva de las discrepancias internas en los grupos (8.406), sin embargo, las discrepancias entre los grupos (0.283) son suficientes para ser estadísticamente relevantes.
El estudio ANOVA señala que las discrepancias entre los grupos del protocolo CBWFQ no son fruto de la casualidad. Esto implica que los grupos ejercen un impacto considerable en la variable analizada.

Tabla 16. Análisis de varianza (ANOVA) con el protocolo CBWFQ

ANOVA					
CBWFQ					
	Suma de cuadrados	Gl	Media cuadrática	F	Sig.
Entre grupos	,283	3	,094	6,683	,000
Dentro de grupos	8,406	595	,014		
Total	8,689	598			

Fuente: Autor

En la tabla 18 muestra el análisis Tukey para contrastar las medias de los grupos evaluados con el protocolo CBWFQ.

El estudio Tukey revela que los protocolos CBWFQ-QoS y CBWFQ-sin QoS se encuentran en un subconjunto uniforme, en cambio, los protocolos CBWFQ WRED-sin QoS y CBWFQ WRED-QoS constituyen otro subconjunto. Esto señala que los protocolos que incluyen WRED y/o QoS producen valores diferentes a los protocolos fundamentales lo que influyen significativamente en los resultados del protocolo CBWFQ.

Tabla 17.Análisis de Tukey aplicado a los valores de jitter

CBWFQ			
HSD Tukey[a,b]			
PROTOCOLO	N	Subconjunto para alfa = 0.05	
		1	2
CBWFQ-QoS	150	1,0093680	
CBWFQ-sin QoS	150	1,0104264	
CBWFQ WRED-sin QoS	150	1,0216057	
CBWFQ WRED QoS	149		1,0628630
Sig.		,810	1,000

Fuente: Autor

En la figura 66 muestra los valores medios de jitter empleados con el protocolo CBWFQ en diferentes configuraciones.

La configuración CBWFQ-QoS es la más eficaz para reducir el jitter, con un valor medio de 1, es perfecto para usos sensibles al tiempo, debido a la priorización que proporciona QoS.

Si la red está saturada, la mezcla de CBWFQ WRED-QoS puede resultar beneficiosa, aunque se debe tener en cuenta el leve incremento del jitter (1,06). Esta configuración es más adecuada en redes mixtas que necesitan manejar colas y dar prioridad.

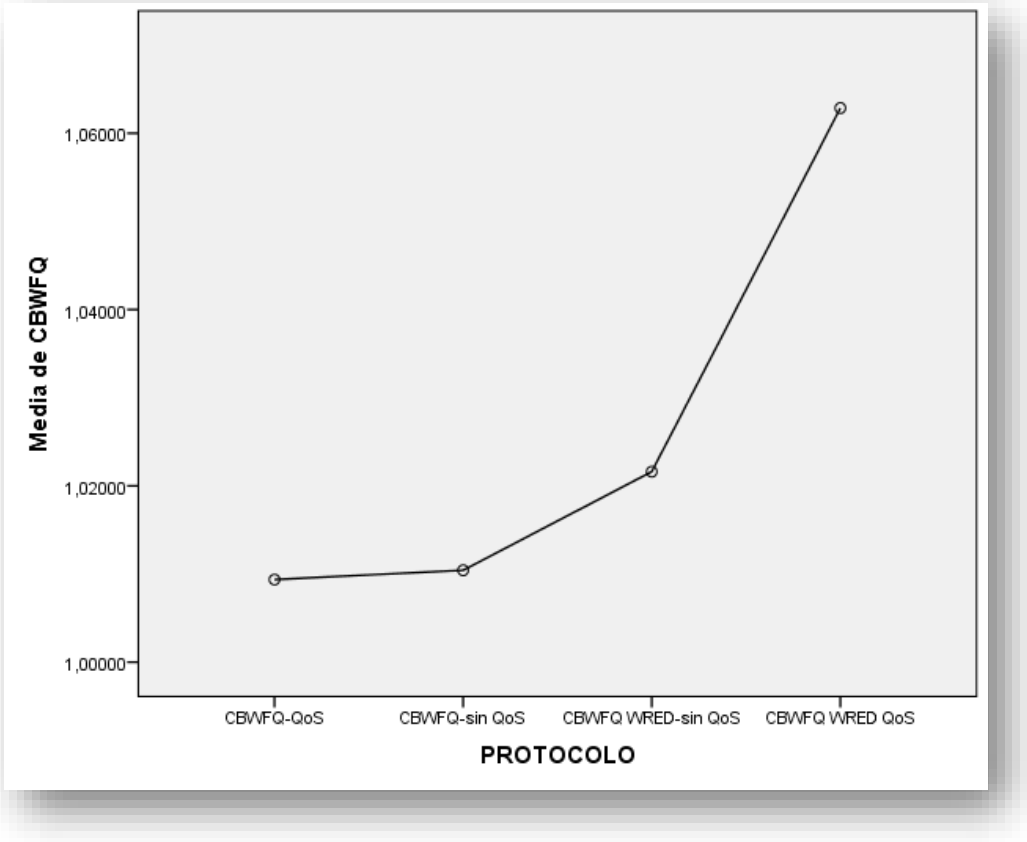


Figura 66: Grafica de medias del jitter con el protocolo CBWFQ
Fuente: Autor

4.8.4 FIFO-THROUGHPUT

En la figura 67 muestra el histograma con los resultados logrados mediante el protocolo Fifo con QoS.
La mayor parte de las evaluaciones de desempeño se enfocan en el intervalo de 9000 a 10,000.
Existen escasos valores extremos inferiores a 8000, lo que indica que el protocolo QoS es consistente y raramente genera valores de bajo nivel.
Este protocolo usualmente no da prioridad al tráfico, lo que podría resultar un desempeño más inconstante en situaciones de carga.

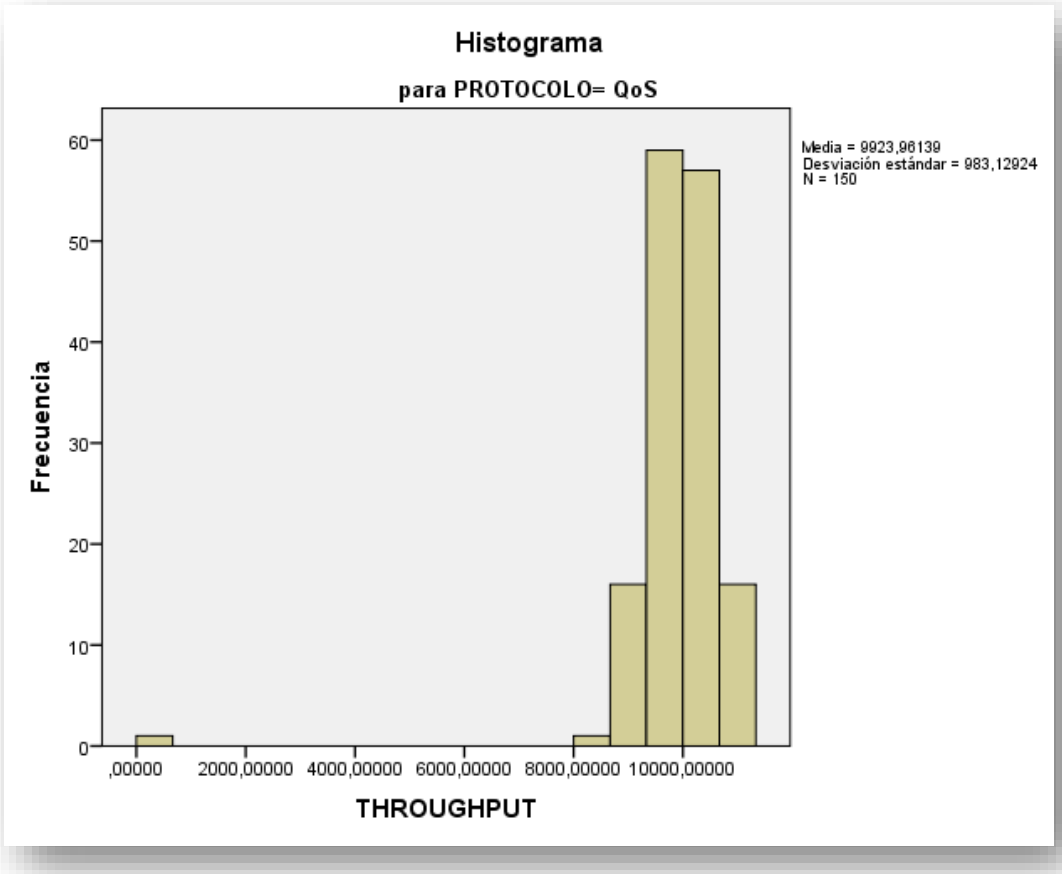


Figura 67: Histograma del Throughput con FIFO y QoS
Fuente: Autor

La figura 68 presenta un histograma que ilustra los resultados del rendimiento empleando un protocolo FIFO sin calidad de servicio (QoS).
El rendimiento medio es bastante bajo, lo que podría estar vinculado con la falta de un control de calidad de servicio (sin QoS).
La elevada desviación estándar indica que los datos poseen una considerable variabilidad, lo que significa que hay diferencias notables entre los valores más bajos y los más elevados de rendimiento.
El protocolo sin QoS parece proporcionar un desempeño irregular, con la mayoría de las mediciones en intervalos reducidos. Esto podría ser resultado de la ausencia de herramientas para ordenar o administrar el tráfico de red, lo que conduce a una distribución desequilibrada del throughput.

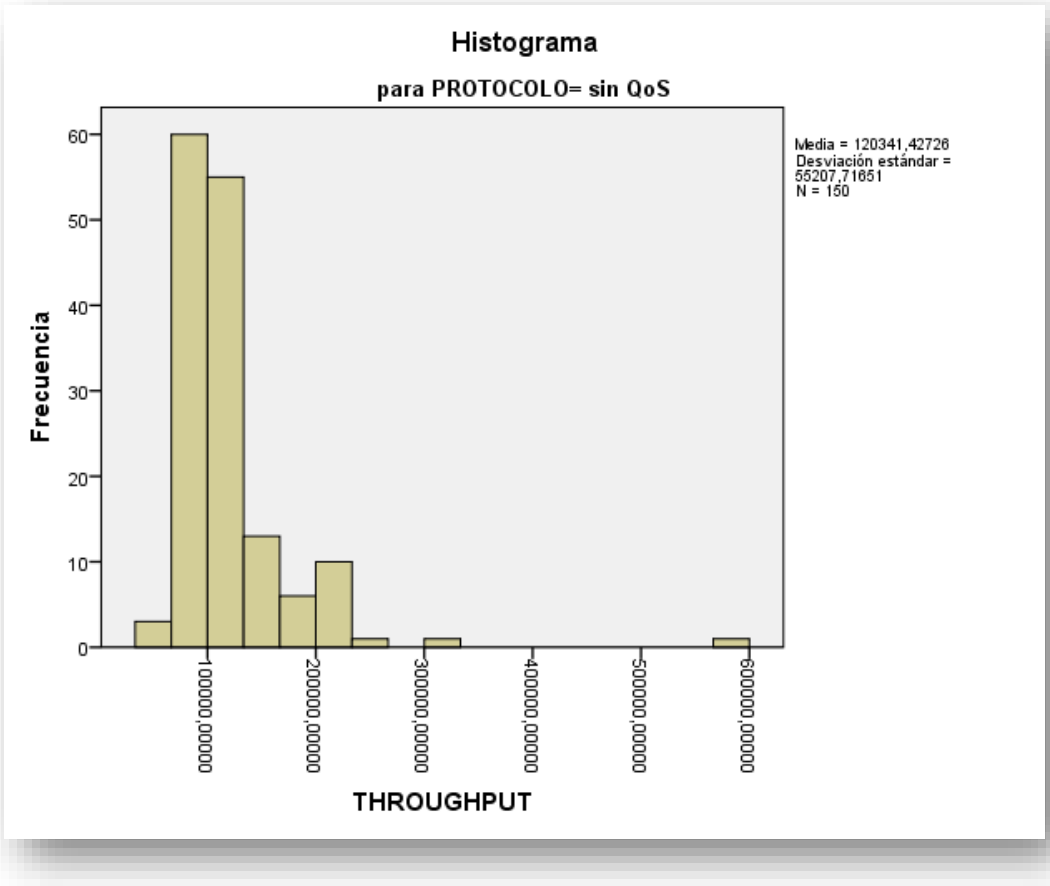


Figura 68: Histograma del Throughput con FIFO sin QoS
Fuente: Autor

La figura 69 muestra histograma muestra los rendimientos obtenidos mediante el uso del protocolo FIFO con WRED sin calidad de servicio (QoS).
La media de rendimiento es bastante baja, lo que indica un rendimiento restringido del protocolo en estas circunstancias.
La elevada desviación estándar señala una amplia variabilidad en los valores, lo que evidencia irregularidades en el desempeño.
La aplicación de FIFO con WRED sin QoS incrementa un poco el rendimiento medio en relación a FIFO sin WRED. No obstante, la elevada variabilidad señala que el protocolo no cuenta con mecanismos consistentes para administrar eficazmente el tráfico de red.

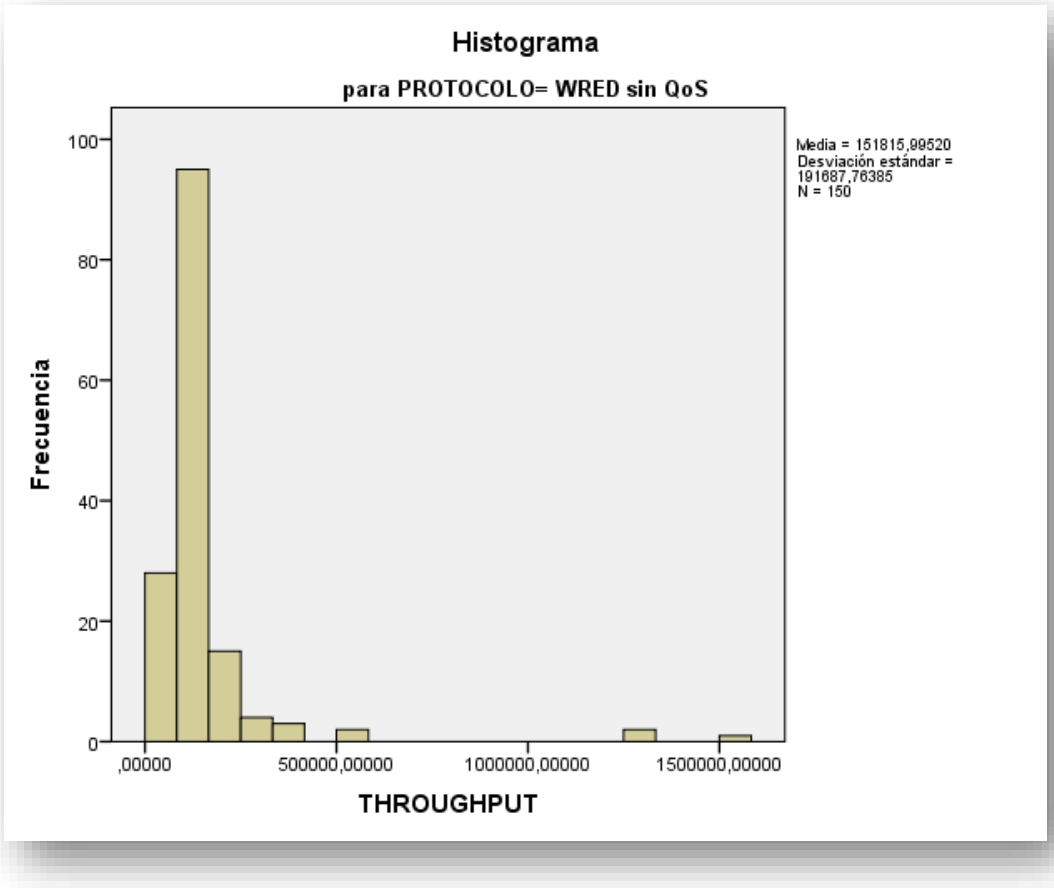


Figura 69: Histograma del Throughput con FIFO - WRED sin QoS
Fuente: Autor

La figura 70 muestra los resultados del rendimiento al emplear el protocolo FIFO con WRED.

El alto promedio señala que el rendimiento medio con WRED y QoS llega a niveles notablemente más elevados en comparación con las configuraciones sin QoS.

La reducida dispersión relativa indica que el protocolo conserva una consistencia superior, minimizando las variaciones extremas.

La implementación de QoS, en conjunto con FIFO y WRED, incrementa notablemente la calidad del servicio al asegurar un rendimiento superior y una reducción en la variabilidad.

Este protocolo es perfecto para situaciones que demandan un rendimiento uniforme y una eficaz priorización de paquetes en redes saturadas.

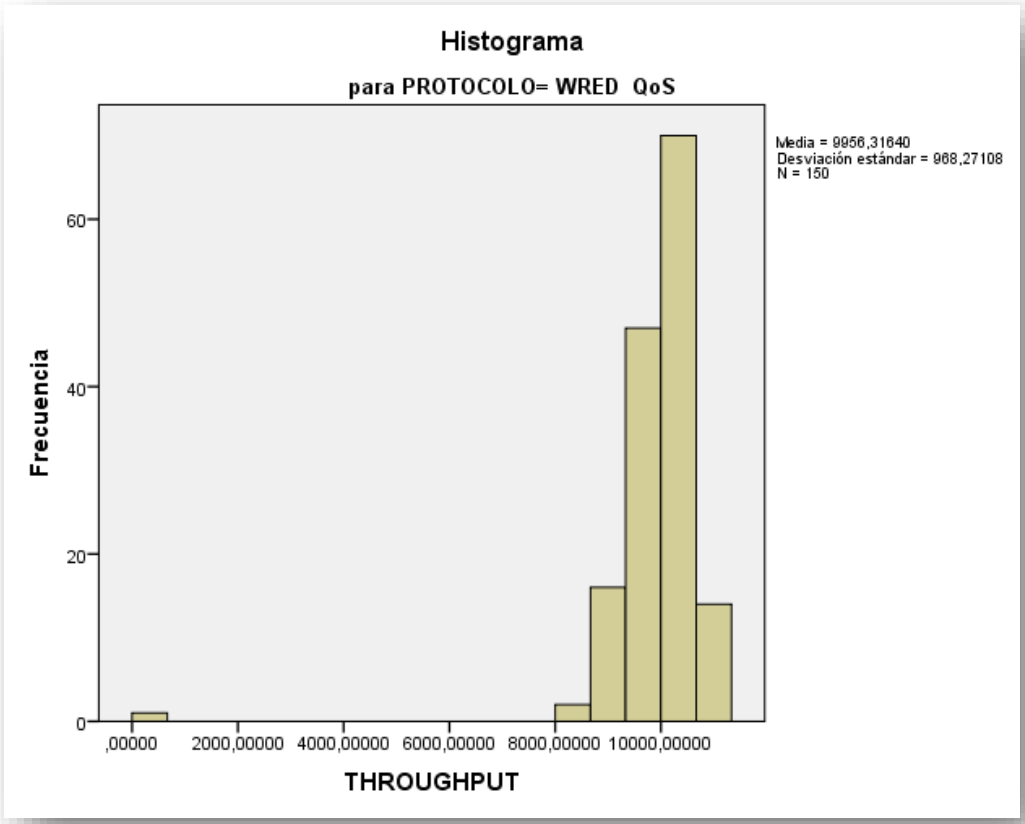


Figura 70: Histograma del Throughput con FIFO - WRED con QoS
Fuente: Autor

La figura 71 muestra un esquema de cajas que contrasta el throughput bajo diversas configuraciones del protocolo FIFO.

- QoS: Posee un throughput sumamente reducido (cerca de cero), esta configuración disminuye de manera significativa el desempeño.
- Sin QoS: A pesar de que presenta una mediana un poco más alta que la del QoS, el throughput continúa siendo bajo, esto señala una mayor variabilidad, pero todavía un rendimiento deficiente.
- Wred sin QoS: Existen valores extremadamente atípicos (hasta 448), lo que señala que esta configuración posibilita lograr picos de rendimiento más elevados, aunque también con una cierta variabilidad.
- Wred con QoS; Los números excepcionales (como 547 y 478) corroboran que esta mezcla mejora tanto el desempeño como la calidad del servicio.

El estudio indica que la utilización de WRED con QoS activado ofrece el rendimiento superior en cuanto al throughput. En cambio, la implementación de FIFO básico con QoS activa presenta el rendimiento más deficiente.

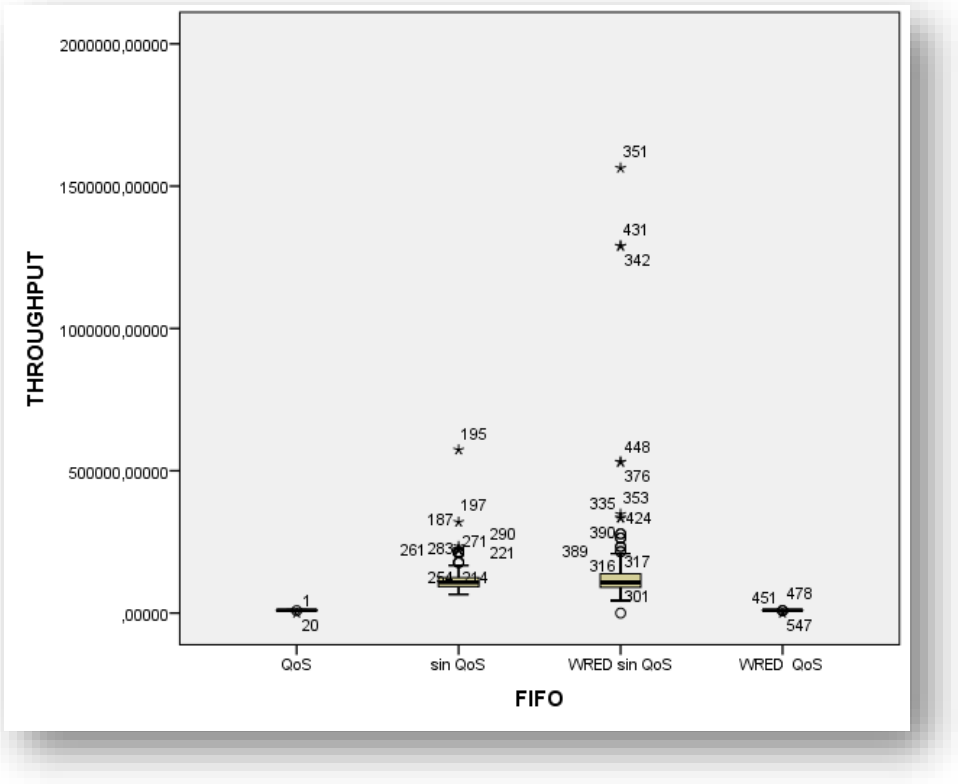


Figura 71: Diagrama de cajas del Throughput con el protocolo FIFO
Fuente: Autor

La tabla 19 muestra el análisis descriptivo del throughput en el protocolo FIFO.
La elevada variabilidad entre los grupos (suma de cuadrados y el valor de F) las configuraciones del protocolo FIFO tienen un impacto considerable en el throughput, probablemente, la configuración de WRED y QoS ofrece el rendimiento más alto.
Es necesario dar prioridad a aquellas que mejoren el rendimiento, como WRED QoS, con el fin de optimizar el throughput en contextos donde la gestión eficaz del tráfico es esencial.

Tabla 18.Análisis ANOVA aplicado al throughput en el protocolo FIFO

ANOVA					
THROUGHPUT					
	Suma de cuadrados	Gl	Media cuadrática	F	Sig.
Entre grupos	2460939624943,287	3	820313208314,429	82,456	,000
Dentro de grupos	5929305235055,072	596	9948498716,535		
Total	8390244859998,359	599			

Fuente: Autor

En la figura 72 muestra el rendimiento medio basado en diversas configuraciones del protocolo FIFO bajo diferentes contextos de calidad de servicio.
Se alcanza el máximo rendimiento con WRED sin QoS, en el que el sistema da prioridad al rendimiento sin imponer limitaciones de calidad.
La activación de QoS (ya sea con o sin WRED) impacta de manera negativa en el desempeño, dado que incorpora mecanismos extra que otorgan prioridad a la calidad del servicio sobre los costos del rendimiento global.

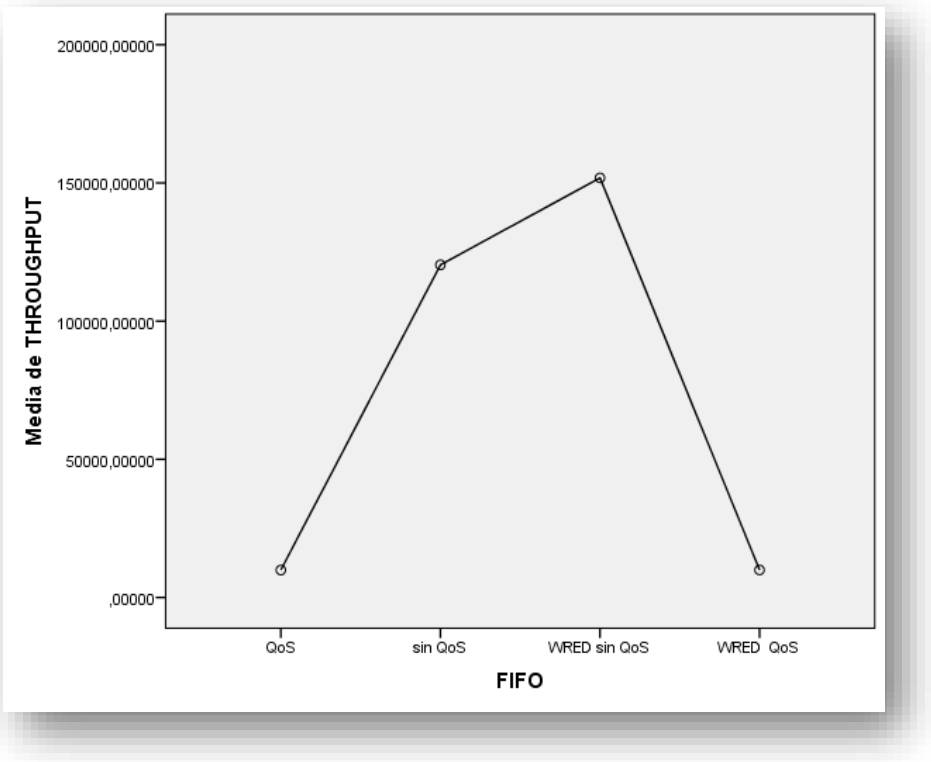


Figura 72: Gráfica de medias del throughput con el protocolo FIFO
Fuente: Autor

4.8.5 WFQ – THROUGHPUT

En la figura 73 muestra el cálculo del throughput con el protocolo WFQ con QoS:
Las barras más elevadas (frecuencia superior a 60) se relacionan con el rango de rendimiento más alto, lo que señala que este nivel se logra de manera constante en la mayoría de las pruebas.
Se observan frecuencias más bajas (casi nulas) lo que sugiere que el sistema pocas veces experimenta un rendimiento notablemente disminuido.

La aplicación de WFQ bajo QoS demuestra ser eficaz para dar prioridad al tráfico y mantener un alto rendimiento. La acumulación de valores elevados evidencia que la distribución de recursos es eficaz y que se reducen los obstáculos en el flujo de datos.

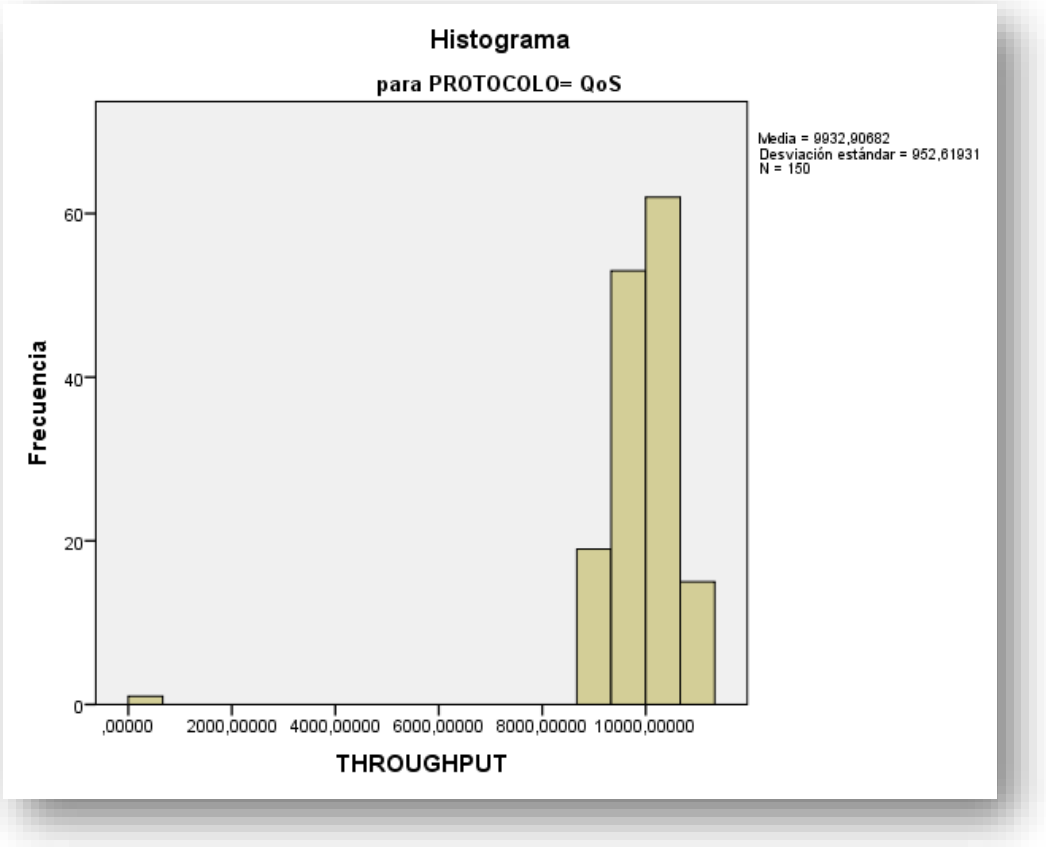


Figura 73: Histograma del Throughput con WFQ con QoS
Fuente: Autor

La figura 74 muestra el histograma del Throughput con el protocolo WFQ sin QoS.
El valor más elevado (frecuencia mayor a 80) se relaciona con los valores que superan las unidades de rendimiento, lo que constituye la mayoría de las mediciones.
Hay valores que superan esta concentración (hacia niveles de rendimiento superiores), aunque con frecuencias inferiores. Este fenómeno podría señalar incrementos ocasionales en el rendimiento, pero no uniformes.
La falta de QoS en este protocolo da un rendimiento alto, genera más inestabilidad y variabilidad en los resultados.
La existencia de valores altos pero irregulares puede indicar circunstancias en las que el tráfico no está adecuadamente regulado y algunos flujos controlan los recursos, dejando otros en una situación de desventaja.

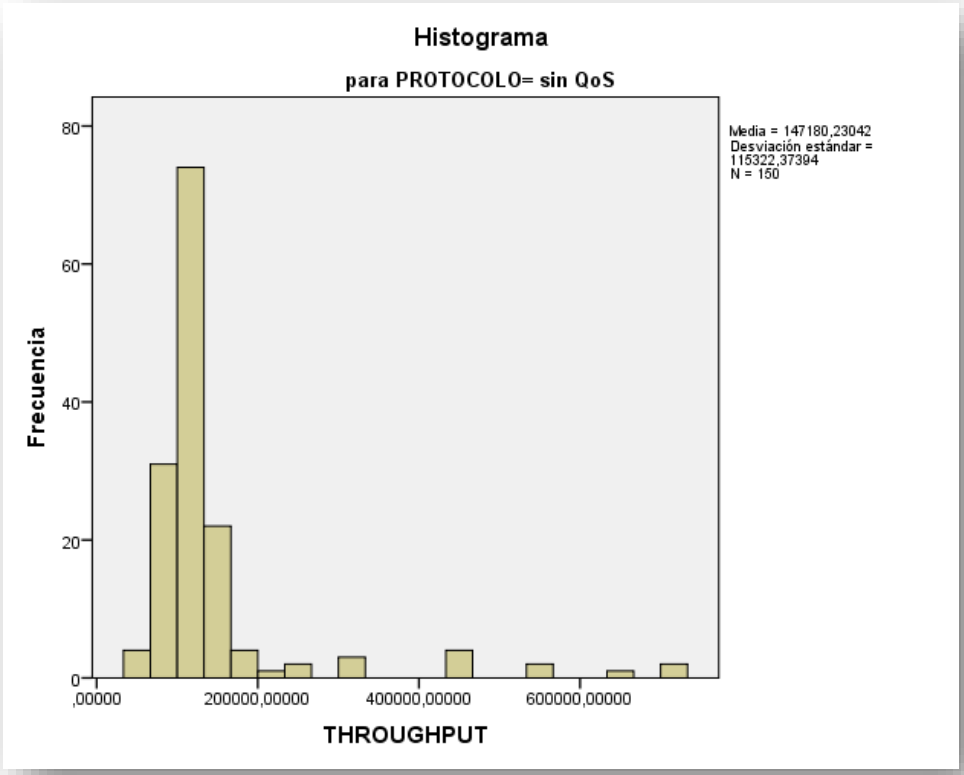


Figura 74: Histograma del Throughput con WFQ sin QoS
Fuente: Autor

La figura 75 muestra los resultados obtenidos mediante el uso del protocolo WFQ con WRED sin QoS:

La media del rendimiento es de 10104.23728 unidades, lo que indica un desempeño alto y constante, parecido al comportamiento del WFQ con QoS activado.

Se trata de 945.78411 unidades, lo que señala una dispersión reducida en los datos. Esto indica que el desempeño es bastante estable.

Aunque no se emplea QoS, el desempeño es bastante estable y se aproxima a la configuración con QoS, aunque probablemente sin la habilidad para otorgar prioridad al tráfico crítico.

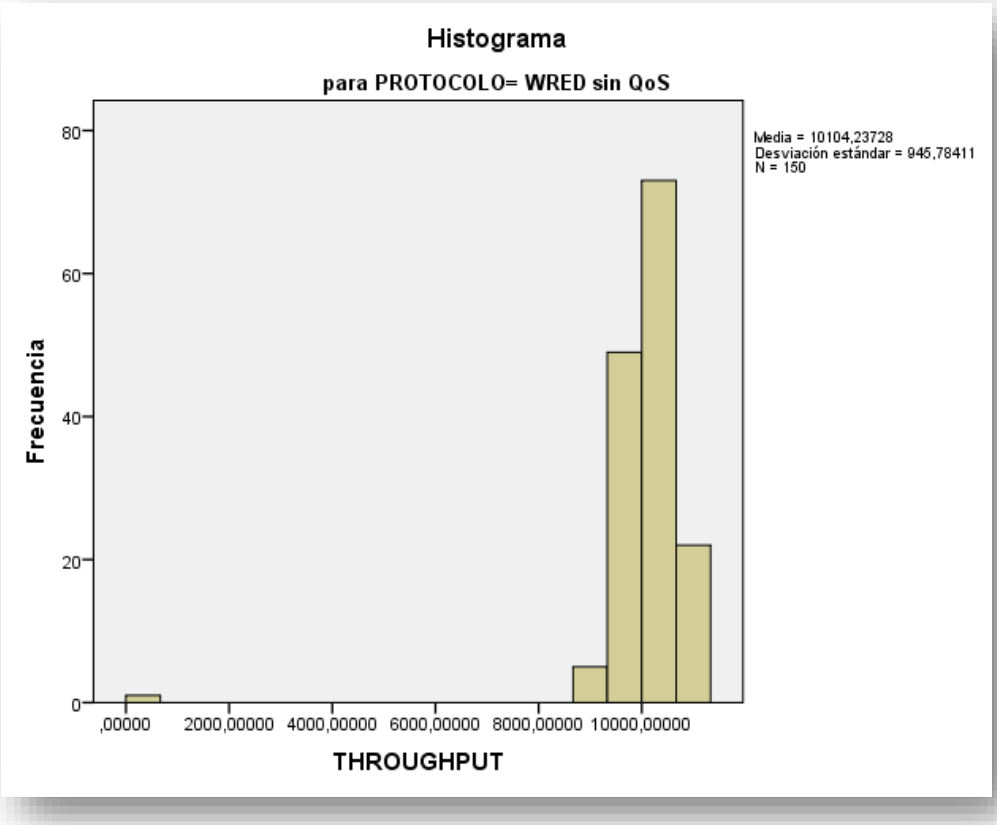


Figura 75: Histograma del Throughput con WFQ-WRED sin QoS
Fuente: Autor

En la figura 76 muestra histograma de los resultados del rendimiento utilizando el protocolo WFQ con WRED y QoS:

La media de rendimiento es de 9031.10358 unidades, lo que evidencia un buen rendimiento global del sistema.

La desviación estándar es de 965.06236 unidades, lo que señala una variabilidad reducida y, en consecuencia, un desempeño uniforme.

La configuración WFQ + WRED + QoS es perfecta para redes que requieren estabilidad, uniformidad y priorización del tráfico.

Este método balancea eficazmente el desempeño y la calidad del servicio, previniendo atascos y garantizando una experiencia de confianza.

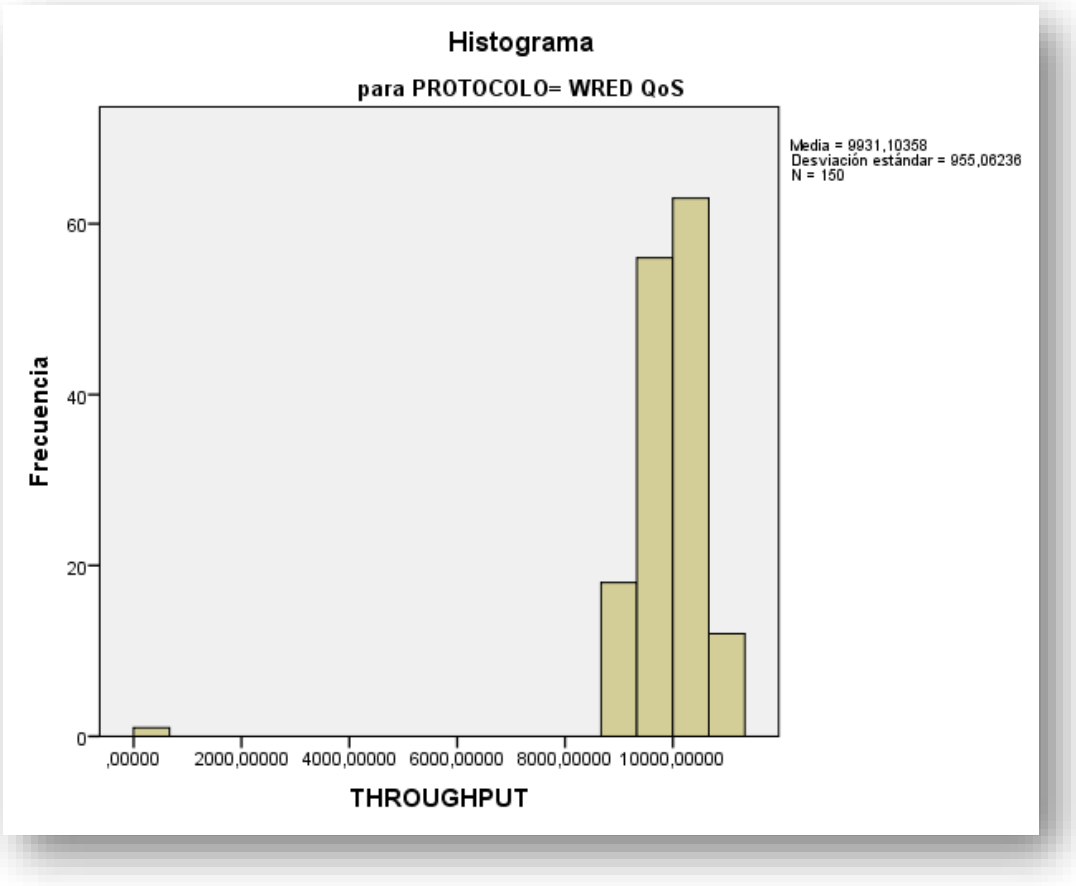


Figura 76: Histograma del Throughput con WFQ-WRED y QoS
Fuente: Autor

La figura 77 muestra los resultados del rendimiento en diversos escenarios vinculados con el protocolo WFQ:
Los escenarios sin QoS suelen tener un rendimiento superior, aunque con fluctuaciones considerables.
Los casos con QoS o combinaciones con WRED exhiben un rendimiento medio, sin embargo, presentan valores irregulares que podrían sugerir periodos de mayor eficiencia bajo determinadas circunstancias.

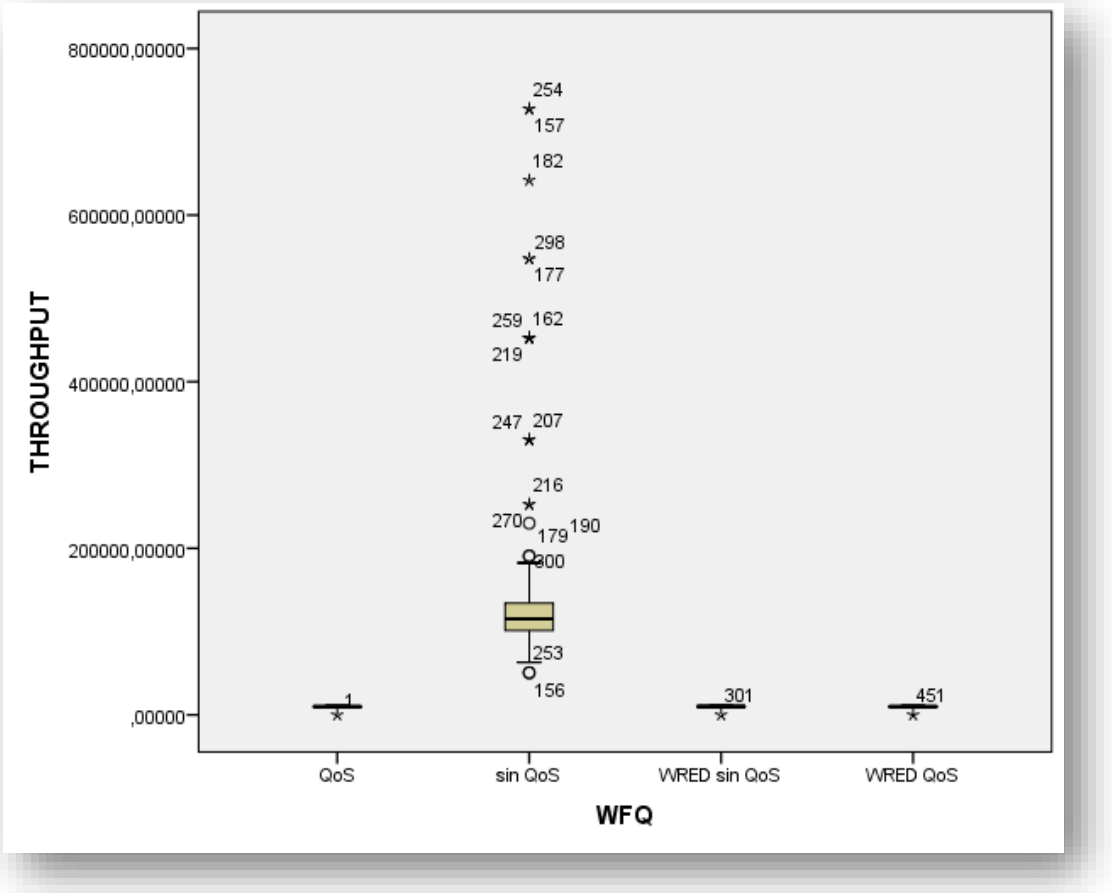


Figura 77: Diagrama de cajas del protocolo WFQ
Fuente: Autor

La tabla 20 muestra el estudio de la tabla ANOVA que facilita la valoración de las diferencias en el throughput entre los grupos del protocolo WFQ.

El coeficiente de significancia ($p < 0.05$) corrobora que hay variaciones estadísticamente relevantes en el throughput entre los escenarios analizados (QoS, sin QoS, WRED sin QoS, WRED QoS).

El valor del estadístico F (212.239) es considerablemente elevado, lo que indica que las discrepancias entre los grupos ejercen un efecto considerablemente más significativo que las variaciones internas de cada grupo. Esto apoya la conclusión de que los diversos escenarios influyen de manera significativa en el throughput.

De acuerdo con los hallazgos, resulta evidente que el rendimiento del protocolo WFQ varia considerablemente entre los escenarios analizados.

Tabla 19. Anova del throughput con el protocolo WFQ

ANOVA					
THROUGHPUT					
	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	2117401420567,383	3	705800473522,461	212,239	,000
Dentro de grupos	1981992646043,132	596	3325491016,851		
Total	4099394066610,515	599			

Fuente: Autor

En la tabla 21 muestra las diferencias del throughput para los escenarios del protocolo WFQ integra el análisis ANOVA y facilita la identificación de qué grupos muestran diferencias estadísticamente relevantes en el desempeño.

- Subgrupo 1 (WRED QoS, WRED sin QoS):
  Las medias de tráfico son bastante parecidas y bajas
  No existen diferencias notables entre estos tres contextos.
  Esto indica que ni la aplicación de WRED ni la aplicación de QoS consiguen un incremento significativo en el desempeño del protocolo.
- Subgrupo 2 (sin QoS)
  Este escenario se diferencia totalmente de los otros tres, lo que señala que sin QoS ofrece un rendimiento considerablemente más elevado.
- El coeficiente de significancia es 1.000 para los subconjuntos uniformes, lo que señala que las medias de cada subconjunto no difieren de manera significativa.

Tabla 20.Análisis Tukey del throughput con el protocolo WFQ

HSD Tukey[a]			
WFQ	N	Subconjunto para alfa = 0.05	
		1	2
WRED QoS	150	9931,1035806	
QoS	150	9932,9068223	
WRED si QoS	150	10104,2372841	
sin QoS	150		147180,2304225
Sig.		1,000	1,000

Fuente: Autor

En la figura 78 muestra el estudio del throughput medio relacionado con diversas configuraciones de calidad de servicio (QoS) empleando el protocolo CBWFQ.
El mayor balance entre el rendimiento y estabilidad: Es aconsejable "QoS activado" si la red gestiona aplicaciones relacionadas con la calidad del servicio, como videollamadas o VoIP, dado que disminuye la latencia y otorga prioridad al tráfico esencial.
Al aplicar WRED resulta beneficioso en redes susceptibles a congestión grave, no resulta apropiado si el throughput es un indicador crucial. Su influencia en el desempeño bruto es notable, incluso cuando se fusiona con QoS.

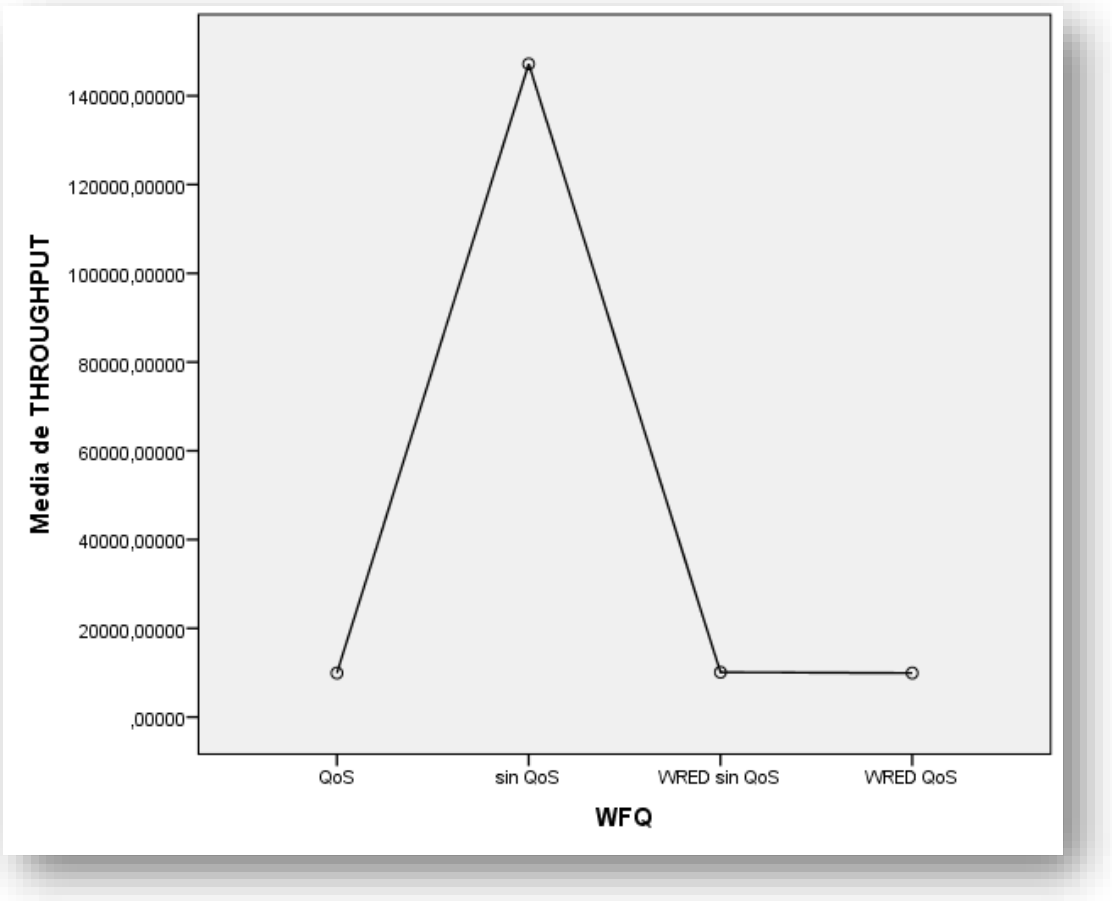


Figura 78: Gráfica de medias del throughput con el protocolo WFQ
Fuente: Autor

4.8.6 CBWFQ – THROUGHPUT

La figura 79 muestra un histograma que mide el rendimiento a través del protocolo CBWFQ scon QoS.
La elevada desviación estándar (7,038) frente a la media (10,683) señala que los índices de rendimiento se encuentran dispersos en un espectro extenso. Esto podría derivarse de

variaciones en la carga de tráfico, la priorización del QoS, o la conducta particular del protocolo CBWFQ en distintas clases de tráfico.

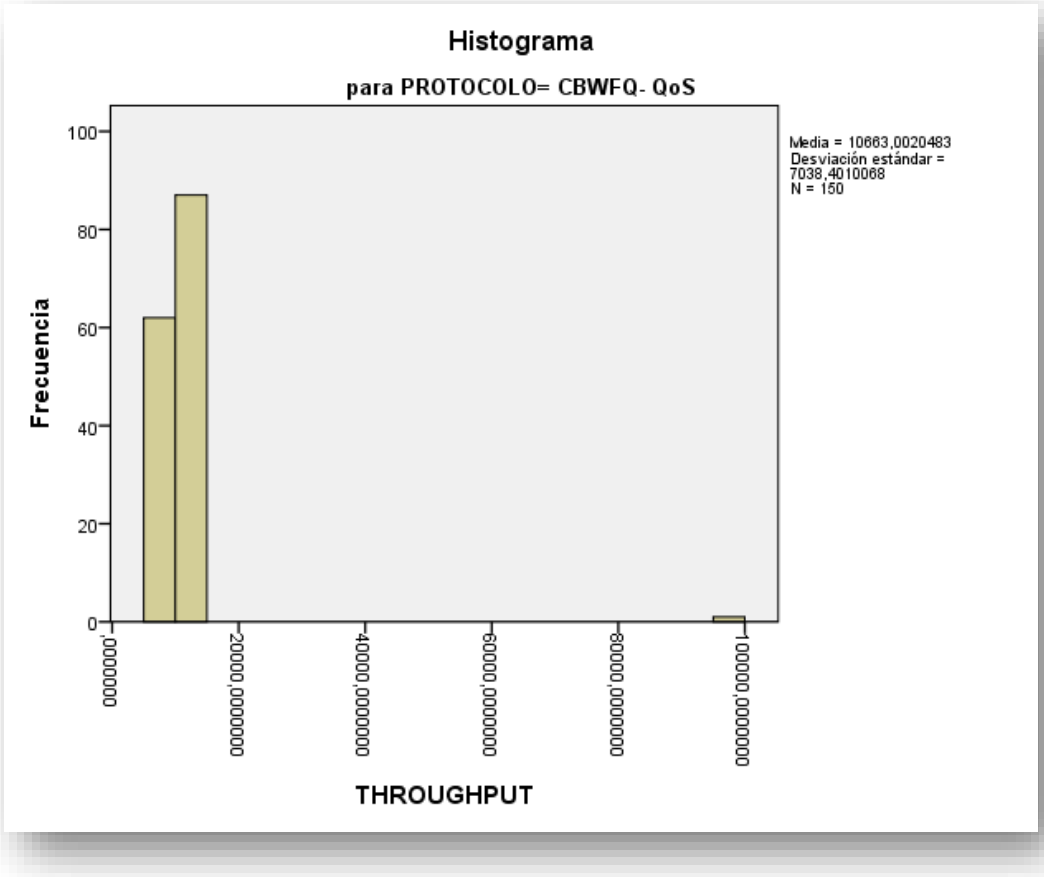


Figura 79: Histograma del Throughput con el protocolo CBWFQ con QoS
Fuente: Autor

En la figura 80 muestra un histograma que evalúa el rendimiento con el protocolo CBWFQ sin QoS.

El protocolo CBWFQ sin QoS ofrece un desempeño más uniforme y predecible, aunque sacrifica la priorización del tráfico. No obstante, en redes de alta demanda o tráfico crítico, la ausencia de QoS puede provocar problemas de congestión y deterioro del desempeño de aplicaciones delicadas.

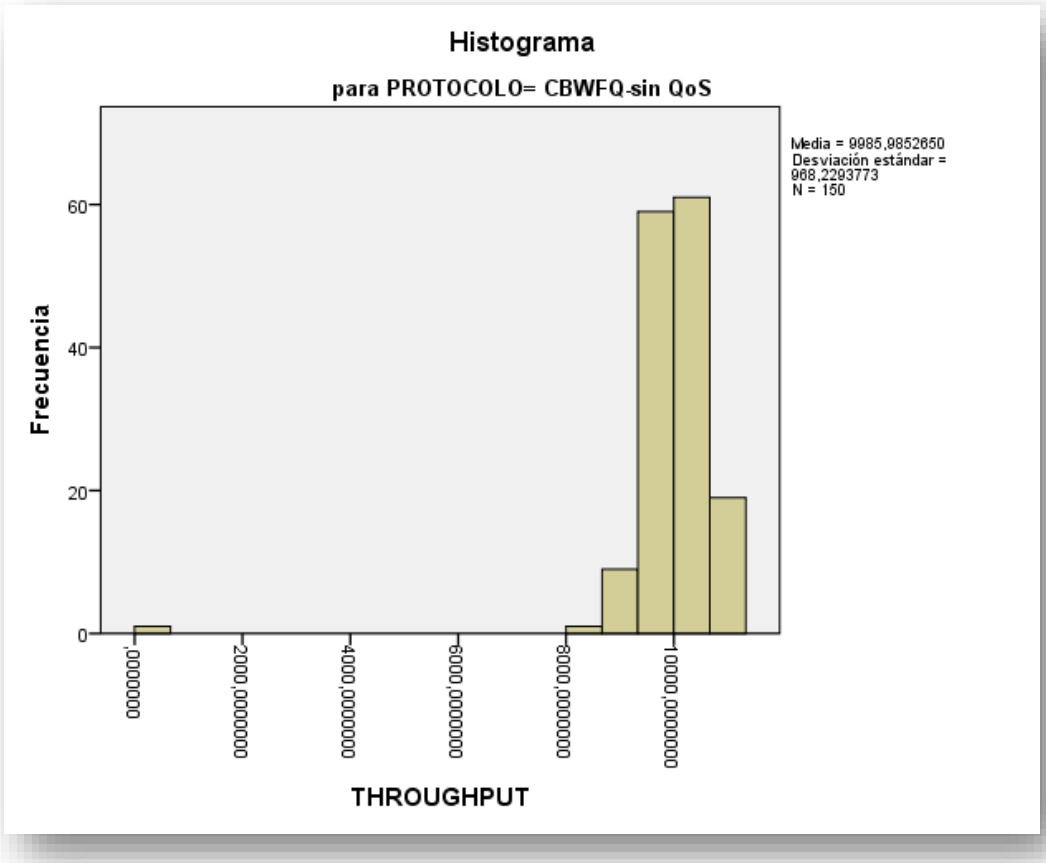


Figura 80: Histograma del Throughput con el protocolo CBWFQ sin QoS
Fuente: Autor

La figura 81 muestra el histograma con los resultados del rendimiento utilizando el protocolo CBWFQ con WRED sin QoS.
La desviación estándar reducida muestra una conducta estable, lo que podría deberse a la puesta en marcha de WRED, que controla la congestión.
Es posible que el rendimiento reduzca cargas altas debido al desecho de paquetes, particularmente en aplicaciones susceptibles a pérdidas.
La incorporación de WRED optimiza el manejo de la congestión, pero conlleva gastos reducidos en el rendimiento.

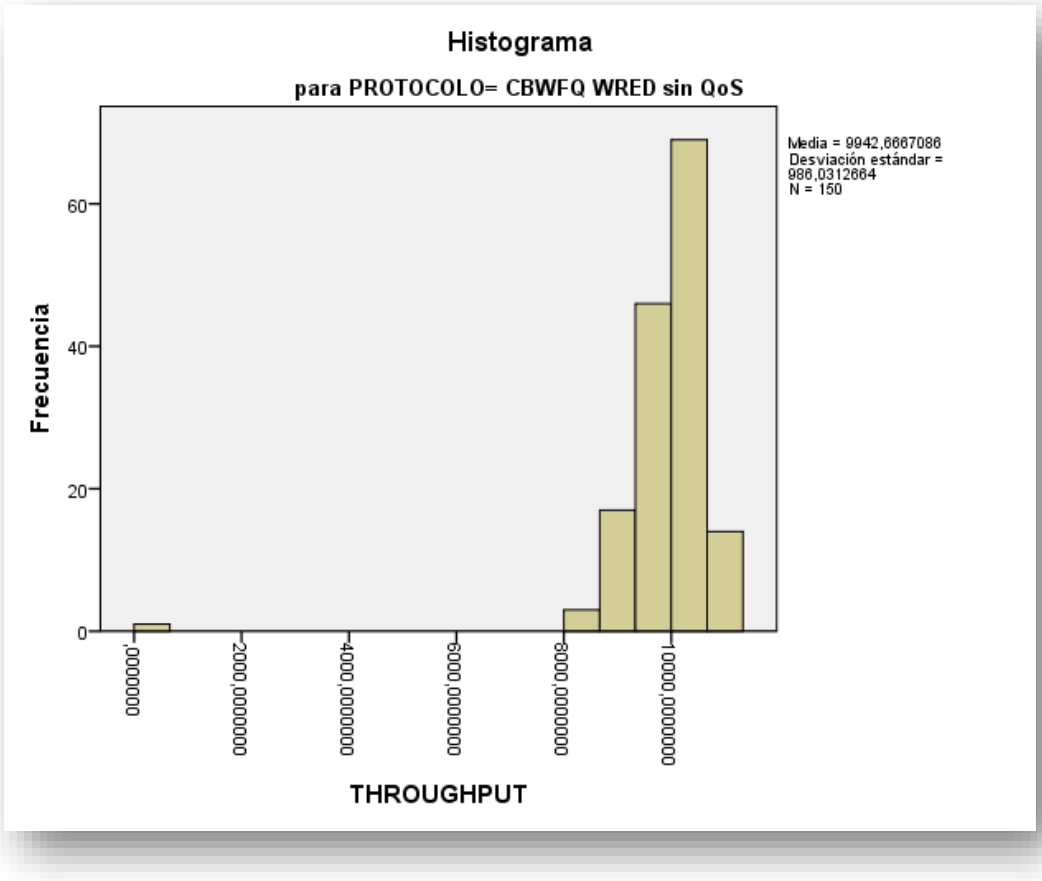


Figura 80: Histograma del Throughput con el protocolo CBWFQ-WRED sin QoS
Fuente: Autor

La figura 81 muestra el análisis del rendimiento utilizando el protocolo CBWFQ con WRED y QoS.

- Sin QoS, el throughput muestra una mayor variabilidad debido a la ausencia de priorización, lo que podría provocar caídas considerables para el tráfico esencial.
- Con QoS habilitado, los resultados del throughput se mantienen más constantes y se ajustan a las demandas de las aplicaciones esenciales.
- CBWFQ con WRED y QoS incrementa de manera notable la estabilidad del throughput. Esto se debe a la asignación del ancho de banda a clases y la administración eficaz de la congestión.

Para situaciones donde el rendimiento y la baja latencia son cruciales (como la voz sobre IP o las videoconferencias), esta mezcla de tecnologías brinda resultados ideales.

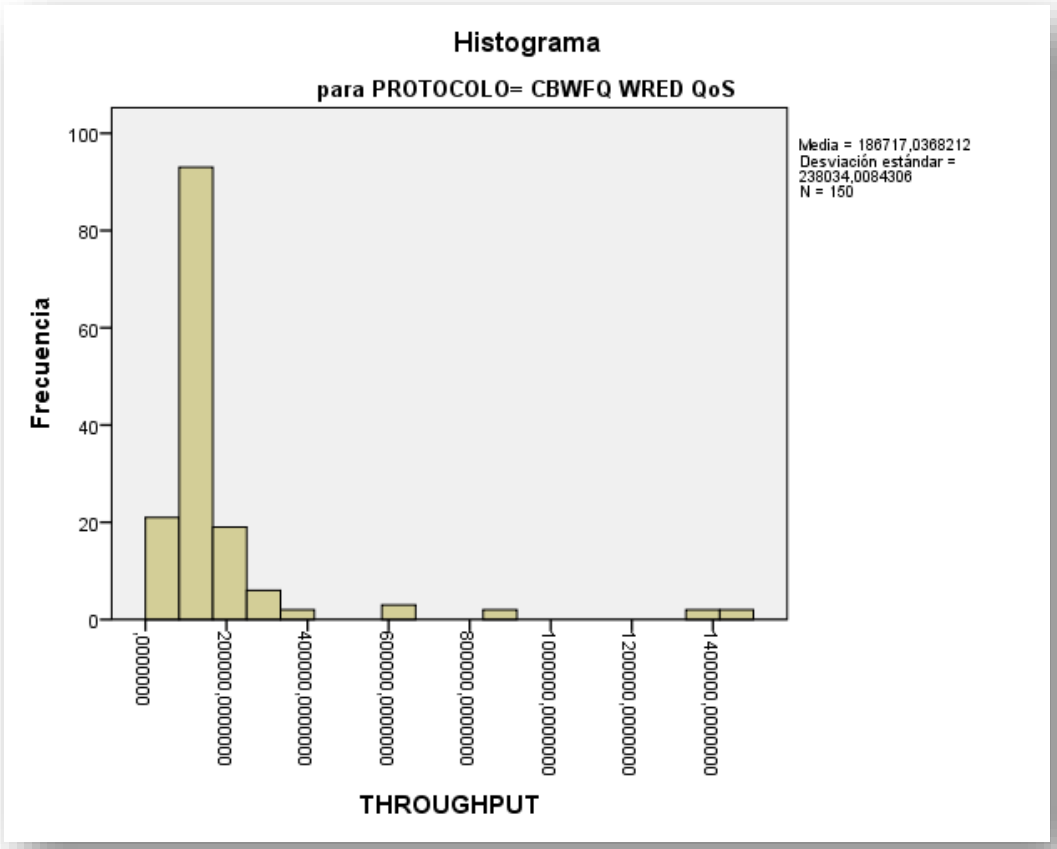


Figura 81: Histograma del Throughput con el protocolo CBWFQ-WRED y QoS
Fuente: Autor

La figura 82 muestra una evaluación comparativa del throughput en diversos contextos empleando el protocolo CBWFQ.

- Cbwfq-QoS: Sin WRED, el protocolo experimenta congestión y no puede utilizar de manera eficaz el ancho de banda disponible, particularmente en situaciones de elevada demanda.
- Cbwfq-sin QoS: La falta de QoS disminuye el desempeño, dado que no se definen prioridades ni se otorga un ancho de banda asegurado a las clases esenciales.
- Cbwfq-Wred-sin QoS: A pesar de que mejora en escenarios, la ausencia de QoS restringe el desempeño para el tráfico crítico.
- La combinación de CBWFQ para administrar colas, WRED para regular la congestión y QoS para dar prioridad al tráfico crítico optimiza el uso del ancho de banda y eleva la calidad del servicio.

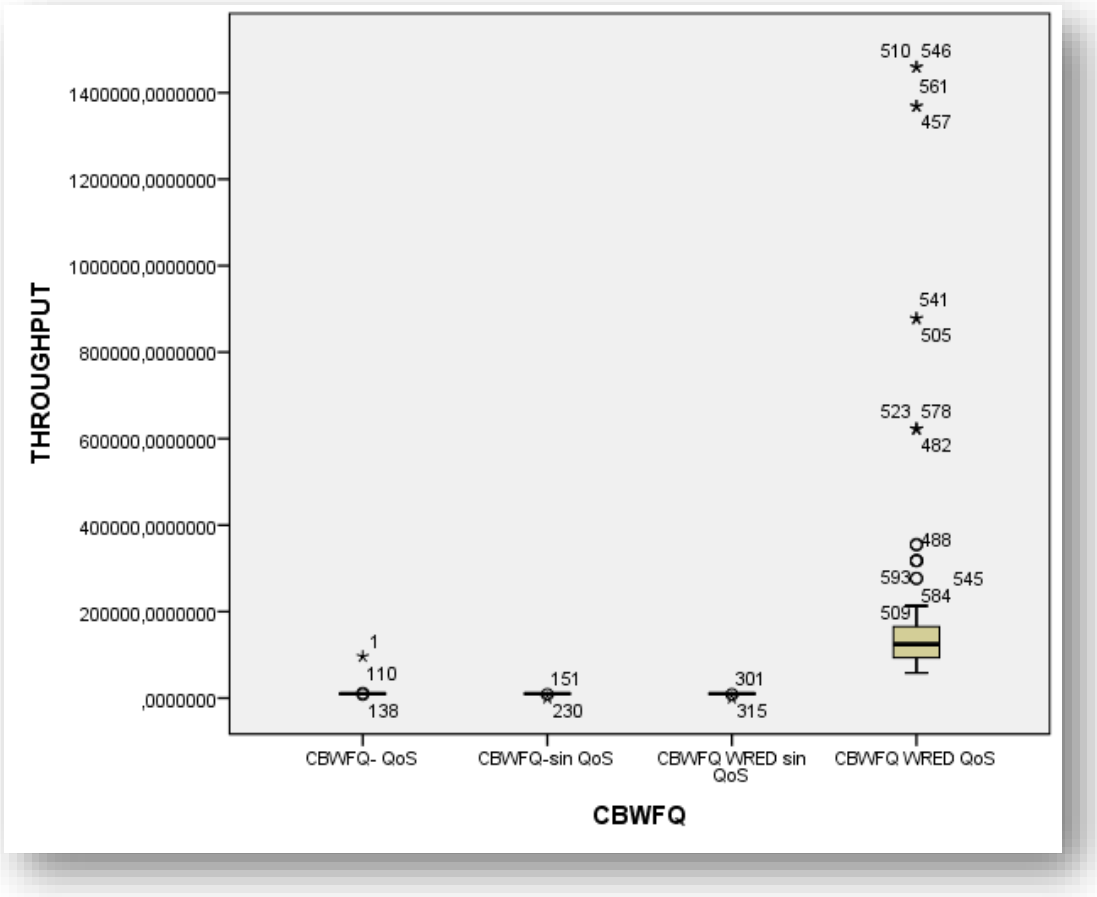


Figura 82: Diagrama de cajas del Throughput con el protocolo CBWFQ
Fuente: Autor

En la tabla 22 muestra el análisis del throughput en diferentes configuraciones del protocolo CBWFQ.

El valor sig=0.00 es inferior al nivel de significancia usualmente empleado (0.05), corroborando que las variaciones detectadas entre los grupos son de relevancia estadística.

El estudio ANOVA corrobora que las configuraciones del protocolo CBWFQ ejercen un efecto considerable en el throughput. Las discrepancias detectadas son estadísticamente relevantes, destacando el escenario con CBWFQ + WRED + QoS como el más eficaz en cuanto a desempeño. Esto evidencia que la combinación de control de congestión (WRED) y priorización (QoS) es fundamental para mejorar el desempeño de la red.

Tabla 21. Anova del throughput con el protocolo CBWFQ

ANOVA					
THROUGHPUT					
	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	3505464179396,628	3	1168488059798,876	82,416	,000
Dentro de grupos	8450034059622,480	596	14177909496,011		
Total	11955498239019,110	599			

Fuente: Autor

En la tabla 23 mediante el uso de una prueba post hoc Tukey HSD, se pueden valorar las diferencias relevantes entre los grupos.

- CBWFQ sin QoS y WRED sin QoS:

Estas estructuras constituyen el primer subconjunto homogéneo. Esto señala que, de manera estadística, el throughput promedio entre ambas no muestra diferencias relevantes.

- CBWFQ-QoS y QoS WRED de CBWFQ:

Estas estructuras poseen medias más elevadas y se encuentran en el segundo subgrupo homogéneo. La implementación de QoS, especialmente la mezcla de QoS con WRED, potencia de manera notable el throughput.

El valor de significancia (Sig.) en ambas columnas es de 1.000, corroborando que las variaciones dentro de cada subconjunto homogéneo no tienen relevancia estadística, pero sí lo tienen entre los subconjuntos.

Tabla 22.Diferencias Tukey del throughput con el protocolo CBWFQ

THROUGHPUT			
HSD Tukey[a]			
CBWFQ	N	Subconjunto para alfa = 0.05	
		1	2
CBWFQ WRED sin QoS	150	9942,666708640	
CBWFQ-sin QoS	150	9985,985264973	
CBWFQ- QoS	150	10663,002048280	
CBWFQ WRED QoS	150		186717,036821200
Sig.		1,000	1,000

Fuente: Autor

En la figura 83 muestra el análisis del throughput promedio para diversas configuraciones de calidad de servicio empleando el protocolo CBWFQ.

- CBWFQ-QoS es el ajuste sugerido para redes en las que la calidad de ciertos flujos (como la VoIP o el video) es esencial. A pesar de que el throughput medio es inferior, se asegura estabilidad, menor latencia y una gestión eficaz de los flujos prioritarios.
- Las configuraciones que incorporan WRED resultan beneficiosas en situaciones de gran congestión. No obstante, estas penalizan considerablemente el throughput promedio y solo deben emplearse cuando se requiera prevenir caídas significativas en el rendimiento.

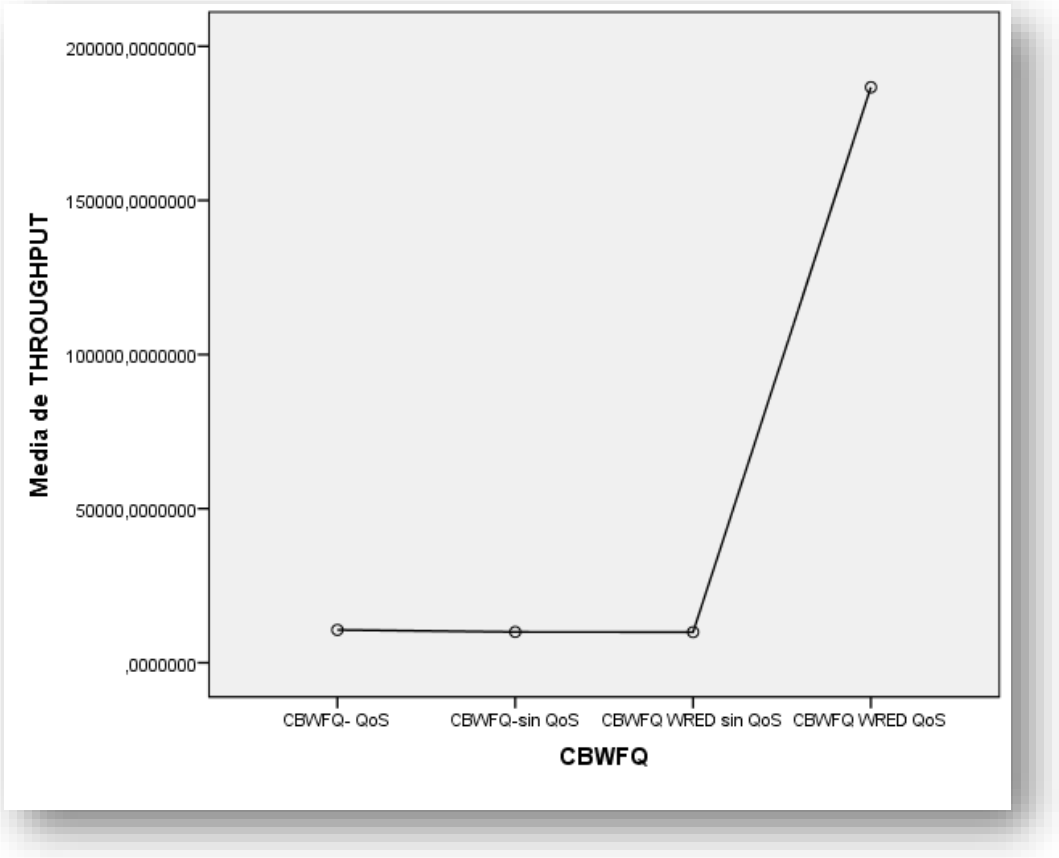


Figura 83: Gráfica de medias del throughput con el protocolo CBWFQ
Fuente: Autor

4.9 Comparación de los modelos

4.9.1 Jitter

En la tabla 23 el valor F adquirido es de 0,581, lo que señala que no existe una discrepancia estadísticamente relevante entre los grupos en cuanto a jitter.
El coeficiente de significancia es de 0,560, lo que supera ampliamente el coeficiente de significancia habitual (0,05). Esto corrobora que las discrepancias detectadas entre los grupos son insignificantes en términos estadísticos.

Tabla 23. Anova del Jitter en los protocolos

ANOVA					
JITTER					
	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	,011	2	,006	,581	,560
Dentro de grupos	4,242	447	,009		
Total	4,253	449			

Fuente: Autor

En la tabla 24 muestra una prueba de Tukey, empleada tras un análisis ANOVA, que determinar qué grupos muestran diferencias relevantes entre sus medios.
Los tres protocolos poseen medios de jitter bastante parecidos y se reúnen en el mismo subgrupo uniforme. Esto implica que, en términos prácticos, los tres protocolos proporcionan un rendimiento similar en cuanto a jitter.

Tabla 24. Análisis de Tukey con los protocolos

JITTER		
HSD Tukey[a]		
Protocolo	N	Subconjunto para alfa = 0.05
		1
CBWFQ-QoS	150	1,0094
FIFO-QoS-WRED	150	1,0184
WFQ-QoS-WRED	150	1,0209
Sig.		,562

Fuente: Autor

En la figura 84 muestra los métodos de jitter para diversas configuraciones de red. A continuación, se examina cada ajuste y su influencia en el jitter.
En función de los hallazgos, CBWFQ-QoS resulta ser el protocolo más apropiado para una red en un inmueble estudiantil ya que:

- Proporciona el jitter más reducido, lo que asegura una estabilidad superior en las aplicaciones que requieren de latencia.
- Facilita la priorización de tráfico esencial, tales como plataformas educativas, videoconferencias o sistemas de administración en línea.
- Optimiza la experiencia del usuario en un entorno en el que la necesidad de aplicaciones multimedia es elevada.

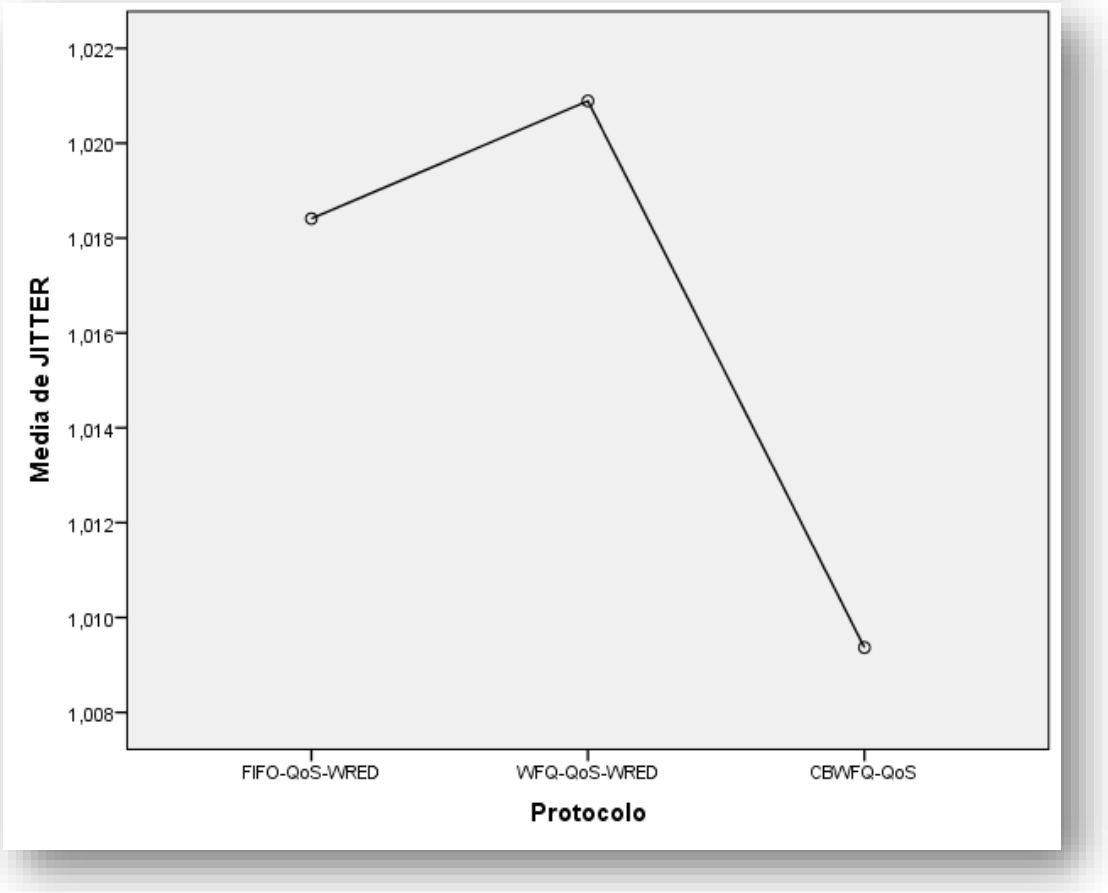


Figura 84: Gráfica de medias del jotter con la variación de los protocolos
Fuente: Autor

4.9.2 Throughput

En la tabla 25 muestra la varianza (ANOVA) del desempeño bajo distintos protocolos.
Valor 82.1, que señala que la variabilidad entre protocolos supera significativamente a la variabilidad interna de los grupos.
El valor de pag<0,001 evidencia que las variaciones en el rendimiento entre los protocolos son estadísticamente significativas, lo que indica que el protocolo influye de forma significativa en el rendimiento del sistema.
Es claro que los protocolos influyen de manera considerable en el rendimiento. La puesta en marcha de protocolos ideales podría optimizar el desempeño global del sistema.

Tabla 25.Anova del Throughput en los protocolos

ANOVA					
THROUGHPU					
	Suma de cuadrados	Gl	Media cuadrática	F	Sig.
Entre grupos	2011813917553,948	2	1005906958776,974	82,124	,000
Dentro de grupos	5475153207215,888	447	12248664893,100		
Total	7486967124769,836	449			

Fuente: Autor

La tabla 26 muestra el análisis del throughput bajo distintos protocolos.
El protocolo FIFO-WRED (sin QoS) presenta un rendimiento medio considerablemente superior (151815,995) y se encuentra en un subgrupo distinto a los demás protocolos, lo que señala que sus diferencias son estadísticamente relevantes con un nivel de confianza del 95%.
WFQ con QoS (9932,9068) y CBWFQ con QoS (10022,273) constituyen un subconjunto uniforme, lo cual sugiere que no existen diferencias notables entre ambos en cuanto a desempeño.
En la última columna de la tabla, los valores de significancia entre los subconjuntos son 1,000, corroborando que los protocolos de cada subconjunto no muestran diferencias de relevancia estadística entre sí.

Tabla 26. Análisis del tukey del throughput

THROUGHPU			
HSD Tukey[a]			
Protocolo	N	Subconjunto para alfa = 0.05	
		1	2
WFQ-QoS	150	9932,9068	
CBWFQ-QoS	150	10022,2732	
FIFO-WRED-sin QoS	150		151815,9952
Sig.		1,000	1,000

Fuente: Autor

En la figura 85 presenta los umbrales de rendimiento para tres protocolos distintos, ilustrando su rendimiento.
Si la red soporta usos esenciales como videollamadas y transmisión en tiempo real, CBWFQ con QoS proporciona un balance apropiado entre calidad y control ya que puede

ser más eficaz en contextos con diversas clases virtuales ya que ofrece un control más amplio sobre la priorización del tráfico.

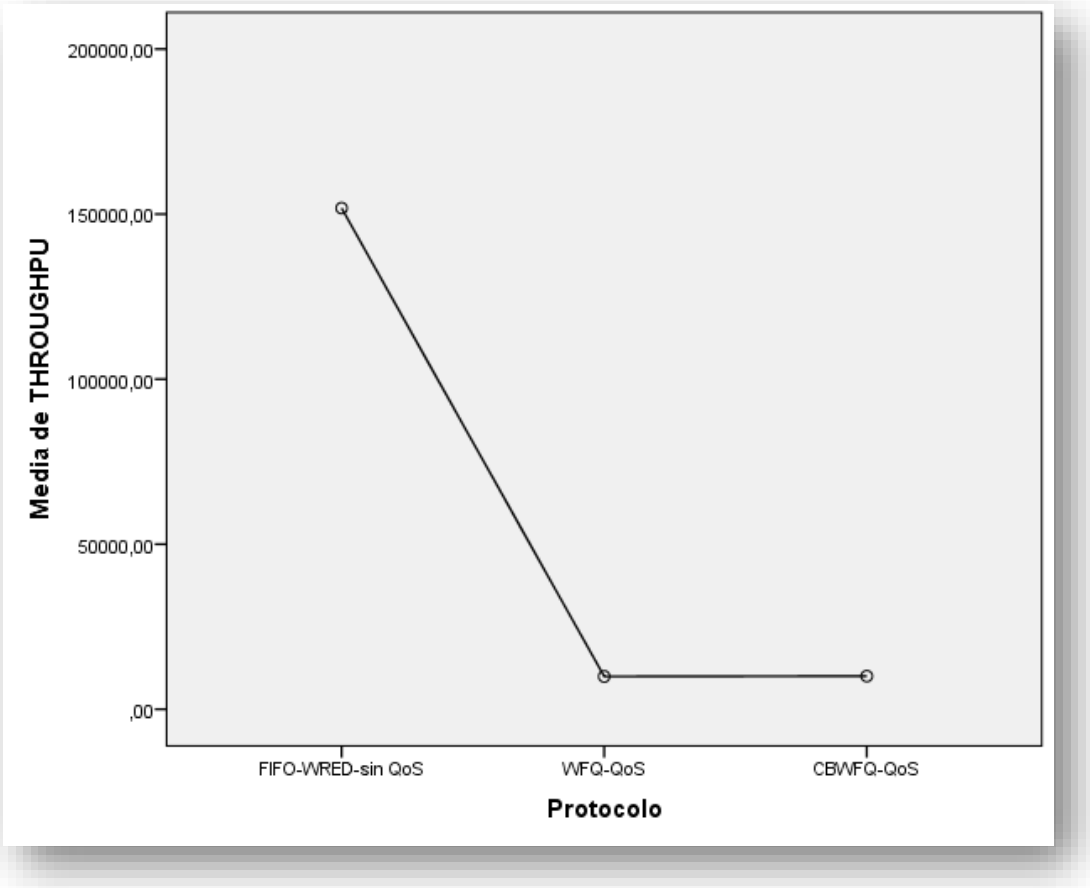


Figura 85: Grafica de medias del throufhput con la variación de los protocolos
Fuente: Autor

CAPÍTULO V

5. Conclusiones y Recomendaciones

5.1 Conclusiones

- El estudio de la infraestructura del Bloque A mostró que, en su condición actual, la red se encuentra con problemas considerables de variación en los tiempos de demora (jitter) y una deficiente en la utilización del throughput, los obstáculos en la transmisión de datos se originan por una inadecuada priorización del tráfico crítico y la ausencia de calidad de servicio.
- La aplicación de métricas concretas para la calidad del servicio facilitó la identificación de los aspectos críticos a mejorar: el jitter tiene un impacto severo en aplicaciones sensibles al tiempo (como VoIP y videollamadas), y el throughput no es suficiente para afrontar la demanda de tráfico simultáneamente.
- Las simulaciones demostraron que el protocolo CBWFQ en combinación con QoS es la alternativa más efectiva, este protocolo incrementa notablemente el jitter al otorgar prioridad al tráfico según su relevancia y asegurar un desempeño óptimo incluso en situaciones de gran congestión. La división y categorización del tráfico mejora el uso del ancho de banda y eleva la calidad global del servicio.
- La configuración de CBWFQ con QoS resultó tener un avance significativo en todos los parámetros evaluados, en particular en aplicaciones esenciales. Esto confirma que su puesta en marcha garantiza un desempeño uniforme y previsto en el Bloque A.

5.2 Recomendaciones

- Efectuar simulaciones regulares para evaluar el efecto de cambios futuros en la infraestructura o en las políticas de tráfico.
- Aplicar políticas de QoS en los equipos de red para otorgar prioridad al tráfico sensible al jitter como (voz y video).
- Incrementar la capacidad de los enlaces troncales (backbone) para soportar mayor capacidad en periodos de alta demanda.
- Aplicar subredes para disminuir el atasco en los dominios de difusión y garantizar un uso más eficiente del rendimiento disponible.

BIBLIOGRAFÍA

[1] M. J. O. Mejía, C. A. A. Ortiz, W. E. V. Ramos, y Luis Enrique Pacheco Moscoso, «Gestión del tráfico de red en la calidad de servicio "QoS" WAN en Tambopata-Perú 2021», *Rev. Cienc. Soc. Ve*, vol. XXVIII, n.º 2, pp. 300-317, 2022.

[2] «Evaluación de la atención al cliente a través del Modelo Servqual en el Paradero Sabor Latino.pdf». Accedido: 24 de abril de 2024. [En línea]. Disponible en: http://dspace.unach.edu.ec/bitstream/51000/6411/1/Evaluaci%C3%B3n%20de%20la%20atenci%C3%B3n%20al%20cliente%20a%20trav%C3%A9s%20del%20Modelo%20Servqual%20en%20el%20Paradero%20Sabor%20Latino.pdf

[3] Labbo, «QoS: ¿Qué es y cuáles son sus beneficios? - OSTEC Blog», OSTEC | Segurança digital de resultados. Accedido: 17 de enero de 2024. [En línea]. Disponible en: https://ostec.blog/es/seguridad-perimetral/qos-y-sus-beneficios/

[4] «(11) ¿Por qué es tan importante evitar la pérdida de paquetes de datos en mi red? | LinkedIn». Accedido: 22 de enero de 2024. [En línea]. Disponible en: https://www.linkedin.com/pulse/por-qu%C3%A9-es-tan-importante-evitar-la-p%C3%A9rdida-de-paquetes/?originalSubdomain=es

[5] N. A. B. Rodriguez, «DECLARATORIA DE AUTORÍA».

[6] «¿Qué es la calidad de servicio (QoS) en las redes? | Fortinet». Accedido: 17 de enero de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service

[7] S. E. Pérez, J. M. Arana, I. Meza, y C. Erazo, «Implantación de Calidad de Servicio (QoS) en redes inalámbricas Wi-Fi».

[8] D. M. Llerena Delgado, «Algoritmos de Calidad de Servicios (Q0S) y la Congestión en los Enlaces de Comunicación de los Usuarios de la Empresa Uniplex Systems de la Ciudad de Quito», bachelorThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Redes y Telecomunicaciones, 2011. Accedido: 17 de enero de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/42

[9] «Repositorio Universidad Técnica de Ambato: Modelos de configuración de calidad de servicios QoS en el tráfico de voz y su impacto en el sistema de telefonía IP de la empresa Cemento Chimborazo C.A.» Accedido: 17 de enero de 2024. [En línea]. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/2335

[10] «content.pdf». Accedido: 24 de abril de 2024. [En línea]. Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/505ee25c-49e0-4dc6-9f4e-b3a550a16449/content

[11] «content.pdf». Accedido: 24 de abril de 2024. [En línea]. Disponible en: https://apirepositorio.unh.edu.pe/server/api/core/bitstreams/3dfd0d0f-c07f-49f7-922d-985f520b0ef2/content

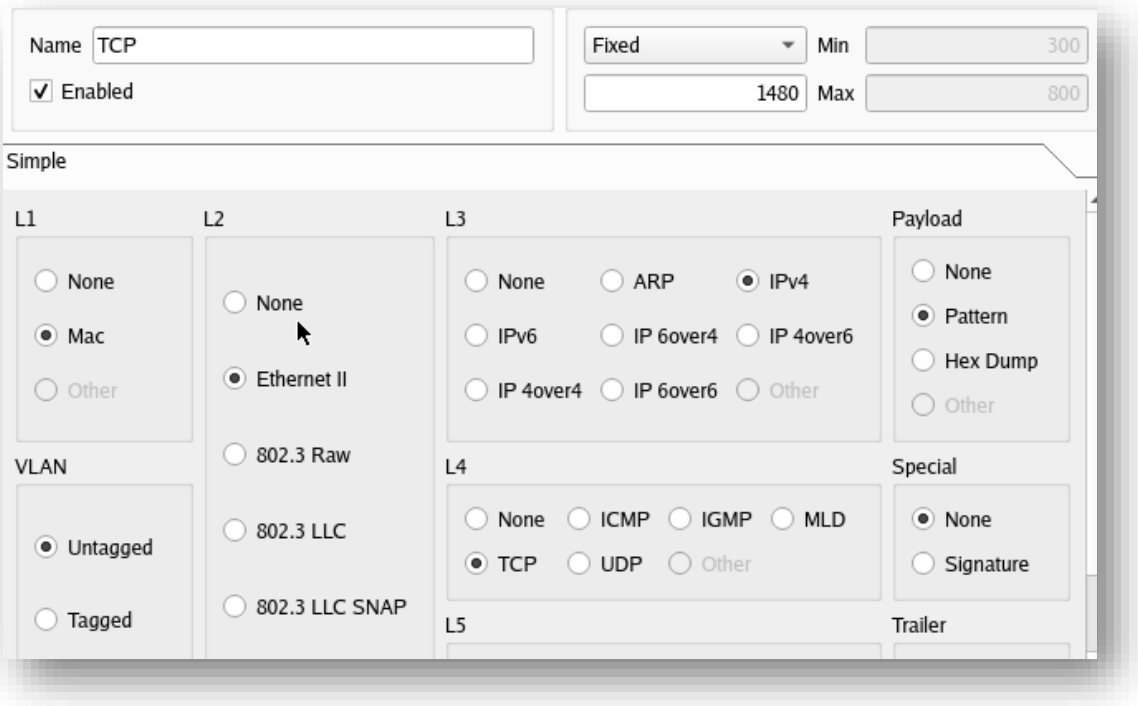
[12] «"DISEÑO E IMPLEMENTACIÓN DE UNA RED MPLS PARA EL SISTEMA DE COMUNICACIÓN DE EDITORIAL OCEANO DOMINICANA, EN SANTO DOMINGO Y ZONA METROPOLITANA DE SANTIAGO, AGOSTO-DICIEMBRE 2014". | PDF». Accedido: 24 de abril de 2024. [En línea]. Disponible en: https://es.slideshare.net/vanessajcontreras16/informe-final-modificado

[13] «info@citel». Accedido: 25 de abril de 2024. [En línea]. Disponible en: https://www.oas.org/es/citel/infocitel/2010/abril/calidad_e.asp
[14] «Calidad de servicio | Quality of Services (QoS) - ManageEngine NetFlow Analyzer». Accedido: 25 de abril de 2024. [En línea]. Disponible en: https://www.manageengine.com/latam/netflow/calidad-de-servicio-qos.html
[15] V. Briones, «Víctor Briones: [REDES DE TELECOMUNICACIONES] Lab 4: Calidad de servicio (QoS)», Víctor Briones. Accedido: 26 de abril de 2024. [En línea]. Disponible en: https://vic-en-fime.blogspot.com/2013/02/redes-de-telecomunicaciones-lab-4.html
[16] «SABER UCV: Identificador inválido». Accedido: 26 de abril de 2024. [En línea]. Disponible en: http://saber.ucv.ve/jspui/bitstream/123456789/731/3/Anexo%202.pdf
[17] «Monografia manejo de colas.pdf».
[18] «¿Cómo se analiza el tráfico de red y la congestión utilizando la teoría de colas?» Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://es.linkedin.com/advice/0/how-do-you-analyze-network-traffic-congestion?lang=es
[19] D. G. Kendall y J. Little, «TEORÍA DE COLAS: MODELO M/M/1».
[20] dalmar, «PPT - Modelo M | M | 1 PowerPoint Presentation, free download - ID:1943108», SlideServe. Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://www.slideserve.com/dalmar/modelo-m-m-1
[21] «Modelo M/M/c». Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://www.um.es/or/ampliacion/node13.html
[22] «Aplicaciones y análisis de modelos de teoría de colas en sistemas de espera». Accedido: 28 de abril de 2024. [En línea]. Disponible en: https://es.linkedin.com/pulse/aplicaciones-y-an%C3%A1lisis-de-modelos-teor%C3%ADa-colas-en-espera-gonz%C3%A1lez
[23] «¿Qué es la calidad de servicio (QoS) en las redes?», Fortinet. Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/qos-quality-of-service.html
[24] «Utpl_Torres_Ontaneda_Auliriar_004x790. (1).pdf».
[25] «Qué es la calidad del servicio, cómo se mide y cómo mejorarla». Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://blog.hubspot.es/service/calidad-del-servicio
[26] «Carta de métricas de rendimiento de IP (ippm)». Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://www.ietf.org/proceedings/52/222.htm
[27] Victor.Lopez.Macias@tajamar365.com, «Conceptos generales de tecnologías WAN», Tech Riders. Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://techriders.tajamar.es/conceptos-generales-tecnologias-wan/
[28] «85201908.pdf». Accedido: 8 de mayo de 2024. [En línea]. Disponible en: https://www.redalyc.org/pdf/852/85201908.pdf
[29] Wild IT Academy, *9.3 Algoritmos de Encolamiento | CCNA 200-301 | Wild IT Academy*, (13 de febrero de 2021). Accedido: 10 de junio de 2024. [En línea Video]. Disponible en: https://www.youtube.com/watch?v=LDhiGFfAZM4

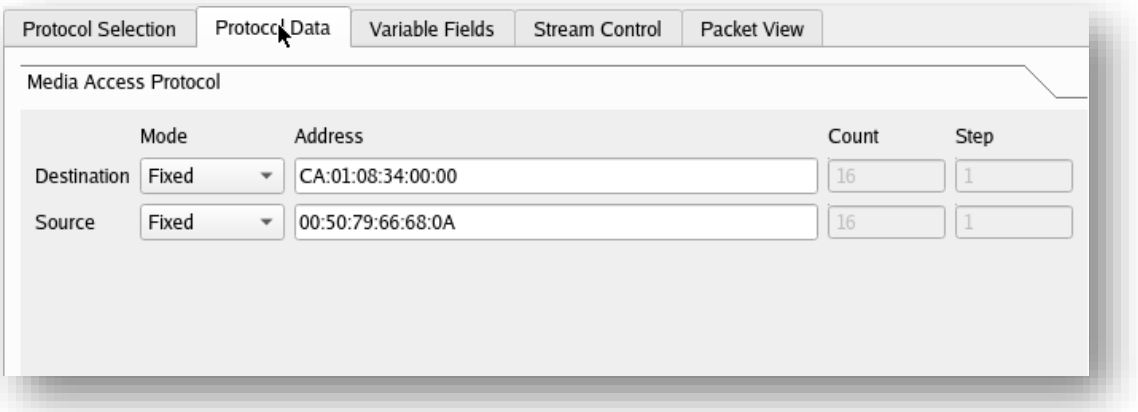
[30] Q. B. D. Patricio, «DISEÑO E IMPLEMENTACIÓN DE CALIDAD DE SERVICIO (QoS) EN LA RED DE TRANSPORTE DE DATOS DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO (MDMQ).».
[31] «manejo de colas en redes 2.pdf».
[32] M. J. M. Salazar y M. V. U. Jaramillo, «INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES.».
[33] «WRED - GlosarioIT: Glosario Informático». Accedido: 16 de septiembre de 2024. [En línea]. Disponible en: https://www.glosarioit.com/WRED
[34] «Appliances | Marketplace | GNS3». Accedido: 16 de septiembre de 2024. [En línea]. Disponible en: https://gns3.com/marketplace/appliances
[35] «Sobreviela - Calidad de servicio (QoS) con routers Cisco.pdf».

ANEXOS

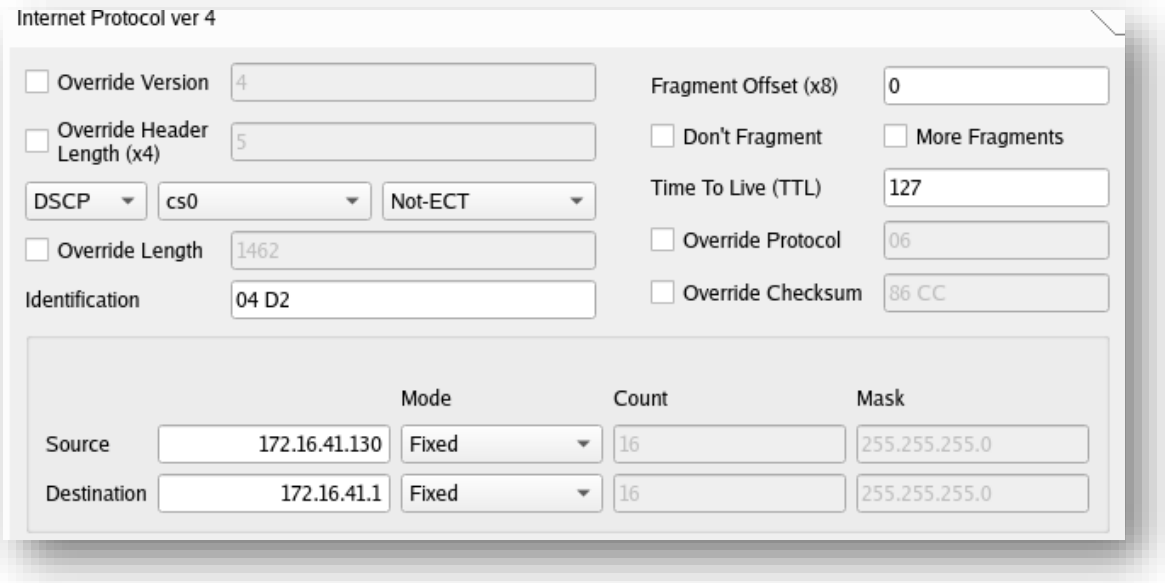
Configuración para crear paquetes de red a medida. Esta configuración se aplica en instrumentos de prueba y simulación de redes, tales como generadores de paquetes o analizadores de protocolos, con el objetivo de modelar diversos escenarios de tráfico en redes.



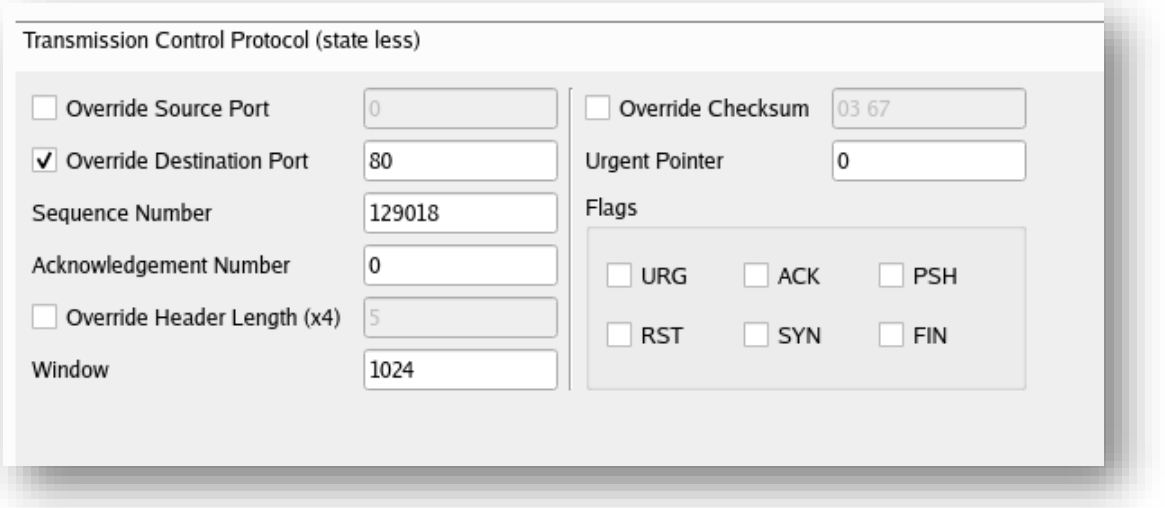
Se realiza la configuración en el generador de paquetes, concretamente en la sección vinculada al Protocolo MAC. Esta herramienta ofrece control en las pruebas de redes sofisticadas, asistiendo a los administradores y programadores en la detección de fallos o en la mejora del desempeño de los sistemas.



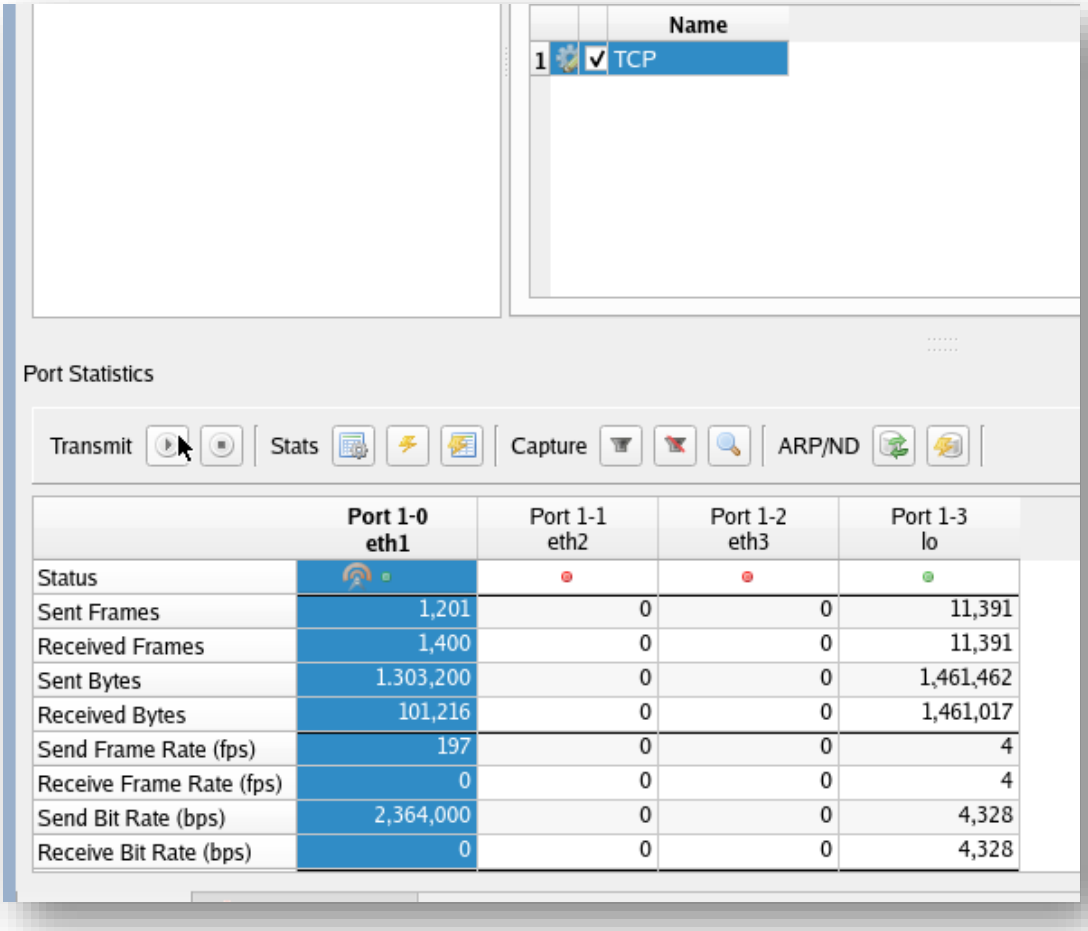
Se realiza la configuración de parámetros de un paquete IPv4 para la red, este tipo de interfaz se emplea para adaptar las propiedades de los paquetes IP.



Se ajuste para un paquete TCP (Protocolo de control de transmisión), para una herramienta de prueba como es la simulación de red. Esto se emplea para ajustar el comportamiento de un paquete TCP antes de su envío, posibilitando la comprobación de las respuestas del sistema.



Se realiza la interfaz de seguimiento y estadísticas de tráfico en el simulador como el generador de tráfico o un evaluador de rendimiento para el protocolo de red TCP.



Se presenta la captura de tráfico de red, realizada con el programa de análisis Wireshark. En esta imagen se pueden apreciar paquetes TCP con un patrón de retransmisión, lo que señala que existen dificultades de comunicación o pérdida de paquetes entre el punto de origen y el destino y esto nos ayuda a probar la estabilidad y eficiencia de sistemas de comunicación.