Comparación de Técnicas de QoS en una red IP para aplicaciones de VideoStreaming

Documento presentado como opción de grado para el programa de Ingeniería Electrónica en la facultad de Ingenierías en la Universidad Tecnológica de Bolívar.

Autores
Diego Camilo Torres Torres
Martin Emilio Rosales González
Cartagena de Indias D.T. y C.

2012

Comparación de Técnicas de QoS en una red IP para aplicaciones de VideoStreaming

DIEGO CAMILO TORRES TORRES

MARTIN EMILIO ROSALES GONZALEZ

Asesor:

M. Sc. RICARDO JAVIER ARJONA ANGARITA

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA ELECTRÓNICA

CARTAGENA DE INDIAS D. T. Y C.

2012

Dedicado a Dios y a nuestros padres,

Que nos dieron la fortaleza para sacar

Este trabajo adelante.

AGRADECIMIENTOS

Diego Camilo Torres y Martin Rosales González, expresan sus agradecimientos a:

El Ingeniero especialista en telecomunicaciones Antonio Carlos Bustillo Cabana, por el tiempo dedicado, su colaboración desinteresada en el desarrollo de este trabajo de investigación y por ayudarnos a abrir el camino de este proyecto.

Al nuestro asesor, MsC. Ricardo Javier Arjona Angarita, por otorgarnos la oportunidad de investigar y desarrollar un tema tan interesante y de índole actual como el tratado en el siguiente trabajo de investigación.

Al profesor Ingeniero Isaac Zúñiga por su aporte y colaboración a los problemas presentados durante todo el proceso de implementación del caso de estudio.

Al profesor Ingeniero Gonzalo López Vergara, por ser nuestro maestro y mostrarnos por primera vez el mundo de las telecomunicaciones.

A todas las personas, compañeros, profesores, familiares y amigos, que de alguna u otra manera nos impulsaron a desarrollar este trabajo y que además han sido parte de nuestra formación como ingenieros electrónicos y electricistas.

TABLA DE CONTENIDO

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

Ancho de Banda: es la cantidad de información que se puede transmitir a través de una red de telecomunicaciones.

Assured Forwarding AF PHB: tipo de marcación en el campo DSCP que da precedencia a paquetes en una red de telecomunicaciones.

Best effort service: servicio que provee las redes de telecomunicaciones es aquel que se encarga de hacer todo lo posible para que los paquetes de datos alcancen su destino final.

CBWFQ: tipo de encolamiento de paquetes, tiene la misma función de FQ, pero además de la lectura del campo DSCP toma como parámetro las clases de trafico creadas por los administradores de red para dar prelación a los paquetes.

Códec: abreviatura de codificador-decodificador, programa capz de transformar un archivo con un flujo de datos para facilitar su transporte.

Contenedor: tipo de archivo que almacena información de audio o video siguiendo un formato prestablecido

Differentiated Services, DiffServ: arquitectura de red que proporciona calidad de servicio en redes de telecomunicaciones, analizan varios flujos de datos, en vez de conexiones únicas. Los cuales se encargan de cumplir Acuerdos de Nivel de servicio o SLA, los cuales especifican en las clases de tráfico. a transmitir y estas clases son las que dan prioridad a los paquetes de diferentes aplicaciones que se desplieguen sobre la red.

DSCP, differentiated service codepoint field: hace referencia al Segundo byte en la cabecera de los paquetes IP este es usado para dar prioridad en la transmisión en los datos que se transportan a través de una red. Definido en la RFC2474

Expedited Forwarding: definido en la RFC2599, es un tipo de marcación en el campo DSCP, el cual le da una prioridad absoluta a los paquetes de transmision,

FIFO queing, first in- first out: tipo de encolamiento en donde el primer paquete que entra es el primer paquete que sale, no hay clasificación de la información.

FQ, fair queueing: tipo de encolamiento de paquetes el cual lee el campo DSCP de la cabecera de los paquetes IP, y según esto les otorga prioridad.

H.264: es un códec de video capaz de dar buena calidad de imagen con una tasa de bits muy baja esta definido en la norma ITU.T H.264.

Integrated Services, IntServ: arquitectura de red que se encarga de gestionar los recursos necesarios para garantizar calidad de servicio en una red de telecomunicaciones. Esta requiere de protocolos difícilmente escalables, ya que funciona realizando reservas de extremo a extremo en los elementos que constituyen la red de telecomunicaciones.

IPTV: corresponde a todo lo relacionado para los sistemas de subscripción para señales de televisión o video usando como medio de transporte las conexiones de banda ancha que van sobre el protocolo IP.

Jitter: Variabilidad temporal presente en el envío de señales digitales o paquetes de datos.

Latencia: corresponde al valor de la suma de todos los retardos temporales dentro de una red de telecomunicaciones. Los cuales son producidos por la demora en la propagación y la transmisión de los paquetes presentes en las redes de telecomunicaciones.

LLQ: encolamiento de baja latencia, consta de colas de prioridad personalizadas basadas en clases de trafico

Mp4a(AAC): es un formato contenedor, el cual se utiliza para transmitir flujos audiovisuales. Esta definido en el estándar MPEG-4 de la ISO/IEC

MPEG-TS: formato de transporte estándar, almacena la información de las características de un streaming de video, esta definido en el estándar ISO/IEC 13818-1.

Multicasting: corresponde al envío de información desde un punto a la red a numerosos destinos simultáneamente.

OWD: one way delay, retardo que presenta un paquete, cuando es transportado de un extremo de la red a otro

PHB: per hop behavior, comportamiento que presenta un flujo de datos cuando pasa de un equipo de la red a otro.

QoE Quality of Experience: calidad de la experiencia, es el grado de aceptabilidad que le otorgan los usuarios a los servicios desplegados a través de las redes de telecomunicaciones.

QoS, Calidad de servicio: tecnologías que garantizan la transmisión de cierta cantidad de paquetes de información en un tiempo establecido, también se conoce como la capacidad de una red de comunicaciones en proveer en excelente servicio, en donde se de prioridad a los datos que realmente son importantes.

RTP, real time Protocol: Protocolo a nivel de sesión, usado para enviar paquetes de aplicaciones en tiempo real. Publicado como estándar en la RFC1889 y posteriormente actualizado en la RFC3550.

Sniffer:

UDP, User Datagram Protocol: protocolo a nivel de transporte, no orientado a la conexión.

Unicasting: corresponde al proceso del envío de información de un receptor a un emisor único.

RESUMEN

En el siguiente documento se realiza un estudio comparativo e introductorio de las estrategias de calidad de servicio utilizadas para la transmisión de video. En primera instancia se ilustra al lector sobre los conceptos básicos de QoS y de técnicas de video-streaming. Se definen conceptos, técnicas y estrategias para el manejo de congestión en redes ip y lo concerniente a la codificación de los archivos antes de transmitir para hacer más eficiente procesos como partición de información, serialización y transmisión de los datos a través de la red.

En segundo lugar, se define el tráfico a usar en la aplicación, y al cual se le aplican las políticas de calidad de servicio, las cuales son el objeto de comparación en el siguiente trabajo de investigación.

Para realizar el análisis correspondiente, se configura en el laboratorio un escenario apto para evaluar y comparar las técnicas de calidad de servicio escogidas, este está conformado por dos redes LAN de dos computadores cada una, comunicadas entre sí por dos dispositivos enrutadores que emulan una WAN y que mediante un enlace de 1544 kbps generan un cuello de botella que facilita la generación de congestión en el circuito en los momentos de transmisión.

La transmisión es hecha en una sola dirección utilizando como protocolo de transporte RTP y con los requerimientos de ancho de banda definidos previamente. El contenido está configurado para que en el momento en que los servidores transmitan al tiempo encuentren que el enlace no es suficiente para los dos y se produzcan errores y pérdidas de paquetes.

Basados en esta congestión se aplican tres estrategias de encolamiento para evaluar su funcionamiento ante el problema de congestión. FIFO, WFQ y CB-WFQ son las técnicas escogidas. Se realizan capturas mediante un software de tipo ***sniffer*** en las interfaces de los clientes y se evalúan los parámetros de medida de calidad de servicio como lo son: pérdida de paquetes, *Jitter*, OWD (*One Way Delay*) y caudal.

Teniendo los resultados de cada estrategia, se compara el desempeño de cada una en el momento de cogestión y se concluye con base en esto.

INTRODUCCION

Durante las últimas décadas las redes de telecomunicaciones han presentado un crecimiento exponencial. Desde la aparición del protocolo IP, muchas tecnologías de uso cotidiano, como la radio y la televisión han migrado sus plataformas hacia la nube de internet o de redes *ip* privadas.

Con el crecimiento de las redes convergentes y la inclusión de tráfico multimedia en estas surge el problema de que cada tipo de información ya sean datos, audio o video requieren distintas condiciones de la red las cuales en su momento no se podían garantizar. Debido a esto, se desarrollan las políticas de calidad de servicio o *QoS,* estas determinan la capacidad que tiene una red de comunicaciones para sostener un comportamiento adecuado del tráfico que circula por ella, garantizando los requerimientos ofrecidos a un cliente o usuario final.

La aparición de *QoS* ha permitido, el desarrollo de servicios que requieren flujo de datos en tiempo real (voz y video), donde es necesario que no ocurra perdida de información, que exista una gran disponibilidad en el ancho de banda y que los retrasos de los paquetes sean mínimos; todo esto para garantizar a los usuarios del servicio una alta calidad en la experiencia.

Las mejoras tecnológicas tanto en la infraestructura de redes como en las estrategias de QoS han logrado que la difusión de contenidos audiovisuales se haya proliferado vertiginosamente (*youtube*, *netflix*, señales en vivo de canales privados como *RCN*, *CNN*, Caracol). Muchos de estos servicios son pagos y principalmente por ello los usuarios son más exigentes a la hora de evaluar y comparar su servicio, por ello al contar con políticas de calidad de servicio en productos como *IPTV*, *VOD* o *Internet Video* es posible asegurar la correcta entrega de la información, dando preferencia a los flujos de datos de carácter critico (p.e. Voz y Video en tiempo real), priorizando los flujos de datos según su importancia relativa y otorgándoles un tratamiento preferencial. Haciendo el rendimiento de la red más predecible y garantizando un uso más eficiente del ancho de banda.

El presente documento pretende comparar el funcionamiento y las bondades de utilizar diferentes estrategias de *QoS* en redes *ip* donde el tráfico es principalmente de contenido audiovisual. Para ello será necesario conocer conceptos de configuración de redes *ip*, *unicasting, multicasting, broadcasting*, *QoS*, compresión de datos multimedia y parámetros de medición de la calidad de servicio.

DESCRIPCIÓN DEL PROBLEMA

A la hora de diseñar una red que preste servicios a una cantidad fija o dinámica de usuarios se necesita tener seguridad en cuestiones como el tipo de tráfico que va a circular por la red, la disponibilidad que cada servicio debe tener, qué información es sensible al tiempo y cual no, qué requerimientos de ancho de banda se necesitan para soportar todos este tráfico y qué escalabilidad se le debe dar.

Desde el inicio de la era digital, cuando los contenidos audiovisuales migraron al mundo binario se tiene el problema que estos servicios necesitan unas garantías permanentes por parte de la red para poderse desarrollar como deben. Para esto existen las estrategias de calidad de servicio *QoS*. Toda LAN que pida un servicio a otra y que necesiten de una WAN para como intermediario para comunicarse es vulnerable a cambios en los caminos y las rutas disponibles para la información encontrándose muchas veces con enlaces con ofertas de ancho de banda muy angostos para las necesidades de la comunicación proveedor de servicio-usuario o servidor-usuario en un caso más sencillo. He aquí donde, si dichos enlaces cortos en recursos tienen la capacidad de elegir qué información es más vulnerable al tiempo, a la perdida de paquetes o a la desorganización en la entrega de información. Así mismo, existen variedad de técnicas y estrategias para administrar este tipo de decisiones, unas más eficientes que otras dependiendo de las necesidades de la información.

En la rama de la transmisión de video digital a través de redes ip, se necesitan estrategias que controlen la llegada de los paquetes completos y en el momento indicado. Es importante saber entonces ¿qué estrategias son las más usadas? y ¿por qué para estas aplicaciones? Si hay que enfrentarse ante una situación de red congestionada, ¿qué técnica produce los mejores resultados si hay tráfico de *video-streaming* en ella? Estas preguntas se pretenden responder en el siguiente documento.

OBJETIVOS

GENERAL

Implementar y comparar el uso de distintas técnicas de administración de recursos de red para la gestión de calidad de servicio (*QoS*) aplicado a tráfico de tipo *Video-Streaming* en una red con limitaciones de ancho de banda.

ESPECÍFICOS

- Establecer el estado del arte de técnicas de QoS aplicables a tráfico de video sobre redes IP, con el fin de seleccionar las técnicas a evaluar sobre una red de prueba que emule a pequeña escala las características reales de una red de distribución de contenido multimedia.

- Implementar una red que permita emular a pequeña escala las características reales de una que distribuya contenido multimedia utilizando servidores y computadores interconectados por medio de dos *routers* que entre sí crean un cuello de botella simulando una WAN como Internet para poder aplicar las técnicas de QoS escogidas y medir su funcionamiento.

- Realizar un análisis comparativo de las técnicas de QoS utilizando las métricas para evaluar su funcionamiento, tales como retardo, jitter, throughput y pérdida de paquetes, en el manejo de tráfico multimedia.

1. QoS Calidad de Servicio

La calidad de servicio se define como la capacidad que posee una red de telecomunicaciones de enfatizar la prioridad de su funcionamiento sobre un tipo de tráfico establecido. Esto se lleva a cabo otorgando niveles de servicio a los distintos tipos de tráfico presentes en la red de comunicaciones, en el cual se da una mayor importancia a los datos que necesitan correr aplicaciones en donde se requiere que el envío y la recepción de paquetes se realicen de manera exacta. Por ejemplo las aplicaciones en donde se manejan datos sensibles al tiempo (*IPTV*, llamadas de voz y Video, entre muchos otros).

La aplicación de parámetros de calidad de servicio en una red de telecomunicaciones permite obtener un mayor aprovechamiento de los recursos de red como el ancho de banda. Además, el funcionamiento de esta misma será mucho más predecible por lo tanto más óptimo, para esto es necesario definir las características o factores que son percibidos por los usuarios finales, y que determinan si existe o no calidad en el servicio.

Según [1] estos conceptos la calidad de servicio puede significar infinidad de cosas, según el enfoque de quien lo estudie, usuarios, proveedores de servicio, etc[1].

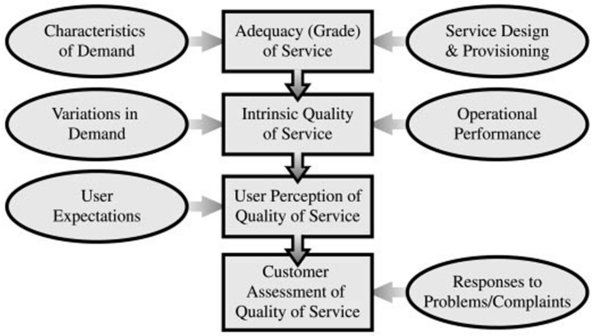

Figura 1 Percepción de la Calidad de Servicio

[1] Hardy, William C. Titulo "QoS Measurement and Evaluation of Telecommunications Quality of Service" pag 5; Ed. Jhon Wiley and Sons

1.1. Arquitectura en QoS

La calidad de servicio es un factor importante en la construcción y diseño de redes de telecomunicaciones, debido al crecimiento desmesurado de los servicios sobre el protocolo *IP*, el desarrollo de aplicaciones y su convergencia. Para esto existen modelos de arquitectura que se encargan de realizar la gestión del tráfico de los paquetes sobre la red.

1.1.1. Servicio al mejor esfuerzo (best effort service)

Se conoce como servicio al mejor esfuerzo a aquel en donde la red hace todo lo necesario para asegurar que el paquete llegue a su destino, es el servicio que prestan actualmente protocolos como ftp y http[2]. En este las aplicaciones envían datos en cualquier cantidad sin preguntar a la red. Por lo cual no lo hace adecuado para las aplicaciones sensibles al retardo o en aplicaciones en donde halla grandes variaciones en el ancho de banda. Por excelencia la red que opera de esta forma es Internet.

1.1.2. Servicios Integrados o IntServ

El tipo de arquitectura *IntServ*, es un modelo de servicios múltiples que permiten configurar variedad de políticas de *QoS*, en este las aplicaciones piden a la red un tipo específico de servicio antes de comenzar con la transmisión. Este requerimiento se realiza con señalización explicita, la aplicación informa a la red el perfil de su tráfico, y pide a esta un tipo particular de servicio que concuerde con sus requerimientos de retardo y ancho de banda. En esta arquitectura se espera que la aplicación comience la transmisión solo luego de obtener una autorización de la red y este tráfico debe cumplir con el perfil que se haya descrito.

IntServ clasifica el flujo del tráfico sirviéndose de las cabeceras de los datagramas IP. Clasificándolos en 3 tipos con el fin de especificar el tratamiento que se le debe realizar a cada uno de ellos, estos tipos son **servicios garantizados**, entre estos se encuentran los servicios de datos en tiempo real, **servicios de carga controlada**, para trafico en tiempo real menos critico como el VoD (video on demand), y **el best effort service** descrito en la anterior sección.

Para realizar su despliegue, IntServ utiliza el protocolo de reserva de recursos RSVP el cual se encarga de las necesidades de calidad de servicio para el tráfico de las aplicaciones a lo largo de toda la infraestructura de la red. Asegurando que cada dispositivo de red sea capaz de reservar el ancho de banda necesario para que pueda comenzar la transmisión.

[2] Valenzuela, Agustín Jose; Álvarez Moraga, Sebastián Titulo: "Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM".

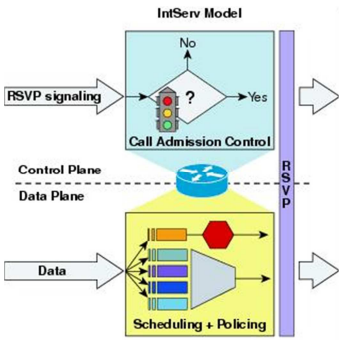

Figura 2 Arquitectura de Servicios integrados IntServ

1.1.3. Servicios Diferenciados DiffServ

El protocolo de servicios diferenciados, nace debido a la necesidad clara de tener un método sencillo y amplio para la prestación de diferentes clases de servicio para el trafico IP, con el fin de tener soportar diversos tipos de aplicación y el requerimiento de ciertos modelos de negocio. Diffserv se enfoca en proporcionar calidad de servicio a redes que emplean un conjunto bien definido de bloques de construcción en los cuales se pueden configurar más de un tipo de comportamiento en los paquetes de datos de cada servicio. Esta configuración es realizada en un pequeño segmento de la cabecera IP, para la versión 4 este es conocido como el octeto DSCP y, clase de servicio para IPv6. Este es usado para marcar los paquetes para que reciban un tratamiento preferencial en cada nodo de la red. Se requiere que se llegue a un acuerdo en el comportamiento de este campo entre los servicios inter-dominio, la interoperabilidad entre proveedores y consistencia en el comportamiento esperado de los servicios agregados a la red. Por lo tanto se ha estandarizado un esquema para el uso final de DiffServ llamado el campo DS. Los cuales son definidos en la RFC 2475[3].

Para proveer calidad de servicio de extremo a extremo DiffServ usa dos componentes principales para el marcado de paquetes, usando el segmento ToS o configurando comportamientos por salto.

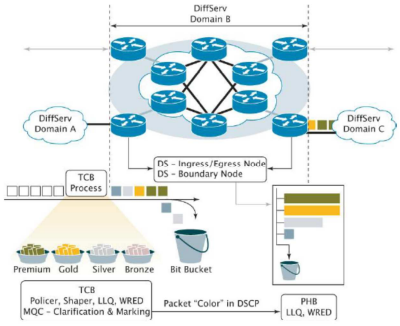

Figura 3 Arquitectura de Servicios Diferenciados DiffServ

[3] White paper "Diffserv—the scalable end-to-end quality of service model" Cisco Systems. 2005

1.1.3.1. Marcación de paquetes

A diferencia de la solución de la precedencia de paquetes IP, el datagrama ToS ha sido completamente redefinido en la arquitectura DiffServ, para clasificar paquetes se usan ahora seis bits. Y el campo se toma la denominación de campo DS o servicios diferenciados, en donde quedan dos bits sin usar. Estos seis bits sustituyen a los 3 bits de la solución de la precedencia IP, y es llamado DSCP. Con DSCP es posible tener hasta 64 clases de servicio en cada nodo de la red. Toda la clasificación y la calidad de servicio son manejadas por el DSCP en la arquitectura Diffserv.

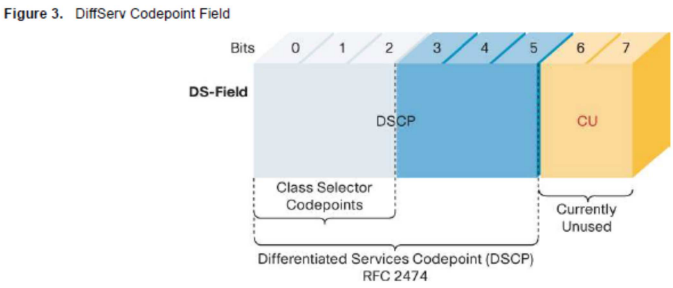

Figura 4 Campo DSCP Diffserv Codepoint Field

1.1.3.2. Comportamiento per Hop PHB

Una vez definido el campo DSCP, se debe ofrecer diferentes clases de servicio y además proveer las políticas de QoS que se requieren. Para esto se recogen los paquetes que tienen el mismo valor en el campo DSCP, y se asigna a ellos una dirección conocida como agregado de comportamiento o BA. Los paquetes de múltiples aplicaciones pueden pertenecer al mismo BA .

De este modo los enrutadores les asignan a los paquetes comportamientos de reenvío predeterminados, esta asignación es conocida como comportamiento por salto o PHB. El cual permite la gestión de colas, y aplicar mecanismos de control de flujo de información en los *Routers* de la red.

A continuación se definen los tipos de comportamiento por salto existentes. Adicionales al servicio de *best effort* el cual se provee por defecto.

1.1.3.3. EF PHB comportamiento por salto de reenvío expedito

Funciona de manera similar al protocolo RSVP de la arquitectura de servicios integrados, el EF PHB es el protocolo clave de la arquitectura de servicios diferenciados para proveer la menor perdida, menor latencia, bajo *jitter* y un servicio con un ancho de banda completamente asegurado.

Expedited Forwarding PHB puede ser implementado usando encolamiento prioritario, junto con limitaciones en el ancho de banda para las clases.

Aunque EF PHB cuando es usado en *Diffserv* provee un servicio Premium, debe ser únicamente direccionado a las aplicaciones mas criticas, ya que no es posible tratar a todos los servicios de red como servicios *Premium.*

EF PHB es recomendado para aplicaciones en tiempo real como *VoIP* y video ya que en ellas se requieren las características de tráfico anteriormente mencionadas, bajo *jitter*, etc. El campo DSCP usado para marcar el tráfico con EF es 1011100.

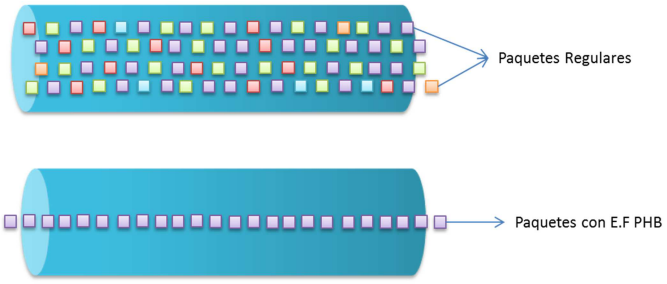

Figura 5 Expedited Forwarding EF PHB

1.1.3.4. AF PHB

Funciona de tal manera que asegura que el tráfico conforme a un perfil establecido, se entregue sin perdidas, definiendo 4 tipos de clases estandarizadas para reservar los recursos de la red y 3 clases para la configuración del descarte de paquetes.

Es equivalente al servicio de carga controlada del protocolo IntServ, este es un método por el cual los comportamientos de los agregados de tráfico pueden dar distintas características de reenvio de los paquetes. En este tipo los paquetes pueden ser divididos en tres clases p.e Oro, Plata y Bronce. Al cual se le pueden asignar a la clase Oro 50% del porcentaje del ancho de banda, a la clase plata el 30% y el 20% a bronce respectivamente.

El AFxy PHB define cuatro clases AFx: las cuales son AF1, AF2, AF3, AF4, respectivamente. Cada clase tiene asignado una cierta cantidad del espacio en el buffer y del ancho de banda de la interfaz, características que son dependientes del acuerdo de nivel de servicio SLA y de las políticas del proveedor.

A continuación se muestra la tabla de códigos DSCP para la configuración de AF-PHB.[4]

Table 1. DiffServ AF Codepoint Table

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

Figura 6 Numeración para la implementación de AF PHB

[4] White paper "Diffserv—the scalable end-to-end quality of service model" Cisco Systems. 2005 pag 6

2. Métodos de administración de la congestión

El manejo de la congestión en QoS corresponde al estudio de las estrategias de encolamiento, para sobrellevar las situaciones en donde el ancho de banda que es demandado por todas las aplicaciones excede el máximo que proporciona la red; esto se realiza llevando control sobre el tráfico entrando a la red y estableciendo prioridad de ciertos flujos de paquetes.

Existen distintos tipos de encolamiento entre los más destacados se encuentran son:

- FIFO
- Fair Queuing
- Encolamiento de prioridad o PQ
- CBWFQ
- LLQ

2.1. FIFO

Es el método de encolamiento más sencillo, en el encolamiento FIFO, todos los paquetes son tratados igualmente y son puestos dentro de una única cola, y son entregados en el mismo orden en el que son colocados dentro de la cola, es decir el primero paquete que ingresa es el primero que sale. Su desventaja es que maneja una cantidad de flujo de paquetes limitada, es decir cuando la cola esta llena los paquetes se descartan. En esta configuración los paquetes no son reordenados y el retardo máximo viene determinado por el tamaño máximo de la cola.

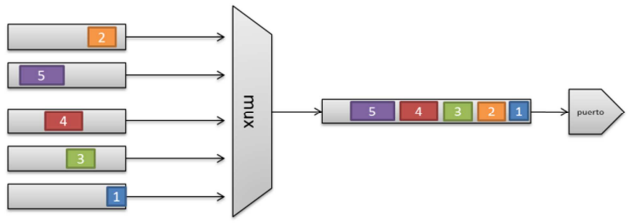

Figura 7 Encolamiento FIFO

2.2. Fair Queueing:

Generalmente conocido como ***WFQ, Weighted Fair Queueing***, este método provee una asignación de ancho de banda para todo el tráfico de la red, esta asignación de ancho de banda es la que determina el orden de como serán entregados los paquetes, y es hecha usando filtros disponibles en el datagrama IP, como las direcciones de origen y destino o el campo TOS.

FQ crea una cola distinta para cada tipo de tráfico asignándole a cada uno valores de profundidad para las colas. Las cuales siguen pasan a través de un servidor round robín, es decir siguiendo un orden secuencial circular. Como cada flujo tiene una cola asignada si se presentan demasiadas tramas de datos solo se vera afectado el rendimiento de la cola para cada clase especifica.

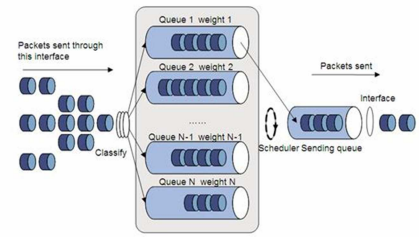

Figura 8 Encolamiento WFQ

2.3. Encolamiento de Prioridad PQ

Consiste 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 cuales son entregadas siguiendo estrictamente la prioridad que estas lleven asignadas. Las colas de mayor prioridad son atendidas primero, luego se atiende la de menor prioridad. Si una cola de prioridad baja esta siendo atendida, e ingresa un paquete de mayor prioridad, esta es atendida inmediatamente.

Este método de encolamiento se puede usar cuando se necesite dar prioridad a un tráfico importante, pero puede generar muy bajo desempeño en la entrega de paquetes que no sean considerados prioritarios.

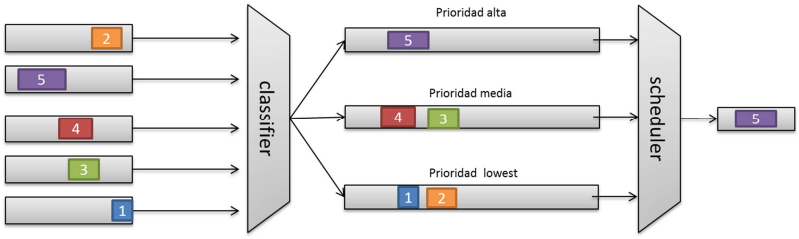

Figura 9 Encolamiento PQ

2.4. Class based weigthed fair queueing CB-WFQ

Extiende las características del encolamiento tipo FQ, ya que le otorga a los usuarios la habilidad de crear diferentes clases de trafico, estas son definidas usando el campo *DSCP* del datagrama *IP*, configurando listas de acceso o usando las interfaces de entrada como herramientas para configurar el encolamiento de paquetes. En este tipo de encolamiento, una cola es reservada para cada clase, y el tráfico correspondiente a cada una de ellas va directamente a la cola asignada para esa clase.

Para caracterizar las clases, se debe especificar el límite de la cola para esa clase, así como el ancho de banda, el peso, y el número máximo de paquetes que soportara. El ancho de banda que se le asigne será el ancho de banda que tendrá esa clase durante la congestión.

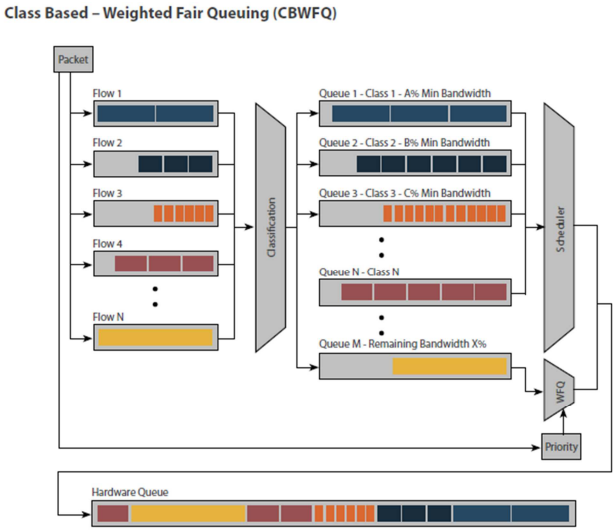

Figura 10 Encolamiento CBWFQ

2.5. Encolamiento de baja latencia Low Latency queueing LLQ

Es una mezcla entre el tipo de encolamiento de prioridad y el anteriormente explicado CBWFQ, es el método de encolamiento característico de las aplicaciones de telefonía IP y VoIP, LLQ esta basado en el uso de colas de prioridad personalizadas, las cuales están basadas en clases de trafico pre configuradas por el administrador de los servicios de red, estas clases de trafico en conjunto con una cola de prioridad, la cual tiene la mayor preferencia sobre las demás colas correspondiente a los diferentes flujos de datos.

Si hay presencia de tráfico en la cola de prioridad esta es atendida antes que las demás colas de prioridad personalizadas, si la cola de prioridad absoluta no esta encolando paquetes, las demás colas son atendidas según su prioridad asignada.

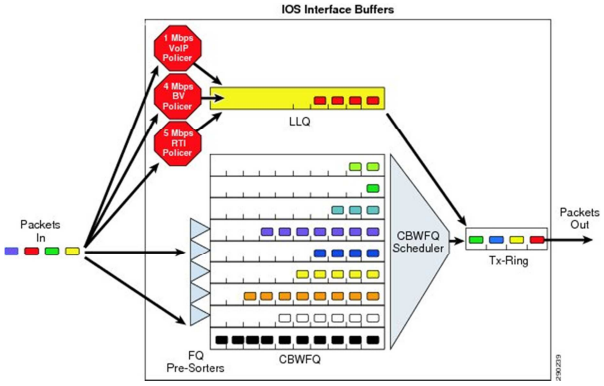

Figura 11 Encolamiento de Baja Latencia LLQ

2.6. Políticas de tráfico

Las políticas de tráfico son usadas para administrar de manera eficiente los recursos existentes en la red, estas limitan la tasa de transmisión de datos basándose en las clases de tráfico existente, para así tener control sobre el ancho de banda disponible en los enlaces.

Las políticas de tráfico son configuradas de extremo a extremo. Cuando se alcanza el máximo ancho de banda prestablecido, los paquetes empiezan a ser descartados, o se transmitirán con una prioridad diferente. Con esto garantiza que nunca se excederá el nivel de ancho de banda predefinido, sin embargo no se permitirá el almacenamiento de paquetes para ser enviados mas adelante[5]. [4]

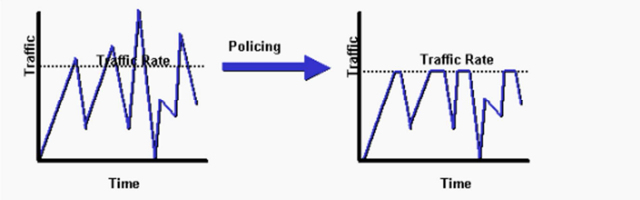

Figura 12 Politicas de Trafico Vs Modelamiento de Trafico

[5] Document ID 19645 "Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting" Cisco Systems 2008.

3. Parámetros de medición de calidad de servicio

La calidad de servicio, es generalmente medida en los extremos de la red de comunicaciones (proveedores y clientes), ya que pueden ser considerados como los puntos críticos, debido a que es en ellos en donde se nota el desempeño real de las aplicaciones y de los servicios que se despliegan a través de la red. El cual es cuantificado usando parámetros como el ***delay,*** **variación del retardo o** ***jitter,*** **caudal o** ***troughput,*** **latencia,** entre muchos otros.

3.1. Variación del retardo o *JITTER*

Se define como una variación en el retado de los paquetes que se reciben, y se explica de la siguiente forma, en el emisor los paquetes son enviados usando un flujo continuo, colocando cada paquete aparte de otro en intervalos de tiempo definidos, debido a la congestión de la red, a encolamiento inadecuado, o errores en la configuración, este flujo puede perder su uniformidad, y el tiempo puede variar en vez de permanecer constate, lo que puede producir congestión o abultamiento de los paquetes de información.

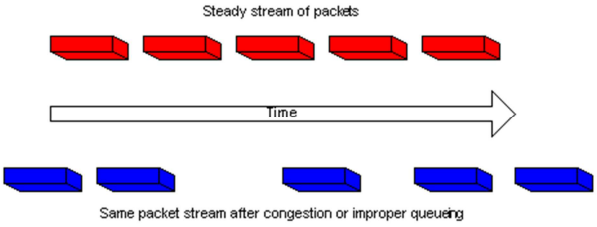

Figura 13 Variación del retardo Jitter

Si la magnitud del ***jitter*** es muy grande, se puede provocar que los paquetes queden por fuera del rango del buffer configurado en la estrategia de encolamiento y sean descartados, esto se ve reflejado directamente en el desempeño de la aplicación que esta siendo desplegada o ejecutada por la red[6].

En aplicaciones de video, la presencia de ***jitter*** se puede notar en distorsiones del video y el audio, lo que genera mala calidad de servicio percibida por el usuario final.

3.2. Delay

Es la cantidad de tiempo que toma un paquete para ir de un extremo de la red a otro, este tiempo es afectado directamente por los procesos que se realizan sobre los paquetes, mientras se abren paso por la red comunicaciones.

El retardo no es directamente una medida que determina la presencia de congestión, esta es generalmente implementada para la identificación del camino físico que recorren los paquetes sobre la red.

[6] Document ID: 18902 "Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)" 2009.

De igual manera es necesario poseer un buen manejo de las métricas del retardo, ya que existen aplicaciones que no tienen un buen desempeño. Si esta medida no es manejada debidamente, por ejemplo, las aplicaciones en tiempo real con variaciones muy irregulares en el retardo se hacen inmanejables, ya que entre mayor es el retardo se hace mas complicado mantener características como el ancho de banda, la cual es muy importante para prestar un excelente servicio a lo usuarios finales.

3.2.1. *One-way delay* OWD

La norma RFC-2679 define el ***one way delay*** como el tiempo que toma un paquete de datos para alcanzar su destino, este puede ser descompuesto en retardos por salto, los cuales se pueden convertirse en retardos por enlace o por nodo según su ubicación en la red de datos. El OWD es equivalente a la suma de todos los retardos individuales provenientes de los procesos que atraviesa el paquete de información, mientras se realiza su despliegue a través de la red.

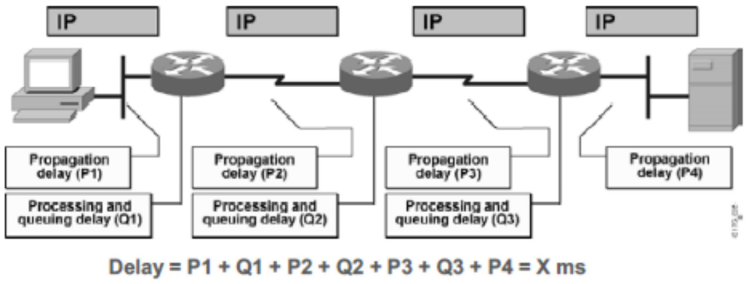

Figura 14 Medición de One Way Delay

La figura 14 muestra el impacto que tiene sobre el retardo de extremo a extremo, cada salto que el paquete da mientras se desplaza de un punto a otro, cada salto aumenta la magnitud en el retardo debido a los siguientes factores:

- El retardo de propagación, esta asociado al enlace, es causado por las características físicas del conductor o por el medio por el cual son transmitidos los paquetes de datos.
- Retardo debido al proceso de encolamiento. Corresponde al tiempo que espera el paquete en las colas del proceso de transmisión, este puede ser manejado implementado políticas de encolamiento.
- Retardo de enrutamiento, es el tiempo que toman los routers, en recibir los paquetes y darles un correcto encaminamiento[7].

[7] Knowledge.net "Implementing Cisco Quality Of Service (QoS) v2.0" student guide 2004

3.3. Caudal o *Throughput*

Es la medida del volumen de información que fluye a través de un sistema en nuestro caso, la red de telecomunicaciones. El caudal se mide por la tasa de paquetes sin errores, que fluyen a través del circuito, que hacen parte de una aplicación especifica, del conjunto de flujos que van de un nodo a otro, o el flujo de paquetes que van de un sistema autónomo a otro.

Entre mayor sea el valor del caudal obtenido, se establece que se prestan mejores parámetros de calidad de servicio, ya que el flujo de paquetes sin errores transmitido es mayor.[8]

El parámetro mas eficiente que se configura para tener control de caudal, es la cantidad de ancho de banda reservado para los diferentes tipos de paquetes.

Cuando el tráfico en las redes es diferenciado, se generan varias colas para cada tipo de tráfico y se controla el ancho de banda reservado para cada una de ellos. De esta manera en caso de congestión se podrá repartir el caudal entre los distintos tipos de tráfico.

3.4. Calculo de Métricas

El sniffer basado en el estándar RFC3550 realiza el calculo de las métricas siguiendo las siguientes expresiones:

- Jitter

$$D(i,j) = (R_j - R_i) - (S_j - S_i) - (R_i - S_i)$$

  En donde S es el RTP *timestamp* del paquete i, y Ri es el tiempo de llegada en unidades de RTP timestamp del paquete i.
  El jitter entre llegadas debe ser calculado continuamentem desde el momento que cada paquete i es recibido, usando el valor de la diferencia D para el paquete i y el paquete inmediatamente anterior se calcula mediante la siguiente expresión.

$$J(i) = J(i-1) + \frac{|D_{(i-1,i)}| - J(i-1)}{16}$$

- Through-put

  En esta se muestra el nivel de ancho de banda usado por el flujo RTP, corresponde a la suma de todos los octetos, incluyendo las cabeceras del protocolo IP y UDP, de todos los paquetes del flujo RTP en el ultimo segundo.[9]

[8] Alarcón Llamas, Ricardo. Título: "Estudio e implementación de mecanismos de calidad de servicio sobre una arquitectura de servicios diferenciados". Universidad Politécnica de Cartagena. Enero 2003.
[9] Tomado de :http://wiki.wireshark.org/RTP_statistics

4. PROTOCOLOS

Dentro de las arquitecturas de redes destinadas a administrar tráfico multimedia se deben tener en cuenta especificaciones que permitan que la calidad, el nivel retardo y el ancho de banda utilizado sean garantizados para que el usuario final logre tener un servicio excelente a nivel de calidad de imagen y sonido.

Para definir los aspectos críticos que la red debe cumplir, se plantea a manera de contextualización el modelo de capas de la suite TCP/IP **(figura 15).**

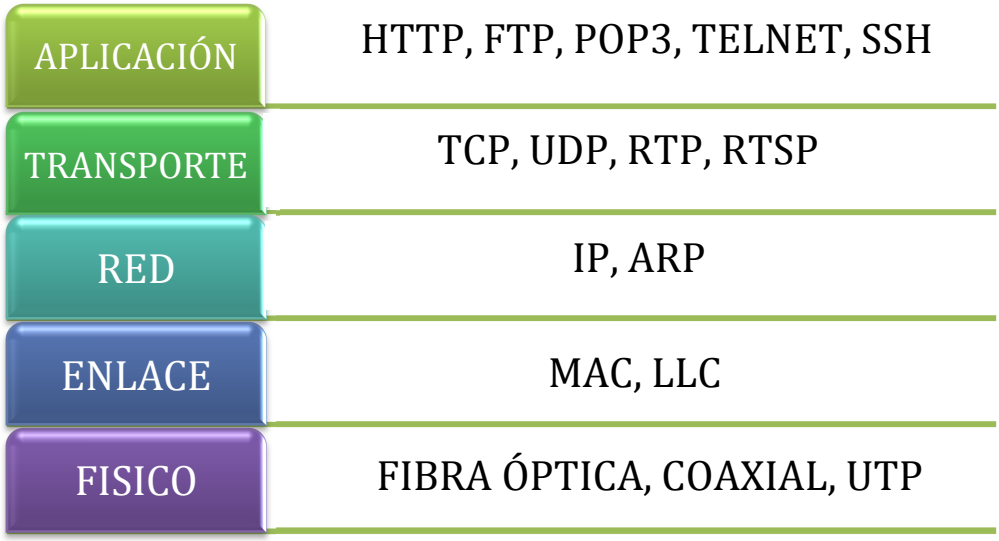

Figura 15 Modelo de capas protocolo IP

Los protocolos que deben garantizar la comunicación extremo-extremo y procurar la fiabilidad de los datos estableciendo conexiones y haciendo control de errores pertenecen a la capa de transporte. Es muy importante tener en cuenta el tipo de información o tráfico que va a transitar por la red para saber sobre qué protocolo de transporte va a viajar la información; en el caso del flujo multimedia en tiempo real es necesario un protocolo no orientado a la conexión que en caso tal halla pérdida de paquetes no reenvíe paquetes que ya hallan sido enviados ya que eso provocaría una pérdida en la calidad de la experiencia del contenido multimedia fuera audio o video el caso que es precisamente lo que al final se busca garantizar. Por excelencia el protocolo que cumple con estos requerimientos es el protocolo UDP.

4.1. UDP

UDP es uno de los más sencillos protocolos de la suite IP. Se utiliza frecuentemente para vídeo y otros datos muy sensibles al tiempo. En este protocolo, el dispositivo de origen puede controlar la rapidez con que los datos pertenecientes a un *stream* fluirán a través de la red. En protocolos como TCP, el cual sí es un protocolo orientado a la conexión la red puede afectar drásticamente la forma de transferencia de datos debido a sus técnicas de corrección de errores y reenvíos de paquetes perdidos.

Para transmisión en tiempo real, UDP es una buena elección como protocolo de transporte, ya que no agrega una sobrecarga innecesaria a los *streamings* que ya cuentan con funciones integradas de corrección de errores, debido a esto, UDP no requiere una comunicación bidireccional, es muy útil para transmisiones satelitales y *multicasting*, donde el tráfico más importante va en una sola dirección.

4.2. RTP

Aunque UDP resultaría útil como protocolo de transporte de contenidos multimedia en tiempo real, existe un método que utiliza las bondades de este protocolo adicionando características que ayudan mucho más a la transmisión de este tipo de tráfico, este protocolo se conoce por RTP (*Real-time Transport Protocol*). Su función principal es que logra multiplexar tráfico en un solo flujo de paquetes sobre UDP facilitando las transmisiones sobre todo a varios destinos (*Multicasting*). Este protocolo tampoco tiene funciones de control de flujo, errores, confirmaciones ni recepción de la información. Solo numera los paquetes de manera consecutiva lo que le permite conocer si ha fallado la entrega de algún paquete durante la transmisión y en caso de existir problemas realiza una interpolación de los datos para intentar reducir los efectos del error en la transmisión. También posee una aplicación muy útil para el envío de contenidos multimedia como lo es el *time-stamping* o marcación del tiempo que permite que la fuente del tráfico asocie una marca de tiempo con la primera muestra de cada paquete consiguiendo que en el cliente se puedan almacenar en un pequeño buffer las muestras e irlas reproduciendo el tiempo exacto después del inicio de la transmisión, esto ayuda a reducir los efectos de la fluctuación como también a sincronizar distintos flujos entre si quitándole algo de peso al trabajo que realizan las políticas de *QoS.*

Sin embargo RTP sí está asociado a un protocolo de control llamado RTCP el cual ofrece información de la integridad de los datos que se están manipulando en la red, proveyendo una forma de realimentación de la calidad del servicio, sin corregir nada[10].

[10] Simpson, Wes Greenfield, Howard. "IPTV and Internet Video", focal press Ed. Elsevier 2 Ed. Chapter 5 pag 67

5. IPTV

Actualmente existen muchas formas de enviar información de tipo multimedia a través de redes IP. En el campo de las señales de video se pueden encontrar distintas ofertas de contenidos y de servicios con diferencias tanto en la infraestructura de red, métodos de difusión, técnicas de configuración. Se conocen desde transmisiones gratuitas, video sobre demanda (VOD, *video on demand*), e IPTV. En términos generales lo que diferencia a todos estos tipos de servicio a nivel técnico es el manejo de *QoS*, la forma de transmitir y el protocolo de transporte que utilicen. **La figura 17** muestra un paralelo entre los distintos tipos de difusión de contenido de video mediante redes ip[11].

Dentro de los conceptos básicos necesarios para hablar de transmisión de IPTV son los conceptos de *Unicasting, Multicasting* y Compresión.

5.1. Unicasting

Difusión de cualquier contenido multimedia desde una fuente específica hasta un cliente específico, es decir, una comunicación punto-punto. Si varios clientes requieren el mismo *stream* el servidor debe crear una difusión por separado para cada receptor. Esto implica que cada receptor tenga que hacer la petición del video directamente a la fuente y este direccionar a cada uno de los clientes el flujo de datos para poder hacerles llegar el video. Normalmente es usado para el flujo de video por internet ya que este no es apto para hacer *multicasting* y los usuarios pueden controlar su *streaming*, es decir, adelantar, retroceder, pausar y repetir.

5.2. Multicasting

Difusión de contenidos simultáneamente desde una fuente hacia varios clientes que los solicitan utilizando protocolos particulares. Estos protocolos logran que sea la red la que replique los flujos y envíe el contenido a los usuarios que lo soliciten; también se requiere que los datos tengan direcciones especiales que los identifiquen como flujo *multicasting*. Los usuarios por su parte le avisan a la red mediante otros protocolos que se quieren unir a la multidifusión. Este tipo de entrega del tráfico multimedia se da unidireccionalmente lo que a nivel básico no da posibilidades a la interactividad entre el usuario y el proveedor de servicios durante las transmisiones, esto se logra mediante otros mecanismos. **La figura 16** da a grandes rasgos y esquemáticamente la diferencia entre *unicasting y multicasting*.

[11] Simpson, Wes Greenfield, Howard. "IPTV and Internet Video", focal press Ed. Elsevier 2 Ed. Pag. 76

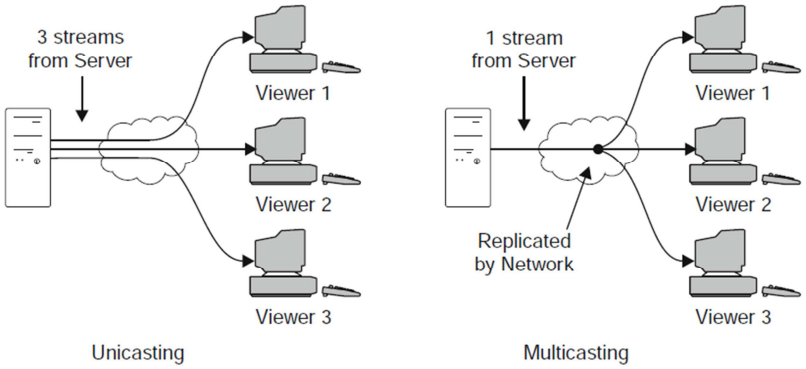

Figura 16 Unicasting Vs Multicasting [7]

Service Attributes	IPTV	IPVOD	Internet TV	Internet Video
Network Type	Private Network	Public Network	Public Network	Public Network
Quality of Service	Managed QoS	Unmanaged QoS	Unmanaged QoS	Unmanaged QoS
Multipoint Method	True Multicasting	Unicasting	Replicated Unicasting	Unicasting
Key Protocols	True Streaming RTP over UDP	Progressive Download+Play	HTTP Streaming; Progressive D+P	HTTP Streaming; Progressive D+P
Viewing Devices	STB with Television	STB with Television or PC	PC, Mobile or Network Appliance	PC, Mobile or Network Appliance
Program Choices	Hundreds of Channels of Continuous TV	Thousands of Discrete Video Files	Thousands of Channels of Continuous TV	Millions of Discrete Video Files
User Experience	Similar to Broadcast or Cable TV	Similar to DVR or VoD	Similar to Web Surfing	Similar to Web Surfing
Channel Change Time	Quick: 1-2 seconds	Reasonable: 5-10 seconds	Slow: 10-20 seconds	Slow: 10-20 seconds (including search time)
Rewind/Fast Forward	No	Yes	No	Yes
Production Values	Professionally Produced	Professionally Produced	Professionally Produced	User Generated
Content Types	Live or Prerecorded	Prerecorded Only	Live or Prerecorded	Prerecorded Only
Program Library	Walled Content Garden	Walled Content Garden	Worldwide Reach; Quality Varies	Viewer Beware
Ownership Rights	Strong, with Digital Rights Management	Strong, Often with DRM	Fairly Strong	Weak or Nonexistent; Frequent Copyright Violations
Revenue Models	Paid by Subscription	Subscription, Fee per Episode or Ads	Often Free or with Advertising	Often Free or with Advertising
Example Providers	Local Telcos, AT&T U-Verse	Netflix, Hulu, CBS.com, ABC.com, Cartoon Network	NASA.tv, Local TV Broadcasters, Mogulus, mobiTV	YouTube, FaceBook

Figura 17 Clasificación de los distintos sistemas de difusión de video

6. Compresión

La demanda de material multimedia en las redes ha aumentado vertiginosamente los últimos años obligando a que los proveedores de servicio hallan tenido la necesidad de buscar soluciones económicas para ofrecerle mayor contenido y **por lo menos** la misma calidad a la que los usuarios están acostumbrados. Para esto, el concepto de compresión y su uso ha sido determinante. De no ser por la aparición de técnicas como el *MP3* (entre otros), no existiría la versatilidad, flexibilidad de almacenar y la portabilidad de los archivos en este caso de audio como se tiene en la actualidad.

La compresión busca básicamente: la mejor administración de los datos suponiendo un uso más eficiente de los recursos de máquina y(o) de red sea cual sea el caso. El avance en los métodos de compresión hoy en día ha logrado que muchos canales de video puedan transmitirse en el mismo espacio por el cual se transmitía un solo canal análogo anteriormente dando esto economía para los proveedores que pueden ofrecer más contenido utilizando la misma infraestructura de red existente. En otras palabras, los flujos comprimidos demandarán menores tasas de bits para su transmisión, es decir, menor ancho de banda que los datos no comprimidos lo cual da mucha flexibilidad para administrar los recursos de red; los archivos comprimidos que tengan que ser guardados en unidades de almacenamiento pesarán mucho menos que los que no lo están, proporcionando esto optimización del espacio.

Existen en la actualidad innumerables técnicas de compresión, pasando por los contenedores o formatos hasta llegar a los llamados códec.

El formato es el programa que se encarga de empacar la información, de hacerla útil para su reproducción. Existen muchos contenedores en la actualidad, dentro los más comunes se encuentran las diferentes versiones de *MPEG, avi, MP4, vob* entre otros, los cuales se usan en distintas aplicaciones.

Por su parte los códec, son los programas que realizan la compresión de descompresión de la información cuando esta va a ser utilizada ya sea para reproducción, almacenamiento o transporte. Dependiendo si es audio o video existen distintos tipos de códec. En la actualidad los más prolíferos en aplicaciones de video son *H.264, MPEG-2, Xvid* para las imágenes y *mp3, mp4a, AAC* entre otros para audio. La **figura 18** muestra diferentes tipos de formatos y códec compatibles entre sí lo cual se debe tener en cuenta a la hora de intentar comprimir archivos.[12]

[12] Simpson, Wes Greenfield, Howard, Op. Chapter 6. Cit Pag 83

Format	VCD	SVCD	DVD	Blu-ray	MKV HD MP4 HD H264 HD WMV HD	AVI DivX XviD WMV	MOV QuickTime	FLV MP4	AVI DV
Resolution NTSC/PAL	352x240 352x288	480x480 480x576	720x480² 720x576²	1920x1080 1280x720	1920x1080² 1280x720²	640x480²	640x480²	640x480²	720x480 720x576
Video Compression	MPEG1	MPEG2	MPEG2, MPEG1	H264 VC1 MPEG2	H264 VC1	DivX, Xvid, MPEG4 ASP, WMV	H264	H264, FLV, VP6, VP7, VP8	DV
Video bitrate	1150Kbit/s	~2000Kbit/s	~7000Kbit/s	~30Mbit/s	~10Mbit/s	~1000Kbit/s	~1000Kbit/s	~700Kbit/s	25Mbit/s
Audio Compression	MP1	MP1	MP1, MP2, AC3, DTS, PCM	DTS-HD, EAC3, TrueHD, AC3, DTS, PCM	AAC, AC3, DTS, WMA	MP3, WMA, OGG, AAC, AC3	MP3, AAC	MP3, AAC	DV
Audio bitrate	224Kbit/s	~224Kbit/s	~448Kbit/s	~448Kbit/s	~448Kbit/s	~128Kbit/s	~128Kbit/s	~64Kbit/s	~1500Kbit/s
Size/min	10 MB/min	10-20 MB/min	30-70 MB/min	50- 150MB/min	50MB/min	4-10 MB/min	4-20 MB/min	4-10 MB/min	216MB/min
Min/74min CD	74min	35-60min	10-20min	4min-10min	10min	60-180min	60-180min	60-180min	3min
Hours/DVD	N/A	N/A	1-2hrs	30min-1hrs	1hrs	7-18hrs	7-18hrs	7-18hrs	20min
Hours/ DualLayerDVD	N/A	N/A	2-4hrs	60min-2hrs	2hrs	13-30hrs	13-30hrs	13-30hrs	37min
Hours/ Blu-ray 25GB	N/A	N/A	8-16hrs	2-4hours	6hours	40-100hrs	40-100hrs	40-100hrs	110min
DVD Player Compatibility	Great	Good	Excellent	None	None	Good	None	None	None
Computer CPU Usage	Low	Low	Low	Very high	Very high	Low	Low	Low	Low
Quality	Bad	Good*	Great*	Superb*	Excellent*	Great*	Great*	Great*	Good

Figura 18 Formatos y códec

7. Caso de estudio

El caso de estudio de esta monografía consiste en implementar una red a través de la cual se curse tráfico multimedia, audio y video, y evaluar el desempeño de las técnicas de encolamiento FIFO, WFQ y CWFQ en el tratamiento de tráfico multimedia.

La **figura 20,** muestra el diagrama de flujo de cómo se va a trabajar para esta monografía.

7.1. Descripción de la red

La red a implementar realiza una comunicación de dos *LAN* remotas a través de un enlace WAN simulado por una conexión entre dos *routers*. Una *LAN* consta de dos servidores de video y la otra de dos clientes a los cuales llegan los *streams* de video. **La figura 19** muestra el esquema gráfico de la red.

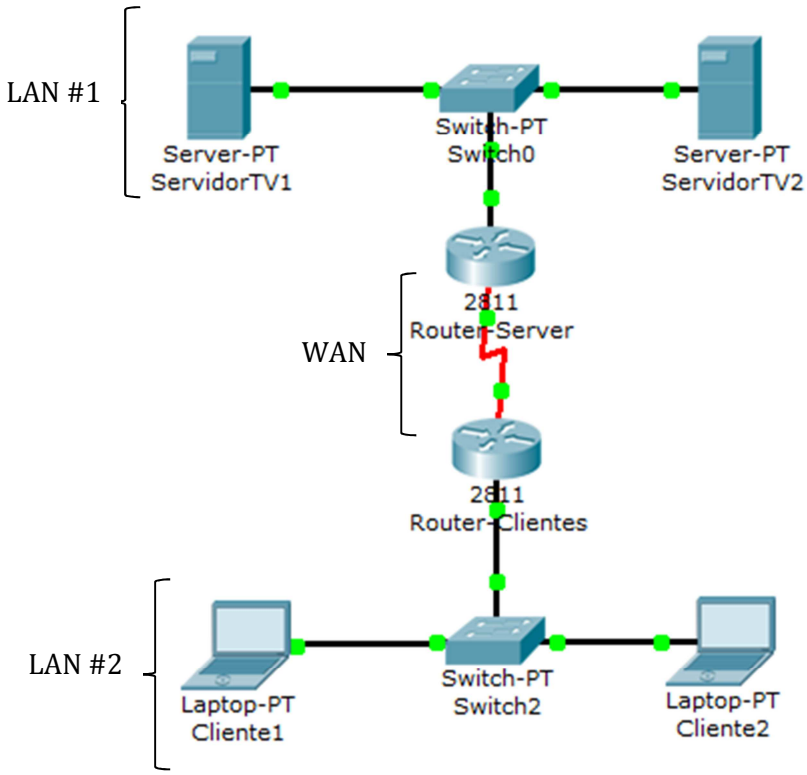

Figura 19 Gráfica de la red a implementar

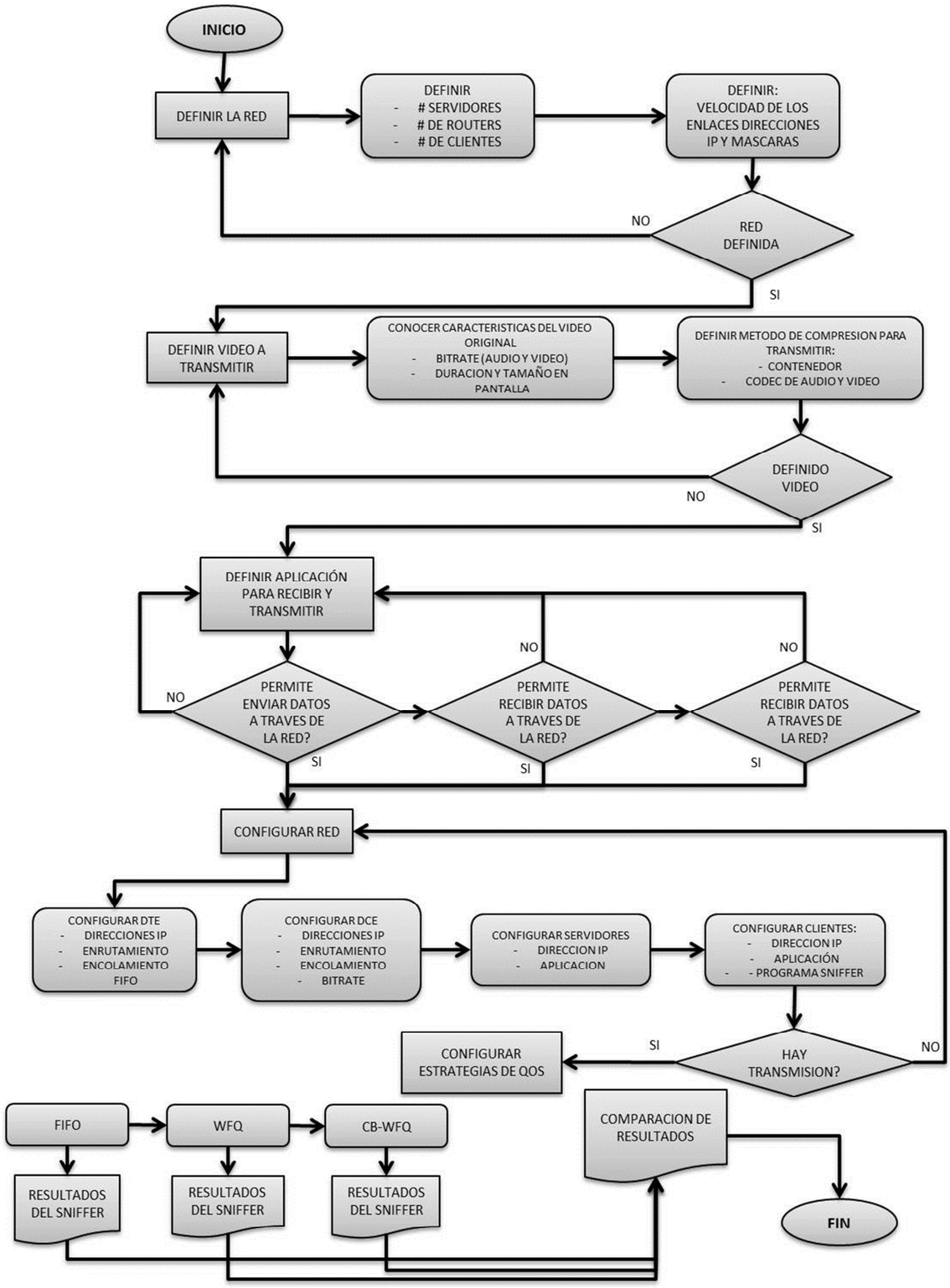

Figura 20 Diagrama de flujo para desarrollo del caso de estudio

La red lleva las siguientes características:

- **LAN #1:**
  - Dirección IP de red: 192.168.1.0
  - Máscara: 24
  - Gateway: Router-Server, 192.168.1.1
  - Dirección IP de ServidorTV1: 192.168.1.2
  - Dirección IP de ServidorTV2: 192.168.1.3
- **LAN #2:**
  - Dirección IP de red: 192.168.2.0
  - Máscara: 24
  - Gateway: Router-Clientes, 192.168.2.1
  - Dirección IP de Cliente1: 192.168.2.2
  - Dirección IP de Cliente2: 192.168.2.3
- **WAN:**
  - Dirección IP de red: 172.16.1.0
  - Máscara: 30
  - Gateway: Router-Server, 172.16.1.1
  - Dirección IP Router-Clientes: 172.16.1.2
  - Velocidad del enlace: T1, 1544kbps

Para poder hacer claramente visible la actuación de las estrategias de *QoS* en el funcionamiento de la red se busca formar un cuello de botella en el enlace *WAN* para forzar congestión en dicha conexión y producir pérdidas de información debido a que no hay disponibilidad de ancho de banda en el canal. Esto se consigue mediante el uso de las interfaces seriales de los ***router*** y una transmisión de video que al enviarse al tiempo desde los dos servidores demande más recursos de los existentes.
Antes de mostrar las configuraciones de los equipos que hacen parte de la red, se va a describir las características de software, del video y compresión del mismo como paso previo a la implementación de la fase física del proyecto.

7.2. Características del video

Para poder transmitir el archivo de video utilizado, este se debe comprimir y empaquetar. Esto requiere de la escogencia de un códec de audio y de video los cuales deben ser lo más óptimos posible en cuestiones de nivel de compresión y de conservación de la calidad original de los archivos. Adicionalmente se debe tener conocimiento de cuanto ancho de banda requiere el contenido para llegar sin errores al destino.

Las características del video son:

- Video:
  - Duración: 1:40:38
  - Alto fotograma: 1280
  - Ancho de fotograma: 720
  - Velocidad en bits (Ancho de banda): 2396 Kbps
  - Fotogramas: 29 fotogramas/s
- Audio:
  - Velocidad en bits: 151 Kbps
  - # de canales: 2 (estéreo)
  - Frecuencia de muestreo: 44,1kHz

7.3. Compresión

Como se menciona en el capítulo 6, la compresión es necesaria e inherente a la hora de hablar de una óptima administración de los recursos de máquinas y redes que cursan contenido multimedia. Saber el tipo de contenedor y códec que se debe utilizar según la necesidad que se tenga es muy importante. Para el caso de este proyecto, la necesidad es que el formato o contenedor en el cual viaje el archivo de video sea hecho para difusión en redes; los *codecs* usados deben tener la facultad de hacer una gran compresión y a la vez que mantengan la mayor calidad posible de la imagen y el video para promover que el ancho de banda requerido por el archivo para su adecuada reproducción no sea demasiado exigente para la red incluso conociendo que para este caso se intenta congestionar el enlace.
Un contenedor o formato apropiado para esta ocasión es *MPEG-TS* ya que es la versión *Transport Stream* del formato *MPEG* el cual está diseñado como dice su nombre para transportar flujos de contenido multimedia a través de redes. Su característica principal es que empaqueta la información de manera que pueda circular más fácilmente por la red.
Los *codecs* escogidos deben ser entonces compatibles con el formato, en esta caso se escogen los siguientes:

- Video: H.264. es un *códec* de alta compresión que permite comprimir video de alta calidad sin ocasionar una gran pérdida de esta en el momento de descomprimir.
- Audio: mp4a. hace parte de la familia de *codecs* AAC o *Advanced Audio Coding* el cual también posee grandes posibilidades de compresión para transmisión a bajas tasas de bits garantizando una gran calidad en el audio.

Conocer qué tipo de archivo se va a transmitir y qué herramientas de compresión son las apropiadas para utilizar, se debe buscar la aplicación que permita hacer la transmisión a través de la red del archivo multimedia.
La aplicación escogida para esto es un software de licencia gratuita llamado VLC **(figura 21)** producido por el grupo y organización sin ánimo de lucro francés ***VideoLAN organization*** de desarrollo de soluciones multimedia de promoción libre y código abierto. *VLC* tiene las bondades de ofrecer transmisiones de video por red con una gran cantidad de opciones de compresión, marcación diferenciada del campo ***DSCP*** para los paquetes enviados entra otras opciones las cual se ajustan adecuadamente a las necesidades de este trabajo.
Se debe instalar y configurar *VLC* en los servidores y en los clientes según su función para enviar o recibir la misma información desde o hacia la red. Las características del archivo que en realidad va a atravesar la red, es decir, después de comprimido y empaquetado son:

- Formato: *MPEG-TS*
- Códec de video: *H.264*, tasa de bits: 800 kbps, alto, ancho y tramas por segundo sin modificar.
- Códec de audio: *mp4a (AAC)*, tasa de bits: 128 kbps, 2 canales, 44,1khz.

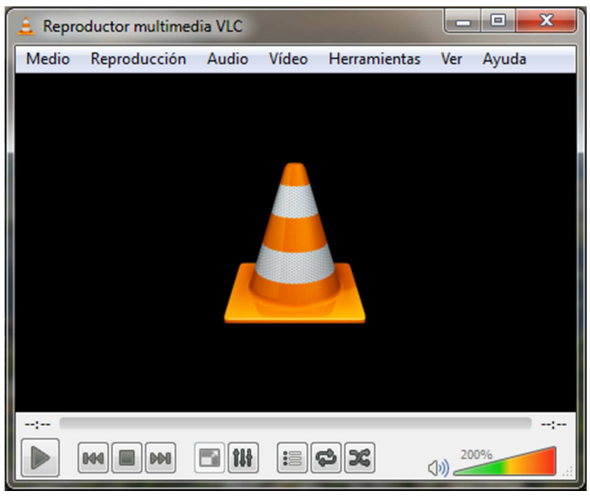

Figura 21 Imágen del software VLC, de la VIDEO LAN Organization

A simple vista se podría decir según las especificaciones del archivo, que el ancho de banda que el contenido necesita para reproducirse son 928 kbps resultantes de la suma de la tasa de bits necesaria de la compresión del video más la de audio, pero en realidad no es así.
Una de las características adicionales de la versión TS del formato MPEG, es que así como parte la información en varios grupos, agrega encabezados tanto a los paquetes de audio como a los de video para proveer el programa de tabla de mapas y el programa de referencia de reloj. Esto le da un agregado en la tasa de bits de 45kbps adicionales a los 928kbps del contenido, adicionalmente se tienen en cuenta 380 kbps que demandará el encabezado de encapsulamiento IP que también llevan los datos. Según [7], el ancho de banda que requerirá el video para poder ser transportado por la red se puede calcular de la siguiente manera:

$$(Bitrate\ video) * 1{,}038 + (bitrate\ audio) * 1{,}093 + 45kbps + 380\ kbps = Bitrate\ minimo$$

Basado en la suma mostrada, el archivo que se va a transmitir necesitará al menos:

$$(800kbps) * 1{,}038 + (128kbps) * 1{,}093 + 45kbps + 380\ kbps = 1395\ kbps$$

7.4. Configuración y preparación de la red

Recapitulando, el ancho de banda del enlace WAN tiene es igual al de un enlace T1, es decir, 1544kbps y cada servidor transmite el mismo archivo de video. Debido al ancho de banda que requiere cada transmisión de los servidores, 1544kbps es un ancho de banda muy angosto para poder transmitir al tiempo y sin errores los dos archivos que cada servidor envía. Es aquí donde en aras de solucionar un problema de congestión se usan técnicas de *QoS* que puedan identificar qué paquetes presenta una marca prioritaria sobre otras para que sean estos los que se reproduzcan en los clientes sin inconvenientes, con alta disponibilidad y calidad y así comparar el desempeño de cada técnica

7.4.1. Estrategias QoS

Las estrategias a comparar son: FIFO (*first in-first out*), WFQ (*Weighted Flow based queuing*) y CB-WFQ (*class based – weighted flow based queuing*).
La red tiene ciertas configuraciones que se utilizan como premisas base, es decir, un ambiente unificado para realizar todos los análisis: ServidorTV2 será el computador en el cual *VLC* está configurado para marcar los paquetes en el capo *DSCP* con una marca 'ef' o *expedited forwarding* la cual por defecto es la marca con mayor prioridad para las políticas Diffserv; las técnicas de *QoS* son implementadas solamente en el llamado *Router-server* mientras que en el **Router-clientes** está configurado siempre un encolamiento FIFO para que este no realice ningún tratamiento adicional a los paquetes que ya el **Router-server** es el elegido para realizar dichas tareas.

Para cada tipo de encolamiento se toman varias capturas en las **NICs** de los clientes mediante un programa tipo *sniffer* capaz de arrojar la información de los parámetros de medida para calificar los servicios de QoS, en este software se visualizan parámetros como pérdida de paquetes, *jitter*, OWD, y el *Through-put*.
Como es sabido, las estrategias de *QoS* pueden ser Intserv o Diffserv. En este caso, se utiliza *DiffServ* porque permite al administrador de la red tener un control más dinámico de los recursos de red que se le asignan a cada servicio. Básicamente, esto se basa en el valor que tengan los paquetes en su campo *TOS o DSCP* (dependiendo de cuantos bits se tomen, 6 u 8 respectivamente).

7.4.2. Configuración VLM

Para esto VLC es una herramienta muy adecuada ya que dentro de sus opciones de configuración trae la posibilidad de darle el valor decimal para servicios diferenciados **(figura 21)**. Para el **ServidorTV1**, no se modifica este valor, es decir, se deja en cero y para el **ServidorTV2** se le va a configurar el valor de ef *expedited forwarding* en su valor decimal el cual es: 184, obtenido de la conversión del número de 8 bits "10111000" que se configura en el campo *DSCP* (ver nota)[13].

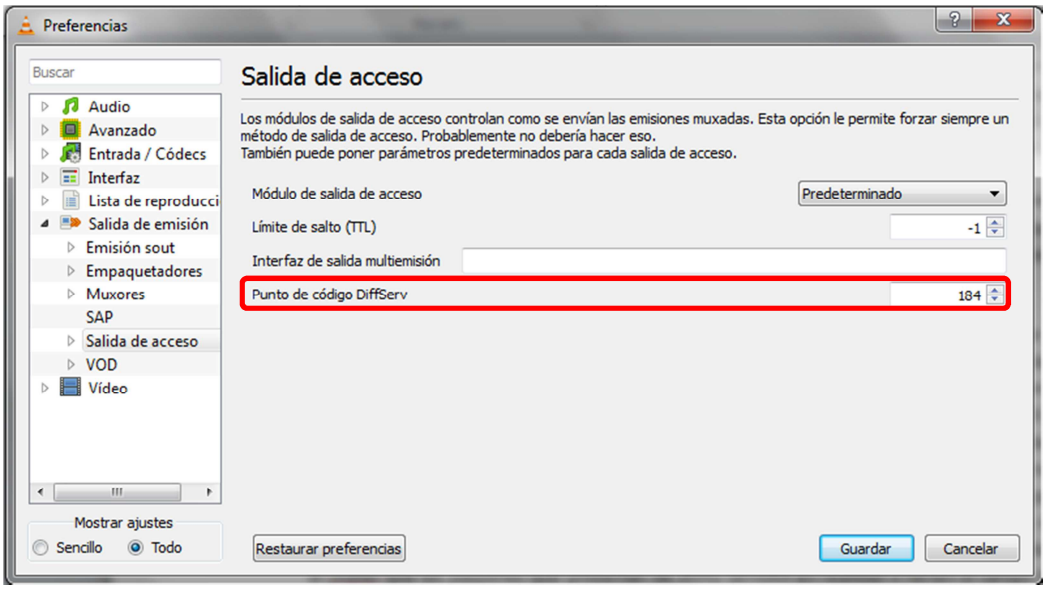

Figura 22 Punto de código DiffServ en VLC

[13] ***Nota:*** *se hicieron pruebas con VLC como fuente de transmisión tanto en Windows 7, Windows xp y Ubuntu. Solo en Ubuntu VLC marcó correctamente los paquetes, en Windows xp la transmisión funciona pero no marcó y en Windows 7, el programa no logró realizar la difusión. El servidor que tiene marca por defecto, se deja así porque maneja Windows xp.*

VLC contiene una función llamada VLM que permite realizar difusiones a través de redes. Esta función es en la que se configuran los contenidos que se van a transmitir, el tipo de compresión, el protocolo a través del cual van a viajar y las direcciones IP que van a recibir el volcado de información **(figuras 23 y 24).**

Teniendo ya todas las premisas de funcionamiento y los resultados que se desean, se prosigue con la configuración de los equipos. A continuación se presenta la forma como se configuran los equipos para conformar la red (los enlaces entre todos los elementos que la conforman).

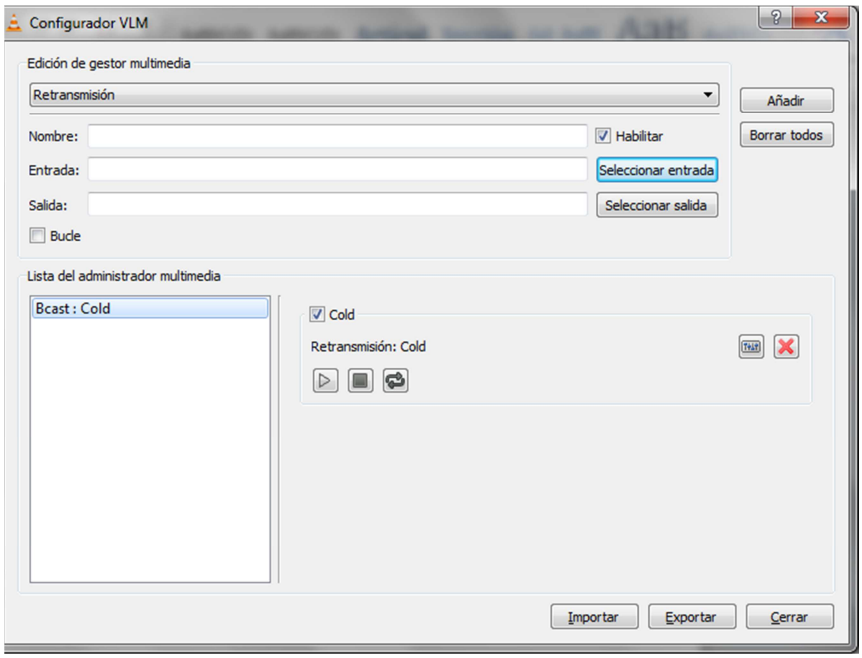

Figura 23 Configuración VLM

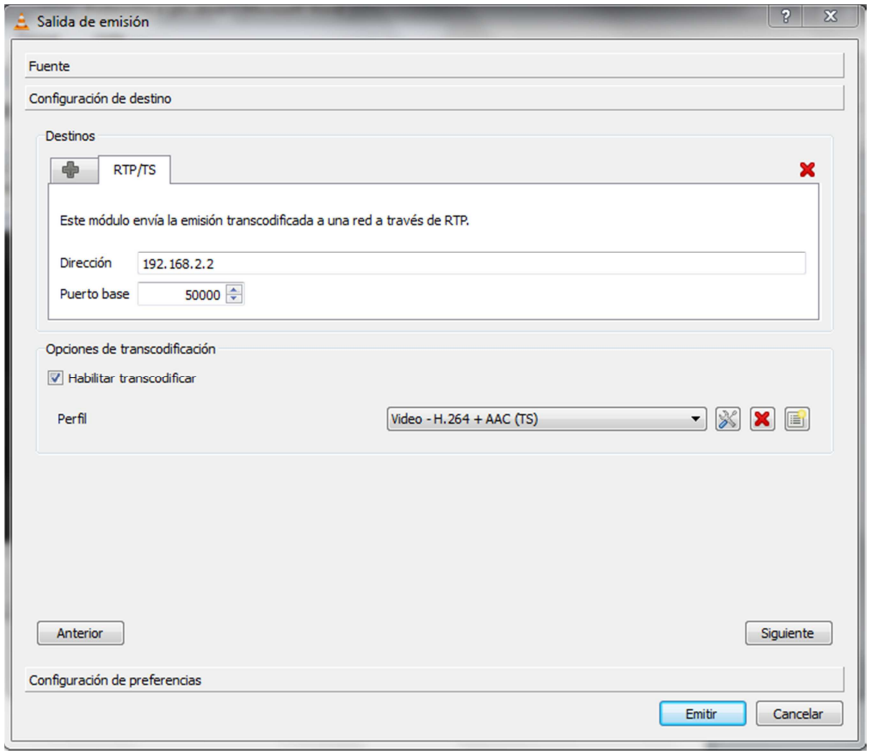

Figura 24 Configuración VLM

7.4.3. Configuración VLC en los clientes

Así como se configura VLC para transmitir a través de la red se debe conocer cómo recibir en los clientes el ***streaming*** que llega a la ***NIC.*** La **figura 25** muestra la opción de reproducir volcado de red que donde se especifica la dirección ip, el protocolo y el puerto del cliente que recibe la información.

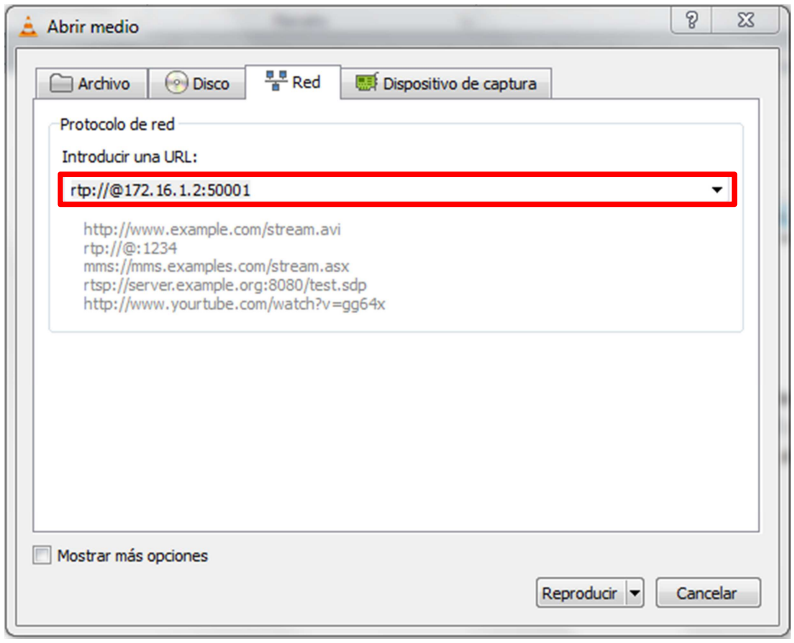

Figura 25 Configuración de VLC para recibir transmisión

7.4.4. FIFO

Primero se va a configurar el **Router-cliente**, este será el que sea el *DTE* de la conexión:

Modelo: Cisco 2811
IOS: Advanced Enterprise
Router-cliente> enable
Router-cliente # config terminal
Router-cliente(config)# interface serial 0/3/0
Router-cliente(config-if)# ip address 172.16.1.2 255.255.255.252
Router-cliente(config-if)# no fair-queue
Router-cliente(config-if)# no shutdown
Router-cliente(config-if)# exit
Router-cliente(config)# interface FastEthernet 0/0
Router-cliente(config-if)# ip address 192.168.2.1 255.255.255.0
Router-cliente(config-if)# no shutdown
Router-cliente(config-if)# exit
Router-cliente(config)# router rip
Router-cliente(config-router)# version 2
Router-cliente(config-router)# network 192.168.2.0
Router-cliente(config-router)# network 172.16.1.0
Router-cliente(config-router)# end
Router-cliente# write

Configuración del **Router-Server**, este será el DCE de la conexión:
Modelo: Cisco 2811
IOS: Advanced Enterprise

```
Router-server> enable
Router-server# config terminal
Router-server(config)#ip cef
Router-server(config)#ip multicast-routing
Router-server(config)# interface FastEthernet 0/0
Router-server(config-if)# ip address 192.168.1.1  255.255.255.0
Router-server(config-if)# no shutdown
Router-server(config-if)#exit
Router-server(config)# interface serial  0/3/0
Router-server(config-if)# ip address 172.16.1.1 255.255.255.252
Router-server(config-if)# clock rate 2000000
Router-server(config-if)# max-reserved-bandwidth 100
Router-server(config-if)# no fair-queue
Router-server(config-if)# no shutdown
Router-server(config-if)# exit
Router-server(config)# router rip
Router-server(config-router)# version 2
Router-server(config-router)# network 192.168.1.0
Router-server(config-router)# network 172.16.1.0
Router-server(config-router)# end
Router-server# write
```

Para enrutar se utiliza el protocolo ***RIP versión 2***. Por defecto el *router* en la interfaz serial solo permite utilizar el 75% del ancho de banda total por ello puede que en un principio el sistema diga que solo hay acceso a 1158kbps disponibles de ancho de banda, para lograr disponer de los 1544kbps nominales de la interfaz, se debe utilizar el comando *"max-reserved-bandwidth [percent]".* Para la configuración del *clock-rate* hay que tener en cuenta el tipo de tráfico que se va a cursar y que esto implica cierto tráfico de control adicional sin importar que el protocolo como tal de la transmisión sea RTP o UDP los cuales no son orientados a conexión, por tanto se configura un *clock-rate* de 2'000.000bps.
Con estas configuraciones, sumadas a la asignación de las direcciones IP antes mostradas de cada equipo terminal, todos los equipos tienen enlace entre sí y se puede hacer un **PING** desde cualquier punto de la red hasta cualquier otro. Adicionalmente hay que mencionar que por defecto las interfaces seriales de estos *routers* vienen configuradas para realizar encolamiento tipo ***WFQ***. En principio se les deshabilita esta característica dejando la red funcionando sin encolamiento, es decir, ***FIFO***. Con esta configuración se inician las pruebas del siguiente capítulo.
En este punto de la configuración la **figura 26** muestra las características de la red.

Para la configuración que se mostró anteriormente, los *routers* simplemente dejan pasar todos los paquetes que lleguen a sus terminales ya que la configuración hecha no tiene algoritmos de encolamiento, esto es, método ***FIFO***. A partir de aquí se inician las pruebas con la transmisión mediante ***VLC*** del video caracterizado en el apartado anterior. Las demás pruebas se realizan configurando un encolamiento de tipo ***WFQ y CB-WFQ.***

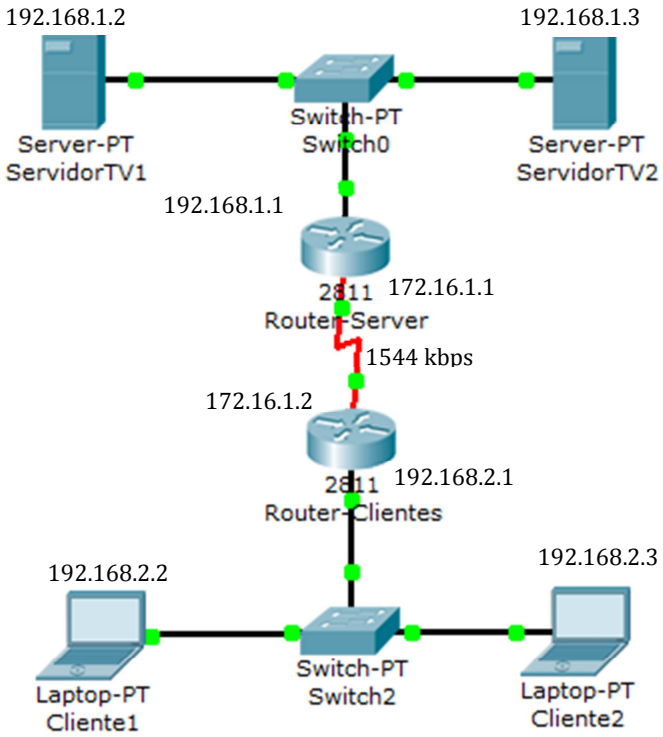

Figura 26 Red configurada

La información de los ***routers*** utilizados se encuentra en el enlace mostrado en el capítulo de Anexos.

7.4.5. WFQ

Esta configuración viene por defecto en las interfaces serial de los ***routers*** que se están utilizando, por tanto solamente hay que reactivar esta configuración y el *router* la aplicará. Recordando que *WFQ* presta atención al campo *DSCP* y ya tiene definidas una gestión de ancho de banda y de encolamiento por defecto. Se espera que los paquetes que vengan marcados tengan un trato prioritario sobre los que no.

La configuración para el router es la siguiente:
Router-server> enable
Router-server# config terminal
Router-server(config)# interface serial 0/3/0
Router-server(config-if)# fair-queue
Router-server(config-if)# end

Para observar el tipo de encolamiento que cada interfaz tiene configurada se puede utilizar en el modo de usuario el comando *"show interface*" y aparecerá la información detallada de cada interfaz que tenga el *router,* su ancho de banda, su tipo de mecanismo de encolamiento entre otros datos.

7.4.6. CB-WFQ Y LLQ

Para este tipo de encolamiento se requiere utilizar listas de control de acceso, clases y políticas.

- Listas de control de acceso (ACL): Se configura una lista de acceso que filtre el tráfico IP que llegue al *router* con una marca 'ef' en el campo DSCP.
- Clases: Se configurarán dos clases, **IPTV** y **GOLD**. En **IPTV** se cargará la lista de acceso y en **GOLD** el tráfico **IP** en general.
- Políticas: Se configurará una sola política a la salida de la interfaz que se interconecta con la *WAN* en la que se gestionará el ancho de banda y el encolamiento. La política será nombrada como ***POLITICA-QoS.***

```
Router-server> enable
Router-server# config terminal
Router-server(config)# access-list 100 permit ip any any dscp ef
Router-server(config)# class-map IPTV
Router-server(config-cmap)# match access-group 100
Router-server(config-cmap)#exit
Router-server(config)# class-map GOLD
Router-server(config-cmap)# match protocol ip
Router-server(config-cmap)# exit
Router-server(config)# policy-map POLITICA-QoS
Router-server(config-pmap)# class IPTV
Router-server(config-pmap-c)# priority 1400
Router-server(config-pmap-c)# exit
Router-server(config-pmap)# class GOLD
Router-server(config-pmap-c)# bandwidth 120
Router-server(config-pmap-c)# random-detect
Router-server(config-pmap-c)# exit
Router-server(config-pmap)# class class-default
Router-server(config-pmap-c)# fair-queue 16
Router-server(config-pmap-c)# queue-limit 20
Router-server(config-pmap-c)# random-detect
Router-server(config-pmap-c)#end
Router-server# config terminal
Router-server(config)# interface serial 0/3/0
Router-server(config-if)# no fair-queue
Router-server(config-if)# service-policy output POLITICA-QoS
Router-server(config-if)# end
```

Primero se crea la ACL donde se filtra el tráfico que llegue con marca 'ef', luego se crean las clases de servicio necesarias donde en una de ellas *(IPTV)* se asignan los paquetes filtrados por la ACL y en la otra se va a admitir todo el tráfico IP (*GOLD*). Después de configurar las clases se establece la política de encolamiento (POLITICA-QoS), donde la clase IPTV que es a la cual se pretende dar una prioridad máxima se le asigna un ancho de banda estricto de 1400kbps (comando '***priority***') mientras que a la clase GOLD se le configura un canal dedicado con menos prioridad de 120kbps (comando '***bandwidth***') y un descarte inteligente de paquetes WRED (comando ***'random-detect'***). La clase por defecto (***class-default***) que existe en el *router* dejará pasar el tráfico restante, con un encolamiento ***WFQ*** limitado y descarte inteligente WRED (comando *'random-detect'*). Para esta última estrategia el esquema de la red quedaría como en la **figura 27.**

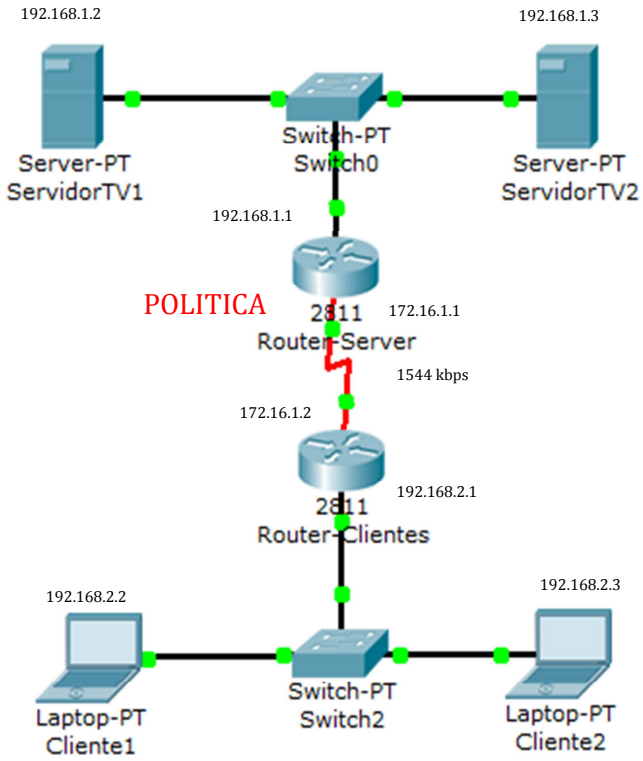

Figura 27 Red bajo configuración de política CB-WFQ

8. RESULTADOS

8.1. FIFO

Para este tipo de encolamiento se realizan dos pruebas para mostrar su funcionamiento. Se reproduce el video desde un solo servidor para que no exista congestión en la transmisión. Luego se transmiten los dos videos con uno de ellos marcado en el campo DSCP con valor 'EF'.

8.1.1. Prueba con un solo cliente

En esta prueba se reproduce un solo video el cual debe transmitirse sin problemas ya que no se está congestionando la red. Los resultados se obtienen de una captura del tráfico RTP a través de la NIC del cliente donde se está reproduciendo el video con el software ***sniffer Wireshark v1.8.2*** durante dos (2) minutos de transmisión para evaluar los parámetros que indican la calidad de la transmisión como lo son el ***Jitter***, el caudal, cantidad de paquetes perdidos y el ***OWD***. Adicional se hace una evaluación cualitativa de la calidad de la imagen y el audio que se percibían en VLC.

A continuación el resultado de la captura.

La **figura 28** muestra las características de la captura, la cantidad de paquetes RTP que transitaron por la interfaz de red del cliente en 119,44s. Además muestra los errores y la cantidad de paquetes que se perdieron durante este intervalo de reproducción.

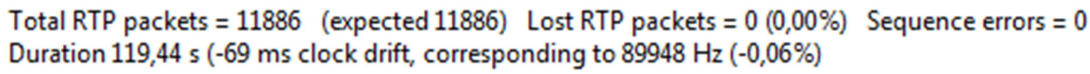

Figura 28 Resultado de la captura usando FIFO y un solo cliente

Como se ve claramente, al no existir congestión en la red, no existen errores de secuencia en la transmisión ni pérdida de paquetes.

La **figura 29**, muestra el comportamiento de la magnitud del ***Jitter*** durante la transmisión y la **tabla 1** los valores pico y promedio.

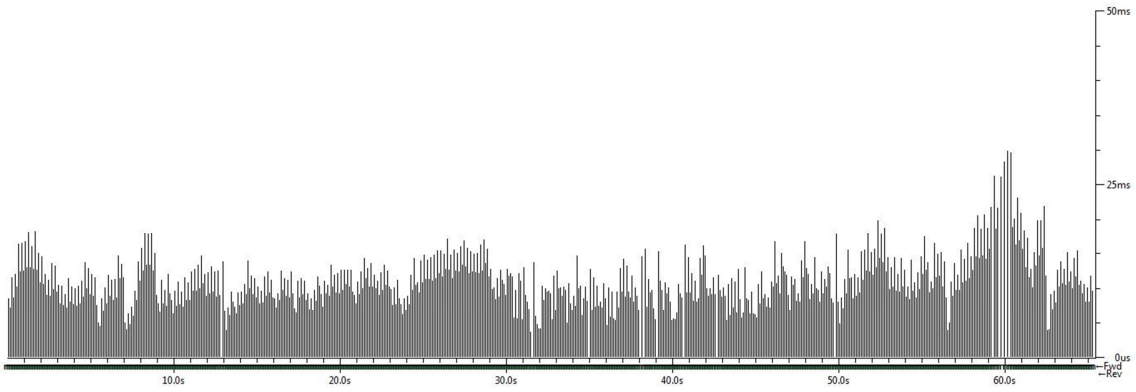

Figura 29 Jitter, FIFO un solo cliente

Jitter	Max(ms)	Min(ms)	Promedio(ms)
Valor	25,29	0,00	8,42

Tabla 1 Valores pico y promedio de Jitter, prueba 1

La **figura 30** muestra la magnitud durante la reproducción del *OWD*. Y la **tabla 2**, sus valores pico y promedio.

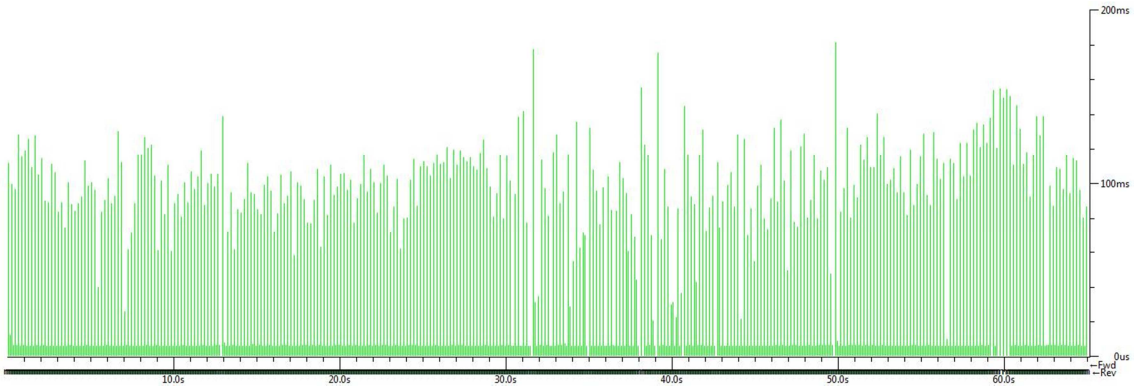

Figura 30 OWD, prueba FIFO con un solo cliente

OWD	Max	Min	Promedio
Valor	180,98	0,00	10,05

Tabla 2 Valores pico y promedio prueba FIFO con un solo cliente

Por último se grafican los valores del caudal durante la transmisión, **Figura 31** y **tabla 3**.

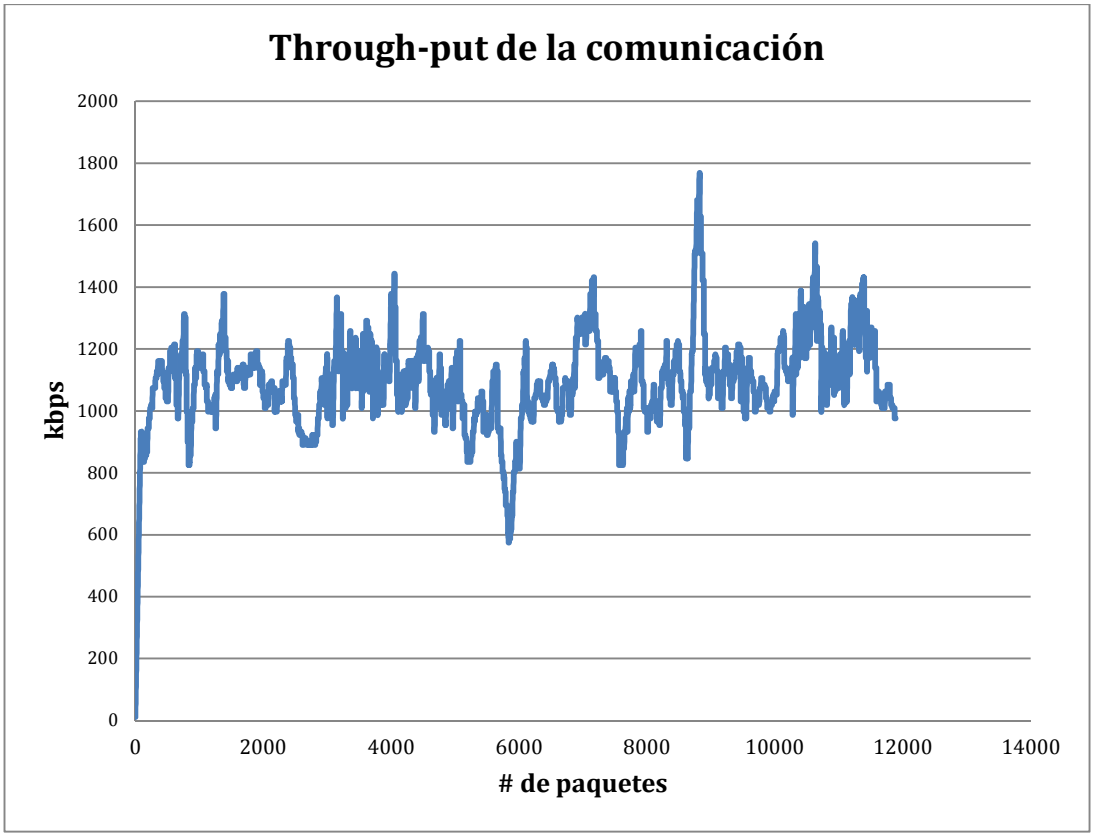

Figura 31 Through-put en prueba FIFO, un solo cliente

Through-put	Max	Min	Promedio
Valor	1768,22	10,85	1093,69

Tabla 3 Valores promedio y picos del caudal presentando en prueba FIFO con un solo cliente

Evaluación cualitativa:

La calidad de la imagen y del sonido era buena, sincronizada y sin errores. No se distorsiono el video ni el sonido en ningún momento ni se distorsionaron pixeles.

8.1.2. FIFO con dos clientes

Luego de observar que mientras al no haber congestión en la red no es totalmente necesaria la utilización de técnicas específicas de encolamiento, se prosigue con convertir el enlace *WAN* en un cuello de botella al reproducir el mismo video pero desde los dos servidores utilizando la misma configuración en el ***router,*** es decir, FIFO. Cabe recordar que uno de los dos servidores está enviando los paquetes con marca '**EF**' en el campo *DSCP* y el otro con el valor por defecto que es cero. La captura del tráfico a través de la *NIC* también fue de dos minutos.

Primero se muestran los datos obtenidos en el cliente donde llegan los paquetes marcados y luego los del cliente sin marca.

La **figura 32** muestra las características de la prueba y la cantidad de paquetes perdidos en el cliente donde arriban los paquetes con marca '***EF***'.

Total RTP packets = 12245 (expected 12245) Lost RTP packets = 556 (4,54%) Sequence errors = 206
Duration 120,18 s (501 ms clock drift, corresponding to 90375 Hz (+0,42%)

Figura 32 Resultado de la captura usando FIFO en el cliente que recibe paquetes marcados

La **figura 33** muestra la gráfica de magnitud del ***Jitter*** y la **tabla 4** los valores picos y promedio del mismo parámetro.

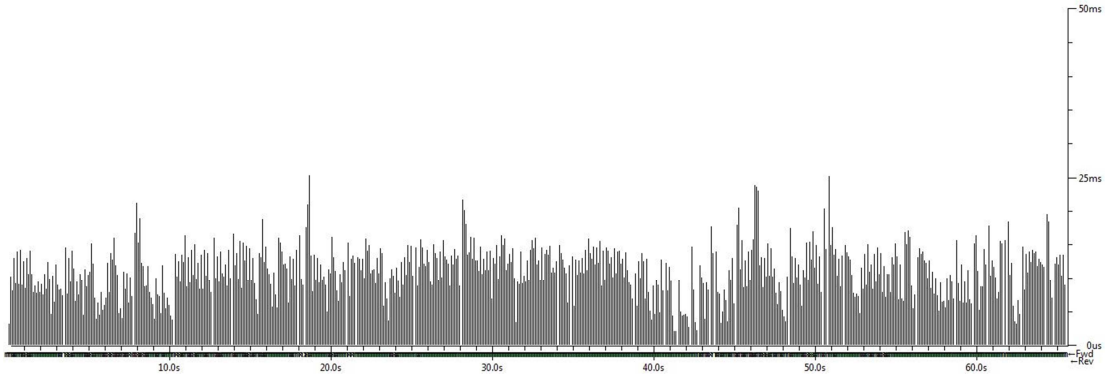

Figura 33 Comportamiento del Jitter en el cliente donde arriban los paquetes marcados

Jitter	Max(ms)	Min(ms)	Promedio(ms)
Valor	29,82	0,00	8,68

Tabla 4 Valores pico y promedio de Jitter en Cliente con paquetes marcados usando FIFO

La **figura 34** y la **tabla 5** muestran los resultados para el *OWD.*

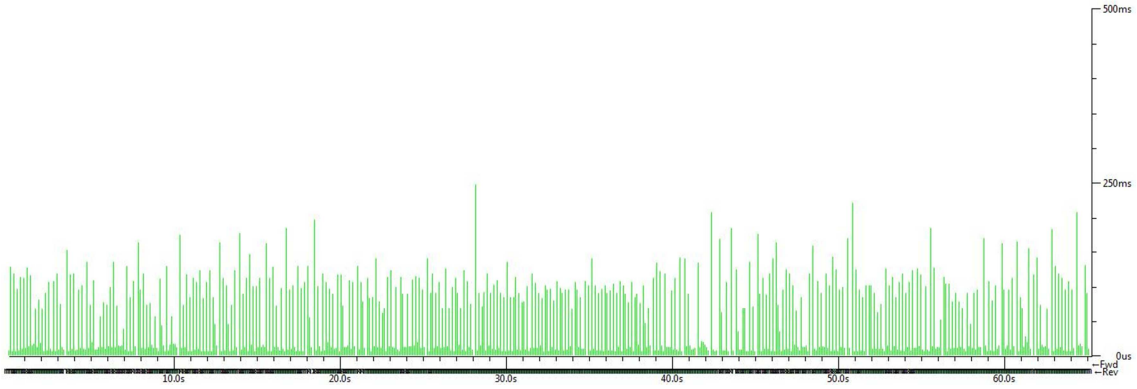

Figura 34 OWD en cliente donde llegan los paquetes marcados usando FIFO

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	289,11	0,00	10,28

Tabla 5 Valores pico y promedio del OWD en el cliente con paquetes marcados usando FIFO

El caudal que hubo durante la transmisión se muestra en la **figura 35** y la **tabla 6**.

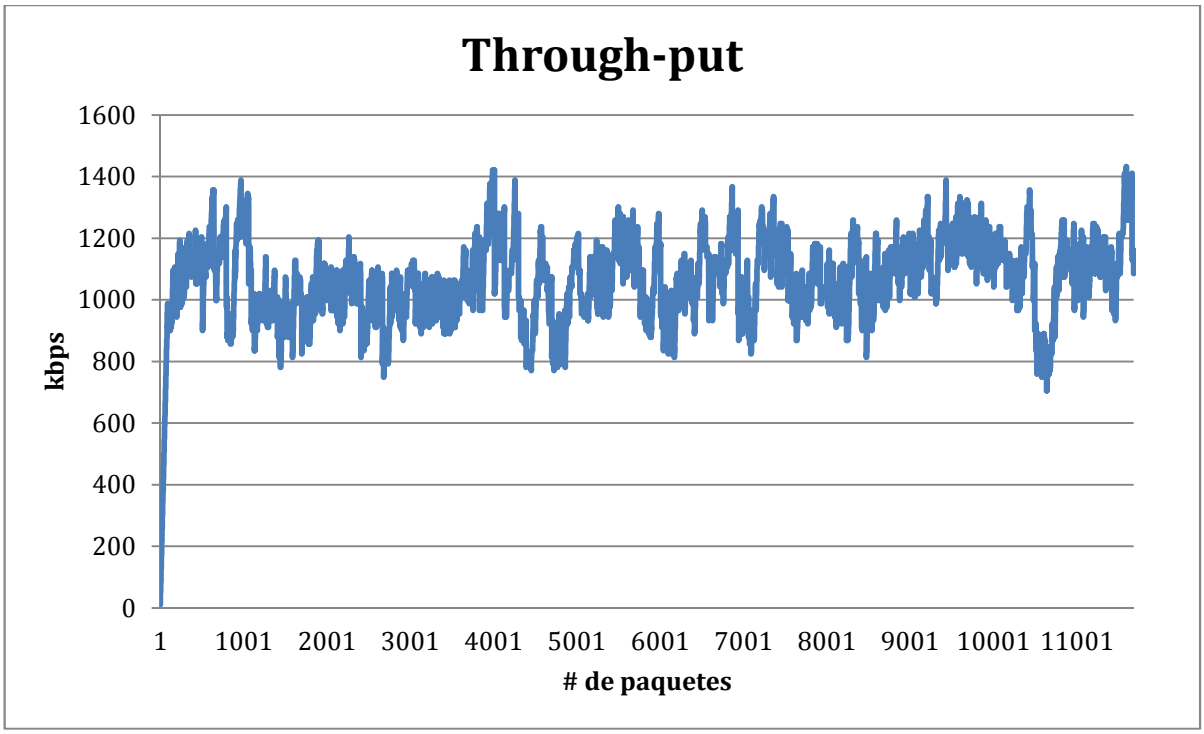

Figura 35, Through-put en la comunicación entre el servidor que marca los paquetes y el cliente, usando FIFO

Through-put	Max(ms)	Min(ms)	Promedio(ms)
Valor	1421	11	1052

Tabla 6 Valores pico y promedio del Through-put en el enlace con paquetes marcados usando FIFO

Ahora se muestran los resultados en el cliente donde llegan los paquetes con el campo *DSCP* en cero. La **figura 36** muestra las generalidades de la captura.

Total RTP packets = 9152 (expected 9152) Lost RTP packets =733(8,83%) Sequence errors = 320
Duration 119,77 s (30 ms clock drift, corresponding to 90023 Hz (+0,03%)

Figura 36 Captura en cliente con paquetes sin marcar usando FIFO

La gráfica de comportamiento y los valores pico y promedios del ***Jitter*** aparecen en la **figura 37** y la **tabla 7.**

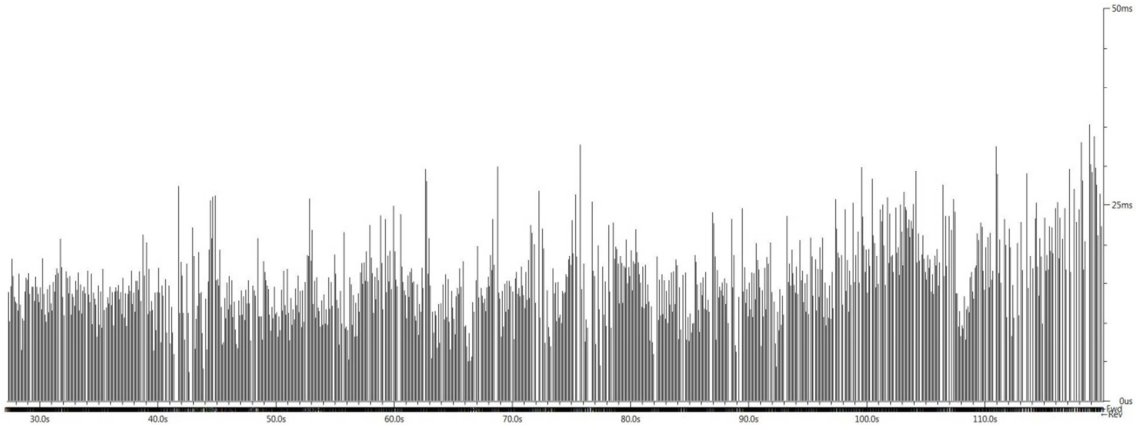

Figura 37 Jitter en cliente con paquetes sin marcar usando FIFO

Jitter	Max(ms)	Min(ms)	Promedio(ms)
Valor	35,19	0,00	12,46

Tabla 7 Valores pico y promedio de Jitter en cliente con paquetes sin marcar usando FIFO

Los resultados de la medida de OWD aparecen en la **figura 38** y la **tabla 8**.

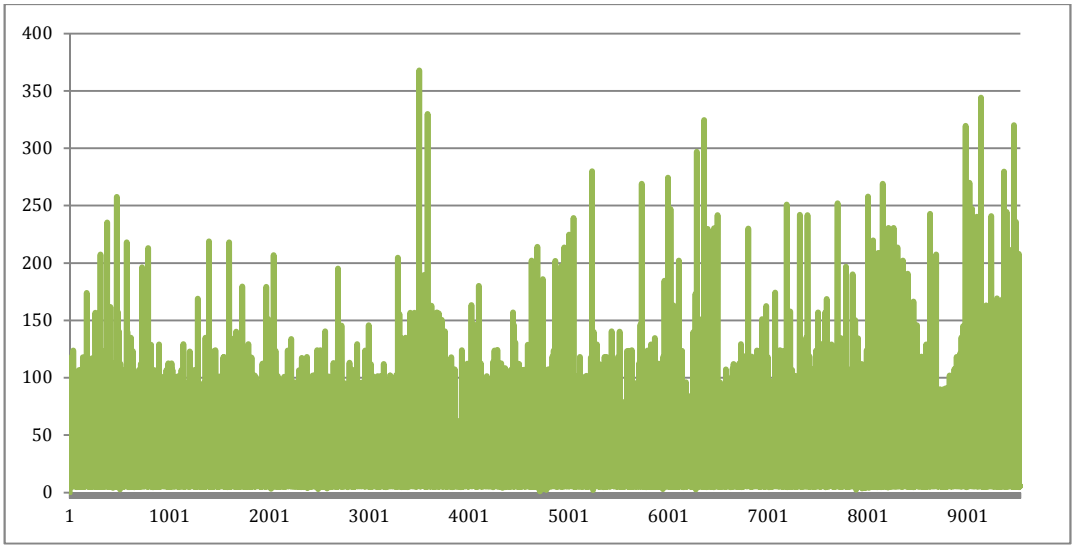

Figura 38 OWD en cliente con paquetes sin marca usando FIFO

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	367,90	0,00	12,59

Tabla 8 Valores picos y promedio de OWD en cliente con paquetes sin marca usando FIFO

La **figura 39** y la **tabla 9** muestran el caudal en la conversación entre el servidor y el cliente.

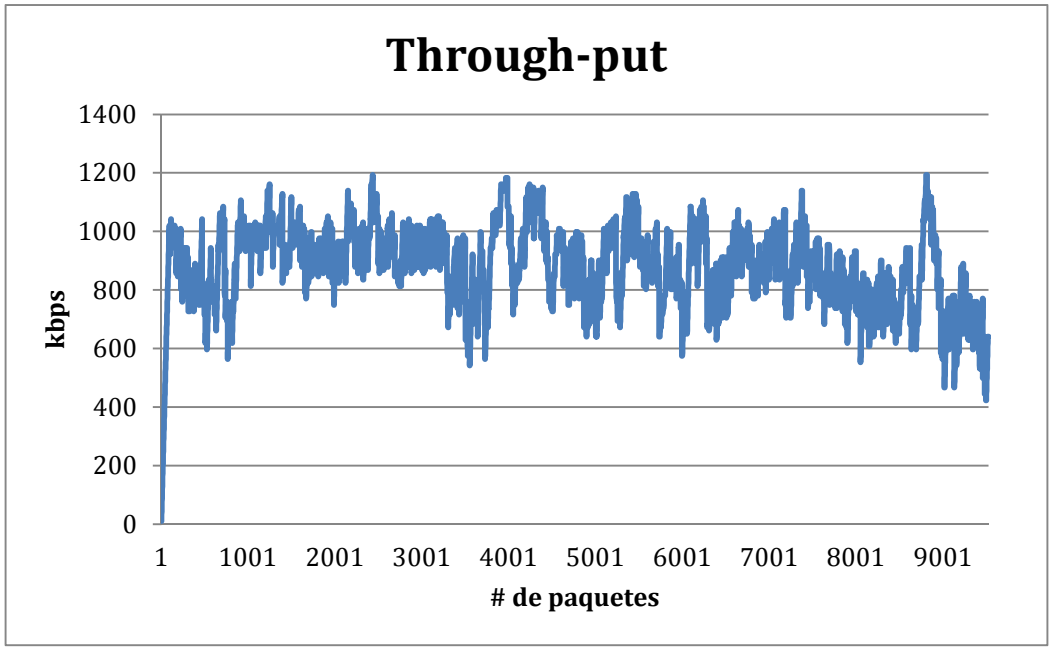

Figura 39 Through-put en cliente con paquetes sin marca usando FIFO

Through-put	Max(ms)	Min(ms)	Promedio(ms)
Valor	1193	11	876

Tabla 9 Valores pico y promedio de through-put para cliente con paquetes sin marca usando FIFO

Evaluación cualitativa

En esta prueba los videos presentan muchos errores tanto en las imágenes como en el audio, se congelan y en el caso del video se distorsiona constantemente la imagen en los dos clientes, siendo esto prueba de que existe congestión en la red y los paquetes compiten por ese recurso escaso en que se convierte el ancho de banda. Los ***routers*** no están utilizando ninguna estrategia de encolamiento ni de manejo de congestión sino que dejan pasar simplemente todo dato que llega a sus interfaces.

8.2. WFQ

Para esta segunda prueba se usa el tipo de encolamiento por defecto que viene configurado en la interfaz serial de los ***routers*** utilizados. Como es normal y se nota en las pruebas con estrategia FIFO, mientras no exista congestión en la red, los paquetes se transmiten sin contratiempos y la calidad de la experiencia (***QoE***) para los usuarios finales es la esperada, por tanto para este caso se realiza directamente la prueba congestionando la red y verificando qué sucede con cada transmisión. La captura en la ***NIC*** de cada cliente es de dos minutos de reproducción constante de los videos. A continuación los resultados.

8.2.1. Resultados de tráfico con marcado 'EF'

En la figura 38 se muestran las características de la captura.

Total RTP packets = 11573 (expected 11573) Lost RTP packets = 0 (0,00%) Sequence errors = 0
Duration 119,74 s (-373 ms clock drift, corresponding to 89720 Hz (-0,31%)

Figura 40 Caracterísiticas de la captura en el cliente con paquetes marcados usando WFQ

La **figura 41** y la **tabla 10**, muestran el comportamiento del ***Jitter*** a lo largo de la captura.

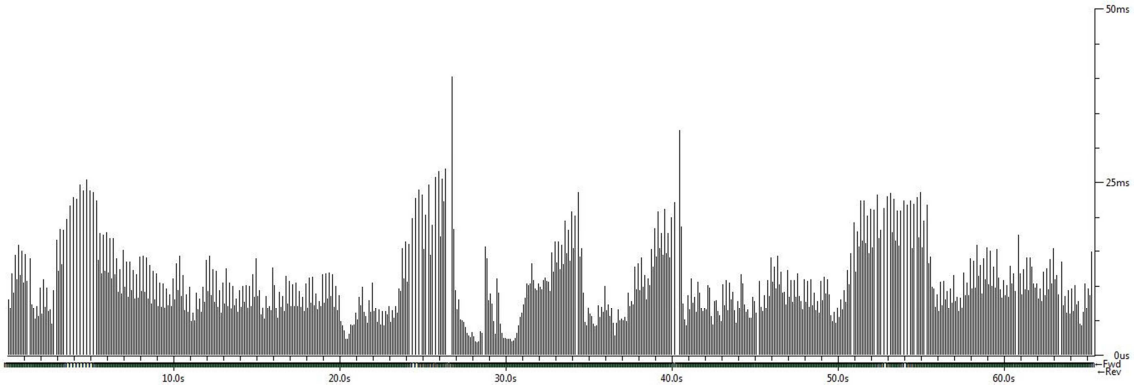

Figura 41 Jiiter en cliente con paquetes marcados usando WFQ

Jitter	Max(ms)	Min(ms)	Promedio(ms)
Valor	327,04	0,00	10,19

Tabla 10 Valores pico y promedio de Jitter en cliente con paquetes marcados usando WFQ

La toma de muestras del OWD se muestra en la **figura 42** y la **tabla 11**

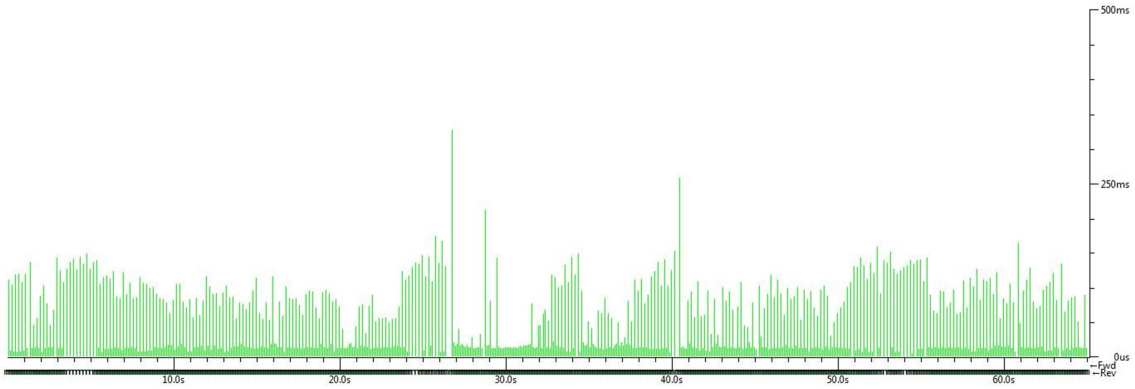

Figura 42 OWD en cliente con paquetes marcados usando WFQ

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	327,04	0,00	10,19

Tabla 11Valores pico y promedio de OWD en cliente con paquetes marcados usando WFQ

La **figura 43** y la **tabla 12** muestran el caudal en la conversación entre el servidor y el cliente.

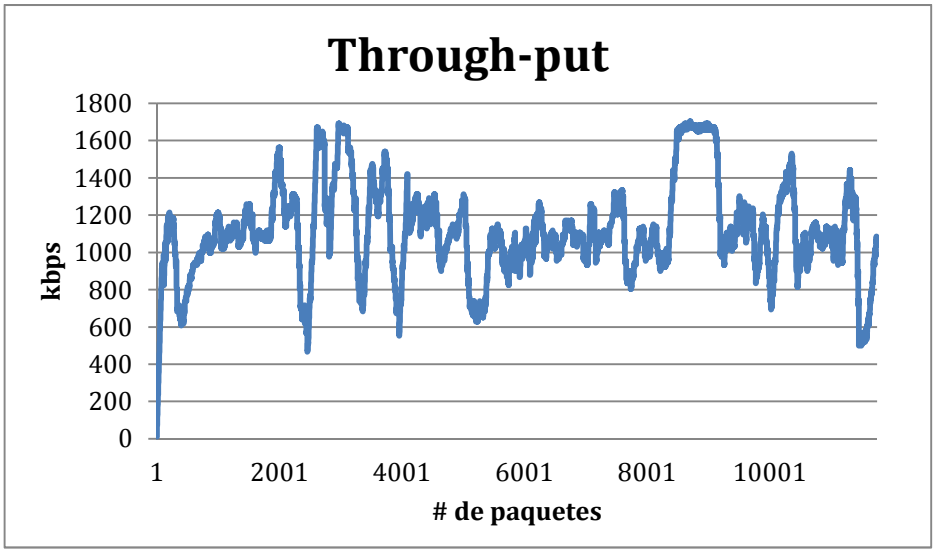

Figura 43 Through-put en cliente con paquetes marcados usando WFQ

Through-put	Max(ms)	Min(ms)	Promedio(ms)
Valor	1703	11	1115

Tabla 12 Valores pico y promedio del Trough-put en cliente con paquetes marcados usando WFQ

La siguiente figura muestra como el ***sniffer*** reconoce que los paquetes en realidad sí están llegando a las interfaces marcados.

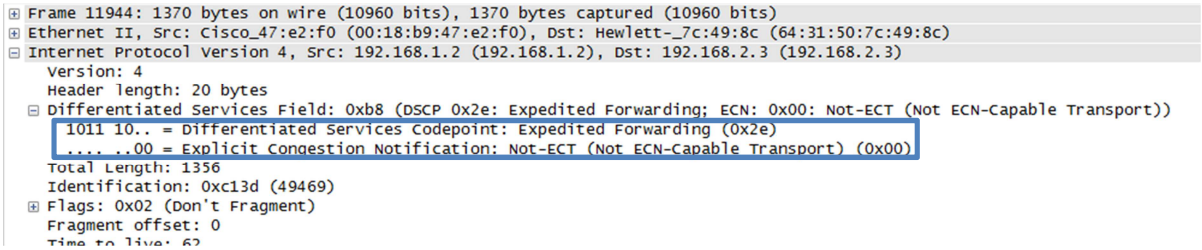

Figura 44 Vista del Sniffer donde se muestra que el paquete está marcado

8.2.2. Resultados de tráfico marcado por defecto

Las características de la captura en este cliente las muestra la **figura 45**

Total RTP packets = 8333 (expected 8333) Lost RTP packets = 986(11,83%) Sequence errors =195
Duration 119,99 s (-373 ms clock drift, corresponding to 90080 Hz (-0,09%)

Figura 45 Cracterísticas de la captura en cliente con paquetes sin marca usando WFQ

La **figura 46** y la **tabla 13** muestran los resultados respectivos de la magnitud de *Jitter*.

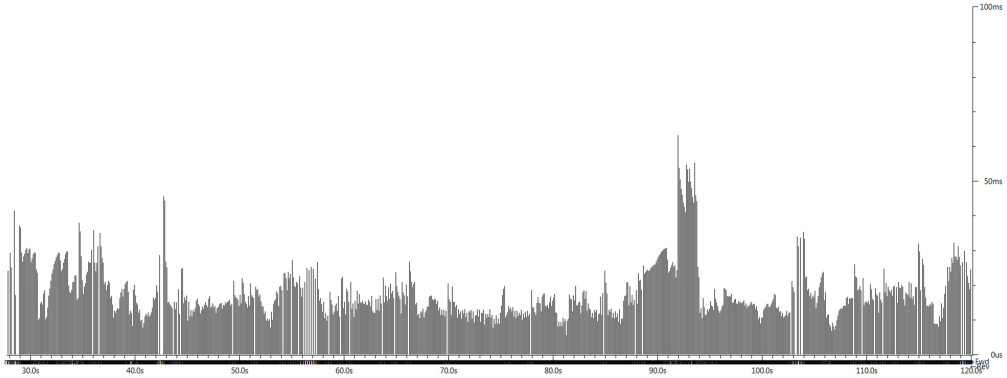

Figura 46 Jitter en cliente con paquetes sin marca usando WFQ

Jitter	Max(ms)	Min(ms)	Promedio(ms)
Valor	63,09	0,00	14,73

Tabla 13 Valores pico y promedio de Jitter en cliente con paquetes sin marca usando WFQ

Los valores de OWD, **figura 47** y **tabla 14**.

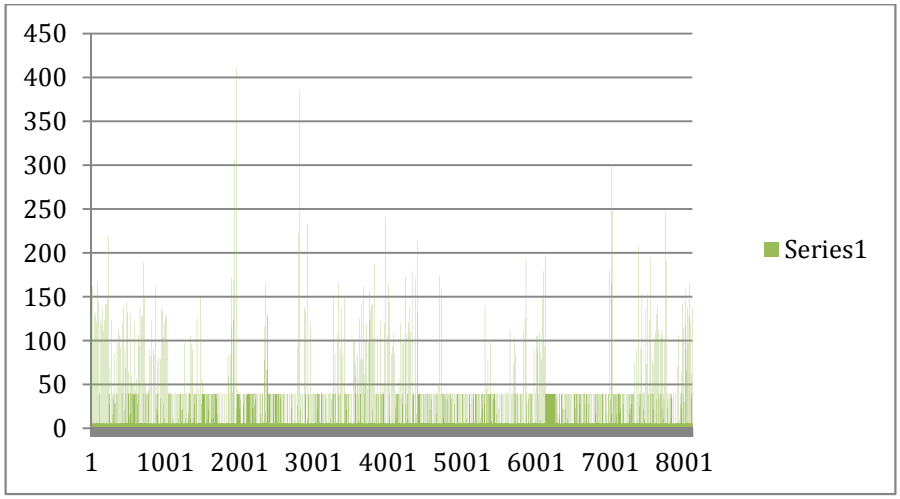

Figura 47 Valores del OWD en cliente con paquetes sin marca usando WFQ

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	411,35	0,00	14,80

Tabla 14 Valores pico y promedio del OWD en cliente con paquetes sin marca usando WFQ

En la **figura 48**, se muestra como el *sniffer* detecta que en el campo DSCP no se ha configurado ningún valor diferente a cero, que es el valor por defecto de este campo.

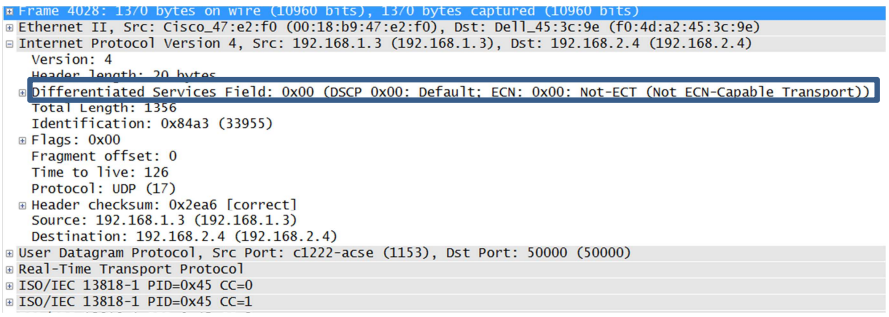

Figura 48 Vista del Sniffer donde se muestra que el paquete no está marcado

8.3. CB-WFQ

Esta prueba se realiza con el fin de gestionar de manera dinámica el ancho de banda ya que el método ***WFQ*** ya tiene pre-establecidas las prioridades que se le dan a los paquetes según su valor en el campo ***DSCP***.
Cuando se aplicó la configuración mostrada en la sección 8.4.3. Los resultados no fueron los esperados, ya que no fue evidente la gestión de ancho de banda que se le configuró al ***router*** y los videos sufrieron problemas en su reproducción, entonces, por efecto de estos problemas que no se pudieron solucionar y que se deja como tema abierto para futuros trabajos en este tema no se utilizó dicha configuración.

Los resultados que se muestran a continuación son resultado de alterar la configuración para demostrar que las políticas asignadas en la interfaz serial del ***router*** sí se aplican y que el problema radica en saber exactamente cómo se gestiona el ancho de banda en los ***routers*** Cisco.

Los cambios en la configuración se basan en la asignación de la política en la clase GOLD, en la cual se había destinado con el comando '***Bandwidth***' un ancho de banda de 120kbps. Este comando se remplaza por el comando ***'drop'*** para que todo paquete que entre en dicha clase sea descartado produciendo que el video ni siquiera se reproduzca.

La prueba se desarrolla de la siguiente manera: se inició la transmisión con el comando ***'drop'*** funcionando y después de cierto tiempo se deshabilita para provocar que los paquetes que hagan parte de la clase ***GOLD*** pasen. Todo esto para visualizar que la política sí se cumple en la interfaz y los paquetes son tratados según dicha configuración. Los resultados obtenidos se muestran a continuación.

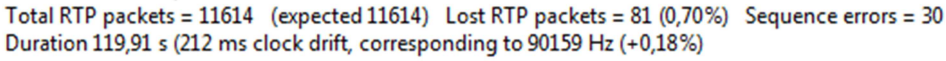

Figura 49 Características de la captura en el cliente donde llegan los paquetes marcados usando CB-WFQ

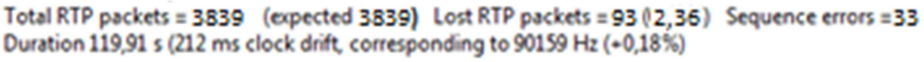

Figura 50 Características de la captura en el cliente donde llegan los paquetes sin marca usando CB-WFQ

La gráfica de ***Jitter*** y sus valores pico y promedio para el cliente donde arriban los paquetes marcados se muestran en la **figura 51** y **tabla 15**

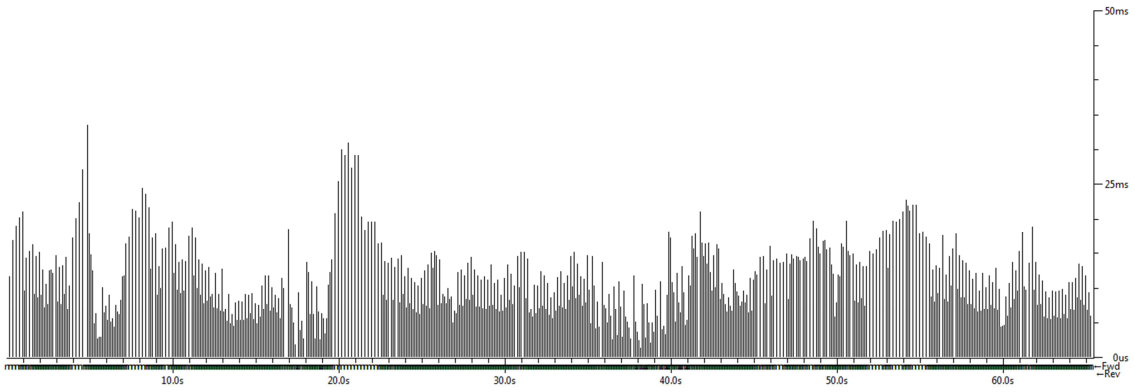

Figura 51 Jiiter en cliente con paquetes marcados usando CB-WFQ

JITTER	Max(ms)	Min(ms)	Promedio(ms)
Valor	33,41	0,0	9,08

Tabla 15 Valores pico y promedio de Jitter en cliente con paquete marcados usando CB-WFQ

La **figura 52** y la **tabla 16** muestran los valores de OWD en el cliente donde llegan los paquetes marcados.

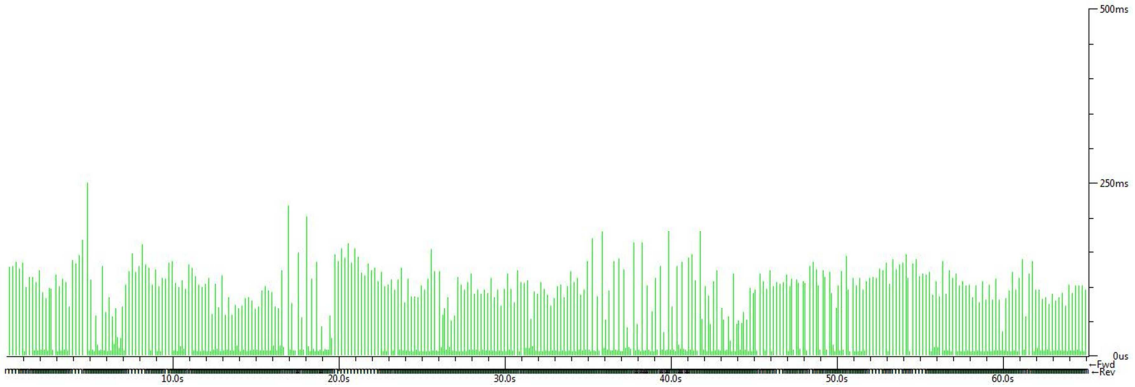

Figura 52 OWD en cliente donde llegan los paquetes marcados usando CB-WFQ

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	248,74	0,0	10,4

Tabla 16 Valores pico y promedio de OWD en cliente con paquetes marcados usando CB-WFQ

La **figura 53** y la **tabla 17** muestran los valores del caudal utilizado por el cliente con paquetes marcados.

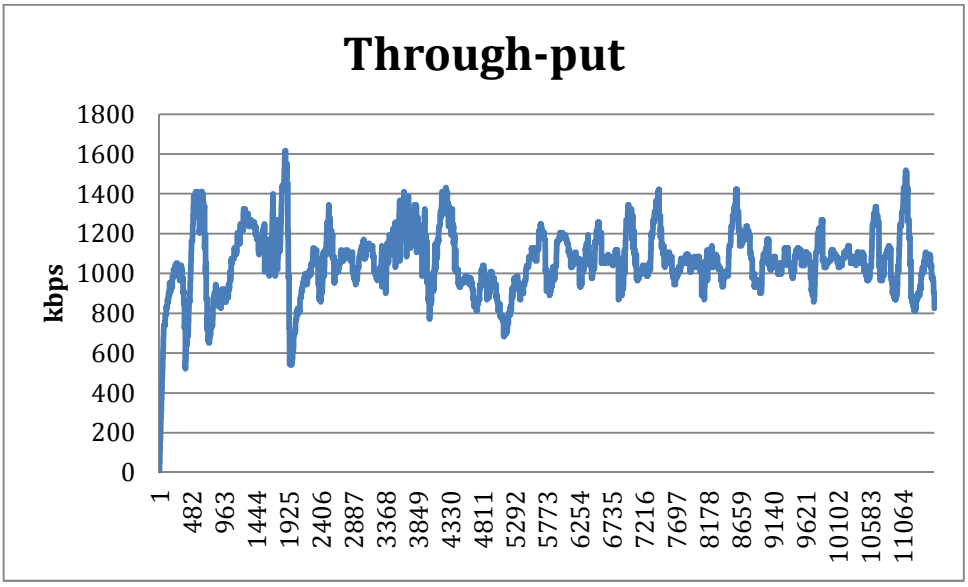

Figura 53 Through-put en comunicación entre servidor-cliente con paquetes marcados usando CB-WFQ

Through-put	Max(ms)	Min(ms)	Promedio(ms)
Valor	1616	11	1061

Tabla 17 Valores pico y promedio del Caudal entre servidor-cliente con paquetes marcados usando CB-WFQ

La gráfica de ***Jitter*** y sus valores pico y promedio del cliente donde arriban los paquetes sin marca se muestran en la **figura 54** y **tabla 18.**

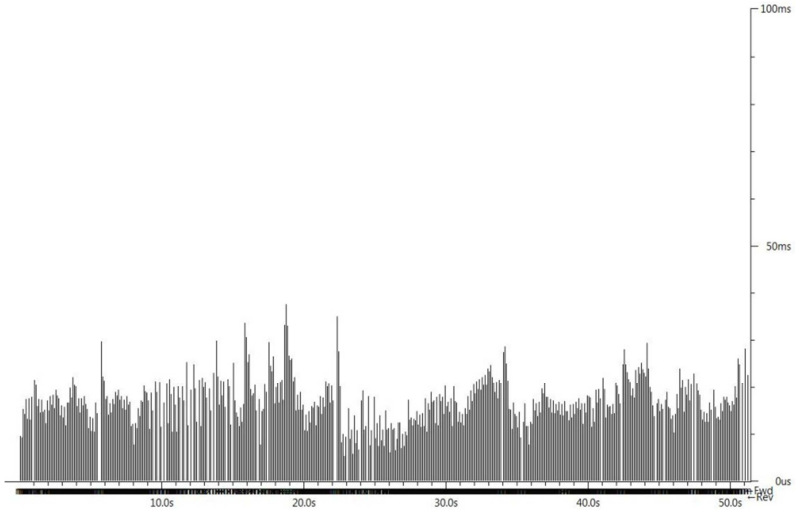

Figura 54 Jitter en cliente con paquetes sin marcar usando CB-WFQ

JITTER	Max(ms)	Min(ms)	Promedio(ms)
Valor	37,39	0,0	14,27

Tabla 18 Valores promedio y pico de Jitter en cliente con paquetes sin marcar usando CB-WFQ

La gráfica de OWD y sus valores pico y promedio del cliente donde llegan los paquetes sin marcar se muestran en la **figura 55** y **tabla 19.**

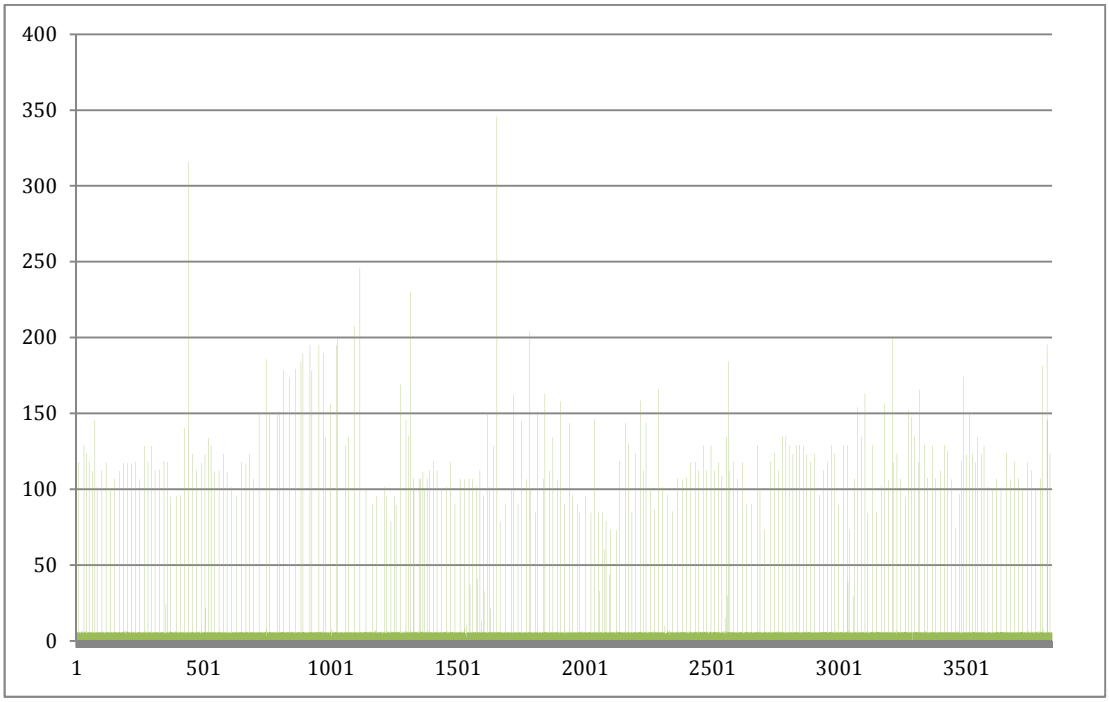

Figura 55 OWD en cliente con paquetes sin marca usando CB-WFQ

OWD	Max(ms)	Min(ms)	Promedio(ms)
Valor	345,75	0,0	13,38

Tabla 19 Valores pico y promedio de OWD en cliente con paquetes sin marcar usando CB-WFQ

La gráfica del ***Through-put*** y sus valores pico y promedio del cliente donde llegan los paquetes sin marcar se muestran en la **figura 56** y **tabla 20.**

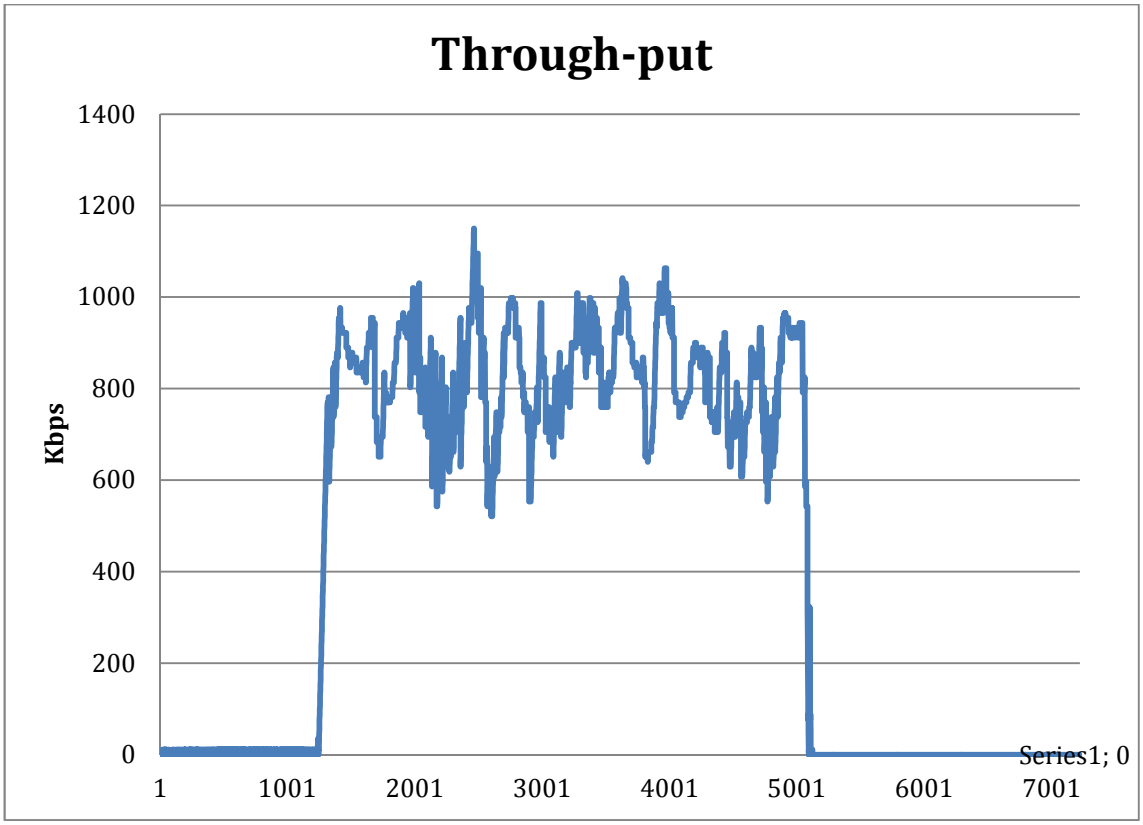

Figura 56 Throug-put en cliente con paquetes sin marcar usando CB-WFQ

Through-put	Max(kbps)	Min(kbps)	Promedio(kbps)
Valor	1150	11	819

Tabla 20 Valores pico y promedio del through-put en cliente con paquetes sin marcar usando CB-WFQ

9. ANALISIS DE RESULTADOS

El análisis de los resultados del capítulo anterior se hace a continuación comparando cada una de las estrategias de encolamiento que se muestran en el capítulo anterior.

9.1. FIFO

Se realizaron dos pruebas para este tipo de encolamiento, una en la cual no hay congestión del canal y otra donde sí.

Los resultados en estas pruebas son evidentes, mientras el canal no está congestionado la transmisión es excelente y sin errores, mientras que al estar congestionado la calidad del ***streaming*** se deteriora notablemente hasta el punto que el audio y el video se distorsionan completamente.

A continuación se hace un paralelo de las magnitudes de los parámetros de evaluación de calidad de servicio medidas durante el transcurso de la transmisión entre servidor y cliente. Como primer punto se muestran los resultados obtenidos en la prueba donde se hay congestión y luego de los datos de la prueba donde no.

9.1.1. Comparación transmisión de dos clientes.

Las **tablas 21** y **22** muestran el paralelo de la prueba donde el canal se congestiona.

	Paquetes analizados	Paquetes perdidos (%)	# De errores de secuencia	Jitter promedio (ms)	OWD promedio (ms)	BW utilizado promedio (kbps)
Cliente con marca DSCP	12245	4,54	206	8,68	10,28	1052
Cliente sin marca DSCP	9152	8,83	320	12,46	12,59	876

Tabla 21 Comparación de resultados usando FIFO

Magnitud	Valor Máximo con marca	Valor máximo sin marca
Jitter	29,82 ms	35,19 ms
OWD	289,11 ms	367,9 ms
Through-put	1421 kbps	876 kbps

Tabla 22 Paralelo de valores máximos

La diferencia en el número de paquetes analizados durante la captura se atribuye a que el servidor que realizaba la transmisión de los paquetes marcados tiene mejores recursos de

máquina, debido a esto logra hacer la transcodificación del audio y del video con una mayor velocidad, lo que a su vez permitía el envío de paquetes con una mayor frecuencia que el otro equipo transmisor y por ello la diferencia de 3093 paquetes que podría en algún momento confundirse con que hay prelación por los paquetes que llegaban marcados lo cual en este caso no es así; a las interfaces del *router* llegan más paquetes desde esa fuente durante los 2 minutos de transmisión por la calidad de los equipos usados. A su vez Esto justifica que el cliente asociado al servidor más eficiente experimente menor cantidad de paquetes perdidos y errores de secuencia. De igual forma los valores de pérdida de paquetes y errores de secuencia están lejos de ser los datos de una transmisión excelente ya que un valor del **4,54%** de paquetes perdidos es considerable en este tipo de aplicaciones sin sumarle los problemas de tiempo de llegada de los que sí alcanzaron a arribar y por no hacerlo en el momento indicado también producen errores en la reproducción del archivo, esto se ve en la **tabla 21** donde se puede apreciar que los valores máximos de los parámetros medidos son altos para los dos clientes demostrando la congestión que existe en el enlace y demostrando las diferencias en el rendimiento de los dos servidores.

Las mediciones de ***Jitter***, ***OWD*** y caudal en sus valores promedio no son tan alarmantes o a simple vista no manifiestan que la transmisión sea pésima, hay que aclarar entonces que no se está analizando un caso real de red donde los paquetes antes de llegar a su destino tienen atravesar largas distancias y ser tratados por muchos equipos de conectividad como ***routers***, antenas y ***switches***. Esto se traduce en magnitudes muy altas en un entorno de cuello de botella como se simula en este caso de estudio. Adicional, al no existir para este trabajo algún acuerdo de nivel de servicio SLA, no existe definición de umbrales para estos valores que dictaminen qué tan bueno o malo es el valor de estos datos.

9.1.2. Transmisión congestionada Vs Transmisión sin congestión

La prueba sin congestión se realiza utilizando el servidor que tenia mejores recursos de maquina entre los dos, por esta razón se comparan los resultados obtenidos en este mismo cliente durante la prueba con congestión en el canal. Las **tablas 23 y 24** muestran la comparación entre las magnitudes obtenidas.

Como se puede apreciar, la prueba sin congestión es contundente ante los datos de la prueba con el canal congestionado. No se pierden paquetes y las magnitudes de ***Jitter*** y ***OWD*** son menores en relación a la prueba con congestión, adicionalmente el promedio del caudal en la comunicación utilizado aumenta en la prueba sin congestión demostrando así que había más libertad para los paquetes de usar el canal. Los datos se tomaron después de reproducir el video por un tiempo de dos minutos.

	Paquetes analizados	Paquetes perdidos (%)	# De errores de secuencia	Jitter promedio (ms)	OWD promedio (ms)	BW utilizado promedio (kbps)
Prueba con congestión	12245	4,54	206	8,68	10,28	1052
Prueba sin congestión	11886	0	0	8,42	10,05	1094

Tabla 23 Comparación de resultados con congestión y sin congestión usando FIFO

Magnitud	Valor Máximo con congestión	Valor máximo sin congestión
Jitter	29,82 ms	25,29 ms
OWD	289,11 ms	180,98 ms
Through-put	1421 kbps	1768,22 kbps

Tabla 24 Paralelo de valores máximos, congestión vs. no congestión

9.2. WFQ

El objetivo de la prueba con este tipo de encolamiento es mostrar cómo se le otorga prioridad a los paquetes marcados en el campo ***DSCP*** de la cabecera ***IP*** según el valor que se halla configurado en dicho campo. Hecho esto se compara con la estrategia ***FIFO*** para analizar cual de las dos produce mejor comportamiento en la transmisión.

	Paquetes analizados	Paquetes perdidos (%)	# De errores de secuencia	Jitter promedio (ms)	OWD promedio (ms)	Through-put promedio (kbps)
Cliente con tráfico marcado	11573	0	0	8,30	10,19	1115
Cliente con tráfico sin marca	8333	11,83	195	14,73	14,80	774

Tabla 25 Comparación de resultados usando WFQ

La **tabla 25** deja claro que los paquetes que provengan del servidor que marque los paquetes no encuentran ningún tipo de embotellamiento en el enlace ***WAN*** y se transmiten sin problemas, usando un caudal alto, y manifestando valores pequeños tanto de ***Jitter*** como de *OWD* resaltando la alta calidad de la transmisión en términos de ***QoE***. Mientras tanto, los paquetes que llegan desde el otro servidor encontraron un canal muy congestionado abarcado por el tráfico marcado con el valor 'EF' en su campo DSCP lo cual provocó que dicha difusión experimentara muchos errores, un ***Jitter y OWD*** más altos y un caudal efectivo considerablemente más bajo ya que no alcanzo los 1000 kbps. Los datos

demuestran claramente como el método ***WFQ*** reconoce a qué información le debe dar prelación sobre las demás en los casos donde la red o el canal estén congestionados o saturados.

Si se compara el funcionamiento de esta estrategia con la estrategia ***FIFO***, es claro que ***WFQ*** utiliza las cualidades de las técnicas ***DiffServ*** para administrar los recursos de la red mientras que cuando no hay encolamiento **(FIFO)** no hay una mínima optimización del uso de los enlaces siendo perjudicial en redes de alto tráfico. La **tabla 26** muestra para el cliente donde llegaban los paquetes con nivel de servicio 'EF' los resultados cuando hubo encolamiento y cuando no.

	Paquetes analizados	Paquetes perdidos (%)	# De errores de secuencia	Jitter promedio (ms)	OWD promedio (ms)	Through-put promedio (kbps)
WFQ	11573	0	0	8,30	10,19	1115
FIFO	12245	4,54	206	8,68	10,28	1052

Tabla 26 Comparación WFQ vs. FIFO en cliente donde llegan los paquetes marcados

Se aprecia claramente que WFQ tiene un rendimiento muy bueno mientras que FIFO sufrió los problemas de un canal congestionado en el cual se pierden paquetes, se generan secuencias de error, los tiempos de llegada de la información varían y son más altos ***(Jitter* y OWD)** además del caudal, el cual es mayor cuando se trabaja con WFQ.

9.3. CBWFQ

Como se menciona en el capítulo anterior, la gestión de ancho de banda utilizando esta estrategia de ***QoS*** no funcionó como se esperaba y por tanto la prueba se enfocó en demostrar otras posibilidades que se tienen para realizar el tratamiento, administración y control del tráfico que circulan a través de la red o que llegan al ***router*** con dichas políticas implementadas.

La razón que se propone como causa de que la gestión de ancho de banda no se diera se debe a las dimensiones de la red. CB-WFQ se hace fuerte cuando los ***routers*** donde se configuran las políticas **realmente** son ***routers*** de frontera, es decir, si la WAN utilizada no fuera una simulación hecha mediante una interfaz que tiene un ancho de banda angosto sino que se utilizara una mayor cantidad de equipos de procesamiento y(o) enrutamiento, esto ocasionaría un aumento en las magnitudes de los parámetros de QoS (Jitter, OWD, Through-put) que aportaría a que la clasificación de los paquetes en las colas creadas y la asignación de ancho de banda mediante las clases y las políticas puede ser más efectivo.

Para efectos de mostrar cómo las políticas configuradas en las interfaces del ***router*** dictaminan qué entra y(o) sale de este, se bloquea el tráfico IP que no satisface la Lista de control de Acceso (*ACL*) configurada en la clase IPTV. Los resultados que se recopilaron se

muestran en la **tabla 27**. La prueba nuevamente fue una captura de dos minutos de transmisión.

	Paquetes analizados	Paquetes perdidos (%)	# De errores de secuencia	Jitter promedio (ms)	OWD promedio (ms)	BW utilizado promedio (kbps)
Cliente con tráfico GOLD	3839	2,39	33	14,27	13,38	819
Cliente con tráfico IPTV	11614	0,7	30	9,08	10,40	1061

Tabla 27 Comparación de resultados configurando CB-WFQ en el router

Lo primero que se observa es que la cantidad de paquetes analizados por el ***sniffer*** es muy diferente en cada clase esto se debe a que durante gran parte de la transmisión el tráfico IP estuvo bloqueado y por ello el ***stream*** que corresponde a la clase ***GOLD*** ni siquiera atraviesa el ***router*** durante cierto tiempo de transmisión, como sí sucedió con el tráfico de la clase IPTV. Los paquetes que se pierden en la clase IPTV se dieron durante los momentos en los cuales el comando 'drop' de la clase GOLD estaba habilitado.

La figura 54 muestra como se comporta el uso del canal en el cliente donde llegan los paquetes sin marcar durante la transmisión, se aprecia como durante un tiempo la conversación entre servidor-cliente era nula y luego aumenta repentinamente, debido al efecto del comando 'drop'. Esto evidencia como el uso de las técnicas que abarca CB-WFQ permiten mucha versatilidad a la hora de decidir qué se necesita hacer con cada tipo de información que llegue al ***router*** de frontera de una LAN en particular.

Para resumir el análisis presentado, se muestra la **tabla 28**, donde se muestra el paralelo de todas las pruebas y de todas las métricas tomadas en cada cliente como también el comentario de la calidad del video.

Prueba vs. Medidas	# de paquetes	% Perdidos	# Errores de secuencia	Jitter	OWD	Through -put	QoE
FIFO Sin marca	9152	8,83	320	12,46	10,28	876	Muchos errores y la calidad de la recepción es inaceptable
FIFO Con marca	12245	4,54	206	8,68	10,28	1052	Muchos errores y la calidad de la recepción es inaceptable
WFQ Sin marca	8333	11,83	195	14,73	14,80	774	El video se reproduce mal y no es aceptable
WFQ Con marca	11573	0	0	8,30	10,19	1115	Reproducción sin errores y perfecta
CB-WFQ GOLD	3839	2,39	33	14,27	13,38	819	Transmisión bloqueada en varios intervalos. En los momentos de transmisión había congestión
CB-WFQ IPTV	11614	0,7	30	9,08	10,40	1061	Con congestión, se reproduce si errores, cuando sí hubo, aparecieron retardos y pérdida de imagen y audio

10.CONCLUSIONES

Luego de observar el comportamiento de los paquetes bajo 3 tipos de estrategias de QoS distintas se llegó a las siguientes conclusiones.

Dependiendo del tipo de red se debe implementar una estrategia de ***QoS***, ya que siempre existirán servicios que requerirán ciertos recursos de red inexorablemente y si las redes no son capaces de ofrecer los mínimos requerimientos para ello, los usuarios nunca van a estar conformes con las aplicaciones que usan. En las redes ***WAN*** reales, la información atraviesa muchos saltos representados por sistemas activos de conectividad y medios físicos que aumentan la probabilidad de que exista pérdida de calidad y por ende malos servicios. Para este tipo de redes mantener una estrategia ***FIFO*** es totalmente errado ya que es normal que en algún momento la red presente congestión y esta estrategia carece de la inteligencia para saber qué servicios son más críticos y vulnerables al retraso. Para evitar esto son necesarias técnicas que le permitan a los ***routers*** tomar decisiones con mayor criterio que protejan el funcionamiento por sobre todo de esos servicios como las comunicaciones de voz o las transmisiones de video en los cuales la pérdida de paquetes y la llegada no sincronizada de los datos resulta fatal a la hora utilizar dichas aplicaciones y donde en muchos casos los usuarios han pagado más dinero que otros para gozar de mayor calidad de imagen, audio y disponibilidad. Para ello existen técnicas como ***WFQ*** donde por defecto se toman esas decisiones partiendo de la información que contenga el campo ***DSCP*** de la cabecera ***IP*** de los paquetes que llegan a los ***routers*** y ***CB-WFQ*** la cual le permite al administrador de red decidir cómo quiere que los equipos de conectividad actúen ante cada tipo de tráfico.

Las pruebas realizadas demostraron que cuando se usa ***FIFO*** en un ambiente congestionado no se puede obtener una buena recepción de los videos en ningún momento y el porcentaje de perdida de paquetes es del **8,83%** para el caso de estudio. Esta estrategia no es conveniente aplicarla en ambientes reales donde todos los problemas que se pudieron observar en laboratorio se multiplican debido a las grandes distancias físicas de los enlaces y el sin número de equipos de procesamiento que van a recibir a los paquetes durante su transmisión.

Las pruebas ***WFQ*** dejaron ver que es la estrategia más sencilla de configurar en los routers cisco y la que su funcionamiento se da de la manera más transparente al administrador de red ya que todas las políticas de decisión ya vienen configuradas por defecto permitiendo tratar de manera preferencial el tráfico, gestionando de manera definida el ancho de banda según el valor en el campo ***DSCP*** que tengan los paquetes. Para el caso de estudio al configurar uno de los videos con una marca '***EF***' y el otro con cero, el ***router*** dio total prelación a dicha marca y asignó un ancho de banda tal que no se presentó perdida de paquetes, errores de frecuencia y los valores de ***Jitter y Delay*** fueron bajos respecto al otro video. Donde llegaron los paquetes sin marcar hubo una pérdida del ***11.83%*** de los

paquetes, siendo esta la mayor perdida de paquetes de las pruebas adicional a que ***Jitter y OWD*** fueron mayores en un ***77,4% y 45,2%*** respectivamente.

El uso de la estrategia CB-WFQ no cumplió los objetivos de gestión de ancho de banda pero dejó claro que es una herramienta poderosa ya que permite una manipulación más personalizada de la información. Utilizando el comando ***'drop'*** en la política configurada en la salida de la terminal WAN del ***router*** se logra decidir de forma particular qué iba a pasar con los paquetes durante la transmisión ya que los eliminó todos los que iban a uno de los clientes durante el tiempo que estuvo activo produciendo que durante una captura de dos minutos donde en promedio dicho cliente recibía entre 8000 y 9000 paquetes RTP solo se contabilizaran 3839. Además, poder utilizar ***ACLs*** en este tipo de configuración de ***QoS*** da la posibilidad de filtrar y seleccionar los paquetes de muchas formas permitiendo construir todo un complejo de parámetros de decisión para el ***router*** según las necesidades que se presenten.

En resumen, es claro que la información que se transmite por redes y que es sensible al tiempo necesita que se le garantice el valor de ancho de banda, que exista control de ***Jitter*** y retardo para poder reproducirse en cualquier usuario que requiera del contenido. Para esto las técnicas de ***QoS*** facilitan esta misión y bajo la comparación hecha, es claro que no todas las estrategias producen los resultados esperados. Así como el encolamiento en momentos de congestión es necesario para evitar la pérdida de paquetes, si el tiempo que estos permanecen dentro de los Buffers es muy largo también habrá problemas en la calidad del servicio. Por tanto hay que promover un término medio entre estas herramientas.

11. SUGERENCIAS PARA FUTUROS TRABAJOS

Así como la elaboración de este documento deja una gran cantidad de aprendizaje y conocimientos nuevos también abre posibilidades que no son parte de los alcances de este trabajo pero que pueden significar futuros e interesantes estudios en materia de ***QoS*** y transmisión de contenido multimedia a través de redes.

En primer lugar, experimentar con otras técnicas de encolamiento y ***QoS*** podría traer consigo conclusiones adicionales a las que se llegaron en el presente documento. Estrategias como ***Intserv, CQ, PQ, LLQ, WRED*** pueden ser manipuladas en muchas formas.

Construir un prototipo de red, o tener la disponibilidad de equipos para implementar una red más compleja que obligue a los equipos de conectividad a tomar más decisiones y por ende exigir a los ingenieros que configuren dicha red de implementar estrategias muy eficientes para que los servicios se otorguen de la mejor forma a los hosts.

Ampliar el tipo de servicio multimedia, incluyendo Voz y ***Multicasting***. En este documento solo se aplicó ***Unicasting*** siendo más sencilla la configuración de la red. Servicios como Videoconferencias, y transmisiones en vivo requieren saber las diferencias entre estos dos conceptos y cómo se implementan cada uno.

Siempre y cuando se logren implementar redes más complejas, es muy pertinente no solo congestionar la red mediante tráfico idéntico, sino tráfico que exija requerimientos de red distintos, es decir, redes que presten servicios sobre ***TCP, UDP, RTP*** y que no solo sean unidireccionales sino que se logren aplicaciones donde el usuario también proporciona un tráfico importante aguas arriba de la red, involucrando todo esto aplicaciones interactivas que son muy comunes en la actualidad.

12. ANEXOS

Se anexa los enlaces para ver la hoja de especificaciones de los ***routers*** Cisco 2811 utilizados en este trabajo.

http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68.pdf

BIBLIOGRAFIA

[1]. Simpson, Wes. Greenfield, Howard. IPTV and Internet Video: Expanding the Reach of Television Broadcasting. Ed.2. OXFORD,UK. Elsevier 2009.

[2]. Hardy, William C. QoS Measurement and Evaluation of Telecommunications Quality of Service. USA. Jhon Wiley & Sons LTD. 2009

[3]. Estados Unidos de America, KNOWLEDGENET, Implementing Cisco Quality of Service QoS V2.0 Student Guide. 2004, 1067p

[4]. Barreiros, Miguel. Lundqvist, Peter. QOS-ENABLED NETWORKS Tools And Foundations. USA. Jhon Wiley & Sons LTD. 2011

[5]. Nichols, K. , Blake , S. , Baker , F. and Black , D. (1998) RFC2474, Definition of the Differentiated Services Field. 1998.

[6]. Le Faucheur. F. and Lai, W. RFC3564, Requirements for Support of Differentiated Services – Aware MPLS Traffic Engineering. 2003.

[7]. San Francisco, USA. Cisco Systems. DiffServ The Scalable End To End Quality Of Service Model. 2005 19p

[8]. San Fco, USA. Cisco Systems. Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting. 2008 8p.

[9]. San Fco, USA. Cisco Systems, Understanding Jitter In Packet Voice Networks (Cisco IOS platforms). 2006 7p.

[10]. San Fco, USA, Cisco Systems. Cisco IOS software: Quality of Service The Differentiated Service Model (DiffServ). 2001. 4p

[11]- San Fco, USA. Cisco IP/TV and QoS: How to Enable IP Precedence on an IP/TV Server for Use with QoS Policy. 1999. 3p

[12]. Alarcón Llamas, Ricardo. Título: “Estudio e implementación de mecanismos de calidad de servicio sobre una arquitectura de servicios diferenciados”. Universidad Politécnica de Cartagena. Enero 2003.

[13]. Álvarez Moraga, Sebastián A.; González Valenzuela, Agustín J. Título: “Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM”.

[14]. Caliad de Servicio (QoS) en redes [diapositiva]. Sevilla, España, Dra Maria del Carmen Romero Ternero [28 diapositivas].

[15]. Protocolos de datagramas de Usuario UDP disponible en: http://personales.upv.es/rmartin/TcpIp/cap02s11.html

[16]. USA, Tektronix. A Guide to MPEG Fundamentals and Protocols Analysis. Mpeg Tutorial. 2000. 58p.