ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Faculta de Ingeniería en Electricidad y Computación

ANÁLISIS COMPARATIVO DE LAS TÉCNICAS TRADICIONALES DE CALIDAD DE SERVICIO APLICADO A UN ENLACE WAN PUNTO A PUNTO

TRABAJO DE TITULACIÓN PREVIA A LA OBTENCIÓN DEL TITULO DE MAGISTER EN TELECOMUNICACIONES

DIANA CAROLINA DECIMAVILLA ALARCÓN

Guayaquil, Ecuador
Año 2018

AGRADECIMIENTOS

Agradezco a Dios y la Virgen María por darme salud y sabiduría para poder continuar mis estudios e ir alcanzando las metas que me propongo en la vida.

A mi Familia quienes me han apoyado y acompañado constantemente en cada una de mis decisiones y me han dado la fortaleza para continuar y quienes cada vez que me veían perder el rumbo, me tomaban de la mano llevándome al camino correcto, expresando en reiteradas ocasiones que todo proyecto que uno se proponga se puede alcanzar.

Un especial agradecimiento a mi tutor el MSC. Albert Espinal S. y al grupo de trabajo la Academia CISCO por su paciencia y dedicación, además de compartir sus conocimientos invaluables y permitirme largas jornadas de trabajo mientras realizaba las pruebas pertinentes para el presente trabajo.

DEDICATORIA

El presente proyecto lo dedico a mi familia y a Dios, motores principales de mi vida quienes me han enseñado a diario que con amor y perseverancia todo se puede lograr. Y quienes jamás desertaron y me dieron su apoyo incondicional para que pudiese culminar este proyecto.

A mis profesores de la Cuarta Promoción de la MET quienes me brindaron sus conocimientos, y son pilares fundamentales para que éste trabajo de titulación pueda desarrollarse exitosamente.

TRIBUNAL DE EVALUACIÓN

.....

Ph.D. César Martín Moreno

PRESIDENTE SUBDECANO DE LA FIEC

.....

Msc. Albert Espinal S.

DIRECTOR TRABAJO DE TITULACIÓN

.....

Msc. Miguel Molina.

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".

.....

Diana Carolina Decimavilla Alarcón

RESUMEN

La presente tesis pretende realizar un análisis comparativo que servirá de punto de apoyo para los administradores de redes que buscan ofrecer una adecuada política de Calidad de Servicio (Quality of Service - QoS) al tráfico de las aplicaciones, la cual debido a la integración del mismo generado en una red de comunicaciones de datos, voz y video, afecta al rendimiento y tiempos de respuesta de la red. El avance de la tecnología, ha logrado incrementar la cantidad de usuarios, así como de nuevas aplicaciones en teléfonos móviles y sistemas conectados que permiten disponer de una gran cantidad de información digital de tipo educativa, comercial, empresarial, entre otras, demandando altas tasas de tráfico que exige requerimientos de tiempos de respuestas más eficientes. Debido a este escenario es importante un estudio comparativo entre las técnicas de QoS, tales como WFQ, LLQ y PQ en un escenario específico de conectividad para analizar su comportamiento y obtener la optimización de ese escenario garantizando los parámetros de eficiencia de una red de comunicaciones, como ancho de banda, latencia de extremo a extremo, fluctuación de latencia y porcentajes de paquetes perdidos y condiciones de un enlace WAN punto a punto.

En las comunicaciones convergentes, los administradores deberían tomar en cuenta y priorizar la exigencia de los valores mínimos de latencia para evitar comportamientos no deseados en las comunicaciones; por ejemplo, llamadas de Voz sobre IP, las cuales deben tener un máximo de perdida de paquetes del 1% y latencia de 150 milisegundos [1], si no se cumplen estas condiciones obtendríamos como resultado: problemas de compresión y/o voz entrecortada, debido a la perdida de paquetes.

Para el desarrollo de la presente investigación, es necesario comprender como operan las redes punto a punto a través de un enlace WAN.

El capítulo 1 contiene la descripción, importancia y justificación de la problemática a analizar, adicionalmente, se muestran los objetivos que se pretende cumplir con el avance del presente trabajo.

El capítulo 2 contiene los conceptos necesarios a los conceptos de calidad de servicio, parámetros que influyen en la decisión de una buena o mala calidad de un servicio en específico.

El capítulo 3 contiene información sobre el escenario a analizar, algoritmos de configuración y herramientas de medición de parámetros.

El capítulo 4 contiene el análisis del escenario y comparación de resultados obtenidos.

El capítulo 5 contiene los ajustes a realizar a los diferentes tipos de tráfico bajo el mismo escenario.

ÍNDICE GENERAL

AGRADECIMIENTOS ii

DEDICATORIA iii

TRIBUNAL DE EVALUACIÓN iv

DECLARACIÓN EXPRESA v

RESUMEN vi

ÍNDICE GENERAL viii

CAPÍTULO 1 1

1. MARCO REFERENCIAL 1

1.1 Definición del Proyecto 1

1.2 Importancia y justificación 3

1.3 Objetivos del Proyecto 4

1.3.1 Objetivo general 4

1.3.2 Objetivos específicos 4

1.4 Alcances y limitaciones 4

CAPÍTULO 2 6

2 MARCO CONCEPTUAL 6

2.1. Calidad de Servicio, QoS 6

2.2. Métodos básicos de QoS 7

2.2.1. Clases de Servicios 8

2.2.2. Tipos de Servicios 9

2.3. Parámetros de Calidad de Servicio 10

2.3.1. Caudal o Throughput 10

2.3.2. Retardo o Delay 10

2.3.3. Variación del retardo o Jitter 11

2.3.4. Pérdida de paquetes o Packet Loss 12

2.4. Modelos de Servicio 13

2.4.1. FIFO 13

2.4.2. PQ 14

2.4.3. LLQ 15

2.4.4. WFQ 15

CAPÍTULO 3 17

3. ESCENARIO PROPUESTO Y SOLUCIÓN PLANTEADA 17

3.1. Descripción del escenario 17

3.1.1. Comparación de hardware 18

3.1.2. Selección de hardware 24

3.2. Algoritmo de configuración de escenario 25

3.3. Algoritmo de medición de parámetros de QoS 31

3.4. Análisis de herramientas de medición de parámetros de eficiencia 35

3.4.1. PingPlotter 35

3.4.2. Microsoft Network Monitor 37
3.4.3. MRTG 38
3.4.4. Smokeping 40
3.5. Comparación y selección de herramientas de medición de datos 42
CAPÍTULO 4 44
4. PRUEBAS Y ANÁLISIS DE RESULTADOS 44
4.1. Configuración del Sistema 44
4.2. Experimentación y Análisis de Escenario 47
4.2.1. Análisis experimental de datos 47
4.2.2. Modelamiento y Validación de datos 55
4.3. Análisis comparativo de resultados 57
CAPÍTULO 5 60
5. AJUSTES DE QoS EN EL MODELO PROPUESTO 60
5.1. Ajuste de QoS a un Tráfico ICMP sobre IPv4 60
5.2. Ajuste de QoS a un Tráfico ICMP sobre IPv6 61
5.3. Ajuste de QoS para Tráfico de VoIP 62
5.4. Ajuste de QoS para Tráfico WEB 64
CONCLUSIONES Y RECOMENDACIONES 66
BIBLIOGRAFÍA 69

CAPÍTULO 1

1. MARCO REFERENCIAL

En el Capítulo No. 1, se detallan los problemas que dieron origen a la realización del presente estudio; adicionalmente, se muestran temas que deben considerarse para una completa comprensión del tema a desarrollar, como son:

- Definición del Proyecto.
- Importancia y justificación.
- Objetivos del Proyecto
- Alcances y limitaciones.

1.1 Definición del Proyecto

El término Calidad de Servicio se puede definir desde varias perspectivas, de acuerdo a las necesidades de los diferentes tipos de usuarios, básicamente los administradores de redes aplican diversas técnicas para lograr la política de Calidad de Servicio (Quality of Service - QoS) que sea más adecuada considerando a la integración del tráfico generado en una red de comunicaciones de datos, voz y video. Por estas razones es de relevancia un estudio comparativo entre las técnicas de QoS.

Para garantizar los parámetros de eficiencia de una red de comunicaciones, como ancho de banda, latencia de extremo a extremo, fluctuación de latencia y porcentajes de paquetes perdidos, los administradores de red deberían hacer un análisis considerando las características que definen a la Calidad de Servicio de las aplicaciones y/o servicios y que son dirimentes en las experiencias de los usuarios. Por tal motivo surge la necesidad de comparar las técnicas de Calidad de Servicio tales como WFQ, LLQ y PQ

en un escenario específico de conectividad para analizar su comportamiento y obtener la optimización de ese escenario bajo los parámetros antes descritos y condiciones de un enlace WAN punto a punto.

Un factor de gran importancia en comunicaciones convergentes es priorizar la exigencia de los valores mínimos de latencia para evitar comportamientos no deseados en las comunicaciones; por ejemplo, llamadas de Voz sobre IP, las cuales deben tener un máximo de perdida de paquetes del 1% y latencia de 150 milisegundos [1], si no se cumplen estas condiciones obtendríamos como resultado: problemas de compresión y/o voz entrecortada, debido a la perdida de paquetes.

La actual problemática presenta en los ruteadores una cola de hardware asociada a cada interface física disponible para despachar paquetes de la red de acuerdo a sus prioridades o requerimientos [2]. Existen varias técnicas que se encargan de marcar y clasificar estos paquetes en colas, como por ejemplo: WFQ (Weighted Fair Queuing), LLQ (Low Latency Queuing) o PQ (Priority Queuing), los cuales han sido diseñados e implementados para la optimización en términos de latencia para los enlaces de red [2].

En muchas ocasiones, la solución a este tipo de problemas ha sido aumentar el ancho de banda de los enlaces, pero esto conlleva a obtener costos adicionales y a cambios en los medios de transmisión. Para el análisis de este proyecto de titulación, debemos aclarar que el ancho de banda de la red no sufrirá de cambio alguno durante el proceso investigativo. Para sobrellevar los problemas que ya hemos expuesto anteriormente urge la necesidad de medir y analizar el factor de latencia en el tránsito de paquetes, que pueden surgir debido a [2] [3]:

1. Latencia de procesamiento: define lo que hace el dispositivo intermedio, analizar y procesar la información de los paquetes para la toma de decisiones al reenviarlos.

2. Latencia de encolamiento: una vez tomada la decisión de envío (forwarding), el paquete es enviado a la interfaz física de salida, que generalmente es de tipo FIFO (primero que llega primero que se despacha).

3. Latencia de propagación: este se debe a la transmisión y propagación de los paquetes enviados como señales, que dependen del ancho de banda disponible y del tipo de medio de comunicación físico que se utilice, como fibra óptica, cobre o radioenlace.

De estas variables en términos de latencia, lo que deseamos para este proyecto de titulación es medir es el segundo factor, la latencia debido a los procesos de encolamiento, que permitan afinar la técnica y optimizar el tiempo que los paquetes pueden pasar en una cola de despacho.

1.2 Importancia y justificación

Debido a que en el Ecuador, en el área de redes de dispositivos se manejan diferentes tipos de tráfico, sintetizados en la convergencia de datos, voz y video, sumado al desarrollo de nuevos servicios, los cuales requieren tratamientos diferentes para que el tránsito de estos paquetes no se vea afectado por la latencia, es necesario analizar y medir el comportamiento de las técnicas de calidad de servicio para luego mejorar la técnica que mejor se adapte al escenario propuesto para este trabajo de investigación.

Esta propuesta de estudio y análisis está dirigido a las empresas que tienen matrices y sucursales y usan redes con enlaces WAN punto a punto; pretende hacer mediciones de latencia para mejorar el desempeño del enlace, mediante la prueba de las técnicas de calidad de servicio tradicionales dentro de un mismo escenario, con un tránsito donde se incluya datos, voz y video, sin necesidad de incrementar el ancho de banda. Se propone medir la latencia de encolamiento de tres (3) técnicas tradicionales de calidad de servicio, como lo son PQ, LLQ y WFQ bajo el mismo escenario, con la finalidad de obtener mediciones de la latencia, que permitan mejorar el desempeño del tránsito de los paquetes a través de los dispositivos intermedios de la red y por ultimo afinar la técnica de calidad de servicio existente para mejorar el desempeño del enlace, de esta manera se proporcionará información técnica a los administradores de red de empresas con enlaces punto a punto que consideren de suma importancia el impacto de latencia en una comunicación.

En la actualidad, no se cuenta con un estudio actualizado de comparación de las técnicas de calidad de servicio en un enlace WAN punto a punto con la finalidad de medir la latencia de encolamiento de un ruteador, pero si bajo otros tipos de escenarios como NGN [4] y UMTS [5].

1.3 Objetivos del Proyecto

1.3.1 Objetivo general

Medir y analizar la latencia de un enlace WAN punto a punto, mediante la comparación de diferentes técnicas de Calidad de Servicio, originado por la generación de diferentes patrones de tráfico sobre un mismo escenario de conectividad, con la finalidad de establecer las técnicas de QoS adecuada para determinadas aplicaciones y de esta forma optimizar los tiempos de retardo.

1.3.2 Objetivos específicos

- Establecer una medición del comportamiento del tráfico generado por una red punto a punto con diferentes patrones de tráfico.
- Proponer 3 tipos de técnicas de calidad de servicio existentes para la medición de latencia de la red punto a punto.
- Comparar las técnicas de QoS propuestas WFQ, LLQ y PQ para mejorar el desempeño de la red.
- Afinar las técnicas de QoS propuestas para optimizar su operación en un enlace punto a punto de acuerdo a las aplicaciones o tráficos más comunes.

1.4 Alcances y limitaciones

El alcance de esta propuesta técnica de investigación de datos, tiene como objetivo principal la aplicación de una técnica llamada benchmarking, la cual pretende desarrollar un mecanismo clave para la mejora continua de los procesos. En este caso en particular, de las técnicas tradicionales de Calidad de Servicio (QoS), mediante la recolección y comparación de datos que se obtienen de la aplicación de las técnicas de QoS, como son WFQ, LLQ y PQ con diferentes tipos de tráfico, dentro del mismo enlace WAN punto

a punto. Cabe indicar que el ancho de banda del enlace no será modificado para la toma de datos, siendo esta nuestra principal limitante al momento de la transmisión de tráfico generado por la red.

CAPÍTULO 2

2 MARCO CONCEPTUAL

2.1. Calidad de Servicio, QoS

Calidad de Servicio (QoS) es la manipulación de trafico de tal manera que un elemento de red (ejemplo: router o switch) redirige el tráfico de una forma consistente con los parámetros requeridos de la aplicación que genera el tráfico. En otras palabras, QoS permite a un dispositivo de red diferenciar el tráfico y aplicar diferentes criterios a dicho tráfico.

QoS fue desarrollado para resolver problemas de congestionamiento en la red. Históricamente, en las redes físicas existían 2 tipos de tráfico, voz y datos. Cada red estaba diseñada para llevar un tipo de tráfico en especial, para lo cual era necesario proveer de un cierto nivel de calidad de servicio. En la actualidad, las mismas aplicaciones usan redes convergentes o redes basadas en paquetes. En dichas redes, los recursos son compartidos, infraestructura común y recursos de red. Estas redes de paquetes son diseñadas con el fin de entregar tráfico utilizando metodología del mejor esfuerzo (Best Effort Service); en otras palabras no tienen QoS.

Aun cuando, las redes no tienen QoS, subscriptores de audio y video demandan estos servicios con niveles aceptables de calidad. Estas redes pasan cantidades masivas de trafico de un Punto A al B con contratos de servicios y requerimientos de desempeño de todas las aplicaciones que generan tráfico. Por este motivo es necesario desarrollar técnicas de QoS.

QoS es esencial para manejar el tráfico en las redes actuales. QoS incluye las siguientes funciones:

- Priorizar trafico sobre otros tipos de tráfico basados en protocolos, dirección IP y números de puerto.
- Filtrar tráfico de ingreso y egreso
- Controlar el ancho de banda permitido en el dispositivo para transmitir y recibir información.
- Leer y escribir requerimientos de QoS en el encabezado de paquetes.
- Controlar congestión de tal manera que el dispositivo envié tráfico de alta prioridad basado en prioridades de programación (scheduling)
- Controlar perdidas de paquetes usando algoritmos de detección aleatoria temprana (RED), de tal manera que los dispositivos conozcan los paquetes o procesos que pueden descartar

Dichas funciones de QoS pueden ser realizadas por routers o switches de la siguiente manera:

- El dispositivo recibe paquetes en su interface de entrada, examina los paquetes, y los clasifica en grupos clases de servicio (QoS)
- Si una política opcional es configurada, limita el tráfico o asigna del tráfico a una clase diferente.
- Las colas mantienen paquetes mientras esperan recursos de transmisión
- El programador toma los paquetes de las colas y los transmite usando el orden que el programador tiene configurado.
- Si existen configuraciones adicionales para el tráfico, se aplican al mismo.
- Se aplican nuevos encabezados para el valor de DS-Filed del encabezado IP para que el siguiente dispositivo pueda reconocerlo y clasificarlo.

2.2. Métodos básicos de QoS

Para el estudio de este apartado mencionaremos dos tipos básicos para dar QoS Con reserva y sin reserva.

Método de QoS con reserva.

En este método se realiza la reserva de recursos con la finalidad de que la red clasifique el flujo de paquetes de datos entrantes y manipule la identificación extendiendo un servicio diferenciado a cada uno de ellos.

Método de QoS sin reserva

En este método no se dan las reservas de recursos de manera explícita, el tráfico de datos se lo clasifica en un tipo de clase y la red provee del servicio a las distintas clases basándose en su prioridad Es muy necesario que la red diferencie el tipo de tráfico, controlando la cantidad de tráfico de una determinada clase permitida, para mantener la calidad de servicio que se le brinda a otros paquetes de la misma clase.

2.2.1. Clases de Servicios

La clase de servicio es un esquema de clasificación de datos con los que son agrupados los diferentes tipos de tráficos que tienen tratamientos similares con el objetivo de diferenciar los tipos de tráfico y por ende poder priorizarlos, la Clase de Servicio es el esquema de prioridad 802.1 p, como muestra la Figura 2.1

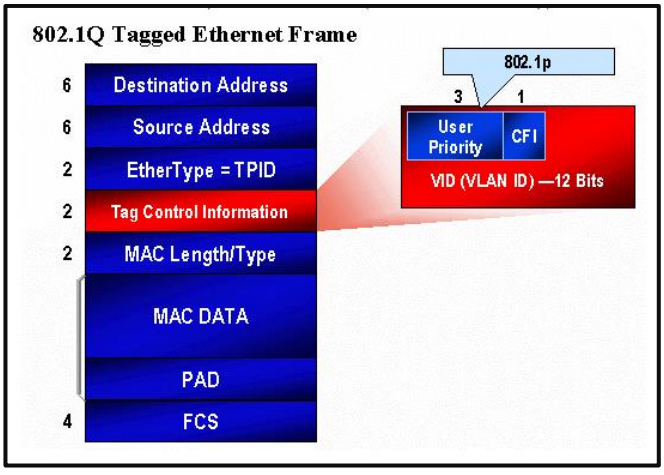

Figura 2.1 Prioridad del usuario (802.1p)

Fuente: www.cisco.com [6]

2.2.2. Tipos de Servicios

El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir un datagrama a través de una red en particular el campo ToS consta de ocho bits, de los cuales los tres primeros bits se utilizan para indicar la prioridad del paquete IP. Estos tres primeros bits son conocidos como bits de precedencia IP, para detallarlo mejor, se muestra en la Figura 2.2.

Estos bits pueden configurarse de cero a siete: cero representa la prioridad más baja y siete, la más alta como muestra la Figura 2.3.

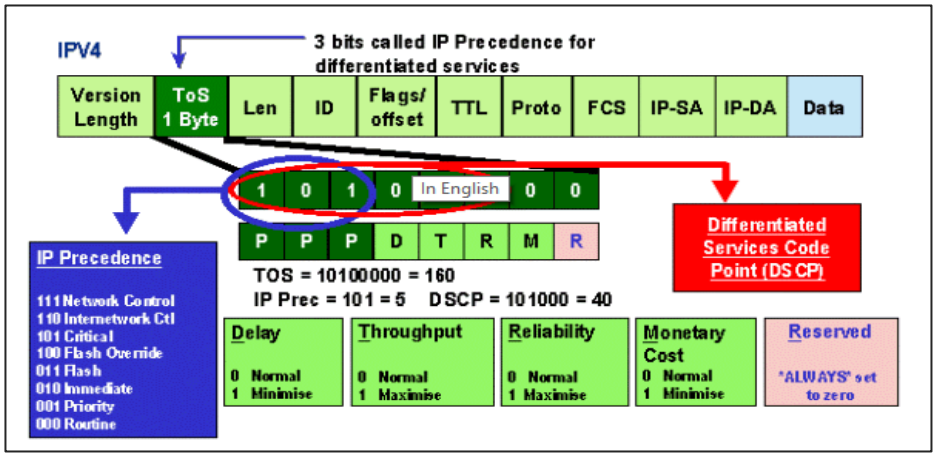

Figura 2.2 Gráfica detallada de ToS

Fuente: www.cisco.com [6]

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

Figura 2.3 Equivalentes de los bits de Procedenvia

Fuente: www.cisco.com [6]

2.3. Parámetros de Calidad de Servicio

La calidad de servicio desde todo ámbito es moderada desde los extremos de la red de comunicaciones siendo los consumidores y los proveedores los que podrían denominarse como puntos críticos debido a que son ellos los que captan el desempeño real de las aplicaciones y de los servicios brindados que se extienden a través de la red.

Esta medición se puede cuantificar por medio del uso de las siguientes técnicas usando parámetros como los que mostramos a continuación.

2.3.1. Caudal o Throughput

Este parámetro de medición de calidad de servicio nos muestra el volumen de información que fluye a través de un sistema de telecomunicaciones. El parámetro caudal se mide por la tasa de paquetes sin errores que fluyen a través de un circuito que hace parte de una aplicación específica, del conjunto de flujos que van de un punto a otro punto.

Como regla general se obtiene que entre mayor sea el valor del caudal obtenido en la medición se entiende que se prestan mayores y mejores parámetros de calidad de servicio, ya que el flujo de paquetes transmitidos sin errores es mayor.

2.3.2. Retardo o Delay

Este parámetro define la latencia que ocurre cuando el tráfico es enviado a través de la red. Existen varias fuentes de delay:

• **Delay de Serialización**: Se refiere al tiempo suficiente para que una interface codifique/ decofique bits de datos en un medio físico. Para calcular dicho delay se utiliza la siguiente fórmula matemática:

$$(1.1)\ \frac{\#\ bits}{bits\ per\ second\ (bps)}$$

Por ejemplo, el delay por Serialización para codificar 128000 bits en un link de 64 Kbps seria 2 segundos.

• **Delay de Propagación:** Se refiere al tiempo necesario para que un bit llegue desde su origen a su destino a través de un medio físico. La fórmula para cellular ester delay es:

$$(1,2)\ \frac{Longitud\ del\ cable\ en\ metros}{velocidad\ \ de\ la\ luz\ en\ el\ cable}$$

• **Delay de Procesamiento:** Se refiere al tiempo necesario para que un router o switch mueva un paquete desde el puerto de entrada al puerto de salida. Este delay es afectado por diferentes factores, como el método de conmutación o enrutamiento, la velocidad del CPU del dispositivo o el tamaño de la tabla de enrutamiento.

• **Delay de Encolamiento:** Se refiere al tiempo de espera de un paquete para que los paquetes previos puedan ser enviados por el medio. Colas que son muy pequeñas pueden congestionarse y por ende descartar paquetes que llegan al mismo (tail drop). Esto obliga a un protocolo de capa alta (e.g. TCP) a reenviar paquetes. Por otra parte, colas grandes generar delays de procesamiento ya que pueden existir muchos paquetes en la cola.

• **Delay de la red:** Se refiere al tiempo en que el paquete se encuentra en la red del proveedor. Este tipo de delay es muy difícil de cuantificar debido a que no es posible determinar la estructura de la red.

• **Delay de cambio:** Se refiere al delay iniciado por mecanismos de cambio (shaping) con la intención de reducir tráfico y prevenir que paquetes sean descartados por congestión.

2.3.3. Variación del retardo o Jitter

Jitter se determina como la alteración en el retardo de los paquetes que se reciben explicándoselo de esta manera, en el emisor los paquetes son enviados usando un flujo

continuo, insertando cada paquete separadamente de otro en intervalos de tiempos definidos, debido a la congestión de la red, a encolamientos incorrectos o errores de la configuración este flujo puede perder su uniformidad y el tiempo puede variar en vez de mantenerse constante lo que puede producir congestión de los paquetes de información. Así mismo describe la fragmentación que ocurre cuando el tráfico arriba en tiempos irregulares o en orden incorrecto. Se puede describir al Jitter como una variación de delay. Uno de los servicios más afectados por este problema es la comunicación por voz. Por este motivo, existen buffer que mitigan dicho efecto para Comunicaciones de voz.

2.3.4. Pérdida de paquetes o Packet Loss

Se defina a la pérdida de datos que ocurre por congestión en el enlace. Una cola llena descartara paquetes recién llegados.

Si uno de estos parámetros es extremadamente grande puede afectar de manera seria el desempeño de cualquier aplicación. Por ejemplo, VoIP, comienza a degradarse cuando el delay es mayor a 150 ms y la perdida de paquetes es mayor al 1%.

Aun cuando QoS, tiene aplicaciones específicas, existen diferentes metodologías que pueden ser implementados por QoS:

- **Best-Effort:** Esta metodología implica que no existen parámetros para QoS. El tráfico es enrutado en base a una metodología FIFO (fisrt come-first serve). Best Effort es la configuración por defecto que todo equipo de enrutamiento posee, por lo cual es muy fácil de implementar y escalar.
- **Integrated Services (IntServ):** IntServ QoS puede ser usado por una aplicación que requiere un nivel específico de servicio. Un control de admisión responde a este requerimiento al colocar o reservar recursos en los extremos para una aplicación. En caso de no existir recursos suficientes, el requerimiento es denegado. Todo dispositivo debe soportar protocolos IntServ QoS. Sin embargo, esta opción no es considerable para una solución escalable por 2 razones:

• El ancho de banda es finito y no se puede reservar más allá de la capacidad asignada.

• Protocolos IntServ QoS agregan un encabezado grande, debido a que el tráfico debe mantenerse estable. Un ejemplo de este tipo de protocolo es Resource Reservation Protocol (RSVP).

• Differentiated Services (DiffServ)

Este tipo de QoS fue diseñado como una solución escalable de QoS. Diferentes tipos de grafico son organizados en clases específicas, y marcados para identificar su clasificación. Las políticas son creadas en términos de los saltos necesarios para proveer un nivel de QoS requerido, dependiendo de la clasificación del tráfico.

DiffServ QoS es popular por su escalabilidad y flexibilidad en ambientes empresariales. Sin embargo, DiffServ QoS es considerado una especie de soft QoS, por el hecho de no garantiza una calidad de servicio absoluta como IntServ QoS. DiffServ QoS no emplea señalización y no obliga a reservar recursos de punto a punto.

2.4. Modelos de Servicio

2.4.1. FIFO

El presente método de encolamiento es el más sencillo de todos, en el encolamiento FIFO todos los paquetes de datos son tratados igualmente y son colocados dentro de una misma y única cola, estos son entregados en el mismo orden en el que son colocados previamente dentro de la cola, esto quiere decir que el primer paquete en entrar es el primero en salir, este método de encolamiento presenta una gran desventaja y es que maneja una cantidad de flujo de paquetes limitada, esto quiere decir que cuando la cola está llena los paquetes se descartan, en esta configuración los paquetes no son reordenados y el retardo máximo viene dado por el tamaño de la cola, ver Figura 2.4

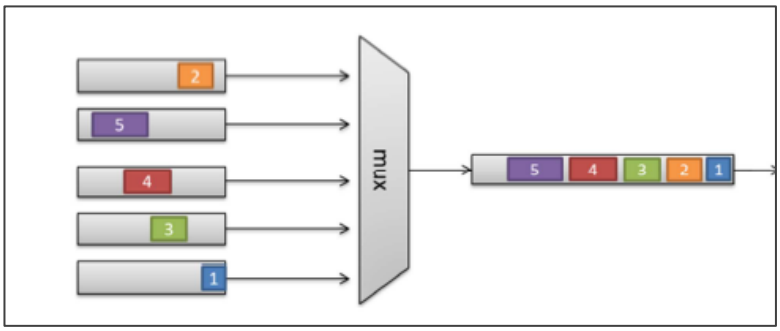

Figura 2.4 Método de Encolamiento - FIFO

Fuente: http://biblioteca.utb.edu.co/ [7]

2.4.2. PQ

Este método de encolamiento llamado encolamiento de prioridad (PQ) se fundamenta en un conjunto determinado de colas que son clasificadas según su prioridad, cada flujo de datos es enviado a cada una de estas colas, las mismas que son entregadas siguiendo estrictamente la prioridad que estas lleven asignadas.

Las colas de mayor prioridad son atendidas primero, luego se atiende las de menor prioridad. Si una cola de prioridad baja está siendo atendida, e ingresa un paquete de mayor prioridad, esta es atendida inmediatamente dejando en standbye la anterior. Este método de encolamiento se puede usar cuando se necesite dar prioridad a un tráfico importante, con la contrariedad de que puede generar muy bajo desempeño en la entrega de paquetes que no sean considerados prioritarios, ver Figura 5.

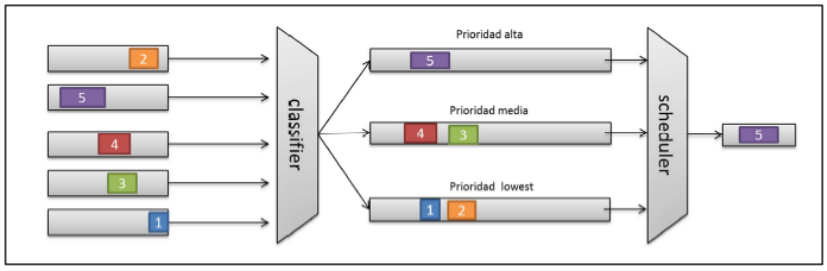

Figura 2.5 Encolamiento PQ [7]

Fuente: http://biblioteca.utb.edu.co [7]

2.4.3. LLQ

El encolamiento de baja latencia LLQ es un método de encolamiento mezcla entre el tipo de encolamiento de prioridad PQ y el Class based weigthed fair queueing CB-WFQ.

Es un encolamiento típico de las aplicaciones de telefonía IP i VoIP. El LLQ, está basado en el uso de colas de prioridad personalizadas las mismas que están pre configuradas por el operador de los servicios de red, estas clases de tráfico en conjunto con una cola de prioridad, la cual tiene mayor preferencia sobre las demás colas correspondientes a los diferentes flujos de datos ya existentes, esto quiere decir que si hay presencia de tráfico de datos en una cola de prioridad esta es atendida antes que las colas de prioridad personalizadas, se debe tomar en cuenta que si la cola de prioridad absoluta no está generando cola de paquetes las demás colas son atendidas según su prioridad asignada, como muestra la Figura 2.6.

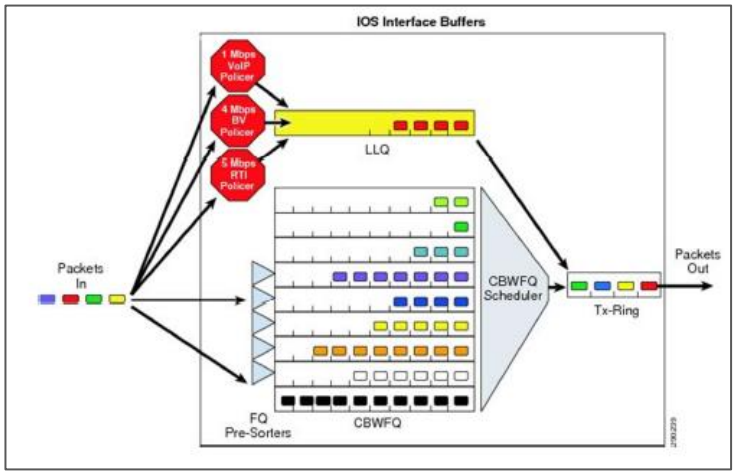

Figura 2.6 Encolamiento LLQ

Fuente: http://biblioteca.utb.edu.co [7]

2.4.4. WFQ

Método de encolamiento conocido como Weighted Fair Queueing (WFQ) esta modalidad provee una asignación de ancho de banda para todo el tráfico de red, dicha asignación

de ancho de banda en la que determina el orden en que serán entregados los paquetes y se realiza usando filtros en el datagrama IP como las direcciones de salida y llegada o el campo TOS.

El WFQ genera un tipo de cola distinta para cada modelo de trafico asignándole individualmente valores de profundidad para las colas, las mismas que pasan a través de un servidor round robín, lo que quiere decir que se siguen un orden secuencial circular, y tomando en cuenta que cada flujo tiene una cola asignada si se presentaren demasiadas tramas de datos solo se verá afectado el rendimiento de la cola para cada clase especifica como muestra la Figura 2.7.

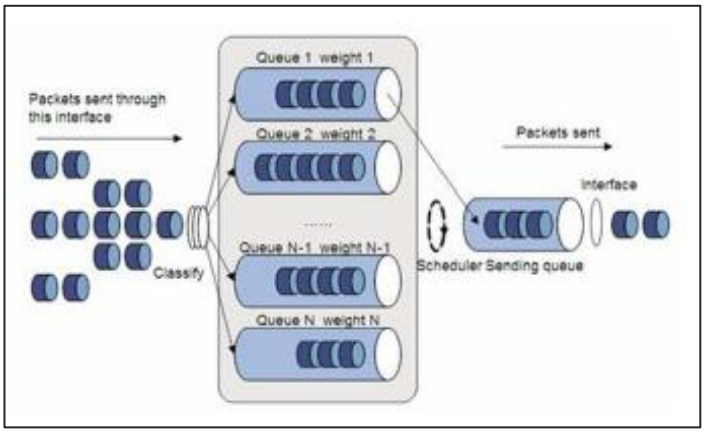

Figura 2.7 Encolamiento WFQ

Fuente: http://biblioteca.utb.edu.co [7]

CAPÍTULO 3

3. ESCENARIO PROPUESTO Y SOLUCIÓN PLANTEADA

3.1. Descripción del escenario

Para el presente proyecto de investigación la topología de red a utilizar se basa en un grupo de computadoras conectadas entre sí y que puede ser diseñada tanto física como lógicamente, para lo cual se muestra en la Figura 3.1 la topología en IPv4 a utilizar y en la Figura 3.2 la topología en IPv6.

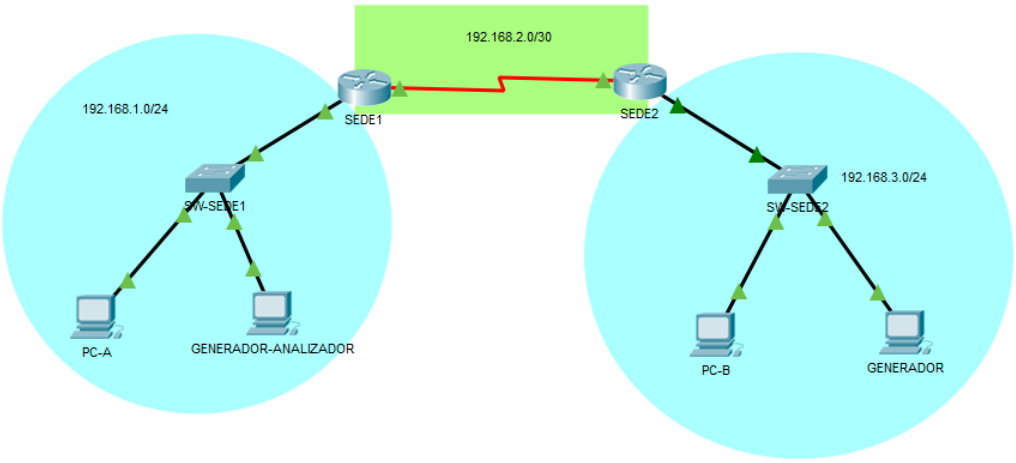

Figura 3.1 Red Punto a Punto en IPv4

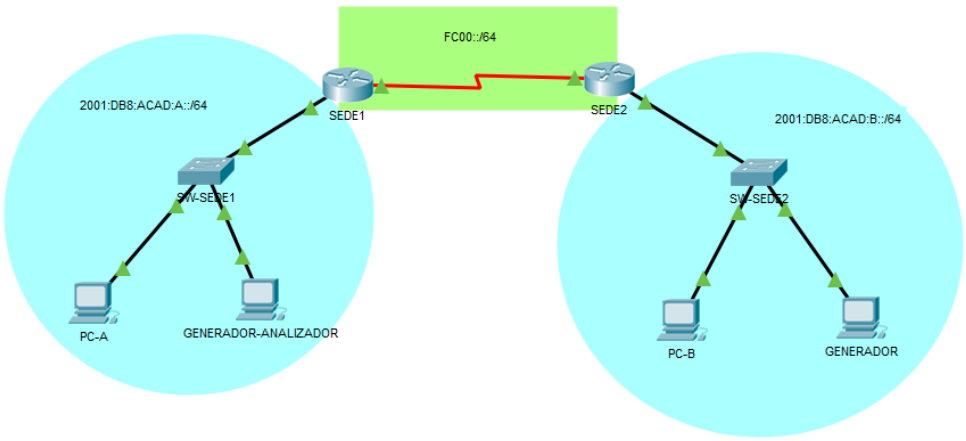

Figura 3.2 Red Punto a Punto en IPv6

3.1.1. Comparación de hardware

Para decidir el hardware a utilizar para la implementación de la red punto a punto se consideró las características de los routers más comunes utilizados a nivel de empresas tipo Pyme, para lo cual se detallan las características de routers en las Tabla 1, 2 y 3 y de Switch en la Tabla 4 y 5.

Característica	Cisco 2851	Cisco 2821	Cisco 2811	Cisco 2801
Form Factor	2 RU	2 RU	1 RU	1 RU
Integrated Routed/WAN Ethernet	2 10/100/1000	2 10/100/1000	2 1/10	2 1/10
10/100 Ethernet Switch Ports	Up to 64	Up to 40	Up to 32	Up to 16
Broadband WAN Support	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC
Analog Modem Ports	WIC or Network Module (optional)	WIC or Network Module (optional)	WIC or Network Module (optional)	WIC (optional)

Interface Card Slots	4 HWIC/WIC/VIC/VWIC	4 HWIC/WIC/VIC/VWIC	4 HWIC/WIC/VIC/VWIC	2 HWIC/WIC/ VIC/VWIC, 1 WIC/VIC/VW IC, 1 VIC/VWIC
Network Module Slots	1	1	1	--
AIM Slots	2	2	2	2
USB Ports	2 (v1.1)	2 (v1.1)	2 (v1.1)	1 (v1.1)
Embedded Crypto Processor	Yes	Yes	Yes	Yes
Default/Max Flash	64/256 MB	64/256 MB	64/256 MB	64/256 MB
Default/Max SDRAM	256/1024 MB	256/1024 MB	256/768 MB	128/384 MB
Gigabit Ethernet, SFP Port	Optional (HWIC)	Optional (HWIC)	Optional (HWIC)	--
Cisco Router and Security Device Manager(SDM)	Yes	Yes	Yes	Yes

Tabla 1 Tabla comparativa de Routers Seres 2800 – Generales

Fuente: Router-switch.com. (2018). *Cisco 2800 Series Routers Models Comparison 2801 2811 2821 2851*. Accedido Sept 2018 [En línea]. Disponible en: http://www.router-switch.com/cisco-2800-series-routers-models-comparison-2801-2811-2821-2851-pd-45.html [20].

Características	Cisco 2851	Cisco 2821	Cisco 2811	Cisco 2801
Advanced Security				
VPN Technologies	DM-VPN, GET VPN, V3PN, with GRE, Easy VPN, and Cisco IOS SSL VPN	DM-VPN, GET VPN, V3PN, with GRE, Easy VPN, and Cisco IOS SSL VPN	DM-VPN, GET VPN, V3PN, with GRE, Easy VPN, and Cisco IOS SSL VPN	DM-VPN, GET VPN, V3PN, with GRE, Easy VPN, and Cisco IOS SSL VPN
Stateful Firewall	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image
URL Filtering	Yes	Yes	Yes	Yes
Voice Support				
DSP (PVDM) Slots on Motherboard	3	3	2	2

Survivable Remote Site Telephony (SRST)	Yes, up to 96 users	Yes, up to 48 users	Yes, up to 36 users	Yes, up to 24 users
Cisco Unified Communications Manager Express	Yes, up to 96 users	Yes, up to 48 users	Yes, up to 36 users	Yes, up to 24 users
Cisco Unity Express	Yes, up to 250 mailboxes	Yes, up to 250 mailboxes	Yes, up to 250 mailboxes	Yes, up to 50 mailboxes
Unified Messaging Gateway	Yes	Yes	Yes	--
Digital Voice	Yes, up to 192 calls	Yes, up to 128 calls	Yes, up to 80 calls	Yes, up to 30 calls
Analog Voice	Yes, up to 52 FXS, 36 FXO ports	Yes, up to 52 FXS, 36 FXO ports	Yes, up to 28 FXS, 24 FXO ports	Yes, up to 16 FXS, 16 FXO ports
Local Conferencing and Transcoding	Yes, use PVDMs	Yes, use PVDMs	Yes, use PVDMs	Yes, use PVDMs

Tabla 2 Tabla comparativa de Routers Seres 2800 – Seguridad y Soporte

Fuente: Router-switch.com. (2018). *Cisco 2800 Series Routers Models Comparison 2801 2811 2821 2851*. Accedido Sept 2018 [En línea]. Disponible en: http://www.router-switch.com/cisco-2800-series-routers-models-comparison-2801-2811-2821-2851-pd-45.html [20]

Característica	Cisco 2851	Cisco 2821	Cisco 2811	Cisco 2801
Wireless LAN				
Integrated 802.11 b/g Access Point	HWIC (optional)	HWIC (optional)	HWIC (optional)	HWIC (optional)
Integrated 802.11 a/b/g Access Point	HWIC (optional)	HWIC (optional)	HWIC (optional)	HWIC (optional)
RP-TNC Connectors for Field-replaceable Optional High-gain Antennas	Yes	Yes	Yes	Yes
Diversity (Dual) Antennas	Yes	Yes	Yes	Yes
Wireless LAN Controller Module	6, 8, 12 802.11a/b/g/n AP controller	6, 8, 12 802.11a/b/g/n AP controller	6, 8, 12 802.11a/b/g/n AP controller	--

Tabla 3 Tabla comparativa de Routers Series 2800 – Wireless LAN

Fuente: Fuente: Router-switch.com. (2018). *Cisco 2800 Series Routers Models Comparison 2801 2811 2821 2851*. Accedido Sept 2018 [En línea]. Disponible en: http://www.router-switch.com/cisco-2800-series-routers-models-comparison-2801-2811-2821-2851-pd-45.html [20]

	2960-S	2960 LAN Base	2960 LAN Lite	3750-X IP Base	3560-X IP Base	3K-X LAN Base
Uplinks	1 GE, 10 GE	GE	GE	1 GE, 10 GE (modular)	1 GE, 10 GE (modular)	1 GE, 10 GE (modular)
PoE	Partial PoE+	FE PoE	FE PoE	Full PoE+	Full PoE+	Full PoE+
Stacking	FlexStack 20G (modular)	No	No	StackWise+ 64G	No	StackWise+ (3750-X Only)
DRAM/Flash	128/64MB & USB	128/32MB	128/32 MB USB (2960-S)	256/238MB & USB	256/238MB & USB	256/238MB & USB
StackPower	No	No	No	Yes	No	No
Upgradable IOS	No	No	No	Yes	Yes	Yes
Modular Uplinks	No	No	No	Yes	Yes	Yes
Modular PS/Fan	No	No	No	Yes	Yes	Yes
MACSec	No	No	No	Yes	Yes	No
Enhanced LLW	Yes	No	Yes (2960-S)	Yes	Yes	Yes
RPS / XPS	RPS	RPS	No	XPS	XPS	XPS

Tabla 4 Comparación entre Swicth 2960 vs 3560 – Características generales

Fuente: Comparison of Cisco Switches: (2960 vs 3560), (. (2018). *Comparison of Cisco Switches: (2960 vs 3560), (Cisco 3560 X vs 3650 vs 3750-X vs 3850)*. Accedido Sept 2018 [En línea]. Blog.51sec.org. Disponible en: https://blog.51sec.org/2016/01/comparison-of-cisco-switches-2960-vs.html [21]

Hardware		
	Catalyst 2960	Catalyst 3560
Auto-MDIX	Yes	Yes
Digital Optical Monitoring	Yes	Yes
Generic Online Diagnostics (GOLD)	–	Yes
IEEE 802.3af (PoE) support	Yes	Yes
SDM Templates	Yes	Yes
Capa dos		
	Catalyst 2960	**Catalyst 3560**
Errdisable Autorecovery	Yes	Yes
Flex Links	Yes	Yes
IEEE 802.1ab (LLDP)	Yes	Yes
IEEE 802.1D STP	Yes	Yes
IEEE 802.1Q Tunneling	–	Yes
IEEE 802.1Q Trunking	Yes	Yes
IEEE 802.1s (MST)	Yes	Yes
IEEE 802.1W (RSTP)	Yes	Yes
IEEE 802.1x	Yes	Yes
IEEE 802.3ad (LACP)	Yes	Yes
Jumbo Frames	Yes	Yes
Layer 2 Protocol Tunneling (L2PT)	–	Yes
Per-port VLAN Policing	–	Yes
Port Security	Yes	Yes
Private VLANs	–	Yes
Storm Control	Yes	Yes
STP BackboneFast	Yes	Yes
STP Loop Guard	Yes	Yes
STP PortFast	Yes	Yes
STP Root Guard	Yes	Yes

STP UplinkFast	Yes	Yes
SPAN	Yes	Yes
RSPAN	Yes	Yes
UDLD	Yes	Yes
VLAN ACLs	–	Yes
VLAN-aware Port Security	Yes	Yes
VTPv2	Yes	Yes

Tabla 4 Comparación entre Swicth 2960 vs 3560 – Hardware y Capa dos

Fuente: Comparison of Cisco Switches: (2960 vs 3560), (. (2018). *Comparison of Cisco Switches: (2960 vs 3560), (Cisco 3560 X vs 3650 vs 3750-X vs 3850)*. Accedido Sept 2018 [En línea]. Blog.51sec.org. Disponible en: https://blog.51sec.org/2016/01/comparison-of-cisco-switches-2960-vs.html [21]

Capa Tres		
	Catalyst 2960	**Catalyst 3560**
Cisco Express Forwarding	–	Yes
DHCP Server	–	Yes
DHCP Snooping	Yes	Yes
DHCPv6	–	Yes
HSRP	–	Yes
IGMP Snooping	Yes	Yes
IP SLA Monitor	–	Yes
IP Source Guard	–	Yes
IPv4 Routing	–	Yes
IPv6 Routing	–	Yes
MLD Snooping	Yes	Yes
NSF Awareness	–	Yes
Policy Routing	–	Yes
Source-Specific Multicast (SSM)	–	Yes
VRF Lite	–	Yes
WCCPv1	–	Yes
WCCPv2	–	Yes

Administración		
	Catalyst 2960	Catalyst 3560
AutoQoS VOIP	Yes	Yes
Configuration Rollback	Yes	Yes
Configuration Diff	Yes	Yes
Embedded Event Manager	–	Yes
Enhanced Tracking Support	–	Yes
NTP	Yes	Yes
RADIUS Authentication	Yes	Yes
RMON	Yes	Yes
SCP	Yes	Yes
SSHv2	Yes	Yes
SNMPv2c	Yes	Yes
SNMPv3	Yes	Yes
Syslog over IPv6	Yes	Yes
TACACS+ Authentication	Yes	Yes

Tabla 4 Comparación entre Swicth 2960 vs 3560 – Capa Tres y Administración

Fuente: Comparison of Cisco Switches: (2960 vs 3560), (. (2018). *Comparison of Cisco Switches: (2960 vs 3560), (Cisco 3560 X vs 3650 vs 3750-X vs 3850)*. Accedido Sept 2018 [En línea]. Blog.51sec.org. Disponible en: https://blog.51sec.org/2016/01/comparison-of-cisco-switches-2960-vs.html [21]

3.1.2. Selección de hardware

- 2 Routers Cisco 2811 con puertos Ethernet 10/100, con memoria flash entre 64 - 256 MB, tarjeta serial WIC 2T y IOS 15.1 que simulan una red WAN de dos sedes separadas entre sí.
- 2 Switchs Cisco Catalyst 2960 con 64MB de Memoria RAM, U1, 48 PUERTOS Fast Ethernet, 32MB de Memoria Flash, utilizados para dividir el canal para video, voz y datos.

- Sede 1, incluye 2 ordenadores con 4GB de Memoria RAM, 2 Núcleo, 1.6 GHz hasta 2.48 GHz, Disco Duro interno de 500BG y Sistema Operativo Windows 10, las cuales se organizan de la siguiente manera:
    - Un ordenador se utiliza para la generación de tráfico general y análisis en la red, el cual tiene como objetivo inundar el enlace WAN provocando congestión y así poder examinar el comportamiento de las técnicas de encolamiento en estas situaciones.
    - El otro ordenador se utiliza para el envío de un tipo de tráfico en particular que será analizado durante su transmisión.
- Sede 2, incluye 2 ordenadores con 4GB de Memoria RAM, 2 Núcleo, 1.6 GHz hasta 2.48 GHz, Disco Duro interno de 500BG y Sistema Operativo Windows 10, las cuales se organizan de la siguiente manera:
    - El primer ordenador se utiliza para el generación de tráfico específico al ordenador de la Sede 1, así tendremos la seguridad de que existe paso de tráfico abundante en el enlace WAN.
    - El segundo ordenador se utiliza para la recepción del tipo de tráfico transmitido por el ordenador de la Sede 1.
- 6 Cables Directos
- 1 Cable Serial

3.2. Algoritmo de configuración de escenario

Router 1

```
Router>en

Router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname SEDE_1
SEDE_1(config)#no ip domain-lookup
SEDE_1(config)#int s0/0/0
SEDE_1(config-if)#ip address 192.168.2.1 255.255.255.252
SEDE_1(config-if)#clock rate 128000
SEDE_1(config-if)#no shutdown
```

```
SEDE_1(config)#int fastEthernet 0/0
SEDE_1(config-if)#ip address 192.168.1.1 255.255.255.0
SEDE_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up
SEDE_1(config-if)#exit
SEDE_1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
SEDE_1(config)#do wr
Building configuration...
[OK]
```

Router 2

```
Router>en
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname SEDE_2
SEDE_2(config)#no ip domain-lookup
SEDE_2(config)#int s0/0/0
SEDE_2(config-if)#ip address 192.168.2.2 255.255.255.252
SEDE_2(config-if)#no shutdown
SEDE_2(config)#int fastEthernet 0/0
SEDE_2(config-if)#ip address 192.168.3.1 255.255.255.0
SEDE_2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to
up
SEDE_2(config-if)#exit
SEDE_2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
SEDE_2(config)#do wr
Building configuration...
[OK]
```

PC_GENERADOR_ANALIZADOR

Para la PC_GENERADOR_ANALIZADOR, quien se encarga de generar y analizar el tráfico dentro del enlace WAN debe tener la configuración mostrada en la Figura 3.3.

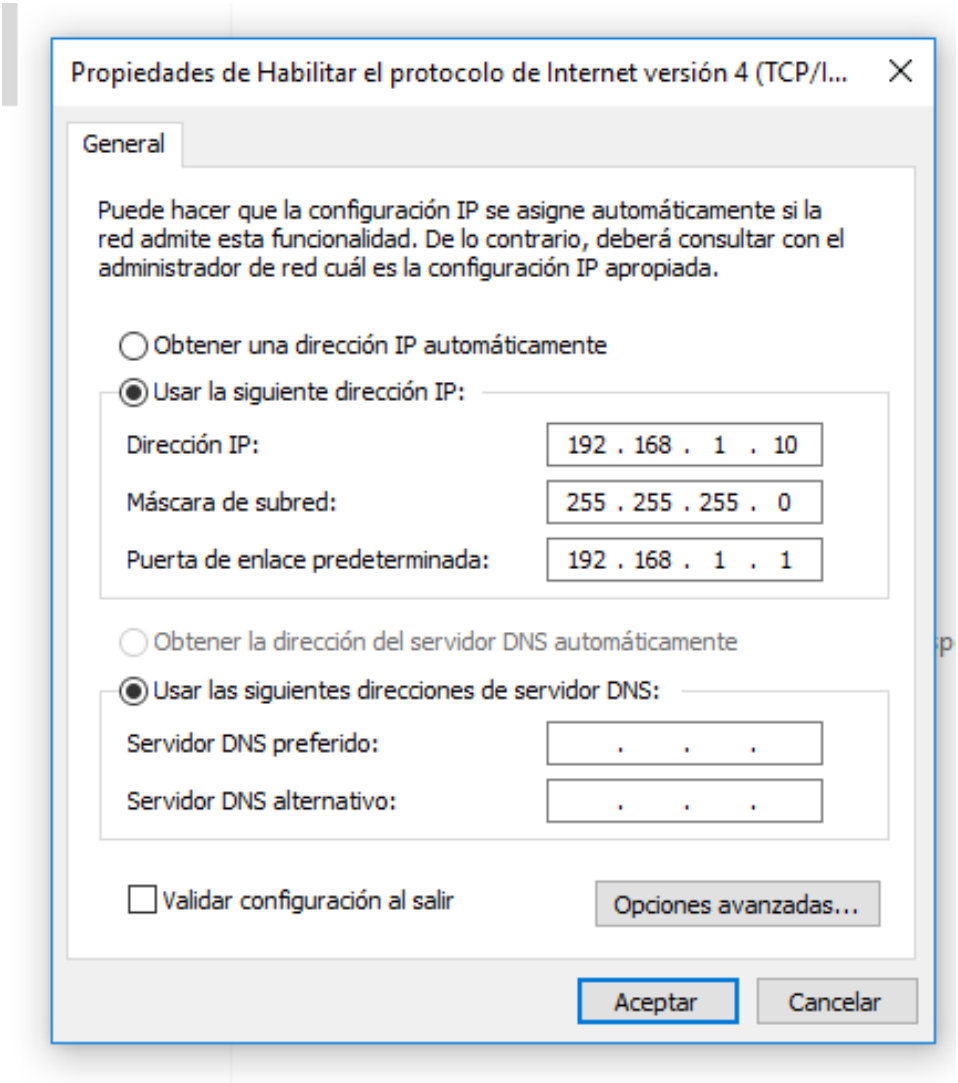

Figura 3.3 Configuración de IP del Ordenador PC_GENERADOR_ANALIZADOR

PC_A

Para la PC_A ubicada en la red de la SEDE_1 se deberá configurar la dirección ip que se muestra en la Figura 3.4, quien tiene como principal objetivo enviar un tipo de tráfico definido hacia la PC_B.

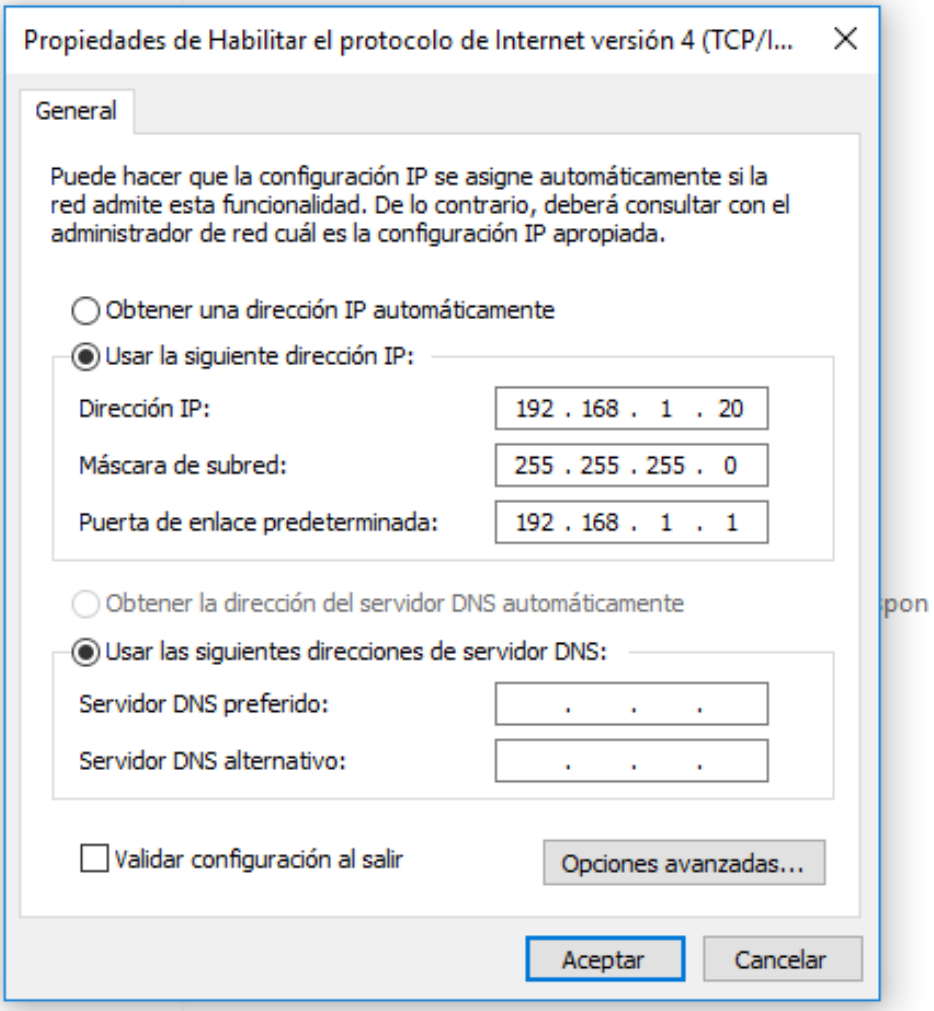

Figura 3.4 Configuración de IP del Ordenador PC_A

PC_GENERADOR

Para la PC_GENERADOR ubicada en la red de la SEDE_2 se deberá configurar la dirección ip que se muestra en la Figura 3.5, quien tiene como principal objetivo enviar un tipo de tráfico definido hacia la PC_B con el fin de inundar el enlace WAN.

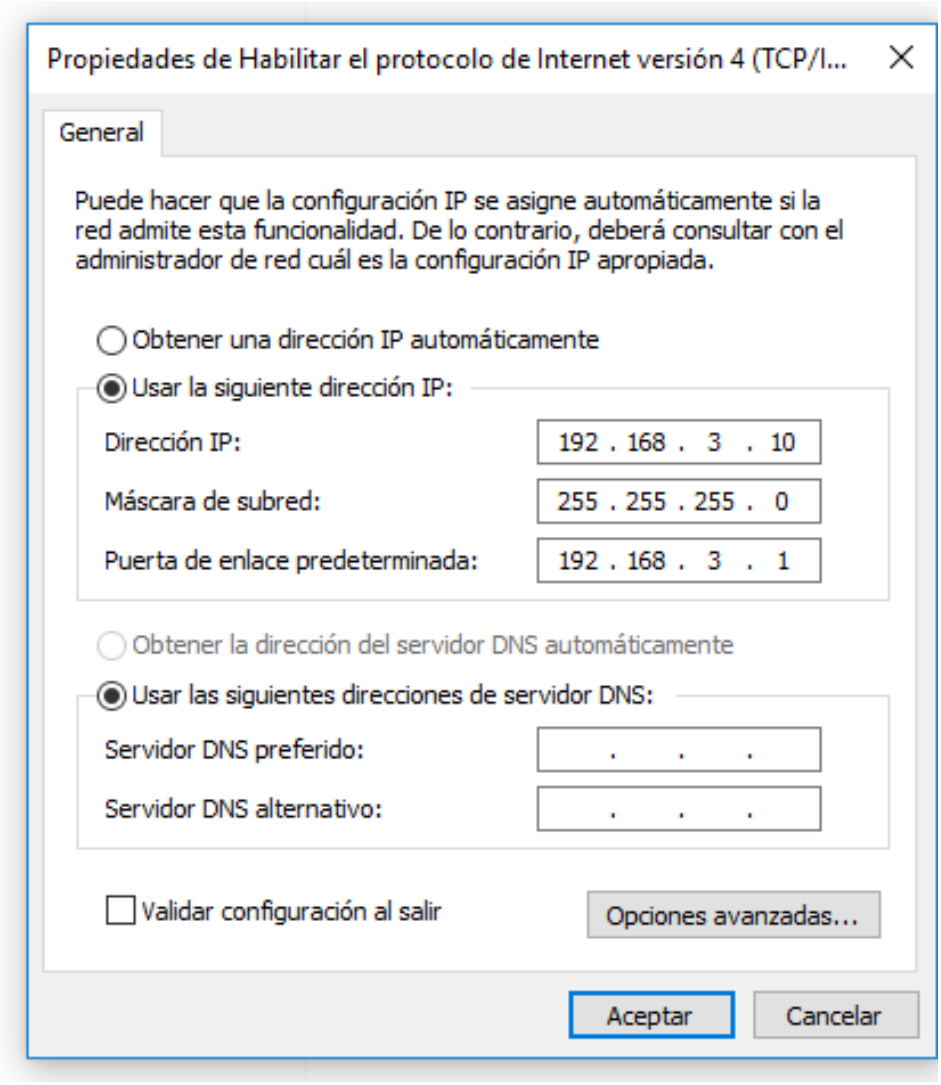

Figura 3.5 Configuración de IP del Ordenador PC_GENERADOR

PC_B

Para la PC_B ubicada en la red de la SEDE_2 se deberá configurar la dirección ip que se muestra en la Figura 3.6, quien será el ordenador al cual convergerá todo el tráfico de la red enviado tanto por PC_A como por la PC_GENERADOR_ANALIZADOR

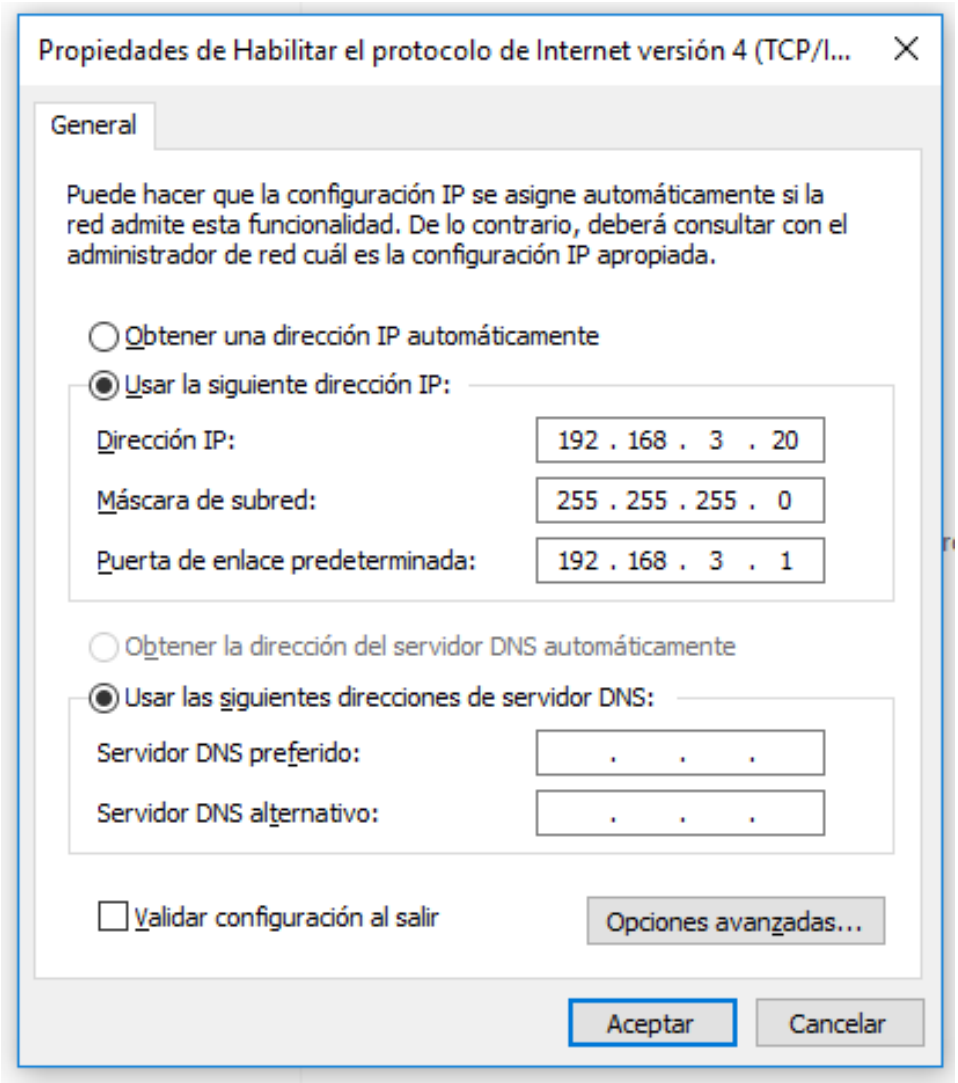

Figura 3.6 Configuración de IP del Ordenador PC_B

3.3. Algoritmo de medición de parámetros de QoS

Configuración de PQ

Tráfico IPv4

```
configure terminal
priority-list 1 protocol ip high
priority-list 1 default low
interface S0/0/0
priority-group 1
```

Tráfico IPv6

```
configure terminal
priority-list 1 protocol ipv6  high
priority-list 1 default low
interface S0/0/0
priority-group 1
```

Tráfico VoIP

```
configure terminal
priority-list 1 protocol ip high udp 69
priority-list 1 default low
interface S0/0/0
priority-group 1
```

Tráfico WEB

```
configure terminal
priority-list 1 protocol http high
priority-list 1 default low
interface S0/0/0
priority-group 1
```

Configuración de LLQ

Tráfico IPv4

```
configure terminal
!
class-map LLQ-IPv4
match protocol ip
exit
!
policy-map LLQ-IPv4
class LLQ-IPv4
priority percent 20
exit
interface serial 0/0/0
service-policy output LLQ-IPv4
```

Tráfico IPv6

```
configure terminal
!
class-map LLQ-IPv6
match protocol ipv6
exit
!
policy-map LLQ-IPv6
class LLQ-IPv6
priority percent 20
exit
interface serial 0/0/0
service-policy output LLQ-IPv6
```

Tráfico VoIP

```
configure terminal
!
```

```
class-map VoIP
match protocol udp
exit
!
policy-map VoIP
class VoIP
priority percent 20
exit
interface serial 0/0/0
service-policy output VoIP
```

Tráfico WEB

```
configure terminal
!
class-map HTTP
match protocol http
exit
!
policy-map LLQ
class HTTP
priority percent 50
exit
interface serial 0/0/0
service-policy output LLQ
```

Configuración de WFQ

Tráfico IPv4

```
!
configure terminal
!
class-map IPv4
match protocol ip
```

```
exit
!
policy-map WFQ
class IPv4
bandwith percent 10
exit
```

Tráfico IPv6

```
!
configure terminal
!
class-map IPv6
match protocol ipv6
exit
!
policy-map WFQ
class IPv6
bandwith percent 10
exit
```

Tráfico VoIP

```
!
configure terminal
!
class-map VoIP
match protocol udp
exit
!
policy-map WFQ
class VoIP
bandwith percent 10
exit
```

Tráfico WEB

```
!
configure terminal
!
class-map HTTP
match protocol http
exit
!
policy-map WFQ
class HTTP
bandwith percent 10
exit
```

3.4. Análisis de herramientas de medición de parámetros de eficiencia

Para el análisis de las herramientas de medición los parámetros de las técnicas de QoS, es dirimente realizar una descripción de cada una de las posibles herramientas a usar, con el fin de elegir la más adecuada para los objetivos de este proyecto de titulación.

3.4.1. PingPlotter

PingPlotter es una herramienta de diagnóstico que aporta con el análisis gráfico de conectividad de la red punto a punto, para este caso. En específico PingPlotter hace el seguimientos de los paquetes que salen del ordenador de origen hasta el destino, mostrando cada salto en una gráfica diferente, realizando así un seguimiento segmentado para una mejor resolución de problemas a través de una interfaz muy sencilla de comprender, pudiéndose observar todos los datos que interfieren en la conexión con un simple vistazo [10], [11].

Las principales características de PingPlotter son:

- Realiza seguimiento de los paquetes desde el ordenador origen hasta que llegan al servidor destino.

- Comprobar la latencia, los paquetes perdidos y jitter.
- Guardar y comentar los resultados obtenidos.
- Bajo consumo y mayor rendimiento
- Soporte para IPv6.

Adicionalmente, en la Tabla 5 se muestran detalles técnicos de PingPlotter, que puede usarse en resolución de problemas como en monitoreo de la red.

Resolución de Problemas		
Característica	**Libre**	**Profesional**
Objetivo	Uno a la vez	Cientos a la vez
Métricas	Latencia, paquetes perdidos	Latencia, paquetes perdidos, jitter
Paquetes	ICMP	ICMP, UDP, TCP (Windows), agentes remotos
Rutas	Visualiza la ruta actual	Visualiza la ruta actual, ajusta el enfoque para ver los cambios de ruta
Protocolos	IPv4, IPv6	IPv4, IPv6
Análisis	Enfoque gráfico superior	Enfoque gráfico superior, escala y líneas de tiempo de desplazamiento
Monitoreo		
Característica	**Libre**	**Profesional**
Historial	10 minutos, grafica solo el salto final	Ilimitado, grafica todos los saltos.
Background collection	Funciona como servicio nativo	Funciona como servicio nativo
Administración	Guardar automáticamente los datos recogidos	Guarda automáticamente los datos recopilados, ventanas de acoplamiento y flotación, espacios de trabajo personalizados, pantallas de resumen, configuraciones con nombre
Acceso Remoto	N/A	Interfaz WEB
Condiciones de alertas	N/A	Latencia, pérdida de paquetes, basado en tiempo, basado en conteo
Alerta de eventos	N/A	Iniciar sesión en archivo, enviar correo electrónico, reproducir sonido, notificación de bandeja, llamada REST, modificar resumen

Comunidad		
Característica	**Free**	**Profesional**
Guarda	Texto, archivos PingPlotter, imágenes	Texto, archivos PingPlotter, imágenes
Carga	Propios archivos	Cualquier archivo PingPlotter

Tabla 5 Comparación de Características de Pingplotter

Fuente: https://www.pingman.com/products/features.html **[11]**

3.4.2. Microsoft Network Monitor

Microsoft Network Monitor. Es un analizador de paquetes que permite la captura, visualización y análisis de datos de una red y descifrar los protocolos de red [8]. Usualmente, se puede utilizar para solucionar problemas de la red y las aplicaciones en la misma [16], como muestra la Figura 3.7.

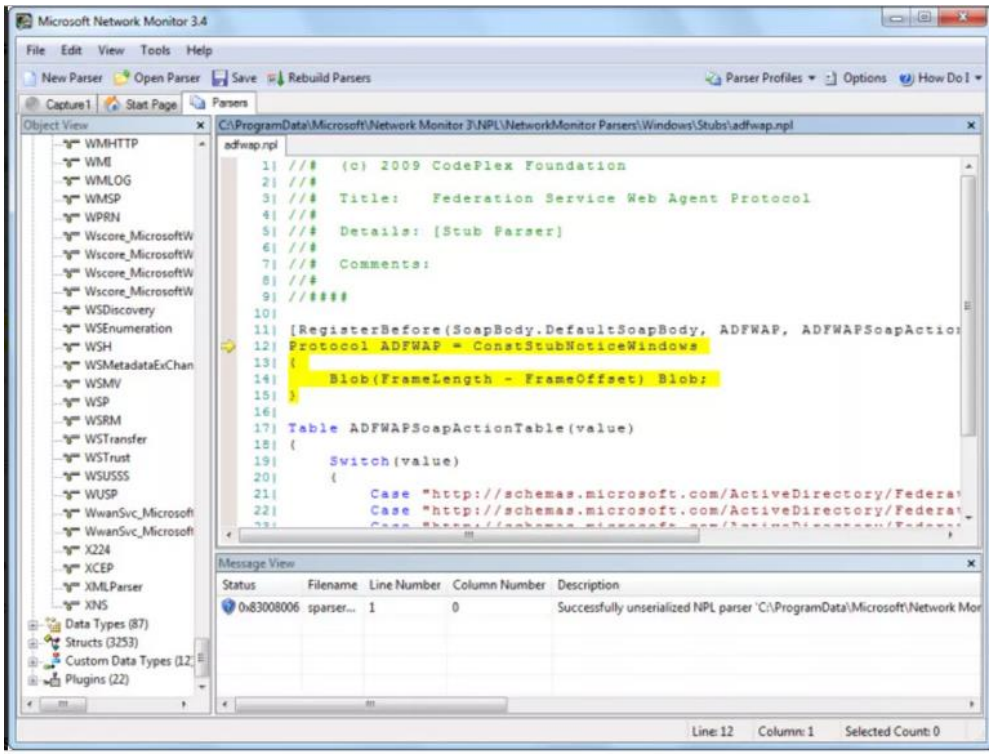

Figura 3.7 Vista de la pantalla principal de Microsft Network Monitor

Fuente: https://microsoft-network-monitor.softonic.com/ **[17]**

Características:

- Realiza seguimiento a los paquetes de la red.
- Se encarga de agrupar la red por conversación.
- Soporta más de 300 protocolos propietarios públicos y Microsoft [16]
- Sesiones de captura simultánea
- Modo Monitor inalámbrico con NICs inalámbricas compatibles
- Realiza capturas en tiempo real y la visualización de frames
- Re ensambla datos fragmentados
- Puede leer archivos de captura libpcap
- Orientado a usuarios avanzados [17]

3.4.3. MRTG

El Multi Router Traffic Grapher, conocido por sus siglas MRTG, es probablemente uno de los programas más populares en lo que a analizadores de tráfico se refiere. MRTG es un programa que se encarga de supervisar los dispositivos de red SNMP y generar gráficas que muestran la cantidad de tráfico que ha pasado por cada interfaz [12] como muestra la Figura 3.8.

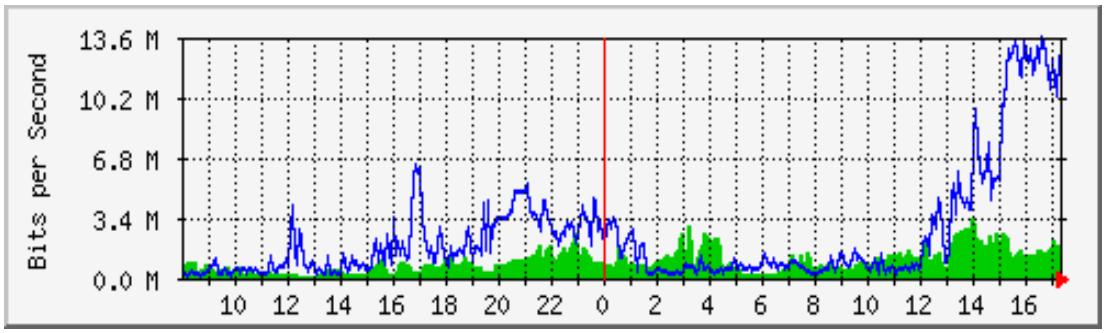

Figura 3.8 Gráfica de MRTG

Fuente: https://oss.oetiker.ch/mrtg/ **[12]**

Los enrutadores son solo el comienzo. MRTG se utiliza para graficar todo tipo de dispositivos de red, así como todo lo demás, desde datos meteorológicos hasta máquinas expendedoras [12]

El programa MRTG al final muestra un informe en formato HTML con gráficas de fácil compresión generando así una representación visual de la evolución del tráfico a lo largo del tiempo. Habitualmente se recolecta la información desde los routers utilizando el protocolo SNMP (Simple Network Management Protocol). Este protocolo proporciona la información en crudo de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Esta cantidad bruta deberá ser tratada adecuadamente para la generación de informes. Adicionalmente, este programa permite realizar consultas aunque no sean desde un dispositivo SNMP, proporcionando al final dos valores numéricos que se corresponden a la entrada y salida. Normalmente, se usan scripts que monitorizan la máquina local. Asimismo, proporciona una aplicación cfgmaker que genera la configuración para un router de forma automática utilizando la meta información que proporciona SNMP [13].
MRTG está escrito en perl y funciona en Unix / Linux, así como en Windows e incluso en sistemas Netware. MRTG es un software gratuito con licencia Gnu GPL [12].

Ventajas de MRTG

- Funciona en multiples plataformas, incluyendo Windows NT/2000.
- Fácil configuración.
- Permite establecer alarmas
- Soporta IPv6
- Recopilar datos es configurable, pudiendo usar SNMP o plugin [14]

Desventajas de MRTG

- Debido a que este escrito en Perl y que gran parte de los scripts de recolección de datos también se realicen en Perl, provoca que ordenadores no tan actuales su rendimiento sea menor.
- Programa monolítico y secuencial. Incluso con las partes que hay escritas en C, el programa es lento.

- No funciona como cliente/servidor.
- Las gráficas solo colorean dos variables en un gráfico, generalmente bytes/s de entrada y de salida debido al origen del programa, por lo tanto al ingresar variables adicionales, nos veremos en la necesidad de usar dos gráficas al mismo tiempo.
- Solo usa valores enteros.

3.4.4. Smokeping

SmokePing, es una herramienta de medición de latencia en la red que se encarga de enviar los paquetes de prueba a la red y mide la cantidad de tiempo que necesitan para viajar de un lugar a otro y de vuelta. Por cada ronda de medición, smokeping envía varios paquetes. A continuación, ordena los diferentes tiempos de ida y vuelta y selecciona la mediana, (es decir, la media). Esto significa que cuando hay 10 valores de tiempo, el valor número 5 se selecciona y se dibuja. Los otros valores se dibujan como tonos de gris sucesivamente más claros en el fondo (smoke).

A veces se envía un paquete de prueba pero nunca se devuelve. Esto se llama pérdida de paquetes. El color de la línea mediana cambia según el número de paquetes perdidos. Toda esta información en conjunto da una indicación de la red. Por ejemplo, la pérdida de paquetes es algo que no debería suceder de la nada. Puede significar que un dispositivo en el medio del enlace está sobrecargado o que la configuración de un enrutador está mal.

La gran fluctuación de los valores de RTT (tiempo de ida y vuelta) también indica que la red está sobrecargada. Esto se muestra en la gráfica como humo (smoke), considere el ejemplo de la Figura 3.8; Cuanto más humo existe en la gráfica, quiere decir que hay más fluctuación. Smokeping no se limita a probar solo el tiempo de ida y vuelta de los paquetes. También puede realizar alguna tarea en el extremo remoto ("sonda"), como descargar una página web. Esto dará una imagen combinada de la disponibilidad del servidor web y el estado de la red [15].

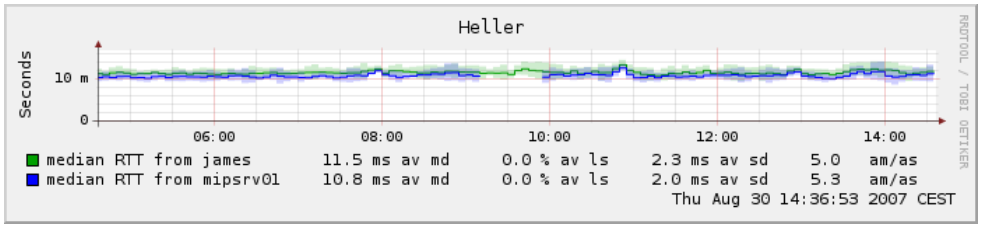

Figura 3.8 Gráfico general de resumen de Smokeping

Fuente: https://oss.oetiker.ch/smokeping/ **[15]**

La Figura 3.8 muestra las medidas actuales para un objetivo. Si el objetivo se mide desde el maestro tan bien como un esclavo, entonces se mostrarán los datos de ambos. En el modo multisistema, se muestran los datos de todos los hosts. Los siguientes números están presentes para cada línea, como muestra la Figura 3.9:

av md: Mediana promedio

av ls: Pérdida promedio

av sd: La desviación estándar promedio de las mediciones múltiples en cada ronda

am/as: La relación entre la media y la desviación estándar promedio.

Detalles del gráfico

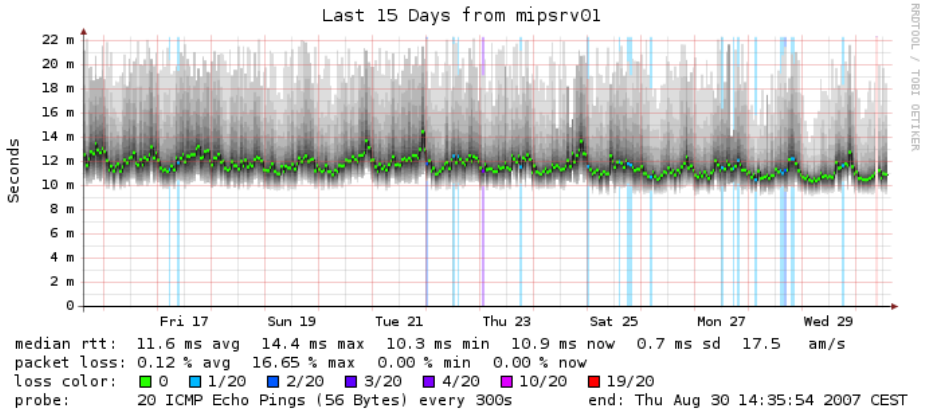

Figura 3.9 Detalle del Gráfico en Smokeping

Fuente: https://oss.oetiker.ch/smokeping/ **[15]**

La Figura 3.9 proporciona una gran cantidad de información para un solo objetivo como se ve desde un solo servidor. El color de la línea representa la cantidad de paquetes perdidos y el área oscura alrededor de la línea muestra la cantidad de variación entre las sondas individuales. Si hace clic en el gráfico, puede hacer un zoom interactivo en el modo de navegador [15]. Los siguientes números están presentes en cada gráfica:

avg, max, min, now: promedio, máximo, mínimo, media actual

sd: desviación estándar de la mañana

am/s: relación de la media vs desviación estándar.

3.5. Comparación y selección de herramientas de medición de datos

En los subcapítulos anteriores se han mostrado las características, ventajas y desventajas de algunos analizadores de tráfico, resumiendo aquello se muestra la Tabla 6, donde se resume las características más importantes.

Característica / Programa	Fácil configuración	Gráfica de Latencia vs # Paquetes	Modelo de ordenador	SO	Tipo de Usuarios	Seguimiento de Paquetes
PingPlotter	SI	SI	Cualquiera	Microsoft	General	SI
Microsoft Network Monitor	SI	NO	Cualquiera	Microsoft	Medio	SI
MRTG	NO	SI	Avanzada	Microsoft	Avanzado	SI
Smokeíng	NO	SI	Avanzada	Linux	Avanzado	SI

Tabla 6 Resumen de diferentes herramientas utilizadas como analizador de Tráfico Web

Para el desarrollo de este proyecto se decidió usar PingPlotter debido a que tiene una interfaz más sencilla de analizar, usa menos recursos, trabaja con Windows y se basa específicamente en analizar la latencia vs cantidad de paquetes en cada salto como muestra la Figura 3.10.

Figura 3.10 Captura de tráfico generado por un tipo de tráfico desde el Punto A de la red al Punto B

CAPÍTULO 4

4. PRUEBAS Y ANÁLISIS DE RESULTADOS

4.1. Configuración del Sistema

Para la configuración del escenario propuesto en el Capítulo 3 debemos de considerar aspectos como:

- Ancho de banda disponible del enlace WAN (serial).
- Ancho de banda utilizado por cada aplicativo (Tráfico específico)
- Tipo de tráfico.
- Cantidad de paquetes por segundo.
- Tamaño de paquetes a enviar.
- Tráfico propio del enlace generado con Ostinato (Generador de Tráfico).
- La unión de todos los tipos de tráfico que congestione el enlace WAN

Parámetros de configuración

Considerando los aspectos antes mencionados, se detalla a continuación las configuraciones de los escenarios de cada prueba realizada:

- Tráfico General: ubicado dentro del enlace WAN y generado con Ostinato, para lo cual se muestra en la Figura 4.1 el nombre del tráfico y el puerto por el que se está conectando para generarlo. Adicionalmente, en la Figura 4.2, 4.3 y 4.4 se muestran los parámetros que se deben configurar para generar un tráfico constante que pase por el enlace serial hasta el otro lado de la red. Los parámetros a configurar son:
    - L1: MAC
    - L2: Ethernet II
    - L3: IPv4
    - L4: TCP
    - L5: Texto
    - Tamaño de Paquetes: Fijo – 64
    - Dirección MAC del Gateway de la red SEDE_1 (Destination)
    - Dirección MAC del PC_GENERADOR_ANALIZADOR (Source)

- Dirección IP del PC_GENERADOR_ANALIZADOR (Source)
- Dirección IP del PC_B (Destination)
- Número de Total de Paquetes
- Rate: Paquetes por segundo

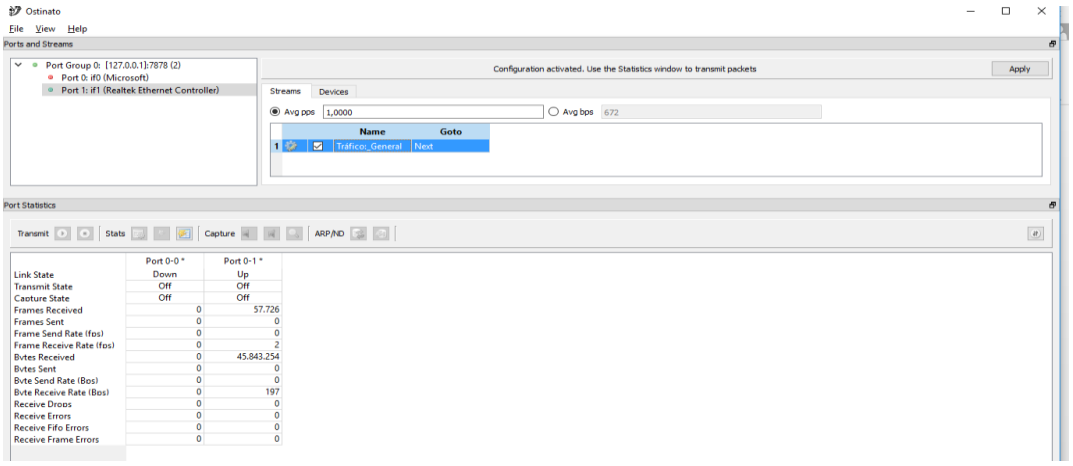

Figura 4.1 Nombre del Tráfico a Generar, puerto de salida, estadísticas del puerto

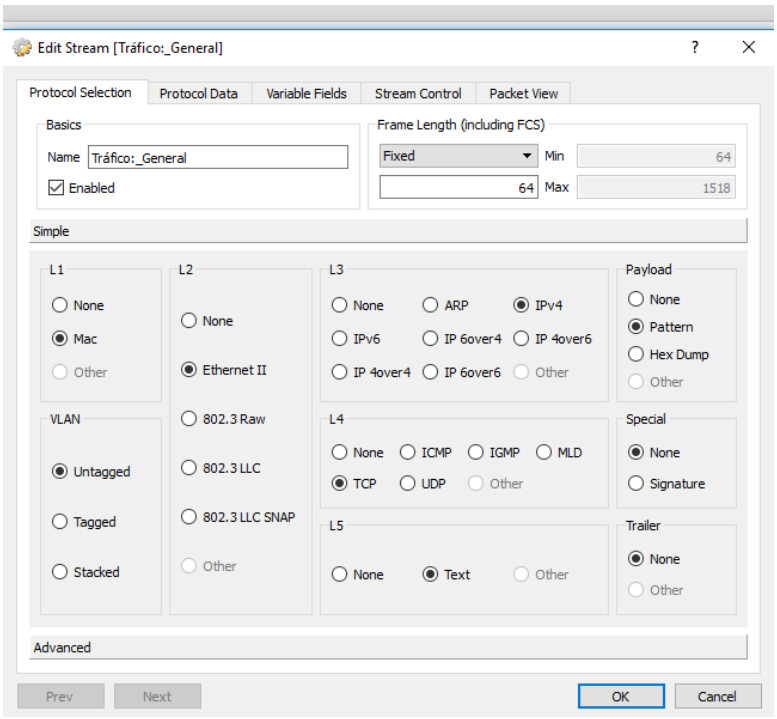

Figura 4.2 Configuración de tipo de tráfico, tamaño de tráfico y protocolo

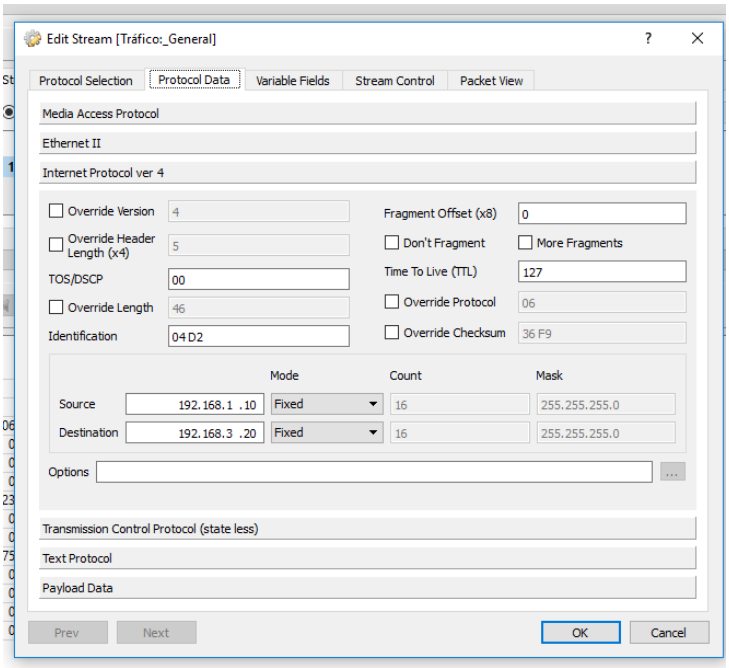

Figura 4.3 Configuración de direcciones origen y destino del tráfico

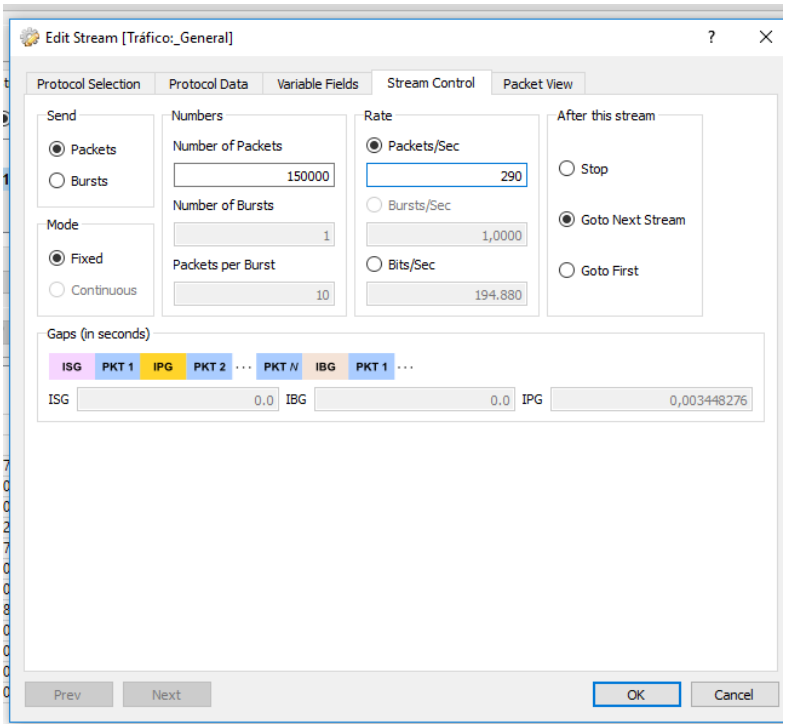

Figura 4.4 Configuración de cantidad total de paquetes y tasa de envío de paquetes.

4.2. Experimentación y Análisis de Escenario

Dentro de este subcapítulo se muestran las gráficas obtenidas del ensamble de una red punto a punto, sobre la cual se genera un tráfico que congestiona el enlace dificultando así la trasmisión de un tipo de tráfico en específico, al mismo que se le realiza el seguimiento desde el ordenador de origen hasta el ordenador destino.

Cabe recalcar que el tráfico general que congestiona la red es fijo, tanto en tamaño como en cantidad y tipo. Lo que varían son los tráficos específicos que durante todo el tiempo cada máquina adicional a la red envíe otro tipo de paquete, para de esta manera observar el correcto funcionamiento de la transmisión de paquetes con las diferentes técnicas de QoS, tales como PQ, LLQ y WFQ, realizando además un contraste con la gráfica obtenida de la trasmisión del mismo tipo de paquete sin usar Calidad de Servicio.

4.2.1. Análisis experimental de datos

Tráfico ICMP sobre IPv4

Figura 4.5 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv4 usando técnica por default FIFO

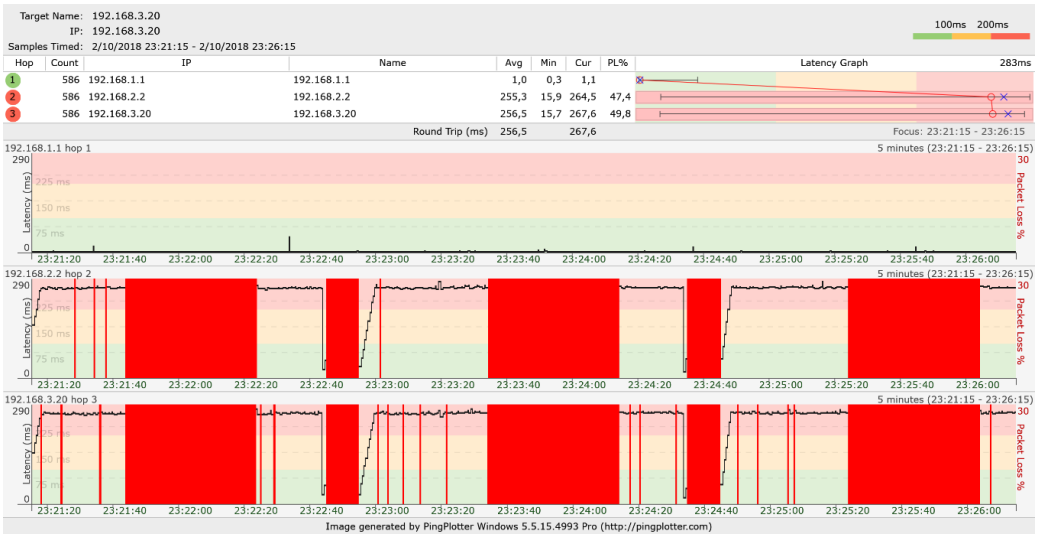

Figura 4.6 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv4 utilizando la Técnica de QoS PQ

Figura 4.7 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv4 utilizando la Técnica de QoS WFQ

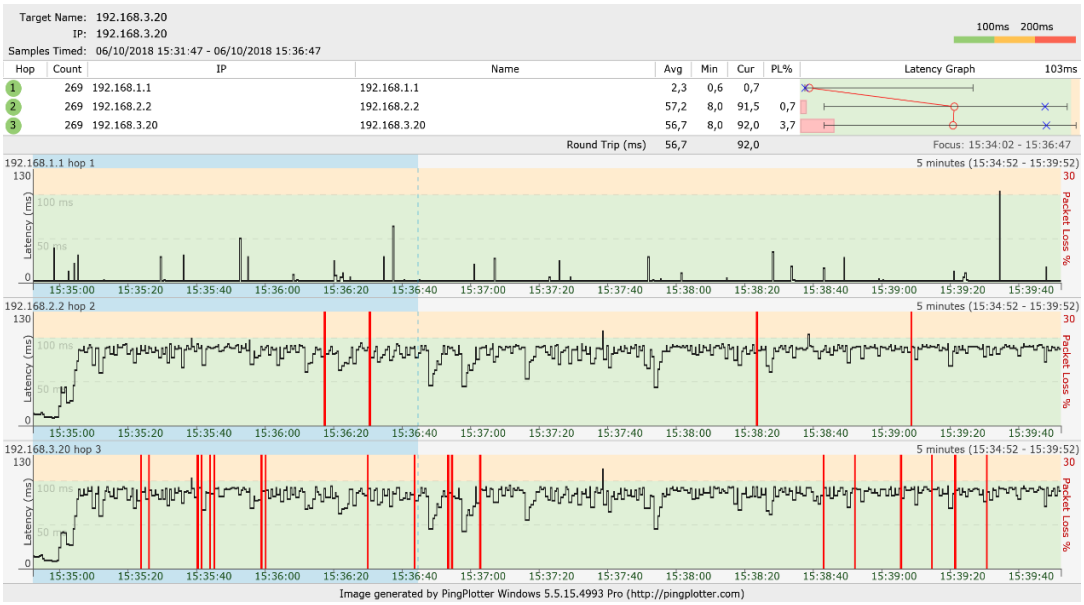

Figura 4.8 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv4 utilizando la Técnica de QoS LLQ

Tráfico IPv6

Figura 4.9 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv6 usando técnica por default FIFO

Figura 4.10 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv6 utilizando la Técnica de QoS PQ

Figura 4.11 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv6 utilizando la Técnica de QoS WFQ

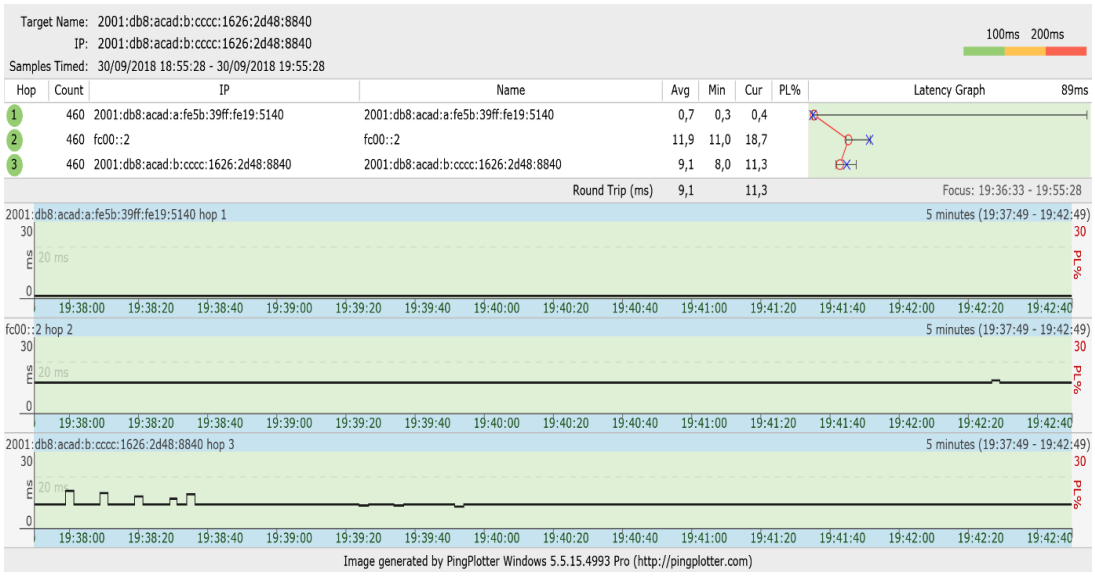

Figura 4.12 Gráfica resultante de la transmisión de Paquetes ICMP sobre IPv6 utilizando la Técnica de QoS LLQ

Tráfico VoIP

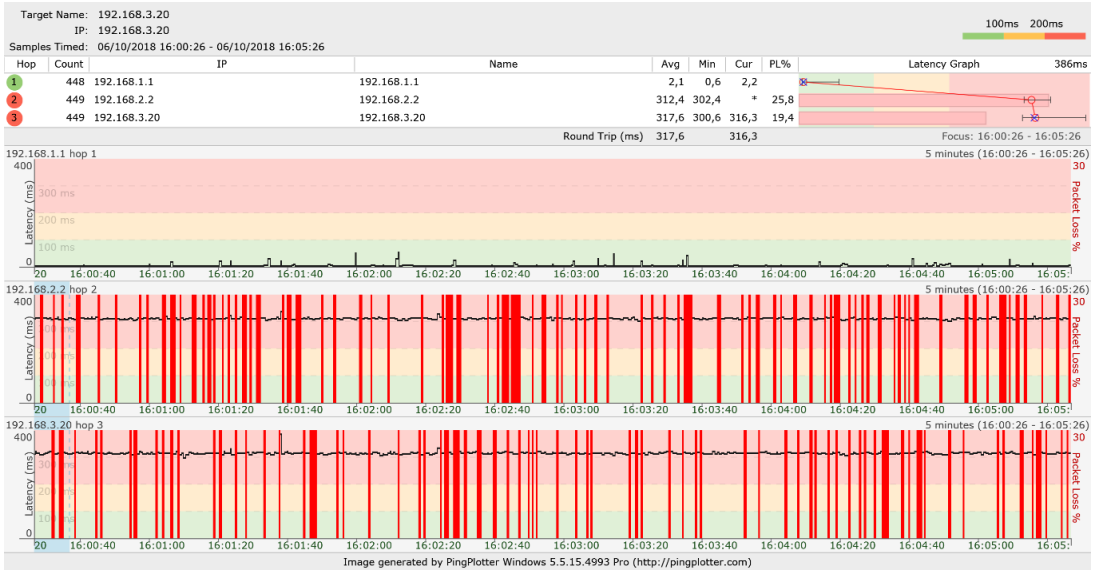

Figura 4.13 Gráfica resultante de la transmisión de VoIP usando técnica por default FIFO

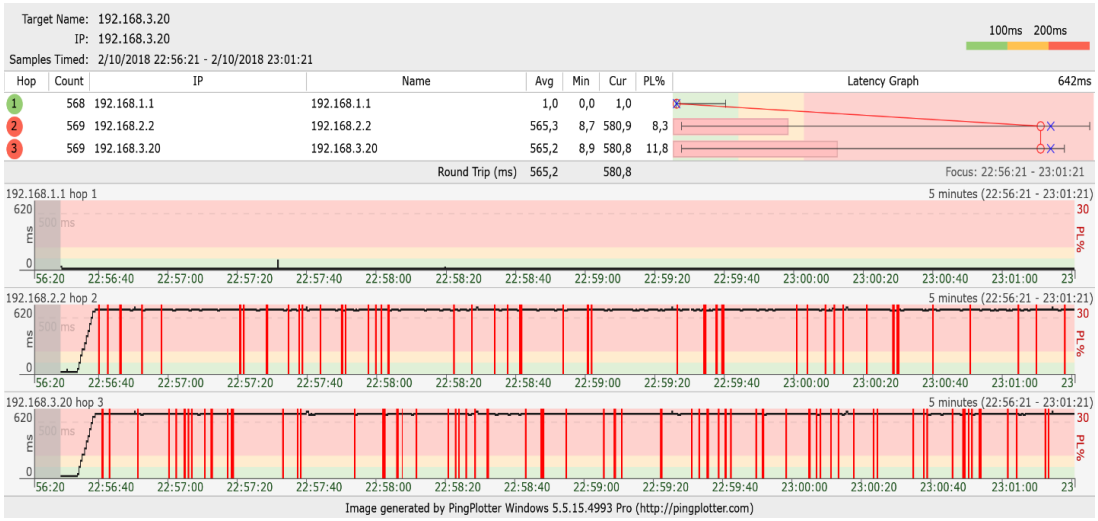

Figura 4.14 Gráfica resultante de la transmisión de VoIP utilizando la Técnica de QoS PQ

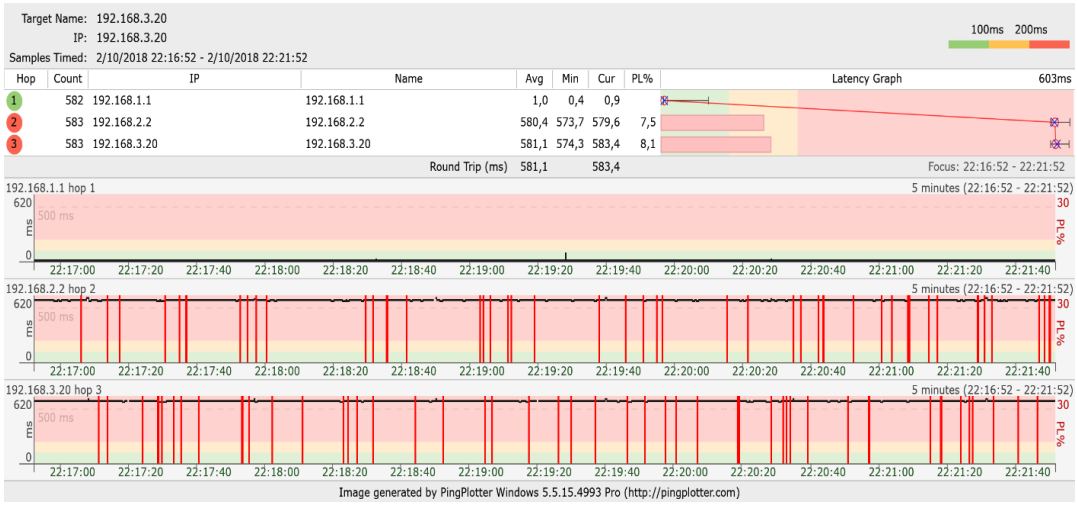

Figura 4.15 Gráfica resultante de la transmisión de VoIP utilizando la Técnica de QoS WFQ

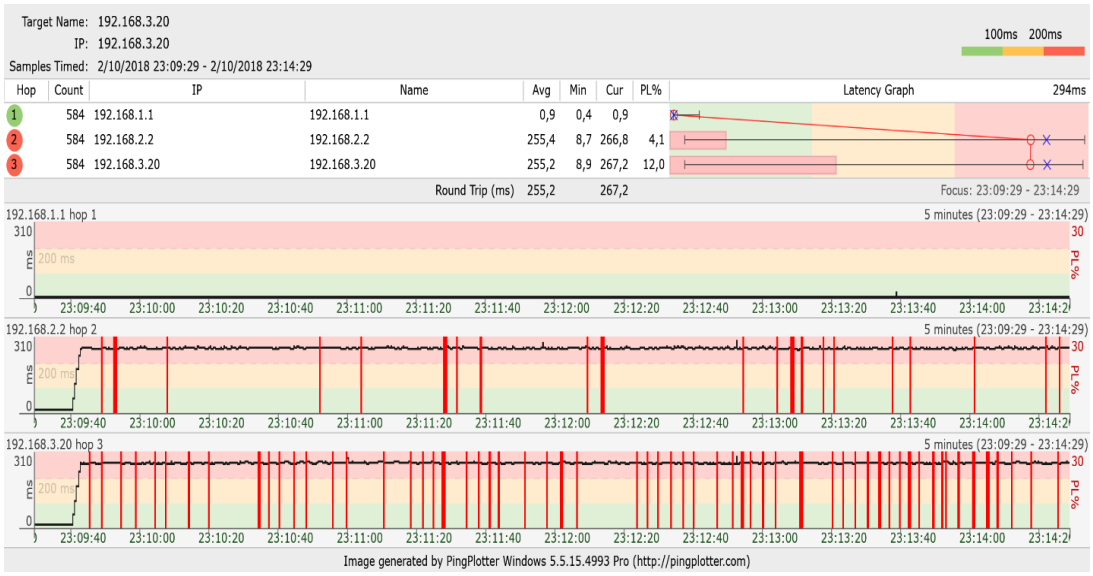

Figura 4.16 Gráfica resultante de la transmisión de VoIP utilizando la Técnica de QoS LLQ

Tráfico WEB

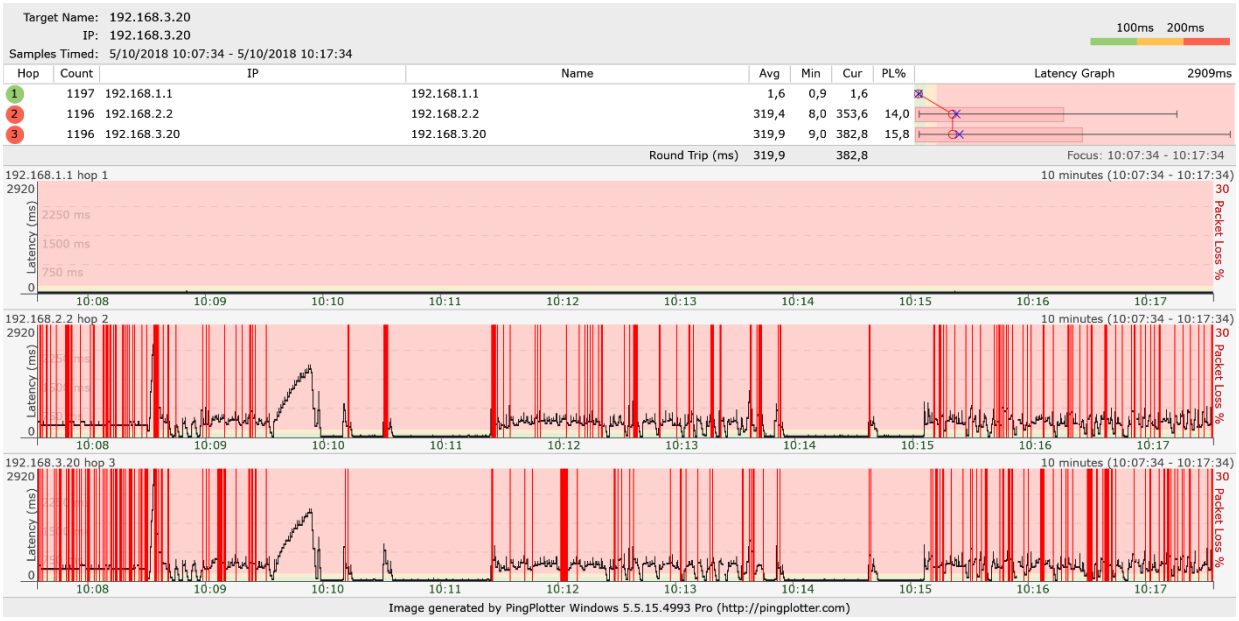

Figura 4.17 Gráfica resultante de la transmisión de Tráfico WEB usando técnica por default FIFO

Figura 4.18 Gráfica resultante de la transmisión de Tráfico WEB utilizando la Técnica de QoS PQ

Figura 4.19 Gráfica resultante de la transmisión de Tráfico WEB utilizando la Técnica de QoS WFQ

Figura 4.20 Gráfica resultante de la transmisión de Tráfico WEB utilizando la Técnica de QoS LLQ

4.2.2. Modelamiento y Validación de datos

Tráfico ICMP sobre IPv4

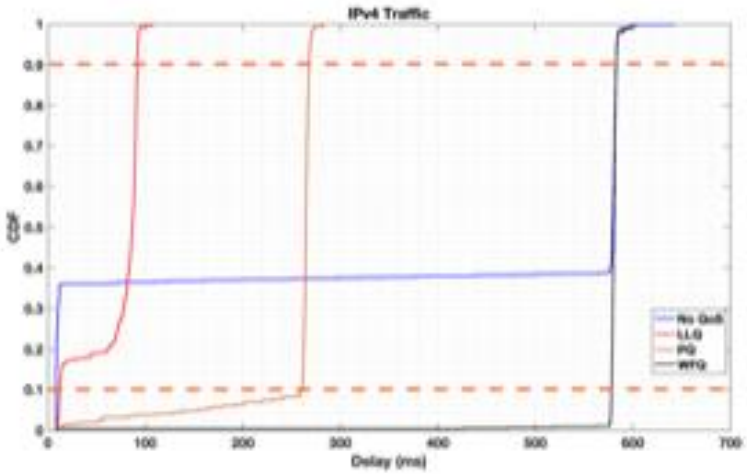

Figura 4.21 Gestión para Tráfico ICMP sobre IPv4 con PQ, WFQ y LLQ

Tráfico IPv6

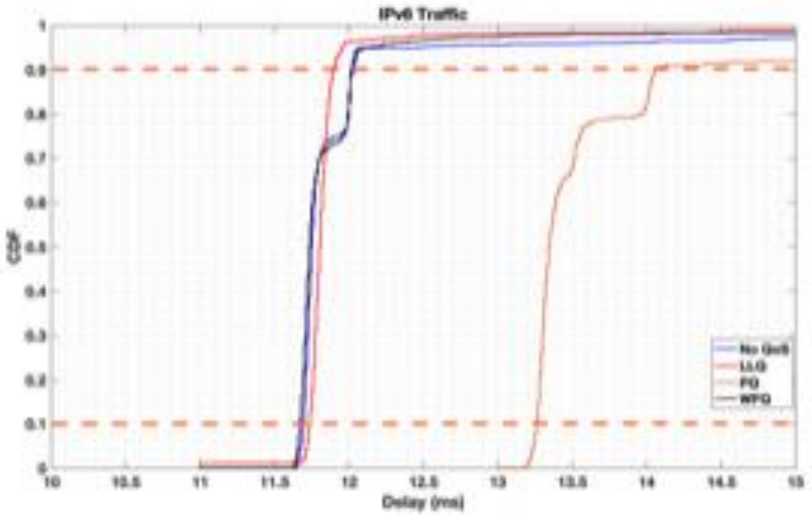

Figura 4.22 Gestión para Tráfico ICMP sobre IPv6 con PQ, WFQ y LLQ

Tráfico VoIP

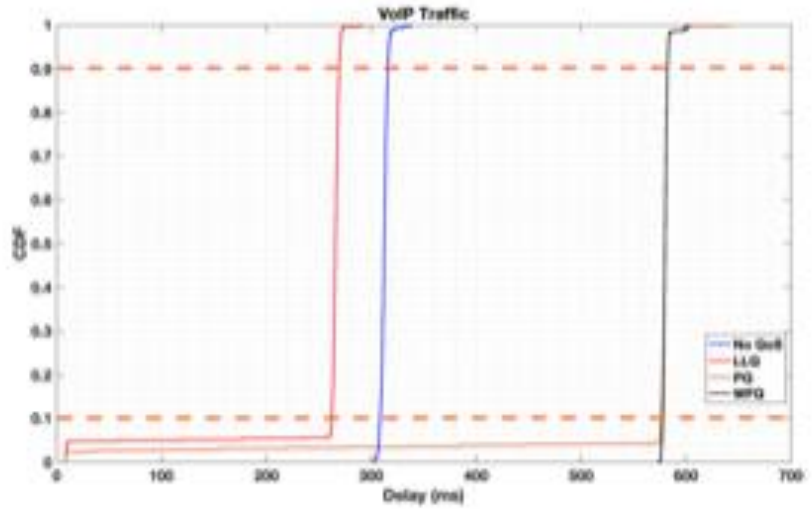

Figura 4.23 Gestión para Tráfico VoIP - UDP con PQ, WFQ y LLQ

Tráfico WEB

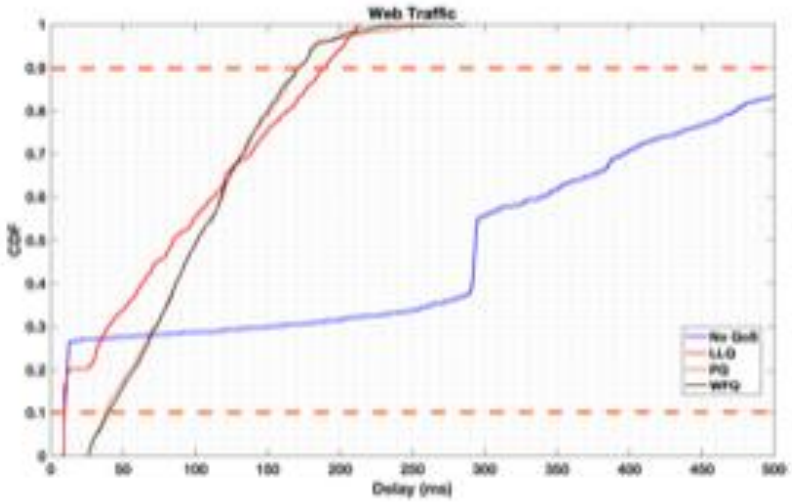

Figura 4.24 Gestión para Tráfico WEB con PQ, WFQ y LLQ

4.3. Análisis comparativo de resultados

Comparar Tráfico ICMP sobre IPv4

Después de realizar la captura de datos y generar gráficas se muestra el consolidado de los resultados en la Tabla 7, donde se puede observar gracias a la herramienta PingPlotter los tiempos de latencia en milisegundos (ms) y porcentaje de paquetes perdidos. El enlace normalmente se encuentra inundado con tráfico TCP de tamaño fijo configurado con la herramienta Ostinato, cada ejecución se hizo en un periodo de 5 minutos por reiteradas ocasiones. Analizando la tabla antes mencionada, se puede observar que los tiempos de latencia Sin QoS son bastante altos al igual que al configurar WFQ, considerando la configuración por default en routers Cisco, FIFO estamos otorgando todo el ancho de banda para todas las aplicaciones que en ese momento se están enviado, haciendo que el router realice su mejor esfuerzo de transmitir todo (Best Effort), con WFQ a pesar de crear colas y asignarle un ancho de banda a cada una de ellas, el tráfico que se envía desde un extremo a otro es mayor al asignado en el canal.

En cambio al configurar PQ asignamos prioridad a ese tipo de tráfico logrando mejorar ese tiempo de latencia dentro del enlace WAN y por ultimo como se muestra tanto la

Tabla 7, Tabla 8, Tabla 9 y Tabla 10, al configurar LLQ se asignas colas y prioridad a la vez logrando así que todos los tiempos de latencia y número de paquetes perdidos sea el menor posible para satisfacer los requerimientos de las aplicaciones que se envían dentro de la red WAN.

Las aplicaciones tienen definidos ciertos tipos de tráfico, tales como: VoIP, HTTP, ICMPv4 e ICMPv6.

		Latencia			Número de Paquetes Perdidos (%)
Tráfico	Técnica	Promedio	Mínimo	Máximo	
IPv4	Sin QoS	556,6	8,9	579,7	3,4
	PQ	255,3	15,9	264,5	47,4
	WFQ	580,3	425,2	579,2	2,7
	LLQ	57,2	8,0	98,5	0,7

Tabla 7 Consolidado de tiempos de Latencia y Número de Paquetes perdidos de Tráfico IPv4 dentro del mismo escenario de red

Comparar Tráfico ICMP sobre IPv6

		Latencia			Número de Paquetes Perdidos (%)
Tráfico	Técnica	Promedio	Mínimo	Máximo	
IPv6	Sin QoS	12,0	11,6	11,8	3,0
	PQ	14,2	13,2	13.3	0,0
	WFQ	11,9	11,6	11,6	3,0
	LLQ	11,9	11	18,7	0,0

Tabla 8 Consolidado de tiempos de Latencia y Número de Paquetes perdidos de Tráfico IPv6 dentro del mismo escenario de red

Comparar Tráfico VoIP

		Latencia			Número de Paquetes Perdidos (%)
Tráfico	Técnica	Promedio	Mínimo	Máximo	
VoIP	Sin QoS	312,4	302,4		25,8
	PQ	565,3	8,7	580,9	8,3
	WFQ	580,4	573,7	579,6	7,5
	LLQ	255,4	8,9	266,8	4,1

Tabla 9 Consolidado de tiempos de Latencia y Número de Paquetes perdidos de Tráfico VoIP dentro del mismo escenario de red

Comparar Tráfico WEB

		Latencia			Número de Paquetes Perdidos (%)
Tráfico	Técnica	Promedio	Mínimo	Máximo	
Web	Sin QoS	319,4	8,0	353,6	14,0
	PQ	105,9	26	164,5	0,0
	WFQ	104,0	25,7	98	0,0
	LLQ	94,6	9,0	9,2	0,0

Tabla 10 Consolidado de tiempos de Latencia y Número de Paquetes perdidos de Tráfico WEB dentro del mismo escenario de red

CAPÍTULO 5

5. AJUSTES DE QoS EN EL MODELO PROPUESTO

5.1. Ajuste de QoS a un Tráfico ICMP sobre IPv4

Configuración de Parámetros: Claramente en el capítulo anterior se observó que la técnica de QoS que muestra mejores resultados al aplicar tráfico IPv4 dentro de una enlace WAN Punto a Punto aunque el enlace se encuentre al punto de colapsar por el tráfico que envían las demás Pc´s conectadas al sistema es LLQ, sin embargo esto se puede mejorar realizando los siguientes cambios a la configuración de la red:

```
!
configure terminal
!
class-map LLQ-IPv4
match protocol ipv4
exit
!
policy-map LLQ-IPv4
class LLQ-IPv4
priority percent 40
exit
interface serial 0/0/0
service-policy output LLQ-IPv4
```

Asignando así un mejor porcentaje del ancho de banda disponible para la transmisión de tráfico IPv4, obteniendo el resultado mostrado en la Figura 5.1, al cual se le asignó el 40% del ancho de banda disponible, en comparación al porcentaje del ancho de banda utilizado para generar la Figura 4.8 quien tenía asignado tan solo el 10% del mismo ancho de banda disponible en el enlace serial de la red de prueba.

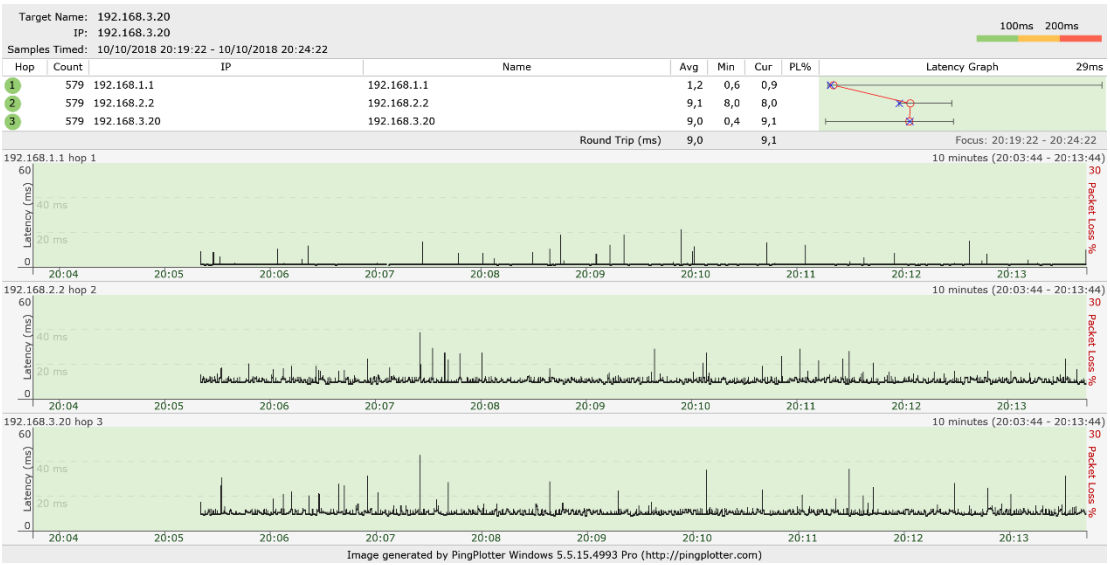

Figura 5.1 Gráfica resultante del ajuste en la configuración de LLQ para la trasmisión de Tráfico IPv4

5.2. Ajuste de QoS a un Tráfico ICMP sobre IPv6

Configuración de Parámetros: Nuevamente se hace énfasis al capítulo anterior donde se observó que la técnica de QoS que muestra mejores resultados al aplicar tráfico IPv6 dentro de una enlace WAN Punto a Punto aunque el enlace se encuentre al punto de colapsar por el tráfico que envían las demás Pc´s conectadas al sistema es LLQ, sin embargo esto se puede mejorar realizando el siguiente cambios a la configuración de la red:

```
!
configure terminal
!
class-map LLQ-IPv6
match protocol ipv6
exit
!
policy-map LLQ-IPv6
```

class LLQ-IPv6
priority percent 40
exit
interface serial 0/0/0
service-policy output LLQ-IPv6

Asignando así un mejor porcentaje del ancho de banda disponible para la transmisión de tráfico IPv6, obteniendo el resultado mostrado en la Figura 5.2, al cual se le asignó el 40% del ancho de banda disponible, en comparación al porcentaje del ancho de banda utilizado para generar la Figura 4.12 quien tenía asignado tan solo el 10% del mismo ancho de banda disponible en el enlace serial de la red de prueba.

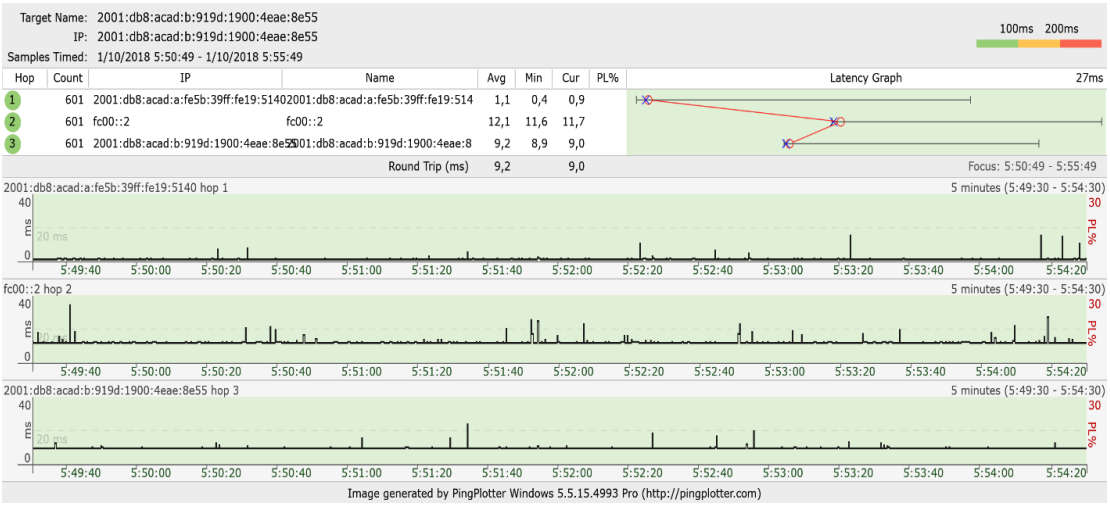

Figura 5.1 Gráfica resultante del ajuste en la configuración de LLQ para la trasmisión de Tráfico IPv6

5.3. Ajuste de QoS para Tráfico de VoIP

Configuración de Parámetros: Evidentemente los resultados del capítulo anterior muestran que la técnica de QoS que muestra mejores resultados al aplicar tráfico VoIP (UDP) dentro de una enlace WAN Punto a Punto aunque el enlace se encuentre al punto de colapsar por el tráfico que envían las demás Pc´s conectadas al sistema

es LLQ, sin embargo esto se puede mejorar realizando los siguientes cambios a la configuración de la red:

```
!
configure terminal
!
class-map VoIP
match protocol udp
exit
!
policy-map VoIP
class VoIP
priority percent 50
exit
interface serial 0/0/0
service-policy output VoIP
```

Así, con la configuración precedente, asignando un mayor porcentaje del ancho de banda disponible para la transmisión de tráfico de VoIP obteniendo el resultado mostrado en la Figura 5.3, al cual se le asignó el 50% del ancho de banda disponible, en comparación al porcentaje del ancho de banda utilizado para generar la Figura 4.16 quien tenía asignado tan solo el 10% del mismo ancho de banda disponible en el enlace serial de la red de prueba.

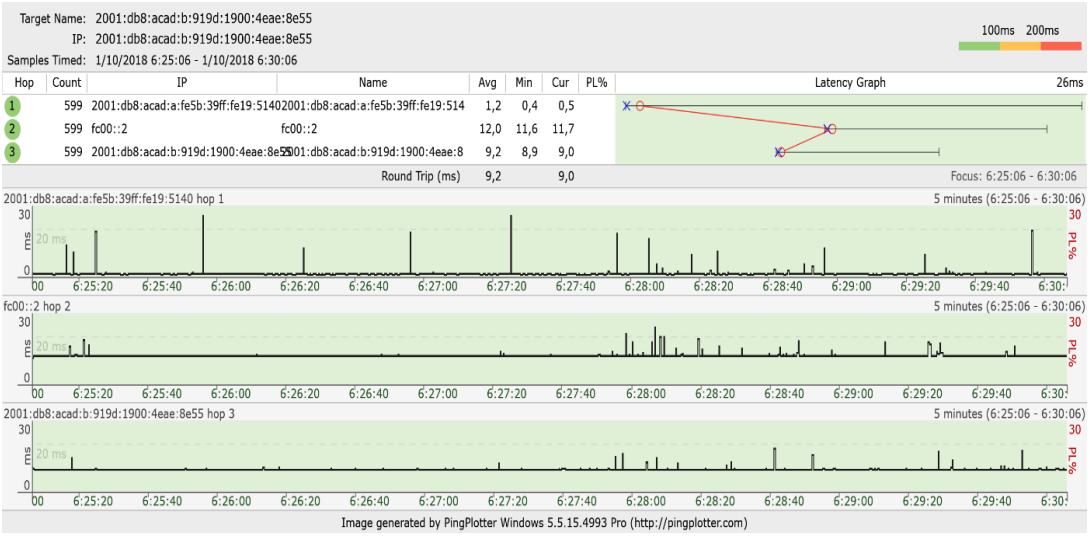

Figura 5.3 Gráfica resultante del ajuste en la configuración de LLQ para la trasmisión de Tráfico de VoIP

5.4. Ajuste de QoS para Tráfico WEB

Configuración de Parámetros: Al analizar las gráficas del capítulo anterior se observó que la técnica de QoS que muestra mejores resultados al aplicar tráfico WEB (http) dentro de una enlace WAN Punto a Punto aunque el enlace se encuentre al punto de colapsar por el tráfico que envían las demás Pc´s conectadas al sistema es LLQ, sin embargo esto se puede mejorar realizando los siguientes cambios a la configuración de la red:

```
!
configure terminal
!
class-map HTTP
match protocol http
exit
!
policy-map WFQ
class HTTP
bandwith percent 75
exit
```

Bajo esta nueva configuración de parámetros que ajustan el mayor porcentaje del ancho de banda disponible para la transmisión de tráfico WEB obteniendo el resultado mostrado en la Figura 5.4, al cual se le asignó el 75% del ancho de banda disponible del enlace, en comparación al porcentaje del ancho de banda utilizado para generar la Figura 4.20 quien tenía asignado tan solo el 10% del mismo ancho de banda disponible en el enlace serial de la red de prueba.

Figura 5.4 Gráfica resultante del ajuste en la configuración de LLQ para la trasmisión de Tráfico WEB

CONCLUSIONES Y RECOMENDACIONES

1. Los algoritmos de Calidad de Servicio se activan cuando el enlace se encuentra congestionado en ambos sentidos, tanto en escenarios reales como virtuales.
2. Para el tráfico ICMP sobre IPv4 bajo condiciones de congestión se obtuvo una latencia máxima de 579,5ms y el 3,4% de paquetes perdidos aplicando el método FIFO. En el caso de PQ, la latencia máxima de 264,5ms y 47,4% de pérdida de paquetes; aplicando WFQ, la latencia máxima de 579,2ms y 2,7% de pérdida de paquetes; utilizando LLQ, la latencia máxima de 91,5ms y 0,7% de pérdida de paquetes, concluyendo de esta manera que dentro de un enlace WAN congestionado, sobre el cual se transmite tráfico ICMP sobre IPv4 la técnica de QoS que da mejores resultados es LLQ.
3. Para el tráfico ICMP sobre IPv6 bajo condiciones de congestión se obtuvo una latencia máxima de 11,8ms y 3% de paquetes perdidos al aplicar el método FIFO. En el caso de PQ, la latencia máxima de 18,7ms sin pérdida de paquetes; aplicando WFQ, la latencia máxima de 11,6ms y 3% de paquetes perdidos; utilizando LLQ, la latencia máxima de 13,3ms y 0,0% de pérdida de paquetes, concluyendo de esta manera que dentro de un enlace WAN congestionado, sobre el cual se transmite tráfico ICMP sobre IPv6 la técnica de QoS que da mejores resultados es LLQ.
4. Para tráfico de VoIP bajo condiciones de congestión se obtuvo una latencia máxima de 312,4ms y 25,8% de paquetes perdidos al aplicar el método FIFO. En el caso de PQ, la latencia máxima de 580,9ms y 8,3% de paquetes perdidos; aplicando WFQ, la latencia máxima de 579,6ms y 7,5% de paquetes perdidos; utilizando LLQ, la latencia máxima de 266,8ms y 4,1% de pérdida de paquetes, concluyendo de esta manera que dentro de un enlace WAN congestionado, sobre el cual se transmite tráfico de VoIP la técnica de QoS que da mejores resultados es LLQ.
5. Para tráfico de WEB bajo condiciones de congestión se obtuvo una latencia máxima de 353,6ms y 14,0% de paquetes perdidos al aplicar el método FIFO. En el caso de PQ, la latencia máxima de 164,5ms y 0,0% de paquetes perdidos;

aplicando WFQ, la latencia máxima de 98,0ms y 0,0% de paquetes perdidos; utilizando LLQ, la latencia máxima de 9,2ms y 0,0% de pérdida de paquetes, concluyendo de esta manera que dentro de un enlace WAN congestionado, sobre el cual se transmite tráfico de VoIP la técnica de QoS que da mejores resultados es LLQ.

6. En este proyecto se demostró la aplicación de las técnicas de QoS más utilizadas al momento de mejorar la latencia generada por diferentes aplicaciones dentro de un enlace punto a punto; se cumplió el objetivo de evaluar FIFO, PQ, WFQ y LLQ bajo el mismo escenario, se logró evaluar otras configuraciones adicionales a publicaciones anteriores (por ejemplo, [22] - [23]).
7. Se ha utilizado una topología de red generalizada; el presente proyecto concluye que tener un enlace WAN punto a punto donde se puede configurar técnicas de QoS, LLQ es sin duda la Técnica de Calidad de Servicio más eficiente para la transferencia de datos tipo IPv4, IPv6, HTTP y VoIP.
8. Para una correcta toma de datos es necesario realizar ajustes al tráfico generado por la herramienta Ostinato, ya que dependiendo del ancho de banda de la aplicación a analizar, tendremos mayor o menor saturación del enlace, sin llegar a la saturación total del mismo, en este caso sencillamente no pasa ningún tipo de tráfico a través de ese enlace. Para estos casos debemos de previamente realizar unos pequeños cálculos considerando: ancho de banda disponible del enlace WAN, ancho de banda de las aplicaciones que utilizan el enlace y ancho de banda del tipo de tráfico generado por Ostinato; porque los tres factores juntos deben de solo llenar en enlace para hacer que se activen las técnicas de QoS.
9. Previo a la configuración de las técnicas de QoS, es recomendable verificar que todos los ruteadores soporten una versión de sistema operativo que tengan la capacidad de soportar QoS.
10. Se recomienda usar herramientas que analicen el tráfico con gráficas puntuales, enfocándose al estudio que las variables por analizar, así no se desperdician recursos y la captura de datos sea más eficiente, con el más mínimo desperdicio de información.
11. Al momento de intentar asignar todo el ancho de banda disponible de la red a un solo tipo de tráfico, el router en su configuración muestra un mensaje de error,

donde explica que el máximo ancho de banda disponible para asignarle a una aplicación específica es del 75% del total, pero si nos vemos en la necesidad de asignarle todo el ancho de banda disponible, debemos conocer un comando especial de asignación de todo el ancho de banda.

12. Es recomendable saber cuál es el ancho de banda requerido por cada aplicación que ingresará al enlace para tener una idea clara al momento de saturar el enlace.

BIBLIOGRAFÍA

[1] Hartpence, Bruce. Packet Guide to Voice Over IP. " O'Reilly Media, Inc.", 2013.

[2] Evans, John William, and Clarence Filsfils. Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice. Morgan Kaufmann, 2010.

[3] Szigeti, Tim, et al. End-To-End QoS Network Design: Quality of Service for RichMedia and Cloud Networks. Pearson Education, 2013.

[4] M. Molina, "Análisis de la utilización de Calidad de Servicio (QoS) en Redes de Nueva Generación en (NGN) en el Ecuador", disertación de Maestría en Telecomunicaciones, Facultad FIEC, ESPOL, Guayaquil, Ecuador, 2013

[5] I Guachilema, "QoS en una red UMTS en Duran", disertación de Ingeniería en Electrónica y Telecomunicaciones, Facultad FIEC, ESPOL, Guayaquil, Ecuador, 2010.

[6] CISCO, (2006, Enero) Acceso octubre 2018. [En línea]. Disponible: 1https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-link-efficiency-mechanisms/24906-152.html

[7] D. Torres, Emilio Rosales, "Comparaciónde Técnicas de QoS en una red IP para aplicaciones de VideoStreaming", disertación de Ingeniería Electrónica en la facultad de Ingenierías en la Universidad Tecnológica de Bolívar, Guayaquil, Ecuador, 2012

[8] EcuRed. (2018). *Microsoft Network Monitor*. Acceso sept 2018. [En línea]. Disponible: https://www.ecured.cu/Microsoft_Network_Monitor#Caracter.C3.ADsticas

[9] CISCO, (2009, Octubre). Cisco Integrated Services Router Generation 2. Acceso sept 2018. [En línea]. Disponible: https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/qa_c67_553891.html

[10] PingPlotter. (1998-2018). Acceso septiembre 2018. [En línea]. Disponible: https://www.pingplotter.com/products/professional.html

[11] Pingman Tools. (1998-2017). Acceso septiembre 2018. [En línea]. Disponible: https://www.pingman.com/products/features.html

[12] Tobi Oetiker. (2017, Mayo). Acceso septiembre 2018. [En línea]. Disponible: https://oss.oetiker.ch/mrtg/

[13] Es.wikipedia.org. (2018). *MRTG*. 2. Acceso sept 2018. [En línea]. Disponible en: https://es.wikipedia.org/wiki/MRTG

[14] Rodríguez, J. (2018). *Monitorización de máquinas*. Acceso sept 2018. [En línea]. Jrodriguez.50webs.com. Disponible: http://jrodriguez.50webs.com/mon.html

[15] (2018). Acceso septiembre 2018. [En línea]. Disponible: https://oss.oetiker.ch/smokeping/doc/reading.en.html

[16] (2018). Acceso septiembre 2018. [En línea]. Disponible: https://www.ecured.cu/Microsoft_Network_Monitor#Caracter.C3.ADsticas

[17] (1997-2018). Acceso septiembre 2018. [En línea]. Disponible: https://microsoft-network-monitor.softonic.com/

[20] Router-switch.com. (2018). *Cisco 2800 Series Routers Models Comparison 2801 2811 2821 2851*. Accedido Sept 2018 [En línea]. Disponible en: http://www.router-switch.com/cisco-2800-series-routers-models-comparison-2801-2811-2821-2851-pd-45.html

[21] Comparison of Cisco Switches: (2960 vs 3560), (. (2018). *Comparison of Cisco Switches: (2960 vs 3560), (Cisco 3560 X vs 3650 vs 3750-X vs 3850)*. Accedido Sept 2018 [En línea]. Blog.51sec.org. Disponible en: https://blog.51sec.org/2016/01/comparison-of-cisco-switches-2960-vs.html

[22] M. M. G. Rashed, M. Kabir, “A Comparative Study of Different Queuing Techniques in VoIP, Video Conferencing and FTP”, Daffodil International University Journal of Science and Technology, Volume 5, Issue 1, January 2010

[23] S. Akhtar, E. Ahmed, A. k. Saka, K. S. Arefin Performance Analysis of Integrated Service over Differentiated Service for Next GenerationInternet, © JCIT, ISSN 2078-5828 (print), ISSN 2218-5224 (online), Vol. 1, Issue 1, 2010

Carlos A.S. Oliveira. “Optimization problems in Telecommunications and the Internet”, dissertation presented to the graduate school of the university of florida in partial fulfillment of the requirements for the degree of doctor of philosophy, Universidad de Florida, USA, 2004.

Vahid Jamali†, Arman Ahmadzadeh†, Nariman Farsad‡, Robert Schober†, and Andrea Goldsmith‡, “SCW Codes for Optimal CSI-Free Detection in Diffusive Molecular Communications”, Stanford University, Stanford, California, USA

J. Basurto, “Análisis Comparativo de la Implementación de Voz sobre IP en Wireless Mesh Networks y Wireless LAN tradicionales tomando en consideración parámetros de Calidad de Servicio y Problemas de Movilidad ocasionados por Handoffs”, disertación de Ingeniería en Electrónica y Telecomunicaciones, Facultad FIEC, ESPOL, Guayaquil, Ecuador, 2010.

M. Moshiur Rahman, “Design Optimization of Wireless Access Virtualization Based on Cost & QoS Trade-Off Utility Maximization”, Student Member, IEEE, Charles Despins, Senior Member, IEEE, and Sofiène Affes, Senior Member, IEEE, 2016.

Naila Bouchemal,Sondes Kallel, Samir Tohme, “A Cross-Layer QoS Solution for Resource Optimization in LTE Networks”, University of Versailles, France, 2016.

Reble, M.; Müller, M.A; Allgower, F., "Unconstrained model predictive control and suboptimality estimates for nonlinear time-delay systems," Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on , vol., no., pp.7599,7604, 12-15 Dec. 2011

Liu, G.P., "Predictive Controller Design of Networked Systems With Communication Delays and Data Loss," Circuits and Systems II: Express Briefs, IEEE Transactions on , vol.57, no.6, pp.481,485, June 2010

Martins, E.C.; Jota, F.G., "Design of Networked Control Systems With Explicit Compensation for Time-Delay Variations," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on , vol.40, no.3, pp.308,318, May 2010

Kun Yang; Ou, S.; Guild, K.; Hsiao-Hwa Chen, "Convergence of ethernet PON and IEEE 802.16 broadband access networks and its QoS-aware dynamic bandwidth allocation scheme," Selected Areas in Communications, IEEE Journal on , vol.27, no.2, pp.101,116, February 2009

Daojun Xue; Yang Qin; Chee Kheong Siew, "Deterministic QoS Provisioning with Network Calculus Based Admission Control in WDM EPON Networks," Communications, 2009. ICC '09. IEEE International Conference on , vol., no., pp.1,6, 14-18 June 2009

Xiaolong Jin; Geyong Min; Lan Wang, "A Comprehensive Analytical Model for Weighted Fair Queuing under Multi-Class Self-Similar Traffic," Communications, 2009. ICC '09. IEEE International Conference on , vol., no., pp.1,5, 14-18 June 2009

Lei Liu; Xiaolong Jin; Geyong Min; Keqiu Li, "An Analytical Model of Deficit Round Robin Scheduling Mechanism under Self-Similar Traffic," Scalable Computing and Communications; Eighth International Conference on Embedded Computing, 2009. SCALCOM-EMBEDDEDCOM'09. International Conference on , vol., no., pp.319,324, 2527 Sept. 2009

Hansen, Jeffrey, et al. Adaptive Flow Control for Enabling Quality of Service in Tactical Ad Hoc Wireless Networks. No. CMU/SEI-2010-TR-030. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2010.

Hwang, I-Shyan, Zen-Der Shyu, and Jhong-Yue Lee. "A QoS-enhanced dynamic bandwidth allocation mechanism in EPONs." J. Comput. Inf. Syst6.11 (2010): 3527-3533.

Senkindu, Samuel. A Quality of Service Architecture for WLAN-wired Networks to Enhance Multimedia Support. Diss. University of Cape Town, 2008.

Khambari, Mohd Najwan Md. "Achieving Stable Throughput to Support QoS in IEEE 802.11 Wireless Networks."

Kumar, Rajender, and Brahmjit Singh. "Comparison of vertical handover mechanisms using generic QoS trigger for next generation network."International Journal of NextGeneration Networks (IJNGN) 2.3 (2010).

Sarma, Manas Pratim. "Performance Measurement of TCP and UDP Using Different Queuing Algorithm in High Speed Local Area Network.". International Journal of Future Computer and Communication, Vol. 2, No. 6, December 2013

I. Guachilema, I. León, “Calidad de Servicio (QoS) de una red UMTS en la ciudad de Durán”, disertación de Ingeniería en Electrónica y Telecomunicaciones, Facultad FIEC, ESPOL, Guayaquil, Ecuador, 2010.

Ghuman, Mandeep, and Shammi Bahel. "QOS Estimation of IEEE 802.3 under the Influence of Intra-Domain Routing Protocols.". IJCSCIVolume 4 • Number 2 pp.1-7. September 2013.

Hamidian, Ali. Supporting Internet access and quality of service in distributed wireless ad hoc networks. PhD Dissertation. Lund University, Sweden. 2009.

Shin, Sangho. Towards the Quality of Service for VoIP traffic in IEEE 802.11 Wireless Networks. Dissertation. Columbia University, 2008.

Skorpil, Vladislav, and David Novak. "Network elements controlled by artificial neural network." Proceedings of the 14th WSEAS international conference on Communications. 2010.

Richard, James, and Paul Zam. "Ethernet in the First Mile: 802.3 ah." (2008). Unpublished.

Hoeft, M., Gierlowski, K., Gierszewski, T., Konorski, J., Nowicki, K., & Wozniak, J. Measurements of QoS/QoE parameters for media streaming in a PMIPv6 testbed with 802.11 b/g/n LANs. Metrology and Measurement Systems, 19(2), 285-294. 2012.

Din, N.M.; Radzi, N.AM.; Sadon, S.K.; Al-Mansoori, M.H., "Approaches in Dynamic Bandwidth Allocation in Passive optical network systems," Photonics (ICP), 2013 IEEE 4th International Conference on , vol., no., pp.10,14, 28-30 Oct. 2013

Talukder, Asoke K., Nuno M. Garcia, and G. M. Jayateertha. Convergence Through All-IP Networks. CRC Press, 2013.

Nucci, Antonio, and Konstantina Papagiannaki. Design, Measurement and Management of Large-Scale IP Networks: Bridging the Gap Between Theory and Practice. Cambridge University Press, 2009.