UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCAS APLICADAS

CARRERA DE TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"EVALUACIÓN DE LA CALIDAD DE SERVICIO EN SISTEMAS DE COMUNICACIÓN MULTIMEDIA IMPLEMENTADAS EN MÁQUINAS VIRTUALES HACIENDO USO DE LA TECNOLOGÍA MIKROTIK"

Trabajo de titulación previo a la obtención del título de Ingeniera en Telecomunicaciones

Línea de investigación: Innovación tecnológica y de productos

AUTOR:

Wendy Dayana Luna Quilumba

DIRECTOR:

MSc. Carlos Alberto Vásquez Ayala

Ibarra – Ecuador 2026

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
APELLIDOS Y NOMBRES:	LUNA QUILUMBA WENDY DAYANA

DATOS DE LA OBRA	
TÍTULO:	"EVALUACIÓN DE LA CALIDAD DE SERVICIO EN SISTEMAS DE COMUNICACIÓN MULTIMEDIA IMPLEMENTADAS EN MÁQUINAS VIRTUALES HACIENDO USO DE LA TECNOLOGÍA MIKROTIK"
AUTOR (ES):	LUNA QUILUMBA WENDY DAYANA
FECHA: DD/MM/AAAA	04/09/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERA EN TELECOMUNICACIONES
DIRECTOR /ASESOR:	MSC. CARLOS ALBERTO VÁSQUEZ AYALA MSC. EDGAR ALBERTO MAYA OLALLA

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días del mes de septiembre de 2026

EL AUTOR:

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
WENDY DAYANA LUNA QUILUMBA

…….
Wendy Dayana Luna Quilumba

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 4 de septiembre de 2026

MSC. CARLOS ALBERTO VÁSQUEZ AYALA,

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CARLOS ALBERTO VASQUEZ AYALA

(f)……

Msc. Carlos Alberto Vásquez Ayala

C.C.: 1002424982

DIRECTOR

DEDICATORIA

"Todo lo puedo en aquel que me fortalece."
Filipenses 4:13

Dedico este trabajo, en primer lugar, a Dios, por ser mi guía, mi fortaleza y mi refugio durante todo este camino. Por darme la sabiduría y la perseverancia necesaria para continuar incluso en aquellos momentos en los que las dificultades parecían superar mis fuerzas.

A mis padres, quienes han sido mi mayor apoyo y el pilar fundamental de mi vida. Gracias por creer en mí incluso cuando yo misma dudaba, por sostenerme en los momentos difíciles y por enseñarme que, con esfuerzo y perseverancia, siempre es posible seguir adelante. Cada consejo, cada sacrificio y cada palabra de aliento me han acompañado hasta llegar aquí. Este logro también es de ustedes, porque detrás de cada paso siempre estuvieron su amor, su confianza y su apoyo incondicional.

A mis hermanos, por formar parte de cada etapa de mi vida y acompañarme también durante este largo proceso. Gracias por cada enseñanza, por los consejos, las palabras de ánimo, las risas y por estar presentes tanto en los momentos buenos como en aquellos que se hicieron difíciles.

Wendy Dayana Luna Quilumba

AGRADECIMIENTO

A Dios, por acompañarme a lo largo de este camino, brindarme fortaleza en los momentos difíciles y permitirme alcanzar una meta tan importante en mi vida. Por darme la sabiduría, paciencia y perseverancia necesarias para continuar y culminar esta etapa de mi formación profesional.

A mis padres, Griselda y Jaime, por ser mi apoyo incondicional durante todos estos años. Gracias por cada sacrificio, por sus consejos, por confiar en mí y por impulsarme siempre a seguir adelante. Su esfuerzo, amor y compañía han sido fundamentales para llegar hasta este momento, y gran parte de este logro se lo debo a ustedes.

A mis hermanos, Alex, Kimberly y Stalin, por acompañarme durante este proceso, por sus palabras de ánimo, sus consejos y por estar presentes en cada etapa. Gracias por compartir conmigo tanto los momentos difíciles como las alegrías y por brindarme siempre su apoyo.

A Anthony, por acompañarme a lo largo de este proceso y permanecer a mi lado incluso en los momentos más complicados. Gracias por tu paciencia, por escucharme en los días de cansancio y frustración, por brindarme tranquilidad cuando las cosas parecían difíciles y, sobre todo, por impulsarme a seguir adelante cuando sentía que ya no podía más. Gracias por creer en mí, por celebrar conmigo cada avance y por recordarme constantemente todo lo que era capaz de lograr.

A mi director de tesis, Msc. Carlos Vásquez, por su orientación, paciencia, tiempo y conocimientos brindados durante el desarrollo de este trabajo. Agradezco cada observación, recomendación y aporte realizado, los cuales fueron fundamentales para fortalecer y culminar esta investigación. De igual manera, agradezco a mi asesor, Msc. Edgar Maya, por su disposición, guía y valiosos aportes durante este proceso. Sus recomendaciones y conocimientos contribuyeron significativamente al desarrollo y mejora de este trabajo de titulación.

A la Universidad Técnica del Norte y, de manera especial, a la Carrera de Telecomunicaciones, por brindarme la oportunidad de formarme profesionalmente, adquirir los conocimientos necesarios para mi desarrollo y crecer tanto en el ámbito académico como personal. A cada docente que formó parte de este proceso, por compartir sus conocimientos y contribuir a mi formación a lo largo de estos años.

Finalmente, agradezco a cada una de las personas que, de una u otra manera, estuvieron presentes durante estos años y dejaron una enseñanza en mi camino. Cada palabra de ánimo, cada consejo y cada gesto de apoyo fueron importantes para llegar hasta aquí. Hoy cierro una etapa llena de esfuerzo, aprendizajes, desafíos y también de momentos inolvidables, con la satisfacción de saber que cada dificultad valió la pena y con el corazón profundamente agradecido por todas las personas que caminaron junto a mí.

Wendy Dayana Luna Quilumba

RESUMEN

Este trabajo analiza el comportamiento de una infraestructura de red virtualizada implementada mediante MikroTik Cloud Hosted Router (CHR), considerando su utilización como una opción de menor costo para administrar tráfico multimedia frente a plataformas comerciales de mayor inversión. El estudio parte de la necesidad de contar con evidencia técnica que permita valorar el funcionamiento de MikroTik en escenarios virtualizados, especialmente cuando los servicios requieren diferenciación y priorización del tráfico. El desarrollo de la investigación siguió un modelo en cascada, organizado en las etapas de análisis, definición de requerimientos, diseño, implementación y pruebas. Para ello se construyó una topología en GNS3 sobre VirtualBox con routers MikroTik CHR, incorporando OSPF, segmentación mediante VLAN y una política de Calidad de Servicio basada en DiffServ. La clasificación del tráfico se efectuó mediante reglas Mangle y marcación DSCP, mientras que la administración del ancho de banda se implementó con Queue Tree y las disciplinas PFIFO y PCQ. En el escenario se generaron flujos de VoIP mediante SIP/RTP, streaming en tiempo real con MediaMTX (RTP/RTSP), video bajo demanda mediante HTTP, navegación web, tráfico MySQL y servicios de menor prioridad como FTP, IMAP y SSH. De manera simultánea, iPerf3 permitió introducir tráfico de fondo para reproducir condiciones controladas de congestión en el enlace de referencia. La valoración del desempeño se efectuó mediante la comparación de dos condiciones de operación: una red sin mecanismos de QoS y otra con la política de priorización implementada. Como marco de referencia se emplearon las métricas contempladas en la Recomendación ITU-T Y.1540, entre ellas ancho de banda, pérdida de paquetes (IPLR), retardo de transferencia de paquetes IP (IPTD), variación del retardo (IPDV) y tiempo de ida y vuelta (RTT). Los resultados obtenidos muestran que la aplicación de QoS favorece principalmente a los servicios de mayor prioridad, al disminuir la pérdida de paquetes y proporcionar un comportamiento más estable del retardo y su variación, con efectos especialmente apreciables en VoIP y streaming. En consecuencia, los resultados respaldan la utilización de MikroTik CHR como una alternativa técnicamente viable para aplicar mecanismos de QoS en redes virtualizadas orientadas al transporte de aplicaciones multimedia, manteniendo una solución de costo reducido.

Palabras clave: Calidad de Servicio, QoS, MikroTik, DiffServ, DSCP, Queue Tree, virtualización, VoIP, streaming RTP.

ABSTRACT

This degree project evaluates the performance of Quality of Service (QoS) in a virtualized network infrastructure implemented using MikroTik Cloud Hosted Router (CHR) as a low-cost alternative for multimedia traffic management compared to higher-cost commercial solutions. The research arises from the limited technical evidence regarding the behavior of MikroTik in virtualized environments, particularly in applications that require traffic prioritization and Quality of Service guarantees.

The methodology was developed using a waterfall model composed of the phases of analysis, requirements definition, design, implementation, and testing. A network scenario was implemented in GNS3 using VirtualBox and MikroTik CHR routers, with OSPF routing, VLAN-based segmentation, and QoS policies based on the Differentiated Services (DiffServ) model. Traffic classification and prioritization were performed using Mangle rules, DSCP marking, and Queue Tree management employing the PFIFO and PCQ queue disciplines. On this infrastructure, traffic corresponding to VoIP (SIP/RTP), real-time streaming via MediaMTX (RTP/RTSP), Video on Demand (VoD over HTTP), HTTP browsing, MySQL database, and low-priority services (FTP, IMAP, and SSH) was generated. Additionally, iPerf3 was used as a concurrent background traffic generator to induce controlled congestion conditions over the reference link.

The system evaluation was carried out by comparing scenarios with and without QoS, using the metrics established in ITU-T Recommendation Y.1540 as a reference: bandwidth, IP Packet Loss Ratio (IPLR), IP Packet Transfer Delay (IPTD), IP Packet Delay Variation (IPDV), and Round-Trip Time (RTT). The results show that the implementation of QoS improves network performance by reducing packet loss and stabilizing packet transfer delay and delay variation for higher-priority services, especially VoIP and streaming traffic. These results demonstrate that MikroTik CHR is a viable alternative for implementing Quality of Service mechanisms in virtualized networks intended for multimedia application transport, providing adequate performance with a low-cost solution.

Keywords: Quality of Service, QoS, MikroTik, DiffServ, DSCP, virtualization, multimedia traffic, VoIP

ÍNDICE DE CONTENIDOS

Capítulo I. Antecedentes **19**
1.1. Tema 19
1.2. Planteamiento del Problema 19
1.3. Objetivos 21
1.3.1. Objetivo general 21
1.3.2. Objetivos específicos 21
1.4. Alcance 22
1.5. Justificación 26
Capítulo II. Fundamentación Teórica **28**
2.1 Concepto de calidad de servicio 28
2.2 Arquitectura de QoS 29
2.3 Normativas de QoS 30
2.3.1 ITU-T E.800 31
2.3.2 ITU-T Y.1540 33
2.3.3 ITU-T Y.1541 40
2.4 Modelos de QoS 42
2.4.1 Modelo de Servicios Integrados (IntServ) 42
2.4.2 Modelo de Servicios Diferenciados (DiffServ) 43
2.5 Teoría de Colas en Redes de Comunicación 47
2.5.1 Elementos básicos de la teoría de colas 47
2.6 Técnicas de Encolado 49
2.6.1 LLQ 50
2.6.2 WFQ 50
2.7 Implementación de QoS 51
2.7.1 Identificación del tráfico y sus requerimientos 52
2.7.2 Clasificación de tráfico 53
2.7.3 Definición de políticas para cada clase 55
2.8 Marcaje de paquetes para clasificación de tráfico 56
2.9 Desafíos de QoS en entornos virtualizados 59
2.10 Tecnologías de virtualización en redes 60
2.10.1 Conceptos básicos de virtualización 61
2.10.2 Uso de máquinas virtuales en redes de Comunicación Multimedia 62
2.10.3 Impacto de la virtualización en el rendimiento de QoS 63

2.11 Sobre Mikrotik....64
2.11.1 ¿Qué es RouterOS?....64
2.11.2 Tipos de licenciamiento en Mikrotik....65
2.12 Herramientas de monitoreo de red....67
2.12.1 NTOP....68
2.12.2 WireShark....68
2.12.3 Torch....69
2.13 Análisis comparativo: Mikrotik en Redes Virtualizadas....69
2.13.1 Comparación entre Mikrotik y otras tecnologías....70
Capítulo III. Diseño e implementación....74
3.1 Metodología de desarrollo....74
3.2 Análisis actual....75
3.3 Definición de requerimientos....76
3.3.1 Nomenclatura de requerimientos....78
3.3.2 Requerimientos funcionales....79
3.3.3 Requerimientos de Calidad de servicio....80
3.3.4 Requerimientos de entorno virtualizado....81
3.3.5 Requerimientos de verificación de la configuración....82
3.3.6 Requerimientos de evaluación de desempeño....83
3.4 Selección del entorno de simulación y virtualización....84
3.4.1 Selección del software....84
3.4.2 Selección de la plataforma de virtualización....85
3.4.3 Selección del tipo despliegue de RouterOs....87
3.4.4 Selección del nivel de licencia CHR....88
3.5 Despliegue de topología virtualiza....90
3.5.1 Topología planteada....90
3.5.2 Plan de direccionamiento IP....91
3.5.3 Diseño de la topología propuesta....94
3.6 Diseño del esquema de enrutamiento....95
3.6.1 Asignación de direccionamiento IP....96
3.6.2 Protocolo de enrutamiento OSPF....97
3.6.3 Diseño de la segmentación mediante VLAN....98
3.6.4 Esquema de segmentación lógica (VLAN 10,20,30)....99
3.6.5 Enlaces troncales....100
3.6.6 Políticas de acceso entre VLAN....100

3.7 Diseño de los parámetros de QoS 102
3.7.1 Auditoría de tráfico de red 102
3.7.1.1 Auditoría VoIP 103
3.7.1.2 Auditoría Streaming 105
3.7.1.3 Auditoría de datos y soporte 108
3.7.2 Clasificación de paquetes 113
3.7.3 Priorización 115
3.7.3.1 Aplicaciones de prioridad critica 117
3.7.3.2 Aplicaciones de prioridad alta 117
3.7.3.3 Aplicaciones de prioridad media 117
3.7.3.4 Aplicaciones de prioridad baja 118
3.7.4 Marcaje de tráfico 118
3.7.4.1 Elección del modelo de QoS 118
3.7.4.2 Elección del método de marcaje de tráfico 121
3.7.4.3 Definición de las clases del servicio 123
3.7.4.4 Asignación de valores DSCP 124
3.7.4.5 Delimitación de la frontera de confianza 129
3.7.4.6 Diseño del esquema de marcas de RouterOS 131
3.7.5 Administración de la congestión 135
3.7.5.1 Elección del método de la administración de congestión 136
3.7.5.2 Teoría de Colas 138
3.7.5.3 Dimensionamiento de parámetros QoS para Queue Tree 141
3.7.5.4 Diseño de la estructura jerárquica de colas 144
3.8 Implementación de los parámetros de QoS 145
3.8.1 Implementación del esquema de marcas 146
3.8.1.1 Marcaje de conexiones 146
3.8.1.2 Modificación del Campo DSCP 147
3.8.1.3 Marcaje de paquetes 148
3.8.2 Implementación de Colas QoS 150
3.8.2.1 Definición de las disciplinas de encolamiento 151
3.8.2.2 Creación de la cola padre 152
3.8.2.3 Creación de las colas por servicio 152
3.8.2.4 Tratamiento del tráfico iPerf y del tráfico por defecto 154
3.8.2.5 Estructura jerárquica resultante del árbol de colas 154
3.9 Aplicación de las herramientas de monitoreo y verificación 155

3.9.1 Herramientas utilizadas 155
3.9.2 Verificación del marcaje en routers de acceso 156
3.9.3 Verificación de la conservación del DSCP en los routers de tránsito 157
3.9.4 Verificación del campo DSCP mediante Wireshark 158
3.9.5 Verificación de colas mediante Queue Tree 160
3.9.6 Criterios de validación de QoS 161
Capítulo IV. Pruebas y evaluación de resultados 164
4.1 Planteamiento de pruebas conforme a la ITU-Y.1540 164
4.1.1 Definición del esquema para la red de pruebas 166
4.1.2 Establecimiento de los parámetros de rendimiento o métricas 167
4.1.3 Definición de los escenarios de prueba 168
4.1.4 Registrar y comparar resultados obtenidos. 169
4.2 VoIP vs iPerf3 170
4.2.1 Condiciones comunes de la prueba 171
4.2.2 Criterios de cálculos 171
4.2.3 Resultados sin QoS 172
4.2.3.1 Ancho de Banda (AB) 173
4.2.3.2 Jitter RTP (IPDV) 174
4.2.3.3 Pérdida de paquete (IPLR) 175
4.2.3.4 Observación de la llamada 176
4.2.4 Resultados con QoS 176
4.2.4.1 Ancho de Banda (AB) 178
4.2.4.2 Jitter (IPDV) 179
4.2.4.3 Pérdida de paquetes (IPLR) 180
4.2.4.4 Observación de llamada 182
4.3 Streming vs iPerf3 182
4.3.1 Condiciones comunes de la prueba 183
4.3.2 Criterios de cálculo 183
4.3.3 Resultados sin QoS 184
4.3.3.1 Ancho de Banda (AB) 185
4.3.3.2 Jitter RTP (IPDV) 186
4.3.3.3 Pérdida de paquetes (IPLR) 187
4.3.3.4 Observación de la reproducción 188
4.3.4 Resultados con QoS 189
4.3.4.1 Ancho de Banda (AB) 190

4.3.4.2 Jitter RTP (IPDV) 191
4.3.4.3 Pérdida de paquetes (IPLR) 192
4.3.4.4 Observación de la reproducción 193
4.4 VOD vs iPerf3 194
4.4.1 Condiciones comunes de prueba 194
4.4.2 Criterios de cálculo 195
4.4.3 Resultados sin QoS 197
4.4.3.1 Ancho de Banda (AB) 198
4.4.3.2 Tiempo de ida vuelta (RTT) 199
4.4.3.3 Variación del RTT (indicador de Jitter TCP) 200
4.4.3.4 Indicador de pérdida TCP 201
4.4.3.5 Observación de la reproducción 202
4.4.4 Resultados con QoS 203
4.4.4.1 Ancho de Banda (AB) 204
4.4.4.2 Tiempo de ida vuelta (RTT) 206
4.4.4.3 Variación del RTT (indicador de Jitter TCP) 207
4.4.4.4 Indicador de pérdida TCP 208
4.4.4.5 Observación de la reproducción 209
4.5 FTP vs iPerf3 209
4.5.1 Condiciones comunes de prueba 210
4.5.2 Criterios de cálculo 211
4.5.3 Resultados sin QoS 213
4.5.3.1 Ancho de Banda (AB) 213
4.5.3.2 Tiempo de ida y vuelta (RTT) 215
4.5.3.3 Variación del RTT (indicador temporal TCP) 215
4.5.3.4 Indicador de pérdida TCP 216
4.5.3.5 Observación de la transferencia TCP 217
4.5.4 Resultados con QoS 218
4.5.4.1 Ancho de Banda (AB) 219
4.5.4.2 Tiempo de ida y vuelta (RTT) 220
4.5.4.3 Variación del RTT (Indicador temporal TCP) 221
4.5.4.4 Indicador de pérdida TCP 222
4.5.4.5 Observación de la transferencia 223
4.6 Registro y comparación de resultados 224
4.6.4 VoIP vs iPerf3 224

4.6.4.1 Ancho de Banda (AB) 225
4.6.4.2 Jitter (IPDV) 226
4.6.4.3 Pérdida de paquetes (IPLR) 227
4.6.4.4 Comparación final 228
4.6.2 Streaming vs iPerf3 229
4.6.2.1 Ancho de Banda (AB) 230
4.6.2.2 Jitter RTP (IPDV) 231
4.6.2.3 Pérdida de paquetes (IPLR) 232
4.6.2.4 Comparación final 233
4.6.3 VOD vs iPerf3 234
4.6.3.1 Ancho de banda (AB) 235
4.6.3.2 Tiempo de ida y vuelta (RTT) 236
4.6.3.3 Variación del RTT 237
4.6.3.4 Indicador de pérdida TCP 239
4.6.3.5 Comparación final 240
4.6.4 FTP vs iPerf3 241
4.6.4.5 Ancho de Banda (AB) 242
4.6.4.6 Tiempo de ida y vuelta (RTT) 243
4.6.4.7 Variación del RTT 244
4.6.4.8 Indicador de pérdida TCP 246
4.6.4.9 Comparación final 247
5. Conclusiones 249
6. Recomendaciones 251
Bibliografía 254
7. Anexos 257
7.1 Anexo A. Configuración de direccionamiento ip 257
7.2 Anexo B. Configuración OSPF: instancia, área e interface 258
7.3 Anexo C. Despliegue de servicios multimedia 259
7.4 Anexo D. Configuración de marcas en RouterOs 269
7.5 Anexo E. Configuración de colas 272
7.6 Anexo F. Verificación de la configuración del campo DSCP 272
7.7 Anexo G. Carpeta de pruebas 277

Índice de figuras

Figura 1 Topología de red virtualizada para gestión de tráfico multimedia 24
Figura 2 Esquema general de la arquitectura de calidad de servicio 29
Figura 3 Cuatro polos de calidad de Servicio 32
Figura 4 Modelo de referencia para la evaluación del rendimiento en la transferencia de paquetes IP según la recomendación ITU-T Y.1540. 35
Figura 5 Conectividad de red IP entre el host de origen y el host de destino según la ITU-T Y.1540 39
Figura 6 Eventos de referencia para la determinación del retardo de transferencia de paquetes IP (IPTD)..... 40
Figura 7 Esquema de funcionamiento del modelo de Servicios Integrados (IntServ)..... 43
Figura 8 Estructura del campo DiffServ en el encabezado IP 45
Figura 9 Modelo básico de un sistema de colas aplicado a redes de comunicación..... 48
Figura 10 Procesos para la implementación de QoS 51
Figura 11 Pasos para la identificación del tráfico de una red 52
Figura 12 Clasificación y Marcado de Paquetes..... 57
Figura 13 Fases metodológicas del proyecto de integración curricular. 74
Figura 14 Estructura y flujo de los requerimientos de QoS..... 78
Figura 15 Topología de red virtualizada para gestión de tráfico multimedia 90
Figura 16 Topología de red implementada en GNS3..... 95
Figura 17 Configuración OSPF R3: instancia, área e interfaces 98
Figura 18 Topología desplegada para la auditoría de red 103
Figura 19 Identificación del tráfico SIP mediante Wireshark..... 104
Figura 20 Identificación del tráfico RTP mediante Wireshark 105
Figura 21 Captura de tráfico RTP identificada durante la auditoría inicial. 106
Figura 22 Identificación del tráfico HTTP mediante Wireshark..... 107
Figura 23 Identificación del tráfico MYSQL mediante Wireshark 109
Figura 24 Identificación del tráfico FTP mediante Wireshark.....110
Figura 25 Identificación del tráfico SSH mediante Wireshark 111
Figura 26 Identificación del tráfico HTTP mediante Wireshark.....112
Figura 27 Identificación del tráfico IMAP mediante Wireshark 113
Figura 28 Delimitación de la frontera de confianza en la topología QoS..... 130
Figura 29 Verificación de las reglas Mangle empleadas para el marcaje del tráfico en R5.157
Figura 30 Conservación del valor DSCP a la entrada y salida del núcleo..... 158
Figura 31 Captura del tráfico en el punto de entrada de Wireshark 159
Figura 32 Secuencia temporal de pruebas 169
Figura 33 Resultado mostrado por iPerf3 durante la prueba de VoIP en Sin QoS. 173
Figura 34 Ancho de banda del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS. 174
Figura 35 Jitter del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS. 175
Figura 36 Pérdida de paquetes del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS. 176
Figura 37 Estadísticas de Queue Tree durante la prueba de VoIP con QoS..... 177
Figura 38 Resultado mostrado por iPerf3 durante la prueba de VoIP con QoS..... 178
Figura 39 Ancho de banda del flujo VoIP RTP frente a la carga iPerf3 durante QoS..... 179
Figura 40 Jitter del flujo VoIP RTP frente a la carga iPerf3 durante QoS. 180
Figura 41 Pérdida de paquetes del flujo VoIP RTP frente a la carga iPerf3 durante QoS . 182
Figura 42 Resultado mostrado por iPerf3 durante la prueba de Streaming en Sin QoS.... 185
Figura 43 Ancho de banda del Streaming RTP frente a la carga iPerf3 durante Sin QoS . 186
Figura 44 Jitter del Streaming RTP frente a la carga iPerf3 durante Sin QoS. 187

Figura 45 Pérdida de paquetes RTP del Streaming frente a la carga iPerf3 durante Sin QoS 188
Figura 46 Pixelación observada en VLC durante la prueba de Streaming sin QoS 189
Figura 47 Resultado mostrado por iPerf3 durante la prueba de Streaming con QoS 189
Figura 48 Estadísticas de Queue Tree durante la prueba de Streaming con QoS..... 190
Figura 49 Ancho de banda del Streaming RTP frente a la carga iPerf3 durante QoS 191
Figura 50 Jitter del Streaming RTP frente a la carga iPerf3 durante QoS 192
Figura 51 Pérdida de paquetes RTP del Streaming frente a la carga iPerf3 durante QoS . 193
Figura 52 Reproducción estable en VLC durante la prueba de Streaming con QoS..... 194
Figura 53 Resultado mostrado por iPerf3 durante la prueba de VoD en Sin QoS. 198
Figura 54 Ancho de banda del VoD frente a la carga iPerf3 durante Sin QoS. 199
Figura 55 RTT del VoD HTTP frente a la carga iPerf3 durante Sin QoS..... 200
Figura 56 Variabilidad temporal del flujo VoD HTTP e iPerf3 durante Sin QoS..... 201
Figura 57 Indicador de pérdida del VoD y pérdida estimada de iPerf3 durante Sin QoS.. 202
Figura 58 Retraso en el inicio y carga del contenido VoD durante la prueba sin QoS..... 203
Figura 59 Intervalos sin recepción de tráfico iPerf3 observados durante la prueba de VoD con QoS 204
Figura 60 Estadísticas de Queue Tree durante la prueba de VoD con QoS 204
Figura 61 Ancho de banda del VoD frente a la carga iPerf3 durante Qo..... 206
Figura 62 RTT del VoD HTTP frente a la carga iPerf3 durante QoS 206
Figura 63 Variación del RTT del VoD HTTP frente a la carga iPerf3 durante QoS. 208
Figura 64 Indicador de pérdida del VoD y pérdida estimada de iPerf3 durante QoS..... 209
Figura 65 Resultado mostrado por iPerf3 durante la prueba FTP en Sin QoS 213
Figura 66 Ancho de banda del FTP frente a la carga iPerf3 durante Sin QoS..... 214
Figura 67 RTT del flujo TCP FTP bajo carga iPerf3 durante Sin QoS..... 215
Figura 68 Variación del RTT del flujo FTP durante Sin QoS..... 216
Figura 69 Indicador de pérdida TCP del FTP y pérdida estimada de iPerf3 durante Sin QoS. 217
Figura 70 Transferencia del archivo FTP observada en FileZilla durante Sin QoS. 218
Figura 71 Estado de iPerf3 posterior a la ventana de medición durante el escenario QoS 218
Figura 72 Estadísticas de Queue Tree durante la prueba FTP con QoS. 219
Figura 73 Ancho de banda del FTP frente a la carga iPerf3 durante QoS 220
Figura 74 RTT del flujo TCP FTP bajo carga iPerf3 durante QoS. 221
Figura 75 Variación del RTT del flujo FTP durante QoS 222
Figura 76 Indicador de pérdida TCP del FTP y pérdida estimada de iPerf3 durante QoS 223
Figura 77 Transferencia del archivo FTP observada en FileZilla durante QoS..... 223
Figura 78 Comparación del ancho de banda del flujo VoIP RTP entre Sin QoS y QoS.... 226
Figura 79 Comparación del jitter promedio del flujo VoIP RTP entre Sin QoS y QoS.... 227
Figura 80 Comparación de la pérdida de paquetes RTP del servicio VoIP entre Sin QoS y QoS. 228
Figura 81 Variación favorable de las métricas de VoIP al aplicar QoS 228
Figura 82 Comparación del ancho de banda del Streaming entre Sin QoS y QoS..... 230
Figura 83 Comparación del jitter promedio del Streaming entre Sin QoS y QoS..... 232
Figura 84 Comparación de la pérdida de paquetes RTP del Streaming entre Sin QoS y QoS 233
Figura 85 Variación favorable de las métricas de Streaming al aplicar QoS..... 234
Figura 86 Comparación del ancho de banda del VoD entre Sin QoS y QoS..... 236
Figura 87 Comparación del RTT promedio del VoD entre Sin QoS y QoS 237
Figura 88 Comparación de la variación del RTT del VoD entre Sin QoS y QoS 238
Figura 89 Comparación del indicador de pérdida TCP del VoD entre Sin QoS y QoS.... 239

Figura 90 Variación favorable de las métricas del VoD al aplicar QoS..... 240
Figura 91 Comparación del ancho de banda de FTP entre Sin QoS y QoS..... 243
Figura 92 Comparación del RTT TCP promedio de FTP entre Sin QoS y QoS..... 244
Figura 93 Comparación de la variación del RTT de FTP entre Sin QoS y QoS..... 245
Figura 94 Comparación del indicador de pérdida TCP de FTP entre Sin QoS y QoS 247
Figura 95 Variación favorable de las métricas de FTP al aplicar QoS. 248

Índice de Tablas

Tabla 1 Cuatro polos de la QoS según la ITU-T E.800 32
Tabla 2 Elementos del modelo de desempeño IP según la ITU-T Y.1540 35
Tabla 3 Parámetros principales definidos por la ITU-T Y.1540 36
Tabla 4 Parámetros de disponibilidad del servicio IP según la ITU-T Y.1540 38
Tabla 5 Clases de QoS y objetivos de desempeño de red según la ITU-T Y.1541 41
Tabla 6 Relación entre clases de QoS de la ITU-T Y.1541 y mecanismos DiffServ 41
Tabla 7 Principales PHB utilizados en DiffServ 46
Tabla 8 Ejemplo de los requerimientos de calidad de servicio 56
Tabla 9 Asignación de prioridades y valores DSCP para aplicaciones en redes QoS 58
Tabla 10 Tasa de Transferencia para Aplicaciones en QoS 58
Tabla 11 Técnicas de Administración del Tráfico en Entornos Virtualizados 62
Tabla 12 Niveles de Licencia 65
Tabla 13 Niveles de licencia de MikroTik CHR 67
Tabla 14 Comparación de soluciones de routing virtual según características técnicas y operacionales 72
Tabla 15 Nomenclatura de requerimientos 79
Tabla 16 Requerimientos funcionales 80
Tabla 17 Requerimientos de calidad de servicio 81
Tabla 18 Requerimientos del entorno virtualizado 82
Tabla 19 Requerimientos de verificación de la configuración 83
Tabla 20 Requerimientos de pruebas de desempeño 83
Tabla 21 Comparación de software de simulación de redes 85
Tabla 22 Comparación de plataformas de virtualización 86
Tabla 23 Resultados de la selección del tipo de router 87
Tabla 24 Comparación de niveles de licencia CHR 89
Tabla 25 Clases de direcciones IP privadas 91
Tabla 26 Asignación de direcciones IPv4 para enlaces punto a punto 92
Tabla 27 Asignación de direcciones IPv4 para VLANs en R3 92
Tabla 28 Asignación de direcciones IPv4 para VLANs en R4 93
Tabla 29 Asignación de direcciones IPv4 para VLANs en R5 93
Tabla 30 Direcciones IP asignadas a los routers e interfaces de la red 96
Tabla 31 Esquema de segmentación lógica de la red mediante VLAN. 99
Tabla 32 Políticas de control de acceso entre VLAN implementadas en la red 101
Tabla 33 Clasificación de tráfico de red basado en protocolos y puertos 114
Tabla 34 Priorización del tráfico identificado en la red simulada 116
Tabla 35 Escala de evaluación para la selección del modelo de QoS 120
Tabla 36 Matriz de cumplimiento de los modelos de QoS 120
Tabla 37 Comparación de métodos de marcaje de tráfico 122
Tabla 38 Definición de las clases de servicio para la política de QoS 123
Tabla 39 Asignación de valores DSCP 127
Tabla 40 Clasificación de routers según su función dentro de la arquitectura QoS 130
Tabla 41 Fases del proceso de marcas en RouterOS 133
Tabla 42 Compilación de marcas de conexión, paquete y DSCP por servicio 134
Tabla 43 Escala de evaluación para la selección del método de administración de la congestión 136
Tabla 44 Matriz de cumplimiento de los mecanismos de administración de congestión 137
Tabla 45 Elementos principales de la administración de colas mediante Queue Tree 139
Tabla 46 Correspondencia teórica entre clases de tráfico y disciplina de cola 140

Tabla 47 Jerarquía y parámetros efectivos de Queue Tree..... 142
Tabla 48 Parámetros de las colas de servicio y del tráfico de fondo..... 143
Tabla 49 Fases del proceso de marcas en RouterOS..... 149
Tabla 50 Compilación de marcas de conexión, paquete y DSCP por servicio 150
Tabla 51 Disciplinas de encolamiento implementadas en Queue Tree. 151
Tabla 52 Cola padre 152
Tabla 53 Parámetros de implementación de colas por clase de servicio..... 153
Tabla 54 Parámetros del tráfico de fondo y del tráfico por defecto 154
Tabla 55 Herramientas de monitoreo utilizadas en la verificación de QoS 156
Tabla 56 Filtros de Wireshark para la identificación de las clases de servicio 160
Tabla 57 Comparación de las métricas de VoIP para una carga de 2 Mbit/s..... 225
Tabla 58 Comparación de las métricas de Streaming para una carga de 2 Mbit/s. 230
Tabla 59 Comparación de las métricas e indicadores del VoD para una carga de 2 Mbit/s.235
Tabla 60 Comparación de las métricas e indicadores de FTP para una carga de 2 Mbit/s 241

Capítulo I. Antecedentes

1.1. Tema

Evaluación de la Calidad de servicio en Sistemas de Comunicación Multimedia implementadas en Máquinas virtuales haciendo uso de la tecnología Mikrotik.

1.2.Planteamiento del Problema

La calidad de servicio (QoS) es un componente esencial para garantizar el rendimiento adecuado de aplicaciones críticas en redes modernas, especialmente en aquellas que gestionan tráfico en tiempo real, como VoIP, videoconferencias y aplicaciones IoT. A diferencia de las redes tradicionales, que operaban de forma aislada con menores exigencias, las redes actuales necesitan ofrecer alta capacidad, baja latencia y evitar la pérdida de paquetes para cumplir con las expectativas de los usuarios. (Shahad H. Majid, 2018)

Esto se complica en entornos virtualizados, donde los recursos físicos compartidos pueden generar cuellos de botella y afectar el rendimiento. En estos entornos, la implementación de QoS se vuelve crucial, ya que permite gestionar y priorizar el tráfico de manera eficiente, asegurando que las aplicaciones críticas operen de forma confiable y en tiempo real.

Además, en el ámbito de las comunicaciones multimedia, la QoS es vital para asegurar la experiencia del usuario. Organizaciones suelen optar por equipos avanzados como los de Cisco, conocidos por su capacidad de configuración y robustez. Sin embargo, estos equipos son costosos, lo que representa una barrera para muchas pequeñas y medianas empresas, instituciones educativas o entornos de investigación, que buscan soluciones de alta calidad a menor costo (Dobladez, 2007)

MikroTik se presenta como una alternativa económica, adoptada por su bajo costo y capacidades de gestión de tráfico. Sin embargo, existe poca información comparativa sobre su desempeño frente a equipos de gama alta, especialmente en lo que respecta a la QoS en entornos de comunicaciones multimedia, donde la precisión es crucial para evitar problemas de latencia, jitter y pérdida de paquetes. La falta de estudios comparativos detallados sobre MikroTik en entornos virtualizados de alta demanda genera incertidumbre, lo que dificulta la toma de decisiones informadas y puede resultar en un uso subóptimo de los recursos o soluciones insuficientes para garantizar comunicaciones multimedia de calidad (Hurtado Crespo, 2017)

Las tecnologías de virtualización han modificado los requisitos de QoS debido a la compartición de recursos físicos entre múltiples máquinas virtuales. Esto introduce nuevos desafíos, como la congestión del tráfico, mayor latencia y variabilidad en el rendimiento. Por ello, es esencial gestionar el tráfico de manera eficiente y priorizar las aplicaciones críticas. Las redes virtualizadas requieren configuraciones avanzadas que aseguren el aislamiento adecuado de recursos, minimizando interferencias entre máquinas, lo que demanda estrategias dinámicas y adaptativas para mantener la calidad en los servicios multimedia. (Fortinet, 2024)

1.3. Objetivos

1.3.1. Objetivo general

Implementar calidad de servicio en sistemas de comunicación multimedia dentro de entornos virtualizados, mediante la configuración de QoS en routers Mikrotik, para determinar sus ventajas y limitaciones.

1.3.2. Objetivos específicos

- Investigar los principios y métodos de calidad de servicio (QoS) aplicados a redes de comunicación multimedia, enfocados en las tecnologías de virtualización.
- Definir los requerimientos de QoS de MikroTik para la gestión de tráfico multimedia en redes virtualizadas, considerando las diferencias con soluciones de alto rendimiento.
- Diseñar una topología de red virtualizada que integre routers MikroTik para la configuración y evaluación de QoS en entornos de comunicación multimedia.
- Realizar pruebas de desempeño y estabilidad de las configuraciones de QoS en routers MikroTik, comparando los resultados obtenidos para evaluar su efectividad en redes virtualizadas.

1.4. Alcance

El alcance de este proyecto incluye una investigación de los principios y métodos de calidad de servicio (QoS) en redes de comunicación multimedia, enfocándose en métricas clave como latencia, jitter, pérdida de paquetes y ancho de banda para establecer una base teórica que sustente las configuraciones y evaluaciones en routers MikroTik, por eso en este proyecto, se trabajará bajo dos escenarios para evaluar la gestión del tráfico en redes virtualizadas utilizando MikroTik. En el primer escenario, se implementará una topología básica sin configuraciones de QoS ni herramientas de auditoría, con el objetivo de analizar el comportamiento del tráfico. Durante esta etapa, se evaluarán métricas clave como la pérdida de paquetes, jitter, latencia y el uso del ancho de banda, estableciendo una línea base para comparaciones futuras. En el segundo escenario, se configurarán las herramientas de QoS y auditorías previamente definidas para analizar las mejoras en el tráfico, priorizando aplicaciones críticas como VoIP y Streaming, aplicando técnicas como LLQ y marcaje de paquetes (DSP). Este enfoque comparativo permitirá validar la efectividad de las configuraciones implementadas y demostrar cómo estas impactan en el rendimiento del tráfico en entornos virtualizados. Para ello, se utilizará la metodología de cascada, estructurada en cuatro fases: análisis, definición de requerimientos, diseño y pruebas.

En la primera fase de análisis, se abordará el estudio de los principios y métodos de calidad de servicio (QoS) aplicados a redes de comunicación multimedia, con especial énfasis en las tecnologías de virtualización. Se profundizará en modelos de QoS como IntServ y DiffServ, analizando su aplicabilidad en entornos virtualizados, donde los recursos físicos son compartidos entre múltiples máquinas virtuales, generando desafíos como la congestión y el jitter. Así mismo, se investigarán las capacidades y herramientas disponibles en dispositivos MikroTik, como Torch, Traffic Flow, Low Latency Queuing (LLQ) y Weighted Fair Queuing (WFQ), y marcaje de paquetes, para implementar QoS y realizar auditorías de red. Además, se

investigarán las mejores prácticas y herramientas utilizadas por dispositivos como MikroTik para implementar QoS en redes virtualizadas, para determinar las limitaciones y ventajas. Esto permitirá establecer una base teórica sólida para evaluar la eficacia de la implementación de QoS en redes virtualizadas y su impacto en el rendimiento de las aplicaciones multimedia.

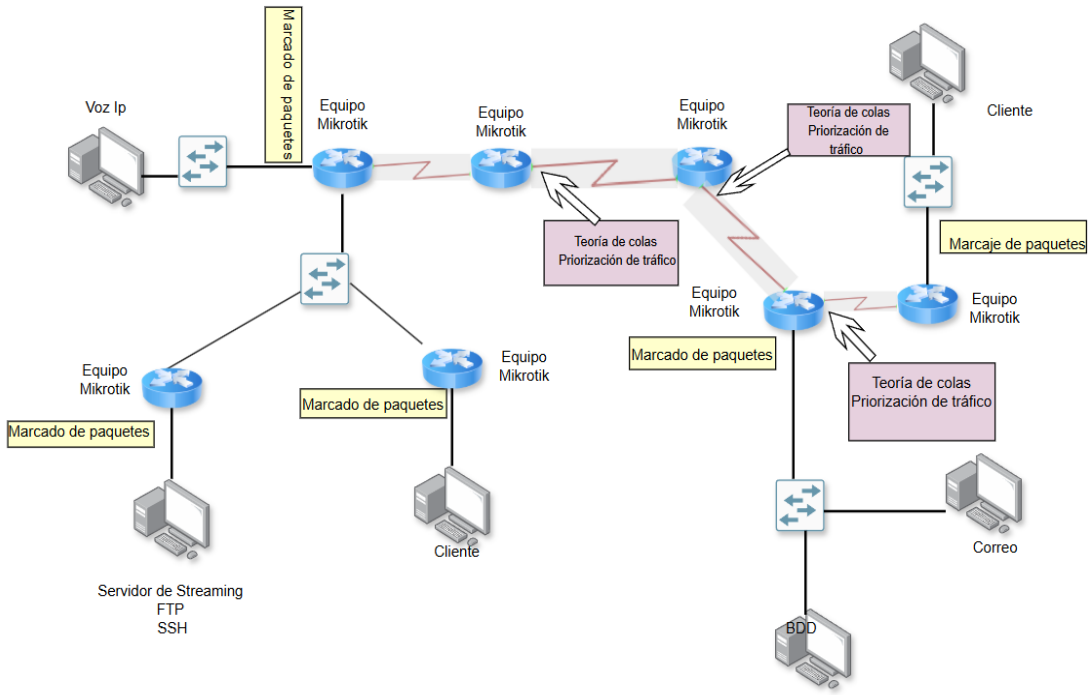
En la segunda fase de definición de requerimientos, se establecerán los aspectos relacionados con la calidad de servicio (QoS) de MikroTik para la gestión del tráfico multimedia en redes virtualizadas, considerando las diferencias con soluciones de alto rendimiento. Los requerimientos incluirán la necesidad de realizar una auditoría de red para identificar y analizar métricas clave como latencia, jitter, pérdida de paquetes y ancho de banda, estableciendo una línea base de rendimiento del tráfico. Se definirá la priorización de tráfico, con el objetivo de garantizar un tratamiento preferencial para aplicaciones críticas como VoIP y videoconferencias, que son sensibles a la variación en el retardo. Además, se establecerá el marcado de paquetes mediante estándares como DSCP para diferenciar y clasificar el tráfico según su importancia y nivel de prioridad. Asimismo, se definirá la clasificación del tráfico, segmentando y organizando los distintos tipos de datos con base en sus características y requerimientos específicos. Por último, se determinarán los requerimientos de gestión de colas, proponiendo el uso de técnicas como Low Latency Queuing (LLQ) y Weighted Fair Queuing (WFQ), para garantizar que el tráfico multimedia cuente con un tratamiento eficiente y prioritario. Estos requerimientos permitirán sentar las bases para un análisis comparativo con soluciones de alto rendimiento, identificando las capacidades y limitaciones de MikroTik en escenarios críticos de tráfico multimedia.

En la tercera fase, se procederá al diseño e implementación de una topología de red virtualizada que integre routers MikroTik con el propósito de analizar y aplicar los parámetros de calidad de servicio (QoS). En un primer escenario, se implementará una topología básica

sin configuraciones de QoS ni herramientas de auditoría, con el objetivo de analizar el comportamiento del tráfico en condiciones estándar. Durante esta etapa, se evaluarán métricas clave como la pérdida de paquetes, jitter, latencia y el uso del ancho de banda, estableciendo una línea base para comparaciones futuras. En el segundo escenario, se configurarán las herramientas de QoS y auditorías previamente definidas para priorizar aplicaciones críticas como VoIP y Streaming, aplicando técnicas avanzadas como LLQ (Low Latency Queuing) y marcaje de paquetes (DSCP). Estas configuraciones permitirán gestionar la congestión, el uso del ancho de banda y analizar las mejoras en el rendimiento del tráfico. En la **Figura 1** se presenta la topología de red virtualizada para gestión de tráfico multimedia.

Figura 1

Topología de red virtualizada para gestión de tráfico multimedia



Nota: *El gráfico muestra la arquitectura de una red con equipos Mikrotik, destacando la conectividad entre servicios como Voz Ip, Streaming, Correo y Base de Datos.* Fuente: Autoría propia

En la fase de pruebas, se llevarán a cabo pruebas de desempeño y estabilidad en las configuraciones de calidad de servicio (QoS) de routers MikroTik, específicamente dentro de redes virtualizadas. Estas pruebas se enfocarán en evaluar la efectividad del dispositivo en la gestión de tráfico multimedia, considerando factores clave como la latencia, el jitter, la pérdida de paquetes y la capacidad de priorización del tráfico. Se establecerán escenarios de prueba representativos de entornos virtualizados, en los que se simularán diversas cargas de tráfico multimedia como VoIP y videoconferencias, para luego comparar el rendimiento del dispositivo en dos escenarios diferentes.

1.5.Justificación

El presente proyecto está alineado con el Objetivo de Desarrollo Sostenible (ODS) 9, que promueve "la construcción de infraestructuras resilientes, la promoción de la industrialización inclusiva y sostenible, y la innovación" (UNIDAS, 2015)**.** En particular, se enfoca en ofrecer soluciones accesibles para la mejora de la calidad de los servicios en redes virtualizadas, apoyando a las organizaciones con recursos limitados a implementar tecnologías eficientes. La investigación busca evaluar alternativas económicas como los routers MikroTik**,** comparándolos con soluciones más costosas como Cisco, con el objetivo de asegurar que las organizaciones, en especial las pequeñas y medianas empresas, puedan mantener altos estándares de calidad de servicio (QoS) en aplicaciones críticas como VoIP y video en tiempo real. Al demostrar que MikroTik puede gestionar eficientemente el tráfico multimedia en entornos virtualizados, se contribuye a la sostenibilidad y competitividad de estas organizaciones.

La tecnología de redes multimedia, que exige una gestión eficiente de recursos como ancho de banda, latencia y jitter, se ha visto dominada por equipos de alto costo como los de Cisco, conocidos por su robustez en la gestión de QoS. Sin embargo, las organizaciones con presupuestos limitados necesitan soluciones alternativas que les permitan acceder a redes de calidad sin comprometer el rendimiento. MikroTik ofrece configuraciones de QoS competitivas a un menor costo, pero la información sobre su desempeño en comparación con Cisco en entornos virtualizados aún es insuficiente. Este estudio proporciona una comparación detallada, evaluando el rendimiento y las limitaciones de cada solución, y determinando la viabilidad de MikroTik como opción económica y eficiente en entornos de alta demanda. La teoría detrás de la QoS en redes multimedia subraya la importancia de asegurar la calidad en la transmisión de datos en tiempo real, especialmente en aplicaciones sensibles. Cisco ha sido

considerado un estándar en la gestión de QoS, mientras que MikroTik ha ganado popularidad por su accesibilidad y flexibilidad. Sin embargo, existe una brecha en la literatura sobre cómo estas dos plataformas se comportan en entornos virtualizados, lo que dificulta la toma de decisiones informadas por parte de las organizaciones. Este proyecto amplía el conocimiento teórico al simular y analizar la QoS en ambos sistemas, proporcionando datos concretos sobre su rendimiento en escenarios de redes virtualizadas, lo que enriquecerá la comprensión sobre sus ventajas y limitaciones en términos de costos y eficiencia.

Capítulo II. Fundamentación Teórica

En este capítulo, se partirá de la problemática identificada, la cual radica en la percepción y uso de dispositivos de red. Los dispositivos Mikrotik, aunque son considerablemente más económicos en comparación con los de Cisco, suelen ser subestimados debido a la falta de investigaciones profundas y estudios técnicos que respalden su desempeño, especialmente en términos de calidad de servicio (QoS). Esta situación lleva a que muchas corporaciones, instituciones educativas y organizaciones opten por soluciones de mayor costo, como los dispositivos de Cisco, bajo la premisa de que ofrecen mejor rendimiento y fiabilidad.

Con esta problemática como punto de partida, se propone una investigación exhaustiva orientada a evaluar la calidad de servicio (QoS) en dispositivos Mikrotik. El objetivo principal es demostrar que, a través de configuraciones adecuadas y un conocimiento técnico sólido, es posible alcanzar niveles de desempeño similares o incluso superiores a los que ofrecen otras marcas reconocidas. De esta manera, se busca contribuir a la toma de decisiones más informadas y a la optimización de recursos en las organizaciones que requieren implementar servicios de comunicación multimedia y redes de alta calidad.

2.1 Concepto de calidad de servicio

La calidad de servicio se refiere al conjunto de mecanismos, políticas y técnicas implementadas dentro de una red con el propósito de garantizar el rendimiento adecuado de ciertos servicios, en especial aquellos sensibles al retardo como la voz, el video en tiempo real o las transmisiones interactivas. Su función principal es asegurar que los recursos de red sean utilizados de manera eficiente y que los flujos de datos críticos reciban el tratamiento adecuado según sus necesidades.

De acuerdo con la Unión Internacional de Telecomunicaciones (ITU-T), la QoS puede definirse como el efecto conjunto del desempeño de un servicio que influye directamente en el nivel de satisfacción percibido por el usuario final (ITU-T, 2008).

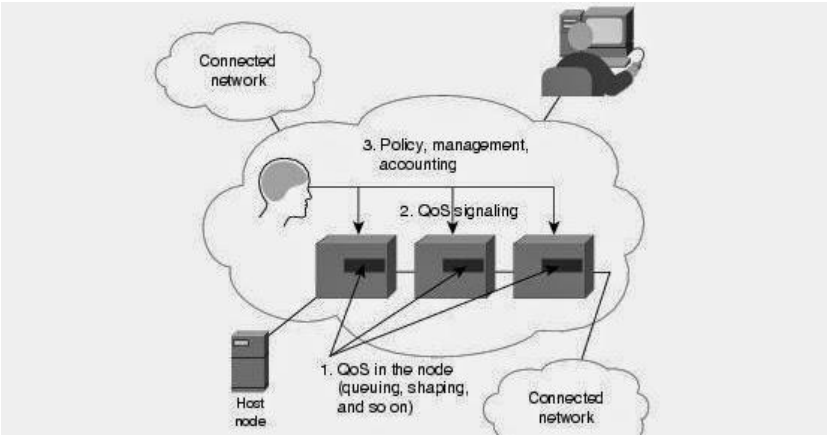
Por su parte, el Grupo de Trabajo de Ingeniería de Internet (IETF), a través del documento RFC 2386, define QoS como el conjunto de requisitos que una red debe cumplir para asegurar un transporte adecuado de los flujos de información, permitiendo así cumplir con las expectativas del servicio (Boutros & Eastlake, 2024).

Desde una perspectiva más técnica, la calidad de servicio representa la capacidad de una red para gestionar y controlar parámetros como el ancho de banda, la latencia, el jitter y la pérdida de paquetes. Esto permite que las redes brinden soporte eficiente a múltiples tipos de tráfico simultáneamente, priorizando aquellos que requieren mayor fiabilidad y consistencia en su entrega (Forouzan & Fegan, 2007).

2.2 Arquitectura de QoS

Figura 2

Esquema general de la arquitectura de calidad de servicio



Nota: *La figura representa los tres niveles funcionales para la gestión de QoS: mecanismos en el nodo, señalización y políticas de control.*

Fuente**:** Espinosa, A. (2015, abril 18). *Arquitectura básica de QoS*. QoS-Informática. Recuperado de https://qos-informatica.blogspot.com/2015/04/arquitectura-basica-de-qos.html

Dentro de la arquitectura básica de Calidad de Servicio (QoS), presentada en la **Figura 2**, se identifican tres componentes fundamentales que permiten garantizar una adecuada administración y entrega del tráfico dentro de la red. Estos componentes trabajan de manera conjunta para optimizar el rendimiento de los servicios y asegurar una utilización eficiente de los recursos de red.

- **Mecanismos de QoS en dispositivos individuales:** Incluyen técnicas como el encolamiento, la planificación del tráfico y herramientas para su modelado, aplicadas dentro de un solo nodo de red.
- **Coordinación mediante señalización entre nodos:** Utiliza protocolos específicos para garantizar la entrega de datos de extremo a extremo, asegurando que cada elemento de la red responda de manera coherente a los requerimientos del servicio.
- **Políticas de administración de QoS:** Encargadas de gestionar y controlar el tráfico en toda la red mediante reglas definidas, permitiendo priorizar servicios y optimizar el uso de los recursos sobre una infraestructura compartida.

2.3 Normativas de QoS

Las redes actuales y de próxima generación requieren garantizar una Calidad de Servicio (QoS) diferenciada, confiable y eficiente, especialmente para aplicaciones sensibles al retardo como voz, video y servicios multimedia. Para lograr una implementación adecuada de QoS en redes IP, es necesario que los proveedores adopten parámetros estandarizados que permitan evaluar objetivamente el desempeño en la transmisión de datos.

En este contexto, organismos internacionales como la Unión Internacional de Telecomunicaciones han establecido normativas que definen los fundamentos y métricas de QoS. Entre las principales se encuentran ITU-T E.800, que conceptualiza la calidad de servicio

desde la perspectiva del usuario; ITU-T Y.1540, que establece los parámetros de medición como retardo, jitter y pérdida de paquetes; y ITU-T Y.1541, que define clases de servicio con niveles de desempeño específicos según el tipo de aplicación.

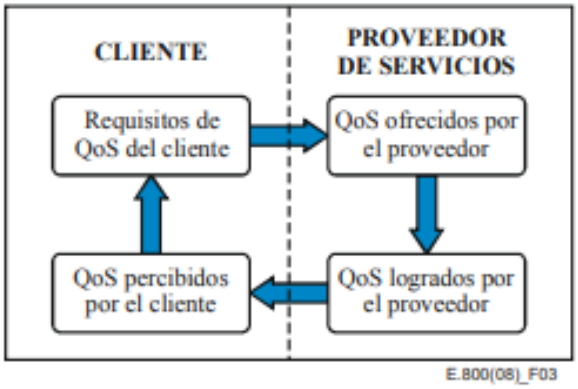
2.3.1 ITU-T E.800

La Recomendación ITU-T E.800 establece el marco conceptual de la calidad de servicio en telecomunicaciones, definiéndola como la totalidad de las características de un servicio que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario. Asimismo, define la calidad de funcionamiento de la red (Network Performance, NP) como la aptitud de una red o de una parte de ella para ofrecer las funciones de comunicación entre usuarios. Desde esta perspectiva, la QoS de extremo a extremo no depende únicamente del desempeño técnico de la red principal, sino también de la contribución de los equipos terminales y de las redes de acceso involucradas en la comunicación (ITU-T E.800, 2008).

Adicionalmente, la ITU-T E.800 propone un modelo de cuatro polos de la calidad de servicio, conformado por los requisitos de QoS del usuario o cliente (QoSR), la QoS ofrecida por el proveedor (QoSO), la QoS proporcionada o lograda (QoSD) y la QoS percibida por el usuario (QoSE). Este modelo permite analizar la calidad desde una visión integral, considerando tanto los valores técnicos medibles como la experiencia final del usuario. De igual forma, la recomendación diferencia parámetros objetivos, cuantificables mediante mediciones, y parámetros subjetivos, asociados a la percepción y opinión del usuario (ITU-T E.800, 2008).

Figura 3

Cuatro polos de calidad de Servicio



Nota: *Tomado de (ITU-T E.800, 2008)*

La **Figura 3** presenta los cuatro polos de la calidad de servicio definidos por la ITU-T E.800: la QoS requerida por el usuario, la QoS ofrecida por el proveedor, la QoS proporcionada y la QoS percibida. Este modelo evidencia que la calidad no debe analizarse solo desde el punto de vista técnico, sino también desde la comparación entre lo esperado, lo ofrecido, lo entregado y lo finalmente experimentado por el usuario.

Tabla 1

Cuatro polos de la QoS según la ITU-T E.800

Polos de QoS	Definición resumida	Enfoques
QoSR	Requisitos de calidad del usuario o cliente	Expectativa
QoSO	Nivel de calidad ofrecido o planificado por el proveedor	Compromiso
QoSD	Nivel de calidad realmente proporcionado	Desempeño medido
QoSE	Nivel de calidad experimentado o percibido por el usuario	Percepción

Nota: *Adaptado de la Recomendación ITU-T E.800.*

En la **Tabla 1** se presentan los cuatro polos de la QoS propuestos por la ITU-T E.800, los cuales permiten relacionar los requisitos del usuario con la calidad ofrecida, proporcionada y percibida del servicio.

2.3.2 ITU-T Y.1540

La Recomendación ITU-T Y.1540 define los parámetros que pueden utilizarse para especificar y evaluar el desempeño de la transferencia de paquetes IP en términos de velocidad, exactitud, confiabilidad y disponibilidad. Estos parámetros son aplicables tanto al servicio IP extremo a extremo, punto a punto, como a las distintas porciones de red que contribuyen a la provisión de dicho servicio. Asimismo, la recomendación considera como rasgo distintivo del servicio IP su naturaleza no orientada a conexión (ITU-T Y.1540, 2007).

Para ello, la norma establece un modelo general de desempeño del servicio IP basado en puntos de medición (MP, Measurement Points)**,** eventos de referencia de transferencia de paquetes IP (IPRE, IP packet transfer reference events) y los posibles resultados de transferencia de paquetes. A partir de este modelo, se definen parámetros de evaluación como el retardo de transferencia de paquetes IP (IPTD)**,** la variación del retardo de paquetes (PDV/IPDV)**,** la tasa de errores de paquetes IP (IPER) y la tasa de pérdida de paquetes IP (IPLR)**,** así como parámetros relacionados con el reordenamiento, duplicación y disponibilidad del servicio.

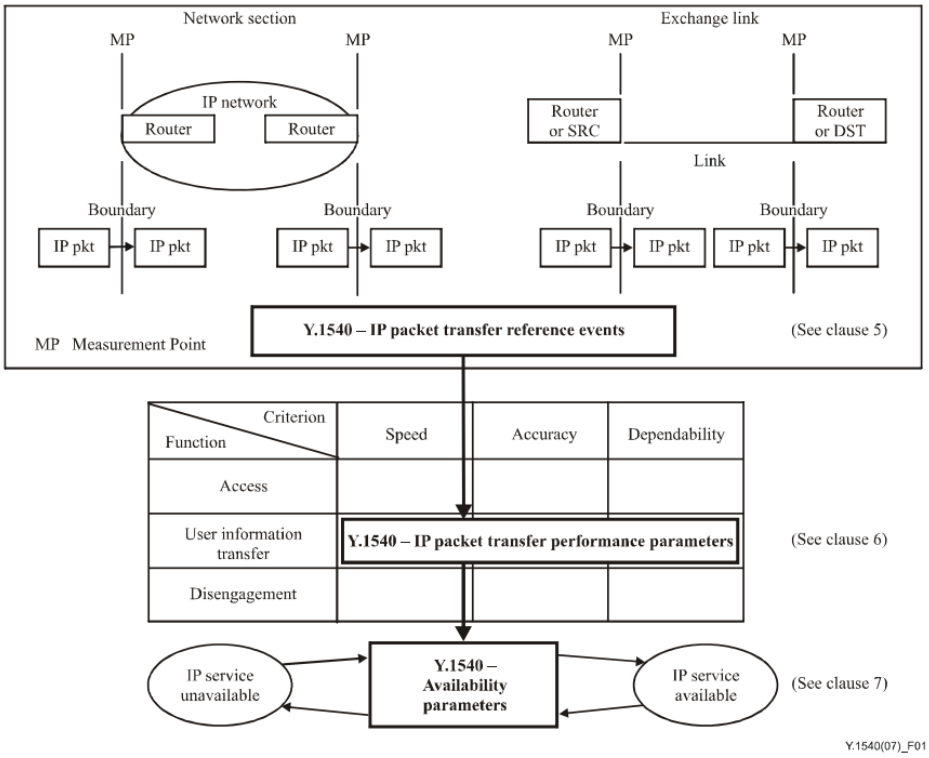
De forma complementaria, la Y.1540 incorpora una definición formal de disponibilidad del servicio IP basada en el comportamiento de la pérdida de paquetes. Para ello utiliza una función de disponibilidad sustentada en un umbral de IPLR, mediante la cual el servicio puede clasificarse en estado disponible o indisponible durante intervalos de observación determinados. Sobre esta base se definen el porcentaje de disponibilidad del servicio IP (PIA)

y el porcentaje de indisponibilidad del servicio IP (PIU**)**. La recomendación establece de forma provisional un criterio de indisponibilidad cuando el valor de IPLR supera el umbral c1 = 0.75, considerando además un intervalo mínimo de evaluación Tav = 5 minutos. Para tráfico generado por el usuario final, se sugiere un mínimo de 1000 paquetes para evaluar dicho estado.

En la **Figura 4** se presenta el alcance general de la Recomendación ITU-T Y.1540. En la parte superior se muestran los componentes de red, los enlaces de intercambio, las secciones de red y los puntos de medición que sirven de base para observar los eventos de referencia de transferencia de paquetes IP. En la parte central se representa la matriz de desempeño 3 × 3, donde se relacionan las funciones de acceso, transferencia de información del usuario y finalización de la conexión con los criterios de velocidad, exactitud y confiabilidad. Finalmente, en la parte inferior se incorpora el modelo de disponibilidad del servicio IP, que permite clasificar el servicio en estado disponible o no disponible.

Figura 4

Modelo de referencia para la evaluación del rendimiento en la transferencia de paquetes IP según la recomendación ITU-T Y.1540.



Nota: *Tomado de (ITU-T Y.1540, 2007)*

En la **Tabla 2** se resumen los elementos principales del modelo definido por la Y.1540. Esta estructura conceptual permite describir la red IP en términos observables y medibles, facilitando la identificación de los puntos donde pueden evaluarse el retardo, la pérdida y otros comportamientos asociados a la transferencia de paquetes.

Tabla 2

Elementos del modelo de desempeño IP según la ITU-T Y.1540

Elemento	Definición resumida	Función en la evaluación
SRC	Host de origen	Punto desde donde se generan los paquetes IP

DST	Host de destino	Punto donde finaliza la transferencia
Router	Dispositivo de encaminamiento	Reenvía paquetes según la dirección destino
EL	Enlace de intercambio	Conecta hosts o secciones de red
NS	Sección de red	Conjunto de hosts y enlaces bajo una misma responsabilidad
NSE	Conjunto de secciones de red	Subconjunto conectado de NS y EL
MP	Punto de medición	Límite donde se observan los eventos de referencia
IPRE	Evento de referencia de transferencia	Base para medir desempeño de la transferencia IP

Nota: *Adaptado de la Recomendación ITU-T Y.1540*

La **Tabla 3** presenta los parámetros más importantes definidos por la Y.1540. Aunque la recomendación contempla varios indicadores, en esta investigación adquieren especial relevancia el IPTD, el PDV/IPDV, el IPLR y los parámetros de disponibilidad, debido a su relación directa con el comportamiento de aplicaciones multimedia sensibles al tiempo real.

Tabla 3

Parámetros principales definidos por la ITU-T Y.1540

Parámetro	**Nombre**	**Qué evalúa**	**Aplicación en Tesis**
IPTD	Retardo de transferencia de paquetes IP	Tiempo que tarda un paquete en llegar al destino	Latencia
PDV / IPDV	Variación del retardo de paquetes	Variabilidad temporal del retardo	Jitter

IPER	Tasa de error de paquetes IP	Integridad de la información entregada	Errores de transmisión
IPLR	Tasa de pérdida de paquetes IP	Proporción de paquetes perdidos	Calidad de voz y video
IPRR	Tasa de paquetes reordenados	Entrega fuera de secuencia	Flujo multimedia
IPDR	Tasa de paquetes duplicados	Repetición de paquetes	Eficiencia del transporte
RIPR	Tasa de paquetes replicados	Aparición de múltiples copias del mismo paquete	Anomalías de red
IPSLBR	Tasa de bloques severos de pérdida	Episodios de pérdida elevada en intervalos de tiempo	Degradación severa del servicio
PIA	Porcentaje de disponibilidad del servicio IP	Tiempo en estado disponible	Continuidad del servicio
PIU	Porcentaje de indisponibilidad del servicio IP	Tiempo en estado no disponible	Interrupciones del servicio

Nota: *Adaptado de la Recomendación ITU-T Y.1540*

La **Tabla 4** resume los parámetros utilizados por la Y.1540 para evaluar la disponibilidad del servicio IP. Estos elementos permiten complementar el análisis del

desempeño de la red, al considerar no solo la calidad de la transferencia de paquetes, sino también la continuidad operativa del servicio durante el tiempo de observación

Tabla 4

Parámetros de disponibilidad del servicio IP según la ITU-T Y.1540

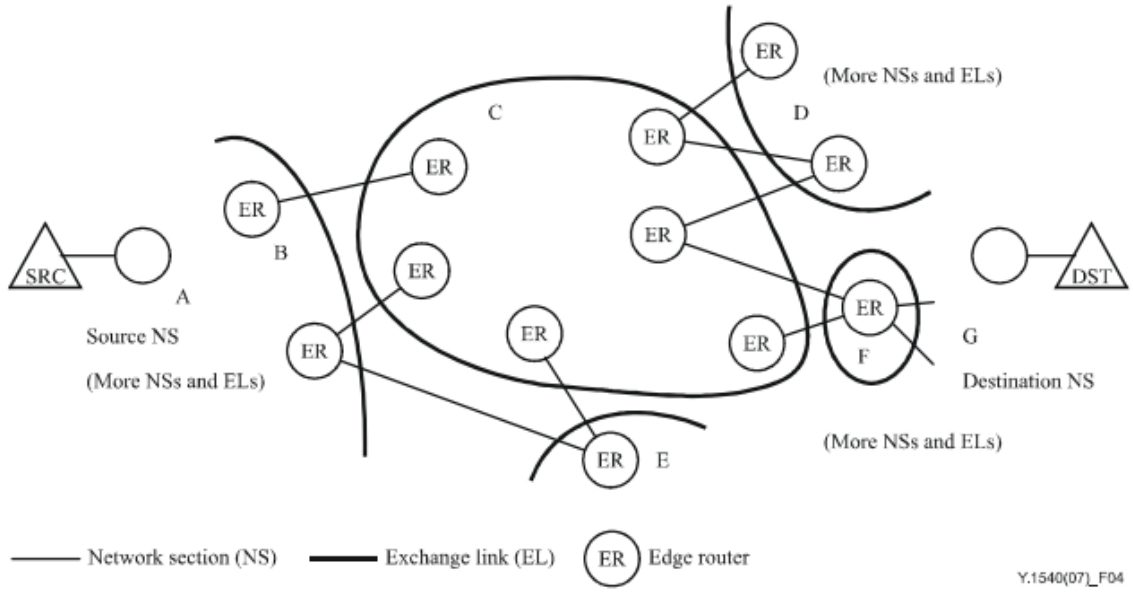
Concepto	Descripción
c1	Umbral de IPLR para declarar indisponibilidad del servicio
Tav	Intervalo mínimo para evaluar el estado de disponibilidad
Mav	Número mínimo de paquetes recomendado para evaluar disponibilidad
PIA	Porcentaje del tiempo en que el servicio está disponible
PIU	Porcentaje del tiempo en que el servicio está indisponible.

Nota: *Adaptado de la Recomendación ITU-T Y.1540.*

En la **Figura 5** se ilustra la conectividad de una red IP entre el host de origen y el host de destino, mostrando la relación entre las secciones de red, los enlaces de intercambio y los routers de borde. Esta representación permite comprender cómo se estructura el trayecto seguido por los paquetes y en qué puntos pueden ubicarse las mediciones empleadas para evaluar el desempeño de la red.

Figura 5

Conectividad de red IP entre el host de origen y el host de destino según la ITU-T Y.1540

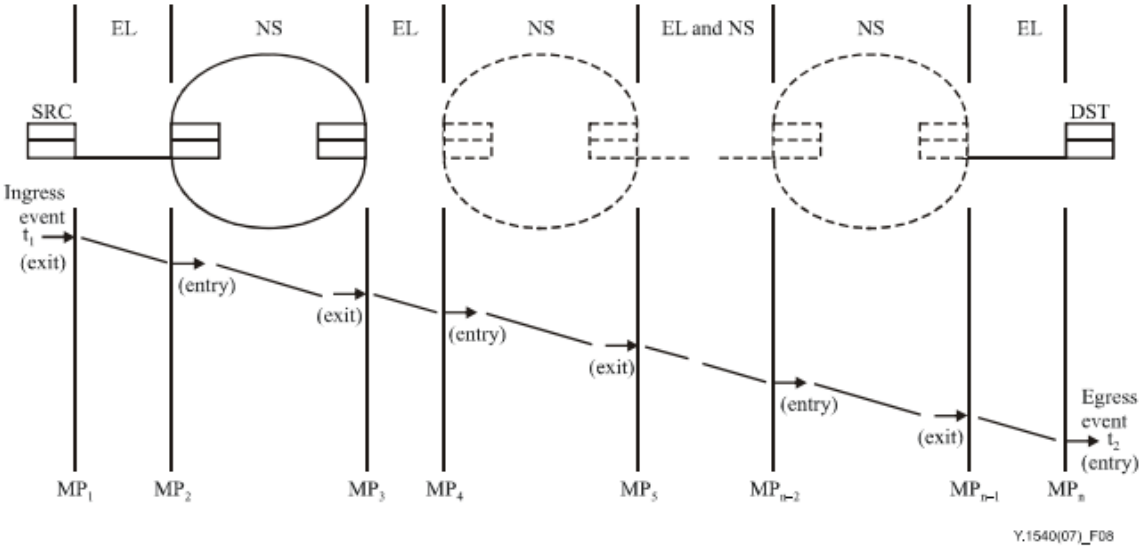


Nota: *Adaptado de la* ***Figura 4*** *de la Recomendación ITU-T Y.1540.*

Dentro la **Figura 6** se representan los eventos de referencia utilizados por la Recomendación ITU-T Y.1540 para determinar el retardo de transferencia de paquetes IP (IPTD). En ella se observa el recorrido del paquete desde el host de origen hasta el host de destino a través de diferentes puntos de medición, permitiendo identificar el instante de ingreso y el instante de egreso que sirven de base para calcular el tiempo total de transferencia.

Figura 6

Eventos de referencia para la determinación del retardo de transferencia de paquetes IP (IPTD)



Nota: *Adaptado de la* ***Figura 8*** *de la Recomendación ITU-T Y.1540.*

2.3.3 ITU-T Y.1541

La Recomendación ITU-T Y.1541 complementa a la Y.1540 al establecer objetivos de desempeño para los parámetros de calidad de funcionamiento de redes IP. Mientras la Y.1540 define los indicadores técnicos que deben medirse, la Y.1541 fija los valores de referencia que permiten determinar el nivel de calidad que una red puede ofrecer. Para ello, la recomendación organiza estos objetivos en seis clases de QoS, cada una asociada a diferentes exigencias de servicio y tipos de aplicación.(ITU-T Y.1541, 2002).

En la **Tabla 5** se presentan las clases de QoS definidas por la Y.1541 junto con los objetivos de desempeño correspondientes para parámetros como el retardo de transferencia de paquetes IP (IPTD), la variación del retardo (IPDV), la tasa de pérdida de paquetes (IPLR) y la tasa de error de paquetes (IPER). A partir de estos valores, es posible observar que las clases 0 y 1 imponen condiciones más estrictas en términos de retardo y jitter, por lo que resultan especialmente adecuadas para aplicaciones multimedia en tiempo real, como la voz sobre IP y

la videoconferencia. En cambio, las clases 2, 3 y 4 responden a requerimientos menos rigurosos en cuanto a variación del retardo, mientras que la clase 5 representa un servicio sin valores objetivo especificados para estos parámetros.

Tabla 5

Clases de QoS y objetivos de desempeño de red según la ITU-T Y.1541

Parámetro	Clase 0	Clase 1	Clase 2	Clase 3	Clase 4	Clase 5
IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	50 ms	50 ms	U	U	U	U
IPLR	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	U
IPER	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	U

Nota: *Adaptado de la Recomendación ITU-T Y.1541. La letra U indica que el parámetro no se encuentra especificado.*

Además de definir objetivos cuantitativos, la Y.1541 incorpora la posibilidad de relacionar sus clases de QoS con los mecanismos de Servicios Diferenciados (DiffServ) propuestos por la IETF. Esta relación resulta importante porque permite trasladar el enfoque normativo a mecanismos concretos de tratamiento del tráfico dentro de la red. En la **Tabla 6** se muestra la asociación entre las clases de QoS de la Y.1541 y los comportamientos de reenvío utilizados en DiffServ.

Tabla 6

Relación entre clases de QoS de la ITU-T Y.1541 y mecanismos DiffServ

PHB / DiffServ	Clases de QoS asociadas	Interpretación
Best Effort (BE)	Clase 5	Tráfico sin garantías estrictas de QoS
Assured Forwarding (AF)	Clases 2, 3 y 4	Tráfico con tratamiento preferencial y control de pérdida

Expedited Forwarding (EF)	Clases 0 y 1	Tráfico en tiempo real con prioridad alta

Nota: *Adaptado del Apéndice VI de la Recomendación ITU-T Y.1541*

Como se observa en la **Tabla 6**, la clase 5 se vincula con el tratamiento Best Effort, las clases 2, 3 y 4 se relacionan con Assured Forwarding (AF), y las clases 0 y 1 con Expedited Forwarding (EF). Esta correspondencia es especialmente relevante para la presente investigación, ya que permite interpretar los resultados de desempeño no solo desde un punto de vista teórico, sino también en función de mecanismos de priorización de tráfico que pueden ser implementados en entornos MikroTik.

2.4 Modelos de QoS

Los modelos de Calidad de Servicio son marcos conceptuales y técnicas que se utilizan en redes de comunicación para gestionar y priorizar el tráfico de datos. Su propósito principal es garantizar que ciertos tipos de datos (como voz, video o aplicaciones críticas) tengan los recursos necesarios para funcionar de manera óptima, minimizando problemas como retrasos, pérdida de paquetes o fluctuaciones en la red (Stanley, 2022). En las redes IP convencionales se utilizaba por defecto el modelo *Best-Effort* o "mejor esfuerzo", en el que todos los paquetes tenían igual prioridad al atravesar los enrutadores, por lo que debían disputar los mismos recursos de la red.

2.4.1 Modelo de Servicios Integrados (IntServ)

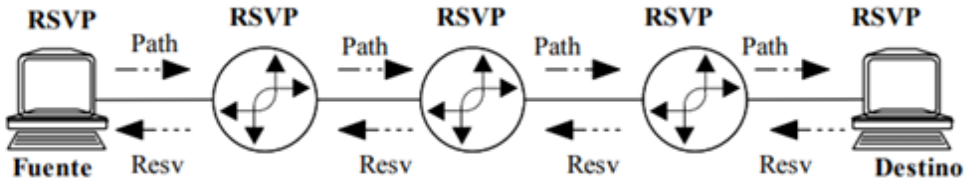
El modelo Integrated Services (IntServ), también conocido como modelo de QoS rígido (hard QoS model), se basa en la gestión de flujos de datos individuales definidos por las direcciones IP y puertos de origen y destino. En este modelo, las aplicaciones son responsables de solicitar una reserva explícita de recursos para cada flujo de datos. Emplea el protocolo de

reserva de recursos (RSVP) mediante el cual la aplicación envía una solicitud a la red para obtener un servicio determinado, asegurando un ancho de banda específico y un límite máximo de retardo aceptable, como se puede observar en la **Figura 7**.

Sin embargo, aunque IntServ permite ofrecer garantías estrictas de QoS por flujo, su principal limitación es la baja escalabilidad**,** debido a que cada flujo requiere señalización, mantenimiento de estado y reserva individual de recursos en los dispositivos de red.

Figura 7

Esquema de funcionamiento del modelo de Servicios Integrados (IntServ)



Nota: *Adaptado de (Moncayo, 2025), a partir de un esquema del intercambio de mensajes RSVP en el modelo IntServ.*

El esquema ilustra el funcionamiento del modelo de Servicios Integrados (IntServ) a través del intercambio de mensajes del protocolo RSVP, destacando la intervención de los sistemas finales en el proceso de solicitud y establecimiento de recursos para cada flujo de datos.

2.4.2 Modelo de Servicios Diferenciados (DiffServ)

El modelo Differentiated Services (DiffServ) surge como una alternativa al problema de escalabilidad presentado por IntServ, ya que no realiza reservas de recursos para cada flujo individual, si no que agrupa los paquetes en clases de tráfico y les asigna un tratamiento diferenciado. En este modelo, la prioridad de cada paquete se define mediante su marcado en

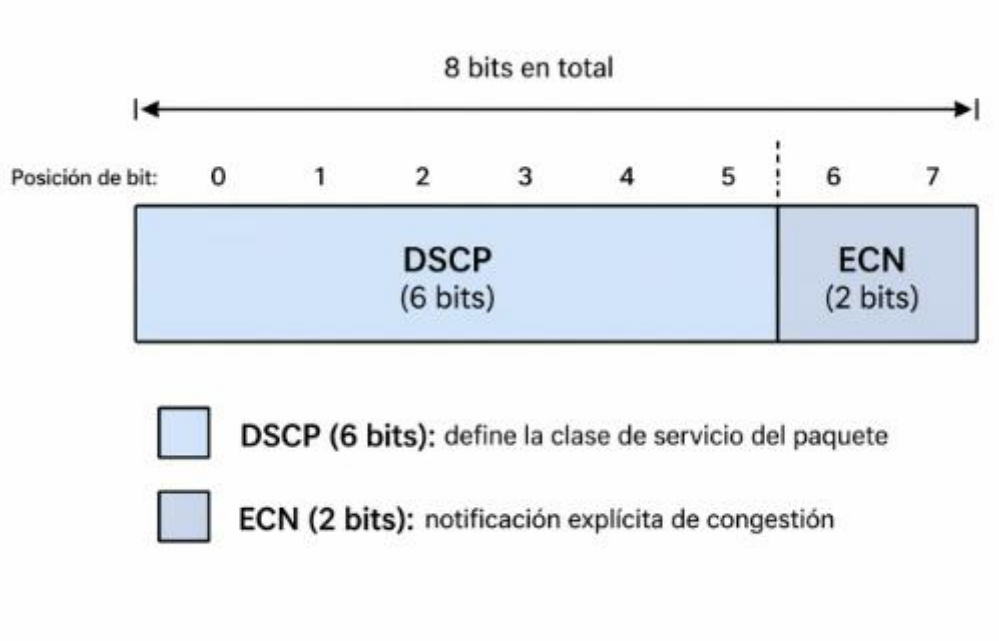
el encabezado IP, lo que permite a los nodos aplicar políticas de QoS de acuerdo con la clase de servicio configurada (Stanley, 2022).

En DiffServ, el tratamiento aplicado a los paquetes se conoce como Per-Hop Behavior (PHB), ya que cada dispositivo de red ejecuta una acción específica sobre un conjunto de paquetes que comparten la misma prioridad. Entre los PHB más utilizados se encuentran Best Effort (BE), Class Selector (CS)**,** Assured Forwarding (AF) y Expedited Forwarding (EF), los cuales permiten establecer distintos niveles de prioridad y tratamiento del tráfico dentro de la red.

Para implementar este mecanismo, DiffServ utiliza el campo DSCP**,** ubicado en el encabezado IP. Este campo está formado por 6 bits, mientras que los 2 bits restantes corresponden al campo ECN. El valor de DSCP permite identificar la clase de servicio asociada a cada paquete y, con ello, aplicar el comportamiento por salto correspondiente (Chan et al., 2003). Cabe señalar que el DSCP no constituye un PHB por sí mismo, sino que funciona como un marcador que permite a los dispositivos de red reconocer la prioridad del paquete y aplicar el tratamiento adecuado.

Figura 8

Estructura del campo DiffServ en el encabezado IP



Nota: *Adaptado de Cisco Systems, (2005)*

La **Figura 8** muestra la estructura del campo de servicios diferenciados en el encabezado IP. En él, los primeros seis bits corresponden al DSCP, utilizado para definir la clase de servicio del paquete, mientras que los dos bits restantes corresponden al ECN, empleado para la notificación explícita de congestión.

Los PHB más utilizados en el modelo DiffServ son Best Effort (BE), Class Selector (CS), Expedited Forwarding (EF) y Assured Forwarding (AF). Cada uno de ellos define un tratamiento distinto para los paquetes dentro de la red, según la prioridad asignada y los requerimientos del servicio. En la **Tabla 7** se resumen sus principales características y aplicaciones.

Tabla 7

Principales PHB utilizados en DiffServ

PHB	Descripción	Formato DSCP	Aplicación general
Best Effort (BE)	Corresponde al servicio por defecto y se aplica al tráfico que no posee una política específica de prioridad.	000000	Navegación y tráfico general
Class Selector (CS)	Se utiliza para mantener compatibilidad con el esquema de precedencia IP.	xxx000	Tráfico clasificado por niveles
Assured Forwarding (AF)	Permite establecer distintas clases de servicio con diferentes niveles de prioridad y descarte.	AFxy	Datos, video y aplicaciones con prioridad diferenciada
Expedited Forwarding (EF)	Proporciona tratamiento preferencial con baja latencia, baja pérdida y menor variación del retardo.	101110	Voz sobre IP y tráfico sensible al retardo

Nota: *Adaptado de Cisco Systems (2005)*

En términos generales, los PHB hacen posible que la red trate de forma distinta a los paquetes según su prioridad. Esto favorece a aplicaciones como la voz y el video, que requieren menor retardo y un tratamiento más estable. Por esta razón, DiffServ constituye una opción escalable para aplicar QoS en redes IP sin reservar recursos de manera individual para cada flujo.

2.5 Teoría de Colas en Redes de Comunicación

La teoría de colas aplicada a la Calidad de Servicio en redes permite gestionar el tráfico de datos de manera eficiente, priorizando ciertos tipos de información y optimizando el uso de los recursos. En estos sistemas, los paquetes de datos actúan como clientes que deben ser procesados por un servidor, y si la tasa de llegada supera la capacidad del dispositivo, se almacenan en una cola hasta ser atendidos. La forma en que se gestionan estas colas influye en el rendimiento de la red y la experiencia del usuario, por lo que la teoría de colas en QoS analiza aspectos como el tiempo de espera de los paquetes, el número de paquetes en el sistema y la utilización de los servidores. A través de diversas técnicas de encolado, se pueden priorizar servicios críticos como voz y video para garantizar su calidad, asegurando una distribución eficiente de los recursos, evitando pérdidas de paquetes y manteniendo un rendimiento óptimo en entornos de alto tráfico, como los sistemas de comunicación multimedia (Paspuel, 2014).

2.5.1 Elementos básicos de la teoría de colas

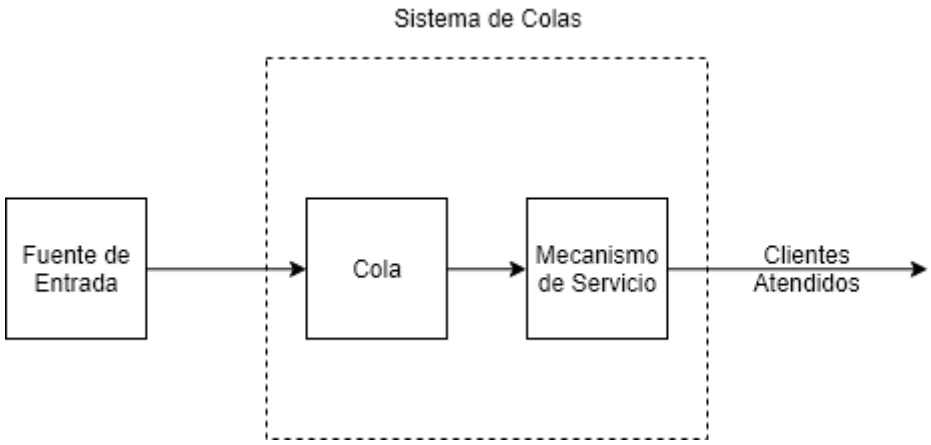
Un sistema de colas aplicado a redes de comunicación está conformado por varios elementos que permiten describir la forma en que los paquetes ingresan, esperan, son procesados y finalmente salen del sistema. Entre sus componentes principales se encuentran la fuente de llegada, la cola de espera, el servidor y el tiempo de servicio, los cuales determinan el comportamiento general del sistema y su desempeño (Medina, 2019).

En la **Figura 9** se presenta el modelo básico de un sistema de colas. En este esquema, la fuente de entrada representa el origen de los paquetes que ingresan al sistema; la cola corresponde al espacio donde permanecen en espera cuando el mecanismo de servicio se encuentra ocupado; y el mecanismo de servicio representa el recurso encargado de atender y procesar dichos paquetes. Una vez completado este proceso, los paquetes abandonan el sistema

como clientes atendidos. Este modelo permite comprender, de manera general, la dinámica de atención del tráfico en una red de comunicación.

Figura 9

Modelo básico de un sistema de colas aplicado a redes de comunicación



Nota: *Tomado de Medina (2019)*

2.5.1.1 Fuente de llegada de paquetes

La fuente de llegada representa el tráfico que ingresa a la red, generado por aplicaciones como videollamadas, descargas de archivos, navegación web o transmisión de datos en tiempo real, la llegada de paquetes no siempre es constante, por lo que suele modelarse con distribuciones probabilísticas, como el proceso de Poisson**,** que describe la llegada de eventos de manera aleatoria con una tasa promedio determinada (Medina, 2019).

2.5.1.2 Servidor de paquetes

El servidor es el componente encargado de procesar los paquetes dentro de la red. Dependiendo del tipo de sistema, un servidor puede ser un router, un switch o una estación base, que gestiona la transferencia de datos y su encaminamiento hacia el destino. La velocidad

y eficiencia del servidor influyen en el tiempo de respuesta de la red, afectando la Calidad de Servicio (QoS) (Medina, 2019).

2.5.1.3 Cola de espera

Cuando la cantidad de paquetes entrantes supera la capacidad del servidor, estos deben almacenarse en una cola de espera hasta que puedan ser procesados. La administración de esta cola se define mediante distintas políticas de encolado, como FIFO (First In, First Out), PQ (Priority Queuing) o WFQ (Weighted Fair Queuing**)**, que determinan qué paquetes se procesan primero y en qué condiciones (Medina, 2019).

2.5.1.4 Tiempo de servicio y salida

El tiempo de servicio corresponde al período necesario para que un servidor procese un paquete antes de enviarlo a su destino. Este tiempo varía según el tipo de tráfico, la capacidad del servidor y la carga de la red, una vez completado el proceso, el paquete sale del sistema y continúa su ruta hasta alcanzar su destino final. Reducir el tiempo de servicio y minimizar las colas de espera es esencial para mejorar el rendimiento de la red y evitar la congestión (Medina, 2019).

2.6 Técnicas de Encolado

Las técnicas de encolado permiten administrar el tráfico de red de manera eficiente, priorizando ciertos servicios y optimizando el uso del ancho de banda disponible. En MikroTik, estas funciones se implementan mediante mecanismos de Queue Tree, colas simples, marcado de paquetes y distintos tipos de cola, lo que permite diferenciar el tratamiento del tráfico según las necesidades de la red. Esta gestión resulta especialmente importante en entornos con aplicaciones multimedia y servicios en tiempo real, donde el retardo, el jitter y la pérdida de paquetes pueden afectar significativamente la calidad del servicio (Mikrotik, n.d.).

2.6.1 LLQ

El Low Latency Queuing (LLQ**)** es una técnica de encolado que mejora el Class-Based Weighted Fair Queuing (CBWFQ) al incorporar una cola de prioridad estricta, permitiendo que el tráfico sensible a la latencia, como la voz, se envíe antes que otros tipos de tráfico. Esta combinación asegura que los paquetes de voz y video se procesen con prioridad, reduciendo la latencia y la transmisión (Check Point Software Technologies, 2024).

En el caso de MikroTik, la gestión del tráfico y la calidad de servicio se implementa mediante el uso de Queue Tree y reglas de marcado de paquetes. Estas herramientas permiten crear estructuras jerárquicas de colas y asignar prioridades al tráfico, asegurando que el tráfico crítico reciba el tratamiento adecuado sin comprometer la eficiencia general de la red (Pulido, 2024)

Por lo tanto, tanto en dispositivos Cisco como en MikroTik, es posible configurar mecanismos que prioricen el tráfico sensible a la latencia, garantizando una calidad de servicio óptima para aplicaciones en tiempo real.

2.6.2 WFQ

Weighted Fair Queuing (WFQ) es un método de encolado utilizado en redes de comunicación para administrar el tráfico de manera equitativa, asignando diferentes niveles de prioridad a los paquetes según su importancia y el tipo de aplicación que los genera (Walton, 2023). A diferencia de otros esquemas que distribuyen el ancho de banda de manera uniforme, WFQ ajusta dinámicamente los recursos disponibles, asegurando que servicios sensibles a la latencia, como VoIP, videoconferencias y tráfico interactivo, tengan prioridad sobre transferencias de archivos o tráfico de gran volumen. Este método organiza los paquetes en

colas separadas basándose en direcciones IP, puertos y protocolos, permitiendo que las aplicaciones críticas mantengan su estabilidad incluso en escenarios de congestión.

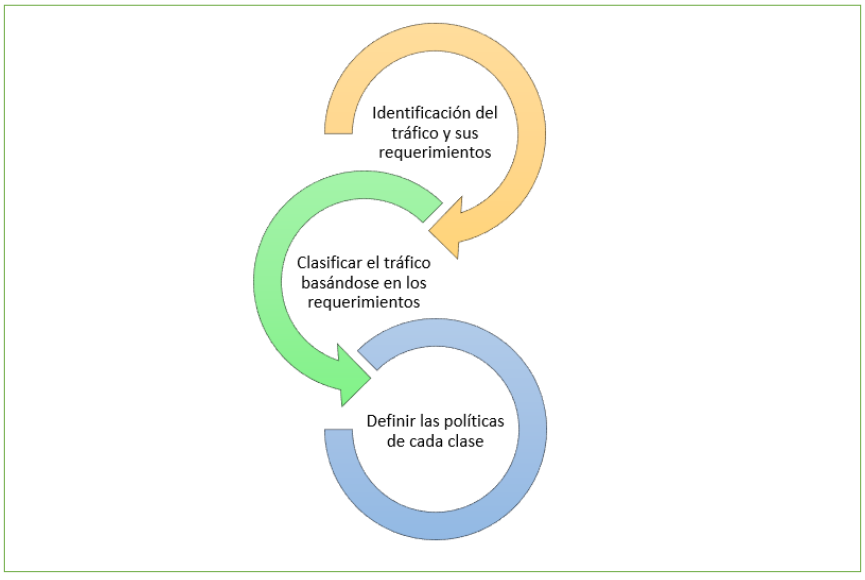
Sin embargo, WFQ tiene ciertas limitaciones, como su incompatibilidad con tráfico encriptado o tunelado, ya que su clasificación se basa en la lectura del encabezado de los paquetes, lo que puede afectar su desempeño en redes que emplean VPN o IPSec. Además, en entornos con alto tráfico, la administración automática de recursos puede no ser suficiente, por lo que se han desarrollado variantes como Class-Based Weighted Fair Queuing (CBWFQ), que permite una gestión más detallada del ancho de banda con clases definidas.

2.7 Implementación de QoS

Para implementar Calidad de Servicio (QoS) es necesario realizar varios procesos que permitan administrar el tráfico de red y optimizar el uso del ancho de banda. Estas capacidades permiten priorizar aplicaciones críticas, reducir congestión y garantizar un mejor rendimiento de los servicios de red, para lo cual se lleva tres procesos , como se muestra en la **Figura 10**.

Figura 10

Procesos para la implementación de QoS



Nota: *Tomado de (Paspuel, 2014)*

2.7.1 Identificación del tráfico y sus requerimientos

La identificación del tráfico constituye la base para implementar QoS, ya que permite reconocer las aplicaciones y servicios que circulan dentro de la red, así como sus necesidades de ancho de banda, latencia y prioridad.

Para realizar la identificación del tráfico es necesario llevar a cabo varios procesos, entre los que destacan la auditoría de red, la determinación de la importancia de cada aplicación y la definición de niveles de servicio para cada clase de tráfico, como se detalla en la **Figura 11**.

Figura 11

Pasos para la identificación del tráfico de una red



Nota: *Tomado de (Paspuel, 2014)*

- **Auditoría de red**

La auditoría de red se realiza con el propósito de recopilar estadísticas y datos relacionados con el comportamiento del tráfico durante los períodos de mayor utilización de la

red o en diferentes intervalos de tiempo. Este proceso permite identificar el consumo de ancho de banda, detectar congestión, reconocer los protocolos y puertos utilizados por cada aplicación, y determinar cuáles son los servicios que generan mayor tráfico dentro de la infraestructura de red.

Para llevar a cabo este proceso se emplean herramientas de captura y análisis de tráfico, como Wireshark, que permiten inspeccionar los paquetes intercambiados en la red e identificar los flujos de comunicación asociados a cada servicio, facilitando así la posterior clasificación del tráfico y la definición de políticas de calidad de servicio.

Determinación de la importancia de cada aplicación

Una vez obtenida la información del tráfico de red, es necesario determinar la importancia de cada aplicación de acuerdo con las actividades y necesidades de la organización. Este proceso permite establecer prioridades para aplicaciones críticas que requieren mayor estabilidad y menor latencia.

Según Ariganello y Barrientos Sevilla (2010), se pueden definir clases de tráfico y establecer requerimientos específicos para cada una de ellas. De esta manera, aplicaciones como VoIP, videoconferencia o bases de datos pueden recibir un tratamiento prioritario frente a servicios menos críticos como navegación web o descargas.

- **Definir los niveles de servicio para cada clase de tráfico**

Después de identificar y clasificar las aplicaciones, es necesario definir niveles de servicio para cada clase de tráfico. Cada nivel de servicio establece características específicas relacionadas con el tratamiento que recibirá el tráfico dentro de la red.

2.7.2 Clasificación de tráfico

La clasificación del tráfico consiste en organizar y agrupar los diferentes tipos de tráfico de red en clases específicas, de acuerdo con las necesidades y objetivos de la organización. Este proceso permite establecer prioridades y asignar recursos adecuados para garantizar el correcto funcionamiento de las aplicaciones y servicios dentro de la infraestructura de red.

Las clases de tráfico representan los distintos servicios y aplicaciones que pueden encontrarse dentro de una red empresarial. Cada clase posee requerimientos diferentes en cuanto a ancho de banda, latencia, jitter y prioridad de transmisión.

- **Clase VoIP**

Esta clase corresponde al tráfico de Voz sobre IP (VoIP). Debido a que las aplicaciones de voz son sensibles a la latencia, jitter y pérdida de paquetes, requieren alta prioridad y un ancho de banda estable para garantizar una comunicación fluida y continua.

- **Clase de tráfico de señalización**

Esta clase incluye el tráfico utilizado para procesos de señalización en aplicaciones de VoIP, videoconferencia y servicios multimedia. Su función principal es establecer, controlar y finalizar las comunicaciones entre dispositivos de red.

- **Clase de aplicaciones de transacción**

Comprende aplicaciones interactivas relacionadas principalmente con bases de datos y sistemas transaccionales. Estas aplicaciones requieren tiempos de respuesta rápidos y una transmisión confiable de datos para garantizar el correcto procesamiento de la información.

- **Clase Best-effort**

La clase Best-effort engloba el tráfico que no pertenece a ninguna de las clases prioritarias anteriormente definidas. Este tipo de tráfico utiliza el ancho de banda disponible restante y no posee garantías específicas de prioridad o rendimiento.

- **Clase sin importancia**

Incluye aplicaciones y servicios considerados de baja prioridad dentro de la red. En esta categoría pueden encontrarse servicios como correo electrónico personal, aplicaciones P2P, juegos en línea y otros tipos de tráfico recreativo o no esencial. Generalmente, este tráfico recibe menor prioridad para evitar afectar el desempeño de aplicaciones críticas.

2.7.3 Definición de políticas para cada clase

La definición de políticas para cada clase de tráfico constituye una etapa fundamental dentro de la implementación de Calidad de Servicio (QoS), ya que permite establecer las condiciones bajo las cuales será administrado el tráfico dentro de la red. Estas políticas tienen como objetivo garantizar un uso eficiente del ancho de banda y priorizar las aplicaciones más importantes de acuerdo con las necesidades de la organización. En esta etapa es necesario realizar diferentes tareas relacionadas con la administración y control del tráfico de red, entre las que destacan:

1. Especificar un ancho de banda máximo.
2. Establecer un ancho de banda mínimo garantizado.
3. Asignar niveles de prioridad.
4. Utilizar mecanismos adecuados para gestionar y controlar la congestión de la red.

Para definir políticas de Calidad de Servicio (QoS), se deben considerar las necesidades de cada aplicación en función de su fiabilidad, retardo, jitter y consumo de ancho de banda. En la **Tabla 8** se muestran estos parámetros según el tipo de servicio analizado.

Tabla 8

Ejemplo de los requerimientos de calidad de servicio

Aplicación	Fiabilidad	Retardo	Jitter	Ancho de Banda
Correo electrónico	Alta (*)	Alto	Alto	Bajo
Transferencia de ficheros	Alta (*)	Alto	Alto	Medio
Acceso web	Alta (*)	Medio	Alto	Medio
Login remoto	Alta (*)	Medio	Medio	Bajo
Audio bajo demanda	Media	Alto	Medio	Medio
Video bajo demanda	Media	Alto	Medio	Alto
Telefonía	Media	Bajo	Bajo	Bajo
Videoconferencia	Media	Bajo	Bajo	Alto

***Nota**: Tomado de (Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia, n.d.)*

(*) La fiabilidad alta en estas aplicaciones se consigue automáticamente al utilizar el protocolo de transporte TCP.

2.8 Marcaje de paquetes para clasificación de tráfico

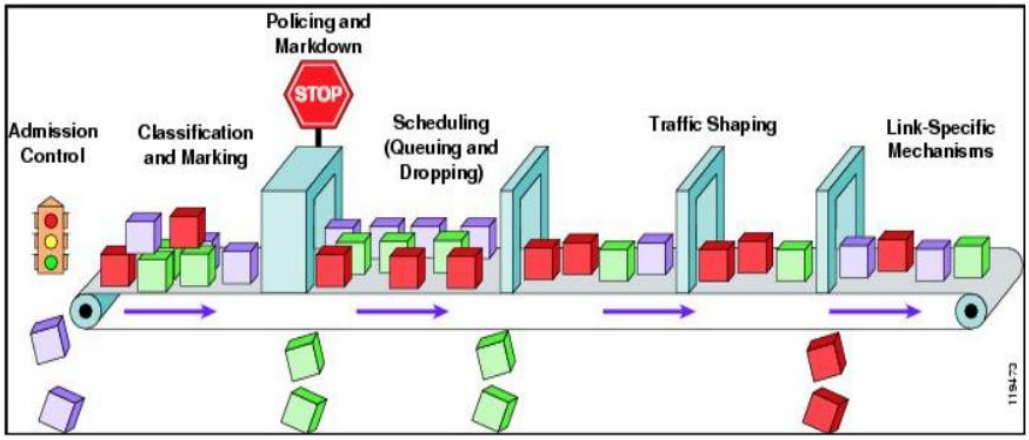
La clasificación consiste en reconocer los flujos de paquetes y organizarlos en diferentes categorías para asignarles parámetros de calidad de servicio (QoS) (Alvarez & Neira, 2015). Un flujo de datos en una red IP se distingue mediante los siguientes criterios:

- Dirección IP de origen y destino.
- Puerto de origen y puerto de destino.
- Protocolo de transporte, ya sea TCP o UDP.

Este proceso se representa en la **Figura 12**, donde se muestra cómo los paquetes son clasificados, marcados y tratados de acuerdo con las políticas de calidad de servicio establecidas.

Figura 12

Clasificación y Marcado de Paquetes



Nota. *La figura ilustra las fases del procesamiento de paquetes para la gestión de Calidad de Servicio (QoS) en redes, incluyendo clasificación, planificación y control del tráfico.*
Fuente: (Alvarez & Neira, 2015)

La gestión de QoS a través de la clasificación se desarrolla en tres fases:

- Los paquetes son identificados y agrupados en diferentes clases.
- Se les asigna una política de planificación de envío basada en su clasificación.
- Se controla la velocidad de transmisión, ya sea de manera general o específica para cada clase.

Para asignar los valores DSCP a cada una de las clases definidas, es necesario establecer políticas que determinen el tratamiento específico para cada una. Estas políticas abarcan funciones dentro de DiffServ, como el marcado de paquetes, la aplicación de reglas de control de tráfico (policing) y el encolamiento, garantizando una gestión eficiente del tráfico en la red, como se detalla en la **Tabla 9**.

Tabla 9

Asignación de prioridades y valores DSCP para aplicaciones en redes QoS

Prioridad	Aplicación	Valor DSCP
Crítica	Telefonía Ip	EF
	Señalización	CS3
	Videoconferencia	AF41
	Video streaming	AF43
Alta	Base de datos	AF31
	Ampliaciones web	AF33
Media	DNS	AF21
Baja	DHCP	AF23
Default	Otro	0

Nota: *Los valores DSCP asignados en esta tabla se basan en recomendaciones comunes para la clasificación de tráfico en redes QoS.*
Tomado de (RFC 2597 - Reenvío Asegurado de PHB Group, n.d.)

De acuerdo a lo que menciona, para gestionar la congestión en la red, es fundamental emplear un mecanismo de encolamiento que regule el tráfico cuando la demanda de ancho de banda supera la capacidad disponible. Este proceso permite asignar prioridades a los distintos tipos de tráfico, optimizando el uso de los recursos y garantizando un flujo eficiente de datos en la red. La distribución detallada de las clases y sus correspondientes tasas de transferencia se presenta en la **Tabla 10**, lo que facilita la visualización y aplicación de estas políticas.

Tabla 10

Tasa de Transferencia para Aplicaciones en QoS

Prioridad	Aplicación	% Tasa de transferencia
Crítica	Telefonía Ip	15%
	Señalización	5%

	Videoconferencia	15%
	Video streaming	15%
Alta	Base de datos	10%
	Ampliaciones web	10%
Media	DNS	3%
Baja	DHCP	2%
Default	Otro	-

***Nota**: Los porcentajes de ancho de banda corresponde a una política de diseño, por lo que puede variar según la capacidad del enlace y los objetivos del servicio.*
Tomado de (RFC 2474 - Definición Del Campo de Servicios Diferenciados (Campo DS) En Los Encabezados IPv4 e IPv6, n.d.)

2.9 Desafíos de QoS en entornos virtualizados

La calidad de servicio (QoS) aborda diversos problemas críticos que pueden impactar significativamente el rendimiento de la red y la experiencia del usuario final. Estos problemas incluyen aspectos técnicos y operativos que, si no se gestionan adecuadamente, pueden generar un deterioro en la calidad percibida de las aplicaciones y servicios (LiveAction, 2023). Entre los principales desafíos que QoS busca solucionar se encuentran:

- La latencia es el retraso que experimentan los paquetes de datos al viajar a través de una red. Niveles elevados de latencia pueden afectar negativamente a aplicaciones y servicios en tiempo real, generando interrupciones y retrasos en la comunicación. Para minimizar este impacto, QoS emplea diversas técnicas, como la priorización del tráfico sensible al tiempo y la asignación adecuada de ancho de banda a aplicaciones críticas. Reducir la latencia garantiza una transmisión ágil de los datos, optimizando la comunicación en tiempo real y mejorando la experiencia del usuario(Monitoring, 2023).

- El jitter, o variabilidad en el retardo de entrega de paquetes, es otro desafío que QoS busca mitigar. Una entrega irregular de paquetes puede generar interrupciones en el flujo de datos, afectando especialmente aplicaciones de tiempo real como VoIP y streaming de video. Para contrarrestarlo, QoS gestiona los recursos de la red de manera eficiente, priorizando paquetes críticos y asegurando una entrega estable y predecible. Esto permite mantener la integridad de las aplicaciones en tiempo real y garantizar un rendimiento consistente.(Monitoring, 2023)
- La pérdida de paquetes también incide en la calidad del servicio y la experiencia del usuario. Ocurre cuando ciertos paquetes no llegan a su destino, causando vacíos en la transmisión. Puede deberse a congestión de red, errores o insuficiencia de ancho de banda. QoS implementa estrategias para minimizar este problema, como la priorización del tráfico esencial, la aplicación de técnicas de corrección de errores y la asignación de recursos suficientes para mitigar la congestión. Al reducir la pérdida de paquetes, QoS asegura una transmisión de datos confiable y continua, optimizando la calidad de los servicios de red(Monitoring, 2023).
- El análisis de paquetes permite a los administradores de red evaluar el impacto de los mecanismos de QoS, ajustando parámetros según sea necesario para mejorar el rendimiento y garantizar una comunicación fluida y eficiente(Monitoring, 2023).

2.10 Tecnologías de virtualización en redes

La virtualización en redes es una tecnología clave que permite abstraer y segmentar los recursos físicos de red, creando múltiples redes virtuales sobre una misma infraestructura física. Esto mejora la flexibilidad, escalabilidad, y eficiencia en la gestión de los recursos de red.

Virtualizar un dispositivo MikroTik implica correr RouterOS, el sistema operativo de MikroTik, en un entorno virtual en lugar de en hardware físico. Esto es particularmente útil para pruebas, desarrollo, simulación de redes, o incluso para implementaciones de producción donde el hardware físico puede ser limitante o se prefiere la flexibilidad de una infraestructura(Sarmiento et al., 2011) . Existen varias formas de virtualizar RouterOS, siendo las más comunes el uso de CHR (Cloud Hosted Router) y la ejecución en plataformas de virtualización estándar como VMware, VirtualBox, o Hyper-V.

2.10.1 Conceptos básicos de virtualización

Una máquina virtual es un entorno de computación independiente que simula un sistema con su propia CPU, memoria, almacenamiento y conexión de red, pero funciona utilizando los recursos de un equipo físico. Su ejecución es posible gracias a un software especializado llamado hipervisor, el cual gestiona la asignación y administración de estos recursos de manera eficiente. El hardware que aloja y opera las máquinas virtuales se conoce como *host*, mientras que cada máquina virtual creada dentro de este entorno recibe el nombre de *guest*. El hipervisor permite distribuir dinámicamente los recursos del sistema, como el procesamiento y la memoria, entre las distintas máquinas virtuales en ejecución (Hat, 2024).

Este enfoque posibilita la ejecución simultánea de varios sistemas operativos en un mismo equipo, permitiendo, por ejemplo, ejecutar Linux en un sistema con MacOS o Windows. Las máquinas virtuales replican el comportamiento de un sistema operativo en un entorno físico, proporcionando una experiencia de usuario prácticamente idéntica a la de un sistema instalado directamente en hardware dedicado (Red Hat, 2021)

2.10.2 Uso de máquinas virtuales en redes de Comunicación Multimedia

Las máquinas virtuales han adquirido un papel fundamental en las redes de comunicación multimedia, permitiendo la ejecución simultánea de múltiples servicios dentro de un mismo entorno físico. Gracias a la virtualización, se logra un mejor aprovechamiento del hardware, reducción de costos operativos y mayor flexibilidad en la asignación de recursos para aplicaciones multimedia.

No obstante, la adopción de máquinas virtuales conlleva ciertos retos en términos de calidad de servicio (QoS). Debido a que estos entornos comparten recursos físicos como CPU, memoria y ancho de banda, la posibilidad de congestión en la red y variaciones en el rendimiento aumenta considerablemente. Esto puede derivar en problemas como latencia, ancho de banda, jitter y pérdida de paquetes, afectando la transmisión en tiempo real de aplicaciones críticas como VoIP y videoconferencias.

Para mitigar estos inconvenientes, es fundamental implementar estrategias de administración del tráfico dentro de los entornos virtualizados. La **Tabla 11** presenta algunas de las técnicas más utilizadas, las cuales permiten optimizar el rendimiento de aplicaciones multimedia y garantizar una mejor calidad de servicio (QoS) en entornos virtualizados.

Tabla 11

Técnicas de Administración del Tráfico en Entornos Virtualizados

Técnica	Descripción
Asignación de recursos garantizados	Aplicación de políticas de limitación y reserva de ancho de banda para garantizar el rendimiento de aplicaciones multimedia.

Monitoreo y gestión de tráfico	Uso de herramientas como Traffic Flow y Queue Management en MikroTik para analizar y optimizar el flujo de datos.
Priorización del tráfico crítico	Implementación de colas y marcado de paquetes para garantizar que servicios como VoIP y videoconferencias tengan preferencia sobre otros tipos de tráfico menos sensibles.

Nota: *Las estrategias mencionadas permiten optimizar la calidad del servicio en entornos virtualizados, minimizando la latencia y mejorando la estabilidad de la red.*
Fuente: Autoría propia

El uso de máquinas virtuales en redes multimedia ha evolucionado significativamente, proporcionando soluciones eficientes para la administración del tráfico de datos en tiempo real. Sin embargo, la correcta aplicación de técnicas de QoS sigue siendo un factor clave para mantener la estabilidad y calidad del servicio en estos entornos dinámicos.

2.10.3 Impacto de la virtualización en el rendimiento de QoS

La virtualización en sistemas de comunicación multimedia con Mikrotik introduce desafíos en QoS debido a la compartición de recursos de red y procesamiento, lo que puede generar latencia, jitter y pérdida de paquetes, afectando aplicaciones en tiempo real como VoIP y videoconferencias (Cando, 2023). La competencia por ancho de banda y capacidad de procesamiento en plataformas como VMware ESXi, KVM o Hyper-V puede provocar una distribución desigual del tráfico, impactando la estabilidad del servicio.

Para mitigar estos efectos, la configuración de colas de encolado en Mikrotik (Queue Tree y Simple Queues) junto con estrategias como marcado de paquetes, segmentación de tráfico mediante VLANs y priorización en switches virtuales es fundamental. Tecnologías como SR-IOV optimizan la eficiencia al reducir la carga del hipervisor en la transmisión de datos. La correcta implementación de estas técnicas garantiza un rendimiento estable y eficiente en entornos virtualizados.

2.11 Sobre Mikrotik

MikroTik es un fabricante de hardware y software especializado en routers, utilizado en millones de redes a nivel mundial y adaptado a diversas escalas. Fundada en 1995 en Letonia, Europa del Norte, MikroTik cuenta con una sólida red de técnicos en todo el mundo que proporcionan soporte especializado a sus productos (S.A, 2025).

2.11.1 ¿Qué es RouterOS?

RouterOS es un sistema operativo independiente (stand-alone) desarrollado por MikroTik**,** diseñado específicamente para instalarse en routers y convertir computadoras o dispositivos en potentes routers de red. Este sistema operativo es reconocido por su alta potencia y flexibilidad, permitiendo configuraciones avanzadas para satisfacer diferentes necesidades de red. (Escalente, 2017)

Entre las configuraciones más populares que ofrece RouterOS se encuentran:

- Firewall: Para garantizar la seguridad en las redes.
- Routing: Para gestionar el enrutamiento eficiente del tráfico.
- Forwarding: Para optimizar el envío de datos entre redes.
- MPLS: Para redes avanzadas con múltiples protocolos.
- VPN: Para establecer conexiones seguras y privadas.

- Wireless: Soporte para redes inalámbricas.
- HotSpot: Gestión de acceso a internet para usuarios.
- Calidad de Servicio (QoS): Para priorizar el tráfico y optimizar la experiencia del usuario.
- Web Proxy: Para almacenamiento y control del acceso a la web.

Gracias a estas capacidades, MikroTik se ha consolidado como una solución confiable para redes de diferentes tamaños y propósitos.

2.11.2 Tipos de licenciamiento en Mikrotik

Las licencias de RouterOS presentan diferentes niveles, cada uno diseñado para cubrir necesidades específicas en entornos de red domésticas, empresariales y de proveedores de servicios. Estas diferencias se detallan en la **Tabla 12**, donde se describen las principales características de cada nivel de licencia.

Tabla 12

Niveles de Licencia

Niveles de Licencia	Características
Nivel 3	• Diseñado para dispositivos que actúan como clientes CPE (Customer Premises Equipment) en redes inalámbricas.
Nivel 4	• Licencia básica para routers y puntos de acceso inalámbricos. • Permite configuraciones inalámbricas AP (Access Point) con un número limitado de clientes. • Admite hasta 200 túneles activos para VPN.

Nivel 5	• Adecuado para implementaciones de red medianas con mayor capacidad. • Permite un número ilimitado de usuarios inalámbricos y hasta 500 túneles VPN. • Soporte mejorado para funciones avanzadas.
Nivel 6	• Licencia completa sin restricciones en la cantidad de túneles VPN, usuarios inalámbricos o funcionalidad. • Diseñada para grandes redes empresariales y operadores.

Nota: *La tabla presenta las características y capacidades asociadas a los diferentes niveles de licencia, que determinan el alcance funcional y de escalabilidad de los dispositivos en una red.*
Fuente: (Mikrotik, 2025)

Tomando en consideración que las licencias no expiran, contienen soporte gratis por 15 días (Rosales, 2022).

- **MikroTik Cloud Hosted Router y licenciamiento CHR**

MikroTik Cloud Hosted Router, conocido como CHR, es una versión de RouterOS diseñada para ejecutarse como máquina virtual en entornos de virtualización. A diferencia del licenciamiento tradicional de RouterOS, que se organiza por niveles, CHR utiliza un modelo propio compuesto por las licencias Free, P1, P10 y P-Unlimited. La principal diferencia entre estos niveles se encuentra en el límite de velocidad permitido por interfaz.

La licencia CHR Free permite utilizar las funciones de RouterOS dentro de una máquina virtual de forma gratuita; sin embargo, limita la velocidad de transmisión a 1 Mbit/s por interfaz. Por su parte, las licencias P1, P10 y P-Unlimited incrementan dicha capacidad a 1 Gbit/s, 10 Gbit/s y velocidad sin límite aplicado por licencia, respectivamente, como se muestra en la **Tabla 13**.

Tabla 13

Niveles de licencia de MikroTik CHR

Licencia CHR	Límite de velocidad por interfaz	Precio	Descripción
Free	1 Mbit/s	Gratis	Licencia gratuita para entornos de prueba
P1	1 Gbit/s	USD 45	Licencia perpetua con mayor capacidad de transmisión
P10	10 Gbit/s	USD 95	Licencia perpetua para escenarios de alto rendimiento
P-Unlimited	Sin límite por licencia	USD 250	Licencia perpetua sin restricción de velocidad aplicada por licencia

Fuente: Tomado de MikroTik.

Por lo tanto, en entornos académicos y de simulación, CHR Free puede ser utilizada para implementar escenarios de prueba con funcionalidades completas de RouterOS, considerando como restricción principal el límite de transmisión de 1 Mbit/s por interfaz. Este valor puede tomarse como referencia cuando se requiera calcular la utilización del ancho de banda dentro de un laboratorio virtualizado.

2.12 Herramientas de monitoreo de red

Las herramientas de monitoreo de red permiten recolectar información relacionada con el comportamiento del tráfico, el consumo de ancho de banda y el rendimiento de los diferentes

servicios dentro de la infraestructura de red. Estas herramientas facilitan la auditoría y supervisión de la red, permitiendo identificar aplicaciones, protocolos y posibles problemas de congestión o rendimiento. Entre las principales herramientas se encuentran este NTOP, Wireshark y PacketShap (Paspuel, 2014).

2.12.1 NTOP

NTOP es una herramienta de monitoreo en tiempo real utilizada para analizar el tráfico de red y supervisar el consumo de recursos por parte de usuarios y aplicaciones. Esta herramienta permite detectar malas configuraciones y evaluar el comportamiento del tráfico mediante estadísticas y gráficos accesibles desde una interfaz web. Además, utiliza la librería libpcap para la captura de paquetes y se encuentra disponible para sistemas Unix y Windows (Vunkers IT Experts, n.d.).

2.12.2 WireShark

Wireshark es un analizador de protocolos de red basado en software libre, utilizado para capturar y analizar paquetes de datos en tiempo real. Esta herramienta permite monitorear el tráfico de red a un nivel detallado, facilitando el análisis de protocolos y la detección de problemas de comunicación dentro de la red (Abba M, 2023).

Wireshark dispone de filtros avanzados que permiten clasificar paquetes según criterios específicos definidos por el usuario, además de presentar gráficamente la información capturada mediante diferentes colores y estadísticas. También soporta más de 1100 protocolos y puede utilizarse en sistemas operativos como Windows, Linux y macOS.

2.12.3 Torch

Torch es una herramienta de monitoreo integrada en MikroTik RouterOS, utilizada para supervisar en tiempo real el tráfico que atraviesa una interfaz del router. Su función principal es mostrar información sobre los flujos activos de la red, permitiendo observar el comportamiento del tráfico según diferentes criterios de análisis.

Esta herramienta permite clasificar el tráfico por protocolo, dirección IP de origen, dirección IP de destino y puerto utilizado. Además, muestra la velocidad de transmisión y recepción de datos, identificada mediante los valores TX y RX, lo que facilita el análisis del consumo de ancho de banda asociado a cada flujo. Gracias a estas características, Torch resulta útil para tareas de diagnóstico, auditoría y verificación del tráfico dentro de una red(Escalante, 2023).

A partir de la versión v5RC6, Torch incorporó soporte para tráfico IPv6, mediante los parámetros src-address6 y dst-address6, los cuales permiten filtrar los paquetes de acuerdo con direcciones IPv6 de origen y destino. Esta funcionalidad amplía su capacidad de monitoreo en redes que utilizan direccionamiento IPv6.

Torch puede utilizarse tanto desde la línea de comandos CLI como desde la interfaz gráfica WinBox. En WinBox, la herramienta presenta una visualización más amigable del tráfico activo y permite aplicar filtros de forma rápida para facilitar la interpretación de los resultados. En el contexto de una política QoS, Torch se emplea como herramienta complementaria para verificar el tráfico que circula por las interfaces del router y observar la tasa de transmisión de los servicios evaluados(Escalante, 2023).

2.13 Análisis comparativo: Mikrotik en Redes Virtualizadas

El uso de Mikrotik en redes virtualizadas es una alternativa viable para la administración y optimización del tráfico en entornos donde se requiere garantizar la calidad de servicio (QoS). La virtualización ha permitido la consolidación de múltiples funciones en una misma infraestructura, lo que representa ventajas en términos de flexibilidad y reducción de costos.

Sin embargo, la implementación de QoS en entornos virtualizados también presenta desafíos relacionados con el rendimiento, la latencia y la escalabilidad. El desempeño de un router virtual depende directamente de los recursos asignados por el hipervisor, como procesador, memoria y adaptadores de red virtuales. En escenarios de alto tráfico, una asignación insuficiente de recursos puede provocar pérdida de paquetes, incremento de latencia y disminución del rendimiento general de la red.

2.13.1 Comparación entre Mikrotik y otras tecnologías

MikroTik se diferencia de otras soluciones debido a su facilidad de configuración y bajo costo de implementación. Su interfaz gráfica WinBox permite administrar funciones avanzadas de routing, firewall y QoS sin requerir configuraciones excesivamente complejas. Además, puede implementarse sobre diferentes plataformas de virtualización, como VMware ESXi, Proxmox, Hyper-V y VirtualBox (Dobladez, 2007).

Un aspecto crítico en redes virtualizadas es la gestión del tráfico entre máquinas virtuales, en este sentido, Mikrotik puede presentar limitaciones debido a la falta de aceleración por hardware en ciertos hipervisores como VMware ESXi o Proxmox. Sin embargo, su compatibilidad con tecnologías como SR-IOV y VLANs permite mejorar el control del tráfico y la segmentación, lo que contribuye a optimizar la distribución del ancho de banda (Reddit, 2023).

En términos de administración de QoS, Mikrotik permite la priorización del tráfico a través de mecanismos como HTB, asegurando una distribución eficiente del ancho de banda entre diferentes tipos de aplicaciones. A pesar de ello, en entornos de alto tráfico, su capacidad de procesamiento puede verse limitada en comparación con routers virtuales de mayor capacidad, lo que puede impactar la estabilidad y el rendimiento de la red (Shahad H. Majid, 2018). En la **Tabla 14** se presenta la comparación de soluciones de routing virtual según características técnicas y operacionales.

Tabla 14

Comparación de soluciones de routing virtual según características técnicas y operacionales

Característica	MikroTik	pfSense	VyOS	OpenWRT	Cisco Virtual	VMware NSX
General						
Tipo de licencia	Propietaria	Open source	Open source	Open source	Propietaria	Propietaria
Enfoque principal	Routing y QoS	Firewall y seguridad	Routing empresarial	Redes embebidas	Redes empresariales	Virtualización y SDN
Costo	Bajo	Bajo / medio	Bajo	Bajo	Alto	Alto
Usabilidad						
Facilidad de configuración	Alta	Media	Media	Media	Baja	Media
Curva de aprendizaje	Baja	Media	Media / Alta	Media	Alta	Alta
Rendimiento y capacidades						
Soporte QoS	Alto	Medio	Alto	Medio	Alto	Alto
Escalabilidad	Media	Media	Alta	Media	Alta	Alta
Consumo de recursos	Bajo	Medio	Bajo	Bajo	Alto	Alto
Seguridad	Buena	Muy buena	Buena	Buena	Excelente	Excelente
Integración y gestión						
Integración con SDN	Baja	Baja	Media / Alta	Baja	Alta	Muy alta

Administración centralizada	Limitada	Media	Media	Limitada	Alta	Muy alta
Virtualización						
Uso en virtualización	Bueno	Bueno	Muy bueno	Bueno	Muy bueno	Excelente
Compatibilidad hipervisores	VMware, Proxmox, VirtualBox	VMware, Hyper-V, Proxmox, KVM, VirtualBox, Xen	KVM, VMware, Proxmox	VirtualBox, VMware, KVM, Proxmox	VMware, KVM	VMware ESXi

Nota. *Los valores corresponden a una evaluación comparativa cualitativa basada en documentación oficial y literatura técnica de cada plataforma según la documentación de (Netgate, 2025).*

Capítulo III. Diseño e implementación

El presente capítulo describe toda la información técnica necesaria para el diseño e implementación de una política de calidad de servicio, la cual se basa en la arquitectura de servicios diferenciados (DiffServ) definida en el RFC 2474 y en los parámetros de desempeño establecidos en las recomendaciones ITU-T Y.1540 e Y.1541, aplicada sobre una topología multiservicio virtualizada con routers MikroTik RouterOS para la priorización del tráfico multimedia en entornos de recursos compartidos.

3.1 Metodología de desarrollo

El Modelo en Cascada se caracteriza por seguir un enfoque secuencial que permite controlar de manera ordenada cada una de las etapas del desarrollo del sistema. Una de sus particularidades más relevantes es la dependencia entre fases, lo que implica que no se puede avanzar a la siguiente etapa sin haber concluido completamente la anterior. Esta condición resulta pertinente para el presente trabajo, ya que la política de calidad de servicio solo puede diseñarse una vez identificado el tráfico que circula por la red, y únicamente puede evaluarse cuando la configuración se encuentra implementada y verificada como se muestra en la **Figura 13**.

Figura 13

Fases metodológicas del proyecto de integración curricular.



Nota: *El diagrama muestra la metodología para implementar y evaluar QoS en una topología virtualizada.*
Fuente: Autoría propia

3.2 Análisis actual

En la actualidad, un número importante de instituciones educativas y organizaciones con recursos limitados operan sus redes de datos bajo un esquema de mejor esfuerzo (Best Effort), en el cual todo el tráfico ya sea voz, video, datos transaccionales o tráfico administrativo recibe el mismo tratamiento, sin ningún tipo de diferenciación ni prioridad. Este esquema resulta insuficiente cuando conviven en la misma red aplicaciones sensibles al retardo, como la telefonía IP y el streaming multimedia, junto con servicios elásticos como la navegación web, el correo electrónico o la transferencia de archivos, ya que ante una congestión del enlace ambos tipos de tráfico compiten por el mismo ancho de banda sin ninguna garantía para los servicios críticos.

A esta situación se suma una barrera de costo: las soluciones de calidad de servicio de alto desempeño, como los equipos Cisco, representan una inversión que muchas instituciones educativas y pequeñas y medianas empresas no pueden asumir. MikroTik se presenta como

una alternativa económica, pero existe poca evidencia técnica documentada sobre su comportamiento al gestionar tráfico multimedia bajo condiciones de congestión, y menos aún sobre su desempeño dentro de entornos virtualizados, donde la compartición de recursos físicos entre varias máquinas virtuales introduce variables adicionales de latencia, jitter y pérdida de paquetes.

Frente a esta situación, resulta necesario contar con un escenario controlado que represente una red multiservicio típica con tráfico de voz, streaming, base de datos, navegación web, correo electrónico y acceso remoto sobre el cual sea posible auditar el comportamiento del tráfico sin QoS, definir los requerimientos técnicos correspondientes, y diseñar e implementar una política de calidad de servicio en routers MikroTik que priorice los servicios sensibles al retardo frente al tráfico de menor exigencia temporal.

Este análisis de la situación actual constituye el punto de partida para la definición de los requerimientos que se presenta en el siguiente apartado, ya que las carencias identificadas ausencia de diferenciación de tráfico, de mecanismos de marcaje y de administración de congestión determinan directamente las capacidades que la solución propuesta debe cumplir.

3.3 Definición de requerimientos

La definición de requerimientos de calidad de servicio permite establecer, antes del diseño de la red, las condiciones que debe cumplir la solución para gestionar tráfico multimedia en routers MikroTik dentro de un entorno virtualizado. Estos requerimientos se plantean a partir de las necesidades de los servicios considerados, las métricas de evaluación y las características propias de una infraestructura basada en máquinas virtuales.

En primer lugar, se requiere que la red permita identificar el tráfico generado por los servicios multimedia y de datos, con el fin de reconocer protocolos, puertos y flujos asociados

a cada aplicación. Esta identificación servirá como base para analizar métricas como el retardo, la variación del retardo, la pérdida de paquetes y el ancho de banda, permitiendo establecer una línea base para la evaluación posterior del desempeño de la red.

A partir de esta identificación, se definen requerimientos orientados a la clasificación y priorización del tráfico. Los servicios sensibles al retardo, como VoIP y video en tiempo real, deben recibir un tratamiento preferencial frente a aplicaciones menos críticas. Asimismo, la solución debe permitir el uso de mecanismos de marcaje que identifiquen las clases de tráfico dentro del dominio de red, de modo que cada flujo pueda recibir un tratamiento acorde con su nivel de importancia.

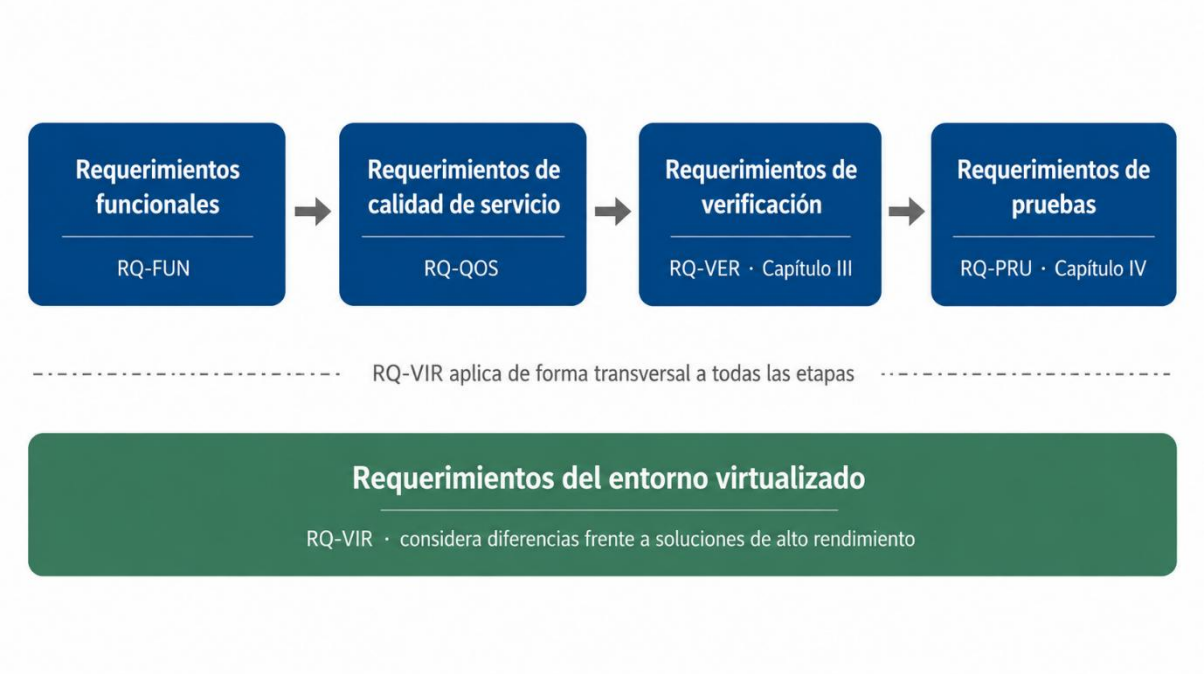
También se consideran requerimientos para la administración de congestión, ya que la red debe contar con mecanismos que permitan organizar el tráfico en colas, asignar prioridades y distribuir el ancho de banda disponible de forma controlada. En este sentido, se toma como referencia el comportamiento esperado de técnicas como Low Latency Queuing (LLQ) y Weighted Fair Queuing (WFQ), no como configuraciones directas en MikroTik, sino como criterios funcionales relacionados con la atención preferente del tráfico sensible y el reparto equitativo de los recursos.

Finalmente, estos requerimientos permiten considerar las diferencias entre MikroTik y soluciones de alto rendimiento abordadas en el marco teórico. Esta comparación se plantea como una referencia técnica para identificar aspectos como costo, disponibilidad, complejidad de configuración, escalabilidad, capacidad de procesamiento y aplicabilidad en entornos académicos virtualizados, sin que ello implique todavía una comparación experimental directa entre plataformas.

La **Figura 14** resume la organización general de los requerimientos definidos para orientar el diseño de la política QoS en la red simulada.

Figura 14

Estructura y flujo de los requerimientos de QoS



Nota. *RQ-VIR aplica de forma transversal a los demás grupos, ya que toda la red opera dentro de un entorno virtualizado*
Fuente: Autoría propia

3.3.1 Nomenclatura de requerimientos

La **Tabla 15** presenta la nomenclatura utilizada para identificar los requerimientos definidos para la política de calidad de servicio. Esta codificación permite organizar las necesidades técnicas de acuerdo con su función dentro del proyecto y facilita su referencia en las etapas posteriores del diseño, implementación, verificación y evaluación.

La clasificación de los requerimientos se estructura en cinco grupos. Los requerimientos funcionales describen las capacidades básicas que debe cumplir la red para identificar y clasificar el tráfico. Los requerimientos de calidad de servicio establecen las condiciones necesarias para priorizar, marcar y administrar el tráfico multimedia. Los requerimientos del

entorno virtualizado consideran las condiciones propias de trabajar con máquinas virtuales y routers MikroTik, incluyendo las diferencias frente a soluciones de alto rendimiento. Finalmente, se separan los requerimientos de verificación y los requerimientos de pruebas, debido a que la verificación corresponde a la comprobación técnica de la configuración en el Capítulo III, mientras que las pruebas se orientan a la evaluación del desempeño en el Capítulo IV.

Tabla 15

Nomenclatura de requerimientos

Código	Descripción
RQ-FUN	Requerimientos funcionales
RQ-QoS	Requerimientos de Calidad de Servicio
RQ-VIR	Requerimientos de entorno virtualizado
RQ-VER	Requerimientos de verificación de la configuración
RQ-PRU	Requerimientos de pruebas de desempeño

Nota: *La nomenclatura permite organizar los requerimientos según su función dentro del diseño de QoS*
Fuente: Autoría propia

3.3.2 Requerimientos funcionales

Los requerimientos funcionales establecen las capacidades básicas que debe cumplir la red para gestionar el tráfico multimedia y de datos dentro del entorno virtualizado. Estos requerimientos no corresponden todavía a una configuración específica de QoS, sino a las condiciones necesarias para que, en las etapas posteriores, sea posible identificar, clasificar y organizar los flujos que circularán por la topología.

En este sentido, la **Tabla 16** presenta los requerimientos funcionales definidos para la red simulada, los cuales se relacionan con la identificación de los servicios implementados, el reconocimiento de protocolos y puertos, la diferenciación del tráfico sensible al retardo y la

agrupación de servicios con características similares. Esta etapa resulta fundamental, ya que una política QoS solo puede aplicarse correctamente cuando el tráfico ha sido previamente reconocido y organizado. Por ello, estos requerimientos sirven como punto de partida para la auditoría, clasificación, priorización y posterior tratamiento del tráfico multimedia y de datos.

Tabla 16

Requerimientos funcionales

Código	Descripción	Criterio de cumplimiento
RQ-FUN-01	La red debe permitir la identificación de los servicios multimedia y de datos utilizados en la topología.	Se reconocen los servicios VoIP, streaming, base de datos, navegación web y tráfico de baja prioridad.
RQ-FUN-02	El tráfico debe poder clasificarse según protocolo y puerto.	Cada servicio se asocia con su protocolo de transporte y puerto correspondiente.
RQ-FUN-03	La red debe permitir diferenciar tráfico sensible al retardo frente a tráfico de menor prioridad.	Los servicios de voz y video se separan de servicios como FTP, IMAP, SSH y tráfico no clasificado.
RQ-FUN-04	La solución debe permitir agrupar servicios con características similares.	Los servicios se organizan en clases de tráfico para facilitar su tratamiento posterior.

Fuente: Autoría propia

3.3.3 Requerimientos de Calidad de servicio

Los requerimientos de calidad de servicio establecen las condiciones necesarias para que la red aplique un tratamiento diferenciado al tráfico multimedia y de datos. A diferencia de los requerimientos funcionales, centrados en identificar y organizar los flujos, estos requerimientos definen las capacidades que debe tener la solución para priorizar servicios críticos, marcar el tráfico, conservar la clase de servicio y administrar la congestión.

La **Tabla 17** presenta los requerimientos de calidad de servicio definidos para la red simulada, con énfasis en proteger aplicaciones sensibles al retardo y a su variación, como voz y video, frente a servicios con menor exigencia temporal. Estos requerimientos sirven de base

para seleccionar el modelo QoS, el método de marcaje y el mecanismo de administración de congestión.

Tabla 17

Requerimientos de calidad de servicio

Código	Descripción	Criterio de cumplimiento
RQ-QoS-01	La política QoS debe priorizar aplicaciones sensibles al retardo, como voz y video, durante toda la ruta del tráfico.	Los servicios críticos reciben tratamiento preferencial en los mecanismos de cola frente al tráfico de datos, administración y baja prioridad.
RQ-QoS-02	La solución debe diferenciar el tráfico según su nivel de importancia.	El tráfico se organiza en clases de servicio según sus requerimientos de funcionamiento.
RQ-QoS-03	La solución debe marcar el tráfico para identificar su clase de servicio.	Cada clase de tráfico cuenta con un mecanismo de identificación dentro del dominio de red.
RQ-QoS-04	El marcaje debe conservarse durante el recorrido del paquete por la red.	Los routers del dominio QoS reconocen la clase de servicio asociada al tráfico.
RQ-QoS-05	La red debe contar con un mecanismo de administración de congestión basado en colas.	El tráfico se organiza en colas u otros mecanismos equivalentes cuando hay saturación del enlace.
RQ-QoS-06	La solución debe permitir definir tasas mínimas o garantías de ancho de banda cuando la política de QoS lo requiera.	La reserva mínima se aplica a la clase agregada SERVIDORES mediante limit-at=700k; las colas de servicio individuales utilizan limit-at=0 y se diferencian mediante priority.
RQ-QoS-07	La solución debe permitir limitar el consumo máximo de ancho de banda por clase de servicio.	La cola padre y las colas hijas se mantienen dentro de max-limit=900k, que constituye el techo operativo configurado para Queue Tree.

Fuente: Autoría propia

3.3.4 Requerimientos de entorno virtualizado

Los requerimientos del entorno virtualizado establecen las condiciones que debe cumplir la solución para operar routers MikroTik dentro de una infraestructura basada en máquinas virtuales. Estos requerimientos consideran aspectos como la compatibilidad con

RouterOS, la conectividad entre segmentos, la disponibilidad de recursos virtuales y las limitaciones propias de un escenario simulado. Además, permiten tomar en cuenta las diferencias frente a soluciones de alto rendimiento, considerando criterios como costo, escalabilidad, complejidad de configuración y capacidad de gestión QoS, sin que esto implique todavía una comparación experimental directa entre plataformas. En este sentido, la **Tabla 18** presenta los requerimientos definidos para el entorno virtualizado.

Tabla 18

Requerimientos del entorno virtualizado

Código	Descripción	Criterio de cumplimiento
RQ-VIR-01	La solución debe poder implementarse en routers MikroTik dentro de un entorno virtualizado.	RouterOS opera correctamente como router virtual dentro de la topología.
RQ-VIR-02	La red debe mantener conectividad entre los segmentos de clientes, servidores y routers.	Existe comunicación entre las redes definidas en la topología virtualizada.
RQ-VIR-03	La solución debe considerar las limitaciones de recursos propias de una implementación virtual.	Se toma en cuenta la capacidad asignada a las máquinas virtuales y el límite de transmisión utilizado en el escenario.
RQ-VIR-04	La solución debe considerar diferencias frente a equipos de alto rendimiento.	Se analizan aspectos como costo, disponibilidad, complejidad de configuración, escalabilidad y capacidad de gestión QoS.
RQ-VIR-05	La solución debe ser aplicable en un entorno académico o de simulación.	La configuración puede ejecutarse con recursos virtuales disponibles y herramientas accesibles.

Fuente: Autoría propia

3.3.5 Requerimientos de verificación de la configuración

Como parte del proceso de validación del diseño QoS, se requiere comprobar que las configuraciones aplicadas en los routers funcionen de acuerdo con lo establecido en la política de calidad de servicio. Para ello, la **Tabla 19** presenta los requerimientos de verificación, orientados a confirmar la correcta identificación del tráfico, el marcaje de los paquetes y el funcionamiento de las colas dentro de la topología.

Tabla 19

Requerimientos de verificación de la configuración

Código	Descripción	Criterio de cumplimiento
RQ-VER-01	La configuración QoS debe poder verificarse mediante herramientas de monitoreo.	Se utilizan herramientas como Wireshark, Torch, y estadísticas propias de RouterOS para confirmar que las reglas están activas.
RQ-VER-02	El marcaje del tráfico debe poder observarse a nivel de paquete.	Wireshark permite identificar el valor de calidad de servicio en la cabecera del paquete capturado.
RQ-VER-03	La actividad del tráfico debe poder observarse en los routers MikroTik.	Torch permite visualizar tráfico por interfaz, protocolo, dirección y tasa de transmisión en tiempo real.
RQ-VER-04	La actividad de las colas debe poder comprobarse durante la generación de tráfico.	Las colas configuradas registran actividad cuando circula tráfico asociado a cada clase de servicio.

Fuente: Autoría propia

3.3.6 Requerimientos de evaluación de desempeño

Los requerimientos de evaluación no rigen directamente el diseño de la red, sino la forma en que se comprobará su desempeño bajo condiciones de prueba. Su definición previa permite establecer criterios uniformes para la medición de parámetros como ancho de banda, retardo, variación del retardo y pérdida de paquetes, garantizando que los escenarios sin QoS y con QoS puedan compararse bajo condiciones equivalentes. La **Tabla 20** presenta los requerimientos de evaluación definidos para este propósito.

Tabla 20

Requerimientos de pruebas de desempeño

Código	Descripción	Criterio de cumplimiento
RQ-PRU-01	La evaluación debe permitir comparar un escenario sin QoS y un escenario con QoS.	Ambos escenarios se prueban bajo la misma topología y las mismas condiciones de generación de tráfico.
RQ-PRU-02	Las pruebas deben considerar métricas de desempeño de red.	Se registran ancho de banda, retardo, variación del retardo y

	pérdida de paquetes en ambos escenarios.

Fuente: Autoría propia

Los requerimientos definidos en esta sección establecen las condiciones previas que orientan las decisiones de diseño desarrolladas en los apartados siguientes. A partir de ellos se justifican la selección del modelo de QoS, el método de marcaje de paquetes, las clases de servicio y el mecanismo de administración de congestión adoptado en la topología simulada

3.4 Selección del entorno de simulación y virtualización

La selección de MikroTik CHR como tipo de router virtual se fundamenta en los requerimientos RQ-VIR-01, RQ-VIR-02 y RQ-VIR-04, debido a que esta alternativa permite ejecutar RouterOS dentro del entorno virtualizado, representar múltiples nodos MikroTik en la topología y cumplir con criterios de compatibilidad, costo, consumo de recursos y soporte de funciones requeridas para la política QoS.

3.4.1 Selección del software

La selección del software de simulación de redes responde a los requerimientos del entorno virtualizado, debido a que la plataforma elegida debe permitir representar routers MikroTik, integrar máquinas virtuales externas y facilitar el análisis del tráfico generado en la topología. Para esta elección se consideraron criterios como compatibilidad con MikroTik CHR, costo, requisitos de hardware e integración con herramientas de monitoreo y virtualización. En particular, esta elección da cumplimiento al RQ-VIR-05, dado que la configuración puede ejecutarse con los recursos virtuales disponibles y con herramientas de acceso libre como GNS3, lo que la hace aplicable en un contexto académico o de simulación.

En este sentido, la **Tabla 21** compara tres alternativas utilizadas en entornos académicos y de laboratorio: GNS3, EVE-NG y Cisco Packet Tracer. Esta comparación permite determinar qué herramienta se ajusta de mejor manera a las necesidades del escenario propuesto.

Tabla 21

Comparación de software de simulación de redes

Criterio	GNS3	EVE-NG	Cisco Packet Trace
Compatibilidad con MikroTik CHR	Compatible de forma nativa mediante QEMU	Compatible mediante imágenes QEMU específicas para MikroTik	No compatible; limitado a equipos y software propios de Cisco
Costo	Gratuito y de código abierto	Edición Community gratuita; edición Pro de pago	Gratuito
Requisitos de hardware	Exige más recursos en topologías grandes	Recomienda una instalación dedicada para un mejor rendimiento	Liviano; funciona en equipos de gama baja
Integración de herramientas	Integra Wireshark, VirtualBox y contenedores Docker	Integra Wireshark en la edición Pro	Integración limitada a su propio entorno

Fuente: Autoría propia

A partir de la comparación realizada, se seleccionó GNS3 como software de simulación de redes, debido a que permite integrar MikroTik CHR mediante QEMU, conectar máquinas virtuales externas y utilizar herramientas de análisis como Wireshark. Además, su flexibilidad facilita la construcción de una topología multiservicio, compuesta por routers, switches, clientes y servidores virtuales. Por estas razones, GNS3 se considera la alternativa más adecuada para implementar el escenario de evaluación de QoS.

3.4.2 Selección de la plataforma de virtualización

La selección de la plataforma de virtualización responde a los requerimientos del entorno virtualizado, debido a que esta debe permitir alojar las máquinas virtuales utilizadas para los servicios multimedia, de datos y soporte dentro del escenario simulado. Además, debe ofrecer compatibilidad con el sistema anfitrión, facilidad de administración, costo accesible y un rendimiento adecuado para la ejecución de varios servicios dentro de la misma infraestructura.

Para esta selección se compararon tres alternativas de uso extendido: VirtualBox, VMware Workstation y Proxmox VE. La comparación considera el tipo de hipervisor, el costo, la compatibilidad con el sistema anfitrión y el rendimiento esperado. En este sentido, la **Tabla 22** presenta la comparación de las plataformas de virtualización consideradas.

Tabla 22

Comparación de plataformas de virtualización

Criterio	Virtual Box	VMware Workstation	Proxox VE
Tipo de hipervisor	Tipo 2, sobre sistema operativo anfitrión	Tipo 2, sobre sistema operativo anfitrión	Tipo 1, instalación directa sobre el hardware (bare-metal)
Costo	Gratuito y de código abierto	Gratuito para uso personal; licencia paga para uso comercial	Gratuito y de código abierto; soporte empresarial opcional
Compatibilidad del sistema anfitrión	Windows, macOS, Linux y Solaris	Windows y Linux (macOS mediante VMware Fusion)	No requiere sistema operativo anfitrión adicional
Rendimiento	Adecuado para entornos académicos y de prueba a pequeña escala	Mayor rendimiento de entrada/salida que VirtualBox	Mayor rendimiento en entornos de servidor; exige administración de Linux

Fuente: Autoría propia

A partir de la comparación realizada, se seleccionó VirtualBox como plataforma de virtualización para alojar los servidores y clientes del escenario. Esta alternativa resulta adecuada para el entorno académico propuesto, debido a que es gratuita, permite ejecutar diferentes sistemas operativos invitados y se integra con el flujo de trabajo utilizado en GNS3. Además, su facilidad de instalación y administración permite desplegar máquinas virtuales destinadas a servicios como VoIP, streaming, base de datos, navegación web, FTP, IMAP y SSH, sin requerir infraestructura física especializada.

3.4.3 Selección del tipo despliegue de RouterOs

Para esta selección se compararon tres alternativas: MikroTik CHR, RouterOS x86 y RouterBOARD físico. La evaluación se realizó mediante los criterios Cumple, Parcialmente y No cumple, considerando la compatibilidad con GNS3, las funciones requeridas de RouterOS, el costo, el consumo de recursos y la facilidad de despliegue. En este sentido, la **Tabla 23** presenta el resultado de la comparación entre las alternativas disponibles para representar los routers de la topología.

La evaluación se realizó mediante una escala cualitativa de cumplimiento, conformada por los criterios Cumple**,** Parcialmente y No cumple. Esta escala permite determinar qué alternativa se ajusta mejor a las condiciones del entorno virtualizado y a las necesidades del diseño QoS. En este sentido, la Tabla R6 presenta el resultado de la comparación entre las alternativas disponibles para representar los routers de la topología.

Tabla 23

Resultados de la selección del tipo de router

Requisito	CHR	RouterOs X86	RouterBoard físico
Compatibilidad con GNS3	Cumple	Parcialmente	No cumple
Funciones de RouterOS v7 (Mangle, Queue Tree, PCQ, OSPF, VLAN)	Cumple	Cumple	Cumple
Múltiples instancias sin licencia individual	Cumple	Parcialmente	No cumple
Costo accesible	Cumple	Parcialmente	No cumple
Bajo consumo de CPU/RAM	Cumple	Parcialmente	No cumple
Instalación directa en el simulador	Cumple	Parcialmente	No cumple
Soporte vigente del fabricante	Cumple	Cumple	Cumple

Puntaje Total	14/14	8/14	4/14

Fuente: Autoría propia

Como se observa en la **Tabla 23**, la alternativa MikroTik CHR obtuvo el mayor puntaje, con un cumplimiento total de 14/14. Este resultado se debe a que CHR está orientado específicamente a entornos virtualizados, permite integrarse con GNS3, facilita la creación de múltiples routers dentro de una misma topología y mantiene las funciones necesarias de RouterOS v7 para el diseño QoS, tales como Mangle, Queue Tree, PCQ, OSPF y VLAN.

RouterOS x86 obtuvo un puntaje intermedio de 8/14, debido a que conserva las funciones principales de RouterOS, pero presenta limitaciones en facilidad de despliegue, consumo de recursos e integración directa con el simulador. Por su parte, RouterBOARD físico alcanzó 4/14, ya que, aunque cuenta con soporte completo de RouterOS, no responde adecuadamente a las condiciones del entorno virtualizado, al requerir equipos físicos individuales y mayor inversión económica.

Con base en estos resultados, se seleccionó MikroTik CHR como tipo de router para representar los cinco nodos MikroTik de la topología. Esta alternativa permite construir un escenario flexible, escalable y compatible con el entorno de simulación, sin depender de infraestructura física especializada. Además, su uso mantiene coherencia con el propósito del trabajo, orientado a evaluar la calidad de servicio en sistemas de comunicación multimedia implementados sobre máquinas virtuales.

3.4.4 Selección del nivel de licencia CHR

Una vez seleccionado MikroTik CHR como tipo de router virtual, es necesario definir el nivel de licencia que será utilizado dentro del entorno de simulación. Esta decisión resulta importante porque las licencias CHR permiten ejecutar las funciones de RouterOS, pero se

diferencian principalmente por el límite de velocidad permitido por interfaz y por el costo asociado.

Para el presente escenario se consideran dos niveles de licencia: CHR Free y CHR P1. Ambos pueden ser utilizados dentro de la topología, ya que permiten acceder a las funcionalidades necesarias de RouterOS para la configuración de enrutamiento, VLAN, Mangle, Queue Tree, PCQ y políticas de calidad de servicio. Sin embargo, la diferencia principal se encuentra en la capacidad de transmisión disponible por interfaz. La **Tabla 24** presenta la comparación entre estos dos niveles de licencia.

Tabla 24

Comparación de niveles de licencia CHR

Criterio	CHR Free	CHR P1
Límite de velocidad por interfaz	1 Mbit/s	1 Gbit/s
Costo	Gratuito	USD 45, licencia perpetua
Aplicabilidad en entorno académico	Alta, para pruebas controladas y simulación	Alta, para escenarios con mayor demanda de tráfico.
Uso recomendado	Laboratorios, pruebas de configuración y evaluación con ancho de banda limitado	Laboratorios avanzados o escenarios donde se requiera mayor capacidad de transmisión.
Impacto del diseño QoS	Permite generar congestión de forma controlada y dimensionar colas con una capacidad de referencia reducida	Permite evaluar el comportamiento de QoS con mayor capacidad de enlace.

Fuente: Autoría propia

Para un escenario académico y de simulación controlada, CHR Free resulta suficiente, debido a que mantiene disponibles las funciones necesarias de RouterOS y establece un límite de 1 Mbit/s por interfaz. Esta restricción puede utilizarse como una capacidad de referencia

para observar el comportamiento de la red ante congestión y dimensionar los parámetros de QoS. De esta manera, la selección del nivel de licencia CHR da cumplimiento al RQ-VIR-03, al considerar las limitaciones de recursos propias de la implementación virtual: el límite de 1 Mbit/s por interfaz se toma como referencia para definir la capacidad de los escenarios de prueba.

No obstante, CHR P1 también constituye una alternativa válida cuando se requiere incrementar la capacidad de transmisión hasta 1 Gbit/s por interfaz, especialmente en escenarios con mayor volumen de tráfico o pruebas más exigentes. Por tanto, la licencia se define verificando el throughput total esperado del laboratorio frente al límite permitido por cada nivel.

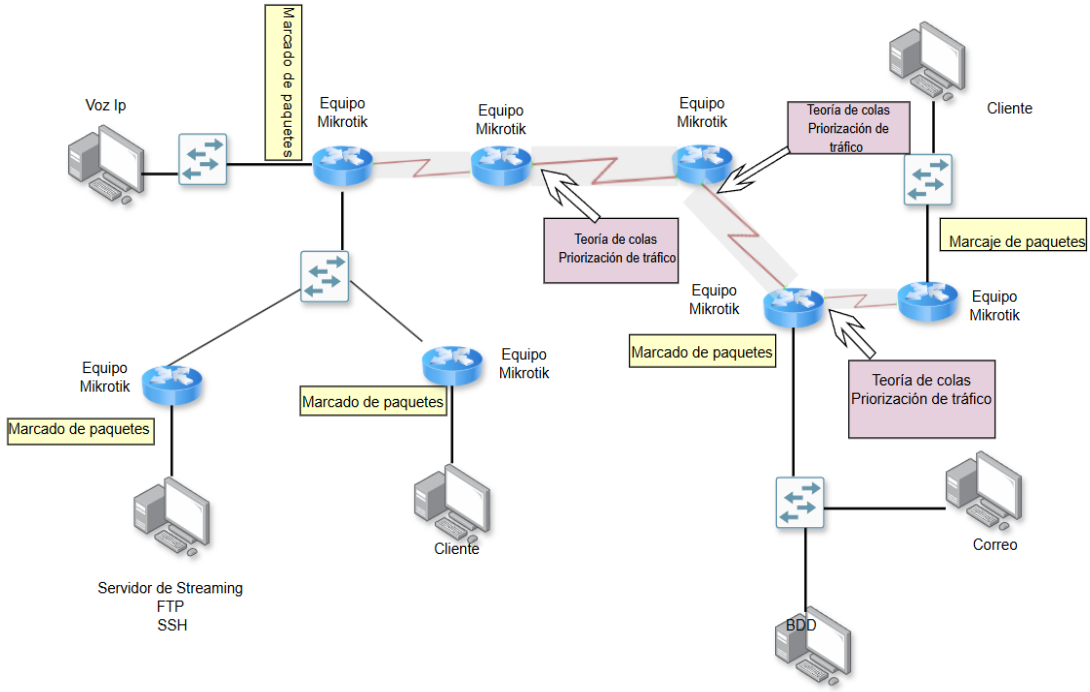
3.5 Despliegue de topología virtualiza

3.5.1 Topología planteada

Como se observa en la **Figura 15**, la topología de red propuesta representa un entorno multiservicio diseñado para la evaluación de políticas de Calidad de Servicio (QoS). La infraestructura se basa en una arquitectura virtualizada que integra routers MikroTik, servidores multimedia y clientes distribuidos en diferentes segmentos de red.

Figura 15

Topología de red virtualizada para gestión de tráfico multimedia



Nota: *El gráfico muestra la arquitectura de una red con equipos Mikrotik, destacando la conectividad entre servicios como Voz Ip, Streaming, Correo y Base de Datos.* Fuente: Autoría propia

3.5.2 Plan de direccionamiento IP

En el siguiente apartado se describe el direccionamiento IP implementado en la topología de red. El direccionamiento permite identificar de manera única a cada dispositivo dentro de la red, facilitando la comunicación entre los distintos segmentos y el acceso a los servicios implementados (Bustos et al., 2023).

Debido a que la implementación se realizó en un entorno de simulación mediante la herramienta de GNS3, se emplearon direcciones IPV4 privadas conforme a lo establecido en el RFC 1918, estas direcciones permiten la construcción de redes internas sin requerir asignaciones públicas, como se puede verificar en la **Tabla 25**.

Tabla 25

Clases de direcciones IP privadas

Tipo	Red	Hasta
Clase A	10.0.0.0	10.255.255.255

Tipo	Red	Hasta
Clase B	172.16.0.0	172.31.255.255
Clase C	192.168.0.0	192.168.255.255

Nota: *Rangos de direcciones IPv4 privadas según su clasificación en clases A, B y C.* Fuente: Autoría propia

Considerando el esquema de direccionamiento IPv4 descrito anteriormente, se procede a la aplicación del método de VLSM con el objetivo de distribuir de manera eficiente las direcciones IP entre los distintos equipos y segmentos de la red. El uso de VLSM permite asignar rangos de direcciones acordes a las necesidades reales de cada subred, optimizando el aprovechamiento del espacio de direcciones disponibles, como se puede verificar en la **Tabla 26**, **Tabla 27**, **Tabla 28** y **Tabla 29**.

Tabla 26

Asignación de direcciones IPv4 para enlaces punto a punto

Sitio	N° Hosts	Dirección de red	Prefijo	Rango	Broadcast
R1 - R5	2	10.10.10.0	/30	.1 - .2	.3
R1 - R2	2	10.10.10.4	/30	.5 - .6	.7
R2 - R3	2	10.10.10.8	/30	.9 - .10	.11
R3 - R4	2	10.10.10.12	/30	.13 - .14	.15

Fuente: Autoría propia

Tabla 27

Asignación de direcciones IPv4 para VLANs en R3

VLAN ID	Tipo de VLAN	Dirección de red	Prefijo	Rango	Interfaz

10	Clientes	172.16.7.0	/24	.1 - .254	ether3
20	Servidores	172.16.8.0	/25	.1 - .126	ether3
30	Administrativa	172.16.8.129	/28	.130 - .144	ether3

Fuente: Autoría propia

Tabla 28

Asignación de direcciones IPv4 para VLANs en R4

VLAN ID	Tipo de VLAN	Dirección de red	Prefijo	Rango	Interfaz
10	Clientes	172.16.1.0	/24	.1 - .254	ether2
20	Servidores	172.16.2.0	/25	.1 - .126	ether2
30	Administrativa	172.16.2.129	/28	.130 - .144	ether2

Fuente: Autoría propia

Tabla 29

Asignación de direcciones IPv4 para VLANs en R5

VLAN ID	Tipo de VLAN	Dirección de red	Prefijo	Rango	Interfaz
10	Clientes	172.16.3.0	/24	.1 - .254	ether1
20	Servidores	172.16.4.0	/25	.1 - .126	ether1
30	Administrativa	172.16.4.129	/28	.130 - .144	ether1
10	Clientes	172.16.5.0	/24	.1 - .254	ether2
20	Servidores	172.16.6.0	/25	.1 - .126	ether2
30	Administrativa	172.16.6.129	/28	.130 - .144	ether2

Fuente: Autoría propia

El diseño de direccionamiento IP implementado responde a los principios de eficiencia, organización y escalabilidad establecidos para la topología propuesta, la aplicación de VLSM permite asignar a cada subred un prefijo acorde con sus requerimientos específicos, tanto los enlaces punto a punto como en las redes asociadas a las VLANS segmentadas por función (clientes, servidores, administrativas), optimizando el uso del espacio de direccionamiento IPV4 y evitando la sobreasignación innecesaria de direcciones.

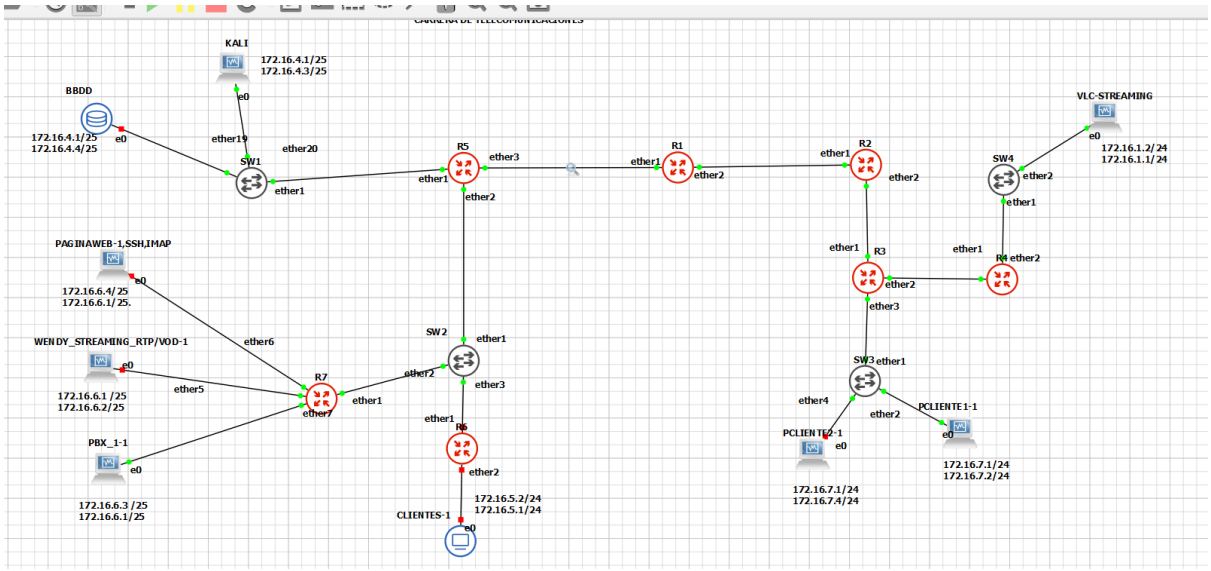
3.5.3 Diseño de la topología propuesta

En esta sección se muestra una red diseñada para interconectar diferentes servicios y equipos finales mediante el uso de RouterOS y switches. Cada segmento de la red corresponde a una red local independiente, en la cual los switches permiten la conexión de los dispositivos, mientras que los routers MikroTik gestionan el envío del tráfico hacia otros segmentos. Esta disposición permite que los datos circulen entre los distintos puntos de la red de forma controlada y ordenada.

La topología implementada facilita la evaluación del comportamiento del tráfico de voz, video y datos al atravesar múltiples enlaces de red. Además, permite aplicar mecanismos de Calidad de Servicio (QoS) sobre los routers, para priorizar determinados tipos de tráfico y evaluar su desempeño bajo condiciones de congestión, tal como se observa en la **Figura 16**.

Figura 16

Topología de red implementada en GNS3



Nota: *La figura muestra la topología de la red implementada con dispositivos MikroTik y sus respectivas conexiones, incluyendo los enlaces punto a punto y las VLANs asociadas a cada router para los segmentos de Clientes, Servidores y Administración.*
Fuente: Autoría propia

La topología implementada permite:

- Evaluar el impacto de la congestión en el tráfico multimedia.
- Analizar métricas de desempeño como latencia, jitter, ancho de banda y pérdida de paquetes.
- Comparar el comportamiento de la red con y sin mecanismos de QoS.
- Validar la efectividad de las herramientas de priorización implementadas en dispositivos MikroTik.

3.6 Diseño del esquema de enrutamiento

La configuración del enrutamiento es fundamental para garantizar la comunicación eficiente y continua entre todos los segmentos de la red. Este procedimiento se llevó a cabo en dos etapas principales: primero, se asignaron direcciones IP a cada interfaz de acuerdo con la

estrategia de VLSM establecida; posteriormente, se implementó el protocolo OSPF, lo que permitió a los routers intercambiar información de rutas de manera automática y dinámica, asegurando la conectividad integral de la red.

3.6.1 Asignación de direccionamiento IP

Siguiendo el plan de direccionamiento definido en las Tablas 9 a 12, se procedió a configurar las direcciones IP en cada interfaz de los routers MikroTik. La asignación considera tanto los enlaces punto a punto entre routers (red 10.10.10.0/30) y la segmentación mediante VLAN. En la **Tabla 30** se presenta las direcciones IP asignadas a los routers e interfaces de la red.

Tabla 30

Direcciones IP asignadas a los routers e interfaces de la red

Router	Interfaz	Dirección IP	Prefijo	Descripción
R1	ether1	10.10.10.1	/30	Enlace R1-R5
	ether2	10.10.10.5	/30	Enlace R1-R2
R2	ether1	10.10.10.6	/30	Enlace R2-R1
	ether2	10.10.10.9	/30	Enlace R2-R3
	ether1	10.10.10.10	/30	Enlace R3-R2
	ether2	10.10.10.13	/30	Enlace R3-R4
R3	vlan10	172.16.7.1	/24	Gateway VLAN 10 (Clientes)
	vlan20	172.16.8.1	/25	Gateway VLAN 20 (Servidores)
	vlan30	172.16.8.130	/28	Gateway VLAN 30 (Administrativa)
	ether1	10.10.10.14	/30	Enlace R4-R3
R4	vlan10	172.16.1.1	/24	Gateway VLAN 10 (Clientes)
	vlan20	172.16.2.1	/25	Gateway VLAN 20 (Servidores)
	vlan30	172.16.2.130	/28	Gateway VLAN 30 (Administrativa)
	ether1	10.10.10.2	/30	Enlace R5-R1
	vlan10	172.16.3.1	/24	Gateway VLAN 10 (Clientes)
R5	vlan20	172.16.4.1	/25	Gateway VLAN 20 (Servidores)

Router	Interfaz	Dirección IP	Prefijo	Descripción
	vlan30	172.16.4.130	/28	Gateway VLAN 30 (Administrativa)
	vlan10-2	172.16.5.1	/24	Gateway VLAN 10 (Clientes - ether2)
	vlan20-2	172.16.6.1	/25	Gateway VLAN 20 (Servidores - ether2)
	vlan30-2	172.16.6.130	/28	Gateway VLAN 30 (Administrativa - ether2)

Nota: *La tabla presenta la asignación de direcciones IP según la estrategia de segmentación por VLANs y enlaces punto a punto entre routers, siguiendo la planificación de direccionamiento VLSM.*
Fuente: Autoría propia

Para evitar redundancia, la configuración completa del direccionamiento IP de los routers se presenta en el Anexo 7.1, denominado Configuración de direccionamiento IP de routers, donde se detalla la asignación de direcciones correspondiente a cada interfaz de la red.

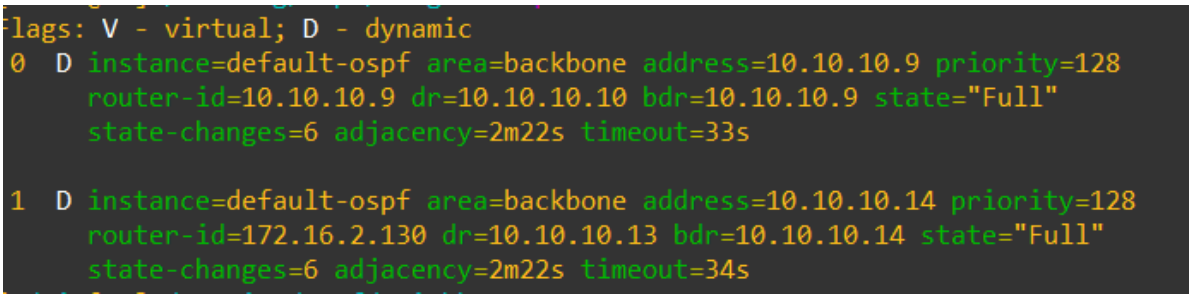
3.6.2 Protocolo de enrutamiento OSPF

Verificada la conectividad a nivel de enlace y la correcta asignación de direcciones IP en cada una de las interfaces de los RouterOS, se procede a implementar el protocolo de enrutamiento OSPF, la elección responde a su soporte nativo para VLSM, garantizando una convergencia rápida ante cambios en la red y es ampliamente utilizado en infraestructuras empresariales.

Los parámetros OSPF en RouterOS, ya sea a través de la interfaz gráfica de Winbox o mediante la interfaz de la línea de comando (CLI), son equivalente e incluyen la definición de área, asignación de interfaces participantes y la configuración de los identificadores de cada uno de los equipos. El proceso de configuración OSPF se realiza en cada uno de los routers; en esta sección, se describe la configuración aplicada dentro de R3, la cual sirve como referencia para el resto de equipos. Las configuraciones correspondientes a los demás equipos se encuentran dentro del **Anexo 7.2,** titulado Configuración OSPF. En la **Figura 17** se presenta la configuración OSPF R3: instancia, área e interfaces.

Figura 17

Configuración OSPF R3: instancia, área e interfaces



3.6.3 Diseño de la segmentación mediante VLAN

La segmentación de la red se lleva a cabo mediante el uso de VLAN, en equipos Mikrotik con RouterOS v7, lo que permite dividir la infraestructura física en múltiples redes lógicas independientes.

Por este motivo, se procede a segmentar la red con el objetivo de:

- Segmentar el tráfico por tipo de usuario.
- Reducir dominios de broadcast
- Incrementar la seguridad
- Facilita la aplicación de las políticas de QoS

Se definieron tres VLAN en cada router de acceso, con el propósito de segmentar lógicamente la red según el tipo de servicio y usuario:

- **VLAN 10:** Red de clientes
- **VLAN 20:** Red de servidores
- **VLAN 30:** Red administrativa

Cada VLAN funciona como un dominio de broadcast independiente, permitiendo el aislamiento del tráfico y la reducción de colisiones dentro de cada segmento, pese a que todas operan sobre la misma infraestructura física.

En el caso de los routers MikroTik, la segmentación se implementa mediante la creación de interfaces VLAN sobre la interfaz física principal y su posterior asociación a un bridge, permitiendo una gestión flexible y centralizada del tráfico. Por su parte, en dispositivos Cisco Systems, la segmentación se realiza mediante la configuración de subinterfaces o interfaces VLAN en conjunto con enlaces troncales, siguiendo el estándar IEEE 802.1Q(CCNA, 2018).

3.6.4 Esquema de segmentación lógica (VLAN 10,20,30)

En correspondencia con el diseño lógico previamente descrito, se procede a implementar las interfaces correspondientes a cada una de las VLAN en los dispositivos de red, estableciendo una base sólida para la segmentación efectiva del tráfico.

En la **Tabla 31** se presenta la estructura de segmentación lógica de la red, indicando el tipo de red, la máscara de subred y el propósito asignado a cada VLAN.

Tabla 31

Esquema de segmentación lógica de la red mediante VLAN.

VLAN	Tipo de RED	Máscara	Propósito
VLAN 10	Clientes	/24	Acceso de usuarios finales
VLAN 20	Servidores	/25	Servicios multimedia
VLAN 30	Administrativa	/28	Gestión y administración

Nota: *Elaboración propia a partir del diseño de segmentación de la red.*
Fuente: Autoría propia

En los dispositivos Mikrotik, la implementación de VLAN se realiza mediante la creación de interfaces virtuales asociadas a una interfaz física. Cada interfaz VLAN se identifica mediante una VLAN ID, el cual permite diferencias los distintos segmentos de red dentro de un mismo enlace físico siguiendo el estándar IEEE 802.1Q.

Posteriormente, a cada interfaz VLAN se le asigna una dirección IP que actúa como puerta de enlace para los dispositivos pertenecientes a cada segmento de red. Además, estas interfaces se integran al protocolo de enrutamiento dinámico OSPF, configurándolas como

interfaces pasivas con el fin de anunciar las redes sin establecer adyacencias innecesarias con otros routers.

3.6.5 Enlaces troncales

Con el fin de permitir la transmisión de múltiples VLAN a través de un mismo enlace físico, se implementan enlaces troncales entre los switches y los routers de acceso de la topología. Estos enlaces permiten transportar tráfico perteneciente a diferentes VLAN mediante el etiquetado de tramas utilizando el estándar IEEE 802.1Q.

En la mayoría de dispositivos Mikrotik, la implementación de enlaces troncales se realiza mediante la utilización de bridges con filtrado VLAN habilitado, dado que esta funcionalidad permite definir que interfaces transportarán tráfico etiquetado (tagged) y cuáles van operar como puertos de acceso dentro de cada VLAN.

En la topología implementada, los puertos conectados hacia los routers se configuran como puertos troncales, permitiendo el transporte simultáneo de las VLAN 10, 20 y 30. Por otro lado, los puertos destinados a dispositivos finales se configuran como puertos de acceso, asignándoles un PVID correspondiente a la VLAN del segmento al que pertenecen.

3.6.6 Políticas de acceso entre VLAN

Para reforzar la seguridad de la red segmentada, se implementan políticas de control de acceso entre VLAN mediante reglas de firewall en los routers de acceso. Estas políticas permiten controlar la comunicación entre los diferentes segmentos de red, evitando accesos no autorizados.

Para esto se procede a definir las listas de direcciones que permiten agrupar las redes asociadas a cada tipo de usuario dentro de la infraestructura de red. Este mecanismo facilita la implementación de políticas de control de acceso y seguridad de forma más estructurada,

permitiendo aplicar reglas de filtrado basadas en grupos de direcciones IP en lugar de configuraciones individuales.

- Clientes (VLAN 10)
- Servidores (VLAN 20)
- Administradores (VLAN 30)

Posteriormente, se establecen reglas de filtrado que determinan qué tipos de tráfico están permitidos entre estos grupos.

Las políticas implementadas permiten que:

- Los administradores tengan acceso completo a todos los segmentos de la red.
- Los clientes puedan comunicarse únicamente con dispositivos dentro de su misma VLAN.
- Los servidores puedan comunicarse entre sí para el funcionamiento de los servicios.
- Todo tráfico inter-VLAN no autorizado sea bloqueado.

Con base en estas políticas, se procede a implementar la configuración correspondiente en los routers del entorno de red.

Tabla 32

Políticas de control de acceso entre VLAN implementadas en la red

Origen	Destino	Acción	Descripción
VLAN 30	Todas	Permitido	Acceso administrativo
VLAN 10	VLAN 10	Permitido	Comunicación entre clientes
VLAN 20	VLAN 20	Permitido	Comunicación entre servidores
VLAN 10	VLAN 20/30	Bloqueado	Restricción de acceso
VLAN 20	VLAN 10/30	Bloqueado	Restricción de acceso

Fuente: Autoría propia

Como se observa en la **Tabla 32**, las políticas implementadas permiten mantener un aislamiento entre los distintos segmentos de red, garantizando que únicamente los administradores dispongan de acceso completo, mientras que los clientes y servidores se encuentran restringidos según su función dentro de la infraestructura.

3.7 **Diseño de los parámetros de QoS**

Como punto de partida se realizó un levantamiento de la red implementada, en el que se registraron los equipos que conforman la topología, los segmentos definidos, las interfaces y enlaces existentes, y los servicios desplegados sobre cada segmento. Este levantamiento, cuyo detalle se presenta en el **Anexo 7.3**, permitió reconocer las condiciones reales sobre las que debe operar la política de calidad de servicio y constituye la base a partir de la cual se procede a realizar la auditoría de tráfico desarrollada más adelante en este capítulo.

3.7.1 Auditoría de tráfico de red

La auditoría de tráfico de red responde al requerimiento RQ-FUN-01, debido a que permite identificar los servicios multimedia y de datos utilizados dentro de la topología. Esta etapa consiste en observar los flujos generados por cada servicio, reconocer los protocolos y puertos asociados, y comprobar el tipo de tráfico que circula entre clientes y servidores.

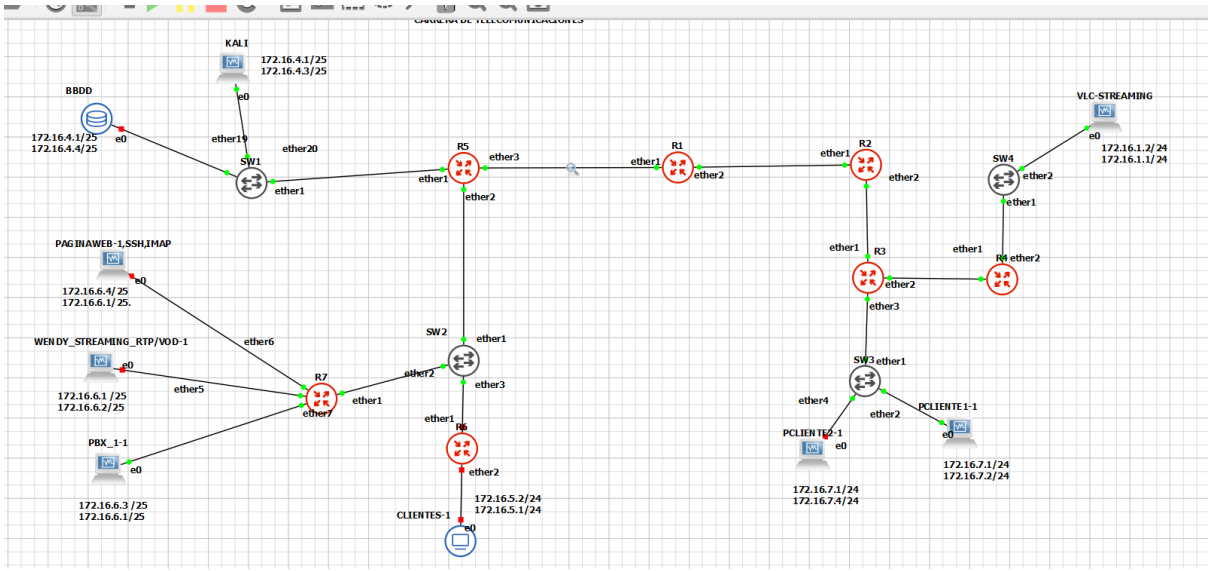
Además, la auditoría sirve como base para establecer la línea de referencia considerada en el requerimiento RQ-PRU-01, ya que permite conocer el comportamiento inicial del tráfico antes de aplicar la política QoS. A partir de esta información será posible comparar, en una etapa posterior, el desempeño de la red bajo condiciones sin QoS y con QoS.

Como etapa previa a la implementación de Calidad de Servicio, se realizó una auditoría de tráfico con el propósito de identificar los protocolos, puertos y flujos generados por los servicios implementados en el entorno virtualizado. Para ello, se tomó como referencia la

topología general de la red, donde se ubican los segmentos de clientes, servidores y dispositivos de interconexión. Esta vista permitió contextualizar el recorrido del tráfico antes de realizar la validación específica mediante capturas en Wireshark. En la **Figura 18** se presenta la topología desplegada para la auditoría de red.

Figura 18

Topología desplegada para la auditoría de red



Fuente: Autoría propia

3.7.1.1 Auditoría VoIP

Dentro del servicio de telefonía IP se identificaron dos tipos de tráfico: la señalización SIP y el flujo de voz RTP. Esta identificación resulta necesaria debido a que el tráfico VoIP es sensible al retardo, a la variación del retardo y a la pérdida de paquetes, condiciones que pueden afectar directamente la calidad de la comunicación. Por ello, estos flujos deben ser reconocidos previamente para su posterior clasificación, marcaje y priorización dentro de las políticas de calidad de servicio.

- **Señalización SIP**

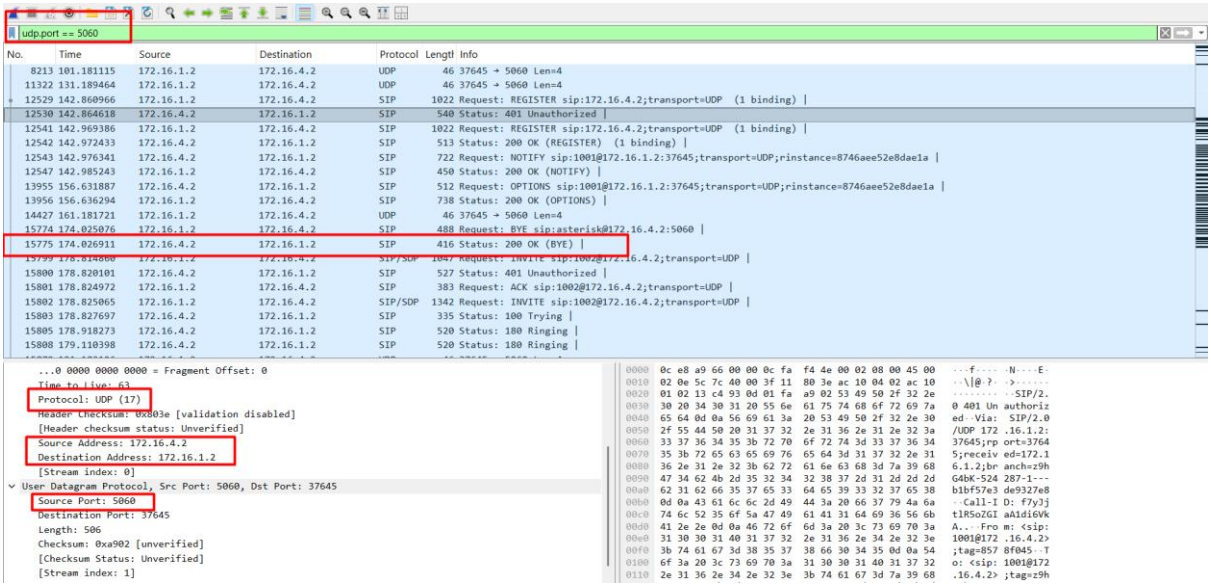
Para el servicio de señalización VoIP se capturó el tráfico generado durante el registro de extensiones y el establecimiento de llamadas entre los clientes configurados en la PBX

Issabel. Con el fin de aislar este flujo en Wireshark, se aplicó el filtro `udp.port == 5060`, correspondiente al puerto empleado por el protocolo SIP.

Como se observa en la **Figura 19**, la comunicación se establece entre el cliente con dirección 172.16.1.2 y el servidor Issabel con dirección 172.16.6.3. En el detalle del paquete se confirma el uso de UDP como protocolo de transporte y el puerto 5060, permitiendo asociar este flujo al servicio de señalización de telefonía IP. La identificación de este flujo permitirá considerar el puerto 5060/UDP como referencia para el tratamiento del tráfico de señalización durante la etapa de calidad de servicio.

Figura 19

Identificación del tráfico SIP mediante Wireshark



Nota: *Captura del tráfico de esteblecimiento VoIP. Se identifica el protocolo SIP sobre UDP, asociado al puerto 5060, durante el registro de extensiones y el establecimiento de llamadas.*
Fuente: Autoría propia

- **Flujo de voz RTP**

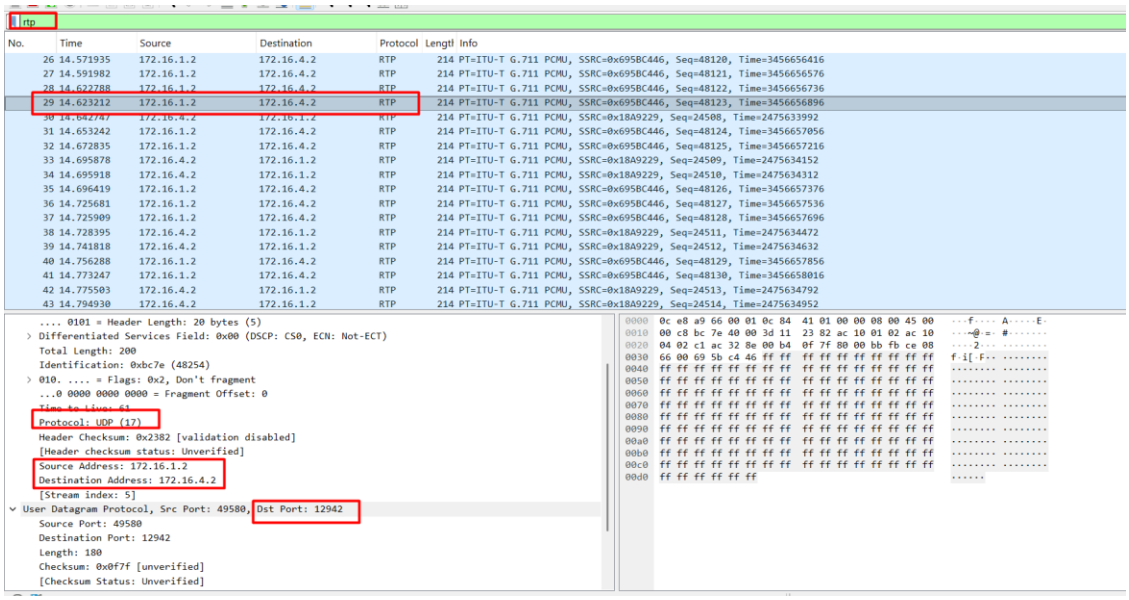
Para el servicio de audio en tiempo real se capturó el tráfico generado durante el establecimiento y mantenimiento de llamadas entre los clientes configurados en la PBX Issabel.

Con el fin de aislar este flujo en Wireshark, se aplicó el filtro ***rtp***, correspondiente al protocolo de transporte en tiempo real utilizado para la transmisión de voz sobre IP.

Como se observa en la **Figura 20**, la comunicación se establece de forma bidireccional entre el cliente con dirección 172.16.1.2 y el servidor Issabel con dirección 172.16.6.3. En el detalle del paquete se confirma el uso de UDP como protocolo de transporte, el códec G.711 PCMU como formato de codificación de audio, y números de secuencia consecutivos que evidencian un flujo continuo de paquetes de voz. La identificación de este flujo permitirá considerar el rango de puertos 10000-20000/UDP como referencia para el tratamiento del tráfico de audio RTP durante la etapa de calidad de servicio.

Figura 20

Identificación del tráfico RTP mediante Wireshark



***Nota**: Captura del tráfico de señalización VoIP. Se identifica el protocolo RTP sobre UDP, asociado a los puertos 10000-20000, durante la señalización de llamada.*
Fuente: Autoría propia

3.7.1.2 Auditoría Streaming

Dentro de los servicios multimedia se identificaron dos tipos de tráfico de video: streaming en tiempo real y VoD. La identificación de estos flujos resulta necesaria debido a

que el tráfico multimedia puede verse afectado por el retardo, la variación del retardo y la pérdida de paquetes. Por ello, estos servicios deben ser reconocidos previamente para su posterior clasificación, marcaje y priorización dentro de las políticas de calidad de servicio.

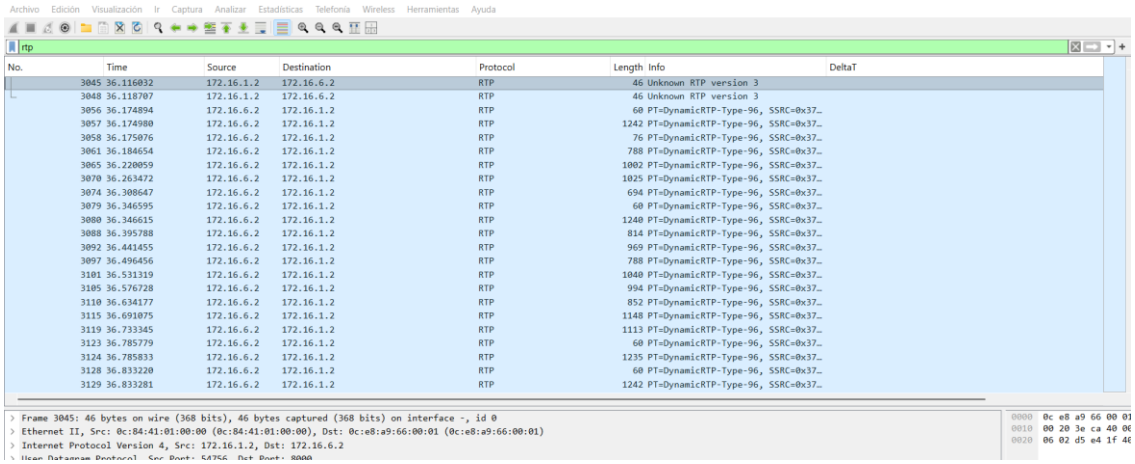
- **Streaming en tiempo real**

Para el servicio de streaming en tiempo real, la política de QoS identifica el tráfico de MediaMTX mediante RTP/RTCP sobre UDP en el rango 8000-8001 y la sesión RTSP sobre TCP en el puerto 8554. En las reglas Mangle se consideran los puertos de origen y destino 8000-8001 para UDP y el puerto de destino 8554 para RTSP, de modo que ambos flujos queden asociados a la marca de conexión rtp-conn.

Esta identificación permite tratar el flujo de streaming en tiempo real como una única clase de servicio: la conexión se marca como rtp-conn, el campo DSCP se reescribe con AF41 (34) y los paquetes reciben la marca rtp-pkt, utilizada posteriormente por Queue Tree. En la **Figura 21** se presenta la captura de tráfico RTMP identificada durante la auditoría inicial.

Figura 21

Captura de tráfico RTP identificada durante la auditoría inicial.



***Nota**: Captura del tráfico de Streaming. Se identifica el protocolo RTP sobre UDP, asociado a los puertos 8000, durante la reproducción.*
Fuente: Autoría propia

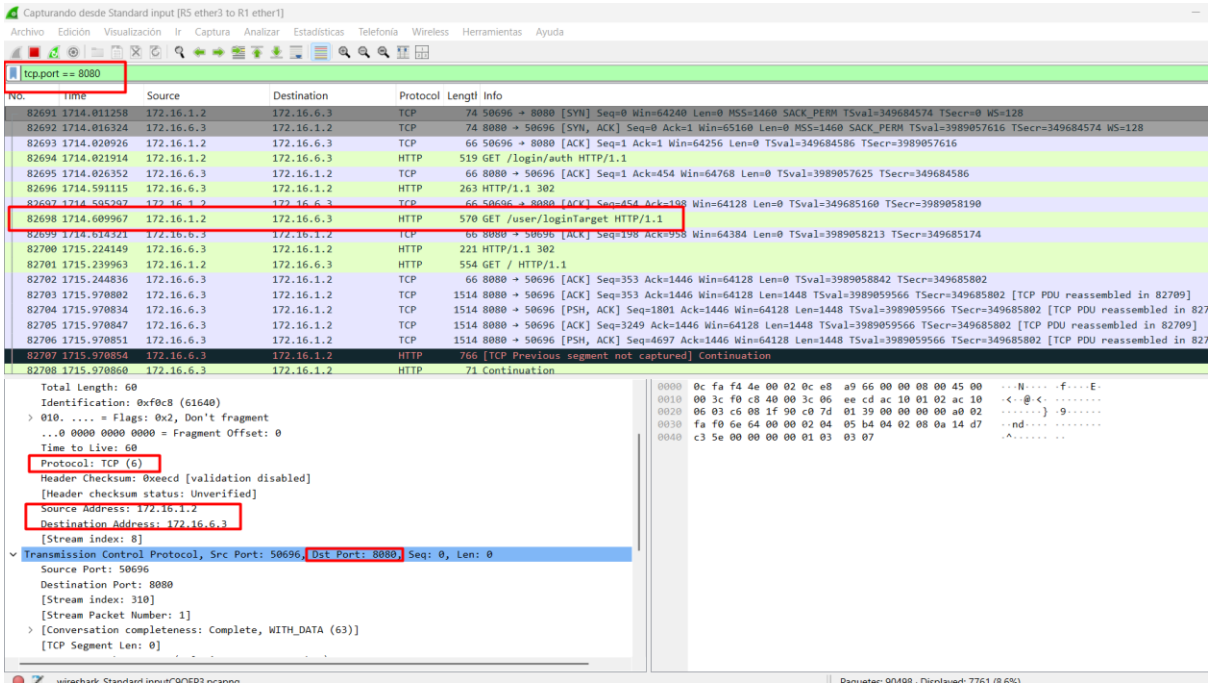
- **VoD**

Para el servicio de streaming almacenado se capturó el tráfico generado durante el acceso a la plataforma Streama. Con el fin de aislar este flujo en Wireshark, se aplicó el filtro ***tcp.port == 8080***, correspondiente al puerto utilizado por la aplicación web del servicio.

Como se observa en la **Figura 22**, la captura permite identificar tráfico HTTP transportado sobre TCP y asociado al puerto 8080. En el detalle del paquete se evidencia el uso de dicho puerto, lo que permite reconocer este flujo como tráfico correspondiente al servicio de streaming almacenado. Esta identificación permite considerar el puerto 8080/TCP como referencia para la clasificación y tratamiento del tráfico VoD durante la etapa de calidad de servicio.

Figura 22

Identificación del tráfico HTTP mediante Wireshark.



Nota: *Captura del tráfico generado durante el acceso a la plataforma Streama. Se identifica el protocolo HTTP sobre TCP, asociado al puerto 8080.*

Fuente: Autoría propia

La identificación de este flujo permitirá considerar el puerto 8080/TCP como referencia para el tratamiento del tráfico correspondiente al servicio de streaming almacenado durante la etapa de calidad de servicio

3.7.1.3 Auditoría de datos y soporte

Dentro de los servicios de datos y soporte se consideraron los flujos correspondientes a base de datos, transferencia de archivos, acceso remoto, navegación web y correo electrónico. La identificación de estos servicios permite reconocer los puertos y protocolos utilizados dentro de la red, con el fin de establecer referencias para su posterior clasificación y tratamiento durante la etapa de calidad de servicio.

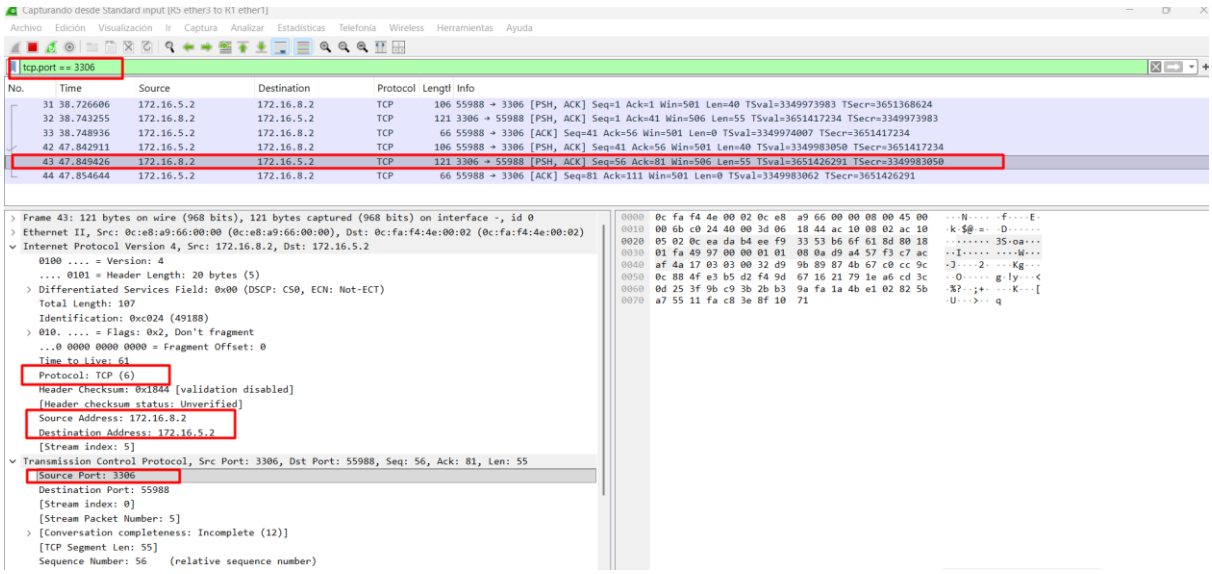
- **Base de Datos**

Para el servicio de base de datos se capturó el tráfico generado durante la ejecución de consultas hacia el servidor MySQL. Con el fin de aislar este flujo en Wireshark, se aplicó el filtro ***tcp.port == 3306***, correspondiente al puerto utilizado por MySQL.

Como se observa en la **Figura 23**, la captura permite identificar tráfico MySQL transportado sobre TCP y asociado al puerto 3306. En el detalle del paquete se evidencia el uso de dicho puerto, lo que permite reconocer este flujo como tráfico de base de datos. Esta identificación permite considerar el puerto 3306/TCP como referencia para su clasificación y tratamiento durante la etapa de calidad de servicio

Figura 23

Identificación del tráfico MYSQL mediante Wireshark



Nota: *Captura del tráfico generado por el servicio de base de datos. Se identifica el protocolo MySQL sobre TCP, asociado al puerto 3306.*
Fuente: Autoría propia

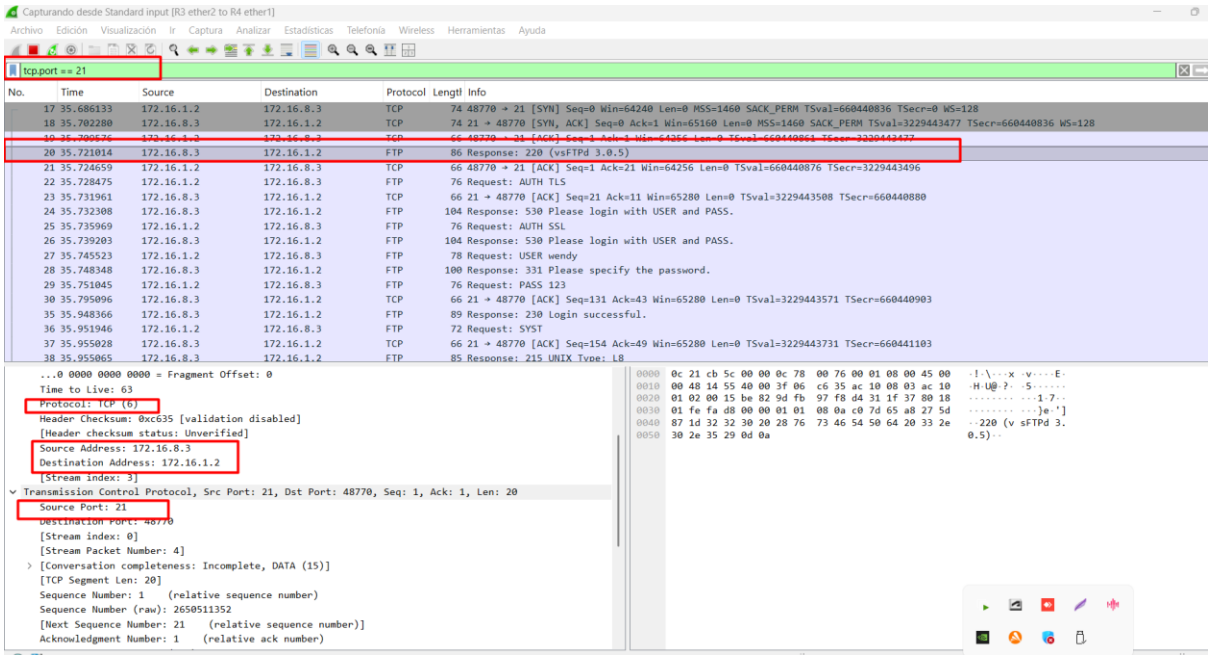
- **Transferencia de archivos FTP**

Para el servicio de transferencia de archivos se identificó el canal de control FTP sobre TCP 21. La configuración de Mangle final también contempla el tráfico de datos con src-port=20, por lo que ambos componentes forman parte de la clase baja-conn.

La clasificación de FTP considera, por tanto, TCP 21 para el control de la sesión y TCP con puerto de origen 20 para el canal de datos, de acuerdo con las reglas aplicadas en RouterOS. Esta distinción evita limitar el reconocimiento de FTP únicamente al canal de control. En la **Figura 24** se presenta la identificación del tráfico FTP mediante Wireshark.

Figura 24

Identificación del tráfico FTP mediante Wireshark



Nota: Captura del tráfico generado durante una sesión de transferencia de archivos. Se identifica el protocolo FTP sobre TCP, asociado al puerto 21.

Fuente: Autoría propia

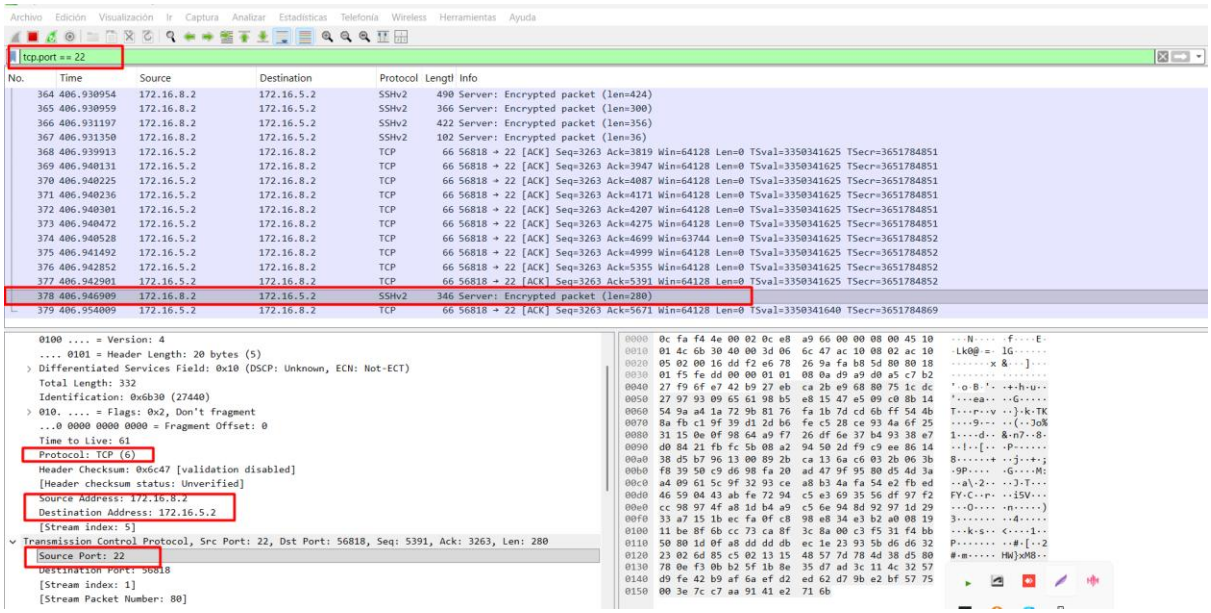
- **Acceso remoto SSH**

Para el servicio de administración remota se capturó el tráfico generado durante una sesión SSH activa. Con el fin de aislar este flujo en Wireshark, se aplicó el filtro ***tcp.port == 22***, correspondiente al puerto utilizado por el protocolo SSH.

Como se observa en la **Figura 25**, la captura permite identificar tráfico SSH transportado sobre TCP y asociado al puerto 22. A diferencia de otros servicios, el contenido de la sesión se mantiene cifrado, característica propia del protocolo SSH para proteger la administración remota. Esta identificación permite considerar el puerto 22/TCP como referencia para su clasificación y tratamiento durante la etapa de calidad de servicio.

Figura 25

Identificación del tráfico SSH mediante Wireshark



Nota: *Captura del tráfico generado durante una sesión de acceso remoto. Se identifica el protocolo SSH sobre TCP, asociado al puerto 22.*
Fuente: Autoría propia

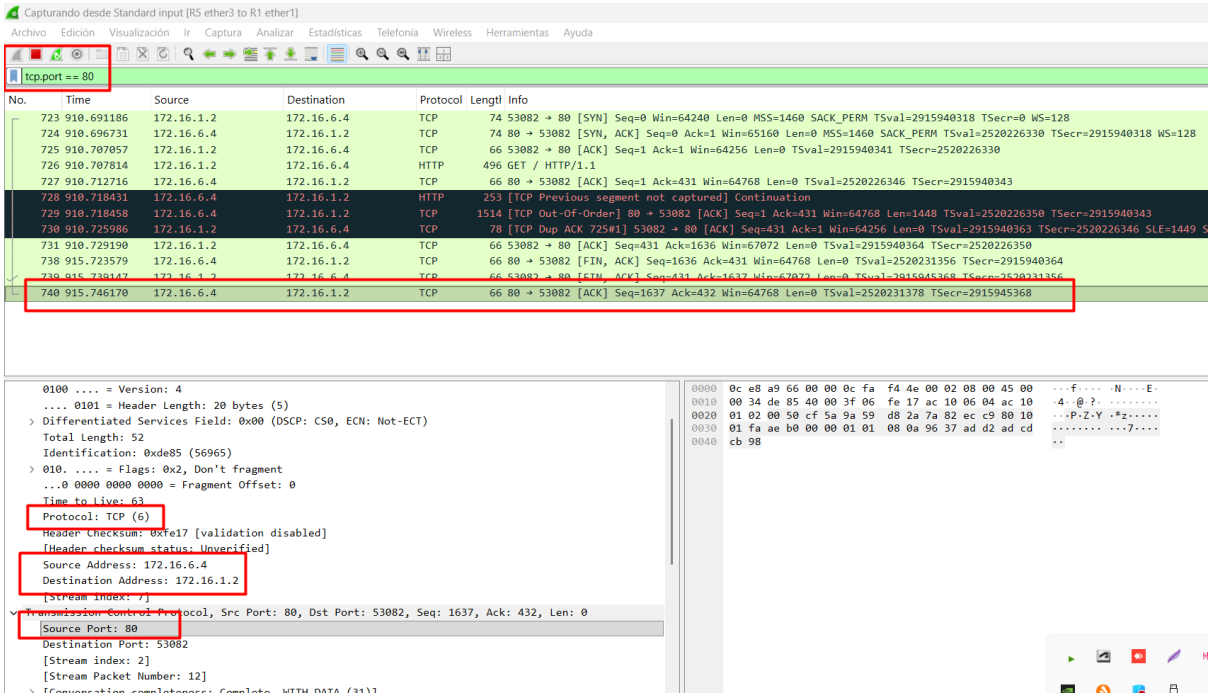
- **Navegación web**

El tráfico del servicio web fue capturado durante el acceso a la aplicación desde un equipo cliente, aplicando el filtro `tcp.port == 80` para delimitar el flujo de interés.

Como se observa en la **Figura 26**, la captura permite identificar tráfico HTTP transportado sobre TCP y asociado al puerto 80. En los paquetes registrados se evidencian solicitudes y respuestas propias del servicio web, lo que permite reconocer este flujo como tráfico de navegación. Esta identificación permite considerar el puerto 80/TCP como referencia para su clasificación y tratamiento durante la etapa de calidad de servicio.

Figura 26

Identificación del tráfico HTTP mediante Wireshark



Nota: *Captura del tráfico generado durante el acceso al servicio web. Se identifica el protocolo HTTP sobre TCP, asociado al puerto 80.*
Fuente: Autoría propia

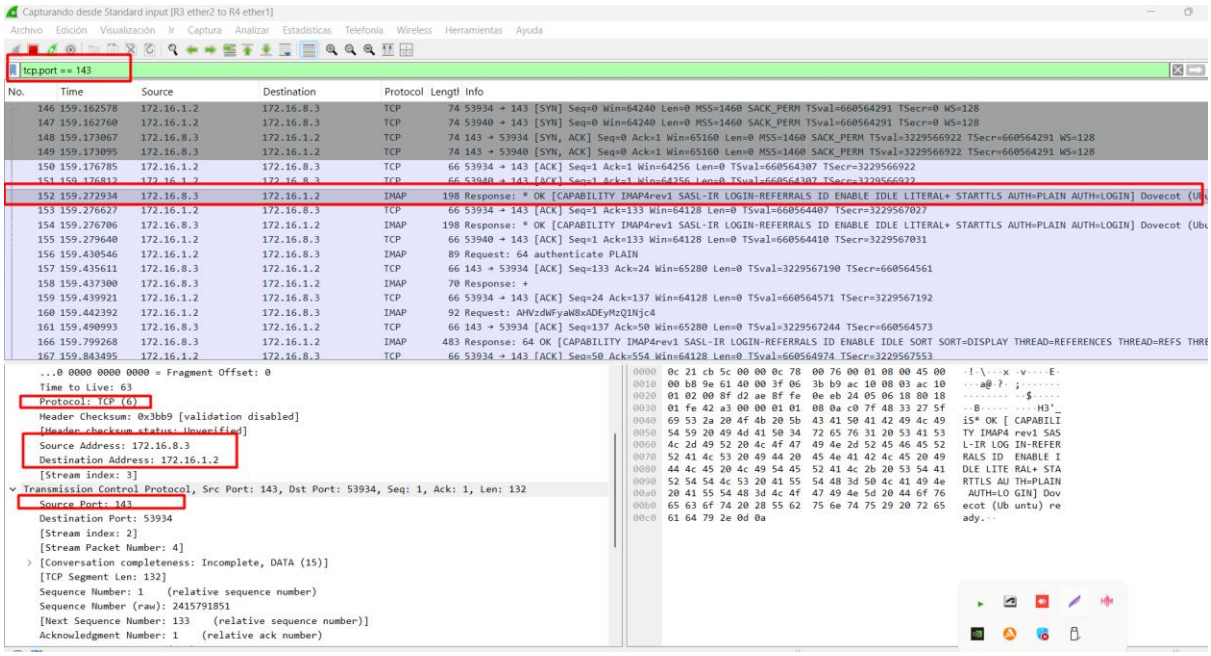
- **Correo electrónico**

Para identificar el tráfico del servicio de correo electrónico se capturó la comunicación generada durante la recepción de mensajes desde el servidor hacia el cliente, filtrando los paquetes con `tcp.port == 143`.

Como se observa en la **Figura 27**, la captura permite identificar tráfico IMAP transportado sobre TCP y asociado al puerto 143. Este protocolo permite la autenticación del usuario y la consulta de mensajes almacenados en el servidor de correo. Esta identificación permite considerar el puerto 143/TCP como referencia para la clasificación y tratamiento del tráfico de correo electrónico durante la etapa de calidad de servicio.

Figura 27

Identificación del tráfico IMAP mediante Wireshark



Nota: *Captura del tráfico generado durante el acceso al servicio de correo electrónico. Se identifica el protocolo IMAP sobre TCP, asociado al puerto 143.*
Fuente: Autoría propia.

Como resultado de la auditoría de red se identificaron los servicios considerados en la política QoS: voz RTP, señalización SIP, streaming en tiempo real, VoD, MySQL, HTTP, FTP, SSH e IMAP. Adicionalmente, iPerf3 se incorporó como tráfico artificial de fondo para generar congestión y el tráfico no identificado se mantuvo como clase por defecto.

La identificación de estos servicios se realizó a partir de capturas de tráfico obtenidas mediante Wireshark, donde se verificaron los protocolos y puertos asociados a cada aplicación. Las capturas utilizadas como evidencia se incluyen en los anexos, ya que cumplen una función documental dentro del proceso de auditoría.

3.7.2 Clasificación de paquetes

La clasificación de paquetes responde a los requerimientos RQ-FUN-02 y RQ-FUN-03, debido a que permite organizar el tráfico según el protocolo y puerto utilizado por cada servicio, además de diferenciar los flujos sensibles al retardo frente al tráfico de menor

prioridad. Esta agrupación de servicios afines según su naturaleza da cumplimiento al RQ-FUN-04 y define las clases sobre las que opera el tratamiento diferenciado (RQ-QoS-02).

A partir de la auditoría de tráfico desarrollada en el apartado 3.3.1, en la que se identificaron los protocolos, los mecanismos de transporte y los puertos asociados a cada servicio, se procedió a clasificar los paquetes según la aplicación que los origina. Mientras que la auditoría tuvo por objeto reconocer qué tráfico circula por la red, la clasificación constituye la etapa que organiza dicho tráfico en categorías bien definidas, estableciendo así la base sobre la cual se asignarán posteriormente las prioridades y las marcas de calidad de servicio.

La clasificación se realizó tomando como criterio el protocolo de transporte utilizado TCP o UDP y los puertos asociados a cada flujo, parámetros observables directamente en las capturas de Wireshark y suficientes para distinguir de manera inequívoca cada servicio implementado. A cada aplicación se añade, además, una indicación de la naturaleza de su tráfico (tiempo real, multimedia, transaccional, elástico o de administración), que anticipa los requerimientos técnicos considerados en la priorización. La **Tabla 33** consolida esta clasificación.

Tabla 33

Clasificación de tráfico de red basado en protocolos y puertos

Aplicación	Protocolo	Puertos	Naturaleza	Observación
Telefonía IP (SIP)	UDP / TCP	5060	Tiempo real	Señalización; UDP se identifica en ambos sentidos y TCP por destino.
Telefonía IP (RTP)	UDP	10000-20000	Tiempo real	Transporte de audio; se identifican puertos de origen y destino.
Streaming en tiempo real	UDP / TCP	8000-8001 / 8554	Multimedia	RTP/RTCP por UDP y RTSP por TCP; ambos se asocian a rtp-conn.
Streaming almacenado (VoD)	TCP	8080	Multimedia	Acceso y reproducción mediante Streama.

Aplicación	Protocolo	Puertos	Naturaleza	Observación
Base de datos (MySQL)	TCP	3306	Transaccional	Consultas y acceso a base de datos.
Navegación web (HTTP)	TCP	80	Elástico	Acceso a páginas web.
FTP / SSH / IMAP	TCP	21, 20 (origen FTP), 22, 143	Datos / administración	Servicios de baja prioridad agrupados en baja-conn.
iPerf3	TCP / UDP	5201	Tráfico de fondo	Generador de carga; se clasifica de forma independiente como iperf-conn.
Tráfico no clasificado	IP	Cualquier otro	Por defecto	Recibe DSCP 0 y packet-mark default-pkt.

Nota: *La clasificación se realizó a partir del análisis de los paquetes capturados en Wireshark, considerando la aplicación, el protocolo de transporte y los puertos identificados durante la auditoría de red.*
Fuente: Autoría propia

Esta clasificación cumple una función doble dentro del diseño. Por una parte, los protocolos y puertos aquí organizados se traducirán directamente en las reglas de coincidencia del marcaje; por otra, la naturaleza de cada tráfico fundamenta la jerarquía de prioridades que se establece a continuación, pues son precisamente los servicios de tiempo real los que requerirán un trato preferente ante la congestión.

3.7.3 Priorización

La priorización del tráfico responde al requerimiento RQ-QoS-01, debido a que permite establecer qué servicios deben recibir un tratamiento preferencial dentro de la red simulada. Esta etapa es necesaria porque no todos los flujos presentan la misma sensibilidad frente al retardo, la variación del retardo, la pérdida de paquetes o la congestión.

Una vez clasificados los paquetes presentados en la **Tabla 33**, se definió la prioridad de cada servicio dentro de la red simulada. Esta etapa permite determinar qué tráfico debe recibir mejor tratamiento cuando existe congestión, tomando en cuenta el retardo, el jitter, la pérdida de paquetes y la necesidad de una transmisión continua.

En una red real, la prioridad del tráfico puede variar según los objetivos de cada empresa o institución; por ejemplo, una entidad educativa podría priorizar las plataformas académicas, mientras que una empresa podría dar mayor importancia a sus bases de datos o sistemas internos. En el presente caso, al tratarse de una simulación, la prioridad no se asignó conforme a una política institucional específica, sino con base en los requerimientos técnicos de cada aplicación.

Para este análisis se tomaron como referencia las recomendaciones de la Unión Internacional de Telecomunicaciones ITU-T E.800, G.114, Y.1540 e Y.1541. La recomendación E.800 aporta el marco conceptual y la definición de los términos de calidad de servicio; la G.114 justifica la prioridad de la telefonía IP, al establecer el límite de retardo de extremo a extremo admisible para la voz; la Y.1540 define los parámetros de desempeño de la transferencia de paquetes en redes IP retardo, variación del retardo y pérdida; y la Y.1541 fija los objetivos de desempeño y las clases de calidad de servicio asociadas a dichos parámetros. Bajo este criterio, los servicios en tiempo real recibieron la mayor prioridad, dado que su funcionamiento se degrada con rapidez cuando los paquetes llegan tarde, se pierden o presentan variación en el retardo, como se muestra en la **Tabla 34**.

Tabla 34

Priorización del tráfico identificado en la red simulada

Aplicación	Protocolo	Puertos	Prioridad	Observación
Telefonía IP (SIP)	UDP / TCP	5060	Crítica / priority 2	Señalización de llamadas.
Telefonía IP (RTP)	UDP	10000-20000	Crítica / priority 1	Transporte de audio durante la llamada VoIP.
Streaming en tiempo real (MediaMTX)	UDP / TCP	8000-8001 / 8554	Alta / priority 3	RTP/RTCP y RTSP del servicio en vivo.
Streaming almacenado (VoD)	TCP	8080	Alta / priority 4	Reproducción de contenido bajo demanda.
Base de datos (MySQL)	TCP	3306	Media / priority 5	Consultas y acceso a bases de datos.
Navegación web (HTTP)	TCP	80	Media / priority 6	Acceso a páginas web.

Aplicación	Protocolo	Puertos	Prioridad	Observación
FTP / SSH / IMAP	TCP	21, 20 (origen FTP), 22, 143	Baja / priority 7	Tráfico Best Effort identificado.
iPerf3	TCP / UDP	5201	Fondo / priority 8	Carga artificial; debe ceder recursos frente a las clases SERVIDORES.
Tráfico no clasificado	IP	Cualquier otro	Por defecto / priority 8	Clase default-pkt.

Nota: *La priorización se definió según los requerimientos técnicos de cada aplicación en la red simulada, con base en las recomendaciones ITU-T E.800, G.114, Y.1540 e Y.1541.*
Fuente: Autoría propia

3.7.3.1 Aplicaciones de prioridad critica

Las aplicaciones de prioridad crítica corresponden a servicios en tiempo real, sensibles al retardo, al jitter y a la pérdida de paquetes. En esta categoría se ubicó la telefonía IP, considerando los flujos SIP y RTP. El protocolo SIP permite el registro, el establecimiento y la finalización de las llamadas, mientras que RTP transporta la voz durante la comunicación. Por esta razón, ambos requieren el mayor nivel de prioridad, a fin de evitar cortes, retardos o pérdida de calidad en la llamada. La recomendación G.114, que fija en 150 ms el retardo de un solo sentido admisible para una conversación de calidad, sustenta directamente esta asignación

3.7.3.2 Aplicaciones de prioridad alta

Las aplicaciones de prioridad alta corresponden al streaming en tiempo real de MediaMTX y al streaming almacenado mediante VoD. El flujo en vivo se identifica mediante RTP/RTCP UDP 8000-8001 y RTSP TCP 8554 y recibe priority=3; VoD utiliza TCP 8080 y recibe priority=4. Ambos requieren continuidad de transmisión, pero se ubican por debajo de VoIP dentro de la jerarquía configurada.

3.7.3.3 Aplicaciones de prioridad media

Las aplicaciones de prioridad media agrupan servicios importantes, pero con mayor tolerancia al retardo. En esta categoría se ubicaron la base de datos (MySQL) y la navegación web (HTTP). Aunque un retraso puede afectar el tiempo de respuesta percibido por el usuario,

no compromete una comunicación en tiempo real, de modo que estos servicios pueden esperar sin que su funcionamiento se degrade de forma significativa.

3.7.3.4 Aplicaciones de prioridad baja

Las aplicaciones de prioridad baja comprenden FTP, IMAP y SSH, agrupadas en la marca baja-pkt y atendidas con priority=7. De forma independiente, iPerf3 se clasifica como tráfico Background con priority=8 y el tráfico no identificado recibe default-pkt, también con priority=8. Esta separación evita confundir el tráfico real de baja prioridad con la carga artificial utilizada para provocar congestión.

3.7.4 Marcaje de tráfico

El marcaje de tráfico constituye una etapa necesaria dentro del diseño de calidad de servicio, ya que permite identificar los paquetes según el tipo de aplicación o servicio al que pertenecen. Esta identificación facilita que la red pueda aplicar un tratamiento diferenciado a los flujos multimedia y de datos, especialmente cuando coexisten servicios con distintos niveles de sensibilidad frente al retardo, la variación del retardo y la pérdida de paquetes.

En este sentido, el marcaje permite relacionar la clasificación y priorización definidas previamente con las políticas de tratamiento que se aplicarán posteriormente en los routers MikroTik. Por ello, antes de establecer los valores de marcaje y su configuración en RouterOS, es necesario seleccionar el modelo de QoS que mejor se ajuste a las características del tráfico identificado en la red simulada.

3.7.4.1 Elección del modelo de QoS

Una vez definidos los requerimientos de calidad de servicio en la sección 3.3.3, se procedió a seleccionar el modelo de QoS que mejor se ajusta a las características del tráfico y a las condiciones de la red simulada. Esta selección permite establecer la arquitectura sobre la

cual se desarrollarán posteriormente los mecanismos de clasificación, marcaje y administración de congestión.

Los requerimientos RQ-QoS-01 a RQ-QoS-07, definidos previamente en la **Tabla 17**, establecen las condiciones que debe cumplir la solución para proporcionar un tratamiento diferenciado al tráfico multimedia y de datos. Entre estas condiciones se encuentran la priorización de aplicaciones sensibles al retardo, la diferenciación del tráfico, el marcaje de paquetes, la conservación de la clase de servicio y la administración de la congestión.

Para seleccionar el modelo de QoS no se establecieron nuevos requerimientos, sino que se utilizaron los requerimientos definidos previamente como referencia para comparar las alternativas disponibles. De esta manera, se mantiene una única nomenclatura de requerimientos durante el desarrollo del proyecto y se evita duplicar las condiciones establecidas en la etapa de definición de requerimientos.

Los modelos considerados para esta selección fueron Best Effort, Integrated Services (IntServ) y Differentiated Services (DiffServ). La comparación se realizó considerando la capacidad de cada modelo para responder a las necesidades de la red propuesta y su compatibilidad con el enfoque de clasificación por clases que será implementado posteriormente en MikroTik RouterOS.

Para determinar el grado de cumplimiento de cada modelo se estableció una escala de valoración cualitativa. Esta escala permite transformar el resultado de la comparación en una puntuación cuantitativa, facilitando la selección de la alternativa que presenta mayor correspondencia con los requerimientos definidos, como se muestra en la **Tabla 35**.

Tabla 35

Escala de evaluación para la selección del modelo de QoS

Valoración	Criterio aplicado	Puntaje
Cumple	El modelo satisface completamente el requisito evaluado.	2
Parcialmente	El modelo cumple el requisito, pero presenta limitaciones técnicas o de implementación.	1
No cumple	El modelo no satisface el requisito evaluado	0

Nota. *La escala permite comparar los modelos de QoS bajo un mismo criterio de evaluación.* Fuente: Autoría propia.

Con base en los requerimientos definidos en la **Tabla 17** y aplicando la escala de evaluación presentada en la **Tabla 35**, se analizaron los modelos Best Effort, IntServ y DiffServ. La evaluación permite determinar cuál de estas alternativas se ajusta mejor a las necesidades de calidad de servicio establecidas para la red simulada.

Tabla 36

Matriz de cumplimiento de los modelos de QoS

Código	Best Effort	IntServ	DiffServ
RQ-QoS-01	No cumple	Cumple	Cumple
RQ-QoS-02	No cumple	Parcialmente	Cumple
RQ-QoS-03	No cumple	Parcialmente	Cumple
RQ-QoS-04	No cumple	No cumple	Cumple
RQ-QoS-05	No cumple	Cumple	Cumple
RQ-QoS-06	No cumple	Parcialmente	Cumple
RQ-QoS-07	No cumple	Parcialmente	Cumple
Puntaje total	**0/14**	**8/14**	**14/14**

Nota. El puntaje se obtuvo aplicando la escala de evaluación definida en la **Tabla 35** Fuente: Autoría propia.

Como se observa en la **Tabla 36**, existen diferencias en el nivel de cumplimiento de los requerimientos entre los tres modelos evaluados. Best Effort obtuvo el puntaje más bajo (0/14), debido a que no proporciona mecanismos específicos para diferenciar y priorizar el tráfico de acuerdo con los requerimientos establecidos. Por esta razón, no resulta adecuado para el

escenario propuesto, en el que coexisten servicios con diferentes niveles de sensibilidad al retardo, la variación del retardo y la pérdida de paquetes.

IntServ alcanzó un puntaje de 8/14. Este modelo permite diferenciar el tráfico y establecer mecanismos de reserva de recursos por flujo; sin embargo, su funcionamiento requiere mantener información asociada a cada flujo y utilizar mecanismos de reserva como RSVP, lo que incrementa la complejidad de implementación y limita su escalabilidad cuando aumenta el número de comunicaciones simultáneas.

Por su parte, DiffServ obtuvo el mayor puntaje, con 14/14, al satisfacer los requerimientos establecidos para la solución. Su arquitectura basada en clases agregadas permite diferenciar el tráfico, utilizar mecanismos de marcaje mediante DSCP y aplicar posteriormente políticas diferenciadas de tratamiento y administración de congestión, sin requerir el mantenimiento del estado individual de cada flujo.

3.7.4.2 Elección del método de marcaje de tráfico

Una vez seleccionado el modelo DiffServ, se definió el método de marcaje que permitirá identificar los paquetes según la clase de servicio asignada, de manera que posteriormente puedan recibir un tratamiento diferenciado mediante las políticas de calidad de servicio.

El método de marcaje debe guardar coherencia con el modelo de QoS seleccionado y, además, ser aplicable dentro de la plataforma utilizada para la configuración de la red. Por ello se consideró el campo DSCP como mecanismo principal, dado que forma parte del campo de Servicios Diferenciados (DS) del encabezado IP. El estándar RFC 2474 (Nichols et al., 1998) establece que los seis bits más significativos del campo DS constituyen el DSCP, empleado para seleccionar el comportamiento por salto (PHB) que recibirá cada paquete en los nodos de la red.

Para fundamentar la elección se analizaron tres alternativas de marcaje: la Precedencia IP (IP Precedence), el DSCP y las marcas internas del router. La comparación se presenta en la **Tabla 37**.

Tabla 37

Comparación de métodos de marcaje de tráfico

Método de marcaje	Característica principal	Evaluación dentro del diseño QoS
Precedencia IP (IP Precedence)	Emplea tres bits del campo ToS para representar niveles de prioridad.	Permite una clasificación básica, pero ofrece menor granularidad que DSCP y se considera un mecanismo heredado.
DSCP	Emplea seis bits del campo DS del encabezado IP para representar clases de servicio.	Ofrece mayor cantidad de valores, se integra de forma nativa con DiffServ y se conserva extremo a extremo en la cabecera IP.
Marca interna del router	Etiqueta local que identifica los paquetes dentro del equipo.	No viaja en la cabecera IP; no sustituye al DSCP, sino que lo complementa al vincular cada paquete con su cola.

Nota. *La comparación se realizó considerando el modelo DiffServ seleccionado y la configuración posterior en la red simulada.*
Fuente: Autoría propia.

A partir de la comparación realizada, se seleccionó el DSCP como método de marcaje, debido a que ofrece mayor capacidad de clasificación que la Precedencia IP y ah que se conserva dentro del encabezado IP, lo que garantiza la coherencia del marcaje extremo a extremo en el dominio DiffServ.

No obstante, conviene precisar que el DSCP y las marcas internas del router no constituyen métodos excluyentes. En la implementación sobre el equipo MikroTik se emplean de forma complementaria: mientras el DSCP porta la semántica DiffServ en la cabecera IP y es interpretado por todos los nodos de la red, las marcas internas de conexión (`connection-mark`) y de paquete (`packet-mark`) son etiquetas locales del equipo que permiten vincular cada

flujo con la cola que le corresponde. Esta articulación entre ambos mecanismos se detalla en los apartados de asignación de valores DSCP y de configuración de marcas.

3.7.4.3 Definición de las clases del servicio

Seleccionados el modelo DiffServ y el método de marcaje, el siguiente paso consiste en definir las clases de servicio sobre las cuales operará la política de calidad. A diferencia del modelo IntServ, que administra el tráfico flujo por flujo, DiffServ agrupa los paquetes en un número reducido de clases denominadas agregados de comportamiento que comparten requerimientos similares y reciben, cada una, un mismo tratamiento. Esta agregación es precisamente la característica que otorga a DiffServ su escalabilidad, pues permite administrar la red por clases y no por el estado individual de cada comunicación (Blake et al., 1998).

La política de QoS distingue nueve categorías operativas: VoIP RTP, SIP, Streaming RTP/RTCP-RTSP, VoD, MySQL, HTTP, Best Effort, iPerf Background y tráfico Default. Cada categoría conserva su propia marca interna y, cuando corresponde, un valor DSCP específico. La **Tabla 38** resume esta correspondencia.

Tabla 38

Definición de las clases de servicio para la política de QoS

Clase de servicio	Aplicaciones que agrupa (protocolo/puerto)	Prioridad
VoIP RTP	RTP/UDP 10000-20000	1
SIP	UDP/TCP 5060	2
Streaming en tiempo real	RTP/RTCP UDP 8000-8001 y RTSP TCP 8554	3
Streaming VoD	Streama TCP 8080	4
Base de datos	MySQL TCP 3306	5
Web	HTTP TCP 80	6
Best Effort	FTP TCP 21, SSH 22 e IMAP 143	7
iPerf Background	TCP/UDP 5201	8
Default	Tráfico no clasificado	8

Nota. *Las categorías se definieron según las marcas implementadas en RouterOS. iPerf3 y el tráfico por defecto se gestionan de forma independiente de Best Effort.*
Fuente: Autoría propia

A continuación, se detalla el tratamiento asignado a cada clase de servicio.

- **Clase VoIP.** Agrupa el tráfico de telefonía IP en tiempo real, esto es, la señalización SIP y el transporte de voz RTP. Es la clase más sensible al retardo, a la variación del retardo y a la pérdida de paquetes, por lo que requiere el tratamiento de mayor prioridad para evitar cortes o degradación en la llamada.
- **Clase Streaming**. El streaming en tiempo real de MediaMTX agrupa RTP/RTCP sobre UDP 8000-8001 y RTSP sobre TCP 8554 bajo rtp-conn/rtp-pkt y DSCP AF41 (34). El streaming almacenado o VoD utiliza TCP 8080, vod-conn/vod-pkt y DSCP AF43 (38). En Queue Tree reciben priorities 3 y 4, respectivamente.
- **Clase Base de datos.** Comprende el tráfico transaccional de MySQL. Aunque tolera mayor retardo que la voz o el video, es sensible a la pérdida de paquetes, por lo que recibe un tratamiento preferencial con respecto a la navegación común dentro de la prioridad media.
- **Clase Web.** Agrupa la navegación HTTP. Representa un tipo de tráfico elástico que se adapta a las condiciones de la red sin comprometer una comunicación en tiempo real; se ubica en la prioridad media, un nivel por debajo de la base de datos.
- **Clase Best Effort.** Agrupa únicamente los servicios identificados de baja prioridad: FTP, IMAP y SSH. Estos flujos reciben baja-conn, baja-pkt y DSCP 0, y se atienden con priority=7 dentro de SERVIDORES. El tráfico iPerf3 y el tráfico no clasificado se mantienen en clases independientes con priority=8.

Además de las clases de servicio, la configuración separa explícitamente el tráfico de saturación iPerf3 mediante iperf-conn/iperf-pkt y DSCP CS1 (8), mientras que los paquetes que no coinciden con ninguna regla reciben DSCP 0 y default-pkt. Esta separación permite observar con claridad qué tráfico debe ceder recursos durante la congestión.

3.7.4.4 Asignación de valores DSCP

Definidas las clases de servicio, se procede a asignar a cada una un valor DSCP. Este valor permite identificar el tipo de tráfico dentro de la red y sirve para que los equipos apliquen un tratamiento diferente según la prioridad del paquete.

El DSCP forma parte del campo de Servicios Diferenciados del encabezado IP. De acuerdo con la RFC 2474, este campo utiliza seis bits para seleccionar el comportamiento por salto o PHB que recibirá un paquete en cada nodo de la red. Por esta razón, el número de valores posibles se obtiene mediante la Ecuación 1.

Ecuación 1.
Número de valores DSCP posibles

$$N = 2^n$$

Donde n representa el número de bits del campo DSCP. Al remplazar:

$$N = 2^6 = 64$$

Por tanto, DSCP permite representar 64 valores posibles, desde 0 hasta 63. Estos valores no se asignan de forma arbitraria, sino de acuerdo con el tipo de comportamiento que requiere cada clase de tráfico.

Para este diseño se consideran tres comportamientos principales. El primero es el Reenvío Expedito o EF, definido en la RFC 3246, utilizado para tráfico de tiempo real que requiere bajo retardo, baja variación del retardo y baja pérdida de paquetes. El segundo es el Reenvío Asegurado o AF, definido en la RFC 2597, que permite organizar el tráfico en clases y niveles de descarte. Finalmente, se considera Best Effort, asociado al tráfico que no requiere garantías específicas.

En el caso de las clases AF, la notación se expresa como AFxy. El valor x representa la clase de servicio y el valor y representa la precedencia de descarte. Su valor decimal se calcula mediante la Ecuación 2.

Ecuación 2.
Cálculo del valor DSCP para clases AF

$$DSCP(AFxy) = 8x + 2y$$

Para los selectores de clase, conocidos como CS, el valor decimal se obtiene mediante la Ecuación 3.

Ecuación 3.
Cálculo del valor DSCP para selectores de clase

$$DSCP(CSx) = 8x$$

La asignación también considera la RFC 4594, que presenta recomendaciones para la construcción de clases de servicio DiffServ, y la Recomendación ITU-T Y.1541, que define clases de calidad de servicio para redes IP. Con base en estas referencias y en la priorización definida previamente, la **Tabla 39** presenta los valores DSCP asignados.

Tabla 39

Asignación de valores DSCP

Clase de servicio	Flujo / servicio	PHB	Binario	Decimal	Referencia
VoIP	Voz RTP	EF	101110	46	RFC 3246; RFC 4594
VoIP	Señalización SIP	CS3	011000	24	RFC 2474; RFC 4594
Streaming	MediaMTX RTP/RTCP-RTSP	AF41	100010	34	RFC 2597; RFC 4594
Streaming	Almacenado VoD	AF43	100110	38	RFC 2597; RFC 4594
Base de datos	MySQL	AF31	011010	26	RFC 2597; RFC 4594
Web	HTTP	AF21	010010	18	RFC 2597; RFC 4594
Best Effort	FTP / SSH / IMAP	CS0	000000	0	RFC 2474; RFC 4594
Background	iPerf3	CS1	001000	8	Política QoS implementada
Default	Tráfico no clasificado	CS0	000000	0	Política QoS implementada

Nota. *Elaboración propia basada en la RFC 2474, RFC 2597, RFC 3246, RFC 4594 y la Recomendación ITU-T Y.1541.*
Fuente: Autoría propia.

La asignación de los valores DSCP se realizó considerando el comportamiento de cada servicio frente al retardo, el jitter, la pérdida de paquetes y la congestión. En este sentido, el tráfico de voz RTP se marcó con EF 46, debido a que es el servicio más sensible dentro de la red. Durante una llamada, cualquier aumento de retardo o pérdida de paquetes puede afectar directamente la calidad de la comunicación.

La señalización SIP se asignó a CS3 24, ya que participa en el establecimiento, mantenimiento y finalización de las llamadas. Aunque este tráfico no transporta el audio, es necesario para que el servicio de telefonía IP funcione correctamente, por lo que requiere un tratamiento preferente.

Para el tráfico de streaming se empleó la clase AF4. El streaming en vivo mediante RTP se marcó como AF41 34, porque necesita mayor continuidad durante la transmisión. En cambio, el streaming almacenado o VoD se asignó a AF43 38, debido a que puede tolerar mejor ciertas variaciones de la red por el uso de almacenamiento temporal en el reproductor. Esta diferencia permite proteger con mayor prioridad al contenido en vivo frente al contenido almacenado.

El tráfico de base de datos MySQL se marcó como AF31 26, al tratarse de un servicio transaccional que requiere estabilidad durante las consultas. Por otro lado, la navegación HTTP se asignó a AF21 18, ya que corresponde a un servicio de prioridad media con mayor tolerancia al retardo.

Los servicios FTP, IMAP y SSH se mantienen con DSCP 0 (CS0) y constituyen la clase Best Effort identificada. iPerf3 se marca de manera independiente con DSCP 8 (CS1), ya que funciona como tráfico Background durante las pruebas. Todo paquete que no coincida con una conexión previamente marcada recibe DSCP 0 y posteriormente default-pkt.

3.7.4.5 Delimitación de la frontera de confianza

La frontera de confianza corresponde al punto lógico de la red a partir del cual los valores de calidad de servicio se consideran válidos para el tratamiento del tráfico. Su delimitación es fundamental, ya que no se debe confiar directamente en el marcaje generado por los dispositivos finales, como clientes o servidores. Estos equipos podrían enviar paquetes sin marca DSCP, con una marca incorrecta o con un valor de prioridad que no corresponde al servicio real, con el fin de obtener ventajas injustas en el consumo del ancho de banda.

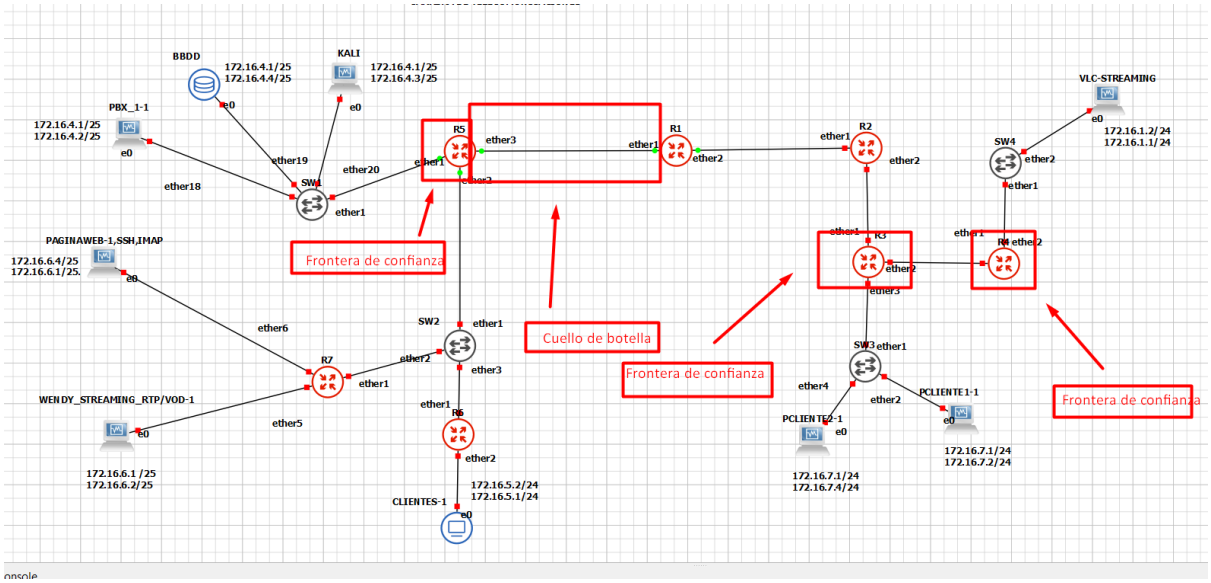
En el presente diseño, la frontera de confianza se ubica en los routers de acceso de Capa 3, debido a que son los primeros equipos administrados que reciben y procesan el tráfico IP proveniente de los segmentos de usuarios y servidores. En estos puntos se verifica el tráfico que ingresa a la red y se realiza su clasificación y marcaje mediante valores DSCP de acuerdo con el servicio identificado. De esta manera, la prioridad de los paquetes no depende de los dispositivos finales, sino de las políticas definidas dentro de la infraestructura QoS.

La **Figura 28** muestra la ubicación de la frontera de confianza dentro de la topología implementada. En ella se observa que los routers R3, R4 y R5 se encuentran conectados directamente con los segmentos de clientes o servidores a través de switches de Capa 2, por lo que actúan como puntos de acceso al dominio QoS. En estos equipos se lleva a cabo la clasificación inicial del tráfico, el marcaje de conexiones, la asignación de valores DSCP y el marcaje de paquetes.

R1 y R2 conservan su función de encaminamiento dentro de la topología. La clasificación, el marcado de conexiones, la escritura del campo DSCP y la generación de packet-mark se realizan en R3, R4 y R5. En R5, además, se aplica Queue Tree sobre ether5 para administrar la congestión en el sentido de tráfico evaluado.

Figura 28

Delimitación de la frontera de confianza en la topología QoS



Nota. *La figura identifica los routers de acceso donde inicia la frontera de confianza y los routers de núcleo encargados del tránsito interno.*
Fuente: Autoría propia

La clasificación de los routers según su función dentro de la frontera de confianza se presenta en la **Tabla 40**.

Tabla 40

Clasificación de routers según su función dentro de la arquitectura QoS

Router	Función dentro de QoS	Interfaz / alcance
R3	Clasificación y marcaje Mangle	Routers de acceso; aplica connection-mark, DSCP y packet-mark.
R4	Clasificación y marcaje Mangle	Routers de acceso; aplica connection-mark, DSCP y packet-mark.
R5	Clasificación, marcaje y administración de congestión	Queue Tree aplicado sobre ether5.
R6	Switch local de Capa 2	Tránsito de Capa 2; no aplica política Mangle de Capa 3.
R7	Switch local de Capa 2	Tránsito de Capa 2; no aplica política Mangle de Capa 3.
R1	Encaminamiento / tránsito	No se incorporan reglas QoS adicionales
R2	Encaminamiento / tránsito	No se incorporan reglas QoS adicionales

***Nota**. El proceso de clasificación y marcaje se realiza en R3, R4 y R5. En R5, Queue Tree se asocia a ether5 con max-limit=900k. R1 y R2 se mantienen como equipos de tránsito y conservan el valor DSCP durante el encaminamiento.*
Fuente: Autoría propia.

Como se observa en la **Figura 28** y se detalla en la **Tabla 40**, la frontera de confianza se establece en los routers R3, R4 y R5. Estos equipos representan los puntos de entrada del tráfico hacia la red administrada. Por esta razón, en ellos se realiza la clasificación de los flujos según el servicio identificado, el marcaje de conexiones, la asignación de valores DSCP y el marcaje de paquetes que serán utilizados posteriormente para la aplicación de las políticas de calidad de servicio.

R1 y R2 conservan su función de encaminamiento dentro de la topología. De acuerdo con la configuración implementada, en estos equipos no se crean packet-mark a partir del DSCP ni se configura el árbol de colas. Por esta razón, la validación en estos nodos se limita a comprobar el tránsito de los paquetes y la conservación del campo DSCP, sin atribuirles funciones adicionales de marcaje o planificación del tráfico.

La separación funcional queda establecida de la siguiente manera: R3, R4 y R5 identifican, clasifican y marcan los flujos mediante reglas Mangle; adicionalmente, R5 aplica Queue Tree sobre la interfaz ether5 para administrar la congestión y establecer el tratamiento diferenciado de las clases de tráfico. Por su parte, R1 y R2 realizan el encaminamiento de los paquetes y permiten comprobar la conservación del valor DSCP durante su tránsito por la red.

3.7.4.6 Diseño del esquema de marcas de RouterOS

El diseño del esquema de marcaje responde a los requerimientos RQ-QoS-03 y RQ-QoS-04, los cuales establecen que la solución debe identificar la clase de servicio de cada flujo y conservar dicha identificación durante el recorrido del paquete a través del dominio QoS.

Para satisfacer estos requerimientos, se plantea un esquema basado en la combinación de marcas internas de RouterOS y del campo DSCP de la cabecera IP.

El propósito del esquema de marcaje es asociar cada flujo de tráfico con la clase de servicio que le corresponde, de manera que los mecanismos de planificación y administración de congestión puedan aplicar el tratamiento diferenciado definido por la política de Calidad de Servicio (QoS).

Dentro del diseño, las marcas internas de RouterOS permiten identificar el tráfico para su procesamiento local dentro de cada router. Sin embargo, estas marcas no forman parte de la cabecera IP y, por tanto, no son visibles para otros dispositivos de la red. Para mantener la clasificación durante el tránsito de los paquetes, el diseño incorpora el uso del campo DSCP, el cual permanece en la cabecera IP y puede ser interpretado por los routers pertenecientes al dominio QoS.

Con base en este criterio, el esquema de marcaje se estructura en tres fases secuenciales. La primera permite identificar el flujo de tráfico y asociarlo con una clase de servicio. La segunda conserva dicha clasificación mediante el valor DSCP en la cabecera IP, mientras que la tercera vincula el tráfico con los mecanismos de planificación que aplicarán el tratamiento correspondiente dentro del router.

- **Fase 1. Identificación y marcado de conexión**

Mediante la acción mark-connection, el router identifica cada flujo de tráfico de acuerdo con el protocolo y los puertos utilizados por el servicio correspondiente. La evaluación se realiza únicamente sobre el primer paquete de la conexión (connection-state=new), reduciendo el procesamiento requerido para los paquetes siguientes. Como resultado, la conexión queda asociada a una marca que identifica la clase de servicio a la que pertenece.

- **Fase 2. Modificación del campo DSCP**

En la segunda fase, la acción change-dscp utiliza la marca de conexión previamente asignada para escribir el valor DSCP correspondiente en la cabecera IP. A diferencia de las marcas internas de RouterOS, este valor permanece en el paquete durante su tránsito por la red, permitiendo que los routers pertenecientes al dominio QoS identifiquen la clase de servicio sin necesidad de repetir el proceso de clasificación.

- **Fase 3. Marcado de paquete local**

Finalmente, mediante la acción mark-packet, el router asigna una marca interna a cada paquete perteneciente a una conexión previamente identificada. Esta marca es utilizada posteriormente por Queue Tree para asociar el tráfico con la cola correspondiente y aplicar las políticas de planificación definidas para cada clase de servicio

La **Tabla 41** resume las fases que conforman el esquema de marcaje diseñado, indicando la acción de Mangle empleada, su función dentro de la política de Calidad de Servicio y el resultado esperado en cada etapa del proceso.

Tabla 41

Fases del proceso de marcas en RouterOS

Fase	Acción en Mangle	Función dentro de la política de QoS	Resultado esperado
Fase 1	mark-connection	Identifica la conexión o flujo según el servicio detectado.	La conexión queda asociada a una clase de tráfico.
Fase 2	change-dscp	Modifica el valor DSCP en el encabezado IP	El paquete conserva su prioridad (PHB) al viajar por el dominio QoS.
Fase 3	mark-packet	Marca los paquetes pertenecientes a una conexión previamente identificada.	Los paquetes quedan vinculados con una cola específica en Queue Tree.

Nota. *Las fases 1 y 3 generan marcas internas utilizadas por RouterOS localmente. La fase 2 modifica la cabecera IP física del paquete.*
Fuente: Autoría propia.

Una vez definido el esquema de marcaje, se establece la correspondencia entre cada servicio, las marcas internas previstas y el valor DSCP asignado. Esta relación constituye la base para la identificación y diferenciación del tráfico dentro de la red y se resume en la **Tabla 42**.

Tabla 42

Compilación de marcas de conexión, paquete y DSCP por servicio

Servicio	connection-mark	packet-mark	Protocolo / puerto	DSCP
VoIP, voz RTP	voz-conn	voz-pkt	UDP src/dst 10000-20000	46
VoIP, señalización SIP	sip-conn	sip-pkt	UDP src/dst 5060; TCP dst 5060	24
Streaming en tiempo real	rtp-conn	rtp-pkt	UDP src/dst 8000-8001; TCP dst 8554	34
Streaming almacenado VoD	vod-conn	vod-pkt	TCP dst 8080	38
Base de datos MySQL	bdd-conn	bdd-pkt	TCP dst 3306	26
Navegación web HTTP	web-conn	web-pkt	TCP dst 80	18
FTP / IMAP / SSH	baja-conn	baja-pkt	TCP dst 21,22,143; FTP src 20	0
iPerf	iperf-conn	iperf-pkt	TCP dst 5201; UDP src/dst 5201	8
Background				
Tráfico no clasificado	Sin marca específica	default-pkt	Cualquier otro tráfico	0

Nota. *La tabla consolida la relación entre el servicio identificado, las marcas internas de RouterOS y el valor DSCP asignado para conservar la clase de servicio en el encabezado IP*
Fuente: Autoría propia.

- **Diseño del procesamiento del tráfico en los routers de acceso y en R5**

El diseño final establece que R3, R4 y R5 realicen la clasificación por protocolo y puerto. En estos routers se ejecutan las tres fases de Mangle: mark-connection, change-dscp y

mark-packet. Las reglas incluyen explícitamente el tráfico de VoIP, SIP, MediaMTX, VoD, MySQL, HTTP, FTP/SSH/IMAP, iPerf3 y el tráfico por defecto.

La administración de congestión se concentra en R5. Las packet-mark generadas localmente se utilizan para vincular cada flujo con Queue Tree sobre ether5. En consecuencia, la política no depende de crear nuevas marcas locales en R1 o R2 para que el árbol de colas funcione.

El campo DSCP permanece como identificador DiffServ durante el tránsito IP y permite verificar que la clasificación realizada en los routers de acceso se conserva a lo largo de la red. Las marcas connection-mark y packet-mark son locales al router donde se generan y no se propagan en la cabecera IP entre los equipos.

3.7.5 Administración de la congestión

La administración de la congestión constituye una etapa complementaria al proceso de clasificación y marcaje del tráfico. Mientras la clasificación permite reconocer los servicios presentes en la red y el marcaje permite identificar los paquetes según la clase a la que pertenecen, la administración de la congestión determina el tratamiento que recibirá cada clase cuando la capacidad del enlace no sea suficiente para atender simultáneamente todo el tráfico.

De acuerdo con los requerimientos de calidad de servicio definidos en el apartado 3.3.3, esta etapa debe permitir priorizar los servicios sensibles al retardo, administrar el tráfico mediante mecanismos de colas, establecer garantías mínimas de ancho de banda y definir límites máximos para las diferentes clases de servicio.

Por esta razón, una vez definidos los valores DSCP y las marcas internas utilizadas para identificar las clases de tráfico, es necesario seleccionar un mecanismo de colas que permita llevar estos requerimientos a la implementación sobre MikroTik RouterOS. El mecanismo

seleccionado debe permitir organizar el tráfico durante condiciones de congestión, priorizar los servicios sensibles al retardo, establecer garantías mínimas de ancho de banda y controlar los límites máximos de utilización para las diferentes clases de tráfico.

3.7.5.1 Elección del método de la administración de congestión

Una vez seleccionado el modelo DiffServ y definido el DSCP como método de marcaje, se procedió a seleccionar el mecanismo de administración de congestión que será utilizado en la red simulada.

Para esta selección se tomaron como referencia los requerimientos RQ-QoS-01, RQ-QoS-05, RQ-QoS-06 y RQ-QoS-07, definidos previamente en la sección 3.3.3. Estos requerimientos se relacionan con la priorización del tráfico, la administración de la congestión mediante colas y el establecimiento de garantías y límites de ancho de banda.

En MikroTik RouterOS se consideraron Simple Queue y Queue Tree como alternativas para implementar la administración de congestión. La evaluación se realizó utilizando los requerimientos previamente definidos, sin establecer nuevos requerimientos, manteniendo así la misma nomenclatura empleada durante el diseño de QoS.

Para determinar el grado de cumplimiento de cada alternativa se utilizó la escala de valoración presentada en la **Tabla 43**.

Tabla 43

Escala de evaluación para la selección del método de administración de la congestión

Valoración	Criterio aplicado	Puntaje
Cumple	El mecanismo satisface completamente el requisito evaluado.	2
Parcialmente	El mecanismo satisface el requisito, pero presenta	1

	limitaciones para el escenario planteado	
No cumple	El mecanismo no satisface el requisito evaluado.	0

Nota. *La escala permite comparar los mecanismos de administración de congestión bajo un mismo criterio de evaluación.*
Fuente: Autoría propia

A partir de esta escala se realizó la comparación de ambas alternativas, cuyos resultados se presentan en la **Tabla 44**.

Tabla 44

Matriz de cumplimiento de los mecanismos de administración de congestión

Código	Simple Queue	Queue Tree
RQ-QoS-01	Parcialmente	Cumple
RQ-QoS-05	Cumple	Cumple
RQ-QoS-06	Parcialmente	Cumple
RQ-QoS-07	Cumple	Cumple
Puntaje Total	6/8	8/8

Nota. El puntaje se obtuvo aplicando la escala de evaluación definida en la **Tabla 43**.
Fuente: Autoría propia.

Como se observa en la **Tabla 44**, Simple Queue obtuvo un puntaje de 6/8, mientras que Queue Tree alcanzó 8/8. En el caso del RQ-QoS-01, relacionado con la priorización de aplicaciones sensibles al retardo, Simple Queue permite establecer prioridades; sin embargo, presenta mayores limitaciones para estructurar el tratamiento diferenciado de las distintas clases de servicio consideradas en el diseño QoS. Por su parte, Queue Tree permite organizar las colas de acuerdo con las clases de tráfico y asignar diferentes niveles de prioridad, por lo que presenta una mayor correspondencia con este requerimiento.

Respecto al RQ-QoS-06, relacionado con la definición de tasas mínimas o garantías de ancho de banda por clase de servicio, Simple Queue permite establecer parámetros de control de ancho de banda, pero su estructura resulta menos adecuada para distribuir garantías entre diferentes clases organizadas jerárquicamente. Queue Tree, mediante una estructura de colas

jerárquica, permite establecer garantías de ancho de banda para las distintas clases de tráfico, por lo que cumple con este requerimiento dentro del escenario planteado.

Ambos mecanismos cumplen con el RQ-QoS-05, debido a que permiten administrar el tráfico mediante mecanismos de colas cuando se presenta congestión. Asimismo, ambos cumplen con el RQ-QoS-07, ya que permiten establecer límites máximos de utilización del ancho de banda. No obstante, Queue Tree presenta una mayor correspondencia con el esquema de QoS propuesto, debido a que facilita la organización de las clases de tráfico y la aplicación diferenciada de políticas de prioridad, garantía y limitación de ancho de banda.

Se selecciona Queue Tree como mecanismo de administración de congestión para la red simulada, al obtener el mayor nivel de cumplimiento respecto de los requerimientos de calidad de servicio considerados. Esta selección permitirá continuar con la configuración de las colas y la asignación de las políticas de prioridad, garantía y límite de ancho de banda correspondientes a cada clase de tráfico.

3.7.5.2 Teoría de Colas

Queue Tree utiliza una estructura jerárquica de colas basada en Hierarchical Token Bucket (HTB), mediante la cual se establecen relaciones entre diferentes niveles de colas para administrar el ancho de banda. Esta estructura puede organizarse mediante una cola padre asociada al recurso que se desea controlar y diferentes colas hijas correspondientes a las clases de servicio definidas en la política QoS. En RouterOS, Queue Tree está orientado a tareas avanzadas de administración de tráfico y permite utilizar marcas de paquete generadas mediante Mangle para dirigir los paquetes hacia las colas correspondientes.

La estructura jerárquica permite distribuir el ancho de banda de acuerdo con las condiciones establecidas para cada clase. La cola padre establece el recurso global que será

administrado, mientras que las colas hijas permiten definir parámetros particulares de tratamiento para cada clase de tráfico. De esta manera, es posible establecer diferentes niveles de prioridad, tasas mínimas y límites máximos sin tratar todo el tráfico como un único conjunto.

En el diseño propuesto, estos principios permiten establecer diferentes condiciones para las clases de tráfico. Las clases asociadas a servicios sensibles al retardo pueden configurarse con mayor prioridad y una tasa mínima garantizada, mientras que las clases de menor prioridad pueden aprovechar la capacidad disponible, siempre dentro de los límites establecidos. Los principales elementos empleados en esta estructura se presentan en la **Tabla 45**.

Tabla 45

Elementos principales de la administración de colas mediante Queue Tree

Elemento	Descripción	Función dentro de la política QoS
Cola padre	Cola principal del árbol	Representa la capacidad total del enlace o interfaz.
Cola hija	Cola asociada a una clase de servicio.	Permite tratar de forma independiente cada tipo de tráfico.
packet-mark	Marca de paquete generada mediante Mangle.	Vincula el tráfico clasificado con una cola específica.
priority	Nivel de prioridad de la cola.	Define qué clase accede primero al ancho de banda sobrante.
limit-at	Tasa mínima garantizada.	Asegura capacidad mínima durante congestión.
max-limit	Tasa máxima permitida.	Define el límite superior que puede alcanzar una clase.
Disciplina de cola	Forma de atender los paquetes dentro de una cola.	Determina si los paquetes se atienden en orden simple o con reparto equitativo.

Nota. *Los elementos indicados permiten relacionar el marcaje del tráfico con el tratamiento que recibirá cada clase dentro del árbol de colas.*
Fuente: Autoría propia.

El parámetro priority se expresa en RouterOS con valores del 1 al 8, donde 1 representa la prioridad más alta y 8 la más baja. Este parámetro define el orden en que las clases pueden aprovechar el ancho de banda excedente una vez atendidas sus garantías mínimas. Por esta

razón, los servicios sensibles al retardo, como voz RTP y señalización SIP, pueden ubicarse en niveles de prioridad superiores.

Los parámetros limit-at y max-limit permiten establecer, respectivamente, la tasa mínima garantizada y el límite máximo de utilización de ancho de banda para cada clase. De esta manera, se establecen las condiciones de capacidad que deben considerar las colas durante la administración del tráfico.

Además de la prioridad y las tasas, cada cola puede utilizar una disciplina de atención que define cómo se gestionan los paquetes que esperan ser transmitidos. Para el tráfico sensible al retardo se considera una disciplina tipo pfifo, debido a que atiende los paquetes en orden de llegada y mantiene una lógica simple de atención. Para las clases que pueden agrupar varios flujos simultáneos se considera PCQ, ya que permite distribuir el ancho de banda entre las conexiones y evita que un único flujo monopolice la capacidad asignada a la clase. En la **Tabla 46** se presenta la correspondencia teórica entre clases de tráfico y disciplina de cola.

Tabla 46

Correspondencia teórica entre clases de tráfico y disciplina de cola

Clase	Prioridad de tráfico	Marca de paquete	Disciplina de cola
VoIP - RTP	1	voz-pkt	REALTIME-pfifo
VoIP - SIP	2	sip-pkt	REALTIME-pfifo
Streaming en tiempo real	3	rtp-pkt	RTP-pfifo
Streaming VoD	4	vod-pkt	QoS-pcq
Base de datos MySQL	5	bdd-pkt	QoS-pcq
Navegación web HTTP	6	web-pkt	QoS-pcq
FTP / IMAP / SSH	7	baja-pkt	QoS-pcq
iPerf Background	8	iperf-pkt	QoS-pcq

Clase	Prioridad de tráfico	Marca de paquete	Disciplina de cola
Tráfico no clasificado	8	default-pkt	QoS-pcq

Nota. *La disciplina de cola se define según la sensibilidad de cada clase frente al retardo y la cantidad de flujos simultáneos que puede agrupar.*
Fuente: Autoría propia.

Se utilizaron dos colas PFIFO: REALTIME-pfifo para VoIP RTP y SIP, y RTP-pfifo para el streaming en tiempo real. VoD, MySQL, HTTP, Best Effort, iPerf Background y Default utilizan QoS-pcq. Esta asignación permite aplicar una disciplina de encolamiento acorde con las características de cada clase de tráfico.

Queue Tree permite implementar una jerarquía de prioridades y límites en RouterOS, pero no debe describirse como una implementación idéntica a LLQ, CBWFQ u otros mecanismos de fabricantes diferentes. En esta tesis la comparación con otras plataformas se mantiene únicamente como referencia funcional; la evidencia experimental corresponde exclusivamente a la política configurada en MikroTik RouterOS.

3.7.5.3 Dimensionamiento de parámetros QoS para Queue Tree

El enlace utilizado como referencia experimental opera con una capacidad de 1 Mbit/s. Para la administración de la congestión, la cola principal QoS-Total se estableció en 900 kbit/s y se asoció a ether5 de R5. Dentro de esta jerarquía se creó la clase agregada SERVIDORES con priority=1, limit-at=700k y max-limit=900k. La reserva de 700 kbit/s corresponde al conjunto de servicios agrupados bajo SERVIDORES y no a cada cola de forma individual.

Dentro de QoS-Total se creó la clase agregada SERVIDORES con priority=1, limit-at=700k y max-limit=900k. Esta reserva de 700 kbit/s se aplica al conjunto de servicios ubicados bajo SERVIDORES, no individualmente a cada servicio.

Las colas VoIP RTP, SIP, Streaming RTP, VoD, MySQL, HTTP y Best Effort son hijas de SERVIDORES. Todas utilizan limit-at=0 y max-limit=900k; su diferenciación se realiza mediante priority y el tipo de cola. iPerf Background y Default son hijos directos de QoS-Total y utilizan priority=8, de modo que quedan fuera de la reserva agregada de SERVIDORES.

Esta estructura explica el comportamiento observado durante las pruebas: los servicios clasificados bajo SERVIDORES compiten dentro de una clase agregada con reserva mínima, mientras que la carga artificial de iPerf3 se mantiene como tráfico de fondo independiente. La **Tabla 47** presenta los parámetros efectivos de la jerarquía principal de Queue Tree.

Tabla 47

Jerarquía y parámetros efectivos de Queue Tree

Elemento / cola	Ubicación y función	Parámetro configurado
QoS-Total	Cola padre en R5	parent=ether5; max-limit=900k
SERVIDORES	Hija de QoS-Total; agrupa servicios reales	priority=1; limit-at=700k; max-limit=900k
VoIP RTP	Hija de SERVIDORES	priority=1; limit-at=0; max-limit=900k; REALTIME-pfifo
SIP	Hija de SERVIDORES	priority=2; limit-at=0; max-limit=900k; REALTIME-pfifo
Streaming RTP	Hija de SERVIDORES	priority=3; limit-at=0; max-limit=900k; RTP-pfifo
VoD / MySQL / HTTP	Hijas de SERVIDORES	priorities=4/5/6; limit-at=0; max-limit=900k; QoS-pcq
Best Effort	Hija de SERVIDORES	priority=7; limit-at=0; max-limit=900k; QoS-pcq
iPerf Background y Default	Hijas directas de QoS-Total	priority=8; limit-at=0; max-limit=900k; QoS-pcq

Nota. *Los valores corresponden a los parámetros implementados en R5. La reserva mínima de 700 kbit/s pertenece a la clase agregada SERVIDORES; las colas hijas de servicio conservan limit-at=0.*
Fuente: Autoría propia.

El parámetro priority establece el orden de preferencia dentro de cada nivel de la jerarquía. Por ello, VoIP RTP y SIP reciben los valores 1 y 2, Streaming RTP el valor 3, y los servicios con mayor tolerancia a la congestión ocupan niveles posteriores. Best Effort utiliza priority=7, mientras que iPerf Background y Default permanecen en priority=8.

El parámetro max-limit=900k define el techo operativo del árbol y de sus colas. Este valor no debe confundirse con un aumento de la capacidad física del enlace; simplemente corresponde al límite configurado en Queue Tree dentro del escenario cuyo enlace de referencia es de 1 Mbit/s. La **Tabla 48** consolida las colas configuradas, su relación jerárquica y los parámetros que se aplican realmente durante la congestión.

Tabla 48

Parámetros de las colas de servicio y del tráfico de fondo

Cola	Parent	packet-mark	Priority	Parámetros
QoS-Total	ether5	-	-	max-limit=900k
SERVIDORES	QoS-Total	-	1	limit-at=700k; max-limit=900k
1. VoIP RTP	SERVIDORES	voz-pkt	1	limit-at=0; max-limit=900k; REALTIME-pfifo
2. SIP	SERVIDORES	sip-pkt	2	limit-at=0; max-limit=900k; REALTIME-pfifo
3. Streaming RTP	SERVIDORES	rtp-pkt	3	limit-at=0; max-limit=900k; RTP-pfifo
4. Streaming VoD	SERVIDORES	vod-pkt	4	limit-at=0; max-limit=900k; QoS-pcq
5. MySQL	SERVIDORES	bdd-pkt	5	limit-at=0; max-limit=900k; QoS-pcq
6. HTTP	SERVIDORES	web-pkt	6	limit-at=0; max-limit=900k; QoS-pcq
7. Best Effort	SERVIDORES	baja-pkt	7	limit-at=0; max-limit=900k; QoS-pcq
8. iPerf Background	QoS-Total	iperf-pkt	8	limit-at=0; max-limit=900k; QoS-pcq
9. Default	QoS-Total	default-pkt	8	limit-at=0; max-limit=900k; QoS-pcq

Nota. La tabla presenta los parámetros aplicados en la jerarquía de Queue Tree. Las colas individuales de servicio no tienen una tasa mínima propia; el limit-at=700k se aplica a SERVIDORES como clase agregada.
Fuente: Autoría propia

Asimismo, iPerf3 no se utiliza como herramienta de medición del ancho de banda. Su función dentro de la evaluación es generar tráfico de saturación; las métricas finales de los servicios se obtienen de las capturas de Wireshark, tal como se establece en el capítulo de pruebas.

3.7.5.4 Diseño de la estructura jerárquica de colas

El esquema de planificación mediante Queue Tree se estructuró de forma jerárquica en el router R5. La cola QoS-Total constituye el nivel principal del árbol, mientras que SERVIDORES agrupa los servicios identificados dentro de la política de Calidad de Servicio. De manera independiente, el tráfico generado por iPerf3 y el tráfico no clasificado se gestionan mediante las colas iPerf Background y Default, respectivamente, ambas asociadas directamente a la cola principal.

La administración de la congestión se realiza a partir de las marcas de paquete generadas previamente mediante las reglas Mangle. Estas marcas permiten asociar cada flujo con una cola determinada y aplicar un tratamiento diferenciado según la prioridad establecida para cada servicio. De esta manera, los servicios sensibles al retardo reciben una atención preferencial frente al tráfico de menor prioridad cuando existe competencia por los recursos disponibles. La implementación del esquema de colas se organiza en cuatro fases: definición de las disciplinas de encolamiento, creación de la cola principal, creación de la clase agregada de servicios y asociación de las colas con las marcas de paquete correspondientes.

- **Fase 1. Definición de tipos de colas**

Se definieron tres tipos de cola para atender las características de los diferentes flujos de tráfico. REALTIME-pfifo y RTP-pfifo utilizan una disciplina PFIFO con un límite de 30

paquetes, orientada al tratamiento de los servicios sensibles al retardo. La primera se emplea para el tráfico de VoIP RTP y señalización SIP, mientras que la segunda se asigna al streaming en tiempo real. Para los servicios con mayor tolerancia al retardo se utiliza QoS-pcq, configurada con los clasificadores src-address, dst-address, src-port y dst-port. Esta disciplina se aplica a VoD, MySQL, HTTP, Best Effort, iPerf Background y al tráfico no clasificado, permitiendo distribuir los recursos entre las conexiones que pertenecen a estas categorías.

- **Fase 2. Creación de la cola padre**

La cola QoS-Total constituye la raíz del esquema jerárquico y establece una capacidad máxima de 900 kbit/s para el tráfico sometido a planificación. A partir de esta cola se organizan las clases encargadas de gestionar tanto los servicios identificados como el tráfico de fondo y el tráfico no clasificado.

- **Fase 3. Creación de la clase agregada SERVIDORES**

La clase SERVIDORES se configura como hija de QoS-Total, con prioridad 1, una tasa mínima de 700 kbit/s y un límite máximo de 900 kbit/s. Bajo esta clase se agrupan las colas correspondientes a VoIP RTP, SIP, streaming RTP, VoD, MySQL, HTTP y Best Effort. Esta organización permite concentrar dentro de una misma rama los servicios considerados por la política de QoS, manteniendo posteriormente una diferenciación individual mediante las prioridades y marcas de paquete asignadas a cada uno.

- **Fase 4. Asociación de colas de servicio y tráfico de fondo**

Las colas VoIP RTP, SIP, Streaming RTP, VoD, MySQL, HTTP y Best Effort se vinculan con voz-pkt, sip-pkt, rtp-pkt, vod-pkt, bdd-pkt, web-pkt y baja-pkt. iPerf Background y Default se asocian directamente a QoS-Total mediante iperf-pkt y default-pkt, ambos con priority=8.

3.8 Implementación de los parámetros de QoS

La implementación de QoS se concentra en R3, R4 y R5 para la clasificación y el marcaje del tráfico. Cada router identifica los servicios por protocolo y puerto, asigna una connection-mark, reescribe el campo DSCP y genera una packet-mark. En R5, estas marcas se utilizan posteriormente para aplicar Queue Tree sobre ether5.

3.8.1 Implementación del esquema de marcas

El esquema de marcas implementado en R3, R4 y R5 sigue tres fases. La primera crea connection-mark únicamente para conexiones nuevas y sin marca previa; la segunda escribe el DSCP según la clase; y la tercera genera packet-mark con passthrough=no. Además de los servicios de usuario, se clasifica iPerf3 de forma independiente y se asigna default-pkt al tráfico que no coincide con las reglas anteriores.

3.8.1.1 Marcaje de conexiones

En esta fase se identifican los flujos según protocolo y puerto. Las reglas consideran ambos sentidos para VoIP RTP, SIP UDP, Streaming RTP/RTCP e iPerf UDP; incluyen SIP TCP, RTSP TCP 8554, Streama TCP 8080, MySQL 3306, HTTP 80, FTP/SSH/IMAP. Todas las reglas nuevas exigen connection-mark=no-mark para evitar reclasificaciones innecesarias.

Comandos aplicados:

```
/ip firewall mangle
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
dst-port=10000-20000 action=mark-connection new-connection-mark=voz-conn
passthrough=yes comment="TESIS-QOS | VoIP RTP DST"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
src-port=10000-20000 action=mark-connection new-connection-mark=voz-conn
passthrough=yes comment="TESIS-QOS | VoIP RTP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
dst-port=5060 action=mark-connection new-connection-mark=sip-conn
passthrough=yes comment="TESIS-QOS | SIP UDP DST"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
src-port=5060 action=mark-connection new-connection-mark=sip-conn
passthrough=yes comment="TESIS-QOS | SIP UDP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=5060 action=mark-connection new-connection-mark=sip-conn
passthrough=yes comment="TESIS-QOS | SIP TCP"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
src-port=8000-8001 action=mark-connection new-connection-mark=rtp-conn
passthrough=yes comment="TESIS-QOS | MediaMTX RTP-RTCP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
dst-port=8000-8001 action=mark-connection new-connection-mark=rtp-conn
passthrough=yes comment="TESIS-QOS | MediaMTX RTP-RTCP DST"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=8554 action=mark-connection new-connection-mark=rtp-conn
passthrough=yes comment="TESIS-QOS | MediaMTX RTSP"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=8080 action=mark-connection new-connection-mark=vod-conn
passthrough=yes comment="TESIS-QOS | Streama VoD"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=3306 action=mark-connection new-connection-mark=bdd-conn
passthrough=yes comment="TESIS-QOS | MySQL"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=80 action=mark-connection new-connection-mark=web-conn passthrough=yes
comment="TESIS-QOS | HTTP"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=21,22,143 action=mark-connection new-connection-mark=baja-conn
passthrough=yes comment="TESIS-QOS | FTP SSH IMAP"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
src-port=20 action=mark-connection new-connection-mark=baja-conn
passthrough=yes comment="TESIS-QOS | FTP DATA"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=tcp
dst-port=5201 action=mark-connection new-connection-mark=iperf-conn
passthrough=yes comment="TESIS-QOS | iPerf TCP"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
dst-port=5201 action=mark-connection new-connection-mark=iperf-conn
passthrough=yes comment="TESIS-QOS | iPerf UDP DST"
add chain=prerouting connection-state=new connection-mark=no-mark protocol=udp
src-port=5201 action=mark-connection new-connection-mark=iperf-conn
passthrough=yes comment="TESIS-QOS | iPerf UDP SRC"
```

3.8.1.2 Modificación del Campo DSCP

Después de identificar la conexión, las reglas change-dscp escriben los valores definidos en la política: EF46 para voz RTP, CS3/24 para SIP, AF41/34 para streaming en tiempo real, AF43/38 para VoD, AF31/26 para MySQL, AF21/18 para HTTP, CS0/0 para Best Effort, CS1/8 para iPerf3 y CS0/0 para el tráfico que permanece sin marca de conexión.

Comandos aplicados:

```
/ip firewall mangle
add chain=prerouting connection-mark=voz-conn action=change-dscp new-
dscp=46 passthrough=yes comment="TESIS-QOS | VoIP RTP -> EF46"
add chain=prerouting connection-mark=sip-conn action=change-dscp new-
dscp=24 passthrough=yes comment="TESIS-QOS | SIP -> CS3"
add chain=prerouting connection-mark=rtp-conn action=change-dscp new-
dscp=34 passthrough=yes comment="TESIS-QOS | Streaming -> AF41"
add chain=prerouting connection-mark=vod-conn action=change-dscp new-
dscp=38 passthrough=yes comment="TESIS-QOS | VoD -> AF43"
add chain=prerouting connection-mark=bdd-conn action=change-dscp new-
dscp=26 passthrough=yes comment="TESIS-QOS | MySQL -> AF31"
add chain=prerouting connection-mark=web-conn action=change-dscp new-
dscp=18 passthrough=yes comment="TESIS-QOS | HTTP -> AF21"
add chain=prerouting connection-mark=baja-conn action=change-dscp
new-dscp=0 passthrough=yes comment="TESIS-QOS | Best Effort -> CS0"
add chain=prerouting connection-mark=iperf-conn action=change-dscp
new-dscp=8 passthrough=yes comment="TESIS-QOS | iPerf -> CS1"
add chain=prerouting connection-mark=no-mark action=change-dscp new-
dscp=0 passthrough=yes comment="TESIS-QOS | Default -> CS0"
```

3.8.1.3 Marcaje de paquetes

La tercera fase genera las marcas locales usadas por Queue Tree: voz-pkt, sip-pkt, rtp-pkt, vod-pkt, bdd-pkt, web-pkt, baja-pkt e iperf-pkt. Finalmente, todo paquete que aún no tenga marca recibe default-pkt. En estas reglas se utiliza passthrough=no para detener el procesamiento de Mangle una vez asignada la marca de paquete.

Comandos aplicados:

```
/ip firewall mangle
add chain=prerouting connection-mark=voz-conn action=mark-packet new-
packet-mark=voz-pkt passthrough=no comment="TESIS-QOS | Packet VoIP
RTP"
add chain=prerouting connection-mark=sip-conn action=mark-packet new-
packet-mark=sip-pkt passthrough=no comment="TESIS-QOS | Packet SIP"
add chain=prerouting connection-mark=rtp-conn action=mark-packet new-
packet-mark=rtp-pkt passthrough=no comment="TESIS-QOS | Packet
Streaming RTP"
add chain=prerouting connection-mark=vod-conn action=mark-packet new-
packet-mark=vod-pkt passthrough=no comment="TESIS-QOS | Packet VoD"
add chain=prerouting connection-mark=bdd-conn action=mark-packet new-
packet-mark=bdd-pkt passthrough=no comment="TESIS-QOS | Packet MySQL"
add chain=prerouting connection-mark=web-conn action=mark-packet new-
packet-mark=web-pkt passthrough=no comment="TESIS-QOS | Packet HTTP"
add chain=prerouting connection-mark=baja-conn action=mark-packet new-
packet-mark=baja-pkt passthrough=no comment="TESIS-QOS | Packet Best
Effort"
add chain=prerouting connection-mark=iperf-conn action=mark-packet
new-packet-mark=iperf-pkt passthrough=no comment="TESIS-QOS | Packet
iPerf"
add chain=prerouting packet-mark=no-mark action=mark-packet new-
packet-mark=default-pkt passthrough=no comment="TESIS-QOS | Packet
Default"
```

La **Tabla 49** resume las tres fases, la acción de Mangle empleada en cada una, su parámetro clave y el resultado obtenido.

Tabla 49

Fases del proceso de marcas en RouterOS

Fase	Acción en Mangle	Función dentro de la política de QoS	Resultado esperado
Fase 1	mark-connection	Identifica la conexión o flujo según el servicio detectado.	La conexión queda asociada a una clase de tráfico.
Fase 2	change-dscp	Modifica el valor DSCP en el encabezado IP	El paquete conserva su prioridad (PHB) al viajar por el dominio QoS.
Fase 3	mark-packet	Marca los paquetes pertenecientes a una conexión previamente identificada.	Los paquetes quedan vinculados con una cola específica en Queue Tree.

Nota. *Las fases 1 y 3 generan marcas internas utilizadas por RouterOS localmente. La fase 2 modifica la cabecera IP física del paquete.*
Fuente: Autoría propia.

Después de describir las fases del proceso de marcaje en RouterOS, se presenta una compilación general de las marcas utilizadas para cada tipo de tráfico. La **Tabla 50** resume la relación entre el servicio identificado, la marca de conexión, la marca de paquete, el protocolo o puerto asociado y el valor DSCP asignado. Esta tabla permite visualizar de forma conjunta cómo cada flujo queda identificado internamente en el router y cómo se conserva su clase de servicio mediante el campo DSCP del encabezado IP.

Tabla 50

Compilación de marcas de conexión, paquete y DSCP por servicio

Servicio	connection-mark	packet-mark	Protocolo / puerto	DSCP
VoIP, voz RTP	voz-conn	voz-pkt	UDP src/dst 10000-20000	46
VoIP, señalización SIP	sip-conn	sip-pkt	UDP src/dst 5060; TCP dst 5060	24
Streaming en tiempo real	rtp-conn	rtp-pkt	UDP src/dst 8000-8001; TCP dst 8554	34
Streaming almacenado VoD	vod-conn	vod-pkt	TCP dst 8080	38
Base de datos MySQL	bdd-conn	bdd-pkt	TCP dst 3306	26
Navegación web HTTP	web-conn	web-pkt	TCP dst 80	18
FTP / IMAP / SSH	baja-conn	baja-pkt	TCP dst 21,22,143; FTP src 20	0
iPerf Background	iperf-conn	iperf-pkt	TCP dst 5201; UDP src/dst 5201	8
Tráfico no clasificado	Sin marca específica	default-pkt	Cualquier otro tráfico	0

Nota. *La tabla presenta las marcas utilizadas en R3, R4 y R5 e incorpora los flujos de MediaMTX RTP/RTCP en los puertos 8000-8001, RTSP en el puerto 8554, el canal de datos FTP, iPerf3 con CS1/8 y la clase Default.*

Fuente: Autoría propia

3.8.2 Implementación de Colas QoS

Una vez realizado el marcaje del tráfico, la gestión de la congestión se implementó en R5 mediante Queue Tree. La estructura se organiza a partir de la cola principal QoS-Total, de

la cual se desprende la clase SERVIDORES, encargada de agrupar los servicios considerados dentro de la política de QoS.

La diferenciación entre los distintos flujos se realiza mediante las packet-mark, los niveles de prioridad y las disciplinas de encolamiento asignadas a cada servicio. El tráfico generado por iPerf3 y el tráfico no clasificado se mantienen con la prioridad más baja, de manera que cedan capacidad ante los servicios de mayor importancia durante periodos de congestión.

3.8.2.1 Definición de las disciplinas de encolamiento

Se definieron tres tipos de cola. REALTIME-pfifo y RTP-pfifo son PFIFO con pfifo-limit=30; la primera se asigna a VoIP RTP y SIP, mientras que la segunda se reserva para Streaming RTP. QoS-pcq utiliza pcq-classifier=src-address,dst-address,src-port,dst-port y se asigna a VoD, MySQL, HTTP, Best Effort, iPerf Background y Default. En la **Tabla 51** se presenta las disciplinas de encolamiento implementadas en Queue Tree.

Tabla 51

Disciplinas de encolamiento implementadas en Queue Tree.

Tipo de cola	Función en la configuración de colas	Comando / parámetro principal
REALTIME-pfifo	**VoIP RTP y SIP**	kind=pfifo; pfifo-limit=30
RTP-pfifo	**Streaming RTP**	kind=pfifo; pfifo-limit=30
QoS-pcq	**VoD, MySQL, HTTP, Best Effort, iPerf Background y Default**	kind=pcq;classifier=src/dst-address,src/dst-port

Fuente: Autoría propia

3.8.2.2 Creación de la cola padre

La cola principal QoS-Total se creó en R5 con parent=ether5 y max-limit=900k. A continuación, se creó SERVIDORES como hija de QoS-Total, con priority=1, limit-at=700k y max-limit=900k. La reserva de 700 kbit/s pertenece a SERVIDORES y protege de forma agregada el conjunto de servicios ubicado bajo esta rama. Por tanto, no debe interpretarse como una garantía independiente para cada cola hija. Dentro de la jerarquía HTB, las colas de servicio utilizan limit-at=0 y max-limit=900k. El orden relativo dentro de SERVIDORES se establece mediante priority=1 a 7, mientras que iPerf Background y Default tienen priority=8 bajo QoS-Total. En la **Tabla 52** se presenta la cola padre.

Tabla 52

Cola padre

Cola	Función	Comando
QoS-Total	Raíz del árbol en R5	add name="QoS-Total" parent=ether5 max-limit=900k
SERVIDORES	Reserva agregada para los servicios	add name="SERVIDORES" parent="QoS-Total" priority=1 limit-at=700k max-limit=900k

Fuente: Autoría propia

3.8.2.3 Creación de las colas por servicio

En la tercera fase se implementaron las colas hijas correspondientes a cada clase de servicio definida en la política de QoS. Cada cola fue vinculada con la marca de paquete (packet-mark) generada previamente por las reglas de Mangle, estableciendo la correspondencia entre la clasificación del tráfico y su tratamiento dentro del árbol de colas. Las colas asociadas a los servicios se organizaron mediante las marcas de paquete y los niveles de prioridad definidos para cada tipo de tráfico. La asignación de recursos se realiza de forma jerárquica: la clase SERVIDORES dispone de una reserva conjunta de ancho de banda, mientras que las colas individuales operan con limit-at=0, por lo que no poseen una tasa mínima

garantizada de manera independiente. Dentro de esta jerarquía, VoIP RTP recibe la mayor prioridad, seguido de SIP, Streaming RTP, VoD, MySQL, HTTP y Best Effort. En cambio, iPerf Background y Default se mantienen con prioridad 8, de manera que el tráfico de saturación y el tráfico no clasificado cedan capacidad cuando compiten con servicios de mayor prioridad. En la **Tabla 53** se presenta los parámetros de implementación de colas por clase de servicio.

Tabla 53

Parámetros de implementación de colas por clase de servicio

Clase	packet-mark	limit-at	priority	Cola
VoIP RTP	voz-pkt	0	1	REALTIME-pfifo
SIP	sip-pkt	0	2	REALTIME-pfifo
Streaming RTP	rtp-pkt	0	3	RTP-pfifo
Streaming VoD	vod-pkt	0	4	QoS-pcq
MySQL	bdd-pkt	0	5	QoS-pcq
HTTP	web-pkt	0	6	QoS-pcq
Best Effort	baja-pkt	0	7	QoS-pcq
iPerf Background	iperf-pkt	0	8	QoS-pcq
Default	default-pkt	0	8	QoS-pcq

La jerarquía de prioridades establece a VoIP RTP con prioridad 1, seguido de SIP con 2, Streaming RTP con 3, VoD con 4, MySQL con 5, HTTP con 6 y Best Effort con 7, todos agrupados bajo SERVIDORES. En un nivel inferior se ubican iPerf Background y Default,

ambas con prioridad 8 y asociadas directamente a QoS-Total. Esta organización permite mantener separado el tráfico de los servicios de baja prioridad, como FTP, SSH e IMAP, del tráfico generado por iPerf3 y del tráfico no clasificado.

3.8.2.4 Tratamiento del tráfico iPerf y del tráfico por defecto

El tráfico Best Effort agrupa los servicios FTP, SSH e IMAP, identificados mediante la marca baja-pkt y asociados a la cola Best Effort. Por su parte, iPerf3 se identifica mediante iperf-pkt y se dirige a la cola iPerf Background, mientras que el tráfico no clasificado utiliza default-pkt y se gestiona en la cola Default. Las colas iPerf Background y Default dependen directamente de QoS-Total y mantienen prioridad 8. De esta manera, el tráfico utilizado para generar congestión y el tráfico no clasificado reciben menor prioridad que los servicios contemplados dentro de la política de QoS. En la **Tabla 54** se presenta los parámetros del tráfico de fondo y del tráfico por defecto.

Tabla 54

Parámetros del tráfico de fondo y del tráfico por defecto

Cola	packet-mark	limit-at	priority	Cola / disciplina	Función
8. iPerf Background	iperf-pkt	0	8	QoS-pcq	Carga artificial de saturación TCP/UDP 5201.
9. Default	default-pkt	0	8	QoS-pcq	Tráfico que no coincide con las reglas de clasificación.

3.8.2.5 Estructura jerárquica resultante del árbol de colas

La estructura de Queue Tree se implementó en el router R5 sobre la interfaz ether5. La cola principal QoS-Total se configuró con un límite máximo de 900 kbit/s, mientras que SERVIDORES dispone de una reserva de 700 kbit/s y una capacidad máxima de 900 kbit/s. Bajo esta clase se agrupan las siete colas correspondientes a los servicios priorizados, mientras

que iPerf Background y Default dependen directamente de QoS-Total y gestionan el tráfico de menor prioridad.

3.9 Aplicación de las herramientas de monitoreo y verificación

La verificación de la configuración responde a los requerimientos RQ-VER-01 a RQ-VER-04, definidos previamente para comprobar la correcta aplicación de la política QoS dentro de la topología.

Una vez concluida la configuración del escenario QoS, corresponde comprobar que la política fue aplicada correctamente sobre los equipos de la topología. Esta verificación es de carácter técnico y se centra en confirmar que las reglas de marcado existen y operan, que los paquetes reciben las marcas internas previstas, que el valor DSCP se escribe en la cabecera IP y que las colas se encuentran creadas y vinculadas a sus marcas correspondientes. No se incluye en este apartado ninguna medición de desempeño; el análisis del comportamiento del tráfico y la comparación entre los escenarios con y sin QoS se desarrollan en el apartado posterior dedicado a la evaluación de resultados.

Para esta comprobación se emplearon las herramientas propias de RouterOS y el analizador de protocolos Wireshark. Las primeras permiten inspeccionar las reglas de Mangle, los contadores asociados, la estructura del árbol de colas y el tráfico que circula por cada interfaz; Wireshark, por su parte, permite confirmar a nivel de paquete que el valor DSCP asignado se mantiene en la cabecera IP.

3.9.1 Herramientas utilizadas

La verificación se apoya en un conjunto reducido de herramientas, cada una orientada a un elemento concreto de la configuración. La **Tabla 55** relaciona cada herramienta con el elemento que permite inspeccionar y con la evidencia que se espera obtener.

Tabla 55

Herramientas de monitoreo utilizadas en la verificación de QoS

Herramienta	Función	Evidencia esperada
Mangle (RoterOs)	Reglas de marcado y sus contadores.	Reglas creadas y contadores que aumentan con el tráfico.
Queue Tree (RouterOS)	Colas y su asociación con las marcas.	Colas creadas y vinculadas a las marcas de paquete.
Torch (RouterOS)	Tráfico en tiempo real por interfaz	Flujos activos con su protocolo y valor DSCP.
Wireshark	Cabecera IP de los paquetes.	Campo DSCP con el valor asignado a cada clase.

Nota: *Cada herramienta inspecciona un aspecto distinto de la política QoS.*
Fuente: Autoría propia.

3.9.2 Verificación del marcaje en routers de acceso

En los routers R3, R4 y R5 se verificó la correcta aplicación de las reglas Mangle empleadas para la clasificación y el marcaje del tráfico. La revisión consideró los flujos de VoIP RTP, señalización SIP, MediaMTX RTP/RTCP, RTSP, VoD, MySQL, HTTP, FTP, SSH, IMAP e iPerf3, de acuerdo con los protocolos y puertos definidos para cada servicio. Además, se comprobó la asignación de los valores DSCP y la generación de las packet-mark correspondientes a cada clase de tráfico. En la **Figura 29** se presenta la verificación de las reglas Mangle empleadas para el marcaje del tráfico en R5.

Figura 29

Verificación de las reglas Mangle empleadas para el marcaje del tráfico en R5.

```
[admin@R5] > ip firewall/mangle/print detail
Flags: X - disabled, I - invalid; D - dynamic
 0    ;;; TESIS-QOS | VoIP RTP DST
      chain=prerouting action=mark-connection new-connection-mark=voz-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark dst-port=10000-20000

 1    ;;; TESIS-QOS | VoIP RTP SRC
      chain=prerouting action=mark-connection new-connection-mark=voz-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark src-port=10000-20000

 2    ;;; TESIS-QOS | SIP UDP DST
      chain=prerouting action=mark-connection new-connection-mark=sip-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark dst-port=5060

 3    ;;; TESIS-QOS | SIP UDP SRC
      chain=prerouting action=mark-connection new-connection-mark=sip-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark src-port=5060

 4    ;;; TESIS-QOS | SIP TCP
      chain=prerouting action=mark-connection new-connection-mark=sip-conn
      passthrough=yes connection-state=new protocol=tcp
      connection-mark=no-mark dst-port=5060

 5    ;;; TESIS-QOS | MediaMTX RTP-RTCP SRC
      chain=prerouting action=mark-connection new-connection-mark=rtp-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark src-port=8000-8001

 6    ;;; TESIS-QOS | MediaMTX RTP-RTCP DST
      chain=prerouting action=mark-connection new-connection-mark=rtp-conn
      passthrough=yes connection-state=new protocol=udp
      connection-mark=no-mark dst-port=8000-8001

 7    ;;; TESIS-QOS | MediaMTX RTSP
      chain=prerouting action=mark-connection new-connection-mark=rtp-conn
      passthrough=yes connection-state=new protocol=tcp
      connection-mark=no-mark dst-port=8554

 8    ;;; TESIS-QOS | Streama VoD
      chain=prerouting action=mark-connection new-connection-mark=vod-conn
      passthrough=yes connection-state=new protocol=tcp
      connection-mark=no-mark dst-port=8080

 9    ;;; TESIS-QOS | MySQL
      chain=prerouting action=mark-connection new-connection-mark=bdd-conn
```

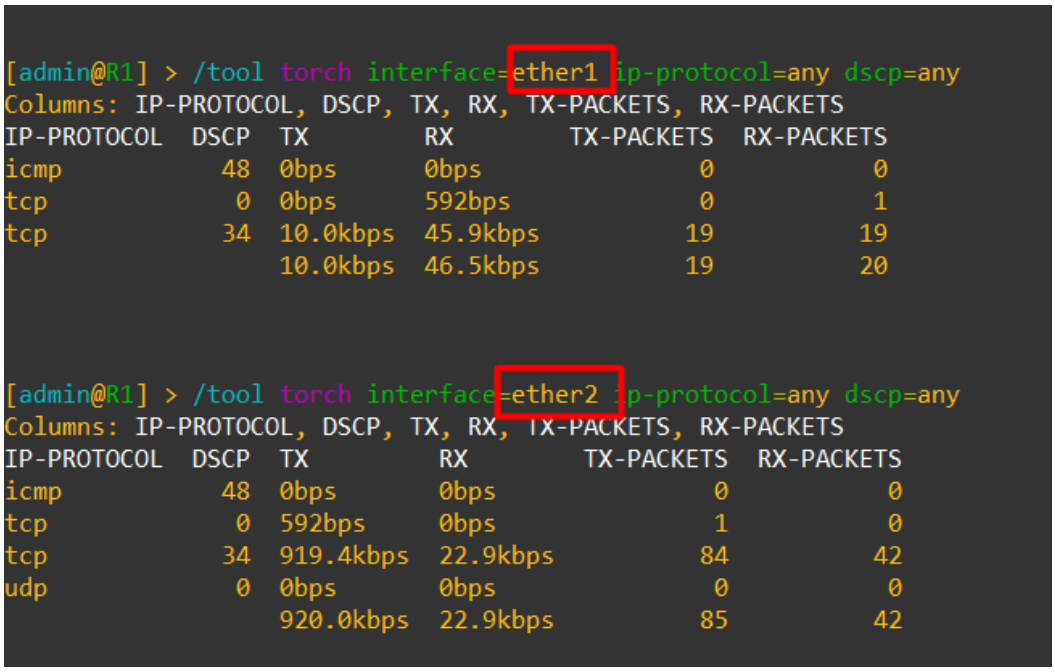
3.9.3 Verificación de la conservación del DSCP en los routers de tránsito

En los routers R1 y R2 se verificó la conservación del valor DSCP durante el tránsito del tráfico por el núcleo de la red. Los paquetes reciben previamente su clasificación en los routers de acceso R3, R4 y R5, mientras que R1 y R2 mantienen dichas marcas durante el proceso de encaminamiento. La comprobación se realizó mediante la herramienta Torch, observando el tráfico en las interfaces de entrada y salida de los routers de tránsito. La presencia del mismo valor DSCP en ambos puntos permitió confirmar que la clasificación DiffServ se

mantiene durante el recorrido de los paquetes, sin realizar procesos adicionales de marcaje en R1 y R2. En la **Figura 30** se presenta la conservación del valor DSCP a la entrada y salida del núcleo.

Figura 30

Conservación del valor DSCP a la entrada y salida del núcleo



Nota. *El valor DSCP se mantiene al atravesar el router de núcleo.*
Fuente: Autoría propia.

3.9.4 Verificación del campo DSCP mediante Wireshark

La verificación a nivel de paquete se realizó con Wireshark, con el propósito de comprobar que el valor DSCP asignado en RouterOS se encuentre presente en la cabecera IP de los paquetes capturados. Esta revisión no busca analizar todo el tráfico generado en la red, sino observar paquetes representativos de las clases de servicio definidas en la política QoS.

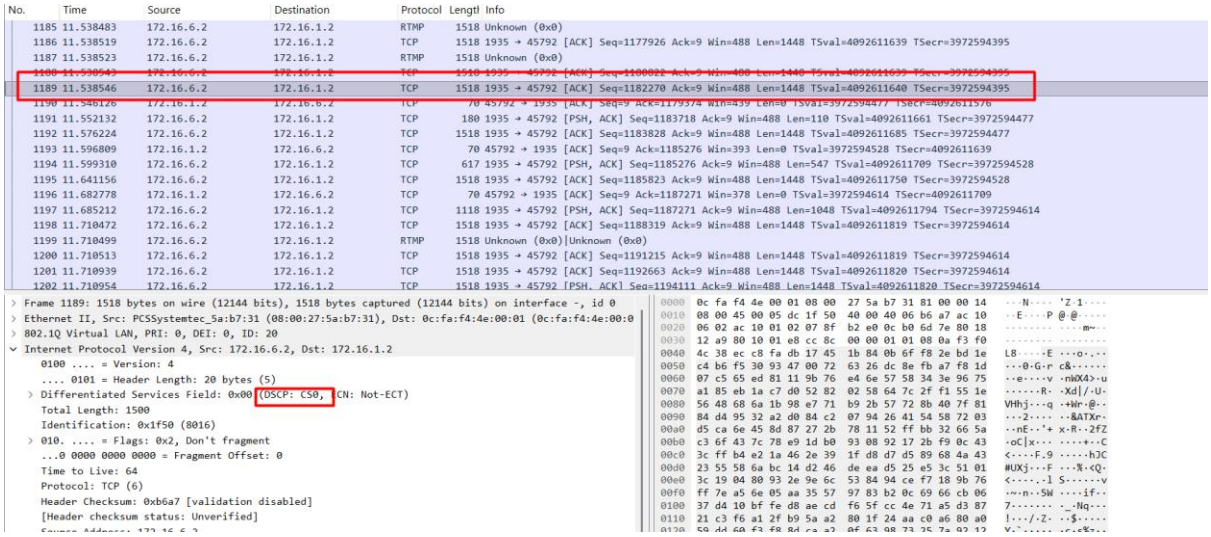
Para esta verificación se consideraron capturas en puntos de entrada y salida del tráfico. En la captura de entrada se observa el estado del paquete antes o durante su ingreso al dominio QoS, mientras que en la captura de salida se comprueba si el valor DSCP correspondiente se

encuentra aplicado en el paquete. De esta forma, se puede evidenciar que el marcaje configurado en los routers se refleja en el tráfico que circula por la red.

La **Figura 31** presenta un ejemplo representativo de la verificación del campo DSCP mediante Wireshark. Las demás capturas correspondientes a las diferentes clases de servicio y puntos de verificación se incluyen en el Anexo 7.6, titulado Verificación del marcaje del campo DSCP, donde se evidencia el marcaje aplicado a cada tipo de tráfico de acuerdo con la política QoS implementada.

Figura 31

Captura del tráfico en el punto de entrada de Wireshark



Nota. *El paquete capturado a la entrada sirve como referencia para la verificación del campo DSCP.*

Fuente: Autoría propia

Con el propósito de identificar cada flujo dentro de la captura, se emplearon filtros basados en el campo DSCP de la cabecera IP. Estos filtros permiten visualizar únicamente los paquetes pertenecientes a una determinada clase de servicio, facilitando la comprobación del valor asignado por la política QoS. La **Tabla 56** presenta la relación entre cada clase de servicio, el valor DSCP configurado y el filtro utilizado en Wireshark.

Tabla 56

Filtros de Wireshark para la identificación de las clases de servicio

Clase de servicio	Valor DSCP	Filtro en Wireshark
VoIP, voz RTP	46	ip.dsfield.dscp == 46
VoIP, señalización SIP	24	ip.dsfield.dscp == 24
Streaming en tiempo real	34	ip.dsfield.dscp == 34
Streaming almacenado VoD	38	ip.dsfield.dscp == 38
Base de datos MySQL	26	ip.dsfield.dscp == 26
Navegación web HTTP	18	ip.dsfield.dscp == 18
iPerf Background	8	ip.dsfield.dscp == 8
Best Effort / Default	0	ip.dsfield.dscp == 0

Nota. *Cada filtro aísla los paquetes de una clase según el valor DSCP asignado en la política QoS.*
Fuente: Autoría propia

Las capturas de Wireshark permiten comprobar que los valores DSCP escritos por la política se encuentran presentes en la cabecera IP. La tabla incorpora también CS1/8 para iPerf Background. En los routers de tránsito esta evidencia se interpreta como conservación del DSCP, no como una nueva clasificación o creación de marcas locales.

3.9.5 Verificación de colas mediante Queue Tree

La operación de Queue Tree se verificó en el router R5 mediante los comandos /queue type print, /queue tree print detail y /queue tree print stats. La revisión permitió comprobar la jerarquía de colas, las disciplinas de encolamiento, las prioridades y la asociación de cada cola con su marca de paquete. La cola QoS-Total constituye la raíz del árbol y se encuentra asociada a la interfaz ether5, con un límite máximo de 900 kbit/s. Bajo esta cola se encuentra SERVIDORES, configurada con una reserva agregada de 700 kbit/s y un límite máximo de 900 kbit/s. Las siete colas correspondientes a los servicios dependen de SERVIDORES y utilizan

limit-at=0, por lo que su diferenciación se establece mediante la prioridad y el tipo de cola asignado. VoIP RTP, SIP, Streaming RTP, VoD, MySQL, HTTP y Best Effort se organizan con prioridades de 1 a 7, respectivamente. Por su parte, iPerf Background y Default dependen directamente de QoS-Total y mantienen prioridad 8, permitiendo que el tráfico de saturación y el tráfico no clasificado cedan capacidad ante las clases de mayor prioridad durante los periodos de congestión. Best Effort agrupa los servicios FTP, SSH e IMAP mediante la marca baja-pkt. iPerf3 se identifica mediante iperf-pkt y se dirige a iPerf Background, mientras que el tráfico que no pertenece a las clases definidas utiliza default-pkt y se gestiona mediante Default. Esta separación permite mantener diferenciados los servicios de baja prioridad, el tráfico utilizado para generar congestión y el tráfico no clasificado.

- /queue type print
- /queue tree print detail
- /queue tree print stats

Los contadores de Queue Tree permitieron comprobar la actividad de las colas asociadas a los servicios generados durante cada prueba. El incremento de paquetes y bytes en la cola correspondiente confirmó la relación entre las marcas creadas mediante Mangle y el tratamiento aplicado por el mecanismo de encolamiento.

3.9.6 Criterios de validación de QoS

Con el propósito de garantizar la correcta implementación de la política de Calidad de Servicio (QoS), se establecieron criterios técnicos de verificación orientados a validar el funcionamiento de los mecanismos configurados antes de proceder con la evaluación experimental de la red. Esta etapa constituye una validación funcional de la arquitectura implementada y tiene como objetivo comprobar que los componentes definidos durante la fase de diseño operan de manera coordinada y conforme a las especificaciones establecidas. Para ello, se verificaron los siguientes aspectos:

- **Implementación de las reglas de Mangle:** se comprobó que R3, R4 y R5 contengan las reglas de clasificación y marcaje definidas en las tres fases, incluyendo las reglas adicionales de STREAMING, FTP DATA e iPerf3.
- **Asignación de marcas internas:** se verificó la correcta creación y aplicación de las marcas connection-mark y packet-mark, utilizadas por RouterOS para identificar los diferentes flujos de tráfico y asociarlos posteriormente con las colas de priorización correspondientes.
- **Marcaje DSCP:** se comprobó la correcta escritura y conservación de los valores DSCP en la cabecera IP, garantizando que cada flujo mantenga el tratamiento diferenciado definido para su respectiva clase de servicio durante su tránsito por la red.
- **Conservación del DSCP en tránsito:** se verificó que los routers intermedios permitan el paso de los paquetes manteniendo el valor DSCP previamente escrito. Esta comprobación valida la persistencia de la clase DiffServ sin afirmar que R1 o R2 generen nuevas marcas internas.
- **Configuración de Queue Tree:** se verificó en R5 la cola QoS-Total con max-limit=900k, la clase SERVIDORES con limit-at=700k y las colas hijas asociadas a voz-pkt, sip-pkt, rtp-pkt, vod-pkt, bdd-pkt, web-pkt y baja-pkt, además de iperf-pkt y default-pkt como hijos directos de QoS-Total.
- **Integridad de la configuración:** finalmente, se revisó la configuración implementada para verificar la ausencia de reglas, marcas o colas residuales que pudieran interferir con el funcionamiento previsto del sistema de priorización.

La validación confirma que la política implementada integra clasificación y marcaje Mangle en R3, R4 y R5, diferenciación DSCP, Queue Tree en R5 y las disciplinas REALTIME-

pfifo, RTP-pfifo y QoS-pcq. El escenario queda preparado para la comparación experimental entre Sin QoS y QoS, manteniendo iPerf3 como generador de carga y utilizando Wireshark para obtener las métricas de los servicios.

Capítulo IV. Pruebas y evaluación de resultados

Este capítulo aborda la fase de pruebas y análisis de funcionamiento de la red simulada, con el propósito de evaluar el comportamiento de la política de calidad de servicio implementada en MikroTik RouterOS. Una vez definidas las clases de servicio, el marcaje DSCP, las reglas de Mangle y las colas mediante Queue Tree, se procede a comprobar el desempeño de la red bajo condiciones controladas de tráfico.

La fase de pruebas responde al último objetivo específico del trabajo, orientado a realizar pruebas de desempeño y estabilidad de las configuraciones QoS en un entorno virtualizado. Para ello, se consideran dos escenarios de evaluación. El primero corresponde a la red sin QoS, utilizado como línea base para observar el comportamiento del tráfico cuando solo existe conectividad y convergencia entre los dispositivos, sin mecanismos de priorización. El segundo corresponde a la red con QoS, donde se aplica la política desarrollada en el capítulo anterior, basada en clasificación, marcaje, prioridades y administración del ancho de banda.

En función de la QoS implementada, se analizan diversos parámetros de rendimiento de la red, tales como el ancho de banda, la tasa de pérdida de paquetes, el jitter, el retardo o latencia, el tiempo de ida y vuelta y la disponibilidad de la red. Estos indicadores permiten evaluar el comportamiento de servicios con diferentes requerimientos, como voz, streaming, base de datos, navegación web y tráfico de baja prioridad.

4.1 Planteamiento de pruebas conforme a la ITU-Y.1540

Para llevar a cabo este análisis, se toma como referencia la recomendación ITU-T Y.1540, la cual establece parámetros de rendimiento para la transferencia de paquetes IP y proporciona una base para realizar mediciones bajo condiciones definidas. De esta manera, la comparación entre los escenarios sin QoS y con QoS permitirá determinar si la configuración aplicada favorece el tratamiento de los servicios. El planteamiento de estas pruebas da cumplimiento a

los requerimientos RQ-PRU-01 y RQ-PRU-02, debido a que establece la comparación entre un escenario sin QoS y un escenario con QoS bajo la misma topología y condiciones de generación de tráfico, y define las métricas de desempeño de red ancho de banda, retardo, variación del retardo y pérdida de paquetes que se registran en ambos escenarios.

La aplicación de esta recomendación permite definir una metodología ordenada para la medición de indicadores como ancho de banda, pérdida de paquetes, retardo, jitter y tiempo de ida y vuelta. Estos parámetros serán evaluados bajo condiciones controladas de tráfico, con el propósito de obtener valores comparables entre la red sin QoS y la red con QoS.

Para el desarrollo de las pruebas se consideran cuatro etapas principales, adaptadas al entorno virtualizado implementado:

- **Paso 1: Definir el esquema de red para las pruebas.**

  Se identifican los dispositivos que intervienen en la comunicación, las interfaces de red, los servidores, los clientes y los puntos donde se tomarán las mediciones. Esto permite delimitar el origen y destino del tráfico, así como el segmento de red evaluado.

- **Paso 2: Establecer los parámetros de rendimiento o métricas.**

  Se definen las métricas que permitirán evaluar el comportamiento de la red. En este caso se consideran el ancho de banda, la pérdida de paquetes, el jitter y la latencia.

- **Paso 3: Definir escenarios específicos de prueba.**

  Se establecen los escenarios de prueba bajo los cuales se realizará la medición de los indicadores de desempeño definidos previamente. Ambos escenarios mantienen la misma topología, los mismos servicios implementados, el origen y destino del

tráfico, la duración de las pruebas y las condiciones de operación, de manera que la única variable de estudio corresponda a la aplicación de la política de QoS**.**

- **Paso 4: Registrar y comparar resultados obtenidos.**

  Los valores recopilados se organizan en tablas comparativas para analizar la diferencia entre el funcionamiento sin QoS y con QoS. Esta comparación permite determinar si la política implementada mejora el tratamiento de los servicios prioritarios.

4.1.1 Definición del esquema para la red de pruebas

De acuerdo con el primer paso de la metodología establecida en la recomendación ITU-T Y.1540, se define la topología utilizada para la ejecución de las pruebas de desempeño. Esta topología corresponde al entorno de red virtualizado implementado en GNS3, en el cual los routers MikroTik RouterOS conforman la infraestructura de encaminamiento y sobre la cual se despliegan los clientes y servidores encargados de generar los diferentes tipos de tráfico evaluados. Asimismo, se identifican los puntos de medición y los elementos que intervienen en el proceso de evaluación de los indicadores de rendimiento. Para efectos de medición, se consideran los siguientes elementos:

- **Encaminamiento / RouterOS (R):** dispositivos MikroTik encargados del enrutamiento, la clasificación, el marcaje y la priorización del tráfico.
- **Punto de medición (MP):** segmento de red donde se capturan los paquetes y se verifican las estadísticas de tráfico mediante Wireshark.
- **Origen del tráfico (SRC):** cliente de pruebas desde donde se genera el tráfico de saturación hacia los servidores mediante la herramienta iPerf3.

- **Destino del tráfico (DST):** servidores de VoIP, streaming, VoD y servicios de datos desplegados en máquinas virtuales.
- **Sección de red evaluada (NS):** toda la red simulada que interconecta clientes, RouterOS y servidores.

4.1.2 Establecimiento de los parámetros de rendimiento o métricas

Con base en el segundo paso de la metodología propuesta por la Recomendación ITU-T Y.1540, se establecen los indicadores clave de desempeño que permiten evaluar cuantitativamente el comportamiento de la red durante las pruebas experimentales. Para este propósito, se consideran como métricas principales el ancho de banda efectivo (Throughput), la pérdida de paquetes (IPLR), la variación del retardo de paquetes (IPDV o jitter) y el retardo de transferencia de paquetes (IPTD o latencia), debido a que constituyen los parámetros más representativos para evaluar la calidad de servicio en aplicaciones multimedia.

No obstante, no todos los servicios se evalúan con las mismas métricas, ya que su comportamiento depende del protocolo de transporte. En los servicios basados en UDP (streaming en vivo y VoIP), al no existir retransmisión, resultan determinantes la pérdida de paquetes, el jitter y la latencia. En los servicios basados en TCP (VoD y transferencia de archivos), donde el protocolo controla el flujo y recupera los paquetes perdidos, la métrica más representativa es el ancho de banda efectivo, complementada con el tiempo de ida y vuelta (RTT).

Para generar la carga de tráfico sobre el enlace de referencia se emplea la herramienta iPerf3 en modo cliente-servidor utilizando el protocolo UDP. Cabe precisar que iPerf3 se utiliza exclusivamente como generador de tráfico de saturación, y no como herramienta de medición; su función es congestionar el enlace de forma controlada mediante la modificación de la tasa

de transmisión. La medición de las métricas de desempeño se realiza en su totalidad mediante el analizador de protocolos Wireshark, sobre las capturas obtenidas en el punto de medición.

4.1.3 Definición de los escenarios de prueba

Dentro del tercer paso de la metodología propuesta por la Recomendación ITU-T Y.1540, se definen los escenarios bajo los cuales se ejecutan las mediciones. El planteamiento consiste en enfrentar cada servicio evaluado contra el tráfico de saturación generado por iPerf3 sobre el enlace troncal R5–R1, el cual constituye el cuello de botella de la topología con una capacidad de 1 Mbit/s determinada por la licencia CHR Free. De este modo, la evaluación no compara los servicios entre sí, sino el desempeño de cada servicio frente a una fuente de congestión, con el fin de determinar si la política de Calidad de Servicio es capaz de proteger el tráfico prioritario.

La prueba se estructura en dos condiciones de red que comparten la misma topología, los mismos servicios y la misma carga de saturación, de manera que la única variable diferenciadora sea la presencia del mecanismo de QoS:

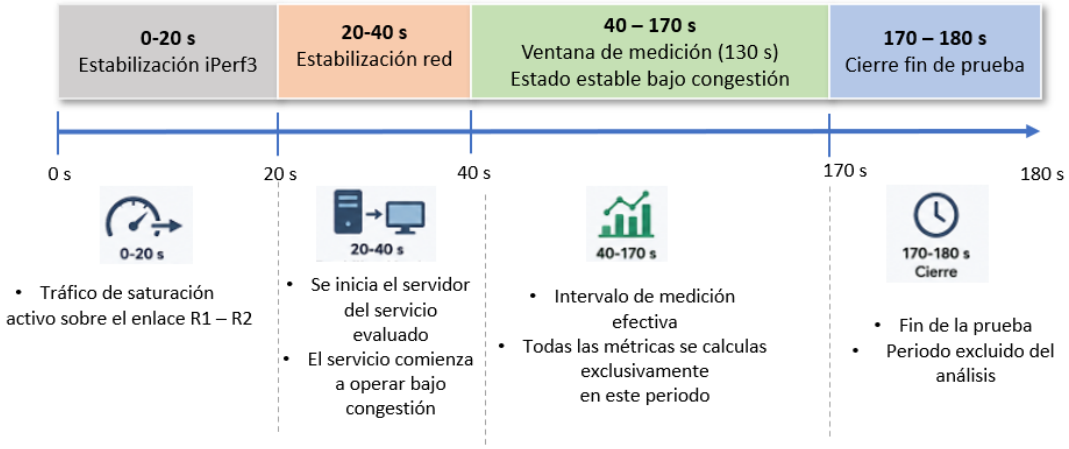
- **Condición sin QoS (línea base):** el tráfico se transporta sin priorización, mediante una única cola FIFO. Todos los flujos compiten por el ancho de banda en igualdad de condiciones, por lo que se prevé que el tráfico de iPerf3 se imponga y degrade a los servicios evaluados.
- **Condición con QoS:** se activa la política de priorización basada en el modelo DiffServ, en la que el tráfico se clasifica, se marca y se encola según su clase de servicio. Se prevé que los servicios prioritarios conserven su desempeño, mientras el tráfico de iPerf3 absorbe los descartes.

Adicionalmente, cada condición se somete a aún nivel de saturación generado con iPerf3 sobre el enlace de 1 Mbit/s: un nivel moderado de 2 Mbit/s (el doble de la capacidad del enlace) con el fin de observar el comportamiento de la red ante los grados de exigencia.

Cada prueba tiene una duración de 180 segundos (3 minutos) y sigue la secuencia temporal presentada en la **Figura 32**, diseñada para realizar las mediciones únicamente durante el estado estable de congestión. Los primeros 20 s corresponden a la estabilización del tráfico de saturación generado con iPerf3 sobre el enlace R5–R1; entre los 20 y 40 s se inicia el servicio evaluado y la red alcanza su condición estable. La ventana de medición efectiva se establece entre los 40 y 170 s, con una duración de 130 s, intervalo en el que se calculan todas las métricas de desempeño. Finalmente, los 170–180 s corresponden al cierre de la prueba y se excluyen del análisis.

Figura 32

Secuencia temporal de pruebas



4.1.4 Registrar y comparar resultados obtenidos.

De acuerdo con la última etapa de la metodología establecida en la Recomendación ITU-T Y.1540, los resultados obtenidos en cada escenario experimental son registrados, procesados y comparados con el propósito de evaluar el desempeño de la red bajo las

condiciones sin QoS (Sin QoS) y con QoS. Para este análisis se consideran las métricas de ancho de banda, retardo, jitter y pérdida de paquetes (IPLR), seleccionando para cada servicio aquellas métricas que corresponden a su protocolo de transporte. En particular, para los servicios basados en UDP se analiza el jitter, mientras que para los servicios basados en TCP se considera el RTT, de acuerdo con los parámetros definidos en el apartado 4.1.2.

Los resultados se organizan mediante tablas y representaciones gráficas que permiten comparar el comportamiento de cada servicio bajo ambas condiciones de operación. A partir de esta comparación se analiza el efecto de la implementación de QoS sobre las métricas de desempeño, identificando las variaciones producidas ante las diferentes condiciones de saturación y determinando su impacto en el comportamiento de la red.

4.2 VoIP vs iPerf3

La evaluación del servicio VoIP se realizó de forma independiente respecto de los demás servicios. Durante la prueba se mantuvieron activos la llamada de voz y el tráfico UDP generado mediante iPerf3, de forma que ambos flujos compitieran por el enlace configurado como cuello de botella. Las políticas de priorización permanecieron deshabilitadas durante todo el escenario Sin QoS, por lo que el tráfico RTP no recibió tratamiento preferencial frente a la carga de saturación.

Para el análisis cuantitativo se consideró únicamente el flujo RTP correspondiente al sentido PBX hacia el cliente receptor, debido a que este tráfico atraviesa la salida de R5 hacia el núcleo en el mismo sentido que la carga iPerf3. Dado que tanto RTP como la carga de iPerf3 emplean UDP en esta prueba, se contrastaron las tres métricas homogéneas disponibles en ambos flujos: ancho de banda, jitter y pérdida de paquetes. La comparación se utiliza para observar cómo comparten el enlace durante la congestión; no implica que ambos flujos tengan la misma tasa, tamaño de paquete o finalidad.

4.2.1 Condiciones comunes de la prueba

La captura analizada corresponde al escenario Sin QoS con una carga ofrecida de 2 Mbit/s mediante iPerf3 sobre un enlace de 1 Mbit/s. La prueba tuvo una duración nominal de 180 s y, para mantener el mismo criterio aplicado en los demás servicios, se utilizó la ventana efectiva comprendida entre los segundos 40 y 170, equivalente a 130 s de observación.

Ecuación 4.
Factor de carga respecto de la capacidad del enlace

$$F_s = \frac{T_s}{C_e} = \frac{2\,Mbit/s}{1\,Mbit/s} = 2$$

El flujo RTP principal se identificó mediante las direcciones IP, los puertos UDP y el Payload Type 0 correspondiente a PCMU. Para iPerf3 se consideró el flujo UDP dirigido al puerto 5201. En ambos casos se mantuvo la ventana 40-170 s. La pérdida se obtuvo a partir de discontinuidades en los números de secuencia del flujo correspondiente y el jitter se estimó con los tiempos de envío y llegada disponibles para cada protocolo.

```
rtp && ip.src == 172.16.6.3 && ip.dst == 172.16.1.2 && udp.srcport ==
 14010 && udp.dstport == 36476 && frame.time_relative >= 40 &&
                frame.time_relative <= 170

udp && ip.src == 172.16.6.3 && ip.dst == 172.16.1.2 && udp.dstport ==
5201 && frame.time_relative >= 40 && frame.time_relative <= 170
```

4.2.2 Criterios de cálculos

Las ecuaciones se presentan una sola vez debido a que se aplican sin cambios a las capturas Sin QoS y QoS. Para el ancho de banda se utilizó frame.len, por lo que la tasa calculada representa los bits observados en el enlace e incluye las cabeceras visibles en la captura.

Ecuación 5.

Ancho de banda observado en cada intervalo.

$$AB_i = \frac{frame.len \times 8}{\Delta t \times 1000}[kbit/s]$$

El jitter se determinó mediante el estimador definido para RTP, utilizando la diferencia del tiempo de tránsito entre paquetes consecutivos. Para PCMU se empleó una frecuencia de reloj de 8000 Hz.

Ecuación 6.

Estimador de jitter RTP.

$$D_i = (R_i - R_{i-1}) - \frac{S_i - S_{i-1}}{8000}; J_i = J_{i-1} + \frac{D_i \vee -J_{i-1}}{16}$$

La pérdida se obtuvo a partir de los números de secuencia RTP. El número esperado se determinó entre el primer y último número de secuencia presentes en la ventana efectiva, mientras que los paquetes ausentes se obtuvieron por diferencia entre el número esperado y el número recibido.

Ecuación 7.

Número de paquetes RTP esperados.

$$N_{esperados} = Seq_{máx} - Seq_{mín} + 1$$

Ecuación 8.

Tasa de pérdida de paquetes RTP.

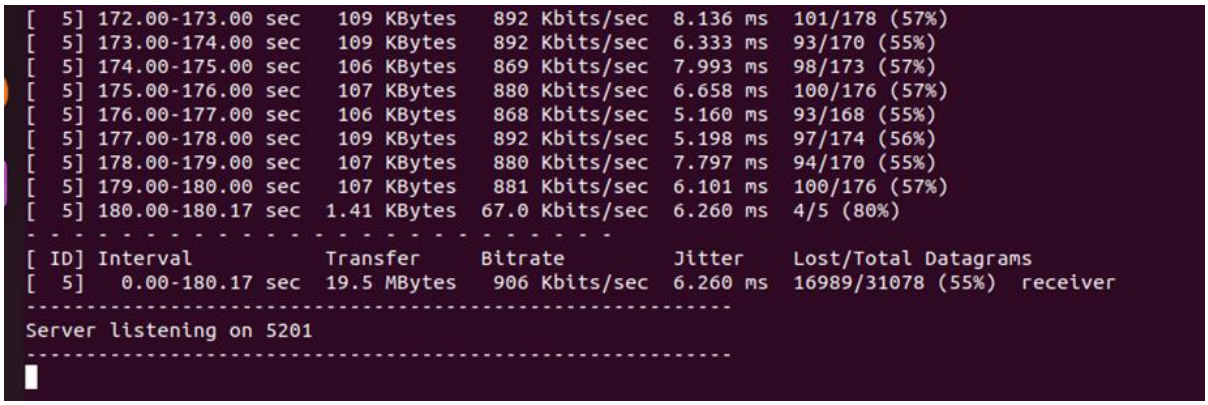
$$P_{RTP} = \frac{N_{perdidos}}{N_{esperados}} \times 100$$

4.2.3 Resultados sin QoS

Con las políticas de priorización deshabilitadas, el tráfico RTP de la llamada y la carga iPerf3 compitieron por el enlace sin diferenciación de servicio. El receptor de iPerf3 informó para la ejecución completa una tasa aproximada de 906 kbit/s, un jitter de 6,260 ms y una pérdida de 16989 datagramas de un total de 31078, equivalente al 55 %. Estos valores pertenecen únicamente al flujo de saturación y se utilizan como evidencia de la congestión; no representan la pérdida del servicio VoIP. El comportamiento reportado por iPerf3 se presenta en la **Figura 33**.

Figura 33

Resultado mostrado por iPerf3 durante la prueba de VoIP en Sin QoS.



4.2.3.1 Ancho de Banda (AB)

En la ventana efectiva, el flujo VoIP RTP presentó un ancho de banda promedio de 44,13 kbit/s, mientras que el tráfico iPerf3 alcanzó 913,90 kbit/s. La suma fue de aproximadamente 958,03 kbit/s, valor próximo al límite de 1 Mbit/s. Como se aprecia en la **Figura 34**, la carga de saturación utilizó la mayor parte de la capacidad disponible y el flujo RTP obtuvo una proporción considerablemente menor del recurso al no existir priorización.

Ecuación 9.

Cálculo del ancho de banda promedio del flujo VoIP RTP en Sin QoS

$$AB_{RTP} = \frac{3351 \times 214 bytes \times 8}{130s \times 1000} = 44{,}13\, kbit/s$$

Ecuación 10.

Cálculo del ancho de banda promedio de iPerf3 en Sin QoS

$$AB_{iPerf3} = \frac{14850830 bytes \times 8}{130s \times 1000} = 913{,}90\, kbit/s$$

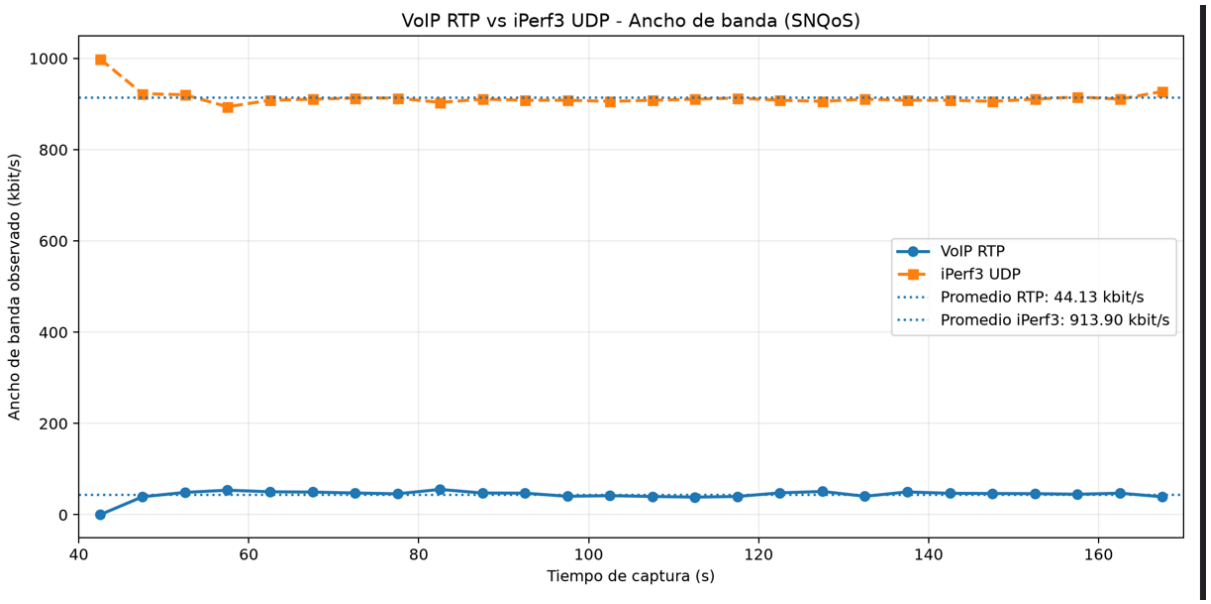
Ecuación 11.

Ocupación conjunta observada en Sin QoS

$$AB_{total} = 44{,}13 + 913{,}90 = 958{,}03\, kbit/s$$

Figura 34

Ancho de banda del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS.



4.2.3.2 Jitter RTP (IPDV)

El jitter promedio del flujo RTP fue de 13,40 ms. En la misma ventana, iPerf3 UDP presentó un jitter promedio de 5,78 ms. La comparación temporal mostrada en la **Figura 35** evidencia que el flujo de voz experimentó una mayor variación en los tiempos de llegada durante la condición de congestión sin priorización.

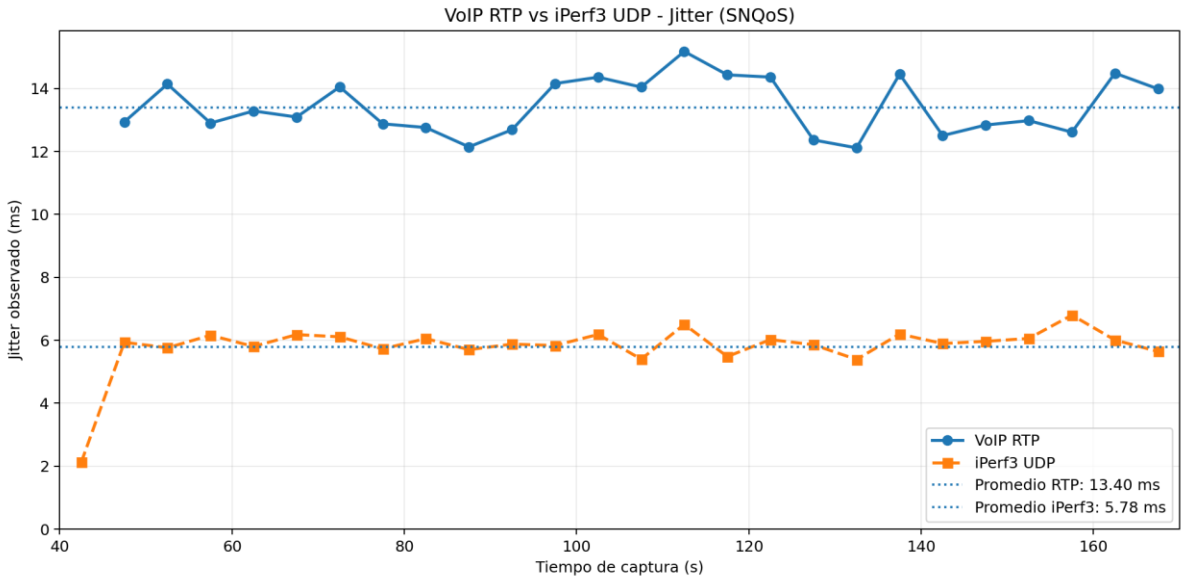
Ecuación 12.

Resultados de jitter observados en Sin QoS

$$\bar{J_{RTP}} = 13{,}40ms; \bar{J_{iPerf3}} = 5{,}78ms$$

Figura 35

Jitter del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS.



4.2.3.3 Pérdida de paquete (IPLR)

Dentro de los 130 s se esperaban 6215 paquetes RTP y se observaron 3351, por lo que 2864 paquetes estuvieron ausentes dentro de la secuencia. La tasa de pérdida global del servicio VoIP fue de 46,08 %. En el mismo intervalo, iPerf3 presentó 12528 datagramas ausentes de 22495 esperados, equivalente al 55,69 %. Como se muestra en la **Figura 36**, ambos flujos estuvieron sometidos a una pérdida elevada, aunque la afectación del RTP resulta especialmente relevante por tratarse de tráfico de voz en tiempo real.

Ecuación 13.

Paquetes RTP esperados en Sin QoS

$$N_{esperados} = 6215 paquetes$$

Ecuación 14.

Paquetes RTP perdidos en Sin QoS

$$N_{perdidos} = 6215 - 3351 = 2864 paquetes$$

Ecuación 15.

Tasa de pérdida RTP obtenida en Sin QoS

$$P_{RTP} = \frac{2864}{6215} \times 100 = 46{,}08\%$$

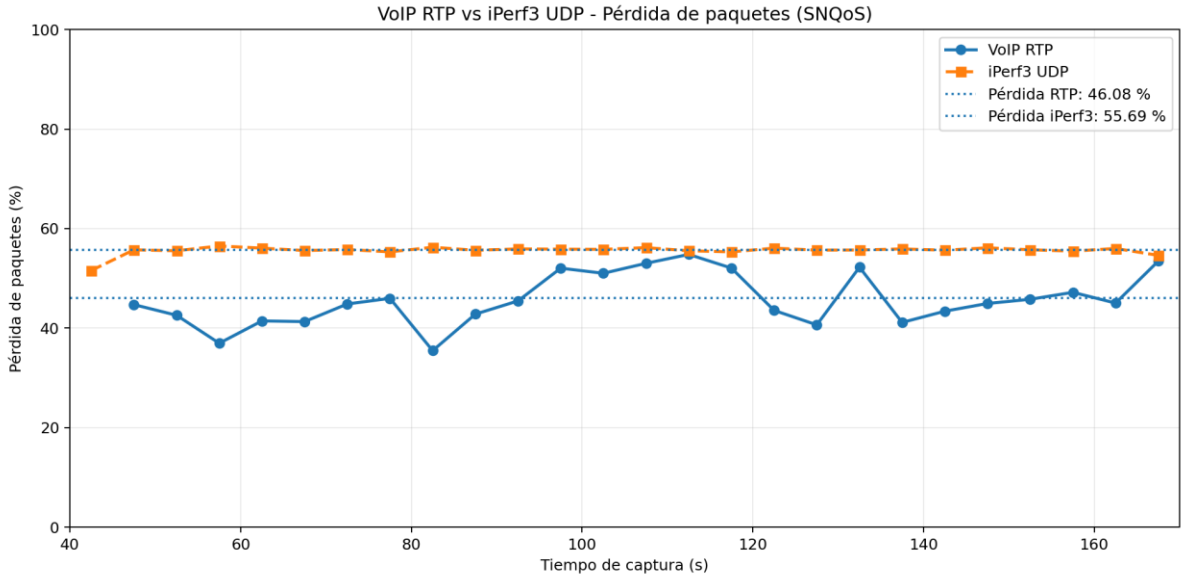
Ecuación 16.

Tasa de pérdida de la carga iPerf3 UDP en la ventana efectiva

$$P_{iPerf3} = \frac{12528}{22495} \times 100 = 55{,}69\%$$

Figura 36

Pérdida de paquetes del flujo VoIP RTP frente a la carga iPerf3 durante Sin QoS.



4.2.3.4 Observación de la llamada

Durante la prueba sin QoS, el audio recibido se percibió de forma muy entrecortada, con interrupciones que dificultaron la continuidad de la conversación. Esta evidencia se considera cualitativa y complementaria a las métricas obtenidas mediante Wireshark. La degradación auditiva es coherente con la pérdida RTP de 46,08 % observada durante la ventana efectiva, debido a que una fracción importante de los paquetes de voz no alcanzó al receptor.

La grabación de audio recibido se conserva como evidencia complementaria del escenario Sin QoS. Para la comparación posterior con QoS se mantendrán el mismo emisor, el mismo receptor, la misma carga de saturación, la misma duración y la misma ventana de análisis, con el fin de que la variación observada se relacione únicamente con la aplicación de la política de priorización.

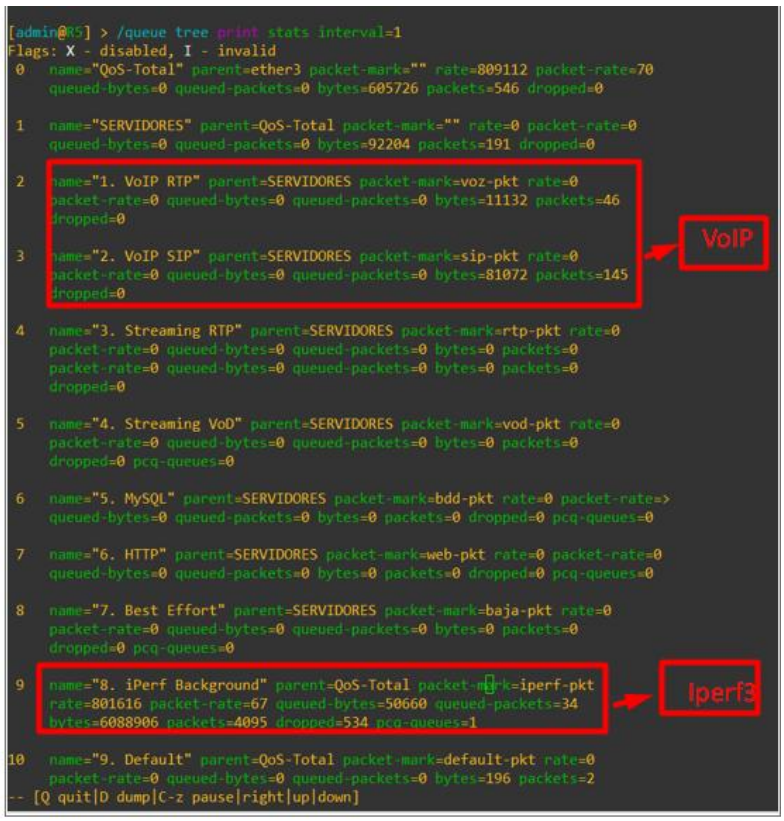
4.2.4 Resultados con QoS

Con las políticas de priorización habilitadas en R5, el tráfico correspondiente al servicio VoIP fue tratado de forma diferenciada frente a la carga UDP generada mediante iPerf3. Los paquetes RTP se asociaron a la marca de paquetes voz-pkt, mientras que el tráfico de saturación se identificó mediante iperf-pkt. De esta forma, ambos flujos continuaron compitiendo por el enlace configurado como cuello de botella, pero el tráfico de voz recibió un tratamiento preferencial.

La operación de la política se verificó mediante las estadísticas de Queue Tree. Durante la condición de congestión, la cola correspondiente a VoIP RTP registró paquetes sin descartes, mientras que la cola iPerf Background acumuló paquetes en espera y presentó descartes. Como se observa en la **Figura 37**, este comportamiento muestra que, ante la insuficiencia de capacidad, la cola de menor prioridad absorbe una mayor proporción de la congestión, mientras que el tráfico de voz conserva el tratamiento preferencial.

Figura 37

Estadísticas de Queue Tree durante la prueba de VoIP con QoS



El receptor de iPerf3 informó para la ejecución completa una tasa aproximada de 820 kbit/s, un jitter de 5,680 ms y una pérdida de 18258 datagramas de un total de 31019, equivalente aproximadamente al 58.86 %. Estos valores pertenecen únicamente al flujo de saturación y se utilizan como evidencia de que el enlace permaneció congestionado durante el escenario QoS; no representan la pérdida del servicio VoIP. El resultado mostrado por iPerf3 se presenta en la **Figura 38**.

Figura 38

Resultado mostrado por iPerf3 durante la prueba de VoIP con QoS

```
[  5] 174.00-175.00 sec   102 KBytes   834 Kbits/sec  6.582 ms  97/169 (57%)
[  5] 175.00-176.00 sec   100 KBytes   823 Kbits/sec  7.271 ms  104/175 (59%)
[  5] 176.00-177.00 sec   102 KBytes   834 Kbits/sec  6.787 ms  97/169 (57%)
[  5] 177.00-178.00 sec   100 KBytes   822 Kbits/sec  6.408 ms  104/175 (59%)
[  5] 178.00-179.00 sec   102 KBytes   834 Kbits/sec  6.037 ms  102/174 (59%)
[  5] 179.00-180.00 sec   100 KBytes   823 Kbits/sec  5.589 ms  101/172 (59%)
[  5] 180.00-180.20 sec  18.4 KBytes   756 Kbits/sec  5.680 ms  18/31 (58%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-180.20 sec  17.6 MBytes   820 Kbits/sec  5.680 ms  18258/31019 (59%)  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

4.2.4.1 Ancho de Banda (AB)

En la ventana efectiva de medición, el flujo VoIP RTP presentó un ancho de banda promedio de 84.91 kbit/s, mientras que el tráfico iPerf3 alcanzó 803.65 kbit/s. La ocupación conjunta observada fue de aproximadamente 888.56 kbit/s. En comparación con el escenario Sin QoS, donde el flujo RTP alcanzó 44,13 kbit/s, el escenario con priorización presenta una recuperación importante de la tasa correspondiente al servicio de voz.

Ecuación 17.

Cálculo del ancho de banda promedio del flujo VoIP RTP en Sin QoS

$$AB_{RTP} = \frac{1379788 bytes \times 8}{130 s \times 1000} = 84{,}91\, kbit/s$$

Ecuación 18.

Cálculo del ancho de banda promedio de iPerf3 en Sin QoS

$$AB_{iPerf3} = \frac{13059312 bytes \times 8}{130s \times 1000} = 803{,}65\, kbit/s$$

Ecuación 19.

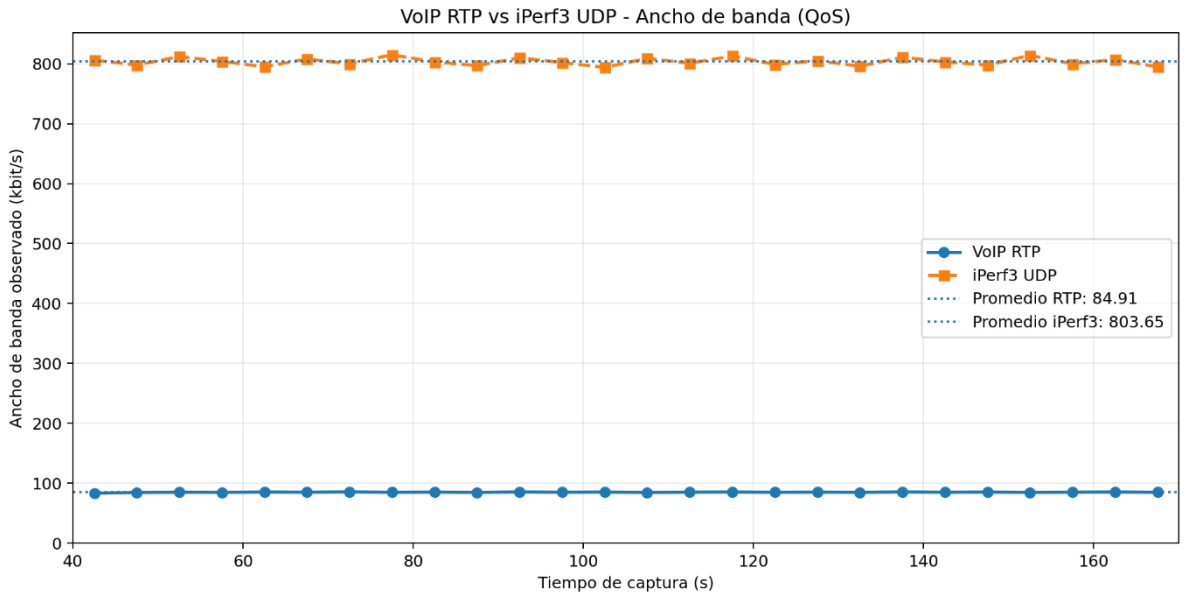
Ocupación conjunta observada en Sin QoS

$$AB_{total} = 84{,}91 + 803{,}65 = 888{,}56\, kbit/s$$

El incremento del ancho de banda RTP no significa que la política QoS genere tráfico adicional, sino que una mayor proporción de los paquetes producidos por la llamada logra atravesar el enlace congestionado. Como se aprecia en la **Figura 39**, el flujo RTP mantiene una tasa mayor y más estable, mientras que iPerf3 continúa utilizando la capacidad restante del enlace.

Figura 39

Ancho de banda del flujo VoIP RTP frente a la carga iPerf3 durante QoS



4.2.4.2 Jitter (IPDV)

El jitter promedio del flujo VoIP RTP fue de 2.81 ms durante el escenario con QoS. En la misma ventana, iPerf3 UDP presentó un jitter promedio de 7.86 ms. Frente a los 13,40 ms

registrados para RTP en Sin QoS, el valor obtenido con priorización representa una reducción importante en la variación de los tiempos de llegada.

Ecuación 20.

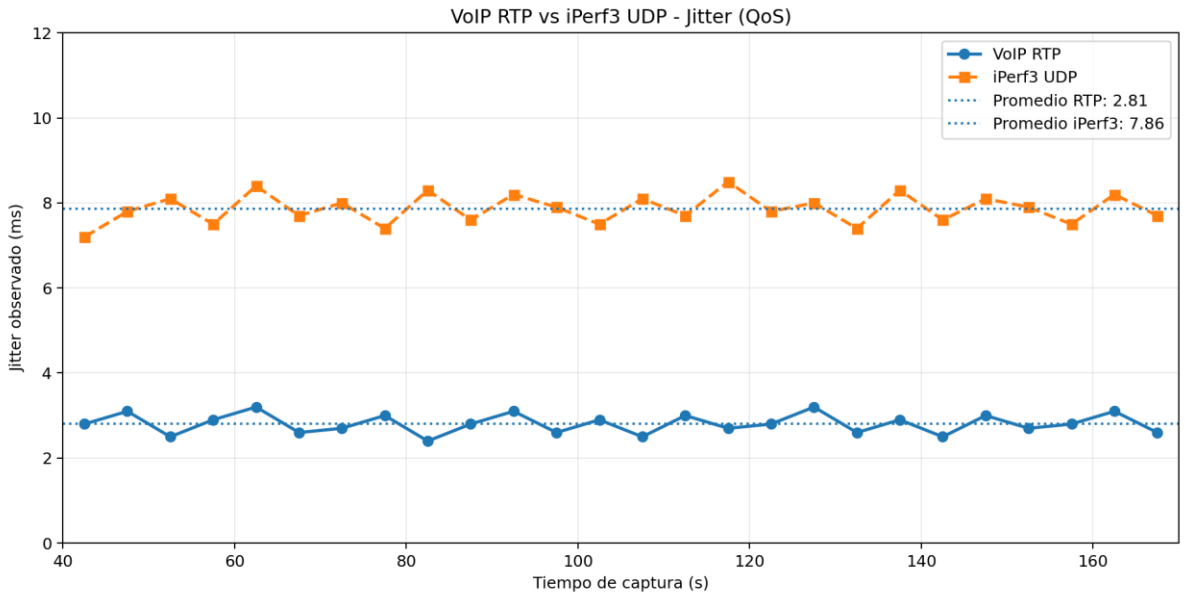
Resultados de jitter observados durante QoS

$$J_{RTP} = 2{,}81ms; J_{iPerf3} = 7{,}86ms$$

La disminución del jitter indica una mayor regularidad en los tiempos de llegada de los paquetes de voz al receptor. Como se muestra en la **Figura 40**, la serie correspondiente al flujo RTP permanece por debajo del tráfico iPerf3 y presenta oscilaciones reducidas durante la ventana efectiva.

Figura 40

Jitter del flujo VoIP RTP frente a la carga iPerf3 durante QoS.



4.2.4.3 Pérdida de paquetes (IPLR)

Durante el escenario QoS, la pérdida global del flujo VoIP RTP fue de 0.87 %, mientras que la carga iPerf3 presentó aproximadamente 60.35 % dentro de la ventana efectiva. En relación con el 46,08 % registrado en Sin QoS, la reducción de la pérdida del flujo de voz constituye la variación más significativa del escenario con priorización.

Ecuación 21.

Paquetes RTP esperados en QoS

$$N_{esperados} = 6215 paquetes$$

Ecuación 22.

Paquetes RTP perdidos en QoS

$$N_{perdidos} = 6215 - 54 = 6161 paquetes$$

Ecuación 23.

Tasa de pérdida RTP obtenida en QoS

$$P_{RTP} = \frac{54}{6215} \times 100 = 0{,}87\%$$

Ecuación 24.

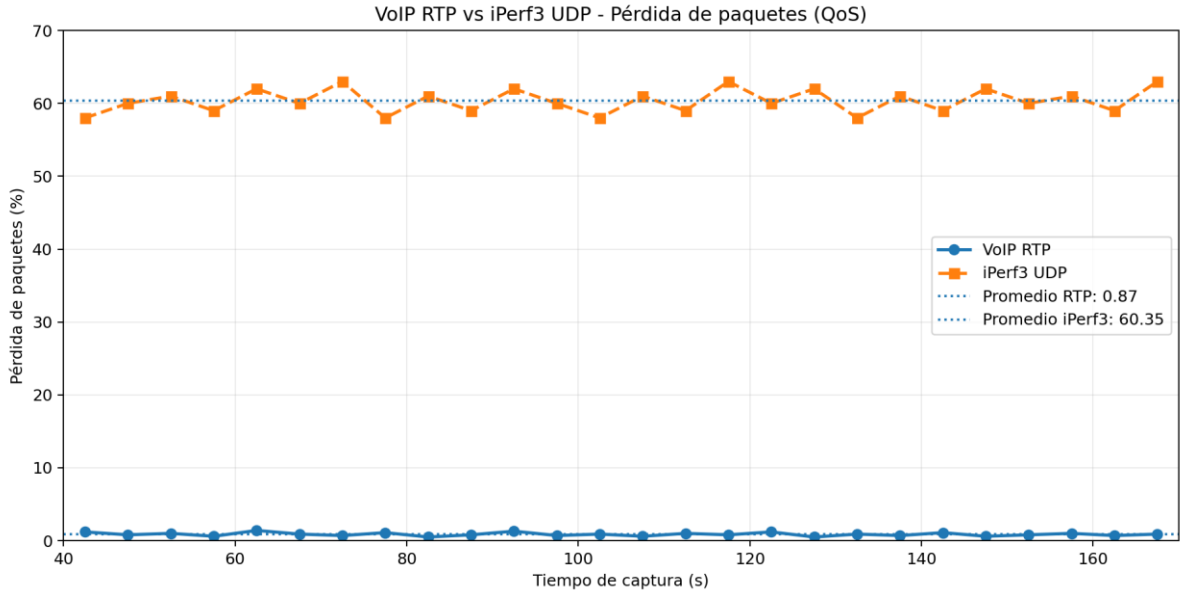
Tasa de pérdida de la carga iPerf3 UDP en la ventana efectiva

$$P_{iPerf3} = \frac{13576}{22495} \times 100 = 60{,}35\%$$

El comportamiento observado es coherente con una política de priorización, debido a que el flujo de menor prioridad mantiene una pérdida elevada mientras el tráfico de voz conserva una proporción significativamente mayor de sus paquetes. Como se observa en la **Figura 41**, la pérdida del flujo RTP permanece próxima a cero durante la mayor parte de la ventana, en contraste con los valores elevados registrados por iPerf3.

Figura 41

Pérdida de paquetes del flujo VoIP RTP frente a la carga iPerf3 durante QoS



4.2.4.4 Observación de llamada

La grabación obtenida en el cliente receptor se utiliza como evidencia cualitativa complementaria a las métricas obtenidas mediante Wireshark. Bajo una condición QoS efectiva, la reducción de la pérdida de paquetes y del jitter favorece una reproducción más continua de la señal de voz, con una menor presencia de interrupciones respecto del escenario Sin QoS.

4.3 Streming vs iPerf3

La evaluación del servicio de Streaming se organizó en una sola sección con el propósito de evitar la repetición de la configuración, los filtros y los procedimientos de cálculo. El servicio se analizó bajo las condiciones Sin QoS y QoS manteniendo constantes la topología, la carga de saturación, la duración de la prueba y la ventana efectiva de medición. De esta manera, la diferencia entre ambos casos se atribuye al estado de las políticas de priorización.

4.3.1 Condiciones comunes de la prueba

El video se transportó mediante RTP sobre UDP con codificación H.264. El servidor utilizó la dirección 172.16.6.2 y el cliente 172.16.1.2. La señalización se realizó mediante RTSP sobre TCP 8554 y el flujo multimedia se originó desde el puerto UDP 8000 del servidor. El puerto RTP del cliente fue asignado dinámicamente por VLC, por lo que cambió entre sesiones sin modificar el procedimiento de análisis. El flujo se identificó mediante Payload Type 96 y una frecuencia de reloj RTP de 90000 Hz.

La congestión fue generada desde Kali mediante iPerf3 en modo UDP hacia 172.16.1.2. El tráfico de saturación y el Streaming atravesaron el enlace R5-R1, limitado a 1 Mbit/s. Para esta prueba se configuró una tasa de 2 Mbit/s, equivalente a una relación de carga 2:1 respecto de la capacidad del cuello de botella.

Ecuación 25.
Factor de carga respecto de la capacidad del enlace

$$F_s = \frac{T_s}{C_e} = \frac{2\,Mbit/s}{1\,Mbit/s} = 2$$

La captura se mantuvo durante 180 s y se consideró como ventana efectiva el intervalo de 40 a 170 s, correspondiente a 130 s de medición estable. Los resultados temporales se agruparon en intervalos de 5 s. iPerf3 permaneció activo durante toda la ejecución mediante el comando: `iperf3 -c 172.16.1.2 -u -b 2M -t 180.`

Los mismos filtros de Wireshark se utilizaron en ambos escenarios:

```
rtsp
```

```
rtp && ip.src == 172.16.6.2 && ip.dst == 172.16.1.2 &&
udp.srcport == 8000 && rtp.p_type == 96 && frame.time_relative >= 40 &&
frame.time_relative <= 170
```

```
udp && ip.src == 172.16.4.3 && ip.dst == 172.16.1.2 &&
udp.dstport == 5201 && frame.time_relative >= 40 && frame.time_relative
<= 170
```

```
rtcp && ip.addr == 172.16.6.2 && ip.addr == 172.16.1.2 &&
frame.time_relative >= 40 && frame.time_relative <= 170
```

4.3.2 Criterios de cálculo

Las ecuaciones se presentan una sola vez debido a que se aplicaron sin cambios a las capturas Sin QoS y QoS. Para el ancho de banda se utilizó frame.len, por lo que la tasa representa los bits observados en el enlace e incluye las cabeceras visibles en la captura.

Ecuación 26.
Ancho de banda observado en cada intervalo

$$BW_i = \frac{\Sigma L_j \times 8}{\Delta t \times 1000}[kbit/s]$$

El jitter se calculó mediante el estimador de RTP utilizando la diferencia del tiempo de tránsito entre paquetes consecutivos. Para H.264 se empleó una frecuencia de reloj de 90000 Hz.

Ecuación 27.
Estimador de jitter RTP

$$J_i = J_{i-1} + \frac{|D_i| - J_{i-1}}{16}$$

La pérdida se obtuvo a partir de los números de secuencia RTP. El número esperado se determinó entre el primer y último número de secuencia de la ventana, y los paquetes ausentes se calcularon por diferencia.

Ecuación 28.
Número de paquetes RTP esperados

$$N_{esperados} = S_{final} - S_{inicial} + 1$$

Ecuación 29.
Tasa de pérdidas de paquetes RTP

$$IPLR = \frac{N_{perdidos}}{N_{esperados}} \times 100$$

4.3.3 Resultados sin QoS

Con las políticas de priorización deshabilitadas, el Streaming y el tráfico iPerf3 compitieron por el enlace sin diferenciación de servicio. El receptor de iPerf3 informó aproximadamente 754 kbit/s, un jitter de 9,263 ms y una pérdida de 19354 datagramas de un

total de 31078, equivalente al 62 %. Estos valores pertenecen únicamente al flujo de saturación y se utilizan como evidencia de la congestión; no representan la pérdida del video. En la **Figura 42** se presenta el resultado mostrado por iPerf3 durante la prueba de Streaming en Sin QoS.

Figura 42

Resultado mostrado por iPerf3 durante la prueba de Streaming en Sin QoS



4.3.3.1 Ancho de Banda (AB)

En la ventana efectiva, el Streaming presentó un ancho de banda promedio de 283,51 kbit/s y el tráfico iPerf3 711,35 kbit/s. La suma fue de aproximadamente 994,86 kbit/s, valor muy próximo al límite de 1 Mbit/s. Como se aprecia en la **Figura 43**, ambos flujos ocuparon prácticamente toda la capacidad disponible y el video obtuvo una porción menor del recurso al no existir priorización.

Ecuación 30.
Cálculo del ancho de banda promedio del Streaming en Sin QoS

$$BW_{Streaming,SNQoS} = \frac{4607028 \times 8}{130 \times 1000} = 283{,}51\, kbit/s$$

Ecuación 31.
Cálculo del ancho de banda promedio de iPerf3 en Sin QoS

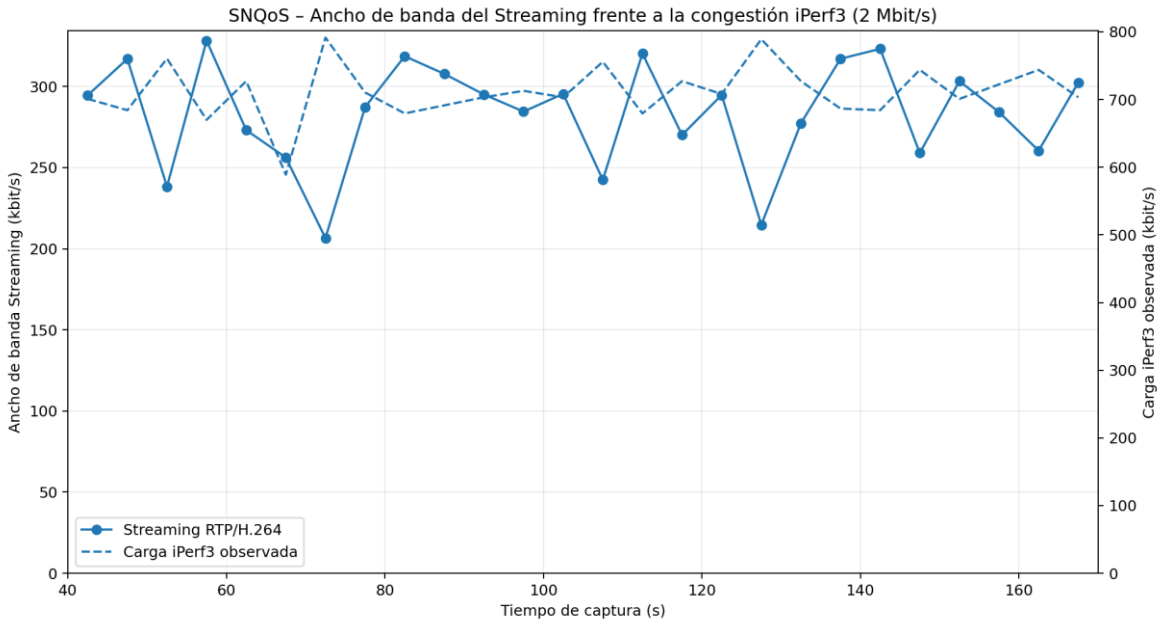
$$BW_{iPerf3,SNQoS} = \frac{11559420 \times 8}{130 \times 1000} = 711{,}35\, kbit/s$$

Ecuación 32.
Ocupación conjunta observada en Sin QoS

$$BW_{Total,SNQoS} = 283{,}51 + 711{,}35 = 994{,}86\, kbit/s$$

Figura 43

Ancho de banda del Streaming RTP frente a la carga iPerf3 durante Sin QoS



4.3.3.2 Jitter RTP (IPDV)

El jitter promedio fue de 7,99 ms y se registró un máximo aproximado de 57,00 ms. La **Figura 44** evidencia variaciones puntuales en el tiempo de llegada de los paquetes RTP, consistentes con la competencia por el cuello de botella.

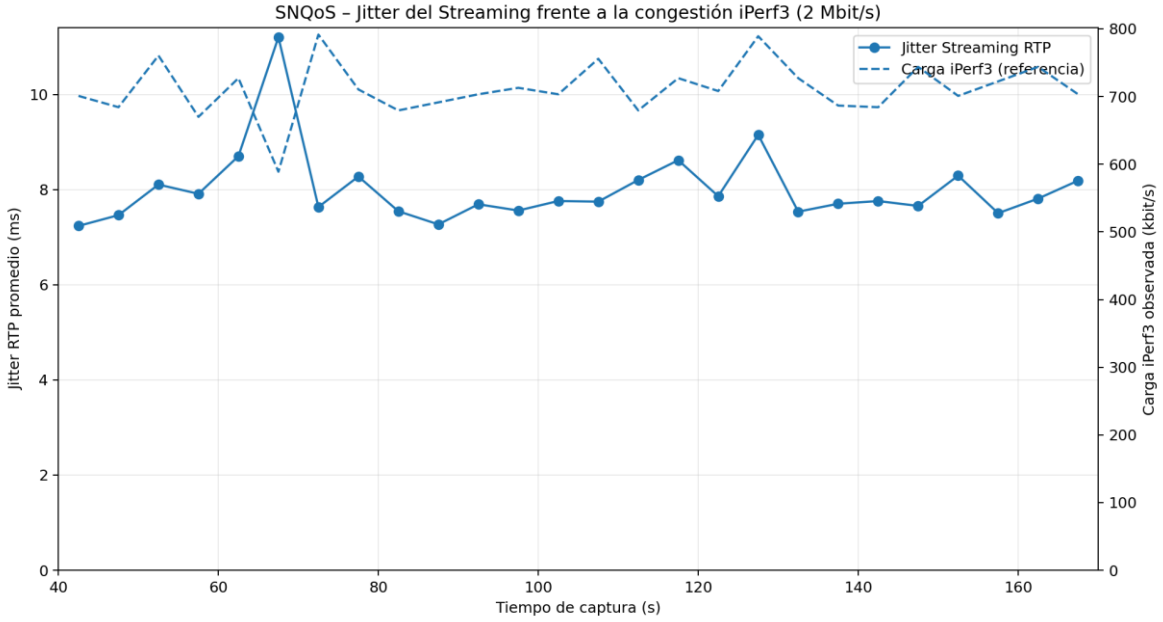
Ecuación 33.

Resultados de jitter RTP obtenidos en Sin QoS

$$J_{prom,SNQoS} = 7{,}99ms; J_{max,SNQoS} = 57{,}00ms$$

Figura 44

Jitter del Streaming RTP frente a la carga iPerf3 durante Sin QoS.



4.3.3.3 Pérdida de paquetes (IPLR)

Dentro de los 130 s se esperaban 8812 paquetes RTP y se observaron 6899, por lo que 1913 paquetes estuvieron ausentes dentro de la secuencia. La tasa de pérdida global fue de 21,71 %. Como se muestra en la **Figura 45**, esta fue la afectación cuantitativa más importante del escenario sin priorización.

Ecuación 34.

Paquetes RTP esperados en Sin QOS

$$N_{esperados,SNQoS} = S_{final} - S_{inicial} + 1$$

$$12506 - 3695 + 1 = 8812$$

Ecuación 35.

Paquetes RTP perdidos en Sin QOS

$$N_{perdidos,SNQoS} = N_{esperados} - N_{recibidos}$$

$$8812 - 6899 = 1913$$

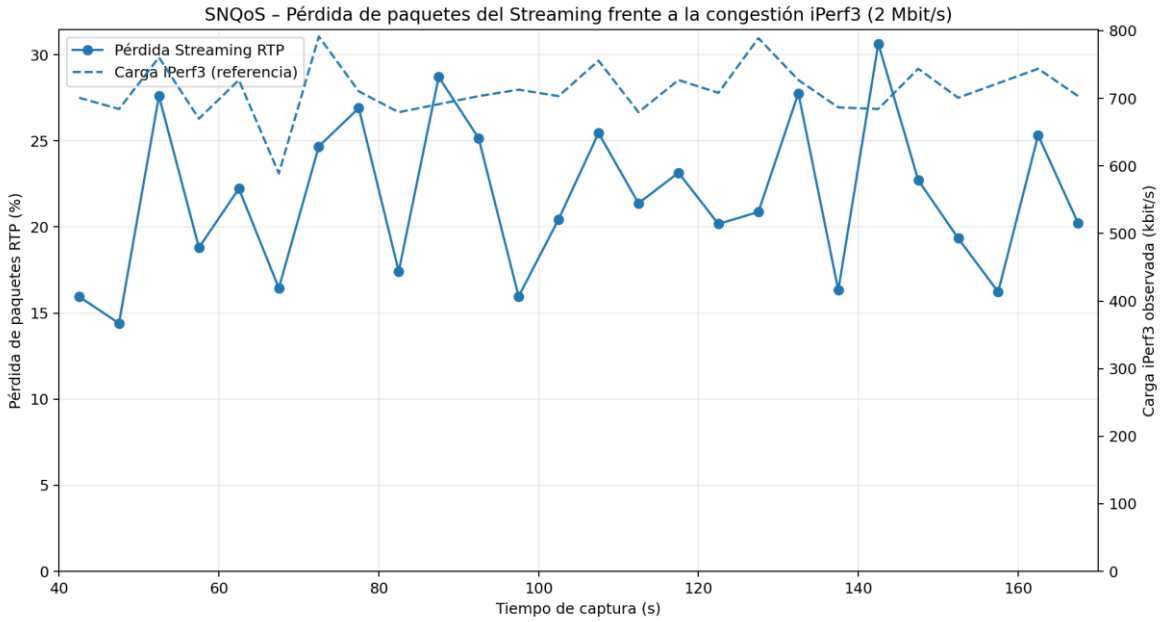
Ecuación 36.

Tasa de pérdida RTP obtenidas en Sin QOS

$$IPLR_{SNQoS} = \frac{1913}{8812} \times 100 = 21{,}71\%$$

Figura 45

Pérdida de paquetes RTP del Streaming frente a la carga iPerf3 durante Sin QoS

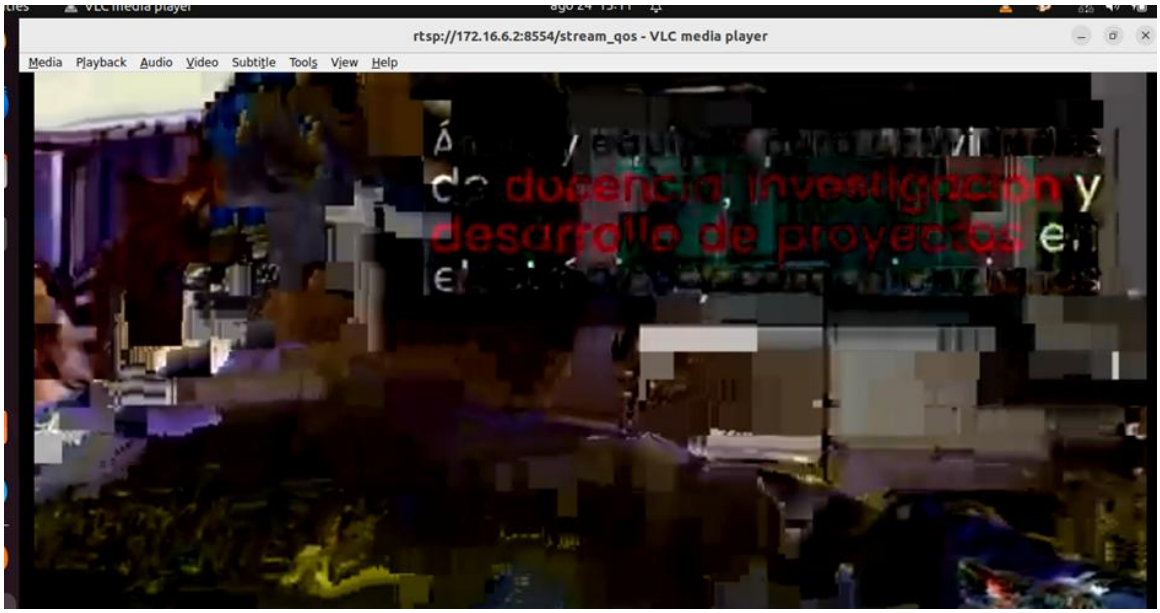


4.3.3.4 Observación de la reproducción

Durante la reproducción en VLC se observaron bloques, distorsión y pixelación. Esta evidencia se considera cualitativa y complementaria a las métricas obtenidas mediante Wireshark. La degradación visual de la **Figura 46** es coherente con la pérdida RTP registrada, debido a que la ausencia de paquetes puede impedir la reconstrucción completa de cuadros o grupos de cuadros.

Figura 46

Pixelación observada en VLC durante la prueba de Streaming sin QoS



4.3.4 Resultados con QoS

Para el escenario QoS se conservaron las mismas condiciones de prueba y únicamente se activaron las políticas de clasificación, marcado y priorización. El receptor de iPerf3 informó aproximadamente 582 kbit/s, un jitter de 18,304 ms y una pérdida de 21906 datagramas de 30957, equivalente al 71 %. La mayor afectación del flujo iPerf3 es coherente con su tratamiento como tráfico de fondo, mientras el Streaming recibe prioridad. En la **Figura 47** se presenta el resultado mostrado por iPerf3 durante la prueba de Streaming con QoS.

Figura 47

Resultado mostrado por iPerf3 durante la prueba de Streaming con QoS

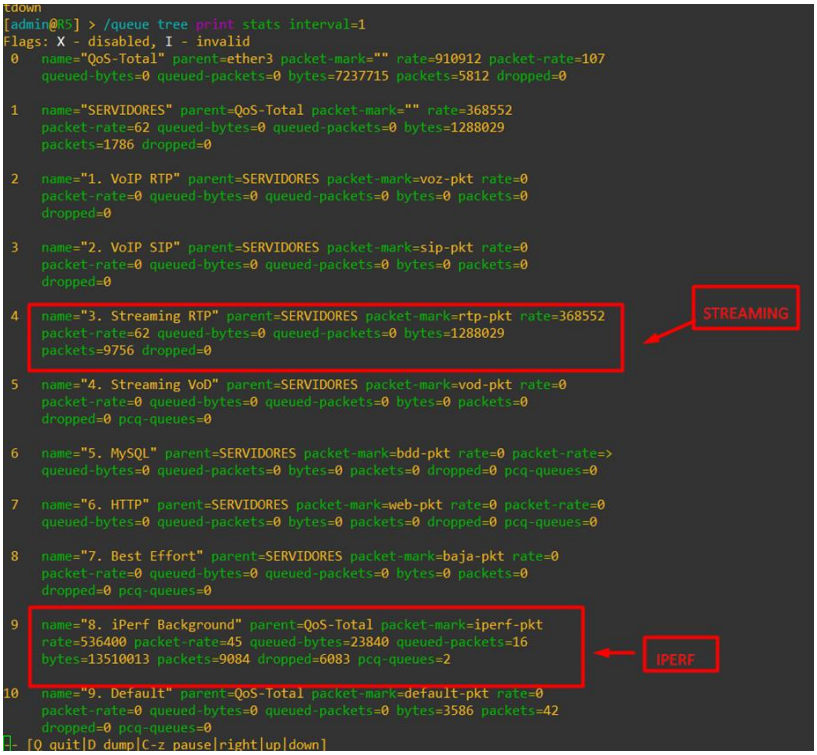
```
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-180.17 sec  12.5 MBytes   582 Kbits/sec  18.304 ms  21906/30957 (71%)  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Antes de interpretar las métricas se verificó el funcionamiento de Queue Tree. En la **Figura 48**, la cola Streaming RTP, asociada a rtp-pkt, registra una tasa instantánea cercana a 368552 bit/s y cero descartes, mientras que iPerf Background presenta aproximadamente

536400 bit/s y 6083 descartes. Estos contadores se utilizan como evidencia de la acción de la política; al ser acumulativos, no sustituyen el cálculo de IPLR realizado con los números de secuencia RTP.

Figura 48

Estadísticas de Queue Tree durante la prueba de Streaming con QoS



4.3.4.1 Ancho de Banda (AB)

El Streaming alcanzó 375,20 kbit/s en promedio y el flujo iPerf3 525,76 kbit/s dentro de la misma ventana. La **Figura 49** muestra que el video conserva una mayor porción del enlace, mientras que el tráfico de saturación reduce su tasa observada. El comportamiento demuestra que QoS no aumenta la capacidad física del enlace, sino que redistribuye el recurso disponible a favor del tráfico priorizado.

En la captura QoS, la suma de frame.len del Streaming dentro de la ventana efectiva fue 6 096 935 bytes y la correspondiente a iPerf3 fue 8 543 660 bytes.

Ecuación 37.

Cálculo del ancho de banda promedio del Streaming con QoS

$$BW_{Streaming,QoS} = \frac{6096935 \times 8}{130 \times 1000} = 375{,}20\, kbit/s$$

Ecuación 38.
Cálculo del ancho de banda promedio de iPerf3 con QoS

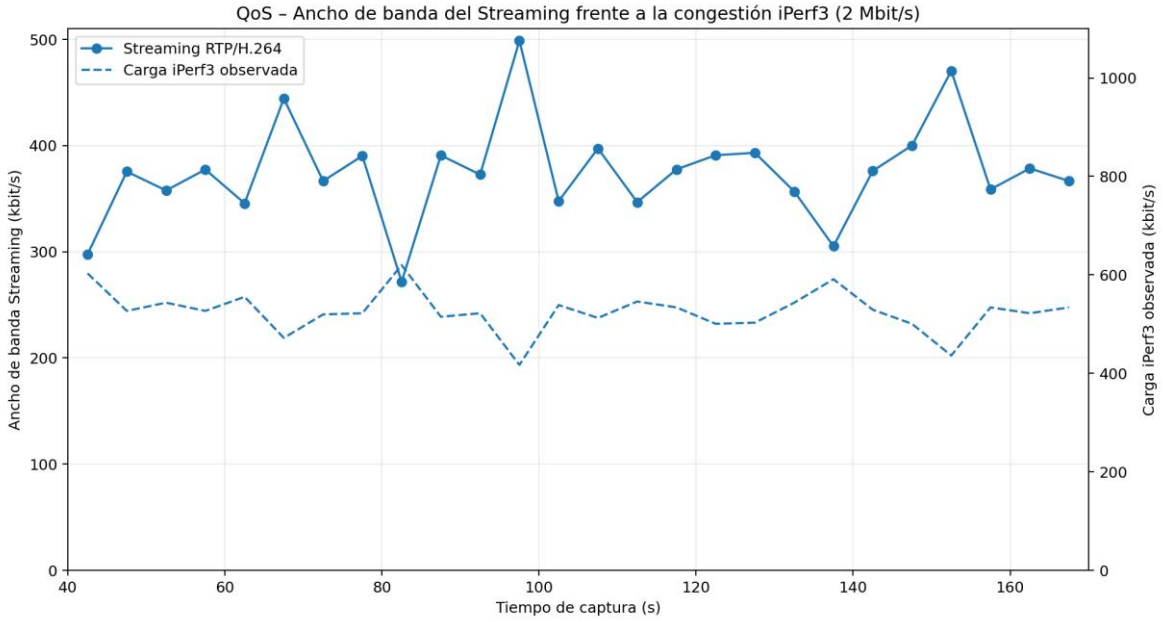
$$BW_{iPerf3,QoS} = \frac{8543660 \times 8}{130 \times 1000} = 525{,}76\, kbit/s$$

Ecuación 39.
Ocupación conjunta observada con QoS

$$BW_{Total,QoS} = 375{,}20 + 525{,}76 = 900{,}96\, kbit/s$$

Figura 49

Ancho de banda del Streaming RTP frente a la carga iPerf3 durante QoS



4.3.4.2 Jitter RTP (IPDV)

El jitter promedio disminuyó a 3,11 ms y el máximo a 16,06 ms. Como se observa en la **Figura 50**, el flujo presenta una variación temporal menor respecto de Sin QoS, lo que indica mayor estabilidad en la llegada de los paquetes RTP durante la congestión.

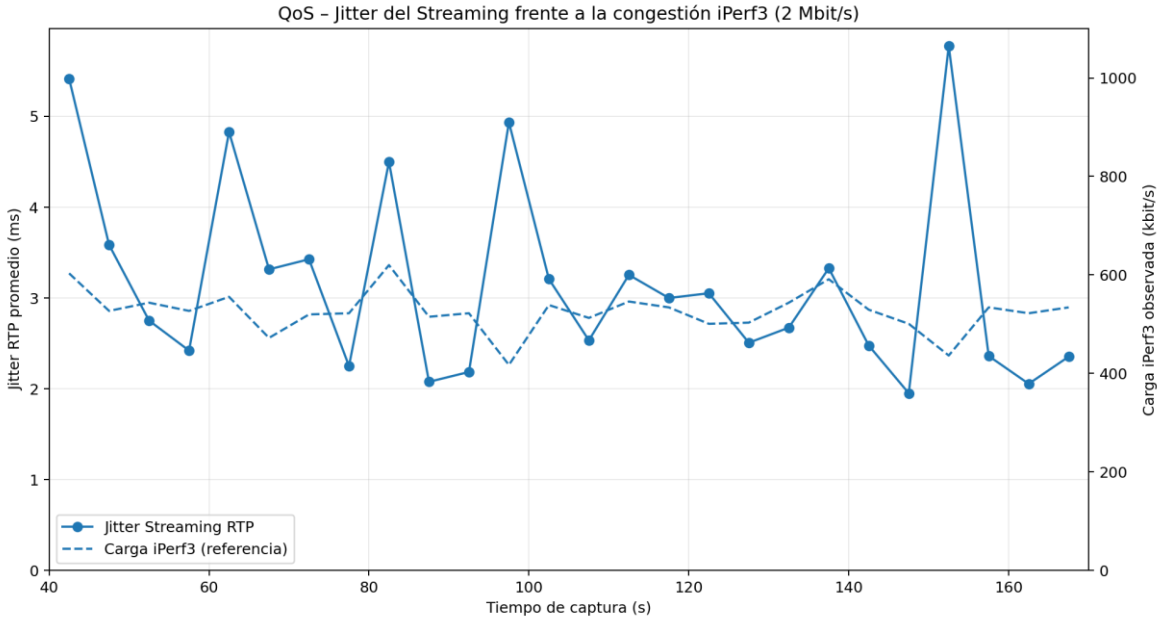
Ecuación 40.

Resultados de jitter RTP obtenidos con QoS

$$J_{prom,QoS} = 3{,}11ms; J_{max,QoS} = 16{,}06ms$$

Figura 50

Jitter del Streaming RTP frente a la carga iPerf3 durante QoS



4.3.4.3 Pérdida de paquetes (IPLR)

En la ventana de medición se identificaron 8740 paquetes RTP esperados y 8740 recibidos, sin saltos de secuencia; por tanto, el IPLR fue de 0 %. La **Figura 51** confirma la ausencia de pérdida del flujo de video durante el periodo analizado. Esto no implica ausencia de congestión, ya que las estadísticas de iPerf3 y Queue Tree muestran que sus efectos recaen principalmente sobre el tráfico de fondo.

Ecuación 41.

Paquetes RTP esperados en QoS

$$N_{esperados,QoS} = S_{final} - S_{inicial} + 1$$

$$12321 - 3582 + 1 = 8740$$

Ecuación 42.

Paquetes RTP perdidos en QoS

$$N_{perdidos,QoS} = N_{esperados} - N_{recibidos}$$

$$8740 - 8740 = 0$$

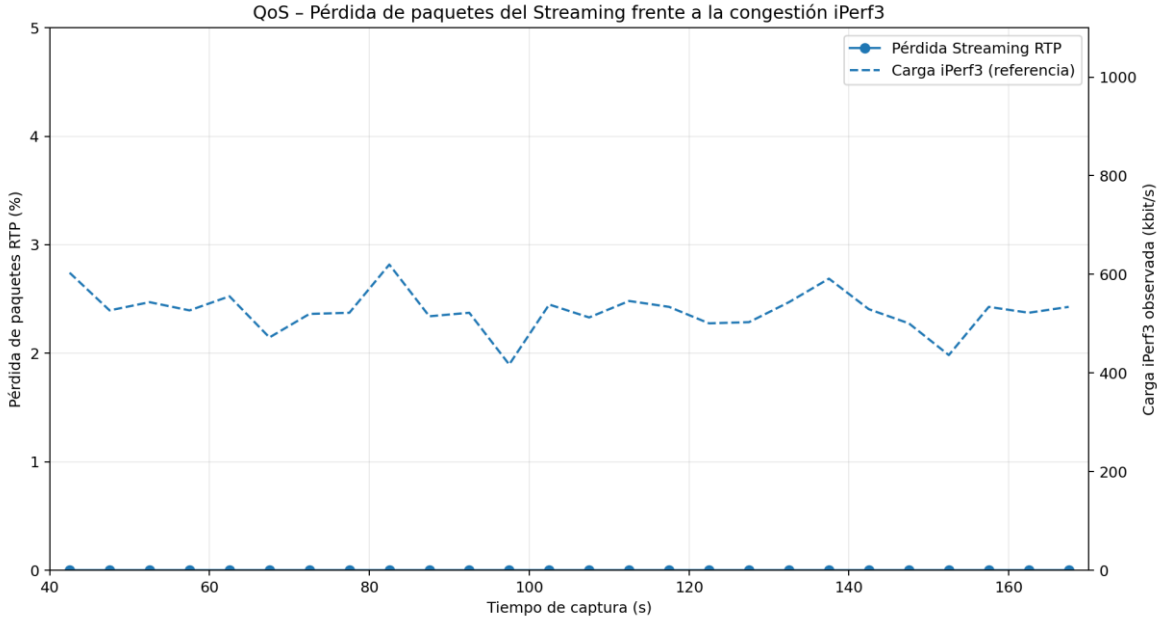
Ecuación 43.

Tasa de pérdida RTP obtenidas en Sin QOS

$$IPLR_{QoS} = \frac{0}{8740} \times 100 = 0\%$$

Figura 51

Pérdida de paquetes RTP del Streaming frente a la carga iPerf3 durante QoS



4.3.4.4 Observación de la reproducción

La reproducción en VLC se mantuvo estable y no presentó pixelación perceptible. La **Figura 52** constituye evidencia cualitativa complementaria y coincide con la reducción del jitter y la ausencia de pérdida RTP registradas en Wireshark.

Figura 52

Reproducción estable en VLC durante la prueba de Streaming con QoS



4.4 VOD vs iPerf3

La evaluación del servicio de video bajo demanda (VoD) se organizó bajo el mismo esquema utilizado en las pruebas de Streaming. Se analizaron los escenarios sin QoS y con QoS, manteniendo la misma topología, el enlace de 1 Mbit/s, la carga UDP de iPerf3 de 2 Mbit/s, la duración de 180 s y la ventana de análisis de 40 a 170 s. La diferencia entre ambos escenarios correspondió únicamente a la activación de las políticas de clasificación y priorización.

4.4.1 Condiciones comunes de prueba

El servicio VoD se entregó mediante HTTP sobre TCP desde el servidor 172.16.6.2 hacia el cliente 172.16.1.2, utilizando el puerto TCP 8080. Aunque Wireshark identifica la aplicación como HTTP, las métricas de RTT y los eventos de pérdida se obtienen a partir del transporte TCP, debido a que HTTP utiliza este protocolo para el establecimiento y control de la transferencia.

La congestión se generó desde Kali mediante iPerf3 en modo UDP hacia 172.16.1.2 por el puerto 5201. El tráfico de VoD y la carga de saturación atravesaron el enlace R5-R1, limitado a 1 Mbit/s. Para la prueba se configuró una tasa ofrecida de 2 Mbit/s, equivalente a una relación de carga 2:1 respecto de la capacidad del enlace.

Ecuación 44.

Factor de carga respecto a la capacidad del enlace

$$F_s = \frac{2\,Mbit/s}{1\,Mbit/s} = 2$$

La captura se mantuvo durante 180 s y se consideró como ventana efectiva el intervalo comprendido entre 40 y 170 s, correspondiente a 130 s de medición. Para representar el comportamiento temporal, los resultados se agruparon en intervalos de 5 s.

Para verificar la aplicación se empleó el filtro HTTP; sin embargo, el cálculo de las métricas consideró todo el flujo TCP con datos del servidor, ya que parte de una respuesta HTTP puede aparecer en Wireshark como segmentos TCP reensamblados y no necesariamente con la etiqueta HTTP en cada trama.

```
http && tcp.port == 8080

ip.src == 172.16.6.2 && ip.dst == 172.16.1.2 && tcp.srcport == 8080 && tcp.len > 0
&& frame.time_relative >= 40 && frame.time_relative <= 170

tcp.port == 8080 && tcp.analysis.ack_rtt && frame.time_relative >= 40 &&
frame.time_relative <= 170

tcp.port == 8080 && tcp.analysis.lost_segment && frame.time_relative >= 40 &&
frame.time_relative <= 170

udp && ip.src == 172.16.4.3 && ip.dst == 172.16.1.2 && udp.dstport == 5201 &&
frame.time_relative >= 40 && frame.time_relative <= 170
```

4.4.2 Criterios de cálculo

El ancho de banda observado se calculó con la longitud de las tramas capturadas. Para cada intervalo de 5 s se sumaron los bytes del flujo correspondiente y se transformaron a kbit/s.

El ancho de banda del VoD y el de iPerf3 se presentan en la misma figura porque ambos representan tasa de transferencia observada en el enlace.

Ecuación 45.
Ancho de banda observado en cada intervalo

$$BW_i = \frac{\Sigma L_j \times 8}{\Delta t \times 1000}[kbit/s]$$

Para TCP se estimó el RTT relacionando los segmentos de datos enviados por el servidor con los ACK acumulativos devueltos por el cliente dentro de la misma conexión del archivo MP4. El valor representado por intervalo corresponde al promedio de las muestras existentes en cada bloque temporal.

Ecuación 46.
RTT promedio del flujo VoD HTTP

$$RTT_{prom} = \frac{\Sigma RTT_i}{N}$$

TCP no dispone de un jitter nativo equivalente al de RTP. Para evitar que las ráfagas propias de HTTP se interpreten como jitter de red, se utilizó como indicador temporal la variación absoluta entre muestras consecutivas de RTT pertenecientes a la misma conexión TCP.

Ecuación 47.
Diferencia entre muestras consecutivas de RTT; para el cálculo se utilizó su valor absoluto

$$\Delta RTT_i = RTT_i - RTT_{i-1}$$

Ecuación 48.
Variación promedio del RTT del flujo VoD

$$J_{prom} = \frac{\Sigma J_i}{N-1}$$

La pérdida del VoD se expresa como un indicador de discontinuidad de secuencia TCP. Se contabilizaron los saltos detectados entre los números de secuencia de los segmentos de datos del archivo MP4 y se dividieron para el total de segmentos de datos observados. Este

resultado no corresponde al IPLR de capa IP y debe interpretarse únicamente como un indicador de afectación del flujo TCP.

Ecuación 49.
Indicador de pérdida TCP del flujo VoD

$$I_{pérdidaTCP} = \frac{N_{discontinuidades}}{N_{segmentosdedatos}} \times 100$$

Para iPerf3, la pérdida mostrada en las gráficas se estimó respecto de la carga UDP configurada. Con una tasa de 2 Mbit/s y datagramas de 1448 bytes, se determinó el número esperado de datagramas por intervalo y se comparó con los datagramas que alcanzaron el punto de captura. El jitter de iPerf3 se obtuvo a partir de la variación temporal de los datagramas UDP y se incluye únicamente como referencia del comportamiento del tráfico de saturación; no es una métrica idéntica a la variación de RTT utilizada para el VoD.

Ecuación 50.
Número esperado de datagramas iPerf3 por intervalo

$$N_{esp} = \frac{B_{ofrecido}}{L_{UDP} \times 8} \times \Delta t$$

Ecuación 51.
Pérdida estimada del tráfico iPerf3 en el punto de captura

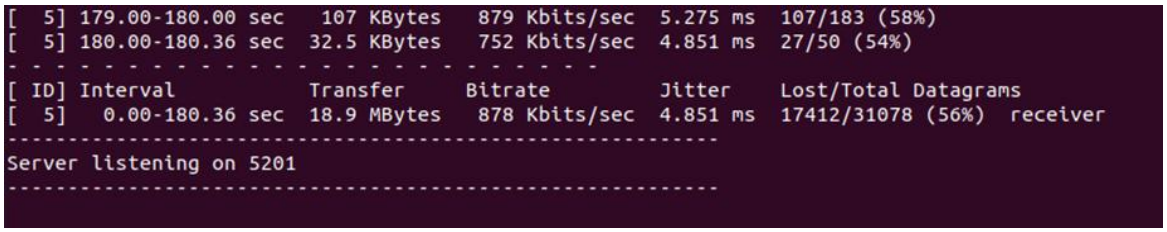
$$P_{iPerf3} = \frac{N_{esp} - N_{obs}}{N_{esp}} \times 100$$

4.4.3 Resultados sin QoS

Con las políticas de priorización deshabilitadas, el VoD y el tráfico iPerf3 compitieron por el enlace sin diferenciación de servicio. El receptor de iPerf3 informó 878 kbit/s para el conjunto de la ejecución, un jitter de 4,851 ms y una pérdida de 17412 datagramas de 31078, equivalente al 56 %. Estos valores pertenecen únicamente al flujo de saturación y se utilizan como evidencia de la congestión; no representan la pérdida del servicio VoD. En la **Figura 53** se presenta el resultado mostrado por iPerf3 durante la prueba de VoD en Sin QoS.

Figura 53

Resultado mostrado por iPerf3 durante la prueba de VoD en Sin QoS.



4.4.3.1 Ancho de Banda (AB)

Dentro de la ventana efectiva, el VoD presentó un ancho de banda promedio de 123,78 kbit/s y el tráfico iPerf3 874,38 kbit/s. La ocupación conjunta fue de 998,16 kbit/s, valor muy próximo al límite de 1 Mbit/s. El resultado muestra que, sin priorización, la mayor parte del recurso fue utilizada por la carga UDP de fondo y el servicio HTTP obtuvo una porción reducida del enlace, como se puede observar en la **Figura 54**.

Ecuación 52.
Cálculo del ancho de banda promedio del VOD en Sin QoS

$$BW_{VoD} = \frac{2011482 \times 8}{130 \times 1000} = 123{,}78\, kbit/s$$

Ecuación 53.
Cálculo del ancho de banda promedio de iPerf3 en Sin QoS

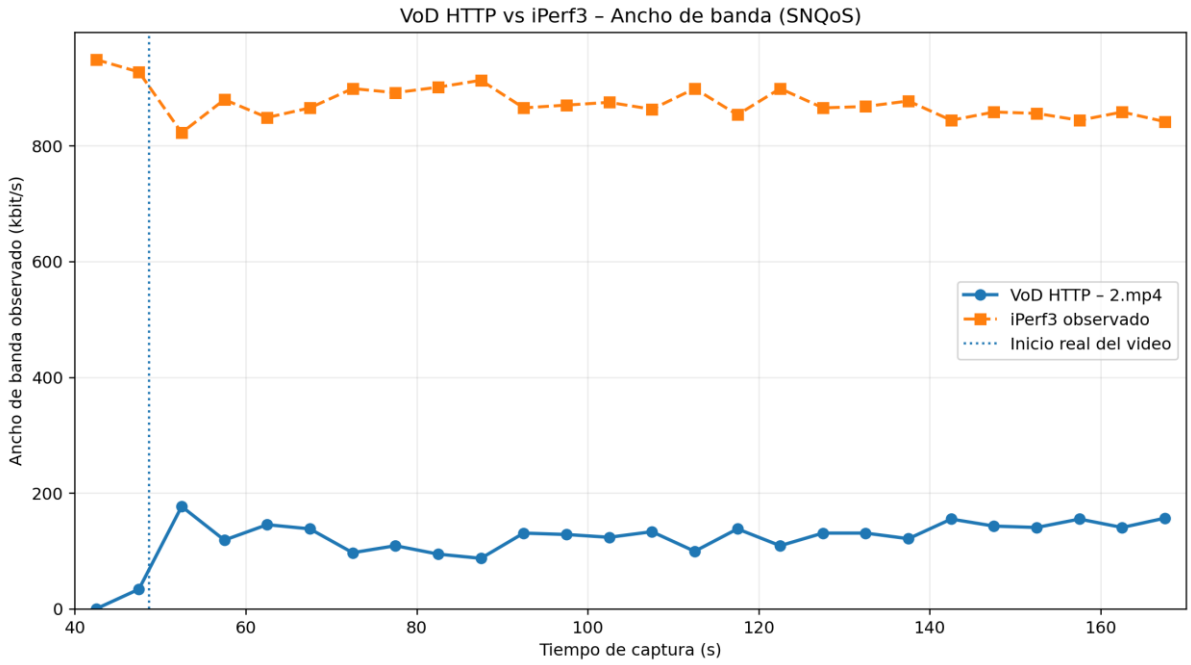
$$BW_{iPerf3} = \frac{14208640 \times 8}{130 \times 1000} = 874{,}38\, kbit/s$$

Ecuación 54.
Ocupación conjunta observada en Sin QoS

$$BW_{total} = 123{,}78 + 874{,}38 = 998{,}16\, kbit/s$$

Figura 54

Ancho de banda del VoD frente a la carga iPerf3 durante Sin QoS.



4.4.3.2 Tiempo de ida vuelta (RTT)

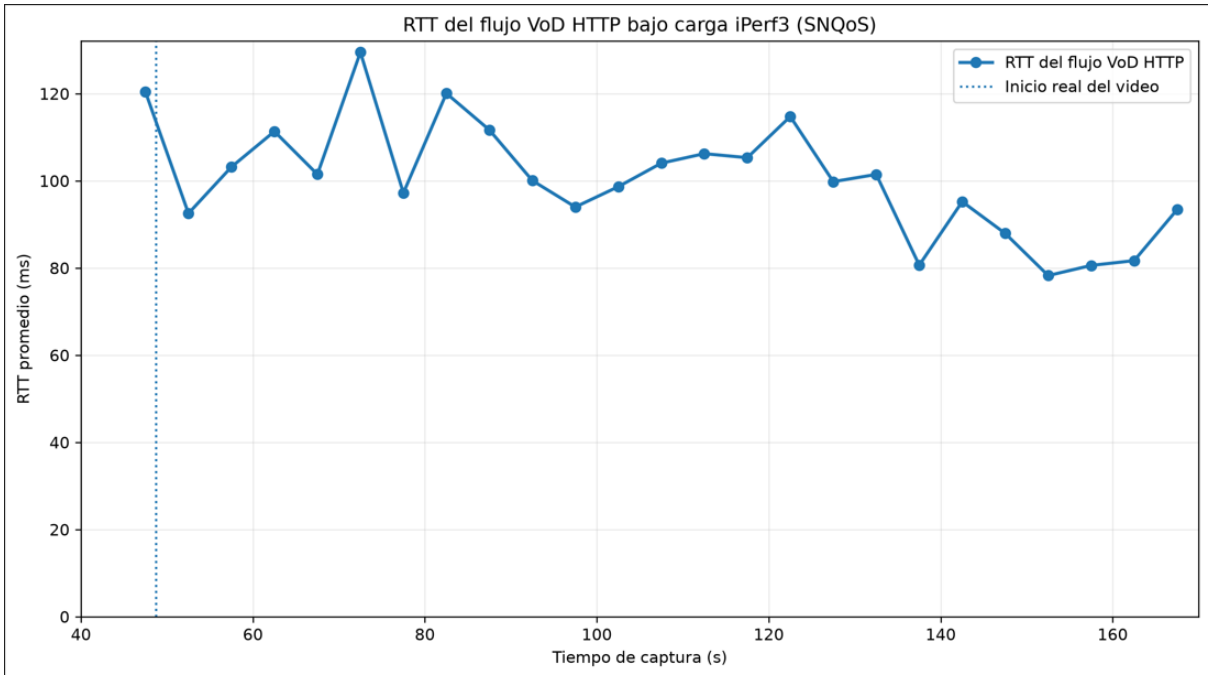
El RTT promedio del flujo MP4 fue de 98,28 ms. La serie temporal presentó valores notablemente superiores a los obtenidos con QoS y varios incrementos durante la congestión. El comportamiento evidencia el efecto de la competencia por el enlace cuando el tráfico no dispone de priorización. En la **Figura 55** se presenta el RTT del VoD HTTP frente a la carga iPerf3 durante Sin QoS.

Ecuación 55.
RTT promedio obtenido para el flujo VoD en Sin QoS

$$RTT_{promSNQoS} = 98{,}28ms$$

Figura 55

RTT del VoD HTTP frente a la carga iPerf3 durante Sin QoS



4.4.3.3 Variación del RTT (indicador de Jitter TCP)

La variación promedio entre muestras consecutivas de RTT fue de 53,52 ms. La figura incorpora también el jitter UDP de iPerf3 como referencia del tráfico de saturación. Ambas series se expresan en milisegundos, pero deben interpretarse de acuerdo con su protocolo: para VoD se representa la variación del RTT TCP, mientras que iPerf3 utiliza su indicador de jitter UDP. En la **Figura 56** se presenta la variabilidad temporal del flujo VoD HTTP e iPerf3 durante Sin QoS.

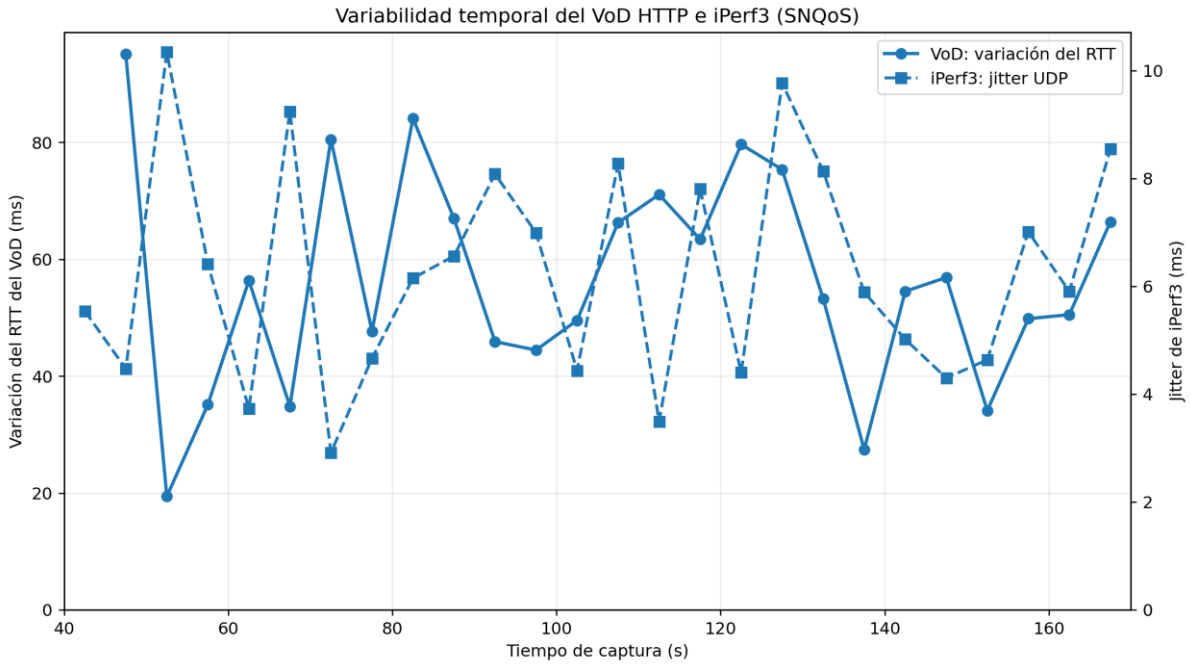
Ecuación 56.

Variación promedio del RTT del VOD en Sin QOS

$$J_{promSNQoS} = 53{,}52ms$$

Figura 56

Variabilidad temporal del flujo VoD HTTP e iPerf3 durante Sin QoS



4.4.3.4 Indicador de pérdida TCP

En las conexiones correspondientes se analizaron 1295 segmentos TCP con datos y se identificaron 101 eventos de discontinuidad de secuencia. El indicador resultante fue de 7,80 %. La pérdida estimada de iPerf3 dentro de la ventana de análisis se situó alrededor del 57,5 % en promedio, valor cercano al 56 % reportado por iPerf3 al finalizar la ejecución completa. En la **Figura 57** se presenta el indicador de pérdida del VoD y pérdida estimada de iPerf3 durante Sin QoS.

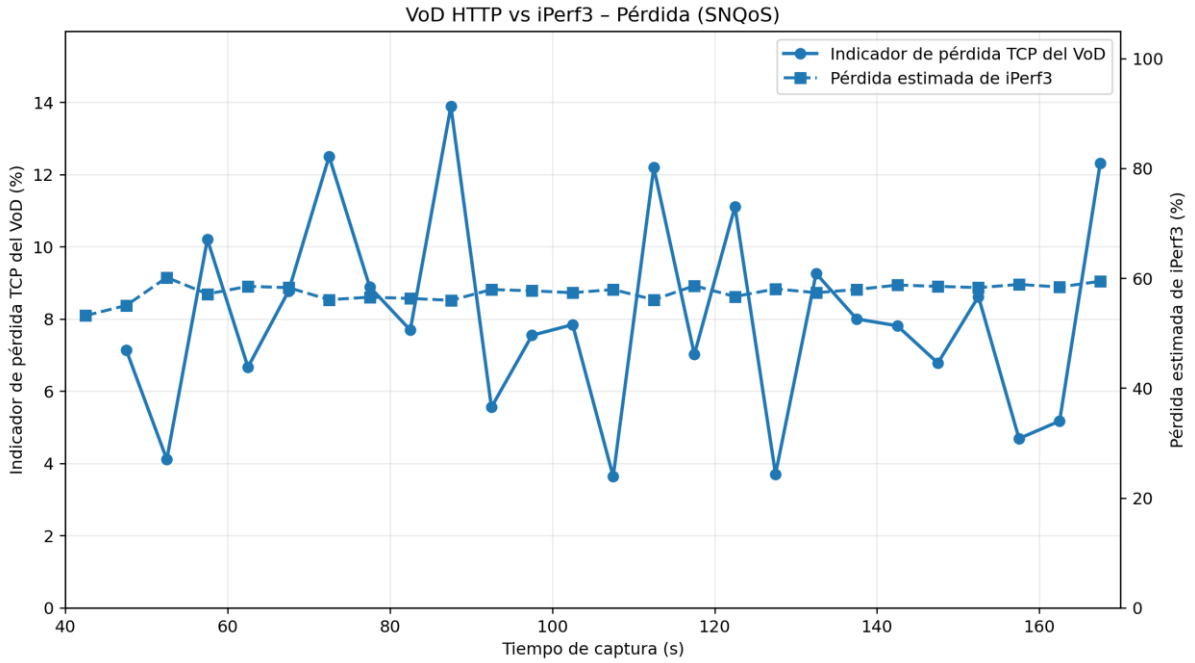
Ecuación 57.

Indicador de pérdida TCP del flujo VoD en Sin QoS

$$I_{pérdidaTCP} = \frac{101}{1295} \times 100 = 7{,}80\%$$

Figura 57

Indicador de pérdida del VoD y pérdida estimada de iPerf3 durante Sin QoS.

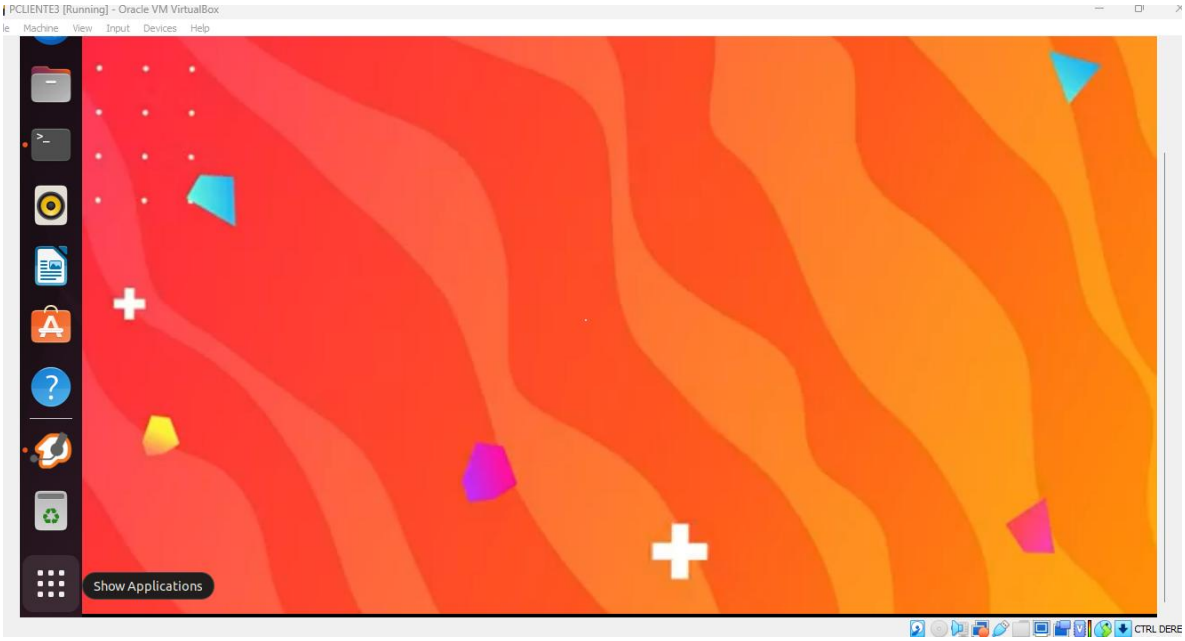


4.4.3.5 Observación de la reproducción

Durante la prueba sin QoS se observó un mayor tiempo de espera para disponer del contenido y periodos de carga antes de la reproducción. Esta evidencia se utiliza únicamente como referencia cualitativa del comportamiento de la aplicación bajo congestión; la evaluación cuantitativa se sustenta en las métricas extraídas del flujo real del archivo MP4. En la **Figura 58** se presenta el retraso en el inicio y carga del contenido VoD durante la prueba sin QoS.

Figura 58

Retraso en el inicio y carga del contenido VoD durante la prueba sin QoS



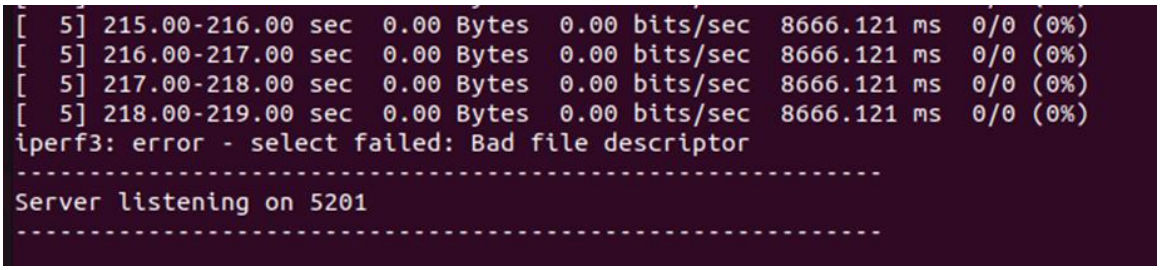
4.4.4 Resultados con QoS

Para el escenario QoS se mantuvieron las mismas condiciones de carga y medición, activando únicamente las reglas de clasificación, marcado y priorización. La captura del control de iPerf3 registra una sesión UDP configurada a 2 Mbit/s durante 180 s; por tanto, la reducción del tráfico iPerf3 observado después del cuello de botella no se interpreta como una tasa configurada en cero, sino como el resultado del tratamiento aplicado al tráfico de fondo en el punto de medición.

Las estadísticas de Queue Tree mostraron que la clase Streaming VoD, asociada a vod-pkt, mantenía una tasa instantánea cercana a 902 kbit/s, mientras que la clase iPerf Background acumulaba 12 197 descartes. Estos valores son instantáneos o acumulativos y no sustituyen las métricas calculadas sobre la captura, pero constituyen evidencia adicional de que la política favoreció el servicio VoD y trasladó una mayor proporción de la afectación hacia el tráfico de saturación. En la **Figura 59** se presenta los intervalos sin recepción de tráfico iPerf3 observados durante la prueba de VoD con QoS.

Figura 59

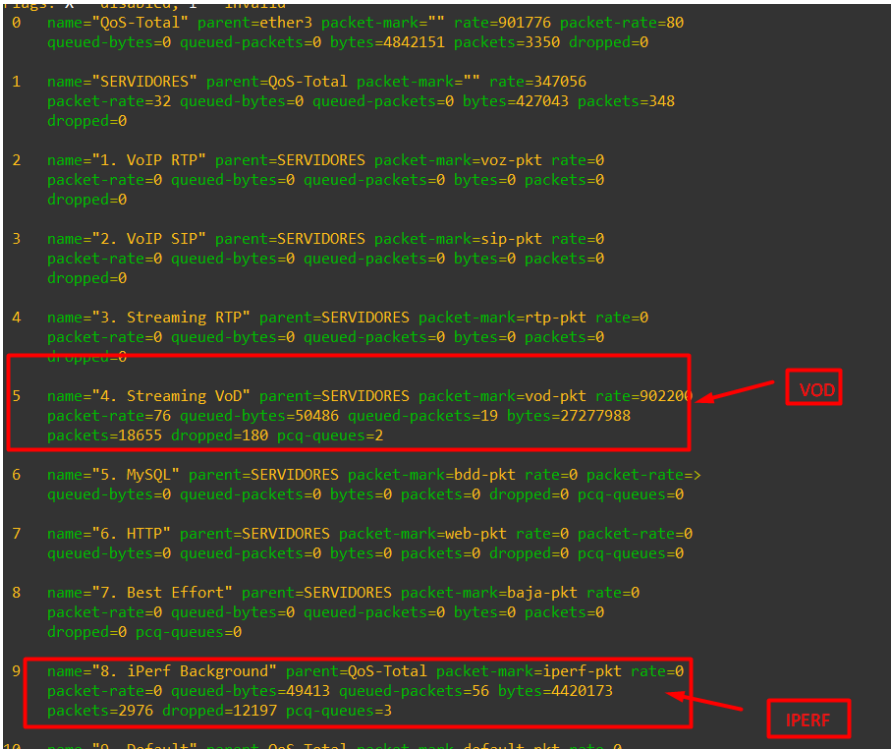
Intervalos sin recepción de tráfico iPerf3 observados durante la prueba de VoD con QoS



Antes de interpretar las métricas se verificó el comportamiento de Queue Tree. La cola Streaming VoD registró una tasa instantánea cercana a 902200 bit/s y 180 descartes acumulados, mientras que iPerf Background presentó una tasa instantánea de 0 bit/s y 12197 descartes acumulados. Los contadores son acumulativos y se emplean únicamente como evidencia de la acción de la política; no sustituyen el cálculo realizado sobre la captura. En la **Figura 60** se presenta las estadísticas de Queue Tree durante la prueba de VoD con QoS.

Figura 60

Estadísticas de Queue Tree durante la prueba de VoD con QoS



4.4.4.1 Ancho de Banda (AB)

Con QoS, el VoD alcanzó un ancho de banda promedio de 902,87 kbit/s, mientras que iPerf3 presentó 14,85 kbit/s dentro de la misma ventana. La ocupación conjunta observada fue de 917,72 kbit/s. El cambio respecto de Sin QoS evidencia que la política no incrementa la capacidad física del enlace, sino que redistribuye el recurso disponible a favor del tráfico priorizado. En la **Figura 61** se presenta el ancho de banda del VoD frente a la carga iPerf3 durante QoS.

Ecuación 58.
Cálculo del ancho de banda promedio del VOD con QoS

$$BW_{VoD} = \frac{14671630 \times 8}{130 \times 1000} = 902{,}87\ kbit/s$$

Ecuación 59.
Cálculo del ancho de banda promedio de iPerf3 con QoS

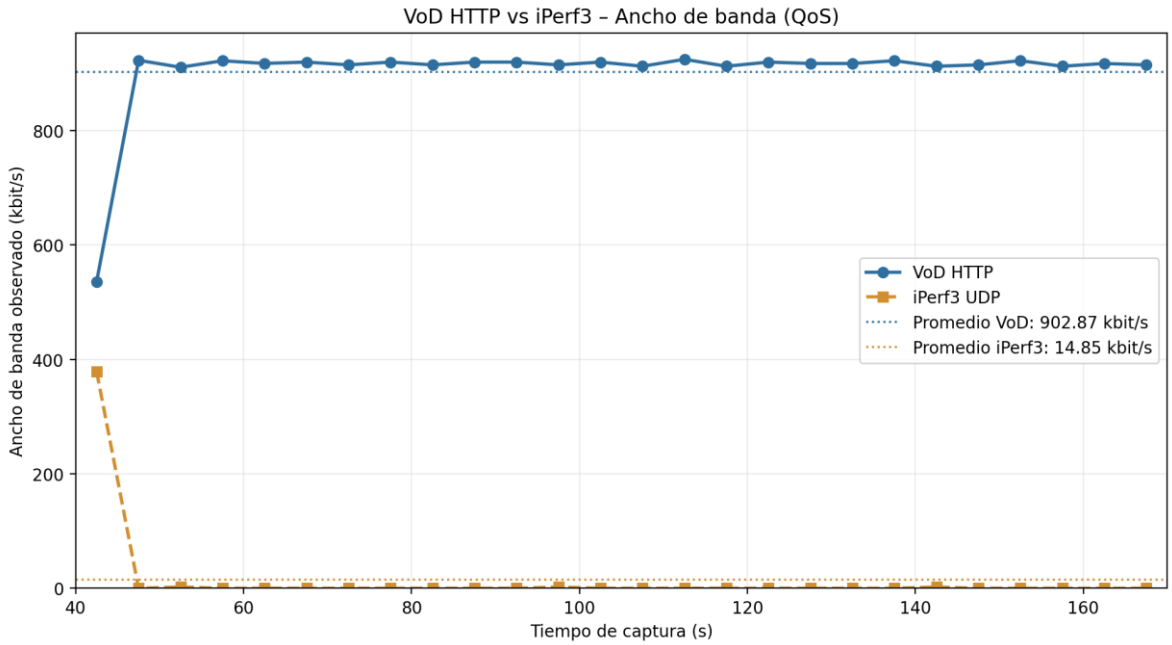
$$BW_{iPerf3} = \frac{241380 \times 8}{130 \times 1000} = 14{,}85\ kbit/s$$

Ecuación 60.
Ocupación conjunta observada en QoS

$$BW_{total} = 902{,}87 + 14{,}85 = 917{,}72\ kbit/s$$

Figura 61

Ancho de banda del VoD frente a la carga iPerf3 durante QoS



4.4.4.2 Tiempo de ida vuelta (RTT)

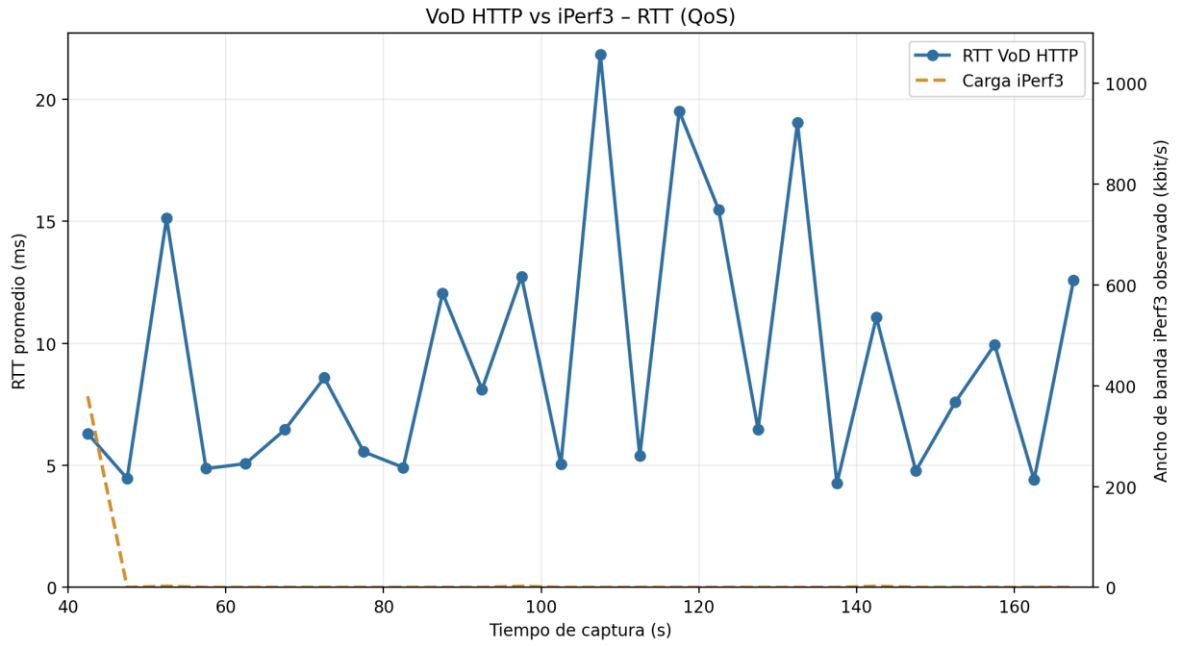
El RTT promedio disminuyó a 8,92 ms y la mediana a 4,01 ms. El máximo registrado fue de 487,75 ms. La reducción del valor promedio indica que los segmentos del VoD recibieron un tratamiento más favorable durante la congestión, disminuyendo el tiempo requerido para sus reconocimientos TCP. En la **Figura 62** se presenta el RTT del VoD HTTP frente a la carga iPerf3 durante QoS.

Ecuación 61.
RTT promedio obtenido con QoS.

$$RTT_{prom} = 8{,}92ms$$

Figura 62

RTT del VoD HTTP frente a la carga iPerf3 durante QoS



4.4.4.3 Variación del RTT (indicador de Jitter TCP)

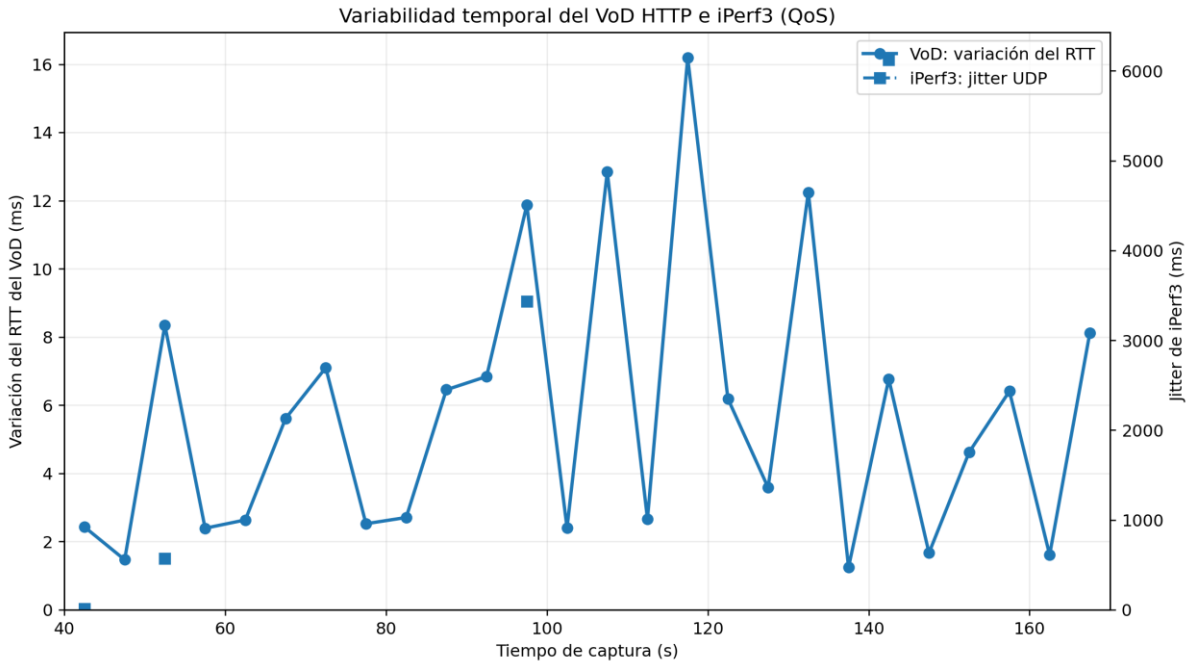
La variación promedio del RTT del VoD se redujo a 5,40 ms. En la misma figura se muestra el jitter de los datagramas iPerf3 que alcanzaron el punto de captura. Debido a los fuertes descartes aplicados al tráfico de fondo, iPerf3 presenta muestras escasas y valores de jitter mucho mayores; por esta razón se emplean escalas independientes y la serie se interpreta únicamente como referencia de la degradación del tráfico de saturación. En la **Figura 63** se presenta la variación del RTT del VoD HTTP frente a la carga iPerf3 durante QoS.

Ecuación 62.
Variación promedio del RTT del VoD con QoS

$$J_{prom} = 22{,}52ms$$

Figura 63

Variación del RTT del VoD HTTP frente a la carga iPerf3 durante QoS.



4.4.4.4 Indicador de pérdida TCP

En la ventana efectiva de análisis se identificaron 9665 segmentos TCP con datos correspondientes al flujo real del contenido VoD y 94 eventos de discontinuidad de secuencia. A partir de estos valores se obtuvo un indicador de pérdida TCP de 0,97 %. Este porcentaje resulta considerablemente menor que el registrado en el escenario Sin QoS, lo que evidencia una reducción de las discontinuidades observadas en el flujo VoD cuando se aplicó la política de priorización. De manera complementaria, las estadísticas de Queue Tree mostraron una mayor acumulación de descartes en la clase destinada al tráfico iPerf3, indicando que, bajo congestión, una mayor proporción de la afectación fue absorbida por el tráfico de fondo. En la **Figura 64** se presenta el indicador de pérdida del VoD y pérdida estimada de iPerf3 durante QoS.

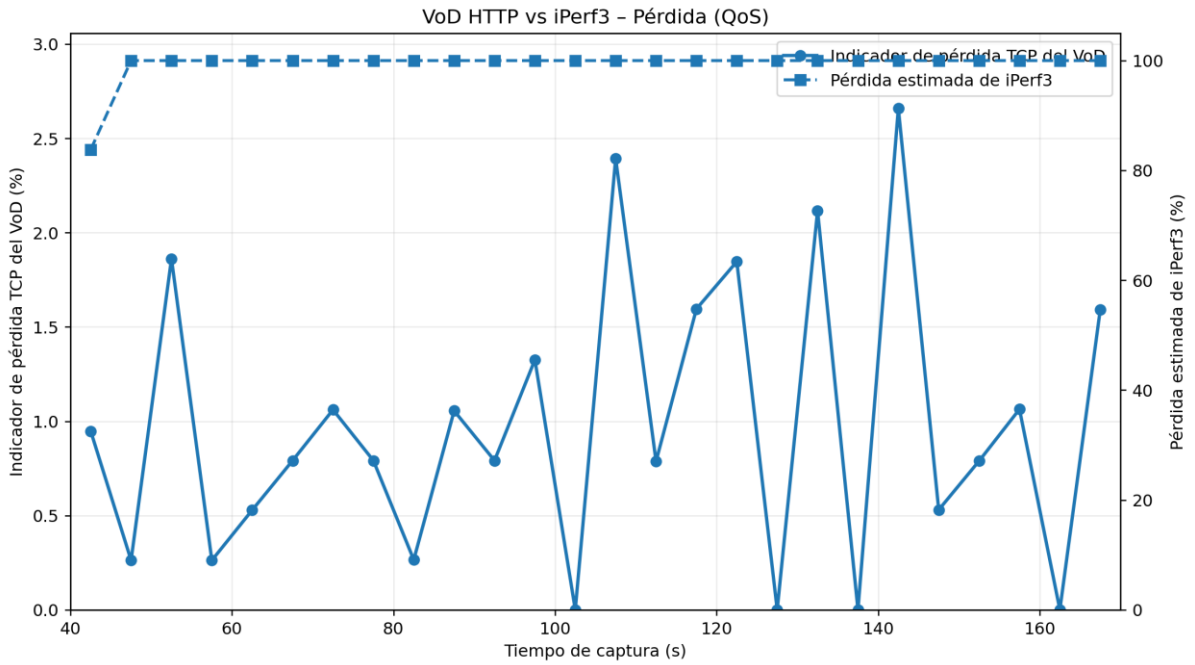
Ecuación 63.

Indicador de pérdida TCP del flujo VoD con QoS

$$P_{loss} = \frac{94}{9772} \times 100 = 0{,}97\%$$

Figura 64

Indicador de pérdida del VoD y pérdida estimada de iPerf3 durante QoS



4.4.4.5 Observación de la reproducción

La activación de QoS modificó claramente la distribución del recurso disponible. El VoD alcanzó una tasa cercana a la capacidad del enlace y presentó reducciones importantes en RTT, variación temporal e indicaciones de discontinuidad TCP. Paralelamente, el tráfico iPerf3 quedó fuertemente degradado en el punto de captura, comportamiento consistente con los descartes registrados en Queue Tree. La disminución del throughput iPerf3 observado no debe interpretarse como una desaparición de la carga configurada, sino como evidencia del tratamiento recibido por el tráfico de fondo después de la priorización.

4.5 FTP vs iPerf3

La evaluación del servicio FTP se organizó bajo el mismo esquema utilizado en las pruebas de Streaming y VoD. Se analizaron los escenarios Sin QoS y con QoS, manteniendo la misma topología, el enlace de 1 Mbit/s, la carga UDP de iPerf3 de 2 Mbit/s, la duración nominal

de 180 s y la ventana efectiva de análisis comprendida entre los segundos 40 y 170. La diferencia entre ambos escenarios correspondió únicamente a la activación de las reglas de clasificación, marcado y Queue Tree.

4.5.1 Condiciones comunes de prueba

El servicio FTP operó desde el servidor 172.16.6.2 hacia el cliente 172.16.1.2. La conexión de control se estableció mediante TCP en el puerto 21 y la descarga se realizó con FileZilla en modo pasivo. En este modo, el contenido del archivo no se transporta por el canal de control, sino por una conexión TCP de datos asociada a un puerto dinámico anunciado mediante PASV. Por esta razón, las métricas se calcularon sobre el flujo TCP que transportó realmente el archivo prueba_ftp_1GB.bin y no únicamente sobre los paquetes identificados como FTP en el puerto 21.

En las capturas utilizadas, el puerto pasivo asociado a la transferencia fue 44042 para Sin QoS y 24170 para QoS. La carga de congestión se generó desde Kali, con dirección 172.16.4.3, hacia 172.16.1.2 mediante iPerf3 en modo UDP por el puerto 5201. Tanto la transferencia FTP como el tráfico de saturación atravesaron el cuello de botella R5-R1 y fueron observados desde el mismo punto de captura en el enlace R1-R2, manteniendo así una condición de medición equivalente para Sin QoS y QoS.

Ecuación 64.
Factor de carga respecto de la capacidad del enlace.

$$F_s = \frac{2\,Mbit/s}{1\,Mbit/s} = 2$$

La captura se mantuvo durante 180 s. Los primeros 20 s se destinaron al establecimiento de la carga de congestión y, posteriormente, se inició la transferencia FTP. Para el procesamiento cuantitativo se utilizó el intervalo de 40 a 170 s, equivalente a 130 s de medición.

Para identificar el servicio se utilizó el canal FTP de control como referencia, especialmente los mensajes PASV y RETR. Una vez identificado el puerto pasivo asignado a la descarga, el cálculo se realizó únicamente sobre la conexión TCP de datos del archivo. Esta separación evita interpretar los pocos paquetes de control FTP como si representaran el volumen total de la transferencia.

```
ftp || tcp.port == 21

RETR prueba_ftp_1GB.bin

tcp.port == <puerto_pasivo_detectado> && frame.time_relative >=
40 && frame.time_relative <= 170

udp && ip.src == 172.16.4.3 && ip.dst == 172.16.1.2 &&
udp.dstport == 5201 && frame.time_relative >= 40 &&
frame.time_relative <= 170
```

4.5.2 Criterios de cálculo

El ancho de banda observado se calculó a partir de la longitud de las tramas capturadas. En cada intervalo de 5 s se sumaron los bytes correspondientes al flujo TCP de datos FTP y al flujo UDP de iPerf3, expresando el resultado en kbit/s. Ambas series pueden representarse en la misma figura porque corresponden a tasa de transferencia observada en el mismo punto de la red.

Para TCP se estimó el RTT relacionando los segmentos de datos enviados por el servidor FTP con los ACK acumulativos devueltos por el cliente dentro de la misma conexión de datos. El valor de cada intervalo corresponde al promedio de las muestras disponibles. Debido a que la captura se efectuó en R1-R2, el resultado se interpreta como RTT TCP observado en el punto de medición y no como una medición unidireccional extremo a extremo.

Ecuación 65.
Ancho de banda observado en cada intervalo

$$BW_i = \frac{\Sigma L_j \times 8}{\Delta t \times 1000}[kbit/s]$$

Ecuación 66.
RTT promedio del flujo TCP de datos FTP

$$RTT_{prom} = \frac{\Sigma RTT_i}{N}$$

TCP no dispone de un jitter nativo equivalente al de RTP. Por ello, la estabilidad temporal del FTP se representó mediante la variación absoluta entre muestras consecutivas de RTT. Este indicador se denomina variación del RTT y no debe interpretarse como jitter RTP.

Ecuación 67.
Variación entre muestras consecutivas de RTT

$$\Delta RTT_i = RTT_i - RTT_{i-1}$$

Ecuación 68.
Variación promedio del RTT del flujo FTP

$$J_{prom} = \frac{\Sigma J_i}{N-1}$$

La afectación del flujo FTP se expresó mediante un indicador de discontinuidad de secuencia TCP. Para ello se contabilizaron los saltos hacia adelante observados en los números de secuencia de los segmentos que contenían datos del archivo y se dividieron para el total de segmentos TCP con datos. Este valor no corresponde al IPLR de capa IP y se utiliza únicamente como indicador comparable entre los dos escenarios.

Ecuación 69.
Indicador de pérdida TCP del flujo FTP

$$I_{pérdidaTCP} = \frac{N_{discontinuidades}}{N_{segmentosdedatos}} \times 100$$

Para iPerf3, la pérdida se estimó respecto de la carga UDP configurada. Con una tasa de 2 Mbit/s y datagramas de 1448 bytes, se determinó el número esperado de datagramas por

intervalo y se comparó con los datagramas observados en el punto de captura. El resultado de iPerf3 se utiliza como referencia de la congestión y no como métrica principal del servicio FTP.

Ecuación 70.
Número esperado de datagramas iPerf3 por intervalo

$$N_{esp} = \frac{B_{ofrecido}}{L_{UDP} \times 8} \times \Delta t$$

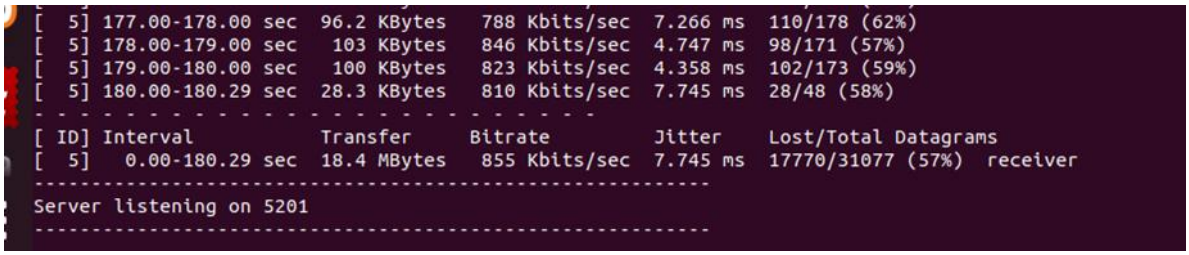
Ecuación 71.
Pérdida estimada del tráfico iPerf3 en el punto de captura

$$P_{iPerf3} = \frac{N_{esp} - N_{obs}}{N_{esp}} \times 100$$

4.5.3 Resultados sin QoS

Con las políticas de priorización deshabilitadas, el flujo de datos FTP y la carga UDP de iPerf3 compitieron por la capacidad disponible sin diferenciación de servicio. En la terminal del receptor, iPerf3 reportó aproximadamente 855 kbit/s para la ejecución completa, un jitter de 7,745 ms y una pérdida de 17770 datagramas de 31077, equivalente al 57 %. Estos valores corresponden únicamente al tráfico de saturación y se conservan como evidencia de la condición de congestión. En la **Figura 65** se presenta el resultado mostrado por iPerf3 durante la prueba FTP en Sin QoS.

Figura 65
Resultado mostrado por iPerf3 durante la prueba FTP en Sin QoS



4.5.3.1 Ancho de Banda (AB)

Dentro de la ventana efectiva, el flujo TCP de datos FTP presentó un ancho de banda promedio de 149,44 kbit/s, mientras que iPerf3 alcanzó 844,76 kbit/s. La ocupación conjunta fue de 994,20 kbit/s, valor muy próximo a la capacidad nominal de 1 Mbit/s. El resultado muestra que, sin priorización, la mayor parte del recurso observado fue utilizada por la carga UDP de fondo, mientras la transferencia FTP conservó una porción reducida del enlace, como se muestra en la **Figura 66**.

Ecuación 72.
Cálculo del ancho de banda promedio del FTP en Sin QoS

$$BW_{VoD} = 149{,}44\, kbits/s$$

Ecuación 73.
Cálculo del ancho de banda promedio de iPerf3 en Sin QoS

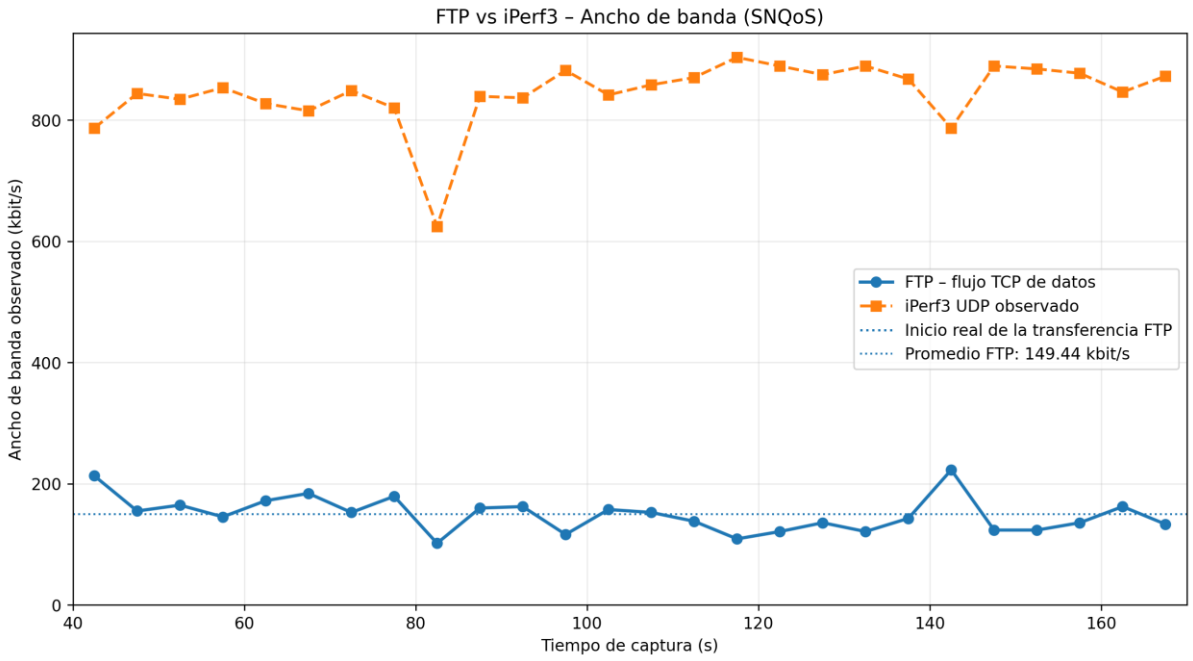
$$BW_{iPerf3} = 844{,}76 kbits$$

Ecuación 74.
Ocupación conjunta observada en Sin QoS

$$BW_{total} = 149{,}44 + 844{,}76 = 994{,}20\, kbit/s$$

Figura 66

Ancho de banda del FTP frente a la carga iPerf3 durante Sin QoS.



4.5.3.2 Tiempo de ida y vuelta (RTT)

El RTT promedio observado para la conexión TCP de datos FTP fue de 38,56 ms. La serie temporal presentó oscilaciones asociadas a la competencia por el enlace, evidenciando un mayor tiempo entre la salida de segmentos de datos y la recepción de sus reconocimientos TCP en el punto de medición, como se observa en la imagen.

Ecuación 75.

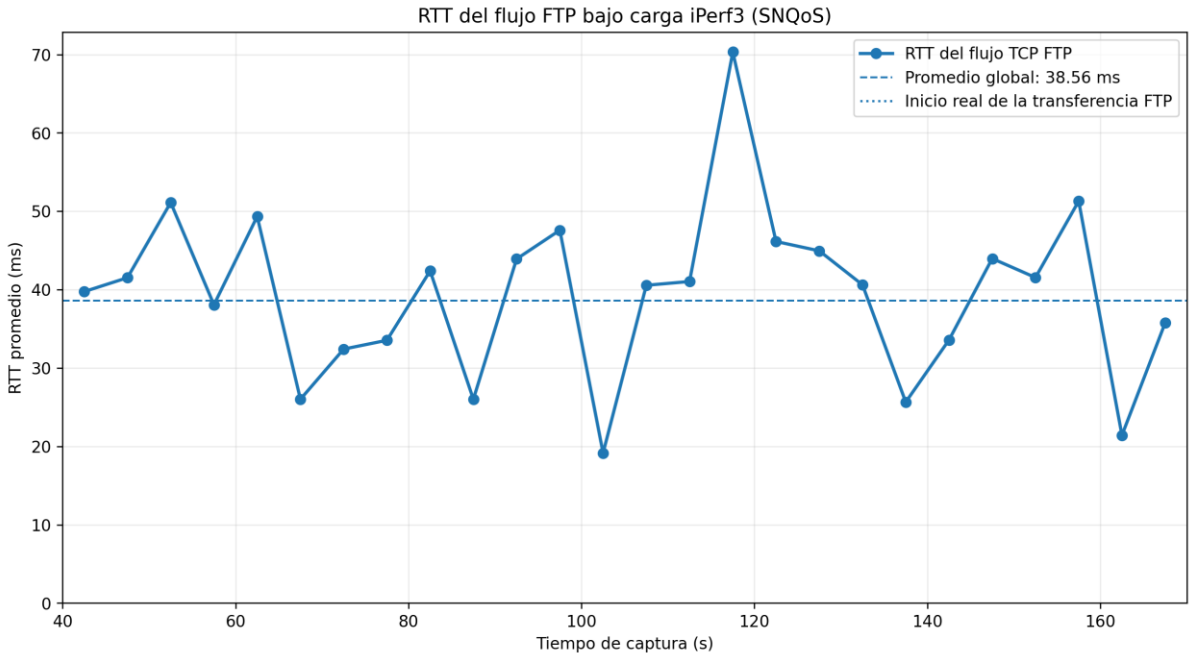
RTT promedio del flujo FTP en Sin QoS.

$$RTT_{prom} = 38{,}56ms$$

En la **Figura 67** se presenta el RTT del flujo TCP FTP bajo carga iPerf3 durante Sin QoS.

Figura 67

RTT del flujo TCP FTP bajo carga iPerf3 durante Sin QoS



4.5.3.3 Variación del RTT (indicador temporal TCP)

La variación promedio entre muestras consecutivas de RTT fue de 57,84 ms. Este valor refleja una alta variabilidad temporal del flujo TCP durante la congestión. A diferencia de

Streaming RTP, esta métrica no corresponde a jitter nativo del protocolo, sino a la diferencia absoluta entre RTT consecutivos, como se muestra a continuación y la **Figura 68**.

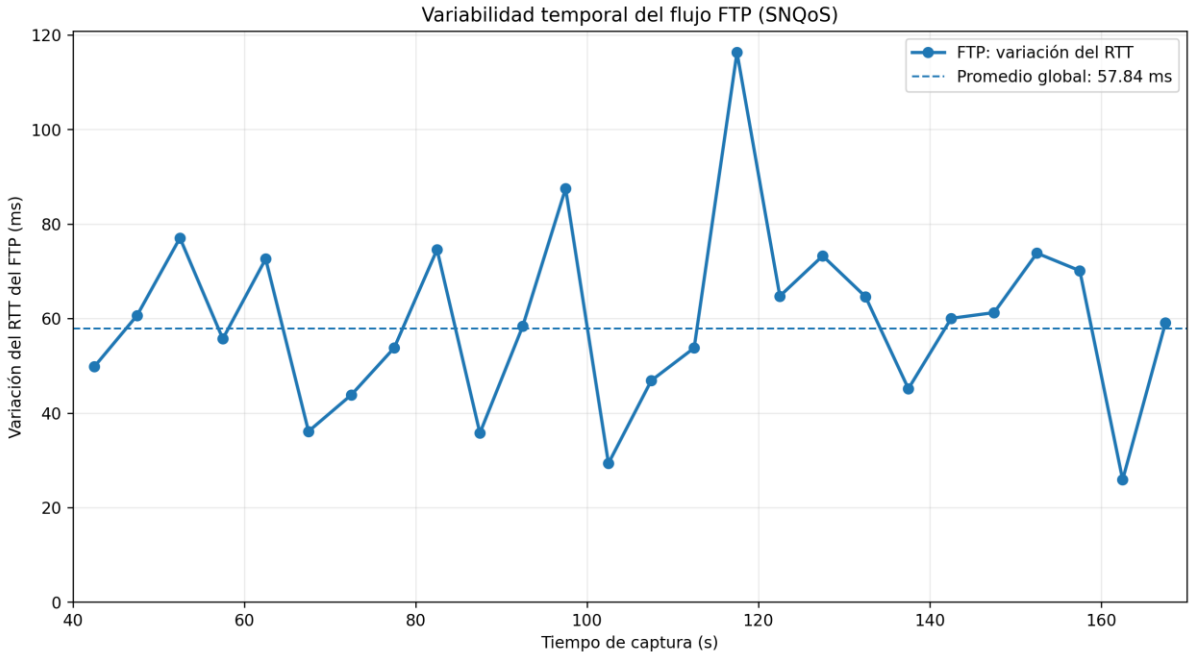
Ecuación 76.

Variación promedio del RTT del FTP en Sin QoS

$$J_{prom} = 57{,}84ms$$

Figura 68

Variación del RTT del flujo FTP durante Sin QoS



4.5.3.4 Indicador de pérdida TCP

En la ventana efectiva se analizaron 1604 segmentos TCP con datos correspondientes a la transferencia del archivo y se identificaron 118 eventos de discontinuidad de secuencia. El indicador resultante fue de 7,36 %. De manera complementaria, la pérdida estimada del tráfico iPerf3 dentro de la ventana fue de 58,73 %, valor coherente con la pérdida del 57 % reportada por la terminal para la ejecución completa.

Ecuación 77.

Indicador de pérdida TCP del FTP en Sin QoS.

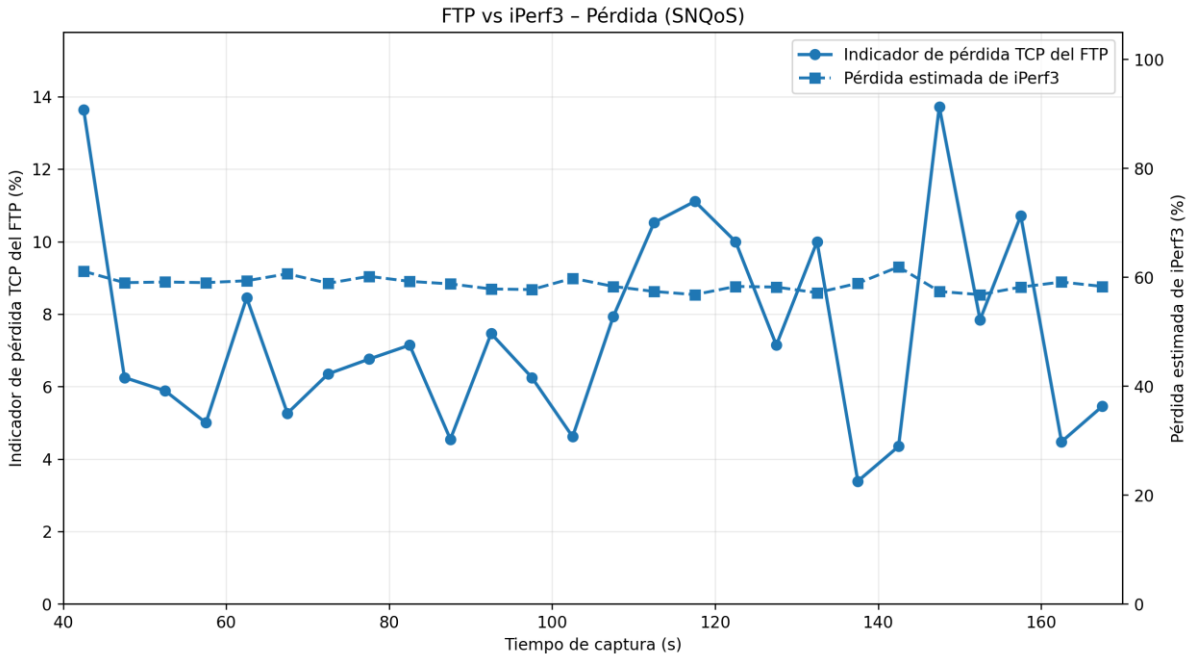
$$I_{TCP} = \left(\frac{118}{1604}\right) x100$$

$$I_{TCP} = 7{,}36\%$$

En la **Figura 69** se presenta el indicador de pérdida TCP del FTP y pérdida estimada de iPerf3 durante Sin QoS.

Figura 69

Indicador de pérdida TCP del FTP y pérdida estimada de iPerf3 durante Sin QoS.

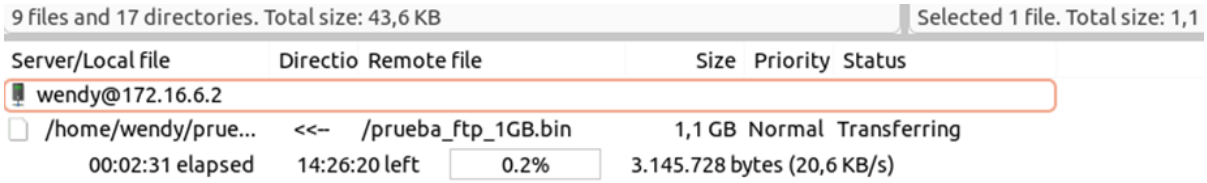


4.5.3.5 Observación de la transferencia TCP

Durante la prueba Sin QoS, FileZilla mantuvo activa la descarga del archivo de 1 GiB. En la evidencia visual se observa una tasa instantánea de aproximadamente 20,6 KB/s en el momento de la captura. Este valor se emplea solo como referencia cualitativa de la aplicación y no sustituye el promedio calculado desde Wireshark entre 40 y 170 s, como se muestra en la **Figura 70**.

Figura 70

Transferencia del archivo FTP observada en FileZilla durante Sin QoS.

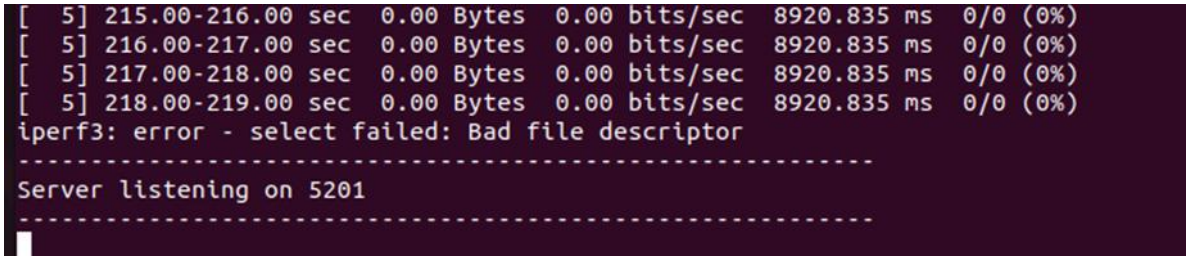


4.5.4 Resultados con QoS

La captura de la terminal de iPerf3 correspondiente al final de la sesión muestra intervalos posteriores con 0 bit/s y el mensaje “Bad file descriptor”. Debido a que los tiempos visibles superan los 180 s de la prueba, esta evidencia no se utilizó para calcular la tasa ni la pérdida dentro de la ventana 40-170 s. Los valores cuantitativos de iPerf3 empleados en los resultados se obtuvieron directamente de la captura de red. En la **Figura 71** se presenta el estado de iPerf3 posterior a la ventana de medición durante el escenario QoS.

Figura 71

Estado de iPerf3 posterior a la ventana de medición durante el escenario QoS



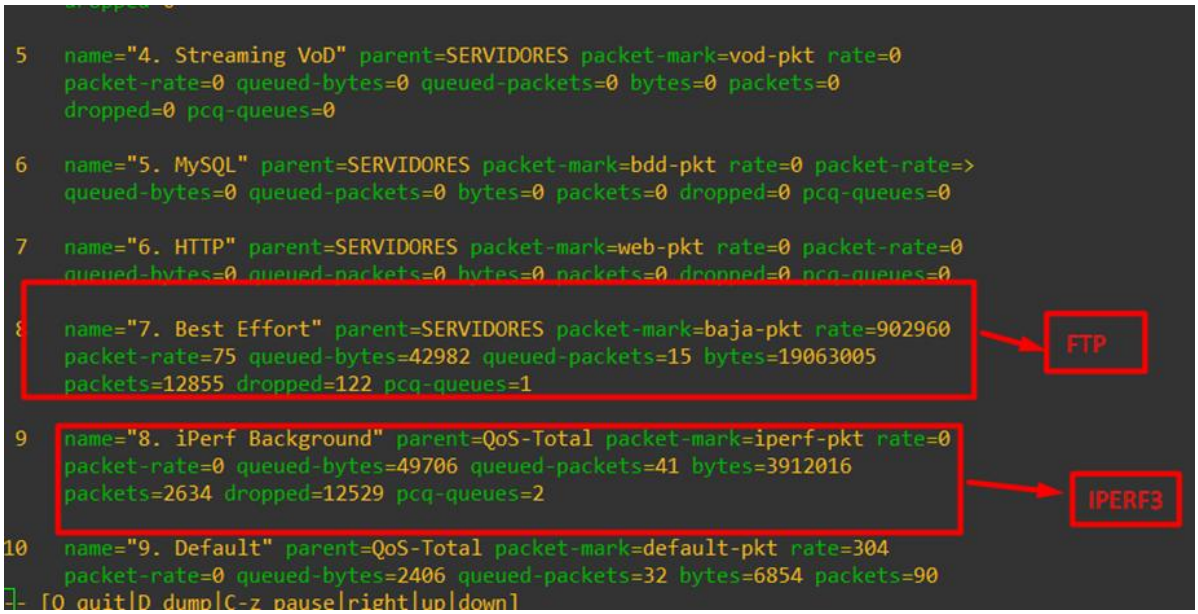
Para el escenario QoS se mantuvieron las mismas condiciones de servicio, carga y medición, activando únicamente las reglas de clasificación, marcado y Queue Tree. La transferencia FTP fue asociada a la clase Best Effort mediante baja-pkt, mientras que iPerf3 fue clasificado como tráfico de fondo mediante iperf-pkt. Aunque FTP ocupó una prioridad inferior a los servicios multimedia, su clase se encontraba por encima de iPerf Background, por

lo que durante esta prueba individual el tráfico artificial de saturación cedió recursos frente al FTP.

Las estadísticas de Queue Tree registraron una tasa instantánea de aproximadamente 902960 bit/s en la clase 7, como se muestra en la **Figura 72**. Best Effort, asociada al tráfico FTP, mientras que iPerf Background presentaba una tasa instantánea de 0 bit/s. Los contadores acumulativos mostraron 122 descartes en Best Effort y 12529 descartes en iPerf Background. Estos valores se utilizan como evidencia operativa del tratamiento de las colas y no sustituyen las métricas obtenidas desde la captura de Wireshark.

Figura 72

Estadísticas de Queue Tree durante la prueba FTP con QoS.



4.5.4.1 Ancho de Banda (AB)

Con QoS, el flujo FTP alcanzó un ancho de banda promedio de 897,97 kbit/s, mientras que iPerf3 presentó 21,82 kbit/s dentro de la misma ventana. La ocupación conjunta observada fue de 919,79 kbit/s. El cambio respecto de Sin QoS no representa un aumento de la capacidad física del enlace; corresponde a una redistribución del recurso disponible en la que el tráfico de

fondo fue afectado con mayor intensidad y la transferencia FTP conservó una proporción superior del ancho de banda, como se muestra en la **Figura 73**.

Ecuación 78.

Cálculo del ancho de banda promedio del FTP con QoS

$$BW_{FTP} = 897{,}97\ kbit/s$$

Ecuación 79.

Cálculo del ancho de banda promedio de iPerf3 con QoS

$$BW_{iPerf3} = 21{,}82\ kbit/s$$

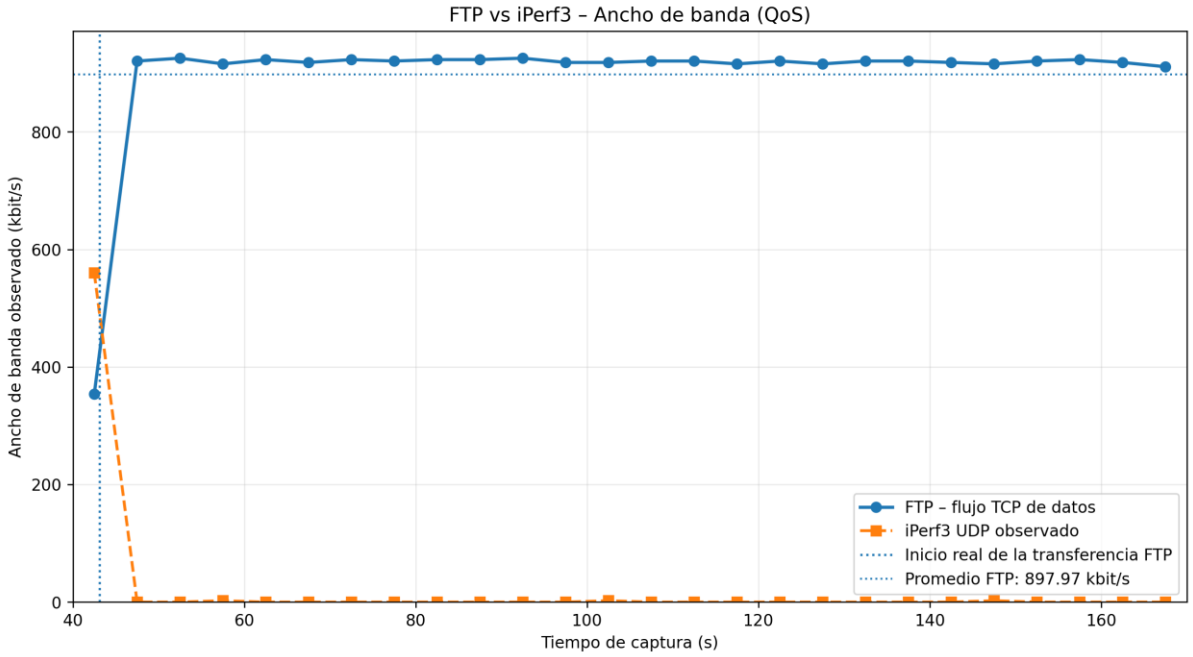
Ecuación 80.

Ocupación conjunta observada con QoS

$$BW_{total} = 897{,}97 + 21{,}82 = 919{,}79\ kbit/s$$

Figura 73

Ancho de banda del FTP frente a la carga iPerf3 durante QoS



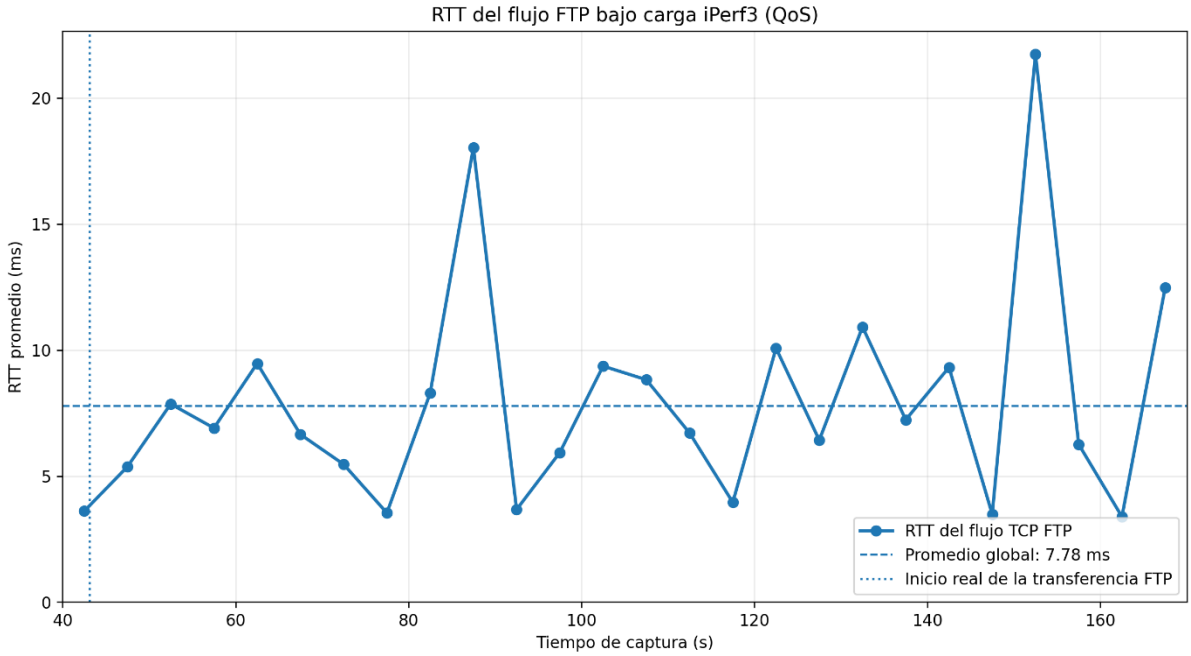
4.5.4.2 Tiempo de ida y vuelta (RTT)

El RTT promedio del flujo FTP disminuyó a 7,78 ms. La reducción observada indica que los segmentos TCP de la transferencia recibieron reconocimientos con menor demora en

el punto de medición cuando la política de QoS se encontraba activa, como se muestra en la **Figura 74**.

Figura 74

RTT del flujo TCP FTP bajo carga iPerf3 durante QoS.



4.5.4.3 Variación del RTT (Indicador temporal TCP)

La variación promedio del RTT se redujo a 5,28 ms. La menor diferencia entre muestras consecutivas evidencia una mayor estabilidad temporal del flujo TCP FTP bajo la misma condición de congestión. El resultado se interpreta como variación del RTT y no como jitter RTP, como se muestra en la **Figura 75**.

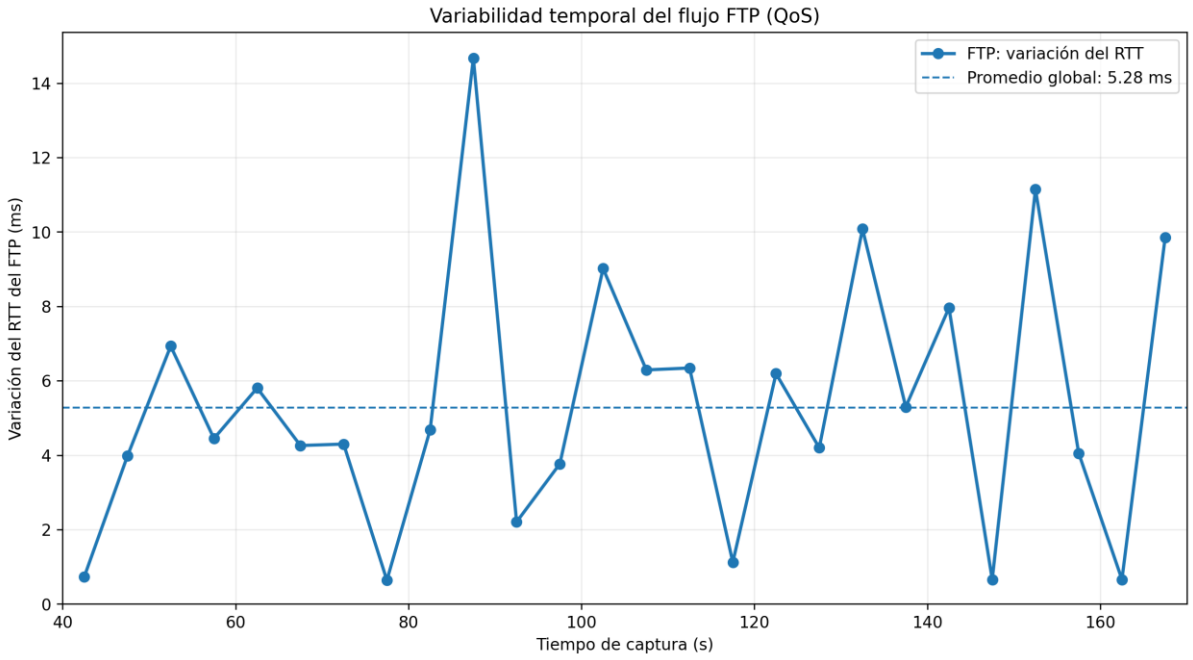
Ecuación 81.

Variación promedio del RTT del FTP con QoS

$$J_{prom} = 5{,}28ms$$

Figura 75

Variación del RTT del flujo FTP durante QoS



4.5.4.4 Indicador de pérdida TCP

En la ventana efectiva se identificaron 9638 segmentos TCP con datos correspondientes al archivo FTP y 88 eventos de discontinuidad de secuencia. A partir de estos valores se obtuvo un indicador de pérdida TCP de 0,91 %. De forma complementaria, la pérdida estimada del flujo iPerf3 alcanzó 98,99 % en el punto de captura. La elevada afectación del tráfico UDP de fondo es consistente con los descartes acumulados observados en la cola iPerf Background, como se observa en la **Figura 76**.

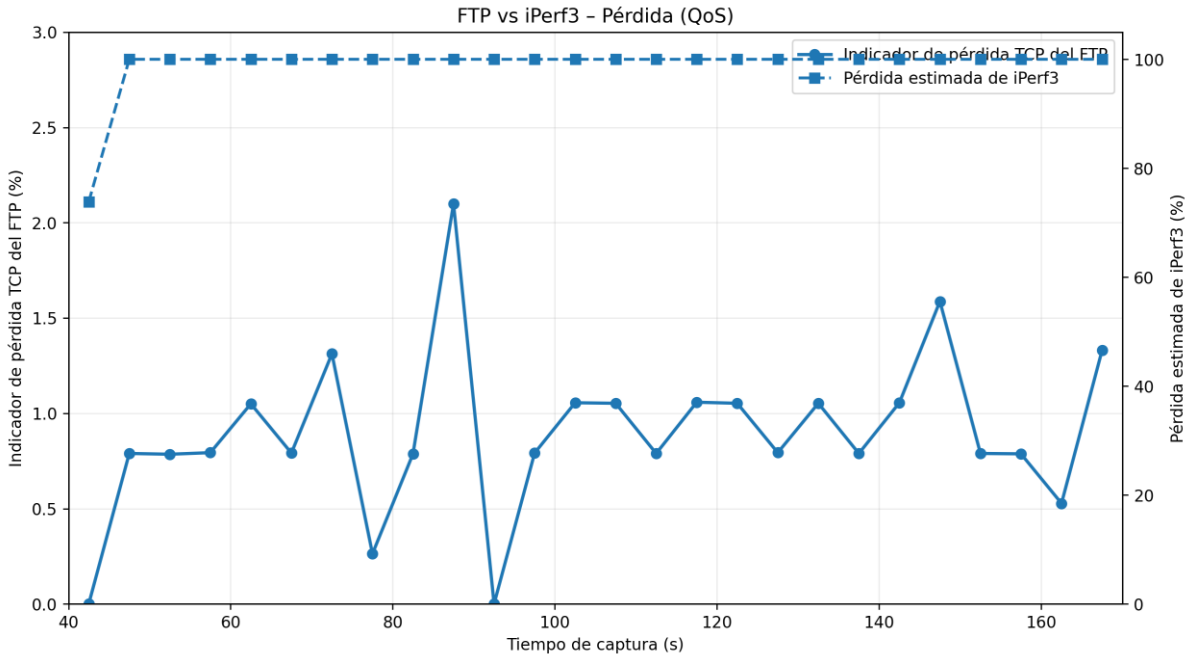
Ecuación 82.

Indicador de pérdida TCP del FTP con QoS

$$I_{TCP} = \left(\frac{88}{9638}\right) \times 100 = 0{,}91\%$$

Figura 76

Indicador de pérdida TCP del FTP y pérdida estimada de iPerf3 durante QoS

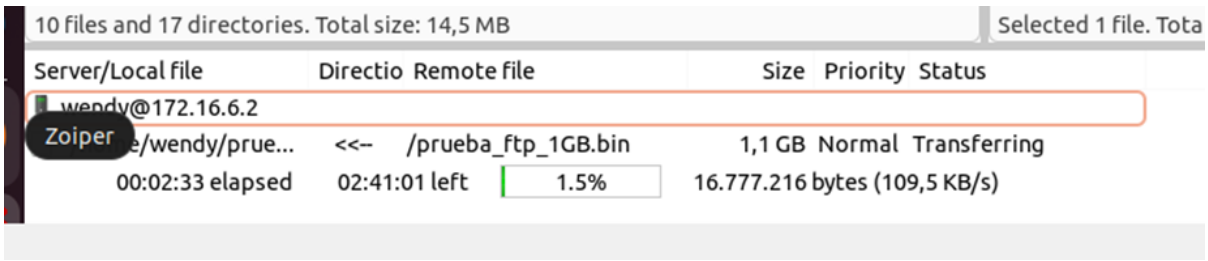


4.5.4.5 Observación de la transferencia

Durante el escenario QoS, FileZilla continuó descargando el mismo archivo de 1 GiB. En la evidencia visual se observa una tasa instantánea de aproximadamente 109,5 KB/s, superior a la registrada en la evidencia Sin QoS. Este dato se utiliza únicamente como observación de la aplicación; la comparación cuantitativa se sustenta en las métricas obtenidas de Wireshark dentro de la ventana efectiva. En la **Figura 77** se presenta la transferencia del archivo FTP observada en FileZilla durante QoS.

Figura 77

Transferencia del archivo FTP observada en FileZilla durante QoS



Los resultados muestran que la política modificó claramente la distribución de la capacidad durante la prueba FTP frente a iPerf3. El servicio evaluado fue FTP y las métricas se calcularon sobre su flujo TCP de datos; iPerf3 se mantuvo únicamente como carga de saturación. Esta distinción permite interpretar la mejora del FTP sin confundir las métricas TCP de la aplicación con los indicadores UDP del generador de congestión.

4.6 Registro y comparación de resultados

Las pruebas realizadas permitieron evaluar el comportamiento de los servicios de VoIP, Streaming, VoD y FTP bajo condiciones controladas de congestión. Para cada servicio se analizaron los escenarios Sin QoS y QoS, utilizando cargas de 2 Mbit/s y 5 Mbit/s sobre un enlace limitado a 1 Mbit/s. Los resultados fueron obtenidos principalmente mediante Wireshark, considerando las métricas aplicables a cada tipo de tráfico, mientras que iPerf3 se utilizó como generador de congestión. A partir de estos valores se comparó el desempeño de los servicios antes y después de aplicar las políticas de QoS, con el fin de identificar los cambios producidos por la priorización del tráfico.

4.6.4 VoIP vs iPerf3

El comportamiento del flujo VoIP RTP se evaluó bajo una carga UDP de 2 Mbit/s, superior a la capacidad de 1 Mbit/s establecida para el enlace R1–R2. Esta condición permitió analizar el desempeño del tráfico de voz en presencia de congestión, tanto sin mecanismos de priorización como bajo la aplicación de las políticas QoS.

El análisis se centró en tres métricas asociadas al comportamiento del flujo RTP: ancho de banda, jitter y pérdida de paquetes. En este contexto, un mayor ancho de banda efectivo destinado al tráfico de voz, junto con menores valores de jitter y pérdida de paquetes, representa un comportamiento más favorable para la transmisión de voz. Los porcentajes presentados

indican la variación observada en cada métrica entre las condiciones evaluadas. En la **Tabla 57** se presenta la comparación de las métricas de VoIP para una carga de 2 Mbit/s.

Tabla 57

Comparación de las métricas de VoIP para una carga de 2 Mbit/s.

Métrica	Sin QoS	QoS	Variación favorable
Ancho de banda	44,13 kbit/s	84,91 kbit/s	92,41 %
Jitter promedio	13,40 ms	2,81 ms	79,03 %
Pérdida RTP	46,08 %	0,87 %	98,11 %

4.6.4.1 Ancho de Banda (AB)

El ancho de banda promedio del flujo VoIP RTP pasó de 44,13 kbit/s en Sin QoS a 84,91 kbit/s con QoS. Para esta métrica, un incremento representa un comportamiento favorable, debido a que una mayor proporción del flujo de voz logra atravesar el enlace durante la congestión.

Ecuación 83.

Incremento porcentual del ancho de banda del flujo VoIP RTP

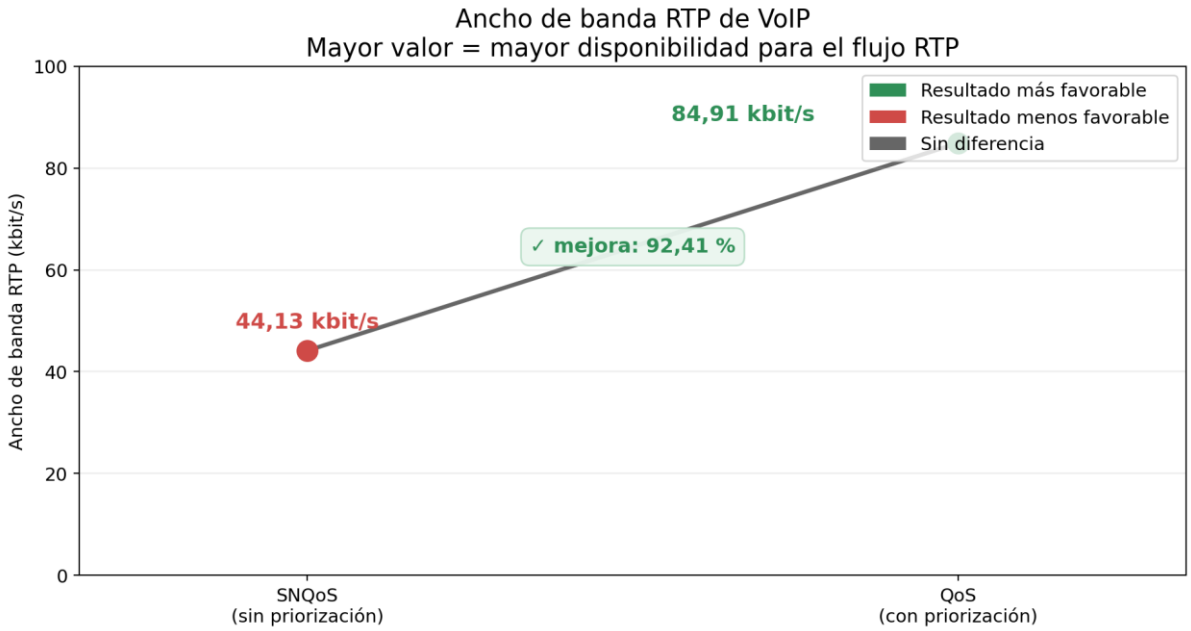
$$V_{AB} = \frac{AB_{QoS} - AB_{Sin\ QoS}}{AB_{Sin\ QoS}} \times 100$$

$$V_{AB} = \frac{84{,}91 - 44{,}13}{44{,}13} \times 100 = 92{,}41\%$$

Como se observa en la **Figura 78**, la activación de QoS produjo un incremento del 92,41 % en el ancho de banda promedio del servicio. Este cambio indica que, ante la misma condición de congestión, el flujo RTP conserva una mayor proporción de la capacidad disponible. La mejora no corresponde a un aumento de la capacidad física del enlace, sino a una redistribución de los recursos hacia el tráfico de voz prioritario.

Figura 78

Comparación del ancho de banda del flujo VoIP RTP entre Sin QoS y QoS



4.6.4.2 Jitter (IPDV)

El jitter promedio disminuyó de 13,40 ms en Sin QoS a 2,81 ms con QoS. En este caso, una reducción representa un comportamiento más favorable, ya que implica una menor variación en el tiempo de llegada de los paquetes RTP.

Ecuación 84.

Reducción porcentual del jitter promedio del flujo VoIP RTP

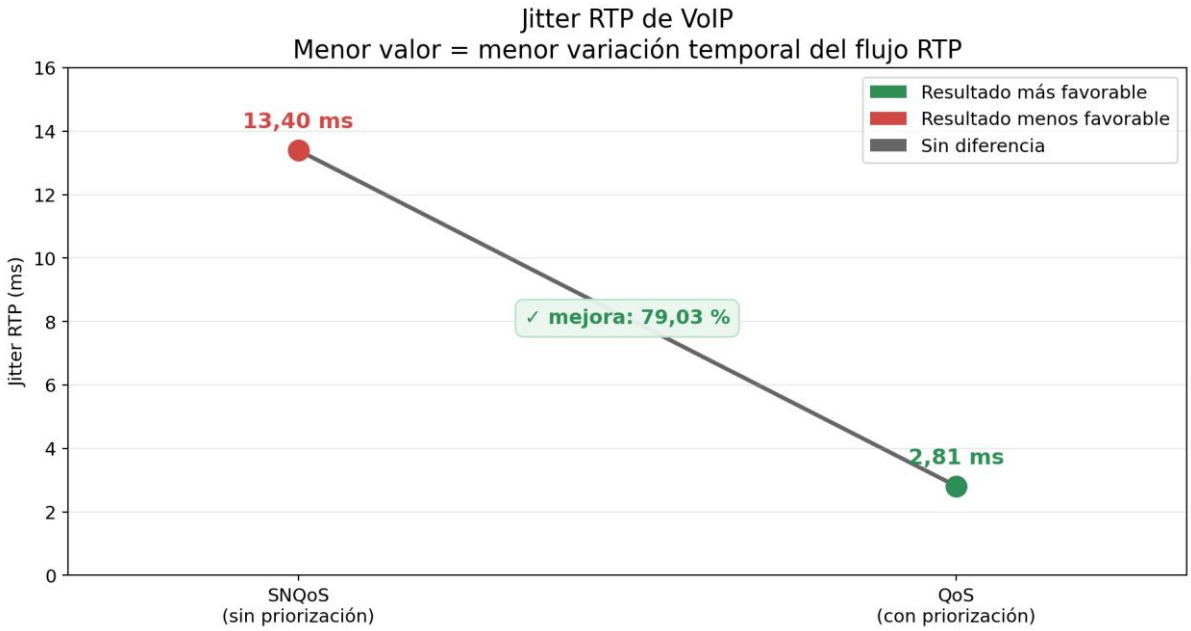
$$R_{Jitter} = \frac{Jitter_{Sin\ QoS} - Jitter_{QoS}}{Jitter_{Sin\ QoS}} \times 100$$

$$R_{Jitter} = \frac{13{,}40 - 2{,}81}{13{,}40} \times 100 = 79{,}03\%$$

La **Figura 79** evidencia una reducción del 79,03 % en el jitter promedio. La menor variación temporal refleja un flujo RTP más estable durante la congestión y favorece la continuidad de la comunicación de voz frente al comportamiento observado en Sin QoS.

Figura 79

Comparación del jitter promedio del flujo VoIP RTP entre Sin QoS y QoS.



4.6.4.3 Pérdida de paquetes (IPLR)

La diferencia más marcada se presentó en la pérdida de paquetes RTP. En Sin QoS se consideró una pérdida global de 46,08 %, mientras que con QoS el valor disminuyó a 0,87 %. Para esta métrica, una reducción representa una menor afectación del servicio de voz durante la condición de congestión.

Ecuación 85.
Reducción relativa de la pérdida de paquetes RTP

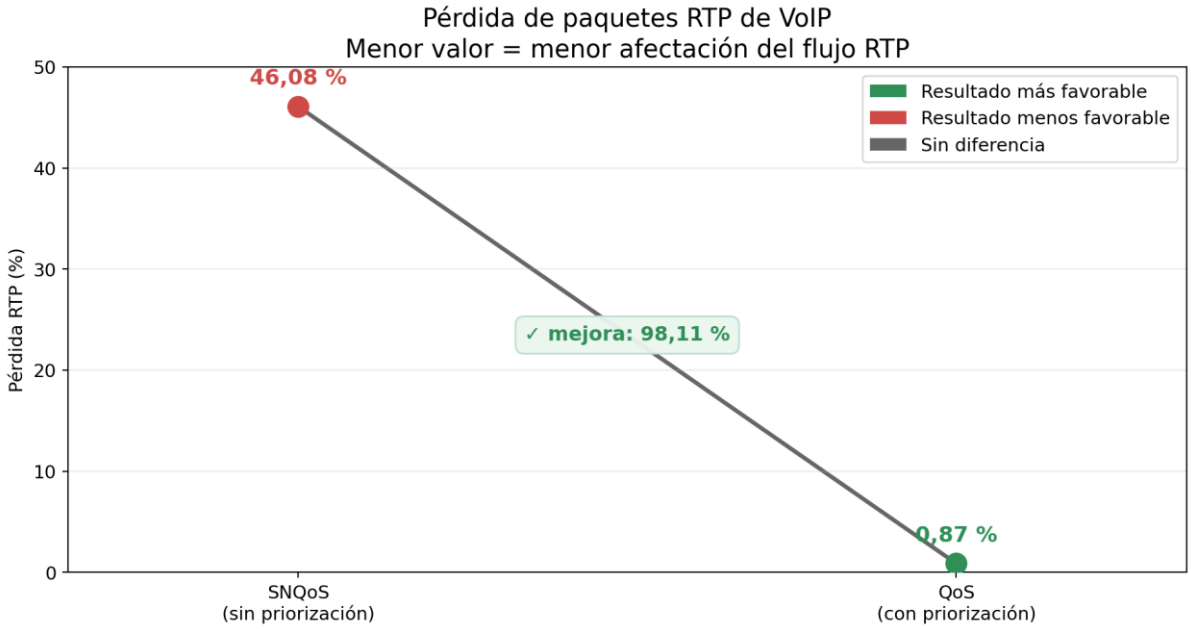
$$R_{IPLR} = \frac{IPLR_{Sin\ QoS} - IPLR_{QoS}}{IPLR_{Sin\ QoS}} \times 100$$

$$R_{IPLR} = \frac{46{,}08 - 0{,}87}{46{,}08} \times 100 = 98{,}11\%$$

En la **Figura 80** se aprecia que la pérdida pasó de 46,08 % a 0,87 %, equivalente a una reducción relativa del 98,11 % y a una diferencia absoluta de 45,21 puntos porcentuales, Este comportamiento muestra que el principal efecto de la priorización se presenta en la protección del flujo RTP frente a los descartes asociados a la congestión.

Figura 80

Comparación de la pérdida de paquetes RTP del servicio VoIP entre Sin QoS y QoS.

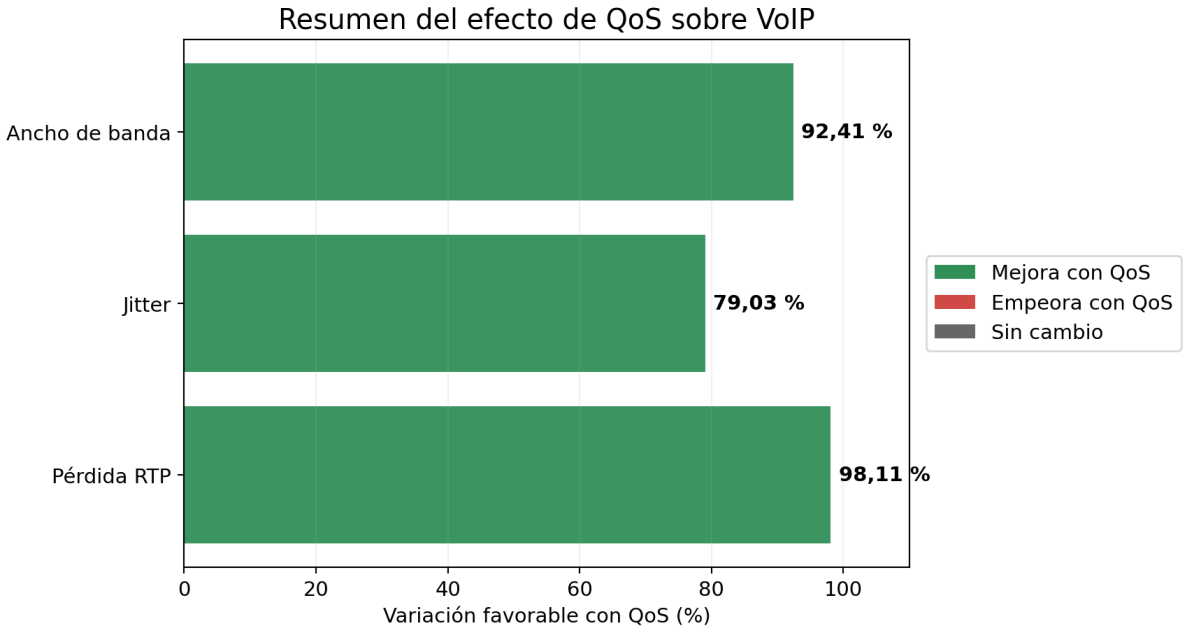


4.6.4.4 Comparación final

De forma conjunta, las tres métricas presentan un comportamiento favorable después de aplicar QoS. El ancho de banda promedio del flujo RTP aumentó un 92,41 %, el jitter disminuyó un 79,03 % y la pérdida de paquetes se redujo un 98,11 % respecto del escenario Sin QoS. Estas variaciones muestran que el efecto principal de la política se concentra en la protección del tráfico de voz durante la congestión.

Figura 81

Variación favorable de las métricas de VoIP al aplicar QoS



Como se observa en la **Figura 81**, la mayor variación favorable corresponde a la reducción de la pérdida de paquetes, seguida por el incremento del ancho de banda y la disminución del jitter. La política QoS no modifica la capacidad física del enlace, sino que redistribuye los recursos disponibles para otorgar preferencia al flujo VoIP RTP y trasladar una mayor parte de la afectación hacia el tráfico de fondo.

4.6.2 Streaming vs iPerf3

La comparación se realizó a partir de los valores obtenidos en la ventana efectiva de medición para el servicio de Streaming, manteniendo la misma carga de 2 Mbit/s sobre el enlace limitado a 1 Mbit/s. De esta manera, la diferencia entre ambos casos corresponde al estado de las políticas de QoS, lo que permite observar su efecto sobre el flujo RTP sin modificar la condición de congestión aplicada.

Para la interpretación de los resultados se consideró favorable el incremento del ancho de banda disponible para el Streaming y la disminución del jitter y de la pérdida de paquetes. Los porcentajes mostrados representan la variación obtenida al pasar de Sin QoS a QoS. En la **Tabla 58** se presenta la comparación de las métricas de Streaming para una carga de 2 Mbit/s.

Tabla 58

Comparación de las métricas de Streaming para una carga de 2 Mbit/s.

Métrica	Sin QOS	QoS	Variación favorable
Ancho de banda	283,51 kbit/s	375,20 kbit/s	32,34 %
Jitter promedio	7,99 ms	3,11 ms	61,08 %
Pérdida RTP	21,71 %	0,00 %	100,00 %

4.6.2.1 Ancho de Banda (AB)

El ancho de banda promedio del Streaming pasó de 283,51 kbit/s en Sin QoS a 375,20 kbit/s con QoS. La variación relativa se obtuvo mediante la siguiente expresión:

Ecuación 86.
Incremento porcentual del ancho de banda del Streaming

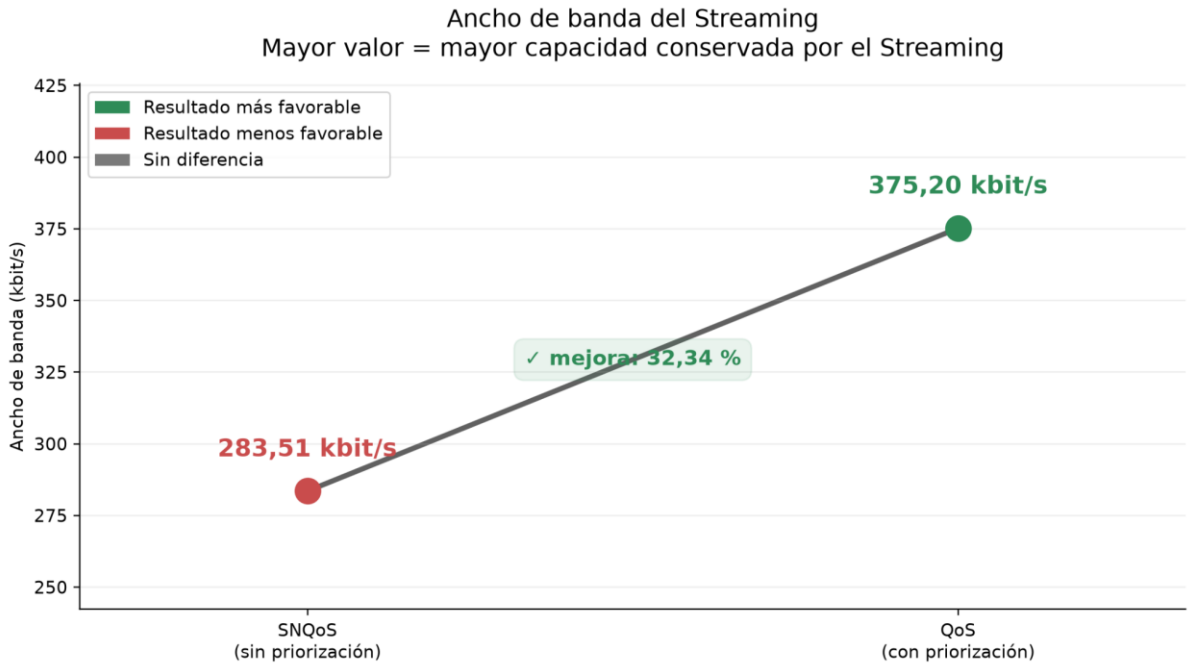
$$V_{AB} = \frac{375{,}20\,kbit/s - 283{,}51\,kbit/s}{283{,}51\,kbit/s} \times 100$$

$$V_{AB} = 32{,}34\%$$

Como se observa en la **Figura 82**, la activación de QoS produjo un incremento del 32,34 % en el ancho de banda promedio del servicio. Este cambio indica que, ante la misma condición de congestión, el flujo RTP conservó una mayor proporción de la capacidad disponible del enlace. El resultado concuerda con la prioridad asignada al Streaming, ya que el tráfico de fondo cedió parte de los recursos durante la saturación.

Figura 82

Comparación del ancho de banda del Streaming entre Sin QoS y QoS



4.6.2.2 Jitter RTP (IPDV)

El jitter promedio disminuyó de 7,99 ms en Sin QoS a 3,11 ms con QoS. En este caso, una reducción representa un comportamiento más favorable, por lo que la variación se calculó respecto del valor obtenido sin priorización.

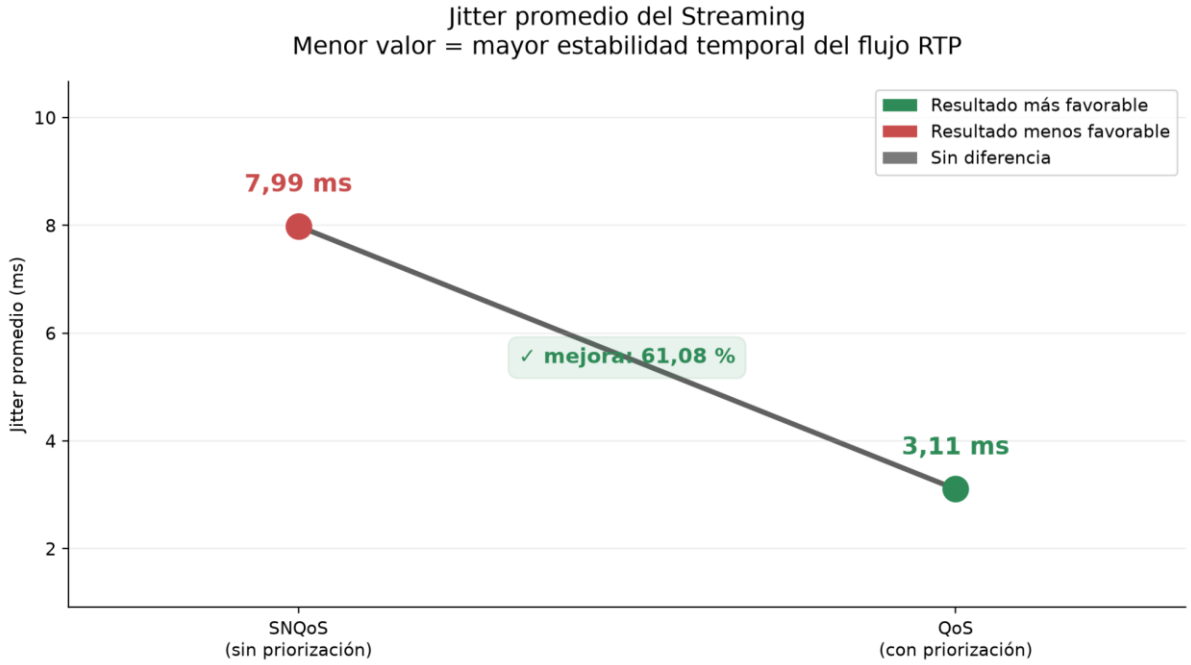
Ecuación 87.
Reducción porcentual del jitter promedio del Streaming

$$V_{Jitter} = \frac{7{,}99 - 3{,}11}{7{,}99} \times 100$$

$$V_{jitter} = 61{,}08\%$$

Figura 83

Comparación del jitter promedio del Streaming entre Sin QoS y QoS



La **Figura 83** evidencia una reducción del 61,08 % en el jitter promedio. La menor variación en el tiempo de llegada de los paquetes RTP refleja un flujo más estable durante la congestión. En consecuencia, la priorización no solo permitió conservar mayor ancho de banda para el servicio, sino también reducir las fluctuaciones temporales que afectaban la entrega del video en Sin QoS.

4.6.2.3 Pérdida de paquetes (IPLR)

La diferencia más marcada se presentó en la pérdida de paquetes RTP. En Sin QoS se registró una pérdida global de 21,71 %, mientras que en la captura correspondiente a QoS no se identificaron paquetes perdidos dentro de la ventana analizada.

Ecuación 88.

Reducción relativa de la pérdida de paquetes RTP

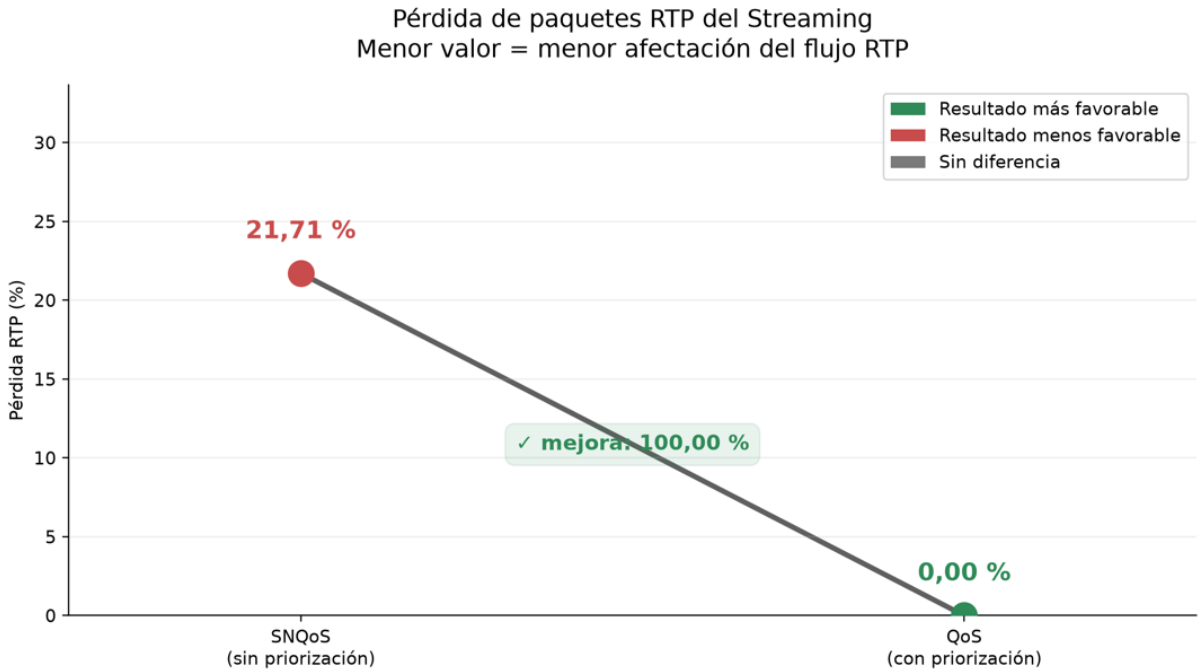
$$V_{IPLR} = \frac{21{,}71 - 0}{21{,}71} \times 100$$

$$V_{IPLR} = 100\%$$

En la **Figura 84** se aprecia que la pérdida pasó de 21,71 % a 0 %, equivalente a una reducción relativa del 100 % y a una diferencia absoluta de 21,71 puntos porcentuales. Este resultado corresponde específicamente a la ventana de medición evaluada y muestra que, durante esta prueba, el flujo RTP fue protegido frente a los descartes asociados a la congestión. La ausencia de pérdida también es consistente con la reproducción estable observada en VLC durante el escenario QoS.

Figura 84

Comparación de la pérdida de paquetes RTP del Streaming entre Sin QoS y QoS



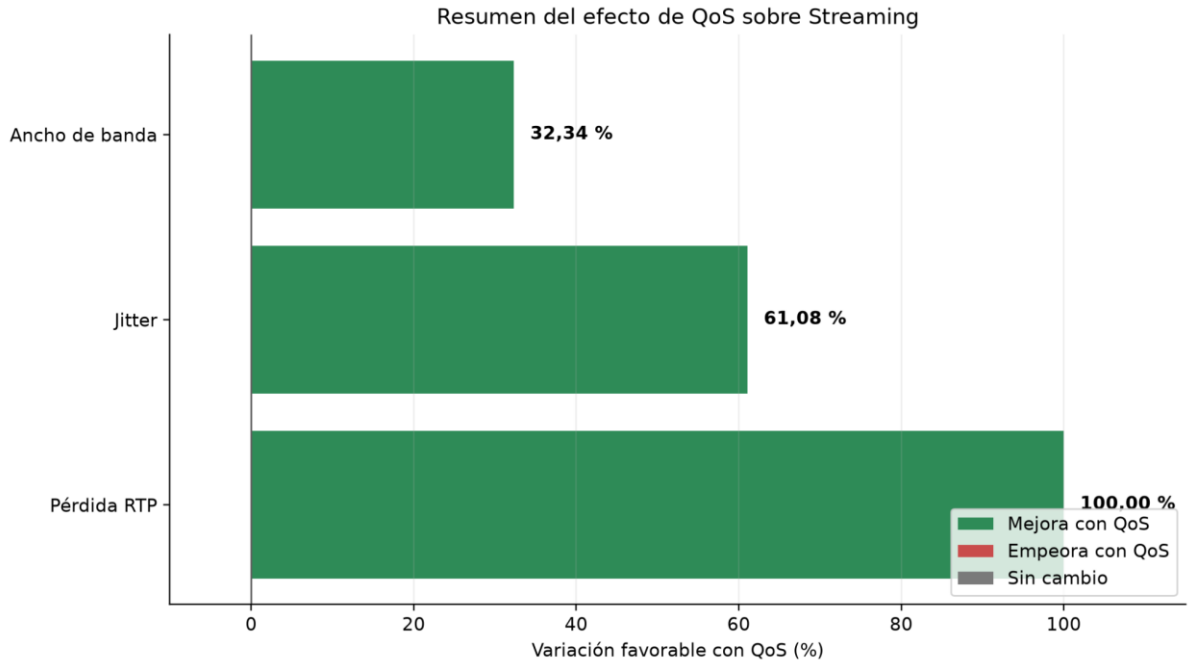
4.6.2.4 Comparación final

De forma conjunta, los resultados muestran una mejora en las tres métricas consideradas. El ancho de banda aumentó un 32,34 %, el jitter promedio se redujo un 61,08 % y la pérdida RTP disminuyó un 100 % dentro de la ventana analizada. La **Figura 85** resume estas variaciones y permite observar que el principal efecto de la política se presentó en la protección del flujo RTP frente a la pérdida de paquetes, seguido por la reducción del jitter.

Por tanto, para la carga de 2 Mbit/s, la política de QoS mejoró el comportamiento del Streaming sin modificar la capacidad física del enlace. La mejora se produjo por la redistribución de los recursos disponibles durante la congestión, otorgando preferencia al tráfico multimedia y trasladando una mayor parte de la afectación hacia el tráfico de fondo.

Figura 85

Variación favorable de las métricas de Streaming al aplicar QoS



4.6.3 VOD vs iPerf3

La comparación se realizó a partir de los valores obtenidos en la ventana efectiva de medición para el servicio VoD, manteniendo la misma carga de 2 Mbit/s generada mediante iPerf3 sobre el enlace limitado a 1 Mbit/s. En ambos escenarios se analizó únicamente la transferencia HTTP/TCP correspondiente al archivo de video MP4, por lo que la diferencia entre los resultados se atribuye al estado de las políticas de QoS y no a un cambio en la condición de congestión aplicada.

Para la interpretación se consideró favorable el incremento del ancho de banda disponible para el VoD y la disminución del RTT, de la variación del RTT y del indicador de

pérdida TCP. iPerf3 se mantuvo como tráfico de fondo para provocar la saturación del enlace; por esta razón, sus resultados se utilizan como referencia de la condición de congestión y no como sustituto de las métricas obtenidas sobre el flujo VoD. En la **Tabla 59** se presenta la comparación de las métricas e indicadores del VoD para una carga de 2 Mbit/s.

Tabla 59

Comparación de las métricas e indicadores del VoD para una carga de 2 Mbit/s.

Métrica	Sin QOS	QoS	Variación favorable
Ancho de banda	120,62 kbit/s	900,42 kbit/s	646,47 %
RTT promedio	98,28 ms	9,00 ms	90,84 %
Variación promedio del RTT	53,52 ms	5,40 ms	89,91 %
Indicador de pérdida TCP	7,80 %	0,97 %	87,53 %

4.6.3.1 Ancho de banda (AB)

El ancho de banda promedio del flujo VoD pasó de 120,62 kbit/s en Sin QoS a 900,42 kbit/s con QoS. La variación relativa se determinó mediante la siguiente expresión:

Ecuación 89.
Incremento porcentual del ancho de banda del VoD

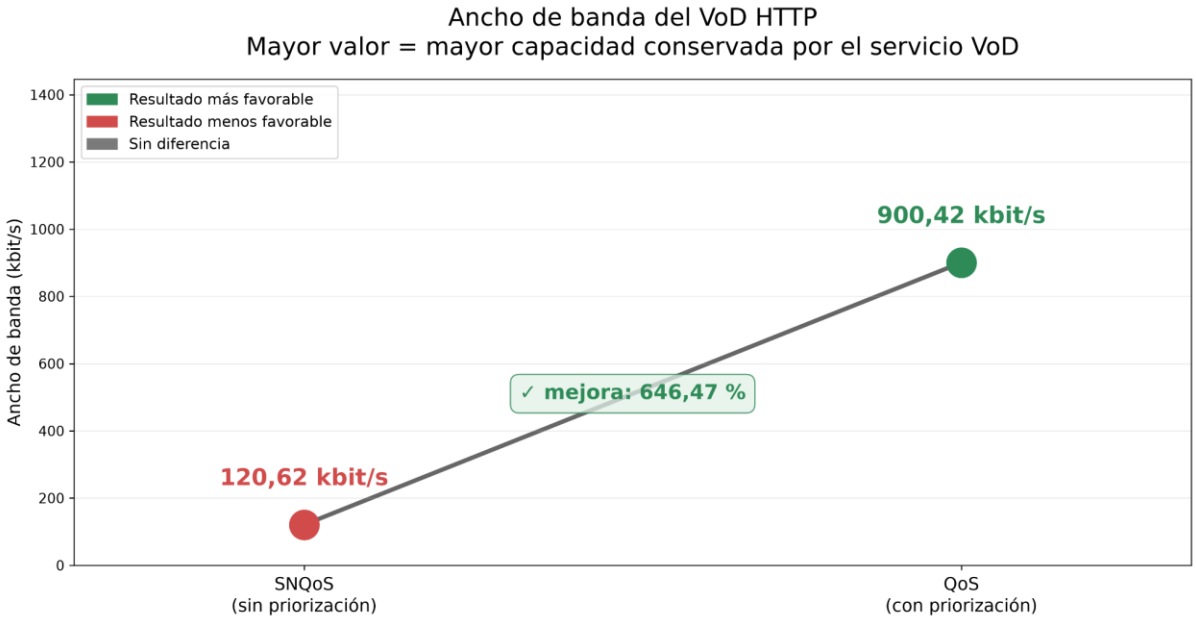
$$V_{AB} = \frac{AB_{QoS} - AB_{Sin\ QoS}}{AB_{Sin\ QoS}} \times 100$$

$$V_{AB} = \frac{900{,}42\ kbit/s - 120{,}62\ kbit/s}{120{,}62\ kbit/s} \times 100$$

$$V_{AB} = 646{,}47\%$$

Figura 86

Comparación del ancho de banda del VoD entre Sin QoS y QoS



Como se observa en la **Figura 86**, la activación de QoS produjo un incremento del 646,47 % en el ancho de banda promedio del servicio VoD. Este porcentaje elevado se debe a que el valor de referencia en Sin QoS fue reducido; por tanto, no implica que la capacidad física del enlace haya aumentado en esa proporción. El resultado muestra que, bajo la misma saturación, el flujo HTTP/TCP asociado al video conservó una mayor parte de la capacidad disponible cuando se aplicó la priorización.

De forma complementaria, el ancho de banda de iPerf3 observado en el punto de captura disminuyó considerablemente al aplicar QoS. Esto es consistente con una redistribución de los recursos del enlace: el tráfico VoD recibió preferencia, mientras que una mayor proporción de la afectación fue trasladada al tráfico de fondo. Esta reducción del tráfico iPerf3 observado no debe interpretarse como una modificación de la carga configurada, que se mantuvo en 2 Mbit/s durante la prueba.

4.6.3.2 Tiempo de ida y vuelta (RTT)

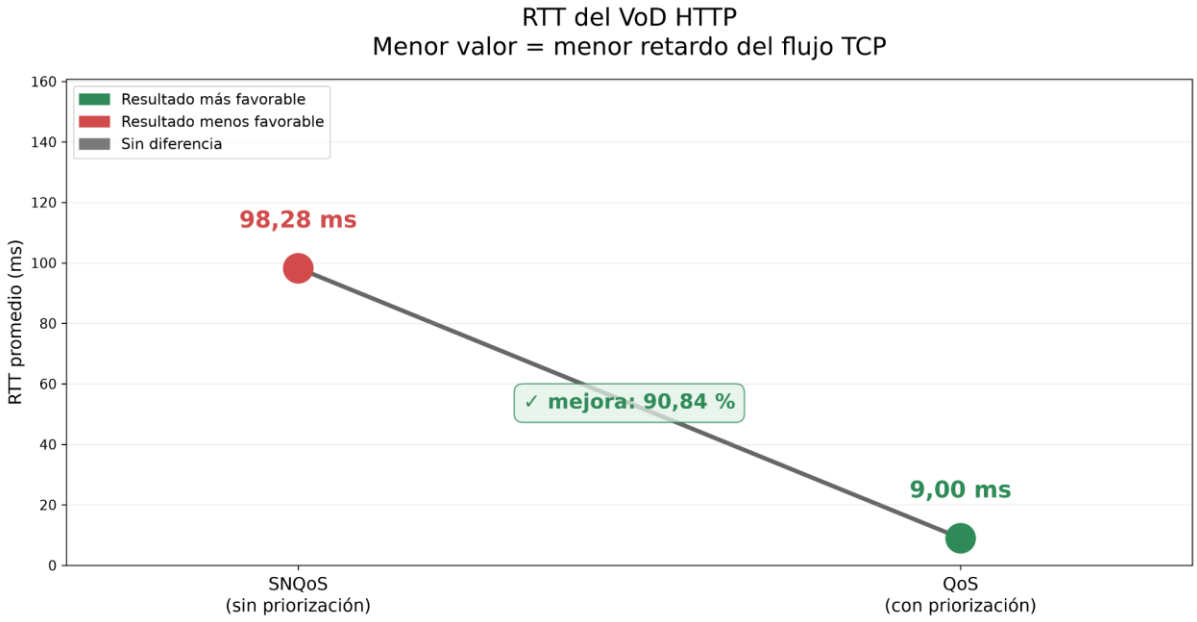
El RTT promedio del flujo VoD disminuyó de 98,28 ms en Sin QoS a 9,00 ms con QoS. Debido a que un menor tiempo de ida y vuelta representa un comportamiento más favorable, la variación se expresó como una reducción respecto del escenario sin priorización.

Ecuación 90.
Reducción porcentual del RTT promedio del VoD

$$R_{RTT} = \frac{RTT_{Sin\ QoS} - RTT_{QoS}}{RTT_{Sin\ QoS}} \times 100$$

Figura 87

Comparación del RTT promedio del VoD entre Sin QoS y QoS



La **Figura 87** muestra una reducción del 90,84 % en el RTT promedio. En Sin QoS, la competencia por el enlace incrementó el tiempo requerido para que los segmentos TCP y sus confirmaciones atravesaran la red. Con QoS, el menor RTT refleja una reducción del retardo asociado a la congestión y una entrega más oportuna del tráfico perteneciente al servicio VoD.

4.6.3.3 Variación del RTT

Debido a que el servicio VoD utiliza HTTP sobre TCP, no se dispone de un campo de jitter equivalente al empleado en RTP. Por esta razón, la estabilidad temporal del flujo se evaluó mediante la diferencia absoluta entre muestras consecutivas de RTT, definida como:

$$V_i = |RTT_i - RTT_{i-1}|$$

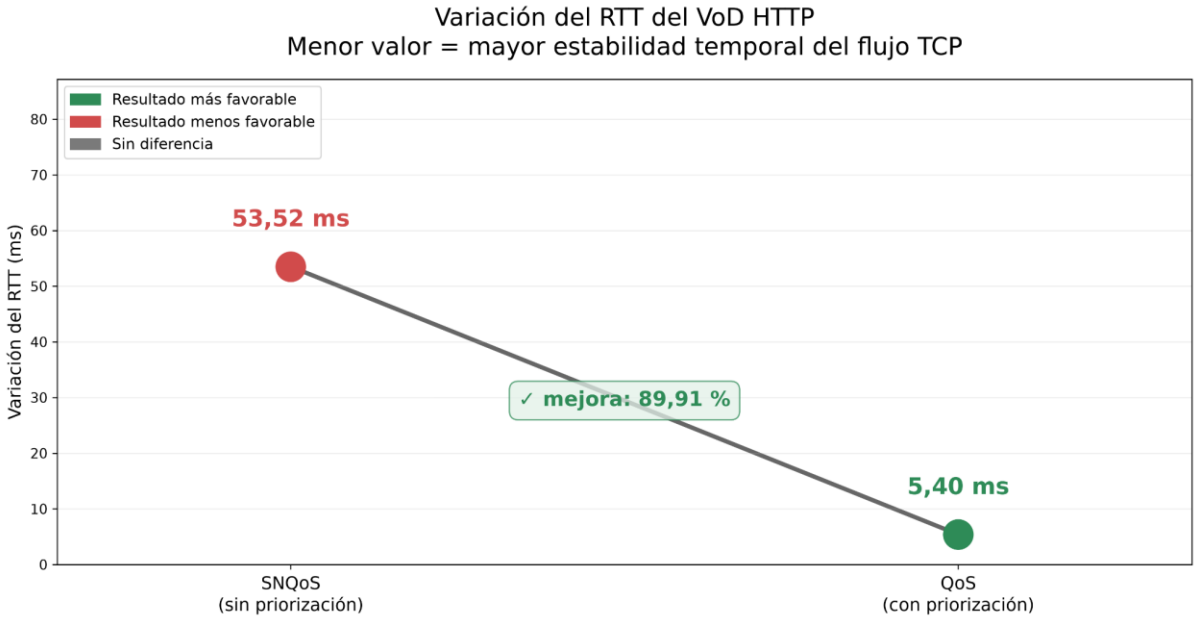
A partir de este criterio, la variación promedio del RTT disminuyó de 53,52 ms en Sin QoS a 5,40 ms con QoS. La reducción relativa se calculó mediante:

Ecuación 91.
Reducción porcentual de la variación del RTT del VoD

$$R_{VRTT} = \frac{VRTT_{Sin\ QoS} - VRTT_{QoS}}{VRTT_{Sin\ QoS}} \times 100$$

Figura 88

Comparación de la variación del RTT del VoD entre Sin QoS y QoS



La **Figura 88** evidencia una reducción del 89,91 % en la variabilidad temporal del flujo. En el escenario Sin QoS se presentaron fluctuaciones considerablemente mayores entre muestras consecutivas de RTT, mientras que con QoS los valores se mantuvieron en un rango inferior. Este comportamiento indica una mayor estabilidad temporal del flujo TCP durante la congestión.

Esta métrica debe interpretarse como una variación derivada del RTT y no como jitter RTP. La distinción es importante porque iPerf3 opera en UDP y su jitter se obtiene mediante

un procedimiento diferente; por ello, la comparación principal se realizó entre la misma métrica del VoD en Sin QoS y QoS.

4.6.3.4 Indicador de pérdida TCP

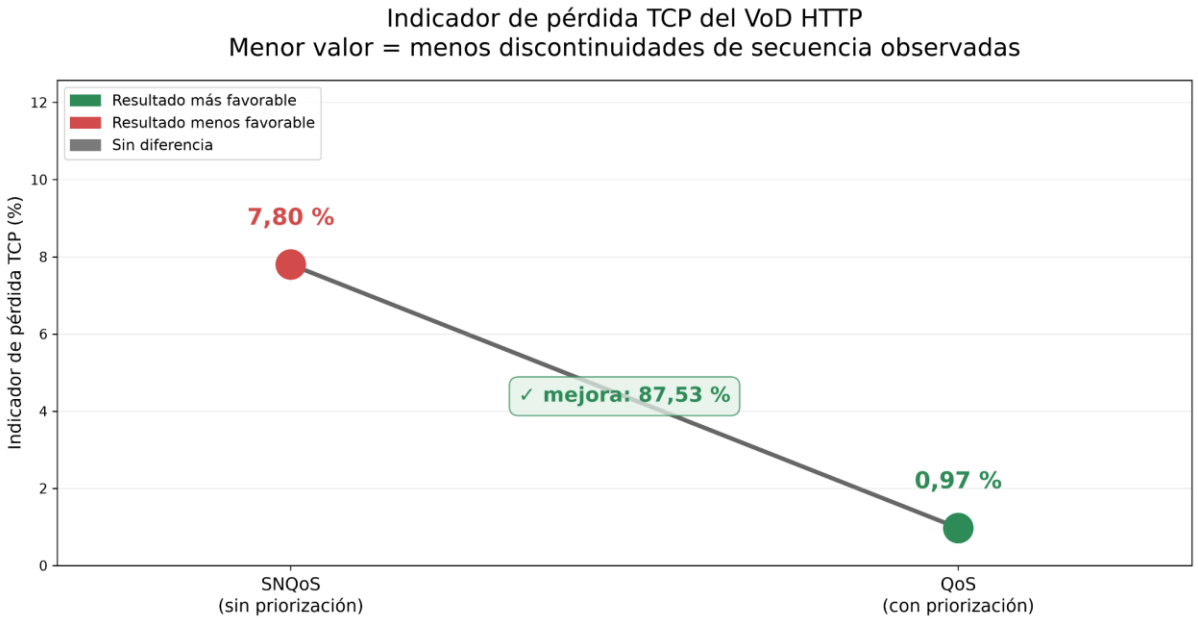
El indicador de pérdida TCP del flujo VoD disminuyó de 7,80 % en Sin QoS a 0,97 % con QoS. Este indicador se obtuvo a partir de las discontinuidades de secuencia observadas en los segmentos TCP con datos correspondientes al archivo MP4 y, por tanto, no se interpreta como IPLR de capa IP.

Ecuación 92.
Reducción porcentual del indicador de pérdida TCP del VoD

$$R_P = \frac{P_{Sin\ QoS} - P_{QoS}}{P_{Sin\ QoS}} \times 100$$

Figura 89

Comparación del indicador de pérdida TCP del VoD entre Sin QoS y QoS.



En la **Figura 89** se observa que el indicador pasó de 7,80 % a 0,97 %, lo que representa una reducción relativa del 87,53 % al utilizar los valores de precisión completa obtenidos de las capturas. La diferencia absoluta entre los valores redondeados es de 6,83 puntos

porcentuales. El resultado muestra que, durante la prueba con QoS, se observaron menos discontinuidades de secuencia en el flujo TCP del video.

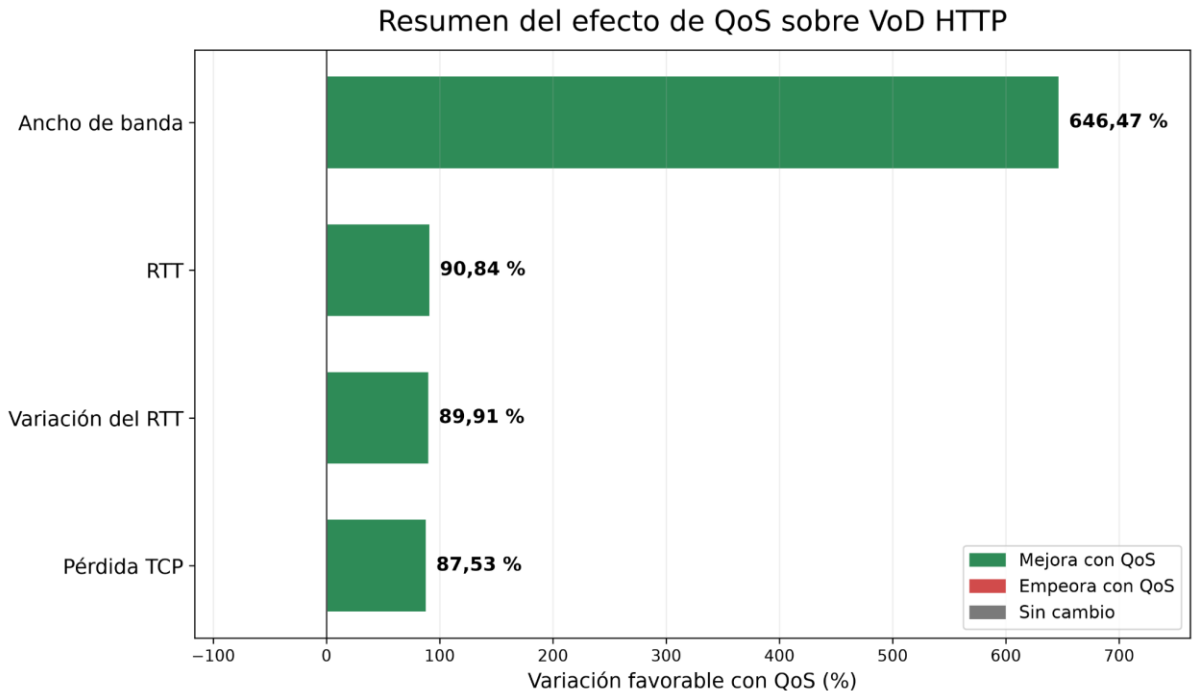
Al tratarse de TCP, una discontinuidad observada puede estar asociada a pérdida, reordenamiento o recuperación mediante retransmisiones. Por esta razón, el resultado se presenta como un indicador de pérdida TCP y no como una medida directa de pérdida de paquetes IP extremo a extremo.

4.6.3.5 Comparación final

De forma conjunta, los resultados muestran una mejora en las cuatro métricas e indicadores considerados. El ancho de banda del VoD aumentó un 646,47 %, el RTT promedio se redujo un 90,84 %, la variación del RTT disminuyó un 89,91 % y el indicador de pérdida TCP se redujo un 87,53 %. La **Figura 90** resume estas variaciones y permite observar que QoS produjo mejoras simultáneas en capacidad disponible, retardo, estabilidad temporal y continuidad del flujo TCP.

Figura 90

Variación favorable de las métricas del VoD al aplicar QoS



El incremento porcentual del ancho de banda es superior al de las demás métricas debido al bajo valor registrado en Sin QoS, por lo que debe interpretarse como una variación relativa respecto de esa línea base y no como un incremento de la capacidad física del enlace. La capacidad se mantuvo limitada a 1 Mbit/s durante ambos escenarios.

En consecuencia, para una carga de saturación de 2 Mbit/s, la política de QoS mejoró el comportamiento del servicio VoD sin modificar las características físicas del enlace. La mejora se produjo mediante la redistribución de los recursos disponibles durante la congestión, otorgando preferencia al tráfico HTTP/TCP del video y trasladando una mayor parte de la afectación hacia el tráfico de fondo generado por iPerf3.

4.6.4 FTP vs iPerf3

El servicio evaluado corresponde a FTP. Debido a que la transferencia del archivo se realiza sobre TCP, las métricas se obtuvieron del flujo TCP de datos asociado al comando RETR y no únicamente de los paquetes del canal de control FTP en el puerto 21. iPerf3 se utilizó como generador de congestión y como referencia complementaria para verificar la redistribución de la capacidad del enlace.

Para la interpretación se consideró favorable el incremento del ancho de banda disponible para FTP y la disminución del RTT, de la variación del RTT y del indicador de pérdida TCP. Los porcentajes presentados representan la variación obtenida al pasar del escenario Sin QoS al escenario QoS. En la **Tabla 60** se presenta la comparación de las métricas e indicadores de FTP para una carga de 2 Mbit/s.

Tabla 60

Comparación de las métricas e indicadores de FTP para una carga de 2 Mbit/s

Métrica	Sin QOS	QoS	Variación favorable

Ancho de banda	149,44 kbit/s	897,97 kbit/s	500,87 %
RTT promedio	38,56 ms	7,78 ms	79,83 %
Variación promedio del RTT	57,84 ms	5,28 ms	90,87 %
Indicador de pérdida TCP	7,36 %	0,91 %	87,59 %

4.6.4.5 Ancho de Banda (AB)

El ancho de banda promedio del flujo de datos FTP aumentó de 149,44 kbit/s en Sin QoS a 897,97 kbit/s con QoS. La variación relativa se calculó respecto del valor obtenido sin priorización mediante la siguiente expresión:

Ecuación 93.
Incremento porcentual del ancho de banda del FTP

$$V_{AB} = \frac{AB_{QoS} - AB_{Sin\ QoS}}{AB_{Sin\ QoS}} \times 100$$

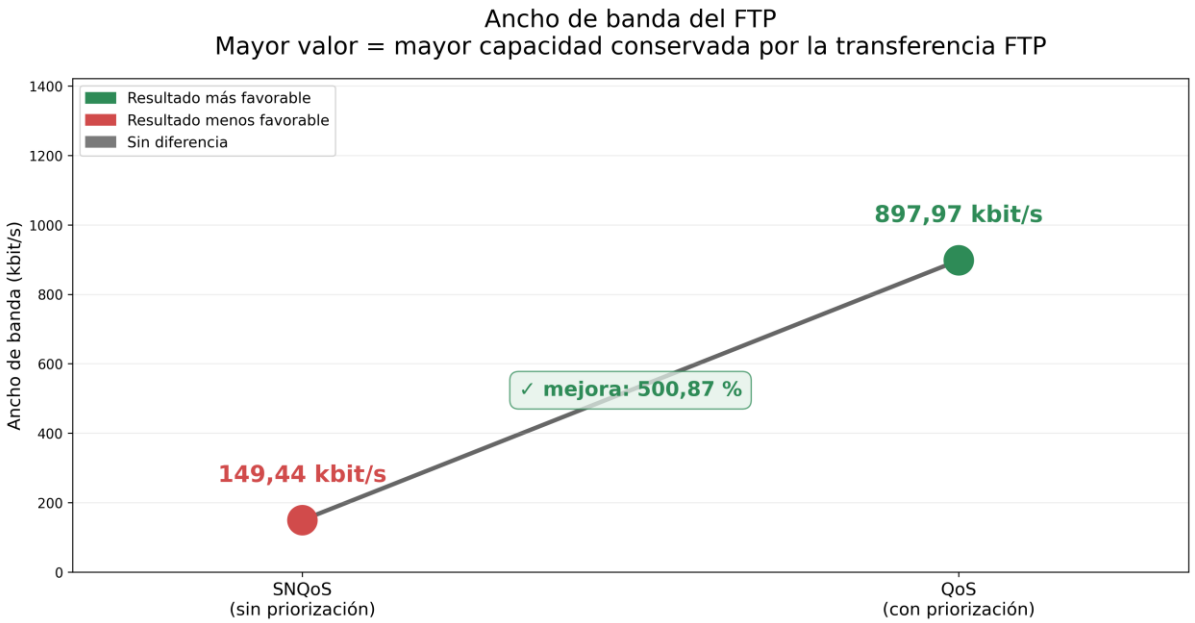
$$V_{AB} = \frac{897{,}97\ kbit/s - 149{,}44\ kbit/s}{149{,}44\ kbit/s} \times 100$$

$$V_{AB} = 500{,}87\%$$

En la **Figura 91** se presenta la comparación del ancho de banda de FTP entre Sin QoS y QoS.

Figura 91

Comparación del ancho de banda de FTP entre Sin QoS y QoS



La activación de QoS produjo un incremento del 500,87 % en el ancho de banda promedio de FTP. El incremento elevado se explica por el bajo valor obtenido en Sin QoS, donde la carga UDP de fondo ocupó la mayor parte de la capacidad disponible. Con la política activa, el flujo FTP conservó una porción considerablemente mayor del enlace. Este resultado no representa un aumento de la capacidad física, sino una redistribución de los recursos disponibles durante la congestión.

Como evidencia complementaria, el ancho de banda observado de iPerf3 disminuyó de 844,76 kbit/s a 21,82 kbit/s, equivalente a una reducción aproximada del 97,42 %. Esto muestra que el tráfico artificial de saturación cedió capacidad cuando se habilitó la política.

4.6.4.6 Tiempo de ida y vuelta (RTT)

El RTT TCP promedio disminuyó de 38,56 ms en Sin QoS a 7,78 ms con QoS. Debido a que las capturas se realizaron en el enlace R1-R2, este valor se interpreta como RTT TCP

observado en el punto de medición y no como una medición extrema a extremo obtenida mediante relojes sincronizados, como se muestra en la **Figura 92**.

Ecuación 94.
Reducción porcentual del RTT TCP promedio de FTP

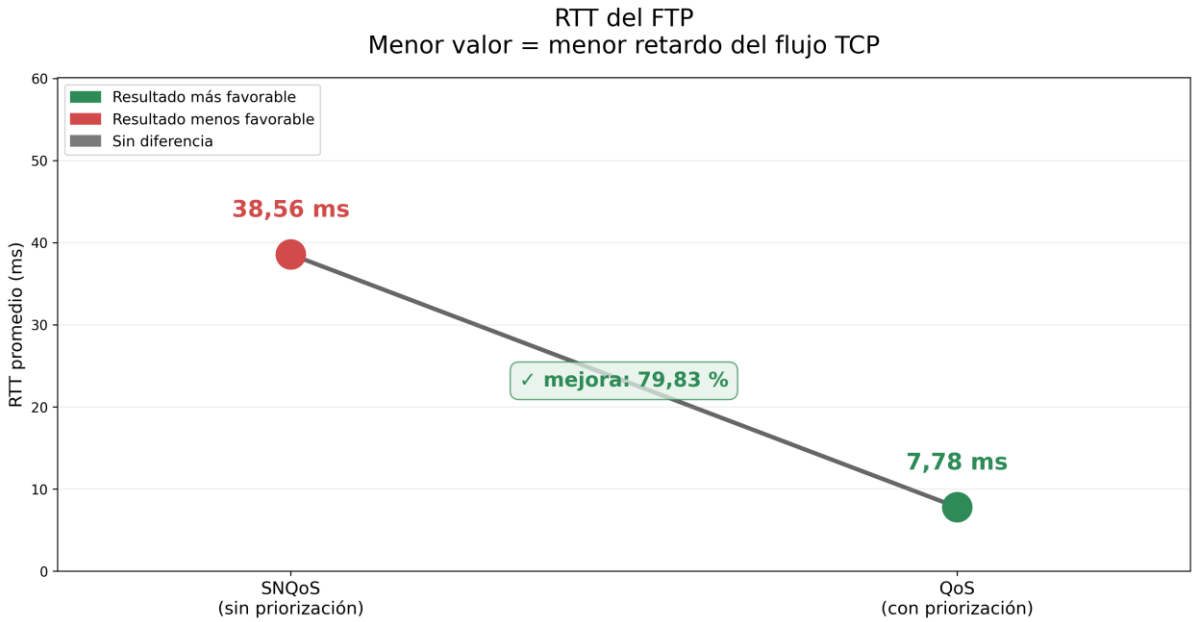
$$R_{RTT} = \frac{RTT_{Sin\ QoS} - RTT_{QoS}}{RTT_{Sin\ QoS}} \times 100$$

$$R_{RTT} = \frac{38{,}56 - 7{,}78}{38{,}56} \times 100$$

$$R_{RTT} = 79{,}83\%$$

Figura 92

Comparación del RTT TCP promedio de FTP entre Sin QoS y QoS



La reducción del 79,83 % indica que, con QoS, los segmentos TCP y sus reconocimientos presentaron menores tiempos de respuesta en el punto de observación. El resultado es coherente con la disminución de la competencia ejercida por iPerf3 sobre la capacidad disponible para la transferencia FTP.

4.6.4.7 Variación del RTT

FTP utiliza TCP, por lo que no dispone de un jitter nativo equivalente al utilizado para RTP. Para caracterizar la estabilidad temporal del flujo se empleó la diferencia absoluta entre muestras consecutivas de RTT. Por esta razón, la métrica se presenta como variación del RTT y no como jitter RTP, como se observa en la **Figura 93**. La variación promedio del RTT pasó de 57,84 ms en Sin QoS a 5,28 ms con QoS. La reducción porcentual se obtuvo mediante:

Ecuación 95.
Reducción porcentual de la variación del RTT del FTP

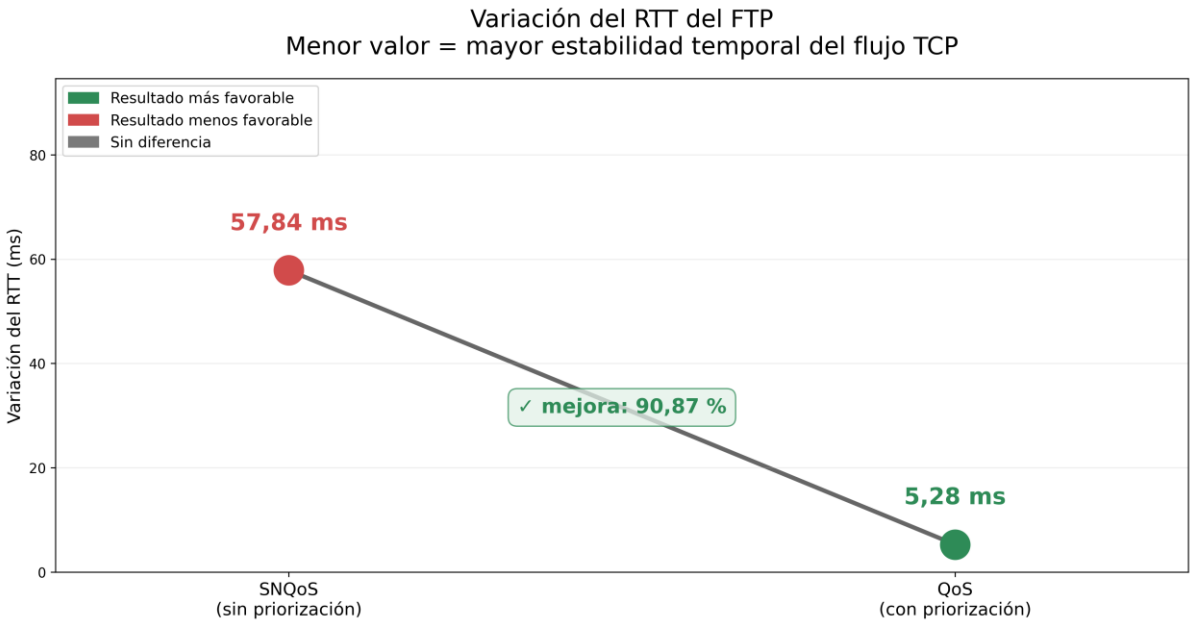
$$R_{FRTT} = \frac{VRTT_{Sin\ QoS} - VRTT_{QoS}}{VRTT_{Sin\ QoS}} \times 100$$

$$R_{FRTT} = \frac{57{,}84 - 5{,}28}{57{,}84} \times 100$$

$$R_{FRTT} = 90{,}87\%$$

Figura 93

Comparación de la variación del RTT de FTP entre Sin QoS y QoS.



La disminución del 90,87 % evidencia una mayor estabilidad temporal del flujo TCP con QoS. En Sin QoS se observaron oscilaciones considerablemente mayores entre muestras

consecutivas de RTT, mientras que con la política habilitada dichas variaciones se redujeron de forma marcada.

4.6.4.8 Indicador de pérdida TCP

En FTP no se reportó IPLR como si se tratara de un flujo RTP. En su lugar se utilizó un indicador basado en las discontinuidades de secuencia observadas en los segmentos TCP con datos correspondientes a la transferencia del archivo. Este indicador permite comparar la afectación relativa del flujo bajo las mismas condiciones de captura, aunque no debe interpretarse como una medida directa de pérdida IP.

En Sin QoS se identificaron 118 eventos de discontinuidad sobre 1604 segmentos TCP con datos, obteniéndose 7,36 %. Con QoS se registraron 88 eventos sobre 9638 segmentos, con un indicador de 0,91 %, como se muestra en la **Figura 94**.

Ecuación 96.
Reducción porcentual del indicador de pérdida TCP del FTP

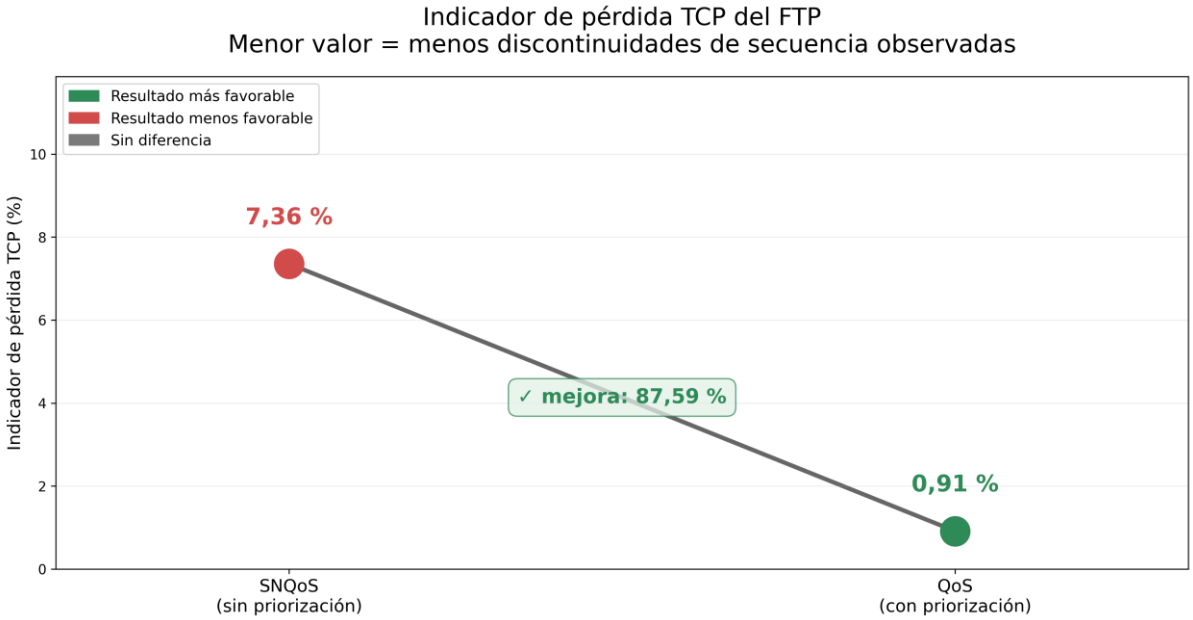
$$R_P = \frac{P_{Sin\ QoS} - P_{QoS}}{P_{Sin\ QoS}} \times 100$$

$$R_P = \frac{7{,}36 - 0{,}91}{7{,}36} \times 100$$

$$R_P = 87{,}59\%$$

Figura 94

Comparación del indicador de pérdida TCP de FTP entre Sin QoS y QoS



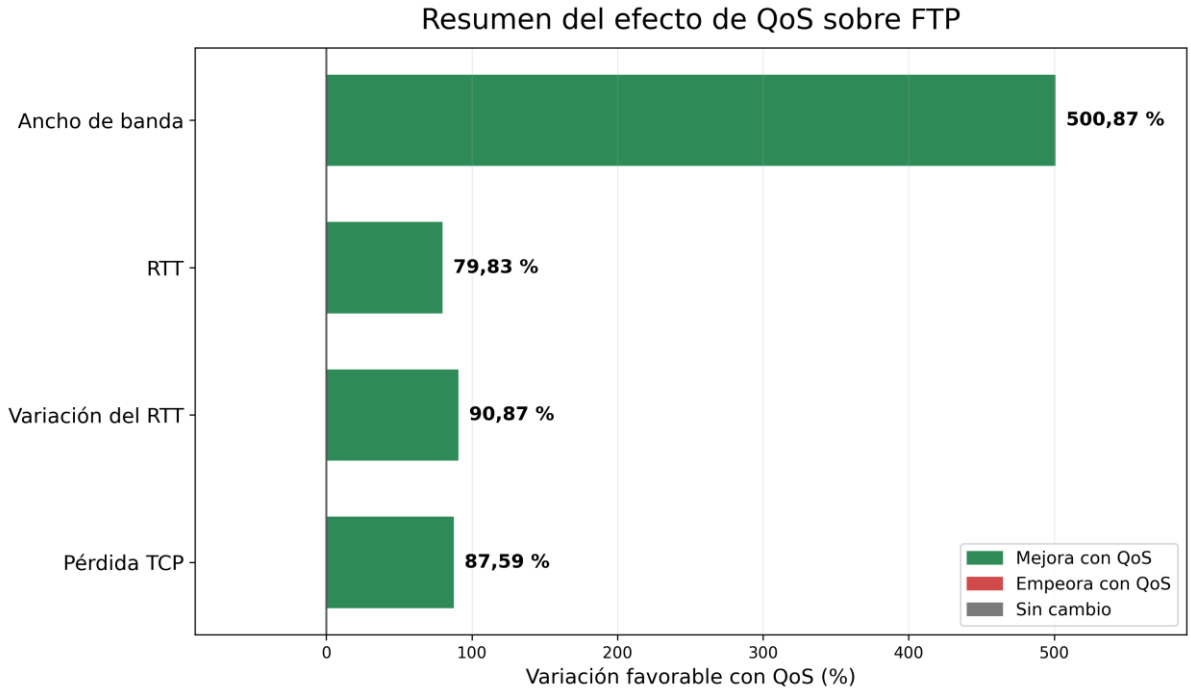
El indicador disminuyó de 7,36 % a 0,91 %, equivalente a una reducción relativa del 87,59 % y a una diferencia absoluta de 6,44 puntos porcentuales. Esto muestra una menor cantidad relativa de discontinuidades de secuencia en el flujo FTP cuando la política de QoS se encontraba habilitada.

4.6.4.9 Comparación final

Los resultados muestran una mejora en las cuatro métricas e indicadores considerados. El ancho de banda de FTP aumentó un 500,87 %, el RTT TCP se redujo un 79,83 %, la variación del RTT disminuyó un 90,87 % y el indicador de pérdida TCP se redujo un 87,59 %. La **Figura 95** resume estas variaciones favorables.

Figura 95

Variación favorable de las métricas de FTP al aplicar QoS.



Como se muestra en la **Figura 95**, este comportamiento responde a la redistribución de la capacidad durante la congestión y no a una modificación del ancho de banda físico del enlace. En la política aplicada, FTP se encuentra en la clase 7. Best Effort, mientras que iPerf3 se gestiona como tráfico de fondo con prioridad 8.

La carga de 2 Mbit/s, la activación de QoS produjo un comportamiento más favorable del servicio FTP bajo congestión. La comparación se sustenta en el flujo TCP de datos del archivo y en el mismo punto y ventana de medición para ambos escenarios, mientras que iPerf3 se mantiene únicamente como generador de carga y evidencia complementaria del tratamiento del tráfico de fondo.

5. Conclusiones

Se concluye que la investigación de los principios y métodos de calidad de servicio permitió determinar que DiffServ constituye la alternativa más adecuada para la gestión del tráfico multimedia en entornos virtualizados, debido a su escalabilidad y a la posibilidad de implementar mecanismos de priorización sin mantener estados por flujo. Asimismo, las Recomendaciones ITU-T E.800, Y.1540 e Y.1541, junto con las RFC 2474, 2597, 3246 y 4594, proporcionaron el marco de referencia para asignar los valores DSCP y seleccionar las métricas empleadas en la evaluación del desempeño de la red.

La definición de los requerimientos permitió establecer que MikroTik RouterOS dispone de las funcionalidades necesarias para implementar políticas de Calidad de Servicio basadas en el modelo DiffServ. A través del uso de reglas Mangle organizadas en tres fases (mark-connection, change-dscp y mark-packet), la asignación de valores DSCP a cada clase de servicio y la administración del tráfico con Queue Tree, empleando disciplinas PFIFO para servicios sensibles al retardo (REALTIME-pfifo y RTP-pfifo) y PCQ (QoS-pcq) para el resto de las clases, fue posible clasificar, priorizar y controlar el ancho de banda de los distintos servicios multimedia. Aunque RouterOS emplea una arquitectura diferente a la de equipos Cisco, sus mecanismos de prioridad, garantía de ancho de banda (limit-at) y restricción mediante max-limit, sumados a la estructura jerárquica basada en HTB, permiten alcanzar un comportamiento funcionalmente equivalente para la gestión del tráfico.

El diseño e implementación de la infraestructura virtualizada demostraron que la integración de GNS3, VirtualBox y MikroTik CHR constituye una plataforma adecuada para evaluar políticas de Calidad de Servicio en redes virtualizadas. La incorporación de OSPF, VLAN y de las políticas basadas en DiffServ permitió reproducir un escenario representativo de una red que soporta servicios de VoIP (Issabel), streaming en tiempo real, video bajo

demanda (Streama), MySQL, HTTP y servicios de baja prioridad. Adicionalmente, mediante iPerf3 se generó tráfico concurrente de saturación que permitió evaluar el comportamiento de la red bajo condiciones controladas de congestión. La verificación se realizó mediante Wireshark, Torch y Queue Tree, confirmando el correcto marcaje DSCP y el funcionamiento de los mecanismos de priorización del tráfico.

La implementación de QoS permitió determinar que el desempeño de la política depende directamente de una correcta identificación y clasificación del tráfico. La definición de puertos y protocolos, el marcado mediante Mangle y la asignación de prioridades en Queue Tree fueron elementos esenciales para diferenciar los servicios multimedia del tráfico de menor prioridad. Asimismo, la separación del tráfico generado por iPerf3 permitió producir condiciones controladas de congestión sin incorporarlo dentro de las clases destinadas a los servicios evaluados, facilitando una medición más consistente del comportamiento de la red.

Los resultados obtenidos permitieron comprobar que MikroTik CHR puede aplicar mecanismos de Calidad de Servicio de manera efectiva en un entorno virtualizado sometido a congestión. La priorización implementada favoreció principalmente a los servicios sensibles al retardo, como VoIP y Streaming en tiempo real, al mejorar su disponibilidad de ancho de banda y reducir parámetros asociados con el retardo, jitter y pérdida de paquetes respecto al escenario sin QoS. En consecuencia, la solución propuesta demuestra la viabilidad de emplear MikroTik para gestionar diferentes tipos de tráfico y mantener un mejor desempeño de los servicios prioritarios cuando existe competencia por los recursos de la red.

6. Recomendaciones

Para implementaciones en entornos con mayores requerimientos de capacidad, se recomienda utilizar licencias MikroTik CHR superiores a la versión Free, debido a que esta presenta una limitación de 1 Mbps por interfaz. Esta restricción resulta adecuada para escenarios experimentales controlados, pero puede condicionar el comportamiento de la red cuando se pretende evaluar servicios multimedia con mayores demandas de ancho de banda. En entornos reales, los parámetros asociados a las colas, reservas de ancho de banda y límites máximos deben establecerse de acuerdo con la capacidad efectiva de los enlaces, el número de usuarios y las características de los servicios transportados. De esta manera, la política de QoS puede adaptarse a las condiciones propias de cada infraestructura sin depender de las limitaciones impuestas por el entorno de pruebas.

También se recomienda asignar recursos suficientes de procesamiento, memoria y almacenamiento a las máquinas virtuales que ejecutan los routers MikroTik CHR, los servidores multimedia y los clientes utilizados durante las pruebas. El rendimiento de una infraestructura virtualizada depende no solo de la configuración de red, sino también de la capacidad disponible en el hipervisor y de la distribución de recursos entre las diferentes máquinas virtuales. Una asignación insuficiente puede introducir retardos adicionales, pérdida de rendimiento o inestabilidad en los servicios, lo que podría afectar la interpretación de los resultados obtenidos. Por esta razón, es conveniente verificar previamente el consumo de recursos del sistema y procurar que las limitaciones del hardware no interfieran con la evaluación del comportamiento de las políticas de Calidad de Servicio.

Para fortalecer la validación del modelo DiffServ, se recomienda realizar capturas de tráfico con Wireshark en distintos puntos de la topología y comprobar que los valores DSCP asignados a cada servicio se conserven durante su recorrido por la red. Esta verificación permite

confirmar que la clasificación realizada en los routers de acceso se mantiene en los nodos intermedios y que cada flujo conserva la identificación establecida antes de llegar al punto donde se aplica la priorización. Asimismo, resulta conveniente contrastar estas capturas con las estadísticas proporcionadas por MikroTik para comprobar que las marcas de paquete y las colas asociadas registren tráfico durante las pruebas. La combinación de ambas verificaciones permite disponer de una evidencia más completa sobre el funcionamiento de la política implementada.

Como trabajo futuro, se recomienda ampliar el escenario experimental mediante enlaces de mayor capacidad, un número superior de usuarios concurrentes y la generación simultánea de varios flujos pertenecientes a un mismo servicio. Esto permitiría analizar el comportamiento de la política de QoS en condiciones más cercanas a una red real, donde varios usuarios pueden utilizar aplicaciones de voz, streaming, navegación y transferencia de archivos al mismo tiempo. Además, sería conveniente evaluar diferentes niveles de congestión y prolongar los tiempos de observación, con el propósito de identificar posibles variaciones en el ancho de banda, retardo, jitter y pérdida de paquetes conforme aumenta la demanda de la red. Estas pruebas permitirían determinar con mayor precisión los límites operativos del esquema de priorización propuesto.

Finalmente, se recomienda evaluar mecanismos adicionales de administración de colas que puedan complementar la estrategia utilizada. Aunque la combinación de PFIFO y PCQ permitió diferenciar el tratamiento de los servicios de acuerdo con sus características, futuras investigaciones podrían comparar su comportamiento con otras disciplinas de gestión de congestión. Esta comparación permitiría determinar qué mecanismos ofrecen mejores resultados para aplicaciones especialmente sensibles al retardo, jitter y pérdida de paquetes. De igual manera, podría analizarse el efecto de modificar las prioridades, reservas de ancho de

banda y límites asignados a cada clase, con el fin de establecer configuraciones más adecuadas para distintos perfiles de tráfico y capacidades de enlace.

Bibliografía

Abba M. (2023). *Wireshark: Analice Tráfico de Red con Precisión ☑*. https://www.innovaciondigital360.com/iot/que-es-wireshark-y-casos-de-uso/

Alvarez, J., & Neira, J. (2015). *ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL*.

Boutros, S., & Eastlake, D. E. (2024). *RFC 9638: Network Virtualization over Layer 3 (NVO3) Encapsulation Considerations*. https://www.rfc-editor.org/info/rfc9638

Bustos, A., Styven, R., & Fecha, O. (2023). *Desarrollo de un plan de migración de una red de área extensa de un proveedor de servicios de internet a una red definida por software SD-WAN*. https://repositorio.utn.edu.ec/handle/123456789/15328

Cando, R. (2023). *Implementación del modelo diffserv (QOS) en un entorno de tráfico real para evaluar el comportamiento de parámetros de calidad de servicio en equipos cisco y mikrotik*.

CCNA. (2018). *▷ Configuración de VLAN [Comandos] » CCNA desde Cero*. https://ccnadesdecero.es/configuracion-vlan/

Chan, K., Sahita, R., Hahn, S., & McCloghrie, K. (2003). *RFC 3317 - Differentiated Services Quality of Service Policy Information Base*. https://datatracker.ietf.org/doc/rfc3317/

Cisco Systems, Inc. (2005). *DiffServ -- The Scalable End-to-End QoS Model [QoS Signaling] - Cisco Systems*. https://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper09186a00800a3e2f.html

Espinosa, O. (2026). *Listado de puertos TCP y UDP de diferentes servicios online*. https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

Evaluación de mecanismos de calidad de servicio en los routers para servicios multimedia. (n.d.). *docto-2-qos*.

Forouzan, B. A. ., & Fegan, S. Chung. (2007). *Data communications and networking*. 1134.

Hat, R. (2024). *¿Qué es una máquina virtual (VM)? ¿Qué son los virtual machines?* Https://Www.Redhat.Com/Es/Topics/Virtualization/What-Is-a-Virtual-Machine.

Introduction to QoS. (2024, June 27). https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_QoS_AdminGuide/Topics-QoSG/Introduction-to-QoS.htm

ITU-T. (2008). *UIT-T Rec. E.800 (09/2008) Definiciones de términos relativos a la calidad de servicio*.

ITU-T E.800. (2008). *UIT-T Rec. E.800 (09/2008) Definiciones de términos relativos a la calidad de servicio*.

ITU-T Y.1540. (2007). *ITU-T Rec. Y.1540 (11/2007) Internet protocol data communication service - IP packet transfer and availability performance parameters*.

ITU-T Y.1541. (2002). *UIT-T Aspectos del protocolo Internet – Calidad de servicio y características de red*.

Mikrotik. (2025). *RouterOS license keys - RouterOS - MikroTik Documentation*. https://help.mikrotik.com/docs/spaces/ROS/pages/328149/RouterOS+license+keys

Medina, H. (2019). *Teoría de Colas – Colas Markovianas – de 1 solo canal – White Hat Developer*. https://whdeveloper.wordpress.com/2019/07/01/teoria-de-colas-colas-markovianas-de-1-solo-canal-y-multicanal/

Mikrotik. (n.d.). *Queues - RouterOS - MikroTik Documentation*. Retrieved April 20, 2026, from https://help.mikrotik.com/docs/spaces/ROS/pages/328088/Queues?utm_source=chatgpt.com

Mikrotik. (2024). *Mangle - RouterOS - MikroTik Documentation*. https://help.mikrotik.com/docs/spaces/ROS/pages/48660587/Mangle

Moncayo Chávez, K. N. (2025). *Aplicación y evaluación de calidad de servicio (QOS) sobre una red inalámbrica definida por software (SDWN).* https://repositorio.utn.edu.ec/handle/123456789/16934

Monitoring, N. (2023). *What Is Quality of Service (QoS)? - LiveAction*. Https://Www.Liveaction.Com/Resources/Blog-Post/What-Is-Quality-of-Service-Qos/.

Paspuel, D. (2014a). *OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)*.

Pulido, R. U. (2024). *Mikrotik: QoS para optimizar tu red - Blog Virtualizacion*. Https://Www.Maquinasvirtuales.Eu/Mikrotik-Qos-Para-Optimizar-Tu-Red/.

Red Hat. (2021). *¿Qué es la virtualización de la red?* https://www.redhat.com/es/topics/virtualization/what-is-network-virtualization

Reddit. (2023). *¿Cuáles son las diferencias entre Mikrotik y otros entornos como pfSense o UniFi? : r/mikrotik*. https://www.reddit.com/r/mikrotik/comments/1eu3wh0/what_are_the_differences_between_mikrotik_and/?tl=es-419

RFC 1918 - Address Allocation for Private Internets. (n.d.). Retrieved February 20, 2026, from https://datatracker.ietf.org/doc/html/rfc1918

RFC 2474 - Definición del campo de servicios diferenciados (campo DS) en los encabezados IPv4 e IPv6. (n.d.). Retrieved October 13, 2025, from https://datatracker.ietf.org/doc/rfc2474/?utm_source=chatgpt.com

RFC 2597 - Reenvío asegurado de PHB Group. (n.d.). Retrieved October 13, 2025, from https://datatracker.ietf.org/doc/html/rfc2597?utm_source=chatgpt.com

Ricardo Alarcón Llamas. (2003). *UNIVERSIDAD POLITÉCNICA DE CARTAGENA*.

Rosales, F. (2022). *Gestión de la calidad de servicio QOS para controlar el tráfico de datos para un ISP local de la provincia de Santa Elena*. La Libertad: Universidad Estatal Península de Santa Elena, 2022. https://repositorio.upse.edu.ec/handle/46000/7713

Salazar, J., & Silvestre, Y. S. (2016). *INTERNET DE LAS COSAS*. http://www.techpedia.eu

Sarmiento, D. A. L., G., D. A. S., & A., F. J. G. (2011). Revista Ingeniería. *Redes de Ingeniería*, *2*(1), 4–18. https://doi.org/10.14483/2248762X.7178

Stanley, A. (2022). *Modelos de QoS: Identifiquémoslos y comparémoslos | Blog de OrhanErgun.net*. https://orhanergun.net/qos-models

Vunkers IT Experts. (n.d.). *NTOP | Vunkers IT Experts | Proveedor de Servicios IT para empresas*. Retrieved May 10, 2026, from https://www.vunkers.com/productos/ntop/

Walton, A. (2023). *Algoritmo de Formación de Colas » CCNA desde Cero*. Https://Ccnadesdecero.Es/Algoritmo-Formacion-Colas/.

7. Anexos

7.1 **Anexo A.** Configuración de direccionamiento ip

Figura 96

Direccionamiento IP en R1

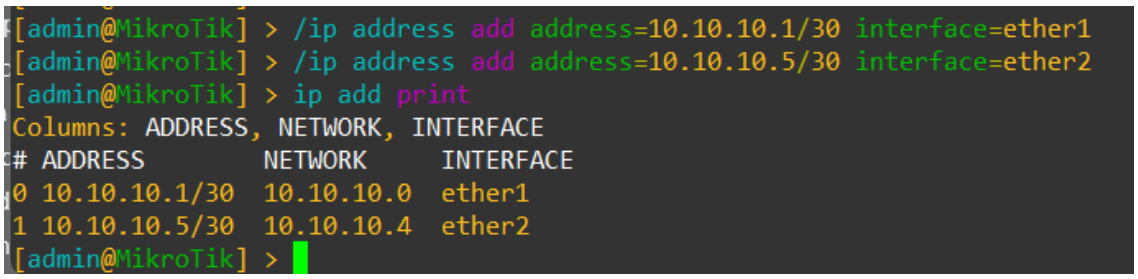


Figura 97

Direccionamiento IP en R2

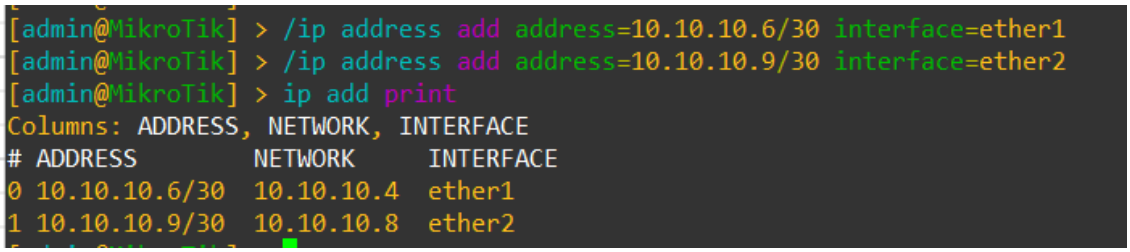


Figura 98

Direccionamiento IP en R3

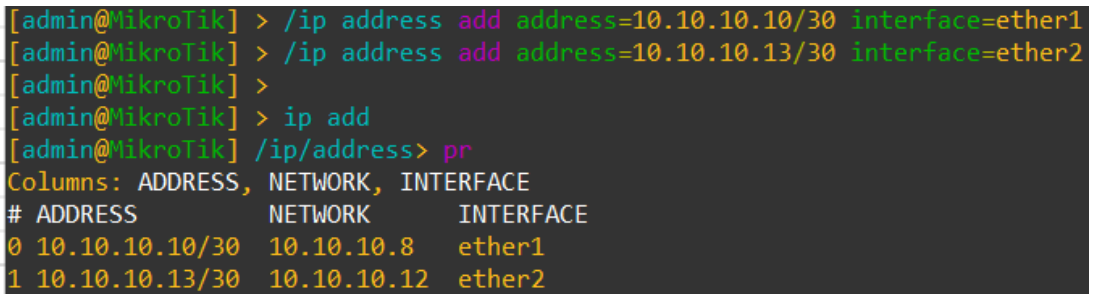


Figura 99

Direccionamiento IP en R4

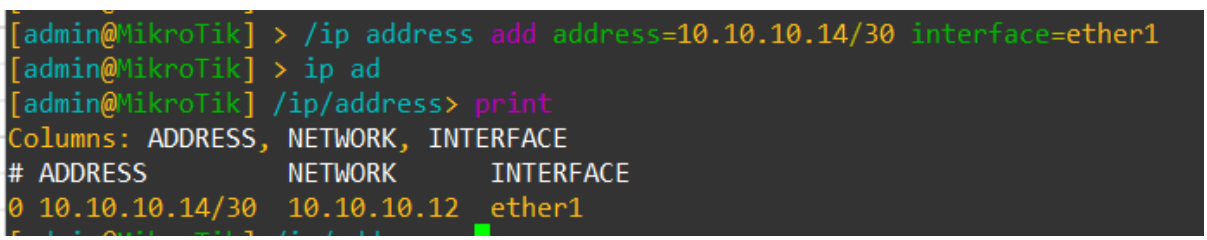


Figura 100

Direccionamiento IP en R5

```
[admin@MikroTik] > /ip address add address=10.10.10.2/30 interface=ether3
[admin@MikroTik] > ip address/print
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS         NETWORK     INTERFACE
0 10.10.10.2/30   10.10.10.0  ether3
```

7.2 Anexo B. Configuración OSPF: instancia, área e interface

Figura 101

Configuración OSPF en R3

```
Flags: V - virtual; D - dynamic
 0  D instance=default-ospf area=backbone address=10.10.10.9 priority=128
      router-id=10.10.10.9 dr=10.10.10.10 bdr=10.10.10.9 state="Full"
      state-changes=6 adjacency=2m22s timeout=33s

 1  D instance=default-ospf area=backbone address=10.10.10.14 priority=128
      router-id=172.16.2.130 dr=10.10.10.13 bdr=10.10.10.14 state="Full"
      state-changes=6 adjacency=2m22s timeout=34s
```

Figura 102

Configuración OSPF en R4

```
[admin@R4] /routing/ospf/neighbor> print
Flags: V - virtual; D - dynamic
 0  D instance=default-ospf area=backbone address=10.10.10.13 priority=128
      router-id=172.16.8.130 dr=10.10.10.13 bdr=10.10.10.14 state="Full"
      state-changes=6 adjacency=2m52s timeout=33s
```

Figura 103

Configuración OSPF en R5

```
[admin@R5] > routing/ospf/neighbor/print
Flags: V - virtual; D - dynamic
 0  D instance=default-ospf area=backbone address=10.10.10.1 priority=128
      router-id=10.10.10.5 dr=0.0.0.0 bdr=0.0.0.0 state="TwoWay"
      state-changes=2 timeout=35s
```

7.3 Anexo C. Despliegue de servicios multimedia

En esta fase se realizó el despliegue de los servicios multimedia dentro de un entorno virtualizado, con el objetivo de simular diferentes tipos de tráfico en la red para las pruebas de calidad de servicio. Cada servicio fue implementado en una máquina virtual independiente, lo que permitió aislar los recursos de procesamiento y facilitar la administración de los servicios durante las pruebas experimentales.

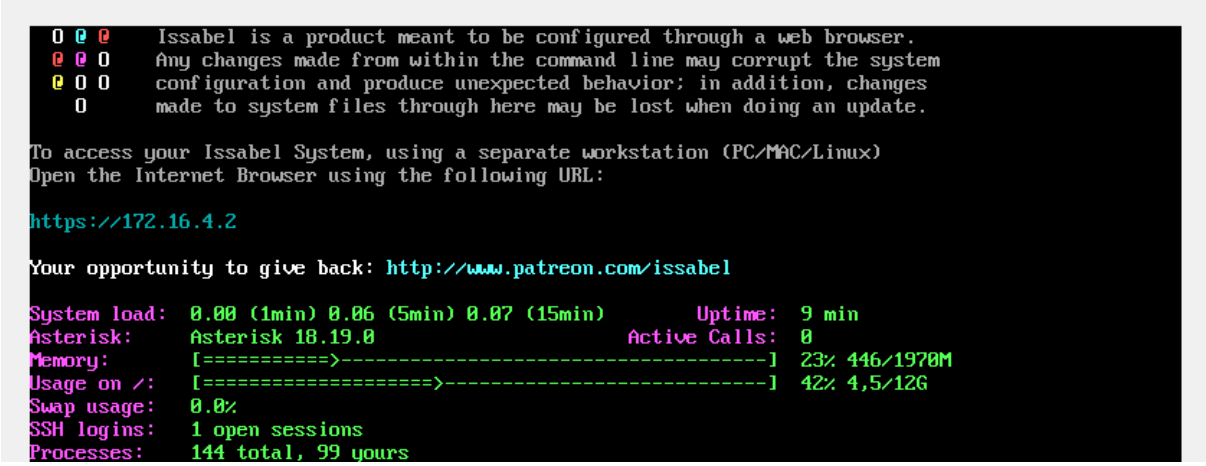
Las máquinas virtuales fueron configuradas con recursos específicos de CPU, memoria RAM, almacenamiento y conectividad de red, con el fin de garantizar un funcionamiento estable y evitar limitaciones por falta de recursos durante la generación de tráfico.

- **Servicio de VoIP**

Para la implementación del servicio de voz sobre IP se desplegó una máquina virtual dentro del entorno de virtualización. Esta máquina fue configurada con los recursos necesarios para soportar el procesamiento de llamadas y la gestión del tráfico de voz dentro de la red de pruebas.

Figura 104

Consola del servidor Issabel PBX ejecutándose sobre Rocky Linux.



A partir de esta configuración, se definieron los recursos virtuales necesarios para el funcionamiento del servidor de comunicaciones dentro del entorno de virtualización, considerando parámetros como el sistema operativo, la memoria asignada, el almacenamiento y la configuración de red utilizada para su integración dentro de la infraestructura virtual.

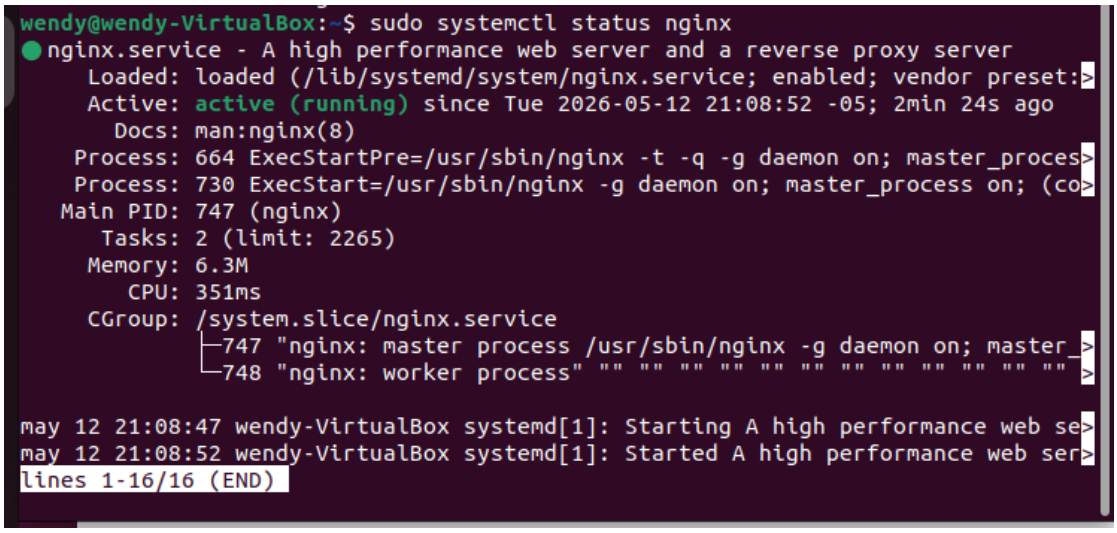
Posteriormente, se realizó la configuración de las extensiones SIP dentro del servidor Issabel PBX, permitiendo el registro de los dispositivos de usuario y la simulación de comunicaciones dentro del entorno virtualizado.

- **Streaming en tiempo real**

Para la implementación del servicio de streaming en tiempo real se desplegó una máquina virtual independiente dentro del entorno de virtualización. Esta máquina fue destinada a la transmisión de contenido multimedia en vivo dentro de la red de pruebas, con el propósito de generar tráfico de video en tiempo real y evaluar su comportamiento frente a los mecanismos de calidad de servicio aplicados en la infraestructura virtualizada.

Figura 105

Estado del servicio NGINX en el servidor de streaming en tiempo real.

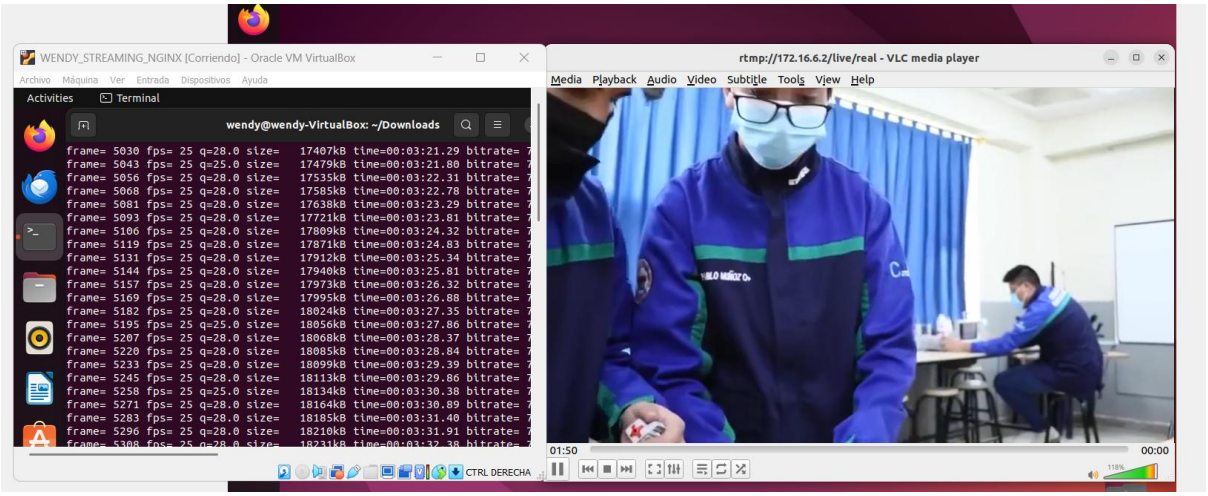


Posteriormente, se realizó la prueba de transmisión de video utilizando VLC Media Player. Como se muestra en la Figura 108, el flujo multimedia fue reproducido mediante la

dirección rtmp://172.16.2.1/live/real, lo que permitió comprobar la correcta entrega del contenido de video desde el servidor hacia el cliente dentro de la red de pruebas.

Figura 106

Estado del servicio NGINX en el servidor de streaming en tiempo real.



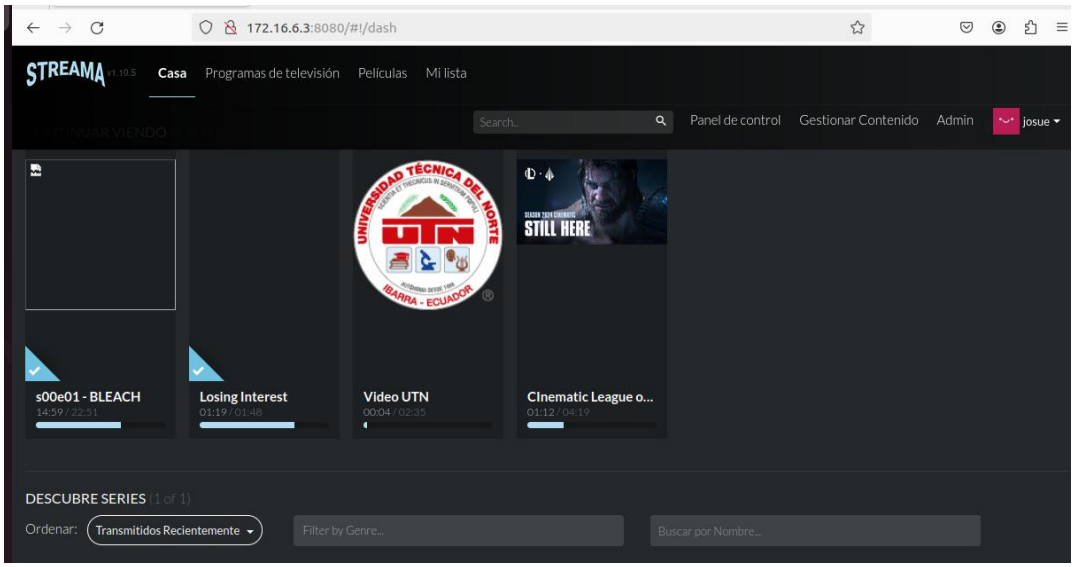
Con la puesta en marcha del servicio NGINX y la reproducción del flujo multimedia mediante VLC Media Player, se dejó operativo el servidor de streaming en tiempo real dentro del entorno virtualizado. Esta implementación servirá como base para la generación de tráfico multimedia en la fase experimental, donde se evaluará el comportamiento de la red frente a aplicaciones sensibles.

- **VoD (Streaming bajo demanda)**

Para el despliegue del servicio de VoD se siguió un procedimiento similar al aplicado en el servidor de streaming en tiempo real, considerando la creación de una máquina virtual independiente, la asignación de recursos virtuales y la integración a la VLAN de servicios multimedia. Sin embargo, este servicio se diferencia por estar orientado al alojamiento y reproducción de contenido multimedia previamente almacenado, simulando un escenario de video bajo demanda mediante la plataforma Streama.

Figura 107

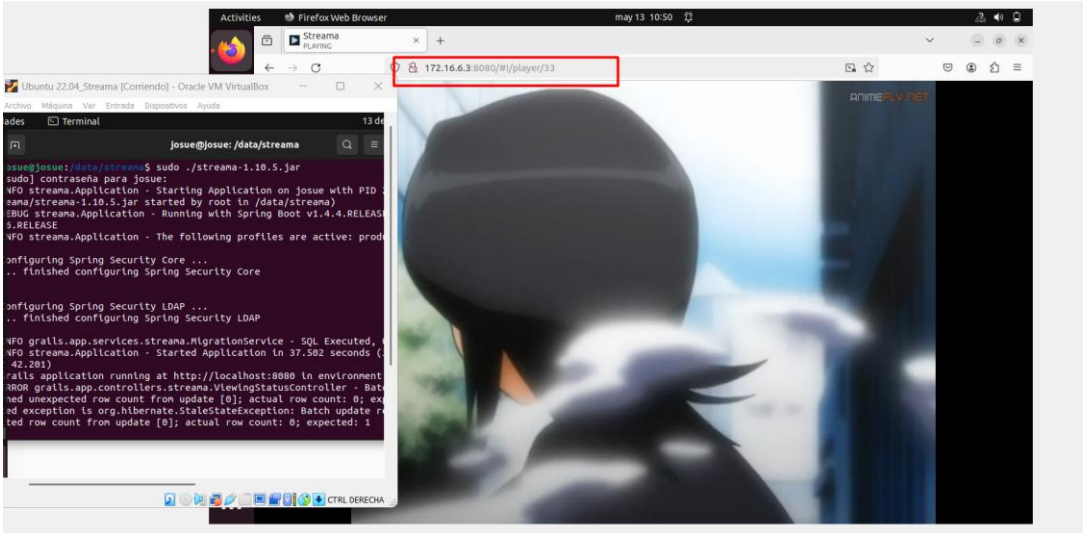
Interfaz web de la plataforma Streama para el servicio de VoD.



Posteriormente, se realizó la reproducción de un archivo multimedia previamente cargado en el servidor. Como se muestra a continuación, el contenido almacenado fue reproducido correctamente desde la plataforma Streama, comprobando la disponibilidad del servicio de video bajo demanda dentro del entorno virtualizado.

Figura 108

Reproducción de contenido multimedia almacenado mediante Streama.



Con la puesta en marcha de Streama, el servidor quedó habilitado para ofrecer contenido multimedia almacenado a los clientes de la red de pruebas. Esta implementación servirá como base para la generación de tráfico de video bajo demanda durante la fase experimental de evaluación de calidad de servicio.

- **Servicio de datos y soporte**

Además de los servicios multimedia, se incorporó un conjunto de servicios de datos y soporte con el propósito de representar funciones habituales dentro de una red institucional. Estos servicios permiten complementar el escenario experimental mediante tráfico generado por navegación web, transferencia de archivos, correo electrónico, acceso remoto, resolución de nombres y asignación dinámica de direcciones IP.

Para este grupo de servicios se estableció una configuración base de recursos virtuales, ajustada según las necesidades de cada servidor y las condiciones del entorno de pruebas.

Estos servicios cumplen un rol complementario dentro del escenario experimental, ya que permiten generar tráfico de datos y administración que será utilizado junto con los servicios multimedia durante la evaluación de calidad de servicio.

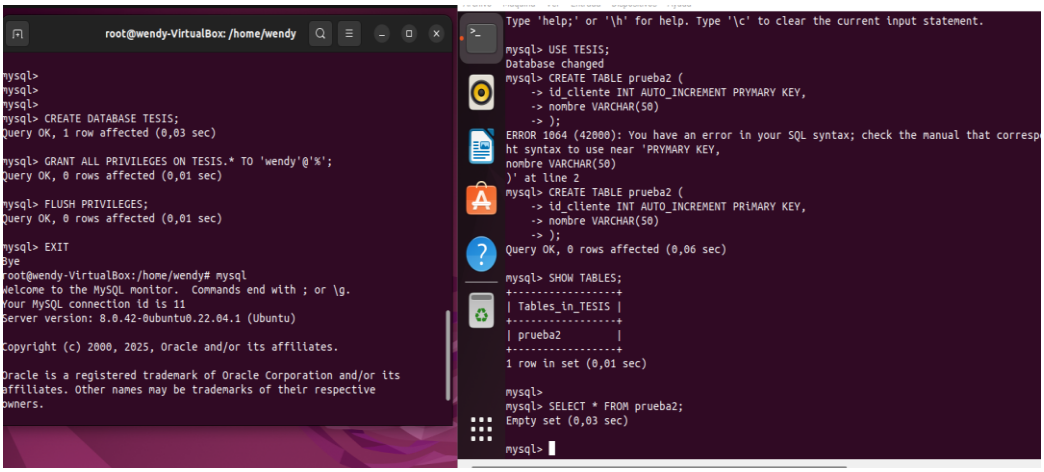
- **Base de Datos**

Para el servicio de base de datos se implementó MySQL, con la finalidad de permitir la gestión de información y la conexión remota desde los clientes de la red de pruebas. Este servicio permite incorporar tráfico transaccional dentro del escenario experimental, generado a partir de consultas, creación de tablas y operaciones básicas de lectura y escritura.

La comprobación del acceso remoto se realizó desde un equipo cliente, estableciendo conexión hacia el servidor MySQL mediante la dirección IP asignada. Como se muestra en la Figura 109

Figura 109

Conexión remota al servidor MySQL desde un cliente de la red virtualizada



Con esta configuración, el servicio de base de datos quedó disponible para generar tráfico asociado a consultas y operaciones de gestión de información durante la fase experimental de evaluación de calidad de servicio.

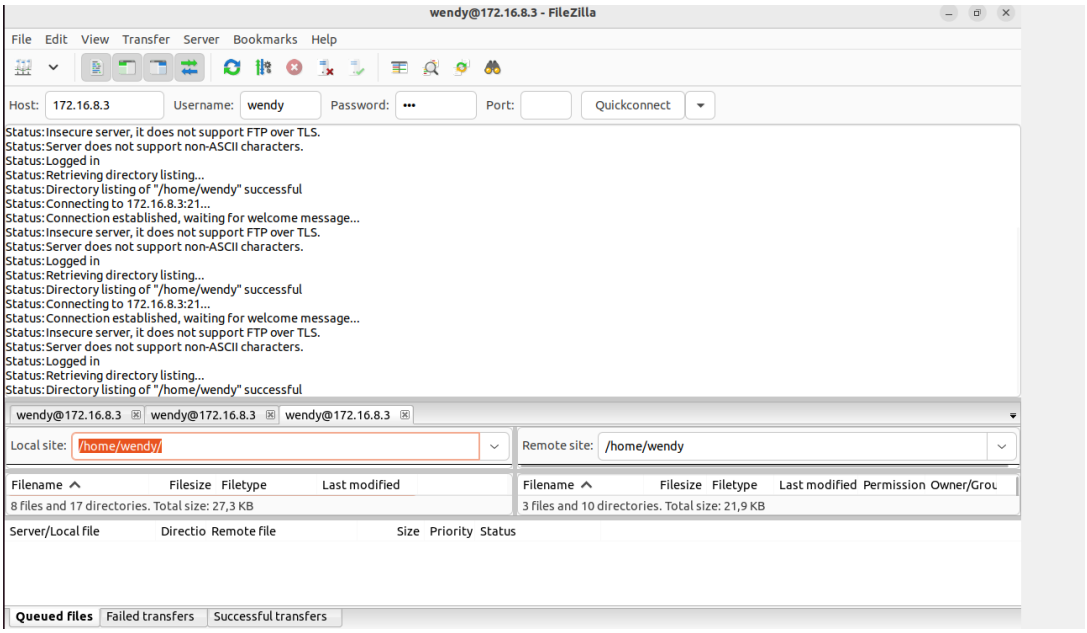
- **Transferencia de archivos FTP**

Para el servicio de transferencia de archivos se configuró un servidor FTP, con el propósito de permitir el intercambio de información entre los equipos cliente y el servidor dentro de la red de pruebas. Este servicio fue considerado dentro del grupo de datos y soporte, debido a que genera tráfico asociado a procesos de carga y descarga de archivos.

La validación del servicio se realizó mediante FileZilla Client, desde donde se estableció conexión hacia el servidor FTP utilizando la dirección IP asignada, el usuario configurado y el puerto correspondiente al servicio. Como se observa en la Figura 110, el cliente logró autenticarse correctamente y acceder a los directorios disponibles en el servidor.

Figura 110

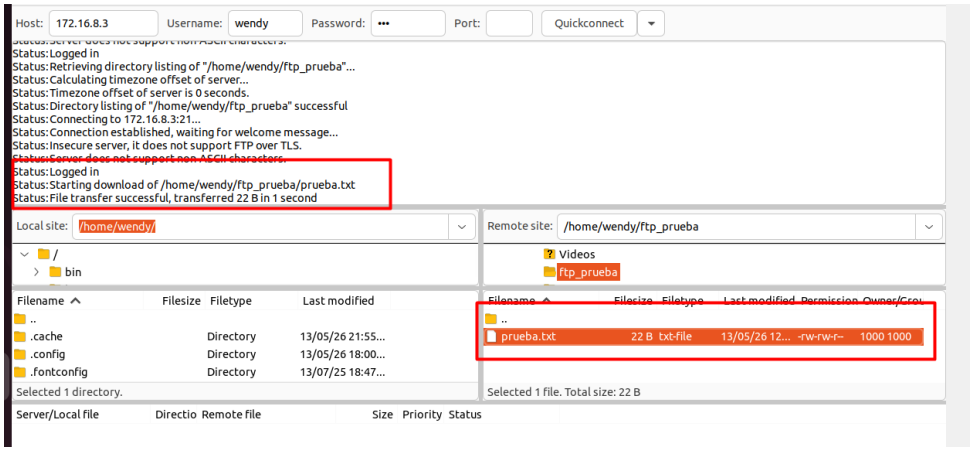
Conexión al servidor FTP mediante FileZilla Client.



A partir de esta conexión, el servicio quedó habilitado para realizar operaciones de carga y descarga de archivos entre el cliente y el servidor. Como se muestra en la Figura 111, la transferencia de archivos mediante FileZilla permite comprobar el intercambio de información dentro del entorno virtualizado.

Figura 111

Transferencia de archivos



Con la puesta en marcha del servicio FTP y su validación mediante FileZilla Client, se incorporó al escenario experimental un servicio capaz de generar tráfico de transferencia de

archivos. Este tráfico será utilizado durante la fase de evaluación de calidad de servicio para analizar el comportamiento de la red ante aplicaciones de intercambio de información.

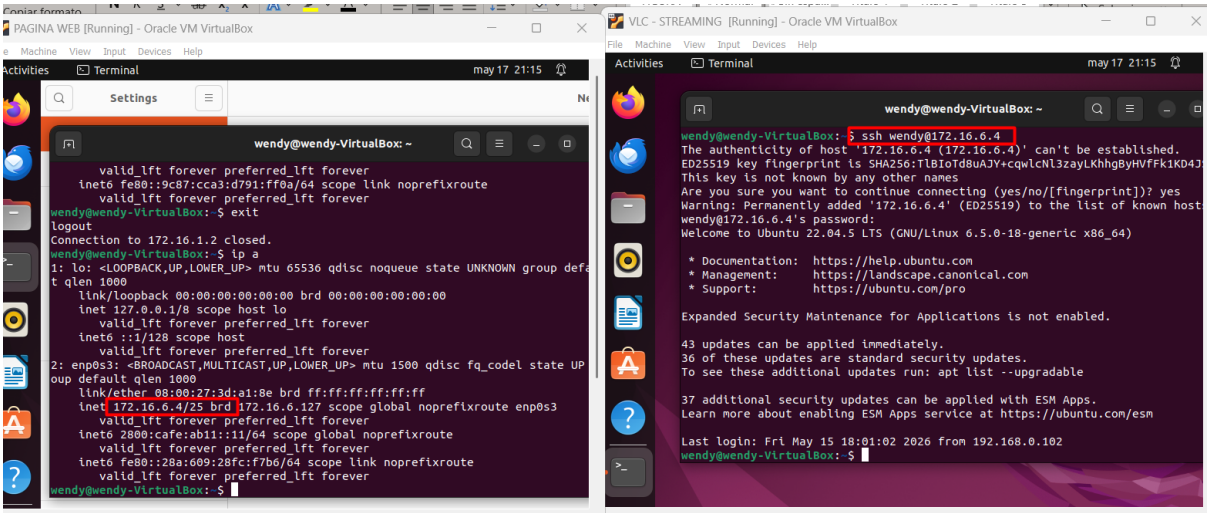
- **Acceso remoto SSH**

Para la administración remota del servidor se configuró el servicio SSH, con el propósito de permitir el acceso seguro a la terminal del servidor Ubuntu desde un equipo cliente dentro de la red de pruebas. Este servicio fue considerado dentro del grupo de datos y soporte, ya que permite realizar tareas de configuración, verificación y mantenimiento del servidor sin necesidad de acceder directamente a la máquina virtual.

La validación del servicio se realizó desde un equipo cliente mediante una conexión SSH hacia la dirección IP asignada al servidor, utilizando el usuario configurado y el puerto correspondiente al servicio. Como se observa en la Figura 112, el cliente logró establecer conexión correctamente con el servidor Ubuntu mediante el comando ssh wendy@172.16.6.4.

Figura 112

Conexión remota al servidor Ubuntu mediante SSH.



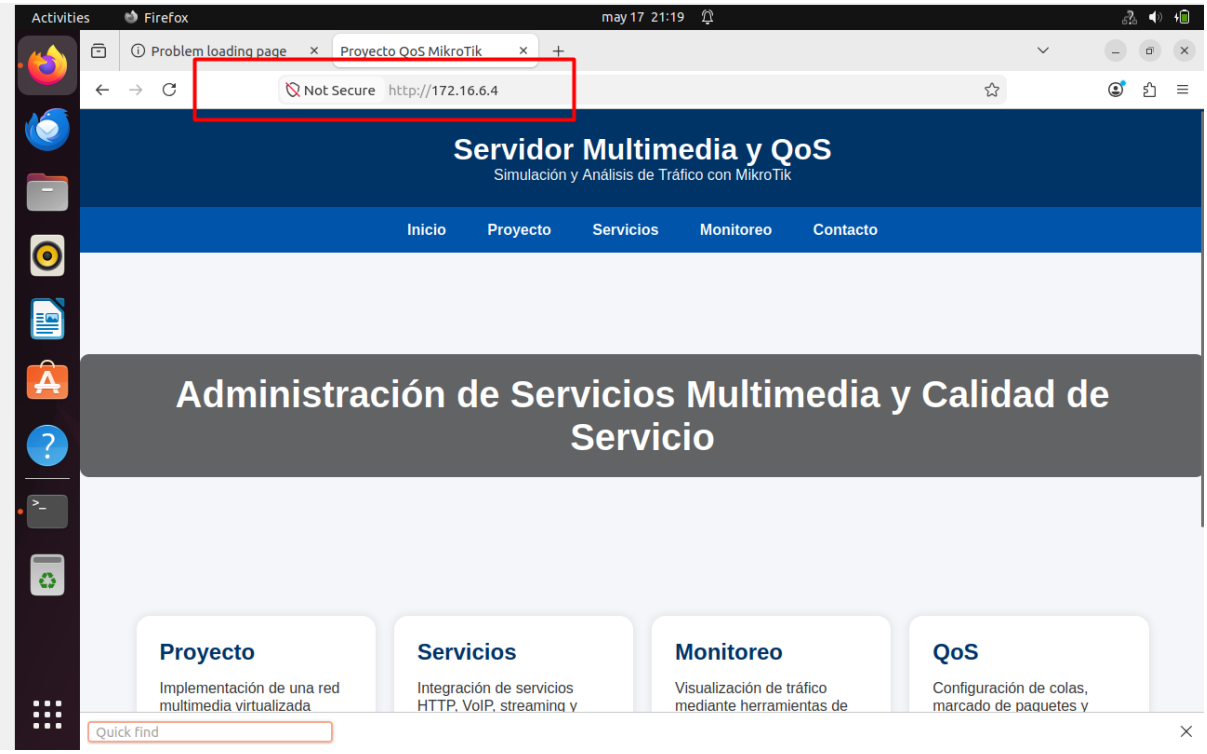
- **Navegación web**

Para el servicio de página web se configuró un servidor web en Ubuntu, con el propósito de permitir el acceso a contenido HTML desde los equipos cliente dentro de la red de pruebas. Este servicio fue considerado dentro del grupo de datos, ya que genera tráfico HTTP asociado a la consulta de páginas web.

La validación del servicio se realizó desde un equipo cliente mediante un navegador web, ingresando la dirección IP asignada al servidor: 172.16.6.2

Figura 113

Acceso a la página web desde el cliente.



- **Correo electrónico**

Para el servicio de correo electrónico se implementaron Postfix y Dovecot, con el propósito de habilitar el envío y recepción de mensajes dentro de la red de pruebas. Postfix fue utilizado para el servicio SMTP, asociado al puerto 25, mientras que Dovecot permitió el

acceso a los buzones mediante los protocolos POP3 e IMAP, correspondientes a los puertos 110 y 143.

Figura 114

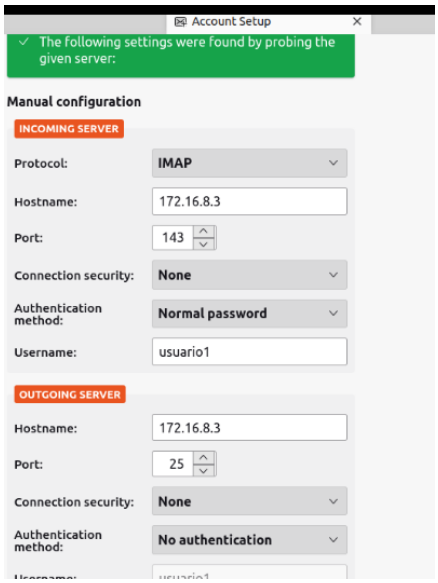
Verificación de los puertos SMTP, POP3 e IMAP en el servidor de correo electrónico.



Para validar el acceso desde un equipo cliente, se configuró la cuenta usuario1@tesis.local en Thunderbird, utilizando el protocolo IMAP para la recepción de mensajes y SMTP para el envío.

Figura 115

Configuración de cuenta de correo electrónico en Thunderbird.



Con esta configuración, el servicio de correo electrónico quedó habilitado para generar tráfico asociado al envío y recepción de mensajes durante la fase experimental de evaluación de calidad de servicio.

7.4 **Anexo D.** Configuración de marcas en RouterOs

- **Marcaje de conexiones en R3, R4 y R5**

Las reglas de mark-connection identifican conexiones nuevas y sin marca previa mediante protocol, src-port y dst-port de acuerdo con cada servicio. Se consideran de forma específica los flujos de MediaMTX, el canal FTP DATA y el tráfico generado por iPerf3.

Fase 1. Marcaje de conexiones

```
/ip firewall mangle
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp dst-port=10000-20000 action=mark-connection new-connection-
mark=voz-conn passthrough=yes comment="TESIS-QOS | VoIP RTP DST"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp src-port=10000-20000 action=mark-connection new-connection-
mark=voz-conn passthrough=yes comment="TESIS-QOS | VoIP RTP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp dst-port=5060 action=mark-connection new-connection-mark=sip-
conn passthrough=yes comment="TESIS-QOS | SIP UDP DST"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp src-port=5060 action=mark-connection new-connection-mark=sip-
conn passthrough=yes comment="TESIS-QOS | SIP UDP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=5060 action=mark-connection new-connection-mark=sip-
conn passthrough=yes comment="TESIS-QOS | SIP TCP"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp src-port=8000-8001 action=mark-connection new-connection-
mark=rtp-conn passthrough=yes comment="TESIS-QOS | MediaMTX RTP-RTCP SRC"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp dst-port=8000-8001 action=mark-connection new-connection-
mark=rtp-conn passthrough=yes comment="TESIS-QOS | MediaMTX RTP-RTCP DST"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=8554 action=mark-connection new-connection-mark=rtp-
conn passthrough=yes comment="TESIS-QOS | MediaMTX RTSP"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=8080 action=mark-connection new-connection-mark=vod-
conn passthrough=yes comment="TESIS-QOS | Streama VoD"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=3306 action=mark-connection new-connection-mark=bdd-
conn passthrough=yes comment="TESIS-QOS | MySQL"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=80 action=mark-connection new-connection-mark=web-
```

```
conn passthrough=yes comment="TESIS-QOS | HTTP"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=21,22,143 action=mark-connection new-connection-
mark=baja-conn passthrough=yes comment="TESIS-QOS | FTP SSH IMAP"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp src-port=20 action=mark-connection new-connection-mark=baja-
conn passthrough=yes comment="TESIS-QOS | FTP DATA"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=tcp dst-port=5201 action=mark-connection new-connection-
mark=iperf-conn passthrough=yes comment="TESIS-QOS | iPerf TCP"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp dst-port=5201 action=mark-connection new-connection-
mark=iperf-conn passthrough=yes comment="TESIS-QOS | iPerf UDP DST"
add chain=prerouting connection-state=new connection-mark=no-mark
protocol=udp src-port=5201 action=mark-connection new-connection-
mark=iperf-conn passthrough=yes comment="TESIS-QOS | iPerf UDP_SRC"
```

- **Modificación del campo DSCP**

Cada connection-mark se utiliza para escribir el valor DSCP correspondiente. iPerf3 recibe CS1/8 y el tráfico no clasificado se mantiene en CS0/0.

Fase 2. Modificación del campo DSCP

```
/ip firewall mangle
add chain=prerouting connection-mark=voz-conn action=change-dscp new-
dscp=46 passthrough=yes comment="TESIS-QOS | VoIP RTP -> EF46"
add chain=prerouting connection-mark=sip-conn action=change-dscp new-
dscp=24 passthrough=yes comment="TESIS-QOS | SIP -> CS3"
add chain=prerouting connection-mark=rtp-conn action=change-dscp new-
dscp=34 passthrough=yes comment="TESIS-QOS | Streaming -> AF41"
add chain=prerouting connection-mark=vod-conn action=change-dscp new-
dscp=38 passthrough=yes comment="TESIS-QOS | VoD -> AF43"
add chain=prerouting connection-mark=bdd-conn action=change-dscp new-
dscp=26 passthrough=yes comment="TESIS-QOS | MySQL -> AF31"
add chain=prerouting connection-mark=web-conn action=change-dscp new-
dscp=18 passthrough=yes comment="TESIS-QOS | HTTP -> AF21"
add chain=prerouting connection-mark=baja-conn action=change-dscp new-
dscp=0 passthrough=yes comment="TESIS-QOS | Best Effort -> CS0"
add chain=prerouting connection-mark=iperf-conn action=change-dscp new-
dscp=8 passthrough=yes comment="TESIS-QOS | iPerf -> CS1"
add chain=prerouting connection-mark=no-mark action=change-dscp new-dscp=0
passthrough=yes comment="TESIS-QOS | Default -> CS0"
```

- **Marcaje de paquetes**

Las packet-mark se utilizan localmente para vincular el tráfico con Queue Tree. El esquema de marcas incluye iperf-pkt y default-pkt, además de las marcas de los servicios.

Fase 3. Marcaje de paquetes

```
/ip firewall mangle
add chain=prerouting connection-mark=voz-conn action=mark-packet new-
packet-mark=voz-pkt passthrough=no comment="TESIS-QOS | Packet VoIP RTP"
add chain=prerouting connection-mark=sip-conn action=mark-packet new-
packet-mark=sip-pkt passthrough=no comment="TESIS-QOS | Packet SIP"
add chain=prerouting connection-mark=rtp-conn action=mark-packet new-
packet-mark=rtp-pkt passthrough=no comment="TESIS-QOS | Packet Streaming
RTP"
add chain=prerouting connection-mark=vod-conn action=mark-packet new-
packet-mark=vod-pkt passthrough=no comment="TESIS-QOS | Packet VoD"
add chain=prerouting connection-mark=bdd-conn action=mark-packet new-
packet-mark=bdd-pkt passthrough=no comment="TESIS-QOS | Packet MySQL"
add chain=prerouting connection-mark=web-conn action=mark-packet new-
packet-mark=web-pkt passthrough=no comment="TESIS-QOS | Packet HTTP"
add chain=prerouting connection-mark=baja-conn action=mark-packet new-
packet-mark=baja-pkt passthrough=no comment="TESIS-QOS | Packet Best
Effort"
add chain=prerouting connection-mark=iperf-conn action=mark-packet new-
packet-mark=iperf-pkt passthrough=no comment="TESIS-QOS | Packet iPerf"
add chain=prerouting packet-mark=no-mark action=mark-packet new-packet-
mark=default-pkt passthrough=no comment="TESIS-QOS | Packet Default"
```

Las tres fases conforman el proceso de clasificación y marcaje aplicado en R3, R4 y R5, permitiendo identificar las conexiones, establecer el valor DSCP y generar las marcas de paquete utilizadas por Queue Tree.

- **Alcance de la configuración de marcaje**

El proceso de marcaje se aplica en R3, R4 y R5. Estos equipos realizan la clasificación por protocolo y puerto, la asignación del valor DSCP y la generación de las packet-mark correspondientes. R1 y R2 se emplean como routers de tránsito y no generan nuevas connection-mark o packet-mark a partir del campo DSCP. La validación en estos equipos se orienta a comprobar el encaminamiento del tráfico y la conservación de la clasificación DiffServ. La conservación del DSCP durante el tránsito puede verificarse con Torch o Wireshark, pero debe distinguirse de la creación de marcas internas de RouterOS.

7.5 **Anexo E.** Configuración de colas

- **Configuración de Queue Tree en R5**

El árbol de colas se aplica sobre ether5 de R5. La jerarquía está formada por los tipos de cola PFIFO y PCQ, la cola principal QoS-Total, la clase agregada SERVIDORES y las colas correspondientes a los servicios, iPerf Background y Default.

Tipos de cola y Queue Tree

```
/queue type
add kind=pfifo name=RTP-pfifo pfifo-limit=30
add kind=pfifo name=REALTIME-pfifo pfifo-limit=30
add kind=pcq name=QoS-pcq pcq-classifier=src-address,dst-address,src-
port,dst-port
/queue tree
add name="QoS-Total" parent=ether5 max-limit=900k
add name="SERVIDORES" parent="QoS-Total" priority=1 limit-at=700k max-
limit=900k
add name="1. VoIP RTP" parent="SERVIDORES" packet-mark=voz-pkt priority=1
limit-at=0 max-limit=900k queue=REALTIME-pfifo
add name="2. SIP" parent="SERVIDORES" packet-mark=sip-pkt priority=2
limit-at=0 max-limit=900k queue=REALTIME-pfifo
add name="3. Streaming RTP" parent="SERVIDORES" packet-mark=rtp-pkt
priority=3 limit-at=0 max-limit=900k queue=RTP-pfifo
add name="4. Streaming VoD" parent="SERVIDORES" packet-mark=vod-pkt
priority=4 limit-at=0 max-limit=900k queue=QoS-pcq
add name="5. MySQL" parent="SERVIDORES" packet-mark=bdd-pkt priority=5
limit-at=0 max-limit=900k queue=QoS-pcq
add name="6. HTTP" parent="SERVIDORES" packet-mark=web-pkt priority=6
limit-at=0 max-limit=900k queue=QoS-pcq
add name="7. Best Effort" parent="SERVIDORES" packet-mark=baja-pkt
priority=7 limit-at=0 max-limit=900k queue=QoS-pcq
add name="8. iPerf Background" parent="QoS-Total" packet-mark=iperf-pkt
priority=8 limit-at=0 max-limit=900k queue=QoS-pcq
add name="9. Default" parent="QoS-Total" packet-mark=default-pkt
priority=8 limit-at=0 max-limit=900k queue=QoS-pcq
```

7.6 **Anexo F.** Verificación de la configuración del campo DSCP

Las figuras incluidas en este anexo presentan las capturas realizadas en el punto de salida del tráfico, donde se inspecciona el campo DS de la cabecera IP. En este campo se observa el valor DSCP correspondiente a la clase de servicio de cada paquete, lo que permite verificar que el

marcaje configurado en RouterOS se conserva durante el proceso de reenvío y se refleja correctamente en el tráfico que circula por la red.

Figura 116

Marcaje en paquetes UDP al servicio en VoIP (Voz RTP)

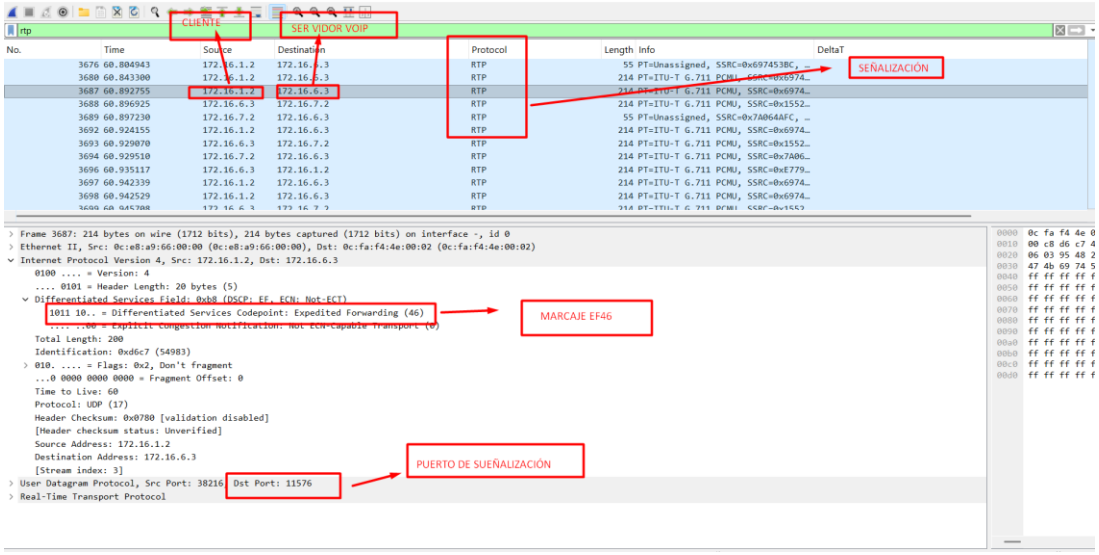


Figura 117

Marcaje en paquetes UDP al servicio en VoIP (Establecimiento llamada)

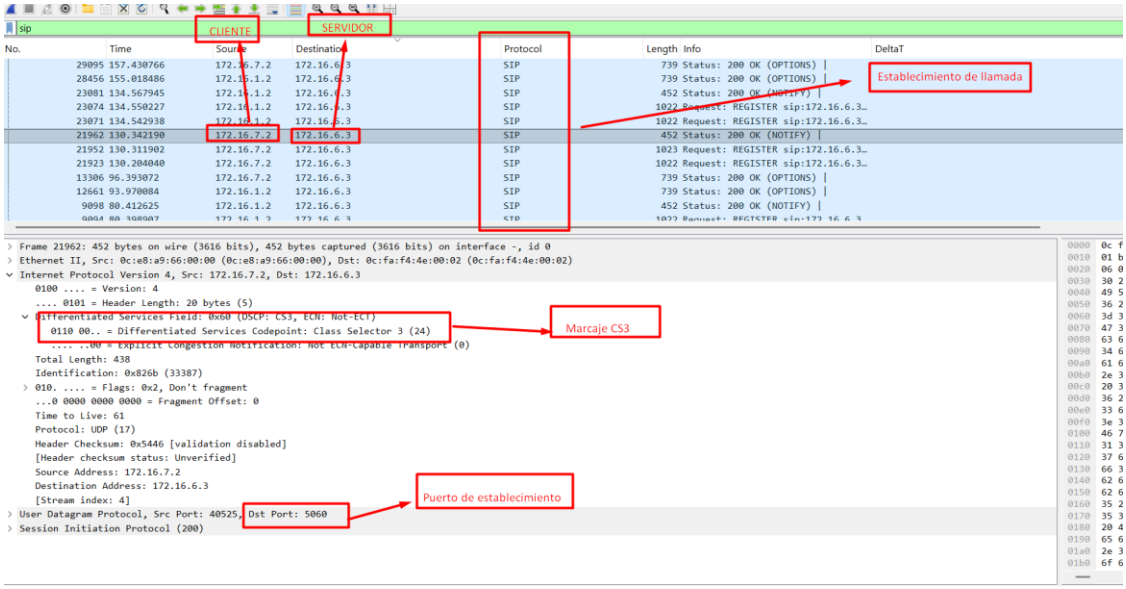


Figura 118

Marcaje en paquetes UDP al servicio en Streaming en tiempo real

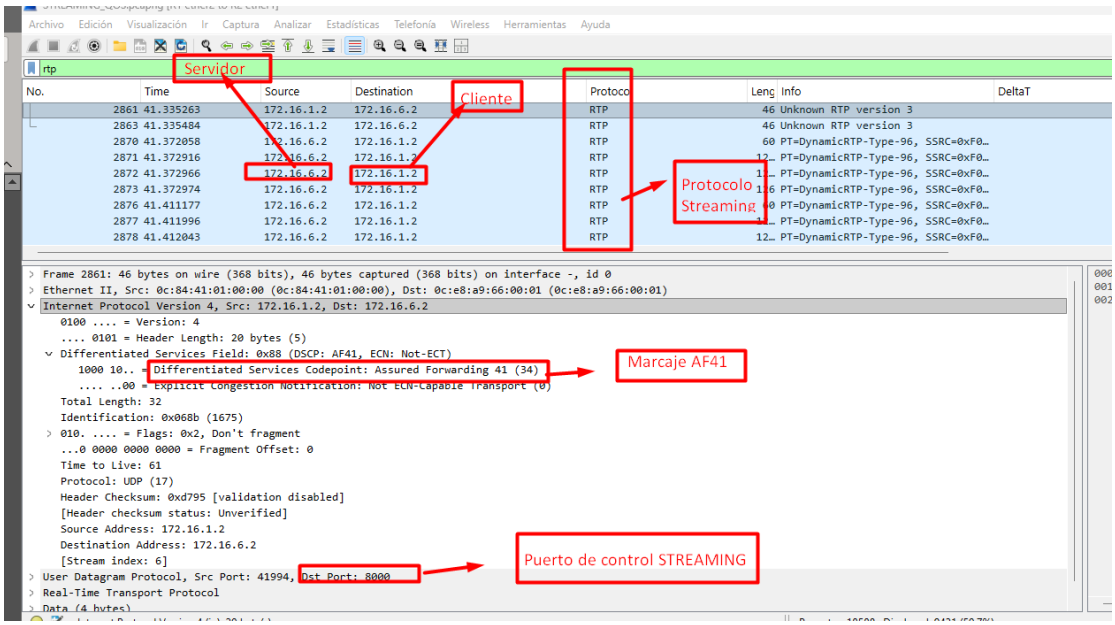


Figura 119

Marcaje en paquetes TCP al servicio en VOD

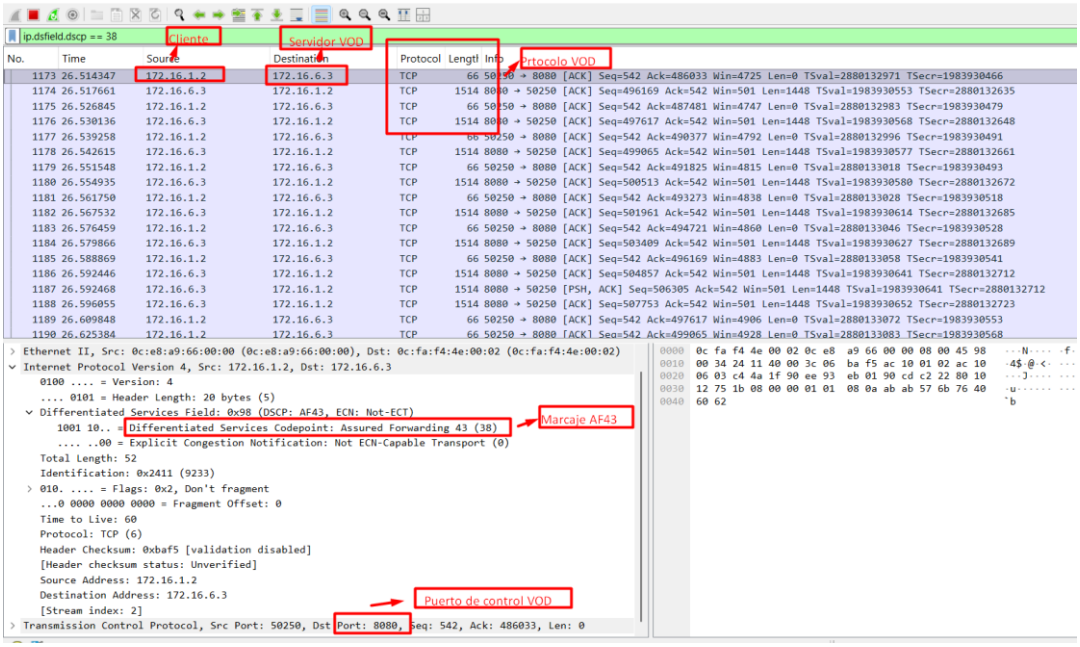


Figura 120

Marcaje en paquetes TCP al servicio en BBDD

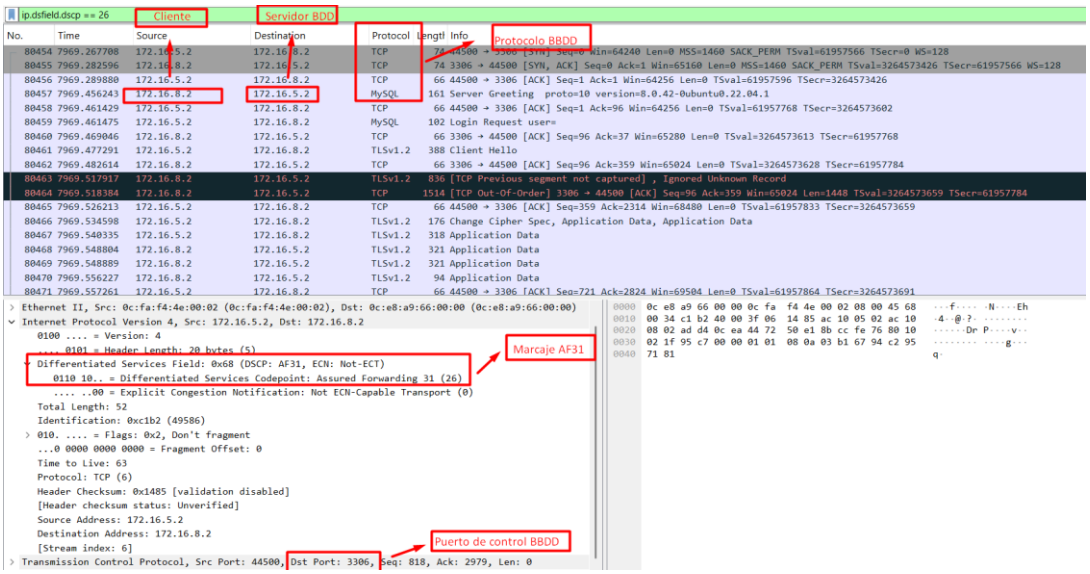


Figura 121

Marcaje en paquetes TCP al servicio en WEB

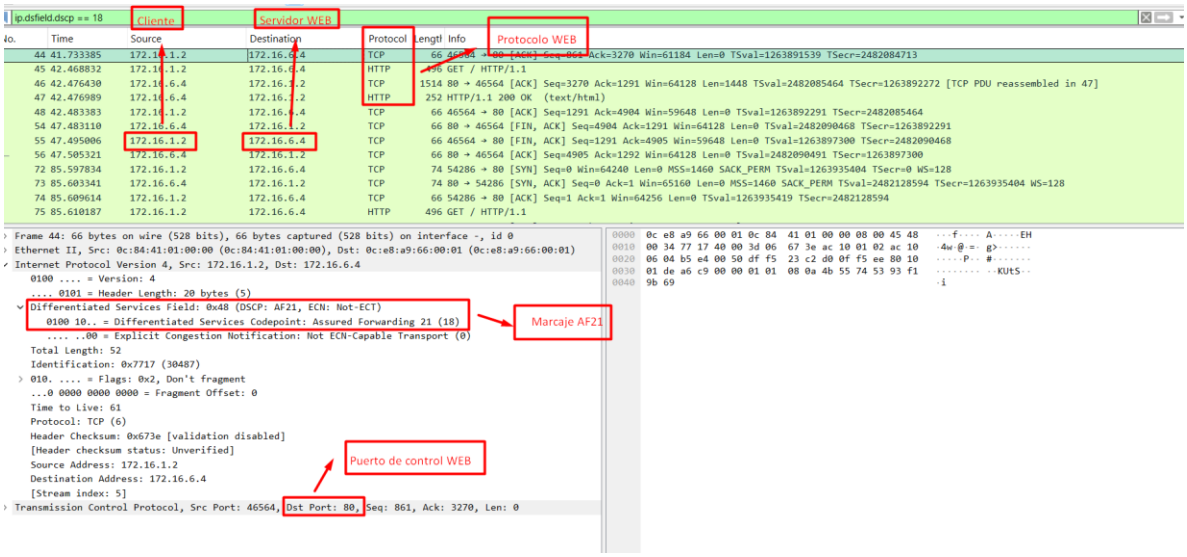


Figura 122

Marcaje en paquetes TCP al servicio en SSH

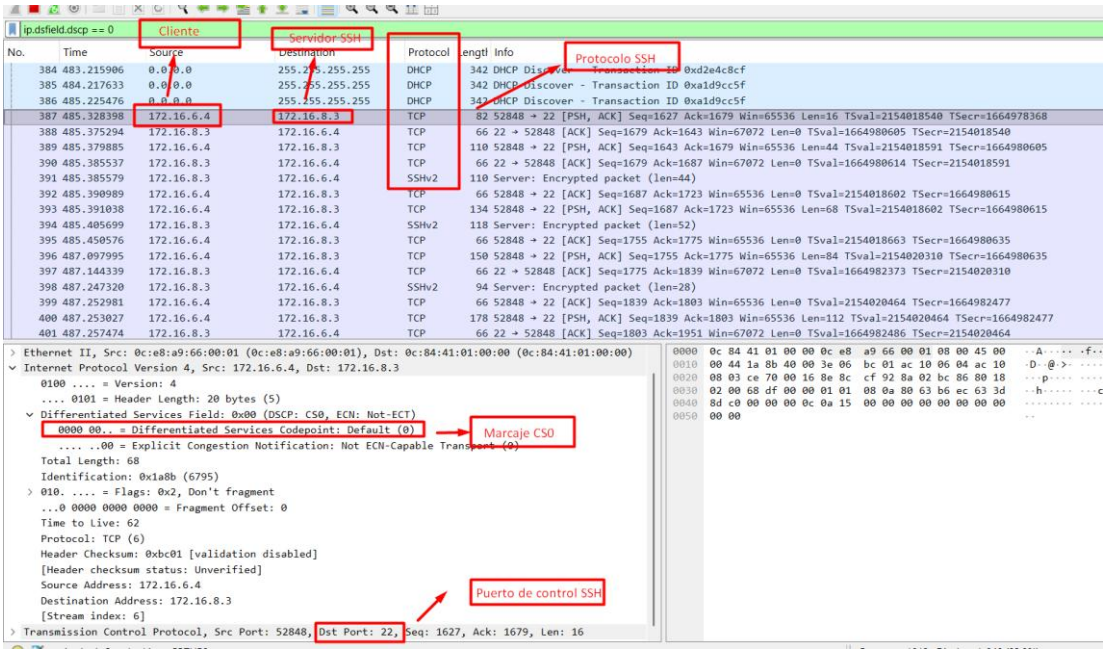


Figura 123

Marcaje en paquetes TCP al servicio en FTP

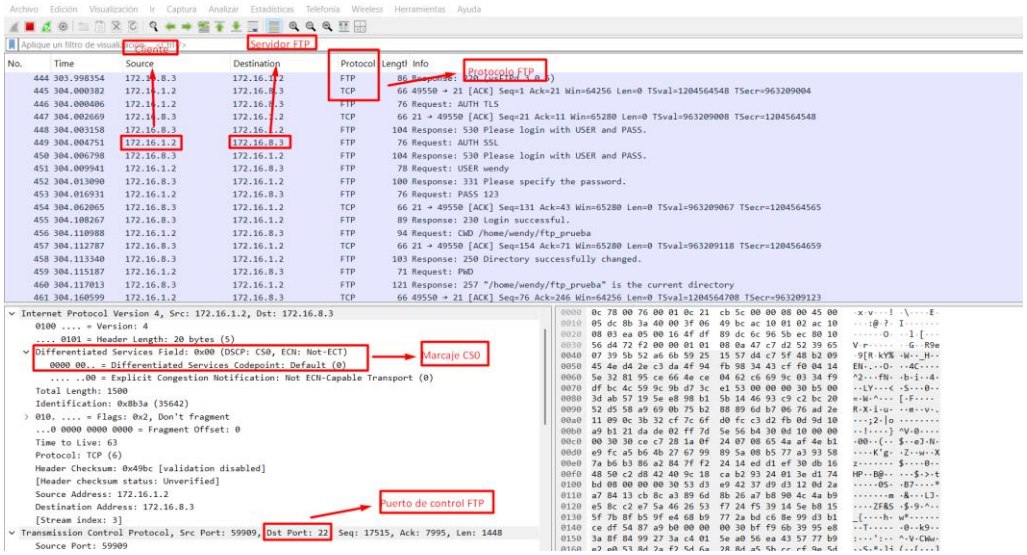
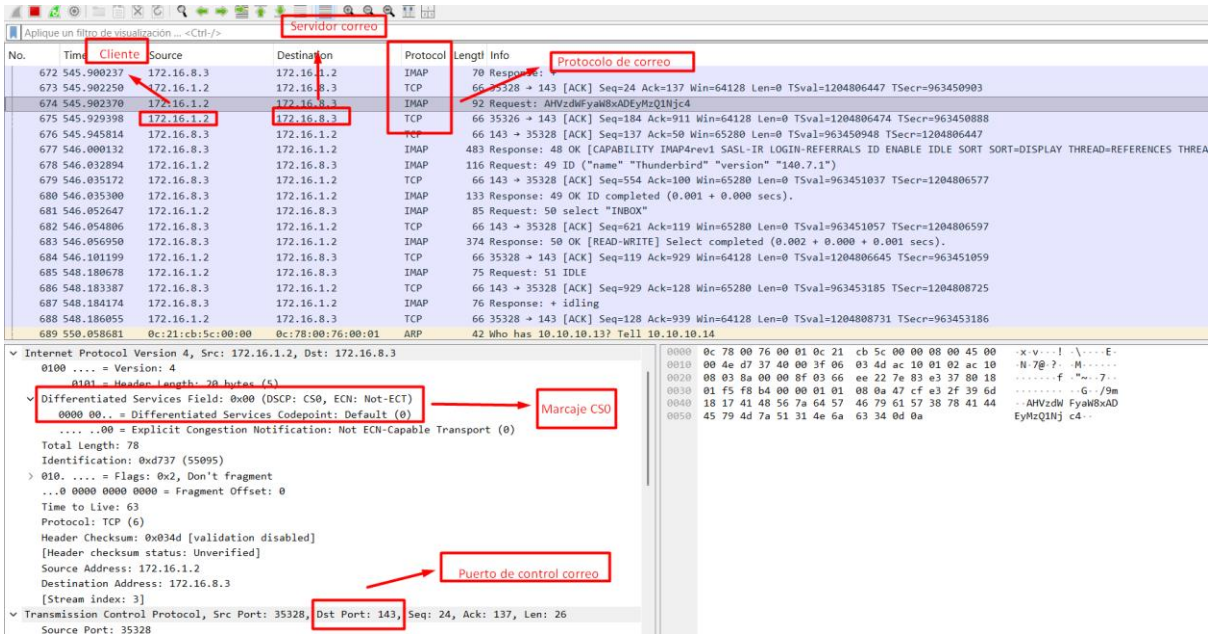


Figura 124

Marcaje en paquetes TCP al servicio en Correo



7.7 **Anexo G.** Carpeta de pruebas

TESIS_LUNAWENDY