



Universidad
Nacional
de Loja

Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos

Naturales No Renovables

Maestría en Telecomunicaciones

**Comparación de las soluciones DIFFSERV (Servicios Diferenciados) E INTSERV
(Servicios Integrados) para proveer Calidad de Servicio QoS en redes LAN
Inalámbricas.**

**Trabajo de Titulación previo a la
obtención del título de Magister
en Telecomunicaciones.**

AUTOR:

Ing. Eduardo Samuel Montalván Celi

DIRECTOR:

Ing. Marco Augusto Suing Ochoa Mg. Sc.

Loja – Ecuador

2023

Certificación

Loja, abril de 2023

Ing. Marco Augusto Suing Ochoa Mg. Sc.

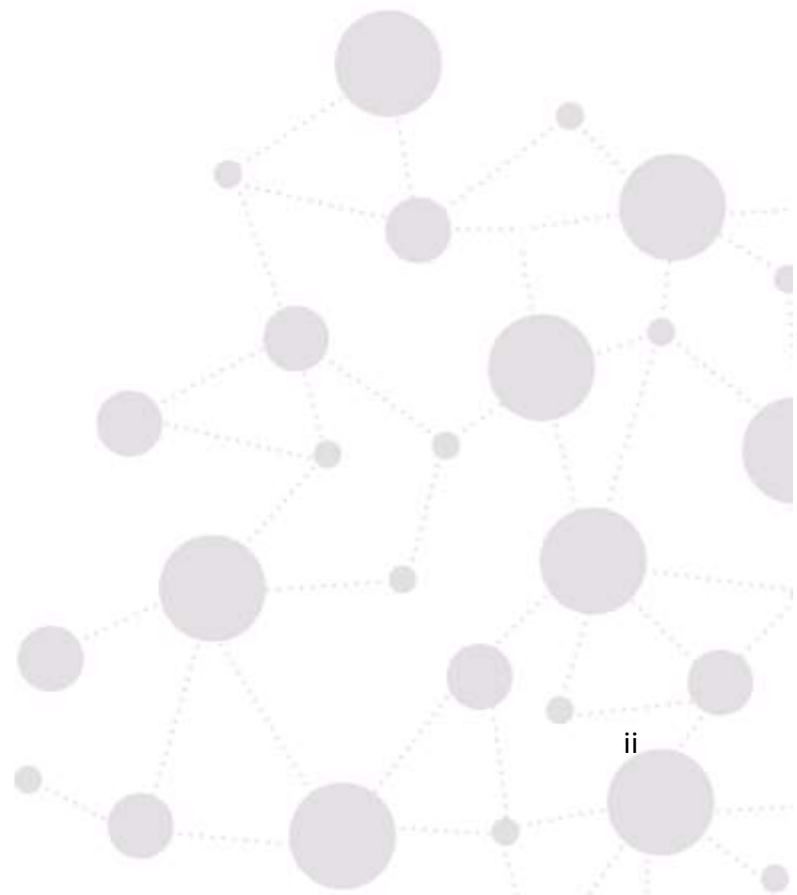
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Comparación de las Soluciones Diffserv (Servicios Diferenciados) E Intserv (Servicios Integrados) para proveer Calidad De Servicio Qos en Redes LAN Inalámbricas**, previo a la obtención del título de **Magíster en Telecomunicaciones**, de autoría del estudiante **Eduardo Samuel Montalván Celi**, con **cédula de identidad N° 11046201676**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Ing. Marco Augusto Suing Ochoa Mg. Sc.

DIRECTOR DE TRABAJO DE TITULACIÓN





Autoría

Yo, **Eduardo Samuel Montalván Celi**, declaro ser autor del trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

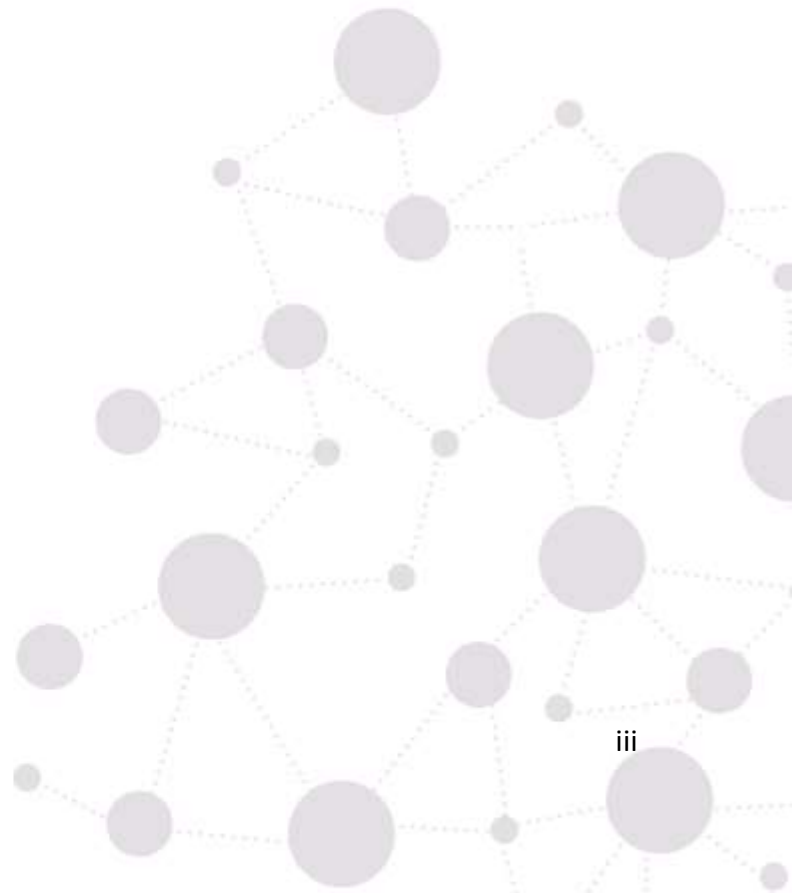
Firma:

Cédula de Identidad: 1104201676

Fecha: 31/05/2023

Correo electrónico: eduardo.montalvan@unl.edu.ec

Teléfono: 0982456959





Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Eduardo Samuel Montalván Celi**, declaro ser autor del Trabajo de Titulación denominado: **Comparación De Las Soluciones Diffserv (Servicios Diferenciados) E Intserv (Servicios Integrados) Para Proveer Calidad De Servicio Qos En Redes LAN Inalámbricas**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los treinta y un días del mes de mayo de dos mil veintitrés.

Firma:

Autor: Eduardo Samuel Montalván Celi

Cédula: 1104201676

Dirección: Loja, Cdla. Daniel Álvarez Burneo

Correo Electrónico: eduardo.montalvan@unl.edu.ec

Celular: 0982456959

DATOS COMPLEMENTARIOS:

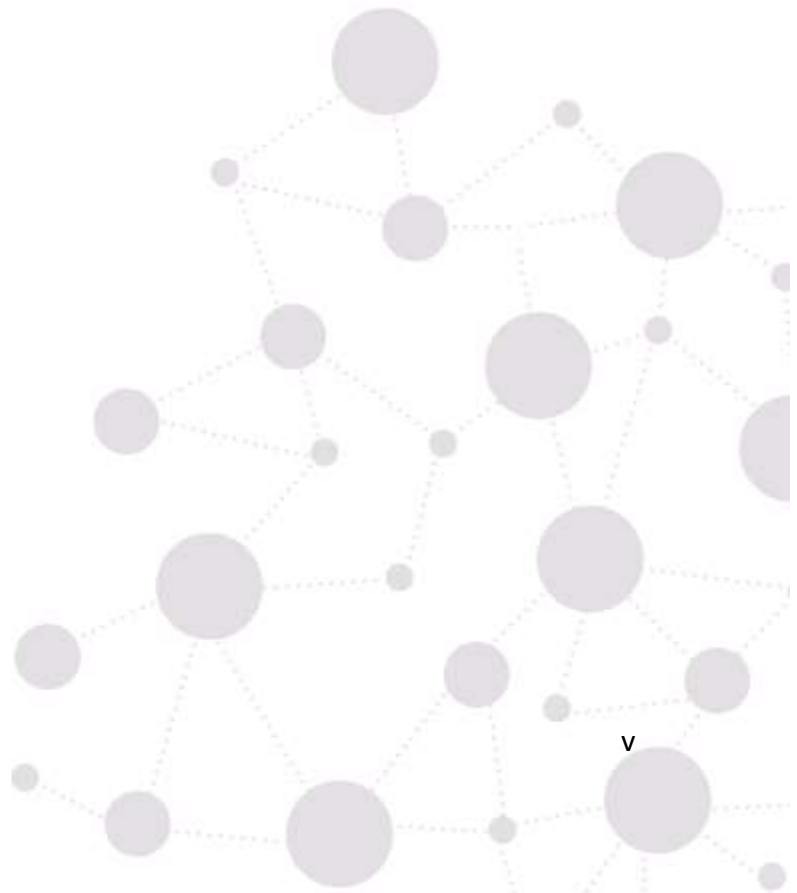
Director de trabajo de investigación: Ing. Marco Augusto Suing Ochoa Mg. Sc.



Dedicatoria

El presente trabajo de investigación está dedicado en primer lugar a Dios quien me ha dado fortaleza y entendimiento para culminar este nuevo reto en mi carrera profesional, en segundo lugar, a mi esposa quién ha sido un apoyo incondicional en todo momento, a mis hijas que son los luceros de mi corazón, a mis padres quienes siempre han sido guía en mi camino y a mis hermanos que me han dado siempre su cariño y respaldo.

Eduardo Samuel Montalván Celi





Agradecimiento

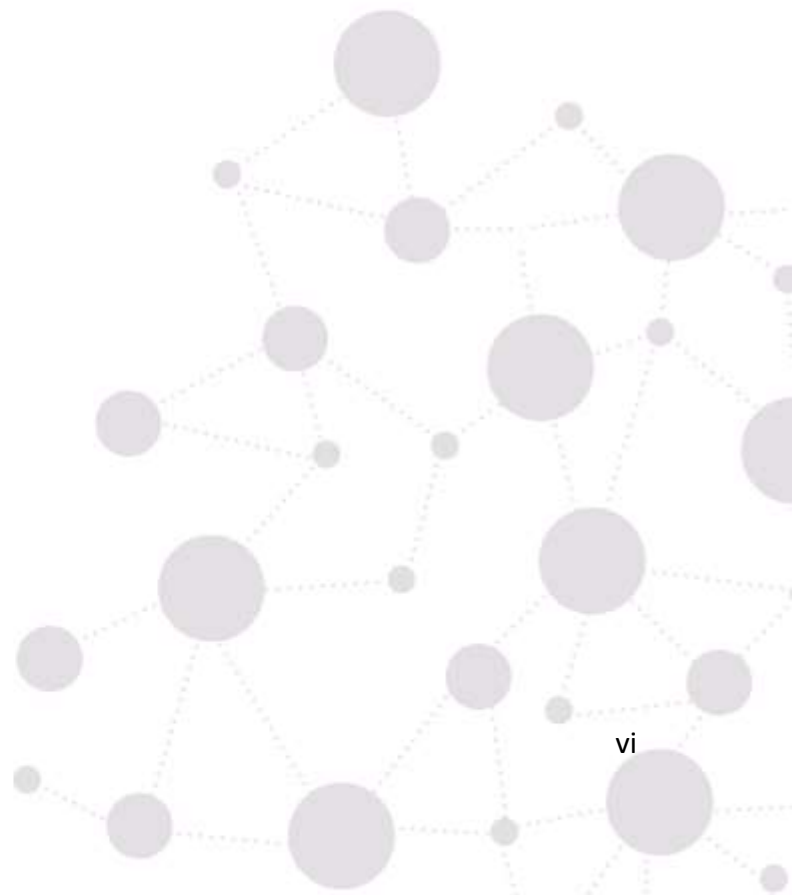
Agradezco a Dios, en primera instancia.

Agradezco a el motor y la luz de mi vida, Alex, Helen y Alice, mis hijos.

A mi esposa, por ser la persona que siempre creyó en mí y ha estado conmigo desde el comienzo de mis estudios.

A todas las personas que confiaron en la exitosa culminación de este reto académico y siempre estuvieron respaldándome.

Eduardo Samuel Montalván Celi





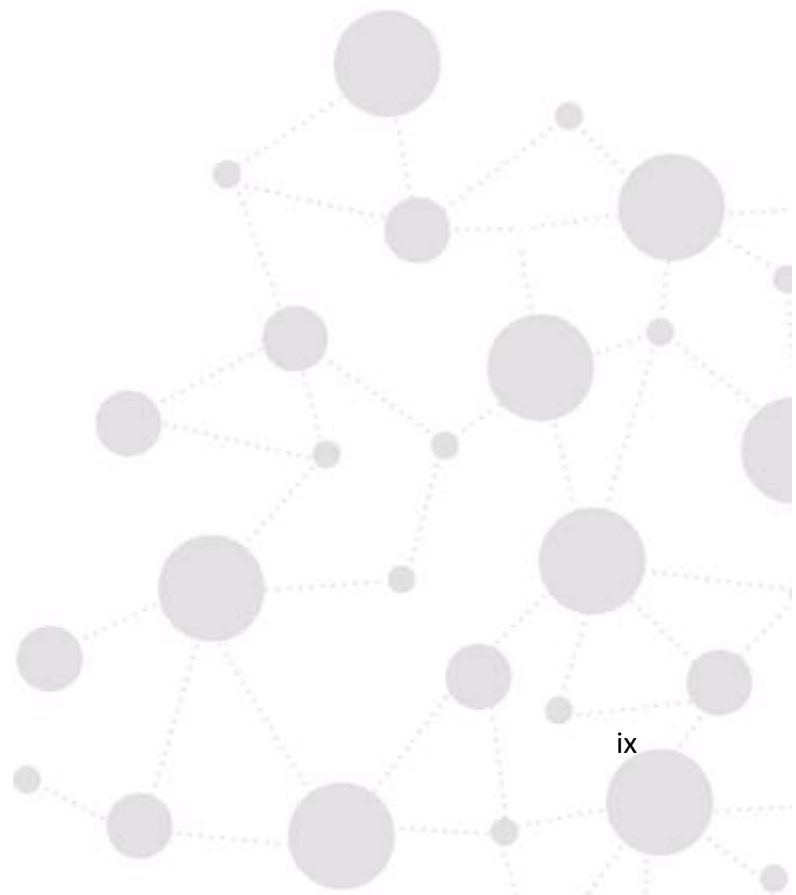
Índice de Contenidos

Certificación	ii
Autoría.....	iii
Carta de autorización.....	iv
Dedicatoria	v
Agradecimiento.....	vi
Índice de Contenidos.....	vii
Índice de tablas	x
Índice de figuras	xi
Índice de anexos.....	xiii
1. Titulo	1
2. Resumen	2
2.1 Abstract	5
3. Introducción.....	7
3.1 Problema de Investigación y Objetivos.....	8
4. Marco Teórico.....	10
4.1 Antecedentes Sobre La Calidad De Servicio En Redes Inalámbricas	10
4.2 Redes De Datos	11
4.2.1 Redes De Área Amplia WAN	12
4.2.2 Redes De Área Metropolitana (MAN).....	13
4.2.3 Redes de área local (LAN)	14
4.2.4 Redes Inalámbricas (WLAN).....	15
4.2.4.1 Tipos De Redes Inalámbricas	16
4.3 Estándares 802.11 WLAN.....	17
4.4 IEEE 802.11e.....	19
4.4.1 El Acceso Distribuido En 802.11 Y 802.11e.....	19
4.4.2 Carencias De 802.11	20
4.4.3 El Modo EDCA	20
4.5 La Calidad De Servicio En Redes De Computadoras.....	21

4.5.1 Priorización del tráfico	22
4.5.2 Pérdida De Paquetes.....	23
4.5.3 Características De Tráfico (Voz, Vídeo Y Datos).....	24
4.5.3.1 Voz.....	24
4.5.3.2. Video	25
4.5.3.3 Datos	25
4.5.4. Algoritmos De Formación De Colas	26
4.5.4.1 First In First Out (FIFO).....	27
4.5.4.2 Weighted Fair Queuing (WFQ).....	27
4.5.4.3 Class-Based Weighted Fair Queuing (CBWFQ)	29
4.5.4.4 Low Latency Queuing (LLQ).....	30
4.5.5 Proceso General de Qos y Secuencia De Operación Sobre El Flujo De Paquetes.....	31
4.5.5.1 Clasificación y Marcación.....	31
4.5.5.2 Marcado De Tráfico En Capa 2.....	32
4.5.5.3 Marcado De Tráfico En Capa 3.....	32
4.5.5.4. Mapeo De Marcado De Capa 2 A Capa 3.....	36
4.6 Definición Y Características De La Calidad De Servicio En Redes Inalámbricas	37
4.6.1 Intserv (Servicios Integrados)	39
4.6.2 Diffserv (Servicios Diferenciados)	41
4.6.2.1 Clases De Servicio.....	43
4.6.3 Ventajas Y Desventajas De Cada Solución	46
4.6.3.1 Diffserv. Ventajas Y Desventajas.....	46
4.6.3.2 Intserv. Ventajas y Desventajas	47
4.6.4 Técnicas Y Herramientas Para Evaluar Los Métodos Diffserv E Intserv	48
5. Metodología	50
5.1 Simulación De Priorización De Tráfico.....	52
5.1.1 Análisis Del Campo DSCP En Las Cabeceras IP Sin Aplicar Políticas De Qos	52
5.1.2 Análisis del campo DSCP en las cabeceras IP aplicando políticas de QoS	57



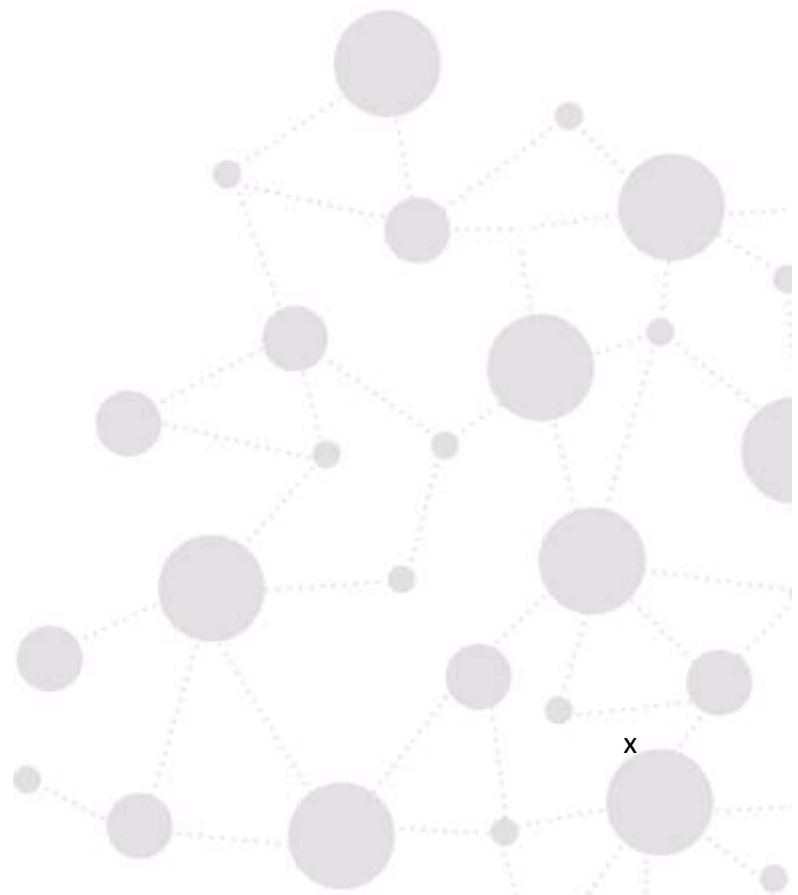
5.1.2.1 Clasificación, Mercado Y Política Del Tráfico En El Router 1.....	57
5.1.2.2 Aplicación De Política En El Router 2	57
6. Resultados	64
6.1 Investigación 1.	64
6.2 Investigación 2.	68
6.3 Investigación 3.	71
7. Discusión	76
8. Conclusiones	78
9. Recomendaciones	80
10. Bibliografía	81
11. Anexos.....	84





Índice de tablas:

Tabla 1. Estándares 802.11	17
Tabla 2. Características del tráfico de voz	24
Tabla 3. Características del tráfico de video	25
Tabla 4. Características del tráfico de datos	25
Tabla 5. Factores del tráfico	26
Tabla 6. Formas de marcado	31
Tabla 7. Marcado de tráfico en capa 2	32



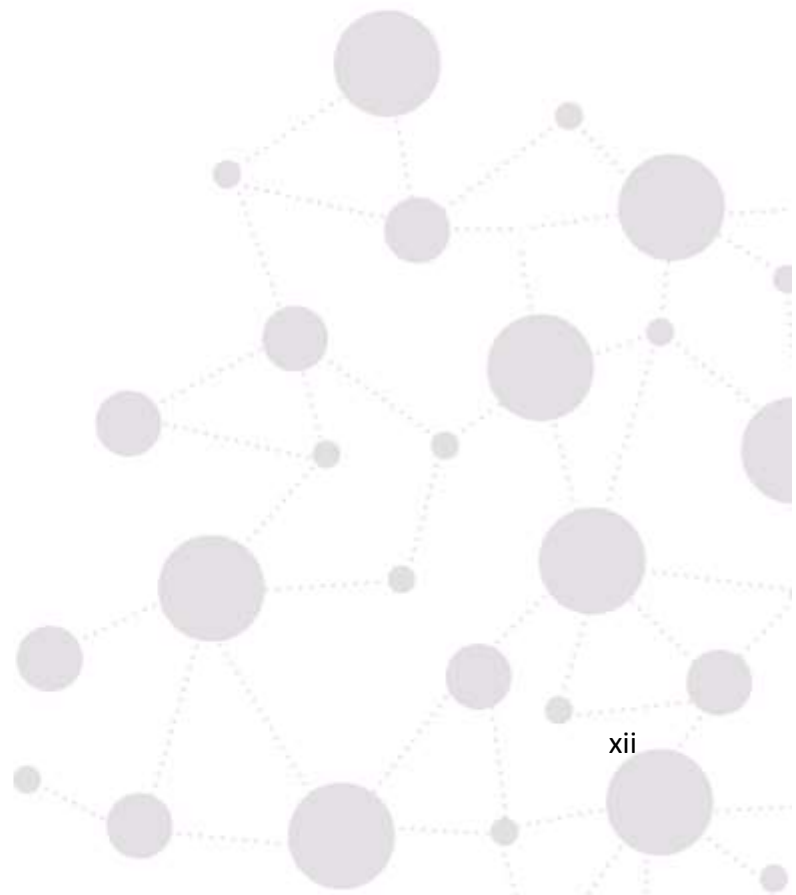


Índice de figuras:

Figura 1. Red WAN.....	13
Figura 2. Red MAN.....	14
Figura 3. Red LAN.....	15
Figura 4. WLAN.....	16
Figura 5. Uso de colas para priorizar trafico	22
Figura 6. Búfer de retardo de reproducción	23
Figura 7. Ejemplo de cola FIFO.....	27
Figura 8. Ejemplo de cola de espera equitativa y ponderada	28
Figura 9. Ejemplo de cola de espera equitativa y ponderada basada en clases	29
Figura 10. Ejemplo de cola de baja latencia.	30
Figura 12. DSCP	34
Figura 13. Valores de AF	35
Figura 14. Valores de CS y su correspondencia con ToS.....	35
Figura 15. Mapeo de marcado de capa 2 a capa 3	36
Figura 16. Ejemplo de Intserv.	40
Figura 17. Ejemplo de Diffserv.....	42
Figura 18. Paquetes expeditos y regulares	44
Figura 19. Reenvío asegurado.....	45
Figura 20. Topología de red en Packet Tracer	52
Figura 21. Comando Ping desde PC 0 a PC 2	53
Figura 22. Cabecera IP en la interfaz de entrada del R1, aplicando tráfico ICMP	54
Figura 23. Cabecera IP en la interfaz de salida del R1, aplicando tráfico ICMP	54
Figura 24. Tráfico Http desde PC 1 hasta el servidor http	55
Figura 25. Cabecera IP en la interfaz de entrada del R1, aplicando tráfico HTTP	56
Figura 26. Cabecera IP en la interfaz de salida del R1, aplicando tráfico HTTP.....	56
Figura 27. Cabecera IP en la interfaz de entrada del R1, aplicando tráfico ICMP	59
Figura 28. Cabecera IP en la interfaz de salida del R1, aplicando tráfico ICMP	59
Figura 29. Cabecera IP en la interfaz de entrada del R2, aplicando tráfico ICMP	60



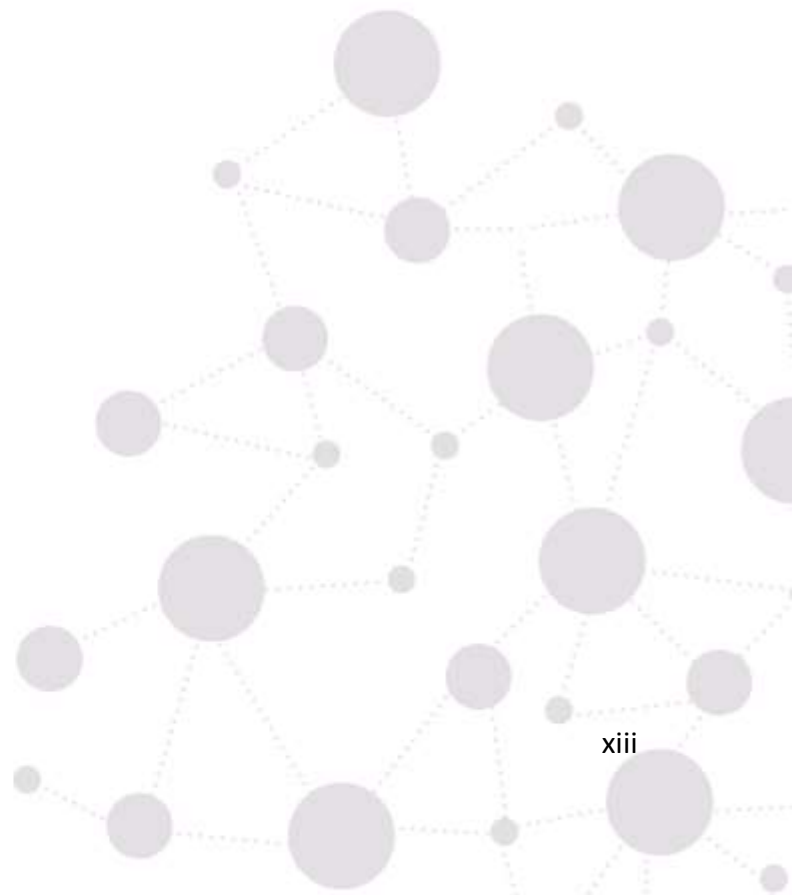
Figura 30. Cabecera IP en la interfaz de salida del R2, aplicando tráfico ICMP	60
Figura 31. Cabecera IP en la interfaz de entrada del R1, aplicando tráfico http	61
Figura 32. Cabecera IP en la interfaz de salida del R1, aplicando tráfico http	62
Figura 33. Cabecera IP en la interfaz de entrada del R2, aplicando tráfico http	62
Figura 34. Cabecera IP en la interfaz de salida del R2, aplicando tráfico http	63
Figura 35. Topología de red	64
Figura 36. Resultado QoS IPv6	65
Figura 37. Resultado Intserv	66
Figura 38. Resultado Diffserv	67
Figura 39. Topología usada en el proyecto	69
Figura 40. Paquetes perdidos	70
Figura 41. Jitter	70
Figura 42. Delay	71
Figura 43. Topología usada en el proyecto	72
Figura 44. Pérdida de paquetes	73
Figura 45. Retardo	74
Figura 46. Jitter	74





Índice de anexos:

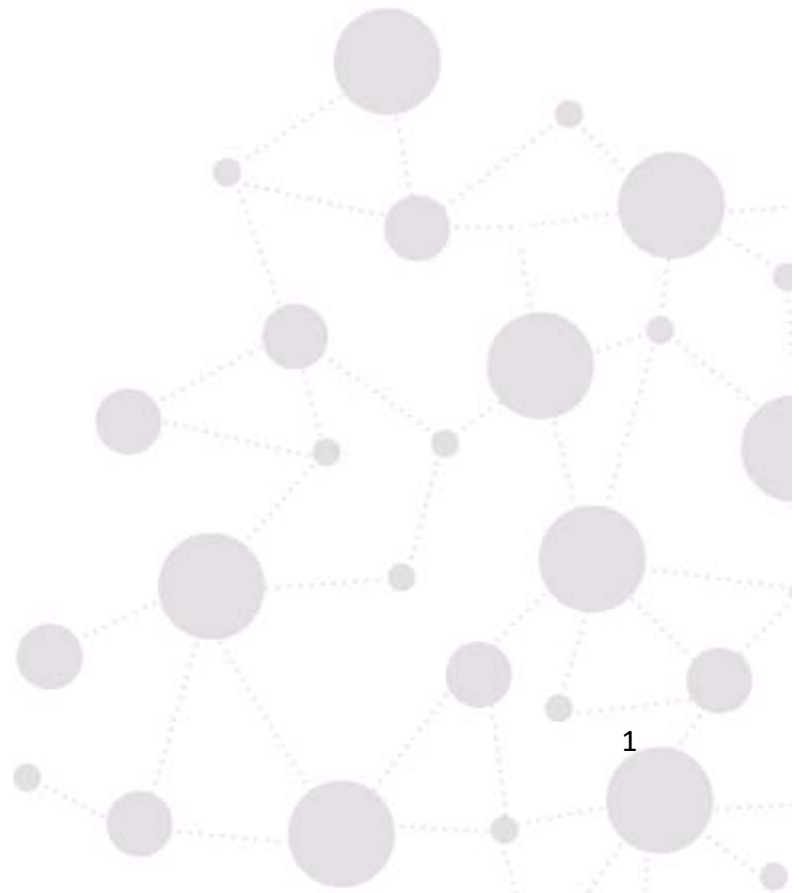
Anexo 1. Configuración de R1, Aplicando Políticas de Priorización De Tráfico	84
Anexo 2. Configuración de R2, Aplicando Políticas de Priorización De Tráfico	86
Anexo 3. Certificación de traducción del resumen	88





1. Título

Comparación de las soluciones Diffserv (Servicios Diferenciados) e Intserv (Servicios Integrados) para proveer Calidad De Servicio QoS en Redes LAN Inalámbricas.



2. Resumen

No cabe duda que cada vez es mayor el uso por parte de los usuarios de los sistemas inalámbricos de comunicaciones, debido a la posibilidad de recepción portable y móvil, facilidad de implementación, flexibilidad para afrontar crecimiento de la demanda, entre otras ventajas [1].

En el presente trabajo de titulación se hace una revisión de los aspectos relacionados con los parámetros que caracterizan al tráfico que circula por las redes, las posibles soluciones a los problemas relacionados con la congestión, así como la comparación de los métodos de QoS, antes y después de implementarlos en la red. Al respecto, haciendo énfasis como solución de esos problemas se hace uso de los métodos Intserv (Servicios Integrados) y Diffserv (Servicios Diferenciados), la efectividad de cada método, se ve reflejado en la bibliografía de los distintos proyectos analizados. En los mencionados proyectos de investigación, se comparan los métodos de QoS, sobre una misma topología de red, y se contrastan los resultados obtenidos.

Los parámetros comunes tomados en cuenta para comparar ambos métodos de QoS, según los distintos autores fueron:

- Pérdida de paquetes
- Retardo y
- Jitter

A continuación, se presenta de forma resumida la estructura del presente trabajo de titulación con la finalidad de facilitar la localización de información dentro del mismo.

En el presente apartado se ha **resumido** de forma breve el proyecto, mencionando los métodos de QoS y cuáles son los parámetros utilizados para compararlos, así como también, la estructura del documento de tesis.

En el apartado de “**Introducción**”, se ha realizado una presentación de los métodos de QoS, como lo son: Best Effort (mejor esfuerzo), Intserv (Servicios Integrados) y Diffserv (Servicios Diferenciados), así como sus ventajas y desventajas.

En la sección de “**Problema de investigación y objetivos**”, se hace una revisión de los problemas que existen en redes congestionadas y el tratamiento equitativo del tráfico de las aplicaciones, lo que provoca que tráfico sensible sea tratado de igual forma que el tráfico no

sensible y resulte en pérdida de paquetes, provocando en algunas aplicaciones baja calidad de servicio. Para contrarrestar estos efectos se utilizan métodos de QoS, de los cuales principalmente se analizaron los siguientes temas:

- Características y los principios de funcionamiento de las soluciones Diffserv e Intserv.
- Ventajas y desventajas de cada método.
- Prestaciones de cada solución en términos de latencia, jitter, ancho de banda y pérdida de paquetes.

En la parte de **“Información de antecedentes sobre la calidad de servicio en redes inalámbricas”**, se analizan libros, proyectos de investigación, temas de tesis, y simulaciones relacionadas con la QoS y de los cuales se obtienen conclusiones valiosas que nos indican que se han realizado variadas investigaciones que tienen como denominador común el hecho de dar importancia al tráfico sensible sobre el tráfico no sensible.

En la sección de **“Marco Teórico,”** se profundiza en la investigación de redes de datos, el estándar 802.11e, la Calidad de Servicio (QoS), características del tráfico en las redes, algoritmos de formación de colas, los métodos de QoS, sus ventajas y desventajas.

En la **“Metodología”**, se describe el procedimiento llevado a cabo para la elaboración de esta investigación bibliográfica.

En el apartado de **“Simulación de priorización de tráfico”**, se realiza la priorización de tráfico utilizando Packet tracer.

En la sección de **“Resultados”**, se analiza los resultados de diferentes investigaciones, se revisan los parámetros sobre los cuales se enfocan las investigaciones y el método como se planteó la topología de red, ya sea mediante simulación, laboratorio de pruebas real o infraestructura de red ya instalada y en funcionamiento.

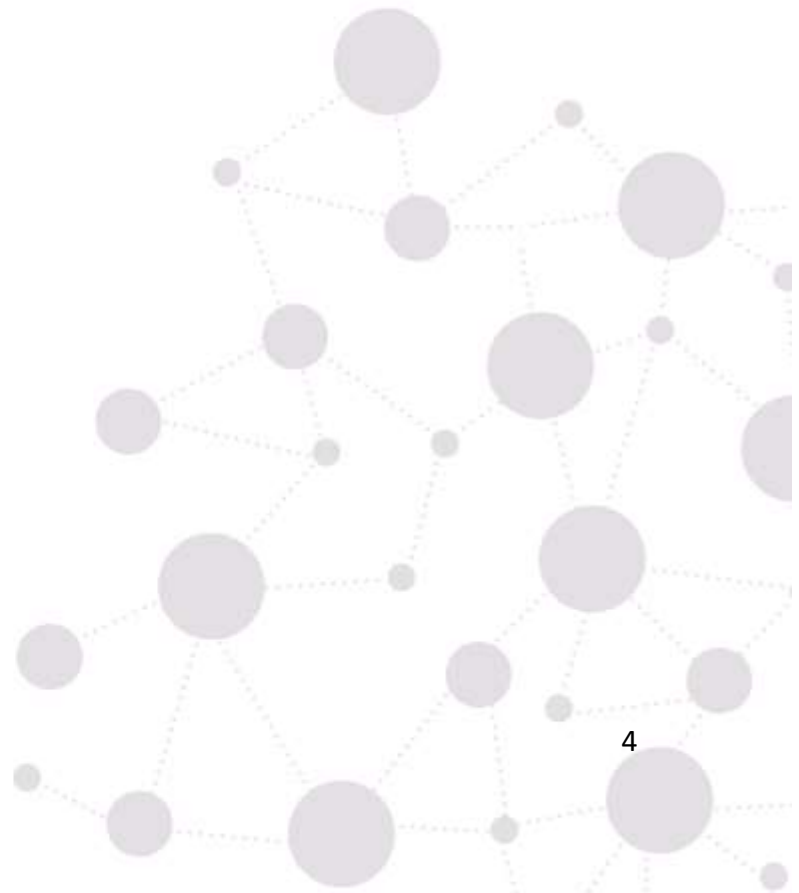
En la **“Discusión”**, se procede a resumir y comparar los resultados obtenidos en la sección anterior y se obtiene la conclusión de cuál es el mejor método de QoS.

Y finalmente, en los apartados de **“Conclusiones”** y **“Recomendaciones”**, se identifican los resultados más relevantes de la investigación y se sugieren aspectos a considerar para futuras investigaciones.



En los “Anexos”, se señalan y describen los comandos utilizados en Packet Tracer para configurar los routers cisco para priorizar el tráfico.

Palabras claves: *Difserv, Intserv, QoS, Packet Tracer, comparación, tráfico, priorización.*



2.1 Abstract

There is no doubt that the use of wireless communications systems by users is increasing, due to the possibility of portable and mobile reception, ease of implementation, flexibility to cope with growing demand, among other advantages [1].

The present research reviews the aspects related to the parameters that characterize the traffic flowing through the networks, the possible solutions to the problems related to congestion, as well as the comparison of the QoS methods, before and after implementing them in the network. The effectiveness of each method is reflected in the bibliography of the different projects analyzed, with emphasis on the use of the Intserv (Integrated Services) and Diffserv (Differentiated Services) methods as a solution to these problems. In the aforementioned research projects, QoS methods are compared on the same network topology and the results obtained are contrasted.

The common parameters taken into account to compare both QoS methods, according to the different authors were:

- Packet loss
- Delay and
- Jitter

The following is a summary of the structure of this degree work in order to facilitate the location of information within it.

In this section we have briefly summarized the project, mentioning the QoS methods and the parameters used to compare them, as well as the structure of the thesis document.

In the "Introduction" section, a presentation of QoS methods, such as: Best Effort, Intserv (Integrated Services) and Diffserv (Differentiated Services), as well as their advantages and disadvantages.

In the "Research problem and objectives" section, a review is made of the problems that exist in congested networks and the equitable treatment of application traffic, which causes sensitive traffic to be treated in the same way as non-sensitive traffic and results in

packet loss, causing low quality of service in some applications. To counteract these effects, QoS methods are used, of which the following topics were mainly analyzed:

- Characteristics and operating principles of Diffserv and Intserv solutions.
- Advantages and disadvantages of each method.
- Performance of each solution in terms of latency, jitter, bandwidth and packet loss.

In the part of "Background information on QoS in wireless networks", books, research projects, thesis topics, and simulations related to QoS are analyzed and from which valuable conclusions are obtained that indicate that there have been several researches that have as a common denominator the fact of giving importance to sensitive traffic over non-sensitive traffic.

In the "Theoretical Framework" section, we delve into data networking research, the 802.11e standard, Quality of Service (QoS), network traffic characteristics, queuing algorithms, QoS methods, their advantages and disadvantages.

In the "Methodology", the procedure carried out for the elaboration of this bibliographic research is described.

In the "Traffic Prioritization Simulation" section, traffic prioritization is performed using Packet tracer.

In the "Results" section, the results of different investigations are analyzed, the parameters on which the investigations are focused and the method by which the network topology was proposed, either by simulation, real test laboratory or network infrastructure already installed and in operation, are reviewed.

In the "Discussion", we proceed to summarize and compare the results obtained in the previous section and conclude which is the best QoS method. Finally, the "Conclusions" and "Recommendations" sections identify the most relevant results of the research and suggest aspects to be considered for future research.

In the "Annexes", the commands used in Packet Tracer to configure cisco routers to prioritize traffic are listed and described.

Keywords: Diffserv, Intserv, QoS, Packet Tracer, comparison, traffic, prioritization.

3. Introducción

La sociedad actual está demandando nuevos servicios que requieren progresivamente una mejor calidad de servicio (QoS). La QoS básica implícita, ofrecida por las redes IP se denomina Best Effort (mejor esfuerzo), donde se intenta realizar un relativo esfuerzo en la transmisión de paquetes, pero sin ofrecer ninguna garantía. En el presente proyecto de titulación se realiza una comparación en la calidad de servicio en redes LAN inalámbricas, considerando los métodos DIFFSER e INTSERV.

Se han definido dos modelos básicos para ofrecer calidad de servicio: Servicios Integrados (IntServ) y Servicios Diferenciados (DiffServ). En IntServ, la QoS se proporciona mediante la reserva de recursos a lo largo del camino mediante RSVP (Protocolo de reserva de recursos: diseñado para reservar recursos de una red). Aunque IntServ junto con RSVP puedan ser útiles para ofrecer QoS, se trata de un modelo complejo de implementar, ya que no es escalable para gestionar grandes cantidades de tráfico, debido a la cantidad de señalización que requiere para gestionar la disponibilidad de QoS y mantenimiento de los diferentes flujos en cada router. Además, conforme aumenta el tráfico en las redes, así como la variedad de servicios y aplicaciones, surge la necesidad de proporcionar niveles diferenciados de QoS a diferentes flujos de tráfico.

DiffServ es más versátil, de mayor simplicidad y funciona de forma más eficiente.

DiffServ es un método de calidad de servicio que garantiza a los usuarios que sus flujos de datos tendrán privilegios de extremo a extremo. Además, DiffServ tiene como principal objetivo la clasificación de paquetes similares para un tratamiento particular, este solo se encarga de marcar los paquetes, ya que los routers son los encargados de interpretar ese marcado y darle el tratamiento adecuado. [2]

En base a las características obtenidas de Diffserv e Inteserv se determinarán cuáles son las que se deban tomar en cuenta para la comparación requerida en lo que respecta a la calidad de servicio en las WLAN.

3.1 Problema de Investigación y Objetivos

El actual modelo de servicio que ofrece IP es el de mejor esfuerzo o best-effort, donde todos los paquetes son tratados de igual forma por la red.

Las aplicaciones tradicionales (Web, FTP, etc.) son tolerantes a retardos, pero no a pérdidas.

La posibilidad de un mayor tráfico multimedia parecía plantearse como el futuro problema para Internet, pero vemos como hoy en día con la evolución de las aplicaciones se requieren mayores prestaciones de las redes, de manera que se garantice que el tráfico sensible llegue a su destino de manera confiable. [3]

El Tráfico multimedia es sensible al retardo (“tiempo real”). Necesita que la pérdida de paquetes sea justa y baja. En redes que no tienen priorizado su tráfico de datos, los paquetes de datos son tratados de la misma manera que los paquetes de tráfico multimedia, ocasionando que la información no sensible llegue a su destino incluso cuando la información sensible no alcance a su receptor.

Por tal motivo, es menester, investigar métodos que permitan diferenciar el tráfico generado por las aplicaciones, para así, garantizar que los datos sensibles sean tratados con prioridad sobre los datos no sensibles que pueden ser flexibles ante falencias de las redes.

El problema de la investigación consiste en comparar las soluciones Diffserv e Intserv para proporcionar calidad de servicio en redes inalámbricas y evaluar su rendimiento en diferentes entornos y escenarios de uso. El objetivo principal de esta tesis es analizar las ventajas y desventajas de cada solución y determinar cuál es más adecuada para satisfacer los requisitos de calidad de servicio en diferentes situaciones de uso. Para alcanzar este objetivo, se plantearán las siguientes preguntas de investigación:

1. ¿Cuáles son las características y los principios de funcionamiento de las soluciones Diffserv e Intserv?
2. ¿Cuáles son las ventajas y desventajas de cada solución en términos de escalabilidad, flexibilidad, complejidad, sobrecarga de red y requisitos de recursos?



3. ¿Cómo se pueden medir y evaluar las prestaciones de cada solución en términos de latencia, jitter, ancho de banda y pérdida de paquetes en diferentes entornos de red y escenarios de uso?
4. ¿Cómo se pueden diseñar y optimizar las redes inalámbricas para utilizar eficientemente las soluciones Diffserv e Intserv y mejorar la calidad de servicio para diferentes aplicaciones y servicios?

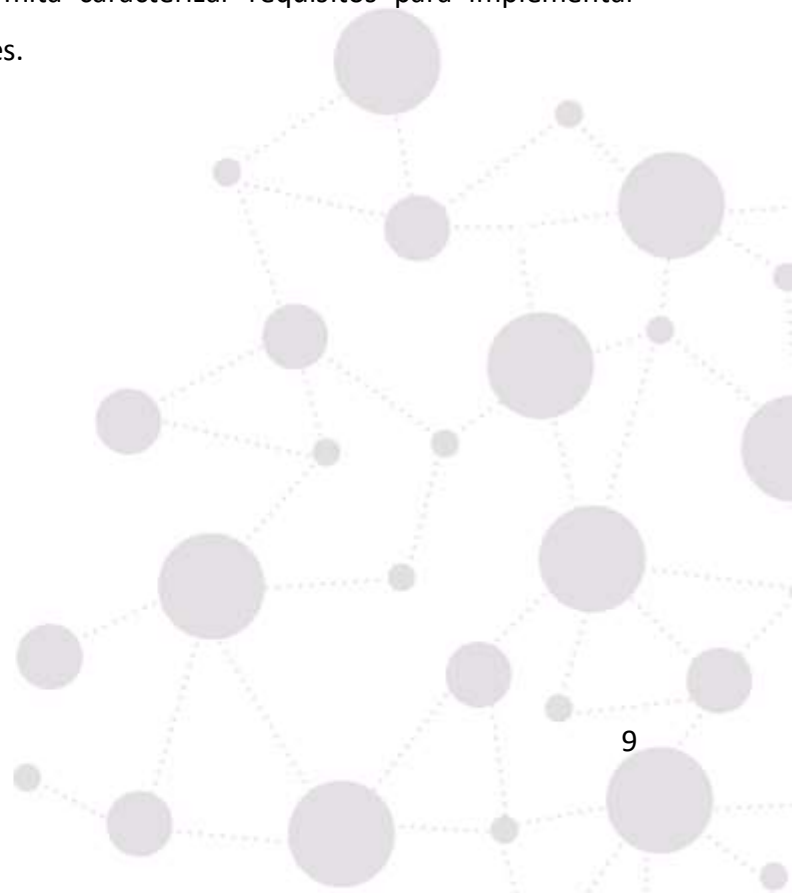
La respuesta a estas preguntas de investigación permitirá comparar y contrastar las soluciones Diffserv e Intserv y ofrecer recomendaciones para su aplicación en redes inalámbricas.

Objetivo general

Definir un marco de trabajo para determinar parámetros relevantes que permitan seleccionar la implementación de una solución de QoS en las WLAN empresariales.

Objetivos específicos

- Realizar un estudio del estado del arte referente a la Calidad de Servicio en las WLAN.
- Establecer los parámetros relevantes para ejecutar una comparativa de las soluciones Diffserv e Intserv.
- Establecer un procedimiento que permita caracterizar requisitos para implementar Diffserv o Intserv en redes empresariales.



4. Marco Teórico

4.1 Antecedentes Sobre La Calidad De Servicio En Redes Inalámbricas

Hoy es visible el hecho de que muchas organizaciones han encontrado en las redes de telecomunicaciones una herramienta invaluable para transportar información que en muchos casos obedecen a aplicaciones en tiempo real. Muchos procesos de negocios también utilizan las redes para el soporte de aplicaciones de gestión que involucran información de misión crítica (información que debe ser priorizada) para la empresa. Lo que realmente interesa es como hacer que a un determinado tipo de tráfico se le dé la prioridad necesaria en la red para que el servicio que lo genera no se afecte en su desempeño; lograr este cometido es lo que implica hablar de calidad de servicio (QoS por sus siglas en inglés). [2]

(Serrano, 2006) [4] en su tesis doctoral muestra como el estándar IEEE 802.11e involucra aspectos para el manejo de QoS en WiFi, presenta ciertas deficiencias y deja entrever el hecho de que aún falta desarrollar más investigación que conduzca a mejorar las prestaciones en QoS de este tipo de red, puesto que, para realizar mejoras a nivel de capa 3, siempre deben ser acompañadas con mejoras en la capa MAC.

Por su parte (Prasad, 2004) [5] desarrolla en su libro toda una temática frente a la aplicación de calidad de servicio en redes WLAN destacando algunos aspectos en lo que se refiere a seguridad. (Kweon & Shin, 2003) trabajaron en el modelamiento de tráfico estadístico de tiempo real, en donde se estudian algunos aspectos paramétricos que condicionan el nivel de calidad de servicio de este tipo de tráfico en una red Fast Ethernet. Ellos ofrecieron un punto de referencia importante para establecer los parámetros de calidad a estudiar y una forma para abordar la caracterización del tráfico de misión crítica.

En lo que al uso de simuladores respecta, (Flores, et al., 2006) [6] realizaron una comparación a nivel de paquetes de tres simuladores de red, los cuales son: NS2, Modeler de OPNET y NCTUns. Esta comparación ofrece un punto de referencia importante para la selección de un simulador de red apropiado para estudiar el tráfico de misión crítica.

Bernal & Salcedo, (2004) [7] abordaron el tema de calidad de servicio a nivel de red inalámbrica, aunque orientado a celulares más no a redes LAN, no obstante, ofrecen una alternativa para abordar el proceso de evaluación de la calidad de servicio, en redes celulares se

prioriza el tráfico de voz y se evalúa este parámetro, este modelo de evaluación sirve de base para aplicarlo a la evaluación de QoS en redes LAN.

Una investigación de (Hu, et al., 2011) [8] presenta un modelo de QoS asimétrico evaluado de manera experimental en donde se muestra que debido al despliegue que ha tenido la tecnología IEEE 802.11e, es necesario mejorar las condiciones de QoS en clientes que no admitan dicha tecnología. Los resultados muestran un buen rendimiento, incluso en escenarios de congestión y con tráfico sensible al retardo como VoIP.

(Sarkar & Paolini, 2011) [9] analizaron el comportamiento de IEEE 802.11e y concluyeron que el tráfico de tiempo no real ve mermada su oportunidad para transitar por la red debido a las prioridades del tráfico de tiempo no real. Por esta razón, ellos propusieron un protocolo a nivel MAC (Medium Access Control) más justo en el que el tráfico de tiempo no real también tenga oportunidad y no “se muera de hambre”. La simulación de comprobación se hizo con QualNet. Los resultados mostraron un acceso más justo a través de la mejora de los tiempos de turno.

En resumen, existen abundantes investigaciones acerca de estudios de calidad de servicio, lo cual nos permite tener abundante literatura para profundizar en el tema de QoS y llevar el desarrollo de la presente investigación bibliográfica a buen término.

4.2 Redes De Datos

Una red de datos es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. [10]

La finalidad principal para la creación de una red de datos es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, el cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

Cuando se desean conectar dispositivos, pueden aparecer las siguientes circunstancias:

- Los dispositivos están muy alejados. En este caso no estaría justificado, por ejemplo, utilizar un enlace dedicado entre dos dispositivos que puedan estar separados por miles de kilómetros.
- Hay un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes. Un ejemplo de esta necesidad es la red de teléfonos mundial o el conjunto de computadores pertenecientes a una compañía. Salvo el caso de que el número de dispositivos sea pequeño, no es práctico utilizar un enlace entre cada dos. La solución a estos problemas es conectar cada dispositivo a una red de comunicación.

Para clasificar las redes tradicionalmente se consideran las categorías: las redes de área amplia (WAN, Wide Area Networks), redes de área metropolitana (WAN), redes de área local (LAN, Local Area Networks) y las redes de área local inalámbricas (WLAN).

4.2.1 Redes De Área Amplia WAN

Generalmente, se considera como WAN a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Generalmente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo los situados en los contornos) no les concierne el contenido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

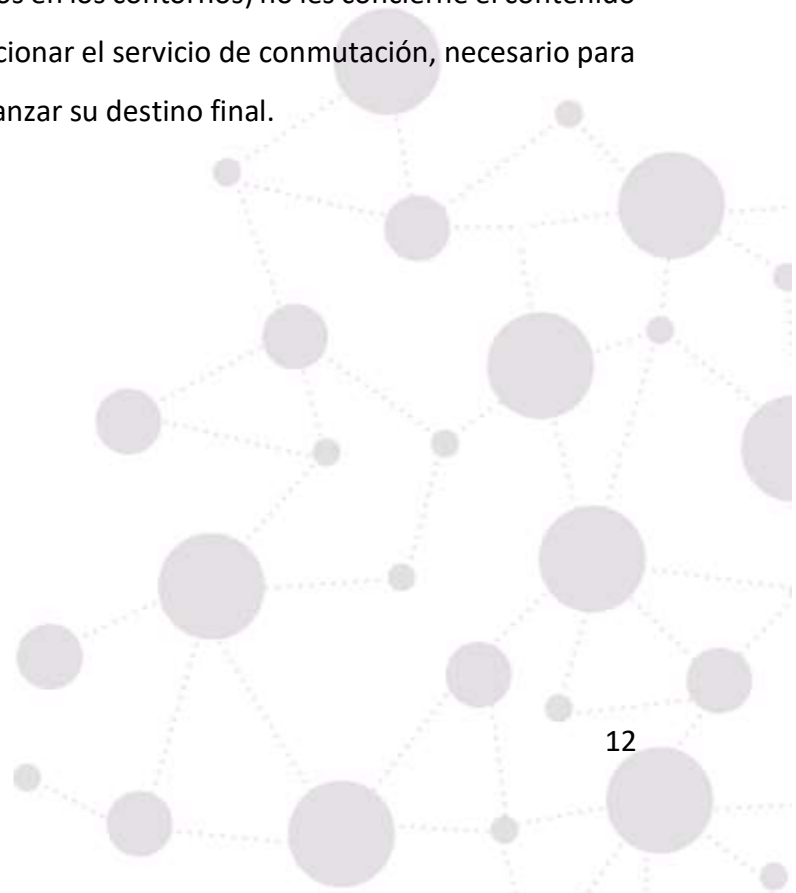
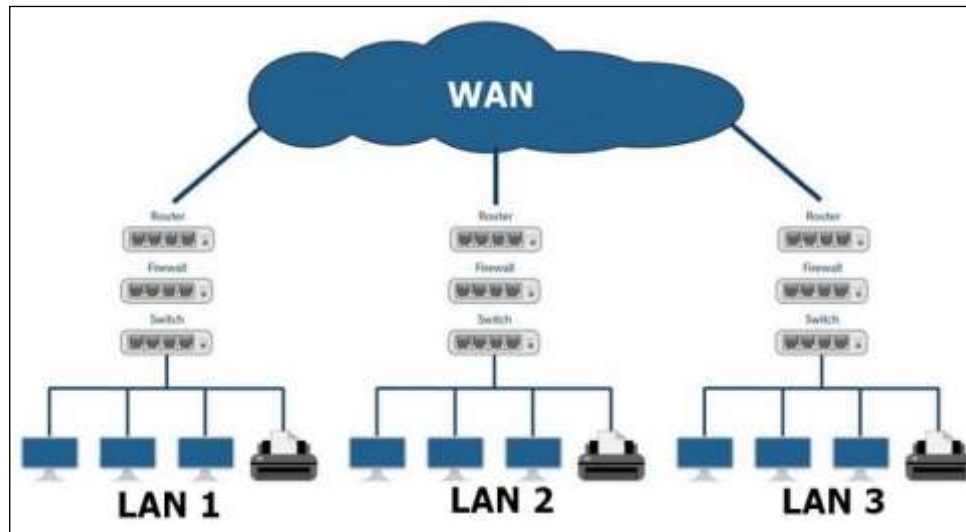


Figura 1.
Red WAN.



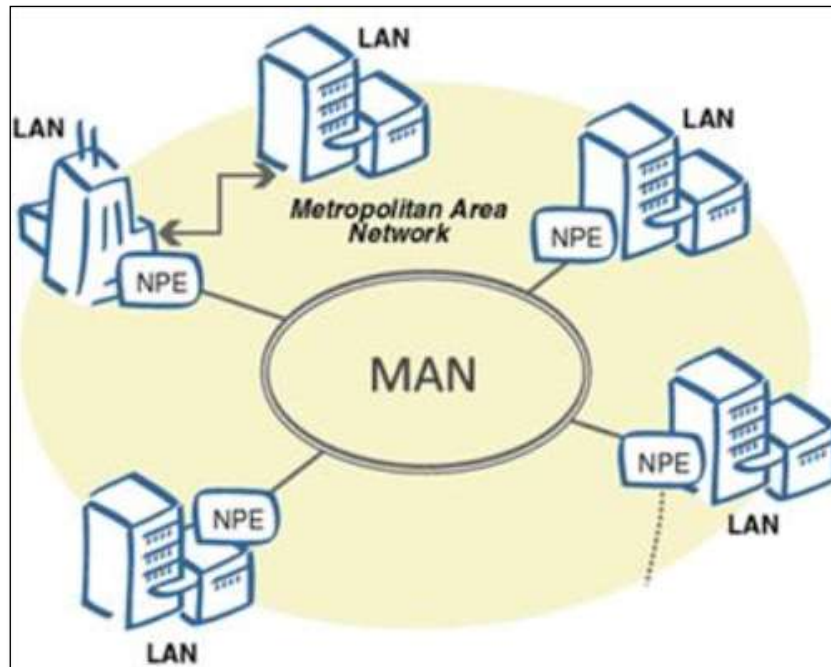
Nota. Adaptado de Red WAN (red de área amplia), por ConceptoABC, (<https://conceptoabc.com/red-wan/>)

4.2.2 Redes De Área Metropolitana (MAN)

Como el propio nombre sugiere, las MAN (Metropolitan Area Network) están entre las LAN y las WAN. El interés en las MAN ha surgido tras ponerse de manifiesto que las técnicas tradicionales de conmutación y conexión punto a punto usadas en WAN, pueden ser no adecuadas para las necesidades crecientes de ciertas organizaciones.

El principal mercado para las MAN lo constituyen aquellos clientes que necesitan alta capacidad en un área metropolitana. Las MAN están concebidas para satisfacer estas necesidades de capacidad a un coste reducido y con una eficacia mayor que la que se obtendría mediante una compañía local de telefonía para un servicio equivalente.

Figura 2.
Red MAN.



Nota. Adaptado de Red de alta velocidad que permite la cobertura de acceso a internet en parroquias rurales de América Latina, (<http://portal.amelica.org/ameli/jatsRepo/383/3831589029/html/index.html>)

4.2.3 Redes de área local (LAN)

Una LAN es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos. No obstante, hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

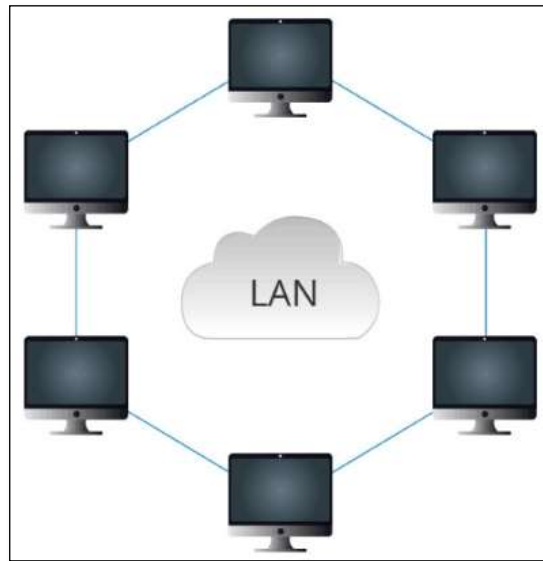
1. La cobertura de una LAN es pequeña, generalmente un edificio o, a lo sumo, un conjunto de edificios próximos. La cobertura geográfica condicionará la solución técnica adoptada.

2. Es habitual que la LAN sea propiedad de la misma entidad propietaria de los dispositivos conectados a la red. En WAN, esto no es tan habitual o, al menos, una fracción significativa de recursos de la red son ajenos. Esto tiene dos implicaciones. La primera es que se debe cuidar mucho la elección de la LAN, ya que, evidentemente, lleva acarreada una inversión sustancial de capital (comparada con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto

en la adquisición como en el mantenimiento. Segunda, la responsabilidad de la gestión de la red local recae solamente en el usuario.

3. Por lo general, las velocidades de transmisión internas en una LAN son mucho mayores que en una WAN.

Figura 3.
Red LAN.



Nota. Adaptado de LAN vs MAN vs WAN: ¿Cuál es la diferencia?
(<https://xxxamin1314.medium.com/lan-vs-man-vs-wan-cu%C3%A1l-es-la-diferencia-7a3545c1611a>)

4.2.4 Redes Inalámbricas (WLAN)

Las LAN inalámbricas son bastante habituales, fundamentalmente en entornos de oficinas. La tecnología inalámbrica es también muy utilizada en redes de área amplia de voz y datos. Las redes inalámbricas proporcionan ventajas evidentes en términos de movilidad y facilidad de instalación y configuración.

Figura 4.
WLAN.



Nota. Adaptado de WLAN, ¿Qué es y cómo funciona?
(<https://clavedemodem.com/wlan/>)

4.2.4.1 Tipos De Redes Inalámbricas

Las LAN inalámbricas (WLAN) se basan en los estándares IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) y se pueden clasificar en cuatro tipos principales: WPAN, WLAN, WMAN y WWAN.

Wireless Personal-Area Networks (WPAN): Redes inalámbricas de área personal - Utiliza transmisores de baja potencia para una red de corto alcance, generalmente de 20 a 30 pies (6 a 9 metros). Los dispositivos basados en Bluetooth y ZigBee se usan comúnmente en WPANs. Los WPAN se basan en el estándar 802.15 y una frecuencia de radio de 2.4 GHz.

Wireless LANs (WLAN): Redes LAN Inalámbricas - Utiliza transmisores para cubrir una red de tamaño mediano, generalmente de hasta 90 metros. Las redes WLANs son adecuadas para uso en casas, oficinas, e inclusive campus. Las WLAN se basan en el estándar 802.11 y una frecuencia de radio de 2,4 GHz o 5 GHz.

Wireless MANs (WMAN) - Redes MAN Inalámbricas - Utiliza transmisores para proporcionar servicio inalámbrico en un área geográfica más grande. Las redes WMANs son adecuadas para proveer acceso inalámbrico a ciudades metropolitanas o distritos específicos. Las WMANs utilizan frecuencias específicas con licencia.

Wireless Wide-Area Networks (WWANs) - Redes inalámbricas de área amplia - Utiliza transmisores para proporcionar cobertura en un área geográfica extensa. Las redes WWANs son adecuadas para comunicaciones nacionales y globales. Las WMANs utilizan frecuencias específicas con licencia. [11]

4.3 Estándares 802.11 WLAN

Los estándares 802.11 WLAN definen cómo se optimiza el uso del canal de acceso, a través de la capa física y enlace de datos a través de técnicas que hacen uso de las frecuencias de radio para los enlaces inalámbricos. La mayoría de los estándares especifican que los dispositivos inalámbricos tienen una o más antenas para transmitir y recibir señales inalámbricas en la frecuencia de radio especificada (2.4 GHz o 5 GHz).

A través de los años, se han desarrollado varias implementaciones de los estándares 802.11. La siguiente tabla destaca los estándares.

Tabla 1.
Estándares 802.11

Estándar IEEE WLAN	Radiofrecuencia	Descripción
802.11	2.4 GHz	<ul style="list-style-type: none"> • velocidades de hasta 2 Mbps
802.11a	5 GHz	<ul style="list-style-type: none"> • velocidades de hasta 54 Mbps • área de cobertura pequeña • menos eficaz para penetrar en las estructuras de los edificios • no es interoperable con el 802.11b y 802.11g
802.11b	2.4 GHz	<ul style="list-style-type: none"> • velocidades de hasta 11 Mbps • de mayor alcance que el 802.11a • más capaz de penetrar en las estructuras de los edificios
802.11g	2.4 GHz	<ul style="list-style-type: none"> • velocidades de hasta 54 Mbps • compatible con 802.11b con capacidad de ancho de banda reducida

802.11n	2.4 GHz/5 GHz	<ul style="list-style-type: none">• las velocidades de datos van de 150 Mbps a 600 Mbps con un rango de distancia de hasta 70 m (230 pies)• los puntos de acceso y los clientes inalámbricos requieren múltiples antenas con tecnología MIMO• compatible con los dispositivos 802.11a/b/g con velocidades de datos limitadas
802.11ac	5 GHz	<ul style="list-style-type: none">• proporciona velocidades de datos que van desde 450 Mbps a 1,3 Gbps (1300 Mbps) usando la tecnología MU - MIMO• se pueden soportar hasta ocho antenas• compatible con dispositivos 802.11a/n con velocidades de datos limitadas• Beamforming
802.11ax	2.4 GHz/5 GHz	<ul style="list-style-type: none">• lanzado en 2019 – último estándar• también conocido como High-Efficiency Wireless (HEW)• mayores velocidades de transmisión de datos• mayor capacidad• maneja muchos dispositivos conectados• eficacia energética mejorada• capacidad de 1 GHz y 7 GHz cuando esas frecuencias estén disponibles• también conocido como WiFi 6

Fuente: Elaborada por el autor.

4.4 IEEE 802.11e

Es una enmienda aprobada del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11 que define un conjunto de mejoras de calidad de servicio (QoS) para aplicaciones de LAN (Red de área local) inalámbrica a través de modificaciones a la capa de control de acceso al medio (MAC). El estándar se considera de vital importancia para las aplicaciones susceptibles a los retrasos, como Voz sobre IP y streaming multimedia.

Con los avances tecnológicos y la aparición de aplicaciones en tiempo real como son la telemedicina, videoconferencia, transmisión de video, juegos online, e-learning, las cuales necesitan ciertos requerimientos para su correcto funcionamiento, esto se logra al aplicar técnicas de QoS a las redes inalámbricas, como lo describe el protocolo 802.11e.

El protocolo MAC del estándar IEEE 802.11 no provee ninguna forma de diferenciar los distintos tipos de tráfico, todos son tratados de la misma forma. A diferencia del 802.11e, en que se puede diferenciar que estaciones están o no utilizando QoS. El estándar 802.11e fue desarrollado para corregir los problemas que se presentan a la hora de brindar QoS en el estándar 802.11

802.11e es una enmienda a los estándares 802.11, que define un conjunto de calidad de servicio (QoS) para aplicaciones LAN inalámbricas a través de alteraciones en la capa de control de acceso a medios. También proporciona servicios esenciales para aplicaciones sensibles al retraso, como transmisión de video y Voz sobre Protocolo de Internet (VoIP) [12].

4.4.1 El Acceso Distribuido En 802.11 Y 802.11e

En el caso más típico, una red 802.11 está constituida por una serie de estaciones y un punto de acceso (Access Point, AP), que suele ser, además, pasarela con una red cableada.

Para regular el acceso al medio, el estándar 802.11 propone dos mecanismos:

- Un mecanismo centralizado, PCF (Point Coordination Function), que se basa en un mecanismo de polling iniciado por el AP. Este mecanismo ha tenido escasa difusión.
- Un mecanismo distribuido, DCF (Distributed Coordination Function), en el que las estaciones emplean un mecanismo del tipo CSMA/CA para compartir el acceso al medio. A diferencia del anterior, este sí ha conseguido una gran aceptación.

El estándar 802.11e propone, también, dos modos de regular el acceso al medio:

- Un mecanismo centralizado, el HCCA (Hybrid coordination function Controlled Channel Access), sucesor del PCF.
- Un mecanismo distribuido, el EDCA (Enhanced Distributed Channel Access), sucesor del DCF.

Debido en parte a la escasa difusión del modo PCF, el futuro del HCCA resulta incierto.

No existe consenso en la comunidad científica ni entre los fabricantes sobre la bondad de una opción centralizada frente a una distribuida.

4.4.2 Carencias De 802.11

El mecanismo de acceso DCF proporciona justicia a largo plazo, entendiendo ésta como que todos los nodos tienen la misma probabilidad de ocupar una ranura de tiempo con una transmisión propia.

Por otra parte, los principales motivos por los que 802.11 no puede proporcionar calidad de servicio (ni en el modo DCF, ni en el PCF) son los siguientes:

- El modo DCF no proporciona mecanismo de diferenciación de tráfico, pues todas las estaciones reciben el mismo tipo de servicio best-effort.
- El modo PCF, de escasa difusión (lo que ya constituiría una limitación drástica), tampoco proporciona diferenciación de flujos.

4.4.3 El Modo EDCA

El acceso distribuido o basado en contienda de 802.11e se denomina EDCA (Enhanced Distributed Channel Access). Parte del modo DCF, cada estación implementa hasta cuatro categorías de acceso (AC) independientes, cada una de las cuales asociada a un determinado tipo de tráfico. El nombre que se da a cada AC indica el tipo de aplicación que se supone que ocupará la misma: voz (VO), vídeo (VI), best effort (BE) y background (BK).

4.5 La Calidad De Servicio En Redes De Computadoras.

Existen aplicaciones que exigen a la red garantías sólidas de desempeño, en especial, las aplicaciones multimedia necesitan con frecuencia una tasa de transferencia real máxima y una latencia mínima para trabajar. Es decir, se requiere proporcionar una calidad de servicio que coincida con las necesidades de cada aplicación. Ésta es un área en la que Internet pasa por un proceso continuo de actualización.

Una solución sencilla para proporcionar una buena calidad del servicio es construir una red con la suficiente capacidad para cualquier tráfico que maneje. La red resultante transportará el tráfico de cualquier aplicación sin pérdidas considerables y, suponiendo que hay un esquema de enrutamiento decente, entregará los paquetes con una latencia baja. El problema con esta solución es que tiene un costo elevado.

Los mecanismos de calidad del servicio permiten que una red con menos capacidad cumpla con los requerimientos de cualquier aplicación con la misma eficiencia, a un menor costo. Además, las redes sobredimensionadas se basan en el tráfico esperado. No se puede asegurar nada si el patrón de tráfico cambia demasiado. Con los mecanismos de calidad del servicio, la red puede honrar las garantías de desempeño, incluso cuando hay picos de tráfico, a costa de rechazar algunas solicitudes.

Es necesario considerar cuatro aspectos para asegurar la calidad del servicio:

1. Lo que las aplicaciones necesitan de la red.
2. Cómo regular el tráfico que entra a la red.
3. Cómo reservar recursos en los enrutadores para garantizar el desempeño.
4. Si la red puede aceptar o no más tráfico en forma segura.

Ninguna técnica maneja todos estos aspectos en forma eficiente. Sin embargo, se ha desarrollado una variedad de técnicas para usarlas en la capa de red (y de transporte). Las soluciones prácticas de calidad del servicio combinan varias técnicas. Existen dos versiones de calidad del servicio para Internet, conocidas como Servicios integrados y Servicios diferenciados.

[13]

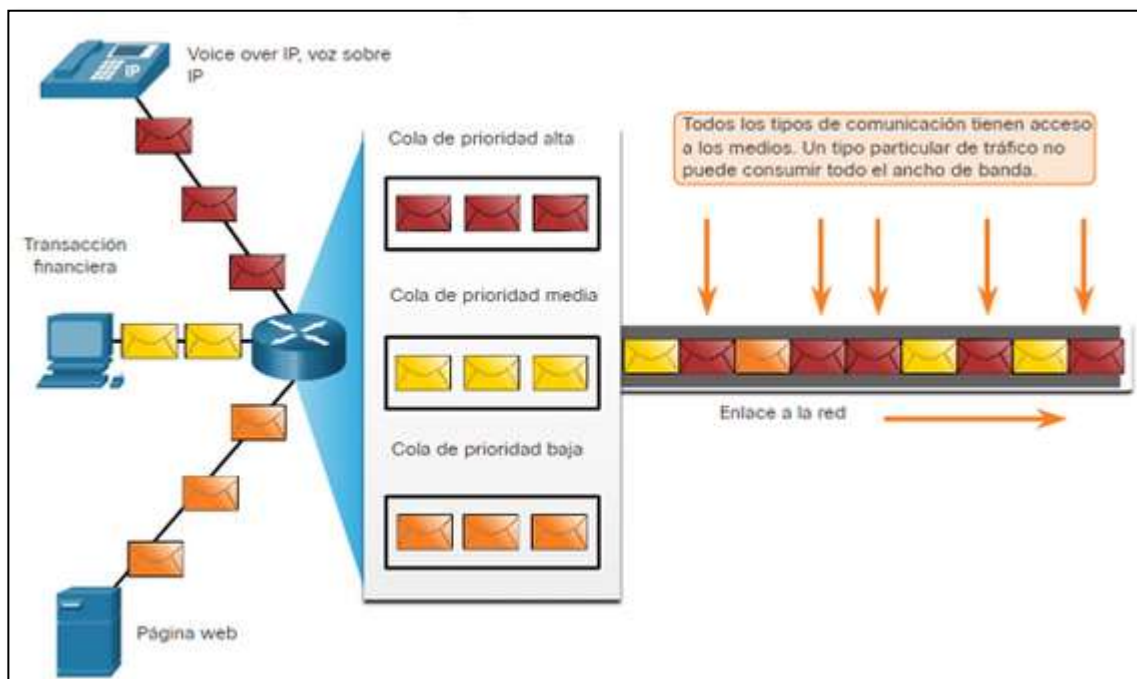
4.5.1 Priorización del tráfico

QoS es un requisito cada vez mayor de las redes hoy en día. Las nuevas aplicaciones, como las transmisiones de voz y video en vivo, crean mayores expectativas de entrega de calidad entre los usuarios.

La congestión ocurre cuando el volumen de tráfico es mayor que el que se puede transportar a través de la red, los dispositivos ponen en cola (retienen) los paquetes en la memoria hasta que los recursos estén disponibles para transmitirlos. Los paquetes en cola causan retrasos, dado que los nuevos paquetes no se pueden transmitir hasta que no se hayan procesado los anteriores. Si sigue aumentando la cantidad de paquetes que se pondrán en cola, la memoria del dispositivo se llenará y los paquetes se descartarán. Una técnica de la QoS que puede ayudar con este problema es la clasificación de datos en varias colas.

Figura 5.

Uso de colas para priorizar tráfico



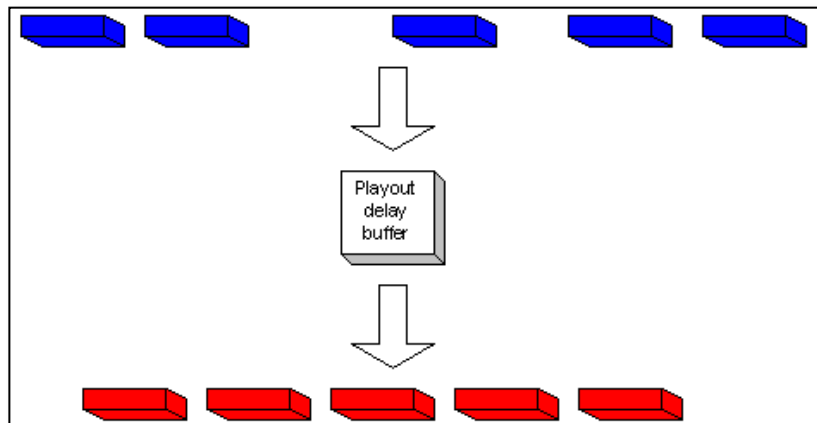
Nota. Adaptado de Calidad de Transmisiones de Red, [ccnadesdecero.es](https://ccnadesdecero.es/calidad-transmisiones-red/)
(<https://ccnadesdecero.es/calidad-transmisiones-red/>)

4.5.2 Pérdida De Paquetes

Sin ningún mecanismo de QoS, los paquetes se procesan en el orden en que se reciben. Cuando ocurre una congestión, los dispositivos de red como routers y switches pueden descartar paquetes. Esto significa que los paquetes urgentes, como el video y la voz en tiempo real, se descartarán con la misma frecuencia que los datos que no son urgentes, como el correo electrónico y la navegación web.

Cuando un router recibe una transmisión de audio digital para Voz sobre IP (VoIP), debe compensar el jitter que se produce. El mecanismo que maneja esta función es el búfer de retardo de reproducción. El búfer de retardo de reproducción debe almacenar estos paquetes en un búfer y luego reproducirlos en un flujo continuo, como se muestra en la figura. Los paquetes digitales se convierten más tarde en un flujo de audio analógico.

Figura 6.
Búfer de retardo de reproducción



Nota. Adaptado de Comprensión de la fluctuación en las redes de voz en paquetes, [www.cisco.com \(https://www.cisco.com/c/es_mx/support/docs/voice/voice-quality/18902-jitter-packet-voice.html\)](https://www.cisco.com/c/es_mx/support/docs/voice/voice-quality/18902-jitter-packet-voice.html)

Si las fluctuaciones son tan grandes que hacen que los paquetes se reciban fuera del alcance de este búfer, se descartan los paquetes que están fuera del rango, y se escuchan interrupciones en el audio.

La pérdida de paquetes es una causa muy común de problemas de calidad de voz en una red IP. Los ingenieros de redes utilizan mecanismos de calidad de servicio para clasificar los paquetes de voz para que la pérdida de paquetes sea cero. El ancho de banda se garantiza para

las llamadas de voz dando prioridad al tráfico de voz sobre el tráfico que no es sensible a los retrasos. [14]

4.5.3 Características De Tráfico (Voz, Vídeo Y Datos)

A principios de la década del 2000, los tipos de tráfico IP predominantes eran voz y datos. El tráfico de voz tiene una necesidad de ancho de banda predecible y tiempos de llegada de paquete conocidos. El tráfico de datos no es en tiempo real, y tiene una necesidad impredecible de ancho de banda. El tráfico de datos puede tener estallidos temporalmente, como cuando se descarga un archivo grande. Este estallido puede consumir todo el ancho de banda de un enlace.

4.5.3.1 Voz

El tráfico de voz es predecible y uniforme. Sin embargo, la voz es muy sensible a los retrasos y a los paquetes descartados. No tiene sentido retransmitir la voz si se pierden paquetes; por lo tanto, los paquetes de voz deben recibir una prioridad más alta que otros tipos de tráfico. La voz puede tolerar una cierta cantidad de latencia, fluctuación y pérdida sin efectos aparentes. La latencia no debe superar los 150 milisegundos (ms). Las fluctuaciones no deben superar los 30 ms y la pérdida de paquetes de voz no debe ser superior al 1%. El tráfico de voz requiere al menos 30 Kbps de ancho de banda.

La tabla ofrece un resumen de las características y requisitos del tráfico de voz.

Tabla 2.
Características del tráfico de voz

Características del tráfico de voz	Requerimientos de sentido único
<ul style="list-style-type: none"> • Fluida • Favorable • Sensible a las caídas • Sensible al retraso • Prioridad UDP 	<ul style="list-style-type: none"> • Latencia $\leq 150\text{ms}$ • Fluctuación $\leq 30\text{ms}$ • Pérdida $\leq 1\%$ de ancho de banda (30 – 128 Kbps)

Nota: Adaptado de Características de Tráfico. ccnadesdezero.es.

<https://ccnadesdezero.es/caracteristicas-trafico/>

4.5.3.2. Video

Sin QoS y una cantidad significativa de capacidad de ancho de banda extra, la calidad del video típicamente se degrada. La imagen aparece borrosa, dentada o en cámara lenta. La porción de audio de la alimentación puede quedar desincronizada con el video.

El tráfico de video tiende a ser impredecible, inconsistente y explosivo comparado con el tráfico de voz. En comparación con la voz, el video es menos resistente a la pérdida y tiene un mayor volumen de datos por paquete.

Tabla 3.

Características del tráfico de video

Características del tráfico de video	Requerimientos de sentido único
<ul style="list-style-type: none">• Ráfagas (Bursty)• Voraz (Greedy)• Sensible a las caídas• Sensible al retraso• Prioridad UDP	<ul style="list-style-type: none">• Latencia \leq 200-400 ms• Jitter \leq 30-50 ms• Pérdida \leq 0.1–1%• Ancho de banda (384 Kbps – > 20 Mbps)

Nota: Adaptado de Características de Tráfico. ccnadesdezero.es.

<https://ccnadesdezero.es/caracteristicas-trafico/>

4.5.3.3 Datos

La mayoría de las aplicaciones usan TCP o UDP. A diferencia de UDP, TCP realiza la recuperación de errores. Las aplicaciones de datos que no tienen tolerancia a la pérdida de datos, como el correo electrónico y las páginas web, utilizan TCP para asegurarse de que, si se pierden paquetes en tránsito, se reenvíen.

Tabla 4.

Características del tráfico de datos

Características del tráfico de datos
<ul style="list-style-type: none">• Fluido o con ráfagas (Smooth/bursty)• Benigno/voraz (Benign/greedy)• Insensible a las caídas• Insensible al retraso• Retransmisiones de TCP

Nota: Adaptado de Características de Tráfico. ccnadesdezero.es.

<https://ccnadesdezero.es/caracteristicas-trafico/>

El tráfico de datos es relativamente insensible a las caídas y los retrasos en comparación con la voz y el vídeo, Hay dos factores principales que un administrador de red debe preguntar acerca del flujo de tráfico de datos:

- ¿Los datos provienen de una aplicación interactiva?
- ¿Es la misión de los datos crítica?

Tabla 5.
Factores del tráfico

Factor	Misión Crítica	No es Misión crítica
Interactivo	Prioriza el menor retraso de todo el tráfico de datos y procura que el tiempo de respuesta sea de 1 a 2 segundos.	Las solicitudes podrían beneficiarse de una menor demora.
No Interactivo	El retardo puede variar enormemente siempre que se suministre el mínimo de ancho de banda necesario.	Obtiene cualquier ancho de banda sobrante después de que todas las necesidades de voz, video y otras aplicaciones de datos sean satisfechas.

Nota: Adaptado de Características de Tráfico. ccnadesdecero.es.

<https://ccnadesdecero.es/caracteristicas-trafico/>

4.5.4. Algoritmos De Formación De Colas

La política de QoS implementada por el administrador de la red se activa cuando se produce una congestión en el enlace. La cola es una herramienta de gestión de la congestión que puede almacenar en un búfer, priorizar y, si es necesario, reordenar los paquetes antes de que se transmitan al destino.

Se dispone de varios algoritmos de colas:

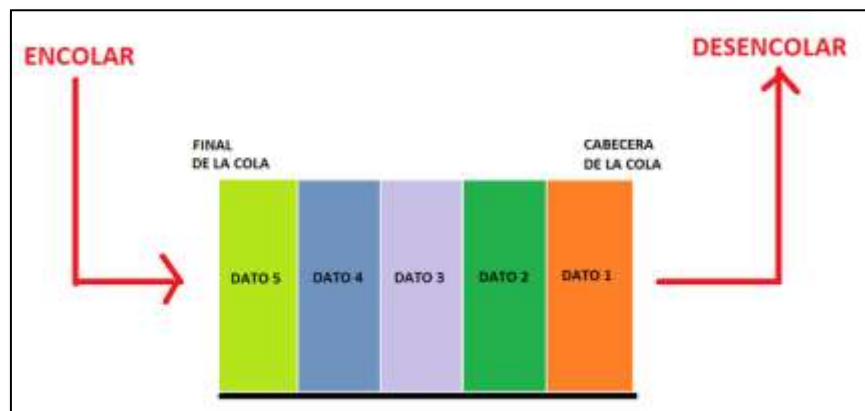
- First-In, First-Out (FIFO)
- Weighted Fair Queuing (WFQ)
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)

4.5.4.1 First In First Out (FIFO)

En su forma más simple, la Primera cola en entrar, es la primera cola en salir (FIFO, First In First Out), también conocida como colas por orden de llegada, amortigua y reenvía los paquetes en el orden de su llegada.

FIFO no tiene un concepto de prioridad o clases de tráfico y, en consecuencia, no toma ninguna decisión sobre la prioridad de los paquetes. Sólo hay una cola, y todos los paquetes son tratados por igual. Los paquetes se envían por una interfaz en el orden en que llegan.

Figura 7.
Ejemplo de cola FIFO



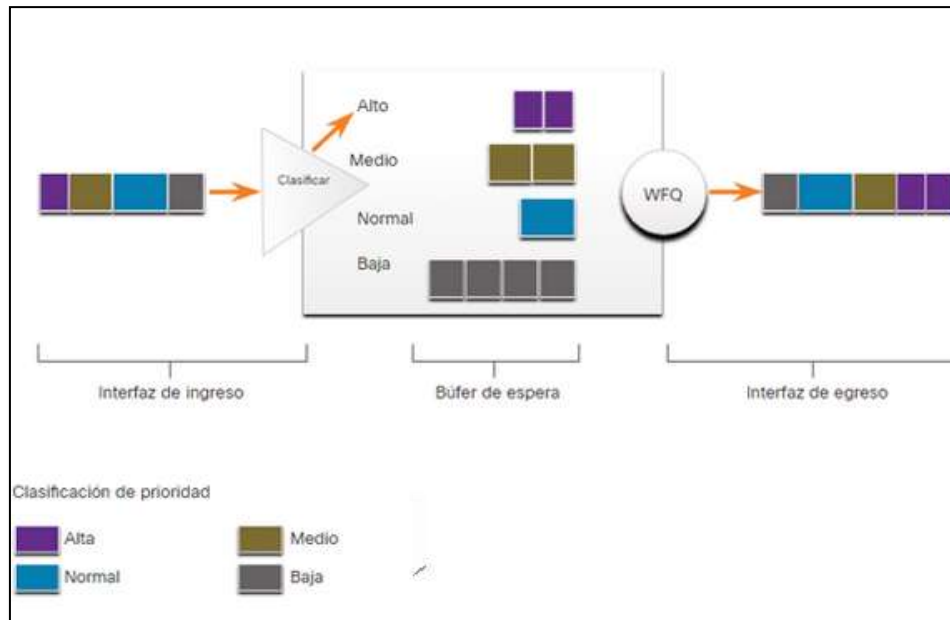
Nota. Adaptado de Algoritmo de CONCEPTO DE «COLA» Y SU IMPLEMENTACIÓN EN PYTHON, (<https://programacionpython80889555.wordpress.com/2019/03/19/concepto-de-cola-y-su-implementacion-en-python/>)

4.5.4.2 Weighted Fair Queuing (WFQ)

Espera equitativa ponderada (WFQ, Weighted Fair Queuing) es un método de programación automatizado que proporciona una asignación justa de ancho de banda a todo el tráfico de la red. El WFQ no permite configurar las opciones de clasificación. WFQ aplica prioridad, o pesos, al tráfico identificado y lo clasifica en conversaciones o flujos, como se muestra en la figura.

Figura 8.

Ejemplo de cola de espera equitativa y ponderada



Nota. Adaptado de Algoritmo de Formación de Colas, ccnadesdecero.es (<https://ccnadesdecero.es/calidad-transmisiones-red/>)

El WFQ determina entonces cuánto ancho de banda se permite a cada flujo en relación con otros flujos. El algoritmo basado en el flujo utilizado por WFQ programa simultáneamente el tráfico interactivo al frente de una cola para reducir el tiempo de respuesta. Luego comparte equitativamente el ancho de banda restante entre los flujos de alto ancho de banda. WFQ permite dar prioridad al tráfico interactivo de bajo volumen, como las sesiones de Telnet y la voz, sobre el tráfico de alto volumen, como las sesiones de FTP. Cuando se producen simultáneamente varios flujos de transferencia de archivos, se da a las transferencias un ancho de banda comparable.

Limitaciones de WQF

El WFQ no es compatible con el tunelado y la encriptación porque estas características modifican la información del contenido de los paquetes que requiere el WFQ para su clasificación.

4.5.4.3 Class-Based Weighted Fair Queuing (CBWFQ)

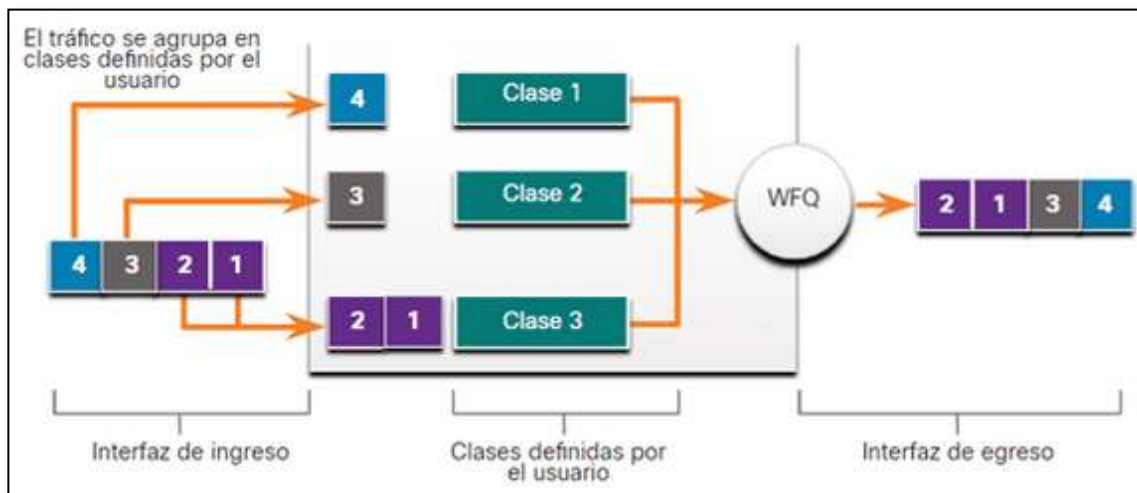
La cola de Espera equitativa ponderada basado en clases (CBWFQ, Class-Based Weighted Fair Queuing) amplía la funcionalidad estándar del WFQ para proporcionar soporte a las clases de tráfico definidas por el usuario. Con CBWFQ, se definen las clases de tráfico basadas en criterios de coincidencia, incluyendo protocolos, listas de control de acceso (ACL) e interfaces de entrada. Los paquetes que satisfacen el criterio de coincidencia para una clase constituyen el tráfico para esa clase. Se reserva una cola FIFO para cada clase y el tráfico perteneciente a una clase se dirige a la cola de esa clase.

Cuando una clase se ha definido según sus criterios de coincidencia, se le pueden asignar características. Para caracterizar una clase, se le asigna el ancho de banda, el peso y el límite máximo de paquetes. El ancho de banda asignado a una clase es el ancho de banda garantizado entregado a la clase durante la congestión.

Para caracterizar una clase, también se debe especificar el límite de cola para esa clase, que es el número máximo de paquetes que se permite acumular en la cola de la clase. Los paquetes pertenecientes a una clase están sujetos a los límites de ancho de banda y de cola que caracterizan a la clase.

Figura 9.

Ejemplo de cola de espera equitativa y ponderada basada en clases



Nota. Adaptado de Algoritmo de Formación de Colas, [ccnadesdecero.es](https://ccnadesdecero.es/calidad-transmisiones-red/) (<https://ccnadesdecero.es/calidad-transmisiones-red/>)

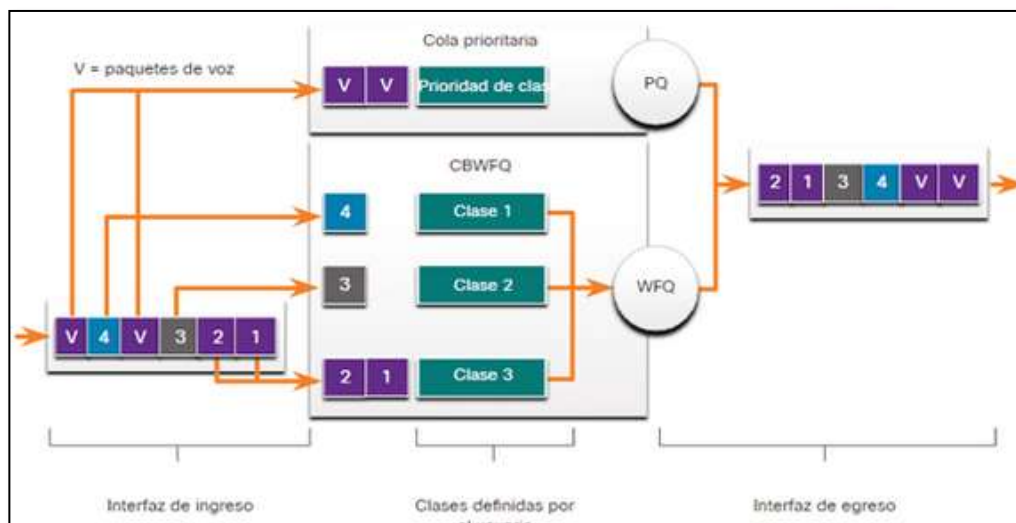
Después de que una cola ha alcanzado su límite configurado, añadir más paquetes a la clase hace que la caída de la cola o la caída de paquetes tenga efecto. La caída de cola significa que un router simplemente descarta cualquier paquete que llegue al final de una cola que haya agotado completamente sus recursos de retención de paquetes. Esta es la respuesta por defecto de la cola a la congestión. La caída de cola trata todo el tráfico por igual y no diferencia entre clases de servicio.

4.5.4.4 Low Latency Queuing (LLQ)

La característica de Cola de Baja Latencia (LLQ, The Low Latency Queuing) trae la estricta cola de prioridad (PQ) al CBWFQ. La PQ estricta permite que los paquetes sensibles al retraso, como la voz, se envíen antes que los paquetes de otras colas. La LLQ proporciona una estricta cola de prioridad para el CBWFQ, reduciendo las fluctuaciones en las conversaciones de voz.

La LLQ permite que los paquetes sensibles al retardo, como la voz, se envíen primero (antes que los paquetes en otras colas), dando a los paquetes sensibles al retardo un tratamiento preferencial sobre el resto del tráfico. Aunque es posible clasificar varios tipos de tráfico en tiempo real en la cola de prioridad estricta, se recomienda que sólo el tráfico de voz se dirija a la cola de prioridad.

Figura 10.
Ejemplo de cola de baja latencia.



Nota. Adaptado de Algoritmo de Formación de Colas, ccnadesdecero.es (<https://ccnadesdecero.es/calidad-transmisiones-red/>)

4.5.5 Proceso General de QoS y Secuencia De Operación Sobre El Flujo De Paquetes

4.5.5.1 Clasificación y Marcación

Antes de que a un paquete se le pueda aplicar una política de QoS, el mismo tiene que ser clasificado. La clasificación y la marcación (Classification & Marking) nos permiten identificar o “marcar” los tipos de paquetes. La clasificación determina la clase de tráfico al cual los paquetes o tramas pertenecen. Solo pueden aplicarse las políticas al tráfico después del marcado.

El cómo se clasifica un paquete depende de la implementación de la QoS. Los métodos de clasificación de flujos de tráfico en la capa 2 y 3 incluyen el uso de interfaces, ACL y mapas de clase. El tráfico también se puede clasificar en las capas 4 a 7 mediante el uso del Reconocimiento de aplicaciones.

La marcación significa agregar un valor al encabezado de paquetes. Los dispositivos que reciben el paquete se basan en este campo para ver si coincide con una política definida. La marcación debe realizarse tan cerca de la fuente como sea posible.

La forma en la que se marca el tráfico generalmente depende de la tecnología. La tabla siguiente describe algunos de los campos de marcado que se usan en diversas tecnologías. La decisión de marcar el tráfico de las capas 2 o 3 (o ambos) no es despreciable y debe tomarse tras considerar los siguientes puntos:

- La marcación de tramas de capa 2 se puede realizar para el tráfico no IP.
- La marcación de tramas de la capa 2 es la única opción de QoS disponible para los switches que no tienen “reconocimiento de IP”.

Tabla 6.
Formas de marcado

Herramientas de la QoS	Capa	Campo de Marcación	Bits
Ethernet (802.1Q, 802.1p)	2	Class of Service (CoS)	3
802.11 (Wi-Fi)	2	Wi-Fi Traffic Identifier (TID)	3
MPLS	2	Experimental (EXP)	3
IPv4 e IPv6	3	IP Precedence (IPP)	3
IPv4 e IPv6	3	Differentiated Services Code Point (DSCP)	6

Fuente: Elaborada por el autor.

4.5.5.2 Mercado De Tráfico En Capa 2

El estándar 802.1p utiliza 3 bits que identifica las marcas de clase de servicio (CoS). Tres bits significan que una trama Ethernet de capa 2 se puede marcar con uno de los ocho niveles de prioridad (valores 0-7) como se muestra en la tabla.

IEEE 802.1p es un estándar que proporciona priorización de tráfico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).

Tabla 7.

Mercado de tráfico en capa 2

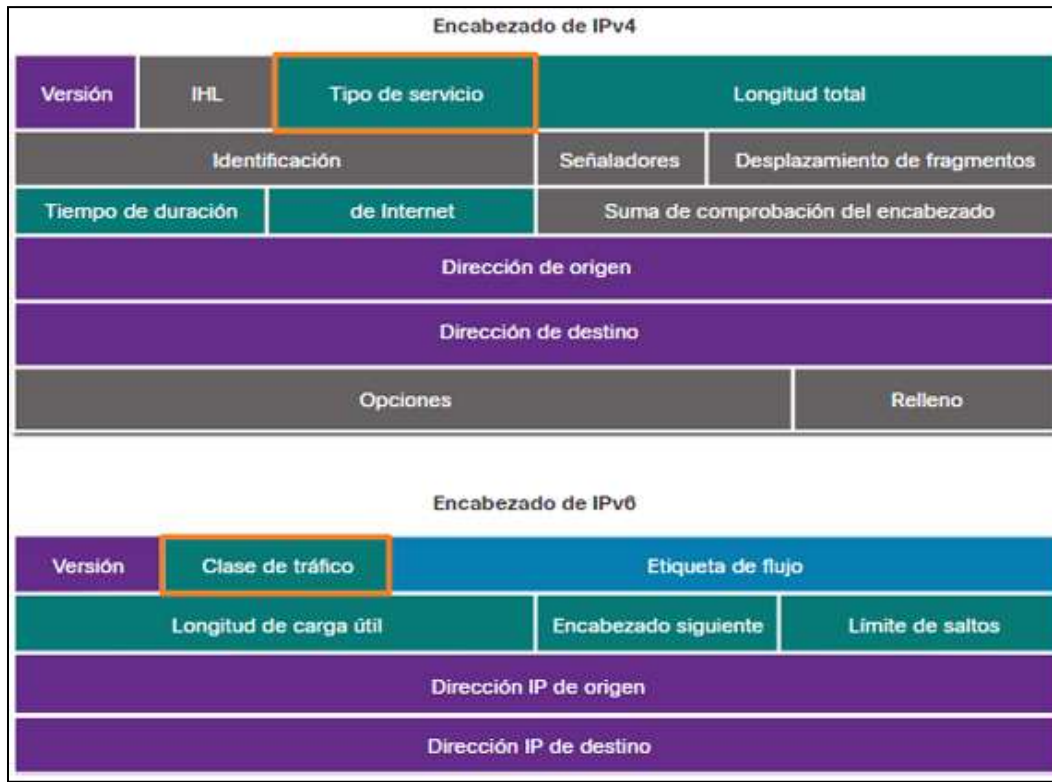
Valor de CoS	Valor Binario de CoS	Descripción
0	000	Datos de mejor esfuerzo
1	001	Datos de prioridad media
2	010	Datos de alta prioridad
3	011	Señalización de llamadas
4	100	Videoconferencia
5	101	Portador de voz (tráfico de voz)
6	110	Reservado
7	111	Reservado

Fuente: Elaborada por el autor.

4.5.5.3 Mercado De Tráfico En Capa 3

IPv4 e IPv6 especifican un campo de 8 bits en sus encabezados de paquetes para marcar los paquetes. Tanto IPv4 como IPv6 admiten un campo de 8 bits para marcar: el campo Tipo de servicio (ToS) para IPv4 y el campo Clase de Tráfico para IPv6.

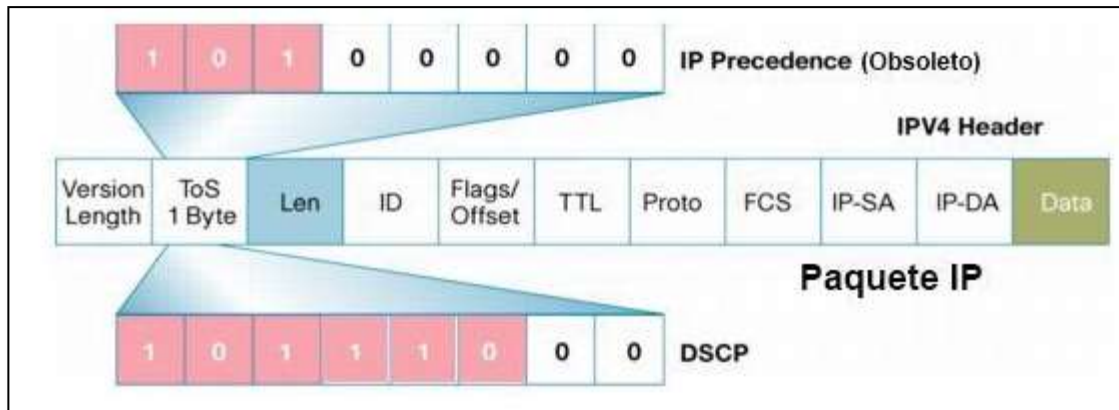
Figura 11.
Encabezados Paquetes IPv4 e IPv6



Nota. Adaptado de Técnicas de Implementación de QoS, ccnadesdecero.es
<https://ccnadesdecero.es/tecnicas-implementacion-qos/>

RFC 2474 reemplaza RFC 791 y redefine el campo de ToS al cambiar el nombre y ampliar el campo de IPP (IP Precedence). El nuevo campo, tiene 6 bits asignados para QoS. Conocido como campo de punto de código de servicios diferenciados (DSCP, Differentiated Services Code Point), estos seis bits ofrecen un máximo de 64 clases de servicio posibles. Los últimos dos bits del campo aún no se utilizan. Debido a que el campo DSCP ocupa la misma posición que el campo ToS se definió que los valores cuyos últimos tres bits fueran cero coincidirían con los valores de Precedence de ToS, permitiendo así la compatibilidad entre los dos campos. [15]

Figura 12.
DSCP



Nota: Adaptado de Configuración de qos en packet tracer para el CCNA 200-301, eclassvirtual.com <https://eclassvirtual.com/configuracion-de-qos-en-packet-tracer-para-el-ccna-200-301/>

Los valores del campo DSCP se pueden clasificar en cuatro grupos:

- Expedited Forwarding (EF): la clase más prioritaria con valor 46 (101110). Esta clase es usada para clasificar el tráfico que necesite unos parámetros de QoS asegurados.
- Assured Forwarding (AF): es la segunda clase más prioritaria. Se puede dividir en cuatro subclases, a las que se les adjudica un ancho de banda distinto en función del tráfico que vaya a circular por ellas. Además, se puede definir cada clase con tres probabilidades de descarte distintas lo que permite tener 12 clases distintas.

Figura 13.
Valores de AF

Drop	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
	AF11	AF21	AF31	AF41
Medium	001100	010100	011100	100100
	AF12	AF22	AF32	AF42
High	001110	010110	011110	100110
	AF13	AF23	AF33	AF43

Nota: Adaptado de CALIDAD DE SERVICIO (QoS) CON ROUTERS CISCO, Sobreviela L. (2019)

- Class Selector (CS): es la clase usada para la compatibilidad con el campo ToS. Tiene ocho valores que coinciden con los de precedence y a los que se le han añadido ceros al final.

Figura 14.
Valores de CS y su correspondencia con ToS

DSCP Class Selector Names	Binary DSCP Values	IPP Binary Values
Default/CS0*	000000	000
CS1	001000	001
CS2	010000	010
CS3	011000	011
CS4	100000	100
CS5	101000	101
CS6	110000	110
CS7	111000	111

Nota: Adaptado de CALIDAD DE SERVICIO (QoS) CON ROUTERS CISCO, Sobreviela L. (2019)

- Default Forwarding (DF): es la clase con la prioridad más baja y la que se aplica por defecto en la generación de paquetes IP. Su valor es de 0(000000).

4.5.5.4. Mapeo De Mercado De Capa 2 A Capa 3

En la siguiente figura se muestra los distintos tipos de mapeos dependiendo del marcado:

Figura 15.

Mapeo de marcado de capa 2 a capa 3

CoS = Class of Service
 DSCP = Differentiated Services Code Point
 ToS = Type of Service
 AF = Assured Forwarding
 IPP = IP Precedence
 CS = Class Selector
 DP = Drop Probability
 ECN = Explicit Congestion Notification

ToS							
DSCP						ECN	
AF (CS,DP)						ECN	
IPP=CS				DP			
				Delay	Thruput	Reliability	
8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
ToS	128	64	32	16	8	4	2
DSCP	32	16	8	4	2	1	
CoS=IPP	4	2	1				

Application	CoS=IPP	AF	DSCP	ToS	ToS HEX	DP	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
Best Effort	0	0	0	0	0		0	0	0	0	0	0	0	0
Scavanger	1	CS1	8	32	20		0	0	1	0	0	0	0	0
Bulk Data	1	AF11	10	40	28	Low	0	0	1	0	1	0	0	0
	1	AF12	12	48	30	Medium	0	0	1	1	0	0	0	0
	1	AF13	14	56	38	High	0	0	1	1	1	0	0	0
Network Mgmt.	2	CS2	16	64	40		0	1	0	0	0	0	0	0
Transaction Data	2	AF21	18	72	48	Low	0	1	0	0	1	0	0	0
	2	AF22	20	80	50	Medium	0	1	0	1	0	0	0	0
	2	AF23	22	88	58	High	0	1	0	1	1	0	0	0
Call Signaling	3	CS3	24	96	60		0	1	1	0	0	0	0	0
Mission-Critical	3	AF31	26	104	68	Low	0	1	1	0	1	0	0	0
Streaming Video	3	AF32	28	112	70	Medium	0	1	1	1	0	0	0	0
	3	AF33	30	120	78	High	0	1	1	1	1	0	0	0
	4	CS4	32	128	80		1	0	0	0	0	0	0	0
Interactive Video	4	AF41	34	136	88	Low	1	0	0	0	1	0	0	0
	4	AF42	36	144	90	Medium	1	0	0	1	0	0	0	0
	4	AF43	38	152	98	High	1	0	0	1	1	0	0	0
	5	CS5	40	160	A0		1	0	1	0	0	0	0	0
Voice	5	EF	46	184	B8		1	0	1	1	1	0	0	0
Routing	6	CS6	48	192	C0		1	1	0	0	0	0	0	0
	7	CS7	56	224	E0		1	1	1	0	0	0	0	0

Nota: Adaptado de eclassvirtual.com

[\(https://eclassvirtual.com/configuracion-de-qos-en-packet-tracer-para-el-ccna-200-301/\)](https://eclassvirtual.com/configuracion-de-qos-en-packet-tracer-para-el-ccna-200-301/)

Ejemplo de mapeo de marcado de capa 2 a capa 3

- Para tráfico voz: CoS = 5 → DSCP = EF = 101110 (6 primeros bit) = 0x2e (Hex) = 46 (Decimal).
- Para tráfico misión crítica: Cos = 3 → DSCP = AF31 = 011010 (6 primeros bit) = 0x1a (Hex) = 26 (Decimal).
- Para tráfico builk data: CoS = 1 → DSCP = AF11 = 001010 (6 primeros bit) = 0x0a (HeX) = 10 (Decimal).

4.6 Definición Y Características De La Calidad De Servicio En Redes Inalámbricas

La calidad de servicio (QoS) en redes inalámbricas se refiere a la capacidad de la red para proporcionar un nivel de servicio específico y consistente en términos de ancho de banda, latencia, jitter y pérdida de paquetes a través de diferentes aplicaciones y servicios de comunicación. En otras palabras, la QoS se refiere a la capacidad de la red para satisfacer los requisitos de rendimiento y disponibilidad de los usuarios finales para diferentes tipos de tráfico y aplicaciones.

Las redes inalámbricas tienen características únicas que las diferencian de las redes cableadas, como la interferencia, la atenuación de la señal, la propagación de las ondas de radio, la movilidad y el acceso compartido al medio. Estos factores pueden afectar la calidad de la señal y el rendimiento de la red, lo que hace que la QoS sea un desafío en las redes inalámbricas. Por esta razón, se han desarrollado diferentes técnicas y mecanismos para garantizar la QoS en redes inalámbricas.

Existen dos enfoques principales para proporcionar QoS en redes inalámbricas: servicios diferenciados (DiffServ) y servicios integrados (IntServ). El enfoque de DiffServ utiliza una arquitectura de red escalable y jerárquica para clasificar y priorizar el tráfico de red en diferentes clases de servicio. Cada clase de servicio tiene un nivel de prioridad y se le asigna un ancho de banda mínimo garantizado. Por otro lado, el enfoque de IntServ proporciona un mecanismo de reserva de recursos de extremo a extremo en la red para garantizar que los flujos de tráfico tengan los recursos necesarios para cumplir con los requisitos de QoS.

La QoS en redes inalámbricas también puede variar según el entorno de la red y los requisitos de la aplicación. Por ejemplo, las aplicaciones de voz y video tienen requisitos estrictos de QoS en términos de latencia y jitter, mientras que las aplicaciones de correo electrónico y navegación web pueden tolerar una latencia más alta y una mayor pérdida de paquetes. Además, las redes inalámbricas en entornos congestionados pueden experimentar una degradación en la QoS debido a la competencia por el ancho de banda y la interferencia.

Para medir y evaluar la QoS en redes inalámbricas, se utilizan diferentes métricas de rendimiento, como latencia, jitter, ancho de banda y pérdida de paquetes. La latencia se refiere al tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino y volver. El

jitter se refiere a la variación en la latencia de los paquetes de datos y puede afectar la calidad de las aplicaciones en tiempo real, como la voz y el video. El ancho de banda se refiere a la cantidad de datos que se pueden transmitir en un período de tiempo determinado. La pérdida de paquetes se refiere a la cantidad de paquetes de datos que no llegan a su destino.

Para garantizar la QoS en redes inalámbricas, se utilizan diferentes técnicas y mecanismos, como la clasificación y priorización del tráfico, la asignación de ancho de banda mínimo garantizado, la reserva de recursos de extremo a extremo.

Características de la calidad de servicio en redes inalámbricas:

5. **Fiabilidad:** La QoS en redes inalámbricas debe proporcionar un servicio confiable y predecible para los usuarios.
6. **Ancho de banda:** La QoS en redes inalámbricas debe garantizar que haya suficiente ancho de banda disponible para satisfacer las necesidades de las aplicaciones de tiempo real.
7. **Latencia:** La QoS en redes inalámbricas debe garantizar una latencia mínima para las aplicaciones de tiempo real, como la voz y el video.
8. **Jitter:** La QoS en redes inalámbricas debe minimizar el jitter para las aplicaciones de tiempo real, como la voz y el video.
9. **Pérdida de paquetes:** La QoS en redes inalámbricas debe minimizar la pérdida de paquetes para las aplicaciones de tiempo real, como la voz y el video.
10. **Escalabilidad:** La QoS en redes inalámbricas debe ser escalable para adaptarse a diferentes entornos de red y requisitos de aplicaciones.
11. **Flexibilidad:** La QoS en redes inalámbricas debe ser flexible para permitir cambios en las prioridades de tráfico y en las necesidades de ancho de banda de las aplicaciones.
12. **Gestión de recursos:** La QoS en redes inalámbricas debe administrar los recursos de manera eficiente para garantizar que se utilicen de manera óptima.
13. **Seguridad:** La QoS en redes inalámbricas debe garantizar la seguridad de los datos y la privacidad de los usuarios.
14. **Adaptabilidad:** La QoS en redes inalámbricas debe adaptarse a diferentes tipos de tráfico de datos y aplicaciones, y ajustarse automáticamente a las condiciones cambiantes de la red.

En resumen, la calidad de servicio en redes inalámbricas se refiere a la capacidad de la red para proporcionar un nivel de servicio predecible y consistente para diferentes tipos de tráfico de datos, especialmente para aplicaciones de tiempo real como voz y video. Para lograr una QoS efectiva, se deben considerar diferentes características, como la fiabilidad, el ancho de banda, la latencia, el jitter, la pérdida de paquetes.

4.6.1 Intserv (Servicios Integrados)

Entre 1995 y 1997, la IETF (Grupo de Trabajo de Ingeniería de Internet) se esforzó mucho en diseñar una arquitectura para la multimedia de flujos continuos. Este trabajo generó cerca de dos docenas de RFC, empezando con los RFC 2205–2212. El nombre genérico para este trabajo es servicios integrados. Se diseñó tanto para aplicaciones de unidifusión como para multidifusión. Un ejemplo de la primera es un solo usuario recibiendo en flujo continuo un clip de video de un sitio de noticias. Un ejemplo de la segunda es una colección de estaciones de televisión digital difundiendo sus programas como flujos de paquetes IP a muchos receptores en distintas ubicaciones.

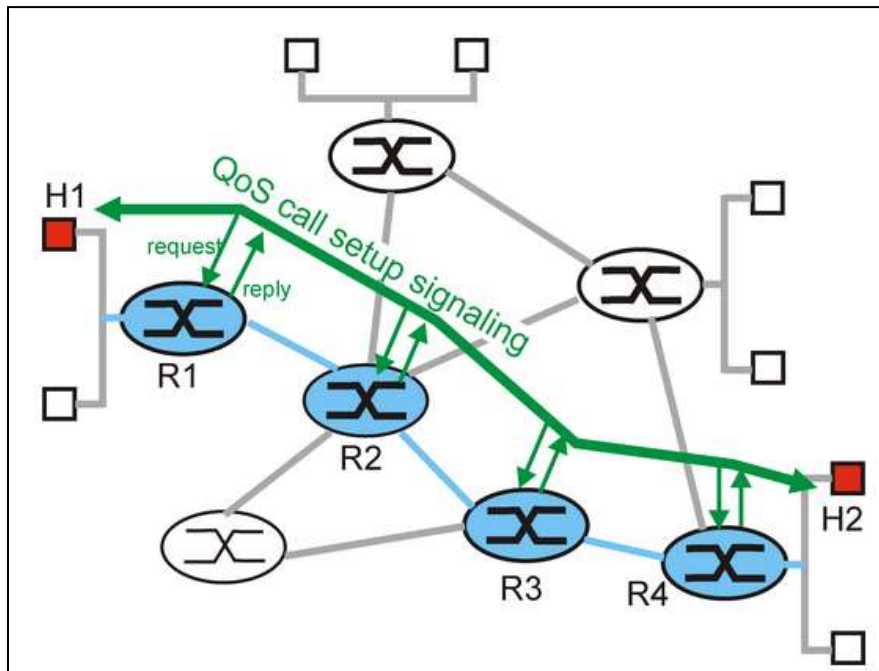
Se considera a la unidifusión como un caso especial de la multidifusión. En muchas aplicaciones de multidifusión, los grupos pueden cambiar su membresía en forma dinámica; por ejemplo, conforme las personas entran a una videoconferencia, se aburren y optan por visitar otros sitios web, para ver contenido multimedia o acceder a juegos en línea. Bajo estas condiciones, el método de hacer que los emisores reserven ancho de banda por adelantado no funciona bien, debido a que requeriría que cada emisor rastreara todas las entradas y salidas de su audiencia. En un sistema diseñado para transmitir televisión con millones de suscriptores, ni siquiera funcionaría. [16]

Se desarrolló para satisfacer las necesidades de las aplicaciones en tiempo real, como el vídeo remoto, las conferencias multimedia, las aplicaciones de visualización de datos y la realidad virtual. IntServ es un modelo de servicios múltiples que puede acomodar muchos requisitos de calidad de servicio.

IntServ ofrece la QoS de extremo a extremo que requieren las aplicaciones en tiempo real. IntServ gestiona explícitamente los recursos de la red para proporcionar la QoS a flujos o

corrientes individuales. Utiliza mecanismos de reserva de recursos y de control de admisión como bloques de construcción para establecer y mantener la QoS. Esto es similar a un concepto conocido como “hard QoS”. La QoS dura garantiza las características del tráfico, como el ancho de banda, el retardo y las tasas de pérdida de paquetes, de un extremo a otro. La QoS dura asegura niveles de servicio predecibles y garantizados para aplicaciones de misión crítica.

Figura 16.
 Ejemplo de Intserv.



Nota. Adaptado de Integrated Services, ic.uff.br (http://www2.ic.uff.br/~michael/kr1999/6-multimedia/6_07-intserv.htm)

IntServ utiliza un enfoque orientado a la conexión heredado del diseño de redes de telefonía. Cada comunicación individual debe especificar explícitamente su descriptor de tráfico y los recursos solicitados a la red. El router de borde realiza el control de admisión para asegurar que los recursos disponibles son suficientes en la red. La norma IntServ supone que los routers a lo largo de una ruta establecen y mantienen el estado para cada comunicación individual.

En el modelo IntServ, la aplicación solicita un tipo específico de servicio a la red antes de enviar los datos. La aplicación informa a la red de su perfil de tráfico y solicita un tipo de servicio concreto que puede abarcar sus necesidades de ancho de banda y de retardo. IntServ utiliza el protocolo de reserva de recursos (RSVP, Resource Reservation Protocol) para señalar las

necesidades de calidad de servicio del tráfico de una aplicación a lo largo de los dispositivos en el trayecto de extremo a extremo a través de la red. Si los dispositivos de la red a lo largo del trayecto pueden reservar el ancho de banda necesario, la aplicación de origen puede comenzar a transmitir. Si la reserva solicitada falla a lo largo del camino, la aplicación de origen no envía ningún dato.

El router de borde realiza un control de admisión basado en la información de la aplicación y los recursos de red disponibles. La red se compromete a cumplir los requisitos de calidad de servicio de la aplicación siempre que el tráfico se mantenga dentro de las especificaciones del perfil. La red cumple con su compromiso manteniendo el estado por flujo y luego realiza la clasificación de paquetes, la vigilancia y las colas inteligentes basadas en ese estado. [10]

4.6.2 Diffserv (Servicios Diferenciados)

Los algoritmos basados en flujo tienen el potencial de ofrecer buena calidad de servicio a uno o más flujos, debido a que reservan los recursos necesarios a lo largo de la ruta. Sin embargo, también tienen una desventaja. Requieren una configuración avanzada para establecer cada flujo, algo que no se escala bien cuando hay miles o millones de flujos. Además, mantienen el estado por flujo interno en los enrutadores, lo cual los hace vulnerables a las fallas de éstos. Por último, los cambios requeridos al código de enrutador son considerables e involucran intercambios complejos de enrutador a enrutador para establecer los flujos.

Por estas razones, la IETF también ha diseñado un método más simple para la calidad del servicio, uno que se pueda implementar ampliamente de manera local en cada enrutador sin una configuración avanzada y sin que toda la ruta esté involucrada. Este método se conoce como calidad de servicio basada en clase (en contraste a la basada en flujo). La IETF ha estandarizado una arquitectura para él, conocida como servicios diferenciados, que se describe en los RFC 2474, 2475.

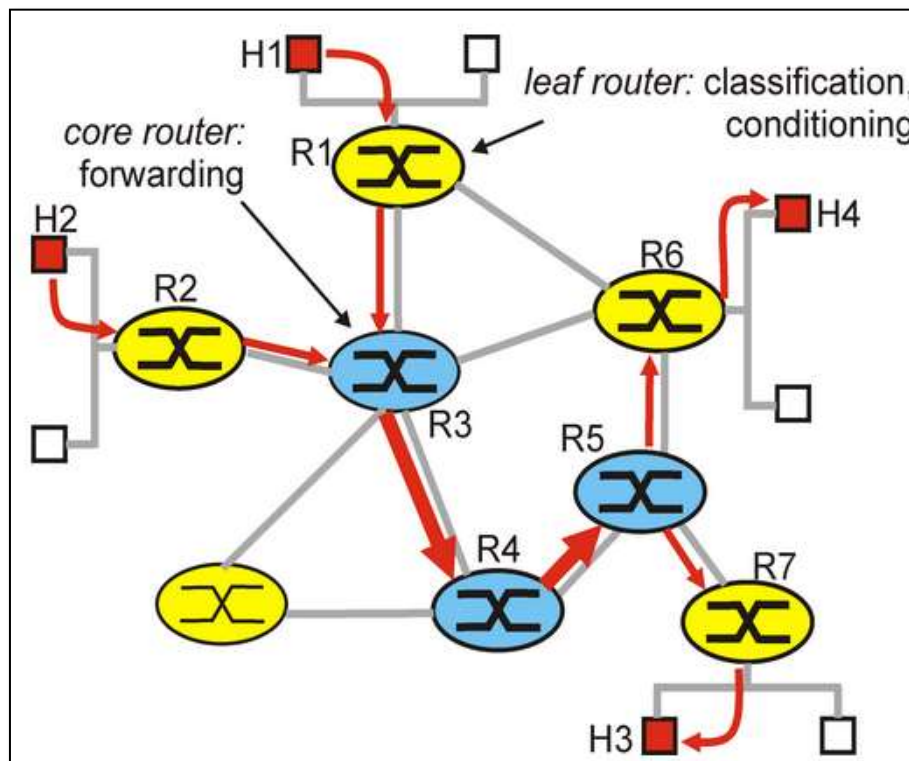
Un conjunto de enrutadores puede ofrecer los servicios diferenciados. La administración define un conjunto de clases de servicios con sus correspondientes reglas de reenvío. Si un cliente se suscribe a los servicios diferenciados, los paquetes del cliente que entran en el dominio se marcan con la clase a la que pertenecen. Las clases se definen como comportamientos por salto, ya que corresponden al trato que recibirá el paquete en cada enrutador y no a una garantía a

través de la red. Se proporciona un mejor servicio a los paquetes con ciertos comportamientos por salto (por ejemplo, servicio premium) que a otros paquetes (por ejemplo, servicio regular).

Cabe mencionar que este esquema no requiere una configuración avanzada o una reserva de recursos, ni tampoco una negociación (end to end) extremo a extremo que consuma tiempo para cada flujo, como sucede con los servicios integrados. Esto hace que los servicios diferenciados sean relativamente sencillos de implementar.

El modelo de QoS de servicios diferenciados (DiffServ) especifica un mecanismo sencillo y escalable para clasificar y gestionar el tráfico de la red. Por ejemplo, DiffServ puede proporcionar un servicio garantizado de baja latencia al tráfico de red crítico, como la voz o el vídeo, y al mismo tiempo proporcionar garantías de tráfico simple de mejor esfuerzo a los servicios no críticos, como el tráfico web o las transferencias de archivos. [16]

Figura 17.
Ejemplo de Diffserv.



Nota. Adaptado de Differentiated Services, ic.uff.br
(http://www2.ic.uff.br/~michael/kr1999/6-multimedia/6_09-diffserv.htm)

Mientras el host envía tráfico a un router, el router clasifica los flujos en clases y proporciona la política QoS apropiada para las clases. DiffServ impone y aplica los mecanismos de la QoS en base a saltos, aplicando uniformemente el significado global a cada clase de tráfico para proporcionar flexibilidad y escalabilidad. Por ejemplo, DiffServ podría configurarse para agrupar todos los flujos de TCP como clase única y asignar el ancho de banda para dicha clase, en vez de para los flujos individuales, como lo haría IntServ. Además de clasificar el tráfico, DiffServ minimiza los requisitos de mantenimiento de señales y estados en cada nodo de red.

Específicamente, DiffServ divide el tráfico de red en clases según los requisitos de la empresa. Se puede asignar a un nivel diferente de servicio a cada una de las clases. A medida que los paquetes atraviesan una red, cada uno de los dispositivos de red identifica la clase de paquete y brinda servicios al paquete según esa clase. Es posible elegir muchos niveles de servicio con DiffServ. Por ejemplo, el tráfico de voz de los teléfonos IP suele recibir un tratamiento preferencial sobre todo el resto del tráfico de aplicaciones, el correo electrónico suele recibir un servicio de mejor esfuerzo, y el tráfico no comercial puede recibir un servicio muy pobre o ser bloqueado por completo. [16]

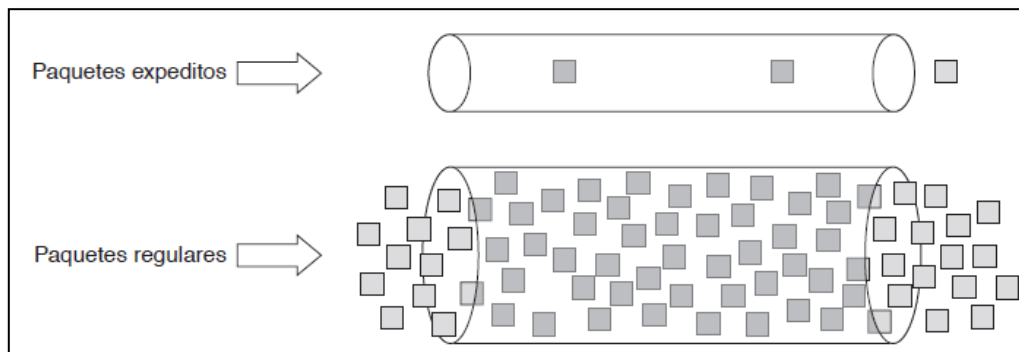
4.6.2.1 Clases De Servicio

4.6.2.1.1 Reenvío Expedito

Cada operador debe elegir las clases de servicios, pero ya que los paquetes con frecuencia se reenvían entre redes operadas por diferentes operadores, la IETF ha definido algunas clases de servicios independientes de la red. La clase más simple es el reenvío expedito, se describe en el RFC 3246.

La idea detrás del reenvío expedito es muy simple. Hay dos clases de servicios disponibles: regular y expedito. Se espera que la mayor parte del tráfico sea regular, pero una pequeña fracción de los paquetes son expeditos. Éstos deben tener la capacidad de transitar por la red como si no hubiera otros paquetes. De esta forma ellos tendrán un servicio con pocas pérdidas, bajo retardo y poca variación del retardo. En la figura se muestra una representación simbólica de este sistema de “dos tubos”. Observe que hay sólo una línea física. Las dos tuberías lógicas que se muestran en la figura representan una forma de reservar ancho de banda para las distintas clases de servicio, no una segunda línea física.

Figura 18.
Paquetes expeditos y regulares

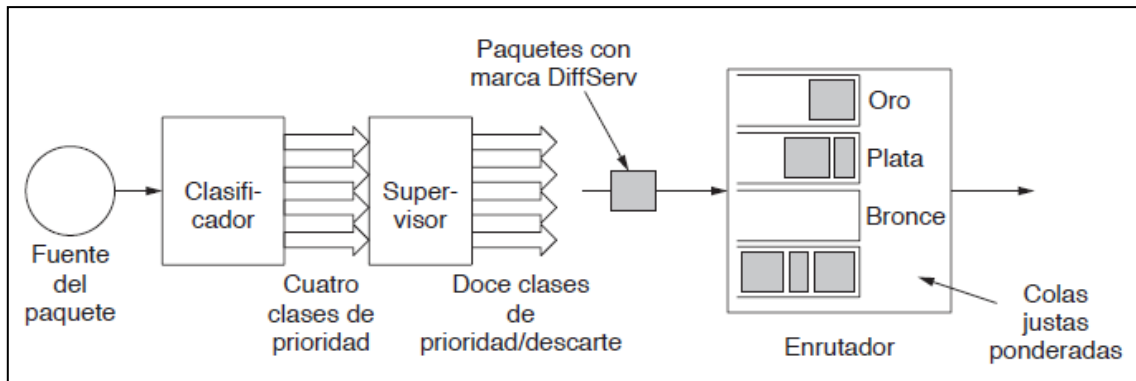


Nota. Adaptado de Redes de computadoras, por A. TANENBAUM y D. WETHERALL, 2012, Pearson Educación

4.6.2.1.2 Reenvío Asegurado

Hay un esquema un poco más elaborado para administrar las clases de servicios, el cual se conoce como reenvío asegurado. Se describe en el RFC 2597 y especifica que debe haber cuatro clases de prioridades, cada una con sus propios recursos. Las primeras tres clases se deben llamar oro, plata y bronce. Además, define tres probabilidades de descarte para los paquetes que están en congestión: baja, media y alta. En conjunto, estos dos factores definen 12 clases de servicios. La figura muestra una forma en que se pueden procesar los paquetes bajo el esquema de reenvío asegurado. El primer paso es clasificar los paquetes en una de las cuatro clases de prioridades. Como en el reenvío expedito, este paso se podría realizar en el host emisor (como se muestra en la figura) o en el enrutador de ingreso; el operador puede limitar la tasa de paquetes de prioridad más alta como parte del servicio ofrecido.

Figura 19.
Reenvío asegurado



Nota. Adaptado de Redes de computadoras, por A. TANENBAUM y D. WETHERALL, 2012, Pearson Educación

El siguiente paso es determinar la clase de descarte para cada paquete. Para ello es necesario pasar los paquetes de cada clase de prioridad por un supervisor de tráfico. El supervisor deja pasar todo el tráfico, pero identifica los paquetes que caben dentro de pequeñas ráfagas con un nivel de descarte bajo, a los paquetes que exceden las pequeñas ráfagas con un nivel de descarte medio y a los paquetes que exceden las ráfagas grandes con un nivel de descarte alto. Entonces, la combinación de las clases de prioridad y de descarte se codifica en cada paquete. Por último, los enrutadores en la red procesan los paquetes mediante un programador de paquetes que distingue las diversas clases. Una elección común es usar el encolamiento justo ponderado para las cuatro clases de prioridad, en donde las clases superiores reciben pesos más altos. De esta forma, las clases superiores obtendrán la mayor parte del ancho de banda pero no se privará a las clases inferiores de todo el ancho de banda. [8]

4.6.3 Ventajas Y Desventajas De Cada Solución

4.6.3.1 Diffserv. Ventajas Y Desventajas

Se presentan algunas ventajas y desventajas de DiffServ en términos de escalabilidad, flexibilidad, complejidad, sobrecarga de red y requisitos de recursos:

Ventajas:

- Escalabilidad: DiffServ es una solución escalable que se adapta bien a las redes grandes y complejas.
- Flexibilidad: DiffServ permite la definición de diferentes clases de tráfico y políticas de calidad de servicio (QoS) según las necesidades de la aplicación y los usuarios.
- Complejidad: DiffServ es una solución menos compleja que IntServ, ya que no requiere la negociación de recursos en tiempo real.
- Sobrecarga de red: DiffServ reduce la sobrecarga de la red, ya que la clasificación y el marcado de paquetes se realizan en los bordes de la red, en lugar de hacerlo en cada router.
- Requisitos de recursos: DiffServ requiere menos recursos que IntServ, ya que no se necesita una reserva de recursos para cada flujo de datos.

Desventajas:

- Complejidad: Aunque DiffServ es menos complejo que IntServ, aún puede requerir cierto nivel de experiencia y conocimientos técnicos para su configuración y gestión.
- Limitaciones en la garantía de ancho de banda: DiffServ no garantiza un ancho de banda específico para cada flujo de datos, lo que puede ser un problema para algunas aplicaciones sensibles al ancho de banda.
- Dificultad en la implementación de políticas de QoS: DiffServ puede ser difícil de implementar y configurar correctamente si no se tiene una comprensión clara de las políticas de QoS necesarias para satisfacer las necesidades de la aplicación y los usuarios.
- Dificultades en el control de congestión: DiffServ no proporciona un mecanismo explícito para el control de congestión, lo que puede ser un problema en redes congestionadas o de alta utilización.
- Limitaciones en la gestión de fallos: DiffServ no proporciona un mecanismo explícito para la gestión de fallos, lo que puede ser un problema en redes críticas o de alta disponibilidad.

4.6.3.2 Intserv. Ventajas y Desventajas

Se presentan algunas ventajas y desventajas de IntServ en términos de escalabilidad, flexibilidad, complejidad, sobrecarga de red y requisitos de recursos:

Ventajas:

- **Garantía de ancho de banda:** IntServ proporciona una garantía de ancho de banda para cada flujo de datos, lo que es importante para aplicaciones sensibles al ancho de banda.
- **Control de congestión:** IntServ proporciona un mecanismo explícito para el control de congestión, lo que es importante en redes congestionadas o de alta utilización.
- **Gestión de fallos:** IntServ proporciona un mecanismo explícito para la gestión de fallos, lo que es importante en redes críticas o de alta disponibilidad.
- **Flexibilidad:** IntServ permite la definición de políticas de QoS precisas según las necesidades de la aplicación y los usuarios.
- **Calidad de servicio garantizada:** IntServ garantiza una calidad de servicio específica para cada flujo de datos.

Desventajas:

- **Escalabilidad:** IntServ no es escalable para redes grandes y complejas, ya que requiere la negociación de recursos en tiempo real en cada router de la red.
- **Complejidad:** IntServ es una solución compleja que requiere un alto nivel de experiencia y conocimientos técnicos para su configuración y gestión.
- **Sobrecarga de red:** IntServ puede generar una sobrecarga de la red, ya que se requiere la negociación de recursos en tiempo real en cada router de la red.
- **Requisitos de recursos:** IntServ requiere una reserva de recursos para cada flujo de datos, lo que puede ser costoso en términos de recursos de la red y de hardware.

En general, IntServ es una solución adecuada para redes más pequeñas y simples que requieren una calidad de servicio garantizada y un control de congestión preciso. Sin embargo, en redes más grandes y complejas, DiffServ es una solución más adecuada debido a su escalabilidad y flexibilidad.

4.6.4 Técnicas Y Herramientas Para Evaluar Los Métodos Diffserv E Intserv

Para medir y evaluar las prestaciones de DIFFSERV en términos de latencia, jitter, ancho de banda y pérdida de paquetes en diferentes entornos de red y escenarios de uso, se pueden utilizar diferentes herramientas y técnicas, tales como:

- Pruebas de carga: se pueden utilizar herramientas de prueba de carga para evaluar el rendimiento de la red bajo diferentes condiciones de carga, lo que permite medir la latencia, jitter, ancho de banda y pérdida de paquetes.
- Herramientas de monitorización: existen herramientas de monitorización que permiten medir y analizar el rendimiento de la red en tiempo real, lo que permite detectar y solucionar problemas de latencia, jitter, ancho de banda y pérdida de paquetes.
- Análisis de tráfico: se pueden utilizar herramientas de análisis de tráfico para identificar patrones de tráfico y detectar cuellos de botella en la red, lo que permite optimizar el rendimiento de la red y reducir la latencia, jitter, ancho de banda y pérdida de paquetes.
- Simulación de red: se pueden utilizar herramientas de simulación de red para evaluar el rendimiento de la red bajo diferentes condiciones y escenarios de uso, lo que permite medir la latencia, jitter, ancho de banda y pérdida de paquetes en entornos controlados.
- Pruebas de campo: se pueden realizar pruebas de campo en entornos reales para evaluar el rendimiento de la red y medir la latencia, jitter, ancho de banda y pérdida de paquetes en situaciones reales de uso.

En general, para medir y evaluar las prestaciones de DIFFSERV en términos de latencia, jitter, ancho de banda y pérdida de paquetes en diferentes entornos de red y escenarios de uso, es importante utilizar una combinación de estas técnicas y herramientas para obtener una visión completa del rendimiento de la red.

Para medir y evaluar las prestaciones de IntServ en términos de latencia, jitter, ancho de banda y pérdida de paquetes en diferentes entornos de red y escenarios de uso, se pueden utilizar diferentes herramientas y técnicas, tales como:

- Pruebas de carga: se pueden utilizar herramientas de prueba de carga para evaluar el rendimiento de la red bajo diferentes condiciones de carga, lo que permite medir la latencia, jitter, ancho de banda y pérdida de paquetes.

- Herramientas de monitorización: existen herramientas de monitorización que permiten medir y analizar el rendimiento de la red en tiempo real, lo que permite detectar y solucionar problemas de latencia, jitter, ancho de banda y pérdida de paquetes.
- Análisis de tráfico: se pueden utilizar herramientas de análisis de tráfico para identificar patrones de tráfico y detectar cuellos de botella en la red, lo que permite optimizar el rendimiento de la red y reducir la latencia, jitter, ancho de banda y pérdida de paquetes.
- Simulación de red: se pueden utilizar herramientas de simulación de red para evaluar el rendimiento de la red bajo diferentes condiciones y escenarios de uso, lo que permite medir la latencia, jitter, ancho de banda y pérdida de paquetes en entornos controlados.
- Pruebas de campo: se pueden realizar pruebas de campo en entornos reales para evaluar el rendimiento de la red y medir la latencia, jitter, ancho de banda y pérdida de paquetes en situaciones reales de uso.

En general, para medir y evaluar las prestaciones de IntServ en términos de latencia, jitter, ancho de banda y pérdida de paquetes en diferentes entornos de red y escenarios de uso, es importante utilizar una combinación de estas técnicas y herramientas para obtener una visión completa del rendimiento de la red. Además, en el caso de IntServ, es importante tener en cuenta que la asignación de recursos se realiza de forma individual para cada flujo de tráfico, por lo que es importante monitorizar el tráfico y ajustar las configuraciones de IntServ para obtener un rendimiento óptimo.

5. Metodología

La metodología utilizada para el desarrollo del presente proyecto será de investigación bibliográfica, que son el conjunto de técnicas y estrategias que se emplean para localizar, identificar y acceder a aquellos documentos que contienen la información pertinente para la investigación [17]. Para lo cual, se procedió a reunir información de diversas fuentes (libros, artículos científicos, sitios web y de proyectos de investigación relacionados al tema) a fin de obtener un panorama completo y conciso del tema propuesto. La recopilación de información bibliográfica permite responder a preguntas relevantes, evaluar los resultados y anticipar mejor las probabilidades y tendencias futuras.

La recolección de información permitió determinar que parámetros fueron utilizados para diseñar y evaluar las redes implementadas en los distintos proyectos, y además, permitió determinar que variables fueron analizadas por los diferentes autores para comparar los métodos de QoS y concluir que método es el más adecuado para optimizar variables como ancho de banda, retardo o pérdidas de paquetes.

Existen diversas técnicas para evaluar el rendimiento de los métodos de QoS, en la bibliografía revisada se usan técnicas como la:

- Prueba de carga: que consiste en saturar una red con distintos tipos de tráfico con el fin de observar el comportamiento de la latencia, jitter, ancho de banda y pérdida de paquetes antes y luego de la saturación de la red.
- En lo que respecta a herramientas de monitoreo y análisis de tráfico, la de mayor uso es el software wireshark, ya que es de fácil uso, se puede utilizar en laboratorios reales de prueba, así como también, este software está incluido dentro de algunos simuladores como en GNS3.
- Simulación: consiste en utilizar herramientas de simulación que permitan emular escenarios y a los cuales se les puede alterar las variables a medir y observar el comportamiento de la red

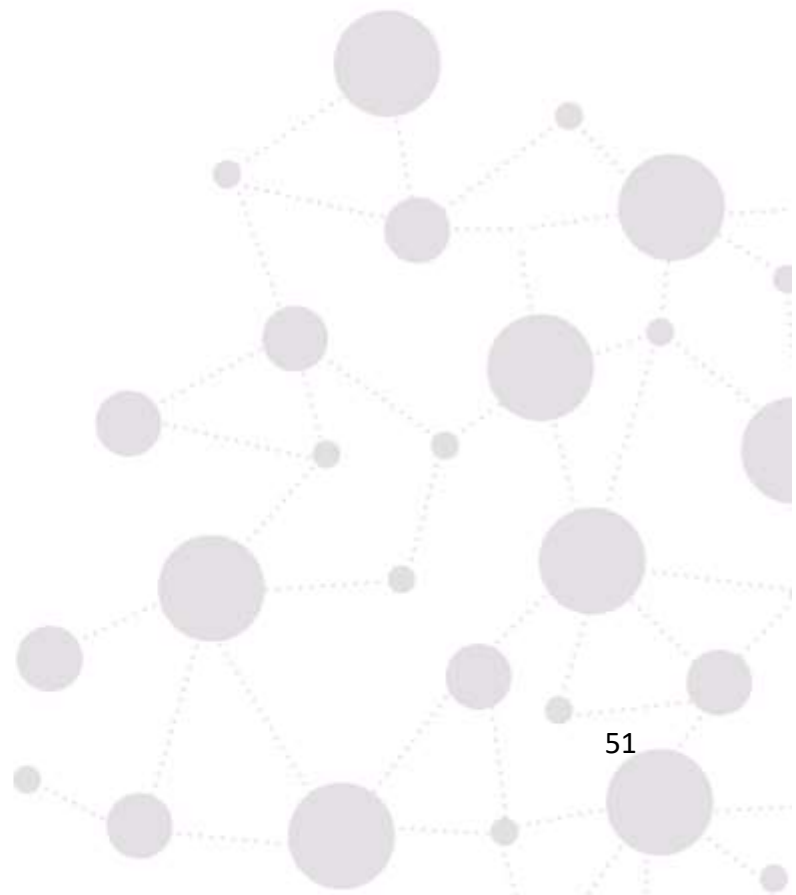
De las técnicas mencionadas para evaluar el rendimiento de los métodos de QoS. Para el presente proyecto de investigación se utilizó la simulación, donde se muestra como el tráfico es clasificado, señalado (marcado) y luego se lo procesa de acuerdo a una determinada política, para

una administración eficiente del ancho de banda y dando prioridad de colas. Dicha simulación se lleva a cabo sobre el software Packet Tracer, que proporciona una interfaz gráfica intuitiva y posee los elementos necesarios para llevarla a cabo.

En la simulación, se generarán 2 tipos de tráfico (ICMP y HTTP), los mismos se marcarán con una DSCP diferente (af31 y af11 respectivamente) mediante un CLASS MAP y se les aplicará una política (POLICY-MAP) para darles un tratamiento diferenciado.

Las configuraciones se realizan en los routers y la descripción de los mismos forman parte de esta investigación y se añadirán en los anexos

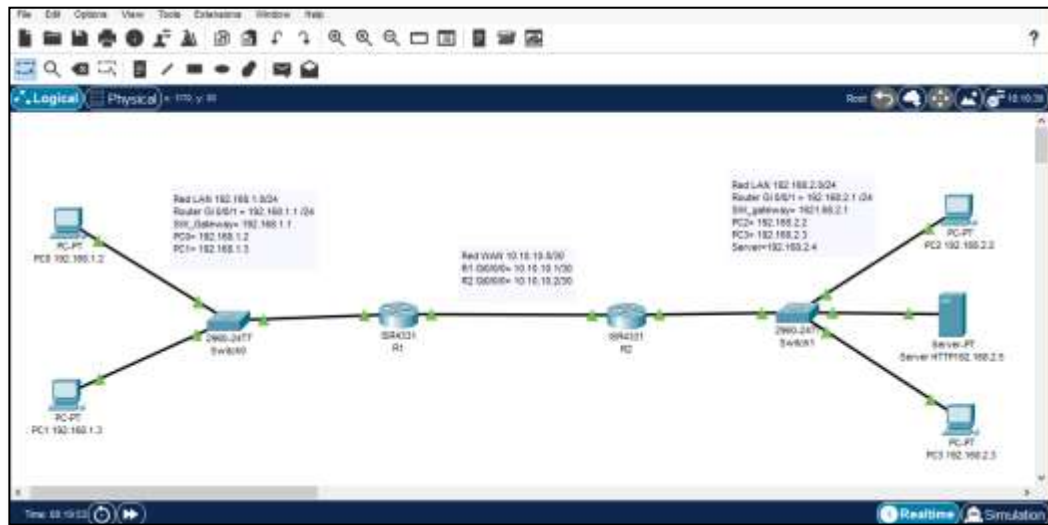
En último lugar, se analiza los beneficios y desventajas que presenta cada método de Qos y obteniendo conclusiones y recomendaciones de la presente investigación.



5.1 Simulación De Priorización De Tráfico.

Figura 20.

Topología de red en Packet Tracer



Nota: Elaboración. El autor

Para un detallado análisis de la priorización de tráfico se realizó la simulación de una red, a la mencionada red se le aplicará tráfico ICMP y HTTPS. El objetivo de la simulación es determinar los beneficios que trae implementar QoS en la red, así como comparar la cabecera de los paquetes IP de la red sin aplicar priorización de tráfico con las cabeceras que tendrían los paquetes IP la red aplicando métodos de priorización de tráfico.

5.1.1 Análisis Del Campo DSCP En Las Cabeceras IP Sin Aplicar Políticas De QoS

El análisis de tráfico no priorizado, es decir, sin aplicar la configuración de QoS en la red. En la red LAN sin QoS, los switches y routers tiene la función de dejar pasar los flujos provenientes de los orígenes, todos ellos sin características de priorización de tráfico de red, es decir, todos los paquetes circulan por la red con la misma cabecera IP, sin asignar ningún marcado o señalización.

Para esta primera instancia, producimos un tráfico ICMP (comando ping) desde PC 0. 192.168.1.2 hasta PC 2 192.168.2.2, en las gráficas resultantes de las interfaces del R1 observamos que no existe ningún cambio en las cabeceras de los paquetes IP específicamente en el campo DSCP.

Figura 21.
Comando Ping desde PC 0 a PC 2

```
PC0 192.168.1.2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20D:BDFE:FEA5:867A
    IPv6 Address . . . . . : ::
    IPv4 Address . . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : ::
                                192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . . :
    IPv4 Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :
                                0.0.0.0

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

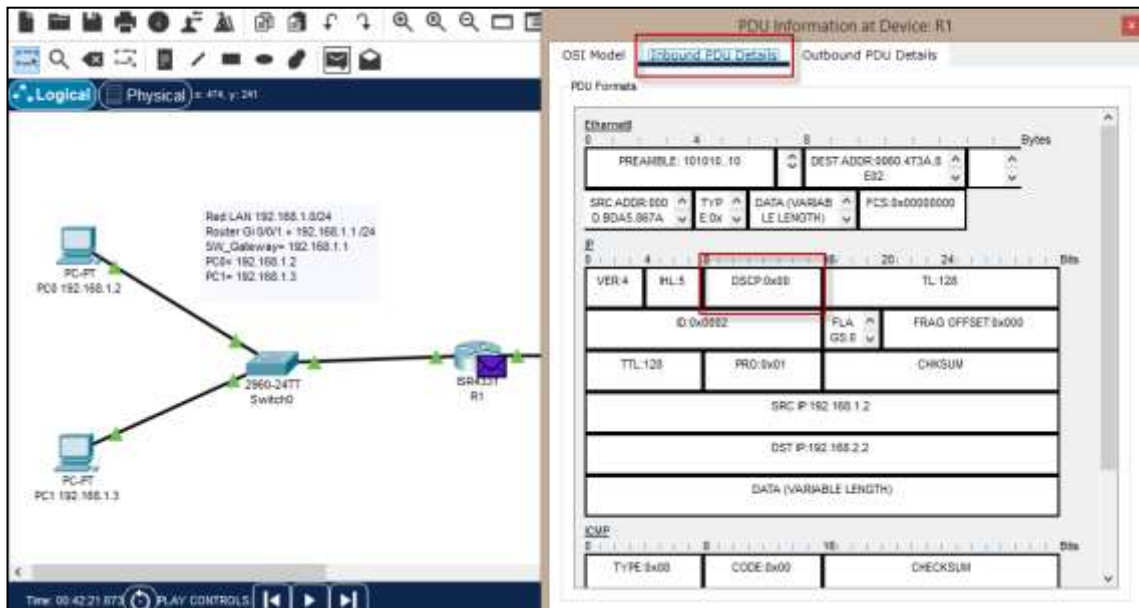
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

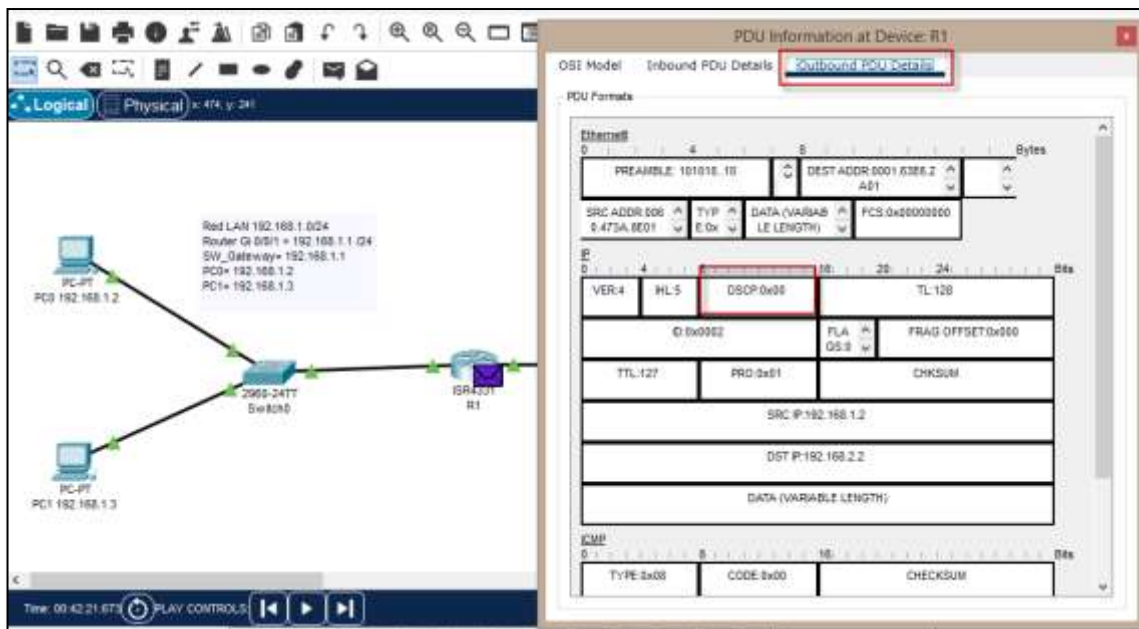
Nota: Elaboración. El autor

Figura 22.
Cabecera IP en la interfaz de entrada del R1, aplicando tráfico ICMP



Nota: Elaboración. El autor

Figura 23.
Cabecera IP en la interfaz de salida del R1, aplicando tráfico ICMP

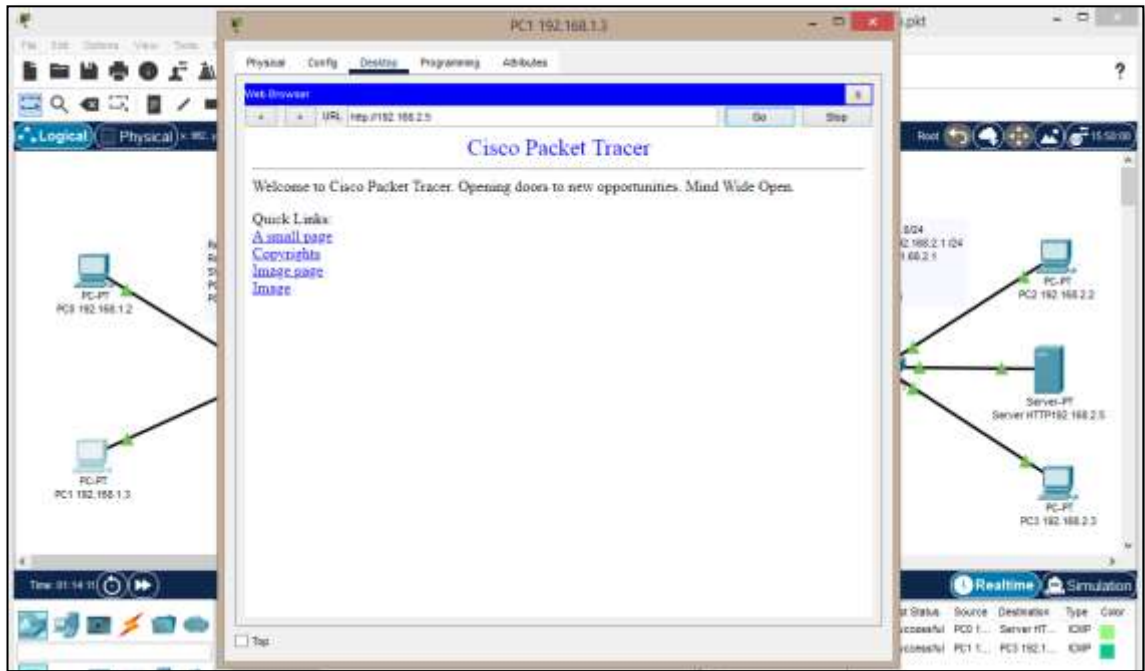


Nota: Elaboración. El autor

Ahora, produciremos tráfico HTTPS, desde PC 1 192.168.1.3 al servidor HTTP 192.168.2.5 y a capturar los paquetes IP con la ayuda de Packet Tracer.

Figura 24.

Tráfico Http desde PC 1 hasta el servidor http



Nota: Elaboración. El autor

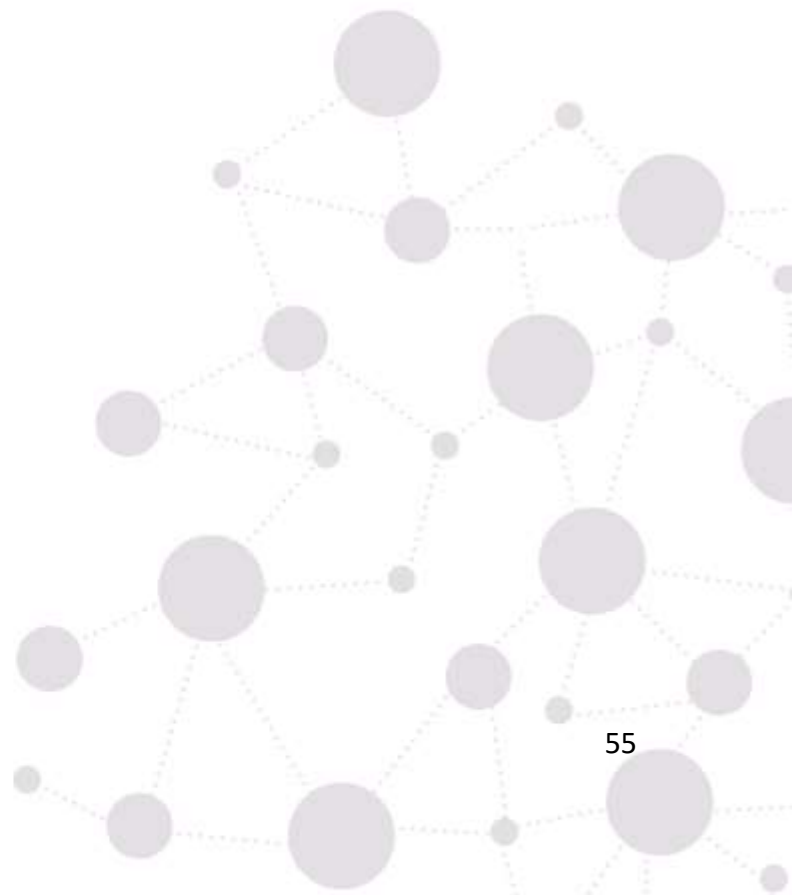
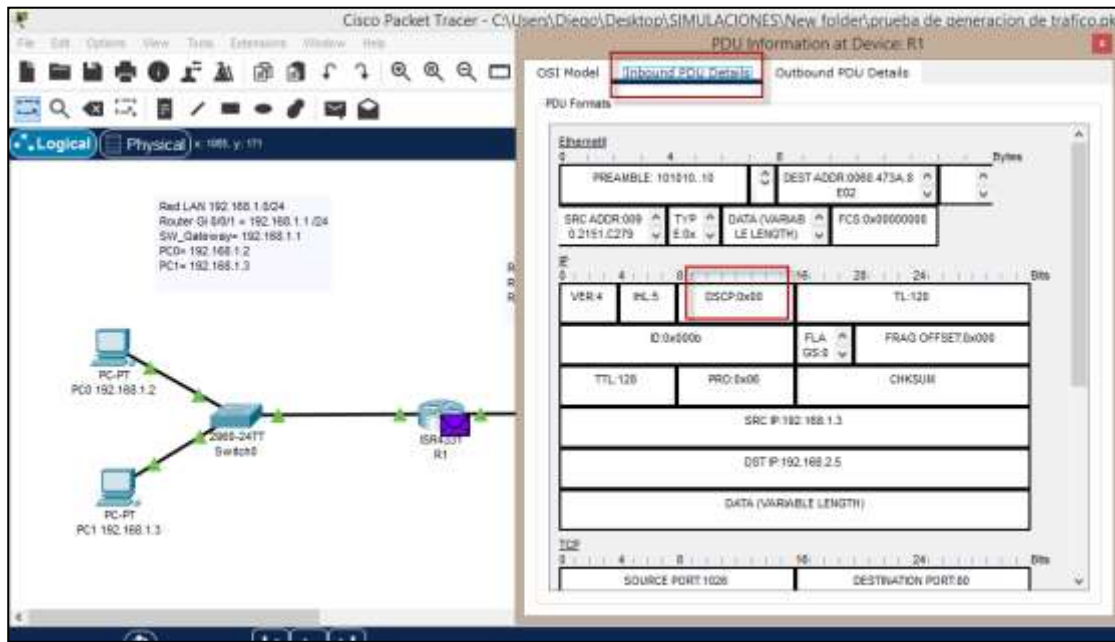
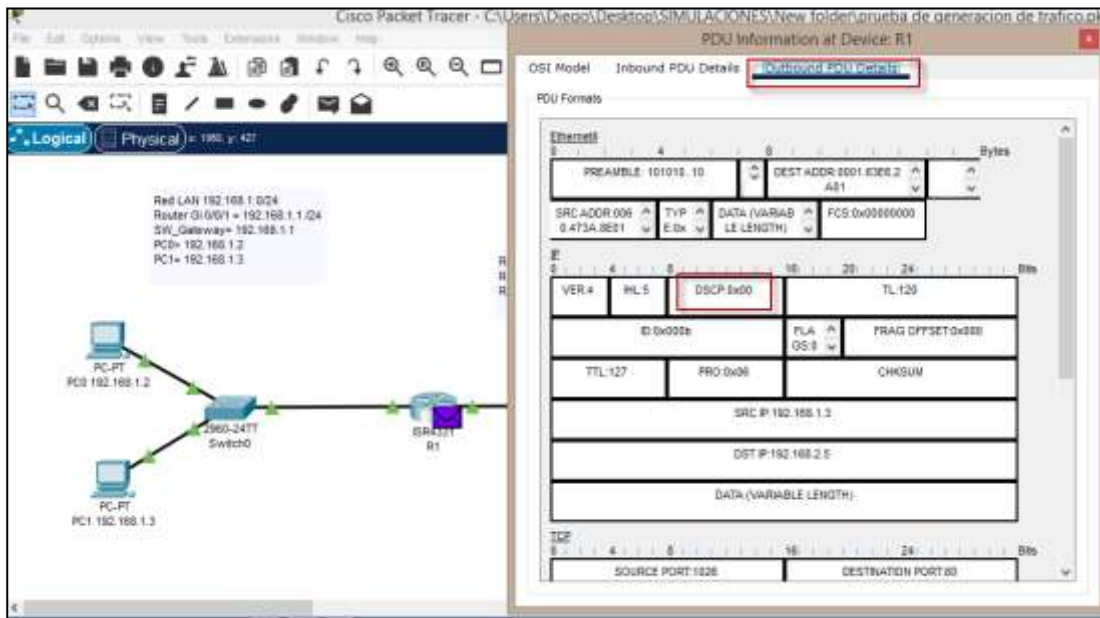


Figura 25.
Cabecera IP en la interfaz de entrada del R1, aplicando tráfico HTTP



Nota: Elaboración. El autor

Figura 26.
Cabecera IP en la interfaz de salida del R1, aplicando tráfico HTTP



Nota: Elaboración. El autor

Nótese, que el campo DSCP no sufre ninguna alteración en ambos casos, debido a que no se ha aplicado ninguna configuración para diferenciar el tráfico.

5.1.2 Análisis del campo DSCP en las cabeceras IP aplicando políticas de QoS

La segunda parte de simulación consiste en aplicar QoS agregando configuraciones de políticas de calidad de servicio en los routers. Los resultados que presenten los paquetes de la red con las configuraciones de priorización de tráfico, permitirán analizar la optimización de la red, antes y después de aplicar QoS.

A continuación, se describe las configuraciones aplicadas.

5.1.2.1 Clasificación, Marcado Y Política Del Tráfico En El Router 1

Los comandos utilizados se detallan a continuación.

```
class-map match-all http // crea la clase http.
```

```
match protocol http // adjunta a la clase http, todo el tráfico que coincida con el protocolo http
```

```
class-map match-all icmp // crea la clase icmp.
```

```
match protocol http // adjunta a la clase icmp, todo el tráfico que coincida con el protocolo icmp.
```

```
policy-map marcado // creamos la política llamada marcado
```

```
class http // indica que marcaremos la clase llamada http
```

```
set ip dscp af31 // a todo el tráfico http le marcaremos con el DSCP = af31
```

Al tráfico ICMP lo marcaremos de la siguiente manera

```
class icmp // indica que marcaremos la clase llamada icmp
```

```
set ip dscp af11 // a todo el tráfico http le marcaremos con el DSCP = af311
```

Aplicamos la política llamada marcado en la interfaz de salida de R1

```
interface gigabitEthernet 0/0/0//ingresamos a la interfaz donde se va a aplicar la política
```

```
service-policy output marcado // con este comando se aplica la política.
```

5.1.2.2 Aplicación De Política En El Router 2

En el Router 2, creamos clases, se las puede denominar con cualquier nombre, en este caso vamos a colocar el mismo nombre que se colocó a las clases del router 1



```
class-map match-all http // creamos la clase http
match ip dscp af31 // dentro de la clase http, se van a ubicar todos los paquetes
que tengan af31
```

```
class-map match-all icmp // creamos la clase icmp
match ip dscp af11 // dentro de la clase icmp, se van a ubicar todos los paquetes
que tengan af11
```

Vamos a aplicar la siguiente política de remarcado al tráfico que proviene del router 1: Si pertenece a la clase http le asignamos el marcado de capa 2 CoS = 3, si pertenece a la clase icmp, le asignamos el CoS = 0

```
policy-map remarcado // se crea la política llamada remarcado
class http // ingresamos a la clase llamada http
set precedence 3 // a los paquetes de la clase http los vamos a remarcar con CoS
=3
```

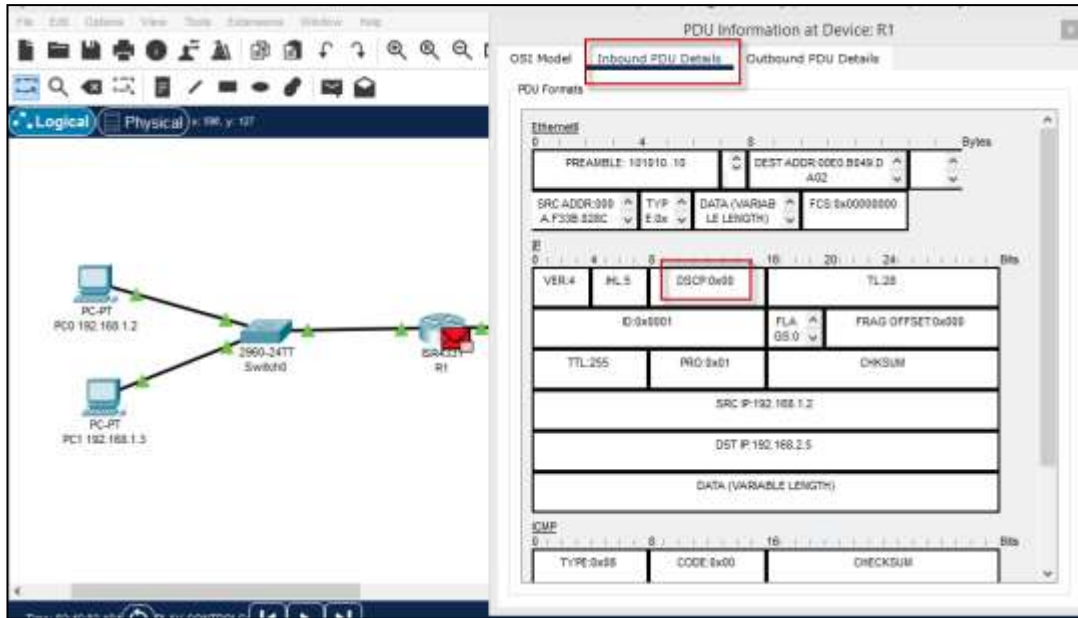
```
class icmp // ingresamos a la clase llamada icmp
set precedence 0 // a los paquetes de la clase http los vamos a remarcar con CoS
=0
```

Para comprobar, la priorización del tráfico, utilizamos el Packet tracer y observamos el campo DSCP en la cabecera del paquete

Cuando aplicamos el comando ping (tráfico ICMP) desde PC 1 192.168.1.3 a PC 2 192.168.2.2, observamos las interfaces de los routers 1 y 2

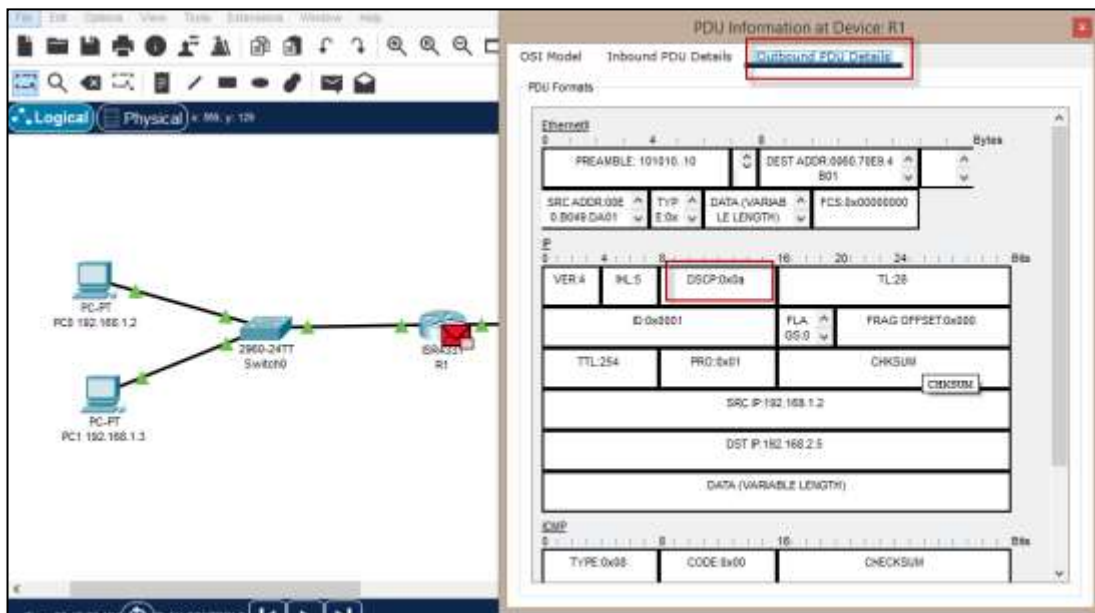
En la interfaz de entrada de R1, el campo DSCP = 0, pues no se ha aplicado ninguna configuración.

Figura 27.
Cabecera IP en la interfaz de entrada del R1, aplicando tráfico ICMP



Nota: Elaboración. El autor

Figura 28.
Cabecera IP en la interfaz de salida del R1, aplicando tráfico ICMP



Nota: Elaboración. El autor

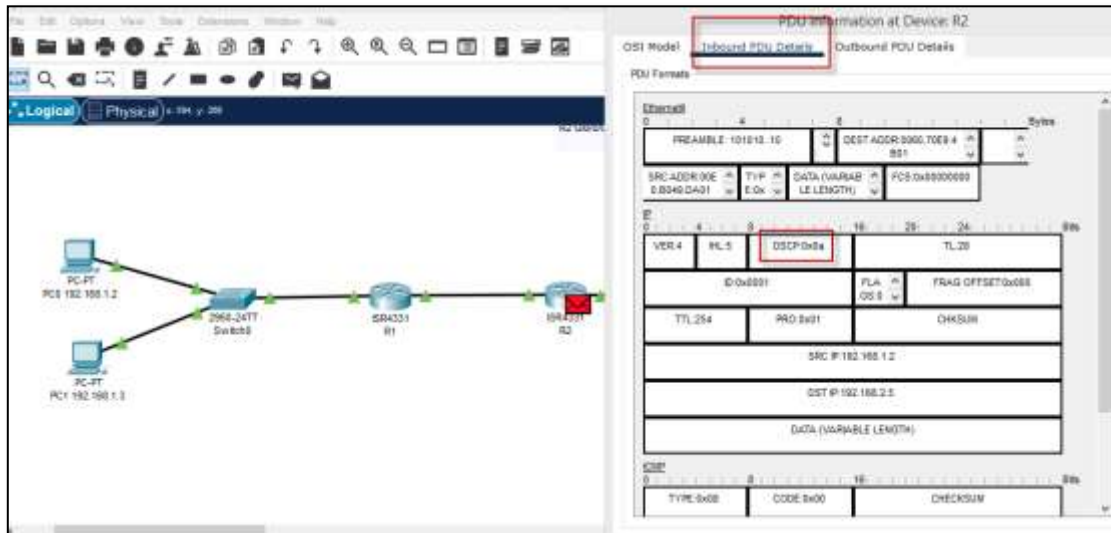
Como se observa en el campo DSCP ya está marcado el tráfico con el valor 0x0a, que es un valor hexadecimal.

0x0a (hex) = 10 (dec) = af11, ver figura 15

Con lo que se comprueba que el tráfico ICMP fue marcado con af11

Figura 29.

Cabecera IP en la interfaz de entrada del R2, aplicando tráfico ICMP

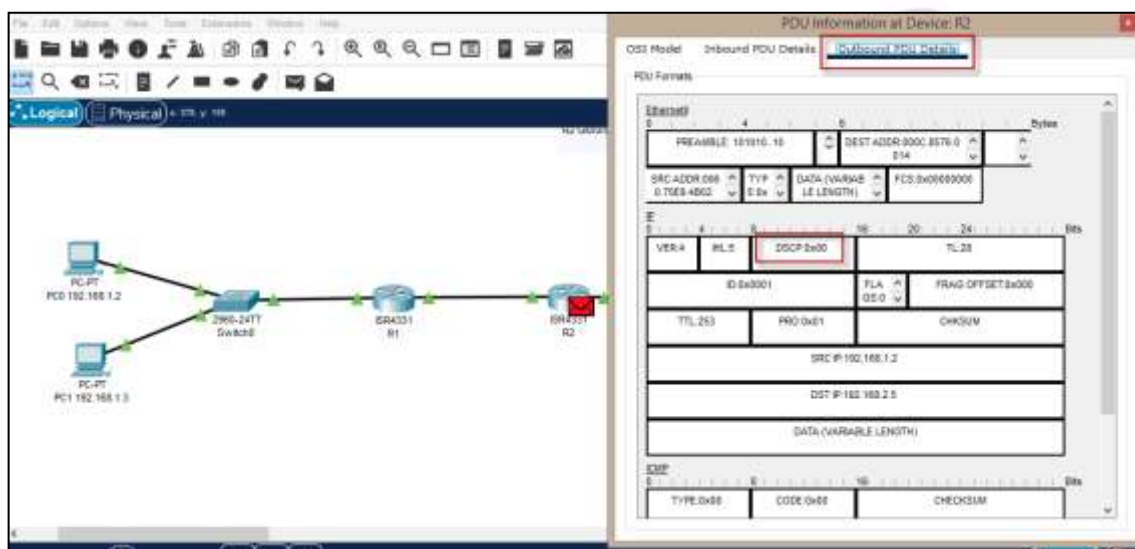


Nota: Elaboración. El autor

En la figura anterior, vemos que se mantiene el valor af11 = 0x0a(hex) en la interfaz de entrada de R2.

Figura 30.

Cabecera IP en la interfaz de salida del R2, aplicando tráfico ICMP



Nota: Elaboración. El autor

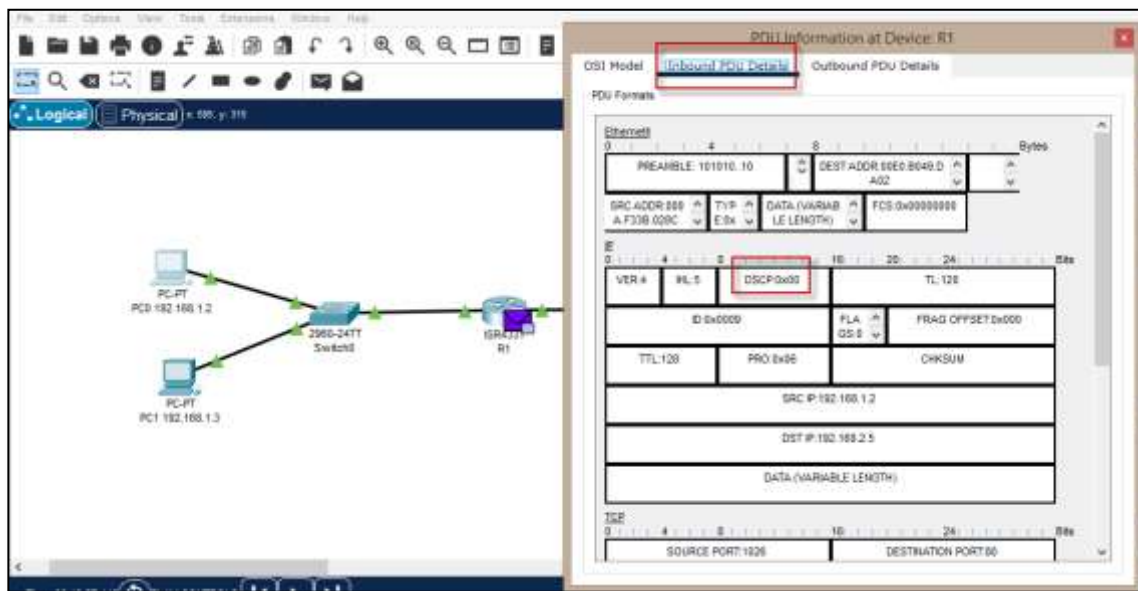
Vemos que se aplica de manera correcta la política denominada “remarcado” que indica que el tráfico ICMP sea remarcado con IPP (IP Precedence) = 0, en la interfaz de salida del R2.

De igual forma sucede con el tráfico http.

Dentro de la PC 0 192.168.1.2, usando la herramienta de Packet Tracer, abrimos un web browser y lo direccionamos al servidor http (192.168.2.5) y observamos lo que sucede en la cabecera IP del paquete, mientras viaja por los routers de la red.

Figura 31.

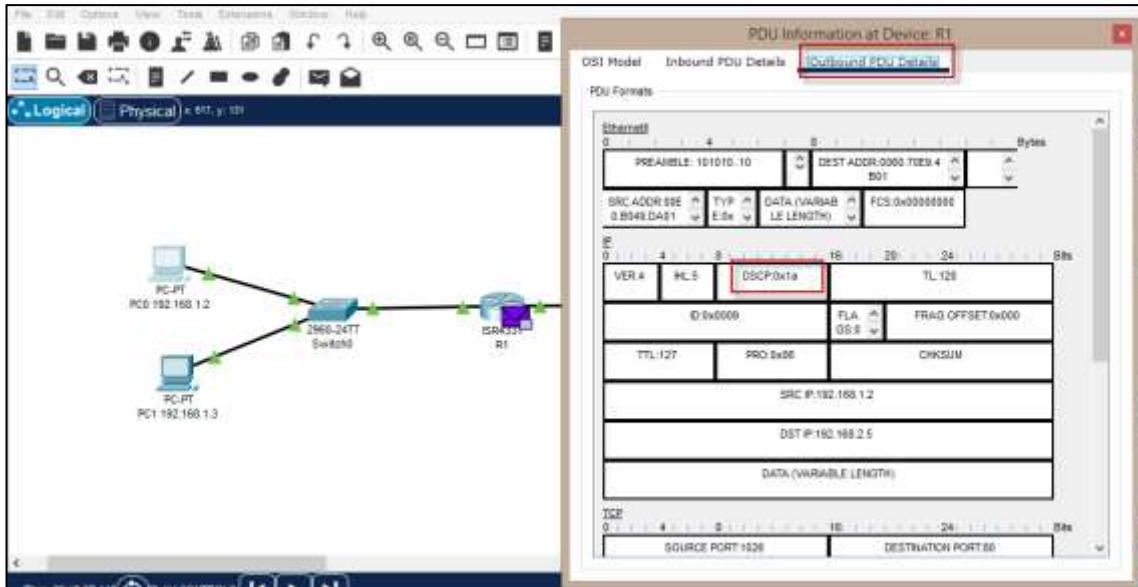
Cabecera IP en la interfaz de entrada del R1, aplicando tráfico http



Nota: Elaboración. El autor

En la figura anterior se muestra que no hay ningún cambio en el campo DSCP de la cabecera del paquete IP

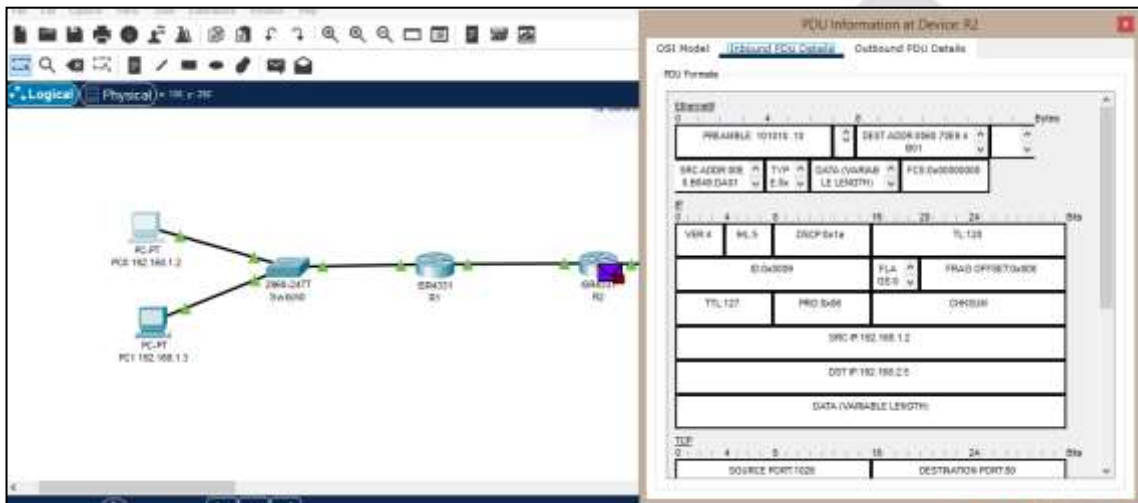
Figura 32.
 Cabecera IP en la interfaz de salida del R1, aplicando tráfico http



Nota: Elaboración. El autor

Luego de aplicar configuraciones para priorizar el tráfico, vemos que en la interfaz de salida de R1, se encuentra marcado con 0x1a (hex)=26 (dec) = af31, según la tabla 15, tiene mayor prioridad que el tráfico marcado con af11.

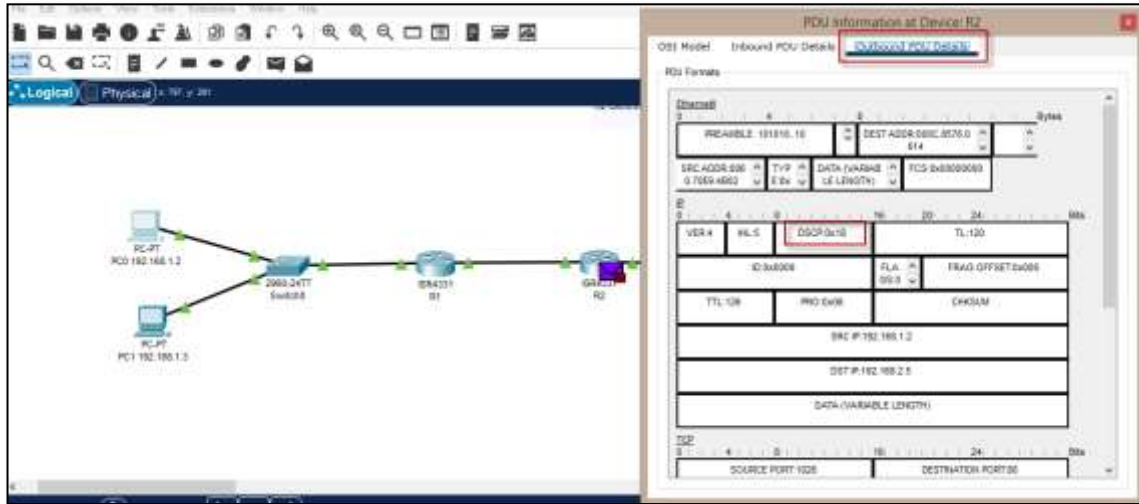
Figura 33.
 Cabecera IP en la interfaz de entrada del R2, aplicando tráfico http



Nota: Elaboración. El autor

En la entrada del R2, se mantiene el mismo DSCP, confirmando las configuraciones, pues, no se aplicó ningún cambio en las mismas.

Figura 34.
 Cabecera IP en la interfaz de salida del R2, aplicando tráfico http



Nota: Elaboración. El autor

Se aplica de manera correcta la política denominada “remarcado” que indica que el tráfico HTTP sea remarcado con IPP (IP Precedence) = 3, en la interfaz de salida del R2.

Con la simulación, se verifica las configuraciones necesarias que se deberían aplicar a los routers para dar prioridad al tráfico sensible de la red. Se puede priorizar cualquier tipo de tráfico, queda a discreción del administrador de la red, analizar que tráfico requiere mayor prioridad.

6. Resultados

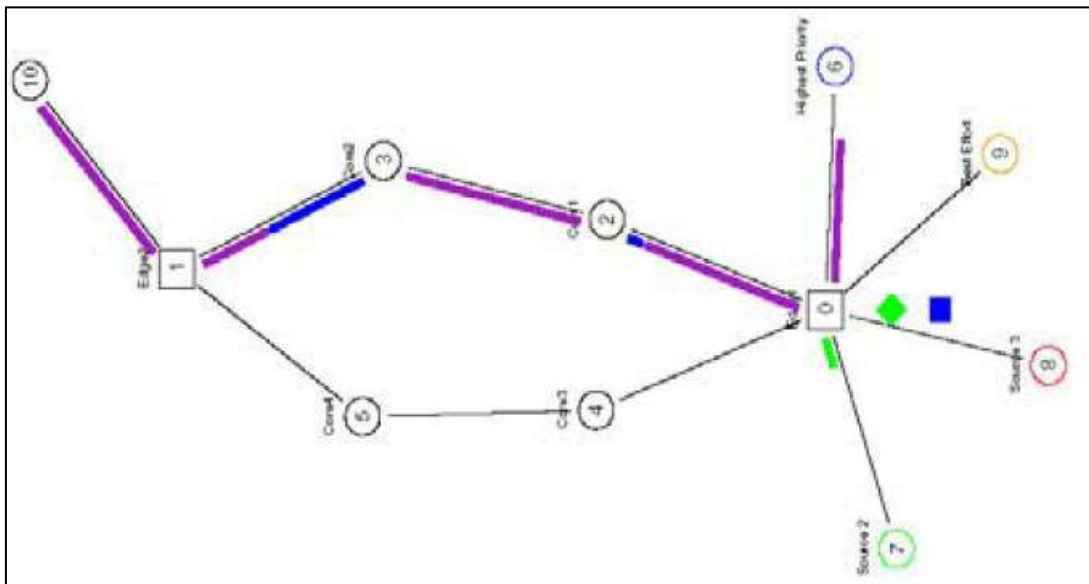
En esta sección se analiza los resultados de diferentes investigaciones, se revisan los parámetros sobre los cuales se enfocan las investigaciones y el método como se planteó la recolección de datos, ya sea mediante simulación, laboratorio de pruebas real o infraestructura de red ya instalada y en funcionamiento.

6.1 Investigación 1.

En la investigación denominada “**Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models**”, en esta investigación los autores comparan los métodos de QoS diffser, interv y QoS en IPv6. [18]

Los tres esquemas de QoS se simulan utilizando el simulador ns-2. [19]

Figura 35.
Topología de red



Nota: Adaptado de Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models, (2005)

Los nodos emisores generan tres flujos de tráfico con distintos niveles de prioridad. La fuente de mayor prioridad genera un tráfico de velocidad constante a una velocidad de 0,5 Mbps y prioridad fijada en 15 (nivel más alto). La fuente 2 genera tráfico constante también, pero a una velocidad de 0,25 Mbps y con los niveles de prioridad fijados en 12. La fuente 3 genera el mejor esfuerzo (Best Effort) a una velocidad igual a 0,25 Mbps, con prioridad fijada en 8.

Los flujos de tráfico se configuran para que violen el ancho de banda solicitado mediante un aumento del 30% poco después del inicio de la simulación. Las políticas de QoS IPv6 se configuran para degradar los flujos de tráfico del nivel 15 al nivel 12 y del nivel 12 al mejor esfuerzo. Este escenario se utilizará para simular todos los esquemas de QoS. A continuación, se resumen los resultados de cada escenario de simulación.

Simulación QoS IPv6

Figura 36.
Resultado QoS IPv6

Traffic Source No.	Flow ID	Av. Delay		P. Degraded		Loss Rate	
		In	Out	In	out	In	Out
H. Priority	15	13.71	14.60	0%	19.3%	0%	0%
Source 2	12	13.59	53.71	0%	10.8%	0%	8.6%
Source 3	8	18.35	102.4	0%	0%	0%	8.1%

Nota: Adaptado de Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models, (2005)

In: flujo de tráfico con congestión.

Out: flujo de tráfico sin congestión.

De la tabla se extraen los siguientes comentarios:

Flujos sin congestión

- El flujo de tráfico ID 15 no tiene paquetes perdidos ni degradados. El retardo de extremo a extremo es de 13,71 ms.
- El flujo de tráfico ID 12 tampoco ha perdido paquetes ni se ha degradado. El retraso ha sido 13,59 msec, que es poco, porque este flujo está configurado para ser un flujo de alta prioridad.
- Best effort no tiene paquetes perdidos. El retardo fue de 18,35ms, es el valor más alto.

Flujos con congestión:

- El flujo ID 15 tiene un 19,31% del total de paquetes degradados al nivel 12. No se descarta ningún paquete. El retardo es de 14,60 msec, lo que supone un aumento de aproximadamente 1 msec en comparación con el caso sin congestión.

- El flujo ID 12 tiene un 10,75% del total de sus paquetes degradados al mejor esfuerzo, lo que resulta en una tasa de pérdida de paquetes del 8,6%. El retardo se incrementa en un factor de 4, es decir: 53,71 mseg.
- El flujo de tráfico Best effort produce un retardo muy elevado, 102,44 mseg, y una tasa de pérdida de paquetes más alta, 8,09%.

Simulación IntServ

Figura 37.
Resultado Intserv

Traffic source no.	Flow ID	Priority Level	Av Delay		Loss rate	
			In	out	In	out
H. Priority	100	15	15.85	1604.9	0%	0%
Source 2	200	12	14.04	1692.3	0%	0%
Source 3	300	B. effort	17.87	136.97	0%	24.17%

Nota: Adaptado de Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models, (2005)

Los ID de flujo identificados para los tres flujos de tráfico son FID 100 para la fuente de tráfico H. Priority, FID 200 para los paquetes Source 2 y FID 300 para los paquetes Source 3, best effort.

El tiempo establecido para el intercambio de mensajes RSRV es de 1 segundo, que se añadirá al retardo de extremo a extremo.

La prueba con flujos sin congestión:

- Los flujos FID 100 y FID 200 presentan un menor retardo de extremo a extremo, 15,85 mseg y 14,04 mseg respectivamente.
- Todos los paquetes pertenecientes a estos flujos fueron entregados.
- Los paquetes del flujo de tráfico de mejor esfuerzo alcanzaron un retardo superior al de las otras dos fuentes (17.87 mseg), ya que no se reservaron recursos.
- En este escenario no se perdió ningún paquete.

En el caso de los flujos con congestión

- El retardo aumenta considerablemente, más de 10 veces que en el caso sin congestión tanto para los flujos FID 100 como 200. No se descartaron paquetes de estos flujos. Porque, los paquetes no se descartan, sino que se ponen en cola, ya que su prioridad es alta.
- Se observa que el retardo de los flujos de la fuente 2 es superior al de los flujos de la fuente 1.

Simulación Diffserv

Figura 38.
Resultado Diffserv

Traffic source no.	Flow ID	Pri Level	Av Delay		Loss rate	
			In	out	In	out
H. Priority	100	15	29.90	211.94	0%	14.78%
Source 2	200	12	26.88	200.85	0%	7.4%
Source 3	300	B.effort	30.88	199.59	0%	5.92%

Nota: Adaptado de Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS 38. models, (2005)

La prueba con flujos sin congestión:

- Los flujos FID100 y 200 han alcanzado un retardo de extremo a extremo de 29,90 mseg y 26,88 mseg respectivamente. No se cayó ningún paquete perteneciente a estos flujos.
- Best effort registró el mayor retardo durante la simulación conforme.

Durante la prueba con flujos con congestión.

- Los flujos FID100 y 200 ambos han alcanzado un retardo mayor, 211,94 mseg y 200,85 mseg.
- También han sufrido pérdidas de paquetes, FID100 tiene un 14,78% y FID200 un 7,4%. Este aumento del retardo y de la tasa de pérdida se debe al aumento de las tasas de tráfico, ya que DiffServ elimina los paquetes no conformes.

- Best effort, sufre pérdida de paquetes, 5,92%, durante la simulación con congestión.

Conclusión de la investigación titulada “Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models”:

Los resultados de delay, son mucho mayores en Intserv comparados con los de Diffserv, el retraso se da porque en Intserv, se negocia una ruta fija antes de empezar la transmisión de flujo.

En cambio, la pérdida de paquetes es menor en Intserv comparado con Diffserv, esto se da por que, una vez establecida la ruta de Intserv, se establece un canal fijo por donde se transmitirá la información.

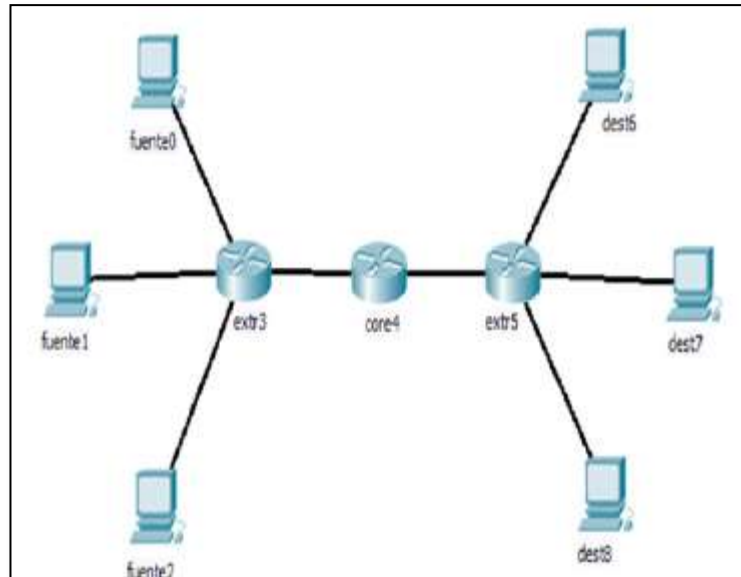
Adicional, los resultados de las simulaciones muestran que el modelo de gestión de la QoS de IPv6 supera a los esquemas IntServ y DiffServ. También muestran que el esquema IPv6 QoS es escalable y sencillo de implementar, ya que los routers centrales no participan en los procedimientos de reserva y no intervienen otros algoritmos QoS.

6.2 Investigación 2.

En la investigación denominada “COMPORTAMIENTO DE LOS SERVICIOS DIFERENCIADOS (DIFFSERV) Y LOS SERVICIOS INTEGRADOS (INTSERV) EN REDES IP PEQUEÑAS” [20]

Los autores muestran los resultados obtenidos de la implementación de los modelos Diffserv, IntServ y Best Effort sobre una misma topología de red, utilizando Network Simulator NS-2.33 con el fin de comparar el desempeño de los modelos, en parámetros como la pérdida de paquetes, el jitter y el retardo.

Figura 39.
Topología usada en el proyecto



Nota. Adaptado de Comportamiento de los servicios diferenciados (diffserv) y los servicios integrados (intserv) en redes ip pequeñas, por Segura D., González F. López D., 2011

Los autores, han determinado 3 fuentes que generan el tráfico

- La fuente 0 es una fuente de tasa constante de bits (CBR), con una tasa de 2Mbps.
- La fuente1 está asociada a un generador de tráfico de tipo Pareto. Pareto On/Off, genera tráfico de acuerdo a una distribución On/Off. Los paquetes son enviados a cierto valor de tasa durante los periodos de encendido (burst_time) y durante los periodos de apagado (idle_time) no se envían paquetes.
- La fuente2 se asocia con un generador de tráfico exponencial. Éste transmite durante 2ms y deja de transmitir otros 2ms.

Para la simulación, se inyecta el tráfico dentro de la red y se observa el comportamiento de las variables: jitter, retardo y perdida de paquetes.

Figura 40.
Paquetes perdidos

CASO	FLUJO 1	FLUJO 2	FLUJO 3
BEST EFFORT	0	0	0
DIFFSERV	146	957	849
INTSERV	0	954	830

Nota: Adaptado de Comportamiento De Los Servicios Diferenciados (Diffserv) Y Los Servicios Integrados (Intserv) En Redes Ip Pequeñas, (2011)

Best effort, se basa en la idea de ofrecer toda la capacidad de canal para transmitir todo el tráfico generado. Es por esto que no se presentan pérdidas de paquetes ni encolamientos, sin embargo, variables como el jitter y el delay sí tienen ciertas variaciones.

En el flujo 1, en Intserv, no presenta pérdida de paquetes. Esto se da porque toda la capacidad del canal está reservada al flujo 1 que está asociado a la sesión que solicita la reserva.

Figura 41.
Jitter

CASO	FLUJO 1	FLUJO 2	FLUJO 3
BEST EFFORT	600ms	1.2ms	1.2ms
DIFFSERV	4ms	7ms	6.8ms
INTSERV	2ms	2.7s	2.7s

Nota: Adaptado de Comportamiento De Los Servicios Diferenciados (Diffserv) Y Los Servicios Integrados (Intserv) En Redes Ip Pequeñas, (2011)

IntServ presenta una desventaja sobre Diffserv y radica en que, si el flujo 1 ocupa todo el canal disponible, el jitter de los flujos 2 y 3 se vuelve muy grande. En este sentido Diffserv tiene ventaja sobre Intserv, pues el jitter tiene un valor promedio de 6ms para los tres flujos.

Figura 42.
Delay

	FLUJO 1	FLUJO 2	FLUJO 3
IDEAL	46.6ms	46.6ms	46.6ms
DIFFSERV	145ms	145ms	145ms
INTSERV	49ms	2.8s	2.8s

Nota: Adaptado De Comportamiento De Los Servicios Diferenciados (Diffserv) Y Los Servicios Integrados (Intserv) En Redes Ip Pequeñas, (2011)

La principal causa de las variaciones del delay es el tipo de tráfico implementado. En el caso del flujo 1, que es originado por la fuente de tráfico CBR el delay alcanza un valor constante de 46ms.

Similar a lo que sucede con el jitter, el delay también toma valores bastante grandes con IntServ cuando un flujo ocupa todo el canal disponible. Ventaja que toma DiffServ sobre IntServ.

Conclusión de la investigación:

Conocido el funcionamiento tanto de DiffServ como de IntServ es difícil decir cuál de los dos modelos es mejor.

Se debe analizar desde el punto de vista de la aplicación o servicio que hará uso del modelo. Por ejemplo, si se habla de la red de un banco para conectar sus cajeros automáticos es posible que se prefiera utilizar IntServ que a pesar de tener un retardo mayor la pérdida de paquetes es muy baja, lo que evitaría errores en las transacciones.

Pero si lo que queremos es utilizar varias aplicaciones con diferentes tipos de fuentes de tráfico es posible que se prefiera usar DiffServ.

6.3 Investigación 3.

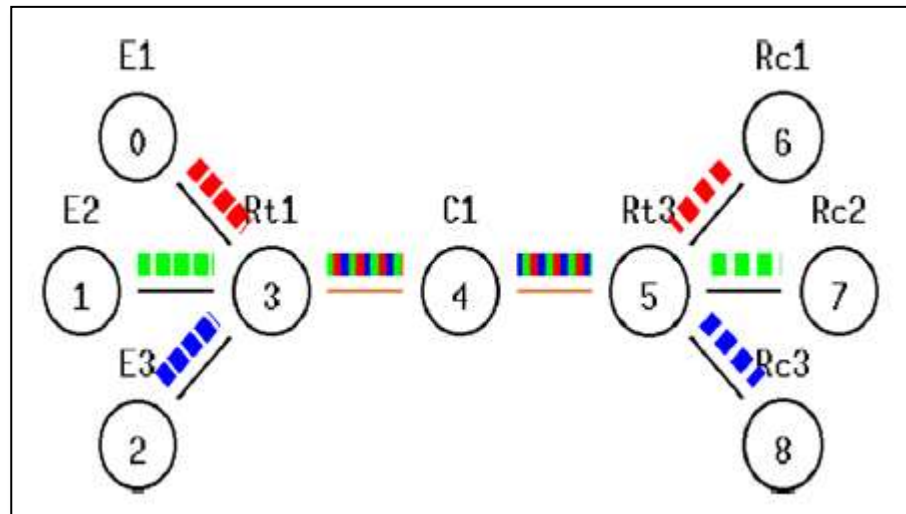
La siguiente investigación a revisar se denomina “**CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2**” [21]. Se evalúan los parámetros para garantizar calidad de servicio como son el ancho de banda, la pérdida de paquetes y el retardo, sobre una topología de red que involucra tres tipos de tráfico (CBR, Pareto y Exponencial). Las configuraciones se implementan en el simulador de redes NS2, donde el primero corresponde a un caso sin QoS, con una

capacidad de canal que es suficientemente grande para transmitir los tres tipos de tráfico, mientras que en los siguientes casos la capacidad se reduce a un menor tamaño y se estudian diferentes parámetros de calidad de servicio.

Para observar el comportamiento de los tráficos se implementa inicialmente una red sin QoS con dos tipos de encolamiento y posteriormente se realiza una configuración que implementa QoS mediante los modelos IntServ y DiffServ.

Los resultados obtenidos de estas simulaciones son graficados y comparados con el fin de determinar el comportamiento más adecuado en redes IP.

Figura 43.
Topología usada en el proyecto



Nota. Adaptado de CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2, por Vallejo J., y Rico J. (2011)

La red se compone de tres fuentes de tráfico con sus respectivos equipos destino donde el núcleo de la misma se compone de un dispositivo de capa 3 central con dos enlaces que lo conectan a un par de DTEs en los extremos.

Cada una de las fuentes corresponde a un flujo distinto, los cuales iniciarán y terminarán en tiempos diferentes con el objetivo de observar el comportamiento del canal al adicionar los tráficos y la forma de funcionar al llegar a la saturación del mismo.

Los flujos de datos simulados tienen las siguientes características:

- El primero se identifica con color rojo y corresponde a un tráfico CBR (tasa constante de bits). Puede utilizarse en servicios como telefonía y videoconferencias [22]. Y utiliza gran parte del ancho de banda del canal, generando congestiones.
- El segundo se representa con color verde y es un flujo tipo Pareto [23]. Se caracteriza por largas ráfagas causadas por manejos de grandes paquetes [24]. Además, tendrá una prioridad intermedia al implementar el modelo DiffServ.
- El último tipo de tráfico es el de color azul y tiene un comportamiento tipo exponencial. Su nombre se debe a que los intervalos de llegada de paquetes tienen una distribución de esta forma [25].

Figura 44.
Pérdida de paquetes

	Ideal	Sin QoS SFQ	Sin QoS Drop Tail	DiffServ	IntServ
CBR	0	126	92	0	0
Pareto	0	67	50	64	118
Exponencial	0	11	37	177	104

Nota: Adaptado de CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2, por Vallejo J., y Rico J. (2011)

Aquí se encuentra que, para el caso de una red sin calidad de servicio, el tráfico que envió más datos (CBR) es quien terminó perdiendo la mayor cantidad de paquetes, sin embargo al garantizar un ancho de banda donde puedan ser transmitidos todos los tráficos no se dieron pérdidas.

Al implementar calidad de servicio se garantizó que todos los paquetes de un tráfico prioritario llegaran a su destino cuando el canal fue saturado, haciéndolo conveniente para aquellas aplicaciones en donde es de vital importancia que los datos lleguen correctamente en el menor tiempo posible, como lo es el caso de las videoconferencias.

Es importante recalcar que al incluir QoS se debe tener en cuenta si se desea aplicar prioridad a más de un tráfico, ya que, si este es el caso, es preferible la implementación de DiffServ, con lo cual se le asigna una prioridad un poco más baja al flujo que menos necesite.

Figura 45.
Retardo

	Sin QoS		DiffServ		IntServ	
	Max	Prom	Max	Prom	Max	Prom
CBR	75	70	65	50	48	48
Pareto	72	68	66	51	63	62
Exponencial	70	69	66	50	63	61.8

Nota: Adaptado de CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2, por Vallejo J., y Rico J. (2011)

En la tabla se puede apreciar que la red sin calidad de servicio presentó los mayores retardos de transmisión tanto máximos como en su valor promedio, mientras que al implementar QoS este disminuyó.

Para el flujo prioritario el modelo IntServ tuvo el mejor tiempo promedio de transmisión, aunque no muy distante del modelo DiffServ, sin embargo, en los demás tráficos el modelo DiffServ obtuvo los mejores valores promedio de retardo.

Figura 46.
Jitter

	Jitter (ms)					
	Sin QoS		DiffServ		IntServ	
	Max	Prom	Max	Prom	Max	Prom
CBR	1	0.1	1	0	1.5	0.001
Pareto	2.3	0.13	2	0.1	2.3	0.02
Exponencial	2.3	0.14	1.98	0.11	2.2	0.02

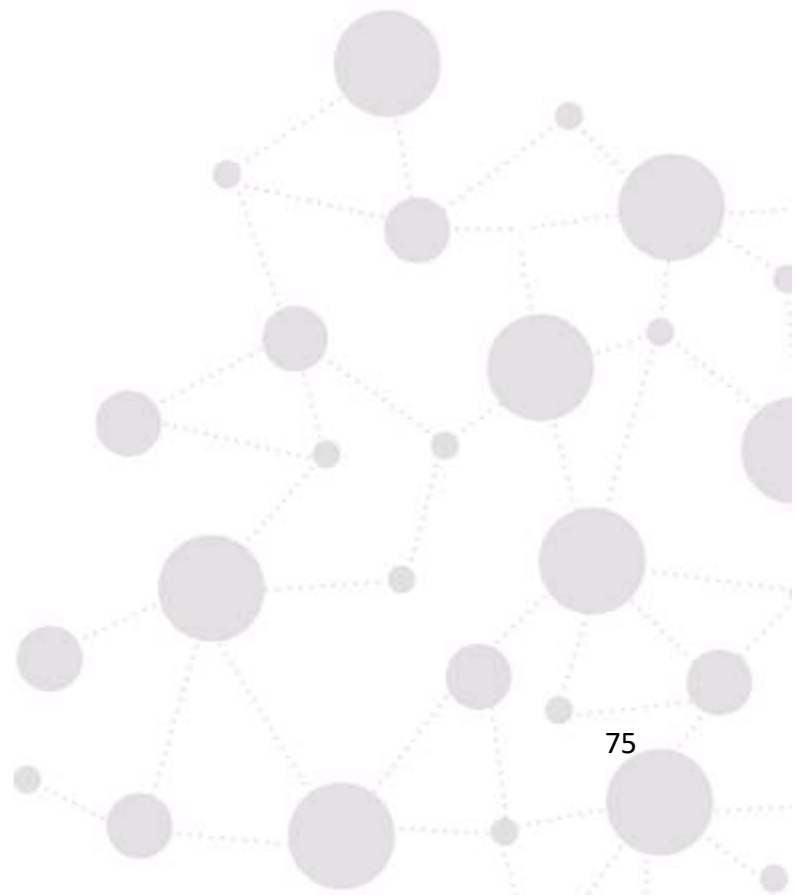
Nota: Adaptado de CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2, por Vallejo J., y Rico J. (2011)



En cuanto al jitter, la tabla permite ver que tanto la red sin calidad de servicio como la misma con la implementación del modelo Diffserv tuvieron promedios similares cercanos a 0.1 ms. Este valor, aunque es despreciable frente al valor de retardo obtenido, es mayor al encontrado con la implementación de IntServ, donde el valor para el tráfico prioritario fue muy cercano a cero.

Conclusión de la investigación:

Se concluye que, cuando surge la necesidad de seleccionar alguno de los dos modelos de QoS. El modelo IntServ aunque garantiza el ancho de banda para el tipo de tráfico seleccionado, deja los tráficos restantes sin QoS, causando que luchen entre ellos para poder enviar sus paquetes, a diferencia del modelo DiffServ, el cual asigna un tipo de prioridad a cada tipo de tráfico otorgando así una calidad de servicio diferente a cada uno, por ello, con DiffServ se pierde mucha información de un tipo de datos si estos tienen asignado el valor más bajo de prioridad y si el canal se encuentra saturado por mucho tiempo.



7. Discusión

En las 3 investigaciones analizadas, los autores consideran como parámetros para evaluar la efectividad de los métodos de QoS al retardo, jitter y pérdida de paquetes.

En las 3 investigaciones se nota una considerable diferencia de los resultados en los parámetros antes y luego de aplicar los métodos Intserv y Diffserv, puesto que con estos métodos se aumenta la probabilidad de que los paquetes prioritarios lleguen a su destino y si existiera congestión en la red, estos paquetes se ponen en cola, resultando en una reducida pérdida de paquetes.

De la investigación “Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models”, resaltamos lo ya expuesto anteriormente, donde se señala que los métodos Intserv y Diffserv, fueron implementados recientemente, es decir, no nacieron junto a IPv4, por lo que, aplicarlos resulta en mayor consumo de procesamiento por parte de los equipos de la red, además, de que no todos los dispositivos soportan estos métodos de QoS, por lo que se debe realizar un inventario de equipos de una red, señalando si es que se desea aplicar algún método de QoS.

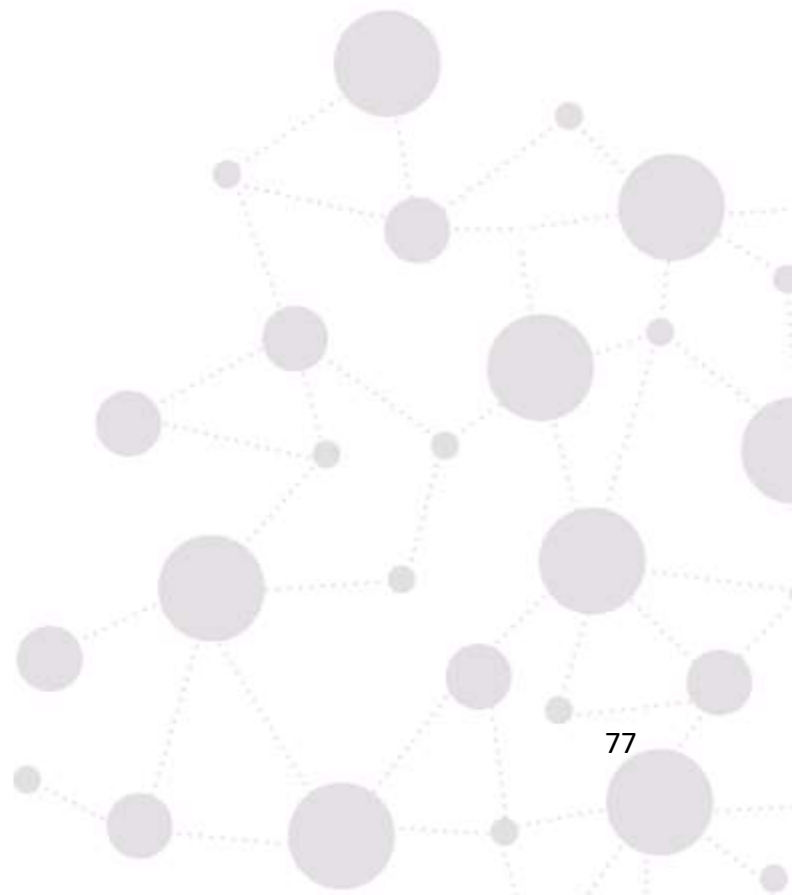
Como denominador común en las 3 investigaciones, tenemos que utilizan el software NS2 para realizar las simulaciones, dando a entender las elevadas prestaciones y versatilidad de este software.

Además, en ninguna de las investigaciones, se concluye de manera definitiva cual método es el mejor, pues como se menciona en las mismas, cada método tiene sus beneficios frente a un escenario, por ejemplo, para un tráfico prioritario como voz o video, bien se podría utilizar Intserv, que garantiza un ancho de banda a las aplicaciones, y se podría aplicar siempre y cuando la diversidad de tráfico sea baja, pues al establecer una ruta dedicada se merma el ancho de banda para el resto de aplicaciones, la desventaja de IntServ es que muchos estados deben almacenarse en cada enrutador dependiendo de las sesiones que se requieran iniciar, por lo tanto puede ser eficiente a pequeña escala pero a una escala grande como la de internet es muy difícil mantener el registro de todas las reservaciones necesarias, que ocuparían: capacidad de procesamiento, memoria y las frecuentes actualizaciones de estado consumirían parte del ancho de banda.

Conocido el funcionamiento tanto de DiffServ como de IntServ es difícil decir cuál de los dos modelos es mejor.

Se debe analizar desde el punto de vista de la aplicación o servicio que hará uso del modelo. Por ejemplo, si se habla de la red de un banco para conectar sus cajeros automáticos es posible que se prefiera utilizar IntServ que a pesar de tener un retardo mayor la pérdida de paquetes es muy baja, lo que evitaría errores en las transacciones.

Pero si por la red sobre la cual deseamos aplicar QoS, utiliza varias aplicaciones con diferentes tipos de fuentes de tráfico es posible que se prefiera usar DiffServ, ya que, al establecer las prioridades a cada tipo de tráfico, hace que la disponibilidad del canal sea dinámica y varíe para cada paquete.

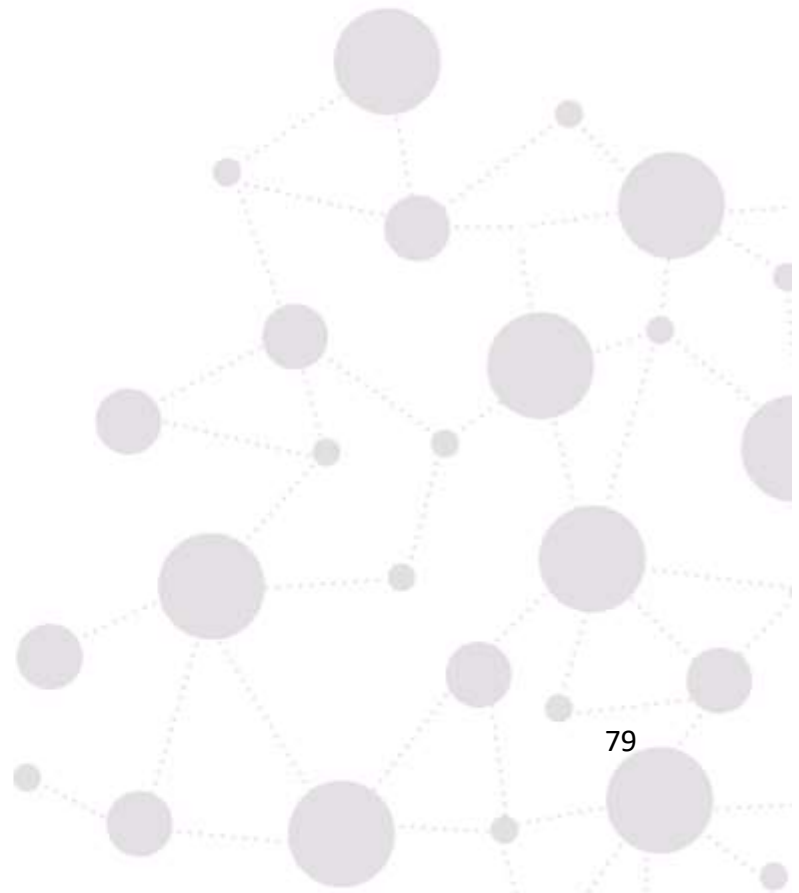


8. Conclusiones

- Se realizó una revisión del estado del arte referente a la calidad de servicio en las WLAN lo que permitió conocer más detalladamente los métodos de QoS como son INTSERV y DIFFSERV, como operan, así como, los elementos que los constituyen.
- Luego de analizar la información recopilada del tema de QoS, se concluye que los parámetros relevantes que permiten realizar una comparativa entre los métodos INTSERV y DIFFSERV son el ancho de banda, retardo, jitter y pérdida de paquetes.
- Para definir un procedimiento que permita a las empresas decidir sobre cual método de QoS aplicar, se debe analizar todos los detalles de los elementos que constituyen la red, pues cada red es diferente, se debe analizar el tamaño, las aplicaciones que utilizan, las prioridades de tráfico o incluso el presupuesto económico ya que incide en la marca y modelo de equipos con los cuales trabajar.
- Tras analizar los resultados obtenidos se ha podido ver la importancia de aplicar una configuración QoS a una red. Si no se utiliza QoS todos los flujos de tráfico tienen que competir entre ellos para enviar los paquetes, provocando un aumento de pérdidas en todos los flujos. Pero con QoS es posible dar prioridad a los flujos que transporten tráfico que necesite unos requerimientos específicos para proporcionar un servicio determinado.
- El método DiffServ es el más utilizado debido a que brinda versatilidad al no reservar previamente recursos, ni introduce sobrecargas en la red para brindar QoS, lo cual ayuda a que el rendimiento de la misma sea óptimo.
- Se concluye que QoS es una solución para priorizar el tráfico, ante situaciones de saturación de canal o congestión en la red ya que cada equipo administrará el tráfico de manera diferenciada, y brinda prioridades al tráfico que más lo requiere. Por el contrario, cuando no existen mecanismos de QoS, todos los diferentes tipos de tráficos son tratados de igual forma.
- La implementación de políticas de QoS permite la disponibilidad de todos los servicios de la red, QoS hace posible que los usuarios accedan a los servicios de manera simultánea, percibiendo un funcionamiento óptimo de la red.



- El mecanismo DiffServ permite dividir el tráfico en clases, controlando la cantidad de tráfico que cada cliente envía a la red y priorizándolo el envío a través de políticas de clasificación mejorando la eficiencia de una red significativamente.





9. Recomendaciones

- Para trabajar con los métodos de QoS, se recomienda verificar las versiones de IOS de los equipos, ya que dependiendo de las versiones se establecerá si soportan o no, la configuración de calidad de servicio (QoS).
- Si se desea aplicar QoS en infraestructuras reales, se debe coordinar los requerimientos con el administrador de la red, debido a que esto permitirá el funcionamiento óptimo de la red, sin crear conflicto con los intereses institucionales, para lograr la adecuada aplicación de políticas que permiten no solo un óptimo desempeño de los recursos tecnológicos sino también la consecución de los objetivos de las instituciones.
- Se recomienda extender la investigación aquí planteada a otros tipos de sistemas, como los de transmisión alámbricos y comparar el comportamiento obtenido con los inalámbricos.

10. Referencias Bibliográficas

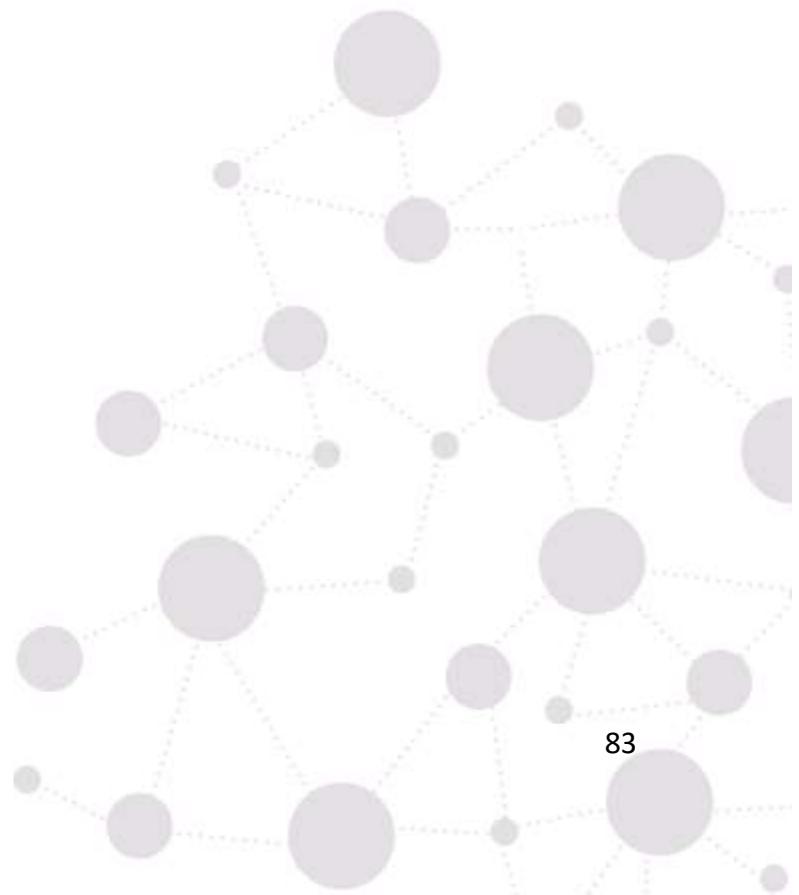
- [1] Flores, M. (2017), Estudio de los problemas de voip en redes de acceso inalámbricas. <https://www.dspace.espol.edu.ec/retrieve/c5759cb0-4fc0-4fca-92fe-2c8d8cd35b49/D-106125.pdf>
- [2] Fuenmayor-Rivadeneira, G. B. (2013), Modelo de Calidad de Servicio a Nivel de Enlace de Datos para Tráfico de Misión Crítica sobre Redes IEEE 802.11g en Modo Infraestructura. <https://www.redalyc.org/pdf/3442/344234341033.pdf>
- [3] Arce, J (abril 2015), Analisis de la provision de calidad del servicio para redes utilizando Diffserv e Intserv, Repositorio PUCE. <https://bibdigital.epn.edu.ec/bitstream/15000/5383/1/T2443.pdf>
- [4] Serrano Y. P. (2006). Estrategias de Configuración de redes WLAN IEEE 802.11e EDCA. Universidad Carlos II de Madrid. Dep. de Ing. Telemática
- [5] Prasad N. R. & Prasad A. R. (2004). 802.11 WLANs and IP Networking: Security, QoS, and Mobility. Prasad Anand.
- Seok-Kyu Kweon & Kang G. Shin. (2003). Statistical Real-Time Communication over Ethernet. IEEE Transactions on Parallel and Distributed Systems, 14.
- [6] Flores L., G., Paredes F., M., Jammeh, E., Fleury. M. J. Reed, M. & Ghanbari, M. (2006). Análisis a Nivel-Paquete de Simuladores de Red Contemporáneos. IEEE Latin America Transactions, 4(4).
- [7] Bernal B., C. A. (2004). Evaluación de la calidad del servicio (QoS) en una red inalámbrica 3G con arquitectura UMTS soportada en tecnología WCDMA, mediante el uso de software para simulación de redes. Tesis. Dir. Octavio José Salcedo Parra. Universidad Nacional de Colombia. Bogotá, D. C.
- [8] Hu, Qi G. W., Williamson, C. & Fapojuwo, A. O. (2011). Experimental evaluation of asymmetric QoS in IEEE 802.11 g wireless networks. En Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks. ACM. 1-8.
- [9] Sarkar, M. & Paolini, C. (2011). A QoS guaranteeing MAC layer protocol for the "underdog" traffic. EURASIP Journal on Wireless Communications and Networking, 2011(1), 1-15.



- [10] Grupo Is.com. (2019). Infraestructura. (<https://www.is.com.mx/infraestructura/redes/>)
- [11] Introducción a Tecnología Inalámbrica. ccnadesdecero.es. <https://ccnadesdecero.es/introduccion-tecnologia-inalambrica/>
- [12] ¿Qué es ieee 802.11e?, es.theastrologypage.com, <https://es.theastrologypage.com/ieee-802-11e>
- [13] TANENBAUM, A. y WETHERALL, D. (2012). Redes de computadoras. Editorial Pearson.
- [14] SOBREVIELA, L (2019). CALIDAD DE SERVICIO (QoS) CON ROUTERS CISCO
- [15] Calidad de Transmisiones de Red. ccnadesdecero.es. <https://ccnadesdecero.es/calidad-transmisiones-red/>
- [16] Modelos de QoS. ccnadesdecero.es. <https://ccnadesdecero.es/modelos-qos/>
- [17] El método de investigación bibliográfica. oocities.org. <https://www.oocities.org/zaguan2000/metodo.html#:~:text=En%20sentido%20m%C3%A1s%20espec%C3%ADfico%20el,informaci%C3%B3n%20pertinente%20para%20la%20investigaci%C3%B3n.>
- [18] EI-BAHLUL F., KENNEY J. (2005). Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models.
- [19] NS-2 The Network Simulator ns-2, Oct. 30, 2004.
- [20] SEGURA D., GONZALEZ F., LÓPEZ D., (2011). COMPORTAMIENTO DE LOS SERVICIOS DIFERENCIADOS (DIFFSERV) Y LOS SERVICIOS INTEGRADOS (INTSERV) EN REDES IP PEQUEÑAS”
- [21] VALLEJO J., Rico J (2011), CALIDAD DE SERVICIO EN REDES IPv4 Y SU SIMULACIÓN EN NS-2.
- [22] Tráfico constante de bits, disponible en: http://en.wikipedia.org/wiki/Traffic_contract#Constant_Bit_Rate_.28CBR.29.
- [23] Wikipedia, disponible en: http://es.wikipedia.org/wiki/Principio_de_Pareto.
- [24] D. Rincón; Introducción a los modelos de tráfico para redes de banda ancha. Departamento de matemática aplicada y telemática (UPC), Barcelona, 2008.



[25] R. Salazar, J. Carlos, A. Urrea; Sistema operativo linux y control de tráfico en redes de computadores. Universidad de Antioquia, Departamento de electrónica. Medellin, 2004.



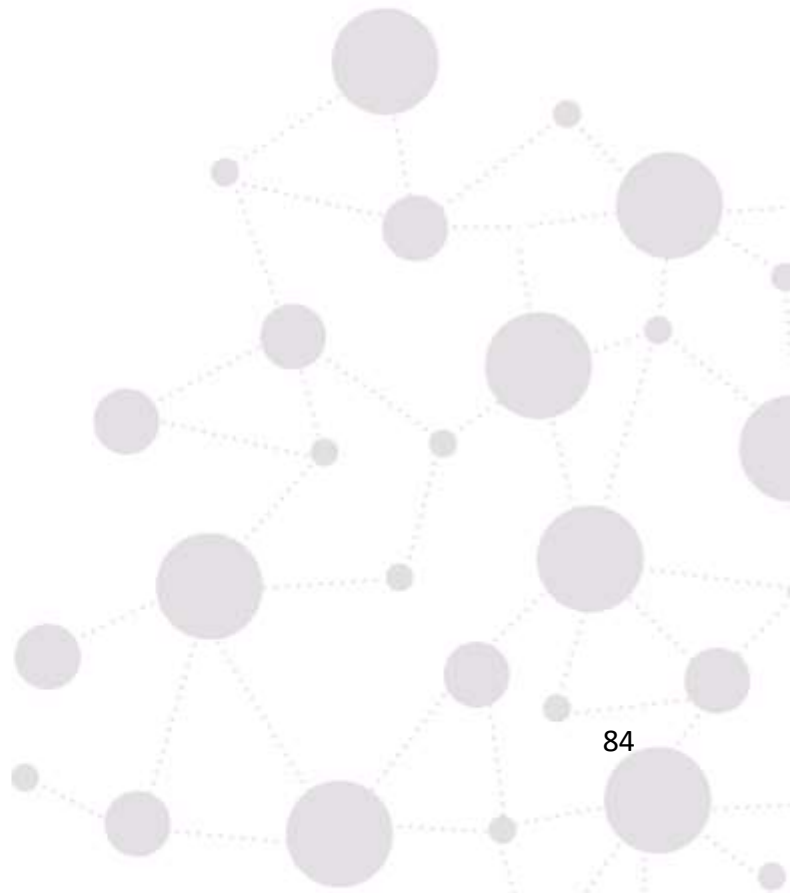
11. Anexos

Anexo 1: Configuración de R1, Aplicando Políticas de Priorización De Tráfico

```
Router#SH Running-config
Building configuration...

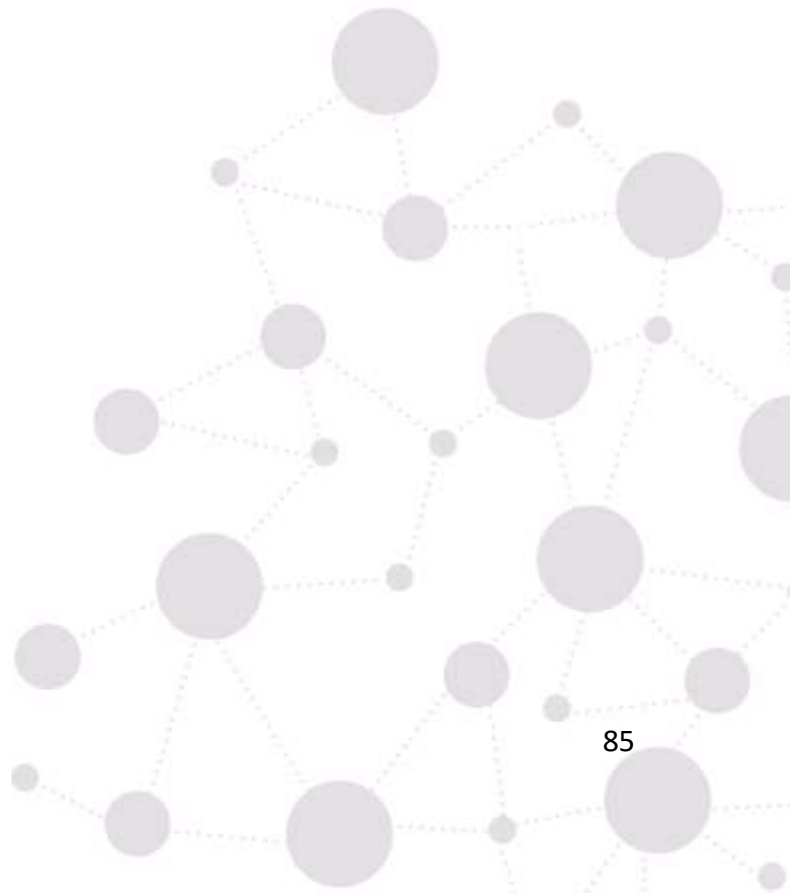
Current configuration : 1078 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
ip cef
no ipv6 cef
!
!

spanning-tree mode pvst
!
class-map match-all voice
match protocol rtp
class-map match-all http
match protocol http
class-map match-all icmp
match protocol icmp
!
policy-map marcado
class voice
priority 100
set ip dscp ef
class http
bandwidth 50
set ip dscp af31
class icmp
bandwidth 25
set ip dscp af11
!
```





```
!  
interface GigabitEthernet0/0/0  
ip address 10.10.10.1 255.255.255.252  
service-policy output marcado  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/0/1  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/0/2  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
version 2  
network 10.0.0.0  
network 192.168.1.0  
no auto-summary  
!  
ip classless  
!  
ip flow-export version 9  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
!  
!  
!  
end
```





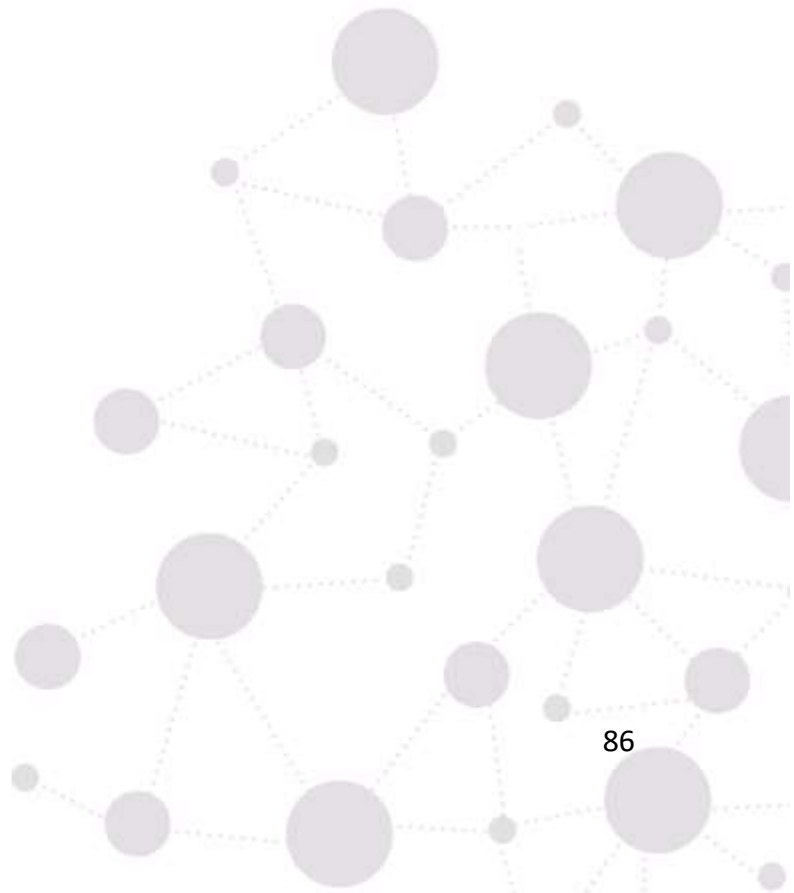
Anexo 2. Configuración de R2, Aplicando Políticas de Priorización de Tráfico

```
Router#sh running-config
Building configuration...
```

```
Current configuration : 1034 bytes
```

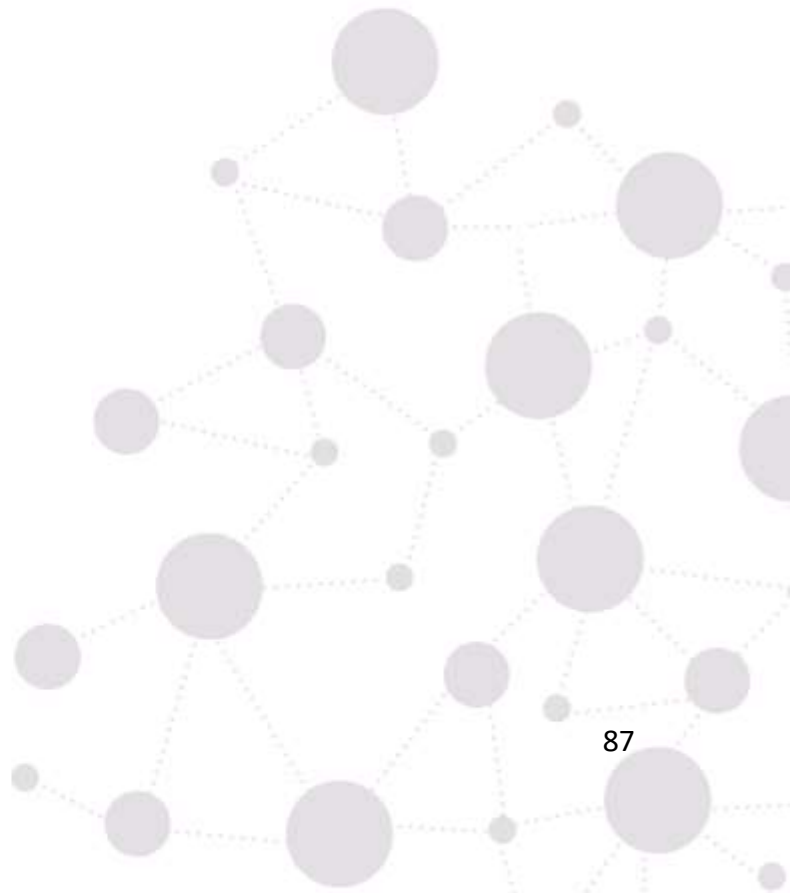
```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
!
class-map match-all voice
match ip dscp ef
class-map match-all http
match ip dscp af31
class-map match-all icmp
match ip dscp af11
!
policy-map remarcado
class voice
set precedence 5
class http
set precedence 3
class icmp
set precedence 0
!
!
```

```
interface GigabitEthernet0/0/0
```





```
ip address 10.10.10.2 255.255.255.252
service-policy input remarcado
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.2.0
no auto-summary
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```





Anexo 3. Certificación de traducción del resumen

Loja, 22 de mayo de 2023

CERTIFICADO DE TRADUCCIÓN

Licenciado.

Luis Eduardo Malla Medina

LICENCIADO EN CIENCIAS DE LA EDUCACION MENCION IDIOMA INGLES

CERTIFICO:

Haber realizado la traducción de español a inglés del resumen de la tesis titulada "Comparación de las soluciones Diffserv (Servicios Diferenciados) e Intserv (Servicios Integrados) para proveer Calidad De Servicio QoS en Redes LAN Inalámbricas." de autoría de EDUARDO SAMUEL MONTALVÁN CELI con cédula de identidad 1104201676, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. Marco Augusto Suing Ochoa Mg. Sc. previo a la obtención del título de Magister en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado en hacer uso del presente en lo que creyera conveniente.



firmado electrónicamente por:
LUIS EDUARDO MALLA
MEDINA

Luis Eduardo Malla Medina

LICENCIADO EN CIENCIAS DE LA EDUCACION MENCION IDIOMA INGLES

Registro Senescyt: 1008-15-1421369